2013 年度

情報セキュリティ市場調査報告書

V1.0

２０１４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。2013 年度調査は、従来方式を一部簡略化し、個別推計調査、インタビュー調査、ワーキンググループメンバによる議論を踏まえて全体集計・推計作業を行い、2014 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、急速に広まってきている。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 年度には遠隔操作マルウェアによる脅迫に関する誤認逮捕事件が起きて一般大衆の関心も呼び、テレビ放送でもしばしば取り上げられるなど、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。2013 年 3 月には韓国に大規模なサイバー攻撃が仕掛けられ、国家安全保障にも関わる課題となっていることが実感された。

このような状況を踏まえ、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、防衛省は 2013 年度 141 億円、2014 年度 205 億円と多額の予算 [1]をサイバー防衛体制整備に割り当てるところまで取組みが積極化してきた。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。更には米国 NSA 元職員による、米国のネット上の諜報活動の実態に関する暴露に端を発した、インターネット自体の信頼への疑問という根本問題も関心を呼んでいる。水飲み場攻撃やリスト攻撃によるネットバンキングへのハッキング被害も深刻化しており、ネットワークセキュリティは国際的な社会問題にまでなっていると言える。

このような現状からの脱却を図るためには、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。そして次に、企業経営のデータや営業秘密、知的財産等の情報資源の安全が確保されなければならない。そのためには企業が持つ情報資産の保護・活用を推進し、企業の内部統制を充実してアカウンタビリティを高める必要がある。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、意図せざる誤用やミスを防

[1] http://www.nisc.go.jp/conference/seisaku/ituse/dai2/pdf/siryou0200.pdf

ぎ、悪意を持った情報の窃取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。セキュリティ脅威の深刻化は、対策に際して専用のツールと専門家の知識・ノウハウ・サービス体系を不可欠のものとしている。情報セキュリティ産業の健全な発展と、その力の正しい活用がなくては、経済社会が安全にインターネットを活用して活動を維持・推進することができない状況にまで至っていると言っても過言ではない。

この調査は、その情報セキュリティ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、政策課題に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。それはまた、経済社会の健全な発展に不可欠なものと言える。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	2011年度（推定実績）		2012年度（推定実績）			2013年度（実績見込）			2014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	**694,036**	**100.0%**	**731,364**	**100.0%**	**5.4%**	**766,124**	**100.0%**	**4.8%**	**797,827**	**100.0%**	**4.1%**
情報セキュリティツール合計	**365,562**	**52.7%** **100.0%**	**384,907**	**52.6%** **100.0%**	**5.3%**	**405,460**	**52.9%** **100.0%**	**5.3%**	**424,829**	**53.2%** **100.0%**	**4.8%**
統合型アプライアンス	19,229	5.3%	20,120	5.2%	4.6%	21,141	5.2%	5.1%	22,203	5.2%	5.0%
ネットワーク脅威対策製品	49,924	13.7%	52,112	13.5%	4.4%	54,122	13.3%	3.9%	56,061	13.2%	3.6%
コンテンツセキュリティ対策製品	139,299	38.1%	147,028	38.2%	5.5%	154,964	38.2%	5.4%	162,176	38.2%	4.7%
アイデンティティ・アクセス管理製品	65,523	17.9%	68,846	17.9%	5.1%	71,791	17.7%	4.3%	74,534	17.5%	3.8%
システムセキュリティ管理製品	51,747	14.2%	55,108	14.3%	6.5%	58,869	14.5%	6.8%	62,620	14.7%	6.4%
暗号化製品	39,838	10.9%	41,693	10.8%	4.7%	44,572	11.0%	6.9%	47,235	11.1%	6.0%
情報セキュリティサービス合計	**328,475**	**47.3%** **100.0%**	**346,457**	**47.4%** **100.0%**	**5.5%**	**360,664**	**47.1%** **100.0%**	**4.1%**	**372,998**	**46.8%** **100.0%**	**3.4%**
情報セキュリティコンサルテーション	67,958	20.7%	70,165	20.3%	3.2%	72,249	20.0%	3.0%	74,250	19.9%	2.8%
セキュアシステム構築サービス	129,395	39.4%	138,889	40.1%	7.3%	144,481	40.1%	4.0%	148,289	39.8%	2.6%
セキュリティ運用・管理サービス	98,417	30.0%	103,189	29.8%	4.8%	108,747	30.2%	5.4%	114,397	30.7%	5.2%
情報セキュリティ教育	25,237	7.7%	26,574	7.7%	5.3%	27,387	7.6%	3.1%	28,132	7.5%	2.7%
情報セキュリティ保険	7,468	2.3%	7,640	2.2%	2.3%	7,799	2.2%	2.1%	7,930	2.1%	1.7%

今回調査の基準年度である 2012 年度は、日本経済が回復の兆しを示す中で、前年度から引き続き、情報セキュリティに対する脅威を実感させる事件事故が相次ぎ、セキュリティ対策に対する社会的認知が一層進んだ年と位置付けることができる。

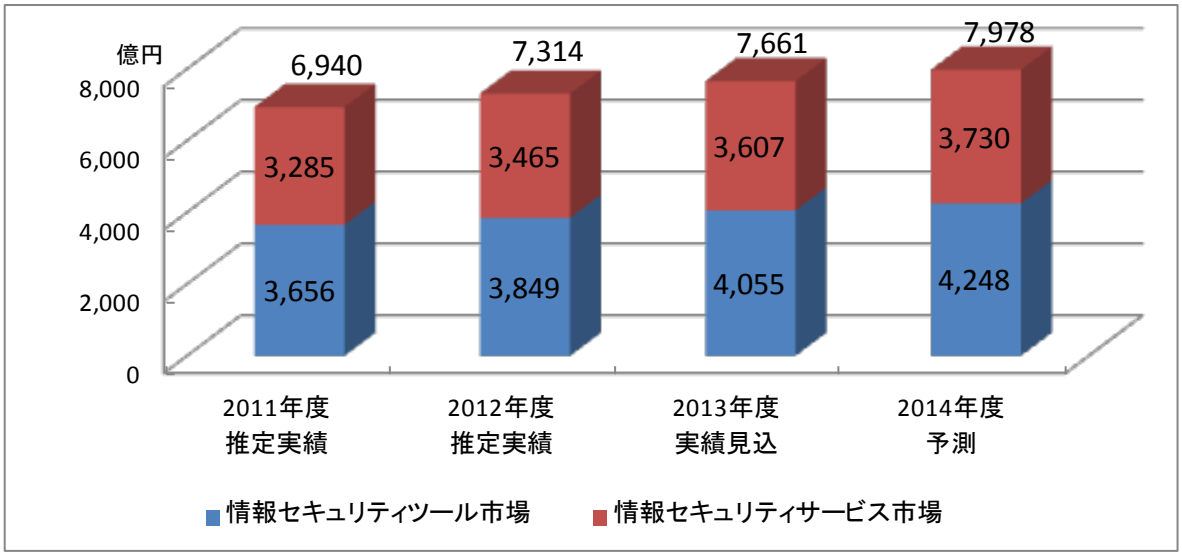
その前年の 2011 年度は、年度開始直前に発生した東日本大震災と原発事故の影響による社会的混乱と経済停滞の中で幕を開け、秋にはタイの大洪水による日系企業の被害など、経済環境の厳しい１年であった。また４月にはソニーグループが世界的ハッキング攻撃に遭い、約１億人の顧客個人情報の流出被害が発生、9 月には防衛産業各社における標的型攻撃にる技術情報等流出被害や、参議院・衆議院での不正侵入による情報盗難が明らかになるなど、サイバー攻撃による

大規模もしくは深刻な被害が相次いだ。このような中、情報セキュリティへの支出は前年度までの抑制基調から拡大に転じたと推測される。その結果、情報セキュリティ市場はツール市場が3,656億円、サービス市場が3,285億円、合計6,940億円に回復したものと推定する。

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、エコカー減税等の政策と急速に国際化を進める日本企業の努力に支えられて実質0.7%、名目マイナス0.2%程度の成長率を確保した。また2012年12月以降アベノミクス効果により円安・株高が進み、経済状況には明るさが兆した。更に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。

このような状況を背景に、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、成長度合いを高め、5.4%拡大して、情報セキュリティツール市場が3,849億円(前年度比成長率5.3%)、情報セキュリティサービス市場が3,465億円(同5.5%)、合計7,314億円となった。本調査の過去のデータと照らすと、2008年度のピークを更新して初めて7,300億円台に到達したものと考えられる。

図 1　国内情報セキュリティ市場規模の推移



2013年度は、アベノミクスと日銀による大胆な金融緩和によって、経済マインドは大幅に好転した。一方でアベノミクス第三の矢である成長戦略の具体化やTPP交渉のもたつき、欧州経済の不安定、中国・韓国との関係悪化等、制約要因も多く見られる。そのような中、年度の経済成長率は概ね実質2%程度と、近年の中では高い成長率を達成できた模様で、デフレも徐々に解消に向かっているようである。

情報セキュリティに関する状況は、米国で発覚したPRISM問題[2]が影を指す中、韓国や米国では大規模な情報漏えい事件が後を絶たず、日本においても水飲み場攻撃やリスト攻撃による情報窃取と、それを悪用した不正預金引き出し等、実被害を伴う犯罪が深刻化している。サイバー犯

[2] 米国NSA(国家安全保障局)がインターネットを広範に監視・盗聴していることが元従業者の暴露により明らかになった事件

罪ではないが、東芝関連企業の元従業員による技術情報の盗み出しと韓国のライバル企業への提供といった情報犯罪も明るみに出ており、情報セキュリティへの関心はかつてないほど高まっている。

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、市場の拡大基調は維持されていると考えられ、概ね 2012 年度並みの成長率を維持したものと推測される。市場規模は情報セキュリティツール市場が 4,055 億円（同 5.3%）と初めて 4,000 億円規模に達し、情報セキュリティサービス市場が 3,607 億円（同 4.1%）と過去最高を更新したものと見られる。その結果、情報セキュリティ市場合計では 7,661 億円（同 4.8%）と、過去最大規模となった。

2014 年度は、経済成長は円安を背景とした生産活動の国内回帰の動きなどのプラス面もあるものの、燃料輸入の急増による国際収支の赤字基調の定着、消費税増税の影響（一時的との見方が支配的だが）、アジアその他の新興経済の停滞、ウクライナ情勢など、不確定要因も多く、予断を許さない。とはいうものの全体としては比較的順調な推移が期待される。

情報セキュリティ市場については、インタビュー調査では引き続き堅調な需要の伸びを期待するベンダが多くみられた。Windows XP のサポート終了問題は、自治体をはじめ未対応の PC がまだ多く存在する問題がある。更新が進めばエンドポイントセキュリティ対策マーケットには追い風となる。一方、2011 年度から 3 年間続いた市場の拡大は、投資サイクルから見て、2014 年度にはやや一服となる可能性も否定できない。

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 2013 年度で一段落したものと考えられ、成長速度は更に鈍化し、3.4%にとどまるものと予測する。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も、IT 投資サイクル面で踊り場に差し掛かると考えられることから成長率は鈍化すると想定される。これに対し、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が期待される要素もあり、企業収益の改善に支えられて、セキュリティ投資もある程度堅調に推移すると考えられる。そのため、2013 年度の+5.3%からは鈍化するものの、+4.8%程度とサービス市場を上回る伸びを確保すると期待される。その結果、金額規模としては、ツールが 4,248 億円、サービスが 3,730 億円と、本統計開始以来最大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 4.1%と 4%代の成長率を維持して、7,978 億円と、8,000 億円に迫る規模に達するものと予測する。

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、一時停滞が続いた情報セキュリティ市場は、経済環境の好転、サイバーセキュリティ脅威の高まりと、それに対する社会的認知の浸透といった追い風要因を受けて、今回調査期間では順調な市場拡大が継続するものと考えられる。2014 年度には 8,000 億円に手が届く規模にまで拡大すると期待されるが、それは取りも直さず、情報セキュリティ対策がより重要かつ必須の経営課題と位置付けられることの反映であり、情報セキュリティ産業の社会経済的責任の加重を意味するものと理解される。

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、2012 年度の国内「情報セキュリティツール」市場は、3,849 億円の規模であったと推測される。2008 年度半ばに発生したリーマンショックにより 2009, 2010 年度に低迷を余儀なくされた情報セキュリティ市場は、東日本大震災の影響を受けつつも、2011 年度は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と推測している。その後も経済活動の回復に支えられ、高まるサイバー脅威への対応に迫られて、市場は拡大傾向にあると見られ、2012 年度の情報セキュリティツール市場の伸びは 5.3%程度を確保したものと見られる。

本調査では「情報セキュリティツール」市場を、その機能に着目していくつかの製品カテゴリに分類している。大分類レベルで、「統合型アプライアンス」、「ネットワーク脅威対策製品」、「コンテンツセキュリティ対策製品」、「アイデンティティ・アクセス管理製品」、「システムセキュリティ管理製品」、「暗号化製品」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	2011年度		2012年度			2013年度			2014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	19,229	5.3%	20,120	5.2%	4.6%	21,141	5.2%	5.1%	22,203	5.2%	5.0%
ネットワーク脅威対策製品	49,924	13.7%	52,112	13.5%	4.4%	54,122	13.3%	3.9%	56,061	13.2%	3.6%
コンテンツセキュリティ対策製品	139,299	38.1%	147,028	38.2%	5.5%	154,964	38.2%	5.4%	162,176	38.2%	4.7%
アイデンティティ･アクセス管理製品	65,523	17.9%	68,846	17.9%	5.1%	71,791	17.7%	4.3%	74,534	17.5%	3.8%
システムセキュリティ管理製品	51,747	14.2%	55,108	14.3%	6.5%	58,869	14.5%	6.8%	62,620	14.7%	6.4%
暗号化製品	39,838	10.9%	41,693	10.8%	4.7%	44,572	11.0%	6.9%	47,235	11.1%	6.0%
セキュリティツール市場合計	365,562	100.0%	384,907	100.0%	5.3%	405,460	100.0%	5.3%	424,829	100.0%	4.8%

図 2 に 2012 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 2012 年度の市場規模は 1,470 億円で、ツール市場全体に占める割合は 38.2%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 688 億円、構成比で 17.9%であった。第 3 位は「システムセキュリティ管理製品」が 551 億円で 14.3%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521 億円・13.5%、201 億円・5.2%で、合計すると 722 億円・18.5%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 417 億円・10.8%となった。

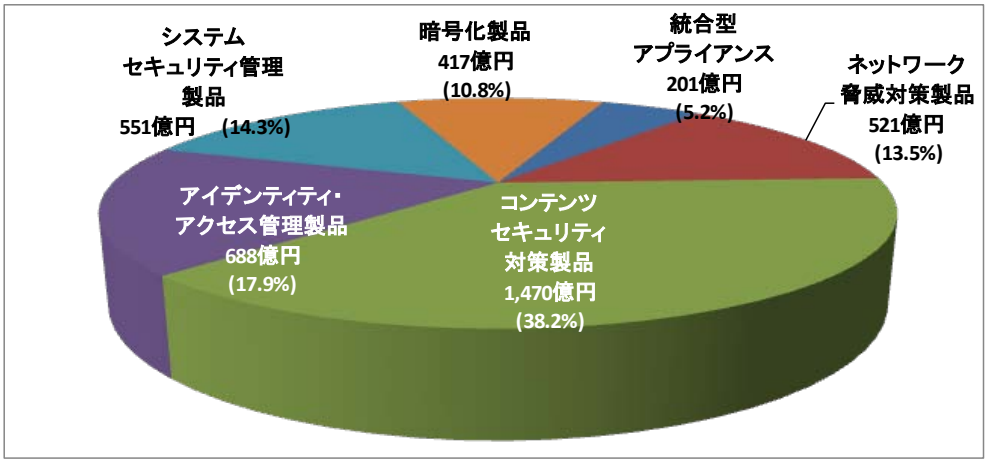
ここ数年のすう勢として、以下のことが観測される。

1)　セキュリティ対策を個別ユーザに最も近いところで守るエンドポイントセキュリティ対

策製品が中心の「コンテンツセキュリティ対策製品」は、対象が広い上に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、導入する位置が限定的で更新サイクルも数年のインターバルが一般的であり、成長度合いは緩やかとなっている。

図 2　2012 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、また昨今は内部者による情報持ち出し等の脅威も意識されるようになった結果、市場拡大速度を速めており、2 番目に大きいセグメントとなっている。

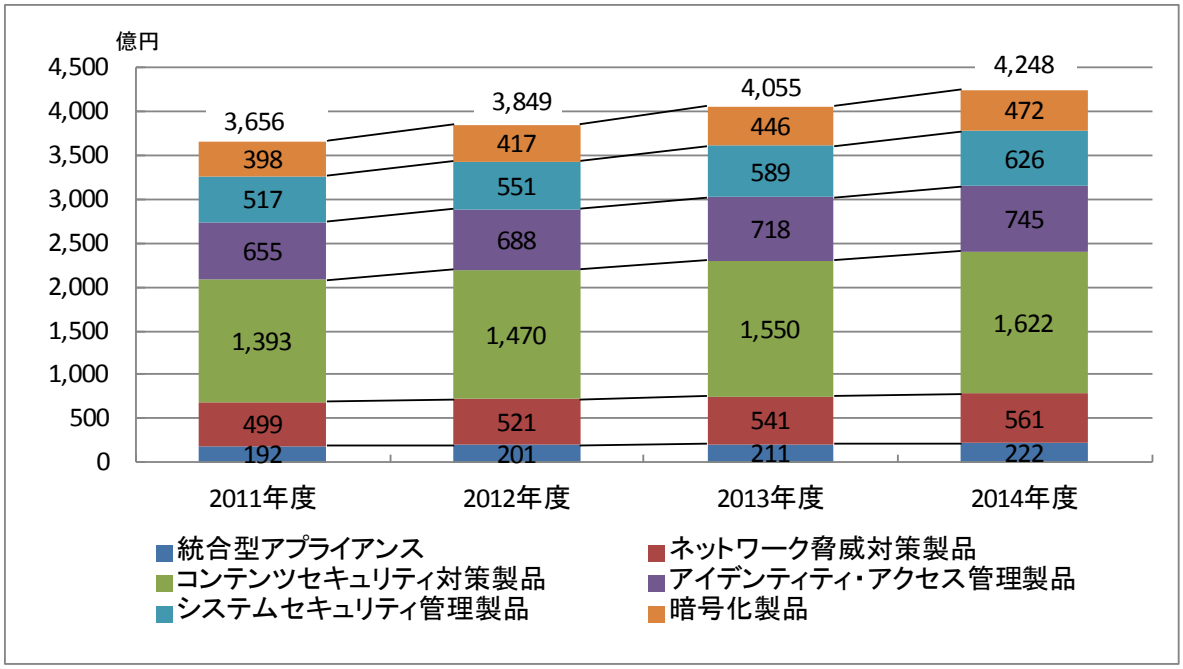
4) 標的型攻撃等、内部ネットワークへの侵入防止が困難となってきた今日の情勢を踏まえ、内部ネットワークの監視や解析、診断を行う「システムセキュリティ管理製品」も伸び率を高めている。このカテゴリには他に、端末のインベントリ・パッチ適用状態・設定等のコンプライアンス状態等を管理する製品やネットワーク検疫製品、さらにはセキュリティ目的のログ解析製品等、内部統制・情報漏えい・標的型攻撃への対応で需要が高まった製品が多く含まれ、高い伸び率を支えていると見られる。

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。

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経済は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、前年度までの投資抑制の反動と、大規模なハッキング被害（顧客情報 1 億人の流出と報道された）や防衛産業での相次ぐ標的型攻撃被害に対応して、企業が対策を急いだ結果、3.0%の成長を確保したものとみられる。（前回報告より）

図 3　国内情報セキュリティツール市場推移



2012 年度に最も高い伸び率を示したカテゴリ（大分類市場）は「システムセキュリティ管理製品」で 6.5%の伸び率であった。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。特に標的型攻撃対策としては、侵入防止だけでなくネットワーク内部の振る舞いや被害を特定するためのログ管理の重要性の認識が浸透しだした結果、この分野の製品の需要に結びついたものと理解される。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「コンテンツセキュリティ対策製品」で、伸び率は 5.5%であった。前年度がやや低い伸びであったことの反動と考えられる。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 5.1%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4.4%、4.6%で、ツール市場全体の伸び率を下回ったが、成熟市場の割には伸び率が高かったと言える。「暗号化製品」市場は 4.7%の伸びにとどまった。情報が漏えいしても中身までは見られないという、最後の砦としての対策や、クラウドの普及に伴い、第三者の管理下に置くデータはアプリオリに暗号で保護するという考え方も広がる中、拡大を続けているが、前年度の伸びが高かった反動か、2012 年度は相対的に低い伸びであった。

2013 年度に入ると、アメリカや韓国での相次ぐサイバーテロの報道やアメリカの PRISM 問題など、情報セキュリティへの関心を呼ぶ事件の増加を背景に、情報セキュリティ対策支出も引き続き増加する傾向がみられた。Windows XP の 2014 年 4 月でのサポート終了がアナウンスされたことも、情報セキュリティ対策への関心を喚起するのに一役買ったと考えられる。その結果、ツール市場は 4,055 億円と、初めて 4,000 億円の大台に達したものと見られる。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。

2014 年度は、消費増税の影響が軽微・短期間に留まると期待される中で、企業の投資態度も積極性を維持すると考えられ、成長ペースはややスローダウンするものの、ツール市場は引き続き+4.8%と高い成長率を維持して、4,248 億円と本統計史上の最高額を更新すると予測した。

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。

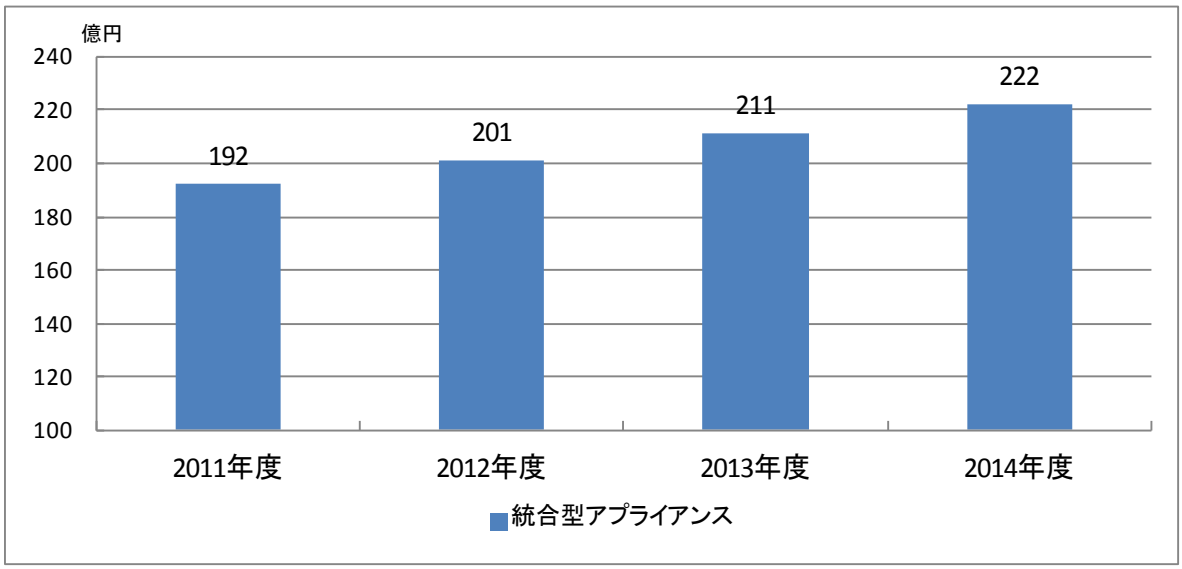
表 3　国内統合型アプライアンス市場規模　実績と予測

市場規模（百万円）	2011 年度	2012 年度	2013 年度	2014 年度
統合型アプライアンス	19,229	20,120	21,141	22,203
対前年度比成長率	―	4.6%	5.1%	5.0%

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、拡大と少しの減少傾向を見せたが、2011 年度以降は小幅ながらプラスが続き、2014 年度も継続して成長傾向が予測される。

2011 年度は、東日本大震災と原発事故、タイの洪水の影響により経済環境は厳しい中、日本企業や公共機関に対する深刻なサイバー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、市場はわずかながら拡大して 192 億円となった。

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の流れが継続したことと、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が背景となって、前年度比+4.6%の成長で 201 億円と 200 億円の大台を回復したものとみられる。これは 2007～2008 年度に前回の投資サイクルのピークがあったと考えられる 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、拡大ペースを維持し、5.1%の成長で 211 億円に達したものと推測する。ネットワーク脅威がますます高まったことや、アベノミクスによる経済回復への期待、投資の積極化に

より、情報セキュリティ投資が進んだと考えられる。

2014 年度も引き続き企業業績の動向とネットワーク脅威対策の必要への認知度によって市場動向が左右されると考えられる。前者については不確定要因が多いものの、普及型アプライアンスの需要層である中小企業の収益回復が期待できることから、やや高めの成長が継続するのではないかと見られ、5.0%の成長で 222 億円に達するものと予測する。

2.1.2.2. ネットワーク脅威対策製品市場

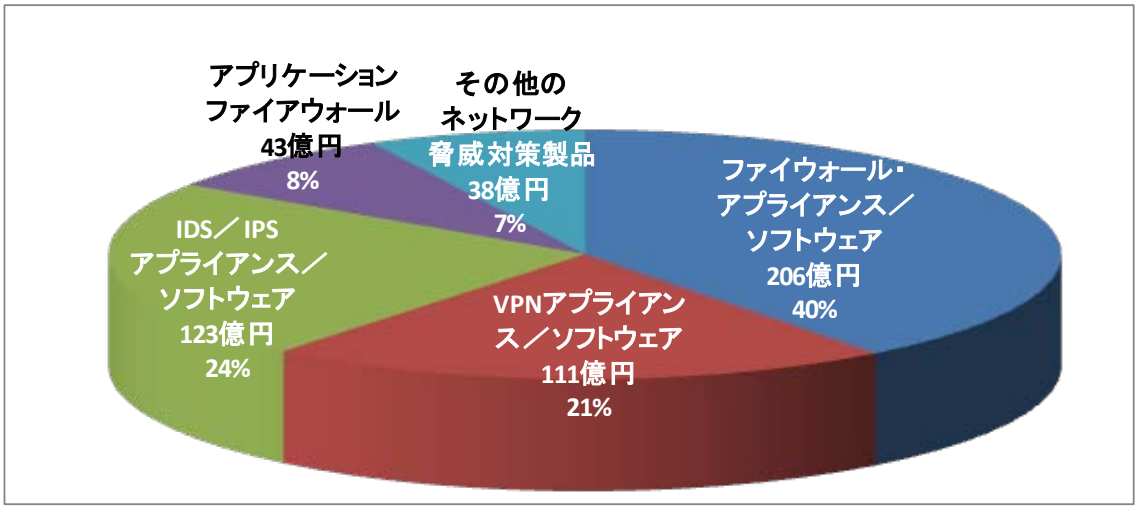
(1) 市場の動向

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　2012 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、他のネットワーク脅威対策製品に比較して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の、2012 年度における売上実績推定値は 521 億円となった。前年度比の市場成長率は 4.4%である。IDS／IPS 製品やアプリケーションファイアウォールが市場を牽引している。ネットワークセキュリティ対策の見直し・再構築の取組みが前年度から継続していることや、経済環境が比較的順調に推移したことが背景にあると考えられる。

2013 年度は、経済環境は企業収益の好調や円安による製造業の採算改善等追い風となったと考えられる。セキュリティ対策の見直しについてはある程度浸透して伸びが鈍化する要素と、ネットワーク脅威の深刻化に対する認知の浸透の要素が両面から作用したと想定される。その結果、伸び率は若干鈍化して 3.9%の成長となり、市場規模は 541 億円程度に達したものと推測される。

2014 年度も基本的には同様の流れが継続すると期待され、前年度比 3.6%増と市場拡大基調を維持して 561 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、2012 年度は 13.5%で 4 番目に大きいセグメントで、「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 18.7%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が確認できる。（表 2 参照）

---

[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

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）	2011 年度	2012 年度	2013 年度	2014 度
ファイアウォールアプライアンス/ソフトウェア	19,879	20,630	21,108	21,465
VPN アプライアンス／ソフトウェア	10,611	11,088	12,888	13,520
IDS／IPS アプライアンス／ソフトウェア	11,719	12,272	12,888	13,520
アプリケーションファイアウォール	4,030	4,273	4,574	4,889
その他のネットワーク脅威対策製品	3,685	3,848	4,088	4,332
合計	49,924	52,112	54,122	56,061
構成比				
ファイアウォールアプライアンス/ソフトウェア	39.8%	39.6%	39.0%	38.3%
VPN アプライアンス／ソフトウェア	21.3%	21.3%	21.2%	21.1%
IDS／IPS アプライアンス／ソフトウェア	23.5%	23.6%	23.8%	24.1%
アプリケーションファイアウォール	8.1%	8.2%	8.5%	8.7%
その他のネットワーク脅威対策製品	7.4%	7.4%	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	－	3.8%	2.3%	1.7%
VPN アプライアンス／ソフトウェア	－	4.5%	3.4%	3.4%
IDS／IPS アプライアンス／ソフトウェア	－	4.7%	5.0%	4.9%
アプリケーションファイアウォール	－	6.0%	7.0%	6.9%
その他のネットワーク脅威対策製品	－	4.4%	6.2%	6.0%
合計	－	4.4%	3.9%	3.6%

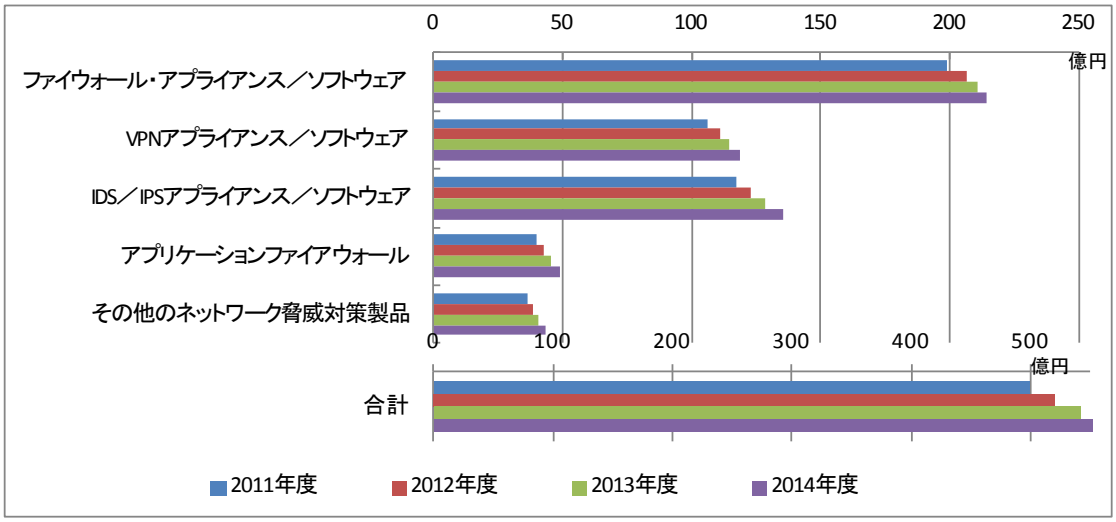
ネットワーク脅威対策製品のカテゴリの中では 1 番大きいセグメントである「ファイアウォールアプライアンス／ソフトウェア製品」は、本調査の対象期間でみると、2011 年度 199 億円、2012 年度 206 億円、2013 年度 211 億円、2014 年度 215 億円と増加傾向を見せている。2008 年度前半までは、通信事業者を中心とするハイエンドのユーザの設備投資サイクル上の更新期に当っていたが、2009, 2010 年度と、その反動と景気の低迷による設備投資控えの影響を受け、急速に市場規模が縮小した。2011, 2012 年度は設備の更新サイクルと対策の見直しが重なって市場規模が回復した。2013, 2014 年度に関しては、経済環境が比較的順調なことと、ネットワーク脅威の深刻化から対策の強化・見直しが続くことから、レイヤー7 対策を中心とした次世代型ファイアウォールへの乗り換えが見込まれ、率は鈍化するものの拡大傾向は続くとの予測となった。

「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が､その市場規模と成長率の推移は、2011 年度 106 億円、2012 年度 111 億円・4.5%増、2013 年度 129 億円・3.4%増、2014 年度 135 億円・3.4%増と、堅調な拡大傾向をたどるものと推定される。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が一層盛んであること、パブリッククラウドの活用が進んでいることから、市場規模は毎年堅調に増加するという予測になっている。

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」市場は、2011 年度は 117 億円であった。2012 年度 123 億円で 4.7%増、2013 年度 129 億円で 5.0%増、2014 年度 135 億円で 4.9%増という拡大傾向の推定・予測となった。特に 2013 年度、2014 年度に関しては、標的型攻撃に対する多段防御の中核を担う対策として、脆弱性を狙うゼロデイ攻撃などのマルウェア対策を振舞検知により行う方式の普及といった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、2011 年度 40 億円から、2012 年度 43 億円で 6.0%増、2013 年度 46 億円で 7.0%増、2014 年度 49 億円で 6.9%増と成長の度合いを徐々に強めると予測される。

「SQL インジェクション」や「クロスサイトスクリプティング」など、Web アプリケーションの脆弱性を利用した攻撃で、多くの大企業に被害が発生するケースが増えており、EC サイトや金融・公共機関などで導入が進んでいる。PCI DSS の要件として Web 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大きな要因になっている。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は、企業秘密の漏えい対策や内部統制への対応から需要が拡大していると考えられる。

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。表 5 で確認できるように、今回調査機関の中では、毎年 100 億円台の数字が増えている。ほぼ毎年 70 億円規模の拡大が続く結果である。年間成長率も 4%~5%台と、市場規模が大きく成熟度も高い割に固い。その要因としては、コンテンツセキュリティ製品の主たる導入対象であるエンドポイントの数そのものが拡大を続けていることが考えられる。企業・個人におけるパソコンの普及に加え、タブレット型端末やスマートフォンが急速に普及している。これ

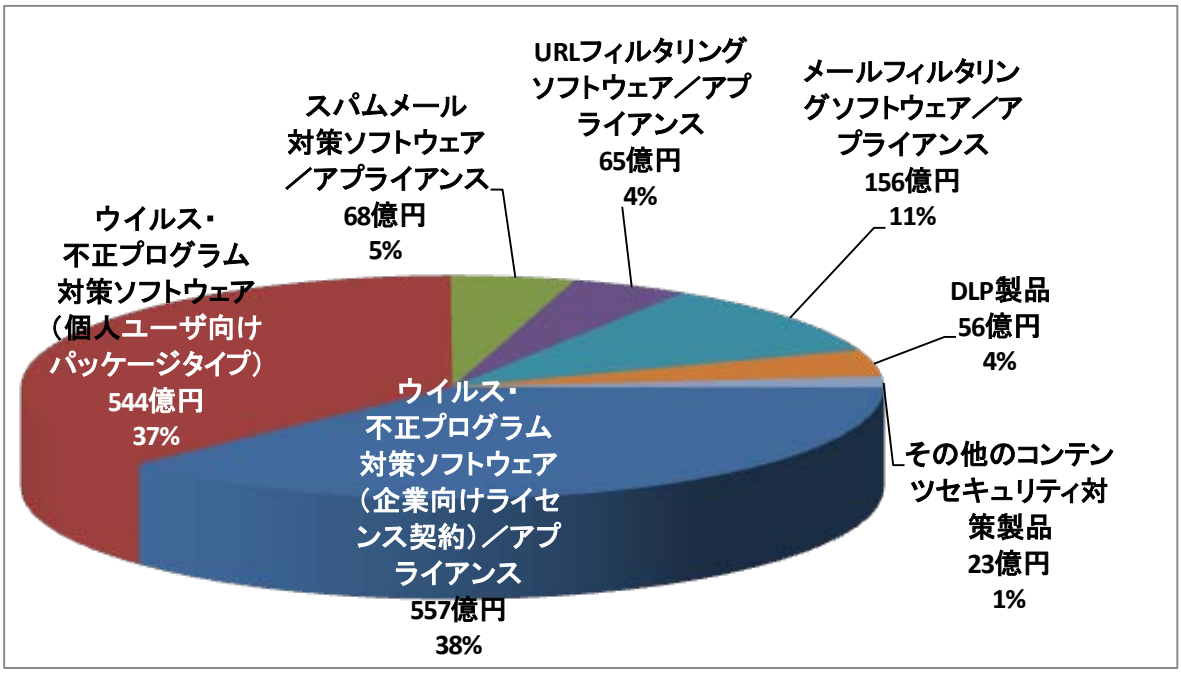
ら端末へのマルウェア対策が強く働きかけられており、導入も進んでいるために、市場規模も順調に拡大しているものと考えられる。

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 2012 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。

なお、BYOD (Bring Your Own Device 個人所有デバイスの業務利用)は徐々に浸透していくものと考えられ、モバイルデバイスを中心に、個人所有の IT 機器に会社のポリシーによるセキュリティ対策が導入されるケースが一般的になると考えられる。これは製品として、また市場として個人向けコンテンツセキュリティ製品と企業向けとの区分がなくなることを意味する。本調査においてはその間の仕分けの見直しが課題となることは留意を要する。

図 7　2012 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 2012 年度で 557 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、2013年度には4.6%増の583億円、2014年度には3.9%増の606億円に達するものと予測される。

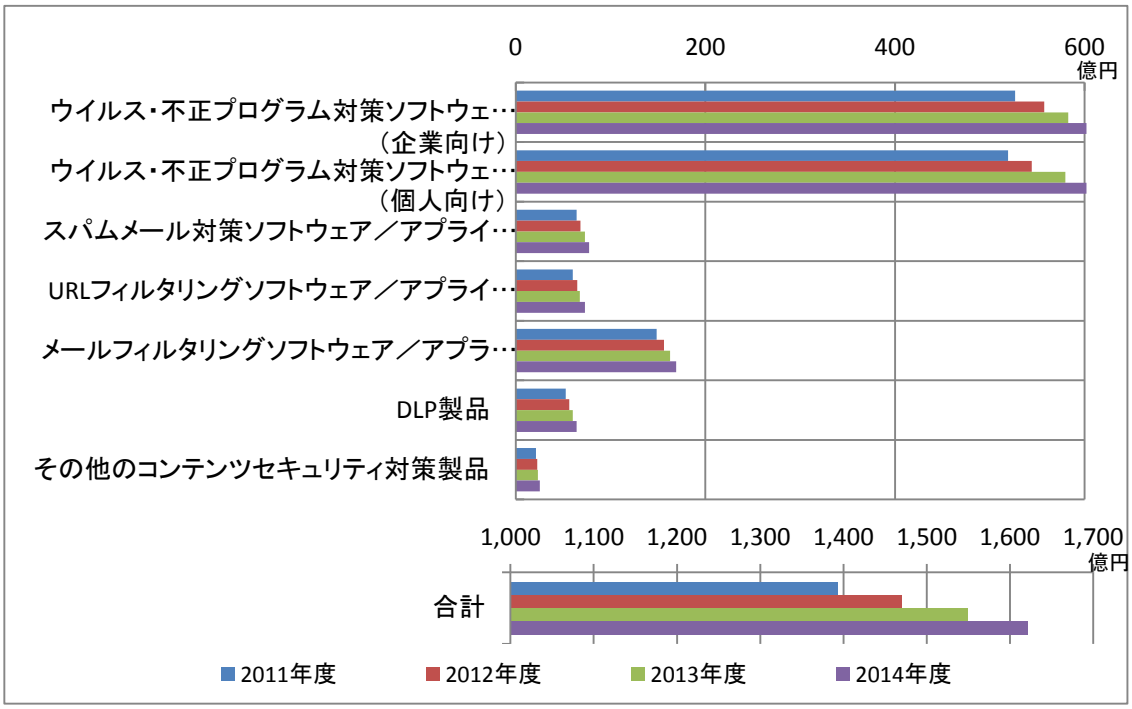
表 5　国内コンテンツセキュリティ対策製品市場規模　実績と予測

市場規模（百万円）	2011 年度	2012 年度	2013 年度	2014 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	52,663	55,736	58,296	60,556
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）	51,931	54,438	57,987	60,727
スパムメール対策ソフトウェア／アプライアンス	6,408	6,832	7,302	7,737
URL フィルタリングソフトウェア／アプライアンス	6,004	6,484	6,743	7,297
メールフィルタリングソフトウェア／アプライアンス	14,869	15,633	16,277	16,924
DLP 製品	5,283	5,642	6,028	6,406
その他のコンテンツセキュリティ対策製品	2,140	2,262	2,332	2,530
合計	139,299	147,028	154,964	162,176
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	37.8%	37.9%	37.6%	37.3%
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）	37.3%	37.0%	37.4%	37.4%
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%	4.7%	4.8%
URL フィルタリングソフトウェア／アプライアンス	4.3%	4.4%	4.4%	4.5%
メールフィルタリングソフトウェア／アプライアンス	10.7%	10.6%	10.5%	10.4%
DLP 製品	3.8%	3.8%	3.9%	3.9%
その他のコンテンツセキュリティ対策製品	1.5%	1.5%	1.5%	1.6%
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	－	5.8%	4.6%	3.9%
ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ）	－	4.8%	6.5%	4.7%
スパムメール対策ソフトウェア／アプライアンス	－	6.6%	6.9%	6.0%

URL フィルタリングソフトウェア／アプライアンス	―	8.0%	4.0%	8.2%
メールフィルタリングソフトウェア／アプライアンス	―	5.1%	4.1%	4.0%
DLP 製品	―	6.8%	6.8%	6.3%
その他のコンテンツセキュリティ対策製品	―	5.7%	3.1%	8.5%
合計	―	5.5%	5.4%	4.7%

「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）」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。2012 年度の市場規模は 544 億円であったと推計される。2013 年度+6.5%、2014 年度+4.7%と順調に拡大し、各々580 億円、607 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大きく寄与すると考えられる。

図 8　国内コンテンツセキュリティ対策製品市場推移



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 2012 年度で 156 億円であるが、2014 年度には 169 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、2012 年度で 68 億円である。この市場も 2013 年度+6.9%、2014 年度+6.0%とコンスタントに拡大して 2014 年度の市場規模は 77 億円に達すると予測される。

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。2012 年度 65 億円、2013 年度 67 億円（4.0%増）、2014 年度 73 億円（8.2%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 2012 年度には 56 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、2013 年度 60 億円（6.8%増）、2014 年度 64 億円（6.3%増）との予測結果となった。

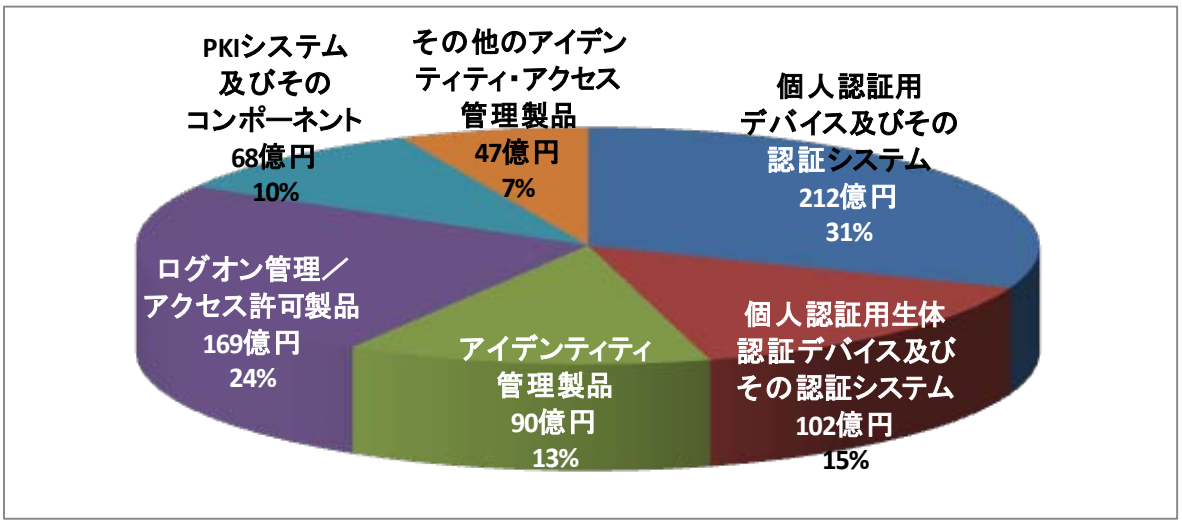
2.1.2.4. アイデンティティ・アクセス管理製品市場

(1) 市場の動向

図 9 に 2012 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。

図 9　2012 年度のアイデンティティ・アクセス管理製品市場



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、データの誤入力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。

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。

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

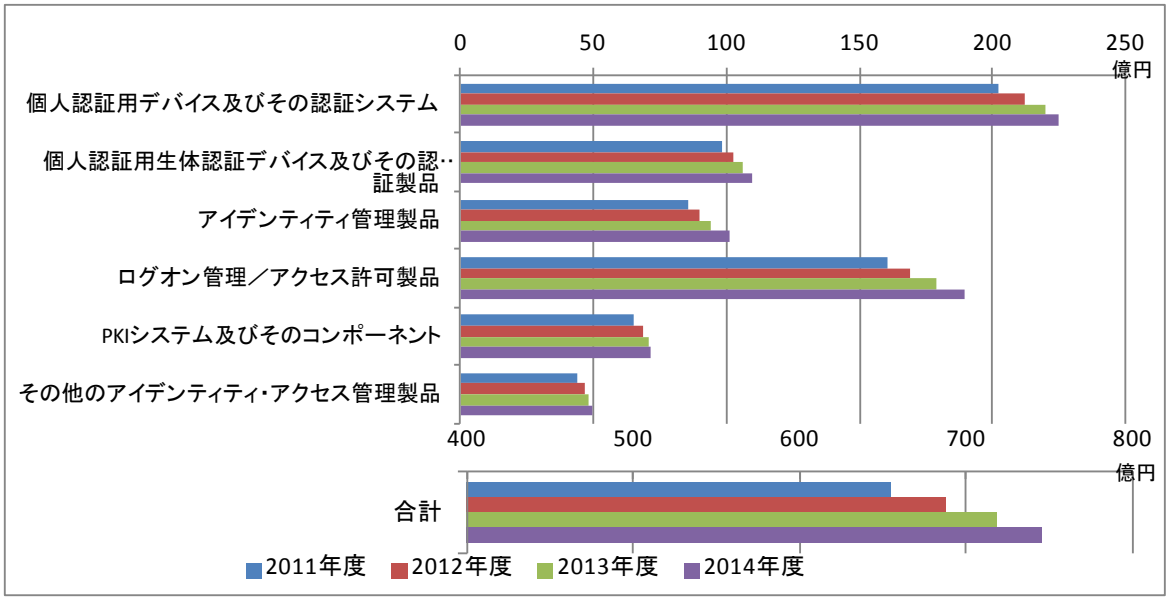
市場規模（百万円）	2011 年度	2012 年度	2013 年度	2014 年度
個人認証用デバイスおよびその認証システム	20,194	21,201	21,995	22,470
個人認証用生体認証デバイスおよびその認証システム	9,842	10,232	10,582	10,942
アイデンティティ管理製品	8,545	8,976	9,406	10,137
ログオン管理／アクセス許可製品	16,042	16,930	17,886	18,926
PKI システムおよびそのコンポーネント	6,486	6,846	7,101	7,131
その他のアイデンティティ・アクセス管理製品	4,414	4,660	4,822	4,927
合計	65,523	68,846	71,791	74,534
構成比				
個人認証用デバイスおよびその認証システム	30.8%	30.8%	30.6%	30.1%
個人認証用生体認証デバイスおよびその認証システム	15.0%	14.9%	14.7%	14.7%
アイデンティティ管理製品	13.0%	13.0%	13.1%	13.6%
ログオン管理／アクセス許可製品	24.5%	24.6%	24.9%	25.4%
PKI システムおよびそのコンポーネント	9.9%	9.9%	9.9%	9.6%
その他のアイデンティティ・アクセス管理製品	6.7%	6.8%	6.7%	6.6%
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	5.0%	3.7%	2..2%

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	4.0%	3.4%	3.4%
アイデンティティ管理製品	ー	5.1%	4.8%	7.8%
ログオン管理／アクセス許可製品	ー	5.5%	5.6%	5.8%
PKI システムおよびそのコンポーネント	ー	5.5%	3.7%	0.4%
その他のアイデンティティ・アクセス管理製品	ー	5.6%	3.5%	2.2%
合計	ー	5.1%	4.3%	3.8%

アイデンティティ・アクセス管理製品の市場規模は、2012 年度の実績で 688 億円（前年比伸び率 5.1%）となったが、「情報セキュリティツール」市場全体の 3,849 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、2011 年 3 月の東日本大震災の影響を受け、 2011 年度は 655 億円にとどまったが、2012 年度は 688 億円まで回復し、2013 年度には 718 億円（前年比伸び率+4.3%）と、700 億円台に到達すると予測される。

「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 2012 年度の構成比で 30.8%と最も大きな部分を占めた。市場規模は 2012 年度で 212 億円であり、2013 年度は 220 億円と前年比 3.7%増と予想される。

図 10　国内アイデンティティ・アクセス管理製品市場推移



これに次いで規模の大きい市場セグメントは「ログオン管理／アクセス許可製品」である。市場規模は 2012 年度に 169 億円で、2013 年度には 5.6%拡大して 179 億円となり、2014 年度には 189 億円（前年度比成長率 5.8%）に達する。

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 2012 年度は、4.0%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 5.5%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。

「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、また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。

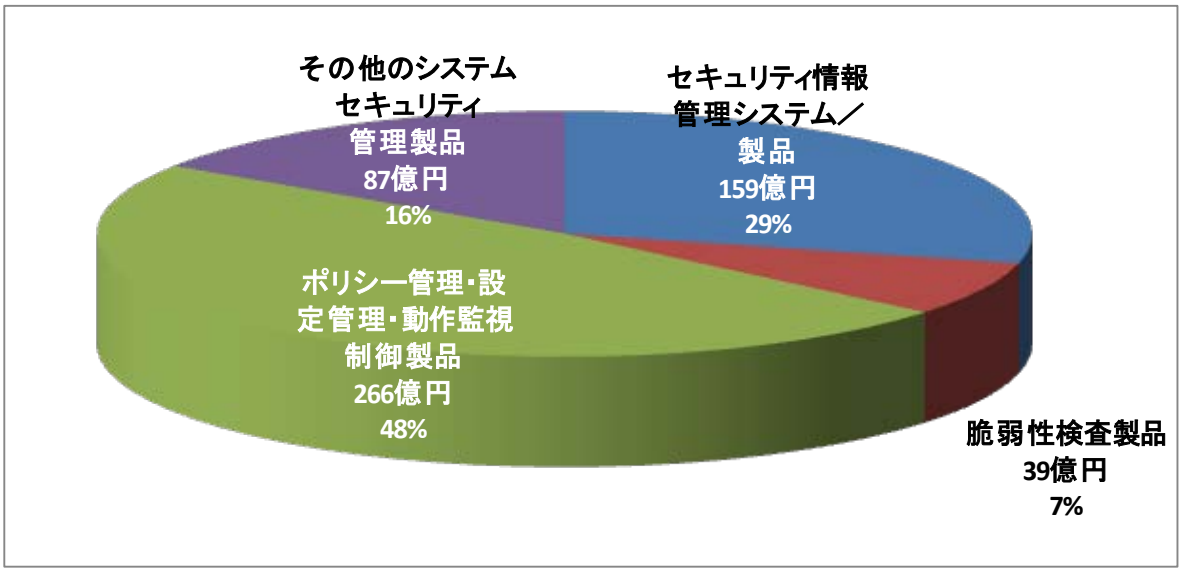
2.1.2.5. システムセキュリティ管理製品市場

(1) 市場の動向

システムセキュリティ管理製品の 2012 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。

図 11　2012 年度のシステムセキュリティ管理製品市場



「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。

「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

[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

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）と呼ばれるリモートロック、リモートワイプ（初期化、無効化）するツールの導入が進み、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BYODの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。

「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 2012 年度には全セグメント合せて 551 億円程度の市場を形成しており、2011 年度と比べると+6.5%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 2013 年度は 6.8%増の 589 億円とさらに高い伸び率を見込んでおり、その傾向は 2014 年度（626 億円、+6.4%）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

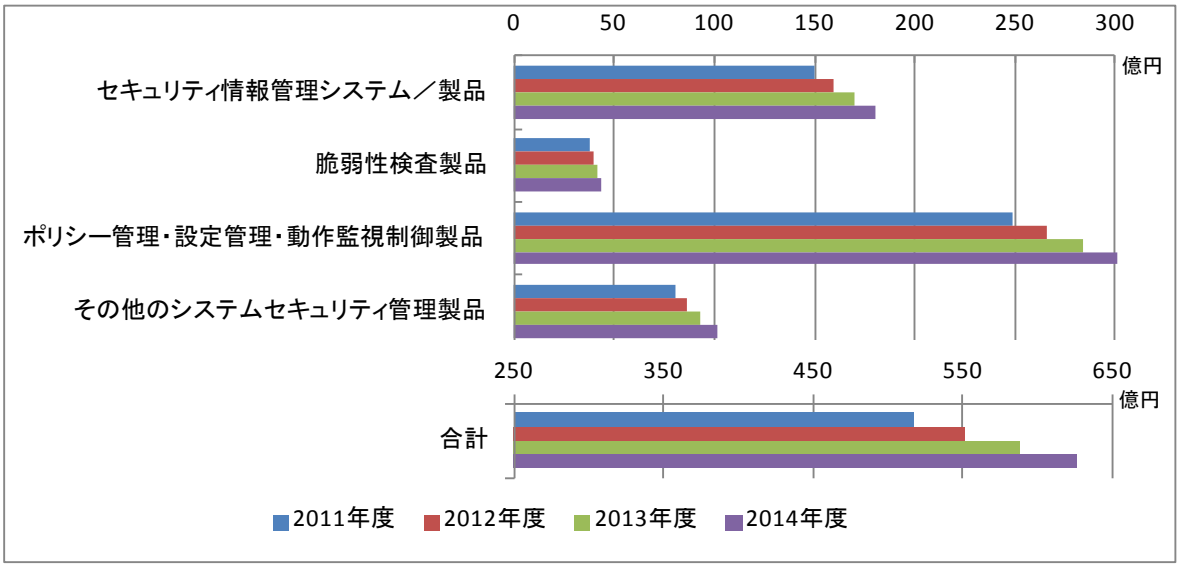
市場規模（百万円）	2011 年度	2012 年度	2013 年度	2014 年度
セキュリティ情報管理システム／製品	15,036	15,922	16,961	17,996
脆弱性検査製品	3,762	3,942	4,154	4,363
ポリシー管理・設定管理･動作監視制御製品	24,862	26,580	28,432	30,132
その他のシステムセキュリティ管理製品	8,088	8,664	9,322	10,129
合計	51,747	55,108	58,869	62,620
構成比				
セキュリティ情報管理システム／製品	29.1%	28.9%	28.8%	28.7%
脆弱性検査製品	7.3%	7.2%	7.1%	7.0%
ポリシー管理・設定管理･動作監視制御製品	48.0%	48.2%	48.3%	48.1%
その他のシステムセキュリティ管理製品	15.6%	15.7%	15.8%	16.2%
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	－	5.9%	6.5%	6.1%
脆弱性検査製品	－	4.8%	5.4%	5.0%
ポリシー管理・設定管理･動作監視制御製品	－	6.9%	7.0%	6.0%
その他のシステムセキュリティ管理製品	－	7.1%	7.6%	8.7%
合計	－	6.5%	6.8%	6.4%

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 2012 年度に 159 億円、前年度比 5.9%増と増加傾向にあり、さらに 2013 年度は 6.5%増の 170 億円、2014 年度は+6.1%の 180 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、2012 年度の予測における成長率も+6.9%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 266 億円である。2013 年度は+7.0%で 284 億円、2014 年度は 6.0%増の 301 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 2012 年度で 39 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、2013 年度+5.4%、2014 年度+5.0%程度と予測され、2014 年度の市場規模は 44 億円と推定される。

図 12　国内システムセキュリティ管理製品市場推移



「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。2012 年度の伸び率は+7.1%で、2013 年度+7.6%、2014 年度+8.7%と高い成長率を示し、2014 年度には 101 億円規模に達するものと予測される。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やログ相関分析の需要が高まっていることを反映していると考えられる。

2.1.2.6. 暗号化製品市場

(1) 市場の動向

2012 年度は、震災の影響を受けた 2011 年に大きく上昇した影響から少し鈍化し 4.7%の上昇となった。ただし、鈍化したとはいえ、暗号化製品は好調な推移を見せている。

これは、「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結果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。また各府省庁が保有す

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、今回調査対象期間における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 により要件の明確化が進んだ結果、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。

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普及している点、WindowsXP の保守終了による PC 買い替えにより、HDD 暗号化製品のリプレースが進んだ点なども挙げられる。また最近ではクラウドサービスが活況となっているが、一方で企業データをクラウドに置くことにリスクを感じる企業向けに「クラウド上のデータを暗号化する」といった新たなソリューションも増えている。企業にとって「外部にデータを置く」というケースが増えることことが予想され、上記の理由を含め今後も暗号化製品の市場は好調に推移していくと推測される。

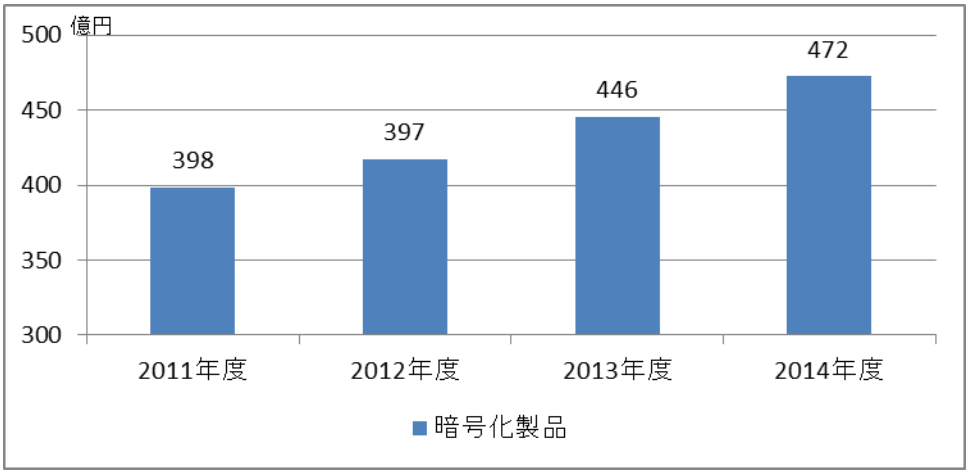
(2)市場規模とその推移

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）	2011 年度	2012 年度	2013 年度	2014 年度
暗号化製品	39,838	41,693	44,572	47,235
対前年度比成長率				
暗号化製品	－	4.7%	6.9%	6.0%

図 13　国内暗号化製品市場推移



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%を占めている。2012 年度の市場規模は 417 億円で前年度比 4.7%増加となった。2013 年度は前年度比 6.9%増の 446 億円と大きく拡大、2014 年度もさらに 6.0%市場規模を拡大させ、472 億円規模の市場になると予測している。

2013 年の市場規模の拡大は Windows XP のリプレースによる HDD 暗号化製品のリプレースも寄与していると予想している。この伸び率はセキュリティツール全体の伸び率を上回り、セキュリティツール全体に占める比率は 11.0%に拡大している。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拡大していくと予測する。

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や、有償で行われる使用に関するトレーニング等の教育については、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	2011年度		2012年度			2013年度			2014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	67,958	20.7%	70,165	20.3%	3.2%	72,249	20.0%	3.0%	74,250	19.9%	2.8%
セキュアシステム構築サービス	129,395	39.4%	138,889	40.1%	7.3%	144,481	40.1%	4.0%	148,289	39.8%	2.6%
セキュリティ運用・管理サービス	98,417	30.0%	103,189	29.8%	4.8%	108,747	30.2%	5.4%	114,397	30.7%	5.2%
情報セキュリティ教育	25,237	7.7%	26,574	7.7%	5.3%	27,387	7.6%	3.1%	28,132	7.5%	2.7%
情報セキュリティ保険	7,468	2.3%	7,640	2.2%	2.3%	7,799	2.2%	2.1%	7,930	2.1%	1.7%
セキュリティサービス市場合計	328,475	100.0%	346,457	100.0%	5.5%	360,664	100.0%	4.1%	372,998	100.0%	3.4%

今回の調査結果では、対象期間の最初の年度である 2011 年度の「情報セキュリティサービス」市場規模は 3,285 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。その結果、これらの市場規模はある段階から縮小に向かうと考えられていた。そのフェーズが顕在化したのが、2009, 2010 年度で、リーマンショック後の経済の低迷の時期と重なり、顕著な変化が見られた。2011 年度は東日本大震災、電力供給の切迫、タイ大洪水と経済環境は厳しさが続いた一方、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。サイバーセキュリティ脅威はその深刻度と複雑性がますます高まり、対策も不断の点検・見直しと更新が必要となってきている。また対策の必要性に対する認知も広く浸透するようになってきた。こういったことを背景にコンサルテーションやシステム構築サービスといった一過性が内在するサービスも循環的に需要が生起するものと考える必要が出てきているようである。

2012 年度は、第 1 章で見たように、経済環境が改善する中、国内大企業や国の機関におけるサイバー攻撃の深刻な被害が顕在化したことにより、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。これには上に見たように、サイバー脅威の質的変化に対応した抜本的見直しの動きが継続したことが大きく、市場規模の大きいセキュアシステム構築サービスが高い成長を示したことから、サービスの伸びはツールを上回る+5.5%に達したと見られ、市場規模は 3,465 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、+4.1%の成長で 3,607 億円と、初めて 3,600 億円台に到達するものと予測される。また 2014 年度も経済条件が引き続き堅調に推移すると期待される中で、サイバー脅威の深刻化も進行することから、伸び率は鈍化するものの市場の拡大は続き、前年度比+3.4%成長して 3,730 億円規模に達するものと予測される。

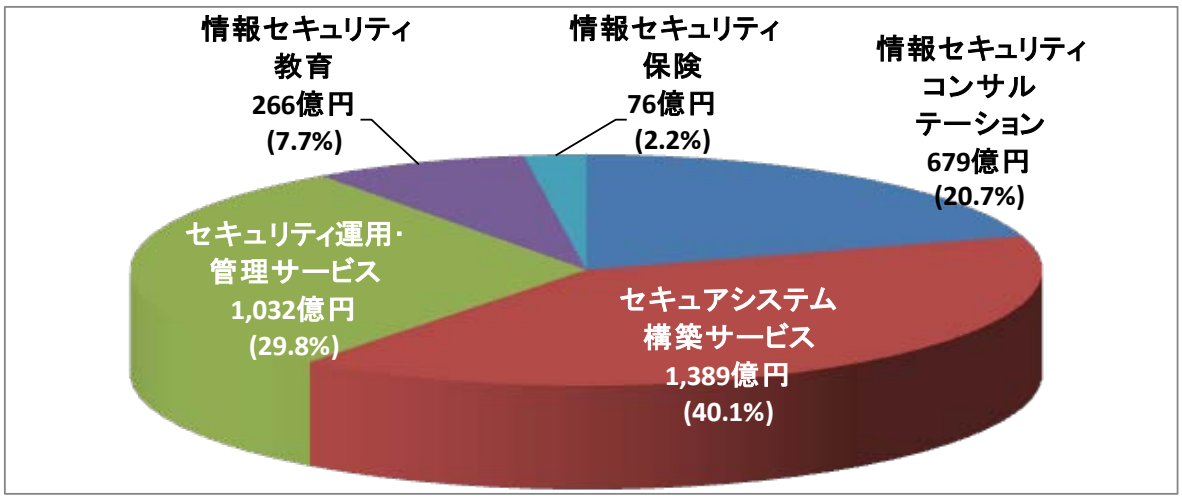
図 14 に 2012 年度の国内情報セキュリティサービス市場のカテゴリ別分布を示す。また図 15 には国内情報セキュリティサービス市場の経年推移を表した。

「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、2012 年度実績推定値で 1,389 億円と、情報セキュリティサービス市場全体の 40.1%を占めた。このカテゴリは、IT システムに対してセキュリティ機能を設計・導入・構築するサービスである。システムインテグレーションに際してセキュリティ機能を組み込む部分のサービスや、既存の IT システムに対してセキュリティ機能を付加したり強化したりするために、IT セキュリティシステムを設計･製品導入･構築するサービスが中心となる。システムインテグレーション的要素が強いために、市場規模も大きなものになっている。

次に大きなカテゴリは「セキュリティ運用･管理サービス」で、2012 年度実績は 1,032 億円と、初めて 1,000 億円の大台に達したものと推定される。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。

図 14　2012 年度の国内情報セキュリティサービス市場



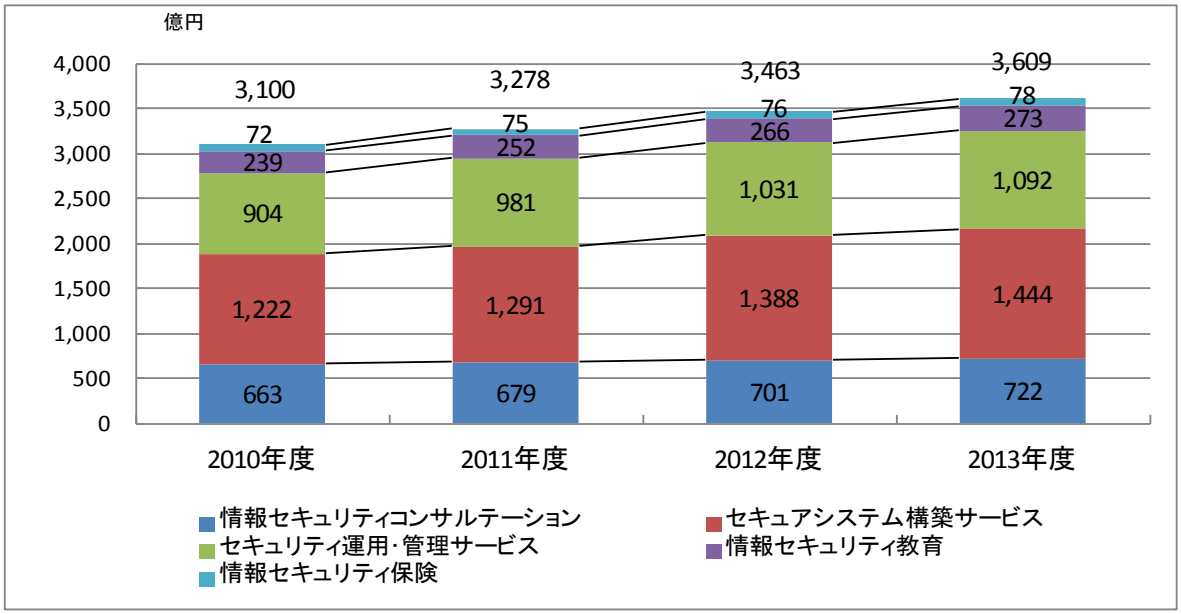
「セキュリティ運用・管理サービス」に関しては、2000 年代半ば頃から複雑化するネットワーク、高度化し頻度が高まる攻撃、特に電子商取引サイトへの攻撃やそれによる被害の深刻化等を背景に、専門サービスへのアウトソーシングを積極活用しようという判断が増えて、需要が堅調に拡大している。深刻な情報セキュリティインシデントが多発し、かつ攻撃側の技術や手法がますます高度化して、専門知識やスキルなしでは対応が困難となってきている。そのため、十分な対策のためには専門家によるサービスに頼らざるを得ない状況が現出し、対策の必要性に対する認識も浸透する中で、需要の堅調な拡大に結びついている。

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。過去において「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、2012 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 3.2%拡大して 702 億円になったと見られる。

「情報セキュリティ教育」の 2012 年度実績推定値は前年度比+5.3%とサービス全体とほぼ同じ拡大ペースで 266 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、標的型攻撃や水飲み場型攻撃対策と

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、継続的に従業員教育を施して最新の知識と注意点を身につけさせる必要が高まっている。教育市場拡大の背景にはそういった要素が存在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。その結果、2000 年代後半は伸び率がほとんどなくなっていたが、2010 年代に入って、インシデントの多発と深刻化が進み、完全な防御は困難との認識が形成されるようになった。その結果、保険への需要は再び拡大傾向を見せている。市場規模は、2012 年度で前年度比+2.3%の 76 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

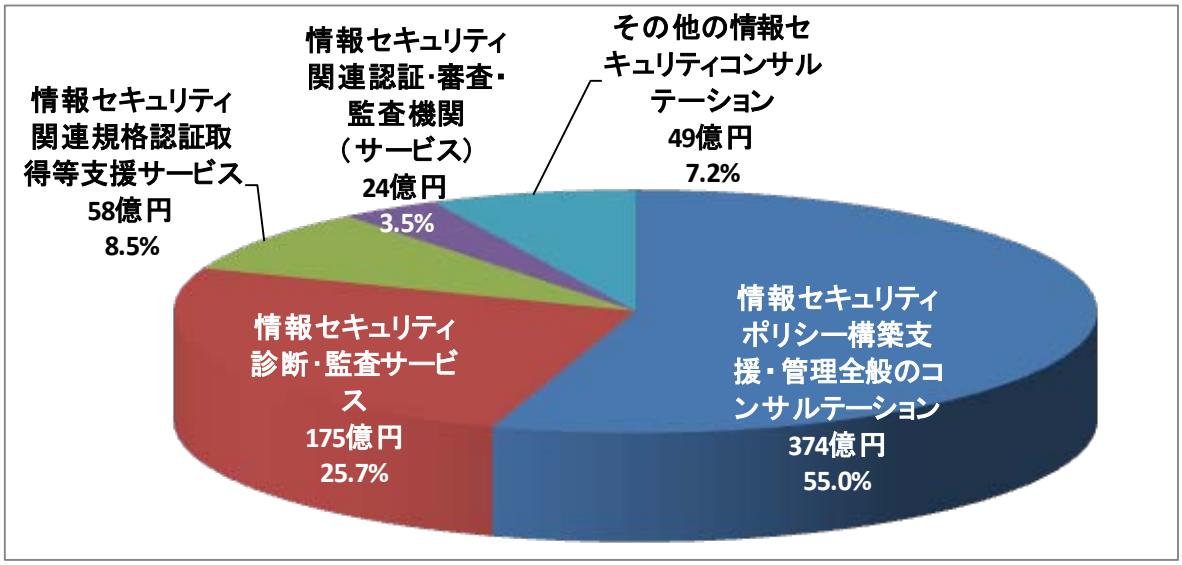
図 16 に、2012 年度における情報セキュリティコンサルテーション市場のセグメント別市場分布を示す。

「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　2012 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、程なくして終息した。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。JIPDEC 統計で 2014 年 3 月現在、ISMS 認証取得組織数は 4,493 件（2013 年 1 月: 4,209 件）、プライバシーマーク認定取得企業数は 13,575 社（2013 年 1 月: 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 といった基準も普及が進んでいる。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、東日本大震災以降は具体的取り組みや対策実施が本格化している。

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、情報セキュリティ企画に関する認証取得関連のサービスはマイナス成長となった。これは、ISMS や P マークの認証取得が一巡したところに東日本大震災が発生した結果、新規認証取得の

取組みが中断した結果と想定される。しかしそれも 2012 年度までで下げ止まり、以降は経済環境の好転に伴って回復すると見込まれる。また、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ことから、事業継続管理を意識した情報セキュリティ対策の抜本的見直しの動きも顕在化している。その背景には、2011 年度ごろから様変わりとも言える変化を見せている、サイバー脅威の深刻化がある。その結果、2013 年度は一転して全ての分野においてプラス成長となり、2014 年度も継続し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

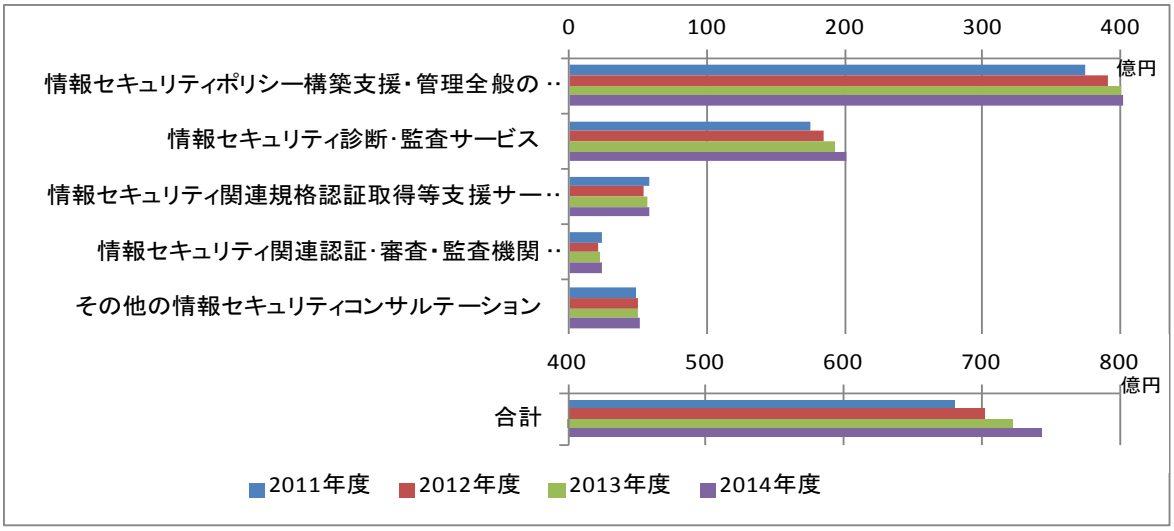
表 10 に国内の情報セキュリティコンサルテーション市場規模の実績推定値と予測値を、図 17 にその市場規模の推移のグラフを示す。

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）	2011 年度	2012 年度	2013 年度	2014 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	37,381	39,139	40,036	40,869
情報セキュリティ診断･監査サービス	17,502	18,489	19,303	20,166
情報セキュリティ関連規格認証取得等支援サービス	5,820	5,426	5,615	5,793
情報セキュリティ関連認証･審査・監査機関（サービス）	2,345	2,169	2,265	2,354
その他の情報セキュリティコンサルテーション	4,909	4,942	5,029	5,068
合計	67,958	70,165	72,249	74,250
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	55.0%	55.8%	55.4%	55.0%
情報セキュリティ診断･監査サービス	25.8%	26.4%	26.7%	27.2%
情報セキュリティ関連規格認証取得等支援サービス	8.6%	7.7%	7.8%	7.8%
情報セキュリティ関連認証･審査・監査機関（サービス）	3.5%	3.1%	3.1%	3.2%
その他の情報セキュリティコンサルテーション	7.2%	7.0%	7.0%	6.8%
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	－	4.7%	2.3%	2.1%
情報セキュリティ診断･監査サービス	－	5.6%	4.4%	4.5%
情報セキュリティ関連規格認証取得等支援サービス	－	-6.8%	3.5%	3.2%
情報セキュリティ関連認証･審査・監査機関（サービス）	－	-7.5%	4.4%	3.9%
その他の情報セキュリティコンサルテーション	－	0.7%	1.8%	0.8%
合計	－	3.2%	3.0%	2.8%

2012 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 702 億円程度となり、前年度比成長率はプラス 3.2%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。2013 年度も全体で 722 億円程度（前年度比成長率+3.0%）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も増加に転じるものと推測される。

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



このカテゴリにおいて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 391 億円、「情報セキュリティ診断・監査サービス」の 185 億円の２つで、合わせて市場全体の約 82%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。

2012 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 7.5%減の 22 億円になった。2013 年度はプラス成長に転じ 4.4%増の 23 億円となると見込まれる。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、PCI DSS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 2012 年度 54 億円（前年度比成長率マイナス 6.8%）となり、2013 年度に至ってプラス成長に転じ 56 億円（同プラス 3.5%）と回復している。

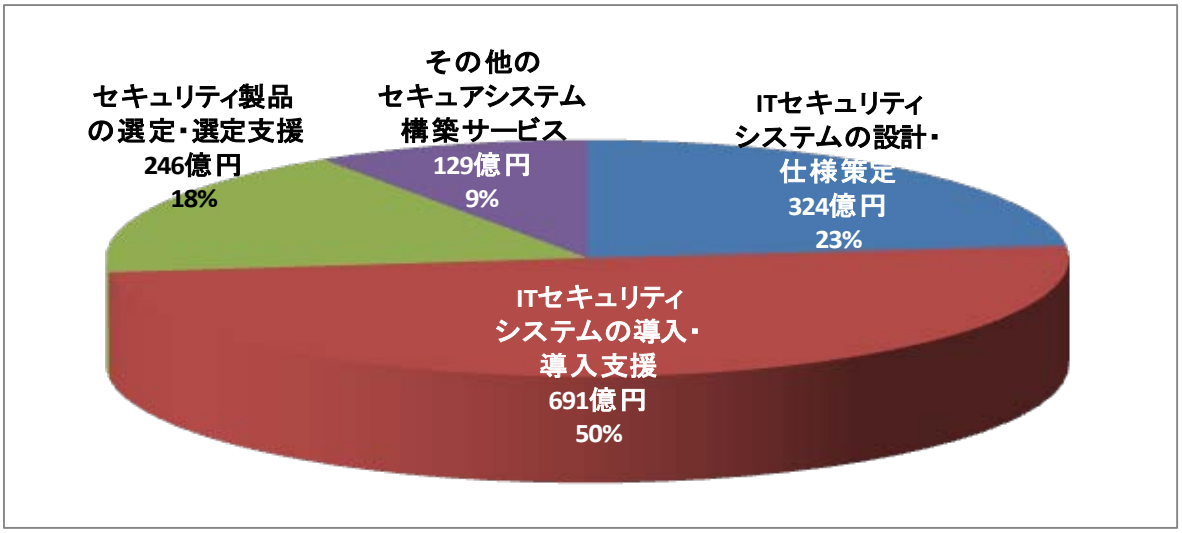
[7] http://www.isms.jipdec.or.jp/lst/ind/suii.html
http://www.iso.org/iso/home/standards/certification/iso-survey.htm

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 2012 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　2012 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、2011 年度 1,294 億円、2012 年度 1,389 億円、2013 年度には 1,445 億円とプラス成長がみられ、2014 年度には 1,483 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 40.1%を占めており、セキュ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、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、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）	2011 年度	2012 年度	2013 年度	2014 年度
IT セキュリティシステムの設計･仕様策定	30,622	32,398	33,702	34,597
IT セキュリティシステムの導入･導入支援	63,372	69,075	71,970	73,887
セキュリティ製品の選定･選定支援	22,978	24,552	25,415	26,096
その他のセキュアシステム構築サービス	12,423	12,864	13,395	13,707
合計	129,395	138,889	144,481	148,289
構成比				
IT セキュリティシステムの設計･仕様策定	23.7%	23.3%	23.3%	23.3%
IT セキュリティシステムの導入･導入支援	49.0%	49.7%	49.8%	49.8%
セキュリティ製品の選定･選定支援	17.8%	17.7%	17.6%	17.6%
その他のセキュアシステム構築サービス	9.6%	9.3%	9.3%	9.2%
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	－	5.8%	4.0%	2.7%
IT セキュリティシステムの導入･導入支援	－	9.0%	4.2%	2.7%
セキュリティ製品の選定･選定支援	－	6.9%	3.5%	2.7%
その他のセキュアシステム構築サービス	－	3.5%	4.1%	2.3%
合計	－	7.3%	4.0%	2.6%

「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、2011 年度 634 億円、2012 年度 691 億円（前年度比+9.0%）、2013 年度 720 億円（同+4.2%）、2014 年度予測 739 億円（同+2.7%）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 2011 年度 306 億円、2012 年度 324 億円（前年度比+5.8%）、2013 年度 337 億円（同+4.0%）、2014 年度予測 346 億円（同+2.7%）と推定する。

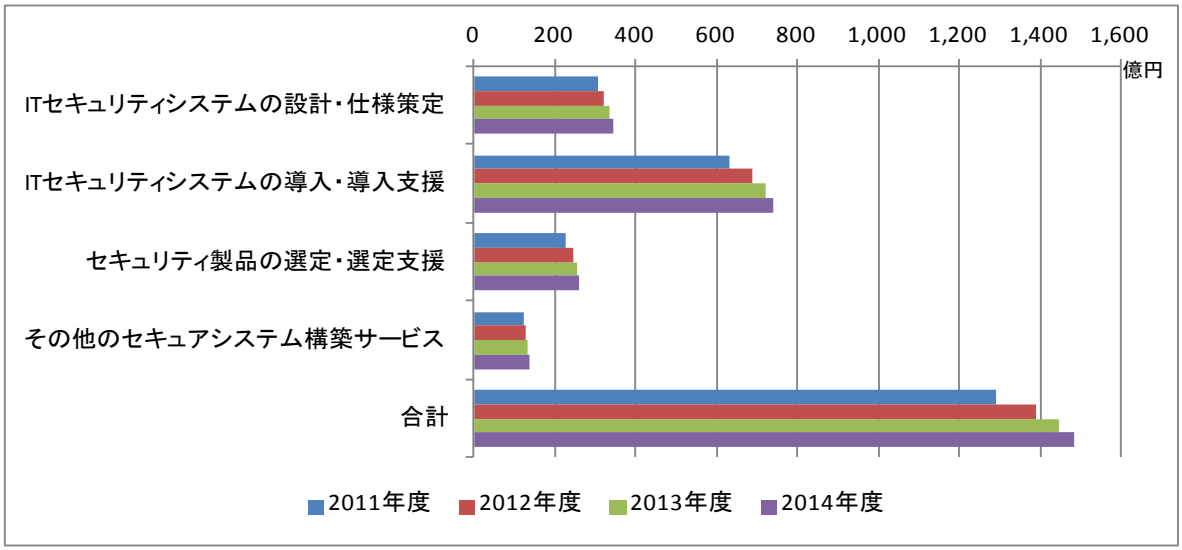
「セキュリティ製品の選定･選定支援」はシステム構築まで至らず個別の製品を選定するに際し

[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

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 年度は 230 億円、2012 年度が 246 億円（前年度比+6.9%）、2013 年度は 254 億円（同+3.5%）、2014 年度には 261 億円（同+2.7%）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

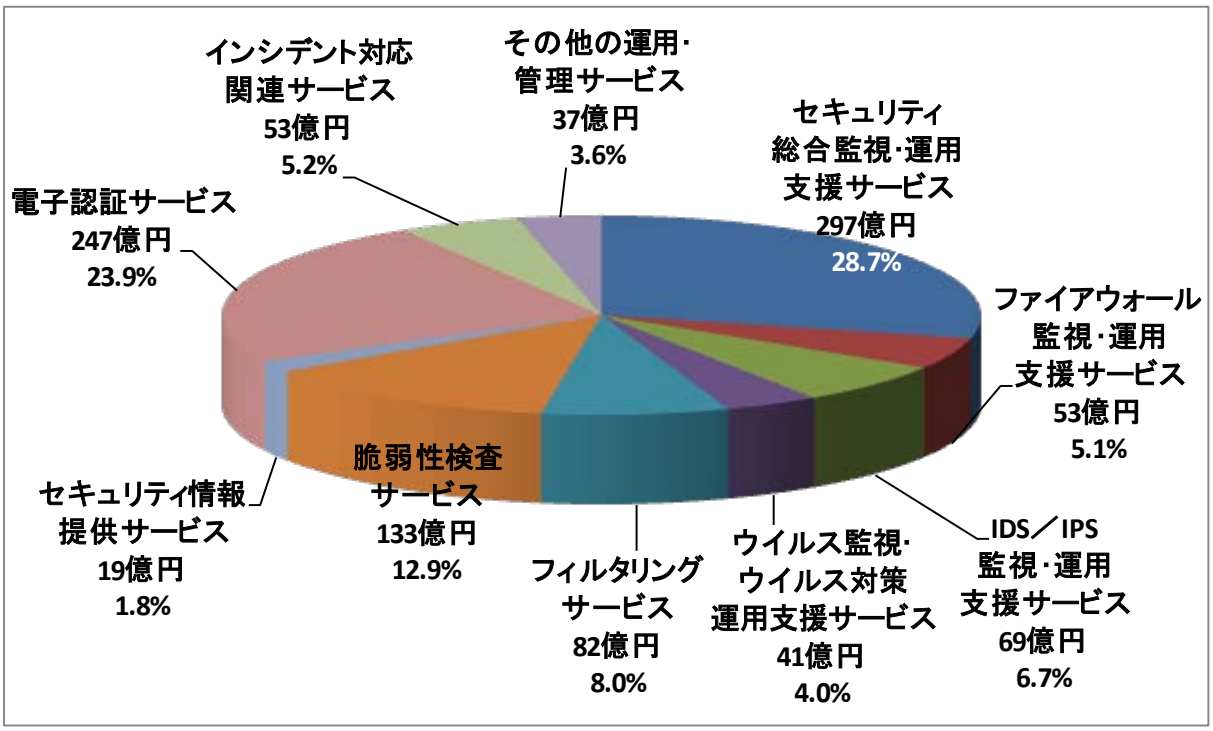
(1) 市場の動向

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業者にアウトソースするのが望ましいという需要によって支えられている。その理由は、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で、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と、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考えられる。サイバー攻撃の増加に伴い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・統合化する一方で、クラウドサービスの増加も牽引し、「セキュリティ運用・管理サービス」市場は中長期的に拡大傾向にある。2011 年度に引続き、2012 年度も全てのセグメントでプラス成長となり、1,000 億円を超える市場となった。2013 年度以降もプラス成長が継続すると予想される。

図 20 に 2012 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」が最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」は多様化していく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。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。特に、中小企業は社内で運用するよりコスト面、人材面からも社外のサービスを受ける傾向にあり、一括して委託できるメリットから今後ますます中小企業での「セキュリティ総合監視・運用支援サービス」の利用が増加していくものと考えられる。

図 20　2012 年度のセキュリティ運用・管理サービス市場



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「フィルタリングサービス」は、クラウド化による社内システムの外部サービス利用がさらに増加し、比較的外部委託しやすいことも加わり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、サイバー攻撃が身近なものとなり一番顕著に増加した。特に昨年以降 Web アプリケーションの脆弱性に関する関心が高まっており、既存のシステムにどのくらい脆弱性が残存しているのかといった現状のセキュリティ対策に対する不安や、IT ガバナンスの有効性確認の目的で「脆弱性検査サービス」を受けた企業が大幅に増加した。サイバーテロや政府の施策等のニュースを見て危機感が高まったことも増加理由の１つである。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検査することも一般化している。この面からも今後も「脆弱性検査サービス」の大幅な成長が予想される。

「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、昨今増加傾向にあるリスト型攻撃に対応するため、二要素認証を取り入れるWebシステムが増加し、今後もコンスタント

な増加が見込まれる。

「インシデント対応関連サービス」は、2011 年度顕著な伸びを示したが、2012 年度は期待に反して、それ程の伸びはなかった。企業における大規模インシデントが減少したことと、サービスメニューの多様化により安価なサービスも出てきたためだと思われる。しかしながら、2013 年度以降もサイバー攻撃は引続き発生すると思われるためこのセグメントの継続的な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、2012 年度の実績推定値が 1,032 億円であり、2011 年度の 984 億円と比較すると 4.8%の増加となった。1,000 億円を超えるカテゴリとしては、コンテンツセキュリティ対策製品市場、セキュアシステム構築サービス市場に次ぐ 3 つ目の市場となった。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る。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(億円)	2011 年度	2012 年度	2013 年度	2014 年度
セキュリティ総合監視･運用支援サービス	28,383	29,658	31,457	33,587
ファイアウォール監視･運用支援サービス	5,077	5,283	5,585	5,841
IDS／IPS 監視･運用支援サービス	6,692	6,919	7,258	7,547
ウイルス監視･ウイルス対策運用支援サービス	4,052	4,144	4,320	4,529
フィルタリングサービス	7,756	8,212	8,653	9,120
脆弱性検査サービス	12,303	13,346	14,143	14,949
セキュリティ情報提供サービス	1,838	1,897	1,938	1,994
電子認証サービス	23,675	24,700	25,848	26,727
インシデント対応関連サービス	5,109	5,342	5,685	6,127
その他の運用･管理サービス	3,532	3,689	3,860	3,976
合計	98,417	103,189	108,747	114,397
構成比				
セキュリティ総合監視･運用支援サービス	28.8%	28.7%	28.9%	29.4%
ファイアウォール監視･運用支援サービス	5.2%	5.1%	5.1%	5.1%
IDS／IPS 監視･運用支援サービス	6.8%	6.7%	6.7%	6.6%
ウイルス監視･ウイルス対策運用支援サービス	4.1%	4.0%	4.0%	4.0%
フィルタリングサービス	7.9%	8.0%	8.0%	8.0%
脆弱性検査サービス	12.5%	12.9%	13.0%	13.1%
セキュリティ情報提供サービス	1.9%	1.8%	1.8%	1.7%

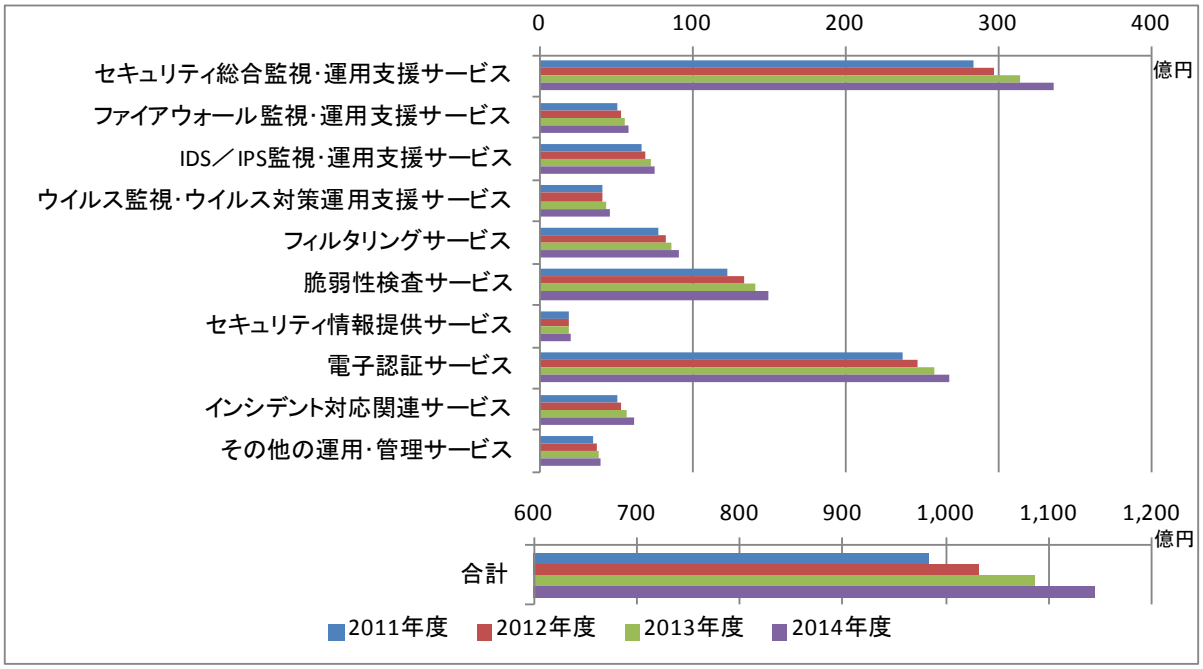
電子認証サービス	24.1%	23.9%	23.8%	23.4%
インシデント対応関連サービス	5.2%	5.2%	5.2%	5.4%
その他の運用･管理サービス	3.6%	3.6%	3.5%	3.5%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
セキュリティ総合監視･運用支援サービス	－	4.5%	6.1%	6.8%
ファイアウォール監視･運用支援サービス	－	4.0%	5.7%	4.6%
IDS／IPS 監視･運用支援サービス	－	3.4%	4.9%	4.0%
ウイルス監視･ウイルス対策運用支援サービス	－	2.3%	4.3%	4.8%
フィルタリングサービス	－	5.9%	5.4%	5.4%
脆弱性検査サービス	－	8.5%	6.0%	5.7%
セキュリティ情報提供サービス	－	3.2%	2.2%	2.9%
電子認証サービス	－	4.3%	4.6%	3.4%
インシデント対応関連サービス	－	4.6%	6.4%	7.8%
その他の運用･管理サービス	－	4.4%	4.6%	3.0%
合計	－	4.8%	5.4%	5.2%

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、2012 年度の推定実績市場規模は 297 億円（前年度比成長率+4.5%）と、2011 年度の 284 億円から増加した。2013 年度もプラス成長を続け、 2014 年度には 336 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 2012 年度で各々53 億円（前年度比成長率+4.0%）、69 億円（同+3.4%）、41 億円（同+2.3%）とプラス成長となり、2013 年度も継続してそれぞれ 56 億円（同+5.7%）、73 億円（同+4.9%）、43 億円（同+4.3%）とプラス成長を続け、2014 年度にはそれぞれ 58 億円（同+4.6%）、75 億円（同+4.0%）、45 億円（同+4.8%）と、同様に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、2012 年度に 82 億円（同+5.9%）と大幅なプラス成長を遂げた。2013 年度には 87 億円（同+5.4%）、2014 年度には 91 億円（同+5.4%）と大幅なプラス成長が継続して見込まれる。

図 21　国内セキュリティ運用・管理サービス市場推移



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、大幅な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。2012年度においては 133 億円（同+8.5%）、2013 年度には 141 億円（同+6.0%）、2014 年度には 149 億円（同+5.7%）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、2012 年度で 19 億円（同+3.2%）と安定した市場である。2013 年度、2014 年度も金額では 19～20 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」の中では、「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 2012 年度は 247 億円（同+4.3%）と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、二要素認証を採用する Web サービス企業が増加傾向にある点があげられる。2013 年度は 258 億円（同+4.6%）、2014 年度は 267 億円（同+3.4%）とコンスタントに増加する見込みとなっている。

「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。サイバー攻撃の影響で 2011 年度は最大の伸び率を示したが、2012 年度は 1 年経過し伸び率は比較的落ち着き 53 億円（同+4.6%）となった。2013 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、2013 年度は同+6.4%で 57 億円となり、2014 年度には 7.8%伸びて 61 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

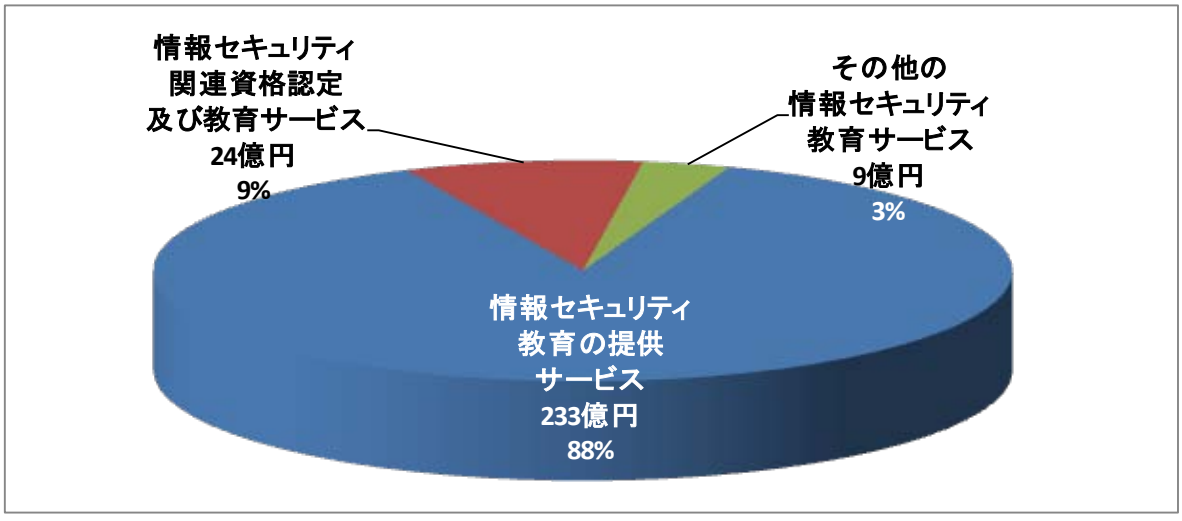
図22に2012年度の情報セキュリティ教育市場のセグメント別分布を示す。

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。経済環境が厳しい状況下では、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が講じられる。その中で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。2012 年度以降、経済活動が回復基調であることも支えになっ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。①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。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。②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。③経営層や上級管理職に対しての教育。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に対する需要を形成している。

①の教育では、e - ラーニングの活用が、大企業を中心として一般化してきている。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、管理者が受講状況と効果を社員一人ごと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、受講者の空き時間を有効活用できる面からも費用対効果の高さが評価されている。また、SaaS 型サービスも提供されるようになってきており、e - ラーニングサービスの活用が容易になることから、中堅・中小企業においても利用が拡大する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。

図 22　2012 年度の情報セキュリティ教育市場



「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、上記②のための教育や、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」を活用するニーズが強くなってきている。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事例が増加している。また、人材採用に際して資格保有を必須または優遇条件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。

③については、情報システム部門や情報セキュリティ管理責任者にとって、経営者の理解をいかに得られるかは、予算や人材の確保のために重要な課題である。近年は情報セキュリィに対する社会的認知も進み、脅威や事故の報道も盛んなことから、状況は改善されつつあるが、費用対効果をどう測り、どう見せるかは引き続き難問である。この分野では経営コンサルティングや会計監査の提供企業もサービスを提供している。

(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

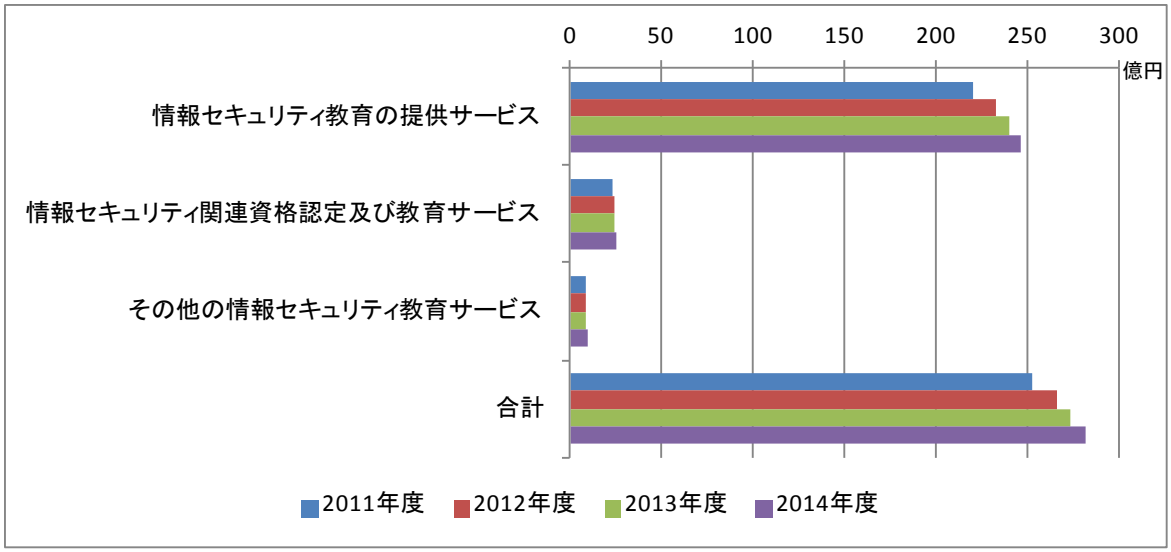
市場規模（百万円）	2011 年度	2012 年度	2013 年度	2014 年度
情報セキュリティ教育の提供サービス	22,059	23,309	24,041	24,675
情報セキュリティ関連資格認定及び教育サービス	2,327	2,387	2,449	2,553
その他の情報セキュリティ教育サービス	851	878	898	905
合計	25,237	26,574	27,387	28,132
構成比				
情報セキュリティ教育の提供サービス	87.4%	87.7%	87.8%	87.7%
情報セキュリティ関連資格認定及び教育サービス	9.2%	9.0%	8.9%	9.1%
その他の情報セキュリティ教育サービス	3.4%	3.3%	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	－	5.7%	3.1%	2.6%
情報セキュリティ関連資格認定及び教育サービス	－	2.6%	2.6%	4.2%
その他の情報セキュリティ教育サービス	－	3.2%	2.2%	0.8%
合計	－	5.3%	3.1%	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、2011 年度の市場規模は 252 億円程度と推測さる。2012 年度は標的型攻撃による被害の深刻化や、内部や外注先からの情報漏えい対策への注力が高まったことを反映して市場は拡大し、5.3%増の 266 億円となった。2013 年度も脅威はより一層深刻

度を増しており、伸び率は鈍ったものの拡大傾向は続き、3.1%成長して 274 億円程度になったものと推測される。2014 年度も同じ傾向が続くものと見られ、2.7%増で 281 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88%を占める「情報セキュリティ教育の提供サービス」である。ここには上記で触れた「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2011年度に221億円、2012年度には233億円（前年度比成長率+5.7%）、2013年度には240億円（同+3.1%）、2014年度は247億円弱（同+2.6%）と、順調に拡大すると予測される。

図 23　国内情報セキュリティ教育市場推移



「情報セキュリティ関連資格認定および教育サービス」は2011年度において23億円のマーケットであり、2012度には前年度比2.6%増の24億円の規模になったと推測される。2013年度もその傾向は続き同2.6%増の24億円、2014年度には同4.2%増の26億円と、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、更には景気の好転を背景にした個人の自分への投資といった要因から、拡大に向かうものと推測される。

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

子会社または大手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、更に製造業その他の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、また日本市場への外資系損保の商品投入も見受けられるようになってきている。さらには、東日本大震災を契機に事業継続計画や災害等不足の自体への備えの考え方･理解が急速に広まっており、これらの要因から、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。

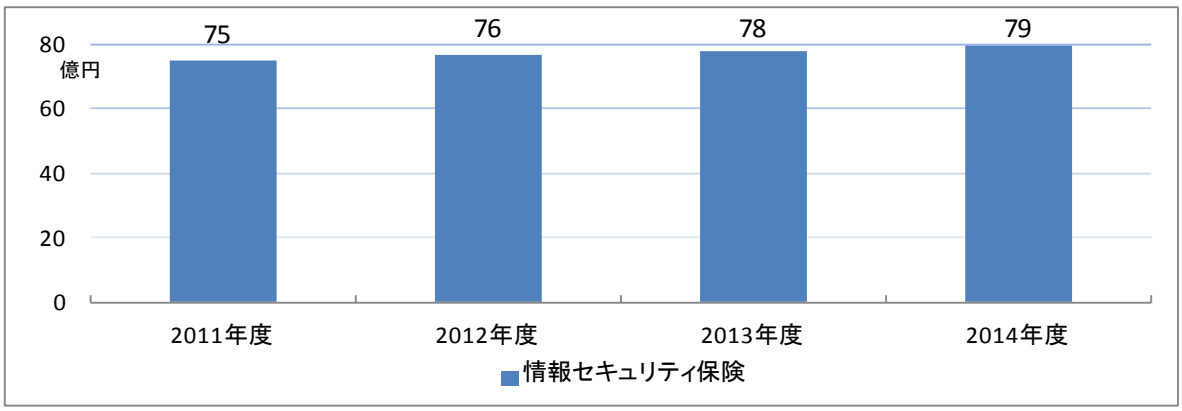
(2)市場規模とその推移

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）	2011 年度	2012 年度	2013 年度	2014 年度
情報セキュリティ保険	7,468	7,640	7,799	7,930
対前年比成長率（%）	－	2.3%	2.1%	1.7%

図 24　国内情報セキュリティ保険市場推移



「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が、2011 年度以降、やや拡大のペースが上がっていると見られる。2011 年度の市場規模は 75 億円程度に拡大したと見込まれ、その後も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しているものと考える。その結果2012年度は2.3%増の76億円、2013年度は2.1%増の78億円となり、2014年度は同じく1.7%増の79億円規模にまで拡大するものと予測した。

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. 2013 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、2014 年 3 月 17 日に「2014 年版 10 大脅威　～複雑化する情報セキュリティ　あなたが直面しているのは？～」[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

	2014 年	2013 年	2012 年
第 1 位	標的型メールを用いた組織へのスパイ・諜報活動	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）
第 2 位	不正ログイン・不正利用	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）
第 3 位	ウェブサイトの改ざん	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
第 4 位	ウェブサービスからのユーザ情報の漏えい	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
第 5 位	オンラインバンキングからの不正送金	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
第 6 位	悪意あるスマートフォンアプリ	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
第 7 位	SNS への軽率な情報公開	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）
第 8 位	紛失や設定不備による情報漏えい	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）
第 9 位	ウイルスを使った詐欺・恐喝	内部犯行	危ない！アカウントの使いまわしが被害を拡大！
第 10 位	サービス妨害	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）

（IPA 各年度発表をもとに JNSA 作成）

2013 年版の見出しは「身近に忍び寄る脅威」であり、2012 年版は「変化・増大する脅威」、2011 年版には「進化する攻撃」の文字が見える。2014 年版は上記のように「複雑化する情報セキュリティ」である。脅威が深刻化して身近に迫っており、ますます複雑化し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、まさに日常業務や日常生活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。

[10] http://www.ipa.go.jp/security/vuln/10threats2014.html

また、3 年間一貫して標的型攻撃が上位に位置づけられていることも注目すべきである。企業の内部ネットワークに潜入して情報を盗み出す攻撃は、その複雑で巧妙な手口から侵入防止は非常に困難で、被害の発見も容易ではないという問題があり、極めて深刻である。そしてこの攻撃が意味するものは明確な意図と目標を持って特定の対象を攻めてくる犯行である点である。企業の持つ営業秘密のみならず、国家安全保障や外交交渉など国益に関わる情報もターゲットとなっている。

「Webサイトに対する攻撃」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。更に、脆弱なWebサイトから、ID・パスワードのリストが盗み出され、それが他のアカウントへのなりすましログインに利用される手口が目立っている。不正送金や金銭の詐取など、実被害も深刻化しており、ネットの脅威が実生活の脅威にますます直結していることを物語っている。

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。2014 年版にも取り上げられている悪意あるアプリは、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をもたらす。さらに、BYOD 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が 8 位に位置付けられている。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。

これらに共通する「怖さ」は、知らないうちに入られ、情報をとられ、それによって金銭などの実被害が発生するという問題である。複雑化し巧妙化する攻撃側の前に、有効な防御手段は限られる。パスワードのこまめな変更、不要なアプリのダウンロードやインストールを避ける、不審なメール、特に添付ファイルに注意するといった、日常の意識の持ちようが重要である。と同時に、企業であれば内部ネットワークとサーバの監視を正しく行い、異常なトラフィックやアクセスを検知すること、そして重要なデータは暗号化の上保管・移動することがますます大事になっている。

こうした傾向を受けて、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。この流れは、IPA が「サイバー領域」という注目キーワードを示して指摘しているよ

[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

うに、防衛空間としてのサイバー空間という政府による位置付けが報道されることで、民間における「サイバー」の脅威とその対策の必要に対する認知となって浸透しつつある。これも情報セキュリティ製品・サービスに対する需要の底堅い動きを支える要因と考えることができる。

3.2. Internet of Thingsのセキュリティ

最近、メディアでもよく見聞きするようになったIoTは、Internet of Thing （モノのインターネット）の略語で、人手を介さない機器やサービスのインターネットを使った連携のことを言う。基本的には、以前からあったM2M（Machine to Machine）を包含する概念となっている。ここ数年、コンピュータ（PC、サーバ等）以外の機器のネットワーク接続が急拡大しており、その多くがインターネットを介しての通信機能を製品の付加価値とするものだ。

たとえば、家電製品はネットワークを使うことにより、相互に連携したり、様々な情報をインターネットとの間で交換することで、多くの新しい機能を獲得している。いわゆるスマート家電だ。世界的に見れば、既にこうしたスマート家電を統合するホームコントローラを介して、自宅の様々なモノをスマートフォンで監視、管理するような製品も市場に出始めている。

一方､たとえば自動販売機ネットワークは､商品管理や機器保守管理を大幅に効率化できるし、各種のセンサーネットワークは農業や、社会の安全、安心といった分野で重要度が増加しつつある。さらに、こうした考え方は現在実験が始まっているスマートグリッド、スマートシティなどの中核であり、また車載情報機器のネットワーク化から始まった自動車においても、今後は自動運転、ナビゲーションを含めたものに発展していくことになる。

(1) IoTの市場

こうしたIoT市場の今後については、様々な予測がある。矢野経済研究所が2014年3月に発表[12]したM2Mの世界市場予測では、2013年度に1兆4,580億円と見込まれるM2Mの世界市場が、2020年度には2倍以上の3兆8,100億円に達するとしている。国内市場規模は同調査によれば2013年度で1,350億円で、世界市場の9.3%を占める。2020年度には2,500億円に達すると予測している。

この予測は、他の調査に比べると、比較的慎重なものと見ることもできる。前提が多少異なる可能性はあるが、2013年11月に野村総研が発表したIT市場予測[13]においては、M2Mの市場規模は、2018年には国内市場のみで1兆1,704億円と、1兆円を超えるとみている。

このようにまだ大きな開きのある市場予測だが、これまでインターネットとは無縁だった様々な機器を含む市場となることを考えれば、大幅な伸びを見せることは間違いないだろう。

(2) IoTがもたらすリスク

様々なメリットを利用者にもたらすIoTだが、ネットワーク化されることで、それらが内包す

---

12 「M2M世界市場に関する調査結果 2014」（矢野経済研究所 2014年3月28日発表）https://www.yano.co.jp/press/pdf/1229.pdf

13 「2018年度までのIT主要市場の規模とトレンドを展望」（野村総合研究所2013年11月27日発表）http://www.nri.com/jp/news/2013/131127.html

るリスクも大きく増加する。基本的なリスクは、ベストエフォート型サービスであるインターネットに依存する機能の増加である。もし、インターネットやそれに関連した機器、設備（これは、利用者の側の機器も含む）に障害が発生した場合、そうした機能が停止もしくは大幅に損なわれる可能性である。

当然ながら、セキュリティ上のリスクも大きい。たとえば機器がネットワークを経由して攻撃されるリスクだ。かつて、組み込み機器のシステムは専用の OS などが使われていたが、最近、特にネットワーク接続されるようになって以降、こうした機能をサポートする汎用 OS、たとえば Linux や Windows の Embedded Edition などが使用されることが多くなった。当然、こうした汎用 OS などの脆弱性情報は広く流通するため、攻撃者にとっては情報源が大きく広がることになる。さらに、これらが利用者のネットワークを介してインターネットに接続されれば、インターネットを介しての攻撃の可能性も高まることになる。

もし、これらのデバイスが、利用者にインターネットを経由してのリモートアクセス機能を提供していれば、それを経由した攻撃の可能性も大きくなるだろう。また、直接、インターネットからアクセスできなかったとしても、たとえば PC に感染したマルウェアがこうしたデバイスを探索して攻撃する可能性もある。実際に、最近のパソコンやスマホの OS では、テレビなどの家電製品を探索して接続する機能が提供されているので、攻撃者もこれらの機能を利用できる。

同様のことは、インターネットに繋がれていないネットワークでも発生する可能性がある。とりわけ、管理用に PC やサーバが接続されているネットワークでは、なんらかの原因でこれらのコンピュータに感染したマルウェアが、デバイス側にも感染を広げる危険がある。一例を挙げるならば、2013 年 3 月に韓国で発生したマルウェア大量感染事件では、管理サーバに感染したマルウェアが、それに接続された銀行 ATM に広がり業務停止に陥った。

最近では、インターネットに接続されていない PC でも、更新プログラムやデータの取得のために、USB メモリなどのデバイスを使って外部の PC などとの間でデータ交換を必要とするケースが多い。また、メンテナンスなどのため、外部の PC が一時的に接続されるような場合もある。マルウェアがこれらを介して出入りする可能性が高くなっているのである。

さらに注意が必要なのは、こうしたデバイスの多くが、インターネットを経由して、メーカや管理会社のサービスを受けているという点である。たとえば、最近のスマート家電では、メーカのサービスサイトに頻繁に接続して、必要な情報を取得するだけでなく、様々なアプリケーションや、ファームウエアのダウンロードと更新も行っている。もし、こうしたサービスを提供する側に問題が発生すると、最悪の場合、すべてのデバイスが影響を受けることになる。とりわけ、こうしたサービスが攻撃を受けて侵入され、データを不正に改ざんされれば、最悪の場合、数万台～数十万台のデバイスが攻撃者の手中に落ちてしまう可能性もある。

想定しなくてはいけないのは、外部からの攻撃ばかりではない。内部者による不正行為は、より致命的だ。ファームウエアやアプリケーションの製造、検査過程におけるバックドアの導入や、サーバ管理者による不正行為などは、すべての利用者を危険にさらしかねない。このようなサービスの運用においては、通常の Web サイトなどに比べれば数段高いセキュリティレベルが求められることは間違いないだろう。

(3) セキュリティ市場としてみた IoT

様々なセキュリティ対策が必要な IoT だが、セキュリティ市場として見ると、その多くが既存の市場に包含されそうだ。と言うのも、デバイス側はメーカに閉じた世界であり、セキュリティ対策の責任は一義的に製造者にある。利用者が自分の必要でソフトウェアを導入して機能を追加できる PC やスマホなどの汎用デバイスとは異なり、ユーザに自由度が無いため、これ自体は付加的な市場を生むことはないだろう。一方で、こうしたデバイスが接続されるネットワークやサービスについては、これまで行われてきたようなセキュリティ対策が必要となるが、今のところ新しい切り口が必要になる様子も見えない。

もちろん、セキュリティ対策そのものの重要性は、そのリスクの大きさから見て、これまで以上に高くなることは間違いないが、それらは、後付けではなく、設計段階から検討され、実装されるべきものである。強いて言えば、IoT に参入するすべての業界に、こうしたことができる人材が必要となり、そうなると、セキュリティの設計、実装ができる組み込みシステム開発者が大量に不足する可能性が出てくる。また、メーカがインターネットを経由してこれらのデバイスに提供するサービスについては、重要インフラ並のセキュリティ対策が必要になるが、メーカ自身が、こうした部分を自社でカバーする（そのためにネットワークセキュリティに高い能力を持った人材の確保が必要となる）のか、アウトソースするのかによって、必要になるリソースも異なってくるだろう。

IoT は主にコンシューマを対象としているように見えるが、一方で企業も無縁ではいられない。実際、家電製品をはじめ、多くのコンシューマ向け機器が企業でも使われている。企業内ネットワークに、こうした異質なものが入り込むことは、新たなリスクを生み出すかもしれない。繋がないのが最も良い選択肢である時間はそれほど長くないだろう。やがて、こうした機器の機能の多くがインターネットやネットワーク接続と密接に結びついてしまうだろうからだ。

IoT デバイスの多くが、ユーザにとってブラックボックスである以上、そのリスクを評価することすらできない可能性もある。こうした企業ユーザに対してメーカがどの程度、仕様を開示できるのか、あるいは、企業自身がこうしたデバイスのネットワークにおける振る舞いを可視化して評価できるのか、しばらくは試行錯誤が続く可能性が高い。

Internet of Things の普及がもたらす、このようなセキュリティ面の課題にも注目し、共通認識の形成に向けて取り組んでいく必要があるだろう。

【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。「2013 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) 2011 年度国内情報セキュリティ市場規模　推定実績値
(2) 2012 年度国内情報セキュリティ市場規模　推定実績値
(3) 2013 年度国内情報セキュリティ市場規模　実績見込値
(4) 2014 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 2012 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、2011 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) 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。

(2) 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。

(3) サンプリング調査

今年度はアンケート調査の実施は見送った。アンケート調査により得られるデータを補強するために、従来から行っている方法を踏襲して、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 470 社（JNSA 会員企業約 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。(2)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、情報セキュリティ市場の拡大に伴い、国内のソフトウェア企業を中心に新規参入が増加しており、今回調査対象は前回に比べて 100 社ほど増加している。

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 2012 年度である。2013 年度、2014 年度の市場規模推定にあたっては、2012 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、表 18 に示す市場分類に対する詳細な説明は、2012 年度版から別冊として提供している。本報告書が大部になることを避ける意味と、市場区分定義の冊子が、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、独立して活用される可能性を視野に入れて、そのような措置とした。なお、2013 年度は、市場区分定義の見直し・改訂は必要ないとの結論に至ったので、別冊である市場区分定義の解説書も 2012 年度版のまま改訂しないこととした。必要があれば、昨年度版[14]を参照していただきたい。

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

[14] http://www.jnsa.org/result/2013/surv_mrk/2012fymarketresearchreport_apx.pdf

	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	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。

	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。	脆弱性検査製品	検査対象となるサーバ等に対し、スキャニングや擬似攻撃を行い、脆弱性や設定の不備等、危険事項を検査し報告する製品群。いわゆる脆弱性スキャナー（ネットワークベース、ホストベース）。
		ポリシー管理・設定管理・動作監視制御製品	1. OSやアプリケーションの設定、パッチ適用、バージョン等を監視・管理する製品群。 2. クライアントマシン等におけるファイルのコピー・印刷その他の操作を監視・制限・制御等する製品群。 3. クライアントPC等の識別情報やインベントリ情報等を収集・分析・管理し、ポリシー等の設定された条件に合致しないアプリケーション等のインストール等の管理（警告・報告・禁止・削除等）を行う製品・システム。 4. その他個別のマシンの設定、状態、動作等に着目してセキュリティを管理する製品群。 5. クライアントPC等の識別情報やインベントリ情報等に基づきネットワーク接続を管理・制御する製品・システム。いわゆる「ネットワーク検疫システム」における機器認証サーバを含む。原則として単体製品またはネットワーク制御装置等のオプションとして取引対象となる製品形態のものを対象とし、その機能がルータ等の一部にデフォルトとして組み込まれている場合は対象外とする。
		その他のシステムセキュリティ管理製品	コンピュータネットワークシステムの、システムとしての状態を監視・解析・管理する機能を持った製品群のうち、上記セグメントのいずれにも分類されない製品群。 主としてセキュリティ、内部統制管理（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	情報セキュリティポリシーおよび情報セキュリテ	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。

	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。	ィ管理全般のコンサルテーション	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	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。

	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。	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[15]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

[15] 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（いわゆるディストリビュータ）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。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定着したと言える。内部統制体制構築段階での支援がセキュリティコンサルティングとして提供され、以降、内部統制監査の一環、あるいは関連サービスとしてのコンサルティングが提供されている。

更に、標的型攻撃等で情報セキュリティリスクが経営リスクの重要要素であるとの認識も広まっており、経営リスク対策としての情報セキュリティ対策との位置づけでコンサルティングを導入する事例が増加していると見られる。

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り合わせて、専業に近い業態で事業展開している。従い、企業規模は小さいケースが多い。

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

標的型攻撃やサイバーテロリズムの被害が顕在化し、頻発することに伴って、対策や防止策の実施のためには専門事業者によるサービスの活用不可欠であるとの理解も浸透してきており、サービス提供事業への参入も徐々に増えていると見られる。

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」「システムセキュリティ管理製品」「ネットワーク脅威対策製品」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」「情報セキュリティコンサルテーション」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。

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）	**470**	79	***97***	56	*87*	28	24	73	26
有効推計対象	**422**	73	***88***	52	*80*	26	21	62	20
情報セキュリティツール全体（X）	**318**	68	***77***	49	*69*	22	5	19	9
統合型アプライアンス	***78***	11	7	*16*	***21***	12	3	6	2
ネットワーク脅威対策製品	***152***	*32*	17	29	***40***	17	3	11	3
コンテンツセキュリティ対策製品	***183***	33	*41*	33	***43***	16	3	10	4
アイデンティティ･アクセス管理製品	***149***	19	23	*27*	***48***	18	3	9	2
システムセキュリティ管理製品	***159***	27	*36*	26	***37***	16	4	11	2
暗号製品	***89***	17	11	*19*	***23***	11	2	3	3
情報セキュリティサービス全体（Y）	**272**	30	40	23	***59***	26	21	*58*	15
情報セキュリティコンサルテーション	***148***	12	11	11	*33*	18	18	***42***	3
セキュアシステム構築サービス	***136***	16	13	13	***40***	25	7	*21*	1
セキュリティ運用･管理サービス	***181***	26	27	19	***38***	19	11	*33*	8
情報セキュリティ教育	***77***	7	7	6	*14*	8	6	***26***	3
情報セキュリティ保険	***17***	1	0	2	1	2	2	*4*	***5***
（参考）									
ツール専業（X∩^Y）	**150**	*43*	***48***	29	21	0	0	4	5
ツール･サービス兼業（X∩Y）	**168**	25	*29*	20	***48***	22	5	15	4
サービス専業（^X∩Y）	**104**	5	11	3	11	4	*16*	***43***	11
生データベースの売上高分布	100.0%	20.7%	7.5%	11.3%	22.9%	25.6%	2.5%	7.0%	2.5%

また、今回調査対象企業数（有効推計対象ベース）が 423 と、前回調査の 358 から大幅に増えた。国産のシステムハウスや再販売事業者を中心に、情報セキュリティに関する製品やサービス

を開発したり仕入れ販売する事業者が大幅に増加していることを反映している。このような参入事業者数の増加は、情報セキュリティ対策の必要性への認知が高まることで事業機会を見出す事業者が増加していることと、IT 分野で事業を営む上でセキュリティ対策を外すことができないという需要側の要請を反映したものと考えることができる。

その結果、ツールだけかサービスだけか両方を提供するかの区分別では、ツールだけでサービスは提供しない事業者が 150、サービスのみに特化する事業者が 104、両方を提供する事業者が 168 と、すべての業態で参入事業者数が大幅に増加している。

前回調査に引き続き、トライアルとして、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届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、前回調査と同様に、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 88 と各業態の中で最も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 年代後半以降、リーマンショックの影響が世界を覆った 2008, 2009 年を除き、世界経済は堅調な拡大過程にあると見ることができる。アジアを中心とする新興経済の好調にアフリカ諸国のキャッチアップ等が加わってのものと考えられる。アメリカ経済も、世界全体の数字よりは低いものの、同様の推移を示しており、特に 2012 年の 2.8%は高い成長率と見ることができる。

表 20　GDP 実質成長率の推移

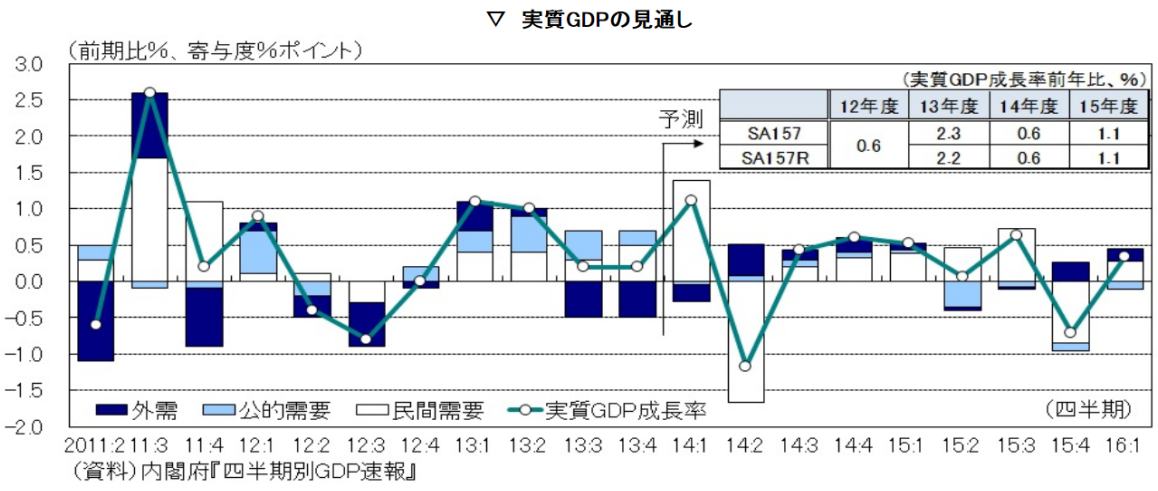
暦年	2005	2006	2007	2008	2009	2010	2011	2012	2013*
世界	3.5	4.1	4.0	1.5	-2.1	4.1	2.8	2.3	3.0
日本	1.3	1.7	2.2	-1.0	-5.5	4.7	-0.5	1.4	1.5
米国	3.1	2.7	1.8	-0.3	-2.8	2.5	1.8	2.8	1.9

（出典：総理府統計局 http://www.stat.go.jp/data/sekai/pdf/2014al.pdf#page=67 より JNSA 加工）

*　2013 年はIMF2014 年 4 月レポート[16]より

日本はリーマンショックによるダメージが、世界全体やアメリカ経済よりはっきり強く表れている。これに加えて 2010 年度末に襲った東日本大震災は、2011 年度のマイナス成長という結果につながっている。その後も 1%台半ばと経済のパフォーマンスは低迷を続けている。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、日銀による超金融緩和と財政出動により経済は明るい見通しを持つようになりつつあるように見える。

図 25　日本経済の短期予測



（日本経済研究センター第 157 回改訂短期経済予測　https://www.jcer.or.jp/research/short/detail4740.html）

[16] http://www.imf.org/external/datamapper/index.php

2014 年春闘では賃金改善にも一定の成果が見られ、消費税増税の影響も一時的で、インフレ脱却への期待も高まっている。情報セキュリティ市場にとっても、マクロ経済的には、リーマンショック以降では比較的好条件が揃いつつあるように見える。

図 25 は日本経済研究センターが 2014 年 3 月に発表した 4 半期予測である。消費税増税直前の駆け込み需要と直後の反動減が影響し、2013 年度の GDP は押し上げられる一方、2014 年度は低成長という予想となっている。しかし落ち込みは一時的であることも読み取れる。

(2)企業の経営環境と設備投資動向

今回の調査対象期間は、過去数年の調査に比べると、企業の経営環境としては、比較的順調な経緯であったと考えられる。表 21 に、野村証券の企業業績見通しレポートから、大企業の経常利益の前年度比増減率の推移を示す。2011 年度に東日本大震災やタイ大洪水による収益減少に見舞われているが、その程度は 2008 年度のリーマンショックに比較すれば軽く、2012 年度、2013 年度と回復している。2013 年度決算で過去最高益を更新した大企業のニュースも多く見かける。2014 年度についても、率は下がるものの増益傾向にあるとの予測になっている。

表 21　大企業経常利益増減率の推移

大企業の経常利益推移(前年度比増減%)						
2008 年度	2009 年度	2010 年度	2011 年度	2012 年度	2013 年度	2014 年度
−79.7%	97.3%	43.8%	−12.1%	12.8%	30.1%	9.1%

(出所:野村証券企業業績見通し 2013 年 12 月 3 日版 [17])

同様の傾向は、日本銀行が 4 半期ごとに行う短期経済観測調査（短観）でも見てとれる。同調査は、景況判断を示す DI 指標（Difusion Index）が特徴的である。2014 年 3 月調査によれば、表 22 に示すように、景況を「良い」と判断する企業の比率が「悪い」を大きく上回っており、それが 2014 年 3 月調査で 2013 年 12 月調査より改善している点が注目される。「先行き」については消費増税の影響で下がる中、中小企業においては持ち直している点も注目される。

表 22　企業の景況判断指数の推移

日銀短観　業況判断 DI　(「良い」ー「悪い」・%ポイント)						
調査時期	大企業		中堅企業		中小企業	
	最近	先行き	最近	先行き	最近	先行き
2013 年 12 月	18	16	9	7	3	0
2014 年 3 月	21	11	14	4	7	4

(出所:日本銀行　全国企業短期経済観測調査　2014 年 3 月調査 [18])

[17] http://www.nomuraholdings.com/jp/news/nr/nsc/20131203/20131203.pdf
[18] http://www.boj.or.jp/statistics/tk/gaiyo/2011/tka1403.pdf

設備投資については、一つの調査ですべてを見ることが困難だったので、日本政策投資銀行、政策金融公庫、日本銀行の各調査結果の抜粋を表 23 にまとめた。2013 年度の予測／見込みはいずれの調査でも高い伸び率を示している。2014 年度については政策投資銀行の 2013 年 6 月調査では大企業で大幅マイナスだが、2014 年 1 月のロイター企業調査[19]では「14 年度の設備投資計画について、現時点では前年度から横ばいとの回答が 60%と最も多い。現時点では翌年度について『まだ判断材料が乏しい』（サービス）といった状況も踏まえる必要がある。前年度より増額する計画の企業は全体の 23%となり、減少計画の 17%を上回り、全体として企業の投資マインドは前向きだ。」との結果となっており、日銀短観でもプラスを示すなど、上向き傾向にある。また日本経済新聞の記事[20]によれば、製造業の設備年齢が極めて高くなっており、税制等の誘導や企業収益の好調持続等の要因が加われば増額修正の可能性もある。またセキュリティ対策の主力となる全産業ソフトウェア投資が 2013 年度に 8.6%と効率の増加を示し、2014 年度も 0.9%とわずかながら増加を維持することも追い風と言えよう。

表 23　設備投資動向調査結果の概要

区分	調査主体	調査時期	2012 年度実績	2013 年度予測	2014 年度計画
大企業	政策投資銀行	2013 年 6 月	2.9%	10.3%	−10.0%
中小製造業	政策金融公庫	2013 年 9 月	16.9%	7.7%	−
全産業*1	日本銀行	2014 年 3 月	−	6.2	0.4
全産業*2			−	8.6	0.9
（*1 は金融機関を含む全産業のソフトウェアを含む全設備投資、*2 は同ソフトウェア投資）					
（出所：政策投資銀行設備投資調査 2013/8 月公表[21]、政策金融公庫中小製造業設備動向調査 2013 年 10 月公表[22]、日本銀行全国企業短期経済観測調査 2014 年 4 月公表[25]を基にJNSA作成）					

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[23]」の中で言及されている。これによれば、

[19] http://jp.reuters.com/article/topNews/idJPTYEA0M08K20140123
[20] 2014 年 5 月 5 日付・東京発行・14 版 P3
[21] http://www.dbj.jp/investigate/equip/national/pdf_all/201308_summary.pdf
[22] http://www.jfc.go.jp/n/findings/pdf/news251010b.pdf
[23] http://www.boj.or.jp/statistics/tk/gaiyo/2011/tka1403.pdf

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、3013 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。総務省が発行する情報通信白書は通信データ量について様々なデータを提供しているが、平成 25 年版 [24]では、インターネットトラフィックとビッグデータの流通量に関する推定値を載せている。表 24 には、それらのデータと、それを指数化した数値をまとめてみた。インターネットトラフィックは 2008 年を 1 とすると、4 年後の 2012 年には 2.03 と 2 倍になっている。ビッグデータは 2005 年から 2008 年の 3 年間で 2.44 倍、2008 年から 2012 年の 4 年間で 2.14 倍と、やはり 4 年で倍になるというペースで伸びている。ほぼこれに見合うサイクルでの能力増強投資が必要と考えられる。

表 24　平成 25 年版 情報通信白書　情報流通量の推移

	2005 年		2008 年	2009 年	2010 年	2011 年	2012 年
インターネット	－		939	1,206	1,363	1,696	1,905
トラフィック	－		1.00	1.28	1.45	1.81	2.03
（各年 11 月･Gbps）							
ビッグデータ	424,306		1,033,904	－	－	1,536,450	2,217,195
流通量	1.00		2.44	－	－	3.62	5.23
（産業計・TB）			1.00	－	－	1.49	2.14

（出所：総務省「情報通信白書平成 25 年版」より JNSA 加工・集計）

当ワーキンググループの過去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。また、同じく過去のヒアリングでは、2007 年ごろに通信事業者の設備投資サイクルの山があったとの指摘も聞いている。その延長で考えると、2011～2012 年度に次の山を迎えていたとも推測できる。今

[24] http://www.soumu.go.jp/johotsusintokei/whitepaper/h25.html

回調査では市場伸び率のピークは 2013 年度に出ているが、2011 年度が景気の谷間で少し後ろずれが起きたと考えれば、この考え方とも一致する。

(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）[25]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）[26]統計を加味し、本調査結果と比較したデータを表 25 に示す。

表 25　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		2011年度	2012年度	2013年度	2012/2011	2013/2012
		千台/億円	千台/億円	千台/億円	%	%
セキュリティ出荷計	金額	6,926	7,309	7,658	105.5%	104.8%
IT出荷計(JEITA)	金額	62,183	62,606		100.7%	
PC国産出荷	台数	11,277	11,152	12,109	98.9%	108.6%
	金額	8,669	7,952	9,263	91.7%	116.5%
メインフレーム、サーバ、WS 出荷	台数	418	407		97.5%	
	金額	3,762	3,779		100.5%	
ソフトウェア	金額	7,353	7,686		104.5%	
SI開発	金額	23,092	23,382		101.3%	
BPOその他サービス	金額	19,307	19,807		102.6%	
（SW,サービス計）	金額	49,752	50,875		102.3%	
ネットワーク機器						
生産	金額	5,176	5,454		105.4%	
輸入	金額	5,230	6,028		115.3%	
輸出	金額	1,527	1,351		88.4%	
国内出荷	金額	8,879	10,131		114.1%	
IT+NW装置	金額	71,062	72,737		102.4%	
セキュリティ市場の比率						
対IT出荷計(JEITA)		11.1%	11.7%			
対IT+NW装置		9.7%	10.0%			

（出典：JEITA、CIAJ の統計を元に JNSA 作成）

JEITA では、IT に関わる各種生産統計を行って公表している。その中から、情報セキュリティに関わるデータとして、「PC の国内出荷」「メインフレーム・サーバ・ワークステーションの国内出荷」「ソフトウェア・IT サービス・アウトソーシングその他のサービス」の 3 種類の統計をピックアップした。表 25 では、「IT 出荷計（JEITA)」の欄で、各々「PC 出荷」

25　一般社団法人電子情報技術産業協会　http://home.jeita.or.jp/
26　一般社団法人情報通信ネットワーク産業協会　www.ciaj.or.jp/

「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（国内生産＋輸入－輸出）も比較対象として掲出した。

表 25 に見られるように、2012 年度の IT 出荷は前年度比微増となった。ネットワーク機器は 14.1%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 8.3%の大幅マイナスだが台数ベースではマイナス 1.1%とほぼ横ばいである。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、2012 年度は前年度比 5.5%の増加となった。IT+ネットワーク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、2011 年度で 9.7%、2012 年度で 10.0%となった。前回調査では 2008 年度：8.9%、2009 年度：9.5%、2010 年度：9.3%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。ネットワーク上のセキュリティ脅威が益々深刻度を増し、その対策の必要度に対する認知が高まることにより、この比率が押し上げられてきていると考えることができる。

(3)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 2012 年版 [27]であり、対象年度は 2011 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 4 回の調査報告書から拾ってまとめたものが表 26 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を経て、東日本大震災の影響が顕著に出た 2011 年度までの期間となる。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。それが 2011 年度は情報処理関連支出が前年比 7%程度増加する一方で情報セキュリティ対策費用は 8.5%減少している。これは、回答企業平均で資本金規模が小さくなる一方年間事業収入規模が拡大するなど母集団の変化が影響しているとも考えられる。

また、情報処理関係支出に占める割合もこの 3 年間は 1.40%→1.68%→1.84%と上昇を見せ

[27] http://www.meti.go.jp/statistics/zyo/zyouhou/result-1.html （2013 年 11 月 1 日発表）

ていたが、2011 年度は 1.57%と落ち込んでいる。情報処理関連支出の対年間事業収入比率が、表 26 の期間一貫して低下していることとの対比では、異変が感じられる。東日本大震災の影響が表れた可能性がある。

表 26　情報処理実態調査母集団の比較（平成 21、22、23、24 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	情報処理関連支出	対年間事業収入比率	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	4,937	9,417	614	625	1.02%	1,050	1.68%
2010 年度	4,832	9,300	633	581	0.92%	1,070	1.84%
2011 年度	4,971	8,436	724	623	0.86%	979	1.57%

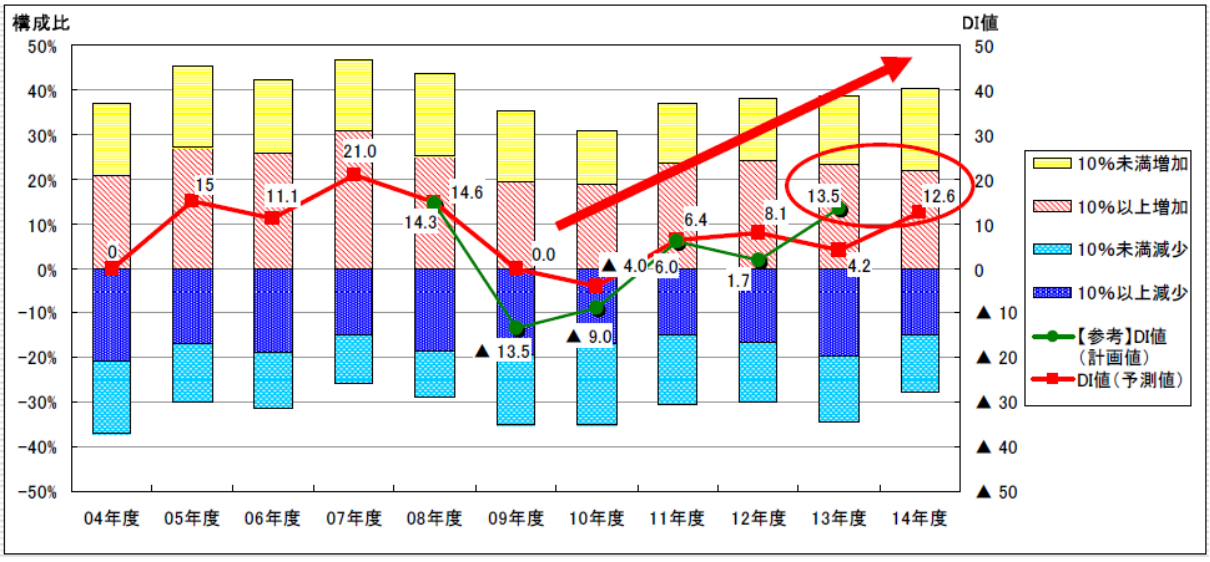
（出典：経済産業省平成 21，22，23，24 年度情報処理実態調査より JNSA 作成）

なお、上の表にある 1 社平均 979 万円という情報セキュリティ対策費用に回答企業数 4,971 を掛けると 4,867 億円となる。同調査の回答率は 52.3%となっており、調査対象企業全体では約 9,300 億円という試算値が得られる。本調査における 2011 年度の市場規模算定値は 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規模の費用が費やされていることは確実に言えるのではないかと考えられる。

(4)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。2013 年度調査結果の概要は 2014 年 4 月 9 日に公表[28]された。

図 26　IT 予算の増減の回答状況



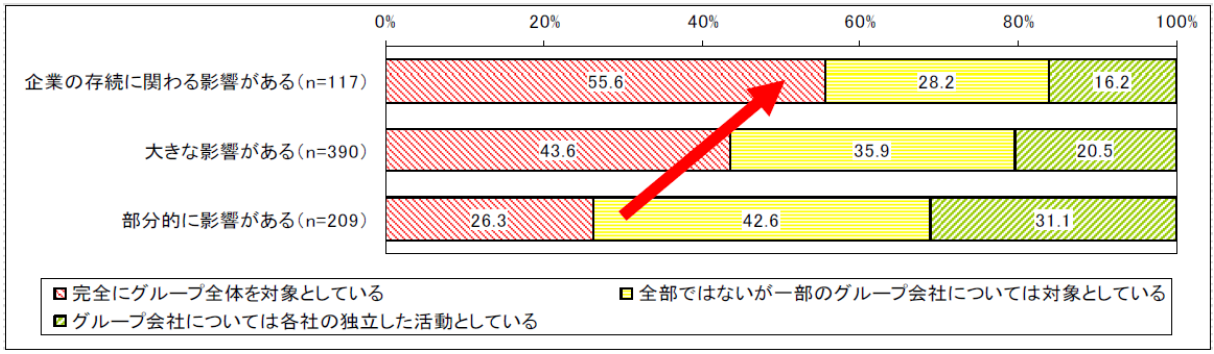
[28] http://www.juas.or.jp/servey/it14/#pr2

（出典：JUAS　企業 IT 動向調査 2014 報告プレスリリースより）

IT 支出の増減傾向を聞く定例の質問に対しては、図 26 のような回答分布となっている。IT 予算の増加と減少の差分を指数化したインデックス値を見ると、2011 年度 6.4、2012 年度 8.1、2013 年度 4.2、2014 年度（予測）12.6 となり、2013 年度の踊り場を挟んで増加傾向は続いていると見られる。特に 2014 年度は増加のモメントが大きいことが注目される。（なお、アンケート調査時点は 2013 年 10~11 月）

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。セキュリティ対策項目のうち、半数以上が「対策ができておらず不安」とした項目は「擬似的な標的型攻撃メールを従業員に送付して開封するか否かのテストの実施」「監査機関による社内ネットワークへの侵入テストによる脆弱性評価」「ソーシャルメディアポリシーの作成」の 3 件で、「情報セキュリティ対策を実行推進する人材の社内育成」がこれに次いだ。いずれも専門知識を持ったサービス事業者による支援を必要とする課題で、情報セキュリティサービスへの需要の潜在力を感じさせる調査結果と言える。

図 27　情報セキュリティ事故の影響度と企業グループでの取組状況



（出典：JUAS　企業 IT 動向調査 2014 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事故の影響度を、企業グループとしての情報セキュリティ対策の実施状況との組み合わせで統計処理した図 27 の分析である。情報セキュリティ事故は、全体の 16%が「企業の存続に関わる影響がある」とし、54%が「大きな影響がある」としている。そして重要度の評価が高い順にグループでの取組も進んでいるとの結果を示している。情報セキュリティが経営リスクレベルの管理対象であるとの認識が急速に広まっていることを示すデータとして興味深い。

7.3. 情報セキュリティに関わる外部環境変化

情報セキュリティに関する状況の変化は、この報告書で繰り返し触れている問題であるが、この 2 年ほどの間に、その深刻度は一段と高まっているように見える。今まで指摘したことも含めて改めて整理すると、主として以下の点があげられる。

(1) ネットワーク脅威の深刻化と複雑化

① マルウェア感染経路の多様化と深刻化

② 特に、水飲み場攻撃をはじめとする、Web サイトを悪用したマルウェアの送りこみ

③ 標的型攻撃の多発
④ 特に、精緻で巧妙なメールの手口や Web を感染経路に使うなど、「入り口」での完全防御が不可能なレベルになっていること
⑤ サイバーテロやサイバーウォーなど、組織力を背景とした攻撃手段の開発と実行
⑥ ソーシャルメディアやスマートデバイス

(2) 相次ぐ汎用ソフトウェアの脆弱性の発見

2014 年に入って一段と深刻になっているのが、無償で配布され、広い範囲で使われているソフトウェアに潜在していた不具合の発見報告である。多くが、悪用されることでコンピュータへの侵入や乗っ取りを許す、重大なセキュリティリスクをもたらす。従来から、Adobe 製品や Java や Internet Explorer での指摘があったが、2014 年に入ってから、OpenSSL、Struts、Internet Explorer など重篤で、かつ公開情報となった段階で解決策が用意されていない、いわゆるゼロデイ脆弱性の指摘が相次ぎ、ネットワーク利用の基盤的部分での信頼を損なう事態が頻発している。

(3) 情報漏えい事件の深刻化

① 標的型攻撃などで内部ネットワークへの侵入を許した場合、企業に深刻な影響を与えかねない重要情報を、知らない間に盗まれ、悪用されるリスクがかつてなく高まっている。
② 元従業員や委託先の社員など、内部者による情報の持ち出し、悪用、売り渡しの事件が多く発覚し、企業の情報防衛に深刻な課題を突き付けている。
③ 職業的ハッカーと想定される攻撃者により、銀行取引関係の情報が窃取され、不正送金など金銭被害が頻発している。
④ EC サイト等からのカード情報の盗み出しと悪用が後を絶たない。

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 年以降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、情報セキュリティ対策費用の支出拡大や、情報セキュリティ対策要員の配置、育成など、対策に対する姿勢も積極化している。

また、法制度・政策対応の面でも、ウイルス作成罪の創設、不正アクセス禁止法の強化（ID やパスワードを盗み出す行為の可罰化）、電磁的記録の証拠収集の制約緩和等の措置が取られるとともに、対策を担う情報セキュリティ人材の育成対策の実施など、より積極的な対応を行う動きが見られる。

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、精度の高い加工や品質を作り込む生産管理のノウハウである。iPS 細胞のように製造業以外でも世界をリードする日本の知的価値は拡大している。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、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。専門家の知識・経験・ノウハウによる支援が必須のセキュリティ対策項目の必要度の認知も、上に見たように高まっている。

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。また、情報セキュリティ対策の必要に対する認知の浸透とともに、需要は伸びているが、特に専門人材の供給が追い付いていない状態である。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。市場の拡大とともに新規参入も増えつつあるが、増大する需要に質量とも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
.2014 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

2014 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

木城　武康　　株式会社日立システムズ

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　※
福岡　かよ子　株式会社インテック　※
佐々木　謙一　株式会社インテリジェントウェイブ
栗田　亮子　　NTT ソフトウェア株式会社
勝見　勉　　株式会社情報経済研究所　※
佐藤　克彦　　三菱電機インフォメーションシステムズ株式会社　※
安武　千尋　　株式会社ユービーセキュア
土屋　日路親　サブスクライバー　※
蜂巣　悌史　　サブスクライバー　※

トピック執筆者（ワーキンググループメンバ外）

二木　真明　　アルテア・セキュリティ・コンサルティング

以上