【特集】「企業IT利活用動向調査2016」にみるIT化の現状

JIPDECは、調査会社株式会社アイ・ティ・アール（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なか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2014年以降の調査結果を比較・分析して紹介する。

1 調査概要

1-1. 調査概要

・実査期間：2016年1月22日～1月27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：672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（26.8%）、次いでサービス業（24.6%）、情報通信（13.8%）、卸売・小売業（10.4%）となった。所属部門では情報システム部門が最も多く（48.2%）、役職は部長（33.8%）、課長（30.5%）、係長・主任（18.6%）の順となっている。

IT戦略／情報セキュリティへの関与度合いを見ると、情報システム部門に所属する回答者が多いことも関係しているためか、「セキュリティ製品の導入、製品選定に関与している」（58.2%）、「全社的なリスク管理／コンプライアンス／セキュリティ管理に責任を持っている」（54.9%）が半数以上を占めた。

2 経営における情報セキュリティの位置づけ

本調査は、国内企業の間で重要テーマとして定着しつつある「情報セキュリティ」をメインテーマとしているが、経営課題のなか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27項目の経営課題について、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」（55.5%）が4年連続で首位となり、次いで「社内コミュニケーションの強化」（36.5%）「情報セキュリティの強化」（36.0%）「社内体制・組織の再構築」（33.0%）があげられた。「情報セキュリティの強化」については前年調査の2位から3位に後退したが、情報セキュリティ対策が経営課題として重視されている傾向に変化はない。

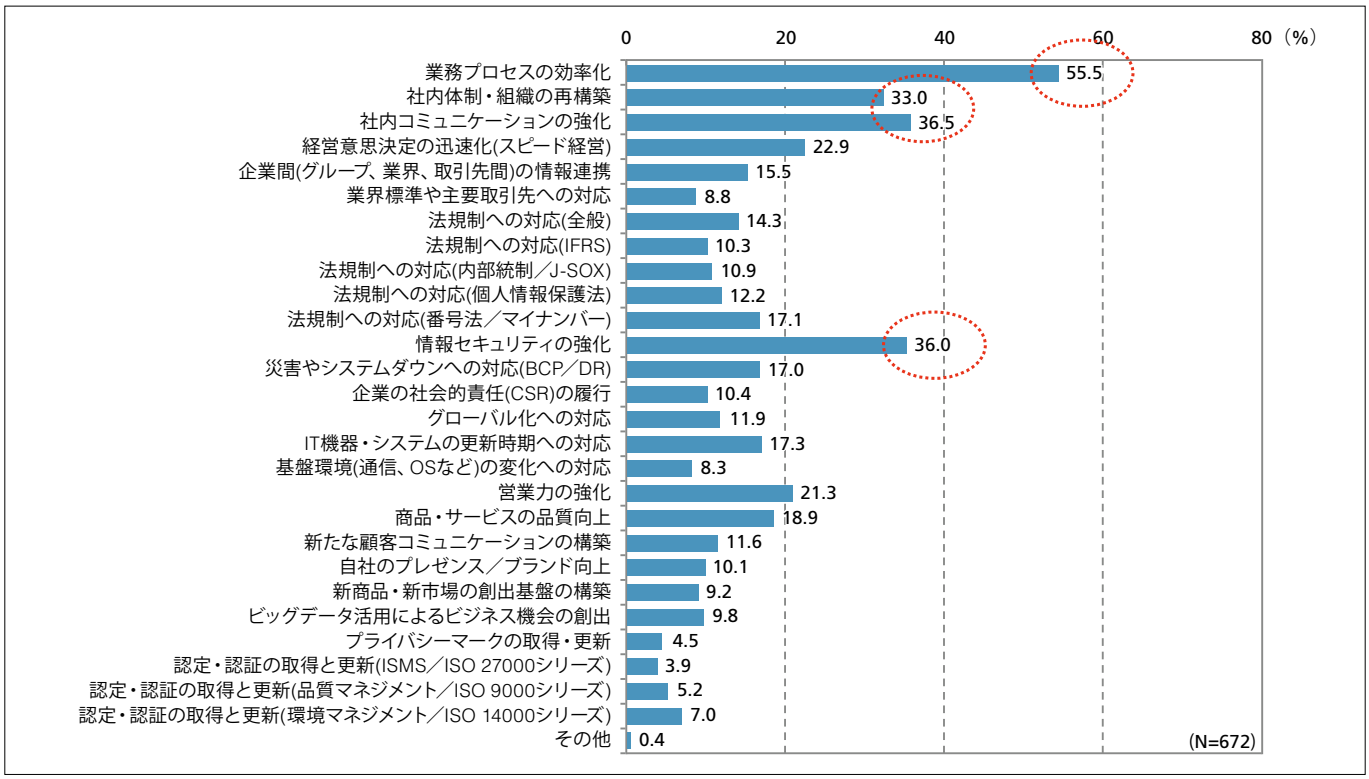


図1-1. 今後重視したい経営課題（複数回答）

ちなみに、上位10項目の課題について、過去3回の回答率の変化を見ると、「業務プロセスの効率化」は一貫して首位であるが、上位項目の回答率は全体的に低下しており、ITによって実現すべき課題が分散化していることがうかがえる（図1-2）。

前年調査で高く伸びた「情報セキュリティの強化」は依然重要課題でありながら回答率が下がる一方で、「マイナンバー制度対応」の回答率が前年の約２倍に伸び上位10項目に入り、この課題に対する国内企業の関心の高さが表れている。

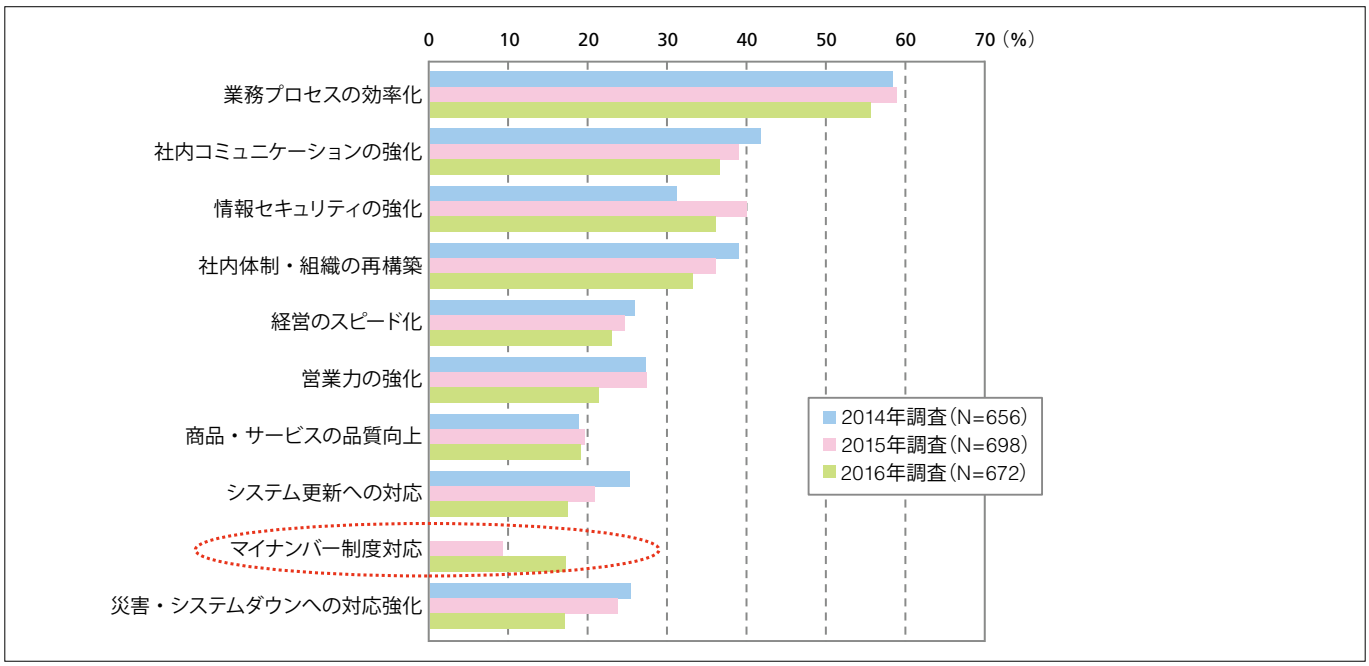


図1-2. 主要経営課題に対する回答率の経年比較（2014～2016年）

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について、認知率が最も高かったのは「従業員によるデータ、情報機器の紛失・盗難」（23.1%）であった。調査開始以来、初めて単独の最上位項目となった。「モバイル用PC」や「スマートフォン、携帯電話、タブレットの紛失・盗難」もそれぞれ約17%の組織で認知されており、モバイル環境下での業務の拡大が、インシデントの発生に影響を及ぼしている現実が改めて浮き彫りとなった（図1-3）。

また、「個人情報の漏えい・逸失」については、人為ミスによる事案が前年調査（12.6%）から若干低下して11.9%となったものの、内部不正による事案は、逆に前年（5.2%）から1.5ポイント上昇して6.7%となった。

個人情報の保護については企業でさまざまな対策が講じられているが、内部不正や人為ミスによるインシデントを少しでも減らすために、社員だけでなく委託先も含めた情報管理の徹底が改めて求められていると言える。

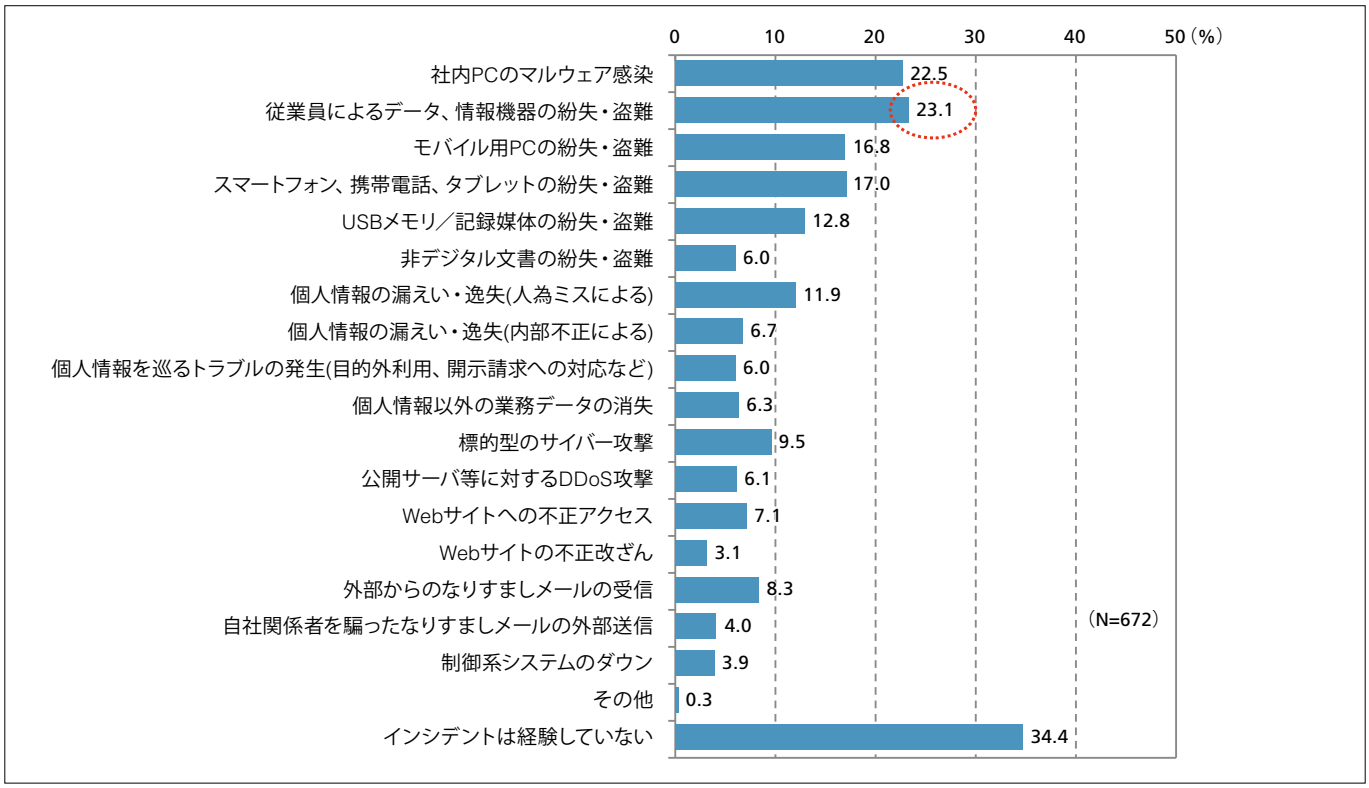


図1-3. 過去1年間に経験したセキュリティインシデント（複数回答）

過去の調査結果との比較で認知率の増加が顕著なのが、外部からのサイバー攻撃に関わるインシデントである。今回の調査では、「外部からのなりすましメールの受信」が8.3%と前年の5.4%から約3ポイント上昇、「標的型のサイバー攻撃」を経験したとする企業の割合が前年から約2ポイント近く上昇した（図1-4）。特に差出人を偽って送信されるなりすましメールは標的型攻撃の初期段階で用いられることが多く、関係者を装って受信者に添付ファイルを開かせ、重要情報を窃取するためのマルウェアを仕込むといった手口に用いられる。電子メールで重要情報を頻繁にやり取りする必要があるような企業・組織においては、その安全性確保に最大限の注意を払う必要がある。

なお、業種別に見ると「金融・保険」および「公共・その他団体」が、また従業員数別に見ると、従業員数が「5,000人以上」の企業での外部攻撃によるインシデントの発生割合が高いことがわかる。（図1-5、図1-6）。

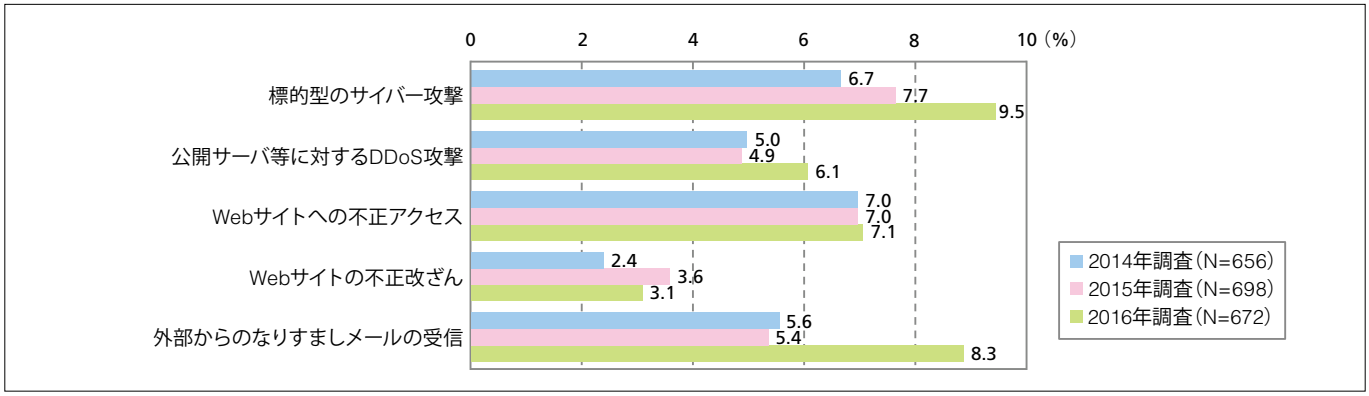
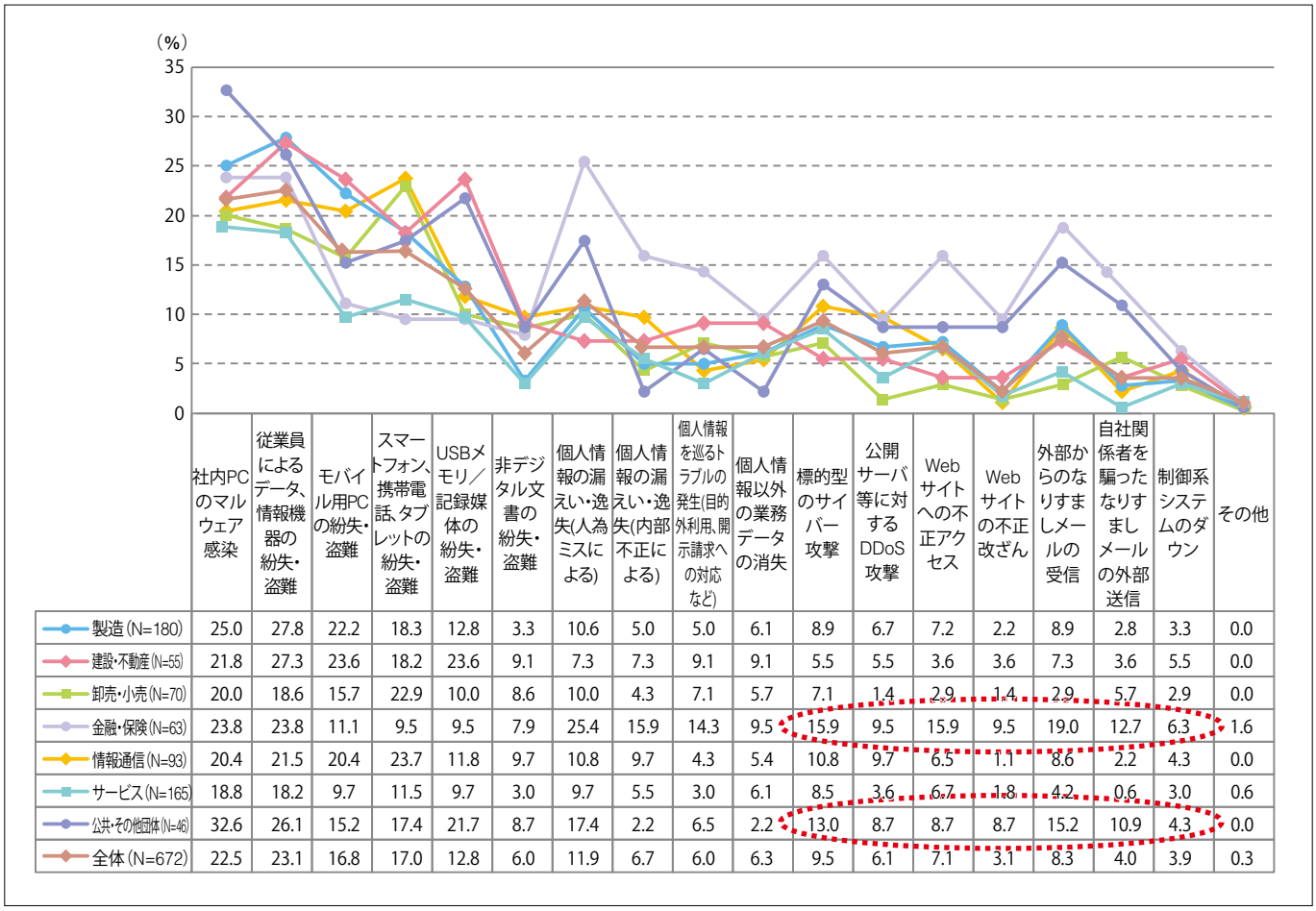
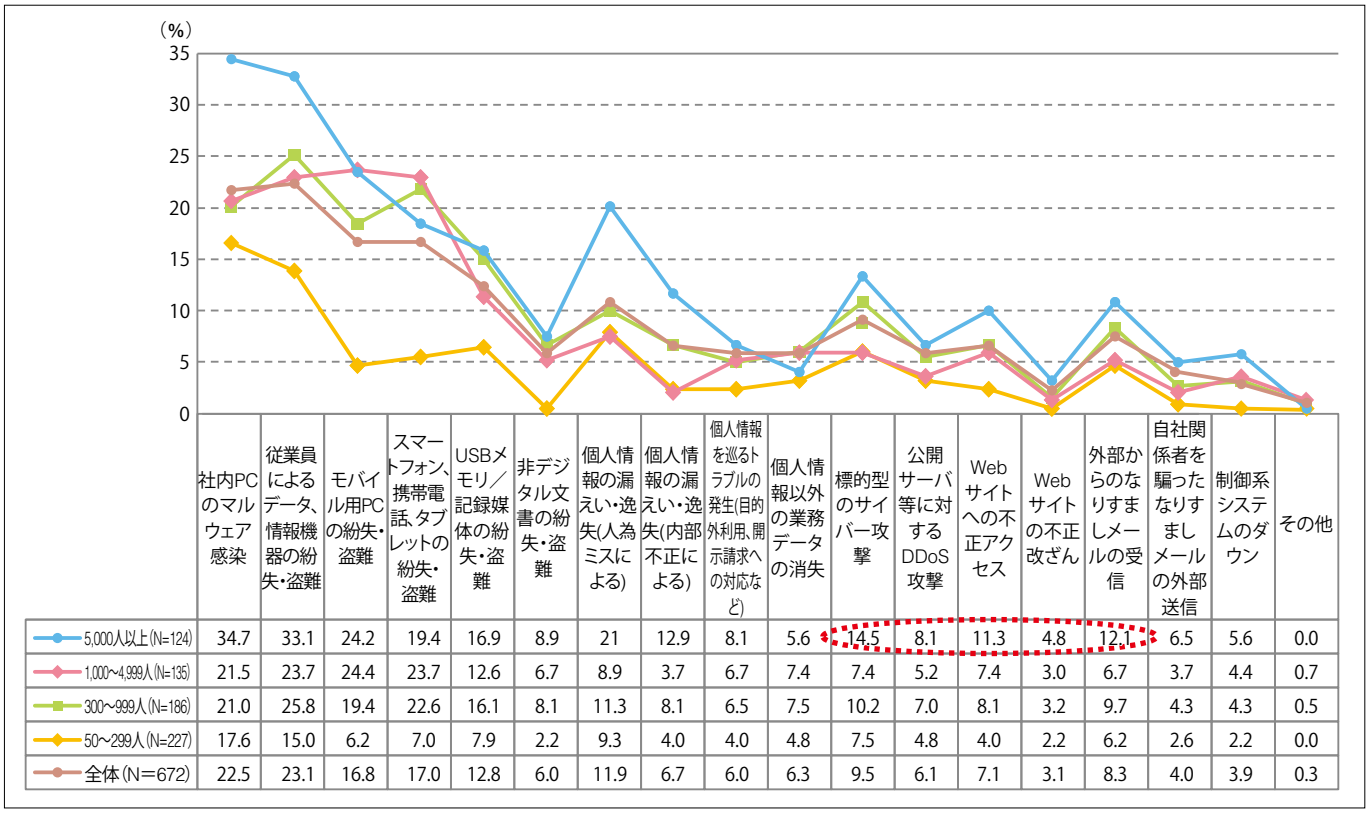


図1-4. サイバー攻撃に関わるセキュリティインシデントの経年比較(2014～2016年調査)



	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)	個人情報を巡るトラブルの発生(目的外利用、開示請求への対応など)	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	外部からのなりすましメールの受信	自社関係者を騙ったなりすましメールの外部送信	制御系システムのダウン	その他
製造(N=180)	25.0	27.8	22.2	18.3	12.8	3.3	10.6	5.0	5.0	6.1	8.9	6.7	7.2	2.2	8.9	2.8	3.3	0.0
建設・不動産(N=55)	21.8	27.3	23.6	18.2	23.6	9.1	7.3	7.3	9.1	9.1	5.5	5.5	3.6	3.6	7.3	3.6	5.5	0.0
卸売・小売(N=70)	20.0	18.6	15.7	22.9	10.0	8.6	10.0	4.3	7.1	5.7	7.1	1.4	2.9	1.4	2.9	5.7	2.9	0.0
金融・保険(N=63)	23.8	23.8	11.1	9.5	9.5	7.9	25.4	15.9	14.3	9.5	15.9	9.5	15.9	9.5	19.0	12.7	6.3	1.6
情報通信(N=93)	20.4	21.5	20.4	23.7	11.8	9.7	10.8	9.7	4.3	5.4	10.8	9.7	6.5	1.1	8.6	2.2	4.3	0.0
サービス(N=165)	18.8	18.2	9.7	11.5	9.7	3.0	9.7	5.5	3.0	6.1	8.5	3.6	6.7	1.8	4.2	0.6	3.0	0.6
公共・その他団体(N=46)	32.6	26.1	15.2	17.4	21.7	8.7	17.4	2.2	6.5	2.2	13.0	8.7	8.7	8.7	15.2	10.9	4.3	0.0
全体(N=672)	22.5	23.1	16.8	17.0	12.8	6.0	11.9	6.7	6.0	6.3	9.5	6.1	7.1	3.1	8.3	4.0	3.9	0.3

図1-5. 業種別に見た過去１年間のセキュリティインシデント



	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)	個人情報を巡るトラブルの発生(目的外利用、開示請求への対応など)	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	外部からのなりすましメールの受信	自社関係者を騙ったなりすましメールの外部送信	制御系システムのダウン	その他
5,000人以上(N=124)	34.7	33.1	24.2	19.4	16.9	8.9	21	12.9	8.1	5.6	14.5	8.1	11.3	4.8	12.1	6.5	5.6	0.0
1,000～4,999人(N=135)	21.5	23.7	24.4	23.7	12.6	6.7	8.9	3.7	6.7	7.4	7.4	5.2	7.4	3.0	6.7	3.7	4.4	0.7
300～999人(N=186)	21.0	25.8	19.4	22.6	16.1	8.1	11.3	8.1	6.5	7.5	10.2	7.0	8.1	3.2	9.7	4.3	4.3	0.5
50～299人(N=227)	17.6	15.0	6.2	7.0	7.9	2.2	9.3	4.0	4.0	4.8	7.5	4.8	4.0	2.2	6.2	2.6	2.2	0.0
全体(N=672)	22.5	23.1	16.8	17.0	12.8	6.0	11.9	6.7	6.0	6.3	9.5	6.1	7.1	3.1	8.3	4.0	3.9	0.3

図1-6. 従業員数別に見た過去１年間のセキュリティインシデント

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

サイバー攻撃にまつわるインシデントの増加は、企業におけるリスクの重視度合いにも影響を及ぼしている。本調査では、「標的型のサイバー攻撃」および「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を毎年調査しているが、今回の調査では「経営陣から最優先で対応するよう求められている」とした回答が23.7%で同率となった。前年調査では「内部犯行」に対するリスクの重視度合いの方が明確に高かった（25.4%）が、今回の調査では、「サイバー攻撃」に対する危機感が高まっていることが見てとれる。

事実、「標的型攻撃」に対するリスクの重視度は、近年、年を経るごとに上昇しており、「経営陣からも最優先で対応するよう求められている」とする企業の割合も、2014年調査の18.9%から徐々に増加している（図1-7、1-8）。

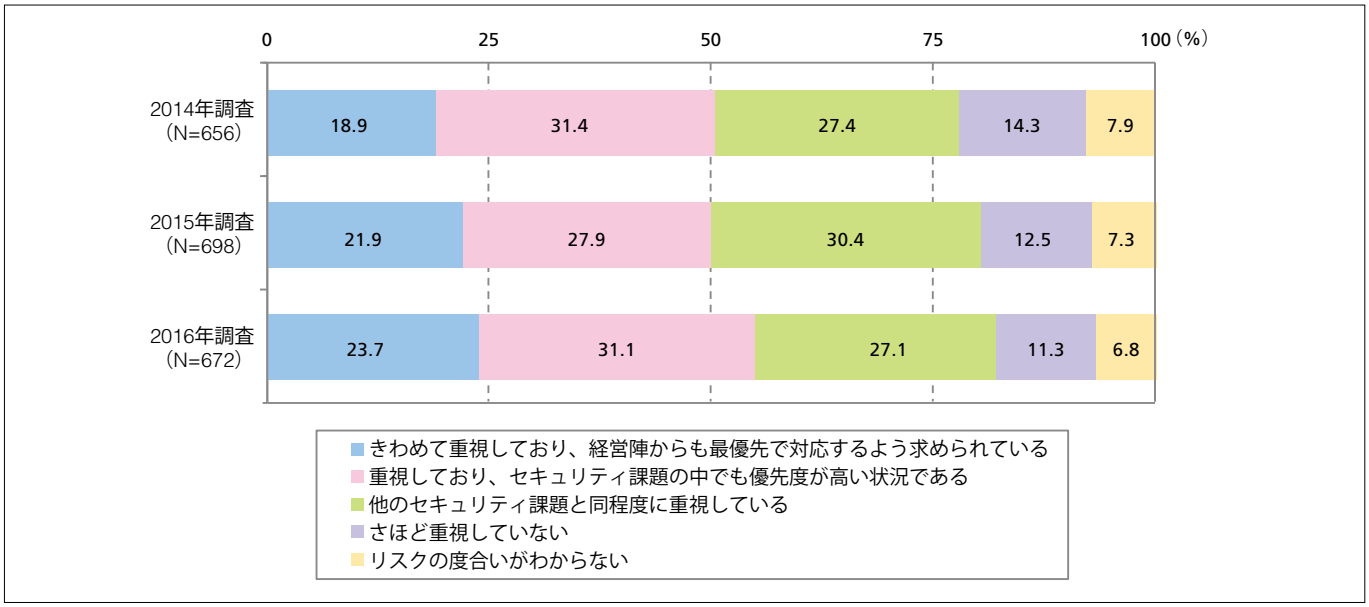


図1-7.「標的型のサイバー攻撃」に対するリスクの重視度合いの経年比較（2014～2016年）

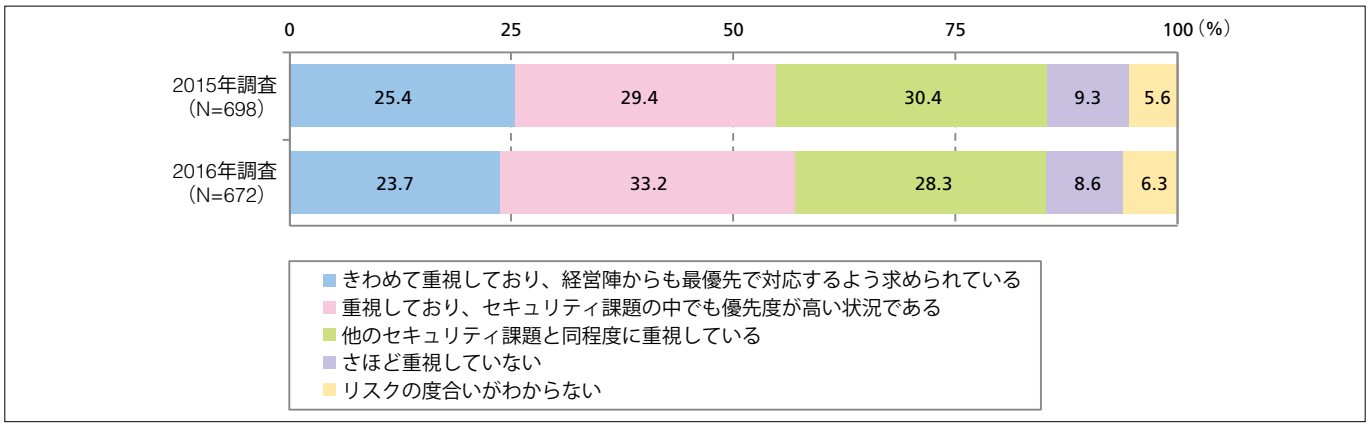


図1-8.「内部犯行による重要情報の漏えい・消失」に対するリスクの重視度合いの経年比較（2014～2016年）

ちなみに、標的型サイバー攻撃対策の実施状況について問うた結果、「実施済み」とした割合が最も高かったのは「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、「重要システムのインターネットからの隔離」とともに実施率が5割を超えた。また、「1年以内に実施予定」とした割合が最も高かったのは、「ネットワークトラフィックデータの保存と分析」と「標的型攻撃対策製品（ネットワーク型）の利用」であった（図1-9）。今後は、巧妙化する攻撃に備えて技術的な対策を強化する企業が増加する可能性も考えられる。

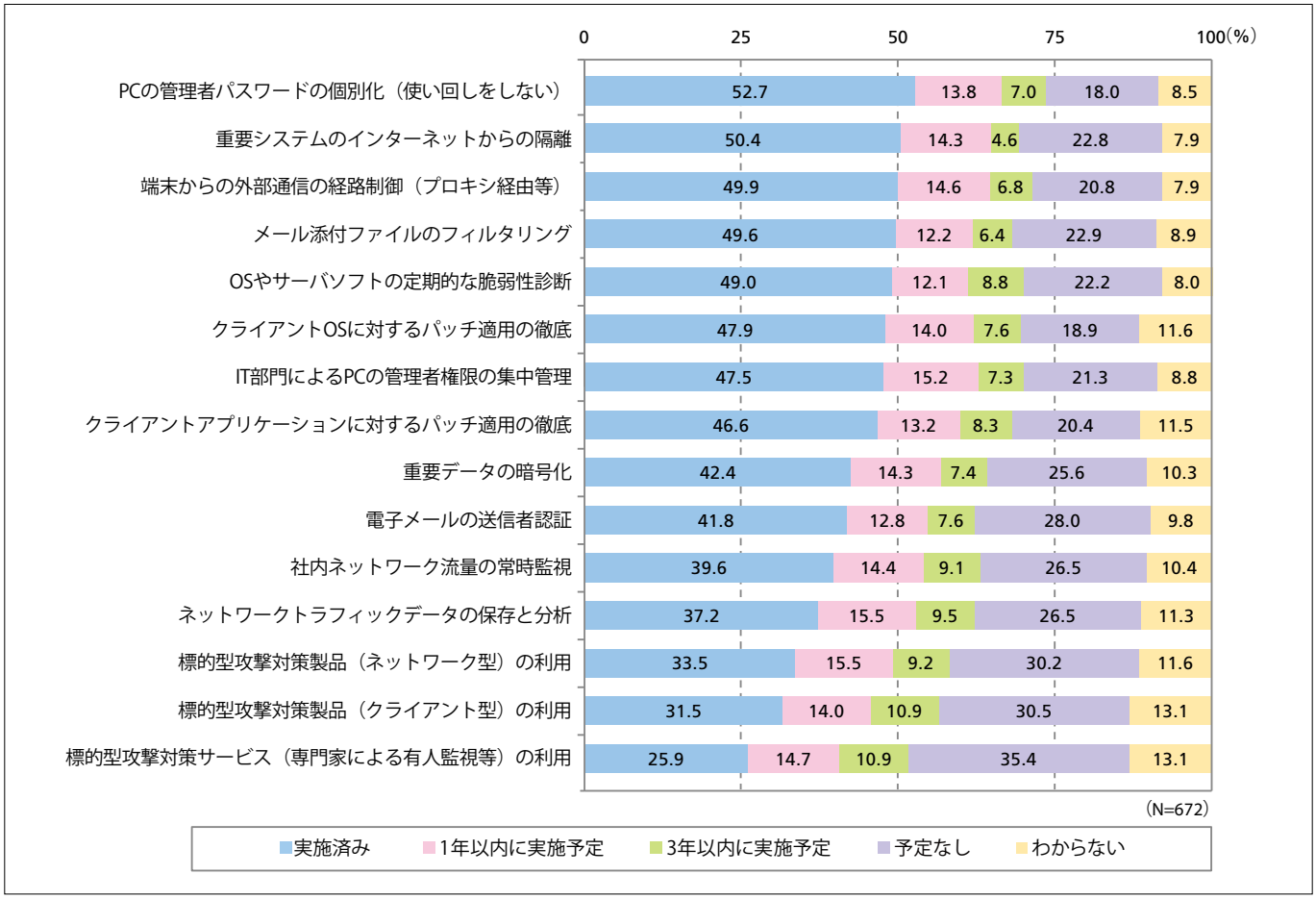


図1-9. 標的型サイバー攻撃対策の実施状況

内部犯行対策については「重要情報の取扱い」に関連した対策が総じて実施率が高く、他には「PCの社外持出しの禁止」「外部デバイスへのデータ移動の制限」「一般社員向けの教育・研修の実施」「退職者に対するアクセス権の早期無効化」を実施している企業が多いことがわかる（図1-10）。

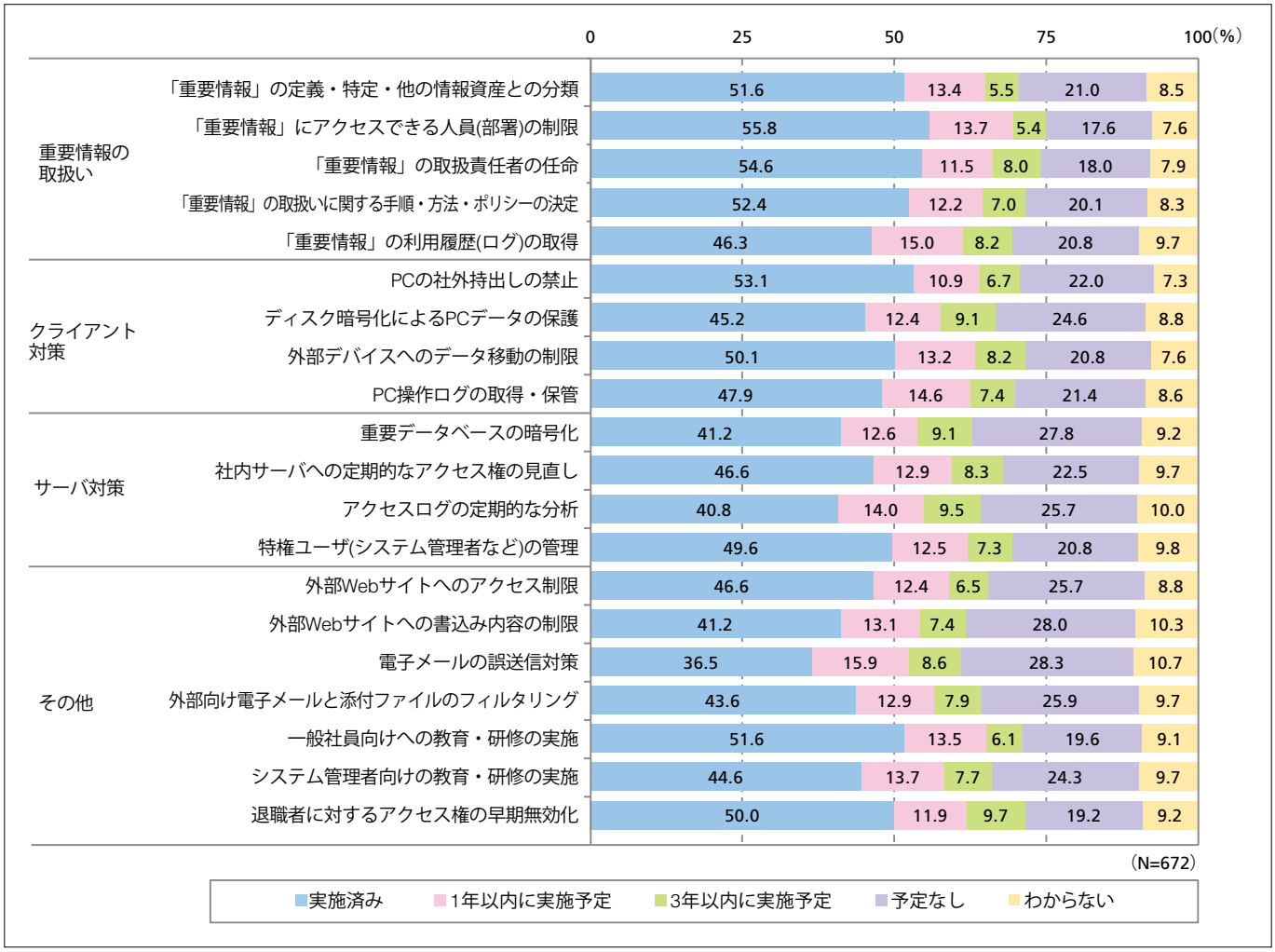


図1-10. 内部犯行対策の実施状況

3 情報セキュリティに関する認定／認証制度の動向

情報セキュリティへの組織的な対応力を強化するための方策として、第三者による認定／認証制度は国内でも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毎年調査している。本章では、その最新動向について紹介する。

3-1. 認定／認証制度等の取得状況

国内において取得可能な10種の認定／認証制度等を取り上げ、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ところ、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1-11）。この2項目は「取得済み」とする割合も高く、前者は約24%、後者は約20%に上っている。

なお、認定／認証制度等に関わる設問では、制度に対する正しい理解を持っていると考えられる517件を有効回答として取り扱っている。

「今後取得する予定」の割合が最も高いのは、「CSMS適合性評価制度」（16.1%）であった。これは、産業用オートメーションおよび制御システムをサイバー攻撃から守るためのセキュリティ対策の強化を目的とした認定／認証制度であるが、制度開始から日が浅いこともあって、本調査の回答企業では取得済みの企業は存在しないが、今後に向けて関心が高まっていることが見てとれる。

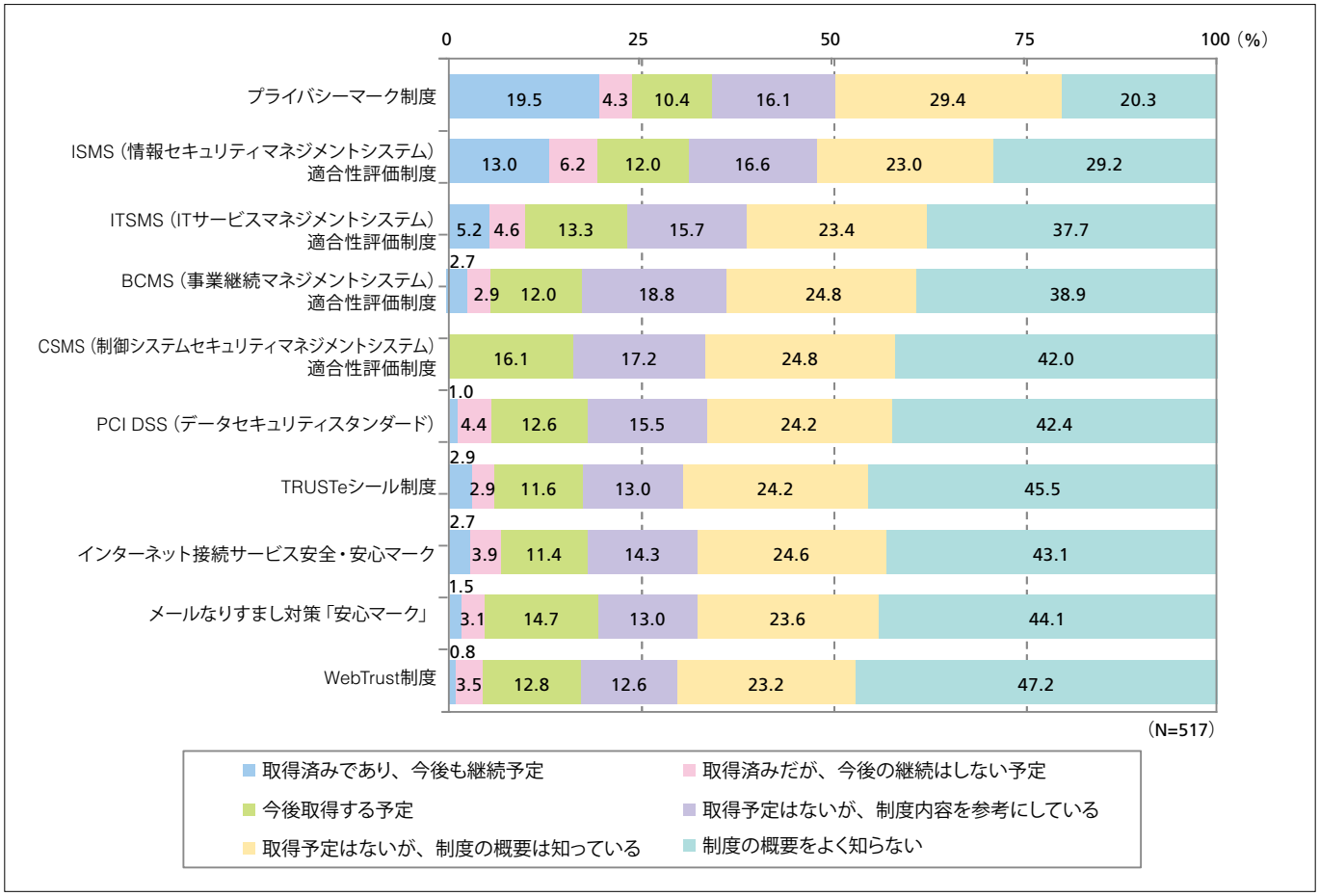


図1-11. 情報セキュリティに関わる認定／認証制度等の取組み状況

また、取得率、認知率ともに最多であった「プライバシーマーク制度」への取組み状況を業種別に見ると、「情報通信業」での取得率が圧倒的に高く（図1-12）、ISMS適合性評価制度についても同様の傾向が見られた。

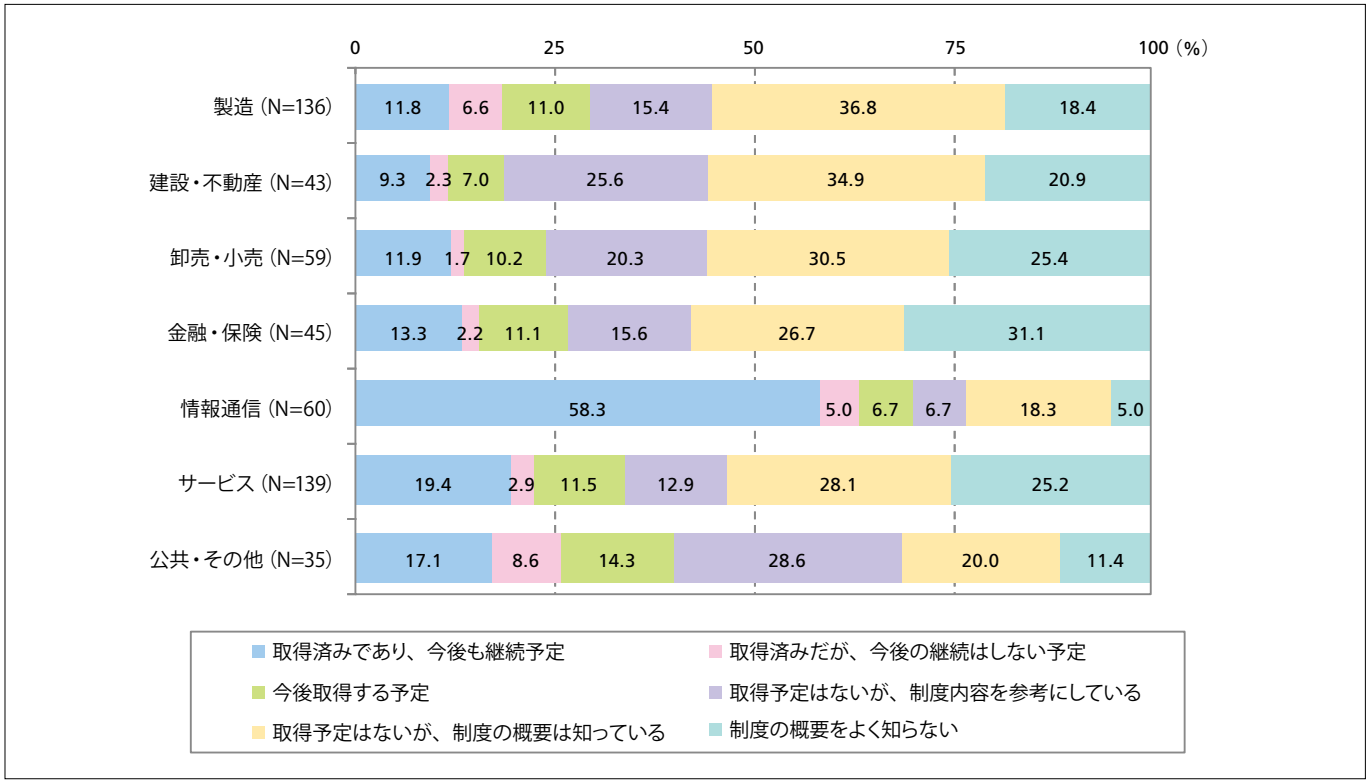


図1-12.「プライバシーマーク制度」に対する取組み状況（業種別）

3-2. 認定／認証制度の価値

国内企業は認定／認証制度全般に対してどのような価値を見いだしているのであろうか。ここでは、有効回答をプライバシーマーク制度またはISMS適合性評価制度の認定／認証を取得している企業（159社）と、取得していない企業（358社）とに分けて回答結果を集計した。当然ながら、取得企業の方が価値を認識する度合いも大きいが、なかでも「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」が最多となり、50%を超えた（図1-13）。認定／認証制度の活用が、ビジネスに必要な信用を得る手段として機能していることがうかがえる。

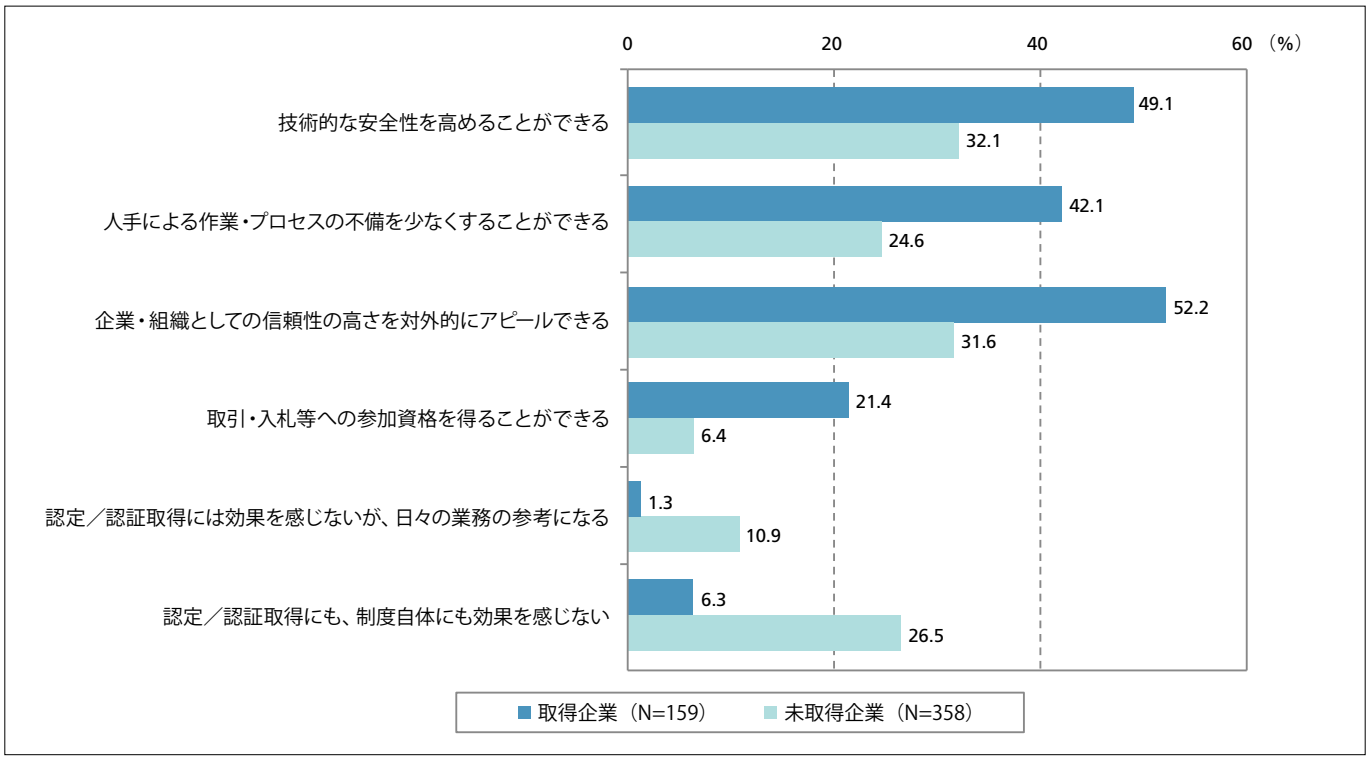


図1-13. 認定／認証を取得することの価値

次に、前年調査に引き続き認定／認証の取得につながりやすいと考えられる「システムリスクの対応策」の実施状況を問うたところ、「事業継続計画（BCP）の策定」「全社的なリスクマネジメントの構築」「ITIL等のベストプラクティスを活用したITサービスマネジメントの実施」の3項目とも、実施率が前年より5ポイント強増加し、進展していることが明らかとなった。また、実施済み企業のうちの約半数は、「変更中またはその予定がある」としており、前年同様、対策の見直しを進める企業が少なくないことも示された（図1-14）。

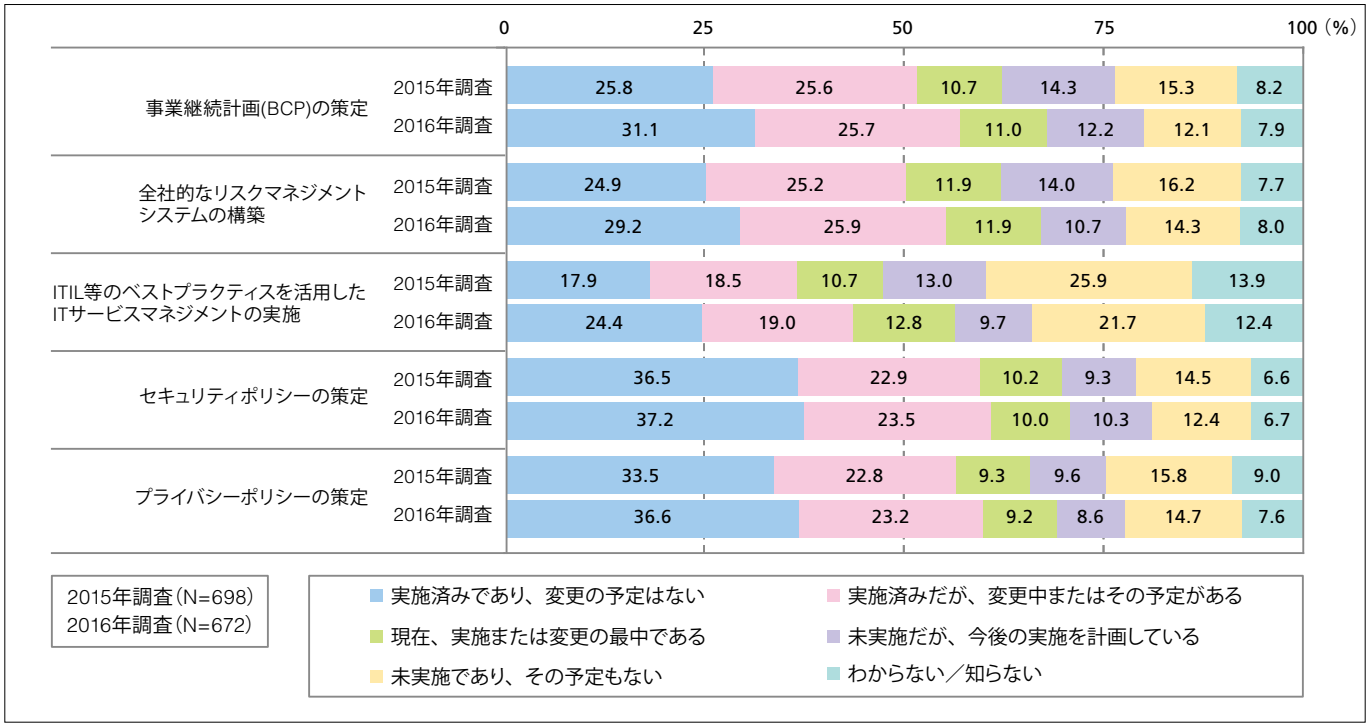


図1-14. 全社的なシステムリスクの対応策の取組み状況

3-3. ISMS適合性評価制度の取得に関わる重視項目とその効果

また、今回の調査では、プライバシーマーク制度に次いで取得率の高いISMS適合性評価制度について、「取得時に重視した（重視する）ポイント」と、「取得後に実感した効果」をそれぞれ問うた。調査対象は、前者はISMSを取得済みもしくは取得予定の企業（161社）、後者は取得済み企業（99社）である。

回答結果を基に、「重要度指数」と「効果指数」を算出[*1]し、その値を表したのが図1-15である。その結果、情報の保護に関わる項目が、重要度が高く、かつ効果の実感度合いも高いという結果になった。

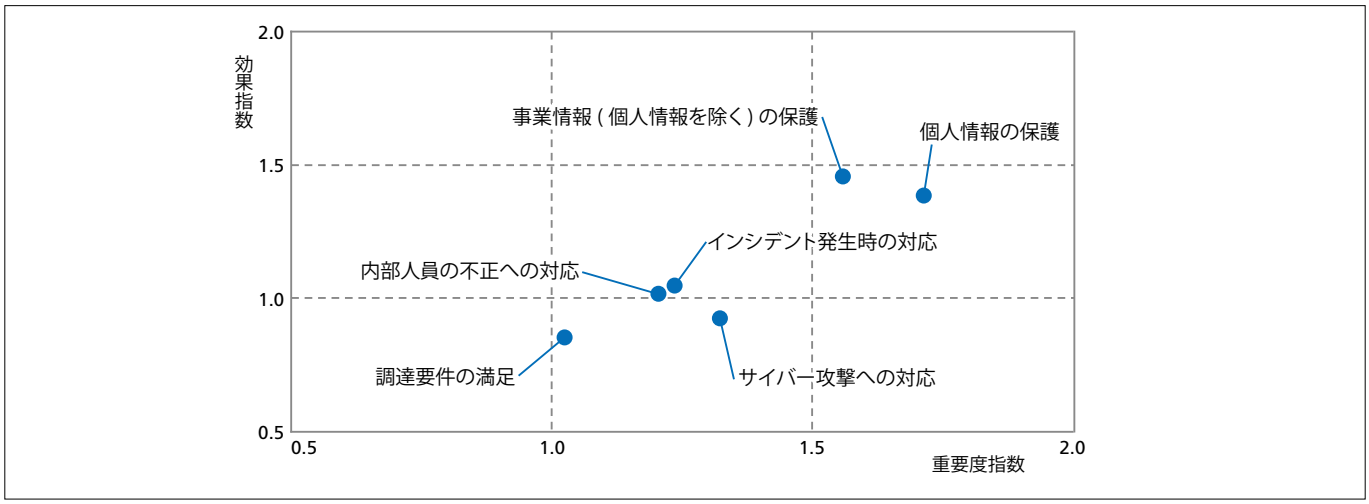


図1-15. ISMS適合性評価制度の重要度と効果

＊1. 重要度指数は、「特に強く意識した（3点）」「どちらかと言えば意識した（1点）」「どちらとも言えない（0点）」「あまり意識しなかった（－1点）」「まったく意識しなかった（－3点）」の加重平均。効果指数は「非常に効果があった（3点）」「少し効果があった（1点）」「どちらとも言えない（0点）」「あまり効果はなかった（－1点）」「まったく効果がなかった（－3点）」の加重平均。

4 セキュリティ支出と組織的な対策の動向

本調査では、例年同様セキュリティ支出の動向も調査対象としている。本章では、組織的なセキュリティ対策の実施状況と併せて紹介する。

4-1. 製品以外にも伸びが見込まれるセキュリティ支出

本調査では、前年同様、主要なセキュリティ支出の内訳として15項目を取り上げ、それぞれについて2016年度の支出の増減見込み（対前年度比）を問うた（図1-16）。

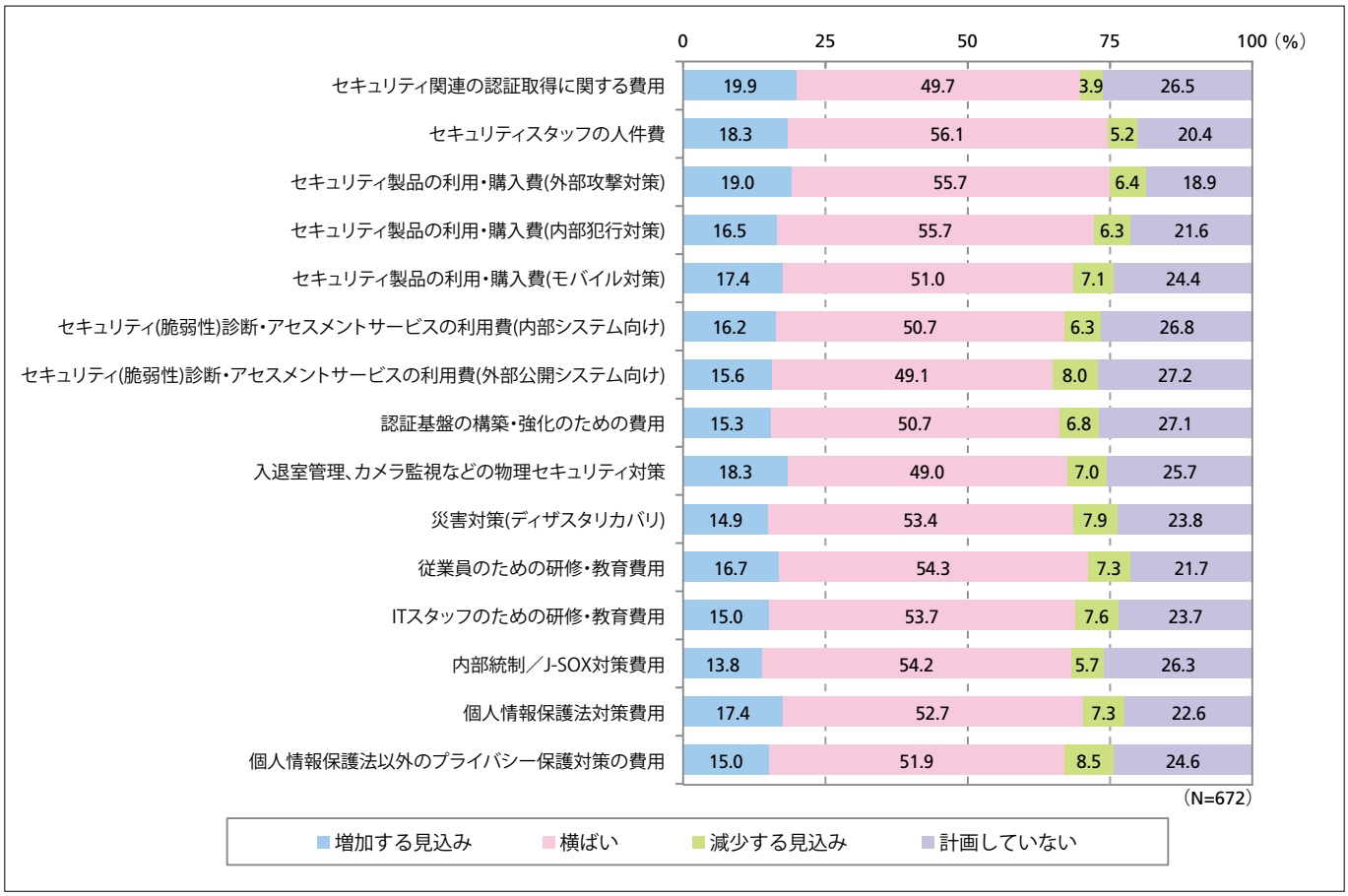


図1-16. 2016年度に想定されるセキュリティ支出の増減傾向

「増加する見込み」の回答は、いずれも約14～20%と近似値であり、セキュリティ対策をあらゆる方面から行いたい企業の意向がうかがえる。そのなかでも、増加を見込む企業の割合が最多となったのは「セキュリティ関連の認証取得に関する費用」（19.9%）であった。次いで「セキュリティ製品の利用・購入費（外部攻撃対策）」（19.0%）、「セキュリティスタッフの人件費」「入退室管理、カメラ監視などの物理セキュリティ対策」が同率（18.3%）で並んだ。2014年、2015年の調査では製品・サービスに対する支出が先行していたが、ここにきてプロセスや組織、人材といったそれ以外の領域にも着目する動きが明らかになった。

また、回答結果を指数化（増加を3、横ばいを2、減少を1とした加重平均）し、その結果を過去2回の結果と比較したところ、2016年度は「個人情報保護法対策費用」「内部統制／J-SOX対策費用」といった、コンプライアンスに関わる支出が過去2年よりも明らかに上向いていることが確認された（図1-17）。これは、改正個人情報保護法やマイナンバー制度の影響も反映されていると見ることができる。

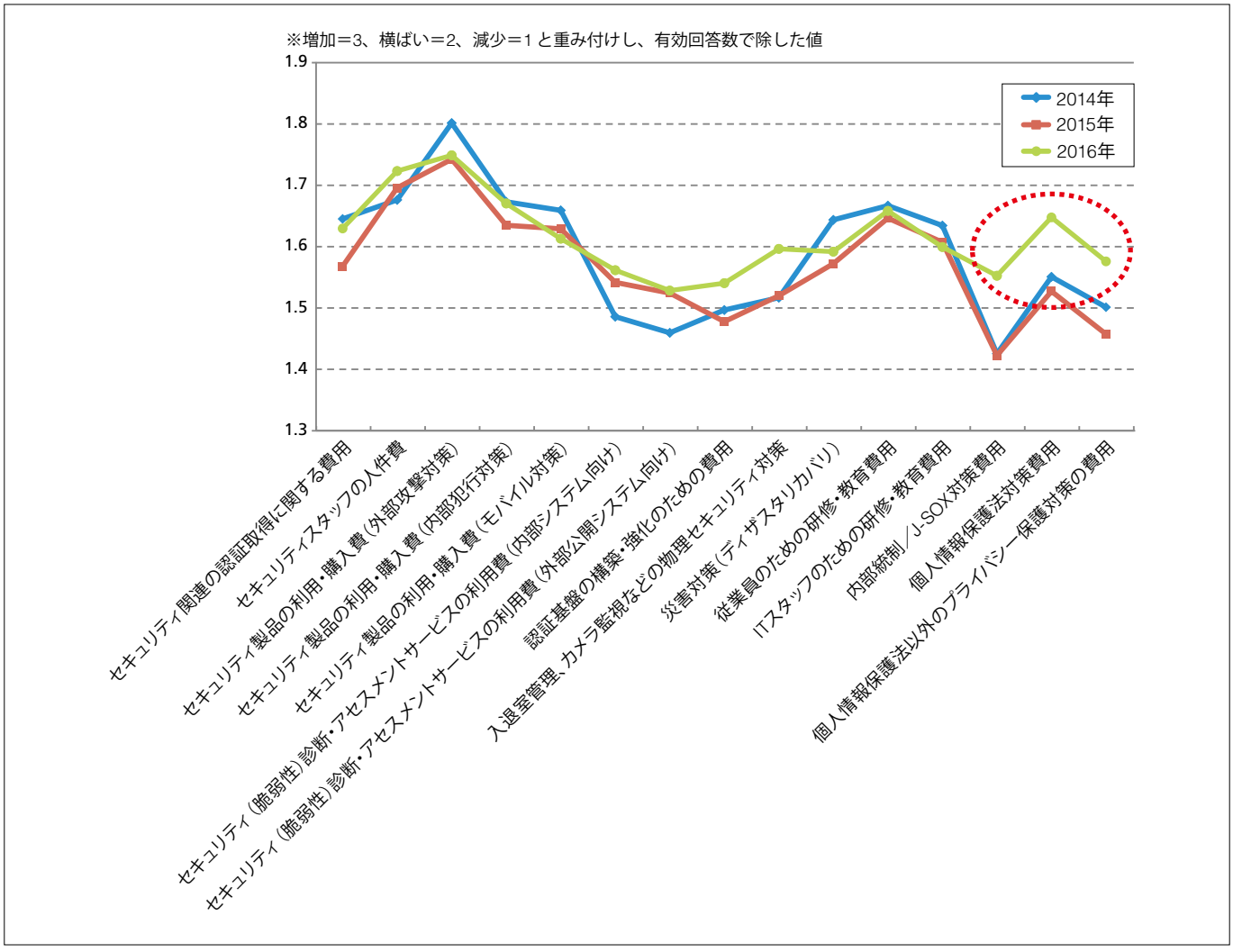


図1-17. セキュリティ支出の増減傾向の経年比較（2014～2016年調査）

4-2. 組織体制の整備は引き続き足踏み状態に

一方、過去の調査結果に引き続き、足踏み状態にあ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毎年調査しているが、今回の調査でも、図1-18にあるように多くの項目が2014年、2015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。

「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、実態がそれに追いついていない状態が続いていると考えられる。

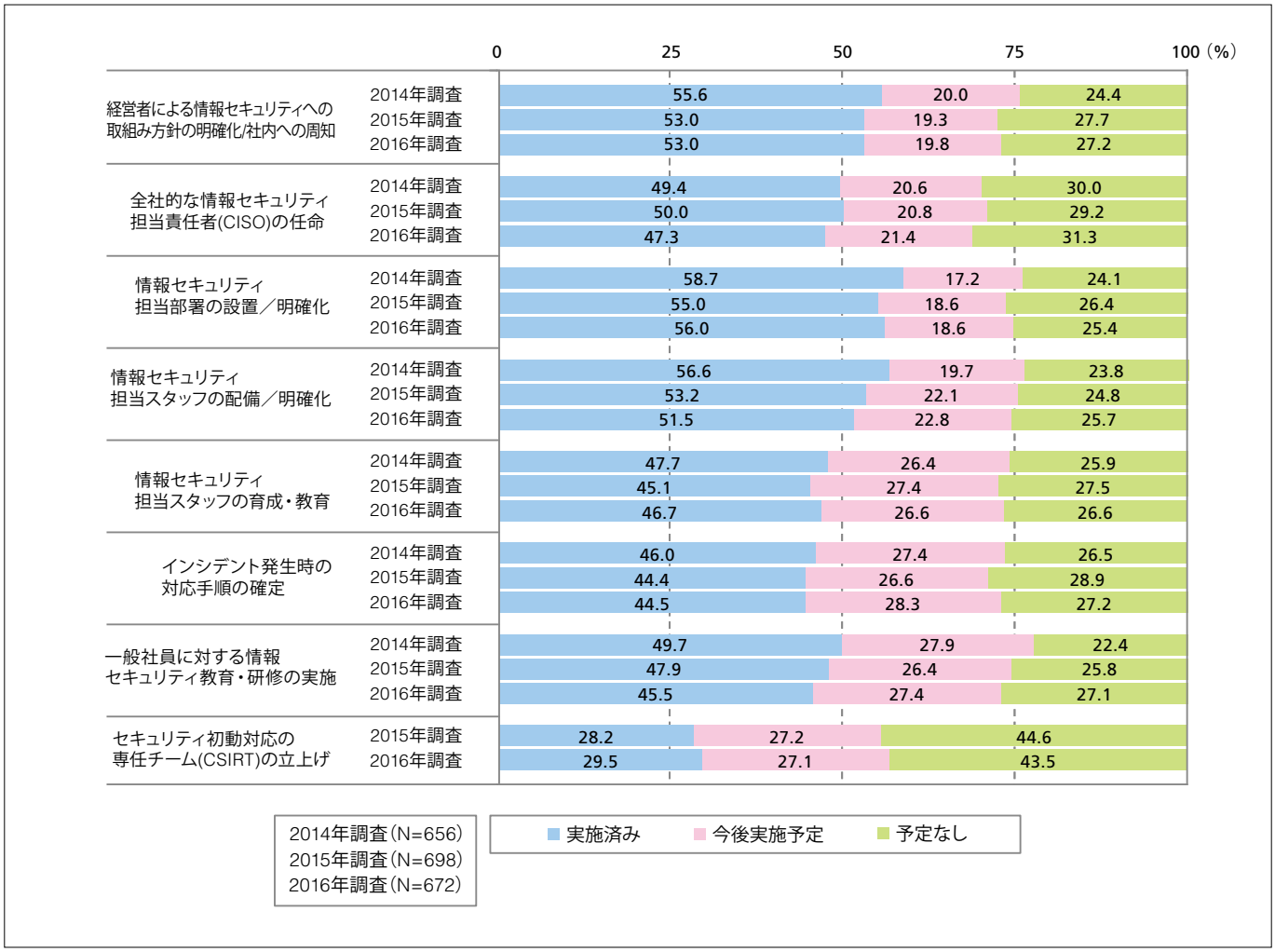


図1-18. 情報セキュリティ対策の実施状況の経年比較（2014～2016年調査）

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。今回の調査では、2015年9月に可決・成立した改正個人情報保護法、2016年1月から本格的な運用がスタートしたマイナンバー制度について意識調査を行った。

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、約10年ぶりに改正された個人情報保護法は、個人情報の定義の明確化や範囲の拡大、第三者機関である個人情報保護委員会の新設など、個人情報の取扱いが厳格化される一方で、氏名、住所などの一部情報を削除する “匿名化” を条件に、個人情報のビジネス活用にも道を開く内容となった。

そこで、本調査では個人情報保護法の改正が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」と回答したが、その割合は前年調査から若干減少した。その一方で、「プライバシーポリシーの変更・修正のみで対応できると思う」とした回答者が約5ポイント増加した（図1-19）。

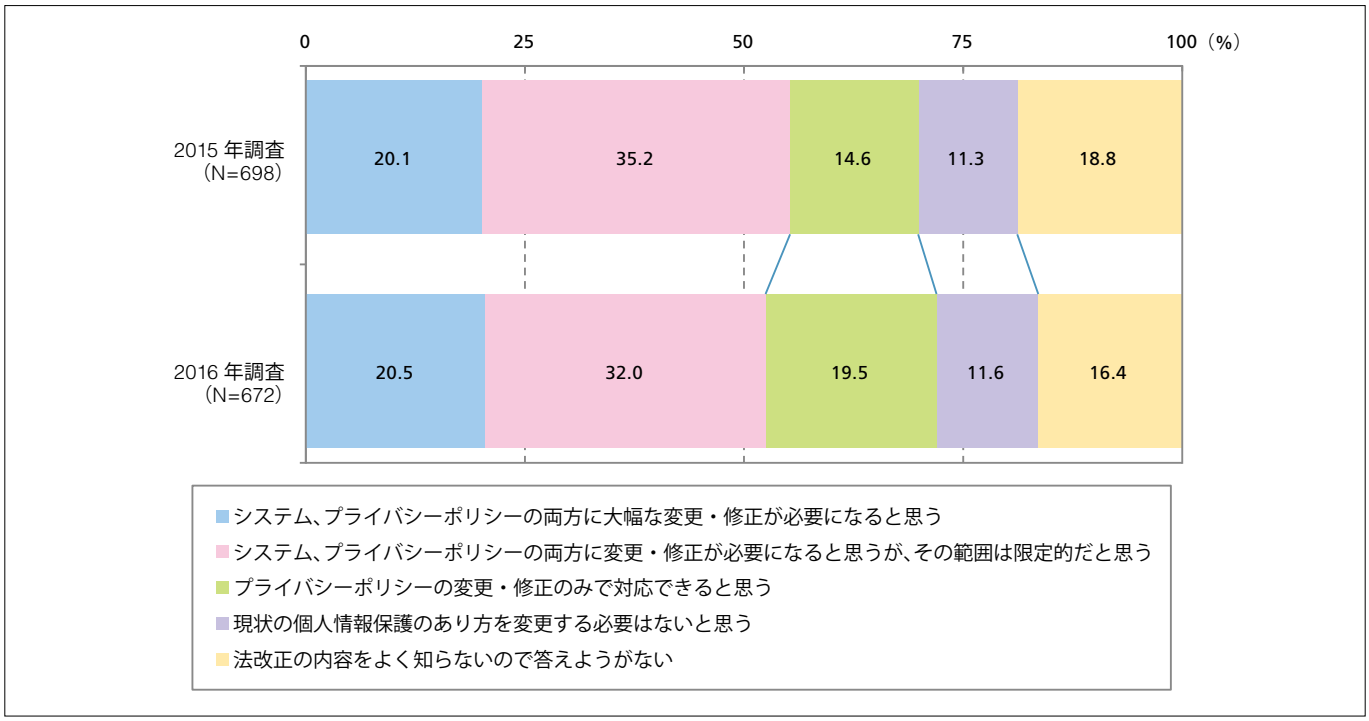


図1-19. 個人情報保護法改正のインパクトの経年比較（2015～2016年）

この結果からは改正個人情報保護法について、多くの企業が特別な対応が必要であると判断しているものの、対応の中身については当初の見込みに対し、システムの改修までは要しないとする企業が多いことが見てとれる。一方で、「法改正の中身をよく知らないので答えようがない」とする人が15%以上であったが、法改正の動向が自社が保有する情報にどのような影響をもたらすか精査する必要があるのではないか。

改正法の内容について気にしている点を問うた結果では、「個人識別符号の定義と範囲、取扱い」（38.1%）という回答が最も多く、「要配慮個人情報の定義と範囲、取扱い」（33.0%）が続いた（図1-20）。個人識別符号とは免許証やパスポートの番号、顔認識データなどの身体的特徴を変換したデータのことであり、要配慮個人情報とは人種や信条、社会的身分、病歴、犯罪歴といったいわゆるセンシティブ情報（機微情報）のことである。いずれも、今回の法改正で個人情報として新たに定義された情報であるが、その詳細は政令によって定められる見込みである。やはり、企業の情報システム／情報セキュリティ担当者としては、どこまでの情報が個人情報として扱われるのか、といった点に最大の関心が向かっているようである。

業種別に見ると、「公共・その他団体」では「個人識別符号の定義と範囲、取扱い」を、「情報通信業」では「要配慮個人情報の定義と範囲、取扱い」を気にする企業の割合が高い（図1-21）。

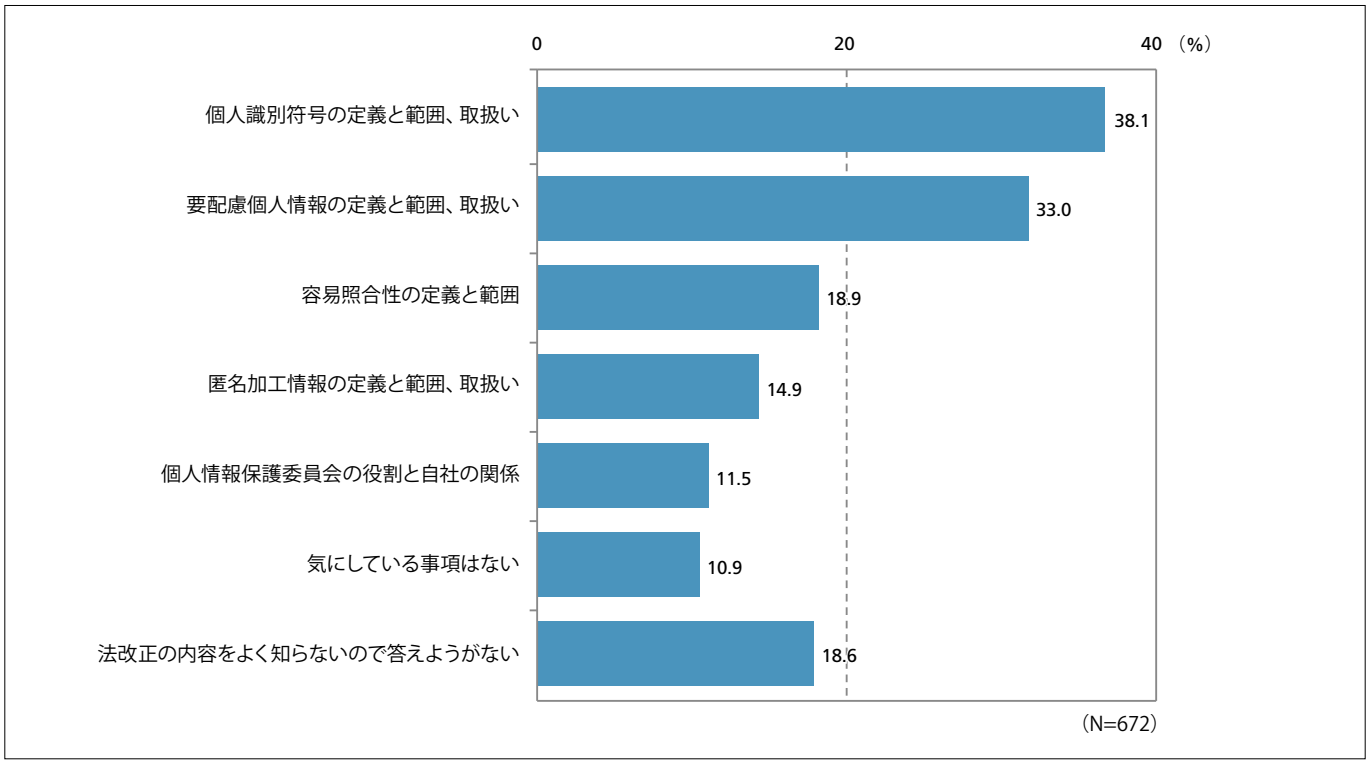
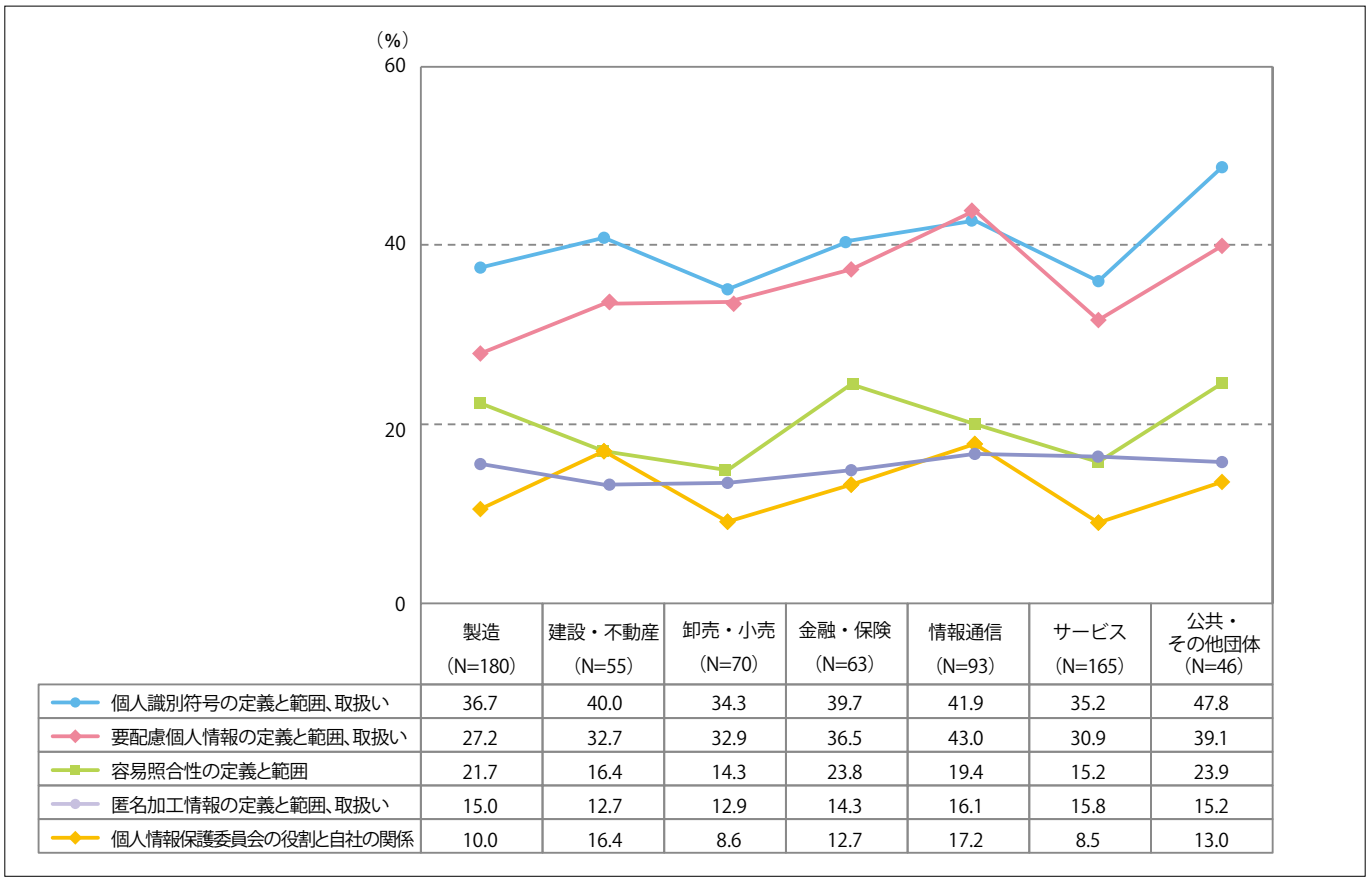


図1-20. 改正個人情報保護法で気にしている点



	製造 (N=180)	建設・不動産 (N=55)	卸売・小売 (N=70)	金融・保険 (N=63)	情報通信 (N=93)	サービス (N=165)	公共・その他団体 (N=46)
個人識別符号の定義と範囲、取扱い	36.7	40.0	34.3	39.7	41.9	35.2	47.8
要配慮個人情報の定義と範囲、取扱い	27.2	32.7	32.9	36.5	43.0	30.9	39.1
容易照合性の定義と範囲	21.7	16.4	14.3	23.8	19.4	15.2	23.9
匿名加工情報の定義と範囲、取扱い	15.0	12.7	12.9	14.3	16.1	15.8	15.2
個人情報保護委員会の役割と自社の関係	10.0	16.4	8.6	12.7	17.2	8.5	13.0

図1-21. 改正個人情報保護法で気にしている点(業種別)

5-2. マイナンバー制度を巡る対応方針

法規制に関しては、マイナンバー制度への対応も重要課題である。社会保障と税分野を中心に、一部の用途に限って原則生涯不変のマイナンバーを活用する同制度では、企業に対しても従業員あるいは取引先のマイナンバーの安全な取得と管理が求められる。

今回の調査は、2015年10月からのマイナンバーの通知をはじめ、制度の運用が開始されるなかで、企業の対応状況がどのように変化したかに注目した。

本調査では、手順やプロセス、役割分担の決定などに代表される「業務の対応」、システムの構築や修正、セキュリティ対策の強化といった「情報システムの対応」それぞれについて、調査時点での進捗状況を問うた。その結果、どちらの対応も前年調査時点から大きな進展が見られた(図1-22)。

業務の対応では、「完了している」企業の割合が前年からほぼ倍増し、情報システムの対応も10ポイント以上増加した。「作業が進行中」とした企業の割合も、業務の対応が32.9%、情報システムの対応が32.0%と、それぞれ大幅に上昇した。ただし、いずれの対応も完了済みの割合は30%台にとどまっており、2016年度も引き続き多くの企業で対応作業が継続されると見られる。

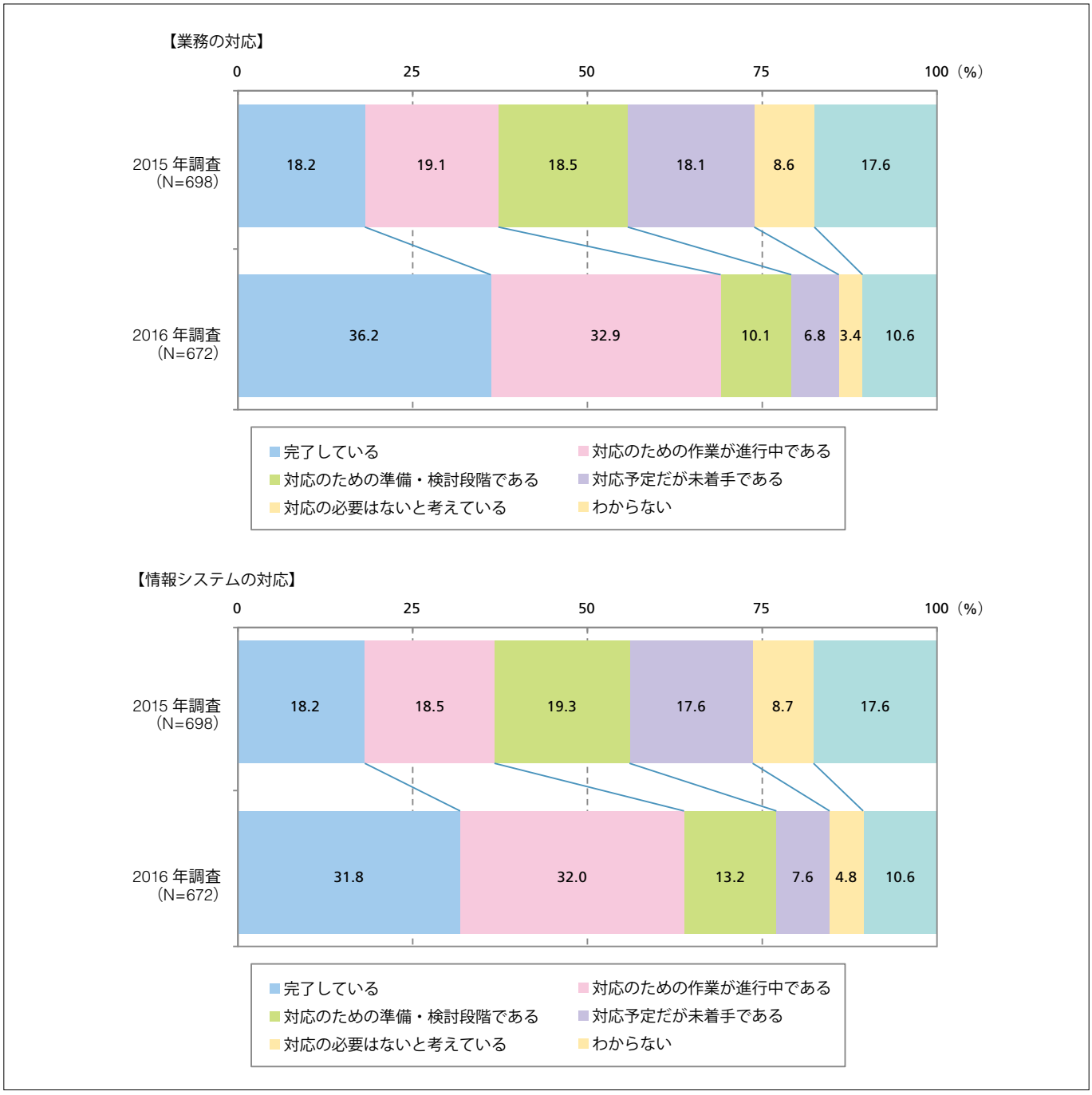


図1-22. マイナンバー制度への対応状況の経年比較（2015～2016年）

一方、調査実施時点で制度運用が始まっているなか、対応が完了していない理由は何か。今回は、情報システムの対応が「まだ完了していない」とした企業の回答者に対してその理由を尋ねたが、その回答結果を進捗状況別に集計すると、それぞれ異なる理由が浮かび上がった。

「作業が進行中」とした企業では、「社内のIT人材リソースの不足」（32.1%）が最も多く、人手不足が対応作業に影響を及ぼしていることが見てとれる。それに対して、「対応のための準備・検討段階」とした企業では、「システム化予算の不足」（25.8%）が最多であり、金銭的な問題で対応作業が滞っている企業が多いことがわかった。「対応予定だが未着手」とした企業ではその理由が分散しており、「社内担当部門との調整不足」（17.6%）など、作業の前提条件が整っていないところが少なくないと見られる（図1-23）。

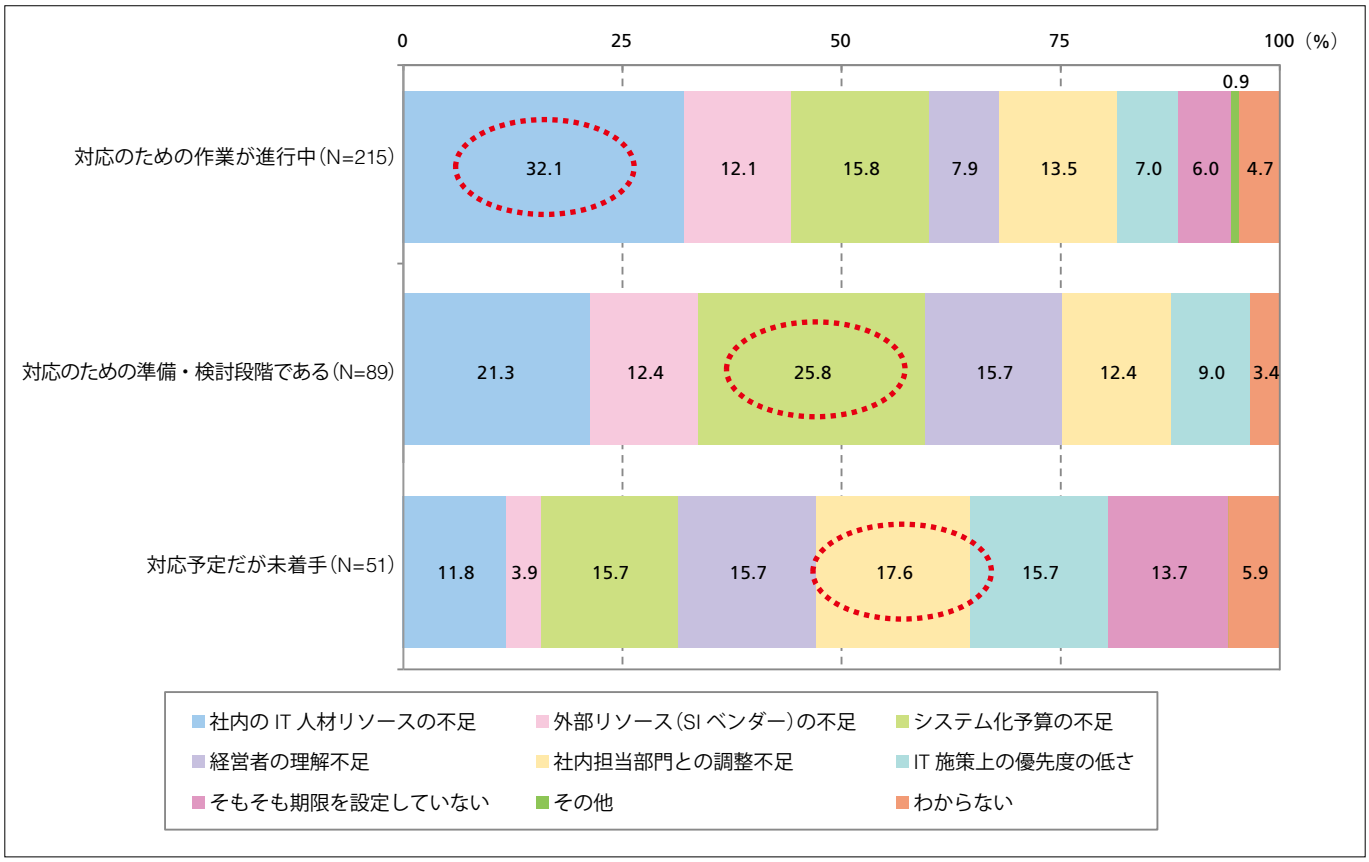


図1-23. 情報システムの対応が完了していない理由（進捗状況別）

また、前年同様、情報システムの対応を実施中またはその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53.8%で前年に続き最多となったが、2番目には「マイナンバーの取得システムの構築」（37.6%）が続いた（図1-24）。マイナンバーが実際に通知されたことで、その安全な収集が課題として浮上した結果であると見ることができる。

また、「マイナンバーの専用管理システムの構築」も前年から増加しており、マイナンバー制度対応に特化したソリューションが市場に出そろいつつあることもうかがえる結果となった。ちなみに、前年の調査では一桁台（8.6%）にとどまっていた「マイナンバー取扱業務の外部委託」も、今回の調査では13.5%に上っており、アウトソーシングの採用を現実的な解決策ととらえる企業が増加したことが示された。

その一方で、「システム全体のセキュリティ強化」は前年の調査結果から6ポイント以上減少した。マイナンバー制度を機にセキュリティ対策全般の見直しが図られるのではないか、との仮説を立てていたが、実際にはリソースが限られるなかで、最小限のコストで制度に対応しようとする企業が多い可能性がある。

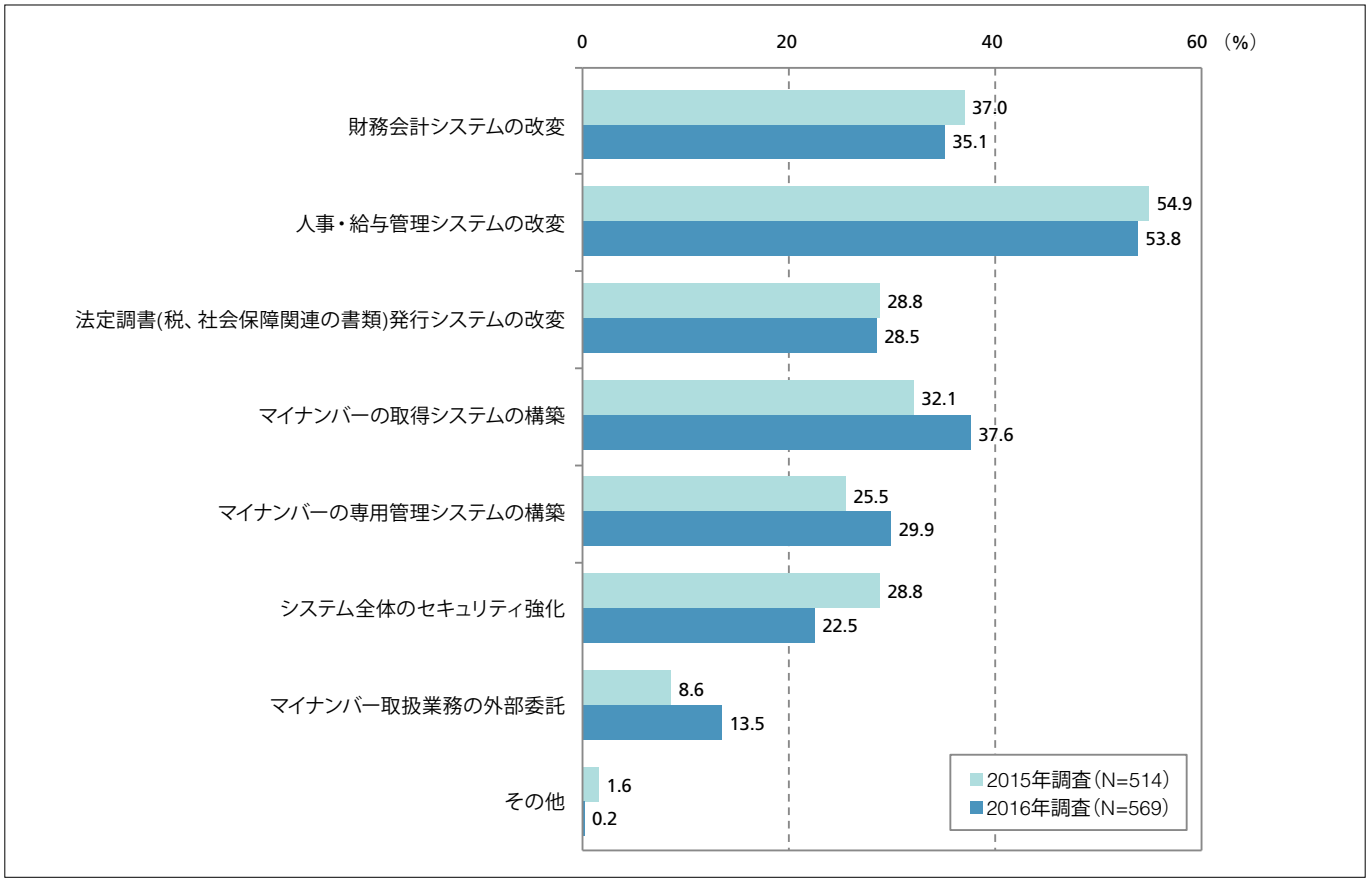


図1-24. マイナンバー制度への情報システムの対応範囲

なお、マイナンバー制度対応における問題点について問うたところ、「マイナンバーを適正に保管するための環境整備」が44.9%と最も多く、「マイナンバーの収集作業にかかる負担」（42.3%）が僅差で続いた（図1-25）。このように、マイナンバーの収集・保管といった実務上の負担を課題と感じる企業が多いことが、専用ソリューションの導入につながっていることの背景にあると考えられる。

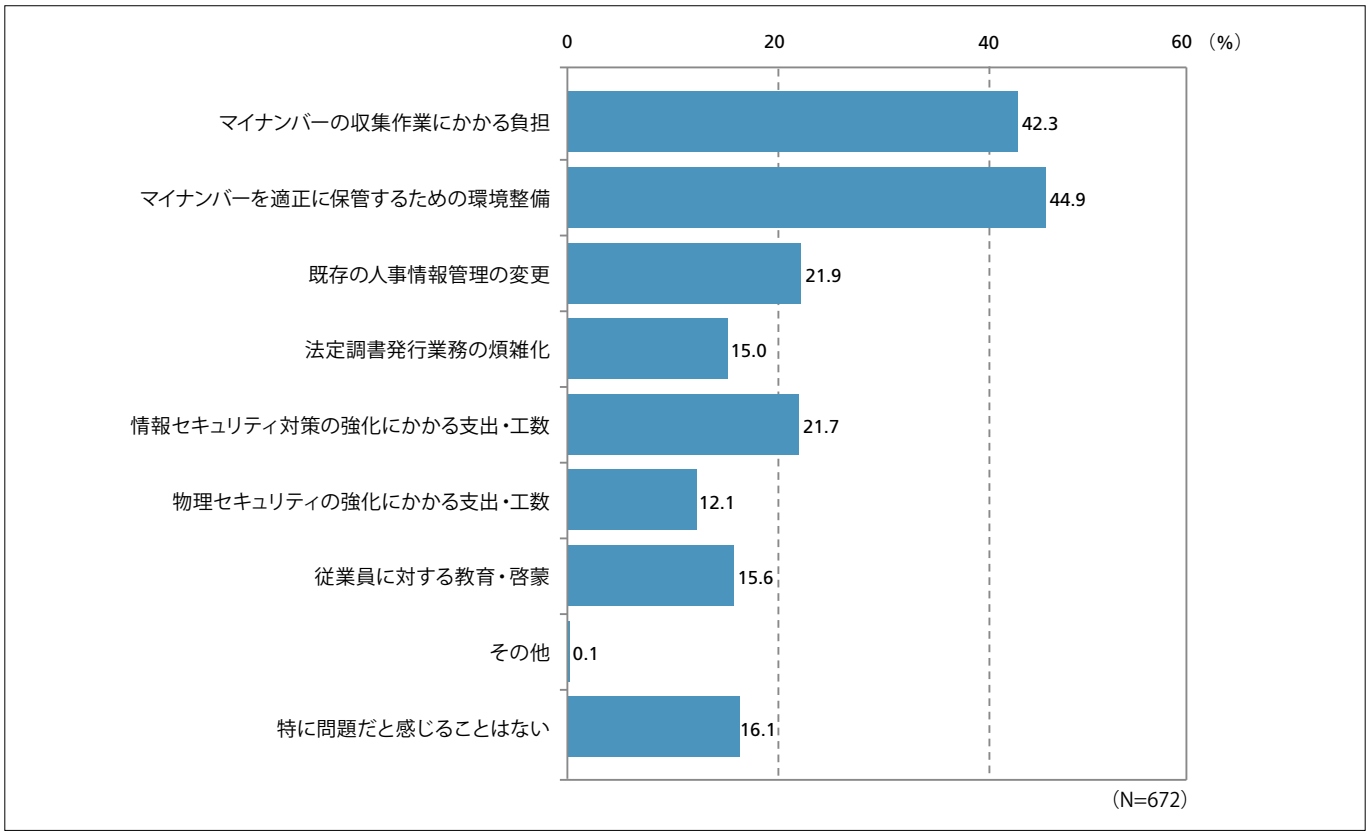


図1-25. マイナンバー制度対応における問題点

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。本章は、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、現時点での導入率、今後の導入意欲ともに高い分野である。項目別に見ると、「ファイアウォール」の導入率が最も高く、「VPN」「URLフィルタリングツール」が続いている。また、今後1年以内の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」「DDoS（サービス妨害攻撃）対策ツール」「フォレンジクスツール」があげられる（図1-26）。

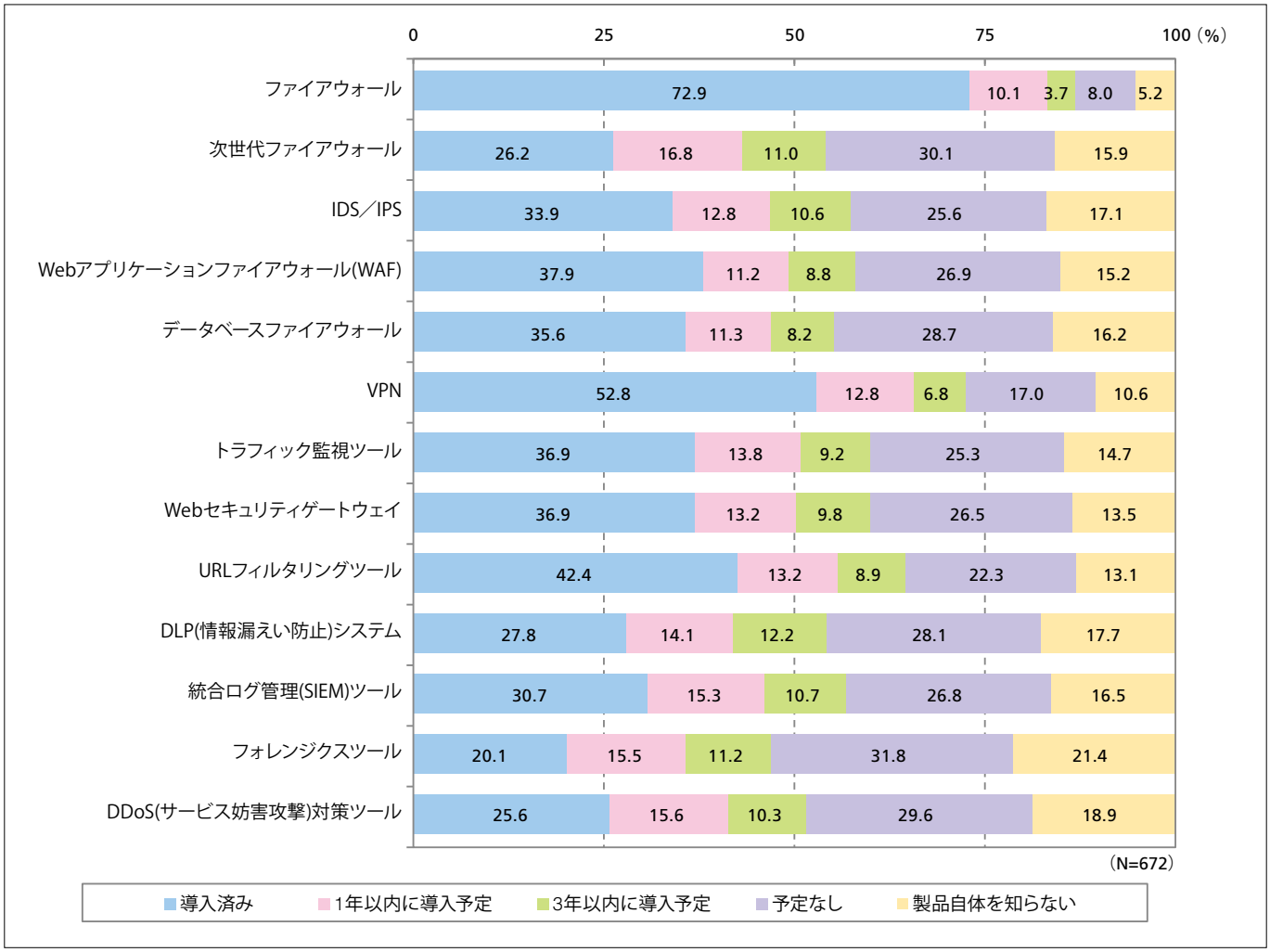


図1-26. セキュリティ製品の導入率（ネットワークセキュリティ）

6-2. クライアントセキュリティ製品の導入状況

主にクライアントPCの保護を目的に利用される製品として、「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であることは過去の調査から特に変化はない。今後1年以内については「検疫ネットワークシステム（NAC）」の導入意欲が高く、PCのモバイル用途が拡大するにつれ、それらを安全に社内ネットワークに接続させるための仕組みが求められていることがうかがえる（図1-27）。

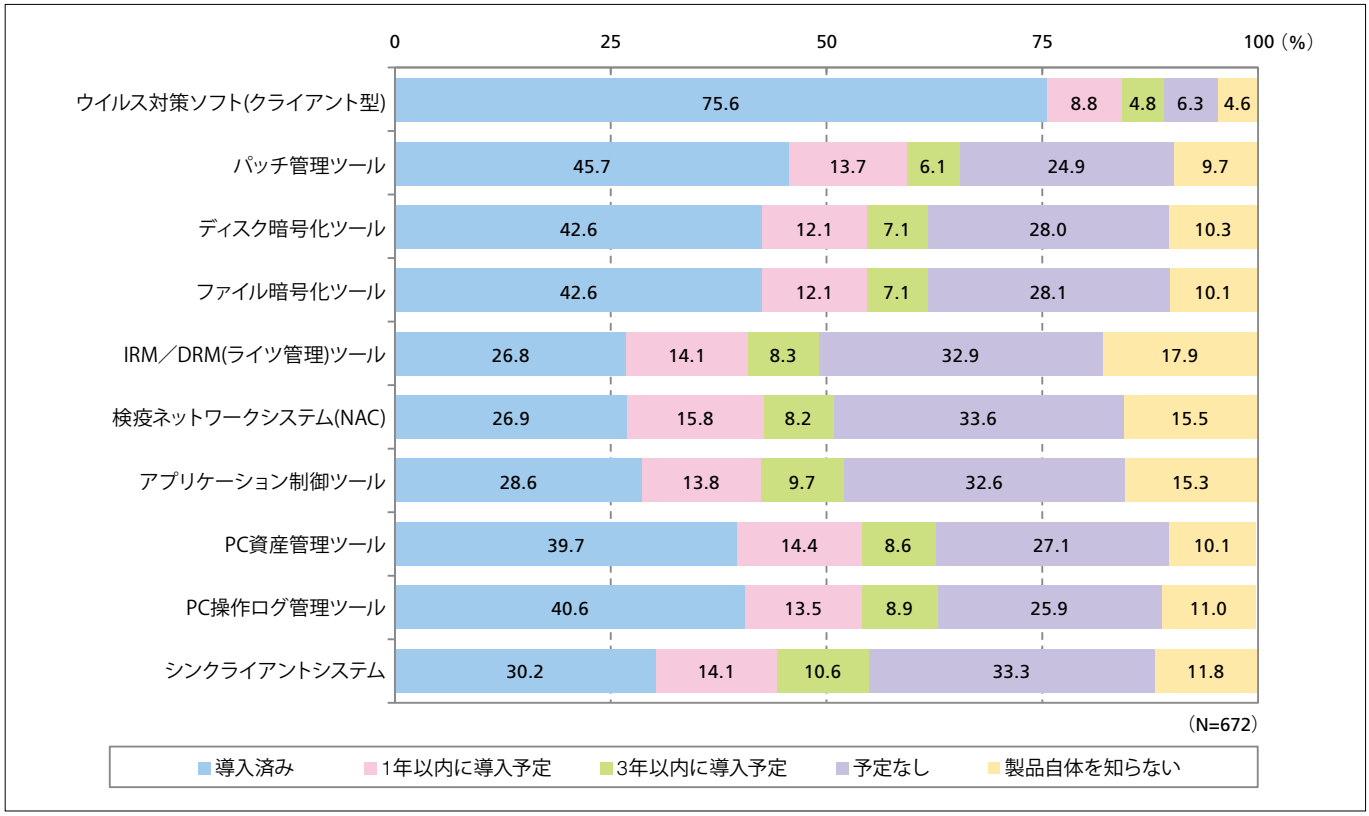


図1-27. セキュリティ製品の導入率（クライアントセキュリティ）

6-3. メールセキュリティ製品の導入状況

メールセキュリティ製品のなかでは例年の調査結果同様、「スパム対策ツール」の導入率が最も高いが、今後1年以内の導入に向けては、「メール監査ツール」などの送信メール対策に関わる製品や、「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、グローバル企業にとって必須のツールとなりつつある「Eディスカバリ（電子証拠開示制度）対策ツール」などに対する需要が高まることが予測される（図1-28）。

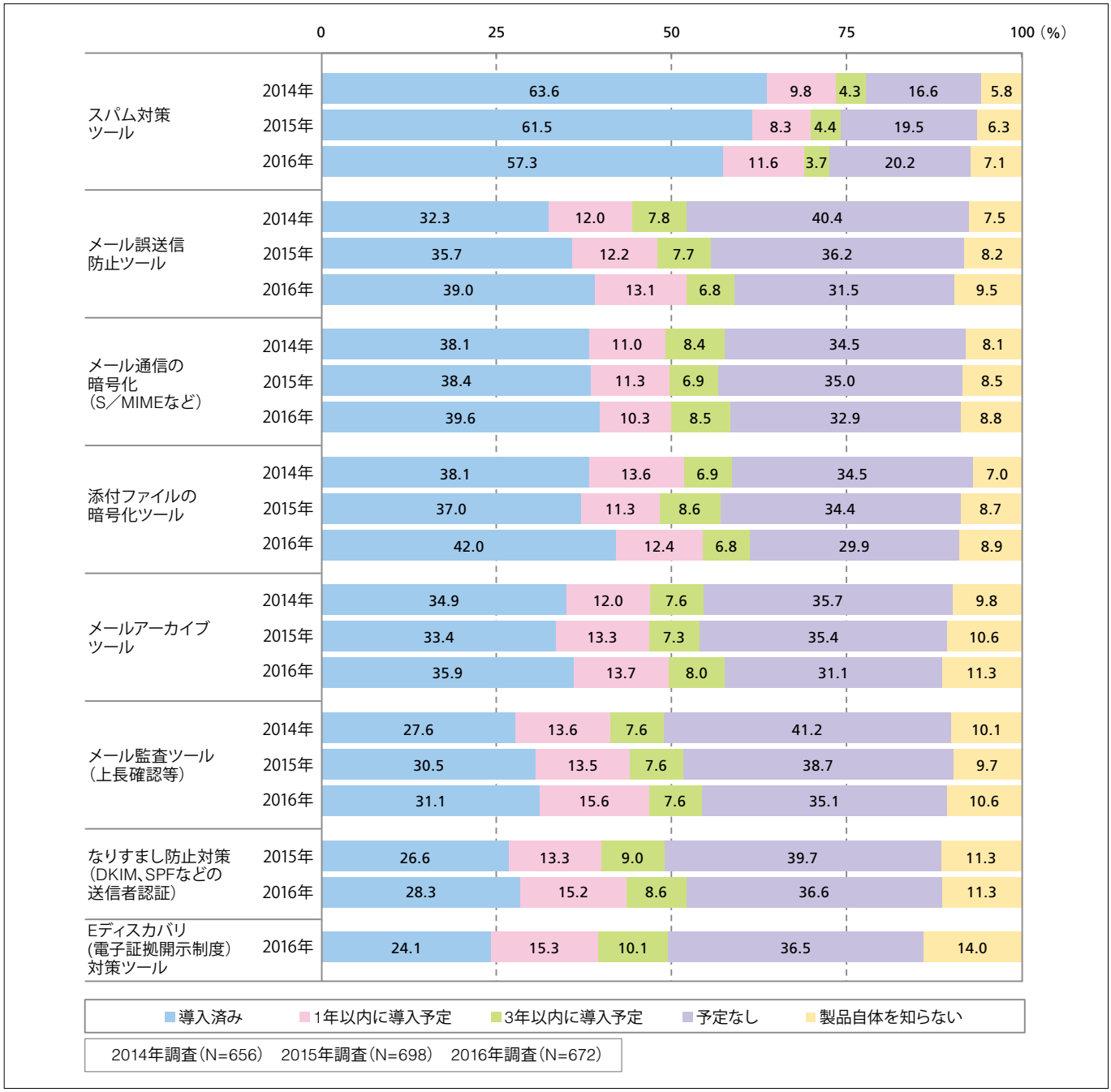


図1-28. セキュリティ製品の導入率（メールセキュリティ）

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、他分野の製品と比較して導入率が低い。そのなかではモバイル端末を活用したワンタイムパスワードや多要素認証システムは導入意欲の高まりが見られる（図1-29）。

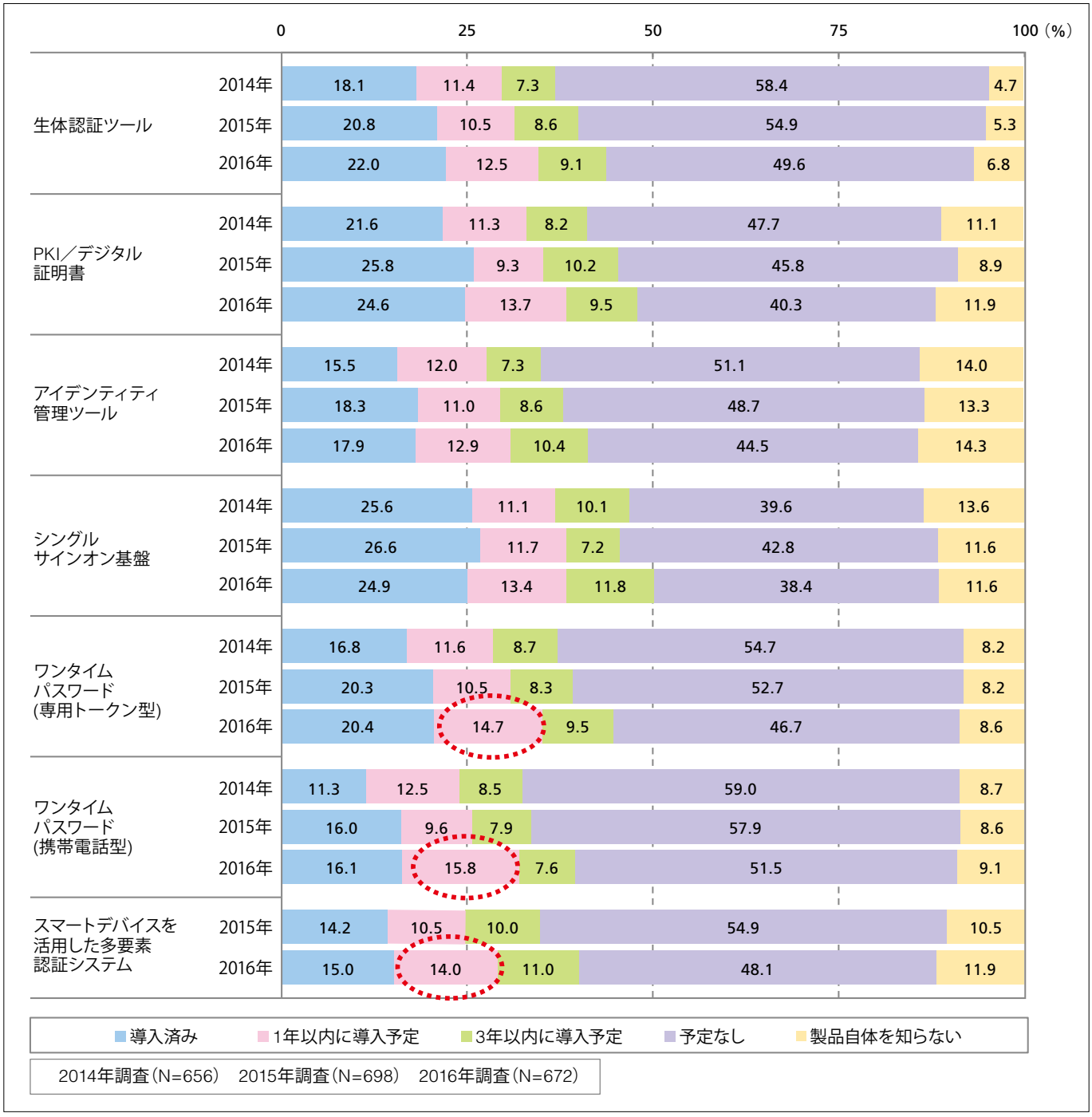


図1-29. セキュリティ製品の導入率（アクセス管理）

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、ほとんどのサービスが３割以上導入されているが、「セキュリティオペレーションセンター（SOC）による総合的セキュリティ監視」「Webサーバに対する脆弱性診断サービス」が「1年以内に導入予定」とする割合が高くなっている（図1-30）。

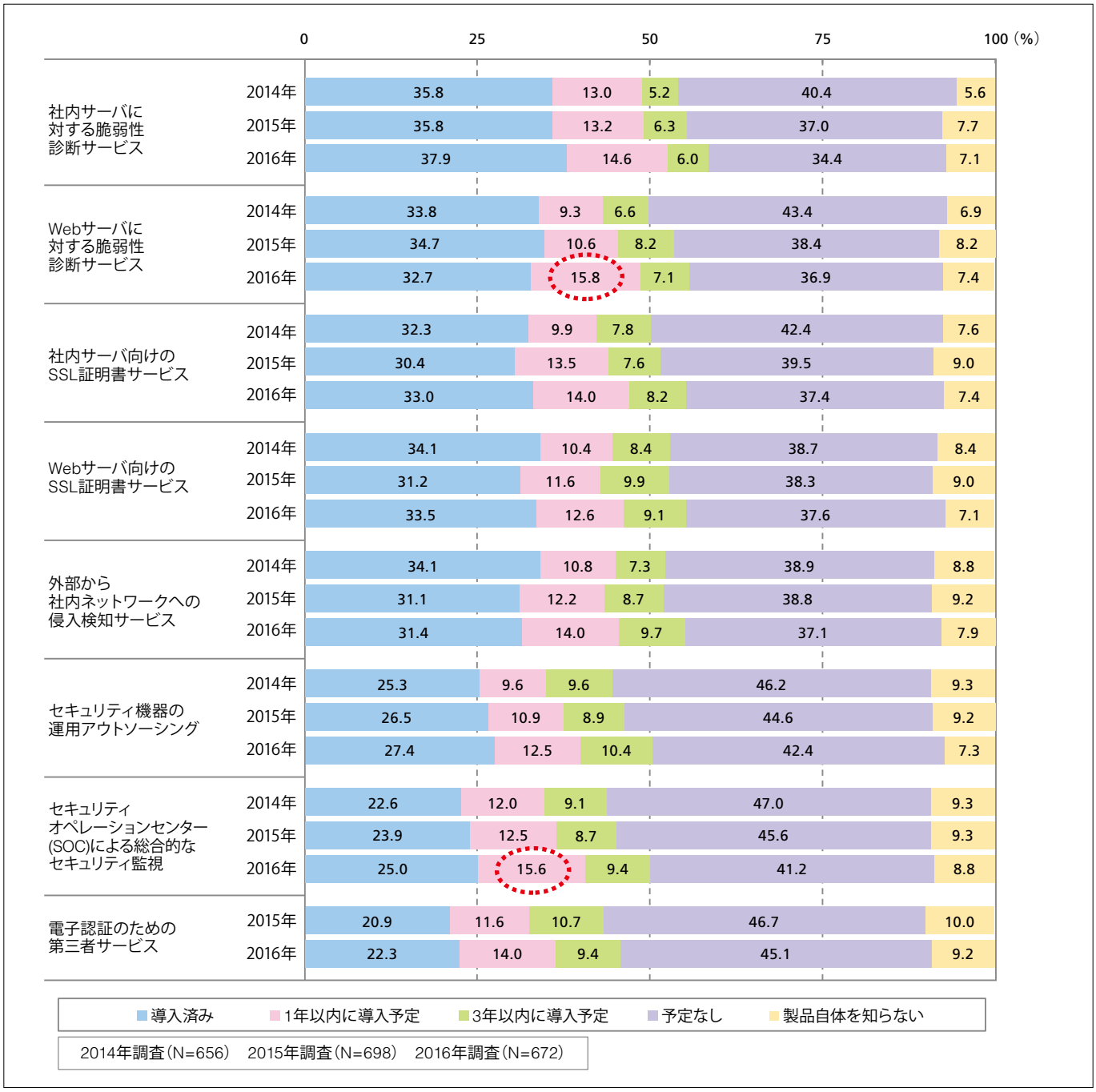


図1-30. セキュリティ製品の導入率（セキュリティサービス）

7 スマートデバイス／クラウドサービスの位置づけ

ここでは企業ITのなか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、クラウドサービス等の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

本調査で恒例となっているスマートデバイスの導入状況について、スマートフォン、タブレットそれぞれの支給と私物利用許可の双方についての取組み状況を見ると、「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50%台後半から60%台前半となった。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1-31）。

なお、本調査では全従業員の50%以上を対象とした取組みを「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」で、20%を超えた。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、なかでもスマートフォンを中心に進んでいることが見てとれる。

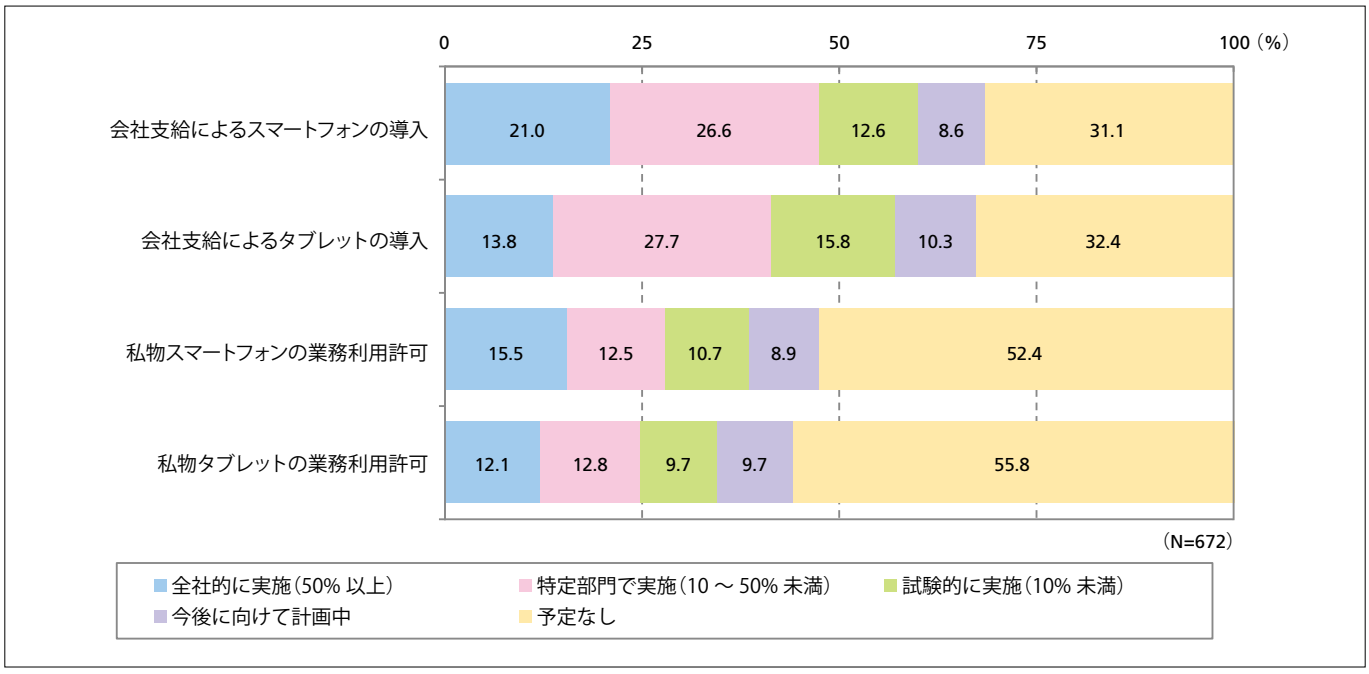


図1-31. スマートデバイスの導入状況

7-2. スマートデバイスの普及はさらに成熟期へ

2013年から行っているスマートデバイスの普及状況について、近年、本調査の結果から見られるのは、スマートデバイスをこれから新たに導入しようとする企業の割合は頭打ちとなっており、それよりも1社当たりの台数の増加が顕著になっているということである。

図1-32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4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、2013年以降、導入を実施または計画する企業の割合はほとんど増加しておらず、すでに実施済みの企業において、その対象範囲が拡大していることがわかる。特にスマートフォンは、2016年の「全社的に実施」とする企業の割合が2013年からほぼ倍増した。

一方、タブレットは台数の拡大は進んでいるが、「全社的に実施」の割合は2014年からほとんど伸びておらず、10%台前半で推移している。また、最新の調査では「予定なし」の割合が、調査開始以来初めて前年を上回る結果となった。昨今、タブレット端末よりも超軽量型のモバイルPCや大画面のスマートフォンの導入が進んでいることの表れと見ることができる。

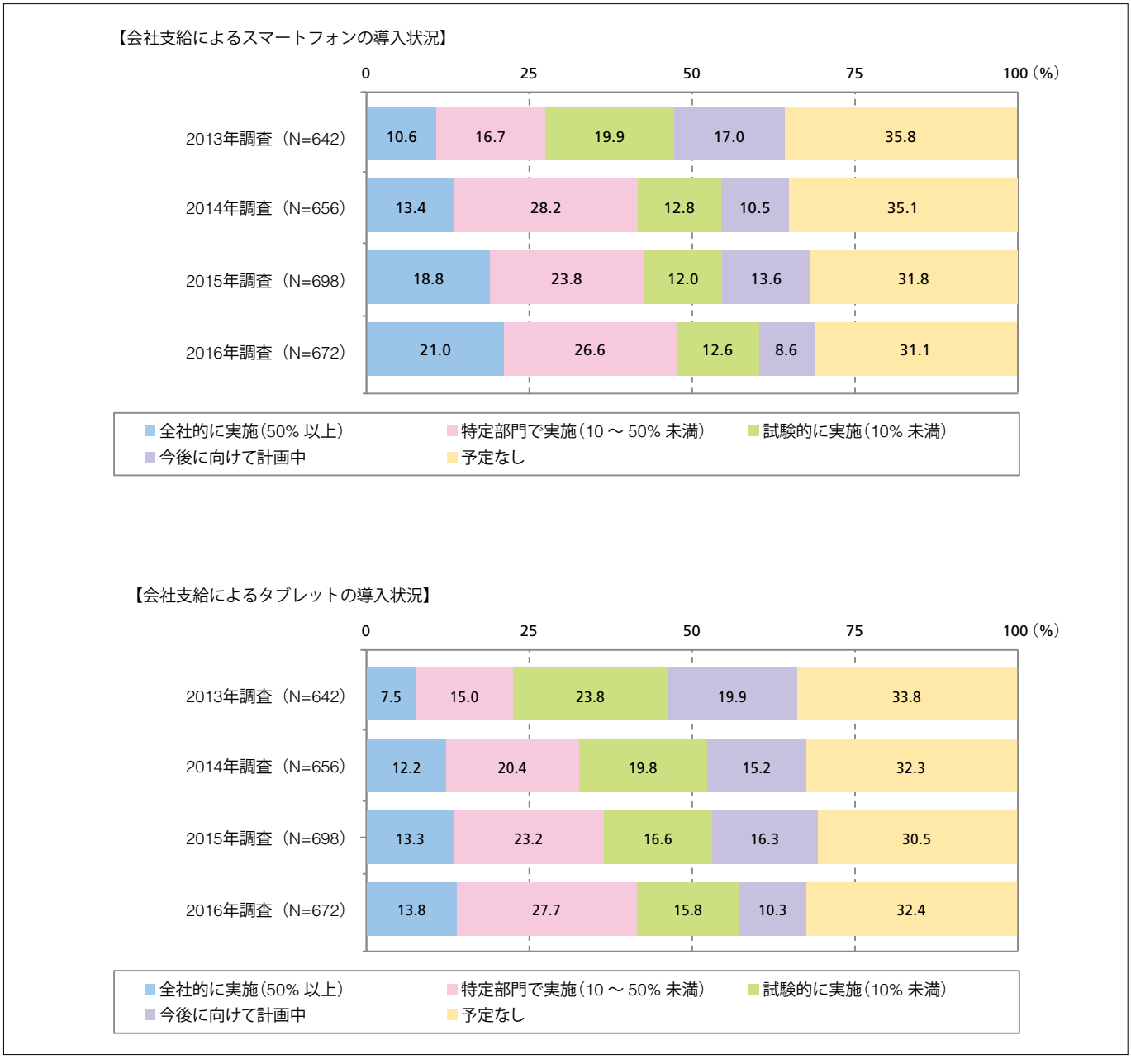


図1-32. スマートデバイスの導入状況の経年比較（2013～2016年）

7-3. クラウドコンピューティングの利用はさらに加速

実用化が進むクラウドコンピューティングについては、前年の調査において可用性やユーザビリティだけでなく、セキュリティにおいてもオンプレミス[*2]システムよりも有利と考える情報システム担当者が多いとの結果が確認された。今回もまた、「可用性・稼働率の高さ」「情報漏えい被害の軽減」など前年と同一の10項目について、「クラウドとオンプレミスのいずれが有利と考えるか」について回答を求めた。その結果、すべての項目について、「クラウドが有利」と回答する人の割合が「オンプレミスが有利」のそれを上回る結果となった（図1-33）。

項目別で、特に「クラウドが有利」と考えられているのは「可用性・稼働率の高さ」「災害発生時の被害の軽減」「マルチデバイスからのアクセスのしやすさ」の3項目であった。一方で、「オンプレミスが有利」と考える人の割合が最も高いのは「情報漏えい被害の軽減」であるが、同項目もクラウドを支持する人の方が多い。その一方で、４割前後は両者ともに「変わらない」との結果となった。

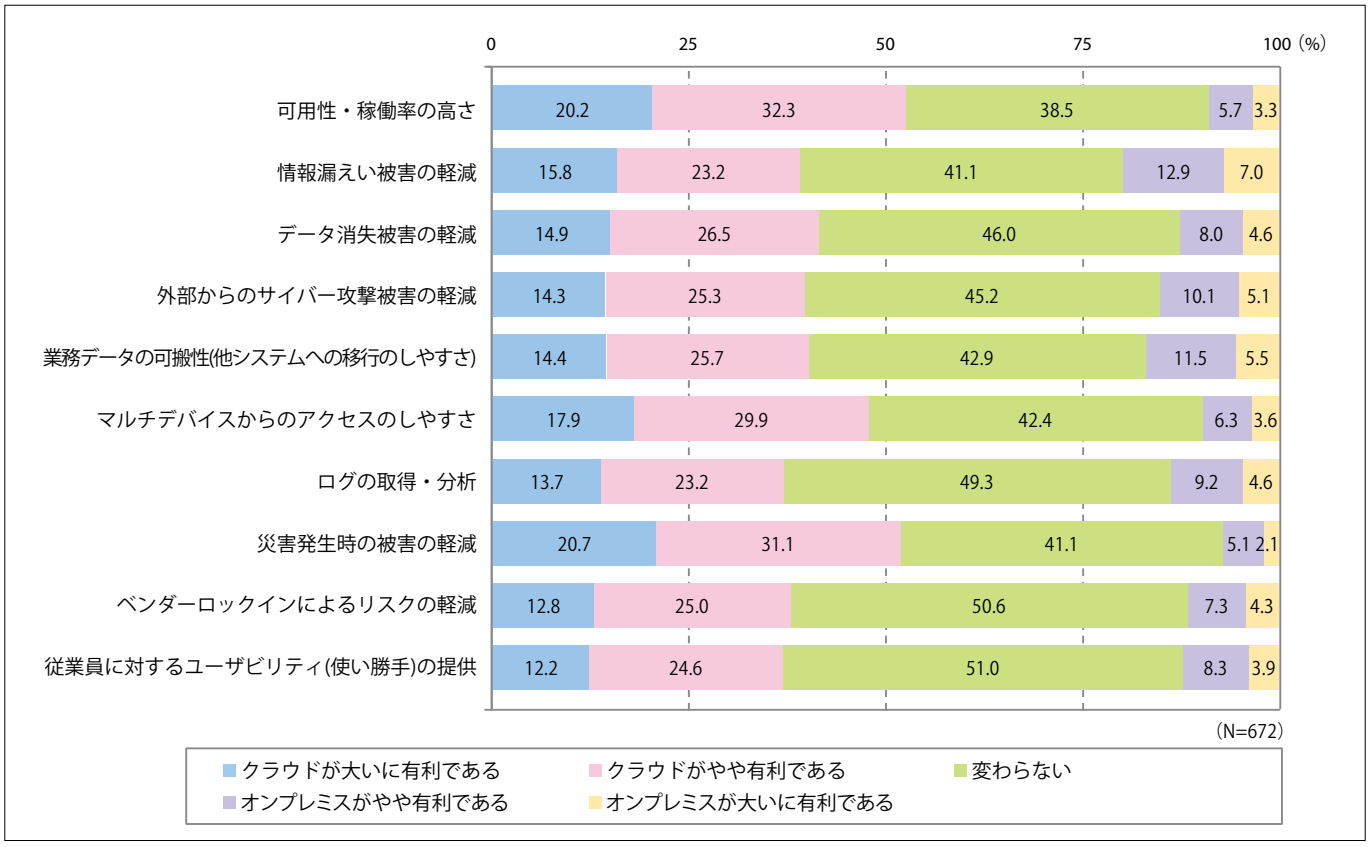


図1-33.「クラウド」と「オンプレミス」に対する認識

＊2. オンプレミスとは、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。

また、興味深いのはすべての項目について、前年調査よりもさらに"クラウド支持派"の割合が上昇していることである。なかでも「可用性・稼働率の高さ」は、クラウドが有利と考える人の割合が前年よりも5ポイント以上増加しており、サービスが進むなかで、クラウド環境の信頼性がさらに高まっていることが見てとれる（図1-34）。

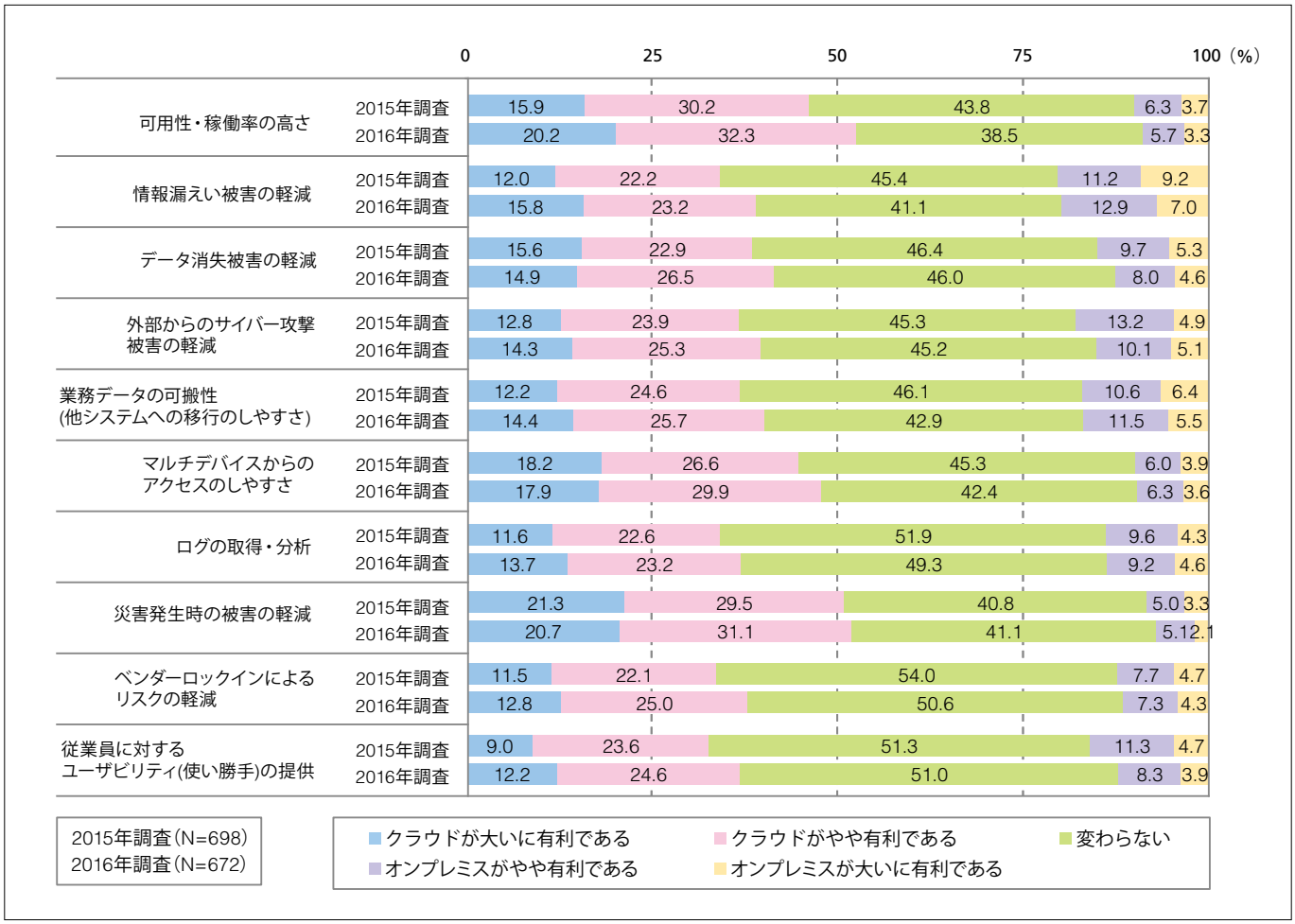


図1-34.「クラウド」と「オンプレミス」に対する認識の経年比較（2015～2016年）

8 総評

本調査は、IT利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2011年から実施しており、今回が5回目となる。今回の調査では、大規模な不正アクセス被害によって情報セキュリティリスクに対する関心が急速に高まった前年と比べれば落ち着いたものの、引き続き情報セキュリティが経営課題として重視されていることが確認された。特に、サイバー攻撃についてはインシデントの認知状況、企業におけるリスクの重視度合いともに上昇しており、多くの企業がその脅威を現実的な問題として受け止めている様子がうかがえた。今後、企業においては、ネットワーク境界部の防御を強化するとともに、電子メールなど日常的なコミュニケーション環境の見直しも求められると考えられる。

本格的な運用がスタートしたマイナンバー制度への対応は、経営課題としても重視されており、情報システム対応も前年から大きく進展した。ただし、完了済みとした企業の割合は未だ3割台にとどまり、多くの企業ではその取組みが道半ばであることも確認された。来る2016年度も、引き続き同制度への対応は国内企業にとって課題として積み残ることになると見られる。

また、改正法が可決・成立した個人情報保護法についても、調査時点で対応に着手している企業は少数にとどまった。とはいえ、セキュリティ支出において、コンプライアンス目的への支出が2016年度は伸びることが見込まれており、企業において、改正個人情報保護法への対応は、主要課題の1つとして認識されていることもうかがえた。

サイバー攻撃の脅威が現実化しつつある一方で、マイナンバー制度、個人情報保護法といったコンプライアンス要求、さらには内部不正の防止と、今日の企業が抱えるセキュリティ課題は多岐にわたる。そうしたなかで、今回の調査では、クラウド／コンピューティングに対する評価が、前年よりもさらに高まっていることが見てとれた。今後は、コストや可用性といった観点だけでなく、リスク対策の面からも、クラウドコンピューティングの活用を推進しようとする企業が増加することが予想される。

回答者プロフィール

業種	回答数	%
製造	180	26.8
建設・不動産	55	8.2
卸売・小売	70	10.4
金融・保険	63	9.4
情報通信	93	13.8
サービス	165	24.6
公共・その他団体	46	6.8
全体	672	100.0

年間売上高	回答数	%
5,000 億円以上	93	13.8
3,000 億～ 5,000 億円未満	33	4.9
1,000 億～ 3,000 億円未満	64	9.5
500 億～ 1,000 億円未満	44	6.5
100 億～ 500 億円未満	133	19.8
10 億～ 100 億円未満	215	32.0
1 億～ 10 億円未満	76	11.3
1,000 万円～ 1 億円未満	9	1.3
1,000 万円未満	5	0.7
全体	672	100.0

従業員規模	回答数	%
5,000 人以上	124	18.5
1,000 人～ 4,999 人	135	20.1
300 ～ 999 人	186	27.7
50 ～ 299 人	227	33.8
全体	672	100.0

業種別内訳

業種		回答数	%
製造	食品・飲料	20	3.0
	繊維	7	1.0
	パルプ・紙・印刷	5	0.7
	化学工業	12	1.8
	石油製品	1	0.1
	鉄鋼・金属	15	2.2
	機械	20	3.0
	電気機器	20	3.0
	情報通信機器	4	0.6
	電子部品・電子回路	16	2.4
	精密機器	9	1.3
	自動車・輸送機器	22	3.3
	医薬品	6	0.9
	その他の製造業	23	3.4
建設・不動産	建設	41	6.1
	不動産	14	2.1
卸売・商社	卸売	26	3.9
	小売	27	4.0
	商社	17	2.5
金融・保険	銀行	38	5.7
	証券	5	0.7
	保険	13	1.9
	その他金融	7	1.0
情報通信	通信	14	2.1
	ITベンダー／システムインテグレータ	64	9.5
	インターネットサービス	5	0.7
	情報システム子会社	10	1.5
サービス	電力・ガス	9	1.3
	運輸・倉庫	30	4.5
	メディア・出版・放送・広告	4	0.6
	医療・福祉・介護	52	7.7
	教育 (学校以外)	4	0.6
	人材派遣・業務代行	7	1.0
	その他サービス	59	8.8
公共・その他団体	学校	12	1.8
	官公庁	4	0.6
	地方自治体・公共機関	14	2.1
	農業・水産・鉱業	3	0.4
	その他の業種	13	1.9
全体		672	100.0