情報セキュリティビジネスに関する調査

調査報告書

情報処理振興事業協会
セキュリティセンター
目次

（サブテーマA）情報セキュリティビジネスの実態調査

1. 調査の概要.................................................................2
   1.1 調査の背景..........................................................2
   1.2 調査の目的..........................................................2
   1.3 調査方法の概略...................................................2

2. 情報セキュリティビジネスの定義 ..................................3
   2.1 情報セキュリティビジネスの背景 ...............................4
       2.1.1 情報化投資の増加........................................4
       2.1.2 インターネット利用の拡大................................4
       2.1.3 電子商取引の市場規模拡大..............................6
       2.1.4 ウイルス被害の拡大......................................7
       2.1.5 不正アクセス被害の拡大................................7
       2.1.6 家庭通信環境における常時接続化の拡大...............8
   2.2 情報セキュリティビジネスの定義 ................................8
       2.2.1 情報セキュリティの定義..................................8
       2.2.2 情報セキュリティビジネスの定義........................9
   2.3 情報セキュリティビジネスの枠組み..........................10

3. 情報セキュリティビジネスの産業構造.............................11
   3.1 情報セキュリティビジネスの構造的特徴........................12
   3.2 情報セキュリティビジネスの対象.............................12
       3.2.1 セキュリティ製品.......................................13
       3.2.2 セキュリティサービス..................................18
       3.2.3 セキュリティ関連サービス.........................20

4. 情報セキュリティビジネスの市場動向............................23
   4.1 日本の市場動向................................................24
       4.1.1 国内のセキュリティ製品市場..........................26
       4.1.2 国内のセキュリティサービス市場...................31
       4.1.3 国内のセキュリティ関連サービス市場.............33
   4.2 米国の市場動向................................................36
       4.2.1 米国のセキュリティ製品市場.......................38
4.2.2 米国のセキュリティサービス市場 ................................................................. 38
4.2.3 米国のセキュリティ関連サービス市場 ......................................................... 39
4.3 日米の情報セキュリティ市場の比較 ................................................................. 40
4.3.1 セキュリティ分野シェア比較 ................................................................. 40
4.3.2 セキュリティ分野金額比較 ................................................................. 41
4.3.3 セキュリティ製品・サービスの導入の状況比較 ............................................... 43

5. 情報セキュリティビジネスの成功と失敗 .......................................................... 44
5.1 各ビジネス分野における成功 / 失敗要因 ...................................................... 44
  5.1.1 セキュリティ製品 ................................................................. 44
  5.1.2 セキュリティサービス ................................................................. 48
  5.1.3 セキュリティ関連サービス ................................................................. 49
5.2 ビジネス分野共通の要因 ................................................................. 50

6. 情報セキュリティビジネスにおける課題 .......................................................... 51
6.1 技術面の課題 ................................................................. 51
6.2 人材面の課題 ................................................................. 51
6.3 制度面の課題 ................................................................. 52

（サブテーマ B）ITセキュリティ評価・認証制度に関する市場予測

1. 調査の概要 ................................................................................................. 55
  1.1 調査の背景 ................................................................................................. 55
  1.2 調査の目的 ................................................................................................. 55
  1.3 調査方法の概略 ................................................................................................. 55

2. セキュリティ評価・認証制度に関する分析と課題 .......................................... 56
  2.1 セキュリティ評価・認証制度の国際動向 .................................................. 57
    2.1.1 海外におけるセキュリティ評価・認証制度 ........................................... 57
  2.2 日本におけるセキュリティ評価・認証制度の経緯 ....................................... 58
  2.3 ISO/IEC 15408 とは ......................................................................................... 59
  2.4 我が国のセキュリティ評価・認証体制 ..................................................... 61
  2.5 調査の実施 ................................................................................................. 63
    2.5.1 調査目的 ................................................................................................. 63
    2.5.2 調査方法 ................................................................................................. 63
    2.5.3 調査項目 ................................................................................................. 63
    2.5.4 調査結果 ................................................................................................. 64
  2.6 問題点の抽出 ................................................................................................. 66
2.6.1 人材面.....................................................................................................................67
2.6.2 体制面.....................................................................................................................68
2.6.3 技術面.....................................................................................................................68
2.6.4 経済面.....................................................................................................................69
2.6.5 その他.....................................................................................................................69
2.7 問題点の整理 ............................................................................................................70

3. ITセキュリティ評価・認証制度の普及対策の提言.........................................................71
3.1 基本認識 .....................................................................................................................71
3.2 他のISO認証制度（ISO9000）との比較 .................................................................71
  3.2.1 体制面 ..................................................................................................................71
  3.2.2 コスト面 ...............................................................................................................72
3.3 対策 .............................................................................................................................72
  3.3.1 人材面 ..................................................................................................................72
  3.3.2 体制面 ..................................................................................................................72
  3.3.3 技術面 ..................................................................................................................73
  3.3.4 経済面 ..................................................................................................................74
  3.3.5 まとめ ..................................................................................................................74

4. セキュリティ評価・認証制度に関する市場予測............................................................75
4.1 現状の申請状況 .........................................................................................................75
4.2 利用者側の需要 .........................................................................................................75
  4.2.1 企業アンケート調査結果 .......................................................................................75
  4.2.2 ヒアリング調査 ...................................................................................................76
4.3 供給者側の取組状況 .................................................................................................76
  4.3.1 ヒアリング調査 ...................................................................................................76
4.4 他の認証制度の普及状況 .........................................................................................76
  4.4.1 ISO9000シリーズ .................................................................................................76
  4.4.2 ISO14000シリーズ ...............................................................................................77
4.5 IT評価・認証制度の市場予測....................................................................................77
  4.5.1 前提条件 ................................................................................................................78
  4.5.2 推計 ........................................................................................................................79
（サブテーマ A）
情報セキュリティビジネスの実態調査
1. 調査の概要
1.1 調査の背景
情報処理振興事業協会セキュリティセンターにおいては、2001年3月に「情報セキュリティビジネスに関する調査報告書」を公開した。

しかし、これ以降の、情報セキュリティに関する新技術・新サービスの開発・普及、xDSL普及等のインフラの変化、電子商取引等の市場構造の変化、電子署名法をはじめとする制度整備の進展、米国同時多発テロ発生等の社会情勢の変化、アウトソーシング拡大や企業間アライアンス拡大等の市場構造の変化などから、情報が陳腐化している部分もある。

このような環境の変化とともに、昨今の景気低迷にも影響され、情報セキュリティビジネスの先行きは不透明な状況にある。情報セキュリティビジネスの総体を把握、整理し、高度知識集約産業としての情報セキュリティビジネスが健全に発展しているかを検証する必要があった。

1.2 調査の目的
前回調査との連続性を重視しつつ、社会・市場等の外部環境の変化に応じて対象を追加・見直しして、情報セキュリティのビジネス・市場の現状と見通しを明らかにする。これにより情報セキュリティビジネス提供事業者および参入意向者に対して、ビジネス実施のためのガイダンス資料を提供する。

1.3 調査方法の概略

ヒアリング調査・アンケート調査

→ 情報セキュリティビジネス産業構造調査

→ 情報セキュリティビジネス市場動向調査

→ 情報セキュリティビジネス成功/失敗 要因の分析、考察

→ 情報セキュリティビジネス活性化のための課題検討

ヒアリング調査:
企業等36社に対しヒアリング調査を実施。

アンケート調査:
Webによるアンケート調査を実施。有効回答数は、個人115名、企業233件。
2. 情報セキュリティビジネスの定義

情報セキュリティビジネスは、企業にとって厳しい経営環境が続く中で着実にその規模を拡大している。その背景には様々な要因が存在するが、インターネット利用の拡大、電子取引の市場規模拡大、ブロードバンドの進展、コンピュータウイルスや不正アクセス被害の拡大などが挙げられる。

本調査においては、「情報セキュリティビジネス」を「情報セキュリティを存立維持させるためのビジネス」と定義し、「セキュリティ製品」、「セキュリティサービス」、「セキュリティ関連サービス」の3つのカテゴリーに分割して整理した。

・「セキュリティ製品」は、アンチウィルスソフトウェア、ファイアウォール、認証関連商品など。

・「セキュリティサービス」は、情報セキュリティシステム設計・構築サービス、ウイルス・不正アクセス監視サービス、情報セキュリティポリシー策定支援サービスなど。

・「セキュリティ関連サービス」は、セキュリティ保険サービス、セキュリティ関連教育、セキュリティ関連書籍出版サービスなど。
2.1 情報セキュリティビジネスの背景
情報セキュリティは、ビジネスとして既に大きな地位を占めており、その規模は確実に拡大している。その背景には、インターネット利用の拡大、電子商取引の市場規模拡大、家庭でのインターネット環境におけるブロードバンド化の広がり、また、それに伴うウイルス被害の拡大や不正アクセス被害の拡大などが挙げられる。

2.1.1 情報化投資の増加
情報セキュリティビジネスは、情報化投資の動向との関連が深いことが想定される。
企業における2002年度の情報化投資は、約5割の企業が増額の見通しで、現状維持を含めるとその割合は約7割に達する。企業の情報化投資への積極性が見受けられるこの現状は、情報セキュリティビジネスに対しても追い風といえる。

図表 2.1 2002年度の情報化投資の増減

資料：日本経済新聞朝刊(2002年8月29日)

2.1.2 インターネット利用の拡大
情報セキュリティビジネスは、インターネット利用の拡大にも大きく影響を受けている。インターネットはもはや一部の企業や特定の人間だけのものではなく、生活のあらゆる場面で利用される社会インフラと言いう切れる状況にある。
特に昨今は、世帯と事業所でのインターネット普及率の伸びが著しい。1997 年末には世帯のインターネット普及率はわずか 6%程度だったが、2001 年末には約 61%とほぼ 10 倍へと成長している。事業所についても同約 12%から約 68%へと 5 倍以上の伸びを見せている。300 人以上の企業についても、世帯や事業所と比較すると伸び率は低いが、1997 年末で約 68%だったが 2001 年末には 100%に近づいて来ている。
インターネットは家庭でもビジネスでも、もはや欠かすことのできない社会インフラとなった。

資料：総務省 2001年「通信利用動向調査」(2002年8月29日)
2.1.3 電子商取引の市場規模拡大
情報セキュリティが求められる分野に電子商取引の分野がある。ネットワーク上で行われる商取引情報は情報セキュリティ上保護されるべきであり、従って電子商取引の市場規模拡大に伴って情報セキュリティビジネス市場も広がると捉えることができる。
電子商取引の BtoB 市場規模は、確実に拡大している。1998 年には約 8 兆円程度だったが 2001 年には約 34 兆円と約 4 倍の伸びを示している。

図表 2.4 電子商取引 BtoB 市場規模の推移

資料：経済産業省、ECOM、NTT データ経営研究所
「平成 13 年度電子商取引に関する市場規模・実態調査」(2002 年 2 月 18 日)

また電子商取引の BtoC 市場規模は、BtoB 市場以上に拡大傾向が顕著である。1998 年には約 645 億円程度だったが 2001 年には約 14,840 億円を記録し約 23 倍の伸びを見せており、今後のさらなる発展が見込まれる。

図表 2.5 電子商取引 BtoC 市場規模の推移

資料：経済産業省、ECOM、NTT データ経営研究所
「平成 13 年度電子商取引に関する市場規模・実態調査」(2002 年 2 月 18 日)
2.1.4 ウイルス被害の拡大
コンピュータウイルスも、情報セキュリティビジネスと密接に関係する。ウイルス被害の拡大は情報セキュリティビジネスの動向を左右する重要なファクタとなる。ウイルス届出件数は 2002 年には前年に比べやや減少したが、1998 年から 4 年間で約 10 倍に伸びている。2003 年 1 月にも「W32/SQLSlammer ワーム」（「Sapphire」と呼ばれることもある）が全世界で猛威をふるうなど下火となる兆しは見えていない。

図表 2.6IPA/ISEC ウイルス届出件数の推移

資料：情報処理振興事業会議セキュリティセンター（IPA/ISEC）

2.1.5 不正アクセス被害の拡大
2.1.6 家庭通信環境における常時接続化の拡大

家庭での通信環境の変化もまた情報セキュリティビジネスを牽引する重要な要素の1つと考えられる。家庭での通信環境のブロードバンド化は急速に拡大している。2000 年末時点ではブロードバンド環境とは CATV 網を利用したインターネット接続サービスとはほぼ同義で、約60万程度の利用者であったが、2001年になりADSL サービスが普及し2002年末にはブロードバンド接続加入者数が約800万弱と2年間で約12倍の伸びを示した。ブロードバンド化の拡大は同時に家庭でのインターネットへの常時接続につながっており情報セキュリティに対する利用者の意識も高まってきた。

資料：総務省「インターネット接続サービスの利用者数等の推移【平成14年12月末現在】（速報）」（2003年1月31日）
（2002年5月10日）においては、「情報セキュリティ」を以下のように定義した。

「情報セキュリティとは、正当な権利を持つ個人や組織が、情報やシステムを意図通りに制御できる性質である」

上記の定義は、以下の性質を満足させることを条件とする。

☑ 可用性
「システムを必要とする場合に所定の方法で利用および制御できること」
システムを構成するハードウェア・ソフトウェア・ネットワークが障害を起こすことなく稼働するという従来の可用性の概念に加え、決められた方法によりシステムの利用を制御できる性質を示す。関連する脅威は、不正アクセス、ドン攻撃、誤作動、コンピュータウイルス、運用に係わる問題、天災である。

☑ 一貫性
「情報の正確性および完全性が維持されていること」
主として、データベース中の情報および運用に係わる情報の、正確性および完全性が維持される性質を示す。関連する脅威は、不正アクセス、誤動作、運用に係わる問題である。

☑ 機密性
「情報が組織および個人により決められた規定通りに守秘されること」
権限のあるものによって、権限のある際に、権限のある方式に則って、情報が守秘される性質を示している。関連する脅威は、機密情報漏洩、成りすまし、詐欺、著作権侵害、プライバシ侵害である。

☑ 道徳性
「情報の公開および流通が組織の信用失墜を招かないこと」
情報の公開が組織の信用失墜を招かないことを示す性質である。具体的には、組織内での有害ペー等の閲覧が該当する。

2.2.2 情報セキュリティビジネスの定義
本調査においては、「情報セキュリティビジネス」は「情報セキュリティを存立維持させるためのビジネス」の意味で使う。
ただし、バックアップや無停電源装置など障害や停電などの情報セキュリティに関連する製品、サービスに関しては対象に含めていない。
また、情報セキュリティの存立維持のために必要となるハードウェアや媒体等も対象に含めない。例えば、ルーター自体は、情報セキュリティとは直接の関係を持たないハードウェアである。よって、ルーターを情報セキュリティビジネスの対象とはしない。情報セキュリティ機能を保有したルーターも存在するが、ルーター本来の製品目的と情報セキュリティと
は無関係であるため情報セキュリティビジネスの対象外とする。

なお、ルーターに対する情報セキュリティ機能の設定支援サービスについては、情報セキュリティを機能させるビジネスであり、情報セキュリティビジネスの範疇とする。

2.3 情報セキュリティビジネスの枠組み

情報セキュリティビジネスの対象を以下の枠組みで整理した（図表 2.9）。

情報セキュリティビジネス全体を大きく 3 つに分類する。「セキュリティ製品」、「セキュリティサービス」および「セキュリティ関連サービス」である。

図表 2.9 情報セキュリティビジネスの対象範囲（概観）
3. 情報セキュリティビジネスの産業構造

本章においては、情報セキュリティビジネスの構造を示す。情報セキュリティ製品・サービスの提供から利用までの流れを示し、その構造の特徴に触れること。

情報セキュリティビジネスの枠組みは、前述のとおり分岐に渡っており、そのビジネス構造全体を大まかに表すと以下の図のとおりとなる（図表 3.1）。

個々の製品・サービスについて、以降において詳細を述べる。なお、情報通信関連機器やサービス等に対して情報セキュリティ機能・サービスを付加するなど、情報セキュリティは、これまで以上に重視されまたコモディティ化している現状があることを付記しておく。

図表 3.1 情報セキュリティビジネスの産業構造概観
3.1 情報セキュリティビジネスの構造的特徴
情報セキュリティに対する関心や対策は、もはや特別なものではなく、一般に不可欠なものになってきたと言うことができる。その要因として、前章で述べたとおりインターネット利用の拡大、電子商取引の市場規模拡大、ウィルス被害・不正アクセス被害の拡大、家庭通信環境における常時接続化の拡大などが挙げられる。また、情報セキュリティに対する意識としてウィルス被害、コンピュータへの不正侵入、データの改ざん・破壊・盗聴の脅威に不安を感じるユーザが少なくない。こうした状況から、情報セキュリティ機能が単体で提供される場合には少なくなりつつあり、情報セキュリティ機能はあくまでも付加価値として提供されることが増えている。すなわちネットワーク機器、コンピュータソフトウェア、OS など多岐に渡る製品がセキュリティ機能を搭載しないと売れない、あるいはセキュリティ機能を搭載しているからこそユーザに選択される、という状況になりつつある。例えばセキュリティ機能が強化されたからこそネットワーク通信装置が売れる、などの状況である。

3.2 情報セキュリティビジネスの対象
情報セキュリティビジネスの対象となる各分野を概観する。まず、その分野が対象とする製品、サービスについて触れ、次に可能であればさらに詳細な分類を行い、また産業構造としての成り立ちを簡略に図示する。
なお、本調査においては、情報セキュリティビジネスの対象としてはいないが、暗号化機能を保有したメールソフトウェアや Web ブラウザ、情報セキュリティ機能を搭載したルーターなども増加しつつある。ブロードバンドルーターに付加された情報セキュリティ機能としてパケットフィルタリングや IP マスキャレードなどが挙げられるが、そのような情報セキュリティ機能を保有した機器市場は ADSL 普及などに伴うインターネットへの常時接続化とともに急激な拡大傾向を見せている。情報セキュリティ機能は特殊機能ではなく、本来、情報セキュリティに関連しない製品・サービスの付加価値機能として搭載されることが増えつつある。
3.2.1 セキュリティ製品

セキュリティ製品は、アンチウィルスソフトウェア、セキュリティ運用ソフトウェア、ファイアウォール・VPN(Virtual Private Network)、認証関連製品、暗号関連製品に分類することができる。

(1) アンチウィルスソフトウェア
「コンピュータウイルス対策基準」(通商産業省告示第 952 号)(2000年12月28日)では、コンピュータウイルスを以下のように定義している。

コンピュータウイルス
「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。」

✓ 自己伝染機能
自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

✓ 潜伏機能
発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

✓ 発病機能
プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能
アンチウイルスソフトウェアは、一般にコンピュータシステムがウイルスに感染しないように防御するためのソフトウェアである。感染しないように監視する機能のほか、感染しているかどうか検査する機能、および感染した場合に駆除する機能などがある。
アンチウイルスソフトウェアを、その搭載されるハードウェアによって分類する。通常のデスクトップマシンに適用するものを「クライアント型」。インターネットのゲートウェイマシンなどに適用するものを「ゲートウェイ型」。その他ファイルサーバーやグループウェアサーバーなどに適用するものを「サーバー型」とした。

アンチウイルスソフトウェアは、アンチウイルスソフトウェアベンダーから提供される。個人ユーザへはメーカー製品のパソコンにバンドルされた形で提供されることも多くある。

(2) セキュリティ運用ソフトウェア
セキュリティ運用ソフトウェアは、フィルタリングソフトウェア、セキュリティ検査ツール、セキュリティ監視ツール（不正侵入検知ツール、IDS（Intrusion Detection System））ラグ解析ツールに分類することができる。ここで、セキュリティ検査ツールとは、ネットワーク上のファイアウォールやルーターを含む機器が正常に動作するかどうかや、ネットワーク上のセキュリティホールの有無を診断するとともに、ネットワーク上の潜在的に存在する
弱点を発見しリスクを評価、レポート化するためのツールである。これまで情報セキュリティリスクの中でも比較的外部からの攻撃に対する意識は高かったが、近年では特に情報漏洩など内部からのリスクも問題となってきた。また、ログ解析ツールについてはマーケティングツールとしての役割も拡大しており新たな展開が期待される。

図表 3.5 セキュリティ運用ソフトウェアの分類

セキュリティ運用ソフトウェアは、主に SI 事業者（System Integrator）を通じて公的機関や民間企業へ行われている。特にログ解析ツールについては販売代理店を通じての販売が主である。しかし、アンケート調査によると不正侵入検知ツールの法人への導入率は約3割弱と一般に行き渡っているとは言えない状況にある。

図表 3.6 セキュリティ運用ソフトウェアの産業構造
(3) ファイアウォール・VPN(Virtual Private Network)

ファイアウォールは、内部ネットワークと外部ネットワークの間に設置され、通過するネットワークトラフィックを監視し許可された通信のみを行えるようにし、ネットワークへの不正侵入や破壊行為を未然に防止するための機能を持ったソフトウェアまたはハードウェアのことである。ここではそれらを大きく3つに分類する。ソフトウェアのファイアウォール製品と、ファイアウォールにVPN機能が付加されたファイアウォール・VPN アプライアンス、およびVPN専用機である。

インテルネットが社会インフラ化し前述の通り法人個人を問わずインターネット接続を行うようになった現在、ファイアウォールの設置が拡大している。個人環境においては、ADSL等ブロードバンド化の動きに合わせ常時接続環境が一般化しつつあり、ファイアウォールの設置もそれに合わせて広まることが予想される。

(4) 認証関連製品

認証関連製品は、ワンタイムパスワード製品、ICカード・トークンデバイス製品、バイオメトリックス製品、PKI（Public Key Infrastructure）関連製品などに分類される。リモートオフィスでの利用や外出先から社内ネットワークシステムへのモバイルアクセスなどで利用されることも多く、市場規模は大きいとは言えないが今後伸びて行く可能性のある分野である。
図表 3.9 認証関連製品の分類

導入は、主に法人向けである。しかし、例えばICカードの導入率は約15%程度と普及が進んでいるとは言えない。ただし企業内部への侵入され、操作権限のない端末を勝手に操作されるなどの物理的なセキュリティのリスクへの意識が高まりつつあるため、今後拡大して行くことが予想される。また、電子政府、電子自治体、GPKI（Government Public Key Infrastructure）などの普及によります公的機関、それに伴い民間企業へと展開して行くことも予想される。

また日本製製品が強い分野でもある。他セキュリティ製品分野ではほとんど存在しないが認証関連製品では例えば指紋認証製品などは日本製製品の輸出も行っている。

図表 3.10 認証関連製品の産業構造

(5) 暗号関連製品

ネットワーク上の情報セキュリティ保護を暗号化により行う製品。機密性の高い情報を盗聴、なりすませ、改ざんから守る。暗号化方式には大きく公開鍵暗号方式と共通鍵暗号方式の2つがある。公開鍵暗号方式では、RSAや楕円曲線暗号、共通鍵暗号方式ではDESが有
名である。
メールソフトウェア、Webブラウザなどに暗号化機能を標準搭載するケースが増えているが、前述の通り、それら暗号機能を搭載したメールソフトウェア、Webブラウザについては情報セキュリティビジネスの範疇には含まないこととする。

図表 3.11 暗号関連製品の分類

<table>
<thead>
<tr>
<th>暗号関連製品</th>
</tr>
</thead>
<tbody>
<tr>
<td>暗号化ソフトウェア</td>
</tr>
<tr>
<td>公開鍵暗号ソフトウェア</td>
</tr>
<tr>
<td>共通鍵暗号ソフトウェア</td>
</tr>
</tbody>
</table>

暗号関連製品は主に法人向けに提供されている。個人向けの提供もあるが1割にも満たない導入率であり規模は大きくない。法人でも暗号化製品の必要性については5割以上が「必要がないと判断」もしくは「必要性が分からない」としており、エンドユーザの意識が変わらない限り市場は大きくは拡大しないものと考えられる。

図表 3.12 暗号関連製品の産業構造

3.2.2 セキュリティサービス
セキュリティサービスは、セキュリティシステム構築サービス、セキュリティ管理サービス、セキュリティコンサルティングサービスに分類することができる。

(1) セキュリティシステム構築サービス
セキュリティシステム構築サービスは、ネットワークセキュリティツールや技術を用いて行うシステム設計構築サービスのことである。すなわち前述のセキュリティ製品などを用いてシステムを設計・構築するサービスと言い替えることができる。
図表 3.13 セキュリティシステム構築サービスの分類

セキュリティシステム構築サービスは、システムインテグレータによりエンドユーザに提供される。提供は公的機関と民間企業であり個人ユーザは対象としていない。

図表 3.14 セキュリティシステム構築サービスの産業構造

(2) セキュリティ管理サービス

セキュリティ管理サービスは、不正アクセス監視サービス、ウイルス監視サービス、電子認証サービス、インターネット VPN サービス、ファイアウォール運用管理サービスなどのことである。コスト削減や運用負担の軽減、セキュリティレベルの向上を図る目的で、情報セキュリティ対策の一部をアウトソーシングする動きがある。またネットワークセキュリティ管理を総合的にアウトソーシングしたいというニーズも立ち上がっている。

図表 3.15 セキュリティ管理サービスの分類

セキュリティ管理サービスは、公的機関と民間企業、個人に向けて提供されている。そのほとんどは、公的機関と民間企業向けへの提供であるが、個人向けに ISP(Internet Service Provider)が提供するウイルス監視サービスがインターネット利用者に対する導入率約 4 割弱と一般化しつつある。
(3) セキュリティコンサルティングサービス

セキュリティコンサルティングサービスは、情報セキュリティ検査サービスと情報セキュリティポリシー策定サービスとからなる。情報セキュリティ監査や、ISO/IEC 15408、BS7799、ISMS 適合性評価制度（Information Security Management System）等の認証制度の拡大、電子政府の実現に向けて市場の拡大が見込まれる分野である。また継続的に対策を行う必要がある分野であることから継続的な需要が期待される。

セキュリティコンサルティングサービスは、公的機関と民間企業に向けて提供されている。特に情報セキュリティポリシー策定サービスについては積極的に取り組んでいる企業も多い。

3.2.3 セキュリティ関連サービス

セキュリティ関連サービスは、セキュリティ保険サービス、セキュリティ関連教育、セキュリティ関連書籍出版に分類することができる。
(1) セキュリティ保険サービス
セキュリティ保険サービスは、情報セキュリティ上のリスクの備えとしての保険サービスのことである。例えば、不正アクセス、DoS 攻撃（Denial of Service attack）、コンピュータウイルスによる被害、機密情報の漏洩、データ破壊、商標権侵害などのさまざまなリスクに対する保険である。セキュリティ保険サービスはセキュリティコンサルティングサービスとアライアンスを組んでいることが多い。これは、保険加入時に保険料算定のため情報セキュリティリスク分析としてのコンサルティングサービスが必要であること、また、コンサルティングの一環としてのセキュリティ保険サービスの提案というオプションがあることにより、お互いにメリットを享受できるためと考えられる。
セキュリティ保険サービスは、公的機関と民間企業向けに提供されており基本的に個人向けには提供されていない。国内損害保険会社は、今後セキュリティ保険サービスへの注力を考えている。また特に米国の外資系保険会社が米国での市場の広がりとともに日本市場へ参入をしている。

図表 3.19 セキュリティ保険サービスの産業構造

(2) セキュリティ関連教育
セキュリティ関連教育は、主に資格試験対策教育と技術者教育の 2 つに大別される。
資格試験対策教育は基本的には個人を対象にするサービスである。しかし社員教育の一環として情報処理技術者試験対策を捉える企業もありその意味では個人ユーザのみならずセキュリティ機器ベンダー、SI 事業者などまで含めた全方位的にサービスの提供を行っていると言うことができる。
また技術者教育は、主に民間企業や公的機関の職員に対する通信教育や外部セミナーへの参加、社内研修への外部講師の利用などがある。外部セミナーにおいては、テキスト作成や、独立系コンサルタントへの講師業務など外部委託することが多い。また通信教育の販売や OEM 供給などのアライアンスもある。
(3) セキュリティ関連書籍出版
セキュリティ関連書籍出版は、基本的には個人を対象とするサービスである。ただし法人の情報セキュリティ対策用に購入することも当然予想され個人ユーザのみならず法人も含めてサービスの提供を行っていると見ることができる。
ただし、セキュリティ関連書籍を購入したことのある個人は約 10％、法人は約 15％と広く普及しているとは言い難い状況となっている。また未購入の理由として、個人・法人ともに「必要がない」とも「必要性が分からない」をもつ花合が約 70％となっている。
情報セキュリティ自体に対する意識は高まりつつある状況にある、これに併せてセキュリティ関連書籍出版に対するニーズも上昇してくると考えられる。
4. 情報セキュリティビジネスの市場動向
本章においては、前述した次の11分野を情報セキュリティ市場として動向調査、分析を行った。日本市場、米国市場ともに様々なデータをもとに動向を調査、整理をした。加えて、情報セキュリティ事業者及びセキュリティ利用者に対するヒアリング調査、情報セキュリティ利用者に対するアンケート調査を実施し、生の声を拾いながら予測・分析を行った。

【セキュリティ市場 11分野】

Ⅰ. セキュリティ製品市場
（1）アンチウイルスソフトウェア
（2）セキュリティ運用ソフトウェア
（3）ファイアウォール・VPN（Virtual Private Network）
（4）認証関連製品
（5）暗号関連製品

Ⅱ. セキュリティサービス
（1）セキュリティシステム構築サービス
（2）セキュリティ管理サービス
（3）セキュリティコンサルティングサービス

Ⅲ. セキュリティ関連サービス
（1）セキュリティ保険サービス
（2）セキュリティ関連教育
（3）セキュリティ関連書籍出版
4.1 日本の市場動向

2001年度の日本国内の情報セキュリティ市場は、セキュリティ製品市場が約9億円、セキュリティサービス市場が約1,856億円、セキュリティ関連サービス市場が約108億円で合計2,953億円と推測できる。5年後の2006年度にはセキュリティ製品市場が約3,836億円、セキュリティサービス市場が約6,135億円、セキュリティ関連サービス市場が約346億円で合計1兆318億円することが予測される。

情報セキュリティビジネスの市場動向に対する考え方として、以下のように整理・分析した。市場において、システム全体の情報化投資を含むセキュリティ投資に対する意思決定がされる。よって、情報化投資の動向と連動する。近年では情報化投資に占める情報セキュリティ投資の割合は平均15%となっており、1つの投資分野として認識されている。公共市場においては、情報化の整備・充実という観点に加え、電子政府化の進展や国の施策などを反映する形で情報セキュリティ製品やサービスの導入が進む。また、個人市場においては、家庭でのブロードバンド化の進展は、情報セキュリティに対する関心やニーズを高め、情報セキュリティ製品の購入やサービスの利用が進むと考えられる。いずれの市場においても情報セキュリティに対する考え方の初期段階と充分に浸透した状態とでは情報化費用に対して情報セキュリティ費用に使用する金額の割合も変化すると考えられる。

各市場の全体的な傾向を以下のように見ている。法人市場においては、大企業を中心情報セキュリティに関する知識や対応の必要性が浸透している。しかしながら、経済環境の悪化などから情報化投資も抑制の傾向にあり、一部の企業を除きネットワークの設定による対策やウイルス対策など限定的な導入にとどまっている。今後、BS7799やISMS等の適合性評価制度、ISO/IEC15408等の制度の浸透やセキュリティ監査の実施とともに総合的な情報セキュリティの重要性が認識されると、情報セキュリティビジネス本格化の局面を迎えることが予測される。

大企業においては、外向けの情報セキュリティ対策（ウイルス対策やファイアウォールの設置など）は実施のところが多く、今後は大企業を中心に内向きの情報セキュリティ対策（認証、情報セキュリティポリシー策定など）にも重点が移っていくことが予想される。一方で、中小企業においてはアンチウイルスソフトウェアなどの導入は進んでいるものの、大企業と比べて全体的にセキュリティ投資は遅れており、今後取引先の要請などからまず外向きの情報セキュリティ対策の需要が増えるものと予想される。

公共市場においては、住民基本台帳ネットワークの導入などに加え、電子政府化のための取り組みが進展している中で、これから市場が伸びる初期段階と言えよう。しかしながら、民間企業も公共機関も「情報セキュリティに対する投資価値は、従来の情報化投資の効果測定よりも難しくその費用対効果を定量的に示すことは難しい」と考えており、順調に拡大するとは言い難い。

個人市場においては、パソコンの普及（2002年3月末：57.2%）(4)とブロードバンドの普及
及び（2002年12月末：約781万契約、普及率約16.6%）（2）（3）で、情報セキュリティに関する
関心が高まっている。しかしながら、情報セキュリティ支出に対する意識は高くない。アン
ケート調査結果によると1年間の情報関連支出のうち情報セキュリティ商品・サービスに支
払っても良い金額は10%と未満と回答した人が約50%（うち年間情報関連支出で一番多い
ものは5〜10万円/年間で約6割を占める）と一番多く、続いて払う意志はない（無料なら
利用する）が約30%となっており、情報セキュリティに支払う意志は少ない。個人市場で需
要が顕在化するためには、時間が必要であろう。

注意：ブロードバンドユーザとは、xDSL、FTTH、CATVの契約者の合計を指す。世帯数は2000年10月の約4,700万
世帯を用いた。情報関連支出は情報機器の購入代金、ソフトウェアの購入代金、ADSL・ISP代金、データ通信
料、情報システム・パソコンなどの書籍・教育、情報サービスなどの情報に関連する全ての支出を指す。
資料：（1）IT投資予算に占める情報セキュリティ投資の割合=ソフトバンクパブリッシング、「N−H Network Guide
2003年2月号」
（2）ブロードバンド普及率=総務省、「インターネット接続サービスの利用者数等の推移」（2003年1月31日）
（3）世帯数=総務省、「統計情報統計センター世帯の種類、世帯人員別世帯数」（2001年10月）
（4）パソコン普及率=内閣府経済社会総合研究所、「耐久消費財普及率」（2002年3月）

図表4.1セキュリティ市場の予想推移
4.1.1 国内のセキュリティ製品市場

(1) アンチウイルスソフトウェア

■ 市場の動向

2001年度の市場は約241億円とセキュリティ製品の中ではファイアウォール・VPN市場に次いで2番目に大きい市場を持っている。2001年はウイルス被害が増加した年であり（2000年：11,109件・2001年：24,261件）、コンピュータ利用者にとってはアンチウイルスソフトウェアの導入は常識となりつつある。アンケート調査結果でも、アンチウイルスソフトウェアは法人ユーザの90%以上が利用し、個人でもインターネット利用ユーザの72%が利用している。

法人ユーザでは、大企業においては何らかの形でほとんどの導入済みであり、クライアント型に限らず、ゲートウェイ型、サーバー型の導入も進んでいる。今後、クライアント型ソフトウェアの導入が中心である中小企業においても、運用管理の容易さの点からゲートウェイ型、サーバー型ソフトウェアの導入が伸びる可能性が高い。個人ユーザはアンケート調査結果では約7割の人々が導入している。アンチウイルスソフトウェアがメール製品のパソコンにバンドルされていることや、ブロードバンド導入等の常時接続化によって必要性を感じて導入したユーザが多いことが予想される。

今後、法人ユーザへの導入が一通り済めば、ウィルス定義ファイルの更新などの運用・保守費用がビジネスの中心となり、安定的な収入源となる。公共ユーザはe-Japan戦略の推進により地方自治体の新規導入が進むことが予想される。また、個人ユーザのブロードバンド導入はしばらく続くと予想されるため、個人ユーザ向けアンチウイルスソフトウェアの導入は更に進むことが予想される。
市場予測要因の分析

（拡大要因）
法人市場：ウィルス定義ファイルの更新など保守サービスが安定的に提供される。
公共市場：e-Japan戦略、電子政府の実現に伴って地方自治体レベルまで導入が進む。
個人市場：家庭でのブロードバンド化に伴う常時接続化で意識が変わり、一層の導入が進む。
また、メーカ製パソコンにはアンチウィルスソフトウェアがバンドルされていることが多く、情報セキュリティを意識していない個人ユーザへの導入も進む。

（阻害要因）
業界構造：アンチウィルスソフトウェアはクライアント型、ゲートウェイ型、サーバー型のいずれのタイプも2〜3社のベンダーで8割以上のシェアを占めており、新規ベンダーの参入が難しいことから寡占市場となり、市場の硬直化の可能性がある。
個人市場：セキュリティの意識が充分に高まっていないユーザではバンドル製品の保守費用に継続して利用料を支払うとは限らず、新規需要が一巡した後は法人ほど安定的な収入が望めずは限らない可能性がある。

(2) セキュリティ運用ソフトウェア

市場の動向

本市場の製品としては「フィルタリングソフトウェア」、「セキュリティ検査ツール」、「セキュリティ監視ツール」、「ログ解析ツール」に大別される。特に外部からの不正アクセスなどの攻撃を防ぐ用途に使うIDS（Intrusion Detection System）は2001年度に約80億円の売上実績があり、今後も伸びが見込まれる。こうした製品群はファイアウォールやアンチウィルスソフトウェア導入後に更なる情報セキュリティ強化という観点で用いられることが多い。一部の大企業ではその局面に入っているが、まだ全体的に知名度や必要性が低い状態である。アンケート調査結果でもセキュリティ運用ソフトウェアは2〜3割の企業での導入にとどまっている。

今後は、大企業がISMS導入によるセキュリティ強化や不正アクセスからの防御のために、外からの脅威に対する防衛策として本製品を導入していくと考えられる。大企業においてこの動きが進めば中堅・中小企業でも導入の対象となることが考えられる。ただし、本製品の導入や運用には専門的知識が必要なため、中堅・中小企業ではASP（Application Service Provider）やアウトソーシングで導入されるケースが中心になるだろう。また、情報漏洩が問題になる中、企業のセキュリティの意識は外向きから内向きに向け、フィルタリングソフトやログ解析ツールの導入も進むものと見られる。本予測では中堅企業、中小企業の導入に加え、大企業も内向きのセキュリティ対策として導入する製品が増え、需要が一層伸びることを前提としている。
■ 市場予測要因の分析
（拡大要因）
法人市場：ISMS 適合性評価などの認証取得に伴いセキュリティ運用ソフトウェアの導入が必要となるケースが出てくる。
市場動向：ログ解析ツールは、市場が大きいファイアウォール・VPN などと連動しており、それらの製品の売れ行きに牽引される。また、これらのツールを実効的に運用するためにはより上位の情報セキュリティポリシーが必要となるため、それらのコンサルティングと合わせた導入が必要となり、総合的な需要が見込まれる。

（阻害要因）
製品特性：現時点でツールとしての認知度は低い。
業界構造：ネットワークや Web サーバー運用のアウトソーシングのサービスメニューとして無料化の可能性もある。
人材育成：セキュリティ運用ソフトウェアは専門的知識が必要なものが多いため、技術者の専門的な教育が必要となる。

(3) ファイアウォール・VPN
■ 市場の動向
セキュリティ製品の市場の中では、最も大きな売上を占める製品である。本市場の製品は認知度高く、大企業での導入は一通り済んでいる。アンケート調査結果でも約 8 割の企業が導入している。今ではこの製品の導入が中堅企業などにも拡大している。本市場はソフトウェア市場を中心に売上を伸ばしている。ファイアウォール・VPN は通信事業者や ISP (Internet Service Provider) などのネットワーク事業者に導入されるハイエンド機から一般企業で導入されるローエンド機まであり製品へのニーズが違う。
また、インターネット VPN は、アクセスラインに xDSL や光ファイバを利用し、インターネット上に仮想私設通信網を構築し、情報をやり取りするサービスである。インターネット上のデータを暗号化することにより、通常のインターネットより安全性を高めている。これら従来までの専用線の代わりに安価で広帯域の広域イーサネットや IP-VPN を利用するという動きとは別である。インターネット VPN はセキュリティが比較的確保されたインターネット網の利用という認識で、企業内もしくは特定企業間の通信に利用されており、安価なため適用範囲を広げつつある。インターネット VPN を実現する機器もこの市場に含まれており、導入が進むものと見ることがある。
今後、成熟しつつある本市場では、伸びは中堅企業への導入の進展とインターネット VPN の普及の度合いに左右されると考えられる。本予測では、大企業の一定割合のリプレースと
適度なインターネット VPN の普及を前提としている。

■ 市場予測要因の分析
（拡大要因）
製品特性：ファイアウォールはソフトウェアを利用する方式から性能バランスや運用管理の容易さから専用のハードウェア利用方式に移行しており、ハードウェアの売上は伸びる。
市場環境：ADSL、光ファイバの普及により、インターネット VPN の利用が促進される。
（阻害要因）
産業構造：成熟しつつある市場に、比較的多くの参入企業があり競争激化による収益増の可能性がある。

(4) 認証関連製品
■ 市場の動向
本市場の製品には「ワンタイムパスワード」、「IC カード」、「PKI 関連製品」、「バイオメトリクス」等、形状的に幅広い製品がある市場であるが、いずれも認証に利用される製品群である。全体的に市場が立ち上がっている時期であり、各製品の市場はそれぞれ大きくはない。PKI 市場に関しては情報政府、電子自営体関連への導入の広がりを見せており、今後もその傾向は続き、法人市場も含め伸びが期待できる。
今後、更なるセキュリティ意識の高まりと政府の GPKI（政府機関向け PKI）の普及などにより、周辺需要も含めて伸びることが予測される。認証製品としては、各分野の製品で代替性があるため市場全体が伸びたとしても、全ての製品で同様の需要があるわけではないことも考えられる。一方で、各製品の特徴を生かしながら機能を補完する利用も想定される。本予測では、複合的に認証方法が利用され各々の製品を補完し、連動して導入が進むことを前提としている。

■ 市場予測要因の分析
（拡大要因）
法人市場：ISMS 適合性評価制度認証取得などの方向からセキュリティ意識が高まり、社内での利用者認証などに対してもセキュリティ製品を導入する動向が出てくる。
公共市場：GPKI、住民基本台帳ネットワークの進展により、認証が必要な場面が出てくる。
運用範囲：モバイル用ノートパソコンの普及と外出先や自宅からのリモートアクセスの広がりでワンタイムパスワードの需要が伸びる傾向にある。ユーザが外出先や自宅から企業の閉域網に入るとときには、固定パスワードを利用するよりも、その時に限り有効なワンタイムパスワードを利用する方が安全である。そのため、勤務形態の多様化に利用される製品の 1 つであると言える。また、IC カードも入退室管
理や少額決済の用途にも利用されており、複合機能付製品としての需要も期待できる。
市場動向：1つの認証方法だけでなく、複数の認証方式を複合的に利用して導入される可能性がある。その場合、シナジー効果によりマーケットが伸びることが予測される。
（阻害要因）
技術問題：PKIは企業間取引においては、端末の仕様などを決めやすいが、個人の取引となるとそうはいかず、不具合の発生の要因となる可能性もあり、導入が進まない可能性もある。
認証方式：認証方法を複数設けることはコスト的にも運用的にも負荷が大きいため、全ての認証方式が生き残るとは限らない。
適用範囲：PKIはまだまだ適用範囲も狭く、対応アプリケーションが少ない。

（5）暗号関連製品
■ 市場の動向
インターネットの進展で、機密性の高い情報のやり取りを安全にするための対策やなりすまし・改ざん等を防ぐための対策として、電子メールの暗号化や電子署名機能に使われているのが暗号関連製品である。ただし、本機能がOSや電子メールソフトウェアの標準機能として搭載されつつあり、本製品を扱うベンダーは売上を当初の予定よりは伸ばすことができていない。アンケート調査結果でも導入企業は2割強と多くはない。
企業、公共機関のセキュリティ意識の高まりから本製品の機能は、今後重要視されることは確かだが、他ソフトウェアへの組み込みが進めば、単体での市場性が失われる可能性がある。特に暗号の標準化がどのような形で進むかによって、各ベンダーへの影響が変わるが、ベンダーが総合的なサービスとして仕掛け、もしくは他製品へのバンドルなどを進めなければ、暗号機能組み込み製品市場が成り立たなくなる可能性がある。本予測では、暗号の標準化がベンダーを中心に進み、企業、公共機関の需要の伸びることを前提とした。

■ 市場予測要因の分析
（拡大要因）
公共市場：e-Japan戦略、電子政府の展開により、公共市場でも本製品の需要が高まる可能性がある。
法人市場：セキュリティ意識の高い企業は導入を検討している。一定規模以上に広がれば、取引先にも広まる可能性が高い。また、ISMS適合性評価制度認証の取得支援や個人情報漏洩防止の手段としても有効であり需要を伸ばす要因となっている。
（阻害要因）
製品特性：メールソフトウェアやOSに標準で暗号化機能が組みこまれることにより、暗号
化ソフトウェア単体の市場は成り立ちにくくなる。
個人市場：個人市場では利用用途や意識の問題から暗号化の需要が増えない可能性がある。

4.1.2 国内のセキュリティサービス市場
(1) セキュリティシステム構築サービス
■ 市場の動向
本市場が2001年度で約1,700億円とセキュリティ市場で最も大きなシェアを占める。本市場のプレーヤは他のセキュリティ市場の製品やサービスを実際に適用する立場となる。
インターネットを利用した電子商取引などの増加により、システムにセキュリティ機能を組み込む必要性が増えることにより、本市場を牽引してきた。一方で、不正アクセス、情報漏洩、ウイルス被害などの報告件数は増える傾向にあり、情報システム全体を見たセキュリティを導入することが望まれるようになり、電子商取引をする企業のみならず重要情報を扱う全ての企業にとって不可欠なサービスであると言える。ただし、現在の経済環境下ではネットワーク構築時のセキュリティやウイルス対策の導入など部分的導入にとどまることも多い。しかしながら、総合的なセキュリティサービスへの需要は高く、導入は進むものと考えられる。本予測では、情報化投資が回復し、セキュリティに対する意識も高まっていくことを見込んでいる。

■ 市場予測要因の分析
（拡大要因）
法人市場：情報セキュリティ対策の不備や脆弱性からくる被害・報告が増え出てきており、セキュリティへの投資意欲は高まっている。そういった中でセキュリティを意識した総合的なSI（System Integration）サービスが求められている。特に、セキュリティについては専門知識が必要で統合的なセキュアなシステム構築から部分的なセキュアなネットワーク構築まで幅広い拡大用途が見込まれる。
公共市場：e-Japan戦略、電子政府の進展に伴い、法人企業同様に、セキュアなシステム、ネットワークが求められる。

（阻害要因）
法人市場：情報セキュリティ投資の費用対効果を測定・評価することは難しい。よって、セキュリティ投資に対する目標レベルの指標化などが進まない場合は阻害要因となる可能性がある。
業界構造：新規参入企業が多くなければ価格競争にさらされることになる。

(2) セキュリティ管理サービス
■ 市場の動向
市場は、企業のセキュリティに関連したアウトソーシング事業やネットワークサービスが主たるものである。現状は約111億円の市場であるが、数年で数倍→10倍の伸びが考えられる。中堅、中小企業においては、専門の技術者を置くよりも外部の専門サービス事業者に頼む方がコストパフォーマンスも良いことから利用が進むと見ることができる。また、電子認証サービス分野などでは国土交通省の公共工事の電子入札、法務省の商業登記に基づく電子認証制度、総務省の電子申請・届出システムなどの電子証明の利用が進んでいる。予測はサービスの受け手が大企業のみならず中堅、中小企業まで裾野を広げることと電子政府化の進展が順調であることを前提にした。

■ 市場予測要因の分析
（拡大要因）
法人市場：大企業から中堅、中小企業まで広く利用が期待できる。
電子認証：電子政府化により、電子認証サービスが促進される。
インターネットVPN：ADSL、光ファイバなどのアクセス回線の普及に伴い増加。

（阻害要因）
業界構造：事業者間の競争の激化に伴い、ウイルス検査サービスなどは基本サービスとして無料化する可能性もある。
電子認証：各サービス事業者が発行する電子証明書の相互認証が進まないと、利用者の負担が大きく、利用が促進されない可能性がある。
中小企業：サービスの受け手には中堅、中小業者が多く想定されるが、経済の停滞や人材不足から、需要が足る可能性もある。

(3) セキュリティコンサルティングサービス
■ 市場の動向
市場は、情報セキュリティポリシーの策定や事前のセキュリティ検査サービスといった企業のセキュリティ管理システムを構築する上でその上流・前段階のサービスのことを指しており、2001年度では約45億円の市場となっていたと推測される。情報セキュリティポリシーの策定は必ずしも情報システムだけを対象としたものではない。さまざまな観点から情報セキュリティ管理に関するポリシーを決めるもので、市場規模は大きくなる可能性がある分野である。ただし、現状では情報セキュリティポリシーの策定市場は一部の企業にとどまり拡がっていない。この要因として、限られた予算の中、個別製品の導入やセキュリティ設定などで情報セキュリティ対策を済ませ、セキュリティの専門知識を備えた人材が少なく必要性を十分理解できないことにある。情報セキュリティに対する意識は高まっていることから、今後は、情報システム構築などを含めた総合的なサービスとして伸びる可能性は充分にある。電子政府化の実現とともに公共分野の需要も期待できる。
また、企業がセキュリティを強化するための情報セキュリティポリシーの策定には、セキュリティ監査、認定資格の取得などがある。セキュリティ監査は一部の社会的インフラを担う企業や公共機関では行われるが、民間企業では一般的ではなく、今後の伸びが期待される。ISMS などの認定資格も認定数を増やしており、今後導入コンサルティングの需要が伸びると予想される。

■ 市場予測要因の分析
（拡大要因）
法人市場：ISMS 適合性評価などの制度が広がれば、情報セキュリティポリシーは必須となり、本市場への投資意欲も高まる。
公共市場：電子政府の実現に伴い、個別に情報セキュリティを判断するのではなく公共機関として総合的に判断できる基準として投資が高まる。
個人市場：企業取引においても情報セキュリティ確保が取引の要件となれば、企業と消費者との取引においても普及が進む可能性がある。

（阻害要因）
公共市場：ポリシー策定といった成果物に対し充分な対価を支払うという意識が薄い。
人材教育：セキュリティ全体を理解し、ポリシーを策定できる人材は技術者市場に不足していると言われている。需要に供給が追いつかなくなる可能性もある。

4.1.3 国内のセキュリティ関連サービス市場

(1) セキュリティ保険サービス
■ 市場の動向
情報セキュリティに関連する保険は、主にネットワーク事業者向けと一般企業向けのサービスがあるが、両方とも程度の需要がある。参入は大手損害保険会社のほか、外資系保険会社、中小損害保険会社も提供しているが、専門性の高い商品のため営業体制の整備や顧客への対応が難しく他の保険のように広範に売ることが難しい。しかしながら、大手損害保険会社と一部の外資系保険会社は積極的に売る体制ができつつある。

法人ユーザに対するアンケート調査結果では約 7%と導入数が、まだ少ないが、今後は企業の顧客情報の漏洩による損害賠償などが増えることも予測されるため、ネットワーク上で顧客情報を扱うような企業を中心に広がっていくと予想される。事前の診断によりセキュリティレベルが低いと認定された企業には保険をつけるない場合もあり、どの企業でも本サービスを購入できるわけではない。また、損害保険事業者と SI 事業者がアライアンスを組むことにより、セキュリティレベル検査やセキュリティポリシーの策定などが進展する動きもある。
■ 市場予測要因の分析
(拡大要因)
法人市場：ユーザの情報漏洩に対する意識が高まっている中、社員の過失などによる外部への加害に対する訴訟や損害賠償が増えれば企業として対応を考えざるを得なくなり、保険加入の動きが促進される。

(阻害要因)
業界構造：専門性の高いサービスのため販売、サービス説明のための要員が不足しており、広範な販売が難しい。
法人市場：セキュリティ保険に対する費用対効果が有効だと判断できなければ導入が進まない。

(2) セキュリティ関連教育
■ 市場の動向
IT 教育としては基礎教育から実践教育まで、長年行われているが、情報セキュリティ教育市場として数々に見れば立ち上がったばかりの市場である。経済産業省の情報処理技術者試験では 2001 年度から情報セキュリティアドミニストレータの区分を設けて、試験を毎年秋に実施している。応募者も、2001 年度 23,778 人(うち合格者 2,111 人)、2002 年度 34,352 人(うち合格者 2,788 人)と秋の情報処理技術者試験高度区分の中では 2 番目に多い応募者数となっており、セキュリティ資格への関心の高さがわかる。この他ではシステムベンダー主催のセキュリティのセミナーやトレーニングがあり、専門家の育成を促している。現在、セキュリティ技術者はベンダー側にもユーザ企業側にも不足感があるが、その他のセキュリティ市場の伸びを考えると今後もその傾向は続き、本市場も伸びが期待できる。
また、セキュリティ製品・サービスが浸透するにつれ、情報セキュリティに関する知識は管理職や企業内ユーザにも必要となり、啓蒙教育などの市場も期待できる。

■ 市場予測要因の分析
(拡大要因)
法人市場：セキュリティ技術者の不足が言われており、今後もこの傾向は続くため、技術者の育成の投資が続く。また、提供事業者のみならず、大企業のユーザ企業でもセキュリティ意識の高まりからセキュリティの専門家を育てようとする動きがある。
(阻害要因)
法人市場：資格試験の合格が人材育成に繋がらず、特定のベンダー製品のプロフェッショナルが優秀なセキュリティ技術者とは必ずしも言えないと判断されれば、投資が抑制される可能性がある。
(3) セキュリティ関連書籍出版
■ 市場の動向
情報セキュリティに関する書籍は、主に技術書と資格対策書籍、雑誌などの特集に大別される。技術書も特定の製品を詳しく説明する書籍から情報セキュリティポリシーに関する書籍など幅広い出版がなされている。また、前述のセキュリティ関連教育の情報セキュリティアドミニストレータ試験、およびネットワーク機器や OS のベンダー資格の書籍などが出版されている。情報セキュリティ意識の高まりにより、雑誌に特集記事なども増えている。資格試験対策書籍に関しては受験者数に応じて増減することが予測される。

■ 市場予測要因の分析
（拡大要因）
個人市場：ウイルス被害や不正アクセスが増えたことにより、専門書だけでなく初心者向けの書籍も多く出る可能性がある。アンチウイルソフトウェアやパーソナルファイアウォールなどの導入が進むにつれて利用方法などの書籍が市場に出る可能性がある。
法人市場：セキュリティ教育の一環として書籍購入が進む。
（阻害要因）
業界構造：専門書は教育機関と競合する可能性もある。
4.2 米国の市場動向

2001年度の米国の情報セキュリティ市場は、セキュリティ製品市場が約45億ドル、セキュリティ関連サービスも含め、セキュリティサービス市場全体が約47億ドルで合計92億ドルと推計できる。5年後の2006年度にはセキュリティ製品市場が約120億ドル、セキュリティサービス市場全体が約92億ドルで合計212億ドルとなることが予測される。

米国においては、2001年9月の同時多発テロ以降は、セキュリティに対する意識や行動が大きく変わっており、それぞれの企業がシステムの災害復旧対策の見直しを進めており、IT投資全体が冷え込む中でもITセキュリティ強化のための支出を2%以上増額した企業は、全体の4割近くに達している。また、米国のコンピュータセキュリティ研究所（CSI）と連邦捜査局（FBI）が2001年に実施した調査によると、回答した企業や政府部門に所属しているセキュリティ担当者のうち85%が「過去1年間の間に自社システムにおいてセキュリティ侵害を経験しており」、そのうち64%が「金銭的な被害を被った」としており、セキュリティ製品やサービスへの関心は高い。

また、2003年には正式なリスク評価手法が確立される可能性が高い。その場合、2004年～2005年にかけて、大企業は保険の適用範囲を拡大することにより企業リスクの軽減をはかるとともに、セキュリティ専門の担当者を育てると配置を急ぐことが予想される。それにあわせて、セキュリティシステムの導入も進むことになる。ユーザ管理の観点からは認証製品が市場に出始めていることから本人同一性管理などのセキュリティシステムは2004年頃までには普及が進むと見られている。その他のセキュリティ管理ソフトウェアは現在個別システムとして導入されている。今後はそれらの個別システムの統合化などがなされる見込みであるが、時期的には2006年以降と見られている。

アンチウイルスソフトウェアやVPN関連投資は、既に市場に浸透しており、堅調に伸びる（維持する）ことが予想されるが、今後はセキュリティ管理（administration）、認定（authorization）、認証（authentication）のソフトウェア分野が拡大すると見られる動きもある。この3つの機能はeビジネスやネットワークシステムを実現する上で、非常に重要で不可欠な機能と考えられているからである。顧客や取引企業との信頼関係を築く上でも欠かせないものであり、これらの個別製品、統合的なサービスが市場を牽引する1つの要因となるだろう。
図表 4.2 米国セキュリティ市場の予想推移

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>セキュリティ製品</td>
<td>4,500</td>
<td>5,250</td>
<td>6,625</td>
<td>8,250</td>
<td>10,100</td>
<td>12,000</td>
</tr>
<tr>
<td>前年比</td>
<td>-116.67%</td>
<td>126.19%</td>
<td>124.53%</td>
<td>122.42%</td>
<td>118.81%</td>
<td></td>
</tr>
<tr>
<td>セキュリティサービス全般</td>
<td>4,700</td>
<td>5,050</td>
<td>5,775</td>
<td>6,850</td>
<td>8,100</td>
<td>9,200</td>
</tr>
<tr>
<td>前年比</td>
<td>-107.45%</td>
<td>114.36%</td>
<td>118.61%</td>
<td>118.25%</td>
<td>113.58%</td>
<td></td>
</tr>
</tbody>
</table>

注意：資料の定義の関係から書店は除いている
資料：各種米国調査会社の公表資料を元に推計
4.2.1 米国のセキュリティ製品市場

アンチウイルスソフトウェアは、前述の CSI のセキュリティ担当者へのアンケート調査によると約 90%の企業が既に導入している製品で浸透度の高い市場であると言える。企業での利用はクライアント型からサーバー型、ゲートウェイ型に移行しており、今後もその傾向は続くであろう。法人市場も個人市場も数社で市場のアンチウイルスソフトウェアのシェアを占めている。ウイルス被害は先述のアンケート調査結果でも 93%の企業が被害を受けており、今後も必要性は高い製品と言える。

セキュリティ管理分野では、ネットワーク侵入を検知する IDS の導入が進んでおり、IDS の総合的なソリューション提供をする企業が出てきた。

ファイアウォールは、ソフトウェアからハードウェアにその比重を移している。ということも、こういった特定の機能を持ち、負荷がかかるような機能をソフトウェアで導入するよりもハードウェアとして導入した方が処理能力も高いため、導入も容易なためである。今後も他の製品にこの傾向が続く可能性がある。2000 年に 11 億 6,000 万ドルであったこの市場でも 2005 年度には 29 億ドルに達するという予測もある。

暗号製品は VPN や PKI の要素技術製品として今後も需要が伸びることが予測される。また、無線 LAN などの無線ネットワーク環境が普及しており、そこに組み込まれる暗号製品の需要も伸びるであろう。

認証分野では、バイオメトリクスがセキュリティ強化のため政府関連に導入が進むと考えられる。企業ユーザにおいても、コストが下がればその利便性から広がる可能性がある。ただし、個人ユーザまで導入が進むかどうかは、対応アプリケーションがどれだけあるかに加えて、機器が持ち運びに便利なサイズ・重さかどうかや、価格にかかっていると言える。また、IC カードはクレジットカードなどへの導入が進み、普及が見込まれる。

4.2.2 米国のセキュリティサービス市場

セキュリティシステムの構築・導入が情報セキュリティ市場で一番大きな市場である。企業も総合的にセキュリティシステムの導入を望んでいることや専門家のサポートが必要なことからこの市場への予算を一番大きく取る傾向にある。本市場の市場予測は他のセキュリティ製品がどれだけ売れるか、必要とされるかにかかっている。

ネットワークサービスプロバイダによる VPN とセキュリティサービスへの支出は、米国では 2007 年に 9 億 3,100 万ドルにのぼると見られている。サービスプロバイダは VPN だけでなく、ファイアウォールや IDS、統合型セキュリティサービスなどを提供できるようにする動きもあり、サービスプロバイダ参入による市場への伸びが期待される。また、企業のシステムがネットワーク化され、セキュリティに対する意識が高まるにつれて、セキュリティの専門化によるセキュリティ監視サービスへの需要が高まると見ている。2001 年にセキュリティコンサルティングが活発に行われ、それにより必要なセキュリティサービスが増えてきた。そのため、セキュリティを一括で管理するサービスが求められるようになり、セキュ
リティ監視市場が数年後には情報セキュリティ市場の牽引サービスの 1 つになることが予測される。
セキュリティコンサルティング市場は、2001 年 9 月の同時多発テロ以降セキュリティへの意識が大きく変わったことから導入が進んでいる。2003 年中に正式なリスク評価手法が確立される可能性が高く、この評価手法をもとにした、セキュリティコンサルティングへの需要が高まることが予測される。

4.2.3 米国のセキュリティ関連サービス市場
米国のセキュリティ教育は、「高度セキュリティ担当者の育成」、「資格取得」、「ベンダー教育」などに分けることができる。日本同様、米国でも優秀なセキュリティ技術者の数は非常に少なく、人材需給バランスはかなり悪い状態にあり、教育・訓練が重要視されている。特に高度なセキュリティ知識・スキルを得る教育方法としてはセキュリティコンサルティング会社に委託する方法が効果的なものでないとされている。総合的かつ企業ニーズに合わせた教育が可能である。また、日本同様、情報システム監査コントロール協会などが行う資格試験を受講し、個別製品のベンダー教育によって、人材を育成する方法もあるが、資格取得や個別製品の利用方法がわかっただけでは情報セキュリティ教育が充分とは言えないケースもある。
セキュリティ保険は、「ネットワークリスク保険」として大手損害保険会社を中心に販売されている。内容としては資産・収益の保護や財務強要への対応、犯人特定につながる情報への報奨金の支払、企業イメージ修復のための費用まで含まれた商品である。保険内容や企業の規模によって金額は違うが 2,000 ドルから 100 万ドルまでの保険費用があり、企業のニーズに合わせた商品提供形態となっている。今後、大手損害保険会社では 2005 年までに 25 億ドル以上の伸びがあると見ている。この拡大要因の 1 つとして、通常の負債保険の更新時に「ハッキング関連の損失については対象外」という契約内容が盛り込まれるケースが出てきており、ハッキング関連のリスク対策には別途専門の保険契約が必要になるとの読みがある。一方で阻害要因として、ハッキングなどの情報セキュリティ分野の損失は多岐に渡っており、予期しない形の損害が出た場合、対象外になることもある。保険への有効性を疑問視する専門家もいる。
4.3 日米の情報セキュリティ市場の比較
4.3.1 セキュリティ分野シェア比較
日米のセキュリティ市場を「セキュリティ製品」「セキュリティサービス」の比率で比較する。以下に2001年度の数値をグラフ化して示す。

図表4.3 日米セキュリティ分野シェア比較

日本に比べて米国の方がセキュリティ製品の割合が高い。これは、全世界のセキュリティ製品のうち、米国に本社を持つ企業の製品が大きく輸出分も含まれていることが考えられる。また、日本はセキュリティシステム構築の分野においては、セキュリティシステムの作りこみなどが行われる傾向にあり、システムサービス比率が高くなっていることが推測される。アンチウイルスソフトウェアやファイアウォール・VPN機器など比較的市場の大きい製品は米国に強い企業がある。
4.3.2 セキュリティ分野金額比較

金額ベースで比較すると、セキュリティ製品、セキュリティサービスともに、米国市場の方が大きい。以下に、2001年、2006年の市場の比較をする。また、参考情報として、IT投資全体の比較をした図を掲載する。1USドル=120円で計算し、比較の都合上米国の数値には書籍が含まれていなかったため、日本市場からも書籍分は除いた。

図表4.4 日米セキュリティ分野別金額比較

資料：本報告書の推計値を用いて作成
2001年に情報セキュリティ市場の金額が3.76倍であったものが、2006年には日米の差が縮まり、2.48倍になると予測される。これは、セキュリティ製品が米国製のものが多く米国から投入されることや、一般にこういった情報セキュリティに対する意識は米国の方が高く（後述）、導入も先行して進めていることから、このような傾向になるものと考えられる。

また、日米IT投資額の比較をすると、米国は、日本の1.96倍のIT投資をしている。ITセキュリティ投資が米国は3.28倍の投資をしていることを考えると、日本ではまだ情報セキュリティ投資は米国ほど進んでいないことがここでもわかる。

図表4.5 日米IT投資額比較（2001年）
4.3.3 セキュリティ製品・サービスの導入の状況比較
以下に、日米間においてセキュリティ製品の導入状況を比較した図を掲載する。

図表 4.6 日米セキュリティ製品導入比較

アンチウイルスソフトウェアは、日本でも普及が高く、アンケート調査結果では同程度の数値を示している。ファイアウォールも日米とも高い導入率で大きな差はない。不正侵入検知や暗号化などの比較的新しい製品については日米の差は大きく日本では導入が進んでいない。これらの日本で導入が進んでいない製品については、米国並に導入が進む可能性がある。
5. 情報セキュリティビジネスの成功と失敗

情報セキュリティビジネスの各分野に対して、その成功/失敗の要因の考察を行う。ビジネスとしての成功は、その分野での主要企業が、当該ビジネスの売上を伸ばしており、あるいは共ビジネスへの参入企業が増加し市場規模が拡大している状況を示している場合と見なした。一方、どの企業も売上を大きく伸ばすことなく参入企業の撤退が続いており、市場規模が低迷または縮小している状況を、ビジネスの失敗と見なした。

以下では、情報セキュリティに関する業務を行う企業へのヒアリング調査の結果と、各種公開資料情報に基づき考察を行った。成功要因と考えられるもののについては（）を、失敗要因と考えられるものを[]の記号で示している。

5.1 各ビジネス分野における成功/失敗要因

5.1.1 セキュリティ製品

(1) アンチウイルスソフトウェア

キライアント型

- インターネットの利用
- デファクトプラットフォームへの適用
- ハードウェアへのバンドルによる普及
- 確立された製品ブランドの利用

サーバー型・ゲートウェイ型

- マーケット専門化
- 技術者の派遣などのきめ細かなサービス
- 多様なプラットフォームへの対応

- ウイルス数の増加に対応できない（資金、人材、技術）
- ビジネスモデルが未確立
- ウイルス発生頻度に依存

a) クライアント型

アンチウイルスソフトウェアは、近年のウイルス被害等の事件を背景に、特にコンシューガマ向けを中心に製品出荷数は増加傾向にある。このようななか、以前は相当数あったクライアント型アンチウイルスソフトウェアは、大手数社の海外製品によってほぼ寡占状態となってきた。大手企業では、インターネットによるウイルス関連情報の提供や、新種のウイルスへ対応するためのウイルスペターンデータをインターネットで自動配布・更新することによって、ユーザの利便性を向上させシェアを伸ばしている。また、多くが Windows プラットフォームを対象としていることから、企業および個人における Windows の普及・定着と機
を一にして、売上を増加していった点もあげられる。このような企業には、パソコン本体に<br>バンドルする形態で、シェア確保に成功している企業がある。一方で、Macintoshのような<br>特定プラットフォームで築いたソフトウェア製品のブランド力を背景に、同プラットフォー<br>ムでのシェアの維持に成功している企業もある。

国内の専門企業は、ウイルスの発爆的増加にともない、ウイルス定義ファイルの更新管理<br>のための、資金、人材、技術等が不足することが多く、廃業に追い込まれ、技術者とともに<br>他メカに吸収されるなど厳しい状況にある。また、ウイルスパターーンデータのメインテナ<br>ンス費用はソフトウェア販売費用から捻出する必要があるが、そのビジネスモデルが確立で<br>きずに失敗した事例があると考えられる。

市場シェアの低いプラットフォームにおいては、ウイルスの発生が少なく、そのプラット<br>フォームに対するアンチウイルスソフトウェアの市場は、全体として大きくなっていない。

ｂ) サーバー型・ゲートウェイ型
サーバー型ソフトウェアやゲートウェイ型ソフトウェアは、法人向けが中心で、クラウド<br>型ソフトウェアベンダーとは異なるベンダーも一定の売上を確保している。クラウド型<br>ではコンシューマ向けの製品出荷数が急激に増加しており、それに呼応して相対的に対<br>顧客サービスが低下するケースがある。これに対して、一定のビジネスが成立しているベン<br>ダーは、法人マーケットに特化することで、きめ細かな対応を可能にして、成功しているケースもある。顧客側にトラブルや不都合が発生した場合の技術者派遣や、顧客に合わせてア<br>ドオンソフトウェアを開発することなどが事例としてあげられる。

また、法人では社内に複数のプラットフォームを保有する場合があり、コンシューマ向け<br>とは異なり、ソフトウェアが多様なプラットフォーム（Windows、UNIX 系各種 OS、<br>Macintosh ほか）に対応していることが成功要因となっている場合がある。

(2) セキュリティ運用ソフトウェア

■外部環境（事件の発生）

検査ツールやログ解析ツールなど、この分野のソフトウェアは運用上必要になる場合が多<br>く、ISP などの専門業者が利用の中心と考えられる。企業での導入率は、多いものでも 26%<br>と他分野の製品に比べ低く、今後拡大の余地は大きい。これまではネットワークインフラの<br>整備につれ、不正侵入などの被害が増加していることや、内部管理の観点から拡大してきて<br>ている分野である。最近では、情報漏洩による信用失墜や損害賠償額の大きさなどが認識され、<br>フィルタリングツールの導入も進みつつある。一方で、情報セキュリティ対策を怠ることに<br>よるリスクの大きさが過小評価されているため売上が伸びない、との意見も聞かれる。

また、従来は個別のコンサルティングで相当の費用が必要であった情報セキュリティポリ<br>シー策定を、作成支援するソフトウェアを開発し、売上を伸ばしている事例もある。このよ
うなソフトウェア製品は、コンサルティング会社だけでなく、一般事業者にも売れており、情報セキュリティマネジメントの適用拡大の動きとも合致している。
主に、海外製品とのアライアンスが成功要因と見なされるが、アクセス制御などの運用管理ソフトウェアでは、国内メーカーの独自開発製品においても一定の成功例が見られる。

(3) ファイアウォール・VPN

- 高価なハードウェアとソフトウェアの組み合わせからアプライアンス製品への移行
- 外部環境

ファイアウォールについては、これまでの高価なハードウェアにファイアウォールソフトウェアを搭載する形態から、専用のアプライアンス製品へと移行しつつある。ファイアウォールソフトウェアは、海外製品が主流であったが、ハードウェア技術を得意とする国内メーカーでは、アプライアンス製品化により一定のシェアを取り戻しつつある。また、ISPなどのサービス提供業者の利用や、モバイル環境の進展による需要拡大が期待される分野である。
ブロードバンド化に伴うインターネットVPNの拡大でVPN製品の売上が増加している。

(4) 認証関連製品

バイオメトリクス
- 研究レベルの段階からの取り組みによる高シェア
PKI
- アプリケーションの不足
- 実用的ではないソリューション
- 認知度の不足
- ビジネスモデルの欠陥
その他
- 周辺分野メーカー等の参入

バイオメトリクス認証は、これまで入退室管理などでの利用に限られ、アプリケーションが十分ないことや識別能力の点での不満から、普及は遅れていた。指紋認証など特定分野で70%以上の世界シェアを有する企業があるなど、国内メーカーが強い分野である。ただし、予想される市場規模からみると、海外への展開はまだあまり進んでいない。
米国では、2001年の同時多発テロ事件以降、認証システムの導入が進んでいる。銀行やスーパーマーケットなどでの本人確認用として指紋認証が普及しつつあり、このようなアプリケーションの増加とともに、ハードウェアの小型化、性能向上による需要拡大が予想される
る。さらに、携帯電話への搭載が開始されるなどの動きもあり、これが本格化すれば、国内だけでなく年間数千万台規模の急速な需要拡大が期待できるとともに、競合の増加、価格競争の激化が予想される。

PKI は、数年前から 2 年後には需要が爆発するとの見通しが毎年繰り返し出されてきた。しかし、これまでは大きな動きがなく、見通しは当たっていない。この背景には、アプリケーションやサービスの不足がある。またパソコン、OS、携帯電話などすべての端末やアプリケーションに PKIが実装されると見込んで、ベンダーは積極的にプロモーションを実施してきたが、ユーザ運用の手間や、勤務先・自宅・携帯端末などひとが複数の端末をもつ状況ではマッチせず、手間とコストのかかるソリューションになっていることも失敗の一因である。

今後、e-Japan 戦略の推進により、市場の立ち上がりが期待される一方、相互認証に関すること細かな運用での不都合など指摘される問題点も多い。認証用の検の取得申請時のみ課金し、署名の確認では課金しないビジネスモデルに問題がある、との指摘もある。

このほかの分野では、時刻認証におけるタイムスタンプ関連メーカ、データの原本性確保における印刷関連メーカなど周辺領域の企業からの参入も増え、競争状態が発生しつつある。

(5) 暗号関連製品

● デファクト対応の遅れ

暗号関連製品は従来ソフトウェア製品が中心であったが、最近は携帯電話や IC カード等への搭載に見られるように、ハードウェア製品に比重が移りつつある。従来から、ブランド力およびデファクト化の進展で海外製品が主流となっている市場である。海外メーカの日本法人、およびこれらとアライアンスを組んだ企業が売上を確保している状況と考えられる。

日米欧にて、暗号アルゴリズムの更改が企図されており、国内メーカも標準方式への採用候補になるなど、技術的優位性はある。国家戦略にも関連する問題であり、単に技術面だけでは成功は難しいと考えられる。国内メーカは、著作権保護などのための電子証明技術や需要拡大が見込まれる無線 LAN 通信への適用など民生機器や産業分野への応用、あるいは GPKI などの国内制度への対応によって、市場拡大を図る進め方を取らざるを得ないので考えられる。
5.1.2 セキュリティサービス

(1) セキュリティシステム構築サービス

- デファクト製品とのアライアンス
- 企業システム形態の内外差異

セキュリティシステムの設計・構築においては、その要素としてセキュリティ製品を利用する場合が多く、セキュリティ製品分野の拡大とともに増加している分野である。また、セキュリティシステム構築後も、定期的あるいは不定期のメンテナンスが必要となること、製品の陳腐化やリース切れ、システム機能の陳腐化等を要因とするシステム改変需要もあることから、一定規模の市場が確保されるものと考えられる。

システム構築企業には、デファクト製品とのアライアンスをもつ場合が多く、システム製品ビジネスの拡大をうまく連携し成功している。

一方で、海外では金融機関などを中心に全社に対して認証システムを構築するなどの事例が見られるものの、国内では金融分野における基幹業務システムは社内で閉じたシステムが多く、内部管理セキュリティに関しては投資が行われるが、外部も含めた大規模な認証システム構築のニーズがないなど、内外の企業環境の違いも大きい。

(2) セキュリティ管理サービス

- 競争の激化

セキュリティ検査・監視サービス、フィルタリングサービス等、セキュリティ管理サービスについては、ISPや通信会社が付加サービスとして提供するなど既存ビジネスの優位性を利用した取り組みを行っている事例がある。また、クライアント端末の管理サービスなどもあり、ネットワークの上流・下流で同様のサービスが競合している。

一方で、ソフトウェアベンダー等が製品販売とともに取り組むケースや、セキュリティ関連コンサルティング会社、さらに警備保障会社など他業態も参入し、トータルサービスを提供するといったケースも見られ、競争は激化している。

(3) セキュリティ・コンサルティング・サービス

- 分野の特化による技術優位の獲得

システム開発などからこの分野に特化し、情報提供やコンサルティングサービスの提供な
どの特にネットワーク分野でのサービスによって成功している事例がある。このような企業では、直接の受託だけでなく、次項のセキュリティ保険サービスにおける技術評価や、SIでの技術指導などアライアンス先からの受託も一定の割合を占める。

従来は情報セキュリティポリシー策定コンサルティングが中心であったが、ISMS適合性評価制度の開始など、情報セキュリティ管理のニーズの高まりとともに参入企業が増え、価格競争に陥りつつあり、厳しい状況の企業もある。一方で情報セキュリティポリシー策定を手がかりに、これに引き続きセキュリティシステム構築サービスを受託し、成功している事例もある。

セキュリティ監査は地方公共団体等において実施する動きはあるものの、未だ一般化するには至っていない。

5.1.3 セキュリティ関連サービス

(1) セキュリティ保険サービス

・ 商品が成熟していない

セキュリティ保険サービスは、通常の保険と商品内容が異なるため、営業担当者に専門知識が要求されること、また顧客の側でもサービス内容がうまく理解されない場合があることから、販売拡大の阻害要因になっている。セキュリティ保険は以前から販売されているものの、査定によっては保険引き受けを拒否できる唯一の商品になっている等、まだ一般的な商品にはなっていない。これは、セキュリティリスクを構成する要素が適切に分割できておりず、リスク算定が難しくなっていることなどが原因と考えられる。

(2) セキュリティ関連教育

・ 参加障壁やブランド、得意分野など

教育分野は情報セキュリティ技術者の不足感から、一定の市場成長が見込まれる分野である。しかし、講師や会場の確保など容量に制約のある部分があり、ノウハウが必要であることから新規参入は少ない。老舗のブランド力や、情報処理教育などを得意とする企業が市場成長分の果実を得ていると考えられる。

技術者だけでなく、利用者や管理者への教育、啓蒙も重要なテーマであり、今後の成長が期待できる。

(3) セキュリティ関連書籍出版
情報セキュリティのテーマと読者層との組み込みの難しさ

セキュリティ関連技術書、資格対策書籍などは通常の技術書等と同じく一定の割合を確保しており、技術書を扱う出版社が優位になっている。雑誌は、IT関連雑誌での特集や別冊、ムックの形式で出版されている程度であり、情報セキュリティ専門の雑誌が多数発行・出版されたことはない。情報セキュリティをテーマとする場合、どうしてもITの枠を超え、リスク管理などの話題にまで拡がるが、その場合に読者層を絞りにくい。一方で、ITのみをテーマとすると、情報セキュリティの話題は、情報セキュリティポリシー等に終始してしまい、限定的になり過ぎる。こうしたことが発行部数の多い雑誌が出ていない理由といわれている。

5.2 ビジネス分野共通の要因

上記の複数の分野、例えば、セキュリティシステムの設計・構築から運用・サービス提供までといったトータルなサービスメニューを揃えることで成功している事例がある。また、複数の事業部門ごとの情報セキュリティ関連製品・サービスを提供している企業で、事業部門を横断する組織を設けるなどして情報共有を進めると、あるいはワンストップサービス体制を構築する等の工夫で成果をあげているケースもある。

このほか、情報セキュリティ製品・サービスを本業としない企業において、取り扱い製品に対して情報セキュリティ機能を付加することによって他社との差別化を実現し成功している事例がある。
6. 情報セキュリティビジネスにおける課題

前章までの情報セキュリティビジネスの市場動向、成功・失敗要因の分析結果から、情報セキュリティビジネスにおける課題を抽出する。これまで分類として利用してきた情報セキュリティビジネスの各分野において、拡大要因を伸張させ成功要因に寄与する、あるいは阻害要因を除去し失敗要因を減ずるよう対応をすることが基本となる。

6.1 技術面の課題
(1) 新しい分野・新たな技術の開発への支援
情報セキュリティビジネスは、今後5年間で3.5倍になると予想されるが、未だ黎明期にあるビジネス分野である。このような成長の速度でビジネスは、試行錯誤や競合の発生など厳しい環境にさらされやすい上、海外のデファクト製品やグローバルにブランド力のある企業に対抗するのは容易ではない。
既にデファクト製品などを基盤とした情報セキュリティビジネスは確固たる位置を占めており、今後の成長要因は、新しい分野や新技術に向けられると考えられる。これらの要素に対して、国内産業を育成する施策が求められる。

(2) 国内の特殊環境
海外諸国と比較し、日本はモバイルネットワークやブロードバンドの普及率は高い。携帯電話などをはじめとする、この分野の周辺における先行技術開発の育成が望まれる。

(3) デファクト標準におけるポジション
情報セキュリティビジネスにおいては、デファクト標準は海外製品・企業に握られており、国内ベンダーが指導力発揮できない要因のひとつになっている。すでに確立した技術についてはデファクト標準に従うことのはやむを得ない点もあるが、新しい技術についてはデファクト標準を獲得できるような、各ベンダーの体制・施策が望まれる。

6.2 人材面の課題
(1) 情報セキュリティ専門人材の育成
情報セキュリティ技術者は今後の市場拡大に見合う規模とはなっていないと想定され、育成が必要である。メカなどにおいては、個社の努力で育成している状況であるが、今後の市場の伸びには追いつかない可能性もあると考えられる。
現在、情報処理技術者試験では、情報セキュリティアドミニストレータ試験が区分として設けられており、受験者数も多い区分となっている。また、経済産業省にて策定された ITスキル標準（ITSS）においても、ITスペシャリスト職種の専門分野としてセキュリティが設けられており、人材の充実が期待できる。しかし、資格の取得とスキルとは必ずしも合致するものではない点に留意が必要であるとともに、資格の継続審査のようなフォローの仕組みが必要であると考えられる。
(2) ユーザ企業での認知度の向上
一方、ユーザ側についても、情報セキュリティの専門家が必要とされている。現在は、情報セキュリティポリシー教育などが実施されている程度であり、ユーザ向け要員への教育の必要性も高い。
また、経営者や管理者に対する情報セキュリティに関する啓蒙も継続的に行っていく必要がある。

6.3 制度面の課題
(1) 制度の認知度の向上
最近では、情報漏洩事件による被害、社会的信用の失墜、高額な損害賠償などの点から、ISMS 構築の取り組みが広がるなど、情報セキュリティに関する認知度は向上している。しかし、これらは一般に感度の高いユーザの動きとも考えられ、セキュリティ保険の調査では情報セキュリティに対する影響の認識が甘いため市場が拡大していないとの意見も出ている。ウィルスについての情報などは一般的に報道されるようになってきており、これ以外の情報セキュリティに関する情報も同様に広く周知されるようになることが望まれる。

(2) 国際標準の整備
情報セキュリティに関する標準は、近年、IT セキュリティ評価・認証制度や ISMS 適合性評価制度など整備されてきている。ISMS 適合性評価制度では認証申請件数が 100 件を超えるなど活発化しており、認証基準の ISO 化が待たれる一方で、英国の同様の認証制度である BS7799 による認証もすすめられており、複雑な状況になっている。また、ISMS のポイントである情報セキュリティシステムの運用と一体をなすともいえる IT セキュリティ評価・認証制度では、認定された製品数が少ないなど課題も多い。これらも含めて、情報セキュリティに関する標準については整備が望まれる。

(3) e-Japan 戦略の推進
企業間の取引条件や、公共機関・地方公共団体等への入札条件に対し、情報セキュリティに関する要件を組み込むことは、ISMS 構築や情報セキュリティ対策、情報セキュリティ監査などの情報セキュリティビジネスにとって追い風になる。
また、電子政府が本格的に稼動すれば、地方公共団体を経由して民間企業までをも巻き込み、電子認証ビジネス市場が拡大することが予想される。この際に、法務局における商業登記に関する認証と民間認証局などとの相互認証に不整合があると報告されている。市場育成には政府の整合の取れた取り組みへの見直しが重要であると考えられる。

(4) リスク定量化手法の確立
情報セキュリティリスクを定量化して、把握・管理したいとの声がある。保険会社でも一定のリスク評価手法が確立しているわけではなく、保険会社間で相互に利用できる情報はなっていない。IT セキュリティ評価・認証制度には認証レベルが設定されているが、これはリスク発生防止の強度を示すものではないため、製品・サービス購入時の基準となって
いない。利用者のとまどいにもつながっている。

このような点から、同制度の認証レベルとは異なり、リスクを定量化できる手法の確立が望まれる。定量化された値は固定的である必要はなく、セキュリティシステムやセキュリティ製品に新たなセキュリティホールが発見されれば数値はさがり、あるいはセキュリティパッチが適用されれば数値があがるような仕組みがむしろ実際的である。これは、いわゆる企業の格付の考え方に近い。情報システムで利用されるセキュリティ製品やサービスは、株式売買のように機動的に交換できるわけではないが、購入時の参考にでき、あるいは製品に対するベンダーの取り組み姿勢を示す指標にもなり得る。これにより、情報セキュリティに関する最新情報を注視していないユーザに対しても一定の有益な情報を与えることが可能である。またメーカにとっても、製品やサービスに対して情報セキュリティ対策に取り組む動機になるとも考えられる。

企業のWebサイトに関して、クロスサイトスクリプティングの調査や、セキュリティインシデントに対する企業のレスポンスを調査している市民グループがあるが、そのようなグループの活動を支援することにより導入するような形態、あるいは中立的機関により実施する形態などが考えられる。
（サブテーマB）

ITセキュリティ評価・認証制度に関する市場予測
1. 調査の概要

1.1 調査の背景
情報処理振興事業協会セキュリティセンターにおいては、2001年2月に「ITセキュリティ評価認証制度に関する市場予測調査概要報告書」を公開した。
これ以降、ITセキュリティ関連の評価・認証の制度が整備されてきたが、ITセキュリティ評価認証ビジネスの立ち上がりは、遅れている状況にあると考えられる。しかし、情報セキュリティビジネスに関する環境変化により、ITセキュリティ評価認証ビジネスにおいて市場の変化が推測され、今後の制度の効率的実施のため、現状を正確に把握しておく必要があった。

1.2 調査の目的
情報セキュリティ政策立案支援及びITセキュリティ評価・認証制度の効率的実施のために現状を正確に把握しておく必要があり、そのための基礎データの収集を行う。ITセキュリティ評価・認証制度に関する市場に対し詳細な調査を実施し、今後5年間の市場予測するとともに、今後の普及に向けた制度に対する課題を明らかにする。

1.3 調査方法の概略

ヒアリング調査・アンケート調査

○セキュリティ評価認証制度に関する事業動向調査

○セキュリティ評価認証制度に関する市場予測

○セキュリティ評価認証制度に関する分析と課題の検討

ヒアリング調査：
中央省庁、国立機関、地方公共団体、民間企業を含む、21組織に対しヒアリング調査を実施。
また、ISO審査機関および審査員、ISMS審査機関および審査員に対して、他制度における審査状況、制度の経緯や課題に関しヒアリング調査を実施。

アンケート調査：
Webによるアンケート調査を実施。有効回答数は、公的機関・企業を含め、275件。
2. セキュリティ評価・認証制度に関する分析と課題

2001年4月に、経済産業省の委託を受けた独立行政法人製品評価技術基盤機構（NITE）が認証機関となって、セキュリティ評価・認証体制が創設され、セキュリティ評価・認証制度が正式にスタートした。

本制度は、1998年10月より欧米諸国ですでに実施されていたCC（Common Criteria）に基づく、情報システム並びにそれを構成するソフト、ハード製品のセキュリティ評価・認証に関する相互承認の動きに対応するため、情報処理振興事業協会（IPA）セキュリティセンターが設立を推進したものである。

しかし、設立から2年経過時点でセキュリティ評価・認証された製品は数件にとどまり、制度として普及しているとは言いがたい状況にある。

本章においては、今後、本制度普及のための施策検討に役立つ基礎資料となるよう、制度普及の阻害要因を抽出し、阻害要因を取り除くための施策の提言並びに制度の利用予測について言及する。
2.1 セキュリティ評価・認証制度の国際動向

日本のセキュリティ評価・認証制度の設立の契機となった世界におけるセキュリティ評価・認証制度の動向について簡単に触れる。

2.1.1 海外におけるセキュリティ評価・認証制度

セキュリティ評価制度は、十数年程前から欧米諸国で、情報システムやそこで取扱う製品を対象に、セキュリティ機能を評価する制度として運用されている。

まず、米国では、1985 年に軍事システム向けに製品調達する際の情報システムや製品について、セキュリティ評価規準並びに同規準を運用するための制度を発足させた。このセキュリティ評価基準は TCSEC（Trusted Computer System Evaluation Criteria）と呼ばれている。TCSEC では、信頼レベルの低さ順から、D、C1、C2、B1、B2、B3、A1 の 7 つのクラスに分類し、クラス毎にセキュリティ機能と品質が満たすべき要件を定めている。

一方、ヨーロッパでは 1991 年の EC 市場統合の動きに合わせ、それまで各国個別に運用してきたセキュリティ基準の統一を図った。このセキュリティ基準を ITSEC（Information Technology Security Evaluation Criteria）と呼んでいる。ITSEC においては、機能要件は、識別と認証、アクセス管理、追跡性、監査、オプジェクトの再利用、完全性、サービスの信頼性、データ交換の 8 種類が定められている。また保証要件としてはセキュリティ機構の有効性と正確性を基に 7 レベルが設定された。

各国のセキュリティ評価基準を国際的に統一することを目指し、1993 年に米国、カナダ、英国、フランス、ドイツ、オランダの 6 カ国が集まりプロジェクトをスタートさせた（CC プロジェクト）。このプロジェクトにおいて 1996 年に作成されたセキュリティ評価基準が CC（Common Criteria）と呼ばれ、そのバージョン 1.0 版が 1996 年に発行された。

この後 ISO 化の方向に進み、1999 年 6 月に ISO/IEC 15408 として正式に規格化される。

图表 2.1セキュリティ評価基準作成の変遷
なお、これまで TCSEC、ITSEC、ISO/IEC 15408 の各評価基準で評価された主な評価済み製品の件数を、下記図表 2.2に示す。

<table>
<thead>
<tr>
<th>年</th>
<th>TCSEC</th>
<th>ITSEC</th>
<th>CC (ISO/IEC 15408)</th>
<th>合計（年）</th>
</tr>
</thead>
<tbody>
<tr>
<td>1990以前</td>
<td>20</td>
<td>1</td>
<td></td>
<td>21</td>
</tr>
<tr>
<td>91</td>
<td>4</td>
<td>0</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>92</td>
<td>6</td>
<td>1</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>93</td>
<td>5</td>
<td>7</td>
<td></td>
<td>12</td>
</tr>
<tr>
<td>94</td>
<td>19</td>
<td>25</td>
<td></td>
<td>44</td>
</tr>
<tr>
<td>95</td>
<td>11</td>
<td>17</td>
<td></td>
<td>28</td>
</tr>
<tr>
<td>96</td>
<td>4</td>
<td>18</td>
<td></td>
<td>22</td>
</tr>
<tr>
<td>97</td>
<td>7</td>
<td>28</td>
<td>1</td>
<td>36</td>
</tr>
<tr>
<td>98</td>
<td>5</td>
<td>32</td>
<td>3</td>
<td>40</td>
</tr>
<tr>
<td>99</td>
<td>2</td>
<td>41</td>
<td>14</td>
<td>57</td>
</tr>
<tr>
<td>2000</td>
<td>3</td>
<td>31</td>
<td>31</td>
<td>65</td>
</tr>
<tr>
<td>01</td>
<td>0</td>
<td>34</td>
<td>26</td>
<td>60</td>
</tr>
<tr>
<td>02</td>
<td>0</td>
<td>17</td>
<td>44</td>
<td>61</td>
</tr>
<tr>
<td>評価中</td>
<td>0</td>
<td>9</td>
<td>68</td>
<td>77</td>
</tr>
<tr>
<td>合計</td>
<td>86</td>
<td>261</td>
<td>187</td>
<td>534</td>
</tr>
</tbody>
</table>

資料：情報処理振興事業協会セキュリティセンター (IPANSEC) 「IT セキュリティ評価及び認証セミナー資料」 (2002 年 12月)

2.2 日本におけるセキュリティ評価・認証制度設立の経緯
1998年10月に前記 CC プロジェクトにおいて、CC に基づいたセキュリティ評価・認証の相互承認に関する協定書 (MRA) が作成・公開された。同時にプロジェクト参加国中、すでにセキュリティ評価に関する制度が運用されているカナダ、フランス、ドイツ、英国、米国がこの MRA に調印し、これから 5カ国間で国際的な相互承認アレンジメントの枠組みがスタートした。これにより、加盟国間では、CC (EAL 1→EAL 4 まで) に基づいて評価・認証をされた情報システムやそこで取扱う製品は、相互に通用するようになる。現在の加盟国としては、前記の 5カ国に加え、オーストラリア、ニュージーランド、フィンランド、ギリシャ、イタリア、オランダ、ノルウェー、スペイン、イスラエル、オーストリア、スウェーデンが参加している。
一方、我が国においては、情報システムやそこで取扱う製品のセキュリティ機能、品質をチェックする制度がなかったため、電子政府構築に伴う、国の情報システムやそれを取扱う製品等へのセキュリティ機能、品質のチェック体制の整備が望まれると共に、日本の情報システムやそれを取扱う製品の国際競争力確保の観点から、このセキュリティ評価に関する国際的な枠組みに参加すべく、本セキュリティ評価・認証制度を設立し、普及を推進している。
特に政府調達では、情報システムやそこで取扱う製品に関して、可能な限り本セキュリティ評価・認証制度によって認証されものを選択することが、2001年の行政情報化推進各省庁連絡会議了承事項として政府方針となっている。

2.3 ISO/IEC 15408 とは

本セキュリティ評価・認証制度では、国際標準であるISO/IEC 15408に基づき、情報システムや製品のセキュリティレベルを評価しているので、以下にISO/IEC 15408について簡単に触れておく。

ISO/IEC 15408は、従来からあるCCのバージョン2.0が1999年6月に規格化され、次の3つのパートで構成されている。

- パート1: Introduction and general model (概説と一般モデル)
- パート2: Security functional requirements (セキュリティ機能要件)
- パート3: Security assurance requirements (セキュリティ保証要件)

ISO/IEC 15408の考え方を要約すると、情報システムやそこで取扱う製品の設計・開発において、適切なセキュリティ機能を設けるため、保護対象の抽出から脅威分析、リスク分析、セキュリティ機能要件の設定というプロセスを踏むよう求めている。その過程において、パート1で定められている「Protection Profile (PP)」(セキュリティ要求仕様書)と「Security Target (ST)」(セキュリティ基本設計書)の策定が必要となる。STやPPには、次の事項が盛り込まれている必要がある。

- 想定する利用条件と脅威
- 脅威に対するセキュリティ方針
- セキュリティ方針を具体化するための機能要件（パート2で規定）
- 具体的なセキュリティ基本仕様
- 保証レベル（パート3で規定）
- 想定した脅威に対するセキュリティ方針、機能要件及び基本仕様が妥当かつ有効であることの認証

STは、情報システムやそこで取扱う製品の選定において、どのようなセキュリティ機能が備わっており、どのような脅威からどの程度保護するかを判断する目安となる。一方PPは、情報システムやそこで取扱う製品の種別ごとに、考慮すべき脅威やセキュリティ対策を示すものとなる。STが具体的な個別製品を対象とするのに対し、PPはある程度の汎用性を有するものとなる。従って、PPがテンプレートであり、STはそのテンプレートを具体的な製品開発に提供した基本設計書と捉えることができる。

実際にSTやPPを策定する為には、パート2に示される機能要件を満たすことが必要となっている。そこで個別の機能要件について簡単に説明する。
セキュリティ監査（監査ログの記録・分析に関する要件）
通信（データ通信における否認に関する要件）
暗号支援（暗号鍵の管理やデータ暗号・複合化、電子署名等の要件）
使用者データの保護（データへのアクセス制御や通信上での機密保持等に関する要件）
識別及び認証（ユーザの識別及び本人確認に関する件）
セキュリティ管理（セキュリティ属性やセキュリティ機能に関する要件）
プライバシ（個人情報の保護に関する要件）
評価対象のセキュリティ機能保護（セキュリティ機能を提供する機構の保護に関する要件）
資源利用（耐障害性や資源割当等に関する要件）
評価対象へのアクセス（ユーザと評価対象製品との間のセッション制御に関する要件）
高信頼パス／チャネル（ユーザと評価対象製品との間の安全な通信路に関する要件）

また、パート 3 の保証要件は、10 の保証クラスが定義されており、情報システムや個別
の製品のセキュリティ機能が実現されていることの保証を求めるものである。

・PP の評価
・ST の評価
構成管理の評価
配布及び運用の評価
開発の評価
手引き書の評価
ライフサイクルサポートの評価
試験の評価
脆弱性評定の評価
保証維持の評価

なお、我が国においては ISO/IEC 15408 を 2000 年 7 月に JIS X 5070 として JIS 化して
いる。
一方、ISO/IEC 15408 を実際に運用するためのセキュリティ評価・認証制度とは、一般に
次のような仕組みを構築する（図表 2.3）。
図表 2.3 セキュリティ評価・認証制度の一般例

参考資料：情報処理振興事業協会「セキュリティ評価・認証」パンフレット

・申請者が、情報システムや製品の認証のための評価を評価機関に依頼し、認証申請を認証機関に行う。
・評価機関は申請者から依頼のあった情報システムや製品の TOE 評価（Target of Evaluation）や PP 評価を実施し、その評価結果を認証機関及び申請者に報告する。
・認証機関は評価の技術指導や監督を行い、評価機関から受けた評価結果に基づき、認証を行う。

なお認証のための評価を行う評価機関は、あらかじめ認定機関による認定と認証機関による承認を受けておく必要がある。

欧米など、既にセキュリティ評価・認証体制を保持している国では、図表 2.3のような仕組みで運用を行っている。

2.4 我が国のセキュリティ評価・認証体制

本セキュリティ評価・認証制度は、ISO/IEC 15408に基づき、情報システムやそれを構成する情報機器、ソフトウェアのセキュリティ機能全般及び目標とするセキュリティレベルを評価し、その結果を公的に検証し、公開するもので、経済産業省の委託を受けて、独立行政法人製品評価技術基盤機構（NITE）を中心に、下記の図表 1-4の体制にて運用されている。

まず、独立行政法人製品評価技術基盤機構（NITE）は、制度全体の維持並びに評価機関の審査、認定、監督、評価機関が評価した結果の認証を行う。

次に調査機関は、独立行政法人製品評価技術基盤機構（NITE）からの調査依頼を受けて、情報システムや製品等の認証のための調査を実施する。

評価機関は、申請者（メーカーやベンダー）から依頼のあった情報システムや製品の評価を行い、その結果を独立行政法人製品評価技術基盤機構（NITE）に報告する。

申請者は、TOE 又は PP の評価、認証及び ST 確認、認証を要請する個人、又は組織で、評価対象の情報システムや製品の提供を行う。
開発者は、申請者が TOE 又は PP の作成者でない場合、申請者の協力要請に基づき、申請者の評価、認証作業をサポートする。

現在、PP（Protection Profile）及び TOE 認証のための評価ができる評価機関は 2 機関、ST（Security Target）確認のための評価ができる評価実施機関は 7 機関（2003 年 2 月時点での NITE ホームページ参照）が存在する。そして評価の種類は、PP 認証、TOE 認証及び ST 確認である。このうち ST 確認は日本独自の評価の種類である。この ST 確認は認証済み製品がほとんどない状況で最初から TOE 評価・認証済み製品を調達条件とした場合、事実上入札ができない場合がでてくる。したがって本制度を早期に普及させていくためにも制度を利用・導入させることを優先させ、TOE 評価に比べて評価が簡易な ST 確認という評価種類を設け、それによる製品調達条件が認められた。

これまでの認証実績は、TOE 評価・認証が 2 件、ST 確認が 3 件となっている（NITE ホームページ。2003 年 2 月現在）。

図表 2.4 セキュリティ評価・認証体制

資料：独立行政法人製品評価技術基盤機構「IT セキュリティ評価及び認証制度」をもとに作成
2.5 調査の実施

2.5.1 調査目的
本調査は、2章で記載したとおり、セキュリティ評価・認証制度の普及を妨げている阻害要因を抽出し、解決策の提言並びに同制度の将来的な利用予測について言及する。

2.5.2 調査方法
文献調査、ヒアリング、及びアンケートによる調査。

2.5.3 調査項目
(1) ヒアリング調査の項目
- セキュリティ評価・認証制度利用時の立場（評価機関、調達者、メーカやベンダー）
- セキュリティ評価・認証制度を利用した製品の種類
- 評価を受けた対象（PP、ST、TOE）
- 上記対象の作成に携わった技術者数並びにキャリア（人数、入社年次、専門分野、職位など）
- 上記評価対象の作成にかかった時間と費用
- 作成上苦労した事柄
- セキュリティ評価・認証制度に対する所感
- 率先して利用すべきか否か
- 上記質問に対する理由
- 利用するとした場合の動機付けは何か
- その他

(2) アンケート調査項目
- IT セキュリティ評価・認証制度の認知状況
- IT セキュリティ評価・認証制度を利用した製品の利用状況及び製品種類
- 評価を受けた対象（PP、ST、TOE）
- IT セキュリティ評価・認証制度を利用していない理由
- セキュリティ対策における IT セキュリティ評価・認証制度の位置づけ
- セキュリティ製品・サービスの調達・購入における IT セキュリティ評価・認証制度に関する意識
- IT セキュリティ評価・認証を受けた製品・サービスに求める認証水準
- IT セキュリティ評価・認証を受けた製品・サービスの価格に関する割高の上限
- 他の認証制度の取得状況
- その認証を取得された理由
2.5.4 調査結果

(1) ヒアリング調査要約

毎業界 A

立場 : 調達者
製品 / 機能 : IC カード
評価対象 : Protection Profile (PP)
技術者 / キャリア等 : 業者委託のため不明
時間 / 費用 : PP2 本で約 2 ヶ月、数千万円
普及における問題点 : 1）PP、ST を作成できる、或いは評価できる技術者不足（評価機関、調達者、メーカやベンダー共々）
                       2）通常の製品開発より余分な時間、費用がかかり開発自体を圧迫する
                       3）評価をても日常運用ではパッチ適用やバージョ
                       ンアップ等への対応が必要になる
                       4）評価機関も不足している。現行数では、電子政府への対応は困難

毎メーカー B

立場 : メーカやベンダー
製品 / 機能 : IC チップとソフト
評価対象 : Security Target (ST)
技術者 / キャリア : 4 名。うち 2 名は入社 15～20 年クラス、残りは入社 5
                   年目程度
時間 / 費用 : 約 2 ヶ月程度 人件費のみで約 300 万程度
普及における問題点 : 1）作成できる技術者不足
                       2）規格自体が難しい
                       3）通常の製品開発より余分な時間、費用がかかり開発自体を圧迫する
                       4）知名度不足
                       5）民間企業の利用にかけるインセンティブがない

毎評価機関 C
<table>
<thead>
<tr>
<th>立場</th>
<th>評価機関</th>
</tr>
</thead>
<tbody>
<tr>
<td>製品 / 機能</td>
<td>特定の製品はない</td>
</tr>
<tr>
<td>評価対象</td>
<td>現在は Security Target (ST) のみ、将来的には Protection Profile (PP)、Target of Evaluation (TOE) の評価認証も目指す</td>
</tr>
<tr>
<td>技術者 / キャリア</td>
<td>不明（回答が得られなかった）</td>
</tr>
<tr>
<td>時間 / 費用</td>
<td>不明（回答が得られなかった）</td>
</tr>
<tr>
<td>普及における問題点</td>
<td>1) 規格自体が難しいので人材育成に時間がかかる</td>
</tr>
<tr>
<td></td>
<td>2) 普及方法に問題あり、海外事例などをもっと研究すべきである</td>
</tr>
<tr>
<td></td>
<td>3) 文化的な素地が日本にはない</td>
</tr>
</tbody>
</table>

**評価機関 D**

<table>
<thead>
<tr>
<th>立場</th>
<th>評価機関</th>
</tr>
</thead>
<tbody>
<tr>
<td>製品 / 機能</td>
<td>IC カード製品を得意分野とする</td>
</tr>
<tr>
<td>評価対象</td>
<td>Security Target (ST)、Protection Profile (PP)、Target of Evaluation (TOE) の評価認証。</td>
</tr>
<tr>
<td>技術者 / キャリア</td>
<td>10人（NITE の有資格者は 1人）</td>
</tr>
<tr>
<td>時間 / 費用</td>
<td>1人月 2,500 千円で 3ヶ月〜1年</td>
</tr>
<tr>
<td>普及における問題点</td>
<td>1) 規格自体が難しいので人材育成に時間がかかる</td>
</tr>
<tr>
<td></td>
<td>2) 評価費用についての相場観が形成されていない</td>
</tr>
<tr>
<td></td>
<td>3) メーカ等ではこの規格を理解できる人材が限られる</td>
</tr>
</tbody>
</table>

**メーカー E**

<table>
<thead>
<tr>
<th>立場</th>
<th>メーカやベンダー</th>
</tr>
</thead>
<tbody>
<tr>
<td>製品 / 機能</td>
<td>ファイアウォール製品</td>
</tr>
<tr>
<td>評価対象</td>
<td>Target of Evaluation (TOE)</td>
</tr>
<tr>
<td>技術者 / キャリア</td>
<td>数名（一桁）</td>
</tr>
<tr>
<td>時間 / 費用</td>
<td>開発費全体で数千万円の水準</td>
</tr>
<tr>
<td>普及における問題点</td>
<td>1) 作成できる技術者不足</td>
</tr>
<tr>
<td></td>
<td>2) 余分な時間、費用がかかり開発自体を圧迫する</td>
</tr>
<tr>
<td></td>
<td>3) ISO/IEC 15408 の規格自体が現状のスパイラル型システム開発手法と合致しない点が多い</td>
</tr>
</tbody>
</table>

65
(2) アンケート調査結果抜粋

図表 2.5 セキュリティ評価認証制度に関する企業アンケート調査抜粋（1）

<table>
<thead>
<tr>
<th>設問内容</th>
<th>民間</th>
<th>公共</th>
<th>合計</th>
</tr>
</thead>
<tbody>
<tr>
<td>「IT セキュリティ認証制度について知っている」（N=275）で知っていると回答した割合</td>
<td>28%</td>
<td>30%</td>
<td>29%</td>
</tr>
<tr>
<td>「本制度の認証取得製品を利用している」（N=80）で利用していると回答した割合</td>
<td>20%</td>
<td>23%</td>
<td>21%</td>
</tr>
<tr>
<td>「本制度の認証取得製品を利用していない理由」で（N=35）本制度の認証の有無を気にしていないと回答した割合</td>
<td>27%</td>
<td>66%</td>
<td>28%</td>
</tr>
<tr>
<td>「IT セキュリティ認証制度をどのように考えているか」（N=275）で本制度をあまり重視していないと回答した割合</td>
<td>33%</td>
<td>33%</td>
<td>33%</td>
</tr>
<tr>
<td>「何らかの評価認証取得の製品を選択する」（N=275）で選択していると回答した割合</td>
<td>27%</td>
<td>35%</td>
<td>29%</td>
</tr>
<tr>
<td>「IT 評価認証制度の認証取得の製品価格が高いでも買う」（N=275）で買うと回答した割合</td>
<td>50%</td>
<td>62%</td>
<td>52%</td>
</tr>
<tr>
<td>「高くなる場合の価格の上限は10%以下」（N=144）で肯定している割合</td>
<td>72%</td>
<td>73%</td>
<td>73%</td>
</tr>
<tr>
<td>情報セキュリティに関する情報の入手源として、「システムベンダー」と回答した割合（N=275）</td>
<td>50%</td>
<td>50%</td>
<td>50%</td>
</tr>
</tbody>
</table>

2.6 問題点の抽出
文献調査、ヒアリング調査、及びアンケート調査から現状の問題点を想定すると、下記のように整理される（図表 2.6）。次項で問題点を概ね下記の分野に沿って記述する。

図表 2.6 セキュリティ評価・認証制度において想定される問題点

<table>
<thead>
<tr>
<th>問題点分野</th>
<th>検証項目</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. 人材面</td>
<td>◆ PP、TOE 等を評価および作成できる人材の整備畳</td>
</tr>
<tr>
<td></td>
<td>◆ 人材育成の体制・機能の整備状況</td>
</tr>
<tr>
<td>B. 体制面</td>
<td>◆ 評価機関数の整備状況（数・水準）</td>
</tr>
<tr>
<td></td>
<td>◆ 官公庁の施設との連携状況</td>
</tr>
<tr>
<td></td>
<td>◆ ユーザ企業・官公庁等での認知度</td>
</tr>
<tr>
<td>C. 技術面</td>
<td>◆ PP、TOE 等の作成の難易度・複雑性</td>
</tr>
<tr>
<td>D. 経済面</td>
<td>◆ 開発コスト・期間に与える影響</td>
</tr>
<tr>
<td>E. その他</td>
<td>◆ 日常の利用実態との整合性</td>
</tr>
<tr>
<td></td>
<td>◆ ST 確認の位置づけ・利用度</td>
</tr>
</tbody>
</table>
2.6.1 人材面

(1) 人材の不足
現状、PP や ST の作成ができ、それらを評価できる人材が、情報システムや製品を開発し納品するメーカーやベンダー側、並びに評価機関自体に不足している。まずメーカー側では、製品納入の要件として ST 作成を求められるという経験が無く、或いは乏しいために、その技術を持つ技術者が社内にほとんどいないのが実態である。また評価機関側も制度そのものが立ち上がって間もないこともあり、PP、ST、TOE 等を評価できる人材が少ない。このため、ST 確認等を依頼しても、評価、認証にかなりの時間がかかる（ヒアリング調査では、現状、評価で 2 ヶ月程度、認証で更に 3 ヶ月程度かかっているようである）ことが多いようである。

このような状況では、特定期間に大量の評価申請があった場合、処理能力がネックとなって希望する期限までに評価・認証が終わらない事態が発生し得る。

(2) 人材育成体制が不十分
PP や ST の作成、PP、ST、TOE の各評価ができる人材については、独立行政法人製品評価技術基盤機構（NITE）が、ST 確認のための評価を行える資格としてセキュリティゲートウェイ検査等の評価者資格を設けているが、その資格を取るための研修プログラムや試験等について詳細な内容が公表されていない。

また、PP 及び TOE 認証については、評価ができる資格を得るには、評価機関において、実際に試行評価を行う必要があるが、試行評価を実施するための知識やノウハウ等に関する研修プログラム等については不明である。（評価機関では評価者育成のために、海外にて研修をおこなっているところもある。）従って、ISO9000 や ISMS 適合性評価制度等で認定された研修機関のようなものが存在していない。
2.6.2 体制面

(1) 評価機関数の不足
現在国内でセキュリティ評価・認証を実施できる機関は2機関、またST確認のみ評価できる評価実施機関は7機関である。また各機関で認証機関である独立行政法人製品評価技術基盤機構（NITE）から認定されている審査員は1〜2名程度である。とても多数の評価申請を処理できる体制とはいえないと、仮に電子政府構築における調達製品すべてにおいて、ST確認を行う場合、現状の評価機関数では処理できないことが十分予想され得る。

(2) 電子政府構築の流れと連携が不十分
電子政府構築に伴う情報システム並びに情報機器、ソフトウェア等については、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が、実際ににはセキュリティ評価されていないものがかなり存在している。もちろんセキュリティ評価・認証制度の確立前に調達されたものはやむを得ないとしても、同制度の確立後、調達されるかなりの製品が本来セキュリティ評価を受けるべきであるにもかかわらず、実際にはほとんど評価されていないようなである。（評価されている製品として登録をしているものがわずかしかない。）これは、制度自体が、当初めざしていた電子政府構築に伴う情報システム並びに情報機器、ソフトウェア等への評価を十分実施できる体制になっていなかったために、製品の調達元（例えば、地方自治体）なども積極的に利用できない状況にあると考えられる。

(3) 認知度不足
ヒアリング調査やアンケート調査結果から、同様に直接携わった技術者やセキュリティ分野に詳しい人以外を除き、同制度について知っている人が想像以上に少なかった。特にエンタープライズ企業ではその傾向が強く、業種業態に関係なく広く普及させていくことを考えるならば、広報活動を今以上に積極的に実施し、知名度を上げる必要がある。

(4) EAL4以上の承認を受けた評価機関はない
2003年2月現在、日本国内では、評価保証レベル（EAL）3までの評価を行う承認を受けた評価機関が2団体あるが、EAL4以上の承認を受けた評価機関は無い。我が国のIT製品の国際競争力を確保するためには、国際的な相互承認アレンジメントにおける最高位の評価保証レベルであるEAL4等の評価を行う評価機関の早期承認が期待される。

2.6.3 技術面

(1) ISO/IEC 15408自体の難しさ
ISO/IEC 15408は、技術規格であり、マネジメントシステムに関する規格に比べ内容が極
2.6.4 経済面
(1) 開発期間との整合性
 メーカやベンダーにとって、もともと開発期間はタイトなことが多い。その中で認証という、更に付加的な期間が組み込まれることになり、開発期間が益々タイトになる。例えば、現在実施されている電子政府関係製品での ST 確認の評価・認証期間は、ある企業のヒアリング調査によると、評価に2ヶ月程度、認証に更に3ヶ月程度かかるようである。またこれが TOE 評価になった場合は、さらに評価期間がかかります。

(2) コスト
 技術的に難解で、自力での PP や ST の作成にはかなりの時間がかかりため、初めは、外部専門家の支援を受けることが多い。また評価申請に関する費用も当然発生する。特にメー カやベンダーでは PP や ST の作成に携わる人材を新たに投入する必要があるため、前記の 費用に追加して内部人件費も含めるとかなりのコストアップに繋がる可能性がある。例えば、 IC カード用チップの ST 確認においては、評価費用は（評価申請に関わるコンサルティング 費用を含む）1件約 300 万円程度かかっている。

2.6.5 その他
(1) ST 確認に関する疑問
 ISO/IEC 15408 の規格上の評価としては、前記の通り、PP 評価と TOE 評価の二つがあ る。また日本独自の制度として ST 確認がある。ST 確認は、ST（セキュリティ基本設計書） が、ISO/IEC 15408 に基づき作成されていることを評価・確認するにすぎず、製品が ST に 基づき、その意図どおり開発されているかどうかまでは評価しない。その意味で、本来の ISO/IEC 15408 の考え方から見れば十分とは言えず、製品の認証を依頼する側からも評価の 價値に対し疑問視する声もある。

(2) 運用可能性に対する疑問視
 現在かなり普及が拡がっている Linux や Sendmail などは、オープンソースであるために
ISO/IEC 15408 の認証が困難である。また、認証取得製品ではセキュリティホールを塞ぐためにパッチを適用すると、バージョンが変わることになり、当初の認証が無効になる。このように現場で行われている日常運用管理と矛盾する部分が一部あるため、本認証制度の実際の運用には困難が伴う。

2.7 問題点の整理
これまですべてできた問題点を整理すると下記図表 2.8のようまとまる。今後各分野別に対策を立案するについて、以下のような点に留意して進みたい。

人材面は制度運用の実質的な担い手の不足を意味し、育成機関の整備から始める必要がある。この問題点が解決しないと制度が運用できないという意味で、問題点としての重要度は高い。

本制度の体制に関する問題点は、機関整備・施策連携・広報活動に関する問題点であり他の人材面や経済面の分野にも関連する。対策としては制度目的に沿って、制度設計や広報活動について多様な手法が考えられ、対策の中心になると考えられる。

技術面の問題は規模の難易度・内容等に関する問題点であり、人材面、体制面から補完することで対策の立て難い分野である。

経済面に関する問題点はメーカ・ベンダーの費用負担・作業負荷の問題点であり、人材面や技術面と深く関連している。対策としては発生するコスト等に対し経済原則に沿って、インセンティブやコスト転嫁策等を検討することが求められる。

その他の日常運用上の問題や ST 確認の位置づけはそれぞれ技術面、体制面と深く関わる問題として、技術面や体制面の対策の中で検討する。

<table>
<thead>
<tr>
<th>問題点分野</th>
<th>検証内容</th>
</tr>
</thead>
</table>
| A. 人材面 | ◆ 絶対の人材不足  
              ◆ 遅れている人材育成機関 |
| B. 体制面 | ◆ 評価機関が不足・弱体  
              ◆ 実質的な意味で本制度利用が勧奨されていない  
              ◆ 官公庁・民間いずれでも低い知名度 |
| C. 技術面 | ◆ 特別な経験や能力を要求される規格内容 |
| D. 経済面 | ◆ 従来に比べ余分な開発コスト・期間が発生 |
| E. その他 | ◆ オープンソフトやバージョンアップへの対応困難  
              ◆ ST 確認は利用しにくい中途半端な評価水準 |
3. IT セキュリティ評価・認証制度の普及対策の提言

3.1 基本認識

阻害要因の整理で示したように、現状の本制度の普及度・知名度の不足はいくつかの要因が複合した結果と言える。このような状況での対策は、特定の少数の施策で一挙に大幅な改善を果たすことは難しい。

評価・認証の制度はあくまで利用者の支持が普及の原動力であり、その利用者すなわち企業・官公庁に働きかけて具体的な動きが出てくるまでには、関係者の相当の努力と時間が必要と考えられる。そのため阻害要因の1つ1つについて、着実に改善していくことが必要となる。

3.2 他の ISO 認証制度（ISO9000）との比較

3.2.1 体制面

ISO9000の認証制度では、下記のような体制となっている（図表 3.1）。

■ 特徴的では制度を支える審査員育成体制が制度の中に織り込まれている点である。
■ 審査を受けるには、ISO の規格に沿った制度設計が必要となるため、その助言や制度整備を行うコンサルティングが発展している。
3.2.2 コスト面
認証取得する企業には制度対応のための社内準備作業のほか、審査登録について審査機関への審査費用の支払や、コンサルティング会社へのコンサルティング料支払など、経費負担が必要となる。しかしISOは事業所単位、企業単位の認証制度であり、これらの費用個々の製品別にかかるものではなく、企業単位の費用である。取引先との取引維持に必要なコストととらえ、企業の品質管理レベルの高さを社外にアピールする宣伝効果や自社の業務改善への効果を考えると、企業にとって余分な、重い負担ではなく魅力ともなっている。

3.3 対策
3.3.1 人材面
企業や評価機関へのヒアリング調査から、絶対的に不足しているISO/IEC15408の評価や策定ができる人材の育成が極めて重要なことが分かる。他のISO標準に基づく制度では研修機関を制度の必須要素として組み込んでいるケースがほとんどであり、本制度においても早急に開設を検討すべきである。

具体的な方法としては、eラーニングの活用による通信教育の導入（基礎レベル）、海外の専門家を招聘しての専門機関の開設（評価者レベル）等が有効と考えられる。また審査員等の資格制度を再構築し、審査能力段階別に人材整備を進めていくことも検討課題となる。

3.3.2 体制面
(1) 評価機関の増強
現状の評価機関数は2社しかなく、人材スタッフも少ないので、申請が集中するとすぐに限界に達してしまう懸念が強い。制度が普及していないので、申請件数が少なく、評価機関がわずかしかない現状であるが、一定数に達するまでの間の立上げの支援、優遇策の検討や評価機関としてのビジネス上の魅力を出すなどの努力が必要となる。

(2) 官公庁の情報化施策等との連携強化
電子政府施策と連携させるという意味では、関係省庁等における本制度の普及徹底が不可欠である。ヒアリング調査においても、「全く知らない」という回答が中央省庁から出て、少なくとも制度の名称・目的についての周知徹底が望まれる。

次には制度内容の広報活動であり、各省庁で推進されるネットワーク計画や情報化計画との連携を進めていくことが有効と考えられる。具体的にはこれらの計画・施策を推進する上で、本認証・評価制度の利用を組み込んでいくようなことが想定される。
例えば住民基本台帳のネットワーク化等が想定され、社会的に話題性のある施策との連携で本制度の知名度向上では有効と考えられる。
(3) 制度の認知度向上施策

認知度向上については、官公庁よりも民間企業での認知度、特にシステムユーザとなる調達側の企業に対するアプローチが有効と考えられる。情報システムベンダー側は調達側が求めれば認証取得に取り組まずを得ない立場であり、利用者側がこれらの制度に関心を持つような仕掛けが必要ではないか。またアンケート調査結果でも調達側の情報セキュリティに関する情報収集は、主に情報システムベンダー等に大きく依存している。

例えば先行している、ISMS制度に関するセミナーや講習会で本制度についても紹介説明し、本制度の情報に触れる利用者を増やす、マスメディアを利用して民間ベースの情報セキュリティ製品・サービスのPR活動と連携して、制度の存在・重要性を認知させる等の取組が想定される。

留意点として、利用者にしろ供給者にしろこの認証・評価制度の利用によってメリットが期待できる業界・分野に狙いを定めて、集中的に活動を行うことが有効と考えられる。

利用者ではセキュリティのレベルが事業の成否や市場での評価を左右するような企業、例えば個人情報機関、データベースサービス等が想定される。

供給者側では、これから需要が見込まれそうな製品・サービスの市場との連携を重点的に進め、製品普及と本制度利用を同調させるような取り組みが想定される。

3.3.3 技術面

(1) 教育カリキュラム

技術的難易度が高いこと自体は変えられないが、教育方法や資格制度を工夫することで、審査者予備軍を育成していくことも有効と考えられる。審査者に必要とされるスキルは難易度が高いが、最終レベルに至るまでの中間的なランク等を創設していくこと等も考えられる。

カリキュラム面では、情報システムの部門経験者と未経験者で異なる教育手法も検討されて良いと考えられる。

(2) 評価機関への評価水準のランク引き上げ

評価機関の評価実績に応じて評価機関が評価できるレベルを引き上げていくことも、制度の利用や評価スキルの向上のためには必要と考えられる。評価できるレベルとしては、評価事業で先行している機関や人材等で体制整備の進んでいる機関に、EAL4までの評価を認めること等が期待される。

(3) 人材派遣・講習会等による支援

情報システムベンダーの中で規模等が小さく、本制度の専門家を社内で保有できない場合、公的機関による登録人材の派遣による支援、講習会等による評価補助員レベルのノウハウ取得の支援策を行う。高度な専門知識について派遣人材が対応し、基本的な知識・現場での対応力習得のために講習会等の集合教育・通信教育を行う。
3.3.4 経済面
情報セキュリティ製品・サービスの供給者側において、この制度が不人気な理由に評価に要するコストと時間があり、対応力に乏しい中小企業クラスでは、官公庁等でこの制度を義務付けた場合、事実上市場から締め出される可能性も高い。
この評価コストを直接利用者側に転嫁することは通常は難しいため、何かの支援施策が求められる。
例えば、セキュリティ評価に要したコストについて評価レベルと連動させて一定割合の補助金あるいは減税措置等が想定される。実際に英国の例ではあるが、中小企業へのISO9000導入を促進するため、コンサルティング費用について最高実費の1/2まで補助金を交付している。
また、官公庁等調達側すなわち利用者に費用負担をさせる方案として、評価制度利用についての直接的な予算枠の設定や補助金の支給、インセンティブの供与等も必要と考えられる。
当初は公的な支援が欠かせないと考えられるが、普及につれて評価費用が引き下がり、公的負担は軽減していくと予想される。

3.3.5 まとめ
現状の阻害要因からみた対策については、概ね上記のとおりであるが、いずれも個別・単発では実効性が弱いと考えられる。
基本は人材育成と知名度と考えられるが、一体のものとして体系的に推進していくことが必要と考えられる。例えば人材育成が不十分な状況での広報活動やマーケティング的活動は制度としての信用やイメージを損なう恐れがあり、人材育成を待つと広報活動では、制度として浸透するのに時間がかかる。一元的な管理の下でのタイミングのよい施策実行が求められる。
4. セキュリティ評価・認証制度に関する市場予測

4.1 現状の申請状況

■ NITE
  ➢ 各評価機関・ベンダー・メーカ等で評価取得へ向けて申請準備中の製品は、およそ20件ぐらいあるのではないかと推測している。

■ ECSEC
  ➢ 評価作業完了後、認証未済の製品がJEITA分も含めて3件あるが、評価の引き合いとしては10数件ほどあるとのこと。
  ➢ 実際の評価作業には1件当たり約1年かかると想定している。
  ➢ 審査員自体の人的余力は少なくNITEの認証を得ている審査員は1名である。当面取り扱い件数を急に増やせる状況ではないと考えられる。

■ JEITA
  ➢ 審査員の人的余力はECSECと同様と考えられるが、また本認証評価事業の専業機関ではなく、ECSECよりも取り扱い件数は少ないと見込まれる。

4.2 利用者側の需要

4.2.1 企業アンケート調査結果

<table>
<thead>
<tr>
<th>図表 4.1 セキュリティ評価・認証制度に関する企業アンケート調査結果（2）</th>
</tr>
</thead>
<tbody>
<tr>
<td>「ITセキュリティ評価・認証制度について知っている」（N=275）で知っていると回答した割合</td>
</tr>
<tr>
<td>「ITセキュリティ評価・認証制度の認証取得製品を利用している」（N=80）で利用していると回答した割合</td>
</tr>
<tr>
<td>「何らかの評価認証取得製品を選択する」（N=275）で選択していると回答した割合</td>
</tr>
<tr>
<td>「ITセキュリティ評価・認証制度の認証取得製品を価格が高くても買う」（N=275）で買うと回答した割合</td>
</tr>
<tr>
<td>「高くなる場合の価格の上限は10％以下」（N=144）で肯定している割合</td>
</tr>
</tbody>
</table>

■ 本制度の認知度は約3割である。情報システム担当者に対するアンケート調査であることを考えると、認知度は低い。
■ ITセキュリティ評価・認証制度による認証取得について、製品取得動機になると考えた割合が約3割程度であり、製品購入の動機としては一部の評価されているが、選択
条件となるレベルではない。

- 民間よりも公共関係の機関の方が、全体的に認証制度への評価・意識付けが高い。
- 價格が高くても買う割合は約半分であるが、実際の価格差は 10%程度とする回答者が官民問わず 7 割以上である。証制度のコスト負担は 10%未満を想定しているのが、利用者側の意識水準と考えられる。

4.2.2 ヒアリング調査
- メーカヒアリング調査によれば、官公庁の調達では ST 確認を仕様書で要求するケースもでている。
- こうした一方で、官公庁・自治体の本制度の認知度は低く、中央省庁関係では制度そのものを知らないという部署が多く、地方自治体の方がいくらか名前・制度内容等をある程度認知している部署が多かった。
- 本認証制度の具体的利用に関する態度や意識面では、普及するかどうかを様子見している印象が強かった。制度を知らないという回答者からは、どこまでこの制度が世の中で広まるかと逆に質問を受けるケースもあった。
- 調達側の企業・官庁から、制度利用についての前向きな意向は確認できなかった。

4.3 供給者側の取組状況
4.3.1 ヒアリング調査

- 供給側である情報システム会社・メーカはこの制度の費用負担と作業負荷に悩んでいる印象。
- 製品自体にコスト負担力があることが必要で、その意味で価格の高い製品あるいは販売量の多い製品でないと認証制度利用は引き合わないという見方のようである。
- ヒアリング調査した業界最大手の企業でも、今後 1 年間の認証制度の申請件数は、せいぜい 1-2 件となっている。
- しかしながらセキュリティ自体が事業の根幹に組み込まれている分野、例えば公共インフラや金融分野の市場では本制度の導入が本格化するケースを想定しているメーカーでも一応の準備はしている。

4.4 他の認証制度の普及状況
セキュリティ評価認証制度の今後の展開について、既に制度として普及している他の ISO 認証制度のこれまでの普及経緯を参考として検討する。

4.4.1 ISO9000 シリーズ
- ISO9000 シリーズの認証取得が始まったのは、1990 年からであるが、当初は制度に
対する民間企業の反応は極めて冷やかなものだったと言われている。

- マネジメントシステムという考え方がわが国にあまり定着していなかったこともあり、早い段階から検討を始める企業は少なかった。
- しかしながら、輸出や海外企業との取引で有効であることや、経済のグローバル化、マネジメントシステムへの関心の高まり等により、急速に認証取得の件数が増加していった経緯にある。
- 実際の認証取得適合事業所数の伸びを日本適合性認定協会資料でみると、1994年から1998年の4年間で累積取得件数は826件から6,627件と、年平均1.7倍程度の増加となっている。
- またこれ以前の資料として、国のモーブル社が行った調査でわが国の認証件数は1992年1月で約200件程度と報告されているので、1992年から1994年の3年間で累積取得件数は約4倍となっている。
- このような急増現象はISO9000のような認証制度は一度社会的に認知されて取得することへの動機付けが企業活動の中で定着すると、新しい流れに乗り遅れまいとして一挙に取得需要が増大することを表している。

4.4.2 ISO14000シリーズ

- ISO14001は地球環境問題への取組と合わせて規格化された認証制度で、1996年に発行された。
- この認証制度は地球環境という新しい価値観に基づく制度であり、環境問題への取組が国内外で本格化するとともに、取得件数が増加してきた経緯がある。
- 実際に取得件数の推移を日本適合性認定協会資料で見ると、1996年から2000年の4年間で累積取得件数は106件から4,019件と、年平均約2.5倍の増加率を見せている。
- ISO9000と異なり、当初から環境問題の取り組みの重要性が民間・官公庁・個人等の中で形成されており、ISO9000の社会的認知もあって、ISO14001は発行時から爆発的に増加した。

4.5 IT評価・認証制度の市場予測

現状の利用者側・供給者側いずれも本制度に関し明確な認識や取組体制が整備されていない状況を勘案すると、市場予測を需要と供給の構造関係から導くのは、難しいと考えられる。特に現時点で利用者側が制度自体を知らない割合が高く、調査条件としてこの制度がいつごろ、どの程度組み込まれるかを予想することは極めて難しいと考えられる。

そのため本調査においては推計のシナリオを2つに分け、1つは評価機関等からのヒアリング調査結果をベースに、当面、評価機関で評価が可能な申請件数の推計による推計シナリオ（A）とし、もう1つは製品自体が既に存在するため比較的制度利用の予想が行いやすい供給者側からの申請件数からみた推計シナリオ（B）として検討することとした。

77
4.5.1 前提条件

(1) シナリオ A

■ 現在の評価機関等への認証取得申請の見込み件数
  ➢ NITE 等のヒアリング調査から各メーカーが本年度において申請へ向けて作業を進めようとしている製品等の件数を認証取得済みも含めて 20 件と推定。
  ➢ この 20 件を本年度も含めて 3 年間の中で認証評価取得をすることとする。
  ➢ 理由：ECSEC 等のヒアリング調査より評価機関の処理能力において、評価機関・評価人材が絶対的に不足であり、メーカーヒアリング調査により、企業側の人材不足、体制不備がある。
  ➢ 人材育成は海外での教育が必須であり、実体験も含めて約 2 年必要。
  ➢ 4 年目以降は人材育成・体制整備が整い、評価処理能力も每年 2 倍増加すると仮定。

(2) シナリオ B

■ 新規に認証取得を申請するセキュリティ製品として可能性の高い、「ファイアウォール・VPN」 「IC カード」 「バイオメトリクス製品」 「PKI 関連製品」 及びセキュリティ製品ではないがセキュリティ機能が重視される「データベース関連ソフト」の申請件数を予想。
  ➢ 理由
    • セキュリティ製品のうちアンチウイルスソフトウェアは寡占市場となっており、販売実績の大きい供給側での認証取得の動機は弱いと推定される。
    • 同じくセキュリティ運用ソフトウェアは商品分野が広く、その商品特性から普及は遅めと考えられることから、供給側の認証取得における優先度は低いと推定。
    • 暗号関連製品も市場規模が小さいことが予想されることから、認証取得における優先度は低いと推定。
    • 「データベース関連ソフト」 は本年度も認証認定されている、セキュリティ機能が重視される製品分野であり、その特性でメーカーの認証取得需要が強いと想定。

■ 「ファイアウォール・VPN」「IC カード」「バイオメトリクス製品」「PKI 関連製品」 「データベース関連ソフト」 各製品の主要日本企業数を下記のように推計。
  ➢ 「ファイアウォール・VPN」：9 社、「IC カード」：8 社、「バイオメトリクス製品」：19 社、「PKI 関連製品」：7 社、「データベース関連ソフト」：5 社

■ 各製品分野の主要企業のうち、認証取得の申請を行う企業数毎年 1/3 ずつ増加するモデルを想定する（= 様子見モデル）。

78
各社の申請件数は毎年1件とする（当面は申請各社の技術者が不足すると予想し年1件程度にとどまると思定）。
加えて予測年度の最終年度は新規参入企業の申請分を加算する意味で、各社1.5件とする。

4.5.2 推計

图表 4.2 セキュリティ評価・認証制度の利用件数予測

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>シナリオA（既存受注分消化）</td>
<td>5</td>
<td>7</td>
<td>8</td>
<td>16</td>
<td>32</td>
<td>68</td>
</tr>
<tr>
<td>シナリオB</td>
<td>5</td>
<td>17</td>
<td>32</td>
<td>48</td>
<td>70</td>
<td>172</td>
</tr>
<tr>
<td>ファイア・ウォール・V P N（9社）</td>
<td>1</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>13</td>
<td>33</td>
</tr>
<tr>
<td>視点</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>25</td>
</tr>
<tr>
<td>パイオメトリクス</td>
<td>0</td>
<td>6</td>
<td>12</td>
<td>19</td>
<td>28</td>
<td>65</td>
</tr>
<tr>
<td>データベース関連</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>10</td>
</tr>
</tbody>
</table>

■ シナリオ A

- 評価機関及び申請側の人材育成が整備されるまでの3年間（2004年度までは）現有人材での対応と考え、相談ベースも含めた手持ちの受注残を消化ベースで推移。
- 2005年以降は、評価能力・申請能力ともに倍増し、利用件数が急増する。
- 予測数値としては最低限の水準と位置づけられる。

■ シナリオ B

- 評価機関が期首から整備されて制度整備が整った2003年度から2006年度までの累計取得件数は、22件から172件と約8倍であり年平均1.7倍の伸びと推定される。これは前述したISO9000の1994年から1998年の累計取得件数の年平均伸び率とほぼ同水準である。
- 対象製品を限定しているが、参入している主要企業が2005年度には本制度を全社利用する想定にしており、予測数値としてはかなり高めの水準と位置づけられる。

以上