2014 年度

情報セキュリティ市場調査報告書

V1.01

２０１５年６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。2014 年度調査では、従来方式を一部簡略化し、個別推計調査、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、2015 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 年度の大企業のハッキング被害や標的型攻撃による被害、衆参両議院における不正侵入や情報流出、2012 年度の遠隔操作マルウェアによる脅迫に関する誤認逮捕事件など、情報セキュリティがしばしば報道で取り上げられ、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。2014 年度に入ると、大企業の内部犯行やマルウェア感染による大規模個人情報漏えいが相次ぎ、内部統制が再び脚光を浴びるようになってきた。

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、多額の予算をサイバー防衛体制整備に割り当てるところまで取り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。

2015 年 1 月には、前年に可決成立したサイバーセキュリティ基本法に基づき、サイバーセキュリティ戦略本部が設置され、各省庁に強い権限を持ち、行政機関や重要インフラのセキュリティを強力に推し進める体制が整った。

更に金融庁の監査マニュアル改定では、CSIRT 組織の設置を明記し、企業は、今後更にサイバーセキュリティの確保が求められることになるだろう。

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、意図しない誤用やミスを防

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、目的に適合するよう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・取り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。

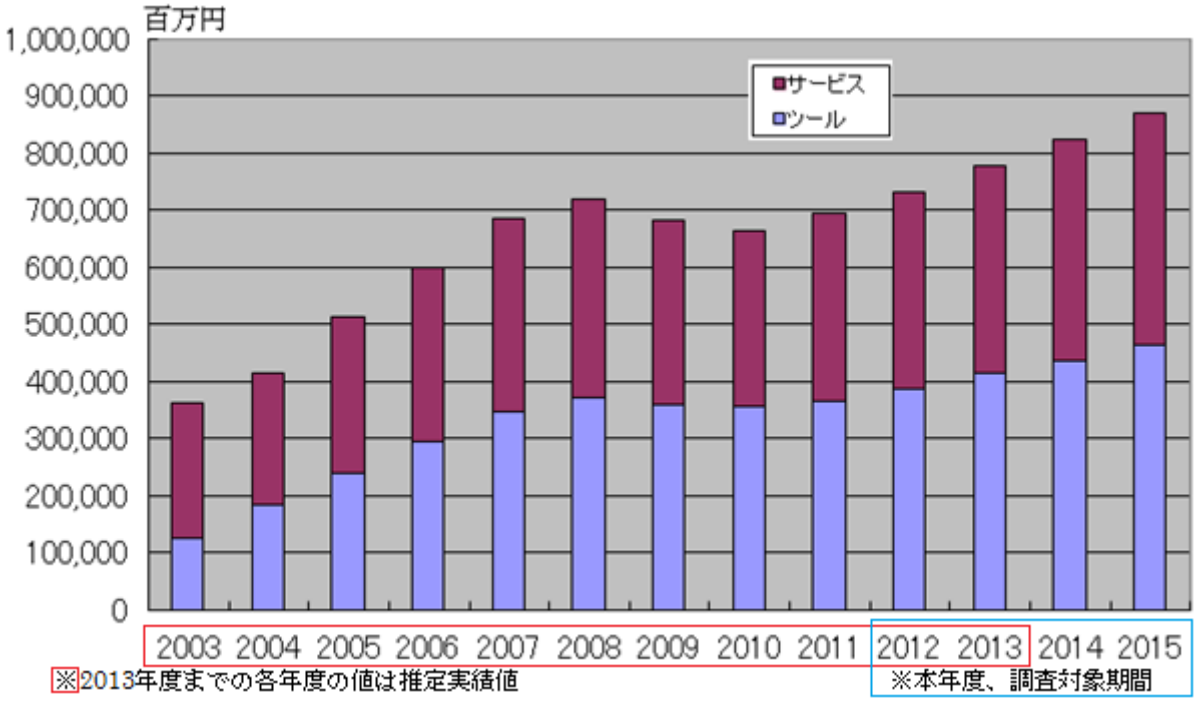
※本調査では、情報セキュリティ市場を大きく「ツール」と「サービス」に分け、各々を大分類市場、中分類市場に体系的に区分している。以下の報告の中では、大分類市場区分を「カテゴリ」、中分類市場区分を「セグメント」と呼ぶ場合がある。

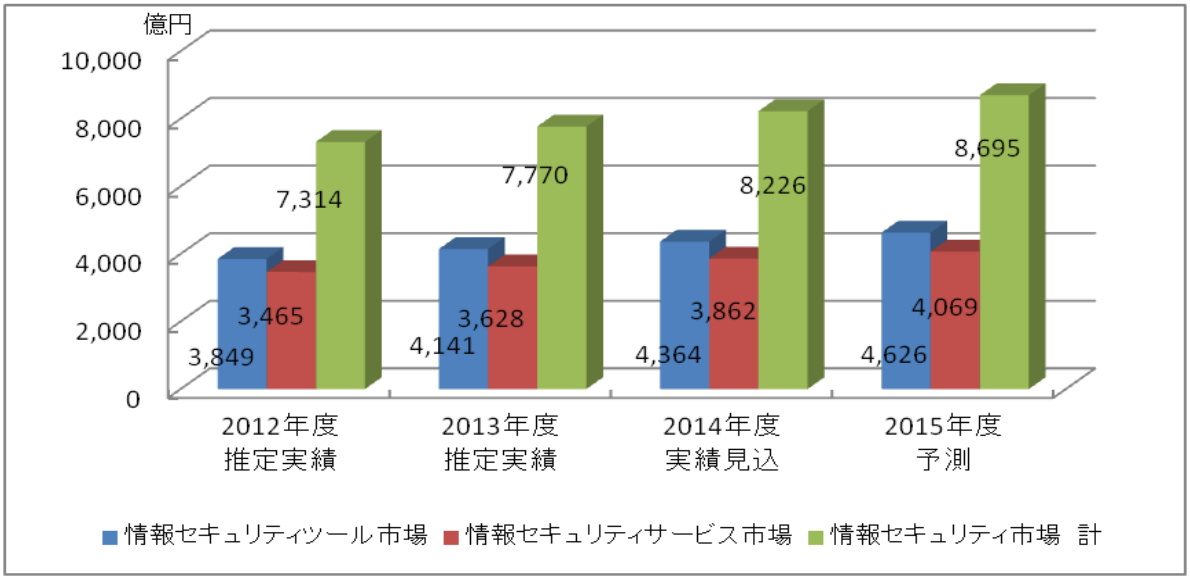
【第一部　情報セキュリティ市場調査結果】

第１章 国内情報セキュリティ市場の実態概要

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。

図 1　国内情報セキュリティ市場規模　経年推移





日本国内の情報セキュリティ市場規模を調査開始して以降の市場規模推計の経年推移は、図１に示すとおり、今回調査の基準年度である 2013 年度は、前年度にリーマンショック前の水準に

並び、いよいよ過去最高を毎年更新する上昇基調に乗った最初の年と考えられ、市場規模総額は7,770億円に達したと推定する。

2013年度を振り返ると、日本経済の立て直しが進行する中、インターネットを使った選挙運動を解禁する改正公職選挙法、米国家安全保障局（NSA）が 一日数百万件の電話記録を盗聴していると報道された所謂スノーデン事件（別名PRISM問題[1]）、JR東日本のSuica履歴情報提供問題など、個人情報とプライバシー保護といった情報管理の問題がクローズアップされた年であった。また一般には、WindowsXPサポート終了に対する備え、SNS投稿による社会的制裁（この年の流行語大賞にノミネートされた「バカッター」に代表される若年層のネットリテラシー問題）、ネットバンキングによる不正送金問題などが取りざたされ、セキュリティ対策の重要性に対する社会的認知がまた更に一歩進んだ年と位置付けることができる。

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）

2014年度市場調査　年度別総計表	2011年度		2012年度			2013年度			2014年度			2015年度		
	売上実績推定値		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	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%	21,449	5.2%	6.6%	22,649	5.2%	5.6%	24,007	5.2%	6.0%
ネットワーク脅威対策製品	49,924	13.7%	52,112	13.5%	4.4%	54,482	13.2%	4.5%	60,124	13.8%	10.4%	63,731	13.2%	6.0%
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%	158,234	38.2%	7.6%	164,537	37.7%	4.0%	174,409	38.2%	6.0%
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%	73,727	17.8%	7.1%	77,027	17.7%	4.5%	81,649	17.5%	6.0%
システムセキュリティ管理製品	51,747	14.2%	55,108	14.3%	6.5%	60,468	14.6%	9.7%	63,268	14.5%	4.6%	67,064	14.7%	6.0%
暗号化製品	39,838	10.9%	41,693	10.8%	4.7%	45,779	11.1%	9.8%	48,779	11.2%	6.6%	51,706	11.1%	6.0%
セキュリティツール製品	365,562	52.7%	384,907	52.6%	5.3%	414,139	53.3%	7.6%	436,383	53.1%	5.4%	462,566	53.2%	6.0%
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%	72,731	20.0%	3.7%	76,331	19.8%	4.9%	80,147	19.9%	5.0%
セキュアシステム構築サービス	129,395	39.4%	138,889	40.1%	7.3%	144,875	39.9%	4.3%	151,375	39.2%	4.5%	158,944	39.8%	5.0%
セキュリティ運用・管理サービス	98,417	30.0%	103,189	29.8%	4.8%	109,379	30.1%	6.0%	120,607	31.2%	10.3%	127,843	30.7%	6.0%
情報セキュリティ教育	25,237	7.7%	26,574	7.7%	5.3%	26,979	7.4%	1.5%	27,979	7.2%	3.7%	29,378	7.5%	5.0%
情報セキュリティ保険	7,468	2.3%	7,640	2.2%	2.3%	8,885	2.4%	16.3%	9,885	2.6%	11.3%	10,577	2.1%	7.0%
情報セキュリティサービス	328,475	47.3%	346,457	47.4%	5.5%	362,849	46.7%	4.7%	386,176	46.9%	6.4%	406,889	46.8%	5.4%
セキュリティツール＋サービス	694,036		731,364		5.4%	776,988		6.2%	822,560		5.9%	869,455		5.7%

表1は、今回の国内情報セキュリティ市場規模の実績と予測をしめした結果であるが、2013年度の情報セキュリティ市場はツール市場が4,141億円、サービス市場が3,628億円、合計7,770億円に達したものと推定する。

また、2014年度はネットワーク脅威製品(ツール)や、セキュリティ運用・管理サービス、保険（サービス）が顕著に伸びる中、全体で5.9%成長し8,226億円と初めて8,000億円の大台を突破すると予測する。

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。2015年度には9,000 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

[1] 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

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。

尚、2015 年度の市場規模予測は、セキュリティ市場を取り巻く経済環境の不透明感から
（1）ツール：　一律 6.0%　　（2）サービス：　一律 5.0%　　で予測した。
ただし、サービスの中で「セキュリティ運用・管理サービス」、「セキュリティ保険」に関しては、伸びが著しく、おのおの 6.0%、7.0%としている。

マイナンバーや消費税対応に追われる企業としては、純粋なセキュリティ投資を控える動きがあるものの、個人消費を中心にセキュリティ対策の必要性が周知されつつあり、市場全体としては 2014 年度ほどの伸びは期待できないが堅調であると予測した。

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、2013 年度の国内「情報セキュリティツール」市場は、4,141 億円の規模であったと推測される。2008 年度下半期に発生したリーマンショックにより一旦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 3～5%程度の成長を続け、その後の経済の回復や高まるサイバー脅威への対応を背景に拡大基調が持続、2013 年度の情報セキュリティツール市場の伸びは 7.6%という高い伸びを示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	2012年度		2013年度			2014年度			2015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	20,120	5.2%	21,449	5.2%	6.6%	22,649	5.2%	5.6%	24,007	5.2%	6.0%
ネットワーク脅威対策製品	52,112	13.5%	54,482	13.2%	4.5%	60,124	13.8%	10.4%	63,731	13.2%	6.0%
コンテンツセキュリティ対策製品	147,028	38.2%	158,234	38.2%	7.6%	164,537	37.7%	4.0%	174,409	38.2%	6.0%
アイデンティティ・アクセス管理製品	68,846	17.9%	73,727	17.8%	7.1%	77,027	17.7%	4.5%	81,649	17.5%	6.0%
システムセキュリティ管理製品	55,108	14.3%	60,468	14.6%	9.7%	63,268	14.5%	4.6%	67,064	14.7%	6.0%
暗号化製品	41,693	10.8%	45,779	11.1%	9.8%	48,779	11.2%	6.6%	51,706	11.1%	6.0%
セキュリティツール市場合計	384,907	100.0%	414,139	100.0%	7.6%	436,383	100.0%	5.4%	462,566	100.0%	6.0%

図 2 に 2013 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 2013 年度の市場規模は 1,582 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 737 億円、構成比で 17.8%であった。第 3 位は「システムセキュリティ管理製品」が 605 億円で 14.6%を占めた。続いて、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545 億円・13.2%、214 億円・5.2%で、合計すると 759 億円・18.4%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 458 億円・11.1%となった。

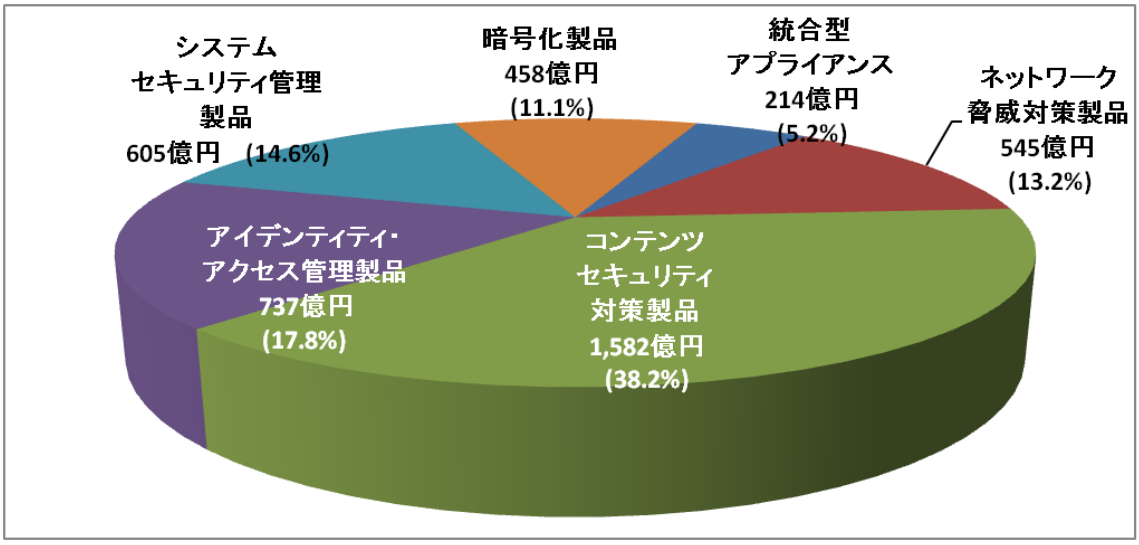
このところ数年のすう勢として、以下のことが観測される。

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、更にスマートデバイス普及に伴うユーザニーズやアプリの多様化に伴い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、脅威の複雑化に伴い大規模システムでは導入が限定的となり、専門管理者を配置しにくい中小規模において単価が比較的安く、数の出る製品の普及、買い替え需要も数年サイクルであることから、金額ベースでの著しい伸びは無いが安定した市場となっている。

図 2　2013 年度の国内情報セキュリティツール市場



3) 「アイデンティティ・アクセス管理製品」では、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。

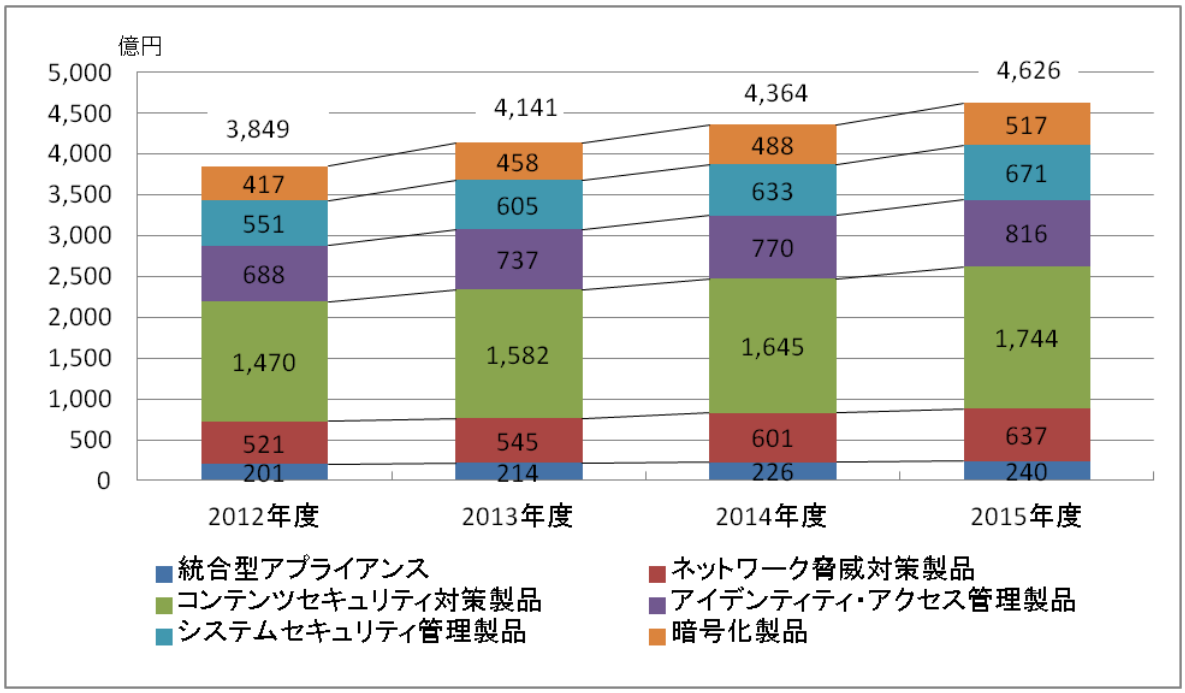
4) 標的型攻撃等、内部ネットワークへの侵入防止が困難となってきた今日の情勢を踏まえ、内部ネットワークの監視や解析、診断を行う「システムセキュリティ管理製品」も伸び率を高めている。このカテゴリには他に、端末のインベントリ・パッチ適用状態・設定等のコンプライアンス状態等を管理する製品やネットワーク検疫製品、さらにはセキュリティ目的のログ解析製品等、内部統制・情報漏えい・標的型攻撃への対応で需要が高まった製品が多く含まれ、高い伸び率を支えていると見られる。

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。
情報セキュリティツール市場は、経済回復の兆しに伴い 2012 年度までの投資抑制への反動と、

大規模な情報漏えい被害（1 億人分の個人情報がハッキングされたとの報道）や相次ぐ標的型攻撃被害に対する防衛産業の投資、企業による脅威対策が急がれた結果、7.6%という高い成長を遂げたものと見られる。これは前年調査（2012 年度市場規模の 2011 年度比 5.3%）に対して、約 1.5 倍にあたる。

図 3　国内情報セキュリティツール市場推移



2013 年度に最も高い伸び率を示したカテゴリ（大分類市場）は「暗号化製品」で 9.8%の伸び率であった。前述のとおり、相次ぐ情報漏えい事件事故に対して、ファイルそのものを暗号化する事で漏れ出た場合もデータを保護する需要、アイデンティティ・アクセス管理を実行する際の認証技術に対する暗号化の需要など、根本的な対策に目を向けるユーザやセキュリティ製品開発者、システム設計 SE 等が増えてきたことを物語る。次に高い伸びを示したのが、「システムセキュリティ管理製品」の 9.7%で、前年調査において、「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た結果と理解される。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。」とした部分がそのまま、伸び率の第 1 位と第 2 位に上がってきた様相である。3 番目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 7.6%であった。ツール市場全体の 38.2%を占めるため、この伸び率がそのままツール全体の伸びにつながっている。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 7.1%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」は 4.5%とツール市場全体としての伸び率に比べ低かったが、これはここ数年脅威の高度化により、事件事故が起きるエンドポイントでの対策や、起きた後の対策に投資の中心が移行しているためと考えられる。その一方で、「統合型アプライアンス」は 6.6%と前年 4.6%に対して伸びが上回った。

これは、アプライアンス製品が、脅威の複雑化に伴い、大規模システムでは導入が限定的となる一方で、専門管理者を配置しにくい中小ユーザにおいて需要が活性化し、単価の比較的低い製品が数量的に増加したためと考えられる。

2014 年度に入ると、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る一方、2012 年度から 2013 年度にかけて起こった経費抑制に対する反動や、消費増税前の駆け込み需要等による伸びはなくなり、ツール市場は 4,364 億円と、2013 年度比伸び率 5.4%に落ち着くと考えられる。

2015 年度は、スマートデバイスやビッグデータ、それを支えるクラウド技術の急速な普及・台頭により、どのセキュリティツールによるソリューション需要が伸びるかが全く予測困難な状況となると考え、各ベンダの業態を参考にツールにおける各カテゴリの伸び率を均一にして捉えることとし+6.0%の成長率を予想。全体で 4,626 億円と順当に過去最高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。

このように統合型アプライアンス市場は市場がハイエンドと中小向け普及機に二極分化し、供給構造も初期と比較すると大きく変化が進んだ。すなわち、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て急成長したが、ここ数年はファイアウォールベンダがコンテンツセキュリティ寄りへ路線を転換し、大手ネットワーク装置ベンダがダウンサイジングして参入し、さらに普及機の市場ではセキュリティソリューションベンダが品質の安定した国内製ルータに自社のセキュリティソリューションを搭載し付加価値提供パッケージ型の事業参入もあり、競争の激しい市場となった。その結果、販売や更新・運用サービスは大手、提供は専業ベンダというサプライチェーンもできてきており、今後新たな伸びが期待できる。

(2)市場規模とその推移

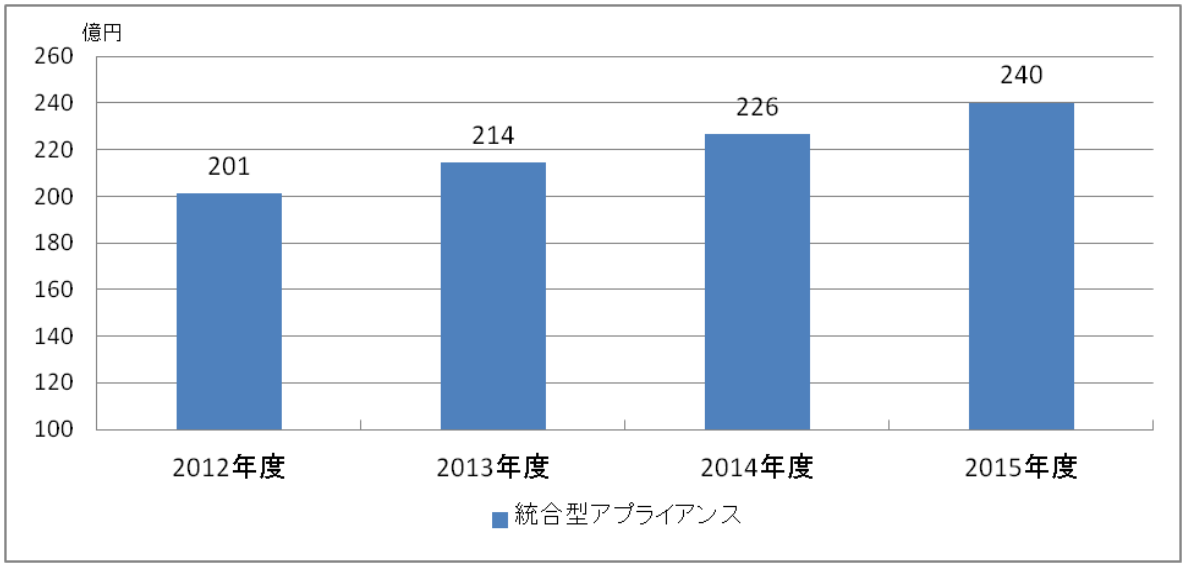
表 3 に国内統合型アプライアンス製品の市場規模の実績推定値と予測値を、図 4 にその市場規模の推移のグラフを示す。

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）	2012 年度	2013 年度	2014 年度	2015 年度
統合型アプライアンス	20,120	21,449	22,649	24,007
対前年度比成長率	－	6.6%	5.6%	6.0%

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、その後も堅調に伸びが続き、継続して成長傾向が予測される。

図 4　国内統合型アプライアンス市場推移



統合型アプライアンスは、大規模ユーザでは限定的用途、中小零細規模においては 3 年～6 年の買い替えサイクルの中で需要が発生するため、2012 年に初めて 200 億円市場となって以降、堅調に推移し、2013 年度は 214 億円、2014 年度は 226 億円になると推測する。

2015 年度も不確定要因は多少あるものの、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。特に普及機の需要層である中小企業の収益回復が鍵を握ると考え、6.0%の成長で 240 億円を超えると予測する。

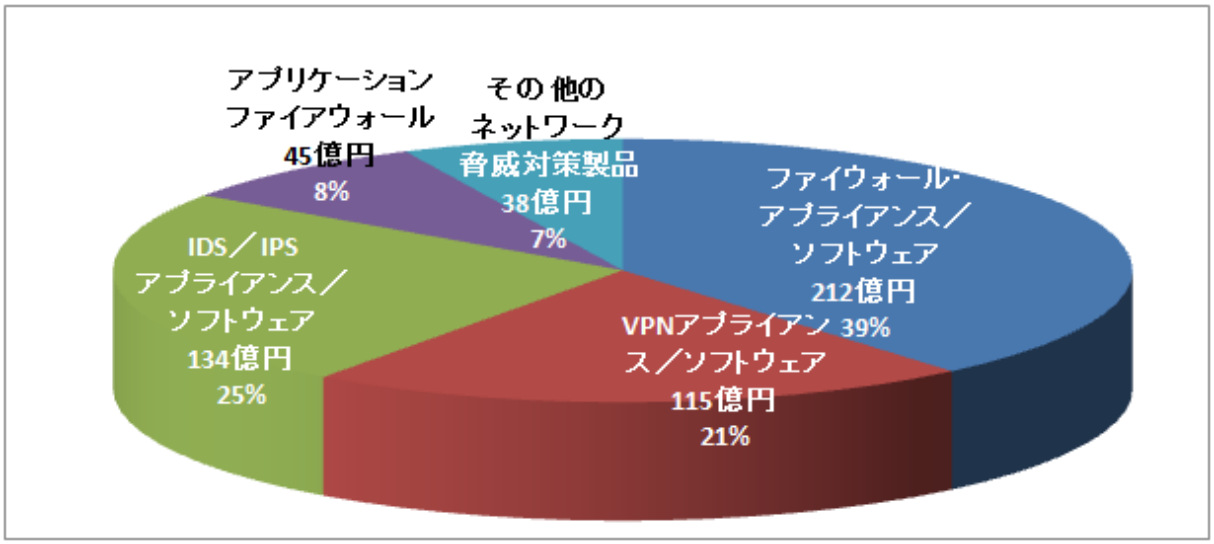
2.1.2.2. ネットワーク脅威対策製品市場

(1) 市場の動向

ネットワーク脅威対策製品の 2013 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。

図 5　2013 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[2]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

[2] 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

（独立行政法人情報処理推進機構）による推奨[3]、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[4]。

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。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。よって以下、市場規模の推移に関しては、前項の統合型アプライアンス市場と合わせて捉え考察を加えていく。

(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、2013 年度における売上実績推定値は 545 億円となった。前年度比の市場成長率は 4.5%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・再構築の取り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。

2014 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。ネットワーク脅威の深刻化と多様化に対する一般認知度も上がり、各企業ともこれまでのセキュリティ対策の見直しが進み出したと想定される。その結果、伸び率は 10.4%の成長となり、市場規模は 601 億円程度に達したものと推測される。

2015 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 637 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、2013 年度は 13.2%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 18.4%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] 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

[4] 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）	2012年度	2013年度	2014年度	2015年度
ファイウォール・アプライアンス／ソフトウェア	20,630	21,168	21,968	23,286
VPNアプライアンス／ソフトウェア	11,088	11,507	11,952	12,670
IDS／IPSアプライアンス／ソフトウェア	12,272	13,440	14,185	15,036
アプリケーションファイアウォール	4,273	4,535	7,435	7,881
その他のネットワーク脅威対策製品	3,848	3,832	4,584	4,859
合計	52,112	54,482	60,124	63,731
構成比				
ファイウォール・アプライアンス／ソフトウェア	39.6%	38.9%	36.5%	38.3%
VPNアプライアンス／ソフトウェア	21.3%	21.1%	19.9%	21.1%
IDS／IPSアプライアンス／ソフトウェア	23.6%	24.7%	23.6%	24.1%
アプリケーションファイアウォール	8.2%	8.3%	12.4%	8.7%
その他のネットワーク脅威対策製品	7.4%	7.0%	7.6%	7.7%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
ファイウォール・アプライアンス／ソフトウェア	－	3.8%	3.8%	6.0%
VPNアプライアンス／ソフトウェア	－	4.5%	3.9%	6.0%
IDS／IPSアプライアンス／ソフトウェア	－	4.7%	5.5%	6.0%
アプリケーションファイアウォール	－	6.0%	64.0%	6.0%
その他のネットワーク脅威対策製品	－	4.4%	19.6%	6.0%
合計	－	4.5%	10.4%	6.0%

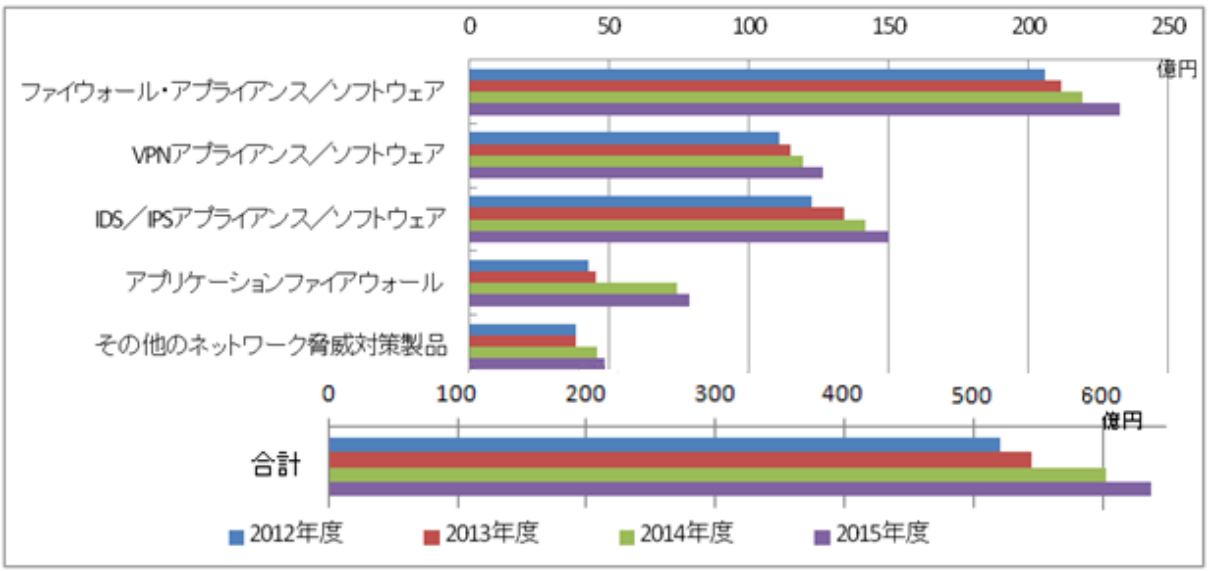
ネットワーク脅威対策製品のカテゴリの中では1番大きいセグメントである「ファイアウォールアプライアンス／ソフトウェア製品」は、本調査の対象期間でみると、2012年度206億円、2013年度212億円、2014年度220億円、2015年度233億円と増加傾向を見せている。2008年度前半までは、通信事業者を中心とするハイエンドのユーザの設備投資サイクル上の更新期に当っていたが、2009, 2010年度と、その反動と景気の低迷による設備投資控えの影響を受け、急速に市場規模が縮小した。その後は、経済環境が比較的順調なことと、ネットワーク脅威の深刻化から対策の強化・見直しが継続的に拡大し、レイヤー7 対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、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、2012年度111億円、2013年度115億円・4.5%増、2014年度120億円・3.9%増、2015年度127億円・6.0%増と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。

「IDS／IPS アプライアンス／ソフトウェア製品」市場は、2012 年度は 123 億円であった。2013 年度 134 億円で 4.7%増、2014 年度 142 億円で 5.5%増、2015 年度 150 億円で 6.0%増という拡大傾向の推定・予測となった。特に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る舞い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、2012 年度 43 億円から、2013 年度 45 億円で 6.0%増、2014 年度にはスマートデバイス向けネットワーク設備投資の需要が生まれ 74 億円 64.0%増の大幅増となった。2015 年度からはこの 2014 年の底上げをベースに他の製品同様 6.0%増の 79 億円と推定しているが、アプライアンス型による実装性・操作性の向上、利用側の運用ノウハウの向上などにより、アプリケーションファイアウォール市場の成長度合いは今後ますます強まると予測される。

「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によって多くの大企業が被害を受けるケースが増えてきており、特に EC サイトや金融・公共機関などの被害は甚大で、よりアプリケーション層に特化した新たな対策の導入が進んでいる。これは、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。当調査においても、このネットワーク脅威対策製品は今後特に注目していく。

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

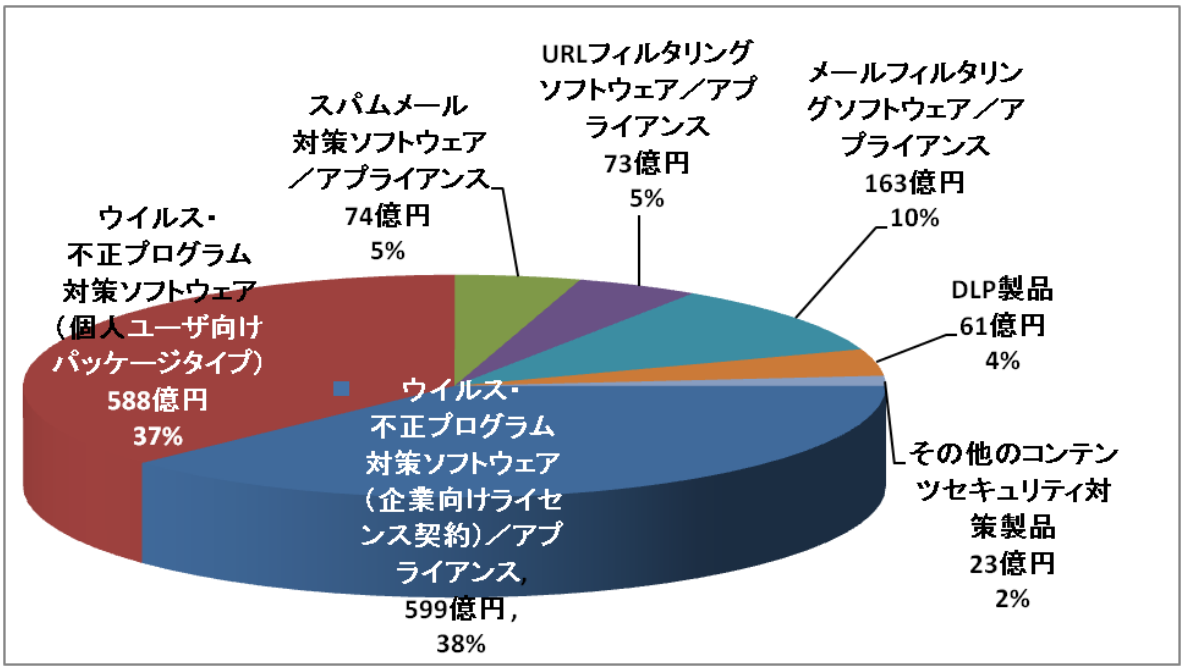
コンテンツセキュリティ対策製品は、情報セキュリティツール市場のうち金額規模が最も大きいカテゴリである。2012 年までの市場はパソコン向けが主流で、企業向けも個人向けもその普及啓発が市場の伸びを支えてきた。2013 年以降は、タブレット型端末やスマートフォン向けのマルウェア対策が主流となりつつある。パソコン向けはライセンス契約・更新型ビジネス、スマートデバイスは電子決済対応の直販ビジネスが主流であるため、市場調査を実施する際に流通実態の変化にも留意する必要がある。いずれにせよ全体的に順調に拡大しているものと考えられる。

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 2013 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 2007 年以降ほぼ 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。

スマートフォン、タブレット、インターネット対応テレビ・ゲーム機等への普及拡大が進む中、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、個人向け市場の拡大も進んでいる。

図 7　2013 年度のコンテンツセキュリティ対策製品市場



なお、BYOD (Bring Your Own Device 個人所有デバイスの業務利用)は中小企業を中心に徐々に進んでいると考えられ、個人所有のモバイル機器に会社のセキュリティポリシーが導入されるケースも多少出てきている。これは製品市場が個人向けと企業向けとの境界がなくなっていくことを意味する。本調査においては引き続きこの境界・区分に留意して動向を見守っていく。

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、企業業績の回復、経済活動における情報セキュリティ対策の重要性の認識浸透、モバイル機器への対策製品の充実等により、2013 年度には前年比 7.5%増の 599 億円に達したと推測する。2014 年度には更新の関係から多少伸びは鈍化して 3.3%増の 619 億円、2015 年度には 6.0%増の 656 億円と予測した。

「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。2013 年度の市場規模は 588 億円であったと推計される。これは前述の企業向け市場の前年比をしのぐ 8.0%の高い成長とみている。2014 年度 3.4%増の 608 億円、2015 年度 6.0%増の 644 億円に達すると予測したが、今後、個人消費の伸びや、ベンダによるスマートデバイス向けソリューションの充実と普及促進へ向けての取り組み次第では、更に大きく増加すると考えられる。

これに次ぐ規模のセグメントは「メールフィルタリングソフトウェア／アプライアンス」で、特にメール本体や添付ファイルで社外に出ていく情報のチェックのために広く使われるようになっている。その市場規模は 2012 年度で 156 億円であるが、2015 年度には 184 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 9.0%増、2014 年度 7.7%増とコンスタントに拡大して 2015 年度の市場規模は 85 億円に達すると予測される。

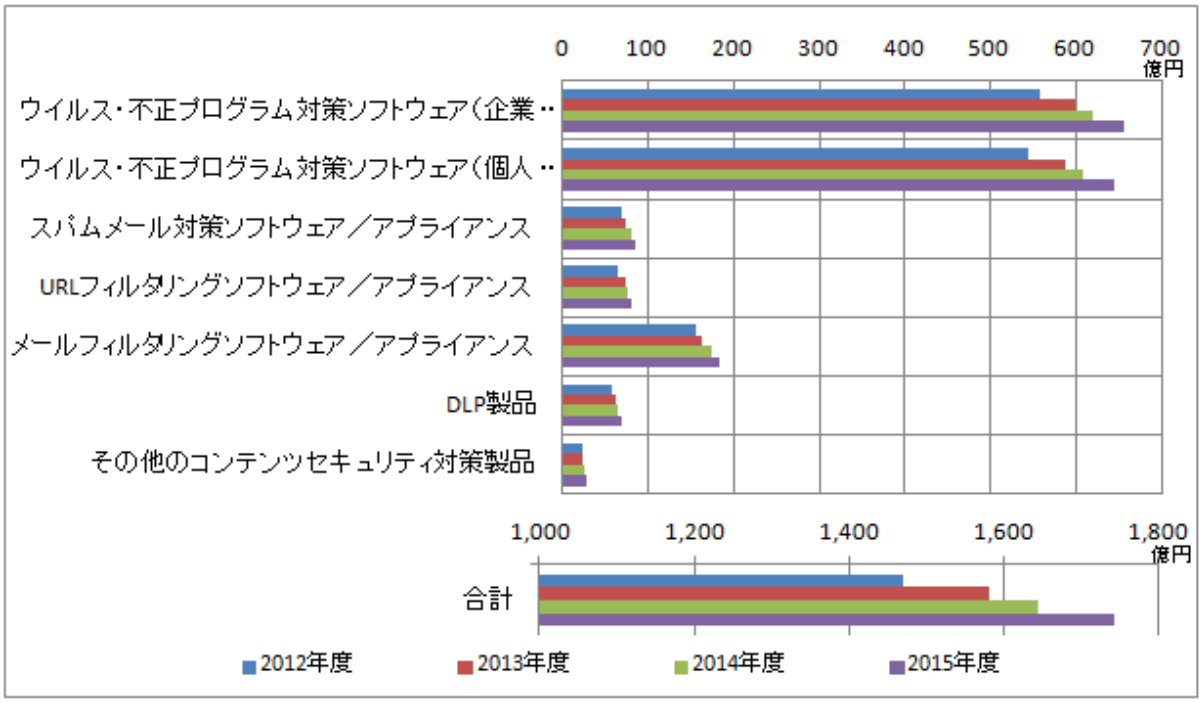
次いで「URL フィルタリングソフトウェア／アプライアンス」がほぼ同規模の市場を形成している。2012 年度 65 億円、2013 年度 73 億円（12.6%増）、2014 年度 75 億円（2.4%増）、2015 年度 80 億円（6.0%増）と 2013 年度に著しい伸びを記録して、80 億円市場に達すると予想する。

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）	2012年度	2013年度	2014年度	2015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	55,736	59,916	61,916	65,631
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）	54,438	58,787	60,787	64,434
スパムメール対策ソフトウェア／アプライアンス	6,832	7,448	8,019	8,500
URLフィルタリングソフトウェア／アプライアンス	6,484	7,304	7,480	7,929
メールフィルタリングソフトウェア／アプライアンス	15,633	16,311	17,311	18,350
DLP製品	5,642	6,133	6,433	6,819
その他のコンテンツセキュリティ対策製品	2,262	2,336	2,591	2,747
合計	147,028	158,234	164,537	174,409
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	37.9%	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）	37.0%	37.2%	36.9%	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%	4.7%	4.9%	4.8%
URLフィルタリングソフトウェア／アプライアンス	4.4%	4.6%	4.5%	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	10.6%	10.3%	10.5%	10.4%
DLP製品	3.8%	3.9%	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%	1.6%	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	－	7.5%	3.3%	6.0%
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）	－	8.0%	3.4%	6.0%
スパムメール対策ソフトウェア／アプライアンス	－	9.0%	7.7%	6.0%
URLフィルタリングソフトウェア／アプライアンス	－	12.6%	2.4%	6.0%
メールフィルタリングソフトウェア／アプライアンス	－	4.3%	6.1%	6.0%
DLP製品	－	8.7%	4.9%	6.0%
その他のコンテンツセキュリティ対策製品	－	3.3%	10.9%	6.0%
合計	－	7.6%	4.0%	6.0%

「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61億円（8.7%増）、2014年度64億円（4.9%増）、2015年度68億円（6.0%増）との予測結果となった。

９図 8　国内コンテンツセキュリティ対策製品市場推移



2.1.2.4. アイデンティティ・アクセス管理製品市場

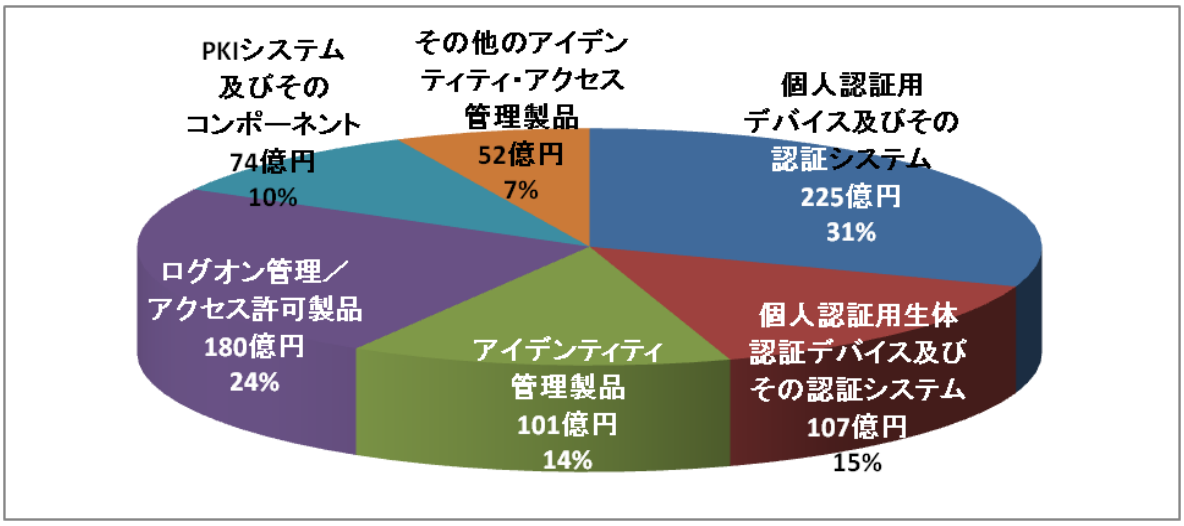
(1)　市場の動向

図 9 に 2013 年度のアイデンティティ・アクセス管理製品のセグメント別市場規模分布を示す。

電子化されたファイルやデータとして保存された多くの重要な情報に対し、ネットワークを通して様々な場所から、昼夜を問わずアクセスできるようになった昨今、ネットワーク、サーバ、アプリケーション等、システム全体を通して、使用する個人を識別し、適切なアクセス権を付与し運用する「アクセス管理」の重要性はますます高まっている。企業の情報資産を情報漏えいや改ざん、盗難、紛失、消失といったセキュリティ上の脅威から守るためにも、「アクセス管理」は非常に重要な機能である。業務効率を重視し、誰もがアクセスできるという利便性を第一優先にする考え方を変え、リソース（情報(処理)資源）にアクセスできる人間を、必要最小限に限定するというセキュリティ重視の思想に基づくシステムを検討する企業が、個人情報保護法や情報漏えい事件を契機に増加する傾向にあった。また、スマートフォンやタブレット PC に代表される携帯端末を業務で使用するニーズや、クラウドサービスの利用が高まっている昨今、携帯端末向けアイデンティティ・アクセス管理製品の登場やクラウドサービス向けアクセス管理、シングル・サインオン（SSO）等のニーズで、この市場は、景気の回復とともに成長が期待できる分野と考えられる。間違いによるアクセスや不正アクセスを IT 技術で管理することで、不必要なアクセスの発生を最小限に抑止する環境を実現することと、データの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。

図 9　2013 年度のアイデンティティ・アクセス管理製品市場



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、海外製と国内製があるが、提供する機能にはベンダごとに差が見られる。例えば、内部統制の観点より承認ワークフローに対するニーズは ID 管理の中でも重要な要素となる場合が多いが、製品の中で提供しているもの、オプションで提供するもの、あるいは別製品として提供しているもの等、様々である。更に、実装方式においても、全てのアクセス先にプログラムをインストールして、より細かい制御やログが取得できるエージェントタイプと、重要な情報リソースへのゲートウェイに実装し、一括でアクセス管理およびログ取得を行うエージェントレスタイプがある。

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

(2)　市場規模とその推移

表 6 に国内アイデンティティ・アクセス管理製品の市場規模推定実績値と予測値を、図 10 にその市場規模の推移のグラフを示す。アイデンティティ・アクセス管理製品の市場規模は、2013 年度の実績で 737 億円（前年比伸び率 7.1%）となったが、「情報セキュリティツール」市場全体の 4,141 億円に対する構成比は 17.8 %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。2014 年度は+4.5%の 770 億円、2015 年度には+6.0%の 816 億円と、800 億円台を駆け上がると予測される。

表 6　国内アイデンティティ・アクセス管理製品市場規模　実績と予測

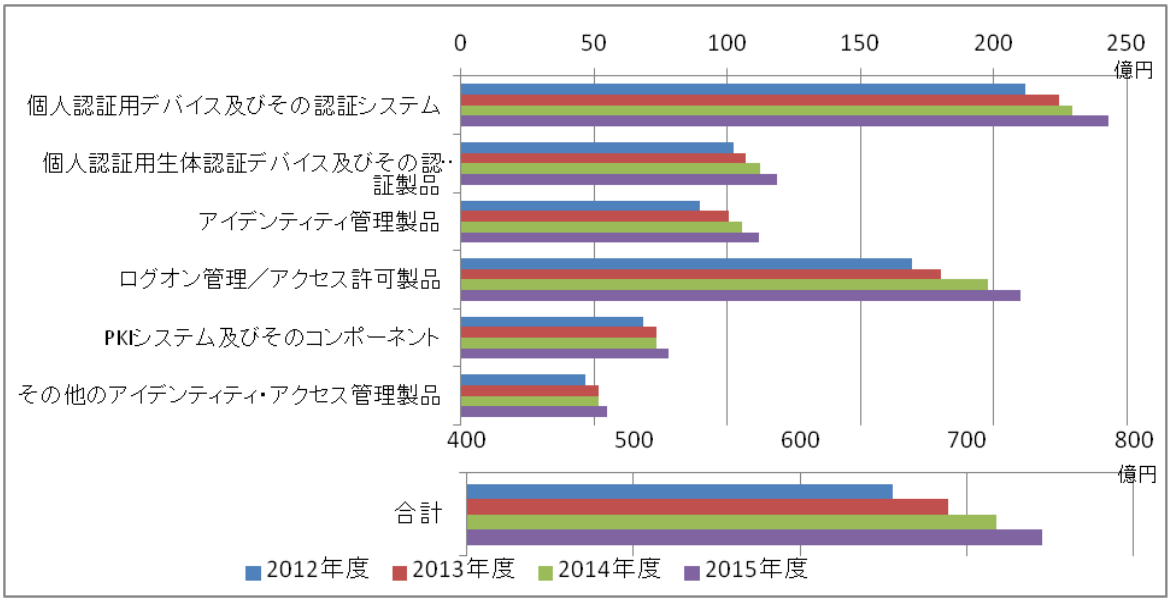
市場規模（百万円）	2012年度	2013年度	2014年度	2015年度
個人認証用デバイスおよびその認証システム	21,201	22,451	22,951	24,328
個人認証用生体認証デバイスおよびその認証システム	10,232	10,709	11,209	11,882
アイデンティティ管理製品	8,976	10,050	10,550	11,183
ログオン管理／アクセス許可製品	16,930	18,003	19,803	20,991
PKI システムおよびそのコンポーネント	6,846	7,356	7,356	7,798
その他のアイデンティティ・アクセス管理製品	4,660	5,158	5,158	5,467
合計	68,845	73,727	77,027	81,649
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%	30.5%	29.8%	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	14.9%	14.5%	14.6%	14.7%
アイデンティティ管理製品	13.0%	13.6%	13.7%	13.6%
ログオン管理／アクセス許可製品	24.6%	24.4%	25.7%	25.4%
PKI システムおよびそのコンポーネント	9.9%	10.0%	9.6%	9.6%
その他のアイデンティティ・アクセス管理製品	6.8%	7.0%	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	－	5.9%	2.2%	6.0%
個人認証用生体認証デバイスおよびその認証システム	－	4.7%	4.7%	6.0%
アイデンティティ管理製品	－	12.0%	5.0%	6.0%
ログオン管理／アクセス許可製品	－	6.3%	10.0%	6.0%
PKI システムおよびそのコンポーネント	－	7.5%	0.0%	6.0%
その他のアイデンティティ・アクセス管理製品	－	10.7%	0.0%	6.0%
合計	－	7.1%	4.5%	6.0%

「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 2013 年度の構成比で 30.5%と最も大きな部分を占めた。市場規模は 2013 年度で 225 億円であり、2014 年度は 230 億円と前年比 2.2%増と予想される。

これに次いで規模の大きいセグメントは「ログオン管理／アクセス許可製品」である。市場規模は 2013 年度に 180 億円で、2014 年度には 10.0%拡大して 198 億円となり、2015 年度には 210 億円（前年度比成長率 6.0%）と 200 億円市場になると予測した。

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 2013 年度は、4.7%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。Apple 社の iPhone6 から指紋認識が標準搭載されているが国内市場において大きく市場規模を押し上げる他のソリューションは未だ出回っていない。

図 10　国内アイデンティティ・アクセス管理製品市場推移



「アイデンティティ・アクセス管理」は、大規模システムや基幹系システムでは以前から組み込まれており、成熟市場のイメージがあったが、内部統制からの必要性や情報セキュリティ対策、クラウドコンピューティングサービス利用拡大の面から適用対象が拡大し、またスマートフォンやタブレット PC の市場拡大に伴い、今後は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 2013 年度におけるセグメント分布を図 11 に示す。

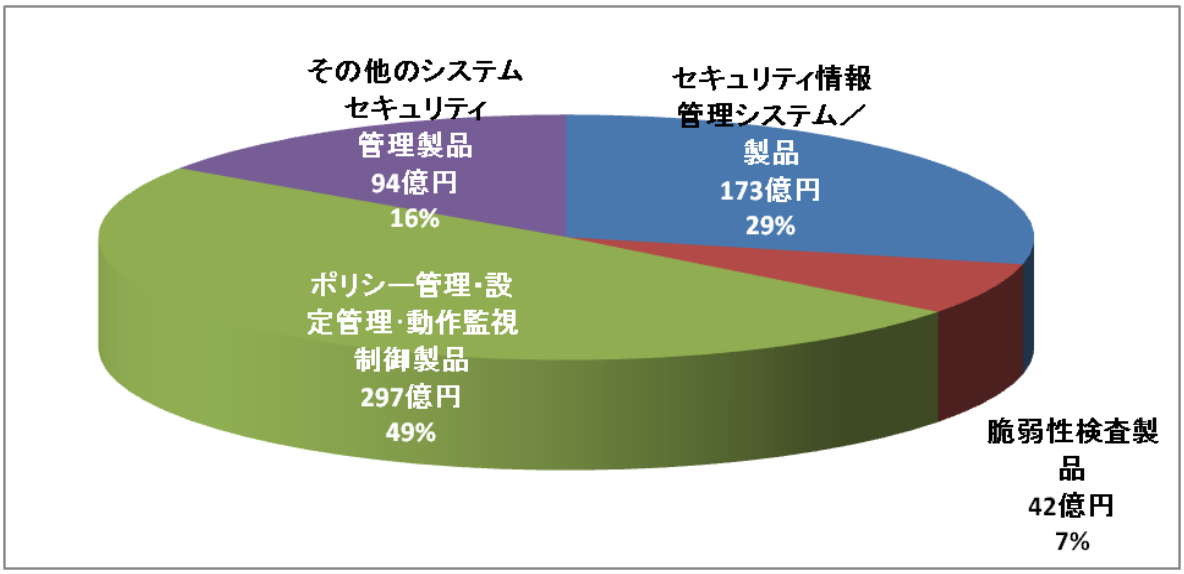
2011 年 9 月に発覚した三菱重工へのサイバー攻撃による機密情報の漏えい事件をきっかけに内部ネットワークの管理を強化する動きが活発化した。その動きはシステムセキュリティ管理製品カテゴリを構成する各セグメント市場に及んでいる。

「セキュリティ情報管理システム/製品」はこれまで外部からの不正トラフィックに対応するためのシステム統合管理ツールとして活用されることが多かったが、リアルタイム性を考慮した、内部から外部へのトラフィックのモニタリングツールとしての利用が浸透している。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と外部の C&C[5]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今後も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、需要は依然高い分野である。スマートデバイスの普及に伴い、MDM（Mobile Device Management）、リモートロック、リモートワイプ（初期化、無効化）ツールの導入が進み、今後更に管理製品や

[5] 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

図 11　2013 年度のシステムセキュリティ管理製品市場



サービスが増えてくることが推測される。

(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2013年度には全セグメント合せて605億円程度の市場を形成しており、2012年度と比べると+9.7%、2014年度は4.6%増の632億円と堅調な伸び率を見込んでおり、その傾向は2015年度（671億円、+6.0%）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動向は前向きであると考えられる。

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2013年度に173億円、前年度比8.4%増と増加傾向にあり、さらに2014年度は5.8%増の183億円、2015年度は+6.0%の194億円と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、2013 年度における成長率も+11.7%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 297 億円である。2014 年度はその反動もあり+1.7%と低い成長率ではあるが初めて 300 億円を突破し 302 億円、2015 年度は 6.0%増の 320 億円と継続成長すると推測している。

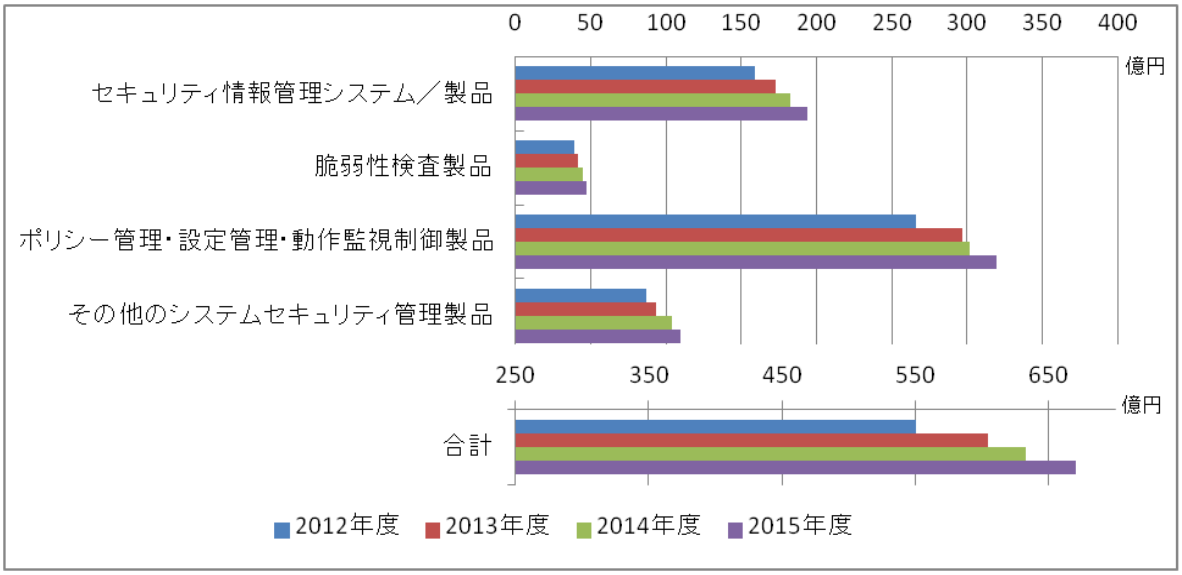
脆弱性検査製品は、Web サイトやネットワークシステムの脆弱性スキャナーであり、検査サービス事業者や SI 事業者等需要が限定的であることから市場規模は 2013 年度で 42 億円と小さい。伸び率も他のセグメントに比較して限定的で、2014 年度+5.3%、2015 年度+7.2%程度と予測され、2015 年度の市場規模は 47 億円と推定される。

「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。2013年度の伸び率は+8.1%で、2014年度+10.7%、2015年度+6.0%と高い成長率を示し、2014年度には100億円を突破するものと予測される。標的型攻撃対

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）	2012年度	2013年度	2014年度	2015年度
セキュリティ情報管理システム／製品	15,922	17,267	18,267	19,363
脆弱性検査製品	3,942	4,153	4,453	4,720
ポリシー管理・設定管理･動作監視制御製品	26,580	29,679	30,179	31,990
その他のシステムセキュリティ管理製品	8,664	9,369	10,369	10,991
合計	55,108	60,468	63,268	67,064
構成比				
セキュリティ情報管理システム／製品	28.9%	28.6%	28.9%	28.7%
脆弱性検査製品	7.2%	6.9%	7.0%	7.0%
ポリシー管理・設定管理･動作監視制御製品	48.2%	49.1%	47.7%	48.1%
その他のシステムセキュリティ管理製品	15.7%	15.5%	16.4%	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	―	8.4%	5.8%	6.0%
脆弱性検査製品	―	5.3%	7.2%	6.0%
ポリシー管理・設定管理･動作監視制御製品	―	11.7%	1.7%	6.0%
その他のシステムセキュリティ管理製品	―	8.1%	10.7%	6.0%
合計	―	9.7%	4.6%	6.0%

図 12　国内システムセキュリティ管理製品市場推移



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。次年度には小分類カテゴリを独立させることも検討したい。

2.1.2.6. 暗号化製品市場

(1) 市場の動向

暗号化製品も 2013 年度には前年比+9.8%と好調な推移を見せている。

「暗号の 2010 年問題」への対応として具体的な移行フェーズに入り市場が活性化し、政府認証基盤（GPKI）の暗号アルゴリズム移行作業フェーズ 1 が実施され、機器更改時には新旧暗号に対応することになっている。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 2014 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。また、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

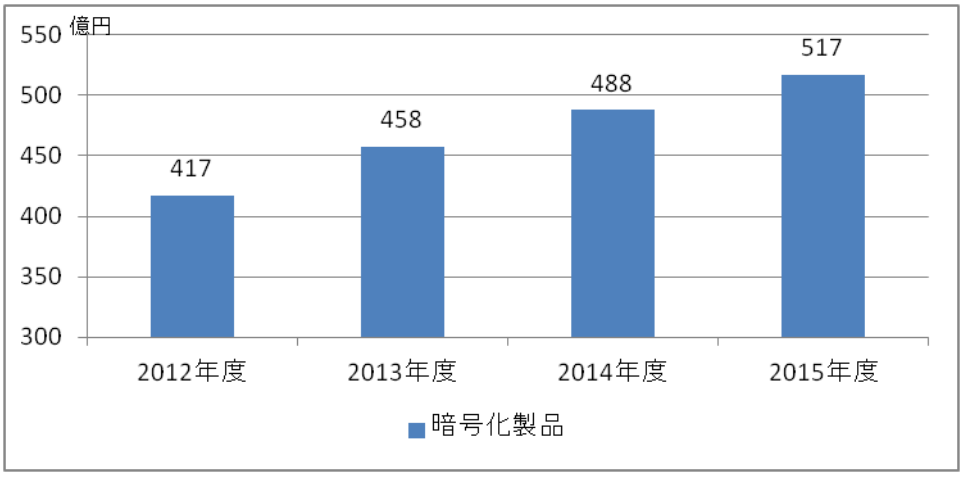
表 8 に国内暗号化製品市場規模の実績推定値と予測値を、図 13 にその市場規模の推移のグラフを示す。

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。2013 年度の市場規模は 458 億円で前年度比 9.8%増加となった。2014 年度は前年度比 6.6%増の 488 億円、2015 年度もさらに 6.0%市場規模を拡大させ、517 億円の市場規模になると予測している。

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）	2012 年度	2013 年度	2014 年度	2015 年度
暗号化製品	41,693	45,779	48,779	51,706
対前年度比成長率				
暗号化製品	－	7.6%	5.4%	6.0%

図 13　国内暗号化製品市場推移



2.2. 国内情報セキュリティサービス市場の分析

2.2.1. 情報セキュリティサービス市場の全体概要

「情報セキュリティサービス」とは、情報セキュリティ実現のための様々なサービスを指すもので、いわゆる役務契約型の商取引、すなわちサービスの提供と定義している。

このカテゴリには、大分類として「情報セキュリティコンサルテーション」、「セキュアシステム構築サービス」、「セキュリティ運用・管理サービス」、「情報セキュリティ教育」、「情報セキュリティ保険」の 5 カテゴリを区分している。ツールに直接関連する保守・サポートや更新サービスはツールの市場に付帯するものとしてツール側に含め、サービス分野には入れていない。ただし、ツール類を導入するに際しての使用条件や各種パラメータの設定といった導入支援サービスや、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	2012年度		2013年度			2014年度			2015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	70,165	20.3%	72,731	20.0%	3.7%	76,331	19.8%	4.9%	80,147	19.9%	5.0%
セキュアシステム構築サービス	138,889	40.1%	144,875	39.9%	4.3%	151,375	39.2%	4.5%	158,944	39.8%	5.0%
セキュリティ運用・管理サービス	103,189	29.8%	109,379	30.1%	6.0%	120,607	31.2%	10.3%	127,843	30.7%	6.0%
情報セキュリティ教育	26,574	7.7%	26,979	7.4%	1.5%	27,979	7.2%	3.7%	29,378	7.5%	5.0%
情報セキュリティ保険	7,640	2.2%	8,885	2.4%	16.3%	9,885	2.6%	11.3%	10,577	2.1%	7.0%
セキュリティサービス市場合計	346,457	100.0%	362,849	100.0%	4.7%	386,176	100.0%	6.4%	406,889	100.0%	5.4%

今回の調査結果では、対象期間の最初の年度である 2012 年度の「情報セキュリティサービス」

市場規模は 3,465 億円と見積もられ、以降年率+5%前後の拡大を期待し、2015 年度には 4000 億円市場になるものとの観測となった。

リーマンショック後の世界経済の低迷による企業の設備投資の引き締めと、コンサルテーションやシステム構築サービスといった初期投資サイクルの閑散期が重なり、2010 年度の 3,100 億円が現在の成長前のボトムだったと推測している。しかし、2011 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と考えられる。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。また端末エッジ側とクラウドセンター側に 2 極分化する中で、従来のツール偏重からサービス主体への対策の必要性に対する認知も浸透するようになってきた。

2013 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、大規模な情報漏えい被害により対策が根本的に見直された時期でもあり、市場規模は 3,628 億円となった。2014 年度は「セキュリティ運用・管理サービス」の強化や「情報セキュリティ保険」の続伸に支えられ、6.4%増の成長で 3,862 億円と、初めて 3,800 億円台に到達するものと予測される。さらに 2015 年度も経済条件の好転が期待される中で、サイバー脅威の深刻化も進行することから、前年度比 5.4%増の成長 4,000 億円の大台に達するものと予測される。

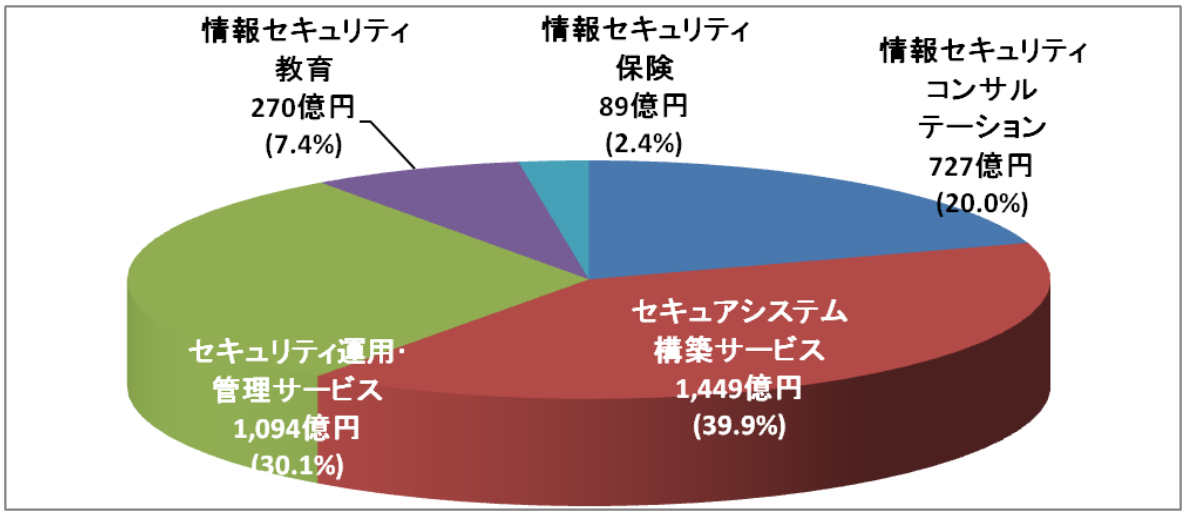
図 14 に 2013 年度の国内情報セキュリティサービス市場のカテゴリ別分布を示す。また図 15 には国内情報セキュリティサービス市場の経年推移を表した。

「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、2013 年度実績推定値で 1,449 億円と、情報セキュリティサービス市場全体の 39.9%を占めた。このカテゴリは、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･構築するシステムインテグレーション的要素が強く市場規模も大きい。

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、2013 年度実績は 1,094 億円。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。水のみ場攻撃に代表される巧妙なサイバー犯罪に対応するための SOC(Security Operation Center)の役割の増大や認知度の向上、さらに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、マイナンバー制度導入に伴い需要が拡大している。

金額規模では情報セキュリティサービス市場の中で 3 番目に位置するのが「情報セキュリティコンサルテーション」である。経営管理の視点から専門家の支援を活用する要素が強く、経営コンサルに近いところに位置するので、会計監査法人系、SI 系、独立系等多様な事業者がサービスを提供している。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

図 14　2013 年度の国内情報セキュリティサービス市場

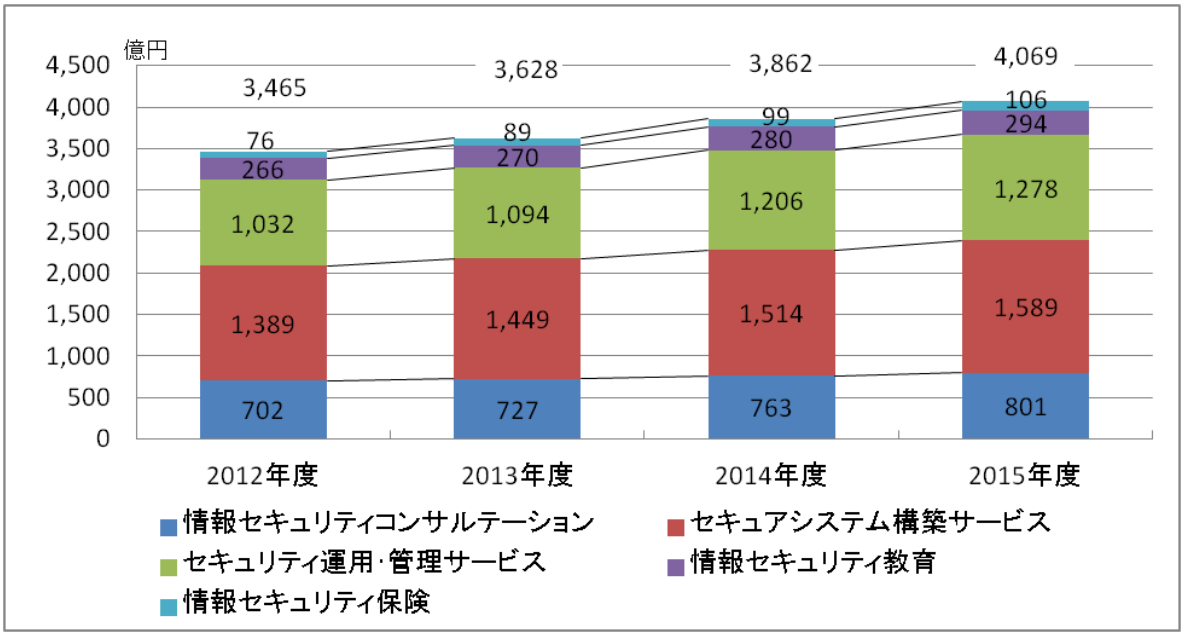


年度から適用された内部統制報告制度、更には新潟県中越・中越沖地震や新型インフルエンザ等のパンデミック対策を契機とした事業継続計画(BCP)への関心の高まりにより、リスクマネジメント系・コンプライアンス系の専門家によるコンサルテーション・ビジネスの商品化が挙げられる。プライバシーマーク認定や ISMS 認証の取得に取り組むケースも増え、その取得支援サービスや、認証サービスの需要が高まった時期があった。その後、対策の浸透や体制構築が一巡すると、市場の成長には急ブレーキがかかり、前回調査の期間中はマイナス成長が続くという調査結果であった。しかし、2011 年度に、過去に構築した対策の体系的見直しの需要が顕在化し、導入必須の大企業のみならず、中堅企業での需要も高まり、再び市場拡大に向かい始めたと見られる。その結果、2013 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 3.7%拡大して 727 億円になったと見られる。

「情報セキュリティ教育」は 2013 年度+1,5%の 270 億円と低めの成長に留まった。これは「情報セキュリティコンサルテーション」に客足を引っ張られた形になった一時的な流れと考えられる。しかし、企業がコンサルテーションを受け導入すると、今度は運用・管理を行うために従業員を教育する必要がある。最近の情報セキュリティコンサルテーションには企業内のセキュリティ教育を行う e ラーニング教材をセットで提案する動きもあり、「情報セキュリティ教育」の成長率は 2014 年度には持ち直すと考えられる。教育市場の継続的拡大の背景には、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、標的型攻撃や水飲み場型攻撃対策など、従業員の日ごろの意識の持ち方に対する投資という側面がある。

情報セキュリティ保険は、ソフトウェア企業も PL 保険に加入し始めた 2000 年前後に設計された比較的歴史の古いサービスではあるが、2010 年代に入って、インシデントの多発と深刻化が進み、完全なセキュリティ防御は困難との認識が形成されるようになり、保険への需要が拡大傾向を見せている。市場規模は、2013 年度で前年度比+16.3%の 89 億円と本調査のツール・サービス合わせた全カテゴリ中、最も成長を遂げたと推測する。

図 15　国内情報セキュリティサービス市場推移



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、2013 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。

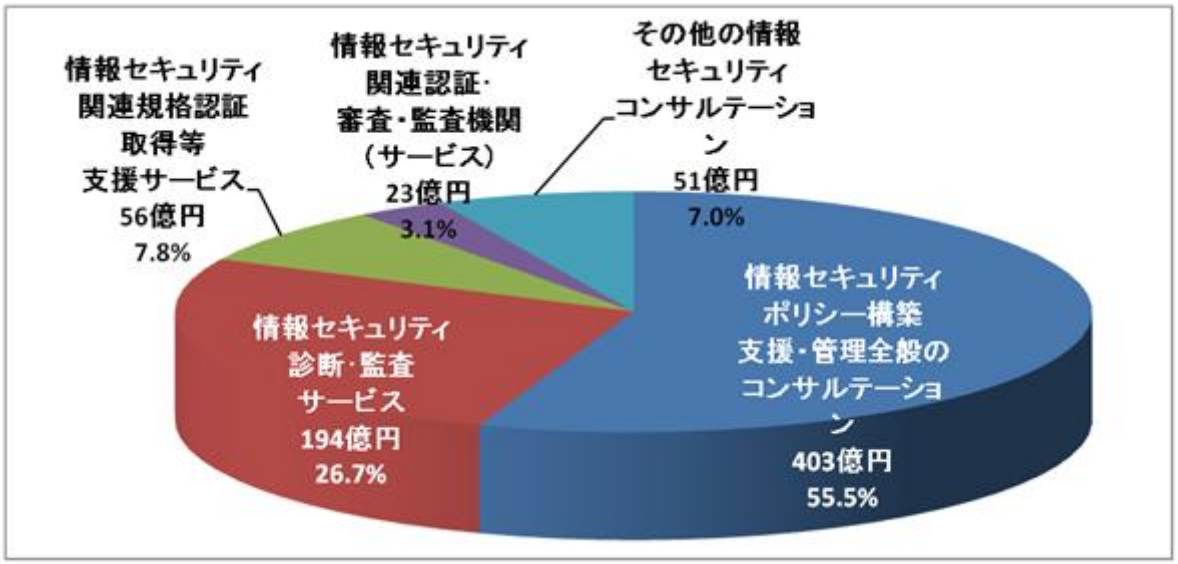
「情報セキュリティコンサルテーション」というカテゴリは、コンサルテーションの特性から、情報セキュリティに関する取り組みの先端を歩むこととなり、必然的に時代の要請に即した内容や市場の問題を反映したものとなる。ここ数年で以下のような変化が起きていると考えられる。

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。

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

図 16　2013 年度の情報セキュリティコンサルテーション市場



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の深い規格として、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、新規認証取得の取り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、2013 年度以降は経済環境の好転に伴って回復したと見込まれる。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+3,7%、2014 年度+4.9%、2015 年度+5.0%と継続して堅調なプラス成長基調に乗ると予想される。

(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。

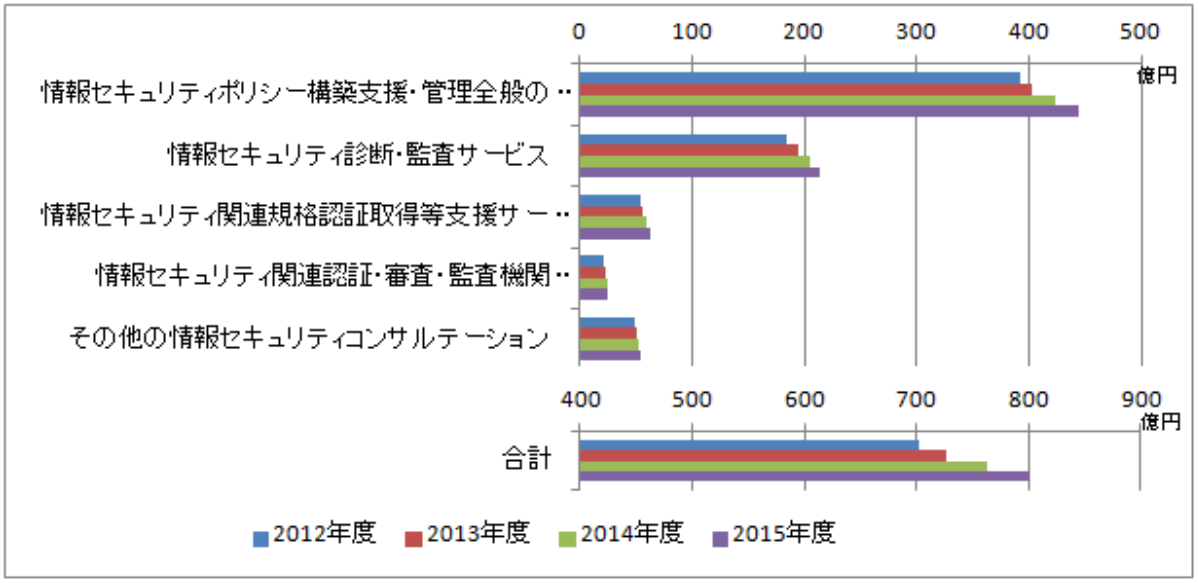
2013 年度においては「情報セキュリティコンサルテーション」市場は全体で 727 億円程度となり、前年度比成長率はプラス 3.7%であった。

最大セグメントの「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 +3.0%403 億円と、2 番目の「情報セキュリティ診断・監査サービス」の+5.0%194 億円の 2 つを合わせると「情報セキュリティコンサルテーション」市場全体の約 82%を占める。

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）	2012 年度	2013 年度	2014 年度	2015 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	39,139	40,332	42,332	44,448
情報セキュリティ診断･監査サービス	18,489	19,421	20,421	21,442
情報セキュリティ関連規格認証取得等支援サービス	5,426	5,639	5,939	6,236
情報セキュリティ関連認証･審査・監査機関（サービス）	2,169	2,276	2,426	2,547
その他の情報セキュリティコンサルテーション	4,942	5,063	5,213	5,474
合計	70,165	72,731	76,331	80,147
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	55.8%	55.5%	55.5%	55.0%
情報セキュリティ診断･監査サービス	26.4%	26.7%	26.8%	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	7.7%	7.8%	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）	3.1%	3.1%	3.2%	3.2%
その他の情報セキュリティコンサルテーション	7.0%	7.0%	6.8%	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	－	3.0%	5.0%	5.0%
情報セキュリティ診断･監査サービス	－	5.0%	5.1%	5.0%
情報セキュリティ関連規格認証取得等支援サービス	－	3.9%	5.3%	5.0%
情報セキュリティ関連認証･審査・監査機関（サービス）	－	4.9%	6.6%	5.0%
その他の情報セキュリティコンサルテーション	－	2.4%	3.0%	5.0%
合計	－	3.7%	4.9%	5.0%

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



「情報セキュリティ関連認証・審査・監査機関（サービス）」のセグメントは、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。また、国内の ISMS 認証取得件数（JIPDEC 認証）[6]はすでに 4000 件を超えており、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 7・8 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。2012 年度までマイナス成長だった「情報セキュリティ関連規格認証取得等支援サービス」市場は、今後は 3～5%の成長基調に戻ると考えられるが、2014 年度に認証取得済み大企業による情報漏えい事件が起き、認証の役割が根本から問われていることから、コンサルテーションの伸びに依存する形での成長となると予想する。

2.2.2.2. セキュアシステム構築サービス市場

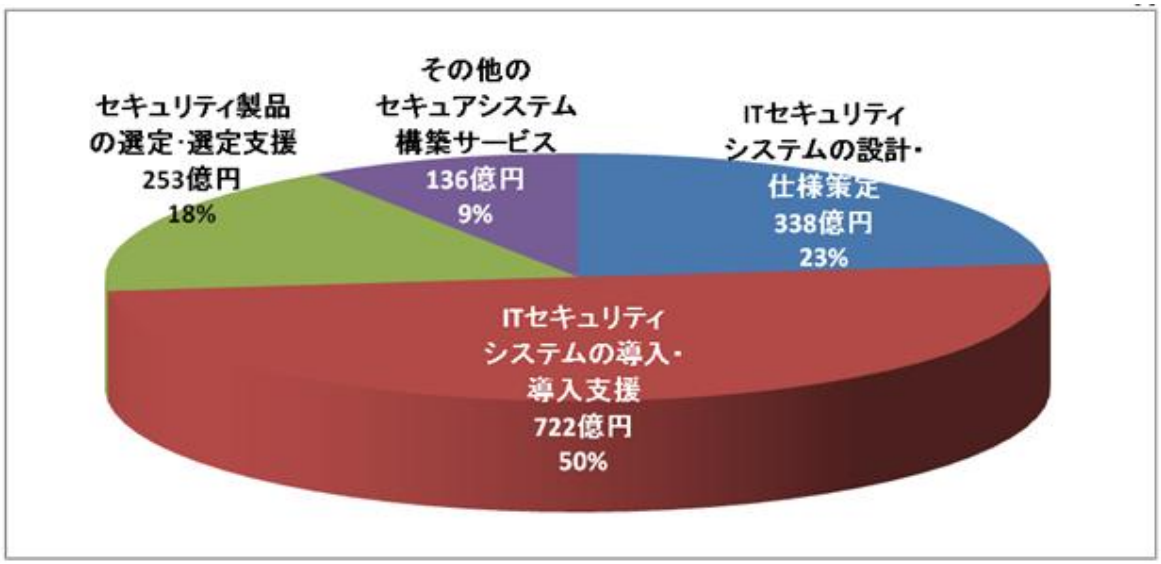
(1) 市場の動向

図 18 に 2013 年度のセキュアシステム構築サービス市場のセグメント別分布を示す。

「セキュアシステム構築サービス」は、セキュリティ製品の導入や構築を含めた、IT セキュリティシステムまたは IT システムのセキュリティに関する構築、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、2012 年度 1,389 億円、2013 年度 1,449 億円、2014 年度には 1,514 億円とプラス成長がみられ、2015 年度には 1,589 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約 40%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 番目の規模である。

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

図 18　2013 年度のセキュアシステム構築サービス市場



「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・構築時に必要なサービスで、さらにシステム全体の設計・仕様の策定時にセキュリティ要素を組み込むため、この全体需要からセキュリティ部分だけを個別に切り出した発注は少ない。よって本調査では、大企業のセキュリティ部門の社内発注（内部振替金額・比率等）を調査して規模を策定している。東日本大震災以後の BCP、大規模情報漏えい事件、標的型攻撃被害などの詐欺・窃盗事件が多発し、これまでのセキュリティポリシーやセキュリティデザイン･運用を見直して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 2011 年度には市場全体がプラス基調に回復し、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、市場規模は堅調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[7]」「IPv6」「DKIM[8]」等、これまで導入・運用に関するノウハウの蓄積が少ない技術への対応は 2010 年頃から本格化し、さらに従業員のモバイル環境活用による生産性向上と安全安心を確保する観点からのセキュアな環境作りが急速に立ち上がり、ますますこの分野の需要に貢献することも期待される。

---

[7] 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

[8] 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

(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。

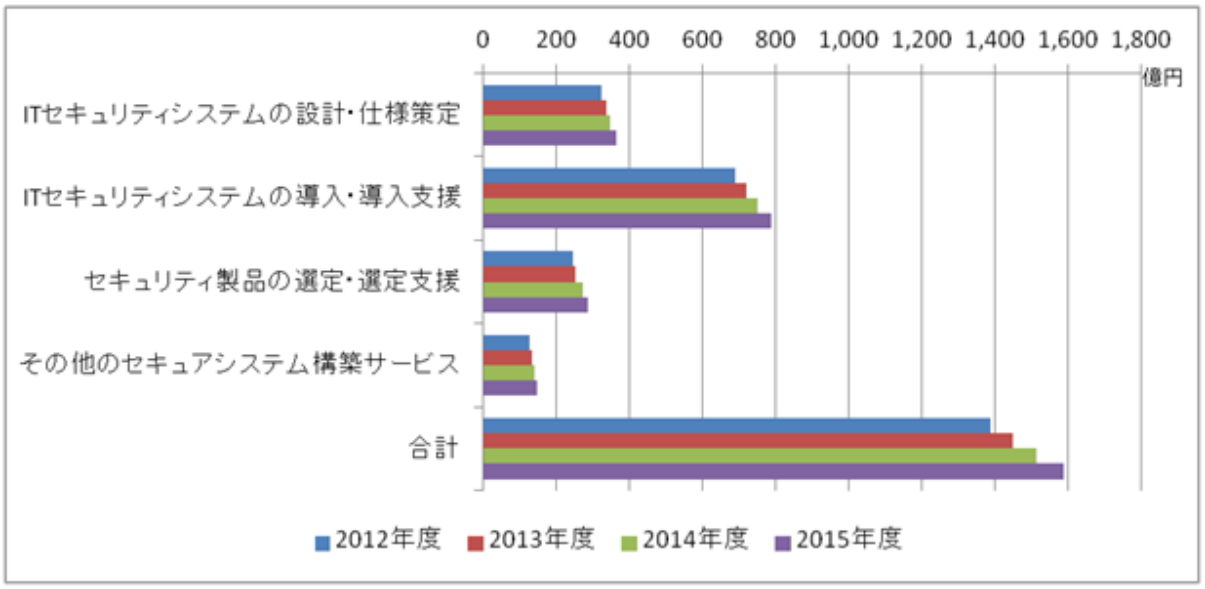
「セキュアシステム構築サービス」カテゴリのうち最大のセグメントは全体の約５割を占める「IT セキュリティシステムの導入･導入支援」であり、2012 年度 691 億円、2013 年度 722 億円（前年度比 4.6%増）、2014 年度 752 億円（同 4.2%増）、2015 年度予測 790 億円（同 5.0%増）の規模と推測される。これに次ぐのが「IT セキュリティシステムの設計・仕様策定」で、約 2 割強を占める。金額は 2012 年度 324 億円、2013 年度 338 億円（前年度比 4.3%増）、2014 年度 348 億円（同 3.0%増）、2015 年度予測 365 億円（同 5.0%増）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は至らないが個別の製品を選定するに際して利用する専門サービスで、従来の PC 環境からモバイル環境になる中、2014 年度 2015 年度はこれまでの堅調な伸びから一転して大きな伸びが期待されており、2012 年度は 246 億円、2013 年度が 253 億円（前年度比 3.1%増）、2014 年度は 273 億円（同 7.9%増）、2015 年度には 287 億円（同 5.0%増）と推測している。

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）	2012 年度	2013 年度	2014 年度	2015 年度
IT セキュリティシステムの設計･仕様策定	32,398	33,777	34,777	36,516
IT セキュリティシステムの導入･導入支援	69,075	72,239	75,239	79,001
セキュリティ製品の選定･選定支援	24,552	25,303	27,303	28,668
その他のセキュアシステム構築サービス	12,864	13,555	14,055	14,758
合計	138,889	144,875	151,375	158,944
構成比				
IT セキュリティシステムの設計･仕様策定	23.3%	23.3%	23.0%	23.3%
IT セキュリティシステムの導入･導入支援	49.7%	49.9%	49.7%	49.8%
セキュリティ製品の選定･選定支援	17.7%	17.5%	18.0%	17.6%
その他のセキュアシステム構築サービス	9.3%	9.4%	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	－	4.3%	3.0%	5.0%
IT セキュリティシステムの導入･導入支援	－	4.6%	4.2%	5.0%
セキュリティ製品の選定･選定支援	－	3.1%	7.9%	5.0%
その他のセキュアシステム構築サービス	－	5.4%	3.7%	5.0%
合計	－	4.3%	4.5%	5.0%

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ますます必要とする一方で、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、さらに同じ会社の社員が社内の事情に左右され判断が鈍ることを回避するといった経営判断が考えられる。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。2012 年度に引続き、2013 年度も全てのセグメントでプラス成長となり、1,000 億円を超える市場である。

図 20 に 2013 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。

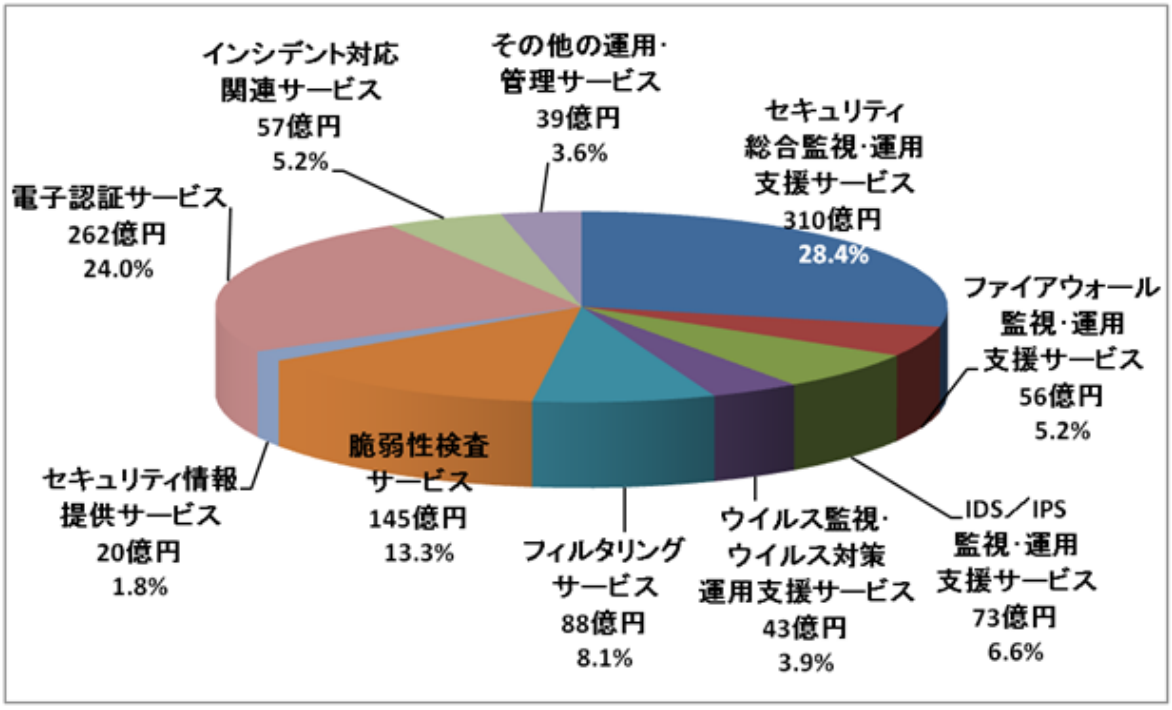
運用支援サービスについては、「ファイアウォール監視・運用支援サービス」と「IDS／IPS 監視・運用支援サービス」それに「ウイルス監視･ウイルス対策運用支援サービス」が各々の市場を形成している。また、それらの機能を統合し総合的に監視・運用支援する「セキュリティ総合監視・運用支援サービス」が最も大きな市場となっている。「ファイアウォール監視・運用支援サービス」と「IDS／IPS 監視・運用支援サービス」は多様化していくサイバー攻撃に対する防御策として新規にサービスを受けた企業が増加しプラス成長となった。それに比べて「ウイルス監視･ウイルス対策運用支援サービス」は、クラウド化への移行が実施され若干増加したものの、「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。

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。

図 20　2013 年度のセキュリティ運用・管理サービス市場



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、2013 年度は期待に反して、それ程の伸びはなかったが、2014 年度は再び二桁成長となると推測している。その要因のひとつとして、投資を控えている時

期は企業業績も芳しくなく、サービス委託量も減るし、インシデントも営業活動のトランザクション比率で低くなる傾向があるが、経済が復活し企業業績が回復すると、今度は拡大基調を守るための経営判断としてインシデントレスポンスの重要性がクローズアップされるという構造が考えられる。2013 年度以降、企業業績は上昇機運にあり、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、2013 年度の実績推定値が 1,094 億円であり、2012 年度に始めて 1,000 億円を超え、1,032 億円前年対比 5.3%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、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

3.　市場規模(億円)	2012 年度	2013 年度	2014 年度	2015 年度
セキュリティ総合監視･運用支援サービス	29,658	31,035	35,035	37,137
ファイアウォール監視･運用支援サービス	5,283	5,647	6,166	6,535
IDS／IPS 監視･運用支援サービス	6,919	7,254	8,254	8,749
ウイルス監視･ウイルス対策運用支援サービス	4,144	4,301	4,801	5,089
フィルタリングサービス	8,212	8,807	9,707	10,290
脆弱性検査サービス	13,346	14,543	15,632	16,569
セキュリティ情報提供サービス	1,897	1,953	2,053	2,176
電子認証サービス	24,700	26,236	28,412	30,117
インシデント対応関連サービス	5,342	5,717	6,617	7,014
その他の運用･管理サービス	3,689	3,886	3,931	4,167
合計	103,189	109,379	120,607	127,843
構成比				
セキュリティ総合監視･運用支援サービス	28.7%	28.4%	29.0%	29.4%
ファイアウォール監視･運用支援サービス	5.1%	5.2%	5.1%	5.1%
IDS／IPS 監視･運用支援サービス	6.7%	6.6%	6.8%	6.6%
ウイルス監視･ウイルス対策運用支援サービス	4.0%	3.9%	4.0%	4.0%
フィルタリングサービス	8.0%	8.1%	8.0%	8.0%
脆弱性検査サービス	12.9%	13.3%	13.0%	13.1%
セキュリティ情報提供サービス	1.8%	1.8%	1.7%	1.7%

構成比	2012 年度	2013 年度	2014 年度	2015 年度
電子認証サービス	23.9%	24.0%	23.6%	23.4%
インシデント対応関連サービス	5.2%	5.2%	5.5%	5.4%
その他の運用･管理サービス	3.6%	3.6%	3.3%	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	―	4.6%	12.9%	6.0%
ファイアウォール監視･運用支援サービス	―	6.9%	9.2%	6.0%
IDS／IPS 監視･運用支援サービス	―	4.8%	13.8%	6.0%
ウイルス監視･ウイルス対策運用支援サービス	―	3.8%	11.6%	6.0%
フィルタリングサービス	―	7.3%	10.2%	6.0%
脆弱性検査サービス	―	9.0%	7.5%	6.0%
セキュリティ情報提供サービス	―	2.9%	5.1%	6.0%
電子認証サービス	―	6.2%	8.3%	6.0%
インシデント対応関連サービス	―	7.0%	15.7%	6.0%
その他の運用･管理サービス	―	5.3%	1.2%	6.0%
合計	―	6.0%	10.3%	6.0%

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、2013 年度の推定実績市場規模は 310 億円（前年度比成長率+4.6%）2014 年度もプラス成長を続け、 2015 年度には 371 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」、「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

2013 年度それぞれ 56 億円（前年度比成長率+6.9%）、73 億円（同+4.8%）、43 億円（同+3.8%）

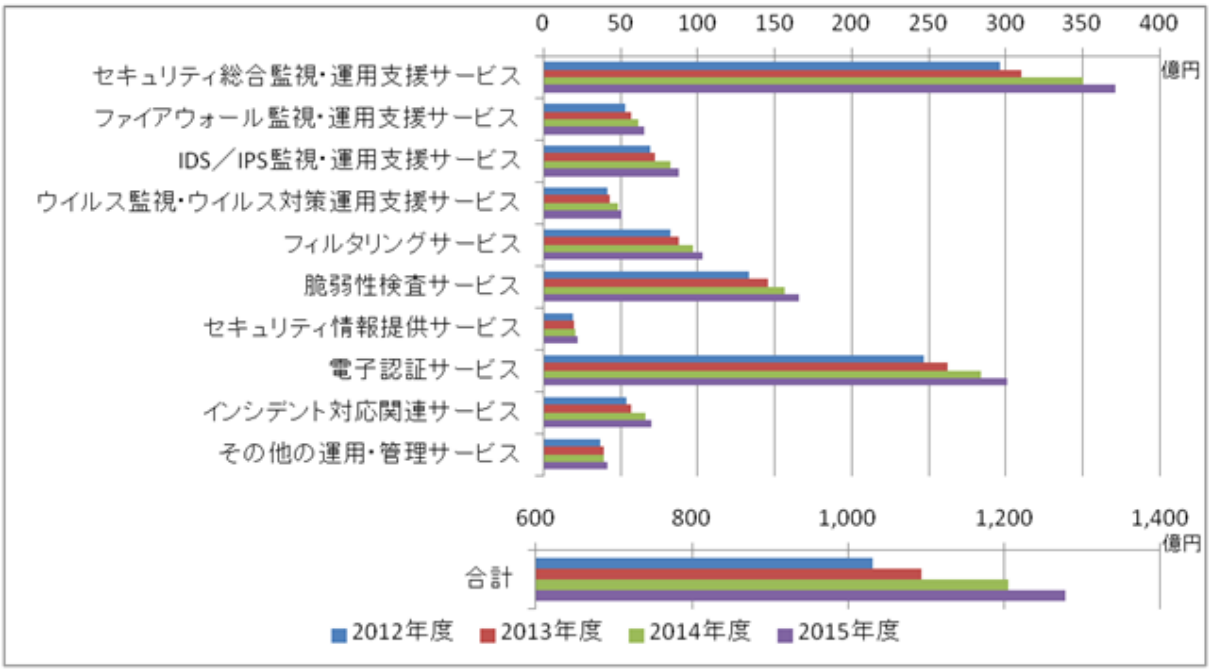
2014 年度それぞれ 62 億円（同+9.2%）、83 億円（同+13.8%）、48 億円（同 11.6%）

2015 年度それぞれ 65 億円（同+6.0%）、87 億円（同+6.0%）、51 億円（同+6.0%）と増加していく見込みである。

クラウド化が進み、社内システムからの外部委託サービスへの移行が増加している「フィルタリングサービス」は、2013 年度に 88 億円（同+7.3%）と大幅成長を遂げた。2014 年度には 97 億円（同+10.2%）、2015 年度には 103 億円（同+6.0%）と 100 億円市場が見込まれる。

近年特に多様化・複雑化する脆弱性やインシデント対応に向けた専門性の高いサービスの需要拡大を受けて、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。2013 年度においては 145 億円（同+9.0%）、2014 年度には 156 億円（同+7.5%）、2015 年度には 166 億円（同+6.0%）と、順調に成長していくと思われる。

図 21　国内セキュリティ運用・管理サービス市場推移



「セキュリティ情報提供サービス」については、2012 年度で 20 億円（同+2.9%）と安定した市場である。2014 年度、2015 年度も金額では 20～22 億円前後と飛躍的な増加はないものの安定して市場を形成していくと思われる。全般的に言えることでもあるが特定の従事者に依存した市場による高齢化、CERT 的な情報発信や SNS・Web ニュースによる速報性とのトレードオフなど、次の世代への課題もある。

「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 2013 年度は 262 億円（同+6.2%）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。2014 年度は 284 億円（同+8.3%）、2015 年度は 301 億円（同+6.0%）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ため、2013 年度は 57 億円（同+7.0%）となった。2014 年度以降もサイバー攻撃等の外部要因的なリスクが継続して発生する可能性が高く、また初動体制の不備が大きな損出につながることが報道等を通じて周知されてきていることから、2014 年度は+15.7%の 66 億円と非常に大きな成長を見込んでいる。2015 年度には 6.0%伸びて 70 億円市場になると見込んでいる。

2.2.2.4. 情報セキュリティ教育市場

(1)　市場動向

図22に2013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 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。

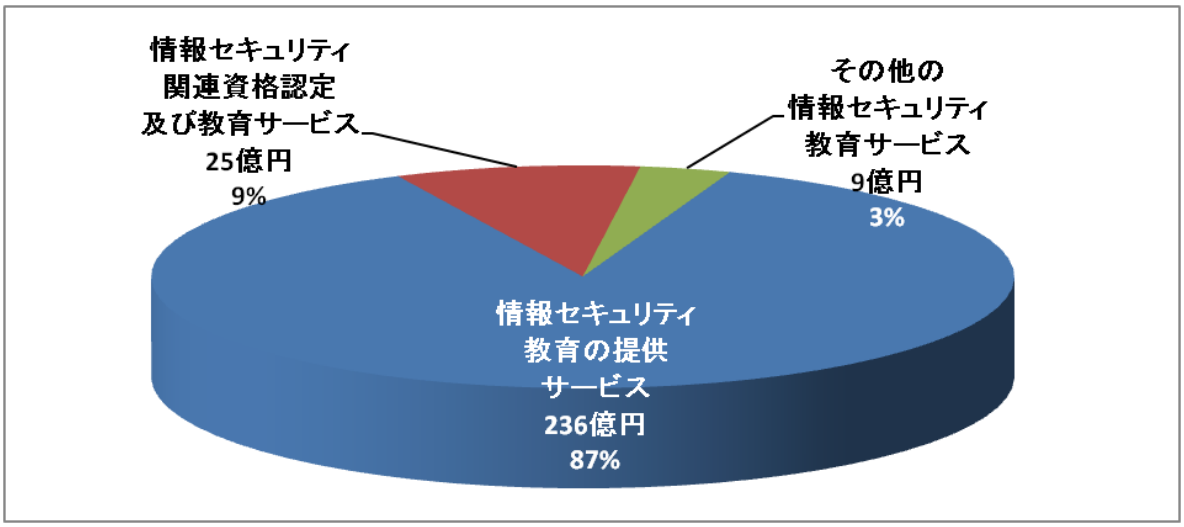
② システム関係部署や情報セキュリティ対応部署に対する専門教育。

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　2013 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。

「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、2012 年度の市場規模は 266 億円程度と推測さる。2013 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、1.5%増の 270 億円となった。

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）	2012 年度	2013 年度	2014 年度	2015 年度
情報セキュリティ教育の提供サービス	23,309	23,575	24,575	25,803
情報セキュリティ関連資格認定及び教育サービス	2,387	2,483	2,483	2,607
その他の情報セキュリティ教育サービス	878	922	922	968
合計	26,574	26,979	27,979	29,378
構成比				
情報セキュリティ教育の提供サービス	87.7%	87.4%	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	9.0%	9.2%	8.9%	9.1%
その他の情報セキュリティ教育サービス	3.3%	3.4%	3.3%	3.2%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
情報セキュリティ教育の提供サービス	－	1.1%	4.2%	5.0%
情報セキュリティ関連資格認定及び教育サービス	－	4.0%	0.0%	5.0%
その他の情報セキュリティ教育サービス	－	4.9%	0.0%	5.0%
合計	－	1.5%	3.7%	5.0%

2014 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、3.7%

成長して 280 億円程度になったものと推測される。2015 年度も同じ増大傾向が続くものと見られ、5.0%増で 294 億円規模に達するものと予測する。

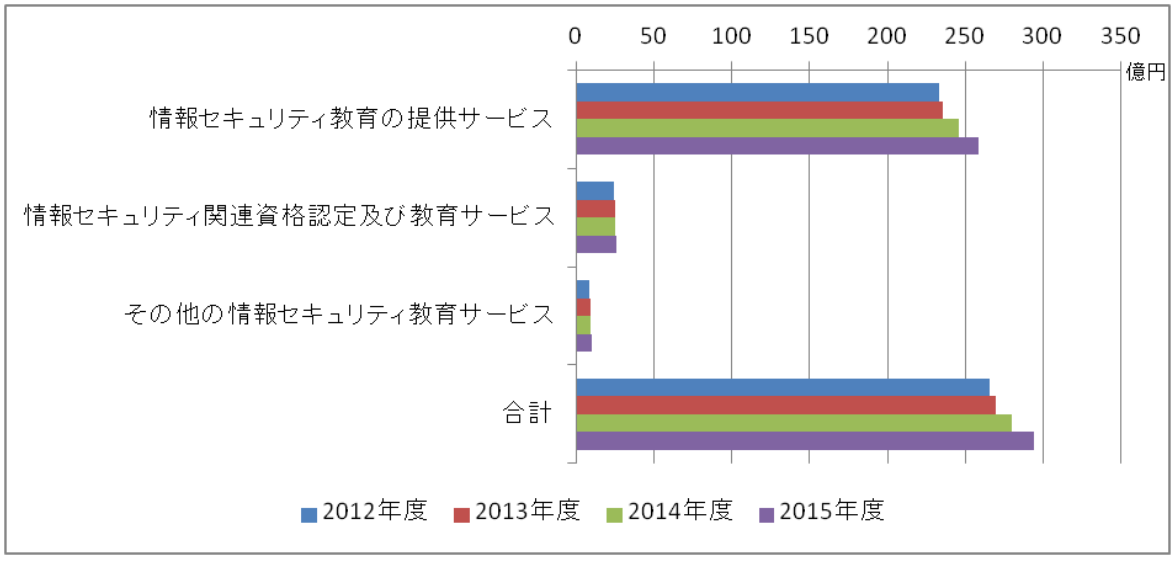
ただし、このセグメントの大部分87～88%を占める「情報セキュリティ教育の提供サービス」が成長を牽引しており、ここには上記で触れた「情報セキュリティ教育のe-ラーニングサービス」が含まれる。市場規模は2012年度に233億円、2013年度には236億円（前年度比成長率+1.1%）、2014年度には246億円（同+4.2%）、2015年度は258億円（同+5.0%）と、拡大すると予測される。

一方、「情報セキュリティ資格認定及び教育サービス」は、2012年度において24億円のマーケットであり、2013度には前年度比4.0%増の25億円の規模になったと推測される。

2014年度は情報漏えい事件・事故の発生により即効性を伴わない資格取得需要が一時的に飽和し、資格取得者の現場での生産性が求められる事情などから、教育の提供側に投資が偏る傾向が起こると思われるため、前年度比横ばい0%成長の25億円を予想している。

2015年度にはその反動もあり、他の市場セグメント同様5.0%増の26億円の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、新たな展開が期待できる。

図 23　国内情報セキュリティ教育市場推移



2.2.2.5. 情報セキュリティ保険市場

(1) 市場の動向

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

情報セキュリティ保険の供給主体は、法律上損害保険事業者に限定される。主として大手の損害保険会社からさまざまなバリエーションの IT 保険、情報セキュリティ保険が提供される。SI 事業を営む大手電機事業者が、SI 事業者の商品・サービスの品揃えの一環としてグループ内損保子会社または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。

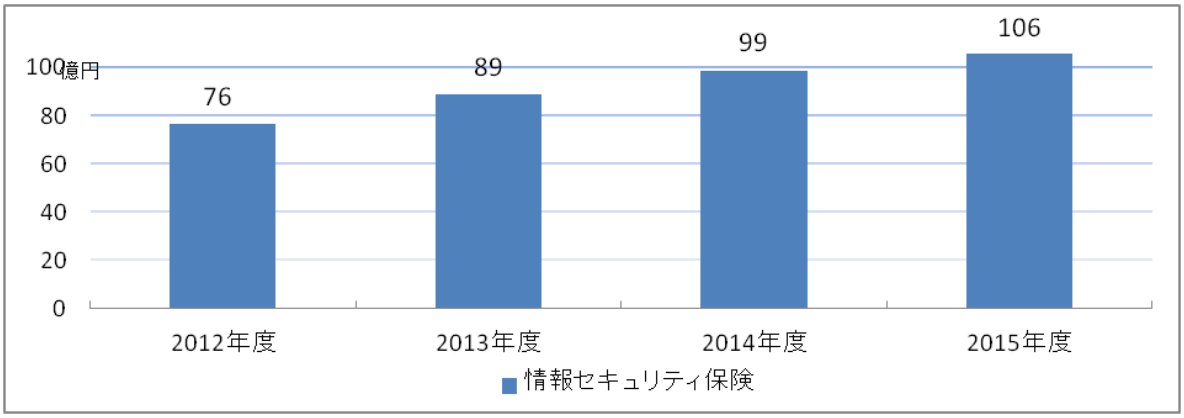
(2)市場規模とその推移

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）	2012 年度	2013 年度	2014 年度	2015 年度
情報セキュリティ保険	7,640	8,885	9,885	10,577
対前年比成長率（%）	－	16.3%	11.3%	7.0%

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、近年は拡大のペースが上がっていると見られる。2012 年度の市場規模は 76 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大企業を中心に保険契約が増加する傾向を示しているものと考える。その結果 2013 年度は 16.3%増の 89 億円、2014 年度は 11.3%増の 99 億円となり、2015 年度は 7.0%増の 106 億円と 100 億円市場にまで駆け上がる注目市場と見ている。

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　2015 年度におけるネットワークの脅威の動向

IPA セキュリティセンターは、2015 年 4 月 3 日に「10 大脅威 2015　～被害に遭わないために実施すべき対策は？～」[9]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。　（IPA 各年度発表をもとに JNSA 作成）

表 15　最近 3 年間の IPA10 大脅威の推移

	2015 年	2014 年	2013 年	2012 年
第 1 位	インターネットバンキングやクレジットカード情報の不正利用	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
第 2 位	内部不正による情報漏えい	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
第 3 位	標的型による諜報活動	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	ウェブサービスへの不正ログイン	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	ウェブサービスからの顧客情報の窃取	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	ハッカー集団によるサイバーテロ	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	ウェブサイトの改ざん	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
第 8 位	インターネット基盤技術を悪用した攻撃	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？
第 9 位	脆弱性公表に伴う攻撃	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	悪意のあるスマートフォンアプリ	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

[9] http://www.ipa.go.jp/security/vuln/10threats2015.html

2014 年版の見出しは「複雑化する情報セキュリティ」である。2013 年版は「身近に忍び寄る脅威」、2012 年版は「変化・増大する脅威」であった。2015 年版は「被害に遭わないに実施すべき対策は？」となっており、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きていることで実際に被害が増えていくことを示している。4 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。

2015 年はインターネットバンキングやクレジットカード情報の不正利用が 1 位になっており、一般ユーザに直接的な被害をもたらす可能性が高まっている。ただ、一般ユーザだけではなく、法人口座も攻撃の対象となってきており、企業としても対策が必要になってきている。

また、4 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 サイトがなくならない上に、ドライブバイダウンロード[10]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。

更に、2015 年は 2014 年には一旦ランク外になっていた、内部不正による情報漏えいが再度上位にランクインしてきいる。昨年度発生した、大手サービス提供会社の内部犯行による顧客情報の窃盗事件などの「個人情報の漏えい」や、社員が転職先へ不正に技術情報を漏えいさせる事件などの「技術情報の漏えい」といった問題も発生している。

---

[10] 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

3.2　日本の組織で求められる「内部統制」の形について

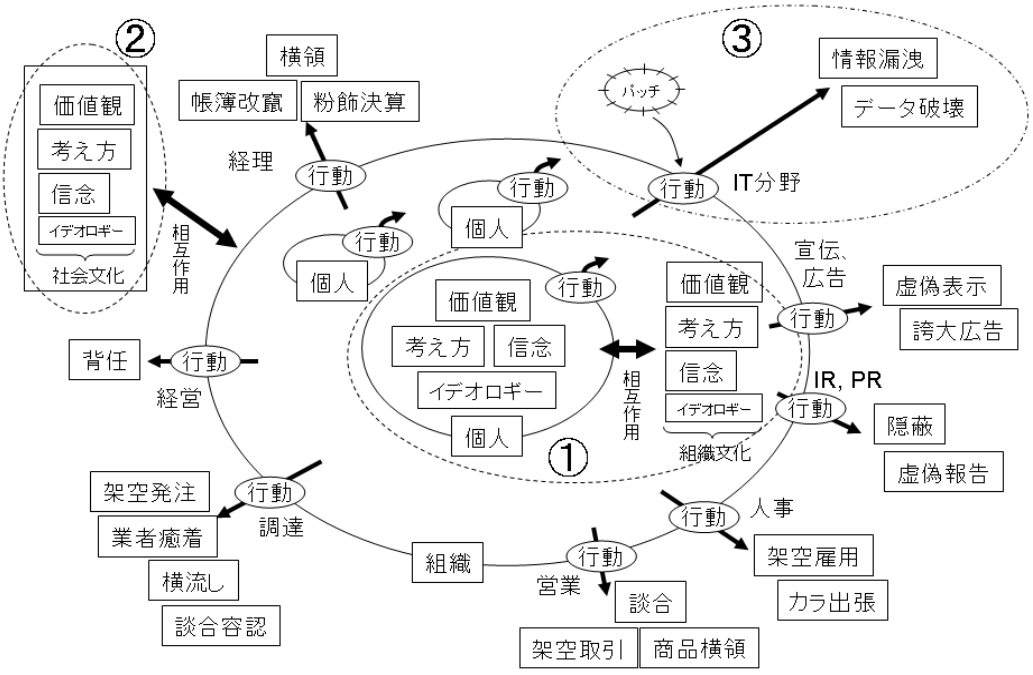
・はじめに　～ 組織運営を圧迫する大きな要因 ～

昨今、組織の内部関係者の手による意図的な情報漏えいによって、その組織のオペレーションが阻害される事故がしばしば見られるようになっている。組織の関係者による情報漏えいは、重要な内部不正(事故)ではあるが、組織の内部に要因がある事故はそれだけに限らない。その他の、組織の関係者による違法（脱法）行為、ルール違反に関係する事故としては、使い込み、内部窃盗、不正経理、取引先等との癒着、意図的不作為・隠蔽、組織の私物化（公私混同）などがあげられる。これらの事故は組織内部の問題として水面下で処理されることも少なくなく、顕在化することはあまり多くはない。しかしながら、これらの事故が、組織や社会に及ぼす影響は決して無視できるものではない。米国では、ビジネスが廃業に追い込まれたケースの相当数が、従業員の内部不正によって起こったと報告[1]されている。

日本においても、公になっているものは少ないものの、米国と同様に、組織における内部要因によって発生する事件、事故は発生する頻度は決して低いわけではなく、組織運営を圧迫する大きな要因の一つとなっている[2],[3]。組織で働く従業員などの関係者が引き起こす違法（脱法）行為、ルール違反への対応は、顕在化はしていないものの、社会的に具体的なソリューションが渇望されている分野ということである。

・JNSA・組織で働く人間が引き起こす不正・事故対応ワーキンググループにおける議論

図 25 に NPO 日本ネットワークセキュリティ協会(JNSA)「組織で働く人間が引き起こす不正・事故対応ワーキンググループ(内部不正 WG)」が、議論のために作成した「組織で働く人間が引



（出典）甘利康文：組織で働く人間が引き起こす不正・事故対応 WG, JNSA Press, Vol.35, pp.6-7 (2013)

図 25　「組織で働く人間が引き起こす不正」発生モデル

き起こす不正」のモデル [4]を示す。組織で働く人間の行動は、その人間の価値観や考え方が表出したものである。

この行動が、組織や社会にとって好ましくない形で立ち現れたものが内部不正・事故となる。この行動が IT 分野において行われたものが、情報漏えいなどの情報セキュリティ関連の事故である。一方、個人の行動が、組織や社会にとって好ましくない形で立ち現れるのは、組織の活動の広範な分野に及び、IT 分野に限られるものではない。情報漏えいに対する対症療法(パッチ)的ソリューション(図中③)は世に多くあり [5]、情報セキュリティ関連事故への対策として一定の効果は認められるものの、それだけでは組織における内部不正・事故の対策として十分ではないのではという問題意識を表したものがこの図である。

・情報漏えい以外の組織事故を防ぐシステムが求められる

犯罪学の分野では、「犯罪機会を減らすことによる防犯」を考える犯罪機会論をベースとした環境犯罪学の考え方が主流となり、それをもとにした防犯対策が相当の効果を発揮している。組織の内部関係者による情報漏えい事故へのシステム的な対策は、情報システムという環境を変えることによって内部不正を行いにくくするという意味で、「IT 分野における犯罪機会を減らすことによる内部不正対策」という理解が可能である。一方、事故の如何によらず「組織のオペレーションが阻害されないこと」というセキュリティの本質 [6], [7]に立ち返ると、情報漏えい事故に対する対症療法的対策だけでは、組織の内部要因事故に対するセキュリティ対策としては必ずしも十分とは言えない。

現在、組織の活動の大部分は、情報システムを使って行われている。組織の「内部統制」支援を、情報システム的な観点に限って考えた場合でも、横領や粉飾決算、背任などの情報漏えい以外の組織内不正などの事故を、リアルタイムに把握し、それを出来ないようにするソリューションが求められているのは間違いないだろう。

・運用的対策で内部統制を強化しようとする際の課題

ここまで述べたように、現在、「組織の内部要因事故」のうちの情報漏えいなどの IT 的な事故に対しては、主に情報システム上で技術的な対策がなされ、横領や粉飾決算、背任などのその他の事故については、主に、内部統制ルールの厳正化と監査の徹底のような形で、運用的対策がなされるのが普通である。

内部統制ルールの厳格化、監査の徹底といった、運用的対策による「組織の内部統制強化」の世界的な潮流は、もともとはエンロンやワールドコムなどの巨大企業が、内部不正によって破綻したことがきっかけとなった米国の内部統制の厳格化に端を発している。そのため、運用的対策の理論や方法論、ノウハウなど [8]は、米国の組織に適用することを前提として開発され、発展してきたものである。各国が、自国において内部統制を強化するルールや制度を作る際の雛形としている内部統制の制度的基盤(SOX 法、COSO フレームワークなど)も、そもそもは米国内の組織に適用するために作られたものである。

日本においても、米国発のこの世界的な潮流に乗る形で、組織における内部要因事故を抑制するためのルールや制度が作られてきている。しかし、この「組織の内部統制強化」の諸施策は、

そのままの形で日本の組織に適用しようとしても、見えないバリアのようなものに邪魔され、必ずしもスムーズには進んでいないようにも見受けられる。

組織の内部統制を強化するためのさまざまな制度は、基本的には米国の組織に適用することを想定してデザインされたものである。米国の組織は、「人々が契約(合意の取れたルール)によって結合している『社会』」としての性格が強い。そのため、「社会」としての性格が強い組織への導入を前提としてデザインされた各種制度は、「人々が暗黙的な一体感によって結合している『世間』」の性格が強い日本の組織に、その本質的なところが合わない。これが、日本の組織に内部統制などの米国生まれの諸制度が、必ずしもうまく定着していかない大きな理由であると考えられる。

・そこには、ルールで統制された「社会」は無く、代わりに「世間」が存在する

日本人が日々活動し、生活する場所から、そこに存在する「人と人との関係」を、学術的な考察対象として、改めて「世間」というコトバ(シニフィアン[11])で分節した阿部は、世間を「自分と利害関係を持つ人々と将来持つであろう人々を総称する概念」と定義した[9]。ここでは組織事故との関係を考えるにあたり、世間を「何らかの主観的な帰属意識を媒介とした利害を共にする複数の人々からなる集団」と再定義する。このように考えると日本人が働く組織(職場)は、「世間」そのものであり、日本の「人々が活動している場」は、「組織(世間)をとりまく大世間」ということになる。

現代に生きる日本人は、この「世間」というコトバで表されるモノ(シニフィエ[12])を指し示す名詞として「社会」ではなく「実社会」というコトバをしばしば使う。「実社会」というコトバで表される「実際に自分の周りにある世界」が、「社会」というコトバが指し示すモノとは異なるものであることに、無意識のうちに気がついているからであろう。

「社会」も「個人」も、今では普通に使われる日本語になっているが、これらのコトバは、明治以降に当時の先進国であった西欧の国家体制を導入するにあたり「Society」や「Individual」の概念を指し示す必要性から人工的に造られたものである。コトバが無かったと言うことは、少なくともそれまでの日本には、その(概念の)存在が無かった(意識されなかった)ということでもある[10]。これを指摘した阿部は、「社会」や「個人」というコトバ(シニフィアン)は日本語に定着したものの、これらのコトバが指し示す「そのもの」(シニフィエ)は、(今になっても)日本には存在しないとしている。

・「内部統制の諸制度」導入の際の見えないバリア

唯一神との契約という「アブラハムの宗教[13]」の影響がその根底に流れている欧米には、契約のベースとなる「個人(という概念)」、そして、その約款であるルールをベースにして個人と個人が集合した「社会」が存在する。このルールに抵触する行為が「罪」であり、人々は、ルールによって統制されている。

---

[11] 「表記」のこと。signifiant ：意味するモノ、表すモノ。Signifier(仏:意味する)の現在分詞形。

[12] 「表記」が指し示しているモノ。signifié：表されているモノ。上記の過去分詞形。(「近代言語学の父」と呼ばれるスイスの言語学者ソシュールによって定義された用語)

[13] ユダヤ教、キリスト教、イスラム教など

一方、アブラハムの宗教の影響を受けていない日本では、共に生きる人々の間で自然発生的に立ち現れる運命共同体、「世間」が根を張り、一体感という観念で人々の行動をコントロールしている。そこに生きる人間(世人)は、常に「同じ世間に属する人々からどう思われるか」を気にしながら生きている。周りの人から後ろ指を指される行為が「恥」であり、人々は「周りの人のまなざし」によって統制されている。

そのため、日本の「実社会」(大世間)を構成する「組織」(世間)で働く人々の行動を統制することを考える場合、「世間」の存在を前提とし、その特質を考えた制度設計が欠かせないものとなる[11], [12]。米国の組織に適用することを前提として開発された「組織の内部統制」に関する諸制度は、ルールによって人々が動く「社会」を前提としたものであり、人と人との関係性を重視する「世間」の存在を前提に、そこに生きる人々の行動が「世間からのまなざしによって統制を受ける」という点を考慮して制度設計されているものではない。これが、「内部統制の諸制度」を日本の組織に適用する際の、「見えないバリアのようなもの」の正体である。

・「皆が守っている」からルールを守る

Benedict は、「菊と刀」[13]で、日本文化を「恥の文化」と位置付け、人々の行動規範が、欧米では、ルール違反への「罪の意識」であるのに対し、日本では「仲間の目」からの「恥の意識」になっていると指摘した。この「恥による行動規範」を「仲間・同僚による規律」として、日本のおける組織の最も重要な社会的統制の要素と位置付ける研究[14]もある。

Benedict 流の解釈では、日本の組織に内部統制などの欧米生まれの諸制度が必ずしもうまく定着しないのは、ルール違反への「罪の意識」を自己統制の前提とするこれらの制度が、「恥の意識」を自己統制の前提とする日本の実社会では必ずしもうまく機能しないから、と言うことができる。

色々な国からの外国人乗客が乗った客船が沈没しはじめた。状況は、乗客を「海に飛び込ませる」のが最善と判断される。船長は乗客を説得して海に飛び込ませなければならない。そして船長は言った。アメリカ人には「飛び込めば英雄(ヒーロー)です」、英国人には「飛び込めば紳士(ジェントルマン)です」、ドイツ人には「飛び込むのが規則(ルール)です」、イタリア人には「飛び込むと女性にもてます」、フランス人には「飛び込まないでください」、そして日本人には、「皆さん飛び込んでいますよ」。有名なエスニックジョーク[15], [16]である。

蓋し、集団となった日本人の本質をついている。私たち日本人は、多かれ少なかれ「皆と一緒か？」、そして「周りの人々にどう思われるのか？」という行動基準を持っており、時にこの価値観が、全てに優先されて自らの行動を決めることは珍しくない。「赤信号、皆で渡れば怖くない」という一世を風靡した流行語にもある通り、私たち日本人には、「皆と一緒」なら、交通法規というルールに反することもあまり気に留めない傾向があるのは本当のところであろう。

私たち日本人は、おそらく「皆が守っている」ことでルールを守るという行動をとっている。逆に、皆がルールを守っていない場合、「周りと同じか？」を行動規範としている日本人は、容易にルールに反する行動をしてしまう。これ一つとっても、組織事故に対する「内部統制」を、運用的施策で実現するためには、「皆」、すなわち世間という存在が決して無視できないものであることが解るだろう。

ルールによって統制される「社会」とは別の存在の「世間」が根を張り、人々の行動をコントロールしている日本の組織において、「内部統制」を本当に実のあるものにするためには、「世間」の特性を考慮した日本独自の仕組みを作る必要がある。

・おわりに　～ 日本を動かしている「和の思想」という OS ～

組織の行動は、そこで働く個々人の「価値観」や「考え方」などにもとづく行動の総体として立ち現れる(図 1)。そして、組織にも、そこで働く人間と相互に影響(図中①)をし合いながら存在する、一般に「組織文化」と呼ばれる「価値観」や「考え方」などがある。それは。また組織の外の世界にも、人々の「価値観」や「考え方」の総体としての実社会の文化(図中②)が存在する。「個人の価値観、考え方」、「組織文化」、「実社会の文化」が、それぞれ影響を与え合いながら存在するということである。日本では、アブラハムの宗教をその大本とする「契約の概念」ではなく、「人と人との誼(よしみ)」を重んじる思想が、「個人の価値観、考え方」、「組織文化」、「実社会の文化」のいずれの根底にも流れており、「人々の行動」、そしてその総体である「組織の行動」、さらには「実社会のあり方」に大きな影響を及ぼしている。日本人の祖国、「和国」に根ざす「和の思想」である。

「和の思想」という OS の上で動いている(制度的な)システムに、「契約の概念」という OS 上のシステムに当てることを想定して作られたパッチを当てようとしてもうまくいかないのは当然である。これが、欧米生まれの内部統制の運用的対策が、日本で必ずしもスムーズに機能しない理由である。「和の思想」という OS の上で動くシステムには、その OS にあったパッチを設計し、実装する必要があるということである。

【参考文献】

[1] Lawrence J. Fennelly, ed: Handbook of Loss Prevention and Crime Prevention (5th Edition), Butterworth-Heinemann, Boston, USA (2012)

[2] 樋口晴彦：組織不祥事研究 ～ 組織不祥事を引き起こす潜在的原因の解明 ～, 白桃書房 (2012)
一般向けとしては、同著者の「組織行動の『まずい!!』学」(2006)、「『まずい!!』学」(2007)、「不祥事は財産だ」(2009) (いずれも祥伝社新書)がある。

[3] (一社)ロスプリベンション協会： http://j-lpa.or.jp/general/lossprevention.html　など

[4] 甘利康文：JNSA ワーキンググループ紹介 組織で働く人間が引き起こす不正・事故対応ワーキンググループ, JNSA Press, Vol.35, pp. 6-7, NPO 日本ネットワークセキュリティ協会 (2013)
http://www.jnsa.org/jnsapress/vol35/4_WG.pdf

[5] JNSA・組織で働く人間が引き起こす不正・事故対応ワーキンググループ：内部不正ソリューションガイド, http://www.jnsa.org/result/2013/surv_acci/ (2013)

[6] 甘利康文：セキュリティの上位概念的考え方について, 信学技報, Vol.105, No.687, pp.5-6 (2006)

[7] Yasufumi AMARI: The Fundamental Definition of Security, Proc. BUEE2008 (The 9th International Symposium on Building and Urban Environmental Engineering), pp.203-207, Hong Kong (2008)

[8] 不正リスク管理実務ガイド検討委員会, 八田進二編：企業不正防止対策ガイド, 日本公認会計士協会出版局 (2009) など

[9] 阿部謹也：「世間」への旅 ～ 西洋中世から日本社会へ ～, 筑摩書房 (2005)

[10] 阿部謹也：「世間」とは何か, 講談社 (1995)

[11] 甘利康文：日本で発生する組織事故に関係する「世間」という存在, JNSA Press, Vol.39, pp. 2-5, NPO 日本ネットワークセキュリティ協会 (2015)

http://www.jnsa.org/jnsapress/vol39/2_kikou.pdf

[12] 甘利康文：世間学の視座から見た組織内不正・事故抑制手法について，JNSA Press，Vol.39，電子公開版別稿，NPO 日本ネットワークセキュリティ協会（2015）

http://www.jnsa.org/jnsapress/vol39/2-1_kikou.pdf

[13] ルース・ベネディクト/長谷川松治(訳)：菊と刀 ～日本文化の型 ～，講談社（2005）

[14] 大野正和：まなざしに管理される職場，青弓社（2005）

[15] 山早坂 隆：世界の日本人ジョーク集，中央公論新社（2006）

[16] NATIONAL STEREOTYPE, http://www.nationalstereotype.com/whats-your-national-stereotype/, 他「ethnic joke sinking ship」によるネット検索で多数ヒット

【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) 2012 年度国内情報セキュリティ市場規模　推定実績値
(2) 2013 年度国内情報セキュリティ市場規模　推定実績値
(3) 2014 年度国内情報セキュリティ市場規模　実績見込値
(4) 2015 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2013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、2014 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（※本年度は実施していない）

これまでは、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ていたが、ある程度、過去の情報蓄積があるため、本年度はワーキンググループメンバの所属する企業の動向をワーキンググループ内で共有する等の方法をとり、ヒアリングは実施しなかった。

(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。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。2014 年度、2015 年度の市場規模推定にあたっては、2013 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。

過去のアンケート調査やヒアリングにおいて収集した回答（事業計画、売上予測等）の数値と、その成長率等を参考データとして、集計時の補正に用いた。予測値または計画値については、従来から実数による調査が困難な傾向があることから、売上高成長率による回答を蓄積し、他の経済成長指標も参考にした。同業者の複数の情報を合わせる事で、供給サイドや需要サイドのマクロの方向感を得ることも行った。

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。

ひとつの製品を開発、仕入れ販売、インテグレート、サービス付加・再販して、利用者に辿り着く商流を細かく実態に則して捉え、2 重に営業収入(売上)が計上されないよう、業態毎・製品カテゴリに補正を加えた。

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、2014 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

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

	状態(いわゆるブレードサーバ型)は含まない。
ソフトウェア	パッケージ製品、ダウンロード製品、ライセンス販売製品等、定型化されたもの 一部カスタマイズの場合は対象に含め、完全な個別開発ソフトウェアは含まない
AV	Anti Virus アンチウイルス
FW	Firewall ファイアウォール
IDS	Intrusion Detection System 侵入検知システム
IPS	Intrusion Prevention/Protection System 侵入防止システム
PKI	Public Key Infrastructure 公開鍵暗号基盤
SSL	Secure Socket layer 暗号通信の一方式
URL	Unifie Resource Locator 統一資源位置指定子
VPN	Virtual Private Network 仮想私設通信網
PCI DSS	Payment Card Industry Data Security Standard PCI データセキュリティ基準
QSA	Qualified Security Assessors 認定審査機関
ASV	Approved Scanning Vendors 認定スキャンベンダー

5.2. 情報セキュリティツールの市場分類定義表

表 17 情報セキュリティツールの市場分類

大分類	中分類	定義、説明、例示 等
統合型アプライアンス		
「ネットワーク脅威対策製品」と「コンテンツセキュリティ対策製品」に分類される機能のいずれかまたは両方を備え、2つ以上の大分類カテゴリにまたがる複数の機能を1台(またはセット)で提供するアプライアンス製品。	統合型アプライアンス	アンチウイルス・アンチワームウイルス・不正プログラム対策(スパム対策・フィッシング対策機能を併設するものを含む), FW, IDS／IPS, VPN のうち、少なくとも二つ以上の機能を装備したアプライアンス製品。(いわゆる「複合脅威対策」<Unified Threat Management =UTM=>製品でアプライアンス型であるもの) 二つ以上の大分類カテゴリにまたがる複数の機能を1台(またはセット)で提供するアプライアンス製品でUTM以外のもの。 ただし、FWとVPNだけの組み合わせはファイアウォールアプライアンスに含める。
ネットワーク脅威対策製品		
主としてネットワークの境界付近に配置して通信のハンドリングまたはモニタリングを行い、設定に基づいてネットワーク通信の許可･不許可、アラート、ログ生成等、通信の制御と管理を行う製品。 通信パケットに暗号化を施し、組織外のネットワーク上でのパケット内容の盗聴・改ざんを防止する、いわゆるVPN(Virtual Private Network)製品を含む。 ファイアウォール、VPN製品、侵入検知･侵入防止製品(IDS／IPS)等を含む。	ファイアウォールアプライアンス／ソフトウェア	ネットワーク上の通信を解析し、送信元アドレス、送信先アドレス、プロトコルの種類、ポート番号、通信のステータス等の情報に基づき、あらかじめ設定されたルールまたはポリシーに従って、通信の許可、遮断、制御を行う製品。 VPN機能を併設するものを含む。 アプライアンス型製品、ソフトウェア型製品の双方を含む。
	VPNアプライアンス／ソフトウェア	ネットワーク上の通信に暗号化処理を施して、通信経路上で第三者からの盗み見、改ざん等を防止し、閉じたネットワークのような通信を可能にする機能(VPN= Virtual Private Network=機能)を提供する製品。SSL(Secure Socket Layer)−VPNを含む。 アプライアンス型、ソフトウェア型(サーバ=ゲートウェイ=型、クライアント型)の双方を含む。 ファイアウォールにVPN機能が付帯する場合はファイアウォールに分類。
	IDS／IPSアプライアンス／ソフトウェア	侵入検知(Intrusion Detection System =IDS=)・侵入防止(Intrusion Prevention System または Intrusion Protection System =IPS=)、すなわち、ネットワーク上の通信の内容や状態を一定の方法・技術に基づき解析し、侵入もしくは攻撃と判断される通信に対して報告･警告･遮断･阻止・監視･ログ記録等の対策を行う製品。

			アプライアンス型製品、ソフトウェア型製品の双方を含む。
		アプリケーションファイアウォール	アプリケーションサーバへのネットワーク通信を監視･解析し、不正侵入その他の攻撃･悪用を目的とする通信に対して報告･警告･遮断･監視･ログ記録等の対策を行う製品。 アプライアンス型、ソフトウェア型の双方を含む。 典型的例として、Webアプリケーションファイアウォールがある。データベースサーバの保護を主目的とするものを含む。
		その他のネットワーク脅威対策製品	外部ネットワーク（インターネット等）から内部ネットワークに対して行われる、不正侵入、盗聴、不正プログラムの挿入等の攻撃に対して、検知、防御、抑止、警告等の防衛の機能を提供する製品で他の中分類に属さないもの。
コンテンツセキュリティ対策製品			
	1. コンピュータウイルス、スパイウェア、ボット等の不正プログラム（マルウェア）等を、ファイル等の電子データや電子メール送受信・Web閲覧等のコンピュータ通信の中から検出し、排除･無害化･警告等の対策を講じる機能を持つ製品群。 2. システム･業務･サービスの目的や適正な運営にとって有害な電子メール送受信やWeb閲覧等の通信を検査し、フィルタリング・警告･排除・ログ記録その他の対応を行う機能を持つ製品群。 3. 電子メール、電子ファイル等の内容（コンテンツ）について、ポリシー等あらかじめ設定された条件に基づいて、その送信・移送・受け渡し等の移動、複製・閲覧・編集・印刷等の加工その他の利用を阻止・防止もしくは制限し、または警告・報告・記録等を行う、情報保護のための製品群。	ウイルス・不正プログラム対策ソフトウェア（企業向けライセンス契約）／アプライアンス	ウイルス、ワームその他の不正プログラムの感染や侵入を検知・防御・排除する機能を持ったソフトウェア（主として企業等向けにライセンス契約方式で提供されるもの）またはアプライアンス。プログラムや定義ファイル更新の年次参照権の販売を含む。 ゲートウェイ型、サーバ型、クライアント型の全てを含む。 付加機能としてFW、IDS、スパム対策、URLフィルタリング等の機能を併設するものを含む。
		ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ）	ウイルス、ワームその他の不正プログラムの感染や侵入を検知・防御・排除する機能を持った、主として個人使用のクライアントパソコン向けソフトウェア。主としてパッケージ形式もしくはオンラインダウンロード形式で販売されるもの。プログラムや定義ファイル更新の年次参照権の販売を含む。 デスクトップFW、HIPS（ホストIPS）、スパム対策、URLフィルタリング等の機能を併設するものを含む。
		スパムメール対策ソフトウェア／アプライアンス	無差別・大量に送りつけられる、不要もしくは有害な内容を含む宣伝・勧誘目的等の電子メール（スパムメール）をフィルタリングし、マーキング、警告、分別、排除等を行うソフトウェアもしくはアプライアンス製品。 ウイルス・不正プログラム対策製品にこの機能が併設される場合は、ウイルス・不正プログラム対策製品に分類する。
		URLフィルタリングソフトウェア／アプライアンス	インターネット上のWebサイト（ホームページ）へのアクセスや閲覧につき、そのアドレスや内容が、所定の条件（有害、危険、不適格、Reputation Serviceによるリスト等）に合致（もしくは違反）する場合に処理（停止、警告、管理者への通報、ログ保存等）を行うソフトウェアもしくはアプライアンス製品。 ウイルス・不正プログラム対策製品にこの機能が併設される場合は、ウイルス・不正プログラム対策製品に分類する。
		メールフィルタリングソフトウェア／アプライアンス	送受信される電子メールにつき、そのアドレスや内容、添付ファイル等を検査し、所定の条件（有害、不適格、情報漏えい、Reputation Serviceによるリスト等）に合致（もしくは違反）する内容を含むものに対して処理（停止、隔離、警告、管理者への通報もしくは回送、ログ保存等。）を行うソフトウェアもしくはアプライアンス製品。単に全メールを無条件にアーカイブするだけのものを除く。 ウイルス・不正プログラム対策製品にこの機能が併設される場合は、ウイルス・不正プログラム対策製品に分類する。

		DLP製品・システム（情報漏えい対策製品・システム）	Data Loss/Leak/Leakage Protection/Preventionと呼ばれる製品またはシステム。 企業内システムやネットワークから外部に向かうデータの流れ（電子メールその他のネットワークトラフィック、別のストレージへの書き込み、外部記憶媒体への書き込み、印刷等）の中に特定の特徴を含むデータがある場合、その行為に対して阻止、警告、記録等の動作を行い、外部への情報・データの流出や紛失を防止する機能を提供するシステムまたは製品。
		その他のコンテンツセキュリティ対策製品	組織内（あるいは個人）と組織外の間でネットワーク通信その他の方法で受け渡しされる電子データに関して、主としてセキュリティの目的でフィルタリングその他の機能を提供する製品で、上記のいずれにも属さない、あるいは特定の中分類に仕分けできないもの。 いわゆるDigital Rights Management(DRM)製品やシステムを含む。 いわゆるフィッシング詐欺目的で送付される電子メールのフィルタリング、フィッシングサイトへのアクセスや閲覧に対する警告、Webサイトのフィッシングに関する安全性の確認等の機能を提供する、ソフトウェア、システムもしくはサービスを含む。 （ただし、一般的なサイト証明書の発行サービスは「運用・管理サービス」に分類する。）
アイデンティティ・アクセス管理製品			
	ネットワーク資源、コンピューティング資源のユーザを電子的手段で特定し、ユーザごとに定義されたアクセス権等に基づいて、ネットワーク資源・コンピュータ資源へのアクセスや利用の許可を行う機能を提供する製品群またはシステム。 本人特定（アイデンティファイ）と認証、アクセス権限の付与と管理、電子証明の発行と管理等の各機能を、個別にあるいは総合・連携して提供する。 いわゆるAuthentication, Authorization, Access Control の機能を提供する製品群。	個人認証用デバイス及びその認証システム	ワンタイムパスワード、ICカード、USBキー、携帯電話等を用いて本人確認する機能を提供するデバイスおよびそのシステム（生体認証を除く）。
		個人認証用生体認証デバイス及びその認証システム	指紋、静脈等の生体の特長のみならず、声紋、筆跡等身体的特徴に着目して本人を特定する機能を提供するセンシングデバイスおよびその認証システム。
		アイデンティティ管理製品	システム並びにデータへのアクセス権について、システムの利用者に関してはその職務や権限に基づく定義のデータベースを、システム並びにアプリケーションに関してはそのアクセス許可ポリシーを管理する機能を提供する製品群。 利用者の異動に伴う変更管理や、システム間のアクセス権の情報連携や統合管理を実現し、情報資産の利用権の即時的一元的管理を可能にする。 プロビジョニング製品を含む。 フェデレーション製品（異システム・異組織間のID連携、プロビジョニング連携のための製品）を含む。
		ログオン管理／アクセス許可製品	ユーザがシステムにアクセスする際の承認・許可機能を提供する製品分類。 シングルサインオン(SSO)およびSSO間連携製品を含む。 但し、個人認証用および個人認証用生体認証デバイスと一体で機能するシステムは当該各デバイス及び認証システムに分類する。
		PKIシステム及びそのコンポーネント	電子証明書の発行、管理、証明サービスを提供するシステムおよびその構成要素。 但し、構築サービス(SI)は含まない。（サービス市場に分類する） なお、電子証明書の発行サービスはサービス市場に分類する。
		その他のアイデンティティ・アクセス管理製品	本人認証、アクセス権管理、ログオン管理等の機能を提供しまたはそれらに関連する機能・サービスを提供する製品で上記のいずれにも属さない製品。 ディレクトリサーバ（単独で製品化されているもの）を含む。
システムセキュリティ管理製品			

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

5.3. 情報セキュリティサービスの市場分類定義表

表 18　情報セキュリティサービスの市場分類

大分類	中分類	定義、説明、例示　等
情報セキュリティ･コンサルテーション		
1. 情報セキュリティについて、主として経営管理およびIT管理の領域において、管理のための政策、管理体系、運用体制等の構築、診断、監査に関する支援やコンサルティングを行うサービス。 2. これらに関連する規格認証枠組みに対応して認証取得を目指す場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。	情報セキュリティポリシーおよび情報セキュリティ管理全般のコンサルテーション	情報セキュリティの管理の体制や手順に関する総合的コンサルティングサービス。 情報セキュリティポリシーや管理･運用基準等の構築および見直しのサービスを含む。 情報セキュリティガバナンスの構築･取組支援サービス･コンサルテーションを含む。
	情報セキュリティ診断･監査サービス	情報セキュリティのポリシー、システム、管理体制、コンプライアンスの現状に対して診断または評価（一部では慣例的に「監査」とも呼ぶ）を行うサービス。ITシステムの弱点を擬似ネットワーク攻撃等で検査するサービスは「セキュリティ運用･管理サービス」の中に位置づける。ここでは管理体制等に対する総合的診断･評価を行うサービスを主体とするサービスを対象とする。 情報セキュリティ監査制度（経済産業省告示に基づく）における情報セキュリティ監査サービスは「情報セキュリティ関連認証･審査･監査機関（サービス）」に分類する。
	情報セキュリティ関連規格認証取得等支援サービス	情報セキュリティ監査の受審、情報セキュリティ格付けの取得、ISMS適合性認証の取得、プライバシーマーク適合認定、PCI DSS準拠認定の取得等を支援するサービス。
	情報セキュリティ関連認証･審査･監査機関（サービス）	情報セキュリティ監査（経済産業省告示に基づく「情報セキュリティ監査制度」における情報セキュリティ監査サービス）、情報セキュリティ格付け、ISMS適合性認証、プライバシーマーク適合認定等を行うサービス。 PCI DSS準拠認定を行うQSA(Qualified Security Assessors)を含む。ただし、ASV(Approved Scanning Vendors)は「セキュリティ運用･管理サービス」のうち「脆弱性検査サービス」に含める。
	その他の情報セキュリティコンサルテーション	その他の情報セキュリティ管理に関するコンサルティングサービス。 内部統制管理、事業継続管理、ITサービスマネジメント等に関連して、情報セキュリティに関わる強化･改善等を**主たる**目的として実施されるコンサルテーション等を含む。（情報セキュリティが従たるもしくは副次的目的の場合は「情報セキュリティコンサルテーション」としてはカウントしない。）
セキュアシステム構築サービス		
ITセキュリティシステム、またはITシステムのセキュリティについて、構築を支援するサービス。ただし、セキュリティツールやそのプラットフォーム自体の価格は含めず、その導入や構築といった役務･サービス部分を集計対象とする。	ITセキュリティシステムの設計･仕様策定	ITシステムのセキュリティについて、その設計、仕様の定義、要求条件の設定等の全体の枠組み、あるいは特定機能の内容について策定するサービス。
	ITセキュリティシステムの導入･導入支援	ITセキュリティシステムまたはITシステムのセキュリティに関する、システムインテグレーションサービス。 原則として設計部分を除く導入部分のみとするが、両者が不可分の場合はこの分類に集計する。
	セキュリティ製品の選定･選定支援	顧客のポリシーや要求条件に基づいて、それに適したITセキュリティ対策製品を選定し、またはそのための情報提供等の支援を行うサービス。
	その他のセキュアシステム構築サービス	その他のITセキュリティシステム構築サービス。 ITセキュリティ製品の保守･サポート等のサービスを、メーカの製品付帯サービスの再販以外に、再販事業者やSI事業者が独自付加価値として提供する場合はこの区分で集計する。

セキュリティ運用･管理サービス

1. ITセキュリティシステム、またはITシステム上のセキュリティ対策機器等の運用や管理の支援を行い、状態の監視、安全対策に対する診断、インシデント等に際しての判断や対応の実施や支援を行うサービス。 2. ITシステムの運用等に関連する各種の情報･利便･機能等を提供するサービス。	セキュリティ総合監視･運用支援サービス	ネットワークシステムのセキュリティ状態を総合的に監視し、またその運用を支援するサービス。 関連するログ解析サービスを含む。
	ファイアウォール監視･運用支援サービス	ファイアウォール等のモニタリング状況やアラート等を監視し、またその運用を支援するサービス。 関連するログ解析サービスを含む。
	IDS／IPS監視･運用支援サービス	IDS／IPSシステム等のモニタリング状況やアラート等を監視し、またその運用を支援するサービス。 関連するログ解析サービスを含む。
	ウイルス監視･ウイルス対策運用支援サービス	コンピュータウイルス等の不正プログラム等に対して監視や対策を行い、またその運用を支援するサービス。関連するログ解析サービスを含む。
	フィルタリングサービス	電子メールの送受信に際して、スパムメール等の有害メール対策や情報漏えい防止のためのフィルタリングもしくは監視を行うサービス。電子メールサーバ機能の提供と一体で提供されるサービスを含む。 インターネット上のWebアクセスに際して、ポリシーやリストに基づき警告、制限、遮断、報告、記録等の管理やフィルタリングを行うサービス。いわゆるレピュティションサービスを含む。
	脆弱性検査サービス	ITシステムの脆弱性やアプリケーションのセキュリティホールに対して、侵入検査等の擬似攻撃手法やコードの解析等によって検査･診断するサービス。
	セキュリティ情報提供サービス	インシデント、脆弱性、パッチその他のITセキュリティに関する情報を提供するサービス。 Web、メールニュース、レポート、出版等、媒体種類を問わない。
	電子認証サービス	電子証明書の発行･認証、無改ざん保証、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	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

	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。		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

[15] NI：Network Integration, ネットワーク構築

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。

最近では、セキュリティ運用監視センタ（SOC）を有し、システム、製品提供だけではなく、セキュリティ運用監視を手掛ける企業も増えて来ている。

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

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

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	507	85	104	61	99	32	27	72	27
有効推計対象	**463**	75	99	54	93	31	25	61	25
情報セキュリティツール全体（X）	298	51	70	37	51	17	17	43	12
統合型アプライアンス	79	12	23	13	14	3	3	9	2
ネットワーク脅威対策製品	142	20	29	16	28	6	12	23	8
コンテンツセキュリティ対策製品	177	36	33	28	34	11	6	24	5
アイデンティティ・アクセス管理製品	146	23	33	17	22	8	12	24	7
システムセキュリティ管理製品	146	24	31	22	25	8	10	21	5
暗号製品	88	14	19	14	14	4	7	12	4
情報セキュリティサービス全体（Y）	247	44	45	33	50	13	16	33	13
情報セキュリティコンサルテーション	140	26	26	17	31	8	9	16	7
セキュアシステム構築サービス	129	20	24	17	24	9	10	21	4
セキュリティ運用・管理サービス	160	25	29	21	35	8	11	24	7
情報セキュリティ教育	74	13	13	12	17	4	5	6	4
情報セキュリティ保険	17	3	5	2	4	1	1	0	1
（参考）									
ツール専業（X∩￣Y）	169	31	47	11	29	15	7	22	7
ツール・サービス兼業（X∩Y）	188	24	33	32	40	6	13	30	10
サービス専業（￣X∩Y）	106	20	19	11	24	10	5	9	8
生データベースの売上高分布	100.0%	9.9%	21.4%	5.4%	26.6%	0.1%	17.4%	18.7%	0.3%

また、今回調査対象企業数（有効推計対象ベース）が、2011 年度調査 358 社、2012 年度調査 422 社、2013 年度は 463 社となった。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、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 169（昨年 150）、サービスのみに特化する事業者が 106（昨年 104）、両方を提供する事業者が 188（昨年 168）と、すべての業態で参入事業者数が増加している。

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は、ご留意いただければ幸いである。

そのような留保条件、制限条項はあるものの、2013 年度は

（1） 海外ベンダの売上割合の大幅縮小：円高、日本ベンダ製品の売行き回復

（2） 国内ベンダ参入・売上割合ともに大幅増加：国産セキュリティの選択が増えた

という特徴が反映されてきており、この傾向は 2014 年 2015 年と更に強まると考えられる。

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、2013 年と 2%台の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	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
世界	5.5	5.7	3.1	0.0	5.4	4.2	3.4	3.4	3.4	3.5
日本	1.7	2.2	-1.0	-5.5	4.7	-0.5	1.8	1.6	-0.1	1.0
米国	2.7	1.8	-0.3	-2.8	2.5	1.6	2.3	2.2	2.4	3.1

（出典：IMF2015 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。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を行ったものの、2013 年も 1.6%と 1%台半ばとなり、更には増税の影響からか 2014 年はマイナス成長となっている。2015 年は増税の影響も一段落し、プラス成長する予測となっている。

図 26　日本経済の短期予測

（資料）内閣府『四半期別GDP速報』

（日本経済研究センター第 159 回改訂短期経済予測　https://www.jcer.or.jp/research/short/detail4800.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 26 は日本経済研究センターが 2015 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、2014 年度第 1 期の GDP は押し上げられる一方、2014 年度第 2 期は低成長となっている。しかし落ち込みは一時的であること予想している。

(2) 企業の経営環境と設備投資動向

今回の調査対象期間は、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り、2015 年度は大幅な増益傾向にな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%)						
2009 年度	2010 年度	2011 年度	2012 年度	2013 年度	2014 年度	2015 年度
97.3%	43.8%	−12.1%	12.8%	37.4%	5.9%	13.4%

(出所:野村証券企業業績見通し 2015 年 3 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 2015 年 3 月調査で 2014 年 12 月調査より改善している点が注目される。「先行き」についても同様となっている。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」−「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
2014 年 12 月	14	12	7	3	0	−4
2015 年 3 月	16	14	10	7	2	0

(出所:日本銀行 全国企業短期経済観測調査 2015 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。2014 年度の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 2014 年 6 月調査ではバラつきがあるものの、企業規模問わずプラスと予測している。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 2014 年度に 0.3%とわずかながらだが増加を示し、継続して 2015 年度も 2.5%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	2013 年度 実績	2014 年度 見込	2015 年度 予測
大企業	政策投資銀行	2014 年 6 月	3.0%	15.1%	−10.6%
中小製造業	政策金融公庫	2014 年 9 月	7.1%	9.0%	−
全産業*1	日本銀行	2015 年 3 月	−	5.2%	−1.7%
全産業*2			−	0.3%	2.5%
（*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 2014/8 月公表[19]、政策金融公庫中小製造業設備動向調査 2014 年 10 月公表[20]、日本銀行全国企業短期経済観測調査 2015 年 4 月公表を基に 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[21]」の中で言及されている。これによれば、システムの利用期間は 10～15 年が最も多いが、パッケージでは 5～10 年程度となる。

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

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

19 http://www.dbj.jp/investigate/equip/national/pdf_all/201408_plant.pdf
20 http://www.jfc.go.jp/n/findings/pdf/news261022a.pdf
21 http://www.boj.or.jp/statistics/tk/gaiyo/2011/tka1503.pdf

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、2013 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 26 年版[22]では、ダウンロード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。ダウロードトラフィックは 2008 年を 1 とすると、4 年後の 2012 年には 2.03 と約 2 倍になっている。ビッグデータは 2008 年から 2012 年の 4 年間で 1.83 倍と、やはり 4 年で約 2 倍になるというペースで伸びている。また 2013 年は 2012 年から約 1.3 倍になっている。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

	2008 年	2009 年	2010 年	2011 年	2012 年	2013 年（見込み）
ダウンロードトラフィック（各年 11 月・Gbps）	939	1,206	1,363	1,696	1,905	2,584
	1.00	1.28	1.45	1.81	2.03	2.75
ビッグデータ流通量（産業計・TB）	1,120,225	－	－	1,639,804	2,048,771	2,395,091
	1.00	－	－	1.46	1.83	2.14

（出所：総務省「情報通信白書平成 26 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。

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

(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）[23]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）[24]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 IT の出荷額比較		2012 年度	2013 年度	2013 /2012
		千台/億円	千台/億円	%
セキュリティ出荷計	金額	7,309	7,658	105 %
IT 出荷計(JEITA)	金額	62,606	69,016	110 %
PC 国産出荷	台数	11,152	12,109	109 %
	金額	7,952	9,263	116%
メインフレーム、サーバ、WS 出荷	台数	407	423	104%
	金額	3,779	3,608	95%
ソフトウェア	金額	7,686	7,669	100%
SI 開発	金額	23,382	27,708	119%
BPO その他サービス	金額	19,807	20,768	105%
(SW,サービス計)	金額	50,875	56,145	110%
ネットワーク機器				
生産	金額	5,454	5,369	98%
輸入	金額	6,028	6,193	103%
輸出	金額	1,351	1,481	110%
国内出荷	金額	10,131	10,081	100%
IT+NW 装置	金額	72,737	79,097	109%
セキュリティ市場との比率				
対 IT 出荷計(JEITA)		11.7%	9.0%	
対 IT+NW 装置		10.0%	10.3%	

（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」「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、2013 年度の IT 出荷は全体で前年度比 1 割増となっており、ほぼ全ての項目で前年度を上回る結果となった。特にコンピュータハードウェア単価は近年続い

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

ていた下落に底打ち感を見せており、出荷台数に比べて金額ベースでプラス幅が大きくなっている。

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。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%と徐々に上がっており、ネットワークトラフィックの増加と比例してネットワーク上のセキュリティ脅威がますます深刻度を増し、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 2013 年版[25]であり、対象年度は 2012 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による経済停滞、そこから回復の期間を経て、東日本大震災の影響が顕著に出た 2012 年度までの期間となる。2012 年度は年間事業収入規模が前年度比 0.91%と落ち込む中、情報セキュリティ対策費用はほぼ変わらない金額が維持されている。

これは度重なるセキュリティ事故を受けて、事業収入規模に関わらずに継続的な情報セキュリティ対策が必要という意識が根付き始めているのではないかと考えられる。

表 26　情報処理実態調査母集団の比較（平成 22, 23, 24, 25 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）	（%）
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%
2012 年度	5,190	8,756	659	592	0.93%	967	1.63%

（出典：経済産業省平成 22, 23, 24, 25 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 967 万円という情報セキュリティ対策費用に回答企業数 5,190 社を掛けると 5,019 億円となる。同調査の回答率は 54.6%となっており、調査対象企業全体

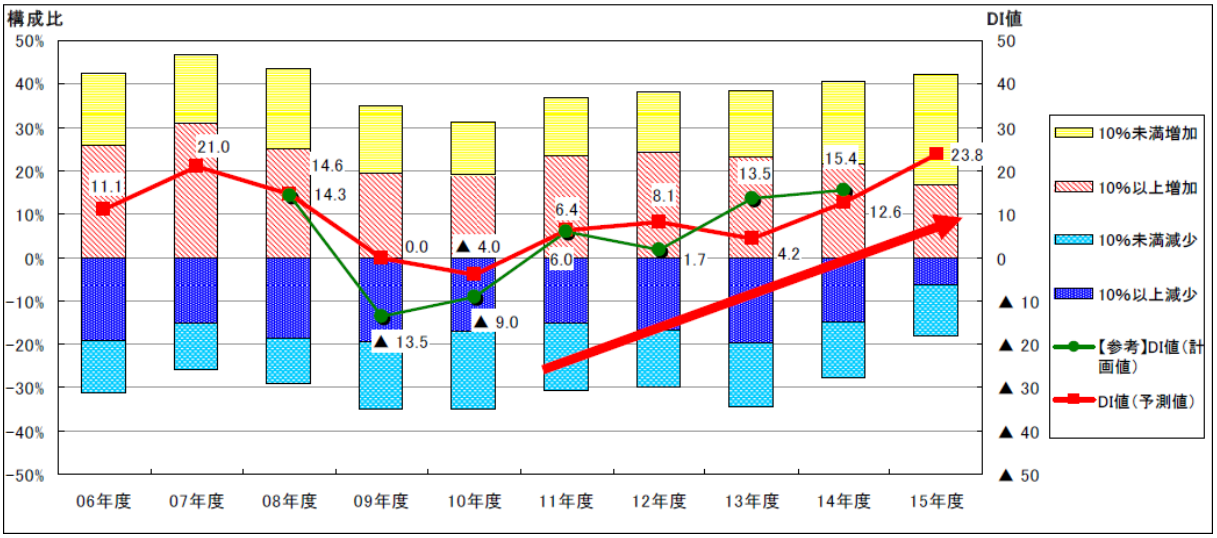
[25] http://www.meti.go.jp/statistics/zyo/zyouhou/result-1.html　（2013 年 11 月 1 日発表）

では約 9,200 億円という試算値が得られる。

(4)社団法人日本情報システム・ユーザ協会「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・ユーザ協会（JUAS）は 1994 年以来継続的に IT 動向調査を行っている。2014 年度調査結果の概要は 2015 年 4 月 15 日に公表[26]された。

図 27　IT 予算の増減の回答状況



（出典：JUAS　企業 IT 動向調査 2015 報告プレスリリースより）

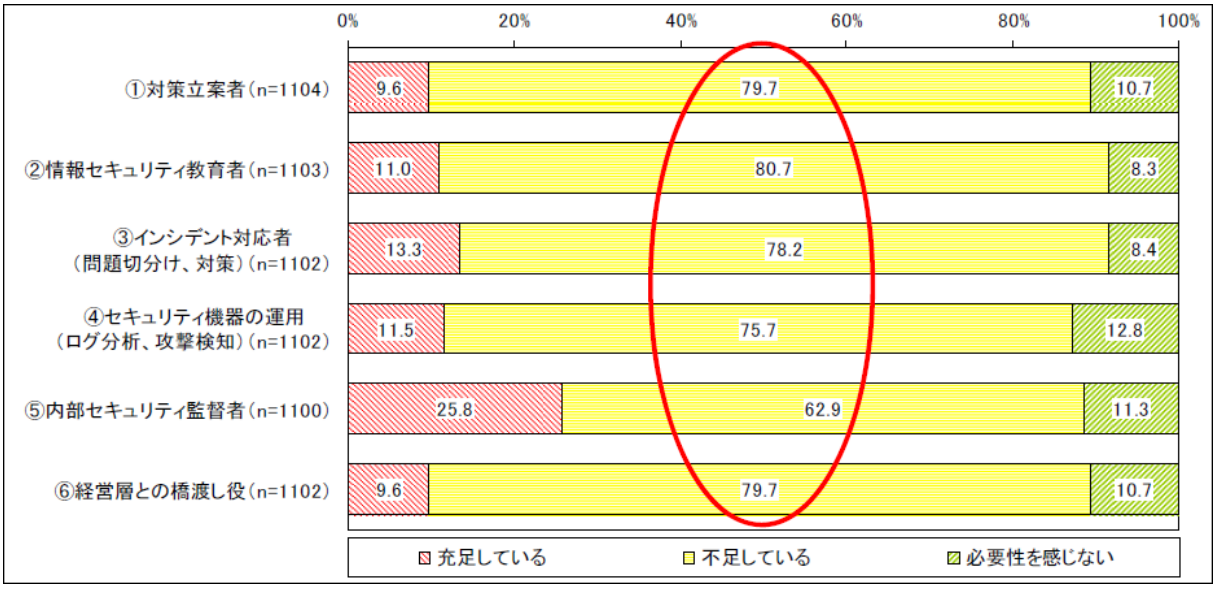
IT 支出の増減傾向を聞く定例の質問に対しては、図 27 のような回答分布となっている。IT 予算の増加と減少の差分を指数化したインデックス値を見ると、2012 年度 8.1、2013 年度 4.2、2014 年度 12.6、2015 年度（予測）23.8 となり、2015 年度の予測値はリーマンショック前の 2007 年度予測の 21.0 を 2.8%上回り、過去 10 年で最高の増加率である。（なお、アンケート調査時点は 2014 年 10~11 月）

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。最初は情報セキュリティ人材の現状を分析である。図 28 にあるように企業の 8 割で情報セキュリティ人材が不足していると認識しており、充足していると答えた企業は 1 割程度である。国内で情報セキュリティに従事する技術者は約 26.5 万人と言われており、そのうちのうち、必要なスキルを満たしていると考えられる技術者は約 10.5 万人に止まる。残り約 16 万人はスキルが不足しており教育やトレーニングを行う必要があるとされている。

不足する情報セキュリティ人材を、今後どのように育成して行くかが課題と言える。

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

図 28　情報セキュリティ人材の過不足状況

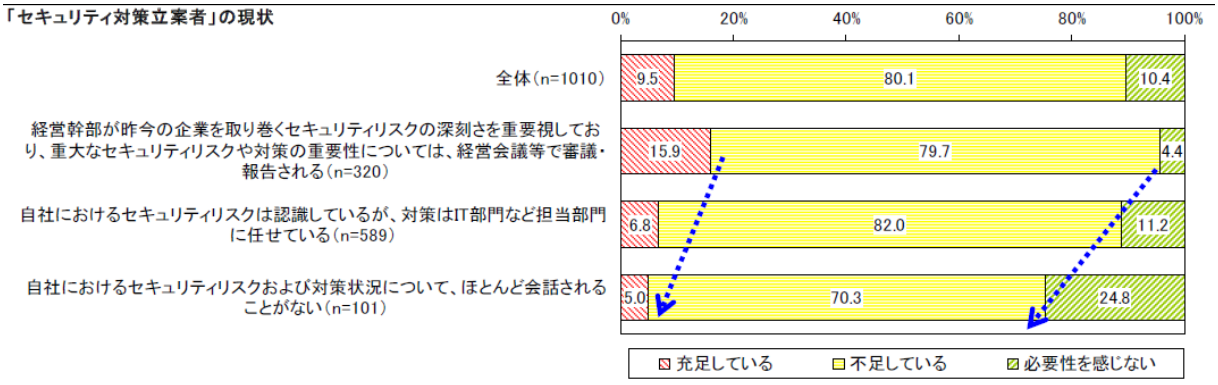


（出典：JUAS　企業 IT 動向調査 2015 報告プレスリリースより）

もう 1 点のトピックは不足している情報セキュリティ人材をいかに確保するかの分析である。図 29 のように、経営幹部がセキュリティ対策へ参画していない企業の約 8 割が「不足している」と答えており、参画しない理由として「情報セキュリティ対する経営層の理解や認識が不足している」が考えられる。逆に経営幹部がセキュリティ対策へ参画している企業ほど「充足している」と答えている。このことから、人材を確保してゆくには経営幹部がセキュリティ対策へ参画することが不可欠となる。

それには、経営幹部も情報セキュリティに対する理解や認識を深めるため情報セキュリティ教育が必要ではないか。

図 29　経営とセキュリティとの関係別「セキュリティ対策立案者の現状



（出典：JUAS　企業 IT 動向調査 2015 報告プレスリリースより）

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的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・取り組みに際し、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
2015 年 6 月 1 日 V1.0	－	初版発行
2015 年 6 月 3 日 V1.01	23 ページ 5, 49, 55, 82 ページ	誤植の訂正 記載文言の表記の統一

情報セキュリティ市場調査報告書

2015 年 6 月 1 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：JNSA

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

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
川越　弘大	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
勝見　勉	株式会社情報経済研究所
蜂巣　悌史	サブスクライバ
森田　翔	サブスクライバ

トピック執筆者（市場調査ワーキンググループメンバ外）

JNSA・組織で働く人間が引き起こす不正・事故対応ワーキンググループ

甘利 康文	セコム株式会社 ＩＳ研究所

以上