JIPDEC IT-Report 2014 Spring

特集

「企業IT利活用動向調査2014」にみるIT化の現状

JIPDEC
一般財団法人日本情報経済社会推進協会

ITは今や私たちの生活に深く浸透するとともに、ITの普及により、新たな価値創造の実現と経済活動の活性化を促すことも、皆様すでにご承知のことと思います。

JIPDECは設立当初より、わが国のIT業界の動向をさまざまな視点から取り上げ、「コンピュータ白書」「情報化白書」にとりまとめ、紹介してきました。

JIPDEC IT-Reportは、これまでの「情報化白書」の後継的な情報発信手段として、JIPDECが今取り組んでいるさまざまな事業に関連するタイムリーなトピックスをお伝えすることを目的として2013年6月に創刊しました。

第3号となる「JIPDEC IT-Report2014 Spring」は、昨年の創刊号に引き続き、JIPDECが2011年から継続して実施しているIT利活用に関わる独自調査でわかった、経営課題の投資効果や情報セキュリティ対策の実施状況、モバイルデバイスの活用状況など、広範囲にわたる企業IT化の現状をご報告するとともに、IT業界を俯瞰するデータをとりまとめ、ご紹介しています。

ぜひ、今後のIT環境整備の参考にしていただければ幸いです。

一般財団法人日本情報経済社会推進協会

JIPDEC IT-Report2014 Spring

目　　次

【特集】「企業IT利活用動向調査2014」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、情報セキュリティ対策に重点を置いた「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:2014年1月27日～1月31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し、IT戦略策定または情報セキュリティ従事者で、係長相当職以上の役職者約2,800人
有効回答数:656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サービス業(26.1%)、次いで製造業(25.3%)、情報通信(15.7%)、卸売・小売業(12.2%)となった。所属部門では情報システム部門が最も多く(54.9%)、役職は部長(35.5%)、課長(30.6%)、係長・主任(14.3%)が回答者のほとんどを占めている。

IT戦略、セキュリティへの関与度を見ると、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」(57.0%)、「全社的なリスク管理／セキュリティ管理に責任をもっている」(53.0%)が半数以上を占めた。前回56.9%だった「セキュリティ対策の実務に関与している」が20ポイント弱減少(37.5%)したが、おそらく今回調査では、実務よりも管理者の立場としてセキュリティに関与している部長クラスの回答が多かったことも影響していると思われる。

2 経営におけるIT戦略の位置づけ

本調査では、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」をメインテーマとしているが、まず、経営課題の中で何が重視されているのか、情報セキュリティの位置づけがどのようになっているかを見てみる。

2-1.重視する経営課題

経営課題として考えられる全26項目について、ITの責任者として今後1～3年で何を重視しようとしているかを調査した。(図1-1)。その結果、「業務プロセスの効率化」(58.2%)が過去2回の調査に続いて選択率でトップとなった。業務プロセス改革に対する課題認識は、近年、さまざまな調査で共通して上位となっているが、今回の結果からも、その傾向が続いていることがうかがえる。

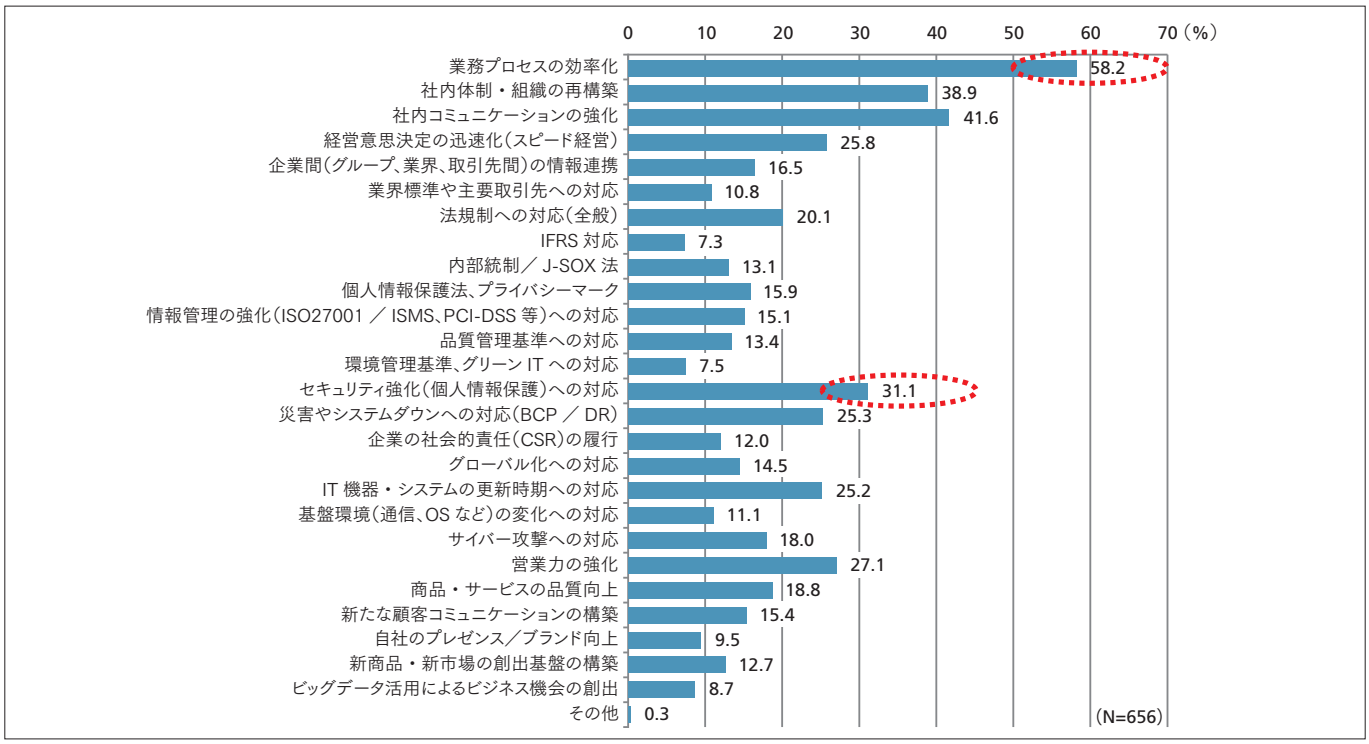

図1-1. 今後重視したい経営課題(複数回答)

セキュリティに関する課題の重視度合いを見ると、最も選択率が高いのは「セキュリティ強化(個人情報保護)への対応」で、31.1%の企業が重視している項目に挙げた。「内部統制/J-SOX法」に代表されるコンプライアンスに関わる項目は、全般的に重視度合いが低くなっている。

本調査は、2011年5月、2013年1月に続いて3度目となるが、上位8項目について選択率の経年変化をみると、「業務プロセスの効率化」が3度とも首位となったが、選択率は前年調査よりも若干下がった。その一方で、回を追うごとにじわじわと値が高まっているのが、最新の調査で2位となった「社内コミュニケーションの強化」、3位の「社内体制・組織の再構築」である(図1-2)。業務の自動化・省人化を目的としたIT整備が一巡するなかで、"ホワイトカラーの生産性向上"が、企業経営においてより重要度を増していると考えられる。

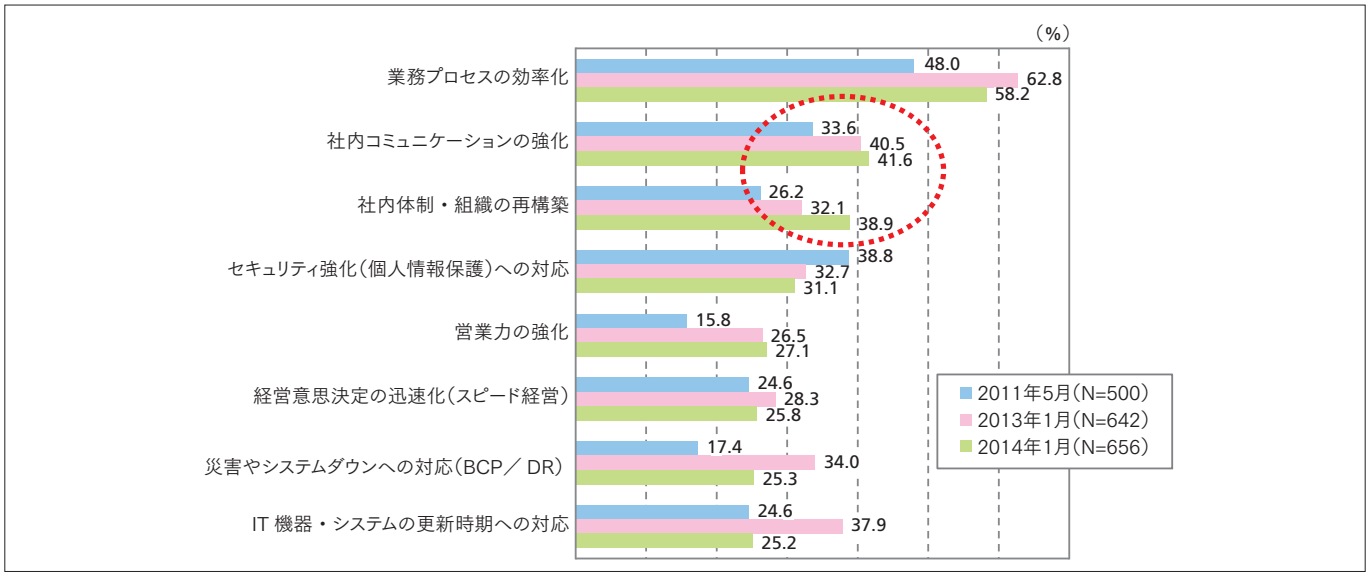

図1-2. 主要経営課題に対する選択率の経年変化(2011年/2013年/2014年)

2-2.ばらつきが大きい投資効果の満足度

次に、同じ項目について、過去に行ってきた投資効果に対する満足度を問うた結果が図1-3である。これを見ると、「満足」が「不満足」を上回っている項目がきわめて少ないことがわかる。重視する経営課題のトップ3に挙げられた「業務プロセスの効率化」「社内コミュニケーションの強化」「社内体制・組織の再構築」を見ると、いずれの項目も、「不満足」が「満足」の2倍以上の割合を占めている。

この結果からは、重視されている経営課題が過去の取り組みがうまくいっていないことの裏返しであることが示唆される。

一方、「個人情報保護法、プライバシーマーク」などのコンプライアンスに関わる項目、「基盤環境（通信、OSなど）の変化への対応」といった項目は、図1-1の結果からは重要度が低くなっているが、その反面で満足度が高くなっている。つまり、「過去の投資が着実に成果につながっているために、相対的な優先度が下がった」と見ることができる。

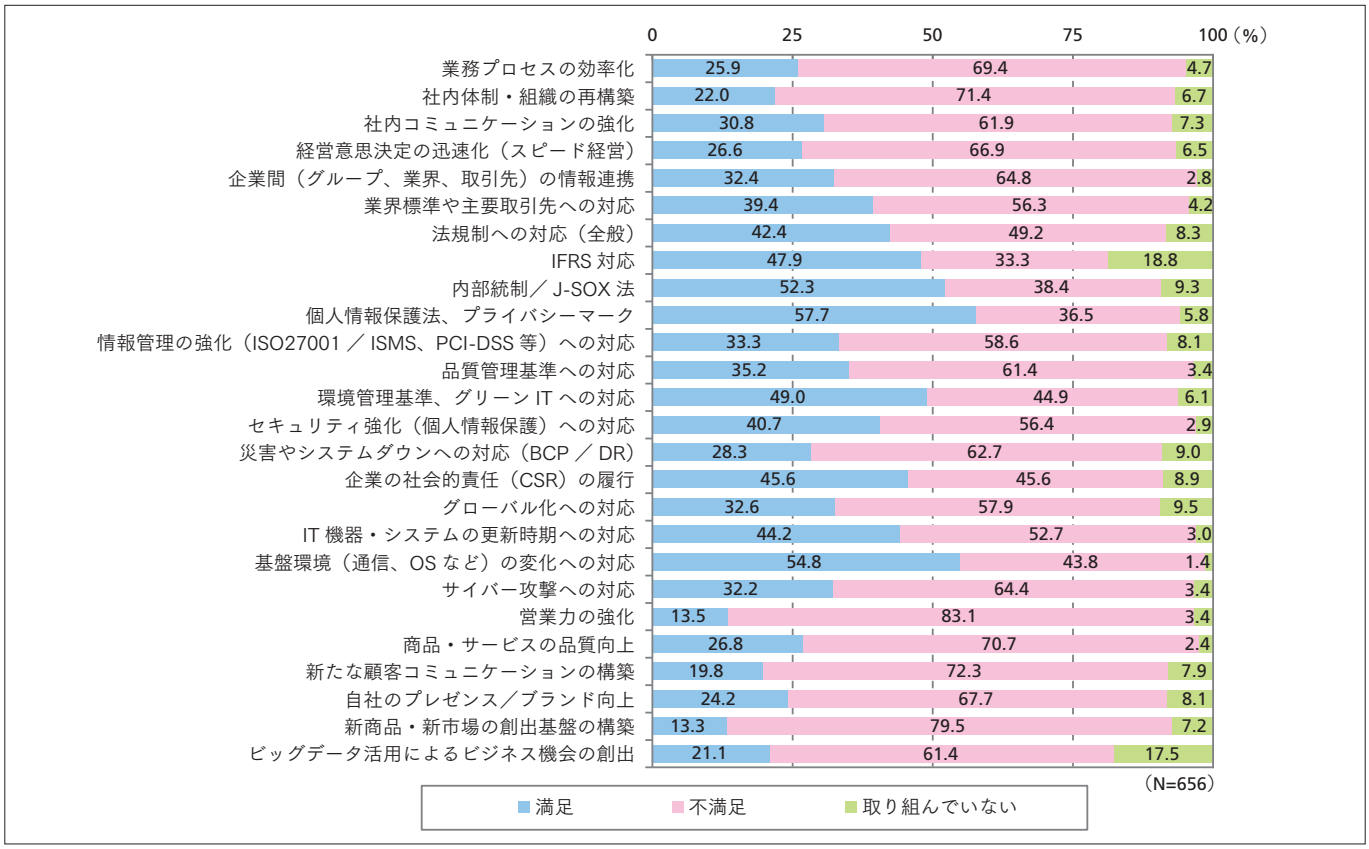

図1-3. 経営課題に対する過去の投資効果の満足度

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見る。

3-1.セキュリティインシデントの認知状況

過去1年間に回答者の勤務先がセキュリティインシデントを経験したか調査した。なお、ここでは被害の規模や回数は考慮していない（図1-4）。

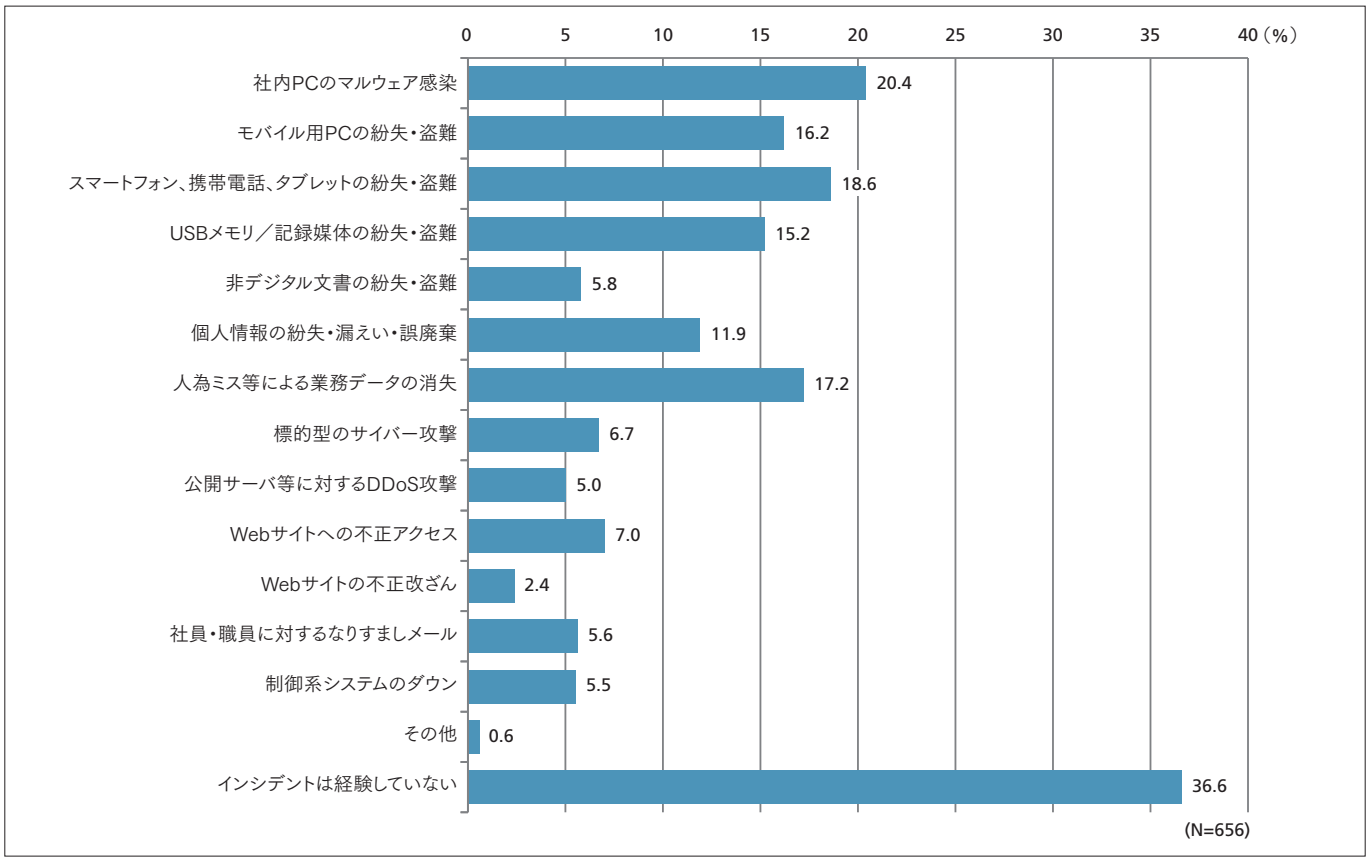

図1-4. 過去1年間に経験したセキュリティインシデント

認知率が最も高かったのは、「社内PCのマルウェア感染」で、20.4％の企業・組織が経験している。次いで「スマートフォン、携帯電話、タブレットの紛失・盗難」が18.6％で続いている。機器や文書の紛失・盗難は、情報漏えいの主な経路であるが、その中でモバイル端末がトップとなったのは、近年のスマートデバイスの普及拡大の影響によるものと見られる。今後その活用がさらに拡大していけば、それに比例して紛失・盗難の発生率も高まると懸念される。

ちなみに、前年の調査結果と比較すると、今年新たに追加した2項目（「Webサイトへの不正アクセス」「社員・職員に対するなりすましメール」）を除く全項目について、認知率は前年より低下している（図1-5）。特に、前年調査で認知率が高かった「人為ミス等による業務データの消失」「制御系システムのダウン」が、大きく数値を下げているのが特徴である。これは、個々の企業におけるミス撲滅の地道な努力や、政府系機関等による制御系システムの安全性確保のための広報活動などが実を結んだ結果として評価できるであろう。

なお、「標的型のサイバー攻撃」「公開サーバ等に対するDDoS攻撃」「Webサイトへの不正アクセス」といった、外部攻撃によってもたらされるインシデントは、いずれも1桁台にとどまった。ただし、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に留意が必要である。

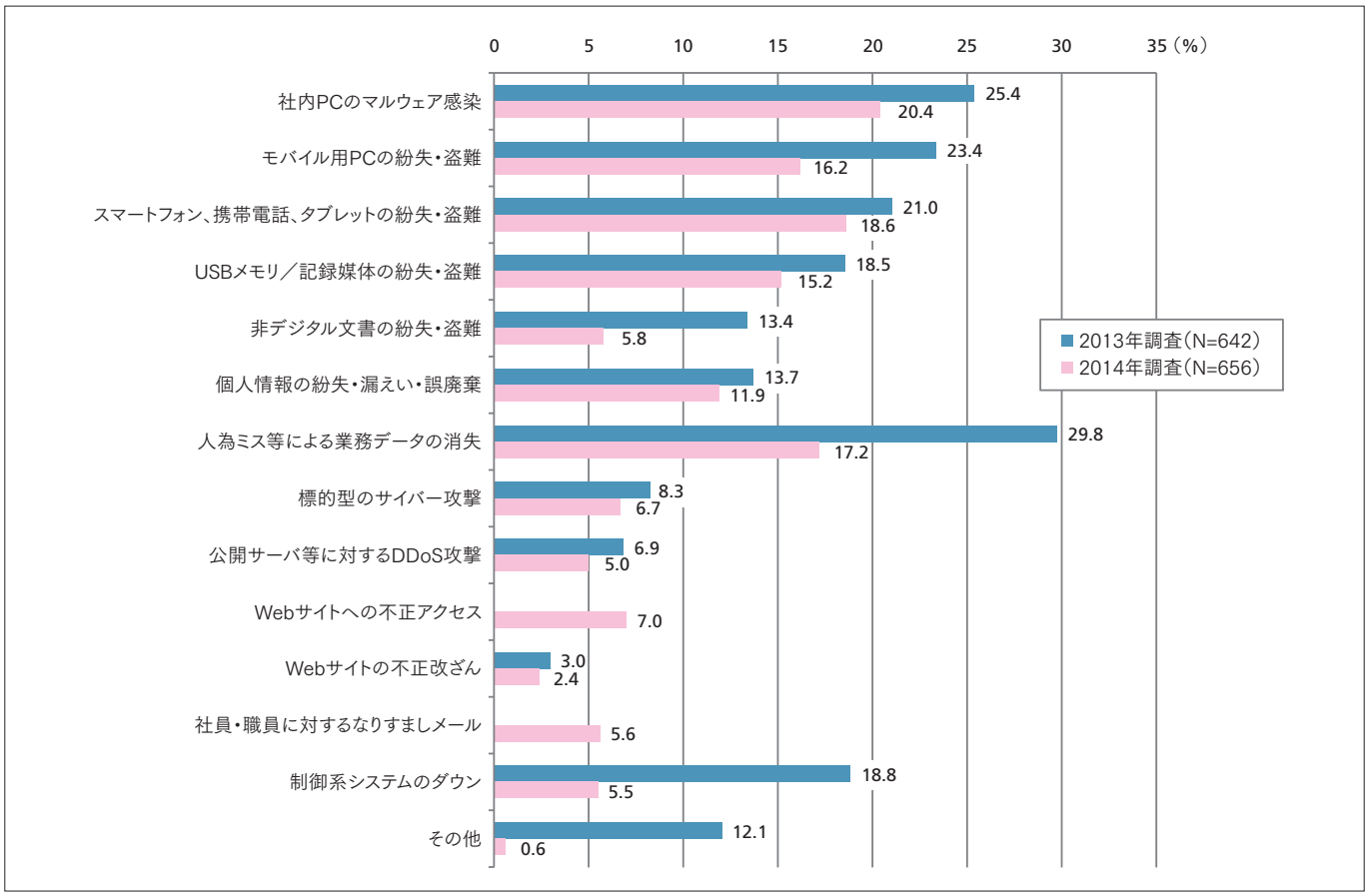

図1-5. 過去1年間に経験したセキュリティインシデント（前年調査との比較）

3-2.「標的型攻撃」の重視度とリスク対策

本調査において、前年調査から注視している動向の一つが、「標的型攻撃」に対する国内企業の意識である。図1-5で示したように、標的型のサイバー攻撃に遭ったとする企業の割合は前年よりも減少したが（8.3％から6.7％）、そのリスクを重視する企業の割合はむしろ増加している。標的型攻撃のリスクを「最優先で対応するよう求められている」とした企業の割合は、前年調査の14.3％から18.9％へと上昇した。それにより、他のセキュリティ課題よりも優先度が高いテーマと位置づける企業が全体の半数を超えた（図1-6）。知的財産や機密情報の重要性が高まるなかで、そうしたデータの窃取を狙う標的型攻撃に対する危機感が、より幅広い企業に共有されるようになったことがうかがえる。

その一方で、「リスクの度合いがわからない」とする回答が増加しており（2.6%から7.9%）、実態が掴みにくい標的型攻撃の影響度合いを測りかねる企業が増えていることも見てとれる。

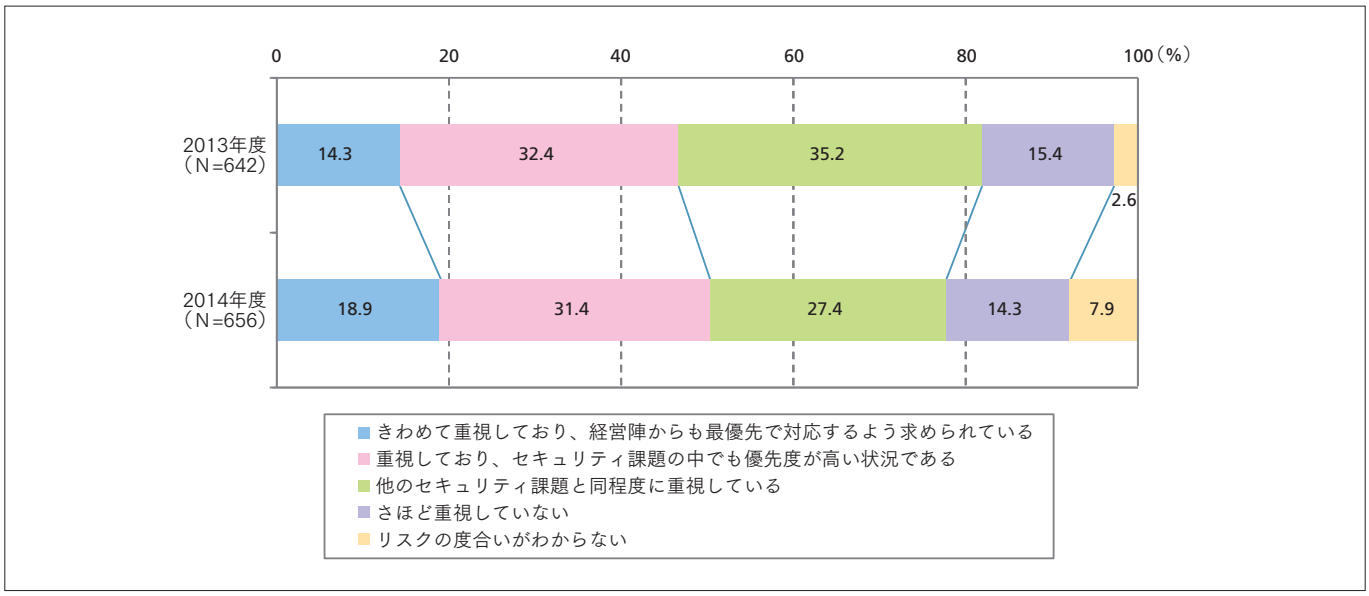

図1-6.「標的型攻撃リスク」の重視度合い（前年調査との比較）

次に、標的型攻撃対策で有効とされるものをいくつかピックアップし、その実施状況についても問うた。その結果、最も実施率が高かったのは「PCの管理者パスワードの個別化（使い回しをしない）」であり、54.9％が実施済みであると回答した（図1-7）。今回取り上げた各対策について、実施率そのものは前年から上昇していないものの、「1年以内に実施予定」とする企業の割合が全体的に高く、今後に向けて対策が進むと期待される。特に、「標的型攻撃対策サービス（専門家による有人監視等）の利用」は、「1年以内に実施予定」「3年以内に実施予定」を合わせると約24％が実施を予定している。大企業を中心に、技術だけでなく人的なサポートを望む企業が増加していることがうかがえる。

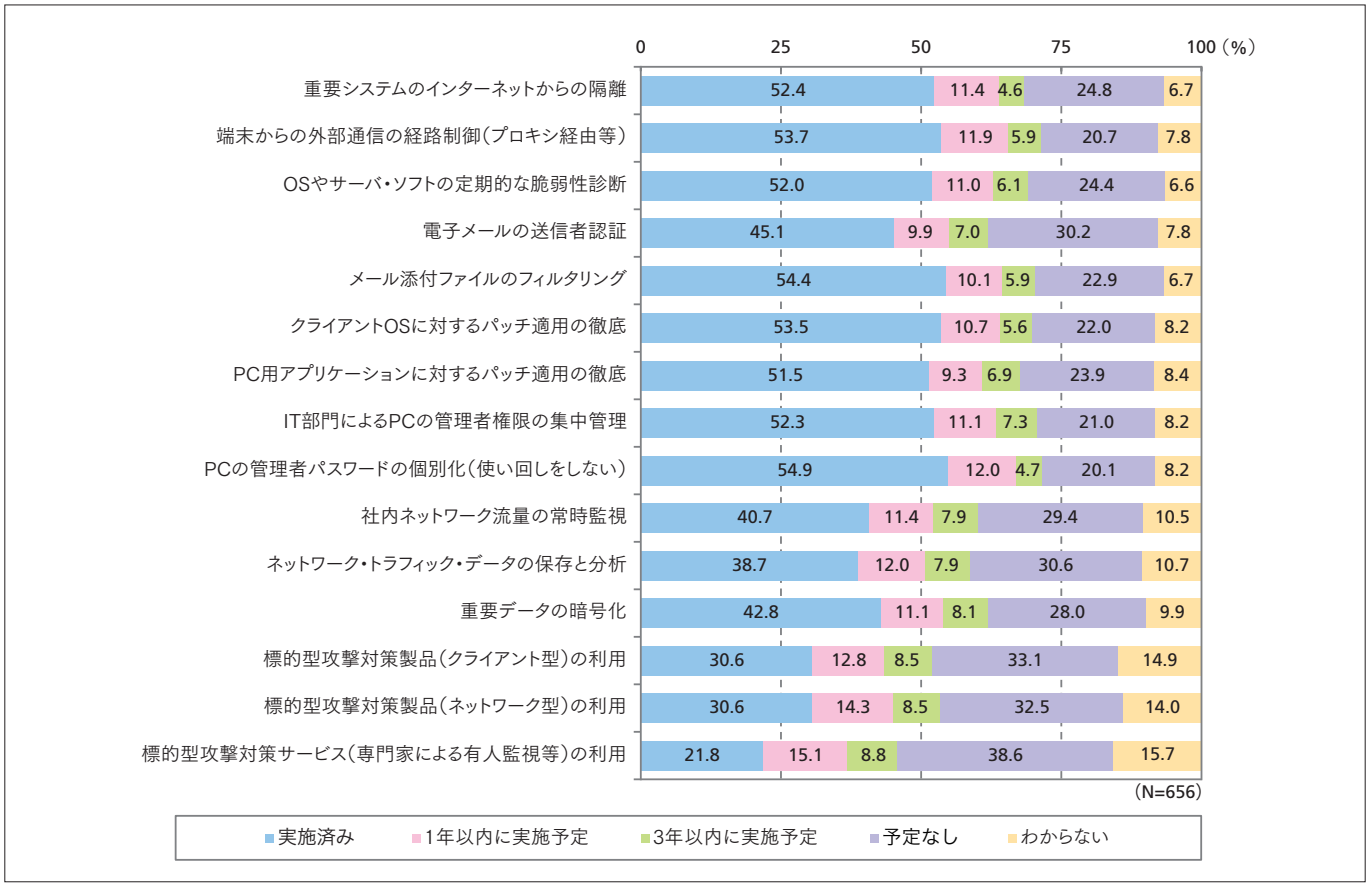

図1-7.「標的型攻撃対策」の実施状況

4 情報セキュリティに関する認証／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証／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問うた。

4-1. 引き続き高い認知率を維持する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つの認証／評価制度を取り上げ、それぞれの取得状況と今後の取得意欲を問うたところ、最も取得率が高かったのは「プライバシーマーク制度」であり、次いで「ISMS適合性評価制度」となった（図1-8）。この上位2つの制度は、回答者の認知度もいずれも7割を超えており、最も定着している認証／評価制度であると評価できる。その他の制度は、いずれも取得率が最大10％台、認知率が最大50～60％台であり、大きな差は見られない。全体的に、認知度と取得率は比例関係にあり、認知度が高い制度ほど取得率も高いことがわかる。こうした評価制度は、多くの企業が認知するものほど取得のインセンティブが働くことになる。認知度向上に向けた取り組みは、制度そのものの有効性を高めるうえでも必須と考えられる。

その一方で、すべての制度について、「取得済みだが、今後の継続はしない予定」とする回答が前年調査に比べ若干増加した。

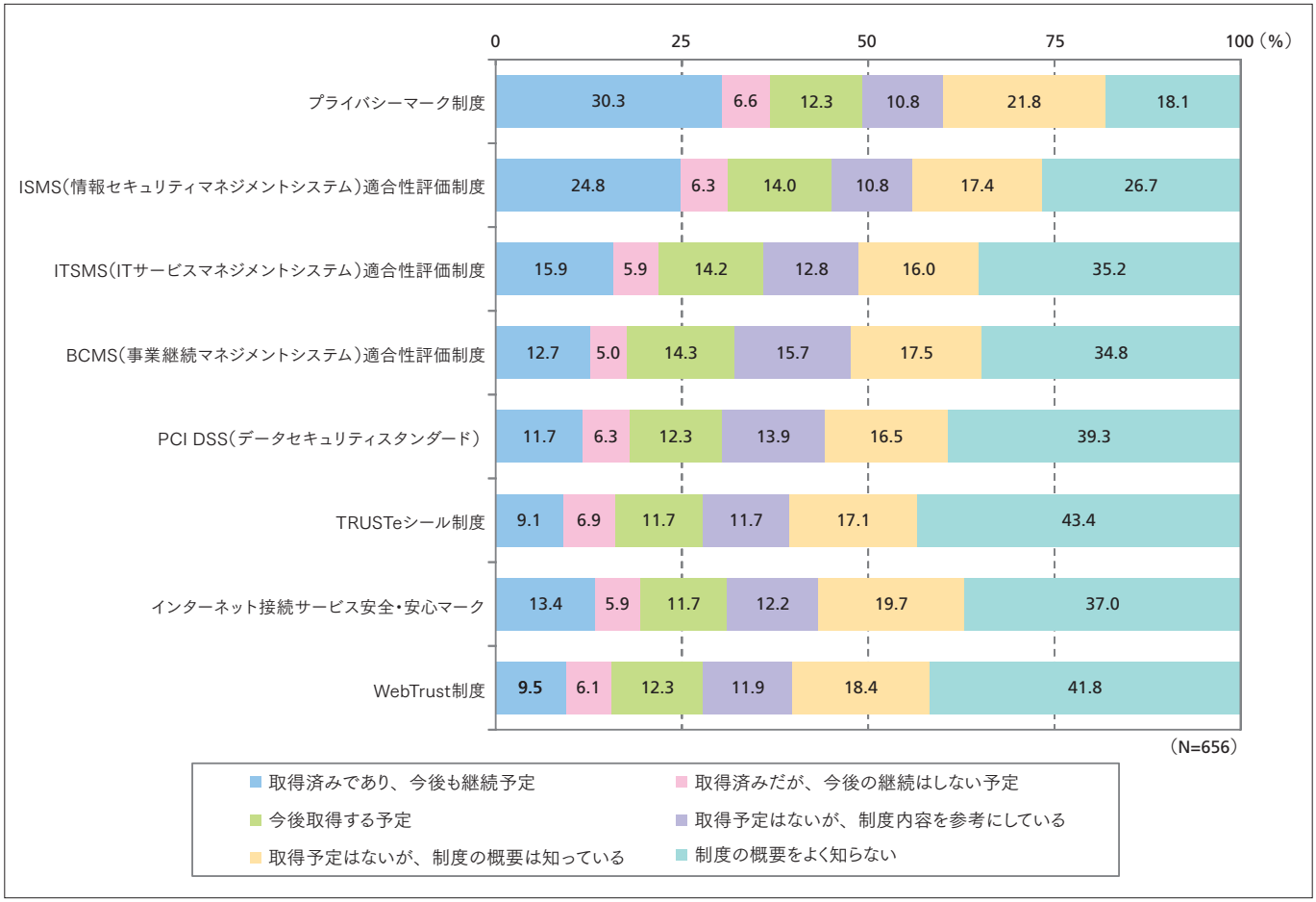

図1-8. 情報セキュリティに関わる認証／評価制度の取り組み状況

4-2.制度取得に積極的な情報通信業

取得率、認知率とも最も高い「プライバシーマーク制度」を取り上げ、その取り組み状況をより詳細に見てみると、業種別では、「情報通信」において圧倒的に取得率が高い（図1-9）。同業界においては、マークの付与を受けることがビジネス取引における主要な要件とされているためであると考えられる。

図1-9.「プライバシーマーク制度」の取り組み状況（業種別／従業員数別）

また、今後に向けて取得意欲の高い業種は「建設」「金融・保険」「サービス」であるが、そのうちの「金融・保険」は、「取得済みだが、今後の継続はしない予定」とした企業の割合も15.4％と他業種よりも高い。

4-3.高まる中堅以下の認証取得意欲

従業員数別では、大企業ほど取得率が高いのは当然であるが、今後に向けては、従業員数300～999人の中堅企業において、取得に向けた意欲が高まっているのが特徴的である。昨今では、サプライチェーン全体でセキュリティレベルを向上させる取り組みが推進されるケースが増加しており、その一環として第三者による認証の取得が取引の条件とされるケースが少なくないことも、取得意欲の高まりの一因であろう。

5 セキュリティ支出と組織的な対策の動向

今回、新たにセキュリティ支出の動向にまつわる調査項目を追加した。本節では、組織的なセキュリティ対策の実施状況とあわせて紹介する。

5-1.支出増が見込まれる「モバイル対策」と「外部攻撃対策」

セキュリティ対策の重要性は、多くの企業で認識されているものの、振り分けられる予算には限りがある。そこで、今回の調査では、どの領域に対して支出を増やそうとしているのか、新たに調査項目を追加した。主要な用途として15項目をピックアップし、それぞれに対して2014年度の支出の増減傾向を問うた結果が、図1-10である。

これを見ると、全体的に支出を増加する項目が目立つが、セキュリティ製品の利用・購入費、とりわけ「モバイル対策」と「外部攻撃対策」に対して、20％以上の企業が支出増を計画しており、特に重視されていることがわかる。前者についてはスマートデバイスの普及、後者については標的型サイバー攻撃に対する懸念の高まりが背景にあることは間違いないであろう。

その他の項目の中では、「災害対策（ディザスタリカバリ対策）」「セキュリティ関連の認証取得に関する費用」について、支出増を見込む企業の割合が高い。

教育・研修もまた、セキュリティ対策においては重視される取り組みであるが、教育関連費用も、一般従業員向け、ITスタッフ向けともに2014年度は支出増を見込む企業が多い。

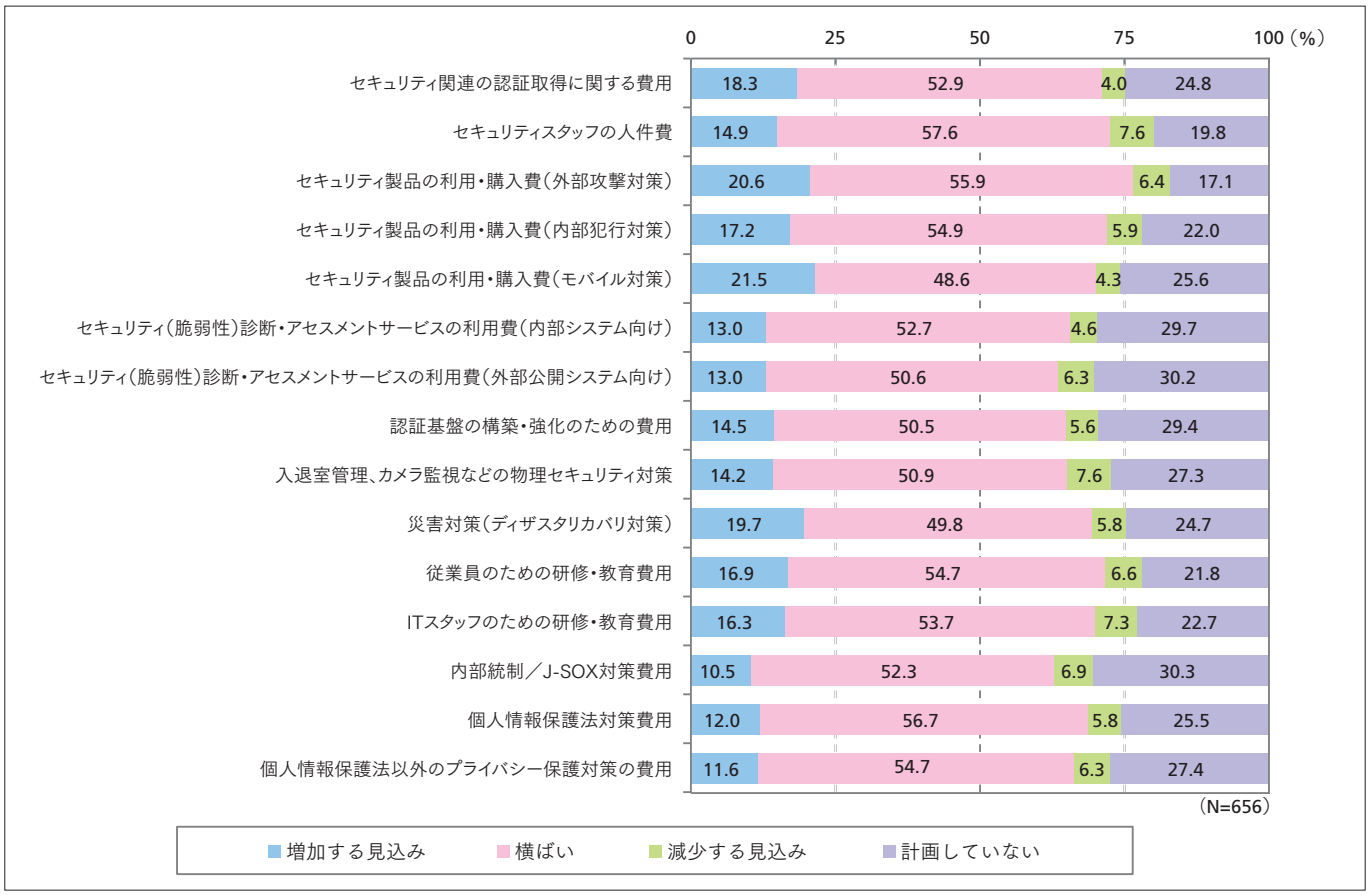

図1-10. セキュリティ支出の増減傾向

5-2.継続して強化が進む組織体制の整備

2013年に実施した前回調査において、大きな改善が見られたのが、組織的なセキュリティ対策の実施率であった。東日本大震災の発生と前後して大規模な個人情報漏えい事件や標的型攻撃による国内企業への被害が次々と明るみに出たことにより、多くの国内企業が真っ先に強化したのが組織体制の整備であったといえる。

今回の調査では、実施率そのものは前年調査から若干低下したものの、すべての項目にわたって実施率が50％前後となり、一定のレベルで取り組みが継続されていることを示す結果となった（図1-11）。

全体的な情報セキュリティ担当責任者（CISO）の任命率は49.4％とほぼ半数に上り、情報セキュリティ担当部署の設置や、情報セキュリティ担当スタッフの配備に取り組む企業の割合も、全体の半数を超えている。

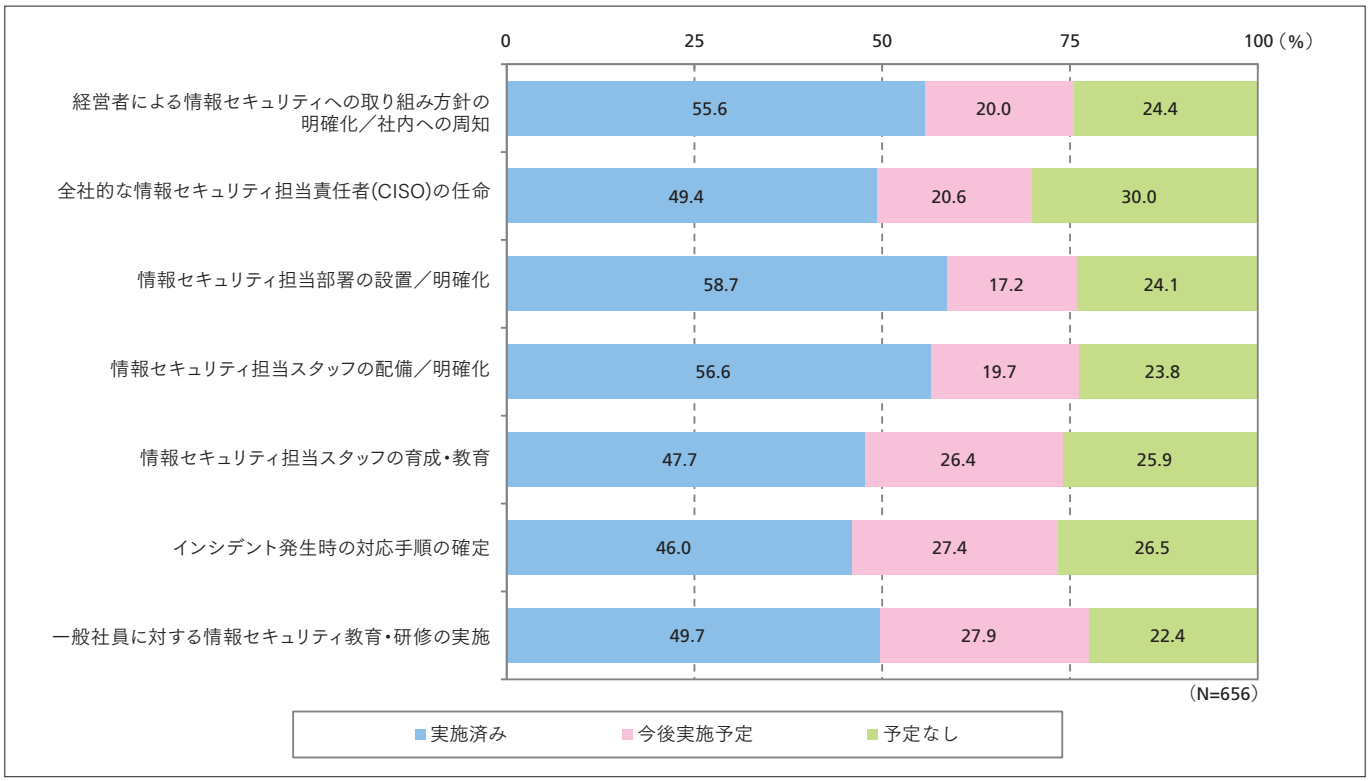

図1-11. 組織に関わるセキュリティ対策の実施状況

6 「重要な情報資産」の取り扱い状況

近年のセキュリティ対策において、より重視されるようになってきているのが、個人情報や機密情報などの情報資産の保護である。今回の調査では、センシティブ情報の保護に関する取り組みなど新たな調査項目を追加し、より多角的に国内企業の情報資産の取り扱い状況の可視化を試みた。

6-1.依然として課題が残る「重要な情報資産の定義・特定」

過去の調査結果において、明確な課題の一つとして浮かび上がったのは、本来最も基本であるはずの「重要な情報資産の定義・特定」ができている企業が思いのほか少ないという事実であった。その傾向は今回の調査にも引き続き表れた。重要な情報資産の取り扱いの現状については、「重要な情報資産」の定義・特定・他の情報資産との分類を行っていると答えた企業の割合は36.4％にとどまり、「アクセスできる人員（部署）の制限」や「管理者の任命」を下回る結果となった（図1-12）。

これは、「守るための仕組み（体制）は構築しているが、守るべき情報が特定されていない」という企業が一定数存在することを示している。

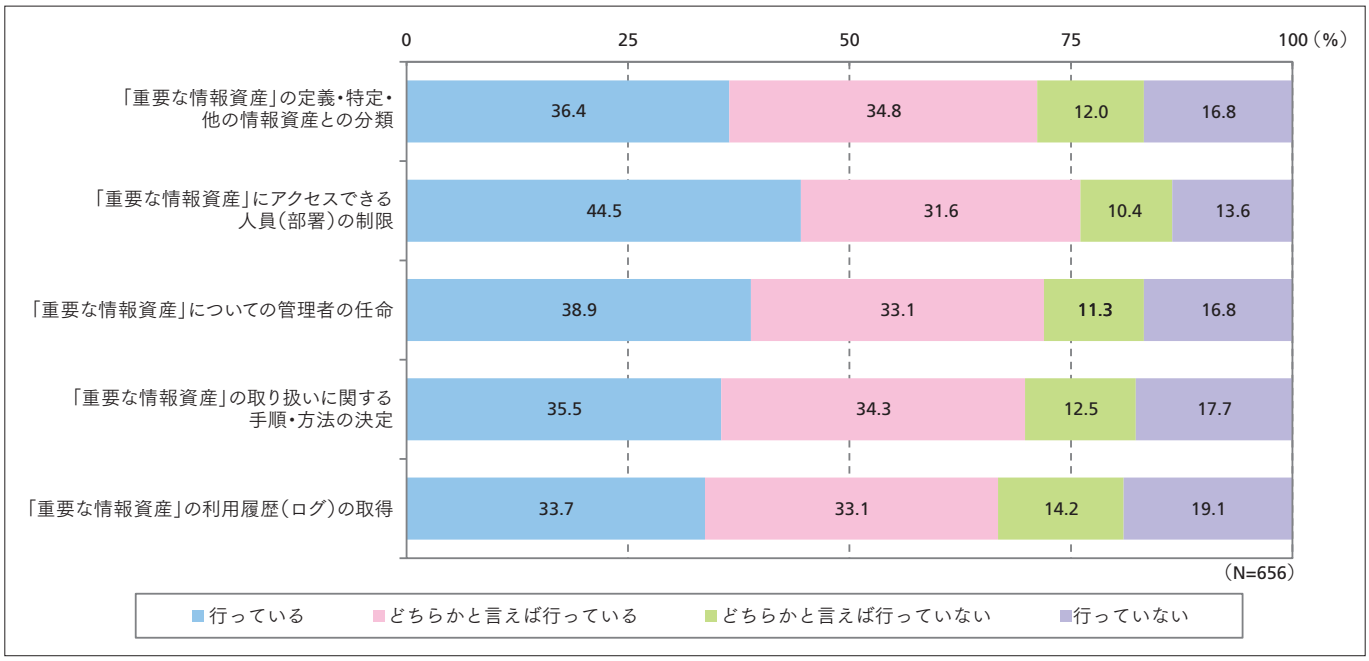

図1-12. 重要な情報資産の取り扱い状況

また、「重要情報」と定義している情報の種類を問うた質問では、「顧客・従業員・採用応募者等の個人情報」については、70％以上の企業が重要情報と定義しているものの、「営業資料／契約書」「技術／研究開発情報」などは対象としていない企業が目立つ。また、サイバー攻撃の被害拡大を防ぐためにきわめて重要となる「社内システムの認証情報」も、あまり重視されていないとの結果が示された（図1-13）。

重要情報を定義することに対する管理者の意識、定義の範囲の明確化は、早急に見直すべき課題だといえる。

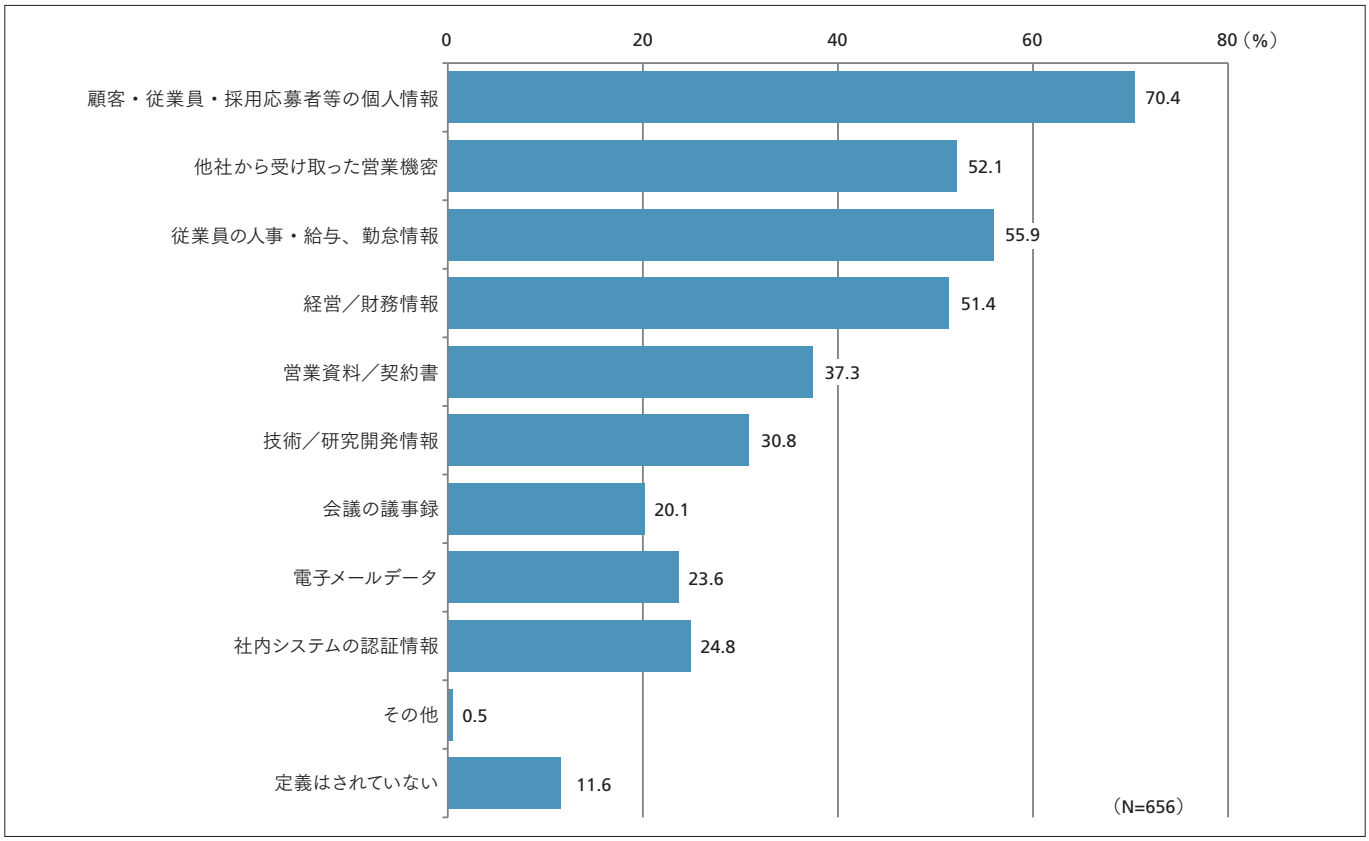

図1-13. 重要と定義している情報の種類

6-2.「センシティブ情報」保護に向けた取り組み

個人情報保護法で定める「個人情報」とは、「生存する個人の情報であって、特定の個人を識別できる情報」とあるように、個人を識別する氏名や生年月日などきわめて限定的である。昨今、ビッグデータの活用といった新しいITトレンドが生まれつつあることを受けて、従来までの個人情報の範疇を越えたセンシティブ情報(思想・信条や政治的立場、医療・性などに関わる情報や、社会的差別の原因となる情報など。機微情報とも呼ばれる。)を保護することの重要性も指摘されるようになってきた。そこで、今回の調査では、こうしたセンシティブ情報の保護に向けた取り組み状況についても調査対象とした。

その結果、「組織として、保護すべきセンシティブ情報の定義ができている」と回答した企業は40%以上に上り、一定の取り組みが進んでいることをうかがわせる結果が示された(図1-14)。ただし、「取得・活用にまつわる方針を外部に公開している」とした企業の割合はわずか14.2%にとどまっており、自社のスタンスを外部に明示するところまでには至っていない企業が多いこともわかる。

業種によっては、顧客や患者の履歴データの活用などが今後ますます進むと予想されるだけに、そうした情報のライフサイクルを企業としていかに管理していくかは、セキュリティ対策の中でも重要な柱となる可能性がある。

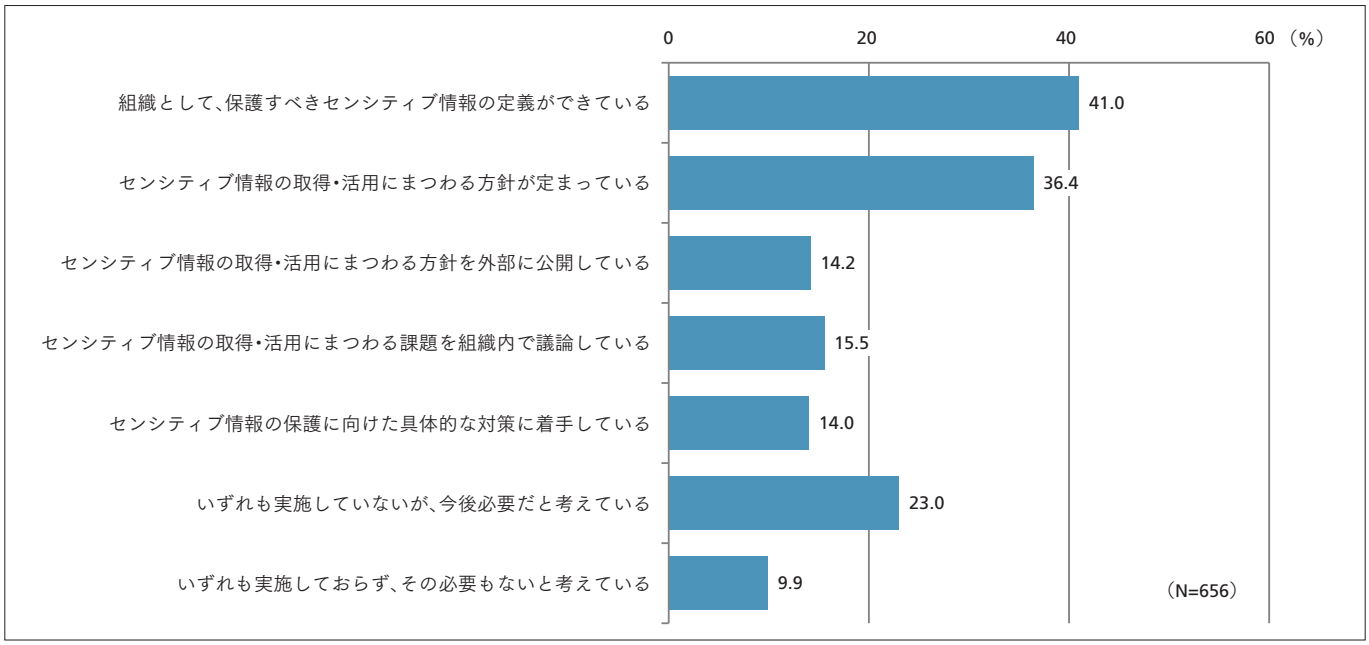

図1-14. センシティブ情報の取得・活用に関する取り組み状況

7 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は複雑化の一途をたどっており、その中で技術が果たす役割は日増しに大きくなっている。本節では、主要なセキュリティ製品の導入状況を分野別に見ることにする。

7-1.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、現在、最も企業の導

入意欲がさかんなカテゴリである。導入率では、「ファイアウォール」が約8割と最も高い導入率となり、「VPN(Virtual Private Network)」が続いている。また、「次世代ファイアウォール」「DLP(情報漏えい防止)」「フォレンジクスツール」など、今後に向けて導入を予定する企業の割合が高い項目が多いのも、この分野の特徴である(図1-15)。

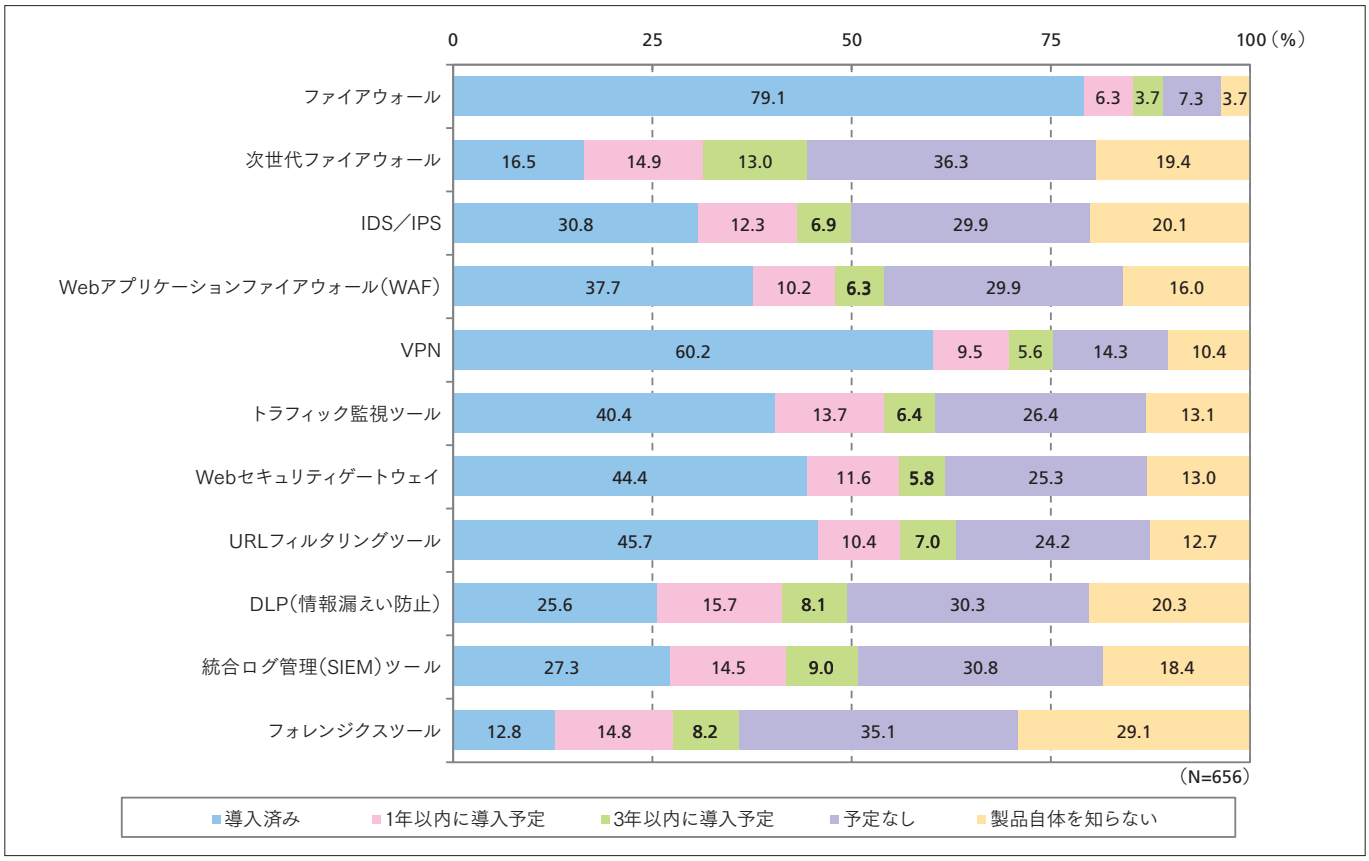

図1-15. セキュリティ製品の導入率(ネットワークセキュリティ)

7-2.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)」の導入率が際立って高いが、「パッチ管理ツール」「PC資産管理ツール」「PC操作ログ管理ツール」といった集中管理型の製品の導入も比較的進んでいる。また、今後に向けては、「シンクライアントシステム」の導入意欲が前年調査(20.5%)に引き続き高く(25.1%)、端末にデータを保存させずにサーバ上で運用できることの価値がセキュリティの観点から重視されていることがうかがえる(図1-16)。

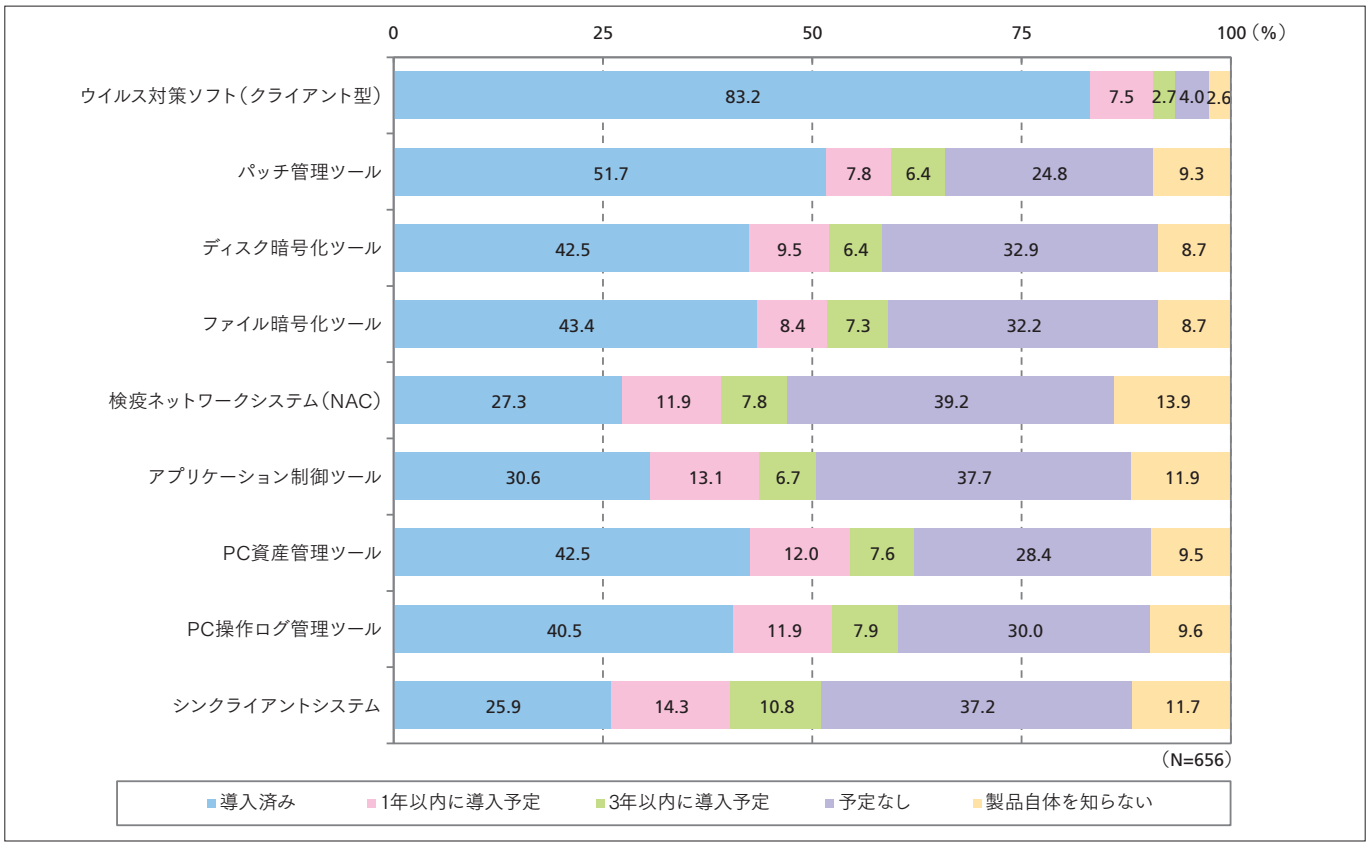

図1-16. セキュリティ製品の導入率（クライアントセキュリティ）

7-3.メールセキュリティ製品の導入状況

外部からのサイバー攻撃の初期侵入に利用されることの多いメールのセキュリティ対策としては、「スパム対策ツール」の導入率が最も高く、それに続いて暗号化や誤送信防止ツールが続く。今後に向けて「メール監査ツール」や「添付ファイルの暗号化ツール」の導入意欲が高いことから、内から外へ向かう送信メール対策を強化しようとする企業が多いことがうかがえる（図1-17）。

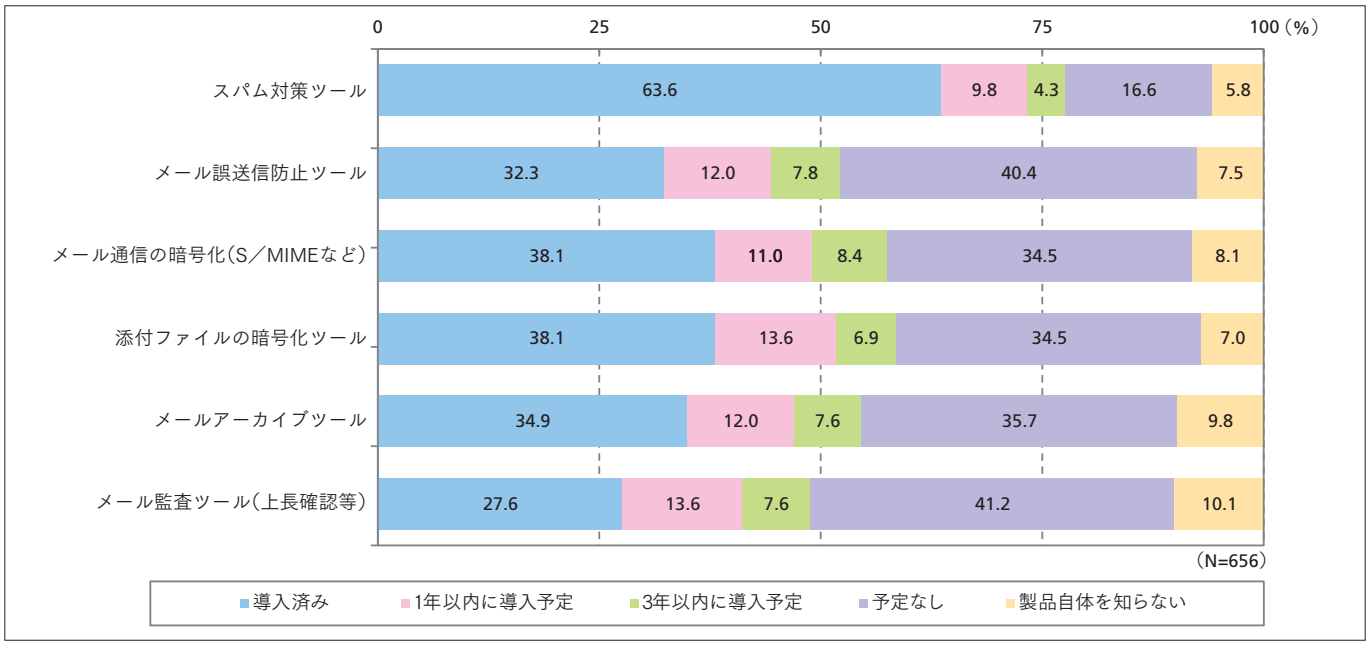

図1-17. セキュリティ製品の導入率（メールセキュリティ）

7-4.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は、過去の調査結果と同様、他分野と比較して導入率が低い分野である(図1-18)。スマートデバイスの普及に伴うモバイル業務の浸透、在宅勤務の普及など、今後、ワークスタイルの多様化が想定されるだけに、認証基盤の堅牢性は企業のセキュリティレベルに直結すると考えられる。外部攻撃に備える意味でも、セキュリティ(製品)業界を挙げてその重要性を訴求していくことが望まれる。

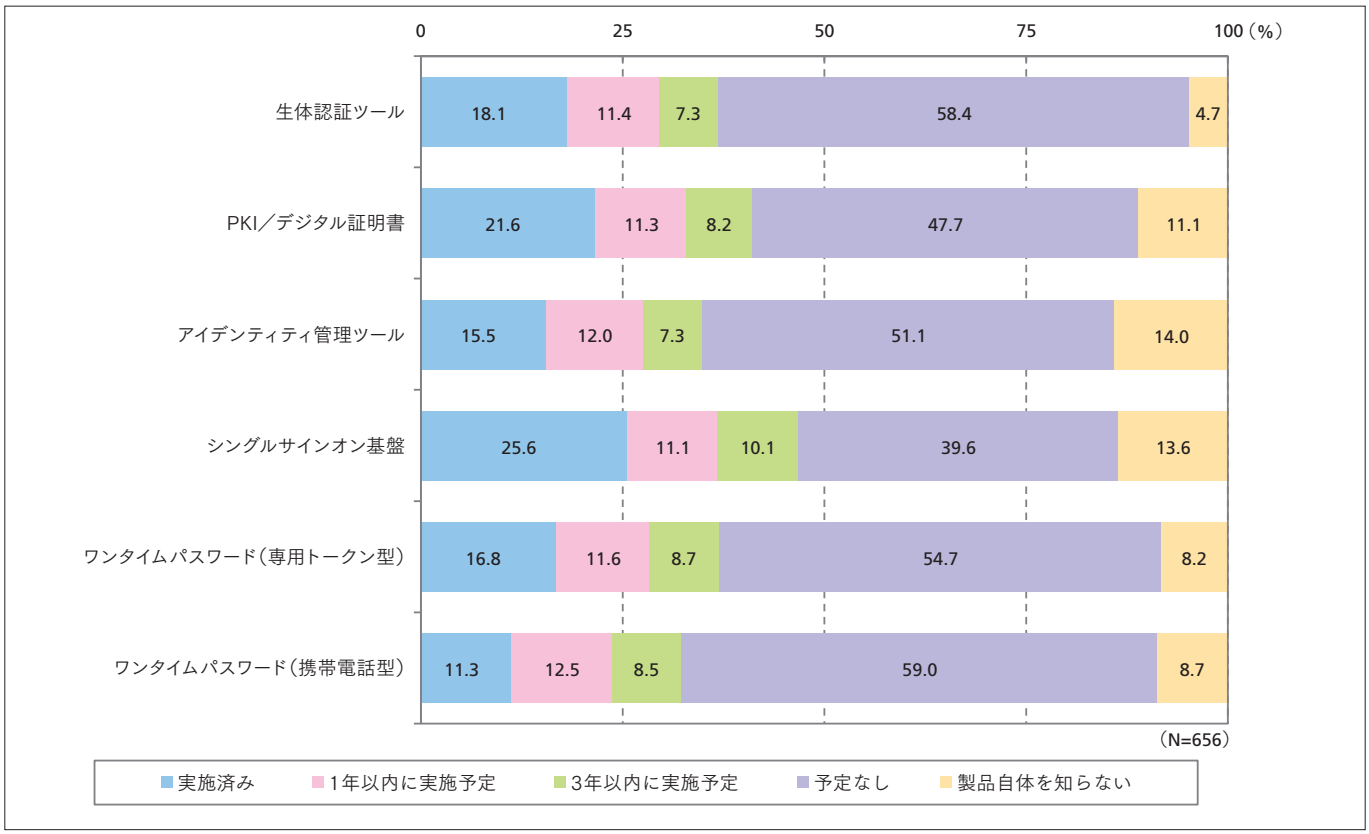

図1-18. セキュリティ製品の導入率(アクセス管理)

7-5.セキュリティサービスの利用状況

今回の調査では、新たにセキュリティサービスの利用状況についても調査対象に加えた。脆弱性診断、SSL証明書、アウトソーシングを対象としたが、多くの項目が30%前後で横並びの利用率となった(図1-19)。

2013年度にWebサイトに対する不正アクセスや不正改ざんなどの被害が頻発したことから、脆弱性診断サービスやSSL証明書サービスといった、外部Webサーバ向けのサービスに対する注目度が高まると予想していたが、今回の結果を見る限り、現在の利用率、今後の利用予定ともに、社内サーバとほぼ同程度の水準にとどまった。

外部Webサーバの保護は、自社の顧客を被害から守るという意味でも重要な対策となるだけに、業界としても、こうしたセキュリティサービスの認知度をより高めていくためのさらなる取り組みが不可欠となる。

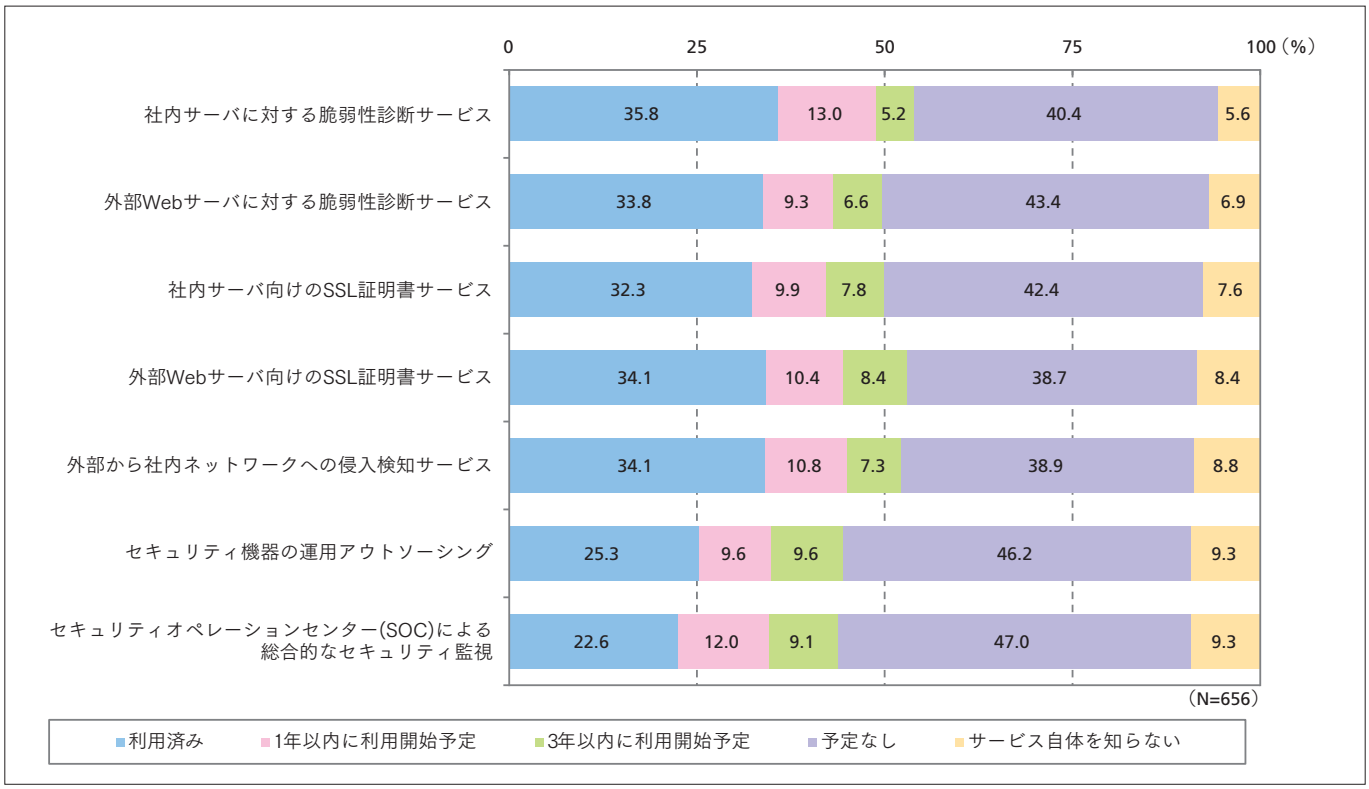

図1-19. セキュリティ製品の導入率（セキュリティサービス）

8 モバイルデバイスの活用状況

スマートフォン、タブレットの普及拡大を受けて、企業ITの中でもメインプレイヤの一角を占めるようになったモバイルデバイス。今回の調査では従来よりも範囲を拡大し、その導入状況から導入目的、実運用におけるポリシーの動向についても対象とした。本節では、その動向をまとめて紹介する。

8-1.スマートデバイスの導入状況

まずは、国内企業におけるスマートデバイスの導入状況を概観する。スマートフォン、タブレットそれぞれについて、会社支給と私物利用許可の両方の取り組み状況を見ると、会社支給については、「試験的に実施」までを含めれば、いずれも50％を超えており、導入が着実に進んでいることが確認できる（図1-20）。注目すべき点は、タブレットの全社利用（50％以上）がスマートフォンとほぼ同水準にまで進展していること、今後の伸びしろは、タブレットのほうがむしろ高いことである。

また、この結果を見る限り、導入は会社支給が主流であり、私物端末の業務利用（すなわちBYOD）の進展は比較的緩やかであることが見てとれる。

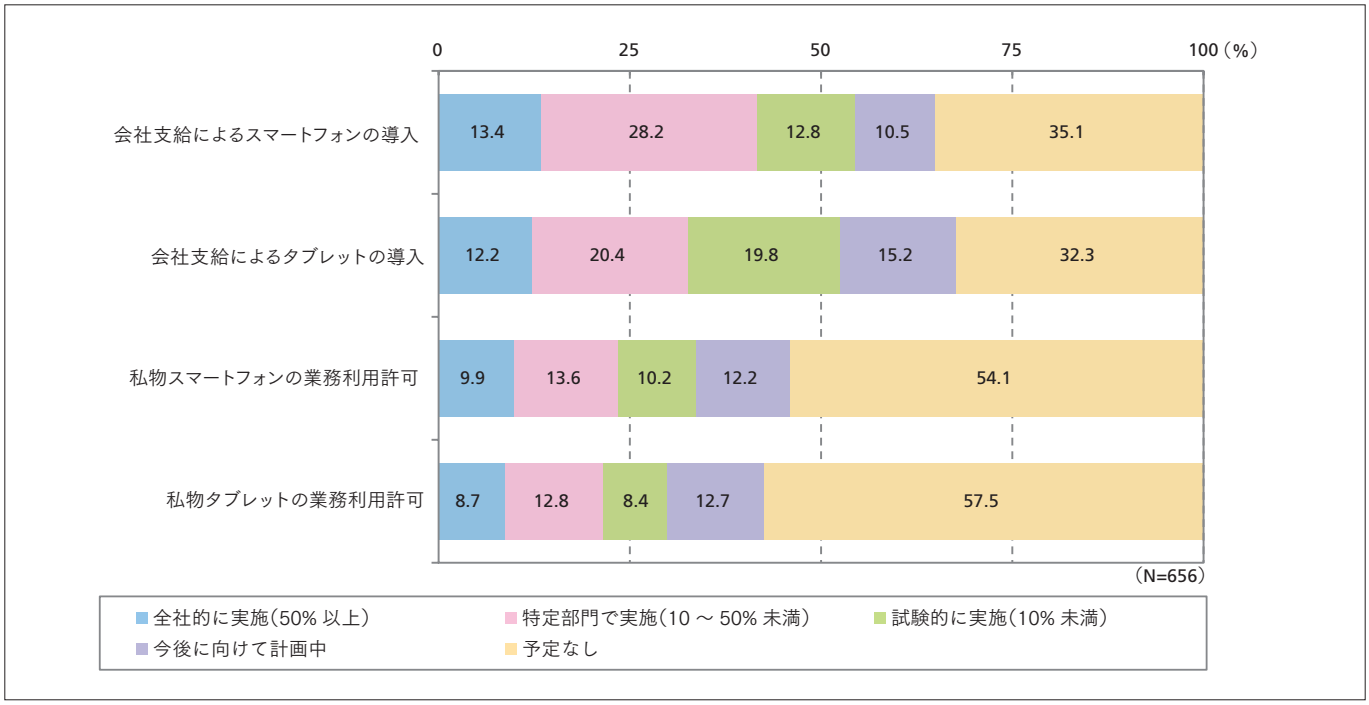

図1-20. スマートデバイスの導入・活用状況

8-2.増加する会社支給と私物の「併用型」

ただし、図1-20の結果をクロス集計すると、ユニークな傾向が見えてくる。それは、BYODを許可している企業の大半は、会社支給も同時に行っている「併用型」であるということである。図1-21にスマートフォン、タブレットそれぞれの運用形態を示したが、スマートフォンを例に取れば、私物端末の業務利用を10％以上認めているとした企業（23.5％）のうち、4分の3（18.0％）は併用型であり、タブレットもほぼ同じ傾向である。

企業の間では「会社支給か、私物か」といった議論は収束しつつあり、両者の共存が当たり前になりつつあることがうかがえる。

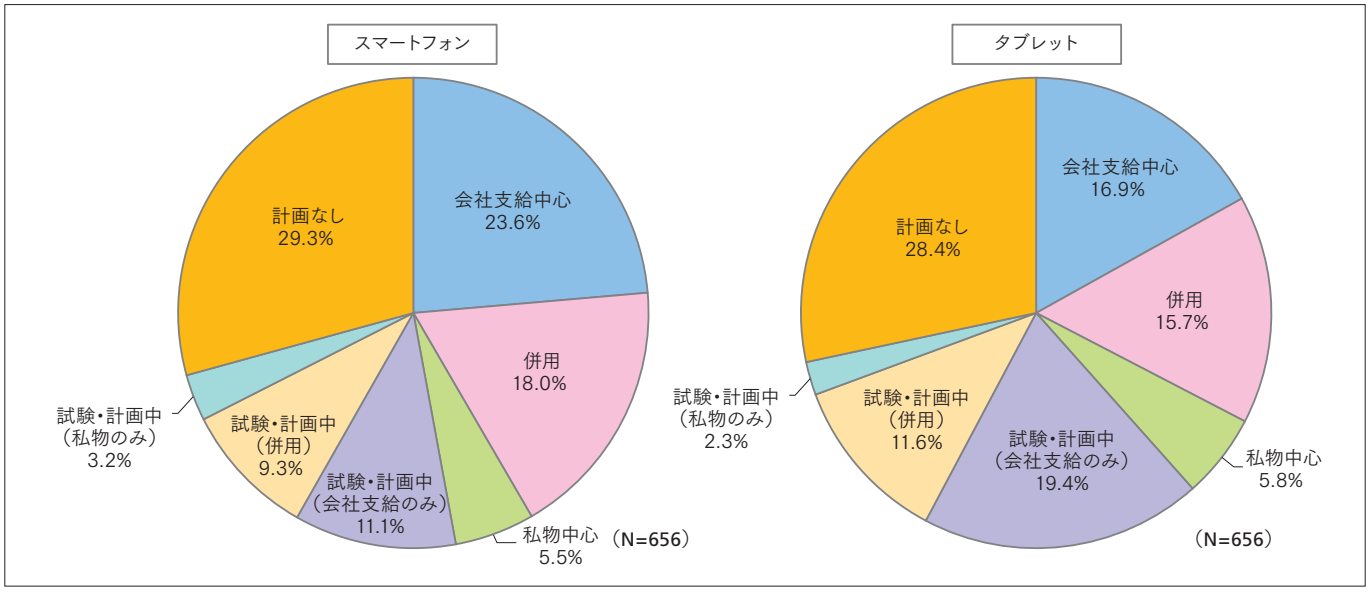

図1-21. スマートデバイスの運用形態

8-3.スマートデバイスの用途

スマートデバイスの導入目的を見ても、その用途が多岐にわたっていることが確認された(図1-22)。現時点で多く導入されているのは「外勤営業スタッフの業務支援」と「役員・管理職の業務支援」の2つであるが、今後に向けて、他の項目についても用途は拡大すると見込まれる。特に、「在宅勤務者の業務支援」は、今後検討している企業の割合が最も高く(24.4%)、柔軟なワークスタイルを実現するためのツールとして、スマートデバイスがきわめて重視されていることをうかがわせる結果となった。

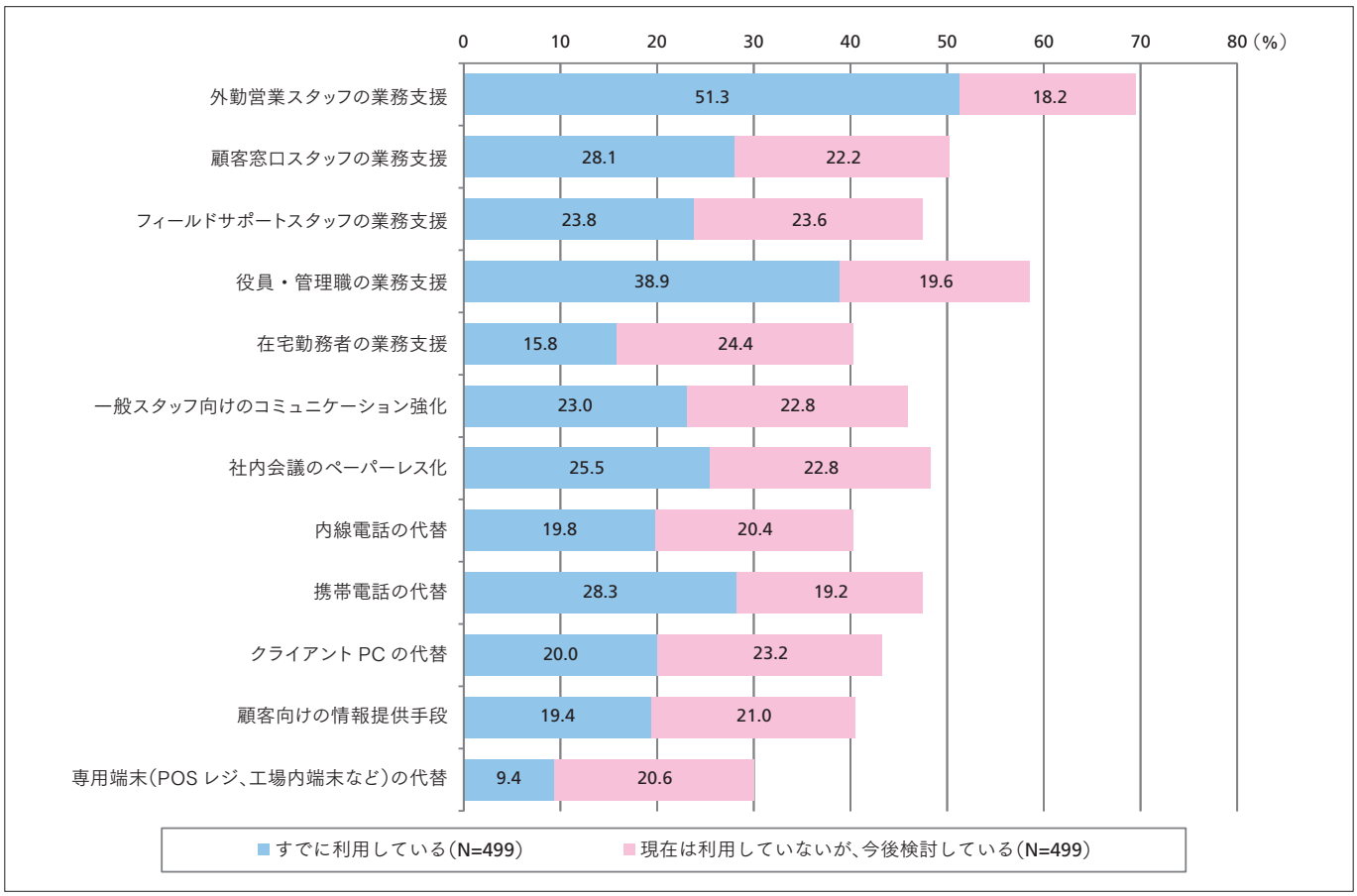

図1-22. スマートデバイスの導入目的(現在／今後)

また、導入目的のデータで興味深いのは、幅広い用途に活用している企業は、「会社支給中心」ではなく、むしろ「併用型」で運用している企業であるということである。図1-22の結果のうち、「すでに利用している」とした項目の割合を、スマートフォンの運用形態別(会社支給中心／併用型／私物中心)に集計すると、併用型の企業が最も多目的にデバイスを活用していることが示された(図1-23)。とりわけ「在宅勤務者の業務支援」が「併用型」の企業では35%利用されているのに対して、「会社支給中心」や「私物中心」の企業では、10%強にとどまっている。

一方、同じBYODの採用企業でも、会社支給を行わず「私物中心」で運用している企業は、用途の幅が最も狭い。そうした企業では、メールチェックやスケジュールの確認など、きわめて限定された用途でスマートデバイスが活用されていると推察される。

BYODを採用する企業において、活用の意欲や実態に明確な差が見られたのも、今回の調査の一つの特徴である。

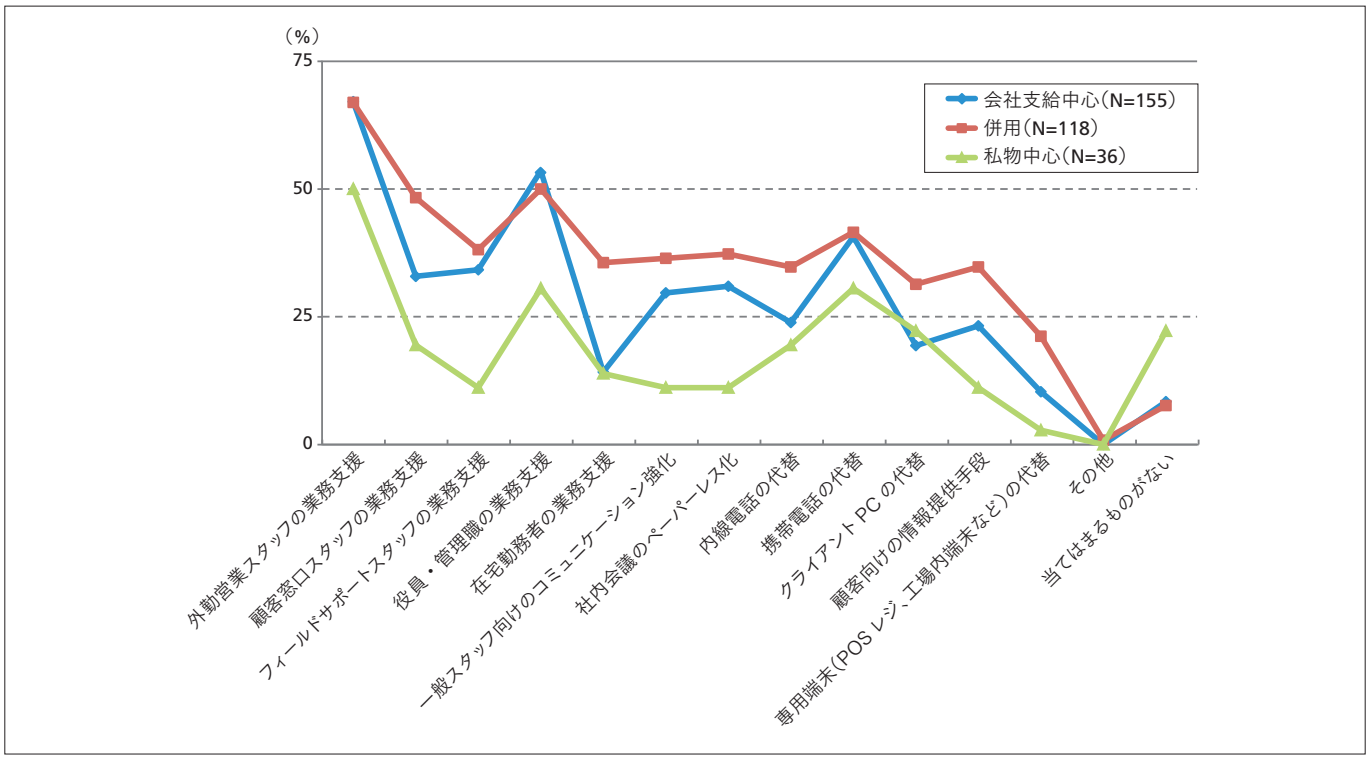

図1-23. スマートフォンの運用形態別に見る現在の導入目的

8-4.ユーザ本位に向かいつつある運用ポリシー

スマートデバイスの導入に取り組む企業が、技術的な課題とは別に頭を悩ませるのが、端末内へのデータ保存を認めるか、社内のイントラネットへのアクセスを許可すべきか、といった運用ポリシーである。今回は、そうした運用ポリシーのバランスをどこに見いだしているか、今後どのような方針をとろうとしているか、スマートデバイス導入企業を対象に回答を求めた。

その結果、多くの項目について、現在よりも今後のほうが、ルールを緩和しようとする傾向が示された(図1-24)。こうした運用ポリシーは厳しく設定すればリスクは抑えられるが、その一方でユーザビリティを犠牲にすることも多く、活用の阻害要因となる。今回の結果からは、国内企業が今後に向けてより「活用」を強く意識していることがうかがえる。

なお、スマートデバイス向けセキュリティツールの導入率は、今後に向けて伸びが見込めるものの、現時点での導入率は決して高くない(図1-25)。今後、運用ポリシーを緩める傾向が本格化するならば、技術的に端末やデータを保護するツールの重要性は大いに増すことになるだろう。

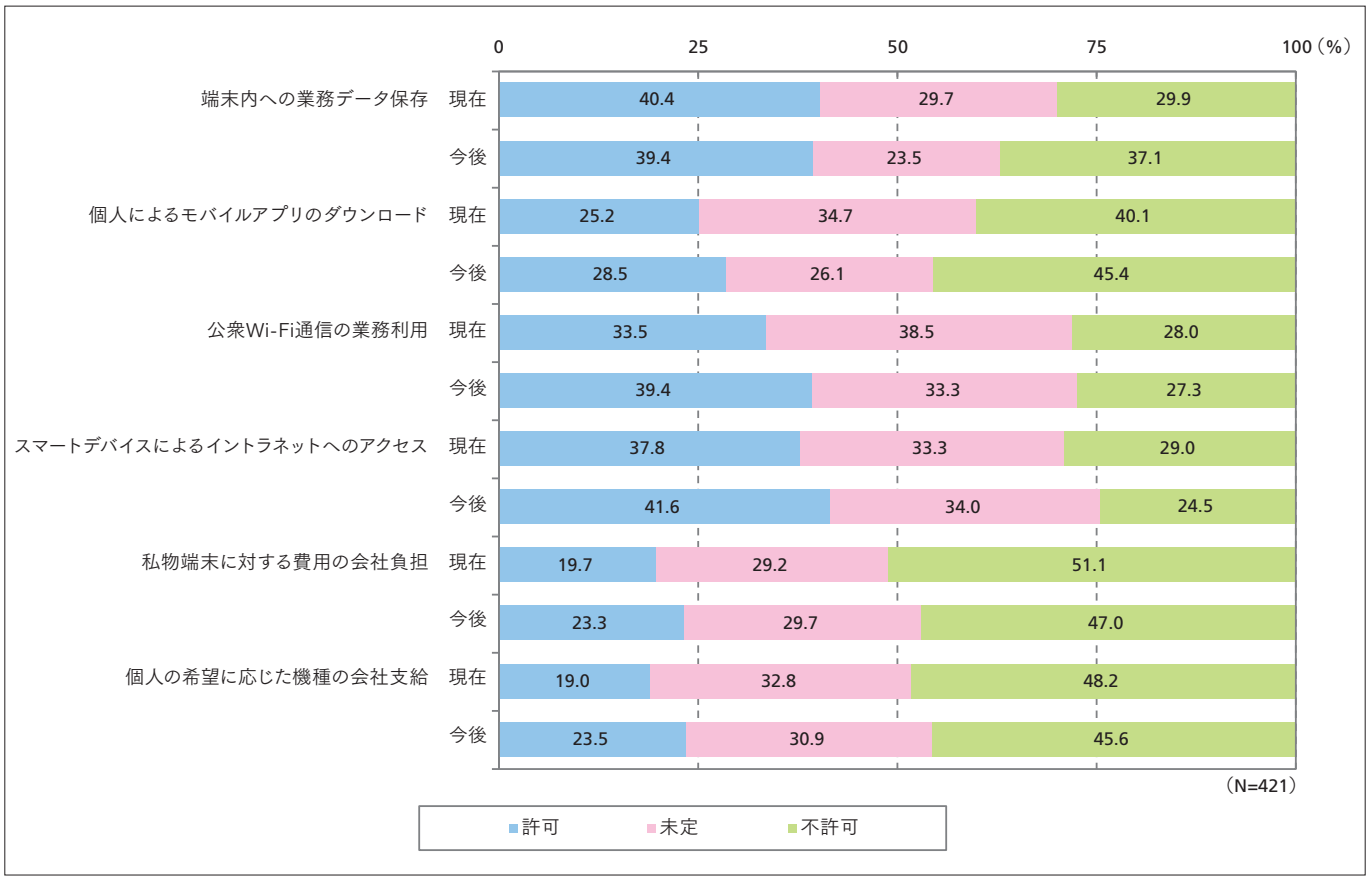

図1-24. スマートデバイスの運用ポリシー（現在／今後）

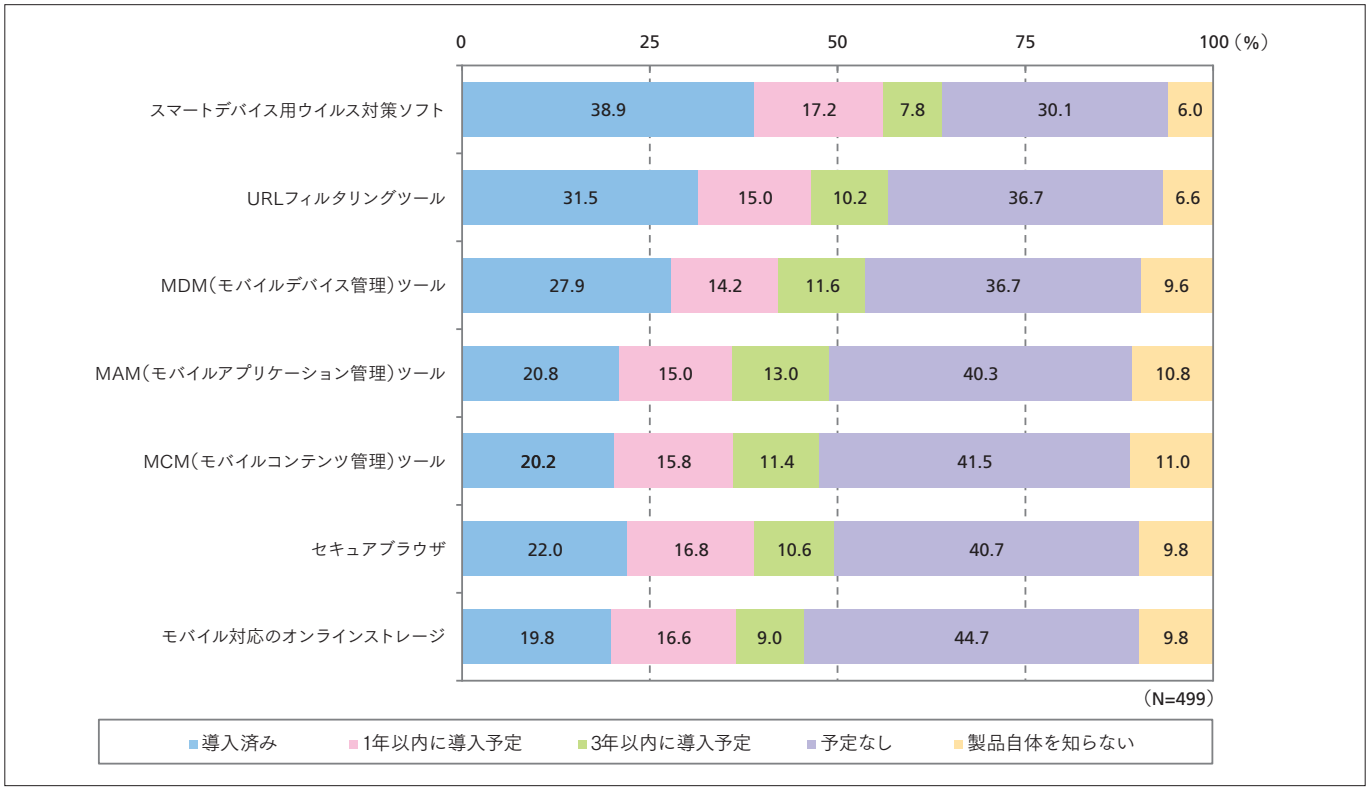

図1-25. スマートデバイス向けセキュリティツールの導入率

9 総評

本調査は、IT活用と情報セキュリティ対策に関する包括的な動向を探ることを目的に実施しており、今回が3回目となる。リーマンショック、東日本大震災といった緊急対応が必要な“歴史的な事件”を経て、国内の経済環境が回復局面にあるなかでの実査となったが、そうした事情を反映してか、「攻めのIT活用」を目指す思いと、サイバー攻撃に代表される「セキュリティリスク」を懸念する思いとの狭間で、情報セキュリティ責任者が難しい局面に立たされていることがうかがえる結果となった。

たとえば、経営課題を取ってみても、コミュニケーションや組織改革、営業力向上といった攻めのテーマに対する重要度が増しており、売上げの増大や生産性の向上が強く求められていることが確認された。技術面でも、スマートデバイス、クラウド、ビッグデータといった、従来までのIT基盤のあり方を大きく変容させるテーマが浮上している。そうしたなかで、セキュリティ対策は、重要度こそ高いものの、具体的な対策についてはやや停滞したといえる。組織体制の整備やツールの導入率、重要情報の取り扱い状況などを見ても、前年の調査から実施状況が同水準かむしろ後退した項目が目立った。サンプルの違いがあるため単純に比較はできないが、セキュリティ面について、前年から大きく進展した取り組みを把握することができなかった。

セキュリティ関連の支出は2014年度に向けて増加傾向にあり、個々の製品・サービスの導入・利用を検討する企業の割合も、総じて前年よりも高かった。増加分の予算をどこに振り向けるかは、セキュリティ責任者の腕の見せ所となろう。

新しいテクノロジが続々と企業ITに入り込む今日において、「活用」と「リスク対策」のバランスをどこに見いだすかは、すべての企業にとって大きな課題である。それを象徴するテーマの一つが「モバイル」である。この分野では、ルールを極力緩和し、活用を推進しつつツールの活用によってリスクを抑えようとする“積極派”と、活用シーンを限定して利用させる“消極派”が明確に分かれつつあることが確認された。こうした動きは、今後モバイルだけでなく、さまざまな分野に及ぶと考えられる。攻めと守りのバランスをいかに“拡大均衡”へと持っていくか。これが、セキュリティ責任者に与えられた重要なミッションである。

回答者プロフィール

業種	回答数	%
製造	166	25.3
建設	32	4.9
卸売・小売	80	12.2
情報通信	103	15.7
金融・保険	52	7.9
サービス	171	26.1
公務・その他	52	7.9
全体	656	100.0

年間売上高	回答数	%
1,000 万円未満	1	0.2
1,000 万～ 1 億円未満	5	0.8
1 億～ 10 億円未満	63	9.6
10 億～ 100 億円未満	212	32.3
100 億～ 500 億円未満	140	21.3
500 億～ 1,000 億円未満	58	8.8
1,000 億～ 3,000 億円未満	48	7.3
3,000 億～ 5,000 億円未満	28	4.3
5,000 億円以上	72	11.0
売上げなし	29	4.4
全体	656	100.0

従業員規模	回答数	%
中小企業	250	38.1
中堅企業	159	24.2
大企業	247	37.7
全体	656	100.0

従業員規模	回答数	%
50～99 人	77	11.7
100～299 人	170	25.9
300～499 人	71	10.8
500～999 人	88	13.4
1,000～2,999 人	90	13.7
3,000～4,999 人	46	7.0
5,000～9,999 人	41	6.3
10,000 人以上	73	11.1
全体	656	100.0

業種	回答数	%
食料 : 飲料品	12	1.8
繊維工業	3	0.5
パルプ・紙・印刷	3	0.5
化学工業	11	1.7
石油製品	2	0.3
鉄鋼・金属	14	2.1
機械 / 電気機器	50	7.6
情報通信機器	8	1.2
電子部品・電子回路	11	1.7
精密機器	11	1.7
輸送機器	21	3.2
医薬	2	0.3
その他の製造業	18	2.7
建設	32	4.9
卸売	24	3.7
小売	25	3.8
商社	31	4.7
通信	12	1.8
(情報システム子会社以外の) 情報処理サービス	56	8.5
メディア・出版・放送・広告代理店	3	0.5
情報システム子会社(外販率50%以上)	17	2.6
情報システム子会社(外販率50%未満)	15	2.3
銀行	27	4.1
証券	9	1.4
保険	8	1.2
その他金融（リースなど）	8	1.2
電力・ガス	9	1.4
運輸・倉庫	27	4.1
不動産	10	1.5
教育	6	0.9
医療・福祉	45	6.9
宿泊・飲食	12	1.8
娯楽・広告	7	1.1
その他のサービス	55	8.4
官公庁	6	0.9
地方自治・公共団体	27	4.1
その他の公務	12	1.8
農林・水産・鉱業	1	0.2
その他の業種	6	0.9
全体	656	100.0