第1章

「企業IT利活用動向調査」にみるIT化の現状

JIPDECは、調査会社アイ・ティ・アール株式会社(ITR)の協力を得て、国内企業の間で改めて関心が高まっている情報セキュリティ対策に重点を置き、国内企業の情報システム系および経営企画系部門などに所属し、IT投資と製品選定、もしくは情報セキュリティ管理に携わる役職者を対象に、2013年1月にインターネットによる「企業IT利活用動向調査」を実施した。

ここでは調査結果の中から特徴的な傾向をピックアップし、日本国内におけるIT利活用の実態を紹介する。

1 調査概要

1-1.調査概要

・実査期間:2013年1月15日～1月22日
・調査方式:ITR独自パネルを利用したWebアンケート
・調査対象:従業員数50人以上の国内企業に勤務するIT戦略策定、または情報セキュリティ従事者、係長相当職以上の役職者約2,800人

有効回答数:642件

1-2.回答者のプロフィール

回答者で最も多かったのは製造業(32.1%)、次いで情報通信業(19.9%)、サービス業(17.9%)となった。所属部門では情報システム部門が最も多く(77.1%)、役職は課長(37.5%)、係長・主任(36.4%)、部長(21.8%)が回答のほとんどを占めている。

IT戦略、セキュリティへの関心度をみると、回答者に情報システム部門所属が多いことも関係しているからか、セキュリティ製品の導入・製品選定に実際に関与している(65.9%)、セキュリティ対策の実務に実際に携わっている(56.9%)が半数以上を占めている。

2 経営におけるセキュリティの位置づけ

ここでは、企業経営においてセキュリティ対策がどのような位置づけにあるかに着目した。

2-1.今後重視する経営戦略

全25項目の経営課題について、今後1～3年で重視する内容で最多の回答を集めたのは「業務プロセスの効率化」で、62.8%の企業が今後重視する課題であるとした(図1-1)。業務プロセスの改革にまつわるテーマは、近年、ITRが実施する他の調査でも共通して重視度が高く、多くの国内企業にとって最優先で取り組むべき課題と認識されていることがうかがえる。

以下、「社内コミュニケーションの活性化」「IT機器・システムの更新時期への対応」「災害やシステムダウンへの対応(BCP/DR)」と続き、情報セキュリティに直接関わる項目では、「セキュリティ強化(個人情報保護)への対応」が32.7%で最上位の5位となった。この値は「営業力の強化」や「商品・サービスの品質向上」といった他の課題よりも選択率が高く、国内企業の多くが個人情報保護対策をきわめて重視していることがうかがえる。

その他のセキュリティ課題では、「サイバー攻撃への対応」(18.2%)が比較的高い選択率となった一方、「法規制への対応(全般)」をはじめとするコンプライアンス課題に関しては、15%未満の選択率にとどまった。

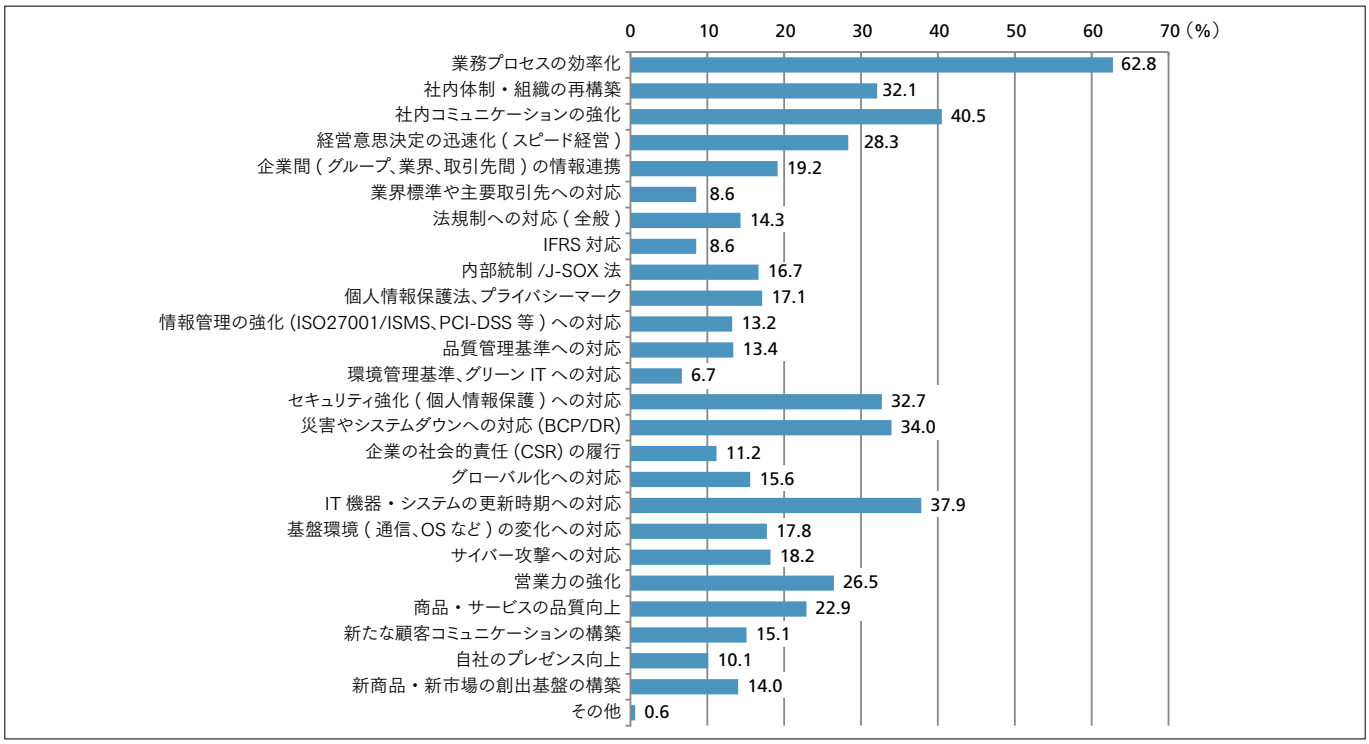

図1-1. 今後重視する経営課題（複数回答）

2-2.2011年調査との比較

なお、本質問は2011年5月実施の「企業IT利活用動向調査2011」（以下、「前回調査」という）でも実施していることから、前回調査との比較結果を図1-2に示す。

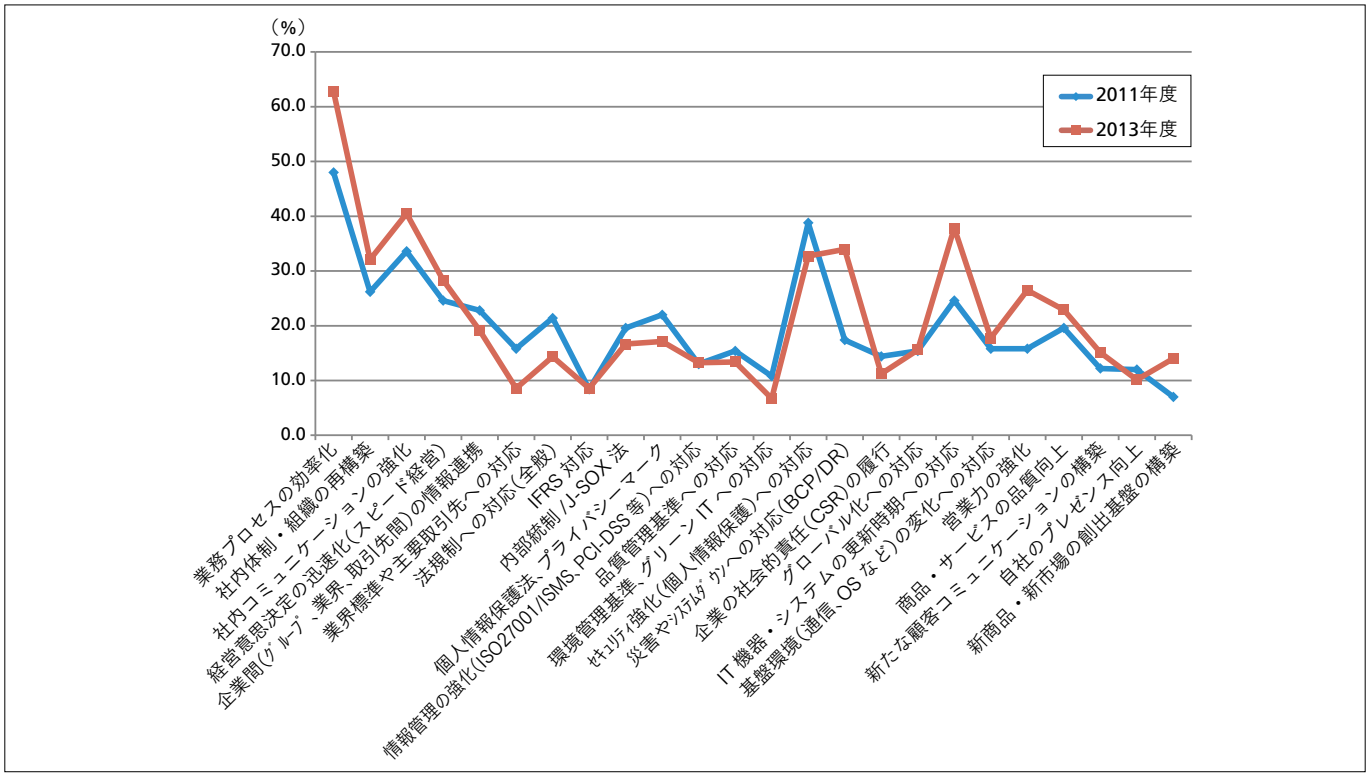

図1-2. 今後重視する経営戦略（2011年/2013年の比較）

比較結果から、セキュリティならびにコンプライアンスに関わる課題の重視度が2011年から若干低下していることがわかる。前回の調査実施時期は、東日本大震災の発生直後であり、ほぼ同時期に国内大手メーカの大量個人情報流出事件も大きく報道された。したがって、今回の結果から情報セキュリティへの課題認識が後退したとは言い切れず、むしろ攻めの経営課題がより重視されるようになったと考えるべきであろう。そうしたなかで、「災害やシステムダウンへの対応」が、震災直後にも増して大きく数値を伸ばしている事実は注目に値する。災害からの復旧がひと段落し、事業を継続することの重要性が幅広い企業で重視されるようになったことを示しているといえる。

また、「法規制への対応(全般)」に代表されるコンプライアンス課題の選択率が低下したことについては、多くの企業で対策が完了ないし定着した結果とみることもできる。本調査では、上記の経営課題に関して過去の投資効果の満足度も調査しているが、コンプライアンス課題は総じて投資効果の満足度が高く、成果がみえやすい課題であるとの結果が示された(図1-3)。

重視される経営課題として上位に挙げられている項目の多くが、過去の投資に「不満足」とする割合が高いため、引き続き重視せざるをえないという様子もうかがえる。

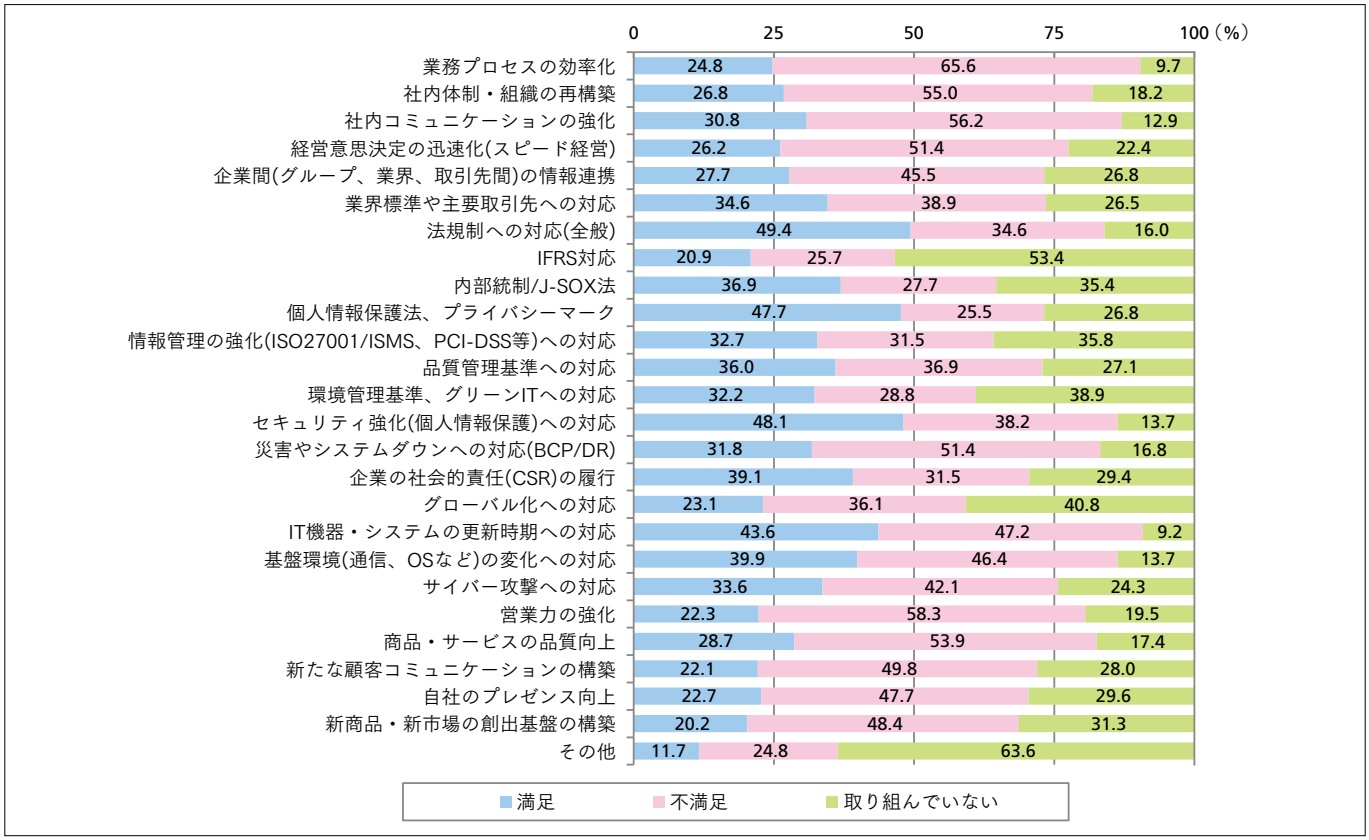

図1-3. 経営課題に対する過去の投資効果の満足度

3 インシデントの発生状況と標的型攻撃対策

本節では、国内企業の直近におけるセキュリティ・インシデントの発生状況と、近年国際的に被害が急増している「標的型攻撃」に対する意識、具体的な対策状況をみる。

3-1. セキュリティ・インシデントの発生状況

過去1年間に回答者の勤務先が経験したセキュリティ・インシデントを図1-4に示す。なお、本質問は発生の有無のみを問うており、被害の規模や回数は考慮していない。

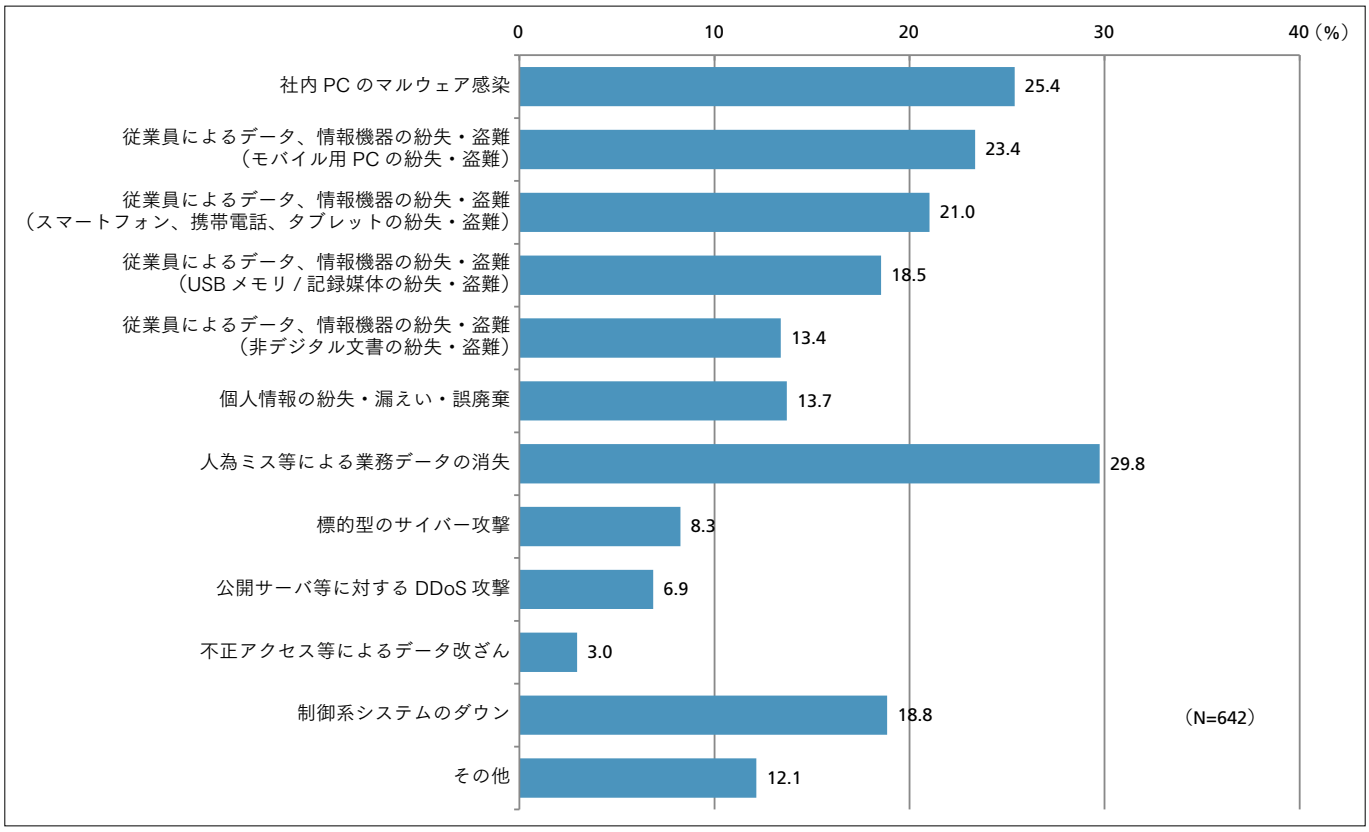

図1-4．過去1年間に経験したセキュリティ・インシデント

発生割合が最も高かったのは、「人為ミス等による業務データの消失」で、約3割の回答者が過去1年間で経験したと回答した。これは、純粋な意味でセキュリティ被害とは言えないが、事業継続性の観点からすれば、情報システムを取り巻く重大な脆弱性の1つである。

続いて目につくのは、データや情報機器の紛失・盗難の発生率の高さである。「モバイル用PCの紛失・盗難」「スマートフォン、携帯電話、タブレットの紛失・盗難」は、いずれも20％を超える回答者が経験しており、情報機器の紛失がセキュリティ被害の大きなきっかけとなりうることがはっきりと示された。これからの情報セキュリティ対策を考えるうえで、モバイル機器の紛失・盗難は「避けられない問題」と捉えるべきであろう。

一方で、「標的型のサイバー攻撃」「公開サーバ等に対するDDoS攻撃」「不正アクセス等によるデータ改ざん」といった組織の外部を発生源とするインシデントの発生率はいずれも1桁台にとどまった。しかしながら、これらのインシデントは秘密裡に実行されるケースが多く、企業にとってその発生がきわめて検知しにくいという特性があることを割り引いて考える必要があろう。また、発生率を事業形態別にみると、Eコマースや会員制Webサイトを運営しているような、ネットビジネスに積極的な企業では、インシデントの発生率が全体平均を大きく上回る傾向もみられる。

3-2.「標的型攻撃」のリスク対策

本調査の中で、特に重視した動向の1つが「標的型攻撃」に対する国内企業の意識である。従来型の無差別型攻撃とは異なり、特定の組織・企業に狙いを定めたこの種の攻撃は、2010年頃から国内でも話題に上るようになったが、その手口や目的は時を追うごとに悪質化している。事実、2012年度には国内でも官公庁や政府関連機関を標的とした攻撃が確認され、研究資料等が不正に窃取された可能性が指摘されたことは記憶に新しい。

こうした標的型攻撃への対処は、経済のグローバル化が進むなか、ビジネスの高付加価値化によって活路を見いだそうとする国内企業にとって死活問題である。本調査では、国内の情報システム管理者がこの問題をどのように認識しているか、また、具

体的な対策としてどのような取組みを行っているかを調査した。

まず、標的型攻撃のリスクへの重視度合いを問うた結果が図1-5である。

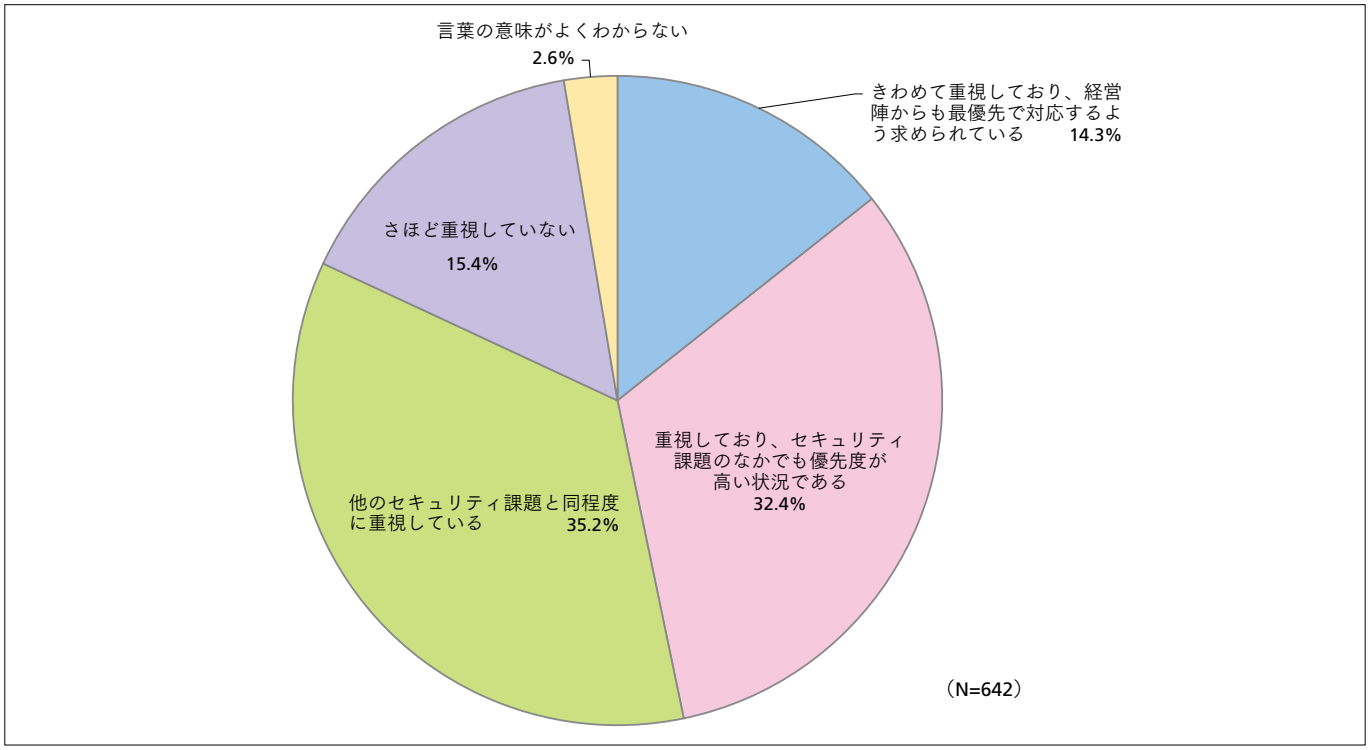

図1-5.「標的型攻撃リスク」の重視度合い

標的型攻撃のリスクを「重視している」との回答は全体の8割を超えており、14.3％が「最優先課題」、32.4％が「セキュリティ課題のなかでも優先度が高い」と回答した。一方で、「さほど重視していない」は15.4％、「言葉の意味がよくわからない」はわずか2.6％にとどまった。政府機関やメディア等による注意喚起の効果もあり、多くの企業でそのリスクの存在が認知されていることがうかがえる。

次に、具体的な標的型攻撃対策に有効とされる施策をピックアップし、その実施状況を調査した。これによると、対策も一定のレベルで進んでおり、「クライアントOSに対するパッチ適用の徹底」（65.6％）「端末からの外部通信の経路制御」（65.0％）「PC用アプリケーションに対するパッチ適用の徹底」（62.8％）「重要システムのインターネットからの隔離」（61.8％）の4項目が6割を超えた（図1-6）。

今後に向けて、特に対策が進むとみられるのは「標的型攻撃対策製品」の利用で、クライアント型製品、ネットワーク型製品のいずれについても、10％前後の回答者が「1年以内の利用開始」を予定している。また「ネットワーク・トラフィック・データの保存と分析」も、10％が1年以内、6％が3年以内の実施を予定している。

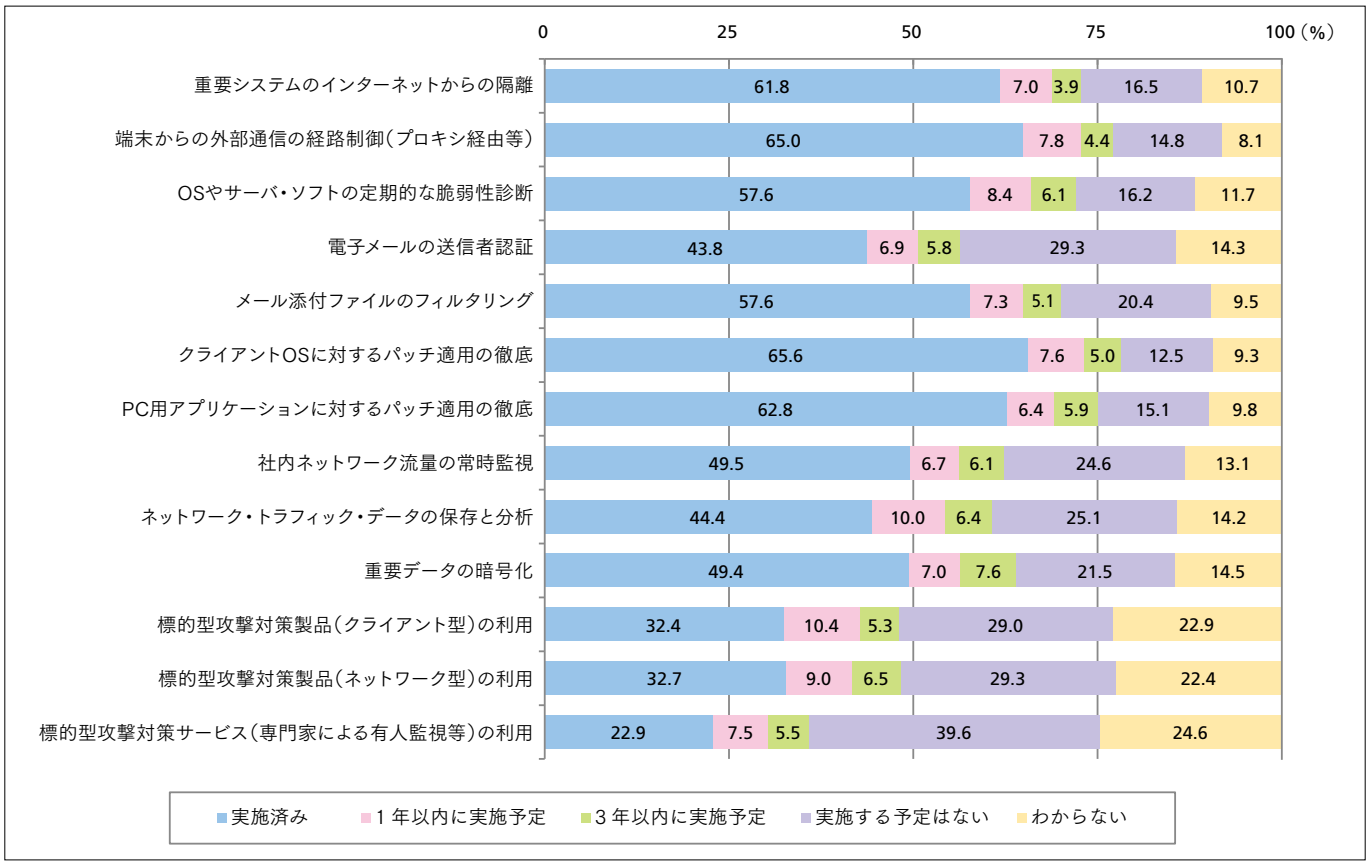

図1-6.「標的型攻撃対策」の実施状況

4 情報セキュリティに関する認定／評価制度の動向

情報セキュリティに対する組織の対応レベルを可視化するための仕組みとして、企業の間で広く認知されているのが第三者による認定／評価制度である。本調査では、主要な制度について、現在の取得状況と今後の取得意欲について調査した。

4-1.高い認知率を示したプライバシーマーク制度

国内において取得可能な主要8つの認定／評価制度を取り上げ、それぞれについての取得状況と今後の対応について調査した。最も取得率が高かったのは「プライバシーマーク制度」（34.7％）、次いで「ISMS適合性評価制度」（27.6％）となった（図1-7）。この上位2つの制度は、回答者の認知度も75％以上と高く、現在、最も定着している認定／評価制度であると言えよう。

その他の制度は、いずれも取得率が10％前後、認知率が5～6割台と大きな差はない。この結果からも、認知度と取得率は比例関係にあることがわかる。

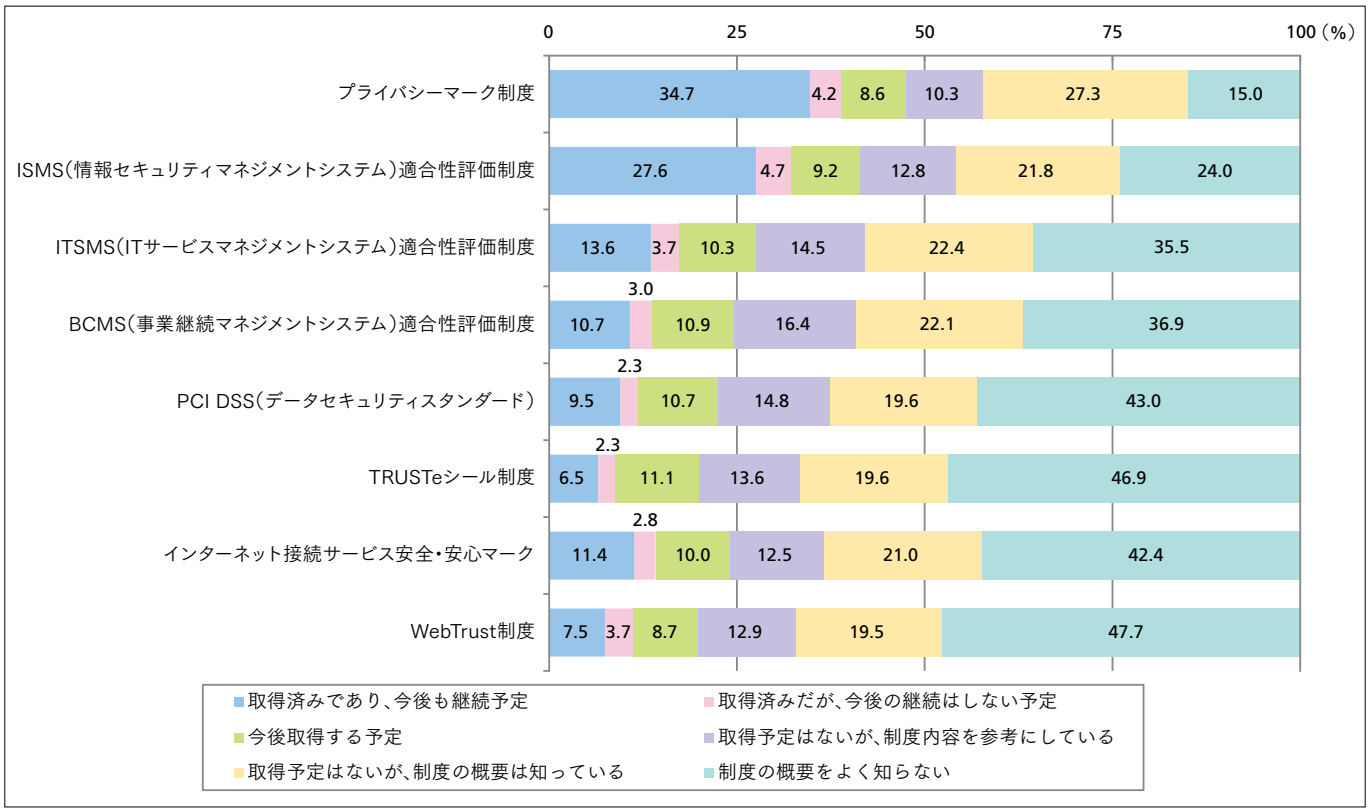

図1-7. 情報セキュリティに関わる認定／評価制度の取組み状況

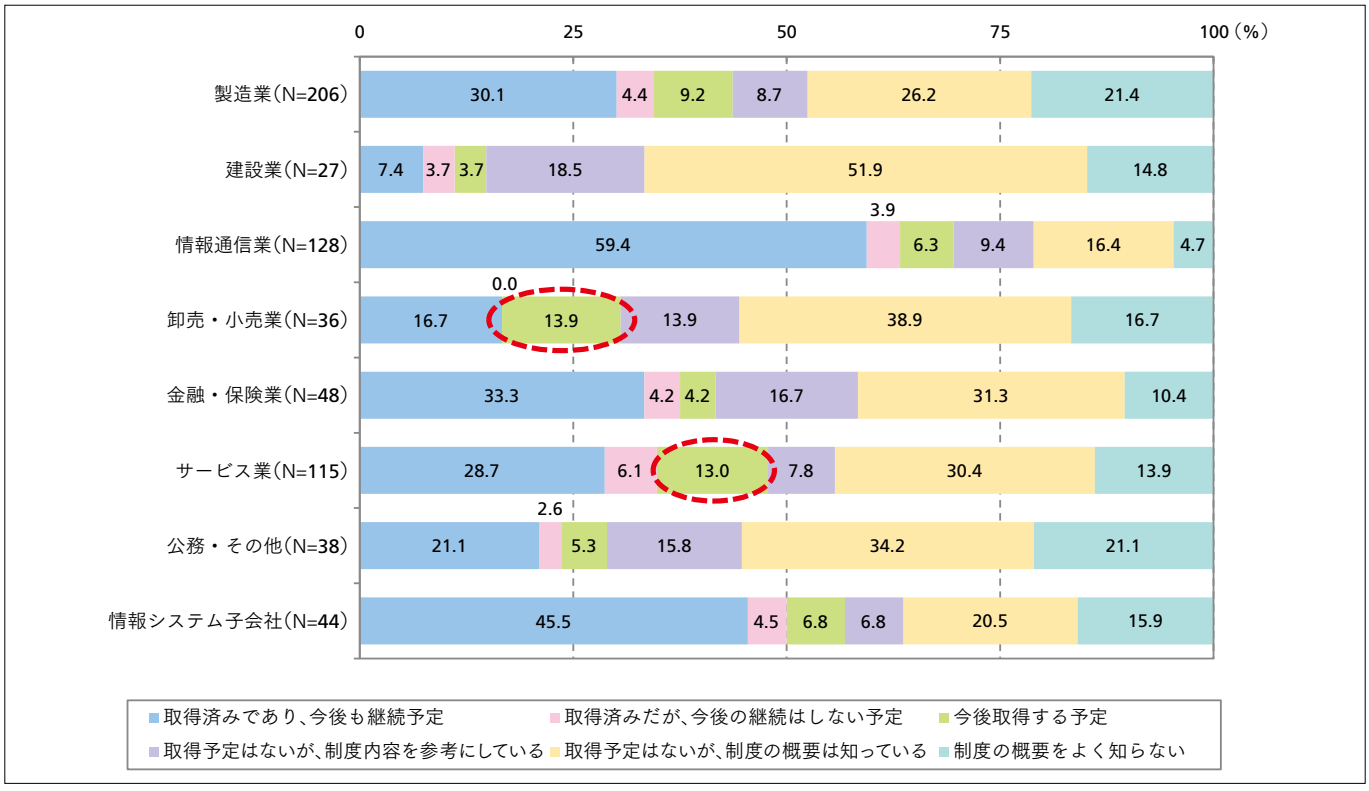

図1-8.「プライバシーマーク制度」の取組み状況（業種別）

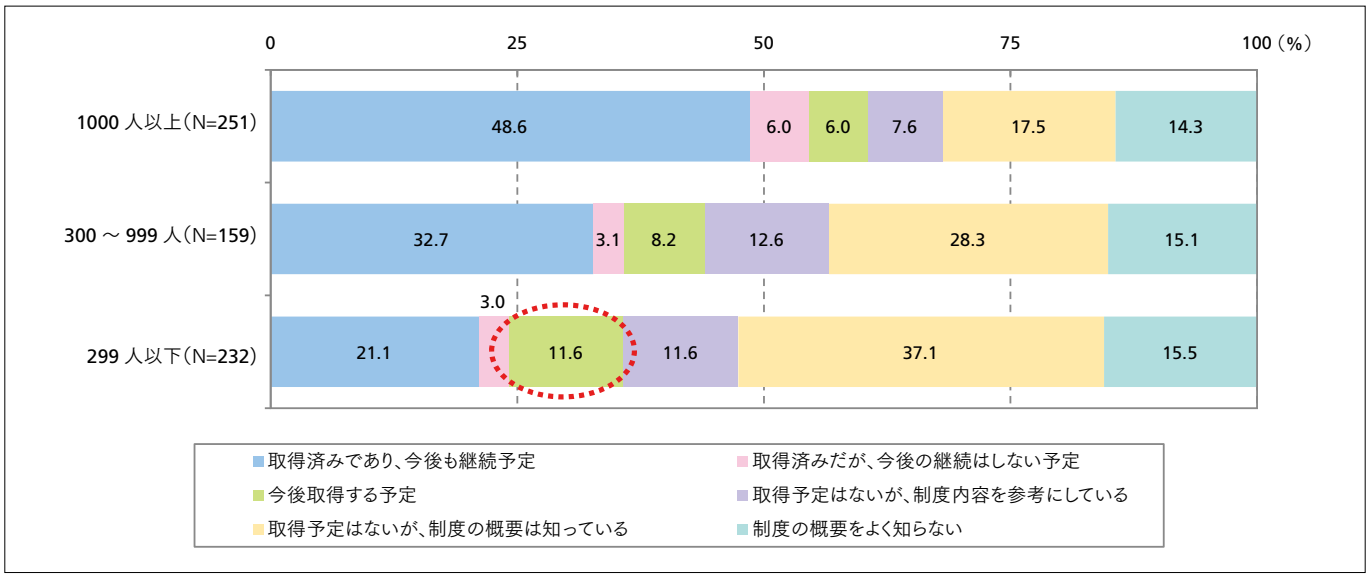

図1-9.「プライバシーマーク制度」の取組み状況（従業員数別）

とりわけ、プライバシーマーク制度は、企業間ビジネスにおいて契約の際の条件とされるケースが多いためか、比較的幅広い業種で取得されているのが特徴である。「今後取得する予定」の分布も幅広く、業種別では「卸売・小売業」と「サービス業」、従業員数別では「299人以下」の中小企業において、取得へ向けた意欲が高い（図1-8,1-9）。

これに対して、ISMS適合性評価制度は、技術面も含めたより包括的なセキュリティ対策が求められることもあり、取得企業の多くが情報系産業という特性がある。

組織的なセキュリティレベルを向上させるうえで、第三者からの認定／評価は推奨されるべき取組みであり、プライバシーマーク制度がその第1段階として幅広い業種や規模の企業から支持を得ていることがわかる。

5 情報セキュリティに関わる組織体制と人材育成

情報セキュリティ対策の有効性を高めるうえで、組織体制の整備と人材育成は避けて通れない課題である。本調査の結果からは、組織の整備は進展がみられたものの、その一方で人材に対する投資は遅れていることがはっきりと示された。

5-1.着実に進む組織体制の整備

前回調査で、今後に向けて課題として浮かび上がったものの1つが、情報セキュリティに対する組織体制の不備であった。全社的な情報セキュリティ担当責任者（CISO）の任命率は4割以下にとどまり、それ以前に、情報セキュリティ担当スタッフを配備している企業が半分に満たない状況であった。

今回の調査で改めて組織体制の整備状況を問うたところ、その課題は着実に改善されていることが確認された（図1-10）。

特に、「情報セキュリティ担当部署の設置／明確化」「情報セキュリティ担当スタッフの配備／明確化」は、前回調査時から大きく実施率が上昇しており、情報セキュリティ対策の責任の所在を明確化しようという動きが進んでいることがうかがえる。

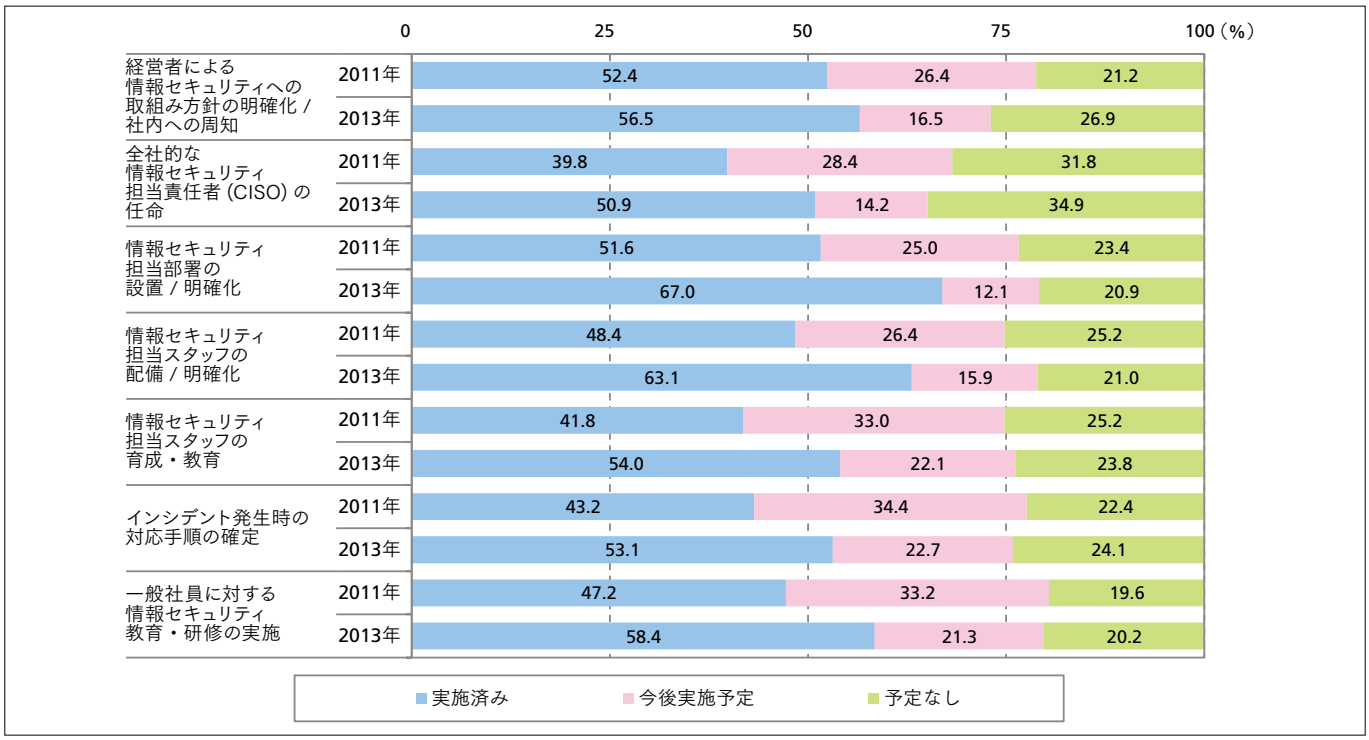

図1-10. 情報セキュリティに関する組織体制の整備状況

また、組織体制の整備という意味では、重要な情報資産の取扱い状況についても前回調査時から進展がみられた。5つの取組みについて、前回調査同様にその実施状況を調査したところ、全項目について実施率が上昇していることが確認できた（図1-11）。

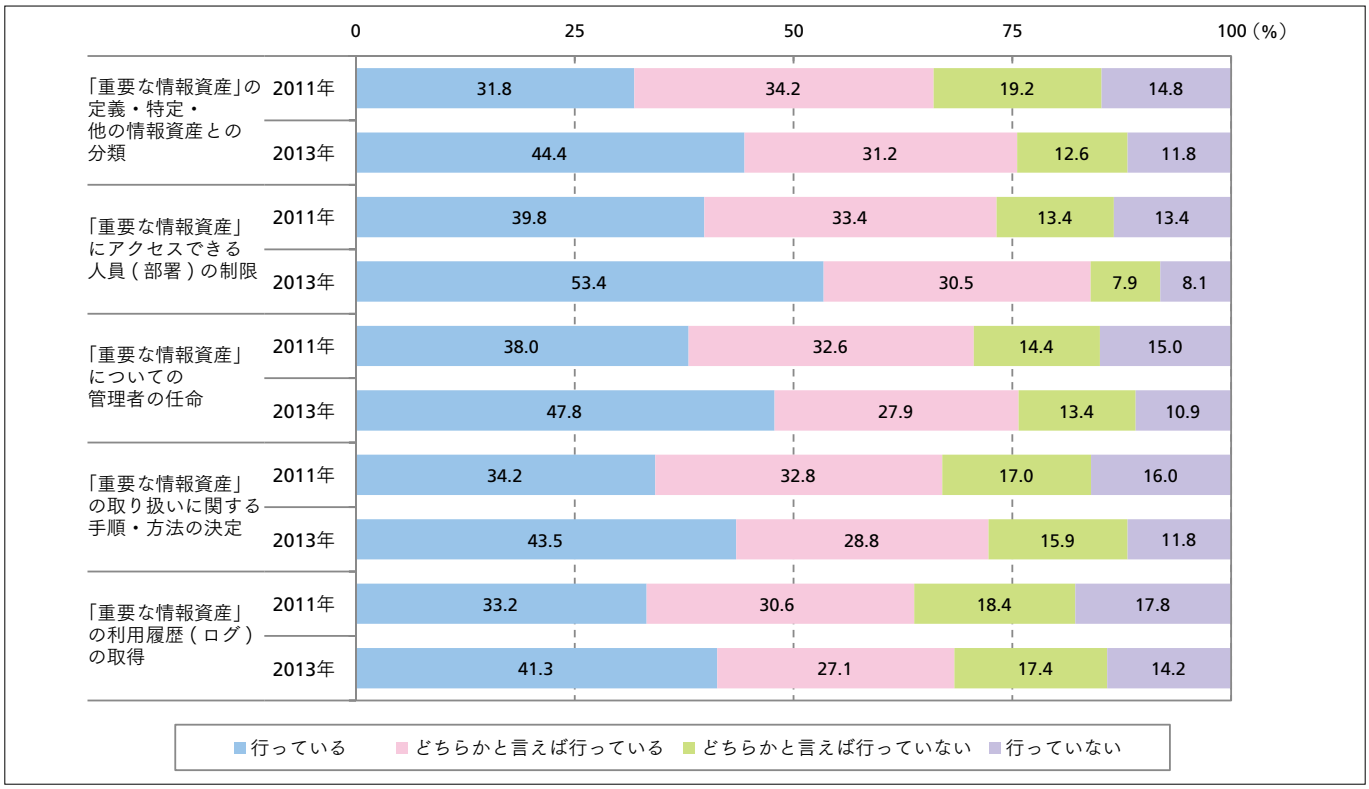

図1-11.「重要な情報資産」の保護に向けた取組み状況

5-2.課題はセキュリティ人材の育成

組織的な取組みに進展がみられた一方で、大きな課題として浮上したのが、セキュリティ管理業務に直接的に携わるスタッフ個々への支援の薄さである。今回の調査では、セキュリティ人材のスキルレベルを確認するために、資格制度に着目し、その取得状況を調査したが、その結果、国内企業においてセキュリティ関連の有資格者がきわめて少ないことが明らかとなった。

図1-12は、代表的な8つのセキュリティ関連資格を取り上げ、取得者の有無や取得推奨に向けた取組み状況を集計したものであるが、その結果をみると、「情報セキュリティアドミニストレーター（現情報セキュリティスペシャリスト）」がいる企業の割合は3割未満にとどまり、その他の資格についても、有資格者がいる企業はきわめて少ない。特に懸念されるのは、こうしたセキュリティ資格の取得を推奨している企業そのものが少ないとみられることである。

もっとも、資格取得はスキルレベルを測る1つの指標にすぎないが、上述のように、情報セキュリティの専任部署や担当者の任命といった取組みがいくら進んでも、実際にそこで活動するスタッフのスキルアップが十分に行われていなければ、昨今増加しているセキュリティ関連障害や、不測の事態への迅速な対応が難しくなる。国内では政府機関や捜査機関においてセキュリティ人材の不足が叫ばれているが、今後は一般企業においても、セキュリティ対策の目利きができる人材をどのように育成するかが課題となるだろう。

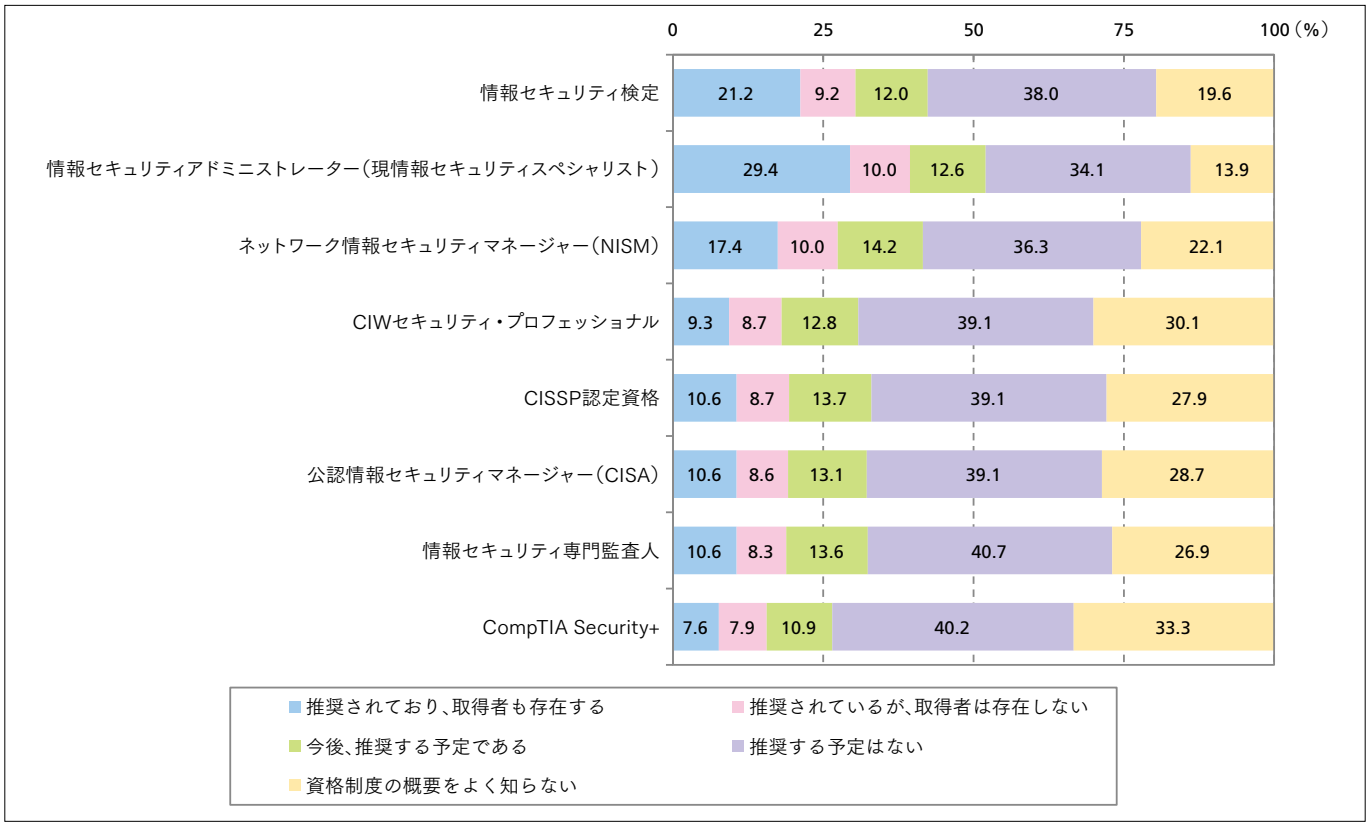

図1-12. セキュリティ関連資格の取得状況

6 情報セキュリティ製品の導入状況

セキュリティ管理業務が複雑化するなかで、技術を活用することの意義はこれまでになく高まっている。本節では、主要なセキュリティ製品を分野で区切り、企業での導入状況をみることにする。

6-1.ネットワークセキュリティ製品の導入状況

社内ネットワークと社外ネットワーク(インターネット)の境界線で動作するネットワークセキュリティ製品は、比較的導入効果がわかりやすく、近年は導入時の初期設定が不要なアプライアンス型製品が続々と投入されていることもあって、市場規模が拡大している分野である。項目別にみると、「ファイアウォール」が9割超と最も高い導入率となり、「通信の暗号化(VPNなど)」「URLフィルタリング・ツール」が続いている(図1-13)。

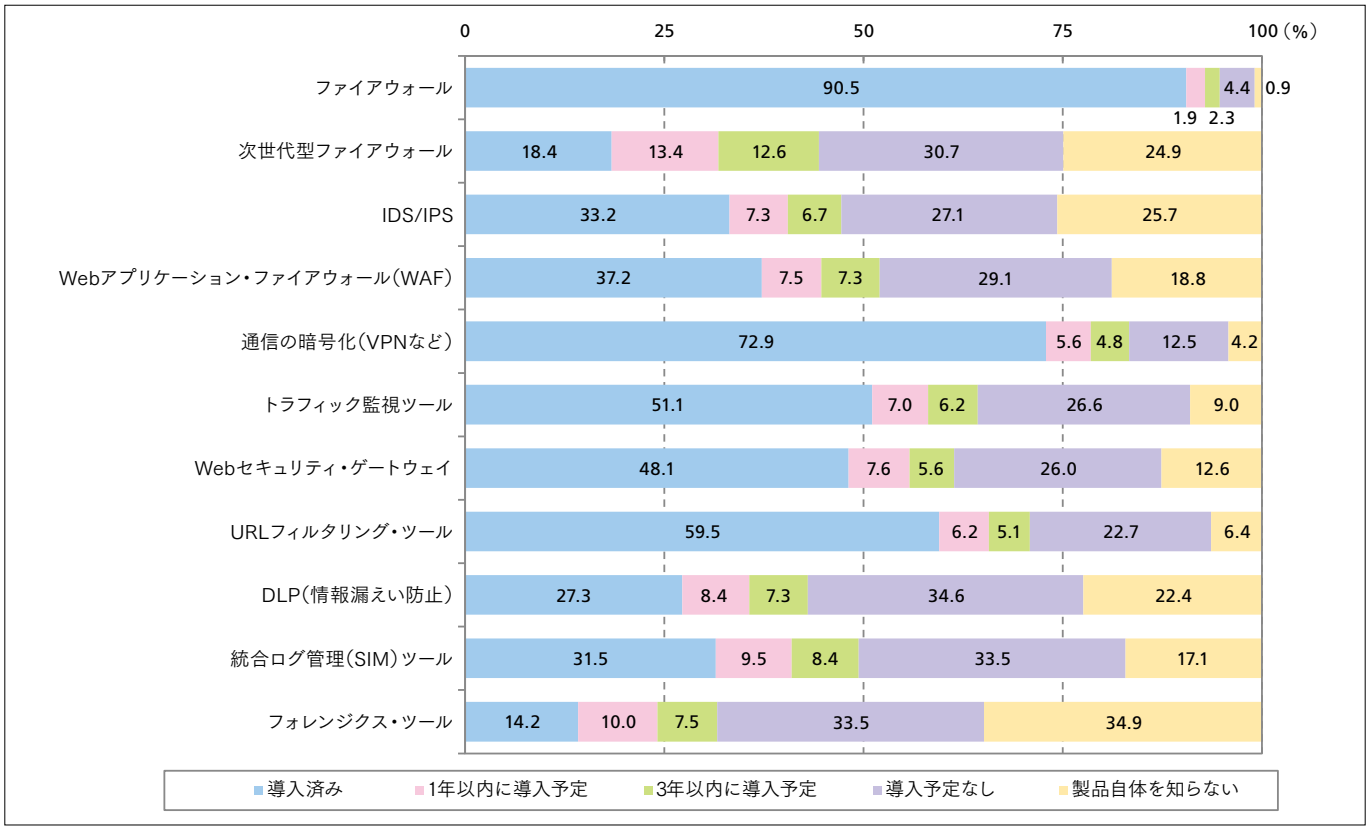

図1-13. セキュリティ製品の導入状況(ネットワーク・セキュリティ)

6-2.クライアント・セキュリティ製品の導入状況

主としてクライアントPCの保護を目的に利用される製品としては、「ウイルス対策ソフト(クライアント型)」の導入率が最も高いのは当然として、「PC資産管理ツール」や「パッチ管理ツール」の導入率も5割を超えており、多台数のPCを集中管理できる製品の導入が比較的進んでいる(図1-14)。

今後に向けては、「シンクライアント・システム」の導入意欲が高く、「1年以内に導入予定」と「3年以内に導入予定」を合わせると、20%以上が導入に前向きである。

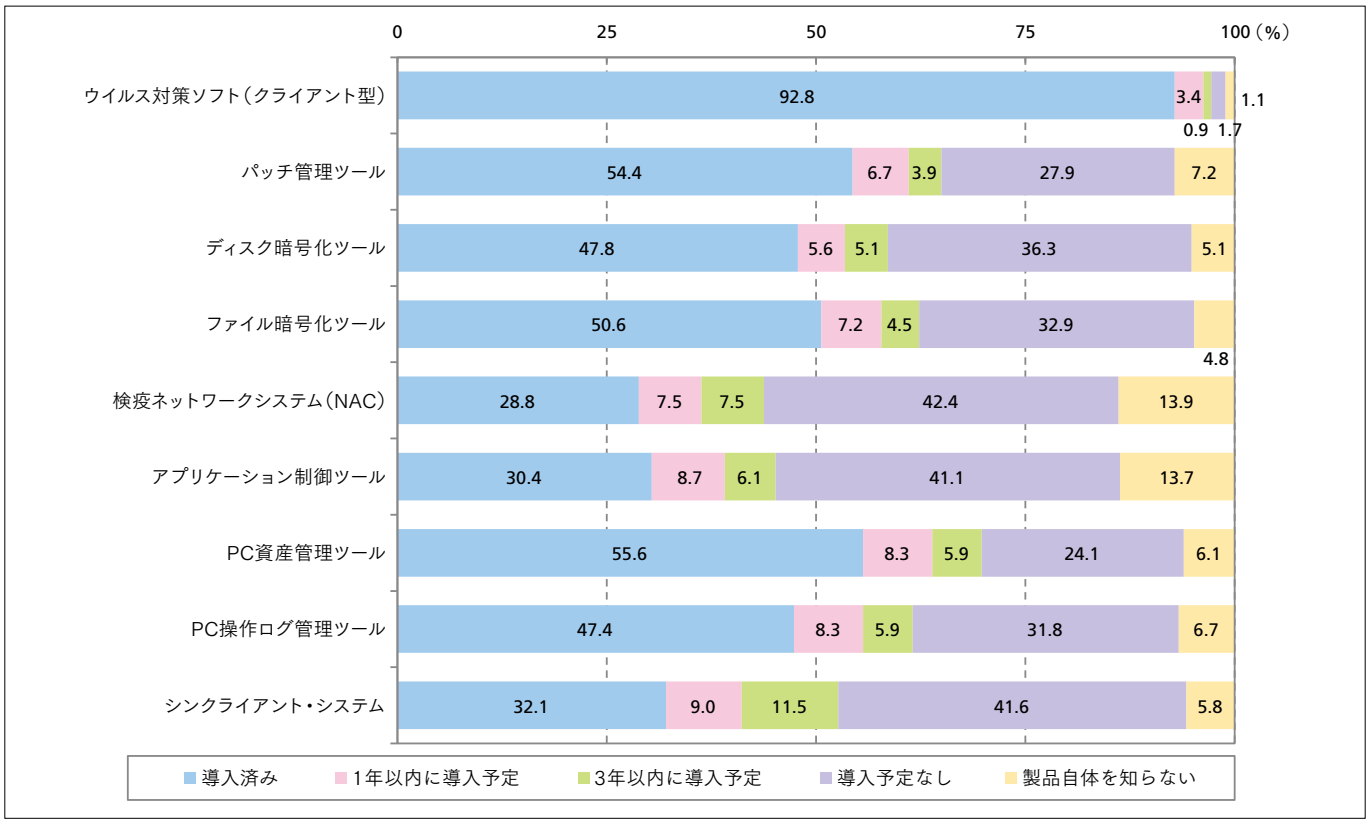

図1-14. セキュリティ製品の導入状況（クライアント・セキュリティ）

6-3. メール・セキュリティ製品の導入状況

標的型攻撃の初期侵入に利用されたり、内部から外部への情報漏えい経路になったりすることが想定される電子メール対応のセキュリティ製品については、あまり大きな動きはみられないものの、直近（1年以内）に新たに導入を予定している企業の割合が比較的高い傾向がある（図1-15）。一方で、中長期的な視点でみると、投資を計画している企業の割合は他の分野と比べるとさほど高くない。

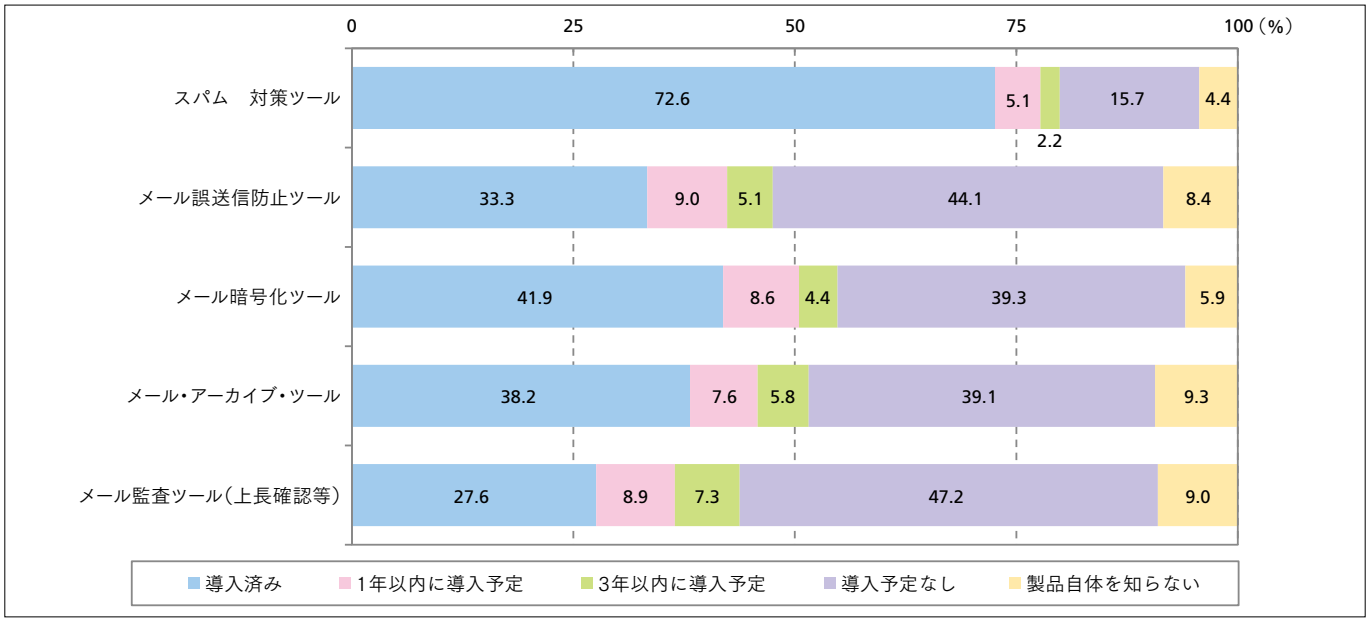

図1-15. セキュリティ製品の導入状況（メール・セキュリティ）

6-4.アクセス管理製品の導入状況

ユーザ認証をつかさどるアクセス管理製品については、他分野と比べて全体的に導入があまり進んでいない(図1-16)。スマートデバイスの普及に伴うマルチデバイス化や、クラウド型サービスの普及等によって、認証基盤の重要性はより高まるとみられるだけに、今後に向けて、さらなる普及・啓発が必要な分野であるといえよう。

そうしたなか、一度の認証処理によって複数のシステムやサービスへのアクセスを可能にする「シングルサインオン基盤」は、現在の導入率が比較的高く、今後に向けても一定の伸びが期待できる製品である。

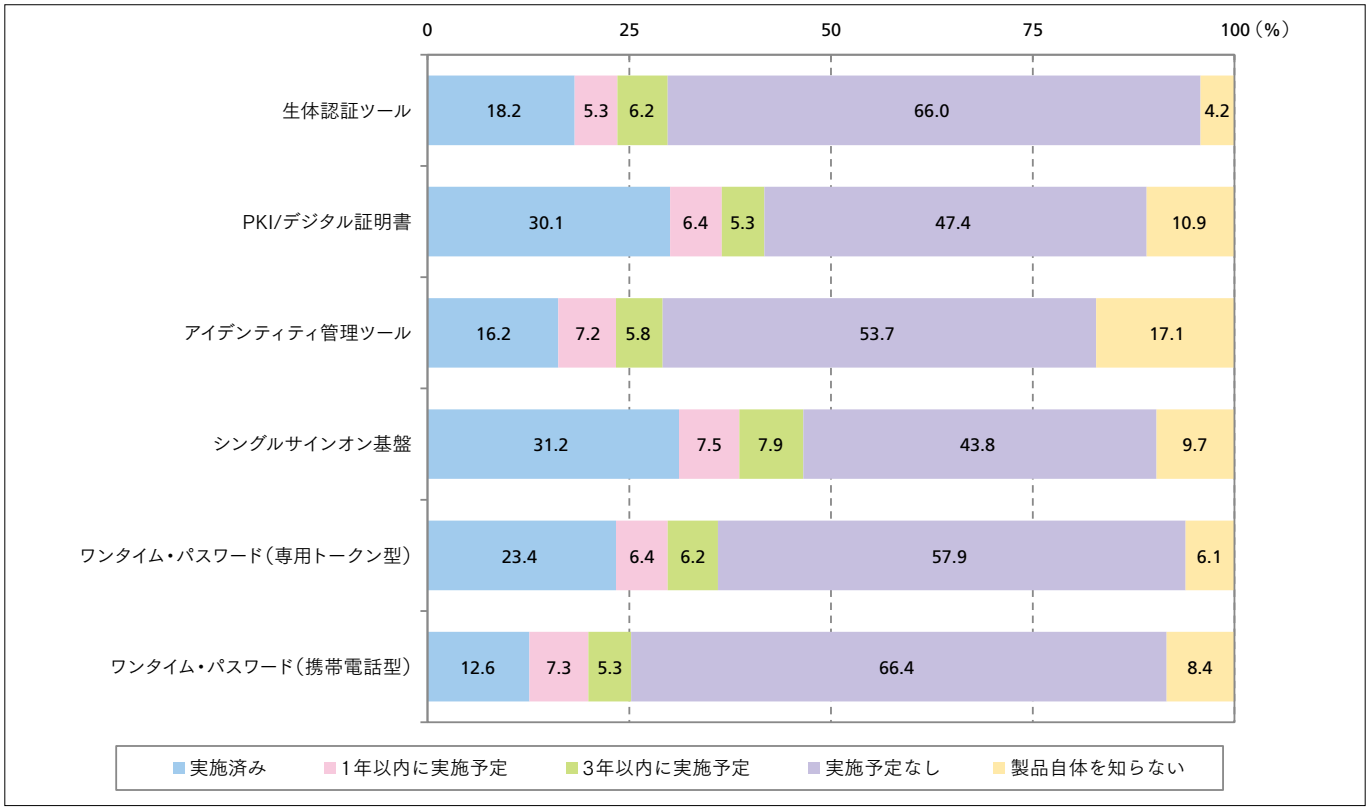

図1-16. セキュリティ製品の導入状況(アクセス管理)

7 モバイルセキュリティと物理セキュリティ

スマートフォン、タブレットの普及に伴い、モバイル環境のセキュリティ対策に改めて注目が集まっている。また、東日本大震災の発生以降、物理セキュリティ/災害対策への関心も高い。本節では、それら2つの対策状況を分析する。

7-1.進展するスマートデバイスの業務活用

モバイルセキュリティの動向を確認するうえでの前提として、回答者の勤務先におけるスマートデバイスの活用状況を調査した。

図1-17は、スマートフォン、タブレットそれぞれの現在の導入状況と今後の利用計画についての結果である。これによると、スマートフォンとタブレットは、試験導入も含めれば5割近い企業が会社支給による導入をすでに実施しており、業務用端末として一定の地位を確立していることがうかがえる。

また、現時点ではスマートフォンを導入する企業の割合が優勢だが、今後に向けてはタブレットの導入を検討する企業の割合が上回っていることも注目に値する。タブレット人気の高まりは、他の調査結果でも共通してみられる傾向であり、今後のセキュリティ対策はタブレットを前提に考える必要があるといえよう。

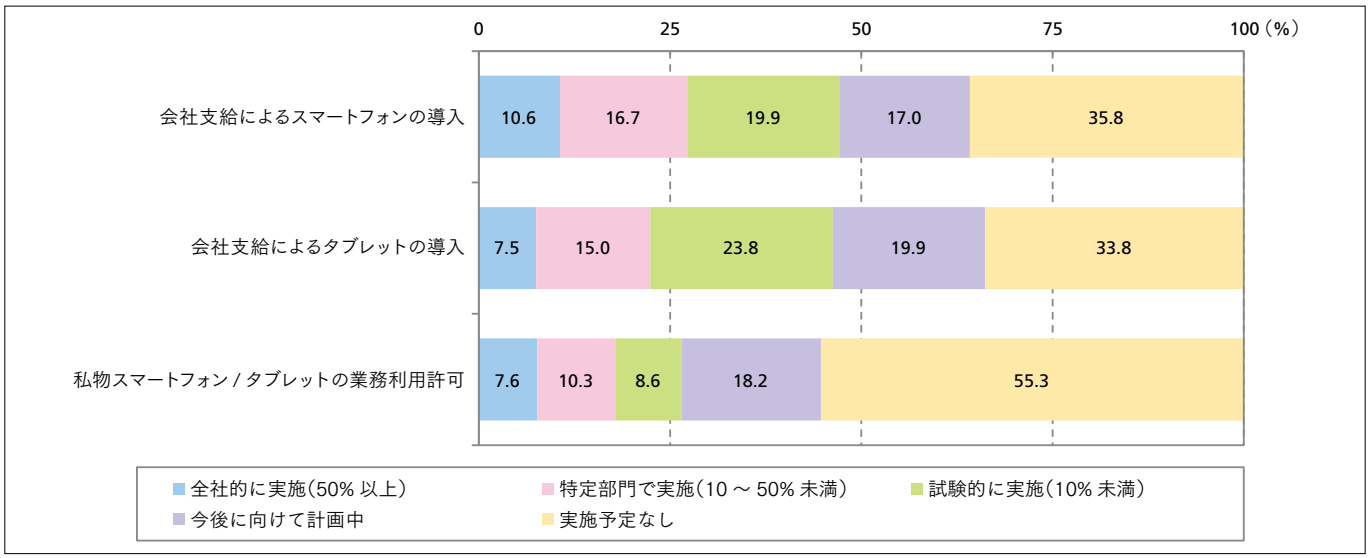

図1-17. スマートデバイスの業務活用状況

会社支給によるスマートデバイスの業務利用が着実に進展している一方で、近年話題となっている私物端末の業務利用（BYOD:Bring Your Own Device）の実施状況はさほど進んでおらず、計画中の企業を含めても、その割合は5割に達していない。少なくとも現時点においては、国内企業のBYODに対するスタンスはきわめて保守的と考えられる。

7-2.スマートデバイス向けセキュリティ対策の実施状況

スマートフォンまたはタブレットの会社支給を「実施済み」、ないしは「計画中」とした企業に所属する回答者（459件）を対象に、どのようなセキュリティ対策を実施しているか、あるいは計画しているかを調査した結果が図1-18である。

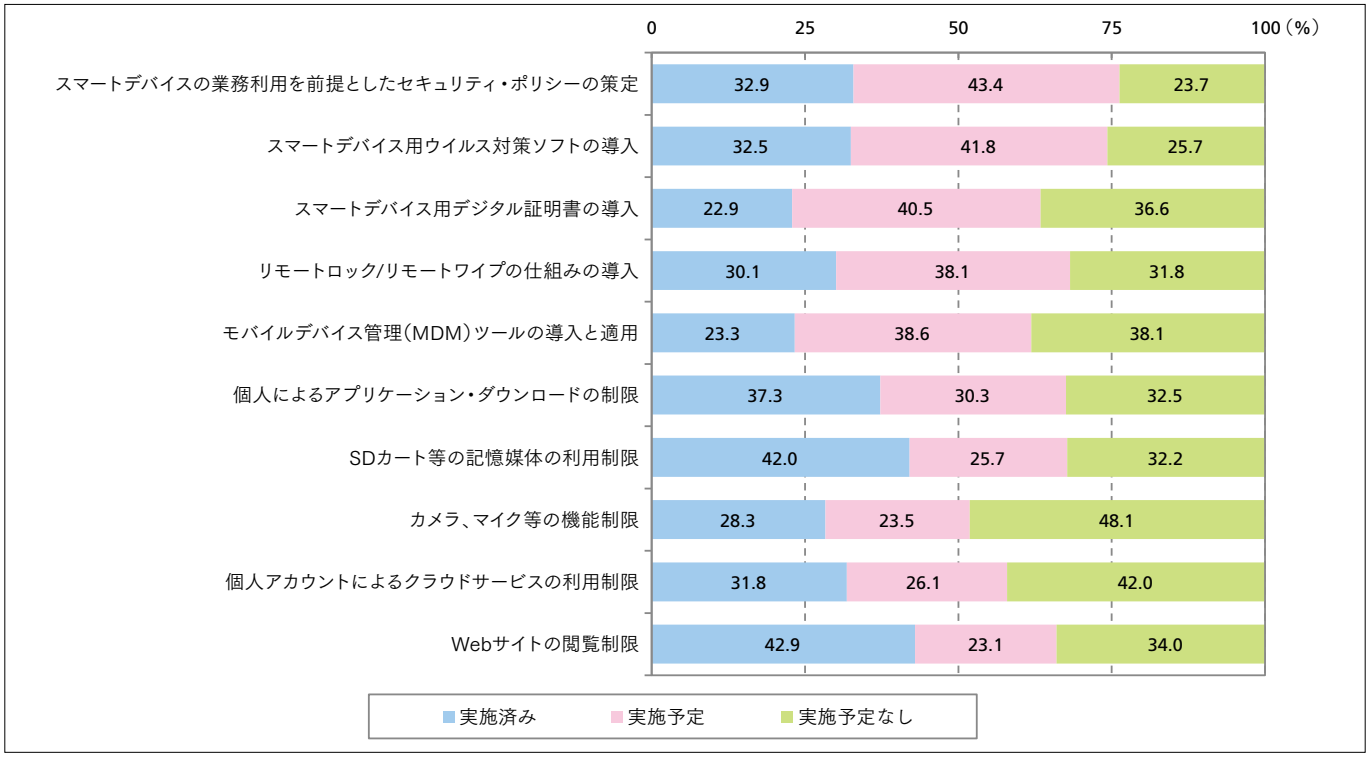

図1-18. 会社支給のスマートデバイス向けセキュリティ対策の実施状況

現時点で最も実施率が高いのは「Webサイトの閲覧制限」と「SDカード等の記憶媒体の利用制限」であった。この結果をみると、多くの企業が社用端末の私的利用と、端末からの情報漏えいを警戒している様子が見てとれる。また、スマートデバイスのセキュリティを確保するうえで有効とされるモバイルデバイス管理（MDM）ツールの導入は、現時点では2割強と高くないが、今後導入を予定している割合が4割近くに上っている。

7-3. 物理セキュリティと災害対策の関心事はデータセンタ

本調査では、物理セキュリティと災害対策に関する取組み状況についても着目した。今回は、主要な8項目に対する実施状況を「東日本大震災前」「東日本大震災後」に分けて調査した（図1-19）。

結果から、震災後にデータセンタの運用にまつわる見直しが積極的に行われたことがうかがえる。「免震構造、防災設備を備えたデータセンタの利用」「停電対策（無停電化）を講じたデータセンタの利用」は、いずれも震災後に1割近い企業が新たに実施し、実施率が5割を上回った。また、従来はごく一部の業種や大企業を中心に実施されてきた「複数のデータセンタへの分散保管」も、2割以上が「今後実施予定」と回答するなど、急速に関心が高まっていることがうかがえる。

今後は、自社内での対策はもとより、データセンタ事業者に対してより高い可用性やセキュリティレベルを要求する企業が増えることが予想される。

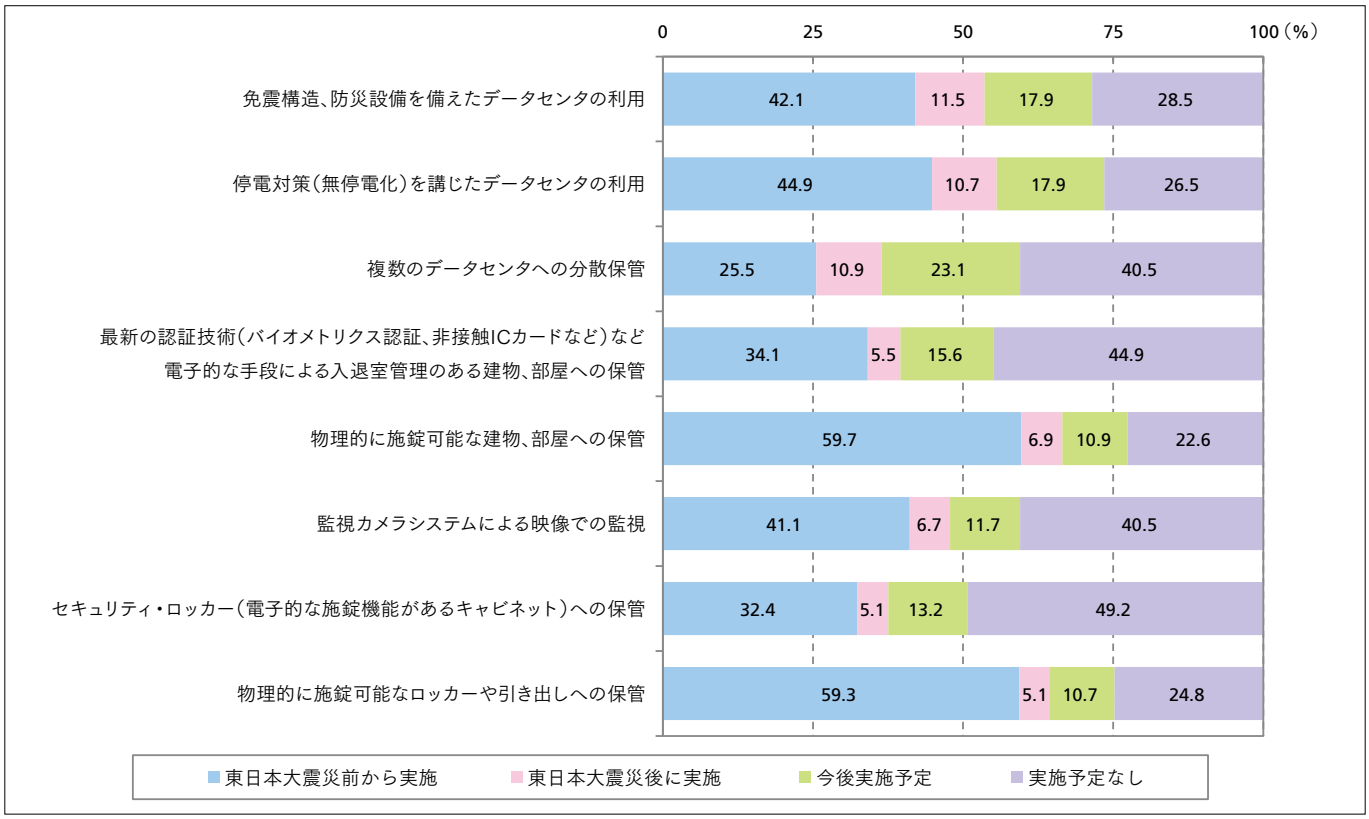

図1-19. 物理セキュリティと災害対策の実施状況

8 総評

標的型攻撃に代表される外部からの脅威に改めて関心が向けられるなか、今回の調査では、国内企業においてセキュリティ対策が重要な経営課題の1つと認知されていることが改めて確認された。また、認定／評価制度の取得やセキュリティ組織の整備、重要な情報資産の取扱いルールの確立など、組織やプロセスにまつわるセキュリティ対策が着実に進展している様子もみてとれた。多くの企業においてセキュリティレベルの高度化に組織を挙げて取り組んでいることが示されたことは積極的に評価できる。

その一方で、個々の人材に対する支援の薄さなど、深刻な課題もまた浮き彫りとなった。たしかに、組織やプロセスの整備はセキュリティ対策を高度化するうえで重要な取組みであるが、その取組みを持続性あるものにするためにも人材の充実は不可欠である。企業のCIOの中には「セキュリティの専門スキルはベンダから調達すればよい」と言い切る向きも少なくないが、今日の企業に求められるのは、さまざまなセキュリティ課題を自社のビジネスと結び付けて、そのインパクトを適正に見極めることのできる目利きの能力である。そうした能力をもつ人材をどのように社内で確保するかは、すべての企業にとって喫緊の課題である。この課題を解決するためには、個々の企業の努力はもちろんだが、政府ならびに業界全体の支援も必要となろう。

セキュリティ製品の導入意欲では、ネットワークレベルでの脅威の検知と可視化、ならびにモバイル環境のセキュリティ強化を実現するための技術に、今後注目が集まることが予想される。また、東日本大震災によって事業継続性の確保が重要課題として浮上するなかで、データセンタ事業者に対する期待が大きく膨らんでいることも確認された。

回答者プロフィール

業種	回答数	%
製造	206	32.1
建設	27	4.2
情報通信	128	19.9
卸売・小売	36	5.6
金融・保険	48	7.5
サービス	115	17.9
公務・その他	38	5.9
情報システム子会社	44	6.9
全体	642	100.0

年間売上高	回答数	%
1,000 万円未満	1	0.2
1,000 万円～ 1 億円未満	6	0.9
1 億～ 10 億円未満	64	10.0
10 億～ 100 億円未満	198	30.8
100 億～ 500 億円未満	140	21.8
500 億～ 1,000 億円未満	60	9.3
1,000 億～ 3,000 億円未満	39	6.1
3,000 億～ 5,000 億円未満	25	3.9
5,000 億円以上	82	12.8
売上げなし	27	4.2
全体	642	100.0

従業員規模	回答数	%
中小企業	232	36.1
中堅企業	159	24.8
大企業	251	39.1
全体	642	100.0

従業員規模	回答数	%
50 ～ 99 人	76	11.8
100 ～ 299 人	156	24.3
300 ～ 499 人	69	10.7
500 ～ 999 人	90	14.0
1,000 ～ 2,999 人	96	15.0
3,000 ～ 4,999 人	45	7.0
5,000 ～ 9,999 人	35	5.5
10,000 人以上	75	11.7
全体	642	100.0

業種	回答数	%
食料 : 飲料品	11	1.7
繊維工業	7	1.1
パルプ・紙・印刷	8	1.2
化学工業	12	1.9
石油製品	5	0.8
鉄鋼・金属	10	1.6
機械 / 電気機器	52	8.1
情報通信機器	14	2.2
電子部品・電子回路	14	2.2
精密機器	25	3.9
輸送機器	22	3.4
医薬	6	0.9
その他の製造業	20	3.1
農林・水産・鉱業	0	0.0
建設	27	4.2
電力・ガス	10	1.6
通信	14	2.2
情報システム子会社	44	6.9
情報（処理）サービス	90	14.0
メディア・出版・放送・広告代理店	8	1.2
調査会社	0	0.0
運輸・倉庫	16	2.5
卸売	24	3.7
小売	18	2.8
商社	18	2.8
銀行	26	4.0
証券	3	0.5
保険	11	1.7
その他金融（リースなど）	8	1.2
不動産	6	0.9
教育	13	2.0
医療・福祉	15	2.3
宿泊・飲食	4	0.6
娯楽・広告	2	0.3
その他のサービス	41	6.4
その他	9	1.4
官公庁	5	0.8
地方自治・公共団体	16	2.5
その他の公務	8	1.2
全体	642	100.0