JIPDEC IT-Report 2017 Spring

特集

「企業IT利活用動向調査2017」
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

はじめに

本誌「IT-Report 2017 Spring」では、JIPDECが2011年から毎年継続して実施しているIT利活用に関わる独自調査の結果をとりまとめ、紹介しています。

本調査では、改正個人情報保護法の機運が高まった2016年から法への対応状況や自社に与える影響について調査を行っていますが、今回の調査では、改正法への対応状況について、約7割が「すでに完了している」「全面施行までに対応完了見込み」と回答しつつも、残り３割は、「年度中」または「わからない」という回答でした。

また、2015年から継続して行っている「個人情報保護法改正のインパクト」に関しては、「システム、プライバシーポリシー両方に大幅な変更・修正が必要」と指摘する回答は3年間ほとんど変化がみられませんでしたが、「変更・修正は必要だが、範囲は限定的」との回答は、2015年から2016年にかけていったん減少傾向にあったものの、今年の調査では約8ポイント増加しました。

本調査開始時より継続して行っている「情報セキュリティインシデントの認知率」については「インシデントを経験していない」とする回答が、昨年調査に比べ約7ポイント減少し、一方で、スマートフォン、携帯電話、タブレットなどの紛失・盗難や標的型サイバー攻撃などが増加傾向にあることがわかりました。また、セキュリティインシデントの認知度の増加の影響か、今回調査ではセキュリティ関連の「認証取得に関する費用」や「セキュリティ製品の利用・購入費」などの支出の増加を見込んでいる企業が多いことがわかりました。

このほか、本調査では、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、スマートデバイス／クラウドサービスの位置づけ、働き方改革とセキュリティ対策との関連性など、広範囲にわたる企業IT化の現状について、経年分析を含めてご報告しています。

あわせて、2016年10月から2017年3月の情報化動向をとりまとめて紹介していますので、本誌をぜひ、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-Report2017 Spring　**目　　次**

【特集】「企業IT利活用動向調査2017」にみるIT化の現状

JIPDECは、調査会社の株式会社アイ・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2015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：2017年1月24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、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：653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（23.4%）、次いでサービス業（23.1%）、情報通信（16.8%）、金融・保険（11.0%）となった。所属部門では情報システム部門が最も多く（46.4%）、役職は部長（34.5%）、課長（30.2%）、係長・主任（19.1%）の順となった。

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・製品選定に実際に関与している」（57.6%）、「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」（56.8%）が半数以上を占めている。過去の調査でも同様の傾向がみられている。

2 経営における情報セキュリティの位置づけ

本調査は、企業における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。まず、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。

2-1. 重視する経営課題

全25項目の経営課題を取り上げ、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）。「業務プロセスの効率化」（53.1%）が5年連続で首位となったが、今回の調査で新たに追加した「従業員の働き方改革」（35.8%）が2位に続き、「情報セキュリティの強化」（33.7%）は3位となった。

なお、今年の調査結果で上位となった14項目について、過去2回の調査結果と選択率の変化を見ると、選択率が下がっている項目が多く、課題テーマの分散化が進んでいることがうかがえる（図2）。新規項目である「従業員の働き方改革」が上位にあがった影響も小さくないと考えられる。

前年調査から選択率が上昇した項目として、「法規制への対応（全般）」が約3ポイント、「システム更新への対応」「個人情報保護法対応」が約2ポイント、「災害・システムダウンへの対応強化」が約1ポイントそれぞれ上昇した。

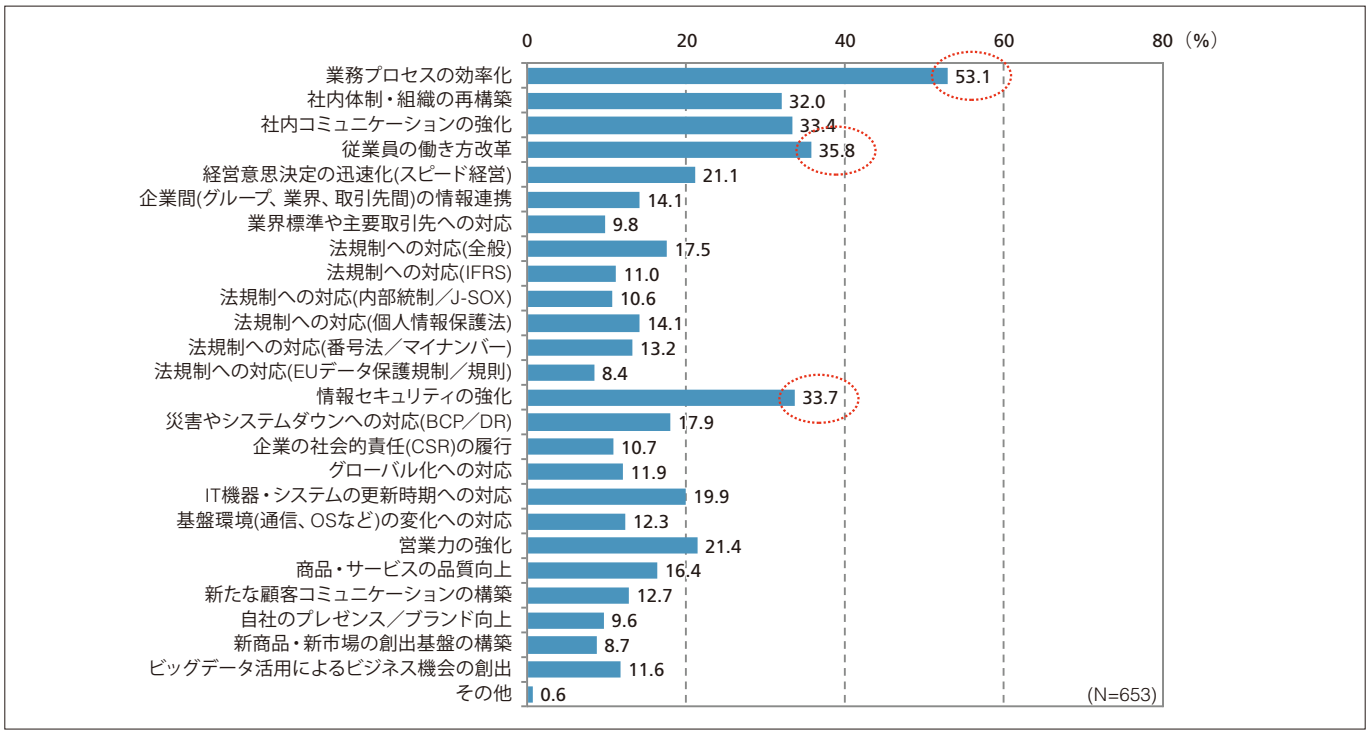

図1. 今後重視したい経営課題（複数回答）

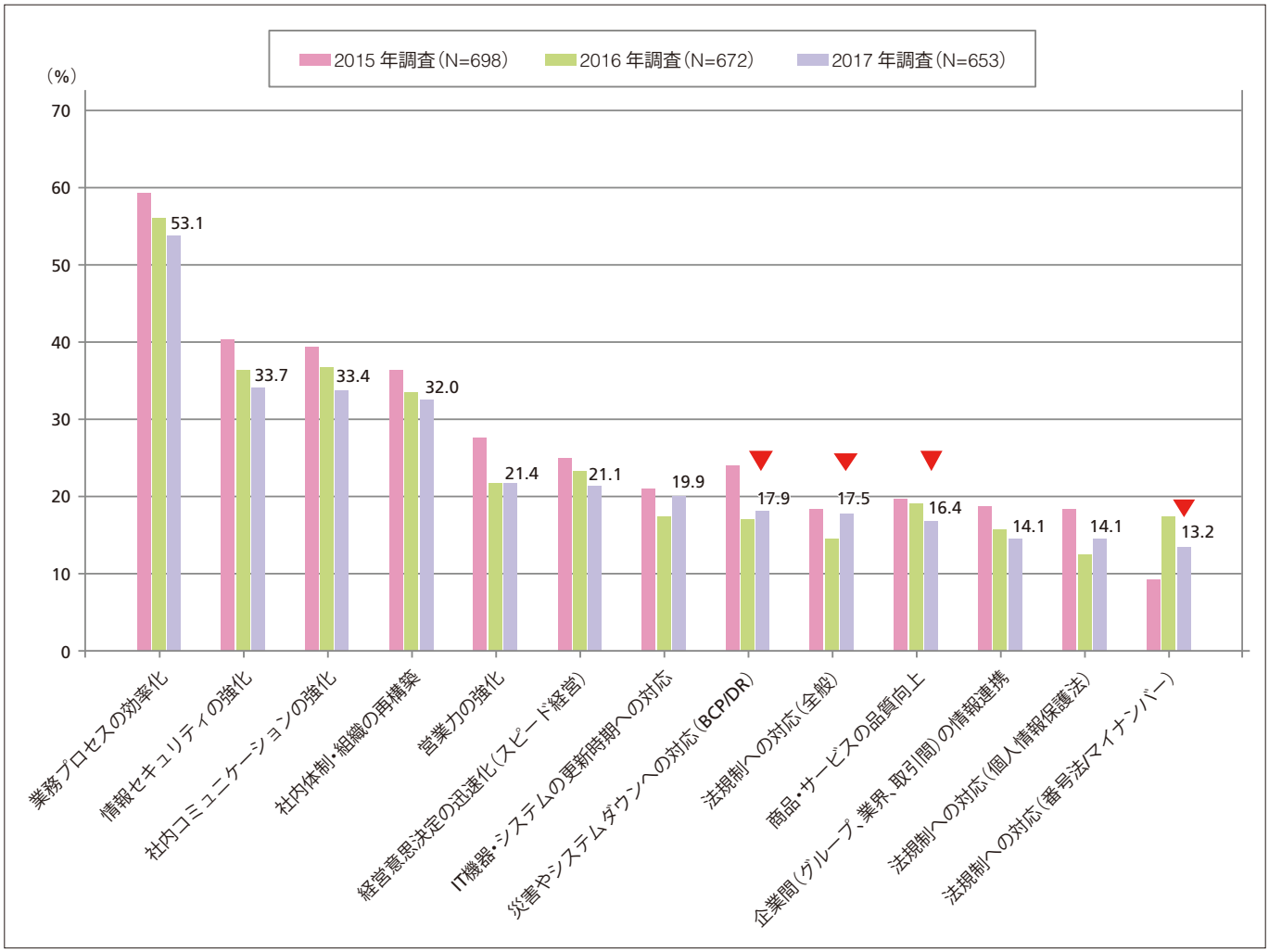

図2. 主要経営課題に対する選択率の経年変化（2015～2017年調査）

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「社内PCのマルウェア感染」（26.6%）で、次いで、「従業員によるデータ、情報機器の紛失・盗難」「スマートフォン、携帯電話、タブレットの紛失・盗難」「モバイル用PCの紛失・盗難」がそれぞれ20%台となった。

「個人情報の漏えい・逸失」に関しては「人為ミス」によるインシデントの認知率が16.2%と高く、内部不正によるインシデントは人為ミスの約半分の8.3%であった（図3）。

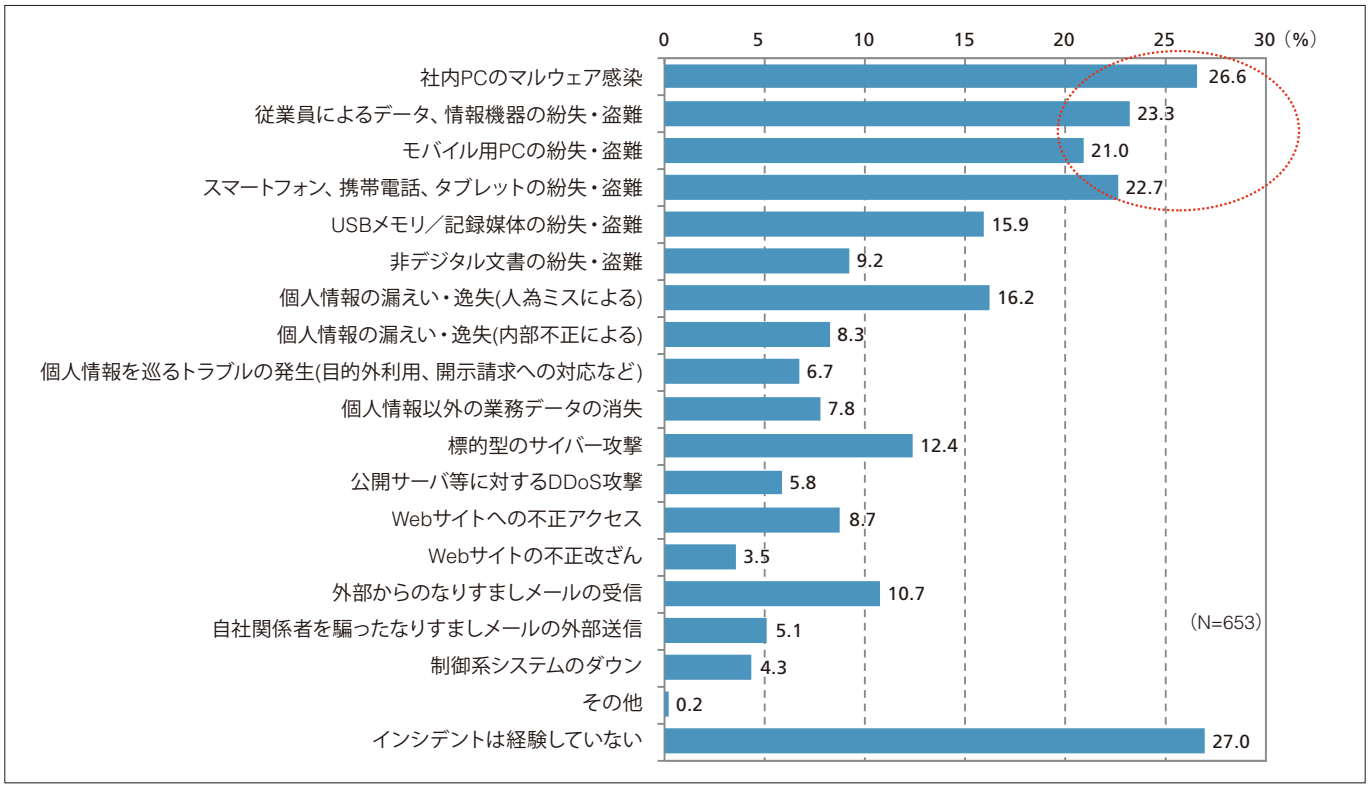

図3. 過去1年間に認知したセキュリティインシデント（複数回答）

過去の調査結果と比較すると、「インシデントは経験していない」とする割合が2015年調査には38.1%だったのが、翌16年には34.4%、今回調査では27.0%まで減少し、インシデントの認知率は全体的に上昇傾向にある。たとえば「スマートフォン、携帯電話、タブレットの紛失・盗難」は、前年と比べ、5ポイント以上の上昇が見られた（17.0%→22.7%）。また、サイバー攻撃の脅威も増しており、「標的型のサイバー攻撃」は今回の調査で初めて2桁台に突入した（9.5%→12.4%）。内部不正による個人情報の漏えい・逸失も、徐々に認知率が高まってきている（図4）。

企業においては、セキュリティインシデントを「起こさない」ことよりも、「起こることを前提とした対策をたてる」ことの重要性が増していると言えよう。

なお、従業員規模別にセキュリティインシデントの認知状況を2016年調査と比較して見ると、たとえば「個人情報の漏えい・逸失」を経験した度合いは、5,000人以上の大手企業と比べ5,000人未満の準大手、中堅・中小企業での増加が見られた。またサイバー攻撃被害に関しては1,000人以上の企業での増加が見られた（図5、6）。

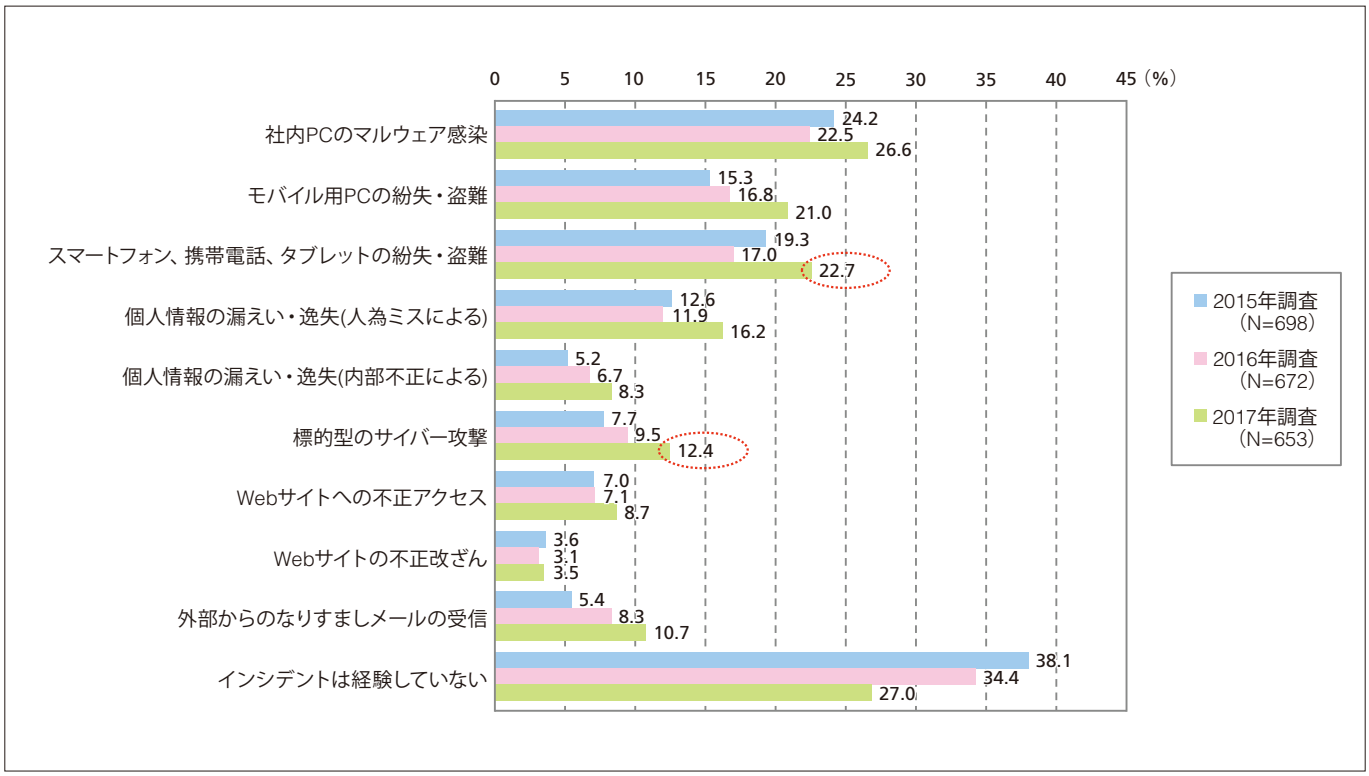

図4. 主要なセキュリティインシデント認知率の経年変化（2015～2017年調査）

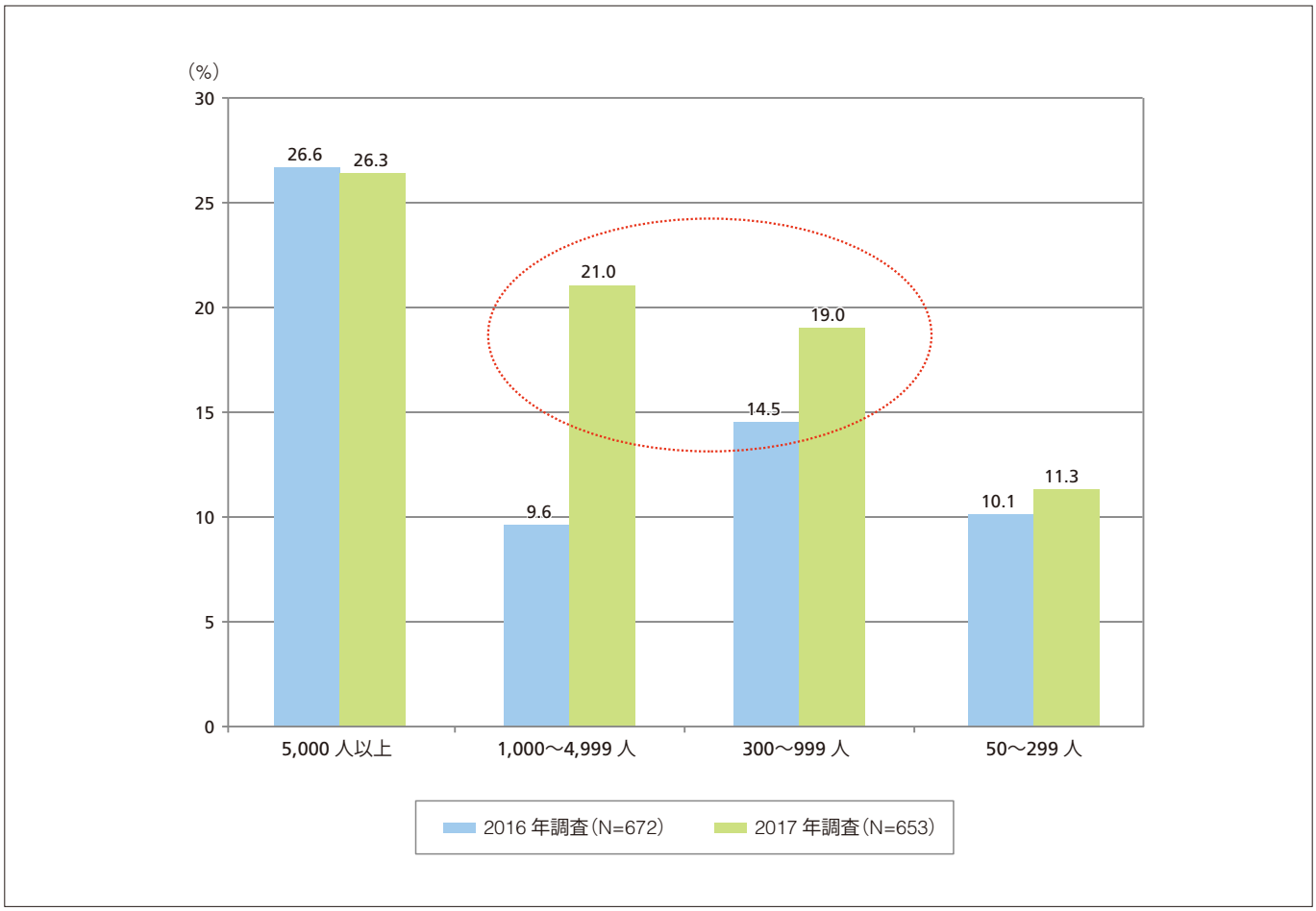

図5.セキュリティインシデント「個人情報の漏えい・逸失を経験」の認知状況（従業員規模別）

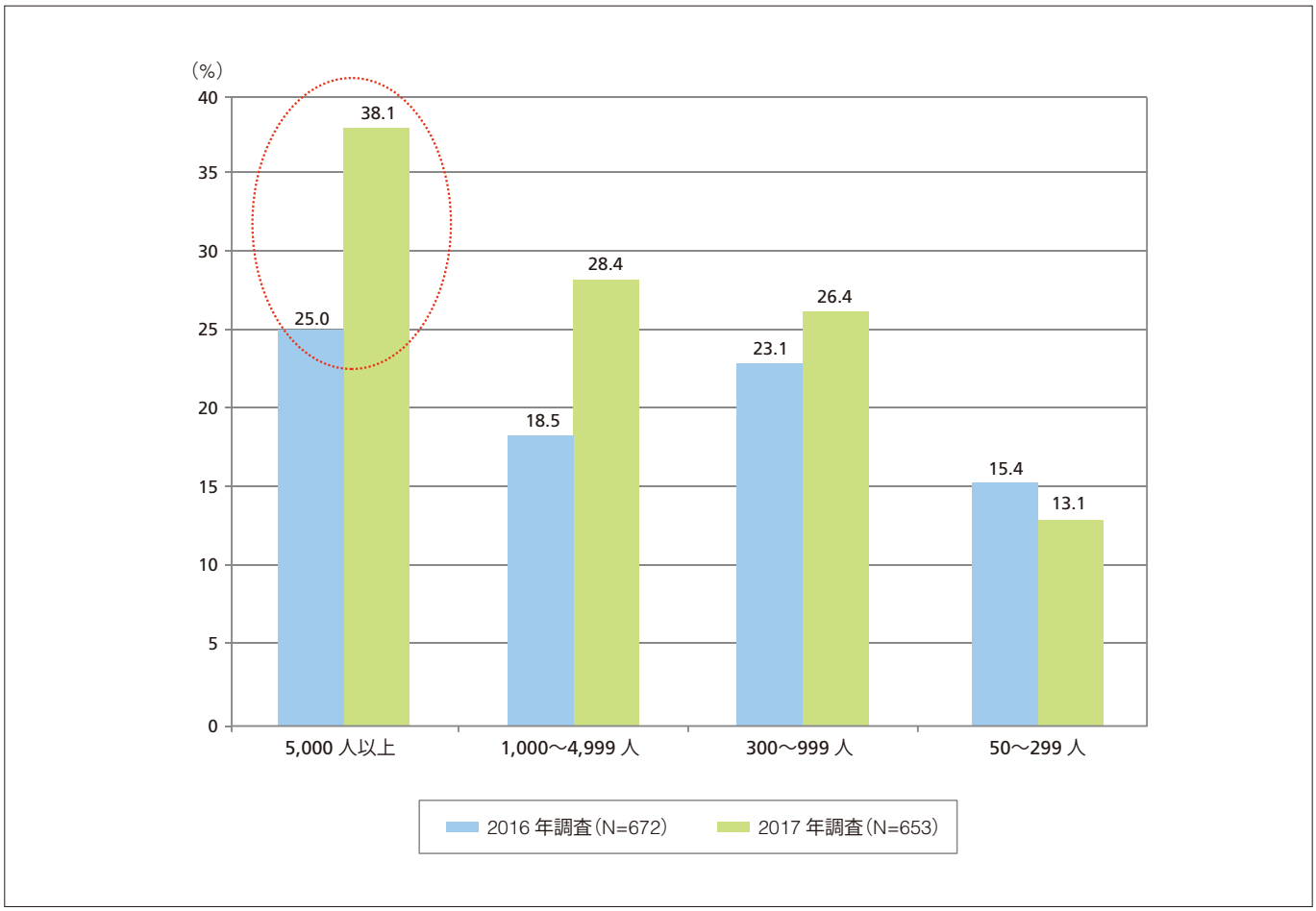

図6.セキュリティインシデント「サイバー攻撃被害を経験」の認知状況(従業員規模別)

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

インシデントの認知率に合わせて、企業におけるリスクの重視度合いも上昇している。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それぞれ調査しているが、今回の調査では、いずれにおいても「きわめて重視しており、経営陣からも最優先で対応するよう求められている」とした回答が2015年以降で最多となった（図7）。特に「サイバー攻撃」に対しては、幅広い企業が重要課題として認識するようになっている。業務におけるITへの依存度が高まるとともに、スマートデバイス、IoTなどエンドポイントの多様化も進展するなか、サイバー攻撃の脅威は今後も増加すると予想される。企業においては、局所的な対策にとどまらず、ITインフラ全体のセキュリティレベルの向上に力を注ぐことが求められるであろう。

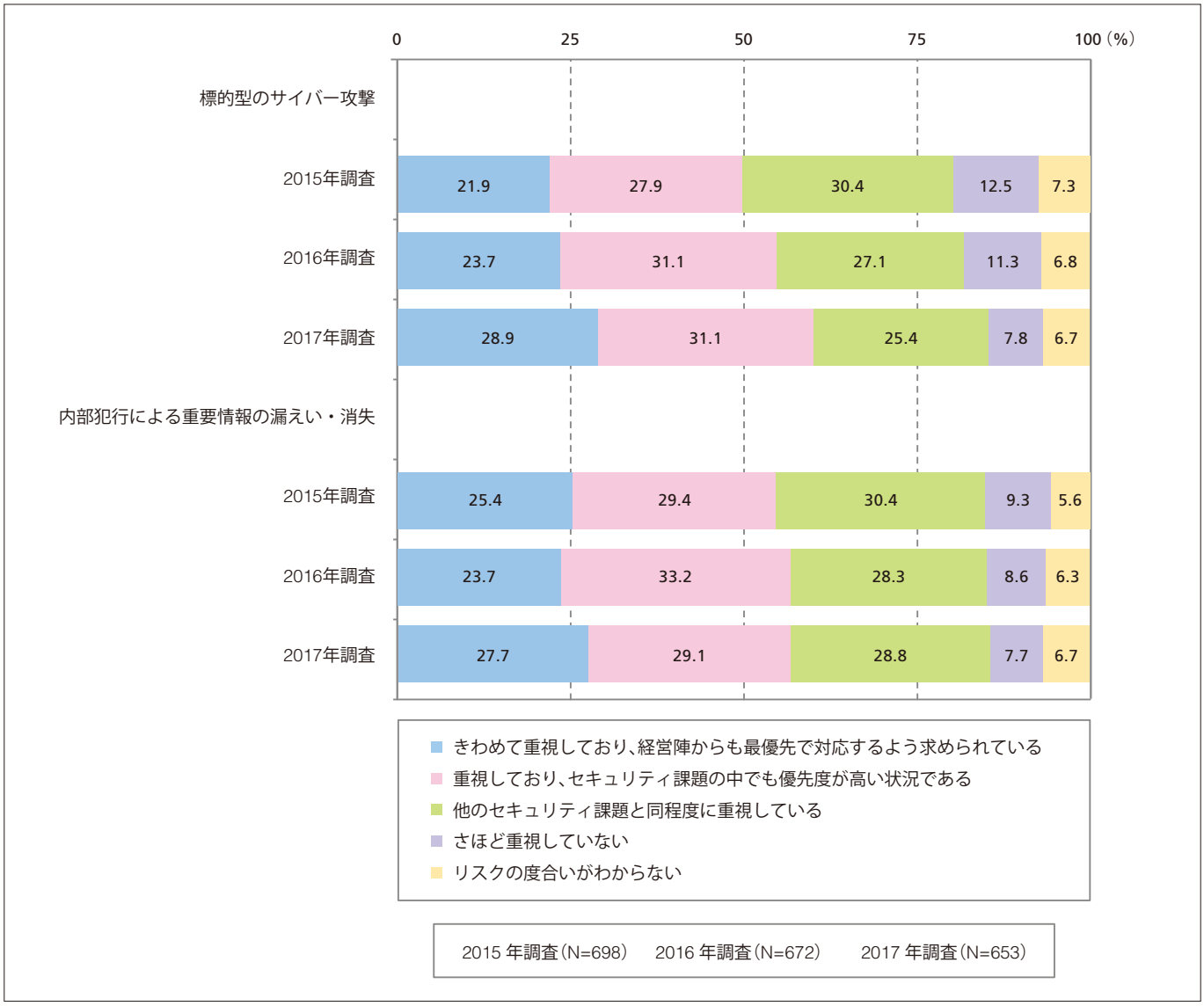

図7.「標的型のサイバー攻撃」および「内部犯行による重要情報の漏えい・消失」に対するリスクの重視度合いの経年変化（2015～2017年調査）

2-4.セキュリティ対策の進展状況

具体的なセキュリティ対策の進展はどのようになっているのか。この調査ではサイバー攻撃や内部犯行への代表的な取組みをピックアップし、その実施率についても調査している。その推移を見ると、あまり対策が進んでいないことがわかる。

たとえば、「標的型サイバー攻撃対策」では、本来重視すべき脆弱性診断やパッチの適用といった取組みの実施率は下がる傾向にある（図8）。一方、「内部犯行対策」も、Webやメールに関する利用制限は多少進展しているが、そもそも何をどのように守るかに関わる「重要情報の取扱方針」に関する対応はやはり実施率が伸びていない（図9）。こうした結果を見る限り、セキュリティの脅威に対する認識と現実の対策との間には重大な乖離があると言わざるを得ない。

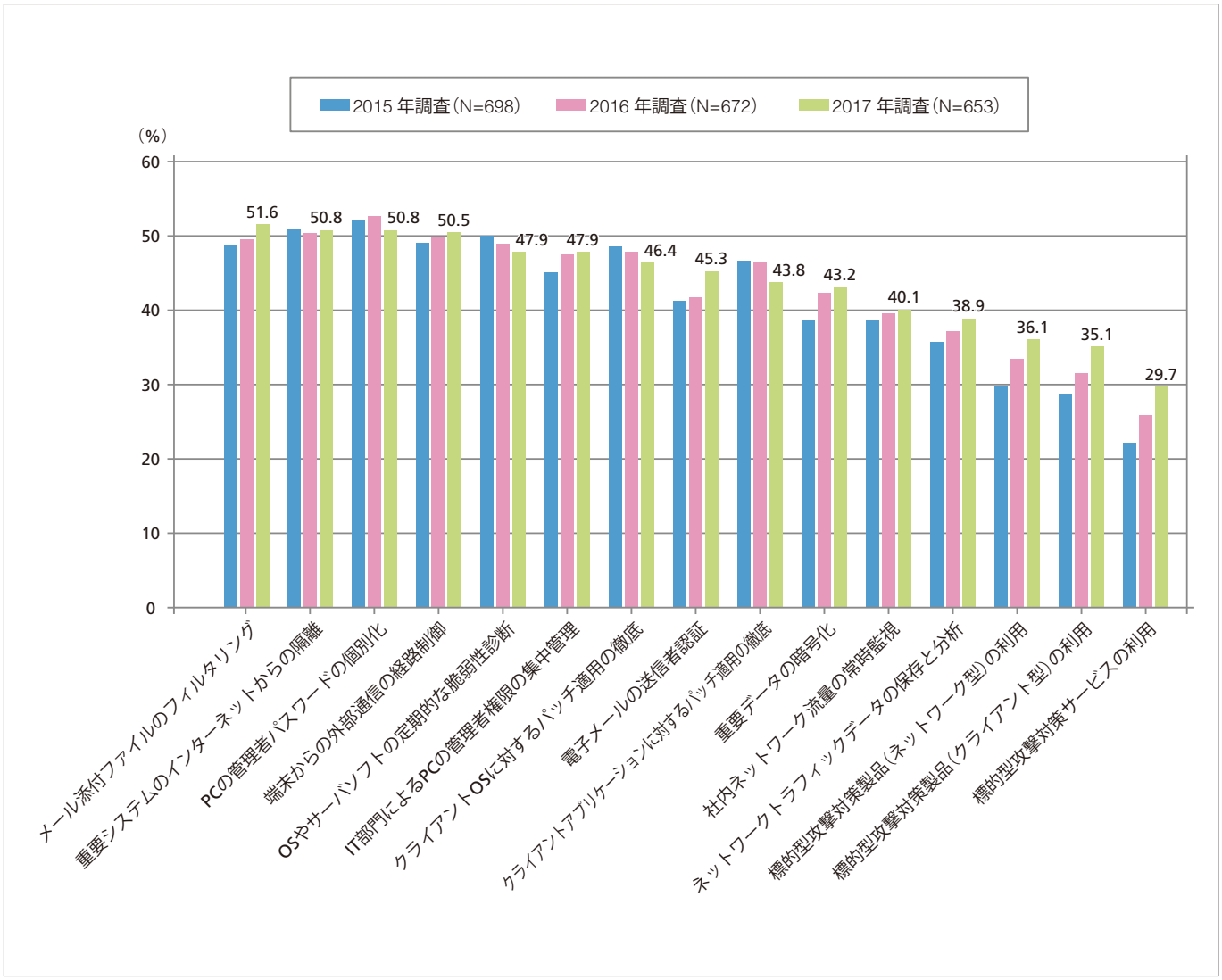

図8. 主要な「標的型サイバー攻撃対策」の実施状況の経年変化（2015～2017年調査）

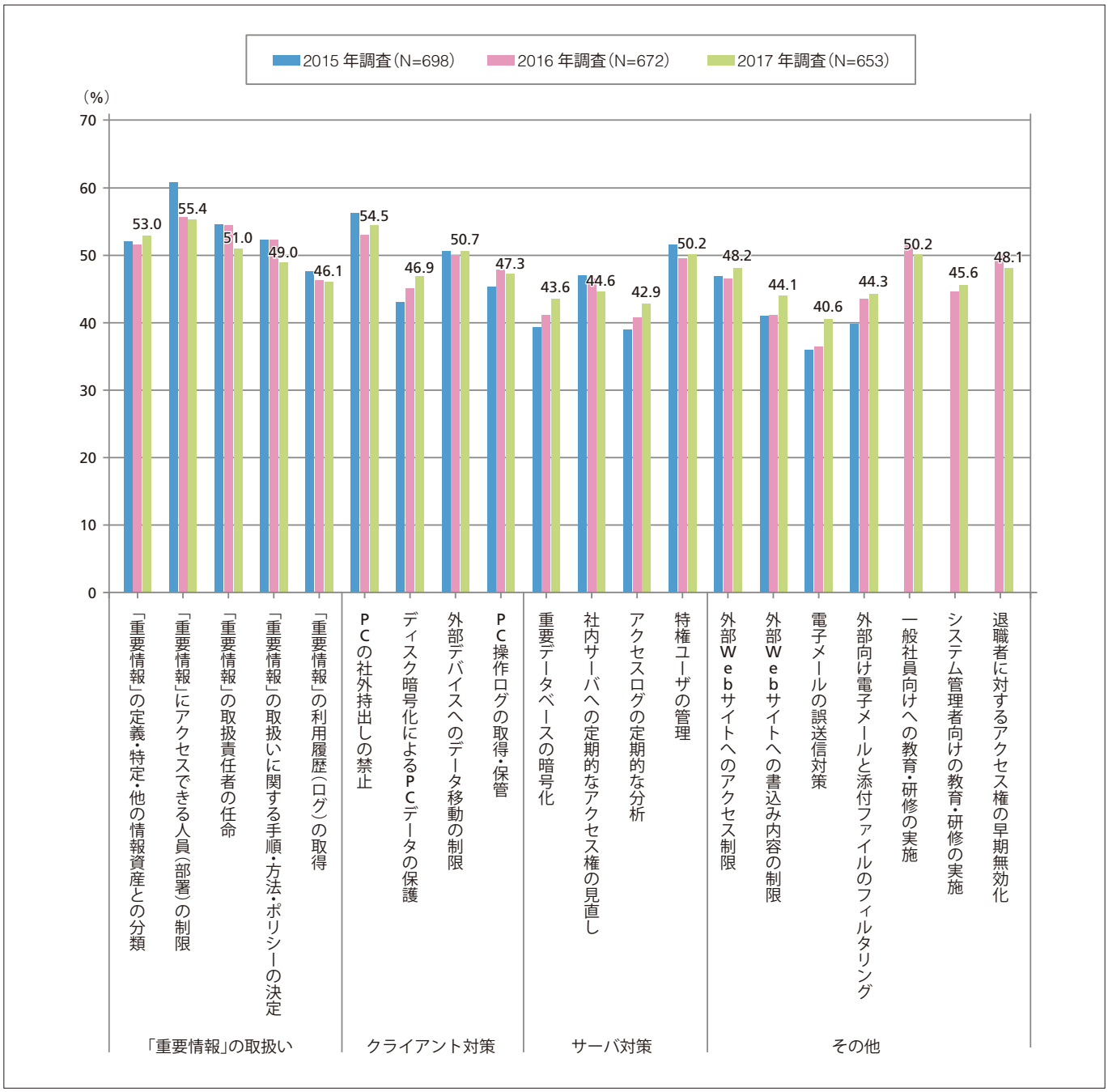

図9. 主要な「内部犯行対策」の実施状況の経年変化（2015～2017年調査）

2-5.増大傾向が見込まれるセキュリティ支出

セキュリティ上の脅威が高まっていることを如実に示しているのがセキュリティ支出の増大である。ここでは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、2017年度の支出の増減見込み（対前年度比）を調査した。

その結果、「増加する見込み」と回答した企業の割合は、全項目とも2桁台となり、そのうち「セキュリティ関連の認証取得に関する費用」をはじめ6項目は20%台に達した。それに対して、減少を見込む割合は全項目が1桁台にとどまった（図10）。

また、回答結果を指数化（増加を＋1、横ばいを0、減少を－1とした加重平均）し、その結果を過去3回の結果と比較したところ、ほとんどの項目が前回調査の指数を上回る結果となった。とりわけ「セキュリティ関連の認証取得に関する費用」「セキュリティ製品の利用・購入費（外部攻撃対策）」「セキュリティ製品の利用・購入費（内部犯行対策）」「認証基盤の構築・強化のための費用」「災害対策（ディザスタリカバリ対策）」の伸びが顕著である（図11）。

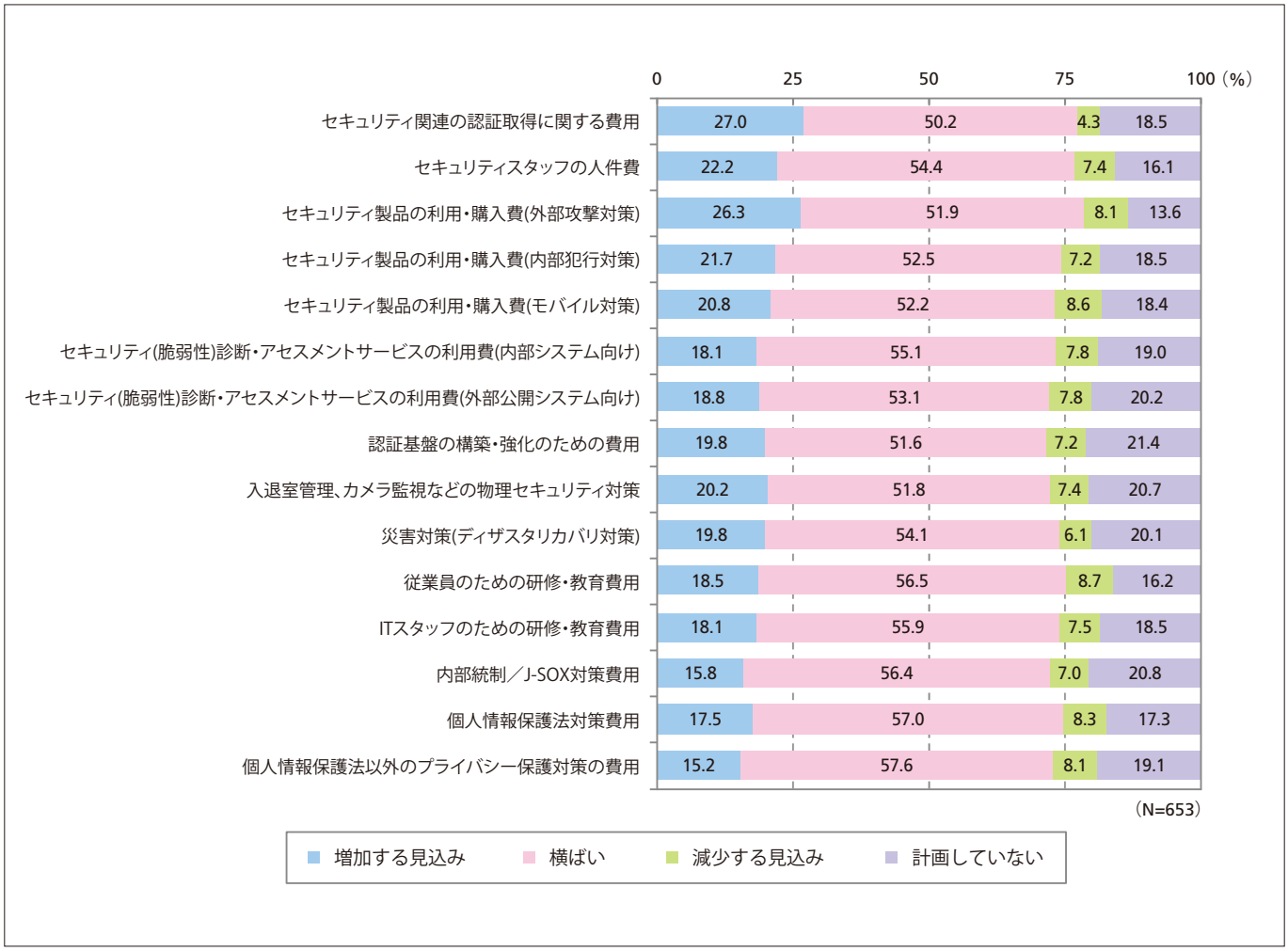

図10. 2017年度に想定されるセキュリティ支出の増減傾向

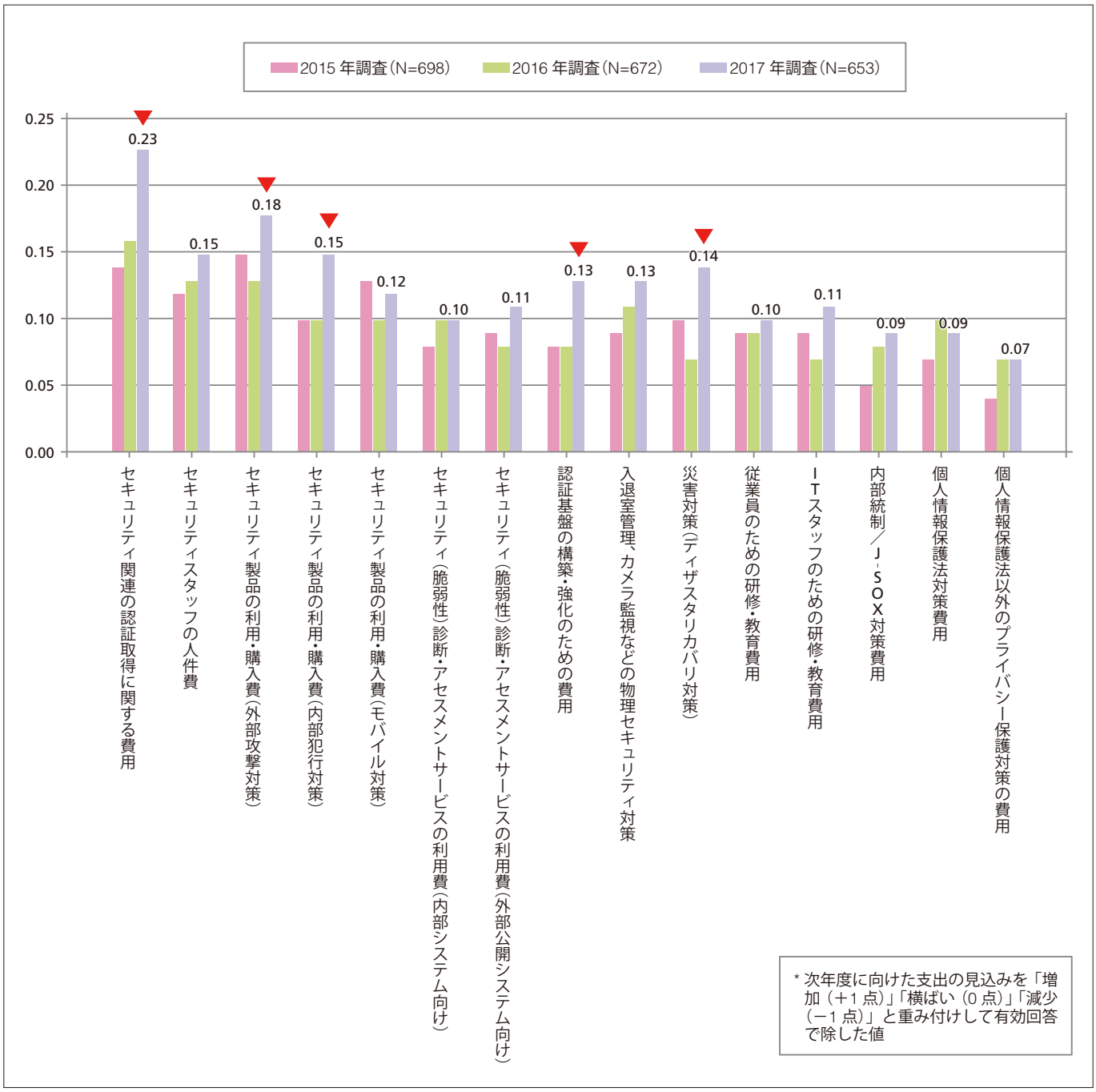

図11. セキュリティ支出の増減傾向の経年比較（2015～2017年調査）

3 情報セキュリティに関する認定／認証制度の動向

情報セキュリティにおける組織的な対応力を強化するための施策として、第三者による認定／認証制度が重要視されつつある。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も調査している。本章ではその最新動向を紹介する。

3-1.認知率、取得率では引き続きプライバシーマークとISMSが高い

国内において取得可能な代表的な認定／認証制度を8項目取り上げ、それぞれの取得状況と今後の取得意欲について問うた。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。これは例年と同様の結果である（図12）。

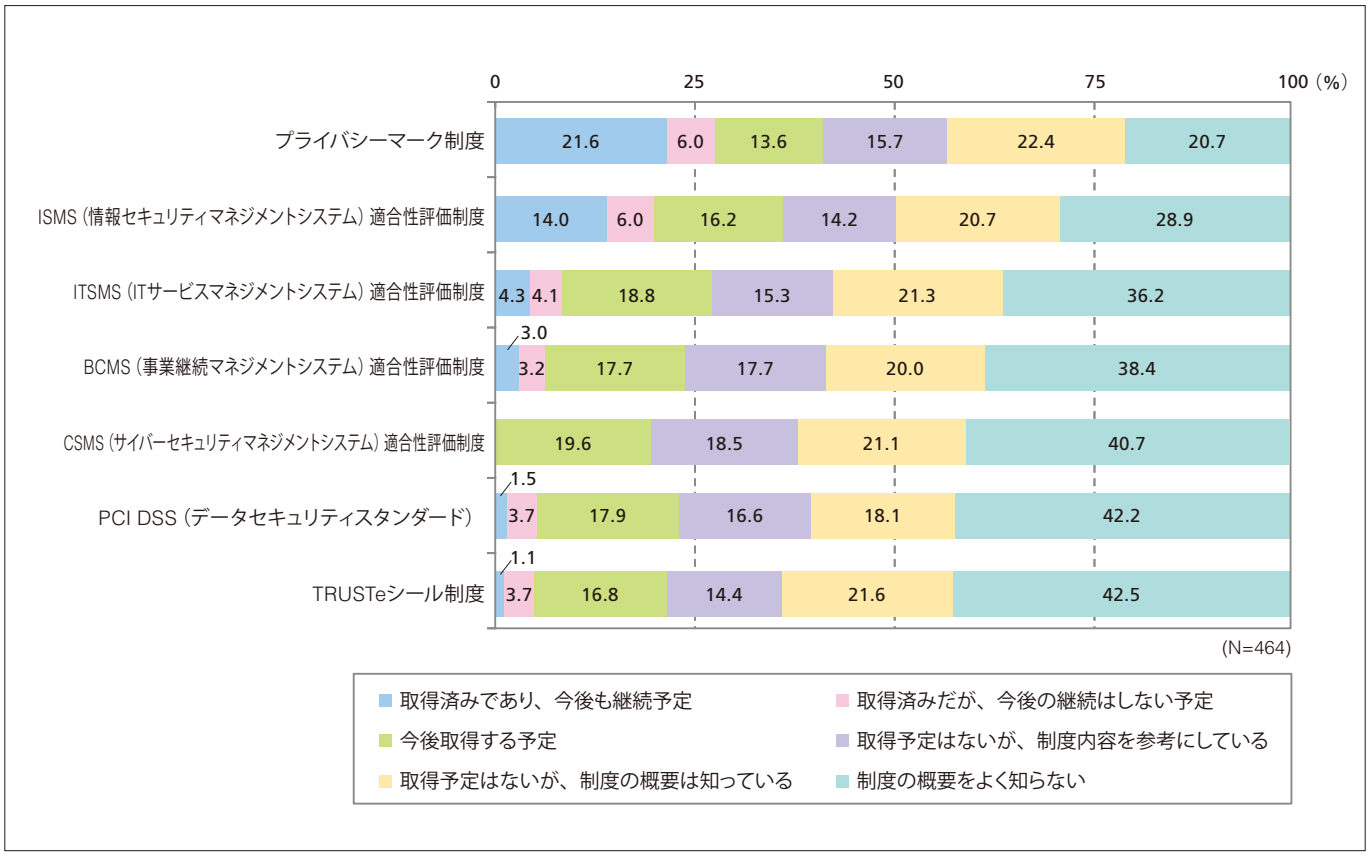

図12. 情報セキュリティに関わる認定／認証制度の取組状況

第三者認証の取得状況は業種による偏りも顕著である。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」への取組状況を業種別に見ると、情報通信業での取得率が50%を超えている反面、他の業種はその半分以下の水準にとどまっている（図13）。この傾向は、ISMS適合性評価制度など他の制度についても同様である。

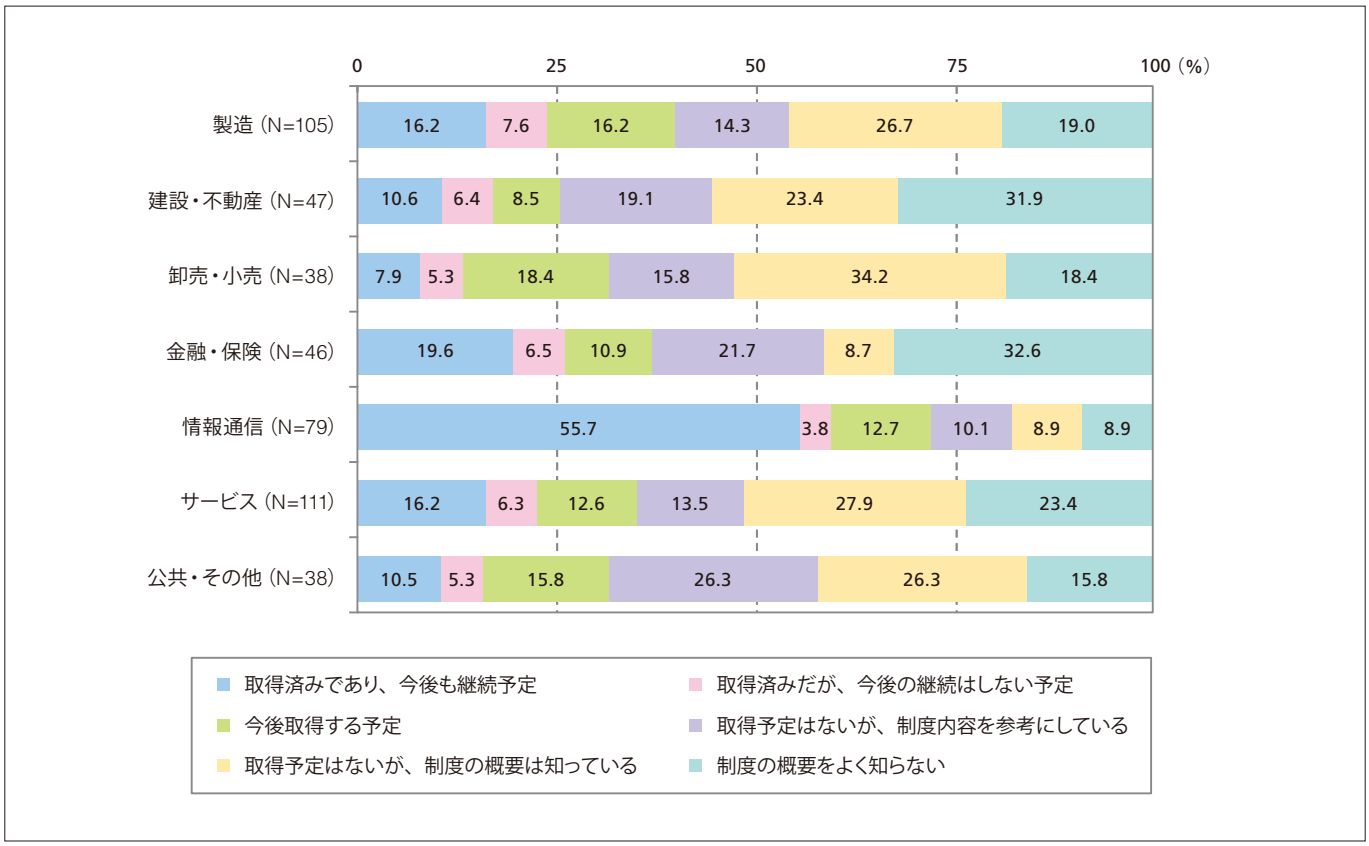

図13.「プライバシーマーク制度」に対する取組状況（業種別）

3-2.認定／認証を取得する価値

［2-5.増大傾向が見込まれるセキュリティ支出］にあるとおり、認定／認証の取得に関わる支出は伸びると見られている。では企業は、認定／認証を取得することに関して、どこにその価値を見いだしているのか。

今回の調査では、第三者認定／認証を取得することの価値について回答を求めた。実際にプライバシーマークを取得済みの企業と、今後取得を予定している企業、いずれにも当てはまらないその他の企業とに分けて集計した結果が図14である。すでに取得済みの企業では、「取引先からの信頼を得るため」が約70%と突出して高く、次いで「社内の情報セキュリティ体制を高度化させるため」（48.4%）が続いた。それに対して、今後取得を予定している企業では、「取引先からの信頼」（55.6%）も重視されているが、それとほぼ同じ比率で「消費者からの信頼を得るため」（50.8%）を選択する企業の割合が高いという結果になった（図14）。

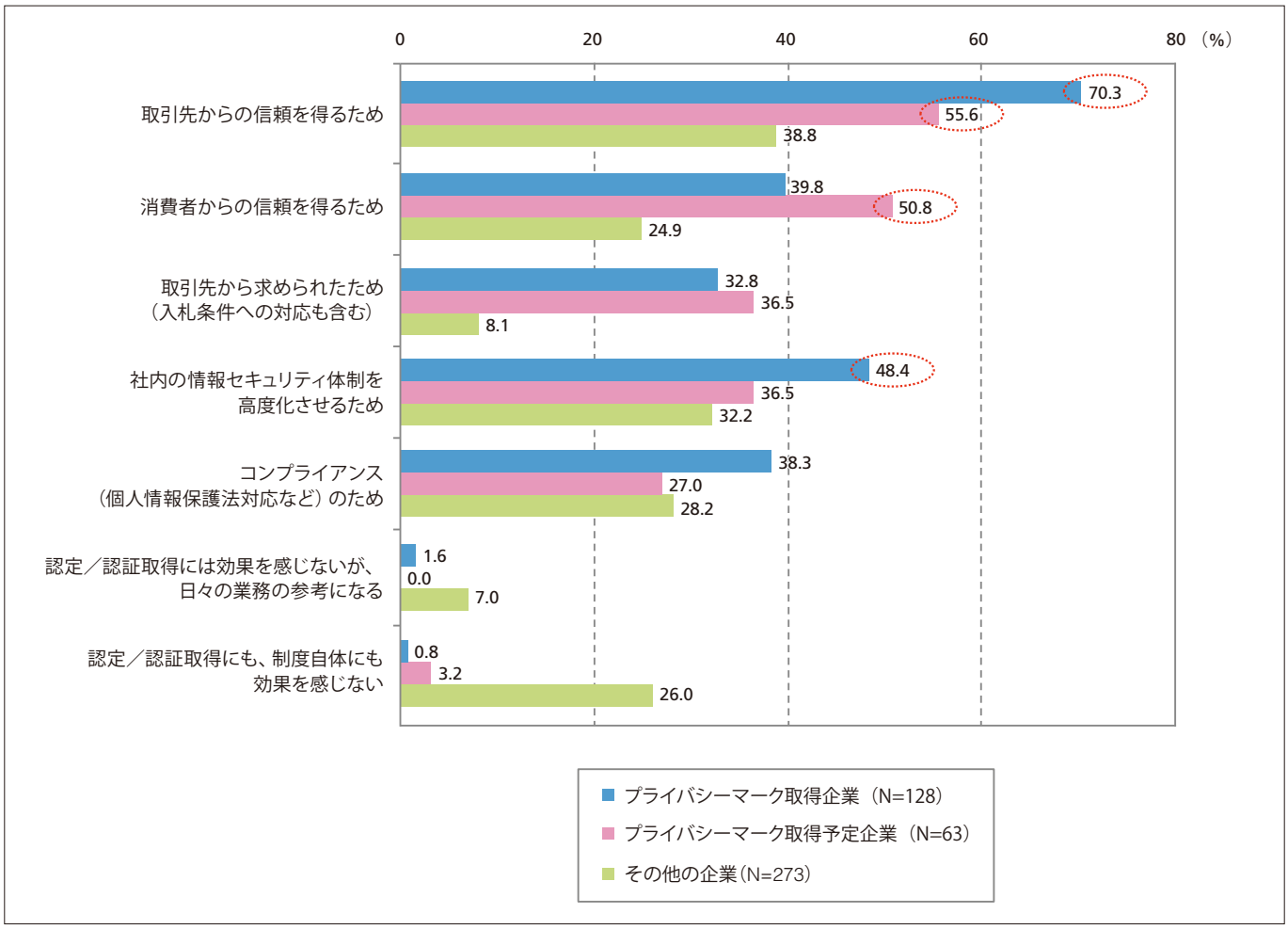

図14. 認定／認証を取得することの価値（プライバシーマーク取得状況別）

4 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。ここでは、改正個人情報保護法への対応状況とあわせて、グローバル企業にとって課題となりつつある海外のプライバシー規制への対応状況に焦点を当てた。また、2016年1月から本格的に運用が開始されたマイナンバー制度の取組状況も併せて紹介する。

4-1.改正個人情報保護法のインパクト

2017年度の法規制を巡る主要トピックの一つが、改正個人情報保護法の全面施行である。2005年の全面施行後、12年ぶりの改正となるが、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、行動履歴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。今回の調査（2017年1月時点）では、改正法の全面施行を直前に控えるなかで、国内企業の意識や取組みがどのように変化したかに着目した。

個人情報保護法の改正が自社にどのような影響をもたらすかについては、「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」と回答した割合が前年から増加したものの、そのうちの「大幅な変更・修正が必要」とした割合は過去2回と比較してほとんど変化がない（図15）。

今回の改正により、個人情報の保有件数が5,000件未満の企業も規制対象となることから、回答結果を個人情報の保有件数別に見ると、1,000～4,999件の企業においても、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」という結果となった（図16）。

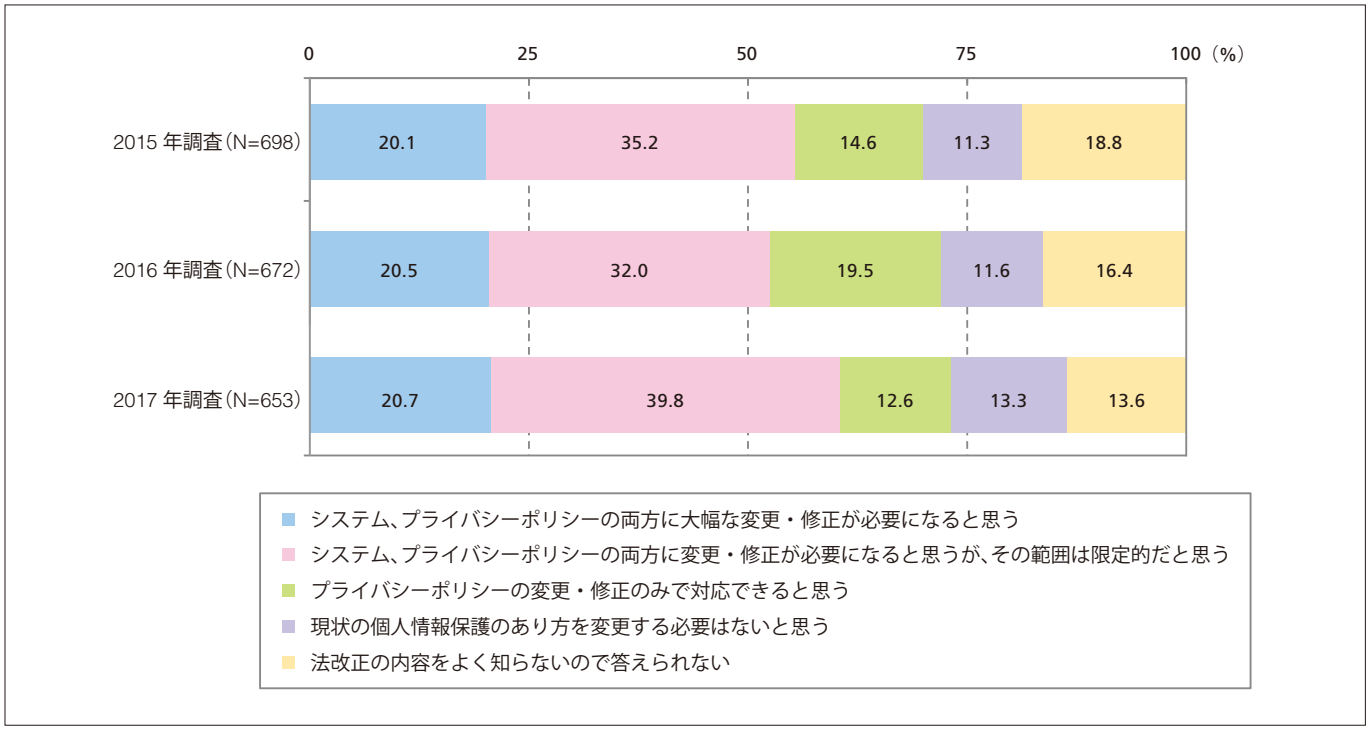

図15. 個人情報保護法改正が及ぼすインパクトの経年比較（2015～2017年調査）

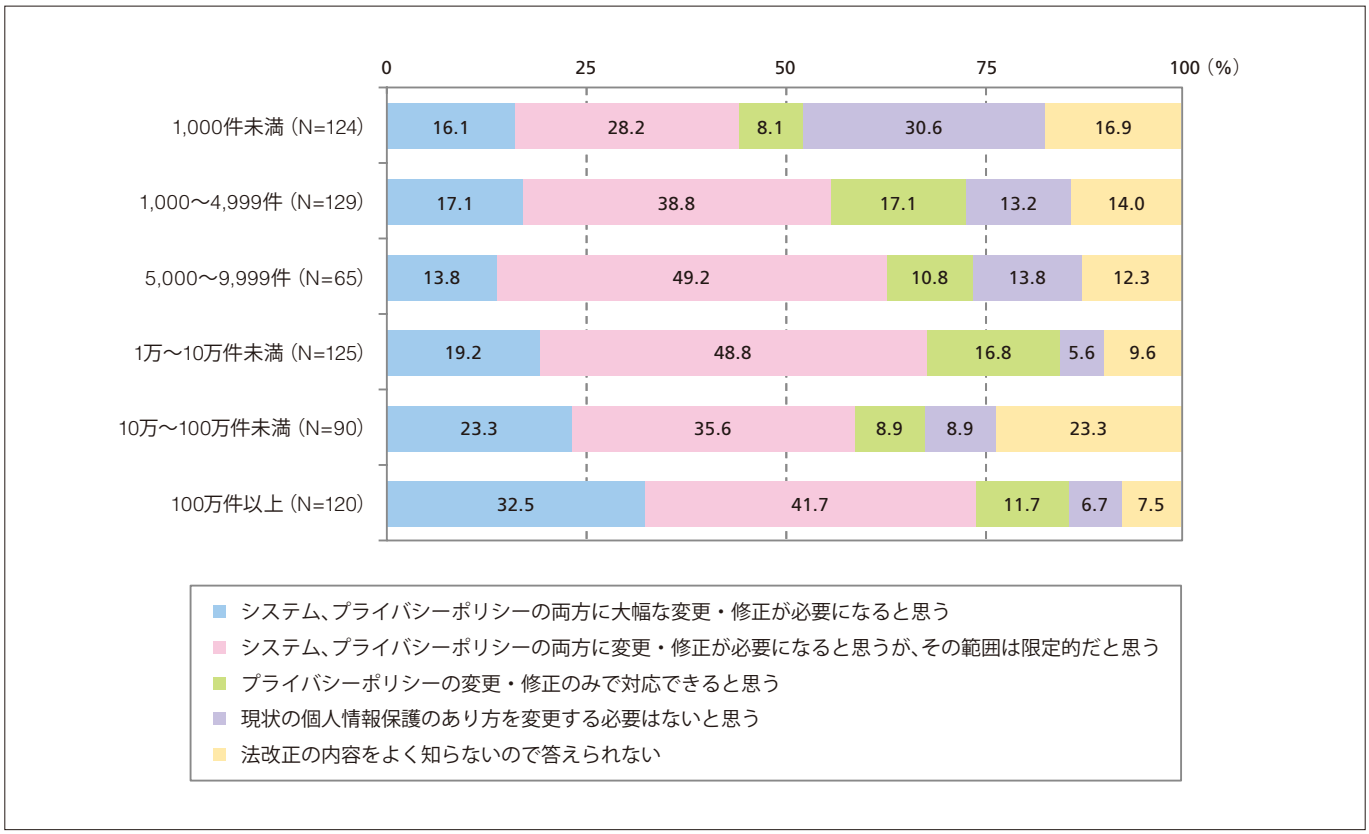

図16. 個人情報保護法改正が及ぼすインパクト（個人情報保有件数別）

改正法で注目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」を選択した回答が最も多く（36.8%）、次いで「要配慮個人情報の定義と範囲、取扱い」が27.9%となった（図17）。いずれも個人情報の定義に関わる問題であり、前年調査でも上位2項目を占めたものであるが、今回の調査結果で特徴的だったのは、前年調査時点で関心があまり高くなかった「匿名加工情報の定義と範囲、取扱い」（14.9%→24.7%）「個人情報保護委員会の役割と自社の関係」（11.5%→22.7%）に対する関心度が高くなったことである。改正法のポイントの一つである個人情報の活用のあり方や、法運用のされ方といった、より実践的なテーマが課題になっていると見られる。

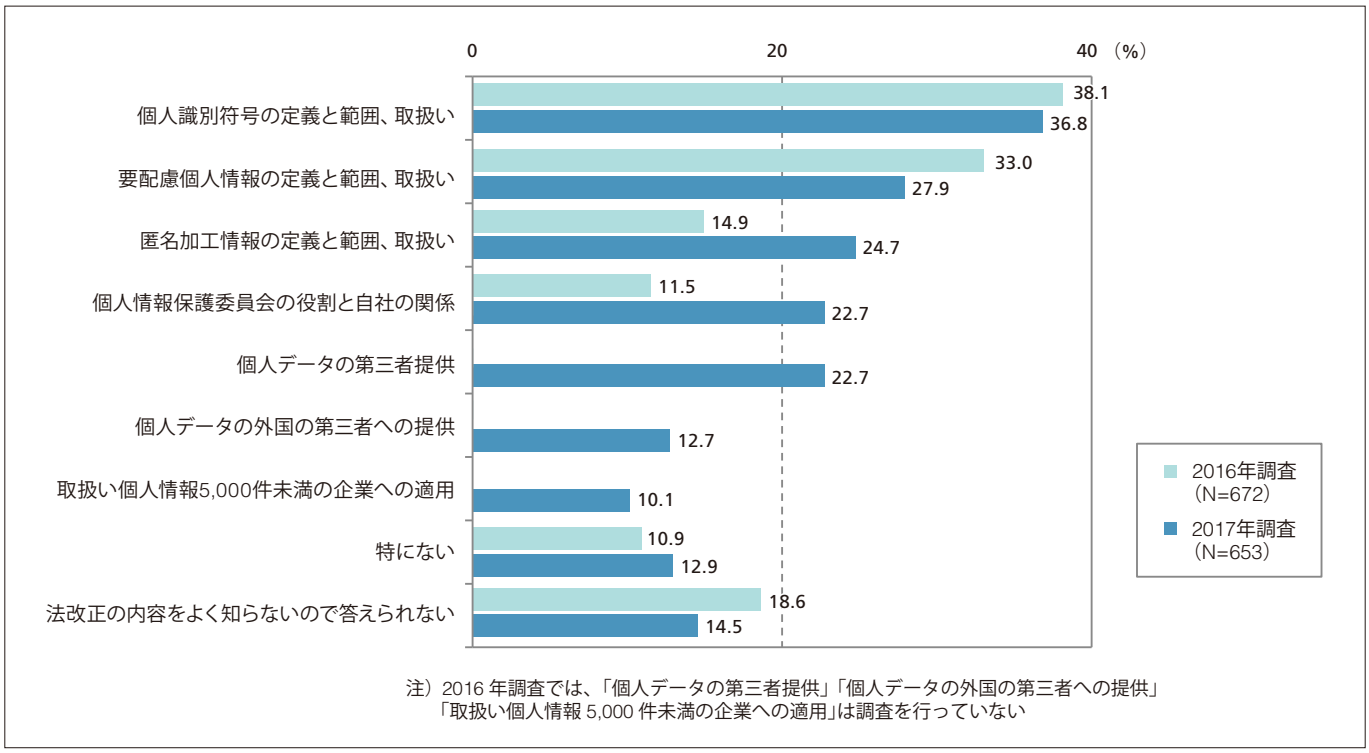

図17. 個人情報保護法改正で気にしている点の経年比較（2016～2017年調査）

4-2.改正個人情報保護法への対応状況

改正個人情報保護法の施行にあたり、なんらかの変更・修正が必要とした回答者（564件）に対して、その進捗状況を問うたところ、「すでに完了している」とする企業は2割強（22.0%）にとどまり、その一方で「全面施行（2017年5月）までには対応が完了する見込みである」とした割合が半数近く（46.3%）を占める結果となった（図18）。

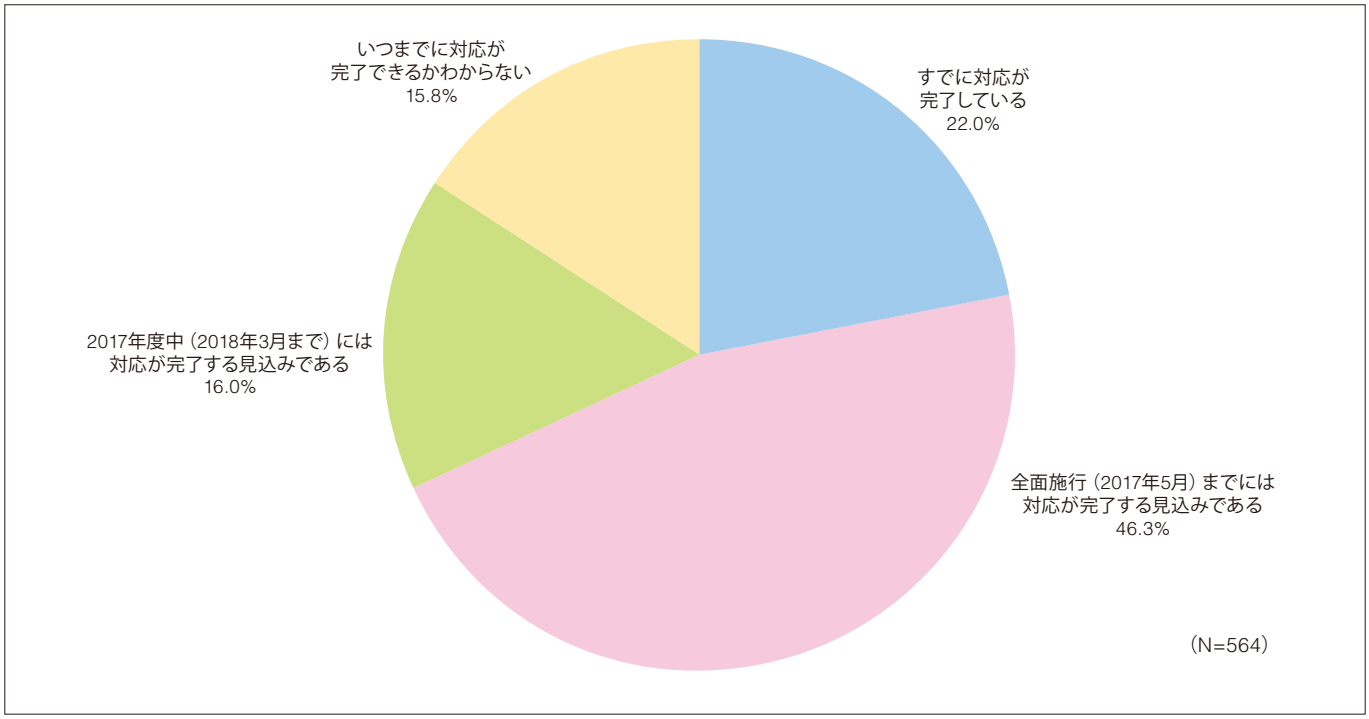

図18. 改正個人情報保護法への対応状況

4-3.EUプライバシー規制への対応状況

今回の調査では、グローバル企業の間で課題となりつつある海外のプライバシー規制への対応状況についても設問項目に加えた。とりわけ、厳しいプライバシー規制を設けていることで知られるEU（欧州連合）域内に事業拠点または顧客をもつとした回答者（189件）に対して、EU域内居住者の個人情報の域外への移転を制限する「EUデータ保護指令（2018年5月から「EU一般データ保護規則」として施行予定）」への対応状況について調査したところ、「規制の存在を初めて知った」（16.4%）と「規制の存在は知っているが勤務先がどのように対応しているかは知らない」（38.6%）で半数を超え、規制対応にIT／セキュリティ従事者があまり関与していないことが明らかとなった。また、「規制に触れぬよう、個人情報は移転しないようにしている」「規制を特に気にすることなく個人情報の移転を行っている」とした割合はそれぞれ13.2%、「規制にのっとったかたちで適正に個人情報の移転を行っている」とした回答はわずか2割弱（18.5%）にとどまった（図19）。

欧州で事業を展開するうえで、いまや顧客や従業員のプライバシーへの配慮は絶対条件であり、その規制対象は世界中の顧客がターゲットとなりうるインターネットビジネスを手がける企業にも及ぶ。現地に拠点を構える企業では、人事系システムの要件などにも影響が及ぶことから、IT部門としても早急に対応状況を確認することが求められる。プライバシー規制への対応を不十分のまま放置しておくことは、グローバルビジネスの競争力を削ぐことにもなりかねない。

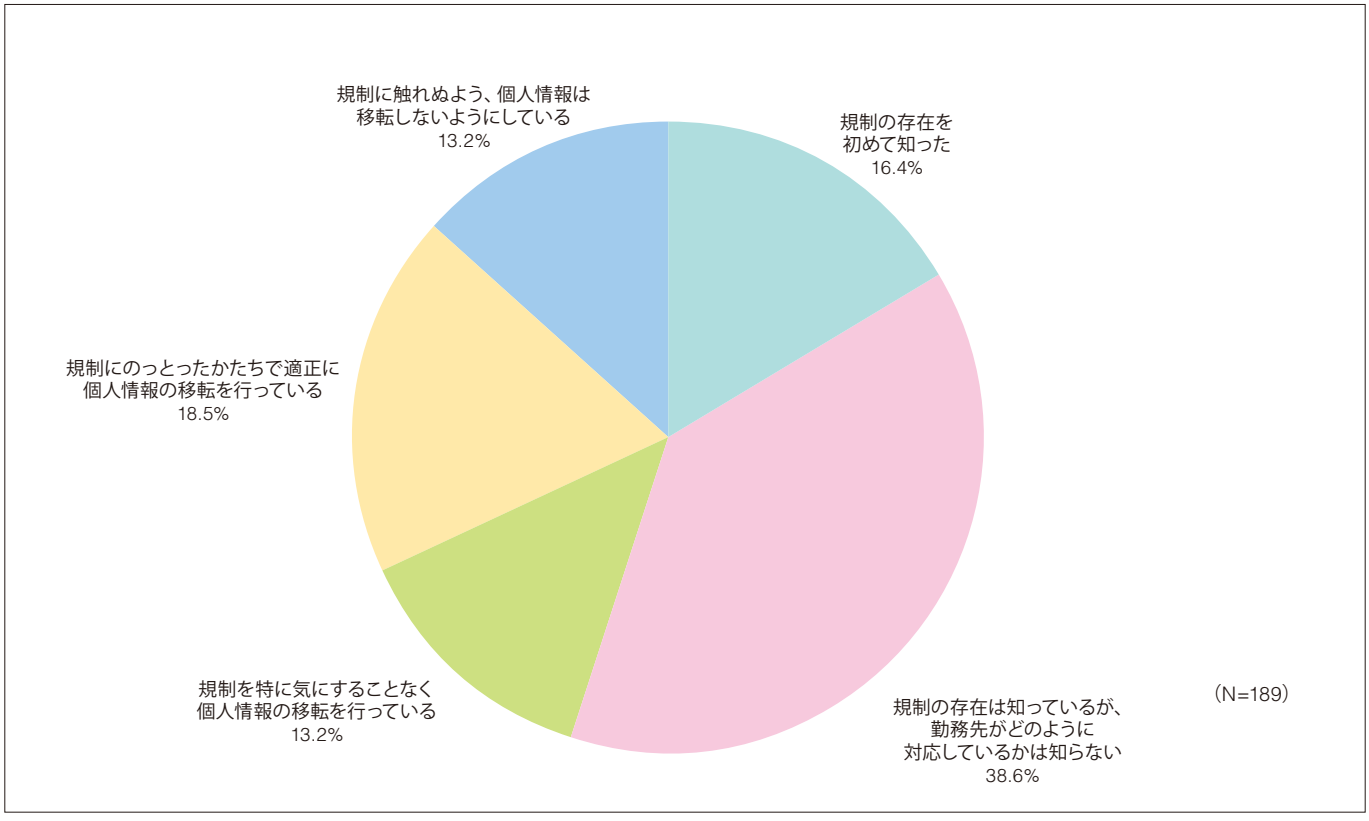

図19. EUのプライバシー規制への対応状況

4-4.マイナンバー制度の対応状況

近年、IT部門にとって法対応の主要テーマであった「マイナンバー制度」への対応状況は、制度運用から1年が経過したにもかかわらず、前年の調査結果から大きな進展が見られなかった。同制度に対する情報システムの対応は、前年調査では取組みが大きく進展したものの、今回の調査では「完了している」とした企業の割合が前年調査から約6ポイント伸びるにとどまった（31.8%→38.0%）。また、「作業が進行中」とした企業の割合は逆に約6ポイント減少（32.0%→25.9%）し、実際に対応作業を行っている企業の裾野はほとんど拡大していないことも明らかとなった（図20）。

社会全体としてマイナンバーの活用が十分に進んでおらず、企業としても情報漏えい時のインパクトが測りにくいという事情があるとはいえ、この結果を見ると、マイナンバー制度対応は明らかにトーンダウンしていると言える。

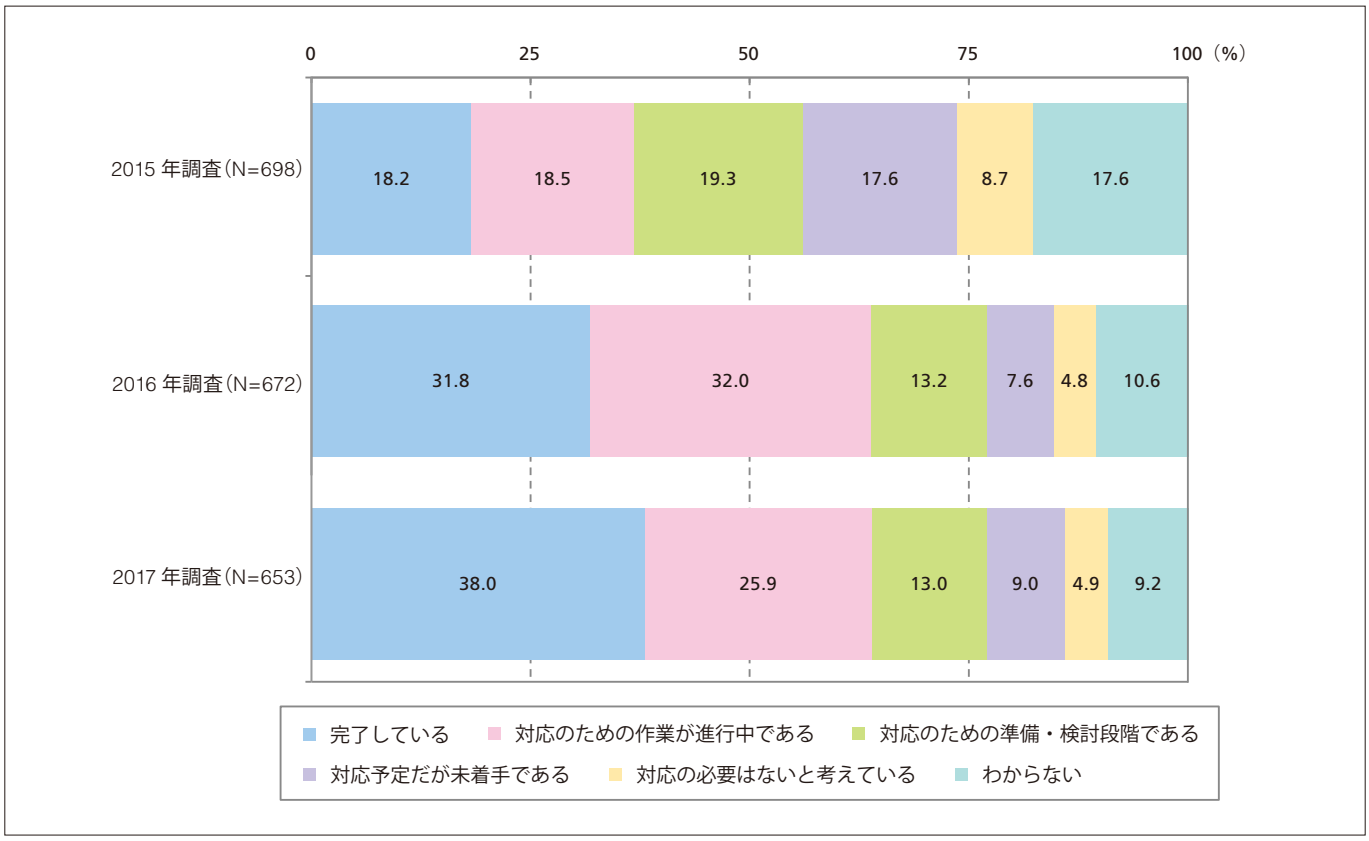

図20.「マイナンバー制度への情報システムの対応状況」の経年変化（2015〜2017年調査）

前年調査同様、対応が完了していないとした回答者にその理由を問うたところ、「システム化予算の不足」をあげる企業が最も多く（25.6%）、前年調査結果（18.3%）を上回った（図21）。情報セキュリティ支出は全体としては増加傾向にあるものの、限られた予算の充当先として優先順位を下げた企業も多いと推察される。

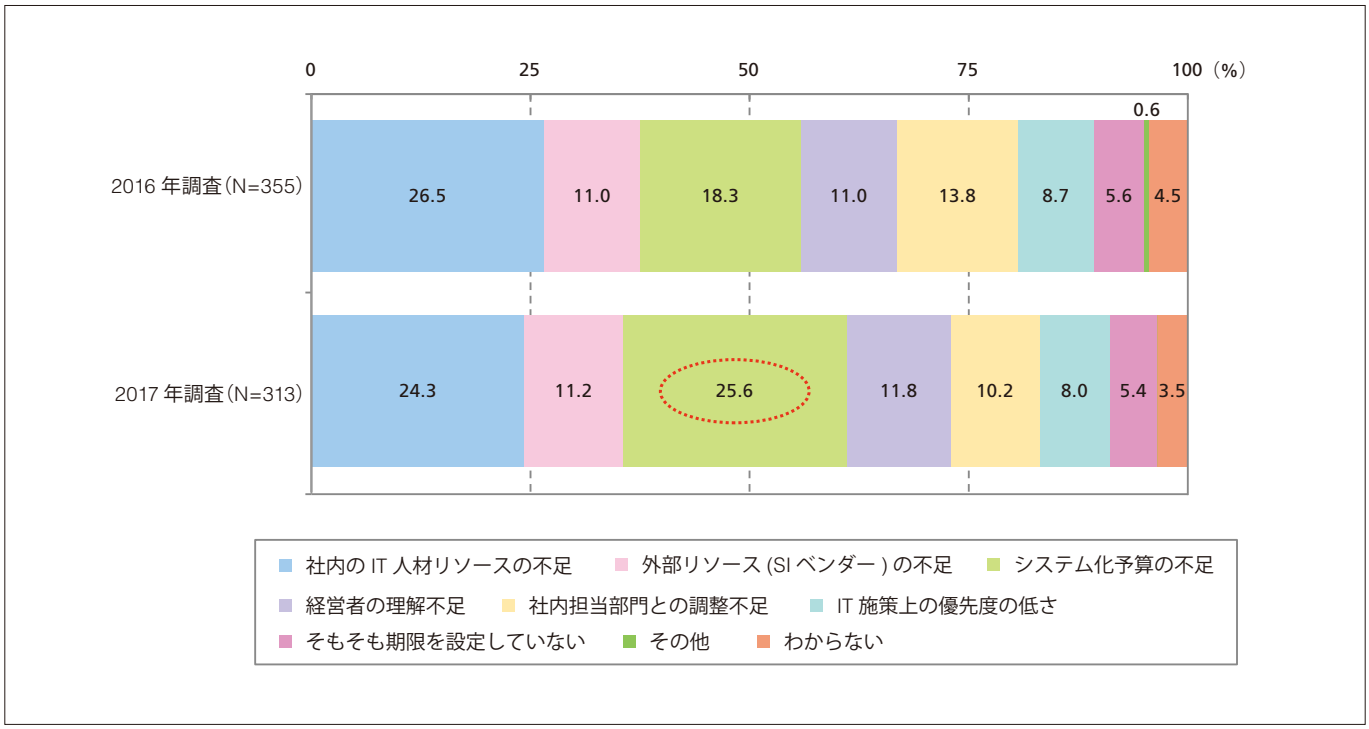

図21. 情報システムの対応が完了していない理由の経年変化（2016〜2017年調査）

5 働き方改革とセキュリティ対策

現安倍政権が重要政策の一つと位置づけている「働き方改革」もまた、企業の間で急速に関心が高まっているテーマである。この取組みを推進するうえではIT活用と柔軟性の高い就労制度の両立がカギとなるため、必然的に情報セキュリティ対策が課題とされるケースが多い。そこで、今回の調査では、この働き方改革の推進状況とセキュリティ対策との関連性について調査項目に追加した。本章では、スマートデバイスの活用状況とあわせてその結果を紹介する。

5-1.スマートデバイスの導入状況

毎年恒例となっているスマートデバイス（スマートフォン、タブレット）の導入・活用状況について、スマートフォン、タブレットの会社支給と私物利用許可の双方についての取組状況を見ると、「会社支給によるスマートフォンの導入」および「会社支給によるタブレットの導入」は、「試験的に実施」までを含めれば導入率がいずれも60%台となった。それに対して、私物端末の業務利用（すなわちBYOD）の実施率は、スマートフォン、タブレットともに30%台と低い水準にとどまっている（図22）。

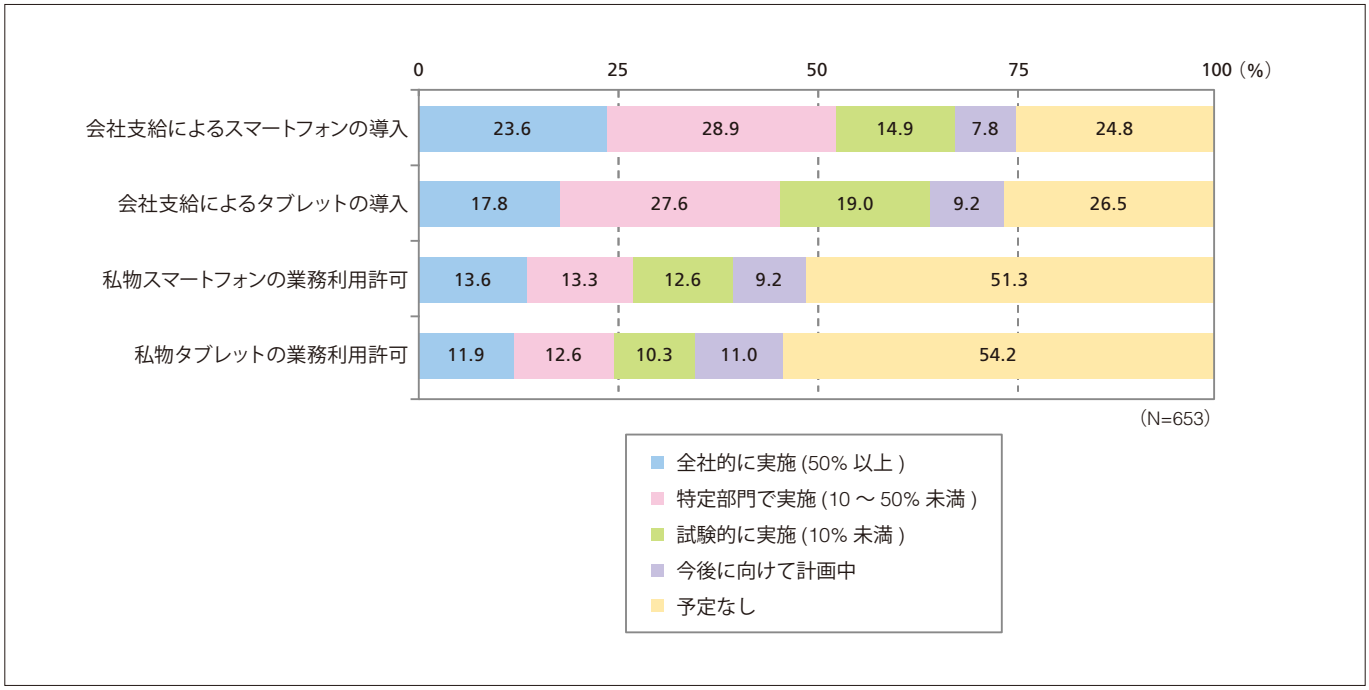

図22. スマートデバイスの導入状況

会社支給によるスマートフォンとタブレットの導入状況について、本調査を開始した2013年から経年で比較すると、2016年までは「今後に向けて計画中」を含め、スマートデバイス導入の意向をもつ企業の割合に変化はあまり見られなかった。だが、今年の調査では、スマートフォン、タブレットともにその裾野が拡大し、「予定なし」の割合が大きく減少していることがわかる（図23）。その背景には働き方改革に対する関心の高まりも関係していると考えられる。

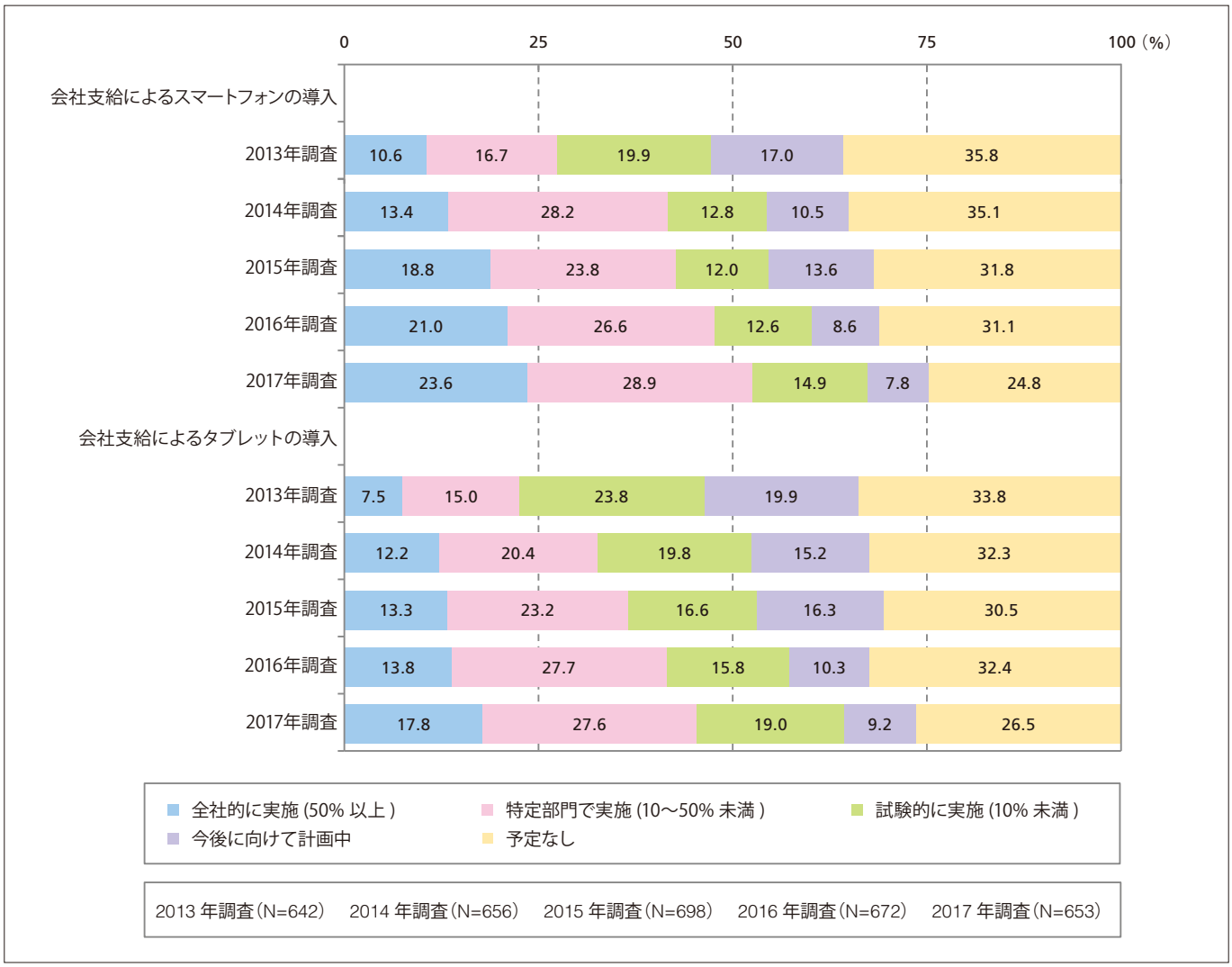

図23. 会社支給によるスマートフォンとタブレットの導入率の経年比較(2013～2017年調査)

5-2.働き方改革の実施状況

働き方改革という取組みは、そのスコープがきわめて広いが、今回の調査では、代表的な施策5つについて各社の取組状況を問うた。調査時点での実施率が最も高かったのは「全社的に業務のペーパーレス化の推進が行われている」(28.9%)で、2番目で高かった「働き方(ワークスタイル)変革が経営目標として掲げられている」(26.8%)とともに4分の1以上の企業が「実施中である」と回答した(図24)。

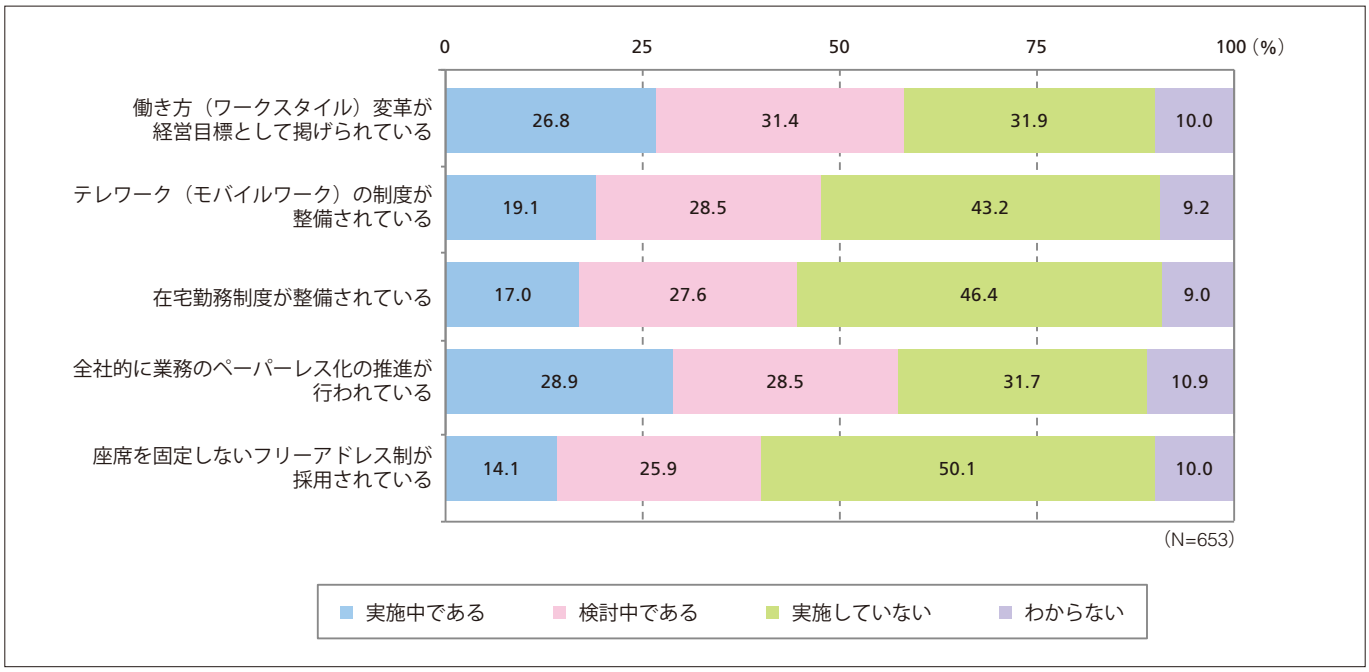

図24. 働き方改革に向けた主要施策の取組状況

5-3. 働き方改革と関わるセキュリティ対策の実施状況

次に、ITの活用を前提とした働き方改革を推進するうえで重視されることの多いセキュリティ対策を10項目選び、現在の実施率と今後の計画について調べた。調査時点では、スマートデバイスの管理にまつわる項目の実施率が高く、「リモートロック／ワイプ環境の整備」が34.2%、「スマートデバイスに対するアプリ／機能の利用制限」が30.2%の企業で実施されている。

一方、現在の実施率は高くないが、今後に向けて実施したいと考えている割合が高い項目としては「在宅勤務、テレワーク用のセキュリティ規程の整備」（22.1%）と「在宅勤務、テレワーク用の従業員向けセキュリティ教育」（20.8%）があげられる。今後、ソフト面での取組みが重視されることが見込まれる（図25）。

今回の調査結果から明らかになったのは、働き方改革を積極的に推進する企業ほど、セキュリティ対策や安全に情報を共有するためのツールの活用が先行しているという実態である。たとえば、働き方改革を経営目標に掲げていたり、在宅勤務／テレワーク制度を運用中の企業では、スマートデバイスの管理や端末にデータを残さないためのリモートデスクトップ環境、メール以外の情報共有ツールの利用率が全体平均の約2倍に達したほか、在宅勤務／テレワークのためのセキュリティ規程やセキュリティ教育も積極的に行われているという傾向が示された（図26）。ITによる働き方改革においては、セキュリティ対策も同時に進めることが求められていると考えられる。

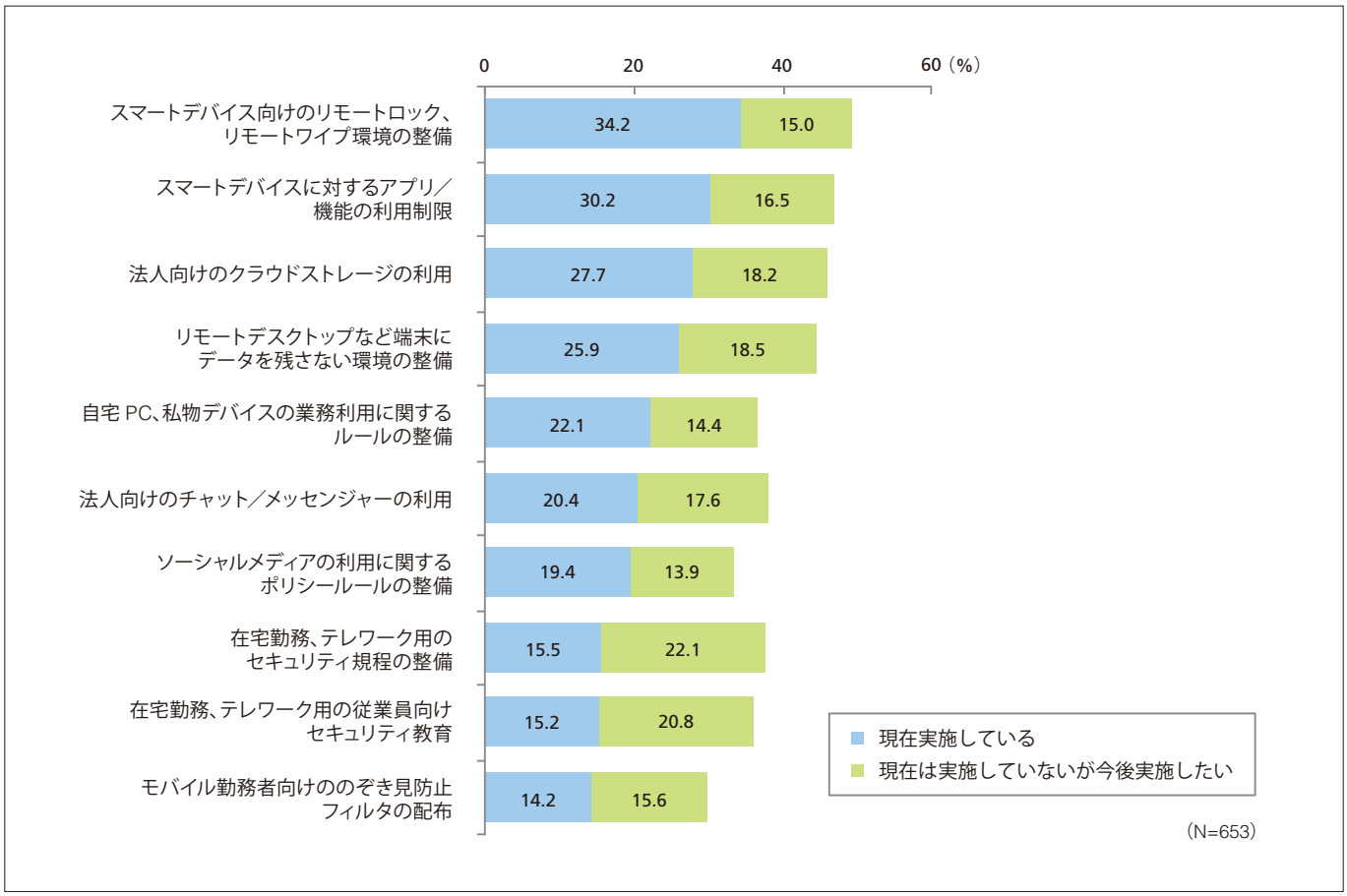

図25. マイナンバー制度対応における問題点

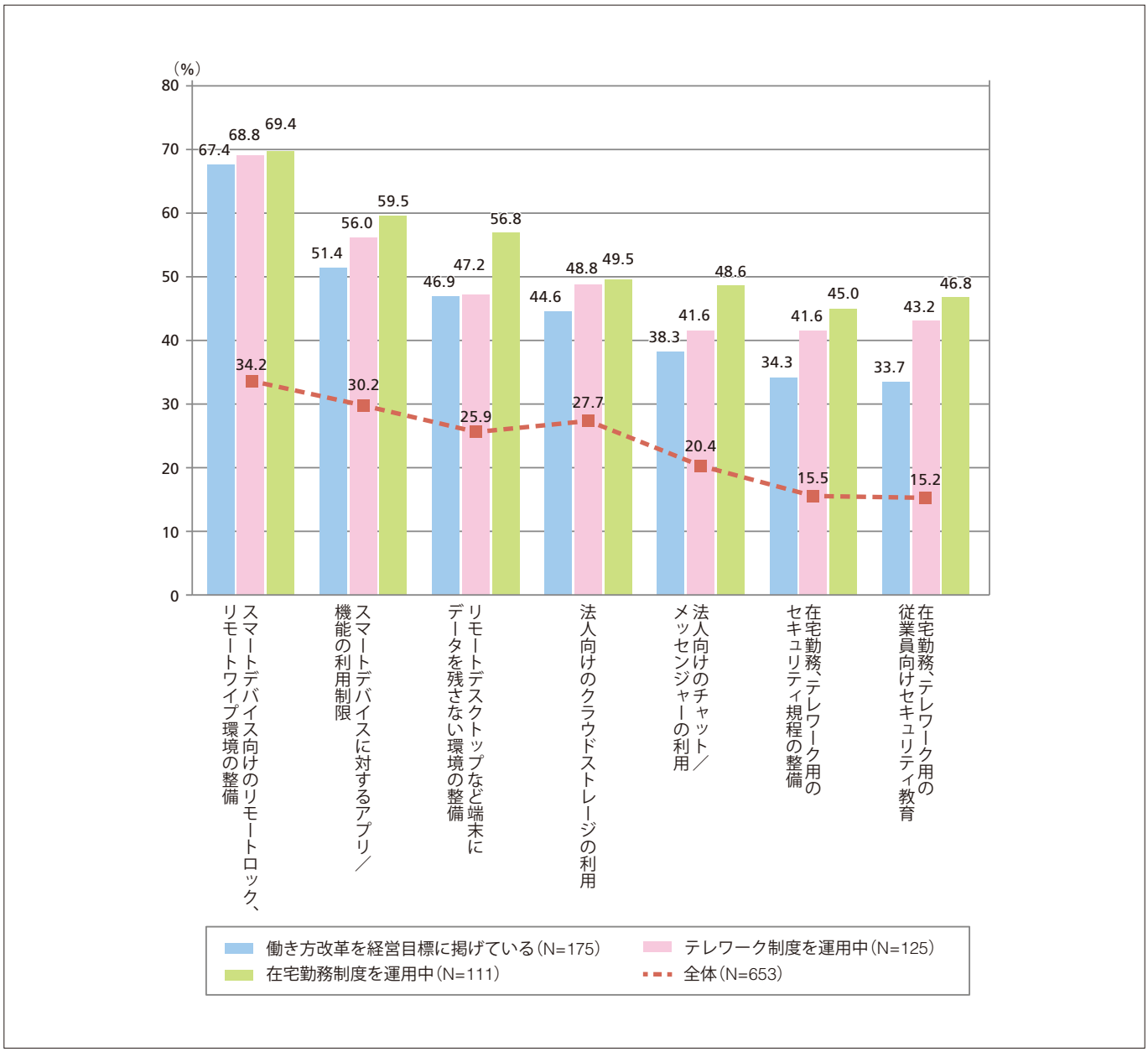

図26. 働き方改革の実施状況とセキュリティ対策との関係

5-4.電子契約の導入状況

働き方改革と関連して、企業では紙ベースで行っている業務をデジタル化しようとする動きも進展してきている。その一つの例が契約業務である。本調査では、電子契約の利用状況についても調査しているが、今回の調査では、利用率が着実に上昇していることが確認された。

電子契約の実現手段としては、一つの組織、部門が複数の取引先と電子契約を行う「1対N型」のシステム環境が多いが、複数の部門、取引先間で電子契約を行える「N対N型」システムの利用も進展している。また、今後に向けて電子契約の採用を検討している企業の割合も2016年調査の10.4%から約5ポイント上昇している。電子契約は、今後に向けて採用が大きく進む有望分野の一つであると見られる（図27）。

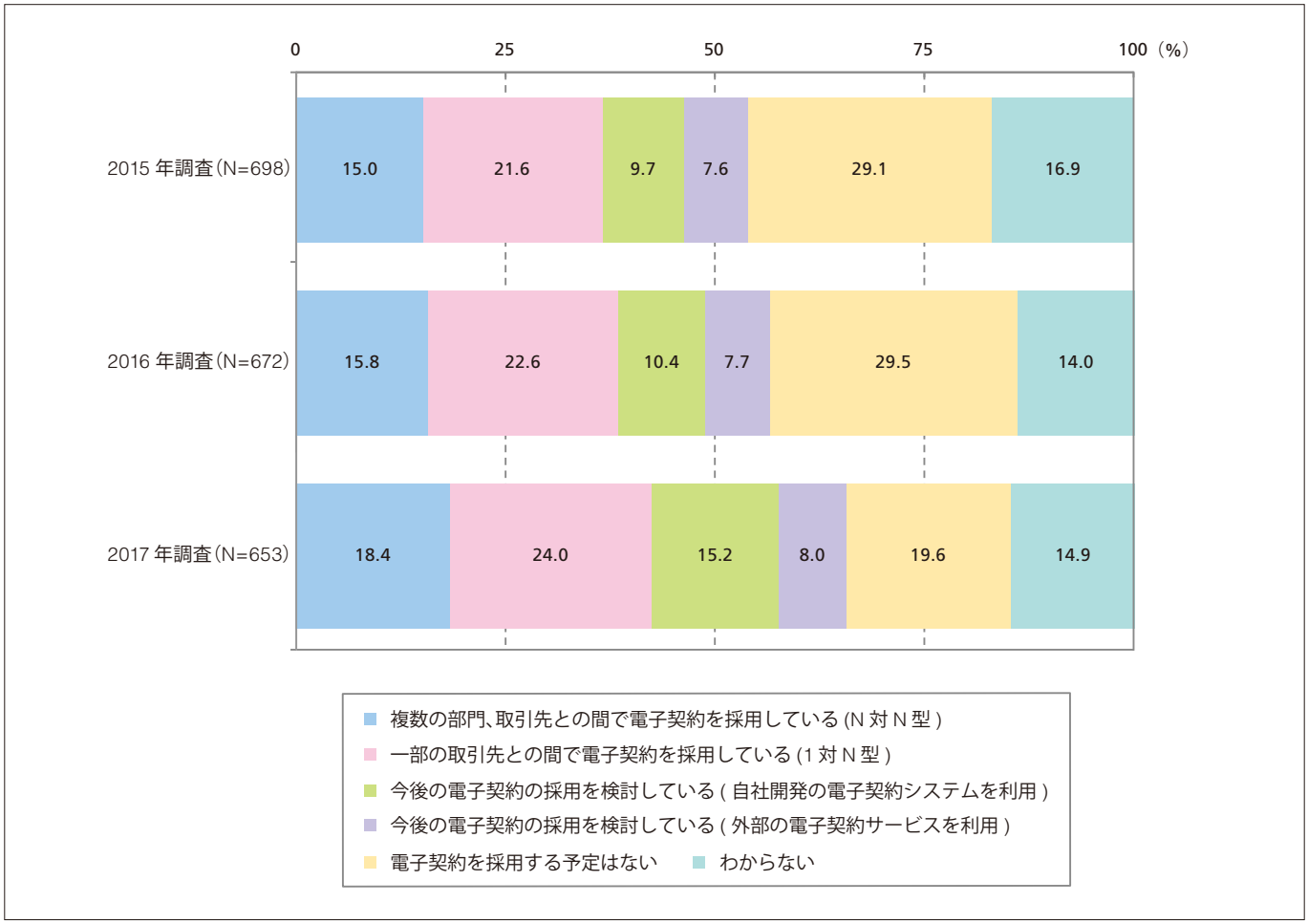

図27. 電子契約の利用状況の経年比較（2015～2017年調査）

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

ネットワークセキュリティ製品は、近年、企業においてもっとも積極的な投資が行われている分野である。項目別に見ると、「ファイアウォール」の導入率が最も高く（71.7%）、「VPN」（52.7%）「URLフィルタリングツール」（46.1%）が続いている。また、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」（17.2%）、フォレンジクスツール（16.2%）などがあげられる（図28）。

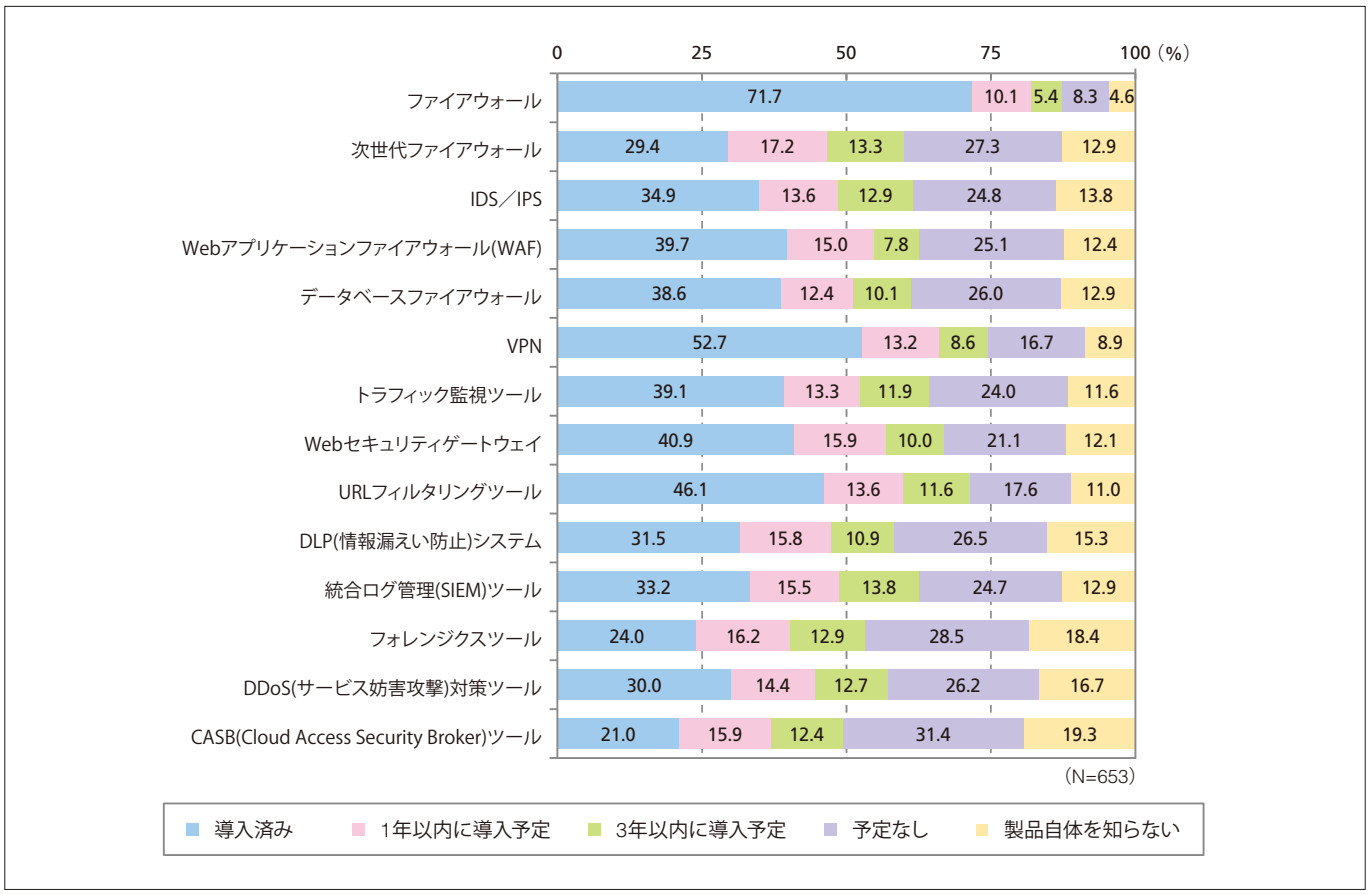

図28. セキュリティ製品の導入率（ネットワークセキュリティ）

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は過去の調査と比べ特に変化はない。今後に向けては、「シンクライアントシステム」の1年以内の導入を予定している割合が高い（図29）。

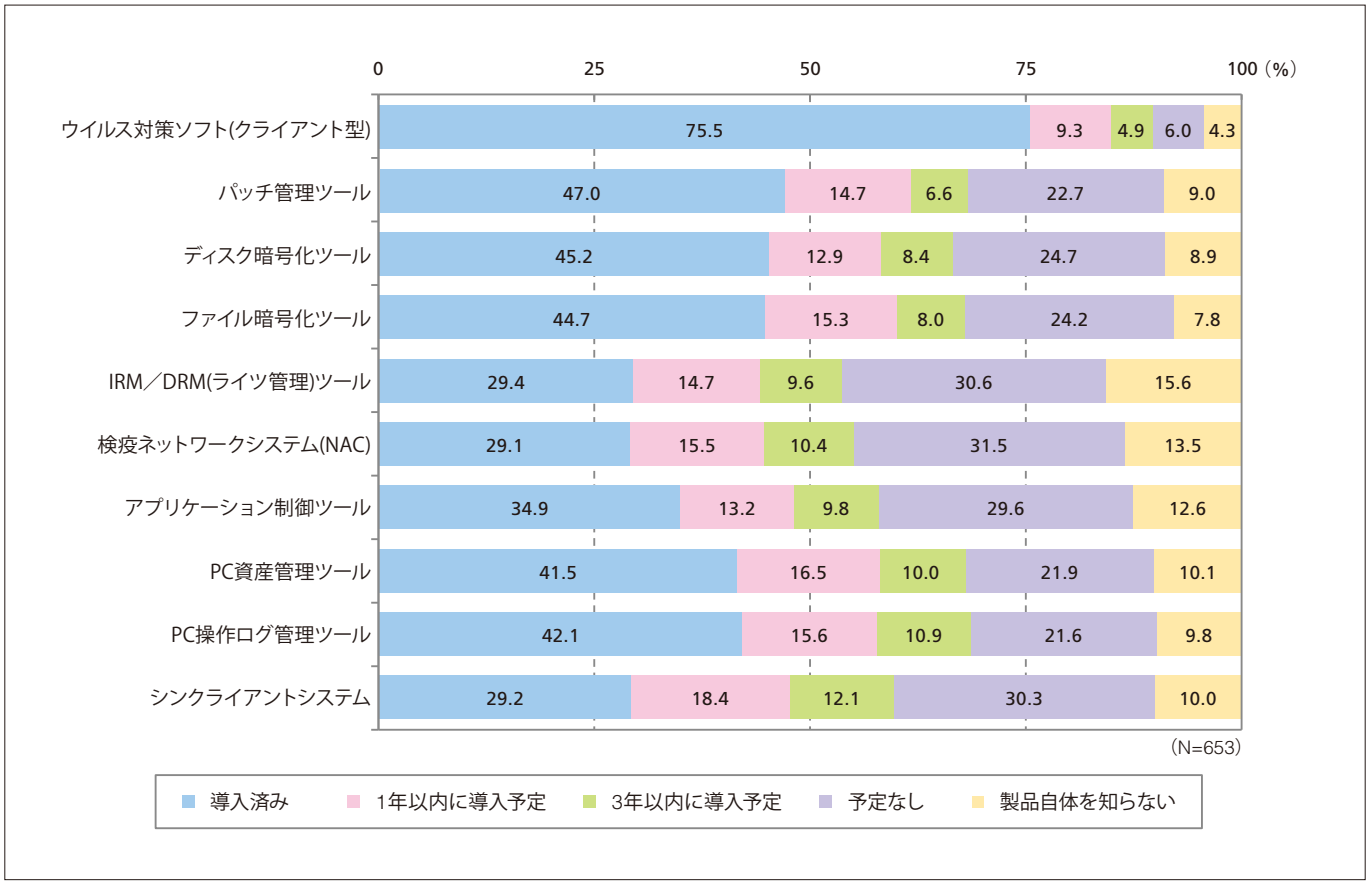

図29. セキュリティ製品の導入率（クライアントセキュリティ）

6-3.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は、近年利用率が上昇している有望分野である。今回の調査で取り上げたサービスの中で、脆弱性診断サービスの利用率が最も高く、なかでも社内サーバ向けの脆弱性診断は半数を超えた(50.8%)。投資対効果が見えにくいセキュリティ対策の中で、自社システムのセキュリティレベルを定量的に把握するための手段として利用率が高いと見られる(図30)。

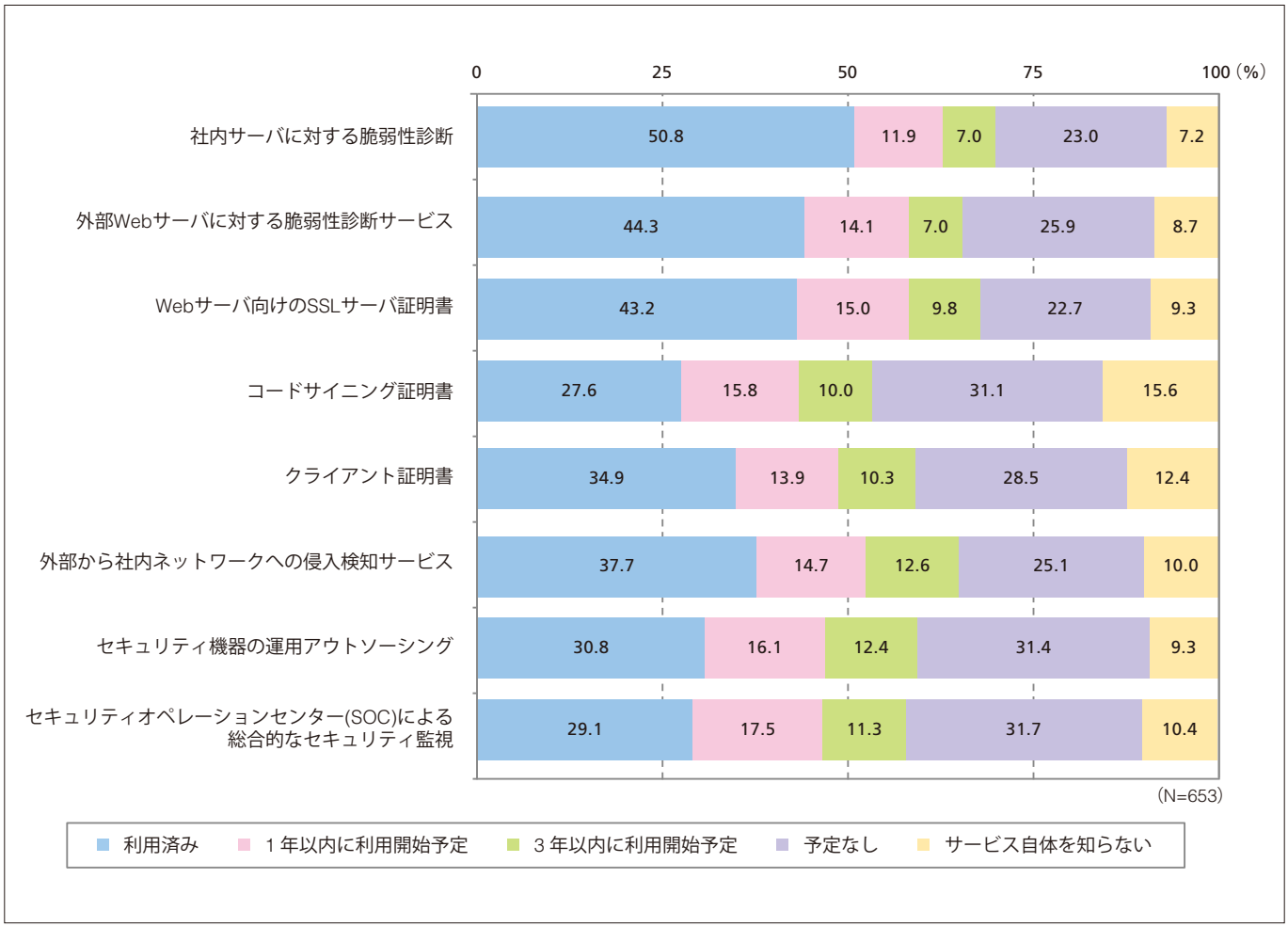

図30. セキュリティ製品の導入率(セキュリティサービス)

また、各種セキュリティ機器の運用アウトソーシング、専門スタッフによる監視などを行う、セキュリティオペレーションセンタ(SOC)といったアウトソーシングサービスも、1〜3年以内の利用開始予定とする回答が29%弱と高く、今後に向けて注目が高まると予想される。

6-4.電子メールのセキュリティ対策の実施状況

［2-4.セキュリティ対策の進展状況］の「標的型サイバー攻撃対策の実施状況」でも企業において実施率が高まっていることが確認された電子メールのセキュリティ対策について、今回の調査でより詳細な実態を回答してもらった。送信者、受信者それぞれについて考えられる主要な対策を選び、その実施状況を問うたところ、送信者側の対策としては「メール誤送信防止ツール」（46.6%）と「zipパスワードによる添付ファイルの暗号化」（45.9%）、受信者側の対策としては「アンチウイルス」（62.5%）と「スパムフィルタ」（50.5%）の導入／実施率が高いとの結果が示された（図31）。

その一方で、メール環境の大きな課題である送信者認証は、今後に向けて関心が高まってはいるものの、まだ十分に普及していないことも確認された。また、SPF、DKIMといった認証手段の利用率も、送信者側は2割前後の企業が利用しているが、受信者側としてそれを検証する仕組みを採用している割合は、送信者側に比べ低い結果となった。メールアドレスさえわかれば誰でもメッセージを送ることのできる電子メールは手軽に使える一方で、セキュリティの抜け穴が多い通信手段の代表格でもある。各種対策ソリューションも登場しているが、企業においては、電子メール以外の安全な情報共有手段の検討も視野に入れるべきであろう。

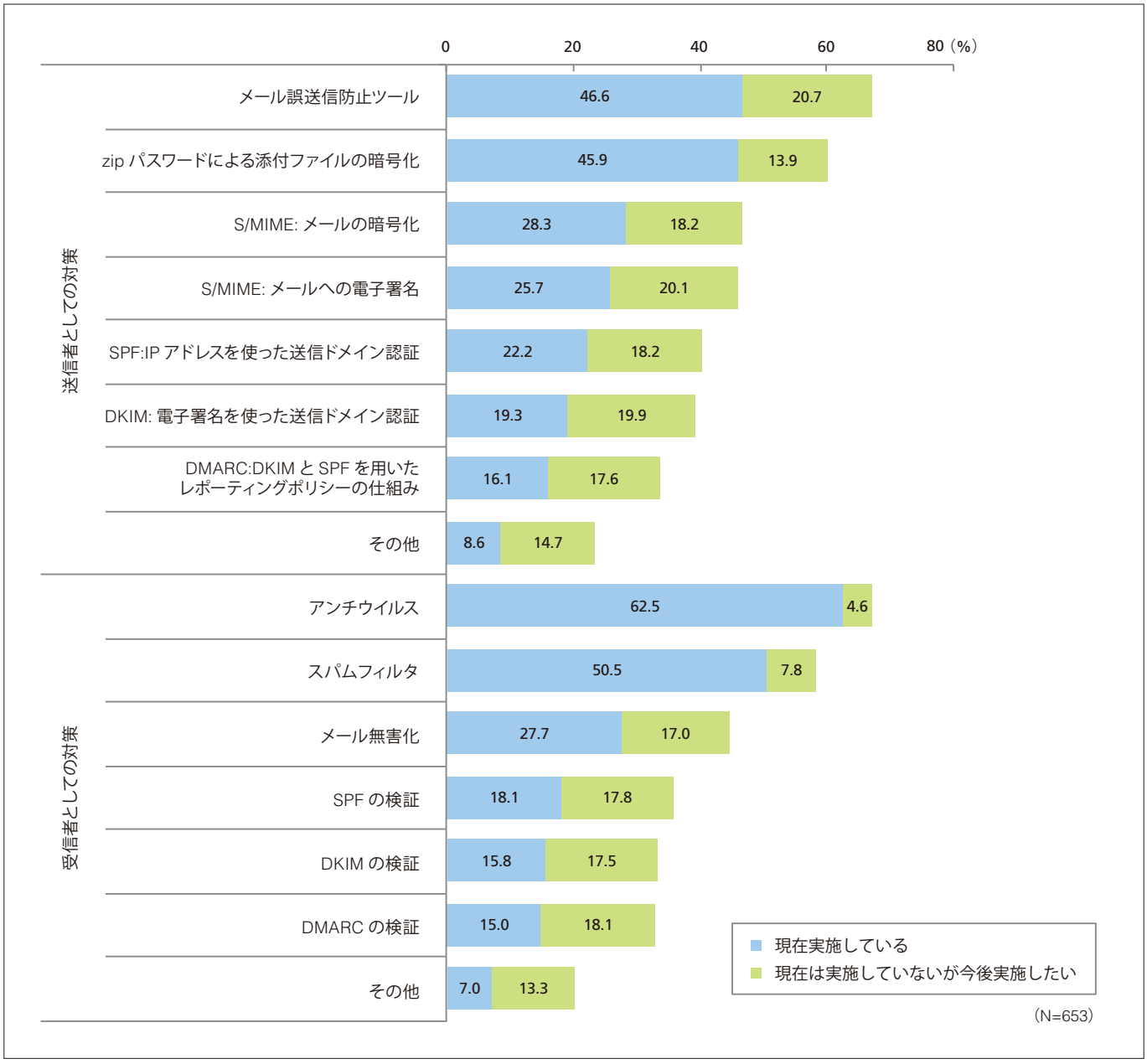

図31. 電子メールセキュリティ対策の実施状況

7 総評

本調査は、情報セキュリティをメインテーマに、その包括的な動向を探ることを目的に、今回を含め6回実施している。回を重ねるなかで見えてくるのは、情報セキュリティ対策のカバーすべき範囲が日増しに拡大しているという現実である。サイバー攻撃の高度化、利用デバイスの多様化などにより、セキュリティインシデントの認知率は大企業だけでなく中堅・中小企業でも上昇している。一方で、企業の対策は依然としてインシデントの削減策（メール／Webの規制、PC持出し禁止など）に重きが置かれている。今後は、重要情報の識別、隔離やデータ暗号化、OS／アプリケーションへのパッチ適用など、インシデントが起こることを前提とした対策を強化する必要があろう。セキュリティ支出は増加傾向であることが示されたが、増えた予算をどこに振り分けるかが問われることになる。

改正個人情報保護法対策は、企業において関心が高まっていることは窺えたものの、対応済みとした企業が2割強にとどまるなど、十分にリソースが割かれていない現実も垣間見られた。改正法の下では、個人情報の「保護」だけでなく「活用」の指針も示されている。海外法への対応も含め、今後はプライバシー保護への対策不足が、ビジネスの足を引っ張るおそれがあるということを認識しておく必要がある。

現安倍政権も積極的に推進している「働き方改革」は、企業における関心がきわめて高く、回答者が重視する経営課題の中でも2位となった。テレワークや在宅勤務など、ITを活用したワークスタイルが飛躍的に自由になることが想定されるだけに、セキュリティ対策上も無視できないキーワードになると見られる。これからのセキュリティ対策においては、利便性と安全性の両立がこれまで以上に求められるようになるのであろう。

回答者プロフィール

業種	回答数	%
製造	153	23.4
建設・不動産	60	9.2
卸売・小売	58	8.9
金融・保険	72	11.0
情報通信	110	16.8
サービス	151	23.1
公共・その他	49	7.5
全体	653	100.0

年間売上高	回答数	%
1,000 万円未満	7	1.1
1,000 万～ 1 億円未満	3	0.5
1 億～ 10 億円未満	53	8.1
10 億～ 100 億円未満	174	26.6
100 億～ 500 億円未満	130	19.9
500 億～ 1,000 億円未満	60	9.2
1,000 億～ 3,000 億円未満	66	10.1
3,000 億～ 5,000 億円未満	44	6.7
5,000 億円以上	116	17.8
全体	653	100.0

従業員規模	回答数	%
5,000 人以上	160	24.5
1,000 ～ 4,999 人	162	24.8
300 ～ 999 人	163	25.0
50 ～ 299 人	168	25.7
全体	653	100.0

所属部門	回答数	%
情報システム部門	303	46.4
経営企画部門	133	20.4
総務・人事部門	151	23.1
業務改革・業務推進部門	31	4.7
その他の部門	35	5.4
全体	653	100.0

役職	回答数	%
経営者	32	4.9
取締役・執行役員	70	10.7
部長	225	34.5
課長	197	30.2
係長・主任	125	19.1
その他	4	0.6
全体	653	100.0

IT 戦略、情報セキュリティへの関与度合い	回答数	%
全社的な IT 戦略に決定権をもっている	285	43.6
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もっている	371	56.8
セキュリティ製品の導入、製品選定に関与している	376	57.6
セキュリティ対策の実務に関与している	277	42.4
全体（複数回答）	653	-

業種別内訳

業種		回答数	%
製造	食品・飲料	19	2.9
	日用品・生活雑貨	2	0.3
	繊維	7	1.1
	パルプ・紙・印刷	7	1.1
	化学工業	8	1.2
	石油製品	6	0.9
	鉄鋼・金属	7	1.1
	プラスチック・ゴム	2	0.3
	機械	16	2.5
	電気機器	28	4.3
	情報通信機器	4	0.6
	電子部品・電子回路	9	1.4
	精密機器	9	1.4
	自動車・輸送機器	18	2.8
	医薬品	3	0.5
	その他の製造業	8	1.2
建設・不動産	建設	41	6.3
	不動産	19	2.9
卸売・商社	卸売	25	3.8
	小売	18	2.8
	商社	15	2.3
金融・保険	銀行	41	6.3
	証券	10	1.5
	生命保険	6	0.9
	損害保険	10	1.5
	その他金融	5	0.8

業種		回答数	%
情報通信	通信	22	3.4
	IT ベンダー／システムインテグレータ	71	10.9
	インターネットサービス	7	1.1
	情報システム子会社	10	1.5
サービス	電力・ガス・水道	9	1.4
	運輸	26	4.0
	倉庫	3	0.5
	宿泊	3	0.5
	飲食	9	1.4
	娯楽・レジャー	5	0.8
	メディア・出版・放送・広告	3	0.5
	生活関連サービス（旅行業など）	8	1.2
	医療	19	2.9
	福祉・介護	23	3.5
	教育（学校以外）	9	1.4
	人材派遣・業務委託	7	1.1
	その他サービス	27	4.1
公共・その他団体	学校	7	1.1
	官公庁	6	0.9
	地方自治体	21	3.2
	その他公共機関	6	0.9
	その他の業種	9	1.4
全体		653	100.0

＜資料＞情報化に関する動向（2016年10月～2017年3月）

国　内	海　外
2016年10月	
・宮城県警、企業のサーバに侵入し、約12万件のID/パスワードを不正取得したとして、不正アクセス禁止法違反の疑いで少年を書類送検。 ・サイバーセキュリティ戦略本部、サイバー攻撃の監視対象に日本年金機構等、国民生活に影響が大きい9法人を追加指定。 ・日・ASEAN情報セキュリティ政策会議開催。「日・ASEANにおける重要インフラ防護に関するガイドライン」承認と、各国重要インフラ防護政策導入・実施に向けた協力合意。 ・経済産業省、サイバーセキュリティ分野初の国家資格「情報処理安全確保支援士」制度開始。 ・金融庁、金融機関対象のサイバー対策演習実施。初の官民連携の金融機関向け大規模訓練。 ・日韓両政府、ソウルで第1回サイバー協議開催。 ＜JIPDEC関連＞ ・愛媛県越智郡上島町、なりすましメール防止「安心マーク」を地方自治体として初めて導入。	・米商務省、インターネットのドメインネームシステム（DNS）の管理権限を非営利団体のICANNに移管。 ・英ROM Group、自動運転車の公道走行テストを英国で初めて実施。 ・米DNSサービス企業のDyn、大規模なDDoS攻撃被害を受け、Twitter、Spotifyなどのサービスが約6時間利用不可に。後日、IoTマルウェア「Mirai」に感染した数千万台のデバイスから攻撃を受けていたと報告。 ・AT&T、Time Warnerの買収合意を発表。モバイルブロードバンドと動画のバンドルによる、米国初のモバイルプロバイダを目指す。 ・Google、ニューラルネットワーク（神経回路網）を用いた暗号化通信の実験に成功。

国　内	海　外
2016年11月	
・東京大学ほか日米英13大学、サイバー攻撃対応に向け国際連携組織設立。 ・人工知能「東ロボくん」、東大合格を断念し、得意分野の試験成績向上を目指す研究に転換。 ・特許庁、IoT関連技術の特許分類（分類記号ZIT）新設。 ・情報処理推進機構（IPA）、「中小企業の情報セキュリティ対策ガイドライン」を7年ぶりに改訂。「経営者編」「管理実践編」「各種ひな型の付録」を追加。 ・経済産業省とIPA、電子行政や企業システムで扱う文字・用語の共通化のための「情報共有基盤（IMI）サイト」開設。「文字情報基盤」「共通語彙基盤」を提供。 ・工業所有権情報・研修館（INPIT）、無償のタイムスタンプ情報保管サービスを開始。 ・個人情報保護委員会、「個人情報の保護に関する法律についてのガイドライン（通則編、外国にある第三者への提供編、第三者提供時の確認・記録義務編及び匿名加工情報編）」を公示。 ＜JIPDEC関連＞ ・イオン銀行、「安心マーク」導入。 ・ISMS適合性評価制度、認証取得組織数が5,000件を突破。	・Google、Apple等、中国の認証局WoSignが不正な証明書を発行したと判断して取り扱わないことを表明。 ・中国全国人民代表大会、サイバーセキュリティ法案可決。ユーザの本名登録、犯罪や国家安全保障に係る調査への協力などを義務付け。2017年6月施行予定。 ・英国政府、ネットユーザのWeb履歴について、インターネットプロバイダに最長1年間の記録を義務づけた、監視能力を大幅に強化した新法案を上下両院で可決。 ・米海軍、契約事業者であるHPES従業員のノートPCを介する不正アクセスにより、海軍兵13万人以上の個人情報が流出。

国　内	海　外
2016年12月	
・IPA、「サイバーセキュリティ経営ガイドライン解説書」公開。 ・地方公共団体情報システム機構、マイナンバーカード管理システム障害により、カードの交付に遅延が生じたとして、システム設計・開発業者５社に対し、総額約1億9,450万円の損害賠償請求を決定。 ・個人情報保護委員会、改正個人情報保護法の全面施行日を2017年5月30日と公表。 ・政府データ流通環境整備検討会、IoT社会基盤における個人データの流通について、個人の意向に応じた「パーソナルデータストア（PDS）」の仕組みなどを整理。 ＜JIPDEC関連＞ ・JIPDEC、CBPR認証事業者第一号としてインタセクト・コミュニケーションズを認証。 ・JIPDEC、中小企業向け改正個人情報保護法対応支援を開始。第一弾として、大阪、東京で実務対応セミナー開催。	・Yahoo!、2013年8月のサイバー攻撃により10億人以上の個人情報流出を発表。 ・Facebook、偽ニュース問題への対策を発表。通報情報の事実確認を第三者機関に依頼し、虚偽情報と判定された場合に警告を表示。 ・Evernote、ユーザのコンテンツを一部の社員が閲覧可能にできるようにするプライバシーポリシーの変更提案を撤回。 ・米政府、次期大統領選にロシアがサイバー攻撃で干渉した報復に、ロシア政府当局者の国外退去処分など制裁発動。

国　内	海　外
2017年1月	
・筑波大学大学院、患者の遺伝子データを暗号化したまま統計処理できる秘密計算技術を開発。 ・経済産業省、国内400万企業の法人情報検索サイト「法人インフォメーション」開設。各省庁での事業委託、許認可実績などが閲覧可能に。 ・千葉県警、全国初の捜査対象者の車両にGPS端末を利用するGPS捜査を実施。 ・サイバーセキュリティ戦略本部、サイバー対策、自然対策強化のための行動計画案をとりまとめ。2020年オリンピックに向け、3年ぶりの改定。 ＜JIPDEC関連＞ ・JIPDEC、経済産業省の「法人インフォメーション」と連携し、「サイバー法人台帳ROBINS」で企業活動の見える化を開始。	・米トランプ大統領、サイバー攻撃防御に向けたセキュリティ対策専門チームの設置を決定。 ・中国国家発展改革委員会、2016～18年の情報インフラ整備に1兆2,000億円を投資することを発表。 ・米ドメイン登録事業者のGoDaddy、SSL証明書の不具合により、8,850件の証明書を失効処理。 ・Google報告、2016年に削除した広告ポリシー違反による悪質広告は17億件。前年比2倍以上。

国　内	海　外
2017年2月	
・最高裁、Google検索結果による過去の犯罪歴の表示が人権侵害にあたるとして、削除を求めた仮処分申立てに対し、社会的影響力等をもとに請求を棄却。 ・情報通信研究機構発表、2016年の国内のサイバー攻撃は前年比2.4倍の約1,281億円。IoT関連機器がターゲットに。 ・東京都、自動運転技術の実証実験着手を正式表明。年度内から羽田空港近辺で開始予定。 ・産業技術総合研究所（AIST）と東京工業大学、「産総研・東工大　実社会ビッグデータ活用　オープンイノベーションラボラトリ」を設立。両団体が持つ計算プラットフォーム構築技術とビッグデータ処理技術を融合。 ・国立情報学研究所（NII）、匿名加工情報の技術的検討結果をまとめた「匿名加工情報の適正な加工の方法に関する報告書 2017年2月21日版」を公表。 ・IoT推進コンソーシアム、インド全国ソフトウェア・サービス企業協会とIoT分野の協力に係る覚書に署名。 ・個人情報保護委員会、匿名加工情報作成時の考え方をまとめた「事務局レポート」発表。匿名加工情報の定義、加工基準の解説、代表的な加工情報を紹介。	・Twitter、誹謗中傷を排除するツールを発表。中傷目的の新規アカウント作成阻止へ。 ・韓国警察庁サイバー安全局、「悪性コードランサムウェア被害注意報」発令。同国の2016年ランサムウェア被害届け出件数は前年比86.8%増の1,438件に。 ・Yahoo!、2015年から2016年にかけて発生したユーザ情報流出に関連し、アカウントの不正侵入の可能性を通知。 ・Googleとオランダ情報工学・数学研究所、電子認証や電子署名に使用される暗号化アルゴリズム「SHA-1」の解読に成功。

国　内	海　外
2017年3月	
・人工知能学会、人工知能自体にも学会員同等の倫理指針の遵守を求めた、人工知能研究開発の倫理指針発表。 ・損保ジャパン日本興亜、ネット炎上の拡散防止、メディア対応費用を補償する、国内初の「ネット炎上対応費用保険」を販売開始。 ・日立製作所、東京大学、AIST、共同提案した位置情報へのデータアクセス仕様「Moving Features Access」の国際標準採択を発表。 ・NEC、米国立標準技術研究所実施の動画の顔認証技術のベンチマークテストで、4年連続世界１位の性能評価を獲得。 ・最高裁、令状なしのGPS捜査はプライバシー侵害にあたるとして、違法の判断。 ・NII、世界初の指紋盗撮防止手法「Biometric Jammer」を国際情報通信見本市「CeBIT 2017」で公開。 ・警視庁、ワンタイムパスワード入力の偽画面から不正送金させる新種ウイルス「DreamBot」感染を国内で初めて確認。 ・経済産業相、第四次産業革命に関する日独協力の枠組みを構築する「ハノーバー宣言」に署名。 ・日本政府、EUとのデータ流通の円滑化をめざし、共同プレステートメントを発表。 ＜JIPDEC関連＞ ・JIPDEC・日本商工会議所共催「中小企業向け改正個人情報保護法実務対応セミナー」参加者アンケート結果を発表。改正個人情報保護法対応　春頃までに体制構築対応を予定している企業は6割、対応済は1割に満たず。 ・JIPDECとITR、「企業IT利活用動向調査」の結果を発表。	・Yahoo!、2014年のサイバー攻撃で、最低5億人の利用者情報流出を発表。その後、事件に関与したロシア人等４人を起訴。 ・IBM、自動運転車の事故回避に人工知能の機械学習技術を利用する特許を取得。

JIPDEC IT-Report 2017 Spring
2017年6月13日発行（通巻第9号）
発行所　一般財団法人日本情報経済社会推進協会
〒106-0032　東京都港区六本木1-9-9　六本木ファーストビル内
TEL：03-5860-7555　FAX：03-5573-0561
制　作　開成堂印刷株式会社