2012 年度

情報セキュリティ市場調査報告書

２０１３年５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

はじめに

NPO 日本ネットワークセキュリティ協会（JNSA）では、2004 年度以来継続して、日本国内の情報セキュリティ市場の調査を実施している。このうち、2009 年度までは経済産業省委託事業として、以降は JNSA 独自の事業として行っている。2012 年度調査は、アンケート調査、個別推計調査、インタビュー調査、全体集計・推計調査等を踏まえ、途中見直し等もはさんで実施し、2013 年 5 月にとりまとめた。

情報セキュリティに対する社会の認知は 2011 年度以降、急速に広まっているように見える。2011 年度には、日本を代表する大企業の多くで、ハッキング被害や標的型攻撃による被害が顕在化した。また、衆参両議院においても不正侵入や情報の流出を許していたことが発覚した。これらの事件が情報セキュリティに対する一般の関心を喚起し、情報セキュリティの脅威や事件に関する報道が、テレビニュースや一般紙の社会面に登場するようになった。2012 年度に起きた遠隔操作マルウェアによる脅迫に関する誤認逮捕事件は、さらに大衆的関心を引くものとなり、情報セキュリティがお茶の間の話題にまで浸透してきていると言える。

また、米国にならって、日本の防衛においてもサイバー空間を第 5 の防衛対象領域と位置付ける決定が行われ、警察は 2013 年度から全国 13 の都道府県警レベルでサイバーセキュリティの専任捜査部隊を配置する等、安全保障や社会の安全の面からの認知・対応も本格化してきた。この背景には、ハクティビストによる主張に基づいた攻撃、産業スパイ活動、戦略的・地政学的背景に起因すると考えられる攻撃の顕在化、攻撃手段の多発化・悪質化という状況がある。認知は進む一方、脅威の度合いや深刻化も進んでいるのが実態と言える。

このような現状に対処するためには、まず第一に、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等、社会の安全安心を脅かす存在への防御が確立されなければならない。そして更に、企業経営のデータや営業秘密、知的財産等の情報資源を保護・活用し、企業の内部統制を充実して経営の質と透明性の維持向上を図り、付加価値と競争力を向上させるために確保されなければならない。IT を外部からの侵入や攻撃から守り、脆弱性に付け入られることを防ぎ、意図せざる利用や悪用に対して防衛するために手立てを尽くすことは、IT を正しく、合目的的に利活用することと表裏一体の行為である。

情報セキュリティ産業は、そのような努力・取組みを支える製品やサービスを提供し、日本の情報セキュリティ対策のバックボーンを担っていると言える。この調査は、その産業の規模と状況を示す調査である。日本の情報セキュリティ産業の活性化は、政策課題ともなっているように、情報セキュリティ対策の根幹をなす重要なテーマである。本調査結果が、産業や政府施策に活用され、情報セキュリティ対策のレベルアップに資することができれば幸いである。

※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。

※本調査では、情報セキュリティ市場を大きく「ツール」と「サービス」に分け、各々を大分類市場、中分類市場に体系的に区分している。以下の報告の中では、大分類市場区分を「カテゴリ」、中分類市場区分を「セグメント」と呼ぶ場合がある。

【第一部　情報セキュリティ市場調査結果】

第１章 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。図１には情報セキュリティツール、情報セキュリティサービスの区分による市場推移のグラフを示した。

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	2010年度（推定実績）		2011年度（推定実績）			2012年度（実績見込）			2013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	**664,264**	**100.0%**	**692,604**	**100.0%**	**4.3%**	**730,876**	**100.0%**	**5.5%**	**765,818**	**100.0%**	**4.8%**
情報セキュリティツール合計	**354,272**	**53.3%**	**364,807**	**52.7%**	**3.0%**	**384,566**	**52.6%**	**5.4%**	**404,954**	**52.9%**	**5.3%**
統合型アプライアンス	18,972	5.4%	19,208	5.3%	1.2%	20,107	5.2%	4.7%	21,146	5.2%	5.2%
ネットワーク脅威対策製品	48,535	13.7%	49,799	13.7%	2.6%	52,050	13.5%	4.5%	54,058	13.3%	3.9%
コンテンツセキュリティ対策製品	136,556	38.5%	138,995	38.1%	1.8%	146,756	38.2%	5.6%	154,506	38.2%	5.3%
アイデンティティ・アクセス管理製品	63,393	17.9%	65,392	17.9%	3.2%	68,857	17.9%	5.3%	71,801	17.7%	4.3%
システムセキュリティ管理製品	49,507	14.0%	51,679	14.2%	4.4%	55,102	14.3%	6.6%	58,864	14.5%	6.8%
暗号化製品	37,307	10.5%	39,734	10.9%	6.5%	41,694	10.8%	4.9%	44,579	11.0%	6.9%
情報セキュリティサービス合計	**309,992**	**46.7%**	**327,797**	**47.3%**	**5.7%**	**346,310**	**47.4%**	**5.6%**	**360,864**	**47.1%**	**4.2%**
情報セキュリティコンサルテーション	66,271	21.4%	67,928	20.7%	2.5%	70,150	20.3%	3.3%	72,181	20.0%	2.9%
セキュアシステム構築サービス	122,229	39.4%	129,116	39.4%	5.6%	138,821	40.1%	7.5%	144,389	40.0%	4.0%
セキュリティ運用・管理サービス	90,375	29.2%	98,071	29.9%	8.5%	103,092	29.8%	5.1%	109,163	30.3%	5.9%
情報セキュリティ教育	23,880	7.7%	25,185	7.7%	5.5%	26,601	7.7%	5.6%	27,332	7.6%	2.7%
情報セキュリティ保険	7,236	2.3%	7,497	2.3%	3.6%	7,647	2.2%	2.0%	7,800	2.2%	2.0%

今回調査の基準年度とした 2011 年度は、年度開始直前の 3 月 11 日に東日本大震災が発生し、津波による被害と原発事故の影響により、年度当初の社会的混乱と経済停滞が顕著な中でのスタートとなった。また、経済活動が復旧の手がかりをつかんだ矢先に、タイで大規模な洪水が発生し、進出した日本企業の多くが 10～11 月を中心に長期間の操業停止と被害に遭う等、環境の厳しい１年となった。

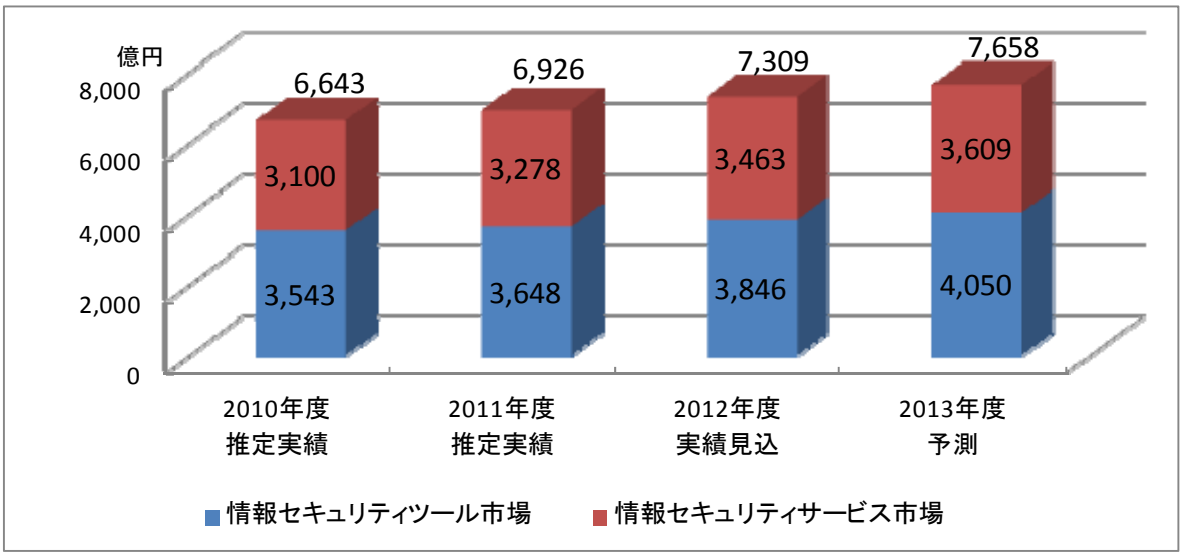
一方、4 月にはソニー本社および複数の海外子会社でハッカーによるサーバへの侵入と、顧客の個人情報流出の被害が発生した。流出した個人情報は１億人にも上り、世界的な衝撃をもたらした。また 9 月には三菱重工業をはじめとする防衛産業各社において、標的型攻撃によってネットワーク侵入を許し、技術情報等が流出したことが発覚した。その直後には、参議院、衆議院で

もネットワークへの不正侵入によりメールアドレスや電子メールが多数盗まれていることが見つかる等、サイバー攻撃による大規模もしくは深刻な被害の報道が相次いだ。

前回調査（2010-2011 年度情報セキュリティ調査報告書[1]）では、2008 年度半ばに世界経済を襲ったいわゆるリーマンショックとそれに伴う世界同時不況の影響で、経済成長が 2008, 2009 年度と停滞する中、2009 年度に国内情報セキュリティ市場はマイナス成長に陥ったとの報告をしている。これは、経済情勢の急速な悪化に加え、2008 年度までに対策が進んだことにより、投資が一巡しており、コンサルティングやセキュアシステム構築関連を中心に投資の抑制が起こったことによる。

2010 年度は経済統計上の実質 GDP は+3.1%と高い成長率となったものの、GDP デフレータは-2.0%とデフレ色が強く、欧州債務危機の暗雲が垂れこめて世界的に経済が不安定だった。このような中、情報セキュリティに対する投資・支出は、抑制基調が継続したとみられ、マイナス成長が続いた。特に第 4 四半期には、2011 年度にかけて新興国経済の堅調を背景に回復テンポが上ることが期待される中で東日本大震災が発生し、年度末に動くべき需要が急速に抑制されたという要因もあったとの指摘もある。情報セキュリティ対策は年度末の余剰予算が充てられる要素が大きく、それが起きなかったことを指摘するベンダの声も確認されている。それらの結果、2010 年度は市場規模の縮小が続き、「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 3,543 億円、「情報セキュリティサービス」が 3,100 億円、合計で 6,643 億円になったものと推定される。

図 1　国内情報セキュリティ市場規模の推移



2011 年度については、前回調査では年度前半に予測値をまとめ、その後年度後半段階で見直すことができていないために、東日本大震災の影響が大きく、マイナス成長が続くものとの予測結果となった。特に、IT と IT セキュリティの投資サイクル上は 2007~2008 年度の次の山に差し掛

[1] http://www.jnsa.org/result/2010/surv/mkr/index.html

かる時期に当っていたものの、先延ばしされる可能性が強いとの観測から、引き続きコンサルティングやセキュアシステム構築分野を中心にマイナス成長が持続するとの予測を固めた。

2011 年度の日本経済は、タイの洪水被害や欧州債務危機による混乱にもかかわらず、民間を中心とした復旧・復興努力の中で年度後半に急速に回復に向かっていた。そのような中で、衝撃的なインシデントが立て続けに起こった。標的型攻撃の脅威に関する啓発・警告が繰り返し行われていた中で、国際的企業が明確にターゲットにされる事態が、大企業に明示的に示され、認知されるにいたったと考えられる。また投資サイクルの面でも更新期を迎えるタイミングであった。こうしたことから、特に年度後半にかけて、情報セキュリティ対策を抜本的に見直す動きが相次いだ模様である（ベンダヒアリングによる）。その中で、セキュリティポリシーを始めとしてマネジメントシステムや体系を見直し、システムのセキュリティを再構築する取組みも多く見られたとの証言もいくつか得られている。

このような動きの結果、2011 年度の国内情報セキュリティ市場は、前回調査で予測したマイナスではなく、プラス成長を達成した模様である。2011 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」が 3,648 億円、「情報セキュリティサービス」が 3,278 億円、合計で 6,926 億円であったと推定される。前年度比伸び率は各々+3.0%、+5.7%、+4.3%となった。

2012 年度は欧州経済の不安定や米国経済の回復ペースが遅い中で円高が進行する展開となり、また化石燃料輸入が急増することで経常収支が大幅に赤字となる等、経済環境は厳しいものがあったが、前半に国内ではエコカー減税等に刺激された消費を中心にやや明るく推移したことや、急速に国際化を進める日本企業の海外での努力が成果を挙げる要素にも助けられて、年度実績見込みで実質 1.0%、名目 0.3%程度の成長率を確保した[2]。また 2012 年 12 月の安倍政権発足後は、アベノミクスと呼ばれる経済対策への期待から、円安・株高が進み、経済状況には明るさが萌している。また遠隔操作マルウェア事件のように一般社会を揺るがすサイバー事件の発生も、情報セキュリティ対策への意識を喚起する方向に働いた。

このような情勢下で、情報セキュリティ市場は 2011 年度に拡大に転じた流れを継続し、企業業績の回復にも後押しされて、プラス成長を達成したものと見込まれる。その規模と伸び率は、ツール：3,846 億円・+5.4%、サービス：3,463 億円・+5.6%、合計：7,309 億円・+5.5%程度になったものと見込まれる。

2013 年度は、アベノミクスと黒田総裁に替った日銀による大胆な金融緩和によって、経済は回復し、デフレも解消に向かうことが期待されている。年度当初の政府経済見通しは実質 2.5%、名目 2.7%という高い成長率を見込んでいる。このような経済情勢と、引き続きサイバー脅威への備えを充実させる経営判断が期待できることから、情報セキュリティ投資も継続し、市場は拡大するものと予測される。インタビュー調査においても、2012 年度並みの売上高成長を目指すとする企業が多かった。ただし、2011 年度、2012 年度と対策が進んできており、市場の拡大速度は 2012

[2] 政府経済見通しによる。http://www5.cao.go.jp/keizai1/mitoshi/2013/0228mitoshi.pdf

年度ほど速くなく、全体としては 4.8%の成長になると見た。

特にサービスについては、2011 年度、2012 年度に行われた抜本的見直しや積極的再構築が一段落することから成長速度は鈍化し、4.2%にとどまる。そのような中で企業収益の改善がアウトソース支出増加の容認につながりやすいことから「セキュリティ運用・管理サービス」が引き続き高い成長率を維持するものと予測される。一方、ツールについては IT 投資サイクル面で高い投資水準が期待できることに加え、Windows XP のサポート終了に伴う更新需要や、スマートデバイスの活用に向けた投資も期待されることから、それに伴うセキュリティ投資も堅調に推移すると考えられる。そのため、+5.3%と、ほぼ 2012 年度並みの成長率を維持するものと予測した。金額規模としては、ツールが 4,050 億円と初めて 4,000 億円台に達すると期待され、サービスも 3,609 億円と、本統計開始以来の規模に達するものと予測される。その結果、情報セキュリティ市場合計では 4.8%と高い成長率を維持して、7,658 億円という規模にまで拡大すると期待される。

このように、リーマンショックとそれに引き続く世界同時不況、そして東日本大震災、タイ大洪水、欧州債務危機と続いてきた逆境下で、2010 年度までは 2 年間落ち込みが続いたものの、情報セキュリティ対策に振り向けるお金の面では、経済の回復に先駆けて 2011 年度から回復の歩みが続いていると見られる。2013 年度は今のところ経済的には明るい話題が増えており、情報セキュリティ市場も、はじめて到達した 7,600 億円規模から、8,000 億円を目指す動きとなることが期待される。

第２章 国内情報セキュリティ市場調査結果の詳細とその分析

2.1. 国内情報セキュリティツール市場の分析

2.1.1. 情報セキュリティツール市場の全体概要

表 2 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、2011 年度の国内「情報セキュリティツール」市場は、3,648 億円の規模であったと推測される。前回調査では、2008 年度をピークとして 2010 年度まで落ち込みを見込み、2011 年度も足踏み状態にとどまると見られていたが、大規模サイバー被害等を契機に回復に向かい、3.0%程度の成長を確保した模様である。

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」、「暗号化製品」の 6 カテゴリに分けた。各カテゴリの定義・内容は第 5 章に詳述した通りである。

表 2　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

年度別売上高推計値	2010年度		2011年度			2012年度			2013年度		
セキュリティ・ツール	売上実績推定値		売上実績推定値			売上高見込推定値			売上高予測値		
	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	18,972	5.4%	19,208	5.3%	1.2%	20,107	5.2%	4.7%	21,146	5.2%	5.2%
ネットワーク脅威対策製品	48,535	13.7%	49,799	13.7%	2.6%	52,050	13.5%	4.5%	54,058	13.3%	3.9%
コンテンツセキュリティ対策製品	136,556	38.5%	138,995	38.1%	1.8%	146,756	38.2%	5.6%	154,506	38.2%	5.3%
アイデンティティ・アクセス管理製品	63,393	17.9%	65,392	17.9%	3.2%	68,857	17.9%	5.3%	71,801	17.7%	4.3%
システムセキュリティ管理製品	49,507	14.0%	51,679	14.2%	4.4%	55,102	14.3%	6.6%	58,864	14.5%	6.8%
暗号化製品	37,307	10.5%	39,734	10.9%	6.5%	41,694	10.8%	4.9%	44,579	11.0%	6.9%
セキュリティツール市場合計	354,272	100.0%	364,807	100.0%	3.0%	384,566	100.0%	5.4%	404,954	100.0%	5.3%

図 2 に 2011 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。

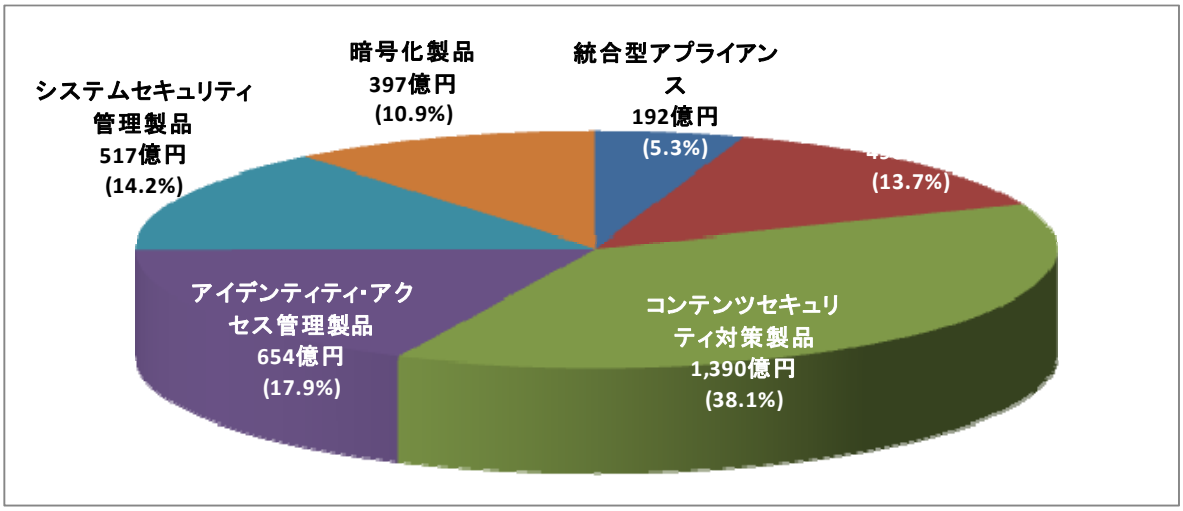
情報セキュリティツール市場において最大のカテゴリである「コンテンツセキュリティ対策製品」の 2011 年度の市場規模は 1,390 億円で、ツール市場全体に占める割合は 38.1%であった。これに次ぐ規模の市場カテゴリは「アイデンティティ・アクセス管理製品」で 654 億円、構成比で 17.9%であった。第 3 位は 2010 年度から順位が入れ替わり、「システムセキュリティ管理製品」が 517 億円で 14.2%を占めた。外部からのネットワークへの不正侵入・不正アクセス対策を担う「ネットワーク脅威対策製品」と「統合型アプライアンス」は、各々498 億円・13.7%、192 億円・5.3%で、合計すると 690 億円・19.0%となる。主としてデータそのものの保護を提供する「暗号化製品」市場は 397 億円・10.9%となった。

ここ数年のすう勢として、以下のことが観測される。

1) セキュリティ対策手段としてクライアント PC まで広く展開する必要があり導入も進んでいる、ウイルス対策を中心とする「コンテンツセキュリティ対策製品」は、普及率が高いため規模が大きく、また成長率は限られるが着実に拡大している。

2) 外部ネットワークからの脅威に対する備えである「ネットワーク脅威対策製品」と「統合型アプライアンス」も比較的導入の進んだ対策手段であるが、一度導入すると次の投資まで数年のインターバルが開くこともあり、サイクルの谷に当った年等は、時として落ち込みを見せる。

図 2　2011 年度の国内情報セキュリティツール市場



3) 内部管理、特にシステムやファイルへのアクセス権の管理は、内部統制報告制度（いわゆる J-SOX）施行を契機に導入が進み、市場拡大速度を速めて 2 番目に大きいセグメントとなった。

4) 標的型脅威等、内部ネットワークへの侵入防止が困難となってきた今日の情勢を踏まえ、内部ネットワークの監視や解析、診断を行う「システムセキュリティ管理製品」も伸び率を高めている。このカテゴリには他に、端末のインベントリ・パッチ適用状態・設定等のコンプライアンス状態等を管理する製品やネットワーク検疫製品、さらにはセキュリティ目的のログ解析製品等、内部統制・情報漏えい・標的型攻撃への対応で需要が高まった製品が多く含まれ、高い伸び率を支えていると見られる。

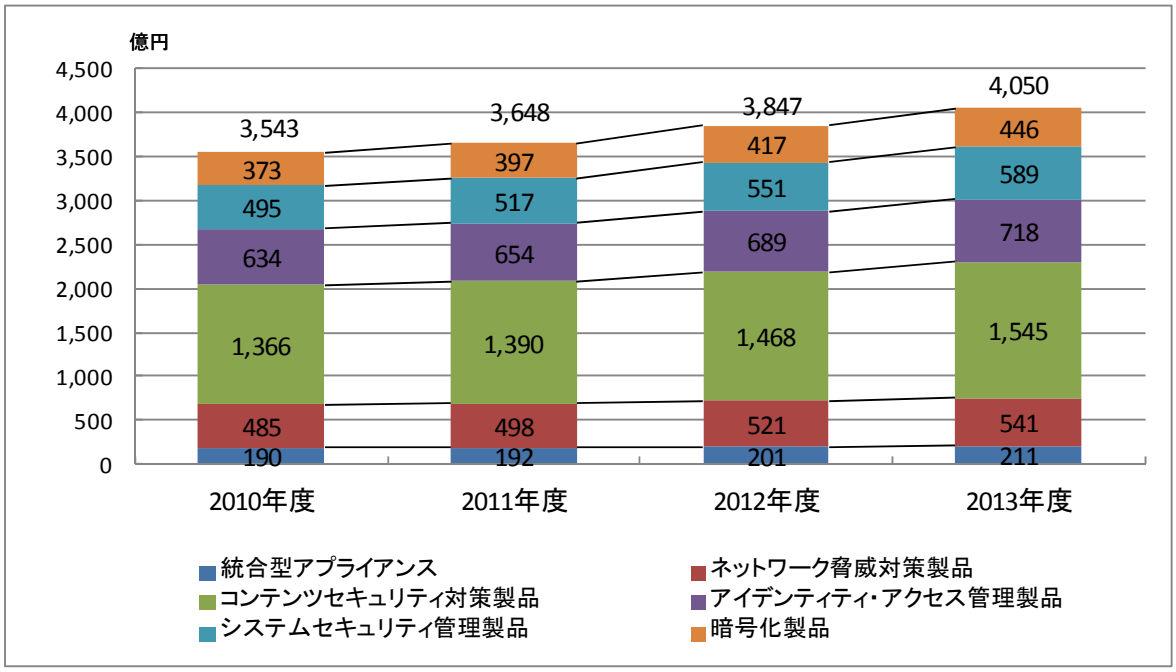
5) 暗号化製品は、内部脅威や外部脅威によってファイルの流出等が起きても、データそのものを保護し、見られたり悪用されたりといったことを防止するニーズの高まりから、やはり市場規模の拡大速度を高めている。

図 3 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。

2010 年度の日本経済は、2008 年度の半ばに始まったリーマンショックを契機とする世界同時不況の影響により、2009 年度が実質 2.0%のマイナス成長（政府経済統計）であったところから急速に回復し、3.4%と相当に高い成長率を示した年度であった。しかし秋口には新興国経済の変調もあり、また年度末直前に東日本大震災を経験する等、数字に比して実体経済は厳しいものがあった。情報セキュリティに向かう資金は引き続き切り詰められ、市場は全体として停滞・やや縮小となった。情報セキュリティツール合計の市場規模は 3,543 億円と推定される。

2011 年度は東日本大震災の影響で特に第 1 四半期の生産停滞が大きかったが、第 2 四半期以降急速に回復し、第 3 四半期に襲ったタイ洪水の被害も吸収して年度としては実質 0.2%ながらプラス成長を確保している。情報セキュリティツール市場は、2009 年度、2010 年度と投資が抑制された反動や、年度当初に起きた国際的電機メーカでのハッキング被害（顧客情報 1 億人の流出と報道された）や秋口に発覚した防衛産業での相次ぐ標的型攻撃被害から、企業が対策を急いだ要素が指摘されており、3.0%の成長を確保したものとみられる。

図 3　国内情報セキュリティツール市場推移



2011 年度に最も高い伸び率を示したカテゴリ（大分類市場）は「暗号化製品」で 6.5%の伸び率であった。情報漏えい対策として、データを直接保護する暗号化への需要が高まったと考えられる。次に高い伸びを示したカテゴリは「システムセキュリティ管理製品」で、伸び率は 4.4%であった。上記のように、端末の動作制御やログ管理等の製品需要が押し上げたと考えられる。サーバやファイルへのアクセスを統制･管理する「アイデンティティ･アクセス管理製品」も 3.2%とそれに次ぐ伸びを見せた。ネットワークからの攻撃に対する防御である「ネットワーク脅威対策製品」と「統合型アプライアンス」は各々2.6%、1.2%で、ツール市場全体の伸び率を下回ったが、マイナスであったと見られる 2010 年度比では回復している。「コンテンツセキュリティ対策製品」は市場が成熟していると同時に安定しており、1.8%プラスという結果であった。

2012 年度の情報セキュリティへの支出に関しては、標的型攻撃やサイバーテロの脅威が個別企業にとって具体的脅威と実感されるようになったことを背景に、2011 年度に引き続き、抜本的対策に取組む流れが見られた。その結果、ツール市場は 3,846 億円と、本統計史上の最高額を更新している。全カテゴリが伸びる中で、特に高い伸びを示したのは「システムセキュリティ管理製品」で、標的型攻撃対策としての内部ネットワークの監視・解析やログ管理の需要が高まった結

果と考えられる。

2013 年度は、引き続き経済状況の好転が期待される中で、企業の投資態度も積極化に向かうと考えられ、特に実物資産に資金が回りやすくなることから、ツールが引き続き+5.3%と高い成長率を維持して、4,050 億円と初めて 4,000 億円の大台に達すると予測した。

2.1.2. 情報セキュリティツール市場のカテゴリ別分析

以下、情報セキュリティツール市場を構成する各製品区分の市場についてその規模と概要を詳述する。

2.1.2.1. 統合型アプライアンス市場

(1)市場の動向

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費用対効果と利便性を同時に両立できる事がポイントとなる。ハードウェア性能の進化に支えられて、一般的能力を持つ低価格の普及機から、高価格だが処理性能に優れたハイエンド機まで品ぞろえが進んでいる。エントリーレベルの製品が提供されることで、小規模ユーザまで普及が進んできている。

低価格の普及機は、特に中堅・中小企業、大企業の出先事業所や部門間接続、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統合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、小規模ネットワーク環境への普及機クラスの導入需要は今後も衰えることはないであろう。

またハイエンド機は、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一般的になっている。特にデータセンタではフットプリント（ラックの占有スペース）が問題になると同時に、ユーザごとのネットワークの分離も必須課題である。このためネットワーク脅威と一部のコンテンツセキュリティ対策を 1 台で実現できる統合型アプライアンスは便利で重要な構成要素となっている。

一方で、クラウドコンピューティングの浸透は、統合型アプライアンスを始めとするハードウェア型製品の需要に影響を与える可能性がある。パブリッククラウドを提供するクラウドサービスプロバイダにおいては、高機能かつ高性能の対策機器を多重化して設置する必要があり、ハイエンド機への一段の需要シフトをもたらす可能性がある。一方、IaaS 等をホスティング環境として利用するユーザにとっては、自分の環境に対するネットワーク防御の選択肢は、仮想アプライアンスが中心となる。機能構成としてはアプライアンスでありながら、仮想化状態で提供されることとなり、製品形態としてはソフトウェア型ということになる。仮想化が急速に普及する中で、ハードかソフトかの区分が意味を持たなくなる可能性もあり、今後の動きに注意する必要が出てきている。

統合型アプライアンスの供給構造も初期と比較すると大きく変化が進んだ。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った。その結果、大手ネットワーク機器ベンダによる買収等の淘汰が進み、

独立の専業ベンダは少なくなってきている。

(2)市場規模とその推移

表 3 に国内統合型アプライアンス製品の市場規模の実績推定値と予測値を、図 4 にその市場規模の推移のグラフを示す。

表 3　国内統合型アプライアンス市場規模　実績と予測

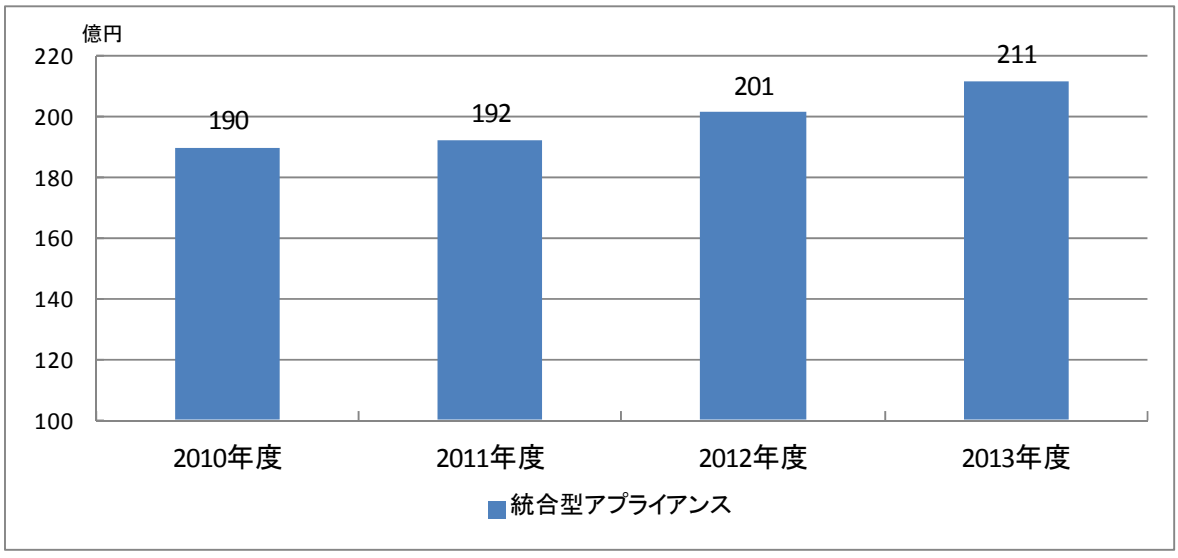
市場規模（百万円）	2010 年度	2011 年度	2012 年度	2013 年度
統合型アプライアンス	18,972	19,208	20,107	21,146
対前年度比成長率	－	1.2%	4.7%	5.2%

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、2007 年度も拡大を続けた。2008 年度にはペースは落ちたものの拡大基調を維持したが、2009 年度から 2010 年度はマイナス傾向となった。2011 年度以降は小幅ながらプラスが続き、2013 年度は更なる成長傾向が予測される。

リーマンショック後の世界同時不況等の影響で、市場全体が縮小傾向で推移した 2009 年度の後、2010 年度は回復が期待されたが、年度当初に景気の踊り場的状況が発生し、これがセキュリティ投資を控える方向に動いたため停滞が持続した。年度後半には回復の動きが強くなったが、年度末に発生した東日本大震災が影響を与えたと想定され、プラスに戻るに至らなかった。

2011 年度は、震災直後の原発事故やタイの洪水の影響でセキュリティへの投資は控える方向に動くであろうと想定していたが、日本企業や公共機関に対する標的型攻撃が多発したため、年度後半は想定以上にセキュリティへの投資が行われたと考えられ、結果、若干ではあるもののプラスとなった。

図 4　国内統合型アプライアンス市場推移



2012 年度は、前年度からのセキュリティ対策見直しと、2007～2008 年度の投資が活発だった時期に導入された製品の再構築の流れが継続し、また円高や欧州不安の中でも経済は微速ながら拡大を維持したと見られることも追い風に、拡大歩調を速めて 4.7%の成長で 200 億円の大台を回復したものとみられる。これは IT の投資サイクル上の更新期に差し掛かっている可能性があることや、ハードウェアの高性能化に伴う入れ替え需要に支えられている面もあると考えられる。

2013 年度は、ネットワーク脅威がますます高まっていることや、アベノミクスによる経済回復への期待から、投資の積極化が期待され、情報セキュリティ投資も進むと予想されることから、拡大ペースを維持し、5.2%の成長で 211 億円に達するものと予測した。

2.1.2.2. ネットワーク脅威対策製品市場

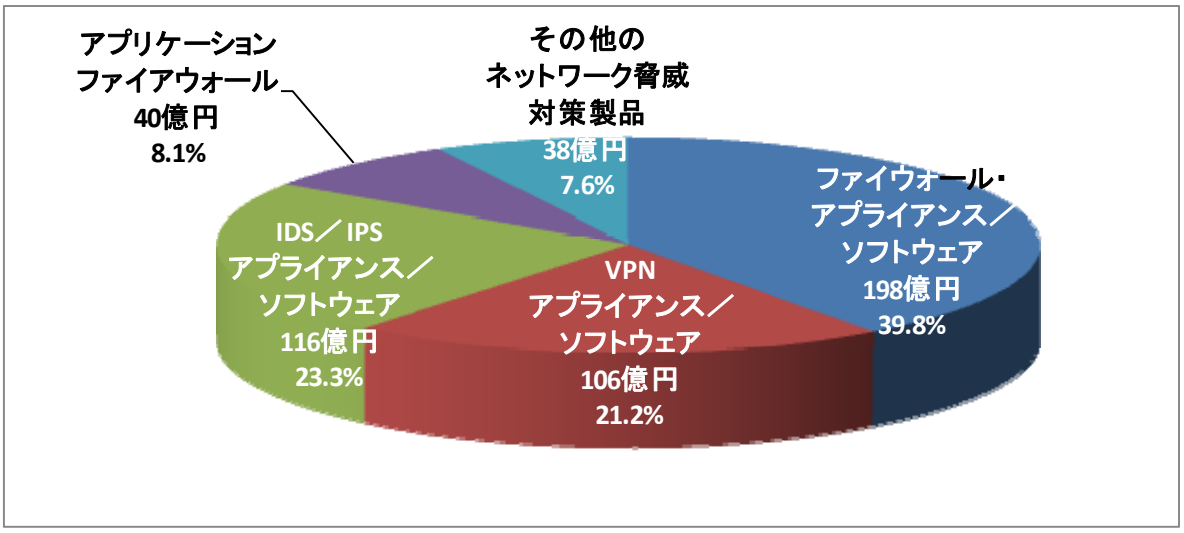
(1) 市場の動向

ネットワーク脅威対策製品の 2012 年度におけるセグメント別市場規模の分布を図 5 に示す。

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開始と同時に利用が始まっている。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。ほぼ同時に VPN も登場している。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が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。

一方、クラウドコンピューティングや仮想化技術の浸透に伴って、ファイアウォールの仮想化も行われるようになってきている。仮想化製品の需要の拡大に伴って、ソフトウェアタイプの製品の比率が回復してくる可能性もある。また、個別機能の製品を多く導入することによるコスト負担や、複数機器を統合的に管理することの困難さから、統合型アプライアンスの導入や移行の動きが続いている。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と言える。

図 5　2011 年度のネットワーク脅威対策製品市場



「アプリケーションファイアウォール」は、2005 年ごろから製品が登場した、比較的新しいジャンルである。Web アプリケーションの脆弱性が悪用されてマルウェア等が仕掛けられ、通常の Web 閲覧だけでマルウェア感染する事例が急増したことから、近年普及速度が上っている模様である。特に PCI DSS[3]が v1.2 で「ウェブアプリケーションファイアウォールの導入」を要求していることが普及に拍車をかけたと考えられる。また、IPA（独立行政法人情報処理推進機構）による推奨[4]、Web の脆弱性を悪用する攻撃が深刻化していることから、導入が進んできている。Web 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存在している[5]。

ファイアウォールや VPN はインターネットが普及した比較的初期から導入が進んでおり、IDS／IPS の設置も一般的になってきたことで、市場は成熟化が進んでいる。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になってきている。但し、ハイエンドの専用機については高信頼性が要求される通信事業者やデータセンタ等の特定市場では確実な需要が見られる他、在宅勤務やクラウドの利用拡大に伴い、リモートアクセスの安全を確保するための VPN 機器は需要の拡大傾向が見られる。

(2) 市場規模とその推移

表 4 に国内ネットワーク脅威対策製品市場規模の実績推定値と予測値を、図 6 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、2011 年度における売上実績推定値が 498 億円で、2009, 2010 年度の大幅な落込みから回復してほぼ 500 億円規模となり、2009 年度並みに戻した。

2012 年度はセキュリティ対策の見直しが前年度から継続して進んだことから、4.5%の成長で 521 億円となり、2013 年度も経済環境の好転と更新サイクルを背景（統合型アプライアンスの項参照）に、3.9%増と市場拡大基調を維持して 541 億円に達すると予測される。これは、過去のピークだった 2008 年度の 560 億円に並ぶ規模となる。

情報セキュリティツール市場の中での構成比で見ると、2011 年度は 13.7%で 4 番目に大きいセグメントで、2010 年度に「システムセキュリティ管理製品」と逆転したが、「統合型アプライアンス」を合わせたネットワーク脅威対策全体では 19%を占め、「コンテンツセキュリティ対策製品」に次いで重要なセキュリティ対策領域であることを示している。（表 2 参照）

表 4　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）	2010 年度	2011 年度	2012 年度	2013 年度
ファイアウォールアプライアンス/ソフトウェア	19,465	19,838	20,631	21,116
VPN アプライアンス／ソフトウェア	10,090	10,556	11,044	11,436

[3] 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

[4] 独立行政法人 情報処理推進機構「Web Application Firewall 読本」
http://www.ipa.go.jp/security/vuln/documents/waf.pdf

[5] 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

IDS／IPS アプライアンス／ソフトウェア	11,411	11,581	12,161	12,820
アプリケーションファイアウォール	3,832	4,043	4,275	4,535
その他のネットワーク脅威対策製品	3,737	3,782	3,940	4,150
合計	48,535	49,799	52,050	54,058
構成比				
ファイアウォールアプライアンス/ソフトウェア	40.1%	39.8%	39.6%	39.1%
VPN アプライアンス／ソフトウェア	20.8%	21.2%	21.2%	21.2%
IDS／IPS アプライアンス／ソフトウェア	23.5%	23.3%	23.4%	23.7%
アプリケーションファイアウォール	7.9%	8.1%	8.2%	8.4%
その他のネットワーク脅威対策製品	7.7%	7.6%	7.6%	7.7%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
ファイアウォールアプライアンス/ソフトウェア	－	1.9%	4.0%	2.3%
VPN アプライアンス／ソフトウェア	－	4.6%	4.6%	3.6%
IDS／IPS アプライアンス／ソフトウェア	－	1.5%	5.0%	5.4%
アプリケーションファイアウォール	－	5.5%	5.7%	6.1%
その他のネットワーク脅威対策製品	－	1.2%	4.2%	5.3%
合計	－	2.6%	4.5%	3.9%

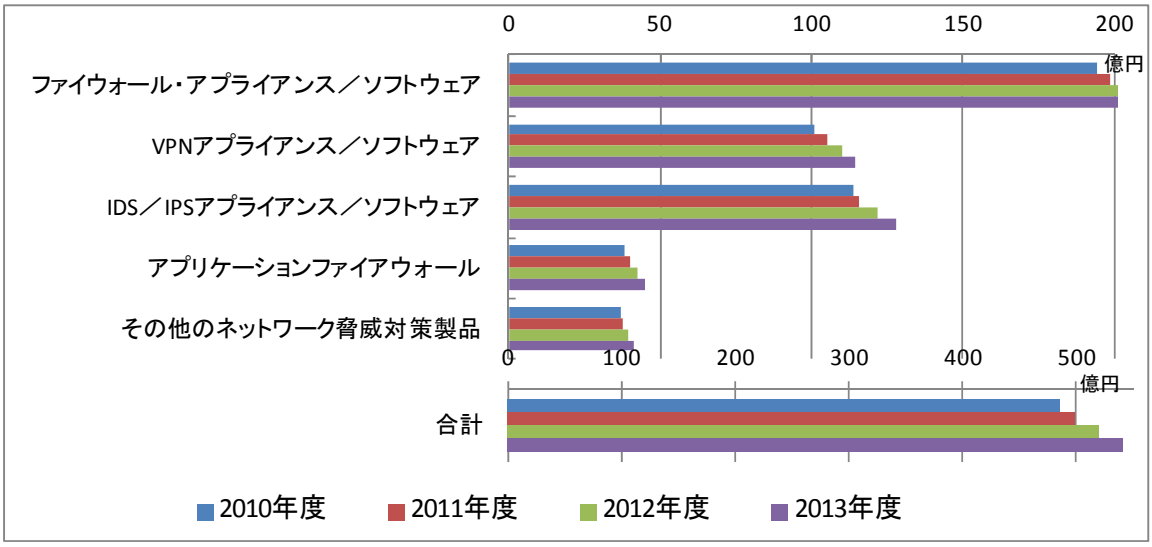
ネットワーク脅威対策製品のカテゴリの中では 1 番大きいセグメントである「ファイアウォールアプライアンス／ソフトウェア製品」は、本調査の対象期間でみると、2010 年度 195 億円、2011 年度 198 億円、2012 年度 206 億円、2013 年度 211 億円と増加傾向を見せている。2008 年度前半までは、通信事業者を中心とするハイエンドのユーザの設備投資サイクル上の更新期に当っていたが、2009, 2010 年度と、その反動と景気の低迷による設備投資控えの影響を受け、急速に市場規模が縮小した。2011 年度、2012 年度にかけては上昇が続き、2013 年度に関しては、政権交代に伴う経済政策が徐々にではあるものの経済状況を好転させてゆくと想定され、更に増加傾向となる予測となった。

「VPN アプライアンス／ソフトウェア製品」は、「ネットワーク脅威対策製品」カテゴリの中では最も経済停滞の影響を受けないセグメントと考えられる。その市場規模と成長率の推移は、2010 年度 101 億円、2011 年度 106 億円・4.6%増、2012 年度 110 億円・4.6%増、2013 年度 114 億円・3.6%増と、市場規模は毎年堅調な増加の予測になっている。この背景には、スマートフォンやタブレット端末等のスマートデバイスの急速な普及に伴うモバイルコンピューティングの浸透と、社外から社内に接続する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きていることがある。これらは、パンデミック、震災に対応しての事業継続管理や、少子化対策に伴う在宅勤務等労働形態の多様化を背景に急速に進んでいる。このためにリモートアクセスに際してのVPN環境を整える動きは強まってきており、市場の堅調さ、逆境の中での伸びを支えている。

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／ソフトウェア製品」は、2010 年度は 114 億円であった。2011 年度 116 億円で 1.5%増、2012 年度 122 億円で 5.0%増、2013 年度 128 億円で 5.4%増という拡大傾向の推定・予

測となった。特に 2012 年度、2013 年度に関しては、セキュリティ対策の抜本的見直し、標的型攻撃対策における内部ネットワーク監視重視等の流れに支えられて拡大が続くと予測される。

図 6　国内ネットワーク脅威対策製品市場推移



「アプリケーションファイアウォール」は、2007 年度に市場が急速に立ち上がった、新しいセグメントである。当初は使い勝手の悪さから需要側にも戸惑い感があり、2008 年度以降横ばいの推移であったが、製品の改良やニーズの高まりを背景に、本調査期間では順調に拡大するとの結果となった。市場規模は、2010 年度 38 億円から、2011 年度 40 億円で 5.5%増、2012 年度 43 億円で 5.7%増、2013 年度 45 億円で 6.1%増と成長の度合いを徐々に強めると予測される。

Web アプリケーションがネットワークからの攻撃対象とされ、多くの大企業にも被害が発生するケースが増えており、手口も巧妙化してきて被害が拡大していることや、PCI DSS 標準の導入要件となった事等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ると考えられる。

2.1.2.3. コンテンツセキュリティ対策製品市場

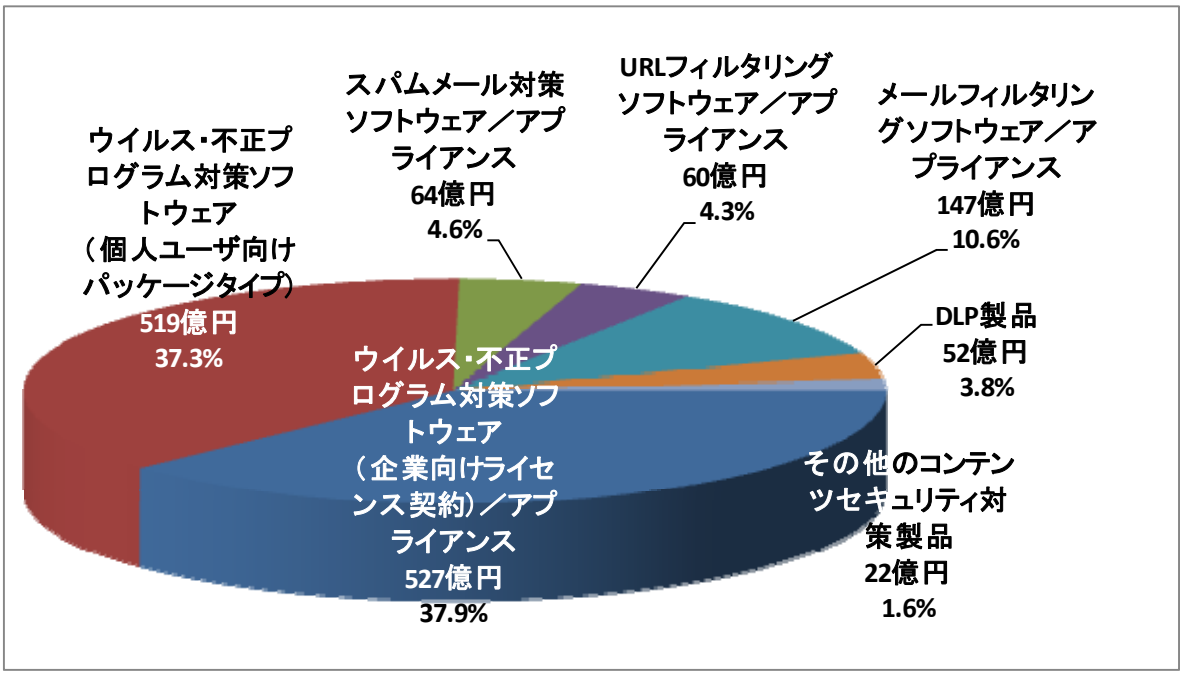
(1) 市場の動向

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が、これまでの調査では 2008 年度の推定実績 1,399 億 7,800 万円をピークに、1,400 億円を突破するところまでは至らなかった。しかし、今回の調査では 2011 年度 1,390 億円、2012 年度 1,468 億円、2013 年度 1,545 億円という予想となった。これは、他の市場に比べ 2008 年度以降の景気低迷の影響が少なかったこと、2012 年度には景気が好転し 2013 年度には伸びに転ずる市場予測に加え、コンテンツに対するセキュリティの重要性が増している社会情勢を背景に、各ベンダが、企業の投資や個人消費の伸びを大いに期待していることを物語っている。

コンテンツセキュリティ対策製品の 7 つの製品分類における 2011 年度の分布を図 7 に示す。

「ウイルス・不正プログラム対策ソフトウェア」が、企業向けと個人向けを合わせると、市場の約 75%を占める。ウイルス対策は、セキュリティ対策のなかでも 20 年の歴史を持つ代表的なものであり、企業向け・個人向けともに利用が浸透している。とりわけ企業における実施率は、既に 5 年前からほぼ 100%となっており、企業規模に関わらずその普及率はきわめて高い。今後もスマートフォン、タブレット、インターネット対応テレビ・ゲーム機等の新しい機器の登場と普及拡大が見込まれる中、標的型攻撃、遠隔操作ウイルス、内部情報漏えい、悪意のある情報改ざん、国際緊張等、コンテンツを守り安心して利用できる環境を維持するために必要な投資であるという理解が広く浸透し、その流れは個人向け市場へも波及し拡大することが期待される。

図 7　2011 年度のコンテンツセキュリティ対策製品市場



コンテンツセキュリティ対策製品市場は、続いて「メールフィルタリング」、「スパムメール対策」、「URL フィルタリング」、「DLP 製品」（情報漏えい対策製品・システム）というセグメントで構成されている。メールや Web アクセスは企業業務でもっともよく利用するインターネット通信機能であり、企業・組織はその安全対策に様々な措置を講じている。また情報をやり取りする手段でなく情報そのものに着目して社外流出を防ぐ仕組みである「DLP 製品」も、使い勝手の向上とともに市場を拡大している。

(2) 市場規模とその推移

表 5 に国内コンテンツセキュリティ対策製品市場規模の実績推定値と予測値を、図 8 にその市場規模推移のグラフを示す。

「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」は中分類レベルでは最大級の市場規模を持つセグメント（市場）であり、その規模は 2011 年度で 527 億円に達すると推測される。情報セキュリティ対策の基本中の基本となるものであり、

2012年度には5.9%増の558億円、2013年度には4.2%増の582億円に達するものと予測される。

表 5　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

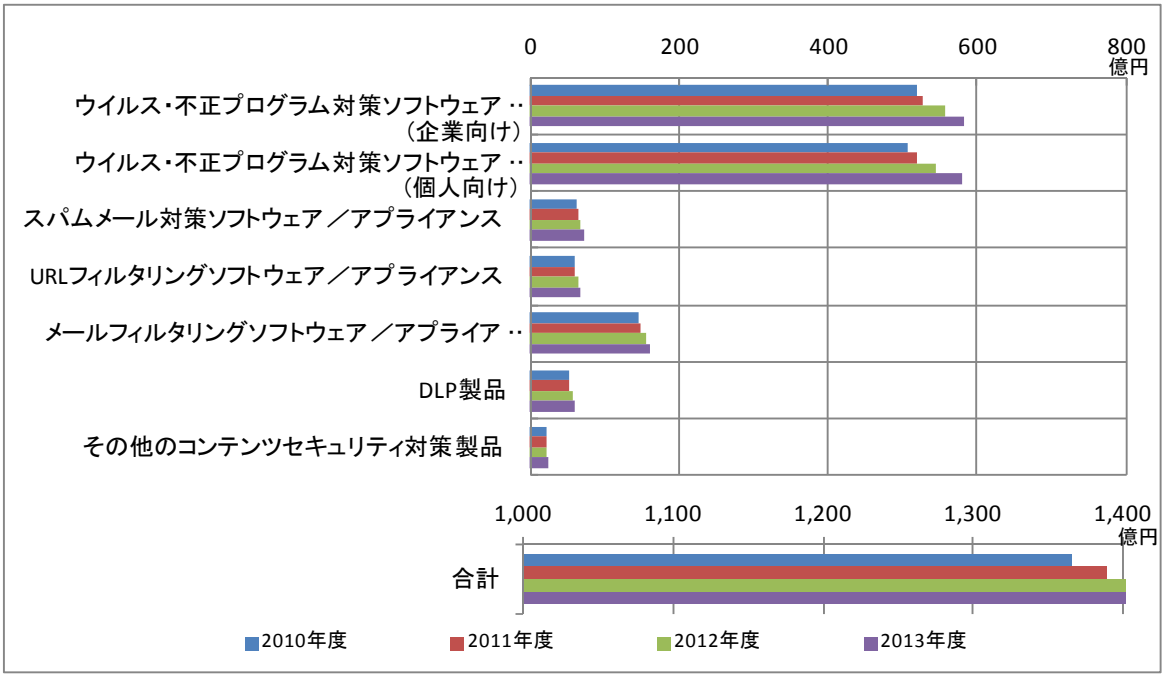
市場規模（百万円）	2010年度	2011年度	2012年度	2013年度
ウイルス・不正プログラム対策ソフトウェア（企業向けライセンス契約）／アプライアンス	51,830	52,708	55,827	58,187
ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ）	50,760	51,858	54,361	57,888
スパムメール対策ソフトウェア／アプライアンス	6,332	6,357	6,775	7,217
URLフィルタリングソフトウェア／アプライアンス	5,941	5,989	6,426	6,722
メールフィルタリングソフトウェア／アプライアンス	14,506	14,686	15,508	16,180
DLP製品	5,123	5,242	5,605	5,976
その他のコンテンツセキュリティ対策製品	2,063	2,155	2,253	2,336
合計	136,556	138,995	146,756	154,506
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	38.0%	37.9%	38.0%	37.7%
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）	37.2%	37.3%	37.0%	37.5%
スパムメール対策ソフトウェア／アプライアンス	4.6%	4.6%	4.6%	4.7%
URLフィルタリングソフトウェア／アプライアンス	4.4%	4.3%	4.4%	4.4%
メールフィルタリングソフトウェア／アプライアンス	10.6%	10.6%	10.6%	10.5%
DLP製品	3.8%	3.8%	3.8%	3.9%
その他のコンテンツセキュリティ対策製品	1.5%	1.6%	1.5%	1.5%
合計	100.0%	100.0%	100.0%	100.0%
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	－	1.7%	5.9%	4.2%
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）	－	2.2%	4.8%	6.5%
スパムメール対策ソフトウェア／アプライアンス	－	0.4%	6.6%	6.5%
URLフィルタリングソフトウェア／アプライアンス	－	0.8%	7.3%	4.6%
メールフィルタリングソフトウェア／アプライアンス	－	1.2%	5.6%	4.3%
DLP製品	－	2.3%	6.9%	6.6%
その他のコンテンツセキュリティ対策製品	－	4.4%	4.6%	3.7%
合計	－	1.8%	5.6%	5.3%

「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）」も同程

度の規模を持つセグメントである。銀行口座やクレジットカードの情報を盗まれる被害が個人にも及んできており、基本的対策であるウイルス対策ソフトの導入が徐々に浸透している。2011年度の市場規模は519億円であったと推計される。2012年度4.8%、2013年度6.5%と順調に拡大し、各々543億円、579億円規模に達すると予測される。スマートデバイスの普及も成長に寄与すると考えられる。

これに次ぐ規模のセグメントは「メールフィルタリングソフトウェア／アプライアンス」で、特にメール本体や添付ファイルで社外に出ていく情報のチェックのために広く使われるようになっている。その市場規模は2011年度で147億円であるが、2013年度には162億円にまで拡大すると予測される。その次の規模のセグメントは「スパムメール対策ソフトウェア／アプライアンス」で、2011年度で64億円である。この市場も2012年度6.6%、2013年度6.5%とコンスタントに拡大して2013年度の市場規模は72億円に達すると予測される。

図 8　国内コンテンツセキュリティ対策製品市場推移



次いで「URLフィルタリングソフトウェア／アプライアンス」がほぼ同規模の市場を形成している。2011年度60億円、2012年度64億円（7.3%増）、2013年度67億円（4.6%増）と予測される。「DLP製品」市場は比較的後発のセグメントであるが2011年度には52億円に達している。この市場も順調に拡大すると考えられ、2012年度56億円（6.9%増）、2013年度60億円（6.6%増）との予測結果となった。

2.1.2.4. アイデンティティ・アクセス管理製品市場

(1) 市場の動向

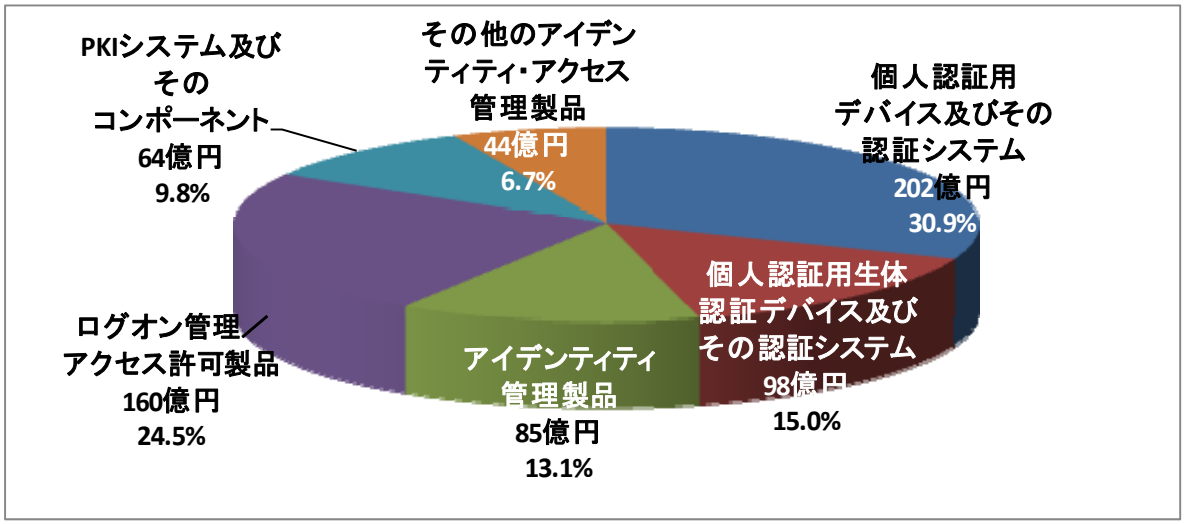
図9に2011年度のアイデンティティ・アクセス管理製品のセグメント別市場規模分布を示す。

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、サーバ、アプリケーション等、システム全体を通して、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。企業の情報資産を情報漏えいや改ざん、盗難、紛失、消失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検討する企業が、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った。また、スマートフォンやタブレット PC に代表される携帯端末を業務で使用するニーズや、クラウドサービスの利用が高まっている昨今、携帯端末向けアイデンティティ・アクセス管理製品の登場やクラウドサービス向けアクセス管理、シングル・サインオン（SSO）等のニーズで、この市場は、景気の回復とともに成長が期待できる分野と考えられる。

間違いによるアクセスや不正アクセスを 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を防止して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。

図 9　2011 年度のアイデンティティ・アクセス管理製品市場



また、クラウドコンピューティングサービスの浸透により、パブリッククラウドの利用だけでなく、プライベートクラウドに対する需要が高まり、クラウドサービスへのアクセスを一元管理させるクラウド・アクセス・セキュリティ（CAS）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、今後も高まることが予測される。

その中でも、SAML（Security Assertion Markup Language）や OpenID 等、各種認証技術と連携させ、シングル・サインオン（SSO）を実現させる製品も表れ、今後の伸びが期待できる。

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、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等、様々である。更に、実装方式においても、全てのアクセス先にプログラムをインストールして、より細かい制御やログが取得できるエージェントタイプと、重要な情報リソースへのゲートウェイに実装し、一括でアクセス管理およびログ取得を行うエージェントレスタイプがある。

また、アイデンティティ管理製品でも、特権IDの追加、削除、権限の割り当てに特化したシステムも登場しており、欧州を中心に導入が進められている。

(2) 市場規模とその推移

表 6 に国内アイデンティティ・アクセス管理製品の市場規模推定実績値と予測値を、図 10 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、2011 年 3 月の東日本大震災の影響で、2011 年度の実績で 654 億円（前年比伸び率 3.2%）となったが、「情報セキュリティツール」市場全体の 3,648 億円に対する構成比は 17.9 %であり、コンテンツセキュリティ対策製品市場に次ぐ規模の市場である。この市場規模は、2008 年秋以降に顕在化した世界金融危機を受け、2010 年度は 634 億円と縮小したが、2012 年度には 689 億円（前年比伸び率+5.3%）に回復すると予測される。

「アイデンティティ・アクセス管理製品」カテゴリの内訳をみると、「個人認証用デバイスおよびその認証システム」セグメントが 2011 年度の構成比で 30.9%と最も大きな部分を占めた。市場規模は 2011 年度で 202 億円であり、2012 年度は 212 億円と前年比 5.0%増と予想される。

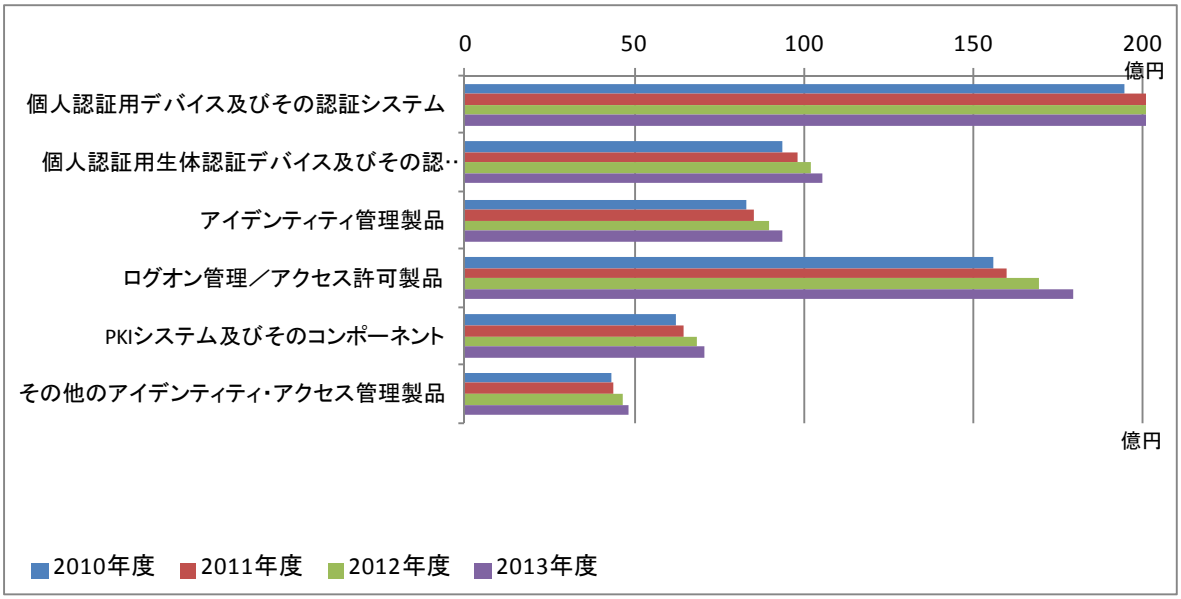
表 6 国内アイデンティティ・アクセス管理製品市場規模 実績と予測

市場規模（百万円）	2010 年度	2011 年度	2012 年度	2013 年度
個人認証用デバイスおよびその認証システム	19,481	20,192	21,207	21,968
個人認証用生体認証デバイスおよびその認証システム	9,405	9,831	10,236	10,552
アイデンティティ管理製品	8,289	8,548	8,962	9,393
ログオン管理／アクセス許可製品	15,634	16,005	16,958	17,956
PKI システムおよびそのコンポーネント	6,253	6,438	6,845	7,092
その他のアイデンティティ・アクセス管理製品	4,332	4,378	4,648	4,840
合計	63,393	65,392	68,857	71,801
構成比				
個人認証用デバイスおよびその認証システム	30.7%	30.9%	30.8%	30.6%
個人認証用生体認証デバイスおよびその認証システム	14.8%	15.0%	14.9%	14.7%
アイデンティティ管理製品	13.1%	13.1%	13.0%	13.1%
ログオン管理／アクセス許可製品	24.7%	24.5%	24.6%	25.0%
PKI システムおよびそのコンポーネント	9.9%	9.8%	9.9%	9.9%
その他のアイデンティティ・アクセス管理製品	6.8%	6.7%	6.8%	6.7%
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およびその認証システム	ー	3.7%	5.0%	3.6%

個人認証用生体認証デバイスおよびその認証システム	ー	4.5%	4.1%	3.1%
アイデンティティ管理製品	ー	3.1%	4.8%	4.8%
ログオン管理／アクセス許可製品	ー	2.4%	6.0%	5.9%
PKI システムおよびそのコンポーネント	ー	3.0%	6.3%	3.6%
その他のアイデンティティ・アクセス管理製品	ー	1.1%	6.2%	4.1%
合計	ー	3.2%	5.3%	4.3%

前年度比成長率でみると、「個人認証用生体認証デバイスおよびその認証システム」が 2011 年度+4.5%と一番高い伸び率を示していたが、2012 年度は、+4.1%と他のセグメントに比較して相対的に低い伸びにとどまると推測される。替って「ログオン管理／アクセス許可製品」および「PKI システムおよびそのコンポーネント」が+6%台の伸びと推測され、情報セキュリティ製品全体を通しても、高い成長率が期待できるセグメントの一つである。これは携帯端末を使用した社外からのリモートアクセスやクラウドコンピューティングサービスの浸透により、個人認証を強化する結果、ログオン管理／アクセス許可製品や PKI システムの導入が進むと予想されるためである。

図 10　国内アイデンティティ・アクセス管理製品市場推移



「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、クラウドコンピューティングサービス利用拡大の面から適用対象が拡大し、スマートフォンやタブレット PC の市場拡大に伴い、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、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考えられるからである。

2.1.2.5. システムセキュリティ管理製品市場

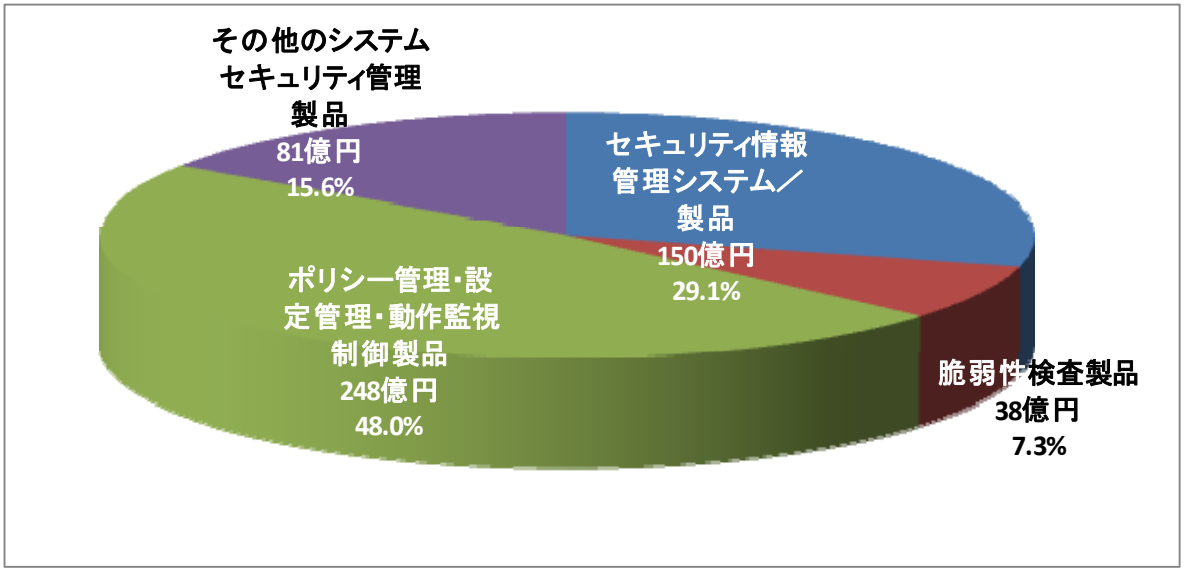
(1) 市場の動向

システムセキュリティ管理製品の 2011 年度におけるセグメント分布を図 11 に示す。

2011 年 9 月に発覚した三菱重工へのサイバー攻撃による機密情報の漏えい事件をきっかけに内部ネットワークの管理を強化する動きが活発化した。その動きはシステムセキュリティ管理製品カテゴリを構成する各セグメント市場に及んでいる。

「セキュリティ情報管理システム/製品」はこれまで外部からの不正トラフィックに対応するためのシステム統合管理ツールとして活用されることが多かったが、リアルタイム性を考慮した、内部から外部へのトラフィックのモニタリングツールとしての利用も積極化している。これは標的型攻撃への対応手段の一つとして、内部に秘かに送りこまれたマルウェアの、外部の C&C[6]サーバとの通信を捕捉する手段として認知されている結果である。この機能を活用した SOC（Security Operation Center）の構築やサービス利用の検討を始める企業が増加する傾向がみられた。このような流れにより市場が拡大する分野であると考えられる。

図 11　2011 年度のシステムセキュリティ管理製品市場



「ポリシー管理・設定管理・動作監視制御製品」は情報漏えい対策につながることから、需要は依然高い分野である。スマートフォンやタブレット型端末の普及もすすみ、従来のPC端末管理ツールでは管理、制御できない領域が発生してきている。そのような流れでMDM（Mobile Device Management）と呼ばれるツールも各ベンダからリリースされてきており、市場の拡大要因の一つとして考えられる。昨今では個人所有のスマートフォンやタブレット型端末を業務にも活用する需要が増えてきた影響により、私的デバイスの管理が課題として挙がってきている。現段階ではベンダ、企業ともに対応策を模索しており、今後管理製品やサービスが増えてくることが推測される。

---

[6] Command and Control 内部に送り込んだBOT、スパイウェア等のマルウェアに指示を与える攻撃者のサーバ

「脆弱性検査製品」市場はSOC需要の高まりやWebの脆弱性検査需要の増加に連動して需要も増加傾向にあると考えられるが、サービスとして提供されることが多いので「脆弱性検査製品」の売上数値への直接的な影響は軽微なものと考えている。

(2) 市場規模とその推移

表7に国内システムセキュリティ管理製品市場規模の実績推定値と予測値を、図12にその市場規模の推移のグラフを示す。

「システムセキュリティ管理製品」市場は 2011 年度には全セグメント合せて 517 億円程度の市場を形成しており、2010 年度と比べると+4.4%と、セキュリティツール全体の伸びより高い伸び率となっている。さらに 2012 年度は 551 億円の 6.6%増とさらに高い伸び率を見越しておりその傾向は 2013 年度（589 億円、+6.8%）も続くと推測している。これらはセキュリティツール製品全体の成長率と比較しても大きな数値となることから、この分野への企業の投資態度は前向きであると考えられる。

表 7　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）	2010 年度	2011 年度	2012 年度	2013 年度
セキュリティ情報管理システム／製品	14,615	15,026	15,942	16,963
脆弱性検査製品	3,620	3,761	3,906	4,140
ポリシー管理・設定管理･動作監視制御製品	23,304	24,829	26,603	28,434
その他のシステムセキュリティ管理製品	7,968	8,062	8,651	9,327
合計	49,507	51,679	55,102	58,864
構成比				
セキュリティ情報管理システム／製品	29.5%	29.1%	28.9%	28.8%
脆弱性検査製品	7.3%	7.3%	7.1%	7.0%
ポリシー管理・設定管理･動作監視制御製品	47.1%	48.0%	48.3%	48.3%
その他のシステムセキュリティ管理製品	16.1%	15.6%	15.7%	15.8%
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	－	2.8%	6.1%	6.4%
脆弱性検査製品	－	3.9%	3.8%	6.0%
ポリシー管理・設定管理･動作監視制御製品	－	6.5%	7.1%	6.9%
その他のシステムセキュリティ管理製品	－	1.2%	7.3%	7.8%
合計	－	4.4%	6.6%	6.8%

各セグメントの推移をみると、「セキュリティ情報管理システム／製品」は 2011 年度に 150 億円、前年度比 2.8%増と増加傾向にあり、さらに 2012 年度は 6.1%増の 159 億円、2013 年度は+6.4%の 170 億円と大きく伸びていくと推測される。

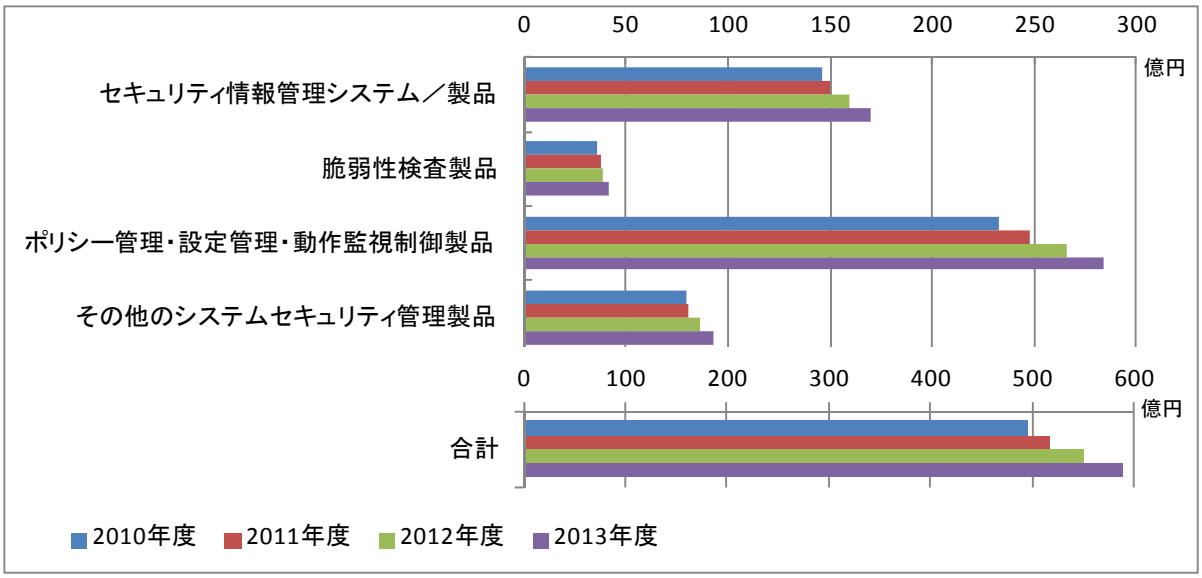
「ポリシー管理･設定管理･動作監視制御製品」はこの区分の約半分を占める市場となっており、2011 年度の予測における成長率も 6.5%増とセキュリティツール全体より高い成長率を示してい

る。市場規模は 248 億円と、ほぼ「システムセキュリティ管理製品」カテゴリの半分を占める。2012 年度は+7.1%で 266 億円、2013 年度は 6.9%増の 284 億円と成長は継続していくと推測している。

脆弱性検査製品は、Web サイトやネットワークシステムの脆弱性スキャナーであり、検査サービス事業者や SI 事業者等需要が限定的であることから市場規模は 2011 年度で 38 億円と小さい。伸び率も他のセグメントに比較して限定的で、2012 年度+3.8%、2013 年度+6.0%程度と予測され、2013 年度の市場規模は 41 億円と推定された。

「その他のシステムセキュリティ管理製品」にはセキュリティ目的でのログ管理製品やフォレンジック関係製品が含まれる。2011 年度の伸び率は+1.2%と限定的だったが、2012 年度 7.3%、2013 年度 7.8%と高い成長率を示し、2013 年度には 93 億円規模に達するものと予測された。標的型攻撃対策や内部不正による情報流出への対策から、内部ネットワークのトラフィック管理需要が高まっていることを反映していると考えられる。

図 12　国内システムセキュリティ管理製品市場推移



2.1.2.6. 暗号化製品市場

(1) 市場の動向

2011 年度は震災の影響等により全般に市場拡大が限定的となる中、6.5%という高い増加率となった。これは前回調査時の見込みでも触れたとおり、「暗号の 2010 年問題」に対応するため、具体的な移行フェーズに入り市場が活性化したと見ることもできる。例えば、政府認証基盤（GPKI）の暗号アルゴリズム移行作業はフェーズ 1 に入り、機器更改時には新旧暗号に対応する計画となっている。なお各府省庁が保有する情報システムに対して新たな暗号方式への対応時期は 2013 年度末となっており、民間の認証機関も同様の動きを見せているため、継続的な成長要因の一つと考えられる。認証基盤以外の部分では、暗号技術を利用した情報漏えい対策ツール、盗難対策ツール類は多くのベンダからリリースされ、一定規模の需要が見込める。また、PCIDSS の Ver2 がリリースされ、要件の明確化が進んだことにより認証取得の活動が増えているのも、「暗

号化ミドルウェア」の需要拡大に寄与していると推測できる。その他、デジタル複合機、ゲーム機等への組み込みも順調に推移している。また、スマートフォンへのハードウェア暗号が OS レベルで実装される等、組み込みモジュールとしての普及も成長要因の一つとして考えられる。

(2)市場規模とその推移

表 8 に国内暗号化製品市場規模の実績推定値と予測値を、図 13 にその市場規模の推移のグラフを示す。

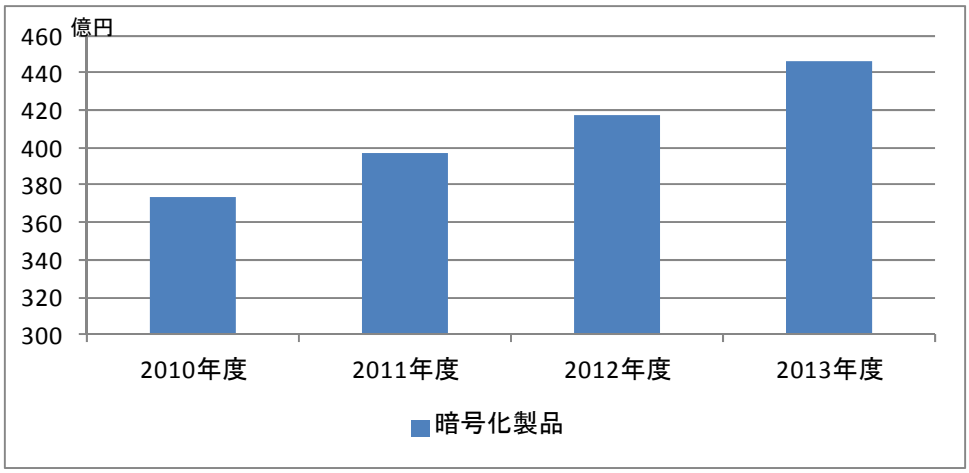
表 8　国内暗号化製品市場規模　実績と予測

市場規模（百万円）	2010 年度	2011 年度	2012 年度	2013 年度
暗号化製品	37,307	39,734	41,694	44,579
対前年度比成長率				
暗号化製品	－	6.5%	4.9%	6.9%

暗号化製品の市場規模はセキュリティツール全体の約 10%を占める。2011 年度の市場規模は 397 億円で前年度比 6.5%増加となった。2012 年度は 4.9%増の 417 億円となり、2013 年度はさらに 6.9%市場規模を拡大させ、446 億円規模の市場になると予測している。この伸び率はセキュリティツール全体の伸び率を上回るため、セキュリティツール全体からみた比率は 11%程度に上昇する。

暗号化製品は認証や情報漏えい対策の基盤となる製品なので、今後も市場は一定規模を維持しつつゆるやかに拡大していくと予測する。

図 13　国内暗号化製品市場推移



2.2. 国内情報セキュリティサービス市場の分析

2.2.1. 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、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 カテゴリを区分している。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 9 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 9　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

年度別売上高推計値	2010年度		2011年度			2012年度			2013年度		
セキュリティ･サービス	売上実績推定値		売上実績推定値			売上高見込推定値			売上高予測値		
	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	66,271	21.4%	67,928	20.7%	2.5%	70,150	20.3%	3.3%	72,181	20.0%	2.9%
セキュアシステム構築サービス	122,229	39.4%	129,116	39.4%	5.6%	138,821	40.1%	7.5%	144,389	40.0%	4.0%
セキュリティ運用･管理サービス	90,375	29.2%	98,071	29.9%	8.5%	103,092	29.8%	5.1%	109,163	30.3%	5.9%
情報セキュリティ教育	23,880	7.7%	25,185	7.7%	5.5%	26,601	7.7%	5.6%	27,332	7.6%	2.7%
情報セキュリティ保険	7,236	2.3%	7,497	2.3%	3.6%	7,647	2.2%	2.0%	7,800	2.2%	2.0%
セキュリティサービス市場合計	309,992	100.0%	327,797	100.0%	5.7%	346,310	100.0%	5.6%	360,864	100.0%	4.2%

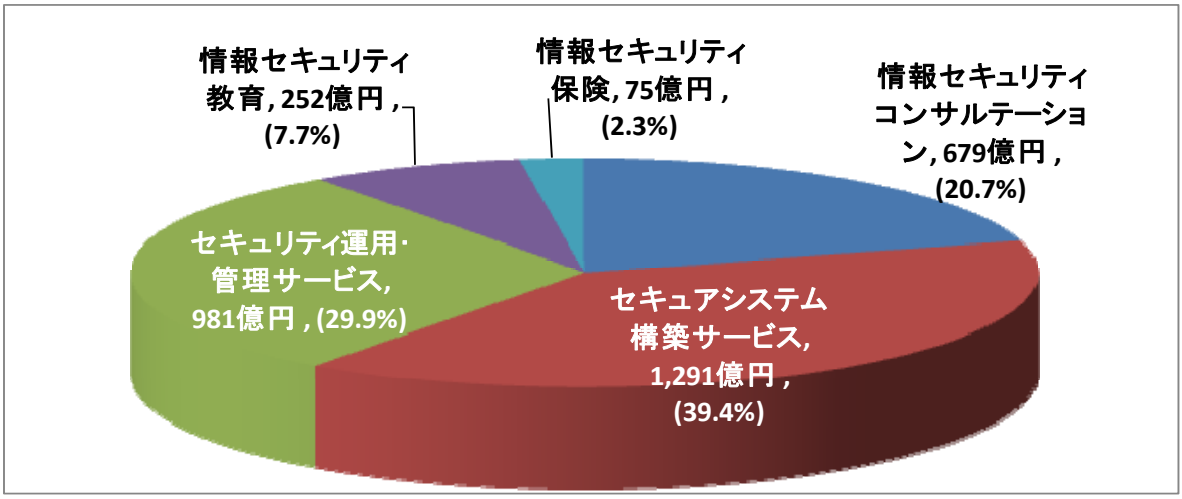
今回の調査結果では、2010 年度の「情報セキュリティサービス」市場規模は 3,100 億円と見積もられ、以降年を追って拡大するものとの観測となった。前回調査と合わせてみると、2010 年度の 3,100 億円規模が当面の底だったと考えられる。セキュリティ対策が企業・組織に浸透することに伴って、対策実施段階で必要となるコンサルテーションやシステム構築サービスの需要は一巡する。その影響が前回調査における 2009, 2010 年度の数値に反映されていた。2011 年度も同様の傾向が続くと見られていたが、今回調査の結果、同年度に発生した複数の大規模インシデントが契機となり、大企業を中心に、すでに構築していたセキュリティ対策を抜本的に見直したり再構築したりする動きが強まり、需要が急速に回復した模様である。その結果 2011 年度の市場規模は前年度比+5.7%と高い成長を見せて 3,278 億円に達したものとみられる。

2012 年度もその流れは継続したと考えられ､セキュアシステム構築サービスを中心に需要が拡大したことから、サービスの伸びはツールを上回る+5.6%に達したと見られ、市場規模は 3,463 億円となった。2013 年度はこれらの動きも一巡して伸び率は鈍化すると考えられ、+4.2%の成長で 3,609 億円と、初めて 3,600 億円台に到達するものと予測される。

図 14 に 2011 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 15 に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。

「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、2011 年度実績推定値で 1,291 億円と、情報セキュリティサービス市場全体の 39.4%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。

図 14　2011 年度の国内情報セキュリティサービス市場



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、2011 年度実績は 981 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・攻撃への対処を専門家が代行するマネージドセキュリティサービス、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。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、システムのサービス提供者、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。

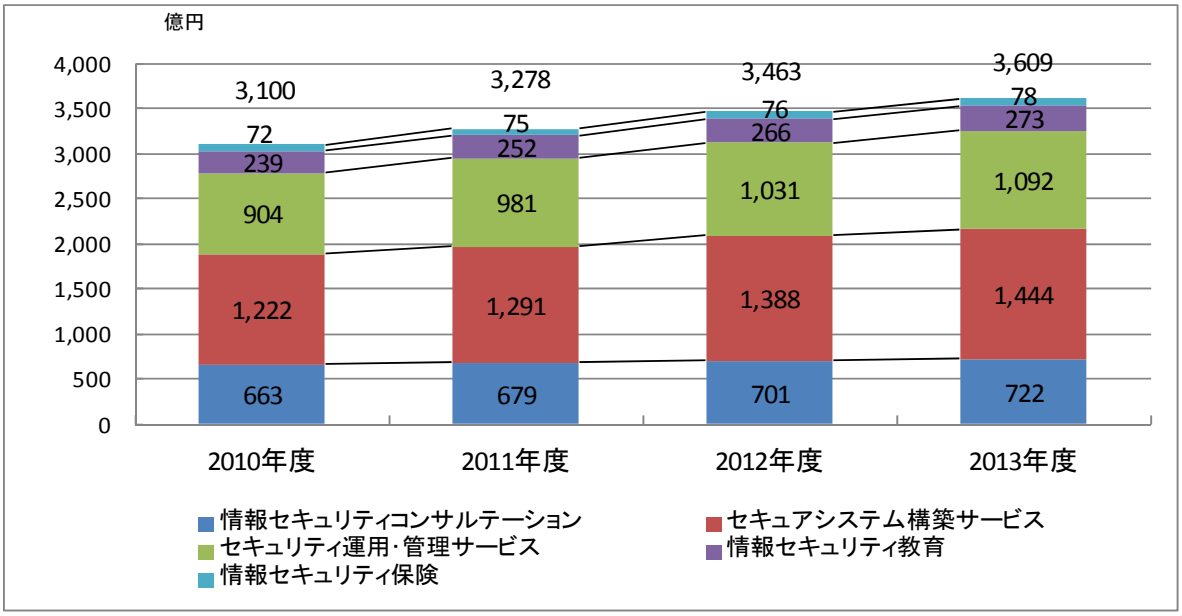
「セキュリティ運用・管理サービス」に関しては、2000 年代半ば頃から複雑化するネットワーク、高度化し頻度が高まる攻撃、特に電子商取引サイトへの攻撃やそれによる被害の深刻化等を背景に、専門サービスへのアウトソーシングを積極活用しようという判断が増えて、需要が堅調に拡大している。競争にさらされる中でサービス品質が高まると共に価格も相当程度低下が進み、また、深刻な情報セキュリティインシデントが多発する中で、対策のために専門家によるサービスが必要であるとの認識も浸透するといった背景から、景気低迷の中でも底堅い動きを示してい

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番目に位置するのが「情報セキュリティコンサルテーション」である。経営管理の視点から専門家の支援を活用する要素が強く、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。かつて「情報セキュリティコンサルテーション」の需要が拡大した要因としては、2005 年 4 月から全面施行された個人情報保護法と、2008 年 4 月以降に開始する会計年度から適用された内部統制報告制度、更には新潟県中越・中越沖地震や新型インフルエンザ等のパンデミック対策を契機とした事業継続計画への関心の高まりが挙げられる。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が高まった時期があった。その後、対策の浸透や体制構築が一巡すると、市場の成長には急ブレーキがかかり、前回調査の期間中はマイナス成長が続くという調査結果であった。しかし、2011 年度に、過去に構築した対策の体系的見直しの需要が顕在化し、再び市場拡大に向かいだしたと見られる。その結果、2011 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 2.5%拡大して 679 億円になったと見られる。

「情報セキュリティ教育」の 2011 年度実績推定値は前年度比+5.5%とサービス全体とほぼ同じ拡大ペースで 252 億円に達したと見られる。近年セキュリティ教育投資が着実に行われるようになった背景には、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、漏えい事件・事故が後を絶たないことがある。また、標的型攻撃対策としては、従業員の日ごろの意識の持ち方が重要な要素となることから、継続的教育の必要性への認知は一層浸透していると考えられる。

図 15　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。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はじめた 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。特に最近のインシデントの多発と深刻化、完全な防御は困難との認識から、保険への需要は拡大傾向を見せている。市場規模は、2011 年度で前年度比+3.6%の 75 億円となったと推定される。

2.2.2. 情報セキュリティサービス市場のカテゴリ別分析

以下、情報セキュリティサービス市場を構成する各サービス区分の市場についてその規模と概要を記す。

2.2.2.1. 情報セキュリティコンサルテーション市場

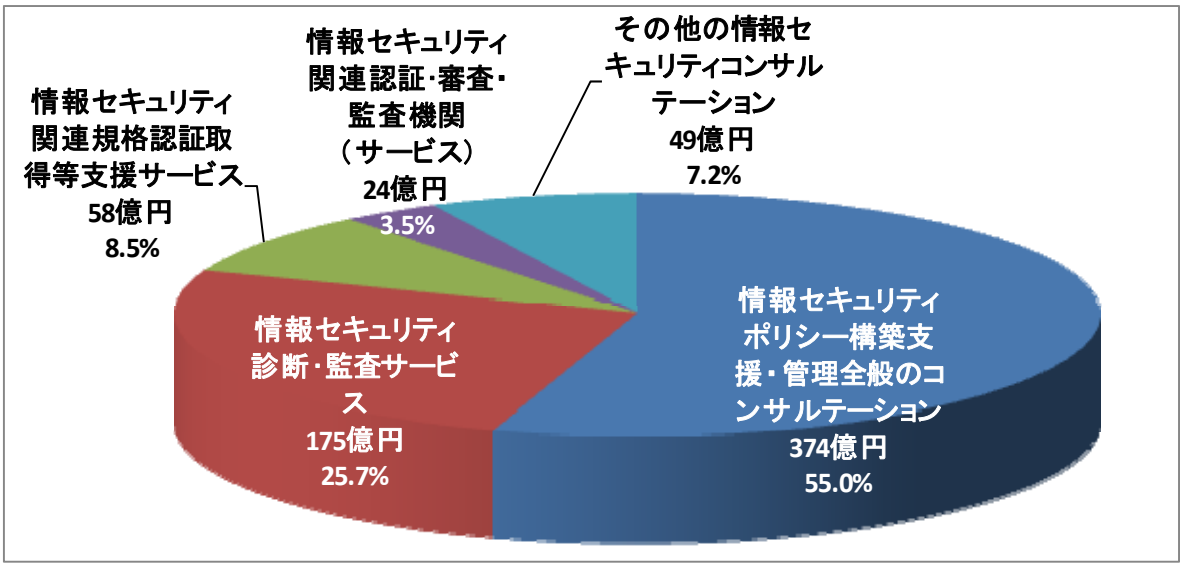
(1) 市場の動向

図 16 に、2011 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、コンサルテーションの特性から、情報セキュリティに関する取組み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。ここ数年で以下のような変化が起きていると考えられる。

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依然として高まっている。内部統制報告制度への対応や個人情報保護法対応、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。

図 16　2011 年度の情報セキュリティコンサルテーション市場



近年相次ぐ個人情報漏えいや企業秘密の持出し・漏えい・紛失等の事件は、企業のガバナンスに対する社会の視線を厳しくしている。企業側はリスク管理の意識が高まり、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に至るようになってきた。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支える要因になっていると言える。

2005 年 4 月から個人情報保護法が全面的に施行され、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。規格の要求する形を取り急ぎ整えてとりあえず認証・認定を得ようとするような傾向も当初は見受けられたが、現在では終息しつつある。一方で、実効性のあるマネジメントシステムを導入したいという企業は常に存在し、認証・認定企業はコンスタントに誕生している。ISMS 認証取得組織数は JIPDEC 統計で 2013 年 1 月現在 4,209 件、プライバシーマーク認定取得企業数は 12,934 社となっている。

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（JISQ20000 規格）や事業継続マネジメントシステム（BS25999）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。更に事業継続管理によって災害等の不測事態から企業経営を守る思想も浸透してきた。

2011、2012 年度は「情報セキュリティコンサルテーション」市場全体ではプラス成長を記録したものの、一部のサービス分野でマイナス成長となった。これは、東日本大震災の発生による影響が大きかったものと想定される。しかし一方で、震災の発生によりこれまで以上に事業継続管理の必要性が広く認知される結果となり、社会的な要請も高まっている。2012 年度の結果からもマイナス傾向が収束しつつあることが認められ、2013 年度は一転して全ての分野においてプラス成長となることが予想される。

(2) 市場規模とその推移

表 10 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 17 にその市場規模の推移のグラフを示す。

表 10　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

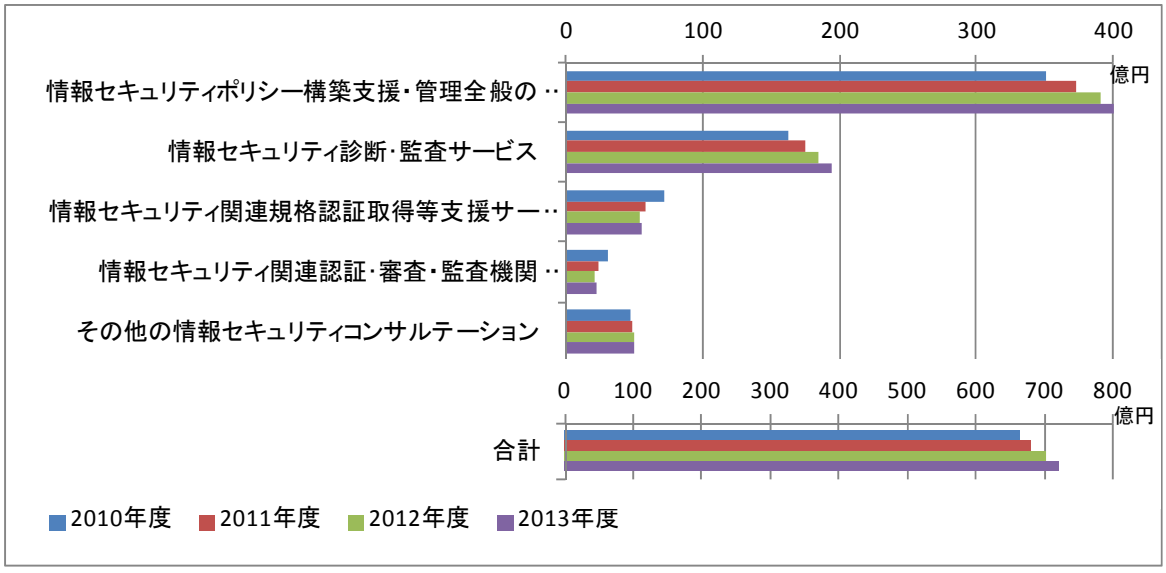
市場規模（百万円）	2010 年度	2011 年度	2012 年度	2013 年度
情報セキュリティポリシー構築支援・管理全般のコンサルテーション	35,093	37,363	39,074	40,031
情報セキュリティ診断･監査サービス	16,231	17,483	18,512	19,365
情報セキュリティ関連規格認証取得等支援サービス	7,230	5,795	5,418	5,554
情報セキュリティ関連認証･審査・監査機関（サービス）	3,015	2,370	2,169	2,195
その他の情報セキュリティコンサルテーション	4,702	4,916	4,977	5,036
合計	66,271	67,928	70,150	72,181
構成比				
情報セキュリティポリシー構築支援・管理全般のコンサルテーション	53.0%	55.0%	55.7%	55.5%
情報セキュリティ診断･監査サービス	24.5%	25.7%	26.4%	26.8%
情報セキュリティ関連規格認証取得等支援サービス	10.9%	8.5%	7.7%	7.7%

情報セキュリティ関連認証･審査・監査機関（サービス）	4.5%	3.5%	3.1%	3.0%
その他の情報セキュリティコンサルテーション	7.1%	7.2%	7.1%	7.0%
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・管理全般のコンサルテーション	ー	6.5%	4.6%	2.4%
情報セキュリティ診断･監査サービス	ー	7.7%	5.9%	4.6%
情報セキュリティ関連規格認証取得等支援サービス	ー	-19.8%	-6.5%	2.5%
情報セキュリティ関連認証･審査・監査機関（サービス）	ー	-21.4%	-8.5%	1.2%
その他の情報セキュリティコンサルテーション	ー	4.6%	1.2%	1.2%
合計	ー	2.5%	3.3%	2.9%

2011 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 679 億円程度となり、前年度比成長率はプラス 2.5%であった。ただし、「情報セキュリティ関連規格認証取得等支援サービス」と「情報セキュリティ関連認証・審査・監査機関（サービス）」では前年度と比べてマイナス成長となっている。これは、経済不況や東日本大震災の影響も一部にあるものの、認証取得への取組みが一巡し、新規取得数が大幅に減少していることが大きな要因であると考えられる。2012 年度も全体で 702 億円程度（前年度比成長率プラス 3.3%）と引き続き増加傾向である中で、認証取得関連のサービスは変わらずマイナス成長であるものの、マイナス幅は縮小しつつあり、2013 年度には増加へ転じるものと予測される。

比較的規模の大きなセグメントは「情報セキュリティポリシー構築支援・管理全般のコンサルテーション」の 374 億円、「情報セキュリティ診断・監査サービス」の 175 億円の 2 つで、合わせて市場全体の 80.7%を占める。この市場構成比は今後も大きくは変わらないものと予想される。

図 17　国内情報セキュリティコンサルテーション市場推移



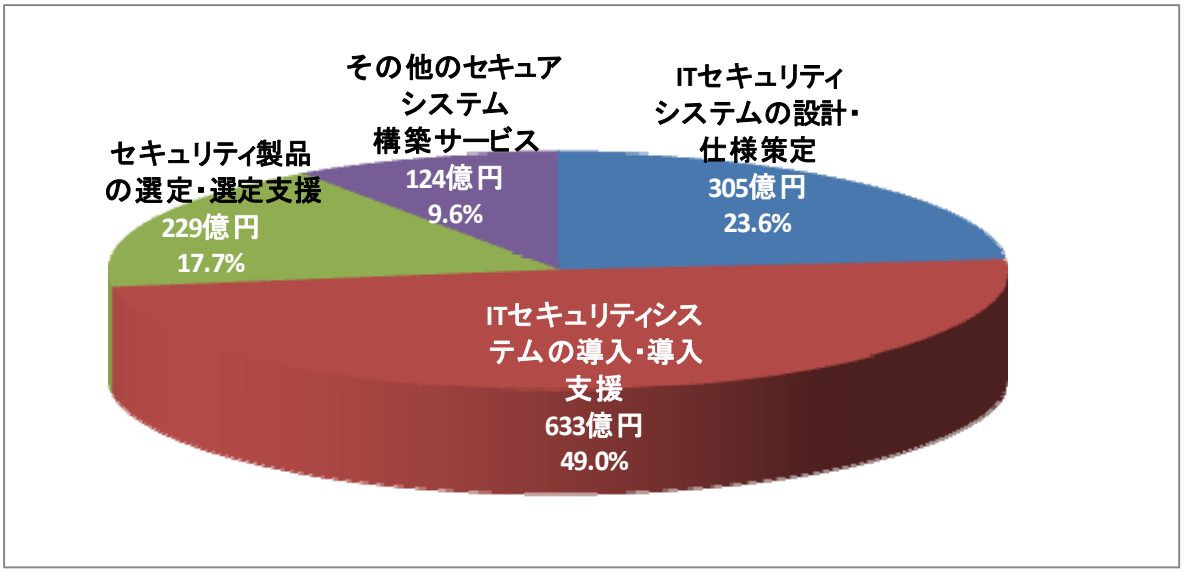
2011 年度において、最も低い前年度比成長率を示したのは「情報セキュリティ関連認証・審査・監査機関（サービス）」のセグメントで、前年度比 21.4%減の 24 億円になった。2012 年度は 8.5%減の 22 億円となる。規格認証取得の市場は取得済み件数の増加分イコール市場であり、増加のペースが落ちれば市場の縮小に直結するという厳しい性格を持ったビジネス分野である。従って、新規取得意欲や取組み余力がそがれる不況期や震災等の非常時には相当厳しいものとなろう。また、国内の ISMS 認証取得件数（JIPDEC 認証）はすでに 4000 件を超えて[7]おり、国際的に見ても突出して高い。また、PCIDSS 認証においては、クレジットカード決済代行を行う国内サービスプロバイダの 6 割が既に認証を取得済みであり、市場が飽和しつつあると考えられる。これらの要素も新規認証取得数の減少に結びついていると考えられる。これを反映して「情報セキュリティ関連規格認証取得等支援サービス」市場も 2011 年度 58 億円（前年度比成長率マイナス 19.8%）、2012 年度 54 億円（同マイナス 6.5%）と縮小している。ただし 2013 年度は全ての分野でプラス成長が見込まれることは前述の通りである。

2.2.2.2. セキュアシステム構築サービス市場

(1) 市場の動向

図 18 に 2011 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。

図 18　2011 年度のセキュアシステム構築サービス市場



「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、およ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、2010 年度 1,222 億円、2011 年度 1,291 億円、2012 年度には 1,388 億円とプラス成長がみられ、2013 年度には 1,444 億円と過去最高の市場規模に達すると推測される。情報セキュリティサービス市場全体の 40%を占めており、セキュ

[7] http://www.isms.jipdec.or.jp/lst/ind/suii.html
http://www.iso.org/iso/home/standards/certification/iso-survey.htm

リティツールも含めた情報セキュリティ市場全体でも 2 番目のカテゴリを形成している。

「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」は、セキュリティ専門家によるシステム設計・構築時に必要であった支援が、昨今設計・仕様の策定時にセキュリティの要素も組み込まれて来ており、そのため個別に切り出した発注は減る傾向にあると観察される。それに対し、2011 年に東日本大震災の発生、1 億人規模の情報漏えい（盗難）、大規模な標的型攻撃被害が発生し、構築済みであったポリシーやセキュリティアーキテクチャを見直したり、再構築する動きが、大企業を中心に一気に広がった。その結果同年度にはプラス成長に転じたと見られる。その後は企業業績の改善が進んだことから、情報セキュリティへの投資を積極化する傾向にあり、これらの動向から市場規模は徐々に拡大する方向にあると見られる。

違う側面で、2009 年度以降、国内事業者から SaaS／PaaS やクラウド型のサービス提供やプライベートクラウドの構築等の事例が増えてきた。SaaS／PaaS やクラウドの場合は、そのシステムを利用し早期に目的を実現できる点にユーザが有意性を見出していることもあり、セキュリティシステムの構築はサービス提供側がパッケージとして組み込んでいるケースが増えていると考えられる。

また新規に対応・導入が必要となるセキュリティ技術に関する相談支援も必要となってくるであろう。「暗号危殆化に対する移行支援」「DNSSEC[8]」「IPv6」「DKIM[9]」等、導入・運用ノウハウのない技術への対応は 2010 年頃から本格化し、当市場の需要に貢献することも期待される。

(2) 市場規模とその推移

表11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19にその市場規模の推移のグラフを示す。

表 11　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）	2010 年度	2011 年度	2012 年度	2013 年度
IT セキュリティシステムの設計･仕様策定	29,226	30,528	32,344	33,650
IT セキュリティシステムの導入･導入支援	60,056	63,304	69,118	71,906
セキュリティ製品の選定･選定支援	21,345	22,902	24,509	25,436
その他のセキュアシステム構築サービス	11,603	12,383	12,849	13,397
合計	122,229	129,116	138,821	144,389
構成比				
IT セキュリティシステムの設計･仕様策定	23.9%	23.6%	23.3%	23.3%
IT セキュリティシステムの導入･導入支援	49.1%	49.0%	49.8%	49.8%
セキュリティ製品の選定･選定支援	17.5%	17.7%	17.7%	17.6%

[8] Domain Name System SECurity extension　DNS サーバが提供する IP アドレスとホスト名の対応付け情報を電子署名を用いて証明することで DNS キャッシュポイズニング等の成りすまし攻撃を防止する技術および機能

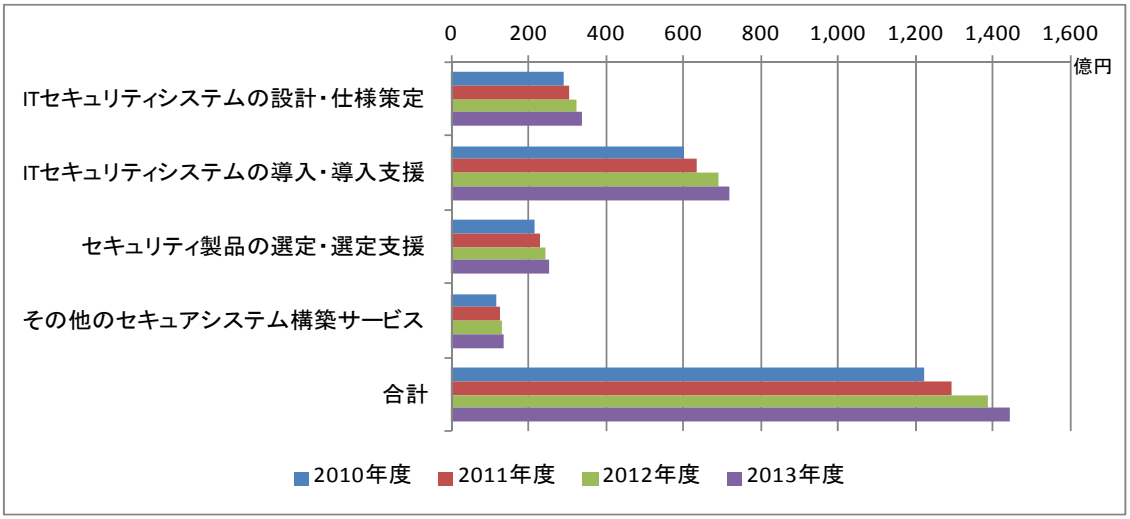
[9] Domain Keys Identified Mail 電子メールの送信元ドメインの実在と真正性を電子署名を用いて確認するための技術

その他のセキュアシステム構築サービス	9.5%	9.6%	9.3%	9.3%
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	―	4.5%	6.0%	4.0%
IT セキュリティシステムの導入･導入支援	―	5.4%	9.2%	4.0%
セキュリティ製品の選定･選定支援	―	7.3%	7.0%	3.8%
その他のセキュアシステム構築サービス	―	6.7%	3.8%	4.3%
合計	―	5.6%	7.5%	4.0%

「セキュアシステム構築サービス」カテゴリのうち最大のセグメントは約 2 分の 1 を占める「IT セキュリティシステムの導入･導入支援」であり、2010 年度 601 億円、2011 年度 633 億円（前年度比+5.4%）、2012 年度 691 億円（同+9.2%）、2013 年度予測 719 億円（同+4.0%）の規模と推測される。これに次ぐのが「IT セキュリティシステムの設計・仕様策定」で、4 分の 1 弱を占める。金額は 2010 年度 292 億円、2011 年度 305 億円（前年度比+4.5%）、2012 年度 323 億円（同+6.0%）、2013 年度予測 337 億円（同+4.0%）と推定する。

「セキュリティ製品の選定･選定支援」はシステム構築まで至らず個別の製品を選定するに際して利用する専門家のサービスで、市場規模も限定的である。2011 年度が 229 億円（前年度比+7.3%）、2012 年度は 245 億円（同+7.0%）、2013 年度には 254 億円（同+3.8%）と推測される。

図 19　国内セキュアシステム構築サービス市場推移



2.2.2.3. セキュリティ運用・管理サービス市場

(1) 市場の動向

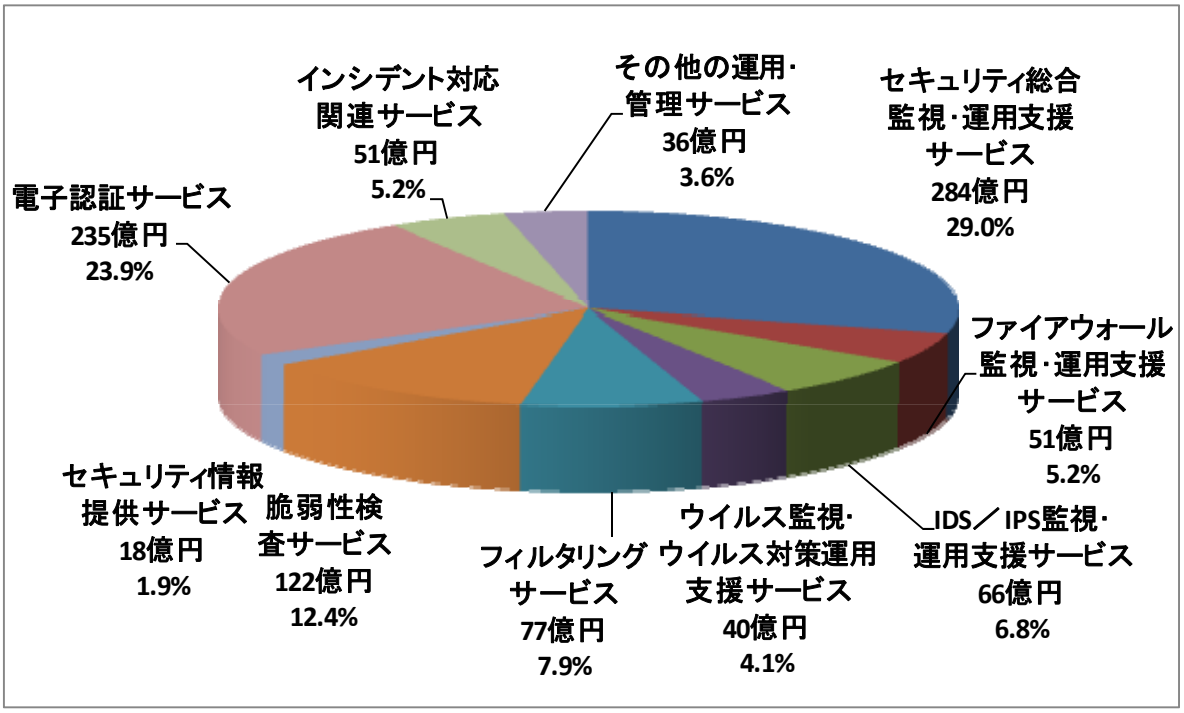
セキュリティ運用・管理サービス市場は、セキュリティ対応は適切な社外の専門サービス提供者にアウトソースする必要があるという需要によって支えられている。背景には、セキュリティ対策機器の運用管理が専門家の知識を益々必要とする一方、そのような専門スキルを有する人材が利用組織内に不足していることや、問題発生時には迅速かつ適切な対応が必要とされることがある。ネットワーク脅威の複雑化・深刻化と、セキュリティ対策が高度化・統合化に向う流れを

背景に、かつ、クラウドサービスの増加も牽引し、この「セキュリティ運用・管理サービス」市場は中長期的に見て拡大傾向にあると考えられる。リーマンショック以降急速に悪化した経済状勢から次第に回復し、2011 年度において日本企業へのサイバー攻撃が危機感を高め、全てのセグメントでプラス成長となった。2012 年度以降もプラス成長が継続すると予想される。

図 20 に 2011 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。

運用支援サービスについては、「ファイアウォール監視・運用支援サービス」と「IDS／IPS 監視・運用支援サービス」それに「ウイルス監視･ウイルス対策運用支援サービス」が各々の市場を形成している。また、それらの機能を統合し総合的に監視・運用支援する「セキュリティ総合監視・運用支援サービス」も大きな市場となっている。「ファイアウォール監視・運用支援サービス」と「IDS／IPS 監視・運用支援サービス」はサイバー攻撃に対する防御策として新規にサービスを受けた企業が増加しプラス成長となった。なお、サイバー攻撃に対しては自社内でツールを導入・運用するよりは社外の専門サービスを利用した方が効果があると判断した企業が増え、ツールよりもサービスの方が大幅成長となった。それに比べて「ウイルス監視･ウイルス対策運用支援サービス」は、クラウド化への移行が実施され若干増加したものの、「ファイアウォール監視・運用支援サービス」や「IDS／IPS 監視・運用支援サービス」ほどの顕著な成長には至らなかった。

図 20　2011 年度のセキュリティ運用･管理サービス市場



「フィルタリングサービス」は、メールフィルタリングサービスと Web フィルタリングサービスの両方を含むが、クラウド化が進み社内システムの外部サービス利用化に移行し始めているが、この両システムが比較的外部委託しやすくクラウド化の手始めにフィルタリングシステムを社外サービスに移行した企業が増えたため大幅な成長となった。

「脆弱性検査サービス」は、サイバー攻撃が危機感をあおり、増加傾向にある。特に Web 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。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サービスが増加したことにより、コンスタントな成長を続けている。また大手システムインテグレータでは、新規開発の Web アプリケーションを、カットオーバー・引渡し前に第三者に委託してテストすることも一般化しつつあり、この面からも「脆弱性検査サービス」の成長が期待される。

「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経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Web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続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。

2011 年度最大の伸び率を示したのが「インシデント対応関連サービス」である。これはまさにサイバー攻撃を受けた企業や国の機関が増加しため大幅成長となった。インシデント対応は機械的にできない部分も多く人件費等サービス単価が高いこともありこのような結果となった。2012 年度もサイバー攻撃は継続されると思われるためこのセグメントの市場規模の拡大が見込まれる。

(2)市場規模とその推移

表 12 にセキュリティ運用・管理サービス市場規模の実績推定値と予測値を示す。

「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、2011 年度の実績推定値が 981 億円であり、2010 年度の 904 億円と比較すると 8.5%の増加となった。金額規模では、「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おり、かつ、「情報セキュリティサービス市場」の中では最大の成長率となった。これは、サイバー攻撃に起因するものと考えられる。情報セキュリティ脅威の深刻化と複雑化に伴い、また経済の IT 依存度の上昇に伴い、専門家によるサービスである当市場は他のカテゴリに比べて安定的な拡大傾向にあり、また、部分的にはサイバー攻撃等の外部要因にも左右される傾向が強い。

表 12　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	2010 年度	2011 年度	2012 年度	2013 年度
セキュリティ総合監視･運用支援サービス	26,556	28,427	29,781	32,154
ファイアウォール監視･運用支援サービス	4,709	5,096	5,296	5,647
IDS／IPS 監視･運用支援サービス	6,222	6,635	6,876	7,202
ウイルス監視･ウイルス対策運用支援サービス	3,924	4,005	4,117	4,367
フィルタリングサービス	7,084	7,722	8,197	8,641
脆弱性検査サービス	11,484	12,199	13,284	14,051
セキュリティ情報提供サービス	1,707	1,829	1,905	1,941
電子認証サービス	21,311	23,488	24,641	25,555
インシデント対応関連サービス	3,903	5,107	5,298	5,761

その他の運用･管理サービス	3,476	3,563	3,697	3,843
合計	90,375	98,071	103,092	109,163
構成比				
セキュリティ総合監視･運用支援サービス	29.4%	29.0%	28.9%	29.5%
ファイアウォール監視･運用支援サービス	5.2%	5.2%	5.1%	5.2%
IDS／IPS 監視･運用支援サービス	6.9%	6.8%	6.7%	6.6%
ウイルス監視･ウイルス対策運用支援サービス	4.3%	4.1%	4.0%	4.0%
フィルタリングサービス	7.8%	7.9%	8.0%	7.9%
脆弱性検査サービス	12.7%	12.4%	12.9%	12.9%
セキュリティ情報提供サービス	1.9%	1.9%	1.8%	1.8%
電子認証サービス	23.6%	23.9%	23.9%	23.4%
インシデント対応関連サービス	4.3%	5.2%	5.1%	5.3%
その他の運用･管理サービス	3.8%	3.6%	3.6%	3.5%
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	－	7.0%	4.8%	8.0%
ファイアウォール監視･運用支援サービス	－	8.2%	3.9%	6.6%
IDS／IPS 監視･運用支援サービス	－	6.6%	3.6%	4.7%
ウイルス監視･ウイルス対策運用支援サービス	－	2.1%	2.8%	6.1%
フィルタリングサービス	－	9.0%	6.2%	5.4%
脆弱性検査サービス	－	6.2%	8.9%	5.8%
セキュリティ情報提供サービス	－	7.2%	4.1%	1.9%
電子認証サービス	－	10.2%	4.9%	3.7%
インシデント対応関連サービス	－	30.9%	3.7%	8.7%
その他の運用･管理サービス	－	2.5%	3.8%	4.0%
合計	－	8.5%	5.1%	5.9%

図 21 に国内セキュリティ運用・管理サービス市場規模の推移のグラフを示す。表 12 と合せて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、2011 年度の推定実績市場規模は 284 億円（前年度比成長率+7.0%）と、2010 年度の 266 億円から大きく増加した。2012 年度もプラス成長を続け、 2013 年度には 322 億円と順調に成長していくものと予測される。

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」、および「ウイルス監視・ウイルス対策運用支援サービス」の実績市場規模推定値は 2011 年度で各々51 億円（前年度比成長率+8.2%）、66 億円（同+6.6%）、40 億円（同+2.1%）とプラス成長となり、2012 年度も継続してそれぞれ 53 億円（同+3.9%）、69 億円（同+3.6%）、41 億円（同+2.8%）とプラス成長を続け、2013 年度にはそれぞれ 56 億円（同+6.6%）、72 億円（同+4.7%）、44 億円（同+6.1%）と、増加していく見込みである。

クラウド化が進み、社内システムからの外部委託サービスへの移行が増加している「フィルタ

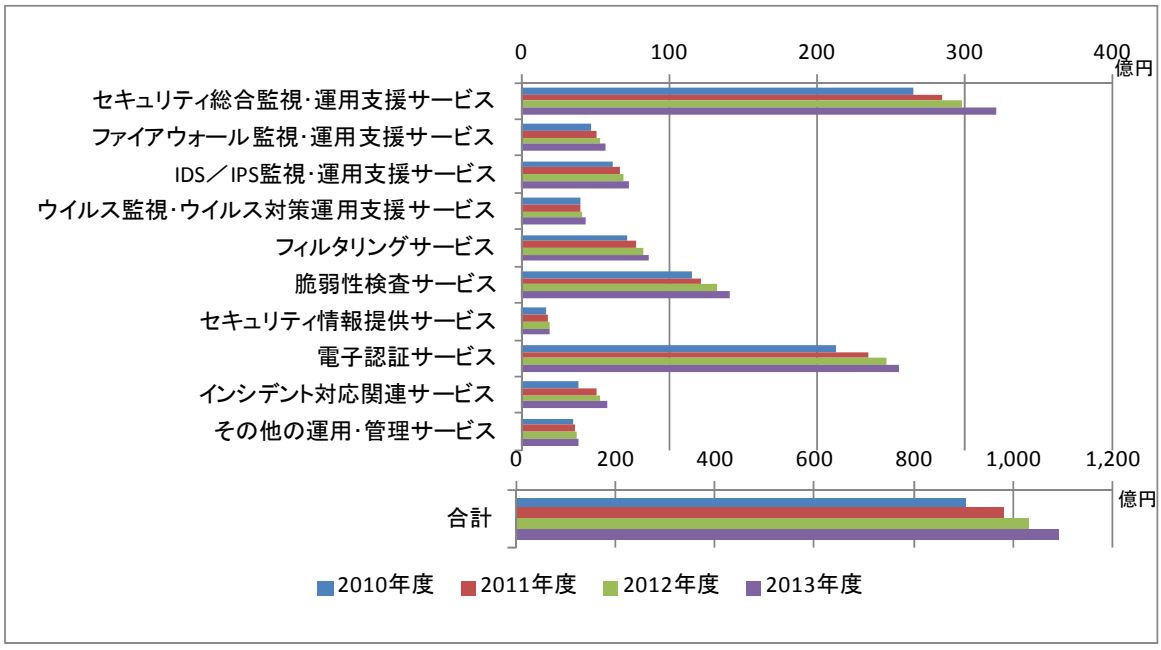
リングサービス」は、2011 年度に 77 億円（同+9.0%）と大幅なプラス成長を遂げた。2012 年度には 82 億円（同+6.2%）、2013 年度には 86 億円（同+5.4%）と大幅なプラス成長が継続して見込まれる。

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、増加傾向を示しているセグメントが「脆弱性検査サービス」であるが、2011 年度においては 122 億円（同+6.2%）、2012 年度には 133 億円（同+8.9%）、2013 年度には 141 億円（同+5.8%）と、順調に成長していくと思われる。

「セキュリティ情報提供サービス」については、2011 年度で 18 億円（同+7.2%）と限定的な市場である。2012 年度・2013 年度も金額では 19 億円前後と横ばいになり、今後それ程の市場拡張は望めないと予測される。

「電子認証サービス」は、「セキュリティ運用・管理サービス」では、「セキュリティ総合監視・運用支援サービス」に次ぐ最大の市場であり 2011 年度は 235 億円（同+10.2%）と大幅にプラス成長している。これは一度電子証明書を導入した顧客は継続して利用を行なうためマイナス成長にはなりづらい点や、仮想化の普及で証明書数が増加したことやサイバー攻撃からの防御策の 1 つとして暗号化通信を広く実施したこと等が挙げられる。2012 年度以降も 2011 年度程顕著ではないがコンスタントな伸びが予測され、2012 年度は 246 億円（同+4.9%）、2013 年度は 256 億円（同+3.7%）の見込みとなっている。

図 21　国内セキュリティ運用・管理サービス市場推移



「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あるためにインシデントの発生頻度や個々のインシデントの大きさによって市場規模に影響を与える傾向が強い。2011 年度はサイバー攻撃の影響でセキュリティ市場最大の伸び率を示し、51 億円（同+30.9%）と爆発的に高い伸びを見せた。2012 年度以降もサイバー攻撃は継続して発生する可能性が高く、

2012 年度は同+3.7%で 53 億円となり、2013 年度には 8.7%伸びて 58 億円と予想される等、順調な成長傾向にあると見込んでいる。

2.2.2.4. 情報セキュリティ教育市場

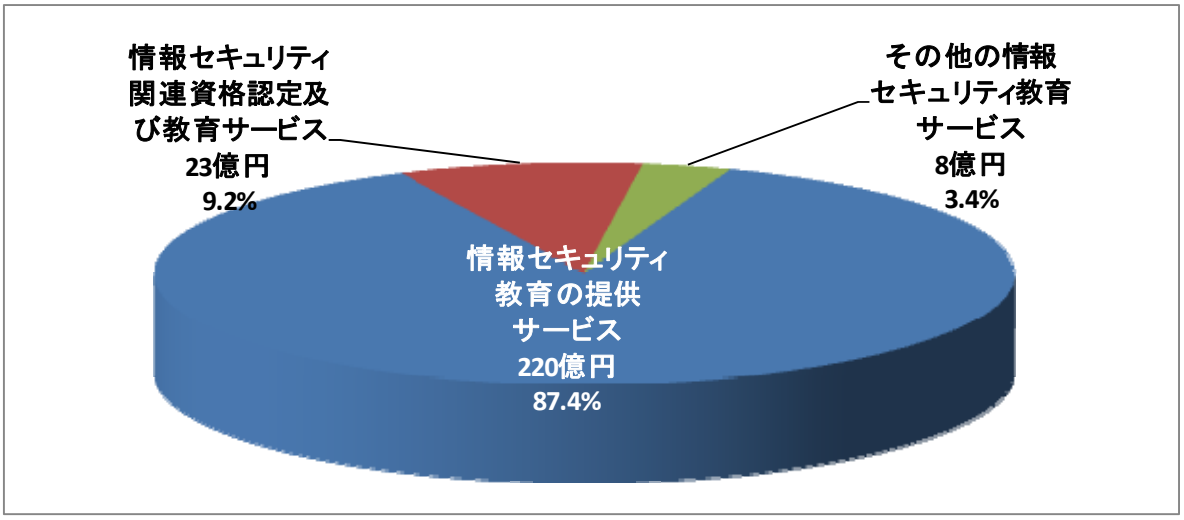
(1) 市場動向

図22に2011年度の情報セキュリティ教育市場のセグメント別分布を示す。

教育は、一般的には 3K と言われて不況下でいち早く抑制対象とされる経費と言われている。情報セキュリティ教育については、サイバー脅威の高まりと、そのリスクに対する企業の認知の浸透に支えられて、緩やかながら市場規模の拡大が続いている。ただし、経済環境が厳しい中で経費削減を求められるところから、従来専門家のノウハウを取り入れるために外部委託していたものを、一部内製に切り替えるとか、対象を絞って実施するといった経費節減策の影響は表れていると考えられる。

情報セキュリティ教育は、大きく 3 つに大別できる。一つは新入社員を含む全社員を対象とする情報セキュリティリテラシ教育で、知的財産や個人情報の漏えい・紛失のリスク、標的型攻撃の手口とリスクを教え、日ごろの対策や注意点を理解させる。二つ目はシステム関係部署や情報セキュリティ対応部署に対する専門教育。そして三つ目は経営層や上級管理職に対しての、経営リスクとしての情報セキュリティリスクとそのリスクマネジメントの視点からの知識や考え方の理解を目指したものとなる。このように情報セキュリティ教育は多岐にわたり、専門知識を必要とするものが多く、専門家によるサービスの需要を形成している。

図 22　2011 年度の情報セキュリティ教育市場



新入社員や全社員を対象とする一般・基礎知識（リテラシ）の教育では、e - ラーニングがよく使われる。受講者の都合に合わせて受講できる一方、同一のコンテンツを提供でき、受講状況と効果を個別にフォローできるメリットがある。集合研修よりも費用を抑えるメリットが高く、教育・研修費の削減傾向が利用拡大につながっている。また、SaaS モデルによる低価格も期待でき、中堅・中小企業においても e - ラーニングサービスの活用が容易になることから、利用者拡

大の傾向にあると見られる。自営の場合は本統計外だが、外部サービスとして提供されるものやコンテンツの外部購入部分は「情報セキュリティ教育の提供サービス」にカウントしている。

「情報セキュリティ関連資格認定および教育サービス」市場は、対象者が資格取得を目的とする個人に特定されるため、基本的には小規模な市場である。しかし、企業において情報セキュリティ対策に従事する技術者のスキルレベルの確認手段として、グローバルな「世界標準の情報セキュリティ資格」を活用するニーズも現れてきている。そのため資格取得に向け費用面の会社負担やインセンティブの提供のほか、資格保有を採用に際しての必須または優遇条件基準とする等の活用策も見られる。このような動きを背景に、企業の指示によるものや、自らのキャリアパスのために個人の負担で資格に挑戦する受講者も増えていると見られる。

(2) 市場規模とその推移

表 13 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 23 にその市場規模の推移のグラフを示す。

表 13　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）	2010 年度	2011 年度	2012 年度	2013 年度
情報セキュリティ教育の提供サービス	20,798	22,018	23,335	23,989
情報セキュリティ関連資格認定および教育サービス	2,249	2,321	2,392	2,467
その他の情報セキュリティ教育サービス	834	846	875	876
合計	23,880	25,185	26,601	27,332
構成比				
情報セキュリティ教育の提供サービス	87.1%	87.4%	87.7%	87.8%
情報セキュリティ関連資格認定および教育サービス	9.4%	9.2%	9.0%	9.0%
その他の情報セキュリティ教育サービス	3.5%	3.4%	3.3%	3.2%
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	－	5.9%	6.0%	2.8%
情報セキュリティ関連資格認定および教育サービス	－	3.2%	3.0%	3.1%
その他の情報セキュリティ教育サービス	－	1.5%	3.4%	0.2%
合計	－	5.5%	5.6%	2.7%

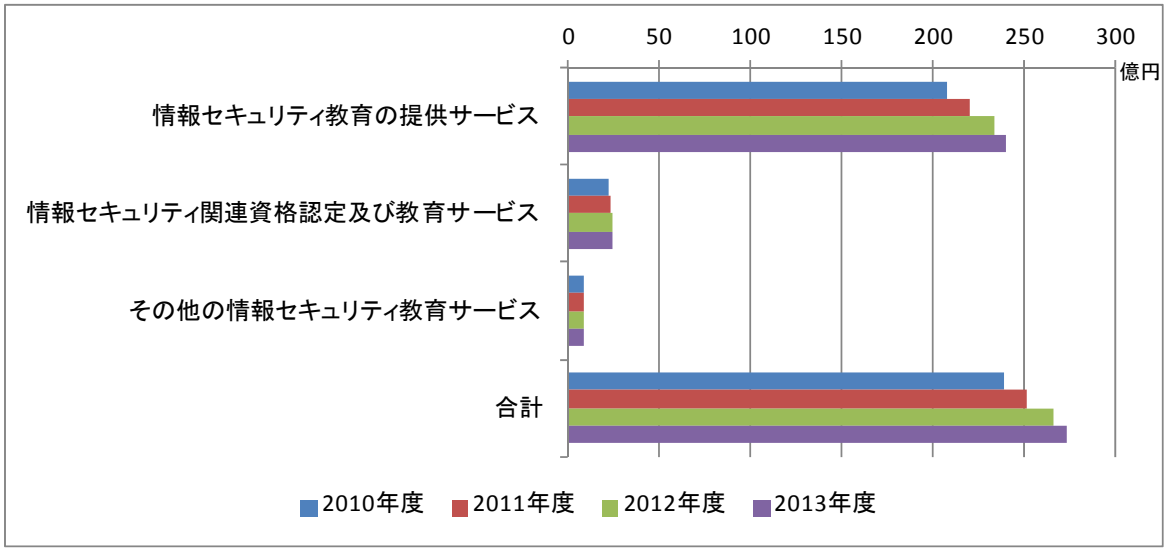
「情報セキュリティ教育」カテゴリは、情報セキュリティサービス全体の市場に占める割合が 8%弱程度と比較的小さい市場であり、2010 年度の市場規模は 239 億円程度と推測され、若干の縮小傾向が見られた。2011 年度は内部犯行（外注含む）や標的型攻撃による被害の深刻化から対策への注力が高まったことを反映しての市場は拡大し、5.5%増の 252 億円となった。2012 年度も同様の傾向が続き、5.6%成長して 266 億円程度になったものと推測される。2013 年度も同じ傾向は続くものの成長率は鈍化し、2.7%増で 273 億円規模に達するものと予測する。

このカテゴリの最大のセグメントは87%を占める「情報セキュリティ教育の提供サービス」で

ある。ここには前々回まで別掲としていた「情報セキュリティ教育のe-ラーニングサービス」が含まれる。市場規模は2010年度に208億円、2011年度には220億円（前年度比成長率+5.9%）、2012年度には233億円（同+6.0%）、2013年度は240億円弱（同+2.8%）と、順調に拡大すると予測される。

「情報セキュリティ関連資格認定および教育サービス」は2010年度において22億円のマーケットであったが、2011度には前年度比3.2%増の23億円の規模になったと推測される。2012年度もその傾向は続き同3.0%増の24億円、2013年度には同3.1%増の25億円と、少しずつではあるが拡大傾向に向かうと考えられる。リーマンショック以降の企業の経費節減と個人の投資縮小の両面から影響を受けて縮小傾向が続いていたが、企業の対策強化や投資拡大への転換、また定年を迎える団塊世代が第二の人生の武器として資格取得に取り組むといった要因から、拡大に向かうものと推測される。

図 23　国内情報セキュリティ教育市場推移



2.2.2.5. 情報セキュリティ保険市場

(1) 市場の動向

情報セキュリティ保険は、情報資産、すなわち IT システム並びにその上で取り扱われる情報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。

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が、SI 事業者の商品・サービスの品揃えの一環としてグループ内損保子会社または損保会社と提携して開発する事例も見られる。

情報セキュリティ保険の需要者は、通信事業者、金融業や通信販売、小売業のような個人情報

を多量に扱う業態、更に一般事業法人等多岐にわたる。販売チャネルも一般の保険販売ルートの他、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、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。また、ネットワークセキュリティ対策製品とのバンドル販売も行われている。さらに、保険の代理店が情報セキュリティ保険の営業過程で情報セキュリティに関するコンサルテーションを提供するケースもある。また、保険料の算定に際しても、例えば ISMS 認証取得企業の料率が優遇される等、情報セキュリティ対策との組合せによるバリエーションがあるのも特徴と言える。

アメリカでは標的型攻撃のリスクに対して保険を買う動きが強まっているとの情報もあり、日本の情報セキュリティ保険市場も拡大に向かうことが予測される。

(2)市場規模とその推移

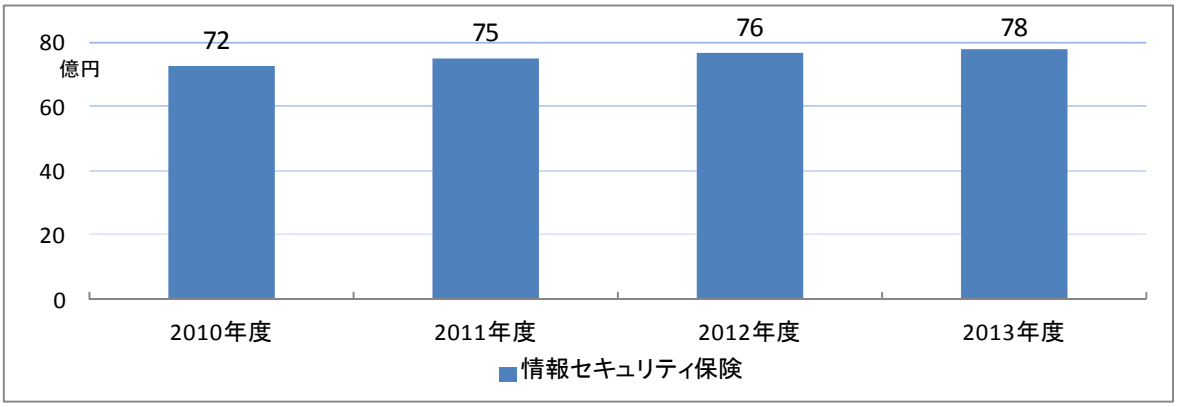
表 14 に国内情報セキュリティ保険市場規模の実績推定値と予測値を、図 24 にその市場規模の推移のグラフを示す。

表 14　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）	2010 年度	2011 年度	2012 年度	2013 年度
情報セキュリティ保険	7,236	7,497	7,647	7,800
対前年比成長率（%）	－	3.6%	2.0%	2.0%

「情報セキュリティ保険」市場は、2006 年度に急拡大して 70 億円規模に達した後は落ち着いた動きで推移してきたと考えられ、2010 年度の市場規模は 72 億円程度と見込まれる。その後は情報セキュリティ対策の見直し・強化や深刻化する情報流出リスクへの対応から漸増傾向を示すものと考えられる。その結果 2011 年度は 3.6%増の 75 億円、2012 年度は 2.0%増の 76 億円となり、2013 年度は同じく 2.0%増の 78 億円規模にまで拡大するものと予測した。

図 24　国内情報セキュリティ保険市場推移



第３章 情報セキュリティにおける新しい課題と動き

3.1. 2012 年度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は、2013 年 3 月 12 日に「2013 年版 10 大脅威　身近に忍び寄る脅威」[10]を発表した。この 3 年間の 10 大脅威をリスト化して見ると、以下のようになる。

表 15　最近 3 年間の IPA10 大脅威の推移

	2013 年	2012 年	2011 年
第 1 位	クライアントソフトの脆弱性を突いた攻撃	機密情報が盗まれる！？新しいタイプの攻撃 （標的型攻撃に関する脅威）	「人」が起こしてしまう情報漏えい
第 2 位	標的型諜報攻撃の脅威	予測不能の災害発生！引き起こされた業務停止 （災害に関する脅威）	止まらない！ウェブサイトを経由した攻撃
第 3 位	スマートデバイスを狙った悪意あるアプリの横行	特定できぬ、共通思想集団による攻撃	定番ソフトウェアの脆弱性を狙った攻撃
第 4 位	ウイルスを使った遠隔操作	今もどこかで…更新忘れのクライアントソフトを狙った攻撃	狙われだしたスマートフォン
第 5 位	金銭窃取を目的としたウイルスの横行	止まらない！ウェブサイトを狙った攻撃	複数の攻撃を組み合わせた「新しいタイプの攻撃」
第 6 位	予期せぬ業務停止	続々発覚、スマートフォンやタブレットを狙った攻撃	セキュリティ対策不備がもたらすトラブル
第 7 位	ウェブサイトを狙った攻撃	大丈夫！？電子証明書に思わぬ落し穴 （証明書に関する脅威）	携帯電話向けウェブサイトのセキュリティ
第 8 位	パスワード流出の脅威	身近に潜む魔の手・・・あなたの職場は大丈夫？ （内部犯行に関する脅威）	攻撃に気づけない標的型攻撃
第 9 位	内部犯行	危ない！アカウントの使いまわしが被害を拡大！	クラウドコンピューティングのセキュリティ
第 10 位	フィッシング詐欺	利用者情報の不適切な取扱いによる信用失墜 （プライバシーに関する脅威）	ミニブログサービスや SNS の利用者を狙った攻撃

（IPA 各年度発表をもとに JNSA 作成）

2012 年版の見出しは「変化・増大する脅威」となっており、2011 年版には「進化する攻撃」の文字が見える。2013 年版は上記のように「身近に忍び寄る脅威」であり、脅威が深刻化して身近に迫っていることを示している。3 年間で、同じまたは類似の脅威が繰り返し取り上げられており、それを色分けしてみた。いずれも、まさに日常業務と隣り合わせのところに、サイバー攻撃の脅威が迫っている。

最も上位に位置すると考えられるのがアプリケーションの脆弱性を狙った脅威である。永年利

[10] http://www.ipa.go.jp/security/vuln/10threats2013.html

用されてきたJAVAに最近になって深刻な脆弱性が見つかる等、問題は深刻化している。同時に、JAVA等はブラウザの中で意識しない間に動いているプログラムであり、ITリテラシが十分でなければ気付かないし、対策もしようがないというところに脅威が迫っているという問題でもある。

次に「常連化」している脅威は標的型攻撃である。本当に用意周到に、組織内部にしか通用しない情報を組み込んだメールと添付ファイルでわなを仕掛けられると、一般の従業者では、すべてを見破ることは不可能と言ってよい。

そして「Webサイトを狙った攻撃」も常態化している。改ざんやマルウェア埋め込みに無防備なWebがなくならない上に、ドライブバイダウンロード[11]を仕掛けたサイトへの誘導メールも巧妙化しているので、これも被害に遭うことを未然防止することは不可能に近い。

この3項目に共通していることは、本人が気付かないうちにマルウェアを仕掛けられる可能性である。従い、自分のPCに、少なくとも自分が接続しているネットワークセグメントのどこかに、何らかのマルウェアが潜入している可能性がかなりの確度であることを、すべての人が覚悟しなければならない。

そのような自覚の上で、以下のようないくつかの注意を常に払う必要がある。秘密の情報にはパスワード等で暗号化やアクセス制御を施すこと。サーバ等へのログオンのための認証情報（ID、パスワード等）はPC内に裸で保管することは避けること。データは原則としてローカルに保存せず、きちんと管理されたサーバに格納すること。等である。

10大脅威で次に目につくのは、スマートデバイスに関する脅威である。スマートフォンやタブレット型PC等は、ほぼ「電話もできるPC」である。マルウェア感染の脅威はPCと同等以上にある。特に昨今脅威となっているのが、デバイス上にある個人情報等が勝手に外部に送信されることによる情報漏えいやプライバシー侵害である。さらに、BYOD[12]を含め、業務でのスマートデバイスの活用が広まる中で、スマートデバイスに収納した秘密情報が紛失したり盗難に遭ったりする問題である。スマートデバイスの高い携帯性は、持ち運び途中や先での紛失盗難置忘れ等のリスクも高まる。ログオン認証の敷居は概して低い傾向にあり、紛失すれば中を見られる可能性は高い。その普及の早さもあり、新たな脅威となっている。

もう一つ注目すべきなのが「内部犯行」である。2009年の三菱UFJ証券における顧客情報持ち出し・売却事件や2007年のデンソーにおける技術情報盗難事件が典型例だが、情報にアクセスできる立場やその周辺にいる内部者が、そのアクセス権を悪用して情報を持ち出す事件も後を絶たない。これはインターネットからの脅威だけでなく、内部にもリスクが存在することを意味している。

いずれの場合も、すでに内部ネットワークは往来と同レベルのセキュリティと考えざるを得ない。目の前を見知らぬ人が自由に行き来できる環境では、身の回りのものすべてに鍵をかけ、ワイヤを回さなければならないが、それと同じ覚悟でネットワークを使う時代になってきた、ということを認識する必要がありそうである。

こうして傾向を受けて、セキュリティ対策の面では、内部ネットワークの監視やログの徹底取

---

[11] Webサイトに見えない形でマルウェアを仕掛け、そのサイトを閲覧することやサイト上のボタン等をクリックすることによって、閲覧者のパソコン等にマルウェアをダウンロードさせる攻撃

[12] Bring Your Own Device 個人所有のPC、スマートデバイス等を業務に利用すること

得と効率的解析が課題として顕在化し、関連するソリューションやサービスへの需要となって表れている。また、情報そのものを守るという意味でアクセス管理のための製品、DLP 製品、そして暗号化製品への需要が相対的に高まってきている。

また、2011 年の防衛産業への標的型攻撃による被害を契機に、セキュリティ対策にはじめて本腰を入れるようになった動きや、既存のセキュリティ対策を全面的・抜本的に見直す動きも強まっている。2011 年度以降の情報セキュリティ市場の再拡大の背景には、このような状況の変化があると見ることができそうである。

3.2. Security as a Service とクラウド化の市場構造・規模への影響

(1) Security as a Service の概要

Security as a Service（以下 SecaaS）とは、セキュリティの機能をクラウドサービスとして提供することを言う。従来 IT 設備は基本的にその多くの要素を利用者が所有し、利用者の責任において運用するものであった。そのような中、クラウドコンピューティングの登場は、事業者が提供する IT サービスを設備等所有することなく利用するという、新たな選択肢を IT 利用者に与えるものとなった。クラウドを利用することによって、設備投資をすることなく、必要なときに必要な量のコンピューティングリソースを使うといった、柔軟な運用が可能となった。そのメリットは特にスタートアップ企業やスモールスタートの新事業を開始する場合のメリットが大きい。一般の企業においても、そのようなメリットを取り込むべく、IT システムにおけるクラウド利用を活発に検討・導入するようになってきている。

情報セキュリティに関する機能は、企業システムにとっては欠かせないものであるが、部分的にアウトソースサービスが利用されていたものの、従来、ガバナンスの観点から積極的に外部に出すものではなかった。しかし、システムのクラウド化の進行に伴い、そのセキュリティもクラウドサービス事業者に依存することが必然に、あるいは自然の流れになってきている。それをさらに進めて、多くの事業者がセキュリティ機能を独立のクラウドサービスとして提供するという流れを加速させている。

(2) SecaaS の種類

Cloud Security Alliance（以下 CSA）では、クラウド上で行われているセキュリティサービスをカテゴリ分けしたリサーチレポートを公表[13]している。そのカテゴリと概要は以下のようなものである。(なお、各カテゴリはあくまでも概要であり、正確な内容については CSA のレポートを参照[13]いただきたい)

Category 1: Identity and Access Management

アカウント管理、ディレクトリサービス、シングルサインオン等といった、ID マネジメント系サービスを SecaaS 事業者が提供する

Category 2: Data Loss Prevention

データのラベリング等をサービスとして提供し、データがどう使われているかといっ

[13] https://cloudsecurityalliance.org/csa-news/csa-issues-first-secaas-white-paper/
https://cloudsecurityalliance.org/research/secaas/

たモニタリングやデータ保護を SecaaS 事業者が提供する

Category 3: Web Security

Web フィルタリング等のように、Web のトラフィックをクラウドプロバイダが中継し、セキュリティ機能を SecaaS 事業者が提供する

Category 4: Email Security

SPAM 対策やアンチウイルス、アンチスパイウエア等、Email のセキュリティ機能を SecaaS 事業者が提供する

Category 5: Security Assessments

コンプライアンス監査や脆弱性検査といった、検査・監査系の機能を SecaaS 事業者が提供する

Category 6: Intrusion Management

クラウド環境内で、侵入検知や不審な挙動を検知する等のサービスを SecaaS 事業者が提供する

Category 7: Security Information and Event Management (SIEM)

セキュリティ関連のログやイベントをマネジメントするサービスを SecaaS 事業者が提供する

Category 8: Encryption

暗号化によるデータ保護、タイムスタンプ、フィンガープリントといった、暗号に関連する機能を SecaaS 事業者が提供する

Category 9: Business Continuity and Disaster Recovery

インフラの冗長化、バックアップ、データのレプリケーションといった事業継続に関わる機能を SecaaS 事業者が提供する

Category 10: Network Security

FW、IDS、DDoS プロテクションといったネットワークセキュリティに関わる機能を SecaaS 事業者が提供する

(3) 市場への影響

上記の通り、SecaaS はコンサルティングやユーザ教育等を除き、数多くの既存のセキュリティ機能をカバーしており、運用・管理系のほとんどの機能がサービスとして利用可能となっている。しかしながら、クラウドサービスはサービスを提供する事業者それぞれがサービス仕様を決めており、別事業者のサービスと連携して動作することは基本的に前提とされていない。また、ベンダ仕様によるロックイン問題も発生する可能性がある。

そのため、セキュリティ機能の大半をクラウドサービスで賄うというところまで踏み込むことは、現時点では困難ではないかと考えられる。ただし、クラウドブローカーと呼ばれる、各種のクラウドサービスを束ねて総合的にソリューションとして提供する事業者が現れることによって、これらのサービスが協調して動作可能となった場合には、流れが変わる可能性がある。

セキュリティ機能の一部の要素をクラウド化することは比較的容易に行うことができる可

能性があり、セキュリティ市場においてもクラウドによるサービス化は徐々に進行すると思われる。が、その速度は、上記のような要因から、一般の IT システムのクラウド化と比較して穏やかなものになるのではないだろうか。

市場調査における扱いについては、基本的に機能別区分としているので、従来型 SOC ベースでもクラウドベースでも、サービスの種類ごとに集計することになる。一方、Identity and Access Management (Identity as a Service)や Business Continuity and Disaster Recovery (BC & DR)等の新種のサービスは当面その他として集計対象としていくことになる。クラウドの浸透に伴い、量・質・種類とも拡大に向かうと考えられるので、引き続き注目していく予定である。

3.3. スマートデバイスのセキュリティ事情

(1) スマートデバイスの急速な普及の実態

Google のシュミット CEO は、2013 年 4 月 16 日、D: Dive Into Media 2013 の中で、Android 端末は、1 日 150 万台がアクティベートされ、2013 年末には端末の数が 10 億台に到達する見込みである事を明らかに[14]した。4 月時点で Android スマートフォンの数は 160 カ国の 320 キャリアで 7.5 億台に達しており、年末までにさらに 2.5 億台がネットワークに接続される見込みであるという。また Microsoft は、1 月 8 日、ラスベガスで開催中の 2013 International CES の JP Morgan Tech Forum で、発売からこれまでに 6000 万件の「Windows 8」ライセンス（新規 PC の OEM, アップグレード含む）を販売した事を発表[15]している。Windows8 は PC とスマートデバイスに共通で搭載可能な OS であり、Microsoft 陣営からもスマートデバイス市場への攻勢が始まっている。これにスマートフォンという新しい市場を創造したアップルの iPhone が加わり、スマートフォンだけでなくタブレット型端末を含むスマートデバイスの市場は極めてホットな状況が続いている。

スマートフォンは、従来の携帯電話と同じようにユーザが常に携帯し、場所に制約されることなくネットワークを利用する。従来の携帯電話では音声とメールの利用が中心で、キャリアや第三者が提供するサービスを小さい画面で受動的に利用する形にとどまっていた。一方、スマートフォンは有償無償の多様なアプリケーションをダウンロードし、端末側で自由に利用できる。いわば利用シーンが PC に近い形となっており、ユーザに利用の自由度と広がりを大きく提供している。その結果、特に「常に繋がっていたい」ミレニアム世代のユーザにおいては、音声や文字情報、画像や動画と言ったデータをシームレスに利用し、あるいは自己を表現するといった事が当たり前のように行われている。

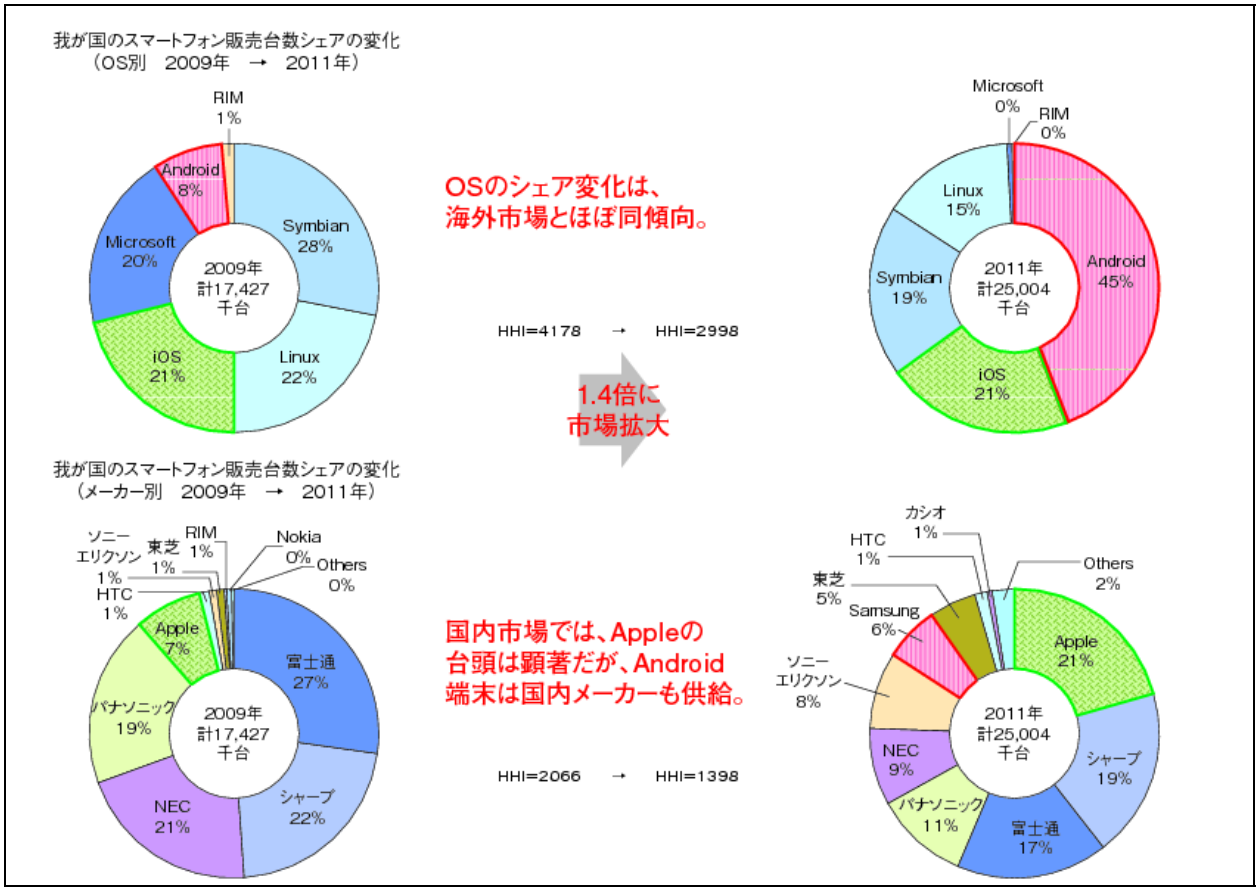
またスマートフォンの普及と同期する形で、Facebook や Twitter といった SNS や、動画投稿・共有サイトサービスが急速に広まっており、その利用端末としてもスマートデバイスの特性がうまくマッチして、普及・利用に拍車をかけていると考えられる。さらに、高解像度のカメラの搭載や、高精細の画面でのゲームの利用、電子音楽プレーヤーとしても機能す

[14] http://mashable.com/2013/04/16/eric-schmidt-on-mobile/
[15] http://redmondmag.com/articles/2013/01/08/60-million-windows-8-licenses.aspx

る等、手のひらに乗る総合電子デバイスとも言えるスマートフォンは、携帯電話を超える新次元の個人情報端末としての地位を確立しつつあるように見える。

2012 年度版情報通信白書[16]（総務省）は、世界のスマートフォン販売台数予想を、2011 年：472 百万台、以降 2012:655、2013:841、2014:1012、2015:1165、2016:1303（単位:百万台）としている。年率 23%の伸びである。また国内市場の変化として図 25 を示し、Android 端末の急速な普及を指摘している。このように、特に Android を OS に採用したスマートフォンの普及が著しい。その背景には、ソースコードが無償公開されている Android の場合、端末ベンダが自由に端末機能を設計できることや、アプリケーションベンダが自由にアプリケーションを開発してビジネスを展開できるという環境があると考えられる。

図 25　我が国のスマートフォン市場におけるメーカーシェア変化（台数ベース）



(2)　スマートデバイスにおけるアプリケーションの問題点

スマートデバイス用のアプリケーションの供給は、通常、OS メーカや通信サービスを提供するキャリアが運営するサイトからのダウンロードという形をとる。有償無償のアプリケーションが提供されている。Apple の iPhone であれば App Store から、Android の場合は Google Play から、となる。これらは「正規」のサイトと呼ばれる。また、Google Play 以

[16] http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/html/nc122110.html

外に、キャリアマーケットや独自に Google Play のアプリに対するリンクを紹介するといった、いわゆる独自なマーケットが存在している。

Apple は厳密な検証手続きを行っていると言われているが、Google Play はアプリケーションベンダの自主申告を基本にしており、セキュリティ上問題のあるアプリケーションが配布される可能性を否定できない状況にある。さらに、キャリア以外の第三者のサイトに関しては何らの保証もないと考えるべきであろう。現実に端末から不正に情報を抜き取るアプリの Google Play からの配布が確認され、IPA が警告[17]を発している。

このほかに、非正規のマーケットやネット上の口コミによる拡散も行われている。スマートフォンでは、SNS による情報拡散あるいはマーケットの検索からソフトウェアを探し出し、簡単にインストールする事が可能である。この機能自体は、Google Play を利用しないという柔軟な選択をアプリの提供者及びユーザに与えるもので有効に利用されているケースも多い。そのようなアプリのインストールには「提供元不明アプリのインストール」を許可する手順を経る必要があり、それらのサイトには懇切丁寧な手順が明示してある。しかしながら、そのようにセキュリティチェックを経ないで提供されるアプリに不正な機能やマルウェアが潜んでいるリスクは、それだけ大きくなる。

(3) スマートデバイスのマルウェア脅威

このように、マルウェアは正規のアプリを装って端末に侵入するケースが多い。いったん侵入すると、脆弱性を衝いてルート権限を乗っ取り、不正な動作を行わせたり、端末内部の情報を不正に外部に送信したりといった動作をする。また情報を破壊する活動をするマルウェアも確認されている。

Apple の iOS の場合、App Store から購入した正規のアプリ以外はインストールできないよう、ロックがかかっている。ところが、他のアプリケーションを使うためにこのロックを外す行為が行われ、その方法に関する情報もネット上に流通している。Jail Break と言われるこの行為を行うと、不正規のアプリも容易にインストール可能になり、マルウェアの侵入を許す危険が大きくなる。

スマートデバイスに感染するマルウェアの動きは、基本的にパソコンに感染するマルウェアと同じである。2011 年 1 月の段階で既に、IPA からは警告が出されて[18]いる。それによれば、トロイの木馬、スパイウェア、ボットが確認されている。勝手に SMS を送信したり、電話をかけたりするウイルスもいる。また情報を勝手に持ち出すウイルスも確認されている。スマートフォンの場合、電話帳や位置情報等、パソコンにはない要保護情報が勝手に第三者の手に渡るリスクがあり、より深刻とも言える。ボットに感染すれば、被害だけでなく、加害者になるリスクも負うことになる。

(4) スマートデバイスに固有の不正アプリの脅威

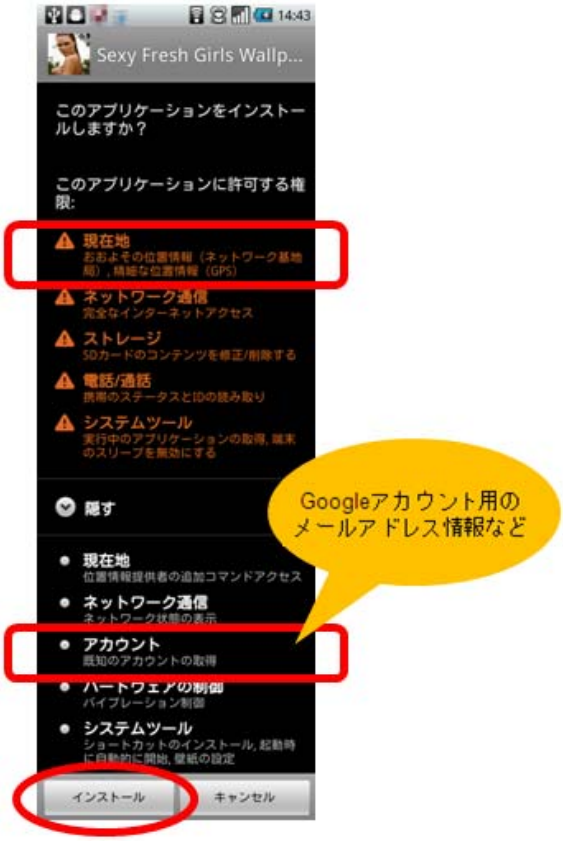
スマートデバイスに特有の現象で、ユーザの承認を得た形をとることで、スマートフォン

[17] http://www.ipa.go.jp/security/txt/2012/05outline.html#5
[18] http://www.ipa.go.jp/security/topics/alert20110121.html

内部の情報を勝手に外部に送信するアプリがある。その機能は不正なものだが、巧妙に仕組まれたインターフェイスにより、形式的にはユーザの承認を得て行っていることになるので、一層の注意が必要である。

図 26　不正アプリのインストール画面例

その手口とは、インストール時に画面上でいくつかの許可を求めてくるというものである。例えば IPA が発表している 2013 年 3 月の注意喚起[19]では、Google Play からダウンロードしたアプリのインストール時に、「このアプリケーションに許可する権限」として①現在地　②ネットワーク通信　③ストレージ　④電話/通話　⑤システムツールを要求してくる。（図 26）これを受け入れなければインストールは開始されないが、受け入れてインストールしても、目指すアプリは起動しない。その代わりに、その端末の位置情報や電話帳の情報、場合によっては SD カードに格納されている秘密情報等を「ネットワーク通信」を使って外部に勝手に送信してしまう。



そして、この機能が問題となった”The Movie”事件では、開発企業の経営者はいったん逮捕されたが、処分保留で釈放されている。理由は、アプリケーションがインストール時に目立たない形ながらユーザの同意を得る手続きを踏んでいたためと推測されている。しかし、逮捕の報道とともになりを潜めていた類似のアプリが、釈放の報道と同時に多数マーケットに復帰したという観測情報もあり、情報詐取を狙ったアプリがはびこっているのは明らかである。

これは明確に悪意を持って情報を盗み出すケースだが、単純にビジネス目的で情報を吸い上げる機能を持つアプリケーションも存在する。例えば、ロケーション情報を利用してユーザに利用確度の高いクーポンを配布する事や、適切なナビゲーションを行う等ユーザの利便性に対して貢献するサービス等を合法的な形で展開する事ができる。このようにマーケティング目的で端末内の情報や位置情報を吸い上げるアプリは珍しくない。

しかも、そのような機能は、自ら開発することも可能だが、市販の機能モジュールを埋め込むだけで実現できる。特に「情報収集モジュール」という場合には後者を指し、バイナリの形で、あるいはソースコードそのものの形で提供される。情報収集モジュールの多くは広告の表示等を行うモジュールで、利用者情報を利用して広告を表示し、ユーザが広告をクリ

[19] http://www.ipa.go.jp/security/txt/2013/03outline.html#5

ックした際にアプリ提供者に対して対価を支払う仕組みとなっている。この事自体は、何ら悪い事ではなく、ユーザに対しても有用な情報や無償のアプリケーションを提供できる等有用な場合も多い。

しかし、端末情報をアプリ提供者でなくモジュール開発者が暗黙裡に収集し、転売その他の別目的のために利用するケースが確認されている。こうなると完全にスパイ行為であり、情報詐取に当る。問題は、アプリ提供者が、外部調達して組み込んだモジュールのそのような機能を把握していない場合が多い事である。その結果アプリ提供者は、利用者情報の流出について、何らかの責任を負う事になる等のリスクを背負い込むことになる。

このように情報収集型不正アプリをめぐっては、利用者、ベンダともに複雑なリスクを抱えている現状がある。ユーザは必要外のアクセス・権限を要求するアプリのインストールには慎重を期すべきである。

(5) 2013 年度のスマートデバイスのセキュリティ状況展望

スマートフォンの普及は、LTE 等アクセス回線の高速化と端末の高性能化・多様化・低価格化等により、ますます進むと考えられる。これに合わせてアプリケーションも数多く提供され続けるであろう。昨今は、タブレット端末をビジネスで活用する動きが広がって[20]おり、その動きは加速するものと考えられる。

これに伴い、マルウェアや不正アプリもより多く現れるものと考えられる。スマートフォンは生活に密着するデバイスであることから、蓄積されるデータは個人情報の宝庫と言え、これらの情報を入手するための攻撃が今後も増加する事は想像に難くない。

不正な要素を含まない形でも、ユーザに関する情報の集積は進み、そのビッグデータの活用が次のビジネステーマとして広がるものと見られている。効率的なマーケティングのためには、データの収集と分析は必要不可欠である。この問題に関しては総務省「スマートフォン・クラウドセキュリティ研究会」（座長：山口英 奈良先端科学技術大学院大学教授）報告書[21]でも取り上げられ、また 2013 年 3 月にはフォローアップ報告[22]もされている。

また、同研究会の報告を受ける形で、2012 年 10 月には「スマートフォンの利用者情報等に関する連絡協議会 （SPSC）[23]」が発足している。さらに、日本スマートフォンセキュリティ協会（JSSEC）でも技術部会内に「スマートフォン アプリケーション プライバシーポリシー検討グループ」及び「情報収集モジュール調査グループ」が設置され活動を開始する予定である。

このように、スマートデバイスの利活用によるビジネスチャンスやアプリケーションビジネスの展開が進むことに期待が集まる一方で、その情報セキュリティリスクも多様化・複雑

---

[20] 例として生保外務員の端末、フライトアテンダントのマニュアルをタブレットに取り込み、クレジット決済機能をスマートフォンと簡易読み取り装置で実現、等がある。
[21] http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000020.html
[22] http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000043.html
[23] http://jssec.org/spsc/

化する様相を見せている。ユーザはセキュリティに関する情報に関心を持ち、アプリケーションの取捨選択やインストールには細心の注意を払って、安全にスマートデバイスを活用することが必要である。また、不正アプリ等の跋扈を防ぐための官民の協力体制の充実も期待されるところである。

【第二部　情報セキュリティ市場調査の事業概要と結果に関する考察結果】

第４章 調査の概要

4.1. 調査対象

本調査の対象は国内情報セキュリティ市場である。「2012 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、以下の推定市場規模データを算出した。

(1) 2010 年度国内情報セキュリティ市場規模　推定実績値
(2) 2011 年度国内情報セキュリティ市場規模　推定実績値
(3) 2012 年度国内情報セキュリティ市場規模　実績見込値
(4) 2013 年度国内情報セキュリティ市場規模　予測値

なお本調査は、前回の 2010～11 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、2010 年度の市場規模の算定に当っては、前回調査結果も参考としている。

4.2. 調査方法ならびに調査に使用したデータおよび情報

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

2012 年 9 月に、JNSA 会員企業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、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、流通上の数字のダブルカウントの可能性を排除する工夫をした。

調査対象とした年度は 2010～2013 年度で、基準年度を 2011 年度とした。数字としては 2011 年度を基本として回答を求め、たの 3 年度については、実数または伸び率で回答を得る形とした。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、直近の会計年度の数字での回答も可とした。

アンケートは電子メールによる依頼・配布、電子メールによる回答とし、Excel ベースの調査票を使用した。アンケートの回収件数は 27 件（うち有効回答数 25 件）であり、回収率は約 19%であった。

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。従って本調査では、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。

(2) 各種統計資料調査

国内の事業所、産業、投資等に関する政府およびその関連機関、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

アンケート調査と平行して、事業として何らかの形で情報セキュリティに関わっていると考えられる企業については、JNSA 独自の推計調査を実施した。対象は、市場規模を推計する上で重要と考えられる企業 370 社（アンケート調査対象とした JNSA 会員企業 140 社を含む）である。調査員が個別に、有価証券報告書、Web 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。(3)項のヒアリングにより得られる情報も加味している。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。

4.3. 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点が基本となる。）

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。

4.4. 市場規模の予測値の算定方法

推計作業の対象とする年度は基準年度である 2011 年度である。2012 年度、2013 年度の市場規模推定にあたっては、2011 年度の市場規模の実績推定値を基に、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。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、売上高成長率による回答表記も可能なようにした。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。これらのデータを、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、各業態区分（6.2 章参照）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。

第５章 情報セキュリティ市場の分類および定義

情報セキュリティ市場規模算出作業の基礎となる市場の区分として、まず「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。本調査では、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んでいる。

「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。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、この取引形態は市場区分の基準とはせず、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。

なお、表 17 に示す市場分類に対する詳細な説明は、本報告書を大部にすることと、独立して、例えば JNSA の提供するソリューションガイド利用のための参照用として、等の活用を視野に入れて、別冊にまとめて別途提供することとする。

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・用語解説

以下、表 16 には、表 17、表 18 で使用する用語･略号等の説明を載せている。

表 17、表 18 には、情報セキュリティ市場調査で用いた「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。

表 16 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 1 台のコンピュータで複数の機能を提供するサーバ型コンピュータ。内部バスに複数の機能モジュールを接続して複数の機能を実現する形（いわゆるシャーシ型）を含む。ブレードサーバ形式で複数の機能サーバが並列して機能を実行し、全体として統括する OS が存在しない状態（いわゆるブレードサーバ型）は含まない。
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	Anti Virus アンチウイルス
FW	Firewall ファイアウォール
IDS	Intrusion Detection System 侵入検知システム
IPS	Intrusion Prevention/Protection System 侵入防止システム
PKI	Public Key Infrastructure 公開鍵暗号基盤

SSL	Secure Socket layer 暗号通信の一方式
URL	Unifie Resource Locator 統一資源位置指定子
VPN	Virtual Private Network 仮想私設通信網
PCI DSS	Payment Card Industry Data Security Standard　PCI データセキュリティ基準
QSA	Qualified Security Assessors 認定審査機関
ASV	Approved Scanning Vendors 認定スキャンベンダー

5.2. 情報セキュリティツールの市場分類定義表

表 17　情報セキュリティツールの市場分類

大分類	中分類	定義、説明、例示　等
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、2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	アンチウイルス・アンチワームウイルス・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だけの組み合わ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／ソフトウェア	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。 VPN機能を併設するものを含む。 アプライアンス型製品、ソフトウェア型製品の双方を含む。
	VPNアプライアンス／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）を提供する製品。SSL(Secure Socket Layer)-VPNを含む。 アプライアンス型、ソフトウェア型（サーバ=ゲートウェイ=型、クライアント型）の双方を含む。 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／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・技術に基づき解析し、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。 アプライアンス型製品、ソフトウェア型製品の双方を含む。
	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、不正侵入その他の攻撃･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、Web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等の攻撃に対して、検知、防御、抑止、警告等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）等を、ファイル等の電子データや電子メール送受信・Web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Web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。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。 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FW、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。
		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Web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。）を行うソフトウェアもしくはアプライアンス製品。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。 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。
		DLP製品・システム（情報漏えい対策製品・システム）	Data Loss/Leak/Leakage Protection/Preventionと呼ばれる製品またはシステム。 企業内システムやネットワークから外部に向かうデータの流れ（電子メールその他のネットワークトラフィック、別のストレージへの書き込み、外部記憶媒体への書き込み、印刷等）の中に特定の特徴を含むデータがある場合、その行為に対して阻止、警告、記録等の動作を行い、外部への情報・データの流出や紛失を防止する機能を提供するシステムまたは製品。
		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)製品やシステムを含む。

			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、Web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を含む。（ただし、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。）
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またはシステム。 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各機能を、個別にあるいは総合・連携して提供する。 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およびそのシステム（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およ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関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関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。 プロビジョニング製品を含む。 フェデレーション製品（異システム・異組織間のID連携、プロビジョニング連携のための製品）を含む。
		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・許可機能を提供する製品分類。 シングルサインオン(SSO)およびSSO間連携製品を含む。 但し、個人認証用およ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およびその構成要素。 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。 ディレクトリサーバ（単独で製品化されているもの）を含む。
システムセキュリティ管理製品			
	1．ネットワークトラフィックを監視・制御する装置等の状態やその発する情報を統合管理し、セキュリティについて分析し、表示・統計・警告・記録等を行う製品群。 2．ネットワークを構成する装置やサーバ等の設定やアプリケーションの脆弱性を検査し、結果を報告する製品群。 3．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	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リアルタイムで総合的に管理する機能を持つ製品およびシステム。 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

	定や動作の監視・診断・制御・記録等の機能を持つ製品群。 4. 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。 5. 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。 6. 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。		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（ITガバナンス）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。
暗号化製品			
	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。	暗号化製品	1. 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。 2. ハードディスク、USBメモリ、磁気テープ装置等に組み込まれて書き込み・読み出しの際に暗号化・復号化を自動で行う機能部分を構成する暗号化モジュール。 3. 暗号ライブラリ、暗号化モジュール等の中間製品で、製品または部品として単独で取引されるもの。 4. 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。

5.3. 情報セキュリティサービスの市場分類定義表

表 18 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、主として経営管理およびIT管理の領域において、管理のための政策、管理体系、運用体制等の構築、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	情報セキュリティポリシーおよび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。 情報セキュリティポリシーや管理・運用基準等の構築および見直しのサービスを含む。 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評価（一部では慣例的に「監査」とも呼ぶ）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」の中に位置づける。ここでは管理体制等に対する総合的診断・評価を行うサービスを主体とするサービスを対

	合の支援サービスおよび規格等の審査･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。		象とする。 情報セキュリティ監査制度（経済産業省告示に基づく）における情報セキュリティ監査サービスは「情報セキュリティ関連認証・審査・監査機関（サービス）」に分類する。
		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、PCI DSS準拠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（経済産業省告示に基づく「情報セキュリティ監査制度」における情報セキュリティ監査サービス）、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。 PCI DSS準拠認定を行うQSA(Qualified Security Assessors)を含む。ただし、ASV(Approved Scanning Vendors)は「セキュリティ運用･管理サービス」のうち「脆弱性検査サービス」に含める。
		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。 内部統制管理、事業継続管理、ITサービスマネジメント等に関連して、情報セキュリティに関わる強化・改善等を**主たる**目的として実施されるコンサルテーション等を含む。（情報セキュリティが従たるもしくは副次的目的の場合は「情報セキュリティコンサルテーション」としてはカウントしない。）
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。 ITセキュリティ製品の保守・サポート等のサービスを、メーカの製品付帯サービスの再販以外に、再販事業者やSI事業者が独自付加価値として提供する場合はこの区分で集計する。
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。 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。	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モニタリング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システム等のモニタリング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。
		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Web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。 Web、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。 ITセキュリティ製品の保守・サポート等のサービスを、メーカの製品付帯サービスの再販以外に、監視・運用支援サービス提供事業者、SI事業者等の第三者が独自の付加価値として提供する場合はこの区分で集計する。
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、情報セキュリティポリシーやルールの組織内への周知徹底、および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およびe-ラーニングサービス	情報セキュリティ教育の提供･実施サービス。 講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。 情報セキュリティ教育のためのe-ラーニングのコンテンツの開発・提供およびe-ラーニングの実施サービスを含む。 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。 情報セキュリティ製品の使用等に関して製品ベンダが行う教育のうち、製品取扱知識だけでなくネットワークセキュリティー般についての知識・技術習得を主たる目的とする教育（資格認定を伴うものを含む）サービスを含む。 システムのセキュリティを作り込む技術やセキュアプログラミング、安全なWebサイトの作り方等、セキュリティ技術の教育を主たる目的とする教育を含む。
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インシデントならびにネットワークを中心としたITシステムのセキュリティ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。

第６章 情報セキュリティ市場参入事業者の業態と産業構造

情報セキュリティのためのツール・サービスは上に見たように多岐にわたることから、それを供給する事業者も多岐にわたり、また業態についてもバリエーションが多い。本調査では、約 400 社弱を集計対象としているが、その情報セキュリティ事業におけるビジネスモデルをいくつかのパターンに類型化している。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、その概要について述べる。

6.1. 情報セキュリティ市場参入事業者の業態区分

本調査で設定している情報セキュリティ事業者の業態区分は以下の通りである。

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[24]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

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。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

[24] NI：Network Integration, ネットワーク構築

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、暗号化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に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の電機・通信メーカは、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、あるいはそれを事業の主体にした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み合わせて、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。

6.2. 業態区分と市場区分における分布

上記による業態区分と、市場分類との組合せによる、集計対象企業の分布は、表 19 に示す通りである。全体の傾向としては、製品を自ら製造・供給する「ベンダ」は特定の市場に特化する傾向が強く、流通事業者やシステムインテグレータは幅広くツール・サービスを取り扱っている。

業態別に集計対象となる事業者の数が多いのは「SI・NI 機能を有する二次･三次販売店」である。これに次ぐのが「国内のセキュリティツールメーカ」と「セキュリティサービス提供事業者」である。参入企業数はそれほど多くないが、「SI が主たる付加価値の大手システムインテグレータ」は事業規模が大きく、市場に与える影響も大きい傾向がある。

市場区分別に供給事業者の数をみると、「コンテンツセキュリティ対策製品」「セキュリティ運用・管理サービス」「情報セキュリティコンサルテーション」の供給事業者が多く、「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」「システムセキュリティ製品」がこれに次ぐ。なお、これらの順位は前回調査から若干入れ替わっている。製品やサービスのバリエーションの多い市場区分ほど参入事業者の数が多い傾向がうかがえる。

なお、ツールだけかサービスだけか両方を提供するかの区分について見ると、ツールだけでサービスは提供しない事業者が 111、サービスのみに特化する事業者が 95、両方を提供する事業者が 152 と、サービス専業がやや減り、ツール・サービスの両方を提供する業態が増加している。

表 19　国内情報セキュリティ市場推計対象企業およびその分布

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25件）	370	50	*74*	41	***82***	26	15	65	17
有効推計対象	358	48	*71*	39	***81***	26	15	64	14
情報セキュリティツール全体（X）	263	48	*64*	38	***65***	20	3	19	6
統合型アプライアンス	***68***	7	6	*14*	***21***	13	2	4	1
ネットワーク脅威対策製品	***132***	*23*	16	20	***40***	18	2	11	2
コンテンツセキュリティ対策製品	***161***	19	*38*	30	***44***	16	2	10	2
アイデンティティ・アクセス管理製品	***136***	13	*24*	22	***51***	16	3	7	0
システムセキュリティ管理製品	***130***	*23*	22	22	***33***	16	2	11	1
暗号製品	***86***	11	14	*16*	***27***	12	2	2	2
情報セキュリティサービス全体（Y）	247	11	35	18	***73***	25	15	*60*	10
情報セキュリティコンサルテーション	***147***	5	9	7	*44*	21	13	***46***	2
セキュアシステム構築サービス	***131***	6	13	8	***57***	23	5	*19*	0
セキュリティ運用・管理サービス	***157***	9	24	13	***49***	20	7	*30*	5
情報セキュリティ教育	***80***	5	3	5	*19*	12	4	***29***	3
情報セキュリティ保険	***13***	0	0	1	*2*	*2*	*2*	*2*	***4***
（参考）									
ツール専業（X∩^Y）	111	***37***	*36*	21	8	1	0	4	4
ツール・サービス兼業（X∩Y）	152	11	*28*	17	***57***	19	3	15	2
サービス専業（^X∩Y）	95	0	7	1	*16*	6	12	***45***	8
生データベースの売上高分布	100.0%	14.7%	4.5%	3.8%	18.7%	50.2%	2.4%	4.1%	1.5%

今回、新たな試みとして、各業態区分の生データベースの売上高シェアを算出した。ベンダから流通を経てエンドユーザにとどく過程での重複カウントの排除調整や、特異データ、過去の傾向線とのかい離、ヒアリング調査に基づく修正等を加味する前のもので、必ずしも市場規模として算出された数値に対応するものではないことを、くれぐれもご留意いただきたい。

そのような留保条件、制限条項はあるものの、全体の傾向としては、大手システムインテグレータが主要なプレーヤ、供給主体となっていることが推測される。これに次ぐのが、同じくインテグレーション機能の提供主体である SI・NI 機能を有する二次･三次販売店と、海外メーカまたはその日本法人である。参入企業数が 74 と比較的多い国内のセキュリティツールメーカは、金額的にはサプライヤとしての存在感はそれほど大きくないと言わざるを得ない。

第７章 情報セキュリティ市場および産業の状況と、変化をもたらす要因

7.1. マクロ経済指標と企業経営環境等に関する統計データ

(1) 世界と日本、アメリカの経済成長率

表 20 は、総理府統計局が公表している実質 GDP の成長率（暦年ベース）である。2000 年代前半から 2007 年にかけて、世界的に順調な経済成長が続いたことがわかる。日本も世界全体やアメリカよりは低いが比較的順調だった時期で、2002 年 2 月～2007 年 10 月の過去最長の景気拡大期間を経験している。

それが 2008 年 9 月のリーマンショックにより急ブレーキがかかった。日本は 2008 年-1.0%、2009 年-5.5%と極端な不調に陥り、お膝元であるアメリカ以上に悪化した。これは輸出依存度の高い経済構造が世界同時不況の波をまともにかぶったことが大きい。2010 年は世界経済、特に新興国経済の好調により日本は高い成長を達成したが、2011 年は 3 月に発生した東日本大震災により生産が停滞し、再びマイナス成長に陥っている。2012 年の数値は年度ベースだが、欧州経済の低迷もあり、経済の力強さは見られない。

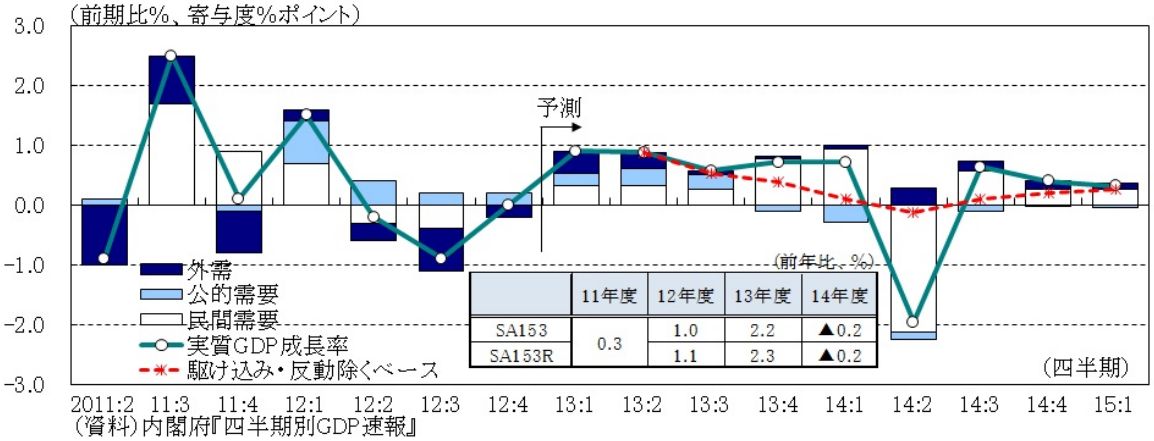
表 20 GDP 実質成長率の推移

暦年	2004	2005	2006	2007	2008	2009	2010	2011	2012*
世界	4.0	3.5	4.1	4.0	1.4	-2.1	4.0	2.7	―
日本	2.4	1.3	1.7	2.2	-1.0	-5.5	4.7	-0.6	1.1
米国	3.5	3.1	2.7	1.9	-0.4	-3.1	2.4	1.8	2.2

（出典：総理府統計局 http://www.stat.go.jp/data/sekai/pdf/2013al.pdf#page=67 より JNSA 加工）
* 2012 年は年度ベース、日本経済研究センターデータより

ただし、そのような中、2012 年 12 月の政権交代を機にアベノミクスによる経済刺激策がとられ、経済は明るい見通しを持つようになっている。起業マインドが好転することで、投資が積極化することが期待される。

図 27 日本経済の短期予測



（日本経済研究センター第 153 回改訂短期経済予測 http://www.jcer.or.jp/research/short/detail4565.html）

図 27 は日本経済研究センターが 2013 年 3 月に発表した 4 半期予測であるが、2013 年 1

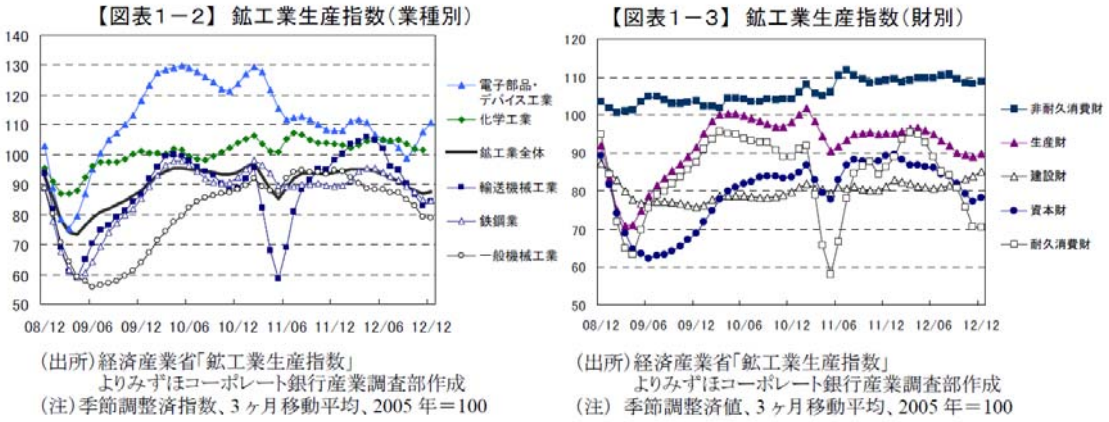
月以降、5 四半期は年率 2%程度の順調な景気拡大が続くとの予測になっている。

(2)企業の経営環境と設備投資動向

今回の調査対象期間も、前回に引き続き企業の経営環境の変動は激しかった。みずほコーポレート銀行が 2013 年に発行した「2013 年度の日本の産業動向」には日本の業種別生産指数と在庫･出荷バランスの推移がグラフで示されている（図 28)。2012 年版と合わせてみると、2008 年度前半の好調が後半に急降下し、2009 年 4 月ごろを底に回復に向かうものの、リーマンショック前まで戻せないまま 2010 年度半ばにアジア経済変調から中だるみに陥り、その後持ち直してきた矢先に東日本大震災に見舞われた。その結果、2011 年度前半は自動車を中心に大幅な生産の低下に陥っている。その後の回復も力強さはなく、2010 年前半の生産水準にも届いていない。その後 2012 年度に入ると欧州の債務危機が深刻化する中で米国経済も低迷し、輸出が低調で生産レベルも落ち込むという姿で推移している。

同レポートが指摘するように、2013 年度は回復の兆しが見え、やや明るい展望が開けつつある所であると言えよう。

図 28　企業の生産・出荷・在庫の推移



（出典：　みずほコーポレート銀行　http://www.mizuhocbk.co.jp/fin_info/industry/sangyou/pdf/1041_01.pdf）

設備投資については、同レポート 2012 年版では「2011 年度の設備投資は 2007 年度以来 4 年ぶりに前年度比増加となり、景況感の改善を受けて、リーマンショック以降控え気味であった維持・更新投資等を再開する動きが出てきている。今後は復興需要に伴う設備投資の増加や通信業による通信設備の補強等を中心に設備投資は増加すると見込む」と述べている。2012 年度については、2013 年 3 月度の日銀短観[25]によれば、「ソフトウェアを含む設備投資額（除く土地投資額)」の 2012 年度実績見込みは全産業ベースで上期+8.7%、下期+3.1%年度平均では 5.5%となっている。同調査における 2013 年度計画は上期+7.9%、下期-7.7%年間で-0.7%と、前半は好調を持続、後半は一転して縮小というデータである。が、2013 年度については全般に楽観的見方をする経済予測が多く、三菱 UFJ リサーチ&コンサルティングが

[25] http://www.boj.or.jp/statistics/tk/zenyo/2011/all1303.htm/

2013 年 3 月 11 日に発表した 2013／2014 年度経済見通し[26]では、2013 年度の設備投資見通しについて「企業業績の改善を反映して、競争力を維持するための投資や維持・更新投資等が行なわれ、景気を下支えする要因となろう。」と指摘している。

従い、情報セキュリティ投資にも影響が大きい設備投資動向は、2011～2013 年度は増加傾向にあると考えられる。

7.2. 企業・組織の IT 支出ビヘイビア

(1)IT 投資サイクル

IT 投資にはいくつかの要因に基づくサイクルがあると考えられる。情報セキュリティに対する支出や投資も、一定の部分はそのサイクルに影響を受けると考えられる。例えばネットワーク機器の更新に合わせてファイアウォールを更新するようなケースである。そこで、IT 投資サイクルが把握できれば、情報セキュリティ市場の需要変動を見る場合に参考になると考えられる。

IT 投資に影響を与えるものとしては、システムライフサイクルがあり、これは 2004, 2005 年度に IPA の委託により JUAS（社団法人日本情報システム・ユーザー協会）が調査を行ってまとめた「システム・リファレンス・マニュアル[27]」の中で言及されている。これによれば、システムの利用期間は 10～15 年が最も多いが、パッケージでは 5～10 年程度となる。

次に考えられるのは事業のライフサイクルである。IT が支える事業が新陳代謝されれば、そのための IT も変化する。特にネットビジネスではそのサイクルは極端に短く、最短 1 年のようなこともありうると考えられる。

サプライサイドからは、いわゆるムーアの法則が、IT 投資サイクルに大きな影響を与えると考えられる。ハードウェアの性能は概ね 2 年で 2 倍上がる、というものである。ハード性能が上がればソフトウェアはそれを前提とした仕様・機能を盛り込んでくるから、常に最新のアプリケーションを利用しようとすれば 2 年というサイクルが想定される。

しかし、現実に業務プロセスはそこまでの速度では変化せず、経験則的には 3～4 年がサイクルの目安と考えられる。一例では、マイクロソフトのオフィスシリーズのバージョンは、97、2000、2003、2007、2010 と概ね 3 年サイクルで上がってきている。上記数字を裏付ける事例と言える。

同様に、通信ネットワークの容量も IT 投資サイクルに影響を与えると考えられる。ネットワークの容量そのものではないが、日本での通信網上の情報流通量の統計は、総務省が発行する情報通信白書[28]に示されており、2011 年版のデータは表 21 のようになっている。数字が細かいが、2009 年度の情報流通量は 2001 年度比 198.8%となっており、10 年で倍のペースである。これは昨今のブロードバンドの広がりやネット上の動画配信等の普及、スマートデバイスの急速な浸透等を考えるとややスローな感じもする。

---

[26] http://www.murc.jp/thinktank/economy/economy_prospect/short/short_1303.pdf
[27] http://www.ipa.go.jp/about/jigyoseika/04fy-pro/chosa/srm/srm2.pdf
[28] http://www.soumu.go.jp/menu_news/s-news/01tsushin02_01000017.html

表 21　平成 23 年版 情報通信白書　情報流通量の推移

情報流通量	単位	平成13	14	15	16	17	18	19	20	21年度	平成13年度を100とした場合	期間平均伸び率
流通情報量	ビット	3.83×10^{21}	3.85×10^{21}	3.89×10^{21}	4.02×10^{21}	4.36×10^{21}	4.97×10^{21}	5.96×10^{21}	7.12×10^{21}	7.61×10^{21}	198.8	9.0%
対前年度伸び率			(0.5%)	(1.0%)	(3.5%)	(8.5%)	(13.9%)	(20.1%)	(19.5%)	(6.9%)		
消費情報量	ビット	2.63×10^{17}	2.63×10^{17}	2.68×10^{17}	2.69×10^{17}	2.68×10^{17}	2.68×10^{17}	2.75×10^{17}	2.91×10^{17}	2.87×10^{17}	109.0	1.1%
対前年度伸び率			(−0.1%)	(2.2%)	(0.4%)	(−0.4%)	(−0.1%)	(2.8%)	(5.8%)	(−1.6%)		

（出典：総務省　情報通信白書 2011）

当ワーキンググループのヒアリング調査では、通信事業者の設備更新サイクルは 3～4 年程度という発言を記録している。職場のパソコンのリース期間は概ね 3～5 年と考えられ、税法上の償却期間等からも、概ねこの 3～5 年を IT 投資サイクル、したがって情報セキュリティ関連の需要にも影響を及ぼすサイクルと考えてよいと思われる。

なお、前回の投資ピークは 2007 年ごろだったという証言もあり、これが事実とすれば、2011 年度から 2012 年度に次の山が現れる可能性もある。

(2) IT 投資全体市場との比較（JEITA 統計に対する比率）

本調査では、例年、一般社団法人電子情報技術産業協会（JEITA）[29]統計による IT 投資（JEITA 参加企業の出荷額ベース）との比較を行ってきた。JEITA 統計並びに一般社団法人情報通信ネットワーク産業協会（CIAJ）[30]統計を加味し、本調査結果と比較したデータを表 22 に示す。

表 22　IT 市場、通信市場と情報セキュリティ市場規模の比較

セキュリティとITの出荷額比較	2010年度	2011年度	2011/2010
	億円	億円	%
セキュリティ出荷計	6,643	6,926	104.3%
IT出荷計(JEITA)	63,249	62,183	98.3%
PC出荷	9,206	8,669	94.2%
MF, WS, Svr 出荷計	4,054	3,762	92.8%
ソフトウェア	7,413	7,353	99.2%
SI開発	23,119	23,092	99.9%
BPOその他サービス	19,457	19,307	99.2%
（SW,サービス計）	49,989	49,752	99.5%
ネットワーク機器			
生産	4,930	5,176	105.0%
輸入	4,596	5,230	113.8%
輸出	1,633	1,527	93.5%
国内出荷	7,892	8,879	112.5%
IT+NW装置	71,141	71,062	99.9%
セキュリティ市場の比率			
対IT出荷計(JEITA)	10.5%	11.1%	0.0%
対IT+NW装置	9.3%	9.7%	0.0%

29　一般社団法人電子情報技術産業協会　http://home.jeita.or.jp/

30　一般社団法人情報通信ネットワーク産業協会　www.ciaj.or.jp/

（出典：JEITA、CIAJ の統計を元に JNSA 作成）

JEITA では、「年度パーソナルコンピュータ国内出荷実績[31]」「わが国におけるサーバ・ワークステーションの出荷実績[32]」「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[33]」の 3 種類の統計を公表している。表 22 では、「IT 出荷計（JEITA）」の欄で、各々「PC 出荷」「MF, WS, Svr 出荷計」「ソフトウェア、SI 開発、BPO その他サービス」にその数字を示している。また、情報セキュリティ投資に対応する IT 投資にはネットワーク機器も含まれることから、CIAJ 統計に基づきその国内出荷額も比較対象として掲出した。

表 22 に見られるように、2011 年度の IT 出荷は前年度比微減となった。一方ネットワーク機器は 12.5%増と高い伸びを見せた。コンピュータハードウェアは単価の下落により金額ベースではプラスになることが難しくなっている。例えば PC 出荷は 5.8%のマイナスだが台数ベースでは 8%増加している。またネットワーク機器の増加はスマートデバイスや SNS の普及等ネットワークトラフィックを増大させる社会要素が増えていることに対応した能力増強によるものと考えられる。

これらの増加要因はセキュリティへの支出を押し上げる方向に働く可能性が強い。本調査結果では、2011 年度は前年度比 4.3%の増加となった。IT+NW 装置の合計市場規模に対するセキュリティ出荷額の比率は、2010 年度で 9.3%、2011 年度で 9.7%となった。前回調査では 2008 年度：8.9%、2009 年度：9.5%であったので、この比率は徐々に上がってきているものとみられる。

(3)総務省「情報通信白書」における情報通信産業の市場規模との比較

総務省は毎年情報通信白書を発行している。その 2012 年度版[34]には、情報通信産業の国内生産額が国民経済統計ベースで示されている。（図 29）ここには通信、放送だけでなく、そのための設備の製造業や建設業、情報サービス業（ソフトウェアや SI の提供事業等）、コンテンツの制作や情報通信関連サービスまで、情報と通信に関する業種が網羅されている。

その生産額の合計は、ピーク時には 100 兆円近い額があったが、主として通信業と通信関連製造業の金額が縮小することによって漸減し、2010 年度には 85 兆 3,530 億円となっている。特にリーマンショック後の 2009、2010 年度の通信関連製造業の落ち込みが大きいことがグラフから読み取れる。

また直近のピークは 2007 年度であるが、この年の前後に通信関連設備投資が盛り上がったことが前回調査で確認されており、このグラフからもそれが裏付けられることがわかる。本調査（前回調査を含む）では、セキュリティ産業の出荷額も 2007 年度に直近のピークがあり、リーマンショック後の 2009、2010 年度が低迷したとの結果になっている。図 28 のグラフが

31 「2009 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/2009/

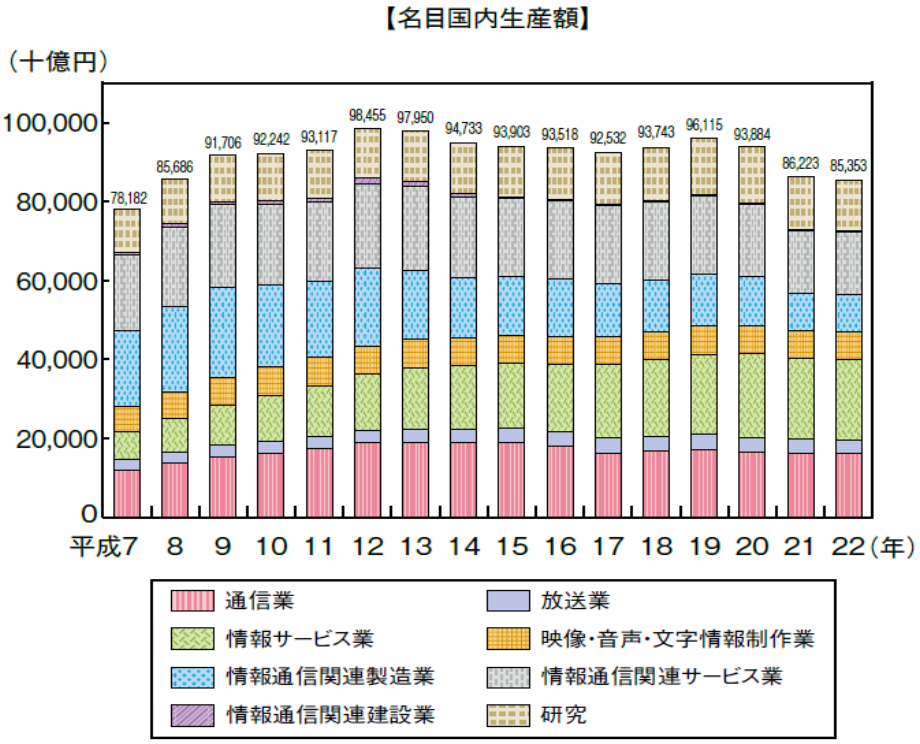
32 「わが国におけるサーバ・ワークステーションの平成 21 年度（平成 21 年 4 月～平成 221 年 3 月）出荷実績」 http://home.jeita.or.jp/is/statistics/server/h21/index.html

33 社団法人電子情報技術産業協会「2009 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 22 年 6 月 17 日
http://home.jeita.or.jp/is/statistics/soft_sol/2009/index.html

34 http://www.soumu.go.jp/johotsusintokei/whitepaper/h24.html

示すすう勢とよく一致していると言える。

図 29　情報通信産業の名目国内生産額



(4)経済産業省「情報処理実態調査」に見られる支出・投資動向

経済産業省は毎年情報処理実態調査を実施しその結果を公表している。発表までのリードタイムが長いので、現在公表されている最新の調査は 2011 年版[35]であり、対象年度は 2010 年度である。しかし、情報セキュリティの状況について直接 IT ユーザに調査したものとして参考になる。

◆ 情報セキュリティ対策の全般状況

情報セキュリティに関する全体状況としては、情報処理実態調査では以下のようにまとめている。

- 平成１５年度以降低下傾向にあった情報セキュリティトラブル発生率は、平成１８年度以降横ばいで推移している。
- 東日本大震災等の影響により、外部要因によるシステム停止が急増している。
- コンピュータウィルスの感染経路や重要情報漏えいの原因等をみると、USB 経由のウイルス感染や携帯情報端末の盗難・紛失等、モバイル端末利用等に伴う情報セキュリティトラブルの発生が目立っている。
- 情報処理関係支出の抑制が続くなか、一社平均の情報セキュリティ対策費用は増加しており、情報セキュリティ対策費用を維持する企業が多い。

[35] http://www.meti.go.jp/statistics/zyo/zyouhou/result-1.html

情報処理関係支出は抑制傾向にある中で、情報セキュリティ対策費用が増加傾向にあるとの指摘は興味深い。

◆ 情報セキュリティ対策費用の状況

同調査では、情報セキュリティ対策費用について、金額幅による選択肢で回答を求めており、そこから見做しで 1 社平均の対策費用を算出している。その値を過去 3 回の調査報告書から拾ってまとめたものが表 23 である。

この期間はリーマンショック、それによる経済停滞、そこからの回復の期間に当る。2010 年度は経済指標は好転したが、売上高の回復には至らず、費用面も総じて厳しい抑制が継続していた時期である。情報処理関係支出の抑制が継続していることが確認できる。そのような中上記に引用したように、わずかずつではあるが 1 社当りの情報セキュリティ対策費用は増加傾向を見せている。

また、情報処理関係支出に占める割合もこの 3 年間は 1.4%前後で安定してきている。2006 年度 1.04%、2007 年度 0.95%[36]と数字も低く、変動も大きかったのに比べて、進化が見られるということもできそうである。

表 23　情報処理実態調査母集団の比較（平成 20、21、22 年度調査）

対象年度	回答企業数	1社当り					
		資本金規模	年間事業収入規模	情報処理関係支出	年間事業収入比	情報セキュリティ対策費用	対情報処理関係支出比率
	（社）	（百万円）	（億円）	（百万円）	（%）	（万円）	（%）
2008年度	5,021	9,509	643	736	1.14%	1,030	1.40%
2009年度	4,651	9,417	614	756	1.23%	1,050	1.39%
2010年度	4,537	9,300	633	748	1.18%	1,070	1.43%

（出典：経済産業省平成 20, 21,22 年度情報処理実態調査より JNSA 作成）

なお、上の表にある 1 社平均 1,070 万円という情報セキュリティ対策費用に回答企業数 4,537 を掛けると 4,855 億円となる。同調査の回答率は 50.9%となっており、調査対象企業全体では約 9,500 億円という試算値が得られる。本調査における 2010 年度の市場規模算定値 6,643 億円であり、日本全体として情報セキュリティ対策に数千億円が費やされているという規模感は一致すると言える。

(5)社団法人日本情報システム・ユーザー協会「IT 動向調査」に見られる情報セキュリティ対策

社団法人日本情報システム・ユーザー協会（JUAS）は 1994 年以来継続的に IT 動向調査を行っている。2012 年度調査結果の概要は 2013 年 3 月 29 日に公表[37]された。

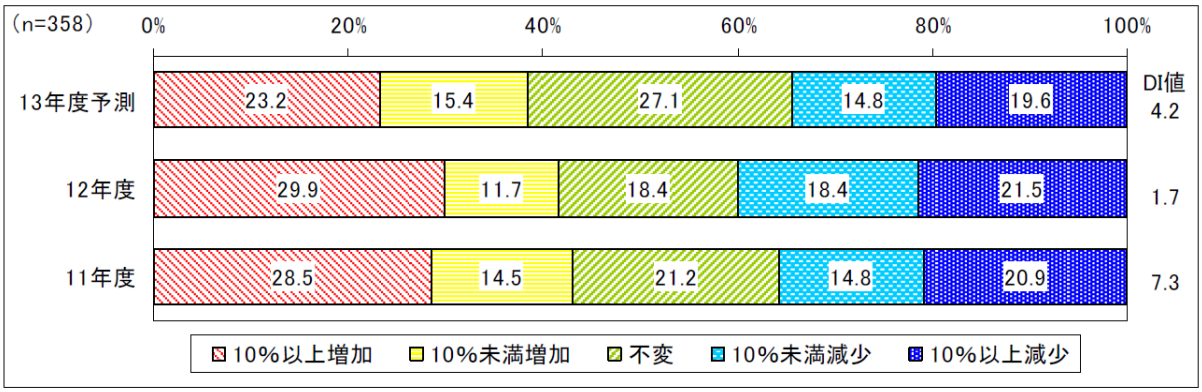
IT 支出の増減傾向を聞く定例の質問に対しては、図 30 のような回答分布となっている。10%以上の増減を 2 倍して増加のスコアから減少のスコアを差し引いたインデックス値を見

[36] いずれも前回調査報告書参照

[37] http://www.juas.or.jp/servey/it13/index.html#pr5

ると、2011 年度 14.9、2012 年度 20.2、2013 年度（予測）7.8 となり、増加傾向は続いているものの 2012 年度が最も積極的であり、2013 年度はそのペースは鈍ると見られる。（なお、アンケート調査時点は 2012 年 11 月）

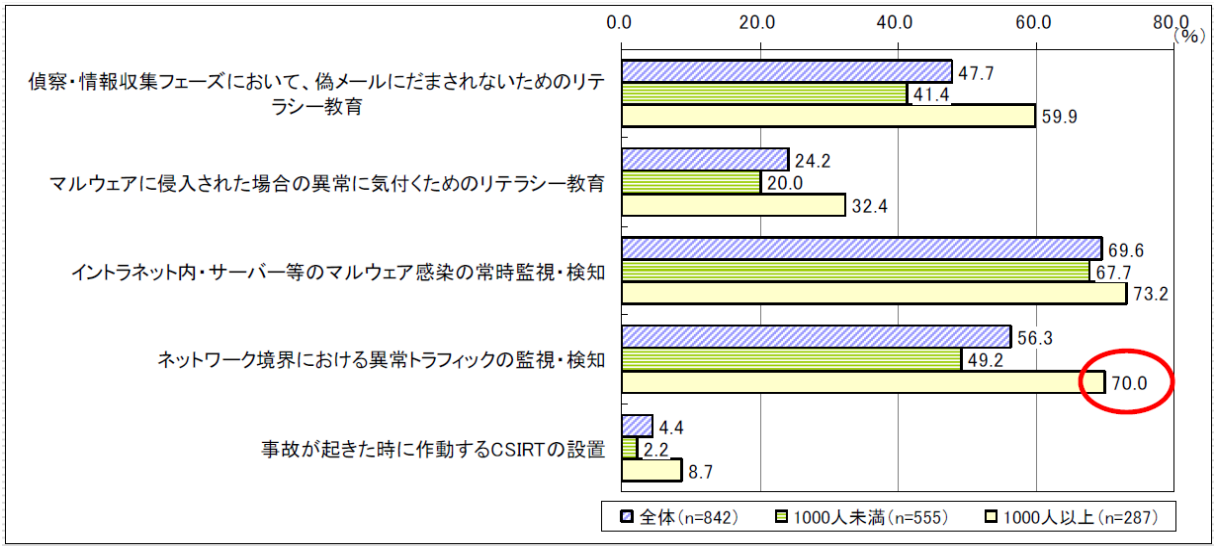
図 30　IT 予算の増減の回答状況



（出典：JUAS　企業 IT 動向調査 2013 報告プレスリリースより）

セキュリティ対策についてはトピック的要素の 2 点について概要報告がされている。標的型サイバー攻撃を受けたと認知している企業の割合が、従業員 1000 人以上で 19.1%、同 1000 人未満で 6.1%、全体で 10.2%という結果になったとして、大企業の方が攻撃対象となる可能性が高いことを指摘している。なお、対策としては図 31 に見られるように、重層的な対策が積極的に取られていることが確認された。

図 31　標的型サイバー攻撃対策の実施状況



（出典：JUAS　企業 IT 動向調査 2013 報告プレスリリースより）

もう 1 点のトピックは情報セキュリティ対策の自己評価の中で「対策ができておらずかなり不安」とした選択肢に、「ソーシャルメディアポリシーの作成（私的利用）」が 61.1%、「同（企

業利用)」が 57.5%と非常に高率の回答があった。これに続くのが「データの暗号化等の保護策」で 30.3%に上っている。情報の流出・漏えいに対する対策への不安が感じられる。特にソーシャルメディアを通じての情報漏えいについては、ルール化や歯止めのかけ方の難しさが強く意識されているものとみられる。

7.3. 情報セキュリティに関わる外部環境変化

この点については、前回調査報告書で詳述した。指摘すべき項目は基本的に同じなので、以下項目のみを列記する。ただし(3)については 2012 年度に起きた変化を簡単に記した。詳細は前回報告書を参照されたい。ただし、各項目とも、状況は改善されたとは言えず、むしろ脅威は高まっていると認識する必要がある。

(1)ネットワーク脅威の状況とその変化（IPA 公表を中心に）

① マルウェア感染経路の多様化と深刻化
② 標的型攻撃の多発
③ Advanced Persistent Threat（新しいタイプの攻撃）
④ ソーシャルメディアを利用する攻撃
⑤ スマートデバイスへのマルウェアの拡散

(2) 情報漏えい事件の深刻化

(3) 法制度等の強化

2011 年度には刑法改正が行われ、いわゆるウイルス作成罪が明示的に規定された。マルウェア等によるコンピュータやデータの破壊等は物理的被害を伴わないことから罪名の適用が困難で捜査・摘発が困難であったが「不正指令電磁的記録に関する罪」とすることで直接罰することができるようになった。関連して刑事訴訟法も改正され、電磁的記録・証拠の収集方法に関する制約を緩和する措置が取られた。

2012 年には不正アクセス禁止法が改正された。改正により、いわゆるフィッシング詐欺等で ID やパスワードを盗み出す行為そのものが処罰の対象となった。また、不正に入手した ID・パスワードの保管や他者への譲渡も明示的に処罰対象となった。

7.4. 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みと、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。

情報セキュリティの経営課題としての重要性に対する認識は、2011 年の一連のサイバー被害の事例や、スマートデバイスの業務活用の必要と、マルウェア等による情報流出の危険への認識等から、着実に高まってきていると見られる。その結果、IT 支出を抑制する中で情報セキュリティ対策費用の支出は拡大する等、対策に対する姿勢も積極化している。

また、政策対応の面でも、対策を担う情報セキュリティ人材の不足が重要課題として意識され、自由民主党が提起した、情報セキュリティ分野での 20 万人の雇用創出等、政府もより積極的な

対策に乗り出す動きを見せている。

日本企業のグローバル化が進み、世界のあらゆる場所で生産と販売に取り組むようになってきた。そこでの競争力の源泉、日本企業の付加価値は設計・技術情報であり、制度の固い加工や品質を作り込む生産管理のノウハウである。このような無形資産を守ることは日本を守ることそのものである。世界に開きつつ価値を守るためには情報セキュリティ対策は欠かせない。世界に展開する先で日本と同等以上の対策ができるようにならなければならない。

そのためには、セキュリティ対策を実施する主体の体系的な取り組みが第一に必要であるが、それを支え実現するため製品やサービスの提供、そしてそれらのメンテナンスやアップデートを支える情報セキュリティ産業・企業の役割も飛躍的に高まっている。

世界に通用する国産技術を持つベンチャーもわずかながら存在するが、国産情報セキュリティ企業はまだまだ弱小でひ弱である。その強化育成も課題となる。公的研究開発支援、社会全体としての情報セキュリティ人材育成、産業資金の供給等、産業振興のための条件の整備が急がれるところである。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。

一方、情報セキュリティ産業としては、そのような支援に呼応して、技術開発や製品・サービスの一層の充実、そして海外市場も含めた市場開拓に向けて自助努力を強める必要がある。中小企業まで浸透しつつある情報セキュリティ対策は、それを支えるためにより多くの企業と人材を必要としている。それに応え得るサプライサイドの充実と成長・発展モデルの開発が必要なのではないだろうか。

おわりに

IT のフロンティアは、スマートフォン、タブレット PC、ソーシャルメディア等個人の情報生活の革新を促す技術から、クラウドコンピューティングのような情報処理のパラダイムを転換する可能性のある技術・サービス、更にはスマートグリッドやスマートシティといった社会枠組みの進化をもたらす活用スキームまで、イノベーションを進めている。

このことは、情報セキュリティのフロンティアをも拡張し、複雑さと重要度を飛躍的に高めている。

2011 年には、日本の情報セキュリティについて考えさせられる、極めて多くのことが立て続けに起こった。東日本大震災、みずほ銀行のシステムトラブル、ソニーグループにおける国際的広がりと影響を伴う 1 億人規模の個人情報の流出、防衛産業に対するサイバー攻撃、国の機関に対する執拗なサイバー攻撃と感染被害等があった。急速に普及するスマートデバイスも、マルウェア攻撃にさらされている。

2012 年にも、これらサイバーリスクの脅威は全く衰えを見せていない。ハクティビストの活動も強まり、またサイバーウォーと呼ばれる国家間のサイバー破壊活動や、国が背後にいる指摘されるサイバー攻撃・産業スパイ等、複雑化・深刻化が進んでいる。身近なところでは遠隔操作マルウェアによる誤認逮捕という衝撃的事件も発生して、一般市民にもサイバーリスクの深刻さを認識させた。

情報セキュリティ対策は、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、事業継続管理等を統括するコーポレートリスクマネジメントの主要要素となることで、企業価値を守り支え高める積極的役割へと、その価値を大きく変化させた。IT セキュリティ、情報セキュリティは社会システムの安全・安定・安心の中核をなす要素と化していると言っても過言ではない。

情報セキュリティ産業はそのための貢献という役割を担っている。すなわち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。そしてその結果として、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。

本報告書は、情報セキュリティ市場規模のデータを提供し、若干の解説、分析を加えることで、日本の情報セキュリティ産業の現況を表している。政策を進める立場、対策を進める立場、ソリューションを提供する立場、産業を育成し投資する立場等、関連する各主体の活動・取組みに際し、参考となれば幸いである。

以上

修正・改訂履歴

時期・版	対象箇所	修正・改訂内容
.2013 年 5 月 31 日 V1.0	－	初版発行

情報セキュリティ市場調査報告書

2013 年 5 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

調査研究部会　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・編集参加者）

菅野　泰彦　　アルプスシステムインテグレーション株式会社
清水　聡史　　株式会社イーセクター
浜　　義晃　　株式会社イーセクター
兵藤　直嗣　　株式会社イーセクター
土屋　日路親　イーロックジャパン株式会社
福岡　かよ子　株式会社インテック
木城　武康　　株式会社日立システムズ
熊谷　裕吾　　三井物産セキュアディレクション株式会社
塩見　友規　　三井物産セキュアディレクション株式会社
蜂巣　悌史　　株式会社 km2y

以上