2016 年度
情報セキュリティ市場調査報告書

V1.1

2017 年 6 月 21 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。この間 2009 年度までは経済産業省委託事業として、以降は JNSA 独自の事業として継続している。委託事業期間を含む過去の調査数値との整合性を重視し、個社別推計調査・ワーキンググループメンバによる議論を踏まえ調査分析作業を行い、毎年 1 月に速報値を発表し、6 月に年次報告書をとりまとめている。

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、国の機関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、更にスマートフォンの急速な普及により一般家庭の話題にまで浸透した。さらに 2015・16 年には公的機関、大手企業／団体が DDoS 攻撃、標的型攻撃、サイバー攻撃を受け、情報セキュリティ対策の重要性が倍旧周知されている。

政府では、2015 年 1 月に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・内閣サイバーセキュリティセンター(NISC)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。金融庁の監査マニュアルが改定され、CSIRT 組織の設置を明記することとなり、重要インフラを保有する企業から順次サイバーセキュリティの確保が義務となった。

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、さらに Mirai マルウェア感染によりボット化された IoT デバイスによる DDoS 攻撃の急増等､今後進展するであろう IoT のセキュリティ動向にも注目する必要がある。IoT セキュリティ関連のコンソーシアムも立ち上がって来ている。

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、国家の意思やイデオロギー対立が背景にあるとみられるスパイ活動や破壊工作、戦略的地政学を背景とした攻撃の顕在化、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、IoT デバイスに対するマルウェア感染も増加しており、ネットワークセキュリティは国際的にも社会問題となっている。

このような現状からの脱却を図るためには、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、企業データや営業秘密、知的財産等の情報資産を自らが把握し守るべき対象に対する安全確保が不可欠である。そのためには企業が、情報資産の保護、内部統制の充実を計り、防御能力を高める必要がある。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の対策を施し、悪意を持った情報・デマや詐欺に対する耐性を向上させる教育も肝要である。そして万一、セキュリティ事故が発生した場合を想定した CSIRT の整備を進め早期解決の意識を定常化しておく必要がある。

情報セキュリティ産業は、これらの脅威に対する対策を支える製品やサービスを提供し、国民

の経済活動全般の安全安心の確保の一翼を担っている。公的機関を通じた体系的な情報セキュリティガイドラインによる導入指南に重点を置いた普及啓発の注力、情報セキュリティ従事者の育成・認定制度やCISO（企業内情報セキュリティ取締役）の設置などの人への投資も増えた。

この様な状況下、更に新たなセキュリティリスクとして、フェイクニュース(デマ)や企業炎上（従業員不祥事の拡散）など、情報モラル・リテラシーが企業の事業継続に打撃を与える事態も頻発しており、コンテンツ管理、運用監視、保険などの需要が高まっている。

本書は、日本の情報セキュリティ産業の規模と現状を調査・分析・推測する調査報告書である。
政府の施策や企業の対策の参考となって、経済社会の健全な発展と国際競争力の維持・向上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。
また昨今「サイバーセキュリティ」が広く用いられているが、これらと同義とする。

※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から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 2015 年度の市場規模総額は 8,965 億円に達したと推定する。

この 10 年で見ると 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が、東日本大震災を被ってもなお 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されている。

2015 年度を振り返ると、2014 年度に引き続き大規模な情報漏えい事件の発生や、広く利用されているソフトウェアの脆弱性によりインターネット基盤の根幹に関わるような事案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、ランサムウェア、標的型攻撃による被害も拡大傾向にあり、既知のセキュリティ対策では対策が不十分であると再認識させられた。このような背景の元、政府も、金融庁「監査マニュアル」、経済産業省「サイバーセキュリティ経営ガイドライン」が発行される等、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、日本全体の情報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。

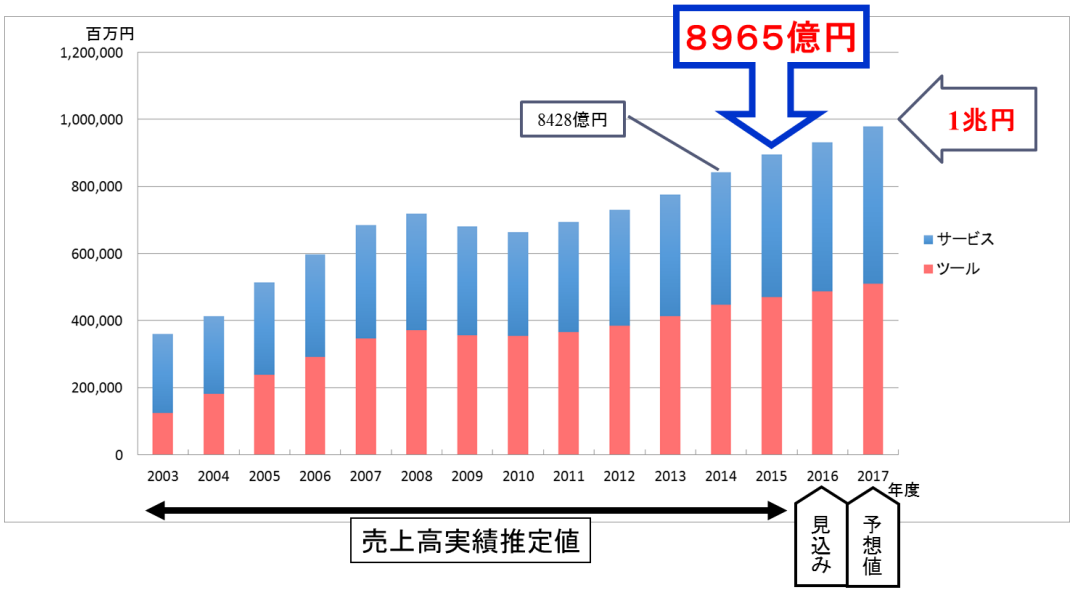


図 1　国内情報セキュリティ市場規模　経年推移

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。

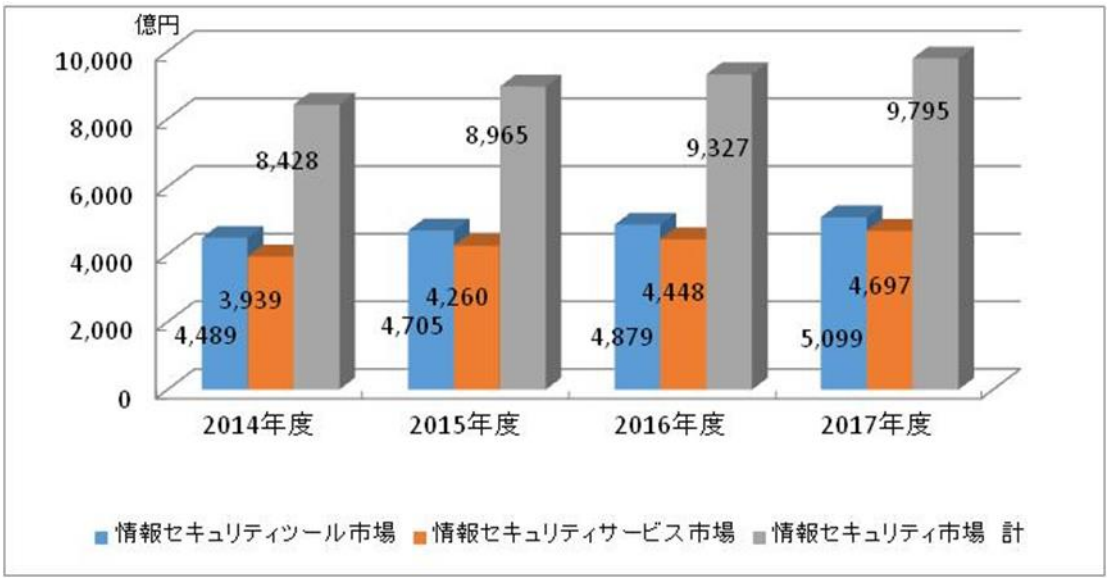


図 2　国内情報セキュリティ市場規模　経年推移（2014 年度～2017 年度）

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。2015 年度の情報セキュリティ市場は、ツール市場が 4,705 億円、サービス市場が 4,260 億円、合計 8,965 億円に達したものと推定する。 また、2016 年度はアイデンティティ・アクセス管理製品、暗号化製品や情報セキュリティ保険が顕著に伸びる中、全体で 4.0%成長し 9,327 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：億円、成長率：対前年比増加率）

年度別売上高推計値	2014年度		2015年度			2016年度			2017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	236	5.3%	233	4.9%	-1.4%	237	4.9%	2.0%	249	4.9%	5.0%
ネットワーク脅威対策製品	618	13.8%	644	13.7%	4.2%	670	13.7%	4.0%	703	13.8%	5.0%
コンテンツセキュリティ対策製品	1,712	38.1%	1,767	37.6%	3.2%	1,802	36.9%	2.0%	1,862	36.5%	3.3%
アイデンティティ・アクセス管理製品	772	17.2%	843	17.9%	9.2%	885	18.1%	5.0%	930	18.2%	5.0%
システムセキュリティ管理製品	663	14.8%	702	14.9%	5.9%	737	15.1%	5.0%	774	15.2%	5.0%
暗号化製品	488	10.9%	517	11.0%	5.8%	548	11.2%	6.0%	581	11.4%	6.0%
セキュリティツール市場合計	4,489	53.3%	4,705	52.5%	4.8%	4,879	52.3%	3.7%	5,099	52.1%	4.5%

年度別売上高推計値	2014年度		2015年度			2016年度			2017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	715	18.1%	806	18.9%	12.8%	830	18.7%	3.0%	872	18.6%	5.0%
セキュアシステム構築サービス	1,564	39.7%	1,323	31.1%	-15.4%	1,389	31.2%	5.0%	1,458	31.1%	5.0%
セキュリティ運用・管理サービス	1,252	31.8%	1,742	40.9%	39.1%	1,812	40.7%	4.0%	1,903	40.5%	5.0%
情報セキュリティ教育	304	7.7%	271	6.4%	-10.9%	281	6.3%	3.9%	308	6.6%	9.6%
情報セキュリティ保険	105	2.7%	118	2.8%	12.4%	135	3.0%	15.0%	156	3.3%	15.0%
セキュリティサービス市場合計	3,939	46.7%	4,260	47.5%	8.1%	4,448	47.7%	4.4%	4,697	47.9%	5.6%

セキュリティツール＋サービス	8,428	100%	8,965	100%	6.4%	9,327	100%	4.0%	9,795	100%	5.0%

このように、情報セキュリティ市場は、引き続き、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。2017 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、それはすなわち、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であり、そしてまた、情報セキュリティ産業の社会的責任が益々重要となることを意味する。

尚、2017 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 2016 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（本報告書の市場分類に当てはまる様な製品サービスによる）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 年度と比較し伸び率をやや抑えて予測した。

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、2015 年度の国内「情報セキュリティツール」市場は、4,705 億円（伸び率：前年比 4.8%）の規模であったと推算した。

本調査では「情報セキュリティツール」市場を、「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」と機能別に 6 つの製品カテゴリに分類している。

各カテゴリの定義は第 5 章を参照されたい。

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:億円

年度別売上高推計値	2014年度		2015年度			2016年度			2017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	236	5.3%	233	4.9%	-1.4%	237	4.9%	2.0%	249	4.9%	5.0%
ネットワーク脅威対策製品	618	13.8%	644	13.7%	4.2%	670	13.7%	4.0%	703	13.8%	5.0%
コンテンツセキュリティ対策製品	1,712	38.1%	1,767	37.6%	3.2%	1,802	36.9%	2.0%	1,862	36.5%	3.3%
アイデンティティ・アクセス管理製品	772	17.2%	843	17.9%	9.2%	885	18.1%	5.0%	930	18.2%	5.0%
システムセキュリティ管理製品	663	14.8%	702	14.9%	5.9%	737	15.1%	5.0%	774	15.2%	5.0%
暗号化製品	488	10.9%	517	11.0%	5.8%	548	11.2%	6.0%	581	11.4%	6.0%
セキュリティツール市場合計	4,489	53.3%	4,705	52.5%	4.8%	4,879	52.3%	3.7%	5,099	52.1%	4.5%

図 3 に 2015 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 2015 年度の市場規模は 1,767 億円で、ツール市場全体に占める割合は 37.6%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 843 億円、構成比で 17.9%であった。第 3 位は「システムセキュリティ管理製品」が 702 億円で 14.9%を占めた。続いて、「ネットワーク脅威対策製品」644 億円・13.7%、「統合型アプライアンス」233 億円・4.9%で、この 2 つを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製品として合計すると 877 億円・18.6%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 517 億円・11.0%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、2015 年度の伸び率は微増となった。

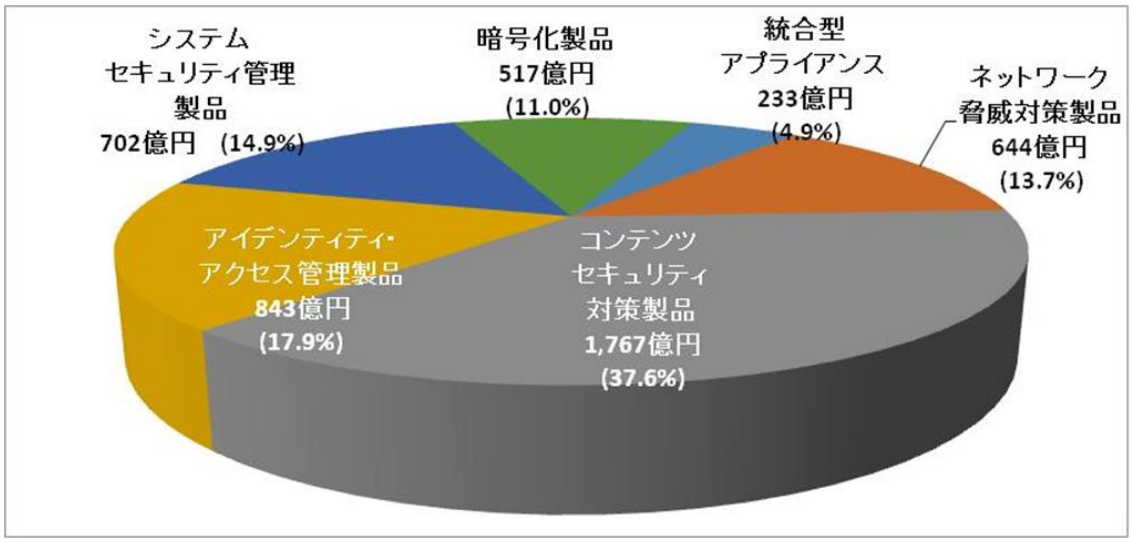


図 3　2015 年度の国内情報セキュリティツール市場

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、マルウェア感染後の特権 ID 取得による情報窃取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、高度で組み込み易い暗号化モジュールの需要が年々高まっている。

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、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、市場全体がモバイル化・クラウド化等のサービス寄りにシフトする中、4.9%の成長を遂げたものと見られる。

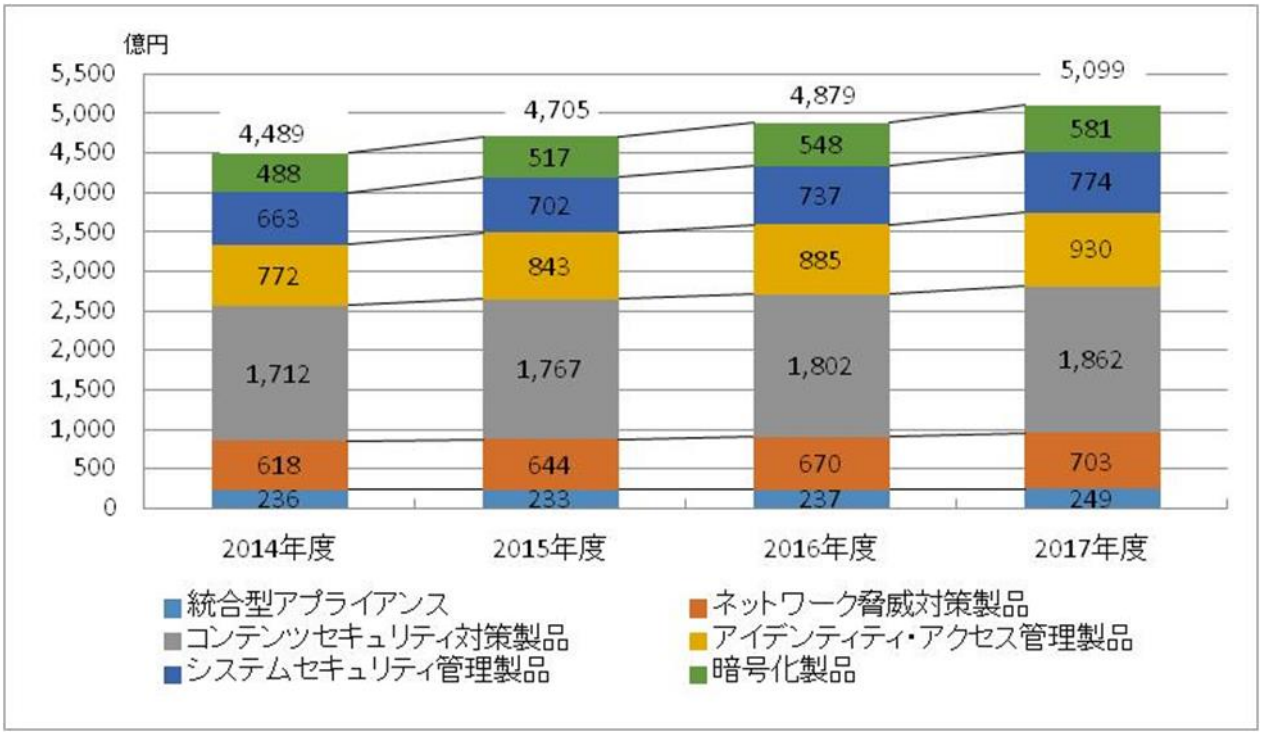


図 4　国内情報セキュリティツール市場推移

2015 年度に最も高い伸び率を示したカテゴリ（大分類市場）は「アイデンティティ・アクセス管理製品」で、9.2%の伸び率である。ここ数年多発している情報漏えい事件を受けて、ID 管理、アクセス権管理に対する意識が高まったと考えられる。次に高い伸びを示したのが、「システムセキュリティ管理製品」の 5.9%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。

3 番目に高い伸びを示したカテゴリは、「暗号化製品」であり、5.8%の伸び率であった。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。

4 番目に高い伸びを示したカテゴリは「ネットワーク脅威対策製品」の 4.2%で、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。

「コンテンツセキュリティ対策製品」はツール市場全体の 37.6%を占めるため、このカテゴリの伸び率 3.2%がツール市場全体の伸び率（4.8%）に大きく影響する。

「統合型アプライアンス」は-1.4%とマイナス成長となり、前年の 10.1%に対して大きく落ちた。これは、この市場が成熟し、中小ユーザでほぼ導入が進んだ結果と考えられる。2016 年度は、買い替えで 2.0%の微増と予想した。

2016 年のツール市場は、サイバーセキュリティ脅威の増加に伴う社会的認知・浸透はあるもの

の、ツールからサービスへの移行の流れが顕著で、4,879 億円(2015 年比 3.7%増)と見込んだ。

2017 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、更に製品が多様化する中、サービスへの移行も進むと予測されるため、各ベンダの業態を参考に最も大きな市場であるコンテンツセキュリティ対策製品を 3.3%増、需要の伸びの高い暗号化製品を 6.0%増、その他カテゴリの伸び率を 5.0%増と見積り、ツール全体で初の 5000 億円超えとなる 5,099 億円を予測した。

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。また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・中小企業や、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。

一方ハイエンド機は、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。さらに近年、オンプレミスからクラウドに転換を図る企業が増え、2015 年度には初めてマイナス成長となった。

この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全てのハードウェア型製品の需要に影響を与えている。

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一方、台数的には減る傾向がある。また 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、仮想化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、商品形態としてはサービス要素が増えるということになる。

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、当市場調査各カテゴリのアプライアンス製品分類の見直しも注視する。

当市場調査が予想した通り、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、2016 年度は緩やかに伸びが回復し、新たな形態の統合型アプライアンスツール市場が形成されると期待できる。

(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

統合型アプライアンス	2014 年度	2015 年度	2016 年度	2017 年度
市場規模（億円）	236	233	237	249
対前年度比成長率	―	-1.4%	2.0%	5.0%

前述の通り、導入が進んだ結果 2015 年度は一旦マイナス成長(-1.4%)となったが、限定的用途、中小零細規模においては 3 年～6 年での買い替えサイクル需要が発生するため、2016 年度は 237 億円、2017 年度は 249 億円になると推測する。

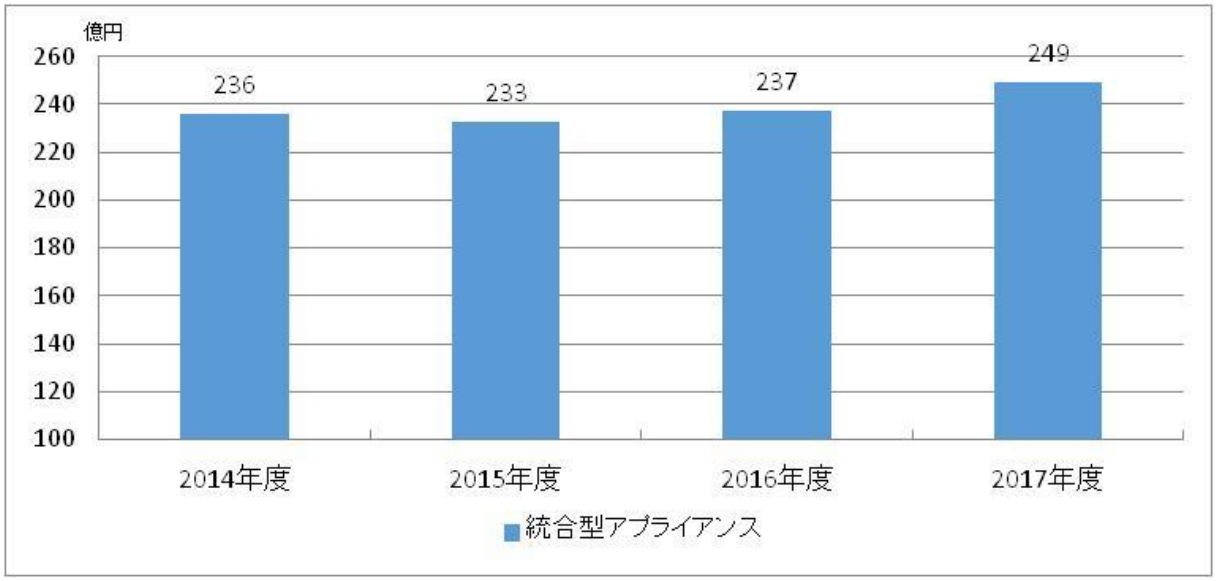


図 5　国内統合型アプライアンス市場推移

国内統合型アプライアンス製品ツール市場は、ほぼ導入が進んだ結果、マイナス成長となったが、ネットワークのマイクロセグメント化へのニーズ等で、今後ネットワークセグメント単位での導入が進む可能性があり、今後大きく変動する可能性がある。

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 2015 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が、現在はハードとソフトを一体化したアプライアンス型製品が主流となっている。

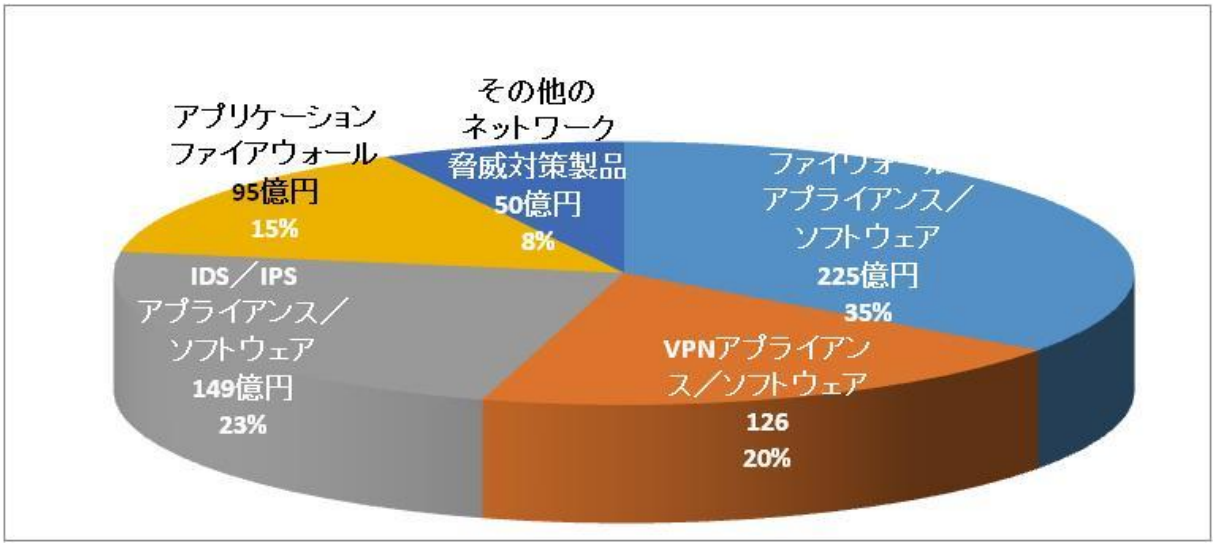


図 6　ネットワーク脅威対策製品市場

「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、情報が窃取される情報漏えい事件やマルウェア等が仕掛けられる改ざんを防止する為、近年急速に導入が進んでいる。また提供する形態もオンプレミスで導入するのに加え、同様の機能をクラウドで提供するサービスも増加している。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登場してきている。

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、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（億円）	2014 年度	2015 年度	2016 年度	2017 年度
ファイウォール・アプライアンス／ソフトウェア	227	225	234	246
VPN アプライアンス／ソフトウェア	124	126	131	137
IDS／IPS アプライアンス／ソフトウェア	144	149	155	163
アプリケーションファイアウォール	78	95	98	103
その他のネットワーク脅威対策製品	46	50	52	54
合計	618	644	670	703
構成比				
ファイウォール・アプライアンス／ソフトウェア	36.7%	35.0%	35.0%	35.0%
VPN アプライアンス／ソフトウェア	20.0%	19.5%	19.5%	19.5%
IDS／IPS アプライアンス／ソフトウェア	23.2%	23.1%	23.1%	23.1%
アプリケーションファイアウォール	12.7%	14.7%	14.7%	14.7%
その他のネットワーク脅威対策製品	7.4%	7.7%	7.7%	7.7%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
ファイウォール・アプライアンス／ソフトウェア	－	-0.7%	4.0%	5.0%
VPN アプライアンス／ソフトウェア	－	1.6%	4.0%	5.0%
IDS／IPS アプライアンス／ソフトウェア	－	3.7%	4.0%	5.0%
アプリケーションファイアウォール	－	21.1%	4.0%	5.0%
その他のネットワーク脅威対策製品	－	8.3%	4.0%	5.0%
合計	－	4.2%	4.0%	5.0%

ネットワーク脅威対策製品の 2015 年度における売上実績推定値は 644 億円(前年比 4.2%)となった。アプリケーションファイアウォールや IDS／IPS、VPN が市場を牽引している。ネットワーク脅威が加速増大する中、各ベンダのネットワークセキュリティ対策製品が拡充したことが要因と考えられる。

2016 年度は、企業の設備投資が引き続き好調に進むと予測し 4.0%成長の 670 億円と推定した。

2017 年は前年比 5.0%増 703 億円に達すると予測した。

ツール市場全体の中で「ネットワーク脅威対策製品」が占める構成比は 2015 年度 13.7%となり

規模は 4 番目であるが、「統合型アプライアンス」の項の最後で述べた通り、今後「統合型アプライアンス」市場分類を見直すこととなった場合、この「ネットワーク脅威対策製品」と「統合型アプライアンス」を合わせた＜脅威対策ツール＞とすると、ツール市場の 18.6%を占め、「コンテンツセキュリティ対策製品」に次いで 2 番目の規模となる。（表 2 参照）

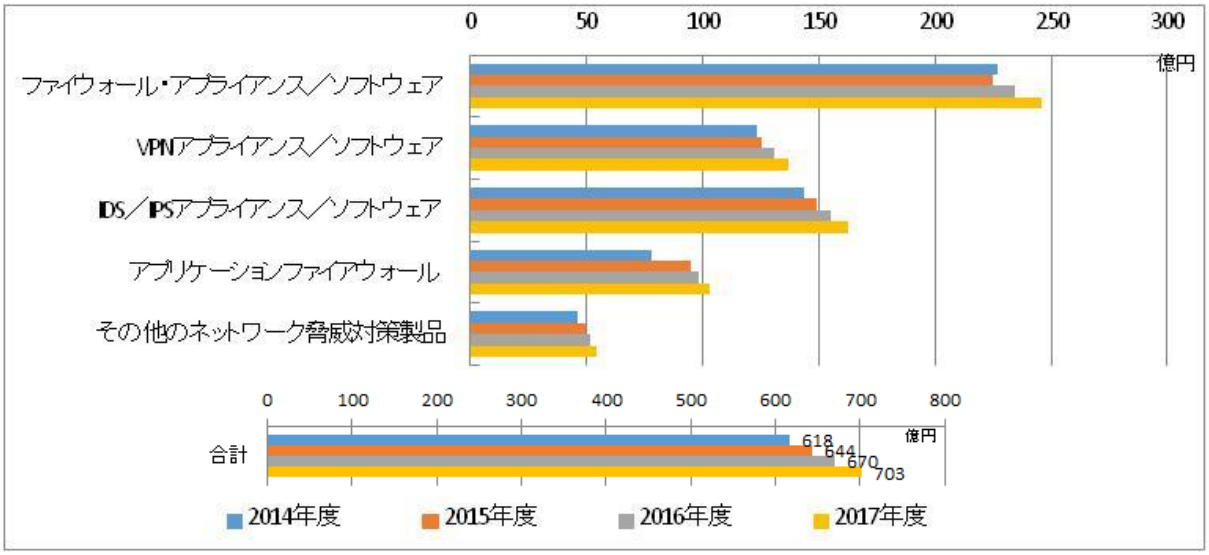


図 7　国内ネットワーク脅威対策製品市場推移

「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、2014 年度 227 億円、2015 年度 225 億円、2016 年度 234 億円、2017 年度 246 億円と 2015 年には若干の減少が見られるが、概ね増加傾向にある。昨年度調査に比べ伸び率が下方修正となった要因は、オンプレミスからクラウド化、自社管理から仮想化・クラウド運用サービスの利用に購買層がシフトした事が考えられる。

「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」のカテゴリの中では経済動向に左右されにく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、2014 年度 124 億円、2015 年度 126 億円、2016 年度 131 億円、2017 年度 137 億円と堅調な推移をすると推定される。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、今後も堅調に増加すると考える。

「IDS／IPS アプライアンス／ソフトウェア製品」市場は、2014 年度 144 億円、2015 年度 149 億円、2016 年度 155 億円、2017 年度 163 億円という予測となった。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堅調に推移すると予測される。

「アプリケーションファイアウォール」は、2007 年度に市場が立ち上がり、Web サーバへのサ

イバー攻撃の急増に伴い成熟したセグメントである。当初は使い勝手の悪さから需要側にも戸惑い感があり、リーマンショック以降もさほど大きな伸びはなかったが、製品の改良やニーズの高まりを背景に、本年度調査では拡大に転ずる結果となった。市場規模は、2014 年度 78 億円、2015 年度 95 億円、2016 年度 98 億円、2017 年度 103 億円となった。この背景には、前述した通り、Web サーバに対するサイバー攻撃の増加や、PCIDSS が v3 に上がることに伴う需要喚起等があったものと見られる。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」、「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、PCIDSS 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の普及により、導入範囲が広がってきている。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 2015 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 71%を占める。昨年度調査ではここの占有率が約 75%であったことから、他のコンテンツセキュリティ対策製品の伸びが顕著だったこと、個人向けパソコン出荷台数が減少したため市場が変化したことが要因と考えられる。一方、企業向けは大きな伸びは無く、前年度横ばいのゼロ成長・飽和市場となっている。

従来の PC から、スマートフォン、タブレットへの転換が進む中、標的型攻撃、遠隔操作ウイルス、ランサムウェア、内部情報漏えい、悪意のある情報改ざん等、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が、ウイルス対策だけでなく、不正通信のフィルタリング、振る舞い検知等、多層防御の形にシフトしてきている。

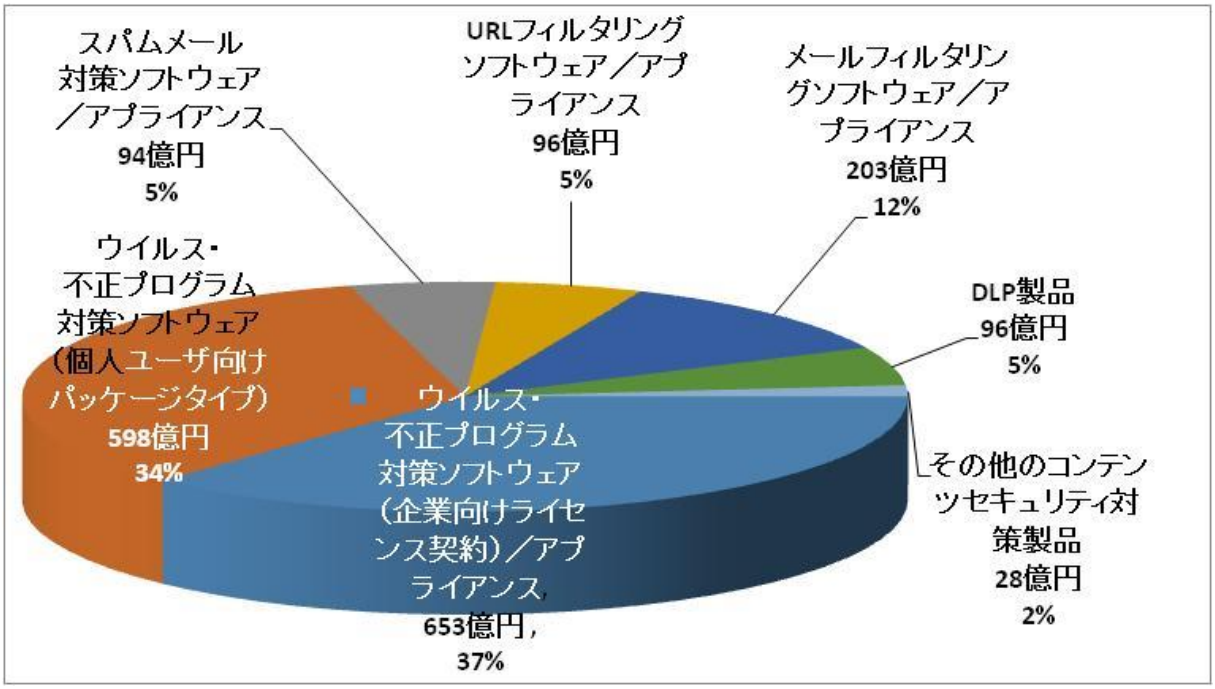


図 8　コンテンツセキュリティ対策製品市場

営業職などの外出の多い部門の社員の業務をスマートデバイスで効率化し、MDM（Mobile Device Management）などのシステムを導入する大企業が増えている一方、中小企業では BYOD（Bring Your Own Device 個人所有デバイスの業務利用）が定着して来ていると考えられ、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」市場規模は、「ウイルス・不正プログラム対策ソフトウェア」の次に「メールフィルタリング」が大きいが、本年度特筆すべきは、「URL フィルタリング」、「DLP 製品」（情報漏えい対策製品・システム）が、「スパムメール対策」を規模で抜いたという点である。これは標的型攻撃の増加に伴い、C&C サーバへの通信遮断、不正サイト、業務必要外サイトへのアクセスを遮断する目的で導入が進んだ為と考えられる。

なお、未だ数値的には小さいが将来拡大が見込まれる「その他」コンテンツセキュリティ対策製品として、APP コントローラ（アプリケーション制御）や、詐欺防止の AI 技術などが、今後台頭してくると考えられる。

(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、2014 年度には 650 億円に達した。2015 年度は前述の通り、企業のスマートデバイス積極採用等により伸びは鈍化し横ばいの 653 億円となった。2016 年度は新たなマルウェア脅威の増加により 3.0%増の 672 億円、2017 年度は 5.0%増の 706 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（億円）	2014 年度	2015 年度	2016 年度	2017 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	650	653	672	706
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）	628	598	598	598
スパムメール対策ソフトウェア／アプライアンス	84	94	97	102
URL フィルタリングソフトウェア／アプライアンス	77	96	98	103
メールフィルタリングソフトウェア／アプライアンス	181	203	209	220
DLP 製品	67	96	99	104
その他のコンテンツセキュリティ対策製品	26	28	29	30
合計	1,712	1,767	1,802	1,862
構成比				
ウイルス・不正プログラム対策ソフトウェア（企業向けライセンス契約）／アプライアンス	38.0%	36.9%	37.3%	37.9%
ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ）	36.7%	33.9%	33.2%	32.1%
スパムメール対策ソフトウェア／アプライアンス	4.9%	5.3%	5.4%	5.5%
URL フィルタリングソフトウェア／アプライアンス	4.5%	5.4%	5.5%	5.6%
メールフィルタリングソフトウェア／アプライアンス	10.6%	11.5%	11.6%	11.8%
DLP 製品	3.9%	5.4%	5.5%	5.6%
その他のコンテンツセキュリティ対策製品	1.5%	1.6%	1.6%	1.6%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
ウイルス・不正プログラム対策ソフトウェア（企業向けライセンス契約）／アプライアンス	－	0.4%	3.0%	5.0%
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）	－	-4.7%	0.0%	0.0%
スパムメール対策ソフトウェア／アプライアンス	－	12.2%	3.0%	5.0%
URL フィルタリングソフトウェア／アプライアンス	－	23.5%	3.0%	5.0%
メールフィルタリングソフトウェア／アプライアンス	－	12.2%	3.0%	5.0%
DLP 製品	－	43.9%	3.0%	5.0%

その他のコンテンツセキュリティ対策製品	―	7.1%	3.0%	5.0%
合計	―	3.2%	2.0%	3.3%

「ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ）」も企業向けと同程度の規模を持つセグメントであるが、従来の方式ではスマートデバイス対策が困難になってきたこと、単価が安く設定されていること、ネット決済サービス一体型の商品が多く出ていること、詐欺対策等のコンテキスト防御に主体が移動し始めていることなどから、2015 年度の市場規模は前年対比-30 億（-4.7%）の 598 億円となったと推計した。2016 年度 2017 年度はゼロ成長と予測している。

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 2014 年度で 181 億円であるが、2017 年度には 220 億円にまで拡大すると予測される。

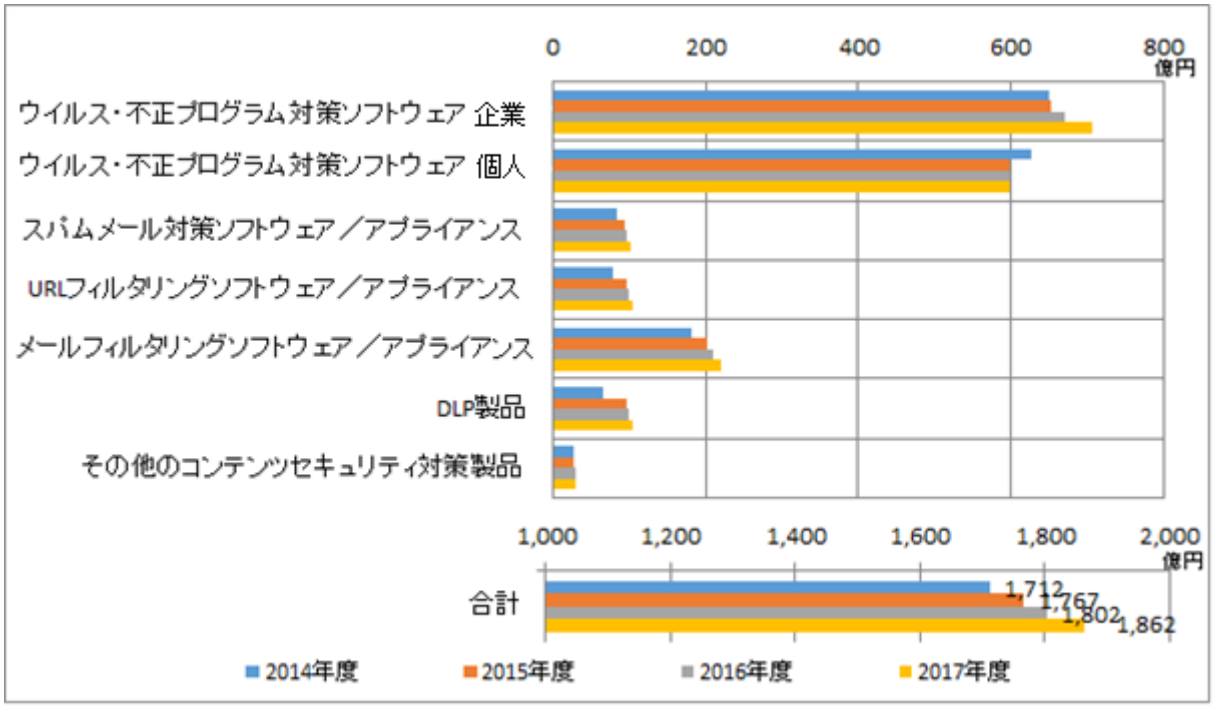


図 9　国内コンテンツセキュリティ対策製品市場推移

「URL フィルタリングソフトウェア／アプライアンス」と「DLP 製品」がほぼ同規模の 96 億円市場となった。

「URL フィルタリングソフトウェア／アプライアンス」は 2014 年度 77 億円、2015 年度 96 億円（23.5%増）、2016 年度 98 億円（3.0%増）、2017 年度 103 億円（5.0%増）と予想。

「DLP 製品」は、13 年間にわたる本報告書調査の中で最も新しく 2010 年度調査から分類に加わ

ったセグメントであるが、2014 年度 67 億円、2015 年度 96 億円(43.9%増)、2016 年度 99 億円(3.0%増)、2017 年度 104 億円（5.0%増）と 3 年でほぼ倍増する勢いで、「コンテンツセキュリティ対策製品」の中で第 3 位の市場規模になる可能性も考えられる。

「スパムメール対策ソフトウェア／アプライアンス」は、2014 年度 84 億円、2015 年度 94 億円（12.2%増)、2016 年度 97 億円（3.0%増)、2017 年度 102 億円（5.0%増）と予測した。

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 2015 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（情報資源･情報処理成果）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。

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、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る、シングル・サインオン（SSO）も今後更に伸びが予想される。

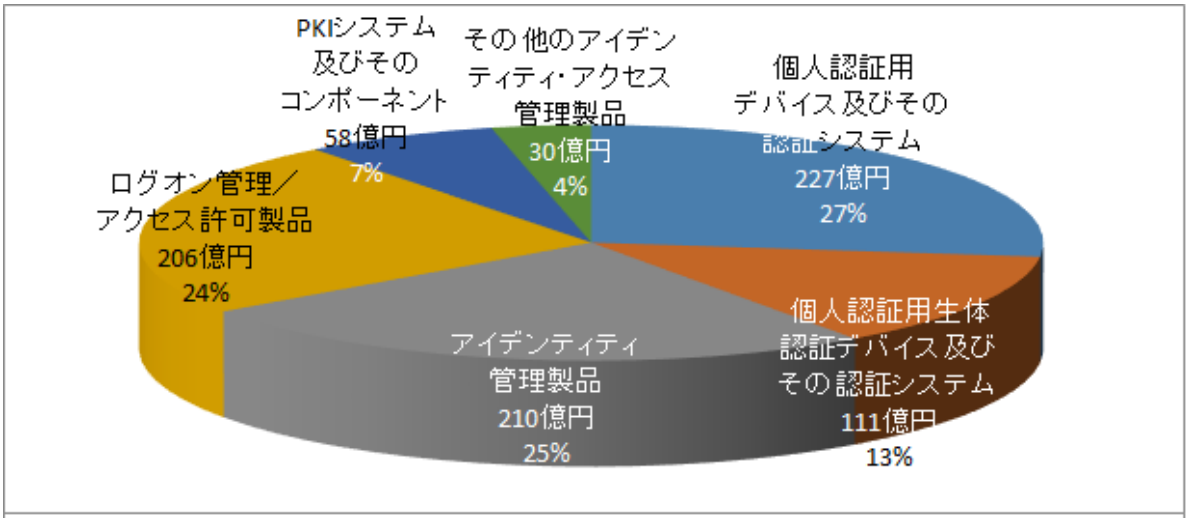


図 10　アイデンティティ・アクセス管理製品市場

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。昨今の情報漏えい事件の増加を受け、企業・団体ではアイデンティティ管理を拡充させる動きが加速している。情報漏えいの多くの原因は、内部犯行であると統計が出ている事もあり、従業員の認証技術の導入は、今後も伸びると予想出来る。

(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（億円）	2014 年度	2015 年度	2016 年度	2017 年度
個人認証用デバイス及びその認証システム	235	227	238	250
個人認証用生体認証デバイス及びその認証システム	113	111	117	123
アイデンティティ管理製品	110	210	221	232
ログオン管理／アクセス許可製品	202	206	216	227
PKI システム及びそのコンポーネント	76	58	61	64
その他のアイデンティティ・アクセス管理製品	36	30	32	33
合計	772	843	885	930
構成比				
個人認証用デバイス及びその認証システム	30.4%	26.9%	26.9%	26.9%
個人認証用生体認証デバイス及びその認証システム	14.6%	13.2%	13.2%	13.2%
アイデンティティ管理製品	14.2%	25.0%	25.0%	25.0%
ログオン管理／アクセス許可製品	26.2%	24.4%	24.4%	24.4%
PKI システム及びそのコンポーネント	9.9%	6.9%	6.9%	6.9%
その他のアイデンティティ・アクセス管理製品	4.7%	3.6%	3.6%	3.6%

合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
個人認証用デバイス及びその認証システム	—	-3.3%	5.0%	5.0%
個人認証用生体認証デバイス及びその認証システム	—	-1.6%	5.0%	5.0%
アイデンティティ管理製品	—	92.1%	5.0%	5.0%
ログオン管理／アクセス許可製品	—	1.8%	5.0%	5.0%
PKI システム及びそのコンポーネント	—	-23.5%	5.0%	5.0%
その他のアイデンティティ・アクセス管理製品	—	-17.0%	5.0%	5.0%
合計	—	9.2%	5.0%	5.0%

アイデンティティ・アクセス管理製品の市場規模は、2015 年度の実績で 843 億円（前年比伸び率 9.2%）となったが、「情報セキュリティツール」市場全体の 4,705 億円に対する構成比は 17.9 %であり、コンテンツセキュリティ対策製品市場に次ぐ規模の市場である。2016 年度は+5.0%の 885 億円、2017 年度には+5.0%の 930 億円と、900 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 2015 年度の構成比で 26.9%と最も大きな部分を占めた。市場規模は 2015 年度で 227 億円であり、2016 年度は 238 億円と前年比 5.0%増と予想される。

これに次いで規模の大きいセグメントが 2014 年度の「ログオン管理／アクセス許可製品」から 2015 年度は「アイデンティティ管理製品」となった。これは前述した通り、昨今の情報漏えい事件の増加を受け、企業・団体ではアイデンティティ管理を拡充させる動きが加速したと予想出来る。市場規模は 2015 年度に 210 億円で、2016 年度には 5.0%拡大して 221 億円となり、2017 年度には 232 億円の市場規模になると予測した。なお、「ログオン管理／アクセス許可製品」も 3 番目に大きなセグメントとなっており、2015 年度の構成比で 24.4%となっている。アクセスする際の承認・許可はもちろんのこと、職務や権限に基づくアクセス権において、注目度が高まっているといえる。

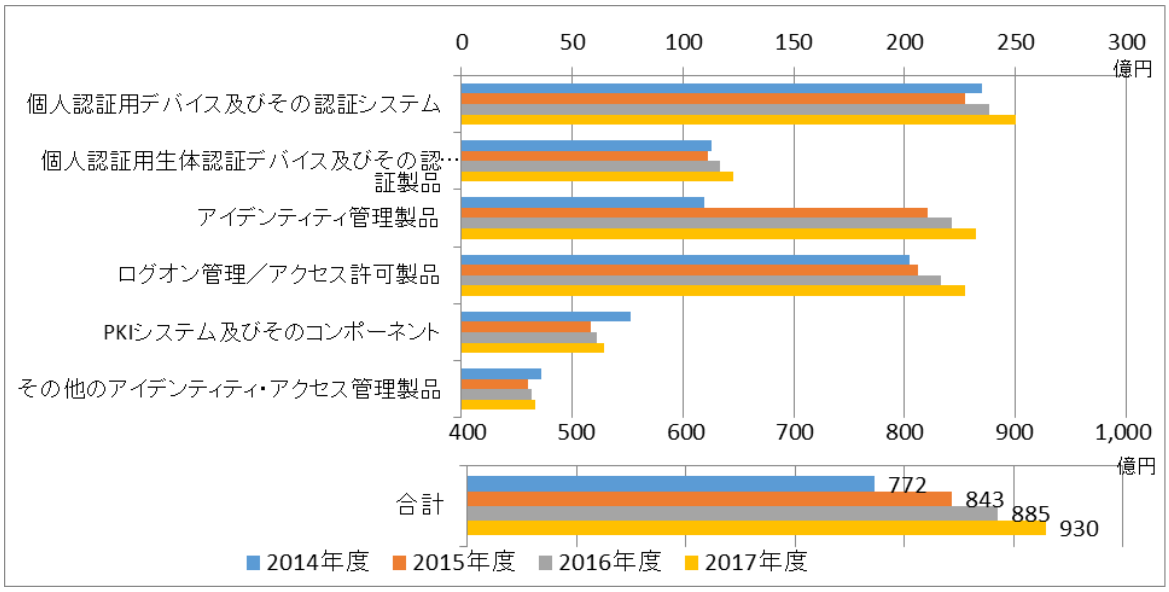


図 11　国内アイデンティティ・アクセス管理製品市場推移

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 2015 年度におけるセグメント分布を図 12 に示す。ここ近年の度重なる大型情報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ており、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。

様々なセキュリティ対策をとってもサイバー攻撃や情報漏えいを完全に防ぐことが難しい状況において、サーバやネットワーク機器、セキュリティ関連機器、各種アプリケーションなどからのイベントログ情報を集め、一元的に管理する「SIEM」(Security Information and Event Management/セキュリティ情報イベント管理) が伸びてくると思われる。

人間では取り扱うことが出来ない多種多量のログをリアルタイムに分析し、異常があればアラートを検出し、レポートする。人的運用負荷を軽減し、また技術者の不足を補うという観点からも有用である。個々のイベントを正常とみなしても、複数のイベントを相関分析することでリスクを見つけ出せるのも、この製品群の大きなポイントである。

「ポリシー管理・設定管理・動作監視制御製品」は情報漏えい対策につながることから、需要は依然高い分野である。企業から従業員へのスマートデバイスの支給が進み、以前はシステム面での管理が後手にまわっていたこの分野においても、紛失などに備えたリモートロック、リモートワイプ（初期化、無効化）ツールや、私用によりインストールされてしまう不正アプリによるリスクなどに備えるために MDM（Mobile Device Management）製品などの導入が大幅に進んできていると思われる。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。また、広まりつつある BYOD（私物端末で業務を行うこと）の普及度合によっては、MDM（モバイルデバイス管理）の適用が難しいため、MAM（モバイルアプリケーション管理）

やMCM（モバイルコンテンツ管理）が普及していくと考えられる。

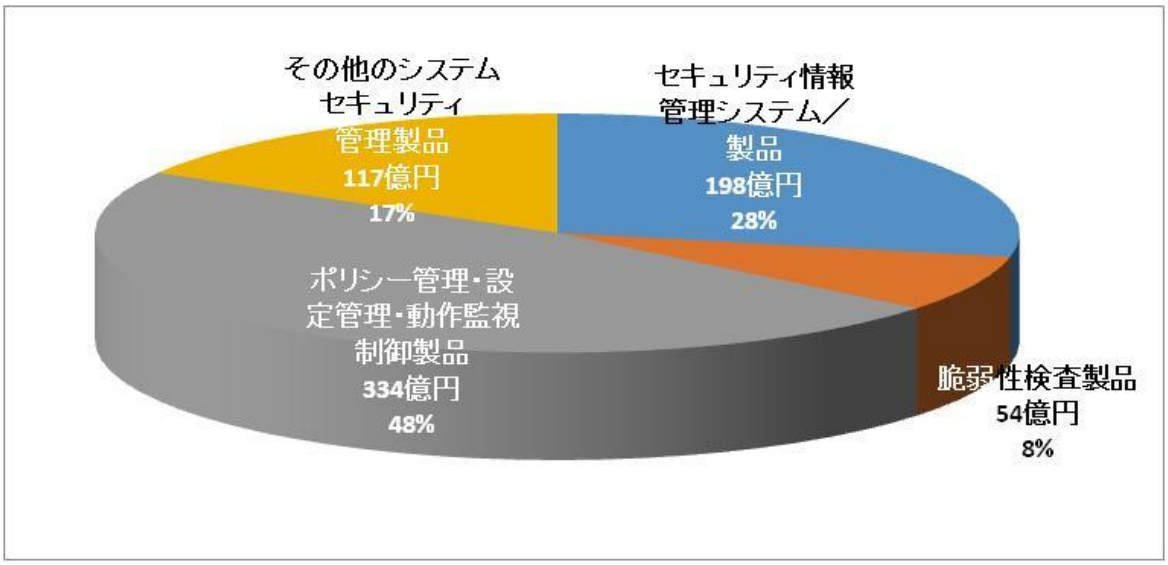


図 12　システムセキュリティ管理製品市場

(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。

「システムセキュリティ管理製品」市場は2015年度には全セグメント合せて702億円程度の市場を形成しており、2014年度と比べると+5.9%の伸びとなる。2016年度は5.0%増の737億円と少々伸び率は下がるものの、その傾向は2017年度（774億円、+5.0%）も続くと推測している。これらはセキュリティツール製品全体の成長率と比較しても上回っており、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（億円）	2014 年度	2015 年度	2016 年度	2017 年度
セキュリティ情報管理システム／製品	194	198	208	218
脆弱性検査製品	54	54	56	59
ポリシー管理・設定管理･動作監視制御製品	311	334	350	368
その他のシステムセキュリティ管理製品	104	117	122	129
合計	663	702	737	774
構成比				
セキュリティ情報管理システム／製品	29.3%	28.2%	28.2%	28.2%
脆弱性検査製品	8.1%	7.6%	7.6%	7.6%
ポリシー管理・設定管理･動作監視制御製品	46.9%	47.5%	47.5%	47.5%
その他のシステムセキュリティ管理製品	15.6%	16.6%	16.6%	16.6%
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	―	1.9%	5.0%	5.0%
脆弱性検査製品	―	-0.4%	5.0%	5.0%
ポリシー管理・設定管理･動作監視制御製品	―	7.2%	5.0%	5.0%
その他のシステムセキュリティ管理製品	―	12.5%	5.0%	5.0%
合計	―	5.9%	5.0%	5.0%

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2015年度に198億円、前年度比1.9%増と増加傾向にあり、さらに2016年度は5.0%増の208億円、2017年度も同様に+5.0%の218億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、2015 年度における成長率は+7.2%、市場規模は 334 億円、2016 年度も伸び率は下がるものの、350 億円規模への拡大が見込まれ、2017 年は 368 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 2015 年度で 54 億円と小さい。伸び率も他のセグメントと比較すると限定的であり､2017 年度にかけ+7.6%程度と予測され、2017 年度の市場規模は 59 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。2015年度の伸び率は+12.5%で、2016年度、2017年度ともに+5.0%の成長率を示し、2016年度に122億円、2017年度には129億円に達するものと予測される。

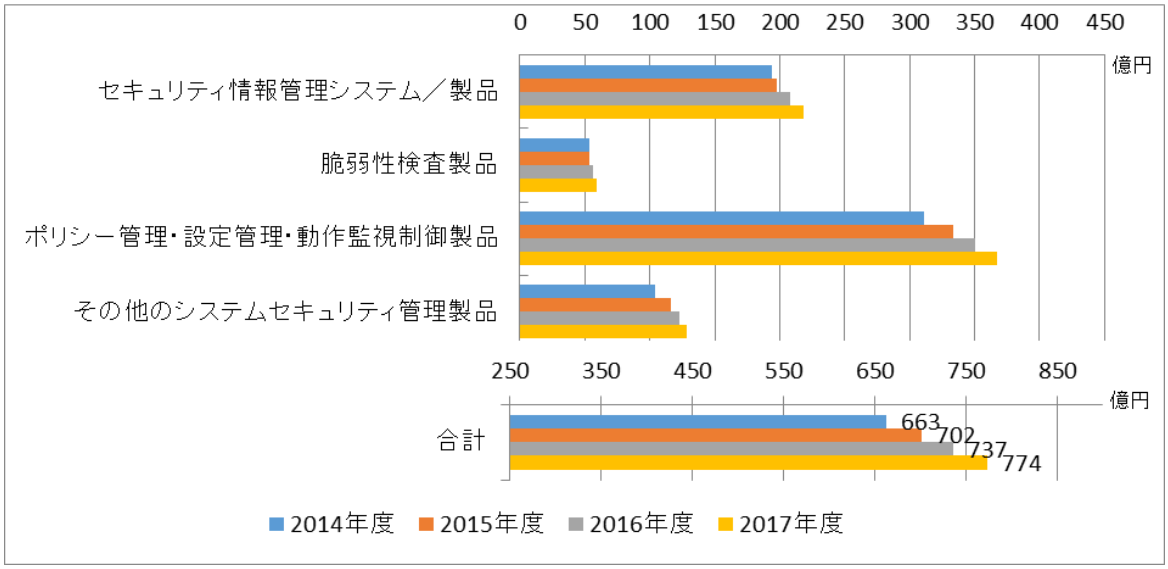


図 13　国内システムセキュリティ管理製品市場推移

2.1.2.6. 暗号化製品市場

(1) 市場の動向

暗号化製品も 2015 年度には前年比+5.8%と堅調な推移を見せている。

暗号化製品のここ数年の市場推移として、政府認証基盤（GPKI）の暗号アルゴリズム移行作業フェーズ 2 が開始され認証局による新暗号更改が実施されており、民間認証機関でもそれに准じた動きがみられ、継続的な成長が続いていると考えられる。認証基盤以外の部分では、暗号技術を利用した情報漏えい対策ツール、盗難対策ツール類は多くのベンダからリリースされ、一定規模の需要が見込める。また、PCIDSS 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が予想され、上記の理由を含め、今後コンテンツセキュリティ関連製品の DLP 製品の伸びと相俟って、暗号化製品の市場も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（億円）	2014 年度	2015 年度	2016 年度	2017 年度
暗号化製品	488	517	548	581
対前年度比成長率				
暗号化製品	―	5.8%	6.0%	6.0%

暗号化製品の市場規模はセキュリティツール全体の約 11%を占めている。2015 年度の市場規模は 517 億円で前年度比 5.8%増となった。2016 年度は前年度比 6.0%増の 548 億円、2017 年度もさらに 6.0%市場規模を拡大させ、581 億円の市場規模になると予測している。これは昨年度の予測値を超えるもので、取り扱うデータの総量が増えていく限りこの傾向は継続すると思われる。

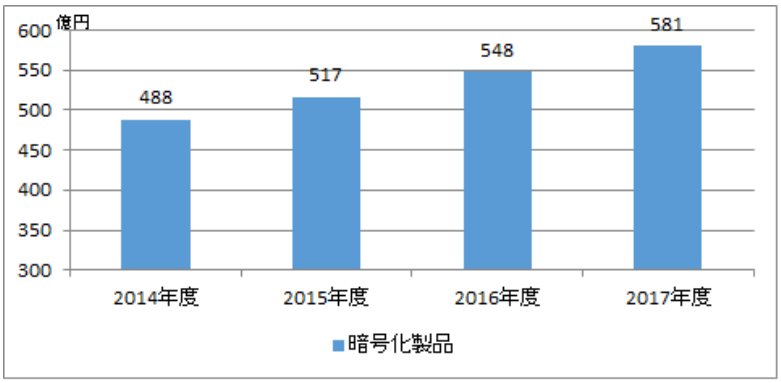


図 14　国内暗号化製品市場推移

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、それがツールとは切り離して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。反対に、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:億円**

年度別売上高推計値	2014年度		2015年度			2016年度			2017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	715	18.1%	806	18.9%	12.8%	830	18.7%	3.0%	872	18.6%	5.0%
セキュアシステム構築サービス	1,564	39.7%	1,323	31.1%	-15.4%	1,389	31.2%	5.0%	1,458	31.1%	5.0%
セキュリティ運用・管理サービス	1,252	31.8%	1,742	40.9%	39.1%	1,812	40.7%	4.0%	1,903	40.5%	5.0%
情報セキュリティ教育	304	7.7%	271	6.4%	-10.9%	281	6.3%	3.9%	308	6.6%	9.6%
情報セキュリティ保険	105	2.7%	118	2.8%	12.4%	135	3.0%	15.0%	156	3.3%	15.0%
セキュリティサービス市場合計	3,939	46.7%	4,260	47.5%	8.1%	4,448	47.7%	4.4%	4,697	47.9%	5.6%

今回の調査結果では、2015年度の「情報セキュリティサービス」市場規模は4,260億円と実に前年比+8.1%の急成長を果たし、2016年度には4.4%増の4,448億円市場になると推計した。

現在の成長軌道に乗る前のボトム期として捉えている2010年度（市場規模3,100億円）から、年を追う毎に事件・事故・被害の報道が増え続け、サイバーセキュリティ脅威はその深刻さ複雑さが増し、従来までのように単発的にツールを導入したところで効果的な対策にならないことが、多くの経営層・システム部門に理解され、コンサル・構築・運用管理・教育・保険といった関係従事者の意志が反映された「サービス」の必要性が益々重要となってきたことから、市場は順調に拡大している。すなわち、ユーザ層がツール偏重からサービス主体へ対策の転換を図る、それに相俟ってツール提供ベンダがサービス提供に事業体質を転換してきている。

「ツール」対「サービス」は2014年の53.3%：46.7%から2017年の52.1%：47.9%と、わが国のセキュリティ市場は半分がサービスである、というところまで近付いている。

2015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4,260億円と、4,000億円を超す市場に成長している。2016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、4,448 億円に達すると予測される。2017 年度は経済状況が不透明なため、成長率は鈍化して推計しているものの、脅威の高度化･深刻化に伴う専門サービスの利用が増加し 5.6%増の成長を予測している。

図 15 に 2015 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。

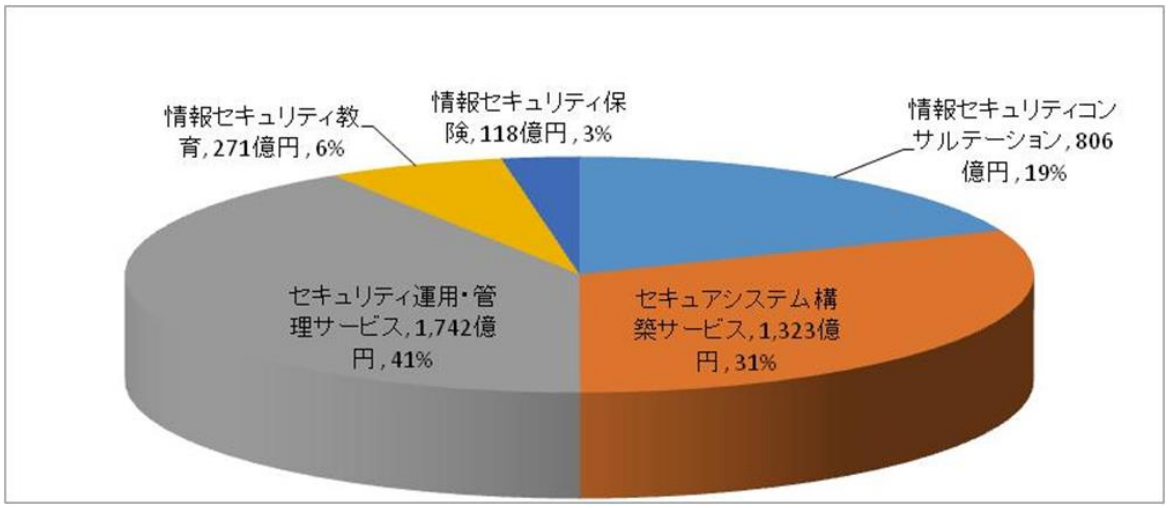


図 15　国内情報セキュリティサービス市場

「情報セキュリティサービス」市場でこれまで最大のカテゴリだった「セキュアシステム構築サービス」が前年から 240 億円マイナスの 1,323 億円と 15.4%も落ち込んだのに対し、「セキュリティ運用・管理サービス」は前年から 490 億円 39.1%増の 1,742 億円と大きく伸ばし、サービス市場の 40.9%を占めた。

「セキュリティ運用・管理サービス」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急速に拡大している。

一方、「セキュアシステム構築サービス」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、ここにきて「セキュリティ運用・管理サービス」に抜かれることとなった。これは相次ぐ脅威の報告を踏まえ、大規模ユーザが外部のサービス専門業者に役務を委託する場面が増えたため、予算の配分が構築から運用管理にドラスティックにシフトしたためと推測している。

金額規模で 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。元々、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、経営コンサルティングに近いところに位置していたが、最近ではランサムウェアに対する事業リスクのコンサルティングなどの需要が伸

びており、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 2014 年度以降、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、2015 年度は前年度比 12.8%増 806 億円となり持ち直して来た。更に景気回復や、情報セキュリティに対する認知度向上、セキュリティ投資への経営者の理解、脅威対策の抜本的見直し等により、大企業を中心に再びコンサルティング需要を高めていくと考え、2016 年度以降も拡大していくと予測している。

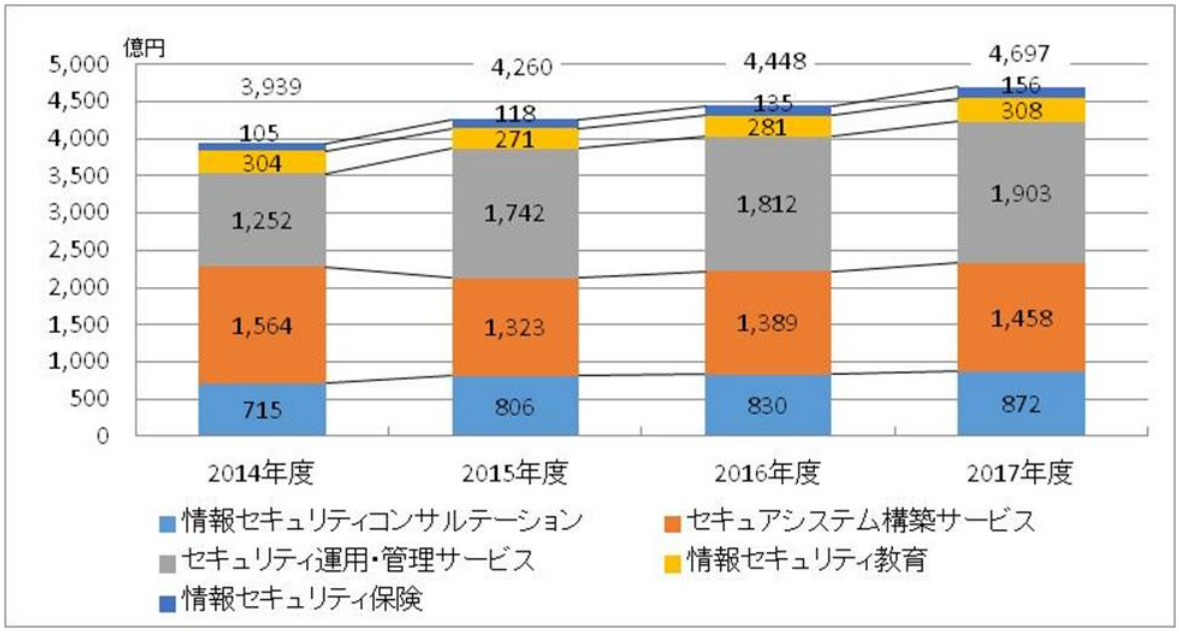


図 16　国内情報セキュリティサービス市場推移

2015 年度「情報セキュリティ教育」市場は 10.9%減の 271 億円となった。これは外部へ委託していた教育業務の内製化を進めた結果と考えられる。

しかし、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、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すると考えられ、2016 年度以降は再び拡大すると見込まれる。また、情報処理安全確保支援士試験(情報セキュリティスペシャリスト)の資格試験に対する外部教育などにより 2017 年には 9.6%の高い伸びを示すと予測している。

「情報セキュリティ保険」は、情報漏えい事件の増加、インターネットバンキングからの不正

送金被害を受け、伸びたカテゴリである。昨今その保障領域を広げており、サイバーセキュリティ保険として、今後保障の拡充、加入企業・団体の増加が見込まれる。

2.2.2. 情報セキュリティサービス市場のカテゴリ別分析

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

2.2.2.1. 情報セキュリティコンサルテーション市場

(1) 市場の動向

2015 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。

企業が情報システム化を実施する場合に受けるコンサルテーションの内、情報セキュリティだけを切り出して市場分析を行うことは困難である。よってこれまでベンダの提供規模から推算して「その他情報セキュリティコンサルテーション」の小分類に計上していた部分が大きかったが、今年度(2015 年度確定実績)以降、セキュリティ要件が明確化され、その他で分類していた数値が各小分類に流れた。その結果、各分類ともに 2014 年度に対する 2015 年度比は大きく伸びる形となったが、金額ベースでは「情報セキュリティポリシー構築支援・管理全般のコンサルテーション」が+16.6%、63 億円の伸びとなった。

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。つまりコーポレート・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のためのコンサルティング需要、さらに CSIRT の構築コンサル、超上流コンサルではなく、リスクベースのコンサルティングの需要増加が、情報セキュリティコンサルテーション市場の伸びの回復要因になっていると言える。

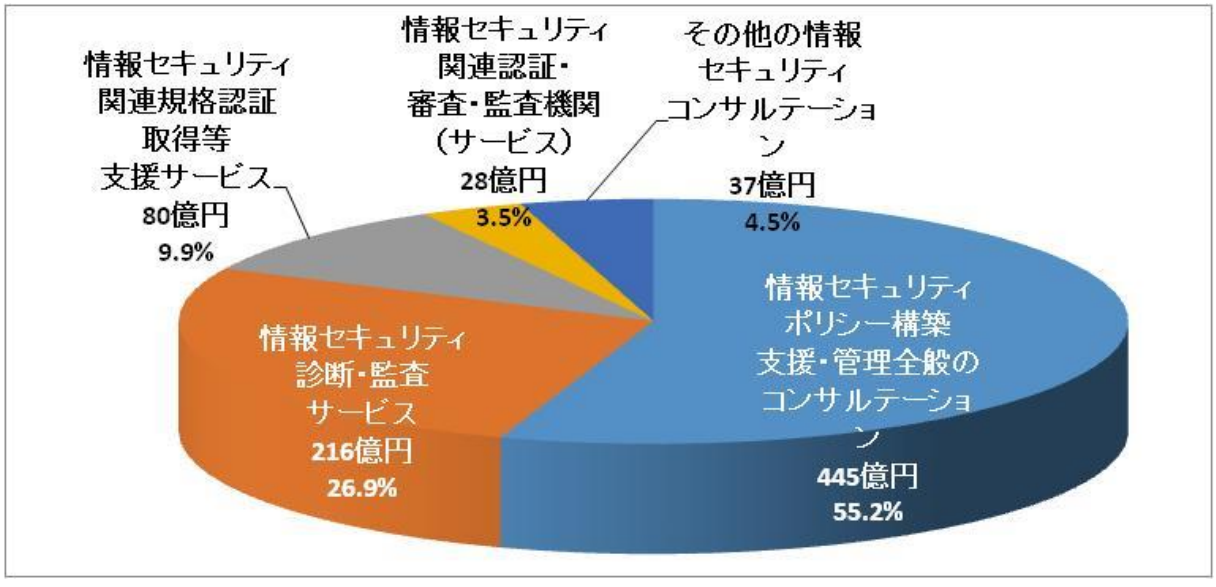


図 17　情報セキュリティコンサルテーション市場

歴史的には、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。更に 2017 年 5 月から改正個人情報保護法が施行され、JIPDEC 統計で 2016 年 3 月現在、ISMS 認証取得組織数は 2017 年 3 月：5,154 件（2016 年 3 月 4,827 件）、プライバシーマーク認定取得企業数は 2017 年 4 月：15,261 社（2016 年 6 月：14,710 社、2015 年 9 月：14,221 社）と増加している。

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、民間がイニシアチ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 PCIDSS 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 やプライバシー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 年度はその他カテゴリが減った分で各カテゴリが数字的には伸びているが、2016 年度以降は再び堅調に拡大すると予想する。

(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　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（億円）	2014 年度	2015 年度	2016 年度	2017 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	382	445	458	481
情報セキュリティ診断･監査サービス	203	216	223	234
情報セキュリティ関連規格認証取得等支援サービス	54	80	82	86
情報セキュリティ関連認証･審査・監査機関（サービス）	23	28	29	31
その他の情報セキュリティコンサルテーション	52	37	38	40
合計	715	806	830	872

構成比				
情報セキュリティポリシー構築支援・管理全般のコンサルテーション	53.4%	55.2%	55.2%	55.2%
情報セキュリティ診断･監査サービス	28.4%	26.9%	26.9%	26.9%
情報セキュリティ関連規格認証取得等支援サービス	7.6%	9.9%	9.9%	9.9%
情報セキュリティ関連認証･審査・監査機関（サービス）	3.2%	3.5%	3.5%	3.5%
その他の情報セキュリティコンサルテーション	7.3%	4.5%	4.5%	4.5%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
情報セキュリティポリシー構築支援・管理全般のコンサルテーション	－	16.6%	3.0%	5.0%
情報セキュリティ診断･監査サービス	－	6.5%	3.0%	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	－	46.5%	3.0%	5.0%
情報セキュリティ関連認証･審査・監査機関（サービス）	－	23.7%	3.0%	5.0%
その他の情報セキュリティコンサルテーション	－	-29.8%	3.0%	5.0%
合計	－	12.8%	3.0%	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(前年度比マイナス 1.8%)であったが、2015 年度は 806 億円(12.8%の伸び)となった。

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 445 億円と、2 番目の「情報セキュリティ診断・監査サービス」の 216 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。

「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）[1]はすでに 5,000 件を超えている。

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、マイナンバー制度の運用、法改正、認証制度の再構築、ネット決済の普及などによって、飽和気味であった市場が「情報セキュリティ関連規格認証取得等支援サービス」を中心に、年率 3～5%の成長基調に戻ると考えられる。

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

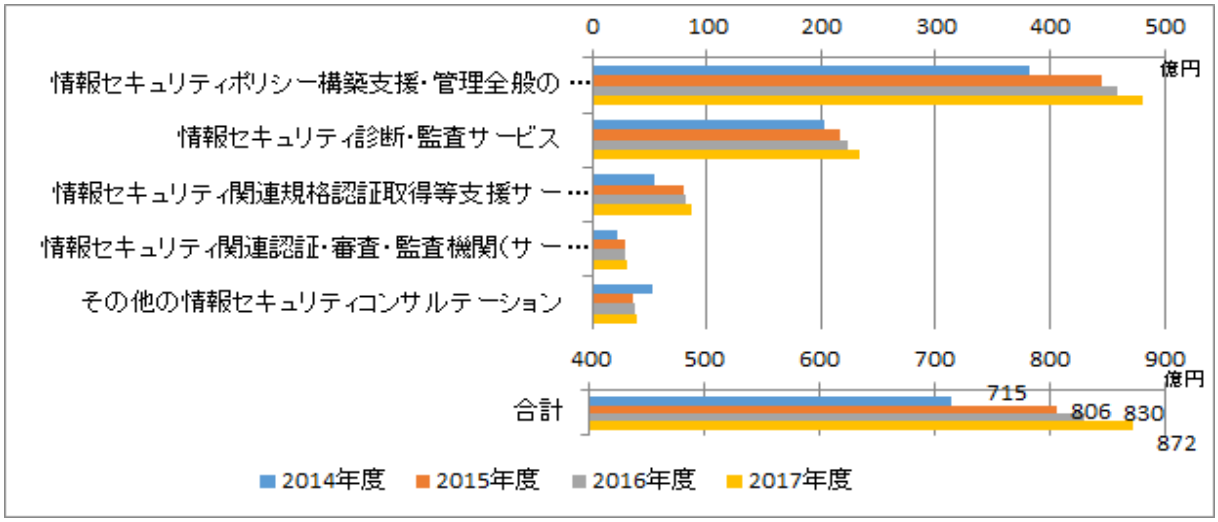


図 18　国内情報セキュリティコンサルテーション市場推移

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 2015 年度のセキュアシステム構築サービス市場のセグメント別分布を示す。

「セキュアシステム構築サービス」は、セキュリティ製品の導入や構築を含めた、IT セキュリティシステムまたは IT システムのセキュリティに関する構築､および構築を支援するサービスのカテゴリである。本カテゴリの市場規模は、情報セキュリティサービス市場全体の約 30%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 3 番目の規模である。

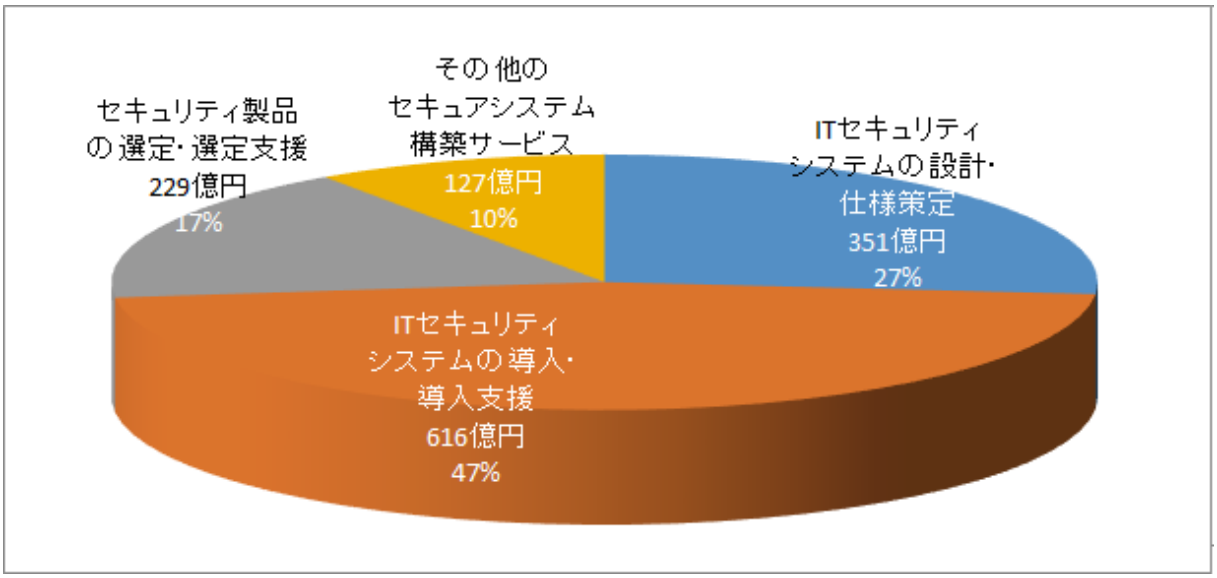


図 19　2015 年度のセキュアシステム構築サービス市場

「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。しかし、大規模情報漏えい事件、標的型攻撃被害などの詐欺・窃盗事件が多発した影響もあり、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的に行う傾向にあり、市場規模は堅調に拡大したとみられる。さらに、マイナンバー制度の導入など国家的プロジェクトも市場規模拡大につながったと考えられる。

しかし、セキュアシステム市場は、構築フェーズから運用フェーズへ移行し、更にクラウドサービスの市場が更に広がり、クラウドベンダが用意したセキュリティ機能モジュールをユーザが選択して実装する形が増加した結果、2015 年度は、-15.4%と大きく落ち込んだと考えられる。今後、オンプレミス向け市場は、横這いと考えられるが、クラウドサービスを活用するセキュアシステム構築市場が伸びると予想される。

(2) 市場規模とその推移

表11に国内セキュアシステム構築サービス市場規模の実績推定値と予測値を、図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」である。2014年度781億円、2015年度616億円（前年度比-21.2%）と大幅なマイナスとなっている。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2014年度362億円、2015年度351億円（前年度比-3.1%）とこちらもマイナス成長となった。

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（億円）	2014 年度	2015 年度	2016 年度	2017 年度
IT セキュリティシステムの設計･仕様策定	362	351	368	387
IT セキュリティシステムの導入･導入支援	781	616	646	679
セキュリティ製品の選定･選定支援	283	229	241	253
その他のセキュアシステム構築サービス	137	127	134	140
合計	1,564	1,323	1,389	1,458
構成比				
IT セキュリティシステムの設計･仕様策定	23.2%	26.5%	26.5%	26.5%
IT セキュリティシステムの導入･導入支援	50.0%	46.5%	46.5%	46.5%
セキュリティ製品の選定･選定支援	18.1%	17.3%	17.3%	17.3%
その他のセキュアシステム構築サービス	8.8%	9.6%	9.6%	9.6%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
IT セキュリティシステムの設計･仕様策定	―	-3.1%	5.0%	5.0%

IT セキュリティシステムの導入・導入支援	—	-21.2%	5.0%	5.0%
セキュリティ製品の選定・選定支援	—	-19.0%	5.0%	5.0%
その他のセキュアシステム構築サービス	—	-7.2%	5.0%	5.0%
合計	—	-15.4%	5.0%	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ある。2014年度は283億円、2015年度が229億円（前年度比-19.0%）とマイナスとなっている。

2015年度はセキュアシステム構築サービス自体が対前年度成長率－15.4%となった。これは構築のフェーズから運用管理のフェーズにシフトしたとも考えられる。実際2015年度にはマイナンバーの通知が始まるといった動きがあった。サイバー脅威の対策強化のためのシステム再構築や、企業向けモバイル情報管理の需要も高まって、より高度なSI構築ニーズが当該市場の拡大を牽引していくと予想されるが、2016年度は上昇に転じるものの2014年度の水準までは回復しないと予想される。

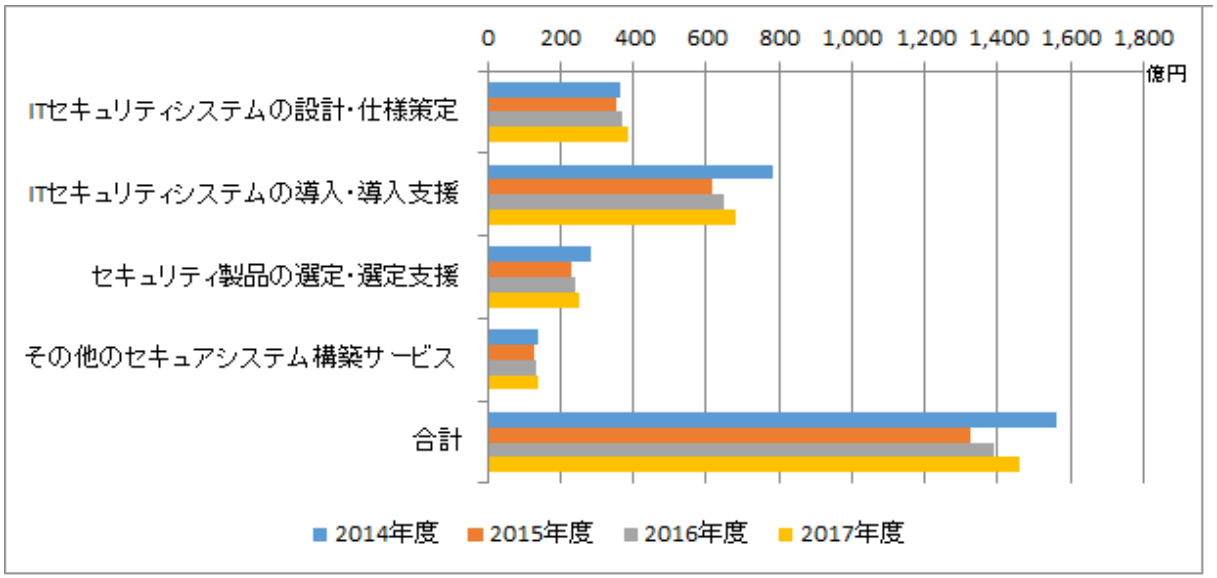


図 20　国内セキュアシステム構築サービス市場推移

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、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。中分類の構築サービスと教育サービスが前年比大幅減の中、当市場調査始まって以来の 39.1%490 億円の大幅な伸びを示した。これは、サイバー攻撃が激化する中、最も重要な SOC や運用管理に多額の予算をかけ、政府関連施設・重要インフラを防御する緊急対策が講じられたためと推察される。

なお、当調査の中では、セキュリティ運用・管理サービス市場は、「セキュリティ総合監視･運用支援サービス」、「ファイアウォール監視･運用支援サービス」「IDS／IPS 監視･運用支援サービス」、「ウイルス監視･ウイルス対策運用支援サービス」「フィルタリングサービス」、「脆弱性検査サービス」、「セキュリティ情報提供サービス」「電子認証サービス」、「インシデント対応関連サービス」「その他運用・管理サービス」と 10 の小分類に分けてサービス市場の変化を細かく分類していたが、この数年間の調査実績から、「その他」分類を廃止し、数値を各々に振り分けた。

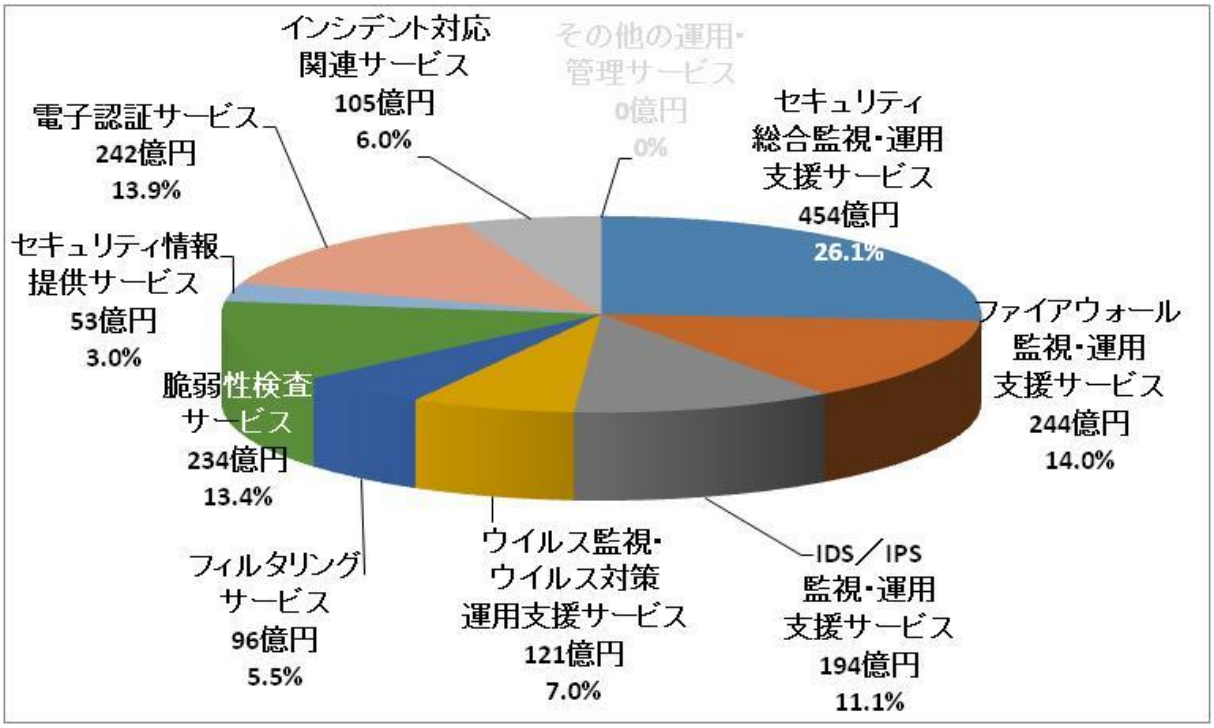


図 21　セキュリティ運用・管理サービス市場

(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、2015 年度の実績推定値は 1,742 億円(前年比 39.1 増)となった。

表 12　国内セキュリティ運用・管理サービス市場規模　実績と予測

市場規模（億円）	2014 年度	2015 年度	2016 年度	2017 年度
セキュリティ総合監視･運用支援サービス	365	454	472	496
ファイアウォール監視･運用支援サービス	65	244	253	266
IDS／IPS 監視･運用支援サービス	86	194	202	212
ウイルス監視･ウイルス対策運用支援サービス	50	121	126	133
フィルタリングサービス	101	96	100	105
脆弱性検査サービス	162	234	243	256

セキュリティ情報提供サービス	21	53	55	58
電子認証サービス	294	242	251	264
インシデント対応関連サービス	69	105	109	114
その他の運用･管理サービス	39	0	0	0
合計	1,252	1,742	1,812	1,903
構成比	2014 年度	2015 年度	2016 年度	2017 年度
セキュリティ総合監視･運用支援サービス	29.1%	26.1%	26.1%	26.1%
ファイアウォール監視･運用支援サービス	5.2%	14.0%	14.0%	14.0%
IDS／IPS 監視･運用支援サービス	6.9%	11.1%	11.1%	11.1%
ウイルス監視･ウイルス対策運用支援サービス	4.0%	7.0%	7.0%	7.0%
フィルタリングサービス	8.1%	5.5%	5.5%	5.5%
脆弱性検査サービス	13.0%	13.4%	13.4%	13.4%
セキュリティ情報提供サービス	1.7%	3.0%	3.0%	3.0%
電子認証サービス	23.5%	13.9%	13.9%	13.9%
インシデント対応関連サービス	5.5%	6.0%	6.0%	6.0%
その他の運用･管理サービス	3.1%	0.0%	0.0%	0.0%
合計	100%	100%	100%	100%
対前年度比成長率	2014 年度	2015 年度	2016 年度	2017 年度
セキュリティ総合監視･運用支援サービス	－	24.5%	4.0%	5.0%
ファイアウォール監視･運用支援サービス	－	277.3%	4.0%	5.0%
IDS／IPS 監視･運用支援サービス	－	125.2%	4.0%	5.0%
ウイルス監視･ウイルス対策運用支援サービス	－	143.1%	4.0%	5.0%
フィルタリングサービス	－	-4.9%	4.0%	5.0%
脆弱性検査サービス	－	44.2%	4.0%	5.0%
セキュリティ情報提供サービス	－	147.7%	4.0%	5.0%
電子認証サービス	－	-17.9%	4.0%	5.0%
インシデント対応関連サービス	－	52.8%	4.0%	5.0%
その他の運用･管理サービス	－	-100.0%	4.0%	5.0%
合計	－	39.1%	4.0%	5.0%

表 12 および図 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を示す。セグメントの内訳を見ると、「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、2015 年度の推定実績市場規模は 454 億円（前年度比成長率+24.5%）であった。2016 年度もプラス成長を続け、 2017 年度には 496 億円と順調に成長していくものと予測される。

「ファイアウォール監視・運用支援サービス」は、2014 年度 65 億円から 244 億円と実に +277.3%の大幅増となった。これは深刻化する外部からの攻撃、度重なる企業内の不正・情報漏えい事件事故により、政府機関・公的機関・重要インフラ企業・大企業が一斉に、監視・運用を

専門サービス業者に委託したためである。また東京オリンピックへ向けての情報管理：2W200M というキーワード（2014 年 2 月、ロンドンオリンピック情報セキュリティ責任者オリバー・ホーア氏が IPA に招待され、ロンドンでは 2 週間の開催期間で 2 億 2,100 万のサイバー攻撃があったと語ったこと）も 2015 年度の伸びを助長した。しかしこの 65 億円から 244 億円という大幅な伸びは 2015 年度の一過性の特徴であり、2016 年度以降は現状の高い数値を維持したまま他の市場セグメント同様+4～5%の伸びに落ち着くと考えている。

「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」も同様に 2015 年は自社の監視・運用では追いつかない現状から、専門業者への移管が加速的に進み、実績市場規模推定値は、2015 年度それぞれ 194 億円（前年度比成長率+125.2%）、121 億円（同+143.1%）になったと推定した。2016 年度・2017 年度は「ファイアウォール監視・運用支援サービス」と同様それぞれ+4～5%の伸びに落ち着くと考えている。

「フィルタリングサービス」は、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 2014 年度に 101 億円（2013 年度比+15.2%）と大幅成長を遂げたが、その反動もあり、2015 年度には 96 億円（前年比-4.9%）となったと予測した。2016 年度以降 100 億円台の市場定着が見込まれる。

「脆弱性検査サービス」は、2015 年度においては 234 億円（同+44.2%）、2016 年度には 243 億円（同+4.0%）、2017 年度には 256 億円（同+5.0%）と成長したが、昨年度の当報告書で予想していた規模に対して全体的に 50 億円以上増加して推移している。これはスマートフォンやタブレットの普及によりアプリ業者が増え、検査委託案件が大幅に伸びているためと考えている。

「セキュリティ情報提供サービス」については、昨年の調査では、2014 年度で 21 億円（同+9.4%）の安定市場で 2015 年度、2016 年度も飛躍的な増加はないものと予想していたが、上述の監視・運用サービスの大幅な伸びに呼応して、2015 年度 53 億円（前年度比+147,7%）となった。これは大企業の経営者への情報提供にと留まらず、CSIRT を立ち上げる組織・団体が増え、情報収集の為、セキュリティ情報提供サービスに対するニーズが高まり、また、一般企業や個人への普及啓発的な要素も含み、出す所がきちんと金を出して提供サービスを活性化したからであると考える。その結果 2016 年度 55 億円、2017 年度 58 億円と、このまま高留まった業績を維持すると予想している。

「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るが、2014 年度 294 億円から 2015 年度は 242 億円（同-17.9%）とマイナスとなった。これのカテゴリには電子証明書の発行も含まれるが、証明書の発行枚数に変化は無いものの、安価な証明書へ移行した結果、減少したものと思われる。。ただし、一度電子証明書を導入した顧客は継続して利用するため今後大幅なマイナス成長にはならないと考え、2016 年度は 251 億円、2017 年度は 264 億円と一定の増加を見込んでいる。

「インシデント対応関連サービス」は、多様化・複雑化するサイバー攻撃の増加に伴い、インシデント対応へのニーズが高まった結果、昨年の調査では 2014 年度は 69 億円（2013 年度比+19.9%）で今後も大幅な伸びが予想されるとしたが、今年度調査でも 2015 年度 105 億円（同+52.8%）となった。2016 年度以降もコンスタントな伸びを見込んでいる。

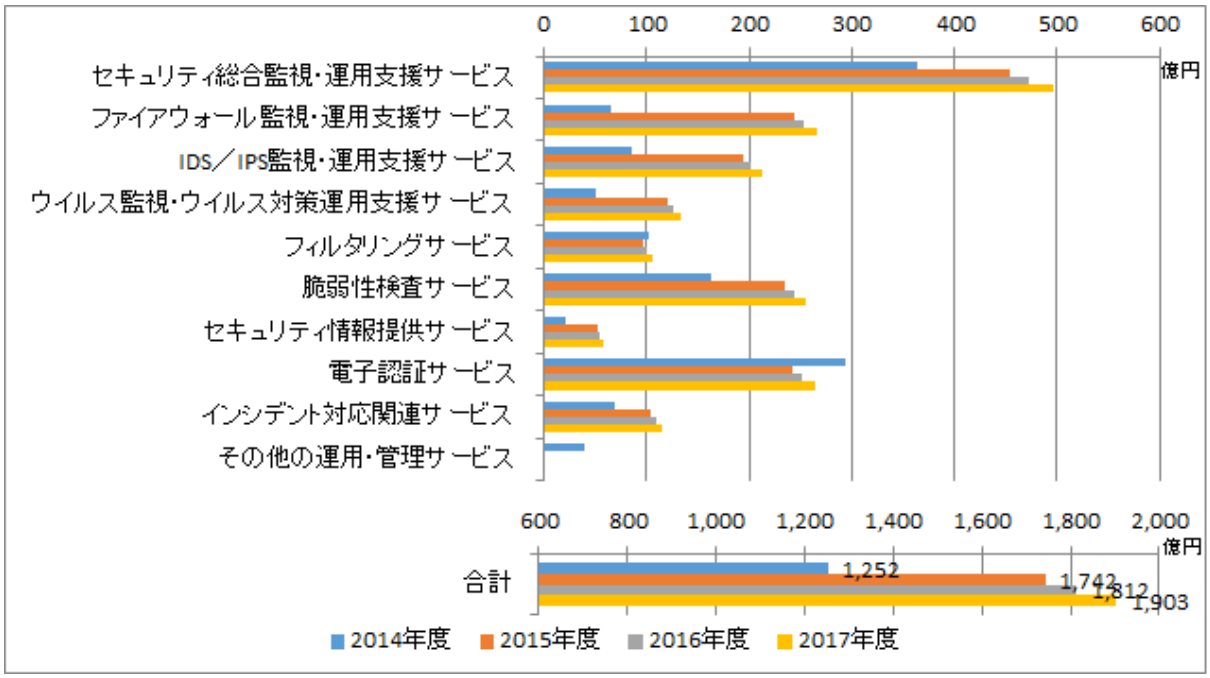


図 22　国内セキュリティ運用・管理サービス市場推移

2.2.2.4. 情報セキュリティ教育市場

(1)　市場動向

図23に2015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。

日々発生している事件・事故の恐ろしさを学習しても、時間が経つと意識は低下するため、基本的なことでも継続的に繰り返し復習する必要があることから、教育の需要は絶えず存在する。

しかし、不況下においては、真っ先にコスト削減の対象とされがちである。

そのような状況において、基本的なことの復習については、内製化あるいは e-ラーニングサービスの活用が増え、一方、技術の進展など専門的なことや新たなサイバー攻撃手法が出現してくるといったトピックスについては､外部の専門的な組織に委託するといった一般的な傾向があり、顕著な伸びを示している。

ひとたびオリンピックなど世界から注目がされるような機会・出来事、その他の時事的な要素により、サイバー攻撃の増加が予想される。サイバー攻撃は大規模な組織だけではなく、実は中小企業も約半数を占め、踏み台などとして狙われている事実が認識されていくにつれて、従来、コストと見られがちな教育も、企業が公器としての社会的責任を果たすために投資として、教育に力が入ってくると思われる。

情報セキュリティ教育は、大きく 3 つに大別できる。

① 一般社員向け教育：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もの。

② 専門社員向け教育：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向け教育：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。一般社員向け教育では、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。また、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 型のもの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。

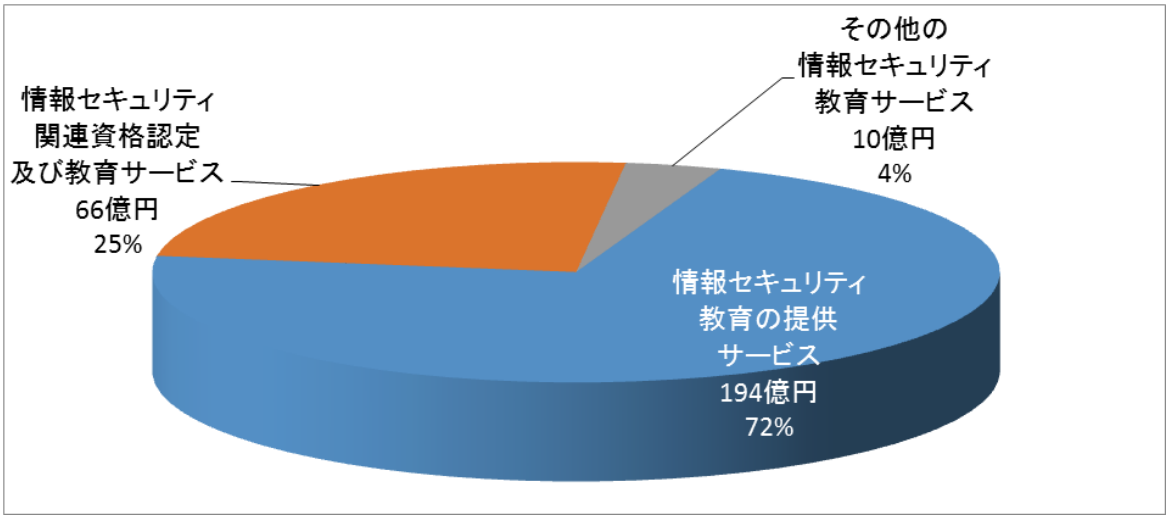


図 23　2015 年度の情報セキュリティ教育市場

「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、対象が主に個人単位となるため、基本的には小規模な市場である。しかしながら、②の専門社員向け教育や、顧客会社からの受託選定理由となる従事技術者のスキルレベルの確認手段として、グローバルな CISSP、GIAC などの国際セキュリティ資格取得のニーズが強くなってきている。

そのような状況において、不足しているセキュリティ人材を養成する早急な手段として、企業や組織のサイバーセキュリティ対策を担う専門人材を育成・確保するために、新たな国家資格制度として、情報処理安全確保支援士（通称 登録情報セキュリティスペシャリスト 又は 登録セキスペ）制度が、平成 28 年 10 月 21 日に創設された。登録セキスペは、サイバーセキュリティに関する専門的な知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し、サイバーセキュリティ対策の調査・分析・評価やその結果に基づく指導・助言を担う者である。企業は従来から人材配置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から資格取得の奨励などを行っており、また自らの昇進や転職市場での評価といったキャリアパスのために個人の受講者も増えていると見られる。

③ の経営層・上級管理職向け教育については、情報セキュリティがコストではなく投資であることを、情報システム部門や情報セキュリティ管理責任者から経営層に対して伝え、あるいは

経営層が自らの理解のために、必要であることを認識できるかにかかっている。近年は、脅威や事故の報道も盛んになり、情報セキュリィに対する社会的認知が進んだことから、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。

また、有事に正しい経営判断ができるよう、状況を正しく把握して経営層に平易な言葉で伝えることが出来る橋渡し人材を育てておく必要性についても認識させることが非常に重要なポイントである。

(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ほぼ 6～7%で推移する比較的小さい市場である。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事件などにより全体で 304 億円の規模であったが、2015 年度はこの教育サービス自体が企業内に取り込まれマイナス 10.9%の 271 億円に縮小。2016 年度はやや持ち直して 3.9%増の 281 億円となり、2017 年度には、2015 年度、2016 年度に立ち上げた CSIRT 向け教育及び訓練、標的型攻撃メール訓練、サイバー演習等の需要が高まり、9.6%増の 308 億円へ回復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（億円）	2014 年度	2015 年度	2016 年度	2017 年度
情報セキュリティ教育の提供サービス	265	194	202	222
情報セキュリティ関連資格認定及び教育サービス	29	66	69	76
その他の情報セキュリティ教育サービス	9	10	10	10
合計	304	271	281	308
構成比				
情報セキュリティ教育の提供サービス	87.3%	71.8%	71.9%	72.1%
情報セキュリティ関連資格認定及び教育サービス	9.7%	24.5%	24.6%	24.6%
その他の情報セキュリティ教育サービス	3.0%	3.7%	3.5%	3.2%
合計	100.0%	100.0%	100.0%	100.0%
対前年度比成長率				
情報セキュリティ教育の提供サービス	－	-26.7%	4.0%	10.0%
情報セキュリティ関連資格認定及び教育サービス	－	126.0%	4.0%	10.0%
その他の情報セキュリティ教育サービス	－	7.9%	0.0%	0.0%
合計	－	-10.9%	3.9%	9.6%

このセグメントの大部分は、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」を含む「情報セキュリティ教育の提供サービス」が70%以上占めているため、市場規模推移の全体傾向がカテゴリとセグメント間で一致する。すなわち市場規模としては、2014年度は265億円であったが、2015年度には194億円(同-26.7%)と大幅に縮小したものの、2016年度は202億円(同+4.0%)と持ち直し、2017年度には222億円（同+10.0%）と回復に転ずると予測される。

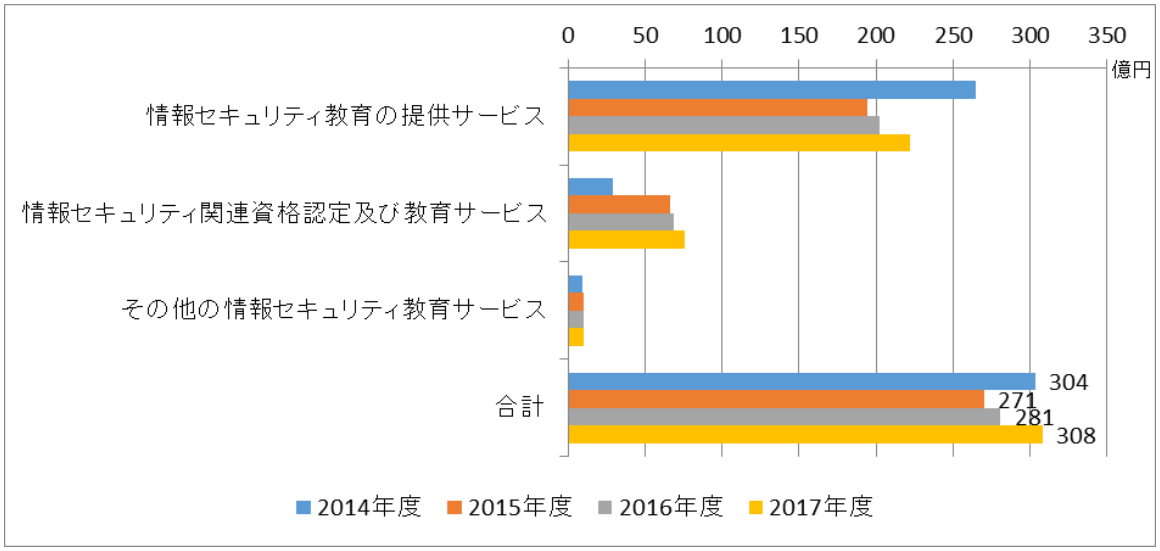


図 24　国内情報セキュリティ教育市場推移

一方、「情報セキュリティ資格認定及び教育サービス」は、2014年度は29億円のマーケットであったが、情報漏えい事件・事故の発生により社内教育をリードする専門資格者養成の需要が急拡大し、2015年度は前年度比126.0%増の66億円に達したと思われる。この増加は一過性のものではなく、2016年度は4.0%増の69億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、提供各社により内容は異なるが、概ね(a)情報漏えい等に伴う第三者への賠償責任、(b)これらに伴う自社損害・逸失利益、(c)弁護士費用・第三者機関への調査依頼費用等がある。掛け金の大きな(a)タイプの保険商品は、1990 年代後半からメーカを中心に幅広く利用されている製造者責任(PL)保険の延長で、情報セキュリティ損害補償を特約付与した法人契約も増えている。尚、一般的には(b)タイプの保険は少ない。

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。

これまでは主に大規模小売チェーンや大企業、顧客を多く抱えるサービス業などが対象であったが、今後、多様な商品が登場すると予想される。例えば、ロットが大きく掛け金の安い一般向け・青少年保護者向けの損害補填（見舞金型）や積み立て型、さらに小規模事業者向けの優遇税制連動型など多彩な商品の登場も期待される。

(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（億円）	2014 年度	2015 年度	2016 年度	2017 年度
情報セキュリティ保険	105	118	135	156
対前年度比成長率	―	12.4%	15.0%	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、近年は上述の通り大企業の情報漏えい対策の一環で、拡大ペースが上がっていると見られる。2014 年度の市場規模は 105 億円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し続け、2015 年度は 12.4%増の 118 億円、その後多様なサービスの登場により 2016 年度 135 億円、2017 年度 156 億円と年率 15%で伸びると予測する。

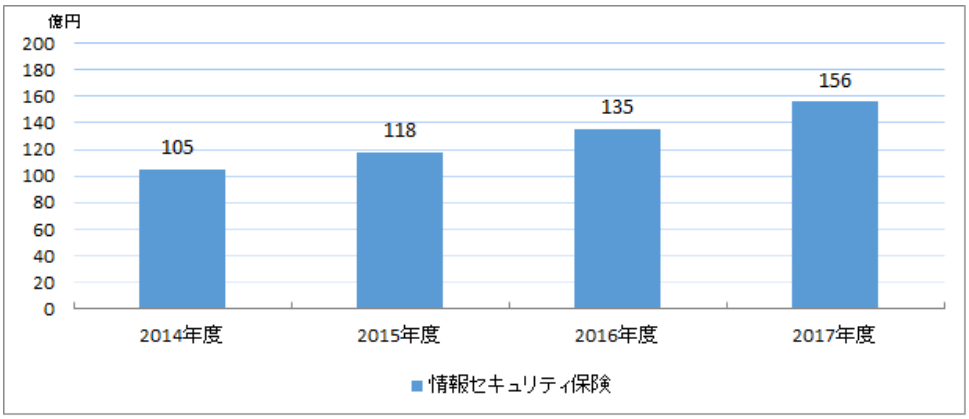


図 25　国内情報セキュリティ保険市場推移

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.　2016 年度におけるネットワークの脅威の動向

IPA は、2017 年 1 月 31 日に「情報セキュリティ 10 大脅威 2017」を発表した。昨年同様、「個人」と「組織」という異なる視点で 10 大脅威を選出している。昨年と比較して見ると、以下のようになる。

表 15　IPA　10 大脅威　昨年との比較（個人・法人）

個人			法人	
2017 年	2016 年		2017 年	2016 年
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	**第 1 位**	標的型攻撃による情報流出	標的型攻撃による情報流出
ランサムウェアによる被害	ランサムウェアを使った詐欺・恐喝	**第 2 位**	ランサムウェアによる被害	内部不正による情報漏えいとそれに伴う業務停止
スマートフォンやスマートフォンアプリを狙った攻撃	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	**第 3 位**	ウェブサービスからの個人情報の窃取	ウェブサービスからの個人情報の窃取
ウェブサービスへの不正ログイン	巧妙・悪質化するワンクリック請求	**第 4 位**	サービス妨害攻撃によるサービスの停止	サービス妨害攻撃によるサービスの停止
ワンクリック請求等の不当請求	ウェブサービスへの不正ログイン	**第 5 位**	内部不正による情報漏えいとそれに伴う業務停止	ウェブサイトの改ざん
ウェブサービスからの個人情報の窃取	匿名によるネット上の誹謗・中傷	**第 6 位**	ウェブサイトの改ざん	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
ネット上の誹謗・中傷	ウェブサービスからの個人情報の窃取	**第 7 位**	ウェブサービスへの不正ログイン	ランサムウェアを使った詐欺・恐喝
情報モラル欠如に伴う犯罪の低年齢化	情報モラル不足に伴う犯罪の低年齢化	**第 8 位**	IoT 機器の脆弱性の顕在化	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
インターネット上の	職業倫理欠如による	**第 9 位**	攻撃のビジネス化	ウェブサービスへの

サービスを悪用した攻撃	不適切な情報公開		（アンダーグラウンドサービス）	不正ログイン
IoT 機器の不適切な管理	インターネットの広告機能を悪用した攻撃	**第 10 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	過失による情報漏えい

（出典：IPA 各年度発表をもとに JNSA 作成）

毎年の見出しは、2013 年版「身近に忍び寄る脅威」、2014 年版「複雑化する情報セキュリティあなたが直面しているのは？」、2015 年版「被害に遭わないために実施すべき対策は？」、2016 年版「個人と組織で異なる脅威、立場ごとに異なる対応を」、2017 年版「職場に迫る脅威！　家庭に迫る脅威！？　急がば回れの心構えでセキュリティ対策を」と推移してきている。

2017 年の脅威は、個人、法人ともに 1 位は変動がなく、個人は「インターネットバンキングやクレジットカード情報の不正利用」、法人は「標的型攻撃による情報流出」となった。

そして、ランサムウェアによる被害が拡大したことから、個人・法人ともに 2 位に「ランサムウェアによる被害」が入った。ある端末がランサムウェアに感染すると、組織内の他のサーバなどのファイルも暗号化されてしまうため、組織にとっては、警戒すべき脅威である。

また、2016 年の後半には、IoT 機器を踏み台にして DDoS 攻撃に利用するマルウェアによって、ネットサービスが数時間にわたって接続しにくくなるなど､被害を受けた組織が多数確認された。それまでは仮説に過ぎなかった「IoT 機器の脅威」が、もはや現実のものとなった。その結果、個人 10 位「IoT 機器の不適切な管理」、組織 8 位「IoT 機器の脆弱性の顕在化」と、「IoT 機器の脅威」が初めてともにランクインした。

既に日本へのサイバー攻撃の半数以上は IoT 機器を狙ったものとされている。IoT 機器を乗っ取ったマルウェアは、外部からの指示を受けた時だけ動作し、その間だけ IoT 機器の動作が遅くなることが多いため、乗っ取られたことに気付くことが難しい。

昨年の事件は初期設定のままでセキュリティ設定が不十分であった機器を利用した攻撃であったが、今後は高度な攻撃手法を用いて IoT 機器を乗っ取ってくることが考えられる。それを防ぐためには、IoT 機器の開発者が、設計段階からセキュリティ対策を前提として取り組む必要がある。ちなみに、設計時のセキュリティ対策コストを 1 とすると、開発時からセキュリティ対策を行うと 6.5 倍、テスト時からでは 15 倍、そして運用中のものに対しては 100 倍のコストが掛かるとも言われている。[2]

IPA からは、適切なセキュリティ対策を施した IoT 機器が供給されるよう、製造者・開発者向けに IoT のセキュリティ設計について解説した「IoT 開発におけるセキュリティ設計の手引き」が公開されているので、参考にしたい。

セキュリティ対策は、これ一つで完璧というものはなく､「多層防御でリスクを下げていくしかない」ということが多くで語られており､「一人一人がセキュリティ意識を持って携わっていくこ

[2] 「セキュリティ・バイ・デザイン入門」2016 年 11 月 17・18 日 総合技術展 ET/IoT2016 IPA ブースプレゼンより　http://www.ipa.go.jp/files/000055823.pdf

とも多層防御の一部となり、セキュリティ対策のレベルを高めていくことに繋がる」とも言われていることを再認識したい。

3.2. セキュリティ関連トピック

3.3. 改正個人情報保護法と情報セキュリティの果たすべき役割の変化

3.3.1. 改正個人情報保護法と情報セキュリティの関係

2017 年 5 月 30 日、改正個人情報保護法（以後：改正法）が全面施行された。この改正法は、情報セキュリティビジネスにどのような影響を及ぼすのであろうか。2005 年全面施行された旧個人情報保護法は、情報セキュリティビジネスに対して多大な影響を与えたことは間違いない。このことは、情報セキュリティの啓発という意味においても非常に重要な出来事であった一方、あるべき個人情報の利活用を阻んだ面も否定できない。

今回の改正法の大きな目標の一つは、個人情報の保護と利活用の両立になる。今後の society5.0、第 4 次産業革命といった社会において、IoT により広く大量に集められたパーソナルデータを如何に利活用し、かつ保護するかということが、 日本だけではなく世界的な課題となっている。こうした状況も踏まえ、改正法 1 条では、以下のように記述されている。

「この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の 個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報 を取り扱う事業者の遵守すべき義務等を定めることにより、 個人情報の適正かつ効果的な利活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。」

改正法では、旧法から「個人情報の適正かつ効果的な利活用が新たな産業の創出並びに 活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の」が追記された。

改正法において、情報セキュリティビジネスに影響を与えそうな話としては、例えば、個人情報が 5000 件 以下の小規模事業者も、個人情報保護法の対象となることなどがある。しかし、改正法 1 条の記述に見られるような理念、更には、改正法だけではなく、少子高齢化する日本の社会の変化、そして、世界の動向を鑑みた場合、情報セキュリティ関係者が一番考えるべきことは、「個人情報の保護と利活用の両立」であり、そのための情報セキュリティ技術、および、ビジネスではないだろうか。

改正法の施行に伴い、多くのガイドラインが、個人情報保護委員会から公表されている。これらのガイドラインは、実質的な情報セキュリティの対応に関係するものも多い。こうしたガイドラインにおいて注目されるものの一つに、「個人データの漏えい等の事案が発生した場合等の対応について」[1][2]がある。このガイドラインでは、「高度な暗号化がされた個人データの漏えい」に

[1] 個人データの漏えい等の事案が発生した場合等の対応について（平成 29 年個人情報保護委員会告示第 1 号） 平成 29 年 2 月 16 日

ついての記述があり、個人データの漏えい等の事案において個人情報保護委員会等への報告を要しない場合として「漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合」と明記されている。

こうしたことも、「個人情報の保護と利活用の両立」と無関係ではないと考えられる。ここでは、そもそも個人情報の安全管理措置としての、暗号技術に依拠した情報セキュリティソリューションの在り方を念頭に、この個人情報の高度な暗号化について考察する。

3.3.2. 個人情報の高度な暗号化に関する考察

3.3.2.1. 個人情報の暗号化に関するこれまでの議論

個人情報の「高度な暗号化」については、改正以前の 2005 年の個人情報保護法施行の頃から議論されているものの、そもそも「高度な暗号化」自体が明らかにはなっていないところがある。こうした中、適切な技術的保護措置としての「高度な暗号化」の意味するところが明確になれば、「高度な暗号化」に対応したソリューションの開発が促される。それは、こうしたソリューションが利用され、結果として個人情報保護の本来の目標である実体的なプライバシー侵害を減少させる方向に向かうことになる。そのため、ここで必要となるのは「高度な暗号化」に関する何らかの技術的なガイドラインの存在になる。

この「高度な暗号化がされた個人データ」に関連した議論と動向は、2012 年 9 月発行の JNSA Press 第 34 号に「暗号技術による個人情報保護の制度と技術の動向」（以後、JNSA Press 記事）[3]として執筆しており、記事内の結論として、以下の 3 つを挙げている。

- 個人情報保護法に関連する技術ガイドラインの統合
- 暗号技術における鍵管理技術の重要性の周知と施策
- 情報化社会における技術と制度の整合

残念ながら、改正法おけるガイドラインの Q&A[2]により「高度な暗号化がされた個人データ」の意味するところが補足されたものの、この記事を執筆してから現在に至るまで、状況はあまり変わっているようには見受けらない。

改正法の全面施行によりガイドラインに関する権限が一元化され、各主務大臣が保有している個人情報保護法に関する勧告・命令等の権限が個人情報保護委員会に一元化されることになった。

---

https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf

[2] 「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関する Q&A　平成 29 年 2 月 16 日 個人情報保護委員会
http://www.ppc.go.jp/files/pdf/kojouhouQA.pdf

[3] [3]JNSA、“暗号技術による個人情報保護の制度と技術の動向”（2012）
http://www.jnsa.org/jnsapress/vol34/3_kikou.pdf

これを機に個人情報保護法に関連する技術ガイドラインの統合と、その一環としての「高度な暗号化」に関するガイドラインの作成等も検討されるべきであろう。

ここでは、以上を踏まえて、また、これまでの経緯も含め以下の意見を記述する。

- 高度に暗号化された個人データは保護された状態とみなすべき
- 暗号化鍵破棄による個人データ削除を制度的にも明確にするべき
- 暗号化された個人データのアクセス制御の考え方を明確にするべき
- 業界を横断する技術ガイドラインを作成する体制が検討されるべき

3.3.2.2.高度に暗号化された個人データは保護された状態とみなすべき

以前から「暗号化した個人データは個人情報なのか？」という議論があった。暗号化された個人データが非個人情報だと解釈するならば、多くの情報漏えいは「事案」とはならない。しかしながら改正法においても、暗号化した個人データも個人情報と見なすべきである。いわゆる個人情報の「提供元基準説」を取る限り、暗号化した個人データであっても、暗号化鍵を保持している人または暗号化鍵にアクセス権限のある人は、暗号化した個人データから元の個人データを復元できるためである。元のデータに復号できる限りは、個人情報と見なすのが妥当かと考えられ、この妥当性については改正法でも変わらないと考えられる。

では、個人データを暗号化して管理することは、意味がないのであろうか。当然、個人情報に関する安全管理措置として大いに意味がある。これまでの議論で欠けていたのは、高度な暗号化がされた個人データに関連する、個人情報の漏えい定義、アクセス制御の定義等ではないだろうか。JNSA Press 記事では、米国の HIPPA における事例を紹介しているが、「暗号化した個人データ」は、保護された状態、アクセス制御が出来ているという解釈のようである。

これまで「暗号化した個人データは個人情報なのか？」という議論に拘り過ぎたこと自体が、あるべき技術的な個人情報保護の方向性を見出せていなかった理由の一つかもしれない。

3.3.2.3.暗号化鍵破棄による個人データ削除を制度的にも明確にするべき

高度な暗号化の「高度」の意味は、「JNSA Press 記事」にも書いたとおり、概ね「暗号アルゴリズム」、「暗号モジュールの実装」、「暗号化に利用する鍵の管理」が高度であることを意味すると考えられる。

暗号化した個人データと暗号化鍵が別に管理されている場合、暗号化した個人データのみが第3 者に渡ったとしても、暗号化鍵が安全に保管されている限り、個人データは暗号化鍵によりアクセス制御がなされている状態と解釈されるべきではないであろうか。更には、暗号化鍵の破棄を行う事により、第3者に渡った（暗号化した）個人データを削除したとみなすべきではないだろうか。この点を明確にするべきだと考えられるが、この際、この暗号化に用いられる暗号アルゴリズムは、単に CRYPTREC 暗号リストと言うだけでなく、長期間に渡る機密性を保持するために、その鍵長も十分に考慮される必要はある。

このような暗号化鍵の破棄によるデータの削除の仕組みは、2014 年に発行された、米国 NIST

の SP800-88 rev.1 Guidelines for Media Sanitization[4]において、Cryptographic Erase として明記されている。ちなみに、データ保存の方法が、磁気ディスクから、SSD 等へ広がっており、手元にある保存媒体からクラウド上へ（暗号化されつつ自動的に）保存される事も多くなる中、何をもって個人情報を削除した事とするかは、それなりに複雑な問題になる。

個人データには、当然のことながらデータとしてのライフサイクルがあり、最終的には削除が要求され､削除されていない個人データは安全管理措置義務が課せられることになる｡ところが、この個人情報の安全管理措置の中でも非常に重要なデータ削除に関して、米国における SP800-88 rev.1 に対応する技術ガイドラインが、日本には存在しないという問題もある。そのような事情もあり、Cryptographic Erase のようなデータ削除の方法が、法的に適合しているか判断できないのが現在の状況であり、これは「高度な暗号化」の意味や有用性を理解する妨げにもなっていると考えられる。

3.3.2.4.暗号化された個人データのアクセス制御の考え方を明確にするべき

USB メモリのような持ち運びができるデバイスに関して、有用な安全管理措置として、耐タンパー性のあるハードウェアによる暗号化鍵の保護を施したフルディスク暗号化（ここでは、ハードウェア暗号化と称する）がある。ハードウェア暗号化は、多くのモバイルデバイスでも採用されており、技術ガイドラインとしては米国 NIST の SP800-111 Guide to Storage Encryption Technologies for End user Devices[5]があり、また、非常によく検討されたプロテクションプロファイル[6]も存在する。

ハードウェア暗号化を実装したモバイルデバイスには、暗号化鍵格納領域にログインしない限り復号できない仕組みが提供されており、またログインパスワードの照合をハードウェア暗号化ディスク自体ないしハードウェア暗号化ディスクと信頼関係があるセキュアデバイスのみに限定することにより、ログイン機構に対するオフラインでのブルートフォース攻撃・辞書攻撃に対して耐性を持つ。

これに関しては、ログイン機構のロック解除方法等のバックドアの存在を指摘されたり、FBI がアップル等のベンダに対して、ロック解除方法等のバックドアの存在自体を求めるといった動きもある[7]。これは、逆説的になるが、ハードウェア暗号化デバイスによるデータの暗号化が、

---

[4] NIST Special Publication 800-88 Revision 1, “Guidelines for Media Sanitization” (2014)
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

[5] NIST Special Publication 800-111, “Guide to Storage Encryption Technologies for End user Devices” (2007)
http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

[6] IPA、“USB フラッシュドライブ用のプロテクションプロファイル”(2011)
https://www.ipa.go.jp/files/000015355.pdf

[7] 日本経済新聞、“アップル　VS　FBI　米司法、割れる判断 NY 地裁は保護解除認めず　長期化

それだけ完成度が高いとも考えられる。

このような状況において、個人データが格納されたハードウェア暗号化デバイスの物理的な紛失を直ちに「個人データ漏えい（事案)」と見做すのかという疑問が生じる。例え、デバイスが、第3者に渡ったとしても、デバイスへのログインのパスワード等の技術的保護措置によるアクセス制御が適切になされているならば、格納された個人データは漏えいしていないという解釈もあるのではないだろうか。

インターネットに接続されたサイトにおいて、弱いパスワードでアクセス制御がなされた個人データは、残念ながら多く存在すると思われる中、何が「個人データ漏えい（事案)」に当たるかを適切に提示した上で、個人データの適切な技術的保護措置について考える必要があるだろう。

3.3.2.5.業界を横断する技術ガイドラインを作成する体制が検討されるべき

JNSA Press 記事での結論として「(1)個人情報保護法に関連する技術ガイドラインの統合」がある。個人情報保護法に関する勧告・命令等の権限が個人情報保護委員会に一元化されたことで、統合されたガイドラインは作りやすくなったと言える。

しかし、深い専門性が必要な技術ガイドラインに関しても、個人情報保護委員会が作成することが可能なのか、また、そもそも個人情報保護委員会が作成するべきなのかという疑問が残る。安易な「高度な暗号化」に関するガイドラインは、自称高度な暗号化が蔓延する結果ともなりかねない。

技術ガイドラインは技術を中心に担当している組織が作成し、そのガイドラインを個人情報保護委員会が作成するレポートで参照することにより、何らかのお墨付きを与えるといった枠組みが必要ではないだろうか。

業界、官庁を横断した、強制力のある技術ガイドラインは、誰が作成できるのか、その能力及び権限に着目した場合、日本には対応する機関がないという問題に直面する。米国においては、FISMA(2002 年施行の連邦情報セキュリティマネジメント法)に基づく法的 責務を果たす一環としてNIST（アメリカ国立標準技術研究所）がNIST SP 800-88 などのSP800シリーズを作成しているが、日本にはそのような制度も機関もない。個人情報保護委員会が設立されたことにより、個人情報保護法に関する勧告・命令等の権限も一元化できる訳であり、技術的な側面でも一元化できる何らかの方策が検討されるべきであろう。

NIST SP 800 シリーズは、個人情報保護のためのガイドラインではなく、一般的に機密情報を扱うガイドラインとしての立て付けになるが、個人情報の安全管理措置自体、機密情報の保護の一つとみなされることが、ガイドライン作成自体が共通化でき、その負担も軽減できる。

は必至”(2016)

http://www.nikkei.com/article/DGKKASGM01H60_R00C16A3FF1000/

3.3.3. まとめ

2005 年全面施行された旧個人情報保護法から、現在まで、個人情報を取り囲む社会の状況は、大きく変わっており、更に society5.0、第 4 次産業革命、スマート社会等の世界観の元、大きく変貌しようとしている。サイバー攻撃の対象としての個人情報があり、その保護の重要性が増す一方で、これまでの枠組みにとらわれない個人情報連携、個人情報共有が、社会から求められている。

こうした状況において、今後取り組むべきことに、「情報化社会における技術と制度の整合」があるが、これは JNSA Press 記事においても、最後の結論の一つとして挙げている。今回の改正法でも、この技術と制度の整合に大変な労力が掛かっており、さらに解決するべき課題も多いのではないだろうか。

個人情報保護法が改正に向かったきっかけの 1 つに、パーソナルデータに関する検討会・技術検討ワーキンググループ報告書[8]がある、この WG の主査を務められた国立情報学研究所佐藤一郎教授は、こうした時代の背景を「技術と制度が不可分になる時代」[9]と表現している。

「高度な暗号化がされた個人データ」に関しても、「高度な暗号化」[10]に関するある程度強制力のある技術ガイドラインが作成されるべきであるが、法制度と技術の双方からのアプローチが必要な故に、技術ガイドラインの作成が置き去りにされてきた面があるかと思われる。このような課題を置き去りにすることは、デジタル社会への本質的な移行を阻む結果になりかねない。改正法をきっかけとして、このような課題の解決が期待される。

こうした中、情報セキュリティの関係者は、「高度な暗号化」に限らず、個人情報の保護と利活用を両立するための制度、技術、ビジネスの在り方等を、社会に提言していく必要がある。

---

[8] パーソナルデータに関する検討会、“技術検討ワーキンググループ報告書”(2013)
http://www.kantei.go.jp/jp/singi/it2/pd/dai5/siryou2-1.pdf

[9] 佐藤一郎、“技術と制度が不可分になる時代”、DIAMOND online (2014)
http://diamond.jp/articles/-/54978

[10] 「個人情報の高度な暗号化について考える」 JNSA セキュリティしんだん
http://www.jnsa.org/secshindan/secshindan_23.html

【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.　調査対象期間

本調査の対象は国内情報セキュリティ市場である。「2016 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) 2014 年度国内情報セキュリティ市場規模　推定実績値
(2) 2015 年度国内情報セキュリティ市場規模　推定実績値
(3) 2016 年度国内情報セキュリティ市場規模　実績見込値
(4) 2017 年度国内情報セキュリティ市場規模　予測値

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（※2013 年度以降は実施していない）

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り、また企業がその活動の透明性を図るべく自社のホームページ等に業績を載せるケースが増えてきたため、2013 年度以降はワーキンググループメンバの所属する企業の動向をワーキンググループ内で共有し、またその同業他社の状況を推定する等の方法をとることで分析し、外部へのヒアリングは実施していない。

(3) サンプリング調査（※2014 年度以降は実施していない）

2014 年度以降、アンケート調査によるサンプリングは実施していないが、セキュリティ事業に関わる日本全国 520 社（JNSA 会員企業 190 社を含む）を、ワーキンググループメンバが、調査会社より購入した売上業績データ･有価証券報告書･Web ページ･製品資料等の外部公表資料と様々なニュースリリース･傍証的情報を元に市場規模を算定･推計し、調査結果に反映させる方法を取っている。なお、市場規模拡大に伴い新規参入事業者の増加が続いており、今回調査対象では前回に比べ 23 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 2015 年度である。2016 年度、2017 年度の市場規模推定にあたっては、2015 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。

2012 年度までのヒアリング調査や 2013 年度までのアンケート調査で収集した回答(事業計画、売上予測等）の数値と、それらの翌年以降毎年の調査会社の基準年の決算売上データと比較して増減を推計している。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、各種世界統計･政府統計等を参考に売上高成長率を収集し、他の経済成長指標等も参考にした。その上でワーキンググループメンバの業種における複数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ている。

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、二重に営業収入(売上)が計上されないよう、業種毎に製品のカテゴリ毎に独自の補正を加えた。この独自の補正は 2013 年度以降毎年精度が上がってきており、ヒアリングやアンケートに替わる手段として、当ワーキンググループ独自の調査分析ノウハウとなって蓄積されつつある。

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。今年度も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、本書 5.2、5.3、6.1 章にある市場区分定義の解説書も 2012 年度版を引き続き踏襲することとした。必要があれば、昨年度版[3]を参照していただきたい。

5.1. 情報セキュリティツール･サービスの市場分類定義表・用語解説

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

表 17、表 18 には、情報セキュリティ市場調査で用いた「情報セキュリティツール」「情報セキュリティサービス」の市場区分とその定義、もしくは説明･例示等の一覧表を掲げる。

表 16　用語説明

アプライアンス	ハードウェアとソフトウェアを一体として特定の機能を提供する販売形態をとる製品 1 台のコンピュータで複数の機能を提供するサーバ型コンピュータ。内部バスに複数の機能モジュールを接続して複数の機能を実現する形（いわゆるシャーシ型）を含む。ブレードサーバ形式で複数の機能サーバが並列して機能を実行し、全体として統括する OS が存在しない状態（いわゆるブレードサーバ型）は含まない。
ソフトウェア	パッケージ製品、ダウンロード製品、ライセンス販売製品等、定型化されたもの 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

[3] http://www.jnsa.org/result/2016/surv_mrk/data/2015_mrk-report.pdf

VPN	Virtual Private Network 仮想私設通信網
PCIDSS	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	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。

	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。	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	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。

	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。	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、PCIDSS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。 PCIDSS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一部ととらえ、「セキュリティ教育サービス」には集計しない。	情報セキュリティ教育の提供およびe-ラーニングサービス	情報セキュリティ教育の提供･実施サービス。 講師が実施する集合教育・実地教育・演習等のサービス提供の形態、ならびにセキュリティ教育の内容または教材（いわゆるコンテンツ）の販売もしくはライセンス提供を行う形態の双方を含む。 情報セキュリティ教育のためのe-ラーニングのコンテンツの開発・提供およびe-ラーニングの実施サービスを含む。 セキュリティ資格関連のサービスは「セキュリティ資格認定及び教育サービス」に分類する。
		情報セキュリティ関連資格認定及び教育サービス	情報セキュリティ関連の資格の認定（継続・維持を含む）を行い、または資格認定のための教育研修の実施や受験準備のための講習等を行うサービス。
		その他の情報セキュリティ教育サービス	その他の情報セキュリティ教育に関するサービス。情報セキュリティ教育を直接の目的としたコンサルテーションやシステム構築サービスを含む。 情報セキュリティ製品の使用等に関して製品ベンダが行う教育のうち、製品取扱知識だけでなくネットワークセキュリティ一般についての知識・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、今年度 520 社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[4]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

[4] NI：Network Integration, ネットワーク構築

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

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

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

H　その他

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

6.2.　業態区分と市場区分における分布

上記による業態区分と、市場分類との組合せによる、集計対象企業の分布は、表 19 に示す通りである。

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	589	97	128	74	115	39	25	85	26
有効推計対象	**520**	76	115	64	111	36	24	76	18
情報セキュリティツール全体 (X)	349	54	92	58	85	28	3	23	6
統合型アプライアンス	87	11	8	19	24	17	1	7	0
ネットワーク脅威対策製品	160	22	23	32	49	22	1	10	1
コンテンツセキュリティ対策製品	181	23	36	34	52	21	1	13	1
アイデンティティ・アクセス管理製品	151	19	37	23	41	21	2	7	1
システムセキュリティ管理製品	164	18	37	30	44	20	2	11	2
暗号製品	86	12	13	17	27	12	1	2	2
情報セキュリティサービス全体 (Y)	298	29	42	20	75	34	23	63	12
情報セキュリティコンサルテーション	154	10	14	9	38	22	19	40	2
セキュアシステム構築サービス	158	10	21	11	55	29	8	23	1
セキュリティ運用・管理サービス	186	23	26	15	39	27	9	41	6
情報セキュリティ教育	92	6	6	5	21	17	9	25	3
情報セキュリティ保険	16	1	0	1	2	2	1	3	6
(参考)									
ツール専業 (X∩^Y)	178	33	63	40	31	1	0	6	4
ツール・サービス兼業 (X∩Y)	171	21	29	18	54	27	3	17	2
サービス専業(^X∩Y)	127	8	13	2	21	7	20	46	10

まず、調査対象・有効推計対象の企業数を、昨年の調査と今年度の調査とで比較してみると、昨年は、調査対象 571 社・有効推計対象 497 社で、今年度は調査対象 589 社・有効推計対象 520 社となり、昨年と今年の差は、調査対象が 18 社増え、有効推計対象が 23 社増えたということになる。

業種別の事業参入増減を見ると 2015 年度は、

（1） 海外ベンダの多くが、ツールからサービスへ事業の柱を移行している。

（2） 国内ベンダ・大手 SIer は、ツール事業の寡占化、サービスへの移行が進んでいる。

（3） 販売流通は事業者が減った。

（4） SI･NI 事業者は専門領域を微妙に変えながら増えている。

（5） サービス提供や異業種による情報セキュリティ市場参入は減った。

という特徴が反映されており、クラウド化・モバイルビジネスに対応した事業転換や、大手の事業再編などが影響していると推察される。

事業の傾向としては、「ベンダ」は自らが製造・供給する製品を特定のカテゴリでビジネスにするため各カテゴリに幅広く分布する傾向がある。また、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」と「国内のセキュリティツールメーカ」である。

なお、参入企業は多くないが、「SI が主たる付加価値の大手システムインテグレータ」は事業規模が大きいため、市場に与える影響も大きくなる。また、「コンテンツセキュリティ対策製品」と「セキュリティ運用・管理サービス」への参入企業は依然として最多であるが、前述の通り、寡占化・専門化が進んでいると読み取れる。

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。2010 年半ば以降、世界経済は回復基調を維持しながらも、それまでの勢いをやや失っており、2011 年に入り、世界経済の回復に陰りが見え始めている。米国の財政懸念とユーロ圏債務危機の深刻化を反映し、2011 年夏から秋には世界同時株安、国債価格の下落、為替市場の変動など、世界的な金融市場の混乱が生じている。

2013 年には米国経済が底堅く推移し、欧州も 長期的な低迷から回復へと転ずる兆しが見られるなど、先進国が堅調さを示す一方、新興国については、 2013 年は全般的に景気減速が目立った。こうした状況から、2013 年の世界経済は全体として緩やかな成長にとどまった。

2016 年の成長率は、2015 年の 3.2%の伸びから鈍化して、3.1%となった。低成長には、米国の予想外の失速、日本、欧州各国の低成長の持続といった日米欧の動きと、原材料価格の急落の影響を大きく受けた資源輸出国の低迷、そして中国に代表される新興国の成長率の鈍化といった要素が作用している。

2016 年の冴えない結果の後、2017 年と 2018 年には、特に新興国地域と途上国地域に おいて、経済が勢いをやや回復すると予想されている。

表 20　GDP 実質成長率の推移（単位%）

暦年	2010	2011	2012	2013	2014	2015	2016	2017
世界	5.4	4.2	3.5	3.3	3.4	3.2	3.1	3.4
日本	4.7	-0.5	1.7	1.4	0.0	0.5	0.5	0.6
米国	2.5	1.6	2.2	1.7	2.4	2.6	1.6	2.2

（出典：IMF2016 年 4 月レポート[5]より）

米国経済は回復が続いている。金融危機後に 10%前後にまで上昇した失業率は 5%弱にまで改善した。実質 GDP も金融危機前の水準を上回って推移している。ただし、金融危機前に比べれば、経済成長率が低いことは否めない。2017 年以降は、トランプ大統領の政策動向や市場動向が注目される。日本の成長率に関して、2015 年から少し回復し、横ばいで推移しているが、個人消費はサービスや耐久財を中心に増加が続き、企業の生産活動も持ち直しに向けた動きを見せていることから横ばいの圏内から抜け出しつつあると期待されている。ただし、海外経済の不確実性や金融資本市場の変動の影響に留意する必要があるとして、景気回復の動きは下振れのリスクを抱えており、確実なものとはなっていない事が示唆されている。

2012～2016 のスパンで見ると、世界経済は 3%台の堅調な成長軌道をたどっている。低迷しているとはいえ 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

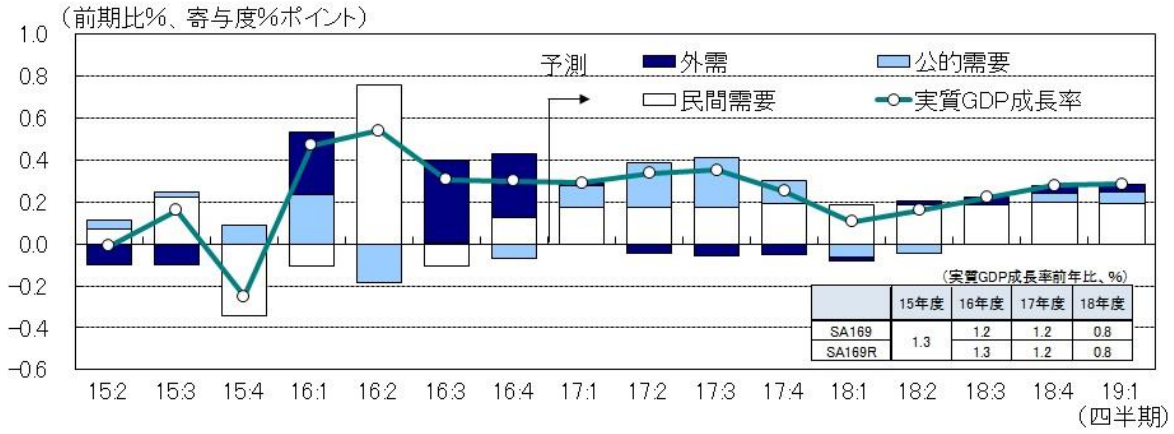
[5] http://www.imf.org/external/datamapper/index.php

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。第 2 の矢の奏功に期待したい処ではあったが 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。また、2016 年に入ってからの急激な円高や海外経済の減速は、このようなアベノミクス効果にブレーキをかける要因となっている。

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。

2016 年春闘では 3 年連続増とはなったものの 14、15 年に比べると賃上げの鈍化が目立った。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に回復したのは 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」



日本経済研究センター第 169 回改訂短期経済予測
（2017 年 1-3 月期～2019 年 1-3 月期）[6]

図 26 は日本経済研究センターが 2017 年 3 月に発表した 4 半期予測である。2015～2016 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、引き続き外需主導での持ち直しであり、内需の伸びは横ばいにとどまるなど、回復の勢いに力強さはない。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

6 https://www.jcer.or.jp/research/short/detail5177.html

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 年度と大幅に回復し、2014 年度は率が下がるものの増益傾向にある。2015 年度は製造業の減益により、-0.6%となった。2016 年度は、若干の回復は見せるもののほぼ横ばいで推移すると予想されている。

表 21　大企業経常利益増減率の推移

大企業の経常利益推移（前年度比増減%）						
2011 年度	2012 年度	2013 年度	2014 年度	2015 年度	2016 年度	2017 年度
-12.1%	12.8%	37.4%	6.9%	-0.6%	0.8%	12.7%

（出所：野村証券企業業績見通し　2016 年 2 月 28 日版[7]）

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。2017 年 3 月調査によれば、表に示すように、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。大企業の業況判断 DI は+16%pt と前回調査(14%pt)から改善を予測している。円安が収益改善に寄与したほか、IT サイクル改善に伴う需要拡大が、電子部品産業などで景況感の回復に繋がったとみられている。先行きは、海外の政治情勢の不透明感が残存しており、慎重姿勢が維持されることから横ばいとなっている。

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
2016 年 12 月	14	13	12	7	2	-3
2017 年 3 月	16	14	15	8	5	-1

（出所：日本銀行　第 172 回 全国企業短期経済観測調査　2017 年 3 月調査[8]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。2015 年度の実績について、大企業の伸び率は小幅に留まっており、中小企業は伸び悩んでいる状況となる。一方 2016 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）は横ばいを見込んでおり、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、2015 年度には 0.4%の増加から 2016 年度見込みは 2.2%増と、若干の持ち直し感が見られる。

[7] http://www.nomuraholdings.com/jp/news/nr/nsc/20170228/20170228.pdf
[8] http://www.boj.or.jp/statistics/tk/gaiyo/2016/tka1703.pdf

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	2015 年度 実績	2016 年度 見込	2017 年度 予測
大企業	政策投資銀行	2016 年 8 月	4.8%	10.9%	5.7%
中小製造業	政策金融公庫	2016 年 10 月	0.0%	0.0%	-
全産業*1	日本銀行	2017 年 3 月	7.1%	1.1%	1.5%
全産業*2			0.4%	2.2%	3.1%
（*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 2016/8 月公表[9]、政策金融公庫中小製造業設備動向調査 2016 年 10 月公表[10]、日本銀行全国企業短期経済観測調査 2017 年 3 月公表[11]を基に JNSA 作成）					

7.2.　企業・組織の IT 支出ビヘイビア

(1) IT 投資サイクル

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

IT 投資に影響を与えるものとしては、システムライフサイクルがあり、これは 2004, 2005 年度に IPA の委託により JUAS（社団法人日本情報システム・ユーザ協会）が調査を行ってまとめた「システム・リファレンス・マニュアル[12]」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。尚、2008 年には「企業 IT 動向調査 2008 報告書[13]」にて、傾向調査が行われているが、大きく変わっていないことを示している。

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。

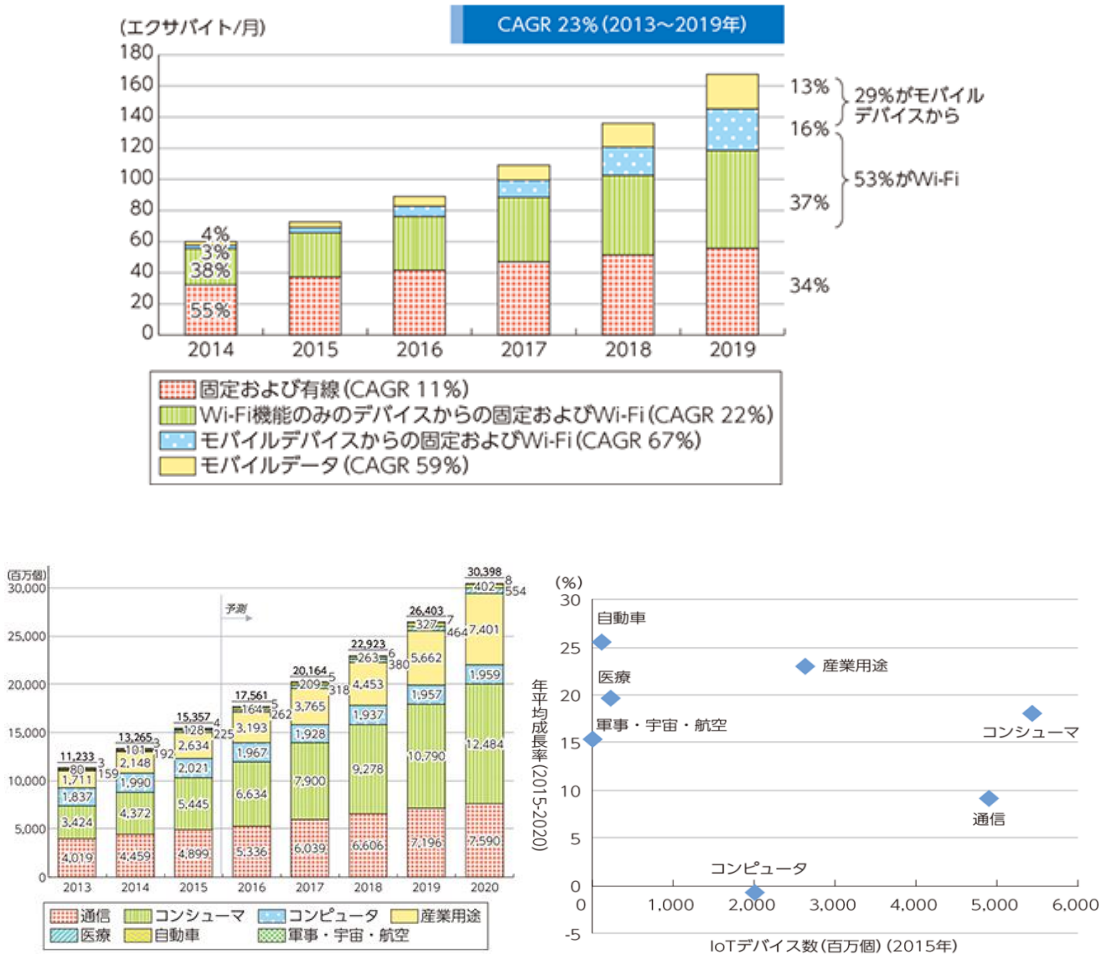
サプライサイドからは、いわゆるムーアの法則が、IT 投資サイクルに大きな影響を与えると考えられる。ハードウェアの性能は概ね 2 年で 2 倍上がる、というものである。ハード性能が上がればソフトウェアはそれを前提とした仕様・機能を盛り込んでくるから、常に最新のアプリケーションを利用しようとすれば 2 年というサイクルが想定される。

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。

9 http://www.dbj.jp/investigate/equip/national/pdf_all/201608_plant.pdf
10 https://www.jfc.go.jp/n/findings/pdf/news281024b.pdf
11 http://www.boj.or.jp/statistics/tk/gaiyo/2016/tka1703.pdf
12 http://www.ipa.go.jp/about/jigyoseika/04fy-pro/chosa/srm/index.pdf
13 http://www.juas.or.jp/cms/media/2017/02/08itdoukou.pdf

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 28 年版[14]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 に見られるように世界のトラフィックは 2014 年～2020 年で約 23%の増加を見込んでいる。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 28 年版 情報通信白書　情報流通量の推移



（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、2015 年時点で 154 億個となっており、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

14 http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27/html/na000000.html

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）[15]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）[16]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、独自 OS Srv 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、2015 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。

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		2014 年度	2015 年度	2016 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	8,428	8,965	9,326
IT 出荷計(JEITA)	金額	67,546	67,102	－
PC 国産出荷	台数	9,187	7,111	－
	金額	7,336	6,239	－
メインフレーム（MF)、サーバ（Srv）独自 OS サーバ	台数	315	320	－
	金額	3,343	3,203	－
ソフトウェア	金額	8,146	7,661	－
SI 開発	金額	29,113	29,344	－
BPO その他サービス	金額	19,608	19,783	－
(SW,サービス計)	金額	56,867	56,788	－
ネットワーク関連機器				
生産	金額	5,287	4,087	－
輸入	金額	6,472	6,478	－
輸出	金額	1,716	1,815	－
国内出荷	金額	5,821	5,121	－
IT+NW 装置	金額	73,367	72,223	－

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

16　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/statistics

セキュリティ市場との比率				
対 IT 出荷計(JEITA)※1		12.4%	13.3%	-
対 IT+NW 装置※2		11.5%	12.4%	-

※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、2014 年度で 11.5%、2015 年度で 12.4%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が、平成 27 年度は調査見直し作業のため調査を実施していない。そのため以下は、昨年の内容を記載する。

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ため、現在公表されている最新の調査は 2014 年版[17]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。

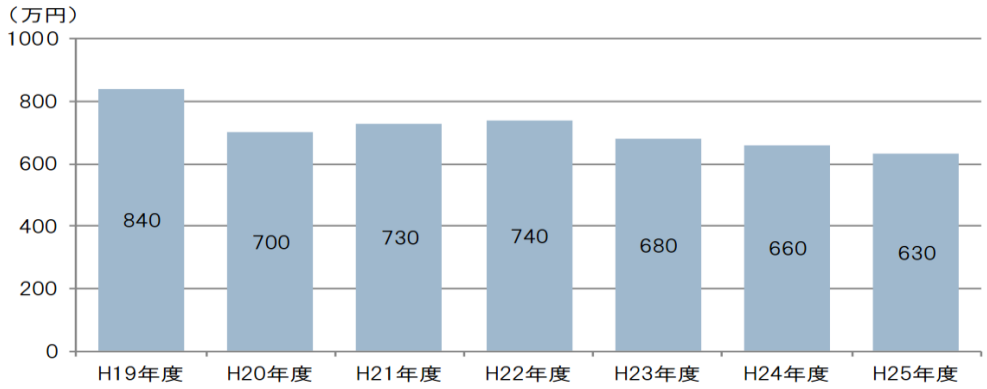


図 28　一社平均情報セキュリティ対策費用

【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)[18]】
(出典：経済産業省平成 26 年度情報処理実態調査より)

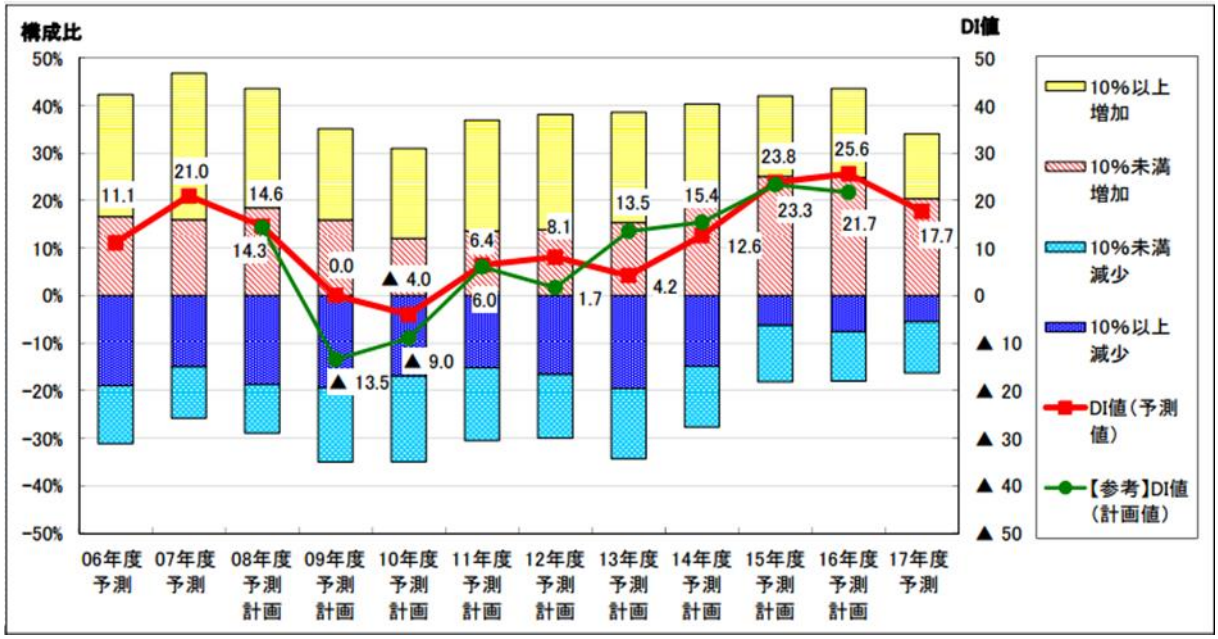
[17] http://www.meti.go.jp/statistics/zyo/zyouhou/result-1.html　(2015 年 6 月 4 日発表)

[18] http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/H26_report.pdf

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。2017 年度調査結果の概要は 2017 年 5 月 10 日にプレスリリースとして公表[19]された。



（出典：JUAS　企業 IT 動向調査 2017 報告プレスリリースより）

図 29　IT 予算の増減調査（2006 年度～2017 年度）

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 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、2013 年度 4.2、2014 年度 12.6、2015 年度 23.8、2016 年度 25.6 となり、IT 投資を積極的に行う傾向から、2017 年度は 17.7 と DI 値の減少が見受けられる。

2016 年度の 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ていたが、頭打ちとなり増加傾向は鈍化している。

セキュリティ対策についてトピック的要素の 2 点について概要報告がされている。

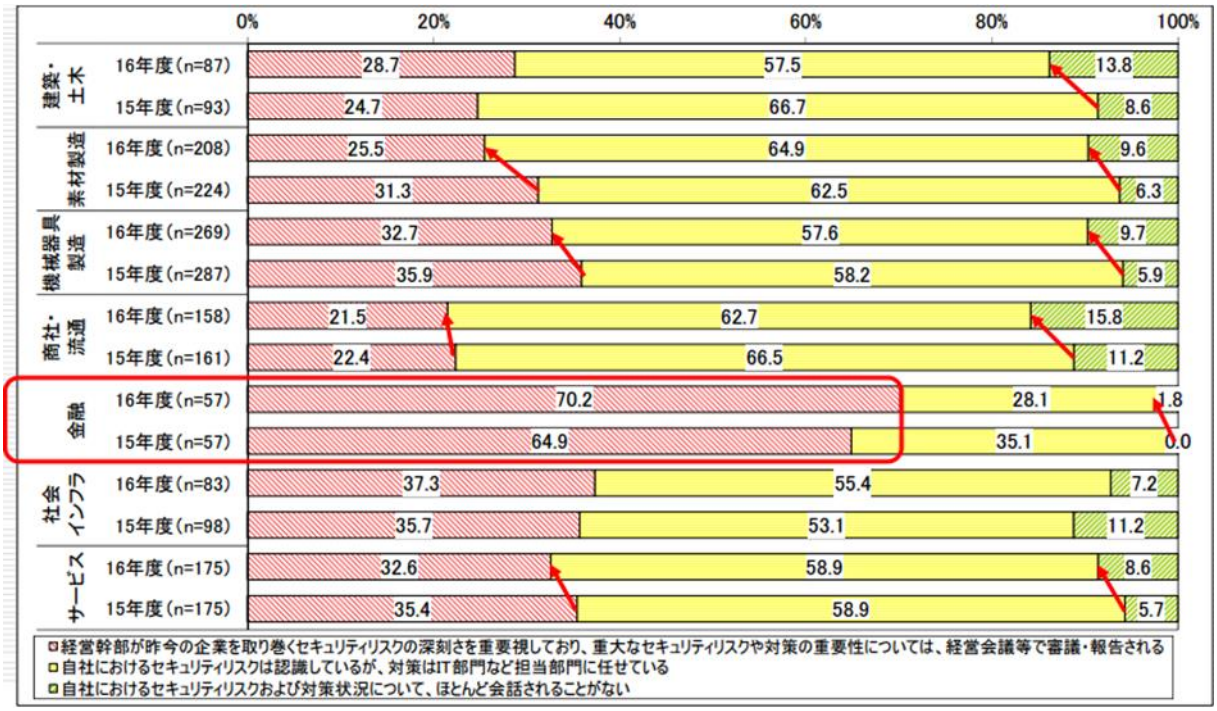
経営幹部の情報セキュリティへの関連度合いに関して、図 30 にあるように業種別でみると金融業界の多くが昨今のセキュリティリスクに対して敏感な反応を見せていると捉えられる。

また、他の業種においては、15 年度から 16 年度にかけてセキュリティに対する関連度の低下が見える中、金融業界の関連度の高まりが注目される。これは経営戦略と IT 戦略が強い企業ほど

[19] http://www.juas.or.jp/cms/media/2017/04/it17_ppt.pdf

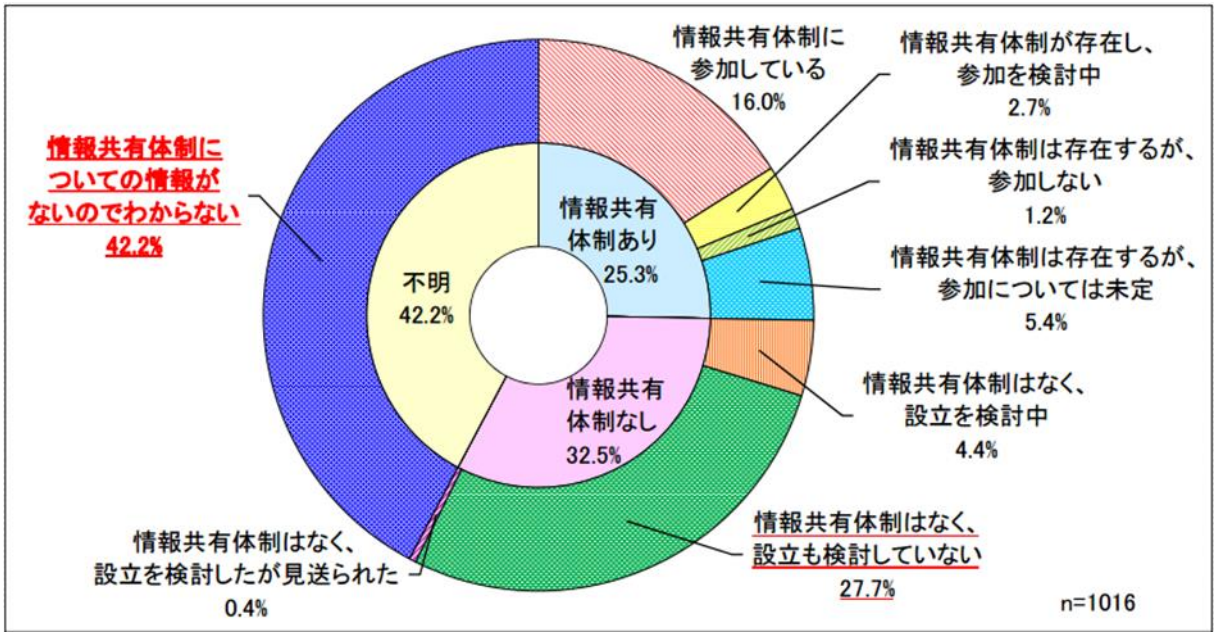
経営幹部が情報セキュリティの確保が重要な課題であると捉えている結果を示している。今後 Iot 等を扱う業種においては、よりセキュリティリスクが高まっていくため、経営幹部の積極的な関与が必要であると考えられる。

図 30　業種グループ別　経営幹部の情報セキュリティへの関連度合い



（出典：JUAS　企業 IT 動向調査 2017 報告プレスリリースより）

もう 1 点のトピックは情報セキュリティに関する「情報共有体制（サイバー情報共有イニシアチブ（J-CSIP)、ISAC、日本シーサート協議会 など)」の存在についてである。図 31 を見ると、約 4 割の企業で認知されておらず、「情報共有体制なし」の企業も 3 割を超えており、約 7 割の企業が情報共有体制を敷いていないことが分かる。サイバー攻撃等の情報を企業間で共有し、対策につなげることの必要性について周知が必要となる。



（出典：JUAS　企業 IT 動向調査 2017 報告プレスリリースより）

図 31　情報セキュリティに関する「情報共有体制」について

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、この数年ほどの間に、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

IPA 発表の『ソフトウェア等の脆弱性関連情報に関する届出状況（2015 年第 4 四半期（10 月～12 月））』によれば、脆弱性の届出件数の累計は 11,494 件（ソフトウェア製品に関するもの 2,376 件、ウェブサイトに関するもの 9,118 件）となっている。なお、届出件数は過去 10 年間、右肩上がりを続けている。CVE Details が製品別にまとめた 2015 年の脆弱性報告件数トップ 50 のリスト「Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2015」によると 1 位は 384 件の Mac OS X、2 位が 375 件の iOS、3 位が 314 件の Adobe Flash Player となっている。

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。

今後、攻撃手法が巧妙化していくなかでの対策として、機械的に検知する方法も考えられるが、脆弱性の試験や、定期的なアップデートなど脆弱性対策を行っていくことが現実的な対策ではないかと考えられる。

(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。
⑥ 被害があった場合の社会的な影響度が高まっている。

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おり、重視する経営課題においては、「情報セキュリティの強化」が上位となっている。

また、2016 年にはマルウェアに感染した IoT 機器からインターネット市場最大とも言われている大規模なサービス停止攻撃（DDOS）が発生しており、今後 IoT が急激に普及する兆しがある中で、セキュリティ課題が顕在化している状況にある。

法制度・政策対応の面では、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、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。その他にも官民連携による人材育成やサイバー攻撃に関する情報共有の取り組みにも力を入れ始めている。

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り、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。2016 年には、国家資格となる「情報処理安全確保支援士」制度を 2016 年度内に新たに創設するとともに、「情報処理安全確保支援士試験」を 2017 年度から実施することを公表している。

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

2015 年に政府が「サイバーセキュリティ」という用語を組織・政策に採用して戦略姿勢を質的に転換させたことに象徴されるように、情報セキュリティは個人情報の保護から軍事手段まで、すべての社会要素に密接不可分の要素となってきた。特定の企業のニッチなビジネス領域であったセキュリティは、今やあらゆる産業が備えなければならない機能要素であり、それに対応して供給サイドも多様化と多角化が進んでいる。

「情報セキュリティ」の呼称で継続的にその状況を追ってきた本調査も、サイバーセキュリティの進化と拡散に対応して対象を拡大してきた。その規模も、調査開始当初の 3000 億円台から、今や 1 兆円に迫るところまで達しており、産業としては、経済の成熟化の中で高成長を続ける新産業の一角と位置付けられるであろう。クラウド、AI、ビッグデータ、IoT といった新パラダイムに基づく IT 産業とはしかし、一線を画す位置にいる。それは、IT、ひいては全産業、さらには国家の経済と安全保障に至るバックボーンを形成し、それらが正しく機能することと外部からの脅威に対抗することを可能にするという任務を負っているからである。新たな付加価値を追求するよりはむしろ、基本的・共通的価値を保護する使命を負っている。

産業の発展と、その発展を支援しリードする政策対応のためには、市場の姿を映し、そのデータを、一定の基準に基づいて継続的に観測する統計の存在が不可欠である。社会的認知がほとんど得られない 2000 年代初頭から、そのテーマに、民間の努力を基本に一貫して取り組んできた本調査は、その意味で現在の日本社会において重要な役割を果たしていると言える。

本報告書が、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、関連する各主体の企画、活動、取組みの参考となり、社会の安全と発展を支える一助となれば幸いである。

修正・改訂履歴

時期・版	対象箇所	修正・改訂内容
2017 年 6 月 14 日 V1.0	―	初版（JNSA 市場調査 WG 校了）
2017 年 6 月 21 日 V1.1	図・表	金額単位の統一、誤記訂正
	44～45 ページ	情報セキュリティ保険市場の本文補足

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（2017 年 5 月 31 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
福岡　かよ子	株式会社インテック
大塩　暁子	SCSK 株式会社
瀬戸口　広樹	サイエンスパーク株式会社
奥井　康文	大日本印刷株式会社
玉川　博之	株式会社 VSN
増田　聖一	三井物産セキュアディレクション株式会社
許　　弘智	株式会社メトロ
蜂巣　悌史	サブスクライバー
森田　翔	サブスクライバー

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）
＜改正個人情報保護法と情報セキュリティの果たすべき役割の変化＞

松本　　泰	セコム株式会社 IS 研究所

以上