【特集】「企業IT利活用動向調査2015」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。

本調査は2011年より継続して行っているが、本誌では、主に2013年からの調査結果を比較・分析して紹介する。

1 調査概要

1-1. 調査概要

・実査期間：2015年1月26日～1月30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、情報システム、経営企画、総務・人事、業務改革系部門に所属する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2,000人

有効回答数：698件（1社1人）

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（24.6%）、次いでサービス業（24.1%）、情報通信（14.9%）、卸売・小売業（12.3%）となった。所属部門では情報システム部門が52.9%と最も多く、役職は部長（34.2%）、課長（30.4%）、係長・主任（19.2%）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」（60.7%）、「全社的なリスク管理／セキュリティ管理に責任を持っている」（57.7%）が半数以上を占めた。本調査については、2013年調査から比較分析を行っているが、2013年に56.9%だった「セキュリティ対策の実務に関与している」が2014年調査では37.5%と20ポイント弱減少したが、今回調査では若干増加し、43.6%となった。また、「全社的なIT戦略に決定権を持っている」が2013年26.5%、前回44.8%、今回43.4%となっており、前回、今回とも、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が調査結果に影響していると思われる。

2 経営における情報セキュリティの位置づけ

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。まずは、経営課題の中での情報セキュリティの位置づけと、リスクの重視度合いを中心に調査結果を見ていくことにする。

2-1. 重視する経営課題

全26項目の経営課題を取り上げ、IT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複数回答であげてもらった（図1-1）。その結果、「業務プロセスの効率化」が過去3回の調査に続いて首位となった。業務プロセス改革に対する課題認識は、ここ数年、あらゆる調査で共通して上位項目となっているため納得の結果であるが、今回はそれに次いで「情報セキュリティの強化」が2位となった。

業種別にみると、「業務プロセスの効率化」は、「公務・その他」を除く各業種で、5割以上となっているが、「情報セキュリティの強化」については、特に「公務・その他」（49.3%）「金融・保険」（48.2%）で高くなっている。

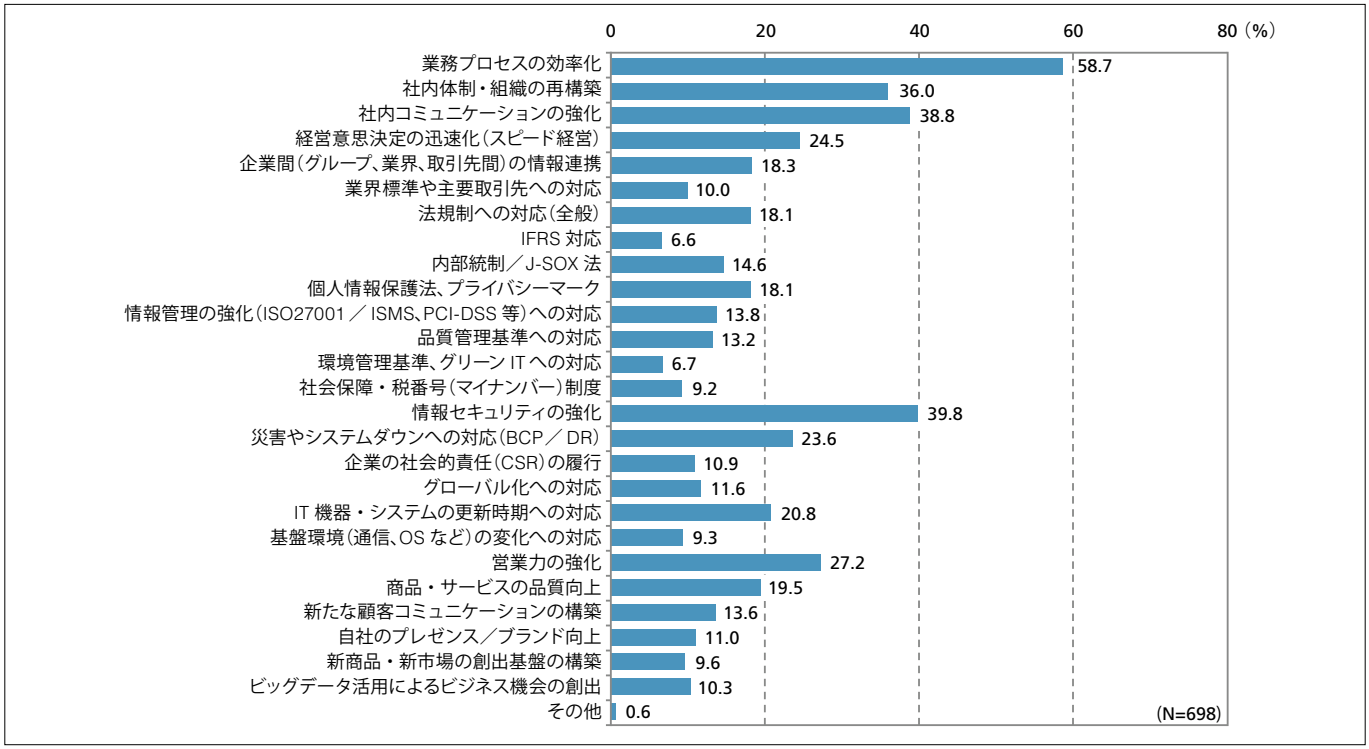


図1-1. 今後重視したい経営課題（複数回答）

上位8項目について、2013年、2014年の調査結果との経年変化を見てみると、「業務プロセスの効率化」は一貫して首位であるが、「情報セキュリティの強化」の選択率が今回調査で大きく上昇している。その一方で、3位の「社内コミュニケーションの強化」、4位の「社内体制・組織の再構築」の選択率は、2014年から若干低下した。守りを固めたいとする国内企業の意識が表れていると見られる（図1-2）。

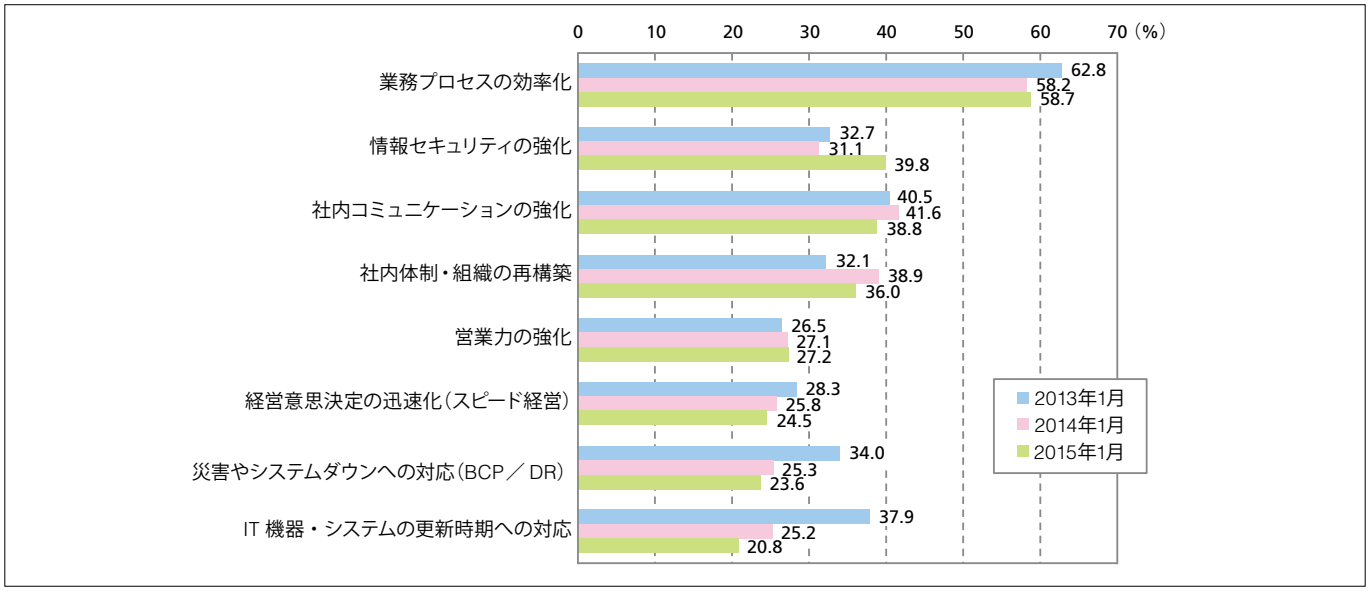


図1-2. 主要経営課題に対する選択率の経年変化（2013年～2015年）

2-2.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経験したセキュリティインシデントを見ると、認知率が最も高かったのは、「社内PCのマルウェア感染」と「従業員によるデータ、情報機器の紛失・盗難」であり、ともに24.2%の同率となった。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19.3%と続いており、スマートデバイスの普及拡大がインシデントの認知に影響を及ぼしていることが明確となった(図1-3)。

また、「個人情報の漏えい・逸失」は、今回調査から「人為ミス」によるものと「内部不正」によるものとを分けて認知状況を問うているが、前者が12.6%、後者が5.2%であった。2014年は、大手教育サービス会社においてシステム管理者の不正による個人情報の漏えい事件が発生して社会問題となったが、今回の結果からは、内部不正による被害が決して対岸の火事とは言えない状況であることがうかがえる。

業種別に見ると、「個人情報の漏えい・逸失(人為ミスによる)」が他の業種と比べ際立って多いのが「公務・その他」「金融・保険」となった(図1-4)。

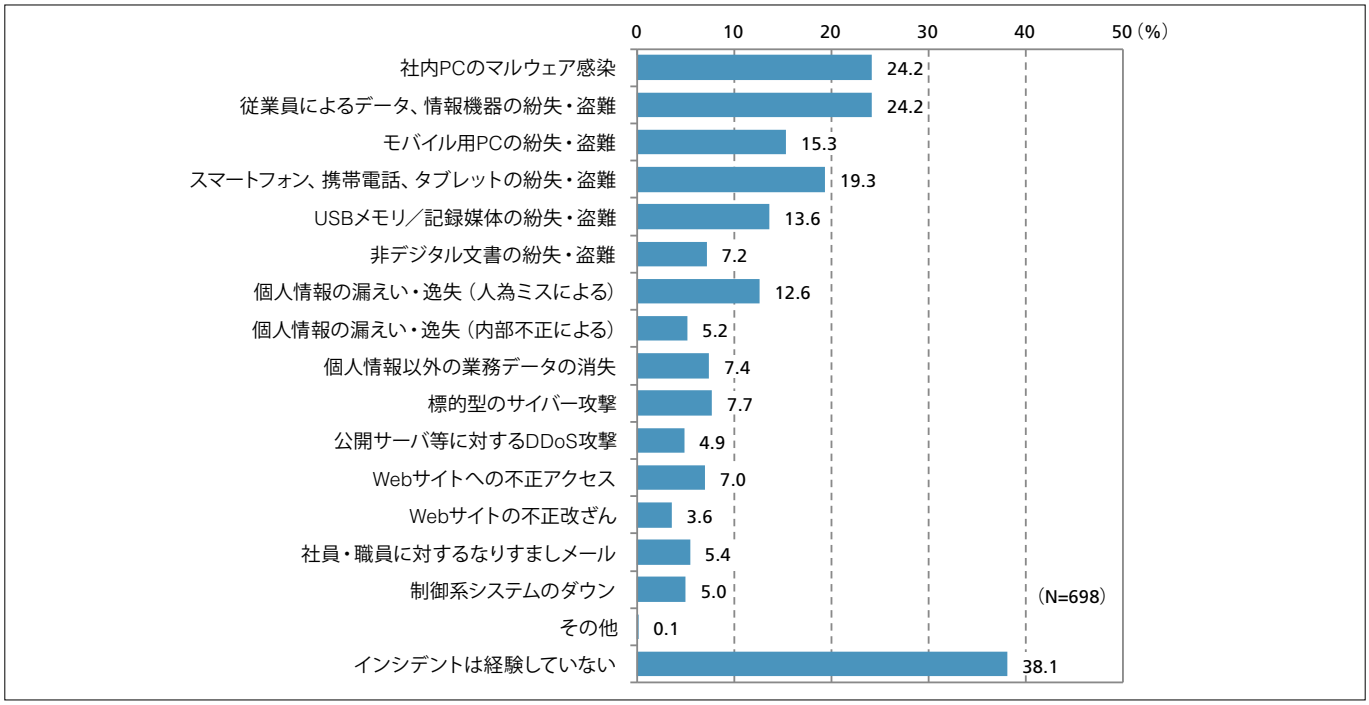
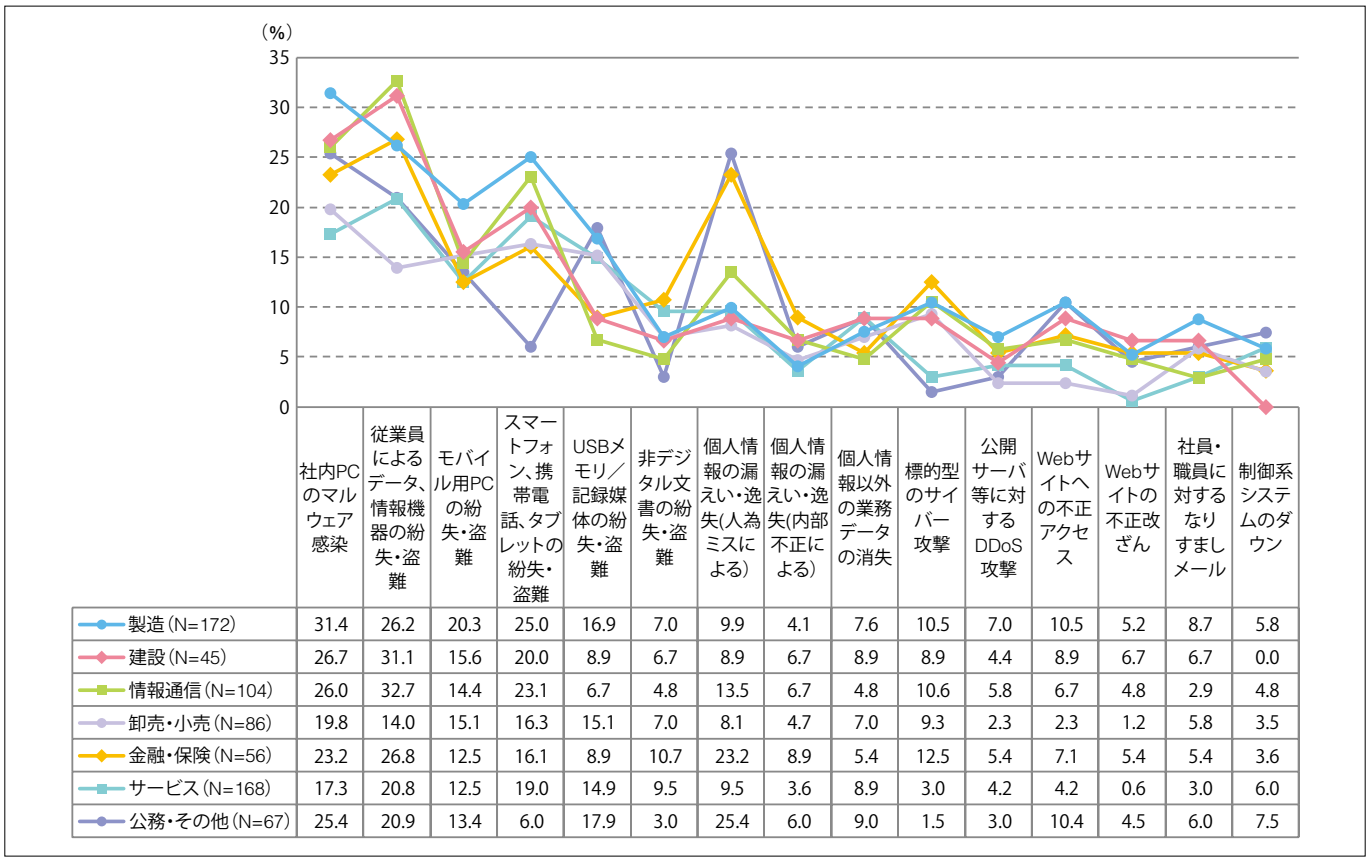


図1-3. 過去1年間に経験したセキュリティインシデント(複数回答)



	社内PCのマルウェア感染	従業員によるデータ、情報機器の紛失・盗難	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	USBメモリ／記録媒体の紛失・盗難	非デジタル文書の紛失・盗難	個人情報の漏えい・逸失(人為ミスによる)	個人情報の漏えい・逸失(内部不正による)	個人情報以外の業務データの消失	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	Webサイトの不正改ざん	社員・職員に対するなりすましメール	制御系システムのダウン
製造(N=172)	31.4	26.2	20.3	25.0	16.9	7.0	9.9	4.1	7.6	10.5	7.0	10.5	5.2	8.7	5.8
建設(N=45)	26.7	31.1	15.6	20.0	8.9	6.7	8.9	6.7	8.9	8.9	4.4	8.9	6.7	6.7	0.0
情報通信(N=104)	26.0	32.7	14.4	23.1	6.7	4.8	13.5	6.7	4.8	10.6	5.8	6.7	4.8	2.9	4.8
卸売・小売(N=86)	19.8	14.0	15.1	16.3	15.1	7.0	8.1	4.7	7.0	9.3	2.3	2.3	1.2	5.8	3.5
金融・保険(N=56)	23.2	26.8	12.5	16.1	8.9	10.7	23.2	8.9	5.4	12.5	5.4	7.1	5.4	5.4	3.6
サービス(N=168)	17.3	20.8	12.5	19.0	14.9	9.5	9.5	3.6	8.9	3.0	4.2	4.2	0.6	3.0	6.0
公務・その他(N=67)	25.4	20.9	13.4	6.0	17.9	3.0	25.4	6.0	9.0	1.5	3.0	10.4	4.5	6.0	7.5

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(業種別)

ちなみに、インシデントの認知状況を過去の調査結果と比較した結果が図1-5である。さほど大きな変動はないが、「社内PCのマルウェア感染」の認知率が再び上昇するなど、依然として課題となっていることがうかがえる。また、「モバイルPCの紛失・盗難」や「USBメモリ／記録媒体の紛失・盗難」が減少する一方で、「スマートフォン、携帯電話、タブレットの紛失・盗難」は高止まりしているのも特徴的である。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」といった外部攻撃系のインシデントはいずれも1割未満とはいえ、一定割合の企業が被害を認知しており、予断を許さない状況である。

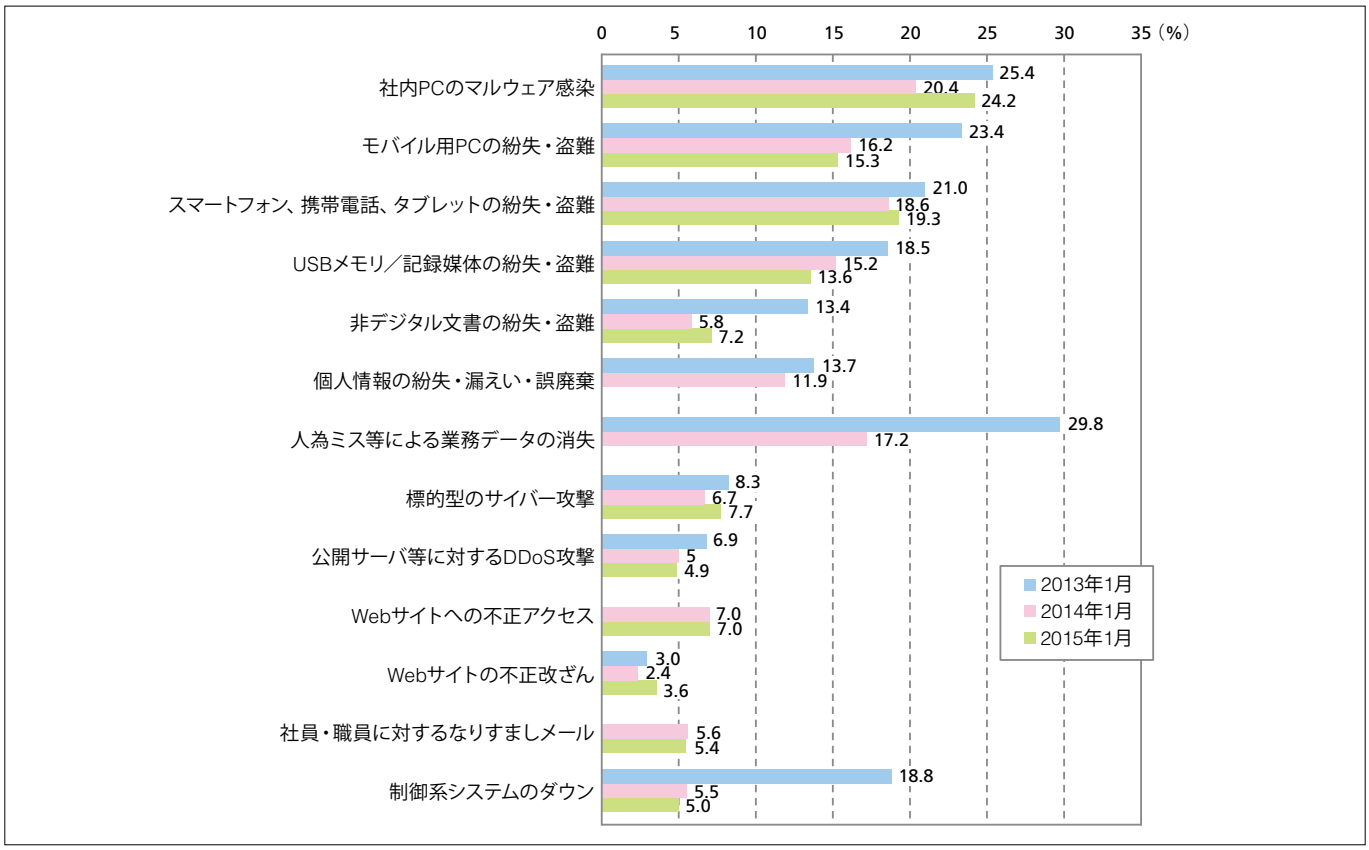


図1-5. 過去1年間に経験したセキュリティインシデントの経年変化（2013〜2015年）

2-3.「標的型攻撃」と「内部犯行」に対するリスクの重視度合い

本調査では、2013年から継続的に「標的型のサイバー攻撃」に対するリスクの重視度合いを調査しているが、今回は、「内部犯行による重要情報の漏えい・消失」に対するリスクの重視度合いも初めて調査対象とした。両者の回答結果を並べると、「内部犯行」に対するリスクの重視度合いの方が高いことがわかった（図1-6）。後者については、4分の1以上の企業が「経営陣からも最優先で対応するよう求められている」としており、「セキュリティ課題の中でも優先度が高い」を含めれば、リスクを特に重視している企業の割合は半数を大きく上回っている。ここにも、2014年に発生した大規模情報漏えい事件の影響が色濃く反映されていることがうかがえる。

しかしながら、「標的型攻撃」についても、重要度が決して下がったわけではない。過去の調査結果と比較すると、「経営陣からも最優先で対応するよう求められている」とする企業の割合が、2013年の14.3%から、2014年に18.9%、2015年には21.9%と、年ごとに増加していることが確認できる（図1-7）。

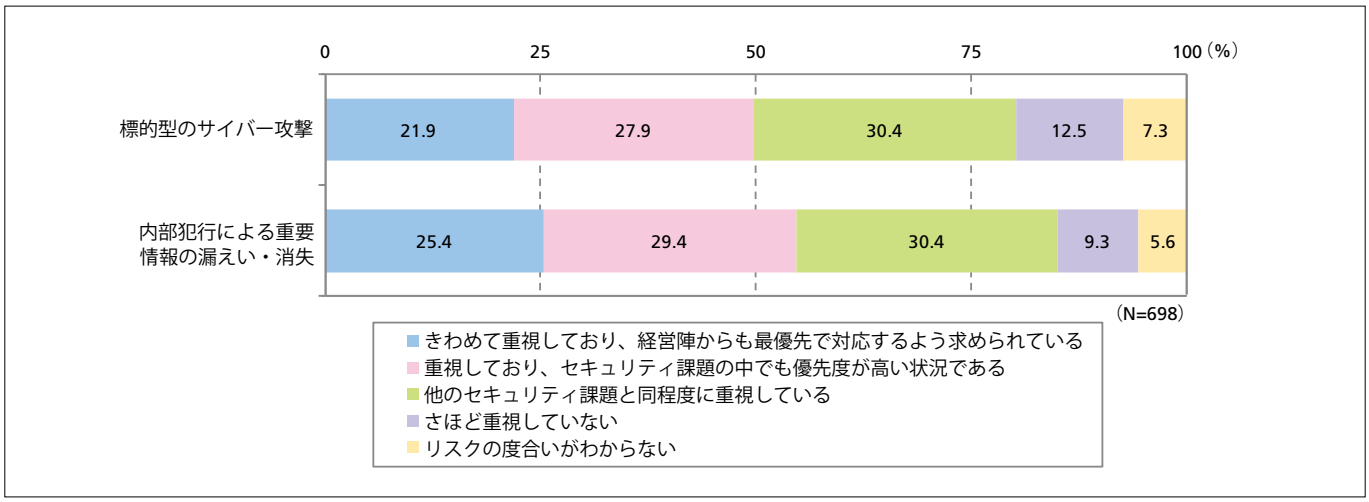


図1-6.「標的型のサイバー攻撃」と「内部犯行による重要情報の漏えい・消失」に対するリスクの重視度合い

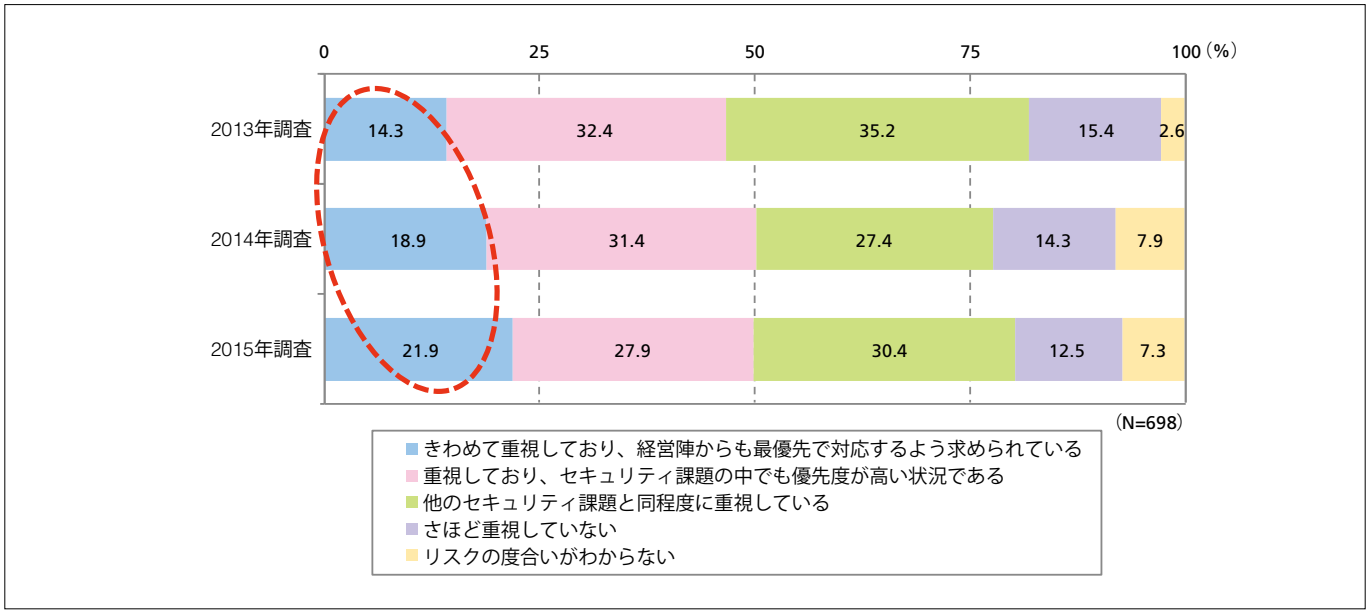


図1-7.「標的型のサイバー攻撃」に対するリスクの重視度合いの経年変化(2013～2015年)

ちなみに、今回の調査で設問に追加した「情報漏えい対策」の実施状況の結果を見ると、「重要情報にアクセスできる人員(部署)の制限」「PCの社外持ち出しの禁止」「重要情報の取り扱い責任者の任命」が実施率の上位3項目となった。だが、本来重視されるべき「重要情報の定義・特定・他の情報資産との分離」については、それよりも実施率が低く、「どんな情報を守るべきか」がそもそも明確になっていないことが改めて浮き彫りとなった(図1-8)。

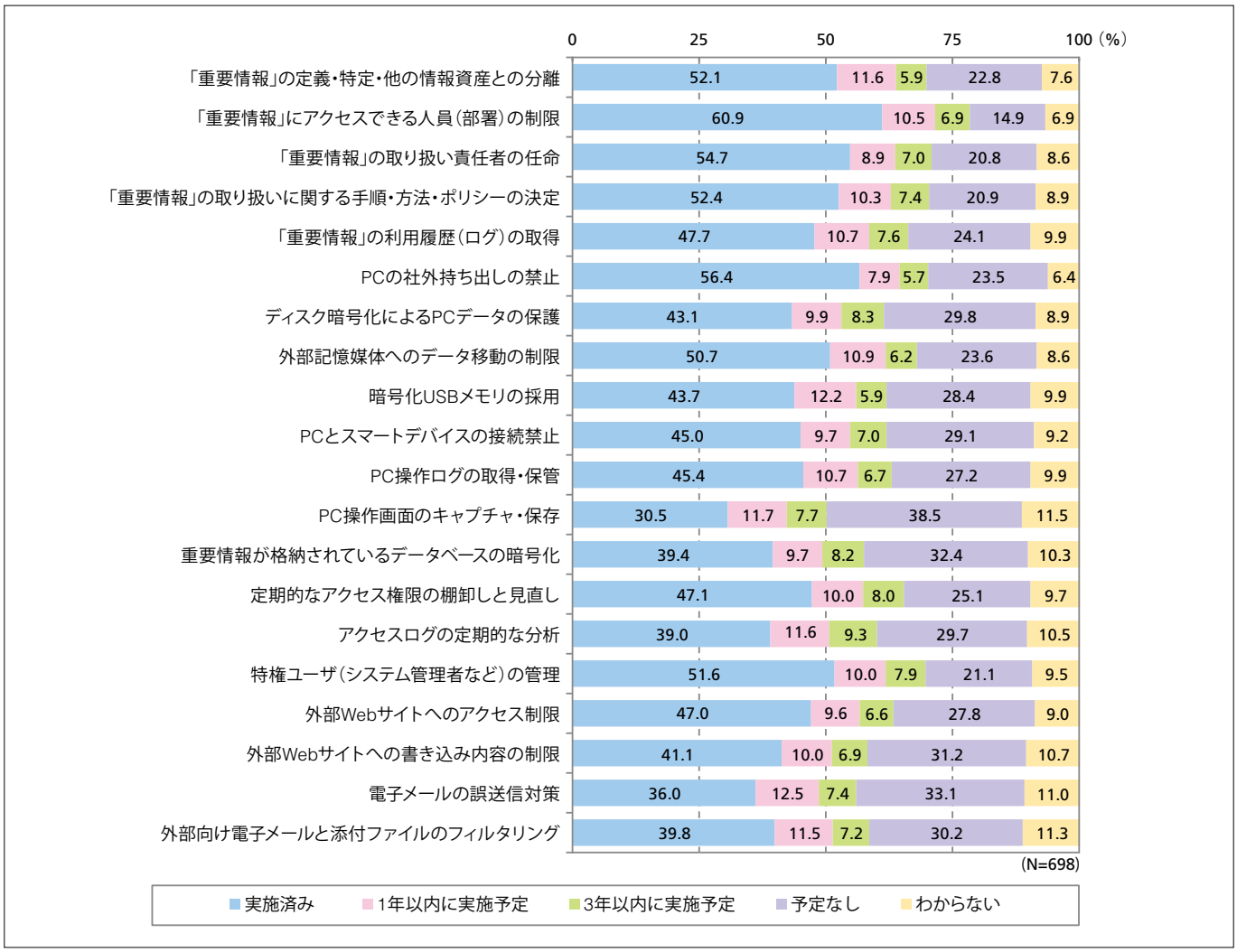


図1-8.「情報漏えい対策」の実施状況

3 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、第三者による認定／認証制度は広く認知されている。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定点観測を行っている。本章では、その最新動向について紹介する。

3-1.引き続き高い認知率を維持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9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取得意欲について問うた設問では、最も取得率が高かったのが「プライバシーマーク制度」、次いで「ISMS適合性評価制度」となった(図1-9)。この上位2項目はいずれも認知度も高く、70%を上回った。認知度の高さと取得率の高さは連動しており、それは、認定／認証制度を取得することの価値を問うた結果で、「企業・組織としての信頼性の高さを対外的にアピールできる」という回答が2番目に多いことにも表れている(図1-10)。

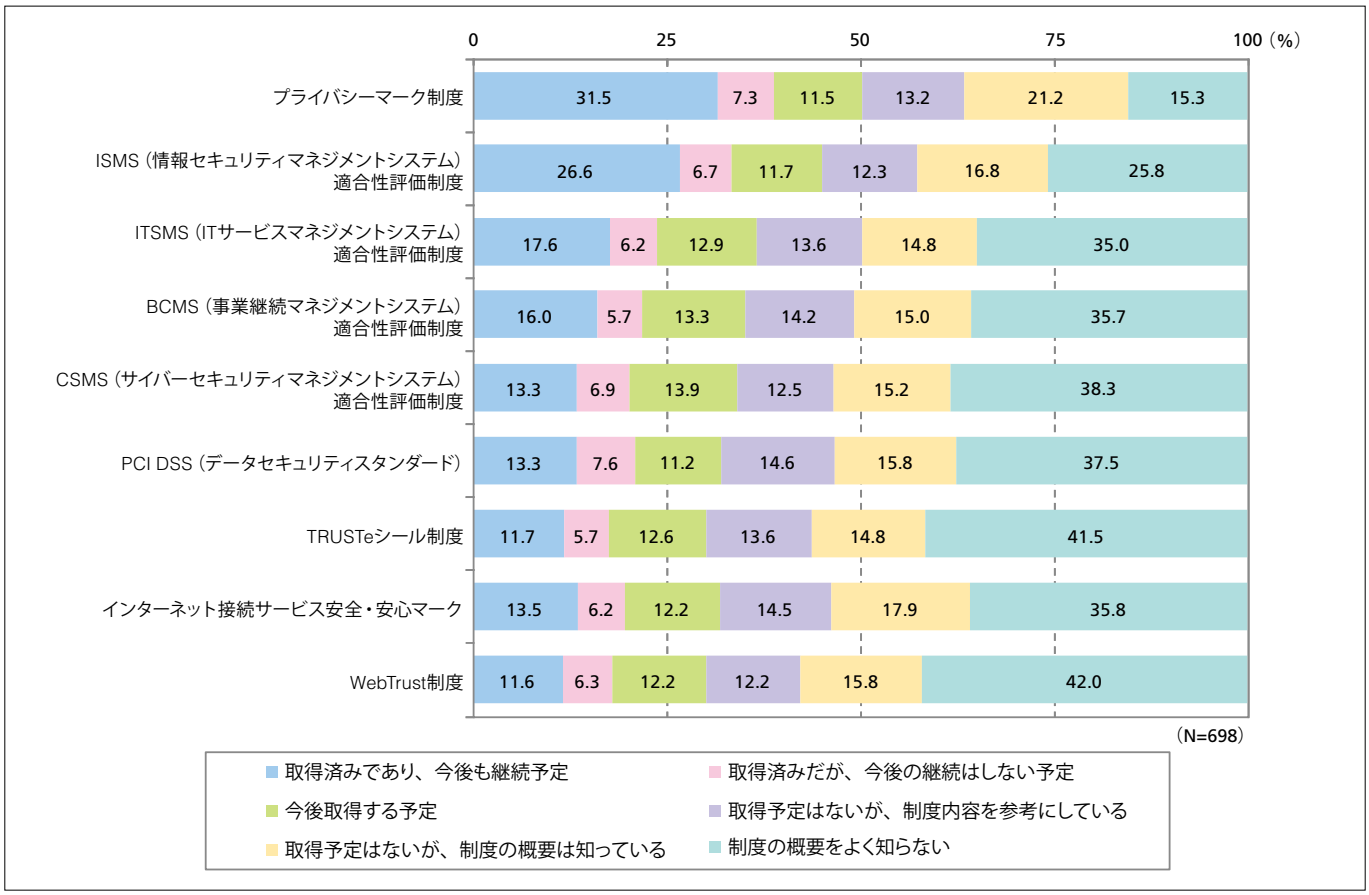


図1-9. 情報セキュリティに関わる認定／認証制度の取り組み状況

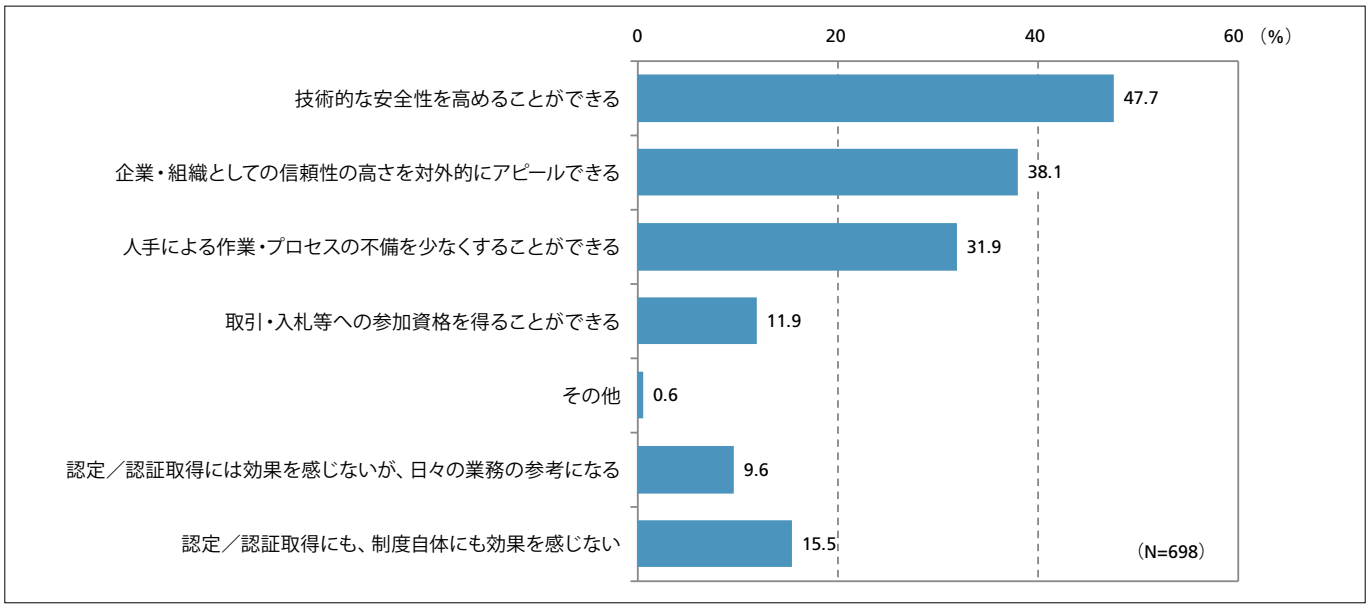


図1-10. 認定／認証を取得することの価値

認定／認証の取得につながりやすいと考えられる「システムリスクの緩和策」の実施状況を問うたところ、「事業継続計画（BCP）の策定」と「全社的なリスクマネジメントの構築」は、いずれも実施率がほぼ半数に上った。特に後者については、「実施済み」とした企業のうちの半数以上がISMS適合性評価を取得しており、リスク対策のためのツールとして認定／認証制度が定着していることがうかがえた（図1-11）。

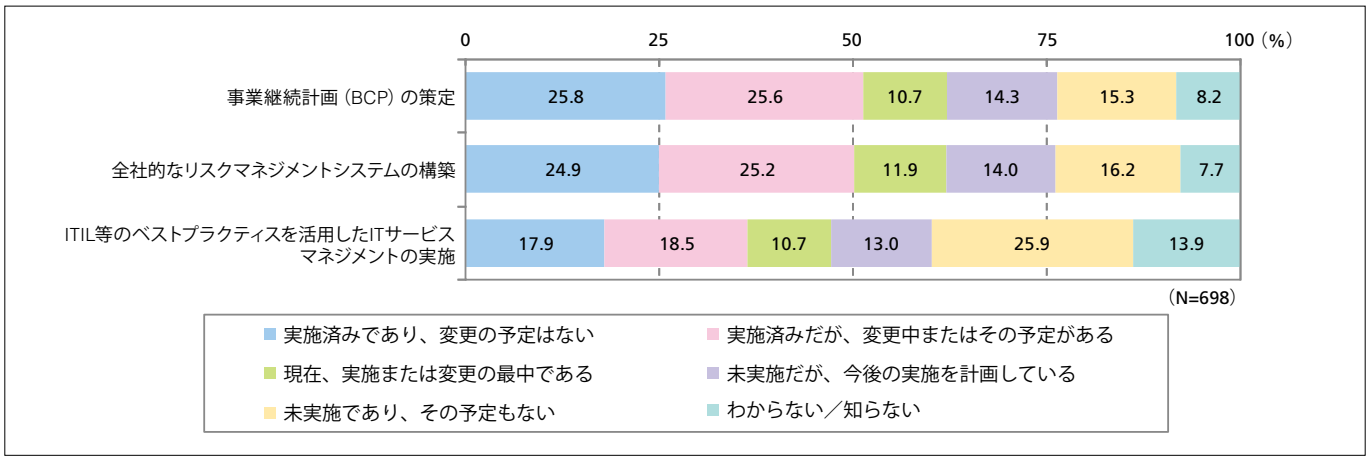


図1-11. システムリスクの対応策の取り組み状況

3-2.プライバシーマーク制度に期待を寄せるサービス業

最も普及している認定／認証制度であるプライバシーマークに対する取り組み状況を業種別に見ると、現時点での取得率では「情報通信」が圧倒的に高いが、今後に向けて取得を予定している割合では、「サービス」と「卸売・小売」が高い値を示した（図1-12）。こうした業種では、Eコマースやポイントカードシステムの採用などに伴い、個人情報を管理する必要性に迫られる企業が増加しており、その影響も大きいと考えられる。

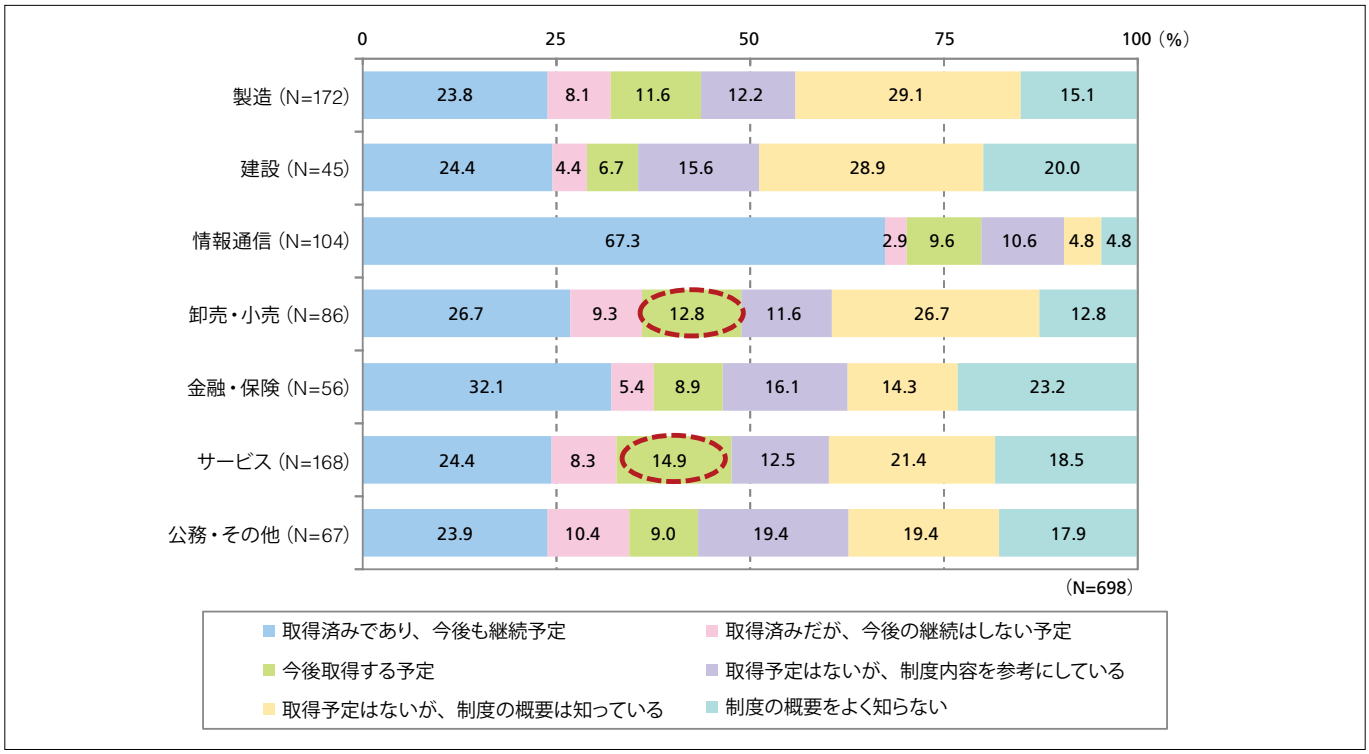


図1-12.「プライバシーマーク制度」に対する取り組み状況（業種別）

なかでもサービス業では、認定／認証取得をビジネスを成長させるために利用しようとする企業が多いと考えられる。同業種では、プライバシーマーク制度に望むこととして、「プライバシーマークの取得のビジネス価値を最大化してほしい」と考える企業がきわめて高く、43.1%を占めた（図1-13）。

デジタルマーケティングやビッグデータ活用といった新たなテーマが浮上するなかで、プライバシーマーク制度には、企業におけるデータ活用の適正性を証明するための指針としての役割も期待されていると言える。

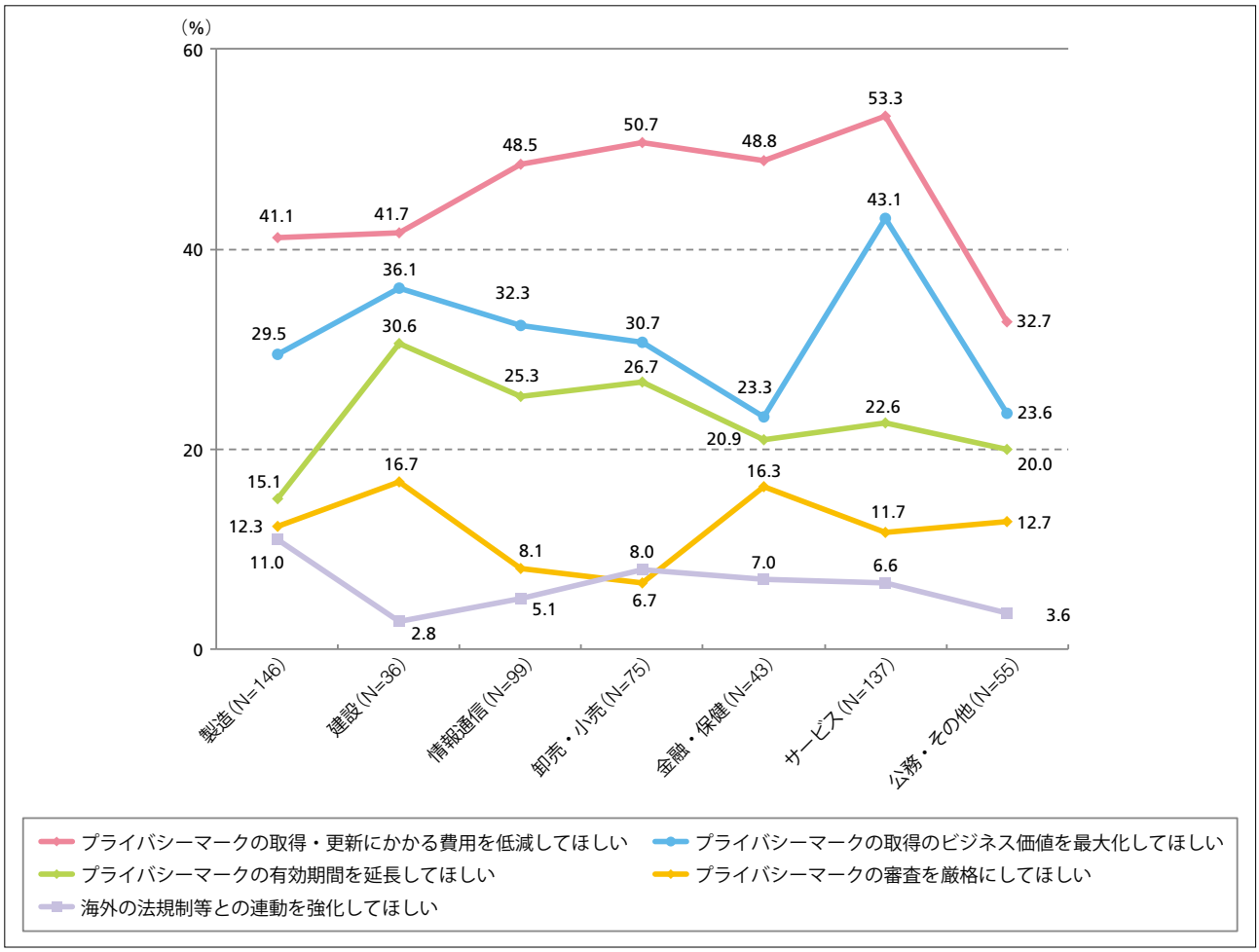


図1-13.「プライバシーマーク制度」に対して望むこと(業種別)

4 セキュリティ支出と組織的な対策の動向

本調査では、2014年に引き続きセキュリティ支出の動向にまつわる調査を実施した。ここでは、組織的なセキュリティ対策の実施状況と合わせて紹介する。

4-1.支出の増加を見込む企業が多い「外部攻撃対策」と「モバイル対策」

ここでは、2014年同様、主要用途として15項目を取り上げ、それぞれに対して2015年度支出の増減見込みを問うた（図1-14）。

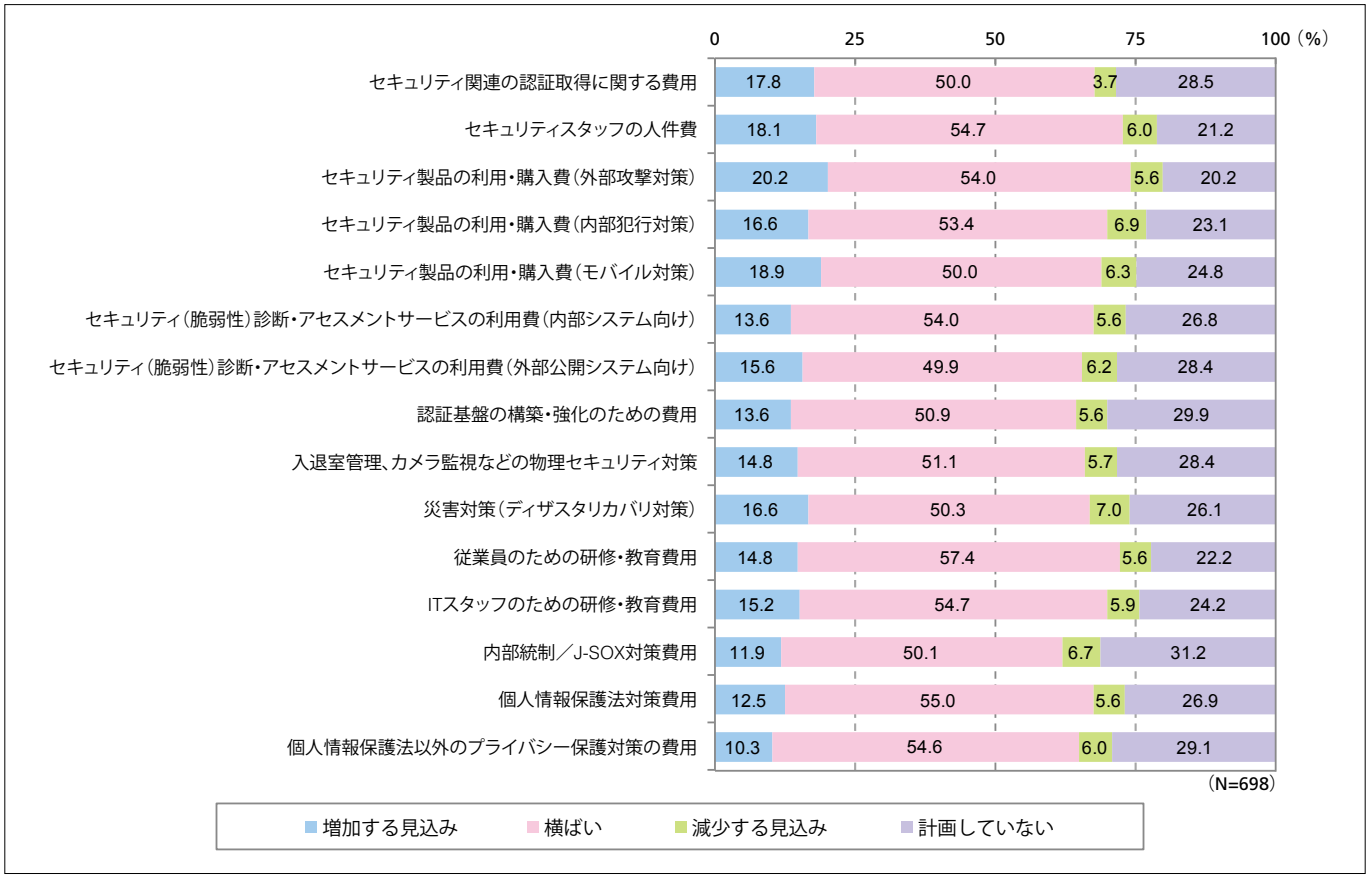


図1-14. 2015年度に想定されるセキュリティ支出の増減見込み

「増加する見込み」と回答した企業の割合が最も高かったのは「セキュリティ製品の利用・購入費（外部攻撃対策）」であり、唯一20%を超えた。続いて「セキュリティ製品の利用・購入費（モバイル対策）」となり、上位2項目は前年結果と同一となった。前者については標的型サイバー攻撃に対する懸念、後者についてはスマートデバイスの普及が背景にあると見られる。

なお、回答結果を指数化（増加を3、横ばいを2、減少を1とした合計値を有効回答で除す）し、その結果を2014年調査結果と比較したところ、2015年度は、セキュリティ製品の利用・購入に直接関わる支出が絞られ、代わって「セキュリティスタッフの人件費」や「セキュリティサービス」に対して振り向けられる可能性があることが確認された（図1-15）。

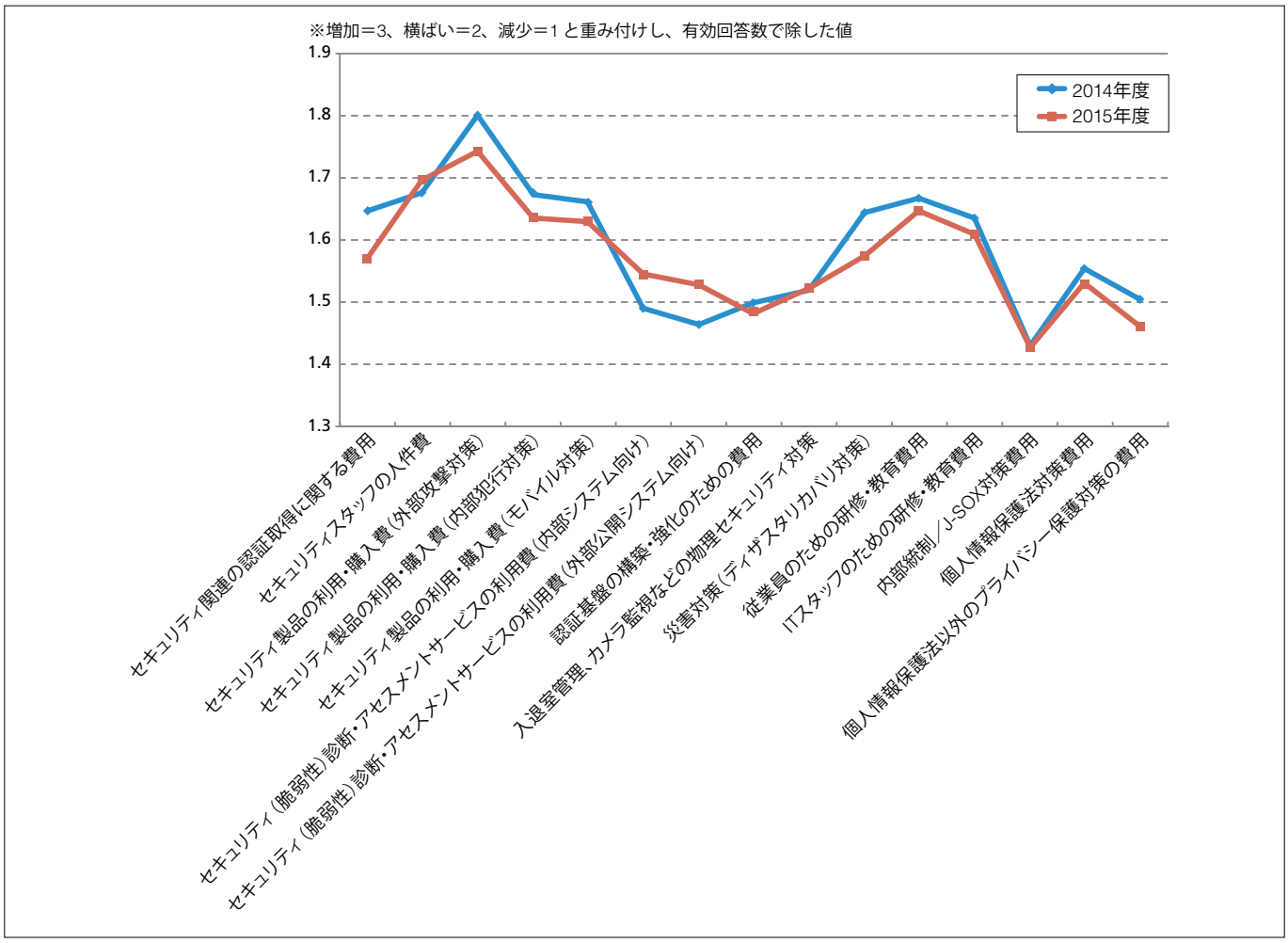


図1-15. セキュリティ支出の増減見込みの比較（2014年度／2015年度）

4-2.組織体制の整備はやや足踏み

一方、やや足踏み状態になっていると見られるのが、組織体制の整備である。本調査では、経営者の関与による方針の明確化や担当部署の設置、責任者の任命などに関する動向を定点観測しているが、最新の結果では、図1-16にあるように多くの項目が50%前後の実施率となってはいるものの、2013年、2014年調査の数値からほとんど伸びていないことが明らかになった。

いずれも「今後実施予定」とする割合が高いことから、企業としても組織体制の整備は重要課題になっているはずであるが、現実が追いついていないと考えられる。

なお、今回新たに項目に加えた「セキュリティ初動対応の専任チーム（CSIRT）の立ち上げ」は、28.2%が実施済み、27.2%が今後実施予定と回答した。

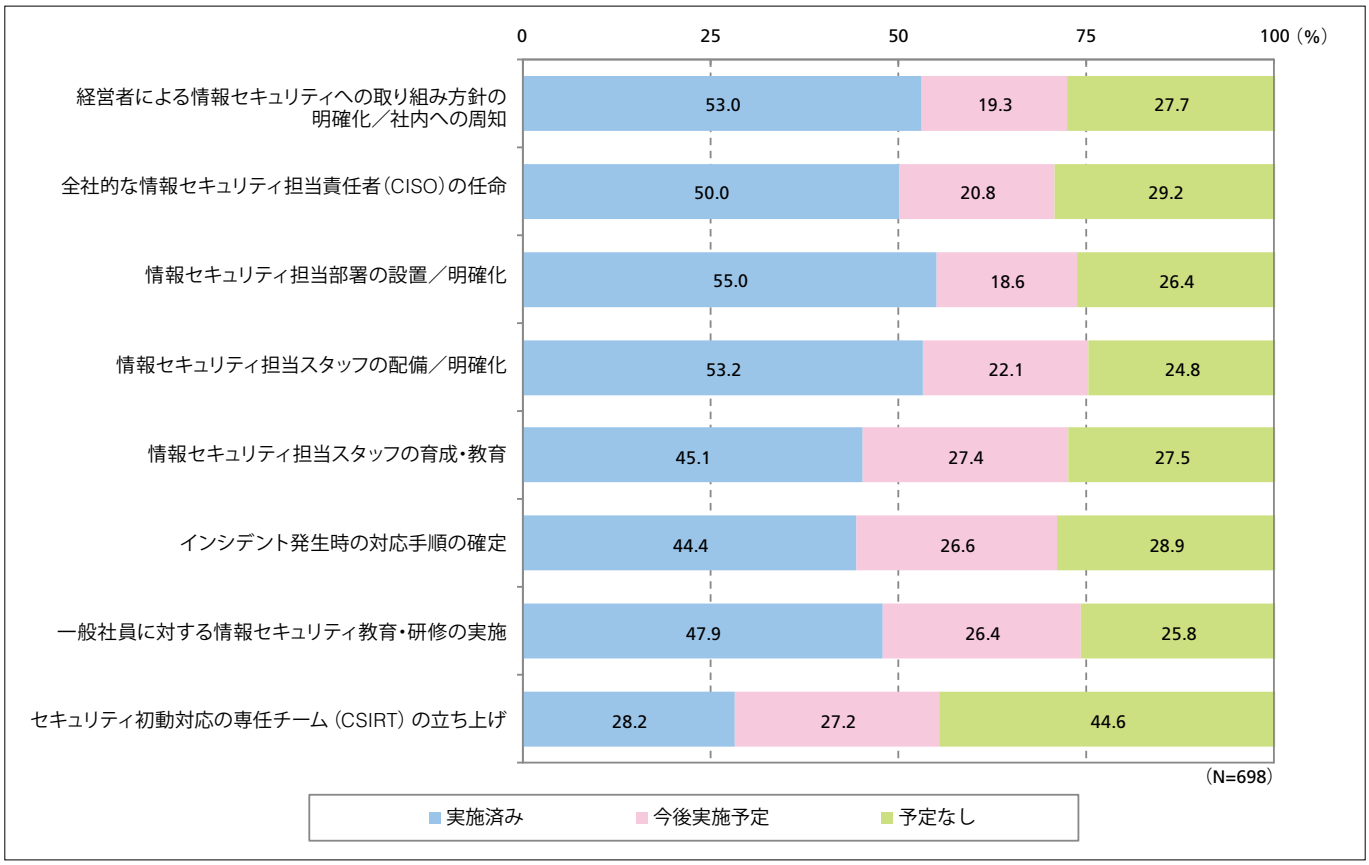


図1-16. 組織に関わるセキュリティ対策の実施状況

5 法制度への対応方針

法令の改正や施行も、企業の情報セキュリティ対策に大きな影響を及ぼすテーマである。今回の調査では、そうした法制度の中でも特に関心が高いと考えられる個人情報保護法の改正と、社会保障・税番号（マイナンバー）制度について対象に加え、企業のIT／セキュリティ責任者の意識度合いを調査した。

5-1.個人情報保護法改正を巡る対応方針

2005年の全面施行以来、初めての大幅改正となる見込みの個人情報保護法については、個人情報の定義の明確化や第三者機関の新設、グローバル化への対応などについて見直されることになると見られている。そこで、本調査では、個人情報保護法が改正された場合、自社にどのような影響が及ぶかについての意識を問うた。その結果、全体の半数以上が、「システム、プライバシーポリシー両方の変更・修正が必要になる」と回答した（図1-17）。

全面施行から約10年間、企業の情報セキュリティ対策の方向性に大きな影響を及ぼしてきた同法だけに、IT／セキュリティ責任者もそのインパクトは小さくないと見ていることがわかる。

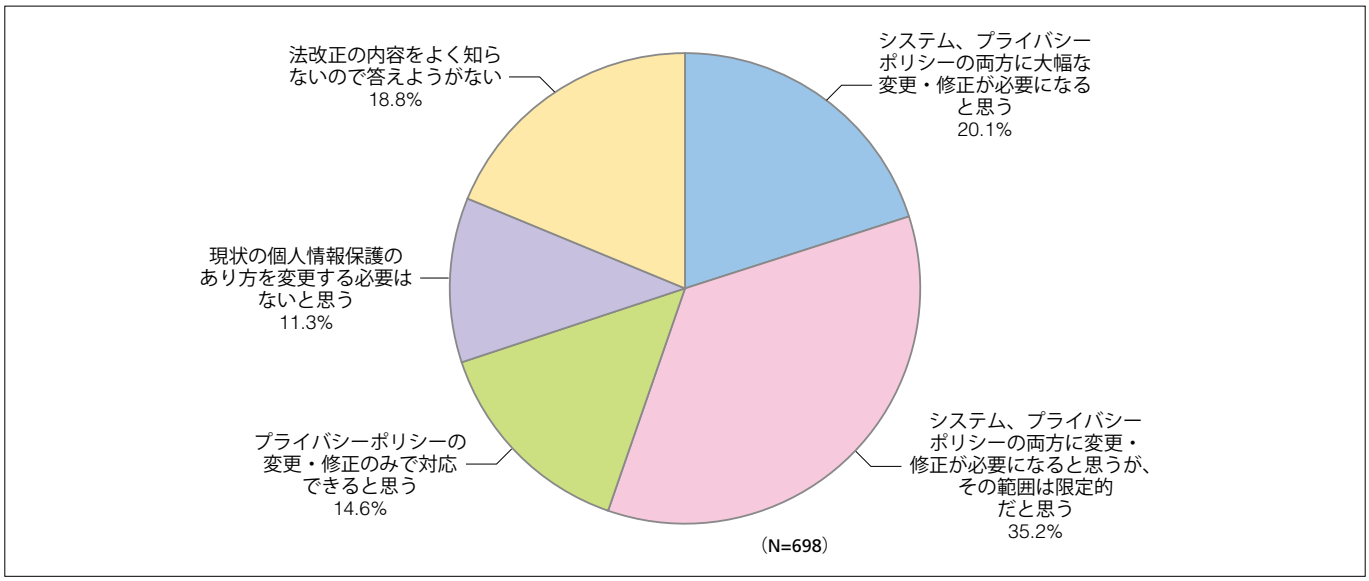


図1-17. 個人情報保護法改正のインパクト

なお、企業が個人情報の取り扱い方針を明記しているプライバシーポリシーについては、消費者にとってわかりにくい、読みにくいといった問題点が指摘されることが多く、その問題に起因したトラブルもたびたび報告されている。そうしたプライバシーポリシーのあるべき姿について回答を求めたところ、「読み手にとって、よりわかりやすく、確実な同意を得やすい文書にすべきである」とした企業が40%以上に達した一方で、「読み手のわかりやすさを多少犠牲にしてでも、内容の網羅性や企業としての免責を重視すべき」、または「同業他社と同レベルの内容でよい」とした企業も約40%となり、意見が割れていることも明らかとなった（図1-18）。

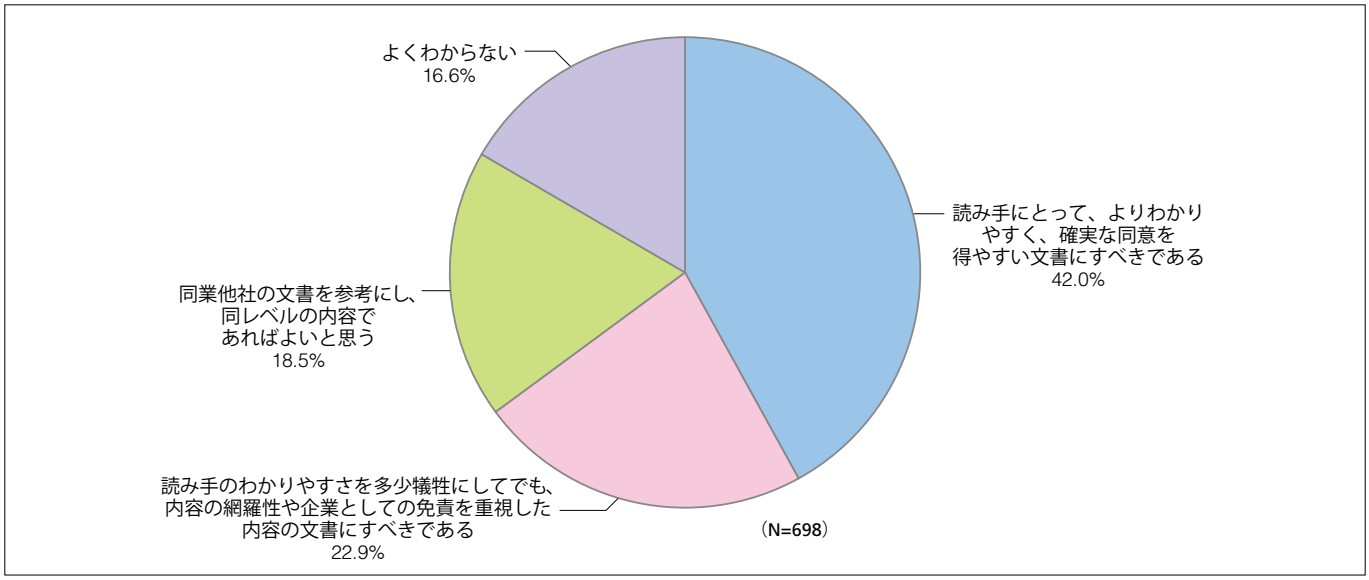


図1-18. プライバシーポリシーのあるべき姿

また、プライバシーポリシーの策定や変更にかかる作業を誰が主導しているかについても、企業によってまちまちであるという実態が明らかになった。最も多かったのは「社内の情報システム部門が主導している」であるが、「社内の法務部門」「個人情報を取り扱う事業・サービス部門」とした回答も僅差で続いた。また、「外部の専門家（弁護士など）が主導している」

とした企業はわずか3.6%にとどまり、あくまでも社内のスタッフが中心となって文書の策定・変更を主導していることがわかった（図1-19）。

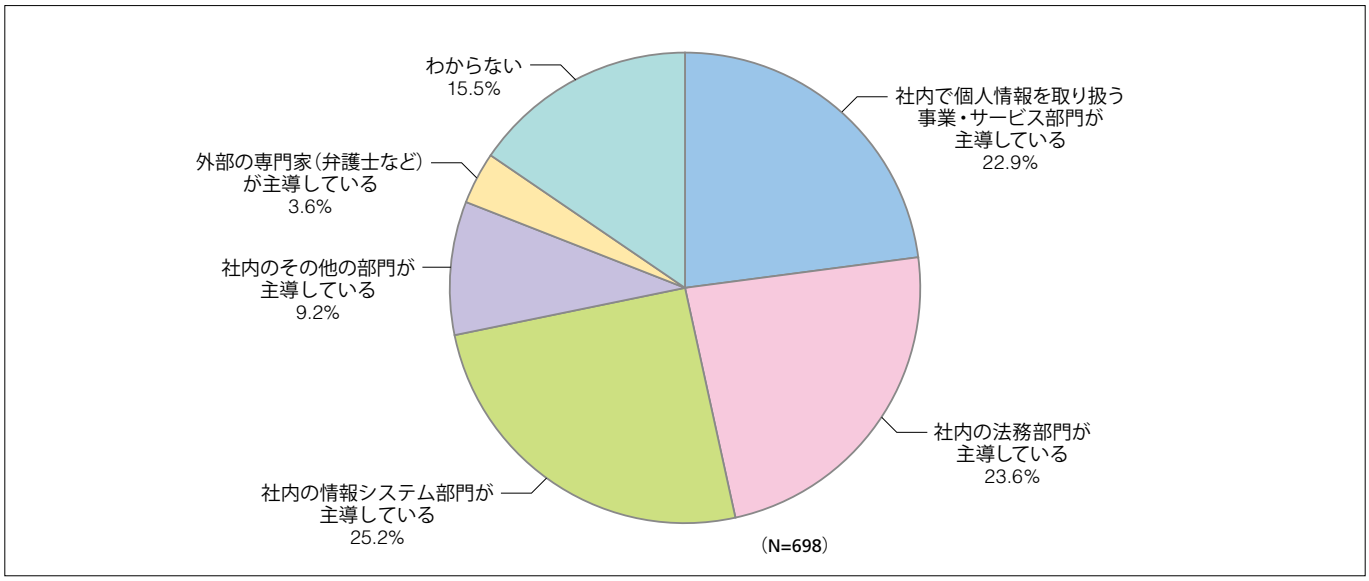


図1-19. プライバシーポリシー策定・変更の主導者

5-2.社会保障・税番号制度を巡る対応方針

2015年度におけるもう1つの重要テーマが、社会保障・税番号（マイナンバー）制度への対応である。社会保障、税分野を中心に一部の用途に限って、生涯不変の個人番号（マイナンバー）を活用する同制度については、法定調書の発行が必要な企業に対しても、個人番号の安全な取得・管理が求められる。まず、本調査で情報システムの対応状況について問うたところ、図1-20のような結果となった。

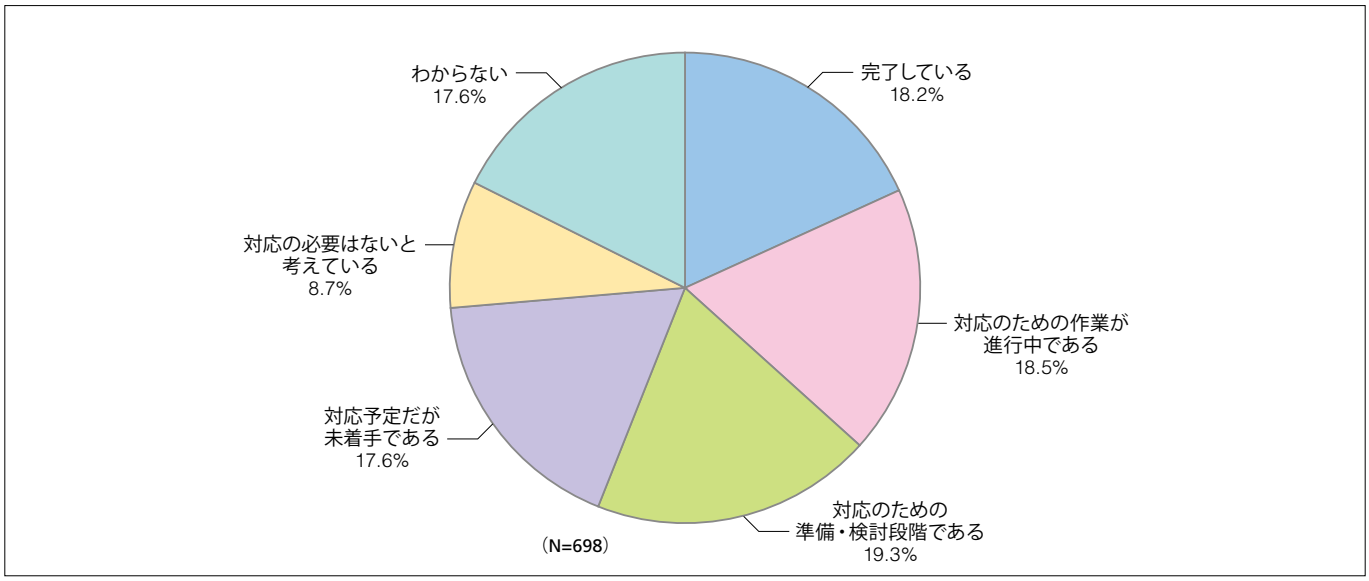


図1-20. 社会保障・税番号（マイナンバー）制度への情報システムの対応状況

「準備・検討段階」も含めた着手の割合が半数を超えたが、第三者機関である特定個人情報保護委員会による「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」が2014年12月中旬に公表されて間もない翌年1月の時点で、約2割が「完了」と回答している。一方で、「わからない」とした回答者も多い。IT／情報セキュリティ責任者の中には、かならずしも、制度対応として何をすべきか十分に把握できていない状況にありながら、システム対応が完了していると理解している可能性も考えられる。なお、本調査では、「業務（手順、プロセス、役割分担など）の対応状況」についても回答を求めたが、結果は上記とほぼ同一となり、業務と情報システムの対応が併行して進められていることがわかった。

また、対応または対応予定とした企業に、具体的な対応の範囲を問うたところ、「人事・給与管理システムの改変」が54.9%で最多となり、「財務会計システムの改変」が続いた（図1-21）。この結果からは、多くの企業が既存アプリケーションシステムの改変を中心とした限定的な対応を想定していることがうかがえる。

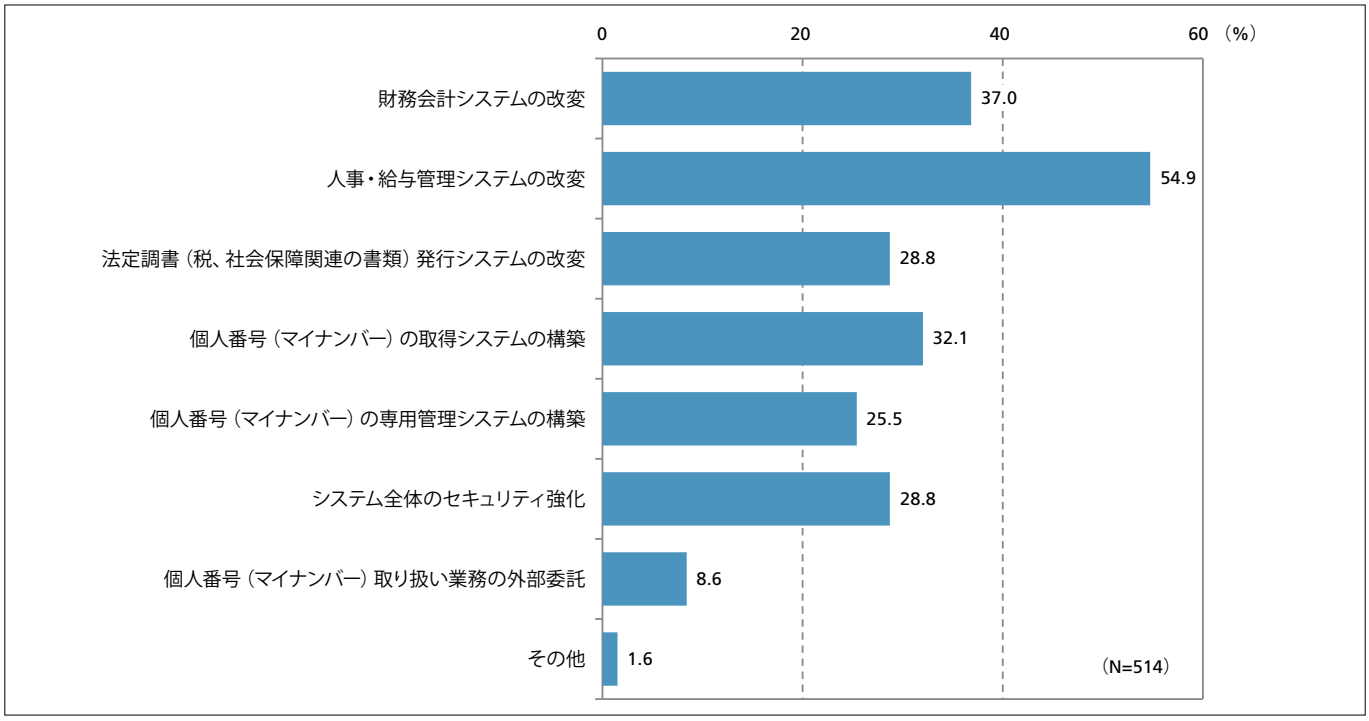


図1-21. 社会保障・税番号（マイナンバー）制度への情報システムの対応範囲

また、同制度の対応状況に大きく影響すると見られるのが、厳格な管理が求められる従業員の個人番号の取り扱い責任をいったい誰が担うのか、ということである。この点について問うたところ、全体の約65%が「本社（人事部門など）が全社の情報を集約して管理する方針」であると回答した（図1-22）。この結果は企業の規模を問わず、ほぼ一定である。

個人番号の管理対象は社員だけでなく、パートやアルバイトの職員、さらには源泉徴収が発生する個人など、きわめて多数に及ぶ。その情報を全社的に集約化するとなれば、その収集（本人確認作業を含めて）および管理のために何らかの専用システムが必要になる可能性が高いだろう。仮に、この方針どおりに対応を進めるのであれば、対応に必要な工数はかなり膨大なものになると想定される。IT部門は人事部門などと連携し、早期に自社のシステム要件を精査することが求められるであろう。

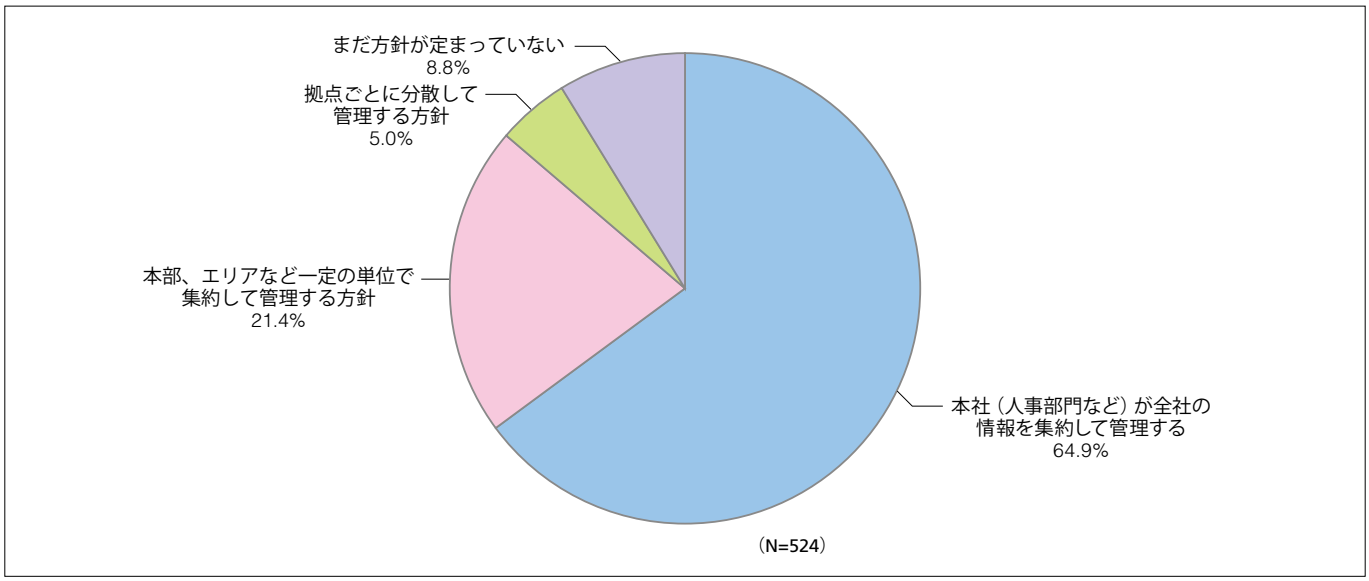


図1-22. 個人番号の取り扱い方針

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において製品／サービスが果たす役割は大きい。ここでは、主要なセキュリティ製品の導入状況を分野ごとに見ることにする。

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）の境界部で動作するネットワークセキュリティ製品は、「ファイアウォール」が最も高い導入率であり、「VPN」が続いている。また、今後に向けて導入を計画する企業の割合が高い項目としては「次世代ファイアウォール」「DLP（情報漏えい防止）システム」「統合ログ管理（SIEM）ツール」が上位となった（図1-23）。

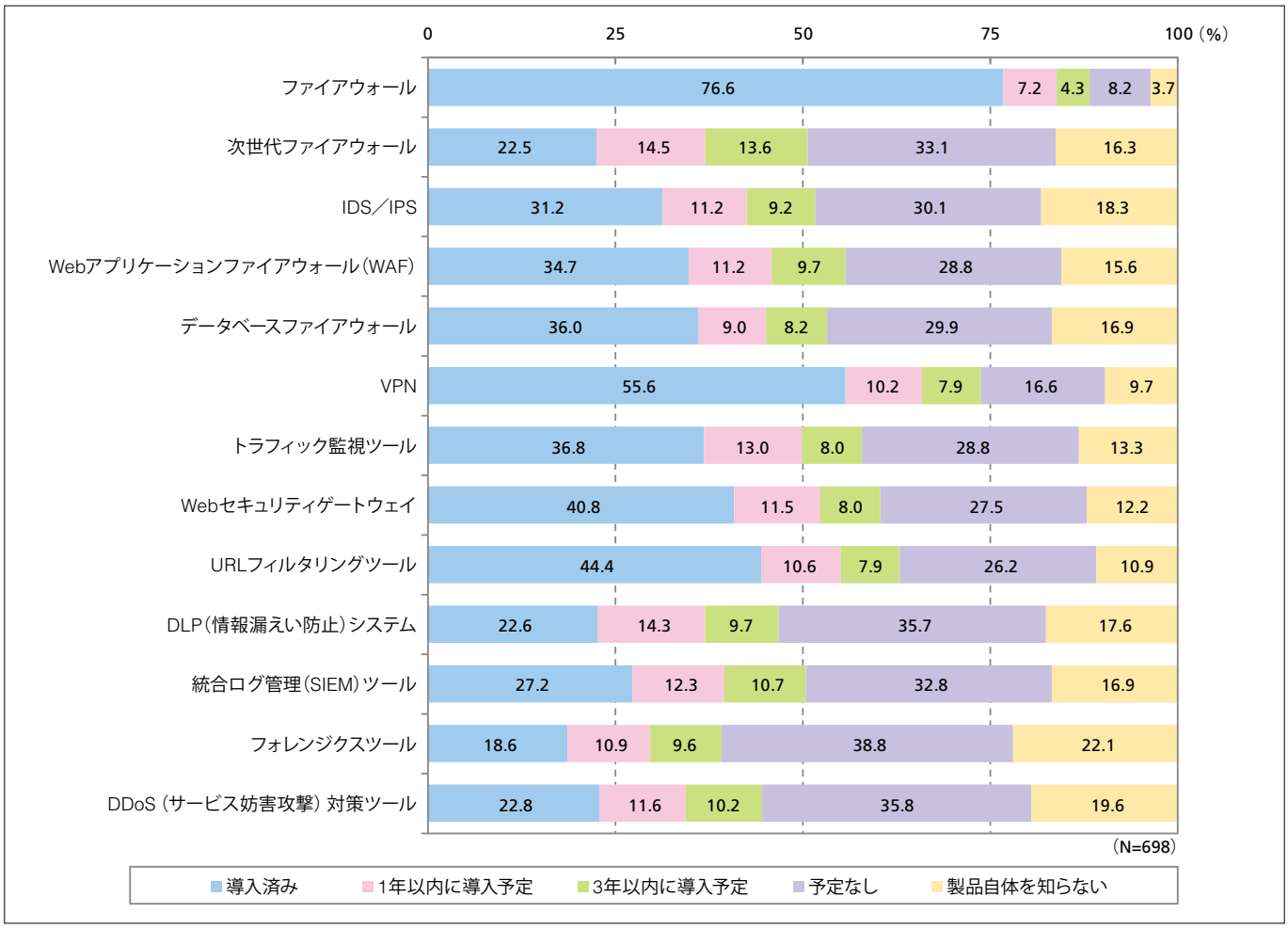


図1-23. セキュリティ製品の導入率(ネットワークセキュリティ)

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)」の導入率が際立って高い傾向に変化はない。今後に向けては、「IRM／DRM(ライツ管理)ツール」「PC資産管理ツール」「PC操作ログ管理ツール」「シンクライアントシステム」の導入意欲がそれぞれ2割程度となった(図1-24)。

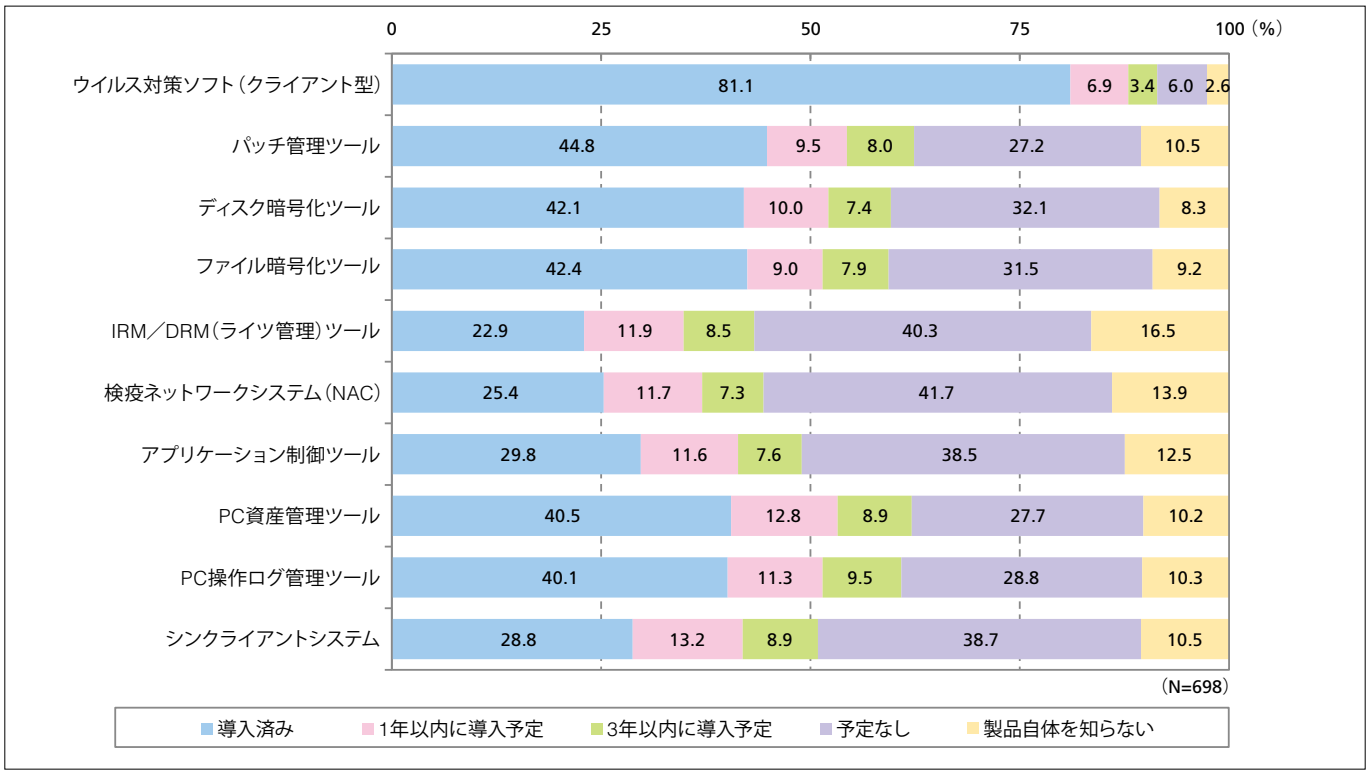


図1-24. セキュリティ製品の導入率(クライアントセキュリティ)

6-3.メールセキュリティ製品の導入状況

外部からのサイバー攻撃の初期侵入防止や、外部への不適正な送信防止を目的に利用されることの多いメールセキュリティ製品の中では、「スパム対策ツール」の導入率が最も高い。今後に向けては、「メール監査ツール」「メールアーカイブツール」「なりすまし防止対策」などのサイバー攻撃対策を強く意識した製品の導入を予定している割合が2割超となっている(図1-25)。

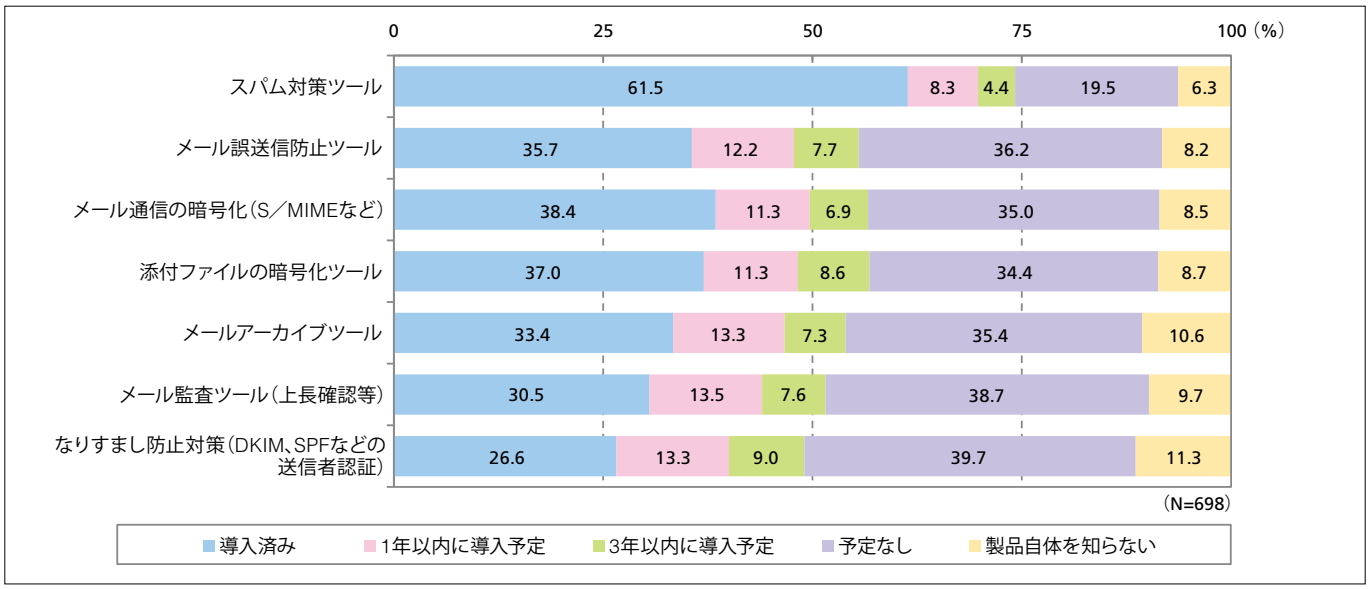


図1-25. セキュリティ製品の導入率(メールセキュリティ)

6-4.アクセス管理製品の導入状況

ユーザ認証に関わるアクセス管理製品は、例年の調査結果と同様、他分野と比較して導入率が低い分野である。その中では、多数の業務アプリケーションに対して一貫したアクセス環境を提供する「シングルサインオン基盤」に対する導入意欲が上昇傾向にある（図1-26）。

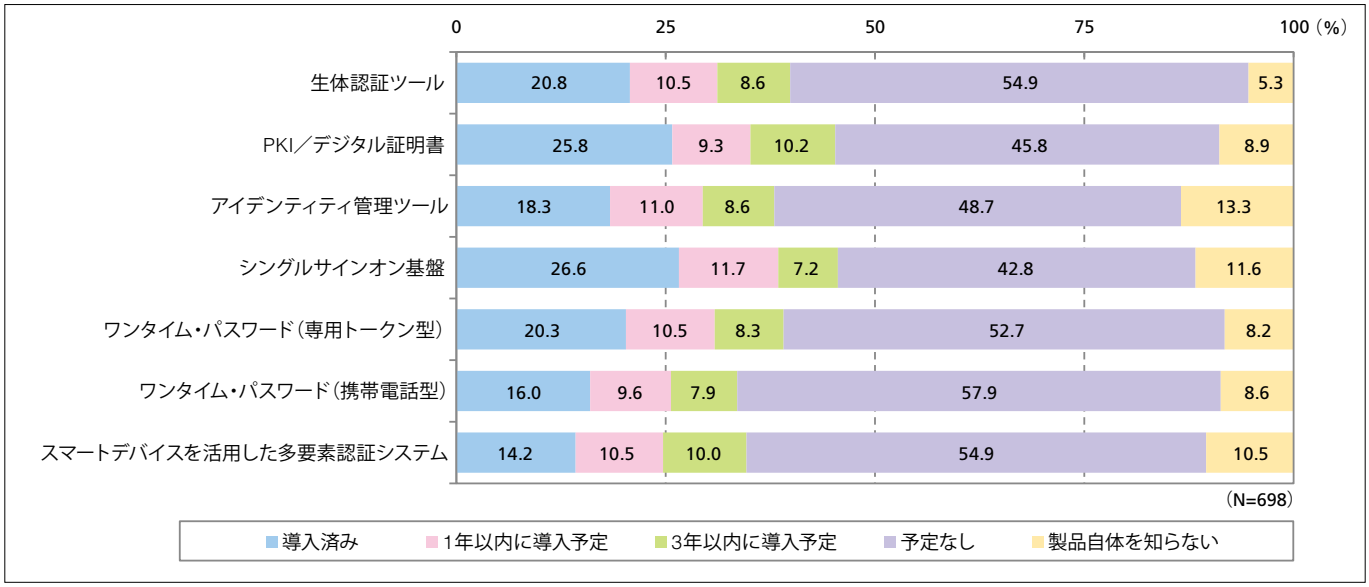


図1-26. セキュリティ製品の導入率（アクセス管理）

6-5.セキュリティサービスの利用状況

セキュリティサービスについては、前述の支出動向でも増加傾向が示されており、今後に向けた有望分野であると考えられる。現在の利用率は20～30%台にとどまっているが、「1年以内に利用開始予定」とした企業の割合がいずれも10%を超えており、今後の利用拡大が見込まれる（図1-27）。

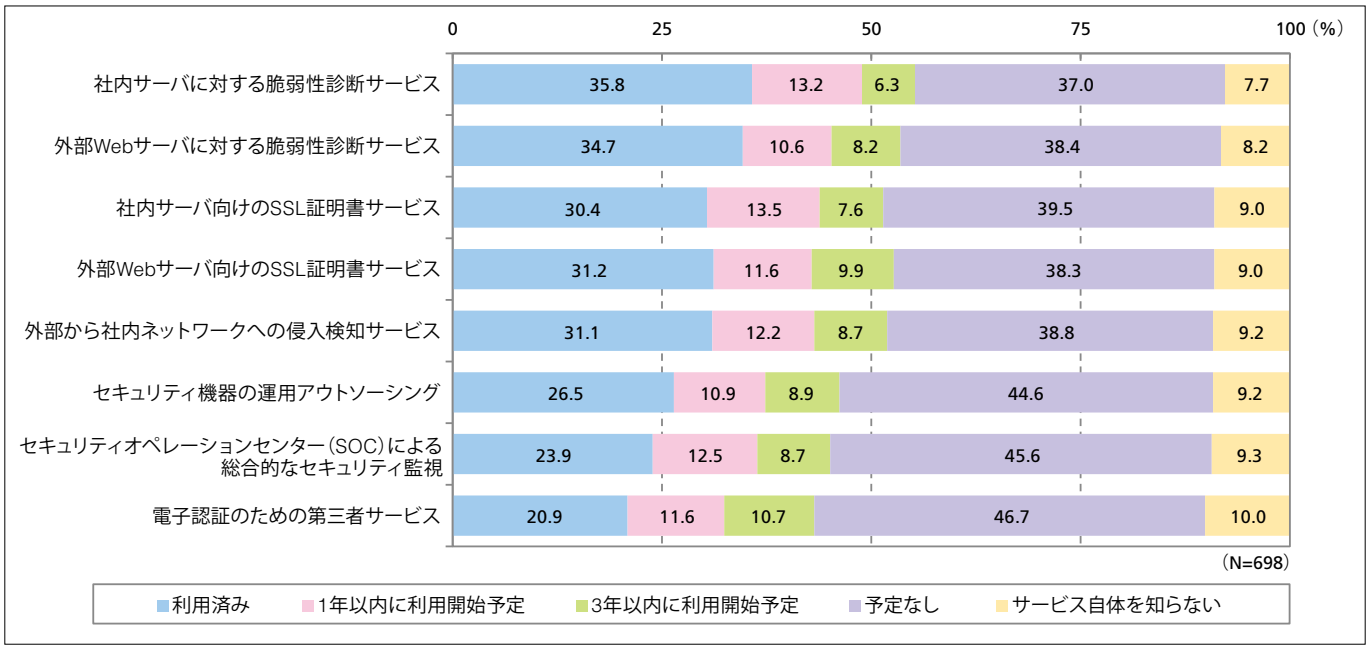


図1-27. セキュリティ製品の導入率（セキュリティサービス）

7 スマートデバイス／クラウドサービスの位置づけ

企業ITの中でその重要性が増しているスマートフォン、タブレットなどのスマートデバイス、クラウドサービスにまつわる動向をまとめて紹介する。

7-1.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から見てみることにする。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についての取り組み状況を見ると、「会社支給によるスマートフォンの導入」「会社支給によるタブレットの導入」は、「試験的に実施」までを含めた導入率がいずれもほぼ55%程度となった。それに対して、私物端末の業務利用（いわゆるBYOD）の実施率は、スマートフォン、タブレットともに30%台である（図1-28）。

なお、本調査では、全従業員の50%以上を対象とした取り組みを「全社的に実施」としているが、その割合が最も高いのは「会社支給によるスマートフォンの導入」（18.8%）であった。このことから、スマートデバイスの導入はやはり会社支給が主流であり、私物端末の業務利用の進展は限定的であることが見てとれる。

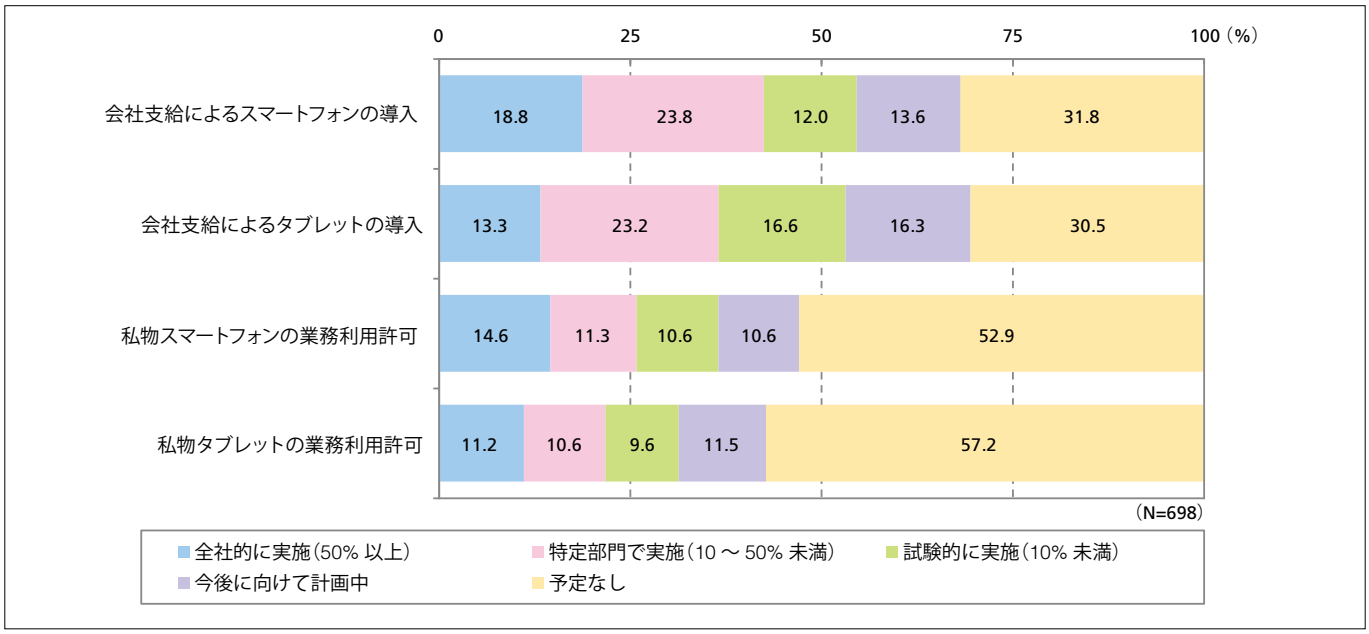


図1-28. スマートデバイスの導入状況（2015年1月時点）

7-2.スマートデバイスの普及は台数が増加する成熟期へ

今回の調査結果から明らかなのは、スマートフォンにせよタブレットにせよ、新たに活用しようとする企業の数は2割にも満たず、1社当たりの台数の増加がより顕著になっているということである。

図1-29は、「会社支給によるスマートフォンの導入」と「会社支給によるタブレットの導入」それぞれについて、過去3回の調査結果の推移をまとめたものである。これを見ると、全体の導入率はさほど変化しておらず、すでに実施済みの企業の中で、大規模導入の割合が増えていることが読み取れる。特にスマートフォンについては、「全社的に実施」とする企業の割合が今回大きく増加しており、その傾向がより顕著である。

すでにスマートデバイスを導入している企業は、デバイスの“多台数化”を想定した運用管理プロセスを整備することが求められるであろう。

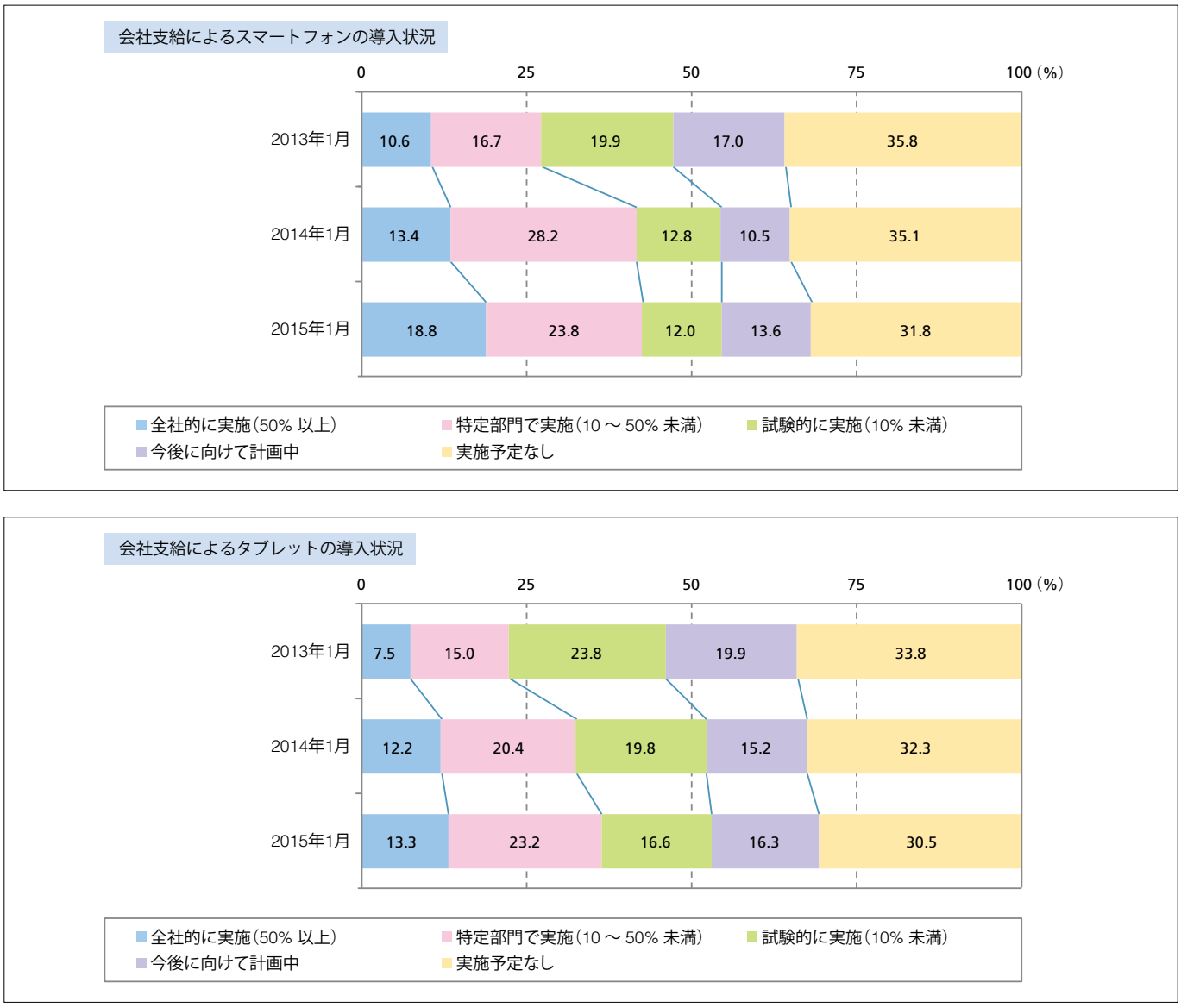


図1-29. スマートデバイスの導入状況の経年変化（2013年～2015年）

7-3.スマートデバイスの用途

スマートデバイスを導入済みの企業に対して、その用途を問うた結果は、2014年の調査結果から傾向にほとんど変化が見られない。現時点の利用目的として値が高いのは「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項目である。

一方、今後の利用目的としては、「在宅勤務者の業務支援」を想定する企業が最も多く、次いで「クライアントPCの代替」「顧客窓口スタッフの業務支援」が続いた。デバイスの性能向上に伴い、従来のPCに変えてスマートデバイス活用を検討する企業が増加することが見込まれる（図1-30）。

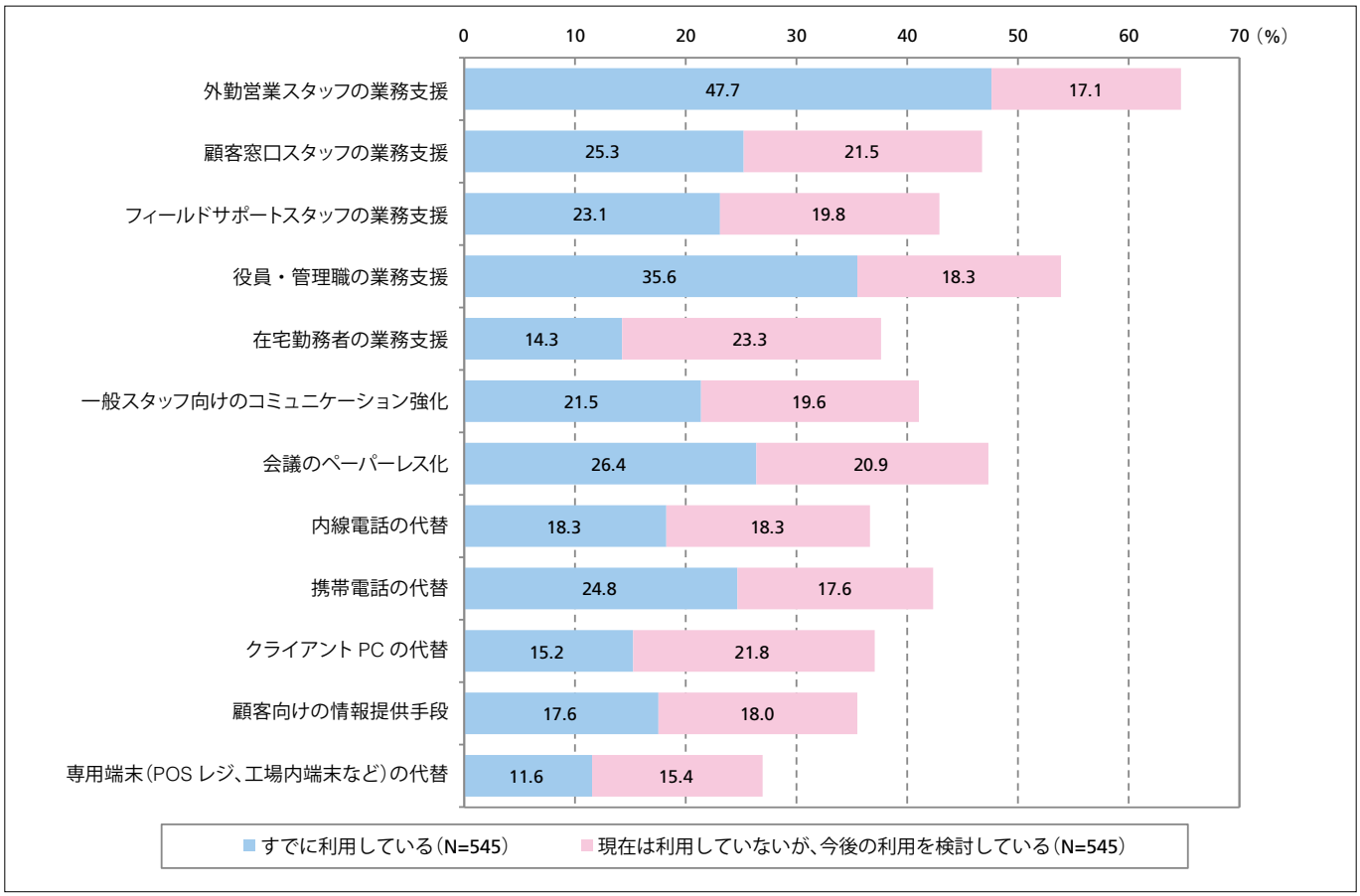


図1-30. スマートデバイスの利用目的(現在／今後)

7-4.払拭されつつあるクラウドコンピューティングへの不安

クラウドコンピューティングについては、確実に普及が進む一方で、セキュリティや継続性などに対するIT部門からの不安もいまだに大きいとされている。今回の調査では、「可用性・稼働率の高さ」「情報漏えい被害の軽減」など複数の評価項目を設定し、それぞれについて、「クラウドとオンプレミス[*1]のいずれが有利と考えるか」を問うた。その結果、すべての項目で「クラウドが有利」と回答する企業の割合が「オンプレミスが有利」を上回るという結果になった(図1-31)。IT責任者の心理として、クラウドに対する不安はかなり払拭されつつあることが推察される。

＊1.オンプレミス:情報システムをユーザ企業自身が管理する設備内に導入・設置して運用する形態。

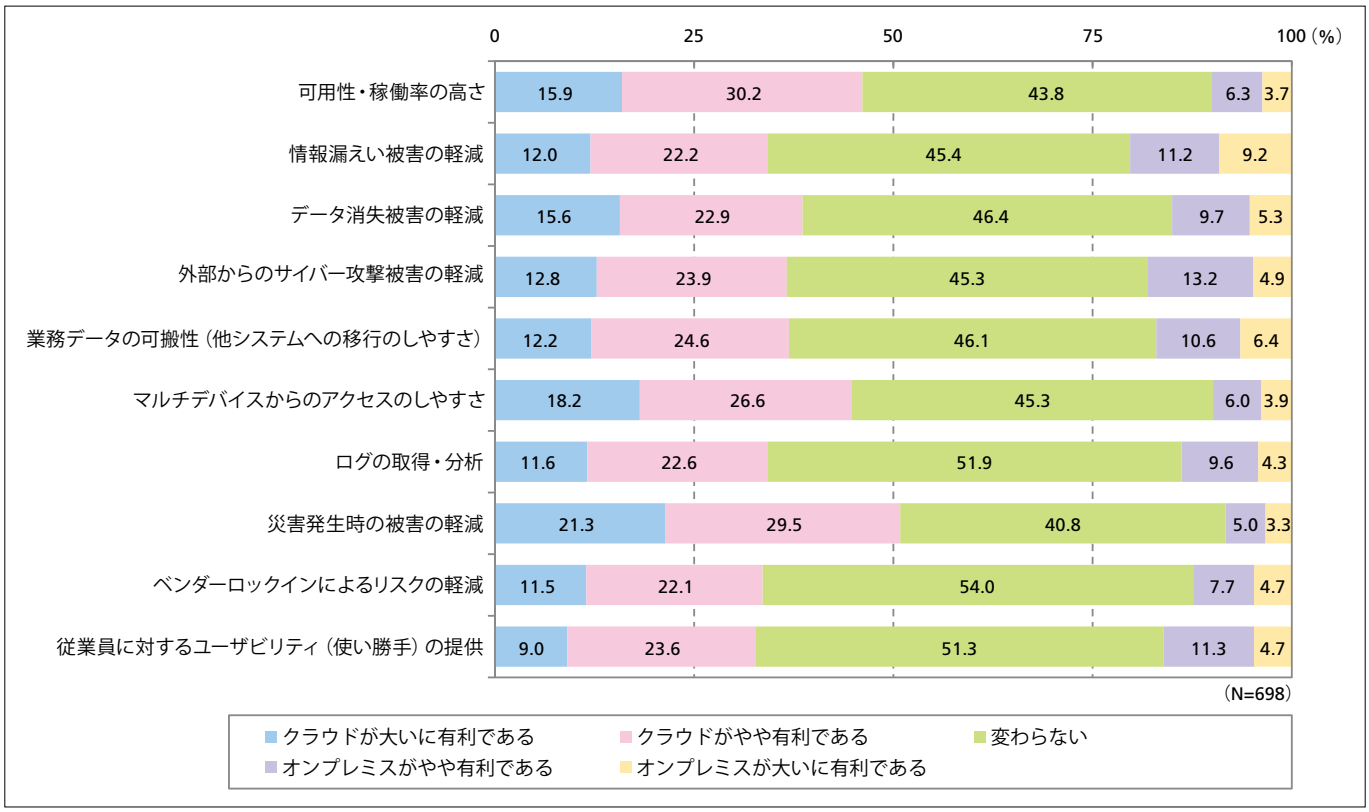


図1-31.「クラウド」と「オンプレミス」に対する認識

注目されるのは、セキュリティ関連のテーマについても「クラウドが有利である」と考える人が多数派を占めていることである。これは、業種による温度差が顕著であるという傾向も出ており、たとえば、「情報漏えい被害の軽減」の回答結果を業種別に見ると、「金融・保険」「情報通信」「製造」の3業種では回答結果が比較的拮抗しているものの、他の業種は圧倒的に「クラウドが有利である」と考える人が多いことがわかる（図1-32）。

システム構築の手法として、これまで主流の考え方であった「セキュリティを重視するならオンプレミス環境が望ましい」という考え方は、今後急速に力を失うことも考えられる。

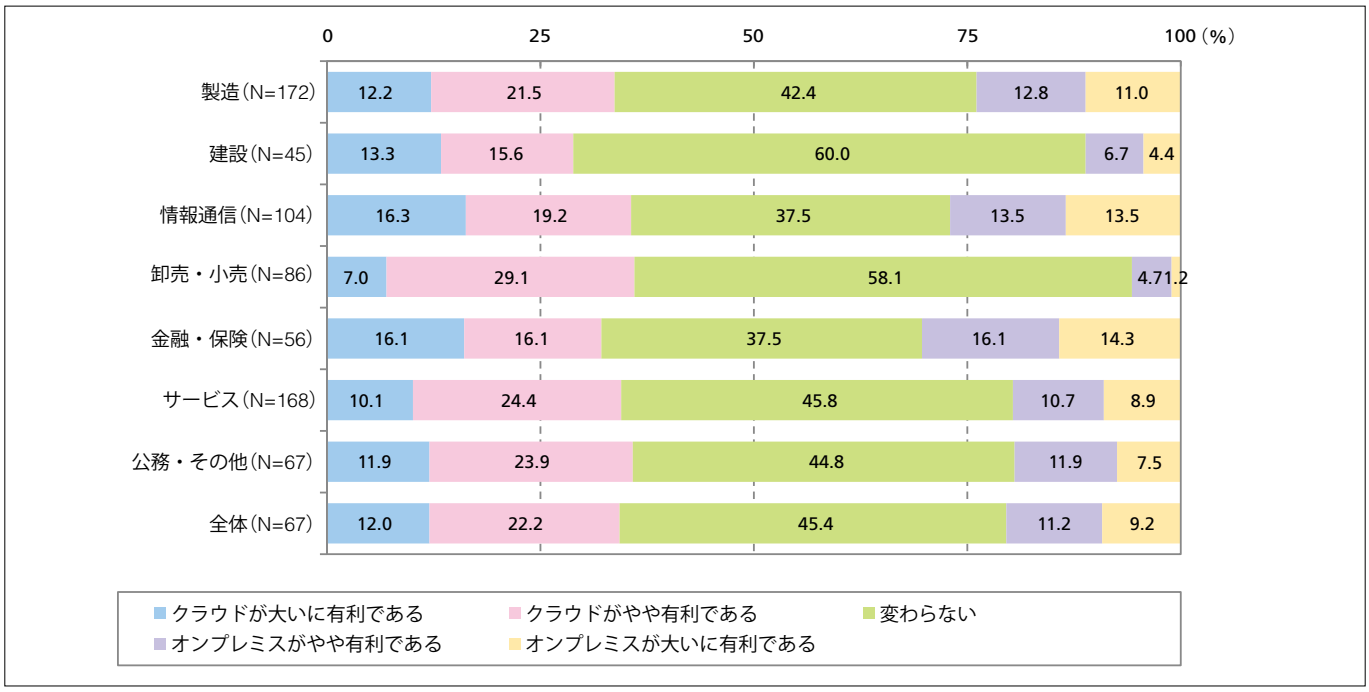


図1-32.「情報漏えい被害の軽減」に関するシステム環境への認識(業種別)

8 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4回目の実施となる。今回の調査では、セキュリティリスクに対する関心が、国内企業においてこれまで以上に高まっていることが確認された。重視する経営課題に関する設問でも、「情報セキュリティの強化」は全項目中2番目に高い重視度合いとなり、守りを固めようとする意識が顕著である。とりわけ内部不正によるセキュリティ被害に対する危機感は大きく、2014年に発覚した大規模情報漏えい事件の影響が色濃く反映されていると見られる。また、個人情報保護法の改正や社会保障・税番号(マイナンバー)制度の本格施行など、コンプライアンスに関わる課題も眼の前に迫っており、2015年度は「情報セキュリティ対策の組織的な見直し」がさまざまな企業を舞台に繰り広げられることが予想される。

しかしながらその一方で、組織的なセキュリティ体制の整備や情報の取り扱い方針の見直しといった肝心の具体策については、前年調査からほとんど進展しておらず、どこから手をつけてよいか判断のつかない企業が少なくないことが確認された。セキュリティ支出も引き続き増加傾向にはあるものの、その伸び幅は「アベノミクス効果」によって景気状況が大きく改善された前年と比べるとむしろ縮小している。情報セキュリティ責任者は、限られた経営資源をどのような対策に振り分けるか、これまで以上に厳正な判断が求められることであろう。

もう1つの不安要素は、2015年10月からスタートし、年明けから本格化すると見られる社会保障・税番号(マイナンバー)制度への対応である。今回の調査では、IT／セキュリティ担当者の主体的な関与が不十分であり、その影響を正しく把握できていない様子もうかがえた。

問題が発生してから対処する「後追い型のセキュリティ対策」の問題点はかねてから指摘されているが、モバイルやクラウドも含めてシステム環境の多様化が著しい今日において、そうした対処はもはや限界となっている。IT／セキュリティ担当者には、自社を取り巻くリスクの現状を改めて可視化・分析するとともに、計画性をもったセキュリティ対策のロードマップを描くことが強く求められる。

回答者プロフィール

業種	回答数	%
製造	172	24.6
建設	45	6.4
情報通信	104	14.9
卸売・小売	86	12.3
金融・保険	56	8.0
サービス	168	24.1
公務・その他	67	9.6
全体	698	100.0

年間売上高	回答数	%
5,000 億円以上	71	10.2
3,000 億～ 5,000 億円未満	42	6.0
1,000 億～ 3,000 億円未満	46	6.6
500 億～ 1,000 億円未満	57	8.2
100 億～ 500 億円未満	142	20.3
10 億～ 100 億円未満	217	31.1
1 億～ 10 億円未満	66	9.5
1,000 万円～ 1 億円未満	8	1.1
1,000 万円未満	3	0.4
売上げなし	46	6.6
全体	698	100.0

従業員規模	回答数	%
5,000 人以上	122	17.5
1,000 人～ 4,999 人	147	21.1
300 ～ 999 人	183	26.2
50 ～ 299 人	246	35.2
全体	698	100.0

業種別内訳

業種		回答数	%
製造	食料 : 飲料品	14	2.0
	繊維工業	7	1.0
	パルプ・紙・印刷	4	0.6
	化学工業	10	1.4
	石油製品	2	0.3
	鉄鋼・金属	14	2.0
	機械 / 電気機器	43	6.2
	情報通信機器	9	1.3
	電子部品・電子回路	16	2.3
	精密機器	10	1.4
	輸送機器	21	3.0
	医薬	4	0.6
	その他の製造業	18	2.6
建設		45	6.4
情報通信	通信	19	2.7
	(情報システム子会社以外の)情報処理サービス	55	7.9
	メディア・出版・放送・広告代理店	4	0.6
	情報システム子会社 (外販率 50% 以上)	14	2.0
	情報システム子会社 (外販率 50% 未満)	12	1.7
卸売・商社	卸売	34	4.9
	小売	26	3.7
	商社	26	3.7
金融・保険	銀行	26	3.7
	証券	9	1.3
	保険	15	2.1
	その他金融 (リースなど)	6	0.9
サービス	電力・ガス	8	1.1
	運輸・倉庫	30	4.3
	不動産	10	1.4
	教育	14	2.0
	医療・福祉	41	5.9
	宿泊・飲食	10	1.4
	娯楽・広告	7	1.0
	その他のサービス	48	6.9
公務・その他	官公庁	15	2.1
	地方自治・公共団体	38	5.4
	その他の公務	2	0.3
	農林・水産・鉱業	2	0.3
	その他の業種	10	1.4
全体		698	100.0