

経済産業省委託調査

# 国内情報セキュリティ市場調査

## 調査報告書

平成 17 年 3 月

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

## 目次

1. はじめに	1
2. 調査分析結果の概要	2
2.1. 調査概要	2
2.2. 国内情報セキュリティ市場の実態概要	2
2.3. 海外市場との比較の概要	4
2.4. 国内情報セキュリティ市場の特性概要	4
3. 調査内容	6
4. 調査方法（調査対象、調査実施期間）	7
4.1. データポイントの定義	7
4.2. 市場規模の算出方法	8
4.3. 市場予測の算定方法	8
5. 情報セキュリティ市場及び分類	10
5.1. 情報セキュリティツール市場	10
5.2. 情報セキュリティサービス市場	14
6. 国内情報セキュリティ市場を取り巻く状況及び市場の概要	18
6.1. 市場規模	19
6.2. 市場の沿革	20
6.3. 成長速度	21
6.4. 市場の形成と成長の促進要因	21
6.5. 国内情報セキュリティ市場の特徴点	23
7. 国内情報セキュリティツール市場の分析	26
7.1. 情報セキュリティツール市場の全体概要	26
7.2. 情報セキュリティツール市場のカテゴリ別分析	30
7.2.1. 統合型アプライアンス市場	30
7.2.2. アクセス管理製品市場	32
7.2.3. アクセス制御製品市場	39
7.2.4. システムセキュリティ管理製品市場	44
7.2.5. セキュアコンテンツ管理製品市場	48
7.2.6. 暗号製品市場	53
8. 国内情報セキュリティサービス市場の分析	57
8.1. 情報セキュリティサービス市場の全体概要	57
8.2. 情報セキュリティサービス市場のカテゴリ別分析	63
8.2.1. セキュリティ・コンサルティング市場	63
8.2.2. セキュアシステム構築サービス市場	67
8.2.3. セキュリティ運用・管理サービス市場	71

8.2.4.	セキュリティ教育市場 .....	76
9.	海外情報セキュリティ市場との比較 .....	80
9.1.	世界全体の情報セキュリティ市場（世界情報セキュリティ市場）との比較 .....	80
9.1.1.	世界全体の情報セキュリティ市場の概観 .....	80
9.1.2.	世界の情報セキュリティ市場との全体像比較 .....	82
9.1.3.	世界の情報セキュリティ市場とのツール対サービスの構成比の比較 .....	85
9.1.4.	世界の情報セキュリティ市場とのハード対ソフトの構成比の比較 .....	87
9.2.	世界の各地域の情報セキュリティ市場との比較 .....	88
9.2.1.	世界の地域別情報セキュリティソフトウェア市場との比較 .....	88
9.2.2.	地域別情報セキュリティハードウェア市場との比較 .....	96
9.2.3.	地域別情報セキュリティサービス市場との比較 .....	100
9.3.	韓国情報セキュリティ市場との比較 .....	101
10.	まとめ .....	105
	【付録 1】韓国情報セキュリティ市場調査分析報告 .....	108
●	韓国情報セキュリティハードウェア市場 .....	108
	ファイアウォール・アプライアンス .....	110
	IDS / IPS アプライアンス .....	110
	VPN アプライアンス .....	111
	セキュリティスマートカード .....	111
	生体認証デバイス .....	112
●	韓国情報セキュリティソフトウェア市場 .....	113
	セキュリティ管理ソフトウェア .....	115
	侵入検知ソフトウェア .....	116
	アンチウイルス / アンチスパム・ソフトウェア .....	116
	システム / アプリケーションセキュリティソフトウェア .....	117
	セキュリティ 3A ソフトウェア .....	118
	無線 / モバイルセキュリティ .....	118
●	韓国情報セキュリティサービス市場 .....	119
	韓国認証サービス市場 .....	122
	韓国セキュリティ監視サービス市場 .....	122
	韓国セキュリティコンサルティング市場 .....	123
	韓国セキュリティ運用管理サービス市場 .....	123
	韓国技術供給サービス市場 .....	124
	韓国その他セキュリティーサービス市場 .....	124
	【付録 2】英文字略語に関する簡単な説明 .....	125

## 表目次

表 1	国内情報セキュリティ市場規模 実績と予測 .....	2
表 2	国内情報セキュリティ市場予測の前提条件 .....	9
表 3	情報セキュリティツールの市場分類 .....	12
表 4	情報セキュリティサービス分類 .....	16
表 5	国内情報セキュリティ市場推移 .....	18
表 6	国内情報セキュリティツール市場規模 実績と予測 .....	28
表 7	国内統合型アプライアンス市場規模 実績と予測 .....	31
表 8	国内アクセス管理製品市場規模 実績と予測 .....	36
表 9	国内アクセス制御製品市場規模 実績と予測 .....	42
表 10	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 .....	46
表 11	国内セキュアコンテンツ管理製品市場規模 実績と予測 .....	51
表 12	国内暗号製品市場規模 実績と予測 .....	55
表 13	国内情報セキュリティサービス市場規模 実績と予測 .....	61
表 14	国内セキュリティ・コンサルテーション市場規模 実績と予測 .....	65
表 15	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 .....	69
表 16	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 .....	73
表 17	国内セキュリティ教育市場規模 実績と予測 .....	78
表 18	世界全体の情報セキュリティ市場規模 実績と予測 .....	81
表 19	日本の情報セキュリティ市場規模 実績と予測 .....	83
表 20	本調査の定義と IDC 社定義の比較 .....	86
表 21	日本の情報セキュリティ市場の世界市場に対するシェア .....	87
表 22	日本の IT 市場の世界市場に対するシェア 2004 年 (製品分野別、米ドルによる市場規模比較) .....	87
表 23	世界の IT 市場規模及び各国、地域のシェア、2004 年 (米ドルによる比較) .....	90
表 24	世界の情報セキュリティソフトウェア地域別市場規模 実績と予測 (百万円) .....	91
表 25	世界の情報セキュリティソフトウェア地域別市場シェア 実績と予測 .....	92
表 26	世界の情報セキュリティソフトウェア地域別市場成長率 .....	93
表 27	情報セキュリティソフトウェアに関する本調査の定義と IDC 定義の比較 .....	94
表 28	セキュリティソフトウェア製品分類別の日本市場の対アジア太平洋地域 / 世界シェア .....	94
表 29	日本の情報セキュリティソフトウェア市場規模 実績と予測 (百万円) .....	96
表 30	世界のセキュリティ・アプライアンス 各国、地域別市場規模 実績と予測 (百	

万円) .....	98
表 31 日本のセキュリティ・アライアンス市場規模 実績と予測 (百万円) .....	99
表 32 世界地域別情報セキュリティサービス市場規模 実績と予測 (百万円) ...	101
表 33 韓国情報セキュリティ市場規模 実績と予測 (百万円) .....	104
表 34 韓国情報セキュリティハードウェア市場規模現況 (百万円) .....	108
表 35 韓国情報セキュリティハードウェア市場予測 (百万円) .....	110
表 36 韓国情報セキュリティソフトウェア市場規模実績 (百万円) .....	113
表 37 韓国情報セキュリティソフトウェア市場予測 (百万円) .....	115
表 38 韓国情報セキュリティサービス市場規模実績 (百万円) .....	119
表 39 韓国情報セキュリティサービス市場予測 (百万円) .....	121

## 図目次

図 1	国内情報セキュリティ市場推移.....	19
図 2	国内情報セキュリティツール市場推移.....	29
図 3	国内統合型アプライアンス製品市場推移.....	32
図 4	国内アクセス管理製品市場推移.....	38
図 5	国内アクセス制御製品市場推移.....	44
図 6	国内システムセキュリティ管理製品市場推移.....	47
図 7	国内セキュアコンテンツ管理製品市場推移.....	53
図 8	国内暗号製品市場推移.....	56
図 9	平成 15 年度国内情報セキュリティサービス構成比.....	58
図 10	国内情報セキュリティサービス市場推移.....	62
図 11	国内セキュリティ・コンサルティング市場推移.....	67
図 12	国内セキュアシステム構築サービス市場推移.....	70
図 13	国内セキュリティ運用・管理サービス市場推移.....	75
図 14	国内セキュリティ教育市場推移.....	79
図 15	情報セキュリティ市場、世界市場と日本市場の比較.....	84
図 16	韓国セキュリティハードウェア市場、分野別構成.....	109
図 17	韓国ファイアウォール・アプライアンス予測、2004 年～2009 年（百万円） .....	110
図 18	韓国 IDS / IPS 市場予測（百万円）.....	111
図 19	韓国 VPN アプライアンス市場予測（百万円）.....	111
図 20	韓国セキュリティスマートカード市場予測（百万円）.....	112
図 21	韓国生体認証デバイス市場予測（百万円）.....	113
図 22	韓国情報セキュリティソフトウェア市場構成、2003 年～2004 年.....	114
図 23	韓国セキュリティ管理ソフトウェア市場予測（百万円）.....	115
図 24	韓国 IDS / IPS ソフトウェア市場予測（百万円）.....	116
図 25	韓国アンチウイルス / アンチスパム市場予測（百万円）.....	117
図 26	韓国システム / アプリケーションセキュリティ市場予測（百万円）.....	117
図 27	韓国セキュリティ 3A ソフトウェア市場予測（百万円）.....	118
図 28	韓国無線 / モバイルセキュリティ市場予測（百万円）.....	119
図 29	韓国情報セキュリティサービス構成.....	120
図 30	韓国認証サービス市場予測（百万円）.....	122
図 31	韓国セキュリティ監視サービス市場予測（百万円）.....	122
図 32	韓国セキュリティコンサルティング市場予測（百万円）.....	123

図 33	韓国セキュリティ運用管理サービス市場予測（百万円） .....	123
図 34	韓国技術供給サービス市場予測（百万円） .....	124
図 35	韓国その他セキュリティサービス市場予測（百万円） .....	124

## 1. はじめに

ウイルス・ワームの被害頻発や、スパム、フィッシングといったネットワーク脅威の拡大が認識され、また個人情報保護法の全面施行を前に情報管理に対する企業の責任が改めて意識されるようになったことから、情報セキュリティ対策への関心は急速に高まっている。これに対して、情報セキュリティ対策のためのツール、システム、サービスの提供も活発化し、既に一つの産業としての形成を見たと言ってよい。

そのような中、供給サイドについての統計的データの収集は、一部に民間企業からの調査報告書の上梓があるものの限られた供給であり、ベンダーサイドの事業計画や新規参入の企画において、あるいは産業政策、ひいては情報セキュリティ政策立案の面において包括的な調査が期待されるところ大であった。

このような状況を背景として、NPO 日本ネットワークセキュリティ協会(JNSA)では、経済産業省からの委託により、「国内情報セキュリティ市場実態調査」を実施した。

本調査は、情報セキュリティ産業の実態を把握し、我が国における情報セキュリティの普及度と到達度を明らかにするための基礎データの提供を目的とする。それにより、経済産業省における情報セキュリティ基盤整備事業の基礎資料として活用されることを期待するとともに、同事業の一層の充足と充実が望まれるところから、それに向けての課題を整理する上で、参考となれば幸いである。

以下にその結果を報告する。

## 2. 調査分析結果の概要

### 2.1. 調査概要

本調査は、平成 17(2005)年 2 月～3 月に実施した、国内情報セキュリティ販売事業者に対するアンケート調査をベースに、官民の各種統計や分析資料ならびに国内事業者へのヒアリング結果を加味して、国内情報セキュリティ市場の市場規模実績並びに予測数字を導き出した。併せて、対象とした市場区分に関する解説と分析を加え、限られた範囲ではあるが国際比較を行った。

### 2.2. 国内情報セキュリティ市場の実態概要

表 1 に国内情報セキュリティ市場の推定結果を示す。

**表 1 国内情報セキュリティ市場規模 実績と予測**

	金額（百万円）			構成比			対前年度比 成長率	
	平成 15 年度	平成 16 年度	平成 17 年度	平成 15 年 度	平成 16 年 度	平成 17 年 度	平成 16 年 度	平成 17 年 度
<b>情報セキュリティツール市場</b>				34.9%	32.7%	33.2%		
統合型アプライアンス	883	4,089	7,296	0.7%	2.8%	4.3%	363%	78.4%
アクセス管理製品	34,412	39,108	45,584	27.3%	26.9%	27.0%	13.6%	16.6%
アクセス制御製品	36,428	37,612	40,751	28.9%	25.9%	24.2%	3.3%	8.3%
システムセキュリティ管理製品	5,259	9,449	11,450	4.2%	6.5%	6.8%	79.7%	21.2%
セキュアコンテンツ管理製品	45,418	50,781	58,671	36.1%	34.9%	34.8%	11.8%	15.5%
暗号製品	3,565	4,289	4,893	2.8%	3.0%	2.9%	20.3%	14.1%
情報セキュリティツール合計	125,964	145,328	168,645	100.0%	100.0%	100.0%	15.4%	16.0%
<b>情報セキュリティサービス市場</b>				65.1%	67.3%	66.8%		
セキュリティ・コンサルテーション	18,409	28,923	35,523	7.8%	9.7%	10.5%	57.1%	22.8%
セキュアシステム構築サービス	177,491	217,485	242,820	75.6%	72.9%	71.7%	22.5%	11.6%
セキュリティ運用・管理サービス	33,874	42,953	48,609	14.4%	14.4%	14.4%	26.8%	13.2%
セキュリティ教育	4,912	9,088	11,658	2.1%	3.0%	3.4%	85.0%	28.3%
情報セキュリティサービス合計	234,686	298,448	338,611	100.0%	100.0%	100.0%	27.2%	13.5%
<b>情報セキュリティ市場合計</b>	<b>360,650</b>	<b>443,776</b>	<b>507,256</b>	<b>100.0%</b>	<b>100.0%</b>	<b>100.0%</b>	<b>23.0%</b>	<b>14.3%</b>

平成 15(2003)年度の国内情報セキュリティ市場規模の実績値は、「情報セキュリティツール」（アプライアンスとソフトウェア）が 1,260 億円、「情報セキュリティサービス」が 2,347 億円、合計で 3,607 億円であったと推定される。

平成 16(2004)年度の市場規模予測は、「情報セキュリティツール」が 1,453 億円（対前年度比成長率 15.4%）、「情報セキュリティサービス」2,984 億円（同 27.2%）合計 4,438 億円（同 23.0%）という結果となったが、ほぼ実績見込みレベルの数字として算出した。平

成 17(2005)年度はそれぞれ 1,686 億円(対前年度比成長率 16.0%)、3,386 億円(同 13.5%)となり、合計では 5,073 億円(同 14.3%)と、初めて 5,000 億円に達するものと予測される。

「情報セキュリティツール」市場では、アンチウイルス、アンチスパイウェアなどを含む「セキュアコンテンツ管理製品」(平成 15(2003)年度の「情報セキュリティツール」合計に対する構成比 36.1%)、個人認証製品、ログオン管理製品などを含む「アクセス管理製品」(同 27.3%)、ファイアウォール、VPN、IDS/IPS 製品を含む「アクセス制御製品」(同 28.9%)の 3 分野が既に確立した市場となっている。このうち「アクセス制御製品」は「統合型アプライアンス」へのシフトの影響と見られる伸び率の鈍化が見られるが、他の 2 カテゴリーはほぼツール市場全体と同程度の伸びを続け、「情報セキュリティツール」市場を構成する主要セグメントの位置を維持する。ポリシー管理やセキュリティイベント管理などの「システムセキュリティ管理製品」、「統合型アプライアンス」などは、平成 15(2003)年度の市場規模はそれぞれ 53 億円(同 4.2%)、8.8 億円(同 0.7%)と小さい。しかし、「システムセキュリティ管理製品」は平成 16(2004)年度は前年度比 79.7%伸びて 94 億円に達し、平成 17(2005)年度も 21.2%と高い伸びを維持して 115 億円に達する見通しである。また「統合型アプライアンス」は平成 16(2004)年度が本格立ち上り期と見られ、4.6 倍の 41 億円に急拡大し、平成 17(2005)年度も 78.4%増と拡大を続けて 73 億円に達すると予測される。

「情報セキュリティサービス」市場は、その 70%以上を「セキュアシステム構築サービス」が占めるといってやや偏在的な市場構造を持つ。「セキュアシステム構築サービス」は平成 15(2003)年度で 1,775 億円(平成 15(2003)年度の「情報セキュリティサービス」合計に対する構成比 75.6%)に達し、そのうちでも「IT セキュリティシステムの導入・導入支援」セグメント単独で 1,006 億円を占める。これは情報セキュリティに関する SI サービスに位置するもので、IT 産業における、ハード・ソフトの合計と同程度以上のコストがインテグレーション(統合構築)サービスに必要であるという特徴的な構造がセキュリティにも反映した結果と考えられる。このカテゴリは平成 16(2004)年度に対前年度比成長率 22.5%、平成 17(2005)年度も同 11.6%と順調な伸びを見せるが、「情報セキュリティサービス」市場は他のカテゴリの伸びが著しく、「情報セキュリティサービス」全体に占めるセキュアシステム構築サービスの構成比は平成 16(2004)年度 72.9%、平成 17(2005)年度 71.7%と徐々に下がる。次に大きなウェイトを占めるのが「セキュリティ運用・管理サービス」で、平成 15(2003)年度の市場規模は 339 億円(平成 15(2003)年度の「情報セキュリティサービス」合計に対する構成比 14.4%)であった。このカテゴリはサービス市場全体とほぼ同様の伸びを見せ、平成 16(2004)年度、平成 17(2005)年度は各 430 億円、486 億円で「情報セキュリティサービス」合計に対する構成比は両年度とも 14.4%と予測される。「セキュリティ・コンサルテーション」は平成 15(2003)年度 184 億円で平成 15(2003)年度の「情報セキュリティサービス」合計に対する構成比の 7.8%を占めたが対前年度比成長率は平成 16(2004)年度 57.1%、平成 17(2005)年度 22.8%と高い伸びを続け、平成 17(2005)年度には 355 億円

(平成 17(2005)年度の「情報セキュリティサービス」合計に対する構成比 10.5%) に達すると予測される。これは、個人情報保護法の全面施行を控えて企業の情報セキュリティ対策が本格化し、専門家のコンサルテーションを積極的に活用した結果であると見られ、その流れは平成 17(2005)年度も継続するものと見る。同様に市場が急拡大する動きを見せているのが「セキュリティ教育」である。平成 15(2003)年度の市場規模が 49 億円とかなり小さい分野ではあるが、対前年度比成長率は平成 16(2004)年度 85.0%、平成 17(2005)年度 28.3%と最も高い伸び率を見せ、平成 17(2005)年度には 117 億円に達すると予測する。

### 2.3. 海外市場との比較の概要

世界の情報セキュリティ市場に関する統計データは、米国 IDC 社の調査報告を採用して比較を行ったが、同報告と本調査の金額対比では、日本は世界市場の 13~14%程度を占めるとの結果になった。IT 市場全体では、通常日本は世界の 10 分の 1 と言われるところと比べると相当高い比率となる。これは、ツールとサービスの構成比で日本はサービスの比率が極めて高いことによると見られ、日本における、特に「IT セキュリティシステムの導入・導入支援」の突出が、日本の特殊要因 (IT システムの導入・構築におけるシステムインテグレーション=SI=依存度の高さ) もしくは対象市場の定義の差によって影響を与えていると判断される。

市場の伸び率に関しては、日本が平成 16(2004)年度に高く、平成 17(2005)年度に落ちるという年度による変動を示している一方で、世界市場は一定した伸び率を見せるものの、平成 15(2003)年度を基点とする 2 年間の平均伸び率ではそれほど差がなく、むしろ世界市場が日本を若干上回る関係となっている。北米はやや成熟に近づき、西欧が堅調に伸びる中で、アジア太平洋地域の伸び率は、北米や西欧に比べて高いものになっている。

なお、今回調査では、韓国についても情報収集と分析を行った。公表された 2 種類の統計から本調査と対照できる形で数字を整理した結果では、市場規模は平成 15(2003)年度が 569 億円と日本の 16%、平成 17(2005)年度予測は 760 億円と同 15%となった。

### 2.4. 国内情報セキュリティ市場の特性概要

本調査を通じて、国内の情報セキュリティ市場について得られた観測の要点は、次のようにまとめられる。

1. 国内情報セキュリティ市場規模は製品とサービスを合せて平成 15(2003)年度時点で 3,600 億円に達し、近年中に 5,000 億円規模を達成すると見られること。
2. その成長率は年率 20%近く、日本経済の成長率や IT 投資の伸び率に比べても著しく高い伸び率を維持すると見られ、急速な拡大が続いていること。
3. 製品とサービスの比率では概ね「製品」:「サービス」が 1:2 となり、IT 全体の構造と基本的に一致していることが確認できたこと。
4. 市場規模の割に、特に製品分類が細分化され、単独の市場規模はかなり小さい

こと。また技術革新が早いいため新領域の出現や製品の更新代謝も極めて早いこと。

5. 世界的にも市場の拡大速度は速く、市場構造は先進国偏在型と見られること。ただし、アジア太平洋地域の市場の成長率は高まっており、新興経済国・地域の存在感が増してきていること。
6. 本調査は平成 17(2005)年 4 月の個人情報保護法施行直前の時期にあたったため、市場の変局点の状況を捉えることができたこと。特に法制度への対応という経営レベルでの課題が、情報セキュリティのコンサルテーションや教育といったサービスの需要に集中的に向かい、市場としての確立を促したと見られること。
7. 市場の細分化とも関連して、市場カテゴリ毎の参入企業の数必ずしも多くななく、かつ海外メーカーが国内市場に占める位置が大きいこと。
8. その結果、技術面、製品供給面での海外依存度が高く、セグメントが細分化されて事業規模が限られる等、国内産業存立基盤が貧弱で、産業育成策が課題となると思われること。

### 3. 調査内容

本調査の対象は国内情報セキュリティ市場であり、それを供給側からの数字の調査を中心にして、サンプルから全体像を推測するというアプローチを行っている。具体的には、情報セキュリティ製品及び情報セキュリティサービスの提供者へのアンケート調査で得られた、ベンダー段階での出荷額のデータをベースにして、各種統計データ、ベンダーへのヒアリング調査、更には市場調査経験者のノウハウを活かして様々な影響要素を定量化するアプローチを加え、推定市場規模を導き出した。

その結果を、平成 15(2003)年度における情報セキュリティ製品及び情報セキュリティサービスの分野別市場規模推定結果と平成 16(2004)年度と平成 17(2005)年度の市場予測、また市場実態の分析結果として報告するものであり、以下の項目を含む。

- 平成 15(2003)年度国内情報セキュリティツール市場規模実績推定
- 平成 16(2004)年度、平成 17(2005)年度国内情報セキュリティツール市場規模予測
- 平成 15(2003)年度国内情報セキュリティサービス市場規模実績推定
- 平成 16(2004)年度、平成 17(2005)年度国内情報セキュリティサービス市場規模予測
- 海外市場との比較による国内市場の特性分析
  - 世界市場との比較
  - 北米、西欧、アジア太平洋各地域との比較
  - 韓国との比較

#### 4. 調査方法（調査対象、調査実施期間）

本調査では、以下の情報源を基に経験則等を援用して市場規模を推定するアプローチを行った。

##### 情報セキュリティベンダーに対するアンケート調査

平成 17(2005)年 2 月から 3 月にかけて、国内で情報セキュリティツールを販売、あるいは情報セキュリティサービスを提供するベンダー延べ 320 社（ツール、サービスの重複を除く実数で 266 社）に対して、アンケート調査を実施し、市場規模算定に関する基礎資料とした。

対象ベンダーのリストアップに際しては、NPO 日本ネットワークセキュリティ協会の会員を始めとして国内で情報セキュリティビジネスを展開する企業全てを網羅するよう心がけた。そのうち、情報セキュリティツールについては国産のものはそのメーカー、海外製品についてはそのメーカーの日本法人か支店、もしくは一次代理店の位置にあって国内に製品を提供している業態を対象にした。サービスについては情報セキュリティ関連のサービスに特化した企業その他、システムインテグレータにおいて情報セキュリティに関するサービスを提供する事業者も全て含むようにした。

なお、アンケートの回収件数は情報セキュリティツール、情報セキュリティサービス合わせて 62 社、76 件であり、回収率は 23.8%となる。また、アンケートで回答された数値の単純集計値は、本調査の最終予測結果に対して約 11%を占めている。

##### 各種統計調査資料

国内の事業所、産業、投資などに関する政府及びその関連機関、ならびに民間企業による調査結果を補足資料として参照した。

##### 参入事業者へのヒアリング

参入事業者のうち、情報セキュリティ事業担当者へのヒアリング調査を実施した。

#### 4.1. データポイントの定義

データのポイントとしては、ベンダー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。つまり、ベンダーの出し値レベルでの市場規模を計算している。サービスについても、サービスの提供事業者からの提供価格に基づく集計となる。対象としては後に示すサービスの定義に該当するサービスの範囲となる。

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、その部分の売上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。

#### 4.2. 市場規模の算出方法

今回調査では、ベンダーに対するアンケート調査で得られた承継数値をそのまま市場規模数字とすることは妥当性に欠けると判断した。ベンダーに対する網羅性・市場捕捉率の問題が一つあり、製品分類と製品定義が、業界として一貫したものとして確立していない関係上、ある程度の誤差を見込まざるを得ない問題が次にあり、更に、ベンダーサイドの情報開示方針の関係で全てのデータが詳らかに開示される訳ではないという問題もある。これらを捨象して得られたままのデータだけに依存することは現実から乖離した数値を提示することになり、議論を誤った方向に導く結果となる恐れが強い。

そこで、複数の情報源を活用し、調査分析に参加した分析者の経験や識見を援用することにより市場実態に近いと推測されるものを導き出すこととした。以下に、市場規模、予測を調査結果からどのように導き出したかを述べる。

##### ステップ1：ベンダーアンケートによる市場規模の積上げ

平成 17(2005)年 2 月～3 月に実施したベンダーアンケートを基に市場規模を積上げ。

##### ステップ2：市場規模算定モデルの構築

ベンダーアンケートを基に国内流通経路の構造を把握し、流通段階での重複計上要素を排除すると共に、提供形態の要素を加味して国内市場モデルを構築。

##### ステップ3：国内市場規模算定

上記モデルを基に国内事業者、ユーザ動向を加味して国内市場全体の規模を算定。

#### 4.3. 市場予測の算定方法

平成 16(2004)年度、平成 17(2005)年度の市場規模推定にあたっては、平成 15(2003)年度の市場規模実績推定値を基に、アンケートによって得られたベンダーの業績予想と下記に示すマクロな経済、技術条件などを勘案し、予測を立てている。

表 2 は、国内情報セキュリティ市場を予測するにあたっての前提条件の記述である。

表 2 国内情報セキュリティ市場予測の前提条件

大項目	小項目	前提条件	前提条件成立の確度*	当該市場への影響の強さ
経済全般の状況	国内経済の状況	景況の回復は平成 16 年度、17 年度も持続する。	4	中
セキュリティに対する脅威の顕在化	セキュリティ・インシデントの発生状況	大規模なセキュリティ・インシデントが発生することで、セキュリティ対策に対する認知度、優先度が高まる。	3	強
製品・サービスの開発	製品の向上	ベンダー間の競争により、製品の機能性能の向上が続く。	4	強
	サービス提供の拡大	セキュリティベンダー以外からのセキュリティサービス提供が拡大する。	4	中
法的規制	個人情報保護法	個人情報保護法への対応投資が平成 17 年までは持続する。	5	強
	新たな法規制の影響	欧米の法令に対応する形で、セキュリティに関する新規の法令が制定される。	3	中
	海外の法規制の影響	米国や欧州の法規制に対応する必要性がグローバル企業を中心に高まる。	4	中
ソリューションの変化	統合ソリューション	ポイントソリューションから統合ソリューションに基軸が移る。	3	中
	アプライアンス	セキュリティ・アプライアンスへの選好が強まる。	4	強
	アウトソーシング	セキュリティ管理のアウトソーシングが進展する。	3	強

\* 前提条件成立の確度：5（非常に高い）から、1（非常に低い）までの5段階評価

## 5. 情報セキュリティ市場及び分類

今回情報セキュリティの市場規模をベンダー側の数字を基に算出するに際して、市場の定義として、「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。以下、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ぶ。

「ツール」と言ってもその多くはソフトウェア製品もしくはシステム製品であり、有形物でない場合もあるが、ビジネスモデル的には単価と数量により定義が可能で商品的に取引され流通する形態のものが中心である。また、「サービス」は個別的に、多くは供給者と需要者の相対取引で提供され消費されるビジネスモデルを、主として想定している。これらは下記の市場分類における定義内容からも読み取っていただけるものと思う。

なお、小分類レベルになると、例えばファイアウォールで言えばパケットフィルタリング型かアプリケーションゲートウェイ型かその併用型か、といった区分になるし、生体認証デバイス（装置・機器）では指紋か指の静脈パターンか手のひらの静脈パターンか、といった区分を導入することになる。個別事業の評価や事業企画のためには必要な分類レベルであるが、このレベルではメーカー名や機種名と市場数値との対応関係が相当直接化して元データの保護が困難になる等の弊害の他に、データの把握や予測における精度の問題もあり、予測や分析をいたずらに煩雑にして全体像を見えにくくする恐れもある。従って、本調査では中分類レベルまでの予測と分析にとどめている。

以下、二つの情報セキュリティ市場の定義、分類内容について述べる。

### 5.1. 情報セキュリティツール市場

「ツール」については、ハードウェアとソフトウェアの両方を含むものとし、製品・商品化されて販売されているものを対象とした。製品カテゴリとしては「統合型アプライアンス」、「アクセス管理製品」、「アクセス制御製品」、「システムセキュリティ管理製品」、「セキュアコンテンツ管理製品」、「暗号製品」の6区分とした。

#### 1. 統合型アプライアンス

「統合型アプライアンス」は、ハードウェアとソフトウェアを一体化して一つの製品として販売する製品形態として位置付けられる「アプライアンス」製品の中で、二つ以上のカテゴリにまたがる機能を複数統合して一つのアプライアンス上を実現する製品が増えていることに対応して定義した。従来からファイアウォールとVPNゲートウェイを一体で実現する製品は、アプライアンスであれソフトウェア製品であれ多く見られたが、近年これに留まらず不正侵入監視やウイルス監視機能を併設し、1台でほとんどの防御機能を実現する製品が登場してきている。このため単純に特定機

能分類に仕分けすることができず、またこれをコンパクトなハードと一体化して提供するという特徴に注目して単一カテゴリとして定義することとした。

## 2. アクセス管理製品

「アクセス管理製品」は、情報システムやネットワークに対してユーザがアクセスする際に、本人であることを認証し、そのユーザに与えられた権限の範囲内で情報資源にアクセスさせることを保証する一連の製品である。各種認証デバイス（装置・機器）、アイデンティティ管理システム、ディレクトリ管理システム、PKI 関連システム、シングルサインオンシステムなどがこのカテゴリに含まれる。

## 3. アクセス制御製品

「アクセス制御製品」は、主として外部からの不正な侵入、アクセスを防ぐファイアウォール、VPN（Virtual Private Network 仮想私設通信網）、IDS / IPS（Intrusion Detection System 不正侵入検知システム、Intrusion Prevention System 不正侵入防御システム）の3種類の製品分類を含む。

このうちファイアウォールは内外のネットワークの境界において、あらかじめ設定されたルールに従って通信をチェックし、ルールに沿ったもの以外の通信を遮断したり、制限したりする機能を提供する。これに対してIDSは、たとえ許可された通信であっても、それが不正な通信パターンやネットワーク攻撃に特有の特徴を含む通信である場合にはそれを検知し、警報を発したり記録を保全したりする機能がある。IPSは、そのようなケースにおいて自動的に通信を遮断したり制限したりする機能を併せ持った製品と定義できる。

## 4. システムセキュリティ管理製品

「システムセキュリティ管理製品」とは、主にシステム全体のセキュリティ情報を監視して統合管理と統計処理を行い、その結果を統合表示したり、アラート（警報・警告）を出したりする製品である。システム全体に関して、ある判断基準に従いチェックを行い、ポリシーへの準拠性を確認する製品（いわゆる脆弱性検査製品やコンプライアンス管理製品）等が含まれる。

これらの製品が登場した背景には、ネットワークの防御がファイアウォールに象徴されるような「点」の守りだけでは十分でなく、複数のポイントにおける情報から統合的かつ一元管理しなければならないという問題意識がある。特に、最近頻発する情報漏えいの教訓からネットワーク内部の管理・監視も不可欠であるという観点、更にはネットワーク全体のセキュリティレベルの維持にはポリシーレベルでの一貫性をもった統合管理が不可欠であるという観点に基づく問題意識を背景に需要を伸ばしている。

ネットワークの主要資源を一元管理する思想はネットワーク統合管理プラットフォームのアーキテクチャには以前から取り込まれていたが、セキュリティに着目し、かつ単にセキュリティ・インシデント（事件・事故・事案）だけでなく状態管理も含めた考え方が普及して来たのは最近である。

#### 5. セキュアコンテンツ管理製品

このカテゴリは、ネットワークを介して伝播するウイルス、ワーム、スパイウェアなどの悪意あるプログラムを検知、排除するソフトウェア、アプライアンス製品、いわゆるアンチウイルス製品、スパムメールやフィッシングに対するコントロール（管理・制御）やフィルタリング（選別）を行う製品、メールの内容をチェックしたりログ（動作記録）を取ったりして情報漏えい等を防止する製品、更には有害ウェブサイト等特定の情報源（リソース）へのアクセスをデータの内容を検査して防ぐ製品等、ファイルやメールや通信の内容に対するチェックやコントロールを提供する製品のグループである。

#### 6. 暗号製品

暗号技術そのものは、PKI、VPNの基幹技術を構成する他、各種情報セキュリティ製品の内部処理等に広範に使われている。ここではPKI、VPNはその使用目的から各々アクセス管理製品、アクセス制御製品に分類しており、データの保護等を目的とする製品を中心に定義している。具体的にはメールやデータを暗号化するソフトウェア、及び暗号化のためのライブラリやモジュールなどが含まれる。

表3に「情報セキュリティツール」の市場区分と中分類レベルでの製品の定義一覧を示す。

**表 3 情報セキュリティツールの市場分類**

大分類	中分類	定義
統合型アプライアンス	統合型アプライアンス	アンチウイルス・アンチワーム（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2つ以上の機能を装備したアプライアンス製品。ただし、FWとVPNだけの組合せはファイアウォール・アプライアンスに含める。
	その他統合型アプライアンス	上記条件以外の統合型アプライアンス。
アクセス管理製品	個人認証用ワンタイムパスワード製品	同一アルゴリズムを持つ乱数発生機能を認証サーバ側と被認証端末側にもち、その結果の一致をもって端末の本人真正性を確認して認証するシステム。
	個人認証用ICカードシステム	あらかじめ資格認定して交付したICカードに格納した特定の情報に基づき本人確認・認証するシステム。

	個人認証用 USB キーシステム	USB キーに格納した情報とパソコン側またはネットワーク上の認証サーバ側の情報の照合により本人確認・認証するシステム。
	個人認証用生体認証デバイス/システム	指紋、虹彩パターン、静脈パターン等、生体を持つ唯一性の高い、かつ複製の困難な情報を元に本人確認・認証を行うシステム。
	ログオン管理 / アクセス許可製品	本人確認情報を元に、あらかじめ設定された、その本人がアクセスできるネットワーク資源・コンピュータ資源へのアクセスをコントロール（管理・制御）するシステム製品。ディレクトリ管理やシングルサインオンといった製品が含まれる。
	PKI システム及びそのコンポーネント	暗号技術を応用して電子的に本人を特定する複製・解読不可能な電子証明書を発行し真正性を保証するシステム。
	その他のアクセス管理製品	その他ユーザからシステム等へのアクセスを管理する製品で上記に含まれないもの。
アクセス制御製品	ファイアウォール・アプライアンス	ネットワークゲートウェイに設置され、特定の通信の通過阻止や制限を行うアプライアンス。VPN 機能を併設するものを含む。
	ファイアウォール・ソフトウェア（企業向けライセンスタイプ）	ネットワークゲートウェイのサーバにインストールされ、特定の通信の通過阻止や制限を行うソフトウェア。VPN 機能を併設するものを含む。
	ファイアウォール・ソフトウェア（デスクトップ・ファイアウォール）	クライアントマシンにインストールされ、特定の通信の通過阻止や制限を行うソフトウェア。クライアント用アンチウイルス機能を併設するものはアンチウイルスの分類となる。パーソナル・ファイアウォール、クライアント・ファイアウォール等の呼び方もある。
	VPN ソフトウェア	VPN（Virtual Private Network 仮想私設通信網）を提供するソフトウェア。ファイアウォール機能併設型はファイアウォールに分類される。
	VPN アプライアンス	VPN（仮想私設網）を提供するアプライアンス。ファイアウォール機能併設型はファイアウォールに分類される。
	IDS / IPS アプライアンス	ネットワークシステムへの不正侵入を検知、防御するアプライアンス製品。
	IDS / IPS ソフトウェア	ネットワークシステムへの不正侵入を検知、防御する機能を持つソフトウェア。
	その他のアクセス制御製品	その他アクセス制御機能を主とするソフトウェアで上記に含まれないもの。
システムセキュリティ管理製品	セキュリティ情報管理システム / 製品	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。
	脆弱性検査製品	システムに脆弱性が存在しないかの検査・分析を行う製品。
	ポリシー違反管理製品	セキュリティポリシーに反するアクセス権その他のシステムの設定やバージョンアップの不備等を検出して警告・報告する機能を持つ製品。
	その他のシステムセキュリティ管理製品	上記に属さないセキュリティ管理に関わる製品。

セキュアコンテンツ管理製品	アンチウイルス・アンチワーム・ソフトウェア	アンチウイルス・ワーム、アンチスパイウェアなどの機能を持つ企業向けライセンスタイプのソフトウェア。ゲートウェイ型、サーバ型、クライアント型の全てを含む
	アンチウイルス・アンチワーム・ソフトウェア・パッケージ	アンチウイルス・ワーム、アンチスパイウェアなどの機能を持つ個人ユーザ向けパッケージタイプ。ファイアウォール・IDS 機能併設型を含む。シュリンクラップ形式の箱売り形態で流通するものが中心だが、ネットワーク経由のダウンロード販売も含む。
	アンチスパム・ソフトウェア/アプライアンス	アンチスパムの機能を持つソフトウェア。アンチウイルスソフトウェアにこの機能が併設される場合は、アンチウイルスの分類となる。
	URL フィルタリング・ソフトウェア/アプライアンス	特定の URL へのアクセスを制限する機能を持つソフトウェア。アンチウイルスソフトウェアにこの機能が併設される場合は、アンチウイルスの分類となる。
	アンチフィッシング・ソフトウェア/アプライアンス	金融機関などになりすまし、個人の銀行口座やクレジットカードなどの情報を不正に入手する詐欺行為（フィッシング、Phishing）からの防御機能を持つソフトウェアとアプライアンス。アンチウイルスソフトウェアにこの機能が併設される場合は、アンチウイルスの分類となる。
	メールフィルタリング・ソフトウェア	電子メールに不適切な内容がないか、また機密情報が電子メールを経由して流出していないかといったことを電子メールの内容に踏み込んで検査し、送信を防いだり、送信のログを収集するソフトウェア。アンチウイルスソフトウェアにこの機能が併設される場合は、アンチウイルスの分類となる。
	その他のセキュアコンテンツ管理製品	通信された情報の内容を解析し、セキュリティ上の障害を防止、記録するソフトウェアの内、上記に含まれないもの。
暗号製品	メール暗号化製品	電子メールのメッセージを暗号化する製品。
	ファイル暗号化製品	ファイルの内容を暗号化する製品。
	暗号化ミドルウェア	通信やファイルの暗号化機能をモジュール、ライブラリ等で提供する製品。
	ファイル/データアクセス管理製品	ファイルやデータに対するアクセス許可、コピー・印刷制御等の機能を持つ製品。
	その他の暗号製品	その他暗号化を主たる機能とするソフトウェアの内、上記に含まれないもの。

## 5.2. 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」市場には、情報セキュリティソリューションを具現化するために提供される各種サービスが含まれる。

本調査では、情報セキュリティサービスとして、国内サービスプロバイダー（サービス提供事業者）から提供されているものを対象とした。カテゴリとしては、「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」,「セキュリティ教育」の4区分とした。

#### 1. セキュリティ・コンサルティング

情報セキュリティに関するポリシー、システム、運用体制及び各種セキュリティ規格認証の取得支援に関するコンサルティングである。この分野は、ITコンサルティングの中でも技術的な専門性が高く、確立した分野であるが、最近では企業のコンプライアンス（法令・ルール遵守）重視の立場から、情報セキュリティ認証制度など客観的な資格要件の取得を目指す企業が増加している。それに対応して、その認証取得を支援するサービスも様々な事業者から提供され、増加傾向にある。逆にこうした資格を審査し、認証するサービスもまた、公的機関に限らず、民間事業者から提供されている。この、認証を提供する側のサービスもこの分野に含んでいる。

#### 2. セキュアシステム構築サービス

セキュアシステム構築サービスは、実際にセキュアなシステムを構築する段階で必要となるサービスであり、ITセキュリティシステム的设计、仕様策定といった上流工程から、ソフトウェアの開発、カスタマイズ（個別対応改造）、セキュリティソフトウェア及びハードウェアの選定、導入、設定などのサービスが含まれる。

#### 3. セキュリティ運用・管理サービス

セキュリティ運用・管理サービスは、導入済のセキュリティシステムの全体あるいは一部の管理運用を、外部事業者が事業所内に常駐し、あるいは事業所外から遠隔操作によって代行するサービスが中心で、その対象はシステムの総合監視、ファイアウォール監視、IPD / IPS 監視、ウイルス監視等がある。この他にネットワークの攻撃に対する弱点を検査する脆弱性検査サービス、セキュリティ情報提供サービス等の予防的サービスや、PKI、VPN といったシステム運用に関連する特定のサービスもこのカテゴリに含めた。

#### 4. セキュリティ教育

セキュリティ教育には、企業などの情報システム、情報セキュリティ担当者など専門家への技術的な教育と、経営者や一般社員などに対する情報セキュリティのポリシーや運用に関する教育の二つが含まれる。こうしたサービスは情報セキュリティ製品やサービスのプロバイダー（提供事業者）や、教育を専門とする事業者から提供されている。

表 4 に情報セキュリティサービスの市場区分と中分類レベルでのサービスの定義一覧を示す。

表 4 情報セキュリティサービス分類

大分類	中分類	定義
セキュリティ・コンサルティング	セキュリティポリシー構築支援	セキュリティポリシー策定のためのコンサルティングサービス。
	セキュリティ運用管理全般のコンサルティング	セキュリティの運用管理に関する一般的・総合的なコンサルティングサービス。
	セキュリティ監査サービス	セキュリティに関わるポリシー、システム、管理体制、コンプライアンス(法令・ルール遵守)状態等を外部監査するサービス。
	セキュリティ診断サービス	セキュリティの運用体制、管理体制の安全性などに関する診断サービス。
	セキュリティ認証取得支援サービス	ISMS、プライバシーマークなどのセキュリティ認証を取得するためのコンサルティングサービス。
	セキュリティ認証・審査機関(サービス)	ISMS、プライバシーマークなどのセキュリティ規格適合の認証サービス。
	その他のセキュリティ・コンサルティング	上記に属さないセキュリティ関連コンサルティングサービス。
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の設計・仕様策定	IT セキュリティシステムの設計や仕様策定を行うサービス。
	IT セキュリティシステムの導入・導入支援	ITセキュリティツールやシステムの導入・実装またはその支援サービス。
	セキュリティ製品の選定・導入支援	セキュリティ製品の選定及びその支援サービス。
	その他のセキュアシステム構築サービス	上記に属さないセキュアシステムの構築に関わるサービス。
セキュリティ運用・管理サービス	セキュリティ総合監視・運用支援サービス	専用センサまたは複数のファイアウォール、IDS、IPS等の情報を総合的に監視してネットワークシステムのセキュリティを総合的に監視し、運用をサポートするサービス。ログ解析サービスを含む。
	ウイルス監視・フィルタリングサービス	ウイルスの監視とフィルタリングを提供するサービス。ISPがメール配信に際して提供するタイプ、ウイルス監視ソフトを遠隔地または現地で運用するサービスの3タイプがある。
	IDS/IPS監視・運用支援サービス	IDS/IPSの監視、運用を代行するサービス。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	ファイアウォールの監視及び運用を代行するサービス。ログ解析サービスを含む。
	脆弱性検査サービス	ITシステム検査、侵入検査等、技術的弱点を検査し指摘するサービス。
	セキュリティ情報提供サービス	セキュリティシステム、セキュリティ・インシデント、OS等の脆弱性などに関する情報提供サービス。
	電子認証サービス	PKI証明書の発行・認証、無改竄保証、否認防止、タイムスタンプ証明等のサービス。

	インターネット VPN サービス	インターネット VPN の提供サービス。
	その他の運用・管理サービス	上記に属さないセキュリティ運用管理サービス。
セキュリティ教育	セキュリティ教育コンテンツの提供	セキュリティ教育コンテンツ(情報の内容)の販売もしくはライセンス提供。
	セキュリティ教育実施	セキュリティに関する集合教育・実地教育・演習等。
	セキュリティ教育 ASP サービス	セキュリティに関する教育をリモート型・eラーニングサービス等で提供するサービス。
	その他のセキュリティ教育サービス	IT セキュリティに関わる教育サービスまたはコンテンツの提供のうち、上記以外の形式で提供されるもの。

## 6. 国内情報セキュリティ市場を取り巻く状況及び市場の概要

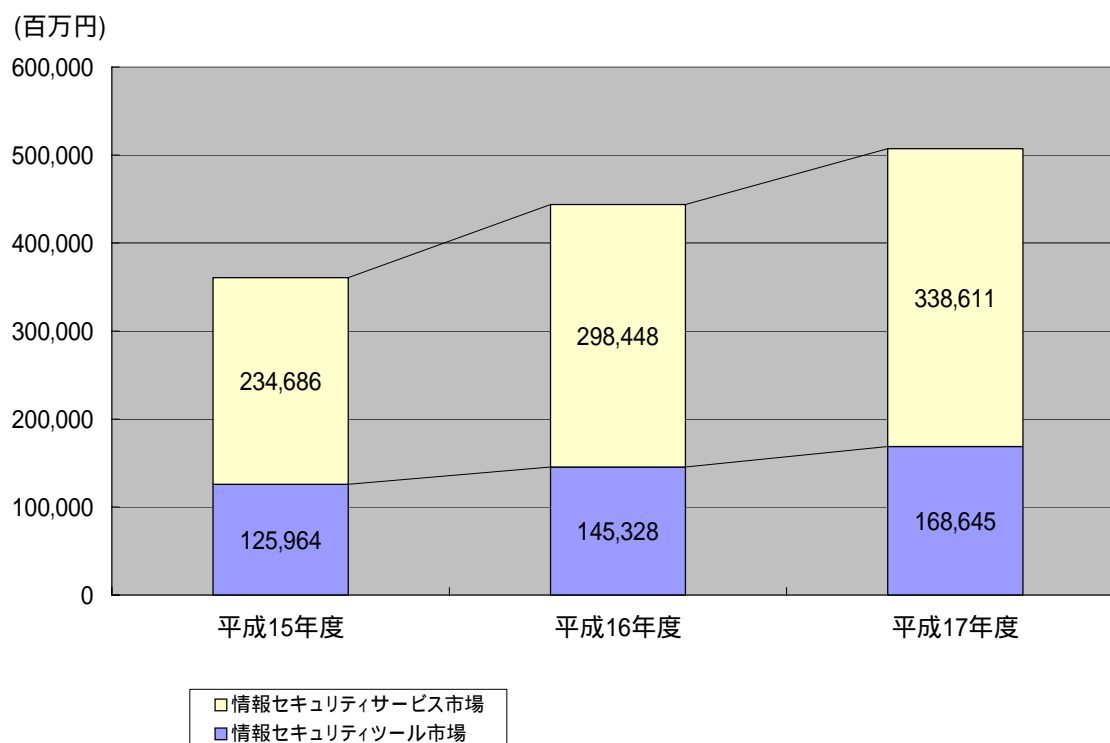
4章で説明した調査・予測方法により導き出した国内情報セキュリティ市場の概要は以下の通りである。

国内情報セキュリティ市場の推定金額規模は、表5に示す通り、ベンダー売上ベースで、平成15(2003)年度が3,607億円、平成16(2004)年度が4,438億円、平成17(2005)年度が5,073億円となった。

表5 国内情報セキュリティ市場推移

市場規模(百万円)	平成15年度	平成16年度	平成17年度
情報セキュリティツール市場	125,964	145,328	168,645
情報セキュリティサービス市場	234,686	298,448	338,611
情報セキュリティ市場 計	360,650	443,776	507,256
<b>成長率</b>			
情報セキュリティツール市場		15.4%	16.0%
情報セキュリティサービス市場		27.2%	13.5%
情報セキュリティ市場 計		23.0%	14.3%

図 1 国内情報セキュリティ市場推移



### 6.1. 市場規模

国内情報セキュリティ市場はツール、サービスを合わせて平成 15(2003)年度実績として約 3,600 億円程度の規模と推定される。これが年平均成長率 20%近い高成長を 2 年続けることで、平成 17(2005)年度には 5,000 億円規模に達するとの予測結果となった。

これを IT 自体の投資規模との関連で見ると、SI 関連の市場統計との比較を試みる。社団法人電子情報技術産業協会 (JEITA) の公表する「平成 16 年度ソリューションサービスに関する調査報告書」<sup>1</sup>によれば、平成 15(2003)年度のソフトウェアサービスの売上は 5 兆 2,417 億円 (うち SI 開発 2 兆 3,514 億円、ソフトウェア 7,911 億円、アウトソーシング・その他サービス 2 兆 992 億円) である。同調査は参考として同年度におけるハードウェアの出荷額も併載しているが、総額 2 兆 5,596 億円 (うちメインフレーム 2,625 億円、サーバ 5,313 億円、ワークステーション 494 億円、パソコン 1 兆 7,164 億円) となっており、合計すると 7 兆 8,013 億円に達する。情報セキュリティの 3,607 億円はその約 4.6%に相当する。ここ数年行われている内外の各種調査から、一般に IT セキュリティ投資は IT 投資全体に対して数パーセント (調査により概ね 1%から 7%程度の範囲にばらつく) を占めるものと見られているが、本調査を JEITA の数字と比較する限りでは、この一般に言われて

<sup>1</sup> 社団法人電子情報技術産業協会「平成 16 年度ソリューションサービスに関する調査報告書 概要」(05-計-2)

いる範囲の中間に近いところに該当すると言える。また、同調査では、上記数字にも見られるように、IT 投資におけるハード対ソフトの比率が 1 : 2 であると指摘している。本調査では、ソフトウェアツールを搭載すべきハードウェア(ほとんどが PC または UNIX / Linux サーバ) はカウントしていないので単純な比較はできないが、ツールとツール以外のサービス(約 7 割を SI 的要素が占める)の比率がそれに近いものになっていることは興味深い。

また産業としての規模感を得るために参考データとして IT 関連の機械統計月報を参照すると、平成 16(2004)年の出荷額ベースで、集積回路が約 3 兆 6,000 億円で約 10 倍、複写機を中心とする事務用機械がほぼ情報セキュリティ市場と同額の 3,770 億円であり、情報セキュリティ業界も全体では事務用機械と肩を並べる産業規模となってきたと言える。

## 6.2. 市場の沿革

情報システムにおけるセキュリティ対策は、メインフレームを中心とするいわゆるレガシーシステムの時代には、それ自身が独立したカテゴリとして取り扱われることはなかった。コンピュータシステム自体の中にセキュリティ対策の機能や手順が盛り込まれ、個別システムの構築に際しても仕様・設計の段階からシステムと一体のものとして組み込まれるのが通常であった。また、オープンアーキテクチャやオープンネットワークという構造がないために、情報セキュリティの対象領域も限られたものであり、その対象とする事象も限定的な範囲で済んでいたのである。

その後 1980 年代から UNIX、DOS、更には Windows が普及し IP ベースのオープンネットワークが一般化してきた。また高速データ通信手段の多様化と低価格化、末端個人ユーザまでの普及という通信環境の革新が進む中で、企業内ユーザであれ個人であれ、パソコンとインターネット接続が当り前の環境がごく短時間のうちに実現してしまった。その成果は二つのことを意味した。一つは、個人のパソコンが、そして企業の社内 LAN やそこに収容されるパソコン端末が、ほとんど無防備で不特定多数が行き交う往来に放り出されるのと同じ状態にさらされるようになったこと。そしてもう一つは、システムはその使用上の安全対策をあらかじめ組み込んだものではなく、それはユーザなり管理者なりが後付けで用意しなければならないものになった、ということである。

このことにより、ネットワークセキュリティやシステムのセキュリティを独立の機能として用意する必要が生じ、そのための技術が開発され、ツールとして商品化されてきた。また、それらを選定し組み込み使いこなすため、あるいは運用保守のためのサービスも生まれ供給されるようになった。これらツールやサービスが市場として形成され始めてから高々 10 年程度の歴史であるが、それが国内だけで 3,000 億円から 5,000 億円の規模の市場となり産業となったことは大きな意味を持つと考えられる。

### 6.3. 成長速度

もう一つ特筆すべきこととして、この産業の成長率の高さが挙げられる。今回調査により得られた数字の範囲では、平成 16(2004)年度において前年度比 23.0%、平成 17(2005)年度において同 14.3%、平均で 18.6%という、高い成長率を示している。デフレ・低成長下の日本経済の中では、IT 産業は比較的順調に成長を続ける分野ではあるが、その中でもこの数字は、薄型テレビやデジタルカメラ等の一部 IT 消費財を別とすれば、例外的な高成長率である。

前述のように、情報セキュリティが独立した市場として形成されだしてからの経過年数は高々 10 年強程度と考えられる。初期の市場規模がどの程度であったのか、スタート時点をとどこに取るべきかは特定が難しい要素であるが、例えば 10 年で 100 倍となるためには毎年倍近い伸びが必要である。後述するように、ある種の製品やサービスは、その立ち上り時期には前年比何倍増というスピードで普及が進むことがある。ネットワークセキュリティは技術革新が一段と激しい世界であり、次々と新しい技術・製品が登場することで市場形成を促進し成長を維持・加速してきた。そのような積み重ねが高い成長率を維持して市場規模を短時間に拡大する原動力となったものと分析できる。

このように見ると、今も年率 20%近い成長を続けていることも理解できるし、この高成長は今後しばらく続く可能性もあると考えることもできよう。

### 6.4. 市場の形成と成長の促進要因

報道媒体における取扱いの頻度の高まり、特に一般のニュースでしばしば取り扱われるようになってきたことや、各種セミナーや展示会の開催頻度とその集客数の伸び、企業社会のトピックとして一般化してきたこと、等の要素を総合的に見ると、やはり平成 15(2003)年度から平成 16(2004)年度あたりに市場の変局点があるように見られる。そのことが、前述したように高い成長率になって現れていると推測される。

その背景としては、下に述べるようないくつかの要因が作用しているものと推測される。

#### 1. セキュリティ・インシデントの増加

ウイルス・ワームの種類急増、特に亜種の多様化と、出現・発生頻度が近年急速に高まっている。独立行政法人情報処理推進機構（IPA）への届出状況の統計によれば、平成 15(2003)年で 1 万 7,425 件、平成 16(2004)年で 5 万 2,151 件に上っており<sup>2</sup>、その報道に接する機会や、実際にウイルス対策ソフトによる検知、あるいは不幸にして感染するケースが増え続けている。

これらのことが、企業の情報セキュリティ実務担当者あるいは情報セキュリティ対策責任者の意識を喚起し、対策導入を積極化させている。対策内容についても、より総合的な防御対策や、単なるガードから監視・管理へといった高度化が

<sup>2</sup> 独立行政法人情報処理推進機構「コンピュータウイルス・不正アクセスの届出状況について」2005 年 1 月 6 日  
<http://www.ipa.go.jp/security/txt/2005/01outline.html>

進んでいる。

## 2. 脆弱性情報の取扱い・対応体制の整備

ウイルス・ワームの頻発・蔓延を許す一因ともなっている OS やアプリケーションの脆弱性発現頻度が高まっており、世界的にその対策について関心と懸念が持たれている。また情報漏えいにつながりやすいウェブ・アプリケーションの脆弱性も増大しており、その潜在的脅威は日々大きくなっていると言っても言い過ぎではない。

これに対応するために経済産業省ではコンピュータセキュリティ早期警戒パートナーシップという枠組みを作って平成 16(2004)年 7 月から運用を開始した。現在、独立行政法人情報処理推進機構( IPA )を届出機関、有限責任中間法人 JPCERT コーディネーションセンター( JPCERT/CC )を調整機関として運用されており、JNSA はじめ IT 関連の民間業界団体がパートナーシップに参加している。

このような動きも企業や公共団体などでネットワークの脅威とその対策に対する意識を高め、情報セキュリティ対策の導入につながっているのではないかと推測される。

## 3. 情報漏えい事件の頻発と深刻化

平成 15(2003)年から 16(2004)年にかけて、コンビニエンスストアやインターネットプロバイダーといった一般個人消費者と密接に結びついている業態で個人情報の大量漏えいが発覚する事件が相次いだ。また、これらの事件は、漏えいした情報の主体である個人に対して金銭的補償を行い、その支払総額が多額のものに上ることで企業業績に深刻な影響をもたらした。このことは、企業関係者に衝撃を与えた。1999 年に発生した自治体での情報漏えい事件では、直接の当事者であるシステム請負業者だけでなく情報の管理責任者である自治体自体の責任を認定すると同時に、情報価値を 1 件当たり 1 万円(更に訴訟費用として 5,000 円を上乗せ)という高額な被害認定がなされたことでも注目された。

情報漏えい事件の報道は後を絶たず、本来は取り締りや指導すべき立場にある警察や官公庁でも頻発するなど世間の関心を一気に高めるものとなった。これにより企業の情報セキュリティ意識は急速に高まり、次に述べる個人情報保護法の全面施行を控えて対策が急速に浸透する駆動力となったと言える。

## 4. 個人情報保護法の成立と全面施行

個人情報保護法は平成 15(2003)年 5 月に成立し、平成 17(2005)年 4 月 1 日からの全面施行に伴い民間企業も全て法規制の対象とされるようになった。

この法律は個人情報の取扱いに関する企業の保護対策を義務付けるもので、企業の情報セキュリティへの関心を一気に高めるものとなった。このため、企業ではその体制作りの一環として ISMS 認証取得やプライバシーマークの認定取得に取り組んだり、自社の対策を、法の指定する人的、組織的、物理的、技術的対策

の4側面から点検する動きが広範に見られた。

これらの動きが特に情報セキュリティサービスへの需要となり、更には対策ツールの導入につながるといった循環が起きたことが観測されている。

#### 5. 経済情勢と企業業績の好転

バブル経済と信用構造の崩壊で長く低迷の底にあった日本経済も、不良債権処理が強権発動的に急速に進んだことをきっかけに、また企業サイドでの長年の構造改革への取り組みが実を結ぶ段階に入ったことなどで、平成16(2004)年初頭には明るい日差しが見え出していた。このことが、上に述べた様々な後押し要因と相俟って、企業に情報セキュリティ対策への投資を促した面も大きかったと推測される。

情報セキュリティ対策はその業績貢献効果が直接には捉えられず、投資や対策費用投入の優先順位が後回しになる傾向があるが、業績・景況の好転に伴って後順位の案件にまで資金が回って来たとも捉えられる。

#### 6.5. 国内情報セキュリティ市場の特徴点

以上の分析を踏まえつつ、ここでは、今回調査の結果得られたデータに関して、総括的な視点からいくつかの特徴を抽出し分析することとする。

##### 1. 「情報セキュリティツール」市場と「情報セキュリティサービス」市場

情報セキュリティ市場のツール対サービスの構成比率は、調査対象とした3年間で多少変動はあるものの、概ね1:2の割合となっている。「情報セキュリティサービス」市場は「情報セキュリティツール」市場に比べてほぼ倍の市場規模とすることができる。

この比率をもたらず要素は「情報セキュリティサービス」市場の中に占める「セキュアシステム構築サービス」のカテゴリの規模の大きさにある。その中でも「ITセキュリティシステムの導入・導入支援サービス」という単一のセグメントが例外的と言っても過言でない大きさを持っているからである。このセグメントは「情報セキュリティサービス」市場全体に対してほぼ4割前後、情報セキュリティ市場全体に対しても4分の1強を占めており、これを除くとツールとサービスの市場規模はかなり近接してくる。

この「ITセキュリティシステムの導入・導入支援」サービスとは、いわゆるSI、システムインテグレーションと言われるカテゴリである。つまり、セキュリティツールの設置、インストール(コンピュータへの組み込み)、設定、立ち上げ、チューニング(調整)といったサービスを意味する。逆に言えば、ITシステムのインテグレーションのうち、セキュリティに関する部分を切り出したもの、とも言える。

その意味するところは、「通常のシステムインテグレータが行う作業のうちセ

セキュリティ部分を切り出して統計に加えるところという数字です」ということであり、必ずしも IT セキュリティに特化したベンダーの提供するものではないということである。

情報セキュリティのためのツールやサービスの多くが、その専門の企業によるものであったり、あるいは情報セキュリティを主たる事業対象としてビジネスを行う事業部によるものであったりするのに比べると、この言わば「セキュリティ SI」は提供主体が異なる。従って、供給サイドとしては外すことのできない要素であるのは間違いないが、ベンダーサイドを一括していわゆる「業界」的に捉える場合には、その規模感や構成要素・構成比を若干注意して見る必要がある。

## 2. 市場の成長

市場の伸びは「情報セキュリティサービス」が平成 16(2004)年度に約 27%とかなり高い伸びが見込まれるのを除くと概ね年率 15%前後の伸びが持続すると見られる。これは IT 投資の動向に照らしても高い伸びを示しており、IT 投資が平成 15(2003)年度、平成 16(2004)年度と低い伸びに留まった中で情報セキュリティへの重点的な投資が起こったことを示すものとして注目される。

平成 16(2004)年度は「情報セキュリティサービス」市場の中分類レベルのセグメントでほとんどが高い伸びを示している。特に、平成 15(2003)年度に約 184 億円とそれなりの規模に達しているセキュリティ・コンサルティングが、57%と高い伸びで 289 億円にまで規模を膨らませている。相次ぐインシデントに、個人情報保護法など法規制の具体化が後押しをする形で、情報セキュリティに関しては専門家の力を頼るべきという判断が浸透しつつあるものと分析できる。

繰り返しになるが、全体として情報セキュリティ投資はここ当面高い市場の伸び率を維持する見込みで、世間の関心や興味、あるいは漠然とした懸念といったものが、法的、社会的、経済的要因によって具体的投資となって顕在化している過程と見ることができるのではないか。

## 3. 情報セキュリティ事業のビジネスモデルと産業構造

今回調査対象とした企業は、国内で情報セキュリティのツールまたはサービスを提供する企業合計 266 社を対象とした。平成 15(2003)年度の推定市場規模は 3,607 億円なので、単純計算をすれば、1 社平均の売上高規模は 13.6 億円となる。全てが情報セキュリティ専門ではなく、むしろ兼業の事業者の方が多い状態ではあるが、1 社当りの情報セキュリティの事業規模が 14 億円に満たないというのはどちらかと言うと零細な業態と言わざるを得ない。

また、情報セキュリティ製品の圧倒的多くが海外からの輸入品であることも大きな特徴である。特に、ウイルス対策製品やファイアウォール、IDS / IPS 製品等は国産品が皆無に近い状態である。海外製品も、圧倒的に米国企業のものが多い。この理由はいくつか挙げられる。

- 1) インターネット技術が米国を中心に発達して技術の中心が今も米国にあること。
- 2) 米国における豊富なベンチャーキャピタルとその育成（インキュベーション）機能が、多くの情報セキュリティベンダーを支援し、情報セキュリティ製品の開発と供給を支えていること。ちなみに米国の情報セキュリティベンダーの多くが専業であり、ベンチャー型企業である。
- 3) 情報セキュリティの市場規模が極めて限られるため、米国のような大市場でないと限界規模に達せず、事業が成立しにくいこと。また米国とヨーロッパの市場の近さも米国企業に有利に働く。ちなみに、米国に次いで情報セキュリティベンダーが多いのがヨーロッパであり、軍事技術の先進地であるイスラエルも比較的多くの情報セキュリティベンダーを擁する。

情報セキュリティサービスベンダーについては、企業規模は様々である。システムインテグレーション（SI）の一環として情報セキュリティ対策についても一元的に提供する、大手汎用機系ならびに独立系のシステムインテグレータは例外的に超大規模企業が含まれる。またセキュリティ・コンサルティングは大手監査法人系のコンサルティング会社が手がけることもある。管理・運用サービスは大手や中堅の通信事業者がネットワーク管理と平行して提供するケースも多い。それ以外は専業のサービス事業者によるものが多く、ここでも経営基盤という意味で厳しい環境にあると言える。

このことは、ごく一部の特定のサービス領域以外の市場分野では、限られた市場規模の中に比較的規模の小さい専門特化企業がひしめいて事業を営んでいるという実態を示唆しているのではないかと推測される。つまり情報セキュリティ業界とは比較的単独事業で規模の小さい企業により形成されていると言っても過言ではなさそうである。

#### 4. 産業政策上の課題

これは産業の存立基盤を考えた時に重大な意味を持つ。一つ目は、技術面、製品の供給面では米国を始めとする海外の技術と資本に依存する要素が強いこと。二つ目は、国内市場構造が大手 SI ベンダーと弱小専業ベンダーの二極化傾向にあり、弱小ベンダーが競争上厳しい立場にあると想定されることである。そして上に見たように、専業ベンダーは一般的に事業規模が限られることから経営基盤が弱く、技術開発や先行投資、社員の育成といった面で十分な取り組みができない恐れが強いことである。

情報セキュリティが IT 立国、e-Japan、u-Japan 政策の中核の一翼を担うことと照らし合せると、政策面での産業対策の役割と課題は大きいと言えるのではないか。

## 7. 国内情報セキュリティツール市場の分析

### 7.1. 情報セキュリティツール市場の全体概要

表 6 より、平成 15(2003)年度の国内「情報セキュリティツール」市場は、1,260 億円の規模であったと推測される。

本調査では「情報セキュリティツール」市場を、その機能に着目していくつかの製品カテゴリに分類している。大分類レベルで、「統合型アプライアンス」、「アクセス管理製品」、「アクセス制御製品」、「システムセキュリティ管理製品」、「セキュアコンテンツ管理製品」、「暗号製品」の 6 カテゴリに分けた。各カテゴリの定義・内容は第 5 章に詳述した通りである。

この分類において最大のカテゴリは「セキュアコンテンツ管理製品」で、平成 15(2003)年度には約 454 億円、構成比にして全体の 36.1%を占めた。これに続くのが「アクセス制御製品」と「アクセス管理製品」で、各々364 億円・構成比 28.9%、344 億円・構成比 27.3%とほぼ同規模である。これら 3 カテゴリで「情報セキュリティツール」市場全体の 90%以上を占める。このカテゴリにはウイルス対策製品、ファイアウォール、個人認証製品が含まれている。これら 3 製品カテゴリは、NPO 日本ネットワークセキュリティ協会が 2005 年 2 月に発表した「IT セキュリティ対策施策の導入・実施状況とその満足度調査」報告書<sup>3</sup>でも 90%以上の導入率が確認されているほど普及の進んだセグメントであり、ベンダー側の数字でもそれが裏付けられる結果となった。

平成 16(2004)年度の国内「情報セキュリティツール」市場は、対前年比 15.4%増の 1,453 億円規模と予測される。この内大きな伸びを示すのが、「統合型アプライアンス」、「システムセキュリティ管理製品」、「暗号製品」の分類である。

特に「統合型アプライアンス」については、平成 15(2003)年度比で 4.6 倍と大幅な伸びを見せた。平成 15(2003)年度が市場の立ち上り期で市場規模が極端に小さかったのが、平成 16(2004)年度になって、前年度から市場に投入されていた製品がようやく市場に浸透するようになり、特に管理者のいない中堅中小企業向け市場及び大企業の地方拠点向けなどに受け入れられ始めている。このセグメントについては、平成 17(2005)年度も更に市場規模の大幅な拡大が見込まれる。

「システムセキュリティ管理製品」については、従来統制なく導入されてきた各種情報セキュリティ製品の、統合管理化によるセキュリティレベルの向上と管理性の向上を目指す動きが背景にある。これに加えて、企業レベルでのリスクマネジメントの重視といった姿勢が更に市場拡大を牽引したものと考えられる。こうした傾向は平成 17(2005)年度においても、一層強まると考えられるため高い成長率が維持されるものと見られる。

「暗号製品」に関しては、情報漏えい対策や、個人情報保護法への対応から情報の保護

<sup>3</sup> [http://www.jnsa.org/active/2004/active2004\\_15a.html](http://www.jnsa.org/active/2004/active2004_15a.html)

に市場の意識が向いて来た結果、平成 16(2004)年度に相当高い伸びを示したものと考えられる。このため、平成 16(2004)年度と比較すると平成 17(2005)年度は伸び率が若干鈍化するものと予測される。

逆に「アクセス制御製品」は伸び率が低くなっており、これは市場の成熟化と統合型アプライアンスへの需要のシフトが要因と推測される。

国内「情報セキュリティツール」市場全体としては、平成 17(2005)年度に対前年度比 16.0%の市場の伸びが見込まれ、市場規模は推定 1,700 億円に達する。カテゴリ別には、「統合型アプライアンス」が引き続き 78%増と高い伸びを維持するほか、「システムセキュリティ管理製品」も 21%と、平均より高い伸びが見込まれる。いずれも市場の立ち上がりから製品の浸透する時期に当たっていることが要因であると考えられる。

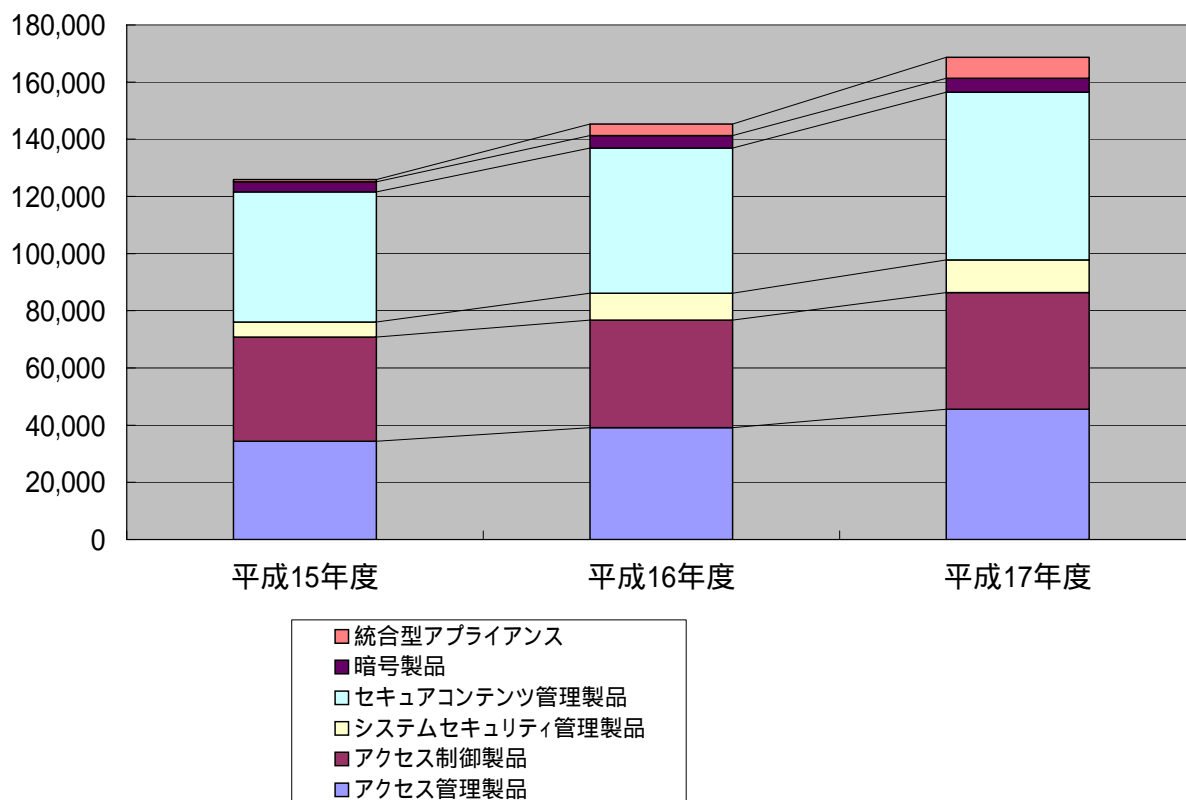
そのほかのカテゴリも全体としては順調な伸びを見せ、市場全体としては平成 16(2004)年度よりは安定した成長となると見られる。特に「セキュアコンテンツ管理製品」、「アクセス管理製品」といった、市場規模も大きく普及率も高いカテゴリが比較的高い成長を見せることが注目される。これは平成 16(2004)年度が需要側（情報保護対策を中心に統合的セキュリティ対策を強化）・供給側（統合型アプライアンスの本格投入）それぞれの要因で市場構造に変動が生じたのが、平成 17(2005)年度は巡航速度に戻る方向に動くことによるものと分析する。

表 6 国内情報セキュリティツール市場規模 実績と予測

製品別出荷金額（百万円）	平成 15 年度	平成 16 年度	平成 17 年度
統合型アプライアンス	883	4,089	7,296
アクセス管理製品	34,412	39,108	45,584
アクセス制御製品	36,428	37,612	40,751
システムセキュリティ管理製品	5,259	9,449	11,450
セキュアコンテンツ管理製品	45,418	50,781	58,671
暗号製品	3,565	4,289	4,893
合計	125,964	145,328	168,645
<b>製品別構成比</b>			
統合型アプライアンス	0.7%	2.8%	4.3%
アクセス管理製品	27.3%	26.9%	27.0%
アクセス制御製品	28.9%	25.9%	24.2%
システムセキュリティ管理製品	4.2%	6.5%	6.8%
セキュアコンテンツ管理製品	36.1%	34.9%	34.8%
暗号製品	2.8%	3.0%	2.9%
合計	100.0%	100.0%	100.0%
<b>対前年度比成長率</b>			
統合型アプライアンス	-	363.2%	78.4%
アクセス管理製品	-	13.6%	16.6%
アクセス制御製品	-	3.3%	8.3%
システムセキュリティ管理製品	-	79.7%	21.2%
セキュアコンテンツ管理製品	-	11.8%	15.5%
暗号製品	-	20.3%	14.1%
合計	-	15.4%	16.0%

図 2 国内情報セキュリティツール市場推移

(百万円)



## 7.2. 情報セキュリティツール市場のカテゴリ別分析

### 7.2.1. 統合型アプライアンス市場

#### 【製品の特性と市場の動向】

アクセス制御系技術では、ソフトウェアタイプの製品からハード・ソフト一体型のアプライアンス製品への移行が進行すると同時に、同一アプライアンス上に複数の機能を盛り込んで、1台で様々な防御機能を提供しようとする製品が相当種類供給されている。これら製品は機能区分による仕分けになじみにくいので「統合型アプライアンス」と呼ばれるようになってきている。

その機能としては、アクセス制御領域であるファイアウォール、VPN、IDS/IPSと、コンテンツセキュリティ領域であるアンチウイルス、アンチスパム、URLフィルタリング(選別)が主なもので、製品により、1台のアプライアンス上にこれらのうち2~3種類以上が搭載されている。

このような複数機能の搭載が可能になったのは、ハードウェアの性能が飛躍的に高まってきたことによる。パケットを、その中身を見ながら処理する部分をハードウェアで実現する技術も一役買っている。しかしそれでも、アンチウイルス、VPN、IDSを同時に使うと相当の負荷となり、通信量やハードウェアの仕様によっては処理性能の低下はまぬがれない。従って、統合型アプライアンスの機種構成としては飛びぬけてハードウェア性能の高い専用機による高価格機か、IAサーバの普及レベルの装置を使った低価格の普及機かに二極分化の傾向が見られる。

特に普及型の価格帯では、中小企業のネットワーク環境や、大企業の出先事業所等で専門家の確保が難しいネットワーク環境で、複数の機能を一元的に簡易に実現できる、「お任せ型」一括ソリューションとして導入される例が増加している。この市場セグメントを狙って、流通チャネルを活用して攻勢をかけるベンダー側の営業戦略と相俟って、出荷を伸ばしていると見られる。この傾向はここ数年持続するものと予測されており、複数のセキュリティ機能を有する統合型アプライアンスは、今後も急速な市場の伸びが期待される領域である。

供給サイドを見ると、情報セキュリティ専業で製品品揃え拡大や統合ソリューションの提供を志向する大手ベンダーと、統合型アプライアンスに特化して参入してきたベンチャー型に二分される。一部のベンダーでは、複数機能の同時実現のために単機能のエンジンは外部からのOEM調達に依存するところもある。また、IDSやアンチウイルスの定義ファイル等の更新・提供が必須であり、ベンダーにとってのランニング・サポート(日常使用に対応する保守・更新サービス)の負担は小さくない。ベンチャー型企业ではOEM先への依存に頼るケースも見られる。普及価格帯の製品は既に相当低価格になっており、市場は急拡大しつつも、新規参入の可能性もあり、競争は厳しいものになると予測される。

【市場規模とその推移】

表 7 に国内統合型アプライアンス市場の市場規模実績推定値と予測値を示す。

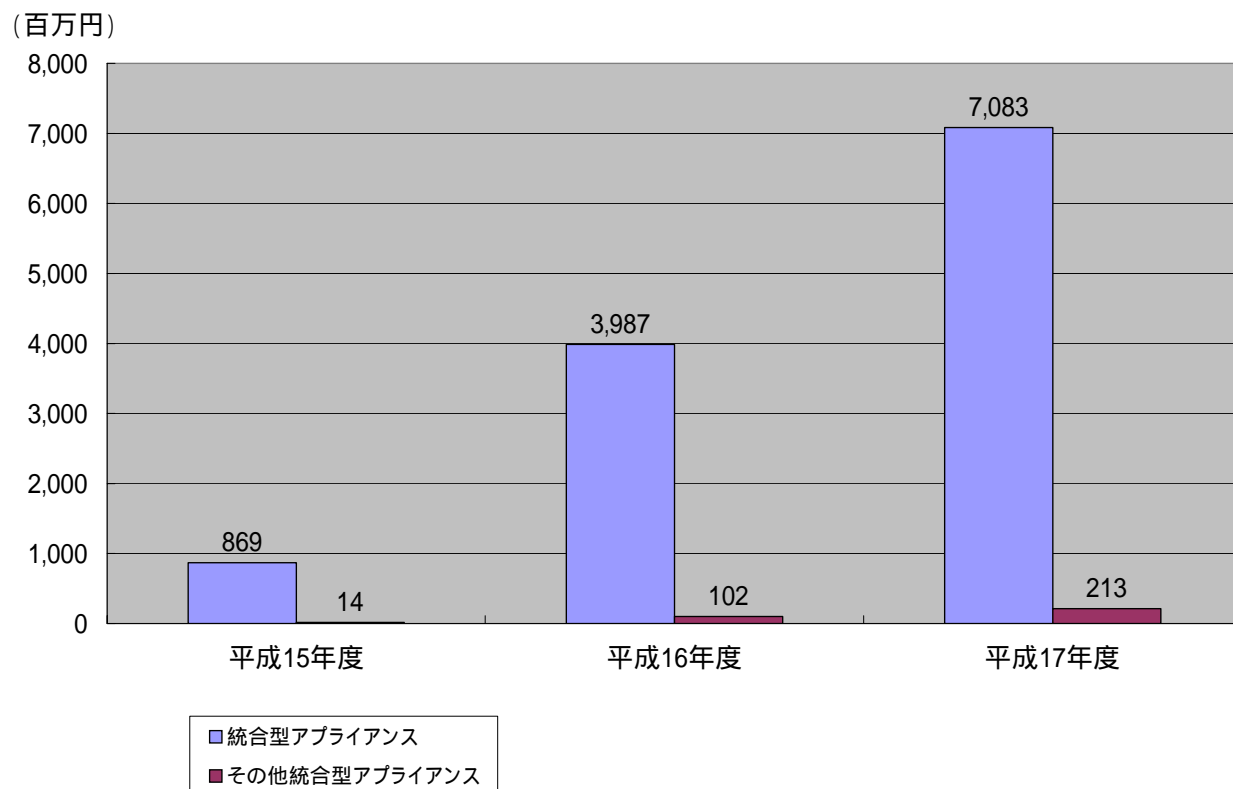
表 7 国内統合型アプライアンス市場規模 実績と予測

製品別出荷金額	平成 15 年度	平成 16 年度	平成 17 年度
統合型アプライアンス	869	3,987	7,083
その他統合型アプライアンス	14	102	213
統合型アプライアンス合計	883	4,089	7,296
製品別構成比			
統合型アプライアンス	98.4%	97.5%	97.1%
その他統合型アプライアンス	1.6%	2.5%	2.9%
統合型アプライアンス合計	100.0%	100.0%	100.0%
対前年比成長率			
統合型アプライアンス	-	358.9%	77.6%
その他統合型アプライアンス	-	628.6%	108.8%
統合型アプライアンス合計	-	363.2%	78.4%

平成 15(2003)年度は、各ベンダーから新製品が投入された。しかし、使い勝手や価格対性能比、特にネットワークのスループットに悪影響を及ぼすことと、製品自体の品質に難があるものもあったことから、なかなか販売が進まなかった。市場規模も 9 億円弱であり、とりあえず市場が形成された、というレベルの立ち上りであったと言える。

平成 16(2004)年度は対前年比 363%増と、市場が大きく伸張したと見られる。平成 16(2004)年度になり、製品自体の品質向上、製品品揃えの拡充、価格の低下といった供給サイドの努力に加え、インテグレータ・ユーザ側での使いこなしなど経験や工夫も追い風となり、導入が急速に進むこととなったのではなかろうか。また、従来単発的・逐次的に導入されてきたアクセス制御ソフトウェアやアプライアンスを、統合型製品によって置き換え、管理性の向上と運用コストの低減を図ろうとする考え方もこの動きを推し進めていると考えられる。この流れはここ当面続くものと予測され、平成 17(2005)年度においても急速な市場拡大が続くものと予測する。

図 3 国内統合型アプライアンス製品市場推移



### 7.2.2. アクセス管理製品市場

#### 【製品の特性と市場の動向】

「アクセス管理製品」とは、情報システムやネットワーク、あるいはファイルといった IT 資源にユーザがアクセスする際に、そのアクセスする本人がシステムに登録された正規のユーザであるかを確認・検証し、正規の権限を認められていない者を排除することで情報システムの安全を確保する技術的手法である。

重要な情報の多くが電子化されたファイルやデータとして保存され、ネットワークを通して様々な場所からアクセスできるようになった昨今、ネットワークに対するアクセス管理はもちろん、サーバ環境、ウェブ・アプリケーション環境下も含め、システムを使用する個人を識別し、適切なアクセス権を与え運用する、アクセス管理ソフトウェアの重要性が高まっている。企業の情報資産を情報漏えいやセキュリティ上の脅威から守るためにも、たいへん重要視されている分野である。

認証の場、あるいは管理対象とするアクセスについて言えば、まず各個人の情報処理端末として最も一般的なパソコンへのログインがある。更にそれが社内ネットワークに接続

する段階での認証、特定のアプリケーションを利用する場合の認証、特定のデータ、ファイル、あるいはデータベースへのアクセスの際の認証、そして社外ネットワークから社内ネットワークへの接続、いわゆるリモートアクセスに際しての認証等がある。

認証は通常、ユーザを特定するための情報（ID）と、そのユーザが本人であることを確認するための情報（通常は本人しか知らないものや本人しか持っていないもので、コンピュータシステムにより認識ができるもの）の組合せにより行うのが一般的である。本人しか知らない情報の典型例がパスワードあるいはPIN（Personal Identification Number: 本人確認番号、暗証番号）と呼ばれるものである。これは他人が容易に入手できる可能性が高いことから、近年これに代わる、あるいは付け加えるものとして、本人しか持っていないものを導入することが一般化しつつある。それはICカードであったり、ワンタイムパスワード（使い捨てパスワード）と呼ばれる一種の乱数発生装置であったりする。

アクセス管理は精度・頻度を高めることで安全性を高めることが可能な一方、ユーザの利便性を阻害する要素を持っている。利便性を犠牲にすることには二面の問題がある。一つは直接的な効果もしくは影響で、業務効率が落ちること、すなわち生産性を阻害することになる。二つ目の問題は、ユーザ側が認証のわずらわしさから安全管理を犠牲にする方向に逃げる可能性が強まることである。現在多くのシステムで最も一般的に行なわれている本人認証方法はユーザIDと固定パスワードの組合せである。このパスワードを、システムごとに別のものにするとか、更新頻度を高めるとか、容易に想像されにくい、意味性の低いものにするとかの要求が、安全管理面からは出てくるが、本人にとっては対応が困難になり、ついパスワードを紙に書いて保存するというような安全を脅かす方向に逃げがちになる。これは結局安全を追求する余り安全を阻害するという自家撞着に帰結するので、それを回避する合理的手段、すなわち使い勝手がよく、かつ安全なもの、を志向する必要が出てくる。

その要求に対応する一つの方法として、近年、本人の身体の特徴を抽出することで、他人が成りすますことが物理的に不可能な情報を使おうとする動きがある。本人の持っているものという意味では他人が入手もしくは偽造することが極めて困難な身体的特徴を利用するという発想である。これは生体認証と呼ばれている。身体的特徴の情報として利用されるものにはいくつかあり、現在も新たな開発が進んでいるが、実用化されているものとして指紋、手や指の静脈パターン、虹彩や網膜のパターン、顔そのもの、更には行為や行動の癖や特徴、声といったものがある。

いずれも特徴情報認識と特徴データ抽出の精度と速度が向上して実用に耐えるものになってきた結果、近年急速に普及が進みだした。指紋認証以外の方式では、静脈パターンの読み取りによる認証方式が情報セキュリティ用のアクセス管理製品として普及する可能性が高い。顔認証、虹彩認証、筆跡認証などの他の認証方式は、設備費用の問題から、アクセス管理よりは入退室管理のような物理的セキュリティ市場への採用等、当面は限定的な使われ方になるかもしれない。また、生体認証に使われる情報はID・パスワードと違って、

個人を特定する上で代替のきかない性格を持つため、一旦そのデジタルデータが漏えいした場合の影響は大きく、そのデータ自身の管理に対して、システムのにも心理的にも厳格な管理が求められる、

一方、「本人が持っているもの」としてはやはり偽造の困難さから、また物理的に存在の管理の容易さから、IC カードや USB キーといったものも使われている。これらはその情報容量の大きさに着目して、社員証のような身分証明書との兼用や、暗号システムとの組合せで使われることが多い。暗号については、暗号キーの格納やその入手のための情報をデバイス（装置・機器）の中に持つことにより、データの暗号化も実現して、認証のみならず、データの安全も実現するアプローチが行われている。

ハードウェアによるアクセス管理の特徴は簡便性にある。パスワードの打ち込みや認証局への登録、暗号キーの取得など、煩雑な認証プロセスを取り除くことによって、認証情報漏えいの危険度も軽減される。IC カードは利用範囲の広さによる多様性と記憶情報量の大きさ、USB キーは低価格性と記憶容量の大きさ、生体認証は物理的な管理が不要、というようにそれぞれの特徴の上に立った市場形成がなされていくであろう。

業務システムが IT 化するのに伴って、顧客訪問中、出張先、あるいは外出中の立ち寄り先等から自社ネットワークにログオンして、その業務システムやサーバ上のデータを活用することによって業務効率を高める、ということも一般的に行われるようになった。このような場合の本人確認は、遠隔地であり確認のための情報が限られること、端末側での認証手段に制約があること、認証のための情報伝達路にも制約があること、等から、その手段には限界がある場合が多い。そのようなケースで比較的容易に利用できるのがワンタイムパスワード（使い捨てパスワード）と呼ばれる方式で、乱数を活用することで、1 回 1 回違う数字の組合せを使うことができる。基本スタイルはリモートアクセスユーザ（遠隔地から利用するユーザ）が持つ乱数発生器で、あるキーにより生成される乱数を、全く同じアルゴリズム（動作原理）で動作する認証サーバが生成する乱数と比較することで本人確認をしようとするものである。このとき本人の持つ乱数発生器は、活性化のための暗証番号（PIN）により保護されているので、盗難による悪用に対する耐性がある。そのようにして生成された数字の列は 1 回限り有効で、次に使われる数字の列を予測することは不可能に近いので、安全度と利便性とを兼ね備えた汎用的な認証システムと言える。この方式は比較的早い時期から製品が提供されてきており、外務員を多く使う保険、証券、医薬等の分野での利用が活発に行われている。

業務システムをネットワーク化するアプリケーションの導入も盛んで、そのような場合は決裁権限を本人認証と対応させて管理することも必要であり、認証手続きは単に情報処理資源（リソース）へのアクセス管理に留まらず、業務管理そのものとも密接にリンクするプロセスとなりつつある。すなわち、アクセス管理は、不正アクセスや成りすましといった単なるセキュリティ上の脅威に対する防御だけでなく、業務システムにおける権限と

責任の管理にも直結する管理手段として定着しつつあると言える。ディレクトリ・システムやシングルサインオン(1回の認証で複数のシステムへのアクセスを可能にする管理システム)と呼ばれる製品群がこれに該当する。その延長線上には、いわゆるアイデンティティ(本人特定情報)管理も含まれる。ユーザIDは、システムやアプリケーションが個人を識別するためのものであり、その個人を主体に、企業内に種々点在するシステムのID管理を統合するアイデンティティ管理ツールは、物理的な一元化が困難な環境において、論理的に一元化できる仕組みを構築するためのツールとして今後普及が見込まれる。

誰もがアクセスできる、という利便性・効率第一優先の考え方から、必要な人だけがリソース(情報処理資源)にアクセスできるというセキュリティ重視の思想に基づくシステムを構築・導入する企業が、個人情報保護法や情報漏えい事件をきっかけに増えている。また、この分野の製品には監査証跡として使用可能なログを取得・保存する機能を有する製品もある。個人情報保護法に基づく各省庁のガイドライン等では、ログ取得・ログ管理を推奨する記載があり、それを実現するための補完として評価されている面もあると見られる。アクセス管理は、従来の第一優先であった外部からの、部外者のアクセスに対する防御から、内部者の権限外のアクセスのコントロール(管理・制御)へと関心がシフトするに伴って、今後も市場の伸びが期待できると見られる。

金額的に「アクセス管理製品」市場の相当部分を占める「ログオン管理/アクセス許可製品」は、一般にシステム全体に対するアクセスを統合的に管理するため、機能間の連携が求められる領域であり、大規模ベンダーによるトータルソリューション提供が行われるケースが多い。従ってベンダー数も限られることになる。そしてインプリメンテーション・サービスで各企業のセキュリティポリシー・プロセスに合せた導入が成功のキーとなる市場でもある。「個人認証用ワンタイムパスワード製品」市場ならびに「PKIシステム及びそのコンポーネント」は歴史が長く成熟していることから淘汰が進み、世界的に寡占状態が形成されている。ほかのハードウェア認証手法であるICカード、USBキー、生体認証は普及期の市場で、ICカードに大手半導体メーカーやコンピュータメーカーの参入がある他は、比較的小規模のベンチャー型企業がシェア争いを演じている。

なお、本レポートでは、直接的に情報システムへのアクセス権を管理するための製品市場規模を取りまとめているため、間接的なアクセス管理製品、例えば入退室管理や現金自動預け払い機(ATM)などに利用されているアクセス管理製品(認証装置)の数字は含んでいない。

#### 【市場規模とその推移】

表8に国内アクセス管理製品市場の市場規模実績推定値と予測値を示す。

アクセス管理製品の市場規模は、平成15(2003)年度の実績で344億円、「情報セキュリティツール」市場に対する構成比27.3%(表6参照)であったと推定する。セキュアコンテ

ソツ管理製品、アクセス制御製品に次ぐ規模であり、この 3 カテゴリで「情報セキュリティツール」市場のほとんどを構成するものである。NPO 日本ネットワークセキュリティ協会による前述の報告書<sup>4</sup>によれば、アンチウイルスシステム、ファイアウォール、個人認証及びユーザ管理システムはいずれも 100%近い導入率であり、この 3 カテゴリが突出した構成比を形成することを裏付けている。

その普及率の高さから、市場の伸びは「情報セキュリティツール」市場全体ほど高くないが、平成 16(2004)年度には対前年度比 13.6%増の 391 億円、平成 17(2005)年度には同 16.6%増の 456 億円に達すると予測する。

**表 8 国内アクセス管理製品市場規模 実績と予測**

製品別出荷金額 (百万円)	平成 15 年度	平成 16 年度	平成 17 年度
個人認証用ワンタイムパスワード製品	2,056	2,530	2,868
個人認証用 IC カードシステム	2,192	2,828	3,344
個人認証用 USB キーシステム	981	1,315	1,634
個人認証用生体認証デバイス / システム	2,659	4,354	6,677
ログオン管理 / アクセス許可製品	19,212	20,098	22,296
PKI システム及びそのコンポーネント	4,122	4,576	4,977
その他のアクセス管理製品	3,190	3,407	3,790
アクセス管理製品 計	34,412	39,108	45,584
<b>製品別構成比</b>			
個人認証用ワンタイムパスワード製品	6.0%	6.5%	6.3%
個人認証用 IC カードシステム	6.4%	7.2%	7.3%
個人認証用 USB キーシステム	2.8%	3.4%	3.6%
個人認証用生体認証デバイス / システム	7.7%	11.1%	14.6%
ログオン管理 / アクセス許可製品	55.8%	51.4%	48.9%
PKI システム及びそのコンポーネント	12.0%	11.7%	10.9%
その他のアクセス管理製品	9.3%	8.7%	8.3%
合計	100.0%	100.0%	100.0%
<b>対前年度比成長率</b>			
個人認証用ワンタイムパスワード製品	-	23.1%	13.3%
個人認証用 IC カードシステム	-	29.0%	18.2%
個人認証用 USB キーシステム	-	34.1%	24.3%
個人認証用生体認証デバイス / システム	-	63.8%	53.3%
ログオン管理 / アクセス許可製品	-	4.6%	10.9%
PKI システム及びそのコンポーネント	-	11.0%	8.8%
その他のアクセス管理製品	-	6.8%	11.2%
合計	-	13.6%	16.6%

<sup>4</sup> P26(7.1 章)脚注 3 参照「IT セキュリティ対策施策の導入・実施状況とその満足度調査」

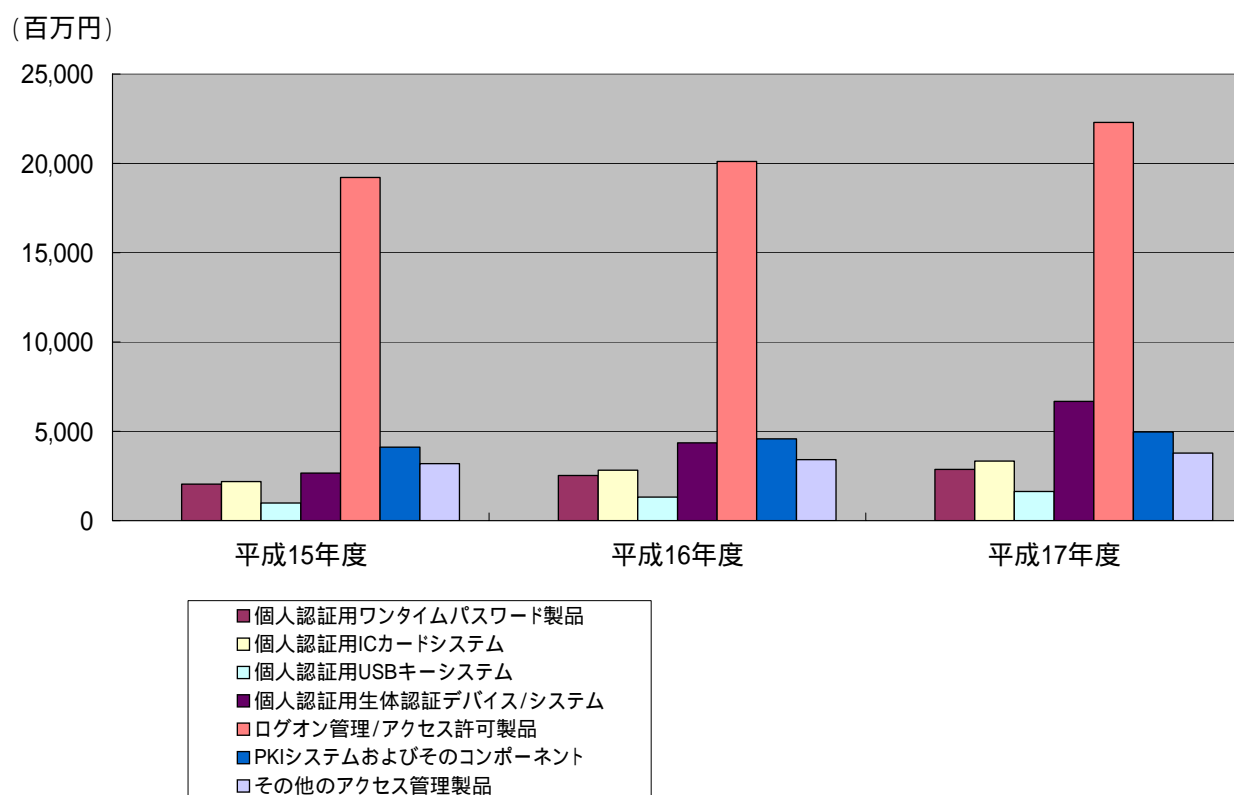
「アクセス管理製品」カテゴリでは、中分類レベルのセグメントで、「ログオン管理/アクセス許可製品」が最も大きな部分を占めた。市場規模は平成 15(2003)年度で 192 億円であり、平成 16(2004)年度は 4.6%増の 201 億円、平成 17(2005)年度には 10.9%増の 223 億円に達すると推測する。

ログオン管理製品には、OS などと連動した認証機能が含まれているが、特に個人認証用の各システムとも関わりが深い。例えば入り口部分で個人認証を強化する際に、シングルサインオン(1回の認証で複数のシステムへのアクセスを可能にする管理システム)と連動させセキュリティを強化、ユーザの利便性を上げると共に、ユーザがアクセスできるアプリケーションを制限するようなシステムを導入する場合も多い。アクセス許可製品は、社内情報処理資源(リソース)に対するアクセスについて、正しいユーザにアクセス権限を付与することでアクセスをコントロール(管理・制御)する。ポリシールールに基づきアクセスコントロールリスト(ACL)を作成し、それを運用することで、どのようなユーザにどのようなアクション(システムやネットワークへのログオン、アプリケーションの実行、データベースの参照、ファイル操作等)が許されるのか、を管理する。アクセス許可製品での保護対象資源(リソース)はファイルやディレクトリをはじめ、ポートやログインアプリケーション、TCP、マシン名、ネットワーク ID、メモリ、等多岐に渡る。単独で販売されるディレクトリ・サービス製品、ネットワーク統合管理製品におけるユーザ管理モジュール、また、人事情報等と連携してユーザのアクセス権限を動的に管理する、いわゆるプロビジョニング(ユーザ別のシステム利用権限の定義)やアイデンティティ(本人特定情報)管理製品等がこのカテゴリを構成している。社員の流動化と派遣・パート等従業員構成の複雑化、業務の IT 化、システムのネットワーク化の進展につれ、このセグメントも拡大を続けると見る。

個人認証をソフトウェアベースでかつ信頼できる第三者の電子証明に依存して実現するものに PKI(Public Key Infrastructure)システムがある。市場規模は平成 15(2003)年度で 41 億円であり、平成 16(2004)年度は 11.0%増の 46 億円、平成 17(2005)年度には 8.8%成長して 50 億円に達するものと見る。

これも約 10 年の歴史を持つ確立した技術であり、一定の市場を形成しているが、認証局の自社運用における管理コストや商用認証局を利用する場合のランニングコスト等が阻害要因となって幅広い普及には至っていない。また、住民基本台帳のネットワーク化と、電子政府・電子自治体サービス利用に際しての本人確認ツールとして、住民基本台帳カードが導入され、公的個人認証の仕組みが取り入れられて、いわば公営の PKI システムも稼働を始めている。が、まだそのサービスの充実と利便性の周知が進んでいない面もあって利用は限定的なものに留まっている。安全性・利便性の認識とサービスの充実により広く普及することが期待される。

図 4 国内アクセス管理製品市場推移



ソフトウェア認証に対して、何らかの物理的存在を組合せる方式が広まりつつある。より高いセキュリティレベルの実現のために、2要素認証(2-factor authentication)方式を採用しようという動きによる。2要素認証とは、本人が持っているものと知っているものというように二つの違う要素を組合せた認証で、落としたり盗まれたりというリスクを回避しやすくなる。具体的にはICカード、USB装置、生体認証装置等が使われる。またワンタイムパスワード(使い捨てパスワード)もこれに類似するものと定義できる。上で見たように、その使い勝手の良さや安全性から、急速に普及が進むものと見られる。また、情報漏えい防止の観点からアクセス管理に関心が高まっていることも追い風となっている。

この、ワンタイムパスワード、ICカード、USBキー、生体認証をハードウェア方式と定義して「アクセス管理製品」市場に占める割合の推移を見ると、平成15(2003)年度は合計79億円で22.9%に留まるが、平成16(2004)年度は110億円で28.2%、平成17(2005)年度には145億円で31.9%までシェアを上げると予測される。

ハードウェア方式の中で特に高い伸びを示すのが「個人認証用生体認証デバイス/システム」市場で、平成15(2003)年度実績推定値は27億円であるが、平成16(2004)年度に63.8%、

平成 17(2005)年度に 53.3%伸びて 67 億円の市場規模に達する。次に大きなセグメントは「個人認証用 IC カードシステム」で平成 15(2003)年度が 22 億円、平成 17(2005)年度には 33 億円と予測する。

ワンタイムパスワードは導入の歴史も長く、先行した米国企業を中心に市場地図はほぼ固まると同時に伸びも緩やかなものになりつつあるが、IC カードや生体認証のように高度のデバイス（装置・機器）技術を必要とするものは、その技術・製品開発と歩を合せて今後伸びを高めるものと見られる。また、単に狭義の IT セキュリティ領域に留まらず、昨今安全性が問題となっている金融機関のキャッシュカードへの導入や、電子マネーの媒体としての普及も期待される。これらの分野は日本のデバイス（装置・機器）メーカー、システムメーカーの得意分野でもあり、国産メーカーが世界的に見ても主導権をとりやすい市場として注目される。

### 7.2.3. アクセス制御製品市場

#### 【製品の特性と市場の動向】

アクセス制御製品とは、システムにアクセスする行為を、その主体であるユーザ、すなわち人、という単位でなく、通信という切り口で制御しようという思想に基づく技術・製品である。通信インフラが非常に高いレベルで整備され、高速で安価な通信が世界中どこでも可能な時代となった。その通信路をベースにインターネットと呼ばれる通信ネットワークが著しい普及を見せ、インターネットベースでの通信がほとんど全てのコンピュータシステム間で可能になっている。通信プロトコルも IP（インターネットプロトコル）がベースになり、その上に TCP、UDP をベースとする各種の通信プロトコルが飛び交う状態になっている。そのおかげで電子メール、ウェブ検索、ファイルの送受信といった情報手段が自由に使える一方、意図せざる相手からのアクセスや、第三者によるシステムや情報の悪用といった弊害も多発している。インターネットの利便性はそのような危険性とも表裏のものとして存在しているのである。

従って、通信の中身を確認して、必要とするもののみを許可し、不要なもの、悪意あるものは遮断するという制御が必要となる。具体的には、インターネットその他の外部ネットワークから社内ネットワークに接続する入り口において、その通信の種類や内容をチェックし、あらかじめ定められたルールに基づく通信のみを許可する、ファイアウォールと言われる製品がその典型例である。この機能はルータと呼ばれる通信中継機器のフィルタリング（選別）機能で一部実現可能であるが、今調査ではルータは調査対象から除外し、アクセス制御を主目的とする製品に限定している。ファイアウォールはアクセス制御の根幹を成す装置で、ファイアウォールを正しく設置し、その通信制御機能を正しく設定すれば、外部からの脅威のかなりの部分を遮断することが可能である。このために、インターネット接続における必須の防御アイテムとして、インターネットが一般化する比較的初期

の段階から使われてきたし、現在もウイルス対策と並んで最も普及が進んでいる情報セキュリティツールである。

ファイアウォールは典型的には社内ネットワークとインターネットの境界線に設置するものだが、ウイルスのみならず外部からの不正侵入や乗っ取り、スパイウェアの脅威が身近に迫る中で、ネットワークの入り口だけでなく、各パソコン端末個別にもガードを固めようという考え方も出てきている。これはクライアント・ファイアウォールまたはデスクトップ・ファイアウォールと呼ばれる。法人のクライアント（端末）マシン、個人用パソコンを問わず、デスクトップ・ファイアウォールの導入も進んでいる。なお、デスクトップ・ファイアウォールはウイルス対策ソフトと一体化した製品として提供されるケースも多いが、そのようなケースはアンチウイルスの製品セグメント（「セキュアコンテンツ管理製品」カテゴリ）で集計しており、アクセス制御製品のカテゴリには算入していない。

アクセス制御製品カテゴリのもう一つのセグメントが侵入検知・侵入防止製品分野である。英語ではIDS（Intrusion Detection System）、IPS（Intrusion Prevention System）あるいはIDP（Intrusion Detection and Prevention）と呼ばれる。ファイアウォールに設定されたルールに基づいて許可された通信のプロトコルを活用しつつ、想定外、権限外、目的外のアクセスや利用を試みようとする、言ってみれば招かれざるユーザが存在する。IDSは、それに対し、ネットワークを流れるパケットを監視することで、不正なアクセスや侵入の試みを検知しようという発想に立つ技術・製品で、国内では1997年頃から使われるようになった。パケットを解析して、攻撃等の不正アクセスパターンだと認識すれば警報を発する。警報の方式には警告音、電子メール、音声案内、ポケベルや電話の発信等がある。また、IDSの一種で、パケットを見るのではなく、サーバ等の個別マシンの動きを監視して不正アクセス等を検知する製品もある。前者がネットワークタイプと呼ばれるのに対して、後者はホストタイプと呼ばれる。IPS、IDPは比較的新しい発想で、単に検知するだけでなく、ファイアウォールと連携して、あるいは自ら通信コントロール機能を持つことで、不正な通信を自動的に遮断するところまで踏み込んで、サービスしようという技術・製品である。これらの製品は、使いこなす上でかなりのレベルのネットワーク技術が必要とすることや、誤報・誤検知のコントロール（適正化制御）が簡単ではないこと等の理由で、普及は一定レベルに留まっている。

ファイアウォールが特定通信限定許可型ゲートウェイ製品であることから、インターネット経由のリモートアクセスに対してVPN接続を提供するために、VPNゲートウェイを併設するものが一般的である。VPN製品を暗号応用製品、あるいはアクセス実現手段と区分する考えもあるが、通信経路における盗聴や覗き見への対策、あるいはより積極的に、あらかじめ認定されたユーザ以外のアクセスを排除するという意味でアクセス制御製品と位置付けることができる。ファイアウォールとセットで提供されることが多い要素もあり、暗号製品カテゴリよりはアクセス制御製品カテゴリに区分けすることが一般化している。

従って VPN ゲートウェイ製品はアクセス制御と同一カテゴリで扱うものとする。

家庭内に複数のパソコンを持ち、無線 LAN 等の簡便なツールを使って家庭内 LAN が構築されるようになると、ファイアウォール、IDS とともに家庭向けの製品の導入が期待される。中期的には数量面で有望な市場である可能性はあるが、基本的に単価が安いこと、当面は導入率も大きくは上がらないと見られることなどから、少なくとも当面は市場を大きく押し上げる要因にはならないと見ている。

アクセス制御製品、特にファイアウォールは、インターネットの普及と軌を一にして提供されてきており、長い歴史を持つ。IDS / IPSも含めて、ネットワーク通信技術開発と密接に関連して開発されてきた経緯から、その歴史の長い米国やイスラエルを起源とするベンダーも多く、国内に流通するほとんどの製品が海外製品であることが供給側の特徴と言える。またその歴史と普及率を反映して業界地図は比較的固まっている。

ファイアウォール・ソフトウェア（企業向けライセンスタイプ）は、競争の歴史の中で淘汰が進んでおり、世界的に数社の寡占状態が続く。ファイアウォール・アプライアンスは、上位5社で市場の9割程度を占める。既存のファイアウォール・ソフトウェアベンダーの多くがファイアウォール・アプライアンス製品に注力するようになったが、上位のファイアウォール・アプライアンス専門ベンダーのシェアに影響を及ぼすまでには至っていない。IDS / IPSアプライアンス及びソフトウェアは、10社以上が製品を投入しているが、トップ1社が50%以上のシェアをとり、上位数社の寡占状態と言える。VPNソフトウェア及びアプライアンスは、IPSec-VPNについては、上位2社の寡占状態と言えるが、SSL-VPNについてはベンチャー企業が強く、この分野の市場拡大に寄与している。

【市場規模とその推移】

表 9 に国内アクセス制御製品市場の市場規模実績推定値と予測値を示す。

表 9 国内アクセス制御製品市場規模 実績と予測

製品別出荷金額（百万円）	平成 15 年度	平成 16 年度	平成 17 年度
ファイアウォール・アプライアンス	17,625	13,926	15,086
ファイアウォール・ソフトウェア （企業向けライセンスタイプ）	5,282	6,073	6,384
ファイアウォール・ソフトウェア （デスクトップ FW）	880	1,012	1,064
VPN ソフトウェア	2,641	3,036	3,192
VPN アプライアンス	1,958	2,458	1,676
IDS / IPS アプライアンス	2,679	5,766	7,660
IDS / IPS ソフトウェア	4,984	5,215	5,594
その他のアクセス制御製品	378	127	95
アクセス制御製品 計	36,428	37,612	40,751
<b>製品別構成比</b>			
ファイアウォール・アプライアンス	48.4%	37.0%	37.0%
ファイアウォール・ソフトウェア （企業向けライセンスタイプ）	14.5%	16.1%	15.7%
ファイアウォール・ソフトウェア （デスクトップ FW）	2.4%	2.7%	2.6%
VPN ソフトウェア	7.2%	8.1%	7.8%
VPN アプライアンス	5.4%	6.5%	4.1%
IDS / IPS アプライアンス	7.4%	15.3%	18.8%
IDS / IPS ソフトウェア	13.7%	13.9%	13.7%
その他のアクセス制御製品	1.0%	0.3%	0.2%
アクセス制御製品 計	100.0%	100.0%	100.0%
<b>対前年度比成長率</b>			
ファイアウォール・アプライアンス	-	-21.0%	8.3%
ファイアウォール・ソフトウェア （企業向けライセンスタイプ）	-	15.0%	5.1%
ファイアウォール・ソフトウェア （デスクトップ FW）	-	15.0%	5.1%
VPN ソフトウェア	-	15.0%	5.1%
VPN アプライアンス	-	25.5%	-31.8%
IDS / IPS アプライアンス	-	115.3%	32.9%
IDS / IPS ソフトウェア	-	4.6%	7.3%
その他のアクセス制御製品	-	-66.5%	-25.1%
アクセス制御製品 計	-	3.3%	8.3%

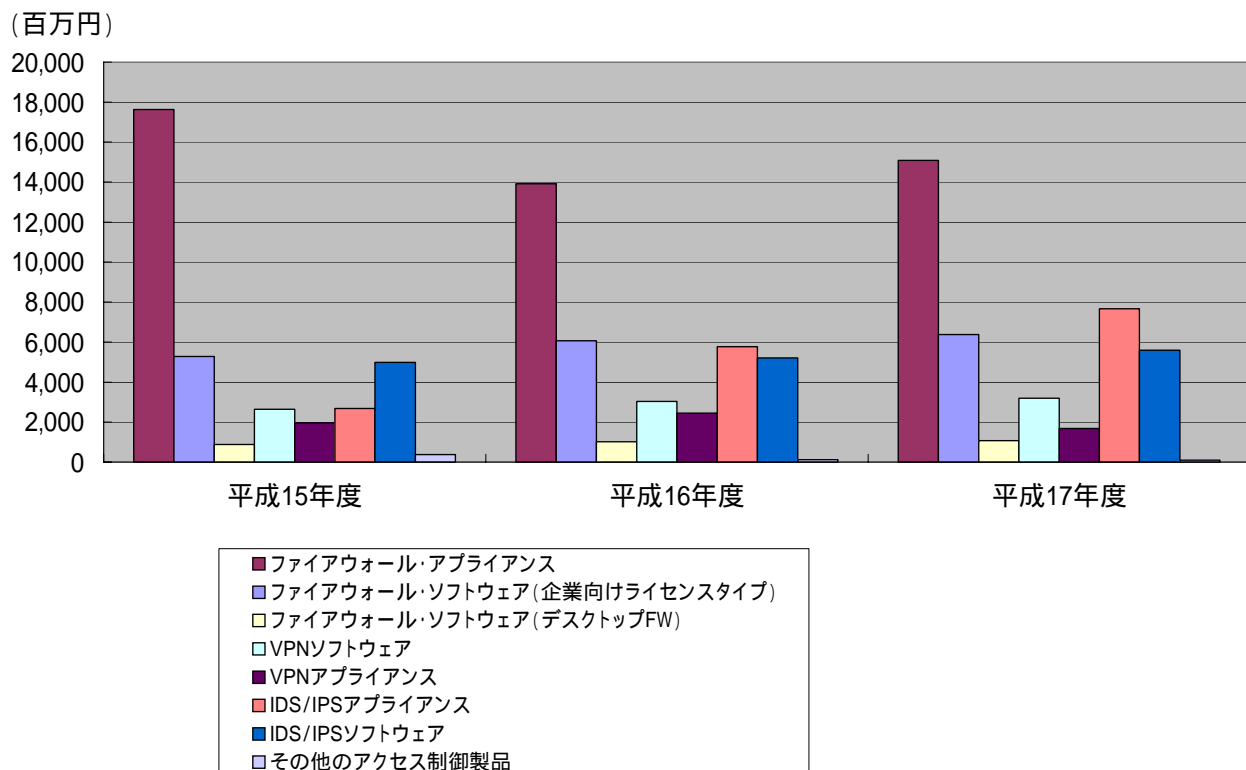
アクセス制御製品カテゴリで最大のセグメントはファイアウォールで、インターネット接続の広がりにつれて最低限の防御手段という認識から、比較的早期に、また比較的順調に普及の進んだセグメントである。平成 15(2003)年度の市場規模は、「ファイアウォール・アプライアンス」、「ファイアウォール・ソフトウェア(企業向けライセンスタイプ)」、「ファイアウォール・ソフトウェア(デスクトップFW)」の3セグメント合せて238億円に達していると推定される。単一の製品カテゴリとしては相当規模の大きい市場である。

このセグメントの特徴としては、普及率が極めて高く導入は一巡していると思われる中で、更新や機能強化に際してソフトウェア型からアプライアンス型へのシフトが進行していること、更に、特にアプライアンス型においては単機能のファイアウォール(VPNは一般的に併設されるが)から、侵入検知機能やウイルス対策機能等を併せ持つ、いわゆる統合型アプライアンスへの移行も見られることである。その結果として、平成 16(2004)年度には前年度比 11.7%減少して 210 億円となる。ただ、平成 17(2005)年度予測は 7.2%増の 225 億円と若干の回復を予測する。これはファイアウォール・アプライアンスの増減によるところが大きく、製品ライフサイクルの狭間や、ファイアウォール・アプライアンスと統合型アプライアンスの間でベンダーの製品定義の変遷があったこと等によるものと推測される。

アクセス制御製品カテゴリの二つ目の製品カテゴリである「IDS/IPS アプライアンス」、「IDS/IPS ソフトウェア」市場は合計で平成 15(2003)年度推定実績が 77 億円であった。このセグメントは、特に「IDS/IPS アプライアンス」が平成 16(2004)、17(2005)年度に各々 115.3%、32.9%の高い伸びを示しており、ソフトウェア製品も含めた市場規模は平成 16(2004)年度 110 億円、平成 17(2005)年度 133 億円と急成長を遂げると予測される。ファイアウォールを補完する防御という面があることに加えて、企業内ネットワークにおける無権限アクセスを監視することで情報漏えい防止に役立てようとする考え方が出てきていることによる。

VPN(Virtual Private Network=仮想私設通信網)は多くの場合、ファイアウォールに付属する機能として提供されるが、専用回線や電話等のダイヤルアップ回線経由のアクセスに対してVPN単独機能の製品も使われる。ソフトウェアタイプ、アプライアンスタイプの両方が製品化されており、両者合せた市場規模は平成 15(2003)年度で 46 億円、平成 16(2004)年度 55 億円、平成 17(2005)年度 49 億円と、ほぼ横ばいで推移するものと予測する。

図 5 国内アクセス制御製品市場推移



#### 7.2.4. システムセキュリティ管理製品市場

##### 【製品の特性と市場の動向】

「システムセキュリティ管理製品」というカテゴリは従来、比較的認知度が低かった領域である。表 6 に示すように、市場規模は本調査でも他のカテゴリに比べて小さいが、統合型アプライアンスと並んで平成 15(2003)年度から平成 17(2005)年度に極めて高い伸びを示すという予測結果となった。

このカテゴリには主に 3 種類の製品区分が含まれる。一つ目は、ネットワーク上の複数のセキュリティ対策製品やネットワーク管理製品の情報を集約して、一元管理し表示する「セキュリティ情報管理システム/製品」であり、IDS やファイアウォールが複数ある場合にその情報を統合管理する製品や、ネットワーク管理システムにおいて特にセキュリティ情報に関して取りまとめ、ネットワーク管理コンソール等に情報やアラート(警報・警告)を上げる製品がある。二つ目は「脆弱性検査製品」と呼ばれるもので、擬似的な攻撃を仕掛けたり設定状態を調べたりすることで、システムの弱点を洗い出す製品である。そして三つ目のカテゴリが「ポリシー違反管理製品」と呼ばれ、ネットワーク上のサーバ等

の内部を調べて、OS やアプリケーションの状態や設定などを調べる製品である。

本カテゴリの中で「ポリシー違反管理製品」と同様2年間で3倍程度の伸びを示すと予測されるのが、「セキュリティ情報管理システム / 製品」である。セキュリティ管理だけにとられず、ネットワーク及びその上にあるコンピュータ資源の可用性、つまり障害なくいつでも使える状態と性能を保つ必要性から、ネットワーク管理全体を中核に据え、その一つの要素としてセキュリティを管理しようという発想をベースとしたものである。この面からのアプローチの思想も以前からあるものであるが、今後その統合管理の考え方は一層浸透していくと考えられる。セキュリティ上の脅威に対抗するために、企業等ではファイアウォール、IDS / IPSなどのアクセス制御製品や、アンチウイルス、URLフィルタリング（選別）、スパムメール対策などセキュアコンテンツ管理製品を導入している。これらの機能を「統合型アプライアンス」として導入すれば、ある程度一元管理が可能な場合もあるが、全てをカバーすることは現実として難しい。実際には、多くの運用管理すべき情報セキュリティ製品が社内に存在する状況が発生してしまう。このような中、各々の製品から出力される大量のセキュリティログへの対応、製品運用の効率化、コスト削減、総合的なセキュリティ強化等のニーズが高まり、セキュリティ情報の一元管理、統計分析、製品の統合管理を実現する「セキュリティ情報管理システム / 製品」の重要度が増すようになってくるであろう。

「ポリシー違反管理製品」は、ポリシーの遵守という考え方の重要性が認識されるに従って、需要が高まる可能性がある。ネットワークのリスク管理を行う上で、セキュリティポリシーという判断基準から社内のリスクを把握し、未然に対策を行うためには、ネットワーク上の各機器の状況を監視する必要があるからである。「ポリシー違反管理製品」を導入することで、パッチの適用状況やアクセス権の設定状況、更にはパスワード管理について、その更新頻度や指定する属性を満たしているかなどを調べることができる。OS 等の脆弱性が発見され、それを突く攻撃を防ぐためにパッチが配布されるが、それが適正に対策されているかをツールによって確認することも可能で、これらの管理によりセキュリティレベルを高めることができる。また、情報セキュリティ関連の法令への遵守（コンプライアンス）を把握する製品としても、今後の法整備に従って需要が高まる可能性がある。実際、平成 15(2003)年度は 10 億円に達していないが、後に見るように翌年、翌々年にかけて高い伸びを見せると想定されている。

また個人情報保護法をきっかけとし、ISMS、プライバシーマークといった認証取得企業や情報セキュリティ監査制度に取り組む企業が急増している。認証取得企業においては、認証取得後の情報セキュリティ管理策を実現していくためには、机上的・組織的のプロセスだけでは困難で、システムの中でポリシーがどのように設定に反映され、運用がルールどおりに実行されているか監視する必要がある。そのための管理ツールとしての「ポリシー違反管理製品」は、この面からも需要が顕在化し、今後急速に市場に浸透していくものと予測される。

「脆弱性検査製品」は一部先進ユーザの間で関心を呼び、かなり使われたが、やはり専門知識が必要なことから一般ユーザへの普及は限られている。今後は、脆弱性診断サービス等のために使われる形や、前述の「ポリシー違反管理製品」の一要素として組み込まれる使われ方が増えていくと推測される。

「セキュリティ情報管理システム/製品」はいわゆるネットワーク管理プラットフォームと呼ばれるシステムのコンポーネントとして提供されるものもあり、それらは大手システムベンダーからの供給が主力である。その他はセキュリティ専門のベンダーから単体製品で提供されるものが多い。脆弱性検査製品等には比較的長い歴史を持つ製品もある一方、ポリシー違反管理製品等で新興企業から新しいコンセプトの製品の供給も見られる等、需要の顕在化に伴って供給側も多様化・活性化を予感させる動きが出ていると言える。

これらの製品の特徴は、インシデントの発生など「何かがあってから対処する」のではなく、社内のリスクを未然に把握して対策を事前に行うという予防保全型の思想をベースに成立していることにある。

#### 【市場規模とその推移】

表10に国内システムセキュリティ管理製品市場の推定市場規模実績と予測値を示す。

表 10 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

製品別出荷金額(百万円)	平成 15 年度	平成 16 年度	平成 17 年度
セキュリティ情報管理システム/製品	1,444	2,674	4,338
脆弱性検査製品	2,407	3,565	3,254
ポリシー違反管理製品	963	2,674	3,254
その他のシステムセキュリティ管理製品	446	536	605
システムセキュリティ管理製品 計	5,259	9,449	11,450
<b>製品別構成比</b>			
セキュリティ情報管理システム/製品	27.5%	28.3%	37.9%
脆弱性検査製品	45.8%	37.7%	28.4%
ポリシー違反管理製品	18.3%	28.3%	28.4%
その他のシステムセキュリティ管理製品	8.5%	5.7%	5.3%
システムセキュリティ管理製品 計	100.0%	100.0%	100.0%
<b>対前年度比成長率</b>			
セキュリティ情報管理システム/製品	-	85.2%	62.2%
脆弱性検査製品	-	48.1%	-8.7%
ポリシー違反管理製品	-	177.7%	21.7%
その他のシステムセキュリティ管理製品	-	20.3%	12.8%
システムセキュリティ管理製品 計	-	79.7%	21.2%

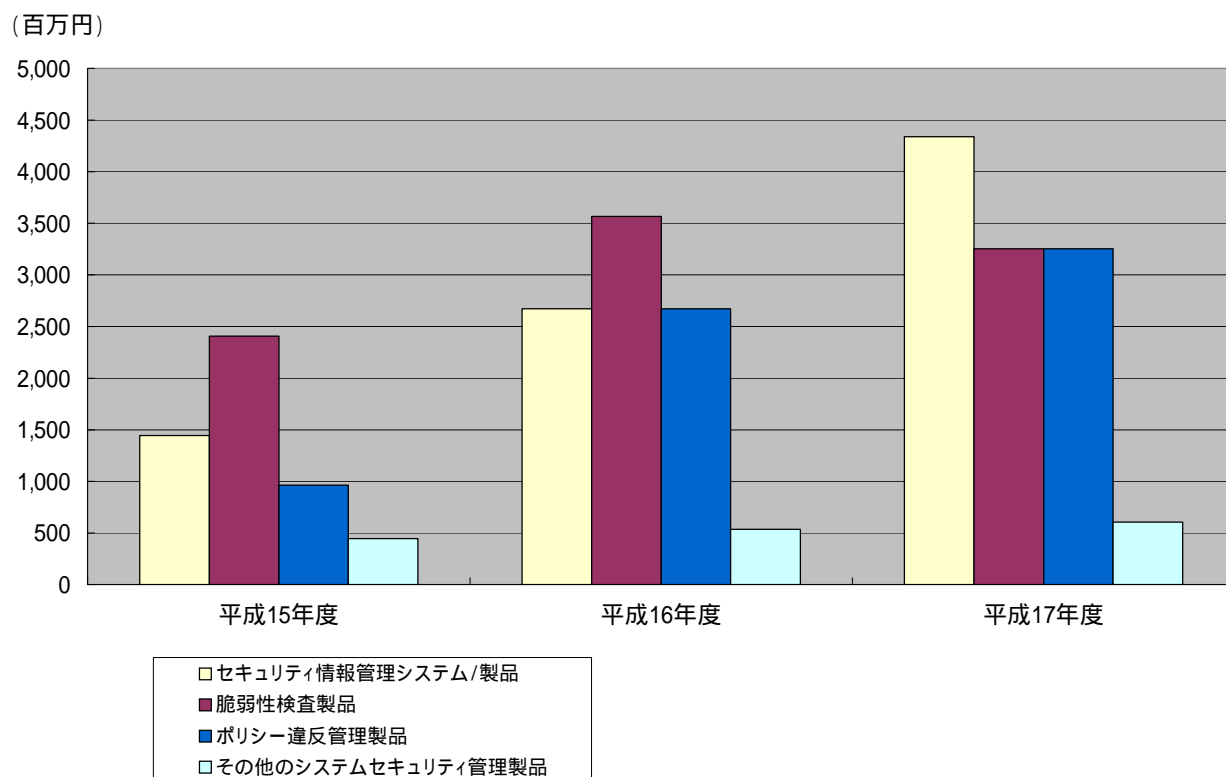
「システムセキュリティ管理製品」市場は平成 15(2003)年度は全セグメント合せても 53 億円程度の市場であったが、平成 16(2004)年度には 79.7%と急拡大して 94 億円に達し、更

に平成 17(2005)年度には 21.2%伸びて 115 億円になるものと予測する。これは、上に見てきたように、「セキュリティ情報管理システム / 製品」及び「ポリシー違反管理製品」が各々 3 倍以上の高成長を遂げることによる。

このうち「セキュリティ情報管理システム / 製品」は平成 16(2004)年度 85.2%、平成 17(2005)年度 62.2%と、安定した高い伸び率を見せて平成 15(2003)年度の 14 億円から平成 17(2005)年度の 43 億円に達する。「ポリシー違反管理製品」は対照的に平成 16(2004)年度に 177.7%といきなり 3 倍近い伸びを見せ、翌平成 17(2005)年度は 21.7%と全体並みの伸び率に落ち着く。市場規模としては平成 15(2003)年度以降 10 億円、27 億円、33 億円という推移になると予測される。

「脆弱性検査製品」は比較的早くから製品が提供され市場に浸透していた関係で、平成 15(2003)年度時点では 24 億円と、「システムセキュリティ管理製品」カテゴリでは最大のセグメントであるが、上述のように成熟期に達していると考えられ、平成 16(2004)年度に 48.1%と伸びた後は平成 17(2005)年度には一転マイナス 8.7%と減少に転じ、33 億円規模に留まると予測される。

図 6 国内システムセキュリティ管理製品市場推移



## 7.2.5. セキュアコンテンツ管理製品市場

### 【製品の特性と市場の動向】

「セキュアコンテンツ管理」、あるいは「コンテンツセキュリティ管理」とは、コンテンツ（通信される情報の内容）に着目してセキュリティを確保しようとする製品群である。その代表がアンチウイルス・アンチワーム製品である。ウイルスやワームの感染経路や感染手法は多様化しており、必ずしもコンテンツに付帯して動くものとは限らなくなっているが、もともとウイルスはそれ単独では動かず、何らかのアプリケーションが生成するファイルに寄生して存続し、広まる性質を持っていたため、コンテンツセキュリティというカテゴリで捉えられている。言うまでもなく、アンチウイルス製品は今やウェブ閲覧やファイル共有といった様々な感染手段に対して検査能力を身に付けている。とは言え、ウイルス・ワームは際限なく毎日のように新種・亜種の登場する世界であり、ネットワーク管理者にとっては定義ファイルの更新に追われざるを得ない厳しい世界でもある。

アンチウイルス製品の設置場所もバリエーションがあり、インターネットとの入り口やネットワークセグメント間に置くゲートウェイタイプ、サーバの安全を守るサーバ設置型、そして各端末を守るクライアント型の区分がある。このようにウイルス・ワーム対策は複数階層で製品が展開され、ユーザ側も複数階層に導入することで様々な感染経路・感染パターンに対応してセキュリティを守っている。

JNSA による「セキュリティ対策施策の導入・実施状況とその満足度調査」（2005年2月）によれば、ウイルス対策ツールの導入率は約97%に達している。その他各種調査によってもウイルス対策の導入は相当進んでいることが確認されている。普及率が100%近くに達するという事は市場がほぼ飽和していることを意味しているが、同様に普及率の高いファイアウォールに比較しても、市場規模は比較的安定した伸び率を示している。これは、一つにはウイルス定義ファイルの更新サービスを毎年継続的に購入する必要があるビジネスモデルにより、売上のベースライン（基礎部分）を確保する戦略が取られていることによる。と同時に、複数レイヤーへの導入、機能強化版へのアップグレード等により収入増を図るビジネスモデルが、市場に浸透できていることも要因と言える。これに加え、IT化の進展と浸透により、一企業当りの対策台数の増加、または稼働端末（パソコン）の絶対数の増加といった要因も大きく寄与していると推測できる。また、わずかではあるが中小企業を中心に新たにインターネット接続をすることによる新規需要や、インターネットビジネスの新規事業モデルが次々と開発され、新規参入も活発化していることにより市場の裾野も拡大していると想定される。

ウイルス対策製品の供給ベンダーは、世界的にビジネスを展開する比較的規模の大きい企業を中心である。これは、24時間365日、新種のウイルスを検出してそれに対応するウイルス定義ファイルを数時間以内に作成し、全ユーザに提供するというサービスモデルが必須であり、そのために世界的な対応体制が欠かせないためである。米国企業を中心であ

るが、日米を基盤とする企業、欧州や韓国ベースの企業もあり、国際市場を前提とした競争が存在する。市場の成熟度が進んでいることと市場地図が比較的固まっていることから新規参入は困難であり、既存事業者の間でのシェア争いの展開となっている。

ウイルス対策以外のコンテンツセキュリティ対策としては、不特定多数に大量にばら撒かれることで通信帯域やサーバの記憶スペース、更にはクライアント（端末）の作業効率に悪影響を及ぼすスパムメールのチェック、メールの受信者をだまして秘密情報や機微情報を入手しようとするフィッシングと呼ばれる不正アクセスに対する対策製品、そして有害あるいは業務に支障をきたすウェブサイトへのアクセスを制限するURLフィルタリング（選別）と呼ぶ対策製品もある。

業務効率やネットワークの通信容量を低下させるスパムメールの対策として、アンチスパム製品がある。ゲートウェイやサーバ上に設置するタイプや、メールクライアントソフトに実装されているタイプなどがあり、アンチウイルス製品と同梱されている場合も多い。スパム判定を行うフィルタリング（選別）エンジンは、各国の言語特性に合せた開発が必要であり、配信アドレスのブラックリストを参照するなど、判定制度をあげるために様々な方法が利用されている。アンチスパム製品については定義ファイルの開発にスピードと信頼性が求められており、大手ベンダーでシェアを分け合っているのが現状である。

URLフィルタリング製品は、業務上、あるいは教育上ふさわしくないウェブサイトや、ウイルス感染やフィッシング詐欺などの有害なサイトへのアクセスを制限する製品である。ゲートウェイに設置するものから、ブラウザに内包されるタイプまでさまざまであり、フィルタリングエンジンはリスト参照タイプや、ウェブサイトの内容を判定するタイプなどがある。

また、主として情報漏えい防止の観点からメールの送受信内容をチェックする、メールフィルタリング製品もある。メール本体や添付ファイルの内容をチェックして不適切なものは送受信を防止したり管理者に事前チェックにまわす、といった機能を持つ。また、フィルタリング（選別）ではなく、後日の追跡のために内容も含め全ての記録を保存する製品も提供されるようになってきている。

メールやURLのフィルタリング（選別）については、製品数はまだ多くない。また、言語の問題やウェブサイトの地域性の問題もあり、国産ベンダーの製品供給が目立つことも特徴と言える。ほかの製品やシステムへの組み込みで提供されることから、大手ベンダーへのエンジン部分の部品としての提供という形態も見られる。URLフィルタリングは下記に見るように個人向け・消費者向け市場での需要もある。フィルタリング（選別）需要は、インターネットの利用サイドと供給サイドの拡大につれて、今後も拡大が見込まれる。

デスクトップ（卓上機）レベル、あるいはクライアント（端末）マシンの上では、従来アンチウイルス対策単機能だった製品から、「アクセス制御製品」の項で見たようなデスクトップ・ファイアウォール、更にはIDS機能をも併せ持つ複合型防御製品への進化が進ん

でいる。本調査では、そのような製品も主たる機能がアンチウイルスである場合には「アンチウイルス・アンチワーム・ソフトウェア」に含めており、それが企業向けに販売されるもの場合には「企業向けライセンスタイプ（GW型、サーバ型、クライアント型の全てを含む）」に計上し、主として個人・家庭向けの場合には「個人ユーザ向けパッケージタイプ（FW、IDS 機能併設型を含む）」に計上している。一つの製品でこれら複数のガードを果たすものは、設定によってはPCの使い勝手を阻害するという弊害はあるものの、対策の充実という面で安心感・充実感があるため、今後クライアントレイヤー（端末階層）での対策の主流になっていくものと予測される。

なお、家電量販店等の店頭で、ソフトウェア製品売り場のかなりの面積をウイルス対策製品が占め、ゲームソフト等に交じってソフトウェア販売ランキングの上位を常に占めている実態も見られる。個人向け市場においても、新規顧客の開拓努力と同時に、毎年新バージョンへのアップグレードや、ウイルス定義ファイルの更新サービスの契約更新という形で需要喚起するビジネスモデルとなっており、既存ユーザからの継続需要を確保する戦略が浸透している。また、パソコンの世帯普及率の上昇（一家に複数台持つ家庭も増加している）と対策実施率の上昇により市場が拡大しているのに加え、インターネットサービスプロバイダーが、月額方式の付加サービスでウイルスチェックサービスを提供するビジネスモデルも広がっており、市場の裾野を広げている。

個人消費者市場向けにはこの他に、特に子供が有害サイトにアクセスするのを制限するURLフィルタリングソフトやデスクトップ・ファイアウォール製品があるが、これらをアンチウイルス製品にバンドルした製品も多く、個人消費者向け情報セキュリティ製品市場のほとんどはアンチウイルス市場の数字でカバーできていると見て大きな誤差はないであろう。これらを含むウイルス対策製品の個人向け市場については、PCとインターネットの普及率の上昇と相俟って、ここ当面は引き続き高い成長を維持すると予測される。

個人消費者向け製品の供給は大手ウイルス対策製品ベンダーが平行して手がけるケースが多いが、一部消費者向けソフトという切り口のビジネスモデルからの参入もある。

フィッシングが新たな脅威として認識されだしたことに伴い、対策製品が登場しつつある。国産プレイヤーの参入も見られ、今後本格的に市場が形成されていくものと思われる。

【市場規模とその推移】

表11に国内セキュアコンテンツ管理製品の市場規模実績推定値と予測値を示す。

表 11 国内セキュアコンテンツ管理製品市場規模 実績と予測

製品別出荷金額（百万円）	平成 15 年度	平成 16 年度	平成 17 年度
アンチウイルス・アンチワーム・ソフトウェア （企業向けライセンスタイプ）	33,549	37,803	42,322
アンチウイルス・アンチワーム・ソフトウェア （個人ユーザ向けパッケージタイプ）	8,278	10,217	13,334
アンチスパム・ソフトウェア/アプライアンス	1,780	692	606
URL フィルタリングソフト/アプライアンス	480	528	602
アンチフィッシングソフト・アプライアンス	0	0	60
メールフィルタリング・ソフトウェア	871	1,022	1,160
その他のセキュアコンテンツ管理製品	458	519	587
セキュアコンテンツ管理製品 計	45,418	50,781	58,671
<b>製品別構成比</b>			
アンチウイルス・アンチワーム・ソフトウェア （企業向けライセンスタイプ）	73.9%	74.4%	72.1%
アンチウイルス・アンチワーム・ソフトウェア （個人ユーザ向けパッケージタイプ）	18.2%	20.1%	22.7%
アンチスパム・ソフトウェア/アプライアンス	3.9%	1.4%	1.0%
URL フィルタリングソフト/アプライアンス	1.1%	1.0%	1.0%
アンチフィッシングソフト・アプライアンス	0.0%	0.0%	0.1%
メールフィルタリング・ソフトウェア	1.9%	2.0%	2.0%
その他のセキュアコンテンツ管理製品	1.0%	1.0%	1.0%
セキュアコンテンツ管理製品 計	100.0%	100.0%	100.0%
<b>対前年度比成長率</b>			
アンチウイルス・アンチワーム・ソフトウェア （企業向けライセンスタイプ）	-	12.7%	12.0%
アンチウイルス・アンチワーム・ソフトウェア （個人ユーザ向けパッケージタイプ）	-	23.4%	30.5%
アンチスパム・ソフトウェア/アプライアンス	-	-61.1%	-12.5%
URL フィルタリングソフト/アプライアンス	-	9.9%	14.0%
アンチフィッシングソフト・アプライアンス	-	-	-
メールフィルタリング・ソフトウェア	-	17.2%	13.5%
その他のセキュアコンテンツ管理製品	-	13.4%	13.0%
セキュアコンテンツ管理製品 計	-	11.8%	15.5%

アンチウイルス製品は情報セキュリティ対策ツールの中では最も普及の進んだツールであり、平成 15(2003)年度において、主として企業向け製品で 335 億円、主として個人ユーザ向け製品で 83 億円、合計 418 億円に達すると推定される。この領域が単一セグメントとしては「情報セキュリティツール」市場の中で最大のものである。また、「情報セキュリティ

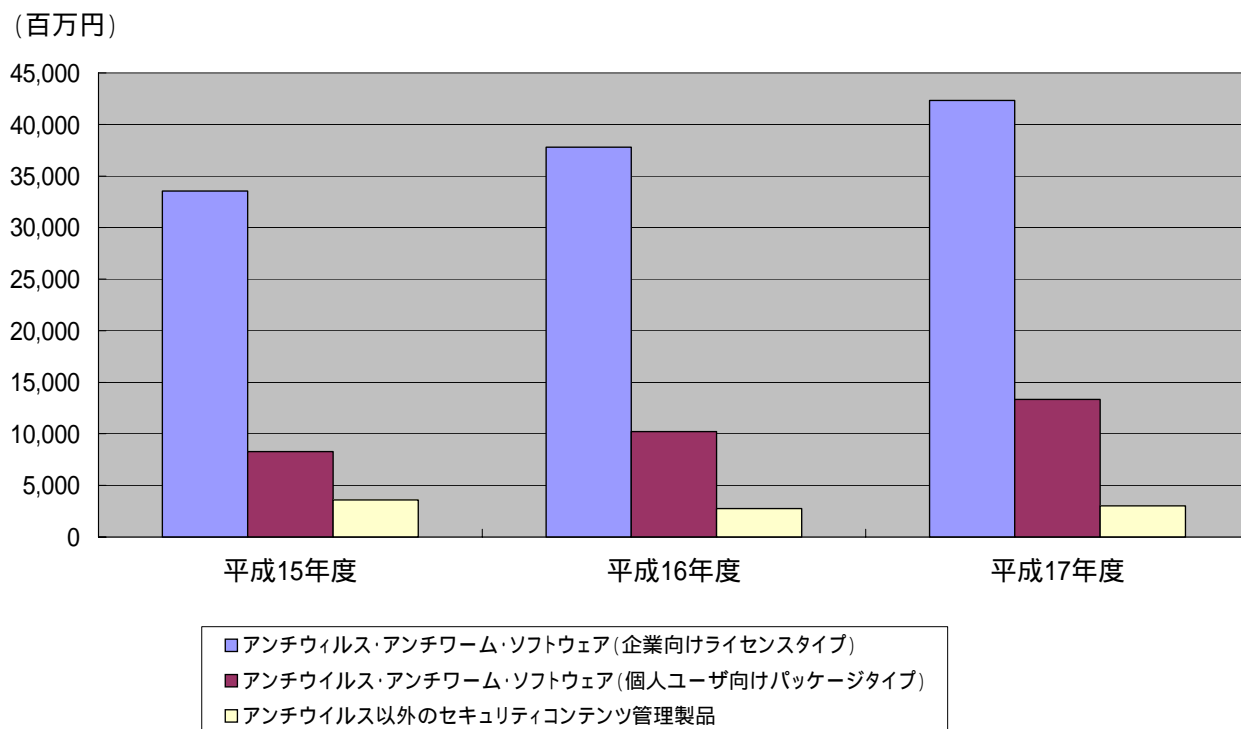
「ツール」市場の中でほとんど唯一、法人向けだけでなく、個人向け・消費者向けの市場が形成されている。

主として法人、公共機関向けである「アンチウイルス・アンチワーム・ソフトウェア（企業向けライセンスタイプ（GW型、サーバ型、クライアント型の全てを含む）」）」セグメントの経年推移を見ると、平成16(2004)年度が378億円で前年度比伸び率が12.7%、平成17(2005)年度が423億円で同12.0%となり、「情報セキュリティツール」市場全体と比較すると、より緩やかな伸びとなる。

個人向けアンチウイルス製品市場は、法人向けより高い成長率で拡大している。「アンチウイルス・アンチワーム・ソフトウェア（個人ユーザ向けパッケージタイプ（FW、IDS機能併設型を含む）」）」セグメントでは、平成15(2003)年度83億円の市場から、平成16(2004)年度は23.4%伸びて102億円に達したものと見られ、更に翌年には30.5%と一段の伸びを示して133億円に達すると予測される。

アンチウイルス製品以外のセグメントはかなり金額的に限られたものとなる。メールフィルタリング（選別）が前述のように情報漏えい対策として今後伸びが期待される場所であるが、平成15(2003)年度では9億円弱に留まっている。また、フィッシング詐欺の広がりに対して対策の必要性が指摘されており、対応する製品・サービスの供給が期待される場所であるが、平成17(2005)年度には具体化が期待され、わずかではあるが予測数字にも反映される結果となっている。

図 7 国内セキュアコンテンツ管理製品市場推移



#### 7.2.6. 暗号製品市場

##### 【製品の特性と市場の動向】

暗号技術はPKIやVPNの形で、あるいは各種情報セキュリティ製品の内部処理やネットワーク通信の場で、様々な形で使われており、それらを暗号の市場規模に含めるとかなりの数字になる可能性があるが、暗号化そのものを基本価値とする製品は、暗号化によるデータの保護を目的としたものに限られてくる。そのように定義したカテゴリの中のセグメンテーションとしては、暗号化対象によりメールとファイルのほぼ二つに大別できる。このほかにはディスク単位での暗号化やUSBメモリへの格納と暗号化を一体化したものなどがあるが、カテゴリとしてはファイル暗号に含めている。その他には他の製品やアプリケーションに組み込むためのミドルウェアや暗号化モジュールが市場を形成している。

いずれにせよ、これら全ての暗号製品の合計で、平成15(2003)年度において約36億円と、限定的なマーケットとなっている。ただし、メールフィルタリング(選別)と同じように、今後情報漏えい対策手段としての暗号化は積極的に活用されるようになって見られる。そ

の場合、単なる暗号化ではなく、暗号・復号キーをアクセス権と結び付けて管理することにより、権利のない人に対しては防御すると同時に権利を有する人にはその権利の範囲で（例えば画面参照だけ、印刷可能、複製可能、編集可能といった区分）利用を保証するといった管理、いわゆる DRM（Digital Rights Management）といった形での利用が普及する兆しを見せている。

既に一部企業では、個人情報保護法対策として、外部持ち出し可能な PC には全て暗号化ソフトウェアを導入している企業もあり、比較的容易に実施可能な対策として暗号化ソフトウェアの利用が進展するものと予測される。

暗号製品の供給サイドは、比較的小規模の事業が多いことと、国産ベンダーの参入が活発であることが特徴と言える。これは、ネットワーク技術と違い、暗号技術では国内メーカーの技術開発も国際的に高いレベルにあることと、その使う場がアプリケーションに近いところにあることが影響していると考えられる。暗号技術は国家レベルの安全保障とも関わるため、特に初期においては輸出入の規制が厳しかったことも影響しており、ネットワーク機器に比べると閉じたマーケットの性格を持つ。ファイルの入出力のたびに操作が必要であるような要素もあり、誰でも簡単に使えるインターフェイスが求められることから、国産ベンダーが取り組みやすい領域であることも一つの理由であろう。

この分野は USB キーとの組合せ等、ベンチャーが簡単な製品で参入しやすい一方、データの利用権をワークフローと絡めて全社で一元管理するレベルではシステム対応能力も必要で、国内大手ベンダーやシステムインテグレータの出番となる。単なるデータ保護から業務と一体化した情報漏えい対策へ向けて、暗号応用の領域を超えて市場が広がる可能性を秘めたカテゴリである。

【市場規模とその推移】

表12に国内暗号製品の市場規模実績推定値と予測値を示す。

表 12 国内暗号製品市場規模 実績と予測

製品別出荷金額（百万円）	平成 15 年度	平成 16 年度	平成 17 年度
メール暗号化製品	784	943	1,016
ファイル暗号化製品	1,533	2,059	2,322
暗号化ミドルウェア	856	815	930
ファイル/データアクセス管理製品	356	429	580
その他の暗号製品	36	43	45
暗号製品 計	3,565	4,289	4,893
<b>製品別構成比</b>			
メール暗号化製品	22.0%	22.0%	20.8%
ファイル暗号化製品	43.0%	48.0%	47.5%
暗号化ミドルウェア	24.0%	19.0%	19.0%
ファイル/データアクセス管理製品	10.0%	10.0%	11.9%
その他の暗号製品	1.0%	1.0%	0.9%
暗号製品 計	100.0%	100.0%	100.0%
<b>対前年度比成長率</b>			
メール暗号化製品	-	20.3%	7.7%
ファイル暗号化製品	-	34.3%	12.8%
暗号化ミドルウェア	-	-4.8%	14.1%
ファイル/データアクセス管理製品	-	20.3%	35.3%
その他の暗号製品	-	20.3%	4.9%
暗号製品 計	-	20.3%	14.1%

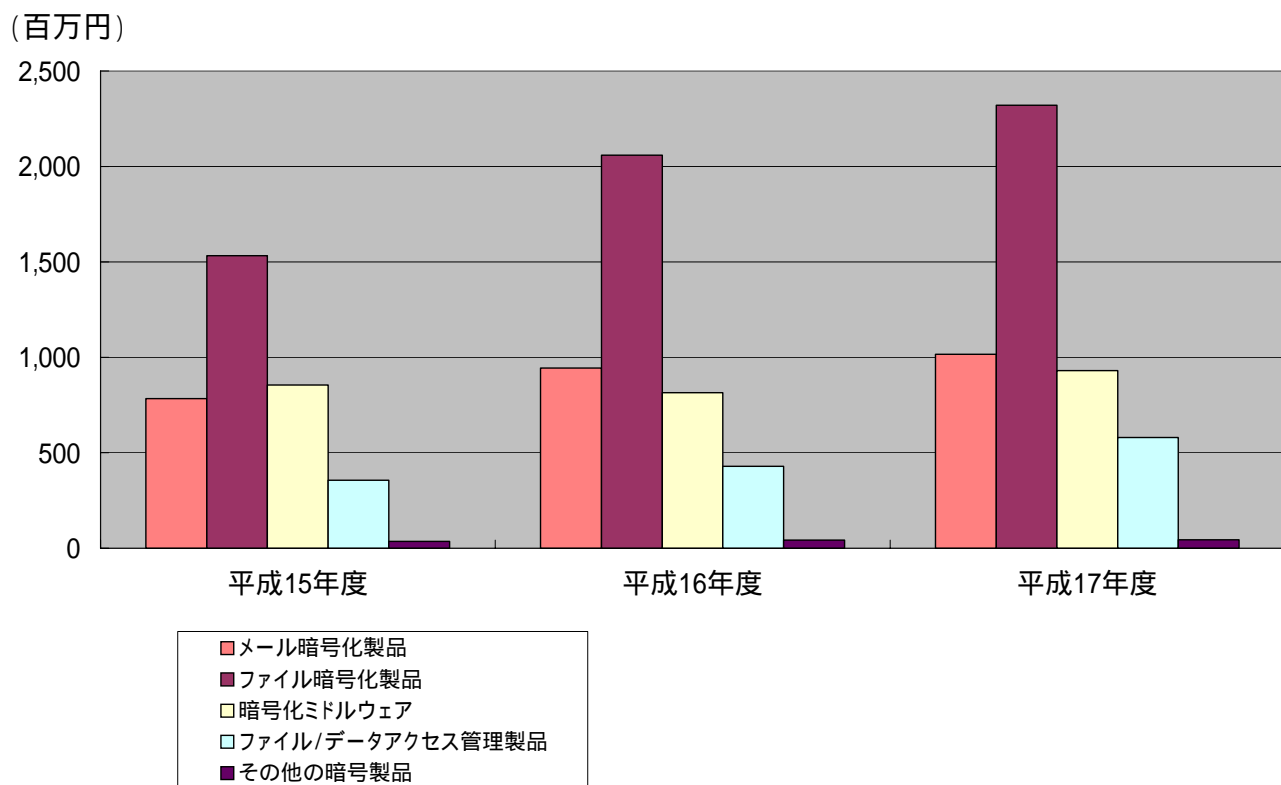
国内暗号製品市場は平成 15(2003)年度実績で約 36 億円であったと推定する。その市場規模推移も緩やかなものと予測され、平成 16(2004)年度は 20.3%の伸びで 43 億円、平成 17(2005)年度は 14.1%と伸び率も鈍化して市場規模は 49 億円と予測する。

情報漏えい対策としての暗号化は個人情報保護法の施行をにらんで平成 16(2004)年度には相当採用が進んだと見られる。その主力は「ファイル暗号化製品」で、同年度には 34.3%の成長率で 21 億円程度の規模になったものと見られる。ただ、翌平成 17(2005)年度には伸び率は 12.8%とほぼ市場平均並みのものになる。「ファイル/データアクセス管理製品」は暗号製品の中で最も高い伸びを示す。これは上述のように、単に暗号化だけでなく、PC やファイルの操作に関してコントロール（管理・制御）ができることから、盗難や紛失だけでなく、内部者の不正の防止や抑制に対する効果を期待してのものであると考えられる。市場が形成されてからの期間が短いため、平成 15(2003)年度で 4 億円弱の市場であるが、平成 16(2004)年度は対前年度比率 20.3%、平成 17(2005)年度は対前年度比率 35.3%と急伸びして 6 億円弱まで拡大するものと期待される。

全体としては、情報保護の観点から需要の伸びは期待できるものの、市場規模は当面限定

的なもので推移するという予測結果となった。

図 8 国内暗号製品市場推移



## 8. 国内情報セキュリティサービス市場の分析

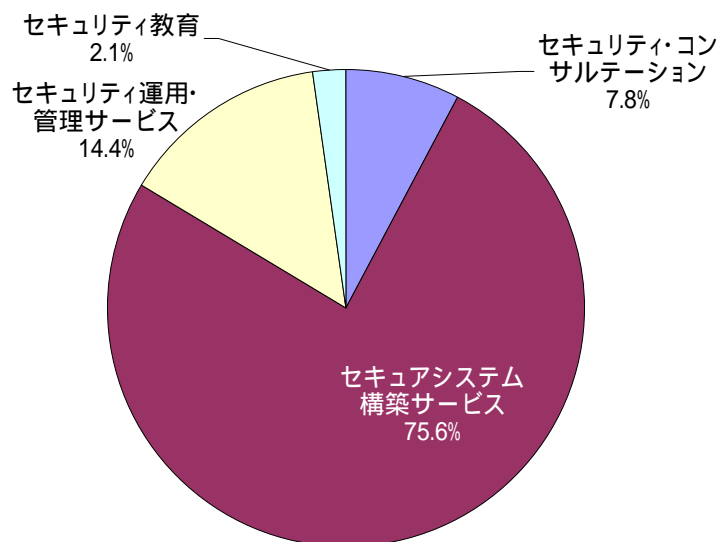
### 8.1. 情報セキュリティサービス市場の全体概要

「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、「情報セキュリティツール」がハードかソフトかは別として、形のある商品、既製品のイメージであるのに対して、全くソフト的なビジネス、形のない、個別対応型のいわゆる役務契約型のサービス提供と定義している。

このカテゴリには、大分類として「セキュリティ・コンサルテーション」<sup>1)</sup>、「セキュアシステム構築サービス」<sup>2)</sup>、「セキュリティ運用・管理サービス」<sup>3)</sup>、「セキュリティ教育」の4カテゴリを定義した。ツールに直接関連する保守・サポートや更新サービスはツールの市場に付帯するものとしてツール側に含め、サービス分野には入れていない。ただし、ツール類を導入するに際しての使用条件や各種パラメータの設定といった導入支援サービスについては、それがツールと独立して価格付けされる場合にはサービス市場としてカウントするものとしている。似たケースで、特定のツールの納品に際して納入業者が無償で簡単な設定やチューニングを行うものについてはツールの対価の一部という仕分になる。

表 13 より、平成 15(2003)年度の「情報セキュリティサービス」市場規模は 2,347 億円と推定される。平成 16(2004)年度は、「情報セキュリティサービス」市場全体で対前年度伸び率 27.2%と大きな伸びを示した。このカテゴリの最大セグメントである「セキュアシステム構築サービス」は全体より低い伸びに留まったが、次に大きなセグメントである「セキュリティ運用・管理サービス」がほぼ「情報セキュリティサービス」市場全体と同じ伸び率であり、「セキュリティ・コンサルテーション」(57.1%増)、「セキュリティ教育」(85.0%増)といった、金額では比較的小さいカテゴリが大きな伸びを示して、全体の成長を引っ張っていく結果となっている。

図 9 平成 15 年度国内情報セキュリティサービス構成比



「情報セキュリティサービス」市場の中で最大のカテゴリは「セキュアシステム構築サービス」で、平成 15(2003)年度実績推定値で 1,775 億円と、全体の 75.6%を占めた。これは、「セキュアシステム構築サービス」のカテゴリに含まれる「IT セキュリティシステムの導入・導入支援」が単一のセグメントで 1,006 億円と突出して大きな金額となっていることによる。それに加え、このカテゴリを構成する他の三つの中分類セグメント、「IT セキュリティシステムの設計・仕様策定」、「セキュリティ製品の選定・導入支援」、「その他のセキュアシステム構築サービス」も他のカテゴリを構成するセグメントに比べて大きな額となっており、その結果「情報セキュリティサービス」市場全体の 4 分の 3 を占めるに至っている。ただ、このカテゴリはそれを構成するセグメントも共に比較的ゆるやかな伸び率を示しており、平成 16(2004)年度で対前年度比 22.5%、平成 17(2005)年度で前年度比 11.6%と、「情報セキュリティサービス」市場全体の伸び率を下回っている。その結果、平成 17(2005)年度では「情報セキュリティサービス」市場全体に占める割合も 71.7%まで低下すると予測される。

次に大きなカテゴリは「セキュリティ運用・管理サービス」で、平成 15(2003)年度実績は 339 億円と推定される。このカテゴリは、顧客のネットワークにセンサを設置し、あるいは顧客の社内 LAN に設置したファイアウォール等の装置の情報を直接吸い上げ、顧客の

ネットワークのセキュリティ状態を監視したり、インシデント発生時の対応を支援したりするサービスが主なものである。外部からの攻撃等によるネットワーク上のトラブルは、専門の技術者でないと対応が難しく、専門家のサービスを利用すべきという判断をする企業も多く、古くからこの種のサービスが専門事業者によって提供されている。このほか、リアルタイムの監視まではしなくても定期的にログ解析を外部委託してネットワークの状態を把握したり、外部ネットワークからの擬似攻撃により潜在的弱点をチェックしたり、といったサービスがこのカテゴリに含まれる。

「セキュリティ運用・管理サービス」に関しては、1990年代後半から、ネットワークインテグレーション分野で情報セキュリティに特化した企業等がプロフェッショナルサービスとして展開してきており、比較的長い歴史を持つが、その主要顧客は「餅は餅屋」という割り切った経営判断をする一部企業に限られてきたと言える。それがここへ来て、複雑化するネットワーク、高度化し頻度が高まる攻撃、そしてOSやネットワークの脆弱性発生（発見）の深刻化等を背景に、専門サービスに対してアウトソーシング化して積極活用しようという判断が増えてきている。そのようなユーザ側の動向に加えて、ベンダーから提供される監視サービスなどが数年前までの需要低迷期に競争が促進され、サービス品質が高まると共に価格が相当程度低下したことも奏功して、漸く拡大期を迎えつつあると言える。

その結果平成16(2004)年度は対前年度比26.8%と比較的高い伸びで430億円に達し、平成17(2005)年度は対前年度比13.2%とやや鈍化するが、「情報セキュリティサービス」市場全体並みの伸びを確保して486億円程度になると予測される。

金額規模は平成15(2003)年度実績で184億円とそれほど大きくないが、ここに来て需要が高まっているのが「セキュリティ・コンサルテーション」である。特に「セキュリティ運用管理全般のコンサルテーション」、「セキュリティポリシー構築支援」、「セキュリティ認証取得支援サービス」等、情報セキュリティの技術の側面よりは経営管理の視点から専門家の支援を活用する動きが顕在化して来た。ツールのようにモノを伴わないし、SIのように工数も大きくなりたくないために、金額はそれほど大きくなりませんが、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。

「セキュリティ・コンサルテーション」に関しては、情報漏えい対策や個人情報保護法対応による効果で、従来は需要の少なかった産業分野でも広く新規需要が発生している。特に小売業（典型的には通信販売業等）、信販業、旅行その他のサービス業等、個人消費者を多数顧客に抱える業態では、従来IT依存度がそれほど高くなく、高度なネットワーク管理や情報セキュリティ対策に関心が低かったものが、個人情報保護法の施行を前にして対応を急いでおり、その際経験や知識を補う意味で、あるいは権威のお墨付きを得る意味で、セキュリティコンサルティングや診断・監査を利用するケースが目立って増えている。この発想を一歩進めてプライバシーマークやISMS認証の取得に踏み切るところも多く、そ

の取得支援サービスや認証サービスの需要も高い伸びを示している。こうした需要に押し上げられて、平成 16(2004)年度の「セキュリティ・コンサルテーション」市場は前年度比 57.1%と極めて高い伸びを示して 289 億円に達したと見られる。この傾向は、全産業の一定規模以上の事業者において対策が一巡するまでは継続するものと考えられ、平成 17(2005)年度も対前年度比 22.8%と比較的高い伸びを維持して 355 億円に達し、平成 15(2003)年度比ほぼ倍増の規模に達するものと予測される。

「セキュリティ教育」は平成 15(2003)年度実績推定値が 49 億円に留まり、構成比も 2.1%と極端に小さいが、これはこの分野が立ち上り期にあるためである。従来情報セキュリティは情報システム部門の専管事項のような理解がされており、一般ユーザに理解させる要素には余り関心が向いていなかった。それに対し、一つはウイルス被害の拡大と社員各自の端末（会社資産の場合も個人資産の場合も）からの感染の頻発、もう一つは個人情報漏えい対策の 2 面から、社員一人一人に対する教育の必要度と重要度が認識され出し、またそれに対応して教育コンテンツ（情報の内容）とサービスの提供も活発化しだしている。

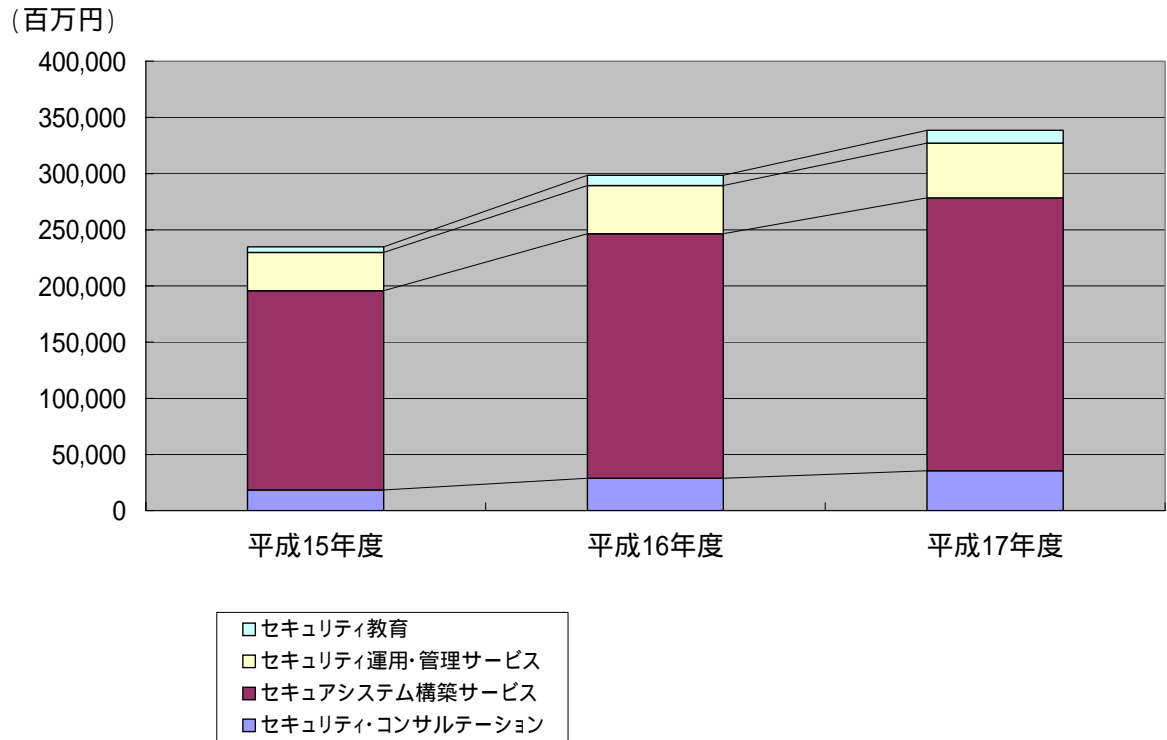
この需要サイドの動きを反映して、「セキュリティ教育」市場は平成 16(2004)年度には前年度比 85%増と急進して 91 億円規模に至ったものと推測する。前述したように、個人情報保護法完全施行を前にして、やはり情報漏えい対策のために、営業や保守サービスなど、一般社員の末端までの情報セキュリティ教育の徹底・浸透の必要性が認識され、教育需要が急速に高まった結果であると見られる。この傾向は平成 17(2005)年度にかけても持続すると見られ、同年度も引き続き 28.3%と高い伸びを続けて 117 億円の市場規模に達すると予測する。

いわゆる情報セキュリティ・リテラシーは、顧客リストの管理等、日々の業務に密着して意識しなければ事故につながりかねない要素が多く、単なる通達や指導だけでは身につかない。従って、集合教育等で直接事例やロールプレイを取り入れた教育も必要だが、一般企業ではなかなか手が回らず、また教材を用意する知識・ノウハウも乏しい。そこで、教育コンテンツを外部調達したり、教育を外部サービスに依存したりする判断が広がりつつある。また、全社員向けということで対象が膨大になるに対するコスト増大対策や、教材の専門化の観点から、eラーニングを導入する動きも、大企業を中心に広がっている。これはネットワークを介してサーバにアクセスして教育プログラムを走らせて自習する仕組みであるが、本人の仕事の都合に合わせて時間を選べることや、空き時間に少しずつ学ぶこと、分らなければ繰り返し視聴できることなどの利点がある。更に、テストと組合せ、ログを管理することで社員一人一人の進捗度や履修の有無を全て把握できる点でも優れた手法であり、今後供給サイドの充実と共に需要が伸びるものと期待される。供給についてはコンテンツ制作や eラーニング供給・管理システムといった特殊要因から、大手情報セキュリティベンダー、大手 SI ベンダー、教育の専門事業者がその中心となるであろう。

表 13 国内情報セキュリティサービス市場規模 実績と予測

サービス別出荷金額（百万円）	平成 15 年度	平成 16 年度	平成 17 年度
セキュリティ・コンサルティング	18,409	28,923	35,523
セキュアシステム構築サービス	177,491	217,485	242,820
セキュリティ運用・管理サービス	33,874	42,953	48,609
セキュリティ教育	4,912	9,088	11,658
合計	234,686	298,448	338,611
<b>サービス別構成比</b>			
セキュリティ・コンサルティング	7.8%	9.7%	10.5%
セキュアシステム構築サービス	75.6%	72.9%	71.7%
セキュリティ運用・管理サービス	14.4%	14.4%	14.4%
セキュリティ教育	2.1%	3.0%	3.4%
合計	100.0%	100.0%	100.0%
<b>対前年度比成長率</b>			
セキュリティ・コンサルティング	-	57.1%	22.8%
セキュアシステム構築サービス	-	22.5%	11.6%
セキュリティ運用・管理サービス	-	26.8%	13.2%
セキュリティ教育	-	85.0%	28.3%
合計	-	27.2%	13.5%

図 10 国内情報セキュリティサービス市場推移



## 8.2. 情報セキュリティサービス市場のカテゴリ別分析

### 8.2.1. セキュリティ・コンサルテーション市場

#### 【市場の特性と動向】

このカテゴリには規模順に書くと「セキュリティ運用管理全般のコンサルテーション」<sub>1</sub>、「セキュリティポリシー構築支援」<sub>2</sub>、「セキュリティ認証取得支援サービス」<sub>3</sub>、「セキュリティ監査サービス」<sub>4</sub>、「セキュリティ診断サービス」<sub>5</sub>、「その他のセキュリティ・コンサルテーション」<sub>6</sub>、「セキュリティ認証・審査機関(サービス)」<sub>7</sub>の7セグメントを定義した。上位3セグメントが50億円以上、次の3セグメントが20億円程度、最後の審査認証機関はその性格上1億～2億円と限定的・特殊なセグメントと言える。

平成15(2003)年度以降多発している大規模個人情報漏えい事件と、それによる実損を伴う経営へのインパクトの顕在化により、経営者の間によく情報セキュリティへの関心が定着して来た感がある。これに個人情報保護法が提起した企業の個人情報保護管理責任が拍車をかける形で、情報セキュリティ対策が経営の中に位置付けられるようになった。そして、経営が情報セキュリティに取り組むに際してプロの知識とノウハウに頼るべきだとの判断もまた自然に出てくる中で、コンサルテーションに対するニーズが顕在化するという流れをたどっていると見られる。

「セキュリティ運用管理全般のコンサルテーション」<sub>1</sub>、「セキュリティポリシー構築支援」<sub>2</sub>、「セキュリティ認証取得支援サービス」という領域は、企業が経営の次元で情報セキュリティ構築に取り組む際に必要とするプロフェッショナルサービスで、その規模が相対的に大きく、伸びも比較的高いということは、企業が本腰を入れて、経営の視点から情報セキュリティに取り組みだしたことを意味するものと解釈できる。この3セグメントに需要が集まっているのも、総合的な情報セキュリティ対策の立案、その骨格を形成するセキュリティポリシーの確立ニーズ、そして、情報セキュリティの管理体制を客観的基準に照らして適合性を確認し証明する公的認証の取得という一連のニーズの高まりを反映したものと言える。この流れは今後、確立した情報セキュリティ対策とその運用の維持管理、定期点検と内部・外部監査へとつながると期待される。そうなると今は比較的小さいセグメントである情報セキュリティ診断や情報セキュリティ監査サービスのニーズも高まってくると予想される。

プライバシーマークの制度は1998年には制定され、ISMS認証もISO17799/BS7799のJIS化と一体のものとして2002年度には運用が始まっている。更に経済産業省が中小情報処理事業者の育成と品質確保を目指して実施していた「情報処理サービス業情報システム安全対策実施事業所認定制度」による認定が、平成13(2001)年度をもって終了したことに伴い、ISMS認証制度と相互補完的に、特に体制整備に外部支援を必要とするような中小事業者や自治体等への対応を意識して、情報セキュリティ監査制度が、平成15(2003)年度

から始まっている。これらの認証制度はその趣旨としては、企業等の個人情報管理体制や情報セキュリティ管理体制の充実を目指して、一定の基準と審査規定を設けて認証を与えるものであるが、ややもすると認証取得が自己目的化する傾向にあった。それが体制構築を主目的に掲げる理解が浸透し、認証取得支援よりは情報セキュリティ運用管理全般のコンサルティングを選好する方向になってきていることが、数字にも反映していると推測できる。

なお、個人情報保護法が、委託先における個人情報保護に関する委託元の管理責任を規定していることから、個人情報を扱うシステム等の受託企業に対して、発注元企業がプライバシーマークの取得を求める動きが、特に平成 16(2004)年度において目立つようになった。そのような関心の高まりを反映して、平成 16(2004)年度には一時的に同マークの認定申請が付与機関である財団法人日本情報処理開発協会 ( JIPDEC ) に短期間に集中するというような経緯も見られた。

セキュリティ・コンサルティングの供給主体は大きく 3 パターンに分類できる。一つ目は、大手のシステムインテグレータが、システム設計や構築の上流として情報セキュリティについても経営レベルのコンサルティングを提供するケース。二つ目は、監査法人系その他の経営コンサルティング企業が情報セキュリティに関するコンサルティングを提供するケース。特に ISMS 等の管理システム構築や監査といったサービスはこの業態となじみやすい。そして三つ目は、専門のベンダーが情報セキュリティのインテグレーション、監査、検査、診断等を専門に提供するケースである。この類型には、純粹のコンサル業態から、運用管理等も手がけるパターン、更にはツールの販売や導入・実装も同時に行うパターン等もある。いずれも国産ベンダーを中心に顧客密着型のサービスを提供するモデルである。

【市場規模とその推移】

表14に国内のセキュリティ・コンサルテーション市場規模の実績推定値と予測値を示す。

表 14 国内セキュリティ・コンサルテーション市場規模 実績と予測

市場規模（百万円）	平成 15 年度	平成 16 年度	平成 17 年度
セキュリティポリシー構築支援	4,240	6,158	7,051
セキュリティ運用管理全般のコンサルテーション	6,891	13,209	16,551
セキュリティ監査サービス	782	1,987	2,576
セキュリティ診断サービス	865	1,231	2,003
セキュリティ認証・審査機関（サービス）	96	154	175
セキュリティ認証取得支援サービス	4,845	5,169	5,198
その他のセキュリティ・コンサルテーション	691	1,015	1,969
セキュリティ・コンサルテーション 計	18,409	28,923	35,523
<b>サービス別構成比</b>			
セキュリティポリシー構築支援	23.0%	21.3%	19.8%
セキュリティ運用管理全般のコンサルテーション	37.4%	45.7%	46.6%
セキュリティ監査サービス	4.2%	6.9%	7.3%
セキュリティ診断サービス	4.7%	4.3%	5.6%
セキュリティ認証・審査機関（サービス）	0.5%	0.5%	0.5%
セキュリティ認証取得支援サービス	26.3%	17.9%	14.6%
その他のセキュリティ・コンサルテーション	3.8%	3.5%	5.5%
セキュリティ・コンサルテーション 計	100.0%	100.0%	100.0%
<b>対前年比成長率</b>			
セキュリティポリシー構築支援	-	45.2%	14.5%
セキュリティ運用管理全般のコンサルテーション	-	91.7%	25.3%
セキュリティ監査サービス	-	154.2%	29.7%
セキュリティ診断サービス	-	42.4%	62.7%
セキュリティ認証・審査機関（サービス）	-	60.3%	13.6%
セキュリティ認証取得支援サービス	-	6.7%	0.6%
その他のセキュリティ・コンサルテーション	-	46.9%	94.0%
セキュリティ・コンサルテーション 計	-	57.1%	22.8%

平成 15(2003)年度の「セキュリティ・コンサルテーション」市場は全体で 184 億円の規模であった。このうち比較的規模の大きなセグメントは「セキュリティ運用管理全般のコンサルテーション」69 億円、「セキュリティ認証取得支援サービス」48 億円、「セキュリティポリシー構築支援」42 億円の三つである。

平成 16(2004)年度には、「セキュリティ・コンサルテーション」市場は、前年度比 57.1% 増と急拡大を見せる。背景に度重なる情報セキュリティ事件・事故と、個人情報保護法により明示的に示されることになった企業の情報管理責任に対する認識の高まりがあると考えられる。これに対応するように、供給サイドでも、平成 16(2004)年度は、大手中堅システムインテグレータ、情報セキュリティベンダーが情報セキュリティ・コンサルテーションのサービス商品を充実させ、営業を強化した。

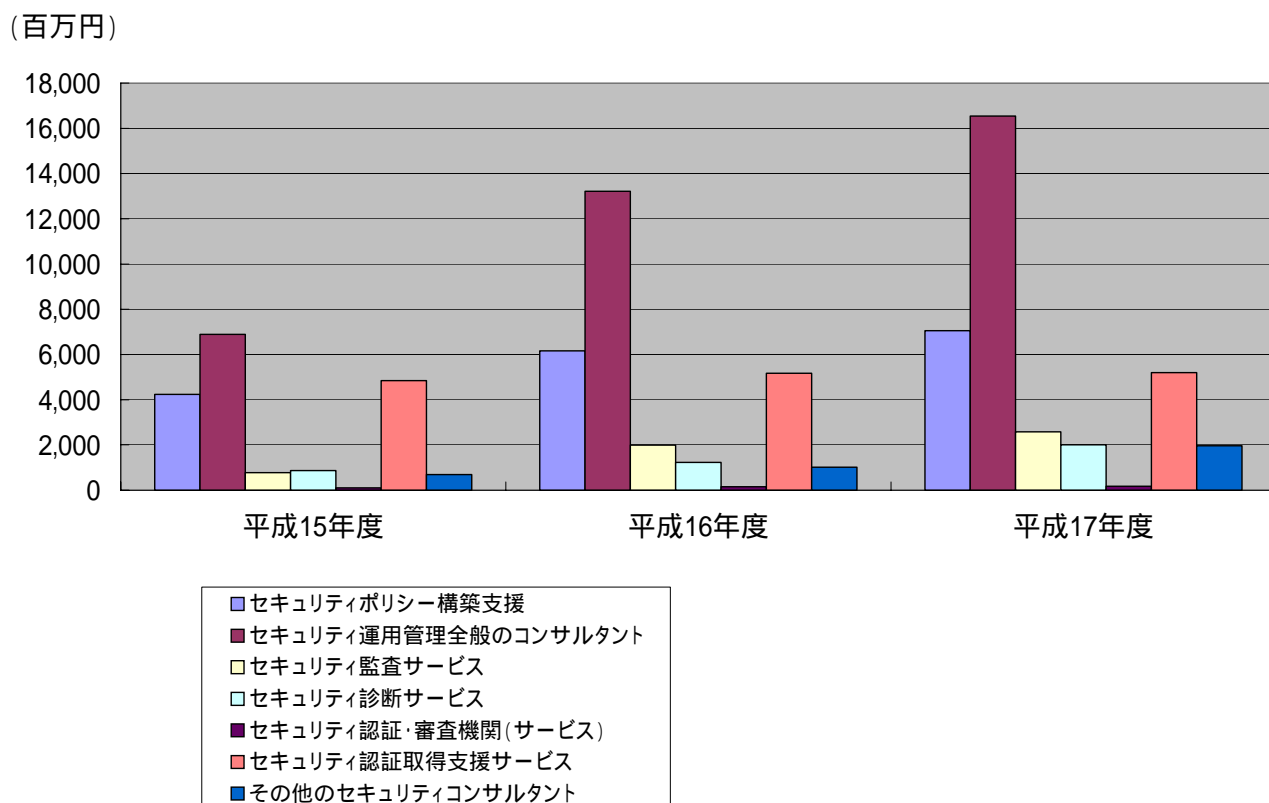
平成 17(2005)年度も、伸び率は鈍化するとは言え 22.8%と比較的高い成長を維持し、全体で 355 億円と、平成 15(2003)年度と比較して倍に近い規模に達すると予測される。

セグメント別の市場規模と成長率を見ると、最大セグメントである「セキュリティ運用管理全般のコンサルテーション」が平成 15(2003)年度の 69 億円から、平成 16(2004)年度には実に 91.7%伸びて 132 億円に達し、平成 17(2005)年度には引き続き 25.3%の高い伸びで 166 億円に達すると見られる。「セキュリティポリシー構築支援」は平成 15(2003)年度は 42 億円で規模としては 3 位であったが平成 16(2004)、平成 17(2005)年度の伸び率が各々 45.2%、14.5%と、これも比較的高い成長を続けて 2 位を逆転し、70 億円規模に達するものと想定している。一方、平成 15(2003)年度には 48 億円と 2 位であった「セキュリティ認証取得支援サービス」が例外的に 6.7%、0.6%とほとんど伸びないと見られ、平成 17(2005)年度の市場規模は 52 億円という予測になった。

「セキュリティ監査サービス」、「セキュリティ診断サービス」も各々平成 15(2003)年度には 8 億円、9 億円と極めて限られた市場であったと見られるが、平成 16(2004)年度から平成 17(2005)年度にかけて著しく高い伸びを示して、各々 26 億円、20 億円の規模に達すると予測できる。これも上記と同様、経営が情報セキュリティの管理体制充実を目指す中で、第三者による客観的評価を積極的に活用しようとする姿勢の表れと解釈できる。

このことが「セキュリティ認証・審査機関(サービス)」の平成 16(2004)年度の 60.3%という高い伸びに反映されていると見られるが、この一時要因が過ぎれば平常ベースに復するであろうことを、同セグメントの平成 17(2005)年度の伸び率の予測 13.6%（「情報セキュリティサービス」市場全体とほぼ同じ）が物語っている。なお、このセグメントは審査・認証そのものを行うサービスであるので、おのずと市場規模は限定され、1 億～2 億円程度と見積られる。

図 11 国内セキュリティ・コンサルテーション市場推移



### 8.2.2. セキュアシステム構築サービス市場

#### 【市場の特性と動向】

「セキュアシステム構築サービス」のカテゴリには、「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」、「セキュリティ製品の選定・導入支援」、「その他のセキュアシステム構築サービス」の 4 セグメントが含まれる。各セグメント共、他の「情報セキュリティサービス」カテゴリを構成するセグメントに比べて市場規模が大きい。中でも「IT セキュリティシステムの導入・導入支援」は 1,006 億円と、このセグメント単独で 1,000 億円を超えており、極めて大きな市場を形成している。

この要因としては、このカテゴリが最もシステムインテグレーションサービスに近く、システムインテグレーション市場のうち「情報セキュリティの確立・導入を主目的とした SI (システムインテグレーション) サービス部分」と定義できる性格を持つからであると推測される。従来から特に大手 SI 事業者が手がけるシステムでは情報セキュリティ対策も一体に組み込まれたものとして導入するケースが多く、そのような SI 案件のうち情報セキュリティ対応部分を抜き出して推計・集計することにより、市場規模が大きく表示されるこ

とになる。が、情報セキュリティに関わるサービスを市場として見るときに、このカテゴリを除外することは逆に市場の実態を見えにくくすることにもなるので、情報セキュリティサービスの市場を考える場合外すことのできないアイテムである。

このカテゴリは、情報セキュリティツールを情報システム上正しく稼働させるためのインテグレーションサービスという関係になるが、「情報セキュリティツール」市場が平成15(2003)年度で1,260億円に対してそのインテグレーションサービスに要する費用が1,775億円、約1.4倍という比率となる。ツールの難易度、システムの規模によってツール対インテグレーションの比率のばらつきは大きいですが、全体を押しなべると概ね妥当な比率と考えられる。

また、「セキュリティ製品の選定・導入支援」が279億円と、相当大きな市場を形成しているところにも市場の特徴があると見られる。やはり情報セキュリティ対策製品という判断基準の難しい技術領域では、専門サービスに対するニーズが強いことを示すものとして注目される。このカテゴリは、市場規模が押しなべて突出して大きい一方、伸び率は平均並み以下という、やや成熟した特性を見せている。その中であって、この「セキュリティ製品の選定・導入支援」サービスのセグメントだけは平成16年度に例外的に大きく伸びたことが確認できる。やはり、企業における情報セキュリティへの取り組み姿勢の面で、専門家のサービスを活用してきちんとした対策を施すという考え方が浸透した結果と考えられる。

前述した通り、今後発生するシステム構築案件は全て何らかのセキュリティ要素を包含する。その内どこまでをセキュアシステム構築サービスとして計測するか、という統計技術的な問題は残るものの、規模、成長率とも安定した市場として存続するものと見られる。

供給主体としてはその性格上、システムインテグレータがその中心となる。これにネットワークインテグレータや情報セキュリティツールの販売業者が、ネットワーク機器や情報セキュリティツール販売の延長線上で構築サービスを提供するビジネスモデルが続く。

【市場規模とその推移】

表15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示す。

表 15 国内セキュアシステム構築サービス市場規模 実績と予測

市場規模（百万円）	平成 15 年度	平成 16 年度	平成 17 年度
IT セキュリティシステムの設計・仕様策定	30,222	36,314	42,396
IT セキュリティシステムの導入・導入支援	100,571	116,865	130,337
セキュリティ製品の選定・導入支援	27,938	42,446	47,363
その他のセキュアシステム構築サービス	18,760	21,860	22,725
セキュアシステム構築 計	177,491	217,485	242,820
<b>構成比</b>			
IT セキュリティシステムの設計・仕様策定	17.0%	16.7%	17.5%
IT セキュリティシステムの導入・導入支援	56.7%	53.7%	53.7%
セキュリティ製品の選定・導入支援	15.7%	19.5%	19.5%
その他のセキュアシステム構築サービス	10.6%	10.1%	9.4%
セキュアシステム構築 計	100.0%	100.0%	100.0%
<b>対前年比成長率</b>			
IT セキュリティシステムの設計・仕様策定	-	20.2%	16.7%
IT セキュリティシステムの導入・導入支援	-	16.2%	11.5%
セキュリティ製品の選定・導入支援	-	51.9%	11.6%
その他のセキュアシステム構築サービス	-	16.5%	4.0%
セキュアシステム構築 計	-	22.5%	11.6%

「セキュアシステム構築サービス」市場は平成 15(2003)年度で 1,775 億円と突出した規模のカテゴリを形成している。上記のように「IT セキュリティシステムの導入・導入支援」セグメントが突出して大きいことと他のセグメントも相当の規模を持つことによる。ただ、「セキュアシステム構築サービス」カテゴリ全体としての平成 16(2004)、17(2005)年度の伸び率は各々22.5%、11.6%と、「情報セキュリティサービス」市場全体の伸び率をかなり下回る水準となっている。これは既に十分巨大な市場規模になっている以上、発展途上の伸び率は期待しがたいことが基本的な理由であろう。逆に言えば、この、最も SI に近い性質を持つカテゴリは、最も普通の姿に近い形で定着していると解釈できる。

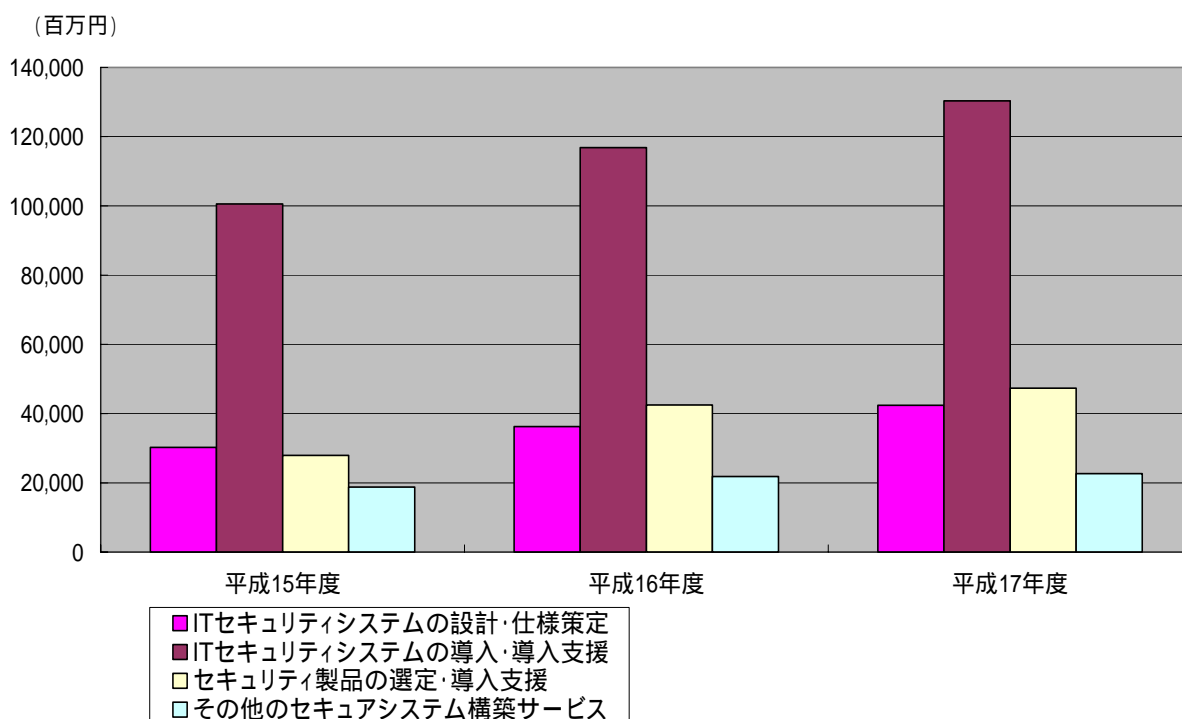
一方、循環要因として、ネットワーク・インフラストラクチャ（基盤設備）の更新需要が平成 16(2004)年度後半から徐々にではあるが高まりつつある。平成 17(2005)年度は通信業界における更新需要期にあたり、大規模システム構築案件が期待される。これに伴い、情報セキュリティ対策面も従来以上に意識した取り組みがなされることが期待されるが、その需要がどのような形でどこまで「情報セキュリティサービス」のカテゴリとして顕在化するかは不明である。上記に見た「セキュリティ製品の選定・導入支援」セグメントの平成 16(2004)年度の突出した伸び率がそれに該当する可能性はあるが、あくまで憶測の域を出ないであろう。

以下、セグメント別の数字の推移を見ていくと、最大セグメントである「IT セキュリティシステムの導入・導入支援」は平成 15(2003)年度で 1,006 億円の規模に達している。これが平成 16(2004)、17(2005)年度各々16.2%、11.5%伸びて平成 17(2005)年度には 1,303 億円の規模に達するものと見られる。

「IT セキュリティシステムの設計・仕様策定」は平成 15(2003)年度の市場規模が 302 億円であったと推定される。平成 16(2004)年度 20.2%、平成 17(2005)年度 16.7%と比較的順調な伸びを続けて平成 17(2005)年度には 423 億円規模に達すると見る。

「セキュリティ製品の選定・導入支援」は平成 15(2003)年度は 279 億円の規模であるが平成 16(2004)年度に 51.9%と急伸し、424 億円の規模になった後、平成 17(2005)年度は 11.6%と伸びは落ち着いて市場規模は 474 億円程度と予測する。

図 12 国内セキュアシステム構築サービス市場推移



### 8.2.3. セキュリティ運用・管理サービス市場

#### 【市場の特性と動向】

「セキュリティ運用・管理サービス」のカテゴリは主としてファイアウォールやIDSといったセキュリティ防護装置（アクセス制御装置）の運用や監視、ログ解析といった支援サービスで構成される。これは、これら情報セキュリティ装置が、本格的に使いこなそうと思えば専門家の知識を必要とする一方、そのような専門スキルを持った人材の供給が非常に限られる、という状況の中で必然的に生まれるアウトソーシング需要が、市場として形成されているということである。プロフェッショナルがその専門スキルに応じてサービスを提供し、需要側がその必要性和情報処理資源（リソース）の制約からアウトソース（サービスの外部委託）する、という構造により形成される市場であり、情報セキュリティという専門性故にかなり大規模な市場となって顕在化していると考えられる。

このカテゴリの特徴としてはサービスの種類が多く、その性格もまちまちなものが混在しており、それを反映してセグメントごとの市場規模のばらつきも、市場の伸び率のばらつきも極めて大きいことである。

その中で最大のセグメントである「セキュリティ総合監視・運用サービス」は「セキュリティ運用・管理サービス」カテゴリの約4割を占めるセグメントで、このカテゴリの典型的なサービスである。伸び率も比較的一定して安定している。事業者は既にセキュリティオペレーションセンター（SOC、セキュリティ監視・対応センター）に対する第2次投資を終え、今後2、3年は投資回収期間と位置付けている。現状では参入事業者数やそのサービス供給能力にはやや過剰感があるものの、頻発するウイルス・ワーム被害や不正アクセス事件に伴う危機感の高まりから、専門サービスの導入が積極化する流れもあり、一時の不需要期のような価格の低下は、今後は抑えられるものと考えられる。

その次に位置するセグメントは「IDS/IPS監視・運用支援サービス」であり、「ファイアウォール監視・運用支援サービス」、「ウイルス監視・フィルタリングサービス」と合わせて一つのグループを形成する。上で見た総合監視・運用サービスに対して、こちらは個別カテゴリのセキュリティ対策装置管理のアウトソースサービスと位置付けられる。これら、専門家の技術と経験とノウハウに依存するのが、コストパフォーマンス（費用対効果）的にも対策効果の面でも得策であるという考えは定着してきたものと見られ、市場は小さいながらも堅調に推移すると見られる。

「ウイルス監視・フィルタリングサービス」は、「IDS/IPS監視・運用支援サービス」であり、「ファイアウォール監視・運用支援サービス」と同様に専門知識への依存という性格を持つと同時に、ASP（Application Service Provider）つまり専門サービスを月額料金あるいは使用量に応じた従量課金で支払うというビジネスモデルも内包している。特に個人消費者向けに後者のパターンのサービス提供が活発化しており、そのためにアンチウイルスツールのベンダーも新しいビジネスモデルとして積極的に支援しているところから、

新たなサービスモデルとして確立されていくと観測される。

次に大きなサービスモデルとしては「脆弱性検査サービス」が挙げられる。「セキュリティ・コンサルテーション」のカテゴリで「セキュリティ監査サービス」や「セキュリティ診断サービス」といったサービスモデルが定義されているが、それらは定性的診断や聞き取り調査、書類審査といった非技術的手法による判断が中心である。それに対してここで言う脆弱性検査は実際にハッカーと同じ視点と同等以上のスキルを用意して、検査対象とするネットワークに付け入る隙はないかという検査を、検査ツールあるいはエンジニアによる擬似攻撃によって実行するものであり、技術ベースの真剣勝負といった趣を帯びる。このサービスは一定のスキルと設備を持った少数のサービス事業者により供給されており、その市場のニッチさ（限定特化領域性）と技術の特異性から独立のセグメントを形成しつつも、市場規模の拡大にはおのずと限度のある推移をたどるものと予想される。

更に、これらネットワーク攻撃技術とは別の地平にいて、むしろ言わば平和時のサービスを提供するビジネスとしてインターネット VPN サービスと電子認証サービスがある。これらは、ともに通信経路の安全性確保なり通信におけるアクセス主体の確認なりで情報セキュリティサービスを提供する、それぞれ独立したサービスセグメントである。共に規模はさほど小さくなく成長性にも限界はあると想定されるが、常に一定の需要と供給が確保されて小規模ながら市場が形成・維持される領域であると考えられる。

「セキュリティ運用・管理サービス」の主力をなす「セキュリティ総合監視・運用支援サービス」、「IDS/IPS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」の提供ベンダーはほぼ共通しており、そのパターンは三つに大別される。一つ目は、ネットワーク監視センターを運営する企業が、ネットワーク監視の付帯サービスまたはオプションとして提供するケースである。大手のシステムインテグレータやネットワークインテグレータ、もしくはそれらの子会社が手がけるケースが多い。また、通信事業者が通信サービスの延長上に顧客の社内網までサービスを提供するケースもある。

二つ目は、インターネットデータセンターの運営主体が副業的に提供するサービスである。これはハウジング（顧客のサーバシステム預かり）またはホスティング（顧客のアプリケーションシステム預かり）・サービスの付帯サービスとして、顧客から預かるシステムに対して監視サービスをオプションとして提供するケースである。また、インターネットデータセンターとしてサービス提供に特化するモデルの場合でも、自社設備の情報セキュリティ管理能力を対外サービスにまで展開する形で「セキュリティ運用・管理サービス」を提供するケースもある。

そして三つ目は、専門のサービス事業者が提供するケースである。ほとんどのケースでは、自社でSOC（Security Operation Center、セキュリティ監視・対応センター）と呼ぶ監視センター設備を持ち、そこから顧客の社内ネットワークに対する監視を行う。そしていざ何らかの異常が検出されると、顧客に警報を発すると同時にその解決に協力していくことになる。この業態は、一部の情報セキュリティツールベンダーが世界的規模で展開して

いる他、国ごとに技術特化した専門企業（業態的にはベンチャー）が手がけるケースが多い。この場合は、ネットワーク監視等との補完効果がなく、また一定規模の設備と24時間運営・対応体制の構築が必要なことから、規模の利益がないと経営的に厳しいものがある。

「セキュリティ運用・管理サービス」カテゴリの他のサービスについても、多くが専門ベンダーで零細な経営規模のところもあり、経営規模の拡大による経営基盤の安定化が課題になるケースが多いと思われる。

【市場規模とその推移】

表16に国内セキュリティ運用・管理サービス市場規模の実績推定値と予測値を示す。

表 16 国内セキュリティ運用・管理サービス市場規模 実績と予測

市場規模（百万円）	平成 15 年度	平成 16 年度	平成 17 年度
セキュリティ総合監視・運用支援サービス	14,702	17,336	20,105
IDS / IPS 監視・運用支援サービス	6,401	8,138	8,641
ファイアウォール監視・運用支援サービス	1,922	2,480	2,864
ウイルス監視・フィルタリングサービス	1,900	2,681	2,979
脆弱性検査サービス	4,167	5,962	6,398
セキュリティ情報提供サービス	164	240	270
電子認証サービス	1,153	1,407	1,559
インターネット VPN サービス	3,286	4,476	5,403
その他の運用・管理サービス	179	234	390
セキュリティ運用・管理サービス 計	33,874	42,953	48,609
<b>構成比</b>			
セキュリティ総合監視・運用支援サービス	43.4%	40.4%	41.4%
IDS / IPS 監視・運用支援サービス	18.9%	18.9%	17.8%
ファイアウォール監視・運用支援サービス	5.7%	5.8%	5.9%
ウイルス監視・フィルタリングサービス	5.6%	6.2%	6.1%
脆弱性検査サービス	12.3%	13.9%	13.2%
セキュリティ情報提供サービス	0.5%	0.6%	0.6%
電子認証サービス	3.4%	3.3%	3.2%
インターネット VPN サービス	9.7%	10.4%	11.1%
その他の運用・管理サービス	0.5%	0.5%	0.8%
セキュリティ運用・管理サービス 計	100.0%	100.0%	100.0%
<b>対前年比成長率</b>			
セキュリティ総合監視・運用支援サービス	-	17.9%	16.0%
IDS / IPS 監視・運用支援サービス	-	27.1%	6.2%
ファイアウォール監視・運用支援サービス	-	29.0%	15.5%
ウイルス監視・フィルタリングサービス	-	41.1%	11.1%
脆弱性検査サービス	-	43.1%	7.3%
セキュリティ情報提供サービス	-	46.6%	12.5%
電子認証サービス	-	22.0%	10.8%
インターネット VPN サービス	-	36.2%	20.7%
その他の運用・管理サービス	-	31.2%	66.3%
セキュリティ運用・管理サービス 計	-	26.8%	13.2%

「セキュリティ運用・管理サービス」のカテゴリ全体の市場規模は、平成 15(2003)年度で 339 億円であった。その伸び率は「情報セキュリティサービス」市場全体の伸び率に極めて近く、平成 16(2004)年度 26.8%、平成 17(2005)年度 13.2%と予測され、市場規模としては平成 16(2004)年度に 430 億円、平成 17(2005)年度に 486 億円と拡大していくものと見る。

このうち平成 15(2003)年度の構成比で 43.4%と最大のセグメントが「セキュリティ総合監視・運用支援サービス」で、同年度の市場規模は 147 億円であった。この市場の伸び率は比較的緩やかで、平成 16(2004)、17(2005)年度各々 17.9%、16.0%と予測され、平成 17(2005)年度の市場規模は 201 億円に達するものと予測する。

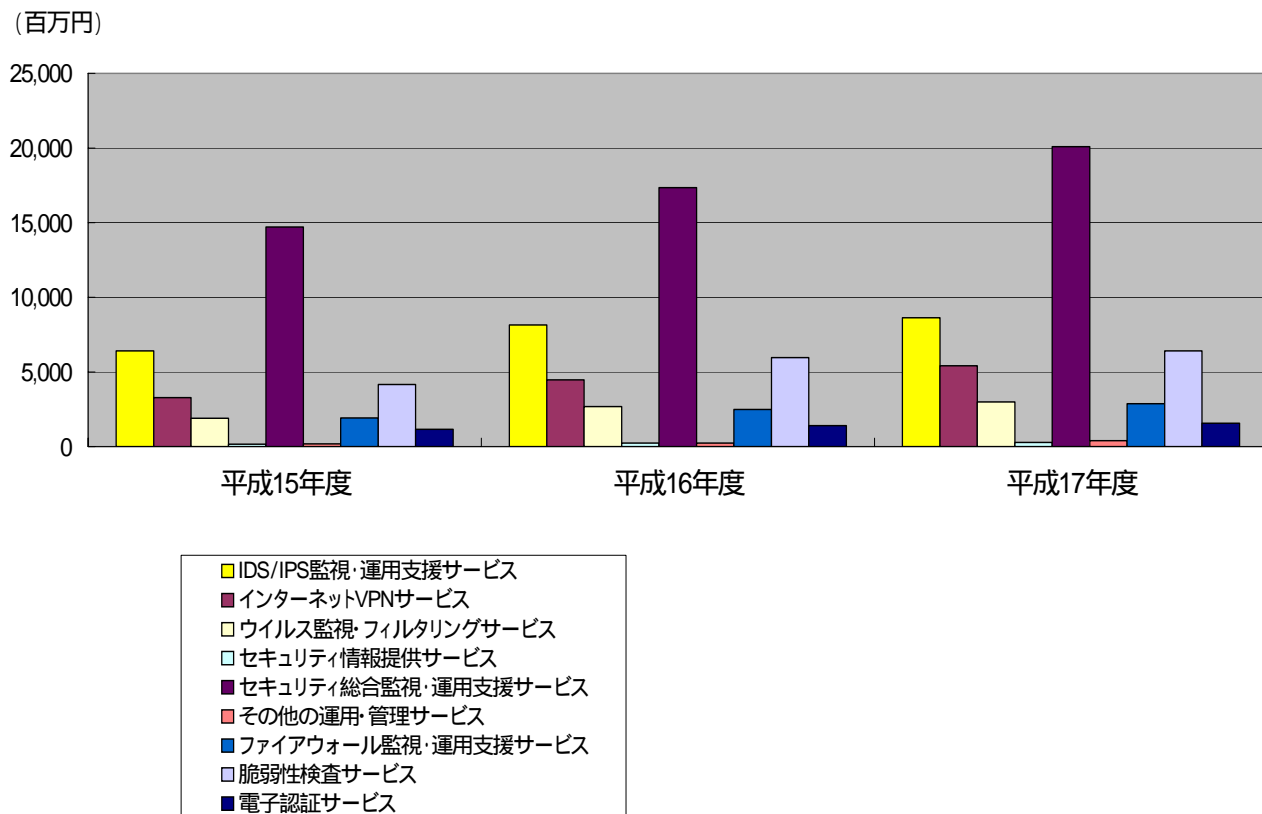
次に大きいセグメントは「IDS / IPS 監視・運用支援サービス」で、平成 15(2003)年度実績市場規模が 64 億円程度と見る。伸び率は平成 16(2004)年度が 27.1%とカテゴリ全体の伸び率に近いが、平成 17(2005)年度は 6.2%と衰える。市場規模は平成 17(2005)年度で 86 億円程度と予測する。

平成 16(2004)年度に 43.1%と高い伸びを見せ、市場規模も平成 15(2003)年度以降 42 億円、60 億円、64 億円と年を追って拡大を見せるのが「脆弱性検査サービス」である。情報セキュリティの診断や判断はプロの能力を活用しようという考え方がここにも現れていると言えるであろう。

20 億円弱から 30 億円弱へと市場規模も成長度合も似た推移をたどると見られるのが「ファイアウォール監視・運用支援サービス」と「ウイルス監視・フィルタリングサービス」である。前者の市場規模と伸び率は平成 15(2003)年度 19 億円、平成 16(2004)年度 25 億円・29.0%、平成 17(2005)年度 29 億円・15.5%であった。後者は同じく 19 億円、27 億円・41.1%、30 億円・11.1%という結果であった。

2 億円程度の極めてニッチな市場ながら、伸び率としては 46.6%と平成 16(2004)年度に最も高い伸びが見込まれるのが「セキュリティ情報提供サービス」である。こちらはむしろ、情報提供だけは受けるが、その後の判断や対策は自前であるいは別途外部業者を活用して、という、自律性の強い対応においてニーズが出るものであり、需要は限られる。一方、供給側としては 24 時間世界中の脆弱性情報やインシデント情報に目配りし、必要に応じて翻訳も解説もこなしながらリアルタイムで情報提供を続ける必要のある、固定費負担の大きいビジネスである。むしろ一般ユーザよりは監視運用サービス提供事業者にとって必要なサービスではあるが、需要量の余りの小ささから、ビジネスモデル的に肯定的条件を達成するのが困難な、極めて特異な市場である。しかし、脆弱性の発見頻度と深刻度は増しており、社会的には必須のサービスとして、非商業的な枠組みの導入も含めて、対策検討が必要なサービスセグメントではないかと考える。

図 13 国内セキュリティ運用・管理サービス市場推移



#### 8.2.4. セキュリティ教育市場

##### 【市場の特性と動向】

「セキュリティ教育」は、比較的最近市場として成立しだしたカテゴリである。教育とは、不特定多数を対象に特定領域の特定知識やスキルを身に付けさせることを目的に提供されるサービスである。その対象が、例えば情報セキュリティに関する技術資格の取得といった少数利用者を対象とする場合には極めて限られた市場規模となる。一方、近年急速に需要が顕在化しているのは、一般社員を対象として最低限の情報セキュリティ知識を身に付けさせ、日常の行動において最低限の情報セキュリティ対応を確保しようという、言わばセキュリティ・ミニマム移植のための教育ニーズである。

この、一般社員対象の教育は、大企業においては数年前から自社開発による導入が進み、情報セキュリティ教育という位置付けよりは、社員教育カリキュラムの一環として情報セキュリティが組み込まれる形で、実現されている。その範囲においては、内製供給に留まり市場形成には至らない。それがここに来て、同じ社員教育でもセキュリティ知識のレベルアップと対策スキルの質的向上を狙って教育需要が外在化される傾向を見せている。それは、一つ目として、ウイルス・ワームのように攻撃手法が日々進化するために社内制作では追いつかないという問題が深刻化していること。二つ目として、防御対策も同様に進化することから常に最新の情報を取り入れる必要があること。そして三つ目として、情報保護対策を徹底させるためには「リテラシィ」として、あるいは一般教養的素養として、社員全員に情報セキュリティの理解を広めなければならないこと、などが背景にある。これらの要因が相俟って、専門家によるサービスの供給に依存する方向が見えて来ている。

専門家によるサービスには、いくつかのセグメントがある。まず、教育の中身そのものを提供する「セキュリティ教育コンテンツの提供」サービス。次に実際に情報セキュリティ教育を外部からのサービスとして実施する「セキュリティ教育実施」サービス。このセグメントには情報セキュリティの専門家育成や資格取得のための専門的な教育の提供サービスも含まれる。更に、一般社員への教育実施に際して大量の受講者を効率よく教育するためのコンピュータ利用教育、いわゆる e ラーニングのサービス、特にインターネット上に教育サイトを置いて時間貸し方式で実施するいわゆる ASP 方式のサービス「セキュリティ教育 ASP サービス」がある。これに「その他のセキュリティ教育サービス」例えば講師派遣サービス等がある。このカテゴリは以上 4 セグメントにより定義した。

「セキュリティ教育 ASP サービス」は、セキュリティ教育を e ラーニングで実施する方式のうち、大企業がイントラネット上で社内展開するのではなく、外部の専門業者がインターネット上で ASP サービスの形で提供するものである。履修管理サービス等を併せて提供することが可能であり、そのコンテンツ（情報の内容）の充実、少人数でも比較的充実したコンテンツを利用可能、等のメリットから、普及が期待される教育サービスである。e ラーニングの先進国米国では、教育提供の専門業者が増えており、日本でも大企業の教育

部門や人材部門からの分社を中心に供給側が充実しつつある。中小企業でも充実した教育が用意でき、履修管理や修得状況管理も容易なので、活用が進むことを期待したい。

なお、情報セキュリティベンダーだけでなく、企業内部で情報セキュリティ対策の企画や運用管理を担う人材の育成、充実は非常に急がれるところである。情報セキュリティ人材の育成は政策課題にもなっており、教育サービスの提供は、足元においては一般社員への基礎的セキュリティ知識の徹底が先行して活況を呈していると思われるが、今後専門の養成機関が充実していくことが望まれる。既に専門の大学院大学も設置された他、大学で一般カリキュラムあるいは社会人向けカリキュラムとして提供する例も増えている。それら高等教育の充実によって、絶対的不足が指摘され危機感が唱えられている、情報セキュリティ対策人材の育成・供給に貢献することが期待される。

そのためのインセンティブとしては資格制度があり、既に情報セキュリティ関連の海外資格の日本進出も始まっている。独立行政法人情報処理推進機構（IPA）による情報セキュリティ資格の提供も行なわれているが、官民の資格認定が活発化し、またそこへ向けての教育の提供が充実することが望まれる。そのためには、資格取得に向けた補助制度や職業訓練補助的な政策対応、企業での育成政策等の充実が期待される。そのような形で需要側が刺激されれば、供給側の積極投資も誘発し、情報セキュリティ人材育成に好循環が期待できるのではないかと。

教育サービスの提供主体は、各種教育を事業とするいわゆる専門学校の運営主体や企業向け教育サービス事業者と、情報セキュリティツールベンダーが自社ツールと関連する領域に関する教育を提供する場合とに大別できる。これに大学等が専門大学院課程やカリキュラムを設定するケース、ASP事業者がASPメニューの一環として情報セキュリティを取り込むケース等も登場している。更には、専門資格認定を商業ベースで行うビジネスモデルもあり、提供主体は多様化の傾向にあるが、事業としては零細規模のものが大半であると見られる。

【市場規模とその推移】

表17に国内セキュリティ教育市場規模の実績推定値と予測値を示す。

表 17 国内セキュリティ教育市場規模 実績と予測

市場規模(百万円)	平成 15 年度	平成 16 年度	平成 17 年度
セキュリティ教育実施	3,822	6,868	9,225
セキュリティ教育コンテンツの提供	575	1,352	1,287
セキュリティ教育 ASP サービス	161	310	415
その他のセキュリティ教育サービス	355	557	732
セキュリティ教育 計	4,912	9,088	11,658
<b>構成比</b>			
セキュリティ教育実施	77.8%	75.6%	79.1%
セキュリティ教育コンテンツの提供	11.7%	14.9%	11.0%
セキュリティ教育 ASP サービス	3.3%	3.4%	3.6%
その他のセキュリティ教育サービス	7.2%	6.1%	6.3%
セキュリティ教育 計	100.0%	100.0%	100.0%
<b>対前年比成長率</b>			
セキュリティ教育実施	-	79.7%	34.3%
セキュリティ教育コンテンツの提供	-	135.3%	-4.9%
セキュリティ教育 ASP サービス	-	93.0%	33.7%
その他のセキュリティ教育サービス	-	56.9%	31.4%
セキュリティ教育 計	-	85.0%	28.3%

「セキュリティ教育」はカテゴリ全体でも平成 15(2003)年度実績が 49 億円ときわめて小さい市場セグメントであるが、平成 16(2004)年度は前年度比 85.0%増と急成長し 91 億円に達したと推測される。平成 17(2005)年度には伸び率こそ 28.3%に落ちるが、それでもセキュリティサービス全体の伸びの 13.5%の倍以上の伸びを続けて 117 億円と、初の 100 億円大台乗せを予測する。

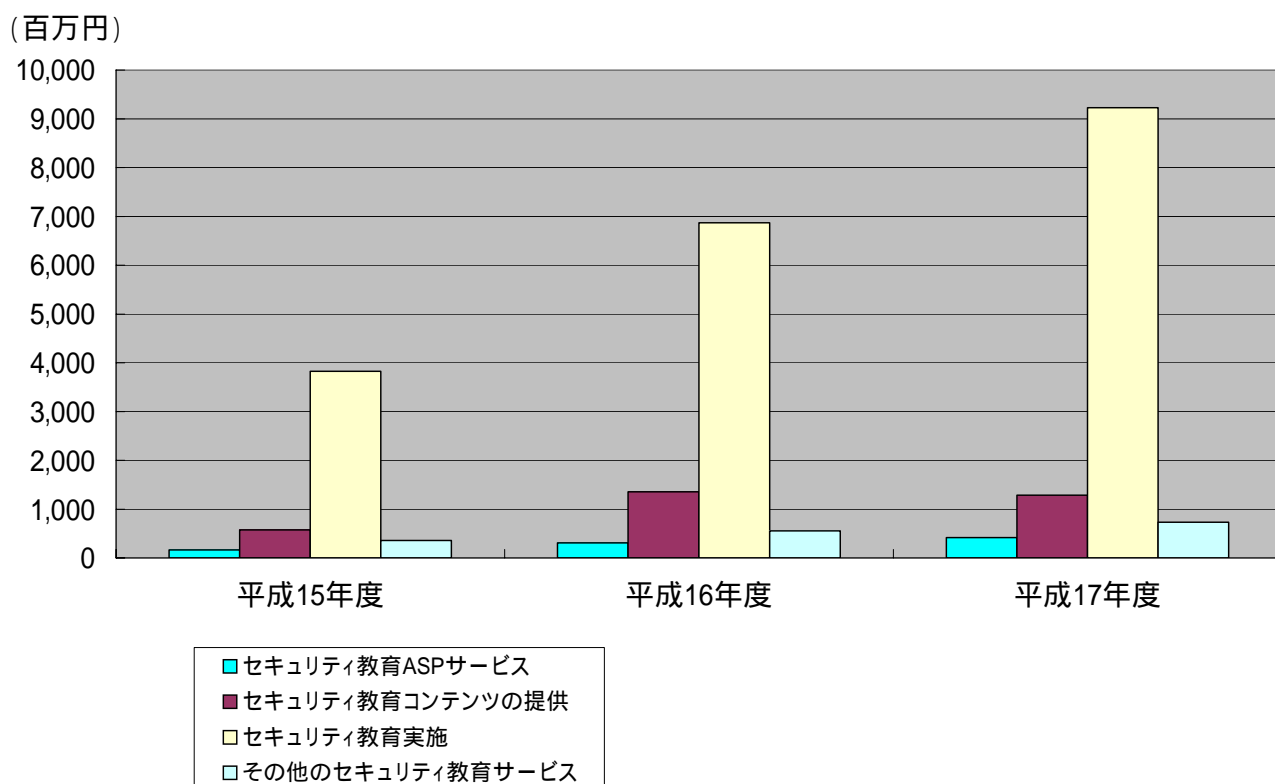
このカテゴリの最大のセグメントは約 8 割を占める「セキュリティ教育実施」であり、市場規模推移は平成 15(2003)～17(2005)年度に 38 億円、69 億円、92 億円、平成 16(2004)、17(2005)年度の前年度比伸び率は 79.7%、34.3%と急拡大する。この要因は上記に見たように、社員教育を外部委託する動きの結果であると分析できる。社員全員に対して情報セキュリティ・リテラシィ(基礎的対応能力)を植え付けて、現場の末端まで情報漏えい対策を徹底する必要に迫られる一方、それを自社内でまかなうことが困難なことから、コンテンツ(情報の内容)の制作や教育の実施等について、専門家による教育サービスに依存しようという発想が、ここに明確に示されていると言える。

「セキュリティ教育コンテンツの提供」は平成 15(2003)年度において 6 億円弱のマーケットであったのが、平成 16(2004)年度には約 2.4 倍伸びて 14 億円弱になったと予測できる。上記と同様の理由で、個人情報保護法対応の社員教育需要が、アウトソース需要として顕

著に顕在化した結果であると考えられる。

平成 15(2003)～17(2005)年度各年度の市場規模推移は 1.6 億円、3.1 億円、4.2 億円、対前年度比伸び率で見ると、93.0%、33.7%と、極めて小さいながら順調な拡大を見せるセグメントが「セキュリティ教育 ASP サービス」である。ワンツーワンの教育が可能であること、場所と時間の制約が少ないこと、進捗度や理解度の個別トレースが容易なこと等、eラーニングのメリットに対する認識が広がりつつあり、今後一層活用が進むと共に、専門プロバイダーの参入も続くものと期待される。

図 14 国内セキュリティ教育市場推移



## 9. 海外情報セキュリティ市場との比較

本章では、本調査で得られた国内情報セキュリティ市場の推定規模を海外情報セキュリティ市場との比較において見ていく。比較対象データとして、世界全体と地域別の情報セキュリティ市場規模は米国 IDC 社（International Data Corporation）が公刊する調査報告書の数値を用いた。（複数の調査結果を比較データとして用いているため、データ出典元の報告書名は図表ごとに記載する。）同調査の対象期間は暦年単位であり、海外市場規模は全て暦年（当年 1 月～当年 12 月期）での値となる。このため、本調査での対象期間（当年 4 月～翌年 3 月の日本で一般的な会計年度）とは若干のずれを生じるが、便宜上今回の年度調査結果（当年 4 月～翌年 3 月期）とそのまま比較している。また海外市場規模の原数字は米ドル建てであるが、比較の便宜上全て円換算した。換算に当たっては、基準年である 2003 年の年間平均為替レート、1 米ドルあたり 116.01 円の為替交換レートを使用して全て換算している。（為替レートデータは、OANDA Currency Converter, Historical Currency Table（<http://www.oanda.com/convert/fxhistory>）による。<sup>5</sup>）

予測数字に対しても基準年の為替レートを適用する理由は、IDC 社の調査が予測値に関しても基準年の為替レートを適用し、為替変動要素を織り込まない数値を示しているため、市場の伸び等を見るに際して一貫したレートの適用が妥当と判断したことによる。

なお、両調査における製品・市場区分にも若干の相違があり、単純に相互の数字を対比することが困難または不適当な要素がある。その点については適宜読み替え並びに補足をすることにより補っているが、細部にわたる厳密な対比という要求には届かない面があり、あくまで参考としての比較考察と理解いただきたい。

### 9.1. 世界全体の情報セキュリティ市場（世界情報セキュリティ市場）との比較

#### 9.1.1. 世界全体の情報セキュリティ市場の概観

表 18 は世界全体の情報セキュリティ市場調査結果である。2004 年 12 月に発表されたデータであり、2004 年と 2005 年の市場規模は予測値である。

世界全体の情報セキュリティ市場は、2003 年において、2 兆 6,458 億円となっている。「情報セキュリティツール」市場と「情報セキュリティサービス」市場の対比で見ると、2003 年～2005 年の年平均成長率が「情報セキュリティツール」市場では 18.7%、「情報セキュリティサービス」市場では 19.5%とほぼ同じペースで市場が拡大すると見られ、その結果、両者の構成比は調査対象年を通じてほぼ 54%対 46%の一定の比率で推移すると予測される。

一方、「情報セキュリティツール」市場をハードウェアとソフトウェアに分けて見ると、

<sup>5</sup> OANDA Corporation の提供している為替情報。同社は、米国に 1995 年に設立されたインターネットベースの為替証拠金取引会社で、この会社が提供する為替情報は世界中の多くの企業が利用している。

2003年においてハードウェア 31.1%、ソフトウェア 68.9%の比率になっている。2003年～2005年の平均市場成長率はハードウェア市場が 25.2%でソフトウェア市場の 15.6%を9.6ポイント上回っており、ハードウェアシフトが進む傾向が見られる。ソフトウェア製品よりは、セキュリティ・アプライアンスを採用して情報セキュリティシステムの構築を行う傾向が強くなっていることが、その要因であると推測される。ソフトウェア製品と比較して導入・設定の容易さ、処理の高速性、保守運用負担の軽減などの要素がアプライアンス選好を強める要因になっていると推測される。アプライアンス製品のこの優位性が評価されることによって、世界的に今後も拡大が見込まれる市場であると言える。

表 18 世界全体の情報セキュリティ市場規模 実績と予測

市場規模 (百万円)	2003年	2004年	2005年
セキュリティツール	1,420,658	1,694,906	2,001,869
セキュリティハードウェア	442,079	556,477	693,438
セキュリティソフトウェア	978,521	1,138,453	1,308,465
セキュリティサービス	1,225,182	1,459,638	1,750,243
合計	2,645,840	3,154,544	3,752,111
<b>製品別市場シェア</b>			
セキュリティツール	53.7%	53.7%	53.4%
セキュリティハードウェア	16.7%	17.6%	18.5%
セキュリティソフトウェア	37.0%	36.1%	34.9%
セキュリティサービス	46.3%	46.3%	46.6%
合計	100.0%	100.0%	100.0%

セキュリティツールシェア	2003年	2004年	2005年
セキュリティツール	100.0%	100.0%	100.0%
セキュリティハードウェア	31.1%	32.8%	34.6%
セキュリティソフトウェア	68.9%	67.2%	65.4%

市場成長率	2003年	2004年	2005年	2003-2005 年平均成長率
セキュリティツール	-	19.3%	18.1%	18.7%
セキュリティハードウェア	-	25.9%	24.6%	25.2%
セキュリティソフトウェア	-	16.3%	14.9%	15.6%
セキュリティサービス	-	19.1%	19.9%	19.5%
合計	-	19.2%	18.9%	19.1%

出典：米国 IDC 社報告書、Worldwide IT Security Software, Hardware, and Services  
2004-2008 Forecast: The Big Picture Document#:32557 2004年12月

< 1ドル=116.01円で円換算 >

### 9.1.2. 世界の情報セキュリティ市場との全体像比較

表 19 は本調査における日本の情報セキュリティ市場規模とその予測値である。ここでは、世界市場と比較するために、「情報セキュリティツール」市場をハードウェア市場とソフトウェア市場に分類し直して再集計した。(ハードウェア市場に含まれる製品は、統合型アプライアンス製品、アクセス制御製品の中のファイアウォール・アプライアンス、VPN アプライアンス、IDS / IPS アプライアンス、セキュアコンテンツ管理製品の中のアンチスパム・アプライアンス、URL フィルタリング・アプライアンス、アンチフィッシング・アプライアンス、その他セキュアコンテンツ管理のアプライアンス、アクセス管理製品の中の個人認証用ワンタイムパスワード、IC カードシステム、USB キーシステム、生体認証デバイス / システム、である。)

まず世界市場と同様に日本の「情報セキュリティツール」市場と「情報セキュリティサービス」市場の年間成長率を見ると、「情報セキュリティサービス」市場の平成 16(2004)年度の対前年度比成長率が 27.2%で突出している。これは前章で解説したように、個人情報保護法の施行を前にしてその対応が駆け込み的に行われ、それが「セキュリティ・コンサルティング」、「セキュリティ教育」分野の需要急増に結びついた結果であると見られる。平成 17(2005)年度については、引き続き同様の需要が持続するものの若干減速し、対前年度比率 13.5%程度の成長が予測される。

表 18 にあるように世界市場では 2003 ~ 2005 年の年平均成長率は 19.1%である。日本市場においては平成 16(2004)年度に対前年度比 23.0%とかなり高い成長率を示した後、平成 17(2005)年度に対前年度比 14.3%と成長率を急速に下げる予測となっている。世界全体の市場伸び率が両年度均等しているのに比べると年によるばらつきが大きくなっているが、両年度を合せて平成 15(2003) ~ 17(2005)年度の年平均成長率で見た場合、日本市場は 18.6%となる。いずれも 20%近い高成長率で市場の拡大が続くと予測される。

表 21 に、情報セキュリティの世界市場に対する日本市場の比率を示す。(表 18 と表 19 より合成。)平成 16 年度の推測値において、日本の情報セキュリティ市場規模は 4,438 億円で、2004 年の世界全体の情報セキュリティ市場規模 3 兆 1,545 億円に対して 14.1%のシェアとなる。同様に平成 15(2003)年度は 13.6%、平成 17(2005)年度は 13.5%と、概ね 13 ~ 14%で推移している。平成 16(2004)年度の、市場分類別の対世界市場比率をみると、「情報セキュリティツール」市場は 8.6%、「情報セキュリティツール」市場の内訳でハードウェアは 6.7%、ソフトウェアは 9.5%、「情報セキュリティサービス」市場は 20.4%のシェアとなる。

ここで、対比のために情報セキュリティを含んだ IT 市場全体の世界市場対日本市場の比率をみると、2004 年では表 22 のようになる。すなわち IT 市場全体ではハードウェア + ソフトウェアが 10.2%、この内訳でハードウェアだけで見ると 11.0%、ソフトウェアは 8.6%、

IT サービス市場は9.8%であり、ハードウェア・ソフトウェア・サービスの総合計で10.0%という数字となる。

情報セキュリティ市場の構成比は、IT 市場全体に比べて、サービスが突出して高く、ハードウェアが極端に低いという結果となる。このうち、ハードウェアの比率が極端に低いのは、情報セキュリティソフトウェアの動作環境としてのハードウェアが算入されていないことが一因と分析できる。サービスの比率が極端に高いことについては次項以降で述べる。

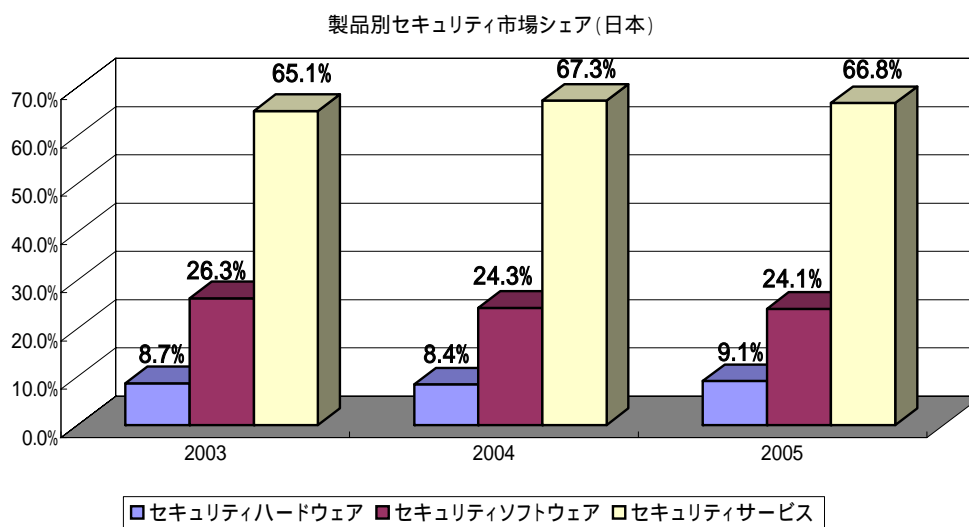
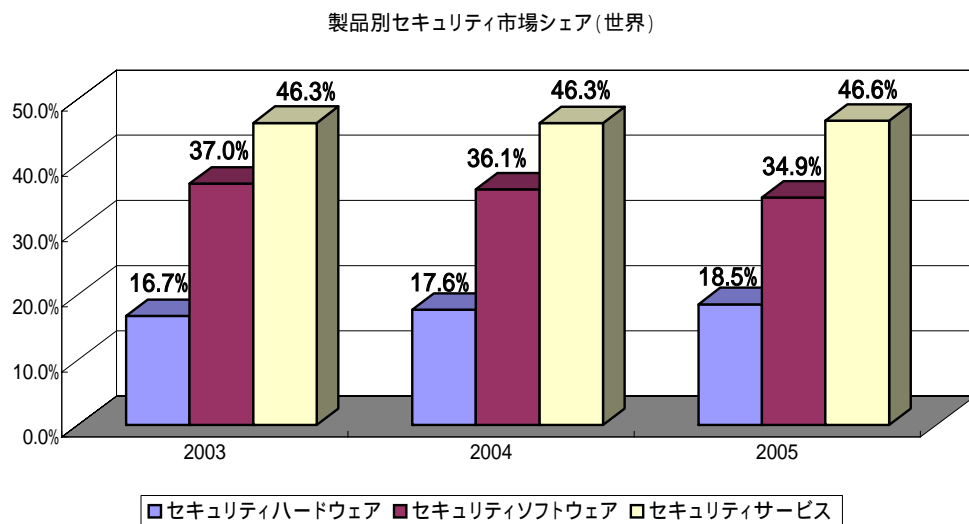
表 19 日本の情報セキュリティ市場規模 実績と予測

市場規模(百万円)	平成 15 年度	平成 16 年度	平成 17 年度
セキュリティツール	125,964	145,328	168,589
セキュリティハードウェア	31,233	37,361	46,330
セキュリティソフトウェア	94,730	107,967	122,315
セキュリティサービス	234,686	298,448	338,611
合計	360,650	443,776	507,256
<b>製品別シェア</b>			
セキュリティツール	34.9%	32.7%	33.2%
セキュリティハードウェア	8.7%	8.4%	9.1%
セキュリティソフトウェア	26.3%	24.3%	24.1%
セキュリティサービス	65.1%	67.3%	66.8%
合計	100.0%	100.0%	100.0%

セキュリティツールシェア	平成 15 年度	平成 16 年度	平成 17 年度
セキュリティツール	100.0%	100.0%	100.0%
セキュリティハードウェア	24.8%	25.7%	27.4%
セキュリティソフトウェア	75.2%	74.3%	72.6%

市場成長率	平成 15 年度	平成 16 年度	平成 17 年度	平成 15-17 年 年平均成長率
セキュリティツール	-	15.4%	16.0%	15.7%
セキュリティハードウェア	-	19.6%	24.0%	21.8%
セキュリティソフトウェア	-	14.0%	13.3%	13.6%
セキュリティサービス	-	27.2%	13.5%	20.1%
合計	-	23.0%	14.3%	18.6%

図 15 情報セキュリティ市場、世界市場と日本市場の比較



### 9.1.3. 世界の情報セキュリティ市場とのツール対サービスの構成比の比較

ここでは、「情報セキュリティツール」市場対「情報セキュリティサービス」市場の構成比の内外比較を行ってみる。表 18、19 から読み取れるように、日本においてはツール対サービスの市場比率がほぼ 1 : 2 であるのに対し、世界市場ではほぼ 1 : 1 ( 54% : 46% ) と全く様相を異にする。この要因として、日本の「情報セキュリティサービス」市場において突出して大きい「セキュアシステム構築サービス」の影響が考えられる。本調査と IDC 調査における定義の差異、情報セキュリティサービスの提供形態の違いなどの幾つかの要因がこのような結果をもたらしていると推測され、市場の特性の差と統計調査の枠組みの違いが現れていると推測する。

この点の検証のために、まず、両調査のセキュリティサービスの定義について考察する。IDC 社ではセキュリティサービスを下記の分類で定義している。

#### Consulting

Security strategy and planning:	セキュリティに関する戦略、ポリシーの策定
Assessment:	セキュリティに関するアセスメント
Compliance audit:	各種法規制に対する監査
Architecture analysis and review:	セキュリティのアーキテクチャに関する分析と評価
Incident response and forensics:	セキュリティ・インシデントへの対策や証拠鑑識

#### Implementation

Design:	セキュアシステムの設計
Hardware and software procurement:	ハードウェア、ソフトウェアの調達
Integration of security architecture:	セキュリティアーキテクチャのインテグレーション
Performance testing:	セキュリティシステムのパフォーマンステスト
Transition/migration:	システムの移行作業
Knowledge transfer:	知識伝達

#### Management

Managed security services:	マネージドサービス
Intelligence services:	情報提供サービス

#### Education and training

Instructor-led training:	インストラクタによるトレーニング
Technology-based training:	e ラーニングなどによるトレーニング
Text-based training:	教材によるトレーニング

これを本調査の定義と対比させると、大まかには以下の対応関係となる。

表 20 本調査の定義と IDC 社定義の比較

IDC調査定義	本調査の定義
<b>Consulting</b>	セキュリティ・コンサルテーション
Security strategy and planning	セキュリティポリシー構築支援、 セキュリティ認証取得支援サービス
Assessment	セキュリティ診断サービス
Compliance audit	セキュリティ監査サービス、 セキュリティ認証審査機関サービス
Architecture analysis and review	セキュリティ運用管理全般のコンサルティング
Incident response and forensics	セキュリティ運用管理全般のコンサルティング
<b>Implementation</b>	セキュアシステム構築サービス
Design	ITセキュリティシステムの設計・仕様策定
Hardware and software procurement	セキュリティ製品の選定・導入支援
Integration of security architecture	ITセキュリティシステムの導入・導入支援
Performance testing	
Transition/migration	
Knowledge transfer	その他のセキュアシステム構築サービス
<b>Management</b>	セキュリティ運用・管理サービス
Managed security services	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 ウイルス監視・フィルタリングサービス 電子認証サービス IDS / IPS監視・運用支援サービス 脆弱性検査サービス その他の運用・管理サービス
Intelligence services	セキュリティ情報提供サービス
<b>Education and training</b>	セキュリティ教育
Instructor-led training	セキュリティ教育実施
Technology-based training	セキュリティ教育ASPサービス
Text-based training	セキュリティ教育コンテンツの提供
	その他のセキュリティ教育サービス

両者を比較すると、セキュアシステム構築サービスにおける IT セキュリティシステムの導入・導入支援に対して、より細かな定義がされているが、定性的には両者の定義する作業内容に極端な差はないように見える。日本では、大手の総合システムインテグレータが情報セキュリティサービスの市場でも大きな役割を占めており、「IT セキュリティシステムの導入・導入支援」サービスは、ネットワークからアプリケーションまでを含むシステムインテグレーションの一部として、セキュアシステム構築サービスが提供されることが多い。このような場合には、セキュアシステム構築に関わるシステムインテグレーション全体をセキュリティサービスとしてカウントすることになるとすれば、その部分の金額が

大きく出る可能性は高い。

この点は別の角度からは、特に大手 SI 事業者に関して調査対象範囲に質的差がある可能性を示唆する。提供形態について言えば、一般論として、ハード・ソフトの導入に際して、その設定・実装・構築作業を、日本企業はシステムインテグレータに依存する度合いが強く、欧米企業は比較的自社で対応を済ませる傾向にある可能性があるかと推測する。

すなわち、サービスの範囲の定義が内外の商習慣の差から一致しない可能性、調査対象ベンダーの範囲のずれ、外部サービスの利用度合という市場構造の差、等が要因として推測される。

**表 21 日本の情報セキュリティ市場の世界市場に対するシェア**

	平成 15 年度	平成 16 年度	平成 17 年度
セキュリティツール	8.9%	8.6%	8.4%
セキュリティハードウェア	7.1%	6.7%	6.7%
セキュリティソフトウェア	9.7%	9.5%	9.3%
セキュリティサービス	19.2%	20.4%	19.3%
合計	13.6%	14.1%	13.5%

**表 22 日本の IT 市場の世界市場に対するシェア 2004 年（製品分野別、米ドルによる市場規模比較）**

	2004 年 日本市場シェア	日本 IT 市場 (\$M)	世界 IT 市場 (\$M)
ハードウェア+ソフトウェア	10.2%	57,414	563,286
ハードウェア	11.0%	40,183	363,990
ソフトウェア	8.6%	17,231	199,296
IT サービス	9.8%	39,425	400,974
IT 市場合計	10.0%	96,839	964,260

出典：米国 IDC 社報告書、The Worldwide Black Book 2004, 2004 年 12 月

#### 9.1.4. 世界の情報セキュリティ市場とのハード対ソフトの構成比の比較

最後に「情報セキュリティツール」市場の内訳としてのハードウェア対ソフトウェアの構成比の内外比較を見ることにする。ここでも世界市場では概ねハードウェア対ソフトウェアの市場比率が、3：7 であるのに対し、日本では 1：3（3：9）と異なっている。この結果は、日本のセキュリティ製品の導入がソフトウェアに偏重している傾向を示している。世界市場との比較において、日本では相対的にセキュリティ・アプライアンスの普及が進んでいないことが要因として推測される。

日本国内では、セキュリティ・アプライアンス製品の供給の大部分を海外メーカー製品に依存している。（米国 IDC 社の資料では、日本のセキュリティ・アプライアンス製品の出

荷金額に占める国産品のシェアは7.5%である。)日本国内のユーザの品質要求や故障時・不具合発生時の対応への要求は、国産ベンダー並みのスピードや徹底した原因究明を求めるものが多い。しかし、海外製品ではなかなかそこまでの対応を取れるベンダーが少なく、また一般的に故障の発生率にも差が見られる。この結果、経験的に海外ハードウェア製品の積極導入をためらう判断が生じる傾向にあることは否めない。このことが、大勢としてはアプライアンスへの移行傾向を示しつつも、そのスピードや実績値で世界市場との乖離が生じている要因であると推測される。

しかし今後は統合型アプライアンスの登場によって、ソフトウェア製品と比較した導入・設定の容易さ、処理の高速性、保守運用負担の軽減などの優位点の認識が更に高まり、中小企業を中心に、「とりあえず箱を一つ入れれば全てまかなえる」点を評価して、日本でも普及が促進されることが予測される。このため、世界市場において2003年から2005年の2年間にハードウェアが3.5%ポイントシェアを拡大するのには若干及ばないものの、日本市場でもハードウェア対ソフトウェアの構成比が平成15(2003)年度の24.8(%):75.2(%)から平成17(2005)年度は27.4(%):72.6(%)と2.6ポイント変化すると予測され、世界市場と同様にハードウェアのシェア拡大の傾向が見出せる。

## 9.2. 世界の各地域の情報セキュリティ市場との比較

一口に世界市場と言っても、地域別に経済状況もインターネットやブロードバンド環境の普及率もかなりのばらつきがある。従い、日本の状況を世界の各地域と比較するに際しても、地域別に分けてその地域の特性をにらみながらの比較が可能であれば、また違った観測も可能になる。この視点から、データが得られる範囲で世界各地の情報セキュリティ市場と日本市場の比較を試みた。

### 9.2.1. 世界の地域別情報セキュリティソフトウェア市場との比較

この項における分析には、同じく米国 IDC 社の公表している別の統計データを用いた。表23は、世界の地域別及び日米韓のIT市場規模とそのシェアであり、表24が世界の地域別・ソフトウェアカテゴリ別の情報セキュリティソフトウェア市場規模の原数値の表である。原数値の世界合計額の絶対額は、表18に示される世界全体の情報セキュリティソフトウェア金額と若干の差がある。これは統計ベースの差によるものであり、表24の数字が表18の数字より約3%程度低く出る結果になっている。

表25に世界の地域別の情報セキュリティソフトウェア市場規模のシェアを示す。地域別の市場規模分布は、ほぼ「北米地域<sup>6</sup>:3 対 西欧地域<sup>7</sup>:2 対 アジア太平洋地域<sup>8</sup>:1」

<sup>6</sup> 北米地域にはカナダ、米国を含む

<sup>7</sup> 西欧地域には、オーストリア、ベルギー、デンマーク、フィンランド、フランス、ドイツ、ギリシャ、アイルランド、イタリア、オランダ、ノルウェイ、ポルトガル、スペイン、スウェーデン、スイス、イギリス、を含む。

<sup>8</sup> アジア太平洋地域は、アジアとオセアニアの各国を含む、アジア地域は、中国、香港、インド、インドネシア、日本、

の比率となる。地域別の市場成長率は調査対象期間において北米がやや低いなど若干のばらつきはあるが、マクロでの地域差を動かすほどのものでなく、予測期間を通じて概ねこの比率が維持される予測となっている。情報セキュリティソフトウェア市場の地域分布を IT 市場全体の地域分布と比較してみると、IT 市場においては 3 地域の比率はそれぞれ 44 : 30 : 19 (表 23 参照) で、北米地域を 3 とすると、3 : 2.1 : 1.3 となり、若干情報セキュリティソフトウェア市場と異なっている。北米と西欧の IT 市場規模比率と情報セキュリティソフトウェア市場規模比率はほぼ同じであるが、アジア太平洋地域では情報セキュリティソフトウェア市場比率が IT 市場比率よりも低い傾向にあり、情報セキュリティソフトウェアに対する投資規模がまだ小さいことが見て取れる。

地域別データのうち、日本を含むアジア太平洋地域の数字と日本の数字との比較を試みる。両統計は時期、対象品目の定義等若干の差はあるが、あえて絶対額そのものを対比すると、2004 年度の見込み値で見た場合、アジア太平洋地域の情報セキュリティソフトウェア市場規模は 1,803 億円、日本市場は表 19 から 1,080 億円と推定され、ほぼ 60% を占めるという結果となった。また GDP ベースで見た場合、日本はアジア太平洋の 55%<sup>9</sup> であり、IT 投資額で見た場合は同じく 52% (表 23 参照) という比率になる。GDP の比率に対して、IT 投資の面では日本はアジア太平洋に対して相対的に低く、情報セキュリティソフトウェア市場規模では相対的に高いという結果になる。しかし、日本は情報セキュリティツールのハード・ソフトの選好面ではソフト志向が強いことは 9.1.1.1 で見た通りである。後述するようにセキュリティ・アプライアンスでは日本の対アジア太平洋シェアは相対的に低くなる。統計ベースが違うものであるが便宜的に情報セキュリティソフトウェアとセキュリティ・アプライアンスの合計における日本の対アジア太平洋シェアを試算すると (表 19、表 24、表 30 より合成) 2004 年において約 53% となり、ほぼ IT 投資のシェアと一致する。これらの数字から導き出される仮説としては、日本はアジア太平洋経済と比較して、GDP 規模の割に IT 投資比率は若干低く、情報セキュリティ投資の IT 投資に占める割合はほぼ同じであるが、相対的にソフトウェア選好が強い、ということになる。

---

韓国、マレーシア、フィリピン、シンガポール、台湾、タイ、ベトナム、を含み、オセアニア地域は、オーストラリア、ニュージーランドを含む。その他の IT 市場規模が比較的小さな各国も、アジア太平洋州地域のその他の国としてまとめて市場規模を計上している。

<sup>9</sup> 外務省発表の APEC の主要経済指標 (2004 年) より JNSA 算出

表 23 世界の IT 市場規模及び各国、地域のシェア、2004 年（米ドルによる比較）

	シェア	IT 市場（\$M）
日本	10.0%	96,839
韓国	1.3%	12,484
米国	40.8%	393,723
アジア太平洋地域	19.2%	184,997
西欧地域	30.2%	291,145
北米地域	43.5%	419,099
その他地域	7.2%	69,019
全世界	100.0%	964,260

出典：米国 IDC 社報告書、The Worldwide Black Book 2004, 2004 年 12 月

次に情報セキュリティソフトウェアの分類別、地域別の分布を見ることとする。表 25 に、各地域におけるソフトウェア製品分類単位ならびにその地域の合計額の世界シェアを示した。

地域別シェアの推移では、北米地域が徐々にシェアを下げる中で西欧地域及びアジア太平洋地域がシェアを高める傾向が見られ、先進地域である北米地域を他の地域がほぼ同スピードで（わずかながらアジア太平洋地域の伸び率が高いが）追いつけていることが読み取れる。

製品分類別で特徴的なのは、北米地域において、「IDS / IPS」及び「その他セキュリティソフトウェア」の対世界シェアが突出して高い点である。これらの製品分類は、比較的能動的に、ネットワーク上の異常や違反を検知して対処しようとするカテゴリであり、ネットワーク先進国、情報セキュリティ製品先進国の米国が高い普及率を実現している結果であると推測できる。逆に、西欧地域におけるこれら 2 製品分類は、西欧地域合計の数字を相当下回っている。一方、ヨーロッパが高く北米が低い製品カテゴリは「セキュアコンテンツ管理」であり、両者の対照は興味深いところであるが、その要因を推測するにはデータが限られるので、現象の指摘にとどめたい。その他は顕著な地域間格差は見られなかった。

次に情報セキュリティソフトウェア市場の地域別の成長率について比較を行った。データを表 26 に示す。前述のように、地域別で最も高い成長率を示すのはアジア太平洋地域である。2003 年～2005 年の 2 年間の年平均成長率は 18.5%となる。これに続くのが西欧地域で 17.5%。最も成熟度が高いと見られる北米地域は 14.5%に留まった。この統計データにおける世界平均は 16.2%であり、表 18 で見た 15.6%よりは若干高い伸び率を見せている。情報セキュリティソフトウェアは、情報セキュリティハードウェアや情報セキュリティサービスよりは、成熟度が進んでいる分伸び率は限られるものの、他の産業に比べれば依然として極めて高い成長を続ける市場分野であると言える。そして、経済成長及び IT 化の勢

いが強いアジア太平洋地域が、絶対規模は北米の3分の1、ヨーロッパの2分の1であるが、最も高い成長を続けると予測される。

表 24 世界の情報セキュリティソフトウェア地域別市場規模 実績と予測（百万円）

地域	セキュリティソフトウェア分類	2003年	2004年	2005年
アジア太平洋	ファイアウォール/VPN	15,628	17,306	19,514
	IDS/IPS	14,388	17,390	20,137
	その他セキュリティソフトウェア	5,629	6,377	7,040
	セキュアコンテンツ管理	65,379	81,438	98,385
	セキュリティ 3A	49,349	57,799	66,141
アジア太平洋州 計		150,373	180,310	211,217
北米	ファイアウォール/VPN	51,882	53,205	54,535
	IDS/IPS	50,867	54,428	58,238
	その他セキュリティソフトウェア	16,867	19,397	22,694
	セキュアコンテンツ管理	182,013	223,876	265,293
	セキュリティ 3A	153,375	172,740	195,876
北米 計		455,004	523,646	596,636
西欧	ファイアウォール/VPN	32,769	34,866	37,028
	IDS/IPS	23,341	27,169	31,271
	その他セキュリティソフトウェア	8,335	9,652	11,322
	セキュアコンテンツ管理	132,523	163,400	196,244
	セキュリティ 3A	96,687	111,307	129,221
西欧 計		293,655	346,394	405,086
その他	ファイアウォール/VPN	7,135	8,180	9,408
	IDS/IPS	4,287	4,753	5,270
	その他セキュリティソフトウェア	1,376	1,618	1,912
	セキュアコンテンツ管理	17,639	21,339	24,891
	セキュリティ 3A	15,815	18,566	21,917
その他地域 計		46,254	54,456	63,399
全体	ファイアウォール/VPN	107,414	113,557	120,485
	IDS/IPS	92,884	103,740	114,917
	その他セキュリティソフトウェア	32,207	37,044	42,968
	セキュアコンテンツ管理	397,554	490,054	584,813
	セキュリティ 3A	315,226	360,412	413,154
総計		945,286	1,104,806	1,276,338

出典：米国 IDC 社報告書、2004 Worldwide Software Market Forecaster: 2004-2008 Forecast Update, December 2004（IDC #PT602, 2004年12月）

<1ドル=116.01円で円換算>

注：セキュリティ 3A とは、承認：Authorization、認証：Authentication、管理：Administration、の3機能の総称

表 25 世界の情報セキュリティソフトウェア地域別市場シェア 実績と予測

地域	セキュリティソフトウェア分類	2003 年	2004 年	2005 年
アジア太平洋	ファイアウォール / VPN	14.5%	15.2%	16.2%
	IDS / IPS	15.5%	16.8%	17.5%
	その他セキュリティソフトウェア	17.5%	17.2%	16.4%
	セキュアコンテンツ管理	16.4%	16.6%	16.8%
	セキュリティ 3A	15.7%	16.0%	16.0%
	アジア太平洋州 計	15.9%	16.3%	16.5%
北米	ファイアウォール / VPN	48.3%	46.9%	45.3%
	IDS / IPS	54.8%	52.5%	50.7%
	その他セキュリティソフトウェア	52.4%	52.4%	52.8%
	セキュアコンテンツ管理	45.8%	45.7%	45.4%
	セキュリティ 3A	48.7%	47.9%	47.4%
	北米 計	48.1%	47.4%	46.7%
西欧	ファイアウォール / VPN	30.5%	30.7%	30.7%
	IDS / IPS	25.1%	26.2%	27.2%
	その他セキュリティソフトウェア	25.9%	26.1%	26.3%
	セキュアコンテンツ管理	33.3%	33.3%	33.6%
	セキュリティ 3A	30.7%	30.9%	31.3%
	西欧 計	31.1%	31.4%	31.7%
その他	ファイアウォール / VPN	6.6%	7.2%	7.8%
	IDS / IPS	4.6%	4.6%	4.6%
	その他セキュリティソフトウェア	4.3%	4.4%	4.5%
	セキュアコンテンツ管理	4.4%	4.4%	4.3%
	セキュリティ 3A	5.0%	5.2%	5.3%
	その他 計	4.9%	4.9%	5.0%
全体	ファイアウォール / VPN	100.0%	100.0%	100.0%
	IDS / IPS	100.0%	100.0%	100.0%
	その他セキュリティソフトウェア	100.0%	100.0%	100.0%
	セキュアコンテンツ管理	100.0%	100.0%	100.0%
	セキュリティ 3A	100.0%	100.0%	100.0%
	総計	100.0%	100.0%	100.0%

出典：表 24 に同じ

注：セキュリティ 3A とは、承認：Authorization、認証：Authentication、管理：Administration、の 3 機能の総称

表 26 世界の情報セキュリティソフトウェア地域別市場成長率

地域	セキュリティソフトウェア分類	2004 年	2005 年	2003 年～2005 年 年平均成長率
アジア太平洋	ファイアウォール/VPN	10.7%	12.8%	11.7%
	IDS/IPS	20.9%	15.8%	18.3%
	その他セキュリティソフトウェア	13.3%	10.4%	11.8%
	セキュアコンテンツ管理	24.6%	20.8%	22.7%
	セキュリティ 3A	17.1%	14.4%	15.8%
アジア太平洋州 計		19.9%	17.1%	18.5%
北米	ファイアウォール/VPN	2.6%	2.5%	2.5%
	IDS/IPS	7.0%	7.0%	7.0%
	その他セキュリティソフトウェア	15.0%	17.0%	16.0%
	セキュアコンテンツ管理	23.0%	18.5%	20.7%
	セキュリティ 3A	12.6%	13.4%	13.0%
北米 計		15.1%	13.9%	14.5%
西欧	ファイアウォール/VPN	6.4%	6.2%	6.3%
	IDS/IPS	16.4%	15.1%	15.7%
	その他セキュリティソフトウェア	15.8%	17.3%	16.5%
	セキュアコンテンツ管理	23.3%	20.1%	21.7%
	セキュリティ 3A	15.1%	16.1%	15.6%
西欧 計		18.0%	16.9%	17.5%
その他	ファイアウォール/VPN	14.6%	15.0%	14.8%
	IDS/IPS	10.9%	10.9%	10.9%
	その他セキュリティソフトウェア	17.5%	18.2%	17.9%
	セキュアコンテンツ管理	21.0%	16.6%	18.8%
	セキュリティ 3A	17.4%	18.1%	17.7%
その他 計		17.7%	16.4%	17.1%
全体	ファイアウォール/VPN	5.7%	6.1%	5.9%
	IDS/IPS	11.7%	10.8%	11.2%
	その他セキュリティソフトウェア	15.0%	16.0%	15.5%
	セキュアコンテンツ管理	23.3%	19.3%	21.3%
	セキュリティ 3A	14.3%	14.6%	14.5%
全体 計		16.9%	15.5%	16.2%

出典： 表 24 に同じ

注：セキュリティ 3A とは、承認：Authorization、認証：Authentication、管理：Administration、の 3 機能の総称

【ソフトウェア製品分類別の地域比較】

ここでは製品分類単位で内外比較を試みることにする。本調査と IDC 社の地域別調査の製品分類は厳密には異なるが、概ね表 27 のような対応関係にある。

表 27 情報セキュリティソフトウェアに関する本調査の定義と IDC 定義の比較

IDC 調査定義	本調査の定義
ファイアウォール / VPN IDS / IPS	アクセス制御製品
セキュリティ 3A ソフトウェア	アクセス管理製品 システムセキュリティ管理製品
セキュアコンテンツ管理製品	セキュアコンテンツ管理製品
その他セキュリティソフトウェア	暗号製品

対比するために日本市場の情報セキュリティソフトウェア製品の数値を集計したものを表 29 に示す。海外の数値については表 24 を用いる。両者を上記対照関係に従って整理し、日本対アジア太平洋地域市場ならびに世界市場のシェア数値としてまとめたものを表 28 に示す。

表 28 セキュリティソフトウェア製品分類別の日本市場の対アジア太平洋地域 / 世界シェア

日本 / アジア太平洋地域比率		2003 年	2004 年	2005 年
セキュリティ ソフトウェア 分類	アクセス管理製品 システムセキュリティ管理製品	64.4%	64.9%	64.3%
	アクセス制御製品	47.2%	44.6%	41.2%
	セキュアコンテンツ管理ソフトウェア	69.5%	62.4%	59.6%
	暗号製品 暗号製品	63.3%	67.3%	69.5%
合計		63.1%	59.9%	57.9%

日本 / 世界比率				
セキュリティ ソフトウェア 分類	アクセス管理製品 システムセキュリティ管理製品	10.1%	10.4%	10.3%
	アクセス制御製品	7.1%	7.1%	6.9%
	セキュアコンテンツ管理ソフトウェア	11.4%	10.4%	10.0%
	暗号製品	11.1%	11.6%	11.4%
合計		10.0%	9.8%	9.6%

出典：表 24 のデータと本調査数字より算出

この結果、日本市場のアジア太平洋地域全体に占める比率は2003年には63.1%であるが、2005年には57.9%まで低下すると予測される。個別セグメントでは、「ファイアウォール/VPNソフトウェア、IDS/IDPソフトウェア」が相当低く、「その他セキュリティソフトウェア」が比較的高い比率となっている。また「セキュアコンテンツ管理ソフトウェア」が急速にシェアを下げる。ファイアウォール/VPN、IDS/IDPといったアクセス制御ツールは最もアプライアンス化の進んだカテゴリであり、その中で日本は相対的にアプライアンス化が遅れている。これは後に表30で見るところにも現れている。しかるに、上記分析ではそれをソフトウェアで補っている姿も見えず、相対的に日本はアジア太平洋に比べてアクセス制御分野へのセキュリティ投資が少ないことを意味する。ファイアウォールの普及率の高さからは想定しにくい結果である。一つの可能性としては、日本では比較的早くからファイアウォールの導入が進み、既に投資が一巡しているため、ソフトウェア、アプライアンスに限らず市場規模が拡大しにくい構造になっているということである。歴史的に見ても日本は1990年代後半からかなりのペースでファイアウォールの導入が進んでおり、アジア地域に先行していたのは事実であるから、これが原因である可能性は高い。

一方世界市場に対する情報セキュリティソフトウェア全体のシェアはおよそ10%程度であるが、ここでもアクセス制御ソフトウェアの比率が7%程度と低くなっている。世界市場との比較においては、情報セキュリティ対策先進地域の北米地域が占める比率が大きいため、同様の論理構成による説明は成立しにくい。この点は今後の時系列的観測が行われ、複数の調査データが得られる中で明らかにされると思われる。ただし、このデータをそのまま受け止めれば、日本におけるファイアウォール等の更新投資が停滞する中で、製品の陳腐化が進んでいる可能性を示唆することになる。セキュリティの脅威の進化につれて対策も更新する必要がある点を、一度見直すきっかけとすべきではないかと考える。

表 29 日本の情報セキュリティソフトウェア市場規模 実績と予測（百万円）

セキュリティソフトウェア分類	平成 15 年度	平成 16 年度	平成 17 年度
アクセス管理製品	26,524	28,081	31,062
アクセス制御製品	14,166	15,463	16,329
システムセキュリティ管理製品	5,259	9,449	11,450
セキュアコンテンツ管理製品	45,217	50,686	58,581
暗号製品	3,565	4,289	4,893
総計	94,730	107,967	122,315
<b>製品別シェア</b>			
アクセス管理製品	28.0%	26.0%	25.4%
アクセス制御製品	15.0%	14.3%	13.4%
システムセキュリティ管理製品	5.6%	8.8%	9.4%
セキュアコンテンツ管理製品	47.7%	46.9%	47.9%
暗号製品	3.8%	4.0%	4.0%
総計	100.0%	100.0%	100.0%
<b>市場成長率</b>			
アクセス管理製品	-	5.9%	10.6%
アクセス制御製品	-	9.2%	5.6%
システムセキュリティ管理製品	-	79.7%	21.2%
セキュアコンテンツ管理製品	-	12.1%	15.6%
暗号製品	-	20.3%	14.1%
総計	-	14.0%	13.3%

### 9.2.2. 地域別情報セキュリティハードウェア市場との比較

情報セキュリティハードウェア製品については、入手可能なデータが限られるため、情報セキュリティハードウェア全体での比較は困難なことから、セキュリティ・アプライアンス製品の地域別市場を日本市場と比較することとする。

この項における分析には、米国 IDC 社から刊行予定の各地域のアプライアンスに関する統計データの提供を受け、それを用いた。またここで対象とするセキュリティ・アプライアンス製品とは、統合型アプライアンス製品、アクセス制御製品の中のファイアウォール / VPN アプライアンス、IDS / IPS アプライアンス、の 3 セグメントに限るものとする。また比較対象とする地域区分の定義も情報セキュリティソフトウェアとは異なり、米国、西欧地域、アジア太平洋地域（日本を除く）、日本、その他地域の 5 区分となる。

表 30 に世界地域別のセキュリティ・アプライアンス市場規模並びに地域別構成比を示した。表 31 は本調査におけるアプライアンスの数字だけを抜き出して再集計したものである。世界市場規模は 2004 年に 1,883 億円、2005 年に 2,661 億円、2006 年に 3,372 億円と予測され、2 年間の平均成長率は 33.8%と非常に高い。2004 年の地域別の市場規模分布は、ほ

ば米国 1.5 対 西欧地域 1 対 「アジア太平洋地域 + 日本」1 の比率となる。地域別の 2003 年～2005 年の平均市場成長率は、西欧が 40.7%、アジア太平洋が 49.9%と高く、米国では 28.3%である。日本は 17.1%とこの比較対照の中では最も低い。この結果米国の対世界セキュリティ・アプライアンス市場シェアは徐々に低下する傾向にある。日本の状況は、9.1 章で分析したように、「情報セキュリティツール」市場ではハードウェアの普及の遅れが見られ、これが顕著に表れた結果と言えよう。

また前章で示した情報セキュリティソフトウェアの地域別構成比、北米 2.3：西欧 1.6：アジア太平洋 1 (9.2.1.章では 3：2.1：1.3 の数字で表したが、アジア太平洋地域を 1 とし再計算した結果)と比較すると、アジア太平洋地域のセキュリティ・アプライアンス市場シェアは相対的に高くなっていることも分る。また日本と日本以外のアジア太平洋地域の市場シェア及び市場成長率の推移を比較してみると、日本以外のアジア太平洋地域でセキュリティ・アプライアンスの普及が急速に進んでいることがわかる。

表 30 に、日本のセキュリティ・アプライアンス市場の対世界市場シェアと対アジア太平洋地域 (日本市場を含む) シェアを示した。2004 年の日本の対世界市場のシェアは 9.9%で、これは IT 市場全体で比較したときのハードウェアの対世界市場シェア 11% (表 22 参照) より若干低い。日本におけるセキュリティ・アプライアンス選好の立ち遅れを示すデータと考えられる。一方、対アジア太平洋地域のシェアは 35.5%であり、前章の情報セキュリティソフトウェア市場の対アジア太平洋地域シェア 60.6%と比較しても、また GDP ベースの相対比 (日本はアジア太平洋地域全体の 55%) や IT 投資額の相対比 (日本はアジア太平洋地域全体の 52%) と比較しても、非常に低い。2003 年段階では 45.5%であり、2004 年に日本を除くアジア太平洋地域のアプライアンス市場が急拡大する影響を受けて 2004 年にシェアは 10 ポイント下がっている。いずれの数字で見ても、GDP の日本対アジア太平洋地域の比率や IT 投資の日本対アジア太平洋地域の比率に比べて極端に低いと言える。

この理由としては、まず一般論的に、アプライアンスが持つ共通特性である、導入の容易さ、スループット等性能の良さ、コストパフォーマンスの良さ等が挙げられる。この特性が、初めてアクセス制御製品を導入しようとするときにソフトウェアよりはアプライアンスを選好する動きを強めることは想像に難くない。日本はアプライアンスの本格供給前に、ファイアウォールや IDS の導入を終えているという事情も加わる。つまり、日本とアジア太平洋地域の市場の成熟度ライフサイクルの差が集中的に現れる、潮目の時期である可能性がある。更に、それに加えてアジア太平洋地域の特性として、サポート・メンテナンス環境の問題が挙げられる。この地域は個別市場規模が小さいために、販売業者が比較的零細で技術蓄積も低く、サポート能力も限られる。そのような中で故障や不具合が発生した場合に、ソフトウェアをサーバに搭載したシステムのように故障箇所の切り分けをすることなく、単体製品を丸ごと入れ替えて、つなぎ直すだけで復旧できる手軽さは大きなメリットとなる。現に世界的ベンダーはアジア太平洋地域で物流業者と組んで短時間の代替品交換体制を整えており、アプライアンス製品の浸透戦略の重要な鍵を握っている。

これらの要因が絡み合って、アジア太平洋地域ではセキュリティ・アプライアンス導入のブームが到来し、日本は逸早く卒業すると同時に 9.1.4.章で見たような外国製ハードウェア導入へのためらいからアプライアンス化のペースが鈍い、その総合的作用の結果である可能性が高いと分析する。

**表 30 世界のセキュリティ・アプライアンス 各国、地域別市場規模 実績と予測（百万円）**

	2003 年	2004 年	2005 年	2003-2005 年平均成長率
日本	23,145	26,239	31,718	17.1%
アジア太平洋地域	27,757	47,751	62,329	49.9%
アジア + 日本	50,902	73,990	94,047	35.9%
米国	77,201	103,710	127,030	28.3%
西欧地域	48,075	72,703	95,221	40.7%
その他地域	12,122	15,706	21,025	31.7%
世界全体	188,298	266,109	337,322	33.8%
<b>地域別シェア</b>				
日本	12.3%	9.9%	9.4%	
アジア太平洋地域	14.7%	17.9%	18.5%	
アジア + 日本	27.0%	27.8%	27.9%	
米国	41.0%	39.0%	37.7%	
西欧地域	25.5%	27.3%	28.2%	
その他地域	6.4%	5.9%	6.2%	
世界全体	100.0%	100.0%	100.0%	
日本の 「アジア+日本」 に対するシェア	45.5%	35.5%	33.7%	

出典：米国 IDC 社調査データ、Asia/Pacific ( Excluding Japan ) Security Appliance 2004 Review and 2005-2009 Forecast、IDC Security Appliance Server Tracker 2005 Q1、Western Europe Security Appliance 2005-2009 Forecast and 2004 Competitive Vendor Shares ( 以上 2005 年 4 月以降公開予定 ) 等のデータ並びに本調査データ ( 表 31 ) より合成

< 1 ドル=116.01 円で円換算 >

表 31 日本のセキュリティ・アプライアンス市場規模 実績と予測（百万円）

アプライアンス製品分類	平成 15 年度	平成 16 年度	平成 17 年度	
ファイアウォール / VPN	19,584	16,384	16,762	
IDS / IPS	2,679	5,766	7,660	
統合型	883	4,089	7,296	
総計	23,145	26,239	31,718	
<b>シェア</b>				
ファイアウォール / VPN	84.6%	62.4%	52.8%	
IDS / IPS	11.6%	22.0%	24.2%	
統合型	3.8%	15.6%	23.0%	
総計	100.0%	100.0%	100.0%	
<b>成長率</b>				平成 15 ~ 17 年 年平均成長率
ファイアウォール / VPN	-	-16.3%	2.3%	-7.5%
IDS / IPS	-	115.3%	32.9%	69.1%
統合型	-	363.2%	78.4%	187.5%
総計	-	13.4%	20.9%	17.1%

### 9.2.3. 地域別情報セキュリティサービス市場との比較

ここでは、「情報セキュリティサービス」市場について日本と海外との比較分析を試みる。(しかし 9.1.2 章で述べたように本レポートにおける「情報セキュリティサービス」の定義と IDC 社の調査における定義に乖離が見られるため、ここでは直接市場規模の比較は行わず、主に市場の変化、成長傾向についてのみの比較とする。)表 37 は米国 IDC 社が 2004 年 12 月に発表した「Worldwide and U.S. Security Services 2004-2008 Forecast, Doc#31054」と題する調査報告書に基づく世界地域別の「情報セキュリティサービス」市場規模である。市場規模は、ほぼアメリカ地域<sup>10</sup>：欧州・中東・アフリカ地域<sup>11</sup> 2.5：アジア太平洋地域<sup>12</sup>：1 となる。IT 市場においては、地域の定義にかなりの違いはあるが、北米、西欧、及びアジア太平洋の 3 地域の比率は、2.3：1.6：1 である。(9.2.1 章、9.2.2 章参照)

IT 市場規模の地域比に対して情報セキュリティソフトウェアのアジア太平洋地域の比率が低いことは 9.2.1.章で見たが、セキュリティ・アプライアンスではアジア太平洋地域の相対的位置は相当大きかった。情報セキュリティサービスにおいては、アジア太平洋地域の相対位置が最も低いように見える。一般的に情報セキュリティ対策は、個別の外部脅威に対する対策を「点」として並べるものが徐々に「線」になり「面」になることでより総合化して行き、更にはトータルな管理体制の構築やそのためのコンサルテーション・教育の活用へと向かっていく流れがある。これをライフサイクルとして捉えると、アジア太平洋地域はその比較的若井段階にあり、そのためにソフト化・サービス化の進捗が遅いと理解してよいと思われる。

このことは逆に市場の活性という意味ではプラスに働くはずで、アジア太平洋地域の「情報セキュリティサービス」市場の成長率は若干他の地域よりは高い。2004 年と 2005 年の年間成長率は、アジア太平洋地域は 21%前後、アメリカは 20%前後、欧州/中東アフリカは 18%前後の成長率で推移している。また前述の通り、日本の「情報セキュリティサービス」市場の成長率は、平成 15(2003)～17(2005)年度の年平均成長率で 20.6%である。やはり若干ではあるがアジア太平洋地域のポテンシャルの高さを暗示させる。ただし、アメリカ地域及び欧州・中東・アフリカ地域については対象とする国の範囲に様々な発展段階の国が混在する定義となっていることから、1～2%の差が意味するところの厳密な評価は難しいと判断する。

サービスの生産・消費の属地性の問題も含め、グローバルな比較を精度高く行うために

<sup>10</sup> アメリカ地域には、北米地域(脚注 5 を参照)とラテンアメリカ地域のアルゼンチン、ブラジル、チリ、コロンビア、メキシコ、ベネズエラ、及びその他ラテンアメリカ各国を含む。

<sup>11</sup> 欧州地域には、西欧地域(脚注 6 を参照)と中東欧地域のブルガリア、クロアチア、チェコ、ハンガリー、ポーランド、ルーマニア、ロシア、スロバキア、及びその他中東欧各国を含む。

<sup>12</sup> アジア太平洋地域は、脚注 7 を参照。

は、ベースデータの収集から改めて取り組み直す必要があると考える。

表 32 世界地域別情報セキュリティサービス市場規模 実績と予測（百万円）

地域	2003 年	2004 年	2005 年
アメリカ	666,825	796,409	958,011
アジア太平洋	166,474	201,625	244,897
欧州 / 中東アフリカ	391,882	461,604	547,335
総計 (Worldwide)	1,225,182	1,459,638	1,750,243
<b>市場シェア</b>			
アメリカ	54.4%	54.6%	54.7%
アジア太平洋	13.6%	13.8%	14.0%
欧州 / 中東アフリカ	32.0%	31.6%	31.3%
総計 (Worldwide)	100.0%	100.0%	100.0%
<b>市場成長率</b>			
アメリカ	-	19.4%	20.3%
アジア太平洋	-	21.1%	21.5%
欧州 / 中東アフリカ	-	17.8%	18.6%
総計 (Worldwide)	-	19.1%	19.9%

出典：米国 IDC 社、(Worldwide and U.S. Security Services 2004-2008 Forecast, Document#31054 2004 年 12 月)

< 1 ドル=116.01 円で円換算 >

### 9.3. 韓国情報セキュリティ市場との比較

次に世界の中でも、IT 先進国としての立場を確立している韓国の情報セキュリティ市場と日本市場の比較を行う。韓国においてはブロードバンドの整備率、インターネットの普及率が逸早く世界有数のレベルに達しており、政府による情報セキュリティ産業政策も手厚く、電子政府への取り組みも進んでいる。そのような韓国の市場実態との比較は、隣国としての意味も含め意義深いものとする。(韓国情報通信部の発表によれば、2003 年時点で韓国のインターネット利用率は 60.3%で世界第 2 位、ブロードバンドインターネット普及率は 23.2%と世界第 1 位である。<sup>13)</sup>

韓国の情報セキュリティ市場実態に関する調査は韓国内の事業者に委託し、2004 年 11 月の韓国情報保護産業協会 (www.kisia.or.kr) の調査結果<sup>14)</sup>と、2004 年 6 月の韓国電算院 (www.nca.or.kr) の統計調査<sup>15)</sup>による研究資料を元にして作成したものである。本章ではその調査結果としての市場規模の数字と日本市場の数字の比較を中心に分析を行う。調査

<sup>13)</sup> IPA / ISEC (独立行政法人 情報処理推進機構 セキュリティセンター) 調査報告書「各国の情報処理セキュリティ投資に対するインセンティブ調査 2005 年 2 月」より抜粋

<sup>14)</sup> 韓国情報保護産業協会「2004 年韓国情報保護産業統計調査報告書」

<sup>15)</sup> 韓国電算院「2004 年情報化統計集」

報告の原文は付録 1 として収録したので、細かいデータはそちらを参照願いたい。

なお、韓国の市場規模は全て暦年（1 月～12 月期）での値となるが、便宜上今回の年度調査結果（4 月～3 月期）とそのまま比較している。また韓国市場規模の金額は、2003 年の年間平均為替交換レート 1 ウォンあたり 0.0971 円を使用して全て換算している。（為替レートのデータは、OANDA Currency Converter, Historical Currency Table（<http://www.oanda.com/convert/fxhistory>）による。<sup>16</sup>）

表 33 に韓国情報セキュリティ市場規模の実績と予測を示す。2003 年の市場規模は 569 億円で、日本の市場規模 3,607 億円の 15.8%、2004 年は 631 億円で日本の 4,438 億円に対して 14.2%という対比となる。IT 市場全体では 2004 年の韓国の市場規模は日本に比較すると 13%（米国 IDC 社報告書、The Worldwide Black Book 2004, 2004 年 12 月による）となる。GDP の比較では韓国は日本の 12%程度である。<sup>17</sup> 日本対韓国という比較で見ると、その経済規模の比に比べて韓国の IT 投資比率は高く、その中に占める情報セキュリティ投資の割合も若干高いということが言える。

韓国における情報セキュリティ市場の成長率に着目すると、2004 年は 10.9%程度であるが、2005 年は 20.4%と急拡大する予測である。一方、付録に記載されている製品カテゴリごとの長期予測からも見て取れるように、2006 年以降の成長率は総じて 10%前後の落ち着いたものになると見られている。日本市場の成長率も年による変動があり、個人情報保護法の施行と情報漏えい事件の頻発の影響で平成 16(2004)年度は 23.0%と高まり、平成 17(2005)年度は 14.3%と落ち着くと予測されている。

2005 年の韓国市場では全ての情報セキュリティ製品市場で成長率が高まると予測されている。市場成長率が最も高い分野は情報セキュリティサービス分野で、対前年比成長率は 2004 年が 12.1%、2005 年が 25.3%と予測されている。しかし情報セキュリティソフトウェア市場も 2004 年の 9.9%から 2005 年の 20.8%へ、情報セキュリティハードウェア市場も 11.5%から 18.6%に急拡大する傾向は同様である。

日本市場と比較した場合、情報セキュリティツールと情報セキュリティサービスの構成比が、2003 年で 86.7%対 13.3%と、極端にツール偏重の結果となっている。ちなみに同年度の日本の比率は 34.9%対 65.1%である。これは、韓国の情報セキュリティサービス統計が、「セキュアシステム構築サービス」を対象としていないことによる。日本の場合「セキュアシステム構築サービス」はサービス全体の 4 分の 3 程度を占めるので、この要素を差し引くと概算でツール対サービスが 2：1 程度となるが、これに比べても韓国のツール偏重の市場構造は注目される。

---

<sup>16</sup> 脚注 4 参照

<sup>17</sup> 外務省発表の APEC の主要経済指標(2004 年)より JNSA 算出

また韓国市場の、ハードウェアとソフトウェアの市場構成比は、調査対象の 2003～2005 年を通じて概ね 46 対 41 であり、(表 33 参照) ほぼ 1:1 と考えられる。世界市場の構成比の 3:7 や、日本市場の構成比 1:3 (9.1.1 章を参照) の比率と比較すると韓国ではハードウェアの構成比が非常に高い。この理由としては調査対象とする情報セキュリティツールの範囲が、たとえば韓国の統計ではファイアウォール・ソフトウェアが含まれていないなど、相当異なることによると見られる。また、ハードウェア市場にカウントされる「セキュリティスマートカード」が日本市場の「個人認証用 IC カードシステム」の 2 倍あるとか、「生体認証デバイス(装置・機器)」が日本市場とほぼ同金額あるとかいう相異が影響していると分析できる。この理由としては、韓国内では、政府や地方自治体の IT 化政策が進展しており、行政サービス提供時の認証手段として IC カード等の個人認証デバイス(装置・機器)の利用が多いことが影響しているのではないだろうか。

韓国では、現在進行中の行政機関情報化計画 e-KOREA ビジョン 2006 に先駆けて、「サイバー21」計画を実施し、1999 年～2001 年に完了している。この計画に基づいて情報通信網の高度化、高速化が行われ、このインフラを利用した情報産業の拡大政策が展開された。日本では Y2K 問題への対応を乗り越え、次のステップとして e-Japan 重点計画が動き出そうという政策対応の流れであったと理解されるが、韓国では逸早く情報基盤の整備に着手していたという関係が見える。2001 年には韓国の政府電子決済率、公共電子調達率は 80%を超えており、行政の電子化については最先端を走っていた。e-KOREA ビジョン 2006 では更にこれを進展させ、グローバル化への対応、ユビキタス環境での業務対応などを整備している。しかしやはり急激な IT 化による弊害として、デジタルデバイドの発生、情報セキュリティの問題がクローズアップされてきたのも事実である。行政が高度に電子化されたことにより、ハッキングやウイルス被害、個人情報漏えいなどへの対策に注力する必要性が高いのである。特に韓国では 1968 年から全国民が必ず一つ住民登録番号を持つ制度になっている。この番号は住民登録台帳に記載されて公共機関のみで使われるだけでなく、あらゆる場所で本人確認の情報として利用されている。韓国ではほとんどのインターネットサイトの会員登録は実名制であり、この住民登録番号が個人認証の手段として利用されることで、個人情報漏えいによる実質的な被害が発生する確率は日本より高く、深刻な問題となりうる。

表 33 韓国情報セキュリティ市場規模 実績と予測（百万円）

	2003 年	2004 年	2005 年
<b>セキュリティツール</b>	49,354	54,636	65,350
セキュリティハードウェア	26,072	29,060	34,452
セキュリティソフトウェア	23,282	25,576	30,898
セキュリティサービス	7,571	8,490	10,639
合計	56,925	63,127	75,990
<b>製品別市場シェア</b>			
セキュリティツール	86.7%	86.6%	86.0%
セキュリティハードウェア	45.8%	46.0%	45.3%
セキュリティソフトウェア	40.9%	40.5%	40.7%
セキュリティサービス	13.3%	13.4%	14.0%
合計	100.0%	100.0%	100.0%
<b>市場成長率</b>			
セキュリティツール	-	10.7%	19.6%
セキュリティハードウェア	-	11.5%	18.6%
セキュリティソフトウェア	-	9.9%	20.8%
セキュリティサービス	-	12.1%	25.3%
合計	-	10.9%	20.4%

出典：2004 年度 11 月の韓国情報保護産業協会（www.kisia.or.kr）の調査結果と、2004 年度 6 月の韓国電算院（www.nca.or.kr）の統計調査による研究資料

< 100 ウォン=97.1 円で円換算 >

全体に、韓国においては政府主導で国全体が動く傾向が日本より強いとの感じを受けるが、情報化政策における官主導の流れは際立っていた感がある。そして、安全保障の観点から国産情報セキュリティ技術の育成策がとられた結果、国内市場依存で存立しうるベンダーを多く輩出する結果になっているとも読み取れる。それらベンダーが、政府の育成策・保護策のない状態で国際競争にさらされていたとしたら、市場原理からは成立が困難な局面も見られた可能性があるのではなかろうか。社会経済的視点から外すことのできない重要部分に関する行政の関与という意味で、一つの示唆を含むものと考ええる。市場経済原理を最も生かす形で情報セキュリティ対策が進展する理想的姿に対して、行政の対応がどのような施策を組合せうるか、という意味で、韓国の状況が示唆を与えていると観測される。<sup>18</sup>

<sup>18</sup> 参考文献 独立行政法人 情報処理推進機構「韓国における情報セキュリティ政策に関する調査」2004 年 9 月

## 10. まとめ

過去 10 年の間に、独立した市場として形成されるようになった国内情報セキュリティ市場は、平成 15(2003)年度からの 2、3 年の間に大きな変化を見せている。本調査からは、以下のような三つの大きな要因を確認することができた。

- 脅威のあり方の変化

これまででも多くの情報セキュリティに対する脅威が発生し、それらに対する様々な対策が取られてきたが、基本的には外部から侵入する脅威に対して、内部の安全性をいかに確保するかという考え方であった。しかし、近年実際に発生したセキュリティ脅威は内部も安全であるという仮定を最早おくことができないことを示している。そのため、脅威対策も外部とのゲートウェイだけでなく、内部をセグメント化し、各セグメント内に脅威対策を施したり、特定セグメントの感染が他のセグメントに波及しないような方策が取られるようになってきている。また内部ユーザの認証/承認のプロセスの強化を含む、内部ユーザのアクセス管理も強化されてきている。このことは情報セキュリティの論理的、技術的な観点からは進化であると捉えることもできるが、現実の組織における業務の運用という点では大きな制約を課することにもなっていく。情報セキュリティが確保された環境での運用、ビジネスの継続性ということも認識されつつある。

- 総合的な情報セキュリティ体制の導入

ISMS、BS7799 そしてプライバシーマークなどの、情報セキュリティ規格適合性認証を取得する企業の増加、という現象に典型的に見られるように、企業の情報セキュリティへの取り組み姿勢が変わりつつある。情報セキュリティ対策を、情報システムにおける限定的な課題として捉えるのではなく、組織全体のあり方を律するアプローチあるいは切り口の一つとして捉え、一貫した総合的な情報セキュリティ体制を構築しようとする動きが、先進企業においては始まりつつある。情報セキュリティポリシーから、システム設計、運用管理、正しい運用のための要員の教育、そしてポリシー遵守状況の監査といったライフサイクル管理、管理サイクルをきちんと廻していこうという取り組みである。このような動きが今後どのくらいの速度でどの範囲の組織にまで拡大するかは見えにくいところもあるが、中央官庁による海外の状況を見据えた制度への後押しもあり、一定以上の規模の企業や自治体などではこうした総合的な情報セキュリティ体制が早期に導入されるものと考えられる。こうした総合型の情報セキュリティ体制の構築が、ツールやサービスだけでなく、コンサルティングや教育など従来は国内市場では比較的小さかった領域に対して、特に大きな促進要因として働くであろう。

- ソリューションの変化

情報セキュリティソリューションの広い層への拡大を受け、ともすれば煩雑になりがちな情報セキュリティの管理をより容易に行えるようなソリューションへの指向が高まりつつ

つある。具体的には、セキュリティ・アプライアンスであったり、クライアント用の統合セキュリティソフトウェアであったり、あるいはセキュリティ運用管理のアウトソーシングサービスであったり、更にセキュリティ情報管理システム／製品であったりするが、こうしたソリューションが適正な価格で広く提供されることで、一層の市場拡大が見込まれる。

こうした状況を受け、国内の情報セキュリティ市場は今後、よりバランスのとれた発展を遂げていくものと、JNSA は予測する。これにより情報セキュリティ産業が健全な姿で発展し社会への貢献を高める中で、国内の政府、自治体、企業その他あらゆる社会経済主体の活動が、より安全かつ信頼性の高い情報通信システム基盤、ならびに組織管理体系の上に、行われるようになっていくことを期待したい。

以上

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

政策部会 マーケットリサーチ・ワーキンググループ

ワーキンググループリーダー

玉井 節朗 株式会社 IDG ジャパン

プロジェクトリーダー

勝見 勉 グローバルセキュリティエキスパート株式会社

ワーキンググループメンバー

前田 浩 株式会社アークン

塚本 卓郎 IDC Japan 株式会社

番野 邦彦 キヤノンシステムソリューションズ株式会社

郷間 佳市郎 京セラ コミュニケーションシステム株式会社

山田 勝志 クオリティ株式会社

金子 以澄 コンピュータ・アソシエイツ株式会社

小川 博久 株式会社シーフォーテクノロジー

中津 有美 株式会社ジェイエムシー

大槻 兼也 株式会社ヒューコム

村上 博 NPO アイタック

オブザーバー

田中 秀幸 東京大学情報学環・学際情報学府 助教授

以上

## 【付録 1】韓国情報セキュリティ市場調査分析報告

以下は韓国情報セキュリティ市場についての、詳細の報告である。この調査分析報告書は韓国内の事業者に委託し、2004年11月の韓国情報保護産業協会（www.kisia.or.kr）の調査結果<sup>19</sup>と、2004年6月の韓国電算院（www.nca.or.kr）の統計調査<sup>20</sup>による研究資料を元にして作成したものである。韓国の市場規模は全て暦年（1月～12月期）での値となる。韓国市場規模の原数字はウォン建てであるが、比較の便宜上全て円換算した。換算に当たっては、基準年である2003年の年間平均為替レートである、1ウォンあたり0.0971円の為替レートを使用して全て換算している（交換レートは、OANDA Currency Converter, Historical Currency Table（http://www.oanda.com/convert/fxhistory）のデータを参照している<sup>21</sup>）。

### ● 韓国情報セキュリティハードウェア市場

2004年韓国情報セキュリティハードウェア市場規模は291億円と予測され、これは2003年の市場規模261億円と比べると11.5%の成長率である（表34参照）。市場規模が大きい分野は伝統的なネットワークセキュリティ分野のファイアウォール及びVPNでそれぞれ68億円と80億円の市場規模を示している。最近ではIDS/IPS分野の躍進でファイアウォールは市場規模が前年より減少したことが2004年の特徴と言える。対前年比で大幅に成長した分野は生体認証デバイスとスマートカード分野で対前年比市場規模成長率がそれぞれ43.0%と39.8%であった。

表 34 韓国情報セキュリティハードウェア市場規模現況（百万円）

	2003年	2004年	成長率(%)
ファイアウォール	8,541	6,752	-21.0%
IDS/IPS	3,415	4,198	22.9%
VPN(仮想私設網)	6,941	7,982	15.0%
スマートカード	4,155	5,810	39.8%
生体認証デバイス	3,017	4,315	43.0%
合計	26,069	29,057	11.5%

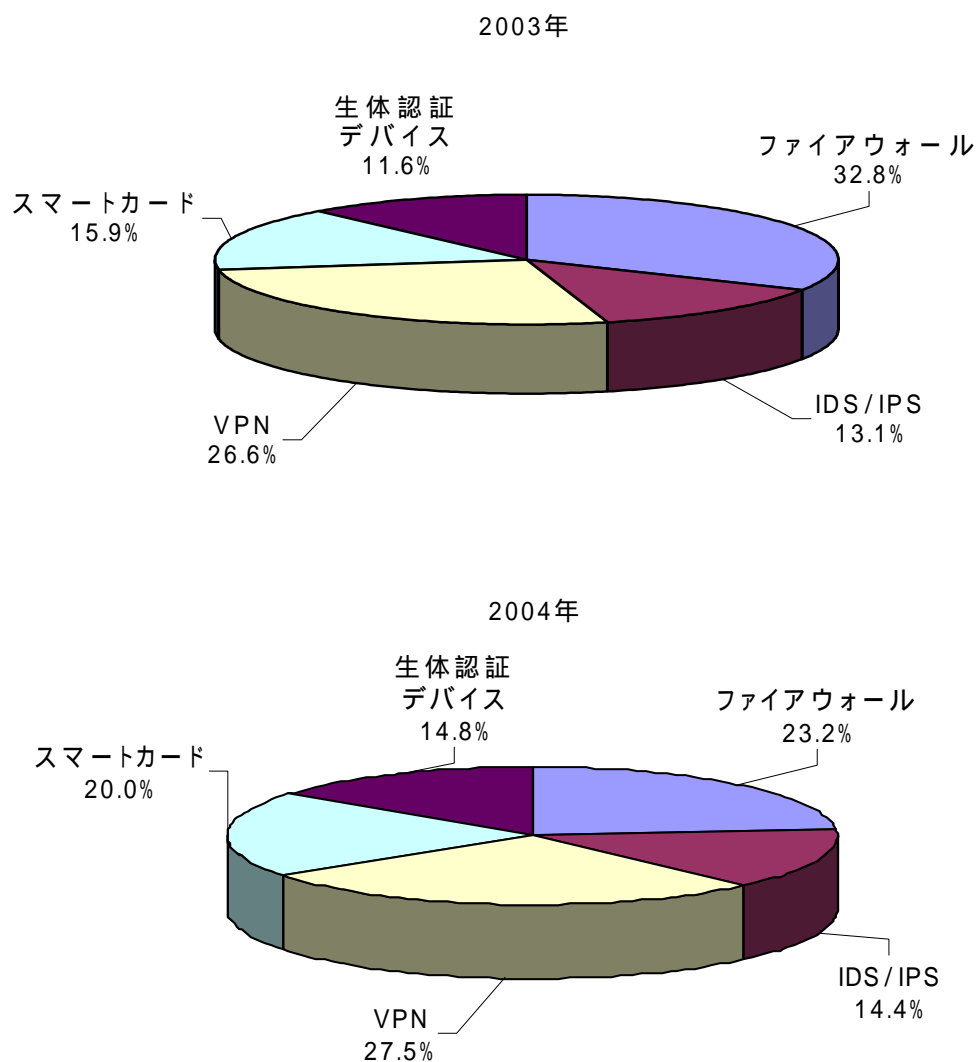
< 100ウォン=97.1円で円換算 >

<sup>19</sup> 韓国情報保護産業協会「2004年韓国情報保護産業統計調査報告書」

<sup>20</sup> 韓国電算院「2004年情報化統計調査」

<sup>21</sup> 脚注4参照

図 16 韓国セキュリティハードウェア市場、分野別構成



韓国情報セキュリティハードウェア市場の2004年～2009年の予測を表35に示す。情報セキュリティハードウェアの市場規模は2004年の291億円から2009年には490億円に拡大し、2004年～2009年の年平均成長率は11.0%と予測されている。

2009年に最大の市場となる分野はVPNで、その規模は143億円と予測されている。

成長率が高いと予測される分野は生体認証デバイス及びスマートカード分野の順で2004年～2009年の年平均成長率がそれぞれ15.3%と13.9%となる。

表 35 韓国情報セキュリティハードウェア市場予測（百万円）

	2004年	2005年	2006年	2007年	2008年	2009年	CAGR (%)
ファイアウォール	6,752	7,286	7,573	7,706	7,767	7,794	2.9%
IDS / IPS	4,198	5,256	5,973	6,442	6,749	6,949	10.6%
VPN	7,982	9,467	10,873	12,134	13,266	14,282	12.3%
セキュリティ スマートカード	5,810	7,324	8,726	9,831	10,622	11,148	13.9%
生体認証デバイス	4,315	5,116	6,006	6,928	7,866	8,807	15.3%
合計	29,057	34,449	39,152	43,042	46,270	48,981	11.0%

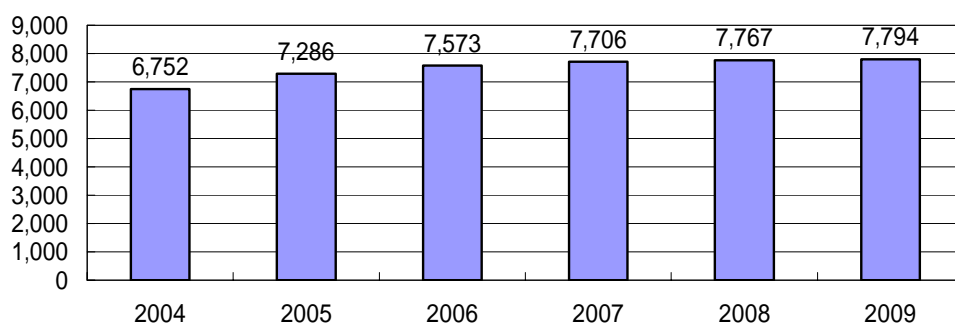
CAGR は、市場規模の 2004 年～2009 年の年平均成長率。

< 100 ウォン=97.1 円で円換算 >

#### ファイアウォール・アプライアンス

セキュリティハードウェア市場のうち、ファイアウォールは市場自体が成熟期の終盤に入っていることと、VPN 等他の製品との機能統合が進展しているためにその成長率は著しく鈍化している。市場規模は 2004 年の 68 億円から 2009 年には 78 億円になる見込みである。2004 年～2009 年の年平均成長率は 2.9%となる。

図 17 韓国ファイアウォール・アプライアンス予測、2004 年～2009 年（百万円）



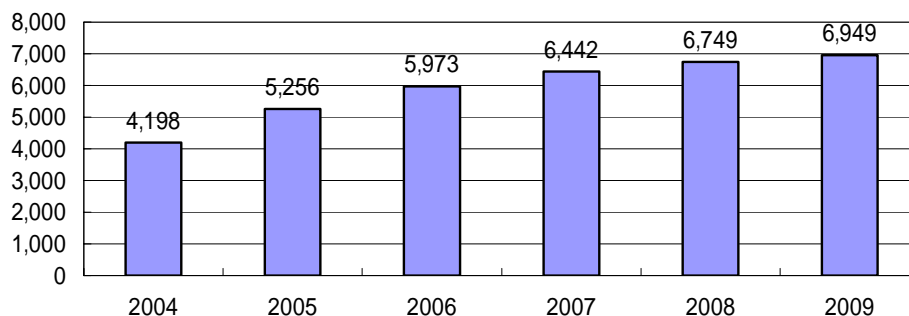
< 100 ウォン=97.1 円で円換算 >

#### IDS / IPS アプライアンス

IDS / IPS ハードウェアは侵入検知、侵入防止システム、統合セキュリティ製品等が含まれているが、市場は成長期に入っている。このため 2005 年以後も変化を見せながら成長の勢いが高くなると予測される分野である。ただし、現在までのデータでは 2009 年までの急激な成長を予測することは難しい。市場規模は 2004 年の 42 億円から 2009 年は 69 億円に

成長すると予測される。

図 18 韓国 IDS / IPS 市場予測 (百万円)

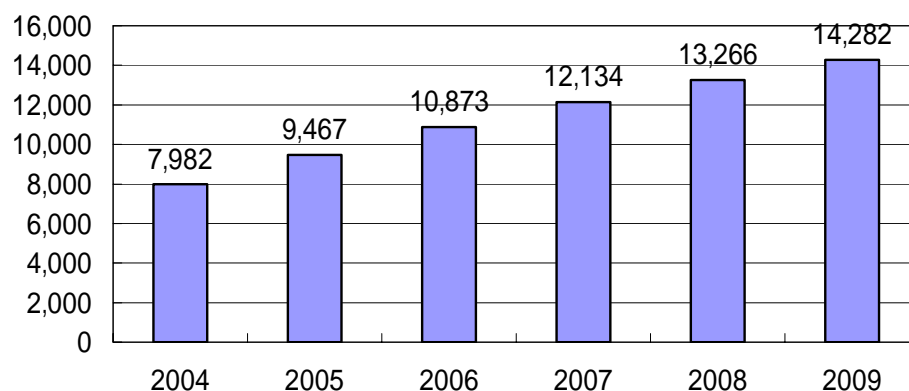


< 100 ウォン=97.1 円で円換算 >

#### VPN アプライアンス

VPN 市場は純粋なプライベートネットワークに準ずるセキュリティ水準が得られることに加えて、価格が低廉であるという長所がある。またファイアウォールシステムと統合された製品の需要が高く、持続的な高成長が予測される分野である。市場規模は 2004 年の 80 億円から 2009 年には 143 億円に達すると予測される。

図 19 韓国 VPN アプライアンス市場予測 (百万円)



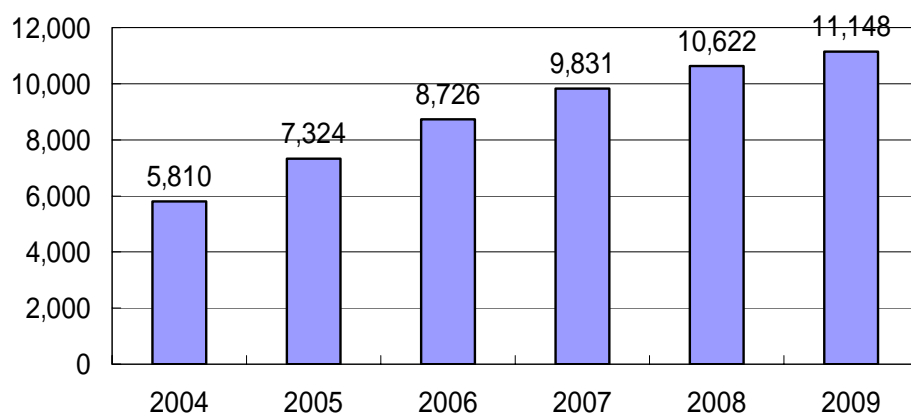
< 100 ウォン=97.1 円で円換算 >

#### セキュリティスマートカード

セキュリティスマートカードは建物の IT 化が急速に広がり、その需要も共に増加するもの

と予測されるが、図 20 に現れているように、その市場規模は 2004 年に 58 億円から 2009 年には 111 億円に拡大する見込みである。(この市場には日本市場調査では除外している入退室管理用途の市場も含まれる。)

図 20 韓国セキュリティスマートカード市場予測(百万円)

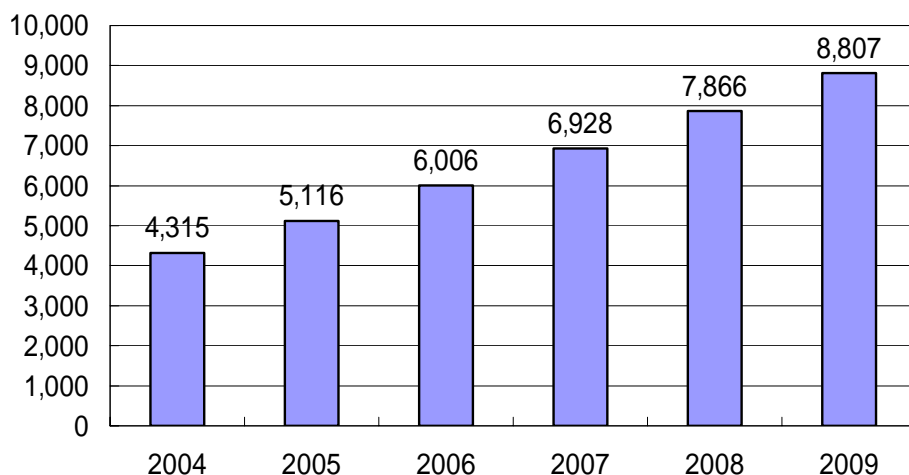


< 100 ウォン=97.1 円で円換算 >

#### 生体認証デバイス

生体認証デバイス製品市場は 2002 年を境目にして、若干の小康状態を見せていた局面もあった。しかし金融業の情報漏えい事故の対応策、デジタル文書及び情報機器アクセス権限統制の手段、テロ防止のための補助手段等で生体認証技術が注目されると見込まれ、今後は安定的な成長が期待される分野である。生体認証デバイスの市場規模は 2004 年の 43 億円から 2009 年は 88 億円まで伸びる見込みである。

図 21 韓国生体認証デバイス市場予測（百万円）



< 100 ウォン=97.1 円で円換算 >

● 韓国情報セキュリティソフトウェア市場

表 36 に示すように、2004 年情報セキュリティソフトウェアの市場規模は 256 億円と予測され、これは 2003 年の 233 億円と比べると 9.9%の成長率である。市場規模の大きな分野はアンチウイルス及びセキュリティ管理ソフトウェアの順となり、その規模はそれぞれ 66 億円と 62 億円であった。

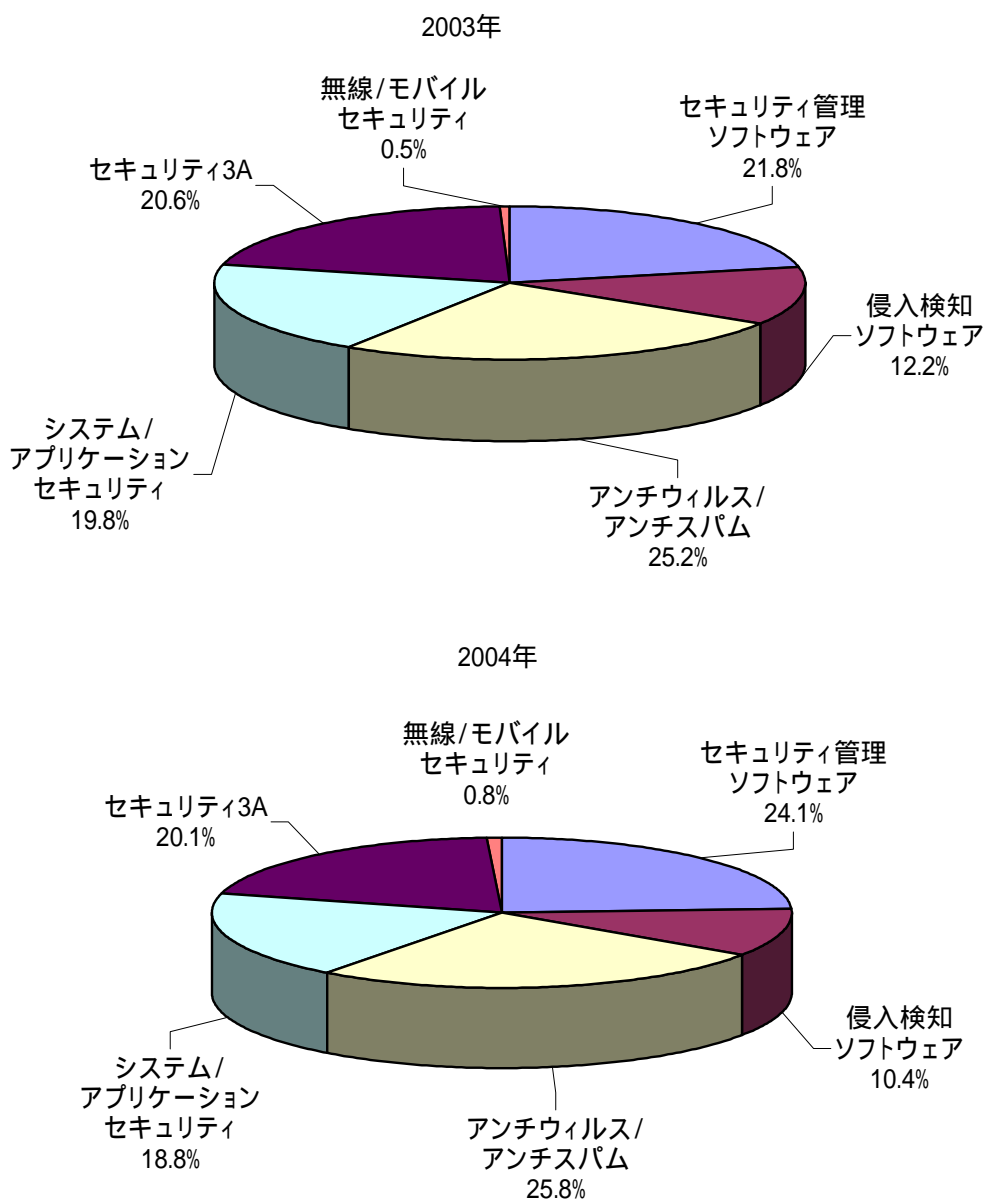
また成長率の最も高い分野は無線モバイルで対前年比成長率が 72.1%で、逆に最も低い分野は侵入検知ソフトウェア市場で対前年比マイナス 6.6%であった。

表 36 韓国情報セキュリティソフトウェア市場規模実績（百万円）

	2003 年	2004 年	成長率 (%)
セキュリティ管理ソフトウェア	5,066	6,170	21.8%
侵入検知ソフトウェア	2,846	2,658	-6.6%
アンチウイルス/アンチスパム	5,863	6,600	12.6%
システム/アプリケーションセキュリティ	4,607	4,817	4.6%
セキュリティ 3A	4,785	5,133	7.3%
無線/モバイルセキュリティ	114	196	72.1%
合計	23,280	25,574	9.9%

< 100 ウォン=97.1 円で円換算 >

図 22 韓国情報セキュリティソフトウェア市場構成、2003年～2004年



韓国情報セキュリティソフトウェアの2004年～2009年の市場予測が表37である。情報セキュリティソフトウェアの市場規模は2004年の256億円から2009年には426億円に達すると見込まれ、2004年～2009年の年平均成長率は10.7%と予測されている。

2009年で最も大きい市場規模の分野はアンチウイルス/アンチスパム及びセキュリティ管理ソフトウェア分野で、その規模はそれぞれ109億円と107億円と見込まれている。また成長率が高いと予測される分野は無線/モバイルセキュリティ分野で2004年～2009年の年平均成長率が29.6%になる。

表 37 韓国情報セキュリティソフトウェア市場予測（百万円）

	2004年	2005年	2006年	2007年	2008年	2009年	CAGR (%)
セキュリティ管理ソフトウェア	6,170	7,551	8,703	9,604	10,256	10,702	11.6%
侵入検知ソフトウェア	2,658	2,765	2,841	2,890	2,920	2,940	2.0%
アンチウイルス/アンチスパム	6,600	7,938	9,065	9,913	10,505	10,896	10.5%
システム/アプリケーション セキュリティ	4,817	5,973	6,858	7,525	8,029	8,410	11.8%
セキュリティ 3A	5,133	6,367	7,093	7,753	8,353	8,899	11.6%
無線/モバイルセキュリティ	196	301	389	489	599	717	29.6%
合計	25,574	30,895	34,949	38,173	40,662	42,564	10.7%

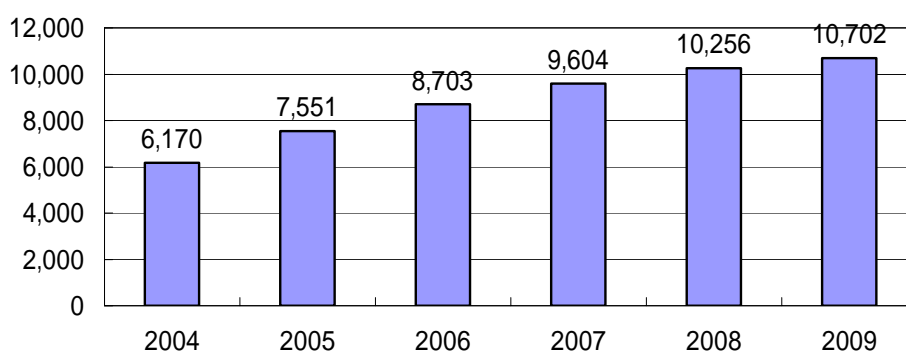
CAGR は、市場規模の 2004 年～2009 年の年平均成長率。

< 100 ウォン=97.1 円で円換算 >

#### セキュリティ管理ソフトウェア

統合セキュリティ管理ツール、ログ分析及び脆弱性分析に対するツール等を含むセキュリティ管理ソフトウェア分野は、セキュリティコンサルティング分野の躍進及び政策的セキュリティ管理認識の強化等に助けられ今後も安定的な成長を見せると期待されている。2004 年の市場規模 62 億円から、2009 年には 107 億円に拡大する見込みである。

図 23 韓国セキュリティ管理ソフトウェア市場予測（百万円）

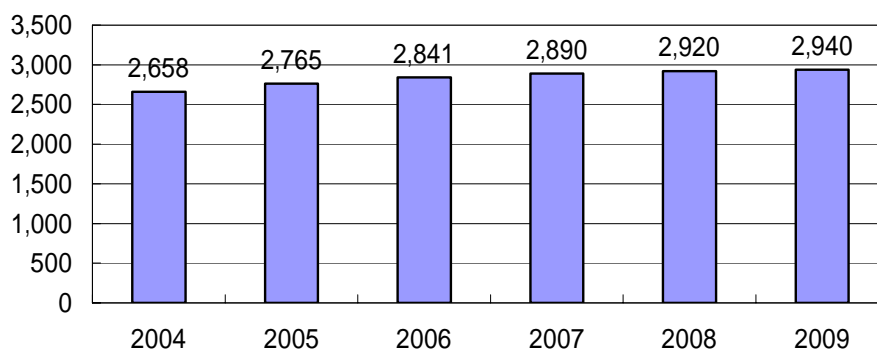


< 100 ウォン=97.1 円で円換算 >

### 侵入検知ソフトウェア

IDS 及び IPS が含まれる侵入検知ソフトウェア市場の場合はハードウェアへの移行等により、典型的な市場成熟期末期の現象を見せている。2004 年～2009 年の年平均市場成長率も 2.0%に留まると予測されている。市場規模は 2004 年の 27 億円から 2009 年には 29 億円になる見込みである。

図 24 韓国 IDS / IPS ソフトウェア市場予測 (百万円)

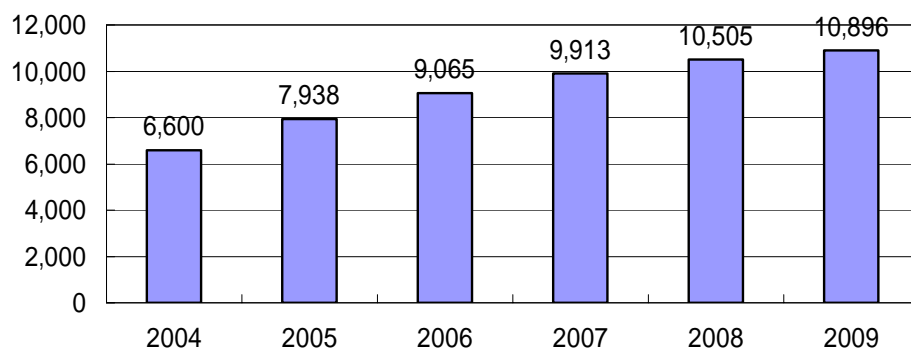


< 100 ウォン=97.1 円で円換算 >

### アンチウイルス / アンチスパム・ソフトウェア

アンチウイルス / アンチスパム市場は徐々に成長の勢いが鈍化する傾向にあるが、統合セキュリティの基礎分野で活用されていることから、ある程度の需要は持続できると見込んでいる。市場規模は 2004 年の 66 億円から 2009 年には 109 億円に拡大する見込みである。

図 25 韓国アンチウイルス/アンチスパム市場予測 (百万円)

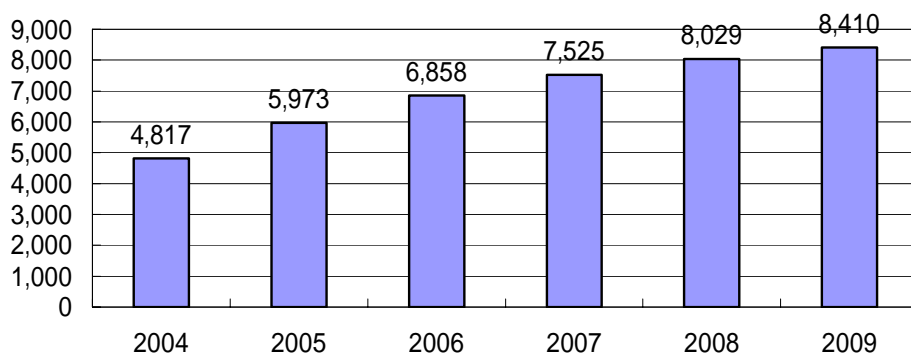


< 100 ウォン=97.1 円で円換算 >

#### システム/アプリケーションセキュリティソフトウェア

システム/アプリケーションセキュリティ分野はインターネット利用の広がりに伴うセキュリティ適用分野の拡大、及びセキュリティ管理の組織化等に助けられて安定的な成長をする見込みである。市場成長傾向は継続し、市場規模は 2004 年の 48 億円から 2009 年は 84 億円に拡大する見込みである。

図 26 韓国システム/アプリケーションセキュリティ市場予測 (百万円)

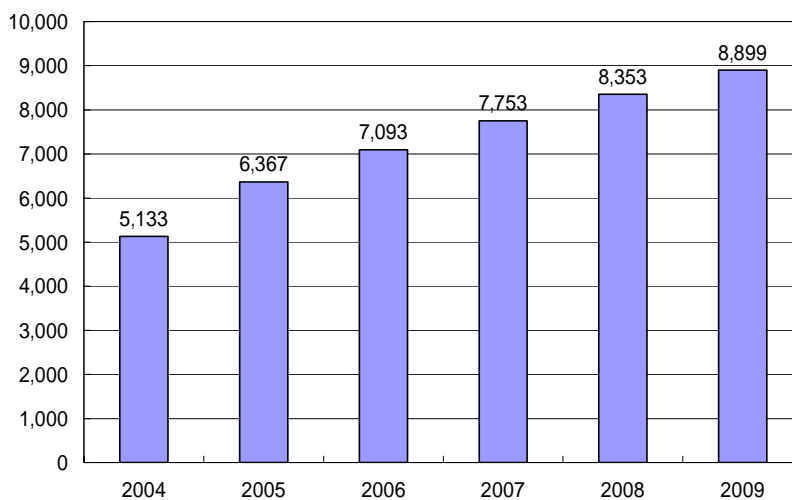


< 100 ウォン=97.1 円で円換算 >

### セキュリティ 3A ソフトウェア

セキュリティ 3A 分野の市場予測は金融業務において PKI に対するユーザー層が一般化されることで、成長率が高まる傾向をみせると予測される分野である。特に、電子取引市場が B2C から B2B 及び B2G へ拡大することが追加的な成長要因として作用すると予測される。市場規模は 2004 年の 51 億円から 2009 年には 89 億円に拡大する見込みである。

図 27 韓国セキュリティ 3A ソフトウェア市場予測 (百万円)

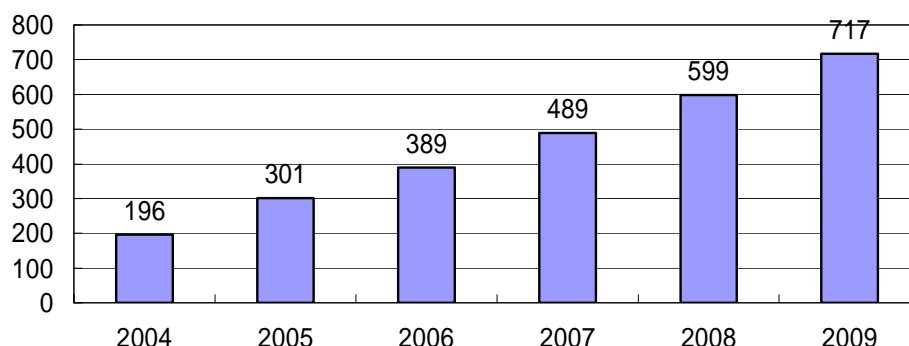


< 100 ウォン=97.1 円で円換算 >

### 無線 / モバイルセキュリティ

無線 / モバイルセキュリティ分野は過去の予測では意外に低い成長率であったが、今後の成長率は情報セキュリティソフトウェア市場の中では最も高いと予測される。市場規模は 2004 年の 2 億円から 2009 年には 7.2 億円に拡大する見込みである。

図 28 韓国無線/モバイルセキュリティ市場予測 (百万円)



< 100 ウォン=97.1 円で円換算 >

● 韓国情報セキュリティサービス市場

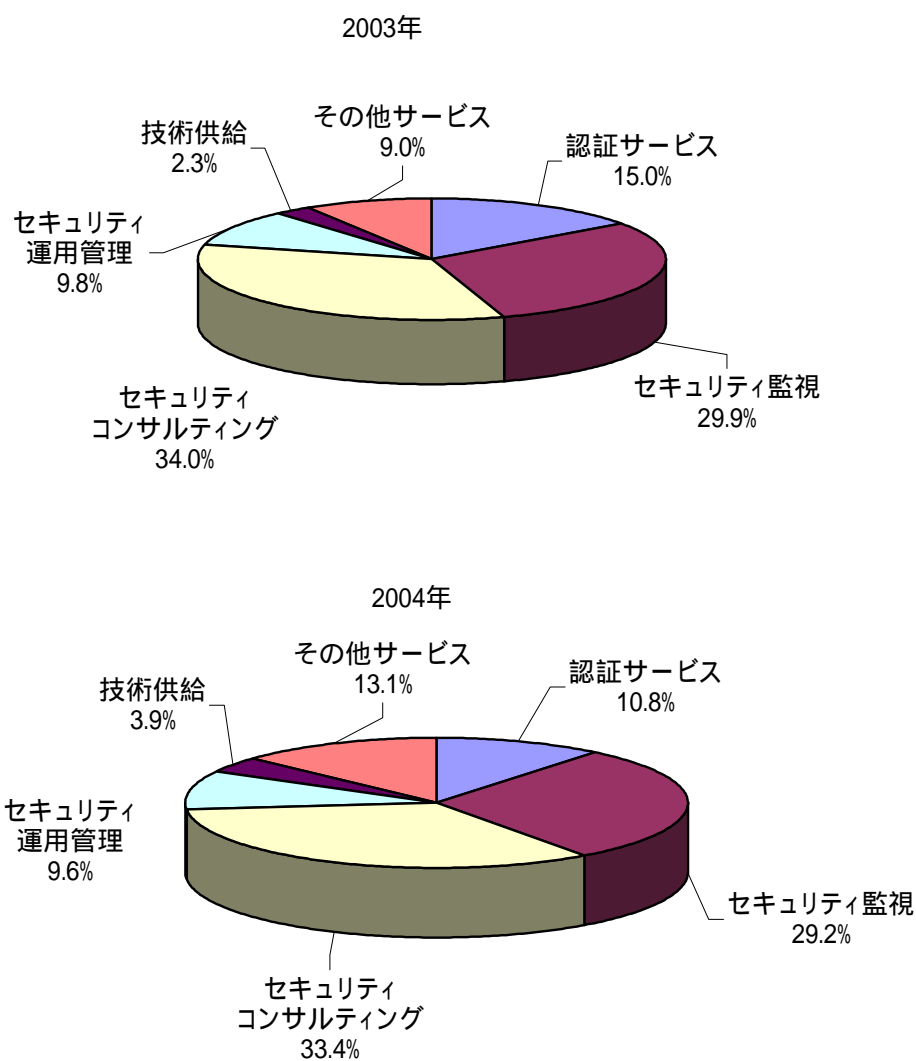
表 38 に示すように、2004 年の韓国情報セキュリティサービスの市場規模は 85 億円と予測され、これは 2003 年の市場規模 76 億円と比較すると 12.1%の成長率である。市場規模の大きい分野はセキュリティコンサルティング及びセキュリティ監視分野で、その規模はそれぞれ 28 億円、25 億円である。前年比で大幅に成長した分野は技術供給及びその他サービス分野で対前年比成長率がそれぞれ 94.1%と 62.5%を示している。特に、教育訓練サービス分野及びレンタルサービス分野を含んでいるその他サービス分野の急成長を注視すべきである。

表 38 韓国情報セキュリティサービス市場規模実績 (百万円)

	2003 年	2004 年	成長率 (%)
認証サービス	1,138	918	-19.4%
セキュリティ監視	2,267	2,481	9.5%
セキュリティコンサルティング	2,571	2,838	10.4%
セキュリティ運用管理	740	811	9.7%
技術供給	171	331	94.1%
その他サービス	683	1,110	62.5%
合計	7,570	8,490	12.1%

< 100 ウォン=97.1 円で円換算 >

図 29 韓国情報セキュリティサービス構成



情報セキュリティサービスの2004年～2009年の市場予測が表39である。情報セキュリティサービス市場規模は2004年の85億円から2009年には192億円に拡大する見込みであり、2004年～2009年の年平均成長率は17.7%と予測されている。2009年で最も大きい市場規模の分野はセキュリティ監視とセキュリティコンサルティングで、それぞれ69億円及び63億円である。また2004年～2009年の年平均成長率(CAGR)は技術供給、セキュリティ監視、セキュリティコンサルティング分野が平均を若干上回ると予測されている。

表 39 韓国情報セキュリティサービス市場予測（百万円）

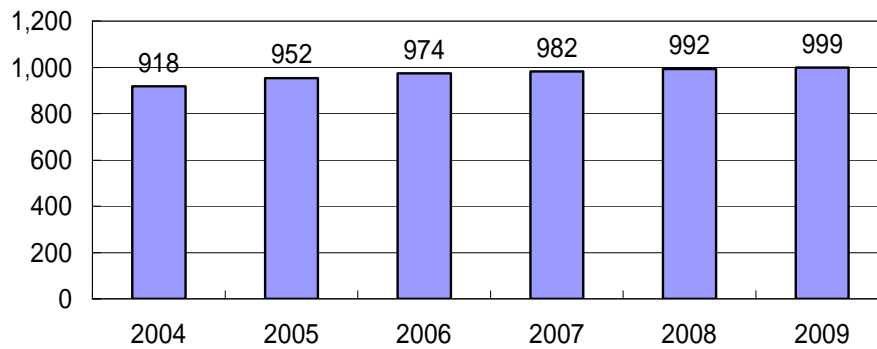
	2004年	2005年	2006年	2007年	2008年	2009年	CAGR (%)
認証サービス	918	952	974	982	992	999	1.7%
セキュリティ監視	2,481	3,376	4,601	5,551	6,339	6,931	22.8%
セキュリティコンサルティング	2,838	3,555	4,308	5,046	5,723	6,307	17.3%
セキュリティ運用管理	811	1,033	1,231	1,387	1,499	1,573	14.2%
技術供給	331	481	678	922	1,202	1,495	35.1%
その他サービス	1,110	1,240	1,384	1,543	1,717	1,909	11.5%
合計	8,490	10,638	13,176	15,430	17,471	19,213	17.7%

CAGR は、市場規模の 2004 年～2009 年の年平均成長率。

< 100 ウォン=97.1 円で円換算 >

韓国認証サービス市場

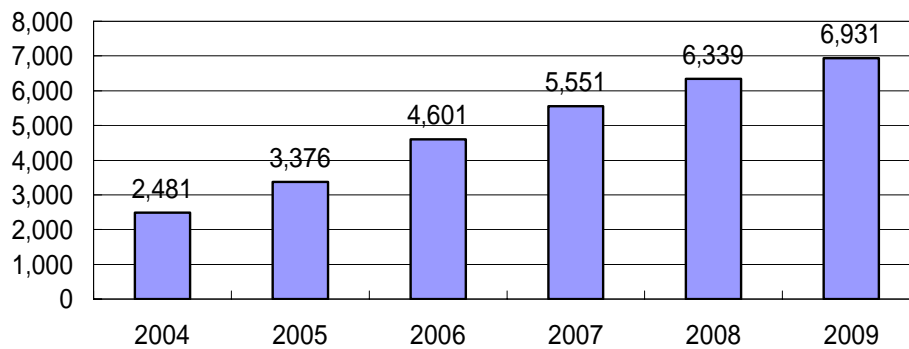
図 30 韓国認証サービス市場予測（百万円）



< 100 ウォン=97.1 円で円換算 >

韓国セキュリティ監視サービス市場

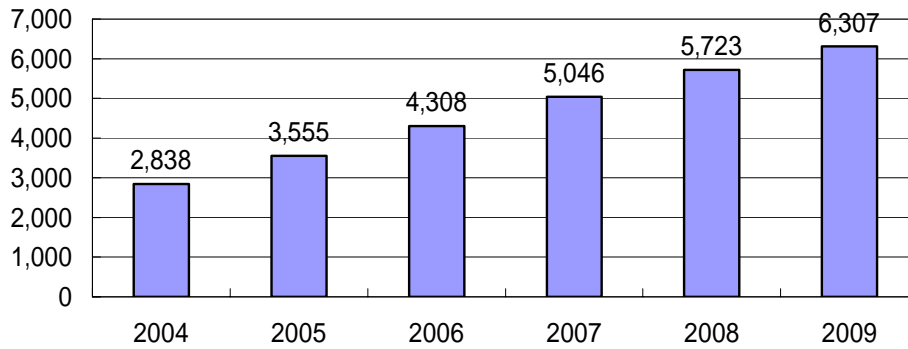
図 31 韓国セキュリティ監視サービス市場予測（百万円）



< 100 ウォン=97.1 円で円換算 >

韓国セキュリティコンサルティング市場

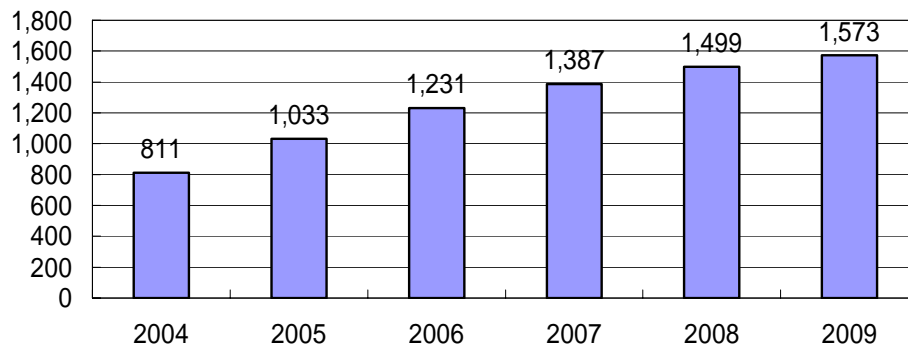
図 32 韓国セキュリティコンサルティング市場予測（百万円）



< 100 ウォン=97.1 円で円換算 >

韓国セキュリティ運用管理サービス市場

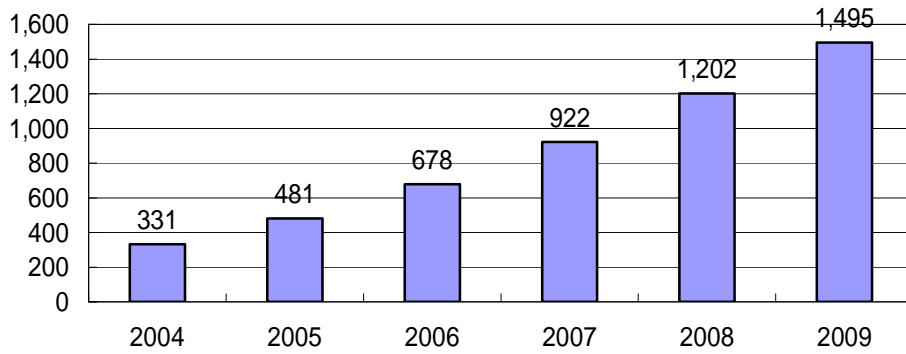
図 33 韓国セキュリティ運用管理サービス市場予測（百万円）



< 100 ウォン=97.1 円で円換算 >

韓国技術供給サービス市場

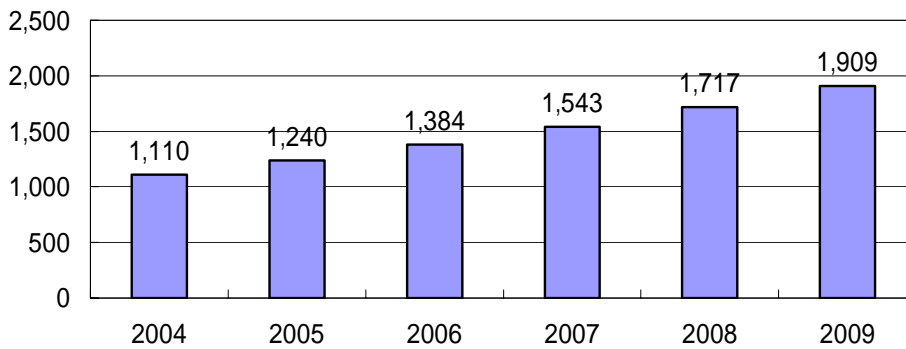
図 34 韓国技術供給サービス市場予測（百万円）



< 100 ウォン=97.1 円で円換算 >

韓国その他セキュリティサービス市場

図 35 韓国その他セキュリティサービス市場予測（百万円）



< 100 ウォン=97.1 円で円換算 >

以上

## 【付録 2】英文字略語に関する簡単な説明

3A	Authentication, Authorization, Administration	Authentication ( 認証 )、Authorization ( 認可 )、Administration ( 管理 )。情報セキュリティにおける 3 大要素。
ACL	Access Control List	ネットワーク利用者のアクセス権限と、アクセス可能なシステム・ファイルなどのリスト。
ASP	Application Service Provider	一般に「ソフトの時間貸し」と呼ばれ、アプリケーションを販売することなく、インターネット上で利用させ、利用料に応じて課金するビジネスモデル、またはその事業者。
ATM	Automatic Teller Machine	現金自動預け払い機。
DRM	Digital Rights Management	デジタル著作権管理。デジタルデータの著作権を保護する技術。複製の制限や、画像への電子透かしなどがこれにあたる。ビジネス上の文書に関しては、その閲覧、編集、複写、印刷等の操作を制限する等の管理を意味する場合がある。
e-Learning	e-Learning	パーソナルコンピュータやネットワークを利用した教育、遠隔地での教育や学習者の進度に合せた教育が提供できるという利点がある。
IDS	Intrusion Detection System	ネットワーク上を流れるパケットを分析し、不正アクセスと思われるパケットを検出して、管理者に通知するシステム。
FW	Firewall	組織内のネットワークが外部から侵入されることを防ぐシステムあるいは機器、ネットワークの界面に置かれ、特定のプロトコルだけを通過させることで制御を行う。
GW	Gateway	ネットワークのセグメント間を接続する機器。
IA	Intel Architecture	米半導体ベンダー Intel 社のマイクロプロセッサのアーキテクチャに互換性のあるマイクロプロセッサ。
ID	IDentification	ユーザや各種リソースを一意に特定する論理要素、コンピュータシステムにおける認証の対象となる。
IP	Internet Protocol	ARPANET で開発されたプロトコルで、OSI 参照モデルの第 3 層 ( ネットワーク層 ) に位置する。
IPA	Information-technology Promotion Agency	独立行政法人情報処理推進機構。ソフトウェア及び情報処理システムの安全で健全な発展を技術、人材の面から支えることを目的とする経済産業省所管の独立行政法人。
IPS	Intrusion Prevention System	サーバやネットワークへの不正侵入を阻止するシステム。IDS の機能を拡張し、侵入を検知するとリアルタイムで防御を実行する。
ISMS	Information Security Management System	組織レベルのセキュリティを確保するために、リスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用すること。セキュリティポリシーに基づき、PDCA サイクルを継続的に繰り返すことができる組織能力。こうし

		た能力を備えた組織を認定するため、財団法人日本情報処理開発協会（JIPDEC）が認定機関となり「ISMS 適合性評価制度」が実施されている。現在の ISMS 認証基準 ver2.0 では、英国の情報セキュリティ認証規格「BS7799-2：2002」と、国内規格「JIS X 5080：2002（ISO/IEC 17799：2000）」との互換性を確保している。
IT	Information Technology	情報通信技術。
OEM	Original Equipment Manufacturing	委託先のブランドで製品を製造・供給すること。
PC	Personal Computer	個人で占有利用する低価格の小型コンピュータ、狭義には Intel 互換 CPU を持ち、Windows を OS として採用するものを指す。
PIN	Personal Identification Number	IC カードやワンタイムパスワードに使用する時に用いる個人用識別番号。「暗証番号」とほぼ同義。
PKI	Public Key Infrastructure	公開鍵暗号による電子認証基盤技術。
SOC	Security Operation Center	遠隔地でのセキュリティ運用監視サービスにおけるオペレーションセンター。
SI	Systems Integration	ユーザの業務に合せた情報システムを設計、構築すること。
TCP	Transmission Control Protocol	インターネットで利用される標準プロトコルで、OSI 参照モデルのトランスポート層にあたる。ネットワーク層の IP と、セッション層よりも上位のプロトコル（HTTP、FTP、SMTP、POP など）の橋渡しをする。
UDP	User Datagram Protocol	インターネットで利用される標準プロトコルで、OSI7 階層参照モデルのトランスポート層にあたる。ネットワーク層の IP と、セッション層よりも上位のプロトコルの橋渡しをする。TCP よりも信頼性には劣るが、転送速度が速い。
URL	Unique Resource Locator	インターネット上の文書、画像などの資源を一意に特定するための記述方法。
USB	Universal Serial Bus	パーソナルコンピュータと周辺機器を接続するための接続装置及び通信規格。
VPN	Virtual Private Network	通信事業者の提供する広域 IP 通信網上に構築された仮想私設通信網。通信相手と仮想的なトンネルをつくることで、プライベートアドレスによる通信や、TCP/IP 以外のプロトコルによる通信も可能となる。また、データを暗号化することで、通信の秘匿性を確保する。

以上

**著作**

経済産業省情報政策局セキュリティ政策室

〒100-8901

東京都千代田区霞ヶ関 1-3-1

URL: <http://www.meti.go.jp/policy/netsecurity/index.html>

e-mail: [it-security@meti.go.jp](mailto:it-security@meti.go.jp)

**制作**

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

〒136-0075

東京都江東区新砂 1-6-35 T.T.ランディック東陽町ビル

TEL:03-5633-6061 FAX:03-5633-6062

URL: <http://www.jnsa.org/>

e-mail: [sec@jnsa.org](mailto:sec@jnsa.org)

この報告書は再生紙を使用しております。