# 2010-2011 年度

# 情報セキュリティ市場調査報告書

# V1.0

２０１２年１月

NPO 日本ネットワークセキュリティ協会

# 目次

**はじめに** ..... 1
**【第一部　情報セキュリティ市場調査結果】** ..... 3
**第１章　　国内情報セキュリティ市場の実態概要** ..... 3
**第２章　　国内情報セキュリティ市場調査結果の詳細とその分析** ..... 6
2.1.　国内情報セキュリティツール市場の分析 ..... 6
2.1.1.　情報セキュリティツール市場の全体概要 ..... 6
2.1.2.　情報セキュリティツール市場のカテゴリ別分析 ..... 9
2.1.2.1.　統合型アプライアンス市場 ..... 9
2.1.2.2.　ネットワーク脅威対策製品市場 ..... 11
2.1.2.3.　コンテンツセキュリティ対策製品市場 ..... 15
2.1.2.4.　アイデンティティ・アクセス管理製品市場 ..... 18
2.1.2.5.　システムセキュリティ管理製品市場 ..... 21
2.1.2.6.　暗号製品市場 ..... 24
2.2.　国内情報セキュリティサービス市場の分析 ..... 26
2.2.1.　情報セキュリティサービス市場の全体概要 ..... 26
2.2.2.　情報セキュリティサービス市場のカテゴリ別分析 ..... 29
2.2.2.1.　情報セキュリティコンサルテーション市場 ..... 29
2.2.2.2.　セキュアシステム構築サービス市場 ..... 33
2.2.2.3.　セキュリティ運用・管理サービス市場 ..... 36
2.2.2.4.　情報セキュリティ教育市場 ..... 40
2.2.2.5.　情報セキュリティ保険市場 ..... 43
**第３章　　情報セキュリティにおける新しい課題と動き** ..... 45
3.1.　2009～10 年におけるネットワークの脅威の動向 ..... 45
3.2.　ソーシャル・ネットワーキングサービスの普及とセキュリティ課題 ..... 46
3.3.　スマートフォンのセキュリティ ..... 48
3.4.　震災を経て変わるクラウドコンピューティングのセキュリティ課題評価 ..... 50
**第４章　　2012 年の展望** ..... 53
**【第二部　情報セキュリティ市場調査の事業概要と結果に関する考察結果】** ..... 57
**第５章　　調査の概要** ..... 57
5.1.　調査対象 ..... 57
5.2.　調査方法 ..... 57
5.3.　データポイントの定義 ..... 58
5.4.　市場規模の予測値の算定方法 ..... 59
**第６章　　情報セキュリティ市場の分類および定義** ..... 60
6.1.　情報セキュリティツール･サービスの市場分類定義表 ..... 60

6.2. 情報セキュリティツール市場の定義に関する説明 ..... 66
6.3. 情報セキュリティサービス市場の定義に関する説明 ..... 79
**第７章 情報セキュリティ市場参入事業者の業態と産業構造** ..... 88
7.1. 情報セキュリティ市場参入事業者の業態区分 ..... 88
7.2. 業態区分と市場区分における分布 ..... 91
7.3. 情報セキュリティ産業の産業構造 ..... 91
**第８章 情報セキュリティ市場および産業の状況と、変化をもたらす要因** ..... 95
8.1. マクロ経済動向と企業経営環境 ..... 95
8.2. 企業・組織の IT 支出ビヘイビア ..... 97
8.3. 情報セキュリティに関わる外部環境変化 ..... 102
8.4. 産業としての課題 ..... 106
**おわりに** ..... 108

# 表目次

表 1　国内情報セキュリティ市場規模　実績と予測.....3
表 2　国内情報セキュリティツール市場規模　実績と予測.....6
表 3　国内統合型アプライアンス市場規模　実績と予測.....10
表 4　国内ネットワーク脅威対策製品市場規模　実績と予測.....13
表 5　国内コンテンツセキュリティ対策製品市場規模　実績と予測.....16
表 6　国内アイデンティティ・アクセス管理製品市場規模　実績と予測.....20
表 7　国内システムセキュリティ管理製品市場規模　実績と予測.....23
表 8　国内暗号製品市場規模　実績と予測.....24
表 9　国内情報セキュリティサービス市場規模　実績と予測.....26
表 10　国内情報セキュリティコンサルテーション市場規模　実績と予測.....31
表 11　国内セキュアシステム構築サービス市場規模　実績と予測.....34
表 12　国内セキュリティ運用・管理サービス市場規模　実績と予測.....37
表 13　国内情報セキュリティ教育市場規模　実績と予測.....42
表 14　国内情報セキュリティ保険市場規模　実績と予測.....44
表 15　2012 年度　国内情報セキュリティ市場規模予測.....55
表 16　用語説明.....60
表 17　情報セキュリティツールの市場分類.....61
表 18　情報セキュリティサービスの市場分類.....64
表 19　国内情報セキュリティ市場推計対象企業およびその分布.....91
表 20　GDP 実質成長率の推移.....95
表 21　平成 23 年版 情報通信白書　情報流通量の推移.....98
表 22　IT 市場、通信市場と情報セキュリティ市場規模の比較.....99
表 23　情報処理実態調査母集団の比較（平成 19 年度、20 年度、21 年度調査）.....101
表 24　2010 年の個人情報漏えいインシデント　概要データ.....105

# 図目次


図 1　国内情報セキュリティ市場規模の推移 ..... 4
図 2　2009 年度の国内情報セキュリティツール市場 ..... 7
図 3　国内情報セキュリティツール市場推移 ..... 8
図 4　国内統合型アプライアンス市場推移 ..... 11
図 5　2009 年度のネットワーク脅威対策製品市場 ..... 12
図 6　ネットワーク脅威対策製品市場推移 ..... 14
図 7　2009 年度のコンテンツセキュリティ対策製品市場 ..... 16
図 8　国内コンテンツセキュリティ対策製品市場推移 ..... 18
図 9　2009 年度のアイデンティティ・アクセス管理製品市場 ..... 19
図 10　国内アイデンティティ・アクセス管理製品市場推移 ..... 21
図 11　2009 年度のシステムセキュリティ管理製品市場 ..... 22
図 12　システムセキュリティ管理製品市場推移 ..... 24
図 13　国内暗号製品市場推移 ..... 25
図 14　2009 年度の国内情報セキュリティサービス市場 ..... 27
図 15　国内情報セキュリティサービス市場推移 ..... 29
図 16　2009 年度の情報セキュリティコンサルテーション市場 ..... 30
図 17　国内情報セキュリティコンサルテーション市場推移 ..... 32
図 18　2009 年度のセキュアシステム構築サービス市場 ..... 33
図 19　国内セキュアシステム構築サービス市場推移 ..... 35
図 20　2009 年度のセキュリティ運用･管理サービス市場 ..... 36
図 21　国内セキュリティ運用・管理サービス市場推移 ..... 39
図 22　2009 年度の情報セキュリティ教育サービス市場 ..... 40
図 23　国内情報セキュリティ教育市場推移 ..... 43
図 24　国内情報セキュリティ保険市場推移 ..... 44
図 25　スマートフォンの脅威についての技術的分類 ..... 49
図 26　日本の情報セキュリティ産業の機能構造－製品・ツール ..... 92
図 27　日本の情報セキュリティ産業の機能構造－サービス ..... 93
図 28　日本の情報セキュリティ産業の役割構造 ..... 93
図 29　四半期別経済成長率推移 ..... 96
図 30　企業の生産・出荷・在庫の推移 ..... 97



## はじめに

2011 年 3 月 11 日､そして続く数日の間に､日本は未曾有の経験をすることとなってしまった。その後、世界の賞賛の的となった忍耐と秩序の下、日本の「現場力」を基盤とする企業の力は急速な経済の回復振りを示したが、なお被災地を中心に市場の復旧と需要の回復は途上にある。被災された方々に心よりお見舞い申し上げ、一日も早い復旧・復興と、震災の経験や結果を踏まえての社会経済の新生を祈りたいと思う。

当ワーキンググループの今回の市場調査活動は、2009 年度まで 7 年間 6 次にわたり継続した経済産業省委託事業としてでなく、JNSA 独自の事業として、2010 年秋から開始した。

基礎となるアンケート調査と個別推計作業は東日本大震災以前に実施され、市場規模の推計作業の大枠は 2011 年 5 月時点で固めた。その後、ワーキンググループメンバによる分析と執筆作業を重ね、このたび 2 年越しで報告書としてまとめることができた。更に 2011 年 12 月時点での 2012 年度への展望についても JNSA 会員に簡易アンケートを行うことで予測を試み、その結果を第 4 章に略述した。ここに届けるのは、従来の枠組みにとらわれずに情報セキュリティ産業の今の姿に迫る試みを続ける、情報セキュリティ市場ワーキンググループの現状認識であり問題意識である。

ソーシャルネットワークの枠組みは、震災に際して、主として家族・友人・知人並びに職場の仲間の間で安否情報を確認する目的では、電話網以上に役立った。ネット上の無償メールやグループウェアを始めとするネットツールと、クラウドサービスプロバイダが提供する無償の IT 機能は、被災者への救援・支援活動のボランティアのための情報ツールとして、また緊急事態における行政対応のための情報インフラとして、大きな力を発揮した。今回津波によって大きな被害を受けた自治体の中で､住民登録台帳や社会保険加入管理の記録を紙媒体に頼っていたところは、システムの回復に大きな困難を生じている。一方で IT 化を実現し、住基ネットとの接続も実施していた自治体は、手元のサーバとストレージのすべてが津波の被害に遭いながら、比較的短期にシステムの復旧にこぎつけている。

このたびの災害は、IT が果たす役割や、その機能、効用、意味を浮き彫りにした面がある。IT は最早、全ての組織の管理と運営にとって、必要不可欠の機能要素となっていると言える。

その IT を安心して、快適に、合目的的かつ効率的に使いこなすすべは、しかし、十分に定着したとは言い切れない｡「快適に」は誰しもが期待するところであり工夫の仕方も多彩となりうるので、絶えず進歩している。「合目的的に」は IT とその利用環境の企画・管理者が意図する以上の機能を IT とインターネットが提供可能なことから､コントロールが極めて困難となっている。利用者は、業務以外のソフトウェアを簡単にインストールして個人の趣味や興味のために利用できるし､業務に関係のないネット経由のコミュニケーションや Web 閲覧が可能である。それらの

行為はしかし、残念ながら単に業務効率を下げる懸念だけでなく、ウイルスその他のマルウェアを呼び込む大きな危険をはらんでいる。組織外の第三者（典型的にはハッカーと呼ばれる人たち）がネットを通じて、管理者の意図を裏切って情報を盗み取ったり破壊工作をする事件も後を絶たない。

このように、IT は「利便性の提供」と同時に、危険の導入、リスクへの曝露という負の効果ももたらす。そのようなマイナス面をコントロールすることで、IT の真の利便・効用を十分に生かすことができるようになる。IT のセキュリティ、情報セキュリティ※はそのための対策であり規範である。

情報セキュリティは、まず第一に、インターネットからの攻撃の脅威、情報通信インフラを悪用した詐欺等の犯罪、情報の流失・紛失やそれに伴う被害等、社会の安全安心を脅かす存在への防御が確立されなければならない。そして更に、企業経営のデータや営業秘密、知的財産等の情報資源を保護・活用し、企業の内部統制を充実して経営の質と透明性の維持向上を図り、付加価値と競争力を向上させるために確保されなければならない。IT を外部からの侵入や攻撃から守り、脆弱性に付け入られることを防ぎ、意図せざる利用や悪用に対して防衛するために手立てを尽くすことは、IT を正しく、合目的的に利活用することと表裏一体の行為である。

特定非営利活動法人（NPO）日本ネットワークセキュリティ協会（JNSA）では、2004 年度以来、情報セキュリティ市場実態調査を実施してきた。本書はその努力を継承し、調査の継続性を維持しつつ、今日情報セキュリティ産業が直面している変化にも向き合うものとして再編成した。情報セキュリティのためのツールやサービスを提供する側にも、それらを活用して情報セキュリティを実現し維持管理する主体にも、そして日本の情報セキュリティに対して責任を負う行政主体にも、その他関係各方面においても、本書が有意義に活用されることを期待する次第である。

※本報告書では、「セキュリティ」という用語を、原則として、情報一般に関わる場合は「情報セキュリティ」、情報システムに固有の場合は「IT セキュリティ」、両者にまたがる場合や文脈から対象が明確な場合は単に「セキュリティ」と表記している。

# 【第一部　情報セキュリティ市場調査結果】

## 第１章 国内情報セキュリティ市場の実態概要

表１に国内情報セキュリティ市場の推計結果を示す。図１には情報セキュリティツール、情報セキュリティサービスの区分による市場推移のグラフを示した。

**表 1　国内情報セキュリティ市場規模　実績と予測**

（金額:百万円、成長率:対前年比増加率）

| 国内情報セキュリティ市場推計 | 2008年度（推定実績） | | 2009年度（推定実績） | | | 2010年度（実績見込） | | | 2011年度（予測） | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 金額 | 構成比 | 金額 | 構成比 | 成長率 | 金額 | 構成比 | 成長率 | 金額 | 構成比 | 成長率 |
| **情報セキュリティ市場合計** | **719,250** | **100.0%** | **682,061** | **100.0%** | **-5.2%** | **664,199** | **100.0%** | **-2.6%** | **648,326** | **100.0%** | **-2.4%** |
| **情報セキュリティツール合計** | **371,663** | **100.0%** | **357,097** | **100.0%** | **-3.9%** | **354,216** | **100.0%** | **-0.8%** | **356,762** | **100.0%** | **0.7%** |
| 統合型アプライアンス | 20,880 | 5.6% | 19,243 | 5.4% | -7.8% | 18,963 | 5.4% | -1.5% | 18,703 | 5.2% | -1.4% |
| ネットワーク脅威対策製品 | 56,003 | 15.1% | 50,022 | 14.0% | -10.7% | 48,515 | 13.7% | -3.0% | 48,508 | 13.6% | 0.0% |
| コンテンツセキュリティ対策製品 | 139,978 | 37.7% | 137,622 | 38.5% | -1.7% | 136,534 | 38.5% | -0.8% | 137,250 | 38.5% | 0.5% |
| アイデンティティ・アクセス管理製品 | 65,225 | 17.5% | 64,269 | 18.0% | -1.5% | 63,392 | 17.9% | -1.4% | 64,191 | 18.0% | 1.3% |
| システムセキュリティ管理製品 | 51,723 | 13.9% | 48,589 | 13.6% | -6.1% | 49,505 | 14.0% | 1.9% | 49,771 | 14.0% | 0.5% |
| 暗号製品 | 37,853 | 10.2% | 37,351 | 10.5% | -1.3% | 37,307 | 10.5% | -0.1% | 38,339 | 10.7% | 2.8% |
| **情報セキュリティサービス合計** | **347,587** | **100.0%** | **324,964** | **100.0%** | **-6.5%** | **309,983** | **100.0%** | **-4.6%** | **291,563** | **100.0%** | **-5.9%** |
| 情報セキュリティコンサルテーション | 76,207 | 21.9% | 72,166 | 22.2% | -5.3% | 66,256 | 21.4% | -8.2% | 60,545 | 20.8% | -8.6% |
| セキュアシステム構築サービス | 147,679 | 42.5% | 130,424 | 40.1% | -11.7% | 122,206 | 39.4% | -6.3% | 108,559 | 37.2% | -11.2% |
| セキュリティ運用・管理サービス | 91,129 | 26.2% | 90,113 | 27.7% | -1.1% | 90,389 | 29.2% | 0.3% | 91,375 | 31.3% | 1.1% |
| 情報セキュリティ教育 | 24,981 | 7.2% | 24,884 | 7.7% | -0.4% | 23,900 | 7.7% | -4.0% | 23,841 | 8.2% | -0.2% |
| 情報セキュリティ保険 | 7,591 | 2.2% | 7,377 | 2.3% | -2.8% | 7,234 | 2.3% | -1.9% | 7,244 | 2.5% | 0.1% |

2008 年度の国内情報セキュリティ市場規模の推定実績値は、「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 3,717 億円、「情報セキュリティサービス」が 3,476 億円、合計で 7,193 億円であったと推定される。

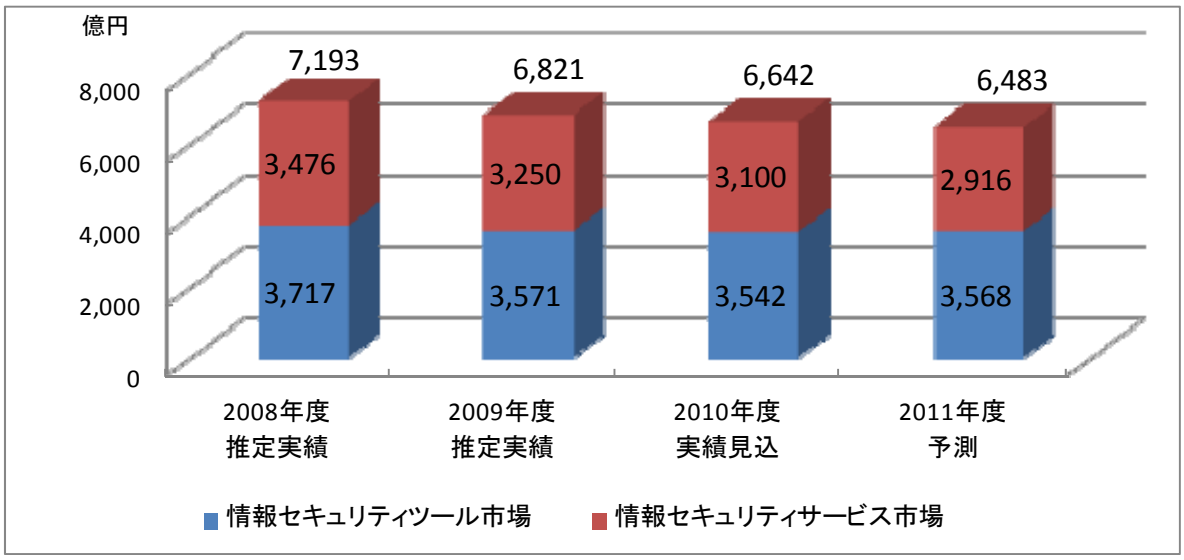
今回調査の基準年度とした 2009 年度は、2008 年度半ばに世界経済を襲ったいわゆるリーマンショックとそれに伴う世界同時不況の影響により、年度全体としては停滞感の強い年となった。2008 年度は、前半が 2007 年度から続く好況と IT 投資サイクルの山の余波により、かなり強い拡大ペースが見られたのに加え、後半の急ブレーキによる混乱の中でも、2009 年度の不透明さに備えるために年度予算の範囲で情報セキュリティ支出の手当をしておく動きもあり、年度全体でプラス基調が維持された。しかし、2009 年度は新興経済圏が比較的早い立ち直りを見せる中、先

進国経済はバランスシート調整という中期課題を抱えていたため、その回復スピードは上らなかった。このため、国内経済においても新規投資は見送られ、維持更新についても絞り込みの動きが見られた。

このことを反映して、国内情報セキュリティ市場も、本調査開始以来初めて、マイナス成長を観測することとなった。2009 年度の市場規模の推定実績値は、「情報セキュリティツール」が 3,571 億円（対前年度比成長率マイナス 3.9%）、「情報セキュリティサービス」が 3,250 億円（同マイナス 6.5%）で、合計 6,821 億円（同マイナス 5.2%）となった。2008 年度にはじめて 7,000 億円の大台を超えたものと推測された国内情報セキュリティ市場は、再び 6000 億円台に戻ったと考えられる。

**図 1　国内情報セキュリティ市場規模の推移**




2010 年度は、年度当初の一時的停滞感、第二四半期において外需にも支えられて回復基調が見られたものの、個人消費の盛り上がりがなく、また秋には円高も進んだことから、全体としては盛り上がりにかける中、2011 年度にかけて新興国経済の堅調を背景に回復テンポが上ることが期待される中で東日本大震災を迎えた、という経緯だったと総括できる。この中で IT 投資は低迷が続いた模様である。2008 年度までにある程度手当されていたサイクルの谷という要因も影響しているのではないかと推測される。

その結果、実績見込みベースの数字であるが、「情報セキュリティツール」は 3,542 億円（対前年度比成長率マイナス 0.8%）とほぼ横ばいとなり、「情報セキュリティサービス」は 3,100 億円（同マイナス 4.6%）とやや大きな落込みで、合計 6,642 億円（同マイナス 2.6%）となった。

なお、情報セキュリティサービスの落込みが大きくなっているのは、単に経済要因だけでなく、「セキュアシステム構築サービス」が一般のシステムインテグレーションの一部にシフトすることによる統計上の数字の縮小と、ISMS 等の規格適合性認証の一巡に伴う関連のサービスの急速な縮小という要因が大きく影響している。

2011 年度については、景気回復が期待されていた矢先の東日本大震災と、それに続く福島第一原発の事故、復興対策の大幅な遅れと有効な手を打てない政治の無力等により、経済の先行きは全く見えなくなっている。製造業が自らの見通しをも大幅に短縮するサプライチェーンの復旧と生産の回復を見せているが、先進国経済は政府債務問題が欧州だけでなくアメリカでも大問題となり、手詰まり感が強まっている。

2011 年度の市場規模の推計値は、2011 年 2 月段階で一旦出していたが、その後 5 月に若干の見直し作業を行っている。ただし、上記の経済不安要素をすべて反映できているわけではない。結論としては、「情報セキュリティツール」は 3,568 億円（対前年度比成長率プラス 0.7%）とわずかながら拡大すると見られ、「情報セキュリティサービス」は引き続き同マイナス 5.9%と大幅な落込みを見せて 2,916 億円と 3,000 億円を割り込むものと予測した。市場合計値は 6,483 億円（同マイナス 2.2%）と縮小が続くことになる。

なお、このうち情報セキュリティサービスの大幅な落込みは 2010 年度と全く同じ理由によるものであり、セキュリティ運用・管理サービスはプラス 1.1%と、わずかながらプラスになる等、基調として極めて悲観的な状況にあるとは考えていない。

# 第２章 国内情報セキュリティ市場調査結果の詳細とその分析

## 2.1. 国内情報セキュリティツール市場の分析

### 2.1.1. 情報セキュリティツール市場の全体概要

表 2 に、国内情報セキュリティツール市場規模データを示す。ここに見るように、2009 年度の国内「情報セキュリティツール」市場は、3,571 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」、「ネットワーク脅威対策製品」、「コンテンツセキュリティ対策製品」、「アイデンティティ・アクセス管理製品」、「システムセキュリティ管理製品」、「暗号製品」の 6 カテゴリに分けた。各カテゴリの定義・内容は第 6 章に詳述した通りである。

**表 2 国内情報セキュリティツール市場規模 実績と予測**

金額単位：百万円

| 年度別売上高推計値 | 2008年度 | | 2009年度 | | | 2010年度 | | | 2011年度 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| セキュリティ・ツール | 売上実績推定値 | | 売上実績推定値 | | | 売上高見込推定値 | | | 売上高予測値 | | |
| | 金額 | 構成比 | 金額 | 構成比 | 成長率 | 金額 | 構成比 | 成長率 | 金額 | 構成比 | 成長率 |
| 統合型アプライアンス | 20,880 | 5.6% | 19,243 | 5.4% | −7.8% | 18,963 | 5.4% | −1.5% | 18,703 | 5.2% | −1.4% |
| ネットワーク脅威対策製品 | 56,003 | 15.1% | 50,022 | 14.0% | −10.7% | 48,515 | 13.7% | −3.0% | 48,508 | 13.6% | 0.0% |
| コンテンツセキュリティ対策製品 | 139,978 | 37.7% | 137,622 | 38.5% | −1.7% | 136,534 | 38.5% | −0.8% | 137,250 | 38.5% | 0.5% |
| アイデンティティ・アクセス管理製品 | 65,225 | 17.5% | 64,269 | 18.0% | −1.5% | 63,392 | 17.9% | −1.4% | 64,191 | 18.0% | 1.3% |
| システムセキュリティ管理製品 | 51,723 | 13.9% | 48,589 | 13.6% | −6.1% | 49,505 | 14.0% | 1.9% | 49,771 | 14.0% | 0.5% |
| 暗号製品 | 37,853 | 10.2% | 37,351 | 10.5% | −1.3% | 37,307 | 10.5% | −0.1% | 38,339 | 10.7% | 2.8% |
| セキュリティツール市場合計 | 371,663 | 100.0% | 357,097 | 100.0% | −3.9% | 354,216 | 100.0% | −0.8% | 356,762 | 100.0% | 0.7% |

図 2 に 2009 年度の国内情報セキュリティツール市場のカテゴリ別分布を示す。

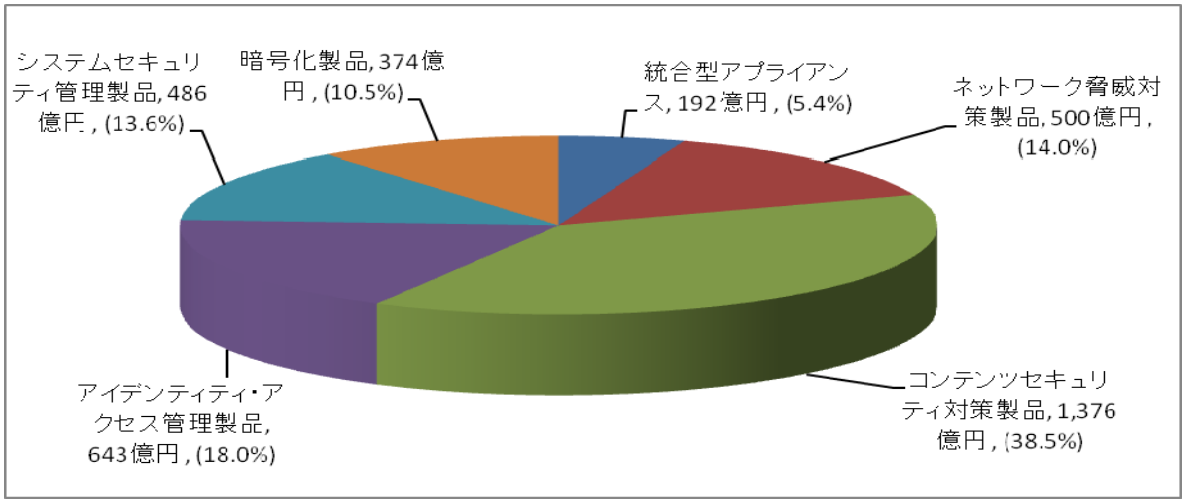
情報セキュリティツール市場において最大のカテゴリは「コンテンツセキュリティ対策製品」で、2009 年度には 1,376 億円、構成比にして全体の 38.5%を占めた。これに続くのが「アイデンティティ・アクセス管理製品」の 643 億円で構成比 18.0%を占め、次には「ネットワーク脅威対策製品」の 500 億円・構成比 14.0%が続く。これら 3 カテゴリで「情報セキュリティツール」市場全体の 71%を占める。これらのカテゴリにはウイルス対策製品、ファイアウォール、個人認証製品が含まれている。これら 3 製品カテゴリは、JNSA が 2005 年 2 月に発表した「IT セキュリティ対策施策の導入・実施状況とその満足度調査」報告書[1]によれば、ユーザ側調査において、既に 2004 年段階で 90%以上の導入率が確認されているほど普及の進んだ領域であり、ベンダ側の数字でもそれが裏付けられる結果となった。

2009 年度の国内「情報セキュリティツール」市場は、全体としては前年度比成長率マイナス 3.9%と、本調査開始以来初めてマイナス成長を記録した年となった。原因は 2008 年 9 月に発生したいわゆるリーマンショックに端を発する世界的信用不安に伴う経済の急速な冷え込みにある。過去、マクロ経済がマイナス成長でも情報セキュリティ市場がプラス成長を維持してきたのは、情報セキュリティ対策の普及度が十分高くなく、その充実の速度が経済停滞度合いを上回っていたからと考えられる。しかし、2008 年度においてはその前年から情報セキュリティ投資が高まり

[1] http://www.jnsa.org/active/2004/active2004_15a.html

普及度が上ってきていたことに加え、経済の落込みが極めて急だったことで、マイナス成長という結果になったものと考えられる。

**図 2　2009 年度の国内情報セキュリティツール市場**




マイナス幅が特に大きいのは「ネットワーク脅威対策製品」市場でマイナス 10.7%と大幅となった。これは、2007, 2008 年度の成長、あるいは更新投資サイクル一巡の反動の要素が加わったことが大きいと考えられる。これに次ぐ「統合型アプライアンス」マイナス 7.8%も全く同じ理由であり、更に「システムセキュリティ管理製品」の落込みも類似の要因によるものと推測される。

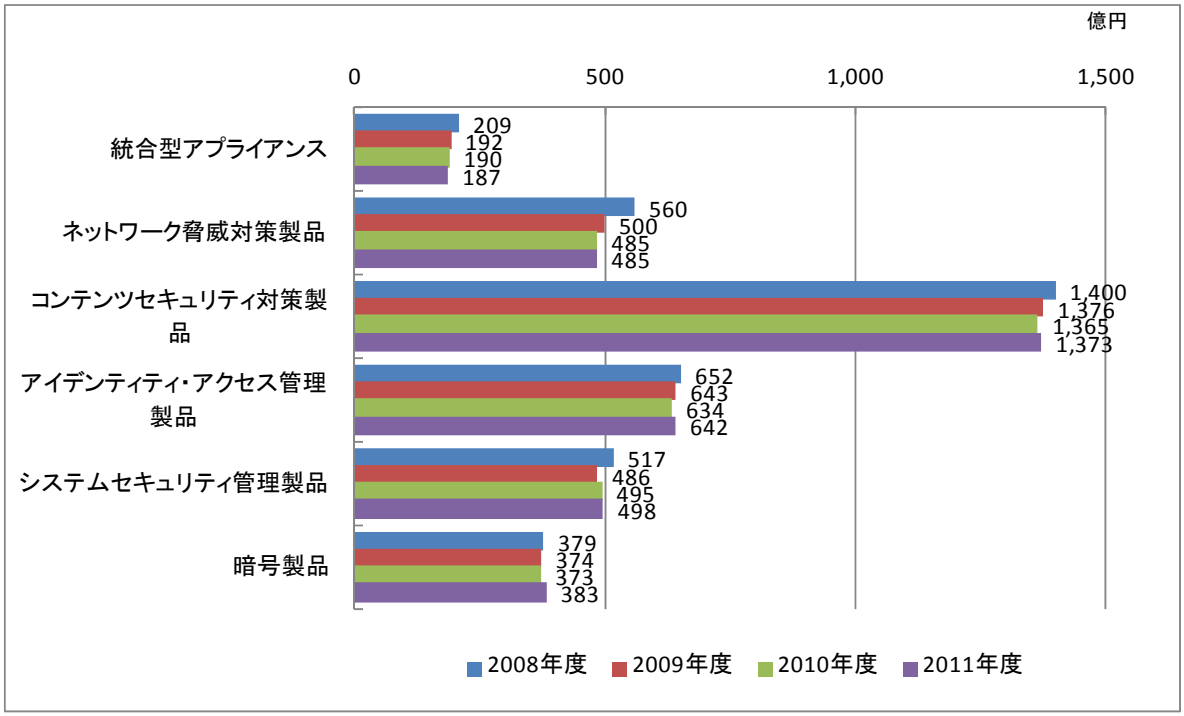
これと対照的にマイナス幅が 1.5%前後に収まった「暗号製品」、「アイデンティティ・アクセス管理製品」、「コンテンツセキュリティ対策製品」は不況の影響が軽微だったと言える。このうち「コンテンツセキュリティ対策製品」はセキュリティ対策の中で最も基本的で普及率も高いマルウェア対策製品が大きなウェイトを占めており、変動要素が少ないことが要因と考えられる。「暗号製品」、「アイデンティティ・アクセス管理製品」は比較的近時まで整備が続けられている情報漏えい対策や内部統制管理対策の中心的製品群を構成するため、その結果と考えられる。同じ要因は「コンテンツセキュリティ対策製品」の一部にも当てはまる。

図 3 に国内情報セキュリティツール市場の経年推移のグラフを示す。

2009 年度は、2008 年度の半ばに始まった世界同時不況の影響が、年度を通じて継続した年と言える。その結果、情報セキュリティツールは全てのカテゴリにおいてマイナス成長に見舞われるという結果となった。また、需要家の一部には 2009 年度の不透明さに備えるために 2008 年度中に繰り上げ実施を決断する動きもあったという業界関係者の話も聞かれ、その反動がマイナスに拍車をかけた面も否定できない。

結果として、2009 年度の実績値は、2008 年度比 3.9%減少して推定 3,571 億円となったものと見る。2010 年度については、全体として引き続き低調な推移が観測され、2 年連続のマイナス成長で、前年度比 0.8%減の 3,542 億円（実績見込値ベース）であったと推定される。

**図 3　国内情報セキュリティツール市場推移**




2010 年度のカテゴリ別には、「システムセキュリティ管理製品」が唯一プラス成長となり、1.9%増の 495 億円となった。前年度の落込みの反動と考えられる。他のカテゴリはマイナス成長が継続しており、中でも「ネットワーク脅威対策製品」の前年度比成長率はマイナス 3.0%と、前年度のマイナス 10.7%に続いて情報セキュリティツールの中で最大の落込みとなった。市場規模は 485 億円である。ネットワーク機器は投資サイクルがあり、その谷が継続した要素の影響もあると推測される。同様の理由で「統合型アプライアンス」も同マイナス 1.5%、190 億円となった。「アイデンティティ・アクセス管理製品」は同マイナス 1.4%で 634 億円となった。内部管理型の領域は不況時には圧縮されやすい傾向にあるためとも考えられる。好不況の影響が最も少ない「コンテンツセキュリティ対策製品」市場は同マイナス 0.8%、1,365 億円であった。同マイナス 0.1%とほぼ横ばいを維持したのは「暗号製品」の 373 億円で、引き続き情報漏えい対策には手が抜けなかったということかもしれない。

2011 年度については、2011 年 3 月に発生した東日本大震災による影響が懸念される。2011 年 9 月現在では、生産の回復速度は予想以上であるが、被災地を中心に消費の落込みが大きく、また世界的信用不安の経済に対する圧迫が強まる中で、不確定要因の極めて大きい状態が続いていると言える。市場規模の推定作業は、2011 年 2 月時点で行っており、これらの要素は反映していない。その結果、「統合型アプライアンス」が特異的に 1.4%減となった他は横這いか若干のプラス成長という予測になっている。経済の、わずかながらではあるが持ち直し傾向、2 年続いたマイナス成長のカバー、外部脅威の高まりとそれに対する認識等の要素が、合計でプラス 0.7%、3,568 億円という予測結果に結びついていると考えられる。震災・津波・洪水、電力不足、信用

不安、円高、株安、就職難、政治不安といった企業や社会を取り巻く幾重もの苦難を乗り越えて、新たな枠組みによる経済が活況を呈することで、明るい兆しが感じられるようになることが望まれる。

### 2.1.2. 情報セキュリティツール市場のカテゴリ別分析

以下、情報セキュリティツール市場を構成する各製品区分の市場についてその規模と概要を詳述する。

#### 2.1.2.1. 統合型アプライアンス市場

(1)市場の動向

統合型アプライアンス製品は、企業のセキュリティ対策において費用対効果と利便性を同時に両立できる事がポイントで、初期には中小企業への導入が進んだ。中小企業が複数のセキュリティ対策製品を統合し、導入費用、運用管理工数の低減を目的に導入を進めたことで、急速に市場が拡大した。しかし、需要一巡後に停滞する時期があった。それを打破できた理由として、ハードウェア性能の飛躍的な向上があげられる。停滞していた時期には、複数の機能を 1 台のハードウェアで稼動させることは性能の劣化を招くことから敬遠されていた。しかし、ハードウェア性能の向上によって実用に耐えるレベルの性能を発揮することが可能になった結果、普及機レベルでは、汎用の IA[2]機で実用上問題ないレベルのパフォーマンスを実現している。

一方、パケットフィルタリング等の特定機能をハードウェア化して非常に高いスループットを実現する技術も発展しており、それを利用することで、飛び抜けてハードウェア性能の高い専用機を実現することも可能になった。ユーザは利用目的によって、このどちらかを選択できることになり、適用の場が大きく広がっている。1 台の装置を設置することで複数の対策が実現できるという使い勝手のよさも市場拡大に大いに貢献している。

低価格の普及機は、特に中堅・中小企業、大企業の出先事業所や部門間接続、小売業のような多店舗展開している企業等に多く受け入れられている。専門家の確保が難しい事業所のネットワーク環境に導入する場合に、複数の機能を一元的に簡易に実現できる統合ソリューションとして、統合型アプライアンスの需要は高まっていると見られ、小規模ネットワーク環境への普及機クラスの導入需要は今後も衰えることはないであろう。

またハイエンド機は、データセンタや企業の基幹ネットワークといった高性能を期待される環境への導入が一般的になっている。特にデータセンタではフットプリント（ラックの占有スペース）が問題になると同時に、ユーザごとのネットワークの分離も必須課題である。このためネットワーク脅威と一部のコンテンツセキュリティ対策を 1 台で実現できる統合型アプライアンスは便利で重要な構成要素となっている。

一方で、クラウドコンピューティングの浸透は、統合型アプライアンスを始めとするハードウェア型製品の需要に影響を与える可能性がある。パブリッククラウドが提供する環境とインターネットの接点においては、高機能かつ高性能の対策機器を多重化して設置する必要があり、ハイ

[2] インテル・アーキテクチャ　インテル社製 CPU を用いて PC 機能を実現するハードウェアセット

エンド機への一段の需要シフトをもたらす可能性がある。一方、IaaS 等をホスティング環境として利用するユーザにとっては、自分の環境に対するネットワーク防御の選択肢は、仮想アプライアンスが中心となる。機能構成としてはアプライアンスでありながら、仮想化状態で提供されることとなり、製品形態としてはソフトウェア型ということになる。仮想化が急速に普及する中で、ハードかソフトかの区分が意味を持たなくなる可能性もあり、今後の動きに注意する必要が出てきている。

統合型アプライアンスの供給構造も大きく変化が進んだ。市場の初期は統合型アプライアンス専業ベンダが市場を開拓し急成長したが、ファイアウォールベンダの路線転換や、大手ネットワーク装置ベンダからの参入もあり、特に普及機クラスは価格競争も発生して競争の激しい市場となった。その結果、大手ネットワーク機器ベンダによる買収等が進み、独立の専業ベンダは少なくなってきている。

(2)市場規模とその推移

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

**表 3　国内統合型アプライアンス市場規模　実績と予測**

| 市場規模(百万円) | 2008 年度 | 2009 年度 | 2010 年度 | 2011 年度 |
|---|---|---|---|---|
| 統合型アプライアンス | 20,880 | 19,243 | 18,963 | 18,703 |
| 対前年度比成長率 | ― | -7.8% | -1.5% | -1.4% |

統合型アプライアンス製品は、2006 年度にはセキュリティ市場における地位をほぼ確立し、2007 年度も拡大を続けた。2008 年度にはペースは落ちたものの拡大基調を維持し、市場成長率も 9.0%を確保したが、2009 年度ではマイナス 7.8%と大幅な落込みを見せた。2010 年度も小幅ながらマイナス、2011 年度も同様の傾向が続くとの予測となった。

2008 年度は、2007 年度から続いた設備投資の好調を背景に、特に前半に市場が伸びたことにより、年度半ばに起きたリーマンショックの影響はありながらも、年度を通じての市場の勢いは維持されていた。2009 年度は、リーマンショック後の世界同時不況で経済全体の停滞が続き、市場は全体に縮小傾向で推移した。2010 年度は回復が期待されたが、年度当初に景気の踊り場的状況が発生し、これが全体として投資を控える方向に動いたため停滞が持続した。年度後半には回復の動きが強くなったが、年度を通じた数字としては、プラスに戻るに至らなかった。年度末に発生した東日本大震災も、若干の影響を与えたと想定される。

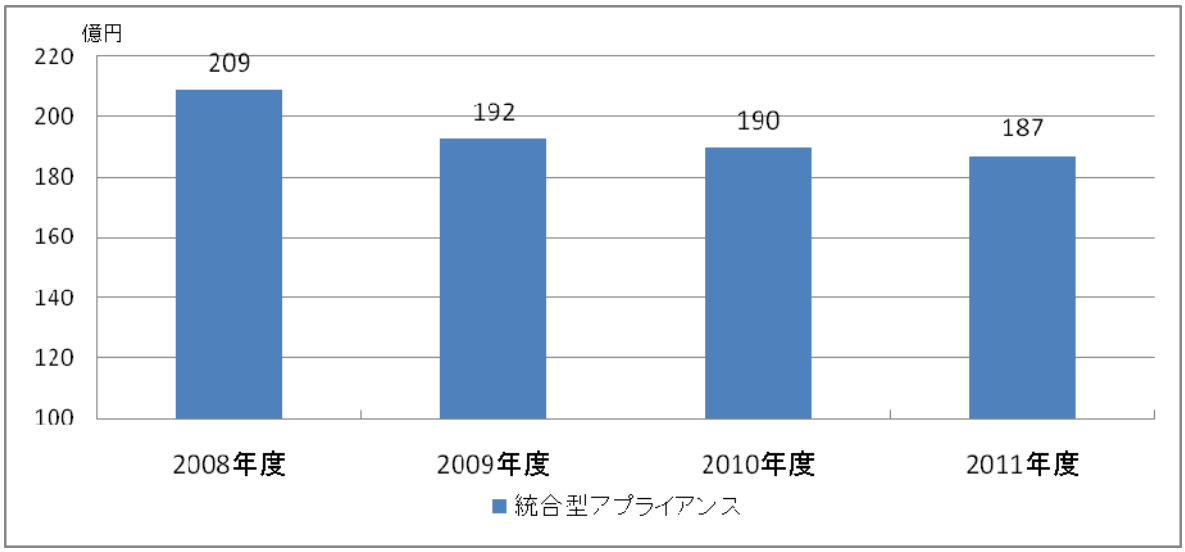
2011 年度は、震災直後の原発事故やサプライチェーンの機能不全による生産停滞の影響と、その回復並びに復興需要への期待があり、市場規模の拡大・縮小の度合いは極めて見通しにくい状態にある。特に、原発政策をめぐる政府の混乱が、電力供給制約を日本中に拡大しており、産業の生産活動への影響は大きなものがあるが、どのような対策、解決策が講じられるのか全く不透明である。このような状況下では、企業も悲観的とならざるを得ず、2011 年度に明るい見通しを持つのは難しい状況にある。

今後については、2007～2008 年度の投資が活発だった時期に導入された製品の更新サイクルを迎えることが、需要拡大要素として挙げられる。クラウドコンピューティングの浸透は、当面は企業のネットワーク構成を変化させるまでには至らず、むしろ事業所の入り口の対策に関しては強化の必要も出ると考えられることから、直ちに大きな影響を考える必要はないであろう。

クラウド環境を含む大規模データセンタのゲートウェイに対するハイエンド機の需要と、クラウドにより促進される小規模事業所のネットワーク接続の需要に期待されるところである。

**図 4　国内統合型アプライアンス市場推移**




### 2.1.2.2. ネットワーク脅威対策製品市場

(1)市場の動向

ネットワーク脅威対策製品の 2009 年度におけるセグメント別市場規模の分布を図 5 に示す。

ネットワーク脅威対策製品は、インターネットの商用利用が解禁されてビジネスに利用されるようになった初期のころから登場していた。1990 年代半ばには、ファイアウォールは先進的なインターネットユーザの間にかなり広まっていた。その後 IDS が登場し、IPS へ発展する流れとなっている。初期の製品はほとんどすべてがソフトウェア製品として提供され、PC サーバや UNIX ワークステーションの上で使われていた。21 世紀に入って、ハードとソフトを一体化して一つの製品として提供するモデルが広がり、今日ではアプライアンス型製品が主流となっている。

一方、クラウドコンピューティングや仮想化技術の浸透に伴って、ファイアウォールの仮想化も行われるようになってきている。仮想化製品の需要の拡大に伴って、ソフトウェアタイプの製品の比率が回復してくる可能性もある。

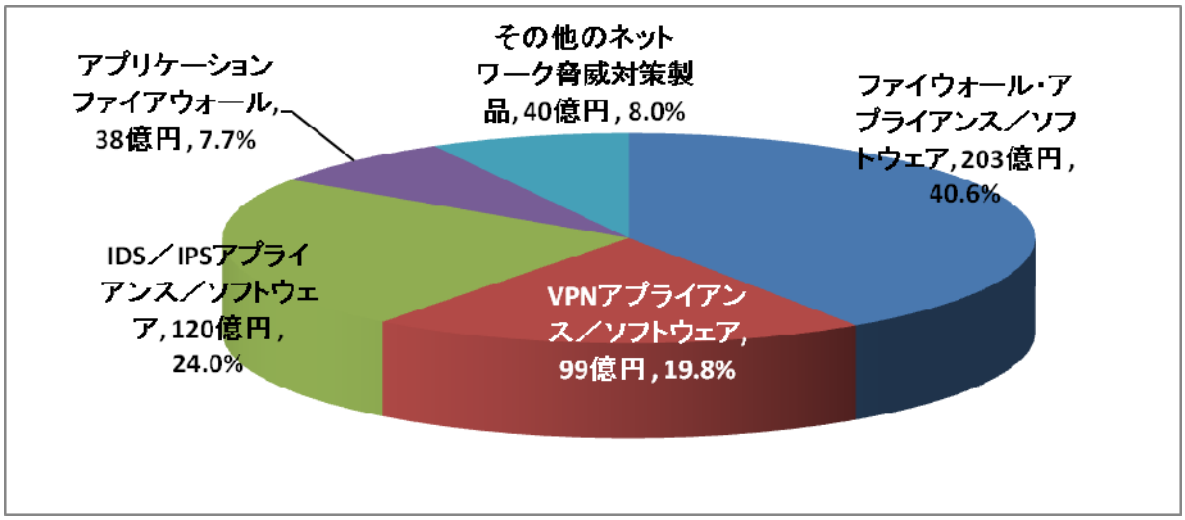
アプリケーションファイアウォールは、2005 年ごろから製品が出だした、比較的新しいジャンルである。Web アプリケーションの脆弱性が悪用されてマルウェア等が仕掛けられ、通常の Web 閲覧だけでマルウェア感染する事例が急増したことから、近年普及速度が上っている模様である。特に PCI DSS[3]の v1.2 により、一般公開されている Web アプリケーションへの要件として「定

[3] PCI DSS: Payment-Card Industry Data Security Standard　クレジットカード事業者の団体が制定した、ク

期的なアプリケーションコードの見直し」または「ウェブアプリケーションファイアウォールの導入」が要求されていることや、OWASP[4]という団体の活動、また日本でも IPA（独立行政法人情報処理推進機構）セキュリティセンターが 2010 年 2 月 16 日に「Web Application Firewall 読本」を公開する[5]等、アプリケーションファイアウォールについては依然として広く注目を集めていることが伺える。Web アプリケーションの他に、データベースをガードする製品も存在している[6]。

このように新しい技術を取り入れた製品が登場し、ネットワークの脅威に対応した製品の市場を広げている。しかし、急速に深刻化する外部ネットワークの脅威に対して内部の IT 環境を保護するために多くのセキュリティ機能を供えることが必要になった結果、個別機能の製品を多く導入することによるコスト負担や、複数機器を統合的に管理することの困難さから、統合型アプライアンスの導入や移行の動きが続いている。ネットワーク脅威対策製品は、単機能型から複数機能統合型への移行が進んでいると言える。

**図 5　2009 年度のネットワーク脅威対策製品市場**




また、ファイアウォールや VPN はインターネットが普及した比較的初期から導入が進んでおり、IDS／IPS の設置も一般化することで、市場は成熟化が進んでいる。その結果、ネットワーク脅威対策製品として市場を見てみると、市場の伸びは限定的になってきている。但し、ハイエンドの専用機については高信頼性が要求される通信事業者やデータセンタ等の特定市場では確実な需要が見られる他、在宅勤務やクラウドの利用拡大に伴い、リモートアクセスの安全を確保す

---

レジットカード事業者や加盟店に準拠を要求するセキュリティ対策基準。
https://www.pcisecuritystandards.org/index.htm

[4] OWASP （Open Web Application Security Project） アメリカで組織され世界的に展開している非営利活動団体。Web アプリケーションのセキュリティ対策を中心に活動している。
http://www.owasp.org/index.php/Main_Page
OWASP の Web アプリケーションファイアウォールについての活動については以下を参照
http://www.owasp.org/index.php/Web_Application_Firewall

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

[6] 業界団体としては、国内ではデータベース・セキュリティ・コンソーシアム（DBSC）が活動している。
http://www.db-security.org

るための VPN 機器は需要の拡大傾向が見られる。

(2)市場規模とその推移

表 4 にネットワーク脅威対策製品市場の市場規模実績推定値と予測値を、図 6 にその市場規模の推移のグラフを示す。

ネットワーク脅威対策製品のカテゴリは、2009 年度における売上実績推定値が 500 億円で、2008 年度から 10.7%減と大幅な落込みを記録した。2010 年度は 3.0%減と若干の縮小で済み、2011 年度はほぼ横ばいとの予測結果となった。情報セキュリティツール市場の中での構成比で見ると、2009 年度は 14.0%で前回の調査と同様 3 番目に位置するが、2010 年度は 13.7%となり、14.0%を占めるシステムセキュリティ管理製品と逆転して 4 位に転落している。

インターネットの登場と共に最も早くから登場したセキュリティ対策手段であったため市場の成熟化が進んでいることに加え、機能が拡充してきている統合型アプライアンスへのシフトが引き続き進んでいることが伸び率鈍化の要因の一つと言える。2007 年度（533 億円）から 2008 年度にかけては 5%の拡大が見られたが、以下に見るように投資サイクル、経済条件等様々な要因から成熟化・安定化（または緩やかな縮小）のステージに入ってきたものと考えられる。

**表 4　国内ネットワーク脅威対策製品市場規模　実績と予測**

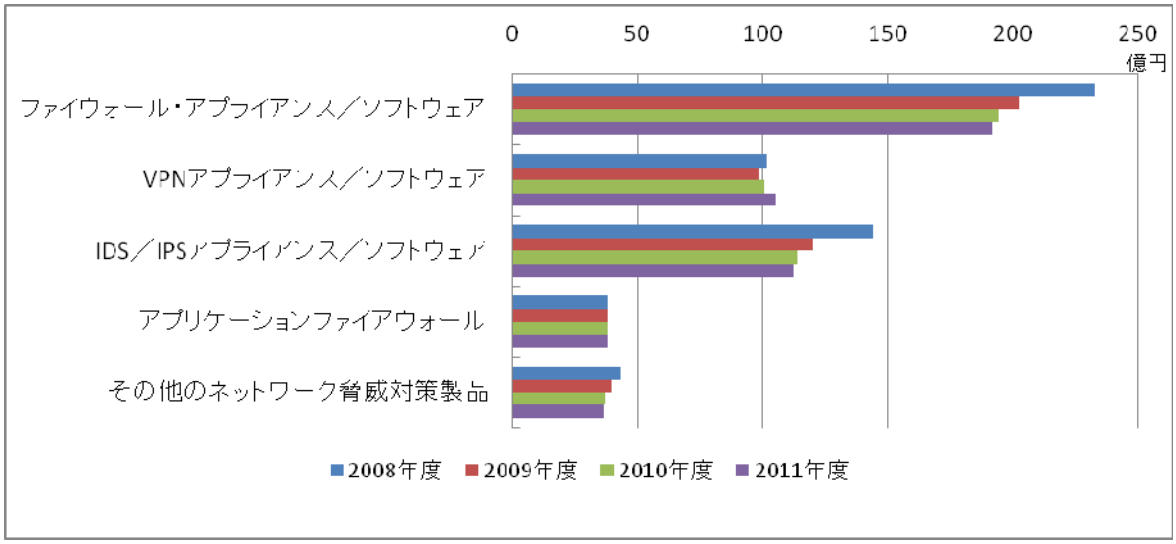
| **市場規模（百万円）** | 2008 年度 | 2009 年度 | 2010 年度 | 2011 年度 |
|---|---|---|---|---|
| ファイアウォールアプライアンス/ソフトウェア | 23,284 | 20,289 | 19,466 | 19,233 |
| VPN アプライアンス／ソフトウェア | 10,171 | 9,889 | 10,070 | 10,520 |
| IDS／IPS アプライアンス／ソフトウェア | 14,397 | 12,022 | 11,411 | 11,248 |
| アプリケーションファイアウォール | 3,836 | 3,837 | 3,832 | 3,820 |
| その他のネットワーク脅威対策製品 | 4,315 | 3,984 | 3,737 | 3,688 |
| 合計 | 56,003 | 50,022 | 48,515 | 48,508 |
| **構成比** | | | | |
| ファイアウォールアプライアンス/ソフトウェア | 41.6% | 40.6% | 40.1% | 39.6% |
| VPN アプライアンス／ソフトウェア | 18.2% | 19.8% | 20.8% | 21.7% |
| IDS／IPS アプライアンス／ソフトウェア | 25.7% | 24.0% | 23.5% | 23.2% |
| アプリケーションファイアウォール | 6.8% | 7.7% | 7.9% | 7.9% |
| その他のネットワーク脅威対策製品 | 7.7% | 8.0% | 7.7% | 7.6% |
| 合計 | 100.0% | 100.0% | 100.0% | 100.0% |
| **対前年度比成長率** | | | | |
| ファイアウォールアプライアンス/ソフトウェア | － | -12.9% | -4.1% | -1.2% |
| VPN アプライアンス／ソフトウェア | － | -2.8% | 1.8% | 4.5% |
| IDS／IPS アプライアンス／ソフトウェア | － | -16.5% | -5.1% | -1.4% |
| アプリケーションファイアウォール | － | 0.0% | -0.1% | -0.3% |
| その他のネットワーク脅威対策製品 | － | -7.7% | -6.2% | -1.3% |

| | | | | |
|---|---|---|---|---|
| 合計 | ― | -10.7% | -3.0% | 0.0% |

ネットワーク脅威対策製品のカテゴリの中では 1 番大きいセグメントであるファイアウォールアプライアンス／ソフトウェア製品は、2008 年度の 233 億円をピークとして、2009 年度 203 億円、2010 年度 195 億円、2011 年度 192 億円と縮小傾向を見せている。2007 年度から 2008 年度前半までは、通信事業者を中心とするハイエンドのユーザの設備投資サイクル上の更新期に当っていたため、2008 年度に当面のピークを迎えたが、2009 年度にはその反動と景気の低迷による設備投資控えの影響を受け、約 13%減の 203 億円と急速に市場規模が縮小した。2010 年度も市場の縮小傾向が続き、4%程度のマイナス成長となっている。以降、経済状況がなかなか好転しない状況から、2011 年度にかけても低迷が続くとの予測となった。

VPN アプライアンス／ソフトウェア製品は、ネットワーク脅威対策製品カテゴリの中では最も経済停滞の影響を受けないセグメントと考えられる。その市場規模と成長率の推移は、2008 年度 102 億円、2009 年度 99 億円・マイナス 2.8%、2010 年度 101 億円・1.8%、2011 年度 105 億円・4.5%となっている。この背景には、モバイル通信を含めたブロードバンド通信環境の一層の充実を背景に、社外から社内に接続するいわゆるモバイルワーカーやテレワーキング（ホームオフィスやサテライトオフィス）が一層盛んになってきていることがある。2008 年度は新型インフルエンザの流行、いわゆるパンデミックに対して事業継続管理のための対策が急に注目された。更に 2011 年度は、震災に対応しての事業継続管理や、電力不足対応での在宅・リモート勤務制度の大量導入の動きが出ている。このためにリモートアクセスに際しての VPN 環境を整える動きは強まってきており、市場の堅調さ、逆境の中での伸びを支えている。

**図 6　ネットワーク脅威対策製品市場推移**




ネットワーク脅威対策製品のカテゴリの中では 2 番目に大きいセグメントである IDS／IPS アプライアンス／ソフトウェア製品は、2009 年度は前年度比 16.5%減の 120 億円となっている。更に 2010 年度はマイナス 5.1%成長で 114 億円まで縮小する。2011 年度には、特段の拡大・縮

小要素は見られず、若干規模が縮小して 112 億円になるとの予測となった。2009 年度の大幅な落込みの背景には、ファイアウォールと同様の投資サイクルの狭間並びに経済要因が考えられるが、それに加え技術的要素も影響している可能性がある。IDS／IPS を効果的に運用するためには専門家の確保や専門企業へのアウトソーシングが必要になりコストが掛かるため、自ら導入し運用する事業者は比較的大規模な事業者に限定されるが、その層の事業者への導入が一巡したと考えられることも背景にあると思われる。

アプリケーションファイアウォールは、2007 年度に市場が急速に立ち上がった、新しいセグメントである。市場規模は、2008 年度は 9.5%と高い成長率を示して 38 億円規模に達した（前回調査による）。2009 年度から 2011 年度も全く横ばいで 38 億円という推定市場規模が継続するとの予測となっている。全体として縮小や低迷が続く中で市場規模がほぼ維持される理由としては、Web アプリケーションがネットワークからの攻撃の対象とされ、多くの大企業にも被害が発生するケースが増えており、手口も巧妙化してきて被害が拡大していることや、PCI DSS 標準の導入要件となったこと、PCI DSS の加盟店への遵守期限が定められたこと等も背景にあるのではないかと考えられる。また、データベースへの防御機能を提供するタイプにおいても、企業秘密の漏えい事件や内部統制への対応から需要が高まると考えられる。2011 年度初頭に発生した、ソニーを始めとする多数のゲームメーカへのサイバー攻撃や、日本のグローバル企業を標的としたと思われる一連の攻撃も、IDS／IPS や WAF の需要を押し上げる要因になると想定される。なお、今回の市場規模推定作業には、2011 年度に入ってからの要素は反映されていないのでご留意いただきたい。

#### 2.1.2.3. コンテンツセキュリティ対策製品市場

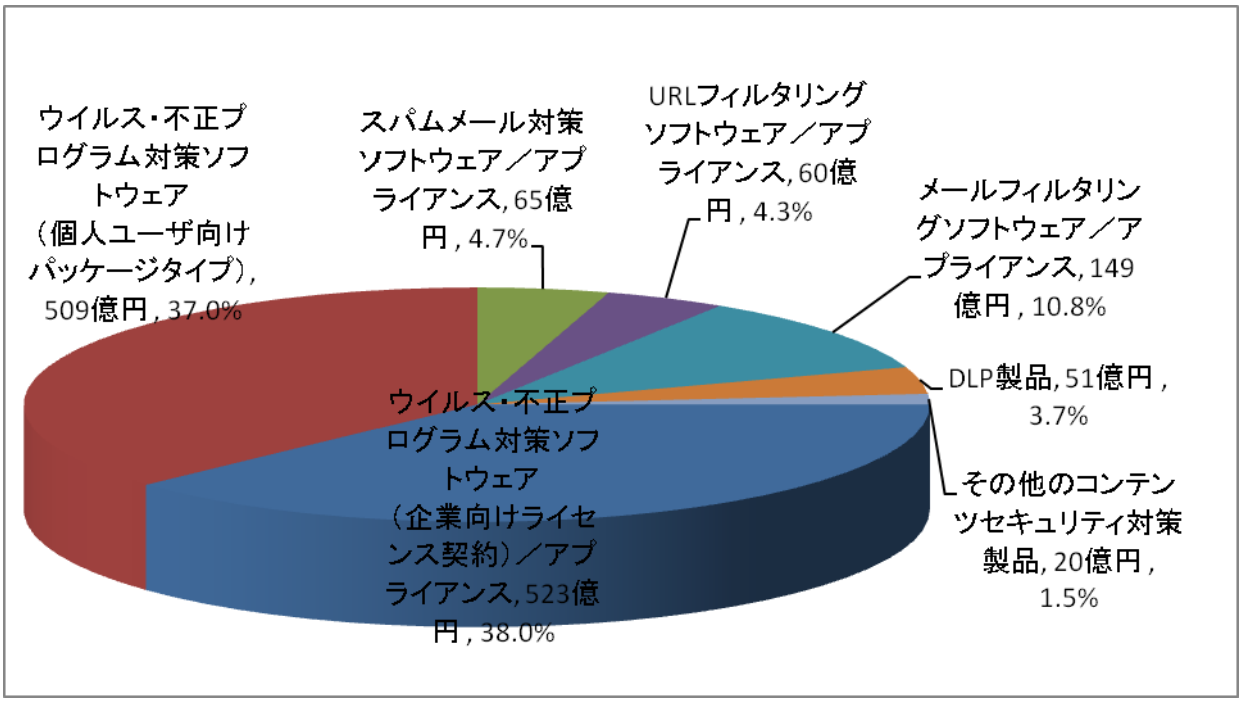
コンテンツセキュリティ対策製品は、情報セキュリティツール市場のうち金額規模が最も大きいカテゴリである。2008 年度には 1,400 億円という規模にまで到達したが、2009 年度、2010 年度推定実績値は 1,370 億円前後で（情報セキュリティツール市場合計に対する構成比 38.5%、2008 年構成比と比較し 0.8 ポイント増）となった。これは、他の市場に比べ、リーマンショックとその後の景気後退の影響が少なかったことを示している。

コンテンツセキュリティ対策製品の 7 つの製品分類における 2009 年度の分布を図 7 に示す。「ウイルス・不正プログラム対策ソフトウェア」が、企業向けと個人向けを合わせると、市場の約 75%を占める。ウイルス対策は、セキュリティ対策のなかでも 20 年の歴史を持つ代表的なものであり、企業向け・個人向けともに利用が浸透している。とりわけ企業における実施率は、既に 5 年前からほぼ 100%となっており、企業規模に関わらずその普及率はきわめて高い。

続いてコンテンツセキュリティ対策製品市場の約 20%を占めるのが「メールフィルタリング」、「スパムメール対策」、「URL フィルタリング」となり、「DLP 製品」（情報漏えい対策製品・システム）が新しい市場を形成し始めた。

**図 7　2009 年度のコンテンツセキュリティ対策製品市場**




「ウイルス・不正プログラム対策ソフトウェア」は、圧倒的な普及率の高さゆえ、新規顧客の減少や市場サイズの縮小により 2009 年度は市場規模の減退を予測していたが、実際には複雑化多様化するウイルス対策には定義ファイルの更新が必要であることが周知され、ライセンス更新による契約が維持されたこと等が要因となり、他の製品が縮小する中、市場規模を維持する結果となった。スマートフォン、インターネット対応のテレビやゲーム機等新しい機器の登場により、この高い普及率は個人向けの市場にも波及し、拡大が期待される。ウイルス作成罪といった法律改正が市場にもたらす影響も含め引き続き注目する必要がある。

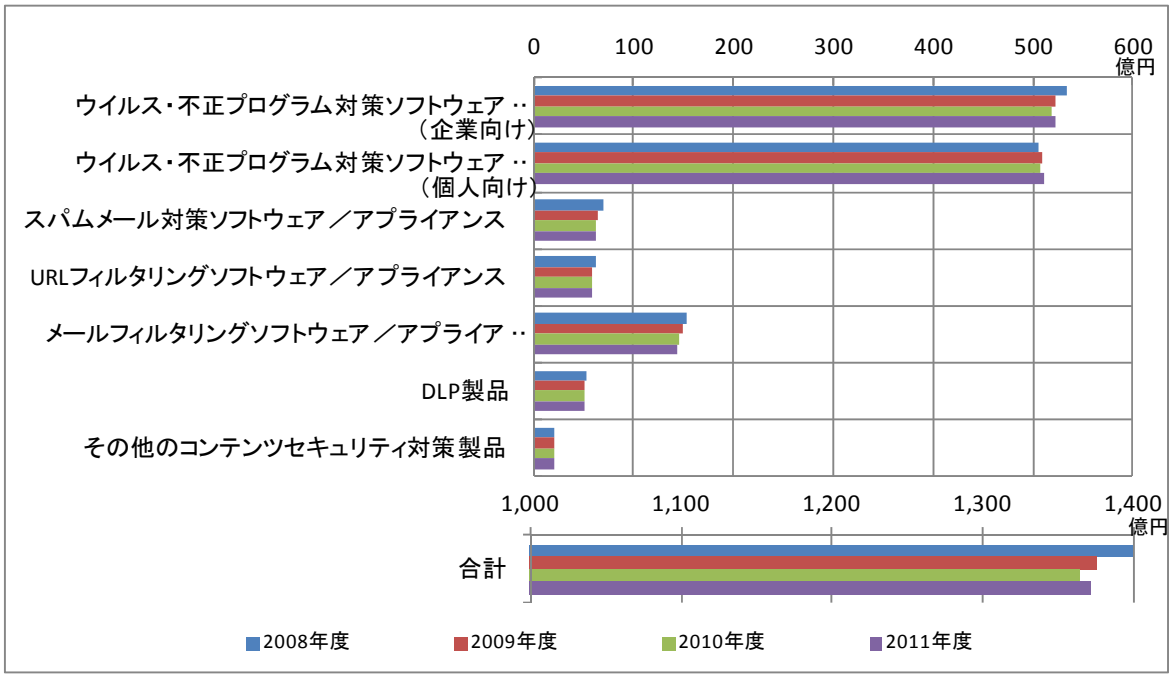
表 5 に国内コンテンツセキュリティ対策製品の市場規模実績推定値と予測値を、図 8 にその市場規模推移のグラフを示す。「コンテンツセキュリティ対策製品」は経済情勢の急激な悪化の影響を大きく受ける中、2008 年度 1,400 億円をピークに、2009 年度 1,376 億円（前年比成長率マイナス 1.7%）、2010 年度 1,365 億円（同、マイナス 0.8%）と微減となったが、2011 年度は景気のゆるやかな回復、個人向けの普及、クラウド環境での新たな設備投資等のプラス要因により、底を脱すると予測している。

**表 5　国内コンテンツセキュリティ対策製品市場規模　実績と予測**

| 市場規模（百万円） | 2008 年度 | 2009 年度 | 2010 年度 | 2011 年度 |
|---|---|---|---|---|
| ウイルス・不正プログラム対策ソフトウェア（企業向けライセンス契約）／アプライアンス | 53,460 | 52,281 | 51,822 | 52,190 |
| ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ） | 50,590 | 50,933 | 50,738 | 51,189 |
| スパムメール対策ソフトウェア／アプライアンス | 6,978 | 6,472 | 6,330 | 6,288 |

| | | | | |
|---|---|---|---|---|
| URL フィルタリングソフトウェア／アプライアンス | 6,249 | 5,953 | 5,943 | 5,883 |
| メールフィルタリングソフトウェア／アプライアンス | 15,387 | 14,878 | 14,496 | 14,455 |
| DLP 製品 | 5,255 | 5,108 | 5,132 | 5,154 |
| その他のコンテンツセキュリティ対策製品 | 2,059 | 1,996 | 2,072 | 2,091 |
| 合計 | 139,978 | 137,622 | 136,534 | 137,250 |
| **構成比** | | | | |
| ウイルス・不正プログラム対策ソフトウェア（企業向けライセンス契約）／アプライアンス | 38.2% | 38.0% | 38.0% | 38.0% |
| ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ） | 36.1% | 37.0% | 37.2% | 37.3% |
| スパムメール対策ソフトウェア／アプライアンス | 5.0% | 4.7% | 4.6% | 4.6% |
| URL フィルタリングソフトウェア／アプライアンス | 4.5% | 4.3% | 4.4% | 4.3% |
| メールフィルタリングソフトウェア／アプライアンス | 11.0% | 10.8% | 10.6% | 10.5% |
| DLP 製品 | 3.8% | 3.7% | 3.8% | 3.8% |
| その他のコンテンツセキュリティ対策製品 | 1.5% | 1.5% | 1.5% | 1.5% |
| 合計 | 100.0% | 100.0% | 100.0% | 100.0% |
| **対前年度比成長率** | | | | |
| ウイルス・不正プログラム対策ソフトウェア（企業向けライセンス契約）／アプライアンス | － | -2.2% | -0.9% | 0.7% |
| ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ） | － | 0.7% | -0.4% | 0.9% |
| スパムメール対策ソフトウェア／アプライアンス | － | -7.2% | -2.2% | -0.7% |
| URL フィルタリングソフトウェア／アプライアンス | － | -4.7% | -0.2% | -1.0% |
| メールフィルタリングソフトウェア／アプライアンス | － | -3.3% | -2.6% | -0.3% |
| DLP 製品 | － | -2.8% | 0.5% | 0.4% |
| その他のコンテンツセキュリティ対策製品 | － | -3.0% | 3.8% | 0.9% |
| 合計 | － | -1.7% | -0.8% | 0.5% |

**図 8　国内コンテンツセキュリティ対策製品市場推移**




### 2.1.2.4. アイデンティティ・アクセス管理製品市場

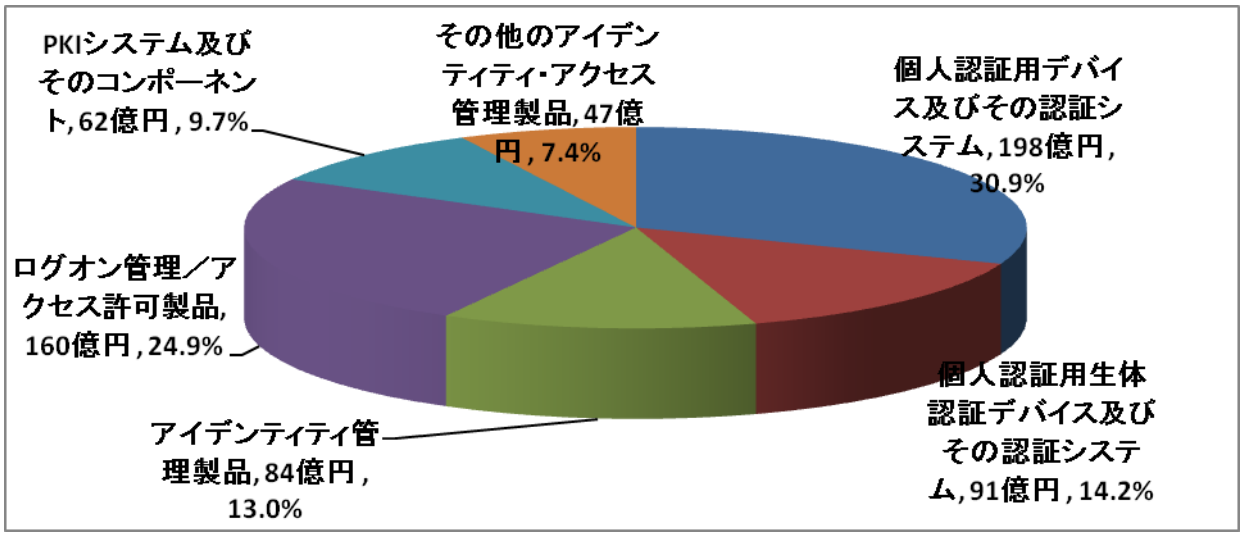
(1)　市場の動向

図 9 に 2009 年度のアイデンティティ・アクセス管理製品のセグメント別市場規模分布を示す。

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

間違いによるアクセスや不正アクセスを IT 技術で管理することで、不必要なアクセスの発生を最小限に抑止する環境を実現することと、データの改ざんやプログラムの改ざんを防止して正確な処理を実施するシステム運用が、IT ガバナンスの要件となる。つまり、情報セキュリティの CIA（Confidentiality：機密性、Integrity：完全性、Availability：可用性）という 3 大基本要素の中の、機密性と完全性という面に、よりフォーカスが当たっていると言えよう。

図 9　2009 年度のアイデンティティ・アクセス管理製品市場




クレジットカードビジネス関連事業者向けに策定された「PCI DSS（PCI データセキュリティ基準)」は、一般企業の情報セキュリティ対策にも有効なものと認識され、具体的な実施策として普及の動きがある。PCI DSS は 12 項目の要件で構成されており、要件 8 では「コンピュータにアクセスする際，利用者ごとに識別 ID を割当てること」を要求している。これを実現するための製品としても、「アイデンティティ・アクセス管理製品」カテゴリの製品への需要が、今後も高まることが予測される。

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

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

(2)　市場規模とその推移

表 6 に国内アイデンティティ・アクセス管理製品の市場規模推定実績値と予測値を、図 10 にその市場規模の推移のグラフを示す。

アイデンティティ・アクセス管理製品の市場規模は、2009 年度の実績で 642 億円（前年比伸び率 -1.5%）となり、「情報セキュリティツール」市場全体の 3,571 億円に対する構成比は 17.9 %であった。コンテンツセキュリティ対策製品市場に次ぐ規模の市場である。この市場規模は、2008 年秋以降に顕在化した世界金融危機を受け、 2010 年度には 634 億円（前年度比伸び率 マイナス 1.4%）と縮小するが、2011 年度には 642 億円（同 1.3%）に回復すると予測され

る。

アイデンティティ･アクセス管理製品市場の 2008 年度の対前年度比伸び率は､7.6%を記録(前回調査）し､情報セキュリティ市場全体の成長を牽引したが､2009 年度の伸びは急激に減速し､対前年度比伸び率は-1.5%となった。これは、情報セキュリティツール市場全体の対前年比伸び率（-3.9%）の中では、比較的マイナス成長が緩やかであったことを示している。

「アイデンティティ・アクセス管理製品」カテゴリの内訳をみると､「個人認証用デバイスおよびその認証システム」セグメントが 2009 年度の構成比で 30.9%と最も大きな部分を占めた。市場規模は 2010 年度で 195 億円であり、2011 年度には 198 億円に達すると見込まれる。

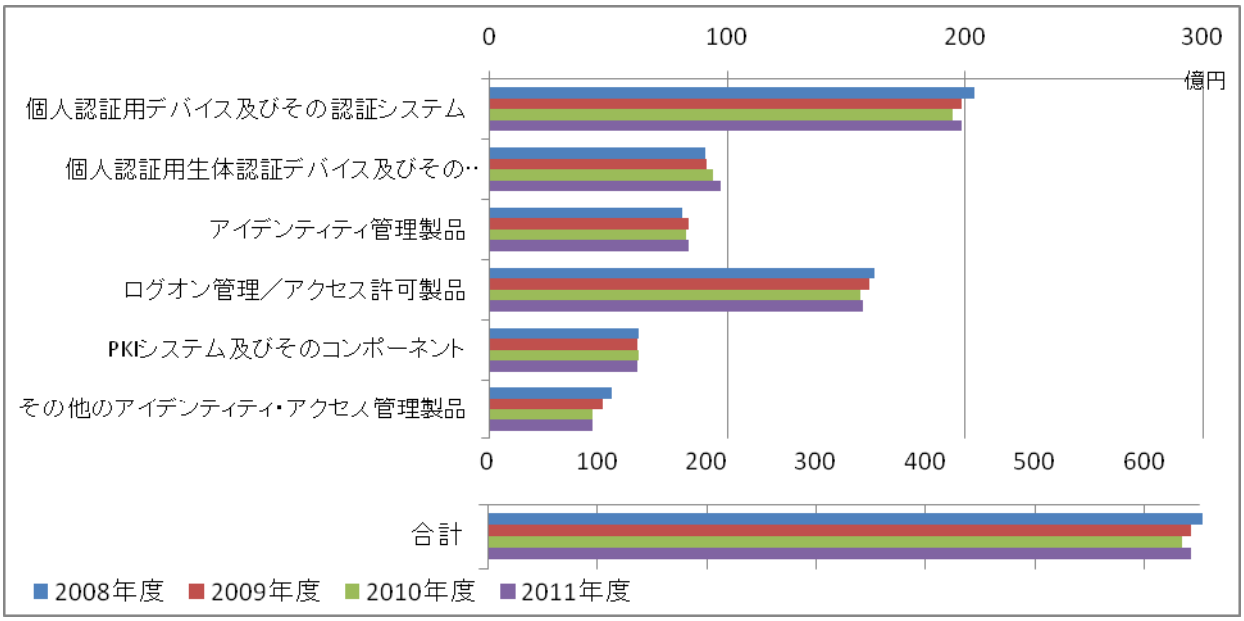
**表 6　国内アイデンティティ・アクセス管理製品市場規模　実績と予測**

| 市場規模（百万円） | 2008 年度 | 2009 年度 | 2010 年度 | 2011 年度 |
|---|---|---|---|---|
| 個人認証用デバイスおよびその認証システム | 20,409 | 19,841 | 19,481 | 19,848 |
| 個人認証用生体認証デバイスおよびその認証システム | 9,085 | 9,109 | 9,417 | 9,726 |
| アイデンティティ管理製品 | 8,100 | 8,365 | 8,288 | 8,386 |
| ログオン管理／アクセス許可製品 | 16,194 | 15,997 | 15,621 | 15,712 |
| PKI システムおよびそのコンポーネント | 6,287 | 6,212 | 6,245 | 6,206 |
| その他のアイデンティティ・アクセス管理製品 | 5,151 | 4,744 | 4,340 | 4,312 |
| 合計 | 65,225 | 64,269 | 63,392 | 64,191 |
| **構成比** | | | | |
| 個人認証用デバイスおよびその認証システム | 31.3% | 30.9% | 30.7% | 30.9% |
| 個人認証用生体認証デバイスおよびその認証システム | 13.9% | 14.2% | 14.9% | 15.2% |
| アイデンティティ管理製品 | 12.4% | 13.0% | 13.1% | 13.1% |
| ログオン管理／アクセス許可製品 | 24.8% | 24.9% | 24.6% | 24.5% |
| PKI システムおよびそのコンポーネント | 9.6% | 9.7% | 9.9% | 9.7% |
| その他のアイデンティティ・アクセス管理製品 | 7.9% | 7.4% | 6.8% | 6.7% |
| 合計 | 100.0% | 100.0% | 100.0% | 100.0% |
| **対前年度比成長率** | | | | |
| 個人認証用デバイスおよびその認証システム | － | -2.8% | -1.8% | 1.9% |
| 個人認証用生体認証デバイスおよびその認証システム | － | 0.3% | 3.4% | 3.3% |
| アイデンティティ管理製品 | － | 3.3% | -0.9% | 1.2% |
| ログオン管理／アクセス許可製品 | － | -1.2% | -2.3% | 0.6% |
| PKI システムおよびそのコンポーネント | － | -1.2% | 0.5% | -0.6% |
| その他のアイデンティティ・アクセス管理製品 | － | -7.9% | -8.5% | -0.6% |
| 合計 | － | -1.5% | -1.4% | 1.3% |

前年度比成長率でみると、「アイデンティティ管理製品」が一番高い伸び率を示しており、2009 年度 3.3%であったが、2010 年度は、「個人認証用生体認証デバイスおよびその認証システム」が 3.4%と推測され、情報セキュリティ製品全体を通しても、最も高い成長率が期待できるセグメントの一つである。

これはアクセス管理のための認証の意味もあるが、ノートパソコンを始め可搬型の媒体からの情報漏えいが後を絶たないことから、万一紛失・盗難にあってもデータにアクセスできないように生体認証を組み込む動きが顕在化した結果と推測される。

**図 10　国内アイデンティティ・アクセス管理製品市場推移**




「アイデンティティ・アクセス管理」は、大規模システムや基幹系システムでは以前から組み込まれており、成熟市場のイメージがあったが、内部統制からの必要性や情報セキュリティ対策の面から適用対象が拡大し、スマートフォンやタブレット PC の市場拡大に伴い、比較的高い市場成長が見込まれる状況となってきた。しかし、情報セキュリティ対策の中では経済状況の悪化の影響を一番受ける市場と予測している。特に大きなプロジェクトへの投資が鈍化する中、製品以外のコンサルティングやプランニング、インプリメンテーション費用が必要なため、導入期間が長期化するアイデンティティ管理、ログオン管理は優先順位を下げられる可能性が強く、その影響を受けやすいと考えられるからである。

### 2.1.2.5. システムセキュリティ管理製品市場

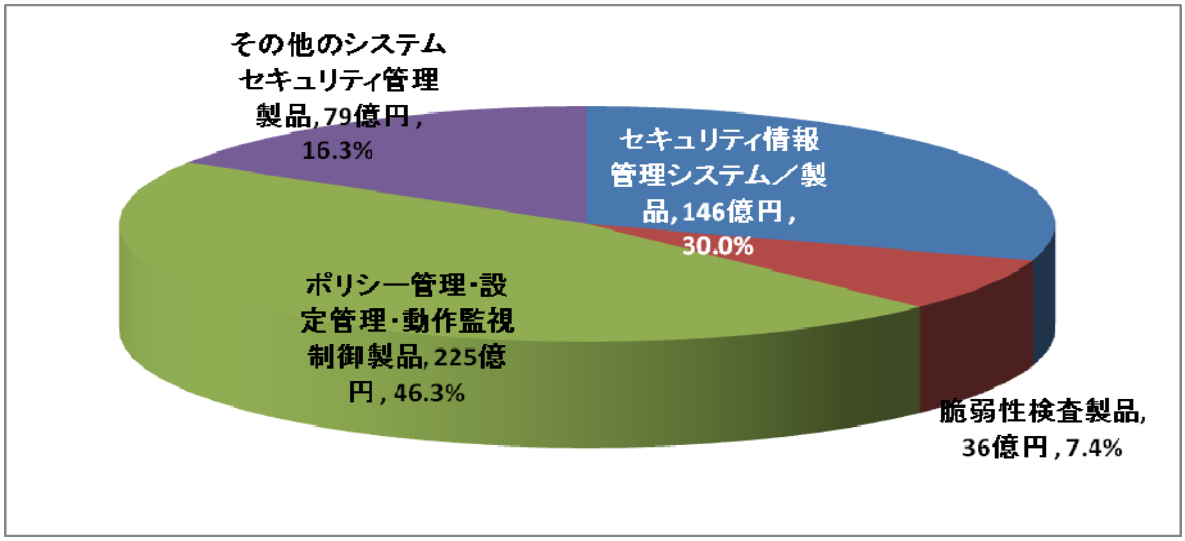
(1)市場の動向

システムセキュリティ管理製品の 2009 年度におけるセグメント分布を図 11 に示す。

昨年度に引き続き内部統制やコンプライアンス対応を意識して、ログ管理やデジタルフォレンジック製品への需要は増加するとみられていたが、市場規模の数字は縮小する結果となった。こ

れは予算執行見送りやツールの低価格化等の影響が考えられる。しかし、内部情報漏えい対策への投資は堅調に推移しているため、2010 年度には回復するとの予測結果となった。

**図 11　2009 年度のシステムセキュリティ管理製品市場**




「セキュリティ情報管理システム／製品」はPCI DSSへの準拠証明の取得期限が2009年12月とされた経緯もあり、製品を活用して対応する動きが見られたが、対応範囲に応じてシステムが大きくなる特徴があるため、製品導入よりも運用や独自ツール等で対応する動きもあり、市場への影響は限定的であった。

「ポリシー管理・設定管理・動作監視制御製品」は情報漏えい対策につながることから、需要は依然高く、漏えいポイントとなるUSBメモリの制御ができる製品群や管理対象マシンのOS情報やセキュリティパッチ適用状況の把握、ウイルス対策ソフトの定義ファイル情報、インストールされているアプリケーション情報等のインベントリ情報を収集する製品群等の市場は堅調に推移している。その他、持ち込み端末による管理ネットワークへの接続を制御する「ネットワーク検疫システム」の市場も堅調に推移している。この製品は上記インベントリ情報を収集するツールと連携して、OSのセキュリティパッチ適用状況やウイルス対策ソフトの定義ファイル更新状況等に応じて接続の可否を決定するといった機能を提供する。提供形態としては、エージェントをインストールするタイプや専用のハードウェアと一体化したアプライアンスタイプのものやVLAN（仮想的LAN）方式、ゲートウェイ方式、ルータに付加機能として載せる形等がある。

「脆弱性検査製品」は検査対象ホストにエージェントをインストールし設定情報等内部から収集し分析を行う「ホスト型」と呼ばれるタイプと、外部から検査対象マシンやWebアプリケーションに対してネットワーク経由で擬似攻撃を行うことにより検査、分析を行う「ネットワーク型」（もしくはスキャンタイプ）と呼ばれるものがある。

(2)市場規模とその推移

表7に国内システムセキュリティ管理製品市場の市場規模実績推定値と予測値を、図12にその市場規模の推移のグラフを示す。

「システムセキュリティ管理製品」市場は 2009 年度には全セグメント合せて 485 億円程度の市場を形成しており、2008 年度の 517 億円に比べて 6.1%減と市場の縮小を示しているが、2010 年度は 495 億円と 1.9%増の成長に転じた。セキュリティツール製品全体の市場全体として 0.9%縮小している中で唯一プラス成長した区分であることを考えると、この区分への企業の投資態度は堅調であったと考えられる。

**表 7　国内システムセキュリティ管理製品市場規模　実績と予測**

| 市場規模（百万円） | 2008 年度 | 2009 年度 | 2010 年度 | 2011 年度 |
|---|---|---|---|---|
| セキュリティ情報管理システム／製品 | 15,941 | 14,586 | 14,612 | 14,594 |
| 脆弱性検査製品 | 4,115 | 3,611 | 3,618 | 3,607 |
| ポリシー管理・設定管理･動作監視制御製品 | 23,226 | 22,493 | 23,306 | 23,647 |
| その他のシステムセキュリティ管理製品 | 8,441 | 7,899 | 7,969 | 7,923 |
| 合計 | 51,723 | 48,589 | 49,505 | 49,771 |
| **構成比** | | | | |
| セキュリティ情報管理システム／製品 | 30.8% | 30.0% | 29.5% | 29.3% |
| 脆弱性検査製品 | 8.0% | 7.4% | 7.3% | 7.2% |
| ポリシー管理・設定管理･動作監視制御製品 | 44.9% | 46.3% | 47.1% | 47.5% |
| その他のシステムセキュリティ管理製品 | 16.3% | 16.3% | 16.1% | 15.9% |
| 合計 | 100.0% | 100.0% | 100.0% | 100.0% |
| **対前年度比成長率** | | | | |
| セキュリティ情報管理システム／製品 | － | -8.5% | 0.2% | -0.1% |
| 脆弱性検査製品 | － | -12.3% | 0.2% | -0.3% |
| ポリシー管理・設定管理･動作監視制御製品 | － | -3.2% | 3.6% | 1.5% |
| その他のシステムセキュリティ管理製品 | － | -6.4% | 0.9% | -0.6% |
| 合計 | － | -6.1% | 1.9% | 0.5% |

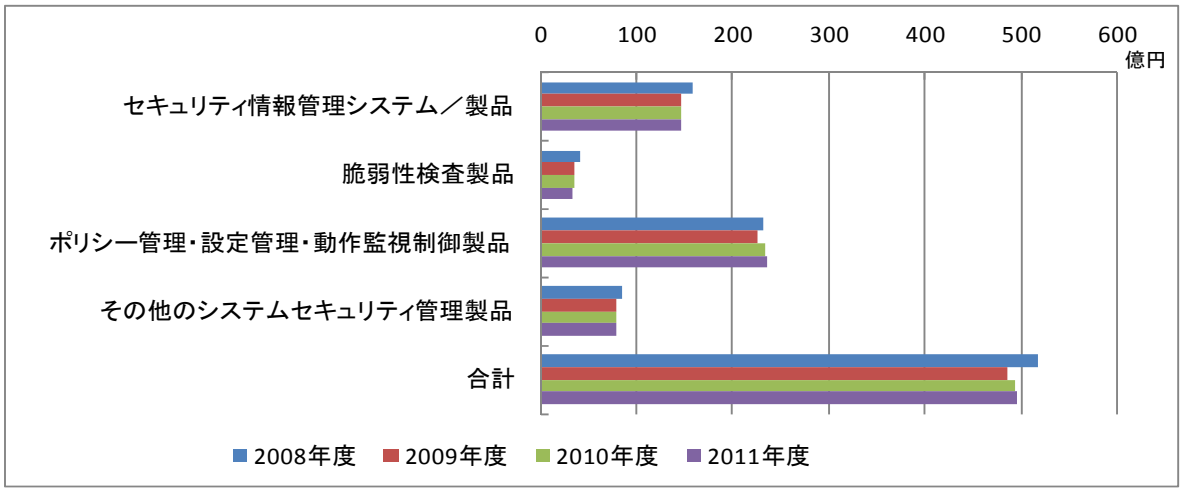
各セグメントの推移をみると、「セキュリティ情報管理システム／製品」は 2009 年度に大きく落ち込んだが 2010 年は 0.2%増とほぼ同じ水準で推移している。2011 年度の予測も同程度であると考えている。「脆弱性検査製品」も同様の動きをしており、2009 年度に大きく落ち込み、2010 年度は 0.2%増と同じ水準で推移している。

「ポリシー管理･設定管理･動作監視制御製品」はこの区分の約半分を占める市場となっており、2010 年度の予測における成長率も 3.6%増とセキュリティツールの中分類全部を並べた中でも 2 番目の成長率である。不況の影響を受けながらも企業のリスクとなる情報漏えいの対策を目的とする投資は行わざるを得ない状況であることが考えられる。この傾向は 2011 年度も継続すると考えられる。「その他のシステムセキュリティ管理製品」は 0.9%増と若干成長していることがわかるが、これは内部統制対応のためにログの収集・蓄積をするシステムの導入が進み、インシデントが発生した際に調査が出来る体制に向けてデジタルフォレンジック対応を進める動き等から

需要が拡大した結果と考えられる。とはいえ不況の影響を受け易い分野なので 2011 年度はニーズが一巡し、市場としては若干縮小するのではないかと推測している。

**図 12　システムセキュリティ管理製品市場推移**




### 2.1.2.6. 暗号製品市場

(1)市場の動向

暗号製品市場の 2009 年度における動向はいわゆる「暗号の 2010 年問題」において市場拡大すると推測していたが、移行に伴う検討段階に留まっているケースが多く実際の着手は 2010 年度以降に実施される傾向にある。具体的な事例としてある国内の政府機関は、2010 年度から開始、2013 年度末までに完了する予定となっている。このように移行が進まない背景には移行に伴う影響範囲が大きいことが考えられる。影響範囲として、認証局、サーバ、ネットワーク機器、クライアント（Web ブラウザやケータイ、ゲーム機、情報家電等の組込み機器）等が考えられ、それぞれ相互の接続性を検証する必要があり、政府機関や民間の相互連携が欠かせない状況となっている。その為 2009 年度の市場への影響はそれほど大きくなく、市場規模としては 2008 年度と同規模で推移している。2010 年度も同規模と考えられ、暗号化通信の方式移行へ実施が始まる 2011 年度から市場は拡大すると予測する。

(2)市場規模とその推移

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

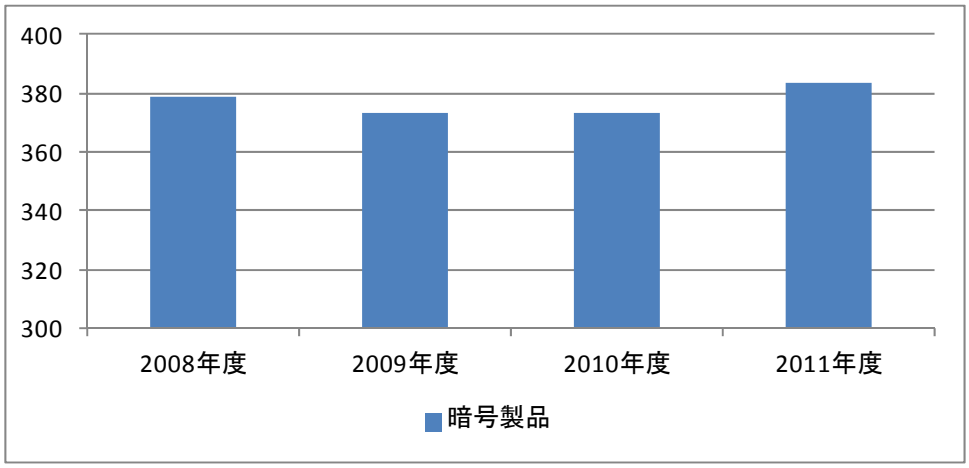
**表 8　国内暗号製品市場規模　実績と予測**

| 市場規模(百万円) | 2008 年度 | 2009 年度 | 2010 年度 | 2011 年度 |
|---|---|---|---|---|
| 暗号製品 | 37,853 | 37,351 | 37,307 | 38,339 |
| **対前年比成長率（%）** | | | | |
| 暗号製品 | - | -1.3% | -0.1% | 2.8% |

暗号製品市場は、2009 年度の市場規模は 374 億円で前年度比 1.3%減となった。昨年度の調査では 1.6%減と推測していたので、ほぼ推測通りの市場であった。2010 年度も同様の市場規模を保ちつつ推移し、「暗号化の 2010 年問題」への実対策フェーズに入る 2011 年度から少しずつ拡大していくと考えている。また、セキュリティツール全体は 3.9%減なので、下落幅は小さいものの国内市場の落ち込みが反映されていることが分かる。「暗号製品」の市場規模としては「セキュリティツール」全体の 10%程度を占める市場である。

2011 年度の予測値としては、「セキュリティツール製品」全体では 0.7%の伸びにとどまる中で、「暗号製品」は 2.8%の伸びを予測している。暗号製品は認証や情報漏えい対策の基盤となる製品なので、今後も市場は一定規模を維持しつつゆるやかに拡大していくと予測する。

**図 13　国内暗号製品市場推移**



## 2.2. 国内情報セキュリティサービス市場の分析

### 2.2.1. 情報セキュリティサービス市場の全体概要

「情報セキュリティサービス」とは、情報セキュリティ実現のための様々なサービスを指すもので、「情報セキュリティツール」がハードウェアもしくはソフトウェアという形のある商品、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商取引、すなわちサービスの提供と定義している。

このカテゴリには、大分類として「情報セキュリティコンサルテーション」、「セキュアシステム構築サービス」、「セキュリティ運用・管理サービス」、「情報セキュリティ教育」、「情報セキュリティ保険」の 5 カテゴリを定義した。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けになる。

表 9 に国内情報セキュリティサービス市場規模の実績推定値と予測値を示す。

**表 9　国内情報セキュリティサービス市場規模　実績と予測**

金額単位：百万円

| 年度別売上高推計値 | 2008年度 | | 2009年度 | | | 2010年度 | | | 2011年度 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| セキュリティ・サービス | 売上実績推定値 | | 売上実績推定値 | | | 売上高見込推定値 | | | 売上高予測値 | | |
| | 金額 | 構成比 | 金額 | 構成比 | 成長率 | 金額 | 構成比 | 成長率 | 金額 | 構成比 | 成長率 |
| 情報セキュリティコンサルテーション | 76,207 | 21.9% | 72,166 | 22.2% | −5.3% | 66,256 | 21.4% | −8.2% | 60,545 | 20.7% | −8.6% |
| セキュアシステム構築サービス | 147,679 | 42.5% | 130,424 | 40.1% | −11.7% | 122,206 | 39.4% | −6.3% | 109,835 | 37.5% | −10.1% |
| セキュリティ運用・管理サービス | 91,129 | 26.2% | 90,113 | 27.7% | −1.1% | 90,389 | 29.2% | 0.3% | 91,375 | 31.2% | 1.1% |
| 情報セキュリティ教育 | 24,981 | 7.2% | 24,884 | 7.7% | −0.4% | 23,900 | 7.7% | −4.0% | 23,841 | 8.1% | −0.2% |
| 情報セキュリティ保険 | 7,591 | 2.2% | 7,377 | 2.3% | −2.8% | 7,234 | 2.3% | −1.9% | 7,244 | 2.5% | 0.1% |
| セキュリティサービス市場合計 | 347,587 | 100.0% | 324,964 | 100.0% | −6.5% | 309,983 | 100.0% | −4.6% | 292,840 | 100.0% | −5.5% |

今回の調査結果では、2008 年度の「情報セキュリティサービス」市場規模は 3,476 億円と見積もられ、2009 年度には対前年度比成長率マイナス 6.5%と急速に縮小して 3,250 億円になったものと推定される。「セキュアシステム構築サービス」が同マイナス 11.7%と大幅なマイナスとなったことに加え、「情報セキュリティコンサルテーション」も 5.3%減となった。その他のカテゴリである「セキュリティ運用・管理サービス」「情報セキュリティ教育」「情報セキュリティ保険」もマイナスであり、2008 年度半ばに発生したリーマンショックに伴う世界的不況の波を真っ向からかぶった結果が、2009 年度に集中的に表れたと見ることができる。

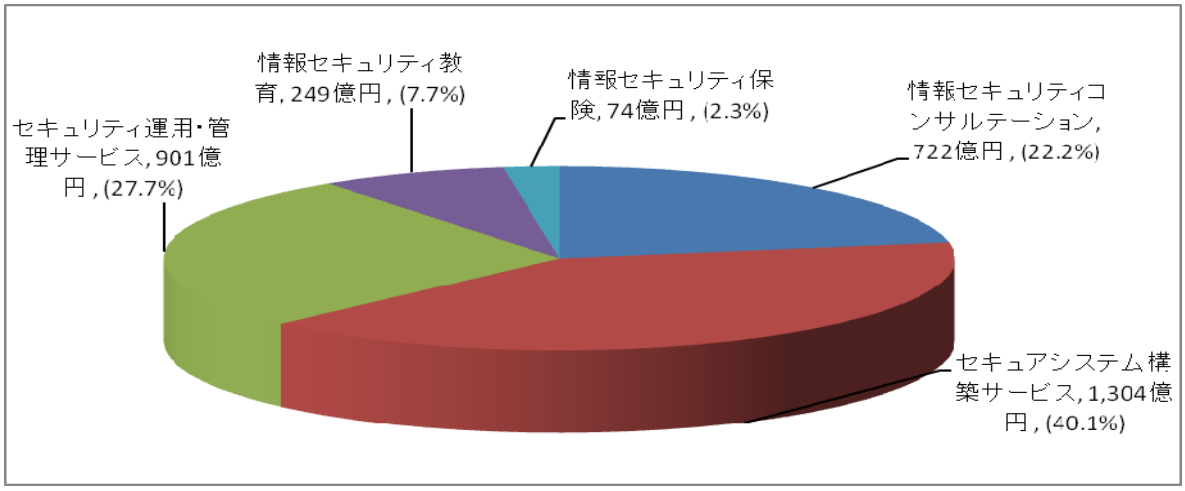
2010 年度以降についても、主として「情報セキュリティコンサルテーション」「セキュアシステム構築サービス」が引き続き大きく落ち込むことから、2010 年度同マイナス 4.6%、2011 年度同マイナス 5.5%と市場の縮小が続くことになる。この二つのカテゴリの衰退は、どちらも情報セキュリティ対策の浸透が一巡したことによる構造的要因を背景としており、今後情報セキュリティサービス市場全体としては低成長軌道に移っていく可能性が強いことを示唆するものと考えら

れる。また、システム構築において当初から情報セキュリティ対策が設計に組み込まれることから、「セキュアシステム構築」を別立てで取引を行う要素が減少していることによって、構造的に最大カテゴリである「セキュアシステム構築サービス」の市場規模が縮小に向かうこともこの傾向に拍車をかけることになると想定される。

図 14 に 2009 年度の国内情報セキュリティサービス市場のカテゴリ別分布を示す。また図 15 は国内情報セキュリティサービス市場の経年推移を表した図である。

「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、2009 年度実績推定値で 1,304 億円と、情報セキュリティサービス市場全体の 40.1%を占めた。このカテゴリは、IT システムに対してセキュリティ機能を設計・導入・構築するサービスである。システムインテグレーションに際してセキュリティ機能を組み込む部分のサービスや、既存の IT システムに対してセキュリティ機能を付加したり強化したりするために、IT セキュリティシステムを設計･製品導入･構築するサービスが中心となる。システムインテグレーション的要素が強いために、市場規模も大きなものになっている。

**図 14　2009 年度の国内情報セキュリティサービス市場**




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、2009 年度実績は 901 億円と推定される。このカテゴリは、ネットワークセキュリティの監視や運用代行サービス（マネージドセキュリティサービスとも呼ばれる）、システムの弱点を専門技術で点検する脆弱性検査やインシデントへの対応を行うプロフェッショナルサービス、そして電子認証サービス等の専門的サービスで構成される。マネージドセキュリティサービスは、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い。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、以前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。この他、プロフェッショナルサービスの一種には、リ

アルタイムのネットワーク監視まではしなくても定期的にログ解析を行ってネットワークの状態を把握し必要な助言をするといったサービスもある。また、電子認証サービスは、サーバ、システムの利用者個人、文書、時刻等の証明に必要な電子証明書を発行するサービスで、内部統制対応や電子商取引の活発化に伴って需要が拡大している。

「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展開していた。その主要顧客は経営の IT への依存度が高いか、セキュリティに対する意識の高い一部企業、あるいはネットワーク管理と一括でアウトソースするようなケースに限られてきたと言える。それが 2000 年代半ば頃から複雑化するネットワーク、高度化し頻度が高まる攻撃、特に電子商取引サイトへの攻撃やそれによる被害の深刻化等を背景に、専門サービスに対してアウトソーシングの形で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、ベンダから提供される監視サービス等が、競争にさらされる中でサービス品質が高まると共に価格も相当程度低下が進み、ユーザにとっては導入しやすくなってきている。また、深刻な情報セキュリティインシデントが多発する中で、対策のために専門家によるサービスが必要であるとの認識も浸透しつつあるように見える。このような背景から、ここ数年成長の度を速めているものと見られる。

金額規模では情報セキュリティサービス市場の中で 3 番目に位置するのが「情報セキュリティコンサルテーション」である。特に「情報セキュリティ管理全般のコンサルテーション」、「情報セキュリティ関連規格認証取得支援サービス」、「情報セキュリティ診断・監査サービス」、等、情報セキュリティの技術的側面よりは、経営管理の視点から専門家の支援を活用する動きが大きくなっている。ツールのようにハードウェアのためのコストがかからず、SI のように工数も大きくなりにくいために、大企業が全社的対策を一気に進める場合等を除き、案件当たりの金額はそれほど大きくならない。経営コンサルに近いところに位置するので、会計監査法人系、SI 系、独立系等多様な事業者がサービスを提供している。

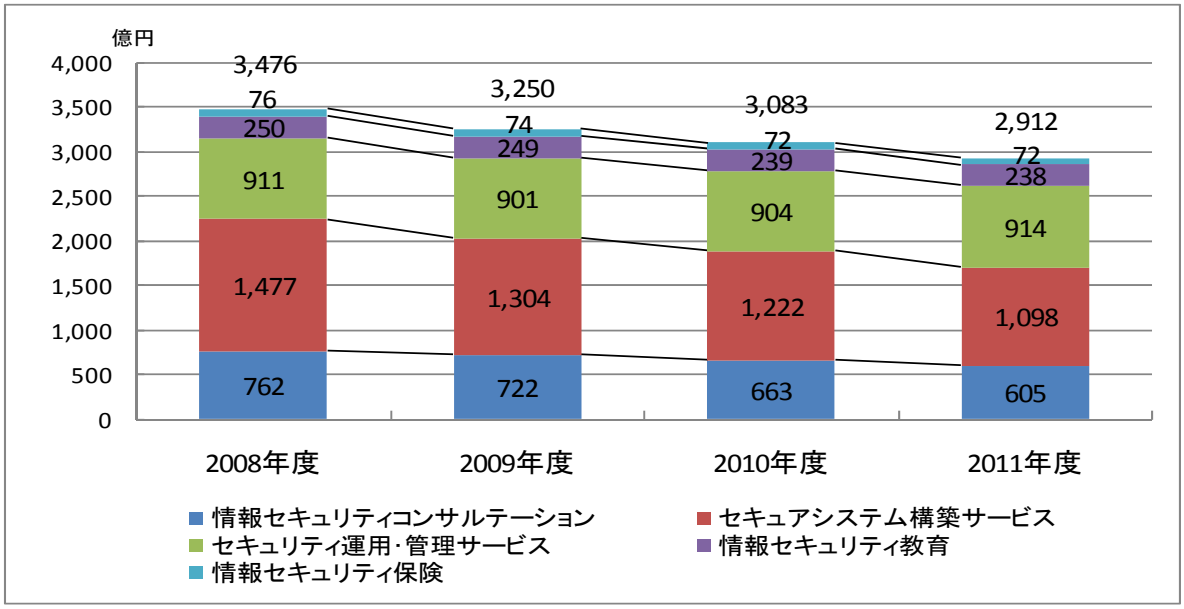
かつて「情報セキュリティコンサルテーション」の需要が拡大した要因としては、2005 年 4 月から全面施行された個人情報保護法と、2008 年 4 月以降に開始する会計年度から適用された内部統制報告制度、更には新潟県中越・中越沖地震や新型インフルエンザ等のパンデミック対策を契機とした事業継続計画への関心の高まりが挙げられる。プライバシーマーク認定や ISMS 認証の取得に取り組むケースも増え、その取得支援サービスや、認証サービスの需要が高まった時期があった。内部統制対応では内部統制管理の仕組みや IT カバナンス構築に際してコンサルティング需要が急拡大した。事業継続管理の国際標準制定の動きも後押しをしている。一方、上述のように対策の浸透や体制構築の一巡から、市場の成長には急ブレーキがかかり出した面もある。その結果、2009 年度の「情報セキュリティコンサルテーション」市場は前年度比 5.3%減の 722 億円にとどまったと見られる。

「情報セキュリティ教育」は 2009 年度実績推定値が 249 億円で前年度比成長率はマイナス 0.4%と、情報セキュリティサービス市場の中では軽微な縮小に留まり、構成比も 7.7%と前年度より 0.5%ポイント拡大した。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、一般社員等のユーザにも理解させる必要があることに対する認識が十分でなかった。それに対し、従業員の故意、ミス、不作為、無知等を直接間接の原因とする情報の盗難、紛失、漏えい事故が後を絶たないことから、従業員の知識と意識の底上げが必須であるとの認識が広がってきた。またウイルスやマルウェアの被害を防ぐには脆弱性の理解と対応を各ユーザに知らせる必要も強まっている。このような理由で教育ニーズが高まり、それに対応して教育コンテンツとサービスの提供も活発化していた。その結果、市場の縮小は軽微に抑えられたが、一般論的に経費節減のターゲットの一つとされる教育投資も、経済環境悪化の影響を免れることはできなかった模様である。

**図 15　国内情報セキュリティサービス市場推移**




情報セキュリティ保険は 1 カテゴリ 1 セグメントで市場区分のバリエーションはないが、情報セキュリティ対策と歩みを同じくして拡大してきた市場である。特に、情報セキュリティ対策が経営課題であるとの認識が浸透しだした 21 世紀以降は、市場への定着と需要の裾野の拡大が進んだと見られる。市場規模は、2008 年度で 76 億円であったが、2009 年度には 74 億円へと若干縮小している。その後もやや縮小気味の横ばいで推移するものと予測される。

### 2.2.2.　情報セキュリティサービス市場のカテゴリ別分析

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

#### 2.2.2.1.　情報セキュリティコンサルテーション市場

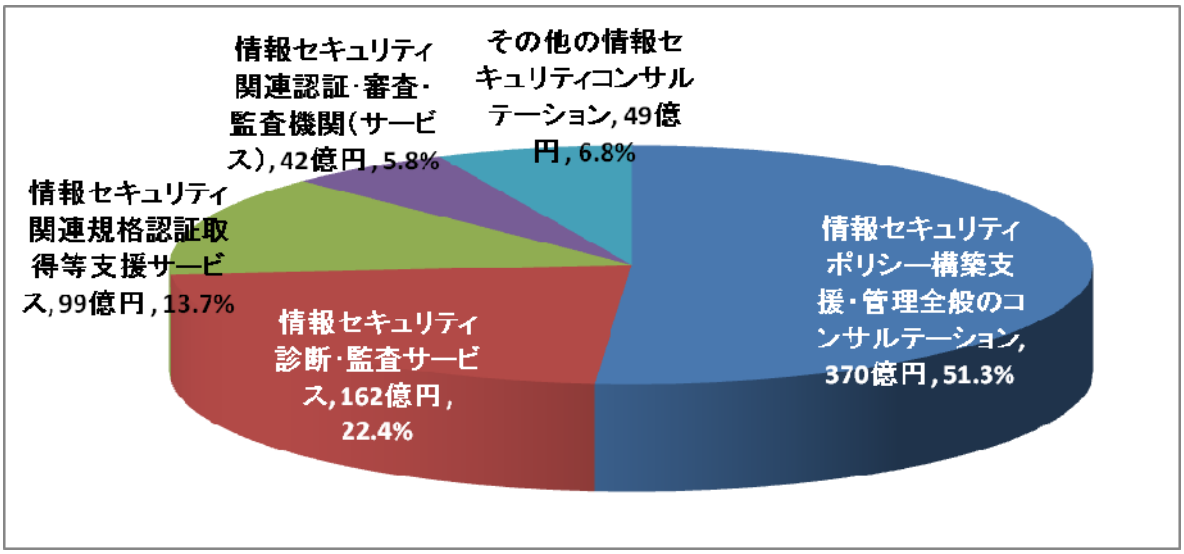
(1)市場の動向

図 16 に、2009 年度における情報セキュリティコンサルテーション市場のセグメント別市場分布を示す。

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

企業においては、経営リスクとしての情報セキュリティに対する認識が急速に進んでいる。内部統制報告制度への対応や個人情報保護法対応、知的財産の防衛、事業継続管理等の課題に直面しており、マネジメントの知識と IT 技術への理解の両面が要求されている。

**図 16　2009 年度の情報セキュリティコンサルテーション市場**




2008 年 4 月から適用開始された内部統制報告制度への対応の一環として、2006 年頃から IT 統制推進への動きが強まり、IT 統制を支える柱の一つである情報セキュリティのあり方も強く意識されるようになっている。IT 統制の考え方の中心はアクセス管理であり、また IT 上で処理される業務プロセスと会計プロセスのコンプライアンス確保と記録の保全、追跡可能性が問われることになる。これらは全て情報セキュリティの確立によって実現される。このことが、アクセス管理、ポリシー管理、ログの保全といった情報セキュリティ需要を押し上げ、またその導入・実現のための情報セキュリティコンサルテーションの需要を押し上げている。内部統制監査の大きな部分を IT 統制監査が占めることから情報セキュリティ監査にも関心が強まっている。

2005 年 4 月から個人情報保護法が全面的に施行されたが、これが引き金となりその前後に ISMS 認証やプライバシーマーク付与認定の取得に取り組む企業が増加した。とりあえず規格の要求する形を取り急ぎ整えるという対応も多く見られたが、企業が情報セキュリティに正面から取り組むきっかけになったと言える。ISMS 認証取得企業数は JIPDEC 統計で 2011 年 7 月 8 日現在 3,833 件、プライバシーマーク認定取得企業数は 2011 年 7 月 12 日現在 12,164 社となっている。

ここ数年来相次ぐ個人情報漏えいや企業秘密の持出し・漏えい・紛失等の事件は、企業のガバナンスに対する社会の視線を厳しくしている。企業側はリスク管理の意識が高まり、情報セキュ

リティの強化が企業の社会的信頼度の向上につながるという認識に至るようになってきた。これがコーポレート・ガバナンスの一環としての情報セキュリティガバナンス確立への動きとなり、情報セキュリティコンサルテーションの需要を押し上げる要因になっていると言える。

その他、情報セキュリティそのものではないが関わりが深い規格として IT サービスマネジメントシステム（JISQ20000 規格）や事業継続マネジメントシステム（BS25999）の認証も同じく JIPDEC により開始されている。また、民間がイニシアティブを取って進めている基準としてクレジットカード情報の保護を目的とする PCI DSS や、決済アプリケーションの開発事業者向けの基準 PA-DSS といった基準も登場し注目を浴びている。更に事業継続管理によって災害等の不測事態から企業経営を守る思想も浸透してきた。

依然として厳しい経済状況が続いていることから、2009 年度の「情報セキュリティコンサルテーション」市場の成長率はマイナス 5.3%となり、2010 年度についてもマイナス 8.2%と低迷する見込みである。ただし 2011 年 3 月に発生した東日本大震災は事業継続管理の意味や必要性に対する認知を高める効果をもたらし、以降の事業活動に大きな影響を与えると予想される。

(2)市場規模とその推移

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

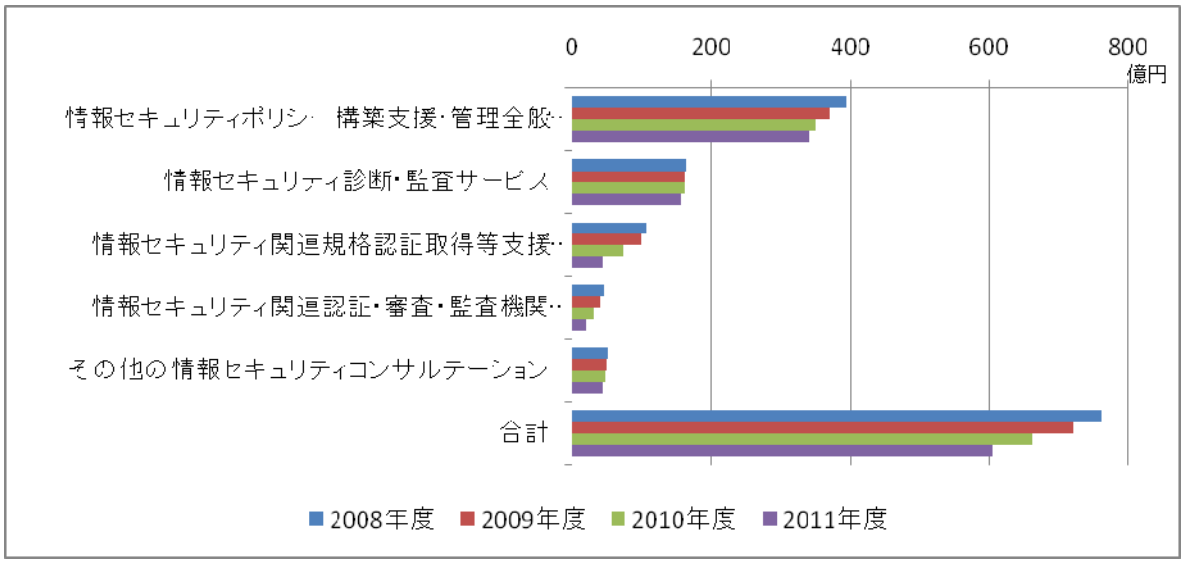
**表 10　国内情報セキュリティコンサルテーション市場規模　実績と予測**

| 市場規模(百万円) | 2008 年度 | 2009 年度 | 2010 年度 | 2011 年度 |
|---|---|---|---|---|
| 情報セキュリティポリシー構築支援・管理全般のコンサルテーション | 39,443 | 36,991 | 35,106 | 34,130 |
| 情報セキュリティ診断･監査サービス | 16,371 | 16,153 | 16,200 | 15,624 |
| 情報セキュリティ関連規格認証取得等支援サービス | 10,615 | 9,913 | 7,236 | 4,356 |
| 情報セキュリティ関連認証･審査･監査機関(サービス) | 4,599 | 4,167 | 3,003 | 1,933 |
| その他の情報セキュリティコンサルテーション | 5,179 | 4,942 | 4,710 | 4,501 |
| 合計 | 76,207 | 72,166 | 66,256 | 60,545 |
| **構成比** | | | | |
| 情報セキュリティポリシー構築支援・管理全般のコンサルテーション | 51.8% | 51.3% | 53.0% | 56.4% |
| 情報セキュリティ診断･監査サービス | 21.5% | 22.4% | 24.5% | 25.8% |
| 情報セキュリティ関連規格認証取得等支援サービス | 13.9% | 13.7% | 10.9% | 7.2% |
| 情報セキュリティ関連認証･審査･監査機関(サービス) | 6.0% | 5.8% | 4.5% | 3.2% |
| その他の情報セキュリティコンサルテーション | 6.8% | 6.8% | 7.1% | 7.4% |
| 合計 | 100.0% | 100.0% | 100.0% | 100.0% |
| **対前年度比成長率** | | | | |
| 情報セキュリティポリシー構築支援・管理全般のコンサルテ | ー | −6.2% | −5.1% | −2.8% |

| | | | | |
|---|---|---|---|---|
| ーション | | | | |
| 情報セキュリティ診断･監査サービス | ― | −1.3% | 0.3% | −3.6% |
| 情報セキュリティ関連規格認証取得等支援サービス | ― | −6.6% | −27.0% | −39.8% |
| 情報セキュリティ関連認証･審査･監査機関（サービス） | ― | −9.4% | −27.9% | −35.6% |
| その他の情報セキュリティコンサルテーション | ― | −4.6% | −4.7% | −4.4% |
| 合計 | ― | −5.3% | −8.2% | −8.6% |

2009 年度においては、「情報セキュリティコンサルテーション」市場は全体で 722 億円程度となり、前年度比成長率はマイナス 5.3%であった。比較的規模の大きなセグメントは「情報セキュリティポリシー構築支援・管理全般のコンサルテーション」の 370 億円、「情報セキュリティ診断・監査サービス」の 162 億円の２つである。いずれのセグメントについても前年度と比べて成長率はマイナスとなっている。そのうち、「情報セキュリティ診断・監査サービス」は前年度比マイナス 1.3%と相対的に低い縮小率を示した。これは、上に見たように内部統制報告制度を中心とした諸法令・諸制度とそれへの対応を含めた企業のリスク管理対応の進展が需要を押し上げているものと見られる。2010 年度も引き続き不況の影響はコンサルティングにより強く表れ、「情報セキュリティ診断・監査サービス」のプラス 0.3%に対して「情報セキュリティポリシー構築支援・管理全般のコンサルテーション」はマイナス 5.1%となっている。

**図 17　国内情報セキュリティコンサルテーション市場推移**




2009 年度において、最も低い前年度比成長率を示したのは「情報セキュリティ関連認証･審査・監査機関（サービス）」のセグメントで、前年度比 9.4%減の 42 億円になった。2010 年度は更に 27.9%減で市場規模は 30 億円と縮小する。プライバシーマーク認定企業数は、2007 年度に約 2,100、2008 年度に約 1,000 増加[7]し、ISMS の認証取得登録数は 2007、2008 年度各々477、531 増加しているが、増加分イコール市場であり、増加のペースが落ちれば市場は縮小するという厳しい性格を持ったビジネスである。従って、新規取得意欲や取組余力がそがれる不況期には厳し

[7] 新規取得数から中止、取消しを差し引いた純増数

いものとなろう。これに対応して「情報セキュリティ関連規格認証取得等支援サービス」市場も2009 年度 99 億円（前年度比成長率マイナス 6.6%）、2010 年度 72 億円（同マイナス 27.0%）と縮小している。

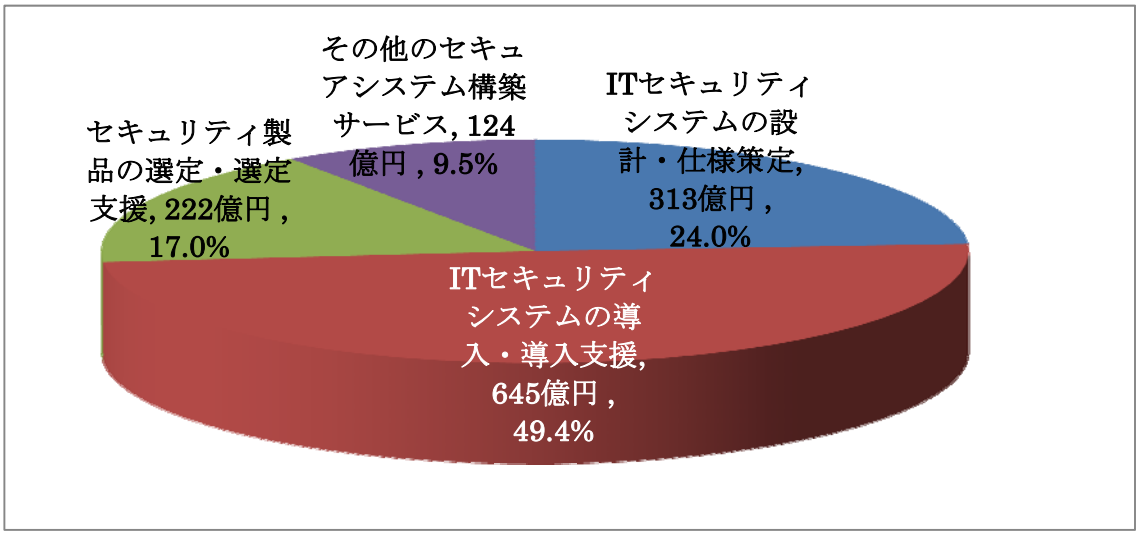
「情報セキュリティコンサルテーション」市場全体として、2010 年度はマイナス 8.2%と大きな落ち込みを見込む。内部統制対応が一段落し、体制や制度の整備への新たなニーズが後退することと企業の不況対策の影響を受けることによるものと考えられる。

#### 2.2.2.2. セキュアシステム構築サービス市場

(1)市場の動向

図 18 に 2009 年度のセキュアシステム構築サービス市場のセグメント別分布を示す。

**図 18　2009 年度のセキュアシステム構築サービス市場**




「セキュアシステム構築サービス」は、セキュリティ製品の導入や構築を含めた、IT セキュリティシステムまたは IT システムのセキュリティに関する構築、および構築を支援するサービスのカテゴリである。本カテゴリの市場規模は大きく、2009 年度で 1,304 億円と推定され、情報セキュリティサービス市場全体の 40.1%を占めており、セキュリティツールも含めた情報セキュリティ市場全体でも 2 番目のカテゴリを形成している。

「IT セキュリティの設計・仕様策定」は、セキュリティ専門家によるシステム設計・構築時の支援が必要であったが､昨今設計･仕様の策定時にセキュリティの要素も組み込まれて来ており、そのため個別に切り出した発注は減る傾向にあると観察される。「IT セキュリティシステムの導入・導入支援」においては、昨今の経済状況により情報セキュリティへの投資を抑える傾向にあり､支援範囲を極力抑えて自分達で導入する動きが見られ､発注額が減少していくと考えられる。これらの動向から市場規模は縮小する方向にあると言える。また市場は縮小傾向ではあるが、これはシステムにおけるセキュリティが認識されてきている裏付けとも捉える事ができるため、セキュリティのあるべき姿としては望ましい方向であると理解したい。

違う側面で、2009 年度は、国内事業者からも SaaS／PaaS やクラウド型のサービス提供やプ

ライベートクラウドの構築等の事例が増えてきた。SaaS／PaaS やクラウドの場合は、そのシステムを利用し早期に目的を実現できる点にユーザが有意性を見出していることもあり、セキュリティシステムの構築はサービス提供側がパッケージとして組み込んでいるケースが増えていると考えられる。このことも当市場が減少傾向を示す要因となっていると推測される。サービス提供側の課題の一つとしてサービス提供先のお客様がクレジットカード決済をとりいれている場合は PCI DSS への準拠も考慮する必要があり、この部分もパッケージとして組み込んでおく事がサービスの差別化として必要と言えるだろう。

プライベートクラウドの構築においてはシステム統合により全体コストを削減することをメリットとしているためセキュリティシステムに対してコストをかけないで構築する傾向にあると推測される。このことはセキュアシステム構築の発注が抑えられ一時的にコストを抑えられるが、構築後にセキュリティ対策を検討する事になり結局コスト高になる可能性がある。

また新規に対応・導入が必要となるセキュリティ技術に関する相談支援も必要となってくるであろう。「暗号危殆化に対する移行支援」「DNSSEC[8]」「IPv6」「DKIM[9]」等、まだ導入・運用ノウハウのない技術への対応は 2010 年頃から本格化し、当市場の需要に貢献することも期待される。

(2)市場規模とその推移

表11に国内セキュアシステム構築サービス市場規模の実績推定値と予測値を、図19にその市場規模の推移のグラフを示す。

「セキュアシステム構築サービス」市場は、2008 年度 1,476 億円、2009 年度 1,304 億円、2010 年度 1,222 億円、2011 年度 1,086 億円（予測）の規模と推測される。2008 年度の 1,400 億円台をピークに 2008 年度半ばから始まった経済不況の影響と市場の縮小傾向を受け 2009 年度には 1,300 億円台と急激な落ち込みを見せた。今後も縮小傾向にあると推測されるが情報セキュリティサービス市場内では依然として 4 割近くを占める大規模な市場である。市場の伸び率を見ると、2009 年度は経済情勢の急激な悪化の影響を受け前年比 マイナス 11.7%、2010 年度も前年比マイナス 6.3%と縮小のスピードは急である。

**表 11　国内セキュアシステム構築サービス市場規模　実績と予測**

| 市場規模（百万円） | 2008 年度 | 2009 年度 | 2010 年度 | 2011 年度 |
|---|---|---|---|---|
| IT セキュリティシステムの設計･仕様策定 | 34,772 | 31,273 | 29,222 | 23,522 |
| IT セキュリティシステムの導入･導入支援 | 74,313 | 64,491 | 60,052 | 54,376 |
| セキュリティ製品の選定･選定支援 | 24,352 | 22,233 | 21,339 | 19,751 |
| その他のセキュアシステム構築サービス | 14,242 | 12,428 | 11,593 | 10,909 |

[8] Domain Name System SECurity extension　DNS サーバが提供する IP アドレスとホスト名の対応付け情報を電子署名を用いて証明することで DNS キャッシュポイズニング等の成りすまし攻撃を防止する技術および機能

[9] Domain Keys Identified Mail 電子メールの送信元ドメインの実在と真正性を電子署名を用いて確認するための技術

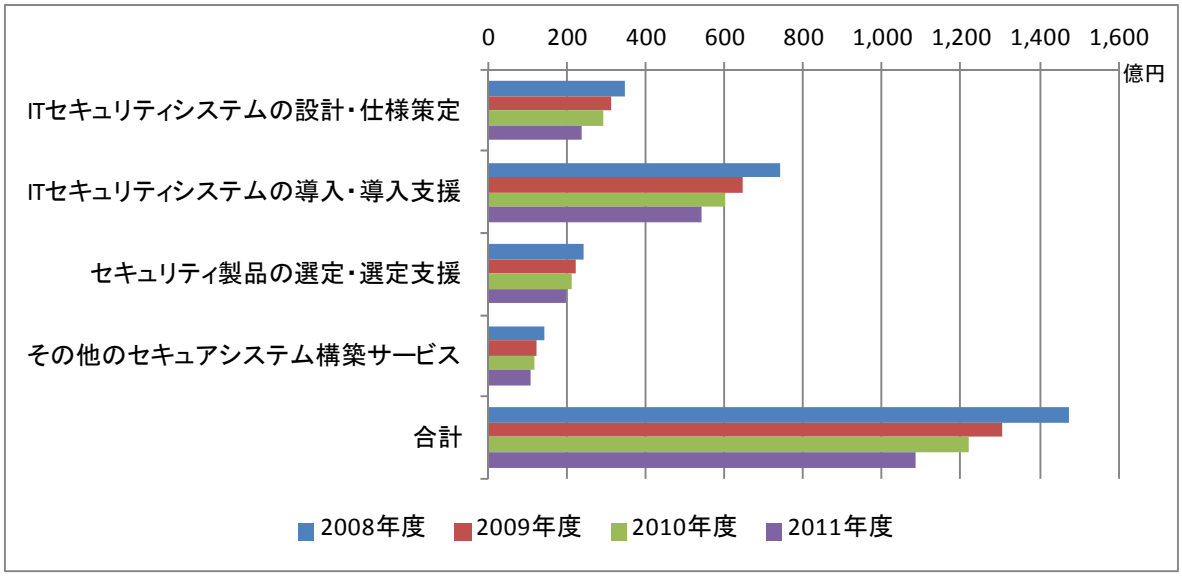

 

| | | | | |
|---|---|---|---|---|
| 合計 | 147,679 | 130,424 | 122,206 | 108,559 |
| **構成比** | | | | |
| IT セキュリティシステムの設計･仕様策定 | 23.5% | 24.0% | 23.9% | 21.7% |
| IT セキュリティシステムの導入･導入支援 | 50.3% | 49.4% | 49.1% | 50.1% |
| セキュリティ製品の選定･選定支援 | 16.5% | 17.0% | 17.5% | 18.2% |
| その他のセキュアシステム構築サービス | 9.6% | 9.5% | 9.5% | 10.0% |
| 合計 | 100.0% | 100.0% | 100.0% | 100.0% |
| **対前年度比成長率** | | | | |
| IT セキュリティシステムの設計･仕様策定 | ― | −10.1% | −6.6% | −19.5% |
| IT セキュリティシステムの導入･導入支援 | ― | −13.2% | −6.9% | −9.5% |
| セキュリティ製品の選定･選定支援 | ― | −8.7% | −4.0% | −7.4% |
| その他のセキュアシステム構築サービス | ― | −12.7% | −6.7% | −5.9% |
| 合計 | ― | −11.7% | −6.3% | −11.2% |

この中で「IT セキュリティシステムの設計・仕様策定」は、2009 年度が 312 億円で「セキュアシステム構築サービス」内の 24%を占めているが、「市場の動向」の項で見たように統計的には縮小傾向にあり 2010 年度は 292 億円で 2011 年度では 235 億円の見込みと縮小傾向が継続すると考えられる。

「IT セキュリティシステムの導入・導入支援」は 2009 年度が 644 億円で「セキュアシステム構築サービス」内では約 50%を占めるもっとも大きな市場ではあるが、縮小傾向は同じで 2010 年度は 600 億円であった。引き続きカテゴリ内の 50%程度を占める市場ではあるが、市場の動向でも記述したとおり拡大する要素があまりない状況と言える。

**図 19　国内セキュアシステム構築サービス市場推移**



### 2.2.2.3. セキュリティ運用・管理サービス市場

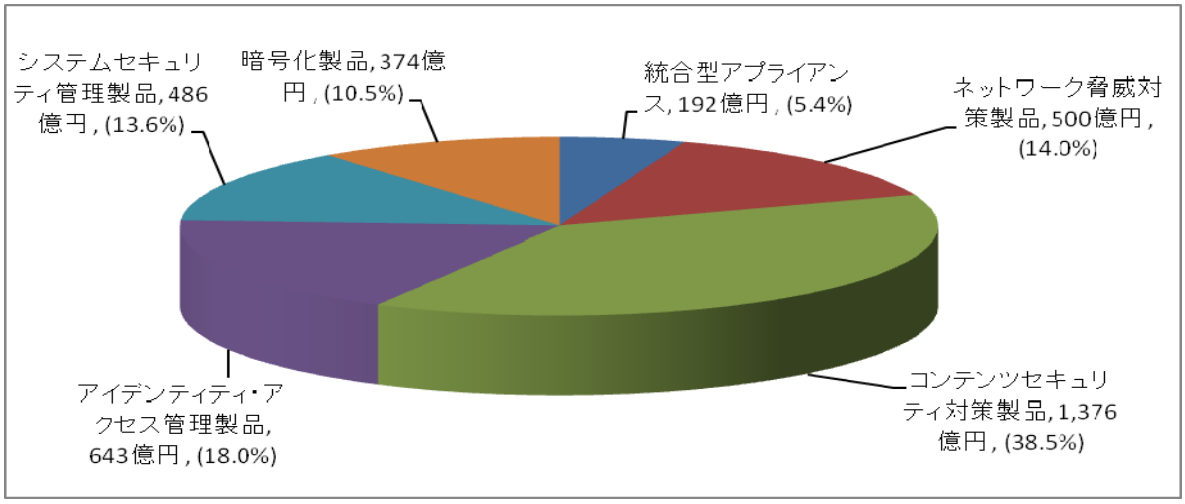
(1) 市場の動向

セキュリティ運用・管理サービス市場は、セキュリティ対応は適切な社外の専門サービス提供者に外部委託する必要があるというアウトソース需要によって支えられている。背景には、セキュリティ対策機器・サービス等の運用管理が専門家の知識を益々必要とする一方、そのような専門スキルを有する人材が利用組織内に不足していることや、問題発生時には 24 時間 365 日の迅速な対応が必要とされるケースが多いことがある。ネットワーク脅威の複雑化・深刻化と、セキュリティ対策が高度化・統合化に向う流れを背景に、この「セキュリティ運用・管理サービス」市場は中長期的に見て拡大基調にあると言える。しかしながら、2008 年度後半から急速に悪化した経済状勢の影響はこの分野においても著しく、2009 年度において多くのセグメントでマイナス成長となった模様である。2010 年度は経済情勢は引き続き厳しかったものの、当セグメントのような専門サービス領域は他の分野より早く持ち直しの動きが見られた。2011 年度にはその傾向が持続して若干ながらプラス成長になるものと見られる。年度当初に起きたソニーグループにおける世界規模での攻撃による情報漏えい事件、更には 2011 年 9 月に発覚した防衛産業へのサイバーアタックが企業等の認識を新たにし危機感を高めると考えられることも市場にとっては追い風要因となる。

図 20 に 2009 年度のセキュリティ運用・管理サービス市場のセグメント別分布を示す。

運用支援サービスについては、「ファイアウォール監視・運用支援サービス」と「IDS／IPS 監視・運用支援サービス」それに「ウイルス監視･ウイルス対策運用支援サービス」が各々の市場を形成している。また、それらの機能を統合化し総合的に監視・運用支援する「セキュリティ総合監視・運用支援サービス」も大きな市場となっている。ただしこの中で「ウイルス監視･ウイルス対策運用支援サービス」については例外であり、2008 年度以降ゆるやかなマイナス成長に転ずると予想されている。

**図 20　2009 年度のセキュリティ運用･管理サービス市場**




「脆弱性検査サービス」は、独自のセグメントと一定の市場を形成しており、需要は増加傾向

にある。近年では特に Web アプリケーションの脆弱性に関する関心が高まっている。検査サービスも、従来型の専門技術者が個別に手作業で実施する脆弱性診断サービスに加えて、既知の攻撃手法を自動化することでコストを大幅に抑えた ASP サービス等も登場してきており、需要のすそ野の拡大が期待される。また大手システムインテグレータでは、新規開発の Web アプリケーションを、カットオーバー・引渡し前に第三者に委託してテストすることも一般化しつつある模様で、この面からも当セグメントの成長が期待される。

「インシデント対応関連サービス」も情報セキュリティインシデントの増加とその対応需要の範囲の拡がり（緊急対応、復旧対応、デジタルフォレンジック対応等）に伴い、一定の市場規模に達している。

その他、ますます複雑化・高度化する各種インシデント・脆弱性・パッチ情報等に対応するための「セキュリティ情報提供サービス」についても、専門性の高いサービスとして、金額的には小規模ながら今後も一定の市場規模を維持するものと思われる。

このような外部からの攻撃対策や脆弱性対策とは異なり、積極的な本人・本物の認証対策や通信路の安全性確保対策として大きなサービスセグメントを形成しているのが、「電子認証サービス」である。従来のWebサーバやセキュリティ対策機器用の電子証明書に加え、ID・パスワードに代わるネット上での本人確認手段の高度化の手段として、また電子情報・電子文書の真正性確認の手段として、タイムスタンプを含めた各種電子認証サービスの利用が定着している。このセグメントは、電子署名法、e-文書法、また個人情報保護法等の法的要請への対応の拡がりを含め、その重要性の高まりと共に市場規模を拡大している。

(2)市場規模とその推移

表 12 にセキュリティ運用・管理サービス市場の実績推定値と予測値を示す。

「セキュリティ運用・管理サービス」の分野全体の市場規模は、2009 年度の実績推定値が 901 億円であり、2008 年度の 911 億円と比較すると 1.1%の減少となった。金額規模では、「情報セキュリティサービス市場」において「セキュアシステム構築サービス」に次ぐ位置を占めている。また、今回調査において、情報セキュリティサービス市場の中では唯一、2010 年度にプラス成長に転換し、2011 年度もプラス基調を維持するという予測結果となった。情報セキュリティ脅威の深刻化と複雑化に伴い、また経済の IT 依存度の上昇に伴い、専門家によるサービスである当市場は他のカテゴリに比べて安定的推移をたどるものと予測される。

**表 12　国内セキュリティ運用・管理サービス市場規模　実績と予測**

| 市場規模（百万円） | 2008 年度 | 2009 年度 | 2010 年度 | 2011 年度 |
|---|---|---|---|---|
| セキュリティ総合監視･運用支援サービス | 26,818 | 26,465 | 26,562 | 26,917 |
| ファイアウォール監視･運用支援サービス | 4,883 | 4,686 | 4,715 | 4,757 |
| IDS／IPS 監視･運用支援サービス | 6,314 | 6,189 | 6,212 | 6,231 |
| ウイルス監視･ウイルス対策運用支援サービス | 4,227 | 3,928 | 3,927 | 3,910 |
| フィルタリングサービス | 6,947 | 6,899 | 7,093 | 7,199 |
| 脆弱性検査サービス | 11,890 | 11,379 | 11,471 | 11,668 |

| | | | | |
|---|---|---|---|---|
| セキュリティ情報提供サービス | 1,775 | 1,733 | 1,709 | 1,718 |
| 電子認証サービス | 21,141 | 21,231 | 21,301 | 21,493 |
| インシデント対応関連サービス | 3,708 | 4,128 | 3,909 | 4,016 |
| その他の運用･管理サービス | 3,427 | 3,475 | 3,491 | 3,465 |
| 合計 | 91,129 | 90,113 | 90,389 | 91,375 |
| **構成比** | | | | |
| セキュリティ総合監視･運用支援サービス | 29.4% | 29.4% | 29.4% | 29.5% |
| ファイアウォール監視･運用支援サービス | 5.4% | 5.2% | 5.2% | 5.2% |
| IDS／IPS 監視･運用支援サービス | 6.9% | 6.9% | 6.9% | 6.8% |
| ウイルス監視･ウイルス対策運用支援サービス | 4.6% | 4.4% | 4.3% | 4.3% |
| フィルタリングサービス | 7.6% | 7.7% | 7.8% | 7.9% |
| 脆弱性検査サービス | 13.0% | 12.6% | 12.7% | 12.8% |
| セキュリティ情報提供サービス | 1.9% | 1.9% | 1.9% | 1.9% |
| 電子認証サービス | 23.2% | 23.6% | 23.6% | 23.5% |
| インシデント対応関連サービス | 4.1% | 4.6% | 4.3% | 4.4% |
| その他の運用･管理サービス | 3.8% | 3.9% | 3.9% | 3.8% |
| 合計 | 100.0% | 100.0% | 100.0% | 100.0% |
| 対前年度比成長率 | | | | |
| セキュリティ総合監視･運用支援サービス | ― | −1.3% | 0.4% | 1.3% |
| ファイアウォール監視･運用支援サービス | ― | −4.0% | 0.6% | 0.9% |
| IDS／IPS 監視･運用支援サービス | ― | −2.0% | 0.4% | 0.3% |
| ウイルス監視･ウイルス対策運用支援サービス | ― | −7.1% | 0.0% | −0.4% |
| フィルタリングサービス | ― | −0.7% | 2.8% | 1.5% |
| 脆弱性検査サービス | ― | −4.3% | 0.8% | 1.7% |
| セキュリティ情報提供サービス | ― | −2.3% | −1.4% | 0.5% |
| 電子認証サービス | ― | 0.4% | 0.3% | 0.9% |
| インシデント対応関連サービス | ― | 11.3% | −5.3% | 2.8% |
| その他の運用･管理サービス | ― | 1.4% | 0.5% | −0.7% |
| 合計 | ― | −1.1% | 0.3% | 1.1% |

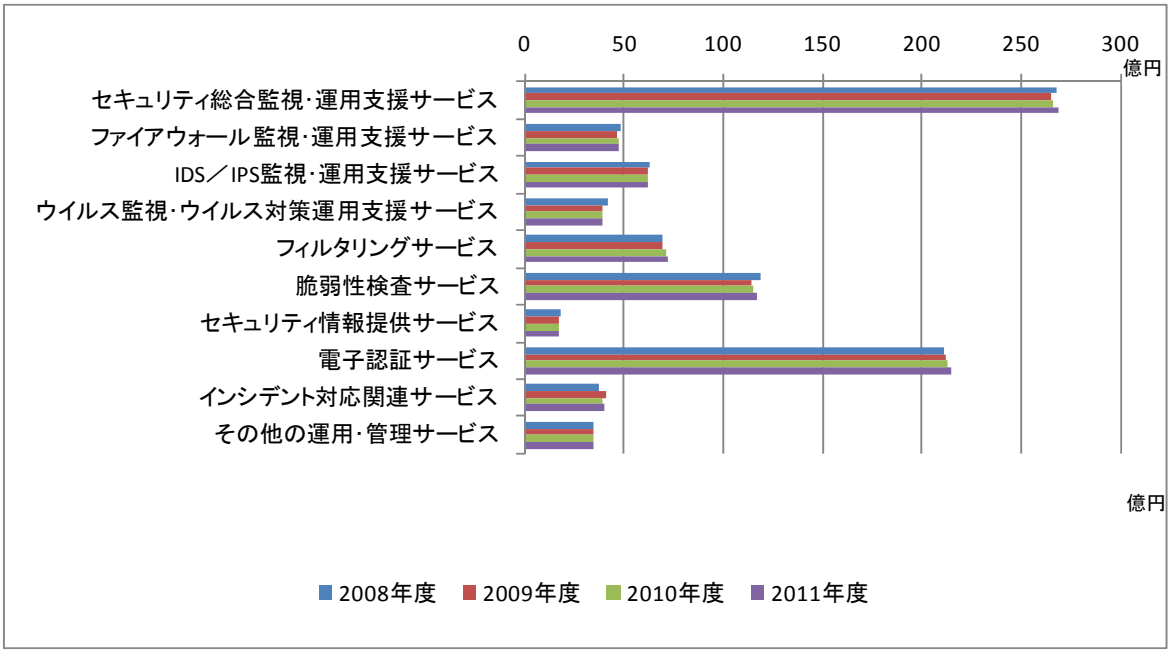
図 21 に国内セキュリティ運用・管理サービス市場規模の推移のグラフを示す。表 12 と合せてセグメント別の内訳を見ると、「セキュリティ総合監視・運用支援サービス」が最大のセグメントではあるものの、2009 年度の推定実績市場規模は 265 億円（前年度比成長率マイナス 1.3%）と、2008 年度の 268 億円から若干縮小した。2010 年度はわずかながらプラス成長に戻り、 2011 年度には 269 億円と、2008 年度並みに回復するものと予測される。

次に大きいセグメントは「電子認証サービス」で、2009 年度の推定実績市場規模は 212 億円

（前年度比成長率プラス 0.4%）と、かろうじてプラスの成長率を確保した。今後の市場規模は、2010 年度は 213 億円（同 0.3%）、20110 年度については 215 億円（同 0.9%）と、従来ほどの成長は見込めないながら、堅調に推移しそうである。

**図 21　国内セキュリティ運用・管理サービス市場推移**




個別機能のサービスである「ファイアウォール監視・運用支援サービス」、および「IDS／IPS 監視・運用支援サービス」の実績市場規模推定値は 2009 年度で各々47 億円（前年度比成長率マイナス 4.0%）、62 億円（同マイナス 2.0%）と、他の監視サービス同様マイナス成長となったが、2010 年度にはそれぞれ 47 億円（同プラス 0.6%）、62 億円（同プラス 0.4%）とプラス成長を回復し、2011 年度にはそれぞれ 48 億円（同プラス 0.9%）、62 億円（同プラス 0.3%）と、微増の趨勢を維持する見込みである。同じく個別機能のサービスである「ウイルス監視・ウイルス対策運用支援サービス」については 2009 年度 39 億円（同マイナス 7.1%）と大幅なマイナス成長となった。ウイルスの感染経路が複雑化し、ゲートウェイでのパターンマッチングによる監視では十分な防御が困難になってきたことの反映とも考えられる。今後も、2010 年度は 39 億円（同マイナス 0.0%）とほぼ横ばいだが、2011 年度は 39 億円（同マイナス 0.4%）と他の部門が微増に転ずる中、減少を続けるものと予想される。

近年特に多様化・複雑化する脆弱性やインシデント対応に向けた専門性の高いサービスの需要拡大を受けて、際立った増加傾向を示しているセグメントが「脆弱性検査サービス」であるが、2009 年度においては 114 億円（同マイナス 4.3%）とやや大幅な落込みを見せた。経費節減に対応して、検査のインターバルを延ばしたり対象範囲を絞り込むといった節減策が行われた結果ではないかと推測される。しかし、2010 年度には 115 億円（同プラス 0.8%）、2011 年度には 117 億円（同 1.7%）と、セキュリティ総合監視・運用サービス並の成長ペースに回復する見込みである。

「インシデント対応関連サービス」については、比較的小さい市場規模であるためにインシデントの発生頻度や個々のインシデントの規模によって市場規模の伸縮が影響を受ける傾向がある。2009 年度は 41 億円（同 11.3%）と例外的に高い伸びを見せた一方、2010 年度は同マイナス 5.3%で 39 億円となり、2011 年度には 2.8%伸びて 40 億円と予想される等、市場の浮沈の波は他のセグメントに比べてやや荒い。一方「セキュリティ情報提供サービス」については、2009 年度で 17.3 億円（同マイナス 2.3%）と限定的な市場である。2010 年度も同マイナス 1.4%といっても金額では 17 億円台は変わらず、2011 年度も金額は横ばい、伸び率はプラス 0.5%という推移をたどると予測される。

#### 2.2.2.4. 情報セキュリティ教育市場

(1) 市場動向

図22に2009年度の情報セキュリティ教育市場のセグメント別分布を示す。

2008 年 9 月のリーマンショック以降、世界的な経済危機と不況の影響によって、不況時の企業コスト抑制姿勢から、3K（交際費・会議費、交通費、教育・研修費）のひとつである教育・研修費用は削減傾向にあり、教育市場全体として縮小傾向にある。その中で情報セキュリティに関する教育の必要に対する認識は高まっており、情報セキュリティに関する教育は堅持される傾向にあると推測される。

情報セキュリティ教育の対象者と教育内容には以下のような組合せがある。①新入社員を含む全社員、全階層を対象とする、知的財産・顧客情報保護等の漏えい・紛失のリスクとその防止策としての情報セキュリティリテラシ教育や基礎的コンプライアンス教育、②情報セキュリティ対策部門、情報システム管理部門、システム開発部門、システム構築・運用部門等の部署が対象となる情報セキュリティ技術者向けには、アイデンティティ管理、アクセス管理等の内部管理と、脆弱性対策、ハッキング対策、セキュアアプリケーション開発等の外部脅威対策に関する知識・スキル教育、③最高情報責任者 Chief Information Officer (CIO)、最高セキュリティ責任者 Chief Security Officer (CSO)をはじめとする上級管理職を対象とする、情報セキュリティの共通知識分野（リスクマネジメント、アクセス制御、通信・ネットワークセキュリティ、事業継続と災害復旧計画等）に関しての経営視点からの高度な知識教育。このように情報セキュリティ教育は多岐にわたり、専門知識を必要とするものが多く、専門家によるサービスの需要を形成している。

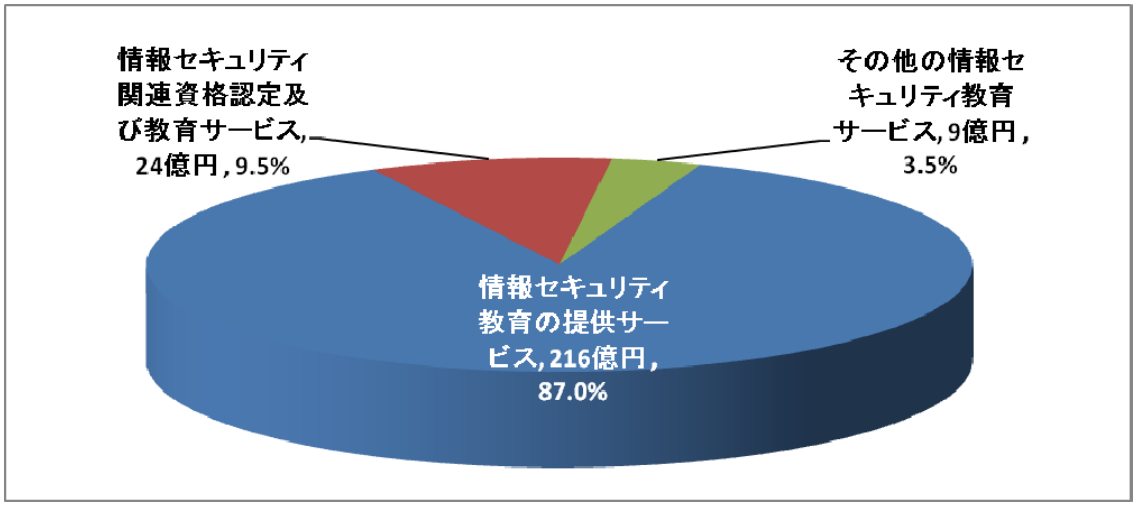
ただし、経済環境が厳しい中で経費削減を求められるところから、従来専門家のノウハウを取り入れるために外部委託していたものを、一部内製に切り替えるとか、対象を絞って実施するといった経費節減策の影響は市場に反映していると考えられる。

e - ラーニングサービスは、今年度から「情報セキュリティ教育の提供サービス」に含めているが、集合研修よりも費用を抑えるメリットが高く、教育・研修費の削減傾向が利用拡大につながっている。特に大企業を中心に、新入社員研修をはじめとして全社員を対象にしたコンプライアンス研修等に導入が進んでいる。ワンオンワントレーニング的利用による個別指導に近い効果も得られることから、集合教育以上の効果が期待できる。また、SaaS モデルによる低価格も期待でき、中堅・中小企業においても e - ラーニングサービスの活用が容易になることから、利用者

拡大の傾向にあると言える。

**図 22　2009 年度の情報セキュリティ教育サービス市場**




「情報セキュリティ関連資格認定および教育サービス」市場は、対象者が資格取得を目的とする者に特定されるため小規模な市場であると考えられてきた。しかし、企業においては情報セキュリティ対策に従事する技術者に対しては、そのスキルレベルの確認手段としてグローバルな「世界標準の情報セキュリティ資格」を活用する機運が生まれてきている。そのため対象者には資格取得を奨励して費用面の会社負担やインセンティブを提供するほか、一部企業では中途採用に際して有資格者を採用基準あるいは優遇基準とするところもある。このような動きを背景に、企業の指示によるものや、自らのキャリアパスのために個人の負担で資格に挑戦する受講者も増えている。2008 年度まではこのような循環により、情報セキュリティ関連の資格に関する教育や資格認定の市場は拡大傾向にあったが、企業の経費節減対策の一環で資格取得補助やインセンティブが後退し、個人においても収入が減少する中で自己投資も縮小傾向にあることから、急速に市場が収縮している模様である。

(2)　市場規模とその推移

表 13 に国内情報セキュリティ教育市場規模の実績推定値と予測値を、図 23 にその市場規模の推移のグラフを示す。

「情報セキュリティ教育」カテゴリは、情報セキュリティサービス全体の市場に占める割合が 8%弱程度と比較的小さい市場であり、2008 年度の市場規模は 250 億円程度と推測される。2009 年度の市場の縮小度合いは比較的軽微で、マイナス幅は 0.4%にとどまり、市場規模は 249 億円であった。2010 年度は経費節減のしわ寄せを受けたと見られ、前年度比伸び率マイナス 4.0%で 239 億円となった。2011 年度も回復は厳しく、マイナス 0.2%とわずかながら縮小して 238 億円程度の規模にとどまると予測される。

このカテゴリの最大のセグメントは87%を占める「情報セキュリティ教育の提供サービス」で

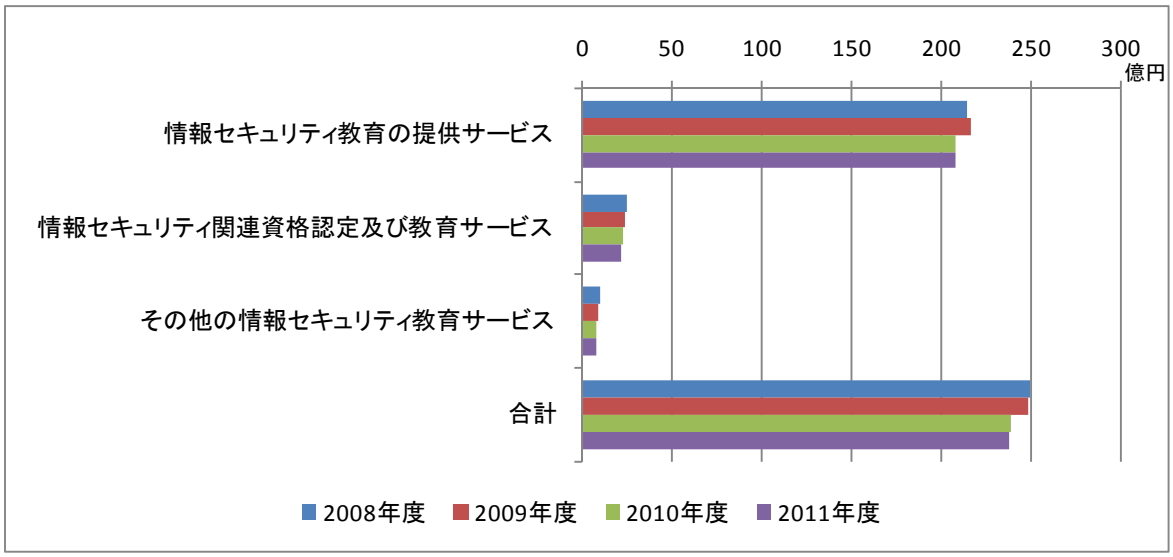
ある。今年度調査では、前年度まで別セグメントとしていた「情報セキュリティ教育のe-ラーニングサービス」を当セグメントに統合した。市場規模は2008年度に215億円、2009年度には216億円（前年度比成長率0.8%）と若干拡大したが　2010年度には失速して前年度比3.9%減の208億円となったと見られる。2011年度はほぼ横ばいで208億円弱になると予測される。

**表 13　国内情報セキュリティ教育市場規模　実績と予測**

| 市場規模(百万円) | 2008 年度 | 2009 年度 | 2010 年度 | 2011 年度 |
|---|---|---|---|---|
| 情報セキュリティ教育の提供サービス | 21,479 | 21,646 | 20,807 | 20,798 |
| 情報セキュリティ関連資格認定および教育サービス | 2,478 | 2,357 | 2,254 | 2,219 |
| その他の情報セキュリティ教育サービス | 1,024 | 880 | 838 | 825 |
| 合計 | 24,981 | 24,884 | 23,900 | 23,841 |
| **構成比** | | | | |
| 情報セキュリティ教育の提供サービス | 86.0% | 87.0% | 87.1% | 87.2% |
| 情報セキュリティ関連資格認定および教育サービス | 9.9% | 9.5% | 9.4% | 9.3% |
| その他の情報セキュリティ教育サービス | 4.1% | 3.5% | 3.5% | 3.5% |
| 合計 | 100.0% | 100.0% | 100.0% | 100.0% |
| **対前年度比成長率** | | | | |
| 情報セキュリティ教育の提供サービス | ― | 0.8% | −3.9% | 0.0% |
| 情報セキュリティ関連資格認定および教育サービス | ― | −4.9% | −4.4% | −1.6% |
| その他の情報セキュリティ教育サービス | ― | −14.1% | −4.8% | −1.6% |
| 合計 | ― | −0.4% | −4.0% | −0.2% |

この市場は上記に見たように、社員教育を外部委託する動きを背景に拡大してきた。社員全員に対して情報セキュリティに対するリテラシを植え付けて、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するという構造がある。しかし、2009年度は不況の影響により各企業が教育への予算の削減、縮小を行うため足踏み状態となり、2010年度はその延長でマイナス成長となったと見ている。

**図 23　国内情報セキュリティ教育市場推移**




「情報セキュリティ資格認定および教育サービス」は2008年度において25億円のマーケットであったが、2009度には前年度比4.9%減の24億円弱の規模になったと推測される。2010年度もその傾向は続き同4.4%減の23億円、2011年度には238億円（前年度比成長率マイナス1.6%）と、ここ当分縮小傾向が続くとの予測となった。上述のように企業の経費節減と個人の投資縮小の両面から影響を受ける。一方、定年を迎える団塊世代が第二の人生の武器として資格取得に取り組む傾向も報告されており、市場縮小を緩和する要因になっている可能性がある。なお、「その他情報セキュリティ教育」はセキュリティ対策機器等の導入・設定・保守のための教育が機器等の落ち込みもあって低迷したことで、特に2009年度に急速な縮小になったものと推測される。

### 2.2.2.5. 情報セキュリティ保険市場

(1)市場の動向

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

情報セキュリティ保険の市場としては、通信事業者、金融業や通信販売、小売業のような個人情報を多量に扱う業態、更に一般事業法人等多岐にわたる。販売チャネルも一般の保険販売ルートの他、ネットワークセキュリティ対策製品とのバンドル販売も行われている。また、保険料の算定に際しても、例えば ISMS 認証取得企業の料率が優遇される等、情報セキュリティ対策との組合せによるバリエーションがあるのも特徴と言える。

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

これら保険商品が、さまざまな販売チャネルを通じてエンドユーザに提供される。損保本来の代理店チャネルの他に、電機や事務機器の販売代理店等もある。特にパソコンや複合機の販売店は、IT の販売と同時にセキュリティ対策についても助言や支援を求められるケースが増えているとみられ、対策手段の一つとして保険の提供も行うようになっている。逆に保険の代理店が情報セキュリティ保険の営業過程で情報セキュリティに関するコンサルテーションを提供するケースもある。

(2)市場規模とその推移

表 14 に国内情報セキュリティ保険市場規模の実績推定値と予測値を、図 24 にその市場規模の推移のグラフを示す。

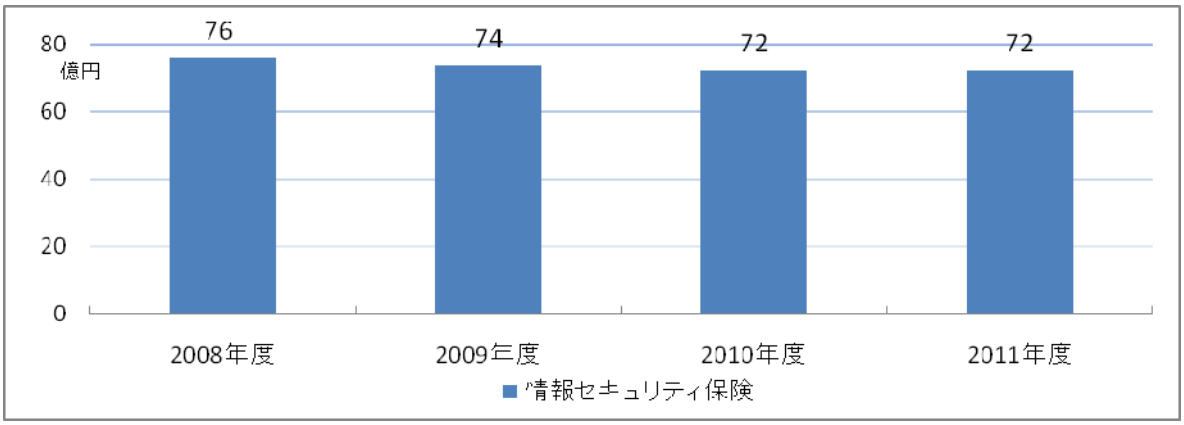
**表 14　国内情報セキュリティ保険市場規模　実績と予測**

| 市場規模（百万円） | 2008 年度 | 2009 年度 | 2010 年度 | 2011 年度 |
|---|---|---|---|---|
| 情報セキュリティ保険 | 7,591 | 7,377 | 7,234 | 7,244 |
| 対前年比成長率（%） | ― | −2.8% | −1.9% | 0.1% |

「情報セキュリティ保険」市場は、2006 年度に急拡大して 70 億円規模に達した後は落ち着いた動きとなっていると考えられ、2009 年度の市場規模は 74 億円程度と見込まれる。その後は経済情勢の急変動や景気の停滞の中で余り大きな変化を見せず、漸減傾向をたどって 72 億円程度の規模で推移しているものと推測される。それでも 2008 年度は 76 億円弱の規模であったので、この 3 年間で 5%弱市場が縮小したことになる。

停滞する経済環境の下でも、情報セキュリティ対策の中でも最も後方での守りとなる情報セキュリティ保険への支出は維持される傾向にあるが、打ち続く不況の中で、じわじわと市場の縮小が進んでいる感じであると推察される。

**図 24　国内情報セキュリティ保険市場推移**



# 第３章 情報セキュリティにおける新しい課題と動き

## 3.1. 2009～10 年におけるネットワークの脅威の動向

IPA（独立行政法人情報処理推進機構）セキュリティセンター発行の「情報セキュリティ白書 2010」の第Ⅱ部「10 大脅威　あぶり出される組織の弱点！」[10]によると、2009 年の脅威の動向が以下の通り挙げられている。

第 1 位 変化を続けるウェブサイト改ざんの手口
第 2 位 アップデートしていないクライアントソフト
第 3 位 悪質なウイルスやボットの多目的化
第 4 位 対策をしていないサーバ製品の脆弱性
第 5 位 あわせて事後対応を！情報漏えい事件
第 6 位 被害に気づけない標的型攻撃
第 7 位 深刻な DDoS 攻撃
第 8 位 正規のアカウントを悪用される脅威
第 9 位 クラウド・コンピューティングのセキュリティ問題
第 10 位 インターネットインフラを支えるプロトコルの脆弱性

この資料の表題の通り、2009～10 年におけるネットワークの脅威は、組織活動に大きな影響を与えるものが顕著となっている。またこのような状況に伴って、事業活動の継続性に対する方策、具体的には事件・事故の発生を防ぐ為の事前対策や、事件・事故が発生した際の被害を最小化する為の事後対策といった活動を予め準備しておくことが強く求められるようになっている。

また、サイバー犯罪をはじめとするネットワークの脅威は、その目的も変化しており、手口の悪質化や巧妙化も進んでいる。警察庁発行の「警察白書」[11]が記載する統計によれば[12]、「不正アクセス行為の動機」として「不正に金を得るため」が年を追って件数、率とも増加し、2009 年度では 2,245 件、88.6%に達している。また、近年低下していた「顧客データの収集等情報を不正に入手するため」が徐々にではあるが増加傾向にあることも注目される。

2009～2010 年に特に目立ったネットワークの脅威として、ここでは、「ウェブサイト改ざん」を取り上げる。

［ウェブサイト改ざん］

ウェブサイトが改ざんされることで、そのウェブサイトを閲覧しただけでウイルスに感染したり他のウェブサイトへ誘導されたりするようなことがある。近年、大手企業や公共機関等のウェブサイトの改ざんが相次ぎ多くの一般利用者が影響を受けたことから、メディア等で大きく取り上げられることとなった。

ウェブサイトを改ざんする手法として 2009 年に広まったのがガンブラーである。ガンブラー

[10] http://www.ipa.go.jp/security/vuln/10threats2010.html
[11] http://www.npa.go.jp/hakusyo/h22/index.html
[12] http://www.npa.go.jp/hakusyo/h22/toukei/01/1-22.xls

の登場以前にも改ざん手法は存在したが、ガンブラーの手法はそれまでのものと異なる。それまでの手法がサーバの脆弱性を突いたものであったのに対し、ガンブラーの場合はウェブサイト管理者の FTP アカウント情報を盗用する。具体的には、既に改ざんされたウェブサイトを閲覧することで別のウェブサイトの管理者がウイルスに感染し、そのウイルスの働きによって自らが管理するウェブサイトの管理者アカウント情報等を抜き取られ、その情報が悪用されることで新たにウェブサイトが改ざんされる。このように、ガンブラーの被害は連鎖的に増えていくという特徴がある。

ガンブラーへの対処としては、まずは PC のソフトウェアを最新の状態にすること（OS であれば Windows Update の実行。その他、Adobe Reader や Flash Player 等についても同様）、およびセキュリティ対策ソフトを導入することである。その上で管理者アカウントの適切な管理やウェブサーバへの改ざん検知システムの導入を実施することが望まれる。

### 3.2. ソーシャル・ネットワーキングサービスの普及とセキュリティ課題

(1) ソーシャル・ネットワーキングサービスの概要

ソーシャル・ネットワーキングサービス（以下SNS）とは社会的、人的ネットワークをインターネット上で構築するサービスと定義される。趣味や嗜好、地域、出身校、勤務先等によって構築されている人的ネットワークをインターネット上で提供するサービスである。既に構築された人的ネットワーク（出身校等）を補間する形で運営されているものや、SNS上で新たに構築された人的ネットワーク等人と人との関係性を生み出す仕組みとなっている。関係性を深めたり、広げる仕組みとしては、お互い発信した情報を共有したり、発信された情報に対してコメントを追記する等SNS内でコミュニケーションが円滑になるような工夫がされていることが多い。発信する情報（コンテンツ）の種類としてはテキストや写真等の画像、動画等があり、企業や団体が活用することによって一つの媒体としてとらえることもできる。活用事例としては、実社会のグループやコミュニテイと連携する形でSNSの中に独自ページやグループを作成し、イベントの告知、集客、報告等リアルな活動の補助ツールとしても活用されている。また、公共に公開されたニュースの共有、プライベートな出来事等多種多様な情報を発信する場として利用されている。簡単に記事を投稿でき、コメント機能やトラックバック機能を提供するミニブログサービスも、人的ネットワークを構築する要素を持っていることからSNSの一種として考えられている。

日本国内で認知度が高い海外の主なSNSとしては 7 億人を超えるユーザを抱えるFacebookや、140文字のショートメッセージを発信共有するサービスTwitter、写真の共有に特化したサービスFlickr、ビジネスマン向けのサービスLinkedIn等がある。国内ではmixi、Gree、mobage等が利用者が多い。国内のサービスの特徴としてはPCからの接続より携帯電話やスマートフォンからの利用が多いことがあげられる。また特定の地域や趣向に特化したSNSも数多く存在している。この要因として、レンタルサーバーの低価格化やSNSサービスを提供するオープンソースプロダクト等がリリースされていること等により、参入の敷居が下がっていることが考えられる。

SNSの多くは無料で利用できるサービスとして提供されており、運営母体は広告収入や一部有料サービスの提供等で収益を上げている。世界では1990年代初頭頃から広まり、日本では2004

年頃から普及しはじめた。様々な種類のSNSがリリースされていると同時に、モバイル端末との連携を深め、利用者の数は拡大の一途をたどっている。普及と同時に様々なセキュリティ課題も顕在化してきた。

(2) ソーシャル・ネットワーキングサービスのセキュリティ課題

匿名（いわゆるハンドルネーム）で運用されるサービスと本名で運用されるサービスがある。それぞれの課題を整理する。匿名で運用されているサービスでは、別の人格を演出したりするユーザ（なりすまし）や反社会的な発言、事実と異なった情報を意図的に発信される等情報の信頼性が低下する傾向にある。また、本来機密扱いである情報等の流出経路となるケースがある。また、実名で運用されているサービスでは、出身地、出身校等詳細な個人情報を登録することができるようになっているため、公開範囲の設定等を適切に行う必要がある。子供の写真等が不特定多数に公開されている状況等が問題として指摘されている。

企業活動においては広報活動の一環で活用されることが多い。特に対象がコンシューマ向けのビジネスの場合はブランディング戦略の位置付けとして重要度は増している。企業活動の一環として活用が進む反面、業務中に個人的に SNS を利用して機密情報やそれに類する情報が流れてしまい、企業に大きな損害を与える事故も発生している。SNS を一つのメディアとして定義し社員の利用に際してガイドラインを策定し運用していく必要がある。

SNS がマルウェアの感染経路になる事例も発生している。SNS 利用時のマルウェア感染の典型例は Koobface で、Facebook を舞台に 2008 年から米国を中心に蔓延が報告されてきている。昨今日本でもスマートフォン等の携帯型情報端末や小型のノート PC 等のサービス・アプリが普及し SNS の利用が更に広がったことで、被害の報告が急増している。主に、詐欺行為による個人の財産を狙ったもの、破壊や迷惑により個人が困り社会が混乱することを狙った愉快犯的なもの、個人情報を盗み出し利益を得ようとするもの等がある。

また、被害者が知らずに加害者（新たな感染源）となってしまうケースが多いのが SNS 利用シーンでのマルウェア感染の特徴ともいえる。実名による情報交換が中心となるため、実際の知り合い等から送られてきた情報に対して、十分精査せずに勧められたアプリをインストールしたり、添付ファイルを開いたり、掲載されいてる URL へアクセスするする傾向が強いことに起因すると考えられる。今後利用者の増加に伴い、ますますサイバー攻撃者の標的となることが考えられ、SNS 利用に際してのセキュリティ脅威は広がっていく傾向にあると言える。

また、携帯やスマートフォン等を利用して、手軽に始められることから情報セキュリティへの意識が低いユーザに利用されているため、設定ミスや操作ミスにより写真データに組み込まれた位置情報から自宅の場所が特定されてしまう等の思わぬトラブルに発展するケースがある。またモラル上不適切な発言等をしてしまった場合、SNS に登録されている情報等を第三者によりネット上に公開、拡散されるという事故も発生している。そのため今後は SNS を利用する上でのリスクを認識してもらう活動や情報セキュリティへの意識向上等を積極的に行う必要がある。

（参考）SNS に関連した事故等の事例

| |
|---|
| 2008/12　Facebook 内でマルウェア「Koobface」が蔓延 |

| |
|---|
| 2010/11　尖閣諸島中国漁船衝突画像流出事件 |
| 2011/01　ホテルアルバイト店員による Twitter による発言が原因でホテル側謝罪 |
| 2011/04　電力会社社員による mixi 内での発言が原因で炎上、アカウント削除 |
| 2011/05　スポーツ用品メーカ社員、Twitter による発言が原因で退職 |

### 3.3. スマートフォンのセキュリティ

スマートフォンは PC と携帯電話の機能を兼ね備えた優れた携帯情報端末として、2009 年から驚異的に販売数量を伸ばしている。利用者の拡大、利用方法の多様化により、当初から想定されているセキュリティリスクで対策が不十分なもの、今後発生すると思われる想定外のリスク等について JNSA をはじめ企業・業界団体が協力し合い、リスクの洗い出しと対策の検討を開始している。

2011 年現在、スマートフォンをはじめとした携帯電話端末は、通話やメールの機能を主体とした従来の携帯電話に、PC のさまざまな機能が追加され、OS やハードウェアのオープン化が進んでいる。インターネットを利用するための付加機能が搭載され、これまで PC でしか利用できなかった膨大な数のアプリケーションが利用可能となり、利便性が劇的に向上した。この結果、スマートフォンで実現できることと、PC で実現できることの差は急速に埋まりつつある。

PC と比較して、スマートフォンは携帯性（モビリティ）が特徴であるため、PC で実現できなかったことを補完するデバイスとして、多くの企業・団体において、スマートフォンの業務利用が導入、あるいは検討されている。また、ユーザが個人所有のスマートフォンを組織内に持ち込み、使用する機会は今後ますます増加すると考えられる。

その一方でスマートフォンのセキュリティ脆弱性が完全に払拭されないまま市場に投入され、これにより、情報漏えい等のリスクや、望ましくない使われ方や想定外の事故の誘発といった事例が発生しはじめている。また、PC の脆弱性がスマートフォンに影響を及ぼすケースや、スマートフォンでは従来の PC セキュリティを適用できないケース等、課題は極めて多い。図 25 に、スマートフォンについて指摘されている脅威の分類と例を、㈱A3 セキュリティが行った整理を引用することにより示す。スマートフォンのセキュリティに関しては特に早急に業界団体の統一的なルール作りや利用環境でのリテラシ向上を目指した普及啓発活動等が必要となっている。

スマートフォンは高いモビリティがあるがゆえに先ず「紛失・盗難が起きやすい」という点が第一のリスクとして上げられる。その上、搭載されているメモリサイズが大容量で常に重要な個人情報やデータを保持しており、電源 Off 後にも記憶している情報が多い。このためこれまでの携帯電話以上に紛失・盗難による情報漏えいリスクが大きくなる。

また、スマートフォンは手軽に公衆無線 LAN に接続できる。このため、現在はまだ少ないがデータの盗み見や詐欺（フィッシング）・悪用等の危険性も高い。現状、マルウェアの出現頻度が低く、これらの対策やインシデント対応想定が難しいというのも不安を助長させる。様々なアプリケーションを手軽にインストールできるスマートフォンは、悪意を持った者たちに、個人を特定した情報の盗み出しを携帯電話よりも容易に行う機会を多く与えてしまう可能性も高くなり、今後、抜本的なセキュリティ対策がなされない限り、業務用としての利用には大幅な制限を設け

るしかない。すなわちスマートフォンを情報機器として見た場合、既存の携帯やパソコンよりもセキュリティ上、脆弱な要素・不透明な部分が多々あり、個人はもとより企業が業務で使うためのセキュリティ対策とガイドライン、それらに見合った運用が求められる。

以上の状況は見方を変えれば、セキュリティベンダにとってビジネスチャンスの到来であり、業界団体活動等を通じて日本の IT セキュリティの新たな事業推進の舞台になる可能性を秘めている。

**図 25　スマートフォンの脅威についての技術的分類**

（1）スマートフォン脅威

①プラットフォーム脅威
脅威：Android：Root 化、iPhone：JailBreak
リスク：他アプリのメモリアクセス、ファイルシステムアクセスによる情報漏洩

②デバイス脅威
脅威：盗難および紛失
リスク：スマートフォン内のデータ流出

③アプリ脅威
脅威：バイナリ逆分析およびデバッグによる分析
リスク：情報漏洩、不正課金発生、バッテリ低下、電話拒否など

④コンテンツ脅威
脅威：OS/アプリの脆弱性利用、
メール・SMS 経由での配布、市場での配布によるマルウェアと Phishing 攻撃
リスク：情報漏洩

⑤ネットワーク脅威
脅威： 脆弱なワイヤレス使用によるパケット分析
リスク：情報漏洩

⑥サービス脅威
脅威：スマートオフィスの場合、スマートフォン経由でのサーバへの攻撃
リスク：情報漏洩

（2）脅威コードの例（抜粋）

①個人情報漏洩関連脅威コードの例

| 区分 | 内容 |
|---|---|
| PBStealer | 端末の電話番号を外部端末に送信 |
| Infojack | 端末情報を送信 |
| iPhone/Privacy.A | ワイヤレス経由で個人情報送信 |
| Duh Worm | SMS 基盤認証コードを特定サーバに送信 |
| Jackeey Wallpaper | 端末内 メールアドレス、SMS メッセージ、電話番号を特定サーバに送信 |
| Christmas Wallpape | USIM 情報ハッキングによる証明書情報を特定サーバに送信 |

②デバイス関連脅威コードの例

| 区分 | 内容 |
|---|---|
| Skull | システムファイル変更により端末使用不可 |
| Bootton | 端末のアイコン変更によりアプリ使用禁止 |
| BlankFont | 端末のフォント使用不可 |
| Ikee | バックグラウンド画面を変更 |
| Liberty | 端末の てのアプリの削除 |

③不正課金関連脅威コードの例

| 区分 | 内容 |
|---|---|

| | |
|---|---|
| Mosquit | SMS 使用による課金発生 |
| CommWarrior | 端末に保存されている全てのアドレスに MMS 送信 |
| Timofonica | 任意の文字を SMS で送信 |
| RedBrowser | プレミアム文字メッセージを送信 |

（3）コンテンツ脅威とアプリ脅威の切り分け

| 脅威 | 対応技術 |
|---|---|
| プラットフォーム | ・プラットフォーム無欠性確保技術 |
| デバイス | ・認証技術<br>・デバイス管理機能<br>・遠隔操作技術 |
| アプリ | ・ソースコード内の重要文字列除去<br>・ファイル無欠性確保技術<br>・バイナリ無欠性確保技術 |
| コンテンツ | ・入力情報保護技術<br>・E2E 部分の保護技術<br>・市場側のマルウェア検知技術 |
| ネットワーク | ・送受信情報の暗号化技術<br>・不適切な AP は使用禁止 |
| サービス | ・重要情報のローカル保存禁止<br>・サーバ側の防御技術 |

（出典：㈱A3 セキュリティ）

### 3.4. 震災を経て変わるクラウドコンピューティングのセキュリティ課題評価

(1) 東日本大震災に際して提供された無償のクラウドサービス

クラウドコンピューティングは、国内市場においては、2010 年の各社からのサービスの一斉登場の段階を経て、2011 年度には一気に普及段階に突入したと見られる。国内の大手・中堅システムインテグレータやデータセンタ事業者は、ほぼ例外なくクラウドコンピューティングのメニューを品揃えし、競うようにその充実とサービスの拡充を図っている。提供される IaaS ホスティング基盤をインフラとして、第三者からの付加価値サービスも SaaS モデルで数多く提供される等、クラウドサービスの品揃えが急速に充実している。それを背景に、大手から中小まで、業務系から基幹系の一部まで、クラウドの活用は予想以上のスピードで進展していると見られる。[13]

そのような最中に、東日本大震災に遭遇することになった。クラウドの視点から注目すべきことは、発災直後から、多くのクラウドサービスプロバイダ（CSP）から、無償のクラウドサービスが提供されたことである。IPA の集計[14]によれば、その例は 4 類型 76 ケースに及んでいる。支援のパターンとしては、同発表によれば、①情報共有・流通基盤（P2P）（被災者・関係者間安否情報、物流向け道路情報、NPO 等支援者－被災者間情報流通・共有）②被災者救援活動の情報インフラ（被災者・避難所の状況把握、救援物資の集積・配布システム、ボランティア管理・派遣コントロール）③行政情報提供サイトの拡張（政府の情報サイトのミラー、自治体情報サイトのミラー、放射線モニタ情報提供）④被災企業等の緊急情報発信・業務処理（メールサーバの代

13 クラウドコンピューティングのセキュリティ課題に関する一般的考察は、JNSA による（経済産業省委託調査）2009 年度情報セキュリティ市場調査報告書で掲載済み。
http://www.meti.go.jp/policy/netsecurity/downloadfiles/21FY_ISmarket_research_report.pdf

14 http://www.ipa.go.jp/security/cloud/cloud_sinsai_R1.html

替、グループウェア・Web 会議等の提供、被災状況画像の発信、サーバ、ストレージ等の提供、業務アプリ等の提供）となっている。

(2) クラウドコンピューティングの社会インフラとしての有効性

このようなサービスは、最も早いものでは発災当日から部分的に提供開始されたものもあり、震災発生の金曜日から週末をはさんで翌週には相当数・種類のサービスが無償提供開始され、概ね 6 ヵ月程度継続された。このような動きの背景には、①パブリッククラウドがオンデマンドでサービス提供できる環境を予め備えていること、②IaaS をはじめ、Web ホスティング、グループウェア、オフィスツール等、様々な用途に柔軟に利用できるサービスが充実していてすぐ使える状態にあること、③CSP 各社にとって、サービス提供のための増分コストがほとんど発生しないため、容易に提供に踏み切れること、が上げられる。

これらは、クラウドコンピューティングのオンデマンド・セルフサービス、スケーラビリティ、アジリティといった特性が正に活かされたものと言える。クラウドはそのコンピューティング利用のパラダイムシフトだけでなく、緊急時に社会を支える基盤としての存在価値も示したと評価できる。

(3) 震災経験を経て変わった、クラウドコンピューティングのリスクに対する評価

更に、東日本大震災に際して、あるいはその後の計画停電や夏季の電力需要抑制策の下において、データセンタがほとんど全て、サービス停止や機能停止に陥らなかった、という事実が注目されている。震度 6 以上を記録した仙台市内のデータセンタも、主たる設備の倒壊や転倒もなく、ほとんど全てのサーバが機能を維持した。実際には通信回線がしばらくの間不通になったために、サービスの利用という点では中断があったが、供給側の能力は維持されたのである。停電による電源断に対しても、自家発電装置によるバックアップ、更にはそのための燃料補給の継続的サポートによって乗り切っている。

このことに対する認識が広まる中で、BCP をクラウドを活用して実現する、あるいは補完する、というニーズが急速に広まっている。従来のコンセプトは、以下のように変容を見せている。

① クラウドにデータを置くことは、データセンタのサービス停止のリスクがある、と考えられていたのが、オンプレミスよりも信頼性、耐障害性が格段に高い、という認識に変わった。

② クラウドにおけるストレージの信頼性は 100%ではないので、ローカルのバックアップやデータの二重化は不可欠である、との考えに対し、現実にはローカルバックアップが津波の被害に遭うとか、データセンタにあるデータは無事だったが、オンプレミスのサーバ上のデータは失われた、という経験があった。その結果、遠隔地のデータセンタ、ストレージの利用や、ローカルバックアップだけでなくクラウドにもバックアップを持つことのメリットを評価する方向に変わった。

③ データが海外に保管されることのリスクが大きく意識されていたが、東日本全域のように広範囲な被害の可能性を考えた場合、海外に予備を置くことの必要性も意識されだし

ている。現実に、シンガポールやオーストラリアのデータセンタの利用を検討する向きもあるとのことで、何がより差し迫ったリスクかの評価尺度に変化が見られる。

④ ライフラインの途絶や交通の麻痺、更には電力のピークデマンド抑制対応等で在宅勤務の有効性や必要性に対する認知が高まった。その結果、システムやデータをクラウド上に置き、リモートアクセスで業務継続する形態を積極的に導入したり検討したりする動きが出ている。その結果、スマートデバイスの業務利用の浸透や、アプリケーションサーバ環境をクラウド上に持つことを肯定する動きが広がっている。

このように、東日本大震災の経験を経て、クラウドコンピューティングは社会経済的価値の認識がより高まっている。更には震災からの復旧・復興に際しても、①初期投資負担の軽減　②システム立ち上げリードタイムの短縮　③運転保守負担の軽減からクラウドの活用が推奨[15]されており、クラウドの利用価値や社会的意義に対する認識が一層高まってきていると言える。

15　前掲 IPA のレポート　http://www.ipa.go.jp/security/cloud/cloud_sinsai_R1.html

## 第４章 2012 年の展望

この市場調査における市場規模の推計作業では、2012 年度については、当初の作業スコープに入れていなかった。が、2011 年度までの検証と報告書執筆に想定以上の時間を要した結果、公表時期が 2012 年度に近づいており、急遽 2012 年度についての概略の展望を追加することとした。

そのために、2011 年 12 月に、JNSA 会員に対して 2012 年度の事業成長度合いの見通しを聞くアンケート調査を実施し、その結果を元に、簡易的予測作業を行った。事業の成長度合いについては、以下の区分で回答を求めた。事業の種類により、また業態や業容の差により、回答は大幅悪化から大幅成長まで、多様であった。全体としては「ほぼ横ばい」や「やや拡大」が多く、マイナスよりはプラス成長を見込む意見の比率が高かった。

| 大幅悪化 | 後退 | 微減速 | ほぼ横ばい | やや拡大 | 成長 | 大幅成長 |
|---|---|---|---|---|---|---|
| −10%以上 | −10%未満～<br>−5%以上 | −5%未満～<br>−2%以上 | −2%未満～<br>+2%未満 | +5%未満～<br>+2%以上 | +10%未満～<br>+5%以上 | +10%以上 |

このアンケート結果を指数化して伸び率換算し、業態別強弱の要素も加味して市場規模の変化を予測した。市場規模の予測結果は、表 15 の通りである。このうち 2011 年度の数値は参考のための再掲である。

ツール市場は 2011 年度比 5.4%と高い伸びを示して 3,761 億円と、2008 年度を上回る規模まで回復する。サービス市場も同 3.9%の伸びを示して 3,028 億円にまで回復するが、まだ 2010 年度に届かない水準である。これは、情報セキュリティコンサルテーションとセキュアシステム構築サービスの 2009～2011 年度の落ち込みが大きかったことが影響している。これら市場も 2012 年度には回復する（特にセキュアシステム構築サービスは 5.0%と大きな伸びが見込まれる）が、まだ 2010 年度の数値には遠く及ばない。一方、セキュリティ運用・管理サービスと情報セキュリティ教育は、過去最高の金額規模（本調査ベース）に達するものと見られる。

このような結果となった背景はいくつか考えられる。経済状況は、欧州の信用不安がなかなか収束に向かう様子が見えないことで、それが途上国経済にも影響を与えだしていることから、マクロ経済的には不確定要素が依然強い。国内経済は、東日本大震災のダメージから、基幹産業は立ち直りを見せており、また個人消費も復興の兆しが見えることから、2012 年度への回復期待が高まっている。このようなことから、経済情勢としては、2010, 2011 年度よりは上向くとの期待があるものと思われる。

二つ目には、投資サイクルの循環が考えられる。2008 年度半ばのリーマンショック以降、企業は事業体質の一層のスリム化に取り組み、コスト削減と投資抑制を継続してきた。しかし、設備は一定のサイクルで更新期を迎え、更新することでより高い生産性や効率性を達成する必要もでてくる。IT は特に技術革新が早いことから新陳代謝のサイクルも短い。3 年間の抑制は、2012 年には更新サイクルを迎えるという期待を抱かせる。

これを後押しする要素として、新製品・新技術の登場と普及も注目すべきである。クラウドコンピューティングは、震災を契機にアウトソーシングの活用や BCP 対策としての有効性が注目

されて普及の速度を増していると見られる。またスマートデバイスの急速な浸透は、クラウドコンピューティングやモバイルワーキングの積極的取入れ（これも震災とそれに続く電力不足の副産物の側面がある）と相俟って、企業の IT 活用の姿を変え、IT の一層の浸透を後押ししている。「ビッグデータ」に対する注目、そこから新たな事業機会を引き出す取組みも追い風といえる。

更に企業を情報セキュリティ対策に注力させる要素として、2011 年度に多発した情報セキュリティインシデントの経験がある。ソニーの事件に見られるような一部ユーザの主義主張に基づく報復的企業攻撃、防衛産業への攻撃に見られる産業戦略または国家戦略を背景にした産業スパイ的攻撃、更に政府機関等に対する特定の意図を持った可能性を感じさせる攻撃、そして内部犯行による情報漏えい。これらから得られる教訓は、情報セキュリティインシデントは、もはや偶発的出来事ではなく、明確に意図を持って公然と仕掛けられる攻撃となってきたことである。一部個人が個人的目的で行うものと考えられていた時代には、攻撃に遭うことは偶発的事象に過ぎないとの評価もありえたが、いまや、どんな企業でも組織的・意図的攻撃を受ける可能性を実感せざるを得ない状況に至っている。このことは、企業・組織が本格的に、組織防衛・事業の保全のために情報セキュリティ対策に本腰を入れる環境が整ったことを意味する。これも、業界関係者が 2012 年度に需要拡大を期待する要因の一つと考えられる。

このような見方を裏付ける象徴的なデータとして、「セキュアシステム構築サービス」需要が大幅に高まるとする予測を寄せた回答者が多かったことが挙げられる。このカテゴリは、システム構築におけるセキュリティ要素の組込みが、企画段階から与件となり、独立の需要として外在化する要素が減ったことからここ数年趨勢的に市場規模を縮めてきた市場である。が、2012 年度は比較的高い伸びを期待するアンケート回答が多く、表 15 に見られるように 5.0%と高い市場の伸びが期待されている。投資サイクルの山や、企業が改めて本格的に対策を講じる動きに対する期待が、ここに表れているように感じられるのである。

2012 年度が、情報セキュリティ産業にとって、久しぶりにフォローの風が吹く年となることを期待したい。

表 15　2012 年度　国内情報セキュリティ市場規模予測

| 年度別売上高推計値 | 2011 年度 | | | 2012 年度 | | |
|---|---|---|---|---|---|---|
| セキュリティ･ツール | 売上高予測値 | | | 売上高予測値 | | |
| | 金額 | 構成比 | 前年比伸び率 | 金額 | 構成比 | 前年比伸び率 |
| 統合型アプライアンス | 18,703 | 5.2% | −1.4% | 19,645 | 5.2% | 5.0% |
| ファイウォール・アプライアンス／ソフトウェア | 19,233 | 39.6% | −1.2% | 19,686 | 39.1% | 2.4% |
| VPN アプライアンス／ソフトウェア | 10,520 | 21.7% | 4.5% | 10,846 | 21.5% | 3.1% |
| IDS／IPS アプライアンス／ソフトウェア | 11,248 | 23.2% | −1.4% | 11,758 | 23.3% | 4.5% |
| アプリケーションファイアウォール | 3,820 | 7.9% | −0.3% | 4,242 | 8.4% | 11.1% |
| その他のネットワーク脅威対策製品 | 3,688 | 7.6% | −1.3% | 3,876 | 7.7% | 5.1% |
| ネットワーク脅威対策製品 | 48,508 | 13.6% | 0.0% | 50,409 | 13.4% | 3.9% |
| ウイルス・不正プログラム対策ソフトウェア（企業向けライセンス契約）／アプライアンス | 52,190 | 38.0% | 0.7% | 55,111 | 38.0% | 5.6% |
| ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ） | 51,189 | 37.3% | 0.9% | 53,630 | 37.0% | 4.8% |
| スパムメール対策ソフトウェア／アプライアンス | 6,288 | 4.6% | −0.7% | 6,831 | 4.7% | 8.6% |
| URL フィルタリングソフトウェア／アプライアンス | 5,883 | 4.3% | −1.0% | 6,732 | 4.6% | 14.4% |
| メールフィルタリングソフトウェア／アプライアンス | 14,455 | 10.5% | −0.3% | 15,037 | 10.4% | 4.0% |
| DLP 製品 | 5,154 | 3.8% | 0.4% | 5,594 | 3.9% | 8.5% |
| その他のコンテンツセキュリティ対策製品 | 2,091 | 1.5% | 0.9% | 2,102 | 1.4% | 0.5% |
| コンテンツセキュリティ対策製品 | 137,250 | 38.5% | 0.5% | 145,034 | 38.6% | 5.7% |
| 個人認証用デバイスおよびその認証システム | 19,848 | 30.9% | 1.9% | 20,227 | 30.1% | 1.9% |
| 個人認証用生体認証デバイスおよびその認証システム | 9,726 | 15.2% | 3.3% | 9,923 | 14.8% | 2.0% |
| アイデンティティ管理製品 | 8,386 | 13.1% | 1.2% | 9,114 | 13.6% | 8.7% |
| ログオン管理／アクセス許可製品 | 15,712 | 24.5% | 0.6% | 16,924 | 25.2% | 7.7% |
| PKI システムおよびそのコンポーネント | 6,206 | 9.7% | −0.6% | 6,456 | 9.6% | 4.0% |
| その他のアイデンティティ・アクセス管理製品 | 4,312 | 6.7% | −0.6% | 4,539 | 6.8% | 5.2% |
| アイデンティティ・アクセス管理製品 | 64,191 | 18.0% | 1.3% | 67,184 | 17.9% | 4.7% |
| セキュリティ情報管理システム／製品 | 14,594 | 29.3% | −0.1% | 15,539 | 29.4% | 6.5% |
| 脆弱性検査製品 | 3,607 | 7.2% | −0.3% | 3,648 | 6.9% | 1.1% |
| ポリシー管理・設定管理･動作監視制御製品 | 23,647 | 47.5% | 1.5% | 25,336 | 47.9% | 7.1% |
| その他のシステムセキュリティ管理製品 | 7,923 | 15.9% | −0.6% | 8,394 | 15.9% | 5.9% |
| システムセキュリティ管理製品 | 49,771 | 14.0% | 0.5% | 52,917 | 14.1% | 6.3% |
| 暗号製品 | 38,339 | 10.7% | 2.8% | 40,894 | 10.9% | 6.7% |
| セキュリティツール製品 | 356,762 | 100.0%<br>54.9% | 0.7% | 376,083 | 100.0%<br>55.3% | 5.4% |

| 年度別売上高推計値 | 2011 年度 | | | 2012 年度 | | |
|---|---|---|---|---|---|---|
| セキュリティ･サービス | 売上高予測値 | | | 売上高予測値 | | |
| | 金額 | 構成比 | 前年比伸び率 | 金額 | 構成比 | 前年比伸び率 |
| 情報セキュリティポリシー構築支援･管理全般のコンサルテーション | 34,130 | 56.4% | −2.8% | 34,795 | 56.4% | 1.9% |
| 情報セキュリティ診断･監査サービス | 15,624 | 25.8% | −3.6% | 16,053 | 26.0% | 2.7% |
| 情報セキュリティ関連規格認証取得等支援サービス | 4,356 | 7.2% | −39.8% | 4,398 | 7.1% | 1.0% |
| 情報セキュリティ関連認証･審査･監査機関（サービス） | 1,933 | 3.2% | −35.6% | 1,912 | 3.1% | −1.1% |
| その他の情報セキュリティコンサルテーション | 4,501 | 7.4% | −4.4% | 4,500 | 7.3% | 0.0% |
| 情報セキュリティコンサルテーション | 60,545 | 20.8% | −8.6% | 61,658 | 20.4% | 1.8% |
| IT セキュリティシステムの設計･仕様策定 | 23,522 | 21.7% | −19.5% | 24,752 | 21.7% | 5.2% |
| IT セキュリティシステムの導入･導入支援 | 54,376 | 50.1% | −9.5% | 57,437 | 50.4% | 5.6% |
| セキュリティ製品の選定･選定支援 | 19,751 | 18.2% | −7.4% | 20,672 | 18.1% | 4.7% |
| その他のセキュアシステム構築サービス | 10,909 | 10.0% | −5.9% | 11,124 | 9.8% | 2.0% |
| セキュアシステム構築サービス | 108,559 | 37.2% | −11.2% | 113,985 | 37.6% | 5.0% |
| セキュリティ総合監視･運用支援サービス | 26,917 | 29.5% | 1.3% | 29,162 | 30.8% | 8.3% |
| ファイアウォール監視･運用支援サービス | 4,757 | 5.2% | 0.9% | 4,611 | 4.9% | −3.1% |
| IDS／IPS 監視･運用支援サービス | 6,231 | 6.8% | 0.3% | 6,752 | 7.1% | 8.4% |
| ウイルス監視･ウイルス対策運用支援サービス | 3,910 | 4.3% | −0.4% | 4,092 | 4.3% | 4.7% |
| フィルタリングサービス | 7,199 | 7.9% | 1.5% | 7,862 | 8.3% | 9.2% |
| 脆弱性検査サービス | 11,668 | 12.8% | 1.7% | 11,690 | 12.4% | 0.2% |
| セキュリティ情報提供サービス | 1,718 | 1.9% | 0.5% | 1,575 | 1.7% | −8.3% |
| 電子認証サービス | 21,493 | 23.5% | 0.9% | 21,914 | 23.2% | 2.0% |
| インシデント対応関連サービス | 4,016 | 4.4% | 2.8% | 3,858 | 4.1% | −3.9% |
| その他の運用･管理サービス | 3,465 | 3.8% | −0.7% | 3,107 | 3.3% | −10.4% |
| セキュリティ運用･管理サービス | 91,375 | 31.3% | 1.1% | 94,622 | 31.2% | 3.6% |
| 情報セキュリティ教育の提供サービス | 20,798 | 87.2% | −0.05% | 21,990 | 87.6% | 5.7% |
| 情報セキュリティ関連資格認定および教育サービス | 2,219 | 9.3% | −1.6% | 2,293 | 9.1% | 3.3% |
| その他の情報セキュリティ教育サービス | 825 | 3.5% | −1.6% | 826 | 3.3% | 0.1% |
| 情報セキュリティ教育 | 23,841 | 8.2% | −0.2% | 25,109 | 8.3% | 5.3% |
| 情報セキュリティ保険 | 7,244 | 2.5% | 0.1% | 7,417 | 2.4% | 2.4% |
| 情報セキュリティサービス | 291,563 | 100.0%<br>45.0% | −5.9% | 302,792 | 100.0%<br>44.6% | 3.9% |
| セキュリティツール＋サービス | 648,326 | 100.0% | −2.4% | 678,874 | 100.0% | 4.7% |

# 【第二部　情報セキュリティ市場調査の事業概要と結果に関する考察結果】

## 第５章 調査の概要

### 5.1. 調査対象

本調査の対象は国内情報セキュリティ市場である。「2010 年 3 月 31 日時点で、国内で情報セキュリティに関するツール、サービス等の提供を事業として行っている事業者（輸入販売、再販売を含み、輸出を含まない）」を対象として、以下の推定市場規模データを算出した。

(1) 2008 年度国内情報セキュリティ市場規模　推定実績値
(2) 2009 年度国内情報セキュリティ市場規模　推定実績値
(3) 2010 年度国内情報セキュリティ市場規模　実績見込値
(4) 2011 年度国内情報セキュリティ市場規模　予測値

なお本調査は､前回の2009年度調査とは対象とする時点が異なるので調査母体に変化があり、調査対象範囲は概ね重複するものの直接の連続性はない。従い、上記の調査対象年度全てについて新たに算定作業を行っている。ただし、2008 年度の市場規模の算定に当っては、2009 年度（前回）調査結果も参考としている。

また、追加情報として 2012 年度の予測を簡易調査に基づいて行い、盛り込んだ。

### 5.2. 調査方法ならびに調査に使用したデータおよび情報

本調査で主として利用した市場規模に関するデータは、以下の通りである。

(1) アンケート調査

2011 年 1 月～2 月の期間に、JNSA 会員企業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。

このうち、情報セキュリティツールについては、流通過程が多岐に渡るため、様々な業態・立場の事業者を幅広く調査対象とすることで漏れを防ぐことを心がけた。と同時に、流通上の諸段階で数字が計上されることによるデータの重複を避けるために、流通構造の模式図を示して自社の立場を回答してもらうことで、ダブルカウントの可能性を排除する工夫をした。

調査対象とした年度は 2008 年度から 2011 年度で、基準年度を 2009 年度とした。2008, 2009 年度については実績値を、2010 年度については実績見込み値を、2011 年度については計画値または予測値を記入してもらった。年度区分については、各年の 4 月から翌年 3 月までを基準とし、極力この期間に対応する数字を回答してもらったが、年度区分が異なる企業については、直近の会計年度の数字での回答も可とした。

アンケートは電子メールによる依頼・配布、電子メールによる回答とし、Excel ベースの調査票を使用した。アンケートの回収件数は 34 件（うち有効回答数 34 件）であり、回収率は約 23%であった。

アンケート方式で数字を把握する場合の問題点として、①調査する側とされる側の製品分

類や定義の差があり、質問に対応する数字を被調査企業で把握していないケース、②関連するサービスの一部がセキュリティに関わる部分であるが、その部分だけの対価が算出されていないために、参入有無では参入ありと回答しつつ金額数字の回答がないケース、③主として外資系企業で、情報開示に関する規制から、日本でのデータが一切公開されないケース、等があり、アンケートのみに依存する、市場の数量的把握には限界がある。従って本調査では、情報セキュリティベンダに対するアンケート調査で得られた集計数値をそのまま市場規模の数字とはせず、全体集計に際しての利用データの一部と位置付けている。

(2) 各種統計資料調査

国内の事業所、産業、投資等に関する政府およびその関連機関、並びに民間企業の資料を調査した。

(3) ヒアリング調査

参入事業者のうち、業界の全体像や動向を予測・分析するのに参考になる企業を中心に、情報セキュリティ事業に関する情報を統括する立場の人たちへのヒアリング調査を実施した。

(4) サンプリング調査

アンケート調査と平行して、事業として何らかの形で情報セキュリティに関わっていると考えられる企業については、JNSA 独自の推計調査を実施した。対象は、市場規模を推計する上で重要と考えられる企業 367 社（アンケート調査対象とした JNSA 会員企業 145 社を含む）である。調査員が個別に、有価証券報告書、Web ページ、製品資料等の外部公表資料や傍証的情報からその事業の概要を推定して事業規模を算定し、集計に反映させる方法を取り入れた。(3)項のヒアリングにより得られる情報も加味している。なお、アンケート回答を得た企業についても、JNSA 独自の調査を実施し、アンケート回答との突合・検証を行っている。

### 5.3. データポイントの定義

データのポイントとしては、ベンダからの出荷額ベースで計測しており、流通マージンや付加サービス（流通・販売業者による設定サービス等）は含まない。またベンダが提供する有償の保守契約やアップデートサービスの価格は、本体製品の付帯品として、本体製品と同一区分で集計している（サービス売上にはカウントしない)。なお、認証・アクセス管理系システムやセキュリティ情報管理システムのように、全体システムを構成するに際して中核となるシステムの一部がセキュリティ機能を提供する形態のうち、そのセキュリティ機能が、セキュリティ対策全体の核機能として重要な意味を持つモジュールであるような場合は、集計対象としている。一方、例えばルータにおけるセキュリティ対応のフィルタリング機能のような、その装置の本来用途からは付帯的な機能として付加されている場合は集計対象としない。(これらの点に関する判断基準としては、モジュールやオプションのような形で切り出しが可能で価格付け対象となるか、最初から装備されている付加機能かという仕分けも援用している。)

サービスの価格についても、サービスの提供事業者からの提供価格に基づく集計を行った。集計対象としたのは、後に示すサービスの定義に該当するサービスの範囲に対応する数字となる。

いわゆるシステムインテグレータが、システムインテグレーションの一部として情報セキュリティに関するサービス（定義範囲内のもの）を提供する場合は、その部分の価格が明示的に把握できる場合に、その売上のみを集計対象としている。また、そのようなケースで情報セキュリティツールの設定サービス等がセキュアシステム構築サービス等の金額に含まれる場合には、例外的にツールの「付加サービス」がサービス売上として計上され、本調査対象に含まれることがある。

### 5.4. 市場規模の予測値の算定方法

推計作業の対象とする年度は基準年度である 2009 年度である。2010 年度、2011 年度の市場規模推定にあたっては、2009 年度の市場規模の実績推定値を基に、いくつかの要素を加味して推計作業を行った。

アンケート調査にベンダが回答した事業計画あるいは売上予測の数値と、その成長率のデータを基本的データとして用いた。予測値または計画値については、実数による回答が得られにくいことから、売上高成長率による回答表記も可能なようにした。また、同じくアンケート調査の最後には、自社の事業だけでなく、業界としての動向、顧客の関心の向いている分野について、回答企業がどう見ているかを問うた。これにより、供給サイドや需要サイドのマクロの方向感を得るための参考にした。

また、各市場区分（セグメント単位）での動向もしくは傾向（市場としての伸びの強度）や、各業態区分（7.2 章参照）における事業展開のマクロ的趨勢を変動パラメータとして加味することで、市場変化の予測値をダイナミックにシミュレーションするアプローチを試みた。

# 第６章 情報セキュリティ市場の分類および定義

今回情報セキュリティ市場の規模をベンダ側の数値を基に算出するに際して、市場の区分として、「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」とはハードウェア製品もしくはソフトウェア製品である。「製品」という表記ではソフトウェアライセンスが含まれないイメージとなることを避けるため、「ツール」という表現としている。また、サービスに対応する「有形物」のイメージとしてもなじみやすいと考えた。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。ただ、一部のソフトウェア商品は、ダウンロード販売のように、物の形を取らないまま取引される場合もある。

「サービス」は、「ツール」のようにモノとしてのやり取りが存在せず、無形の役務提供をビジネスモデルとするものを、基本的に対象としている。「サービス」は、定期開催型教育コースや侵入検査サービスのように定型化・メニュー化され定価設定されるパターンのものと、システム構築やカスタムコンサルテーションのように、供給者と需要者の個別的・相対(アイタイ)的取引で提供され消費されるビジネスモデルの 2 パターンを想定している。ただし、市場区分においてこのパターンを分類の基準とはしていない。取引形態よりはサービスの目的、提供する機能の種類を基準として分類している。

本調査で用いた市場分類体系は、以下に示す通りである。6.1 章にその一覧表を、6.2 章および 6.3 章に各大分類レベルの市場区分に対する簡単な説明を記す。

## 6.1. 情報セキュリティツール･サービスの市場分類定義表

表 17、表 18 に、本調査のアンケート調査に際して使用し、回答者に示した「情報セキュリティツール」「情報セキュリティサービス」の市場区分とその定義もしくは説明･例示等の一覧表を掲げる。なお、表 16 には、表 17、表 18 で使用した用語･略号等の説明を載せた。

**表 16 用語説明**

| | |
|---|---|
| アプライアンス | ハードウェアとソフトウェアを一体として特定の機能を提供する販売形態をとる製品<br>1 台のコンピュータで複数の機能を提供するサーバ型コンピュータ。内部バスに複数の機能モジュールを接続して複数の機能を実現する形（いわゆるシャーシ型）を含む。ブレードサーバ形式で複数の機能サーバが並列して機能を実行し、全体として統括する OS が存在しない状態（いわゆるブレードサーバ型）は含まない。 |
| ソフトウェア | パッケージ製品、ダウンロード製品、ライセンス販売製品等、定型化されたもの<br>一部カスタマイズの場合は対象に含め、完全な個別開発ソフトウェアは含まない |
| AV | Anti Virus アンチウイルス |
| FW | Firewall ファイアウォール |
| IDS | Intrusion Detection System 侵入検知システム |
| IPS | Intrusion Prevention System 侵入防止システム |
| PKI | Public Key Infrastructure 公開鍵暗号基盤 |
| SSL | Secure Socket layer 暗号通信の一方式 |

| | |
|---|---|
| URL | Unifie Resource Locator 統一資源位置指定子 |
| VPN | Virtual Private Network 仮想私設通信網 |
| PCI DSS | Payment Card Industry Data Security Standard　PCI データセキュリティ基準 |
| QSA | Qualified Security Assessors 認定審査機関 |
| ASV | Approved Scanning Vendors 認定スキャンベンダー |

**表 17　情報セキュリティツールの市場分類**

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

| コンテンツセキュリティ対策製品 | | | |
|---|---|---|---|
| | 1. コンピュータウイルス、スパイウェア、ボット等の不正プログラム（マルウェア）などを、ファイル等の電子データや電子メール送受信・Web閲覧等のコンピュータ通信の中から検出し、排除・無害化・警告等の対策を講じる機能を持つ製品群。<br>2. システム・業務・サービスの目的や適正な運営にとって有害な電子メール送受信やWeb閲覧等の通信を検査し、フィルタリング・警告・排除・ログ記録その他の対応を行う機能を持つ製品群。<br>3. 電子メール、電子ファイル等の内容（コンテンツ）について、ポリシー等あらかじめ設定された条件に基づいて、その送信・移送・受け渡し等の移動、複製・閲覧・編集・印刷等の加工その他の利用を阻止・防止もしくは制限し、または警告・報告・記録等を行う、情報保護のための製品群。 | ウイルス・不正プログラム対策ソフトウェア（企業向けライセンス契約）／アプライアンス | ウイルス、ワームその他の不正プログラムの感染や侵入を検知・防御・排除する機能を持ったソフトウェア（主として企業等向けにライセンス契約方式で提供されるもの）またはアプライアンス。プログラムや定義ファイル更新の年次参照権の販売を含む。<br>ゲートウェイ型、サーバ型、クライアント型の全てを含む。<br>付加機能としてFW、IDS、スパム対策、URLフィルタリング等の機能を併設するものを含む。 |
| | | ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ） | ウイルス、ワームその他の不正プログラムの感染や侵入を検知・防御・排除する機能を持った、主として個人使用のクライアントパソコン向けソフトウェア。主としてパッケージ形式もしくはオンラインダウンロード形式で販売されるもの。プログラムや定義ファイル更新の年次参照権の販売を含む。<br>デスクトップFW、HIPS（ホストIPS）、スパム対策、URLフィルタリング等の機能を併設するものを含む。 |
| | | スパムメール対策ソフトウェア／アプライアンス | 無差別・大量に送りつけられる、不要もしくは有害な内容を含む宣伝・勧誘目的等の電子メール（スパムメール）をフィルタリングし、マーキング、警告、分別、排除等を行うソフトウェアもしくはアプライアンス製品。<br>ウイルス・不正プログラム対策製品にこの機能が併設される場合は、ウイルス・不正プログラム対策製品に分類する。 |
| | | URLフィルタリングソフトウェア／アプライアンス | インターネット上のWebサイト（ホームページ）へのアクセスや閲覧につき、そのアドレスや内容が、所定の条件（有害、危険、不適格、Reputation Serviceによるリスト等）に合致（もしくは違反）する場合に処理（停止、警告、管理者への通報、ログ保存等）を行うソフトウェアもしくはアプライアンス製品。<br>ウイルス・不正プログラム対策製品にこの機能が併設される場合は、ウイルス・不正プログラム対策製品に分類する。 |
| | | メールフィルタリングソフトウェア／アプライアンス | 送受信される電子メールにつき、そのアドレスや内容、添付ファイル等を検査し、所定の条件（有害、不適格、情報漏えい、Reputation Serviceによるリスト等）に合致（もしくは違反）する内容を含むものに対して処理（停止、隔離、警告、管理者への通報もしくは回送、ログ保存等。）を行うソフトウェアもしくはアプライアンス製品。単に全メールを無条件にアーカイブするだけのものを除く。<br>ウイルス・不正プログラム対策製品にこの機能が併設される場合は、ウイルス・不正プログラム対策製品に分類する。 |
| | | DLP製品・システム（情報漏えい対策製品・システム） | Data Loss/Leak/Leakage Protection/Preventionと呼ばれる製品またはシステム。<br>企業内システムやネットワークから外部に向かうデータの流れ（電子メールその他のネットワークトラフィック、別のストレージへの書き込み、外部記憶媒体への書き込み、印刷等）の中に特定の特徴を含むデータがある場合、その行為に対して阻止、警告、記録等の動作を行い、外部への情報・データの流出や紛失を防止する機能を提供するシステムまたは製品。 |
| | | その他のコンテンツセキュリティ対策製品 | 組織内（あるいは個人）と組織外の間でネットワーク通信その他の方法で受け渡しされる電子データに関して、主としてセキュリティの目的でフィルタリングその他の機能を提供する製品で、上記のいずれにも属さない、あるいは特定の中分類に仕分けできないもの。<br>いわゆるDigital Rights Management(DRM)製品やシステムを含む。<br>いわゆるフィッシング詐欺目的で送付される電子メールのフィルタリング、フィッシングサイトへのアクセスや閲覧に対する警告、Webサイトのフィッシングに関する安全性の確認等の機能を提供する、ソフトウェア、システムもしくはサービスを含む。 |

| | | | |
|---|---|---|---|
| | | | （ただし、一般的なサイト証明書の発行サービスは「運用・管理サービス」に分類する。） |
| アイデンティティ・アクセス管理製品 | | | |
| | ネットワーク資源、コンピューティング資源のユーザを電子的手段で特定し、ユーザごとに定義されたアクセス権等に基づいて、ネットワーク資源・コンピュータ資源へのアクセスや利用の許可を行う機能を提供する製品群またはシステム。<br>本人特定（アイデンティファイ）と認証、アクセス権限の付与と管理、電子証明の発行と管理等の各機能を、個別にあるいは総合・連携して提供する。<br>いわゆるAuthentication, Authorization, Access Control の機能を提供する製品群。 | 個人認証用デバイス及びその認証システム | ワンタイムパスワード、ICカード、USBキー、携帯電話等を用いて本人確認する機能を提供するデバイスおよびそのシステム（生体認証を除く）。 |
| | | 個人認証用生体認証デバイス及びその認証システム | 指紋、静脈等の生体の特長のみならず、声紋、筆跡等身体的特徴に着目して本人を特定する機能を提供するセンシングデバイスおよびその認証システム。 |
| | | アイデンティティ管理製品 | システム並びにデータへのアクセス権について、システムの利用者に関してはその職務や権限に基づく定義のデータベースを、システム並びにアプリケーションに関してはそのアクセス許可ポリシーを管理する機能を提供する製品群。<br>利用者の異動に伴う変更管理や、システム間のアクセス権の情報連携や統合管理を実現し、情報資産の利用権の即時的一元的管理を可能にする。<br>プロビジョニング製品を含む。<br>フェデレーション製品（異システム・異組織間のID連携、プロビジョニング連携のための製品）を含む。 |
| | | ログオン管理／アクセス許可製品 | ユーザがシステムにアクセスする際の承認・許可機能を提供する製品分類。<br>シングルサインオン(SSO)およびSSO間連携製品を含む。<br>但し、個人認証用および個人認証用生体認証デバイスと一体で機能するシステムは当該各デバイス及び認証システムに分類する。 |
| | | PKIシステム及びそのコンポーネント | 電子証明書の発行、管理、証明サービスを提供するシステムおよびその構成要素。<br>但し、構築サービス(SI)は含まない。（サービス市場に分類する）<br>なお、電子証明書の発行サービスはサービス市場に分類する。 |
| | | その他のアイデンティティ・アクセス管理製品 | 本人認証、アクセス権管理、ログオン管理等の機能を提供しまたはそれらに関連する機能・サービスを提供する製品で上記のいずれにも属さない製品。<br>ディレクトリサーバ（単独で製品化されているもの）を含む。 |
| システムセキュリティ管理製品 | | | |
| | 1．ネットワークトラフィックを監視・制御する装置等の状態やその発する情報を統合管理し、セキュリティについて分析し、表示・統計・警告・記録等を行う製品群。<br>2．ネットワークを構成する装置やサーバ等の設定やアプリケーションの脆弱性を検査し、結果を報告する製品群。<br>3．ネットワークやコンピュータを構成する機器やデバイスの情報を入手し、その状態や属性や設 | セキュリティ情報管理システム／製品 | FW等のセキュリティ監視･制御装置のログまたはサーバのイベントログ等の情報を統合･監視･分析し、ネットワークシステムのセキュリティ状態をリアルタイムで総合的に管理する機能を持つ製品およびシステム。<br>統合ネットワーク管理プラットフォームのうちセキュリティ管理モジュールの製品部分も統計対象とする。 |
| | | 脆弱性検査製品 | 検査対象となるサーバ等に対し、スキャニングや擬似攻撃を行い、脆弱性や設定の不備等、危険事項を検査し報告する製品群。いわゆる脆弱性スキャナー（ネットワークベース、ホストベース）。 |
| | | ポリシー管理・設定管理･動作監視制御製品 | 1．OSやアプリケーションの設定、パッチ適用、バージョン等を監視･管理する製品群<br>2．クライアントマシン等におけるファイルのコピー･印刷その他の操作を監視･制限･制御等する製品群。<br>3．クライアントPC等の識別情報やインベントリ情報等を収集・分析・管理し、ポリシー等の設定された条件に合致しないアプ |

| | | | |
|---|---|---|---|
| | 定や動作の監視・診断・制御・記録等の機能を持つ製品群。<br>4. ネットワークに接続するデバイスの設定状態等を確認し、接続の可否を制御・管理する機能を持つ製品群。<br>5. ファイル等の電子データの移動・複製・編集その他の処理を中心としたコンピュータの動作について監視・制御・記録・警告等をする製品群。<br>6. その他、コンピュータとネットワークの状態や動作をセキュリティ面から管理する機能を持つ製品群。 | | リケーション等のインストール等の管理（警告・報告・禁止・削除等）を行う製品・システム。<br>4. その他個別のマシンの設定、状態、動作等に着目してセキュリティを管理する製品群。<br>5. クライアントPC等の識別情報やインベントリ情報等に基づきネットワーク接続を管理・制御する製品・システム。いわゆる「ネットワーク検疫システム」における機器認証サーバを含む。原則として単体製品またはネットワーク制御装置等のオプションとして取引対象となる製品形態のものを対象とし、その機能がルータ等の一部にデフォルトとして組み込まれている場合は対象外とする。 |
| | | その他のシステムセキュリティ管理製品 | コンピュータネットワークシステムの、システムとしての状態を監視・解析・管理する機能を持った製品群のうち、上記セグメントのいずれにも分類されない製品群。<br>主としてセキュリティ、内部統制管理（ITガバナンス）等を目的としてログの収集、減量・圧縮、保管・アーカイブ、解析等を行う製品、ならびにいわゆるデジタルフォレンジック製品等を含む。<br>ただし、ログ収集・解析機能を提供する製品のうち、リアルタイム監視を主目的とする製品は「セキュリティ情報管理システム／製品」に分類し、当分類では主に傾向解析等スタティックな目的のものを対象とする。 |
| 暗号製品 | | | |
| | データの暗号化を主たる機能とする製品群。<br>通信経路に対する防御を主目的に通信の暗号化を行う、いわゆるVPN製品は、「ネットワーク脅威対策製品」に分類する。 | 暗号製品 | 1. メール、ファイル、ディスク、記憶デバイス等のデータを暗号化することで権限外使用、覗き見、改ざん、漏えい等を防止することを主たる機能とする製品群。<br>2. ハードディスク、USBメモリ、磁気テープ装置等に組み込まれて書き込み・読み出しの際に暗号化・復号化を自動で行う機能部分を構成する暗号化モジュール。<br>3. 暗号ライブラリ、暗号化モジュール等の中間製品で、製品または部品として単独で取引されるもの。<br>4. 暗号化することでセキュリティの目的を満たすことを主たる機能とする製品で上記に属さないもの。<br>ただし、電子証明書発行システムは「アイデンティティ・アクセス管理」に、その関連サービスはサービス市場に分類する。 |

**表 18　情報セキュリティサービスの市場分類**

| 大分類 | 中分類 | 定義、説明、例示　等 |
|---|---|---|
| 情報セキュリティ・コンサルテーション | | |
| 1. 情報セキュリティについて、主として経営管理およびIT管理の領域において、管理のための政策、管理体系、運用体制等の構築、診断、監査に関する支援やコンサルティングを行うサービス。<br>2. これらに関連する規格認証枠組みに対応して認証取得を目指す場合の支援サービスおよび規格等の審査・認証 | 情報セキュリティポリシーおよび情報セキュリティ管理全般のコンサルテーション | 情報セキュリティの管理の体制や手順に関する総合的コンサルティングサービス。<br>情報セキュリティポリシーや管理・運用基準等の構築および見直しのサービスを含む。<br>情報セキュリティガバナンスの構築・取組支援サービス・コンサルテーションを含む。 |
| | 情報セキュリティ診断・監査サービス | 情報セキュリティのポリシー、システム、管理体制、コンプライアンスの現状に対して診断または評価（一部では慣例的に「監査」とも呼ぶ）を行うサービス。ITシステムの弱点を擬似ネットワーク攻撃等で検査するサービスは「セキュリティ運用・管理サービス」の中に位置づける。ここでは管理体制等に対する総合的診断・評価を行うサービスを主体とするサービスを対象とする。<br>情報セキュリティ監査制度（経済産業省告示に基づく）におけ |

| | | | |
|---|---|---|---|
| | サービス。<br>3. これらに類似または直接関連するコンサルティングサービス。 | | る情報セキュリティ監査サービスは「情報セキュリティ関連認証・審査・監査機関（サービス）」に分類する。 |
| | | 情報セキュリティ関連規格認証取得等支援サービス | 情報セキュリティ監査の受審、情報セキュリティ格付けの取得、ISMS適合性認証の取得、プライバシーマーク適合認定、PCI DSS準拠認定の取得等を支援するサービス。 |
| | | 情報セキュリティ関連認証・審査・監査機関（サービス） | 情報セキュリティ監査（経済産業省告示に基づく「情報セキュリティ監査制度」における情報セキュリティ監査サービス）、情報セキュリティ格付け、ISMS適合性認証、プライバシーマーク適合認定等を行うサービス。<br>PCI DSS準拠認定を行うQSA(Qualified Security Assessors)を含む。ただし、ASV(Approved Scanning Vendors)は「セキュリティ運用・管理サービス」のうち「脆弱性検査サービス」に含める。 |
| | | その他の情報セキュリティコンサルテーション | その他の情報セキュリティ管理に関するコンサルティングサービス。<br>内部統制管理、事業継続管理、ITサービスマネジメント等に関連して、情報セキュリティに関わる強化・改善等を**主たる**目的として実施されるコンサルテーション等を含む。（情報セキュリティが従たるもしくは副次的目的の場合は「情報セキュリティコンサルテーション」としてはカウントしない。） |
| セキュアシステム構築サービス | | | |
| | ITセキュリティシステム、またはITシステムのセキュリティについて、構築を支援するサービス。ただし、セキュリティツールやそのプラットフォーム自体の価格は含めず、その導入や構築といった役務・サービス部分を集計対象とする。 | ITセキュリティシステムの設計・仕様策定 | ITシステムのセキュリティについて、その設計、仕様の定義、要求条件の設定等の全体の枠組み、あるいは特定機能の内容について策定するサービス。 |
| | | ITセキュリティシステムの導入・導入支援 | ITセキュリティシステムまたはITシステムのセキュリティに関する、システムインテグレーションサービス。<br>原則として設計部分を除く導入部分のみとするが、両者が不可分の場合はこの分類に集計する。 |
| | | セキュリティ製品の選定・選定支援 | 顧客のポリシーや要求条件に基づいて、それに適したITセキュリティ対策製品を選定し、またはそのための情報提供等の支援を行うサービス。 |
| | | その他のセキュアシステム構築サービス | その他のITセキュリティシステム構築サービス。<br>ITセキュリティ製品の保守・サポート等のサービスを、メーカの製品付帯サービスの再販以外に、再販事業者やSI事業者が独自付加価値として提供する場合はこの区分で集計する。 |
| セキュリティ運用・管理サービス | | | |
| | 1. ITセキュリティシステム、またはITシステム上のセキュリティ対策機器等の運用や管理の支援を行い、状態の監視、安全対策に対する診断、インシデント等に際しての判断や対応の実施や支援を行うサービス。<br><br>2. ITシステムの運用等に関連する各種の情報・利便・機能等を提供するサービス。 | セキュリティ総合監視・運用支援サービス | ネットワークシステムのセキュリティ状態を総合的に監視し、またその運用を支援するサービス。<br>関連するログ解析サービスを含む。 |
| | | ファイアウォール監視・運用支援サービス | ファイアウォール等のモニタリング状況やアラート等を監視し、またその運用を支援するサービス。<br>関連するログ解析サービスを含む。 |
| | | IDS／IPS監視・運用支援サービス | IDS／IPSシステム等のモニタリング状況やアラート等を監視し、またその運用を支援するサービス。<br>関連するログ解析サービスを含む。 |
| | | ウイルス監視・ウイルス対策運用支援サービス | コンピュータウイルス等の不正プログラム等に対して監視や対策を行い、またその運用を支援するサービス。関連するログ解析サービスを含む。 |
| | | フィルタリングサービス | 電子メールの送受信に際して、スパムメール等の有害メール対策や情報漏えい防止のためのフィルタリングもしくは監視を行うサービス。電子メールサーバ機能の提供と一体で提供されるサービスを含む。<br>インターネット上のWebアクセスに際して、ポリシーやリストに基づき警告、制限、遮断、報告、記録等の管理やフィルタリングを行うサービス。いわゆるレピュティションサービスを含む。 |

| | | | |
|---|---|---|---|
| | | 脆弱性検査サービス | ITシステムの脆弱性やアプリケーションのセキュリティホールに対して、侵入検査等の擬似攻撃手法やコードの解析等によって検査･診断するサービス。 |
| | | セキュリティ情報提供サービス | インシデント、脆弱性、パッチその他のITセキュリティに関する情報を提供するサービス。<br>Web、メールニュース、レポート、出版等、媒体種類を問わない。 |
| | | 電子認証サービス | 電子証明書の発行・認証、無改竄保証、否認防止、タイムスタンプ証明等の電子的証明やそれに関連するサービス。 |
| | | インシデント対応関連サービス | 情報セキュリティ･インシデントに際しての緊急対応や復旧に関する専門的スキルを提供するサービス、ならびにいわゆるデジタルフォレンジックに係る専門的スキルを提供するサービス。<br>ただし上記の各監視･運用支援サービスと一体のものとして提供される場合はその分類に集計する。 |
| | | その他の運用･管理サービス | その他の、情報セキュリティの運用･管理に関するサービス。<br>ITセキュリティ製品の保守・サポート等のサービスを、メーカの製品付帯サービスの再販以外に、監視・運用支援サービス提供事業者、SI事業者等の第三者が独自の付加価値として提供する場合はこの区分で集計する。 |
| 情報セキュリティ教育 | | | |
| | 情報セキュリティに関連する知識やスキルの習得、情報セキュリティポリシーやルールの組織内への周知徹底、および情報セキュリティ関連の資格取得のための教育、研修に関するサービス。<br>セキュリティコンサルテーションやセキュアシステム構築サービスの一環として社員や運用担当者等に実施する教育はそれらのサービスの一部ととらえ、「セキュリティ教育サービス」には集計しない。 | 情報セキュリティ教育の提供およびe-ラーニングサービス | 情報セキュリティ教育の提供･実施サービス。<br>講師が実施する集合教育・実地教育・演習等のサービス提供の形態、ならびにセキュリティ教育の内容または教材（いわゆるコンテンツ）の販売もしくはライセンス提供を行う形態の双方を含む。<br>情報セキュリティ教育のためのe-ラーニングのコンテンツの開発・提供およびe-ラーニングの実施サービスを含む。<br>セキュリティ資格関連のサービスは「セキュリティ資格認定及び教育サービス」に分類する。 |
| | | 情報セキュリティ関連資格認定及び教育サービス | 情報セキュリティ関連の資格の認定（継続・維持を含む）を行い、または資格認定のための教育研修の実施や受験準備のための講習等を行うサービス。 |
| | | その他の情報セキュリティ教育サービス | その他の情報セキュリティ教育に関するサービス。情報セキュリティ教育を直接の目的としたコンサルテーションやシステム構築サービスを含む。<br>情報セキュリティ製品の使用等に関して製品ベンダが行う教育のうち、製品取扱知識だけでなくネットワークセキュリティー般についての知識・技術習得を主たる目的とする教育（資格認定を伴うものを含む）サービスを含む。<br>システムのセキュリティを作り込む技術やセキュアプログラミング、安全なWebサイトの作り方など、セキュリティ技術の教育を主たる目的とする教育を含む。 |
| 情報セキュリティ保険 | | | |
| | 情報セキュリティならびにITセキュリティに関する損害を補償する保険。 | 情報セキュリティ保険 | 情報漏えい等の情報セキュリティインシデントならびにネットワークを中心としたITシステムのセキュリティインシデントに起因する損害を補償することを主たる機能とした保険。 |

## 6.2. 情報セキュリティツール市場の定義に関する説明

「ツール」については、ハードウェア製品とソフトウェア製品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」、「ネットワーク脅威対策製品」、「コンテンツセキュリティ対策製品」、「アイデンティティ・アクセス管理製品」、「システムセキュリティ管理製品」、「暗号製品」の 6 区分（大分類）とした。

以下に各市場区分に関する概要解説を記述する。

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である「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に実現する製品と定義した。

ハードウェアの高機能･低価格化と入手の容易さが進むに連れて、ユーザの利便性や保守の簡便性から、アプライアンスへ向かう動きが全般的に強まっている。導入に際して、ハード、OS、ソフトを各々購入して組み合わせる手間や、仕様の整合性を確保するための煩雑さから解放される。アップデートに際してもハードとの整合性はベンダの責任でカバーされる。トラブル対策に際しては、原因の所在をユーザ側で切り分ける必要がない。このようにアプライアンスはユーザにとっての利便性が高く、販売店にとってもユーザ対応が単純化するメリットがあることから、様々なセキュリティ機能がアプライアンスによって提供されるようになっている。

このうち単一機能のアプライアンスは各々の機能別カテゴリに分類し、複数のカテゴリの機能を併せ持つタイプのものを「統合型アプライアンス」として独立カテゴリとした。市場分類定義表では、「『ネットワーク脅威対策製品』と『コンテンツセキュリティ対策製品』に分類される機能のいずれかまたは両方を備え、二つ以上の大分類カテゴリにまたがる複数の機能を 1 台（またはセット）で提供するアプライアンス製品」と定義している。各大分類区分を一言で表わすと次のようになる。

①ネットワーク脅威対策製品

ファイアウォール、IDS／IPS、VPN、フィルタリングといった、主にネットワークの境界付近に配置し通信のハンドリング、モニタリング、ロギング等を行う製品。

②コンテンツセキュリティ対策製品

アンチウイルス、アンチスパム、URL フィルタリングといった、ファイルや電子メールや Web アクセスに対する不正・迷惑・妨害行為を阻止・防止・予防する製品。

本調査の市場分類の原則では、機能に着目して、その装置等が提供する機能の種類ごとに市場区分を定義している。しかし、統合型アプライアンスは、複数の機能を有することがその定義のベースになっており、他のカテゴリのどこにも分類できないために、独立のカテゴリとして調査集計する。

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多く見られたが、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 台でほとんどの外部脅威防御機能を実現する製品が 2003 年頃に登場し、2006 年頃から普及期を迎えた。複数機能の統合と共に、コンパクトなハードと一体化して提供するという特徴も指摘できる。またこれらの製品を、UTM（Unified Threat Management =統合脅威管理=）と総称する呼び方も一般的になっている。これは米国のメーカや調査会社が、製品が登場した初期に使った呼び方が一般に使われるようになった結果と考えられる。Unified Threat Management

の訳語としては「統合脅威管理」が一般的だが、Management という言葉から連想する「管理」よりは対策機能が主体であることに留意し、本調査の市場区分定義では「複合脅威対策」という訳語を当てている。

UTM 以外では、帯域管理にプロキシ、パケットフィルタリング、URL フィルタリング、コンテンツフィルタリング等を組み合わせるようなものも登場している。また、内部ネットワークのスキャンと同時にウイルスやスパムのチェックを行うようなタイプの製品も見られる。認証機能や検疫システム機能といった、これまではソフトウェア製品で実現されていた機能がアプライアンス化される例も見られるようになった。

このように様々なバリエーションを持った複合機能のアプライアンスが登場しているが、ファイアウォールの発展型である UTM が主流であるところから、特に中分類では区分せず、「二つ以上の大分類カテゴリにまたがる複数の機能を 1 台で提供するアプライアンス製品」を「統合型アプライアンス」として、単一セグメントのカテゴリとして定義した。

2. ネットワーク脅威対策製品

「ネットワーク脅威対策製品」の機能は、内部ネットワークと外部ネットワーク（通常インターネット）の境界（Perimeter）やその近傍に配置されて、主として通信のハンドリングまたはモニタリングを行うことである。主たる製品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 侵入検知システム、Intrusion Prevention System 侵入防御システム）の 3 種類の製品分類を含む。

ネットワーク脅威対策製品の分野では、当初はソフトウェアタイプが主流であったが、現在ではアプライアンス型製品が一般的になっている。本調査では、従来、中分類レベルにおいてソフトウェア製品とアプライアンス製品を分けて定義し集計していたが、2009 年度調査からその区分を廃止し統合している。また、個人向けパッケージ製品であるパーソナルファイアウォールも、そのほとんどがウイルス対策ソフトウェアと一体化して単体製品としては存続しなくなったので統合し、再編整理した。詳しくは 2009 年度の調査報告書を参照されたい。

その結果、2009 年度からは「ネットワーク脅威対策製品」は以下の 5 つの中分類市場に分けて市場規模推計を行っている。

①ファイアウォールアプライアンス／ソフトウェア

ファイアウォールは、ネットワーク上の通信パケットに対して、あらかじめ設定されたその組織の通信に関するルールに従って、通信の許可、遮断、制御を行うことで外部からの攻撃に対する防御や不正な通信の制限・遮断を行う製品である。アプライアンス型製品とソフトウェア製品がある。ファイアウォールが使われ出した初期のころはほとんどがソフトウェアタイプであったが、その後専用ハードウェアによってパフォーマンスとメンテナンス性を向上させたアプライアンスが主流となった。クラウドの浸透に伴い、仮想マシン上に実装するソフトウェアタイプが再び増加しつつある。

ファイウォールの多くは VPN 通信を通過させる必要があるため、VPN ゲートウェイの機能を併設している。

ネットワーク上に配置するファイアウォールとは別に、サーバや端末 PC に実装する、パーソナル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ソフトウェア製品もある。過去には先進的な個人や一部企業で用いられていたが、ウイルス対策ソフトウェアがデスクトップファイアウォール機能を併設することが一般的になってからは、単体製品としてのデスクトップファイアウォールは限定的存在となっている。

②VPN アプライアンス／ソフトウェア

ネットワーク通信を暗号化して、オープンなネットワークでも専用線と同様な通信の安全を確保する機能（VPN= Virtual Private Network=機能）を提供する製品で、アプライアンス型のものとソフトウェアタイプの製品がある。ただし、ファイアウォールに VPN 機能が付帯する場合はファイアウォールに分類する。VPN に際しては、通常、外部から VPN 通信のためにアクセスしてきた相手が、通信を許可されている相手かの確認をする認証手続きを伴うが、その認証のための通信のハンドリングも、VPN 製品が行うことが一般的である。

アクセスを受ける LAN 側ゲートウェイはファイアウォールに併設される機能を用い、リモートアクセスする端末 PC にはソフトウェアタイプのクライアントを実装する形が一般的である。クライアントは、IC カードや USB メモリに実装して、VPN 通信を実現するタイプもある。その場合、同時に端末をシンクライアントとして使用する構成を実現する製品も登場している。ただし、シンクライアントは本調査の対象外としているので、シンクライアントに付属の VPN は集計対象外となる。

③IDS／IPS アプライアンス／ソフトウェア

通常ファイアウォールの後方（内側）に置かれ、ファイアウォールに許可された、あるいはフィルタリングされなかった通信に対して、その内容や状態を一定の方法・技術に基づき検査し、侵入もしくは攻撃と判断される通信に対して報告・警告・ログ記録等を行うのが IDS（侵入検知システム）であり、IPS（侵入防止システム）は更に遮断や阻止まで行う。ファイアウォールのポリシーでは許可される種類のパケットやポートを利用して悪意ある通信内容を仕込み、攻撃する手段に対する防御手法である。

アプライアンス型製品とソフトウェア型製品がある。ファイアウォールと同様に、初期のころはほとんどがソフトウェアタイプであったが、その後専用ハードウェアによってパフォーマンスとメンテナンス性を向上させたアプライアンスが主流となった。

また IDS／IPS には上記のネットワーク型のほかにホスト型と呼ばれる製品がある。これは、監視対象となるサーバ等の OS 上に常駐して、そのマシンが授受する通信パケットやシステムの動作を監視し、異常な動きを検知して報告・警告・ログ記録、遮断等を行うものであり、その性質上、ソフトウェアタイプの製品である。ホスト IDS／IPS を略称して HIDS／HIPS とも通称される。

④アプリケーションファイアウォール

アプリケーションファイアウォールとは、ネットワークトラフィック一般を対象とするファイアウォールとは異なり、特定の装置・用途・目的に限定して通信の監視や制御を行うファイアウォールである。主なものとして、ウェブアプリケーションファイアウォール[16]がある。Web サーバの前に配置して、ウェブアプリケーションに固有の攻撃からアプリケーションを保護する目的で使われる。データベースへの攻撃やその不正利用を防ぐ目的で使われるファイアウォール型の装置もある。本調査では、これらを総称してアプリケーションファイアウォールとしている。アプリケーションファイアウォールの利用は広がりつつある。

アプリケーションファイアウォールは、前項の IDS／IPS の一種とも言える。パケットの中身に対して特定の定義に基づき制御するという点で、機能的にはほぼ IDS／IPS の定義が該当するが、そのうち、ウェブアプリケーション等特定の防御対象に特化したものを、アプリケーションファイアウォールと称するようになっており、ひとつの市場セグメントを形成するまでに至っていると考えられる。

⑤その他のネットワーク脅威対策製品

外部ネットワーク（インターネット等）から内部ネットワークに対して行われる、不正侵入、盗聴、不正プログラムの挿入等の攻撃に対して、検知、防御、抑止、警告等の防衛の機能を提供する製品で上記のどのセグメントにも属さないものを集計している。

3. コンテンツセキュリティ対策製品

「コンテンツセキュリティ対策製品」とは、コンテンツ、すなわち、ファイルやデータの内容について、その危険性の有無や、内部規定・セキュリティポリシーに対する違反等の有無をチェックすることを主目的とした製品群である。本調査では、ネットワーク通信に関して、その通信目的をコントロールすることを主目的とするものを、前述の「ネットワーク脅威対策」と定義し、通信の中身について不都合の有無をチェックすることを主目的とするものを「コンテンツセキュリティ対策」と定義した。主として外部からの脅威への対策に用いられるが、情報漏えい対策にも用いられており、大きくは以下の３つの製品群に分かれる。

１．コンピュータウイルス、スパイウェア、ボット等の不正プログラム、マルウェア等を、ファイル等の電子データや電子メール送受信・Web 閲覧等のコンピュータ通信の中から検出し、排除･無害化･警告等の対策を講じる機能を持つ製品群。

２．システム･業務･サービスの目的や適正な運営にとって有害な電子メール送受信や Web 閲覧等の通信を検査し、フィルタリング・警告･排除・ログ記録その他の対応を行う機能を持つ製品群。

３．電子メール、電子ファイル等の内容（コンテンツ）について、内部規定（セキュ

[16] WAF （Web Application Firewall）と略称する場合もある。

リティポリシー）等あらかじめ定められた条件に基づいて送配信を制限し、ログ記録その他の対応を行う機能を持つ製品群。

つまり、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。データそのものの保護については、暗号を利用することが一般的であるため「暗号製品」に分類している。

マルウェアは、出現当初はフロッピーディスク等の記憶媒体を介する感染が主流であり、電子メールの普及に伴って添付ファイルを装ったり、ファイルに付随するマクロを偽装するウイルスが猛威を振るった。電子メール添付ファイルに対する対策が進んだ結果、現在では、Web サイトにマルウェアを仕込み、そのサイトに誘導することで、ファイルのダウンロードや閲覧行為に便乗して感染するタイプが主流となっている。そして、USB メモリという記憶媒体を介するパターンも、OS の自動実行機能を悪用する形で復活している。

2009 年度の中分類市場区分からの変化として、「フィッシング対策ソフトウェア／システム」を「その他のコンテンツセキュリティ対策製品」に統合し、一方「その他のコンテンツセキュリティ対策製品」に含めていた「DLP 製品・システム（情報漏えい対策製品・システム）」を独立した市場区分とした。「フィッシング対策ソフトウェア／システム」は、フィッシングが新たな脅威として注目された 2004 年以降に専用対策製品やベンダが登場したが、その後脅威の複雑化と、それに対応する対策の複層化に伴って専用製品やシステムによる対応が限られるようになっている。標的型脅威対策も含めて総合的対策が一般化していることから、独立の市場セグメントと位置づけることは不要になったと判断した。一方、DLP 製品はやはり 2000 年代前半に登場していたが、近年参入ベンダも増加し製品バリエーションも広がって、導入事例も増えてきたことから、独立のセグメントとして統計対象とすることとした。

当市場調査においては製品区分（市場区分）を次の 7 種類にセグメント分けする。

① ウイルス・不正プログラム対策ソフトウェア（企業向けライセンス契約）／アプライアンス

ウイルス、ワーム、スパイウェア、トロイの木馬、ボット等の不正プログラムを検知し、更に防御や排除する製品。クライアントパソコンやサーバに、ソフトウェアとしてインストールして使う形が一般的で、企業等向けにライセンス契約方式で提供される。また、内部ネットワークの入り口にゲートウェイ型で設置して通過するトラフィックをチェックする使い方もある。この場合はアプライアンス型製品が利用されるケースが多い。ウイルス対策製品の特徴として、不正プログラムを検知するための一種のリストである定義ファイルを常時更新する必要があり、ソフトウェア代金の他に、この定義ファイルの更新権は年間契約で支払う形が一般的だが、その更新料もこの市場を構成する金額としてカウントする。

一方、マルウェアの種類、特に亜種の発生量が桁違いに増加しており、定義ファイルの巨大化と更新頻度を上げる必要が生じている。それは端末とネットワークの負荷

を著しくしく高めるため現実的でなくなってきている。そのため、基本的なフィルタリングは定義ファイルで行い、不振なファイルは挙動を見て判断する手法や、ウイルス対策ソフトベンダのサーバに都度問合わせて判断する方法を組合わせることが一般的になっている。後者の方法はサーバや判断機能がクラウドにあるのでクラウドサービス型アンチウイルスといった呼称も登場している。

この製品には、付加機能として、ファイアウォール、IDS、スパム対策、URL フィルタリング等の機能を併設するものが一般的であるが、最近は脅威の複雑化と深刻化から、それぞれ個別の対策製品を個別に導入する方向にあると見られる。

② ウイルス・不正プログラム対策ソフトウェア（個人ユーザ向けパッケージタイプ）

ウイルスを始めとするマルウェア対策ソフトで、個人ユーザが自宅のパソコンで使うための製品である。製品形態としては、ソフトウェアパッケージとして家電店等の店頭やオンラインショップで販売される形が主流である。またネットワーク越しに製品をダウンロードしてインストールする、オンラインダウンロード販売も増加している。①同様、プログラムや定義ファイル更新の年次参照権の販売代金も含む。また、個人向けウイルス対策製品のほとんどが、デスクトップファイアウォール、HIPS（ホスト IPS)、スパム対策、URL フィルタリング等の機能を併せ持っている。

近年、スマートフォンやタブレット型 PC と呼ばれるスマートデバイスが急速に普及している。モバイルアクセスにおいては、PC に取って代わる勢いである。クラウドコンピューティングの広がりにより、端末でのアプリケーション稼動が不要になっていることも普及に拍車をかけている。同時に、スマートデバイス上で動作するマルウェアも急速に出回っており、その対策製品も各ベンダから登場している。スマートデバイス向けマルウェア対策製品もこのセグメントで集計している。

③ スパムメール対策ソフトウェア／アプライアンス

宣伝、勧誘等の目的で無差別・大量に送りつけられる、不要もしくは有害な内容を含むメール、いわゆるスパムメールに対する対策製品。フィルタリング、マーキング（タグ付け)、警告、隔離、排除（廃棄）等の対応をする。クライアント用、サーバ用、ゲートウェイ型のタイプがあり、製品形態もソフトウェアとアプライアンスがある。

なお、スパム対策は、メールフィルタリングと同様、ISP のサービスの一環として、あるいは SaaS 型の専門サービスとして提供される形も浸透している。これらはサービス市場で集計している。

④ URL フィルタリングソフトウェア／アプライアンス

アクセスしようとするインターネット上のウェブサイトが有害、危険、不適格等と判断される場合に、そのアクセスに対して停止、警告、ログ保存等を行うソフトウェアもしくはアプライアンス製品。判断は、自社の基準により禁止するサイトを指定するブラックリスト、キーワードによるフィルタリング、ツールベンダが提供するリスト等に基づく。近年はレピュティション（評判）ベースと称し、対象となるウェブサイトに関する情報やインシデントを世界中から収集蓄積して解析し、その評価に基づく判断を行う

形が増えている。この場合はベンダのサーバに可否を問合せて判断する形が一般的となっており、クラウド型サービスという呼称も登場している。

企業向けと個人向けの両方がある。特に家庭において子供を有害サイトから守るための使われ方が関心を集めている。特にスマートフォン向けには、携帯販売会社に、年少者の利用に対して有害サイト遮断機能の紹介推奨が義務付けられており、利用は拡大していると見られる。

⑤ メールフィルタリングソフトウェア／アプライアンス

送受信される電子メールに対して、電子メールアドレスや内容、添付ファイル等を検査し、情報漏えい等の情報セキュリティ事故を防止するための製品。所定の条件（有害、不適格、情報漏えい、レピュティションサービス[17]によるリスト等）に合致（もしくは違反）する内容を含むものに対して処理（停止、隔離、警告、管理者への通報もしくは回送、ログ保存等）を行う。単に全メールを無条件にアーカイブするだけのものを除く。ウイルス・不正プログラム対策製品にこの機能が併設される場合は、ウイルス・不正プログラム対策製品に分類する。

製品形態としてはソフトウェア製品とアプライアンス製品がある。また、スパム対策と同様に、ISP または専門事業者によるフィルタリングサービスも提供されている。このサービスについては情報セキュリティサービス市場で集計対象としている。

⑥ DLP 製品・システム（情報漏えい対策製品･システム）

情報漏えい対策手段として、データそのものの存在や移動を検知して警報、通知、阻止等を行う機能を有するソフトウェア、アプライアンスまたはシステムである。メールのコンテンツやファイルに対してフィルタリングやマーキングを行い、情報そのものの動きを直接追いかけて境界外への流出をコントロールする。DLP のうち D は data の頭文字であり、L は loss、leak または leakage を、P は prevention または protection を示す。D は一意だが、L と P はベンダによって用語の選択が違う。比較的多い用法は Data Leak Prevention または Data Loss Protection であろうか。

メールフィルタリングや端末における書き込み動作等だけでは防ぎきれない情報の外部流出を、ファイルやその中のデータの特性を把握することで抑止・防止しようとする考え方の製品である。

⑦ その他のコンテンツセキュリティ対策製品

メール等の電子データに関して、主として情報セキュリティの目的でフィルタリングその他の機能を提供する製品で、上記のいずれにも属さない、あるいは特定の中分類に仕分けできないもの。

いわゆる Digital Rights Management （DRM）[18]と呼ばれる製品群があり、このセグメントに含めた。DRM とは、コンテンツの利用の態様に対してコントロールをかけ

[17] Reputation Service ウェブサイトやメールの発信源等の URL について、過去の不正行為の事例や安全に通信された実績等の情報に基づき、ウイルス対策ツールベンダや専門事業者が安全度の評価をした結果のデータベースを Reputation（英語の元の意味は評判、評価）と呼び、アクセス制御やフィルタリングに際しての判断根拠として利用する技術およびそのサービス。

[18] 一部のベンダは IRM （Information Rights Management）とも呼ぶ。

るもので、利用する人の属性、方法、時間、場所、回数等によってコントロールすることで、権利者の意図する範囲と方法での利用を担保する目的で使われる。これは内容の保護を同時に実現する場合も多いがそれが必然ではなく、暗号を伴わないケースもあることから、「その他のコンテンツセキュリティ対策製品」に含めて集計している。

4. アイデンティティ･アクセス管理製品

「アイデンティティ･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）並びにその認証システム、アイデンティティ管理システム、ログオン管理･アクセス許可システム、ディレクトリ管理システム、シングルサインオンシステム、PKI 関連システム等がこのカテゴリに含まれる。

このカテゴリの呼称については、従来「アクセス管理製品」としてきたが、2008 年度調査から「アイデンティティ管理システム」のセグメントを独立させ、カテゴリの名称を「アイデンティティ・アクセス管理製品」とした。本人認証だけでなく、認証されたユーザに対するリソースへのアクセス範囲と権限を、人事情報と連動させて管理することの重要性に対する認識が高まっている。その領域を管理するツールとして、アイデンティティ管理システムが注目され出したことに対応する変更である。

このカテゴリは、以下の 6 セグメントに区分定義している。

① 個人認証用デバイスおよびその認証システム

ワンタイムパスワード、IC カード、USB キー、携帯電話（個体識別番号含む）等を用いて本人確認する機能を提供するデバイス、およびそのシステム（生体認証を除く）等である。認証は、システムにアクセスするユーザを特定するための情報（ID）と、それ対応する認証情報（credential）を予め登録されている情報と照合することで行う。認証情報は、一般的に本人しか知らないものや本人しか持っていないものを用いる。両者の組合せによる、二要素認証を行うことも普及してきている。

IC カード、特に社員証を兼ねるものが最も普及していると推測される。より安全性が高いとされるワンタイムパスワード製品には、時刻同期方式、カウンタ同期方式、チャレンジレスポンス方式等のハードウェアタイプと、PC や携帯電話にソフトウェアをインストールするものや、Web ブラウザを利用し、位置情報やイメージ情報からワンタイムパスワードを生成するソフトウェアタイプの製品等がある。

②個人認証用生体認証デバイスおよびその認証システム

認証情報として、本人の身体的特徴の情報を用いる考え方・技術があり、独立のセグメントとして集計している。身体的特徴として実用化されているものとしては、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。これら情報の識別技術は、入退室管理に

利用され物理セキュリティ対策製品としても利用が進んでいるが、本調査では、PCやサーバ、ネットワーク等のシステムへのアクセスにおけるユーザ認証デバイスおよびシステムを対象としている。

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、セキュリティレベルを高くできる反面、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、そのデータについてはシステム的に厳格な管理が求められる。また指紋の利用等については、運用面においてもユーザの心理面への配慮が求められる。

③アイデンティティ管理製品

システム並びにデータへのアクセス権について、システムの利用者に関してはその職務や権限に基づく定義のデータベースを、システム並びにアプリケーションに関してはそのアクセス許可ポリシーを管理する機能を提供する製品群で、利用者の異動に伴う変更管理や、システム間のアクセス権の情報連携や統合管理を実現し、情報資産の利用権の即時的一元的管理を可能にする。プロビジョニング製品（ユーザ別のシステム利用権限の定義）やフェデレーション製品（異システム・異組織間のID連携、プロビジョニング連携のための製品）を含む。

アプリケーションやサーバが増加する一方、社員の流動化や従業員構成の複雑化も進んでいる。従業員の所属と職務権限に対応したアクセス権を統合的に管理するために、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、アイデンティティ管理ツールの重要性が増している。

④ログオン管理／アクセス許可製品

「ログオン管理／アクセス許可製品」は、保護対象となる情報処理資源に対してのアクセスをコントロール（管理・制御）する。自らに実装されたテーブルやアイデンティティ管理製品からの情報に基づき、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）を許可するのかを一元的に管理し、アクセスを制御する。保護対象となるのは、PCやサーバのみでなく、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、マシン名、ネットワークID、メモリ等、多岐に渡る。また、大規模なトータルソリューションとなる場合も多い。

一方、昨今発生している主なセキュリティ事故や情報漏えいの多くが、特権アカウントと呼ばれる管理者権限（WindowsのAdministrator権限、UNIX/Linuxのroot権限、データベースのsysdba等）の悪用によることから、より実効的なセキュリティ向上のために、システム本番環境や重要サーバに対する特権IDのアクセス制御・管理に特化した製品も出ている。

ユーザの利便性と一元的なポリシー管理を両立させる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）製品もこのカテゴリに含まれる。

⑤PKI システムおよびそのコンポーネント

公開鍵暗号の仕組みを応用して電子証明書や電子署名を作成し、第三者による保証と組み合わせて、ユーザの認証、文書等の真正性の証明、改ざん防止（無改ざんの確認）、否認防止等に利用する仕組みがある。Public Key Infrastructure、公開鍵基盤と呼ばれる。このセグメントには、そのような公開鍵基盤のための電子証明書の発行、管理、証明サービスを提供するシステムおよびその構成要素等の製品を含む。但し、構築サービス（SI）や電子認証サービスは情報セキュリティサービス市場に計上するものとし、このセグメントには含まない。

⑥その他のアクセス管理製品

このセグメントには、単独で製品化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等が含まれる。また、本人認証の手法として、「リスクベース認証」という方法が登場しており、このセグメントに含めている。これはアクセスしてきたユーザの PC の識別記号、地理的場所、アクセス履歴や行動パターン、予め登録された質問と答えのセット（本人しか知り得ない情報による）等を取り合わせて、高い精度で本人確認を実現するという手法で、インターネットバンキング等、IT に不慣れな人でも特定できる技術である。何をどう取り合わせれば実用目的に耐える精度が得られるかのアルゴリズムが開発されて実用化が始まっている。

5. 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、異常に対してアラート（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（いわゆるコンプライアンス管理製品）や脆弱性検査製品（いわゆるスキャニングツール）等が含まれる。

監視機能としては管理対象となるネットワークやコンピュータから出力されるログ等を取得してリモートから統合的に状態を把握し、その結果を統合表示したり、異常に対してアラートを出したりする機能を持つ。管理機能としては管理対象となるネットワークやコンピュータの構成情報、設定ポリシー等を統合的に管理し、ポリシーへの準拠性を確認する機能がある。制御機能としては自動、手動にてネットワークの接続を拒否したり、アカウントをロックしたり、ファイル等の電子データの処理を停止したりする機能がある。

この市場区分には以下の 4 種類の中分類（セグメント）を設定している。

①セキュリティ情報管理システム／製品

「セキュリティ情報管理システム／製品」区分には、セキュリティ監視・制御装置、ネットワークシステムやサーバ機器やデータベース等様々な対象に対してセキュリティ状態を総合的に管理する機能を持つ製品およびシステムを集計する。ネッ

トワークシステムやサーバから出力されるログを統合的に収集し管理する製品である SIM(Security Information Management:セキュリティ情報管理)製品、収集したログに重要度等の意味付けを行いセキュリティイベントとして管理しリアルタイムに相関関係を分析する SEM(Security Event Management:セキュリティイベント管理) 製品、あるいはそれらを統合した SIEM と呼ばれる製品等がある。ネットワークの統合管理プラットフォームの一部を構成する製品もある。

② 脆弱性検査製品

「脆弱性検査製品」は、ネットワーク機器やサーバ等に対して、ネットワーク越しにスキャニングや擬似攻撃を行うことにより、設定の不備やプログラムの不具合等の危険事項を調べ脆弱性が存在していないかを検査する製品群である。フリーウェアも含めて多くのソフトウェア製品が提供され、脆弱性スキャナーとも呼ばれている。一部にはアプライアンス製品もある。

また、同様の機能を持つモジュールを検査対象内にインストールして内部から脆弱性検査をするホストベーススキャナもある。

③ ポリシー設定管理・動作監視制御

「ポリシー管理・設定管理･動作監視制御製品」は、インベントリ管理（OS のバージョンやパッチ適用状況の情報、インストールされているアプリケーションの情報、CPU 使用率等ハードウェア情報等の収集・管理機能)、ポリシー管理（管理対象マシンにあらかじめ定められたポリシーに準拠した設定がされているかをモニタし報告する機能)、動作監視（管理対象マシンで行われたファイルの編集、更新、複写、印刷、外部記憶装置の使用等といった、情報漏えいにつながる動作や行為に対しての監視、抑制、警告、報告機能）等の管理機能を提供する製品群である。

クライアント PC 等の識別情報やインベントリ情報等に基づきネットワーク接続を管理･制御する、いわゆる「ネットワーク検疫システム」における機器認証サーバや認証エージェントをこのセグメントに含める。この機能は、ネットワークアクセス制御であり、「ネットワーク脅威対策製品」に分類する考え方もあるが、むしろ端末と位置付けられる各ユーザの PC のポリシー順守状況の管理が主眼で、それとネットワーク接続許可を連動させている構造なので、前者に注目して「ポリシー管理･設定管理･動作監視制御製品」に分類することとした。原則として単体製品またはネットワーク制御装置等のオプションとして取引対象となる製品形態のもののみを対象とし、その機能がルータ等の一部にデフォルトとして組み込まれている場合は含まない。

④ その他のシステムセキュリティ管理製品

「その他のシステムセキュリティ管理製品」は、システムセキュリティ管理製品の中で、上記セグメントのいずれにも分類されない製品の区分である。デジタルフォレンジックといわれる、セキュリティ事象や不正アクセスを追跡するために、電磁的記録の証拠保全および調査・分析を行う機能を有する製品や、セキュリティ・

内部統制管理（IT ガバナンス）等を目的としてログの収集、減量・圧縮、保管･アーカイブ、解析等を行う製品等がこれに該当する。（但し、ログ収集・解析機能を有する製品の内、リアルタイム監視を主目的とする製品は「セキュリティ情報管理システム／製品」に分類しており、「その他のシステムセキュリティ管理製品」では主に傾向解析等スタティックな目的のものを対象としている。）

情報漏えい事故等インシデント[19]発生時の追跡や内部統制管理のための取引記録の追跡可能性確保のために、適切なログ取得や管理、改ざん防止対策が必要である。大量のログを統合し統計分析を行える機能や証拠保全のためのログの改ざん防止機能を提供している製品を用いることにより、監査証跡の信頼性を確保し、管理者の負担を軽減することが可能となる。

## 6. 暗号製品

「暗号製品」とはデータ、ファイル、電子メール、ハードディスク等を暗号化する各種製品および半製品を指す。

暗号技術そのものは、PKI や 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。PKI、VPN はその使用目的から各々アイデンティティ･アクセス管理製品、ネットワーク脅威対策製品に分類しており、ここでは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、および暗号化のためのライブラリやモジュール等が含まれる。

「暗号製品」は昨年度まで、「データ暗号化製品」、「暗号化ミドルウェア」、「その他暗号製品」の３つの中分類市場を区分定義していたが、今年度調査からセグメント分けはせず「暗号製品」全体を一つの区分として調査した。「暗号製品」とはハードディスク、文書ファイル、メール、外部記憶デバイス等を暗号化することを主たる機能とする製品群や、データベースの暗号化や組み込み用暗号モジュール等が該当する。

ハードディスク暗号化製品とはハードディスク全体を暗号化するため利用者が意識せず利用することができる。そのため導入後の運用負荷が低いので導入しやすい製品といえる。また、ＰＣを持ち出した際に、紛失・盗難等が発生した時の情報漏えい対策として有効なことから、大企業や大企業と取引を行う中小企業にも導入が進んでいる。

文書ファイルの暗号化製品とはパーティション、フォルダ、ファイル単位でユーザが任意に暗号化処理をすることにより、アクセスするユーザの権限に応じて参照・更新・削除等をコントロールすることができる製品である。これにより情報の重み付けや権限外のユーザによる覗き見や漏えい防止を実現する。実際に運用する際にはユーザ側に判断や操作を求める製品が多いため、暗号化ルールや情報の重み付けルール等導入の際にはある程度の運用設計を実施する必要がある。

メールの暗号化製品とはメール本文および添付ファイルの暗号化を実現するものと添付

[19] 「インシデント」は出来事、事件のような意味。情報セキュリティに関してはウイルス感染、不正侵入、情報漏えい、秘密情報の紛失等の事件･事故･事案を総称して情報セキュリティインシデント又は単にインシデントと言う。

ファイルのみ暗号化するものとがある。メールは情報漏えいを発生させやすいポイントと考えられているため、企業のリスクと運用コストを比較し導入を検討する企業は多い。しかし既存のメールシステムの変更や運用の変更に対するコストは規模が大きいほど膨らむ傾向にあり、ニーズの強さほど市場は伸びていない。この仕組みをアプライアンス型で提供している製品やSaaS型サービスとして提供しているものもある。後者は運用管理サービス市場に分類している。

記憶デバイスの暗号化製品は記憶デバイスを接続する端末側に組み込むものとUSBメモリ等デバイス自体に暗号化の仕組みが組み込まれるものとがある。ハードディスク暗号化製品と同様、利用者への負担も軽く、外部に持ち出した際の紛失・盗難対策として有効な製品であるため、企業のニーズが高い。そのためリリースされている製品の種類も多い。

暗号化ミドルウェア、つまりは暗号化のためのライブラリやモジュールも市場の一部を形成している。通常の情報システムやネットワークを構成する機器に組み込む用途の他OEM提供されるビジネスモデルも多い。デジタル複合機[20]、ネットゲームや家電製品のネットワーク接続に際して、一定の情報を内部に暗号化し、格納する必要があるので、組込み開発の現場でも暗号製品のニーズはあり、一定の需要が存在するものと考えられる。

上記以外に、暗号ライセンス、鍵管理システム周辺製品、電子割符や電子透かし等の暗号製品もある。

なお、情報漏えい対策、内部統制対策として用いられる事が多いDRM（Digital Rights Management）と呼ばれる製品群は、暗号技術を応用している場合がほとんどだが、本調査では「セキュアコンテンツ管理製品」と位置付けており、「暗号製品」には含めていない。

### 6.3. 情報セキュリティサービス市場の定義に関する説明

「情報セキュリティサービス」市場には、情報セキュリティ対策を構築・実践し、情報セキュリティソリューションを実装し機能させ活用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、国内で事業を行うサービスプロバイダ（サービス提供事業者）から、情報セキュリティサービスとして提供されているものを対象とした。カテゴリとしては、「情報セキュリティコンサルテーション」、「セキュアシステム構築サービス」、「セキュリティ運用・管理サービス」、「情報セキュリティ教育」、「情報セキュリティ保険」の5区分とした。

1. 情報セキュリティコンサルテーション

「情報セキュリティコンサルテーション」とは、情報セキュリティに関するポリシー、システム、運用体制の構築を支援するサービスである。情報セキュリティ対策は、情報資産のリスク管理を目的とするところから、単にITシステムへの脅威対策といった技術的領

[20] 複写機にファクス、スキャナー、プリンタの機能を付加したマルチ用途のものをデジタル複合機（MFP, Multi-Functional Printer）と呼びならわしている。複写機の基本構造はスキャナーで読み取ったイメージをプリンタで紙に出力するものであるが、それをデジタル処理にすることでコンピュータによるデータ処理と同等のプロセスとなり、ネットワーク機能とファクス機能、更にデータ蓄積機能を持つことで多彩な複写、印刷機能を提供するようになっている。蓄積機能とネットワーク機能、ネットワーク越しに離れた場所で紙に出力されたものの物理的管理の問題等から、新たな情報セキュリティのフロンティアとしても浮上している。

域にとどまらず、経営資源と位置付けられる情報資産に関する経営のリスクコントロールという視点に基づく必要がある。従い、経営管理と技術方針を包含する、専門性が高く、多様性を伴う分野である。

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、情報セキュリティマネジメントシステム認証制度等客観的な規格要件の認証取得を目指す企業が多い。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ている。一方、こうした規格適合性を審査し、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。

「情報セキュリティコンサルテーション」市場は、大別すると、マネジメント系、診断・監査系、認証取得系に分けることができる。これを、以下の 5 つのセグメントに区分して調査集計している。

① 情報セキュリティポリシーおよび情報セキュリティ管理全般のコンサルテーション

今年度調査から「情報セキュリティポリシー構築支援」と「情報セキュリティ管理全般のコンサルテーション」を統合して 1 セグメントとした。マネジメント系セグメントは当市場 1 つである。主に情報セキュリティポリシーの策定やコンプライアンス対応施策、情報保護対策全般がサービスの中心となる。

情報セキュリティポリシーの策定では、会社の基本方針や情報セキュリティ対策の基準、実際の運用ルールや処理手順等を体系的に整備することを支援する。更に、情報セキュリティ管理全般のコンサルテーションでは、推進組織や責任体制、IT も含めた情報セキュリティの基本枠組であるアーキテクチャの設計開発まで全般にわたって支援を提供する。

② 情報セキュリティ診断・監査サービス

診断・監査系サービスは当市場区分で集計している。

経済産業省告示により、情報セキュリティ監査制度が制定され、情報セキュリティ監査の枠組みを提供している。実際の運用と推進は NPO 日本セキュリティ監査協会に委ねられ、同協会が認定する公認情報セキュリティ監査人が中心となって監査を提供している。ISMS 認証取得企業の内部監査を外部のコンサルタントが実施あるいは支援を行うサービスもある。監査という枠組みによらず、自社の基準やサービス事業者の推奨基準に基づく情報セキュリティ診断を受けるケースも多い。また外部の第三者による委託先に対する監査もある。更に、情報セキュリティ対策がどこまでできているかを絶対基準に基づき評価して評点をつける、情報セキュリティ格付けも行われている。

このような、情報セキュリティ管理に関する監査や診断を専門サービスとして提供するのが「情報セキュリティ診断・監査サービス」である。なお、同じ「診断」「監査」という語を用いても、もっぱらシステムの技術的脆弱性の診断・評価を行うサービスもある。これはマネジメントシステムに対する評価とは異質であり、プロフェッショナルサービスと位置付けて、本調査では、「セキュリティ運用・管理サービ

ス」の１セグメントとして区別して集計している。

③ 情報セキュリティ関連規格認証取得等支援サービス

認証取得系については、企業が認証を取得するための支援を提供するサービスと、その審査・認証を実施し認証証を交付するサービスの両面がある。

当セグメントが対象とするのは、前者の規格適合性の認定、認証の取得を支援するサービスである。規格・基準の適合性認定には、一定のモデルもしくはパターンがあり、それに沿ったルールや書式や体制を構築し、審査に耐える運用、特に PDCA サイクルをうまく回すことが必要となる。その専門的ノウハウを提供し、企業の認証取得を支援するのがこのサービスである。マネジメントシステムの構築と PDCA サイクルの実施を支援し、審査のサポートや取得後の運用の支援等も行う。

④ 情報セキュリティ関連認証・審査・監査機関（サービス）

このセグメントは、認証を提供する側のサービスである。情報セキュリティ関係の認証の主なものとしては、ISMS（Information Security Management System、情報セキュリティマネジメントシステム）認証と、プライバシーマークの認定がある。各々、認定機関に認定された認証機関が審査し、認証する。ISMS は JISQ27001（国際規格である ISO/IEC27001 と同等）に基づいて適合性を認証する制度で、認証機関が審査する。認証機関を認定するのは、日本においては公益財団法人日本適合性認定協会（JAB）と一般財団法人日本情報経済社会推進協会（JIPDEC）がある。

プライバシーマークは、JIPDEC が直接審査し付与するケースの他に、業界団体等が JIPDEC の指定審査機関として審査し、その結果に基づいて JIPDEC が付与するケースがある。基準は JISQ15001 である。

関連する認証として、IT サービスマネジメントシステム（ITSMS）や事業継続マネジメントシステム（BCMS）の構築、認証も行われるようになっている。

⑤ その他の情報セキュリティコンサルテーション

この他、これらが複合した需要や個別ニーズに沿ったコンサルティング、企業独自のメニューや体系をパッケージ化したサービス等がある。また、内部統制管理、特に IT ガバナンスの主たる要素である情報セキュリティガバナンスに関する構築や診断、事業継続管理や IT サービスマネジメントに関連して情報セキュリティに関するコンサルテーションを提供するサービスがある。それらを「その他の情報セキュリティコンサルテーション」というセグメントで集計している。

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、システム構築におけるセキュリティ面の設計や運用について、現状分析、ポリシー、製品選定、情報更新等、専門的な見方から、ソリューションを提供する。IT セキュリティシステムの設計、仕様策定といった上流工程から、セキュリティ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およびハードウェ

アの選定、導入、設定等の現場に近いサービスまでが含まれる。主にネットワークインテグレータ、システムインテグレータによりサービス提供がおこなわれる。

このカテゴリは以下の4種類の中分類（セグメント）にて市場区分を行なった。

① 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・仕様策定」は、IT システムを構築するにあたりセキュリティに関しての設計、仕様の定義を実施するサービスである。システム設計時にセキュリティ対策についてセキュリティ専門家による支援を提供する。また、既存のシステムに対してセキュリティ面を付加するまたは向上させるための対策を設計するニーズもある。

② IT セキュリティシステムの導入・導入支援

「IT セキュリティシステムの導入・導入支援」は、システムのセキュリティに関する部分の構築に際して、セキュリティ製品等を導入し、システムを構築、あるいは、その支援をするサービスであり、セキュリティに関するインテグレーション・エンジニアリングサービスと言える。この市場もまた、情報セキュリティ対策の実施やセキュリティレベル向上という目的のためには、専門家によるセキュリティアーキテクチャの適用が必要だという認識が浸透することで、大きな需要を形成している。

③ セキュリティ製品の選定・選定支援

「セキュリティ製品の選定・選定支援」は、顧客のポリシーや要求に基づいて、それに適したセキュリティ対策製品の選定またはそのための情報提供等の支援を行うサービスである。セキュリティ対策は、システムの利用目的と設置･利用環境をにらんで必要な機能を適正に配置する必要がある。そのため、セキュリティ製品の導入に際して、セキュリティの専門家による製品選定や製品の比較評価のサービスを活用するニーズが存在する。

④ その他のセキュリティシステム構築サービス

上記 3 セグメントに当てはまらない IT セキュリティシステムの構築サービスを「その他のセキュアシステム構築サービス」とした。例えば SI 事業者が行うセキュリティ対策製品の設定や保守、診断等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」市場は､大別してマネージドセキュリティサービス、プロフェッショナルセキュリティサービス、電子認証サービスに分けられる。

マネージドセキュリティサービスは､IT セキュリティシステムまたは IT システム上のセキュリティ対策機器等の運用や管理の支援を行い、システム、サーバ、ネットワーク状態等の監視を行う、いわゆる運用支援サービスである。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形態が中心で、その監視対象別に「セキュリティ総合監視･運用支援サービス」「ファイアウォール監視･運用支援サービス」「IDS／IPS 監視･

運用支援サービス」「ウイルス監視･ウイルス対策運用支援サービス」の 4 セグメントを定義した。またスパム対策や有害ウェブフィルタリングをアウトソースサービスとして提供するビジネスモデルの拡大に対応して「フィルタリングサービス」を今年度から独立セグメントとした。この一部は従来「ウイルス監視･フィルタリング・運用支援サービス」としてウイルス監視と同一セグメントに分類していた。

プロフェッショナルサービスには、ネットワークからの攻撃に対する弱点を検査する「脆弱性検査サービス」、セキュリティに関する脆弱性やインシデント、ネットワーク攻撃の傾向や趨勢等の予防的情報を提供し外部脅威に対するセキュリティ対策をサポートする「セキュリティ情報提供サービス」、何らかの事故等が発生した場合の対応を引き受けたり支援したりする専門家のサービスである「インシデント対応関連サービス」がある。

電子認証サービスは、個人の認証を第三者が発行する電子証明書によって行う PKI（公開鍵基盤）や、Web サーバの実在性・信頼性を保証する SSL[21]サーバ証明に用いられる電子証明書の発行を行うサービスである。文書の完全性・真正性の証明や否認防止、時刻の証明であるタイムスタンプ等にも用途が広がっている。

これに電子認証サービスと「その他」を加え、10 という大きな数のセグメント（中分類市場区分）を設定した。各セグメントの概要は以下の通りである。

① セキュリティ総合監視・運用支援サービス

企業はネットワークに対してファイアウォールや IDS／IPS を設置し、ネットワークシステム上で起こる異常を検知し対策に努めているが、サーバのログ等も含めて総合的に監視し判断をする必要がある。それにはネットワークの知識を十分に持ち、また攻撃や異常状態に関する経験や知識を必要とするが、一般企業ではそれだけの人材を確保したり配置したりすることは容易ではない。

そこで、セキュリティ専門企業がそのノウハウを生かして監視を行い、異常発生時には対応の支援も提供するサービスが提供されている。SIM／SEM や統合型ネットワークセンサを活用して総合的な監視を提供するものがセキュリティ総合監視・運用支援サービスである。

② ファイアウォール監視・運用支援サービス

①と同じサービスをファイアウォール専用に提供するサービスである。

③ IDS／IPS 監視・運用支援サービス

①と同じサービスを IDS／IPS 専用に提供するサービスである。

④ ウイルス監視･ウイルス対策運用支援サービス

①と同じサービスをウイルス・マルウェア対策製品専用に提供するサービスである。

⑤ フィルタリングサービス

電子メールを通じての情報漏えいの防止には、アウトバウンドの全てのメールをスクリーニングする必要があるが、企業が自ら実施するのはシステム面と管理負荷

[21] SSL: Secure Socket Layer　暗号通信の一方式。

の面から現実的でない。インバウンドのメール対策としてはスパムメールの排除がセキュリティ面と事業効率面で必須だが、これも多大な負荷を強いる事態となっている。それらを専門家が専門システムを用いてサービスとして提供するモデルが普及している。本調査では、そのようなサービスをフィルタリングサービスとして調査集計対象としている。なお、このセグメントは 2008 年から独立させた。

⑥ 脆弱性検査サービス

ネットワークシステムやウェブサービスは、構築した側では発見しきれない、隠れた脆弱性を内蔵している可能性が強い。それに対して、ハッカーの視点とスキルを持って擬似攻撃を仕掛けることで脆弱性を発見し、対策を指導することで被害を未然に防ぐ支援を提供するのが「脆弱性検査サービス」である。ペネトレーションテスト（侵入検査。更に縮めてペンテストとも言う。）とも呼ばれ、特定のスキルを持った専門家を擁する企業が専門サービスとして提供している。

また、ネットワーク越しに外から実施する、いわゆるブラックボックス検査のほかに、システム構成図やアプリケーションのソースコードを解析して隠れた弱点を発掘する、ホワイトボックス検査も提供されている。

プロフェッショナルサービスとしての脆弱性検査サービスはあくまで技術的な検査を集計対象としており、マネジメントシステムに対する監査・診断といった評価は、本調査では「情報セキュリティコンサルテーション」サービスの一部として取り扱っている。

⑦ セキュリティ情報提供サービス

「セキュリティ情報提供サービス」は世界中のネットワークの状態を監視、あるいは専門サイトを巡回して情報を収集し、それらを解析してネットワークからの攻撃の予報や警報、傾向分析と対策等を地域別、業種別、時期や時間帯別等きめ細かく提供するサービスで、IT が事業上極めて重要な企業等の組織に提供されている。

また OS やアプリケーションの脆弱性情報や他の場所で発生したインシデントの情報も、解説や推奨対策を付加して提供している。

⑧ 電子認証サービス

「電子証明サービス」は公開鍵暗号技術を応用して公開鍵と秘密鍵のペアで本人性、真正性、無改ざん等を証明するための電子証明書を発行するサービスである。電子証明書の仕組みは PKI（Public Key Infrastructure、公開鍵基盤）とも呼ばれる。

⑨ インシデント対応関連サービス

「インシデント対応関連サービス」はハッキングや情報漏えいといった情報セキュリティインシデントに際して、その対応や原因分析、事後対策等を専門家のノウハウを駆使して支援する専門サービスである。コンプライアンス対応や内部犯行事例の増加に伴い、電子的証拠の収集・解析・保全も必要度が高まっており、そのようなデジタルフォレンジック対応のサービスも提供されるようになってきた。

⑩ その他の運用･管理サービス

これらのセグメントのいずれにも属さない IT セキュリティに関する専門家による運用・管理サービスを「その他の運用･管理サービス」として集計する。SI 事業者が提供する製品の保守やサポート等が含まれる。また、PC 等の安全な廃棄や、逆に破損・焼損・浸水等したハードディスク等からのデータの復元サービス等も需要が増している。これらの特殊なサービスもこのセグメントで集計している。

4. 情報セキュリティ教育

情報セキュリティ対策部門、情報システム管理部門、システム開発部門、システム構築・運用部門等の部門は、情報セキュリティの専門知識・スキル・資格の習得が必要な部署である。ISMS 認証取得企業やプライバシーマーク認定取得企業は、全社員に対する情報セキュリティ教育の定期的・継続教育を実施しなければならない。金融商品取引法に基づく内部統制報告・監査制度（日本版 SOX 法）の施行に伴うコンプライアンス関連教育は欠かせないものとなっている。これらの教育は、それぞれ専門知識を必要とするために全てを自社内で対応することは不可能で、必然的に外部の専門サービスを利用することになる。特に、情報セキュリティ技術は進化が激しく教育のために専門家の知識は不可欠となる。本調査では、これら情報セキュリティ専門家や専業ベンダより提供される教育サービス、e - ラーニングサービス、資格認定教育サービス等が集計の対象となる。

「情報セキュリティ教育」市場は、従来「情報セキュリティ教育の提供サービス」、「情報セキュリティの e - ラーニングサービス」、「情報セキュリティ関連資格認定および教育サービス」、「その他の情報セキュリティ教育サービス」の４つの中分類市場（セグメント）に分類していたが、今年度から「情報セキュリティ教育の提供サービス」に「情報セキュリティの e - ラーニングサービス」を統合し、3 区分とした。e-ラーニングが教育手段として一般に浸透したことと、外部サービスとしての提供は限定的範囲にとどまることによる。

各セグメントの概要は以下の通りである。

① 情報セキュリティ教育の提供サービス

「情報セキュリティ教育の提供サービス」は、教育コンテンツのみを提供して教育実施は客先社内で実施するケースと、教育実施まで一貫して提供するサービスの両方を含めている。情報セキュリティのコンテンツの開発・作成・提供のみを行うサービスは、教育の中身そのものをテキストやデジタルファイル等のコンテンツとして提供するサービスである。教育コンテンツ開発・作成から教育の実施まで一貫して行うサービスは、専業ベンダの教育施設に出向いて教育を受ける集合研修型の「通学授業」と講師が客先に出向いて教育を実施する集合研修型の「出張授業」がある。また、専業ベンダが開発したコンテンツに基づく情報セキュリティ技術分野別のカリキュラムと個別教育コースを標準的な公開講座として受講者を募集する「レディメイド」教育と、客先個々の教育ニーズに対してコンサルティング（教育

目的、目標とそれを達成するための課題、問題点の抽出と解決策等の提供）を行い、受講者のレベルを考慮したコンテンツや育成プログラムの開発と実施を行う「テーラーメイド」教育のビジネスモデルがある。

外部の専業ベンダがコンテンツを Web ベースで提供する e - ラーニングサービスもある。インターネットに接続できる環境さえあれば、いつでもどこでも一定期間内の都合のよい時間に受講者が自分のスケジュールに合わせて受講が可能で、受講可能時間に合わせ途中で受講を止め、後日続きを再開することもできる。管理者も受講者全員の進捗を Web ブラウザ等を通してリアルタイムに把握（可視化）でき管理できる。また、集合研修より総合的に費用を抑えられるメリットも大きい。e-ラーニングのコンテンツ開発・提供サービス面では、紙芝居的なテキストベースの電子版型から、講師の講義の動画提供型や講師による講義のリアルタイム動画配信によるサービスもある。更に Web の特性を活かして遠隔の受講者との質疑応答ができる対話（インタラクティブ）型サービスも生まれ、e - ラーニングサービスの利用を促進する要因となっている。

② 情報セキュリティ関連資格認定および教育サービス

「情報セキュリティ関連資格認定および教育サービス」は、情報セキュリティに関連する各種資格認定と認定資格取得のための専門的な教育を提供するサービスである。特定の製品ベンダに偏らない世界標準の情報セキュリティ認定資格取得技術者の世界的な需要の高まりを受け、国内でもその必要性の認知が進んでいる。

③ その他の情報セキュリティ教育サービス

その他、以上に当てはまらない、教育コンテンツの開発・作成を伴わず、単に講師を派遣するサービス等を「その他の情報セキュリティサービス」とした。また、特定の情報セキュリティ対策製品に関する解説や訓練を第三者が有料で実施する教育サービスもこのセグメントに含む。

5. 情報セキュリティ保険

ウイルスや不正アクセスによる被害並びに情報漏えい等による損害を賠償するタイプの損害保険商品が複数の保険事業者から提供されるようになった。需要側としても、リスク対策の一手段としてリスクの移転を採用する機運が高まっており、IT 保険、ネットワーク保険と共に、あるいはその一部として、情報セキュリティ保険が市場の認知を得ていると見られる。本調査では、これを情報セキュリティサービスの１カテゴリとして調査集計対象とした。

なお、本調査では、原則として、情報セキュリティを付保対象とする情報セキュリティ保険（コンピュータ保険等の一部である場合にはその部分のみ）を集計対象としている。情報セキュリティも、システムインテグレーションにおけるセキュリティの組み込みが一般的に所与の要件となり、その部分を特段計算したり分別集計したりする要素が減っているのと同様に、IT リスク全体の一部として IT システム保険商品に組み込まれたりオプション扱いに

なったりして、情報セキュリティに特化する形での市場形成という認知の度合いは弱まってきている。

# 第７章 情報セキュリティ市場参入事業者の業態と産業構造

情報セキュリティのためのツール・サービスは上に見たように多岐にわたることから、それを供給する事業者も多岐にわたり、また業態についてもバリエーションが多い。本調査では、約 400 社弱を集計対象としているが、その情報セキュリティ事業におけるビジネスモデルをいくつかのパターンに類型化している。この区分を導入することにより、市場参入者の立場による分布を見ることができると同時に、流通構造上の数値計上の重複を回避する参考に役立てている。また、市場の将来予測においても、流通機能の持つ役割の面から成長度合を加減するに際して有効なパラメータの役割を果たしている。

以下、その概要について述べる。

## 7.1. 情報セキュリティ市場参入事業者の業態区分

本調査で設定している情報セキュリティ事業者の業態区分は以下の通りである。

A：海外メーカまたはその日本法人
B：国内のセキュリティツールメーカ
C：販売店･商社等主として流通機能の企業
D：SI・NI[22]機能を有する二次･三次販売店
E：SI が主たる付加価値の大手システムインテグレータ
F：コンサルティング企業
G：セキュリティサービス提供事業者
H：その他

以下、各々の業態の概要を記す。

A　海外メーカまたはその日本法人

海外メーカとは、情報セキュリティ製品の開発製造販売元である海外のメーカを指している。日本に製品やサービスを提供する海外メーカの多くは、日本に子会社となる法人を設立している。支店の形で拠点を設ける場合もある。また自ら日本に組織を持たず、日本国内のパートナーを販売代理店として製品・サービスの提供をする場合もある。直接進出をする場合も、国内での販売・流通の多くを国内の販売パートナーに依存する形態が一般的である。日本の流通構造は複雑で既存の取引関係が重視されることや、直接人対人のコミュニケーションが重視されることから、すでに販売ネットワークを持つ国内企業との提携が合理的だからである。

B　国内のセキュリティツールメーカ

セキュリティ製品がネットワーク脅威対策製品中心だった時期は海外メーカへの依存度が極めて高かったが、個人認証や端末のポリシー管理関連、暗号製品の分野では国内の

[22] NI：Network Integration, ネットワーク構築

セキュリティツールメーカの台頭も目立つ。参入例の多くは国内のベンチャー系ソフトウェアハウスやシステムハウスである。一部に大手製造事業者やその関連会社の参入もあるが、それら事業者の事業の主体がシステムインテグレーション等であるケースが多いので、本統計ではDまたはEに区分している。

国内のセキュリティツールメーカの流通構造は、一部を除き、販売パートナー経由でエンドユーザに提供するパターンが一般的である。海外メーカと同様に既存の販売ネットワークに依存するモデルが多い。また、国内の大手システムインテグレータに標準取扱製品の認定を受けることで、その販路に乗って製品供給を拡大するケースも多く見受けられる。

C　販売店・商社等主として流通機能の企業

日本国内の流通構造においては、総合商社や専門商社が海外製品のみならず国内製品についても重要な役割を果たしている。IT 関連の部品や製品も、多くはその流通機能に依存しており、セキュリティ製品も例外ではない。

セキュリティ製品の場合、特に海外メーカの製品のウェイトが高いことから、輸出入を主要事業とする総合商社や、その子会社として特定分野で小回りを利かせる技術商社が国内総代理店的な立場で取り扱うケースが多い。また、独立系でも特定分野に特化した業態の専門商社あるいは技術対応能力を備えた技術商社が活躍する事例も多い。IT分野では、電機メーカの販売代理店を出発点として技術対応能力も備える販売特化型の企業もある。

D　SI・NI 機能を有する二次･三次販売店

区分Eで定義する大手システムインテグレータは、規模別、分野別、ソリューション別等に細分して、あるいはコスト構造対策から、多くの SI 子会社を抱えるケースが多い。それら子会社は、システム構築における差別化戦略として、セキュリティ対策製品で特徴あるものを、二次･三次の販売店として、あるいは一次代理店として取り扱うケースが多い。二次店といっても、海外メーカの場合、一次店は流通に特化した卸売専念型のケースもあり、技術サポートやインテグレーションを必要とするケースの多いセキュリティ製品においては、流通の中核的機能を担う部分とも言える。

この区分には、前項に記した技術商社系で SI や NI に軸足を置く業態や、次項「SI が主たる付加価値の大手システムインテグレータ」の子会社、電機以外の製造業のシステム子会社から発展したSI事業者、独立系の中堅SI事業者等が入る。背景も多彩なことから、この区分に属する企業数は他の区分に比べて多い。また、SI の中でセキュリティ製品を取り扱うことから、その周辺の付加価値サービスや、情報セキュリティ関連サービスを併せて提供するケースも多い。

E　SI が主たる付加価値の大手システムインテグレータ

メインフレームコンピュータを製造するような大手の電機・通信メーカは、その IT 事業の主力がシステムインテグレーションになってきている。大手の通信事業者も、通信ネ

ットワークと IT がシステム的に一体化の要素を強めるのに対応して、自らあるいは子会社形態でインテグレータ機能を強化している。更に、データ処理サービス系等を源流とする独立のシステムインテグレーション専業の準大手・中堅企業群がある。

これら業態は、システムインテグレーションの中でセキュリティ製品を取り扱うと共に、その周辺のサービスや、システムセキュリティの設計・構築、更にはそれらの基本となる上流コンサル等のサービスも提供している。またシステムに関する総合力を要求されることから、セキュリティツールに関しては自社の標準取扱製品だけでなく、自グループ内の他社の取扱製品も含めて幅広く品揃えする傾向にある。

F　コンサルティング企業

経営コンサルティング企業が情報セキュリティに関してもコンサルティングを行うケースが以前からある。独立系の経営コンサルティング企業、大手企業グループの調査部門等を母体とするシンクタンク、会計監査法人がサービス提供のために別会社化している経営コンサルティング企業等が、情報セキュリティに関してもマネジメント支援を提供するケースが一般的である。

情報セキュリティは情報資産に関わるリスクを取り扱うが、情報資産は経営管理に直結する要素が強いので、両者の間に親和性があると言える。リスク管理の一環としての情報セキュリティ対策の導入という位置付けである。特に内部統制報告制度が制定されて以降は、IT ガバナンスの一環としての情報セキュリティ管理という位置付けがより見えるようになり、内部統制体制構築面での支援もセキュリティコンサルティングとして提供されるようになっている。

G　セキュリティサービス提供事業者

セキュリティサービスに特化した、あるいはそれを事業の主体にした業態の事業者である。コンサルティングサービスや運用・管理サービスの領域で専門的サービスを提供するケースが多い。ISMS やプライバシーマーク等の認証取得支援コンサルティング、システム構築やセキュリティ製品評価等の導入支援、ファイアウォール等の運用管理アウトソーシング、脆弱性検査やインシデント対応等のプロフェッショナルサービスの各領域に特化し、あるいはそれらのいくつかを取み合わせて、専業に近い業態で事業展開している。従い、企業規模は小さいケースが多い。

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

H　その他

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

### 7.2. 業態区分と市場区分における分布

上記による業態区分と、市場分類との組合せによる、集計対象企業の分布は、表 19 に示す通りである。全体の傾向としては、製品を自ら製造・供給する「ベンダ」は特定の市場に特化する傾向が強く、流通事業者やシステムインテグレータは幅広くツール・サービスを取り扱っている。

業態別に集計対象となる事業者の数が多いのは「SI・NI 機能を有する二次･三次販売店」である。これに次ぐのが「国内のセキュリティツールメーカ」と「セキュリティサービス提供事業者」である。参入企業数はそれほど多くないが、「SI が主たる付加価値の大手システムインテグレータ」は事業規模が大きく、市場に与える影響も大きい傾向がある。

市場区分別に供給事業者の数をみると、「コンテンツセキュリティ対策製品」「情報セキュリティコンサルテーション」「セキュリティ運用・管理サービス」の供給事業者が多く、「ネットワーク脅威対策製品」「アイデンティティ・アクセス管理製品」「システムセキュリティ製品」がこれに次ぐ。製品やサービスのバリエーションの多い市場区分ほど参入事業者の数が多い傾向がうかがえる。

なお、ツールだけかサービスだけか両方を提供するかの区分について見ると、ツールだけでサービスは提供しない事業者が 122、サービスのみに特化する事業者が 103、両方を提供する事業者が 139 と、各区分のばらつきはそれほど大きくない。ただし、業態区分との組合せで見ると、表 19 の（参考）から明らかなように、ビジネスモデルとの対応関係ははっきりしていると言える。

**表 19　国内情報セキュリティ市場推計対象企業およびその分布**

| 国内情報セキュリティ市場<br>推計対象企業数と分布 | 対象企業業態区分 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 海外ベンダ/日本法人 | 国内ベンダ | 流通・販売業者 | SI/NI機能ありの二次・三次販売業者 | 大手システムインテグレータ | コンサル会社 | サービス提供事業者 | その他 |
| | 合計 | A | B | C | D | E | F | G | H |
| **調査推計対象**（含:アンケート回答129件） | **367** | 47 | 69 | 38 | 80 | 38 | 21 | 60 | 14 |
| **有効推計対象** | **365** | 47 | 69 | 38 | 79 | 38 | 21 | 60 | 13 |
| **情報セキュリティツール全体（X）** | **261** | 47 | 63 | 36 | 64 | 28 | 4 | 15 | 4 |
| 統合型アプライアンス | **72** | 5 | 6 | 13 | 22 | 19 | 2 | 3 | 2 |
| ネットワーク脅威対策製品 | **125** | 24 | 12 | 19 | 36 | 22 | 2 | 8 | 2 |
| コンテンツセキュリティ対策製品 | **146** | 20 | 30 | 23 | 39 | 22 | 2 | 8 | 2 |
| アイデンティティ・アクセス管理製品 | **129** | 12 | 24 | 21 | 43 | 21 | 2 | 5 | 1 |
| システムセキュリティ管理製品 | **130** | 21 | 17 | 24 | 38 | 18 | 3 | 8 | 1 |
| 暗号製品 | **83** | 9 | 12 | 13 | 28 | 18 | 1 | 0 | 2 |
| **情報セキュリティサービス全体（Y）** | **242** | 10 | 29 | 17 | 66 | 33 | 21 | 57 | 9 |
| 情報セキュリティコンサルテーション | **149** | 5 | 8 | 7 | 41 | 24 | 18 | 43 | 3 |
| セキュアシステム構築サービス | **118** | 5 | 8 | 7 | 46 | 31 | 6 | 15 | 0 |
| セキュリティ運用・管理サービス | **144** | 8 | 19 | 13 | 45 | 22 | 8 | 26 | 3 |
| 情報セキュリティ教育 | **85** | 5 | 3 | 5 | 18 | 17 | 7 | 26 | 4 |
| 情報セキュリティ保険 | **13** | 0 | 0 | 1 | 1 | 5 | 1 | 1 | 4 |
| （参考） | | | | | | | | | |
| **ツール専業（X∩^Y）** | **122** | 37 | 42 | 21 | 14 | 2 | 0 | 3 | 3 |
| **ツール・サービス兼業（X∩Y）** | **139** | 10 | 21 | 15 | 50 | 26 | 4 | 12 | 1 |
| **サービス専業（^X∩Y）** | **103** | 0 | 8 | 2 | 16 | 7 | 17 | 45 | 8 |

### 7.3. 情報セキュリティ産業の産業構造

IPA は、2011 年 9 月 30 日に「情報セキュリティ産業の構造と活性化に関する調査」の報

告書[23]を公表した。その中で、日本の情報セキュリティ産業におけるベンダの分布と流通における物やサービスの流れの図解を掲載している（実際には 2010 年 1 月 28 日公表の「情報セキュリティ産業の構造に関する基礎調査」が初出）。図 26～28 に引用する。

これによると、製品供給においては、特にネットワーク脅威対策製品やコンテンツセキュリティ対策製品の分野で海外ベンダの存在が大きく、日本企業の活躍が目立つのは URL フィルタリングやポリシー管理・設定管理・動作監視制御製品等の特定領域に限られる傾向がある。また、

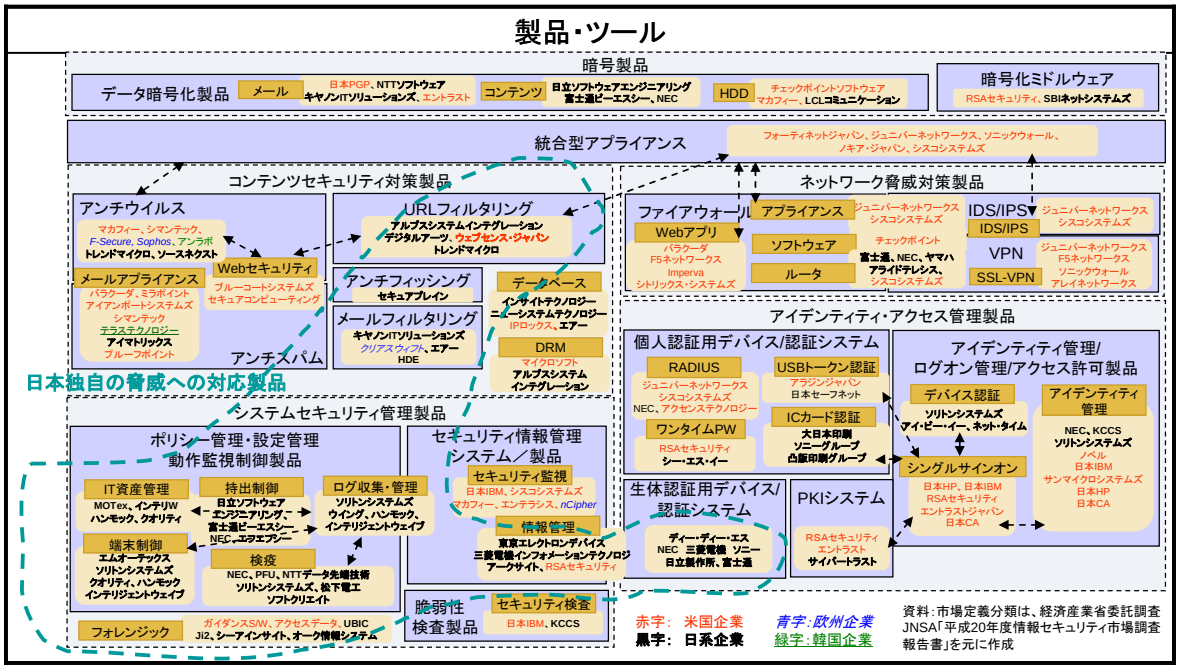
これらの分析を踏まえて、日本の情報セキュリティ産業の特性として、以下のようにまとめている。

① 製品供給において一部分野を中心にアメリカ企業の参入数が多い。

② 日本の市場規模約7000億円の一方、日本で事業を営む情報セキュリティ関連の事業者の事業規模は1社あたり約19億円と小規模である。日本で比較的大手である情報セキュリティ事業者の年間売上はトレンドマイクロを除けば40 ～70億円規模である。一方、米国ではシマンテックが5500億円、マカフィーが1800億円の売上規模である。

③ システムインテグレータが流通や情報セキュリティシステムの構築・実装・運用に占める役割が大きい。

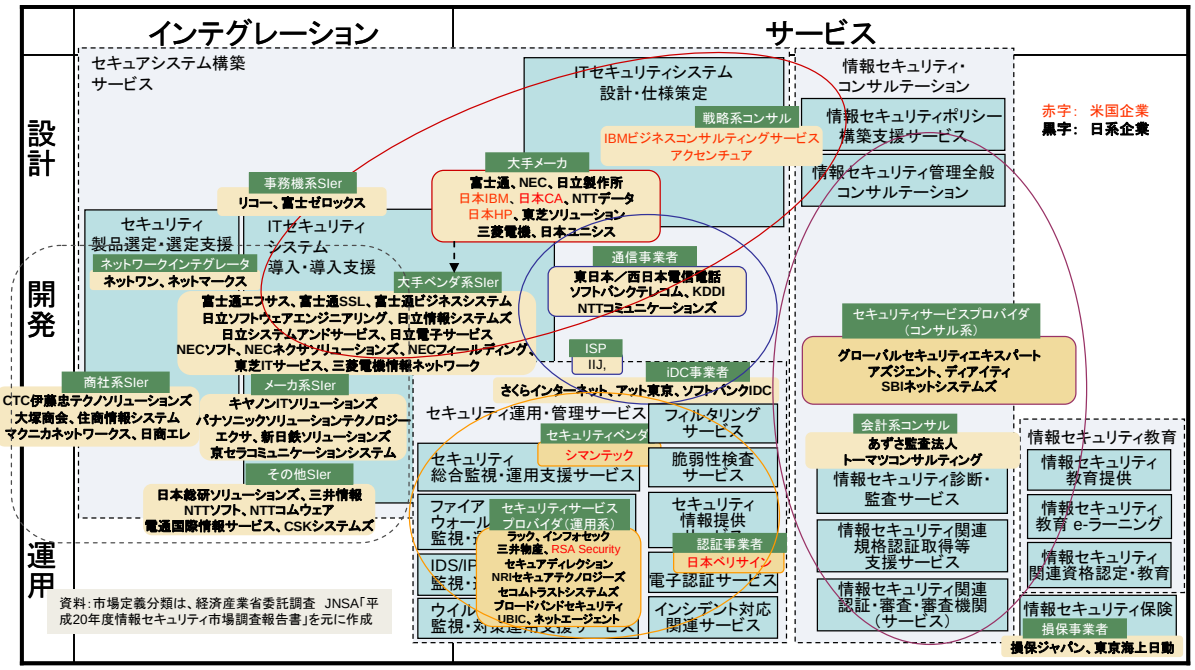
**図 26　日本の情報セキュリティ産業の機能構造－製品・ツール**




（出典：　IPA「情報セキュリティ産業の構造と活性化に関する調査」）

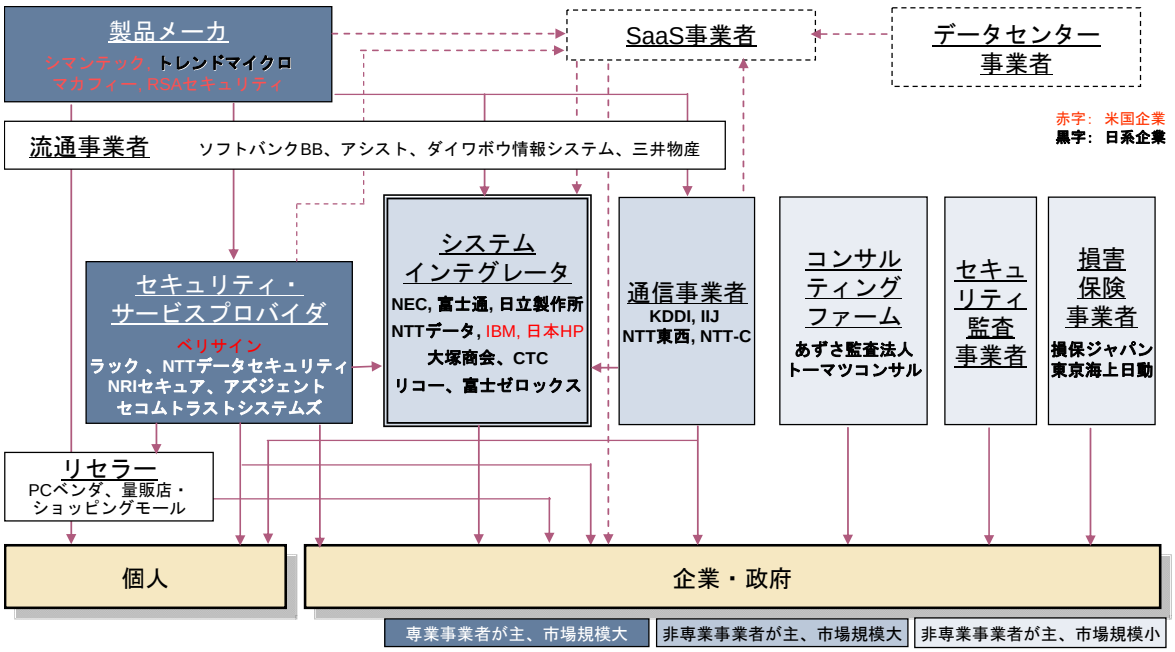
[23] http://www.ipa.go.jp/about/press/20110930.html

図 27　日本の情報セキュリティ産業の機能構造－サービス




（出典：　IPA「情報セキュリティ産業の構造と活性化に関する調査」）

図 28　日本の情報セキュリティ産業の役割構造




（出典：　IPA「情報セキュリティ産業の構造と活性化に関する調査」）

IPA によるまとめでは、日本の情報セキュリティ産業における 1 社平均の売上高規模は 19.0 億円としている。これは本調査の 2009 年度報告書によるものである。この計算を、改めて行ってみると以下のとおりである。

今回市場規模推計作業の対象としたのは、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 365 社である。2009 年度の推定市場規模は 6,821 億円なので、単純計算をすれば、1 社平均の売上高規模は 18.7 億円となる。2008 年度から、市場が縮小した分小さくなり、2%程度の縮小となっている。2009 年度の本調査の報告書でも指摘したとおり、「全てが情報セキュリティ専業ではなく、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 20 億円を切るレベルでは、事業採算性を考えた時に、研究開発投資や人材育成等の面に十分に資金を割けない。特に製品の開発や検証に際して、ベンチャー企業への支援の仕組みの整備は課題となる可能性が高い。」と言える。

# 第８章 情報セキュリティ市場および産業の状況と、変化をもたらす要因

## 8.1. マクロ経済動向と企業経営環境

### (1)2007 年の好調からリーマンショックへ

表 20 は、総理府統計局が公表している実質 GDP の成長率（暦年ベース）である。2000 年代初頭の IT バブル崩壊に伴う低迷の後、日本経済は比較的長期の景気拡大局面を迎え、2007 年が直近のピークだったことがわかる。2008 年度はリーマンショックのお膝元であるアメリカでプラス成長を維持したのとは対照的にマイナス成長となり、2009 年度にはマイナス 5.2%と驚異的な落ち込みを示している。

**表 20 GDP 実質成長率の推移**

国内総生産の実質成長率　　http://www.stat.go.jp/data/sekai/03.htm#h3-05

（単位　%）

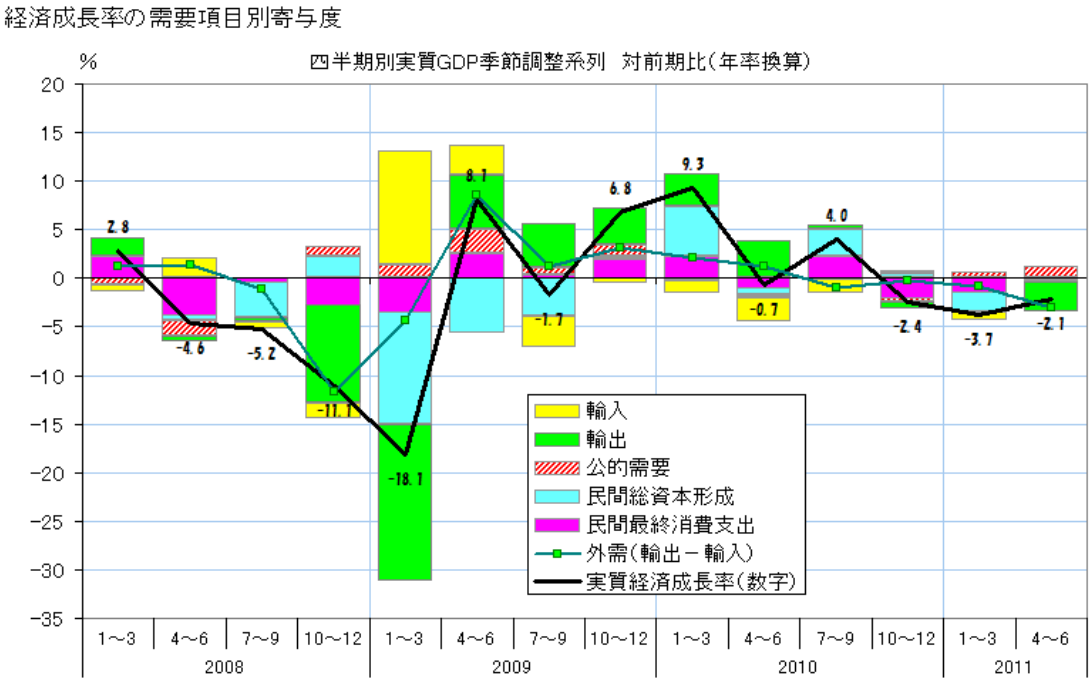
| 国（地域） | 1999 | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **世　界** | **3.4** | **4.4** | **1.8** | **2.1** | **2.7** | **4.1** | **3.6** | **4.1** | **4.0** | **1.7** | **-2.0** |
| 日本 | -0.1 | 2.8 | 0.2 | 0.3 | 1.4 | 2.7 | 1.9 | 2.0 | 2.4 | -1.2 | -5.2 |
| アメリカ合衆国 | 4.9 | 4.2 | 1.1 | 1.8 | 2.5 | 3.6 | 3.1 | 2.7 | 2.1 | 0.4 | -2.6 |

（出典：総理府統計局 http://www.stat.go.jp/data/sekai/03.htm#h3-05 より　JNSA 加工）

2007 年度が近年の日本経済としては好調な年であったことが確認できる。2008 年以降については少し詳しく見ることにする。図 29 は、本川裕氏による「社会実情データ図録」からの引用である。2008 年は、4-6 月期から既にマイナス成長となっていたことがわかる。2008 年度調査で 2009 年 2-3 月に実施した企業からのヒアリングでは、少なくとも 9 月ごろまでは極端な需要の減少は聞かれていなかったが、年度当初から風向きは変わっていたことになる。2008 年 10-12 月期には前期比年率でマイナス 11.1%、翌 2009 年 1-3 月期は同 18.1%と、異常な急減速を示している。この時期、世界経済が一斉に急速にシュリンクしたことは記憶にも新しい。

その後、新興国を中心に経済回復が進み、外需を牽引役に日本経済の回復が 5 四半期続くが、残念ながら力強さはない。

**図 29　四半期別経済成長率推移**




（出典：　社会実情データ図録 http://www2.ttcn.ne.jp/honkawa/4420.html）

(2) 2010 年度の停滞から回復へ、東日本大震災の発生と 2011 年度の日本経済

2010 年度は、2009 年度後半の回復基調を受けて年度当初から期待は高かったが、2010 年 4-6 月期は図 29 に見るように低調であり、実感としても停滞感があった。それが 7-9 月期以降持ち直して、全体としては年度ベースでプラス 2.3%と発表されており、比較的順調な拡大があったと考えられる。

そこに 2011 年 3 月 11 日、東日本大震災が発生し、福島原発の事故を誘発することで日本は未曾有の社会的試練を経験することになった。図 29 からは、生産の停止に伴う輸出の落ち込みを中心とした経済の後退が読み取れる。その後の統計データは余り得られていないが、国内生産は 7-9 月期に順調な回復を見せる一方、欧州債務問題が深刻化すると共に、米国の景気停滞間が強まり、世界全体に暗い影を投げている。

(3) 企業の経営環境

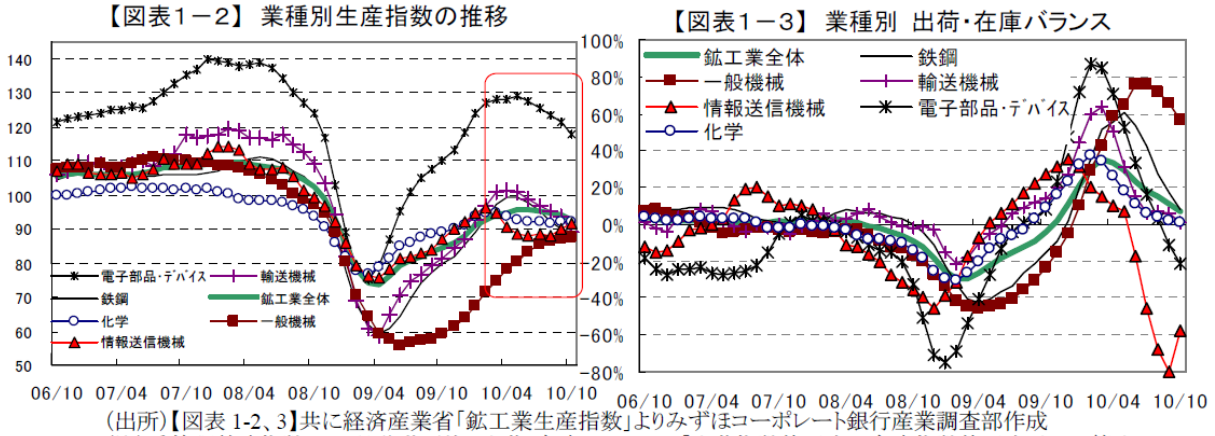
今回の調査対象期間中に、企業の経営環境は激変した。みずほコーポレート銀行が 2011 年に発行した「2011 年度の日本の産業動向」には日本の業種別生産指数と在庫･出荷バランスの推移がグラフで示されている（図 30）。2008 年度前半の好調が後半に急降下し、2009 年 4 月ごろを底に回復に向かうものの、リーマンショック前まで戻せないうちに 2010 年度後半には減速に向かったことが示されている。

マクロの GDP 推移と比較的似た動きとなっているが、企業業績については、同レポートの 2010 年度版[24]では「2009 年度の企業業績（主要 155 社ベース）は、2008 年度後半から続い

[24] http://www.mizuhocbk.co.jp/fin_info/industry/sangyou/m1034.html　2010 年 8 月 18 日

ている世界経済低迷の影響を大きく受けた一方、固定費削減等のリストラ効果により、主要155 社ベースでは、▲11%（2008 年度比、以下同様）の減収、営業利益は同+34%の増益となった。尚、営業利益は危機前の 2007 年度比では 49%と低水準に留まった。」としている。

**図 30　企業の生産・出荷・在庫の推移**




（出所）【図表 1-2、3】共に経済産業省「鉱工業生産指数」よりみずほコーポレート銀行産業調査部作成
（注）季節調整済指数、3 ヶ月移動平均。出荷・在庫バランスは「出荷指数伸び率－在庫指数伸び率」として算出

（出典：　みずほコーポレート銀行　http://www.mizuhocbk.co.jp/fin_info/industry/sangyou/pdf/1035_01.pdf）

また、2010 年度については、同レポートの 2010 年度版[25]において「2010 年度の企業業績（主要 162 社ベース）は、急速に進んだ円高が企業収益を圧迫したものの、景気対策効果とアジア需要に支えられ、主要 162 社ベースでは、売上高は+3.4%（2009 年度比、以下同様）、営業利益は同+37%の増収増益となる見込み。尚、営業利益水準は危機前の 2007 年度比 7 割程度に留まり依然としてピークを下回るものの、当部 7 月時点の予想に比べ大幅な回復となる見込み。」としている。

経営環境が持続的に厳しい中、企業努力により利益は回復を続けていることが分かる。しかし、この間の様々な経済報道に見られるように、雇用や賃金を含む極めて厳しいコスト抑制の成果である要素が強いと推測される。従って、IT や情報セキュリティに振り向ける投資・コストも戦略性や必要度が厳しく吟味された上で実施に移されると考えられ、情報セキュリティ産業にとっての市場環境は厳しい状態で推移すると考える必要があろう。このことは、震災からの回復に、欧州の信用不安やタイの洪水被害等異変が続く 2011 年度も、悪化こそすれよくなる展望は見出しにくいのが実態ではなかろうか。

## 8.2.　企業・組織の IT 支出ビヘイビア

### (1) IT 投資サイクル

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

[25] http://www.mizuhocbk.co.jp/fin_info/industry/sangyou/m1035.html　2011 年 1 月 21 日　震災前であることに注意

考えられる。

しかし、現在、経済学的に、あるいはITガバナンスの視点からIT投資サイクルを定義し、それを追いかけるような研究は具体化していない。少なくとも、ウェブ検索で論文等が探せるほどには人口に膾炙していないようである。

IT投資に影響を与えるものとしては、システムライフサイクルがあり、これは2004, 2005年度にIPAの委託によりJUASが調査を行ってまとめた「システム・リファレンス・マニュアル[26]」の中で言及されている。これによれば、システムの利用期間は10～15年が最も多いが、パッケージでは5～10年程度となる。

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

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

しかし、現実に業務プロセスはそこまでの速度では変化せず、経験則的には3～4年がサイクルの目安と考えられる。一例では、マイクロソフトのオフィスシリーズのバージョンは、97、2000、2003、2007、2010と上がってきている。上記数字を裏付ける事例と言える。

同様に、通信ネットワークの容量もIT投資サイクルに影響を与えると考えられる。ネットワークの容量そのものではないが、日本での通信網上の情報流通量の統計は、総務省が発行する情報通信白書[27]に示されており、2011年版のデータは表21のようになっている。数字が細かいが、2009年度の情報流通量は2001年度比198.8%となっており、10年で倍のペースである。これは昨今のブロードバンドの広がりやネット上の動画配信等の普及、スマートデバイスの急速な浸透等を考えるとややスローな感じもする。

**表 21　平成 23 年版 情報通信白書　情報流通量の推移**

| 情報流通量 | 単位 | 平成13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21年度 | 平成13年度を100とした場合 | 期間平均伸び率 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 流通情報量 | ビット | $3.83\times10^{21}$ | $3.85\times10^{21}$ | $3.89\times10^{21}$ | $4.02\times10^{21}$ | $4.36\times10^{21}$ | $4.97\times10^{21}$ | $5.96\times10^{21}$ | $7.12\times10^{21}$ | $7.61\times10^{21}$ | 198.8 | 9.0% |
| 対前年度伸び率 | | | (0.5%) | (1.0%) | (3.5%) | (8.5%) | (13.9%) | (20.1%) | (19.5%) | (6.9%) | | |
| 消費情報量 | ビット | $2.63\times10^{17}$ | $2.63\times10^{17}$ | $2.68\times10^{17}$ | $2.69\times10^{17}$ | $2.68\times10^{17}$ | $2.68\times10^{17}$ | $2.75\times10^{17}$ | $2.91\times10^{17}$ | $2.87\times10^{17}$ | 109.0 | 1.1% |
| 対前年度伸び率 | | | (−0.1%) | (2.2%) | (0.4%) | (−0.4%) | (−0.1%) | (2.8%) | (5.8%) | (−1.6%) | | |

（出典：総務省　情報通信白書 2011）

当ワーキンググループのヒアリング調査では、通信事業者の設備更新サイクルは3～4年程度という発言を記録している。職場のパソコンのリース期間は概ね3～5年と考えられ、税法上の償却期間等からも、概ねこの3～5年をIT投資サイクル、したがって情報セキュリティ関連の需要にも影響を及ぼすサイクルと考えてよいと思われる。

なお、前回の投資ピークは2007年ごろだったという証言もあり、これが事実とすれば、2011年度から2012年度に次の山が現れる可能性もある。

[26] http://www.ipa.go.jp/about/jigyoseika/04fy-pro/chosa/srm/srm2.pdf
[27] http://www.soumu.go.jp/menu_news/s-news/01tsushin02_01000017.html

(2) IT 投資全体市場との比較（JEITA 統計に対する比率）

本調査では、例年、一般社団法人電子情報技術産業協会（JEITA）[28]統計による IT 投資（JEITA 参加企業の出荷額ベース）との比較を行ってきた。JEITA 統計並びに一般社団法人情報通信ネットワーク産業協会（CIAJ）[29]統計を加味し、本調査結果と比較したデータを表 22 に示す。

**表 22　IT 市場、通信市場と情報セキュリティ市場規模の比較**

| セキュリティとITの比較 | 2008年度 | 2009年度 | 2009/2008伸び率 |
|---|---|---|---|
| | 億円 | 億円 | |
| セキュリティ出荷計 | 7,193 | 6,821 | −5.2% |
| | | | |
| IT出荷計(JEITA) | 72,898 | 65,098 | −10.7% |
| PC出荷 | 9,758 | 8,858 | −9.2% |
| MF, WS, Svr 出荷計 | 5,688 | 4,622 | −18.7% |
| ソフトウェア | 7,484 | 6,851 | −8.5% |
| SI開発 | 27,502 | 24,152 | −12.2% |
| BPOその他サービス | 22,466 | 20,615 | −8.2% |
| （SW,サービス計） | 57,452 | 51,618 | −10.2% |
| | | | |
| ネットワーク機器 | | | |
| 生産 | 6,361 | 5,320 | −16.4% |
| 輸入 | 3,927 | 3,546 | −9.7% |
| 輸出 | 2,103 | 1,824 | −13.3% |
| 国内出荷 | 8,185 | 7,042 | −14.0% |
| | | | |
| IT+NW装置 | 81,083 | 72,140 | −11.0% |
| | | | |
| セキュリティ市場の比率 | | | |
| 対IT出荷計(JEITA) | 9.9% | 10.5% | |
| 対IT+NW装置 | 8.9% | 9.5% | |

（出典：JEITA、CIAJ の統計を元に JNSA 作成）

JEITA では、「年度パーソナルコンピュータ国内出荷実績[30]」「わが国におけるサーバ・ワークステーションの出荷実績[31]」「ソフトウェアおよびソリューションサービス市場規模調査結果[32]」の 3 種類の統計を公表している。表 22 では、「IT 出荷計（JEITA）」の欄で、各々「PC 出荷」「MF, WS, Svr 出荷計」「ソフトウェア、SI 開発、BPO その他サービス」にその数字を示している。また、情報セキュリティ投資に対応する IT 投資にはネットワーク機器も含まれることから、CIAJ 統計に基づきその国内出荷額も比較対象として掲出した。

28　一般社団法人電子情報技術産業協会　http://home.jeita.or.jp/
29　一般社団法人情報通信ネットワーク産業協会　www.ciaj.or.jp/
30　「2009 年度パーソナルコンピュータ国内出荷実績」http://www.jeita.or.jp/japanese/stat/pc/2009/
31　「わが国におけるサーバ・ワークステーションの平成 21 年度（平成 21 年 4 月～平成 221 年 3 月）出荷実績」http://home.jeita.or.jp/is/statistics/server/h21/index.html
32　社団法人電子情報技術産業協会「2009 年度ソフトウェアおよびソリューションサービス市場規模調査結果について」平成 22 年 6 月 17 日　http://home.jeita.or.jp/is/statistics/soft_sol/2009/index.html

表 22 に見られるように、2009 年度は IT 関係の出荷額は前年度比大幅な落ち込みを経験している。これは 8.1 で見たところとも一致する。コンピュータ、ソフトウェア、関連サービスの合計で、2009 年度は前年度比マイナス 10.7%の 6 兆 5,058 億円となっている。SI 開発が 12.2%も落ち込んだことが大きい。これは、不況のためが主たる要因であろうが、IT 投資サイクルの狭間のダブルパンチによるものである可能性が強い。なお、PC は台数ベースでは前年比 8.3%増えているので、金額の減少はそれを上回る単価下落によるものと考えられる。

ネットワーク機器も国内出荷ベースで 14.0%と大幅な落ち込みを記録した。両者を合わせた、国内の IT 投資にほぼ対応すると考えられる出荷合計額は 7 兆 2,140 億円で、前年度比成長率はマイナス 11.0%であった。これに対して、本調査の結果では情報セキュリティ市場の出荷は 6,821 億円（同マイナス 5.2%）である。前年比マイナス幅では IT 出荷の半分以下で済んでいる。その結果、IT 全体に占める情報セキュリティ出荷の比率は 9.5%となる。前回調査におけるこの数字が 7%であったことと比べると、大幅な比率の上昇となった。なお、両統計はベースが違うので厳密な対応関係ではなく、あくまでも参考であり、情報セキュリティが IT の中で占める比率についての一つの指標と位置づけるべきである。この点については、情報処理実態調査が直接ユーザサイドのデータを出しているので、その検討を次項で行う。

### (3)経済産業省「情報処理実態調査」に見られる支出・投資動向

経済産業省は毎年情報処理実態調査を実施しその結果を公表している。発表までのリードタイムが長いので、現在公表されている最新の調査は 2009 年版[33]であり、対象年度は 2008 年度である。しかし、情報セキュリティの状況について直接 IT ユーザに調査したものとして参考になる。

◆ 情報セキュリティ対策の全般状況

情報セキュリティに関する全体状況としては、情報処理実態調査では以下のようにまとめている。

> 「情報セキュリティ対策の取り組みは前年度に続き積極的に行われており、情報セキュリティ対策の実施率（情報セキュリティ対策を「既に実施している」と回答した企業の割合）は高い水準が続き、情報セキュリティ対策費用の対情報処理関係支出総額比は前年度より上昇した。
>
> 情報セキュリティ対策がセキュリティ向上に寄与したと回答した企業の割合は 3 年連続で上昇し、このほか業務効率の向上をあげる企業の割合も上昇した。
>
> 情報セキュリティ対策の阻害要因としては、前年度と同様、コストがかかることやどこまでやるべきかかがわからないことなどをあげた企業が多かった。また前年度と比較すると、CISO（Chief Information Security Officer;最高情報セキュリティ責任者）などの専門家がいないことや予算がとれないことをあげた企業が増加した。」

全体としては、セキュリティ対策は進展しつつも、一般に言われる、「どこまでやればよい

[33] http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/h21jyojitsu.html

かわからない」「専門家がいない」という状況は改善されていない。

◆ 情報セキュリティ対策費用の状況

情報セキュリティ対策費用は金額幅による選択肢で回答を求めておりそこから見做しで 1 社平均の対策費用を算出しているが「各選択肢の中間値を当該選択肢の回答企業の情報セキュリティ対策費用とみなし加重平均値を計算すると、平成 19 年度が 1,230 万円、平成 20 年度が 1,030 万円となり、平成 20 年度情報セキュリティ対策費用が低下したことが示唆される。」と記されている。

しかし、同調査の前年度報告書では平成 19 年度の金額は 756 万円となっており、上記調査との乖離が大きい。

同調査はまた、情報処理支出と情報セキュリティ対策支出の比率も算出している。その記述は「 一社平均情報セキュリティ対策費用と同様、同費用の対情報処理関係支出総額比について、各階級の中間値を当該階級に属する企業の同比率をみなし加重平均値を計算すると、平成 19 年度 6.9%、平成 20 年度 7.4%となり、同比率が上昇したことが示される。」となっており、金額は減少したが比率は上昇したとしている。1 年間で 0.5%ポイントも上昇することも興味深いが、それが 7.4%という比率にまで達したことも興味深い。

なお、本調査の 2009 年度版では、2008 年度版情報処理実態調査が明示的に示さなかった同比率を、同調査に記された他の数字を整理することで算出している。そのデータは表 23 に示す通りで、0.95%となっている。参考に、同表の下に 2008 年度調査の対応するデータを示す。これで見ると情報セキュリティ対策費用の情報処理関係諸費に対する比率は 1.4%となる。おそらく情報セキュリティ対策費用の回答企業を母集団とした同比率が 7.4%という趣旨であろう。0.95%や 1.4%よりは納得性の高い数値である。

**表 23　情報処理実態調査母集団の比較（平成 19 年度、20 年度、21 年度調査）**

| 対象年度 | 回答企業数 | 資本金規模 | 年間事業収入規模 | 情報処理関係諸経費 | 年間事業収入比 | 情報セキュリティ対策費用 | 対情報処理関係費比率 |
|---|---|---|---|---|---|---|---|
| | （社） | （百万円） | （億円） | （百万円） | （%） | （万円） | （%） |
| 2006年度 | 4,264 | 9,857 | 796 | 725 | 0.91 | 757 | 1.04 |
| 2007年度 | 4,645 | 9,884 | 837 | 799 | 0.95 | 756 | 0.95 |
| 2007/2006 | 108.9% | 100.3% | 105.2% | 110.2% | 104.8% | 99.9% | 90.6% |
| 2008年度 | 5,021 | 9,509 | 643 | 736 | 1.14% | 1,030 | 1.40% |

（出典：経済産業省平成 19, 20, 21 年度情報処理実態調査より JNSA 作成）

なお、上の表にある 1 社平均 1,030 万円という情報セキュリティ対策費用に回答企業数 5,021 を掛けると 6,051 億円となり、本調査における 2008 年度の市場規模算定値 7,193 億円と比較的近い数字となることは興味深い。（ちなみに同調査の回答率は 52.9%となっている。）

(4)社団法人日本情報システム・ユーザー協会「IT 動向調査」に見られる情報セキュリティ対策

社団法人日本情報システム・ユーザー協会（JUAS）は 1994 年以来継続的に IT 動向調査を行っている。情報セキュリティ対策も一貫して調査対象であるが、近年はそのウェイトが

以前に比べて低くなっている。2009 年度調査[34]ではリスクマネジメントの一環として、内部統制や BCP、IFRS と同じカテゴリでの報告となった。

同調査の特徴は絶対額よりも増減の傾向を聞くところにあり、情報セキュリティ対策費用についても同じアプローチがされている。「情報セキュリティの概算費用に関する次年度の増減見込み」を聞いた結果は、「情報セキュリティ対策費用を 2009 年度に増やす企業の割合は（前年度比）18 ポイントの大幅ダウンで 1/3 へ、大企業ほど情報セキュリティ投資を抑制」となっている。経済状況の悪化を反映したものと見られる。なお調査時点は 2009 年 11 月であり、かなり実績見込みに近い時点の調査と考えてよい。興味深いのは「今年、『増額予定』の企業の割合が多い業種グループを見ると、トップは『金融』で４２%、続いて『一次産業』が３７%である。」「今年度は、景気の影響を受けつつも、金融が０８年度の『減額予定（１４%)』のトップから『増額予定』のトップにシフトしているのが目立っている。」としている点である。

その他、同報告で述べられているのは「対策が進んでいるのは『②ウィルスへの対策』と『①ネットワーク上の情報アクセスの制限』、対策が進んでいないのは今回追加した新しい課題の『⑥USB 等の書き出し・持ち出し制限』と『⑩情報セキュリティ監査の実施』」「08 年度に比べて、不安感が増したのが『③物理施設での入退出管理』と『④内部コンピュータ犯罪への対策』、安心感が増したのが『⑨全社的な情報管理規定の確立』でほぼ安定期に入ってきた」という点で、「情報セキュリティ対策の強化予定の割合は全体では 2 割～4 割と少ない大企業が力を入れているのは今回追加した新しい課題の『⑥USB 等の書き出し･持ち出しの制限』と『⑩情報セキュリティ監査の実施』」といった動向を紹介しているが、情報セキュリティ関連はこれだけの記述にとどまっている。

### 8.3. 情報セキュリティに関わる外部環境変化

(1)ネットワーク脅威の状況とその変化（IPA 公表を中心に）

独立行政法人情報処理推進機構（IPA）は、定期的にネットワーク脅威に関する統計や警告を発している。特に毎年公表する年間「10 大脅威」は、各年の特徴や課題を浮かび上がらせでいる。

2010 年 3 月 31 日発表の「2010 年版 10 大脅威」では、「あぶり出される組織の弱点」として、「変化を続けるウェブサイト改ざんの手口」「アップデートしていないクライアントソフト」「悪質なウイルスやボットの多目的化」等 10 項目を上げた。また、ウェブ閲覧により感染するガンブラーウイルス、内部者による情報漏えい、管理不足による脆弱性放置の危険に警告を発している。

「2011 年版 10 大脅威」は、2011 年 3 月 24 日に発表されている。2010 年の脅威の特徴として「組織システムや情報資産、ミニブログサービス等のユーザをターゲットとした、外部から攻撃される脅威が半数を占めていることです。特に、Stuxnet（スタックスネット） に代表される複数の攻撃を組み合わせた「新しいタイプの攻撃」は、制御システム系や組織の

[34] http://www.juas.or.jp/servey/it10/index.html

基幹系システム等今まで不可能と考えられていた領域に対しての攻撃が現実のものとなってきており、現状のセキュリティ対策の見直しが迫られています[35]」と述べている。そして 10 大脅威には「止らない!ウェブサイトを経由した攻撃」「複数の攻撃を組み合わせた『新しいタイプの攻撃』」「攻撃に気づけない標的型攻撃」といった進化した脅威を指摘して警告している。

このように、ネットワークからの攻撃の脅威は一段と深刻になっている。その特徴をまとめると、次のように言える。

① マルウェア感染経路の多様化と深刻化

以前はメールへの添付ファイルが感染源の主流であったが、その危険に対する認知が進むと、仕掛けを仕込んだ Web サイトに誘導し、そこからダウンロードさせる、あるいは閲覧だけでマルウェアを送り込む、という手口が広まった。更にその Web サイトも、攻撃者が作ったにせものから、実在する企業の Web サイトを悪用するパターンも生まれ、悪質化が一段と高まった。

個人の間で人気となった、ピアトゥーピアネットワークをベースとするファイル交換・共有ソフトもウイルス感染の温床となった。この場合は、個人の PC に置かれた業務用のファイルが勝手にピアトゥーピアネットワークに放出され拡散する被害が多発して、深刻な社会問題にもなった。

更に、ネットワークと直接接続していないシステムにもマルウェアを送り込める仕組みとして、USB メモリにもぐりこむマルウェアが登場した。写真店店頭でのプリント発注機経由の感染も見られた。より深刻な事例として Stuxnet と呼ばれる、制御システムを狙ったウイルスの被害も明らかになっている。

更に、マルウェア感染を起こさせる行為を誘発する仕掛けが、次項に見るように巧妙になっている。

② 標的型攻撃の多発

不特定多数に多量のウイルスメールをばら撒き、低い確率で無差別に行う感染活動から、特定のターゲットに特定の目的でマルウェアを送り込むための攻撃が増えている。このため、IPA への届出ベースでは発見・感染件数は減少しているものの、被害の実態が急速に深刻度を増しているという現実がある。

この攻撃では、実在の、受信者にとって身近であったり関係性が理解できる発信アドレスが詐称され、件名や添付ファイル名も巧妙に仕組まれて、受信者が疑いを持たずに添付ファイルを開いたり、URL をクリックしたりさせられる。その結果は、自覚症状のないマルウェア感染となり、スパイウェアやボットのひそかな活動を長期にわたって許すことになる。

2011 年になって日本で話題となった、大企業や国家組織における大規模被害は、この形で侵入を許したケースが多い。

③ Advanced Persistent Threat（新しいタイプの攻撃）

[35] http://www.ipa.go.jp/security/vuln/10threats2011.html

標的型攻撃の進化形として 2010 年から取り上げられている攻撃で、標的型攻撃のソーシャルエンジニアリング要素が巧妙化するとともに、送り込むマルウェアも攻撃対象の中で特定の目的を持って活動するタイプのものを指している。「新しいタイプの攻撃」というのは IPA の命名だが、そのレポートによれば、典型的な例として Stuxnet が取り上げられている。

侵入を成功させるためのソーシャルエンジニアリング・標的型攻撃と、侵入後に特定の目的で活動するマルウェアの送り込みの組合せである。マルウェアの行為は、多くは情報の窃取・持ち出しだが、トロイの木馬化して攻撃者の進入を可能にするもの、ボット化するもの、破壊活動を行うものもあるようである。

④ ソーシャルメディアを利用する攻撃

Facebook、mixi 等ソーシャルネットワーキングメディアが世界的に広く浸透している。更にミニブログと称される Twitter や類似のサービスも急拡大している。これらを悪用する攻撃やマルウェアも増加している。

ソーシャルメディア上の通信やゲームを利用しての感染や、短縮 URL をマルウェアサイトへの誘導の隠れ蓑に使う形での攻撃である。一般ユーザが攻撃対象となり、セキュリティ知識の乏しい層が狙われる傾向が強いために、今後深刻な被害に結びつく可能性が強い。

⑤ スマートデバイスへのマルウェアの拡散

スマートフォンやタブレット型端末等、携帯電話から発展した通信端末と、ポケット型 PC の融合した新しいタイプのデバイスが急速に広まっている。ここでは合わせて「スマートデバイス」と呼ぶことにする。　スマートデバイスは、アップル社が主導して登場し、Google による AndroidOS の提供で多品種化が急速に進むとともに、台数ベースで PC をはるかに超えるところまで急拡大している。

ネットワーク（Wi-Fi）機能も電話回線経由のデータ通信機能も備えることから使い方の多様性も広がっている。そこを狙ったマルウェアも数多く報告されるようになった。感染によりいたずらをするだけのタイプだけでなく、端末内部の情報を勝手に送信する機能を持つものが多く、情報漏えいやプライバシー侵害の被害が懸念されている。

特に、クラウドコンピューティングの普及や震災経験を踏まえてスマートデバイスの業務利用への導入が急ピッチで進んでいることと合わせると、スマートデバイス経由の企業秘密や個人情報漏えいが引き起こされる恐れが強く、企業における事前の対策が必要である。

(2) 情報漏えい事件の深刻化

ネットワークからの攻撃は、2010 年初頭の Google への DDoS 攻撃を初め、米国政府をターゲットにした攻撃等特定の意図を持ったと考えられる攻撃が目に付きだしていたが、2011 年に入って、ソニーが世界的に標的にされるほか、国防産業の複数企業への情報窃取目的と

考えられる不正アクセス等が明るみに出た。

JNSA が毎年発表する個人情報漏えい事件の統計は高い社会的注目を集めているが、2010 年版統計[36]では、表 24 のようになっており、引き続き個人情報漏えいが跡を絶たないことを示している。

企業・組織の防衛意識はかつてないほど高まっていると考えられるが、同統計が示す[37]ように、90%近くが組織の側に要因があるものであり、広義の管理の不備が事故を招く構造は変わっていない。特定の企業に意図を持って情報を盗みに来る脅威と合わせ、情報セキュリティに関する状況は決して改善されているとは言えない状況にある。

**表 24　2010 年の個人情報漏えいインシデント　概要データ**

| | |
|---|---|
| 漏えい人数 | 557万9316人 |
| インシデント件数 | 1679件 |
| 想定損害賠償総額 | 1215億7600万円 |
| 一件当たりの平均漏えい人数 | 3468人 |
| 一件当たり平均損害賠償額 | 7556万円 |
| 一人当たり平均損害賠償額 | 4万3306円 |

（出典：　JNSA セキュリティ被害調査 WG　http://www.jnsa.org/result/incident/2010.html）

特に 2011 年は、日本の企業や政府組織が大規模な情報漏えいや不正侵入の被害に遭うケースが頻発している。４月にはソニーが世界規模で情報漏えいを発生させた。特定の目的を持つ集団からの報復攻撃である可能性が指摘されている。9 月には防衛産業の複数企業での不正侵入と情報流出が発覚し、防衛機密や産業秘密に関わる情報の流出懸念が拭い切れずにいる。これを追いかけるように 10 月には衆議院でのサーバや端末 PC への侵入が発覚した。これらはいずれも、そのターゲットや手口等から、特定の目的を持った攻撃と考えられ、特定の攻撃者の存在が推測される。

以前から問題意識を持った人たちが警告し続けてきた、サイバーテロ、サイバーウォーが、日本においても現実に起き出している。

(3)法制度等の変遷

情報セキュリティに関係する法制度等としては、古くはウイルス感染や不正アクセス被害の IPA への届出制度が 1990 年にスタートしている。その後 1999 年には不正アクセス禁止法が成立し、情報セキュリティ対策が社会に浸透するきっかけとなった。

情報セキュリティ意識をより広く植えつけるのに役立ったのが個人情報保護法と言われている。民間企業を含めて全面的に適用となったのが 2005 年 4 月からで、この法律を契機に ISMS 認証やプライバシーマーク認可の取得に取り組む企業が急増し、一時は認証取得ラッシュとなった。

その対応が一段落する暇もなく、米国で成立した S0X 法[38]の流れを受け、日本でも内部統

[36] http://www.jnsa.org/result/incident/2010.html　2011 年 9 月 6 日発表
[37] 情報漏えいの原因上位：管理ミス 36.3%　誤操作 32.3%　紛失・置忘れ 12.6%　盗難 7.6%　計 88.8%
[38] Sarbanes Oxley Act of 2002 米国企業改革法

制に関する報告とそれに対する第三者監査の制度が検討され、改正により衣替えした金融商品取引法に基づいて内部統制報告制度が 2008 年 4 月にスタートした。これは情報セキュリティ対策を直接要求するものではないが、財務諸表の情報に影響を与える業務の執行の適正性の担保とその検証を、株式公開企業の経営者の義務としている。それは IT なしには実現できず、IT の設計・構築・運用・管理の適正性の担保が求められることから、IT ガバナンスが課題となる。また内部統制管理の一環として IT プロセスにおける不正や誤謬の排除やトレーサビリティを要求する構造となっていることから、その中核をなす技術として情報セキュリティが位置付けられるに至っている。その結果、IT におけるセキュリティガバナンスの確立の必要性が認識され、結果として情報セキュリティ対策の促進に寄与したと評価されている。

この間、2004 年には e-文書法が成立して文書を電子的に保持したり利用する道を開くと同時に、電子データの安全にも関心を高めさせることとなった。また、2011 年には刑法改正が行われ、この中でいわゆるウイルス作成罪が初めて規定された。ウイルスを作成したり配布することを直接罰することができるようになったのである。

このように、外部脅威から内部管理へと、対象も推移しつつ、情報セキュリティ対策を促す法制度面での動きも積み重ねられてきている。これらは、日本の企業・組織の情報セキュリティ対策への取り組みを促す面で大きな力を発揮したといえる。逆に言えば、法的縛りや公表義務のようなソフトなペナルティを含む罰則が明定されない限り、直接の付加価値を生みにくい情報セキュリティ対策はなかなか進まない、という経験の過程でもあった。

### 8.4. 産業としての課題

情報セキュリティ産業の現状は、システムインテグレーションに伴う IT セキュリティの組込みと、その上流に位置する情報セキュリティ構築を一元供給する大手 SI 事業者や、対策ツールの多くを供給する海外ベンダが主要な役割を果たし、市場の占有度も高い。一方参入事業者の数では、比較的専業に近い中小事業者が多くを占めるが、その事業規模は総じて小さい。

情報セキュリティの経営課題としての重要性は、またしても大組織の大規模事件によって教えられた恰好だが、その対策はいよいよポイントソリューションでは済まなくなり、総力戦の様相を呈している。情報セキュリティ対策を実施するのは企業・組織だが、その実現には情報セキュリティ対策製品やサービスを提供する産業の力が欠かせない。IPA の「情報セキュリティ産業の構造と活性化に関する調査報告書」でも、そのような問題意識を鮮明にし、産業活性化のための施策の充実と実施を訴えており、具体的施策として、以下の 5 項目を取り上げている。

1. 官民ともに情報セキュリティの達成目標を掲げ、対策実施工程表を具体化し、管理サイクルに基づき継続的に対策を実施することで需要喚起を図る。
2. 国民を守る情報セキュリティ戦略の下に対策実施を加速し、施策に十分な予算を手当てするとともに、戦略的研究開発を推進し、開発成果の民間活用を使い勝手のよい制度で実現する。
3. 高度情報セキュリティ人材教育の機会を一層充実するとともに、情報セキュリティ人材の社会的評価とキャリアパスイメージの形成、共通認識の形成を促進する。

4. 情報セキュリティ産業とそれに関連する資金の出し手､製品やサービスを取り扱うインテグレータ、エンドユーザ等の間の情報流通や人的交流の支援・促進により、資金調達や事業連携、顧客開拓の機会拡大をもたらす。
5. アジアを中心とする国際社会での日本の貢献として、情報セキュリティ技術・ノウハウの提供を政策的に展開する中で、それを支える国内企業の海外展開をサポートする。

官民における情報セキュリティ対策の一層の充実による需要喚起、公的開発支援、人材開発・育成、産業資金供給、国際展開支援が謳われている。　このように、政策側も情報セキュリティ産業の充実の必要性を認識し、支援のための課題が提起されるに至っている。

一方で、情報セキュリティ市場を構成する事業者には、事業規模の小さい企業が多いことも事実である。そして、公的研究開発支援、社会全体としての情報セキュリティ人材育成、産業資金の供給等、至る所で産業振興のための条件の不備が指摘されている。市場の成長に支えられて新規参入や事業拡大が図れている中小事業者も、情報セキュリティの重要性の高まりと対策の高度化の必要性の高まりと共に、より広い、総合的ソリューション提供力が要求され、大手との競争が厳しくなる可能性がある。

これらの点を見据えて、IPA の報告書にもあるように、産業資金の供給、技術開発に対する支援、人材の育成と供給、業界の横の連携による相互補完や規模の拡大等を視野に入れた、情報セキュリティ産業全体に対する政策対応と育成・支援策が傾注されることが期待される。

情報セキュリティ産業としては、そのような支援に呼応して、技術開発や製品・サービスの一層の充実、そして海外市場も含めた市場開拓に向けて自助努力を強める必要がある。特に海外進出を進める日本企業の現地におけるセキュリティ対策は、日本の国益のためにも需給両サイドが一体となって推進する必要がある。

## おわりに

2011 年は、日本の情報セキュリティについて考えさせられる、極めて多くのことが立て続けに起こった年と言える。

東日本大震災、みずほ銀行のシステムトラブル、ソニーグループへの攻撃による、世界的広がりを見せた 1 億人規模の個人情報の流出、防衛産業に対するサイバー攻撃、国の機関に対する執拗なサイバー攻撃、更に APT や Android へのマルウェア攻撃と、枚挙に暇がない。従来、内部からの漏えいに注目が集まり、それが企業への情報セキュリティ対策意識の定着に結実しつつあったが、その間言われつつもやや等閑視されていた外部脅威が、その深刻さをまざまざと見せつけたと言える。

IT のフロンティアは、スマートフォン、タブレット PC、ソーシャルメディア等個人の情報生活の革新を促す技術から、クラウドコンピューティングのような情報処理のパラダイムを転換する可能性のある技術・サービス、更にはスマートグリッドやスマートシティといった社会枠組みの進化をもたらす活用スキームまで、イノベーションを進めている。このことは、情報セキュリティのフロンティアをも拡張し、複雑さと重要度を飛躍的に高めている。

米国では、2010 年には軍事的防衛の対象領域としてサイバー空間が定義され、軍にサイバーコマンドが設置された。更に 2011 年に入って、物理的報復攻撃の可能性まで示唆されるに至っている。情報セキュリティを取巻く状況は次のように一層複雑化し、「安全」と「安心」を確保するための努力は、より多くを必要とするようになっていると感じられる。

- ネットワーク脅威の一層の深刻化：攻撃の頻度・量の拡大、正規のサイトを悪用する等の悪質化・巧妙化等
- ネットワーク犯罪の、地下経済を背景にした利益目的化と分業の進展
- ネットワーク攻撃の、テロや産業スパイやサイバーウォーの手段としての利用の拡大
- 組織内部における故意や不作為、不注意に起因する情報漏えいリスクの拡大と深刻化
- 内部統制、事業継続管理、法令遵守のために IT ガバナンスが必須となり、その中核的管理要素として情報セキュリティガバナンスの確立が必須に

IT セキュリティ、情報セキュリティは社会システムの安全・安定・安心の中核をなす要素と化していると言っても過言ではない。

情報セキュリティ市場に目を転じると、第一部で見たように、2008 年度半ばまでは比較的順調に拡大してきた日本の情報セキュリティ市場は、停滞・縮小の傾向を見せている。その理由の第一には、リーマンショック以降、金融市場と実物経済と財政出動により傷んだ財政の相互作用による経済の停滞がある。天変地異の頻発も回復に取組む企業の足を引っ張っている。

そして、情報セキュリティ市場自体の内側にも、対策が行き渡ったことや経営に定着したことによる需要の縮小、あるいは平準化という要因が確認できる。特にネットワーク脅威対策製品や、コンサルテーション、システム構築の分野にはっきりその傾向が現れている。一方で、コンテンツセキュリティ対策製品、アイデンティティ・アクセス管理製品や、運用・管理サービス、教育

サービスといった運用･維持管理にかかわる領域の停滞は相対的に軽微であることも見てとれる。

情報セキュリティは、コンピュータウイルスやネットワークアタックの危険性の認知を得るのに多大な労力を要した時代から、個人情報の漏えい紛失で世間の耳目を騒がせる時期を経て、情報の戦略的価値の保護やコンプライアンス、ガバナンスの重要要素と位置づけられ、企業経営全般のリスクマネジメントに不可欠の要素として経営に定着しつつある。その結果、情報セキュリティ市場も、日本経済全体のライフサイクルに追いつき、成熟化した経済と類似の様相を示していると言える。それは需要の安定化と同時に要求品質が高まることを意味する。供給側の充実が問われるところである。

情報セキュリティ対策は、ネットワーク脅威や情報漏えいへの受身の防御から、情報セキュリティガバナンス、IT 統制、内部統制、事業継続管理等を統括するコーポレートリスクマネジメントの主要要素となることで、企業価値を守り支え高める積極的役割へと、その価値を大きく変化させた。組織運営と事業経営の基盤に直結し、更には社会的安心を支えるべき情報セキュリティは、中央政府、地方自治体、産業界、学界等、あらゆる社会経済主体がこれを推進し強固にして行く必要がある。産官学民の努力を傾注し、相互の連携を促進することで、第 2 次情報セキュリティ基本計画が目指す世界トップクラスの IT 国家の姿が実現し、安心・安全なネットワーク社会が形成されなければならない。その中で、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行くものと期待される。情報セキュリティ産業はそのための貢献という役割を担っている。すなわち社会経済の神経系の保全というより積極的・基幹的使命を負っている。そしてその結果として、情報セキュリティ産業もよりバランスの取れた姿で発展し、情報セキュリティ対策の高度化と充実に寄与することが期待される。

今年に起きた多くの大規模サイバー攻撃被害を奇禍として、日本の情報セキュリティ対策に一層本腰が入ることを期待するとともに、それと両輪をなして我が国情報セキュリティ産業が充実拡大することが期待される。したがって、情報セキュリティ産業の現状を確認し、動向を把握することは、IT を利活用する全ての人と組織にとって、またその産業を支え動かす全ての人と組織にとって、有意義なことと信ずる。本調査は、情報セキュリティ産業の姿を統計的、金額的に明らかにし､産業動向の分析を行って各方面の参考とすることを目的に取組んだ｡本調査報告書が、関係各方面で参考とされ、官民の情報セキュリティ向上への取組みの参考として生かされることを期待するところである。

以上

# 情報セキュリティ市場調査報告書

2012 年 1 月 31 日

特定非営利活動法人　日本ネットワークセキュリティ協会

調査研究部会　セキュリティ市場調査ワーキンググループ

ワーキンググループリーダ

勝見　　勉　株式会社情報経済研究所

ワーキンググループメンバ（調査・執筆・編集参加者）

菅野　泰彦　　アルプスシステムインテグレーション株式会社
福岡　かよ子　株式会社インテック
橿渕　英久　　NTT データ先端技術株式会社
秋山　卓司　　日本クロストラスト株式会社
木城　武康　　株式会社日立システムズ
佐藤　友治　　ブロードバンドセキュリティ株式会社
熊谷　裕吾　　三井物産セキュアディレクション株式会社
塩見　友規　　三井物産セキュアディレクション株式会社
蜂巣　悌史　　株式会社 km2y
鳥居　肖史

以上

