情報セキュリティビジネス
に関する調査報告書

平成１３年３月

情報処理振興事業協会
セキュリティセンター

はじめに

21 世紀を迎え、わが国の主要産業の不振は底を打った感があるが、その一方で、相次ぐ生保の破綻や株価の低迷、米国のネットバブル崩壊など、依然として不安材料も多い。しかし、1990 年代後半から米国を中心に世界を席巻した IT（情報技術）革命は日本においてもようやく浸透しつつあり、産業界における IT 投資の拡大と、異業種・外資の参入や系列の崩壊による新たな競争環境の形成、2003 年の電子政府実現に向けた政府の積極的な取り組みなど、日本経済の力強い再生を予感させる動きも見られる。その鍵を握るのは、インターネットを軸とする高度なネットワーク社会の形成である。そして、その実現には、ネットワークの脆弱性をカバーするセキュリティ基盤の整備が不可欠とされる。

情報処理振興事業協会セキュリティセンターでは、平成 9 年 1 月の発足以来、情報セキュリティに関する意識の啓発と、具体的な対処方策を講ずるために必要な手段と情報の提供を目指して、諸活動に取り組んでいる。本調査研究は、その一環として、情報セキュリティ環境を支える重要な役割を担うセキュリティベンダを中心に、わが国の情報セキュリティビジネスの現状や市場動向を分析し、その問題点と課題について明らかにすべく、公募により採択された株式会社三菱総合研究所に委託し、実施したものである。本調査研究の成果が、わが国の情報セキュリティビジネスのさらなる活性化と、高度なセキュリティ基盤の実現に資すれば幸いである。

平成 13 年 3 月

情報処理振興事業協会
セキュリティセンター

目　次

序　章

本調査研究の概要

０．１　調査の背景

2000 年１月から２月にかけて相次いで発生した日本の省庁ホームページ連続不正アクセスや、米国有力ポータルサイトを標的とした DDoS（Distributed Denial of Service）攻撃をきっかけとして、情報セキュリティへの関心は急速に高まっており、セキュリティビジネスもかつてないほど活況を呈している。

公共分野では、各省庁におけるセキュリティポリシーの策定や GPKI（Government Public Key Infrastructure）の検討、さらに ISO/IEC 15408 に基づくセキュリティ評価認証制度の実施に向けた取り組みなど、2003 年度までに実施される電子政府の基盤構築に向けて、そのインフラとなるセキュリティ環境の整備が積極的に進められている。

また、ビジネス分野では、ネットワークによる企業間、企業・消費者間の EC（電子商取引）市場が本格的に立ち上がりつつある現在、企業の EC サイトがミッション・クリティカルな役割を担うケースが増加しており、不正アクセスによる機密漏洩やシステムダウンがビジネス上致命的なトラブルをもたらすリスクも顕在化している。そこで、各社とも、限られた予算と時間の中で、リスク・コスト・利便性のバランスを充分に考慮し、自社に最適なセキュリティ環境を整備することが求められている。

さらに、個人・家庭分野においても、広帯域・常時接続のネットワークが人気を集めているが、常時接続の回線を経由した不正アクセスによって個人情報が盗まれたり、他サイト攻撃のための踏み台として悪用される危険性も指摘されている。

こうしたセキュリティ需要の高まりを受けて、セキュリティ製品の供給や、それらを組み合わせてセキュアなシステムを構築・運用するセキュリティサービスの提供を行う事業者（以下セキュリティベンダと呼ぶ）のビジネスチャンスは急速に拡大している。ただし、セキュリティ製品は、軍の需要が大きい米国やイスラエルの企業の製品が世界市場を席巻しており、国内の製品ベンダの劣勢は否めない。また、今後はプラットフォームへの組み込みが進み、販売数が伸びても、市場規模の成長に反映されにくくなることが予想される。一方、コンサルティングや監査、システム構築・運用のサービス市場については、昨今のセキュリティ・ブームの影響から市場環境が一変しており、セキュリティポリシーの策定からセキュリティシステムの導入・運用に至る事業サイクルが回り始めている。ただし、

米国に比べまだ充分でないとされるユーザ企業のセキュリティに対する認識と、広範で高度な技術的知見を要求されるセキュリティコンサルタントの人材の払底が、今後の市場拡大の障壁となる可能性もある。

こうした状況を鑑みて、ネットワークへの依存度が高い現代社会の安全性を高めるために、急速に変化しつつあるわが国の情報セキュリティビジネスの現状を捉え、セキュリティベンダの事業基盤の充実と活性化を促進することが重要と考えられる。

０．２　本調査研究の目的

本調査研究の目的は、以下の通りである。

（１）情報セキュリティビジネスの枠組みを明確化し、その産業構造や参入業種、ビジネストレンドを分析する。

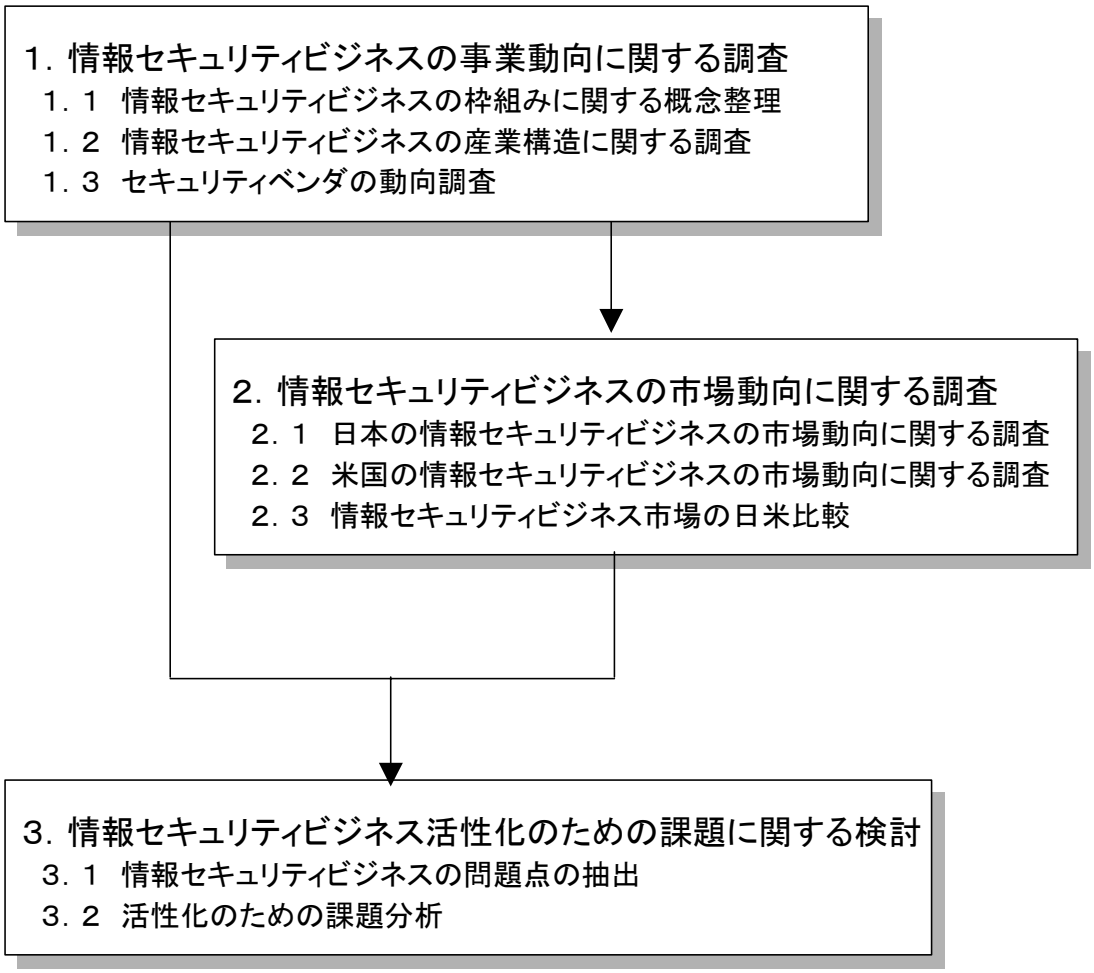
（２）日本と米国の情報セキュリティビジネスの市場規模（現状と予測）を推計し、その規模や構造について比較する。

（３）上記（１）（２）に基づき、ビジネスの活性化のための問題点と取り組むべき課題を提言する。

０．３　調査フロー

本調査のフローを図表０－１に示す。

図表０－１　調査フローのイメージ



０．４　本調査研究の概要

本調査研究の概要を以下に示す。

０．４．１　情報セキュリティビジネスの事業動向

（１）情報セキュリティビジネスの枠組み

本調査研究の対象とする製品・サービスを以下に示す。

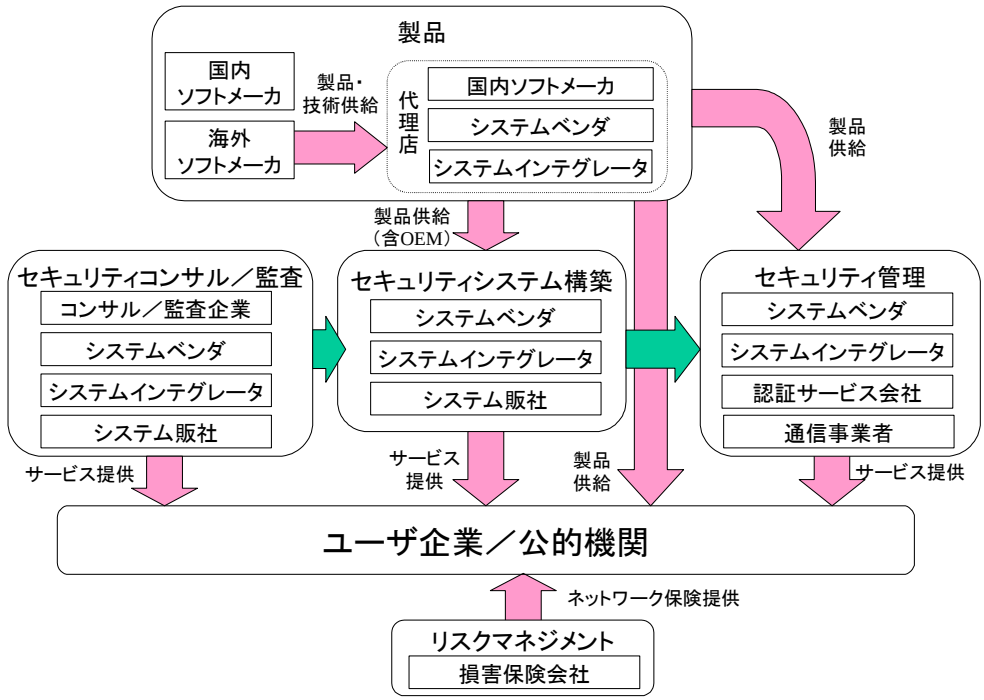
図表０－２　情報セキュリティ分野の製品・サービス構成

対象項目		概　要
製品	アンチウイルス	クライアント向けソフト、サーバ向けソフト
	ファイアウォール・VPN	VPN 機能はファイアウォールに搭載されるケースが多く、不可分として市場を推計
	認証	ワンタイムパスワード、ＩＣカード、バイオメトリクス、PKI 等
	暗号	暗号化製品、暗号ライブラリ、暗号ツールキット、電子透かし等
	セキュリティマネジメント	IDS、セキュリティ検査、アクセスコントロール
サービス	セキュリティシステム構築	セキュリティ技術の適用を前提としたシステム構築
	セキュリティコンサルティング／監査	セキュリティ診断、セキュリティポリシー策定、セキュリティ監査、その他セキュリティコンサルティング
	セキュリティ管理	セキュリティ運用代行、不正アクセス監視、認証サービス
	リスクマネジメント	ネットワーク保険

（２）情報セキュリティビジネスの産業構造

情報セキュリティビジネスの産業構造のイメージを以下に示す。

図表０－３　情報セキュリティビジネスの産業構造



（3）セキュリティベンダの動向

①ソフトウェアメーカ

セキュリティに特化した専従事業者が多く、世界規模で事業を展開している。その一環とした日本代理店でのビジネスが中心となる。自社製品を用いて専門的なサービスを提供するパートナーを増やしており、今後はエンドユーザに対してツールベンダ自らがネットワークを介して自社ツールを提供するサービス形態も普及していくとみられる。

②システムベンダ

システムインテグレーション以外に、コンサルティング、監査系サービスも強化することで、総合的なセキュリティサービスを提供している。また、グループ企業と連携し総合的なサービスを提供できるため、ユーザのあらゆるニーズに対応可能なことが強みである。

③コンサルティング／会計監査企業

セキュリティ・コンサルティングは、従来のコンサルティングの付加価値サービス的な位置付けから、セキュリティに特化した専門サービスとして提供している。また、コンサルテイングのみではなく、インテグレーションまで行うなどサービスの提供範囲の拡大や、情報セキュリティの監査などの新しいサービスへの取り組みも行っている。

④システムインテグレータ

セキュリティ専門の部門を立ち上げ、セキュリティビジネスへの取り組みを強化している。各インテグレータで温度差はあるが、セキュリティ機器の提供からコンサルテイング、検査／監視サービスを含めた総合的なサービスを提供する方向に向かいつつある。

⑤システム販売会社

営業力に強みを持ち、中小企業を中心にきめ細かなサービスを提供している。自社の個性を活かした特徴あるメニューを提供することで、独自マーケットを開拓する企業もある。

⑥通信事業者

ユーザのセキュリティ対策への負担を軽減するために、提供するネットワークサービスのセキュリティ対策を強化し、ユーザが安心して利用できるサービスの提供を目指している。また、通信サービス提供事業者としての利点を生かし、セキュリティ対策を含めたネットワーク運用代行などのアウトソーシングの請負にも注力している。

⑦損害保険会社

ネットワークの安全とセキュリティのリスクを補償するサービスは昨今注目されており、リスク評価等を併せたトータルな補償サービス提供する会社も増えている。

０．４．２　情報セキュリティビジネスの市場動向

（１）日本の情報セキュリティビジネスの市場動向

1999 年の日本の情報セキュリティ市場は、製品市場が 235 億円、サービス市場が 291 億円、合計 526 億円と推計される。5 年後の 2004 年にはそれぞれ市場は順調に拡大し、製品市場が 858 億円、サービス市場が 1,136 億円の合計 1,994 億円になると予測される。

①製品市場の動向

1999 年で最も大きな市場はアンチウイルス市場であり製品市場の 4 割を占める。次いで、ファイアウォール・VPN、認証と続き、暗号とセキュリティマネジメント製品については製品市場の 1 割にも満たない。しかし、2004 年ではアンチウイルスのシェアが下がり、代わりにファイアウォール・VPN が最も大きな市場となる。

②サービス市場の動向

1999 年で最も大きな市場はセキュリティシステム構築であり、サービス市場のほぼ 7 割を占める。2004 年には、セキュリティ管理が 2 割から 4 割近くへとシェアを伸ばす。

（２）米国の情報セキュリティビジネスの市場動向

1999 年の米国の情報セキュリティ市場は、製品市場が 2,069 百万ドル、サービス市場が 2,509 百万ドル、合計 4,578 百万ドルと推計される。5 年後の 2004 年には、製品市場が 5,328 百万ドル、サービス市場が 7,351 百万ドルの合計 12,679 百万ドルになると予測される。

①製品市場の動向

1999 年で最も大きな市場は認証市場であり、製品市場のほぼ半分を占める。次いでアンチウイルス、ファイアウォール・VPN、セキュリティマネジメント、暗号と続くが、この構造は 2004 年になっても大きな変化はない。その中でも高い成長率を示すのは認証とセキュリティマネジメントである。

②サービス市場の動向

1999 年の市場はセキュリティシステム構築がサービス市場のほぼ 4 割を占めている。2004 年までサービス市場全体は堅調に推移するが、その中でもセキュリティ管理が最も高い成長率を示している。

（３）情報セキュリティビジネス市場の日米比較

1999 年の情報セキュリティ市場をみると、米国は世界の 5 割以上を占めるが、日本はわずか 5%である。また、日本の情報サービス市場は米国の約 2 割であるのに、情報セキュリティ市場はわずか 1 割に過ぎない。2000 年の EC 市場でも日本は米国の 31.0%であるが、同年の情報セキュリティ市場で 11.1%と、その差は EC 市場に比べてさらに大きい。したがって、情報セキュリティ市場は情報サービス市場や EC 市場の水準まで日米格差を縮める努力をする必要があるといえよう。なお、こういった市場規模の差は、セキュリティ被害の件数にも現れており、日本よりも米国の方が圧倒的に被害件数が多くなっている。

０．４．３　情報セキュリティビジネス活性化のための課題

（１）情報セキュリティビジネスの問題点

①技術・製品のブラックボックス化

セキュリティ製品市場は、その大半を国やイスラエルのソフトメーカに依存しており、今後 OS やメールソフト、ルータ、携帯端末等へのセキュリティ機能の組み込みがさらに進むことから、ブラックボックスと化し、トラブル処理が後手に回ることも考えられる。

②不充分な相互運用性

インターネット VPN の製品は互換性が乏しいため、接続先がすべて同じメーカの製品を使用しなければならない。また、PKI 製品も相互運用性がなく、電子政府の省庁や窓口ごとに異なる電子証明書を使い分けなければならなくなる可能性もある。

③情報通信環境の多様化に伴う新たな IT リスクの発生

PDA や携帯電話に対するウイルスや不正アクセスのリスク、CATV インターネットにおける情報漏洩、Peer to Peer 接続のウイルスや不正アクセスのリスクなど、端末やネットワークの多様化によって新しい IT リスクが発生し、大きな問題を招く恐れがある。

④セキュリティコンサルタント／エンジニアの不足

セキュリティ分野では、コンサルタントやエンジニアの育成が難しく、米国でもセキュリティベンダ間で優秀な人材を奪い合っている状況にある。このような人材不足が情報セキュリティビジネスの発展の阻害要因となる可能性もある。

⑤スタッフのモラルの低下

サービス事業者のスタッフによる不正行為は、技術だけで防ぐことは困難であり、従業員のモラルの確立や充分なチェックがなされる運用ルールの適用など、組織・制度による対応が不可欠である。

⑥管理サービス強化に伴い求められる責任

セキュリティサービスビジネスは従来の製品ビジネスと違って手離れが悪く、ユーザをサポートするスタッフの負荷が増大する可能性が高い。

⑦セキュリティの投資対効果が不明確

セキュリティ投資は投資対効果が明確でなく、どこまでコストをかければ必要なセキュリティレベルを実現できるのかという点で適正な指標がないため、ユーザ企業側もセキュリティ投資の可否について判断しにくい。

⑧コンサルティングサービスのビジネス基盤の脆弱性

国内では、セキュリティコンサルティングの重要性が充分に理解されておらず、リスク分析に充分なコストをかけられなかったり、セキュリティコンサルタントのモチベーションが上がらず、人材が育ちにくくなる可能性がある。

⑨導入コストと運用コストがアンバランス

セキュリティ投資の許可が得られた場合も、その予算が一時的で、運用コストまでカバーできていないケースが見られる。

⑩セキュリティポリシーやルールが不徹底

セキュリティポリシーやルールを策定したにも係わらず、その実施が徹底されておらず、見込んでいたセキュリティレベルが実現できていないケースが見られる。

⑪セキュリティ担当部門の負荷増大

セキュリティホールや不正アクセスへの対応策の実施、エンドユーザからの反発、社内ネットワークの安全性の維持など、セキュリティ担当部門に要求される項目は多岐に渡り、その負荷も大きい。

⑫内部からの情報漏洩に対する対策の不備

ユーザ企業においても、EC 事業等を通じて得た顧客情報の管理が甘く、外部に流出する事件が発生している。

⑬中小企業や学校、個人・家庭の脆弱性

中小企業や学校、個人・家庭といったセキュリティ予算の確保が難しい層に対してはアプローチしにくく、それらの層がセキュリティレベルの低いセキュリティデバイドとなる可能性がある。

（2）情報セキュリティビジネス活性化のための課題

①次世代セキュリティ技術の開発

次世代の超高速通信環境では、セキュリティ技術にも高速かつ効率的な処理が要求される。そのような次世代セキュリティ技術の開発を先行的に進めることで、セキュリティ技術をリードする米国、イスラエルに負けない基盤技術を確立することも可能である。

②実践的なセキュリティ人材育成機能の整備

情報セキュリティベンダに必要な、高度なセキュリティ技術や優れた分析能力を有するスペシャリストとしてのセキュリティコンサルタント／エンジニアや、セキュリティに関する正しい知識を有するシステムエンジニアを育成する機能を整備する。

③セキュリティレベルの評価指標の策定

侵入テスト等によるチェックリストの結果から製品やシステムのセキュリティレベルを評価し、ユーザ企業がセキュリティ投資の費用対効果の分析や仕様作成に利用できる指標や評価方法を策定する。

④セキュリティデバイドの解消

中小企業や学校、個人・家庭等のセキュリティデバイド層を、ASP 等の集中管理型のサービスプロバイダモデルによってサポートする方向が考えられる。さらに、わが国のトータルセキュリティ実現のために、これらの層の支援施策の実施も考えられる。

第　１　章

情報セキュリティビジネスの事業動向

ここでは、情報セキュリティビジネスの業界・事業者に着目して、その動向について分析する。

１．１　情報セキュリティビジネスの枠組み

まず、既存のセキュリティ製品やセキュリティサービスの内容を整理し、対象とすべき情報セキュリティビジネスの枠組みを明確にする。

（１）情報セキュリティビジネスの発展経緯

①情報セキュリティビジネスの始まり

情報セキュリティがビジネスとして捉えられたのは、軍事技術であった暗号ツールの製品化が最初であろう。暗号技術の発展には第二次世界大戦における日・米・英・独の暗号解読戦が大きく影響しており、現在も米国防総省と米国セキュリティベンダの間には密接なつながりがあるとされる。

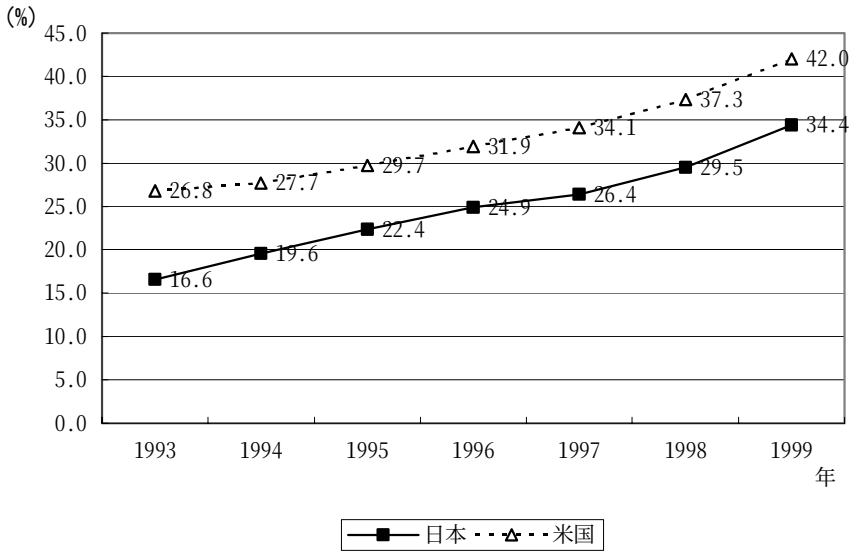
ただし、今日の情報セキュリティビジネスは、軍需ではなく、産業界の需要によって支えられている。軍需から民需への転換のきっかけとなったのは、1977 年、米国政府の標準暗号として制定された DES（Data Encryption Standard）の登場である。DES は、開発者である IBM が、NIST（National Institute of Standards and Technology）による政府機関調達用のデータ暗号規格の公募に提案し、採用された。DES は、アルゴリズムが無償公開されたことで、世界各国の研究者によって研究・検証され、その強度が高く評価されたことから、情報化・グローバル化が先行していた金融機関に採用されるようになり、事実上の世界標準暗号として産業界に普及することとなった。

②IT 投資の拡大とインターネットの飛躍的な成長

情報セキュリティがビジネスとしての形を整えてきた背景には、企業における IT 投資の拡大とインターネットの飛躍的な成長がある。

1999 年の民間企業の設備投資に占める IT 投資の割合は 34.4%と、1993 年時の 2 倍以上の割合を占める存在にまで成長した。IT 革命が先行する米国では 42.0%にまで達している。

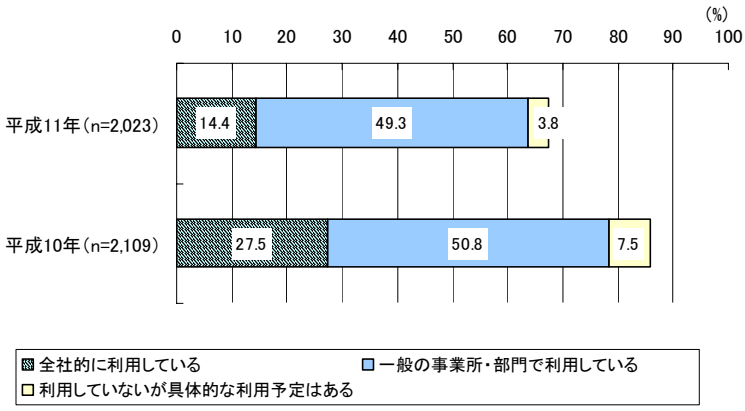
図表１－１　民間設備投資に対する情報化投資比率（財およびソフトウェア）の推移



資料：通商産業省（現経済産業省）「平成 11 年年間回顧　鉱工業生産活動分析」（2000 年 3 月）

また、郵政省（現総務省）「平成 11 年度通信利用動向調査」によると、1999 年 11 月時点の企業におけるインターネット普及率は 78.3%に及んでおり、ビジネスに欠かすことのできない重要な情報インフラとして認知されている状況が伺える。

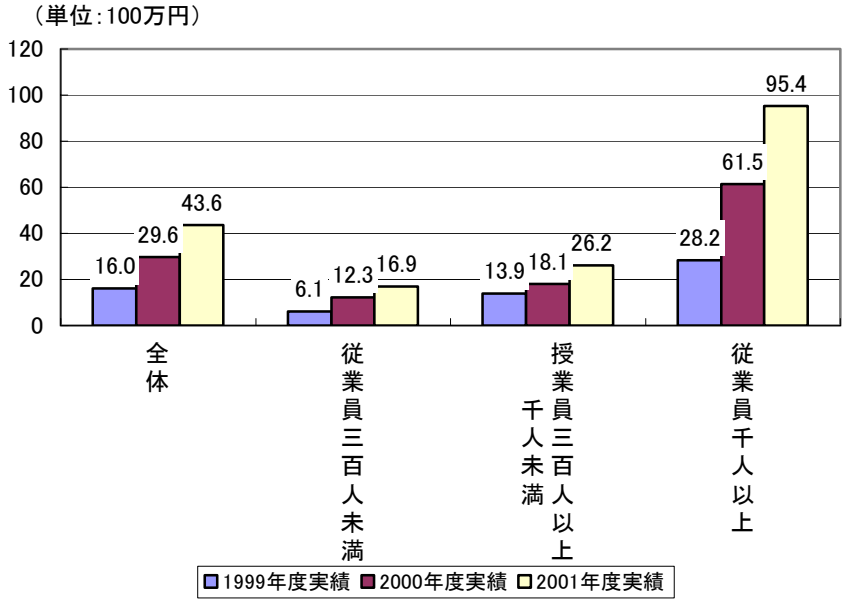
図表１－２　インターネットの利用状況



資料：郵政省（現総務省）「平成 11 年度通信利用動向調査」（2000 年４月）

さらに、企業におけるインターネット・ビジネス関連予算（企業や消費者を対象に、インターネットを使って商品の受発注や情報提供、顧客サポートなどを行う予算）も、全体の平均が 2000 年度の 2,960 万円から 2001 年度には 4,360 万円へ、従業員千人以上の企業では2000年度の6,150万円から2001年度には9,540万円に達する見込みである。

図表１－３　インターネット・ビジネス関連の平均情報化投資額



資料：日経コンピュータ、日経マーケット・アクセス
「2000 年度 企業システムとインターネットに関する調査」（2000 年 5 月）

③ネットワークの脆弱性と脅威の顕在化

しかし、インターネットの急速な普及とそれに伴う IT リスクの拡大にもかかわらず、わが国の情報セキュリティビジネスは、潜在的な需要規模への期待と、一向に立ち上がらない市場の現状とのギャップに長い間苦しんでいた。1992 年度に行われた情報システムに関する意識調査（(社）日本電子機械工業会（現：(社）電子情報技術産業協会)）によると、情報システムに係る４つの脅威（災害、故障、過失、故意）に対する重要度意識で、「故意」（情報に関する盗聴、破壊、改ざん、なりすまし等の行為）に対する評価が、欧米企業では１～２位であるのに対し日本企業では４位と、日本企業の「故意」に対する危機意識の低さが明らかにされた。

図表１－４　４つの脅威に対する重要度意識

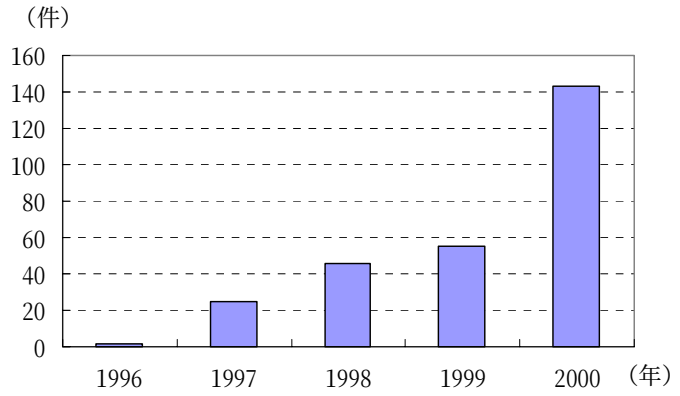
	災　害	故　障	過　失	故　意
日　本	3	1	2	4
北　米	4	2	3	1
欧　州	4	1	3	2
豪　州	3	1	4	2

資料：(社）日本電子機械工業会（現：(社）電子情報技術産業協会）調査

こうした状況が急変したのは、2000 年１月～２月の中央省庁のホームページに対する連続不正アクセス事件と、同じく 2000 年２月の米有力サイトに対するサービス不能攻撃（DDoS：Distributed Denial of Service）の発生がきっかけである。相次ぐ不正アクセス事件とその社会的影響の大きさに、ユーザ企業は、2000 年問題を大過なく終えることができたのも束の間、にわかに警戒心を強めることとなった。

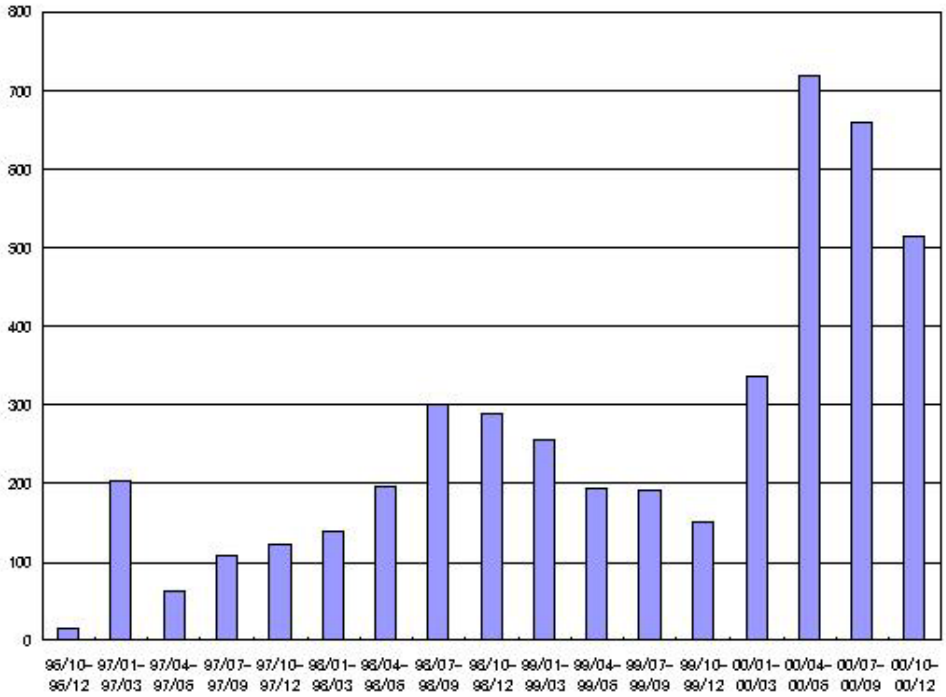
また、これらの事件をきっかけとして、不正アクセスそのものも増加傾向を示している。2000 年のコンピュータ不正アクセスに関する届出は、IPA セキュリティセンターで 143 件（前年比 260%)、コンピュータ緊急対応センター（JPCERT/CC）で 2,232 件（同 283%）と、どちらも前年の３倍近いペースで急増した。

図表１－５　IPA が受け付けた不正アクセス被害届出件数の推移



資料：IPA セキュリティセンター　http://www.ipa.go.jp/SECURITY/index-j.html

図表１－６　JPCERT/CC が受け付けた不正アクセス報告件数の推移



資料：JPCERT/CC　http://www.jpcert.or.jp/stat/reports.html

このような脅威の増加要因として、情報通信利用に係るセキュリティ保護に関する検討会「情報通信利用に係るセキュリティ保護に関する検討会報告書」（2000 年 11 月）では以下の項目を挙げている。

「○インターネットの爆発的普及により重要インフラを始め、各種の EC サイト等攻撃対象が増加した

○企業で利用するネットワークシステムにおいて、オープンネットワークの利用が増加しており、企業における顧客情報や機密情報等の利用価値の高い情報がネットワーク上で流通するようになった

○ネットワークの匿名性によって犯罪因子が誘発されている

○ハッカー同志の情報交換や組織化が容易になった

○IT の爆発的普及に対してシステム技術者が不足しており、十分なセキュリティ保護が施されていないシステムが増加した 等」

政府は、2000 年１月に、「ハッカー対策等の基盤整備に係る行動計画」を発表、各省庁でセキュリティポリシーの策定に着手した。さらに、電子政府の実現に向け、政府認証基盤（GPKI）の構築や、全省庁の局長級からなる「情報セキュリティ対策推進会議」と民間有識者からなる「情報セキュリティ部会」の設置、さらに、内閣官房安全保障・危機管理室への「情報セキュリティ対策推進室」の設置等が進められた。なお、米国政府は、「国家情報システム防衛計画」の 2001 年度予算として、約 20 億ドルが要求されている。

（2）情報セキュリティの定義

IPA セキュリティセンター「情報セキュリティの現状　2000 年版」（2001 年 2 月）によると、情報セキュリティは以下のように定義される。

「『情報セキュリティは、組織における情報およびシステムを、組織の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

『システムが、必要な場合に、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、システムの利用を決められた方法により制御できる性質を示す。スコープとする脅威は、不正アクセス、誤作動、コンピュータウィルス、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関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。スコープとする脅威は、不正アクセス、誤作動、運用に係わる問題である。

機密性

『情報が、権限のあるものが権限のある際に、権限のある方式に則って公開されること』

情報が、組織により決められた規定通りに公開される性質を示している。スコープとする脅威は、機密情報漏洩、著作権侵害、プライバシー侵害である。

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、個人のプライバシー情報の流出による信用失墜などが該当する。」

（http://www.ipa.go.jp/security/fy12/sec2000/index.html）

つまり、情報セキュリティは情報およびシステムの存在が前提であり、人間が情報やシステムを利用する際の基本的なインフラの一つと位置づけられる。情報セキュリティは不可欠な機能であるが、主・従の「主」ではなく、あくまで守るべき情報やシステムがあっての情報セキュリティである。言い換えると、情報セキュリティだけが突出して独自の進化・発展をとげる社会は、すなわち「犯罪多発社会」であり、情報セキュリティへ闇雲にお金をかけなければならない社会を意味する。そのような社会は望ましいものとはいえないであろう。

本調査研究で対象とする情報セキュリティビジネスの範囲は、上記の性質を実現するための製品・サービスを扱うビジネスとする。

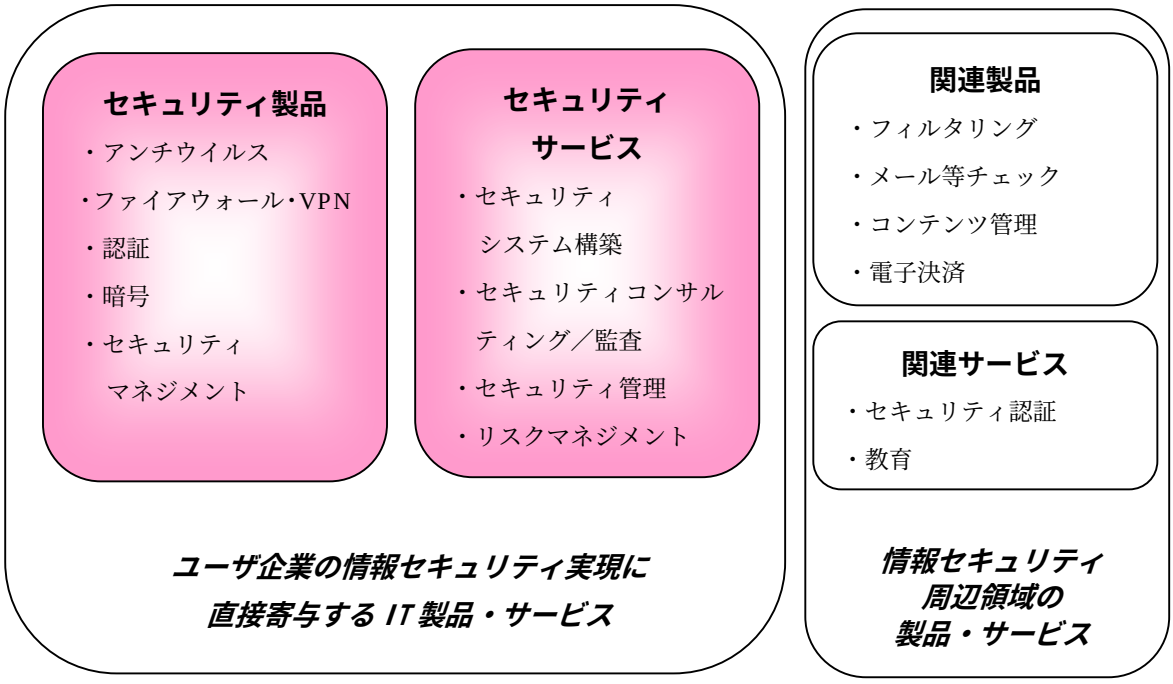
（３）情報セキュリティビジネスの枠組み

①基本的な考え方

市場推計を伴うビジネス領域の定義として、ここでは製品およびサービスを明示する手法を採る。本調査研究において対象とする情報セキュリティビジネスの範囲は、(2)で示した情報セキュリティの性質の実現に直接的に寄与する IT 製品・サービスとし、周辺領域の製品・サービス（例：フィルタリングソフト、教育サービス）等は含めないものとする。なお、ネットワーク保険は、ユーザ企業やサービス事業者にとってのリスクマネジメントサービスとして捉え、本調査の対象に含める。

また、セキュリティ評価認証制度については、ユーザ企業が直接利用するものではなく、現段階では未確定な点も多いことから、本調査研究の対象には含めないものとする。

図表１－７　本調査の対象範囲についての考え方



②情報セキュリティ分野の製品・サービス

①の方針に則り、本調査研究の対象とする製品・サービスは以下の通りである。

(a)アンチウイルス

コンピュータウィルスは、コンピュータシステムの OS やアプリケーションソフトに伝染し、データを改竄・破壊するプログラムであり、これを検出・駆除するソフトを対象とする。

(b)ファイアウォール・VPN

内部ネットワークと外部ネットワークの間に設置され、外部ネットワークからの不正アクセスを遮断するファイアウォールと、暗号・認証技術を駆使して、専用線やフレームリレー等の代わりにインターネットを企業ネットワークとして利用する「インターネット VPN」を実現するための製品群を対象とする。実際にはファイアウォールが VPN 機能をカバーしているケースが多く、両者の市場を分離するのは事実上困難であることから、ここでは重複を避けるため、ファイアウォールと VPN 専用機を対象とする。

(c)認証

認証製品は、ユーザ認証を行うためのしくみであり、具体的には以下の製品を対象とする。

・トークンと呼ばれるカード電卓に似たパスワード発生器を使い、表示されたパスワードを結末に入力することで、遠隔地からでも安全に LAN へログインすることができるワンタイムパスワード製品
・指紋や虹彩、声紋、筆跡などの生体情報を識別子に使用するバイオメトリクス
・本人認証や決済等に使用する IC カード
・公開鍵暗号を用いた PKI（Public Key Infrastructure）製品

(d)暗号

メールやファイルの暗号化機能を組み込んだ暗号化製品（暗号メール、暗号 Web ブラウザ、ファイル暗号化ツール等）と、暗号化機能を組み込むためのツールキットが対象となる。

(e)セキュリティマネジメント

情報セキュリティの管理運用を行うためのツールであり、具体的には以下の製品を対象とする。

・ネットワークを監視し、不正アクセスを含む異常事態の発生を警告する不正アクセス検知ソフト（IDS：Intrusion Detection System）

・不正アクセスのシミュレーションやホストの検査、ネットワークの監視を通じて、ネットワークシステムのセキュリティホールを検出するセキュリティ検査ソフト
・アプリケーションやシステムに対するユーザのアクセス制御環境を一元管理するアクセスコントロール製品

(f)セキュリティシステム構築

ファイアウォールや認証機能を組み込んだLAN構築、インターネットVPN構築、EC、インターネットEDI/CALS構築等、セキュリティ技術の適用を前提としたシステム構築サービスを対象とする。

(g)セキュリティコンサルティング／監査

セキュリティコンサルティングやセキュリティ診断、セキュリティ監査等、セキュリティ関連のコンサルティングサービスを対象とする。

(h)セキュリティ管理

ファイアウォールをはじめとするセキュリティ機能の運用代行、不正アクセス監視、認証サービス等、セキュリティの管理運用サービスを対象とする。

(i)リスクマネジメント

リスク管理に係るサービスであり、ネットワーク保険を対象とする。

図表１－８　情報セキュリティ分野の製品・サービスの構成

対象項目		概　要
製品	アンチウイルス	クライアント向けソフト、サーバ向けソフト
	ファイアウォール・VPN	VPN機能はファイアウォールに搭載されるケースが多く、不可分として市場を推計
	認証	ワンタイムパスワード、ＩＣカード、 バイオメトリクス、PKI等
	暗号	暗号化製品、暗号ライブラリ、暗号ツールキット、 電子透かし等
	セキュリティ マネジメント	IDS、セキュリティ検査、アクセスコントロール
サービス	セキュリティ システム構築	セキュリティ技術の適用を前提としたシステム構築
	セキュリティコンサルティング／監査	セキュリティ診断、セキュリティポリシー策定、 セキュリティ監査、その他セキュリティコンサルティング
	セキュリティ管理	セキュリティ運用代行、不正アクセス監視、認証サービス
	リスクマネジメント	ネットワーク保険

１．２　情報セキュリティビジネスの産業構造

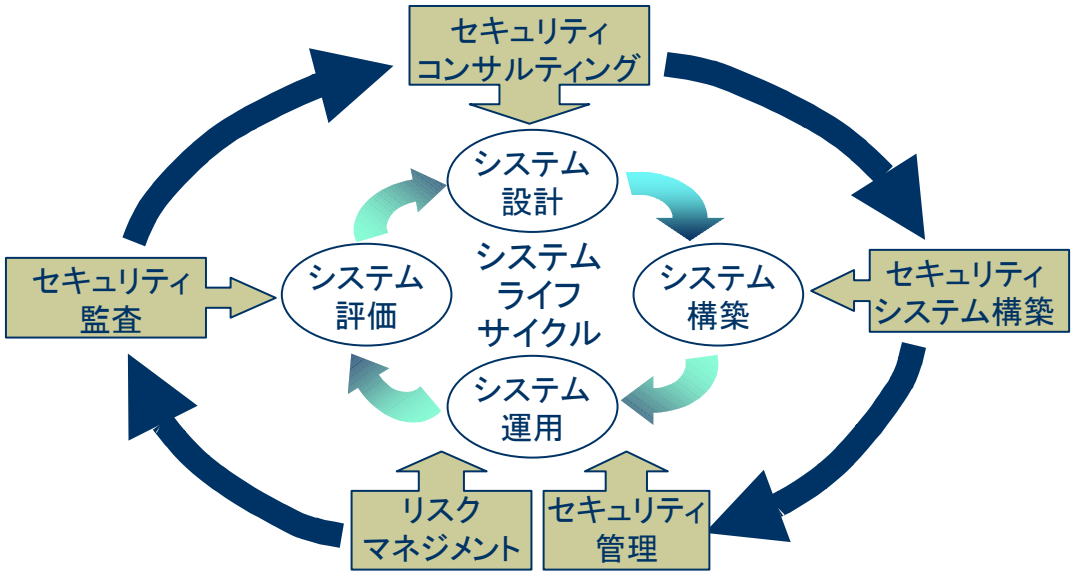
ここでは、情報セキュリティビジネスの産業構造についてまとめる。

（１）情報セキュリティビジネスの特徴

情報セキュリティビジネスは、一般に、情報システムのライフサイクルに沿って展開される（図表１－９）。このような展開に沿って、セキュリティ機能が展開していくことを、セキュリティライフサイクルと呼ぶこともある。

従って、情報セキュリティビジネスの事業領域は、情報およびシステムの普及や応用の広がりに連動して拡大する。現在の情報セキュリティビジネスの活況は、情報化社会がセキュリティ機能を見落としていたことに気づき、本来あるべき水準まで引き上げ、バランスをとろうとする動きと解釈することもできる。

図表１－９　情報システムのライフサイクルと情報セキュリティのライフサイクル



（2）セキュリティベンダの構成

②で示した情報セキュリティビジネスを展開するセキュリティベンダを分類すると、以下の業種で構成される。ただし、各業種に属する企業がすべてセキュリティベンダであるという意味ではない。

(a)ソフトメーカ
(b)システムベンダ
(c)コンサルティング／会計監査企業
(d)システムインテグレータ
(e)システム販売会社
(f)通信事業者
(g)認証サービス会社
(h)損害保険会社

図表１－10　セキュリティベンダの構成

セキュリティベンダ	製品ビジネス	サービスビジネス
ソフトメーカ	セキュリティ製品の供給（間接販売／直接販売）	セキュリティソフトやデータのASP、セキュリティ管理サービスの提供
システムベンダ		セキュリティサービス全般の提供
コンサルティング／会計監査企業	―	セキュリティコンサルティング／監査の提供
システムインテグレータ	（システム構築を通したセキュリティ製品の供給）	セキュリティシステム構築を中心としたサービス全般の提供
システム販売会社	（システム構築を通したセキュリティ製品の販売）	セキュリティシステム構築を中心としたサービス全般の提供
通信事業者	（システム構築を通したセキュリティ製品の供給）	セキュリティ管理を中心としたサービス全般の提供
認証サービス会社	（認証サービスに関連する製品の販売）	セキュリティ管理（認証サービス）を中心としたコンサルティング、システム構築の支援
損害保険会社	―	リスクマネジメントの提供

（3）セキュリティベンダから見た産業構造

セキュリティベンダの観点から見たセキュリティビジネスの産業構造の特徴について以下にまとめる。

・セキュリティソフトメーカは欧米やイスラエルの企業が多いため、ユーザ企業に製品を直接販売するケースは少なく、システムベンダに対する技術提供や製品の OEM 提供、また、システムベンダやシステムインテグレータ、システム販売会社、通信事業者を介した間接販売に依存するケースが多い。

・システムベンダやシステムインテグレータは、セキュリティソフトメーカの製品や技術の供給を受け、ユーザ企業に必要なセキュリティ製品の供給やセキュリティシステムの構築を行う。さらに、それらの事業に軸足を置いた形で、セキュリティコンサルティングや監査、セキュリティ管理などのサービスにも展開している。顧客は大手企業が中心。

・コンサルティング／会計監査企業は、セキュリティ技術だけでなく、ユーザ企業の経営・組織的観点から見たセキュリティポリシーや緊急対応マニュアルの策定等の部分のセキュリティ管理サービスに強みがある。

・システム販売会社は、システムベンダやシステムインテグレータと同様に、セキュリティソフトメーカやシステムベンダの製品の供給を受け、ユーザ企業のニーズに合わせて提供する。さらに、その延長として、セキュリティシステムの構築を行う。さらに、それらの事業に軸足を置いた形で、セキュリティコンサルティングや監査、セキュリティ管理などのサービスにも展開している。中堅・中小企業市場に強い。

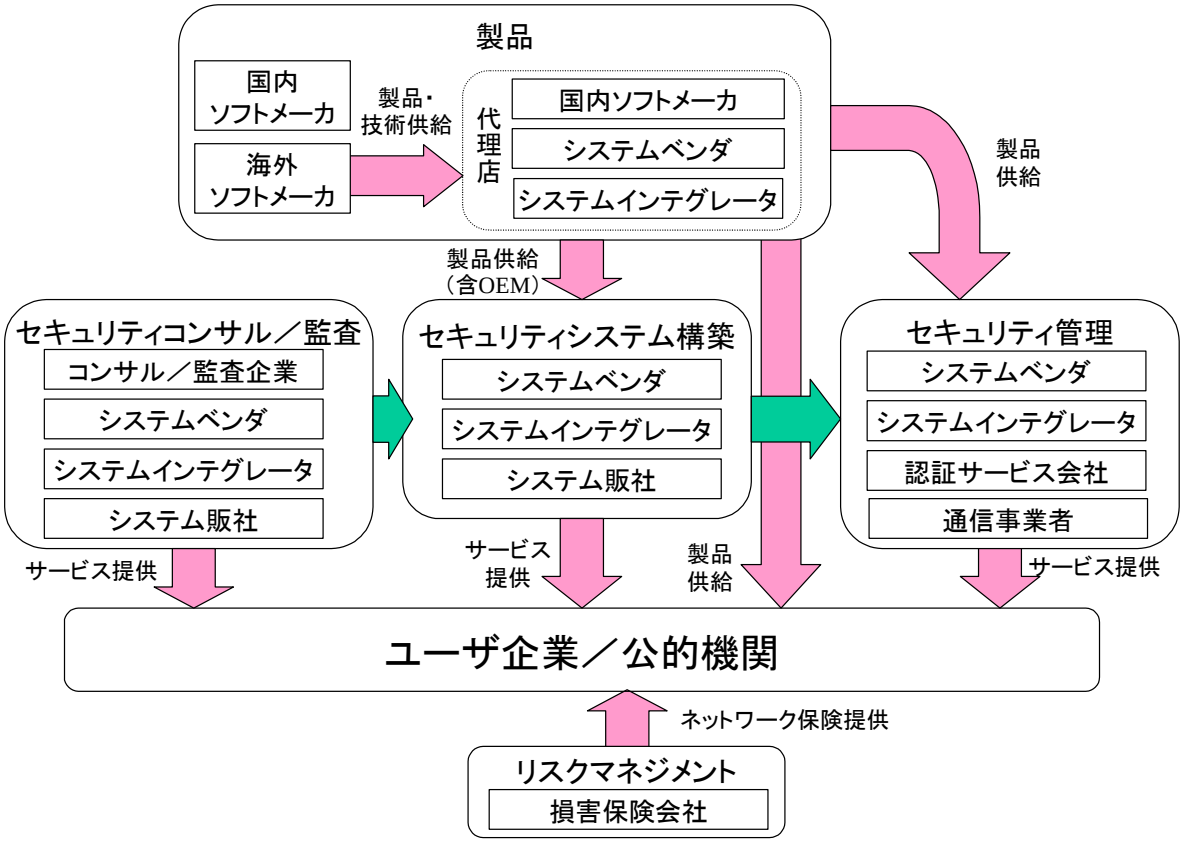
・通信事業者は、ISP サービスのユーザ企業を中心に、付加価値サービスとしてファイアウォールや IDS の運用代行サービス等を提供している。

・損害保険会社は、システムダウンや不正アクセスを想定したネットワーク保険のメニューを開発、提供している。ユーザ企業向けのサービスと、ユーザに対するサービス事業者向けのサービスがある。保険契約時の評価についてコンサルティング／会計監査企業と連携するケースがある。

・認証サービス会社は、認証サービスの提供を中心に、認証局に係わる製品の販売やコンサルティング・システム構築等のサービスを提供している。

これらの特徴を踏まえ、情報セキュリティビジネスの産業構造のイメージを図表１－10 に示す。

図表１－11　情報セキュリティビジネスの産業構造

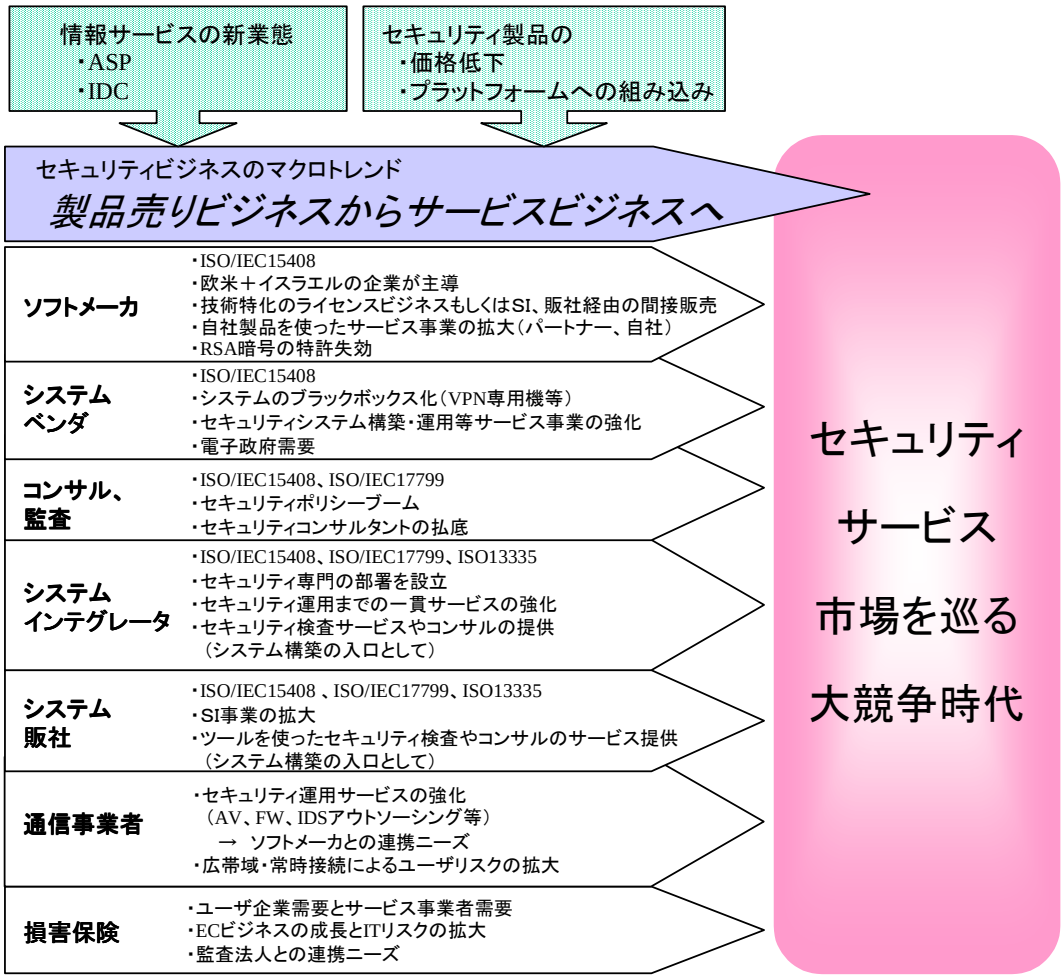


１．３　セキュリティベンダの動向

ここでは、日本のセキュリティ情報セキュリティビジネスに取り組む事業者の動向を業種別に整理・分析する。

ASP や IDC などネットワークを用いた情報サービスにおける新業態の登場、そしてセキュリティ製品の価格低下やプラットフォームへの組み込みが進む中、セキュリティビジネスは、製品をただ売るだけのビジネスから、サービスという付加価値を提供するビジネスへ移行しつつある。各セキュリティベンダも、それぞれが持つ強みを活かし続々とセキュリティビジネスに参入しており、今後セキュリティサービス市場においては大競争時代に突入すると予想される。この状況を図表１－12 にまとめる。

図表１－12　セキュリティサービス市場をめぐる大競争時代



以下、各セキュリティベンダにおけるセキュリティビジネスへの取り組みの状況とその特徴について整理、分析を行う。

（1）ソフトウェアメーカ

1999 年の Happy99 や Merissa、2000 年の Loveletter ウイルス等、日本におけるコンピュータウイルスに対する警戒心やセキュリティに対する意識は急速に高まっている。そのため、海外のセキュリティソフトウェア／ツールベンダも積極的に日本市場に参入しており、多くの事業者が日本法人を設立している。

① 強み

売上の大半を占めるアンチウイルスソフトウェアを中心に、官公庁・大企業や中小企業から、個人・家庭ユーザまで、幅広い層に対してセキュアな製品を提供することで、社会全体のセキュリティレベルを向上させることに寄与している。

② 弱み

主に海外本社で開発されたソフトウェアやツールについて、日本市場向けにローカライズし国内向けに販売するという代理店的役割が主であり、日本独自の技術やノウハウを蓄積しにくい。

③ 今後の事業戦略

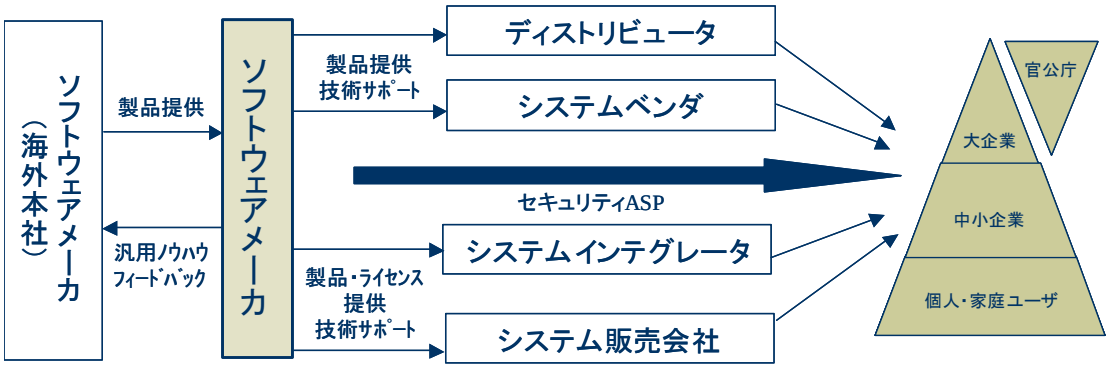
アンチウイルスソフトウェアは、大企業向けクライアント版の普及が一段落した状態であるため、今後は、サーバ版の絞り込みや中小企業市場の開拓に注力するとみられる。また、アンチウイルスとファイアウォールを融合した製品など、機能を統合した製品の開発にも注力するメーカや、ネットワーク機器ベンダなどに要素技術をライセンス提供するビジネスに注力するメーカもある。

大手セキュリティソフトウェアメーカでは、単なる製品の開発・販売に留まらず、製品を軸とした総合的なサービスを提供する事業へ徐々にシフトすることを目標としている。今後は製品導入コンサルティングや運用サポート・教育などに注力し、トータルなセキュリティソリューションを提供する役割に変化することになろう。

また、大手ソフトウェアメーカと大手コンピュータメーカやシステムインテグレータとの提携のように、自社ツールの提供のみならず、自社ツールを用いて独自のサービスの提供を行うパートナーとして他事業者と提携する形が増えるであろう。

一方、2001 年には、エンドユーザに対し、ウイルス対策やセキュリティチェックをネットワークを介して直接行う ASP 型のサービスを提供するソフトウェアメーカも現れた。既に米国においては多くの契約実績があるサービス形態だが、日本においても同様のサービスが普及するかどうか、今後注目されるところである。

図表１－13　ソフトウェアメーカのセキュリティビジネス形態



（2）システムベンダ

システムベンダは、これまでの事業の軸であったシステムインテグレーションにおいてセキュリティ対策のニーズが高まっていることから、セキュリティビジネスにも積極的に対応している。現在では、官公庁・大企業を中心に、セキュアなシステム構築のみならず、コンサルティング、監視サービスも含めた総合的なサービスを提供している。特に、コンサルティングには各社とも注力しており、リスク分析やポリシー策定などのサービスメニューを充実させている。サービス内容としては、ユーザ企業の関心が非常に高い ISO/IEC15408 や ISO/IEC17799 などの国際標準に準拠したサービスを特徴としている。

① 強み

コンサルティングからシステム構築まで、トータルセキュリティ実現のための技術・ノウハウと人材を擁することが強みである。特に大手システムベンダでは、自社グループの販売ディーラ、ソフトウェア開発会社、SE 会社、ネットワークサービス事業者などと連携することで、製品開発や営業面で役割を分担しながら一貫したサービスを提供することが可能である。

② 弱み

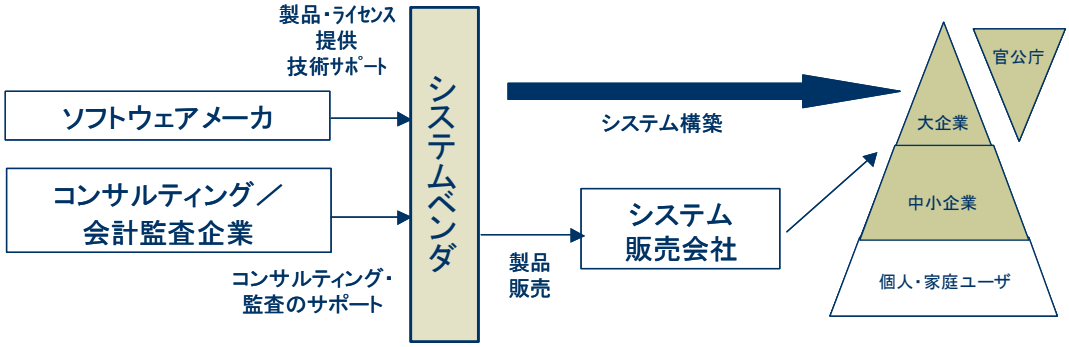
一事業者が提供するサービスが総合的で多岐に渡るため、各社の個性がユーザ企業からは見えにくいという面もある。

③ 今後の事業戦略

グループ企業などと積極的に連携を進めるベンダが多く、サービス提供範囲の拡大に伴い、コンサルティング企業や監査法人と提携する動きや、ベンダ同士の提携によって、セキュリティ対策のレベルを上げようとする動きがある。

また、各事業者ともコンサルティングスキルを持った人員の育成／補強には特に力を入れているが、セキュリティに関して高度な知識を持つ技術者を社内で認定する制度を定め、技術者やコンサルタントのスキル向上を目指すベンダもある。

図表１－14　システムベンダのセキュリティビジネス形態



（3）コンサルティング／会計監査企業

ユーザ企業におけるセキュリティに対する意識が高まるにつれて、セキュリティ対策はシステム的観点からのコンサルティングのみでは不十分であり、経営的観点からのコンサルティングが重要であるという認識が広まってきた。そのため、システムのセキュリティ対策を依頼されたシステムベンダやシステムインテグレータなどの事業者が経営的なコンサルティングを必要とする際に、コンサルティング／会計監査企業が持つコンサルティングのノウハウやスキルが非常に期待されており、提携や協業によってコンサルティングを行うことが多くなっている。

① 強み

もともと経営的観点からのコンサルティングサービスが事業の中心であったため、コンサルティングに関する独自手法を持ち、ノウハウに長けている。

② 弱み

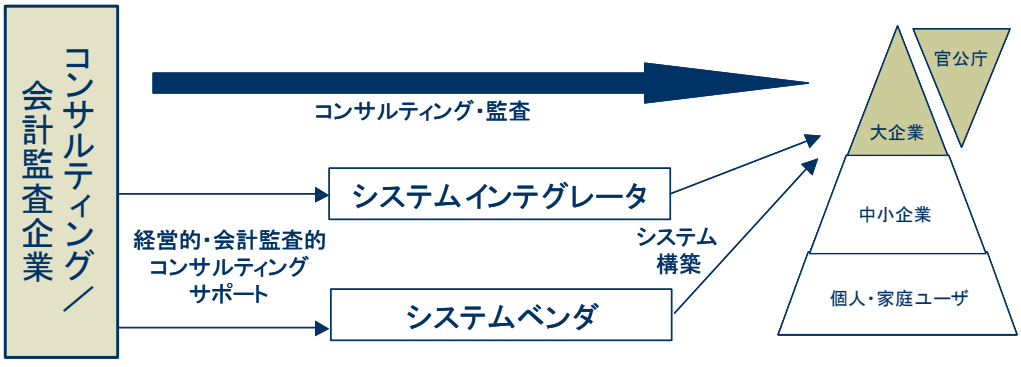
投資対効果の見えにくいセキュリティ分野において、コンサルティングはコスト的な負担感が大きいことから、主な顧客層は大企業や官公庁などに限られる。

③ 今後の事業展開

最近は、セキュリティ専門のグループ会社を設立したり、セキュリティ専門の部署を立ち上げたりなど、セキュリティ事業を独立化、専門化させる動きが強まっている。

現在はポリシー策定・支援サービスがメインであるが、コンサルティングに関連して、疑似ハッキング、ツールを利用した検査・監査するサービスを行うなど、サービスの範囲を拡大する動きもある。

図表１－15　コンサルティング／会計監査企業のセキュリティビジネス形態



（4）システムインテグレータ

システムインテグレータは、単一のセキュリティ製品の販売のみではなく、複数の有力セキュリティベンダと提携することで、様々なツールを組み合わせた顧客ニーズに合ったソリューションを提供している。システムベンダと同様、セキュリティ関連のメニューを拡充させており、コンサルティングから構築、運用そして監視サービスまで含めた総合的なサービスの提供を、主に大企業・官公庁向けに行っている。

① 強み

中立的な立場から、それぞれの分野で最も優れた様々なベンダの製品とツールを用いてシステム構築できることが強みである。また、メニューとしてもコンサルティングからシステム構築、運用・管理まで、トータルセキュリティを実現することが可能である。

② 弱み

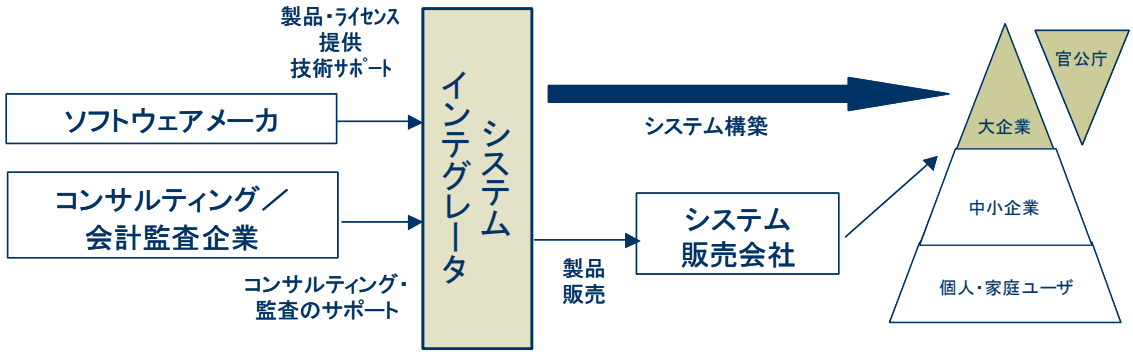
この分野での競争は激しいが、トータルソリューションが主なサービスであるため、他社との差別化をアピールしにくいのが弱みである。

③ 今後の事業戦略

他事業者はもちろん、システムインテグレータ同士で提携関係を結び、協業を行うケースがみられる。

また、システムベンダと同様、各事業者ともコンサルティングには力を入れているが、他事業者との差別化を図るために、特に様々な製品に関する知識やシステム構築に関するノウハウを強みとした、システム面でのコンサルティングに注力する動きもある。

図表１－16　システムインテグレータのセキュリティビジネス形態



（５）システム販売会社

システム販売会社は、ソフトウェアメーカやシステムベンダ、システムインテグレータ等から製品や技術サポートを受け、製品販売やシステムインテグレーションの提供を中心にセキュリティビジネスに取り組んでいる。顧客の様々なニーズに対応するため、他事業者との提携を積極的に進めて製品ラインナップを充実させたり、セキュリティサイクルのそれぞれのフェーズに対応したメニューを準備したりしている。

また、企業のバックグランドによって、独自の分野で強みを発揮した事業を展開する事業者もある。例えば、ソフトウェアベンダと提携してエンドユーザ向けの販売に注力したり、ツールを利用した安価で手軽なセキュリティポリシー策定メニューを揃えたり、国内独占販売権を有するセキュリティ関連書籍を中心とした販売サービスを行ったりなど、事業者によって様々な個性がみられる。

① 強み

強力な営業力により、中小企業を中心に多くの顧客を抱え持ち、顧客ニーズを捉えたきめ細かな対応を強みとしている。

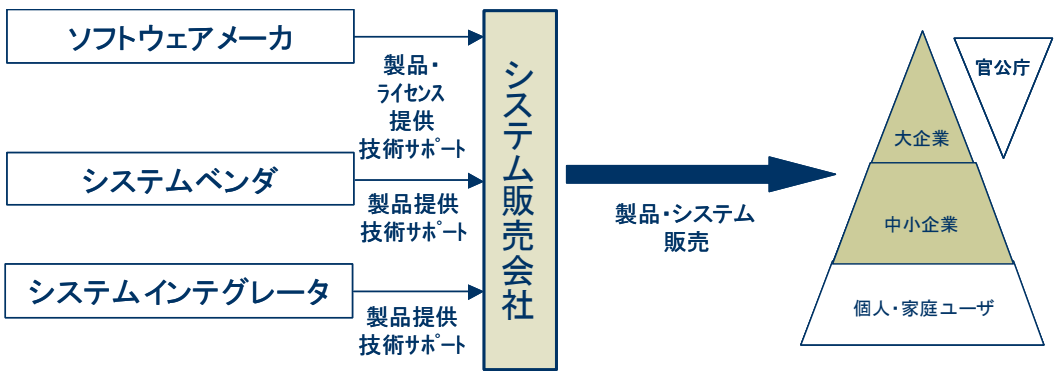
② 弱み

大規模なシステム構築やトータルなソリューション展開をするための技術力や経験が充分でないケースも見られる。

③ 今後の事業戦略

中小企業中心の現在の顧客層を大企業にまで拡大すべく、従来の販売中心のビジネスから付加価値の高い総合的なサービスの提供を目指している。一方、これまで蓄積してきたノウハウを利用して、中小企業向け低価格オールインワンサービスの提供を進めていく。

図表１－17　システム販売会社のセキュリティビジネス形態



（6）通信事業者

ISP を含む通信事業者は、接続サービスを提供する以上、安全な接続環境をユーザに提供する必要がある。このような世間から求められる責任を果たすと同時に、ユーザのセキュリティ意識を啓発するため、各事業者ともセキュリティサービスには注力している。また、事業者側がセキュアな接続環境を提供することによって、中小企業や個人など、自己によるセキュリティ対策が充分でない層へのサポートを期待されている面もある。

主なサービスとしては、官公庁や大企業向けのインターネット VPN サービスや、閉域 IP 網を利用する IP-VAN サービス、ファイアウォール運用代行サービス、ウイルス監視、不正アクセス監視など、接続サービスの提供に附随した形でのセキュリティサービスが挙げられる。

① 強み

ユーザにとって必要不可欠な、ネットワークという最も重要なインフラ部分でのセキュリティサービスを提供することが可能であるため、常にニーズが存在する。

② 弱み

ネットワークサービス提供と合わせたセキュリティサービスについては、付加価値サービスとして対価を取りにくいという性質があるため、特に個人・家庭ユーザなどセキュリティデバイド層においては、セキュリティビジネスそのもので大きな収益を挙げにくい。

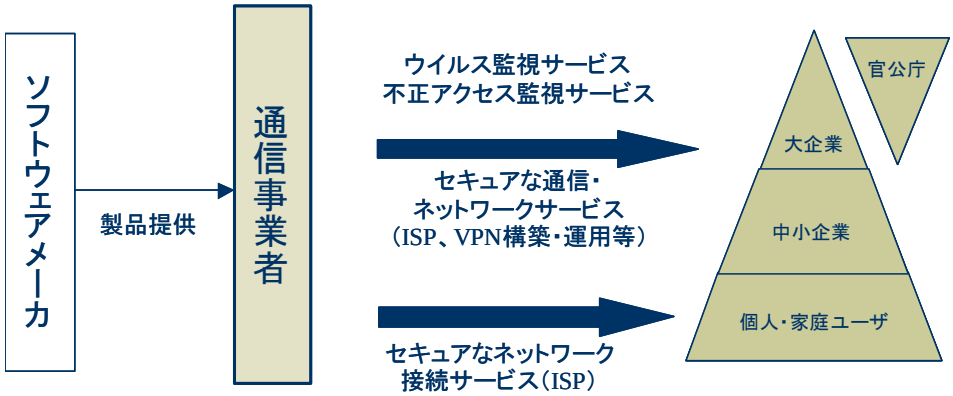
③ 今後の事業戦略

最近では、従来のハイエンド向けセキュリティサービスのみならず、月々の価格が比較的安いローエンド向けのニーズも高まっており、そういったニーズに応えたサービスの提供にも注力していくものとみられる。また、ネットワークサービスの提供のみならず、運用管理までを含めたトータルサービスの提供を開始する動きもある。

さらには、EC の市場拡大に伴い、セキュリティを強化したネットワークインフラの提供のほか、PKI、IDS などのセキュリティサービスや、アウトソーシング、運用サービス、インテグレーションまで事業の拡大を行う事業者もある。

個人・家庭ユーザ向けサービスでは、大手 ISP によって、e-mail に潜むウイルスを監視・駆除するサービスが始まっており、一般ユーザ向けのセキュリティ対策として、今後の普及とサービスの拡充が期待されている。

図表１－18　通信事業者のセキュリティビジネス形態



（7）損害保険会社

ネットワーク保険サービスが本格的に導入されたのは 1998 年と最近である。インターネットの普及とセキュリティ意識の高まりがネットワーク保険へのニーズを増大させたのも当然だが、同年 1 月に実施された企業保険分野の自由化によって、保険会社が企業分野に関する保険商品を自由に設計できるようになった背景もある。当初はカスタムメイド対応が多かったが、現在は各事業者ともメニューの体系化を進めており、ネットワークを用いてビジネスを行う事業者向け保険および一般企業向けの保険とが主な商品となっている。

損害保険会社はコンサルティング企業と協力するケースが多いが、損害保険会社と協力したコンサルティング企業が、保険加入の際のリスク分析・評価を代行したり、コンサルティングを希望したユーザに対しトータルなセキュリティプランの一環として保険を紹介したりする、という協業体制になっている。

① 強み

完全なセキュリティを達成することは本質的に不可能であるため、ユーザにとっては、ある程度のセキュリティ対策の後は保険を利用するというニーズが高まると予想されるが、その際に、保険サービスを提供できるのは損害保険会社だけであるというのは大きなメリットである。

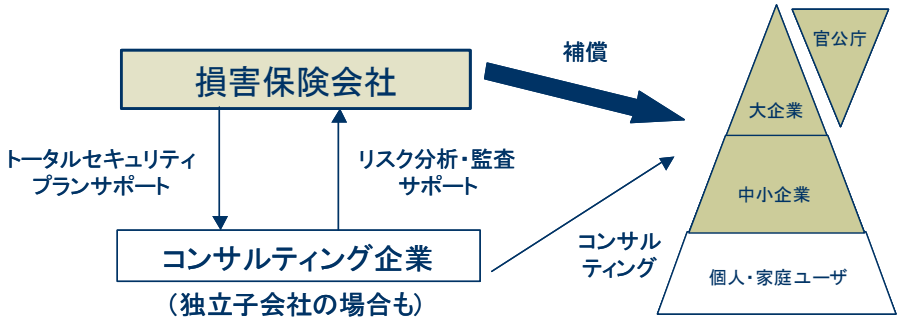
② 弱み

市場が立ち上がって間もないため、リスク評価の方法や掛け金の設定など、未だノウハウが蓄積していないのが現状である。また、保険市場全体からみたネットワーク保険市場は極小さいため、損害保険会社としては今は競争より認知度の向上に努める段階と見ている。

③ 今後の事業戦略

損害保険会社は、ユーザ企業がシステム的・経営マネジメント的に適切なセキュリティ対策を行った上でのカバーとして保険を用意するという立場でセキュリティビジネスに取り組んでいる。今後は企業活動におけるネットワークへの依存がさらに進み、個人情報保護の意識も高まることが予想されるが、損害保険会社としては、企業や官公庁などのセキュリティに対するニーズの高まりなど、市場動向を見ながら順次対応を進めていくとみられる。

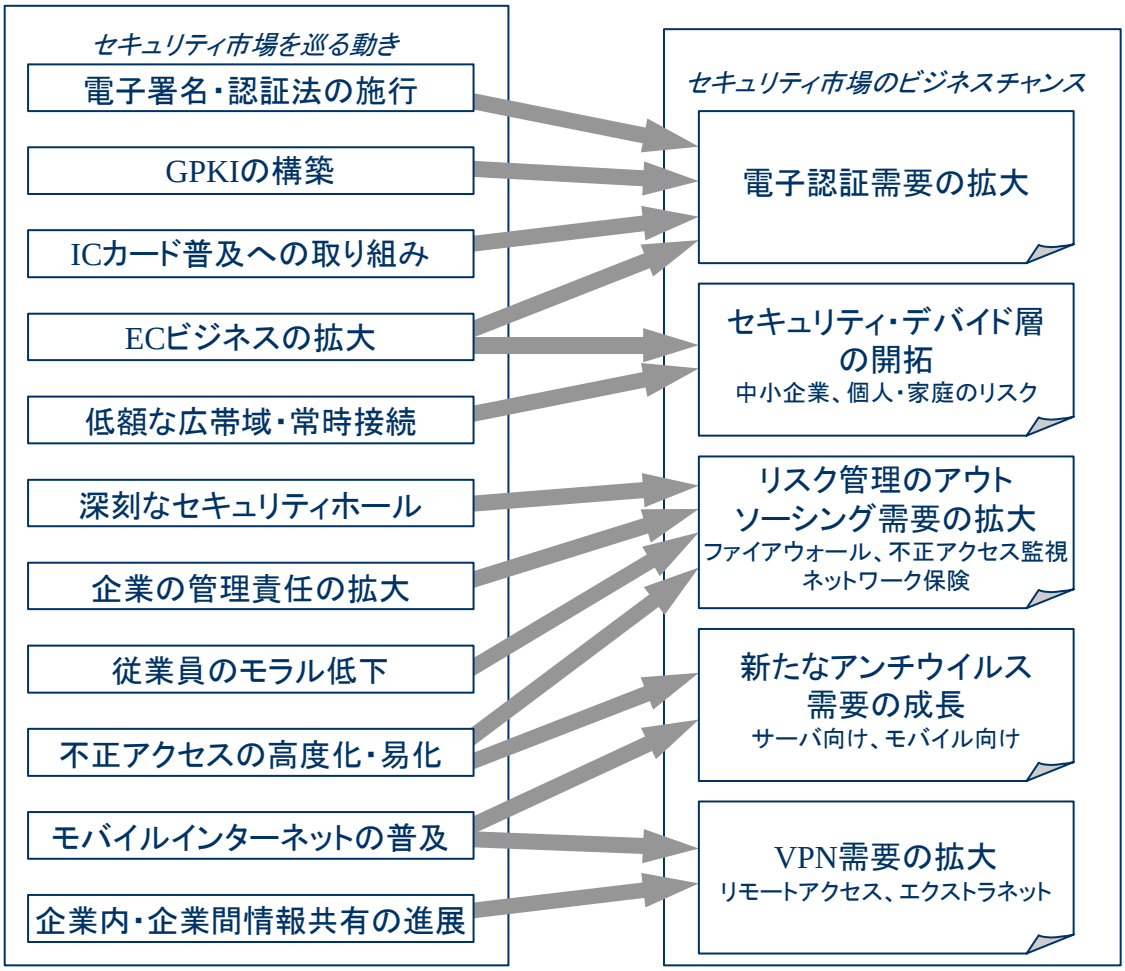
図表１－19　損害保険会社のセキュリティビジネス形態



（８）セキュリティ市場のビジネスチャンス

情報システムを巡る様々な動きは、セキュリティ市場に新たなビジネスチャンスをもたらす。図表１－20 に、セキュリティ市場を巡る動きとそれらによって導かれるセキュリティ市場のビジネスチャンスを示す。

図表１－20　セキュリティ市場を巡る動きとビジネスチャンス



- 電子認証は、「電子署名・認証法」の施行や GPKI の構築などの制度改革、また IC カードの普及や EC ビジネスの拡大等によって利用の必然性が高まり、需要が本格的に拡大する可能性がある。
- EC ビジネスの拡大や低額な広帯域・常時接続サービスの登場によって、中小企業や個人・家庭といった、新しいユーザ層が増える。必然的に、そのような層を対象としたビジネスチャンスが想定される。
- ユーザ企業の情報システム部門において、日常業務と並行して、日々発見されるセキュリティホールや高度化かつ易化する不正アクセスに対応していくことは非常に負担の

大きい作業である。さらに、個人情報保護基本法など、企業が管理責任を問われる情報の範囲は広く、従業員のモラルの低下によって個人情報が漏洩された場合など企業は重大なリスクを負いかねない。このように、セキュリティ管理は大規模化・複雑化の一途を辿っており、今後そのような管理運用をアウトソーシングする需要が高まると予想される。

- モバイルインターネットの普及とともに、モバイル機器に対する脅威もまた顕在化しつつある。既に PDA に対するウイルスが出現しており、Java 対応携帯電話についても危険性が指摘されている。従って、今後、モバイル機器を対象としたアンチウイルスのビジネスが成長する可能性がある。
- モバイルユーザの増加や企業内・企業間の情報共有の進展によって、リモートアクセスやエクストラネットをセキュアに実現する VPN の需要が顕在化する可能性がある。

第　2　章

情報セキュリティビジネスの市場動向

ここでは、世界の情報セキュリティ市場をリードする米国の情報セキュリティ市場および日本の情報セキュリティ市場の動向について、様々な統計データを基に整理する。そして、それぞれの結果を比較・分析することによって、日本の情報セキュリティ市場の特色を明確にすると同時に、日本の情報セキュリティ市場の今後の動向を予測する。

なお、本調査報告書における「情報セキュリティ市場」とは、具体的に次の製品・サービスを対象とする。

＜製品＞

・アンチウイルス
・ファイアウォール・VPN（Virtual Private Network）
・認証
・暗号（暗号化パーソナルプロダクツ、暗号ライブラリ、暗号ツールキット）
・セキュリティマネジメント

＜サービス＞

・セキュリティシステム構築
・セキュリティコンサルティング／監査
・セキュリティ管理（セキュリティ・アドミニストレーション）
・セキュリティ保険[1]

また、資料としては、以下の報告書を参考にした。

- IDC「Information Security Software Market Forecast and Analysis,2000-2004」（2000 年 10 月）
- IDC「Information Security Services Worldwide Market Forecast and Analysis, 1999-2004」（2000 年 11 月）
- 富士キメラ総研「2000 ネットワークセキュリティビジネス調査総覧」（2000 年 8 月）

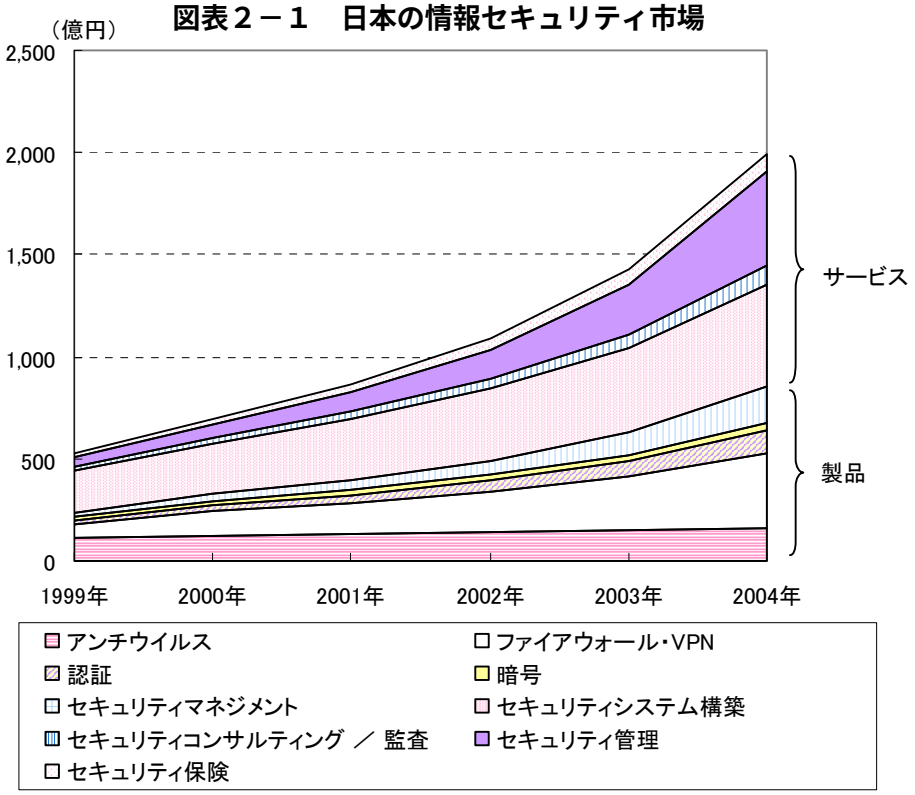
---

[1] セキュリティ保険については、日本市場のみ算出した。

２．１　日本の情報セキュリティビジネスの市場動向

1999 年の日本の情報セキュリティ市場は、製品市場が 235 億円、サービス市場が 291 億円、合計 526 億円と推計される（図表２－１）。5 年後の 2004 年にはそれぞれ市場は順調に拡大し、製品市場が 858 億円、サービス市場が 1,136 億円の合計 1,994 億円になると予測される。

図表２－１　日本の情報セキュリティ市場



【日本市場（市場規模）】　（単位：億円）

市場規模	1999年	2000年	2001年	2002年	2003年	2004年
製品	235	325	395	493	633	858
アンチウイルス	113	124	133	142	151	158
ファイアウォール・VPN	67	120	151	197	261	367
認証	22	31	40	53	74	112
暗号	18	21	24	27	31	35
セキュリティマネジメント	15	29	47	74	116	186
サービス	291	367	472	594	792	1,136
セキュリティシステム構築	206	248	302	349	410	499
セキュリティコンサルティング／監査	19	26	35	48	66	92
セキュリティ管理	50	68	98	145	247	456
セキュリティ保険	16	25	37	52	69	89
全体	526	692	867	1,087	1,425	1,994

資料：前述した IDC、富士キメラ総研資料より推計

以下、個別の製品やサービスについて、市場動向を詳細に分析する。

（１）製品市場の動向

①アンチウイルスソフト

アンチウイルスソフトウェア市場は、1999 年に 113 億円であったが、2004 年には年平均 6.9%増の 158 億円に拡大すると予測される。1999 年から 2000 年にかけ、コンピュータウイルスによる被害が社会的にも大きく採り上げられたことから、アンチウイルスソフトに対する需要は確実に増加している。とはいえ、クライアント用は大企業における導入がかなり進み、コンシューマ用においても PC へのプリインストールによる普及率が高いことから、クライアント／コンシューマ市場はほぼ飽和状態とみられ、アンチウイルス市場全体は微増傾向に落ち着くとみられる。今後の需要はサーバ製品が中心となり、クライアント用におけるユーザ層の中心は、大企業から中小企業にシフトしていくと予想される。また、インターネットの普及により、ウイルスが e-mail などを介して外部から侵入するケースが増加したため、クライアントレベルではなくゲートウェイレベルでのウイルス対策も求められている。

アンチウイルスソフトのベンダは、ウイルスの研究や解析のために研究所を設立し、新たなウイルスが急に発生した際に緊急対応する体制を整備している。そのため、アンチウイルスソフトの性能については、各社製品とも大きな差がなくなりつつあり、販売チャネルの多様化や関連ツールの充実度などが差別化のポイントとなっている。

②ファイアウォール・VPN

ファイアウォール･VPN 市場は､1999 年に 67 億円であったが､2004 年には年平均 40.5%増の 367 億円と市場が大きく成長すると予測される。ファイアウォール市場は、IDC（Internet Data Center）向けのハイエンドモデルおよび中小企業等向けの低価格ハードウェア製品の需要増加が見込まれる。ソフトウェアは値崩れがみられる製品もあり、低価格のハードウェアタイプの普及に押され、普及率は上がるものの市場の成長は鈍化していくとみられる。

また、VPN 市場については、インターネットの普及とセキュリティに対するユーザ意識の高まりによって、1999 年度後半より一気に市場が拡大している。市場が立ち上がったばかりであるため、その多くは大企業や中堅企業での試験的導入に留まっているが、本格導入も徐々にみられるようになってきた。VPN 専用機は、厳重なセキュリティが必要な官公庁や学校の LAN 間接続、海外拠点と社内 LAN 間の接続、外部アクセスポイントから社内 LAN への接続などのケースに特に需要が高かった。加えて、2000 年度には国内の自動車メーカや系列部品メーカによるインターネットを用いた受発注システム JNX（Japanese Automotive network exchange）が稼働したため、VPN 専用機のニーズは急速に高まるとみられる。ただし、VPN 製品を売る際には技術／保守サポートが必須であることから、VPN 製品の市場が予測通り拡大するためには解決すべき課題も多い。

③認証

認証市場は、1999 年に 22 億円であったが、2004 年には年平均 38.5%増の 112 億円に拡大すると予測される。PKI 市場は 1998 年から 1999 年にかけて立ち上がったものの、システム導入の煩雑さや運用管理の難しさから、公開鍵インフラを用いた本人認証システムを構築するのは、一部の先進的なユーザが部分的に導入するケースに限られていた。各製品ベンダにおいても、市場形成の時期として PKI の認知度向上に努めるにすぎなかった。

今後は、金融機関の世界的な決済ネットワークである「Identrus」や電子政府／自治体構想などで PKI の導入が見込まれるため、PKI 市場は大きく伸びるとみられる。電子商取引や各種自治体における手続などにおいては、本人を証明し、電子データの正当性を保証すること必然となることから、PKI を構築してデータを送信することが一般的に行われるようになる可能性は高い。また、2001 年から 2002 年にかけて、クレジットカードの IC カード化が続々と進んでおり、こういったデジタルデバイスが普及するに従って、PKI など認証機能が附随していくことが予想される。

バイオメトリクスについては、指紋認証、サイン認証、光彩認証、声紋認証など様々な方式がある。このうち指紋認証の実用化が最も先行しているが、現在はまだ市場形成期である。

④暗号

暗号市場は、1999 年に 18 億円であったが、2004 年には年平均 14.2%増の 35 億円と、堅調に推移するものとみられる。暗号メールソフトウェアについては、1998 年に代表的な暗号方式である PGP と S/MINE の両規格に対応した暗号プラグインソフトが登場したが、これは導入が比較的容易であることから、セキュリティを重視する官公庁やその関連団体、金融機関などにおける導入が進んでいる。今後、公開鍵、デジタル署名、本人認証など、製品の利用分野が幅広くなりつつあり、それに伴って認証局（CA）や PKI などのインフラストラクチャがある程度整備されることが予想されるが、こういった環境整備によって暗号メールソフトウェアの導入・運用の手間が軽減されれば、市場は大きく成長する可能性がある。

暗号ライブラリやツールキットについては、セキュリティ製品の市場拡大に合わせて順調に市場が拡大している。暗号メールソフトウェアと同様、認証システムの普及に伴って市場は堅調に成長していくものとみられる。

⑤セキュリティマネジメント

セキュリティマネジメント市場は、1999 年に 15 億円であったが、2004 年には年平均 65.5%増の 186 億円と、非常に速いペースで市場が拡大するものと予測される。ネットワークの複雑化と技術の高度化、そしてエンドユーザ数が 1 万を超えるような大規模システム

が増えていることを背景に、セキュリティマネジメントに対するニーズは急速に高まっている。

セキュリティ検査ツールについては、企業向け製品が中心であり、各ベンダともシステムインテグレータと協力して販売チャネルの整備を進めている。市場拡大の要因として、2000 年 1 月の中央官庁の Web ハッキング事件によりユーザ企業のセキュリティに対する意識が強まったこと、ASP などネットワークを必須としたサービスが本格的に普及し始めたことが挙げられる。また、検査ツールを使用した疑似ハッキングテストは、導入の際に専門知識が必要なほか、検査ツール自体ハッキングツールとして使用される危険性があるため、セキュリティサービスベンダのアウトソーシングとしての需要も高まっている。

IDS にはネットワーク型とホスト型があり、現在はネットワーク全体を監視できるネットワーク型が市場の中心を占めている。ホスト型では、OS 上のログを監視できるため、社内で発生した不正行為も検知可能である。また、ネットワーク型とホスト型を統合した製品も登場しており、ユーザも企業からコンシューマ層に拡大していることから、今後、市場が急激に成長する可能性もある。

（2）サービス市場の動向

①セキュリティシステム構築

セキュリティシステム構築市場は、1999 年に 206 億円であったが、2004 年には年平均 19.4%増の 499 億円と、順調に成長するものとみられる。これまで、セキュリティシステム構築は、通常のシステム構築時に個別案件で対応している場合が多かったが、大手システムインテグレータを中心にセキュリティに関するソリューションをメニュー化している事業者も増えており、セキュリティに特化したシステム構築案件も多くみられるようになってきた。セキュリティシステム構築市場では、ファイアウォールの設置のみといった単純なものから、電子証明書を利用したアクセス環境の設定やバイオメトリクスでのアクセスなど、セキュリティを確保する複数の手段を組み合わせた構築案件が増加している。

今後は、ビジネスのネットワーク依存が高まり、システムにセキュリティ対策を講じることは必須になるため、市場は順調に拡大するものとみられる。

②セキュリティコンサルティング／監査

セキュリティコンサルティング市場は、1999 年に 19 億円であったが、2004 年には年平均 37.1%増の 92 億円と、大きく成長すると見込まれる。セキュリティ関連サービスを提供しているほとんどの事業者がコンサルティングサービスをメニュー化しており、最近になって、特にセキュリティホールの検査を行うサービスのニーズが高まっている。システムインテグレータは、セキュリティ検査サービスをきっかけに、コンサルティングやシステム構築に結びつけることでセキュリティ関連サービスの拡充に努めている。特に、2000 年

の中央官庁 Web サイトのハッキングなどの社会的事件を通じて、ユーザのセキュリティ意識が高まったことにより、コンサルティングサービスへのニーズが急増している。中でも、セキュリティポリシー策定を含むコンサルティングの重要性が認識されつつある。

また、セキュアなシステムを構築し安全に運営するためには、検査サービスは不可欠なものであり、セキュリティレベルを維持するためにも定期的にサービスを受けるユーザも増加するとみられる。

③セキュリティ管理

セキュリティ管理市場は、1999 年に 50 億円であったが、2004 年には年平均 55.6%増の 456 億円と、大きく成長するものと予測される。一連の中央官庁 Web サイトのハッキング事件が社会に大きく影響を与えたため、特に不正アクセス対策に対するニーズは高まっている。不正アクセス監視サービスは、侵入検知ツールの提供と合わせたサービスが一般的であるが、ユーザ企業が 24 時間 365 日体制で不正アクセス監視を行うのは事実上不可能であることから、今後不正アクセスの脅威が増大した場合は、サービスの比重がより高まっていくと予想される。

④セキュリティ保険

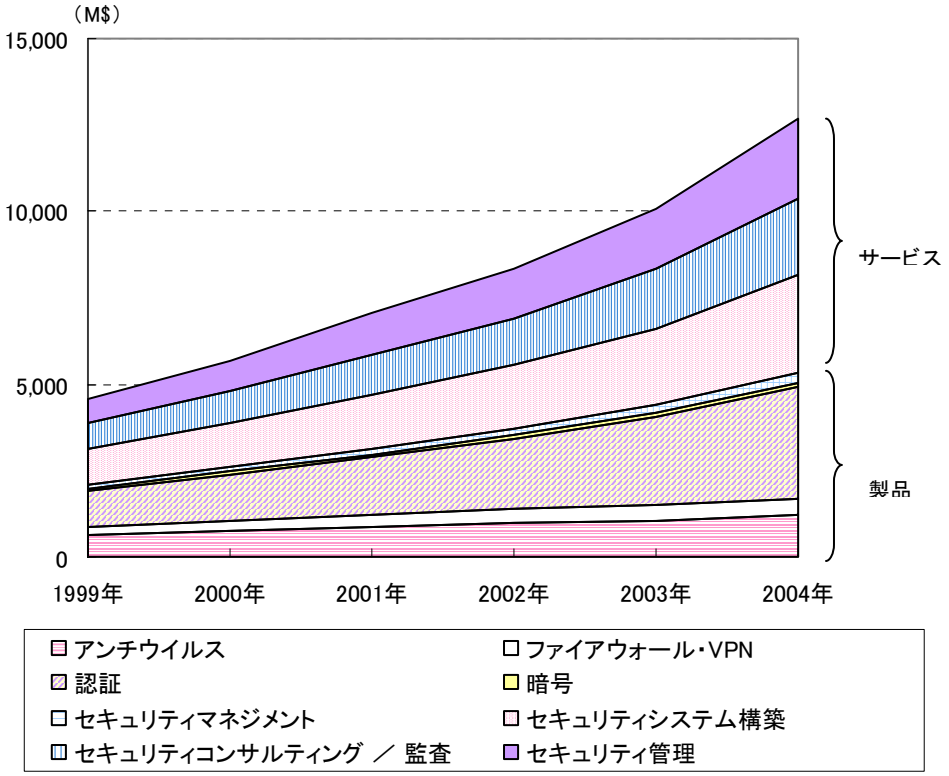
セキュリティ保険市場は、1999 年に 16 億円であったが、2004 年には年平均 40.9%増の 89 億円と、大きく成長することが予測される。コンピュータのハードウェアやメディアの破損に対する保険は従来より存在したが、1998 年前後のセキュリティに対する意識の高まりや、同年 1 月の金融規制緩和などの動きを背景とし、不正アクセスやネットワークの中断による利益損害や日常の業務を継続するための費用を補償する保険が次々と発売された。主にネットワークを用いてビジネスを行う事業者向けと、一般企業向けの商品に分かれる。

現在のユーザとしては、大規模ネットワークを持つ大企業に加えて ISP などネットワークサービス事業者が増加しているが、今後は基本的な補償を安価で提供する手軽なサービスが発売されつつあることから、小規模なネットビジネス系企業や一般企業などの加入も増加するとみられる。ただし、10 兆円産業である損保業界において、本市場はまだごく小規模であるため、損保会社が本格的に競争する状態ではなく、当面は各社とも認知度の方向に力を注ぐものと予想される。

２．２　米国の情報セキュリティビジネスの市場動向

1999 年の米国の情報セキュリティ市場は、製品市場が 2,069 百万ドル、サービス市場が 2,509 百万ドル、合計 4,578 百万ドルと推計される（図表２－２）。5 年後の 2004 年には、製品市場が 5,328 百万ドル、サービス市場が 7,351 百万ドルの合計 12,679 百万ドルになると予測される。

図表２－２　米国の情報セキュリティ市場



【米国市場（規模）】　（単位：M$）

(M$)	1999年	2000年	2001年	2002年	2003年	2004年
製品	2,069	2,601	3,144	3,715	4,421	5,328
アンチウイルス	613	746	881	972	1,065	1,189
ファイアウォール・VPN	274	309	350	393	429	481
認証	1,013	1,329	1,653	2,047	2,566	3,234
暗号	65	81	93	100	105	108
セキュリティマネジメント	104	135	167	204	255	317
サービス	2,509	3,065	3,902	4,601	5,674	7,351
セキュリティシステム構築	1,038	1,266	1,549	1,819	2,194	2,822
セキュリティコンサルティング／監査	796	959	1,168	1,372	1,724	2,217
セキュリティ管理	675	840	1,185	1,410	1,755	2,312
全体	4,578	5,666	7,046	8,316	10,095	12,679

資料：前述した IDC、富士キメラ総研資料より推計

以下、個別の製品やサービスについて、市場動向を詳細に分析する。

（1）製品市場の動向

①アンチウイルスソフト

アンチウイルスソフトウェアの 1999 年の市場規模は 613 百万ドルであった。2004 年においては年平均 14.2%増の 1,189 百万ドルと予測されている。

アンチウイルスソフトウェアの売上が大きな米国のベンダは、Network Associates、Symantec、Computer Associates の 3 社であり、IDC によると、この 3 社の売上の合計は米国ベンダによる売上の 9 割程度を占めている。

アンチウイルスソフトウェア市場が成長している主な理由は、アンチウイルスソフトウェアについて、デスクトップパソコンはもちろん、ファイルサーバ、ゲートウェイ、アプリケーションサーバなど、ネットワークを構成する機器全てに渡ってインストールされないと効果がないという認識がユーザ企業に広まってきたからである。最近はネットワークが主な感染経路となっているため、問題の発生箇所がネットワーク上で多様化しており、対策がより難しくなっている。

このような状況を反映して、アンチウイルスソフトウェアのベンダは、セキュリティ管理者やユーザの日々の運用やアップデート等における負担を軽減するため、開発の方向をより使いやすいコンソールの構築に移行させていくものとみられる。その結果、アンチウイルスソフトウェア単体の製品は徐々に姿を消し、デスクトップの制御をトータルに行うような製品に組み込まれる形になっていくと予想される。

②ファイアウォール・VPN

ファイアウォール・VPN の 1999 年の市場規模は 274 百万ドルであり、2004 年においては、年平均 11.9%増の 481 百万ドルと予測されている。

IDC の調査では、世界市場のシェアは、イスラエルの Check Point Software Technologies が約 3 割と突出しているが、これを除けば米国のファイアウォール・VPN ベンダが市場の大半をカバーしており、Raptor Systems、Trusted Information Systems、Secure Computing 等のシェアが高いとしている。多くのファイアウォールが VPN 機能を組み込んで販売されるようになり、ファイアウォール市場では、ファイアウォール機能のみの製品開発に特化したベンダはほとんどいなくなっている。

ファイアウォール・VPN 市場が急激に成長している理由は、インターネットの普及を背景としたネットワークを用いた企業間取引／リモートアクセスの増加、多様なファイアウォール・VPN への需要の高まりによる高性能・高付加価値製品の供給、ファイアウォールの信頼性向上などが挙げられ、今後も大きく市場が伸びていくことが予想される。

しかし、VPN は既存の ATM やフレームリレー、IP ネットワークの技術を拡張したもので、新規参入企業が成功するのは難しいため、現在の主要なネットワーク機器ベンダなどが今後も VPN 市場を支配するとみられる。

③認証

米国における 1999 年の認証製品市場は 1,013 百万ドルであり、2004 年には年平均 26.1%増の 3,234 百万ドルになるとみられている。

認証製品の売上は、メインフレームと UNIX 環境の強みを反映した IBM が大きく、ソフトウェアベンダでは、Computer Associates や Network Associates の売上が大きい。

IDC の調査によると、米国の認証製品市場は今後も最も大きな市場となる見込みである。認証製品市場の急激な伸びは、インターネット、イントラネット、エクストラネット等、ネットワーク技術の普及によって消費者のセキュリティに対する認識が変わったこと、そしてデジタル署名法などを背景に政府、民間とも PKI が 2001 年から本格的に普及しそうな勢いがあることが理由である。

認証市場の中でも、SSO（Single Sign On）の市場はまだ小さいが、Web ベースの新たな技術によって、市場は成長の兆しをみせている。アメリカの Gartner Group によると、認証製品市場に関しては、SSO とユーザ権限の管理製品は統合が進み、パスワードジェネレータは、クレジット機能だけでなく、個人の秘密鍵と暗号・認証・デジタル署名等の機能を持つ IC カードによって統合されていくとしている。

PKI 市場は、VeriSign、Entrust、Baltimore Technologies、Xcert 等の米国のベンダが中心となっている。PKI 技術については、当初から相互運用性や信頼性についての課題が多く、そのために普及が遅れているといった面が強かったが、これらの問題を解決するために、1999 年 12 月に RSA Security、IBM、Microsoft、Entrust 等の企業が中心となった業界団体「PKI Forum」が設立され、PKI 技術の普及啓発に努めてきた。また、デジタル署名法の成立に加え、ヘルスケア分野における HIPAA（Health Insurance Portability and Accountability Act）など、多くの業界分野でプライバシー関連の法律が新たに制定されたこともあり、最近では電子商取引に向けた PKI 技術が、試験段階から実用段階へ移行しつつあり、遠隔アクセスやセキュリティを確保したメッセージング機能、コンテンツ配信、トランザクション向けセキュリティなどで PKI 技術が使われている。また、PKI 市場全体を PKI 関連製品と認証サービスという２つのカテゴリからみると、99 年は PKI 関連製品が売上高ベースで市場全体の 2/3 を占めていたが、今後は認証サービスが伸び率で上回るという。ただし、PKI は複雑な技術で導入コストが大きいこと、さらに PKI はセキュリティのトータルソリューションではないことから、市場の成長はある程度限られたものになるとみられる。

バイオメトリクスについては、今後 10 年間で普及すると Frost & Sullivan Research の調査は述べている（2000 年 11 月）。ユーザ認証装置市場は、①ハードウェアトークン、②ソフトウェアトークン、③バイオメトリクスの 3 つのカテゴリから成るが、このうちハードウェアトークンが、現在最も広く利用されている認証装置である。市場の成長は、PKI でのデジタル認証に向けたスマートカードや、USB トークン技術に大きく依存することに

なる。現在、米Microsoftや業界団体International Biometric Industry Association(IBIA)、コンソーシアムBioAPIなどが業界標準の策定を進めており、普及の障害となっていたコストもここ数年で下がってきていることから、市場は徐々に拡大すると予想される。

④暗号

1999年における米国の暗号製品市場は65百万ドルで、2004年では年平均10.7%増の108百万ドルと予測されている。

暗号製品市場は様々なベンダが市場に参入しているため、特に製品の売上において際立ったベンダはおらず、各ベンダがそれぞれの特徴を活かした製品を提供している状態である。米国では、軍と政府によるネットワーク利用の増加により、最も強力な暗号製品の市場となっている。2000年には、DESに続く新しい米国標準暗号（Advanced Encryption Standard）としてRijndaelが採用され対応製品も登場していること、クリントン政権が暗号技術の輸出に関する制限を緩和したこと、また、各ベンダに最も多く利用されているRSA Securityの公開鍵暗号技術アルゴリズムの特許が切れたことなどから、暗号製品市場は今後活性化する可能性がある。

⑤セキュリティマネジメント

1999年の米国におけるセキュリティマネジメント市場は104百万ドルの売上であるが、2004年では年平均24.9%増の317百万ドルの市場に成長する見込みである。

セキュリティマネジメント製品のうち、不正アクセス監視製品では、Internet Security Systems、Network Associates（旧Axent Technologies）等のベンダが市場をリードしている。様々な種類のOSの製品や異なるベンダの製品によって構築されるネットワークの複雑化は進んでおり、それらを統括するセキュリティマネジメントに対するニーズは急速に高まっている。企業におけるセキュリティ担当者の負荷を軽減させるよう、比較的簡易な設定によって導入でき、優れたユーザインタフェイスを持つソフトウェアのニーズが高い。ただし、マネジメントは24時間365日必要となる業務もあり、ソフトウェアの導入だけでは対応が困難な継続的・監視的な業務については、アウトソーシングサービスに代替されていくとみられる。

（2）サービス市場の動向

①セキュリティシステム構築

1999年の米国におけるセキュリティシステム構築サービス市場は1,038百万ドルであり、2004年には年平均22.1%増の2,822百万ドルに成長すると見込まれている。ユーザ企業のセキュリティ意識の高まりと、ある程度のレベルのセキュリティ対策が施された製品やシステムの普及により、今後はセキュリティ単独でのシステム構築といった案件は減少し、

システム構築の中の一部としてセキュリティシステム構築が行われていくものと思われる。それゆえ、市場規模を算出するにも困難な面があるが、セキュリティ対策はシステム構築の必須の事項であるため、市場は安定して成長していくものと見込まれる。

②セキュリティコンサルティング／監査

1999年の米国におけるセキュリティコンサルティング／監査サービス市場は796百万ドルであり、サービス市場全体の17.5%を占めている。2004年では年平均22.7%増の2,217百万ドルに達すると予測されている。

製品の高度化やネットワークの複雑化により、製品やシステム導入時のコンサルティングの重要性はますます高まっている。米国では、事業者が製品やシステムを導入する際にもコンサルティングの重要性が高まっていることを認識しており、コンサルタントメニューの充実やコンサルタントの育成に力を注いでいる。システム的なコンサルティングのみならず、セキュリティポリシー策定の際などは、組織活動全体のコンサルティングも必要となることから、製品ベンダやシステムインテグレータなどもコンサルティング企業や監査法人と手を結び、トータルソリューションを展開できる体制を整備している企業が多い。

③セキュリティ管理

1999年の米国におけるセキュリティ管理サービス市場は675百万ドルであり、2004年では年平均27.9%増の2,312百万ドルの市場規模になると予測されている。

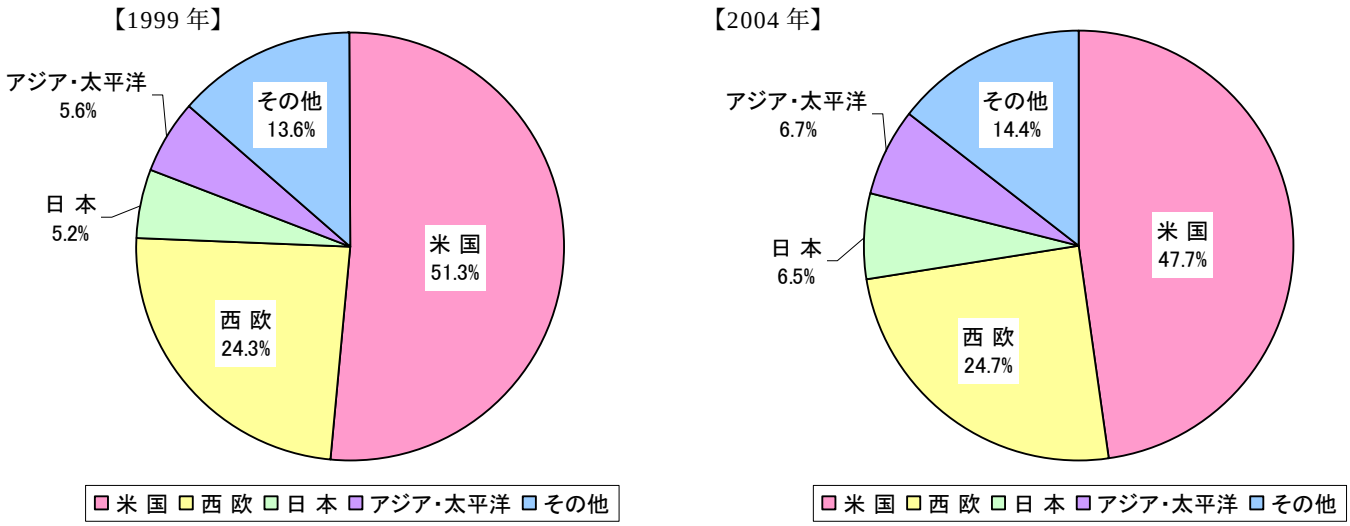
製品やネットワークの複雑化、技術の高度化などを理由に、様々なベンダによる様々な製品を統括するセキュリティ管理に対するニーズは急速に高まっている。米国でも多くのベンチャーが参入している分野であり、市場の急速な拡大が見込まれているが、管理的な業務については24時間365日必要となる業務も多いことから、製品によってユーザ自ら管理する部分と、ASPやMSP（Management Service Provider）といったネットワークによる遠隔管理というモデルによって提供されるサービスで管理する部分とに分かれていくとみられる。これらのサービスによって提供される管理業務は月々のコストが決まっており、しかも自社で管理者を24時間体制で整える必要がないため、情報化予算の乏しい中小企業なども含め急速にマーケットが広がると考えられる。

２．３　情報セキュリティビジネス市場の日米比較

（１）世界市場におけるシェア

図表２－３をみると、1999 年の日本の情報セキュリティ市場は、世界の約 6%を占めている。これは、世界で約 5 割の最も大きなシェアを占める米国、約 4 分の 1 を占める西欧に次いでいる。2004 年になると、米国のシェアは依然として大きいものの 5 割を切り、その分アジア・太平洋地域や、ラテンアメリカ等その他の地域のシェアが増える。西欧と日本については、シェアは微増と予測されている。

図表２－３　1999 年、2004 年の世界の情報セキュリティ市場（国別シェア）



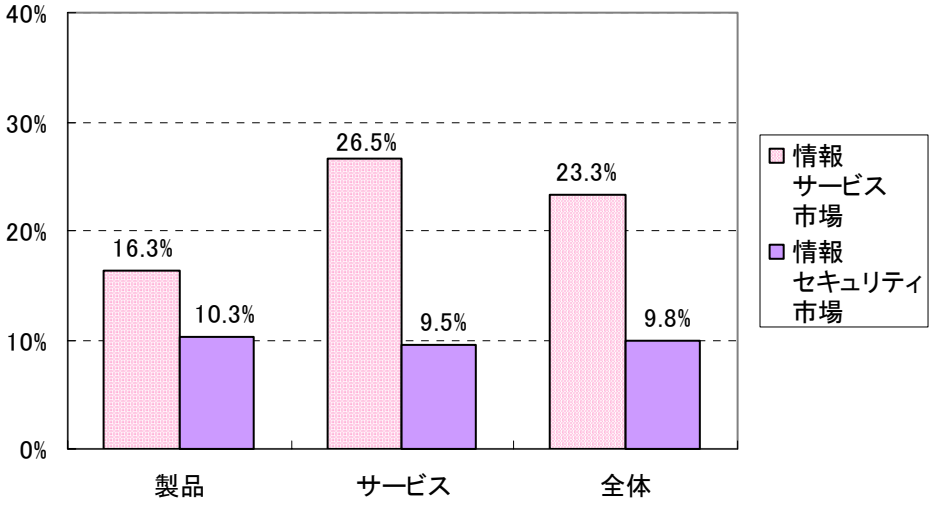
資料：前述した IDC、富士キメラ総研資料より作成
注　：他地域の定義との関係上、日本市場から「セキュリティ保険」は除外している。
　　資料の定義の都合上、サービス市場には「教育・トレーニング」を含んでいる。

なお、セキュリティ市場は、製品、サービスとも順調な成長が予測されているが、これによりセキュリティ製品ベンダの売上も右肩上がりの成長となるとは限らないと考えられる。現在のソフトウェア製品を見ると、ファイアウォールやアンチウイルスソフト、暗号メールのように、セキュリティ製品がハードウェアや OS、ブラウザ等に組み込まれるケースが増加している。これによって、実質的なセキュリティ・ソフトウェアの普及が期待される反面、見かけ上のセキュリティ製品の市場は予測ほど成長しない可能性がある。

（２）情報サービス市場

情報セキュリティ市場と情報サービス市場（ソフトウェア製品市場と専門サービス市場の合計）の比較のため、1999 年における当該市場の米国に対する日本の割合をみると、日本の情報サービス市場は、米国の約 2 割強の規模に相当している（図表２－４）。一方、日本の情報セキュリティ市場は米国の約 1 割の規模に過ぎない。特に、日本の情報サービス市場のサービス分が米国の 26.5%であるのに対し、日本の情報セキュリティ市場のサービス分は米国の 9.5%とその差が大きい。これは、カスタマイズ需要が高い日本の情報サービス市場の構造上の特徴であるが、日本の情報セキュリティ市場においても製品分よりサービス分の方が成長する余地が大きいと見ることもできる。

図表２－４　1999 年の米国市場に対する日本市場の割合
（情報サービス市場、情報セキュリティ市場）

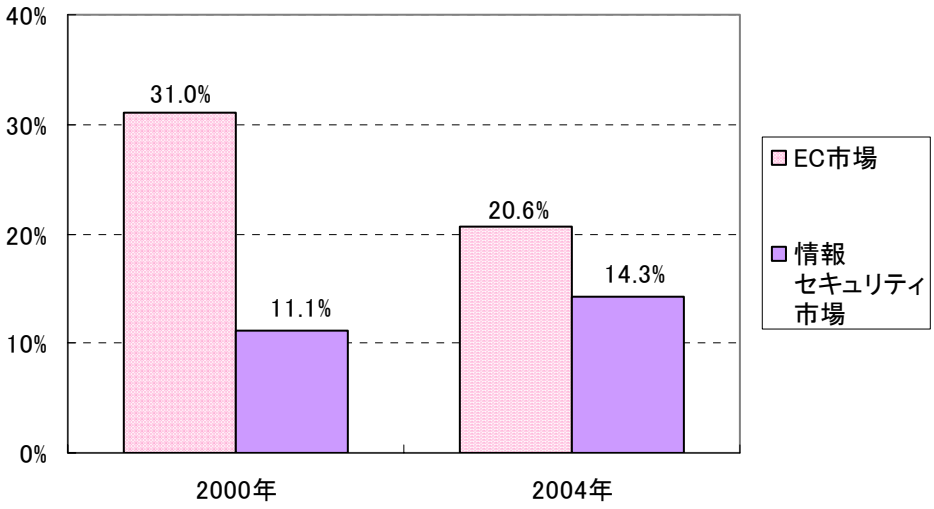


資料： WITSA「Digital Planet 2000」（2000 年 11 月）および本報告書を基に作成
注　：情報セキュリティ市場は、1$=110 円で換算

（3）EC ビジネスの普及状況

セキュリティ導入の有力な促進要素として、EC ビジネスが挙げられる。2000 年の日米の EC 市場を比較すると、B to C 市場では日本の 8,240 億円に対し米国が 8.79 兆円、B to B 市場で日本の 21.6 兆円に対し米国が 63.6 兆円、全体では日本は米国の 31.0%と、GDP 比以上の大きな格差がある（電子商取引推進協議会・アクセンチュア・経済産業省、2001 年 1 月）。さらに、2004 年にはそれが 20.6%にまで縮小し、格差が一層広がると予測されている。この EC 市場と情報セキュリティ市場の米国市場に対する日本市場の割合をみると、2000 年では、EC 市場が 31.0%であるのに対し、情報セキュリティ市場は 11.1%にとどまる。2004 年には、日本の EC 市場が米国の 20.6%であるのに対し、情報セキュリティ市場は 14.3%と、その差はやや縮小するものの、依然として情報セキュリティ市場の日米格差は、EC 市場に比べ大きいと予想される（図表２－５）。したがって、情報セキュリティ市場も EC 市場の水準まで日米格差を縮める努力をする必要があるといえよう。

図表２－５　2000 年および 2004 年の米国市場に対する日本市場の割合
（EC 市場、情報セキュリティ市場）

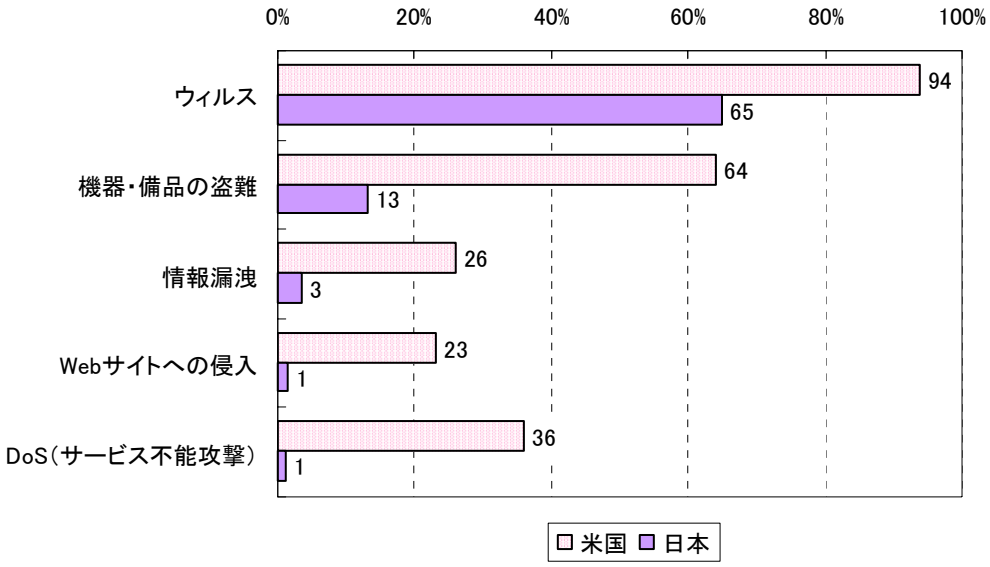


資料：電子商取引推進協議会、アクセンチュア、経済産業省
「平成 12 年度電子商取引に関する市場規模・実態調査」（2001 年 1 月）
を基に作成
注　：1$=110 円で換算

（4）セキュリティ被害の状況

CSI と FBI の共同調査（2001 年３月発表）および KPMG ビジネスアシュアランスによる調査（2000 年 12 月発表）によると、過去１年間に発生したセキュリティ被害の経験は、米国と日本で大きな格差が生じた（図表２－６）。例えば、ウイルス被害については米国の 94%に対して日本が 65%、情報漏洩については米国の 26%に対して日本が 13%となっている。また、Web サイトへの侵入や DoS については、日本はわずか 1%しか経験していないとしている。

図表２－６　過去１年間に発生したセキュリティ被害



資料：

米国－CSI/FBI「2001 CSI/FBI Computer Crime and Security Survey」（2001 年 3 月）

日本－KPMG ビジネスアシュアランス株式会社

「Information Security Survey 2000 Report」（2000 年 12 月）

この結果の解釈としては、日本ではセキュリティ被害の発生件数が少ないため被害経験のある企業が少ないという考え方と、日本ではセキュリティ被害を発見する体制が不十分なため被害経験を自覚している企業が少ないという考え方があり得る。いずれにせよ、このようなセキュリティ被害に対する意識の差が、情報セキュリティ市場の規模の差に影響を及ぼしていると考えられる。

第　３　章

情報セキュリティビジネス活性化のための課題

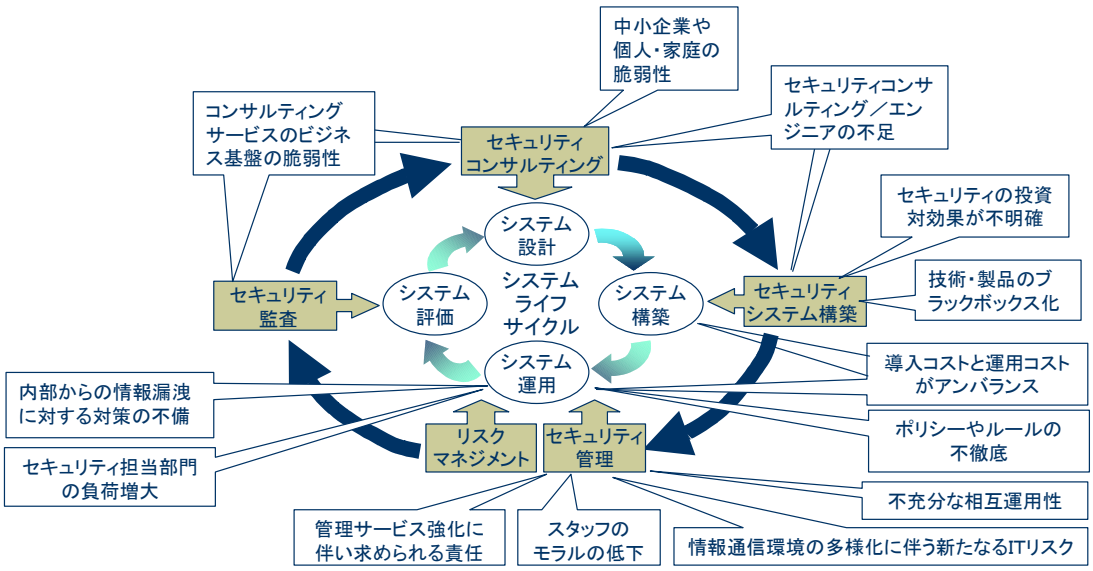
本章では、第１章、第２章の成果を踏まえ、情報セキュリティビジネスの問題点とその活性化に向けた課題についてまとめる。

まず、情報セキュリティビジネスの最終的なゴールをトータルセキュリティの実現とし、そのために達成すべき目標を、セキュリティライフサイクルの円滑な展開とする。本章でとりあげる問題点はこのセキュリティライフサイクルの円滑な展開を妨げるものであり、情報セキュリティビジネス活性化のための課題とは、セキュリティライフサイクルが円滑に展開できるようにするために対応すべき課題である。

３．１　情報セキュリティビジネスの問題点

セキュリティライフサイクルの円滑な展開を妨げる問題点について、技術、人材、市場の観点から、以下の項目を抽出した。

図表３－１　情報セキュリティビジネスの問題点



（１）技術面の問題

①技術・製品のブラックボックス化

現在のセキュリティ製品市場は、その大半をセキュリティ技術の先進国である米国やイスラエルのソフトメーカに依存しており、自社製品を開発・販売する国内のソフトメーカの多くはセキュリティ市場拡大の恩恵に与れずにいると見られる。また今後、OS やメールソフト、ルータ、携帯端末等へのセキュリティ機能の組み込みがより進むと予想され、国内のソフトメーカが参入するのはさらに難しくなると考えられる。これらの影響から、これからのセキュリティ製品は、システム構築や運用を行う技術者を含め、国内の技術者には内部構造がわからないブラックボックスと化し、セキュリティホール対応等についてのトラブル処理が後手に回ることも考えられる。

②不充分な相互運用性

セキュリティ製品の相互運用性が充分でないことが、その普及や利用を阻害しているケースも見られる。例えば、インターネット VPN の製品は互換性が乏しいため、接続先がすべて同じメーカの製品を使用しなければならず、需要はあっても普及が進みにくい状況にある。また、PKI 製品についても、相互運用性が確立されていないため、今後整備される電子政府の構成によっては、政府と取引のある企業は電子政府の省庁や窓口ごとに異なる電子証明書を使い分けなければならなくなる可能性もある。

インターネット VPN 製品については S/WAN（Secure Wide Area Network）プロジェクトや IPv6 対応、PKI 製品については PKI Forum といった、相互運用性確立に向けた業界の取り組みも見られるが、今のところ充分な成果は得られていない。

③情報通信環境の多様化に伴う新たな IT リスクの発生

2000 年には、EPOC や Palm OS を搭載した PDA に対するウイルスが登場した。また、携帯電話も Java 対応になったことで、これまで以上にウイルスやトロイの木馬などの不正アクセスによる被害を受ける可能性が高まったとする見方もある。さらに、CATV インターネットにおいて PC のディスクの中身が見られてしまうリスクや、Peer to Peer 接続がもたらすウイルスや不正アクセスのリスクなど、端末やネットワークが多様化することによって新しい IT リスクが発生し、大きな問題を招く恐れがある。

（2）人材面の問題

①セキュリティコンサルタント／エンジニアの不足

セキュリティ分野は、技術の新陳代謝が激しい上に、製品もブラックボックス化しつつあるため、国内のエンジニアは効率的な技術蓄積が難しい。また、セキュリティコンサルタントは、経営的・組織論的な分析能力も要求されるため、セキュリティ先進国の米国でも人材不足であり、セキュリティベンダ間で優秀な人材を奪い合っているといわれる。一部で、タイガーチーム（依頼を受けて疑似アタックをしかけ脆弱性を評価するサービススタッフ）等に元ハッカー／クラッカーを採用するケースも見られるが、そのような人材に対してポリシー策定等のコンサルティング手法を指導するのは容易ではない。

このように、セキュリティコンサルタントやセキュリティエンジニアの育成は難しい状況にあり、これらの人材不足が、これからの情報セキュリティビジネスの発展の妨げるとする予測も見られる。

②スタッフのモラルの低下

サービス事業者のスタッフによる顧客情報の外部流出事件が後を絶たない。このような不正行為は、技術だけで防ぐことは困難であり、従業員のモラルの確立や充分なチェックがなされる運用ルールの適用など、組織・制度による対応が不可欠である。「個人情報保護基本法制に関する大綱」が提出され、個人情報保護基本法の起案も予定されている状況であり、これからは、事業者側の監督責任が今以上に厳しく追求されるものと予想される。

③管理サービス強化に伴い求められる責任

前章までに述べた通り、セキュリティ管理サービスが有望視されているが、そのようなサービスビジネスは従来の製品ビジネスと違って手離れが悪く、ユーザをサポートするスタッフの負荷が増大する可能性が高い。

また、こうしたサービスビジネスでトラブルが発生すると、ユーザ企業の社会的信用に大きな影響を及ぼしかねない。このような責任の重さを自覚し、適切なレベルでサービスを提供する必要があるが、現状ではサービス品質が充分でなく、トラブルも少なからず生じている。

（３）市場面の問題

①セキュリティの投資対効果が不明確

ユーザ企業にとって、セキュリティ投資はそれ自体が利益を生み出すものではないため、これまで経営者層の理解を得られないケースが多く見られた。昨今の不正アクセス関連の報道により、以前に比べ理解は得やすくなったものの、投資対効果が明確でなく、どこまでコストをかければ必要なセキュリティレベルを実現できるのかという点で適正な指標がないため、ユーザ企業側もセキュリティ投資額の妥当性について判断しにくい状況にある。

②コンサルティングサービスのビジネス基盤の脆弱性

国内では、セキュリティコンサルティングの重要性が充分に理解されておらず、セキュリティポリシーの策定も、それに見合う対価を得るのは容易ではない。セキュリティベンダの中には、システム構築受注のための魅力づくりと位置づけ、最低限の作業で済ませる事業者も含まれている。また、システムベンダの場合、「自社製品ありき」と見られるため、そのコンサルティングサービスはマルチベンダ対応を表明していても、ユーザ側の理解が得られない場合もある。その結果、リスク分析に充分なコストをかけられなかったり、セキュリティコンサルタントのモチベーションが上がらず、人材が育ちにくくなる可能性がある。

③導入コストと運用コストがアンバランス

セキュリティ投資の許可が得られた場合も、その予算が一時的で、運用コストまでカバーできていないケースが見られる。例えば、ファイアウォールやアンチウイルスソフトを導入すればそれだけで安全になる、といった誤解もあり、実際にはそのメンテナンスにも充分なコストを掛けなければ安全性を維持できないということが理解されていない。また、予算措置そのものが、「セキュリティブーム」による一過性のものであり、継続的な取り組みにつながっていない可能性もある。その結果、時間の経過とともにセキュリティレベルが下がり、不正アクセス等の被害が発生することによって、情報セキュリティビジネスそのものへの不信感を招きかねない。

④セキュリティポリシーやルールが不徹底

セキュリティポリシーやルールを策定したにも係わらず、その実施が徹底されておらず、見込んでいたセキュリティレベルが実現できていないケースが見られる。また、当初は適正なセキュリティレベルを実現していた場合にも、日常の運用において徐々にポリシーやルールが形骸化していき、セキュリティレベルが低下することも考えられる。こういったポリシーやルールについては、会社として必ず実現しなければならないとする姿勢を明確にするとともに、実際の運用状況を踏まえ、定期的に監査を行い、セキュ

リティポリシーやルールを見直すしくみを整備する必要がある。

⑤セキュリティ担当部門の負荷増大

日々発見されるセキュリティホールや新たな不正アクセスの手法に対する対応策の実施、利便性や効率性を追求するエンドユーザからの反発、大規模化する社内ネットワークの安全性の維持など、セキュリティ担当部門に要求される項目は多岐に渡り、その負荷も大きい。セキュリティ運用はモチベーションを保ちにくい業務であり、周囲の理解が乏しいこともその負担をさらに増加することになる。

⑥内部からの情報漏洩に対する対策の不備

ユーザ企業においても、EC 事業等を通じて得た顧客情報の管理が甘く、外部に流出する事件が発生している。(2)②に示したサービス事業者におけるスタッフのモラルの問題と同様に、個人情報保護基本法の制定に向けて、顧客情報等の管理の徹底や罰則規定の整備が必要となるであろう。

⑦中小企業や学校、個人・家庭の脆弱性

情報セキュリティビジネスの問題点として、中小企業や学校、個人・家庭といったセキュリティ予算の確保が難しい層に対してはアプローチしにくく、それらの層がセキュリティレベルの低いセキュリティデバイドとなる可能性がある。しかし、情報セキュリティは総合的なものであり、例えば大手企業のセキュリティレベルが高くても、そこに納入する中小企業のセキュリティレベルが低ければ、そこをつかれる危険性は否定できない。

従って、トータルセキュリティを実現するためには、セキュリティデバイド化する可能性のある中小企業や学校、個人・家庭の市場についてもセキュリティベンダのサポートが、適正な料金水準で提供されることが望まれる。

３．２　情報セキュリティビジネス活性化のための課題

３．１を踏まえ、わが国における情報セキュリティビジネスの活性化のための課題について以下にまとめる。

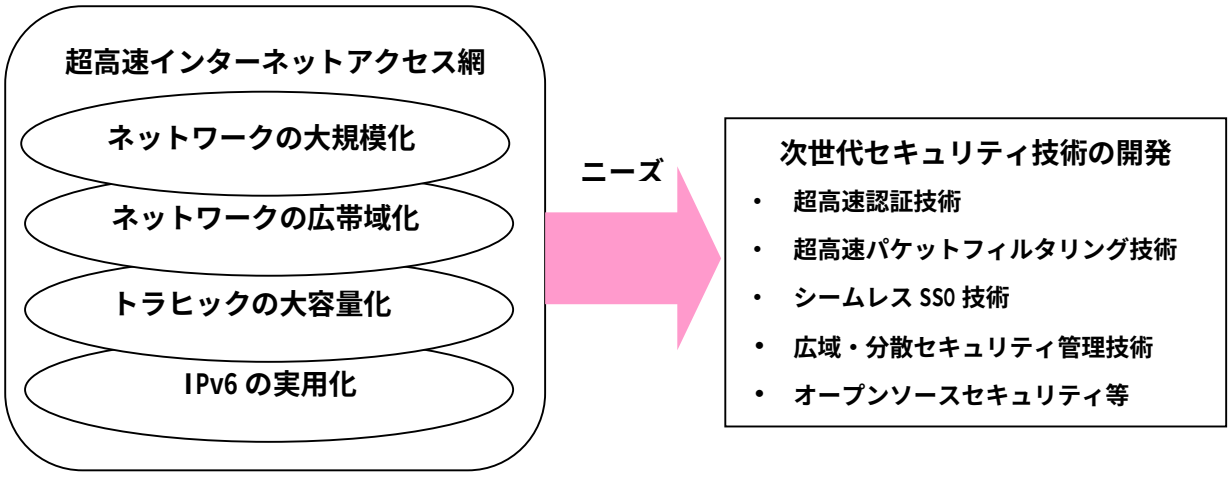
（１）次世代セキュリティ技術の開発

今後、アクセス網が高速化・広帯域化し、映像や音声などの大容量コンテンツがインターネット上を流通することが予想される。また、広帯域のモバイルインターネットの普及により、有線・無線の統合的な利用環境が求められるであろう。さらに、IPv6 とユビキタス・コンピューティングの進展により、家電機器を含む情報機器同士が自律的に通信するようになり、膨大なパケットが絶えず認証し合いながら飛び交う状況も考えられる。

このような次世代の超高速通信環境では、セキュリティ技術にも今以上に高速かつ効率的な処理が要求される。例えば、認証処理やファイアウォールのパケットフィルタリング処理が今のままでは、ネットワーク全体のボトルネックとなる可能性もある。また、ユーザのアクセスルートが有線・無線と変化しても、フレキシブルに対応して、シームレスなシングル・サイン・オン環境を提供する機能、広域・分散環境を統合的に監視し、不正アクセスを迅速かつ正確に検知する機能、オープンソースツールに付加するセキュリティ機能の開発などが想定される。これらの技術開発を他国に先行的に進めることで、セキュリティ技術をリードする米国、イスラエルに負けない基盤技術を確立することも可能である。

ただし、このような技術開発を進めるための環境（超高速インターネットや IPv6 の広域的な利用環境等）は、一民間企業では対応できるものではない。そこで、ギガビットネットワーク等の国の研究開発テストベッドを活用し、IPv6 の広域実証実験をベースに、産学官の協力体制で次世代セキュリティ技術の研究開発を押し進める方向が考えられる。

図表３－２　次世代セキュリティ技術の開発



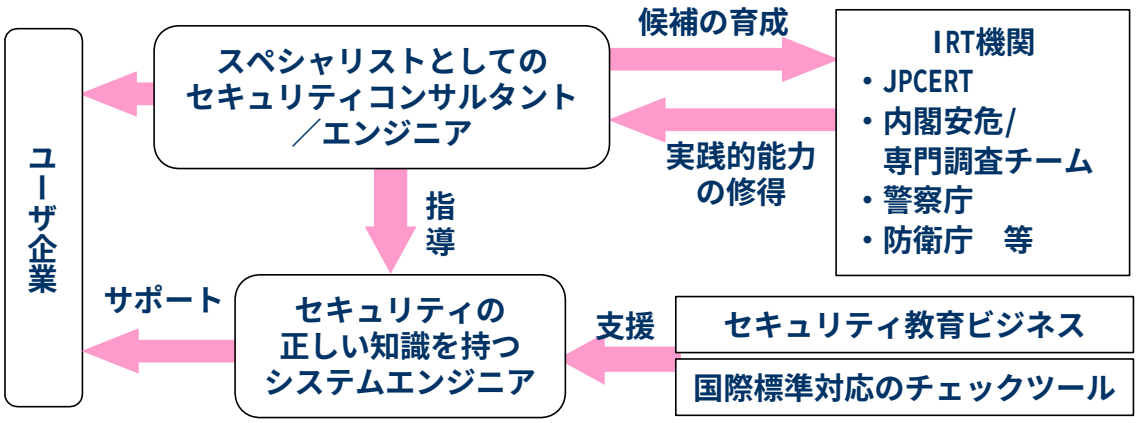
（２）実践的なセキュリティ人材育成機能の整備

わが国の情報セキュリティベンダに必要なセキュリティ人材には、二つのタイプが想定される。一つは、高度なセキュリティ技術や優れた分析能力を有するスペシャリストとしてのセキュリティコンサルタント／エンジニアである。もう一つは、セキュリティに関する正しい知識を有するシステムエンジニアである。前者は、技術開発やユーザ向けサービスの最前線に位置し、情報セキュリティビジネスを牽引する役割を担う。また後者は、一般のシステム構築の場面で、基本的なセキュリティ技術をごく当たり前に導入・活用し、産業・社会のシステムを平均的にセキュアな方向に押し上げる役割を担う。

前者については、３．１(2)①で示した、育成が難しいとされる人材像であるが、このような人材を育成し、活用しない限り、わが国の情報セキュリティビジネスの将来は厳しいものとなることが予想される。具体的には、そのような人材候補を、JPCERT/CC や内閣安全保障・危機管理室の情報セキュリティ対策推進室・専門調査チーム、警察庁、防衛庁等の IRT 機関・部署に預け、実際に起きているインシデントの最前線で経験を積ませることによって、実践的な能力を修得させるアプローチが考えられる。

また、後者については、通常のシステムエンジニアに対するセキュリティ技術の教育を強化し、国際標準（ISO/IEC15408、ISO13335、ISO/IEC17799）への対応を自動化・データベース化したツールを活用することで、大きな負荷をかけずに平均的なセキュリティレベルの底上げを果たすことが期待できる。特に、システムエンジニアを対象としたセキュリティ教育は今後需要が拡大する可能性がある。

図表３－３　実践的なセキュリティ人材育成機能の整備



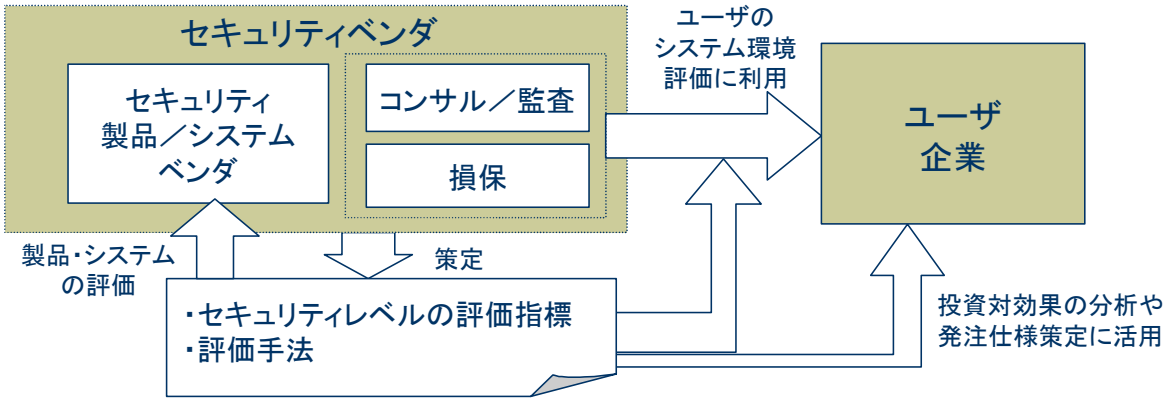
（３）セキュリティレベルの評価指標の策定

製品やシステムのセキュリティレベルを客観的に評価する指標や評価手法の検討。具体的には、民間企業で必要となるセキュリティレベルを想定し、侵入テスト等によるチェックリストの結果からそのセキュリティレベルを評価する。ユーザ企業はこのような指標をもとに、問題とされていたセキュリティ投資の費用対効果を分析し、資材調達時の指標とすることが可能である。

2001 年４月より導入予定のセキュリティ評価・認証制度は、電子政府と国際標準を重視したもので、必ずしもユーザ企業のニーズと合致しない場合もある。そこで、セキュリティ評価・認証制度とは異なる業界標準としての役割として、上記の指標を含め別の指標が必要になってくる。

実際の検討では、損害保険業界や監査企業においてその指標を活用することを想定し、それらの事業者と連携した体制で、検討する方向も考えられる。

図表３－４　セキュリティレベルの評価指標検討の枠組み



また、このような指標の一つとして、ソフトウェアプロセスアセスメントの手法を用いてセキュリティ評価を行う枠組みである SSE-CMM などの手法も検討していく必要がある。

（4）セキュリティデバイドの解消

セキュリティベンダに望まれるものは、社会全体を対象としたトータルセキュリティの実現である。そのためには、各セキュリティベンダは相互に連携し、必要な機能を補い合い、弱点を補完し合う形で、総合的なセキュリティ環境を提供する体制を整えることが望まれる。中小企業や学校、個人・家庭等のセキュリティデバイド層については、複雑な管理が必要となる製品販売や、コストの高い通常のサービスビジネスではなく、ASP 等の集中管理型のサービスプロバイダモデルによってサポートする方向が期待される。これによって、可能な限りサービス提供に要する負担を軽減し、結果としてユーザ層に求められる負担をも軽減することができる。さらに、これらのユーザ層におけるセキュリティ環境整備の推進こそが、わが国のトータルセキュリティ実現に有効であることの考えから、これらのユーザ層のセキュリティ環境整備に対する支援施策を実施することも考えられる。

図表３－５　トータルセキュリティ実現のための枠組み