経済産業省委託調査

平成 20 年度

情報セキュリティ市場調査報告書

平成 21 年 3 月

NPO 日本ネットワークセキュリティ協会

目次

表目次

図目次

1. はじめに

電車に乗る際に非接触 IC カードあるいは携帯電話を改札機にかざし、駅舎内の売店でも同様にそれらを使い、容易に買い物ができるようになり、高速道路は ETC[1]によって料金所もノンストップで通過できるようになった。また、テレビでは地上デジタル放送が開始され、インターネット経由で番組配信も提供され、放送と通信の融合がデジタルをキーワードとして急速な進展を見せている。

このように、情報技術（IT）は国民生活の隅々にまで普及・浸透し、企業活動にとっても不可欠のインフラとなっている。利便性の増大の一方で、IT の利用基盤として重要な役割を担うインターネットにはその安全な利用を妨げる様々な脅威が発生し、残念ながらその深刻さは高まる傾向にある[2]。インターネット利活用の安全を確保し、IT 及び情報通信インフラの一層の高度利用を実現して社会の効率と価値の拡大を達成するために、安全安心なネットワーク基盤と情報セキュリティを確保することは、社会的な課題であり要請となっている。

2009 年 2 月 3 日、政府は第 2 次情報セキュリティ基本計画を策定し公表した[3]。2006 年 2 月 3 日に策定された第 1 次情報セキュリティ基本計画の下で進めてきた、政府機関、重要インフラ、企業、個人各々における情報セキュリティ対策の推進の成果と反省を受け、「事故前提社会」の基本コンセプトの下に、サイバーセキュリティの進化を目指すものである。現実世界があらゆる面で何らかの事件事故の危険性を内包しつつ、それを防止し、制御し、緩和し、回避し、あるいは受容しつつ社会の営みを形成しているように、「サイバー」と言われる情報通信技術の世界においても事件事故の脅威を同様にコントロールできる姿を目指して行く必要がある。

情報セキュリティは、単にインターネットからの攻撃の脅威、情報通信インフラを悪用した詐欺等の犯罪、情報の流失・紛失やそれに伴う被害の防止は無論のこと、企業統治のデータや知的財産の保護、すなわち機密性、完全性、可用性の確保を通じての企業の内部統制や付加価値、競争力の確保といった、社会経済の神経系の保全というより積極的・基幹的使命を負っている。

この認識が広く共有されるに伴って、組織における情報セキュリティ対策への取組も進んできている。またそれを支えるための情報セキュリティ技術、製品、サービスも多くの事業者からさまざまなものが提供され、官公庁、企業、教育機関、家庭等の安全に貢献している。

その姿を統計的、金額的に明らかにし、産業動向の分析を行って各方面の参考とすることを目的に、特定非営利活動法人（NPO）日本ネットワークセキュリティ協会（JNSA）では、2004 年度以来、情報セキュリティ市場実態調査を実施してきた。これは、経済産業省の「わが国情報セキュリティの普及度と到達度を明らかにする」ことにより政府の産業政策、ひいては情報セキュリティ政策立案に資することを狙いとする政策目的に沿って、同省の委託事業として取り組んできたものである。第 2 次情報セキュリティ基本計画のもと、一歩進んだ取組が開始されるにあたって、今日の我が国の情報セキュリティ産業の現状を確認し、その動向を把握することは、情報セ

---

[1] ETC＝Electronic Toll Collection System　http://www.go-etc.jp/riyouhouhou/riyouhouhou.html

[2] 悪質化するネットワーク脅威については独立行政法人情報処理推進機構（IPA）をはじめ多くの機関・組織が警告を発している。最近の警告事例：　http://www.ipa.go.jp/security/txt/2009/03outline.html#5
IPA 発行情報セキュリティ白書 2008：
http://www.ipa.go.jp/security/publications/hakusyo/2008/hakusyo2008press.html

[3] http://www.nisc.go.jp/active/kihon/resp_keikaku2.html

キュリティ政策並びに情報セキュリティ産業政策の推進にとって有意義なことと信ずる。

また、この報告書は、行政当局のみならず、情報セキュリティを支える製品・サービスの提供事業者、その事業への新規参入を企図する企業や個人、その他各方面の参考に供されることも期待している。本報告書が、官民一体となって情報セキュリティ対策を推進するに際しての課題を整理し、具体策を講ずるための一助となれば幸いである。

以下に調査結果を報告する。このうち、2.項は調査結果の要点をまとめたエグゼクティブサマリであり、6.項に市場を全体として見た時の概観を記述している。調査結果及びその解説並びに分析の詳細は 7.項、8.項に記載し、9.項には海外市場との比較考証を掲載した。10.項では、ベンダサイドからの調査統計分析を目的としている本調査結果に対し、ユーザ側を対象とした調査結果との対比において考察を試みた。また数値により浮き彫りになる市場の姿の考証とは別の切り口として、今回、情報セキュリティをめぐる昨今の特徴的、あるいは注目すべき動向をトピック的に 11.項にまとめた。

本報告書が関係各方面において有意義に活用されることを期待する次第である。

なお、本報告書では、「セキュリティ」という用語を、原則として、情報一般に関わる場合は「情報セキュリティ」、情報システムに固有の場合は「IT セキュリティ」、両者にまたがる場合や文脈から対象が明確な場合は単に「セキュリティ」と表記している。

2. 調査分析結果の概要

2.1. 調査概要

本調査は、国内で情報セキュリティに関する製品やサービスを提供する事業者に対して、2008年11月～12月に実施したアンケート調査をベースに、官民の各種統計や分析資料並びに一部事業者へのヒアリング結果を加味して、JNSAセキュリティ市場調査ワーキンググループによる検討･推計作業を経てまとめた。その作業結果としてここに報告する数字は、国内情報セキュリティ市場の金額規模の推定値である。そのデータに、今回の作業過程で得られた情報と観察に基づいてまとめた、市場動向に関する解説と分析を加えて報告書とした。

また､本調査結果と､民間調査機関が提供する海外市場に関するデータとの国際比較を行った。

なお､調査の基準年度としたのは2007年度であり､その実績値と2008年度の見込み数値を元に前後の年度の推定規模を算出している。2006年度実績値については､前年度調査結果も参考とした。

2.2. 国内情報セキュリティ市場の実態概要

表1に国内情報セキュリティ市場の推計結果を示す。

表 1　国内情報セキュリティ市場規模　実績と予測

（金額:百万円、成長率:対前年比増加率）

国内情報セキュリティ市場推計	2006年度（推定実績）		2007年度（推定実績）			2008年度（実績見込）			2009年度（予測）		
	金額	構成比	金額	構成比	成長率	金額	構成比	成長率	金額	構成比	成長率
情報セキュリティ市場合計	**597,198**	**100.0%**	**684,717**	**100.0%**	**14.7%**	**726,767**	**100.0%**	**6.1%**	**687,359**	**100.0%**	**−5.4%**
情報セキュリティツール合計	**292,449**	**49.0%**	**346,100**	**50.5%**	**18.3%**	**374,771**	**51.6%**	**8.3%**	**363,581**	**52.9%**	**−3.0%**
統合型アプライアンス	14,487	5.0%	18,183	5.3%	25.5%	19,663	5.2%	8.1%	19,088	5.3%	−2.9%
ネットワーク脅威対策製品	48,455	16.6%	53,383	15.4%	10.2%	55,925	14.9%	4.8%	51,781	14.2%	−7.4%
コンテンツセキュリティ対策製品	116,446	39.8%	132,309	38.2%	13.6%	142,704	38.1%	7.9%	138,721	38.2%	−2.8%
アイデンティティ･アクセス管理製品	48,821	16.7%	61,533	17.8%	26.0%	66,618	17.7%	7.5%	63,079	17.3%	−4.7%
システムセキュリティ管理製品	38,455	13.1%	46,770	13.5%	21.6%	52,153	13.9%	11.5%	51,615	14.2%	−1.0%
暗号製品	25,785	8.8%	33,922	9.8%	31.6%	38,157	10.2%	12.5%	39,296	10.8%	3.0%
合計	292,449	100.0%	346,100	100.0%	18.3%	374,771	100.0%	8.3%	363,581	100.0%	−3.0%
情報セキュリティサービス合計	**304,748**	**51.0%**	**338,618**	**49.5%**	**11.1%**	**351,996**	**48.4%**	**4.0%**	**323,778**	**47.1%**	**−8.0%**
情報セキュリティコンサルテーション	63,451	20.8%	73,497	21.7%	15.8%	77,708	22.1%	5.7%	71,181	22.0%	−8.4%
セキュアシステム構築サービス	142,585	46.8%	147,130	43.5%	3.2%	149,425	42.5%	1.6%	132,397	40.9%	−11.4%
セキュリティ運用･管理サービス	74,134	24.3%	87,233	25.8%	17.7%	91,777	26.1%	5.2%	89,115	27.5%	−2.9%
情報セキュリティ教育	17,467	5.7%	23,404	6.9%	34.0%	25,461	7.2%	8.8%	23,669	7.3%	−7.0%
情報セキュリティ保険	7,111	2.3%	7,354	2.2%	3.4%	7,625	2.2%	3.7%	7,417	2.3%	−2.7%
合計	304,748	100.0%	338,618	100.0%	11.1%	351,996	100.0%	3.4%	323,778	100.0%	−8.0%

2006年度の国内情報セキュリティ市場規模の推定実績値は、「情報セキュリティツール」（アプライアンスとソフトウェア）が2,924億円、「情報セキュリティサービス」が3,047億円、合計

で 5,972 億円であったと推定される。

今回調査の基準年度とした 2007 年度は市場規模が拡大し、推定実績値は、「情報セキュリティツール」が 3,461 億円（対前年度比成長率 18.3%）、「情報セキュリティサービス」が 3,386 億円（同 11.1%）で、合計 6,847 億円（同 14.7%）となった。2007 年度の前回調査において、2005 年度に初めて 5,000 億円の大台に乗ったものと見られると報告した市場規模は、2006 年度に 6,000 億円近い規模に拡大し、更に 2007 年度には 15%弱という高い伸びを維持して 7,000 億円に近い規模に達したと推測する。

今年度、2008 年度の実績見込み値は、それぞれ 3,748 億円（同 8.3%）、3,520 億円（同 4.0%）となり、合計では 7,268 億円（同 6.1%）と 7,000 億円を上回る市場規模に達するものと見込まれる。日本経済は米国に端を発した金融危機とその影響による世界同時不況の影響を受けて 2008 年 10 月頃から急速に減速したものと見られているが、年度前半がかなり好調な推移をたどったことと、ユーザ企業のセキュリティ投資態度が、「予算手当てがされているものは予定通り実施する」「今年度のうちに手当てできるものはやっておく」といった姿勢も比較的多く見受けられ、生産の縮小ほどには影響を受けていない可能性が高い。

翌年度、2009 年度は、ヒアリング対象とした各社とも全く見通しが立たないとしており、現時点で市場規模の推定をすることは極めて困難である。一般論的に新規投資や能力増強的な投資の動きは鈍ると考えられるが、ウイルス対策のように固定費的支出はそれほど落ち込まないと考えられることと、ツールの集約化統一化によるトータルコストの削減やサービス化への移行に期待する、攻めの営業姿勢を示す事業者も多く、そのあたりが下支えする期待も持てる。この辺を踏まえて推計作業を行った結果、ツール、サービス、合計は各々、3,636 億円（対前年度比成長率マイナス 3.0%）、3,238 億円（同マイナス 8.0%）、6,874 億円（同マイナス 5.4%）と、ほぼ 2007 年並みの規模に後退するものと予測される。

図 1 に今回調査結果による国内情報セキュリティ市場規模の推移を、図 2、図 3 に 2007 年度における国内情報セキュリティツールと情報セキュリティサービス各々の市場区分別分布を示す。（カッコ内は各々の構成比率。）

図1　国内情報セキュリティ市場規模の推移

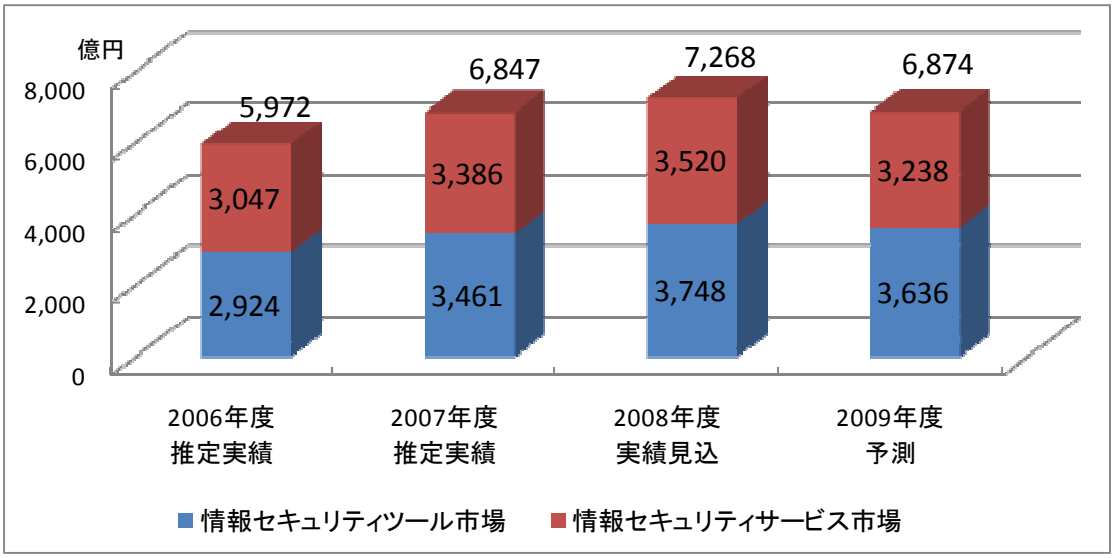


図2　2007 年度の情報セキュリティツール市場

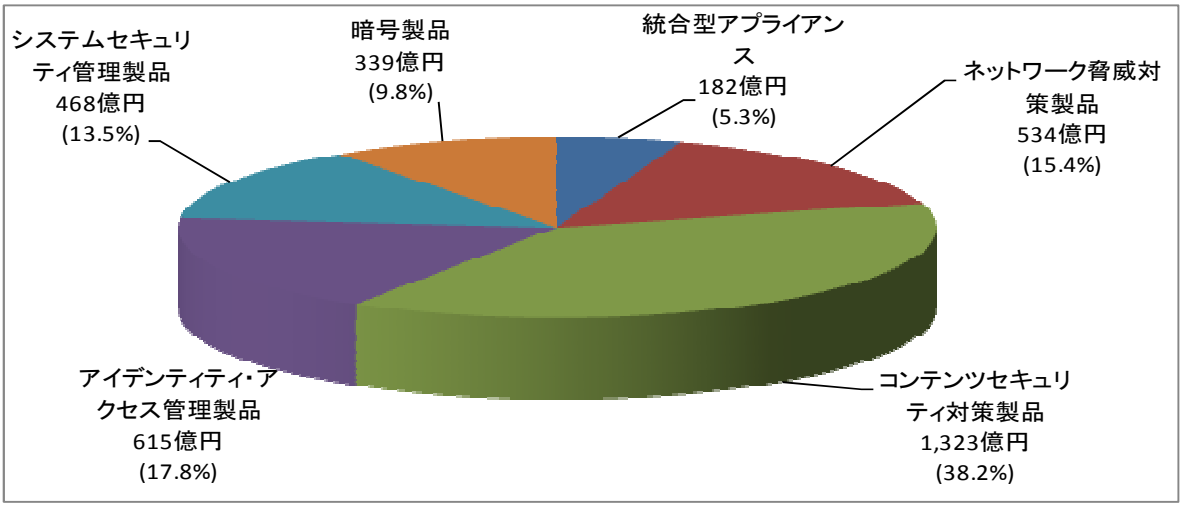
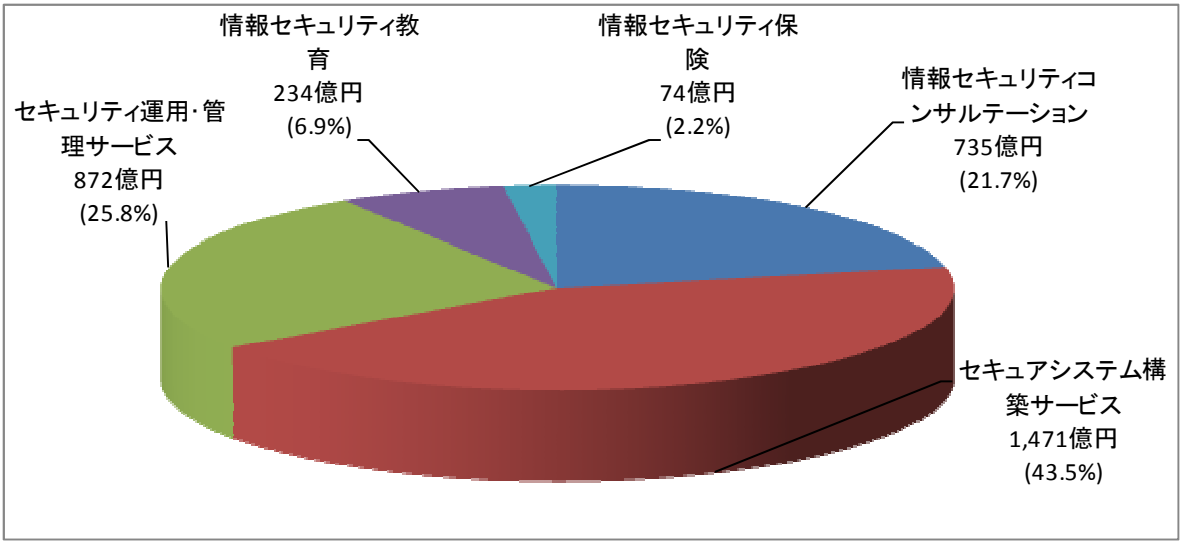


図3　2007 年度の情報セキュリティサービス市場



2.2.1　情報セキュリティツール市場

「情報セキュリティツール」市場について、表 1 に示す通り、「統合型アプライアンス」「ネットワーク脅威対策製品」「コンテンツセキュリティ対策製品」「アイデンティティ･アクセス管理製品」「システムセキュリティ管理製品」「暗号製品」の 6 カテゴリ（大分類）に分類して集計した。（市場分類の定義は 5.項を参照）以下、規模の大きい順に概要を記す。また、図 4, 5, 6 に各々情報セキュリティツール市場のカテゴリ別の規模の推移、構成比の推移、伸び率の推移を示す。

【コンテンツセキュリティ対策製品】

「コンテンツセキュリティ対策製品」は、情報セキュリティツール市場のうち金額規模が最も大きいカテゴリである。2007 年度推定実績値は 1,323 億円（情報セキュリティツール市場合計に対する構成比 38.2%）となった。このカテゴリは主としてウイルス・不正プログラム対策製品で構成されている。ウイルス・不正プログラム対策は最も広く普及している[4]セキュリティ対策である。他の製品は主として企業向けであるのに対し、ウイルス・不正プログラム対策製品は個人消費者向けにも大きな市場を形成している。この二つの要素により、このカテゴリの市場規模は、他のカテゴリに比べ、格段に大きなものとなっている。

【アイデンティティ･アクセス管理製品】

「アイデンティティ･アクセス管理製品」の 2007 年度推定実績値は 615 億円（同 17.8%）で、「ネットワーク脅威対策製品」を抜いて「情報セキュリティツール」市場の中で二番目に大きな規模へと成長した。このカテゴリには、本人認証のための製品や、システム、サーバ、ネットワ

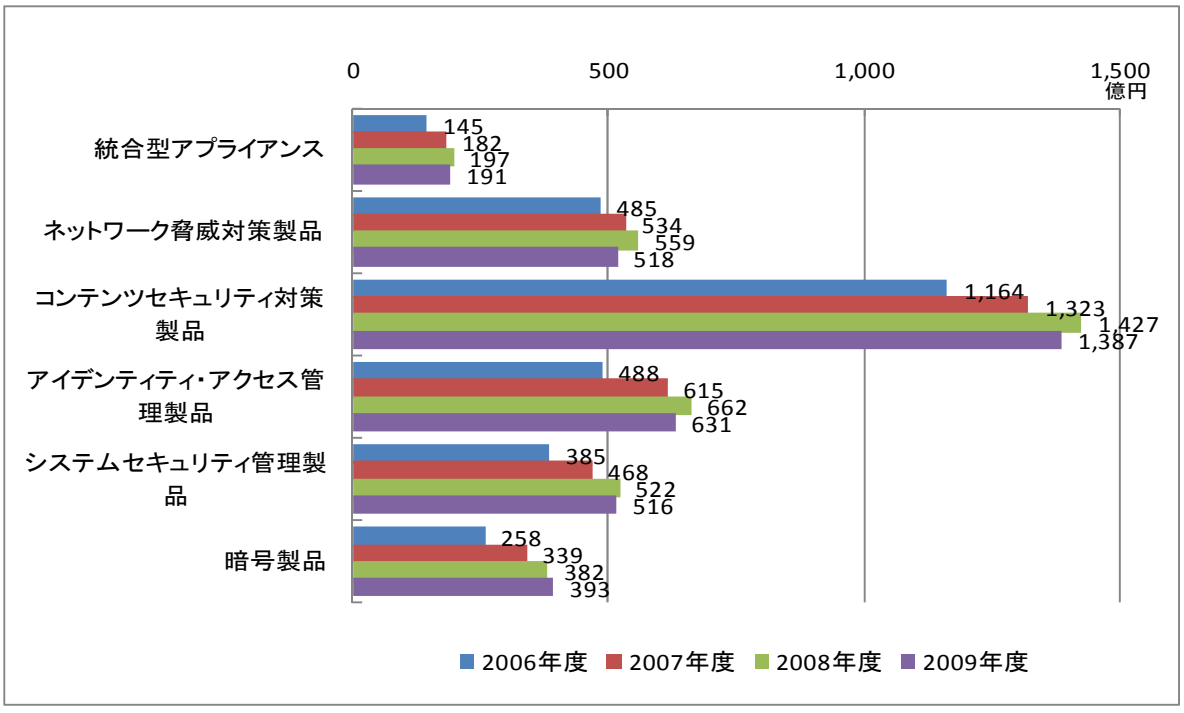
[4] JNSA「IT セキュリティ対策施策の導入･実施状況とその満足度調査」
http://www.jnsa.org/active/2004/active2004_15a.html

ーク､データ等のコンピューティング資源の利用権をシステム全般にわたって管理するシステム、システムやネットワークへのログオンを管理する製品等が含まれる。この市場が拡大する背景には、個人情報保護や情報漏えい対策強化を中心に、ユーザの本人確認や、システムやデータへのアクセス権管理の必要性が、より強く意識されるようになってきたことが挙げられる。また、内部統制のために IT ガバナンスの確立が急がれており、IT の利用を個人に紐付けて管理する管理体制や統制システムの整備が進んできたこともこのカテゴリの規模が急速に拡大している要因と言える。

【ネットワーク脅威対策製品】

「ネットワーク脅威対策製品」は市場規模としては長らく「情報セキュリティツール」市場の中で二番手に位置していたが、2006 年度にはほぼ同規模に並ばれ、2007 年度にはその座を「アイデンティティ･アクセス管理製品」に譲った。2007 年度推定実績値は 534 億円（同 15.4%）であった。この分野には、ファイアウォール、VPN[5]と侵入検知･防御製品を含む。各製品がソフトウェアタイプからハードウェア一体型のアプライアンスタイプに移行すると共に、複数機能を統合し 1 台で提供する「統合型アプライアンス」（単独で別カテゴリに分類）への移行が進んでおり、市場の成長率の面では最も成熟化している。

図4　情報セキュリティツール市場規模の推移



[5] VPN: Virtual Private Network 仮想私設通信網　暗号通信により、公共通信網を仮想専用線のように利用する技術

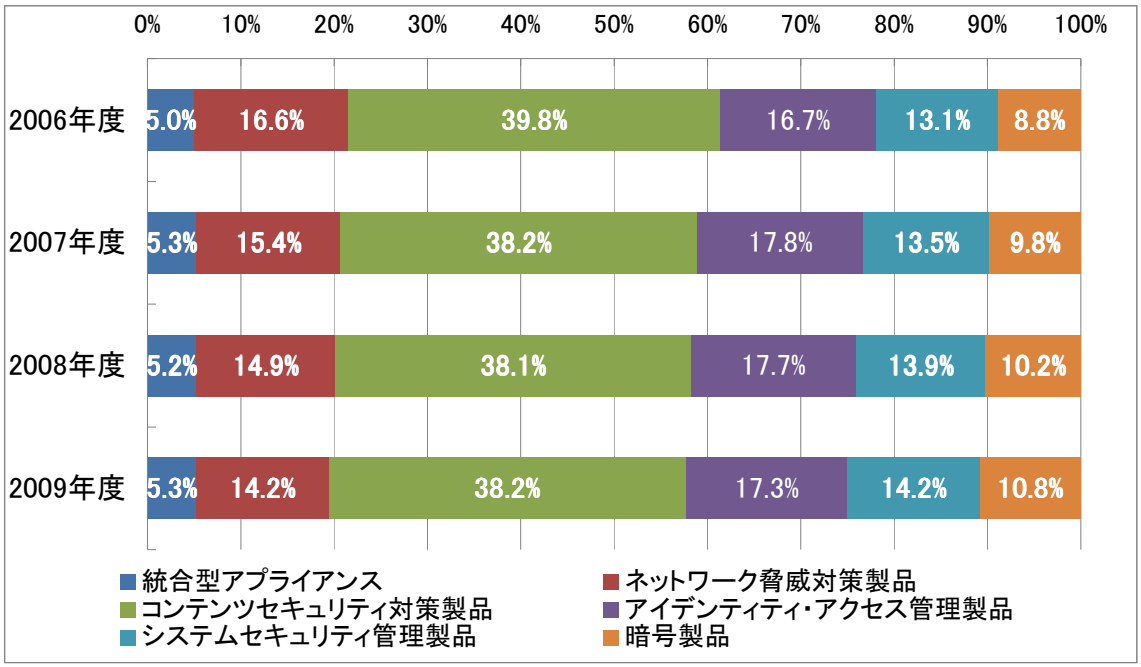
【システムセキュリティ管理製品】

「システムセキュリティ管理製品」の 2007 年度の推定実績市場規模は 468 億円（同 13.5%）であった。「アイデンティティ・アクセス管理製品」と同様の理由で、ネットワーク接続機器・端末におけるアクセス権やセキュリティ設定の状態を管理したり、権限外のアクションを監視したりする製品の市場が急拡大している。また、内部統制やコンプライアンス対応を意識して、ログ管理やデジタルフォレンジック[6]対応を強化する動きが強まっており、これらのための製品に対する需要も急増している模様である。

【暗号製品】

「暗号製品」の市場規模は 2007 年度推定実績値で 339 億円（同 9.8%）であった。このカテゴリも高い市場成長率を示している。情報漏えい対策として、データ暗号化の重要性が強く意識されるようになってきており、記憶媒体への書き込みに際して暗号化を施す製品の需要を押し上げている。この背景には、国産ベンダを中心に安価で手軽に導入できる製品の提供が進み、基本的な情報漏えい対策として導入しやすい点が評価されている面もあると見られる。また、ゲーム機をはじめとする情報家電に組み込まれる暗号モジュールも、最終製品への需要を反映して市場を拡大している。

図5　情報セキュリティツール市場構成比の推移

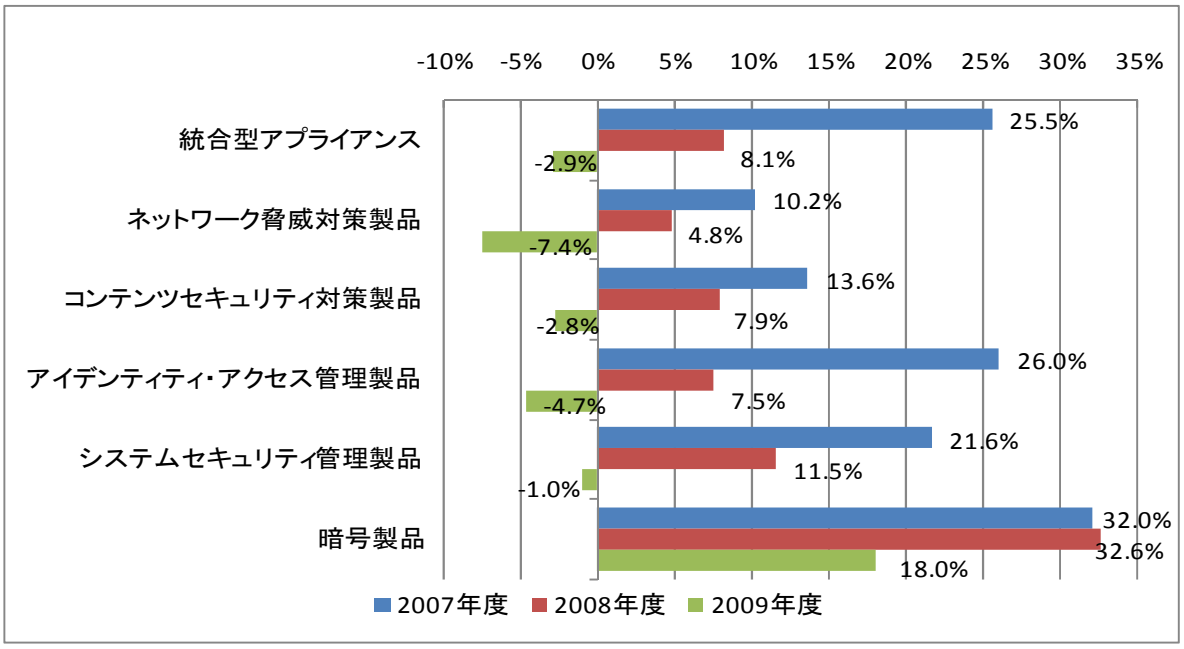


[6] コンピュータ犯罪に関する証拠の法的証拠能力を確保するための収集、保全、解析、立証技術等一連の技術並びに関連するプロセスや理論などを総合的に指す。

【統合型アプライアンス】

「統合型アプライアンス」市場は 2007 年度推定市場規模実績値が 182 億円（同 5.3%）となった。1 台の箱を導入して簡単な設定をするだけで、ウイルス対策、ファイアウォール、侵入検知･防御、VPN ゲートウェイ等の様々な機能を一挙に実現でき、導入が容易で管理の負荷が軽いことから、専任技術者を置くことが難しい中小事業所への導入が急速に進んでいる。特に複数事業所をまたがって企業内 WAN を形成する際に、営業所等の出先拠点の VPN ゲートウェイとして、専門管理者がいなくても比較的導入・管理が容易な小型のアプライアンスを利用する事例が増加している模様である。また、普及機クラスの製品価格が下がって導入の敷居が低くなっていることも、市場急拡大の理由として考えられる。

図 6　情報セキュリティツール市場成長率の推移



2.2.2　情報セキュリティサービス市場

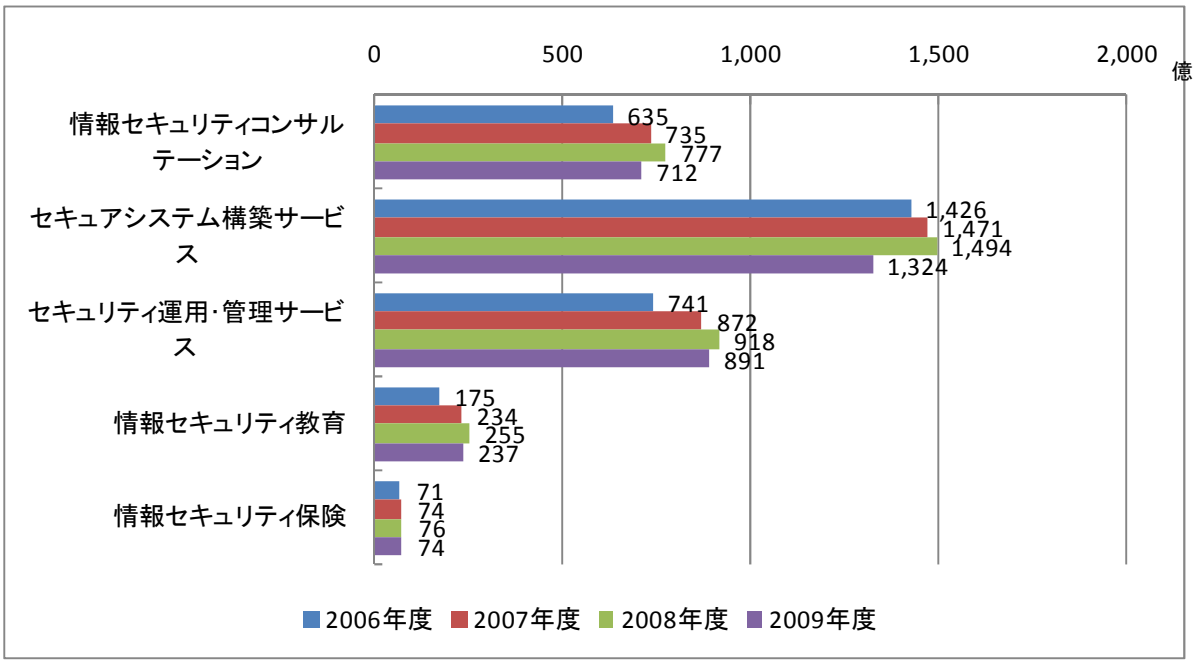
「情報セキュリティサービス」市場は、「セキュリティコンサルテーション」「セキュアシステム構築サービス」「セキュリティ運用･管理サービス」「セキュリティ教育」「情報セキュリティ保険」の 5 カテゴリに分類して集計した。（情報セキュリティツール同様、その市場分類の定義等は 5.項を参照。）以下、規模の大きい順に概要を記す。また、図 7, 8, 9 に各々情報セキュリティサービス市場のカテゴリ別の規模の推移、構成比の推移、伸び率の推移を示す。

【セキュアシステム構築サービス】

「セキュアシステム構築サービス」の市場規模は 2007 年度推定実績値で 1,471 億円（情報セキュリティサービス市場に対する構成比 43.5%）となった。このカテゴリは、セキュリティ対策

をシステムに対して付加するケースのみでなく、システムインテグレーションに際してセキュリティ機能や対策製品の組込をする場合の設計、仕様策定、セキュリティシステムの導入、製品の選定並びにそれらの支援活動といった、いわばセキュリティ SI[7]的サービスも含めたものである。一方、SI においてセキュリティを組み込むことが特別のことと意識されなくなる傾向もあり、「セキュリティサービス」として数字を認識する度合が減っている。そのために、需要の実態よりも市場規模として表れる数字が小さくなり、他のカテゴリと比較すると、殆ど成長しないかのような姿になりつつある。

図 7　情報セキュリティサービス市場規模の推移



【セキュリティ運用･管理サービス】

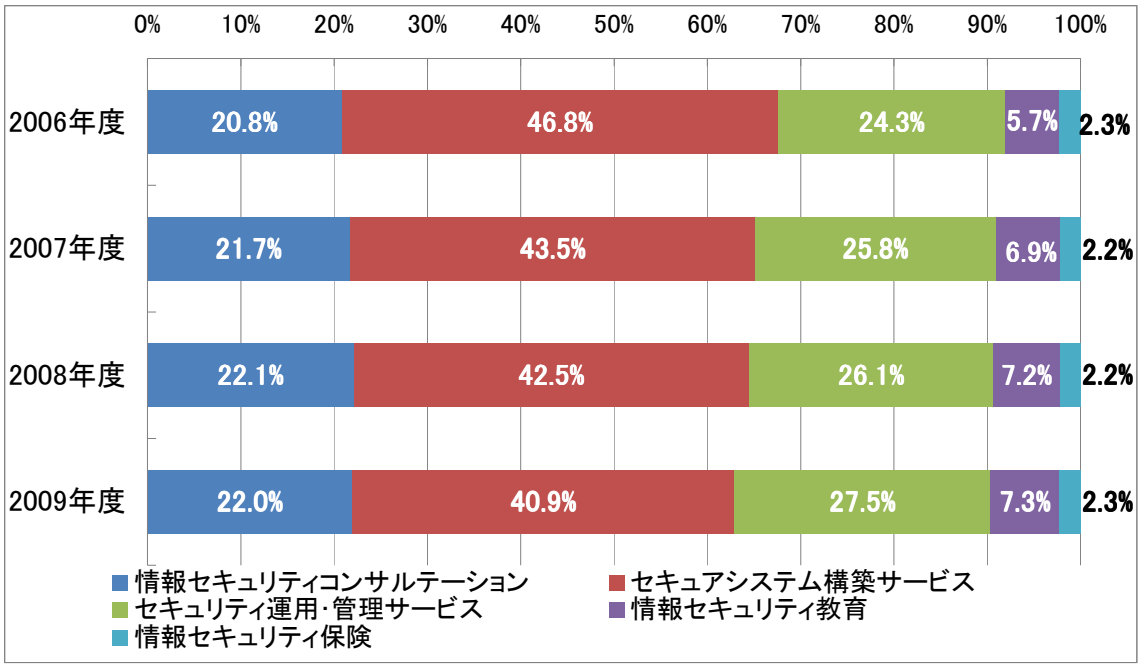
2007 年度推定実績値で 872 億円（同 25.8%）となった。このカテゴリには、ネットワーク上の不正や脅威に対して専門家の目で監視や解析をするサービスを中心に、電子認証サービスやフィルタリングサービスなど多様なサービスが含まれている。特に、複雑化･巧妙化するネットワークからの攻撃の脅威に対して、専門家のノウハウに依存した対策が必要だという考え方が浸透してきていると見られ、この分野が市場を拡大している。また、スパムメール被害の深刻化や、ウイルス感染源としてのウェブサイトの脅威が高まる中、フィルタリングサービスの活用が増加している。（対応して今回調査ではセグメントとして独立させた。）ウェブアプリケーションやサーバに、セキュリティ上の脆弱性が潜んでいないかをプロの目と手法で検査するサービスも着実に需要を伸ばしている。

[7] System Integration　システム構築

【情報セキュリティコンサルテーション】

「情報セキュリティコンサルテーション」の市場規模は 2007 年度推定実績値で 735 億円（同 21.7%）であった。このカテゴリには、全般的コンサルテーションの他、情報セキュリティポリシーの構築、情報セキュリティ監査や診断、公的認証取得支援といった目的を絞ったコンサルテーション等も含まれており、各々の活用が進んでいる。この分野は、情報セキュリティ対策の根幹である情報セキュリティマネジメント、すなわち経営の視点での情報セキュリティ対策への取組に強く関連する領域である。この分野の普及・拡大は、経営レベルでの情報セキュリティ対策への取組の浸透を示す尺度として注目される。また、内部統制への理解の進展と共に、企業のリスクマネジメント、あるいはコンプライアンス管理と一体不可分のものとして情報セキュリティを位置付ける考え方も浸透しつつあり、そういった位置付けでコンサルティングを活用する面も増えているものと推測される。

図 8　情報セキュリティサービス市場構成比の推移



【情報セキュリティ教育】

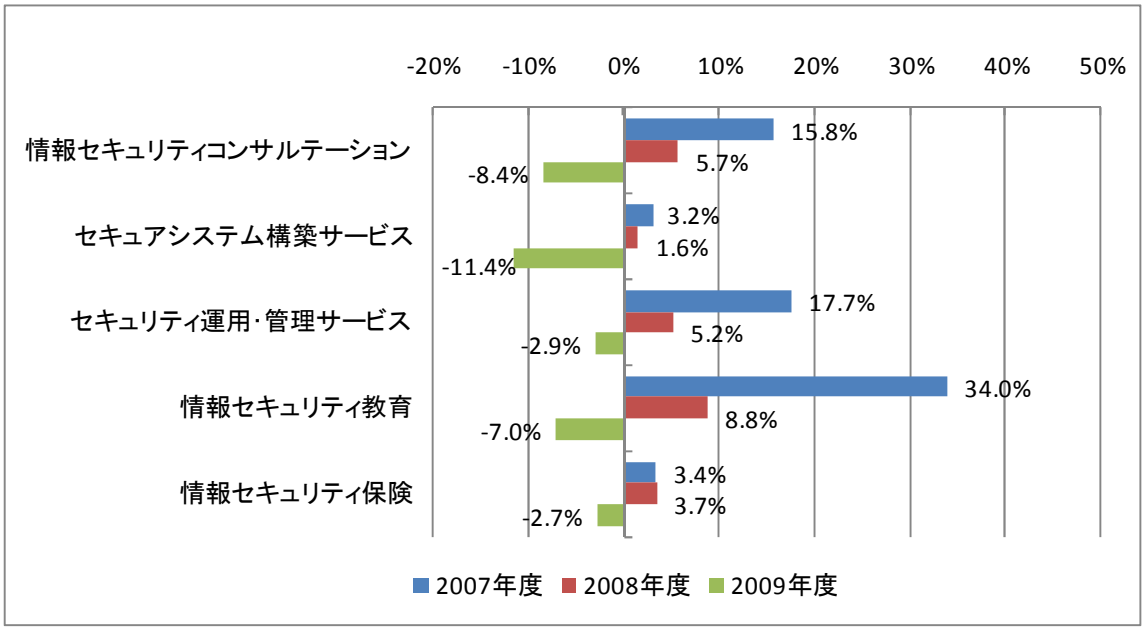
「情報セキュリティ教育」の市場規模は 2007 年度推定実績値で 234 億円（同 6.9%）であった。前年度比成長率が 34.0%と、情報セキュリティサービスの中では突出した伸び率を示している。情報セキュリティ対策、特に日常業務の中の些細なミスや不注意から情報漏えいが多発する状況から、企業が一般従業員の情報セキュリティに関する基礎知識の底上げに積極的に取り組むようになってきたことが、この高い伸びの背景にあると推察される。

【情報セキュリティ保険】

「情報セキュリティ保険」の市場規模は 2007 年度には推定実績値で 74 億円（同 2.2%）とな

った。前回の本調査においては、2005 年度から 2006 年度にかけて規模は小さいながら急速な市場の伸びを見せたが、2007 年度の前年度比は 3.4%増と微増にとどまった。当面の需要はほぼ一巡し、安定期に入ったものと考えられる。

図 9　情報セキュリティサービス市場成長率の推移



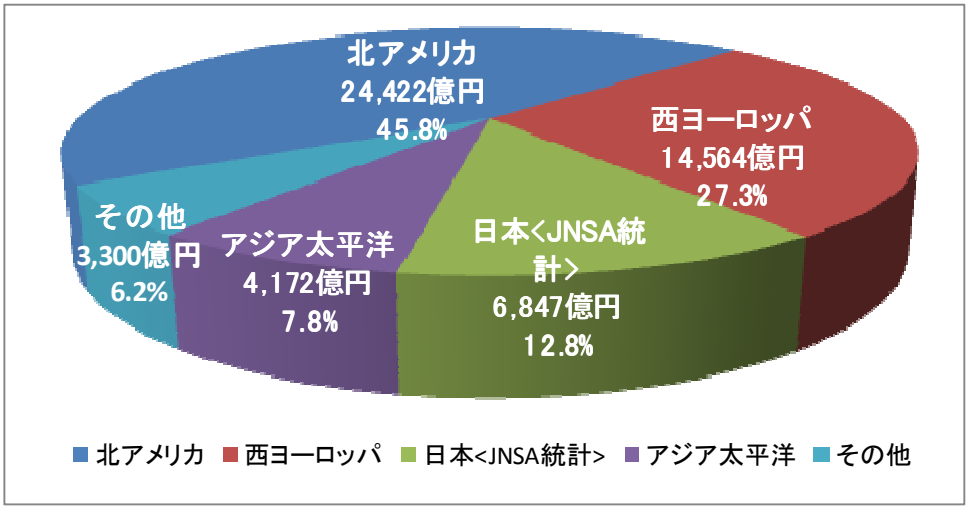
国内情報セキュリティ市場は 2007 年度に前年度比 14.7%という高い成長率を示して推定 6,847 億円の規模に達し、2008 年度にはさらに 6.1%拡大して 7,268 億円と 7,000 億円を超える規模になったと推定される。2007 年度の国内情報セキュリティ市場調査では、2006 年度の対前年度比成長率は 14.6%で、2007 年度の成長率は 11.5%程度と見ていた。今年度調査の結果、2007 年度は 2006 年度と同程度の勢いで市場が拡大したものと見られる。内部統制を含むコンプライアンス対応、事業継続管理等の要請と、相次ぐ個人情報や機密情報の漏えい事件に対する危機感が、企業の情報セキュリティ対策を一層推進した結果であると見られる。

しかしながら、米国発の金融危機とそれに触発された世界同時不況の影響は大きく、2008 年度の実績見込みベースでは 6.1%とその市場成長率は大幅に鈍化する模様である。更に、不況の影響は 2009 年度により顕著に表れてくる可能性が強く、国内情報セキュリティ産業の売上高予測値としては全体でマイナス 5.4%と縮小することが予測される。それでも金額では 6,874 億円とほぼ 2007 年度並みの数字であり、足元で 7,000 億円前後というのが、日本の情報セキュリティ産業の市場規模であると観測される。

2.3. 海外市場との比較の概要

世界の情報セキュリティ市場に関する数値は、米国の調査会社 IDC 社[8]の日本法人から提供を受けた世界市場に関する統計データを使用し（日本市場部分は本調査の数値を算入）、その数値と本調査結果の比較を行った。同報告と本調査の金額対比では、図 10 に示すように、日本は世界市場の 13%弱を占めるとの結果になった。IT 市場全体では、通常日本は世界の 10 分の 1 と言われるところに比べるとやや高い比率となる。日本の GDP の世界シェアは、IMF 統計の 2006 年の数値によると 11.6%であり、この比率に対しても日本の情報セキュリティ市場の世界シェアはやや高めであると言える。IDC 社のデータと本調査では、対象とする製品やサービスの定義では概ね一致すると見られるが、対象とする市場の範囲やデータの収集・分析方法については共通性の確認ができないため、市場捕捉率その他での差異が影響している可能性がある。

図 10　2007 年における世界の情報セキュリティ市場地域分布

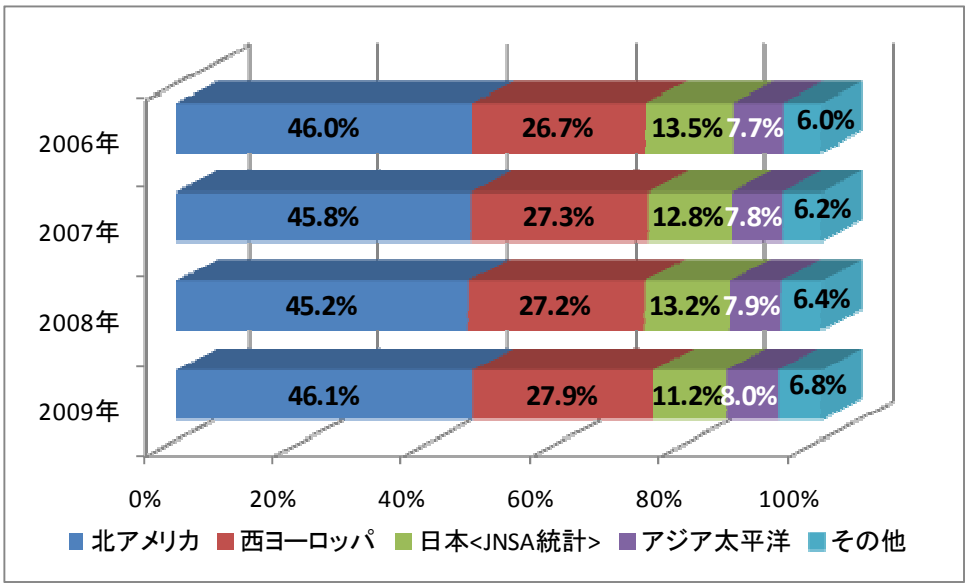


市場の伸び率に関しては、日本市場は本調査によると 2007 年度、2008 年度は各々14.7%、6.1%と、その率を下げつつも比較的高い成長を続け、2009 年度にはマイナス 5.4%と縮小するという結果となっている。世界市場は、2007 年に 20.9%と極めて高い成長を示し、2008 年は 3.5%と急にその速度を落とした後、2009 年には 10.9%と回復を示す姿となっている。IDC 社データは 2008 年 10～11 月段階で予測を行っており、同年の景気後退を一過性ととらえたためにこのような推移となったものと考えられる。

その結果、図 11 に見られるように、日本市場のシェアは 2006 年の 13.5%が 2007, 2008, 2009 年と上下動を繰り返す。2009 年には 11.2%と 2%ポイント以上下がる。これは IDC データと本調査の間で、年度ごとの市場成長率の上下に爬行性があるためと考えられるが、全体的に見ると、北アメリカ市場のシェアは横ばいであり、日本がシェアを落とす分は西ヨーロッパ、アジア太平洋、その他地域が各々シェアを上げる構造となる。これは 2009 年の予測の方向性の差が大きく作用しており、市場の見方が落ち着いた段階で修正される可能性がある。

[8] IDC: International Data Corporation　http://www.idc.com/

図 11　世界の情報セキュリティ市場地域別構成比の推移



2.4.　国内情報セキュリティ市場の概要

本調査を通じて、国内の情報セキュリティ市場について得られた観測の要点は、次のようにまとめられる。

1. 国内情報セキュリティ市場規模は 2007 年度時点で、ツール市場とサービス市場を合わせて 6,847 億円となり、前年度の 5,972 億円から 14.7%と高い伸び率で拡大した。＜2.2 項参照＞
2. 本調査期間の年平均成長率は 4.8%と、最近の日本経済の成長率や IT 産業出荷額の伸び率に比較すると著しく高い伸び率を示しており、2009 年度はマイナス成長に転じると見られるものの、趨勢としては順調な拡大が続いている。
   ＜6.1 項、6.3 項参照＞
3. 世界的には市場の拡大速度は日本に比べて一段と速く、本調査対象期間では、日本以外の地域は平均年率でいずれも 2 桁成長が見込まれている。これに比べると国内市場は世界全体や世界の各地域市場のどれよりも低い成長率を示すという結果になった。ただし、予測作業の実施時点の違いで数値が大きく動く可能性があり、その点に留意が必要である。
   ＜9.2 項、9.4 項参照＞
4. ネットワーク脅威対策製品やセキュアシステム構築サービス等の、市場規模も大きく普及度の高い製品やサービスが 1 桁台の成長に鈍化、またはマイナス成長となっている一方、システムセキュリティ管理製品、暗号製品、教育サービス等は 2006 年度～2009 年度の間の年平均成長率で 2 ケタ成長を維持するものと見られ、カテゴリによって市場の成熟度と成長速度に大きな違いがある。＜7.1 項、8.1 項参照＞

5. 情報セキュリティ対策の重点が、ネットワークへの外部からの脅威に対する防衛から、内部からの情報漏えい・流出の未然防止や抑止、内部統制対応にシフトしており、システムへのアクセスの管理やデータの暗号化、社員教育等への取組に力点が移っていると見られる。と同時に、この 1 年ほどの間にマルウェアの感染手法や侵入経路の多様化とスパムメールの激しさ等により、ネットワーク脅威も深刻さを増しており、企業はその面の対応も迫られるという厳しい事態に直面している。＜7.2 項全般及び 8.2.4 項参照＞
6. 情報漏えい対策や IT 統制対応等組織内部に対する対策の需要が拡大するのに対応して、暗号製品、ログ取得や端末管理に関する製品分野では、国産ベンダの活躍が目立つようになってきている。ただし、市場が細分化しているところへ中小規模の事業者が多く参入する状況にあり、シェア争いも厳しく、現時点では参入企業個々の事業規模は限られていると見られる。＜6.4 項、6.5 項参照＞
7. このように、国内参入企業の拡大傾向が見られるが、折からの不況の影響がどこまで及ぶかはどの事業者も見通しを持てずにおり、その多くは事業基盤が万全でないことから、産業育成策が課題となると思われる。特に IT ベンチャーからの参入に対しては、技術開発、市場開発、信用補完等の面での支援を手厚くすることにより、国内産業の存立基盤を確立する取組が必要と思われる。＜6.5 項、6.6 項参照＞

3. 調査内容

本調査の対象は国内情報セキュリティ市場である。本調査では、産業としての情報セキュリティ業界を調べる意味で、市場に参入している供給事業者の側の売上数値並びに事業の状況を調査対象としている。

調査方法は 4.項に詳述するが、①アンケート調査、②各種統計資料調査、③ヒアリング調査、④サンプリング調査等により得られたデータを基に、様々な関連要素を定量化する作業を行い、推定市場規模を導き出した。

その作業結果として、以下の推定市場規模データを算出した。

(1) 2006 年度国内情報セキュリティ市場規模　推定実績値
(2) 2007 年度国内情報セキュリティ市場規模　推定実績値
(3) 2008 年度国内情報セキュリティ市場規模　実績見込値
(4) 2009 年度国内情報セキュリティ市場規模　予測値

市場規模の数値は、市場を製品やサービスの種類ごとにいくつかに分類し、それぞれの金額規模を推定した上で全体規模を算出するアプローチをしている。そのデータに基づき、市場の解説と推定結果についての分析並びに説明を加えて、本調査報告を構成した。

なお本調査は、「2008 年 3 月 31 日時点で、国内で情報セキュリティに関するツール、サービス等の提供を事業として行っている事業者（輸入販売、再販売を含み、輸出を含まない）」を対象としている。平成 19 年度調査とは対象とする時点が異なるので調査母体に変化があり、調査対象範囲は概ね重複するものの直接の連続性はない。従い、上記の調査対象年度全てについて新たに算定作業を行っている。ただし、2006 年度の市場規模の算定に当っては、平成 19 年度調査結果も参考としている。

また、海外との比較において、上記推定結果がどのような意味を持つのかの分析も試みた。そのために、既存の国際的統計調査データを利用し、海外市場との比較検討を行った。

国内市場データと海外市場データとの比較に関しては以下の比較・分析を行った。

(1) 世界全体の市場規模データと本調査による国内市場推定規模データの比較
(2) 北アメリカ、西ヨーロッパ、アジア太平洋（日本を除く）の各地域の市場規模データと本調査による国内市場推定規模データの比較
(3) 市場分野別・地域別の構成比分布に基づく分析
(4) 情報セキュリティソフトウェアの大分類内訳レベルの地域別比較

4. 調査方法

4.1. 調査に使用したデータ及び情報

本調査で主として利用した市場規模に関するデータは、以下の通りである。

①アンケート調査

2008 年 11 月から 12 月にかけて、国内で情報セキュリティツールを販売、あるいは情報セキュリティサービスを提供していると目される事業者合計 1,141 社に対して、アンケート調査を実施し、市場規模算定に関する基礎資料とした。

このうち、情報セキュリティツールについては、流通過程が多岐に渡るため、様々な業態・立場の事業者を幅広く調査対象とすることで漏れを防ぐことを心がけた。と同時に、流通上の諸段階で数字が計上されることによるデータの重複を避けるために、流通構造の模式図を示して自社の立場を回答してもらうことで、ダブルカウントの可能性を排除する工夫をした。

また、情報セキュリティサービスについては、比較的直接エンドユーザに提供されるケースが多いと考えられるため、流通構造に係る位置付けや重複は考慮していないが、網羅性を高めるため、情報セキュリティ関連のサービスに特化した企業の他、他の事業と関連して情報セキュリティに関するサービスも提供している事業者をできる限り広く含むようにした。

調査対象とした年度は 2006 年度から 2009 年度で、基準年度を 2007 年度とした。2006, 2007 年度については実績値を、2008 年度については計画値または実績見込み値を、2009 年度については計画値または予測値を記入してもらった。年度区分については、各年の 4 月から翌年 3 月までを基準とし、極力この期間に対応する数字を回答してもらったが、年度区分が異なる企業については、直近の年度の数字での回答も可とした。

アンケートは郵送留置き、郵送回収方式で実施した。アンケートの回収件数は 140 件であり、回収率は約 12%であった。回答された数値の単純集計値は、本調査の結果得られた市場規模推定値に対して約 28.7%となっている。

②各種統計資料調査

国内の事業所、産業、投資などに関する政府及びその関連機関、並びに民間企業の資料を調査した。

③ヒアリング調査

参入事業者のうち、業界の全体像や動向を予測・分析するのに参考になる企業を中心に、情報セキュリティ事業に関する情報を統括する立場の人たちへのヒアリング調査を実施した。

④サンプリング調査

アンケートに回答が得られなかった企業のうち、業界の中核を占めると目される代表的企業については、調査員が個別に、有価証券報告書、ウェブページ、製品資料等の外部公表資料や傍証的情報からその事業の概要を推定して事業規模を算定し、集計に反映させる方法を取り入れた。

4.2. データポイントの定義

データのポイントとしては、ベンダからの出荷額ベースで計測しており、流通マージンや付加

サービス（流通・販売業者による設定サービス等）は含まない。またベンダが提供する有償の保守契約やアップデートサービスの価格は、本体製品の付帯品として、本体製品と同一区分で集計している（サービス売上にはカウントしない)。なお、認証・アクセス管理系システムやセキュリティ情報管理システムのように、全体システムを構成するに際して中核となるシステムの一部がセキュリティ機能を提供する形態のうち、そのセキュリティ機能が、セキュリティ対策全体の核機能として重要な意味を持つモジュールであるような場合は、集計対象としている。一方、例えばルータにおけるセキュリティ対応のフィルタリング機能のような、その装置の本来用途からは付帯的な機能として付加されている場合は集計対象としない。（これらの点に関する判断基準としては、モジュールやオプションのような形で切り出しが可能で価格付け対象となるか、最初から装備されている付加機能かという仕分けも援用している。）

サービスの価格についても、サービスの提供事業者からの提供価格に基づく集計を行った。集計対象としたのは、後に示すサービスの定義に該当するサービスの範囲に対応する数字となる。いわゆるシステムインテグレータが、システムインテグレーションの一部として情報セキュリティに関するサービス（定義範囲内のもの）を提供する場合は、その部分の価格が明示的に把握できる場合に、その売上のみを集計対象としている。また、そのようなケースで情報セキュリティツールの設定サービス等がセキュアシステム構築サービス等の金額に含まれる場合には、例外的にツールの「付加サービス」がサービス売上として計上され、本調査対象に含まれることがある。

4.3. 市場規模実績推定値の算出方法

本調査では、情報セキュリティベンダに対するアンケート調査で得られた集計数値をそのまま市場規模の数字とはせず、全体集計に際しての利用データの一部と位置付けている。

アンケート方式で数字を把握する場合の問題点として、①調査する側とされる側の製品分類や定義の差があり、質問に対応する数字を被調査企業で把握していないケース、②関連するサービスの一部がセキュリティに関わる部分であるが､その部分だけの対価が算出されていないために、参入有無では参入ありと回答しつつ金額数字の回答がないケース、③主として外資系企業で、情報開示に関する規制から、日本でのデータが一切公開されないケース　等があり、アンケートのみに依存する、市場の数量的把握には限界がある。

このようなことから、数字的限界を補う意味で、サンプリングによる推定数値を取り入れている。アンケート調査対象とした約 1100 社のうち､アンケート回答が得られなかった企業の中で、市場規模を推計する上で重要と考えられる企業 286 社を抽出し､事業規模の推定を行った。なお、アンケート回答を得た企業についても、JNSA 独自の調査を実施し、アンケート回答との突合・検証を行っている。集計対象企業の、本調査における市場区分に対する分布は、表 2 に示す通りである。情報セキュリティ保険を除き、概ね各市場カテゴリに 70 社から 150 社程度の参入が見られる。

表 2　国内情報セキュリティ市場推計対象企業及びその分布

国内情報セキュリティ市場 推計対象企業数と分布	対象企業業態区分								
		海外ベンダ/日本法人	国内ベンダ	流通・販売業者	SI/NI機能ありの二次・三次販売業者	大手システムインテグレータ	コンサル会社	サービス提供事業者	その他
	合計	A	B	C	D	E	F	G	H
調査推計対象（含：アンケート回答129件）	381	49	54	32	***108***	27	17	*78*	16
有効推計対象	358	47	52	30	***100***	26	17	*73*	13
情報セキュリティツール全体（X）	245	46	*47*	27	***79***	24	0	18	4
統合型アプライアンス	***68***	8	4	12	***26***	*13*	0	5	0
ネットワーク脅威対策製品	***121***	*21*	10	16	***47***	17	0	9	1
コンテンツセキュリティ対策製品	***129***	17	14	*19*	***48***	16	0	12	3
アイデンティティ・アクセス管理製品	***117***	9	19	19	***43***	*21*	0	6	0
システムセキュリティ管理製品	***134***	*23*	20	19	***43***	18	0	9	2
暗号製品	***95***	6	15	13	***39***	*18*	0	3	1
情報セキュリティサービス全体（Y）	248	11	20	15	***82***	23	17	*70*	10
情報セキュリティコンサルテーション	***165***	7	9	8	***51***	19	17	*53*	1
セキュアシステム構築サービス	***114***	5	7	10	***53***	*20*	6	13	0
セキュリティ運用・管理サービス	***145***	7	16	9	***49***	17	10	*33*	4
情報セキュリティ教育	***91***	5	4	6	*19*	16	11	***28***	2
情報セキュリティ保険	***8***	0	0	1	2	*1*	0	0	***4***
（参考）									
ツール専業（X∩^Y）	110	***36***	*32*	15	18	3	0	3	3
ツール・サービス兼業（X∩Y）	135	10	15	12	***61***	*21*	0	15	1
サービス専業（^X∩Y）	113	1	5	3	*21*	2	17	***55***	9

なお、A～H の区分は参入企業の主たる業態を示すもので、各々、

A：海外メーカまたはその日本法人

B：国内のセキュリティツールメーカ

C：販売店・商社等主として流通機能の企業

D：SI・NI[9]機能を有する二次・三次販売店

E：SI が主たる付加価値の大手システムインテグレータ

F：コンサルティング企業

G：セキュリティサービス提供事業者

H：その他

を意味する。

この区分を導入することにより、市場参入者の立場による分布を見ることができると同時に、流通構造上の数値計上の重複を回避する参考に役立てている。また、市場の将来予測においても、流通機能の持つ役割の面から成長度合を加減するに際して有効なパラメータの役割を果たしている。

以下、各々の業態の概要を記す。

A　海外メーカまたはその日本法人

海外メーカとは、情報セキュリティ製品の開発製造販売元である海外のメーカを指している。日本に製品やサービスを提供する海外メーカの多くは、日本に子会社となる法人を設立している。支店の形で拠点を設ける場合もある。また自ら日本に組織を持たず、日本国内のパートナーを販売代理店として製品・サービスの提供をする場合もある。日本法人

[9] NI：Network Integration, ネットワーク構築

を設立する場合、100%子会社とする場合と国内パートナーとの合弁形式とする場合がある。

直接進出をする場合も、国内での販売・流通の多くを国内の販売パートナーに依存する形態が一般的である。日本の流通構造は複雑で既存の取引関係が重視されることや、直接人対人のコミュニケーションが重視されることから、すでに販売ネットワークを持つ国内企業との提携が合理的だからである。

B　国内のセキュリティツールメーカ

セキュリティ製品がネットワーク脅威対策製品中心だった時期は海外メーカへの依存度が極めて高かったが、個人認証や端末のポリシー管理関連、暗号製品の分野では国内のセキュリティツールメーカの台頭も目立つ。参入例の多くは国内のベンチャー系ソフトウェアハウスやシステムハウスである。一部に大手製造事業者やその関連会社の参入もあるが、それら事業者の事業の主体がシステムインテグレーション等であるケースが多いので、本統計ではDまたはEに区分している。

国内のセキュリティツールメーカの流通構造は、一部を除き、販売パートナー経由でエンドユーザへ提供するパターンが一般的である。海外メーカと同様に既存の販売ネットワークに依存するモデルが多い。また、国内の大手システムインテグレータに標準取扱製品の認定を受けることで、その販路に乗って製品供給を拡大するケースも多く見受けられる。

C　販売店・商社等主として流通機能の企業

日本国内の流通構造においては、総合商社や専門商社が海外製品のみならず国内製品についても重要な役割を果たしている。IT 関連の部品や製品も、多くはその流通機能に依存しており、セキュリティ製品も例外ではない。

セキュリティ製品の場合、特に海外メーカの製品のウェイトが高いことから、輸出入を主要事業とする総合商社や、その子会社として特定分野で小回りを利かせる技術商社が国内総代理店的な立場で取り扱うケースが多い。また、独立系でも特定分野に特化した業態の専門商社あるいは技術対応能力を備えた技術商社が活躍する事例も多い。IT分野では、電機メーカの販売代理店を出発点として技術対応能力も備える販売特化型の企業もある。

D　SI・NI 機能を有する二次･三次販売店

区分Eで定義する大手システムインテグレータは、規模別、分野別、ソリューション別等に細分して、あるいはコスト構造対策から、多くの SI 子会社を抱えるケースが多い。それら子会社は、システム構築における差別化戦略として、セキュリティ対策製品で特徴あるものを、二次･三次の販売店として、あるいは一次代理店として取り扱うケースが多い。二次店といっても、海外メーカの場合、一次店は流通に特化した卸売専念型のケースもあり、技術サポートやインテグレーションを必要とするケースの多いセキュリティ製品においては、流通の中核的機能を担う部分とも言える。

この区分には、前項に記した技術商社系で SI や NI に軸足を置く業態や、次項「SI が

主たる付加価値の大手システムインテグレータ」の子会社、電機以外の製造業のシステム子会社から発展したSI事業者、独立系の中堅SI事業者等が入る。背景も多彩なことから、この区分に属する企業数は他の区分に比べて多い。また、SI の中でセキュリティ製品を取り扱うことから、その周辺の付加価値サービスや、情報セキュリティ関連サービスを併せて提供するケースも多い。

E　SIが主たる付加価値の大手システムインテグレータ

メインフレームコンピュータを製造するような大手電機メーカは、その IT 事業の主力がシステムインテグレーションになってきている。大手の通信事業者も、通信ネットワークと IT がシステム的に一体化の要素を強めるのに対応して、自らあるいは子会社形態でインテグレータ機能を強化している。更に、データ処理サービス系等を源流とする独立のシステムインテグレーション専業の準大手・中堅企業群がある。

これら業態は、システムインテグレーションの中でセキュリティ製品を取り扱うと共に、その周辺のサービスや、システムセキュリティの設計・構築、更にはそれらの基本となる上流コンサル等のサービスも提供している。またシステムに関する総合力を要求されることから、セキュリティツールに関しては自社の標準取扱製品だけでなく、自グループ内の他社の取扱製品も含めて幅広く品揃えする傾向にある。

F　コンサルティング企業

経営コンサルティング企業が情報セキュリティに関してもコンサルティングを行うケースが以前からある。独立系の経営コンサルティング企業、大手企業グループの調査部門等を母体とするシンクタンク、会計監査法人がサービス提供のために別会社化している経営コンサルティング企業等が、情報セキュリティに関してもマネジメント支援を提供するケースが一般的である。

情報セキュリティは情報資産に関わるリスクを取り扱うが、情報資産は経営管理に直結する要素が強いので、両者の間に親和性があると言える。リスク管理の一環としての情報セキュリティ対策の導入という位置付けである。特に内部統制報告制度が制定されて以降は、IT ガバナンスの一環としての情報セキュリティ管理という位置付けがより見えるようになり、内部統制体制構築面での支援もセキュリティコンサルティングとして提供されるようになっている。

G　セキュリティサービス提供事業者

セキュリティサービスに特化した、あるいはそれに近い業態の事業者である。コンサルティングサービスや運用・管理サービスの領域で専門的サービスを提供するケースが多い。ISMS やプライバシーマーク等の認証取得支援コンサルティング、システム構築やセキュリティ製品評価等の導入支援、ファイアウォール等の運用管理アウトソーシング、脆弱性検査やインシデント対応等のプロフェッショナルサービスの各領域に特化し、あるいはそれらのいくつかを取り合わせて、専業に近い業態で事業展開している。従い、企業規模は

小さいケースが多い。

また、海外企業は製品メーカ業態が多いが、認証サービスその他、サービスに主体を置いた専業事業者の日本市場参入の事例もいくつかある。

H　その他

その他には保険事業者や、製造業で特定のセキュリティ製品を例外的に供給している事例等をまとめた。

4.4. 市場規模の予測値の算定方法

2008 年度、2009 年度の市場規模推定にあたっては、2007 年度の市場規模実績値の推定値を基に、いくつかの要素を加味して推計作業を行った。

アンケート調査にベンダが回答した事業計画あるいは売上予測の数値と、その成長率のデータを基本的データとして用いた。今回のアンケートでも、予測値または計画値については、実数による回答が得られにくいことから、事業規模と売上成長率について、数字の幅で区分を区切り、その区分により回答を求める試みを行った。これにより、市場区分ごとの事業規模や成長度合の程度を理解する参考とした。また、同じくアンケート調査の最後には、自社の事業だけでなく、業界としての動向、顧客の関心の向いている分野について、回答企業がどう見ているかを問うた。これにより、供給サイドや需要サイドのマクロの方向感を得るための参考にした。

また、各市場区分（セグメント単位）での動向もしくは傾向（市場としての伸びの強度）や、各業態（上記表 2 におけるA～Hの区分）における事業展開のマクロ的趨勢を変動パラメータとして加味することで、市場変化の予測値をダイナミックにシミュレーションするアプローチを試みた。

5. 情報セキュリティ市場の分類及び定義

今回情報セキュリティ市場の規模をベンダ側の数値を基に算出するに際して、市場の区分として、「ツール」と「サービス」という、特性の異なる二つの市場を定義した。各市場は、それぞれを更に大分類、中分類の 2 段階で区分した。以下、便宜的に大分類レベルの各市場区分をカテゴリ、中分類レベルのそれをセグメントと呼ぶ。

「ツール」とはハードウェア製品もしくはソフトウェア製品である。「製品」という表記ではソフトウェアライセンスが含まれないイメージとなることを避けるため、「ツール」という表現としている。また、サービスに対応する「有形物」のイメージとしてもなじみやすいと考えた。ビジネスモデル的には単価と数量により定義が可能で商品的に取引され流通する形態のものが中心である。ただ、一部のソフトウェア商品は、ダウンロード販売のように、物の形を取らないまま取引される場合もある。

「サービス」は、「ツール」のように「モノ」としてのやり取りが存在せず、無形の役務提供をビジネスモデルとするものを、基本的に対象としている。「サービス」は、定期開催型教育コースや侵入検査サービスのように定型化・メニュー化され定価設定されるパターンのものと、システム構築やカスタムコンサルテーションのように、供給者と需要者の個別的・相対(アイタイ)的取引で提供され消費されるビジネスモデルの 2 パターンを想定している。ただし、市場区分においてこのパターンを分類の基準とはしていない。取引形態よりはサービスの目的、提供する機能の種類を基準として分類している。

本調査で用いた市場分類体系は、以下に示す通りである。5.1 にその一覧表を、5.2 に各大分類レベルの市場区分に対する簡単な説明を記す。

5.1. 情報セキュリティツール･サービスの市場分類定義表

表 4、表 5 に、本調査のアンケート調査に際して使用し、回答者に示した「情報セキュリティツール」「情報セキュリティサービス」の市場区分とその定義もしくは説明･例示等の一覧表を掲げる。なお、表 3 には、表 4、表 5 で使用した用語･略号等の説明を載せた。

表 3 用語説明

アプライアンス	ハードウェアとソフトウェアを一体として特定の機能を提供する販売形態をとる製品
ソフトウェア	パッケージ製品、ダウンロード製品、ライセンス販売製品等、定型化されたもの 一部カスタマイズの場合は対象に含め、完全な個別開発ソフトウェアは含まない
AV	アンチウイルス
FW	ファイアウォール
IDS	イントリュージョンディテクションシステム（侵入検知システム）
IPS	イントリュージョンプリペンションシステム（侵入防止システム）
PKI	パブリックキーインフラストクチュア（公開鍵暗号基盤）
SSL	セキュアソケットレイヤー。暗号通信の一方式
URL	ユニファイドリソースロケーター。統一資源位置指定子
VPN	バーチャルプライベートネットワーク

表 4　情報セキュリティツールの市場分

大分類	中分類	定義、説明、例示　等
情報セキュリティツール		
統合型アプライアンス		
「ネットワーク脅威対策製品」と「コンテンツセキュリティ対策製品」に分類される機能のいずれかまたは両方を備え、二つ以上の大分類カテゴリにまたがる複数の機能を 1 台（またはセット）で提供するアプライアンス製品。	統合型アプライアンス	アンチウィルス・アンチワーム・不正プログラム対策（スパム対策・フィッシング対策機能を併設するものを含む）, FW, IDS／IPS, VPN のうち、少なくとも二つ以上の機能を装備したアプライアンス製品。（いわゆる「複合脅威対策」<Unified Threat Management =UTM=>製品でアプライアンス型であるもの） 二つ以上の大分類カテゴリにまたがる複数の機能を 1 台（またはセット）で提供するアプライアンス製品で UTM 以外のもの。 ただし、FW と VPN だけの組合せはファイアウォールアプライアンスに含める。
ネットワーク脅威対策製品		
主としてネットワークの境界付近に配置して通信のハンドリングまたはモニタリングを行い、設定に基づいてネットワーク通信の許可･不許可、アラート、ログ生成等、通信の制御と管理を行う製品。 通信パケットに暗号化を施し、組織外のネットワーク上でのパケット内容の盗聴・改ざんを防止する、いわゆる VPN(Virtual Private Network)製品を含む。 ファイアウォール、VPN 製品、侵入検知･侵入防止製品(IDS／IPS)等を含む。	ファイアウォールアプライアンス	ネットワーク上の通信を解析し、送信元アドレス、送信先アドレス、プロトコルの種類、ポート番号、通信のステータス等の情報に基づき、あらかじめ設定されたルールまたはポリシーに従って、通信の許可、遮断、制御を行う製品のうち、アプライアンス型製品。 VPN 機能を併設するものを含む。
	ファイアウォールソフトウェア（企業向けライセンスタイプ）	ネットワーク上の通信を解析し、送信元アドレス、送信先アドレス、プロトコルの種類、ポート番号、通信のステータス等の情報に基づき、あらかじめ設定されたルールまたはポリシーに従って、通信の許可、遮断、制御を行う製品のうち、ソフトウェア型製品で、サーバ型トポロジーで使用されるもの。 VPN 機能を併設するものを含む。
	ファイアウォールソフトウェア（デスクトップ FW）	ファイアウォールソフトウェアであって、クライアント上で動作する製品。（デスクトップファイアウォール、パーソナルファイアウォール等） VPN 機能を併設するものを含む。 クライアント用ウイルス対策製品に併設されるファイアウォールはウイルス対策製品に分類する。
	VPN アプライアンス	ネットワーク上の通信に暗号化処理を施して、通信系路上で第三者からの盗み見、改ざん等を防止し、閉じたネットワークのような通信を可能にする機能（VPN= Virtual Private Network=機能）を提供するアプライアンス型製品。SSL(Secure Socket Layer)-VPN を含む。 ファイアウォールに VPN 機能が付帯する場合はファイアウォールに分類。
	VPN ソフトウェア	ネットワーク上の通信に暗号化処理を施して、通信経路上で第三者からの盗み見、改ざん等を防止し、閉じたネットワークのような通信を可能にする機能（VPN= Virtual Private Network=機能）を提供するソフトウェア製品。サーバ（ゲートウェイ）型、クライアント型の双方を含む。SSL(Secure Socket Layer)-VPN を含む。 ファイアウォールに VPN 機能が付帯する場合はファイアウォールに分類。

		IDS／IPS アプライアンス	侵入検知（Intrusion Detection System =IDS=）・侵入防止（Intrusion Prevention System または Intrusion Protection System =IPS=）、すなわち、ネットワーク上の通信の内容や状態を一定の方法・技術に基づき判断し、侵入もしくは攻撃と判断される通信に対して報告・警告・遮断・阻止・監視・ログ記録等の対策を行う製品のうち、アプライアンス型製品。
		IDS／IPS ソフトウェア	侵入検知<Intrusion Detection System =IDS=>・侵入防止<Intrusion Prevention System または Intrusion Protection System =IPS=>、すなわち、ネットワーク上の通信の内容や状態を一定の方法・技術に基づき判断し、侵入もしくは攻撃と判断される通信に対して報告・警告・遮断・阻止・監視・ログ記録録等の対策を行う製品のうち、ソフトウェア型製品。
		アプリケーションファイアウォール	アプリケーションサーバへのネットワーク通信を監視・解析し、不正侵入その他攻撃・悪用を目的とする通信に対して報告・警告・遮断・監視・ログ記録等の対策を行う製品。（アプライアンス型、ソフトウェア型の双方を含む） 典型的例として、ウェブアプリケーションファイアウォールがある。データベースサーバの保護を主目的とするものを含む。
		その他のネットワーク脅威対策製品	外部ネットワーク（インターネット等）から内部ネットワークに対して行われる、不正侵入、盗聴、不正プログラムの挿入などの攻撃に対して、検知、防御、抑止、警告などの防衛の機能を提供する製品で他の中分類に属さないもの。
コンテンツセキュリティ対策製品			
	1．コンピュータウイルス、スパイウェア、ボット等の不正プログラム、マルウェアなどを、ファイル等の電子データや電子メール送受信・ウェブ閲覧等のコンピュータ通信の中から検出し、排除・無害化・警告等の対策を講じる機能を持つ製品群。 2．システム・業務・サービスの目的や適正な運営にとって有害な電子メール送受信やウェブ閲覧等の通信を検査し、フィルタリング・警告・排除・ログ記録その他の対応を行う機能を持つ製品群。 3．電子メール、電子ファイル等の内容（コンテンツ）について、ポリシー等あらかじめ設定された条件に基づいて、その送信・移送・受け渡し等の移動、複製・閲覧・編集・印刷等の加工その他の利用を阻止・防止もしくは制限し、または警告・報告・記録等を行う、情報保護のための製品群。	ウイルス・不正プログラム対策ソフトウェア（企業向けライセンス契約）／アプライアンス	ウイルス、ワームその他の不正プログラムの感染や侵入を検知・防御・排除する機能を持ったソフトウェア（主として企業等向けにライセンス契約方式で提供されるもの）またはアプライアンス。 ゲートウェイ型、サーバ型、クライアント型の全てを含む。 付加機能として FW、IDS、スパム対策、URL フィルタリング等の機能を併設するものを含む。
		ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ）	ウイルス、ワームその他の不正プログラムの感染や侵入を検知・防御・排除する機能を持った、主として個人使用のクライアントパソコン向けソフトウェア。主としてパッケージ形式もしくはオンラインダウンロード形式で販売されるもの。プログラムや定義ファイル更新の年次参照権の販売を含む。 デスクトップファイアウォール、HIPS（ホスト IPS）、スパム対策、URL フィルタリング等の機能を併設するものを含む。
		スパムメール対策ソフトウェア／アプライアンス	無差別・大量に送りつけられる、不要もしくは有害な内容を含む宣伝・勧誘目的等の電子メール（スパムメール）をフィルタリングし、マーキング、警告、分別、排除等を行うソフトウェアもしくはアプライアンス製品。 ウイルス・不正プログラム対策製品にこの機能が併設される場合は、ウイルス・不正プログラム対策製品に分類する。
		フィッシング対策ソフトウェア／システム	いわゆるフィッシング詐欺目的で送付される電子メールのフィルタリング、フィッシングサイトへのアクセスや閲覧に対する警告、ウェブサイトのフィッシングに関する安全性の確認等の機能を提供する、ソフトウェア、システムもしくはサービス。（一般的なサイト証明書の発行サービスは「運用・管理サービス」に分類する。） ウイルス・不正プログラム対策製品にこの機能が併設される場合は、ウイルス・不正プログラム対策製品に分類する。

		URL フィルタリングソフトウェア／アプライアンス	インターネット上のウェブサイト（ホームページ）へのアクセスや閲覧につき、そのアドレスや内容が、所定の条件（有害、危険、不適格、Reputation Service によるリスト等）に合致（もしくは違反）する場合に処理（停止、警告、管理者への通報、ログ保存等）を行うソフトウェアもしくはアプライアンス製品。 ウイルス・不正プログラム対策製品にこの機能が併設される場合は、ウイルス・不正プログラム対策製品に分類する。
		メールフィルタリングソフトウェア／アプライアンス	送受信される電子メールにつき、そのアドレスや内容、添付ファイル等を検査し、所定の条件（有害、不適格、情報漏えい、Reputation Service によるリスト等）に合致（もしくは違反）する内容を含むものに対して処理（停止、隔離、警告、管理者への通報もしくは回送、ログ保存等。単に全メールを無条件にアーカイブするだけのものを除く。）を行うソフトウェアもしくはアプライアンス製品。 ウイルス・不正プログラム対策製品にこの機能が併設される場合は、ウイルス・不正プログラム対策製品に分類する。
		その他のコンテンツセキュリティ対策製品	組織内（あるいは個人）と組織外の間でネットワーク通信その他の方法で受け渡しされる電子データに関して、主としてセキュリティの目的でフィルタリングその他の機能を提供する製品で、上記のいずれにも属さない、あるいは特定の中分類に仕分けできないもの。 いわゆる Digital Rights Management(DRM)製品やシステム、DLP (Data Loss/Leak/Leakage Protection/Prevention) 製品やシステムを含む。
アイデンティティ・アクセス管理製品			
	ネットワーク資源、コンピューティング資源のユーザを電子的手段で特定し、ユーザごとに定義されたアクセス権等に基づいて、ネットワーク資源・コンピュータ資源へのアクセスや利用の許可を行う機能を提供する製品群。 本人特定（アイデンティファイ）と認証、アクセス権限の付与と管理、電子証明の発行と管理等の機能を提供する。 いわゆる Authentication, Authorization, Access Control の機能を提供する製品群。	個人認証用デバイス及びその認証システム	ワンタイムパスワード、IC カード、USB キー、携帯電話等を用いて本人確認する機能を提供するデバイス及びそのシステム（生体認証を除く）。
		個人認証用生体認証デバイス及びその認証システム	指紋、静脈等の生体の特長のみならず、声紋、筆跡等身体的特徴に着目して本人を特定する機能を提供するセンシングデバイス及びその認証システム。
		アイデンティティ管理製品	システム並びにデータへのアクセス権について、システムの利用者に対してはその職務や権限に基づく定義のデータベースを、システム並びにアプリケーションに対してはそのアクセス許可ポリシーを管理する機能を提供する製品群。 利用者の異動に伴う変更管理や、システム間のアクセス権の情報連携や統合管理を実現し、情報資産の利用権の即時的一元的管理を可能にする。
		ログオン管理／アクセス許可製品	ユーザがシステムにアクセスする際の承認・許可機能を持つ製品分類。 シングルサインオン、フェデレーション等を含む。 但し、個人認証用及び個人認証用生体認証デバイスと一体で機能するシステムは当該各デバイス及び認証システムに分類する。
		PKI システム及びそのコンポーネント	電子証明書の発行、管理、証明サービスを提供するシステム及びその構成要素。 但し、構築サービス(SI)は含まない。（サービス市場に分類する） なお、電子証明書の発行サービスはサービス市場に分類する。
		その他のアイデンティティ・アクセス管理製品	本人認証、アクセス権管理、ログオン管理等の機能を提供しまたはそれらに関連する機能・サービスを提供する製品で上記のいずれにも属さない製品。 ディレクトリシステムを含む。

システムセキュリティ管理製品			
	1．ネットワークやコンピュータを構成する機器やデバイスの情報を入手し、その状態や属性や設定や動作の監視・診断・制御・記録等の機能を持つ製品群。 2．ファイル等の電子データの移動･複製･編集その他の処理を中心としたコンピュータの動作について監視･制御･記録･警告等をする製品群。 3．ネットワークに接続するデバイスの設定状態等を確認し、接続の可否を制御･管理する機能を持つ製品群。 4．その他、コンピュータとネットワークの状態や動作をセキュリティ面から管理する機能を持つ製品群。	セキュリティ情報管理システム／製品	FW 等のセキュリティ監視･制御装置のログまたはサーバのイベントログ等の情報を統合･監視･分析し、ネットワークシステムのセキュリティ状態を総合的に管理する機能を持つ製品及びシステム。 統合ネットワーク管理プラットフォームのうちセキュリティ管理モジュールの製品部分も統計対象とする。
		脆弱性検査製品	検査対象となるサーバ等に対し、スキャニングや擬似攻撃を行い、脆弱性や設定の不備等、危険事項を検査し報告する製品群。いわゆる脆弱性スキャナー（ネットワークベース、ホストベース）。
		ポリシー管理・設定管理･動作監視制御製品	1．OSやアプリケーションの設定、パッチ適用、バージョン等を監視･管理する製品群 2．クライアントマシン等におけるファイルのコピー･印刷その他の操作を監視･制限･制御等する製品群。 3．クライアント PC 等の識別情報やインベントリ情報等を収集・分析・管理し、ポリシー等の設定された条件に合致しないアプリケーション等のインストール等の管理（警告・報告・禁止・削除等）を行う製品･システム。 4．その他個別のマシンの設定、状態、動作等に着目してセキュリティを管理する製品群。 5．クライアント PC 等の識別情報やインベントリ情報等に基づきネットワーク接続を管理･制御する製品･システム。いわゆる「ネットワーク検疫システム」における機器認証サーバを含む。原則として単体製品またはネットワーク制御装置等のオプションとして取引対象となる製品形態のものを対象とし、その機能がルータ等の一部にデフォルトとして組み込まれている場合は対象外とする。
		その他のシステムセキュリティ管理製品	コンピュータネットワークシステムの、システムとしての状態を監視・解析・管理する機能を持った製品群のうち、上記セグメントのいずれにも分類されない製品群。主としてセキュリティ、内部統制管理等を目的としてログの収集、減量・圧縮、保管･アーカイブ、解析等を行う製品、ならびにいわゆるデジタルフォレンジック製品等を含む。ただし、ログ収集･解析機能を提供する製品のうち、リアルタイム監視を主目的とする製品は「セキュリティ情報管理システム／製品」に分類し、当分類では主に傾向解析等スタティックな目的のものを対象とする。
暗号製品			
	データの暗号化を主たる機能とする製品群。 通信経路に対する防御を主目的に通信の暗号化を行う、いわゆるVPN 製品は、「ネットワーク脅威対策製品」に分類する。	データ暗号化製品	メール、ファイル、ディスク、記憶デバイス等のデータを暗号化することで権限外使用、覗き見、改ざん、漏えい等を防止することを主たる機能とする製品群。
		暗号化ミドルウェア	暗号ライブラリ等の中間製品で単独で取引されるもの。
		その他の暗号製品	暗号化することでセキュリティの目的を満たすことを主たる機能とする製品で上記に属さないもの。 ただし、電子証明書発行システムは「アイデンティティ・アクセス管理」に、その関連サービスはサービス市場に分類する。

表 5　情報セキュリティサービスの市場分類

大分類	中分類	定義、説明、例示　等
情報セキュリティコンサルテーション		
1. 情報セキュリティについて、主として経営管理及びIT管理の領域において、管理のための政策、管理体系、運用体系等の構築、診断、監査に関する支援やコンサルティングを行うサービス。 2. これらに関連する規格認証枠組みに対応して認証取得を目指す場合の支援サービス及び規格等の審査･認証サービス。 3. これらに類似または直接関連するコンサルティングサービス。	情報セキュリティポリシー構築支援	情報セキュリティポリシーや管理･運用基準等の構築サービス。
	情報セキュリティ管理全般のコンサルテーション	情報セキュリティの管理の体制や手順に関する総合的コンサルティングサービス。 情報セキュリティガバナンスの構築・取組支援サービス・コンサルテーションを含む。
	情報セキュリティ診断･監査サービス	情報セキュリティのポリシー、システム、管理体制、コンプライアンスの現状に対して診断または監査を行うサービス。ITシステムの弱点を擬似ネットワーク攻撃等で検査するサービスは「セキュリティ運用･管理サービス」の中に位置付ける。ここでは管理体制等に対する総合的診断サービスを主体とするサービスを対象とする。
	情報セキュリティ関連規格認証取得等支援サービス	情報セキュリティ監査の受審、情報セキュリティ格付けの取得、ISMS適合性認証の取得、プライバシーマーク適合認定の取得等を支援するサービス。
	情報セキュリティ関連認証・審査・監査機関（サービス）	情報セキュリティ監査、情報セキュリティ格付け、ISMS適合性認証、プライバシーマーク適合認定等を行うサービス。
	その他の情報セキュリティコンサルテーション	その他の情報セキュリティ管理に関するコンサルティングサービス。
セキュアシステム構築サービス		
ITセキュリティシステム、またはITシステムのセキュリティについて、構築を支援するサービス。 ただし、セキュリティツールやそのプラットフォーム自体の価格は含めず、その導入や構築といった役務･サービス部分を集計対象とする。	IT セキュリティシステムの設計・仕様策定	ITシステムのセキュリティについて、その設計、仕様の定義、要求条件の設定等の全体の枠組み、あるいは特定機能の内容について策定するサービス。
	IT セキュリティシステムの導入・導入支援	ITセキュリティシステムまたはITシステムのセキュリティに関する、システムインテグレーションサービス。 原則として設計部分を除く導入部分のみとするが、両者が不可分の場合はこの分類に集計する。
	セキュリティ製品の選定・選定支援	顧客のポリシーや要求条件に基づいて、それに適したITセキュリティ対策製品を選定し、またはそのための情報提供等の支援を行うサービス。
	その他のセキュアシステム構築サービス	その他の IT セキュリティシステム構築サービス。
セキュリティ運用･管理サービス		
1. ITセキュリティシステム、またはITシステム上のセキュリティ対策機器等の運用や管理の支援を行い、状態の監視、安全対策に対する診断、インシデント等に際しての判断や対応の実施や支援を行うサービス。	セキュリティ総合監視・運用支援サービス	ネットワークシステムのセキュリティ状態を総合的に監視し、またその運用を支援するサービス。 関連するログ解析サービスを含む。
	ファイアウォール監視・運用支援サービス	ファイアウォール等の運転状況やアラート等を監視し、またその運用を支援するサービス。 関連するログ解析サービスを含む。
	IDS／IPS 監視・運用支援サービス	IDS／IPS システム等の運転状況やアラート等を監視し、またその運用を支援するサービス。 関連するログ解析サービスを含む。

	2. ITシステムの運用等に関連する各種の情報･利便･機能等を提供するサービス。	ウイルス監視･ウイルス対策運用支援サービス	コンピュータウイルス等の不正プログラム等に対して監視や対策を行い、またその運用を支援するサービス。関連するログ解析サービスを含む。
		フィルタリングサービス	電子メールの送受信に際して、スパムメール等の有害メール対策や情報漏えい防止のためのフィルタリングもしくは監視を行うサービス。 電子メールサーバ機能の提供と一体で提供されるサービスを含む。 インターネット上のウェブアクセスに際して、ポリシーやリストに基づき警告、制限、遮断、報告、記録等の管理やフィルタリングを行うサービス。いわゆるレピュティションサービスを含む。
		脆弱性検査サービス	ITシステムの脆弱性やアプリケーションのセキュリティホールに対して、侵入検査等の擬似攻撃手法やコードの解析等によって検査･診断するサービス。
		セキュリティ情報提供サービス	インシデント、脆弱性、パッチその他の IT セキュリティに関する情報を提供するサービス。 ウェブ、メールニュース、レポート、出版等、媒体種類を問わない。
		電子認証サービス	電子証明書の発行･認証、無改竄保証、否認防止、タイムスタンプ証明等の電子的証明やそれに関連するサービス。
		インシデント対応関連サービス	情報セキュリティ･インシデントに際しての緊急対応や復旧に関する専門的スキルを提供するサービス、ならびにいわゆるデジタルフォレンジックに係る専門的スキルを提供するサービス。 ただし上記の各監視･運用支援サービスと一体のものとして提供される場合はその分類に集計する。
		その他の運用･管理サービス	その他の、情報セキュリティの運用･管理に関するサービス。
情報セキュリティ教育			
	情報セキュリティに関連する知識やスキルの習得、ならびに情報セキュリティ関連の資格取得のための教育、研修に関するサービス。 セキュリティコンサルテーションやセキュアシステム構築サービスの一環として社員や運用担当者等に実施する教育はそれらのサービスの一部ととらえ、「セキュリティ教育サービス」には集計しない。	情報セキュリティ教育の提供サービス	情報セキュリティ教育の提供･実施サービス。 教師が実施する集合教育･実地教育･演習等のサービス提供の形態、ならびにセキュリティ教育の内容または教材（いわゆるコンテンツ）の販売もしくはライセンス提供を行う形態の双方を含む。 e-ラーニングのコンテンツ提供のみを行う場合を含む。 セキュリティ資格関連のサービスは「セキュリティ資格認定及び教育サービス」に分類する。
		情報セキュリティ教育の e-ラーニングサービス	情報セキュリティ教育を e-ラーニング方式で提供･実施するサービス。 e-ラーニングのコンテンツ提供のみを行う場合は「情報セキュリティ教育の提供サービス」に含む。 原則として、e-ラーニングのためのシステム（ソフト･ハード）部分の価格は含まないものとするが、コンテンツと一体不可分の場合はコンテンツ価格に含むことも可。
		情報セキュリティ関連資格認定及び教育サービス	情報セキュリティ関連の資格の認定（継続･維持を含む）を行い、または資格認定のための教育研修の実施や受験準備のための講習等を行うサービス。
		その他の情報セキュリティ教育サービス	その他の情報セキュリティ教育に関するサービス。情報セキュリティ教育を直接の目的としたコンサルテーションやシステム構築サービスを含む。
情報セキュリティ保険			
	情報セキュリティならびにITセキュリティに関する損害を補償する保険。	情報セキュリティ保険	情報漏えい等の情報セキュリティならびにネットワークを中心としたITシステムのインシデントに起因する損害を補償することを主たる機能とした保険。

5.2. 情報セキュリティツール市場の定義に関する説明

「ツール」については、ハードウェア製品とソフトウェア製品の両方を含むものとし、製品・商品化されて販売されているものを対象とした。製品カテゴリとしては「統合型アプライアンス」、「ネットワーク脅威対策製品」、「コンテンツセキュリティ対策製品」、「アイデンティティ・アクセス管理製品」、「システムセキュリティ管理製品」、「暗号製品」の 6 区分（大分類）とした。

1. 統合型アプライアンス

「統合型アプライアンス」は、ハードウェアとソフトウェアを一体化して一つの製品として販売する製品形態である「アプライアンス」製品の中で、二つ以上のカテゴリにまたがる機能を複数統合して一つのアプライアンス上に実現する製品と定義した。

従来からファイアウォールと VPN ゲートウェイを一体で実現する製品は多く見られたが、これに留まらず不正侵入監視やウイルス監視機能を併設し、1 台でほとんどの外部脅威防御機能を実現する製品が 2003 年頃に登場し、2006 年頃から普及期に入っている。このため単純に特定機能分類に仕分けすることができず、単一カテゴリとして定義することとした。このカテゴリは、複数機能の統合と共に、コンパクトなハードと一体化して提供するという特徴も指摘できる。またこれらの製品を、UTM（Unified Threat Management = 統合脅威管理=）と総称する呼び方も一般的になっている。

UTM 以外では、帯域管理にプロキシ、パケットフィルタリング、URL フィルタリング、コンテンツフィルタリング等を取み合わせるようなものも登場している。また、内部ネットワークのスキャンと同時にウイルスやスパムのチェックを行うようなタイプの製品も見かけるようになった。

ハードウェアの高機能・低価格化と入手の容易さが進むに連れて、ユーザの利便性や保守の簡便性から、アプライアンスへ向かう動きが全般的に強まっている。導入に際しては、ハード、OS、ソフトを各々購入して取み合わせる手間や仕様の整合性を確保するための煩雑さから解放される。アップデートに際してもハードとの整合性はベンダの責任でカバーされる。トラブル対策に際しては、原因の所在をユーザ側で切り分ける必要がない。このようにアプライアンスはユーザにとっての利便性が高く、販売店にとってもユーザ対応が単純化するメリットがあることから、様々なセキュリティ機能がアプライアンスによって提供されるようになっている。

このうち単一機能のアプライアンスは各々の機能別カテゴリに分類し、複数のカテゴリの機能を併せ持つタイプのものを「統合型アプライアンス」として独立カテゴリとした。上に見たように様々なバリエーションを持った複合機能のアプライアンスが登場しているが、ファイアウォールの発展型である UTM が主流であるところから、特に中分類では区分せず、「二つ以上の大分類カテゴリにまたがる複数の機能を 1 台で提供するアプライアンス製品」を「統合型アプライアンス」として、単一セグメントのカテゴリとして定義した。

2. ネットワーク脅威対策製品

「ネットワーク脅威対策製品」は、主として外部からの不正な侵入・アクセスを防ぐフ

ァイアウォール、VPN（Virtual Private Network 仮想私設通信網）、IDS／IPS（Intrusion Detection System 侵入検知システム、Intrusion Prevention System 侵入防御システム）の 3 種類の製品分類を含む。

このうちファイアウォールは主として組織の内外のネットワークの境界において、あらかじめ設定されたルールに従って通信をチェックし、ルールに適合する以外の通信を遮断したり、制限したりする機能を提供する。イントラネットにおいてアクセス管理やインシデント拡散防止の「防火壁」として使用する形態もある。これに対して IDS は、たとえファイアウォールの設定ルール（ポリシー）で許可された通信であっても、それが不正な通信パターンやネットワーク攻撃に特有の特徴を含む通信である場合にはそれを検知し、警報を発したり記録を保全したりする機能がある。IPS は、そのようなケースにおいて自動的に通信を遮断したり制限したりする機能を併せ持った製品と定義できる。

アプリケーションファイアウォールというセグントを前回調査から新設した。主なものとして、ウェブアプリケーションファイアウォール[10]がある。ウェブサーバの前に配置して、ウェブアプリケーションに固有の攻撃からアプリケーションを保護する目的で使われる。データベースへの攻撃やその不正利用を防ぐ目的で使われるファイアウォール型の装置もある。これらを総称してアプリケーションファイアウォールとした。

3. コンテンツセキュリティ対策製品

このカテゴリは、コンテンツ、すなわち情報の中身そのものに関するセキュリティを保護する製品のグループである。本調査では、ネットワーク通信に関して、その通信目的をコントロールすることを主目的とするものを、前述の「ネットワーク脅威対策」と定義し、通信の中身について不都合の有無をチェックすることを主目的とするものを「コンテンツセキュリティ対策」と定義した。ネットワークを介して伝播するウイルス、ワーム、スパイウェアなどの悪意あるプログラムを検知・排除する、いわゆるアンチウイルス製品、スパムメールやフィッシングに対するコントロール（管理・制御）やフィルタリング（選別）を行う製品、メールの内容をチェックしたりログ（動作記録）を取ったりして情報漏えい等を防止する製品、更には有害ウェブサイト等特定の情報源（リソース）へのアクセスをデータの内容を検査して防ぐ製品等がある。

つまり、ファイルやメールや通信の内容に対するチェックやコントロールを提供する製品のグループである。データそのものの保護については、暗号を利用することが一般的であるため「暗号製品」に分類している。なお、いわゆる Digital Rights Management（DRM）[11]と呼ばれる製品群があり、「その他コンテンツセキュリティ対策製品」に含めた。DRM とは、コンテンツの利用の態様に対してコントロールをかけるもので、利用する人の属性、方法、時間、場所、回数等によってコントロールすることで、権利者の意図する範囲と方法での利用を担保する目的で使われる。これは内容の保護を同時に実現する場合も多いがそれが必然ではなく、暗号を伴わないケースもあることから、「コンテンツセキュリティ対

[10] WAF （Web Application Firewall）と略称する場合もある。
[11] 一部のベンダは IRM （Information Rights Management）とも呼ぶ。

策製品」のカテゴリに含めることとした。

4. アイデンティティ･アクセス管理製品

「アイデンティティ･アクセス管理製品」は、情報システムやネットワークに対してユーザがアクセスする際に、本人であることを認証し、そのユーザに与えられた権限の範囲内で情報資源にアクセスさせることを保証する一連の製品である。各種認証デバイス（装置・機器）並びにその認証システム、アイデンティティ管理システム、ログオン管理･アクセス許可システム、ディレクトリ管理システム、シングルサインオンシステム、PKI 関連システムなどがこのカテゴリに含まれる。

このカテゴリの呼称については、従来「アクセス管理製品」としてきたが、今年度調査においては「アイデンティティ・アクセス管理製品」とした。構造としては、システムにアクセスしてきた者が、その主張する認識符合（ID）に対応する本人であるかを、本人から提供される情報により検証することで「認証」を行い、システム側の設定において、その ID でアクセスする人（入出力・通信の主体）に紐づいたリソース、アプリケーション、データとその操作権限の範囲でシステムへのアクセスを許可する一連のコントロールを構成する各種機能が製品として展開されていると捉えられる。

その中において、内部統制報告制度の要求と関連して、システム上の ID と現実世界の存在である個別の個人の対応関係並びにその個人のシステム上の行為をより厳密に把握し、追跡や検証が可能なかたちで管理する必要が高まってきた。このため、「アクセス管理」に加えて「アイデンティティ管理」を導入するニーズが高まり、急速に広がっていると見られる。この動向を踏まえ、セグメントとして「アイデンティティ管理」を新設すると共にカテゴリの名称を「アイデンティティ・アクセス管理製品」とした。

5. システムセキュリティ管理製品

「システムセキュリティ管理製品」とは、主にシステム全体のセキュリティ情報を監視して統合管理と統計処理を行い、その結果を統合表示したり、異常に対してアラート（警報・警告）を出したりする製品である。システム全体に関して、ある判断基準に従いチェックを行い、ポリシーへの準拠性を確認する製品（いわゆるコンプライアンス管理製品）や脆弱性検査製品（いわゆるスキャニングツール）等が含まれる。

これらの製品が登場した背景には、ネットワークの防御がファイアウォールに象徴されるような「点」の守りだけでは十分でなく、複数のポイントにおける情報から統合的かつ一元的に管理しなければならないという問題意識がある。特に、最近頻発する情報漏えいの教訓からネットワーク内部の管理・監視も不可欠であるという理解、更にはネットワーク全体のセキュリティレベルの維持には、ポリシーレベルでの一貫性をもった統合管理が不可欠であるという理解の浸透に伴い、需要を伸ばしている。

ネットワークの主要資源を一元管理する思想はネットワーク統合管理プラットフォームのアーキテクチャには以前から取込まれていたが、セキュリティに着目し、かつ単にセキ

ュリティインシデント[12]だけでなく状態管理も含めた統合管理の考え方が普及してきている。

また、情報漏えい対策が強く意識される中で、従業員の個別のファイル操作に直接的な制限をかけるニーズが高まっている。具体的には、CD、DVD、外付けハードディスク、USB メモリ等の取外し可能な外部記憶への書き込みや印刷を制限したり監視したりする仕組みのものが多い。このような製品は「ポリシー管理･設定管理･動作監視制御製品」に分類して集計対象としている。

いわゆる検疫ネットワークと呼ばれる製品やソリューション（個別機能の組合せで目的とする複合機能を実現するもの）が供給され、普及し出している。呼称としては NAC（Network Access Control）という呼び方が一般的になりつつあるものの、NAP（Network Access Protection）という表現の他、ベンダ独自のソリューション名を付けるケースもあり、まだ一元的な呼称は定着していない状態である。一時的にでもネットワークの外にあった可搬型 PC 等が、ウイルス等に汚染されたままネットワークに接続すると、そのネットワークにウイルス感染を引き起こすことがある。それを防止するために、ネットワークへの接続を実現する前に、その PC 等のウイルス感染状態や、OS のパッチの適用状態その他のポリシー遵守状態をチェックするのが、検疫ネットワークの基本的な考え方である。またアクセス管理の考え方からは、そもそも企業のネットワークに接続を許可される PC の範囲があらかじめ規定されており、それ以外の PC の接続を防ぐ必要がある。このような機器認証の機能も検疫ネットワークの重要な役割と言える。端末にエージェントを搭載したり、MAC アドレスで管理したりと機器の認識方式も様々で、その認証も認証サーバによるもの、仮想 LAN スイッチによるもの等様々な方式があり、ソリューションとして実現することも可能だが、供給側がパッケージ化する例も増加している。MSBlaser ワーム被害の経験から導入されるようになり、ファイル共有ソフトに感染するウイルスによる情報漏えい被害が深刻化する中で、装備する企業が急速に増加していると見られる。

この機能は、ネットワークアクセス制御であり、「ネットワーク脅威対策製品」に分類する考え方もあるが、むしろ端末と位置付けられる各ユーザの PC のポリシー順守状況の管理が主眼で、それとネットワーク接続許可を連動させている構造なので、前者に注目して「ポリシー管理･設定管理･動作監視制御製品」に分類することとした。

情報漏えい問題や内部統制問題を意識する中で、万一の場合の証拠の収集や保全に対しても必要性が意識されるようになっており、「デジタルフォレンジック」という領域として確立しつつある。このための製品の例としては、全ての通信やログを安全に記録･保管するための製品群や、事故等が起った端末のハードディスクの内容を、その時点のまま固定して再現できるように取出し解析するツール類が挙げられる。本調査では「その他システム

[12] 「インシデント」は出来事、事件のような意味。情報セキュリティに関してはウイルス感染、不正侵入、情報漏えい、秘密情報の紛失等の事件･事故･事案を総称して情報セキュリティインシデント又は単にインシデントと言う。

セキュリティ管理製品」の中で集計することとした。

6. 暗号製品

「暗号製品」とはデータ、ファイル、電子メール、ハードディスク等を暗号化する各種製品及び半製品を指す。

暗号技術そのものは、PKI や VPN の基幹技術を構成する他、各種情報セキュリティ製品の内部処理等に広範に使われている。PKI、VPN はその使用目的から各々アイデンティティ・アクセス管理製品、ネットワーク脅威対策製品に分類しており、ここではデータの保護等を目的とする製品を中心に定義している。具体的にはメールやデータを暗号化するソフトウェア、及び暗号化のためのライブラリやモジュールなどが含まれる。

暗号化のためのライブラリやモジュールは、通常の情報システムやネットワークを構成する機器に組み込む用途の他、それらの範疇からイメージ的に遠い分野でも使われる。具体例としては電子ゲーム機やデジタル複合機[13]への搭載がある。これら用途もセキュリティ目的の暗号の利用という意味で本調査の対象に含めている。

5.3. 情報セキュリティサービス市場の定義に関する説明

「情報セキュリティサービス」市場には、情報セキュリティ対策を構築・実践し、情報セキュリティソリューションを実装し機能させ活用するために提供される、各種サービスが含まれる。

本調査では、情報セキュリティサービスとして、国内のサービスプロバイダ（サービス提供事業者）から提供されているものを対象とした。カテゴリとしては、「情報セキュリティコンサルテーション」、「セキュアシステム構築サービス」、「セキュリティ運用・管理サービス」、「情報セキュリティ教育」、「情報セキュリティ保険」の 5 区分とした。

1. 情報セキュリティコンサルテーション

「情報セキュリティコンサルテーション」とは、情報セキュリティに関するポリシー、システム、運用体制の構築を支援するサービスである。情報セキュリティ対策は、情報資産のリスク管理を目的とするところから、単に IT システムへの脅威対策といった技術的領域にとどまらず、経営資源と位置付けられる情報資産に関する経営のリスクコントロールという視点に基づく必要がある。従い、経営管理と技術方針を包含する、専門性が高く、多様性を伴う分野である。

最近では企業のコンプライアンス（法令・ルール遵守）重視の立場から、情報セキュリティマネジメントシステム認証制度など客観的な規格要件の認証取得を目指す企業が増加している。それに対応して、その認証取得を支援するサービスも様々な事業者から提供さ

[13] 複写機にファクス、スキャナー、プリンタの機能を付加したマルチ用途のものをデジタル複合機（MFP, Multi-Functional Printer）と呼びならわしている。複写機の基本構造はスキャナーで読み取ったイメージをプリンタで紙に出力するものであるが、それをデジタル処理にすることでコンピュータによるデータ処理と同等のプロセスとなり、ネットワーク機能とファクス機能、更にデータ蓄積機能を持つことで多彩な複写、印刷機能を提供するようになっている。蓄積機能とネットワーク機能、ネットワーク越しに離れた場所で紙に出力されたものの物理的管理の問題等から、新たな情報セキュリティのフロンティアとしても浮上している。

れ、増加傾向にある。一方、こうした規格適合性を審査し、認証するサービスもまた、公的機関に限らず、民間事業者から提供されている。この、認証を提供する側のサービスもこの分野に含んでいる。

2. セキュアシステム構築サービス

「セキュアシステム構築サービス」は、実際にセキュアなシステムを構築する段階で必要となるサービスであり、IT セキュリティシステムの設計、仕様策定といった上流工程から、セキュリティソフトウェアの開発、カスタマイズ（個別対応改造）、セキュリティソフトウェア及びハードウェアの選定、導入、設定などのサービスが含まれる。

3. セキュリティ運用・管理サービス

「セキュリティ運用・管理サービス」は、導入したセキュリティシステムの全体あるいは一部の管理運用を、外部事業者が事業所内に常駐し、あるいは事業所外から遠隔操作によって代行するサービスが中心で、その対象にはシステムの総合監視、ファイアウォール監視、IDS／IPS 監視、ウイルス監視等がある。この他にネットワークからの攻撃に対する弱点を検査する脆弱性検査サービス、セキュリティ情報提供サービス等の予防的サービスがある。また、何らかの事故等が発生した場合の対応を引き受けたり支援したりする専門家のサービスであるインシデント対応関連サービスも、このカテゴリの一部であり、需要を高めている。個人の認証を第三者が発行する電子証明書によって行う PKI（公開鍵基盤）や、ウェブサーバの実在性・信頼性を保証する SSL[14]サーバ証明に用いられる電子証明書の発行を行う電子認証サービスもこのカテゴリに含めた。電子認証サービスは、文書の完全性・真正性の証明や否認防止、時刻の証明であるタイムスタンプ等にも用途が広がっている。

4. 情報セキュリティ教育

情報セキュリティ教育には、情報セキュリティ教育の実施、教材等教育実施の中身であるコンテンツの提供や開発受託等のサービスがある。教育の実施手段として、ウェブサーバとブラウザによってネットワークを通じて電子的に実施する、いわゆる e-ラーニングも活発であり、通常の教育実施と区分して集計対象とした。また、資格に関する与える側・取得する側双方のサービスも活発化している。こうしたサービスは情報セキュリティ製品やサービスのプロバイダ（提供事業者）や、教育を専門とする事業者から提供されている。

5. 情報セキュリティ保険

ウイルスや不正アクセスによる被害並びに情報漏えい等による損害を賠償するタイプの損害保険商品が複数の保険事業者から提供されるようになった。需要側としても、リスク対策の一手段としてリスクの移転を採用する機運が高まっており、IT 保険、ネットワーク保険と共に、あるいはその一部として、情報セキュリティ保険が市場の認知を得ていると見ら

[14] SSL: Secure Socket Layer　暗号通信の一方式。

れる。本調査では、これを情報セキュリティサービスの１カテゴリとして調査集計対象とした。

6　国内情報セキュリティ市場を取巻く状況及び市場の概要

6.1. 市場規模及び IT 投資との関係

表 6 並びに図 12 に、国内情報セキュリティ市場の推移を表とグラフで示す。

国内情報セキュリティ市場は、調査対象期間の前半は力強い成長を見せる一方、2008 年 9 月のリーマンショックと言われる事件を契機に急速な世界同時不況の波に見舞われ、後半はマイナス成長に陥るものと見られる。

表 6　国内情報セキュリティ市場推移

市　場　規　模（億円）	2006 年度 推定実績	2007 年度 推定実績	2008 年度 実績見込	2009 年度 予測
情報セキュリティツール市場	2,924	3,461	3,748	3,636
情報セキュリティサービス市場	3,047	3,386	3,520	3,238
情報セキュリティ市場合計	5,972	6,847	7,268	6,874
市　場　成　長　率（%）				
情報セキュリティツール市場	－	18.3%	8.3%	-3.0%
情報セキュリティサービス市場	－	11.1%	4.0%	-8.0%
情報セキュリティ市場合計	－	14.7%	6.1%	-5.4%

国内情報セキュリティ市場の金額規模は、表 6 に示す通り、ベンダ売上ベースで、2006 年度実績が 5,972 億円、2007 年度実績値が 6,847 億円となったと推定され、2008 年度は更に拡大して 7,268 億円と、7000 億円の大台に乗ったものと推測される。これは年度後半に世界同時不況の影響が見られつつも、年度前半の好調と、年度後半についても急減速の動きが一部にとどまったことから、年間では拡大基調が続いたと見られることによる。2009 年度は、本作業の時点[15]での推定値としては 6,874 億円に縮小するものと予測される。

この市場規模を IT 自体の投資規模との関連で見るために、SI 関連の市場統計との比較を試みる。社団法人電子情報技術産業協会（JEITA）の調査報告「2007 年度ソフトウェアおよびソリューションサービス市場規模調査結果」[16]によれば、2007 年度のソフトウェア及びサービスの売上高は 5 兆 6,347 億円（うち SI 開発 2 兆 6,578 億円、ソフトウェア 7,650 億円、アウトソーシング・その他サービス 2 兆 2,119 億円）である。また、同協会のハードウェア統計[17]によれば、2007 年度の出荷額実績はメインフレーム 1,658 億円、サーバ 5,043 億円、ワークステーション 286 億円、パソコン 1 兆 1,346 億円で、ハードウェアの出荷額は、合計で 1 兆 8,333 億円となる。ソフ

---

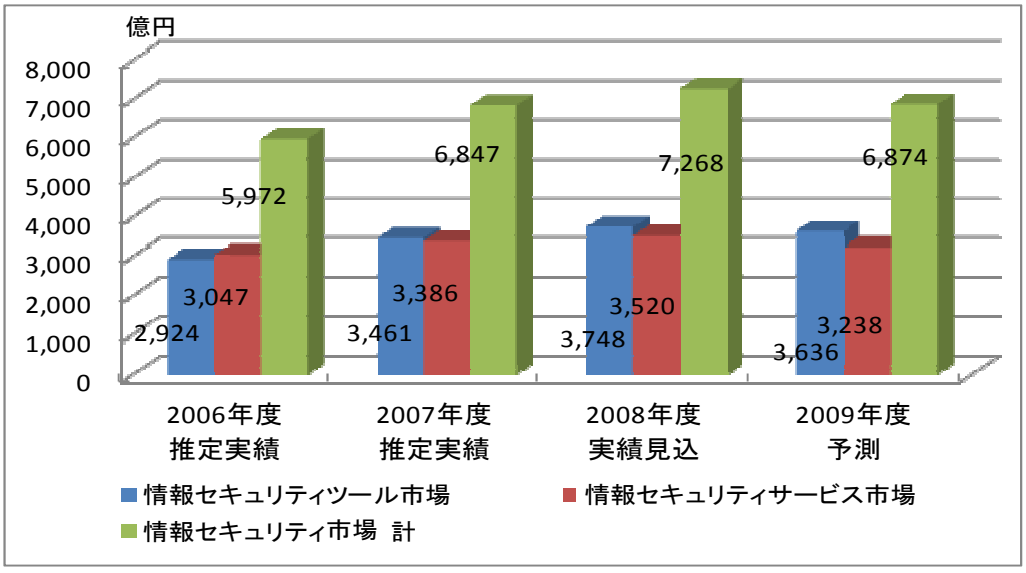
[15] 全体集計作業は 2009 年 1 月から 2 月にかけて行った。この間並行して主要事業者への個別ヒアリングを行い、経済情勢の影響や 2009 年度の見通しについても調査したが、2009 年度は不透明性が極めて高いというのが共通認識であり、世界同時不況の影響の程度は読み切れていない。従い、2009 年度の数字はこの作業時点での感触を数値化したもので、時間の経過と共に変化する可能性があることをお断りしたい。

[16] 社団法人電子情報技術産業協会「2007 年度ソフトウェアおよびソリューションサービス市場規模調査結果について」平成 20 年 7 月 18 日　http://it.jeita.or.jp/statistics/soft_sol/h19/index.html

[17] 「わが国におけるサーバ・ワークステーションの平成 19 年度第 4 四半期（1～3 月）および平成 19 年度（4～3 月）出荷実績」　http://it.jeita.or.jp/statistics/midws/h19/index.html
「2007 年度パーソナルコンピュータ国内出荷実績」http://www.jeita.or.jp/japanese/stat/pc/2007/index.htm

トウェア、サービス、ハードウェアの金額を合計すると 7 兆 4,680 億円に達する。情報セキュリティ市場の 2007 年度の数字は 6,847 億円であり、IT のソフト・ハード合計に対する比率はその約 9.2%に相当する。一般に IT セキュリティ投資は IT 投資全体に対して数パーセント（調査により概ね 1%から 7%程度の範囲にばらつく）を占めるものと見られているが、本調査を JEITA の数字と比較する限りでは、この一般に言われている範囲よりもかなり高い比率を示している。要因の一つとして、IT 投資という場合に周辺装置やネットワーク機器も含める必要があるという点が挙げられよう。前者は同じく JEITA の統計[18]で一部について金額が得られるが、その合計は 9,212 億円であり、後者は情報通信ネットワーク産業協会（CIAJ）の生産・輸入統計[19]によるとネットワーク接続機器の生産は 401 億円、ネットワーク関連機器の輸入は 4,346 億円である。これらを加えたものに対する情報セキュリティ市場の比率は 7.7%である。本調査では、情報セキュリティコンサルテーション、教育、保険等も集計対象としているが。IT 投資との比較においてこれらを含めたもので対比するのが適当かも検討課題である。なお、IT 分野でのハードウェアは価格が趨勢的に下がり続けている。前回調査で引用した JEITA のハードウェア統計の 2005 年度の数値は 2 兆 6,524 億円であり、今回用いた数字はこれより 31%も減少している。セキュリティツールでもアプライアンス等は単価が下がる傾向にあるが、ソフトウェアやサービスはハードウェアほどの下落は示さないので、本調査の数字は時と共に IT 投資の数値に対しては比率が上昇しやすい傾向にある可能性が高い。

図 12　国内情報セキュリティ市場規模の推移



次に、前年度比成長率の比較を見てみる。JEITA による「ソフトウェアおよびソリューションサービス国内市場統計」では、2007 年度の前年度比伸び率が SI 開発で 10%、ソフトウェアでマ

[18] http://it.jeita.or.jp/statistics/intelterm/2007/table-a.html

[19] 情報通信ネットワーク産業協会（CIAJ）　http://www.ciaj.or.jp/content/info/dat/tusin.html　より 2008.3 月「生産統計エクセルファイル」及び「輸入統計エクセルファイル」

イナス 1%、アウトソーシングその他サービスで 1%となっており、総じて伸びは低い。ハードウェアについては、ほとんどの区分で統計対象母体の変化があったために前年度比の数字が示されていないが、唯一メインフレームで数値が示されており、金額ベースでマイナス 8%となっている。CIAJ の統計では、ネットワーク機器の国内生産が 2007 年度に前年比 17.9%伸びている。(輸入統計の伸び率データは空欄) このように、IT 全般としては緩やかな伸び、ハードについては金額ベースの伸びがない状態の中で、ネットワーク関係だけは比較的成長を維持していると見られる。本調査による 2007 年度の前年比成長率は 14.7%となった。IT 全般に比較して、かなり高い成長速度を示していると言える。

6.2. 市場の沿革

情報システムにおけるセキュリティ対策は、メインフレームを中心とするいわゆるレガシーシステムの時代には、コンピュータシステム自体の中にセキュリティ対策の機能や手順が盛り込まれ、個別システムの構築に際しても仕様・設計の段階からシステムと一体のものとして組み込まれるのが通常であった。また、オープンアーキテクチャやオープンネットワークという構造がなく、特定の関係者が専門教育に基づいて限定的な使い方をする形態が一般的なために、情報セキュリティの対象領域も限られたものであり、その対象とする事象も限定的な範囲で済んでいたのである。

その後 1980 年代からコンピュータシステムのオープン化が進む。UNIX、DOS、更には Windows が普及し、1990 年代には IP ベースのオープンネットワークが一般化してきた。また、21 世紀に入り、高速データ通信手段の多様化と低価格化、一般個人ユーザまでの普及という通信環境の革新が進む中で、企業内ユーザであれ個人であれ、PC とインターネット接続がオフィス業務や情報生活の手段として当り前という環境がごく短時間のうちに実現した。

その成果は二つのことを意味した。一つは、個人の PC が、そして企業の社内 LAN やそこに収容される PC 端末が、ほとんど無防備で、不特定多数が行き交う往来に放り出されるのと同じような危険な状態にさらされるようになったこと。そしてもう一つは、システムはその使用上の安全対策をあらかじめ組み込んだものではなく、それはユーザなり管理者なりが個別に用意しなければならないものになった、ということである。

このことにより、ネットワークセキュリティやシステムのセキュリティを独立の機能として用意する必要が生じ、そのための技術が開発され、ツールとして商品化されてきた。また、それらを選定し組み込み使いこなすための、あるいは運用保守のためのサービスも生まれ供給されるようになった。これらツールやサービスが市場として形成され始めてから 10 年程度の歴史であるが、それが国内だけで 6,000 億円から 7,000 億円強の規模の市場となり産業となったことは大きな意味を持つと考えられる。

このような背景の下に形成されてきた情報セキュリティ市場であるが、情報セキュリティがインターネットの急速な発展とそれに伴う様々な副作用・副産物の要素への対応の必要から、いわば受身的に展開してきた流れが、ここへきてはっきり変化を示していると言える。それは、社会の発展が犯罪の発展を排除できずそれへの対応を（多くの場合事後的に）組み込みつつ進むのと

同じように、インターネットと IT システムの活用も、その負の側面への対応をいかに織り込みつつ展開するかの視点に移りつつあるように見える。その表れとして、ネットワーク機器やアプリケーションは必ずセキュリティ特性をその仕様に組み込むようになってきているし、システムインテグレーションもセキュリティ要件を自明のこととして仕様化している。また、規模や被害の大きい情報漏えい事件の報道が後を絶たず、経営へのインパクトが強く意識されるようになった結果、情報漏えい対策が経営課題としての重みを増している。政府の強力な推進努力の効果もあって、情報セキュリティガバナンス[20]を重要な経営課題と位置付け、情報セキュリティポリシーを構築して対応することが、経営者の当然の使命となりつつある。

2008 年 4 月以降に開始する事業年度に対して、株式公開企業の義務となった内部統制報告制度は、財務諸表の情報に影響を与える業務の執行の適正性の担保とその検証を経営者の義務としている。これは IT なしには実現できず、IT の設計・構築・運用・管理の適正性の担保が求められることから IT ガバナンスが課題となり、その中核をなす技術として情報セキュリティが位置付けられるに至っている。この面からも、情報セキュリティの正しい構築運用を管理するための情報セキュリティガバナンスに対して、経営テーマとしてとしての認識が進んでいる。これは内部統制対応のみならず、近年世界的に意識の高まりが見える事業継続管理も含めた危機管理、リスクマネジメントの主要課題としても位置付けられている。法令や規則の順守を意味するコンプライアンスを加え、ガバナンス、リスクマネジメント、コンプライアンスの頭文字をとり、GRC という言い方も出てきている。[21]

このように、従来どちらかというと後付け的･受身的に技術進化と産業展開が進んできた情報セキュリティの技術やソリューションは、ここにきてマネジメント体系への一体統合化が急速に進んでいる。2000 年代前半にはその必要性の理解が浸透しなかった情報セキュリティも、経営課題の重要な一テーマとしての認知が定着しつつあると言える。

政府は 2009 年 2 月、第 2 次情報セキュリティ基本計画を発表した。その基本コンセプトに「『事故前提社会』への対応力強化」を掲げている。ネットワークからの脅威、システムの脆弱性、管理運用上のミスや不正の全てを根絶やしにすることは不可能だという前提に立って、そのリスクにいかに対応するか、その対応を適正に進めることで効率や効用をいかに引き出すかが関心事となる。受け身だけのセキュリティから、マネジメントの課題としての情報セキュリティへ、位置付けの進化と共に取組の深化が進むことが期待されるところである。

6.3. 成長速度

情報セキュリティに関して特筆すべきこととして、この産業の成長率の高さが挙げられる。今回調査により得られた数字の範囲では、2007 年度において前年度比 14.7%と極めて高い成長率を示している。世界同時不況の影響が表れた 2008 年度の実績見込み値は 6.1%と大幅に減速するも

[20] コーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること（2005 年 3 月「企業における情報セキュリティガバナンスのあり方に関する研究会」（座長：土居範久中央大学教授）報告書）

[21] http://www.csiannual.com/pdfs/CSI_2008_Program.pdf,
http://www.informationweek.com/blog/main/archives/2008/11/csi_2008_the_bu.html?cid=RSSfeed_IWK_ALL

のの、他の主要な産業と様相を異にしてまだ増勢を維持している。2009 年度は、本調査の予測作業の時点ではマイナス 5.4%とマイナス成長に陥るものの 1 桁のマイナスにとどまっている。この 3 年間の年平均成長率に換算すると、4.8%となり、名目経済成長率に比しても高い成長率を示している。

一方で、後付けで補うことで IT の進化にキャッチアップするという特性を色濃く持っていた IT セキュリティが、以下に見て行くように、最初から仕様として組み込まれるようになり、また IT 投資と一体で投資が企画される方向に動いてきている。その結果、足りない所を補うために速度を上げて整備する要素が減り、IT 投資と同一歩調で市場が推移するように、徐々にシフトしている。

一方で、外部脅威対策でなく内部管理の充実目的でのセキュリティ装備は進展する傾向を見せている。一つは情報保護のための暗号化対策の進展である。今一つは内部統制上必要なアクセス管理やトレーサビリティ（行為の追跡性）確保のためのアイデンティティ・アクセス管理の導入・強化である。更には何か事が起きた時に操作履歴を検証し証拠としても利用できるための対策として、ログ管理を中心とするデジタルフォレンジック対応も導入が進んできている。また、スパムメールやウェブサイトへの攻撃等、外部脅威の高度化・複雑化の要素も強まっている。

これらの要因から、当面は IT 全般の投資動向よりは強い情報セキュリティ投資の勢いが継続するものと思われる。

6.4. 市場の形成と成長の促進要因

報道媒体における取扱い頻度、テレビの報道番組でもしばしば取り扱われるようになってきたこと、各種セミナーや展示会の開催頻度とその集客数の伸び、企業社会のトピックとして一般化してきたこと、等の要素を含めて振り返って見ると、やはり 2003 年度から 2004 年度あたりに市場の変局点があったように思われる。前回の本調査でも指摘したように、そのことが、この期間の市場の高い成長率もたらしたと考えられる。その勢いは、今回の観測では 2008 年度の前半まで続き、市場は比較的高い成長を維持したものと見られる。

このように市場を力強くドライブしてきた要因としては、以下に述べるようないくつかの要素が作用しているものと推測される。

1. マルウェア等の脅威の複雑化と深刻化

   独立行政法人情報処理推進機構（IPA）へのウイルス・ワームの届出状況の統計によれば、2004 年（暦年、以下同じ）の 52,151 件、2005 年の 54,174 件をピークとして、2006 年 44,840 件、2007 年 34,334 件、2008 年 21,591 件と減少傾向にある。大規模感染を引き起こす大量メール配信型ウイルスの減少によるものと解説されている[22]。最近はむしろ、知らないうちに忍び込んで情報を外に送り出すスパイウェアや、ハッカーの指令に基づいて

[22] 独立行政法人情報処理推進機構「2008 年のコンピュータウイルス届出状況」2009 年 1 月 7 日
http://www.ipa.go.jp/security/txt/2009/documents/2008all-vir.pdf

攻撃等の行動を起すボットの脅威が問題になっている[23]。また、ウェブ閲覧によるウイルス感染や、ファイル共有ソフトを悪用するウイルスによる情報漏えい被害も後を絶たない。発信元の偽装や特定ターゲットへの攻撃など、益々悪質化している。2008 年度は、USB メモリを介して感染を広げるウイルスも話題になっている[24]。

そのために、企業はウイルス対策ソフトを始め様々な防衛手段を講じている。

2. 脆弱性情報の取扱い・対応体制の整備

ウイルス・ワームの頻発・蔓延を許す一因ともなっている OS やアプリケーションの脆弱性の発現頻度が高まっており、世界的にその対策について関心と懸念が持たれている。また情報漏えいにつながりやすいウェブアプリケーションの脆弱性も増大しており、その潜在的脅威は日々大きくなっていると考えられる。

これに対応するために経済産業省ではコンピュータセキュリティ早期警戒パートナーシップという枠組を作って 2004 年 7 月から運用している。現在、独立行政法人情報処理推進機構（IPA）を届出機関、有限責任中間法人 JPCERT コーディネーションセンター（JPCERT／CC）[25]を調整機関として運用されており、JNSA はじめ IT 関連の民間業界団体がパートナーシップに参加している。また、両団体が運営する脆弱性情報提供のウェブサイト JVN（Japan Vendor Status Notes）では、海外からの情報も含めて脆弱性情報の迅速な提供に努めている[26]。更には、これら脆弱性情報の伝達と対応方法の支援のために、民間のボランティアベースの活動 SPREAD[27]も組織され、官民挙げての取組が推進されている。

このような動きも企業や公共団体などでインターネットの脅威とその対策に対する意識を高め、情報セキュリティ対策の導入に繋がっているものと推測される。

3. 情報漏えい事件の頻発と深刻化

JNSA セキュリティ被害調査ワーキンググループの報告書[28]によれば、2007 年には同ワーキンググループが把握した報道件数ベースで 864 件、3,053 万人以上の個人情報が漏えいしている。前年比で件数は 87%に減ったが人数は 137%と急増し、同調査史上最多となっている。情報漏えい事件の報道は後を絶たず、特にファイル共有ソフトに寄生するウイルスによって防衛機密や企業秘密がネットワーク上に出回り、回収不可能の状態にある事件も起きている。

情報漏えい事件の実害が大きいことから、企業は防衛の姿勢を強めている。また、消費者の側も、自分の口座番号やクレジットカード番号が悪用される被害が我が身に降りかかる可能性を、身近に感じるようになっている。

---

[23] http://www.ipa.go.jp/security/isg/bot.html
[24] http://www.ipa.go.jp/security/txt/2009/03outline.html#5
[25] http://www.jpcert.or.jp/
[26] http://jvn.jp/
[27] http://spread-j.org/
[28] http://www.jnsa.org/result/2007/pol/incident/index.html

4. 個人情報保護法の全面施行とプライバシーマーク取得の活発化

個人情報保護法が 2005 年 4 月 1 日から全面施行されるのを前に、企業では、2004 年度の段階で既に活発な対応を開始し、その体制作りの一環として ISMS 認証[29]取得やプライバシーマーク[30]の認定取得に取り組んだり、自社の対策を、法の規定する人的、組織的、物理的、技術的対策の 4 側面から点検したりする動きが広範に見られた。個人情報保護法の全面施行以降は、細かな紛失事件なども公表されるようになり、その相次ぐ報道等が社会の関心をより一層高め、企業における対策への取組が一層積極化するようになった。また、委託先管理の義務が明記されたことから、外注先に体制の整備とその証左としてのプライバシーマーク取得の要請が強まり、個人情報を取り扱う事業体は個人情報取扱事業者に該当するか如何に関わりなく、小規模事業者までがプライバシーマークの取得に取り組むようになっている。その結果、ここ数年、プライバシーマークの新規取得企業数は毎年 1500 件程度に上り、累計取得企業数は 2008 年度末現在で 1 万 139 社に達している[31]。

5. 内部統制対応における情報セキュリティ

2006 年 6 月に金融商品取引法が成立し、企業の財務報告の信頼性に関して、内部統制評価の報告と、公認会計士による監査が義務付けられることになった。このうち、企業取引に関る財務データの処理を担う IT における統制が重要な要素と位置付けられ、IT の全般統制並びに業務処理統制の万全を期する必要が出てきた。そのためには業務の種類とその処理プロセスの詳細を整理してリスク分析を行い、リスク対策を手当てする必要があり、そのためにいわゆる「3 点セット[32]」の整備に取り組む企業が続出した。

そうした中で IT におけるコントロールの基本も見えてきた。すなわち、権限外のアクセスや操作を排除してデータの完全性を守ることと、万が一のシステムトラブルから IT 並びにデータを守る可用性との両面が必要になる。システムトラブルの原因として外部からの不正プログラムの侵入や不正アクセスを防ぐという面からは機密性確保と同等の対策も必要になる。すなわち情報セキュリティそのものが問われるようになった。

このように内部統制対応に何が必要か明らかになるにつれ、情報セキュリティ対策に対する意識も一段と高まり、内部統制を意識した情報セキュリティ対策が積極的に導入されるようになった。具体的には、システムへのアクセス権を従業員個々の職務と権限に基づいて管理するアイデンティティ・アクセス管理や、端末におけるデータ処理、特に外部記憶媒体への複製や印刷、電子メールを通じての転送の統制、データそのものの保護のための暗号化、更に処理の履歴を管理し追跡を可能にするログ管理ツール等が導入されている。

---

[29] Information Security Management System （情報セキュリティマネジメントシステム） 第三者機関が、ISO/IEC27001 規格への適合性を評価し、認証を与える制度。日本では JIPDEC が JIS Q27001 を基準として運用している。

[30] 財団法人日本情報処理開発協会（JIPDEC） が、個人情報管理の体制が適切に構築され運用できているかを審査し、合格者にプライバシーマークの表示･使用を認める制度のこと。審査基準は JIS Q15001 として規格化されている。

[31] http://privacymark.jp/certification_info/list/clist.html

[32] 業務の流れを処理要素に分解し、要素ごとのリスク要因と対策を単解するための書式として「業務フロー図」「業務記述書」「リスクコントロールマトリクス」の 3 種類を作成･活用する手法が一般に浸透している。

その需要は「3 点セット」整備と並行して顕在化し、2007 年度の市場の伸びを押し上げると共に、2008 年度も少なくとも前半までは力強い動きとなって継続していたと見られる。

6.5. 国内情報セキュリティ市場の特徴点

以上の分析を踏まえつつ、ここでは、今回調査の結果得られたデータに関して、総括的な視点からいくつかの特徴を抽出し分析することとする。

1. 市場の成長速度

今回調査における市場の前年度比成長率は、2007 年度 : 14.7%、2008 年度 : 6.1%、2009 年度 : マイナス 5.4%、となった。前年度の調査においては、2007 年度の成長率は 11.5%、2008 年度の成長率は 5.7%と見込んでいた。今回の調査においては、2007 年度、2008 年度共に前回調査で予測したより高い伸びを示したことになる。

これは上記 6.4 項でみたようにいくつかの要因が需要を押し上げた結果であるが、とりわけ内部統制にとって情報セキュリティ整備、情報セキュリティガバナンスがより一層必要になるとの認識が浸透したことが大きいと考えられる。

情報セキュリティ市場を構成するカテゴリレベルでは、以下に見て行くように、成長率に大きな開きがあり、殆ど横這いか縮小傾向のものもある。反面、高い成長率を維持する市場もある。情報セキュリティそのものが新しいテーマで様々な技術や取組が生まれ、取り入れられ、取捨選択される中で拡大を果たし、あるいは成熟化して行く姿が見て取れる。

2. セキュリティの融合、あるいは普遍化

市場数字の伸びか殆ど止まった市場区分に、「セキュアシステム構築サービス」がある。システムの中のセキュリティ部分に対する構築支援サービスであるが、その需要そのものがなくなった訳ではない。通常のシステム構築に対して、セキュリティ部分が分離されなくなった結果であると分析できる。(8.2.項参照)

内部統制においては、「IT への対応」が求める IT 統制は、その相当部分を IT セキュリティが担うことになる。経済産業省が 2004 年度に打ち出した「情報セキュリティガバナンス」は、内部統制における IT 統制=IT ガバナンスの要請、そして IT ガバナンスの中核を占める IT セキュリティ、というコンテクストから、経営管理プロセスの主要要素として浮かび上がってきた。

このように、情報セキュリティが「分らない」「難しい」という捉え方が一般的であった時代は去り、あって然るべき、なくてはならない要素に変化しつつある。これは情報セキュリティの本質が変化したのではなく、その理解が進み受容が積極化した結果である。このように、セキュリティは、ようやくにして、通常の IT マネジメントプロセスや経営プロセスの一部に位置付けられるようになった。

3. 1 社当り事業規模の小ささ

今回市場規模推計作業の対象としたのは、国内で情報セキュリティのツールまたはサー

ビスを提供する企業合計 358 社である。2007 年度の推定市場規模は 6,847 億円なので、単純計算をすれば、1 社平均の売上高規模は 19.1 億円となる。全てが情報セキュリティ専業ではなく、むしろ兼業の事業者の方が多い状態ではあるが、1 社当りの情報セキュリティの事業規模が 20 億円を切るレベルでは、事業採算性を考えた時に、研究開発投資や人材育成等の面に十分に資金を割けない可能性がある。

特に製品の開発や検証に際して、ベンチャー企業への支援の仕組みの整備は課題となる可能性が高い。

4. 供給事業者の業態の分布

表 2 に、今回推計対象とした企業の業態別集計を載せたが、企業数が最も多い業態は、「D：SI・NI 機能を有する二次・三次販売業者」の 100 社であった。セキュリティツールの主たる供給源である「A：海外メーカまたはその日本法人」は 47 社、「B：国内のセキュリティツールメーカ」は 52 社であった。また「G：セキュリティサービス提供事業者」は 73 社で、業態区分ではこの 4 区分で全体の 76%を占める。ツールの供給事業は A,B,D の 3 業態が中心で、サービスの提供源は企業数では D と G が圧倒的に多い。

業態区分別で売上規模が大きいのは、ツールに関しては、流通構造上の重複を考慮する前のベースで「E：SI が主たる付加価値の大手システムインテグレータ」と「A：海外メーカまたはその日本法人」であった。サービスについて供給規模が大きいのは「E：SI が主たる付加価値の大手システムインテグレータ」が圧倒的であり、これに次ぐのが「D：SI・NI 機能を有する二次・三次販売店」であった。特に大手システムインテグレータは、ほぼすべてのカテゴリで 1 位の供給規模となっており、その存在感が極めて大きいことが確認された。

ツールについては、供給元として「A：海外メーカまたはその日本法人」の供給規模も大きい。ネットワーク脅威対策やコンテンツセキュリティ対策などの“伝統的”情報セキュリティツールの市場規模が大きく、海外ベンダのシェアが高いことによる。これに対し、成長率で高い数字を示すシステムセキュリティ管理や暗号製品では、国産ベンダの活躍が見て取れ、従来海外ベンダ一辺倒だった供給構造に、若干変化が現れている模様である。

例えば、「システムセキュリティ管理製品」のうち、端末においてユーザの行為を監視したり、あらかじめ設定されたポリシーに基づいてコントロールしたり、ログを保存･分析したりする機能を持った、使い勝手のよい製品が、国産ベンダから多く供給されるようになった。また、「暗号製品」においても、ディスクへの書き込みを丸ごと暗号化するツールや、USB メモリに暗号化機能を組み込んだツール等が、国内ベンチャー企業や大手メーカの関連企業等から相次いで出されている。ただ、これら国内の参入企業の多くは小規模のベンチャー型企業であり、大規模システム対応も含めた製品の開発力、システム対応力、あるいは品質の確保等が課題になる面もありそうである。

情報セキュリティサービスベンダについては、企業規模は様々である。事業規模で大きい大手システムインテグレータや、中堅規模事業者が多い SI・NI 機能を持つ二次・三次販売業者はセキュアシステム構築の比率が高く、コンサルテーションには、会計事務所系コ

ンサルサービス事業者や専業の中小事業者の参入もある。全体を通して見て、大手システムインテグレータが全てのカテゴリで供給元として大きなウェイトを占めている。それ以外では、セキュアシステム構築のようなSI的サービス領域以外のカテゴリでは、限られた市場規模の中に比較的規模の小さい専門特化企業が多数参入して事業を営んでいるという実態が読み取れる。つまり情報セキュリティ業界は、IT全般と同様に大手システムインテグレータが大きな役割を果たしている他に、SI・NI機能を持つ二次・三次販売店が数多く参入し、特定分野では比較的単独事業で規模の小さい企業が数多く参入するという構造になっていると分析できる。

6.6. 産業としての課題

情報セキュリティ産業の現状は、システムインテグレーションに伴うITセキュリティの組込と、その上流に位置する情報セキュリティ構築を一元供給する大手 SI 事業者や、対策ツールの多くを供給する海外ベンダが主要な役割を果たし、市場の占有度も高い。一方参入事業者の数では、比較的専業に近い中小事業者が多くを占めるが、その事業規模は総じて小さい。情報セキュリティが経営課題として重みを増す中で、その対策もポイントソリューションでは済まなくなりつつある。システム全体のセキュリティを、情報セキュリティポリシーに基づいて設計し展開するには、技術のみならず、経営対応のノウハウやインテグレーション能力、更に品質保証能力が問われる。

そのためにはベンダは、品質確保のための十分な投資やベテランの経営管理ノウハウの活用が必要で、経営基盤の安定や、そのベースとなる産業基盤の確立・充実も必要になってくる。しかし、上記 6.5-3.項でも見たように、情報セキュリティ市場を構成する事業者には、事業規模の小さい企業が多いことも事実である。市場の成長に支えられて新規参入や事業拡大が図れている中小事業者も、市場の成熟と共に、またセキュリティが「普遍化」することで経営に組み込まれるに従って、より広い、総合的ソリューション提供力が要求され、大手との競争が厳しくなる可能性がある。

これらの点を見据えて、産業資金の供給、技術開発に対する支援、人材の育成と供給、業界の横の連携による相互補完や規模の拡大等を視野に入れた、情報セキュリティ産業全体に対する政策対応と育成・支援策が傾注されることが期待される。

7. 国内情報セキュリティツール市場の分析

7.1. 情報セキュリティツール市場の全体概要

表 7 に、国内情報セキュリティツール市場規模データを示す。ここに見るように、2007 年度の国内「情報セキュリティツール」市場は、3,461 億円の規模であったと推測される。

本調査では「情報セキュリティツール」市場を、その機能に着目していくつかの製品カテゴリに分類している。大分類レベルで、「統合型アプライアンス」、「ネットワーク脅威対策製品」、「コンテンツセキュリティ対策製品」、「アイデンティティ・アクセス管理製品」、「システムセキュリティ管理製品」、「暗号製品」の 6 カテゴリに分けた。各カテゴリの定義・内容は 5.項に詳述した通りである。

表 7 国内情報セキュリティツール市場規模 実績と予測

金額単位:百万円

年度別市場規模	2006年度		2007年度			2008年度			2009年度		
情報セキュリティツール	実績推計値		実績推計値			実績見込推計値			予測値		
	金額	構成比	金額	構成比	成長率	金額	構成比	成長率	金額	構成比	成長率
統合型アプライアンス	14,487	5.0%	18,183	5.3%	25.5%	19,663	5.2%	8.1%	19,088	5.3%	−2.9%
ネットワーク脅威対策製品	48,455	16.6%	53,383	15.4%	10.2%	55,925	14.9%	4.8%	51,781	14.2%	−7.4%
コンテンツセキュリティ対策製品	116,446	39.8%	132,309	38.2%	13.6%	142,704	38.1%	7.9%	138,721	38.2%	−2.8%
アイデンティティ・アクセス管理製品	48,821	16.7%	61,533	17.8%	26.0%	66,168	17.7%	7.5%	63,079	17.3%	−4.7%
システムセキュリティ管理製品	38,455	13.1%	46,770	13.5%	21.6%	52,153	13.9%	11.5%	51,615	14.2%	−1.0%
暗号製品	25,785	8.8%	33,922	9.8%	31.6%	38,157	10.2%	12.5%	39,296	10.8%	3.0%
セキュリティツール市場合計	292,449	100.0%	346,100	100.0%	18.3%	374,771	100.0%	8.3%	363,581	100.0%	−3.0%

図 13 に 2007 年度の国内情報セキュリティツール市場のカテゴリ別分布を示す。

情報セキュリティツール市場において最大のカテゴリは「コンテンツセキュリティ対策製品」で、2007 年度には 1,323 億円、構成比にして全体の 38.2%を占めた。これに続くのが「アイデンティティ・アクセス管理製品」の 615 億円で構成比 17.8%を占め、次には「ネットワーク脅威対策製品」の 534 億円・構成比 15.4%が続く。これら 3 カテゴリで「情報セキュリティツール」市場全体の 72%を占める。これらのカテゴリにはウイルス対策製品、ファイアウォール、個人認証製品が含まれている。これら 3 製品カテゴリは、JNSA が 2005 年 2 月に発表した「IT セキュリティ対策施策の導入・実施状況とその満足度調査」報告書[33]でも既に 2004 年段階で 90%以上の導入率が確認されているほど普及の進んだ領域であり、ベンダ側の数字でもそれが裏付けられる結果となった。

2007 年度の国内「情報セキュリティツール」市場は、全体としては前年度比 18.3%と高い伸びを示した。市場の成長率で特に数字が大きかったのは「暗号製品」の 31.6%で、「アイデンティティ・アクセス管理製品」26.0%がこれに次ぐ。「システムセキュリティ管理製品」も 21.6%と高い伸びを示した。いずれも、内部統制に対応する IT 統制や情報流出防止の観点から関心が高まっている分野であり、企業がその方面の対策の充実に注力した結果であると見られる。

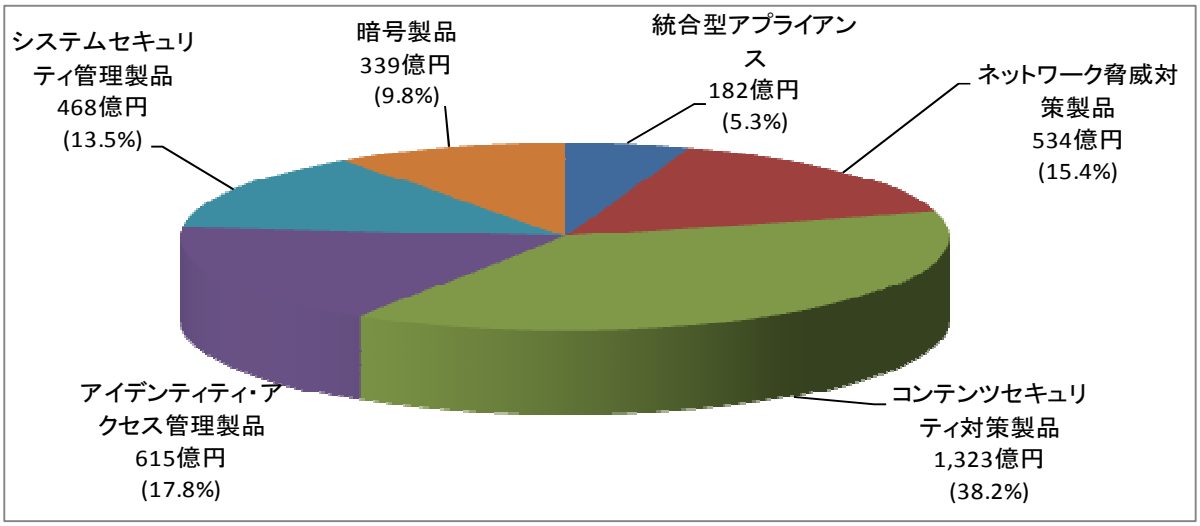
「暗号製品」に関しては、ノートパソコンの盗難・紛失やファイル交換ソフトに感染するウイ

[33] http://www.jnsa.org/active/2004/active2004_15a.html

ルスによる情報漏えいが相次ぎ、社会的にも問題となっていることから、情報流出の防衛とスキャンダルの防止を意識して導入が急速に進んだ結果と見られる。またコンピュータゲーム市場の好調を受けて、ゲーム機に組み込まれる暗号化モジュールが好調に伸びたことも市場規模を押し上げている。その結果、2006 年度で 258 億円程度の市場が、2007 年度には 339 億円の規模に達したと見込まれる。2008 年度は引き続きゲーム機等への需要を背景に他のカテゴリよりも高い伸び率を続け、前年度比 12.5%の成長率で 382 億円に達するものと推測される。

「アイデンティティ・アクセス管理製品」は主として内部統制対応の需要が市場を押し上げたものと見られる。特にこの 2 年ほどでアイデンティティ管理システムへの関心が急速に高まり、導入企業も増加している模様である。これに対応して従来「ログオン許可・アクセス管理製品」あるいは「その他のアクセス管理製品」で集計されていた「アイデンティティ管理製品」を独立したセグメントとした。この結果調査のカバレッジが若干拡大したと考えられ、このカテゴリの規模を大きくする要因ともなっていると思われる。市場規模としては 2006 年度が 488 億円、2007 年度が 615 億円（前年度比成長率 26.0%）、2008 年度は 662 億円（同 7.5%）と拡大を続けると見られる。

図 13　2007 年度の国内情報セキュリティツール市場



「システムセキュリティ管理製品」も高い成長を示した。内部統制対応と情報漏えい対策の両面で需要が加速された結果と見られる。前者はシステム利用者がネットワーク上で権限外や通常業務パターン外の異常な振る舞いをしていないかを統合監視することや、端末におけるコンプライアンス、更には記録の保全と追跡可能性確保のための統合ログ管理等のニーズが各々「セキュリティ情報管理システム／製品」「ポリシー管理・設定管理・動作監視制御製品」「その他のシステムセキュリティ製品」等の需要につながっていると考えられる。後者は主として端末における権限外のコピーや印刷の防止を目的として「ポリシー管理・設定管理・動作監視制御製品」を導入することにつながる。その結果、「システムセキュリティ管理製品」カテゴリは、2006 年度には 385 億円の規模だったものが、2007 年度には 21.6%成長して 468 億円に達したと推定する。

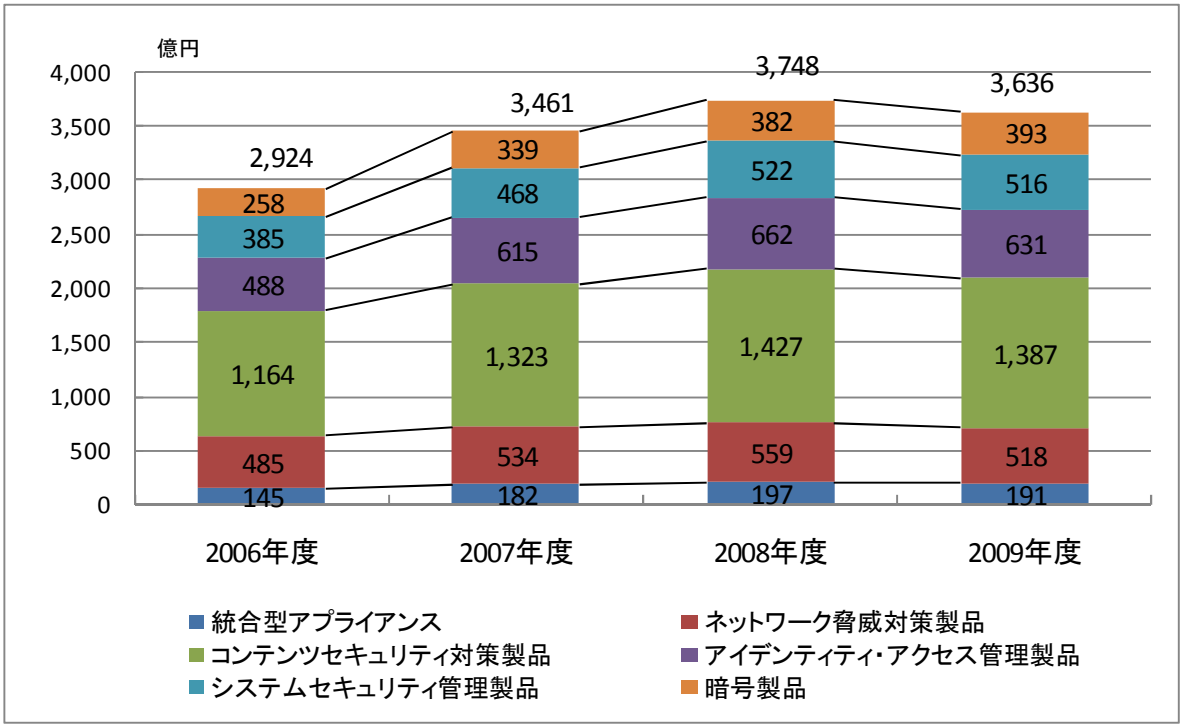
こうした傾向は 2008 年度前半まで持続したと見られ、同年度も前年度比 11.5%増を達成して 522 億円に達したものと推測する。

「統合型アプライアンス」も 2007 年度は前年度比で 25.5%増と大幅な伸びを見せた。統合型アプライアンスは 2003 年頃に製品が登場し、非常に短期間に急速に普及が進んだ製品カテゴリである。1 台のアプライアンス製品でファイアウォール機能を中心に、ウイルス対策や不正アクセス防御、VPN 通信等を同時に実現でき、設定等も比較的単純化していることから、特に専門の管理者のいない中堅中小企業向け市場及び大企業の地方拠点向けなどに積極的に受け入れられるようになっている。また、本社と小規模拠点間の通信や、社員のリモートアクセスに VPN を導入する事例が増えており、VPN ゲートウェイ機能を主眼に統合型アプライアンスを導入するケースも需要を押し上げていると見られる。

「ネットワーク脅威対策製品」の市場規模は、前回調査では 2 位だったが、今回調査では「アイデンティティ・アクセス管理製品」に抜かれて情報セキュリティツール市場第 3 位に転落した模様である。その伸び率は 2007 年度で前年比 10.2%増と二桁の伸び率を示したものの、率ではツール市場で最下位であった。ファイウォールや IDS／IPS は傾向的に統合型アプライアンスへの需要のシフトが進んでおり、また普及率が比較的高いことから市場は成熟化の傾向を見せている。ただし、インターネットバックボーンや大規模システムのゲートウェイ等の大容量・高スループットを要求する世界では、ハイエンドのファイウォールアプライアンスや、高性能ソフトウェアファイアウォールをハイパワーのサーバに搭載した形で使うことが多い。2007 年はこの面でネットワーク投資が比較的盛り上がった模様で、成熟市場の割には高い伸び率を示した。

図 14 に国内情報セキュリティツール市場の経年推移のグラフを示す。

図 14　国内情報セキュリティツール市場推移



2008 年度の国内「情報セキュリティツール」市場は、年度の半ばで世界同時不況の荒波をかぶることになった。ただし、年度の前半は 2007 年度の高い成長トレンドを維持していたと見られ、年度後半に急減速の要素に見舞われつつも年度全体ではプラス成長となったと見込まれる。経済が急激に変調をきたす中で、新規プロジェクトについては延期や実施時期の見定めによる先送りが起きつつも、すでに予算手当て済みの案件は予定通り実施するとか、一部には 2009 年度の不透明さに備えるために 2008 年度中に繰り上げ実施を決断する動きもあったということで、自動車や電機といった基幹産業ほどの急変は見なかった。2008 年度の実績見込み値は、2007 年度比 8.3%増加して推定 3,748 億円に達したものと見る。

カテゴリ別には、情報漏えい対策の需要が強い「暗号製品」が 12.5%、内部統制対応との関連性が強い「システムセキュリティ管理製品」が 11.5%と 2 ケタ成長を実現したと見られる。以下、「統合型アプライアンス」が 8.1%の伸び、スパムメール対策が活発だった「コンテンツセキュリティ対策製品」が 7.9%、「アイデンティティ・アクセス管理製品」が 7.5%と比較的高い率での市場成長が見られ、ネットワーク事業者の需要が堅調だった「ネットワーク脅威対策製品」も 4.8%とプラス成長を維持した。

2009 年度については見通しが極めて難しいが、情報セキュリティ対策は先延ばしできる課題ではないとの認識も経営者の中には生まれている模様で、特に情報漏えい防止の意識が高いことから「暗号製品」はプラス成長を維持する可能性もあり、全体としてはマイナス 3%程度と軽微な減速にとどまり、3,636 億円程度の市場規模を維持するのではないかと予測した。

7.2. 情報セキュリティツール市場のカテゴリ別分析

7.2.1 統合型アプライアンス市場

(1)製品の特性

「統合型アプライアンス製品」は、以下の二つの市場区分大分類（カテゴリ）の片方または両方に挙げられる機能を備え、二つ以上の大分類にまたがる複数の機能を１台に搭載したものと定義している。

①ネットワーク脅威対策製品

ファイアウォール、VPN、フィルタリングといった、主にネットワークの境界付近に配置し通信のハンドリング、モニタリング、ロギングを行う製品。

②コンテンツセキュリティ対策製品

アンチウイルス、アンチスパム、URL フィルタリング、といった、電子メールやウェブアクセスに対する不正行為を阻止・防止・予防する製品。

本調査の機能別市場区分では複数の製品機能を有することで、どこにも分類できないために、独立のカテゴリとして調査集計する。

近年、UTM（Unified Threat Management 統合脅威管理）という呼称が一般的になってきているが、これは米国のメーカや調査会社がつけた名前が一般に使われるようになった結果と見られる。Unified Threat Management の訳語としては「統合脅威管理」が一般化しつつあるが、本調査のアンケートに際しての定義表上は「複合脅威対策」という訳語を当てている。Management という言葉から連想する「管理」よりは対策機能が主体であることに留意したい。

統合型アプライアンス製品は、企業のセキュリティ対策において強く求められる費用対効果と利便性を同時に実現できることがポイントで、そのメリットにより中小企業への導入が進んだと見られる。製品としては、ファイアウォール機能を中心としたゲートウェイ型の製品が主で、セキュリティ対策の専任者を置けない中堅・中小企業が主なターゲットである。

(2)市場の動向

統合型アプライアンスが製品として成立し市場に受け入れられるに至った要因は、ハードウェア性能の飛躍的な向上にある。以前は、複数の機能を１台のハードウェアで稼動させることは性能の劣化を招くことから敬遠されていた。しかし、ハードウェア性能の向上によって実用に耐えるレベルの性能を発揮することが可能になった。その結果、普及機レベルでは、汎用の IA[34]機で実用上問題ないレベルのパフォーマンスが実現している。一方、パケットフィルタリングなどの特定機能をハードウェア化して非常に高いスループットを実現する技術も発展しており、それを利用することで、飛びぬけてハードウェア性能の高い専用機を実現することも可能になった。ユーザは利用目的によってこのどちらかを選択できることになり、適用の場が大きく広がっている。1 台の装置を設置することで複数の対策が実現できるという使い勝手のよさも貢献し、統合型ア

[34] インテル・アーキテクチャ　インテル社製 CPU を用いて PC 機能を実現するハードウェアセット

プライアンスの普及はここ数年で急速に進んできている。

低価格の普及機は、特に中小企業、大企業の出先事業所、小売業のような多店舗展開している企業等に多く受け入れられている。専門家の確保が難しい事業所のネットワーク環境に導入する場合に、複数の機能を一元的に簡易に実現できる一括ソリューションとして、統合型アプライアンスの需要は高まっていると見られる。小規模ネットワーク環境への普及機クラスの統合型アプライアンスの導入需要は今後も継続することが期待される。

またハイエンド機種は、データセンタや企業の基幹ネットワークといった高性能を期待される環境への導入が進んでいる。海外においては、TCO[35]に対する合理的判断に基づき、高性能タイプの統合型アプライアンスの利用が進んでいる。国内では、投資判断の保守性のためか、単機能ごとに従来型製品の高性能機を利用しつづけている事例も見られる一方､データセンタや大企業、通信事業者など広帯域且つ大容量なデータ通信を扱う企業などに多く採用されるようになってきた。

なお、ファイアウォール機能を持たない統合型アプライアンスも現れてきている。認証機能や検疫システム機能といった、これまでは専らソフトウェア製品で実現されていたものがアプライアンス化され、それらの機能群を 1 台のアプライアンスの上で実現する製品が登場している。また、帯域管理とコンテンツフィルタリングを取り合わせたようなものもある。このような非ファイアウォール起源の統合型アプライアンスの動向も注目される所である。

統合型アプライアンスは、市場が拡大していることから供給サイドから見ても魅力的な市場となっている。市場の初期は統合型アプライアンス専業ベンダが市場を開拓し、急成長したが、ファイアウォールベンダの路線転換や、大手ネットワーク装置ベンダからの参入もあり、特に低価格の普及機クラスは価格競争も発生して競争の激しい市場となりつつある。

(3)市場規模とその推移

表 8 に統合型アプライアンス製品市場の市場規模実績推定値と予測値を、図 15 にその市場規模の推移のグラフを示す。

表 8　国内統合型アプライアンス市場規模　実績と予測

市場規模（百万円）	2006 年度	2007 年度	2008 年度	2009 年度
統合型アプライアンス	14,487	18,183	19,663	19,088
対前年比成長率				
統合型アプライアンス	ー	25.5%	8.1%	−2.9%

統合型アプライアンス製品は、2006 年度にはセキュリティ市場における地位をほぼ確立した。2007 年度にはその勢いを維持し、市場成長率も 25.5%と急激な伸びを示していたが、2008 年度には 200 億円に近づくものと推定されるものの、成長率としては停滞域に入った感がある。

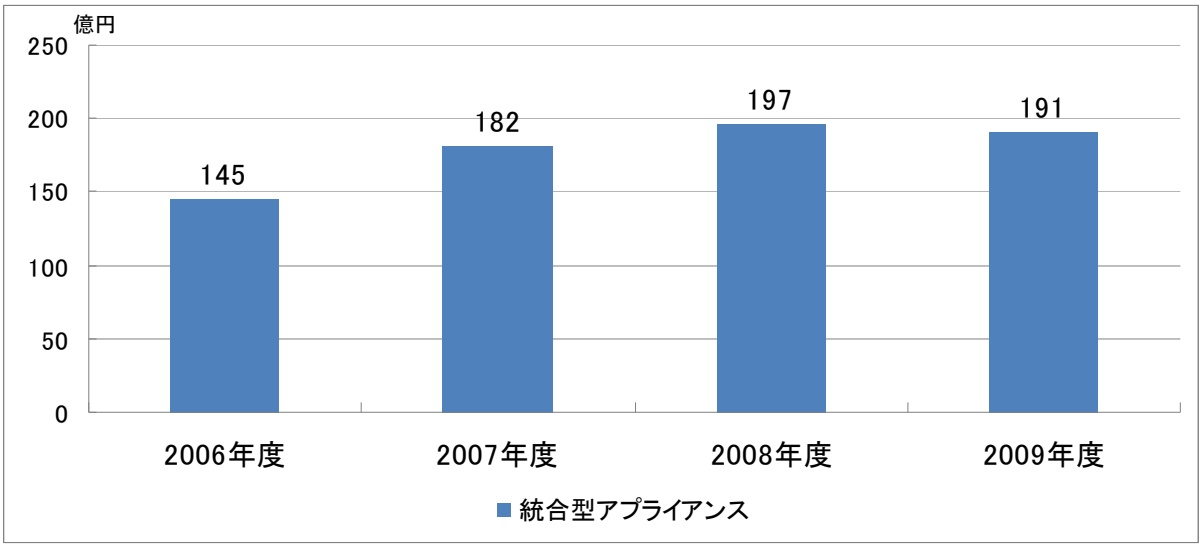
但し、廉価版の販売に関しては、依然として流れは止まっておらず、ファイアウォール製品の入れ替えに伴い、統合型アプライアンスに置き換える動きが進められている。また、市場として

[35] Total Cost of Ownership　総保有コスト又は利用（使用）総コスト

は高価格版（ハイエンド版）の流れ次第でさらに大きな変動の可能性もあると推察される。

今後については、他のセキュリティ製品などと比べて、TCO 削減を推進する企業を中心に、注目される製品になると考えられ、売上規模に関しては依然として高い数値が見込まれると予測する。市場動向で述べたように、海外市場と同様に高価格機の導入が急速に進めば、予測以上の市場成長を示す可能性もあると思われる。

図 15　国内統合型アプライアンス市場推移



7.2.2　ネットワーク脅威対策製品市場

(1)製品の特性

ネットワーク脅威対策製品は、主としてネットワークの境界付近に配置して通信のハンドリングまたはモニタリングを行い、設定に基づいてネットワーク通信の許可･不許可、アラート、ログ生成等、通信の制御と管理を行う製品のことである。通信パケットに暗号化を施し、組織外のネットワーク上でのパケット内容の盗聴・改ざんを防止する、いわゆる VPN（Virtual Private Network）製品や、ファイアウォール、侵入検知･侵入防止製品（IDS／IPS）等もこの市場区分に含んでいる。

このカテゴリでは以下の 9 種類の中分類（セグメント）にて市場区分を行っている。

①ファイアウォールアプライアンス

ファイアウォールは、ネットワーク上の通信パケットに対して、あらかじめ設定されたその企業の通信に関するルールに従って、通信の許可、遮断、制御を行うことで外部からの攻撃に対する防御や不正な通信の制限・遮断を行う製品である。そのうち、アプライアンス型製品がこのセグメントとなる。ファイウォールの多くは VPN 通信を通過させる必要があるため、VPN ゲートウェイの機能を併設している。

②ファイアウォールソフトウェア（企業向けライセンスタイプ）

ファイアウォール製品のうち、ソフトウェアとしてライセンス販売形態で提供される

製品のセグメントである。

③ファイアウォールソフトウェア（デスクトップ FW）

ファイアウォールは、組織の内と外の接点に置いて通信を一括して管理する形態が一般的だが、端末マシン個別に導入し、その端末に届く通信に対して同様の機能を提供するものがある。パーソナルファイアウォールとかデスクトップファイアウォールと呼ばれる。企業向けも個人向けも販売されている。クライアント用ウイルス対策製品がこの機能を併せ持っている場合も多く、その場合はウイルス対策製品に分類するが、単独製品の場合はこのセグメントで集計する。

④VPN アプライアンス

ネットワーク通信を暗号化して、オープンなネットワークでも専用線と同様な通信の安全を確保する機能（VPN= Virtual Private Network=機能）を提供する製品のうち、アプライアンス型のものを指す。ただし、ファイアウォールに VPN 機能が付帯する場合はファイアウォールに分類する。

⑤VPN ソフトウェア

VPN 製品でソフトウェアタイプの製品。VPN に際しては、通常、外部から VPN 通信のためにアクセスしてきた相手が、通信を許可されている相手かの確認をする認証手続きを伴うが、その認証のための通信のハンドリングも、VPN 製品が行うことが一般的である。

⑥IDS／IPS アプライアンス

通常ファイアウォールの後方（内側）に置かれ、ファイアウォールが許可した、あるいはフィルタリングされなかった通信に対して、その内容や状態を一定の方法・技術に基づき検査し、侵入もしくは攻撃と判断される通信に対して報告・警告・ログ記録等を行うのが IDS（侵入検知システム）であり、IPS（侵入防止システム）は更に遮断や阻止まで行う。本セグメントはそのような IDS／IPS 製品のうち、アプライアンス型製品を扱う。

⑦IDS／IPS ソフトウェア

IDS／IPS 製品のうち、ソフトウェア型製品。

⑧アプリケーションファイアウォール

ウェブサーバやデータベースサーバ等のアプリケーションサーバへの攻撃や不正なアクセスに対する防御を行う製品。

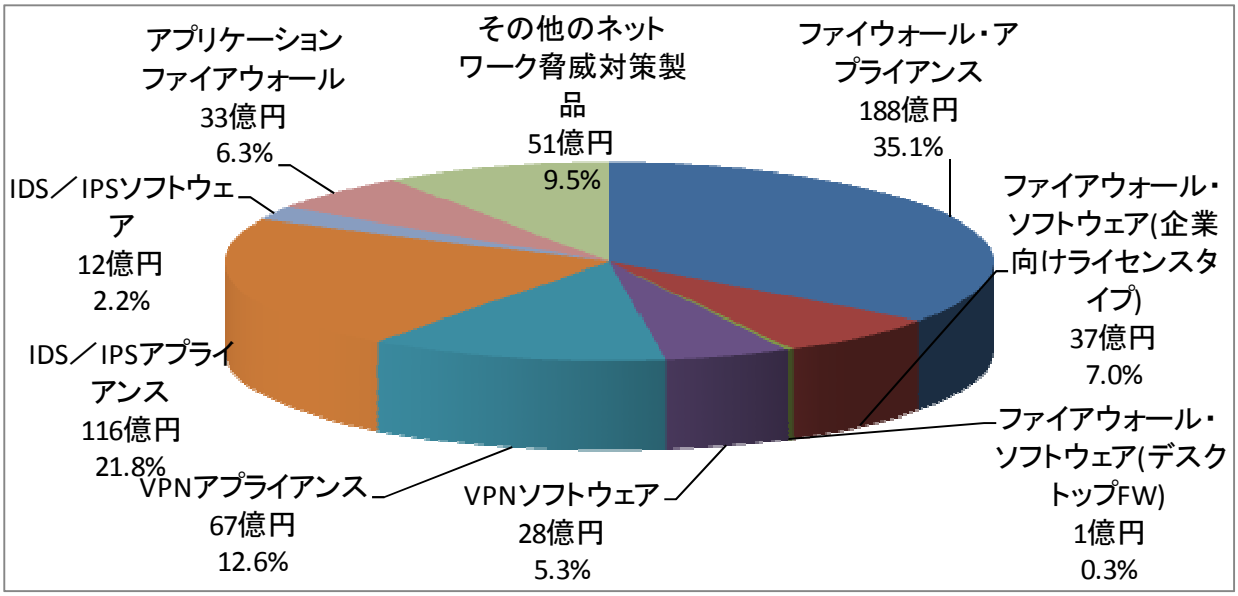
⑨その他のネットワーク脅威対策製品

外部ネットワーク（インターネット等）から内部ネットワークに対して行われる、不正侵入、盗聴、不正プログラムの挿入などの攻撃に対して、検知、防御、抑止、警告などの防衛の機能を提供する製品で上記のどのセグメントにも属さないもの。

⑵市場の動向

これらネットワーク脅威対策製品の 2007 年度におけるセグメント分布を図 16 に示す。

図 16　2007 年度のネットワーク脅威対策製品市場



ネットワーク脅威対策製品は、インターネットの商用利用が解禁されてビジネスに利用されるようになった初期のころから登場していた。1990 年代半ばには、ファイアウォールは先進的なインターネットユーザの間にかなり広まっていた。その後 IDS が登場し、IPS へ発展する流れとなっている。初期の製品はほとんどすべてソフトウェア製品として提供され、PC サーバや UNIX ワークステーションの上で使われていた。21 世紀に入って、ハードとソフトを一体化して一つの製品として提供するモデルが広がり、今日ではアプライアンス型製品が主流となっている。

また、「統合型アプライアンス」の項で見たように、マルウェア対策機能を併せて搭載するなど、複数の機能を統合して 1 台で実現する統合型アプライアンスが目覚ましい普及を見せている。ネットワーク脅威対策製品は、単機能型から複数機能統合型への移行が進んでいる。

また、この市場では、アプリケーションファイアウォールといわれる、内部ネットワークにあるサーバ上のアプリケーションに対する不正な動きを制御する製品が登場している。ファイアウォールは、通常「プロトコル」を構成する通信の内容に対して判断を行うが、アプリケーションファイアウォールはアプリケーションゲートウェイの技術を活用することで、アプリケーションレベルでの攻撃を検知し防御する。SQL インジェクションやクロスサイトスクリプティングなどの、ウェブアプリケーションの脆弱性を狙った攻撃[36]が激しくなっており、その対応を目的としたウェブアプリケーションファイアウォールがその代表例である。PCI DSS[37]でウェブアプリケーションの防御が要求されていることや OWASP[38]という団体の活動からも注目を集めているこ

---

[36] ウェブアプリケーションの脆弱性とその対策については、独立行政法人情報処理推進機構のウェブサイトを参照。　http://www.ipa.go.jp/security/vuln/documents/2005/website_security.pdf

[37] PCI DSS: Payment-Card Industry Data Security Standard　クレジットカード事業者の団体が制定した、クレジットカード事業者や加盟店に準拠を要求するセキュリティ対策基準。
https://www.pcisecuritystandards.org/index.htm

[38] OWASP　（Open Web Application Security Project）　アメリカで組織され世界的に展開している非営利活動団体。ウェブアプリケーションのセキュリティ対策を中心に活動している。
http://www.owasp.org/index.php/Main_Page

とが伺える。ウェブアプリケーションの他に、データベースをガードする製品もある[39]。

このように新しい技術を取り入れた製品が登場し、ネットワークの脅威に対応した製品の市場を広げている一方で、UTM とも呼ばれる統合型アプライアンスに移行する動きも強く表れている。その結果、ネットワーク脅威対策製品として市場を見てみると、市場の伸びは限定的である。但し、ハイエンドの専用機は特定市場では確固たる地位を保っている他、ソフトウェアタイプが主流である VPN のクライアント機能はリモートアクセスの利用拡大から増加しており、金額面にも現れてきた。

(3)市場規模とその推移

表 9 にネットワーク脅威対策製品市場の市場規模実績推定値と予測値を、図 17 にその市場規模の推移のグラフを示す。

ネットワーク脅威対策製品のカテゴリは、2007 年度における売上実績推定値が 534 億円と、情報セキュリティツール市場の中で 3 番目となっており、15.4%の構成比を持っている。しかし前回の調査では情報セキュリティツール市場の中で基準年度である 2006 年度において 2 番手に位置しており、3 番目の規模であったアイデンティティ・アクセス管理製品市場に、今回調査で追い越されたことになる。やはりウイルス対策製品と共に最も早くから登場したセキュリティ対策手段であったため市場の成熟化が進んでいることに加え、統合型アプライアンスへのシフトが引き続き進んでいることが伸び率鈍化の要因と言える。2006 年度(485 億円)からの伸び率は 10.2%とツール市場のカテゴリ別では最後位につけており、特に IDS／IPS ソフトウェアセグメントは対前年度比成長率がマイナス 51.9%と、アプライアンスへのシフトが進んでいることが伺える。

表 9　国内ネットワーク脅威対策製品市場規模　実績と予測

市場規模(百万円)	2006 年度	2007 年度	2008 年度	2009 年度
ファイウォールアプライアンス	17,968	18,751	20,252	18,526
ファイアウォールソフトウェア(企業向けライセンスタイプ)	3,713	3,718	3,801	3,153
ファイアウォールソフトウェア(デスクトップ FW)	141	135	129	93
VPN ソフトウェア	2,530	2,830	2,919	2,689
VPN アプライアンス	5,065	6,730	7,296	7,137
IDS／IPS アプライアンス	10,514	11,615	12,187	11,369
IDS／IPS ソフトウェア	2,455	1,181	1,121	825
アプリケーションファイアウォール	1,679	3,344	3,650	3,731
その他のネットワーク脅威対策製品	4,390	5,079	4,570	4,259
合計	48,455	53,383	55,925	51,781
構成比				
ファイウォールアプライアンス	37.1%	35.1%	36.2%	35.8%
ファイアウォールソフトウェア(企業向けライセンスタイプ)	7.7%	7.0%	6.8%	6.1%
ファイアウォールソフトウェア(デスクトップ FW)	0.3%	0.3%	0.2%	0.2%

[39] 業界団体としては、国内ではデータベース・セキュリティ・コンソーシアム（DBSC）が活動している。
http://www.db-security.org/

VPN ソフトウェア	5.2%	5.3%	5.2%	5.2%
VPN アプライアンス	10.5%	12.6%	13.0%	13.8%
IDS／IPS アプライアンス	21.7%	21.8%	21.8%	22.0%
IDS／IPS ソフトウェア	5.1%	2.2%	2.0%	1.6%
アプリケーションファイアウォール	3.5%	6.3%	6.5%	7.2%
その他のネットワーク脅威対策製品	9.1%	9.5%	8.2%	8.2%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
ファイウォールアプライアンス	ー	4.4%	8.0%	−8.5%
ファイアウォールソフトウェア(企業向けライセンスタイプ)	ー	0.1%	2.2%	−17.1%
ファイアウォールソフトウェア(デスクトップ FW)	ー	−3.9%	−4.6%	−28.2%
VPN ソフトウェア	ー	11.9%	3.2%	−7.9%
VPN アプライアンス	ー	32.9%	8.4%	−2.2%
IDS／IPS アプライアンス	ー	10.5%	4.9%	−6.7%
IDS／IPS ソフトウェア	ー	−51.9%	−5.0%	−26.4%
アプリケーションファイアウォール	ー	99.1%	9.1%	2.2%
その他のネットワーク脅威対策製品	ー	15.7%	−10.0%	−6.8%
合計	ー	10.2%	4.8%	−7.4%

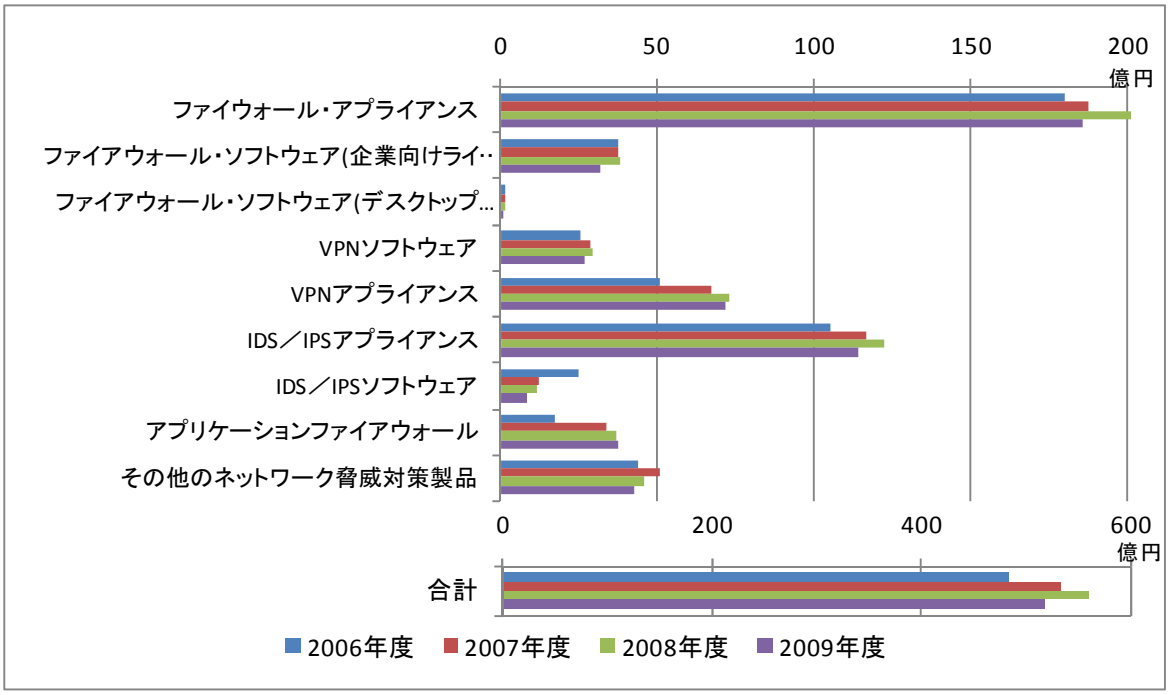
ネットワーク脅威対策製品のカテゴリの中では 1 番大きいセグメントであるファイアウォールアプライアンス製品は、2006 年度 180 億円、2007 年度 188 億円、2008 年度 203 億円と増加している。通信事業者を中心とするハイエンドのユーザは、高機能のファイアウォールを単機能型で導入する例が多い。2007、2008 年度はこれら事業者の設備投資サイクルから更新期に当り、需要を下支えしたものと考えられる。その結果、統合型アプライアンスへのシフトによるマイナスインパクトを吸収して市場の伸びを支えたものと見られる。

ネットワーク脅威対策製品のカテゴリの中では 2 番目に大きいセグメントである IDS／IPS アプライアンス製品は、2007 年度は前年度比 10.5%増の 116 億円という市場規模となっている。これは、ハードウェアの価格が下がったことで導入しやすくなったためと考えられる。

一方、IDS／IPS ソフトウェアは製品供給も限定され、アプライアンスへの移行が進む中で、2007 年度に前年度比マイナス 51.9%と大幅な落ち込みを見せたが、2008 年度以降も落ち込みは進み、2009 年度は 8 億円にまで縮小するという推定値となった。ベンダの多くがアプライアンス製品へ移行しており、パブリックドメインのソフトウェア IDS が使われている他は、商用の供給がほとんどなくなっていることの結果であると考えられる。

VPN アプライアンス製品は、2006 年度から 2007 年度への成長率が 32.9%と極めて高く、67 億円という推定市場規模になった。このセグメントは 2008 年度に 8.4%成長して 73 億円に拡大すると推測される。これは、ブロードバンド通信環境の一層の充実を背景に、いわゆるモバイルワーカーやテレワーキング（ホームオフィスやサテライトオフィス）が一層盛んになっている結果であると考えられ、内部ネットワークへのアクセスのコントロールが進んできたものと見られる。

図 17　ネットワーク脅威対策製品市場推移



前回調査より独立セグメントとしたアプリケーションファイアウォールは、2006 年度から 2007 年度への成長率が 99.1%と非常に高く、33 億円という推定市場規模になった。前回調査において、2005 年度から 2006 年度への成長率も 99.9%だったことから、市場の立ち上がり期に特有の、急速な浸透フェーズにあると見られる。2005 年に著名企業のウェブへの攻撃による事件が起こったことと、PCI DSS 標準の導入要件となったことも背景にあるのではないかと考えられる。また、データベースへの防御機能を提供するタイプにおいても、企業秘密の漏えい事件や内部統制への対応から需要が高まっている模様で、今後も市場規模を押し上げるものと期待される。全体としてはこの先も成長を続けて 2009 年度への成長率もネットワーク脅威対策製品市場の中で唯一のプラス成長が期待できると予測する。

7.2.3　コンテンツセキュリティ対策製品市場

(1)製品の特性

コンテンツセキュリティ対策製品とは、コンテンツ（通信における情報伝達の内容）についてセキュリティに関わる不都合の有無をチェックすることを主目的とした製品群である。ウイルス対策、不正プログラム（マルウェアなどの悪意のあるプログラムを含む）対策、スパムメール（迷惑メール）　対策、URL フィルタリング、メールフィルタリング、フィッシング詐欺対策製品等が該当する。このカテゴリでは以下の 7 種類の中分類（セグメント）にて市場区分を行っている。

① ウイルス・不正プログラム対策ソフトウェア（企業向けライセンス契約）／アプライアンス

ウイルス、ワーム、スパイウェア、トロイの木馬、ボット等の不正プログラムを検知し、更に防御や排除する製品。クライアントパソコンやサーバに、ソフトウェアとしてインストールして使う形が一般的で、企業等向けにライセンス契約方式で提供される。また、内部ネットワークの入り口にゲートウェイ型で設置して通過するトラフィックをチェックする使い方もある。この場合はアプライアンス型製品が利用されるケースが多い。ウイルス対策製品の特徴として、不正プログラムを検知するための一種のリストである定義ファイルを常時更新する必要があり、ソフトウェア代金の他に、この定義ファイルの更新権は年間契約で支払う形が一般的だが、その更新料もこの市場を構成する金額としてカウントする。この製品には、付加機能として、ファイアウォール、IDS、スパム対策、URL フィルタリング等の機能を併設するものが一般的であるが、最近は脅威の複雑化と深刻化から、それぞれ個別の対策製品を個別に導入する方向にあると見られる。

② ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ）

ウイルスを始めとするマルウェア対策ソフトで、個人ユーザが自宅のパソコンで使うための製品である。製品形態としては、ソフトウェアパッケージとして家電店等の店頭やオンラインショップで販売される形が主流である。またネットワーク越しに製品をダウンロードしてインストールする、オンラインダウンロード販売も増加している。①同様、プログラムや定義ファイル更新の年次参照権の販売代金も含む。また、個人向けウイルス対策製品のほとんどが、デスクトップファイアウォール、HIPS（ホスト IPS)、スパム対策、URL フィルタリング等の機能を併せ持っている。

③ スパムメール対策ソフトウェア／アプライアンス

宣伝、勧誘等の目的で無差別・大量に送りつけられる、不要もしくは有害な内容を含むメール、いわゆるスパムメールに対する対策製品。フィルタリング、マーキング（タグ付け)、警告、隔離、排除（廃棄）等の対応をする。クライアント用、サーバ用、ゲートウェイ型のタイプがあり、製品形態もソフトウェアとアプライアンスがある。

④ フィッシング対策・ソフトウェア／システム

いわゆるフィッシング詐欺目的で送付される電子メールのフィルタリング、フィッシングサイトへのアクセスや閲覧に対する警告、ウェブサイトのフィッシングに関する安全性の確認等の機能を提供する、ソフトウェア、システムもしくはサービス。

⑤ URL フィルタリングソフトウェア／アプライアンス

アクセスしようとするインターネット上のウェブサイト（ホームページ）につき、有害、危険、不適格等と判断される場合に、停止、警告、ログ保存等を行うソフトウェアもしくはアプライアンス製品。判断は、自社の基準により禁止するサイトを指定するブラックリスト、キーワードによるフィルタリング、ツールベンダが提供するリスト等に基づく。

企業向けと個人向けの両方がある。特に家庭において子供を有害サイトから守るため

の使われ方が関心を集めている。

⑥ メールフィルタリングソフトウェア／アプライアンス

送受信される電子メールに対して、電子メールアドレスや内容、添付ファイル等を検査し、情報漏えい等の情報セキュリティ事故を防止するための製品。所定の条件（有害、不適格、情報漏えい、レピュティションサービス[40]によるリスト等）に合致（もしくは違反）する内容を含むものに対して処理（停止、隔離、警告、管理者への通報もしくは回送、ログ保存等）を行う。単に全メールを無条件にアーカイブするだけのものを除く。）を行うソフトウェアもしくはアプライアンス製品。ウイルス・不正プログラム対策製品にこの機能が併設される場合は、ウイルス・不正プログラム対策製品に分類する。

⑦ その他のセキュアコンテンツ管理製品

メール等の電子データに関して、主として情報セキュリティの目的でフィルタリングその他の機能を提供する製品で、上記のいずれにも属さない、あるいは特定の中分類に仕分けできないもの。いわゆる Digital Rights Management（DRM）製品やそのシステム、及び DLP （Data Loss/Leak/Leakage Protection/Prevention） 製品[41]やそのシステムもこのセグメントに分類する。

(2)市場の動向

以上見てきた7つのセグメントの2008年度における分布を図18に示す。

ウイルス対策の企業における実施率は、2004年度の段階で100%に近く、その普及度はきわめて高い。その割に「ウイルス・不正プログラム対策ソフトウェア（企業向けライセンス契約）／アプライアンス」の市場規模は安定して拡大してきている。要因としては、ウイルス定義ファイルの更新サービスを毎年継続的に購入する必要があるビジネスモデルにより、安定売上のベースライン（基礎部分）を確保する戦略が取られていることが大きい。また、クライアントパソコンの設置台数が増え続けていると見られることも、販売額の伸びを支えていると考えられる。

個人ユーザ向けウイルス対策製品の市場も順調に拡大してきた。ウイルス、スパム、フィッシングといった脅威が広く報道され、また行政面でもNPO等と連携して注意喚起や啓発イベントが継続的に実施されている。このような動きが市場を活性化させており、2006年度までは、市場はかなりのペースで拡大を続けてきた。市場への新規参入の動きも比較的活発で、一部では価格競争も起きている。一部ベンダで定義ファイルの更新料が不要な売切り型や、同一価格で複数ライセンスが使用可能な商品が提供されるなどの例が見られる。

ウイルス対策製品の供給ベンダは世界的にビジネスを展開する比較的規模の大きい企業が中心であった。これは、24 時間対応で新種のウイルスを検出してそれを反映したウイルス定義ファイルを数時間以内に作成し、全世界のユーザに提供するというサービスモデルが必須であり、組織

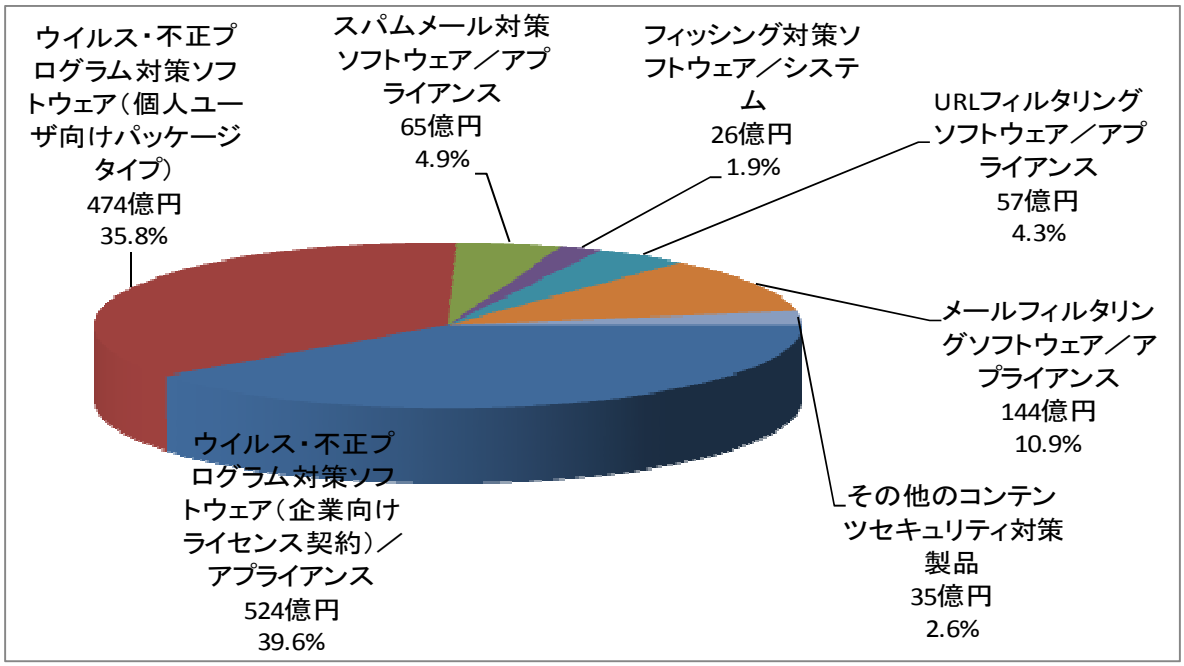
[40] Reputation Service ウェブサイトやメールの発信源等の URL について、過去の不正行為の事例や安全に通信された実績等の情報に基づき、ウイルス対策ツールベンダや専門事業者が安全度の評価をした結果のデータベースを Reputation（英語の元の意味は評判、評価）と呼び、アクセス制御やフィルタリングに際しての判断根拠として利用する技術及びそのサービス。11.5 項(1)参照。

[41] データやファイルそのものの動きを監視・トレースすることで情報漏えい・流出を防止しようとする技術並びに製品。11.5 項(3)参照。

と資本の力への依存度が高かったことによる。しかし近年、ハードウェア価格の下落と対応システムの自動運転や効率的に定義ファイルを開発するアルゴリズムの開発が進み、以前ほどの資本蓄積が必要でなくなったことから、小規模でも特徴ある製品やサービスを提供するベンダが台頭してきた。また不正プログラムの地域性も増しており、ローカルに特徴を出せる環境にもなっている。その結果新規参入が増加し、競争が生じる市場状態になっている。

ウイルスやワーム同様外部から巧妙に送り込まれるが、取り付いた先での破壊活動は行わず、そこから盗み出した情報をひそかに外部に送る機能を果たすものをスパイウェアと呼ぶ。スパイウェアとして検出したものの中には、インターネット利用の利便性のために情報を送出するプログラムもあり、全てが不正と言えない面もあるが、情報窃取目的のものが増えている。スパイウェアは銀行口座や暗証番号の情報を盗み出し被害をもたらした事例もあり、その脅威は深刻化している。悪意や不正な目的で使われるものは「マルウェア」（悪意を持ったソフトウェア）と呼ばれることもある。

図 18　2007 年度のコンテンツセキュリティ対策製品市場



商品やサービスの販売、そのためのウェブサイトへの誘導を目的に、不特定多数に繰り返し多量に送りつけられるメールをスパムメールと呼ぶ。その中には、ポルノ系、出会い系など公序良俗に反するものや未成年者に有害なものも多く、またいわゆるワンクリック詐欺の手段としても多用され、被害が深刻化している。更には個人情報の詐取など悪意を持ったウェブサイトへの誘導を図るものなど、フィッシングの手段ともなっている。また、多量・無差別にばら撒かれ、メールサーバの自動転送機能も利用することから、回線容量を浪費し、通信の質や速度に悪影響を与えるという問題も引き起こしている。これに対応するスパムメール対策製品は、従来はアンチウイルス製品のオプションとして提供される例も多かったが、その脅威の深刻化と共に専用製品化が進み、アプライアンスとして提供される製品が増えている。スパム判定を行うフィルタリン

グ（選別）エンジンは、各国の言語特性に合わせた開発が必要であり、またフィルタリングのためのURL リストの開発にスピードと信頼性が求められている。このために大手アンチウイルスベンダに加え、メールセキュリティ対策に特化する企業の参入も増えている。後者はメールフィルタリングと一体の製品として提供する形態が多い。新しい動きとしては、メールチェック（スパム・マルウェア対策）を、メールボックスを企業から預かってサービスするサービスモデルが売上を伸ばしている。ソースIPアドレスによりフィルタリングする、ERS（E-mail Reputation Service）というサービスも登場している。2007年度から2008年度にかけてはスパルメールの激しさが一段と増した時期で、多くの企業が緊急的に対策ツールの導入を余儀なくされた模様である。この結果、2007年度には市場規模は急拡大したものと見られる。

ネットワークの脅威は、不正アクセス・不正侵入の他に、不正プログラム・マルウェアの侵入が非常に巧妙に行われるようになって深刻度を増している。一時期主流であった電子メールへの添付から、ウェブからの侵入に侵入経路の主流が移っている。スパムメールやフィッシングメールで悪意のあるサイトへ誘導し、クリックや閲覧に伴ってマルウェアを送り込む方式や、正規のウェブサイトを改ざんして目に見えない形でマルウェアを埋め込む等、複雑化・悪質化が進み、標的型攻撃[42]などでは被害の防止が極めて困難になっている。このように攻撃はウイルス・ワーム、スパイウェア、スパムメール、これらを取み合わせて使う等、益々多様化・複雑化している。これらに対する対策は総合化する方向に向かっており、端末を総合的にて守るという趣旨から、「エンドポイントセキュリティ」という言葉が一般化してきた。つまり端末防御は総合化がコンセプトになっていると言える。一方で、端末側の負担の増大を緩和するために、サーバ側、あるいはインターネット経路上でフィルタリング等の機能をサービスとして提供する方向も見えてきている。特にスパムメールの急増に対して処理能力の追随が容易なフィルタリングサービスは運用面・コスト面のメリットもあり、需要を伸ばしている。ツールの自営からサービスの活用への流れと見ることができる。

URL フィルタリング製品は、導入の主目的が、閲覧して欲しくないウェブサイトへのアクセス制限からネットワーク帯域の節約へと変化し、昨今では情報セキュリティ対策（内部からの情報漏えい対策）のツールへと変化してきている。それはウェブ技術の進化が情報発信の多様化と利便性の向上をもたらした反面、ウェブサイトがサイバー犯罪の拠点としても活用が進んでしまったことに対する対策の必要からである。この分野では、言語の問題やウェブサイトの地域性や文化の問題から、国産ベンダの製品供給が目立っている。また、大手ウイルス対策ベンダは従来型のURLフィルタリングとは異なるウェブサイトの評価を行うサービス、いわゆるレピュティションサービスを提供している。レピュティションサービスはフィッシング詐欺サイトやウイルス・スパイウェアなどに感染する恐れがあるサイトなどの危険サイトの情報を提供するもので、URL フィルタリングの参照DBに取込むことで安全を高める取組と言える。また逆に、ベンダが安全を確認したサイトの情報を提供することで、それ以外のURLへのアクセスに際してアラートを出すような使い方もある。

メールフィルタリング製品は、情報漏えいリスクへの関心の高まりから需要は拡大する方向に

[42] 特定の組織に向けて固有の情報を盛り込んで送られるメールにより、悪意あるサイトへ誘導する攻撃。詳しくは IPA が公表する 10 大脅威等を参照。 URL: http://www.ipa.go.jp/security/vuln/10threats2009.html

あり、製品の供給も活発化する傾向が見受けられる。また、言語の問題から、URL フィルタリング同様、国産ベンダの製品供給が目立っている。近年ではメールの誤送信（誤配信）による情報漏えいの危険も顕在化しており、対策を講ずる企業も増加の傾向にある。この誤送信防止対策として、ゲートウェイ側での一次滞留機能や、メールクライアントソフトのプラグインモジュールによる宛先確認機能（ポップアップ表示による注意喚起）などが注目されている。また、ヒューマンエラーを完全に防ぐことは不可能との視点から、データそのものを検知対象としてその社外への流れを制御するDLP（Data Leakage Protection）という考え方も登場している。

フィッシング（詐欺）とは、金融機関などからの正規のメールやウェブサイトを装い、銀行口座の暗証番号やクレジットカード番号などを詐取する詐欺行為である。「釣り」を意味する「fishing」が語源だが、偽装の手法が洗練されている（sophisticated）ことから「phishing」と綴るようになったとする説がある。また、ファーミング（pharming）と呼ばれるDomain Name System（DNS）の設定を書き換えインターネットの閲覧者を偽のウェブサイトに誘導する手口もある。このように手口が悪質化し様々な手法で偽サイトへの誘導が行われているため被害は増加している。フィッシング詐欺への対応策としては、メールの送信者欄を信用しない、ウェブサイトで個人情報などを登録する際にフォームの送受信にSSLが利用されているか確認する、メールに示された連絡方法（リンクなど）以外の正規のものと確認できている電話番号やURLなどから案内が本物かどうかを確認する、などが挙げられる。昨今のフィッシング詐欺の被害（インターネットバンキングにおける不正引出しなど）件数は、2006年度220件、2007年度1,157件（前年度比5.2 倍）と急速な増加傾向にある。その被害の深刻化に伴って、盗難クレジットカード被害と同様に被害補償を実施する動きも出てきている。また、企業側の対策も被害の急増に対応して一気に加速し、2007年度は市場規模が急拡大したものと見られる。金融業界やネット通販などの小売業界における対策や、ISPの協力 、PC ベンダの対応（エージェントのプリインストール）が進むことで、市場も拡大を続けるのではないかと予測される。

「その他コンテンツセキュリティ対策製品」の中ではDRM（Digital Rights Management）とDLP （Data Loss/Leak/Leakage Protection/Prevention）呼ばれる技術が注目される。一般的にDRM は動画や楽曲の著作権保護を目的としたものを指すが、企業の持つ営業秘密や設計図面等の知的財産権の保護にも利用されており、デジタルドキュメントの利用権管理という意味合いがある。具体的には、対象となるファイルに暗号化等によりアクセス･利用の制限をかけ、その制限を利用する人の属性、方法、時間、場所、回数等によってコントロールすることで、権利者の意図する範囲と方法での利用を担保することが可能となる。用途としては、契約書等重要書類向け、CAD データ等の下請け等への提供に際しての技術漏えい対策、有価証券等の電子化に際しての原本性確保や複製防止等が考えられている。企業の営業秘密等の保護対応分野の製品は、ベンダによってはIRM（Information Rights Management）とも呼ぶ。

DLPはネットワークや外部媒体（USBメモリなど） を経由しての情報漏えい対策を行うものである。機密データ固有の特徴を抽出したフィンガープリント（人間でいう指紋のようなもの）、キーワード、特定のデータに固有の文字の配列などを用いて機密データを検知し、流出を防ぐ。ゲートウェイに設置してメールやネットワーク経由の流出を見張るものや、エンドポイントに常駐するエージェントが印刷や取外し可能媒体への書込みを検出するタイプなどがある。メールのチ

ェックやケアレスミスによる誤送信の防止、意図的な持出しを未然に防ぐことが困難なことから、データそのものの動きを直接モニタすることで流出を防ごうという考え方に基づく、新しい技術、新しい製品である。

(3)市場規模とその推移

表10に国内コンテンツセキュリティ対策製品の市場規模実績推定値と予測値を、図19にその市場規模の推移のグラフを示す。

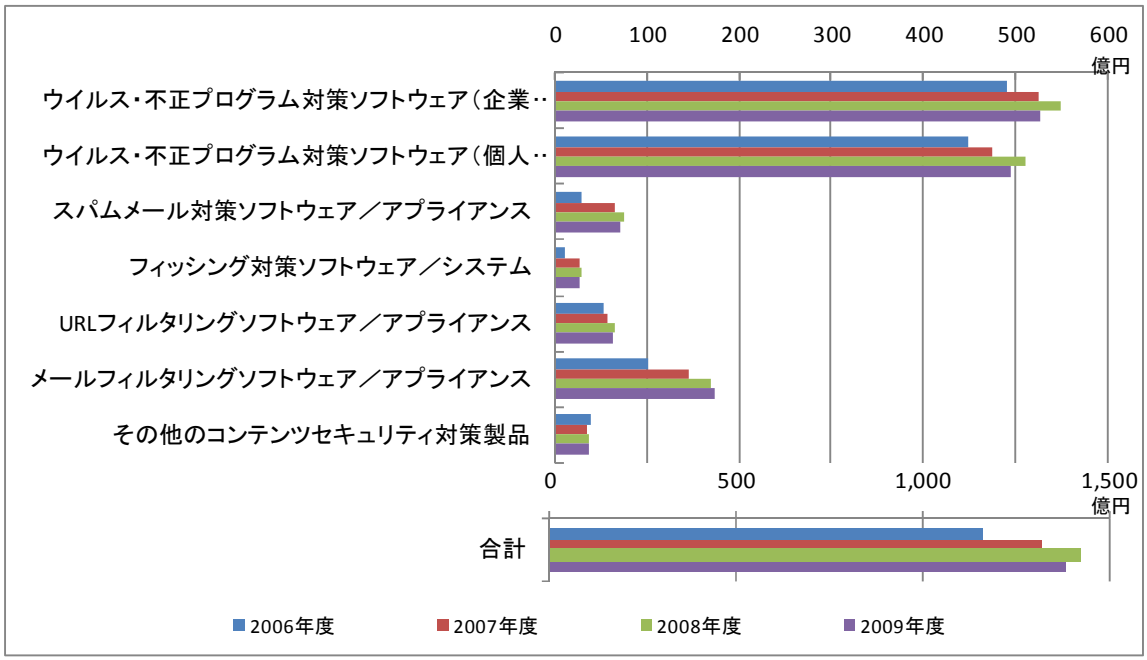
表 10　国内コンテンツセキュリティ対策製品市場規模　実績と予測

市場規模(百万円)	2006 年度	2007 年度	2008 年度	2009 年度
ウイルス・不正プログラム対策ソフトウェア(企業向けライセンス契約)／アプライアンス	48,953	52,370	54,688	52,641
ウイルス・不正プログラム対策ソフトウェア(個人ユーザ向けパッケージタイプ)	44,734	47,371	50,984	49,396
スパムメール対策ソフトウェア／アプライアンス	2,832	6,467	7,392	7,009
フィッシング対策ソフトウェア／システム	947	2,560	2,740	2,522
URL フィルタリングソフトウェア／アプライアンス	5,216	5,664	6,335	6,269
メールフィルタリングソフトウェア／アプライアンス	9,944	14,372	16,888	17,354
その他のコンテンツセキュリティ対策製品	3,820	3,505	3,677	3,529
合計	116,446	132,309	142,704	138,721
構成比				
ウイルス・不正プログラム対策ソフトウェア(企業向けライセンス契約)／アプライアンス	42.0%	39.6%	38.3%	37.9%
ウイルス・不正プログラム対策ソフトウェア(個人ユーザ向けパッケージタイプ)	38.4%	35.8%	35.7%	35.6%
スパムメール対策ソフトウェア／アプライアンス	2.4%	4.9%	5.2%	5.1%
フィッシング対策ソフトウェア／システム	0.8%	1.9%	1.9%	1.8%
URL フィルタリングソフトウェア／アプライアンス	4.5%	4.3%	4.4%	4.5%
メールフィルタリングソフトウェア／アプライアンス	8.5%	10.9%	11.8%	12.5%
その他のコンテンツセキュリティ対策製品	3.3%	2.6%	2.6%	2.5%
合計	100.00%	100.00%	100.00%	100.00%
対前年度比成長率				
ウイルス・不正プログラム対策ソフトウェア(企業向けライセンス契約)／アプライアンス	―	7.0%	4.4%	−3.7%
ウイルス・不正プログラム対策ソフトウェア(個人ユーザ向けパッケージタイプ)	―	5.9%	7.6%	−3.1%
スパムメール対策ソフトウェア／アプライアンス	―	128.4%	14.3%	−5.2%
フィッシング対策ソフトウェア／システム	―	170.3%	7.0%	−8.0%
URL フィルタリングソフトウェア／アプライアンス	―	8.6%	11.8%	−1.0%
メールフィルタリングソフトウェア／アプライアンス	―	44.5%	17.5%	2.8%
その他のコンテンツセキュリティ対策製品	―	−8.3%	4.9%	−4.0%
合計	―	13.6%	7.9%	−2.8%

「コンテンツセキュリティ対策製品」は 2007 年度の市場規模が 1,323 億円に達した。「情報セキュリティツール」市場の中で唯一 1000 億円を上回る最大のカテゴリである。その約８割は企

業向けと個人向けを合わせた「ウイルス・不正プログラム対策ソフトウェア」が占めている。このセグメントは普及率も高く成熟が進んでいるが、スパム対策やフィッシング対策という、深刻化が増す脅威に対する対策製品の伸びに引っ張られて、2007 年度はカテゴリ全体で 13.8%と比較的高い伸びを示した。ただし、2007 年度から 2008 年度にかけては 7.9%と伸び率が縮小し、2009 年度は経済情勢の急激な悪化の影響を受けて前年比 マイナス 2.8%になると推定される。ウイルス・不正プログラム対策ソフトウェアの個人向け市場には低価格及び更新無償版の製品が台頭し、企業向け市場ではサブスクリプションライセンス（ウイルス定義ファイルや URL データベースの年間利用料及び使用料）の見直しを図り、より低価格な製品に乗り換える傾向がある。SaaS などサービスを利用する企業も増えてきているため、ウイルス・不正プログラム対策ソフトウェア／アプライアンス市場の伸びは一層緩やかになると考えられる。2007 年度に極めて高い伸びを示してこのカテゴリの成長率を押し上げたスパム対策やフィッシング対策製品は、普及率が高まると共に伸び率も穏やかなものになると想定されるため、コンテンツセキュリティ対策製品全体としては、緩やかな拡大傾向に移行するものと推測される。（ただし、2009 年度は他市場同様マイナスを見込む。）

図 19　国内コンテンツセキュリティ対策製品市場推移



7.2.4　アイデンティティ・アクセス管理製品市場

(1)製品の特性

アイデンティティ・アクセス管理とは、情報システムやネットワーク、あるいはファイルといった IT 資源にユーザがアクセスする際に、そのアクセスする本人がシステムに登録された正規のユーザであるかを確認・検証し、IT 資源の利用を正規の権限が認められている範囲とレベルに限定することで、情報システムの安全を確保する技術的手法である。この市場には、本人特定（ア

イデンティファイ）と認証、アクセス権限の付与と管理、電子証明の発行と管理等の機能を提供する各種認証デバイス（装置・機器）、アイデンティティ管理システム、ディレクトリ管理システム、PKI 関連システム、シングルサインオンシステムなどが含まれる。Authentication（認証）、Authorization（承認）、Access Control（アクセス権の管理・制御） の 3A という呼び方もされる。昨年までは、アクセス管理製品市場という名称で紹介していたが、本年度よりアイデンティティ・アクセス管理市場という名称に変更した。

このカテゴリには以下の 6 セグメントを区分定義している。

① 個人認証用デバイス及びその認証システム

ワンタイムパスワード、IC カード、USB キー、携帯電話等を用いて本人確認する機能を提供するデバイス、及びそのシステム（生体認証を除く）などがある。認証は、ユーザを特定するための情報（ID）と、そのユーザが本人であることを確認するための情報（通常は本人しか知らないものや本人しか持っていないもので、コンピュータシステムにより認識ができるもの）の組合せにより行うのが一般的である。ワンタイムパスワードとして実用化されているものには、ハードウェアタイプとソフトウェアタイプの２種類の製品が存在する。ハードウェアタイプには、時刻同期、カウンタ同期、チャレンジレスポンス等の方式が存在し、ソフトウェアタイプには、PC や携帯電話にソフトウェアをインストールするものや、ウェブブラウザを利用し、位置情報やイメージ情報からワンタイムパスワードを生成する製品が存在する。

② 個人認証用生体認証デバイス及びその認証システム

生体認証に使われる身体的特徴として実用化されているものとしては、指紋、手や指の静脈パターン、虹彩や網膜のパターン、顔そのもの、更には行為や行動の癖や特徴、声といったものがある。生体認証に使われる情報は ID・パスワードと違って、個人を特定する上で代替のきかない性格を持つため、一旦そのデジタルデータが漏えいした場合の影響は大きく、そのデータについてはシステム的に厳格な管理が求められる。また運用面についてもユーザの心理面への配慮が求められる。

③ アイデンティティ管理製品

人事情報等と連携してユーザのアクセス権限を動的に管理する、いわゆるプロビジョニング（ユーザ別のシステム利用権限の定義）やアイデンティティ（本人特定情報）管理製品等がこのカテゴリを構成している。社員の流動化と派遣・パート等従業員構成の複雑化に伴い、システム上のユーザ管理も必然的に複雑化する。また同時に、業務の IT 化、システムのネットワーク化もますます進展するため、アクセス管理とユーザ管理の重要性と難しさが共に深まって行く。企業内に種々点在するシステムの ID 管理を統合するアイデンティティ管理ツールは、物理的な一元化が困難な環境において、論理的に一元化できる仕組みを構築するためのツールとして今後普及が見込まれる。

④ ログオン管理／アクセス許可製品

「アクセス許可製品」は、正しいユーザにアクセス権限を付与することで、保護対象となる情報処理資源に対してのアクセスをコントロール（管理・制御）する。ポリシールールに基づきアクセスコントロールリスト（ACL）を作成し、それを運用することで、

どのようなユーザにどのようなアクション（システムやネットワークへのログオン、アプリケーションの実行、データベースの参照、ファイル操作等）が許されるのか、をリソースの側で管理する。アクセス許可製品で保護対象となる情報処理資源はファイルやディレクトリをはじめ、ポートやログインアプリケーション、マシン名、ネットワークID、メモリ等、多岐に渡る。

「個人認証用デバイス及びその認証システム」と並び、「アイデンティティ･アクセス管理製品」カテゴリの市場の約３分の１を占める「ログオン管理／アクセス許可製品」は、一般にシステム全体に対するアクセスを統合的に管理するため、機能間の連携が求められる領域であり、大規模ベンダによるトータルソリューション提供が行われるケースが多い。従ってベンダ数も限られることになる。そしてインプリメンテーション（導入・設置）サービスで各企業のセキュリティポリシーや業務プロセスに合った構築をすることが成功の鍵となる。

ログオン許可機能としては、例えばシングルサインオン（1 回の認証で複数のシステムへのアクセスを可能にする管理システム）を導入することで、ユーザの利便性を上げると共に、リソース全体について一元的なポリシーの下にアクセス許可の範囲を決定し管理することができる。

⑤ PKI システム及びそのコンポーネント

このセグメントには、電子証明書の発行、管理、証明サービスを提供するシステム及びその構成要素などの製品が存在する。但し、構築サービス（SI）は含まない。また電子認証サービスも含まない。これらは各々「情報キュリティサービス」に計上される。

⑥ その他のアクセス管理製品

このセグメントには、単独で販売されるディレクトリサービス製品、ネットワーク統合管理製品におけるユーザ管理モジュール等が含まれる。また、本人認証の手法として、「リスクベース認証」という方法が登場している。これはアクセスしてきたユーザの PC の識別記号、地理的場所、アクセス履歴や行動パターン、予め登録された質問と答えのセット（本人しか知り得ない情報による）等を取り合わせて、高い精度で本人確認を実現するという手法で、インターネットバンキングなど、IT に不慣れな人でも特定できる技術である。何をどう取り合わせれば実用目的に耐える精度が得られるかのアルゴリズムが開発されて実用化が始まっている。

(2) 市場の動向

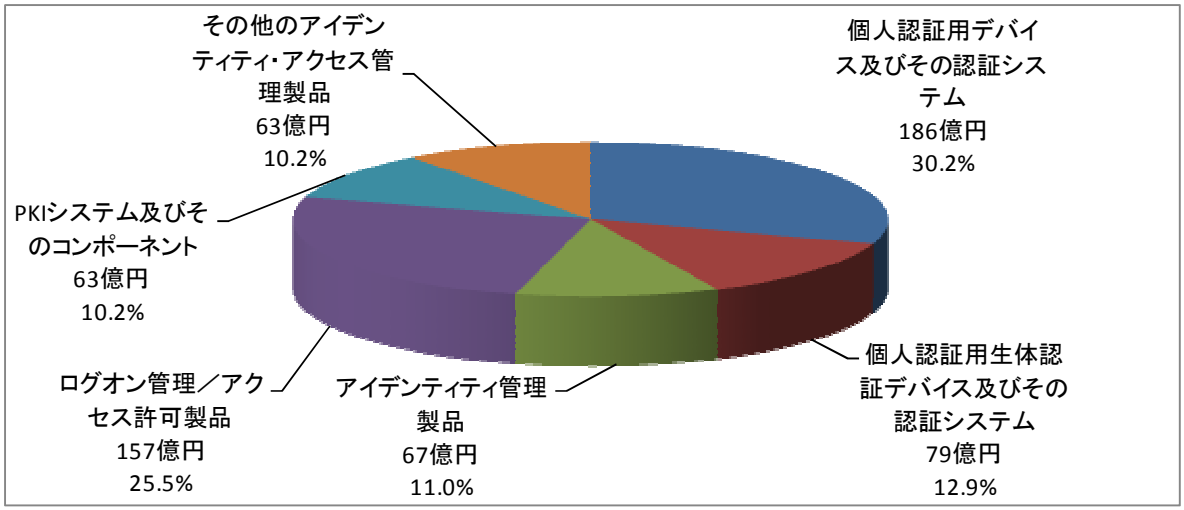
図 20 に 2007 年度のアイデンティティ・アクセス管理製品市場のセグメント別分布を示す。

情報セキュリティツール市場で 2 番目に大きいカテゴリであるこの市場は、2007 年度に前年度比 26.0%という大きな率で成長した。以下に見るように、内部統制の目的のために IT システムの利用管理を徹底するときに、誰がいつ何にどこまでアクセスできるかのコントロールが必須の条件になることから、企業が導入を急いでいることの表れと見られる。

電子化されたファイルやデータとして保存された、多くの重要な情報に対し、ネットワークを通して様々な場所から、昼夜を問わずアクセスできるようになった昨今、ネットワークに対する

アクセス制御の必要性に疑問を挟む余地はない。しかし、それだけでは十分な対策とは言えず、サーバ環境、ウェブアプリケーション環境下も含め、システムを使用する個人を識別し、適切なアクセス権を付与し運用するアクセス管理の重要性はますます高まっていると言えよう。企業の情報資産を情報漏えいや改ざん、盗難、紛失、消去といったセキュリティ上の脅威から守るためにも、「アクセス管理」は非常に重要な機能である。業務効率を重視し、誰もがアクセスできるという利便性を第一優先にする考え方を変え、リソース（情報(処理)資源）にアクセスできる人間を、必要最小限に限定するというセキュリティ重視の思想に基づくシステムを構築・導入する企業が、個人情報保護法や情報漏えい事件を契機に増加する傾向にある。また、内部統制報告制度の要求からも、そのような管理の徹底の必要が認識されている。内部統制が要求する IT ガバナンスのためのインフラとしても特に注目度が高い分野である。

図 20　2007 年度のアイデンティティ・アクセス管理製品市場



万が一の間違いアクセスや不正アクセスにも、IT 技術で管理することで、不必要なアクセスの発生を最小限に抑止する環境を実現することと、データの改ざんやプログラムの改ざんが行われず正確な処理を実施するシステム運用が、IT ガバナンスの要件となる。つまり、情報セキュリティの CIA（Confidentiality：機密性、Integrity：完全性、Availability：可用性）という 3 大基本要素の中の、機密性と完全性という面に、よりフォーカスが当たっていると言えよう。

また昨今、クレジットカードビジネス関連事業者向けに策定された「PCI DSS（PCI データセキュリティ基準)」と呼ばれる基準が注目を集めている。一般企業の情報セキュリティ対策にも有効なものと認識され、具体的な実施策として普及の動きがある。PCI DSS は 12 項目の要件で構成されており、要件 8 では「コンピュータにアクセスする際，利用者ごとに識別 ID を割り当てること」を要求している。これを実現するための製品としても、「アイデンティティ・アクセス管理製品」カテゴリの製品への需要が高まることが予測される。

アイデンティティ管理製品は、海外製品と国内製品とが存在するが、提供する機能にはベンダごとに差が見られる。例えば、近年 IT 内部統制の観点より承認ワークフローに対するニーズは

ID 管理の中でも重要な要素となる場合が多いが、製品の中で提供しているもの、オプションで提供するもの、あるいは別製品として提供しているものなど、様々である。また、近年、海外ではアイデンティティ管理製品の機能強化の一環として、ロール管理の技術に注目が集まっている。主要な ID 管理製品提供ベンダは、ロール管理技術の買収を行い自社ラインナップに追加しており、今後日本市場へも投入されることが予測される。

(3)市場規模とその推移

表 11 に国内アイデンティティ・アクセス管理製品の市場規模の実績と予測を、図 21 にその市場規模の推移のグラフを示す。

アイデンティティ・アクセス管理製品の市場規模は、2007 年度の実績で 615 億円、「情報セキュリティツール」市場全体 3,461 億円に対する構成比は 17.8 %であった。コンテンツセキュリティ対策製品に次ぐ規模の市場である。この市場規模は 2008 年度には、661 億円（前年度比伸び率 7.5%）に拡大するが、2009 年度には 630 億円（同マイナス 4.7%）になると予測される。

表 11　国内アイデンティティ・アクセス管理製品市場規模　実績と予測

市場規模（百万円）	2006 年度	2007 年度	2008 年度	2009 年度
個人認証用デバイス及びその認証システム	15,730	18,582	20,236	19,708
個人認証用生体認証デバイス及びその認証システム	5,875	7,917	8,241	8,200
アイデンティティ管理製品	4,962	6,740	8,004	7,320
ログオン管理／アクセス許可製品	12,239	15,719	16,471	15,541
PKI システム及びそのコンポーネント	4,985	6,276	6,301	6,003
その他のアイデンティティ・アクセス管理製品	5,030	6,299	6,914	6,308
合計	48,821	61,533	66,168	63,079
構成比				
個人認証用デバイス及びその認証システム	32.2%	30.2%	30.6%	31.2%
個人認証用生体認証デバイス及びその認証システム	12.0%	12.9%	12.5%	13.0%
アイデンティティ管理製品	10.2%	11.0%	12.1%	11.6%
ログオン管理／アクセス許可製品	25.1%	25.5%	24.9%	24.6%
PKI システム及びそのコンポーネント	10.2%	10.2%	9.5%	9.5%
その他のアクセス管理製品	10.3%	10.2%	10.4%	10.0%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
個人認証用デバイス及びその認証システム	ー	18.1%	8.9%	−2.6%
個人認証用生体認証デバイス及びその認証システム	ー	34.8%	4.1%	−0.5%
アイデンティティ管理製品	ー	35.8%	18.8%	−8.6%
ログオン管理／アクセス許可製品		28.4%	4.8%	−5.6%
PKI システム及びそのコンポーネント	ー	25.9%	0.4%	−4.7%
その他のアクセス管理製品	ー	25.2%	9.8%	−8.8%
合計	ー	26.0%	7.5%	−4.7%

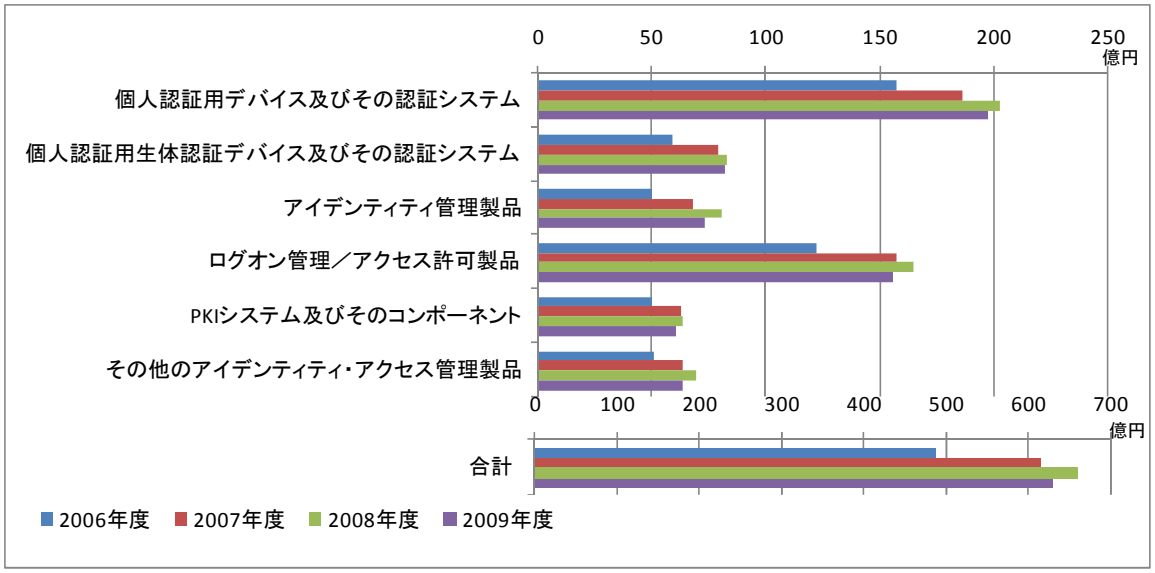
2007 年度の対前年度比伸び率 26.0%は「暗号製品」市場の 31.6%に次ぐ極めて高い成長率である。すでに何度も書いてきたように、金融商品取引法に基づく内部統制報告制度のための対応

として IT ガバナンスの整備が進み、その中核技術の一つとなる認証とアクセス管理の分野の投資と整備が進められた結果であると考えられる。また、内部からの情報漏えい事件の増加も、システムやデータへのアクセス権の管理の在り方の見直しや徹底につながり、アクセス管理への需要を押上げているものと見られる。

「アイデンティティ・アクセス管理製品」カテゴリでは、「個人認証用デバイス及びその認証システム」セグメントが 2007 年度の構成比で 30.2%と最も大きな部分を占めた。市場規模は 2007 年度で 186 億円であり、2008 年度は 202 億円に達すると見込まれる。

前年度比成長率でみると、「アイデンティティ管理製品」が一番高い伸び率を示しており、2007 年度 35.8%、2008 年度 18.8%と推測されている。内部統制（IT 全般統制）対応目的から、プロビジョニング管理という視点で、ディレクトリサービス製品やアイデンティティ管理ツールなどへの需要が高まっていることが、要因であると推定される。

図 21　国内アイデンティティ・アクセス管理製品市場推移



一方、「個人認証用生体認証デバイス及びその認証システム」も 2007 年度の対前年度比伸び率が 34.8%と極めて高い伸びとなった。これはアクセス管理のための認証の意味もあるが、ノートパソコンを始め可搬型の媒体からの情報漏えいが後を絶たないことから、万一紛失・盗難にあってもデータのアクセスできないように生体認証を組み込む動きが顕在化した結果と推測される。

「アイデンティティ・アクセス管理」は、大規模システムや基幹系システムでは以前から組み込まれており、成熟市場のイメージがあったが、内部統制からの必要性や情報セキュリティ対策の面から適用対象が拡大し、また管理の高度化も進展して、比較的高い市場成長が見込まれる状況となってきた。しかし、情報セキュリティ対策の中では経済状況の悪化の影響を一番受ける市場と予測している。特に大きなプロジェクトへの投資が鈍化する中、製品以外のコンサルティングやプランニング、インプリメンテーション費用が必要なため、導入期間が長期化するアイデンティティ管理、ログオン管理は優先順位を下げられる可能性が強く、その影響を受けやすいと予測される。

7.2.5　システムセキュリティ管理製品市場

(1)製品の特性

「システムセキュリティ管理製品」カテゴリは、以下の 4 種類の中分類市場区分（セグメント）により構成されている。

①「セキュリティ情報管理システム／製品」

「セキュリティ情報管理システム／製品」は SIM（Security Information Management セキュリティ情報管理）または SEM（Security Event Management セキュリティイベント管理）とも呼ばれており、セキュリティ対策機器情報の統合管理や、ネットワーク管理システムのセキュリティ情報を取りまとめ、管理コンソール等に情報やアラート（警報・警告）をリアルタイムに上げる製品やシステムを指す。セキュリティ対策製品や、ネットワーク管理製品、サーバなどが出力する複数のログや情報を管理集約することにより、一元管理やリアルタイム監視を実現することが可能となる。

企業内ネットワークには、多数のセキュリティ対策製品が導入されている。また、それらセキュリティ対策製品やサーバのログを収集することも一般化している。それら複数の製品や情報を適切に管理、運用するには熟練の技術者が必要となる。また、複数のログを集中管理して総合分析することにより、異常を検出することも必要となる。だが、実際には熟練技術者の確保も困難で、統合分析を人手で行うことも現実的でない。そこで「セキュリティ情報管理システム／製品」を用いて、必要な情報を収集して分析を行うことにより、技術者不足や運用管理者の過負荷を解消し、リアルタイム監視による異常検出を行う対策が取られている。

②「脆弱性検査製品」

「脆弱性検査製品」は、ネットワーク機器やサーバ等に対して、スキャニングや擬似攻撃を行うことにより、設定不備などによる脆弱性が存在していないかを検査する製品を指す。脆弱性検査製品には、ネットワーク型とホスト型がある。ホスト型は検査対象マシンにエージェントソフト（もしくは検査ツール自体）をインストールし、検査対象マシンの設定情報などの詳細情報をマシン内部から収集して分析を行うことにより、脆弱性を検査する製品を指す。ネットワーク型（もしくはスキャンタイプと呼ばれる製品群）は、インストールしたマシンから検査対象マシンやウェブアプリケーション等に対して、ネットワーク越しに擬似攻撃を行うことにより、脆弱性を検査する製品を指す。ネットワーク型の製品は、脆弱性検査サービスにも用いられる。

③「ポリシー管理・設定管理･動作監視制御製品」

「ポリシー管理・設定管理･動作監視制御製品」は、クライアントやサーバ等の管理対象となるマシンに対して、インベントリ管理（OS のバージョンやパッチ適用状況の情報、インストールされているアプリケーションの情報、ハードウェア情報等の収集・管理機能）、ポリシー管理（管理対象マシンにあらかじめ定められたポリシーに準拠した設定がされているかをモニタし報告する機能）、動作監視（管理対象マシンで行われたファイルの編集、更新、複写、印刷、外部記憶装置の使用等といった、情報操作のた

めの動作や行為に対しての監視、抑制、警告、報告機能）等の管理機能を提供する製品を指す。

また、NAC[43]という呼称が共通化しつつある、ネットワークアクセス認証にも注目したい。「ネットワーク検疫システム」とも呼ばれる。例えば、社内のネットワークに持ち運び可能な PC を接続する時に、その PC が接続を許可されたものであるかどうかを判断して接続の可否を決定するといったものである。判断基準としては、マシン固有の ID による場合や、OS のパッチレベル、ウイルス対策ソフトの定義ファイルが最新か等まで踏み込んで接続可否を判断するものなどもある。方法としてはVLAN（仮想的LAN）、ゲートウェイ方式、ルータに付加機能として載せる形等があり、専用のハードウェアと一体化したアプライアンススタイプの製品も登場している。

情報漏えいや流出事故を未然に防止するには、規則を定め人がチェックする方法もあるが、業務効率を阻害しコスト増を招く。またミスや不注意、故意の防止は困難である。しかし、「ポリシー管理・設定管理･動作監視制御製品」を導入して技術的な管理・制御を行うことにより、これらの問題の相当部分が解決する。更には、きめ細かいルールを定めて漏れなく運用することも可能になり、効率、コスト、精度の面で改善が図れることになる。

④「その他のシステムセキュリティ管理製品」

「その他のシステムセキュリティ管理製品」には、セキュリティ事象や不正アクセスを追跡するために、電磁的記録の証拠保全及び調査・分析を行う機能を有する、いわゆるデジタルフォレンジック製品や、セキュリティ目的のログ収集・保管・解析機能を有する製品をまとめている。（但し、ログ収集・解析機能を有する製品の内、リアルタイム監視を目的とする製品は「セキュリティ情報管理システム／製品」に分類しており、「その他のシステムセキュリティ管理製品」では主に傾向解析等スタティックな目的のものを対象としている。）

インシデントが発生した際に、原因を突き止めるためにもログ確保は重要である。また、内部統制により、監査証跡として複数のログを取得し、保管する際も真正性を確保する必要が出てきている。結果として、膨大な量のログを適切に取得・管理する必要が発生し、管理者の負担が更に増大することとなっている。そのため、証拠保全のためのログの改ざん防止機能や、大量のログを統合し統計分析を行える機能を提供している製品を用いることにより、管理者の負担を軽減することのみでなく、監査証跡の真正性を確保し、説明責任を果たすことが可能となる。

(2)市場の動向

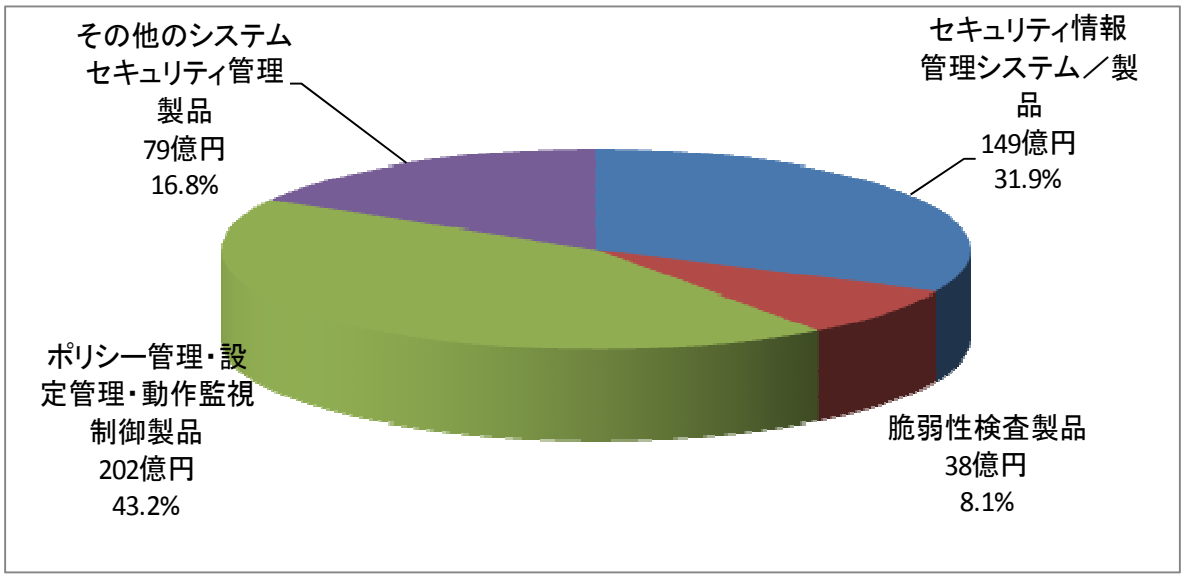
以上見てきた 4 セグメントの 2007 年度における分布を図 22 に示す。

ネットワーク間の連携が進むことにより、利便性が上がることとなったが、情報セキュリティ

[43] NAC: Network Access Control あるいは Network Admission Control の頭文字。ベンダにより異なる。同様の機能・コンセプトを Trusted Network Connect と呼ぶ団体もある。その意味する内容も少しずつ異なり、まだ業界の統一見解や統一規格にまでは至っていない。

上の問題も多く発生している。また、脅威の傾向も変化しており、今までの愉快犯の犯行から、標的を絞った金銭目的の犯行にシフトすると共に、手口も巧妙になり被害が目に見えにくくなってきている。例として、ウイルス対策ソフトによるチェックを回避するためにウェブからの目に見えないダウンロードという経路を利用する攻撃がある。ウェブアプリケーションの脆弱性を狙い、通常のウェブサイトにマルウェアが仕掛けられるケースが増えている。また、組織内のユーザが外部から持ち込んだマシンや USB を組織内のネットワークに接続することによりウイルスに感染する事例も増加している。更に、内部要員の情報持出しやミスに起因する情報漏えい事故の発生も依然後を絶たず、外部の脅威のみに目を向けているだけでは、情報セキュリティ事故は防げなくなってきている。ネットワークの内外の境界線での防御に加え、エンドポイントのセキュリティの確保や､ユーザの行為を監視することの重要性が広く認識されてきており、「ポリシー管理・設定管理・動作監視制御製品」の導入が急速に進んできている。

図 22　2007 年度のシステムセキュリティ管理製品市場



J-SOX[44]への対応等のために、セキュリティの可視化が必要になってきていることから、「セキュリティ情報管理システム／製品」や「その他のシステムセキュリティ管理製品」の重要性も高まっている。「ポリシー管理・設定管理・動作監視制御製品」でログ情報を収集し、SIM で監視を行い、統合ログ管理製品を用いて情報の分析を行うことにより、内部の要員が何をしているのかを把握することも可能になる。また、取得した膨大なログを活用して行くために、収集したログ分析の代行や、コンサルティングの一環としてログの活用方法を提案するサービスも今後増えて行くと推測される。更には、ログの収集から分析までをアウトソースとして行うサービスも出てきており、今後もログ関連市場については成長が期待できる。

[44] 金融商品取引法が規定する内部統制報告制度の要求に基づいて、財務諸表に影響を及ぼす取引の処理・記録の適正性を確保するために企業がさまざまな管理策を整備して実施する対応を総称して J-SOX と呼びならわすようになっている。

脆弱性を作り込まないようにすることが難しいウェブアプリケーションへの攻撃が急増している。この背景としては、アプリケーションへの攻撃を自動化することが可能な攻撃ツールや攻撃を容易にする手段が出てきたことも大きい。インターネット上でサービスを提供している事業者は自社のウェブサイトのセキュリティを確保し安全にする必要に迫られている。そのため、「脆弱性検査製品」の需要が高まっている。「脆弱性検査製品」には、アプリケーションのソースコードに対する脆弱性を検査する製品や、ネットワークから擬似攻撃を行い脆弱性の検査を行う製品がある。自社で導入して使うケース、アプリケーションの開発受託事業者が納品前テストに使用するケース、サービス事業者が検査サービスのために品揃えするケース等がある。

(3)市場規模とその推移

表12に国内システムセキュリティ管理製品市場の市場規模実績推定値と予測値を、図23にその市場規模の推移のグラフを示す。

表 12　国内システムセキュリティ管理製品市場規模　実績と予測

市場規模(百万円)	2006 年度	2007 年度	2008 年度	2009 年度
セキュリティ情報管理システム／製品	12,873	14,923	16,285	15,752
脆弱性検査製品	3,039	3,771	4,032	3,697
ポリシー管理・設定管理・動作監視制御製品	15,770	20,212	23,406	24,279
その他のシステムセキュリティ管理製品	6,773	7,863	8,430	7,887
合計	38,455	46,770	52,153	51,615
構成比				
セキュリティ情報管理システム／製品	33.5%	31.9%	31.2%	30.5%
脆弱性検査製品	7.9%	8.1%	7.7%	7.2%
ポリシー管理・設定管理・動作監視制御製品	41.0%	43.2%	44.9%	47.0%
その他のシステムセキュリティ管理製品	17.6%	16.1%	16.2%	15.3%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
セキュリティ情報管理システム／製品	ー	15.9%	9.1%	-3.3%
脆弱性検査製品	ー	24.1%	6.9%	-8.3%
ポリシー管理・設定管理・動作監視制御製品	ー	28.2%	15.8%	3.7%
その他のシステムセキュリティ管理製品	ー	16.1%	7.2%	-6.4%
合計	ー	21.6%	11.5%	-1.0%

「システムセキュリティ管理製品」市場は 2007 年度には全セグメント合わせて 468 億円程度の市場を形成しており、2006 年度の 384 億円に比べて 21.6%増とかなり高い成長率を示している。2008 年度も前年度比 11.5%伸びて 522 億円と、市場規模が 500 億円台に達するものと予測される。しかし、2008 年に発生した世界的な不況の影響を受け、2009 年度には前年度比マイナス 1.0%の成長率で 516 億円に留まると予測される。このカテゴリでは不況による影響は限定的と予測されている。これは、構成比率でこのカテゴリ全体の約 4 割を占める「ポリシー管理・設定管理・動作監視制御製品」の需要が引続き確保されて行くことによる。

各セグメントの内容を見てみると、「セキュリティ情報管理システム／製品」は前年度比成長率

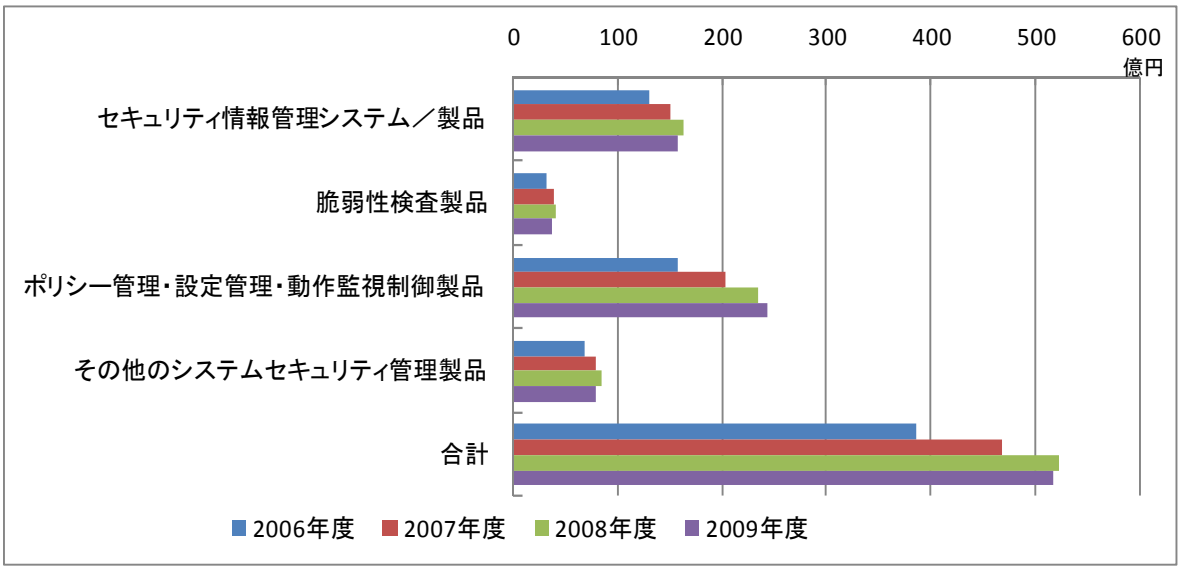
で 2007 年度 15.9%と 2 桁の成長率を維持しているが、2008 年度は不況の影響もあり 9.1%と成長が落ち、2009 年度には市場への浸透が一巡し、設備投資の抑制により成長率がマイナスになると予測する。市場規模としては 2006 年度の 129 億円から 2009 年度には 158 億円に達すると見られる。

「ポリシー管理・設定管理・動作監視制御製品」は 2007 年度に前年度比成長率 28.2%と極めて高い伸び率を示している。今後もエンドポイントでの管理が重要との認識が高まっていることから、需要が確保されて行くと見込まれる。その結果、2008 年度 15.8%、2009 年度 3.7%と成長率は鈍化するものの徐々に市場を拡大して行くと推測され、市場規模は 2006 年度の 158 億円から 2009 年度には 243 億円に達すると見られる。

「脆弱性検査製品」は 2007 年度には前年度比成長率 24.1%と非常に高い伸びを見せた。この分野は比較的早くから製品が提供され市場に浸透していたが、ウェブアプリケーションに対する脅威の深刻化もあり、市場が拡大したものと見られる。「脆弱性検査製品」はサービスと取り合わせて利用されるケースが多く、単独製品としての新規需要は限定的であると考えられ、2008 年度の伸び率は一旦落ち着くものと予測される。また、2009 年度には他のセグメントと同じく、2008 年からの経済環境の変化の影響により、マイナス 8.3%と需要は減退すると予測される。

「その他のシステムセキュリティ管理製品」についても 2007 年度に前年度比成長率 16.1%と 2 桁の伸び率を示している。これは、J-SOX 対応としてのログ収集・解析の需要が大きかったことを反映していると考えられる。2008 年度も同様の需要により 7.2%の成長を見せると見込まれるが、不況の影響により、2009 年度はマイナス成長に転じるものと推測される。

図 23　国内システムセキュリティ管理製品市場推移



7.2.6　暗号製品市場

(1)製品の特性

「暗号製品」は三つの製品群により市場が形成されている。

①データ暗号化製品

データ暗号化製品は、ユーザが直接取り扱うメールや文書ファイル等のデータや、ハードディスク、フロッピーディスクや MO ディスク、USB メモリなどの外部記憶装置のデータを暗号化することを主たる機能とする製品群である。

②暗号化ミドルウェア

暗号化ミドルウェアは、システムやデータベース、及びアプリケーション上でやり取りされるデータの暗号化を行うことを主たる機能とする暗号ライブラリ、組込用暗号モジュールなどの製品である。単体販売よりも組込用や OEM 供給されるビジネスモデルが多い。

③その他の暗号製品

そして三つ目の製品群として、上記二つの製品群に属さない「その他の暗号製品」がある。この製品群には、暗号ライセンス、鍵管理システム等周辺製品、電子割符や電子透かし等が含まれる。

いずれの製品群も、その主目的は、暗号化技術を用いることで、権限外使用、覗き見、漏えい、改ざん等を防止または発見し、様々な脅威からデータを保護することにある。

「データ暗号化製品」には、大きく二つのタイプの製品が存在する。一つ目のタイプの製品は、PC のハードディスクや、USB メモリ等の外部記憶装置を、デバイス丸ごと透過的に暗号化することで、データを利用するユーザ自身が、暗号化をほとんど意識する必要がない製品である。もう一つはユーザがデータの暗号化のために、意識的に個別の操作を行うタイプの製品である。透過的な暗号化機能が提供される製品では、PC の起動時、または USB メモリ等の外部記憶装置を PC に接続した際などに、パスワードや認証デバイス、あるいは生体認証による認証を行うことで、以降は暗号化を意識せずに PC や外部記憶装置上のデータを利用することができる。それゆえユーザの利便性をほとんど変えずに導入及び利用ができるという特徴を持つ。このようなタイプの製品は、PC や外部記憶装置自体の紛失・盗難対策として有効なことなから、PC や USB メモリなどを持ち出すことの多い営業職や技術者の情報漏えい対策の手段として、大企業はもちろんのこと、大企業と取引を行う中小企業にも導入が進んでいる。また近年、企業でのスマートフォン利用のニーズに応える形で、スマートフォン上のフラッシュメモリ及び外部メモリ上のデータを透過的に暗号化する製品も提供されている。

ユーザがデータの暗号化に対して、意識的に個別の操作を行うタイプの製品としては、権限に応じて、暗号・復号鍵を用いることによって、データの暗号化を行う製品が主である。このような製品は、組織やグループなどで共通鍵を作成することにより、組織内もしくはデータをやり取りしたい社外の関係者など、権限を持つユーザであればデータを復号できるが、権限外のユーザに対しては利用の制限や覗き見・漏えいの防止ができる機構を持つ。また多くの製品が、パーティション単位、フォルダ単位、ファイル単位など、必要に応じて、暗号化の対象レベルを変動す

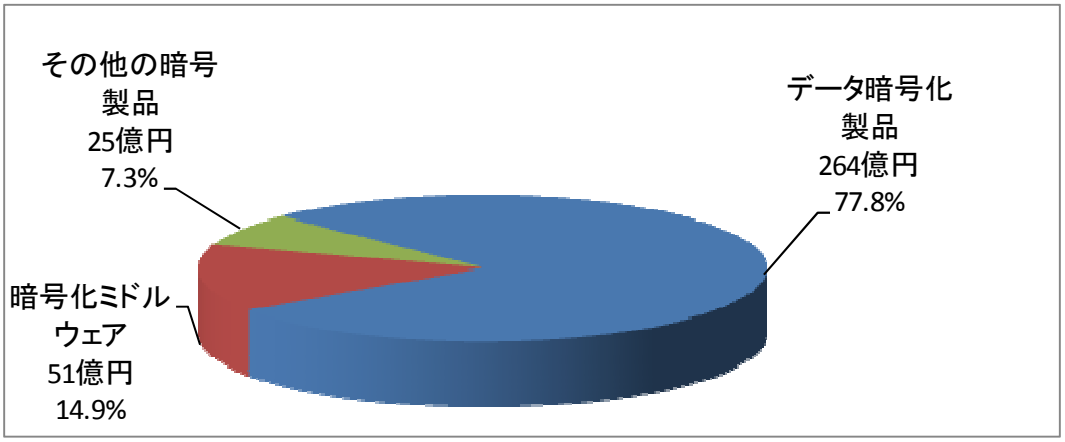
る機能を持つ。また暗号化製品が導入されていない PC との間で機密データの受け渡しを可能にする自己復号形式での暗号化製品もある。パスワードを利用するため、鍵を利用した暗号に比べてセキュリティ強度は低いが､パスワードという手軽さから､組織内あるいは社外の関係者間で、安全にデータを交換したいというニーズに伴って製品が普及している。

また、「秘密分散法」を応用し、暗号化されたデータそのものを分割して管理することで、情報漏えい対策とする製品も提供されている。今日では、PC や外部記憶装置自体の紛失・盗難といったリスク以外への対策も「データ暗号化製品」には求められており、データへのアクセス権限を持つ内部犯による故意のデータの持出しを防ぐために、外部記憶装置への出力を制限、もしくは強制的に暗号化を行う製品や、メール関連のセキュリティ製品との連携やデバイス認証・制御機能を実装することにより情報の移動を制限する製品も提供されている。また電子メールでの誤送信による情報漏えいを防ぐために、情報セキュリティ対策に先進的な一部の企業が、添付ファイルを自動的に暗号化して送信する製品やメール本文までを暗号化する製品の導入を開始しているが、未だ多くの企業では、添付ファイルを手動で zip 暗号化して送信するといった、運用による対策に頼っているのが実情である。

(2) 市場の動向

2007 年度暗号化製品市場を見てみると図 24 のような分布となっている。メール、文書ファイル、ハードディスク、外部記憶装置等の暗号化を主とする「データ暗号化製品」が 2007 年度実績で 264 億円、「暗号製品」市場全体の 77.8%と、このカテゴリのほとんどを占めている。続いてシステムやデータベース及びアプリケーション上でやり取りされるデータを暗号化する「暗号化ミドルウェア製品」が 51 億円で 14.9%と続き、最後に、「その他暗号化製品」の 25 億円、7.3%で、市場が構成されている。

図 24　2007 年度の暗号製品市場



「データ暗号化製品」に分類される製品は、IC カード、USB キーといった認証デバイスや生体認証装置などと取み合わせて利用されるケースも多い。また全社規模で導入されるケースも増えており、管理データベースによる一元管理や、ポリシー管理の機能を有する製品も多く存在する。また、企業間取引や企業内においての情報漏えい対策や内部統制対策として注目を浴びてい

るのが DRM（Digital Rights Management）と呼ばれる製品群、及び DLP （Data Loss/Leak/Leakage Protection/Prevention） 製品群である。これらは暗号技術と密接に関連する製品群ではあるが、その目的がコンテンツの保護や、フィルタリングに重点があるとの理解から、本調査では「セキュアコンテンツ管理製品」として集計し、「暗号製品」には含めていない。

「暗号化ミドルウェア製品」に目を向けると、SaaS／ASP の急速な普及・拡大や、あるいはクラウドコンピューティングといった言葉に表されるように、ネットワークを介してデータをやりとりすることは今後も増え続けると予想されており、そこで取り扱われるデータについては、安全対策を講じることが必要である。また、多くの顧客情報を取り扱うクレジットカードビジネス関連事業者向けに策定された PCI DSS という基準に対応するために、サービス基盤のデータのセキュリティレベルを高める「暗号化ミドルウェア」製品の需要は今後も見込まれる。また、組込用の暗号化モジュールは、ゲーム機や情報家電など、家電製品のネット対応機能が進むにつれ、内部でデータ等を暗号化して保持する必要や、通信時におけるデータの暗号化の必要性から組込ニーズは今後も継続すると考えられる。

(3)市場規模とその推移

表 13に国内暗号製品の市場規模実績推定値と予測値を示す。図25にはそのグラフを示す。

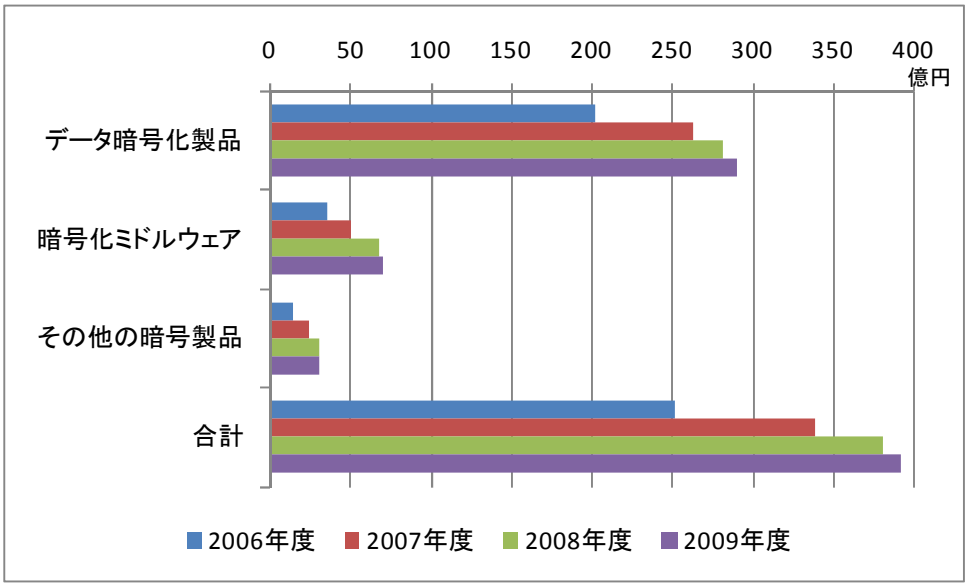
表 13　国内暗号製品市場規模　実績と予測

市場規模（百万円）	2006 年度	2007 年度	2008 年度	2009 年度
データ暗号化製品	20,265	26,382	28,224	29,036
暗号化ミドルウェア	3,711	5,057	6,879	7,124
その他の暗号製品	1,810	2,483	3,054	3,135
合計	25,785	33,922	38,157	39,296
構成比				
データ暗号化製品	78.6%	77.8%	74.0%	73.9%
暗号化ミドルウェア	14.4%	14.9%	18.0%	18.1%
その他の暗号製品	7.0%	7.3%	8.0%	8.0%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
データ暗号化製品	―	30.2%	7.0%	2.9%
暗号化ミドルウェア	―	36.3%	36.0%	3.6%
その他の暗号製品	―	37.2%	23.0%	2.7%
合計	―	31.6%	12.5%	3.0%

国内暗号製品の市場規模は、2007年度の実績で339億円、前年度比伸び率31.6%と高い伸びを示した。「暗号製品」カテゴリとして「情報セキュリティツール」市場全体3,461億円に対する構成比は9.8 %であった。2008年度の「暗号製品」の市場規模は382億円まで拡大し、前年度比伸び率も12.5%と順調に成長したものと推測される。2008年度は、「データ暗号化製品」の前年度比伸び率は7.0%と前年度に比べれば落ち着きを見せた一方、「暗号化ミドルウェア」が前年度比伸び率36.0%、「その他の暗号化製品」が同23.0%と高い伸び率を示したためである。2009年度には、不

況が見込まれるにも拘らず392億円（前年度比成長率3.0%）に達すると予測される。「暗号製品」以外のすべてのカテゴリでマイナス成長が予測される2009年度において、唯一、プラス成長が予測されるカテゴリとなっている。情報漏えい事件が後を絶たず、ネットワークからの攻撃の深刻化や内部犯罪の増加傾向が見られる中で、事件や事故を起こせば本当に命取りになりかねないという経営者の認識が、暗号化という防衛手段の導入は進めるという判断となって表れた結果と見られる。「ポリシー管理・設定管理・動作監視制御製品」のセグメントが2009年度にプラス成長予想となっていることも同様の理由とによると考えられる。

図 25　国内暗号製品市場推移



数年にわたり急速な成長を遂げたこれら暗号製品市場は、2009 年度の成長率は微増にとどまるものの、今や情報漏えい対策の必然性は広く認識されており、その手段として暗号化製品の導入は継続し、市場は順調に拡大するものと思われる。J-SOX 対策の面でも、重要データの改ざんを防止し、ログやファイルの真正性を確保するために暗号製品を導入するというケースも増えている。また情報システムの中核をなすアプリケーション上のデータや、データベースの暗号化の手段として、あるいは、情報家電のセキュリティ確保の手段として、今後もデータを保護するための暗号製品は、様々な機器やシーンでの利用拡大が見込まれる。

8. 国内情報セキュリティサービス市場の分析

8.1 情報セキュリティサービス市場の全体概要

「情報セキュリティサービス」とは、情報セキュリティ実現のための様々なサービスを指すもので、「情報セキュリティツール」がハードウェアもしくはソフトウェアという形のある商品、既製品のイメージであるのに対して、全くソフト的なビジネス、形のない、個別対応型のいわゆる役務契約型の商取引、すなわちサービスの提供と定義している。

このカテゴリには、大分類として「情報セキュリティコンサルテーション」、「セキュアシステム構築サービス」、「セキュリティ運用・管理サービス」、「情報セキュリティ教育」、「情報セキュリティ保険」の 5 カテゴリを定義した。ツールに直接関連する保守・サポートや更新サービスはツールの市場に付帯するものとしてツール側に含め、サービス分野には入れていない。ただし、ツール類を導入するに際しての使用条件や各種パラメータの設定といった導入支援サービスについては、それがツールと独立して価格付けされる場合にはサービス市場としてカウントするものとしている。似たケースで、特定のツールの納品に際して納入業者が無償で簡単な設定やチューニングを行うものについてはツールの対価の一部という仕分けになる。

表 14 に国内情報セキュリティサービス市場規模の実績推定値と予測値を示す。

表 14 国内情報セキュリティサービス市場規模 実績と予測

金額単位:百万円

年度別市場規模	2006年度		2007年度			2008年度			2009年度		
情報セキュリティサービス	実績推計値		実績推計値			実績見込推計値			予測値		
	金額	構成比	金額	構成比	成長率	金額	構成比	成長率	金額	構成比	成長率
情報セキュリティコンサルテーション	63,451	20.8%	73,497	21.7%	15.8%	77,708	22.1%	5.7%	71,181	22.0%	−8.4%
セキュアシステム構築サービス	142,585	46.8%	147,130	43.5%	3.2%	149,425	42.5%	1.6%	132,397	40.9%	−11.4%
セキュリティ運用・管理サービス	74,134	24.3%	87,233	25.8%	17.7%	91,777	26.1%	5.2%	89,115	27.5%	−2.9%
情報セキュリティ教育	17,467	5.7%	23,404	6.9%	34.0%	25,461	7.2%	8.8%	23,669	7.3%	−7.0%
情報セキュリティ保険	7,111	2.3%	7,354	2.2%	3.4%	7,625	2.2%	3.7%	7,417	2.3%	−2.7%
セキュリティサービス市場合計	304,748	100.0%	338,618	100.0%	11.1%	351,996	100.0%	4.0%	323,778	100.0%	−8.0%

今回の調査結果では、2006 年度の「情報セキュリティサービス」市場規模は 3,047 億円と見積もられ、2007 年度には対前年度比成長率 11.1%の伸びを示して 3,386 億円に達したものと推定される。「情報セキュリティ教育」が 34.0%と極めて高い伸びを示した他、「セキュリティ運用・管理サービス」が 17.7%、「情報セキュリティコンサルテーション」が 15.8%と高い成長率を示した。情報セキュリティサービス市場の最大のカテゴリである「セキュアシステム構築サービス」は 3.2%、「情報セキュリティ保険」は 3.4%と伸び率はわずかであったが、全体として前年度比 11.1%のプラス成長となっている。

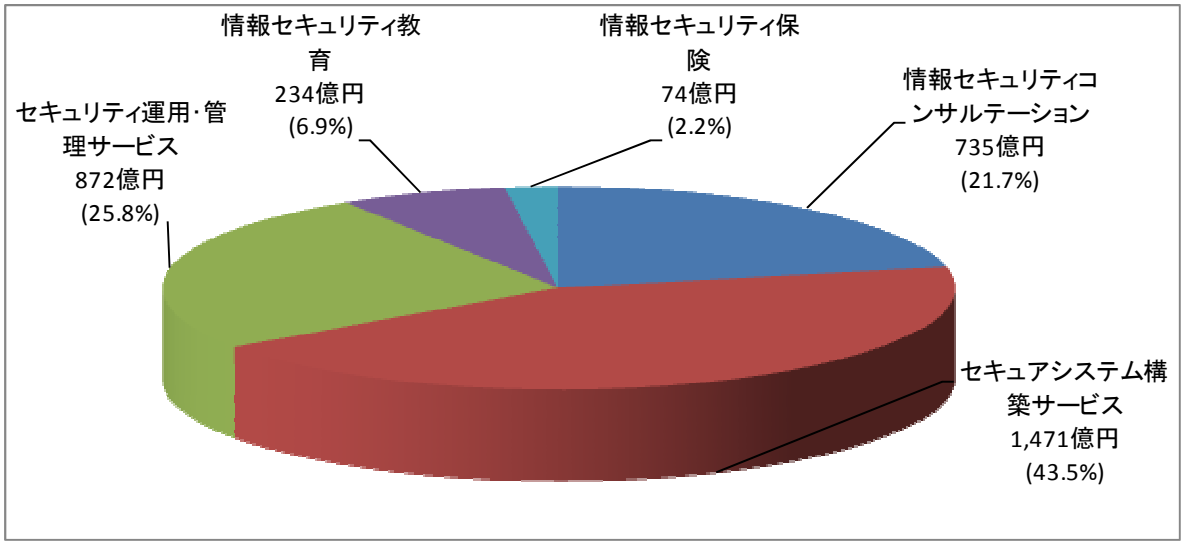
図 26 に 2007 年度の国内情報セキュリティサービス市場のカテゴリ別分布を示す。また図 27 は国内情報セキュリティサービス市場の経年推移を表した図である。

「情報セキュリティサービス」市場の中で最大のカテゴリは「セキュアシステム構築サービス」

で、2007 年度実績推定値で 1,471 億円と、情報セキュリティサービス市場全体の 43.5%を占めた。このカテゴリは、IT システムに対してセキュリティ機能を設計・導入・構築するサービスである。システムインテグレーションに際してセキュリティ機能を組み込む部分のサービスや、既存の IT システムに対してセキュリティ機能を付加したり強化したりするために、IT セキュリティシステムを設計･製品導入･構築するサービスが中心となる。システムインテグレーション的要素が強いために、市場規模も大きなものになっている。

次に大きなカテゴリは「セキュリティ運用・管理サービス」で、2007 年度実績は 872 億円と推定される。このカテゴリは、ネットワークセキュリティの監視や運用代行サービス（マネージドセキュリティサービスとも呼ばれる）､システムの弱点を専門技術で点検する脆弱性検査やインシデントへの対応を行うプロフェッショナルサービス、そして電子認証サービス等の専門的サービスで構成される｡マネージドセキュリティサービスは､顧客のネットワークにセンサを設置し、あるいは顧客の社内 LAN に設置したファイアウォール等の装置の情報を直接吸い上げ、顧客のネットワークのセキュリティ状態を監視したり、インシデント発生時の対応を支援したりするものである。外部からの攻撃等によるネットワーク上のトラブルは、専門の技術者でないと対応が難しい。専門家のサービスを利用すべきという判断をする企業も多く、以前からこの種のサービスが専門事業者によって提供されている。この他、プロフェッショナルサービスの一種には、リアルタイムのネットワーク監視まではしなくても定期的にログ解析を行ってネットワークの状態を把握し必要な助言をするといったサービスもある。また、電子認証サービスは、サーバ、システムの利用者個人、文書、時刻等の証明に必要な電子証明書を発行するサービスで、内部統制対応や電子商取引の活発化に伴って需要が拡大している。

図 26　2007 年度の国内情報セキュリティサービス市場



「セキュリティ運用・管理サービス」に関しては、1990 年代後半から、ネットワークインテグレーション分野で情報セキュリティに特化した企業等が展開していた。その主要顧客は経営の IT への依存度が高いか、セキュリティに対する意識の高い一部企業、あるいはネットワーク管理と

一括でアウトソースするようなケースに限られてきたと言える。それが 2000 年代半ばごろから複雑化するネットワーク、高度化し頻度が高まる攻撃、特に電子商取引サイトへの攻撃やそれによる被害の深刻化等を背景に、専門サービスに対してアウトソーシングの形で積極活用しようという判断が増えてきている。そのようなユーザ側の動向に加えて、ベンダから提供される監視サービスなどが、競争にさらされる中でサービス品質が高まると共に価格も相当程度低下が進み、ユーザにとっては導入しやすくなってきている。このような背景から、ここ数年成長の度を速めているものと見られる

金額規模では情報セキュリティサービス市場の中で３番目だが、ここにきて需要が一層高まっているのが「情報セキュリティコンサルテーション」である。特に「情報セキュリティ管理全般のコンサルテーション」、「情報セキュリティ関連規格認証取得支援サービス」、「情報セキュリティ診断・監査サービス」、等、情報セキュリティの技術的側面よりは、経営管理の視点から専門家の支援を活用する動きが大きくなっている。ツールのようにハードウェアのためのコストがかからず、SI のように工数も大きくなりにくいために、大企業が全社的対策を一気に進める場合等を除き、案件当たりの金額はそれほど大きくならない。経営コンサルに近いところに位置するので、会計監査法人系、SI 系、独立系等多様な事業者がサービスを提供している。

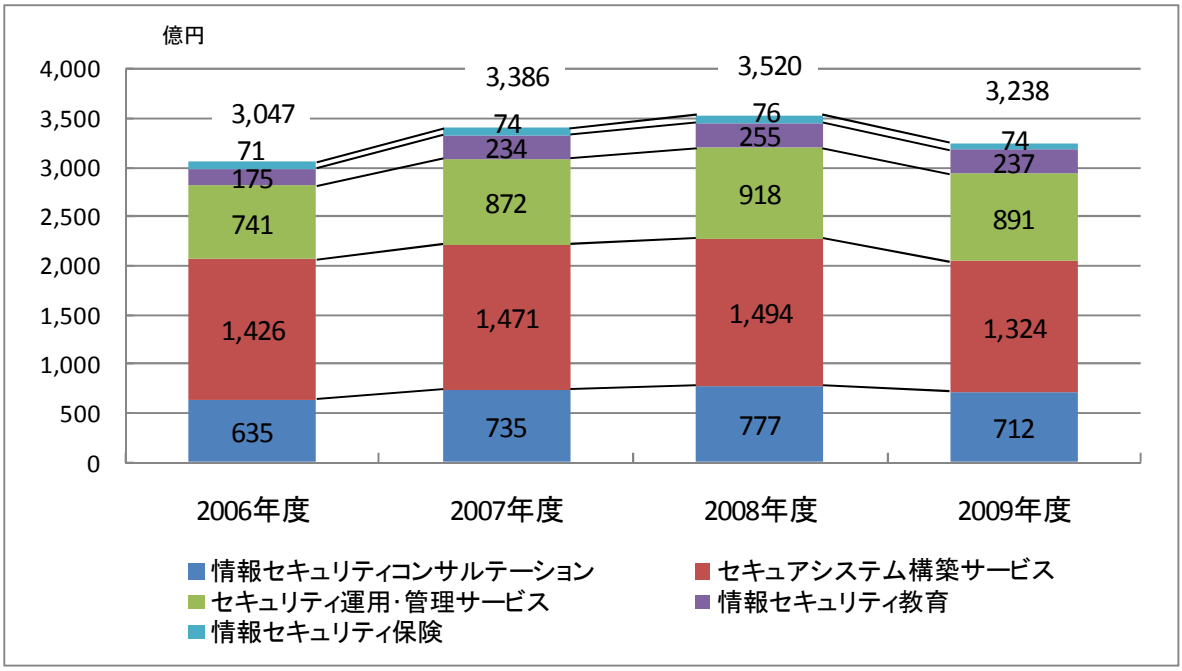
「情報セキュリティコンサルテーション」の需要を拡大した要因としては、個人情報保護法が挙げられる。特に小売業（典型的には通信販売業等）、信販業、旅行その他のサービス業等、個人消費者を多数顧客に抱える業態において、個人情報保護法の施行に伴って情報セキュリティに対する対応が進み、情報セキュリティコンサルティングや診断・監査の利用も広がった。その中でプライバシーマーク認定や ISMS 認証の取得に取り組むケースも増え、その取得支援サービスや、認証サービスの需要も高い伸びを示している。

また今年度から適用が始まった内部統制報告制度や、事業継続計画への関心の高まりなどから、総合的リスク管理としての情報セキュリティ管理という考え方も浸透が進みつつあり、この面から情報セキュリティコンサルティングの導入利用も広がっている。こうした需要に押し上げられて、2007 年度の「情報セキュリティコンサルテーション」市場は前年度比 15.8%増の 735 億円に達したと見られる。

「情報セキュリティ教育」は 2007 年度実績推定値が 234 億円に留まり、構成比も 6.9%と小さいが、前年度比では 34.0%増と、極めて高い伸びを示した。従来情報セキュリティは情報システム部門の専管事項のような理解がされており、一般社員等のユーザにも理解させる必要があることに対する認識が十分でなかった。それに対し、従業員の故意、ミス、不作為、無知等を直接間接の原因とする情報の盗難、紛失、漏えい事故が後を絶たないことから、従業員の知識と意識の底上げが必須であるとの認識が広がってきた。またウイルスやマルウェアの被害を防ぐには脆弱性の理解と対応を各ユーザに知らせる必要も強まっている。このような理由で教育ニーズが強まり、それに対応して教育コンテンツとサービスの提供も活発化してきている。2007 年度の高成長の背景には、大手企業における個人情報漏えい事件の教訓と共に、営業秘密保護の必要が急速に高まったことと、大手システムインテグレータ等が教育の供給にも積極的に取り組むようにな

ったことがあると観測される。

図 27　国内情報セキュリティサービス市場推移



情報セキュリティ保険は 1 カテゴリ 1 セグメントで市場区分のバリエーションはないが、情報セキュリティ対策と歩みを同じくして拡大してきた市場である。特に、情報セキュリティ対策が経営課題であるとの認識が浸透しだした 21 世紀以降は、市場への定着と需要の裾野の拡大が進んだと見られる。市場規模は、2007 年度で 74 億円、前年度比では 3.4%の伸びであった。2007 年度版の本調査では、2005 年度時点で 40 億円程度と見られたものが、翌 2006 年度には 71 億円へと急拡大したとの観測を行ったが、その後は落ち着いて、今回調査では、対象期間中 70 億円台で推移するものと予測される。

8.2 情報セキュリティサービス市場のカテゴリ別分析

8.2.1 情報セキュリティコンサルテーション市場

(1) サービスの概要と特性

「情報セキュリティコンサルテーション」は情報セキュリティポリシー構築支援から、認証取得支援に特化したパッケージコンサルテーションや、上流コンサルから運用までの一連のライフサイクルをすべて提供するものなどの種別があるものの、大別すると、マネジメント系、認証取得系、診断･監査系に分けることができる。

マネジメント系については、主に情報セキュリティポリシーの策定やコンプライアンス対応、情報保護対策全般が、サービスの中心となる。中分類の市場区分としては「情報セキュリティポリシー構築支援」と「情報セキュリティ管理全般のコンサルテーション」がある。情報セキュリティ対策の中心となるのが情報セキュリティポリシーであり、会社の基本方針から情報資産に関わるリスクへの対策を体系的に定めた情報セキュリティ対策基準、更に実際の運用ルールや処理手順まで体系的に整備する必要があり､その支援をするサービスである。「情報セキュリティ管理全般のコンサルテーション」ではこれに加えて推進組織や責任体制、IT も含めた情報セキュリティの基本枠組であるアーキテクチャの設計開発まで全般にわたって支援を提供する。いずれのサービスにおいても、リスク分析も重要な要素となる。

診断・監査系については、「情報セキュリティ診断・監査サービス」市場を定義した。経済産業省告示に基づく制度的枠組みとして、情報セキュリティ監査制度があり、NPO 日本セキュリティ監査協会が推進し、同協会が認定する公認情報セキュリティ監査人が中心となって監査を提供している。ISMS 認証取得企業の内部監査を外部のコンサルタントが実施あるいは支援を行うサービスもある。制度的枠組にとらわれず、自社の基準やサービス事業者の推奨基準に基づく情報セキュリティ診断を受けるケースや、外部の第三者による委託先に対する監査もある。また情報セキュリティ対策がどこまでできているかを一定の尺度で測って評点をつける情報セキュリティ格付けも始まっている。

認証取得系については､「情報セキュリティ規格認証取得等支援サービス」と「情報セキュリティ規格認証・審査・監査機関（サービス)」の市場がある。後者は、主としてプライバシーマークの認定と ISMS の認証について規格に基づいて審査し適合性の認定や認証をする機関のサービスである。プライバシーマークは財団法人日本情報処理開発協会[45]（JIPDEC）が直接審査し付与する他､業界団体等が JIPDEC の指定期間として付与認定する｡基準は JISQ15001 である｡ISMS は JIPDEC が認定する認証機関が JISQ27001（国際規格である ISO/IEC27001 と同等）に基づいて適合性を認証する制度で、民間の規格認証サービスを行う機関が提供する。前者はそのような認定、認証の取得を支援するサービスで、マネジメントシステムの構築と PDCA サイクルの実施を支援し、審査のサポートや取得後の運用の支援等も行う。

この他、これらが複合した需要や個別ニーズに沿ったコンサルティング、企業独自のメニュー

[45] http://www.jipdec.or.jp/

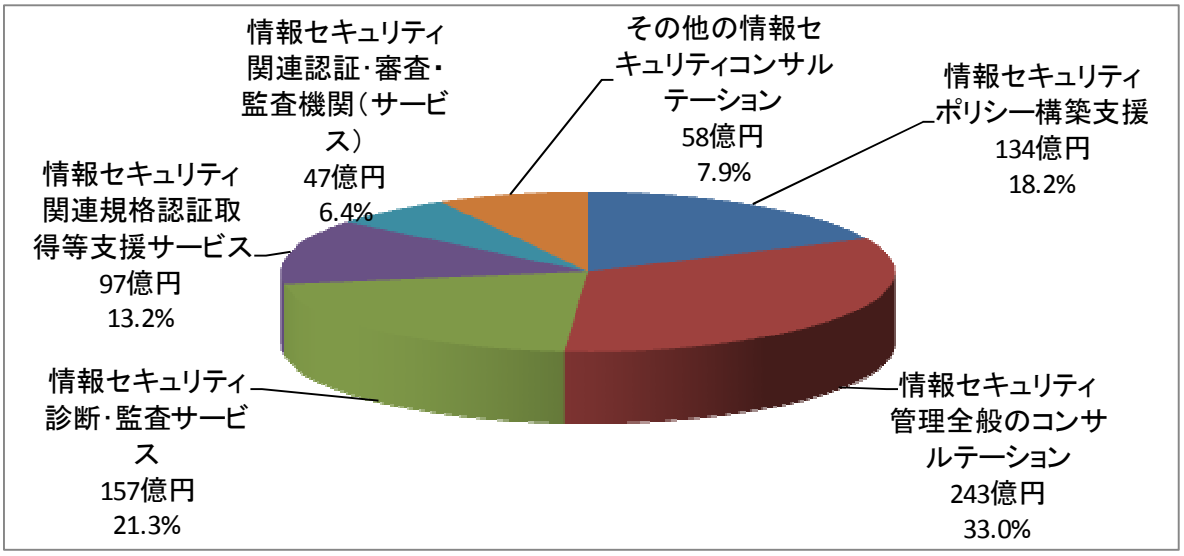
や体系をパッケージ化したサービス等があり「その他の情報セキュリティコンサルテーション」というセグメントを設けている。

(2)市場の動向

図 28 に、2007 年度における情報セキュリティコンサルテーション市場のセグメント別市場分布を示す。

「情報セキュリティコンサルテーション」というカテゴリは、ここ数年で市場の構造が大きく変わってきていると見られる。コンサルテーションはその特性から、情報セキュリティに関する取組の先端を歩むこととなり、必然的に時代の要請に即した内容や市場の問題を反映したものとなる。

図 28　2007 年度の情報セキュリティコンサルテーション市場



企業においては、経営リスクとしての情報セキュリティに対する認識が急速に進んでいる。J-SOX への対応やコンプライアンス対応、知的財産の防衛、事業継続管理等の課題に直面しており、マネジメントの知識と IT 技術への理解の両面が要求されている。それに応えるように、システムインテグレータのみならず、監査法人やその系列のコンサルティングファームによるコンサルテーションが増加してきている。

2008 年 4 月以降に適用開始となる内部統制報告制度への対応の一環として、2006 年頃から IT 統制推進への動きが強まり、IT 統制を支える柱の一つである情報セキュリティのあり方も強く意識されるようになっている。IT 統制の考え方の中心はアクセス管理であり、また IT 上で処理される業務プロセスと会計プロセスのコンプライアンス確保と記録の保全、追跡可能性が問われることになる。これらは全て情報セキュリティの確立によって実現されるものだからである。

このことが、アクセス管理、ポリシー管理、ログの保全といった情報セキュリティ需要を押し上げ、またその導入・実現のための情報セキュリティコンサルテーションの需要を押し上げている。内部統制監査の大きな部分を IT 統制監査が占めることから情報セキュリティ監査にも関心

が強まっている。

2005 年 4 月から個人情報保護法（個人情報の保護に関する法律）が全面的に施行されたが、これが引き金となりその前後にISMS認証やプライバシーマーク付与認定の取得に取り組む企業が増加した。とりあえず規格の要求する形を取り急ぎ整えるという対応も多く見られたが、企業が情報セキュリティに正面から取り組むきっかけになったと言える。ISMS 認証取得企業数はJIPDEC統計で2009年3月末現在3,158件、プライバシーマーク認定取得企業数は同じく10,139社となっている。

このような各種法制度の後押しのみならず、ここ数年来相次ぐ個人情報漏えいや企業秘密の持出し、漏えい、紛失が企業防衛のためのリスク管理の意識を高め、情報セキュリティの強化が企業の社会的信頼度の向上につながるという認識も広がりを見せている。これがコーポレート・ガバナンスの一環としての情報セキュリティガバナンス確立への動きとなり、情報セキュリティコンサルテーションの需要を押し上げる要因になっていると言える。

その他、情報セキュリティそのものではないが関わりが深い規格として IT サービスマネジメントシステム（ISO/IEC20000 規格）の認証も同じくJIPDECにより開始されている。また、民間がイニシアティブを取って進めている基準としてクレジットカード情報の保護を目的とするPCI DSSや、決済アプリケーションの開発事業者向けの基準 PA-DSS といった基準も登場し注目を浴びている。

このような様々な動きを背景として、他のカテゴリ同様「情報セキュリティコンサルテーション」市場の需要も高まり、2007 年度 15.8%、2008 年度 5.7%という前年度比市場成長率をもたらしている。

(3)市場規模とその推移

表 15 に国内の情報セキュリティコンサルテーション市場規模の実績推定値と予測値を、図 29 にその市場規模の推移のグラフを示す。

2007 年度においては、「情報セキュリティコンサルテーション」市場は全体で 735 億円程度となり、前年度比成長率は 15.7%であった。比較的規模の大きなセグメントは「情報セキュリティ管理全般のコンサルテーション」の 243 億円、「情報セキュリティ診断・監査サービス」の 157 億円、「情報セキュリティポリシー構築支援」の 134 億円の三つである。そのうち、「情報セキュリティ管理全般のコンサルテーション」が、前年度比成長率 18.6%と成長が著しかった。「情報セキュリティ診断・監査サービス」も前年度比 16.4%と高い伸びを示した。これらは、上に見たように内部統制報告制度を中心とした諸法例・諸制度とそれへの対応を含めた企業のリスク管理対応の進展が需要を押し上げているものと見られる。2008 年度もこの二つのセグメントは各5.9%拡大しており、同様の傾向が続いたことを示している。2009 年度になると不況の影響は診断・監査により強く表れ、「情報セキュリティ管理全般のコンサルテーション」のマイナス 4.4%に対して「情報セキュリティ診断・監査サービス」はマイナス 9.1%と縮小率が大きくなっている。

「情報セキュリティポリシー構築支援」市場はこれら二つのセグメントに比べて市場拡大の勢いは弱い。単なるポリシー構築・整備の段階は過ぎて、より総合的な情報セキュリティへの取組にシフトしている表れと見られる。

表 15　国内情報セキュリティコンサルテーション市場規模　実績と予測

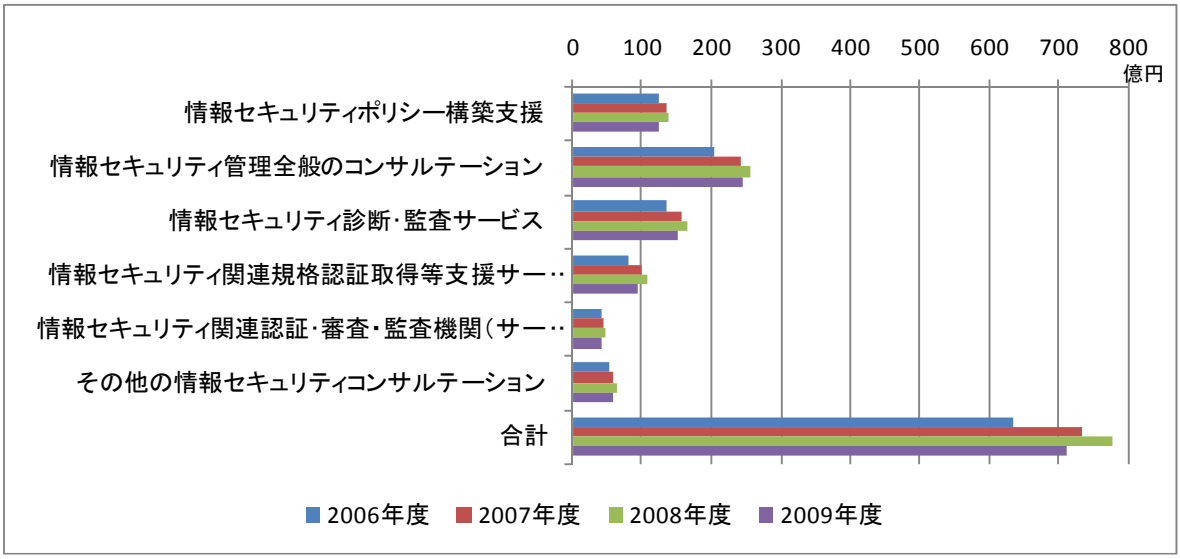
市場規模（百万円）	2006 年度	2007 年度	2008 年度	2009 年度
情報セキュリティポリシー構築支援	12,382	13,365	13,633	12,439
情報セキュリティ管理全般のコンサルテーション	20,480	24,280	25,704	24,574
情報セキュリティ診断･監査サービス	13,466	15,671	16,592	15,087
情報セキュリティ関連規格認証取得等支援サービス	7,892	9,675	10,474	9,039
情報セキュリティ関連認証･審査･監査機関（サービス）	4,143	4,672	4,991	4,337
その他の情報セキュリティコンサルテーション	5,087	5,834	6,314	5,705
合計	63,451	73,497	77,708	71,181
構成比				
情報セキュリティポリシー構築支援	19.5%	18.2%	17.5%	17.5%
情報セキュリティ管理全般のコンサルテーション	32.3%	33.0%	33.1%	34.5%
情報セキュリティ診断･監査サービス	21.2%	21.3%	21.4%	21.2%
情報セキュリティ関連規格認証取得等支援サービス	12.4%	13.2%	13.5%	12.7%
情報セキュリティ関連認証･審査･監査機関（サービス）	6.5%	6.4%	6.4%	6.1%
その他の情報セキュリティコンサルテーション	8.0%	7.9%	8.1%	8.0%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
情報セキュリティポリシー構築支援	―	7.9%	2.0%	−8.8%
情報セキュリティ管理全般のコンサルテーション	―	18.6%	5.9%	−4.4%
情報セキュリティ診断･監査サービス	―	16.4%	5.9%	−9.1%
情報セキュリティ関連規格認証取得等支援サービス	―	22.6%	8.3%	−13.7%
情報セキュリティ関連認証･審査･監査機関（サービス）	―	12.8%	6.8%	−13.1%
その他の情報セキュリティコンサルテーション	―	14.7%	8.2%	−9.6%
合計	―	15.8%	5.7%	−8.4%

2007 年度において、最も高い前年度比成長率を示したのは「情報セキュリティ関連規格認証取得等支援サービス」のセグメントで、前年度比 22.6%伸びて 97 億円に達したと推測される。2008 年度は前年度比成長率 8.3%で市場規模は 105 億円と、100 億円の大台に乗った。プライバシーマーク認定企業数は、2007 年度に約 2,100、2008 年度に約 1,000 増加[46]している。ISMS の認証取得登録数は 2007、2008 年度各々477、531 増加している。このような動きが市場の拡大につながっているものと考えられる。これに対応して「情報セキュリティ認証･審査・監査機関（サービス）」市場も 2007 年度 47 億円（前年度比成長率 12.8%）、2008 年度 50 億円（同 6.8%）と拡大している。これら両市場も 2009 年度にはマイナス 13%台と大きく落ち込む可能性が大きい。

「情報セキュリティコンサルテーション」市場全体として、2009 年度はマイナス 8.4%と比較的大きな落ち込みを見込む。J-SOX 対応が一段落し、体制や制度の整備への新たなニーズが後退することと企業の不況対策の影響を受けることによるものと考えられる。

[46] 新規取得数から中止、取消しを差し引いた純増数

図 29　国内情報セキュリティコンサルテーション市場推移



8.2.2　セキュアシステム構築サービス市場

(1)サービスの概要と特性

本カテゴリには、「IT セキュリティシステムの設計・仕様策定」、「IT セキュリティシステムの導入・導入支援」、「セキュリティ製品の選定・選定支援」、「その他のセキュリティシステム構築サービス」の 4 セグメントが含まれ、主にネットワークインテグレータ、システムインテグレータにより提供されている。

「IT セキュリティシステムの設計・仕様策定」は、IT システムのセキュリティに関しての設計、仕様の定義を実施するサービスである。システム設計時にセキュリティ対策についてセキュリティ専門家による支援を提供する。また、既存のシステムに対してセキュリティを付加しまたは向上させるための対策を設計するニーズもあり、一定の需要を保っている。

「IT セキュリティシステムの導入・導入支援」は、セキュリティに特化したシステムまたはシステムのセキュリティに関する部分の構築に際して、セキュリティ製品などを導入し、システムを構築、あるいは、その支援をするサービスであり、既存システムへのセキュリティ対策の追加やセキュリティに特化したシステム導入なども含まれる。セキュリティに関するインテグレーション・エンジニアリングサービスと言える。この市場もまた、情報セキュリティ対策またセキュリティレベル向上という目的のためには、専門家による総合的セキュリティ機能の構築が必要だという認識が浸透することで、大きな需要を形成している。

「セキュリティ製品の選定・選定支援」は、顧客のポリシーや要求に基づいて、それに適したセキュリティ対策製品の選定またはそのための情報提供等の支援を行うサービスである。過去数年で、情報セキュリティに対する重要性が意識され、情報セキュリティ対策を実施する企業も増加した。その結果、セキュリティ製品の導入に際して、セキュリティの専門家による製品選定や製品の比較評価のサービスを活用するニーズが顕在化してきている。

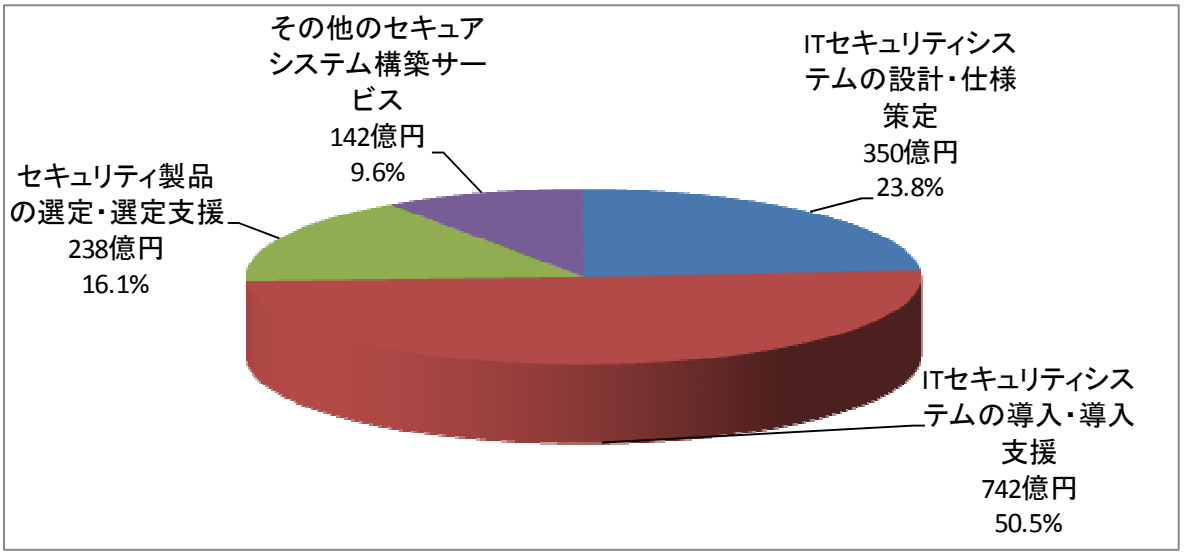
上記３セグメントに当てはまらない IT セキュリティシステムの構築サービスを「その他のセキュアシステム構築サービス」とした。

(2) 市場の動向

図 30 に 2007 年度のセキュアシステム構築サービス市場のセグメント別分布を示す。

「セキュアシステム構築サービス」は、セキュリティ製品の導入や構築を含めた、IT セキュリティシステムまたは IT システムのセキュリティに関する構築、及び構築を支援するサービスのカテゴリである。本カテゴリの市場規模は大きく、2007 年度で 1,471 億円と推定され、情報セキュリティサービス市場の 43.5%を占め、ツールも含めた情報セキュリティ市場全体の中で最大のカテゴリを形成している。

図 30　2007 年度のセキュアシステム構築サービス市場



本カテゴリは、実需としては拡大が継続すると考えられるが、市場規模を示す金額としては横這いか、徐々に下降して行くと予測している。これは、セキュリティ対策をシステムレベルで考える結果、「セキュリティシステムの構築」という切り出し方が段々されなくなり、その部分の金額をセキュリティ目的として分別して計上するケースが減ってくると推測されるためである。

「IT セキュリティの設計・仕様策定」、「IT セキュリティシステムの導入・導入支援」という機能そのものについては、セキュリティに対するスキルが一般的に不足している現在、セキュリティ専門家によるシステム設計・構築時の支援は依然必要であり、実質の需要は今後も増加すると予測される。その一方で、システム構築時に当然に考慮する要素としてセキュリティ設計も組み込まれるようになると見込まれる。その場合、一般のシステムインテグレーションから独立した形でのセキュアシステム構築サービスの発注は減少し、見かけ上の市場規模は縮小する方向に向かうと考えられる。システムにおけるセキュリティが「当り前」になって行く結果、見かけの需要は減少するという現象となって表れるが、セキュリティのあるべき姿としては望ましい方向に向かう結果と理解したい。

(3)市場規模とその推移

表16に国内セキュアシステム構築サービス市場規模の実績推定値と予測値を、図31にその市場規模の推移のグラフを示す。

「セキュアシステム構築サービス」市場は、2006 年度 1,426 億円、2007 年度 1,471 億円、2008 年度 1,494 億円と 1,400 億円台を維持して 1500 億円に迫ったと推測され、「情報セキュリティサービス」の中で 4 割以上を占めると推定される大規模な市場である。ただし、市場の伸び率は、2006 年度から 2007 年度にかけては 3.2%、2008 年度は 1.6%と限定的であり、2009 年度は経済情勢の急激な悪化の影響を受け前年比 マイナス 11.4%になると予測される。

表 16　国内セキュアシステム構築サービス市場規模　実績と予測

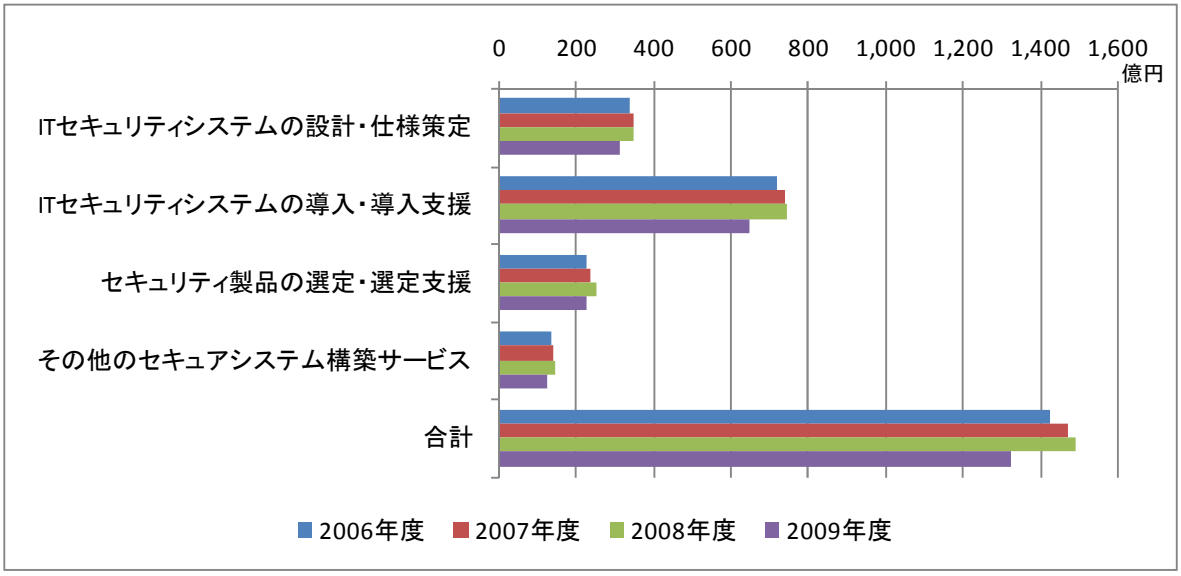
市場規模（百万円）	2006 年度	2007 年度	2008 年度	2009 年度
IT セキュリティシステムの設計･仕様策定	33,912	34,976	35,004	31,474
IT セキュリティシステムの導入･導入支援	72,269	74,231	74,549	65,242
セキュリティ製品の選定･選定支援	22,693	23,755	25,304	22,932
その他のセキュアシステム構築サービス	13,711	14,169	14,567	12,749
合計	142,585	147,130	149,425	132,397
構成比				
IT セキュリティシステムの設計･仕様策定	23.8%	23.8%	23.4%	23.8%
IT セキュリティシステムの導入･導入支援	50.7%	50.5%	49.9%	49.3%
セキュリティ製品の選定･選定支援	15.9%	16.1%	16.9%	17.3%
その他のセキュアシステム構築サービス	9.6%	9.6%	9.7%	9.6%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
IT セキュリティシステムの設計･仕様策定	―	3.1%	0.1%	−10.1%
IT セキュリティシステムの導入･導入支援	―	2.7%	0.4%	−12.5%
セキュリティ製品の選定･選定支援	―	4.7%	6.5%	−9.4%
その他のセキュアシステム構築サービス	―	3.3%	2.8%	−12.5%
合計	―	3.2%	1.6%	−11.4%

この中で「IT セキュリティシステムの設計・仕様策定」は、情報セキュリティポリシーに基づき、IT アーキテクチャとの整合を睨みながら IT 上にセキュリティ対策を実装するための設計を行う仕事であり、「情報セキュリティ管理全般のコンサルテーション」とも連携する市場であるが、「市場の動向」の項で見たように統計的には伸び率は限定的となる。このセグメントは 2007 年度の規模が 350 億円と大きく、「セキュアシステム構築サービス」カテゴリの 4 分の 1 弱を形成している。

「IT セキュリティシステムの導入・導入支援」は「セキュアシステム構築サービス」カテゴリの約半分を占める、セグメントとしては極めて大きい規模の市場である。2007 年度の市場規模は 742 億円と突出して大きな規模となっている。しかし、「IT セキュリティシステムの設計・仕様策定」と同様に統計に表れる数字としての伸び率は限定的となる。更に 2009 年度は内部統制対

応が一段落つくこと、セキュリティシステムがシステム構築上必然の要素として埋没すること、経済情勢の悪化によりシステム投資が鈍化して行くことから、このセグメントの市場規模は12.5%ほど減少して 652 億円となり、700 億円を大きく割り込むことになると推定される。

図 31　国内セキュアシステム構築サービス市場推移



一方、「セキュリティ製品の選定・選定支援」も前者と同様の理由で横這いか若干の減少となるが、例えば J-SOX 対応のログ取得解析システムの構築にセキュリティ製品の選定は欠かせなく、「IT セキュリティシステムの設計・仕様策定」や「IT セキュリティシステムの導入・導入支援」よりは安定した市場であると想定できる。その結果、2009 年度の規模が 229 億円と「セキュアシステム構築サービス」カテゴリの中で唯一、2006 年度を上回るものと見られる。

8.2.3　セキュリティ運用・管理サービス市場

(1)サービスの概要と特性

「セキュリティ運用・管理サービス」は、大きく分けると、IT セキュリティシステムまたは IT システム上のセキュリティ対策機器等の運用や管理の支援を行い、システム、サーバ、ネットワーク状態等の監視を行う、いわゆる運用支援サービス、もしくはマネージドセキュリティサービスと呼ばれる領域と、脆弱性検査、インシデント対応や脆弱性に関する情報の提供等、より専門性の高いニーズを満たすプロフェッショナルサービスの領域、それに SSL サーバ証明書に代表される電子証明書の発行を行う電子認証サービスの三つのカテゴリに大別される。

マネージドセキュリティサービスの領域については、その監視対象別に「セキュリティ総合監視･運用支援サービス」「ファイアウォール監視･運用支援サービス」「IDS／IPS 監視･運用支援サービス」「ウイルス監視･ウイルス対策運用支援サービス」の 4 セグメントを定義した。またスパム対策や有害ウェブフィルタリングをアウトソースサービスとして提供するビジネスモデルの

拡大に対応して「フィルタリングサービス」を今年度から独立セグメントとした。この一部は従来「ウイルス監視･フィルタリング・運用支援サービス」としてウイルス監視と同一セグメントに分類していた。

プロフェッショナルサービスには各々特性の異なる「脆弱性検査サービス」「セキュリティ情報提供サービス」「インシデント対応関連サービス」の 3 セグメントがある。

「脆弱性検査サービス」はペネトレーションテスト（侵入検査）とも呼ばれ、専門家のスキルによりハッカーと同様の攻撃を行ってシステムやアプリケーションの脆弱性を発見し対策を指導するもので、特定のスキルを持った企業が専門サービスとして提供している。アプリケーションについてはコードを解析して弱点を見つけ出すホワイトボックス検査もある。

「セキュリティ情報提供サービス」は世界中のネットワークの状態を監視、あるいは専門サイトを巡回して脆弱性情報を収集し、それらを解析してネットワークからの攻撃の予報や警報、傾向分析と対策等を地域別、業種別、時期や時間帯別等きめ細かく提供するサービスで、IT が事業上極めて重要な企業等の組織に提供している。

「インシデント対応関連サービス」はハッキングや情報漏えいといった情報セキュリティインシデントに際して、その対応や原因分析、事後対策等を専門家のノウハウを駆使して支援する専門サービスである。コンプライアンス対応や内部犯行事例の増加に伴い、電子的証拠の収集・解析・保全も必要度が高まっており、そのようなデジタルフォレンジック対応のサービスも提供されるようになってきた。

「電子証明サービス」は公開鍵暗号技術を応用して公開鍵と秘密鍵のペアで本人性、真正性、無改ざん等を証明するための電子証明書を発行するサービスである。電子証明書の仕組みは PKI（Public Key Infrastructure、公開鍵基盤）とも呼ばれる。

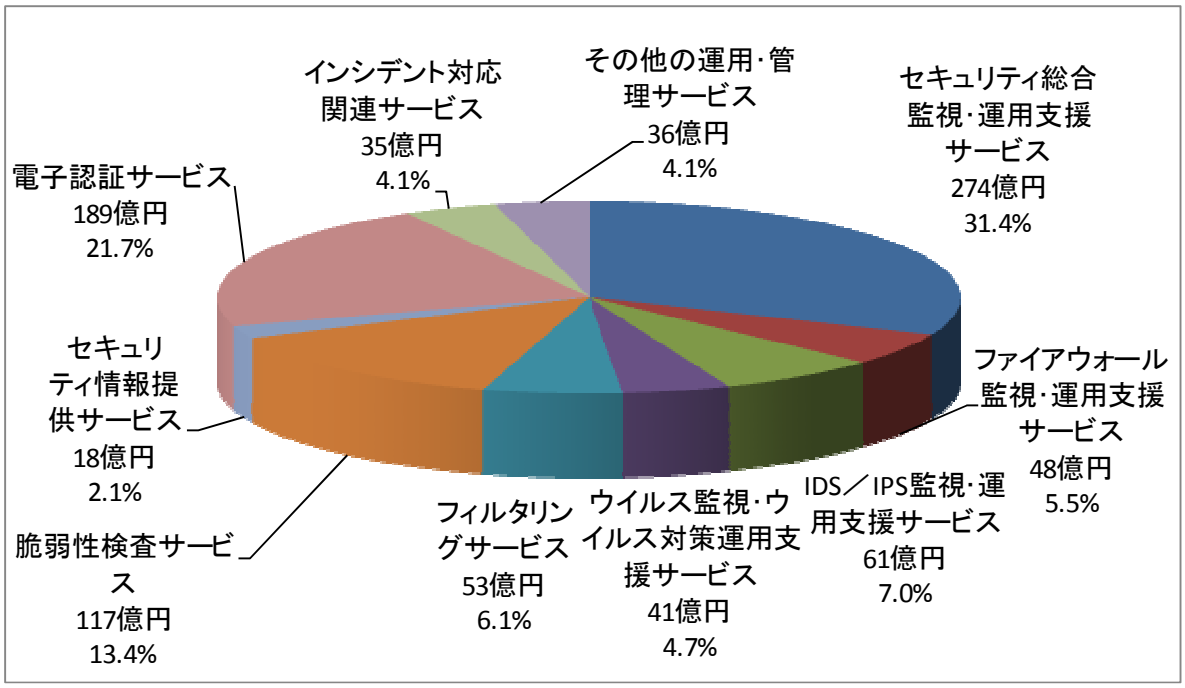
(2)市場の動向

これらのサービスの市場は、セキュリティ対応は適切な社外の専門サービス提供者に外部委託するというアウトソース需要によって支えられている。背景には、セキュリティ対策機器・サービス等の運用管理が専門家の知識を益々必要とする一方、そのような専門スキルを有する人材が利用組織内に不足していることや、問題発生時には 24 時間 365 日の迅速な対応が必要とされるケースが多いことがある。ネットワーク脅威の複雑化・深刻化と、セキュリティ対策が高度化・統合化に向う流れを背景に、この「セキュリティ運用・管理サービス」分野は、各セグメントの成長率には差異があるものの､全体としてはその重要性を増し､市場は拡大基調にあると言える。

図 32 に 2007 年度のセキュリティ運用・管理サービス市場のセグメント別分布を示す。

個々のセグメントを順に見て行くと、まず運用支援サービスについては、個別の「ファイアウォール監視・運用支援サービス」､「IDS／IPS 監視・運用支援サービス」､「ウイルス監視･ウイルス対策運用支援サービス」が従来から各々の市場を形成しており、今後も堅調に推移すると見られる。また、それらの機能を統合化した各種アプライアンス製品の普及を背景としつつ、ネットワーク環境、サーバ稼働状況、場合によってはサーバ上で実行されるソフトウェアまでを統合的に監視・運用支援する「セキュリティ総合監視・運用支援サービス」の伸長が特に著しい。また深刻化するスパムメールの被害への対応から「フィルタリングサービス」需要が急拡大している。

図 32　2007 年度のセキュリティ運用･管理サービス市場



「脆弱性検査サービス」は、独自のセグメントと一定の市場を形成しており、需要は増加傾向にある。近年では特にウェブアプリケーションの脆弱性に関する関心が高まっている。検査サービスも、従来型の専門技術者が個別に手作業で実施する脆弱性診断サービスに加えて、既知の攻撃手法を自動化することでコストを大幅に抑えた ASP サービスなども登場してきており、需要のすそ野の拡大が期待される。

「インシデント対応関連サービス」も情報セキュリティインシデントの増加とその対応需要の範囲の拡がり（緊急対応、復旧対応、デジタルフォレンジック対応等）に伴い、一定の市場規模に達している。

その他、ますます複雑化・高度化する各種インシデント・脆弱性・パッチ情報等に対応するための「セキュリティ情報提供サービス」についても、専門性の高いサービスとして、金額的には小規模ながら今後も一定の市場規模を維持するものと思われる。

このような外部からの攻撃対策や脆弱性対策とは異なり、積極的な本人・本物の認証対策や通信路の安全性確保対策として大きなサービスセグメントを形成しているのが、「電子認証サービス」である。従来のウェブサーバやセキュリティ対策機器用の電子証明書に加え、ID・パスワードに代わるネット上での本人確認手段の高度化の手段として、また電子情報・電子文書の真正性確認の手段として、タイムスタンプを含めた各種電子認証サービスの利用が定着している。このセグメントは、電子署名法、e-文書法、また個人情報保護法等の法的要請への対応の拡がりを含め、その重要性の高まりと共に市場規模を拡大している。

(3)市場規模とその推移

「セキュリティ運用・管理サービス」の分野全体の市場規模は、実績推定値が 2007 年度で 872 億円であり、2006 年度の 741 億円と比較して 17.7%増という高い伸びを示した。また金額ベースでも、「情報セキュリティサービス市場」において「セキュアシステム構築サービス」に次ぐ位置を占めている。しかしながら、今後の予測値では 2008 年度で 917 億円（前年比成長率 5.2%）、2009 年度で 891 億円（同マイナス 2.9%）と、情報セキュリティサービス市場全体と歩調を合わせて成長が鈍化するものと予測される。

表17に国内セキュリティ運用・管理サービス市場規模の実績推定値と予測値を、図33にその市場規模の推移のグラフを示す。

表 17　国内セキュリティ運用・管理サービス市場規模　実績と予測

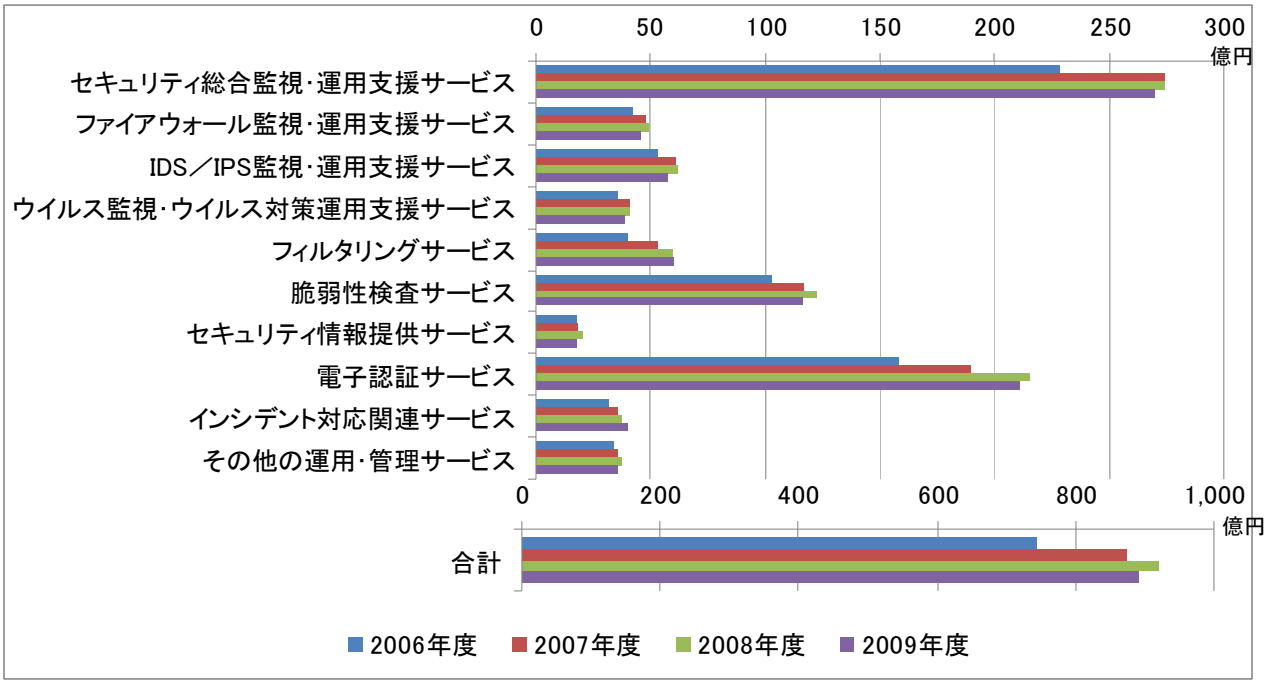
市場規模（百万円）	2006 年度	2007 年度	2008 年度	2009 年度
セキュリティ総合監視･運用支援サービス	22,816	27,373	27,358	26,977
ファイアウォール監視･運用支援サービス	4,161	4,774	4,865	4,550
IDS／IPS 監視･運用支援サービス	5,354	6,093	6,185	5,790
ウイルス監視･ウイルス対策運用支援サービス	3,556	4,093	4,137	3,839
フィルタリングサービス	3,984	5,314	5,888	6,010
脆弱性検査サービス	10,285	11,672	12,231	11,557
セキュリティ情報提供サービス	1,726	1,848	1,974	1,722
電子認証サービス	15,759	18,939	21,576	21,073
インシデント対応関連サービス	3,115	3,538	3,786	4,029
その他の運用･管理サービス	3,377	3,589	3,777	3,569
合計	74,134	87,233	91,777	89,115
構成比				
セキュリティ総合監視･運用支援サービス	30.8%	31.4%	29.8%	30.3%
ファイアウォール監視･運用支援サービス	5.6%	5.5%	5.3%	5.1%
IDS／IPS 監視･運用支援サービス	7.2%	7.0%	6.7%	6.5%
ウイルス監視･ウイルス対策運用支援サービス	4.8%	4.7%	4.5%	4.3%
フィルタリングサービス	5.4%	6.1%	6.4%	6.7%
脆弱性検査サービス	13.9%	13.4%	13.3%	13.0%
セキュリティ情報提供サービス	2.3%	2.1%	2.2%	1.9%
電子認証サービス	21.3%	21.7%	23.5%	23.6%
インシデント対応関連サービス	4.2%	4.1%	4.1%	4.5%
その他の運用･管理サービス	4.6%	4.1%	4.1%	4.0%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
セキュリティ総合監視･運用支援サービス	―	20.0%	−0.1%	−1.4%
ファイアウォール監視･運用支援サービス	―	14.7%	1.9%	−6.5%
IDS／IPS 監視･運用支援サービス	―	13.8%	1.5%	−6.4%
ウイルス監視･ウイルス対策運用支援サービス	―	15.1%	1.1%	−7.2%
フィルタリングサービス	―	33.4%	10.8%	2.1%
脆弱性検査サービス	―	13.5%	4.8%	−5.5%
セキュリティ情報提供サービス	―	7.1%	6.8%	−12.8%
電子認証サービス	―	20.2%	13.9%	−2.3%
インシデント対応関連サービス	―	13.6%	7.0%	6.4%

その他の運用･管理サービス	―	6.3%	5.2%	−5.5%
合計	―	17.7%	5.2%	−2.9%

セグメント別の内訳を見ると、「セキュリティ総合監視・運用支援サービス」が最大のセグメントであり、2007 年度の推定実績市場規模は 274 億円（前年度比成長率 20.0%）と、相対的に高い成長率を示したものの、2008、 2009 年度の市場規模は、各々274 億円（同 マイナス 0.1%）、270 億円（同 マイナス 1.4%）にとどまるものと予測される。

次に大きいセグメントは「電子認証サービス」で、2007 年度の推定実績市場規模は 189 億円（同 20.2%）と、こちらも高い成長率であった。今後の市場規模は、2008 年度は 216 億円（同 13.9%）と拡大基調を維持し、2009 年度についても 211 億円（同マイナス 2.3%）とほぼ前年並みを維持するものと予測される。

図 33　国内セキュリティ運用・管理サービス市場推移



個別機能のサービスである「ファイアウォール監視・運用支援サービス」、「IDS／IPS 監視・運用支援サービス」、「ウイルス監視・ウイルス対策運用支援サービス」についても、それぞれ成長率の鈍化傾向が見られる。実績市場規模推定値は 2007 年度で各々48 億円（前年度比成長率 14.7%）、61 億円（同 13.8%）、41 億円（同 15.1%）で、伸び率はいずれも「セキュリティ運用・管理サービス」全体の平均を下回っており、今後もこの傾向は続くものと予想される。市場規模としては各々、2008 年度に 49 億円（同 1.9%）、62 億円（同 1.5%）、41 億円（同 1.1%）、2009 年度に 46 億円（同マイナス 6.5%）、58 億円（同マイナス 6.4%）、38 億円（同マイナス 7.2%）と推移するものと予測される。

近年特に多様化・複雑化する脆弱性やインシデント対応に向けた専門性の高いサービスの需要拡大を受けて、際立った増加傾向を示しているセグメントに「脆弱性検査サービス」、「セキュリ

ティ情報提供サービス」、「インシデント対応関連サービス」がある。特に、「脆弱性検査サービス」は、 2007 年度の実績市場規模において、117 億円（前年度比成長率 13.5%）と推定されており、今後も「セキュリティ運用・管理サービス」カテゴリの中で一つの極を形成して行くものと予測される。また、「インシデント対応関連サービス」については、比較的小さい市場規模で推移するものの、今後も成長が期待される数少ないセグメントの一つである。一方「セキュリティ情報提供サービス」について、2008 年度は前年度比成長率 6.8%と拡大が続くが 2009 年度はマイナス 12.8%と需要の急激な後退が予測される。

8.2.4 情報セキュリティ教育市場

(1)サービスの概要と特性

情報セキュリティ対策部門やシステム管理部門、システム開発部門のような情報セキュリティの専門的知識やスキル（あるいは資格）の習得が必要な部署への教育は、自社内での対応はほぼ不可能で、外部の専門サービスを利用する。情報セキュリティ専門家や専業ベンダより提供される教育コースを目的に応じて受講して行くケースがほとんどである。本調査では、このような情報セキュリティ専門家や専業ベンダより提供される e-ラーニングサービス及び教育サービスと教育コンテンツ（e-ラーニングのコンテンツ含む）が集計対象となる。

「情報セキュリティ教育」市場は、情報セキュリティの専門家や専業ベンダにより提供されるサービスとして、「情報セキュリティ教育の提供サービス」、「情報セキュリティ教育のe-ラーニングサービス」、「情報セキュリティ関連資格認定及び教育サービス」、「その他の情報セキュリティ教育サービス」の4つの中分類市場（セグメント）に分類した。

「情報セキュリティ教育の提供サービス」は、教育コンテンツのみを提供して教育実施は客先社内で賄うケースと、教育実施まで一貫して提供するサービスの両方を含めている。情報セキュリティ教育コンテンツの作成・提供のみを行うサービスは、教育の中身そのものをテキストやデジタルファイルなどのコンテンツとして提供するサービスである。教育コンテンツの作成から情報セキュリティ教育の実施まで一貫して行うサービスは、実際に情報セキュリティ教育を外部からの「出張授業」として実施するサービスである。また、教育専門事業者が教材を開発しカリキュラム化して公開講座として設定して受講者を募集し、レディメイドのコースを販売するビジネスモデルもある。

「情報セキュリティ教育のe-ラーニングサービス」は、情報セキュリティ教育をe-ラーニングで実施する方式のうち、企業がイントラネットなどで展開するものではなく、外部の専門業者がインターネット上でASP／SaaSの形で提供するものである。企業内実施用やe-ラーニングの教育事業者向けにe-ラーニング用コンテンツの開発・提供をするサービスもこのセグメントに含む。e-ラーニングの特徴として、受講が個別受講者ごとに時間や場所の制約を受けずに可能になること、個別に講師が対応する必要がないこと、大人数に対して効率的に実施できること等が挙げられる。同時に、対象者一人一人の受講の有無や進捗度の管理、理解度の把握など、管理面の利便性が極めて高い。また十分に理解するまで反復受講ができることや長いコンテンツを分割して受講できることなど集合教育に比べて様々なメリットがある。

「情報セキュリティ関連資格認定及び教育サービス」は、情報セキュリティに関連する各種資格の認定・提供サービス及び資格取得のための専門的な教育を提供するサービスである。

この他、以上の分類に当てはまらない講師派遣サービス等を「その他の情報セキュリティ教育サービス」とした。

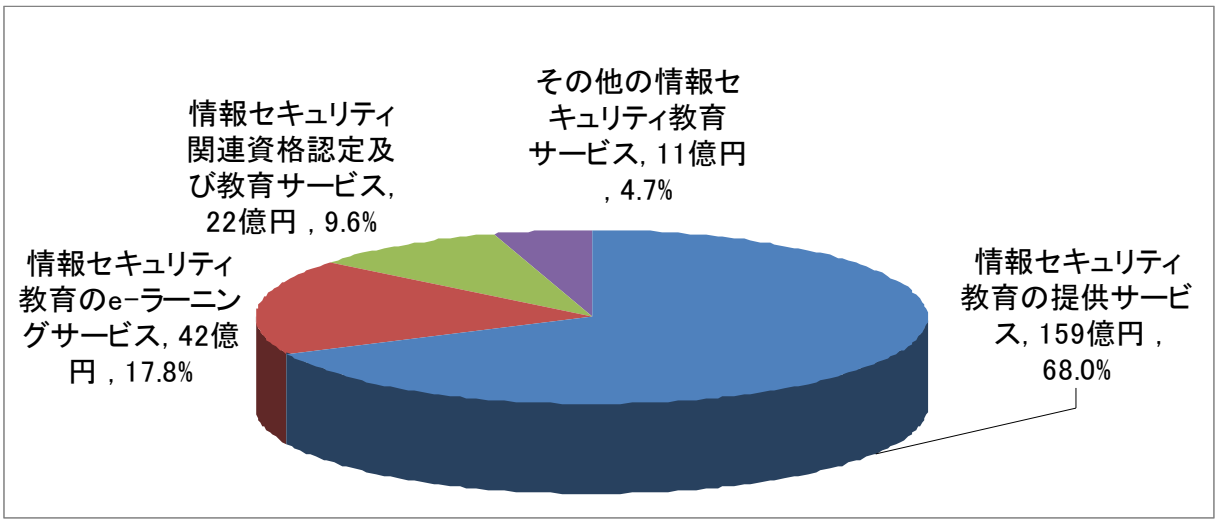
(2) 市場の動向

「情報セキュリティ教育」は、情報セキュリティ市場全体からみると決して大規模とは言えないが、年々確実に成長しているカテゴリである。

図34に2007年度の情報セキュリティ教育サービス市場のセグメント別分布を示す。

情報セキュリティ教育の必要性に対する認識は急速に高まっていると見られる。その要因は、他の情報セキュリティツールやサービスの需要を伸ばしているものと同様、情報漏えい対策とJ-SOX等のコンプライアンス対応である。情報セキュリティが情報システム部や情報セキュリティ管理統括部署など特定部門だけの問題でなく、全社員、全階層に徹底しなくては情報資産の保護やコンプライアンス対応が不可能なことが明らかになった結果である。

図 34　2007 年度の情報セキュリティ教育サービス市場



近年の技術の進歩や社会的要請など企業をとりまく様々な環境変化から、社員教育で必要とされる知識は広範囲となり、且つ多様化してきている。また一般社員向けに理解しやすく教えるためには教材や教育スキルも専門家のノウハウを活用する必要が出てくる。そのような背景から、情報セキュリティ専門家や専業ベンダによるサービスの需要が増大している。従って、情報セキュリティ教育の提供サービスは、主に一般社員向けの教育など、多様で多数の広い層を対象として提供されている。それに加え、CIOやCISOなどの経営陣、システム管理者、情報セキュリティ推進担当者など、特定の対象向けの需要も拡大しつつある。

e-ラーニングのASP／SaaSサービスは、学習履修管理サービス等を併せて利用することが可能、少人数でも比較的充実したコンテンツを安価で利用可能、等のメリットから、今後さらなる普及

が期待されるサービスである。「情報セキュリティ教育の提供サービス」のサービスでは実際に講師を招き、講習を実施する必要があるため、場所（特に首都圏、関西圏以外の地域）や受講する側の時間的拘束など制約事項が多く、またコストもかさむが、e-ラーニングのASP／SaaSサービスでは、そのような要素にとらわれることなく利用できることも大きなメリットである。さらに、ウェブ技術の進歩や通信回線の大容量化・高速化などから、提供できるコンテンツや提供の場・機会も増えてきている。課題としては理解度をどのように測定・管理するかで、e-ラーニングの中にテストの機能を盛り込んだりして対応している。

「情報セキュリティ関連資格認定及び教育サービス」市場は、対象者が資格取得を目標とする者に特定されるため、小規模な市場であると考えられてきた。しかし、近年国内で認定される情報セキュリティ関連資格に加え、グローバルな情報セキュリティ関連資格も普及しつつある。さらにそれらの資格の維持･更新のために継続教育単位（CPE: Continuing Professional Educations creditsなどと呼ばれる）が必要なものがあり、他資格の相互CPE認定も進み出していることなどから、この市場が徐々に拡大してきている。また、SI事業者や情報セキュリティ事業を営む企業を中心に、さらには情報セキュリティへの先進的取組を行う一般企業においても、社員の資格取得を奨励･支援する企業が増えている一方、不況への対策や定年後の収入の手段として個人での資格取得の動きも出てきている。

情報セキュリティ教育サービスは市場での需要増加に伴い、供給も増加して行くものと予測される。だが、その需要に合った教育コンテンツと、その内容を実施する十分な知識とスキルを持った講師の両方が、大幅に不足しているのが現状である。この状況は、情報セキュリティの推進と全体的な底上げに大きな支障となるため、教育できるだけの知識とスキルを持った情報セキュリティ人材の確保が急務である。情報セキュリティ資格の体系化、教育・研修機会の多様化と体系化、情報セキュリティ専門職のキャリアパスや人材モデルなど、政策的な対応も含めた社会的基盤整備の推進が必要と思われる。[47]

(3)市場規模とその推移

表 18 に国内情報セキュリティ教育市場規模の実績推定値と予測値を、図 35 にその市場規模の推移のグラフを示す。

「情報セキュリティ教育」カテゴリは、情報セキュリティサービス全体の市場に占める割合が7%程度と比較的小さい市場であるが、2007 年度には前年度比 34.0%増と急成長し、234 億円に達したと推測される。しかし 2008 年度には前年度比伸び率 8.8%と伸び率が縮まり、2009 年度にはマイナス 7%と縮小すると予測される。

---

[47] 人材育成並びに教育のための人材確保の必要性については、近年いくつかの研究報告や関連団体の創設がされている。

[1] 情報処理推進機構（IPA）, 情報セキュリティプロフェッショナル育成に関する調査研究, 2003. http://www.ipa.go.jp/security/fy14/reports/professional/ikusei-seika-press.html

[2] 経済産業省, 情報セキュリティ教育に関する調査報告書, 2004. http://www.meti.go.jp/policy/netsecurity/edu_report.html

[3] JNSA 情報セキュリティ推奨教育の検討に関する調査報告, 2005　http://www.jnsa.org/

[4] 情報セキュリティ教育事業者連絡会（ISEPA）　http://www.jnsa.org/isepa/index.html

表 18　国内情報セキュリティ教育市場規模　実績と予測

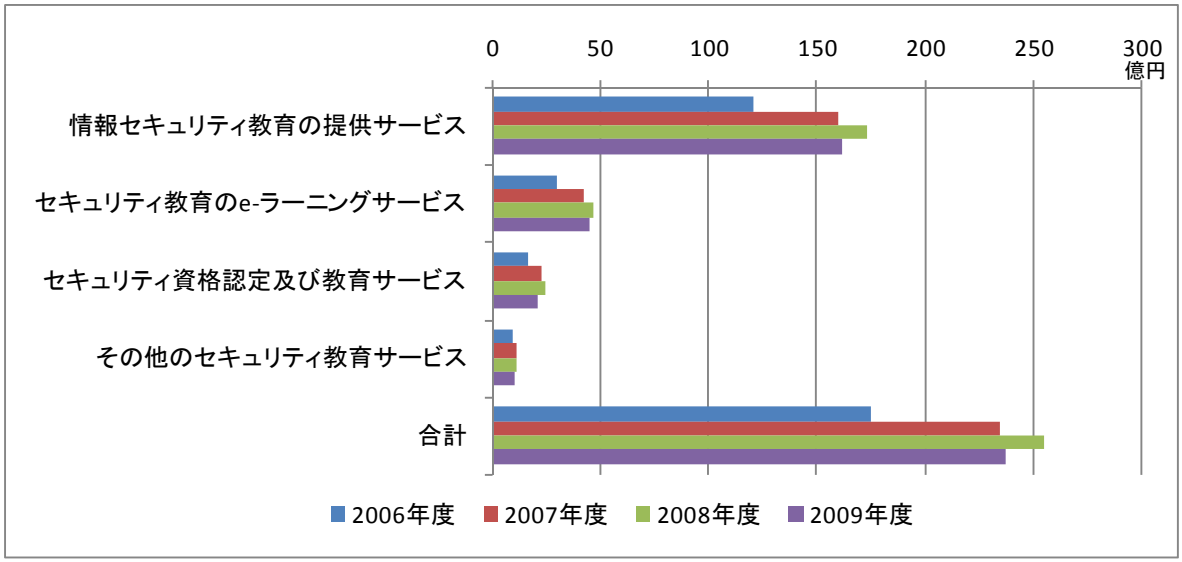
市場規模（百万円）	2006 年度	2007 年度	2008 年度	2009 年度
情報セキュリティ教育の提供サービス	12,051	15,909	17,313	16,114
情報セキュリティ教育の e-ラーニングサービス	2,978	4,165	4,635	4,455
情報セキュリティ関連資格認定及び教育サービス	1,590	2,236	2,406	2,084
その他の情報セキュリティ教育サービス	848	1,094	1,107	1,016
合計	17,467	23,404	25,461	23,669
構成比				
情報セキュリティ教育の提供サービス	69.0%	68.0%	68.0%	68.1%
情報セキュリティ教育の e-ラーニングサービス	17.0%	17.8%	18.2%	18.8%
情報セキュリティ関連資格認定及び教育サービス	9.1%	9.6%	9.4%	8.8%
その他の情報セキュリティ教育サービス	4.9%	4.7%	4.3%	4.3%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
情報セキュリティ教育の提供サービス	―	32.0%	8.8%	−6.9%
情報セキュリティ教育の e-ラーニングサービス	―	39.9%	11.3%	−3.9%
情報セキュリティ関連資格認定及び教育サービス	―	40.6%	7.6%	−13.4%
その他の情報セキュリティ教育サービス	―	29.1%	1.2%	−8.2%
合計	―	34.0%	8.8%	−7.0%

このカテゴリの最大のセグメントは68%を占める「情報セキュリティ教育の提供サービス」であり、市場規模は2006年度に121億円、2007年度には159億円（前年度比成長率32.0%）と推移し、2008年度には173億円（同8.8%）に達するが、2009年度は一転161億円（同マイナス6.9%）に戻ると予測される。この要因は上記に見たように、社員教育を外部委託する動きの結果であると分析できる。社員全員に対して情報セキュリティに対するリテラシを植え付けて、現場の末端まで情報漏えい対策を徹底する必要に迫られる一方、それを自社内でまかなうことが困難なことから、コンテンツの制作や教育の実施等について、専門家による教育サービスに依存しようという発想が、ここに明確に表れている。ただし、2009年度は不況の影響により各企業が教育への予算の削減、縮小を行うためマイナス成長となると予測する。

2006～2009年度各年度の市場規模推移が30億円、42億円、46億円、45億円と、市場規模としては小さいセグメントである「情報セキュリティ教育のe-ラーニングサービス」は、対前年度比伸び率で見ると、2007、2008年度に各々39.9%、11.3%と非常に速いペースで拡大するが、2009年度はマイナス3.9%とマイナス成長を余儀なくされるものと見られる。

「情報セキュリティ資格認定及び教育サービス」は2006年度において16億円のマーケットであったが、2007年度には前年度比40.6%増とさらに成長して22億円の規模になったと推測される。2008年度には24億円弱（前年度比伸び率7.6%）とさらに拡大するが、2009年度には企業側の資格取得投資が絞り込まれることから13.4%と大幅なマイナスとなり、21億円の市場規模に落ち着くと予測する。

図 35　国内情報セキュリティ教育市場推移



8.2.5　情報セキュリティ保険市場

(1)サービスの概要と特性

「情報セキュリティ保険」とは、情報セキュリティインシデントによって生じる経済的損失を補償する保険商品である。

情報セキュリティ保険は、歴史的に見るとコンピュータ保険の派生商品ということができる。コンピュータ保険は、コンピュータ装置自体の破損等とそこで扱うデータあるいはデータの保管媒体の破損に伴う損失の補てんを目的としたものである。情報セキュリティに起因するこれら損害を担保するオプション商品が 1980 年代に登場している。また、ネットワークの普及に伴って、1990 年にはネットワークの中断リスクに特化したネットワーク中断保険も開発された。

これらの保険商品の上に、1990 年代の後半には本格的な情報セキュリティ保険が開発される。名称としては、IT 保険やネットワーク保険などとも呼ばれる。その開発の背景には、インターネットの商用利用への開放に伴う経済活動への急速な普及と、企業向け保険商品開発の自由化という需給両面での変化がある。前者については、事業活動のネットワークシステムへの依存度が高まり、情報セキュリティインシデントが発生したときの経営へのインパクトが極めて大きくなっていったことと、その一方で IT システムやネットワークシステムの信頼性を 100%確保することが困難であるという現実があると考えられる。従って、当初は保険を契約する主体は IT 事業者がメインであった。また製造物責任の考え方が整備されたこともサービス事業者側の保険需要を押し上げたと想定される。

当初保険対象として想定していたリスクは、電源遮断、自然災害や誤操作などによるネットワークの停止やデータの喪失に伴う事業損失が中心であったが、ウイルス感染や不正アクセス等の脅威が顕在化してくると、それらも外来の不可抗力要因として必然的に保険対象となった。同時に、販売対象も IT 事業者だけでなく、一般の事業法人にも広がった。IT の利用者にとっても、

事業者の責任だけを追求して済む訳に行かなくなった状況があるためと言える。

2000 年代になると、LOVE ウイルス等の大規模感染や省庁ウェブサイトのハッキングなどを通じて、情報セキュリティは広く社会及び企業の関心事となってくる。個人情報の大規模漏えいが社会問題となり、損害賠償請求訴訟や、企業の「おわび金」支払いのような事例も発生したことから、個人情報漏えいに伴う一次的・二次的被害や復旧対策費を補償対象とする「個人情報漏えい保険」なども開発され、情報セキュリティに対する様々な補償を提供する保険商品の充実を見るようになった。現在では、個人情報漏えい、データ消失、ネットワーク中断など様々な情報セキュリティに関わる損害を補償する保険商品が提供されている。

情報セキュリティ保険の需要を後押しする要因の一つとして、情報セキュリティマネジメントシステム（ISMS）が挙げられる。ISMS の普及に伴い、低減、回避、予防等の情報セキュリティ対策と取み合わせて、「リスクの移転」を対策の一つとして取り入れることで情報セキュリティに対するリスクマネジメントを確立する取組が進んでいる。情報セキュリティ保険は、いわゆるリスクファイナンスの考え方で利用するサービスと言える。

「情報セキュリティ保険」に加入しておくことで、情報セキュリティ事故が発生することを恐れることなく、情報システムの利点を活かしたビジネス展開をより積極的に行うことができる。このような位置付けから、企業が情報セキュリティ対策を本格化させ、経営的視点で総合的対応を考えるようになってきた中で、様々な対策手段を取み合わせても、なお残るリスクをカバーする最後の手段として採用するケースが増えている。

なお、本調査では、原則として、情報セキュリティを付保対象とする情報セキュリティ保険（コンピュータ保険等の一部である場合にはその部分のみ）を集計対象としている。

(2)市場の動向

情報セキュリティ保険は、上にも見てきたように、IT システム並びにその上で取り扱われる情報､総称して情報資産と言われるものに関する損害を補てんする保険である｡付保対象としては、IT システム自体の破損等の損害、IT システムの上で取り扱われるデータの破壊や喪失に伴う損害、情報漏えい等に伴う第三者への賠償責任、これらに伴う業務損害や逸失利益等がある。

また、特定のセキュリティ製品と取み合わせて、その製品の防御対象に対する防御のほころび等を保険でカバーすることに限定した、いわゆるバンドル商品として開発される保険も登場している。このように、情報セキュリティ保険は、情報セキュリティに関わるリスクの複雑化とニーズの多様化に対応してその商品バリエーションを拡大している。

情報セキュリティ保険の供給主体は、法律上損害保険事業者に限定される。主として大手の損害保険会社からさまざまなバリエーションの IT 保険、情報セキュリティ保険が提供される。SI 事業を営む大手電機事業者のグループに属する損保子会社が、SI 事業者の商品・サービスの品揃えの一環として開発する事例も見られる。これら保険商品が、さまざまな販売チャネルを通じてエンドユーザに提供される。基本的には損害保険事業者の販売代理店経由となる。販売代理店には、損保本来の代理店チャネルである金融機関、建設事業者、自動車販売の他に、電機や事務機器の販売代理店等もある。特にパソコンや複合機の販売店は、IT の販売と同時にセキュリティ対策についても助言や支援を求められるケースが増えていると見られ、対策手段の一つとして保険

の提供も行うようになっている。

(3)市場規模とその推移

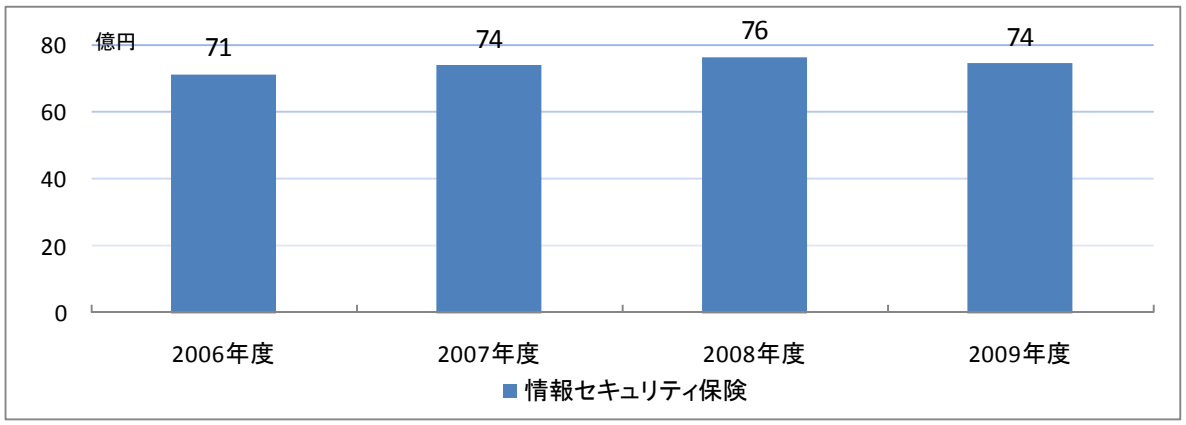
表 19 に国内情報セキュリティ保険市場規模の実績推定値と予測値を、図 36 にその市場規模の推移のグラフを示す。

表 19　国内情報セキュリティ保険市場規模　実績と予測

市場規模（百万円）	2006 年度	2007 年度	2008 年度	2009 年度
情報セキュリティ保険	7,111	7,354	7,625	7,417
対前年比成長率				
情報セキュリティ保険	－	3.4%	3.7%	-2.7%

「情報セキュリティ保険」市場は、2006 年度には 71 億円に達していたと見られる。その前年度から急速に規模を拡大したと推測されるが、これは、2005 年度の個人情報保護法の全面施行により情報の紛失・漏えいの公表件数が飛躍的に増え、企業におけるリスク認識と対策意識が強まったことが主因となって、リスクファイナンスの視点から「個人情報漏えい保険」の購入が一気に進んだ結果と見られる。2007 年度には一転して市場の伸び率は落ち着いたものとなり、3.4%増の 74 億円程度の規模であると推測される。2008 年度は、年度途中からの急激な経済状況の変化はあるものの、情報セキュリティ市場全体として成長を維持する中で若干市場を拡大し、76 億円程度の市場となるものとみられる。2009 年度は極めて予測の困難な状況であるが、景気の悪化の影響は避けられず、前年度比 2.7%減少して再び 74 億円程度に戻るのではないかと予測する。

図 36　国内情報セキュリティ保険市場推移



「情報セキュリティサービス」市場全体との比較では、2007 年度、2008 年度は伸び率で下回っている。一方、2009 年度の予測では、「情報セキュリティサービス」市場全体ほどの落ち込みは見込まれていない。これは情報セキュリティコンサルテーション、特に認証取得関連や、セキュアシステム構築のような新規取組部分のブレーキが大きく効くのに対して、運用管理等の日常業務に近い部分は最低限のものが維持される結果と考えられる。

9. 海外情報セキュリティ市場との比較

この項では、本調査において推計した国内情報セキュリティ市場規模を海外の情報セキュリティ市場規模と比較する。比較対象として用いたデータは、国際的な市場調査会社である米国 IDC 社（International Data Corporation）の日本法人から、本調査との比較のために提供を受けた、世界の情報セキュリティ市場に関する市場規模データである。なお、同社の推計方法と、本調査における国内市場規模の推計方法が異なる。また、市場区分の定義も完全には一致しない。その結果、本調査結果の数字と、IDC 社が日本市場の規模として推定している数字には、相当の乖離がある。従い、海外市場の数字についても、違う基準で集計されていると考えられるが、本調査と類似の市場定義により、世界各地域をカバーする調査データは他には少ないことから、同社のデータとの比較を行う。従い、あくまでも参考としての比較となることに留意いただきたい。

また、IDC 社の統計数字は、その作業時期が本調査よりも早い時期であり、2008 年 9 月～10 月以降急速に深刻度を増した世界的な金融危機と同時不況の影響について、十分には織り込んでいないと見られる。本調査も 2008 年度、2009 年度に及ぶ影響については具体的見通しが得られないまま作業時点（2009 年 1 月～2 月）で得られた情報に基づいて推計を行っている。従い、その作業時点の差に基づく差異や、時間の経過と共に起こる変化との間のギャップが生じうることをお断りしたい。

国内市場規模調査の対象期間は日本での一般的な会計年度単位（当年 4 月～翌年 3 月）であるのに対し、海外市場規模は全て暦年（当年 1 月～同年 12 月）であるが、便宜上そのまま比較する。また、海外市場規模の原数字は米ドル表示であり、IDC 社の採用する基準レートにより円換算した額を比較対象としている。

換算に使用した為替レートは次の通りである。

2006 年・暦年：116.3310 円／米 $
2007 年・暦年：117.8145 円／米 $
2008 年・暦年：105.8768 円／米 $
2009 年・暦年：105.8768 円／米 $

9.1 市場区分の定義の比較

IDC 社は、市場の区分を基本的にアプライアンス、ソフトウェア、サービスの 3 区分に分類している。これは商品の形態を第一に区分基準としていることになる。本調査では「アプライアンス」と「ソフトウェア」をまとめて「ツール」という括りとし、統合型アプライアンスを除いては機能別にカテゴライズしている。つまり「モノ」と「サービス」の形態区分に機能区分を取り合わせている。その対応関係は、概ね表 20、表 21 のように仕分けられると考えられ、両調査は、市場区分の定義においては概ね対応付けられると言える。

表 20　アプライアンスに関する IDC 定義と本調査の定義の対応

IDC 調査の定義	本調査の定義
セキュリティアプライアンス Security Appliance	統合型アプライアンス
	ネットワーク脅威対策製品のうち ファイアフォールアプライアンス VPN アプライアンス IDS／IPS アプライアンス アプリケーションファイアウォール

注：IDC 社のアプライアンスには、ネットワーク脅威対策型だけでなく、セキュアコンテンツ管理型も分類されている。具体的には、ウイルス、ウェブ、メール等のフィルタリングを提供するアプライアンス製品である。本調査では、これら製品について、ソフトウェア製品とアプライアンス製品の区分をしていないため、IDC の区分に対応付けることができない。従来これら分野ではアプライアンスの比率はそれほど高くなかったこともあり、影響は軽微と考えている。ただし、メールやウェブのフィルタリングは急速にアプライアンス製品の提供が進んでおり、今後は本調査においても必要に応じアプライアンスを分別して調査集計することが課題となる。

表 21　情報セキュリティソフトウェアに関する IDC 定義と本調査の定義の対応

IDC 調査の定義	本調査の定義	
脅威管理及びセキュアコンテンツ管理 (Threat and Secure Content Management)	ネットワーク脅威対策製品 （アプライアンスを除く）	各カテゴリとも「その他セグメントを除く
	コンテンツセキュリティ対策製品	
	暗号製品のうちデータ暗号化製品	
アイデンティティ・アクセス管理 (Identity and Access Management)	アイデンティティ･アクセス管理製品	
セキュリティ・脆弱性管理 (Security and Vulnerability Management)	システムセキュリティ管理製品	
その他セキュリティソフトウェア (Other Security Software)	暗号製品のうち暗号化モジュール 各カテゴリの「その他」セグメント	

注：IDC 社のソフトウェア製品の市場区分は概ね本調査の市場定義と対応する関係にある。従来同社の「その他セキュリティソフトウェア」の中心は暗号製品と考えられたが、データ暗号化についてはコンテンツセキュリティの一部ととらえていることが確認され、一方本調査で各カテゴリの「その他」に入れている各種製品は IDC では「その他セキュリティソフトウェア」にまとめていると見られることから、上表のように対応関係の仕訳を再整理した。

以下、日本の市場を世界市場またはその地域別市場との対比で検討することとする。

なお、ここで日本市場との比較対象とする世界市場の数字は、そのうち日本地域については IDC 社の数字を入れずに JNSA 調査の数字を代入して世界合計値を出したものである。上述のように日本市場の数字については両者間で乖離があり、ベースの違う日本の数字を含む世界の数字と本調査の日本の数字を比較することは矛盾があるからである。

9.2　世界全体の情報セキュリティ市場の概観

表 22 に、世界全体の情報セキュリティの市場規模集計データを示す。

2006 年の全世界の情報セキュリティ市場は、4 兆 4,103 億円の規模であったと試算される。2007 年以降は、2007 年：5 兆 3,306 億円、2008 年：5 兆 5,153 億円、2009 年：6 兆 1,181 億円との予測となった。

2007 年が強い市場の成長力を見せたという認識で本調査と基本的に一致する。2008 年に急速に伸び率が鈍化する点も認識は共通すると言える。が、2009 年は世界全体で 10%強の拡大をするとの予測結果となっており、本調査の結果とも、また 2009 年 3 月時点における経済情勢の観測とも一致しない。IDC の調査時点のずれが主たる要因であると推測する。

セキュリティアプライアンス、セキュリティソフトウェア、セキュリティサービスという 3 区分別に 4 年間の平均成長率を見ると、各々15.8%、8.9%、12.2%となる。セキュリティアプライアンスが最も高い成長を遂げ、次いでセキュリティサービスも比較的高い伸びを示す一方、セキュリティソフトウェアは相対的に低い伸びに留まるという結果となった。セキュリティサービスとセキュリティアプライアンスのどちらがより高い伸びを示すかは、地域により、また年によりばらつくが、各地域ともこの両者が相対的に高い伸びを示し、セキュリティソフトウェアがやや低めの伸びとなることは共通した傾向として見て取れる。

表 22　世界全体の情報セキュリティ市場規模　実績と予測

金額単位：百万円

世界 情報セキュリティ 市場規模推計	2006年 実績推計値		2007年 実績推計値			2008年 実績見込推計値			2009年 予測値		
	金額	構成比	金額	構成比	成長率	金額	構成比	成長率	金額	構成比	成長率
アプライアンス	611,589	13.9%	850,600	16.0%	39.1%	870,571	15.8%	2.3%	950,273	15.5%	9.2%
ソフトウェア	1,629,029	36.9%	1,899,878	35.6%	16.6%	1,955,447	35.5%	2.9%	2,106,680	34.4%	7.7%
ツール合計	2,240,618	50.8%	2,750,478	51.6%	22.8%	2,826,017	51.2%	2.7%	3,056,952	50.0%	8.2%
サービス	2,169,633	49.2%	2,580,146	48.4%	18.9%	2,689,244	48.8%	4.2%	3,061,120	50.0%	13.8%
情報セキュリティ合計	4,410,251	100.0%	5,330,625	100.0%	20.9%	5,515,261	100.0%	3.5%	6,118,073	100.0%	10.9%

また、セキュリティアプライアンスとセキュリティソフトウェアを合わせた情報セキュリティツール市場と情報セキュリティサービス市場の対比で見ると、サービスは 2007 年に 48.4%と前年から 0.8%ポイントその比率を落とすが、その後は徐々に比率を高めて、2009 年の予測値ではちょうど 50%と、ツール対サービスの規模は均衡する。これは、2006 年から 2007 年にかけては逆の動きを示したものの、傾向としては、情報セキュリティ対策の浸透と市場の拡大につれて、市場ニーズが専門家によるサービスをより必要とする方向に動いて行くことを示している。

一方、情報セキュリティツールをアプライアンスとソフトウェアの対比で見ると、年平均成長率は、セキュリティアプライアンスが 15.8%、ソフトウェアが 8.9%と、アプライアンスの伸びがソフトウェアの伸びをかなり上回っており、ツールにおけるソフトウェアからアプライアンスへのシフトの傾向をはっきりと示している。この結果、両者の構成比の値も、表 22 に見るように、アプライアンス対ソフトウェアの数字は、2006 年の 13.9：36.9 が、2009 年の 15.5：34.4 へと変化している。

9.3　世界情報セキュリティ市場と国内情報セキュリティ市場の全体比較

表 23 は本調査において推定した日本の情報セキュリティ市場のデータを、国際比較のために再編成したものである。世界市場と比較するために、表 20 の区分に基づいて、情報セキュリティツール市場をアプライアンスとソフトウェアに分類し直して再集計した。

アプライアンスに含まれる製品は、統合型アプライアンスのカテゴリ全てと、ネットワーク脅威対策製品カテゴリのうち、ファイアウォールアプライアンス、VPN アプライアンス、IDS／IPS アプライアンス及びアプリケーションファイアウォールの各セグメントである。なお、これ以外の数値をソフトウェアとして括っているが、コンテンツセキュリティ対策製品の中にはアンチスパムアプライアンス、URL フィルタリングアプライアンス、メールフィルタリングアプライアンスが含まれ、アイデンティティ・アクセス管理製品の中には個人認証用デバイス及び生体認証デバイスとしてハードウェアが含まれる。これらは厳密にはソフトウェアとして集計するべきでないが、現データがハードソフトの区別を得られないことと、重要性において影響が軽微と思われることから、便宜的にソフトウェアに組み込んで集計している[48]。

表 23　日本の情報セキュリティ市場規模　実績と予測

金額単位：百万円

日本（JNSA調査）情報セキュリティ市場規模推計	2006年 実績推計値		2007年 実績推計値			2008年 実績見込推計値			2009年 予測値		
	金額	構成比	金額	構成比	成長率	金額	構成比	成長率	金額	構成比	成長率
アプライアンス	49,713	8.3%	58,623	8.6%	17.9%	63,049	8.7%	7.5%	59,851	8.7%	-5.1%
ソフトウェア	242,736	40.6%	287,476	42.0%	18.4%	311,722	42.9%	8.4%	303,729	44.2%	-2.6%
ツール合計	292,449	49.0%	346,100	50.5%	18.3%	374,771	51.6%	8.3%	363,581	52.9%	-3.0%
サービス	304,748	51.0%	338,618	49.5%	11.1%	351,996	48.4%	4.0%	323,778	47.1%	-8.0%
情報セキュリティ合計	597,198	100.0%	684,717	100.0%	14.7%	726,767	100.0%	6.1%	687,359	100.0%	-5.4%

まず、日本市場のセキュリティアプライアンス、セキュリティソフトウェア、セキュリティサービスの各市場の成長率を見ると、集計対象の 4 年間における年平均成長率は、各々6.4%、7.8%、2.0%となる。最も高い成長率を示すのがソフトウェア、続いてアプライアンス、最も伸び率の低いのがサービスとなり、IDC の予測する世界市場とは伸び率順位が逆転している。

7.項、8.項で見てきたように、日本市場における情報セキュリティツールの世界では、UTM を中心にアプライアンスの需要が高まると共に、内部からの情報漏えい脅威への対策や内部統制対応から、端末での情報操作から情報を守るための端末管理、アクセス管理、暗号といったソフトウェアの需要が急速に拡大している状況がある。一方、サービス市場は構成比率の高い「セキュアシステム構築サービス」が 8.2.2 項で見たように数字としての伸びを欠く。このために、世界市場ではセキュリティサービスの伸び率がセキュリティソフトウェアを上回っているのに、国内市場ではその逆となっていると考えられる。また、特に 2009 年の予測において、日本市場は不況の影響を織り込んで、サービスの市場規模縮小が最も大きいと見ているのに対して、全体としては順調な拡大（もしくは 2008 年の減速からの回復）を予測する IDC 調査がサービスの伸び率

[48] IDC の集計においては、これらのうちアプライアンス製品はアプライアンスとして集計され、認証デバイス類はどちらにも含まれないと見られる。

を高めに見ていることも影響していると考えられる。

次に、情報セキュリティツール合計と情報セキュリティサービスの構成比を見ると、日本市場では、観測した 4 年間に、情報セキュリティツールは一貫してそのウェイトを上げ、2006 年に 49.0%だったものが 2009 年には 52.9%と 3.9%ポイント上っている。この間、表 22 に見られるように世界市場では情報セキュリティツールがその構成比率を下げている。日本においては、2008 年 4 月以降に開始する会計年度から、株式公開企業に内部統制報告制度が適用されることの影響が出ていると見られる。内部統制のための IT 統制においては、IT のセキュリティを確保することが重要になる。システムやデータへのアクセスを、権限のある者に限定すること、人の移動や業務の変更に合わせてアクセス権を IT 上で適切に変更管理すること、データの完全性と可用性を確保すること、操作や変更の履歴を記録し追跡できる状態で保全すること等が求められる。そのソリューションとしては、認証、アイデンティティ･アクセス管理、ポリシー管理、暗号化など、セキュリティソフトウェアで実現するものが多い。このために日本市場では 2006 年度以降セキュリティソフトウェアの需要が伸び、市場全体を押し上げると共に、情報セキュリティ市場の中でアプライアンスやサービスを上回る伸びを示したものと推測される。

次に、日本市場の世界市場に対するシェアの視点で見てみる。表 24 は、表 23 の数値を表 22 の数値で割って比率として示している。日本市場の 2006 年における対世界シェアは 13.5%であるが、2007 年には 12.8%に低下し、2008 年は 13.2%に回復するものの 2009 年は 11.2%に急落するとの予測結果となった。このうちソフトウェアが 2006 年に 14.9%あるものが、2007 年に 15.1%、2008 年に 15.9%と急上昇した後 2009 年には 14.4%に急落する。これは、2009 年については予測作業の実施時期により見方が大きく変わることによるので除外するとして、2007, 2008 年については上記で見た要因により、日本のソフトウェア市場が独自要因で高い伸びを見せた結果によると考えられる。

また、情報セキュリティサービスは 2007 年、2008 年、2009 年と継続的にシェアを下げている。日本市場では、セキュアシステム構築サービスが、一般的なシステムインテグレーションの一部に吸収されて表面に出にくくなる一方、世界市場ではそのような要素は考慮されず、引続き需要は拡大するとの読みの下に推計がなされている結果と推測する。

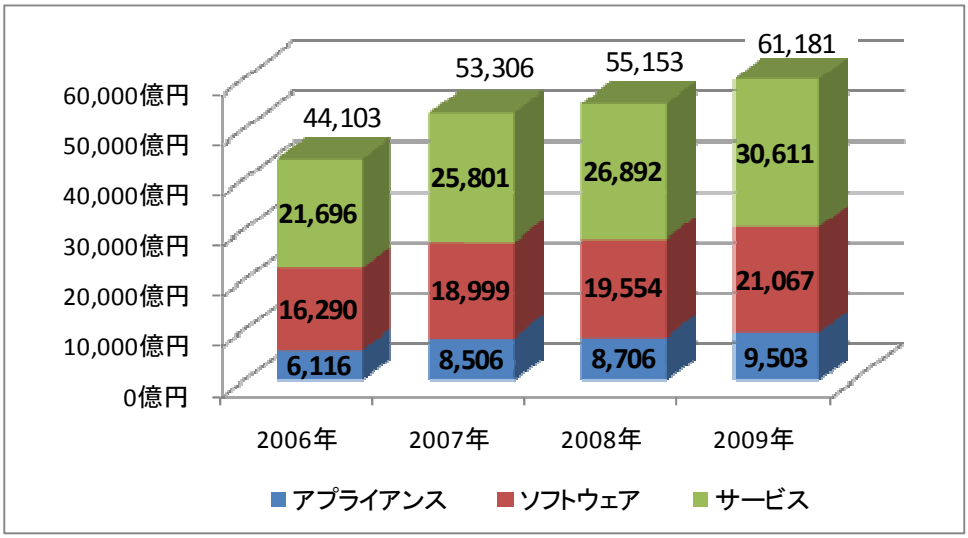
表 24　日本の情報セキュリティ市場の世界市場に対する比率

日本市場の対 世界市場シェア	2006 年	2007 年	2008 年	2009 年
アプライアンス	8.1%	6.9%	7.2%	6.3%
ソフトウェア	14.9%	15.1%	15.9%	14.4%
サービス	14.0%	13.1%	13.1%	10.6%
セキュリティ合計	13.5%	12.8%	13.2%	11.2%

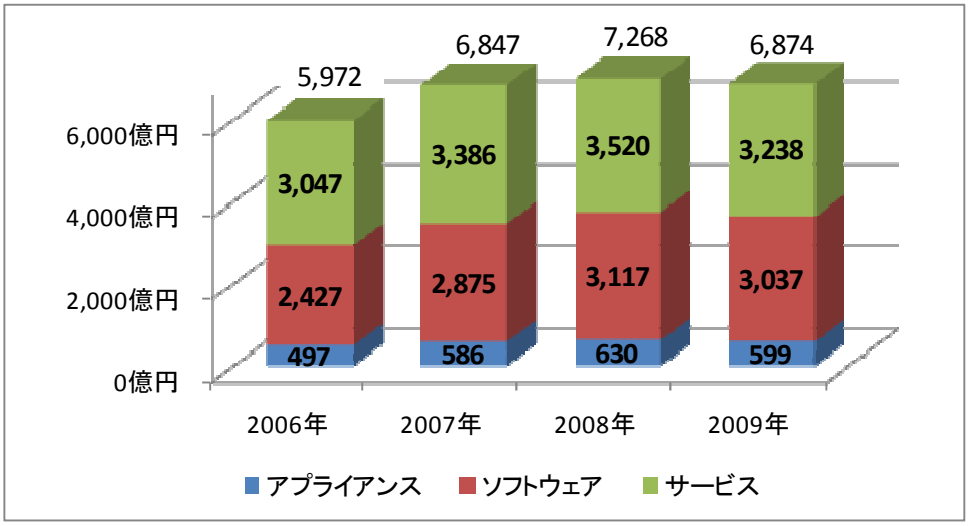
図 37 に世界と日本各々の情報セキュリティ市場規模の推移のグラフを示す。

図 37　情報セキュリティ市場、世界市場と日本市場の市場規模推移の比較

(a) 世界市場の構成と推移



(b) 日本市場の構成と推移



9.4　世界の地域別市場と日本市場の比較

この項では、世界の各地域の市場データと、本調査における日本市場のデータの比較検討を試みる。

表 25 は、今回用いたデータを、地域別･市場区分別に構成比で表したものである。全体としてみると、北アメリカが全世界の 45%から 47%を占め、圧倒的なシェアを誇っている。これに続くのが西ヨーロッパで、27%前後で推移している。次が日本で 13%前後、更にアジア太平洋の 8%弱、その他地域の 6%強となる。

表 25　地域別市場区分別構成比

地域別市場区分別シェア分布		2006年	2007年	2008年	2009年
北アメリカ	アプライアンス	45.1%	44.7%	45.3%	45.0%
	ソフトウェア	46.5%	45.3%	43.4%	43.9%
	サービス	45.8%	46.5%	46.6%	47.9%
	セキュリティ計	46.0%	45.8%	45.2%	46.1%
西ヨーロッパ	アプライアンス	24.1%	27.0%	25.6%	26.0%
	ソフトウェア	27.0%	27.1%	27.2%	27.3%
	サービス	27.2%	27.6%	27.8%	28.8%
	セキュリティ計	26.7%	27.3%	27.2%	27.9%
アジア太平洋	アプライアンス	16.8%	15.6%	16.1%	16.6%
	ソフトウェア	6.6%	7.0%	7.5%	7.9%
	サービス	6.0%	5.9%	5.6%	5.5%
	セキュリティ計	7.7%	7.8%	7.9%	8.0%
日本	アプライアンス	8.1%	6.9%	7.2%	6.3%
	ソフトウェア	14.9%	15.1%	15.9%	14.4%
	サービス	14.0%	13.1%	13.1%	10.6%
	セキュリティ計	13.5%	12.8%	13.2%	11.2%
その他	アプライアンス	5.9%	5.7%	5.8%	6.1%
	ソフトウェア	4.9%	5.4%	6.0%	6.5%
	サービス	6.9%	6.9%	7.0%	7.3%
	セキュリティ計	6.0%	6.2%	6.4%	6.8%
世界合計	アプライアンス	100.0%	100.0%	100.0%	100.0%
	ソフトウェア	100.0%	100.0%	100.0%	100.0%
	サービス	100.0%	100.0%	100.0%	100.0%
	セキュリティ計	100.0%	100.0%	100.0%	100.0%

マクロでは、ほぼ各地域の経済規模を反映していると言える。比較のために、OECD 加盟 30 ヵ国を同様の区分に分けて 2006 年の時価換算の GDP[49]を仕分けしてみると、表 26 のような分布となる。OECD には、アジア太平洋地域からは韓国、オーストラリア、ニュージーランドのみが加盟しており、その他地域に含まれる加盟国はメキシコ、トルコ、ポーランド、ハンガリー、チェコ、スロバキア、アイスランドの 7 カ国で、IDC の調査データとは差があるが、単純比較をすれば、GDP 分布に比べて北アメリカの情報セキュリティ市場シェアが高く、西ヨーロッパが低い。また OECD 統計には中国、インド、台湾、香港、ASEAN 緒国が含まれないという母集団の差から当然ながら、アジア太平洋は情報セキュリティ市場シェアが OECD ベースの GDP シェアより高くなる。日本は OECD シェアに比較すると情報セキュリティ市場のシェアは若干高い状態にあると言える。

表 26　OECD 加盟国の地域別 GDP 分布

北アメリカ	西ヨーロッパ	アジア太平洋	日本	その他
37.3%	40.7%	5.0%	10.8%	6.2%

[49] http://www.oecd.org/dataoecd/48/4/37867909.pdf

通信やネットワークインフラの差、IT の社会への浸透度の差等も情報セキュリティ市場の分布に大きく影響を与えるものと考えられるが、北アメリカが IT 先進地域でネットワークに深く依存した社会構造になっていることと、国家安全保障に直結する情報セキュリティとの認識から、官民とも手厚い対策を打っていることの反映と考えられる。

9.4.1 北アメリカ市場と日本市場

表 27 に、北アメリカ市場の市場規模データを示す。

北アメリカのアプライアンス、ソフトウェア、サービスの構成比は、全世界合計のそれ（表 22 参照）と非常に似たものとなっている。アメリカ経済のサービス化の進展から、サービスの比率が世界平均より高めになることが想定されるが、集計結果も 2006 年度を除いてそのような結果になっている。市場の成長率も、世界全体と似た動きを示す。調査対象の 4 年間の年平均成長率で見ると、世界全体が 11.5%、北アメリカ市場は 11.6%と、ほぼ同率である。アプライアンスは世界全体：15.8%、北アメリカ：15.7%と似た動きとなっているが、ソフトウェアの市場は世界全体：8.9%、北アメリカ：6.9%と北アメリカ市場の伸び率が低く、逆にサービス市場は世界全体：12.2%、北アメリカ：13.8%と北アメリカの伸び率が高くなっている。

表 27 アメリカの情報セキュリティ市場推計

金額単位：百万円

北アメリカ 情報セキュリティ 市場規模推計	2006年 実績推計値		2007年 実績推計値			2008年 実績見込推計値			2009年 予測値		
	金額	構成比	金額	構成比	成長率	金額	構成比	成長率	金額	構成比	成長率
アプライアンス	275,904	13.6%	380,634	15.6%	38.0%	394,429	15.8%	3.6%	427,687	15.2%	8.4%
ソフトウェア	758,107	37.4%	861,470	35.3%	13.6%	848,521	34.0%	−1.5%	924,921	32.8%	9.0%
ツール合計	1,034,011	51.0%	1,242,104	50.9%	20.1%	1,242,951	49.8%	0.1%	1,352,608	48.0%	8.8%
サービス	993,925	49.0%	1,200,134	49.1%	20.7%	1,252,168	50.2%	4.3%	1,465,867	52.0%	17.1%
情報セキュリティ合計	2,027,935	100.0%	2,442,238	100.0%	20.4%	2,495,119	100.0%	2.2%	2,818,475	100.0%	13.0%

SaaS、クラウドなど、IT の新しい動きは引き続きアメリカ主導の様相が強く、情報セキュリティ市場においてもその傾向を反映した動きとなっていると考えられる。

一方、日本市場は表 23 で見たように、足元で 51.0%のウェイトを占めるサービスが徐々にその比率を下げ、2009 年度予測では 47.1%まで低下するとの結果になった。2006～2009 年のセキュリティサービスの平均伸び率が、北アメリカでは 13.8%あるのに対し、日本は 2.0%に留まることからこのような彼我の逆方向展開となっている。ここには上述のように 2009 年度の予測時点の差による見方の差も反映しているが、市場の伸び率で両市場を比較すると 2007 年の北アメリカ市場でのサービスの伸び率の高さと 2008 年の日本市場でのツールの伸び率の高さという好対照の現象があり、そのことによる要素も大きいと考えられる。

9.4.2 西ヨーロッパ市場と日本市場

表 28 に、西ヨーロッパ市場の市場規模データを示す。

西ヨーロッパ市場は、サービス化とアプライアンス化の同時進行という現象が見て取れる。観測期間において、サービスの構成比は 50.1%から 51.7%へと高まって北アメリカ市場におけるサービスの構成比に近い構成比にまで達する。アプライアンスも 2006 年の 12.5%が 2009 年には 14.5%までシェアを上げる。その分、セキュリティソフトウェアはその構成比を下げる予測とな

っている。

表 28　西ヨーロッパの情報セキュリティ市場推計

金額単位:百万円

西ヨーロッパ 情報セキュリティ 市場規模推計	2006年 実績推計値		2007年 実績推計値			2008年 実績見込推計値			2009年 予測値		
	金額	構成比	金額	構成比	成長率	金額	構成比	成長率	金額	構成比	成長率
アプライアンス	147,169	12.5%	230,075	15.8%	56.3%	222,882	14.8%	−3.1%	246,977	14.5%	10.8%
ソフトウェア	439,994	37.4%	514,647	35.3%	17.0%	532,138	35.4%	3.4%	576,121	33.8%	8.3%
ツール合計	587,164	49.9%	744,723	51.1%	26.8%	755,020	50.3%	1.4%	823,098	48.3%	9.0%
サービス	590,613	50.1%	711,718	48.9%	20.5%	747,126	49.7%	5.0%	880,944	51.7%	17.9%
情報セキュリティ合計	1,177,776	100.0%	1,456,440	100.0%	23.7%	1,502,146	100.0%	3.1%	1,704,042	100.0%	13.4%

西ヨーロッパ市場の伸び率が、他のどの地域よりも高いことも注目すべき点である。世界全体の 2006～2009 年の年平均成長率が、アプライアンス、ソフトウェア、サービス、セキュリティ合計各々15.8%、8.9%、12.2%、11.5%であるのに対し、西ヨーロッパ市場は同じ順に 18.8%、9.4%、14.3%、13.1%といずれも世界全体市場を上回っている。特にアプライアンス市場の成長率が他の地域と比較しても突出した高い成長率を示している。

ツールにおけるアプライアンス化と、ツール対サービスの比較におけるサービス化の傾向は世界の趨勢であると言え、西ヨーロッパもその方向で市場が動いて行くものと見られる。特に 2007 年にアプライアンスが前年比 56.3%増と極めて高い伸びを示している。2006 年度の西ヨーロッパ市場のアプライアンスの構成比が 12.5%と、北アメリカや世界全体に比して低かったものが、2007 年に一気にほぼ同等の構成比にまで上がっている。2007 年には、この地域に一律の導入機運が高まったものと見られる。

日本の場合は、情報漏えい対策や内部統制対応でコンサルティングや SI 的サービスなどサービス需要が増加していたのが、今回の予測期間ではその伸び率が相対的に緩やかになる一方、IT 統制に対応するツールの適用が進展するために、ソフトウェアの伸びが高くなっているものと見られる。

9.4.3　アジア太平洋地域市場と日本市場

表 29 に、アジア太平洋地域市場（日本を除く）の市場規模データを示す。

アジア太平洋地域には中国・韓国を含むアジア全域（中東地域は含まない）と大洋州を含んでいる。地域の括りという意味では日本も含めるべきだが、日本の規模がそれ以外のアジア太平洋地域の全体より大きな市場を形成している状態では、日本市場の数値の影響で、その特徴が埋没する可能性があることから、日本を除くベースのものを日本市場及び他の地域と比較することとする。

他の地域と同様に、まずセキュリティサービスの構成比を見てみると、34%～38%と、世界全体及び他の地域に比べて極端にその比率が小さいことが一目瞭然に見て取れる。含まれる国や地域は多種多様で、地域として共通の文化や経済の要因を挙げることは困難である。それでも、全体としてその経済発展段階から考えると、情報セキュリティ市場も成熟化の要素が最も少ない地域と言えると思われ、それがセキュリティサービスの構成比を低くしていると分析できると考える。

表 29　アジア太平洋地域の情報セキュリティ市場推計

金額単位:百万円

アジア太平洋(除日本) 情報セキュリティ 市場規模推計	2006年 実績推計値		2007年 実績推計値			2008年 実績見込推計値			2009年 予測値		
	金額	構成比	金額	構成比	成長率	金額	構成比	成長率	金額	構成比	成長率
アプライアンス	102,778	30.1%	132,619	31.8%	29.0%	139,795	32.1%	5.4%	157,420	32.1%	12.6%
ソフトウェア	107,957	31.6%	133,228	31.9%	23.4%	145,772	33.4%	9.4%	165,596	33.7%	13.6%
ツール合計	210,735	61.7%	265,847	63.7%	26.2%	285,567	65.5%	7.4%	323,016	65.8%	13.1%
サービス	130,992	38.3%	151,345	36.3%	15.5%	150,508	34.5%	−0.6%	168,140	34.2%	11.7%
情報セキュリティ合計	341,727	100.0%	417,191	100.0%	22.1%	436,075	100.0%	4.5%	491,157	100.0%	12.6%

もう一つ特徴的なこととして、セキュリティアプライアンスの占める比率が高いことが挙げられる。推計対象年の 2006 年から 2009 年の間で、情報セキュリティ市場全体に対する構成比は約 30%から 32%で推移しており、世界全体の 13.9%～16.0%とは倍以上の開きがある。この地域でアプライアンスが高いウェイトを占める特定の要因があると考えられる。

第一の要因としては、アプライアンスが持つ、導入の容易さ、スループット等性能の良さ、コストパフォーマンスの良さ等の特性が挙げられる。初めてネットワーク脅威対策製品を導入しようとする時にこの特性は魅力的であると言える。また、セキュリティ対策の第一歩として、ネットワーク脅威対策製品やウイルス対策製品の導入から始めるということからも、アプライアンスの比率が高まる可能性がある。日本や欧米の、比較的早期にネットワーク脅威対策を導入した地域は、その導入が盛んだった 1990 年代後半にはアプライアンス型製品の供給が盛んでなかったことから、ソフトウェア製品の導入による対策が実施され、既に製品の導入が一巡している面も考えられる。

更に、アプライアンスの場合は、不具合等の発生に際してサポート・メンテナンスが容易である点も挙げられる。地域が広く経済密度が薄い場合には、地域経済単位では、販売事業者が高度のサポート力を備えるだけの規模の経済が働かない。その結果、サポート技術への投資を最小限に抑えられるアプライアンスを選好する可能性が高くなる。アプライアンスの場合は障害が発生したら代替品との交換で対応することが多く、分析や修理の技術を余り必要としないからである。

9.5　分野別・地域別分布の全体像分析

図 38 に、2007 年の分野別地域別並びに地域別分野別の世界市場の構成比をグラフ化したものを示した。

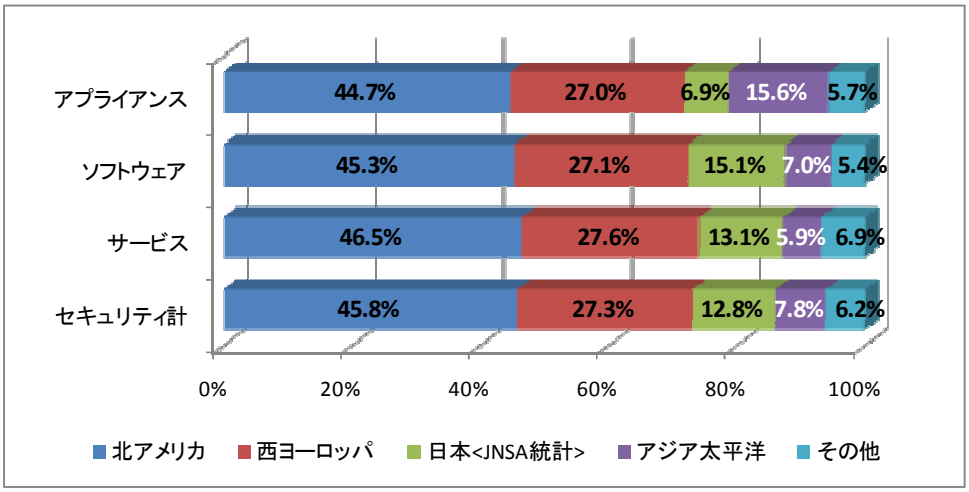
大括りで見ると、北アメリカが、セキュリティ合計で世界の 45.8%を占めて圧倒的に大きな市場を形成している。これに次ぐのが西ヨーロッパで、27.3%と世界の 4 分の 1 強を占める。日本がこれに続き 12.8%と世界の 8 分の 1 を占める。アジア太平洋地域は 7.8%と、日本の 3 分の 2 弱のマーケットと言える。その他地域は 6.2%と、アジア太平洋地域の規模に近づいてきている。

地域ごとの特徴としては、アジア太平洋地区におけるアプライアンスの構成比の突出した高さが挙げられる。これとの対照において、日本は 8.6%と逆に極端に低い構成比となっている。日本においても、中小事業所において低価格タイプの統合型アプライアンスが浸透するなど、アプライアンス化の方向は明確に見えるものの、他地域に比較してその移行の度は必ずしも高くないと言わざるを得ない。統計的に、日本市場にはメールフィルタリング等のいくつかのアプライアン

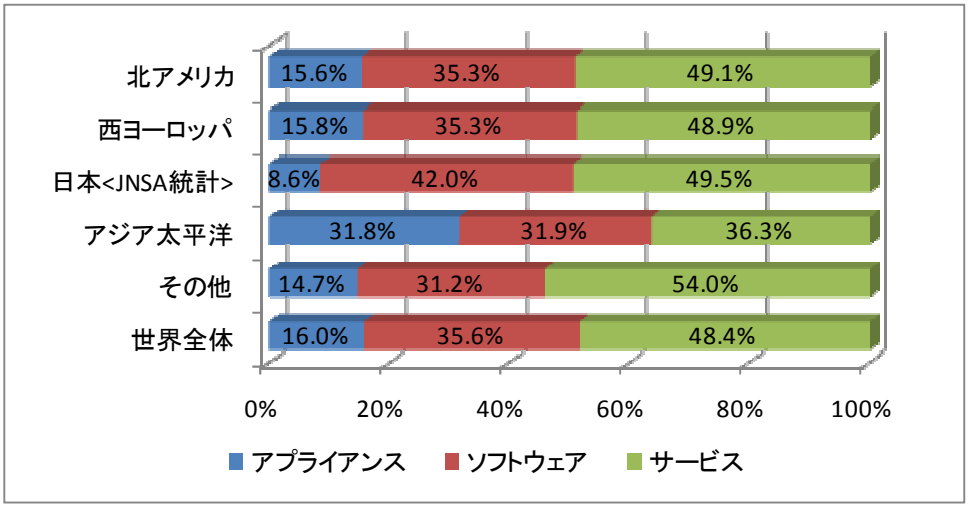
ス製品を含まないことも、若干影響している可能性がある。

図 38　情報セキュリティ市場、世界市場と日本市場の構成比推移の比較

(a) 2007 年情報セキュリティ市場分野別地域別構成比



(b) 2006 年情報セキュリティ市場地域別分野別構成比



主としてアプライアンス、ソフトウェア、サービスの構成比率の面から比較してみると、上にも見たように、アジア太平洋市場がその構成比で各市場が概ね 3 分の 1 ずつになっているのに対し、他の地域はサービスが約半分を占めるという違いが見える。そしてツールの内訳では、アプライアンス対ソフトウェアが北アメリカと西ヨーロッパで概ね 15%対 35%となっているのに対し、日本はアプライアンスが約 9%弱、ソフトウェアが約 42%前後とソフトウェア比率が高い。統計区分の差の要素も多少影響していると考えられるが、地域別にかなりはっきりと構造的な差があることを示すものとして興味深い。

9.6　セキュリティソフトウェアのカテゴリ別・地域別比較分析

セキュリティソフトウェアについては、大分類レベルで比較可能な地域別データが得られたので、日本市場と世界各地域のセキュリティソフトウェアの種類別比較を試みる。表 30 に、地域別・カテゴリ（市場大分類）別の市場規模推計値の一覧を、また表 31 に、表 30 の世界合計を100%としたときの各市場のシェア分布を示す。このうち日本市場については本調査の数字であり、その他は IDC 社の提供数字を元に整理したものである。また、市場区分定義の対応関係は表 21 に示した通りである。

表 30　世界のセキュリティソフトウェア地域別市場規模　実績と予測

金額単位：百万円

セキュリティソフトウェア 地域別カテゴリ別 市場規模推計		2006年 実績推計値		2007年 実績推計値			2008年 実績見込推計値			2009年 予測値		
		金額	構成比	金額	構成比	成長率	金額	構成比	成長率	金額	構成比	成長率
北アメリカ	セキュアコンテンツ・脅威管理	430,867	56.8%	498,601	57.9%	15.7%	484,822	57.1%	−2.8%	516,336	55.8%	6.5%
	アイデンティティ・アクセス管理	160,794	21.2%	162,298	18.8%	0.9%	153,892	18.1%	−5.2%	163,553	17.7%	6.3%
	セキュリティ・脆弱性管理	132,873	17.5%	158,410	18.4%	19.2%	166,292	19.6%	5.0%	195,722	21.2%	17.7%
	その他セキュリティソフトウェア	33,574	4.4%	42,161	4.9%	25.6%	43,515	5.1%	3.2%	49,310	5.3%	13.3%
	ソフトウェア合計	758,107	100.0%	861,470	100.0%	13.6%	848,521	100.0%	−1.5%	924,921	100.0%	9.0%
西ヨーロッパ	セキュアコンテンツ・脅威管理	268,323	61.0%	307,143	59.7%	14.5%	313,836	59.0%	2.2%	335,619	58.3%	6.9%
	アイデンティティ・アクセス管理	102,078	23.2%	121,024	23.5%	18.6%	126,054	23.7%	4.2%	136,611	23.7%	8.4%
	セキュリティ・脆弱性管理	56,166	12.8%	71,326	13.9%	27.0%	76,983	14.5%	7.9%	87,632	15.2%	13.8%
	その他セキュリティソフトウェア	13,427	3.1%	15,154	2.9%	12.9%	15,265	2.9%	0.7%	16,259	2.8%	6.5%
	ソフトウェア合計	439,994	100.0%	514,647	100.0%	17.0%	532,138	100.0%	3.4%	576,121	100.0%	8.3%
アジア太平洋	セキュアコンテンツ・脅威管理	74,350	68.9%	92,912	69.7%	25.0%	102,533	70.3%	10.4%	117,443	70.9%	14.5%
	アイデンティティ・アクセス管理	22,855	21.2%	27,665	20.8%	21.0%	29,860	20.5%	7.9%	33,685	20.3%	12.8%
	セキュリティ・脆弱性管理	7,418	6.9%	8,755	6.6%	18.0%	9,246	6.3%	5.6%	10,125	6.1%	9.5%
	その他セキュリティソフトウェア	3,333	3.1%	3,896	2.9%	16.9%	4,133	2.8%	6.1%	4,342	2.6%	5.1%
	ソフトウェア合計	107,957	100.0%	133,228	100.0%	23.4%	145,772	100.0%	9.4%	165,596	100.0%	13.6%
日本	セキュアコンテンツ・脅威管理	141,730	58.4%	163,050	56.7%	15.0%	175,221	56.2%	7.5%	170,987	56.3%	−2.4%
	アイデンティティ・アクセス管理	43,791	18.0%	55,235	19.2%	26.1%	59,254	19.0%	7.3%	56,771	18.7%	−4.2%
	セキュリティ・脆弱性管理	31,682	13.1%	38,907	13.5%	22.8%	43,723	14.0%	12.4%	43,728	14.4%	0.0%
	その他セキュリティソフトウェア	25,534	10.5%	30,285	10.5%	18.6%	33,525	10.8%	10.7%	32,243	10.6%	−3.8%
	ソフトウェア合計	242,736	100.0%	287,476	100.0%	18.4%	311,722	100.0%	8.4%	303,729	100.0%	−2.6%
その他	セキュアコンテンツ・脅威管理	54,502	67.9%	68,884	66.8%	26.4%	79,304	67.6%	15.1%	91,540	67.2%	15.4%
	アイデンティティ・アクセス管理	16,503	20.6%	23,196	22.5%	40.6%	25,718	21.9%	10.9%	30,153	22.1%	17.2%
	セキュリティ・脆弱性管理	7,034	8.8%	8,214	8.0%	16.8%	9,179	7.8%	11.7%	11,039	8.1%	20.3%
	その他セキュリティソフトウェア	2,196	2.7%	2,762	2.7%	25.8%	3,093	2.6%	12.0%	3,580	2.6%	15.8%
	ソフトウェア合計	80,234	100.0%	103,057	100.0%	28.4%	117,293	100.0%	13.8%	136,313	100.0%	16.2%
世界合計	セキュアコンテンツ・脅威管理	969,771	59.5%	1,130,591	59.5%	16.6%	1,155,716	59.1%	2.2%	1,231,924	58.5%	6.6%
	アイデンティティ・アクセス管理	346,021	21.2%	389,417	20.5%	12.5%	394,778	20.2%	1.4%	420,773	20.0%	6.6%
	セキュリティ・脆弱性管理	235,173	14.4%	285,612	15.0%	21.4%	305,422	15.6%	6.9%	348,247	16.5%	14.0%
	その他セキュリティソフトウェア	78,063	4.8%	94,258	5.0%	20.7%	99,531	5.1%	5.6%	105,736	5.0%	6.2%
	ソフトウェア合計	1,629,029	100.0%	1,899,878	100.0%	16.6%	1,955,447	100.0%	2.9%	2,106,680	100.0%	7.7%

9.6.1　北アメリカ市場と日本市場の比較

北アメリカ市場は、上に見たように情報セキュリティ市場全体でも世界の 45%程度を占めているが、セキュリティソフトウェアにおいてもその合計は表 31 に見られるように世界の 45%程度を占めていることがわかる。このうち、2007 年を基準として見ると、「セキュリティ・脆弱性管理」が約 56%と突出して高いシェアを示し、「アイデンティティ・アクセス管理」が約 42%とやや低いシェアにとどまっている。経年変化としては、2009 年にかけて「セキュリティ・脆弱性管理」と「その他セキュリティソフトウェア」がシェアを上げるのに対し、「セキュアコンテンツ・脅威管理」と「アイデンティティ・アクセス管理」がシェアを下げる推移をたどる。

日本と北アメリカ市場の規模の比較においては、2007 年において北アメリカ市場は日本の約

3.6 倍の規模となっている。OECD 統計における 2007 年の GDP で比較すると、アメリカとカナダの合計は日本の約 3.6 倍となっており、対 GDP 比では、日本と北アメリカの情報セキュリティ市場の規模はほとんど同レベルと見ることができる。

表 31　世界のセキュリティソフトウェア地域別市場シェア　実績と予測

地域別ソフトウェアカテゴリ別シェア分布		2006年	2007年	2008年	2009年
北アメリカ	セキュアコンテンツ・脅威管理	44.4%	44.1%	41.9%	41.9%
	アイデンティティ・アクセス管理	46.5%	41.7%	39.0%	38.9%
	セキュリティ・脆弱性管理	56.5%	55.5%	54.4%	56.2%
	その他セキュリティソフトウェア	43.0%	44.7%	43.7%	46.6%
	ソフトウェア合計	46.5%	45.3%	43.4%	43.9%
西ヨーロッパ	セキュアコンテンツ・脅威管理	27.7%	27.2%	27.2%	27.2%
	アイデンティティ・アクセス管理	29.5%	31.1%	31.9%	32.5%
	セキュリティ・脆弱性管理	23.9%	25.0%	25.2%	25.2%
	その他セキュリティソフトウェア	17.2%	16.1%	15.3%	15.4%
	ソフトウェア合計	27.0%	27.1%	27.2%	27.3%
アジア太平洋	セキュアコンテンツ・脅威管理	7.7%	8.2%	8.9%	9.5%
	アイデンティティ・アクセス管理	6.6%	7.1%	7.6%	8.0%
	セキュリティ・脆弱性管理	3.2%	3.1%	3.0%	2.9%
	その他セキュリティソフトウェア	4.3%	4.1%	4.2%	4.1%
	ソフトウェア合計	6.6%	7.0%	7.5%	7.9%
日本（JNSA統計）	セキュアコンテンツ・脅威管理	14.6%	14.4%	15.2%	13.9%
	アイデンティティ・アクセス管理	12.7%	14.2%	15.0%	13.5%
	セキュリティ・脆弱性管理	13.5%	13.6%	14.3%	12.6%
	その他セキュリティソフトウェア	32.7%	32.1%	33.7%	30.5%
	ソフトウェア合計	14.9%	15.1%	15.9%	14.4%
その他	セキュアコンテンツ・脅威管理	5.6%	6.1%	6.9%	7.4%
	アイデンティティ・アクセス管理	4.8%	6.0%	6.5%	7.2%
	セキュリティ・脆弱性管理	3.0%	2.9%	3.0%	3.2%
	その他セキュリティソフトウェア	2.8%	2.9%	3.1%	3.4%
	ソフトウェア合計	4.9%	5.4%	6.0%	6.5%
世界合計	セキュアコンテンツ・脅威管理	100.0%	100.0%	100.0%	100.0%
	アイデンティティ・アクセス管理	100.0%	100.0%	100.0%	100.0%
	セキュリティ・脆弱性管理	100.0%	100.0%	100.0%	100.0%
	その他セキュリティソフトウェア	100.0%	100.0%	100.0%	100.0%
	ソフトウェア合計	100.0%	100.0%	100.0%	100.0%

9.6.2　西ヨーロッパ市場と日本市場の比較

西ヨーロッパ市場は、世界市場の概ね 27%程度を占めている。日本市場の 2 倍弱の規模とシェアである。その特徴的な点は、「アイデンティティ・アクセス管理」の構成比が世界合計や他の地域に比べて高く、逆に「セキュリティ・脆弱性管理」がわずかではあるが低い点にある。「その他キュリティソフトウェア」もやや低い。ソフトウェア合計では、4 年間の年平均成長率は 9.4%で、

世界全体の 8.9%、日本市場の 7.8%よりも高い成長が見込まれている。ただし、アプライアンスは同 18.8%と突出して高い成長率が見込まれており、市場全体が拡大する中でアプライアンスへのシフトが進むことを見込んでいるものと解釈される。

もう一つの特徴点は、暗号モジュールやフォレンジック系ソフトウェアが主体の「その他」のシェアが、他のカテゴリに比べて著しく低いことである。アジア太平洋地区でも同様の傾向が見られるが、「セキュリティ・脆弱性管理」の比率が低いことと合わせ、外部脅威への備えに対する関心が高い一方、内部からの漏えい対策や資産保全に対する意識が熟していないことを示唆している可能性がある。

逆に日本市場は、セキュリティソフトウェア合計では世界市場の 15%程度にも拘らず、「その他キュリティソフトウェア」は倍以上の 32%前後のシェアがある。2007 年時点の地域ごとのソフトウェア種類別構成比で見ると、北アメリカ 4.9%、西ヨーロッパ 2.9%、アジア太平洋 2.9%、世界合計 5.0%であるのに対し、日本は 10.5%を占める。IDC 統計と本統計では、厳密な市場区分定義はずれがある可能性があるため、比較は困難ながら、日本市場ではデジタル複合機やゲーム機向けに需要の高い暗号モジュール等が含まれており、これら機器は日本の世界シェアも高いため、この部分で日本市場が突出している可能性がある。

9.6.3 アジア太平洋市場と日本市場の比較

アジア太平洋市場は、セキュリティソフトウェア合計の対世界市場シェアを比較対象の 4 年間に徐々に高め、2006 年の 6.6%から 2009 年には 7.9%に達するものと予測されている。情報セキュリティ市場全体では、4 年間平均で世界全体の伸び率が 11.6%であるのに対してアジア太平洋は 12.9%と、やや高い程度の成長率であるが、ソフトウェアは同じく 15.3%と高い伸び率（世界市場は 8.9%）を示す。アプライアンスも同じく 15.3%と高い伸びを示し、セキュリティツールの普及が進むことを示している。

ソフトウェアの種類別では、「セキュアコンテンツ・脅威管理」の構成比率が高く、「セキュリティ・脆弱性管理」や「その他セキュリティソフトウェア」が低い。「アイデンティティ・アクセス管理」はほぼ世界市場の構成比並みである。外部脅威対策のウェイトが高まり、認証系は世界全体並みの成長を続ける一方、システム内部の脆弱性やログ管理といった内部管理面は他地域ほど重視されない傾向と読み取ることができる。

9.6.4 他地域との比較で見た日本のセキュリティソフトウェア市場

日本のセキュリティソフトウェア市場は、2007 年度の前年度比成長率で見ると、その他地域を除けばアジア太平洋地域の 23.4%に次ぐ 18.4%という高い成長率を示した。2008 年も同様に、アジア太平洋地域の 9.4%に次ぐ 8.4%と、アジア太平洋地域に比べれば市場の成熟度が進んでいると思われる割に、市場の拡大が続いたと見られる。これは今まで見てきたように、内部統制対応という日本固有の事情が作用した結果と推測できる。

2006 年から 2009 年までの 4 年間のソフトウェアの平均成長率で見ると、北アメリカ：6.9%、

西ヨーロッパ：9.4%、アジア太平洋：15.3%、日本：8.3%、世界全体：8.9%と、北アメリカ市場が最も低く、次いで日本市場という順番になる。北アメリカ市場は「セキュリティ・脆弱性管理」と「その他セキュリティソフトウェア」が各々13.8%、13.7%と高い伸びを見せる一方、「アイデンティティ・アクセス管理」は0.6%とほぼ横ばいにとどまり、これが全体として低い伸び率につながっている。一方、日本市場は「セキュリティ・脆弱性管理」「その他セキュリティソフトウェア」「アイデンティティ・アクセス管理」が各々11.3%、9.9%、9.3%と牽引役になる一方、「セキュアコンテンツ・脅威管理」は6.6%と低めの伸びであり、内部管理面での強化が優先されていることが読み取れる。

図 38 に見られるように、北アメリカ、西ヨーロッパ、日本の市場の構成比はかなり似通った形になってきている。特に、前回調査に比べてサービスの比率が高まった西ヨーロッパは北アメリカと非常に似た構成比となり、アプライアンスが低くソフトウェアが高いという日本の情報セキュリティ市場の構造は、両者とやや開きが生じた感がある。一方、表 25 と 26 の比較から、2006 年時点では、対 GDP 構成比で比較した時に、GDP の世界シェアより低い情報セキュリティ市場シェアを示すのは西ヨーロッパだけという結果となっている。アジア太平洋については、OECD 統計に中国もインドも含まれないことが情報セキュリティシェア＞GDP シェアの要因になっていると考えられるのでこれを除く（その他地域も除外）と、日本はアメリカに次いで市場の成熟度が進み、西ヨーロッパは市場の構成比では成熟が進みつつも、GDP との比較ではまだ市場の潜在成長余力がある可能性がある。

10. 情報セキュリティユーザ動向との対応分析

この項では、本調査において推計した国内情報セキュリティ市場規模及びその動向を、ユーザサイドの動向分析及びデータとの対応関係において分析することを試みる。

ユーザサイドの動向データについては、経済産業省が毎年実施している情報処理実態調査を用い、2008 年 7 月 14 日に公表された「平成 19 年情報処理実態調査結果報告書」によった。この調査の対象年度は 2006 年度であり、本調査の対象期間の最初の年と合致する。従い、本調査の 2006 年度の姿を基本として比較を行うが、情報処理実態調査が対前年比較での記述が多いのに対して、本調査では 2006 年の対前年比較は得られないので、その意味での制限がある。必要に応じ、本調査の平成 19 年度版の数字も援用しつつ分析を試みることとする。

10.1 平成 19 年情報処理実態調査結果報告書の要点

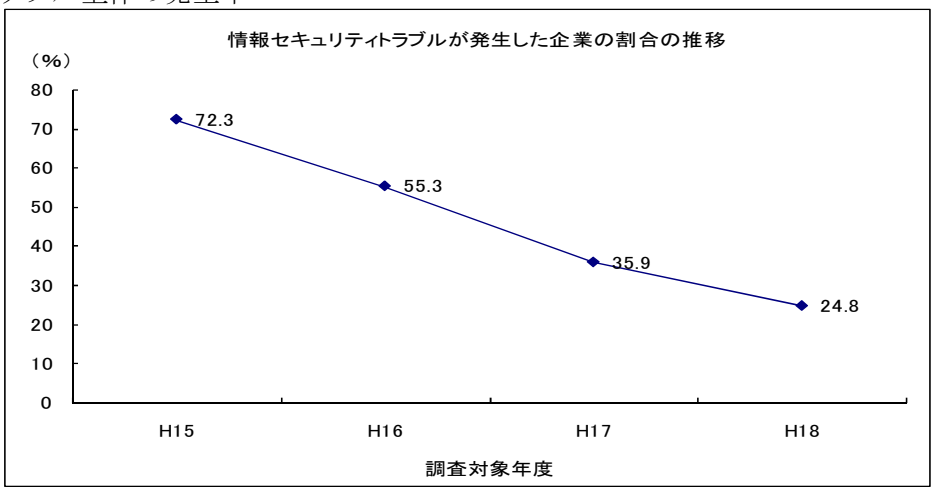
以下、本項における記述並びに図表の出典は特に断らない限り経済産業省 2008 年 7 月 14 日発表[50]「平成 19 年情報処理実態調査結果報告書の概要」及び「平成 19 年情報処理実態調査結果報告書」による。

10.1.1. トラブルの発生状況

2006 年度の回答企業におけるトラブルの発生率は 24.8%で、3 年連続の低下となった。トラブルの発生要因（複数回答）のうち、最も高い比率を占めるのが「コンピュータウィルス[51]」であり、この要因の減少が全体の減少に結びついていると思われる。（図 39）

図 39 情報セキュリティトラブルの発生状況（平成 19 年情報処理実態調査）

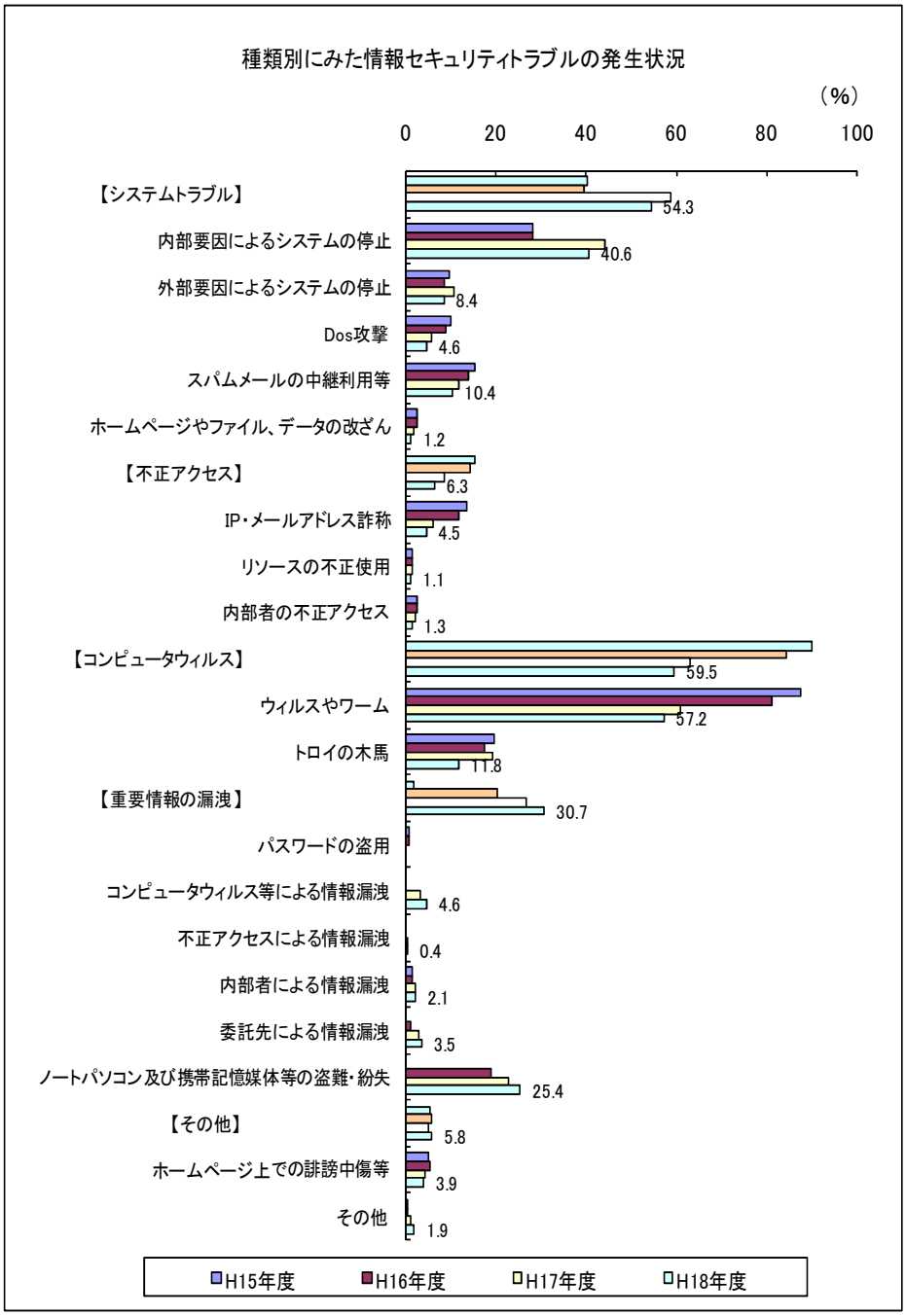
①トラブル全体の発生率



50 http://www.meti.go.jp/press/20080714001/20080714001.html

51 本調査報告では用字として「ウイルス」を使うが引用部分は原文のまま「ウィルス」とした。以下同じ。

②トラブルの種類別



（注）
1.情報セキュリティトラブルが発生したと回答した企業の割合の推移と、情報セキュリティトラブルが発生した企業において当該種類のトラブルが発生したと回答した企業の割合の推移。
2.回答企業数は、情報セキュリティトラブルの発生状況に関する設問が 4,215 社、種類別情報セキュリティトラブルの発生状況に関する設問（複数回答可）が 1,037 社。

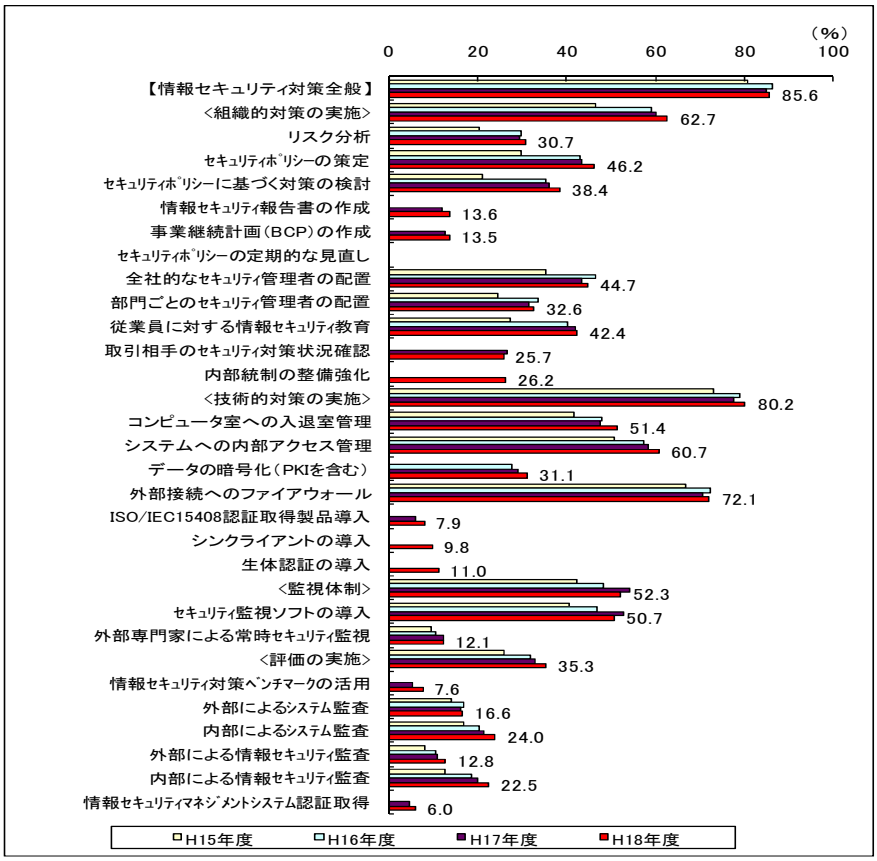
一方、「重要情報の漏えい」は2006年度で30.7%を占め、かつ年を追って増加する傾向にある。情報漏えいの原因としては、「ノートパソコン及び携帯記憶媒体等の盗難・紛失」がほとんどを占

め、かつ増加傾向にある。以下、同報告書の記述を引用すると「トラブルのカテゴリー[52]別にみると、発生率の低下幅が最も大きかったカテゴリーは『システムトラブル』で、次に『コンピュータウィルス』が続いた。一方、『重要情報の漏えい』や『その他』の発生率は前年度より上昇し、特に『重要情報の漏えい』は３年連続の上昇となった。内訳をみると、低下幅が大きいトラブルの種類は『トロイの木馬』、『ウィルスなどの感染』で、反対に上昇幅が大きいトラブルの種類は『ノートパソコン及び携帯記憶媒体等の盗難・紛失』、『コンピュータウィルス等による情報漏えい』であった。」

10.1.2. 対策状況

対策状況については、「既に実施している」と回答した企業の割合が前年度比若干上昇して2006年度には85.6%に達しており、同調査は「情報セキュリティ対策の実施状況については、実施率が上昇したものの依然として技術的対策が中心であることや、規模の小さい企業において対策の実施が遅れ気味であることがうかがわれる。」としている。対策の内容については、同調査では次のように記述している。(図 40)

図 40 各情報セキュリティ対策について実施している企業の割合の推移（平成 19 年情報処理実態調査）



[52] 本調査報告では用字として「カテゴリ」を使うが引用部分は原文のまま「カテゴリー」とした。「ウイルス」についても同様に、原文のまま「ウィルス」とした。以下同じ。

（注）
1.情報セキュリティ対策の実施状況について「既に実施している」と回答した企業の割合の推移。
2.情報セキュリティ対策全般の実施率は、いずれかのセキュリティ対策の実施状況について回答した企業数に対する、いずれかのセキュリティ対策について「既に実施している」と回答した企業数により計算。
3.各カテゴリーの実施率は、それぞれのカテゴリーに属するいずれかのセキュリティ対策の実施状況について回答した企業数に対する、同カテゴリーに属するいずれかのセキュリティ対策について「既に実施している」と回答した企業数の割合により計算。
4.回答企業数は、概表5-2-1-1 参照。

「カテゴリー別に実施率をみると、『技術的対策』が 80.2%、『組織的対策』が 62.7%、『監視体制』が 52.3%、『評価の実施』が 35.3%となり、『監視体制』を除きいずれも前年度より上昇したが、『技術的対策』の実施率が突出して高い傾向は変わらなかった。

これを対策の種類ごとにみると、『外部接続へのファイアウォールの配置』や『重要なシステムへの内部でのアクセス管理』、『重要なコンピュータ室への入退室管理』における実施率が高く、いずれも 50%を上回った。また前年度と比較すると、ほとんどの対策で実施率が上昇し、なかでも『重要なコンピュータ室への入退室管理』、『セキュリティポリシーの策定』、『内部によるシステム監査』の上昇幅が大きかった。」

ここでいう「対策のカテゴリー」とは、同調査では次のように定義されている。

「情報セキュリティ対策のカテゴリーとして、以下の４つを提示している。

組織的対策の実施：リスク分析、セキュリティポリシーの策定、セキュリティポリシーに基づく対策の実施、情報セキュリティ報告書の作成、事業継続計画の作成、全社的なセキュリティ管理者の配置、部門ごとのセキュリティ管理者の配置、従業員に対する情報セキュリティ教育、取引相手における情報セキュリティ対策実施状況の確認、内部統制の整備強化

技術的対策の実施：重要なコンピュータ室への入退出管理、重要なシステムへの内部でのアクセス管理、データの暗号化、外部接続へのファイアウォールの配置、ISO/IEC15408 認証取得製品の導入、シンクライアントの導入、生体認証の導入

監視体制　：　セキュリティ監視ソフトの導入、外部専門家による常時セキュリティ監視

評価の実施　：　情報セキュリティ対策ベンチマークの活用、外部専門家による定期的なシステム監査、内部による定期的なシステム監査、外部専門家による定期的な情報セキュリティ監査、内部による定期的な情報セキュリティ監査、情報セキュリティマネジメントシステム認証の取得」

10.1.3.　対策効果

情報セキュリティ対策の効果として、情報セキュリティ向上への寄与の状況を聞く質問に対しては、88.3%が「寄与した」と回答しており、対策のカテゴリー別では「『組織的対策』が 79.5%、『技術的対策』が 88.3%、『監視体制』が 82.3%、『評価の実施』が 81.2%となり、『監視体制』

を除くすべてのカテゴリーで前年度より上昇した。」となっている。

「寄与した」と回答した企業の割合が増加した対策項目としては「情報セキュリティマネジメントシステムの認証の取得」「リスクの分析」「ISO/IEC15408 認証取得製品の導入」が挙げられている。

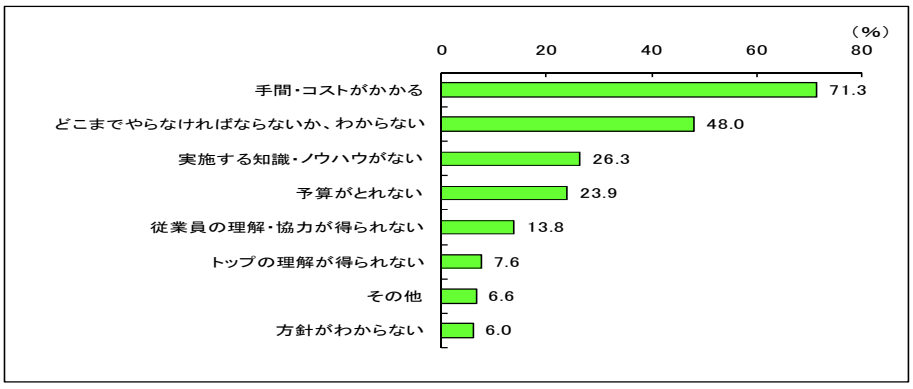
また、情報セキュリティ向上以外の効果については、2006 年度の回答として「特に効果はなかった」とするものが 41.8%を占めるものの前年度より 8.3%ポイント減少しており、効果があった項目として（複数回答）「顧客・取引先からの評価の上昇」25.1%、「業務効率や生産性の向上」14.8%、「製品やサービスの質の向上」8.8%、「市場や投資家からの評価の上昇」4.1%と、前向きにとらえる企業も多いことが伺える。

なお、これに関連する情報として、情報処理実態調査の主たる調査対象である IT 投資動向の調査では、IT 投資の効果として「業務革新」88.7%「IT インフラの強化」84.4%に次いで「セキュリティ対策」78.0%が挙げられており、8 割近い企業がセキュリティへの投資効果を確認している。

10.1.4. 対策の阻害要因

対策の阻害要因としては、図 41 に見られるように「手間・コストがかかる」「どこまでやらなければならないか、わからない」が多数を占め、4000 社の回答企業の約 4 分の 1 は「実施する知識・ノウハウがない」「予算が取れない」と答えている。

図 41 情報セキュリティ対策の阻害要因（平成 19 年情報処理実態調査）



（注）
1. 情報セキュリティ対策の阻害要因に関する設問の回答状況（複数回答可）。
2. 回答企業数は、4,000 社。

なお、上記と同様に IT 投資動向の調査からセキュリティに関する項目を抜粋すると、IT 投資と企業の全体最適化との関係において、次のような分析が行われている。

「IT 投資の拡大が生産性や競争力の向上に結びつくためには、IT 投資の実施を通じて全体最適を実現することが必要であり、我が国企業は部署横断的な最適化や企業横断的な最適化が遅れているといわれている。そこで、これらの全体最適化の阻害要因をみると、いずれもコストの高さや業務プロセスの標準化の遅れを指摘する企業が多かったが、その他に部署横断的な最適化の

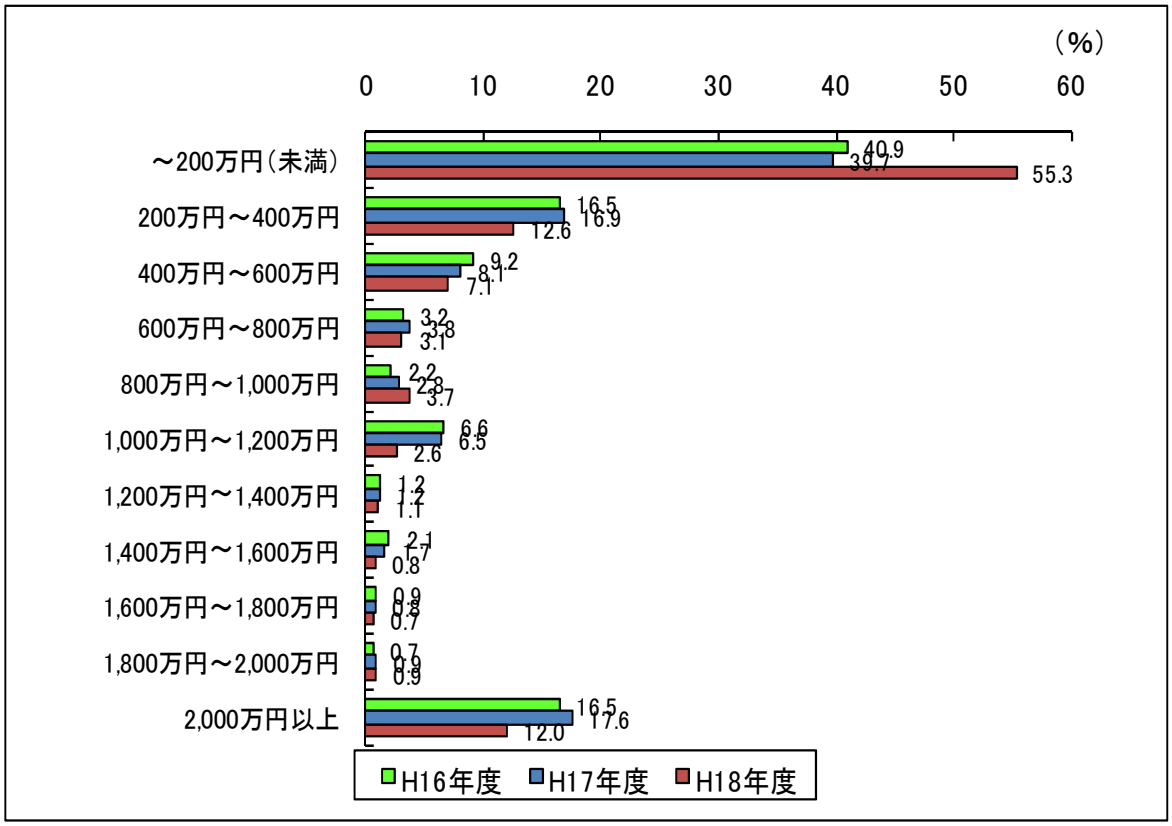
阻害要因として人材不足、企業横断的な最適化の阻害要因としてセキュリティの問題を挙げる企業が多かった。このため、全体最適化を推進して行くためには、全体最適化に要するコストの抑制や業務プロセスの標準化を進める他、人材面、セキュリティ面の課題を解決することが求められることが推察される。」

10.1.5. 対策費用

対策費用は企業規模によって額が大きく変わってくるので金額の絶対値だけから判断することは困難ながら、対策金額の分布及びその比率の経年変化は図 42 のようになっている。

企業規模の分布は図 43 のようになっており、小規模事業者が偏在しているとは言えない中でセキュリティ対策費が 200 万円以下に集中している実態が確認できる。この点について、同報告書は「概要」の中で「平成 18 年度における情報セキュリティ対策費用の分布状況をみると、200 万円未満が 55.3%と半数以上を占め最も多かったが、2,000 万円以上とする企業も多く、二極化していることがうかがわれる。情報セキュリティ対策の実施率が高まっているなか、この 200 万円未満の企業の割合は前年度（39.7%）に比べ上昇していることから、個々の情報セキュリティ対策が小規模化している可能性があると思われる。」と述べている。

図 42 情報セキュリティ対策費用分布の推移（平成 19 年情報処理実態調査）



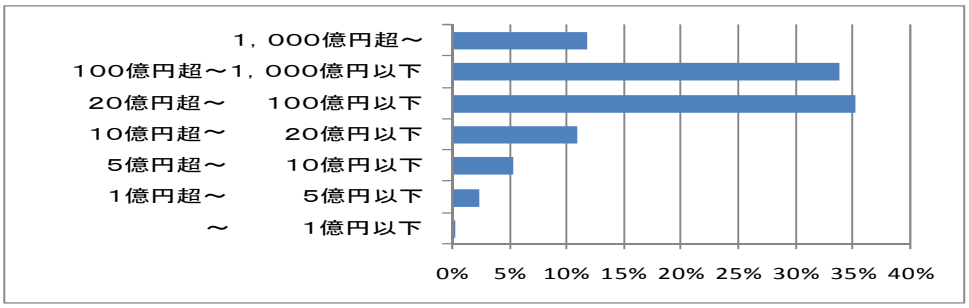
（注）
1.情報セキュリティ対策費用の設問の回答状況。
2.平成16年度及び平成17年度は、各情報セキュリティ対策費用階級の企業数の情報セキュリティ対策に関する外部支払い費用が発生した企業数に対する割合。平成18年度は各費用階級の企業数の情報セキュリティ対策費用の設問で「わからない」及び「発生しなかった」以外の選択肢を回答した企業数に対する割合。
3.平成16年度及び平成17年度は各回答企業の情報セキュリティ対策費用の回答に基づき、費用分布を計算。
4.平成18年度の回答企業数は4,009 社で、2.の分母（「わからない」及び「発生しなかった」以外の選択肢を回答した企業数）は2,961 社。

また、報告書本体では 1 社当たりの平均対策費用の試算を試みている。その算出方法及び結果は、報告書の脚注によれば、次のようになっている。

「情報セキュリティ対策費用の分布に基づき、各階級の中間値をその階級に属する企業の情報セキュリティ対策費用と考え、その加重平均値を求めると、平成 17 年度 1,030 万円、平成 18 年度 750 万円となり、平成 17 年度から平成 18 年度にかけて低下している。

なお、実際は情報セキュリティ対策費用が 2,000 万円以上の階級において、広く企業が分布しているため、実際の情報セキュリティ対策費用の平均値と、上記の方法で求められた加重平均値では大きな乖離が生じている。」

図 43　平成 19 年情報処理実態調査回答企業の年間事業収入額別企業数分布（無回答除く）

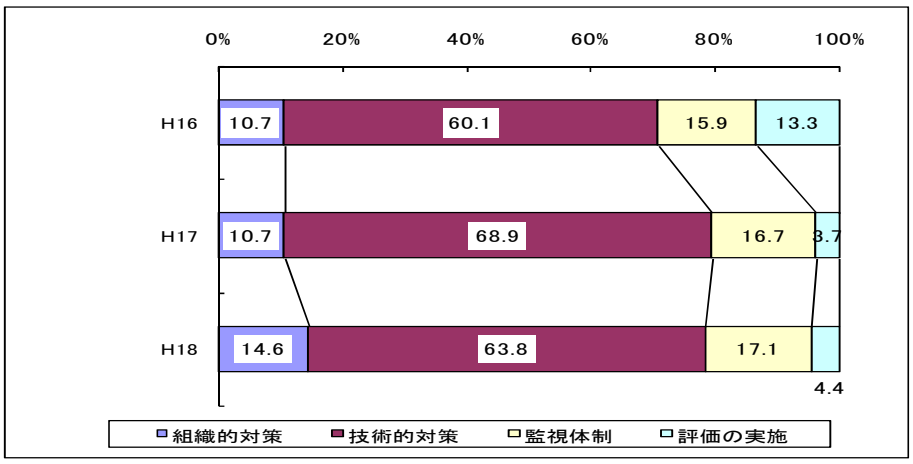


（出典：経済産業省公表データより JNSA 作成）

ここに示された 2006 年度の対策費 750 万円という回答の加重平均値は（金額のみなし要素があるのであくまで目安程度ではあるが）、調査対象企業の年間事業収入の平均値 795 億 8 千万円という額に比較すると、1 万分の 1 以下となり、極めて低いと考えられる。

情報セキュリティ対策費用の内訳構成比については、図 44 のような集計が示されている。技術的対策の占める割合が高いが、組織的対策、監視体制、評価の実施に対しても前年度より高い比率の費用が振り向けられていることが読み取れる。

図 44　情報セキュリティ対策費用の内訳の推移（平成 19 年情報処理実態調査）



（注）
1. 情報セキュリティ対策費用の内訳構成比。
2. 平成１６年度及び平成１７年度は、各企業が回答した情報セキュリティ対策費用総額と内訳構成比の数値を用いて、各対策費用の金額を計算し、積み上げた結果に基づき構成比を算出。
3. 平成１８年度は、以下の通り回答された情報セキュリティ対策費用の選択肢の中間値を回答企業の情報セキュリティ対策費用総額とみなし、これと各企業が回答した各対策の構成比を用いて 2. の方法で各対策の構成比を算出。
「200 万円未満」＝100 万円、「200～400 万円」＝300 万円、「400～600 万円」＝500 万円、
「600～800 万円」＝700 万円、「800～1,000 万円」＝900 万円、「1,000～1,200 万円」＝1,100 万円、
「1,200～1,400 万円」＝1,300 万円、「1,400～1,600 万円」＝1,500 万円、「1,600～1,800 万円」＝1,700 万円、
「1,800～2,000 万円」＝1,900 万円、「2,000 万円以上」＝4,000 万円
4. 平成１６年度の構成比は、社内 IC カードを除いた情報セキュリティ対策費用総額に対する内訳構成比。
5. 平成１８年度の回答企業数は 1,520 社。

10.2　国内情報セキュリティ市場調査との比較分析

ここでは上に見てきた情報処理実態調査における情報セキュリティ関係の統計結果について、本調査結果との関係において考察を試みることにする。

10.2.1.　トラブルの発生状況に関して

回答企業全体の 24.8%が何らかのトラブルを経験している。特に「ウィルスやワーム」の被害経験の比率が飛びぬけて高い。ウイルス・ワームの亜種の多さ、その出現リードタイムやサイクルの短さはウイルス対策ソフトメーカをも悩ませる激しさであり、また 2005 年には異例の官房長官談話まで引き出されるほど頻発したファイル共有ソフトに感染するウイルスの被害等を見ても、引続きこの問題が大きな比率を占めることは符合すると考えられる。

コンテンツセキュリティ対策製品が、その普及率の高さの割に市場規模の拡大が継続するのも、この辺に要因がある可能性が高い。

次に「ノートパソコン及び携帯記憶媒体等の盗難・紛失」も回答者の 25.4%が経験しており、かつこの被害は経年増加傾向にある。この対策としては外部記憶等への書き出しやコピーを監視・禁止する「ポリシー管理・設定管理・動作監視制御製品」や万一紛失してもデータを読み取られないようにする暗号製品の需要に結びついていると考えられ、本調査における 2006 年から

2008 年度にかけての活発な動きに結びつくものとして注目される。

10.2.2. 対策状況に関して

情報処理実態調査では、対策のカテゴリとして「組織的対策」「技術的対策」「監視体制」「評価の実施」の 4 区分を定義している。これらのうち何らかの対策を実施している企業は 2006 年で 85%に達し、情報セキュリティ対策はほとんどの企業で何らかの対策を講じるレベルにまできていることが確認できた。このうち技術的対策は 80%の企業で取り入れており、IT 面での防御、保護が進んでいることがわかる。同調査における技術的対策には物理的アクセス管理や ISO15408 認証製品の導入なども含まれるが、アクセス管理、ファイアウォール、生体認証など本調査におけるセキュリティツール区分の相当部分が対応する。

本調査の平成 19 年度版においては、2006 年度の情報セキュリティツールの対前年度比市場成長率を 20.5%としていた。本調査の 2007 年度の対前年度比市場成長率は 18.3%であり、この高い伸び率を裏付けるものとして、情報処理実態調査の結果があると分析することができよう。

同じく「組織的対策の実施」によるセキュリティポリシーの策定や従業員教育、「監視体制」を構成する外部専門家による常時セキュリティ監視、「評価の実施」における情報セキュリティ監査や情報セキュリティマネジメントシステム認証の取得などは情報セキュリティサービスを構成するサービスメニューであり、これらの対策に振り向ける費用の比率が増加することは、これらサービスへの需要喚起に結びつくものと分析できる。

10.2.3. 対策効果に関して

情報セキュリティ対策実施の効果の評価と情報セキュリティ市場の動向を直接結びつける要素は、数字的紐付けの面では多くないが、多くの企業がセキュリティ面での向上だけでなく、顧客の評価その他における経営への貢献も認識していることは、情報セキュティ対策への継続的取組を支えるものとしてとらえることができる。

このような経営的に前向きの評価が、情報セキュリティ対策を後押しするものとして、重要と言える。

10.2.4. 対策費用に関して

情報処理実態調査では、回答企業の対策費用の加重平均の試算を行っているが、2006 年度は 2005 年度の 1,030 万円に対して 750 万円と、1 社当たりの情報セキュリティ対策費用の額が 27%減少している。一方、本調査のデータは、順調な市場の拡大を見ており、両者の間には一見矛盾した関係が見える。そこで、情報処理実態調査の両年度の母集団に関するデータを整理して比較してみた[53]。（表 32）

[53] 平成 18 年情報処理実態調査に関しては http://www.meti.go.jp/press/20071113001/20071113001.html

2006 年度は回答企業数が 17%増加、平均資本金規模は 10%程度増加しているが、年間事業収入規模の平均値はほぼ同じである。一方、情報処理関係諸経費の 1 社当り平均金額は約 25%減っている。1 社当り情報セキュリティ対策費の加重平均値は 2005 年度から 2006 年度にかけて 27.2%減っており、ほぼ 1 社当り情報処理関係諸経費の減少と同程度の落ち込みであることがわかる。では日本全体で IT 投資や IT 費用の総額が 4 分の 3 程度に減ったのかというと、6.1 項で参照した JEITA の統計[54]によれば、2006 年度の「ソフトウェアおよびソリューションサービス」の出荷額は前年度比 101%であり、極端な市場の落ち込みは考えにくい。

表 32　情報処理実態調査母集団の比較（平成 18 年度調査、平成 19 年度調査）

対象年度	回答企業数	資本金規模	年間事業収入規模	情報処理関係諸経費	年間事業収入比	情報セキュリティ対策費用	対情報処理関係費比率
	（社）	（百万円）	（億円）	（百万円）	（%）	（万円）	（%）
2005年度	3,647	8,956	803	958	1.19	1,030	1.08
2006年度	4,264	9,857	796	725	0.91	750	1.03
2006/2005	116.9%	110.1%	99.0%	75.7%	76.4%	72.8%	96.2%

従って、情報処理実態調査の 1 社当り平均情報セキュリティ対策費用はたまたま 2006 年の数字が低く出た（1 社当り平均情報処理関係諸経費も同様）ものと考えられる。

むしろそのことよりも、ここでは、情報処理関係諸経費の売上高比率が 1%前後であることと、情報セキュリティ対策費用が IT 費用の 1%程度に過ぎないことに注目したい。財団法人日本情報システム・ユーザ協会（JUAS）は毎年企業 IT 動向調査を実施しているが、その 2008 年度版報告書[55]によれば、調査対象企業の IT 投資額の対売上高比率は 2006 年度実績で 1.12%、2007 年度計画で 1.28%程度である。情報処理実態調査よりは 1 割程度高い比率となっている。しかも 2007 年度予算額ベースで 1 社平均 2,582 百万円と、情報処理実態調査の 3.6 倍の規模であり、より規模の大きい母集団では対策費用の率も高いことを伺わせる。いずれにせよ、情報セキュリティ対策費が売上高対比 1%程度の IT 費用のさらに 1%程度しかかけられていないとすれば売上高比では 1 万分の 1 となり、非常に小さい市場であることを示している。

また、1 社当り 1 千万円とか 750 万円という年間費用規模は、発注段階ではさらにいくつもの対策ツールやサービス項目に分散されることが瞭然で、情報セキュリティの商談規模が非常に細かいものになることを示唆し、当市場が事業効率の面や、したがって採算性の面で、事業者には非常に厳しい市場であることを物語っていると言える。

[54] http://it.jeita.or.jp/statistics/soft_sol/h19/index.html
[55] http://www.juas.or.jp/project/survey/it08/index.html

11. 情報セキュリティをめぐる新しい動きについて

11.1. 情報セキュリティに関わる最近の動き概観

情報セキュリティに関する状況は、様々な要素に影響を受ける。それは①インターネット環境からもたらされる、外部からの攻撃の脅威、②外部脅威に対する対策のためのツール・サービス類や、セキュアな IT 環境（IT システム、ネットワーク、OS 及びプラットフォーム、アプリケーションプログラム）実現のための情報や知識、ノウハウ、③情報セキュリティを組織の経営と業務運営の中で守るためのマネジメントシステム、すなわち経営対応（IT 環境のセキュアな運用に関わる、IT 環境の設定や運用ルール等を含む。また、組織の構成員の過失や故意による情報漏えい・データロスやシステム障害に対する人的･組織的対策もここに含まれる）、④政府や公的機関が定める法令や規格・基準類や立案実施する政策、等である。

これらの各々につき、状況は日々変化している。脅威は残念ながら当面衰えることを期待できないが、ネットワークセキュリティの技術も進化し、広い意味でのコンプライアンス対応も進んでいる。マネジメントシステムも、規格・基準関係も、進化と深化を続けている。

情報セキュリティの脅威が日々深刻化する一方で、それへの対策の幅も広がっている。情報セキュリティ状況の構成要素の各々が、日々変化して相互に影響を与えつつ、関わりを持って動いている。その結果、情報セキュリティを取巻く環境は流れを形成しながら変化を続けていると言える。その多くを、本調査報告の中で、７.項、８.項、９.項を中心に見てきた。

以下では、その中で取り上げなかった、あるいは断片的に触れるに留まった動きの内、特にこの数年の間の動きの中で注目すべき点について､簡単に触れることにする｡取り上げるテーマは、次の通りである。

① 2007～08 年におけるネットワークの脅威の動向
② SaaS、仮想化環境やクラウドのセキュリティ課題
③ セキュリティにおける SaaS（Security as a Service）の利用
④ セキュリティの新技術動向：レピュティション、ホワイトリスト、DLP について
⑤ 情報セキュリティのパラダイム拡大の動き（GRC とは）

11.2. 2007～08 年におけるネットワークの脅威の動向

IPA（独立行政法人情報処理推進機構）セキュリティセンター発行の「情報セキュリティ白書 2008」の第Ⅱ部「10 大脅威 ますます進む『見えない化』」[56]によると、2007 年の脅威の動向が以下の通り挙げられている。

1 高まる「誘導型」攻撃の脅威
2 ウェブサイトを狙った攻撃の広まり
3 恒常化する情報漏えい

[56] http://www.ipa.go.jp/security/vuln/20080527_10threats.html

4 巧妙化する標的型攻撃
5 信用できなくなった正規サイト
6 検知されにくいボット、潜在化するコンピュータウイルス
7 検索エンジンからマルウェア配信サイトに誘導
8 国内製品の脆弱性が頻発
9 減らないスパムメール
10 組込み製品の脆弱性の増加

この資料の表題の通り、ネットワークの脅威は 2007～08 年に「見えない化」が大きく進んだ。これは、従来のセキュリティ対策では、ネットワークからの攻撃の検出が困難になってきていることを示している。また、サイバー犯罪をはじめとするネットワークの脅威は、その目的も変化しており、手口の悪質化や巧妙化も進んでいる。警察庁発行の「警察白書」[57]が記載する統計によれば[58]、「不正アクセス行為の動機」として「不正に金を得るため」が年を追って件数、率とも増加し、2007 年度では 1,186 件、82.5%に達している。サイバー犯罪の目的は好奇心や自己顕示欲などを満たそうとする愉快犯的なものから、金銭などが目当ての営利目的に大きく移っている。また、以前はコンピュータウイルスに感染させることや不正アクセスをすることが「目的」だったものが、単なる「手段」となっている。脅威のターゲットもサーバ自体やそこに格納された情報から、個人の認証情報（ID、パスワード、クレジットカード情報等）に移ってきている。

2007～2008 年に特に目立ったネットワークの脅威として、ここでは、SQL インジェクション、ボットの二つを取り上げてみる。

まず「SQL インジェクション」とは、2000 年頃には既に認識されていた攻撃手法であるが、アプリケーションのセキュリティ上の不備を悪用し、想定しない SQL 文[59]を注入（Injection）し実行させることにより、データベースシステムを不正に操作する。これにより、情報の漏えいや改ざん、サーバの停止、ネットワークへの侵入などの更なる攻撃を行う。独立行政法人情報処理推進機構は 2008 年 5 月に SQL インジェクション攻撃に関する注意喚起を発表している[60]。また民間のセキュリティ対策サービス提供企業が公表しているネットワーク観測統計でも、その後現在（執筆時点：2009 年 3 月）に至るまで、攻撃件数は引き続き高い数値で推移している[61]。

ボットは、コンピュータを遠隔操作で悪用することを目的に作られたマルウエア（悪意のプログラム）の 1 種である。ボットに感染したコンピュータは、攻撃者が用意した指令サーバなどに自動的に接続され、数十～数百万台のボット感染コンピュータを従えた「ボットネット」と呼ば

57 http://www.npa.go.jp/hakusyo/h20/index.html
58 http://www.npa.go.jp/hakusyo/h20/toukei/t1-23.pdf
59 リレーショナルデータベース管理システム用の操作言語である SQL 言語で書かれた問合せ文
60 http://www.ipa.go.jp/security/vuln/documents/2008/200805_SQLinjection.html
61 同企業は 2009 年 3 月に発表した「JSOC 侵入分析レポート」でも SQL インジェクションの脅威を取り上げ警告している。

れるネットワークを形成する。このボットネットを通じて攻撃者が、感染したコンピュータを外部から遠隔操作し、スパムメールの大量配信、特定サイトへの DDoS 攻撃[62]、感染者のコンピュータ内の情報の詐取など深刻な被害をもたらしている。

このように、ボットに感染したコンピュータは他への攻撃の「踏み台」にされる。ボットは、感染したとしても目に見える特別な症状が現れないことが多く、違和感なくコンピュータを使用できるなど、ユーザに感染を気づかせない特徴を持っている。このため、感染したコンピュータのユーザは被害者でありながら、同時に知らぬ間に加害者にもなってしまう。結果としてネットワークに深刻な被害を及ぼすことになる。

ボットのソースコードやボットを簡単に作成するツールはインターネット上に公開されており、ひとつのボットプログラムを元にした数多くの亜種が作成されている。さらに、いくつかのボットは攻撃のコードが配布されるサイトと定期的に通信を行い、自分自身を自動的にアップデートする機能を持ち、新しい攻撃の機能を追加したり自身の不具合を修正するなどしている。このアップデートはかなり短い周期で頻繁に行われており、絶えずその姿を変えると共に進化していると言える。この点もウイルス対策ソフト等によるボットの検出を困難にしている。一度感染すると中々気づきにくく、その間に被害者が加害者になって、本人が知らない間に攻撃を続けることになってしまう。

「見えない化」が進んでいる脅威に対しては、従来のセキュリティ技術では検出ができない場合も増えてきている。そのため、新たな技術を使用した製品やサービスも市場に登場してきている。今後、このような新たな検出技術にも注目したい。また、経済産業省と総務省が共同で運営するサイバークリーンセンター（CCC）では、ボット対策のための注意喚起と対策ツールの配布を行っている[63]。このような仕組みも活用して、ボットの感染を防ぎ、いち早く発見すると共に、自らが知らないうちに加害者になる事態を避けるように努力する必要がある。

11.3. SaaS、仮想化環境やクラウドのセキュリティ課題

(1)SaaS 普及のポイントと ASP 型サービスとの違い

2006 年頃から本格的に普及し始めた SaaS（Software as a Service）は企業アプリケーションのデリバリーモデルとして定着した。いわゆるパッケージソフトウェアは、多くのユーザが共通に使用するソフトウェア機能の集合体と見なすことができるが、一般にソフトウェアの進化・成長に伴って「肥大化」（ある特定のユーザにとって、あまり使用しない機能の増加）を招く。その解決策として、ケーブルテレビや電話などの“サービス”のように、ユーザが利用したい機能を、必要になったときにネットワーク経由でサービスプロバイダから直接入手し、その使用分に対して対価を支払うようにするというコンセプトが SaaS である。

---

[62] Distributed Denial of Service 攻撃＝分散サービス妨害攻撃　特定のサーバに通信パケットを集中して送りつけることで機能不全を起こさせるサービス妨害攻撃を、複数の発信元から一斉に実行することで防御を困難にする不正アクセス攻撃の手法

[63] https://www.ccc.go.jp/

ユーザにとっては SaaS の最大のメリットは導入の容易性である。だが、かつての ASP（Application Service Provider）[64]と比較して、なぜこれほど普及したのだろうか。SaaS が ASP と比較して違う点は大きく二つある。

一つは、SaaS はマルチテナントであること。仮想化などの技術を活用することで、同一のアプリケーションとプラットフォームによるサービスを複数の企業に対して提供する。

二つ目はカスタマイズ性の高さである。SaaS では、画面構成や使用する機能の選択などを中心に、顧客ごとに一定のカスタマイズが可能である。

かつての ASP についての問題点を振り返ってみると、導入や運用でコストメリットをまったく出せないケースが多かった。ユーザの要求に応じるには、どうしても専用の環境を用意することになるからである。アプリケーションごとにカスタマイズすれば、当然メンテナンス性が悪くなって費用もかさむといった問題があった。このような事情に対して、最近のネットワークコストの大幅な低下や、IT 資産の管理や業務プロセスを外部に委託することへの企業の抵抗感がなくなってきたことが重なり、SaaS のマーケットは大きく広がった、特にアプリケーションがカスタマイズ可能なことは、SaaS が幅広い顧客を獲得する大きな要因となったと考えられる。

⑵仮想化技術

仮想化という技術はすでに企業ユーザにとって、特段目新しいというわけではなくなってきている。サーバの仮想化には、ユーザは次第に違和感を覚えることなく取組を進めるようになってきている。更に、サーバに加えてストレージ、クライアントデバイスの仮想化が急速に進んでいる。

ストレージの仮想化によって、ファイルがオリジナルの場所に格納されているようなイメージでシステムからアクセスできる環境が提供できるようになる。そうすることで、実際のストレージデバイスの複製をなくすことも可能になり、ストレージデバイスや情報を格納する媒体のコストを大幅に削減できる可能性がある。

一方のクライアントデバイスの仮想化では、ホスト型仮想デスクトップが注目される。これは、ブレードをベースにした PC に相当する環境を提供することになるが、PC のマザーボードの機能がハードウェアとしてデータセンタに実装される代わりに、実体のない仮想的なマシンとして実装されることになる。

⑶クラウドコンピューティング

クラウドコンピューティングはすでに多くのベンダ企業からさまざまなモデルが提供されつつある。クラウドコンピューティングのさまざまな定義を大きく二つのカテゴリに分類すると、一つはインターネット“クラウド”を介して提供するサービスとコンピューティング・リソースへのリモートアクセスに特化したもの、そしてもう一つはサービス・ベースのコンピューティング機能を開発／提供するための仮想化や自動化といった技術に特化したものである。

前者の「サービス・カテゴリ」に含まれるのは、CRM（顧客関係管理）や HR（人事管理）／

[64] ソフトウェアをライセンス販売するのでなく、ネットワーク経由でサービスとして提供し、用益に対して対価を得るビジネスモデル。「ソフトウェアの時間貸し」とも呼ばれた。

給与計算サービスなどの SaaS アプリケーション、及び米国 Amazon.com の「Amazon EC2（Elastic Compute Cloud)」など、ウェブを介してサーバ（CPU）リソースやストレージ・リソースへのアクセスを提供するベンダ／サービスプロバイダである。クラウドコンピューティング環境をサービスとして提供するビジネスモデルで、パブリッククラウドという呼び方もされている。

後者の「技術カテゴリ」は、「従来のデータセンタのアプローチを拡張することで、サードパーティ提供の外部機能を使わずに完全に社内の IT システムに適用する」ことを目指すユーザ企業のためのものである。これはクラウドコンピューティング技術をオープンなサービスのために使うのでなく、そのスケーラビリティその他のメリットを自社内で使うことを目的とするビジネスモデルで、プライベートクラウドとも呼ばれる。

どちらもクラウドに対するアプローチとしては間違いでないが、混乱を避けるため、それぞれを明確に区別して考える必要がある。ユーザにとっては、クラウドコンピューティングとそのサービスの利用について考えることと、社内システムを構築するためクラウドコンピューティング関連のコンセプトと技術を利用することはまったく別物だと理解する必要がある。クラウドのサービスと技術は両方とも重要な視点であり、それぞれ追求して行くべきではあるが、この二つの要素は関連性を持ちつつも、別々のイニシアティブである。

前者のモデルとしての特徴は、①各種機能を“サービス”として提供、②拡張性と柔軟性に優れた環境でサービスを提供、③インターネット技術と手法を利用してサービスを開発・提供、④外部顧客への提供を念頭に置いたデザイン、と４つある。このコンピューティング形式の最大のメリットは、クラウドコンピューティングが本来持ち合わせている柔軟性と拡張性で、導入のハードルが著しく低くなる。システム開発には開発環境をハードウェアから整える必要があり、システムの必要資源の見積りに始まり、プラットフォームの調達だけで数ヵ月を要することもざらである。クラウドの場合は、プロバイダにインターネット経由でアクセスして必要な資源を要求し、サインアップするだけで済む。短ければ数分で開発準備は完了する。またカットオーバーに際しても当面必要なリソースを手当てすれば済み、拡張が必要になればその都度追加が可能であり、迅速な拡長も可能になる。このように、クラウドコンピューティングは中小規模の企業にとって、システムコスト面でのメリットをもたらす可能性が極めて高い。

セキュリティ対策面でも、そのための対策を潤沢に用意できない、あるいは、日々の運用に十分手を割けない中小規模のユーザにとってはメリットが大きい。ファイウォールを始めネットワークからの脅威に対する防御はそのプラットフォームの信頼性を左右する重要要素であり、専門家が万全の対策を施すので、資金と資源の制約のもとで最低限の手当てに走りがちな個別ユーザにとっては格段にレベルの高いサービスが実現できることになる。また、脆弱性を解決する修正パッチの適用やプラットフォーム技術の更新は､クラウド環境の所与の条件として提供されるし、アクセス管理等、自社の情報資産の管理についても、ひとつのサービスとして提供を受けることができる。このようにセキュリティ面の手当てが充実することも、中小規模ユーザにとっては大きなメリットとなる。

(4)仮想化環境やクラウドサービス利用上のセキュリティ課題

企業が仮想化やクラウドの利用で得られる最大のメリットは、物理システムの運用効率を高めることでのコスト削減効果だろう。仮想化環境を活用すれば、物理マシンを多数抱えることなく柔軟なシステム構成を可能にする。クラウドを利用すれば、最小限の物理システムさえ保有していれば、必要なシステム環境を必要なタイミングで調達・運用することができる。またシステム運用上のセキュリティ対策が整合性をもってアーキテクチャとして構築され施されていることもメリットである。

だが、仮想化やクラウドは企業にとって新たなセキュリティホールになる可能性があることも指摘されている。アメリカの大手調査会社は、2008 年 7 月の「Accessing the Security Risks of Cloud Computing」[65]というレポートで、クラウドサービスが抱える 7 つのセキュリティリスクを指摘している。

① サービス側特権ユーザの不正行為がないか
② 自社コンプライアンスとの適合ができるか
③ データの保管場所による法律的な問題はないか
④ データの論理的な分離方法が安全か
⑤ 障害時の復旧手順が明確であるか
⑥ 不適切行為や違法行為への調査支援はあるか
⑦ クラウドサービス事業者の破綻や買収時に継続的に利用できるか

これらの問題が指摘していることは、サービスの実体がネットワークの向こうにあるというメリットの裏返しである。不特定多数が共用するインフラ上に構築されたサービスでは、特定のユーザだけに特権を与えることは難しい。結果として、汎用的なレギュレーションを定義せざるを得ず、これが個別のユーザ企業にとって適切であるとは限らない。

また、こうしたリスクに対してどのような対応をとっておくかはコストに直結する。稼働率の保証がある程度はあるとは言え、復旧などの問題については的確に問題や見通しが把握できるとは限らない。結果として、自社の事業継続管理（BCM）に大きな影響を受けるリスクは残る。これを回避するための手法などを講じるとすると、大きなコストが発生する。特にデータを取り出せなくなるリスクは最も危険度が高いと言える。

例えばこのデータの可用性の問題を例にとれば、次のような問題が想定できる。まず、データの可用性確保の手段としては、①契約先クラウドプロバイダとの契約によるバックアップと可用性の保障、②自社にデータバックアップ環境を整え、クラウド環境での運用とローカルのバックアップを取み合わせて使用する、③メインのクラウドサービスの他に別のクラウドサービスプロバイダと契約を結び、後者をバックアップとして利用する、などが考えられる。これに対して各々の問題点は対応する番号順に、①契約先のシステム、アクセス回線、アクセスのためのローカル端末のいずれかの障害によるアクセス障害とクラウド内でのデータロスのリスク、②ローカルバックアップシステムの調達・運用コスト及びスケーラビリティの制約、クラウド内データとバックアップデータの同期やインテグリティ（同一性、首尾一貫性）の確保、③クラウド事業者間でのバックアップデータの受け渡しに際しての同期やインテグリティの確保、データロス時の責任

[65] http://www.techworld.jp/channels/security/102125/

の切り分け・保障問題、などが想定できる。

(5)仮想化環境やクラウド運用上のセキュリティ課題

仮想化環境では仮想マシンが氾濫することでセキュリティ管理の複雑性が増す。クラウドでは重要なデータの所在やユーザのアクセス権限などの管理を企業がすべて掌握できない場合がある。これらの重大なセキュリティ課題がすでに顕在化しているわけではないが、これらのクラウドに固有の環境特性の弱点を突く方法が見つかれば、サイバー攻撃者はすぐに標的にする可能性がある。クラウド環境に重要情報や個人情報が委ねられていれば、そのような金銭につながる情報が保管されたインフラはサイバー犯罪ネットワークの格好の攻撃対象とされるであろう。

仮想化やクラウドにおける情報セキュリティ管理を考える上では、これらのインフラが持つ特徴と既存のアプローチを取り合わせて行くことになる。

仮想化では、仮想マシンへのインタフェースを保護する方法と、仮想化プラットフォームを含めてシステム全体を保護して行く方法がある。例えば仮想化プラットフォームと物理ネットワークの境界に IPS（不正侵入防御）アプライアンスを置き、個々の仮想マシンへの不正アクセスをブロックする。次のステップとして、個々の仮想マシンと仮想化プラットフォームを包括的に管理するシステムを用意する。仮想化環境に対応したアプライアンスはセキュリティベンダ各社が現在注力する分野の一つである。また、実マシン環境、仮想化プラットフォームのいずれでも透過的に管理できる、包括的なセキュリティ管理システムが今後必要となってくるであろう。

11.4. セキュリティにおける SaaS（Security as a Service）の利用

(1)SaaS（Security as a Service）とは

ネットワークを介してのアプリケーションやプラットフォーム用益の提供を”Software as a Service”の SaaS と呼ぶのにならって、ネットワークを介して、情報セキュリティ対策のための機能をサービスとして提供するビジネスモデルを、”Security as a Service”の頭文字を取って別の意味での” SaaS”と呼ぶことがある。本調査における「セキュリティ運用・管理サービス」が、広い意味では”Security as a Service”に該当するが、一般には、このうちいわゆるマネージドセキュリティサービス、すなわちセキュリティ機器の遠隔運用・監視サービスが、ほぼ”SaaS”の意味するところと一致すると考えられる。その意味では、サービス自体は以前からあって、そこに”SaaS”という呼び方が後から加わった意味合いが強いと言える。

セキュリティ機能をネットワーク経由で提供する SaaS では、セキュリティ機器は SaaS サービス事業者の網内に設置されているため、企業は各拠点に機器を設置することなく、必要な時に必要なだけセキュリティ機能を利用することが可能となる。また SaaS サービス提供側が、企業側の各拠点に機器を設置し、セキュリティ運用を一括して管理提供する形態もある。

現在実用化されている SaaS には以下のような種類があり、ネットワークと一緒に提供される。

① インターネット接続部分のファイアウォール機能、侵入検知機能

② 社内メールサーバと連携したウイルスやスパムの駆除機能

③ URL フィルタ、ウイルス・スパイウェア駆除をするウェブアクセスの検疫機能
④ 社内外ネットワーク上での通信プロトコルのトレンドを分析し、脅威を診断する機能
⑤ 日本版 SOX 法に対応したログの収集、保管、分析機能を有するログ管理機能

例えばウイルスやスパムの駆除機能を利用すると、該当するメールを発見すると社内のメールサーバに届く前に駆除し、安全なメールのみ送付するため、有事の場合にウイルス感染やスパムの過負荷でサーバがパンク、という事態を避けることができる。 また、この SaaS と既存のセキュリティ対策を取み合わせることも効果的である。検疫機能の強化として PC のウイルス対策ソフトウェアと SaaS を併用すると、ユーザが PC 上でウイルス対策ソフトウェアを無効にしてしまったり、ウイルス定義ファイルを更新し忘れたりした場合のリスクを低減できる。

(2) SaaS（Security as a Service）利用の意味とメリット

上記のような機能は、もちろん市販のソフトウェアやアプライアンスでも実現できるもので、自前での運用も可能であるが、SaaS には自前でツール、運転管理要員、運用管理業務を持たず、専門家のサービスを利用することによるメリットがある。特に同じ対策を複数拠点で実施しようとする場合にその利点が顕著に表れる。 複数拠点で同一のサービス（SaaS） を使うメリットには、SaaS 提供事業者の集中管理により複数拠点で共通の設定・対策を同時に一律に適用できる点と、複数拠点に複数の機器を導入・管理しなくてよいコストやリソース面での利点とがある。

従来、セキュリティ対策については高度に専門的な知識を必要とすることが多く、専門知識を持った担当者を確保することが難しい多くの中小企業においては、十分なセキュリティ対策を実施することは困難であったが、SaaS で提供されるサービスを用い、専門知識を保有するサービス事業者にセキュリティ対策を委託することにより、企業規模に制約されずに高度なセキュリティ対策の確保を実現することが可能になる。また、会社の規模が大きくなると脅威の入り込む隙も増え、リスクは規模の拡大以上に高まるので、担当者はますます頭を悩ませることになる。実際、事業展開のスピードに合わせ、セキュリティ対策を講じて行くことは大変な労力を要する。特にグローバル企業の場合、世界で統一したセキュリティ対策を実施しそのレベルを一律にそろえることは極めて困難になる。SaaS を利用することで、グローバルで均一な対策を講じることが容易になる。更に、進出先国に固有の環境や法的規制等によって拠点ごとに個別の対策や対応が必要な場合は、世界一律の対策を適用した上で、各拠点に個別のセキュリティ対策を追加することで対応が可能となる。このように、グローバル企業においても SaaS をうまく活用することで、グローバルで多層な防御体制を、迅速かつ容易に実現することが可能となる。

Security as a Service は、中小企業においてはセキュリティ対策機器の導入・メンテナンスの問題と運用管理の要員・スキルの問題を、大企業においては国内や海外に複数展開する拠点に対して一律・均質のセキュリティ対策を講じる上での同様の問題、更には統一性確保の問題を、サービスを導入することによって解決できるメリットがある。しかも多くの場合、自社で対策ツールや要員を抱えるより質の高い対策を、専門家のサービスを利用することで実現できる。この意味で SaaS は、中小企業や大企業の出先拠点でのセキュリティを促進・充実させる手段として期待できる。

11.5. セキュリティの新技術動向：レピュティション、ホワイトリスト、DLP について

IT の飛躍的な発展と通信の量的・質的な進化は多くのメリットをもたらしているが、同時にネットワークからの悪意の攻撃の脅威も進化し、その傾向の変化や多様化もあり、従来の対策技術だけではスパムメールやボット、マルウェア、情報漏えいなどの脅威から情報を守ることが困難になってきている。情報セキュリティの技術も進化を続けているが、脆弱性の増加と攻撃側の技術の変化に対応して新しい技術で対策を行う、言わば「いたちごっこ」を続けていると言える。

その結果、近年の情勢の変化に伴い、新しい技術とも言える対策技術が現れ始めている。ここでは、それら新しい技術のうち、「レピュティション」、「ホワイトリスト」、「DLP」について見ることにする。

(1) レピュティション

「レピュティション（reputation）」とは、直訳すると「評判」「名声」を表す。また、「事実を蓄積することにより、ある評価を出す」ことを指して用いられることもある。情報セキュリティ技術としてのレピュティションも同じような考えで、サービスを提供しているサーバの運用履歴や運用状況を評価することにより、相手が提供しているサービスが信頼できるものかを判断する。サービス提供側の評価には、IP アドレスや URL をベースとした評価データを蓄積した評価データベースが一般的に用いられる。評価データは、多く集めることでレピュティション評価の信頼度が上がるため、多数の評価データを世界中から蓄積することが重要になる。一事業者が多くの事例を収集することには限界があるため、評価データベースの提供を行うレピュティションサービス事業者も存在している。そのことにより、競合関係にある複数事業者の持つデータを総合して、よりレベルの高いレピュティション評価も可能になるので、相互にメリットがあると言える。

レピュティションが使われるようになってきた背景としては、従来のパターンマッチングをベースとしたフィルタリング技術では、迷惑メールやマルウェアのブロックが困難になってきたことが挙げられる。例えば迷惑メールの場合、迷惑メール対策ソフトがコンテンツフィルタリングの技術を導入し、メール本文への検知を行うようになると、迷惑メールの送り手であるスパマー達はそれを回避するために、メール本文を画像データで表示するという手口を編み出した。それに対して、迷惑メール対策ベンダが画像解析技術を導入して画像データを用いた迷惑メールも検知対象にすると、今度は画像解析技術での判定を困難にするために、画像中へのノイズ混入や、画像の文字色に複数色をランダムに使用した迷惑メールが発生した。他にも、PDF を用いた迷惑メールや、件名に本文を記載する迷惑メールなど、スパマー達は様々な手口を用いて迷惑メールを送信してきている。この状況はマルウェア対策についても同様で、すさまじいスピードで膨大な量の新型の亜種が生み出され攻撃に用いられている状況である。これに対抗するためには、シグネチャや定義ファイルと呼ばれるパターンマッチングのためのデータベースをリアルタイムに更新して行く必要がある。そのため、迷惑メール自体やマルウェア自体の内容をフィルタリング対象とした方式では、検知するための定義情報のサイズの肥大化や、更新頻度の頻繁化により、結果としてクライアントとネットワークへの負荷が著しく増大することになる。

そこで出てきたのが、レピュティション技術による発信元の評価である。迷惑メールやマルウェアに特徴があるように、迷惑メールやマルウェアを発信する側にも、短期間での多数のメール送信、頻繁な URL の変更、一つの IP で複数のドメインへの登録や短期間でのドメイン変更などの特徴がある。評価データベースでは、事前にそれらの情報を収集・蓄積しておき、それら複数の特徴を元にサービス提供側の信頼性を評価し、評価項目ごとにスコアリングすることにより、定量的な信頼性を算出している。そして、評価データベースで評価された点数毎に、レピュティションを利用する側で判断基準を定義する。そうすることにより、迷惑メールやマルウェアが送付されてきたとしても、評価データベースに問い合わせを行い、評価点数を取得して判定することにより、遮断などの事前に決められた対処をすることが可能になる。

しかし、定量的に算出された点数を評価するのは利用者側であり、利用者側が可用性を考慮して高い点数でなければ遮断しない、もしくは安全性を考慮して少しでも怪しければ低い点数でも遮断するなど、利用者側の状況に応じてレピュティションの利用のし方は異なる。また、サービス提供側の判定が困難な場合は、必ずしも点数が高く算出される訳ではないため、従来の対策と取み合わせて用いる必要がある。例えば、迷惑メール対策の場合は、受信したメールの送信情報から、送信元ドメインの検証を行う「送信ドメイン認証」方式を併用し、更に従来のフィルタリング方式等とも取み合わせることにより、初めてレピュティションの効果を高めることが期待できる。そういう意味では、レピュティションはあくまで従来の対策の補完的な位置付けであり、レピュティションのみで対策を行うことは現実的でないと言える。

市場動向としては、送信元 IP アドレスやウェブサイト（URL）の信頼性を評価する形で、迷惑メール対策製品、ウェブフィルタリング製品、ウイルス対策製品などに導入されるケースが増えている。最近では、ファイルの信頼性も評価データベースに登録しておき、IP アドレスやウェブサイトの評価データベースと連携して動作する技術を導入するベンダも出てきており、今後も他の機能と連携した技術の発展が期待できる。また、蓄積した情報を適切に評価するための評価データベースを運営するレピュティションサービス事業者も今後重要視されて行くことになるだろう。

(2) ホワイトリスト

「ホワイトリスト（white list)」は新しい技術ではなく、「ブラックリスト（Black List)」の対義語として旧来からある考え方の一つである。従来主として、ウェブアクセスコントロールにおける URL フィルタリングや、スパムメール対策におけるメールフィルタリングに際しての参照先として利用するのが基本的用途であった。例えば、スパム対策等でブラックリスト方式を用いた際の「誤検知（False Positive)」が発生した場合に、メールの送受信が不能になるのを防ぐための例外的処置として「ホワイトリスト」に登録する方法が取られることが多かった。

しかし、前述したように近年の攻撃側の手口の多様化・複雑化が進んだ結果、マルウェア対策において、ブラックリスト方式のみでは定義情報の肥大化や、未知の不正や脅威には対応できない等の問題が発生してきており、方式の転換が求められてきている。そこで、前述したレピュティション等と共に、「ホワイトリスト」を用いた方式が注目されてきている。既に情報セキュリティの複数の分野でホワイトリスト方式の活用は行われているが、ここでは比較的新しい動きとし

て、ウイルス対策を初めとするマルウェア対策としての「ホワイトリスト」について紹介する。

ウイルス対策製品におけるホワイトリスト方式といっても、実際の使われ方は製品や機能等で異なっている。以下に、いくつかの例を記載する。

まず挙げられるのは、スキャン結果から誤検知を取除くために、信頼性の高いファイルをホワイトリストに登録する方式である。これは、従来のスパム対策で用いられていたのと同じく、ヒューリスティック方式やビヘイビア方式等の従来の検知機能に対する例外措置としてのホワイトリスト活用方法と言える。

次に、ホワイトリストに登録されたファイルをスキャン対象から除外する方式がある。信頼できるファイルをホワイトリストに登録することにより、スキャン対象を絞り込み、マシンへの負荷を軽減することができる。

最後に、ホワイトリストに登録されているものしか実行を許可しない方式が挙げられる。この方式を用いて、実行を許可するファイルやアプリケーションをホワイトリストに登録することにより、厳格なアプリケーションコントロールも可能になる。しかし、実行を許可するファイルやアプリケーションを厳密に定義する必要があり、実際に運用する際に特定の環境以外では困難を伴うと予想される。

上記の各方式についても、実際に用いられる際に単体で用いられることは少なく、従来のルールベース方式やヒューリスティック方式、また前述したレピュティション等の技術と併せて用いられることが多い。最近では、仮想化技術と取み合わせてホワイトリストに定義されたファイル以外は機能を制限された仮想環境で動作させて振舞いを確認するような技術も活用されている。今後も各技術の組合せにより、より効果的なマルウェア対策が出てくることが期待できる。

このように、ホワイトリスト方式の活用のされ方は様々である。ホワイトリスト方式を上手く活用することで、従来の方式のみでは困難であった未知の不正や脅威に対してもプロアクティブな対応（事前対応）をすることが可能になる。しかし、ブラックリストと異なりホワイトリストの定義に不備が存在すると、逆にセキュリティの穴が開いてしまう可能性もあるため、どのように信頼性の高いホワイトリストを定義して行くかが今後の課題となって行くだろう。

(3)DLP

2007 年半ばごろから、DLP という技術が注目されるようになっている。D は Data、L は Leak もしくは Loss、P は Prevention もしくは Protection で、DLP のソリューションを提供するベンダによって組合せは異なる。定訳はないが情報流出防止、情報漏えい防御といった意味となる。情報の流出の経路や手段ではなく、情報そのものに着目して流出や漏えいの防止を図る考え方である。DLP は、その企業にとって機密であるデータと機密でないデータを区別し、機密データだけを外部に漏えいさせないように保護する仕組みを持つ。つまり、従来の情報漏えい対策が IT やそれを操作する人間の行為を対象にしたシステムであるのに対して、DLP はデータを対象とした技術となっている。

DLP が注目を集めるに至った背景として、内部要因による情報漏えいの深刻化がある。各企業はアクセス制御やセキュリティポリシーに基づく機密情報や媒体類の持出し制限による対策を講じているが、情報の流出、漏えい、紛失事件は後を絶たない。経路としては、ファイル共有ソフ

トに感染する暴露ウイルス、スパイウェア、メールの（誤）送信、USB メモリ等の可搬型媒体やノート PC などまちまちである。原因も、マルウェアへの感染、ミスや不注意、故意や悪意、あるいはこれらの組合せ等、一律の対応が困難な様々な要因がある。

従って、人の要素やデータを扱う手段にフォーカスを当てて制限を行う従来の情報漏えい対策のみでは、情報漏えいを防ぐことは困難である。人の要素の制御であるアクセス権での制御も、手段の制御である USB メモリの使用禁止、添付メールの送信制限、印刷制限なども、どちらも過剰に制限を掛けすぎると業務効率を阻害することになる。また、故意で行われる行為に対してはほとんど抑止力がない。そこでデータ自体を管理・保護することで、従来の対策の限界や不備を補い、より確実に情報の保護を行うことを可能にするものとして、データそのものを管理対象とする技術である DLP が注目されてきている。

DLP は発展途上の技術であり、対象とするデータの特定方法だけでも、キーワード方式、タグ方式、ハッシュ方式（フィンガープリント、シグネチャ等様々な呼び方がされる）など、複数の方式があり、またそれらを取り合わせて使うソリューションもある。このうち注目されているのがフィンガープリントと呼ばれる技術で、一種のハッシュ値を用いるが、対象とするファイルが部分的に変更されていても、その一部が抜き出されていても、一定範囲までは検知が可能と言われている。

典型的な DLP のシステムを例にとり、その構成と仕組みを解説する。この例では、DLP は以下の三つの構成要素からなる。

- パソコンに常駐するクライアントソフトウェアである「DLP エージェント」
- 機密データ登録や DLP エージェント監視を行うサーバソフトウェアである「DLP サーバ」
- ネットワークを流れるデータを監視する「DLP アプライアンス」

DLP エージェントはユーザが利用する端末にインストールされ、端末のシステム上に常駐する。この DLP エージェントによって、その端末で利用されるデータを監視し、DLP サーバに登録されている機密データが外部に漏れないようする。この機能を利用し、同一ポリシーが実装されている端末間でのデータの交換は許容するが、外部メディアへの書出しやメールへの添付などを制限する。

DLP サーバは，機密データを DLP エージェントが認識できるようにポリシーを登録、配布する役割を担う。ファイルサーバの共有フォルダにある機密データを DLP サーバに登録すると，DLP サーバは登録した機密データの「フィンガープリント」を生成し、そのデータの管理を始める。

DLP アプライアンスは，オフィスネットワークを流れるデータを監視する機能を持つ。このアプライアンスは、DLP エージェントがインストールされていない端末や，DLP エージェントソフトが対応していない OS で動作する端末がある場合にも DLP による保護機能を利用できるようにするために設置する。ただし，DLP アプライアンスで保護できるのは，ネットワーク上を流れる機密データに限定される。

このようなシステムを導入することで、マルウェアに感染した端末から機密データが漏えいすることを防ぐことが可能となる。また、イントラネット上で動くべきところでない所に動くべきでないデータが動いていることを検知し、権限外のアクセスや操作を把握することで事故を未然

に防ぐこともできる。そうすることで、チェックと承認のルールをやたら複雑にして業務効率を阻害するのではなく、事後的な検知と警告でコンプライアンスを定着させて行くことで情報保護と業務効率の両立を実現する効果も期待できる。

DLP を導入するに際しては、単にシステムを導入するだけでなく、組織内の文書やデータの重要度のランク付けと取扱いポリシーの整備が重要となる。導入に際してはドキュメント・コンサルティングとの連携が導入成功への鍵となるだろう。何の目的で、どこまでの情報を対象にして、どこまでの効果を期待するのかをあらかじめ明確にすることで、効果的な利用が可能になる。新しい技術をうまく活用することで、セキュリティ対策が更に進化することを期待したい。

11.6. 情報セキュリティのパラダイム拡大の動き（GRC とは）

情報セキュリティの要素として、CIA を指すことが一般化している。CIA とは、Confidentiality、Integrity、Availability の頭文字である。それぞれ日本語では機密性、完全性、可用性という語を充てるのが広い範囲での共通認識となっている。

CIA という「情報セキュリティの定義」は、古くは OECD のガイドライン、EU 指令等で用いられ、また BS7799 にも示され、そのまま ISO 基準である ISO/IEC27001 に継承されたことから、世界的な共通認識となっている。手元の辞書では英語の secure の語源は securus で、se（離れて）+cura（心配）+-us の合成で、心配のない状態を指す[66]。その用法から、概念としては、ものや場所や状態が、それがそのものとして一般に理解されている（共通認識として合意形成されている）位置、状態、属性、機能、動作、等が、その理解のとおりであり、それに外れることがない、ということが確保されている姿ではないかと推測される。このために、実は ISO/IEC27001 では情報セキュリティの定義として「情報の機密性、完全性及び可用性を維持すること」としつつ「さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい」としている。

このように情報セキュリティは、その基本要素としての CIA のみならず、それを適用し実践する組織の目的、目標や必要に応じてその管理対象、管理策、管理目標を柔軟に設定し適用していけばよいことがわかる。

企業においては、近年、CIA を基本とする情報セキュリティは当然のこととして、企業統治（コーポレートガバナンス）が企業目的に照らして完全に機能している状態を確保するために、企業の事業プロセスが健全に維持されることを目指した内部統制、それを支える IT 統制あるいは IT ガバナンス、そして IT ガバナンスの中核をなす情報セキュリティガバナンスというコンテクストにおいて情報セキュリティが捉え直されつつある。

企業という組織体かつ運動体にとって、情報セキュリティ、企業統治、対社会説明責任を含む CSR（Corporate Social Responsibility）=企業の社会的責任=が、かつてないほど問われている。企業活動を通じて実現される、製品やサービスの社会的効用の発揮、社会の一員としての役割の分担引き受けは無論として、そのプロセスが法律をはじめとする社会規範に適合することや、社会の構成・推進要素としての存在の継続性、そしてそれらを安定的に維持推進でき

[66] プログレッシブ英和中辞典（小学館）

るためのリスク対応体制までの備えが問われ始めている。

これらの要件を整理して、GRC という新たな 3 語の頭文字が語られ出している。それは各々ガバナンス（Governance）、リスクマネジメント（Risk Management）、コンプライアンス（Compliance）を意味する。

ガバナンス（Governance）は企業統治と訳される。企業がその事業目的に向かって保有する資源を最大限活用することと、その活用プロセスが企業目的に沿って無駄なく推進されること、それを阻害する社内の個人や組織の動きが排除され矯正されて企業目標に統合されること、を意味する。企業統治は会計的数値を軸に管理される要素が強い。会計的数値の“セキュリティ”を保証するのは IT 統治でありそれを支える情報セキュリティガバナンスである。情報セキュリティはガバナンスというコンテクストにおいて、更なる前向きの役割が求められている。

リスクマネジメント（Risk Management）は企業の存続可能性とコンプライアンスの保全の意味を担っている。リスクとは本来の意味の“セキュリティ”が想定している通常状態を逸脱して企業に迫る異常事態と、それがもたらすマイナスインパクトを指す。リスクマネジメントとは、リスクの発生を想定しそれがもたらすインパクトを事前評価して、発生時のインパクトをコントロールすると共に、通常状態に復するまでのプロセスを司るシナリオである。通常外の事態への対応をあらかじめプログラムして、組織とその活動の継続性を担保する仕組みがリスクマネジメントであり、広い意味で捉えられるセキュリティの一環と言える。

コンプライアンス（Compliance）は、より社会的関わりの中で意識されるテーマである。企業組織が社会の構成員である限りにおいて、社会的規範を遵守する主体であることは必然の要求事項であり、社会からの期待でもある。それを満たして初めて、社会の構成員としての責務を全うすることになり、社会の一員としての企業の存在意義が認められることになる。この意味で、企業存在の社会的コンテクストにおける“セキュリティ”のアジェンダの一つとして、コンプライアンスが改めて提起されている。

経済産業省は、2004 年度に情報セキュリティガバナンスのコンセプトを示し、情報セキュリティベンチマーク、事業継続計画ガイドライン、情報セキュリティ報告書モデルを提起した。これは GRC の先駆け的提起と解釈することも可能である。このように情報セキュリティガバナンスの目指すところと GRC の意味するところの共通性が確認できれば、両者の目指すところの究極は、ゴーイングコンサーンであり社会の一員である企業組織の「セキュリティ」の貫徹という表現で括ることができる。

このような位置付けにおいて、企業にとっての GRC は、情報セキュリティの新たな地平を示す言葉として注目に値する。

12. まとめ

情報セキュリティは、その必要性の理解を得るのに苦労した時代を経て、経営管理とリスク対応の重要な要素としての認識が急速に高まり、社会的アジェンダとして定着した。需要側の確立に対応して、供給側は IT 産業、コンサルティング、教育、専門サービスなど様々な業態が情報セキュリティのツール、サービス、ソリューションを提供し、一つの産業と言える規模にまで拡大している。その一方で、情報セキュリティを取り巻く状況は次のように一層複雑化し、「安全」という意味で「改善」が進んでいるとは言えない状況にある。

- ネットワーク脅威の一層の深刻化（攻撃の頻度、質的高度化）と複雑化
- ネットワーク犯罪目的の、自己顕示･愉快犯から経済的利潤への明確な変質
- 組織内部における情報の窃盗、紛失、誤操作など、故意や不作為、不注意に起因する情報漏えいリスクの拡大と深刻化
- 内部統制、事業継続管理、法令遵守といった経営管理の視点から、情報セキュリティガバナンスを目指す情報セキュリティ対策の必要性とその経営的意味の認知が進展

これらが企業の情報セキュリティ対策を一層促し、市場を拡大するための大きな原動力となっていると見られる。ウイルス対策やファイアウォールの導入が情報セキュリティ対策と思われた時代から、ISMS 認証やプライバシーマークの取得件数の増加によって裏付けられるような、管理面での対応・対策の強化にまで厚みを増してきた流れを読み取ることもできる。さらに、内部統制や事業継続管理の視点も意識され、企業の経営レベルでのリスクマネジメントの中核的課題へと、経営視点での位置付けは確実に進化している。本報告書で見てきた様々な要因、技術、経営管理、政策対応のそれぞれの面からの推進要因が情報セキュリティ問題の本質に対する認識を進め、市場の拡大を加速してきたと考えられる。

ネットワーク脅威や情報漏えいへの受身の防御から、情報セキュリティガバナンス、IT 統制、内部統制、事業継続管理、そしてコーポレート・ガバナンスへと連携する総合的な経営管理の一環へと昇華することで、情報セキュリティは単なる守りの位置付けから、企業価値を守り支え高める、積極的価値へと、その価値を大きく変化させた。

このような変化を背景に、国内の情報セキュリティ市場は、今後、よりバランスのとれた発展を遂げて行くものと期待される。そのことにより、情報セキュリティ産業もよりバランスの取れた姿で発展し、情報セキュリティ対策の高度化と充実に寄与することが期待される。

その一方で、ネットワークからの脅威やネットワークを手段として利用する犯罪の脅威は複雑さと巧妙さを増し、その対策に、ユーザ企業、セキュリティ対策を提供する企業、独立行政法人情報処理推進機構（IPA）や警察等の公的機関は対応に忙殺されていると言っても過言ではない。また情報セキュリティを経営の中に積極的に位置付けるという情報セキュリティガバナンスの視点はまだ一部の大企業の範囲に留まっており、中小規模の企業では、自前・自己責任での対策は引き続き荷の重いものがある。従って、社会的枠組の中で情報セキュリティの価値を積極的に評価し認知し、また支援する取組はまだまだ必要だと言える。

加えて、2008 年後半から急速に悪化し続けている世界の経済情勢は、日本の多くの企業にとっ

ても存続の危機であり、情報セキュリティはおろか事業の本体そのものの防衛が優先されざるを得ない状況にある。体力のある企業は経営管理の中核である IT とそのガバナンスの中核である情報セキュリティへの手当てを継続させる必要を理解し、最低限の手当てをする意思があるようだが、そこまでの体力や余裕のない企業においては優先順位が下がる恐れもある。

そのような中にあっても、組織運営と事業経営の基盤に直結する情報セキュリティは、中央政府、地方自治体、産業界、学界等、あらゆる社会経済主体がこれを支え推進して行く必要がある。それにより、より安全かつ信頼性の高い情報通信システム基盤と社会経済基盤が形成されることが望まれる。第 2 次情報セキュリティ基本計画が策定され、2009 年度からは第 1 次基本計画の成果を踏まえた、より進化した情報セキュリティ政策が進められることになっている。第 2 次情報セキュリティ基本計画では、政府機関・地方公共団体、企業共に情報セキュリティガバナンスの確立が重要な柱となっており、推進対策の確立と経営課題としての定着が求められている。また、産官学民の努力を引き続き傾注して、第 2 次情報セキュリティ基本計画が目指す世界トップクラスの IT 国家の実現と、事故前提型の、安心・安全なネットワーク社会の形成が、全社会の参画による取組の中で実現することを期待したい。

以上

【付録 1】英文字略語に関する簡単な説明

3A	Authentication, Authorization, Administration	Authentication（認証）、Authorization（認可）、Administration（管理）。アクセス管理における 3 大要素。”Administration”については”Access Control”とする説もある。
ACL	Access Control List	ネットワーク利用者のアクセス権限と、アクセス可能なシステム・ファイルなどのリスト。
ASP	Application Service Provider	一般に「ソフトの時間貸し」と呼ばれ、アプリケーションを販売することなく、インターネット上で利用させ、利用料に応じて課金するビジネスモデル、またはその事業者。
ATM	Automatic Teller Machine	現金自動預け払い機。
DLP	Data Loss Prevention Data Leak Protection	組織内の重要なデータを検知・追跡することで流出･漏えいを防ごうとする技術の呼称
DRM	Digital Rights Management	デジタル著作権管理。デジタルデータの著作権を保護する技術。複製の制限や、画像への電子透かしなどがこれにあたる。ビジネス上の文書に関しては、その閲覧、編集、複写、印刷等の操作を制限する等の管理を意味する場合がある。
e-Learning	e-Learning	パーソナルコンピュータやネットワークを利用した教育、遠隔地での教育や学習者の進度に合わせた教育が提供できるという利点がある。
FW	Firewall	組織内のネットワークが外部から侵入されることを防ぐシステムあるいは機器、ネットワークの界面に置かれ、特定のプロトコルだけを通過させることで制御を行う。
IA	Intel Architecture	米国半導体ベンダ Intel 社のマイクロプロセッサのアーキテクチャに互換性のあるマイクロプロセッサ。
ID	IDentifier	ユーザや各種リソースを一意に特定する論理要素、コンピュータシステムにおける認証の対象となる。
IDS	Intrusion Detection System	ネットワーク上を流れるパケットを分析し、不正アクセスと思われるパケットを検出して、管理者に通知するシステム。
IP	Internet Protocol	ARPANET で開発されたプロトコルで、OSI 参照モデルの第 3 層（ネットワーク層）に位置する。
IPA	Information-technology Promotion Agency	独立行政法人情報処理推進機構。ソフトウェア及び情報処理システムの安全で健全な発展を技術、人材の面から支えることを目的とする経済産業省所管の独立行政法人。
IPS	Intrusion Prevention System	サーバやネットワークへの不正侵入を阻止するシステム。IDS の機能を拡張し、侵入を検知するとリアルタイムで防御を実行する。
ISMS	Information Security Management System	組織レベルの情報セキュリティを確保するために、リスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用すること。情報セキュリティポリシーに基づき、PDCA サイクルを継続的に繰り返すことができる組織能力。

		こうした能力を備えた組織を認定するため、財団法人日本情報処理開発協会（JIPDEC）が認定機関となり「ISMS適合性評価制度」が実施されている。現在のISMS認証基準 ver2.0では、英国の情報セキュリティ認証規格「BS7799-2：2002」と、国内規格「JIS X 5080：2002（ISO／IEC　17799：2000)」との互換性を確保している。
IT	Information Technology	情報通信技術。
PC	Personal Computer	個人で占有利用する低価格の小型コンピュータ、狭義にはIntel互換CPUを持ち、WindowsをOSとして採用するものを指す。
PIN	Personal Identification Number	ICカードやワンタイムパスワードに使用する時に用いる個人用識別番号。「暗証番号」とほぼ同義。
PKI	Public Key Infrastructure	公開鍵暗号による電子認証基盤技術。
SaaS	Software as a Service	ソフトウェアをネットワーク上でその機能を利用することによりサービスとして提供するビジネスモデル
SaaS	Security as a Service	セキュリティに関する運用･監視やフィルタリング等の機能をオンラインで提供するサービスモデル
SOC	Security Operation Center	遠隔地でのセキュリティ運用監視サービスにおけるオペレーションセンター。
SI	Systems Integration	ユーザの業務に合わせた情報システムを設計、構築すること。SIerはSIを提供する事業者
SSL	Secure Socket Layer	暗号を用いセキュリティを確保した通信用プロトコル。HTTP通信でセキュリティを確保する場合に広く使われている。
TCP	Transmission Control Protocol	インターネットで利用される標準プロトコルで、OSI参照モデルのトランスポート層にあたる。ネットワーク層の IP と、セッション層よりも上位のプロトコル（HTTP、FTP、SMTP、POPなど）の橋渡しをする。
URL	Unique Resource Locator	インターネット上の文書、画像などの資源を一意に特定するための記述方法。
USB	Universal Serial Bus	パーソナルコンピュータと周辺機器を接続するための接続装置及び通信規格。
VPN	Virtual Private Network	通信事業者の提供する広域IP通信網上に構築された仮想私設通信網。通信相手と仮想的なトンネルをつくることで、プライベートアドレスによる通信や、TCP／IP以外のプロトコルによる通信も可能となる。また、データを暗号化することで、通信の秘匿性を確保する。

【付録 2】アンケート調査表サンプル

平成20(2008)年度　国内情報セキュリティ市場実態調査

情報セキュリティ市場調査票

2008年11月7日

特定非営利活動法人　日本ネットワークセキュリティ協会

本調査について

国内情報セキュリティ市場実態調査にご協力いただき有難うございます。

本調査は経済産業省の委託事業の一部を請け負う形で、日本ネットワークセキュリティ協会(JNSA)が実施するものです。

調査票は1～5まであります。下記の回答要領をご参照のうえ、各調査票の質問に沿ってご回答ください。

本調査票が、本件対象データの所管部署以外に送達された場合は、恐れ入りますがご担当部署にご回送くださいますようお願いします。

調査対象データについて

1．調査対象基準年度

- 調査対象基準年度を2007年度（2007年4月～2008年3月）としています。大半の企業で3月決算を採用しておられると考え、その年度の実績額をお聞きしています。決算期の異なる企業も、極力この期間に対応した数字をご回答いただけるよう、ご協力をお願いします。
- この期間に合わせた数字の算出が困難な場合は、これに最も近い決算期における、過去1年間の数値をご回答下さい。その場合、調査票に期間を明記下さい。
- この基準年度に対し、その前年度の実績ならびに翌年度、翌々年度の計画・予想数字をお伺いします。
- いずれの数字も、厳密な、あるいは正確な数値の算出や提出が困難な場合は、概算値等、推定値や丸めた数字でも結構ですから、できるだけ金額数字でご記入くださるよう、お願いします。

2．調査区分

- 情報セキュリティに関するツール（ハードウェア製品、ソフトウェア製品）とサービスに区分し、それぞれを提供する機能別に分類してツール･サービスの分類定義を行っています。
- 提供されている、あるいは取り扱われているツールやサービスの主たる機能や用途をこの分類に合わせて頂き、最も近い分類に該当する数値をご記入下さい。
- 関連する情報として、事業の方向性や市場動向の観測、ご意見等をお聞きしています。分析の参考情報として活用させていただきたく、併せてご回答にご協力をお願いします。（調査票5）

3．回答数値について

- **回答数値については、正確な算出が困難な場合は、概数等でも結構ですので、できるだけ金額ベースでご回答をお願いします。**
- 金額の基準は、回答企業からの出荷額ベースで算出下さい。

ご回答データの取扱い

- 本調査にご回答いただいた情報は、全て統計処理の上使用します。個別の記入内容については、事務処理の委託先に対して、守秘契約を締結の上統計処理を依頼するほかは、外部への提供、開示、公表等は一切いたしません。
- また、今回の調査結果は、本調査の目的以外には一切使用いたしません。
- 個別の調査票は、当協会にて厳重に管理し、不要になれば適切に処分します。
- ご回答いただいた方の個人情報は、(1)回答内容の確認、(2)調査結果の通知、および、(3)調査結果報告書の送付以外の目的での使用はいたしません。また、委託元の経済産業省を含め、第三者への委託・提供は一切行ないません。本事業終了後は、適切に廃棄いたします。

電子ファイルのご利用について

- 本件回答の作成を電子的に処理されたい場合は、電子ファイルをご提供します。以下のURLからExcel形式のファイルをダウンロードしてご利用下さい。

http://www.jnsa.org/market_research/index.html

- その場合も、データの秘密保護のため、ご回答の送付に際しては、記入済みのファイルを全頁印刷の上、同封の返信用封筒にてご返送下さい。

調査結果のご提供について

- 集計対象として利用可能なデータをご回答いただいた調査先に対しては、本調査報告書が経済産業省から公表された時点で、そのURLをお知らせし、またJNSAが作成する報告書冊子を1部ご提供させていただきます。
- ご希望の方は調査票1．の解答欄にご記入ください。

回答期限：

2008年12月5日（金）までに、返信用封筒にてご投函ください。

お問い合わせ先

特定非営利活動法人　日本ネットワークセキュリティ協会

（以下略）

調査票1、企業の概要　　記入日：2008年＿＿＿＿月＿＿＿＿日

問1．ご回答者についてお尋ねいたします。以下の設問についてご記入ください。

(1)企業名				
(2)本社所在地	〒			
(3)調査票回答 ご担当者	**所属部署：**			
	氏名：		**お役職：**	
	ご住所（本社と異なる場合のみ）：			
	電話番号：			
	メールアドレス：			

問2．御社の概要をお尋ねいたします。以下の設問についてご記入ください。

(1)資本金		**（百万円）**		
(2)従業員数		**（人）**		
(3)直近年度の 全社売上高	A．対象年度：	＿＿＿＿年＿＿＿＿月 ～ ＿＿＿＿年＿＿＿＿月		
	B．全社売上高と成長率	全社売上高	**（百万円）**	前年度比伸び率 ．（%）

※(3)は「売上高」が該当しない場合は、事業規模の指標となる数値をお答えください。

問3．経済産業省において報告書が公開された場合、JNSAより案内を受け取ることを希望されますか。
また、アンケートにご協力いただいた方には、JNSA発行の報告書冊子をお送りいたします。
報告書冊子の送付を希望されますか。下記のいずれかに○をお付けください。
なお、本件で「希望する」を選択された場合は、ご連絡に上記問1.の個人情報を使用いたします。

平成20(2008)年度調査結果に関する通知を	1．希望する (問1に必ずご記入ください)	2．希望しない
平成20(2008)年度調査結果報告書の送付を	1．希望する (問1に必ずご記入ください)	2．希望しない

調査票2. セキュリティ事業の売上高及び事業別概要

問4. 御社の直近年度の**セキュリティ事業**の(1)**売上高**ならびに**全社売上高に占める割合**および(2)**前年度比伸び率**をご記入ください。

直近年度の セキュリティ事業の売上高 (調査票1. 問2(3)と同年度)	(1)セキュリティ事業売上高 (または 全社売上高に占めるセキュリティ事業売上高の割合)				(2)前年度比伸び率
	セキュリティ事業売上高	(百万円)	全社売上高に占める割合	. (%)	. (%)

※別紙のセキュリティ製品・サービス市場区分の定義をご参照いただき、情報セキュリティ事業に該当すると考えられる事業についてご記入ください。
ただし、御社で独自に情報セキュリティ事業を定義しておられる場合は、その定義に基づくデータで結構です。

問5. 御社のセキュリティ事業の概要につきお聞きします。下記の区分における(1)事業規模ならびに(2)成長率について、**当てはまる記号**をお答えください。

事業の分類は、別紙のセキュリティ製品・サービス市場区分の定義をご参照いただき、できるだけこれに沿った仕訳をしていただけるようお願いします。

厳密な数字に基づくものでなくても、感覚ベースでも結構ですので、該当すると思われる**記号**をご記入ください。

◎事業規模の金額区分	
1	500万円以下
2	500万円～1000万円以下
3	1000万円～3000万円以下
4	3000万円～5000万円以下
5	5000万円～1億円以下
6	1億円～3億円以下
7	3億円～5億円以下
8	5億円～10億円以下
9	10億円超

◎事業の成長率区分	
A	－20%以下
B	－20%～－10%程度
C	－10%～ －5%程度
D	－5%～ －0%程度
E	±0%程度
F	0%～ ＋5%程度
G	＋5%～ ＋10%程度
H	＋10%～ ＋20%程度
I	＋20%以上

事業規模ならびに成長率の概要		(1)事業規模	(2)成長率		
		2007年度	2007年/2006年成長率(実績)	2008年/2007年成長率(見通し)	2009年/2008年成長率(予測値)
セキュリティ製品	統合型アプライアンス				
	ネットワーク脅威対策製品				
	コンテンツセキュリティ対策製品				
	アイデンティティ・アクセス管理製品				
	システムセキュリティ管理製品				
	暗号製品				
セキュリティ製品 合計					
情報セキュリティサービス	情報セキュリティ・コンサルテーション				
	セキュアシステム構築サービス				
	セキュリティ運用・管理サービス				
	情報セキュリティ教育				
	情報セキュリティ保険				
情報セキュリティサービス 合計					

調査票3. 取扱い製品分野及び製品名

問6. 御社が国内で販売されているセキュリティツール製品についてお伺いします。

（1）御社が国内市場で販売されているセキュリティツール製品が該当する区分に、分類表に従って「取扱有無」欄に○をお付けください。

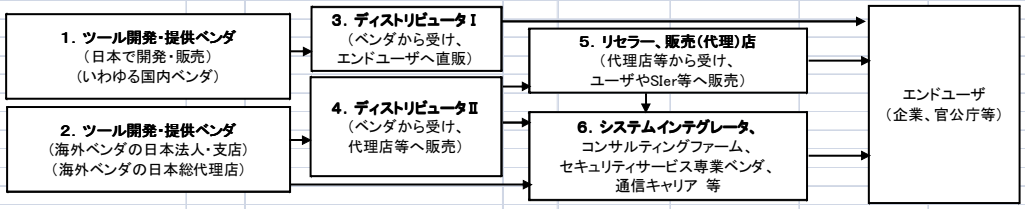
（2）（1）で○を付けられた製品分類ごとに、主要製品名を「製品名」欄にご記入ください。複数の場合は、可能な限りご記入ください。

（3）（1）で○を付けられた製品分類ごとに、御社の流通上のお立場について、図1を参照いただき、各分類の主力製品について1～6のうち最もよく当てはまる番号を1つ「流通上の立場」欄にご記入ください。

（4）（1）で○を付けられた製品分類に対応する、御社取扱い製品の直近年度（表紙　問2（3）でご記入いただいた年度）の国内売上高をご記入ください。
集計区分の差異、決算期のずれ、見込み数字が未確定、開示に関するポリシー等のために正確な数字の記入が難しい場合は、概数でも結構です。また、売上額等を非開示の場合でも、総合計金額と各大分類・中分類の構成比（%）のような形での開示が可能であれば、その形式によっていただいても結構です。

※　御社が国内でセキュリティツール（製品）を販売されていない場合は、調査票4へお進み下さい。

図1　製品の流通図



（回答欄）

大分類	中分類	（1）取扱有無	（2）代表的なツール（製品）名称	（3）流通上の立場	（4）販売額 2006年度（2007年3月期）売上実績（百万円）	（4）販売額 2007年度（2008年3月期）※下記、実績/割合のいずれかをご記入ください 売上実績（百万円）	（4）販売額 2007年度（2008年3月期）※下記、実績/割合のいずれかをご記入ください セキュリティ事業全体に占める割合（%）	（4）販売額 2008年度売上計画額（百万円）	（4）販売額 2009年度売上計画額（百万円）
統合型アプライアンス　合計		－	－	－					
	統合型アプライアンス								
ネットワーク脅威対策製品　合計		－	－	－					
	ファイアウォール・アプライアンス								
	ファイアウォール・ソフトウェア（企業向けライセンスタイプ）								
	ファイアウォール・ソフトウェア（デスクトップFW）								
	VPNアプライアンス								
	VPNソフトウェア								
	IDS／IPSアプライアンス								
	IDS／IPSソフトウェア								
	アプリケーションファイアウォール								
	その他のネットワーク脅威対策製品								

大分類	中分類	(1)取扱有無	(2)代表的なツール(製品)名称	(3)流通上の立場	(4)販売額				
					2006年度(2007年3月期)売上実績(百万円)	2007年度(2008年3月期) ※下記、実績/割合のいずれかをご記入ください		2008年度売上計画額(百万円)	2009年度売上計画額(百万円)
						売上実績(百万円)	セキュリティ事業全体に占める割合(%)		
コンテンツセキュリティ対策製品 合計		–	–	–					
	ウイルス・不正プログラム対策ソフトウェア(企業向けライセンス契約)/アプライアンス								
	ウイルス・不正プログラム対策ソフトウェア(個人ユーザ向けパッケージタイプ)								
	スパムメール対策ソフトウェア/アプライアンス								
	フィッシング対策ソフトウェア/システム								
	URLフィルタリングソフトウェア/アプライアンス								
	メールフィルタリングソフトウェア/アプライアンス								
	その他のコンテンツセキュリティ対策製品								
アイデンティティ・アクセス管理製品 合計		–	–	–					
	個人認証用デバイス及びその認証システム								
	個人認証用生体認証デバイス及びその認証システム								
	アイデンティティ管理製品								
	ログオン管理/アクセス許可製品								
	PKIシステム及びそのコンポーネント								
	その他のアイデンティティ・アクセス管理製品								
システムセキュリティ管理製品 合計		–	–	–					
	セキュリティ情報管理システム/製品								
	脆弱性検査製品								
	ポリシー管理・設定管理・動作監視制御製品								
	その他のシステムセキュリティ管理製品								
暗号製品 合計		–	–	–					
	データ暗号化製品								
	暗号化ミドルウェア								
	その他の暗号製品								
セキュリティ製品売上高 総合計		–	–	–					

調査票4. 提供しているサービス分野

問7. 御社が国内で提供されている情報セキュリティに関するサービスについてお伺いします。

（1）御社が国内市場で提供されている情報セキュリティサービスが該当する区分に、分類表に従って「提供サービス分野」欄に○をお付けください。

（2）（1）で○を付けられたサービス分類ごとに、商品名称をお持ちの場合は、主要商品名を「提供サービスの商品名」欄にご記入ください。 複数の場合は、可能な限りご記入ください。

（3）（1）で○を付けられたサービス分類に対応する、御社提供サービスの直近年度（表紙 問2（3）でご記入いただいた年度）の国内売上高をご記入ください。集計区分の差異、決算期のずれ、見込み数字が未確定、開示に関するポリシー等のために正確な数字の記入が難しい場合は、概数でも結構です。また、売上額等を非開示の場合でも、総合計金額と各大分類・中分類の構成比（%）のような形での開示が可能であれば、その形式によっていただいても結構です。

※ 御社が国内で情報セキュリティサービスを提供されていない場合は、調査票5へお進み下さい。

（回答欄）

大分類	中分類	（1）取扱有無	（2）提供するサービスの商品名・呼称等	流通上の立場	（3）販売額				
					2006年度（2007年3月期）売上実績（百万円）	2007年度（2008年3月期）※下記、実績/割合のいずれかをご記入ください		2008年度売上計画額（百万円）	2009年度売上計画額（百万円）
						売上実績（百万円）	セキュリティ事業全体に占める割合（%）		
情報セキュリティ・コンサルテーション 合計		－	－	－					
	情報セキュリティポリシー構築支援								
	情報セキュリティ管理全般のコンサルテーション								
	情報セキュリティ診断・監査サービス								
	情報セキュリティ関連規格認証取得等支援サービス								
	情報セキュリティ関連認証・審査・監査機関（サービス）								
	その他の情報セキュリティコンサルテーション								
セキュアシステム構築サービス 合計		－	－	－					
	ITセキュリティシステムの設計・仕様策定								
	ITセキュリティシステムの導入・導入支援								
	セキュリティ製品の選定・選定支援								
	その他のセキュアシステム構築サービス								

大分類	中分類	（1）取扱有無	（2）提供するサービスの商品名・呼称等	流通上の立場	（3）販売額				
					2006年度（2007年3月期）売上実績（百万円）	2007年度（2008年3月期）※下記、実績/割合のいずれかをご記入ください 売上実績（百万円）	2007年度（2008年3月期）※下記、実績/割合のいずれかをご記入ください セキュリティ事業全体に占める割合（%）	2008年度売上計画額（百万円）	2009年度売上計画額（百万円）
セキュリティ運用・管理サービス 合計		－	－	－					
	セキュリティ総合監視・運用支援サービス								
	ファイアウォール監視・運用支援サービス								
	IDS／IPS監視・運用支援サービス								
	ウイルス監視・ウイルス対策運用支援サービス								
	フィルタリングサービス								
	脆弱性検査サービス								
	セキュリティ情報提供サービス								
	電子認証サービス								
	インシデント対応関連サービス								
	その他の運用・管理サービス								
情報セキュリティ教育　合計		－	－	－					
	情報セキュリティ教育の提供サービス								
	情報セキュリティ教育のe-ラーニングサービス								
	情報セキュリティ関連資格認定及び教育サービス								
	その他の情報セキュリティ教育サービス								
情報セキュリティ保険　合計		－	－	－					
	情報セキュリティ保険								
情報セキュリティサービス売上高総合計		－	－	－					

調査票5　国内情報セキュリティ市場の動向等についてのご質問

問8. 最後に、情報セキュリティ市場に関してご質問をさせていただきますので、ご回答をお願いいたします。

（1）2007年度における国内セキュリティツール製品全体の市場規模は前年比で、どのように変化したとお考えでしょうか。以下の1～5のうち最もよく当てはまるものに1つ○をお付けください。

1	2	3	4	5
減少（−20%以上）	微減（−20%未満）	変化なし（5%内の増減）	微増(20%未満）	増加（20%以上）

（2）2007年度における国内セキュリティサービス全体の市場規模は前年比で、どのように変化したとお考えでしょうか。以下の1～5のうち最もよく当てはまるものに1つ○をお付けください。

1	2	3	4	5
減少（−20%以上）	微減（−20%未満）	変化なし（5%内の増減）	微増(20%未満）	増加（20%以上）

（3）2008年度における国内セキュリティツール製品の市場規模は、どのように変化するとお考えでしょうか。以下の1～5のうち最もよく当てはまるものに1つ○をお付けください。

1	2	3	4	5
減少（−20%以上）	微減（−20%未満）	変化なし（5%内の増減）	微増(20%未満）	増加（20%以上）

（4）2008年度における国内セキュリティサービスの市場規模は、どのように変化するとお考えでしょうか。以下の1～5のうち最もよく当てはまるものに1つ○をお付けください。

1	2	3	4	5
減少（−20%以上）	微減（−20%未満）	変化なし（5%内の増減）	微増(20%未満）	増加（20%以上）

（5）以下のセキュリティビジネス分野において、①御社が今後注力しようとしている分野、②ユーザが現在最も関心を寄せている分野、③今後セキュリティビジネスで成長が期待できない分野はそれぞれどこだとお考えになりますか。①～③の各設問において、当てはまる分野に全て○をお付けください。

大分類	中分類	①今後注力しようとしている分野	②ユーザが関心を寄せている分野	③今後成長が期待できない分野
統合型アプライアンス	統合型アプライアンス			
ネットワーク脅威対策製品	ファイアウォール・アプライアンス			
	ファイアウォール・ソフトウェア（企業向けライセンスタイプ）			
	ファイアウォール・ソフトウェア（デスクトップFW）			
	VPNアプライアンス			
	VPNソフトウェア			
	IDS／IPSアプライアンス			
	IDS／IPSソフトウェア			
	アプリケーションファイアウォール			
	その他のネットワーク脅威対策製品（　　）			
コンテンツセキュリティ対策製品	ウイルス・不正プログラム対策ソフトウェア（企業向けライセンス契約）／アプライアンス			
	ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ）			
	スパムメール対策ソフトウェア／アプライアンス			
	フィッシング対策ソフトウェア／システム			
	URLフィルタリングソフトウェア／アプライアンス			
	メールフィルタリングソフトウェア／アプライアンス			
	その他のコンテンツセキュリティ対策製品（　　）			
アイデンティティ・アクセス管理製品	個人認証用デバイス及びその認証システム			
	個人認証用生体認証デバイス及びその認証システム			
	アイデンティティ管理製品			
	ログオン管理/アクセス許可製品			
	PKIシステム及びそのコンポーネント			
	その他のアイデンティティ・アクセス管理製品（　　）			

大分類	中分類	①今後注力しようとしている分野	②ユーザが関心を寄せている分野	③今後成長が期待できない分野
システムセキュリティ管理製品	セキュリティ情報管理システム／製品			
	脆弱性検査製品			
	ポリシー管理・設定管理・動作監視制御製品			
	その他のシステムセキュリティ管理製品			
暗号製品	データ暗号化製品			
	暗号化ミドルウェア			
	その他の暗号製品 （　　）			
その他のセキュリティツール・製品（　　）				
情報セキュリティ・コンサルテーション	情報セキュリティポリシー構築支援			
	情報セキュリティ管理全般のコンサルテーション			
	情報セキュリティ診断・監査サービス			
	情報セキュリティ関連規格認証取得等支援サービス			
	情報セキュリティ関連認証・審査・監査機関（サービス）			
	その他の情報セキュリティコンサルテーション （　　）			
セキュアシステム構築サービス	ITセキュリティシステムの設計・仕様策定			
	ITセキュリティシステムの導入・導入支援			
	セキュリティ製品の選定・選定支援			
	その他のセキュアシステム構築サービス （　　）			
セキュリティ運用・管理サービス	セキュリティ総合監視・運用支援サービス			
	ファイアウォール監視・運用支援サービス			
	IDS／IPS監視・運用支援サービス			
	ウイルス監視・ウイルス対策運用支援サービス			
	フィルタリングサービス			
	脆弱性検査サービス			
	セキュリティ情報提供サービス			
	電子認証サービス			
	インシデント対応関連サービス			
	その他の運用・管理サービス （　　）			
情報セキュリティ教育	情報セキュリティ教育の提供サービス			
	情報セキュリティ教育のe-ラーニングサービス			
	情報セキュリティ関連資格認定及び教育サービス			
	その他の情報セキュリティ教育サービス （　　）			
情報セキュリティ保険	情報セキュリティ保険			
その他のセキュリティサービス（　　）				

次ページにお進みください

（6）今後情報セキュリティ対策の普及・充実のために重要となる要素はどのようなものだとお考えでしょうか。政策面、技術面、経営面、社会面、文化面、その他　ご自由にご意見をご記入ください。

例：　政府のセキュリティ関連施策の充実、製品及びサービス提供者の啓蒙活動等

（7）最後に、本アンケート全般についてお気づきの点やご感想等がありましたら以下にご意見をご記入ください。本調査を、継続して定期的に実施する上での参考にさせていただきます。

＝　以上で質問は終了です。ご協力いただき誠に有難うございました。　＝

★回答用紙は同封の返信用封筒で**12月5日（金）**までに投函をお願い申し上げます。

情報セキュリティ市場調査報告書

2009 年 3 月 31 日

特定非営利活動法人　日本ネットワークセキュリティ協会

政策部会　セキュリティ市場調査ワーキンググループ

ワーキンググループリーダ

勝見　　勉　株式会社情報経済研究所

ワーキンググループメンバ（調査・執筆参加者）

市川　順之　伊藤忠テクノソリューションズ株式会社
岡本　英世　伊藤忠テクノソリューションズ株式会社
塩見　友規　オー・エイ・エス株式会社
風間　勇人　サイバーエリアリサーチ株式会社
森田　弥生　新日本有限責任監査法人
秋山　卓司　日本クロストラスト株式会社
金子　以澄　日本 CA 株式会社
光野　元彦　パスロジ株式会社
中木　篤郎　株式会社日立情報システムズ
佐藤　友治　ブロードバンドセキュリティ株式会社
長谷川長一　株式会社ラック

以上