2015 年度
情報セキュリティ市場調査報告書

V1.02

２０１６年９月８日

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。2015 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ーによる議論を踏まえて全体集計・推計作業を行い、2016 年 6 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る中で急速に広まり、お茶の間の話題にまで浸透した。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。

2015 年度に入り、日本年金機構を始め多くの企業／団体に対するマルウェアばらまきメールの増加、DDoS 攻撃の増加、標的型攻撃、サイバー攻撃の更なる巧妙化／高度化が観測・確認されるようになり、これにに伴って、情報セキュリティ対策の重要性は増すばかりである。

このような状況を踏まえ、政府では、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。また、経済産業省が 2015 年 12 月に発行したサイバーセキュリティ経営ガイドラインでは、経営 3 原則、対策推進する重要 10 項目が明記され、CSIRT 等の組織、多層防御の仕組みを経営者が推進するよう求めている。

IT システムだけではなく、製造業分野でも自動車に搭載されている車載システムに対する脆弱性が多く発見されるなどの事象が報じられており、今後具体化が進むであろう IoT のセキュリティ動向にも注目する必要がある。IoT に関しては、IoT 推進コンソーシアムが立ち上がり、事業モデルだけでなく、IoT セキュリティの検討も進められる。

これら深刻化するサイバー脅威の背景には、ハクティビストによる主張に基づいた攻撃、国家の意思が背景にあるとみられる産業スパイ活動、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。政治的意図を持った DDoS 攻撃の増加、ランサムウェアを用いた脅迫事案の著増、水飲み場攻撃を足場としたネットバンキングへのハッキング被害も年々増加しており、ネットワークセキュリティは国際的にも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産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防御能力自体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。

本調査は、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と国際競争力の維持確保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

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結果の経年推移は、図１に示すとおりである。今回調査の基準年度である 2014 年度は、前年に引き続き、上昇基調は変わらず、市場規模総額は 8,428 億円に達したと推定する。今後数年の間は同様に上昇基調が継続する傾向にあると推測している。

2014 年度を振り返ると、内部犯行による史上最大規模の情報漏えい事件の発生や、インターネット基盤の根幹に関わるような広く利用されているソフトウェアの脆弱性が相次いで公表されるなど、セキュリティ担当者が様々な対応に追われる１年となった。また、インターネットバンキングをねらったフィシング詐欺など、アカウント情報を詐取する手口などによる被害の拡大が見られ、さらにはランサムウェア、標的型攻撃による被害も拡大傾向にあった。11 月にはサイバーセキュリティ基本法が成立し、国やサイバー関連諸機関などの責務や戦略、基本的施策が明確化され、日本全体のセキュリティ対策レベルを上げる意志が強まった年と位置付けることができる。

図 1　国内情報セキュリティ市場規模　経年推移

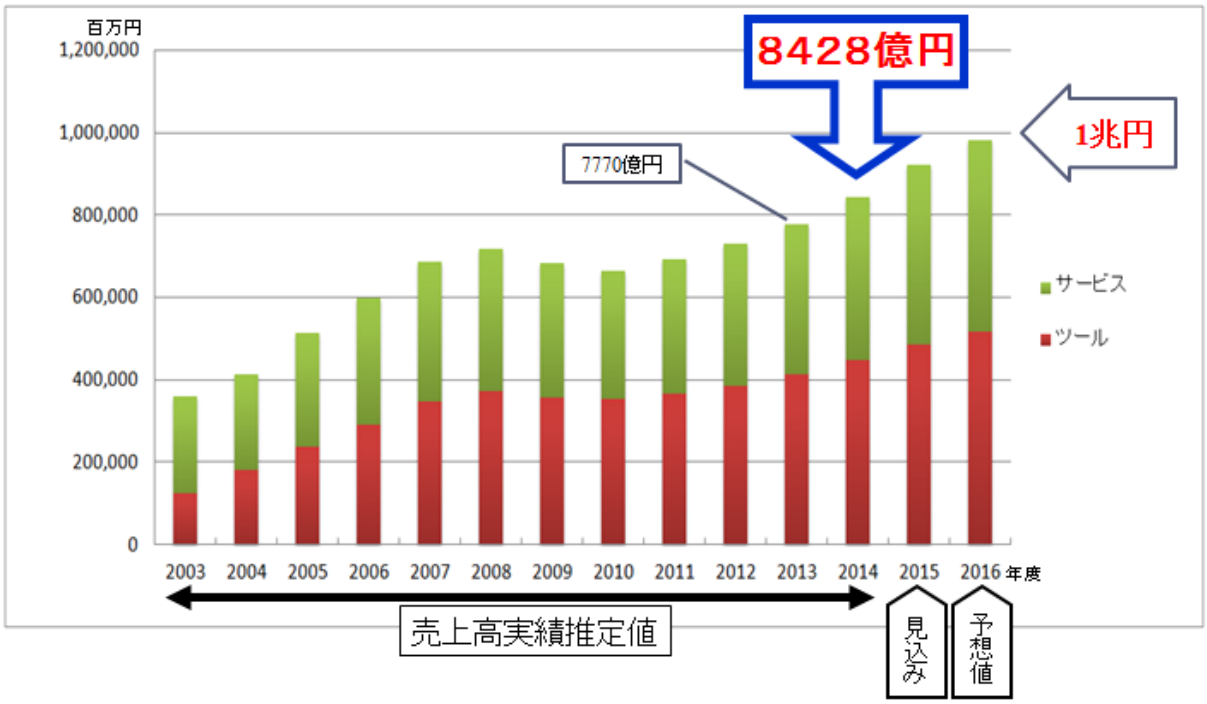


図２は、今回の調査対象年度における、情報セキュリティのツールとサービス別の市場規模推移をグラフにした。

図 2　国内情報セキュリティ市場規模　経年推移（2013 年度~）

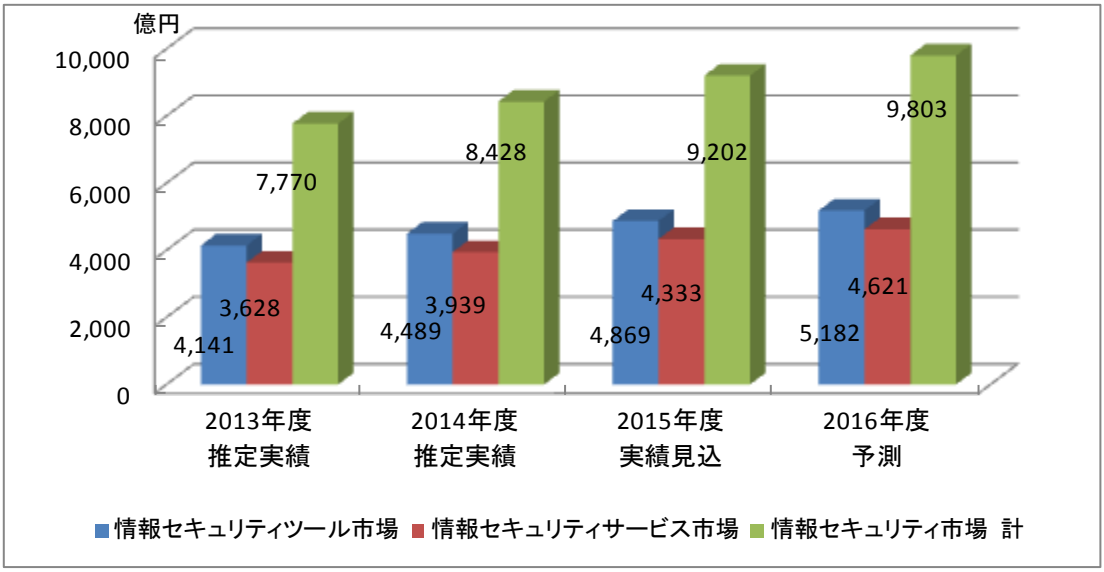


表 1 は、今回の国内情報セキュリティ市場規模推計結果の実績と予測をしめした。2014 年度の情報セキュリティ市場は、ツール市場が 4,489 億円、サービス市場が 3,939 億円、合計 8,428 億円に達したものと推定する。 また、2015 年度はコンテンツセキュリティ対策製品、システムセキュリティ管理製品や情報セキュリティ保険が顕著に伸びる中、全体で 9.2%成長し 9,202 億円と初めて 9,000 億円を突破すると予測する。

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）

年度別売上高推計値	2013年度		2014年度			2015年度			2016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	21,449	5.2%	23,622	5.2%	10.1%	25,511	5.2%	8.0%	27,297	5.2%	7.0%
ネットワーク脅威対策製品	54,482	13.2%	61,776	13.2%	13.4%	66,718	13.8%	8.0%	71,388	13.2%	7.0%
コンテンツセキュリティ対策製品	158,234	38.2%	171,192	38.2%	8.2%	185,377	37.7%	8.3%	196,091	38.2%	5.8%
アイデンティティ・アクセス管理製品	73,727	17.8%	77,220	17.8%	4.7%	82,112	17.7%	6.3%	87,934	17.5%	7.1%
システムセキュリティ管理製品	60,468	14.6%	66,288	14.6%	9.6%	75,402	14.5%	13.8%	81,108	14.7%	7.6%
暗号化製品	45,779	11.1%	48,844	11.1%	6.7%	51,774	11.2%	6.0%	54,363	11.1%	5.0%
セキュリティツール市場合計	414,139	100.0%	448,941	100.0%	8.4%	486,895	100.0%	8.5%	518,181	100.0%	6.4%

年度別売上高推計値	2013年度		2014年度			2015年度			2016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	72,731	20.0%	71,452	20.0%	-1.8%	75,778	19.8%	6.1%	79,567	19.9%	5.0%
セキュアシステム構築サービス	144,875	39.9%	156,356	39.9%	7.9%	171,992	39.2%	10.0%	180,592	39.8%	5.0%
セキュリティ運用・管理サービス	109,379	30.1%	125,248	30.1%	14.5%	138,348	31.2%	10.5%	149,419	30.7%	8.0%
情報セキュリティ教育	26,979	7.4%	30,365	7.4%	12.6%	33,603	7.2%	10.7%	36,871	7.5%	9.7%
情報セキュリティ保険	8,885	2.4%	10,479	2.4%	17.9%	13,623	2.6%	30.0%	15,667	2.1%	15.0%
セキュリティサービス市場合計	362,849	100.0%	393,901	100.0%	8.6%	433,345	100.0%	10.0%	462,115	100.0%	6.6%

セキュリティツール＋サービス	776,988	100.0%	842,841	100.0%	8.5%	920,240	100.0%	9.2%	980,296	100.0%	6.5%

このように、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昨年度より一層強く受けて、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。2016 年度には 9,000 億円台後半から 1 兆円に手が届く規模にまで拡大すると期待されるが、それは取りも直さず、情報セキュリティ対

策がより重要かつ必須の経営課題と位置付けられることの反映であり、情報セキュリティ産業の社会的責任の加重を意味するものと理解される。

尚、2016 年度の市場規模予測は、継続的な成長を予測していることから 2015 年度の傾向を踏襲している。ただ消費税増税などを見越した経済環境の不透明感から、セキュリティ対策の必要性が周知されてきつつも、純粋なセキュリティ投資を控える可能性も想定し、市場全体としては 2015 年度ほどの伸びは期待できないと予測した。

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、2014 年度の国内「情報セキュリティツール」市場は、4,489 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、2014 年度の情報セキュリティツール市場の伸びは前年比 8.4%という高い率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	2013年度		2014年度			2015年度			2016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	21,449	5.2%	23,622	5.2%	10.1%	25,511	5.2%	8.0%	27,297	5.2%	7.0%
ネットワーク脅威対策製品	54,482	13.2%	61,776	13.2%	13.4%	66,718	13.8%	8.0%	71,388	13.2%	7.0%
コンテンツセキュリティ対策製品	158,234	38.2%	171,192	38.2%	8.2%	185,377	37.7%	8.3%	196,091	38.2%	5.8%
アイデンティティ・アクセス管理製品	73,727	17.8%	77,220	17.8%	4.7%	82,112	17.7%	6.3%	87,934	17.5%	7.1%
システムセキュリティ管理製品	60,468	14.6%	66,288	14.6%	9.6%	75,402	14.5%	13.8%	81,108	14.7%	7.6%
暗号化製品	45,779	11.1%	48,844	11.1%	6.7%	51,774	11.2%	6.0%	54,363	11.1%	5.0%
セキュリティツール市場合計	414,139	100.0%	448,941	100.0%	8.4%	486,895	100.0%	8.5%	518,181	100.0%	6.4%

図 3 に 2014 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。

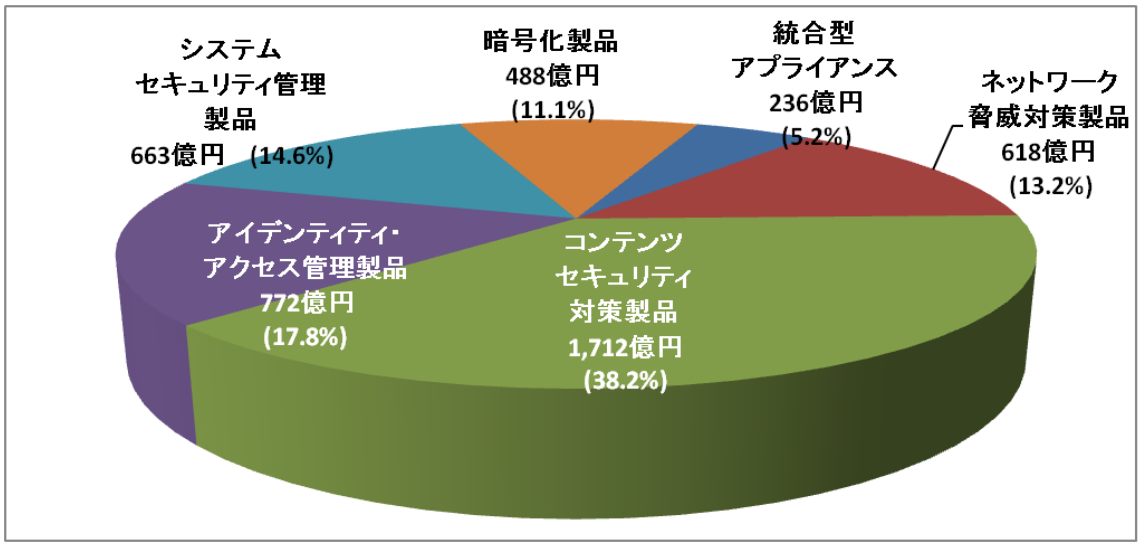
情報セキュリティツール市場において最大のカテゴリである「コンテンツセキュリティ対策製品」の 2014 年度の市場規模は 1,712 億円で、ツール市場全体に占める割合は 38.2%であった。これに次ぐ規模の市場カテゴリは「アイデンティティ・アクセス管理製品」で 772 億円、構成比で 17.8%であった。第 3 位は「システムセキュリティ管理製品」が 663 億円で 14.8%を占めた。続いて、外部からのネットワークへの不正侵入・不正アクセス対策を担う「ネットワーク脅威対策製品」と「統合型アプライアンス」は、各々618 億円・13.2%、236 億円・5.2%で、合計すると 854 億円・18.4%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 488 億円・11.1%となった。

ここ数年、以下の様な状況が観られる。

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、脅威の高まりと投資サイクルの波が重なって、2014 年度は高い伸びとなった。

図 3　2014 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。

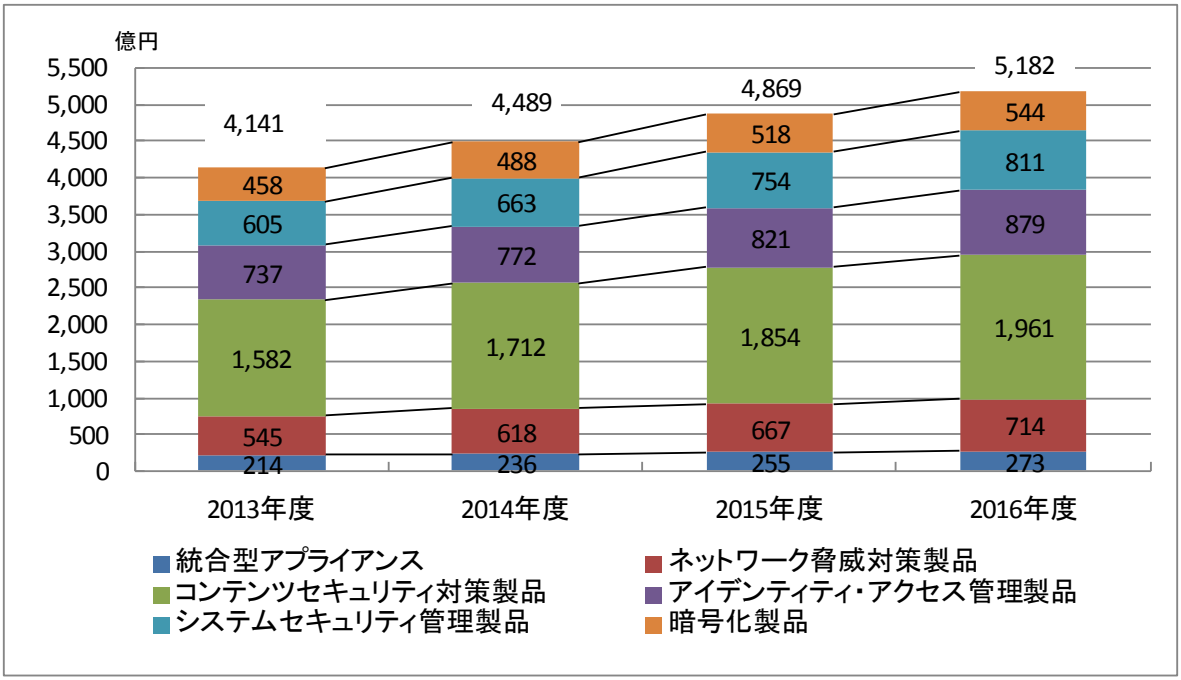
4) 標的型攻撃等、内部ネットワークへの侵入防止が困難となってきた今日の情勢を踏まえ、内部ネットワークの監視や解析、診断を行う「システムセキュリティ管理製品」も伸び率を高めている。このカテゴリには他に、端末のインベントリ・パッチ適用状態や設定等のコンプライアンス状態等を管理する製品やネットワーク検疫製品、さらにはセキュリティ目的のログ解析製品等、内部統制・情報漏えい・標的型攻撃への対応で需要が高まった製品が多く含まれ、高い伸び率を支えていると見られる。

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速めている。

図 4 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、経済回復の兆しを背景に、大規模な情報漏えい被害や相次ぐ標的型攻撃被害に対する企業サイドの自衛のための投資等、企業による脅威対策が急がれた結果、8.4%という高い成長を遂げたものと見られる。

図 4　国内情報セキュリティツール市場推移



2014 年度に最も高い伸び率を示したカテゴリ（大分類市場）は「ネットワーク脅威対策製品」で、13.4%の伸び率で、前年の 4.5%に対して大きく伸びきた。前述のとおり、サイバー攻撃の巧妙化、高度化が進む中、アプリケーション層の解析まで行う新技術を組み込んだファイアウォール製品の登場など、技術進化が市場を喚起した結果と考えられる。次に高い伸びを示したのが、「統合型アプライアンス」の 10.1%で、このカテゴリも前年の 6.6%に対して、大きく伸びてきた。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。3 番目に高い伸びを示したカテゴリは、「システムセキュリティ管理製品」の 9.6%で、前年調査同様、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。4 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 8.2%であった。ツール市場全体の 38.1%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。前年度伸び率トップであった「暗号化製品」は、6.7%の伸び率であった。伸び率は下がっているが、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、クラウドの活用に伴うデータ暗号化利用の進展などによるところが多い結果と考えられる。サーバやファイルへのアクセスを統制・管理する「アイデンティティ・アクセス管理製品」も 4.7%の伸び率を見せた。前年より伸び率は下がっているが、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。

2015 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中で、ツール市場は 4,868 億円と、2014 年度比伸び率 8.5%に達したものと推測される。

2016 年度は、サイバー攻撃対策として多層防御、IoT セキュリティ等、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+6.4%の成長率を予想。全体で 5,181 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達成できる事が普及を支えている。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た付加価値提供パッケージ型製品による事業参入もあり、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、今後も堅調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 5 にその市場規模の推移のグラフを示す。

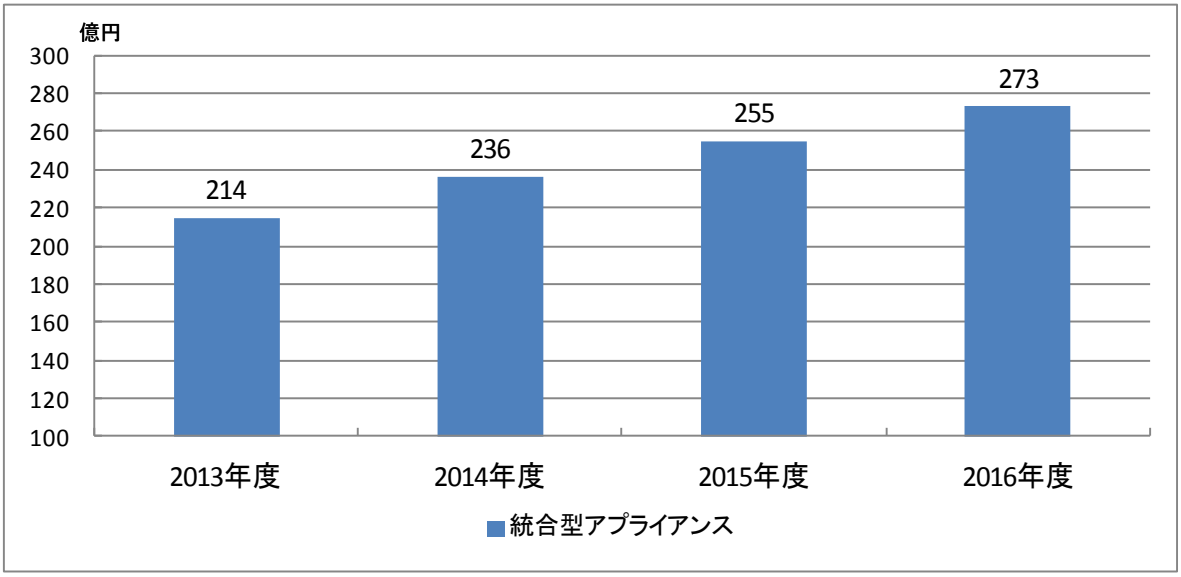
表 3　国内統合型アプライアンス市場規模　実績と予測

市場規模（百万円）	2013 年度	2014 年度	2015 年度	2016 年度
統合型アプライアンス	21,449	23,622	25,511	27,297
対前年度比成長率	－	10.1%	8.0%	7.0%

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。

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、2014 年度は 236 億円、2015 年度は 255 億円になると推測する。

図 5　国内統合型アプライアンス市場推移



2016 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、7.0%の成長で 270 億円を超えると予測する。

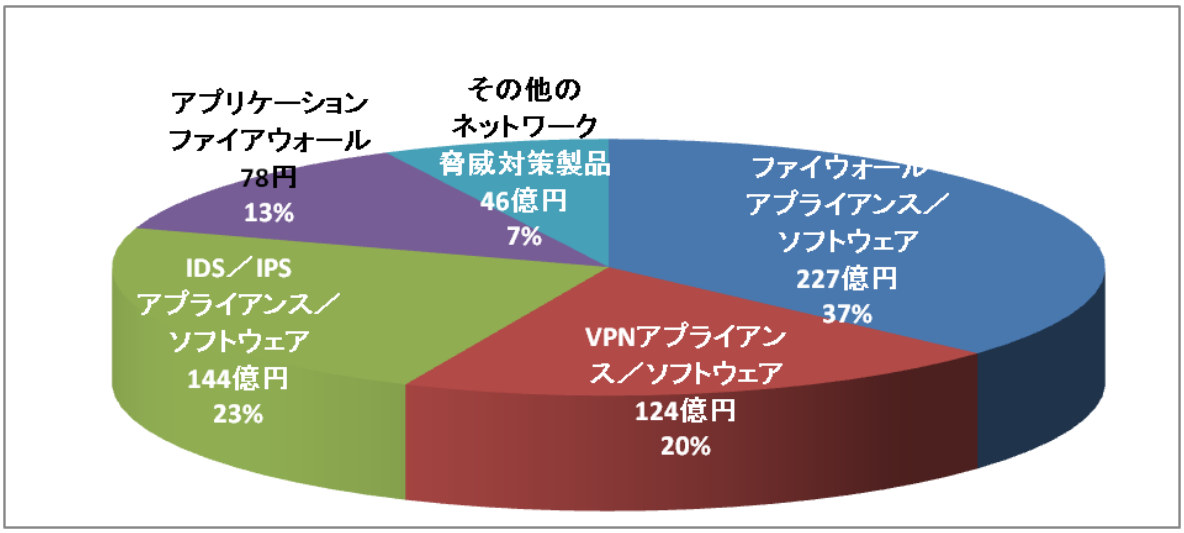
2.1.2.2. ネットワーク脅威対策製品市場

(1) 市場の動向

ネットワーク脅威対策製品の 2014 年度におけるセグメント別市場規模の分布を図 6 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 6　2014 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、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[1]が v1.2 で「ウェブアプリケーションファイアウォールの導入」を要求していることが普及に拍車をかけたと考えられる。また、IPA（独立行政法人情報処理推進機構）による推奨[2]、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[3]。

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。また、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

---

[1] 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

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

[3] 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

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きていると見られる。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必要がある。

(2) 市場規模とその推移

表4に国内ネットワーク脅威対策製品市場規模の実績推定値と予測値を、図7にその市場規模の推移のグラフを示す。

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）	2013年度	2014年度	2015年度	2016年度
ファイウォール・アプライアンス／ソフトウェア	21,168	22,672	24,486	26,200
VPNアプライアンス／ソフトウェア	11,507	12,350	13,338	14,272
IDS／IPSアプライアンス／ソフトウェア	13,440	14,355	15,503	16,588
アプリケーションファイアウォール	4,535	7,816	8,441	9,032
その他のネットワーク脅威対策製品	3,832	4,583	4,950	5,296
合計	54,482	61,776	66,718	71,388
構成比				
ファイウォール・アプライアンス／ソフトウェア	38.9%	36.7%	36.7%	36.7%
VPNアプライアンス／ソフトウェア	21.1%	20.0%	20.0%	20.0%
IDS／IPSアプライアンス／ソフトウェア	24.7%	23.2%	23.2%	23.2%
アプリケーションファイアウォール	8.3%	12.7%	12.7%	12.7%
その他のネットワーク脅威対策製品	7.0%	7.4%	7.4%	7.4%
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	－	7.1%	8.0%	7.0%
VPNアプライアンス／ソフトウェア	－	7.3%	8.0%	7.0%
IDS／IPSアプライアンス／ソフトウェア	－	6.8%	8.0%	7.0%
アプリケーションファイアウォール	－	72.4%	8.0%	7.0%
その他のネットワーク脅威対策製品	－	19.6%	8.0%	7.0%
合計	－	13.4%	8.0%	7.0%

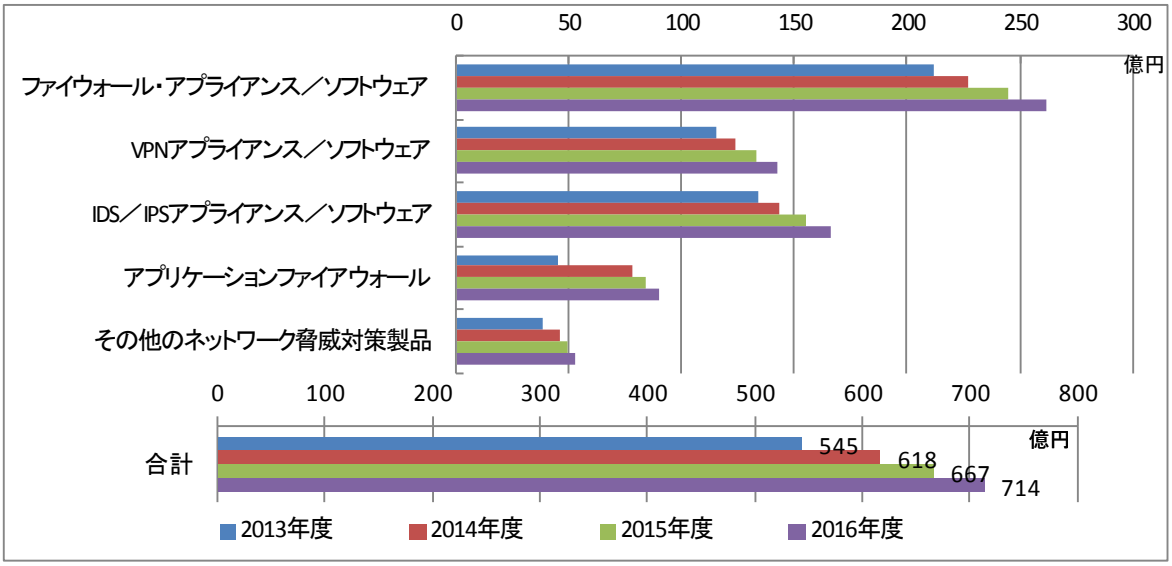
ネットワーク脅威対策製品のカテゴリの、2014年度における売上実績推定値は618億円となった。前年度比の市場成長率は13.4%である。IDS／IPS製品やアプリケーションファイアウォ

ールが市場を牽引している。ネットワークセキュリティ対策の見直し・再構築の取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。

2015 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 8.0%の成長となり、市場規模は 667 億円程度に達したものと推測される。2016 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 7.0%増と市場拡大基調を維持して 774 億円に達すると予測される。

情報セキュリティツール市場の中での構成比で見ると、2014 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)

図 7　国内ネットワーク脅威対策製品市場推移



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、2013 年度 212 億円、2014 年度 227 億円、2015 年度 245 億円、2016 年度 262 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、2013 年度 115 億円、2014 年度 124 億円・7.3%増、2015 年度 133 億円・8.0%増、2016 年度 143 億円・7.0%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、2013 年度は 135 億円であった。2014 年度 144 億円で 6.8%増、2015 年度 155 億円で 8.0%増、2016 年度 166 億円で 7.0%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。

「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、2013 年度 45 億円から、2014 年度 78 億円で 72.4%増、2015 年度には 8.0%増の 84 億円規模となった。2016 年度はこの 2014 年の底上げをベースに他の製品同様 7.0%増の 90 億円と推定している。この背景には、クラウドをはじめとする Web ベースコンピューティングの一層の浸透や、PCI DSS が v3 に上がることに伴う需要喚起等があるものと見られる。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」、「ドライブバイダウンロード用 Web 改ざん」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。

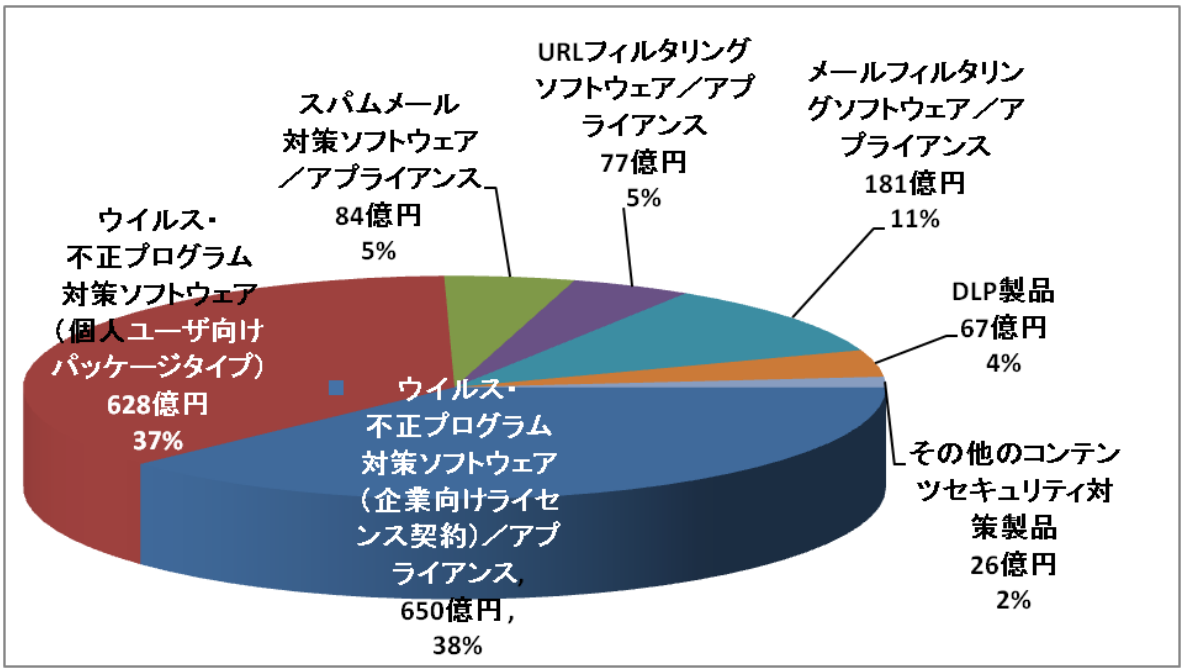
コンテンツセキュリティ対策製品の 7 つの製品分類における 2014 年度の分布を図 8 に示す。

「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、当市場の約 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、国境を超える目的と意図を持った攻撃等、脅威が深刻化する中で、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 8　2014 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 9 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 599 億円に達した。2014 年度も市場は順調に推移し、8.4%増の 650 億円となった。2015 年度も市場の順調な伸びを勘案し 10.0%増の 715 億円に達すると思われる。2016 年度は伸びもやや落ち着いて、6.0%増の 758 億円と予測した。

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）	2013 年度	2014 年度	2015 年度	2016 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	59,916	64,979	71,476	75,765
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）	58,787	62,756	65,894	69,188
スパムメール対策ソフトウェア／アプライアンス	7,448	8,371	9,208	9,761
URL フィルタリングソフトウェア／アプライアンス	7,304	7,737	8,510	9,191
メールフィルタリングソフトウェア／アプライアンス	16,311	18,100	19,910	20,905
DLP 製品	6,133	6,659	7,658	8,424
その他のコンテンツセキュリティ対策製品	2,336	2,591	2,721	2,857
合計	158,234	171,192	185,377	196,091
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%	38.0%	38.6%	38.6%
ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ）	37.2%	36.7%	35.5%	35.3%
スパムメール対策ソフトウェア／アプライアンス	4.7%	4.9%	5.0%	5.0%
URL フィルタリングソフトウェア／アプライアンス	4.6%	4.5%	4.6%	4.7%
メールフィルタリングソフトウェア／アプライアンス	10.3%	10.6%	10.7%	10.7%
DLP 製品	3.9%	3.9%	4.1%	4.3%
その他のコンテンツセキュリティ対策製品	1.5%	1.5%	1.5%	1.5%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
ウイルス・不正プログラム対策ソフトウェア（企業向けライセンス契約）／アプライアンス	―	8.4%	10.0%	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）	―	6.8%	5.0%	5.0%
スパムメール対策ソフトウェア／アプライアンス	―	12.4%	10.0%	6.0%
URL フィルタリングソフトウェア／アプライアンス	―	5.9%	10.0%	8.0%
メールフィルタリングソフトウェア／アプライアンス	―	11.0%	10.0%	5.0%
DLP 製品	―	8.6%	15.0%	10.0%
その他のコンテンツセキュリティ対策製品	―	10.9%	5.0%	5.0%
合計	―	8.2%	8.3%	5.8%

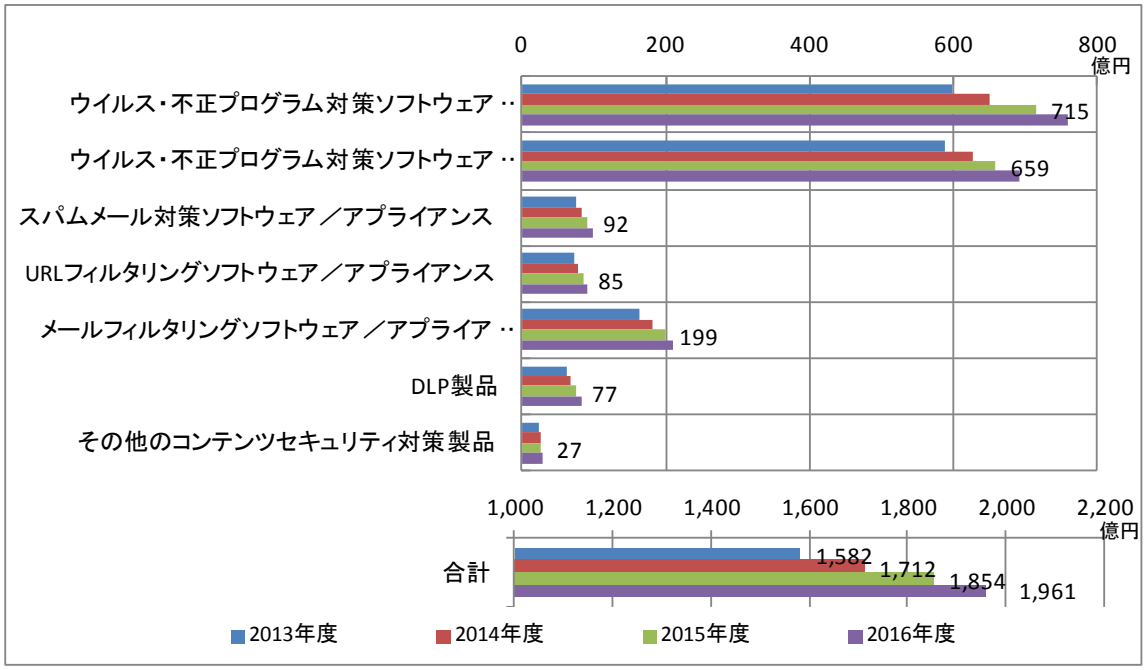
「ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ）」も企業向けと同程度の規模を持つセグメントである。銀行口座やクレジットカードの情報を盗まれる被害が個人にも及んできており、金融機関や決済代行会社などの注意喚起もあり、基本的対策であ

るウイルス対策ソフトの導入が徐々に浸透している。2014 年度の市場規模は 628 億円であったと推計され、前年比 6.8%増の成長となった。。2015 年度は前年比 5.0%増の 659 億円、2016 年度は前年比 5.0%増の 692 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、金融機関と決済代行会社の啓発活動などで更に大きく増加する可能性もある。

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 2013 年度で 163 億円であるが、2016 年度には 209 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、2013 年度 74 億円から、2014 年度 12.4%増の 84 億円、2015 年度 10.0%増の 92 億円とコンスタントに拡大して 2016 年度の市場規模は 98 億円に達すると予測される。

図 9　国内コンテンツセキュリティ対策製品市場推移



次いで「URL フィルタリングソフトウェア／アプライアンス」がほぼ同規模の市場を形成している。2013 年度 73 億円、2014 年度 77 億円（5.9%増）、2015 年度 85 億円（10.0%増）、2016 年度 92 億円（8.0%増）と予想する。

「DLP 製品」市場は比較的後発のセグメントであるが 2013 年度には 61 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、2014 年度 67 億円（8.6%増）、2015 年度 77 億円（15.0%増）、2016 年度 84 億円（10.0%増）との予測結果となった。

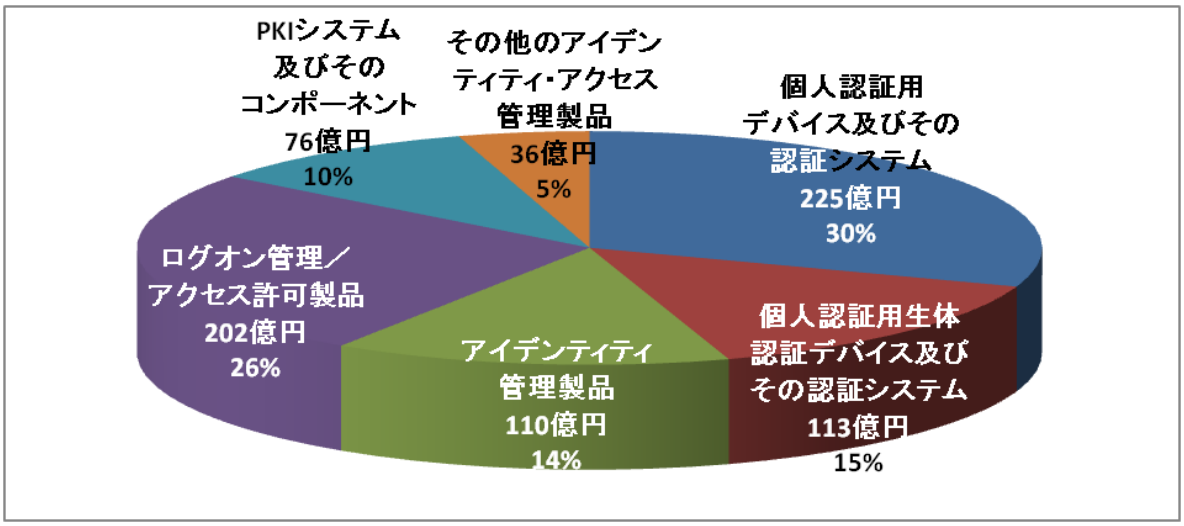
2.1.2.4. アイデンティティ・アクセス管理製品市場

(1) 市場の動向

図 10 に 2014 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 10　2014 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するクラウド・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。

また、SAML（Security Assertion Markup Language）や OpenID 等、各種認証技術を組み合

わせたり、システム間で認証情報を連携することで認証の効率性と信頼性を向上させ、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 11 にその市場規模の推移のグラフを示す。

表 6　国内アイデンティティ・アクセス管理製品市場規模　実績と予測

市場規模（百万円）	2013 年度	2014 年度	2015 年度	2016 年度
個人認証用デバイスおよびその認証システム	22,451	23,473	24,412	25,632
個人認証用生体認証デバイスおよびその認証システム	10,709	11,299	11,751	12,339
アイデンティティ管理製品	10,050	10,960	12,056	13,261
ログオン管理／アクセス許可製品	18,003	20,246	22,270	24,497
PKI システムおよびそのコンポーネント	7,356	7,624	8,005	8,405
その他のアイデンティティ・アクセス管理製品	5,158	3,618	3,618	3,799
合計	73,727	77,220	82,112	87,934
構成比				
個人認証用デバイスおよびその認証システム	30.5%	30.4%	29.7%	29.1%
個人認証用生体認証デバイスおよびその認証システム	14.5%	14.6%	14.3%	14.0%
アイデンティティ管理製品	13.6%	14.2%	14.7%	15.1%
ログオン管理／アクセス許可製品	24.4%	26.2%	27.1%	27.9%
PKI システムおよびそのコンポーネント	10.0%	9.9%	9.7%	9.6%
その他のアイデンティティ・アクセス管理製品	7.0%	4.7%	4.4%	4.3%
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	－	4.6%	4.0%	5.0%
個人認証用生体認証デバイスおよびその認証システム	－	5.5%	4.0%	5.0%
アイデンティティ管理製品	－	9.0%	10.0%	10.0%

ログオン管理／アクセス許可製品	―	12.5%	10.0%	10.0%
PKI システムおよびそのコンポーネント	―	3.6%	5.0%	5.0%
その他のアイデンティティ・アクセス管理製品	―	-29.9%	0.0%	5.0%
合計	―	4.7%	6.3%	7.1%

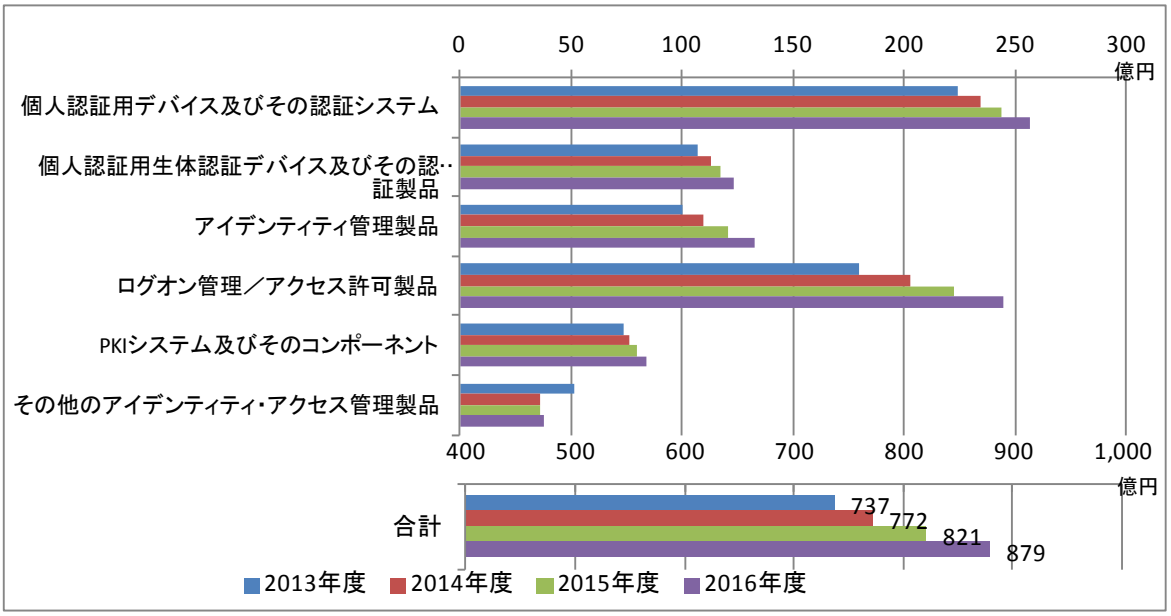
アイデンティティ・アクセス管理製品の市場規模は、2014 年度の実績で 772 億円（前年比伸び率 4.7%）となったが、「情報セキュリティツール」市場全体の 4,489 億円に対する構成比は 17.1 %であり、コンテンツセキュリティ対策製品市場に次ぐ規模の市場である。2015 年度は+6.3%の 821 億円、2016 年度には+7.1%の 879 億円と、880 億円規模にまで拡大すると予測される。

「アイデンティティ・アクセス管理製品」カテゴリの内訳をみると、「個人認証用デバイスおよびその認証システム」セグメントが 2014 年度の構成比で 30.4%と最も大きな部分を占めた。市場規模は 2014 年度で 235 億円であり、2015 年度は 244 億円と前年比 4.0%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 2014 年度に 202 億円で、2015 年度には 10.0%拡大して 223 億円となり、2016 年度には 245 億円（前年度比成長率 10.0%）の市場規模になると予測した。

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 2014 年度は、5.5%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。

図 11　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

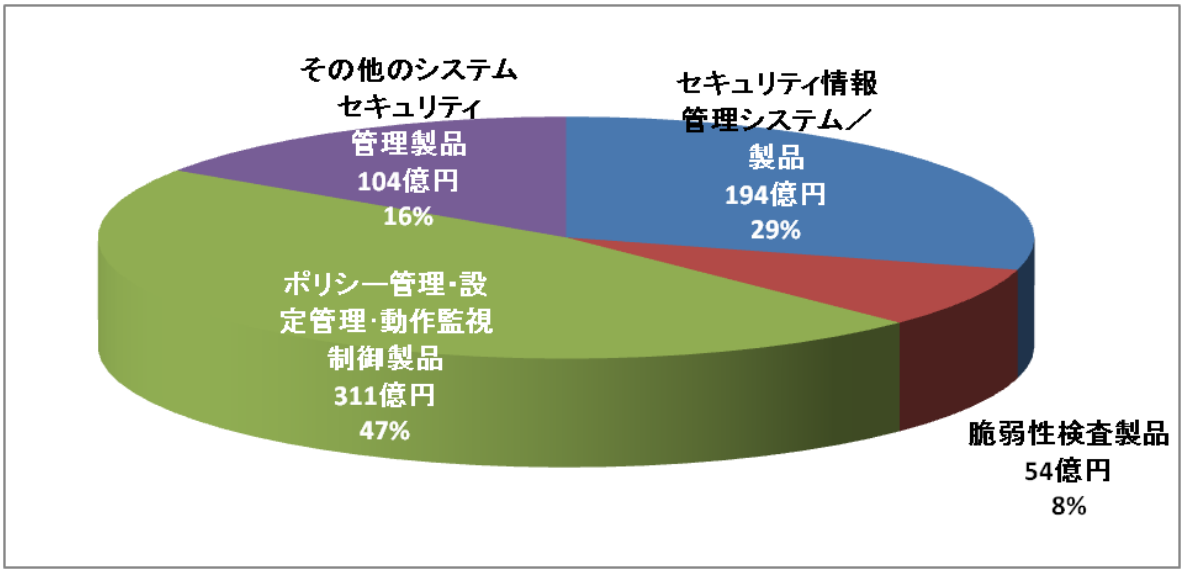
(1) 市場の動向

システムセキュリティ管理製品の 2014 年度におけるセグメント分布を図 12 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[4]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。

図 12　2014 年度のシステムセキュリティ管理製品市場



「ポリシー管理・設定管理・動作監視制御製品」は情報漏えい対策につながることから、需要は依然高い分野である。スマートデバイスの普及に伴い、、リモートロック、リモートワイプ（初期化、無効化）ツールや、それら機能を含みインベントリ管理なども行う MDM（Mobile Device Management）製品などの導入が進み、今後更に管理製品や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13にその市場規模の推移のグラフを示す。

---

[4] 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

「システムセキュリティ管理製品」市場は2014年度には全セグメント合せて663億円程度の市場を形成しており、2013年度と比べると+9.6%の伸びとなる。2015年度は13.8%増の754億円と堅調な伸び率を見込んでおり、その傾向は2016年度（811億円、+7.6%）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。

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）	2013年度	2014年度	2015年度	2016年度
セキュリティ情報管理システム／製品	17,267	19,426	21,369	23,078
脆弱性検査製品	4,153	5,375	5,805	6,269
ポリシー管理・設定管理･動作監視制御製品	29,679	31,118	37,341	40,329
その他のシステムセキュリティ管理製品	9,369	10,369	10,887	11,432
合計	60,468	66,288	75,402	81,108
構成比				
セキュリティ情報管理システム／製品	28.6%	29.3%	28.3%	28.5%
脆弱性検査製品	6.9%	8.1%	7.7%	7.7%
ポリシー管理・設定管理･動作監視制御製品	49.1%	46.9%	49.5%	49.7%
その他のシステムセキュリティ管理製品	15.5%	15.6%	14.4%	14.1%
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	－	12.5%	10.0%	8.0%
脆弱性検査製品	－	29.4%	8.0%	8.0%
ポリシー管理・設定管理･動作監視制御製品	－	4.8%	20.0%	8.0%
その他のシステムセキュリティ管理製品	－	10.7%	5.0%	5.0%
合計	－	9.6%	13.8%	7.6%

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2014年度に194億円、前年度比12.5%増と増加傾向にあり、さらに2015年度は10.0%増の214億円、2016年度は+8.0%の231億円と伸びていくと推測される。

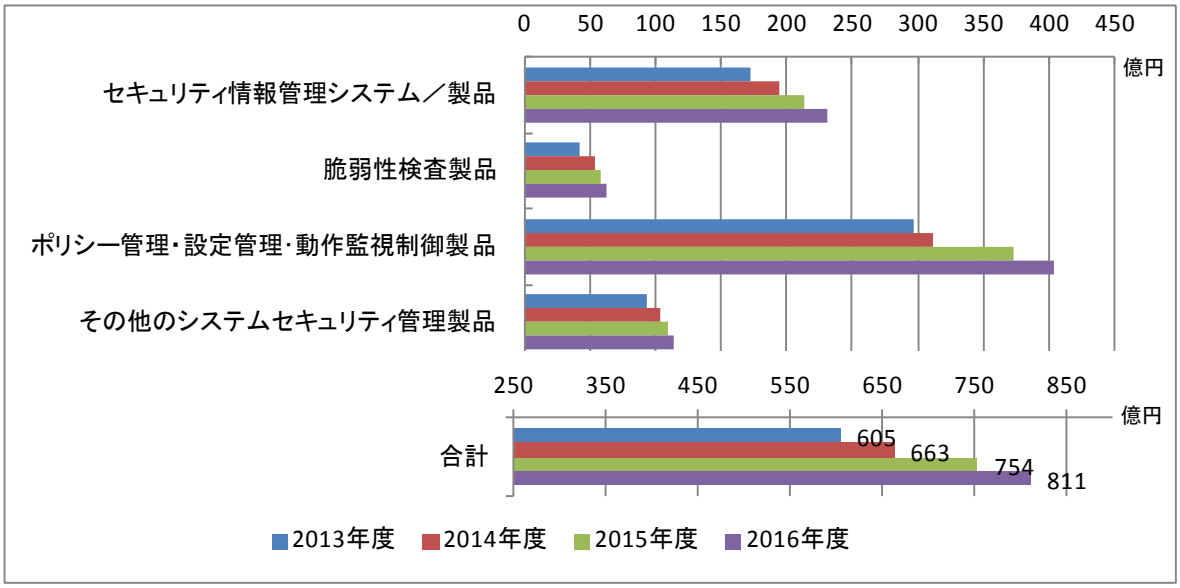
「ポリシー管理・設定管理･動作監視制御製品」はこの区分の約半分を占める市場となっているが、2014 年度における成長率は+4.8%となり、市場規模は 311 億円と 300 億円の大台を突破した。2015 年度も 373 億円規模への拡大が見込まれ、2016 年は 400 億円市場への成長が予想される。

「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 2014 年度で 54 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、2015 年度+8.0%、2016 年度+8.0%程度と予測され、2016 年度の市場規模は 63 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。2014年度の伸び率は+10.7%で、2015年度+5.0%、2016年度+5.0%の成長率を示し、2014年度には100億円を突破し、2016年度には114億円に達するものと予測される。

図 13　国内システムセキュリティ管理製品市場推移



2.1.2.6. 暗号化製品市場

(1) 市場の動向

暗号化製品も 2014 年度には前年比+6.7%と堅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。更に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、民間の認証機関でも同様の動きがあり、今回の調査対象期間において継続的な成長が観られたと考える。

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、PCI DSS におけるデータ暗号化強化の要求も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」といった新たなニーズも増えている。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

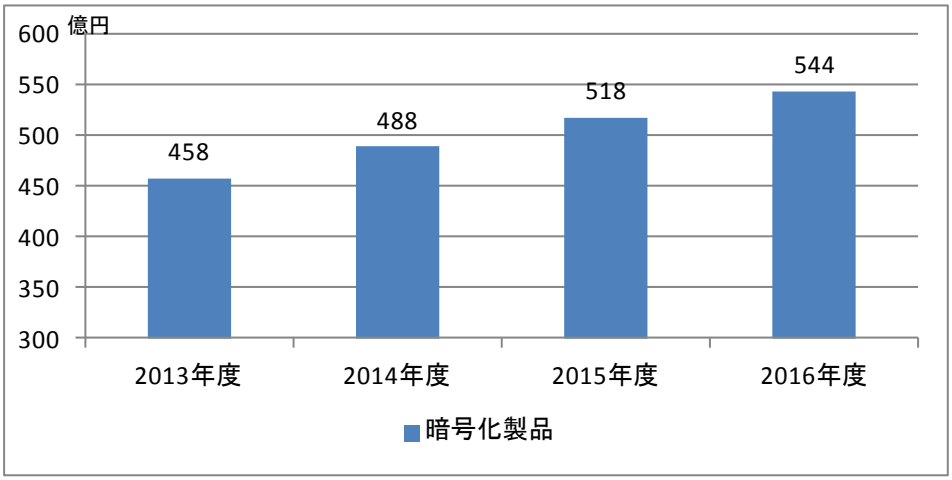
表 8 に国内暗号化製品市場規模の実績推定値と予測値を、図 14 にその市場規模の推移のグラフを示す。

表 8　国内暗号化製品市場規模　実績と予測

市場規模（百万円）	2013 年度	2014 年度	2015 年度	2016 年度
暗号化製品	45,779	48,844	51,774	54,363
対前年度比成長率				
暗号化製品	―	6.7%	6.0%	5.0%

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。2014 年度の市場規模は 488 億円で前年度比 6.7%増加となった。2015 年度は前年度比 6.0%増の 518 億円、2016 年度もさらに 5.0%市場規模を拡大させ、544 億円の市場規模になると予測している。

図 14　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

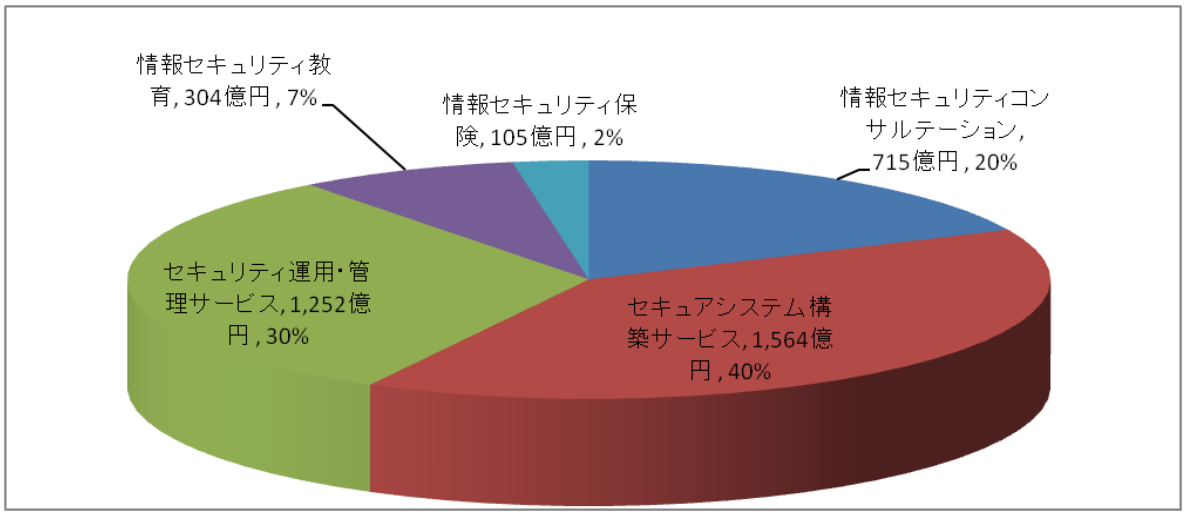
年度別売上高推計値	2013年度		2014年度			2015年度			2016年度		
セキュリティ・サービス	売上実績推定値		売上実績推定値			売上高見込推定値			売上高予測値		
	金額	構成比	金額	構成比	成長率	金額	構成比	成長率	金額	構成比	成長率
情報セキュリティコンサルテーション	72,731	20.0%	71,452	20.0%	-1.8%	75,778	19.8%	6.1%	79,567	19.9%	5.0%
セキュアシステム構築サービス	144,875	39.9%	156,356	39.9%	7.9%	171,992	39.2%	10.0%	180,592	39.8%	5.0%
セキュリティ運用・管理サービス	109,379	30.1%	125,248	30.1%	14.5%	138,348	31.2%	10.5%	149,419	30.7%	8.0%
情報セキュリティ教育	26,979	7.4%	30,365	7.4%	12.6%	33,603	7.2%	10.7%	36,871	7.5%	9.7%
情報セキュリティ保険	8,885	2.4%	10,479	2.4%	17.9%	13,623	2.6%	30.0%	15,667	2.1%	15.0%
セキュリティサービス市場合計	362,849	100.0%	393,901	100.0%	8.6%	433,345	100.0%	10.0%	462,115	100.0%	6.6%

今回の調査結果では、対象期間の最初の年度である 2013 年度の「情報セキュリティサービス」市場規模は 3,628 億円と見積もられ、2014 年度には+8.6%拡大、2015 年度にはさらに 10.0%拡大し 4,333 億円市場になるとの観測となった。現在の成長軌道に乗る前のボトムとして捉えている 2010 年度から、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関係で、市場は順調に拡大している。また、セキュリティ脅威の複雑化に伴い、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が浸透するようになってきたことも、市場が拡大している要因の一つとして考えられる。

2014 年度は、第 1 章で見たように経済環境が改善する中、国内大手企業や国の機関、個人に対するサイバー攻撃による被害の拡大が認知され、さらなる投資の必要に迫られた時期となり、市場規模は 3,939 億円と、4,000 億円に迫る市場に成長している。2015 年度は情報セキュリティサービスのすべてのカテゴリで成長することが見込まれ、10%増の 4,333 億円に達すると予測される。2016 年度は経済状況が不透明となり、成長率は鈍化するものの、セキュリティへの脅威が高度化、深刻化するため専門的なサービス利用が増加し 6.6%増の成長と予測される。

図 15 に 2014 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 16 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。

図 15　2014 年度の国内情報セキュリティサービス市場



「情報セキュリティサービス」市場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、2014 年度実績推定値で 1,564 億円と、情報セキュリティサービス市場全体の 40%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。

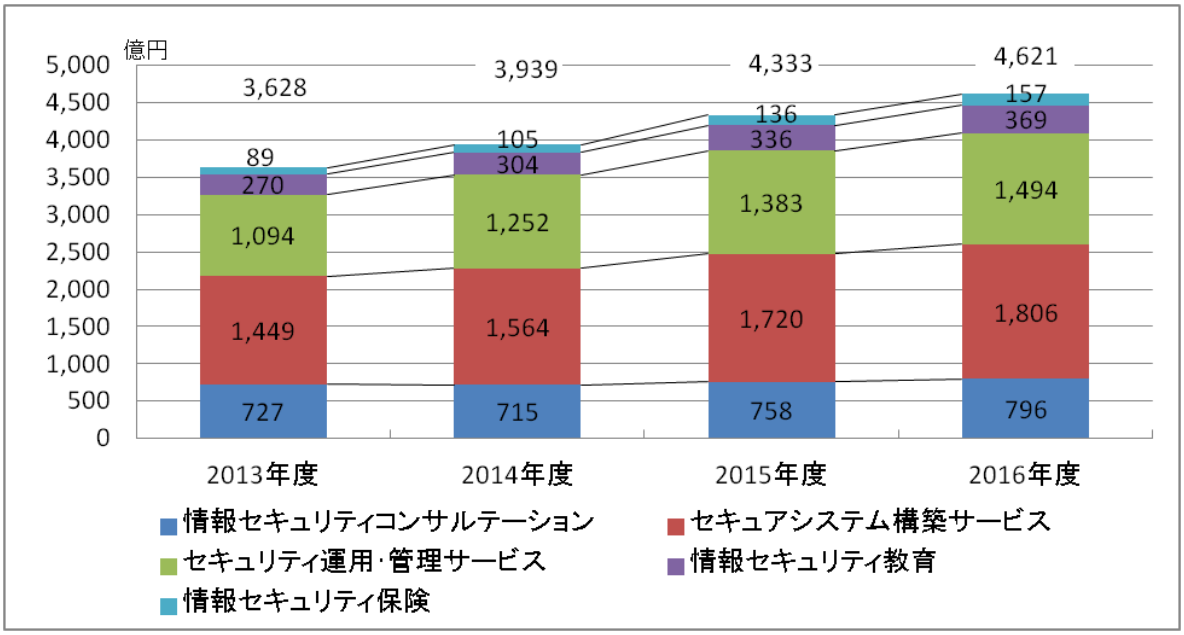
次に大きなカテゴリは「セキュリティ運用・管理サービス」で、2014 年度実績は 1,252 億円。このカテゴリは、ネットワークセキュリティの監視や運用、攻撃への対処を専門家が代行するマネージドセキュリティサービス、システムの弱点を専門技術で点検する脆弱性検査サービスやインシデントへの対応を行うプロフェッショナルサービス、そして電子認証サービス等の専門的サービスで構成される。特に自社で SOC（Security Operation Center）をもたずに、セキュリティセンサやエンドポイントのログを転送し高度な分析結果の提供を受けるマネージドセキュリティサービスへの需要は拡大している。

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や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、数年前の調査ではマイナス成長が続くという結果となる時期があった。しかしその後、過去に構築した対策の体系的見直しの需要が、大企業のみならず中堅企業での需

要も高まり、2013 年度には持ち直したが、2014 年度は若干市場が縮小し前年度比 2%減の 715 億円となった。しかし 2015 年度は再び拡大していくカテゴリだと予測される。

図 16　国内情報セキュリティサービス市場推移



2014 年度「情報セキュリティ教育」市場は 12.6%増の 304 億円となった。これは標的型攻撃への対応のためエンドユーザを含めた定期的な訓練の必要性が認知され、またそれに特化したサービスを提供するベンダも増えてきたためと考えられる。

2015 年度以降も教育市場の拡大のペースは堅調に推移すると見込まれる。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取り組みが定着した結果とみられる。

「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、2014 年度で前年度比+17.9%の 105 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。

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

2014 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は図 17 のセグメント比率となる。

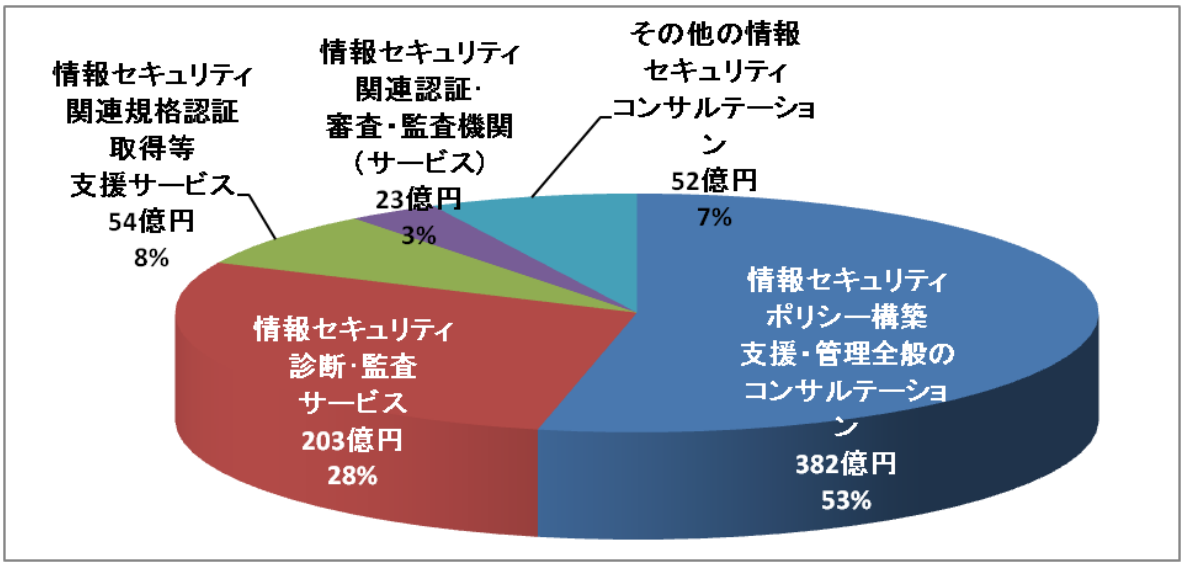
「情報セキュリティコンサルテーション」というカテゴリは、コンサルテーションの特性から、

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引き続き高まっている。企業は、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、情報セキュリティ管理の責任者には、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。

図 17　2014 年度の情報セキュリティコンサルテーション市場



2005 年 4 月から個人情報保護法が全面的に施行され、これが引き金となりその前後に ISMS 認証やプライバシーマーク認定の取得に取り組む企業が増加した。規格の要求する形を取り急ぎ整えてとりあえず認証・認定を得ようとするような傾向も当初は見受けられたが、程なくして終息した。一方で、実効性のあるマネジメントシステムを導入したいという企業は常に存在し、認証・認定取得企業はコンスタントに誕生している。JIPDEC 統計で 2016 年 3 月現在、ISMS 認証取得組織数は 4,827 件（2015 年 3 月：4,696 件）、プライバシーマーク認定取得企業数は 14,710 社（2015 年 9 月：14,221 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。

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時期を経て 2012 年度には下げ止まり、2013 年度以降は経済環境の好転に伴って回復した。しかし、2014 年度は若干縮小となった。背景には直近の課題への対応に迫られ、他の情報セキュリティサービスへの投資へ一時的に向いたものと考えられる。2015 年度以降は再び堅調に拡大すると予想される。

(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 18 にその市場規模の推移のグラフを示す。

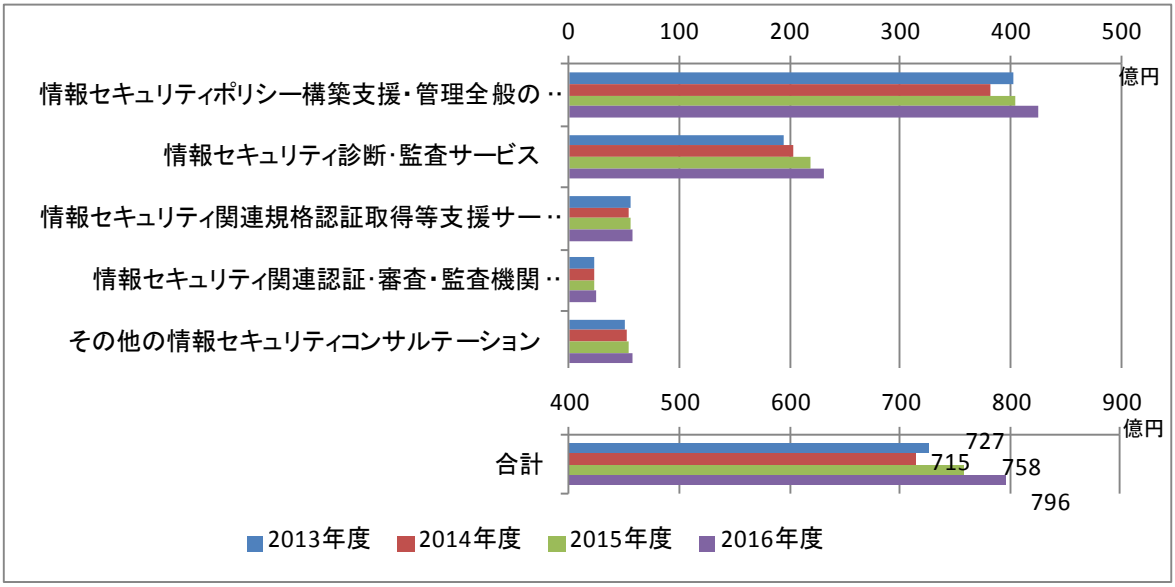
表 10　国内情報セキュリティコンサルテーション市場規模　実績と予測

市場規模（百万円）	2013 年度	2014 年度	2015 年度	2016 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	40,332	38,184	40,476	42,499
情報セキュリティ診断･監査サービス	19,421	20,327	21,953	23,051
情報セキュリティ関連規格認証取得等支援サービス	5,639	5,444	5,552	5,830
情報セキュリティ関連認証･審査・監査機関（サービス）	2,276	2,284	2,375	2,494
その他の情報セキュリティコンサルテーション	5,063	5,214	5,422	5,693
合計	72,731	71,452	75,778	79,567
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	55.5%	53.4%	53.4%	53.4%
情報セキュリティ診断･監査サービス	26.7%	28.4%	29.0%	29.0%
情報セキュリティ関連規格認証取得等支援サービス	7.8%	7.6%	7.3%	7.3%
情報セキュリティ関連認証･審査・監査機関（サービス）	3.1%	3.2%	3.1%	3.1%
その他の情報セキュリティコンサルテーション	7.0%	7.3%	7.2%	7.2%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
情報セキュリティポリシー構築支援・管理全般のコンサルテーション	―	-5.3%	6.0%	5.0%
情報セキュリティ診断･監査サービス	―	4.7%	8.0%	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	―	-3.5%	2.0%	5.0%
情報セキュリティ関連認証･審査・監査機関（サービス）	―	0.3%	4.0%	5.0%
その他の情報セキュリティコンサルテーション	―	3.0%	4.0%	5.0%
合計	―	-1.8%	6.1%	5.0%

2014 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 715 億円程度となり、前年度比成長率はマイナス 1.8%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」は382億円と、2番目の「情報セキュリティ診断・監査サービス」の203億円の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。情報セキュリティコンサルテーションは、この2つのセグメントが主たる構成要素であると言える。

図 18　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）[5]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、情報セキュリティ関連認証・審査・監査機関（サービス）は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、市場は厳しい環境が続くことも予想される。

2.2.2.2. セキュアシステム構築サービス市場

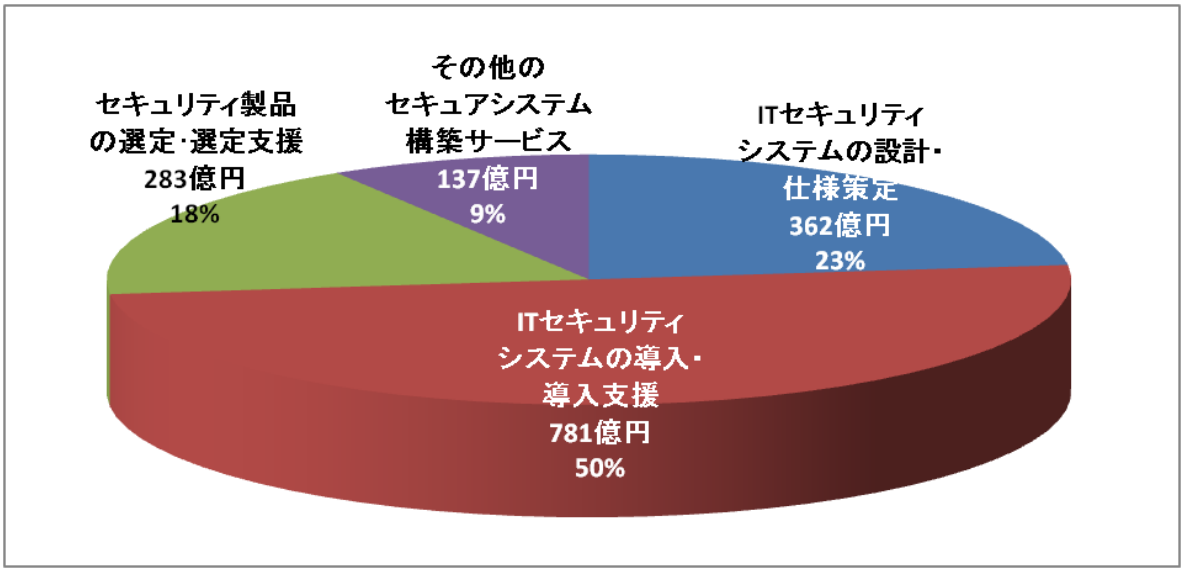
(1) 市場の動向

図 19 に 2014 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。

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

「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、加えて 2013 年度 1,449 億円、2014 年度 1,564 億円、2015 年度には 1,720 億円と拡大が続くとみられ、2016 年度には 1,806 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。

図 19　2014 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。その結果、一時期はこの市場はほとんど伸びが見られない時期が続いた。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。

一方、2009 年度以降、国内 IT ベンダからの参入も一気に増えることで、クラウドサービスの市場が急速に立ち上がった。プライベートクラウドの導入も含め、クラウドコンピューティングの活用はますます市場に浸透している。パブリッククラウドにおけるセキュリティは、SaaS、PaaS、IaaS というサービスモデルによっても大きく異なるが、クラウドベンダがすべて整えてサービスの機能の一部として提供する形、主として IaaS におけるユーザが自前で用意して組み込む形、ベンダが用意した機能モジュールをユーザが選択して実装する形などがある。このような実装や組み込みに際して、セキュアシステム構築の専門サービスが活用される場面も想定され、新しい需要の源となってきていると考えられる。

(2) 市場規模とその推移

表11に国内セキュアシステム構築サービス市場規模の実績推定値と予測値を、図20にその市場規模の推移のグラフを示す。

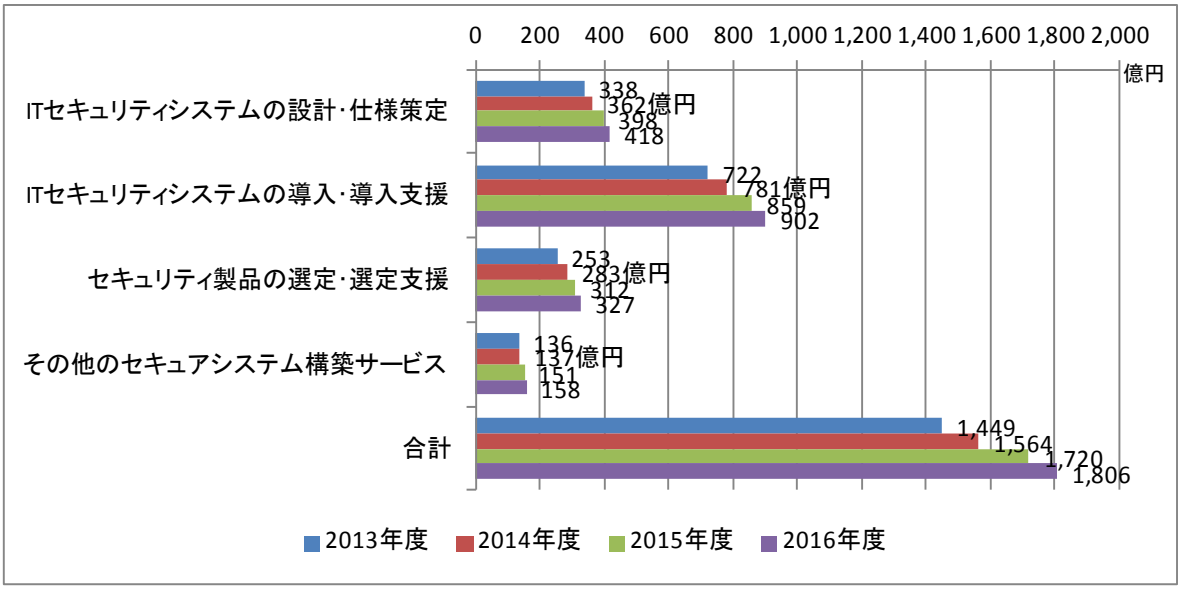
「セキュアシステム構築サービス」カテゴリのうち最大のセグメントは全体の約５割を占める「ITセキュリティシステムの導入･導入支援」であり、2013年度722億円、2014年度781億円（前年度比8.1%増）、2015年度859億円（同10%増）、2016年度予測902億円（同5.0%増）の規模と推測される。これに次ぐのが「ITセキュリティシステムの設計・仕様策定」で、約2割強を占める。金額は2013年度338億円、2014年度362億円（前年度比7.2%増）、2015年度398億円（同10.0%増）、2016年度予測418億円（同5.0%増）と推定する。

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）	2013 年度	2014 年度	2015 年度	2016 年度
IT セキュリティシステムの設計･仕様策定	33,777	36,206	39,826	41,818
IT セキュリティシステムの導入･導入支援	72,239	78,113	85,925	90,221
セキュリティ製品の選定･選定支援	25,303	28,321	31,153	32,711
その他のセキュアシステム構築サービス	13,555	13,716	15,088	15,842
合計	144,875	156,356	171,992	180,592
構成比				
IT セキュリティシステムの設計･仕様策定	23.3%	23.2%	23.2%	23.2%
IT セキュリティシステムの導入･導入支援	49.9%	50.0%	50.0%	50.0%
セキュリティ製品の選定･選定支援	17.5%	18.1%	18.1%	18.1%
その他のセキュアシステム構築サービス	9.4%	8.8%	8.8%	8.8%
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	－	7.2%	10.0%	5.0%
IT セキュリティシステムの導入･導入支援	－	8.1%	10.0%	5.0%
セキュリティ製品の選定･選定支援	－	11.9%	10.0%	5.0%
その他のセキュアシステム構築サービス	－	1.2%	10.0%	5.0%
合計	－	7.9%	10.0%	5.0%

「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見られ、2013年度は253億円、2014年度が283億円（前年度比11.9%増）、2015年度は312億円（同10.0%増）、2016年度予測には327億円（同5.0%増）と推測している。

図 20　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。その理由としては、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働くことなどが考えられる。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、セキュリティ対策の高度化・統合化が進行する一方で、クラウドベースのセキュリティサービスも登場し、「セキュリティ運用・管理サービス」市場は継続的に拡大傾向にある。2014 年度も全てのセグメントで前年度に対して 15%近い顕著な成長率となっている。

図 21 に 2014 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して、今まで社内で防御策を構築・運用していた企業が、専門性の面からも自力での対応に限界を感じ、サービス業者に運用を移管するケースが増加し大幅なプラス成長となった。特に、IDS/IPS は運用にノウハウが必要となることから外部サービスを利用する傾向が大きい。

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、クラウドを活用したサービス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

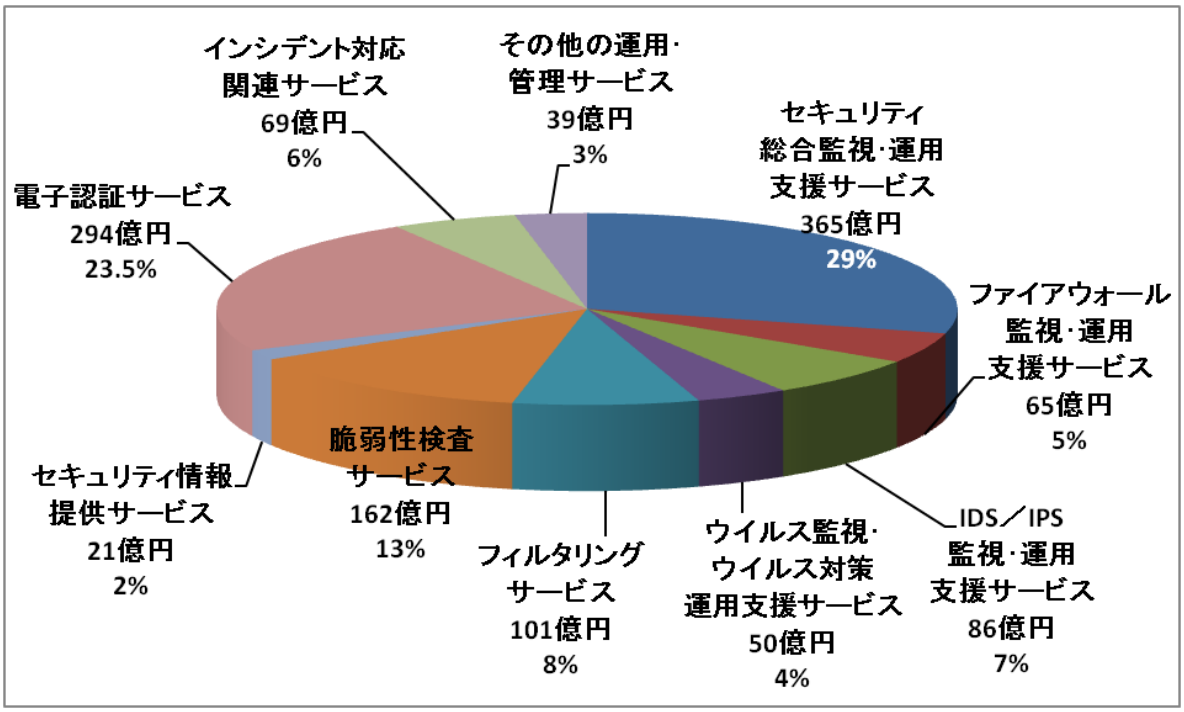
運用するよりコスト面、人材面からも社外のサービスを受ける傾向にあり、一括して委託できるメリットから今後ますます中小企業での「セキュリティ総合監視・運用支援サービス」の利用が増加していくものと考えられる。

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から外部サービス利用への移行などにより昨年同様の成長を示している。

「脆弱性検査サービス」は、Web アプリケーションの脆弱性を利用したサイバー攻撃が定常的に発生していることもあり、昨年同様の増加率となった。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。

「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 21　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等、、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、もっとも顕著に成長した分野である。このサービスは、ハッキングや内部犯行などに伴う情報漏えい事案に際して、インシデントレスポンスの活動を提供するサービスで、事件事故の増加、社会的対応の注目度と重要度の高まり、攻撃手口の複雑化や漏えい情報量の増大等に伴って、急速に需要が拡大している。

(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、2014 年度の実績推定値が 1,252 億円と、前年の 1,094 億円に対し 14.5%の増加となった。サイバー攻撃の脅威の深刻化と複雑化に伴い、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。

表 12　国内セキュリティ運用・管理サービス市場規模　実績と予測

市場規模（百万円）	2013 年度	2014 年度	2015 年度	2016 年度
セキュリティ総合監視･運用支援サービス	31,035	36,467	41,937	46,131
ファイアウォール監視･運用支援サービス	5,647	6,454	6,906	7,320
IDS／IPS 監視･運用支援サービス	7,254	8,612	9,215	9,768
ウイルス監視･ウイルス対策運用支援サービス	4,301	4,993	5,343	5,663
フィルタリングサービス	8,807	10,144	11,159	12,051
脆弱性検査サービス	14,543	16,235	17,858	19,287
セキュリティ情報提供サービス	1,953	2,136	2,242	2,355
電子認証サービス	26,236	29,423	32,365	34,954
インシデント対応関連サービス	5,717	6,852	7,195	7,555
その他の運用･管理サービス	3,886	3,932	4,128	4,334
合計	109,379	125,248	138,348	149,419
構成比	2013 年度	2014 年度	2015 年度	2016 年度
セキュリティ総合監視･運用支援サービス	28.4%	29.1%	30.3%	30.9%
ファイアウォール監視･運用支援サービス	5.2%	5.2%	5.0%	4.9%
IDS／IPS 監視･運用支援サービス	6.6%	6.9%	6.7%	6.5%
ウイルス監視･ウイルス対策運用支援サービス	3.9%	4.0%	3.9%	3.8%
フィルタリングサービス	8.1%	8.1%	8.1%	8.1%
脆弱性検査サービス	13.3%	13.0%	12.9%	12.9%
セキュリティ情報提供サービス	1.8%	1.7%	1.6%	1.6%
電子認証サービス	24.0%	23.5%	23.4%	23.4%
インシデント対応関連サービス	5.2%	5.5%	5.2%	5.1%
その他の運用･管理サービス	3.6%	3.1%	3.0%	2.9%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率	2013 年度	2014 年度	2015 年度	2016 年度
セキュリティ総合監視･運用支援サービス	－	17.5%	15.0%	10.0%
ファイアウォール監視･運用支援サービス	－	14.3%	7.0%	6.0%
IDS／IPS 監視･運用支援サービス	－	18.7%	7.0%	6.0%
ウイルス監視･ウイルス対策運用支援サービス	－	16.1%	7.0%	6.0%
フィルタリングサービス	－	15.2%	10.0%	8.0%

脆弱性検査サービス	－	11.6%	10.0%	8.0%
セキュリティ情報提供サービス	－	9.4%	5.0%	5.0%
電子認証サービス	－	12.1%	10.0%	8.0%
インシデント対応関連サービス	－	19.9%	5.0%	5.0%
その他の運用･管理サービス	－	1.2%	5.0%	5.0%
合計	－	14.5%	10.5%	8.0%

図 22 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 と併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、2014 年度の推定実績市場規模は 365 億円（前年度比成長率+17.5%）であった。2015 年度もプラス成長を続け、 2016 年度には 461 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、2014 年度それぞれ 65 億円（前年度比成長率+14.3%）、86 億円（同+18.7%）、50 億円（同+16.1%）、2015 年度それぞれ 69 億円（同+7.0%）、92 億円（同+7.0%）、53 億円（同+7.0%）、2016 年度それぞれ 73 億円（同+6.0%）、98 億円（同+6.0%）、57 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、2014 年度に 101 億円（同+15.2%）と大幅成長を遂げた。2015 年度には 112 億円（同+10.0%）、2016 年度には 121 億円（同+8.0%）と 100 億円市場定着が見込まれる。

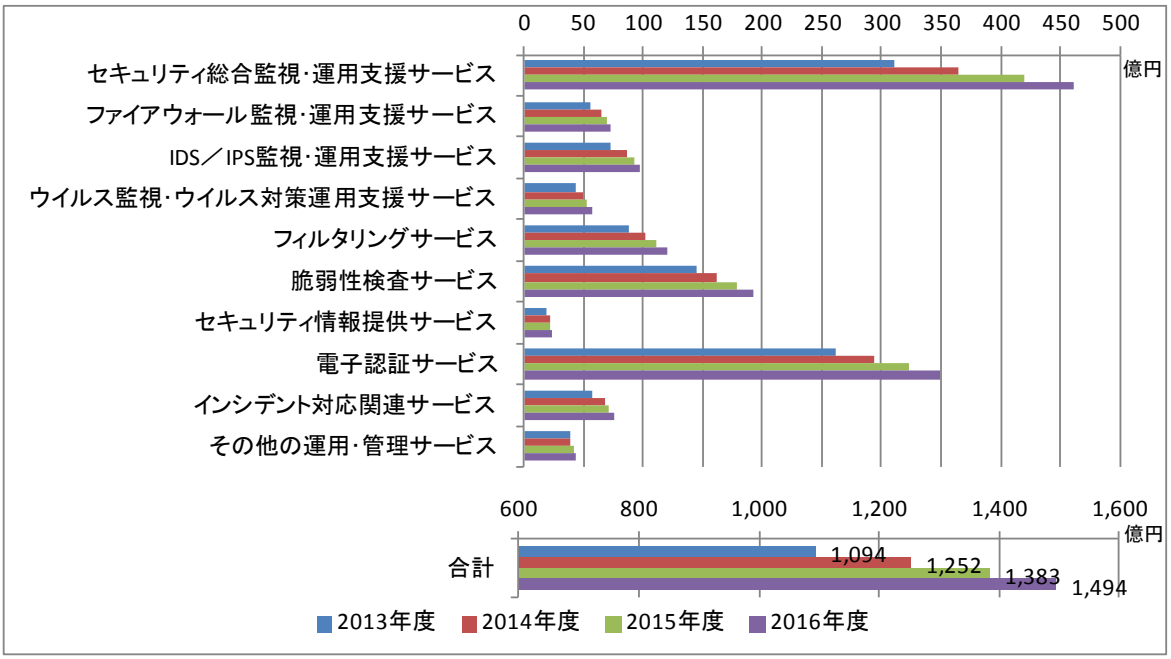
「脆弱性検査サービス」は、2014 年度においては 162 億円（同+11.6%）、2015 年度には 179 億円（同+10.0%）、2016 年度には 193 億円（同+8.0%）と、順調に成長していくと思われる。

「セキュリティ情報提供サービス」については、2014 年度で 21 億円（同+9.4%）と安定した市場である。2015 年度、2016 年度も金額では 20～23 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。

「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」に次ぐ大規模市場であり 2014 年度は 294 億円（同+12.1%）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があげられる。2015 年度は 324 億円（同+10.0%）、2016 年度は 350 億円（同+8.0%）とコンスタントに増加する見込みとなっている。

近年特に多様化・複雑化する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「インシデント対応関連サービス」である。2014 年度は 69 億円（同+19.9%）となった。2015 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、2015 年度、2016 年度もコンスタントな伸びを見込んでいる。

図 22　国内セキュリティ運用・管理サービス市場推移



2.2.2.4. 情報セキュリティ教育市場

(1)　市場動向

図23に2014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、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が、サイバー攻撃等の専門性のある教育コンテンツは内製が難しいという面もあり、外部のサービスを利用する傾向が高い。そのため、非常に顕著な伸びを見せている。

情報セキュリティ教育は、大きく 3 つに大別できる。

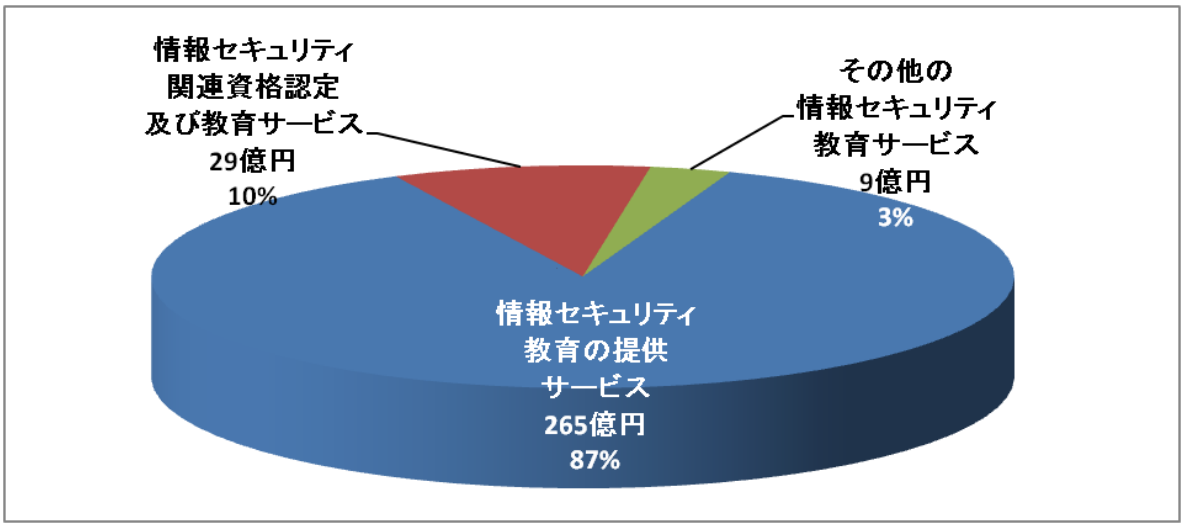
① 新入社員を含む全社員を対象とする情報セキュリティリテラシ教育。知的財産や個人情報の漏えい・紛失のリスク、標的型攻撃の手口とリスクを教え、日ごろの対策や注意点を理解させる。

② システム関係部署や情報セキュリティ対応部署に対する専門教育。

③ 経営層や上級管理職に対しての教育。経営リスクとしての情報セキュリティリスクとそのリスクマネジメントの視点からの知識や考え方の理解を目指したものとなる。

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。

図 23　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 24 にその市場規模の推移のグラフを示す。

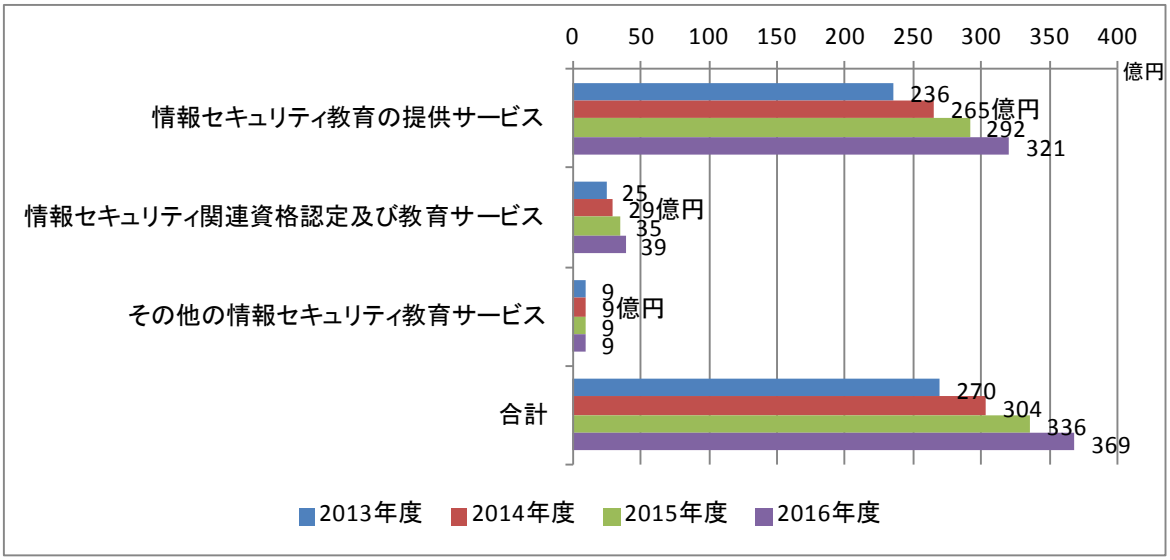
「情報セキュリティ教育」カテゴリは、情報セキュリティサービス全体の市場に占める割合が 8%弱程度と比較的小さい市場であり、2013 年度の市場規模は 270 億円程度と推測さる。2014 年度は標的型攻撃による被害の深刻化や、内部や外注先からの情報漏えい対策への注力が継続的に増加していることを反映して市場は拡大し、12.6%増の 304 億円となった。2015 年度も脅威はより一層深刻度を増しており、伸び率は鈍るものの拡大傾向は続き、10.7%成長して 336 億円程度になるものと推測される。2016 年度も同じ増大傾向が続くものと見られ、9.7%増で 369 億円規模に達するものと予測する。

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）	2013 年度	2014 年度	2015 年度	2016 年度
情報セキュリティ教育の提供サービス	23,575	26,508	29,158	32,074
情報セキュリティ関連資格認定及び教育サービス	2,483	2,935	3,523	3,875
その他の情報セキュリティ教育サービス	922	922	922	922
合計	26,979	30,365	33,603	36,871
構成比				
情報セキュリティ教育の提供サービス	87.4%	87.3%	86.8%	87.0%
情報セキュリティ関連資格認定及び教育サービス	9.2%	9.7%	10.5%	10.5%
その他の情報セキュリティ教育サービス	3.4%	3.0%	2.7%	2.5%
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	―	12.4%	10.0%	10.0%
情報セキュリティ関連資格認定及び教育サービス	―	18.2%	20.0%	10.0%
その他の情報セキュリティ教育サービス	―	0.0%	0.0%	0.0%
合計	―	12.6%	10.7%	9.7%

このセグメントの大部分、約87%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2013年度に236億円、2014年度には265億円（前年度比成長率+12.4%）、2015年度には292億円（同+10.0%）、2016年度は321億円（同+10.0%）と、大幅に拡大すると予測される。

図 24　国内情報セキュリティ教育市場推移



一方、「情報セキュリティ資格認定及び教育サービス」は、2013年度において25億円のマーケットであり、2014度には前年度比18.2%増の29億円の規模になったと推測される。2015年度は情

報漏えい事件・事故の発生によりさらに、資格取得傾向が高まると想定されるので20.0%成長の35億円が見込まれる。2016年度も同様に10.0%増の39億円に拡大するものと考えられる。

昨今の情報漏えい事件を受けて、企業の対策強化や投資拡大、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。また、スマートデバイスやBYOD対策等情報セキュリティに関する教育の需要はますます増加傾向にある。

2.2.2.5. 情報セキュリティ保険市場

(1) 市場の動向

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

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

情報セキュリティ保険の需要者は、通信事業者、金融業や通信販売、小売業のような個人情報を多量に扱う業態、更に製造業その他の一般事業法人等多岐にわたる。販売チャネルも一般の保険販売ルートの他、電機や事務機器の販売代理店等もある。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。

情報セキュリティ事件・事故に対する経営リスクとしての認識が浸透していること、マイナンバー制度に対応した保険商品も増えていることから、今後も堅調な拡大となるとが予測される。

(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 25 にその市場規模の推移のグラフを示す。

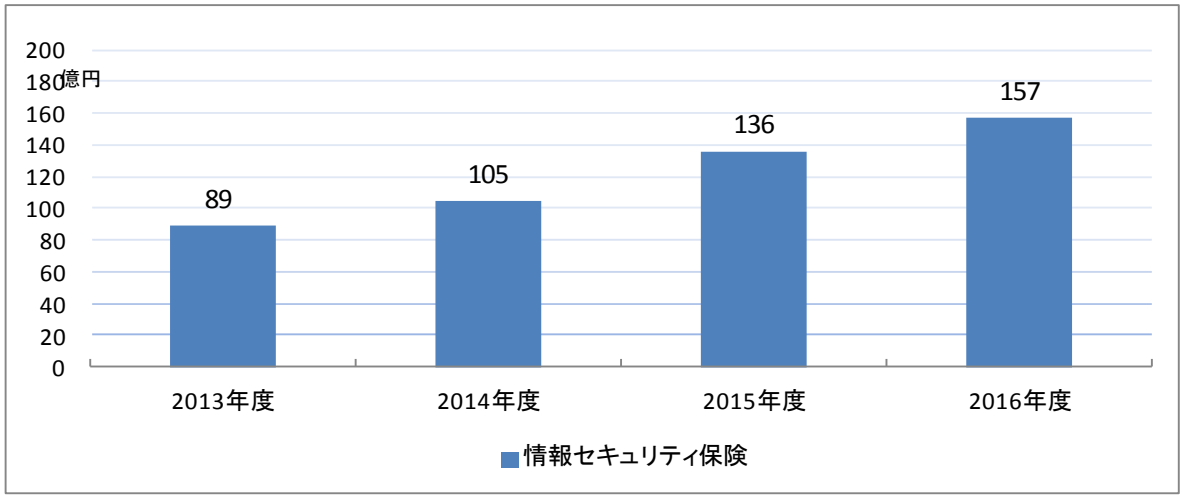
表 14　国内情報セキュリティ保険市場規模　実績と予測

市場規模（百万円）	2013 年度	2014 年度	2015 年度	2016 年度
情報セキュリティ保険	8,885	10,479	13,623	15,667
対前年比成長率（%）	－	17.9%	30.0%	15.0%

「情報セキュリティ保険」市場は、2006 年度に急拡大して 70 億円規模に達した後は落ち着いた動きで推移してきたが、近年は拡大のペースが上がっていると見られる。2013 年度の市場規模は 89 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 2014 年度は 17.9%増の 105 億円と、100 億円市場にまで成長した市場と見てい

る。それがさらに拡大して 2015 年度は 30.0%増の 136 億円となり、2016 年度は 15.0%増の 157 億円にまで達すると予測する。

図 25　国内情報セキュリティ保険市場推移



第３章 情報セキュリティにおける新しい課題と動き

3.1　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、2016 年 4 月 27 日に「情報セキュリティ 10 大脅威 2016　～個人と組織で異なる脅威、立場ごとに異なる対応を」[6]を発表した。この 4 年間の 10 大脅威をリスト化して見ると、以下のようになる。

表 15　最近 4 年間の IPA10 大脅威の推移

	2016 年	2015 年	2014 年	2013 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	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
第 2 位	標的型攻撃による情報流出	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
第 3 位	ランサムウェアを使った詐欺・恐喝	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
第 4 位	ウェヴサービスからの い個人情報の窃取	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
第 5 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
第 6 位	ウェブサイトの改ざん	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
第 7 位	審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ	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
第 8 位	内部不正による情報漏えいとそれに伴う業務停止	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
第 9 位	巧妙・悪質化するワンクリック請求	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
第 10 位	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加	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

（出典：IPA 各年度発表をもとに JNSA 作成）

2015 年版の見出しは「被害に遭わないために実施すべき対策は？」である。2014 年版は「複雑化する情報セキュリティ被害に遭わないために実施すべき対策は？」、2013 年版は「身近に忍び寄る脅威」であった。2016 年版は「個人と組織で異なる脅威、立場ごとに異なる対応を」となっており、初めて個人と組織に分けて修正された。本報告書では、個人と組織を合わせた総合結果で解説していく。情報漏えいやウェブサービスに対する脅威が上位を占めており、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

[6] http://www.ipa.go.jp/security/vuln/10threats2016.html

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。

2016 年は昨年同様、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引き続き高まっている。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、企業側被害もメガバンクから地銀、信金へ被害が拡大し、更に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。

2016 年度の特徴としては、ランサムウェアを使った詐欺・恐喝が 3 位へランキングされた。ランサムウェアに感染すると PC 内ファイルが暗号化され、復元するための身代金を要求される事から、身代金要求型ウイルスとも呼ばれている。2014 年から日本でも検知され始めたが、2015 年に増え始め、2016 年も更に増加するとみられている。

「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[7]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。2015 年度よりも、2016 年度は上位にランクされている。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。2015 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。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 年は上位にランクされていた、内部不正による情報漏えいが 8 位となっている。一昨年発生した、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で、2015 年版は上位ランクとなっていたが、「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」といった問題も引き続き対策が必要である。

---

[7] 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　セキュリティの本質　～安全、安心のための原理の大本を考える ～[8]

3.2.1　業界の人々は、セキュリティの本質を知っているか

日本の情報セキュリティ市場規模が１兆円を超えようとしている。その１兆円市場で禄を食む関係者は、自分たちが扱っている「セキュリティ」、そしてそれにより実現される「安全」、「安心」などのコトバ[9]で指し示されている「そのもの」の本質について、どれくらい深く理解しているのであろうか。

人間が「何が『その具体的な名前で表される対象』か」、例えば「何が犬か」を学ぶ機会は、成長過程で多く存在する。これそのものが、私たちが母国語を身につけるプロセスであるとも言える。一方、逆の「『ある具体的な名前で表されている対象』とは何か」(「犬とは何か」)については、経験的に学ぶ機会はあまり存在しない。「チョコレートはおやつ」、「ケーキはおやつ」、・・・ということは毎日の生活で経験的に学べるのに対し、「おやつとは何か」を、経験的に学ぶ機会はほとんど存在しない。セキュリティについても全く同様であって、日々の経験ベースでは「暗号化はセキュリティ」、「マルウェア対策はセキュリティ」、・・・を知るのみであって、「セキュリティとは何か」の本質を知り、考える機会はほとんど存在しない。

私たちは「おやつとは何か」を意識しなくても、おやつのためのチョコレートを買ったり、ケーキを作ったりすることができる。同様に、「セキュリティ」の本質について考えることを棚上げにしていても、セキュリティのための対策を検討したり、その維持を考えたシステムを構築したりすることは十分可能である。法制や行政など、セキュリティのための制度的な社会インフラを制定、実施することについても同様である。

情報セキュリティに限らず、防犯や防災、食の安全など、現在世の中に提供されている(広い意味での)セキュリティを実現するための、商品、サービス、システム、体制や制度などの多くは「セキュリティの何たるか」の本質をほとんど意識することなしに、対症療法的に世に提供されている。また、これらの「セキュリティのための手段」によって、セキュリティのレベルが上がった事例は少なくない。

しかし、医師が、「健康の何たるか」の本質について考えることを棚上げにした状態で、診察をしたり薬の処方をしたりに追われる状態が好ましくないのと同様に、日々「セキュリティ」に携わっている人間が、「セキュリティの何たるか」の本質について考えることを棚上げにした状態のままで、「セキュリティのための」、「セキュリティのレベルを上げる」さまざまな取組みを行い続けているという現状は、決して良い状況とは言えない。その本質をおざなりにしたままでは、「病気を治して病人を癒やさず」の状態になりかねないからである。医療における「病気を診ずして病人を診よ」という理念は、セキュリティにもそのまま当てはまる。

「セキュリティ」、「不安」、「安心」、これらのコトバで指し示されている「対象」は概念であって、物理的に存在したり、起こったりするものではない。そのため、「その何たるか」は、一般的

---

[8] 本章は、日本ネットワークセキュリティ協会(JNSA)設立 15 周年記念論文「甘利康文： セキュリティとは何か？～安全、安心を実現する原理をその本質から理解する～」の内容を要約、一部加筆を施したものである

[9] 本章では、「ある対象」を指し示す役割をするもの(表記：[近代言語学におけるシニフィアン])を「コトバ」と表している。

に使われている自然科学的なアプローチやエンジニアリング手法によって解明することは難しい。このことから、本章では、先人が遺してくれた「『ある概念』の何たるか」を探索するための方法論である「哲学の理路」の一部を道具として使い、その視点から、これらの正体について考えていく。

本章が最終的に目指すところは、情報セキュリティを含む広い意味でのセキュリティに関係する産業界にいる人々に対し、Semantics(意味論)的観点から「セキュリティの何たるか」についての本質を示し、私たちの日々の生活に欠かせない「セキュリティ」をより高いレベルで実現する指針を提示することである。

3.2.2 「認識」についての認識

・二元論

人は皆、世界が自分の外に拡がっており、その中で生きる自分達は、視覚、聴覚などの知覚によってその世界を認識していると考えている。私たちが生まれてきたときから慣れ親しんで来た、「外を主、人の抱いた内なる『感じ』を従」とする一般的な考え方である。たとえば、「なにか『黄色い色のもの』が自分の外の世界にあって、それを視覚で認識することで、『黄色』を感じている」という考え方である。

この「まず、原因としての何モノかが自分の外にあって、私たちは、知覚によってそれを認識する、つまりそれを感じることで、結果としてその存在を感じている」とする考え方は、もともとはデカルト(1596-1650)によって提唱されたものであり「二元論」と呼ばれている。

二元論、すなわち世界には「主観：認識する『主体』」と「客観：認識される『客体』」があって、そのうえで認識の主体(主観)である「意識」が、自分の周りにある「世界」を客体(客観)として理解、把握しているという考え方は、科学的な態度の基盤をなす思想として、科学を大きく進歩させる原動力となり、現代社会においては常識のように感じられるようにもなっている。

現代に生きる私たちにとっては、疑う余地がなく、至極当然のように感じられるこの考え方は、その一方で、「主体(主観)としての意識は、客体(客観)である世界を『正しく』把握できるのか」という人の「認識」に関する一大問題を生じさせた。

形のある物体(モノ)を対象とした場合、そのモノに対する認識は人によって大きくブレるものではない。従って、この場合、ある一個人の認識をベースに論を展開しても、それは一般性を失わず、多くの人間が納得できるものとなる。科学はこのようにして進歩し、さらにその知見は「科学技術」の形に結実して、私たちの日々の生活に役立つものとなっている。

一方、「概念」や「感覚」、「価値」など、実体を持たない存在(コト)が認識対象(客体)の場合、認識主体としての人が持つ感覚(主観)は、人それぞれになるのが普通である。例えば、「日本経済」のような対象の認識では、エコノミストによって見解が分かれるのはよく見られることである。自然界で具体的な形を持たない存在(コト)が認識対象(客体)の場合、ある人物が認識したことを敷衍して一般化し、「万人が納得できる知見」(科学的な知)や、その応用である技術にしようとしても、なかなか一筋縄では行かないのはこれが理由である。

セキュリティのための機器やシステムなどは実体を持つモノである。従って、これらを進歩させるために、科学的手法は道具として有効に機能する。実際、セキュリティを実現するための手

段である機器やシステムなどは、そのようにして研究、開発され、進歩してきた。

しかし、これらの機器やシステムなどによって実現する「セキュリティ」、そして人々が感じる「安全」や「安心」というコトバによって指し示されている「そのもの」は、「実体を持たない概念」(コト)である。それゆえ、セキュリティそのものや安全、安心といった対象を客体として扱う場合、いわゆる「科学的手法」は、道具として必ずしも有効に機能しない。「実体を持たない存在」(コト)を扱う際には、これらを客体として認識する主体としての「人の主観」が問題となるからである。

・現象学

これに対して、「主と従、原因と結果を逆転させる考え方」の体系がある。認識を、「『主観(としての意識)がそれを感じている』ということが原因となって、私たちの意識(主観)に、外に『それがある』という確信を抱かせる結果をもたらしている」とする考え方である。いわば「人が抱いた内なる『感じ』を主、外の世界を従」とする認識論である。この「人の感じ方を主」とすることを起点として構築された「認識に関する考え方」が、フッサール(1859-1938)が見出し、体系化した「現象学」である。先の例を、この考え方で表現すると「視覚が『黄色』を感じているから、私たちの意識はそこに『黄色い色のものがある』と確信している」となる。

一見、言葉遊びのようでもあるが、この「人の感じ方を主」とすることを出発点に構築された「人がものごとを捉えること」に関する考え方、現象学は、現代の学術分野にも大きな影響を及ぼしている。

「外を主、人の『感じ』を従」とする考え方、デカルトを祖とする二元論では、外の世界に「存在があること」を前提とする必要がある。たとえば「黄色を感じること」を実現するためには、黄色い色の物体を持ってきて、そこからの光を目に入れることで「黄色」を感じるようにする必要がある。

一方、「人の抱いた『感じ』を主、外を従」とする考え方、フッサールによる現象学では、外の世界に「存在があること」を前提とする必要はない。「黄色」を実現するために、必ずしも黄色い色の物質を持ってくる必要は無いと言うことである。人間の認識は、「黄色」を感じれば、そこに黄色い色のものがあると根拠がなくても信じ込むように出来ている。そのため、「黄色」を感じさせることさえ出来れば、その手段は何でも良いということになる。

人間の視覚は「赤」と「緑」の光が同時に目に入ることで「黄色」を感じるようになっている。すなわち、赤と緑の光で黄色を表現できるということである。実際、ディスプレイの画面上で「黄色い花」を表現するために「黄色」い光は必要なく、「人が黄色を感じる」ための赤と緑の光があるだけで良い。この方法による色再現は、人特有の視覚の感じ方をベースに構成された技術であるため、人と全く構造が異なる視覚や認識のシステムを持つ宇宙人がいたとすると、ディスプレイの上に映し出された「黄色い花」が、彼には全く異なる何ものかに見える可能性がある。このように、現在使われているカラーディスプレイや印刷による「色再現」は、現象学の基本的考え方と、３原色を基本とした人が色を感じる感じ方をベースとしている。

私たちが、モノゴトを理解する認識主体は「意識」である。意識は、私たちの「肉体」の中に閉じ込められており、外に出ることはできない。そのため、意識は、自分の肉体の外が「実際に

はどうなっているか」という「本当のところ」を知ることはできない。一方で、肉体に閉じ込められた意識には、肉体に備わった目や耳などのセンサーからの「外の世界」の知覚情報や、記憶などからの情報がもたらされる(これを「意識に現象する」と表現する)。認識の主体である意識には、もしかすると「本当ではない[10]」のかもしれないのに、これらの情報を、根拠なく信じ込むことしか選択肢が残されていない。肉体に閉じ込められた私たちの意識は、このようにして、世界を把握、理解しているわけである。

「世界」は、自分の外に広がっている存在ではない。それぞれの人の内なる意識の前に立ち現れる(現象する)ことによって意識が感じている存在が「世界」である。これが現象学の基本的考え方である。すなわち、「世界」は、主観としての意識の前に立ち現れる(現象する)のであって、外側にあるのではない、というのが現象学の解釈である。

3.2.3 「意識」が追い求めるもの

私たちが、モノゴトを把握する認識主体、「意識」は、本能とも呼ぶべき共通の特性を持っている。「快という感覚を求め、逆に不快を避ける」という共通特質である。

もともと人は、一個体として自らの命を維持したり、自らの遺伝子を次世代に残したりする行為への生物としての欲求、そして、これらの欲求が満たされたときに「快」を感じ、満たされないときに「不快」を感じるような本能的特質(報酬系)を持っている。これが、「『個や遺伝子の生に近づくこと』から『快』を感じ、『遠ざかること』からは『不快』を感じる」という人の意識が持つ特質、本来の意味での「エロス[11]」である。

人の意識が持つ「快」を求め、「不快」を避ける本能は、「私たち人間が、『自ら、そして自らの遺伝子の生(以後「広義の生」)』に少しでも近づきたい存在である」ということに他ならない。人は、みずからの内なる意識の持つこの特性に支配されて、無意識のうちに「快」を求め「不快」を避けるように振る舞っている。意識の持つこの特性に例外はない。好奇心や向上心、自由欲、支配欲、名誉欲なども、直接、間接に「快」を求め「不快」を避ける(すなわち「広義の生」を求める)という意識の特質が姿を変えたものである。

人の活動の全ては、「広義の生への接近」によりもたらされる「快を感じること」を求め、不快を感じること(すなわち「広義の生からの離遠」)を避けるという「意識の特質」から発しているという理解が可能である。

私たちが、額に汗して働くのは、その行為が、直接的には「日々の糧を得ること(生理欲求)」、そして長い目で見た場合は、その行為が社会欲求や承認欲求の充足につながり、そこから「快」の感覚が得られるからである。もちろん、疲労やストレスなどの意識に「不快」をもたらす要因は無視できない。それにもかかわらず、私たちが働くのは、労働によって得られる収入や達成感、周りから認められることなどによる「快の感覚」が、それによる疲労感などの「不快な感覚」に勝っているからである。その証拠に、私たちは、働くことによってもたらされる「不快」が「快」より大きい場合、その大本になる労働を続けることはできない。

---

[10] 操作された情報提示によって認識主体である意識がだまされるケースが「錯覚」である。

[11] いわゆる性的欲求に関連することによく使われるようになった用語だが、本来は、これに限らない広い意味を持つ。

現代社会では、お金は「日々の糧」、そして様々な「広義の生に近づく手段」が姿を変えたものである。これが増えることは「広義の生に近づくこと」、減ることは「遠ざかること」である。それゆえ、人は手元にあるお金が増えることに「快」を、減ることに「不快」を感じる。お金と「モノやコト」を交換する「購入」という行為は、手元のお金が減る「不快」よりも、代わりに手に入るモノゴトがもたらす「快」の感覚の方がより大きい(はず)という確信もしくは予測から発する。そのため、購入後に感じる「快」が思いの外大きい場合、人は、お買い「得」と感じ、逆に小さい場合は「損」と感じる。

人は、(通常は無意識のうちに)ある行動によって得られると予想される「快」と「不快」を比較し、「快」が大きいと感じるときその行動を起こす。これには例外がない。歴史上、聖人と呼ばれてきた人物の(無私のように見える尊敬される)行動も、その人間にとって、その行動によって得られる「快」の感覚が、しなかったときの「不快」の感覚よりも大きいと感じられたからである。結局、人は「気持ち良いかどうか」に支配され、「気持ちの損得感情で動く」ということである。

人の意識は「広義の生」に近づくこと、すなわち「得」(快)を求め、そこから遠ざかる「損」(不快)を避ける。人の行動の全ては、この「意識の特性」に支配されているといっても過言ではない。「損得勘定」という四字熟語(コトバ)は、「『快』を求め、『不快』を避ける」という、「人の意識が持つ本質」をうまく言い表している。損得勘定は、実は人の意識の本質、「快・不快勘定」なのである。

3.2.4 セキュリティとは何か　～「組織」そして「オペレーション」の本質 ～

繰り返しとなるが、「セキュリティ」というコトバによって指し示される「そのもの」は、概念であり実体を持たない。そのため、これまで述べたように「セキュリティの何たるか」についての認識、すなわち意識にもたらされる(現象する)イメージは、人それぞれとなって、複数の人間の共通認識はなかなか成立しない。実際、「セキュリティ」というコトバは、防犯、情報システム、エネルギー問題、食糧問題、国防など、現れる文脈によって様々な意味合いで使われている。

世の中の「セキュリティ」という言葉が使われているケースを抽象化、一般化することで導出した「セキュリティの定義」を提唱し、その考え方を体系化しようとする試みがある。その定義では、セキュリティとは「対象となる組織のオペレーション(日々の営み)が、運営主体によってあらかじめ定められたプランに則って運営され、理由の如何によらず、それが阻害されないこと」であり、セキュリティ対策によって守るべきそもそもの対象を「組織のオペレーション」としている。情報漏洩や風評被害など、オペレーションを阻害する何らかの要因がインシデント(事故)である。

一般に、セキュリティを考える際には、人・物・金、そして情報をインシデントから守る必要があると言われる。これらは、組織を運営するために必要なもの、「リソースプロパティ」であり、保全されないと、その組織のオペレーションは、あらかじめ定めたプラン通り回らなくなる。それゆえ、「組織のオペレーションが回り続ける状態」を実現するためには、これらのリソースプロパティを守る必要が生じる。

組織のセキュリティを考える場合、人・物・金、そして情報などのリソースプロパティを守る

ことに目が向いてしまいがちになる。しかし、「本来のセキュリティ」のそもそもの「守るべき対象」は、いかなる場合においても、その組織の「オペレーション」であるというのが、その「セキュリティの定義」から導かれた主張であった。

一方、その「セキュリティの定義」には「組織」そして「オペレーション」というコトバが、何を指し示すのか明言されることなく現れる。ここでは、これまで論じた内容をベースに、「組織」、そして「オペレーション」を考え、「セキュリティ」に関する理解を深めていく。

前述したように、あらゆる個人は、内なる意識に支配され、「広義の生」を求めることで「快」を得るように、また、「広義の生」から遠ざかる「不快」を避けるように行動する。そのため、複数の「個人」によって構成された存在である「組織」は、基本的には関係する各個人が感じる「快」の総和を最大化、「不快」の総和を最小化するように行動する。

「組織」というコトバが指し示している「そのもの」は、物理的な実体を持たない。組織とは、あくまでも、複数の個人(ステークホルダー)が「ある目的」を達成するために複合した概念上の存在である。この考え方は、セキュリティを考察するうえにおいて、非常に重要である。

その「組織」が自動車メーカーである場合、「ある目的」とは「『良い車を提供すること』で、組織に関係する各ステークホルダーが得る『快』の総和を最大化、『不快』の総和を最小化すること」である。すなわち、(1)車を購入する顧客には「代金支払い(お金の減少)による『不快』に勝る『快』(満足)を感じてもらうこと」、(2)働く人間には「労務の提供やそれにより生じるストレスなどによる『不快』に勝る賃金を支給し、同時にやりがいなどの従業員満足（共に働く人間にとっての『快』)を感じてもらうこと」、そして、(3)組織の活動資金を出している株主には「そのリスク(不快)に勝る「配当とキャピタルゲイン」(お金の増加)を提供し、投資家としての『快』を感じてもらうこと」、これらの「目的」のために存在するのが、自動車メーカーという「組織」である。

組織の種類が、例えば自動車メーカーからホテルに変わっても、目的を実現するための手段が、「良い車の提供」から「快適な滞在環境の提供」のように変わるだけで、「各ステークホルダーが得る『快』の総和を最大化、『不快』の総和を最小化すること」という、組織の本質的な目的自体は変化しない。ここから、あらゆる組織は、「組織に関係する各ステークホルダー(個人)が得る『快』、『不快』の総和を、それぞれ最大化、最小化する」という「オペレーション」を実現するために存在しているという理解が可能となる。

ここまでのセキュリティに対する考察をまとめると次のようになる。セキュリティを考える場合の守る対象である「組織のオペレーション」とは、「組織に関係する各ステークホルダー(個人)が得る『快』、『不快』の総和を、それぞれ最大化、最小化する」行為のことである。組織は、これを実現しようとする際に、犯罪被害や情報漏洩などの、その所作を阻害する要因(インシデント)に直面する場合がある。それゆえ組織には、インシデントが起こり、オペレーションに影響を及ぼすことを想定して、その影響を最小化するための施策(セキュリティ対策)を行う必要性が生じる。これらの一連の概念を包括して一言で指し示すコトバが「セキュリティ」である。

セキュリティにより実現する「安全、安心」は、主観として、組織に関係する個人、一人ひとりの意識の前に現れている確信のことである。「安心」は、自らの「快」が最大化され「不快」が最小化されるだろうという確信、「安全」は、「快が最大化、不快が最小化されている」と、「多く

の人の意識が確信するに違いないと合理的に考えられる状態」のことである。そのため「安全」を感じてもらうためには、例えば確率値のような形で、「多くの人が合理的と納得するに足る(科学的な)情報」を提示する必要がある。

ここから、多くの人が「安全」と認める状態であっても、ある一個人の意識に必ずしも「安心」が現象する(立ち現れる)かどうかは保証できないことが解る。安全は客観、安心は主観と言われることが多いが、安心のみならず安全も、結局のところ、個人の意識に立ち現れた観念(主観)であることに注意が必要である。与えられた合理的と信じるに足る情報によって、大多数の人間が「大丈夫と感じている」状態が「安全」の正体である。

3.2.5 Happiness の最大化

あらゆる組織は、その種類によらず、「関係するステークホルダーの一人ひとりに現象する(『意識』が感じる)『快』、すなわち各個人の Happiness の総和を最大化する営み」である「オペレーション」を行うために存在する。「様々なインシデントが起ころうとも、この『オペレーション』が乱されない」ということが「セキュリティの本質」である。

過去、個人情報保護法の施行時に、人々の間で、一部行き過ぎとも見える反応が見られ、世の中で回る様々なオペレーションを逆に妨げかねない状況が散見された。これは、世の中に対するセキュリティのための対策が、逆に働き、新たなインシデントになった一例だったとも考えられる。何らかのセキュリティ対策を行う際には、同様の事態が起こらないように注意する必要がある。

たとえどのようなことが起ころうとも「一人ひとりの感じる Happiness の総和を最大化する営み」である「オペレーション」を維持しようとするコトが、「セキュリティ」というコトバで表されている「そのもの」だということを忘れないようにしたい。

組織は存在しない。実際に存在するのは、組織に関係するステークホルダーの個人、一人ひとりである。日本の情報セキュリティ市場が 1 兆円規模を超えようとしているのは、その一人ひとりが、自らの Happiness を追い求めてやまないところから来ている。研究や技術開発、商品の企画・開発、システム構築、さらには法律や行政などの社会制度の整備など、様々な分野で、また様々な形でセキュリティに携わる人間が、「セキュリティの本質」を強く意識し、日々の仕事に邁進することで、世の中は良い方向に変わっていくことだろう。

【参考文献】

[1] 甘利康文：セキュリティとは何か？ ～安全、安心を実現する原理をその本質から理解する～，日本ネットワークセキュリティ協会(JNSA)設立 15 周年記念論文(2015),
http://www.jnsa.org/seminar/2015/nssf15/data/103_AmariYasufumi.pdf
日本セキュリティ・マネジメント学会誌, Vol.29 No.3 pp.15-29 (2016)

[2] JNSA 組織で働く不正・自己対応ワーキンググループ： 内部不正対策 14 の論点（第 1 部 セキュリティの本質），インプレス R&D (2015)

[3] 池田清彦：構造主義科学論の冒険，講談社学術文庫 (1998)

[4] 西條剛央：構造構成主義とは何か 次世代人間科学の原理，北大路書房 (2005)

[5] R.デカルト：方法序説 (山田弘明 訳)，ちくま学芸文庫 (2010)

[6] E.フッサール：ヨーロッパ諸学の危機と超越論的現象学(細谷常夫、木田元 訳)，中央公論社 (1974)

[7] 竹田青嗣：完全解読 フッサール「現象学の理念」，講談社 (2012)

[8] 竹田青嗣：現象学入門，NHK 出版 (1989)

[9] 竹田青嗣：はじめての現象学，海鳥社 (1993)

[10] 竹田青嗣：現象学は「思考の原理」である，筑摩書房 (2004)

[11] 竹田青嗣：エロスの現象学，海鳥社 (1996)

[12] 山口一郎：現象学ことはじめ[改訂版]，日本評論社 (2012)

[13] 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.5-8 (2006)

[14] 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)

【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。「2015 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) 2013 年度国内情報セキュリティ市場規模　推定実績値
(2) 2014 年度国内情報セキュリティ市場規模　推定実績値
(3) 2015 年度国内情報セキュリティ市場規模　実績見込値
(4) 2016 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 2014 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ー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 497 社（JNSA 会員企業 164 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 27 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 2014 年度である。2015 年度、2016 年度の市場規模推定にあたっては、2014 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[12]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

[12] 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[13]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

[13] 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	571	91	128	73	111	35	27	82	24
有効推計対象	497	62	113	71	101	35	22	73	20
情報セキュリティツール全体（X）	344	58	87	62	74	29	3	24	7
統合型アプライアンス	85	10	7	22	23	17	1	5	0
ネットワーク脅威対策製品	160	25	22	32	44	23	1	11	2
コンテンツセキュリティ対策製品	185	27	37	40	44	21	1	14	1
アイデンティティ･アクセス管理製品	160	18	36	26	45	23	2	8	2
システムセキュリティ管理製品	164	22	34	33	42	17	2	11	3
暗号製品	84	12	10	18	27	10	1	3	3
情報セキュリティサービス全体（Y）	289	22	38	25	75	33	21	61	14
情報セキュリティコンサルテーション	153	9	13	11	41	22	15	41	1
セキュアシステム構築サービス	157	9	17	14	53	29	9	23	3
セキュリティ運用･管理サービス	181	18	22	20	46	25	9	34	7
情報セキュリティ教育	94	4	9	6	21	16	7	28	3
情報セキュリティ保険	19	1	0	2	3	3	2	3	5
（参考）									
ツール専業（X∩~Y）	173	39	59	40	22	2	0	7	4
ツール･サービス兼業（X∩Y）	171	19	28	22	52	27	3	17	3
サービス専業（~X∩Y）	118	3	10	3	23	6	18	44	11

また、今回調査対象企業数（有効推計対象ベース）は 497 社となった。2011 年度調査 358 社、

2012 年度調査 422 社、2013 年度 463 社であったので、年を追うごとに調査対象企業数は増加している。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 173（昨年 169、一昨年 150）、サービスのみに特化する事業者が 118（昨年 106、一昨年 104）、両方を提供する事業者が 171（昨年 188、一昨年 168）と、推移している。

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、2014 年度は

（1） 海外ベンダの市場シェアは引き続き大きい：3 割前後と、特にツールの依存度は高い

（2） 国内ベンダはサービス中心にソリューション面で貢献が続く

（3） 2010 年代に入り国産ベンダの数と参入製品分野が徐々に拡大傾向にある

という特徴が反映されてきており、この傾向は 2015 年 2016 年も継続すると考えられる。

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、国際通貨基金（IMF）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 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 年からは 2%台の高い成長率で推移している。世界全体として、世界第 2 位の GDP をもつ中国経済の景気減速により、今後の動向が注目される。

表 20　GDP 実質成長率の推移（単位%）

暦年	2009	2010	2011	2012	2013	2014	2015	2016
世界	0.0	5.4	4.2	3.4	3.4	3.4	3.1	3.6
日本	-5.5	4.7	-0.5	1.8	1.6	-0.1	0.6	1.0
米国	-2.8	2.5	1.6	2.3	2.2	2.4	2.6	2.8

（出典：IMF2016 年 4 月レポート[14]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により 2011 年度は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、更には消費税増税の影響からか 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。

2012～2016 のスパンで見ると、アメリカの堅調な経済成長がはっきりと見て取れる。世界経済も 3%台の成長軌道をたどっている。落ちたりとはいえ 6%を超える成長率を示す、世界第二位の経済大国である中国や、成長著しいインド経済などの新興経済の力に負うところが大きいと考えられる。その中で日本の低調は明らかである。アベノミクス第 2 の矢の奏功に期待したい処であるが 2015 年から変調が見られ、消費税増税も先送りの決断を余儀なくされている。中国経済のバブル崩壊、EU 内向き志向や英国離脱問題、米国大統領選の混迷など、世界的に不確定要因が増す中で、引き続き厳しい経済状況が続くものと覚悟する必要がありそうである。

2015 年春闘では 2 年連続 2%増と賃金改善にも一定の成果が見られ、2015 年段階ではデフレ脱却への期待も高まっていた。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かのように見えるが、リーマンショック後回復したのは 2010 年度だけで、2011 年度は震災ショックで低迷など、2013 年度まではもたつき気味であった。アベノミクスも 2013 年の円安株高効果だけで、企業業績は企業努力もあり回復したが、規制改革がもたついているために構造転換が進まず、経済成長には火が付かないままの状態が続

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

いており、2015 年以降は上に見たように世界経済の変調にさらされているのが現状であるといえる。楽観視はできない状況にある。

図 26　日本経済研究センター「短期経済予測」

（実質GDP成長率前年比、%）

	14年度	15年度	16年度	17年度
SA165	▲1.0	0.7	1.0	0.1
SA165R		0.7	1.0	0.1

（資料）内閣府『四半期別GDP速報』
日本経済研究センター第 165 回改訂短期経済予測（2016 年 1-3 月期～2018 年 1-3 月期）
https://www.jcer.or.jp/research/short/detail4993.html）

図 26 は日本経済研究センターが 2016 年 3 月に発表した 4 半期予測である。2014~2015 年度の需要部門別成長寄与度をみてみると、民間需要が依然として牽引力にならず、外需、それも円安よりはむしろ原油安の恩恵で得られた黒字が支えているという構造が読み取れる。予測は民間需要の寄与度を大きく見ているが、国際情勢の不確実性が高まる中で、どの程度経済のダイナミクスが働くのか、見通しは明るいとは言えない。

(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、リーマンショックや東日本大震災の時期を含む期間の調査に比べると、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、2012 年度、2013 年度と回復している。2014 年度、2015 年度については、率は下がるものの増益傾向にある。2015 年度は円安の影響もあり、訪日外国人消費の恩恵が働くる中で推移したものと考えられる。

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%）						
2010 年度	2011 年度	2012 年度	2013 年度	2014 年度	2015 年度	2016 年度
43.8%	−12.1%	12.8%	37.4%	6.9%	5.5%	6.3%

（出所：野村証券企業業績見通し　2016 年 3 月 2 日版[15]）

表 22 は、日本銀行が 4 半期ごとに行う短期経済観測調査（短観）からの抜粋である。同調査は、景況判断を示す DI 指標（Difusion Index）が特徴的である。2016 年 3 月調査によれば、表

15 http://www.nomuraholdings.com/jp/news/nr/nsc/20160302/20160302.pdf

に示すように、景況を「良い」と判断する企業の比率が「悪い」を上回っているが。2 四半期ぶりの悪化となった。中国をはじめとする新興国経済の減速や円高を受け、「鉄鋼」や「電気機械」、「自動車」などの輸出関連を中心に幅広い業種で企業心理が慎重姿勢に転じたものとみられる。

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
2015 年 12 月	18	13	14	8	3	−2
2016 年 3 月	13	11	12	5	1	−4

（出所：日本銀行　第 168 回 全国企業短期経済観測調査　2016 年 3 月調査[16]より JNSA 抜粋）

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ため、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 年度の実績はいずれの調査でも高い伸び率を示している。一方 2015 年度については大企業（政策投資銀行）が伸び率を高めるのに対して中小製造業（政策金融公庫）は一転マイナスを見込んでおり、先行き見通しがばらついていることを感じさせる。またセキュリティ投資に最も関連が深い全産業ソフトウェア投資は、2014 年度には 3.0%と増加を示すものの 2015 年度見込みは 0.3%増と、一服感が出ていた可能性がある。

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	2014 年度 実績	2015 年度 見込	2016 年度 予測
大企業	政策投資銀行	2015 年 8 月	6.3%	13.9%	7.3%
中小製造業	政策金融公庫	2015 年 6 月	10.2%	−7.6%	−
全産業*1	日本銀行	2016 年 3 月	8.3%	7.1%	−1.5%
全産業*2			3.0%	0.4%	1.5%
（*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 2015/8 月公表[17]、政策金融公庫中小製造業設備動向調査 2015 年 6 月公表[18]、日本銀行全国企業短期経済観測調査 2016 年 4 月公表[19]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

16 http://www.boj.or.jp/statistics/tk/gaiyo/2016/tka1603.pdf
17 http://www.dbj.jp/investigate/equip/national/pdf_all/201508_plant.pdf
18 https://www.jfc.go.jp/n/findings/pdf/news270622a.pdf
19 http://www.boj.or.jp/statistics/tk/gaiyo/2016/tka1603.pdf

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[20]」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。

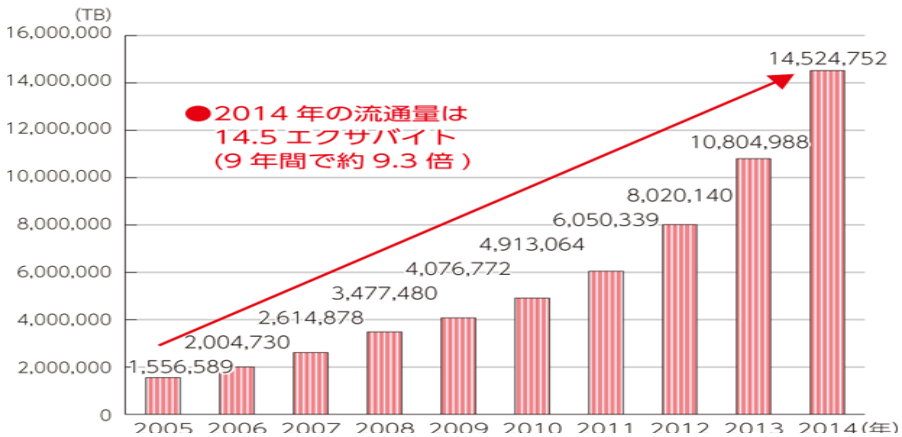
次に考えられるのは事業のライフサイクルである。IT が支える事業の新陳代謝が活発になれば、そのための IT も変化する。特にネットビジネスではそのサイクルは極端に短く、最短 1 年のようなこともありうると考えられる。

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

しかし、現実に業務プロセスはそこまでの速度では変化せず、経験則的には 3～4 年がサイクルの目安と考えられる。一例では、マイクロソフトのオフィスシリーズのバージョンは、97、2000、2003、2007、2010、2013、2016 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。

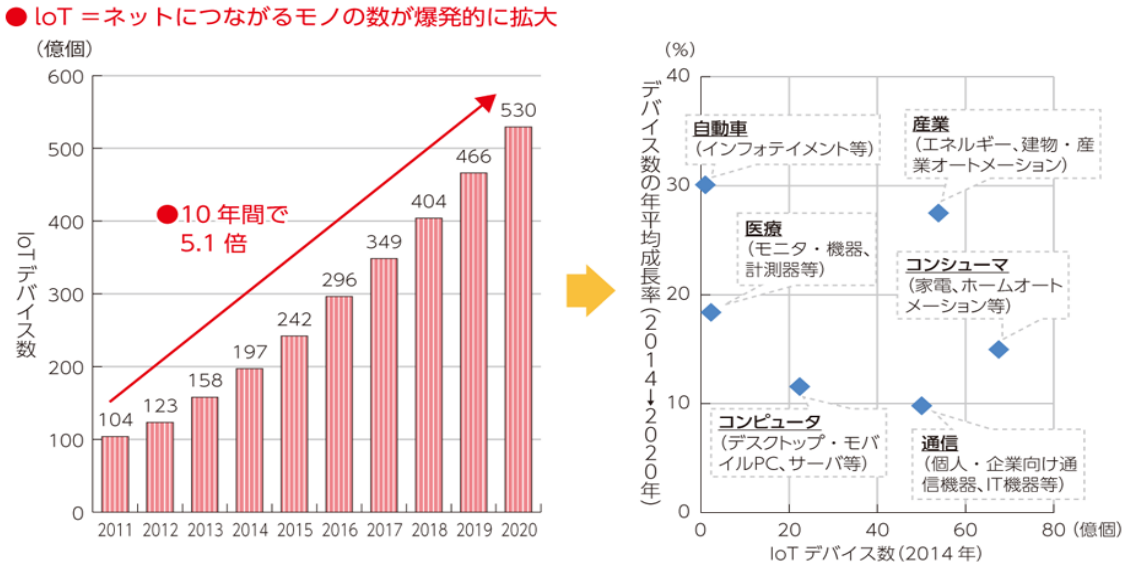
同様に、通信ネットワークの容量も IT 投資サイクルに影響を与えると考えられる。総務省が発行する情報通信白書は通信データ量について様々なデータを提供しているが、平成 27 年版[21]では、情報流通量の推移と IoT デバイスの普及に関する推定値を載せている。情報通信量としては、図 27 に見られるように、2005 年~2014 年で約 9.3 倍にまで膨れ上がっている。通信量の増加に比例して、企業では設備投資が必須になっていくと予想される。設備投資が増えるとそれに比例して、セキュリティの考慮も必要になってくるため、セキュリティ市場の活性化も見込まれる。

図 27　平成 27 年版 情報通信白書　情報流通量の推移



[20] http://www.ipa.go.jp/about/jigyoseika/04fy-pro/chosa/srm/index.pdf

[21] http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27/html/na000000.html



（出所：総務省「情報通信白書平成 27 年版」より）

IoT デバイス数は、10 年間で 5.1 倍となっており、今後は様々なデータが IoT を通じて収集・分析され、業務効率化等につなげる動きが活発化されると予想されることから、爆発的に拡大すると予想される。IoT デバイスの増加にも、上記のサイクルが当てはまると考えられる。

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 年が IT 投資サイクルとなる。

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。

(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）[22]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）[23]統計を加味し、本調査結果と比較したデータを表 24 に示す。

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 4 種類の統計をピックアップした。表 24 では、「IT 出荷計（JEITA）」の欄で、各々「PC 出荷」「MF、Srv、WS 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 24 に見られるように、2014 年度の IT 出荷は全体で前年度比から微減となっており、これは PC 出荷が数量・金額とも落ち込んだ影響が大きい。

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

表 24　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		2013 年度	2014 年度	2015 年度
		千台/億円	千台/億円	千台/億円
セキュリティ出荷計	金額	7,770	8,428	9,202
IT 出荷計(JEITA)	金額	69,016	67,681	-
PC 国産出荷	台数	12,109	9,187	6,108
	金額	9,263	7,336	5,374
メインフレーム（MF)、サーバ（Srv)、WS 出荷	台数	423	390	-
	金額	3,608	3,478	-
ソフトウェア	金額	7,669	8,146	-
SI 開発	金額	27,708	29,113	-
BPO その他サービス	金額	20,768	19,608	-
(SW,サービス計)	金額	56,145	56,867	-
・ネットワーク関連機器				
生産	金額	5,369	5,287	-
輸入	金額	6,193	6,472	-
輸出	金額	1,448	1,716	-
国内出荷	金額	10,081	10,043	-
IT+NW 装置	金額	79,097	77,724	-
セキュリティ市場との比率				
対 IT 出荷計(JEITA)※1		11.1%	12.4%	-
対 IT+NW 装置※2		9.6%	10.8%	-

※1 セキュリティ出荷計÷IT 出荷計(JEITA)、※2 セキュリティ出荷計÷IT+NW 装置

（出典：JEITA、CIAJ の統計を元に JNSA 作成）

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、2013 年度で 9.6%、2014 年度で 10.8%と、概ね IT 投資の 1 割を占めるようになってきている。これは、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結果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 2014 年版[24]であり、対象年度は 2013 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。

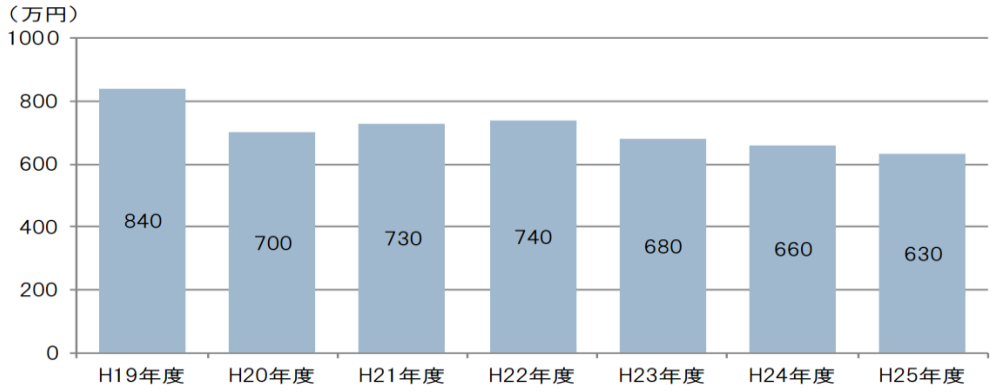
◆ 情報セキュリティ対策費用の状況

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図 28 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ており、調査対象である 2013 年度までは近年減少傾向で推移している。

[24] http://www.meti.go.jp/statistics/zyo/zyouhou/result-1.html　（2015 年 6 月 4 日発表）

図 28　一社平均情報セキュリティ対策費用



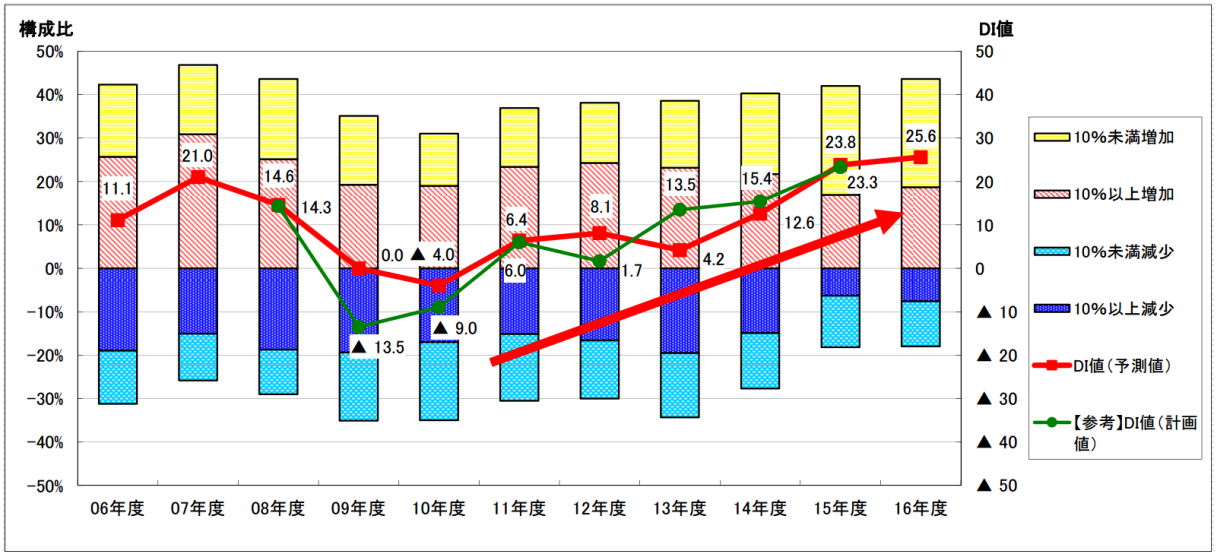
【一社平均情報セキュリティ対策費用(加重平均による推計) [25]】
（出典：経済産業省平成 26 年度情報処理実態調査より）

なお、上の表にある 1 社平均 630 万円という情報セキュリティ対策費用に回答企業数 5,210 社を掛けると 3,282 億円となる。同調査の回答率は 44.5%となっており、調査対象企業全体では約 7,376 億円という試算値が得られる。本調査の 2013 年度の推定値が 7,770 億円であり、非常に近似の数値となっていることが確認できる。

(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。2015 年度調査結果の概要は 2016 年 4 月 22 日にプレスリリースとして公表[26]された。

図 29　IT 予算の増減調査（2006 年度～2015 年度）



（出典：JUAS　企業 IT 動向調査 2016 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 29 のような回答分布となっている。IT

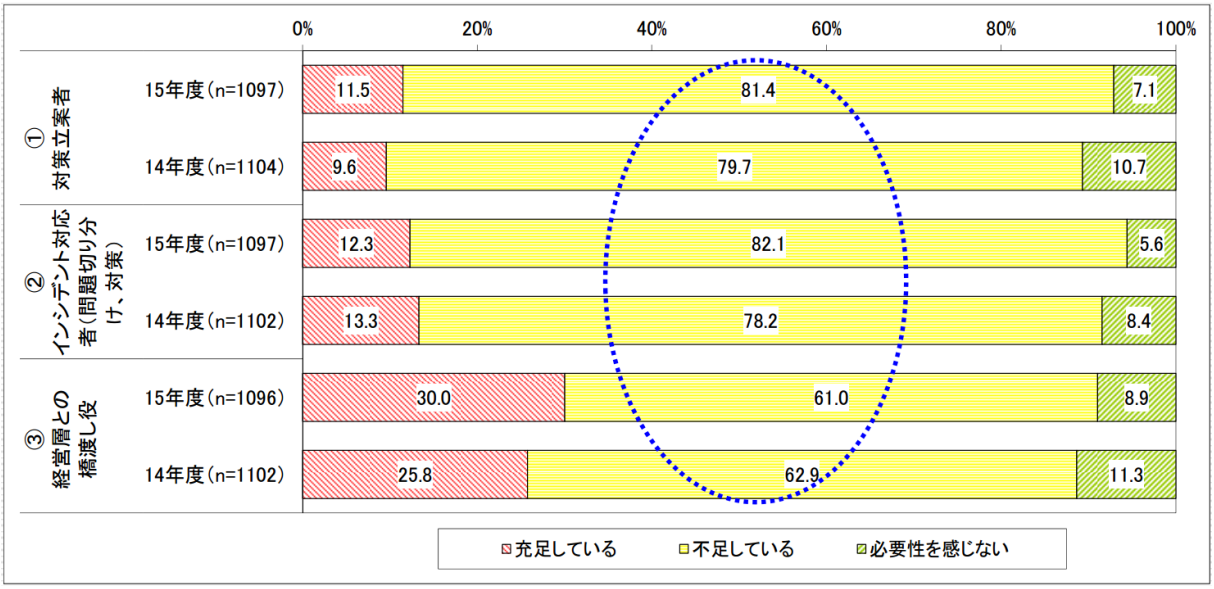
[25] http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/H26_report.pdf
[26] http://www.juas.or.jp/servey/it16/#pr2

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 23.8 となり、2016 年度も IT 投資を積極的に行う傾向となっており、DI 値はさらに増加し 25.6（予測値）となっている。

2016 年度予測の DI 値 25.6 はリーマンショック前の 2007 年度予測の 21.0、過去 10 年で最大の伸びとなった 2014 年度の 23.8 をともに上回っている。

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 30 にあるように「対策立案者」「インシデント対応者（問題切り分け、対策)」は、約 8 割 の企業が「不足している」と回答。 「経営層との橋渡し役」は、他の役 割よりも若干改善しているが、それでも約 6 割が「不足している」と回答している。内閣サイバーセキュリティセンター（NISC）が発表した「サイバーセキュリティ戦略」（平成 25 年 6 月 10 日情報セキュリティ政策会議決定） によると、国内で約 8 万人の情報セキュリティ人材が 不足しており、情報セキュリティ技術者の中でも約 16 万人が、スキルが不足と言われている。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。

図 30　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 2016 報告プレスリリースより）

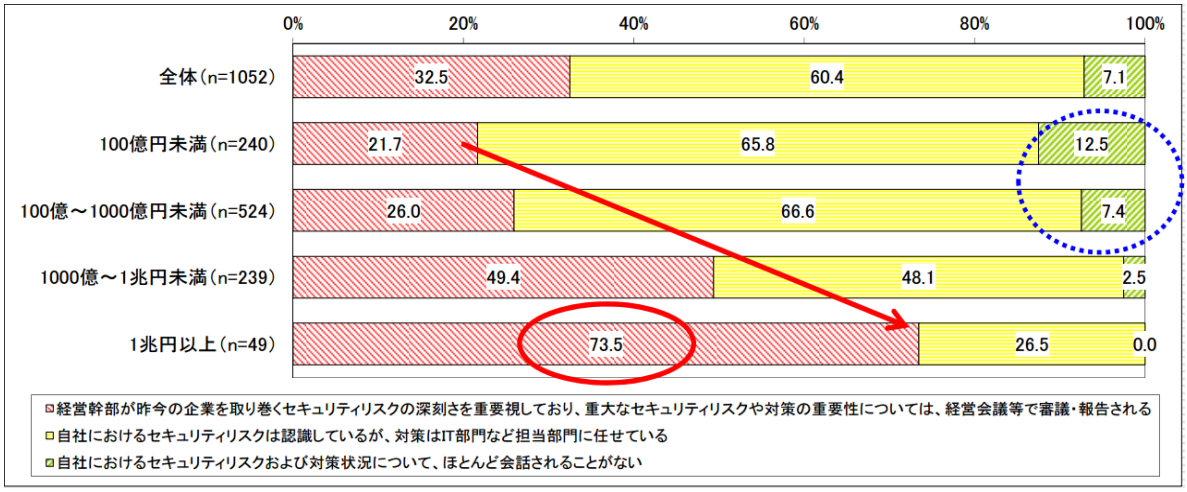
もう 1 点のトピックは不足している情報セキュリティ人材をいかに確保するかの分析である。図 31 のように、経営幹部が積極的にセキュリティ対策に関わっている割合は、企業規模（売上高）が大きくなるほど高くなるが、中小・中堅企業における経営幹部の情報セキュリティに対する意識は、不足しているとみられ、意識向上は急務と言える。

このことから、人材を確保してゆくには経営幹部が積極的に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と考える。

2015 年 6 月に発表され た日本年金機構の事案が世間を大きく賑わせ、情報セキュリティガバ

ナンスのあり方が 問題視された。しかし、調査時点では、いまだ経営幹部と情報セキュリティの関わり方に変化は見られず、引き続き経営層を交えた情報セキュリティ対策の課題が残ったままである。

図 31　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 2016 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 年度に深刻な事態として問題にされたのが、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し、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、BIND 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。

また、2015 年からは、マイクロソフトが Windows10 の無償配布と自動アップグレードを推進しだした。この結果、OS やその組み込みモジュール等における脆弱性対策が進むことが期待される。現時点で深刻な欠陥の指摘はないが、引き続き注意が必要である。

(3) 情報漏えい事件の深刻化

以下のような状況が継続的に発生しており、引き続き大きな課題となっている。

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、悪用される事例がかつてなく増えている。

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。

⑤ 直接漏えいしないまでも、ランサムウェアにより消去・改ざんされ、復元できなくなるか、金銭被害にあう事例が急増している。

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性と、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、この 10 年ほどの間に、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続いてきた。

2015 年 1 月 9 日には、「サイバーセキュリティ基本法」が全面施行された。それに伴い、内閣に「サイバーセキュリティ戦略本部」が設置された。実務などを担当する「内閣官房情報セキュリティセンター」（NISC）も併せて改組され、同日付で「内閣サイバーセキュリティセンター」として発足した。同本部では、情報セキュリティ政策会議が実施してきたセキュリティ戦略案の作成や、行政機関のセキュリティ基準の策定に加えて、行政機関で発生したセキュリティインシデントの調査なども実施する。各企業や自治体は、セキュリティ対策を戦略投資として位置づける必要があり、その供給に追いついていく必要がある。

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ている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

スマートフォン、タブレット PC、ソーシャルメディア等、個人の生活を根底から変革する様々な用途開発技術から、クラウドコンピューティング・ビッグデータ、AI・ディープラーニング等のこれまでのパラダイムを完全に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、IT フロンティアはイノベーションを進め、情報セキュリティ全般を拡張し、重要度を飛躍的に高めている。

また、2014 年に発生した大手企業内に蓄積された個人情報持ち出し事件、2015 年に発生した公共機関への標的型攻撃による大量の情報漏えい事件などが契機となり、繰り返し発生する「人の悪事」と企業リスクに関し、国・警察・防衛・企業・大学など幅広く産学官連携に取り組む機運が生まれ、情報セキュリティ産業の果たす役割は益々重要となってきた。

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、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
2016 年 7 月 8 日 V1.0	－	初版（JNSA 市場調査 WG 内校了）
2016 年 7 月 11 日 V1.01	表 1,9,19 の訂正 用語表記の修正／他	誤記修正・一般公開用改訂
2016 年 9 月 8 日 V1.02	円グラフの修正	P.15,19,22,25,30,32,35,38,42

情報セキュリティ市場調査報告書

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ー

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ー（2016 年 7 月 8 日現在）
及び、集計作業やデータ分析・執筆に携った方々　＜所属組織名五十音順＞

勝見　勉	アドバイザー
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
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
瀬戸口　広樹	サイエンスパーク株式会社
蜂巣　悌史	サブスクライバー
森田　翔	サブスクライバー
増田　聖一	三井物産セキュアディレクション株式会社

トピック執筆協力者（市場調査ワーキンググループ外からのご協力）

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