

# JIPDEC IT-Report 2016 Spring

特集

「企業IT利活用動向調査2016」  
にみるIT化の現状

## はじめに

本誌「2016 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。

今回の調査で注目すべき点は、2015年10月から付番・通知・収集が開始されたマイナンバー制度に対するIT/セキュリティ責任者の意識調査結果です。

経営課題として何を重視しているかの調査では、「マイナンバー制度への対応」が前回調査(2015年1月時点)の9.2%から、17.1%と約2倍に増加しています。また情報システムの対応状況について、前回調査では全体の7割以上が対応の必要性を感じつつも、そのうちの約4割弱が「準備中・未着手」と回答していました。1年後の実施となった今回の調査においては、「完了」「作業が進行中」という企業が6割を超えており、対応が進んでいることがわかりました。なお、対応が「進行中」、または「準備・検討中」の理由としては、「社内のIT人材不足」「システム化予算の不足」があげられています。

このほか、本調査では、経営課題へ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、経年分析を含めて報告しています。

あわせて、IT業界を俯瞰するデータ、2015年度後期の情報化動向をとりまとめて紹介していますので、本誌を今後のIT環境整備の参考にさせ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

<b>【特集】「企業IT利活用動向調査2016」</b>	<b>&lt;資料&gt;データ編</b>	<b>33</b>
<b>にみるIT化の現状</b>	1.世界のITインフラ普及状況	34
1.調査概要	2.情報処理実態調査	36
2.経営における情報セキュリティの位置づけ	3.行政の情報化	37
3.情報セキュリティに関する認定/認証制度の動向	4.コンピュータおよび関連装置の生産推移	38
4.セキュリティ支出と組織的な対策の動向	5.情報サービス市場	40
5.法制度への対応方針	6.電子商取引市場	40
6.情報セキュリティ製品の導入状況	7.電気通信市場	41
7.スマートデバイス/クラウドサービスの位置づけ	8.情報化に関する動向	43
8.総評		31
回答者プロフィール		32

## 【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。

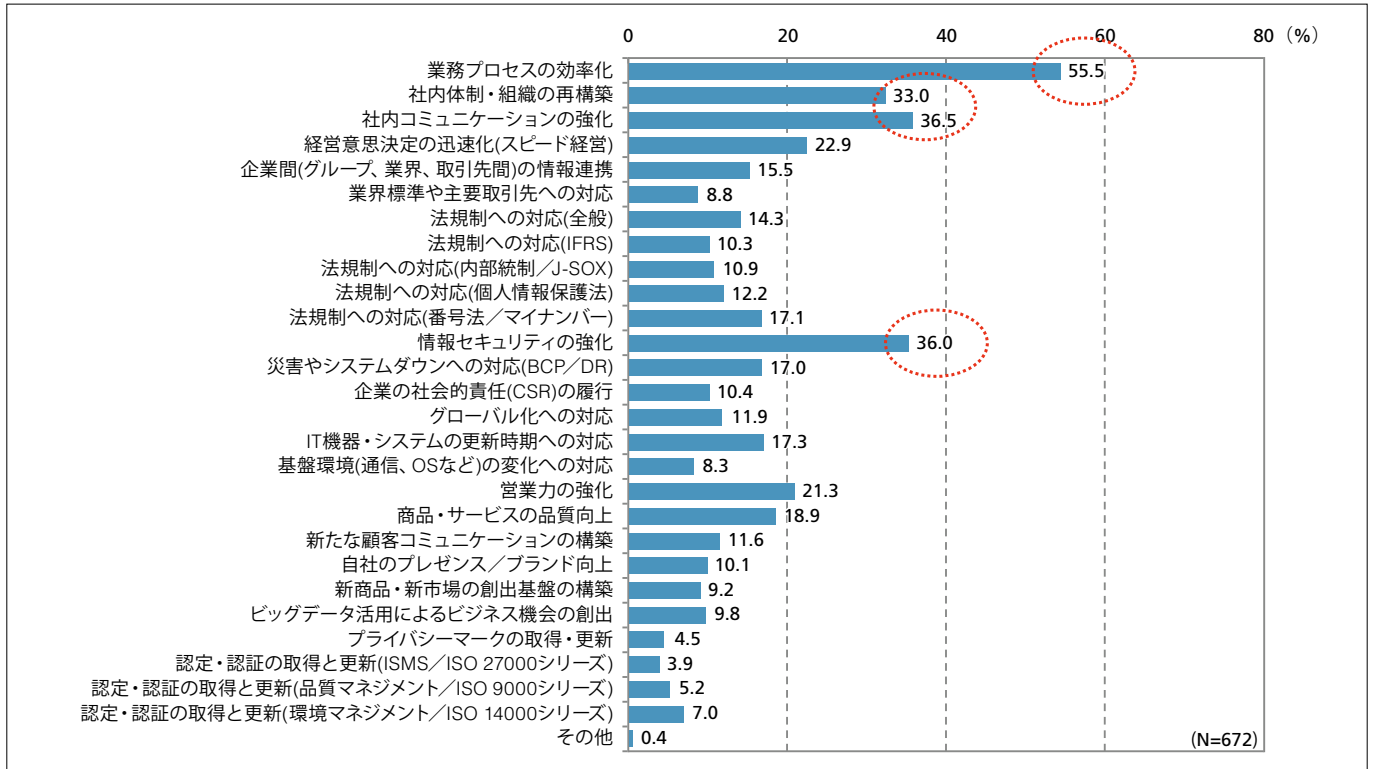


図1-1. 今後重視したい経営課題(複数回答)

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。

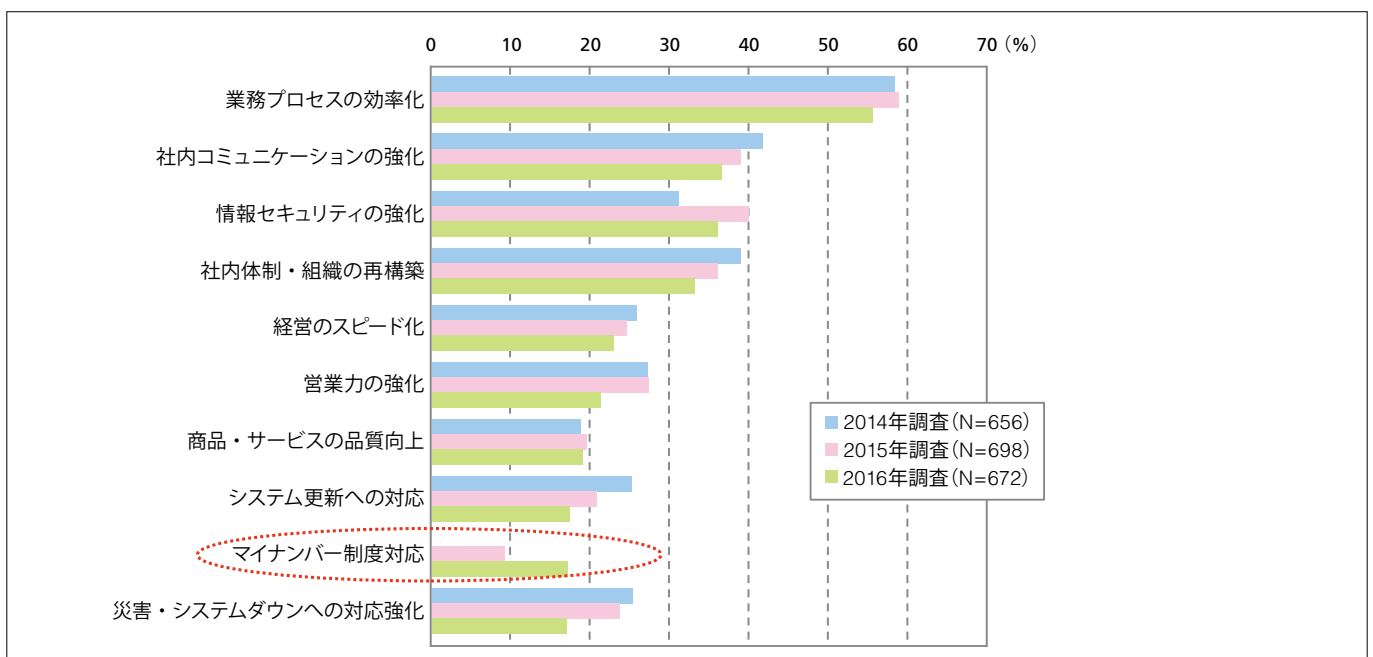


図1-2. 主要経営課題に対する回答率の経年比較(2014~2016年)

## 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。

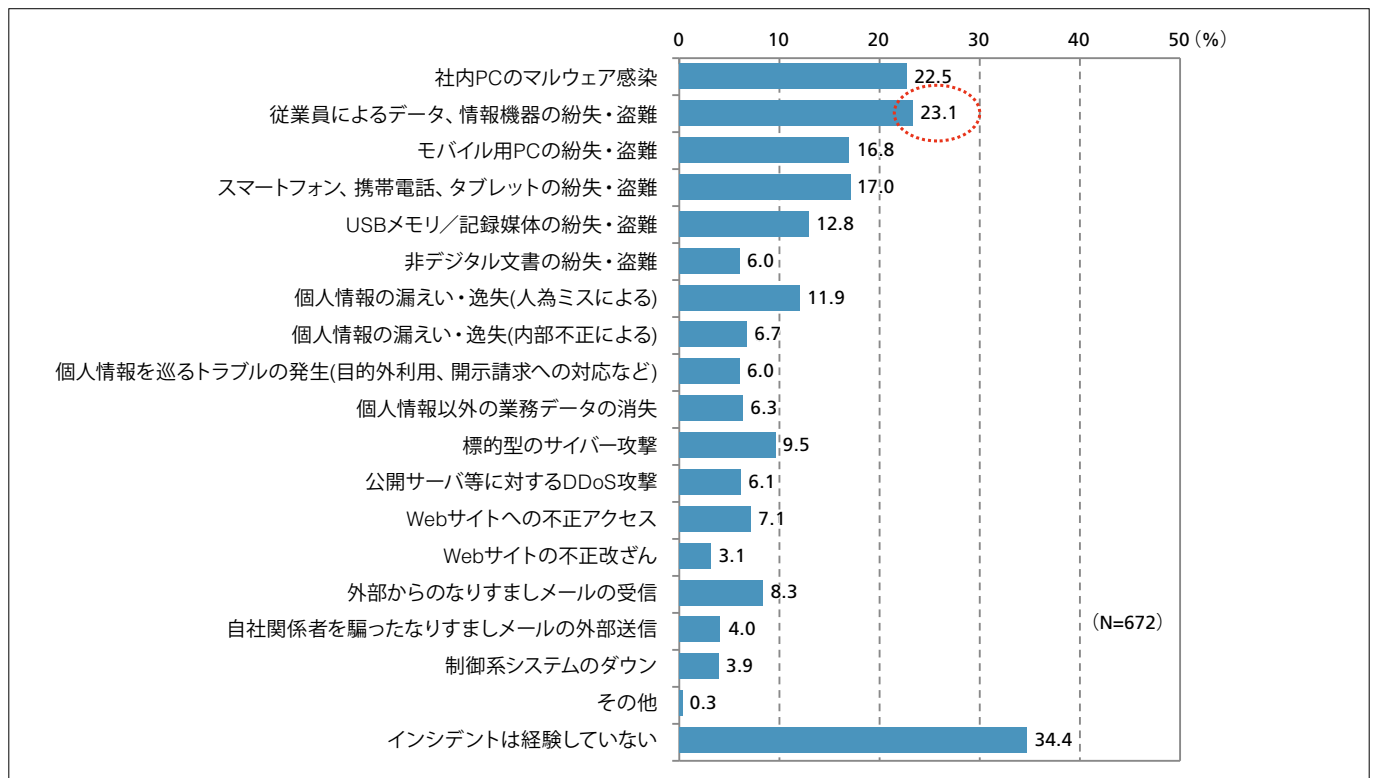


図1-3. 過去1年間に経験したセキュリティインシデント(複数回答)

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)。

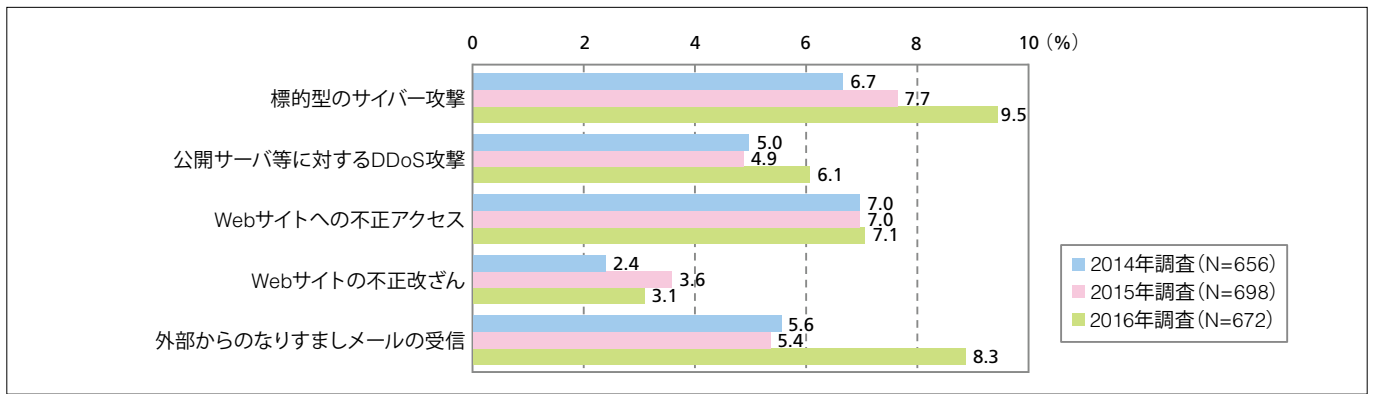


図1-4. サイバー攻撃に関わるセキュリティインシデントの経年比較(2014~2016年調査)

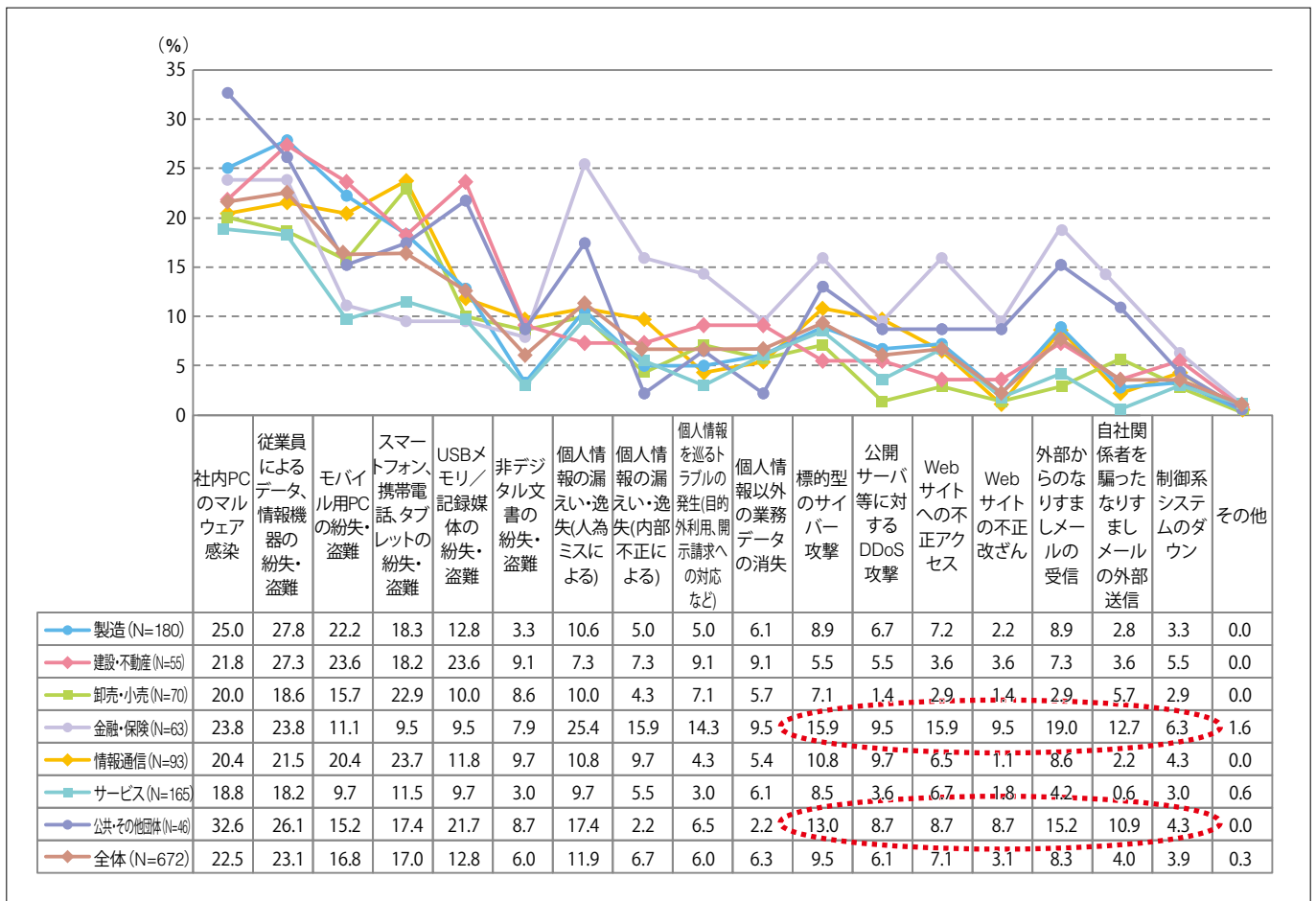


図1-5. 業種別に見た過去1年間のセキュリティインシデント

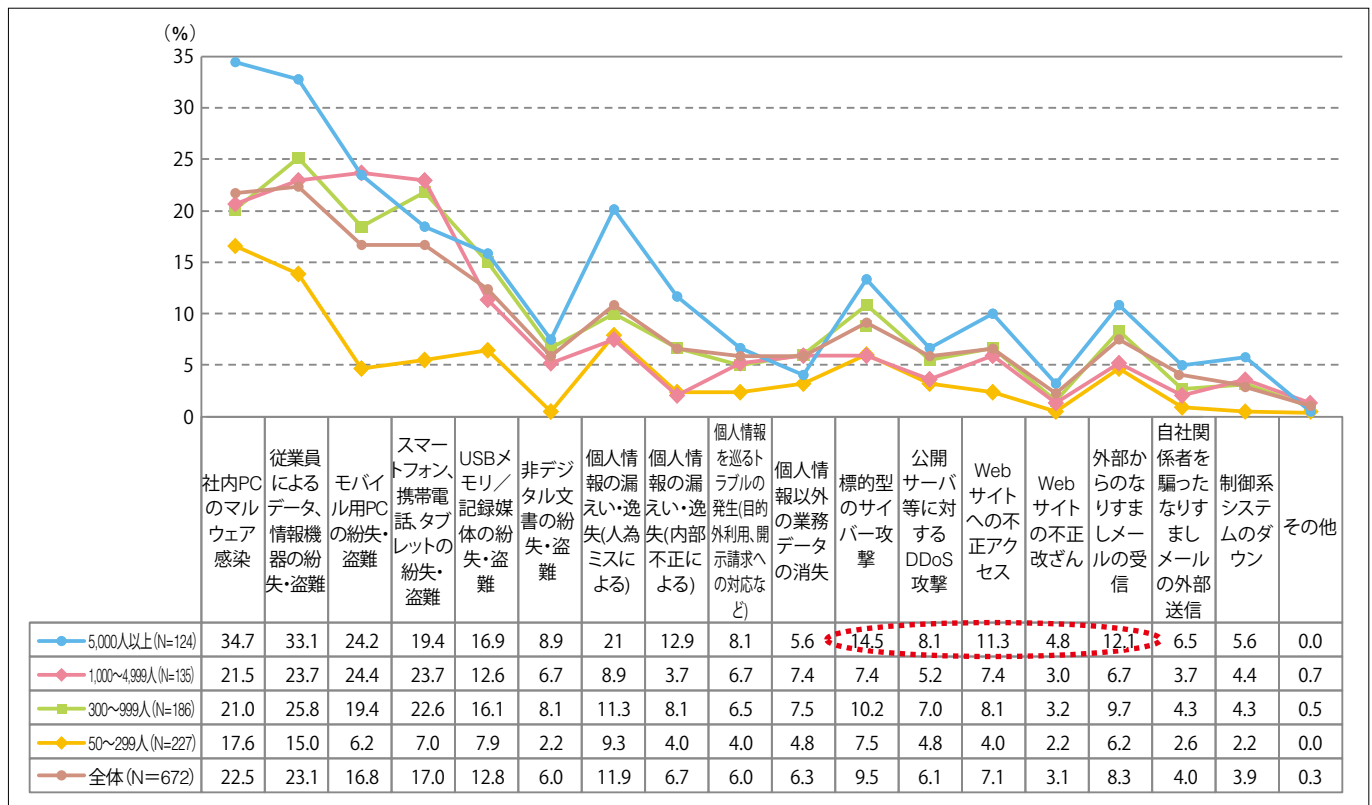


図1-6. 従業員数別に見た過去1年間のセキュリティインシデント

### 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)。

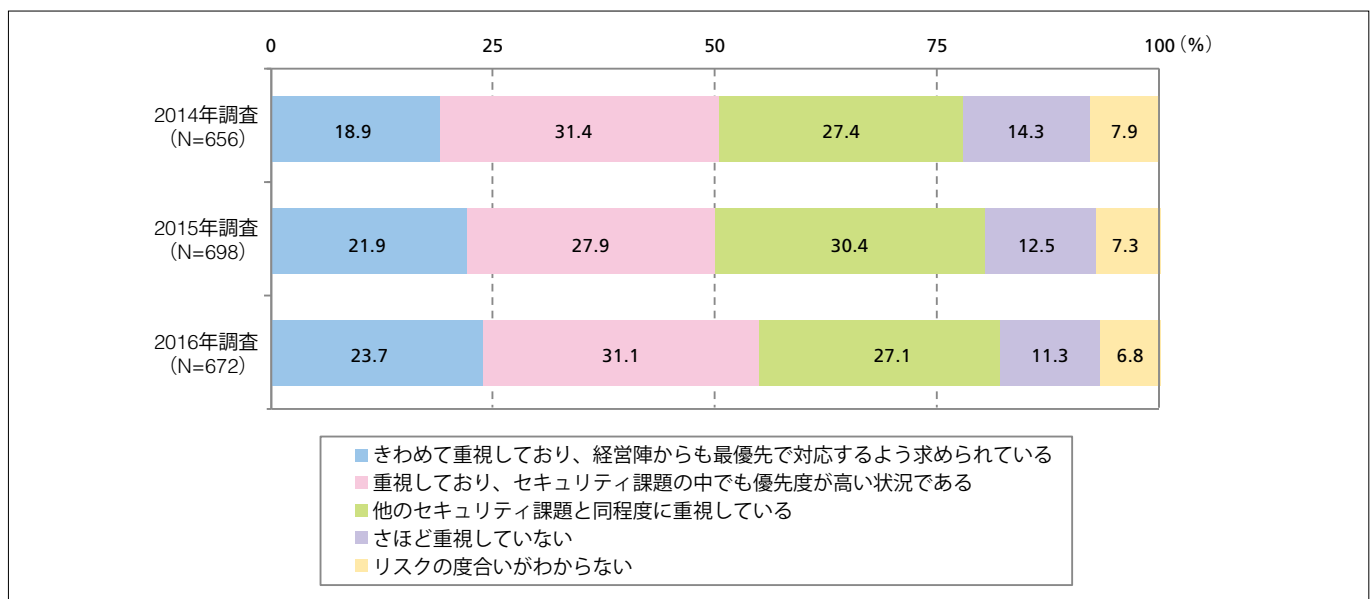


図1-7. 「標的型のサイバー攻撃」に対するリスクの重視度合いの経年比較(2014~2016年)

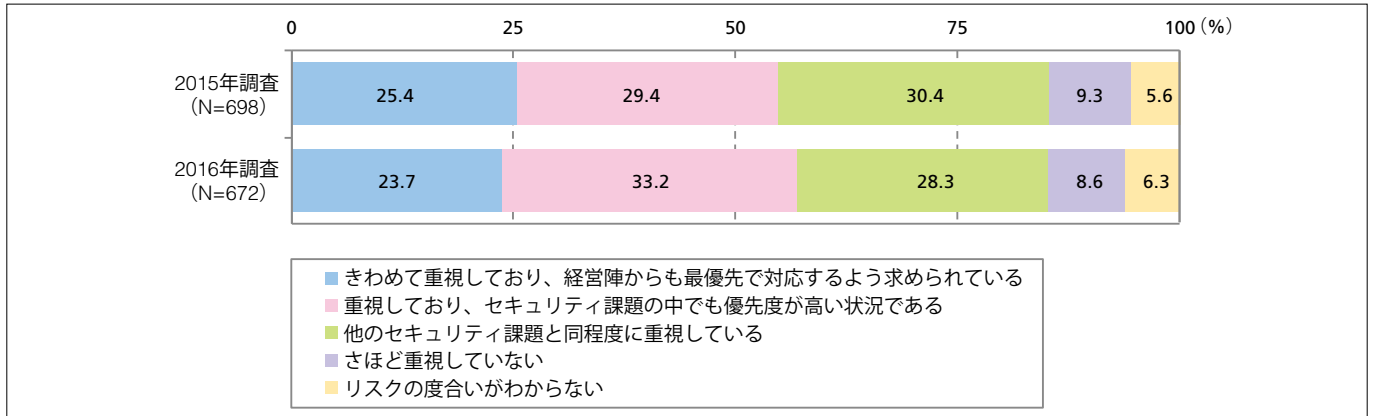


図1-8. 「内部犯行による重要情報の漏えい・消失」に対するリスクの重視度合いの経年比較(2014~2016年)

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。

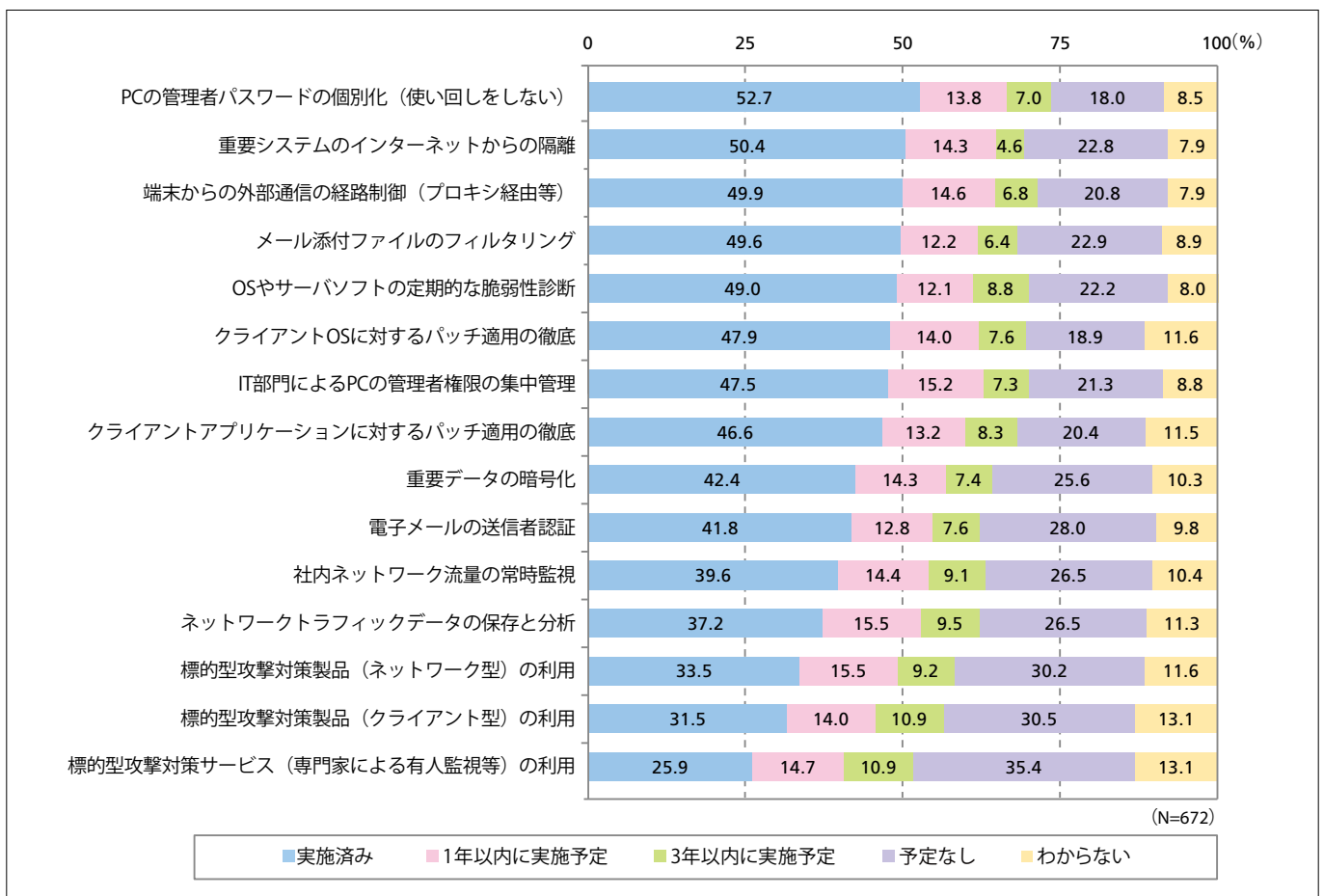


図1-9. 標的型サイバー攻撃対策の実施状況



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)。

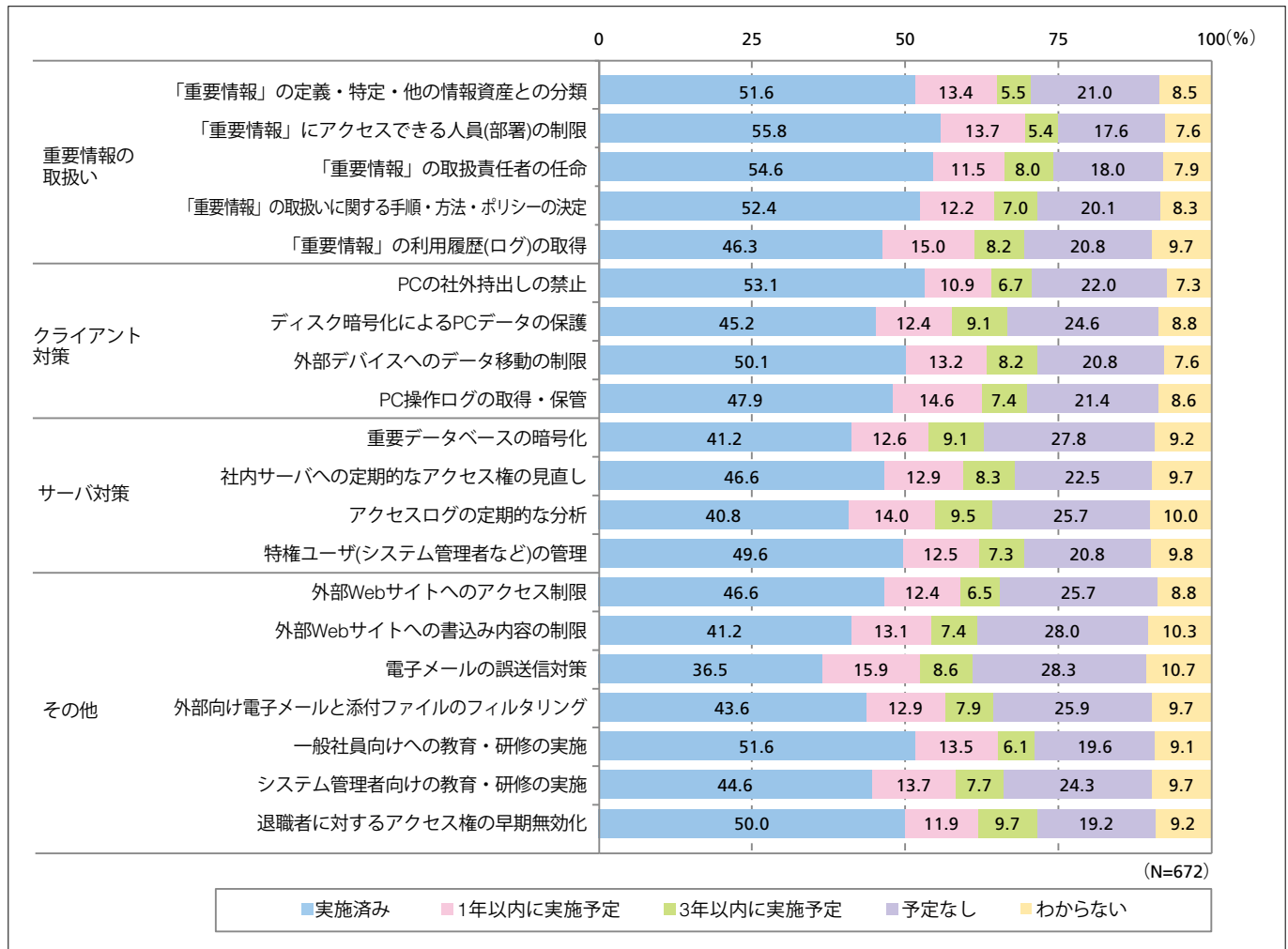


図1-10. 内部犯行対策の実施状況

# 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。

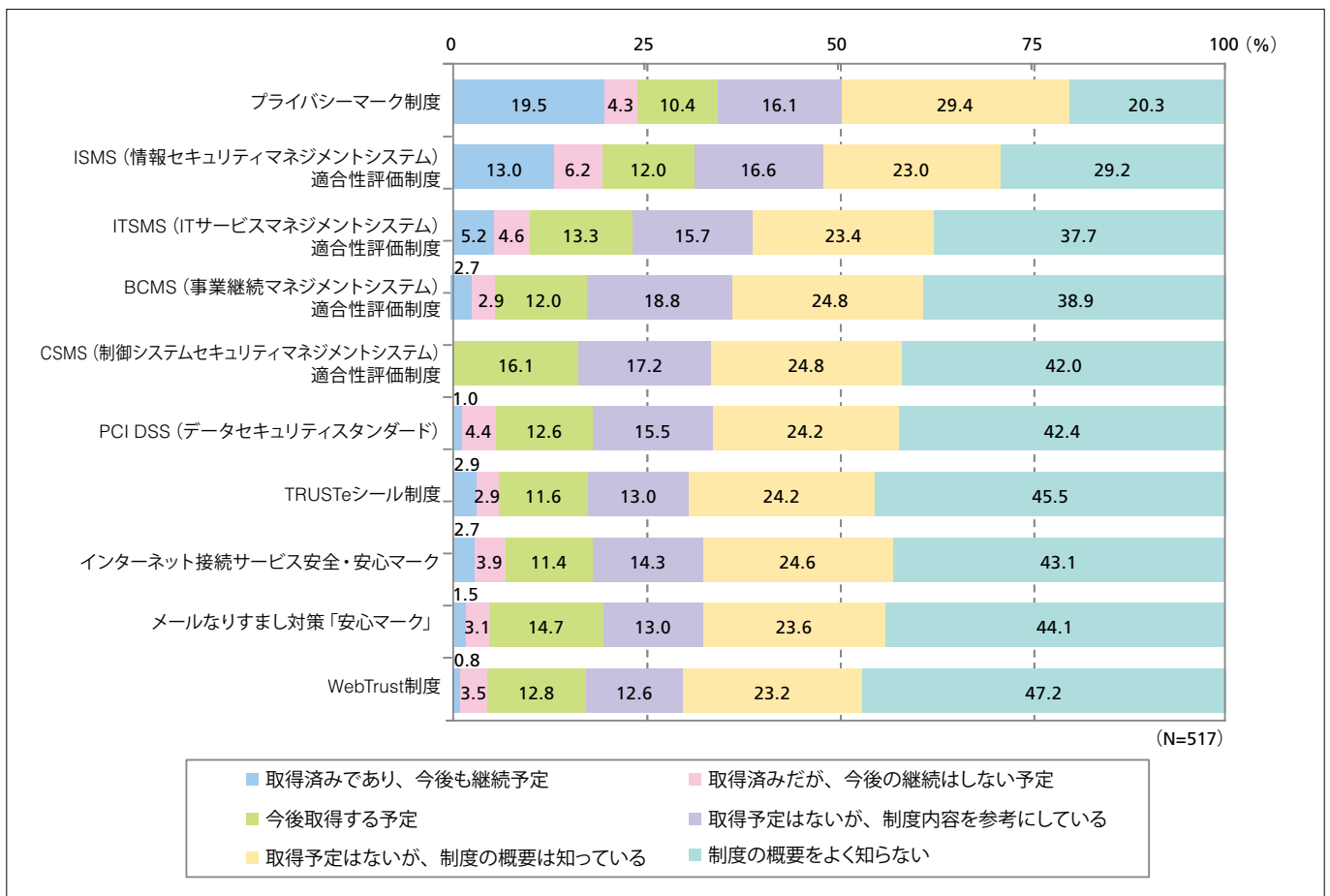


図1-11. 情報セキュリティに関わる認定／認証制度等の取組み状況

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。

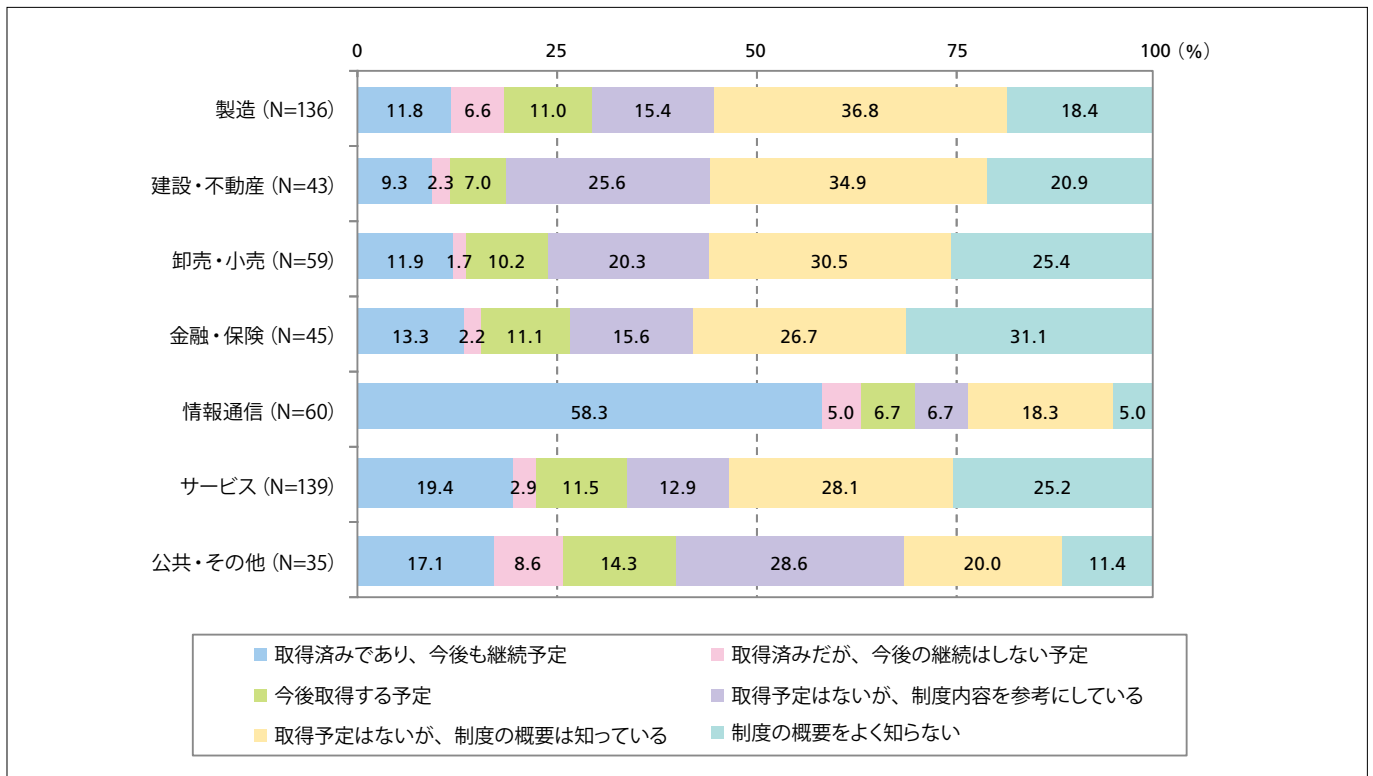


図1-12. 「プライバシーマーク制度」に対する取組み状況(業種別)

### 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込んでいるのであろうか。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ですが、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。

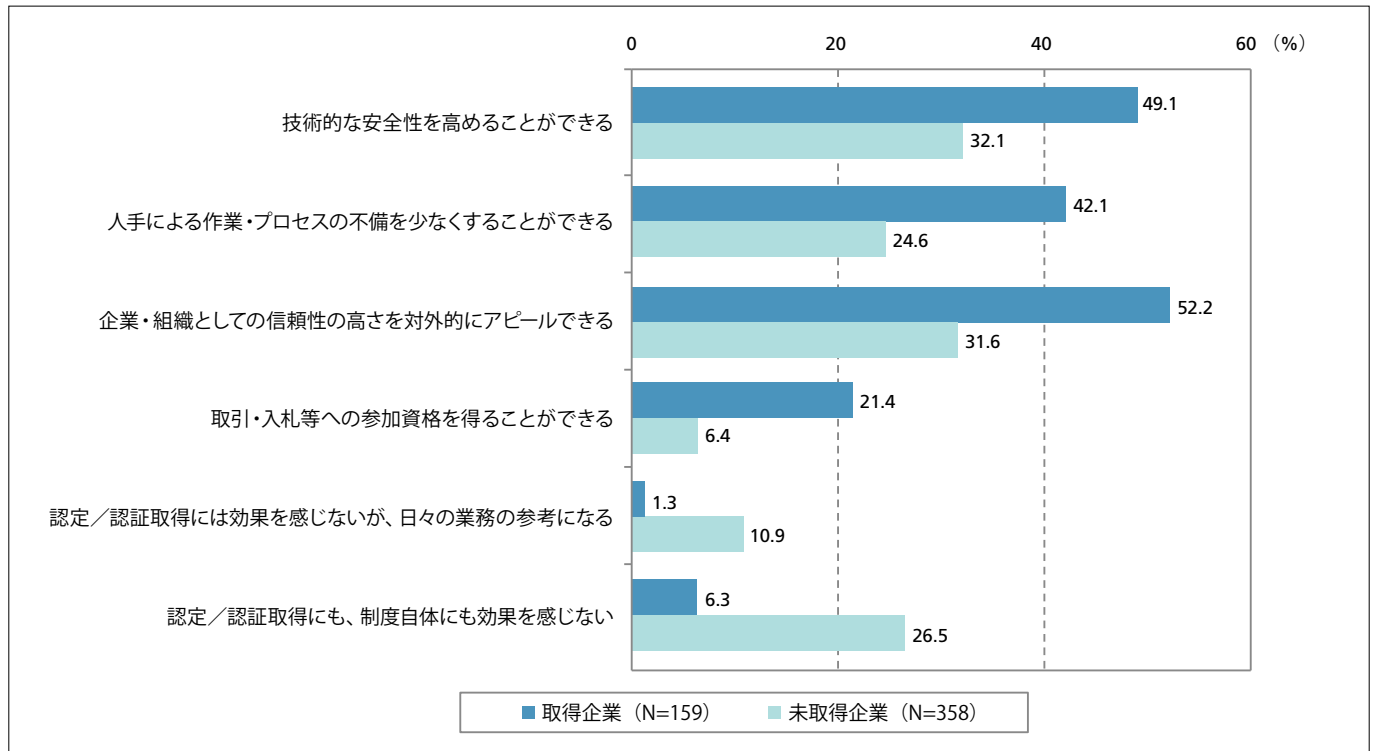


図1-13. 認定／認証を取得することの価値

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)。

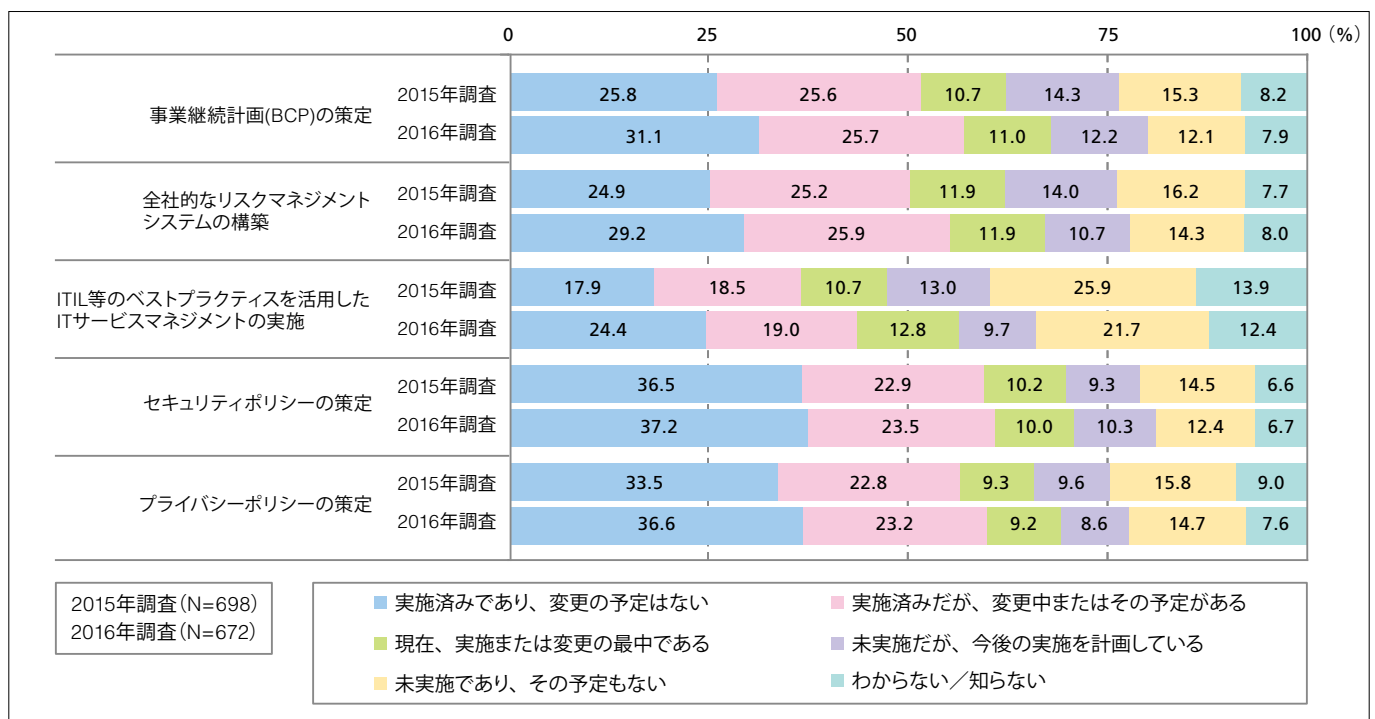


図1-14. 全社的なシステムリスクの対応策の取組み状況

### 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<sup>\*1</sup>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。

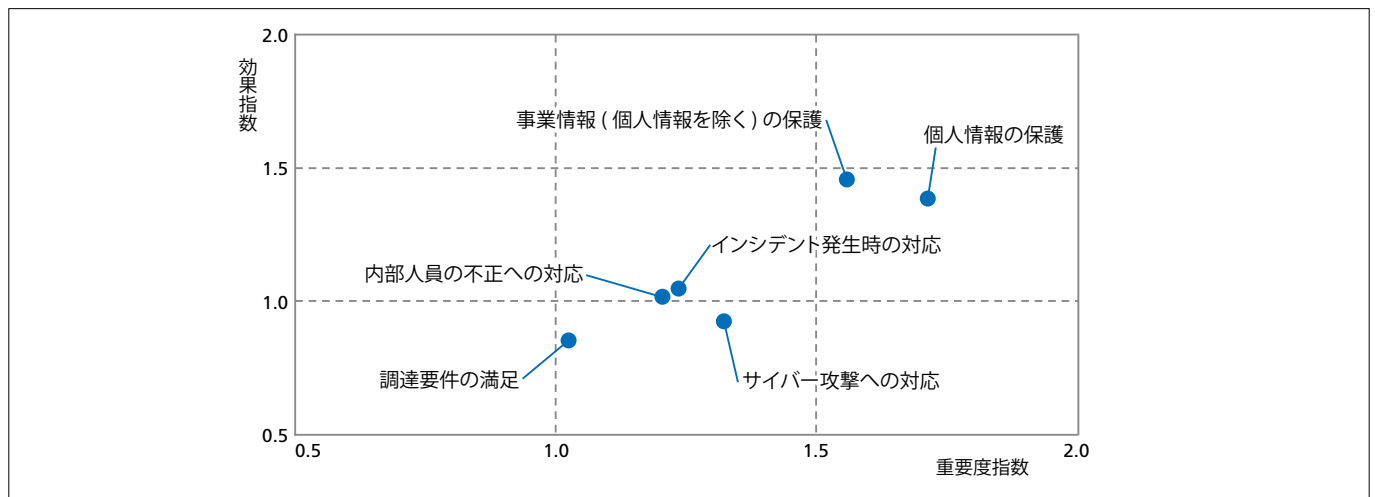


図1-15. ISMS適合性評価制度の重要度と効果

\*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)。

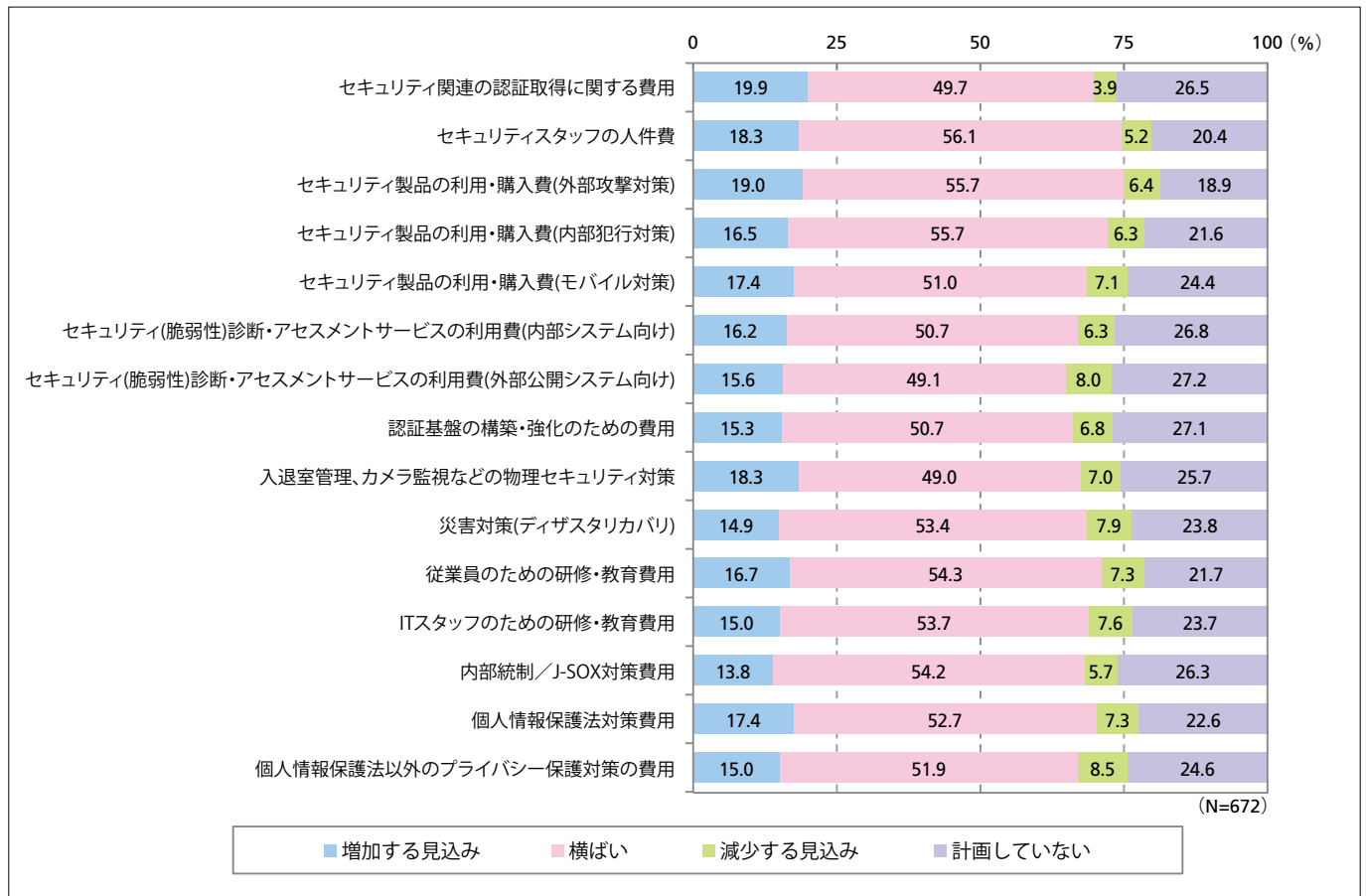


図1-16. 2016年度に想定されるセキュリティ支出の増減傾向

「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 person 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、ここに来てプロセスや組織、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し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。

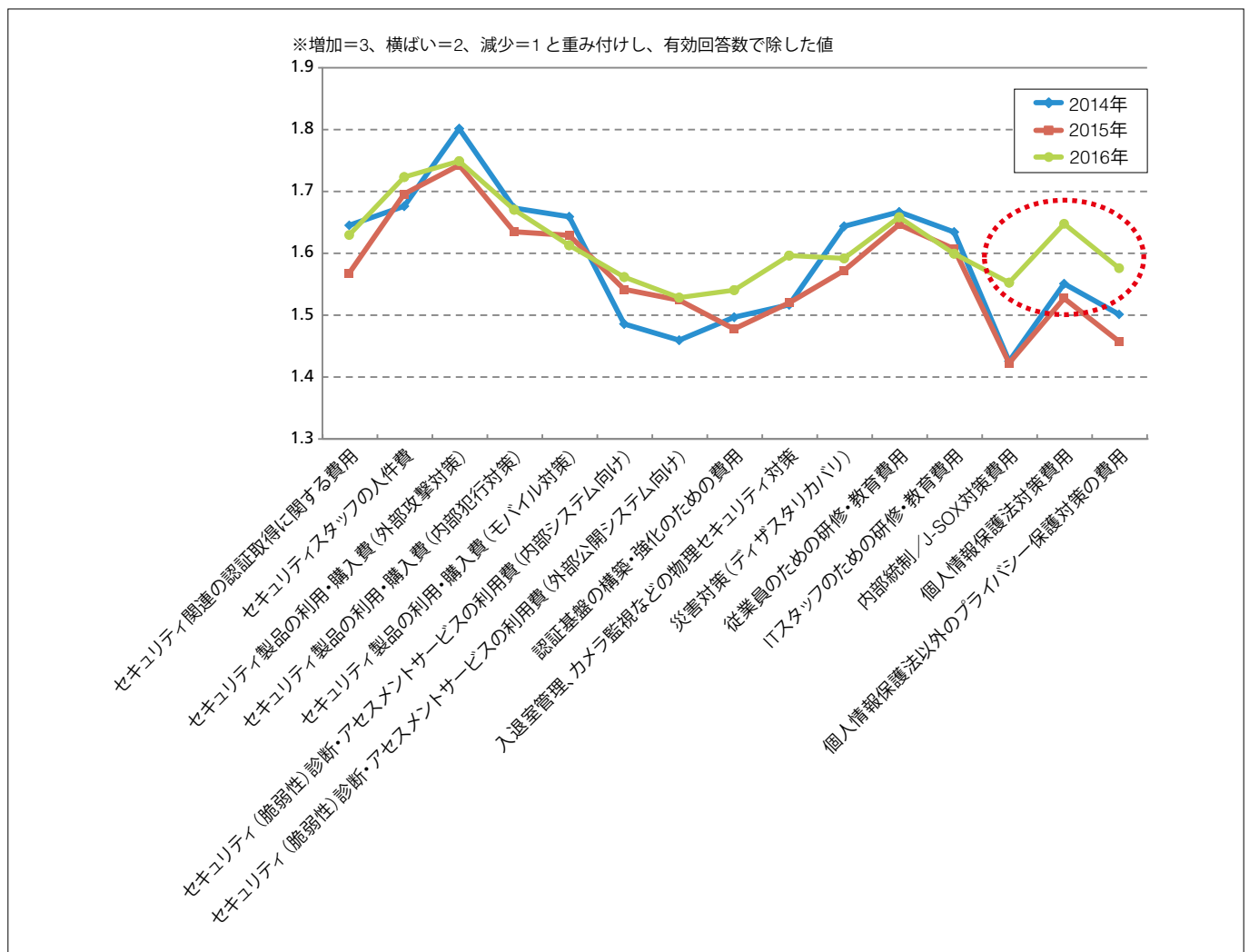


図1-17. セキュリティ支出の増減傾向の経年比較（2014～2016年調査）

## 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。

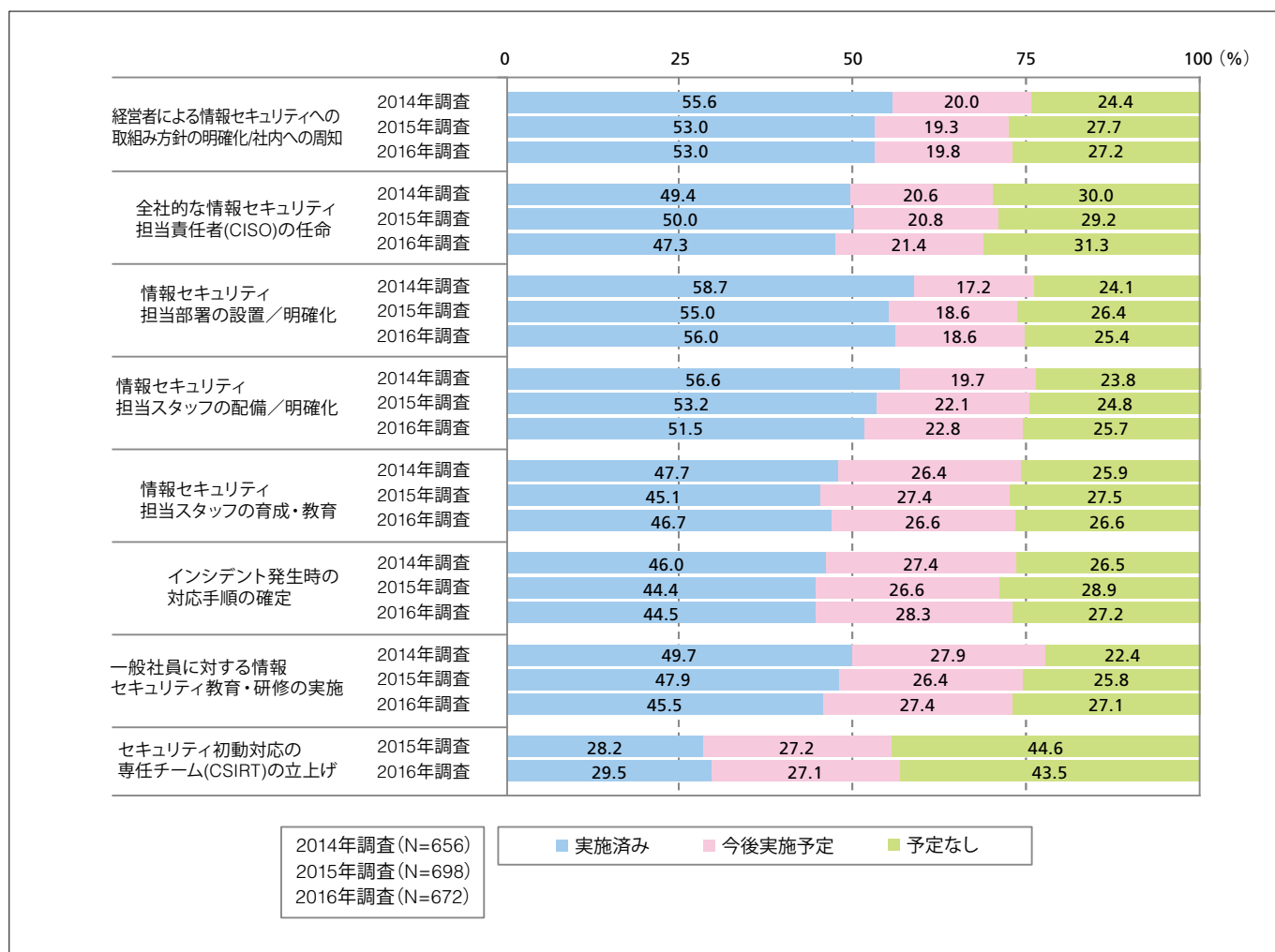


図1-18. 情報セキュリティ対策の実施状況の経年比較(2014～2016年調査)



## 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)。

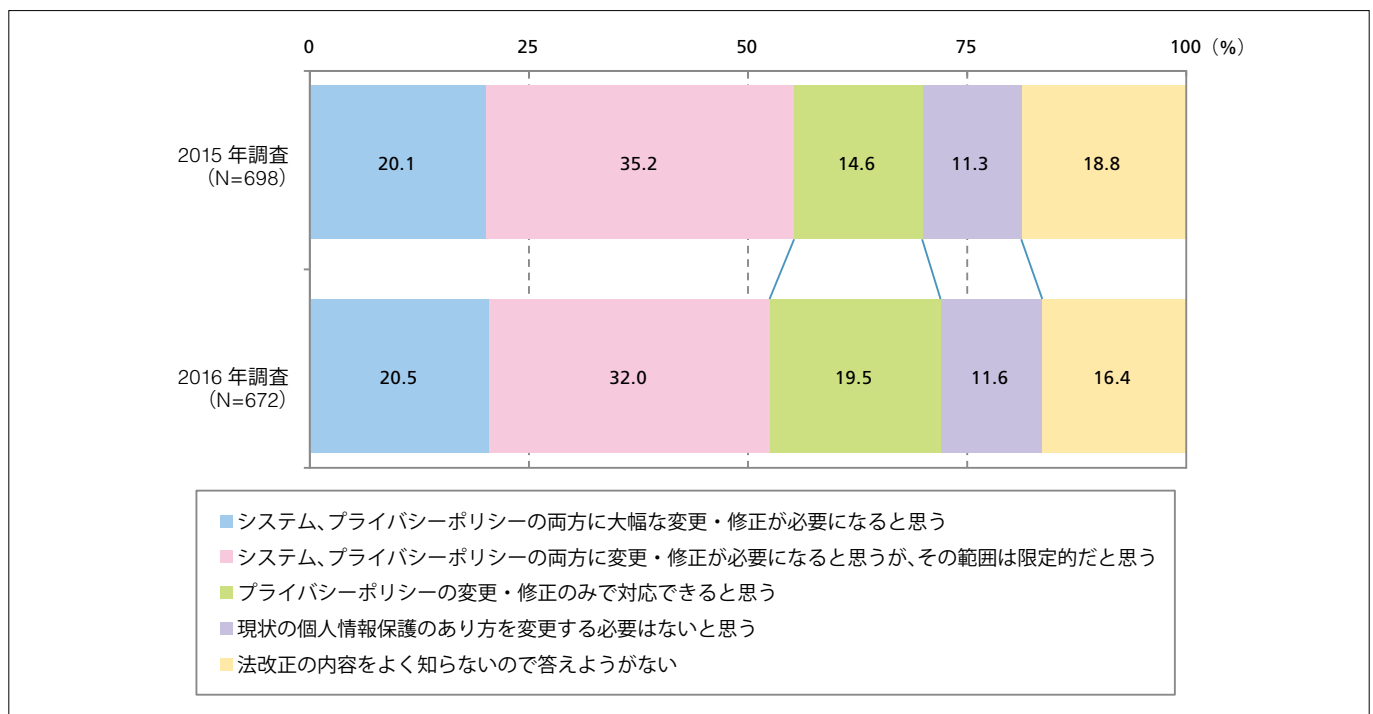


図1-19. 個人情報保護法改正のインパクトの経年比較(2015～2016年)

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)。

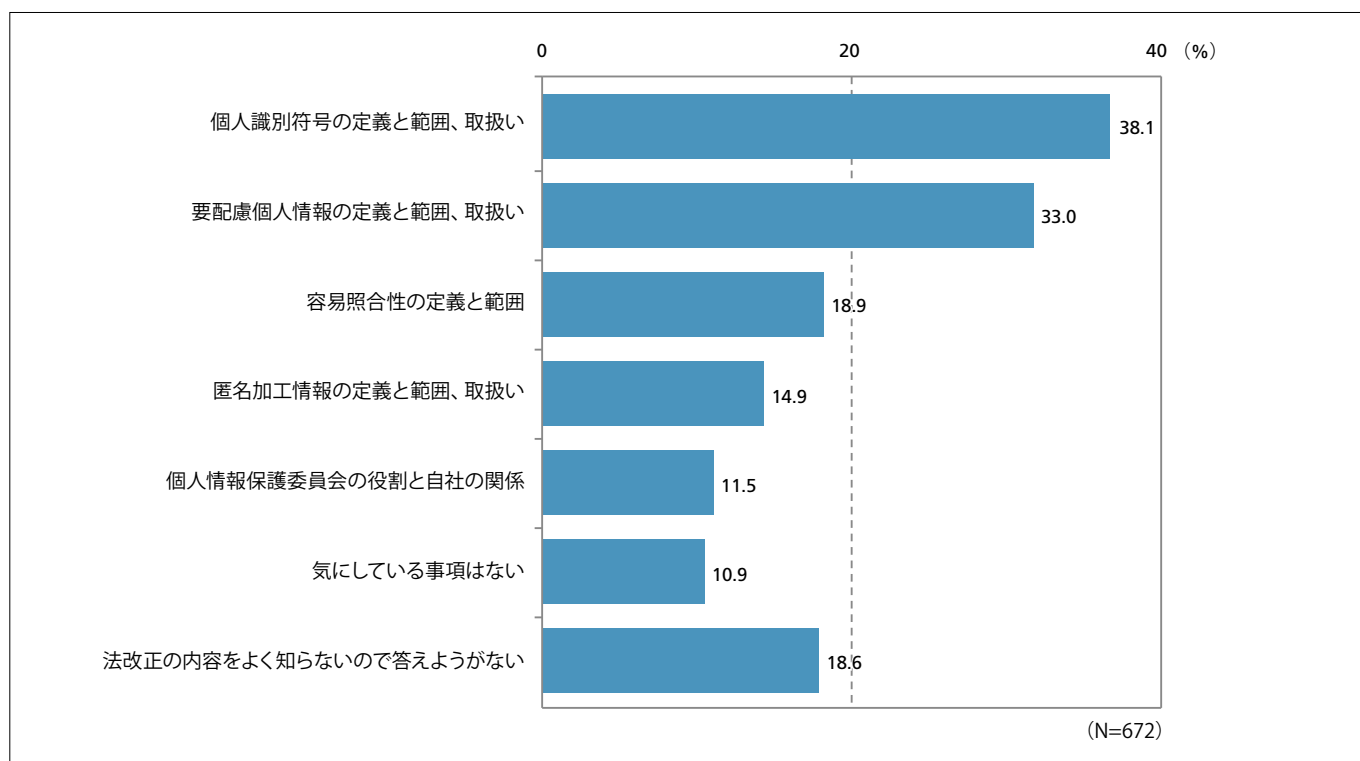


図1-20. 改正個人情報保護法で気にしている点

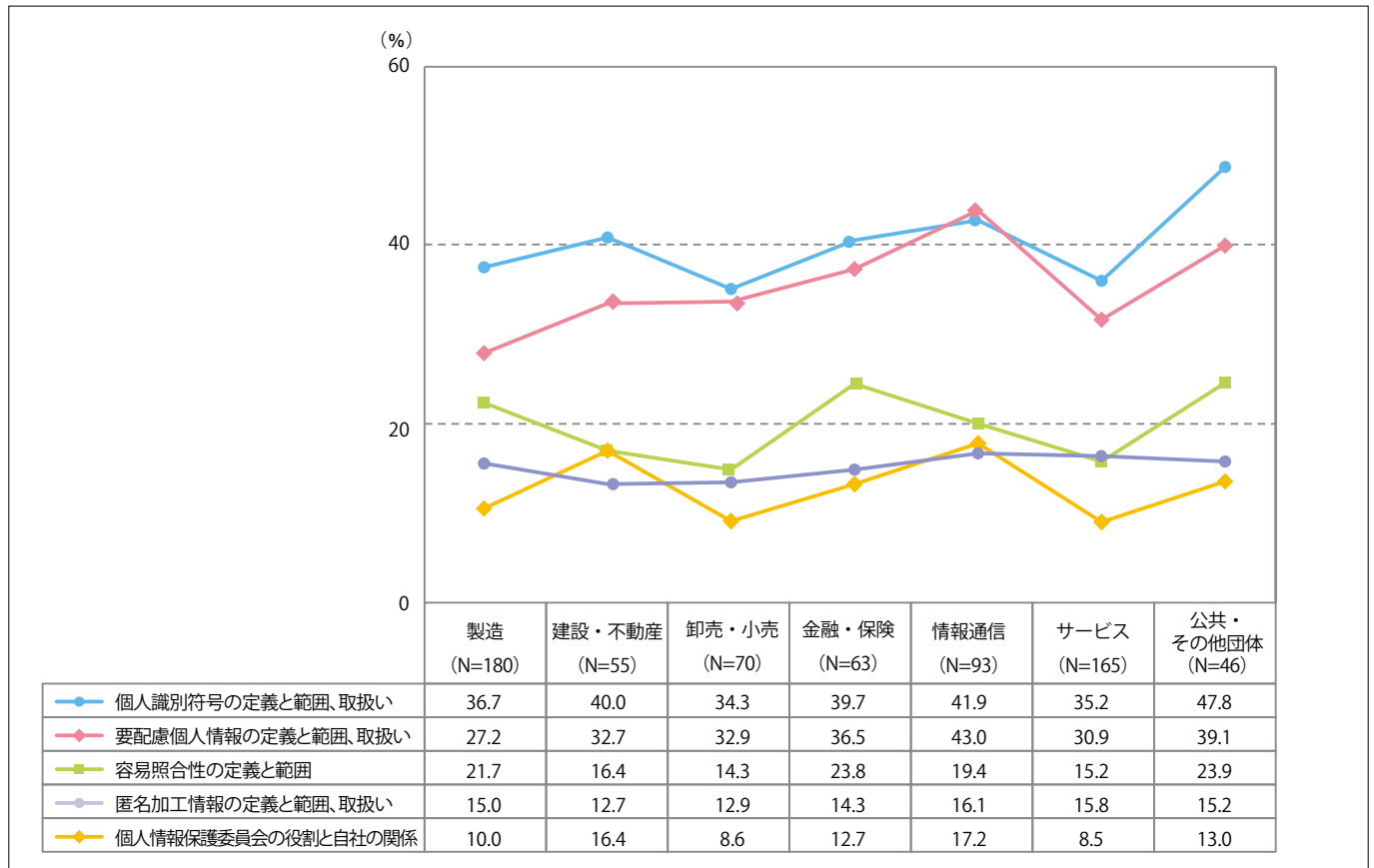


図1-21. 改正個人情報保護法で気に入っている点(業種別)

## 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。

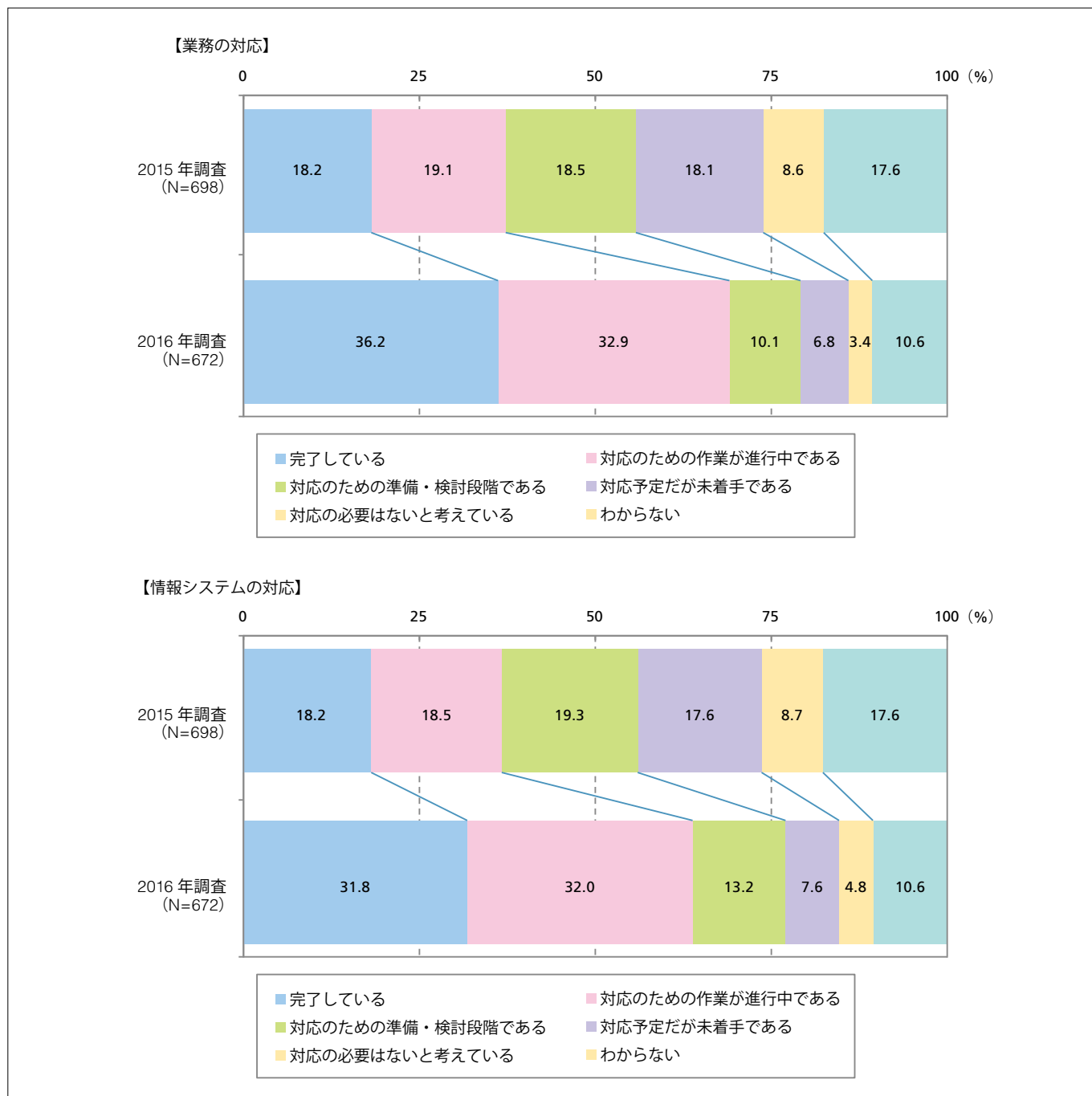


図1-22. マイナンバー制度への対応状況の経年比較(2015～2016年)

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)。

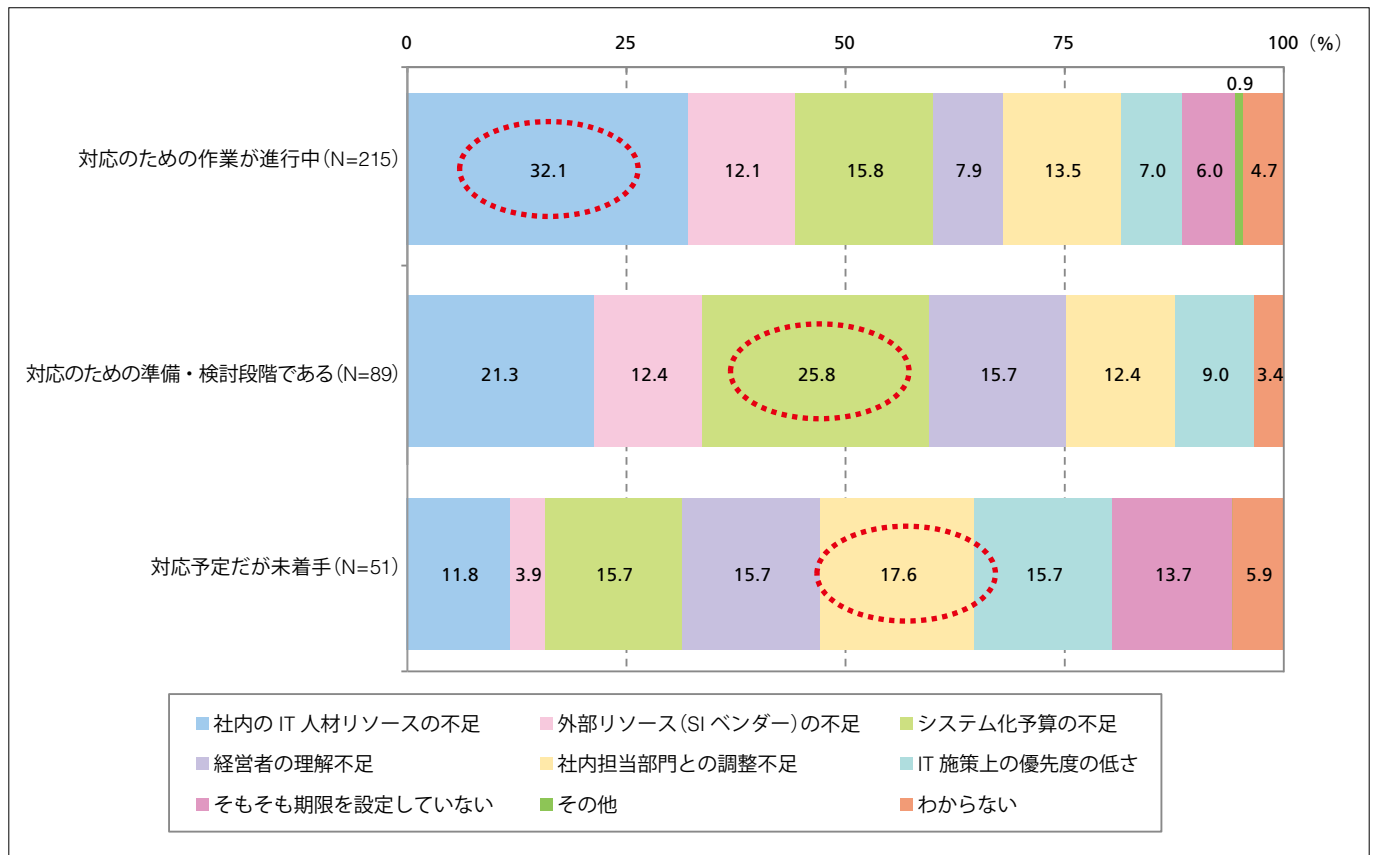


図1-23. 情報システムの対応が完了していない理由(進捗状況別)

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変更」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、こ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。

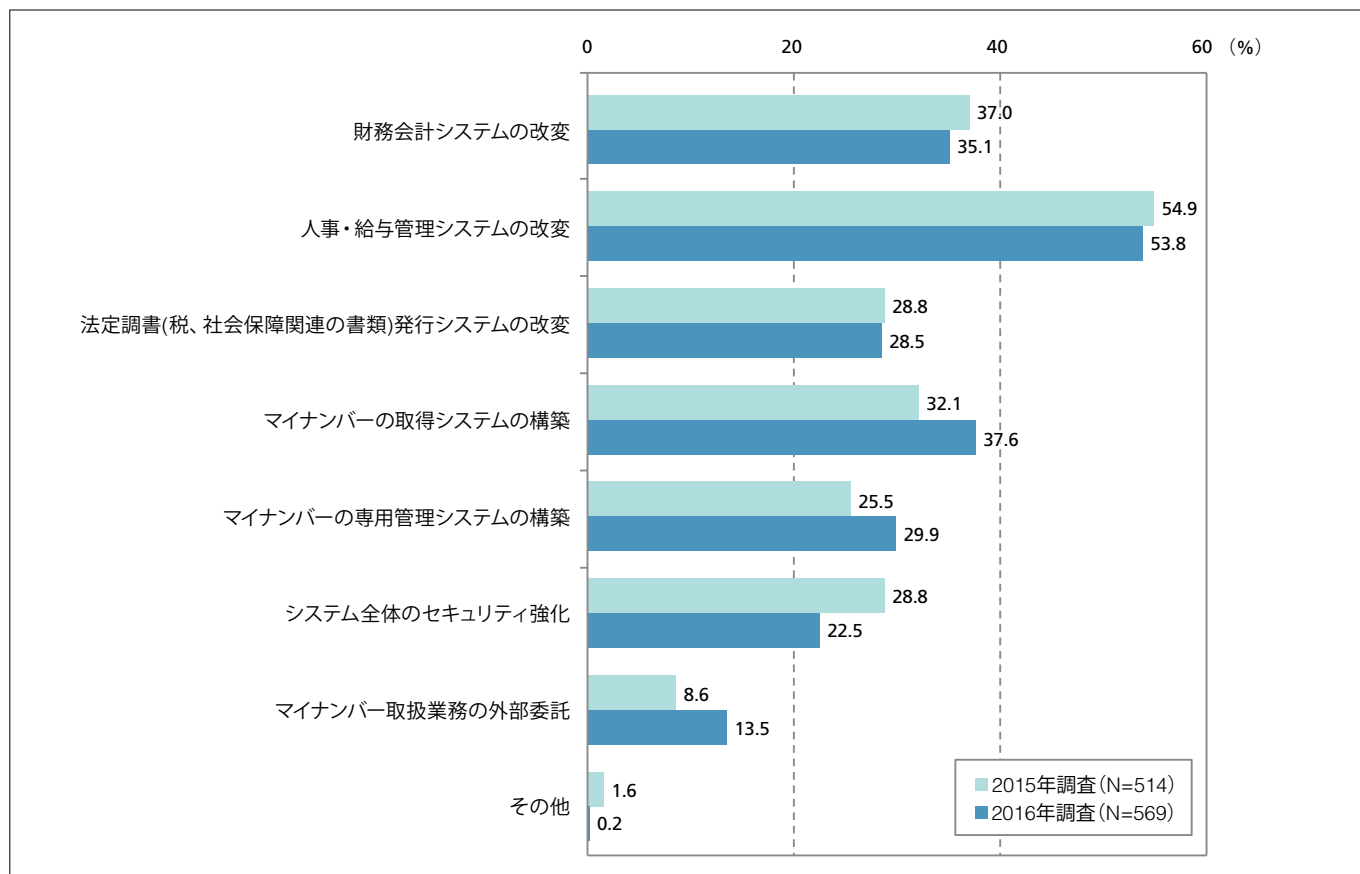


図1-24. マイナンバー制度への情報システムの対応範囲

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。

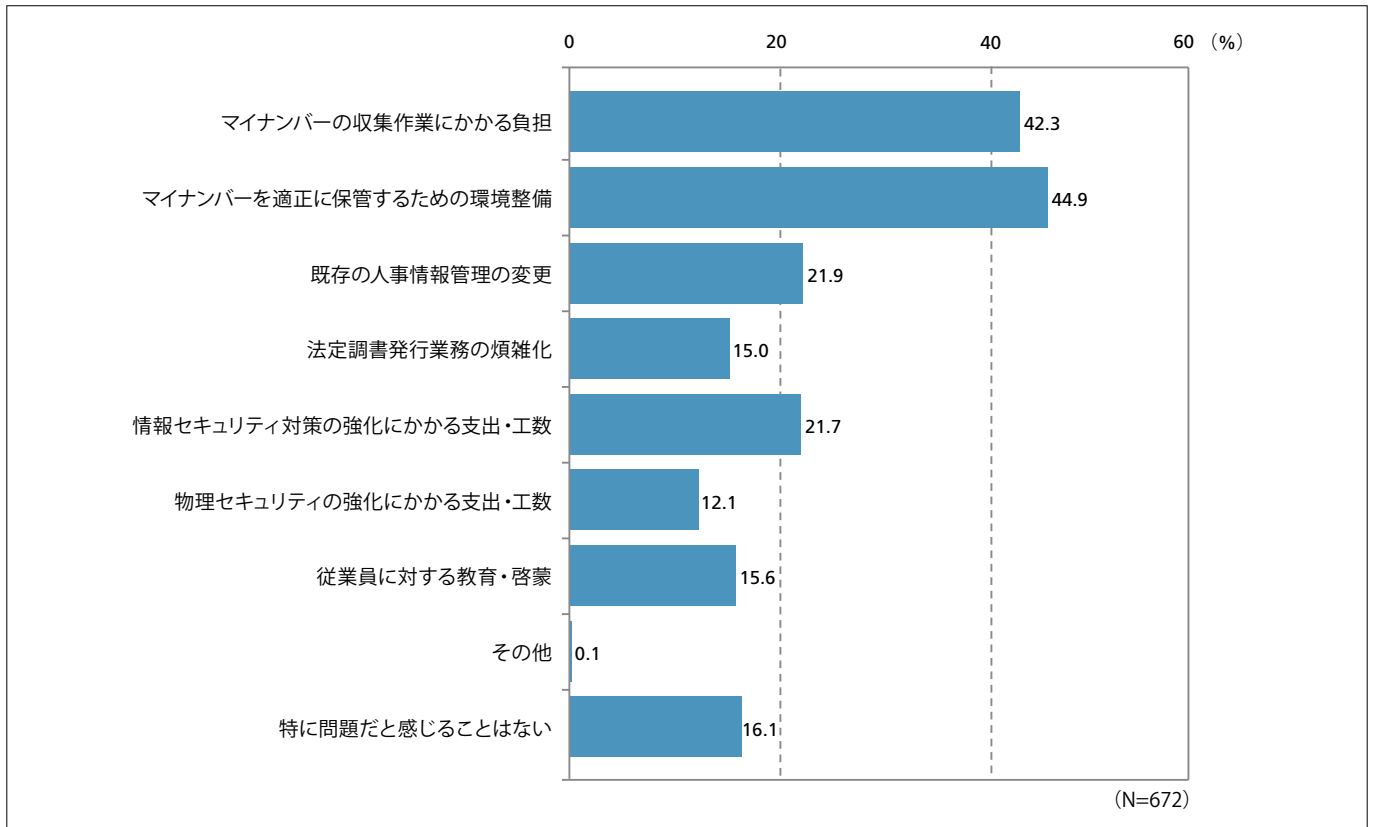


図1-25. マイナンバー制度対応における問題点

# 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とする。

## 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)。

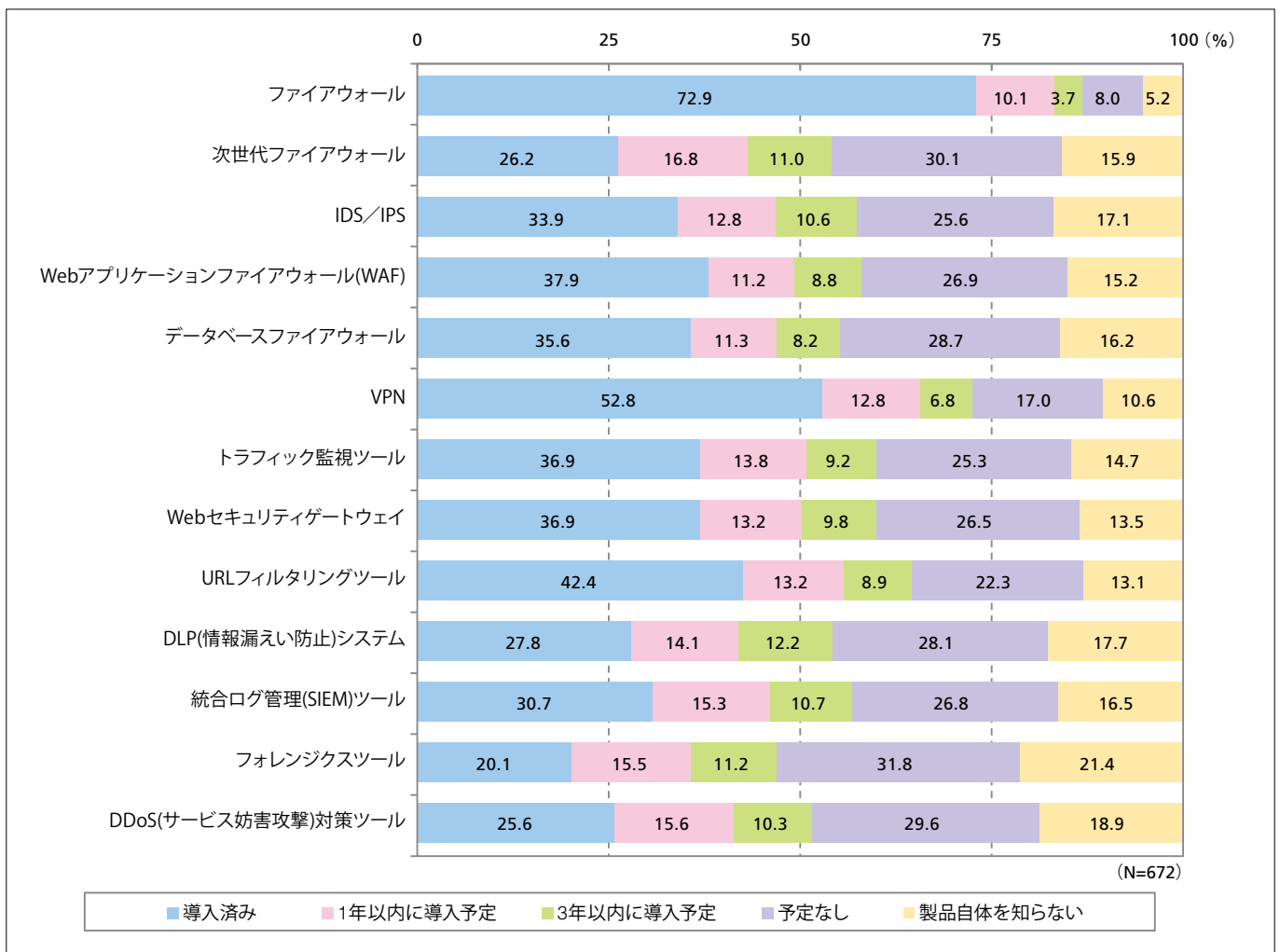


図1-26. セキュリティ製品の導入率(ネットワークセキュリティ)



## 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)。

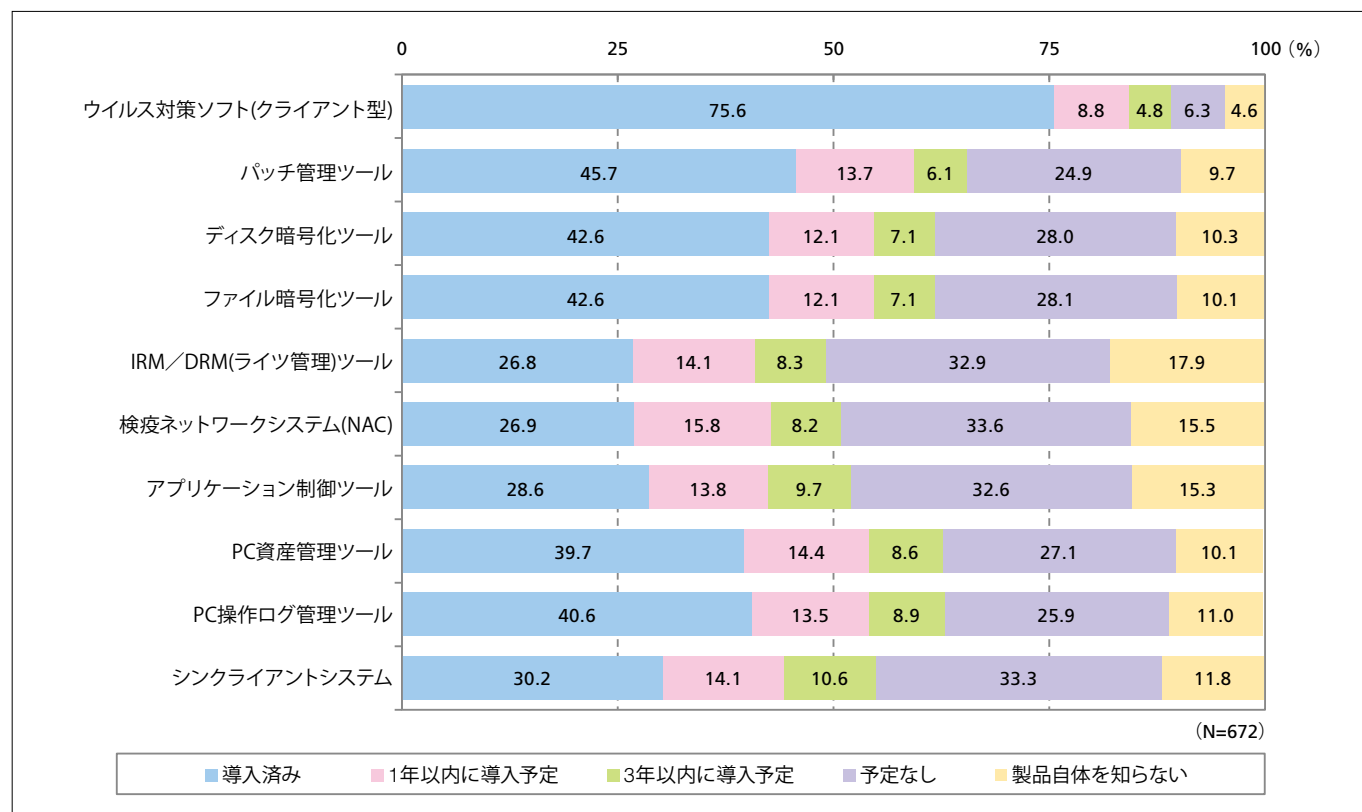


図1-27. セキュリティ製品の導入率(クライアントセキュリティ)

### 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)。

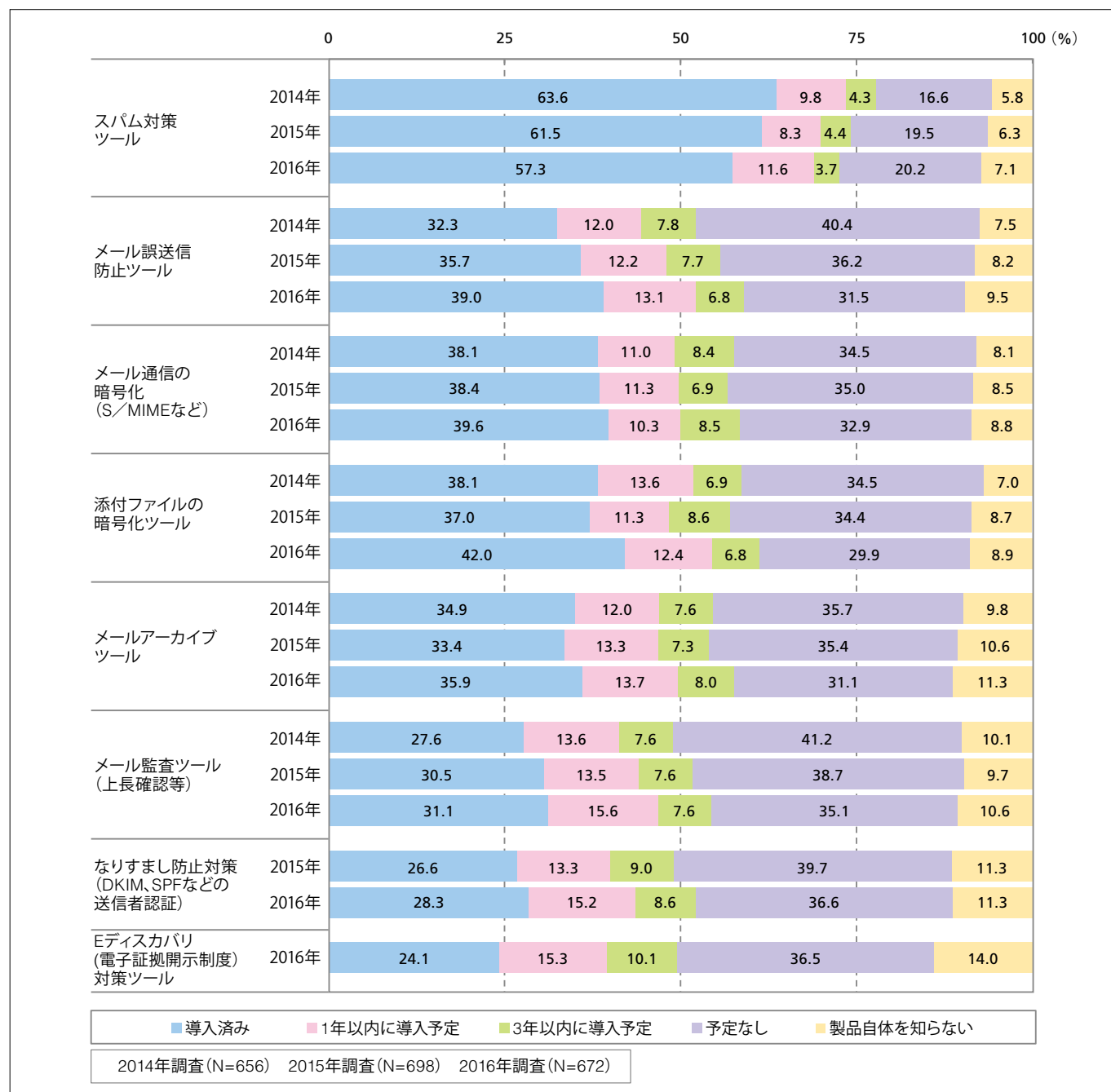


図1-28. セキュリティ製品の導入率(メールセキュリティ)

## 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)。

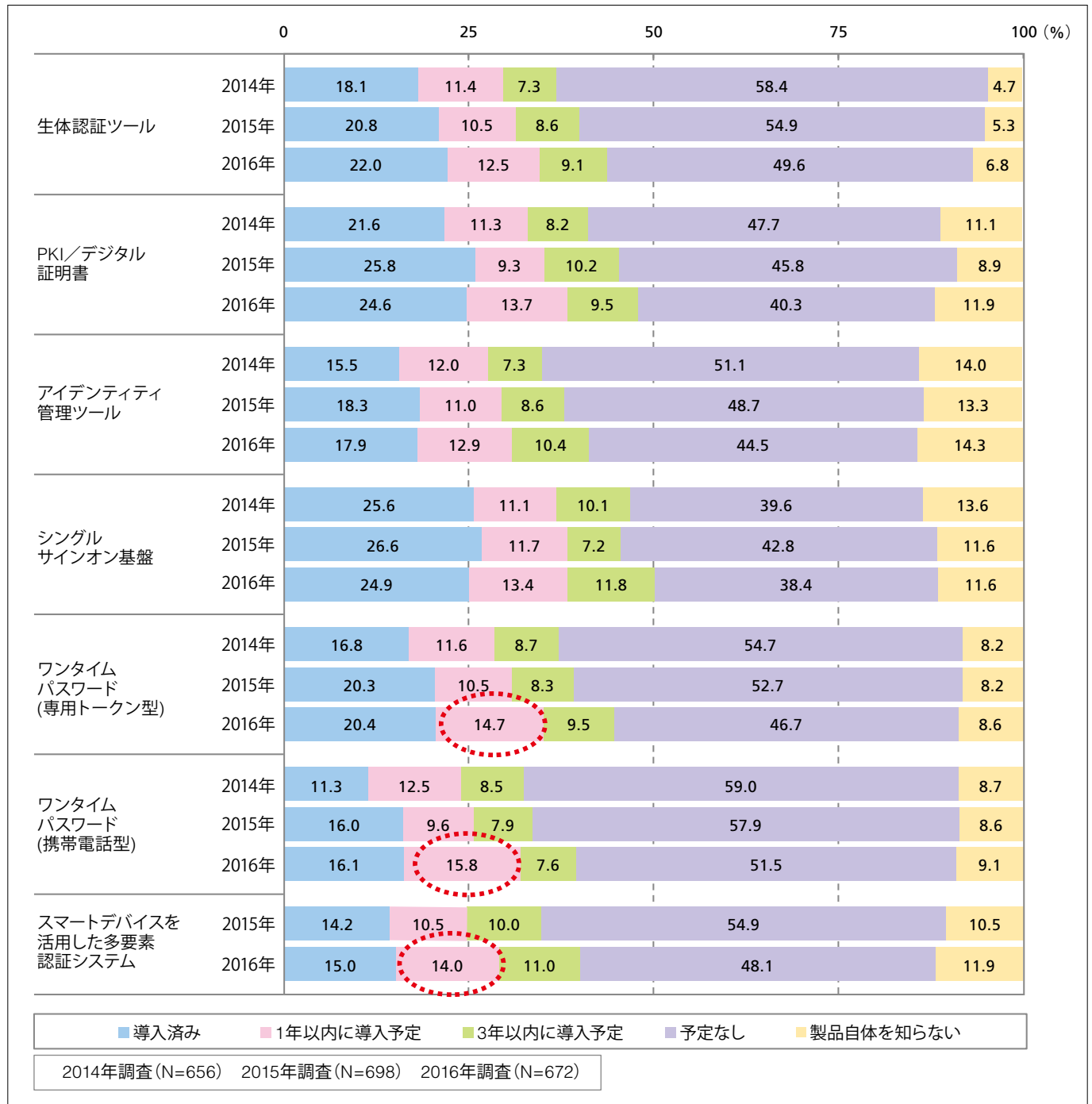


図1-29. セキュリティ製品の導入率(アクセス管理)

## 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)。

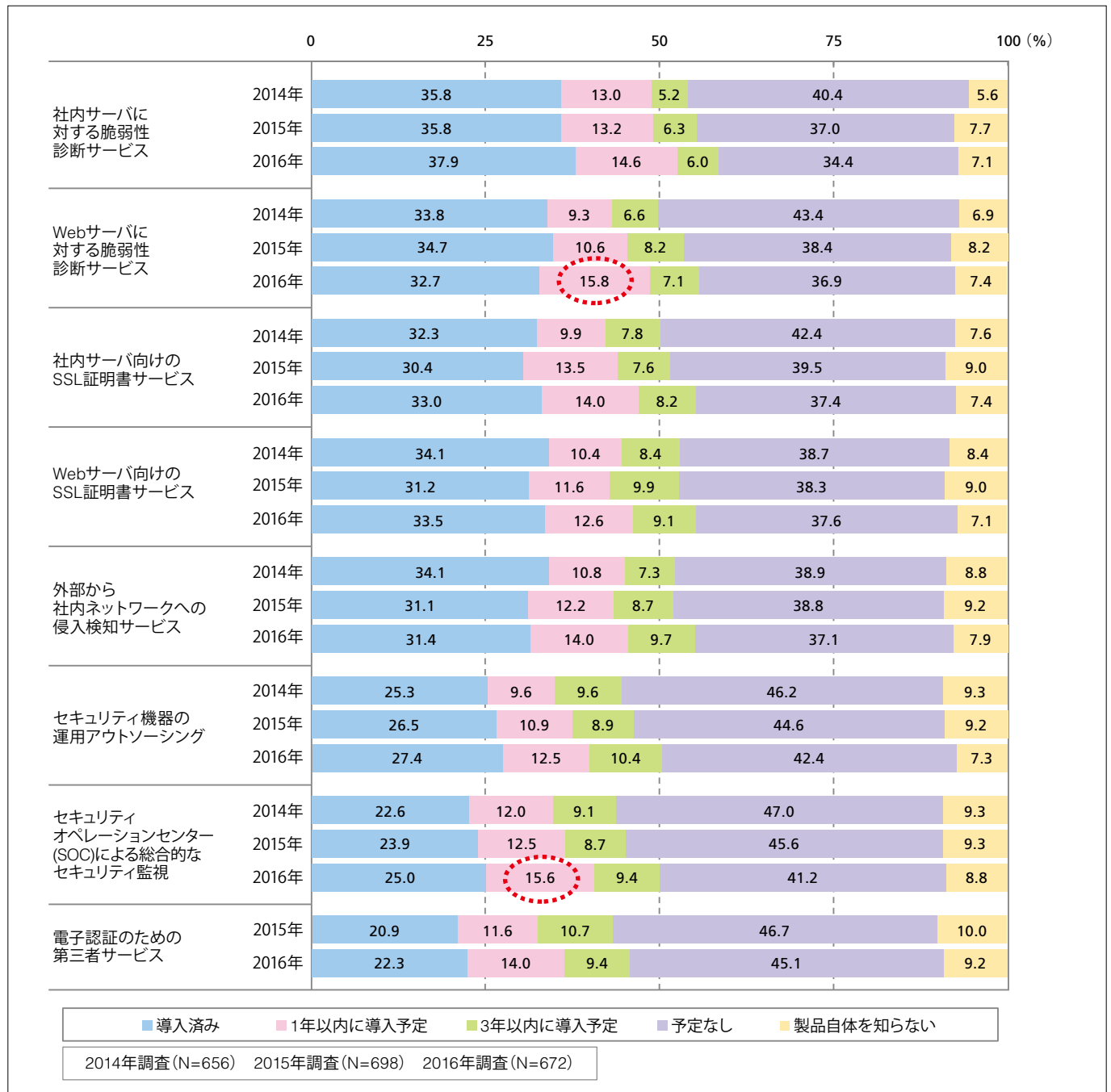


図1-30. セキュリティ製品の導入率(セキュリティサービス)

## 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。

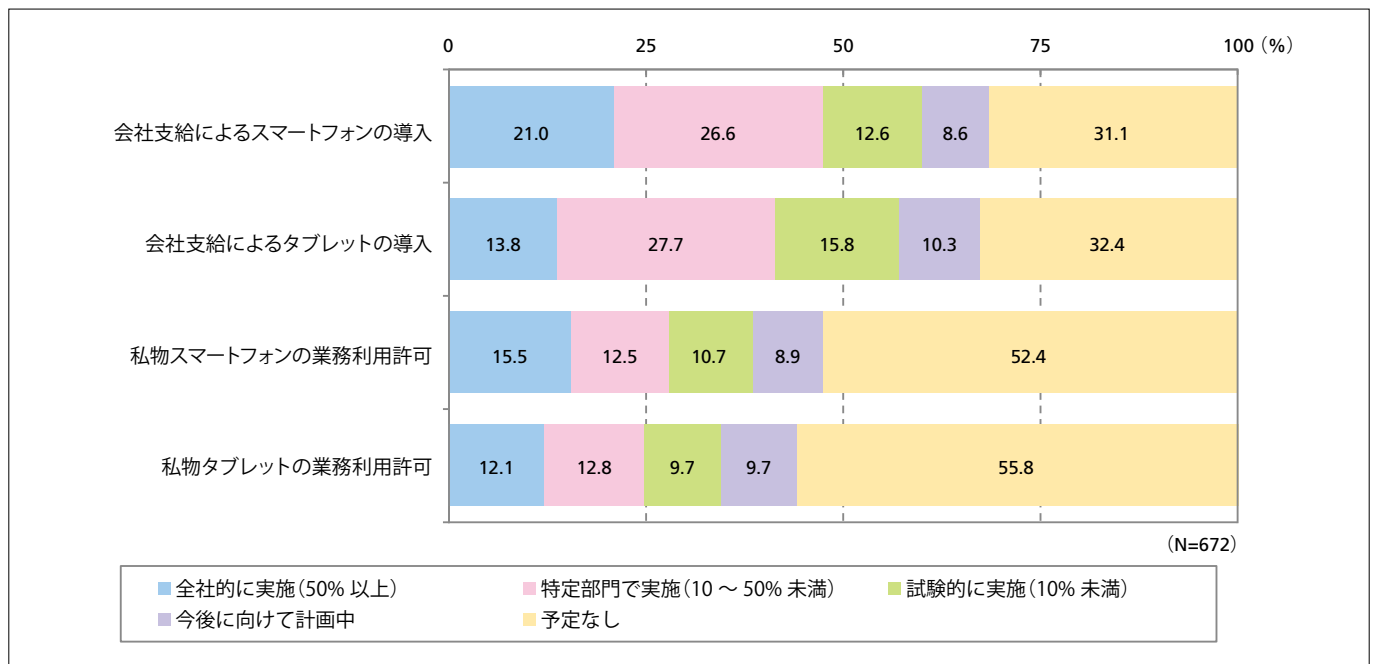


図1-31. スマートデバイスの導入状況

## 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事ができる。

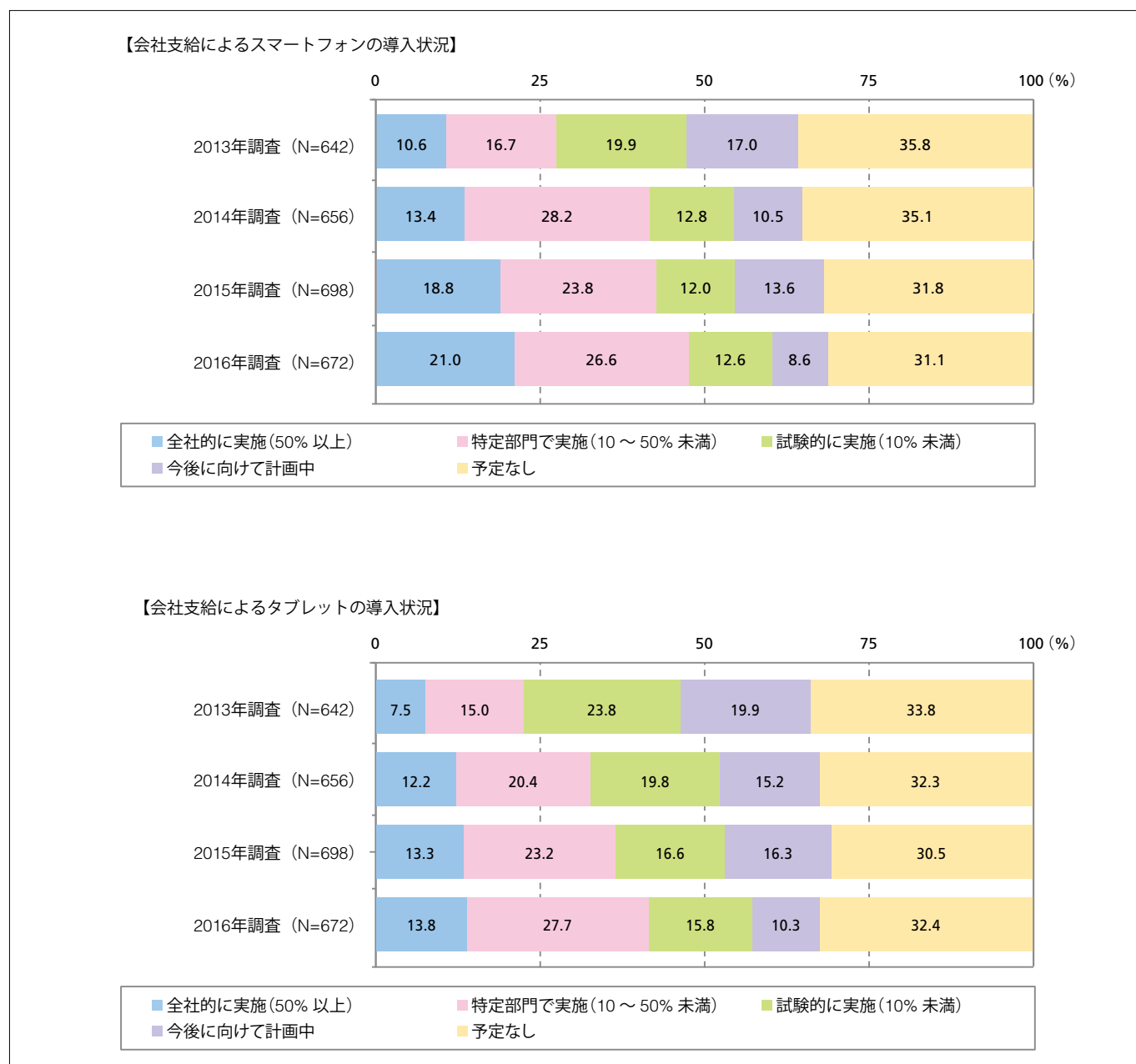


図1-32. スマートデバイスの導入状況の経年比較(2013~2016年)

### 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。

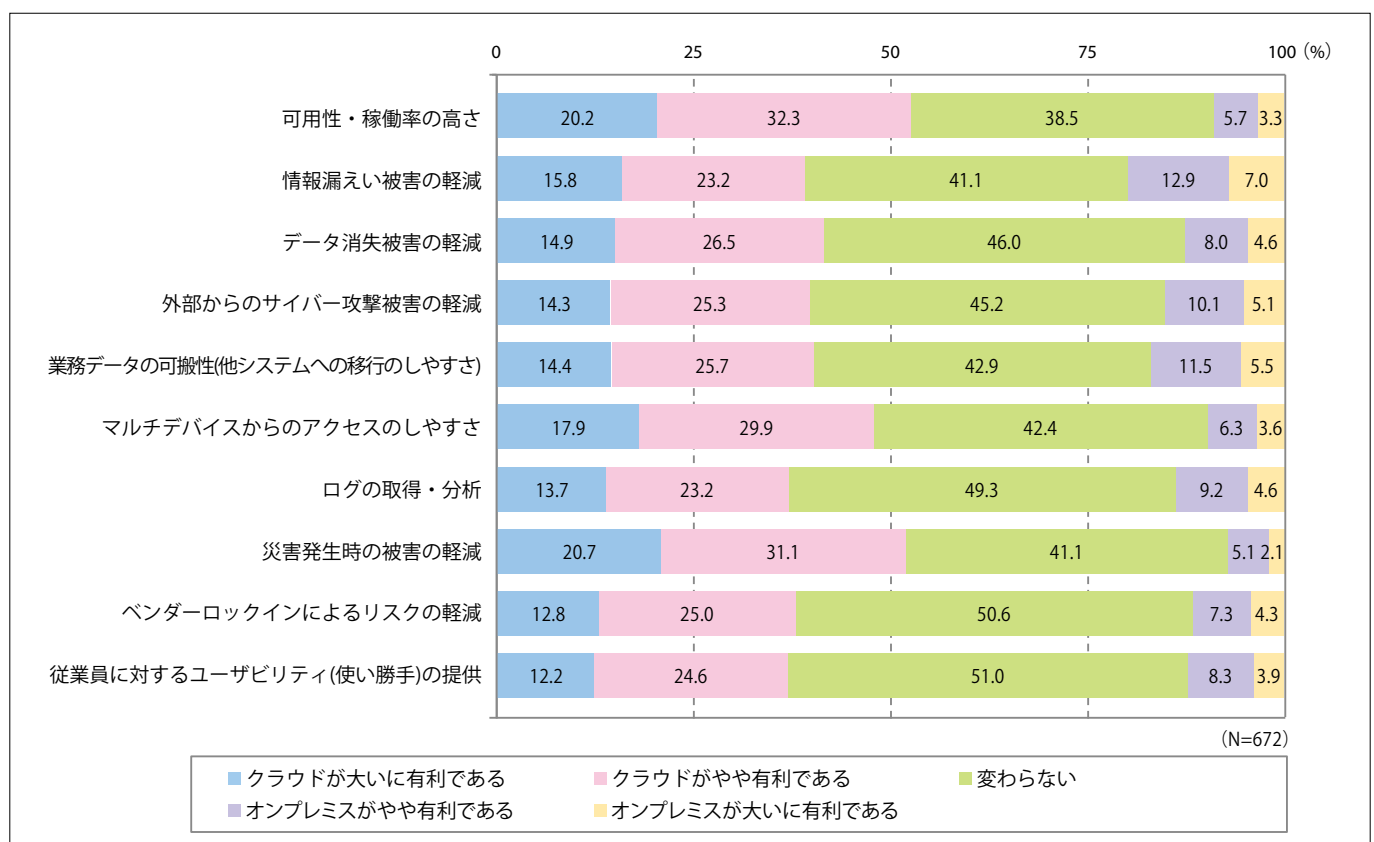


図1-33. 「クラウド」と「オンプレミス」に対する認識

\*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)。

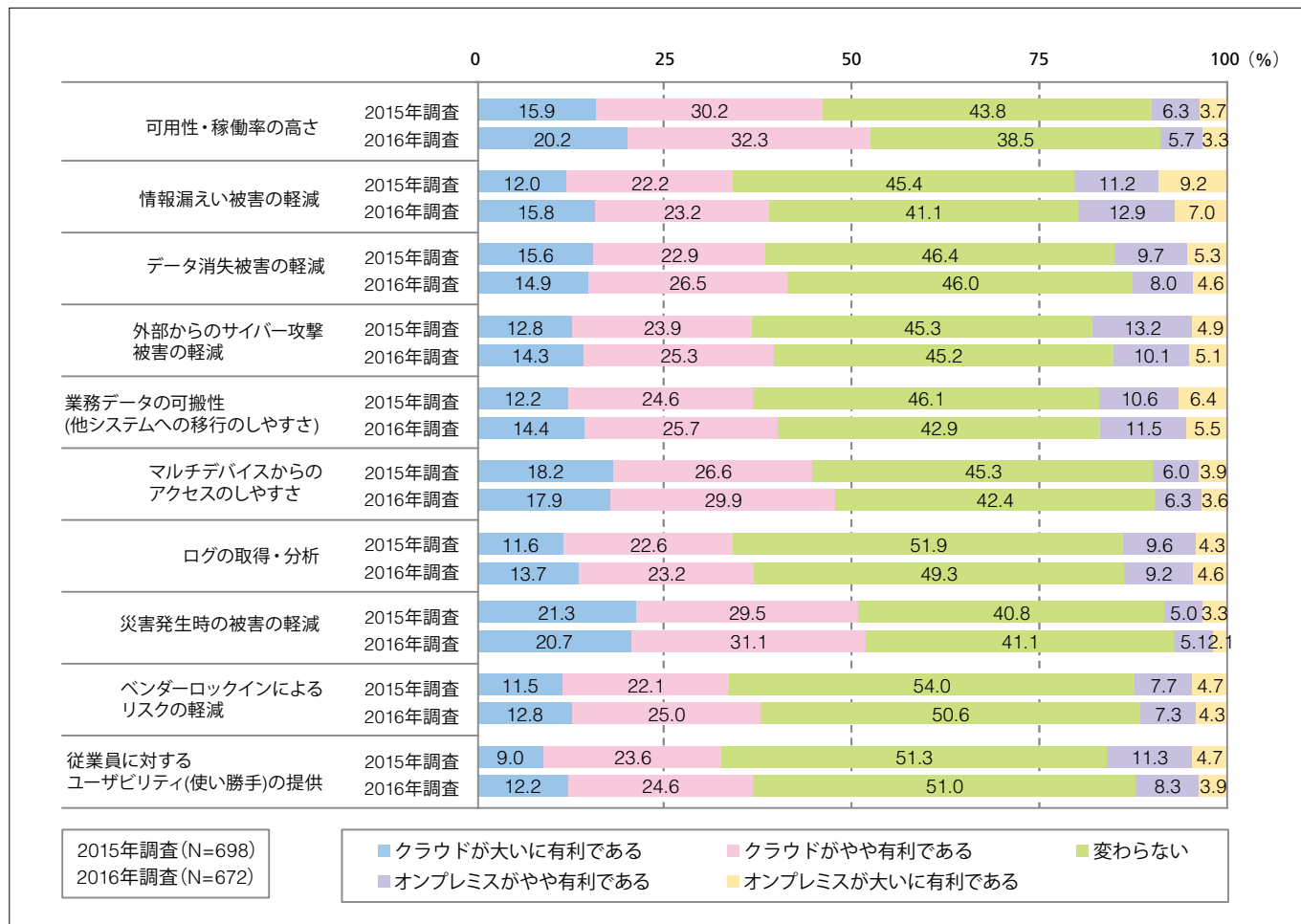


図1-34. 「クラウド」と「オンプレミス」に対する認識の経年比較(2015~2016年)



## 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見えてきた。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・小売・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

## 〈資料〉 データ編

データ編では、ITインフラ普及状況、産業・行政の各分野の情報化の進展状況、コンピュータ・情報サービス・電子商取引・電気通信の市場動向と、2015年10月から2016年3月までの情報化に関する動向を掲載しています。

### 情報源リスト

<b>1.世界のITインフラ普及状況</b>	
IT基本データ(ITインフラ普及状況、ユーザ数)	総務省(通信利用動向調査) 総務省(ブロードバンドサービスの契約数等) 一般社団法人電気通信事業者協会(TCA)
OECD各国の固定電話・ワイヤレスブロードバンド加入率(比較)	OECD「Broadband statistics」
<b>2.情報処理実態調査</b>	
1社平均情報処理関係諸経費と対年間事業収入比	経済産業省「情報処理実態調査」
<b>3.行政の情報化</b>	
国の行政機関が扱う申請・届出等手続きのオンライン利用状況(オンライン利用促進対象手続)	総務省「平成26年度における行政手続オンライン化等の状況」
国の行政機関が扱う手続き(オンライン利用状況)	
<b>4.コンピュータおよび関連装置の生産推移</b>	
コンピュータおよび関連装置の生産推移 コンピュータおよび関連装置の生産推移(数量) コンピュータおよび関連装置の生産推移(金額)	経済産業省「機械統計年報」
<b>5.情報サービス市場</b>	
情報サービス産業の年間売上高と常用従業員数	一般社団法人情報サービス産業協会(JISA)
<b>6.電子商取引市場</b>	
日本の電子商取引市場規模推移(BtoC)	経済産業省「電子商取引に関する市場規模・実態調査」
<b>7.電気通信市場</b>	
携帯電話・PHS・無線呼び出し・BWA累計契約数の推移	TCA、総務省 情報通信国際戦略局 「第3世代(3G)携帯電話の契約数の推移」
ブロードバンドサービス等の契約数の推移	総務省 総合通信基盤局 「ブロードバンドサービス等の契約数の推移」(2015/9末現在)
<b>8.情報化に関する動向</b>	2014年10月から2015年3月の動向

# 1

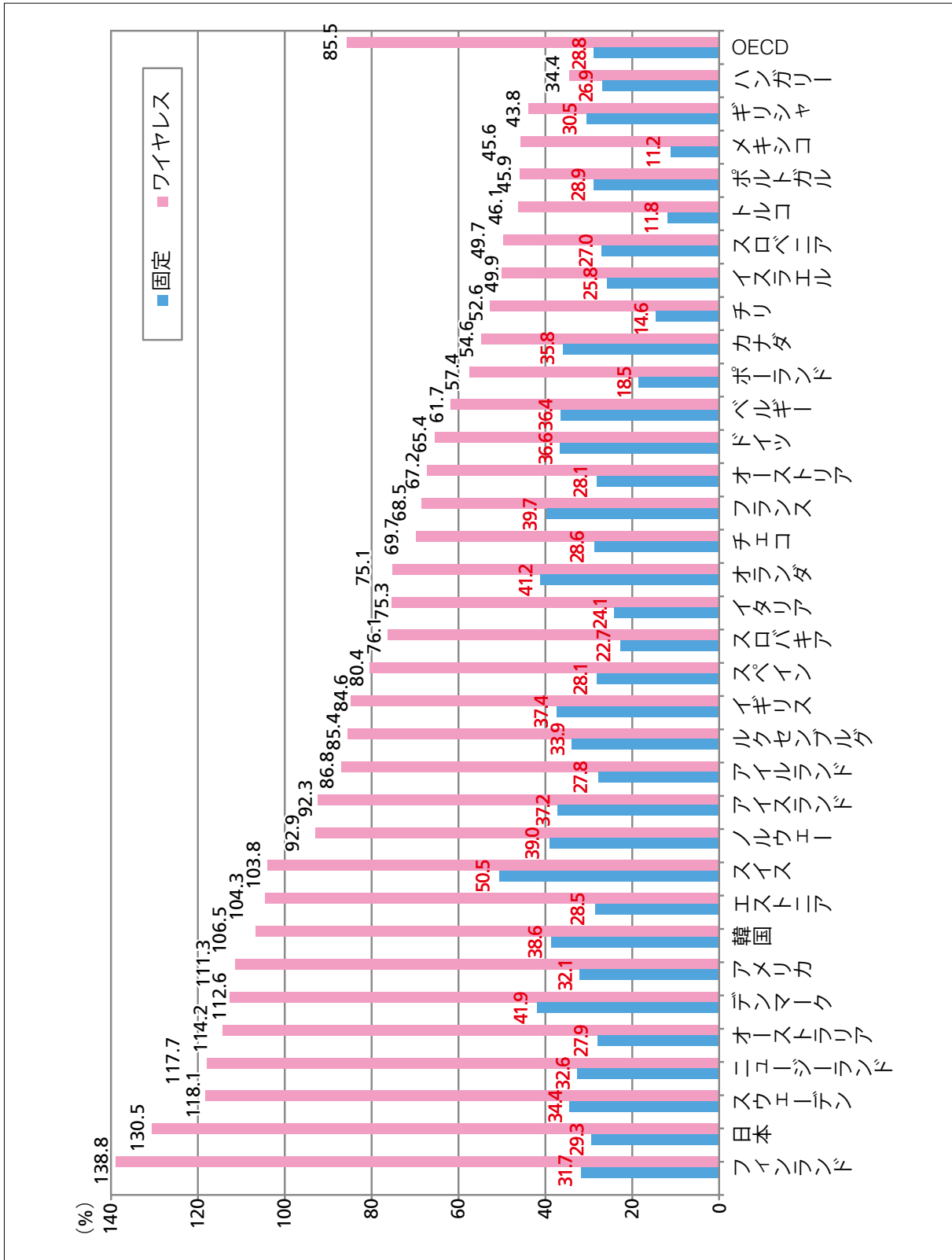
## 世界の IT インフラ普及状況

データ編/図表2-1.IT基本データ(ITインフラ普及状況、ユーザ数)

カテゴリ	統計データ (調査年月)	調査元・調査名	備考		
インターネットユーザ数	10,018 万人 人口普及率 82.8% (2014 年 12 月末)	総務省 (通信利用動向調査)	調査は毎年。利用端末別(PC, 携帯電話, 携帯情報端末, ゲーム機・TV) ユーザ数 (推計) を算出		
	10,044 万人 人口普及率 82.8% (2013 年 12 月末)				
ブロードバンド	CATV アクセスサービス 契約数	総務省 (ブロードバンドサービスの契約数等)	323 事業者の合計契約数		
				670 万 9,249 契約 (2015 年 12 月末)	
	DSL アクセスサービス 契約数			630 万 8,177 契約 (2014 年 12 月末)	
				331 万 8,343 契約 (2015 年 12 月末)	
	FTTH アクセスサービス 契約数			392 万 1,870 契約 (2014 年 12 月末)	23 事業者の合計契約数
				2,757 万 6,762 契約 (2015 年 12 月末)	
	FWA アクセスサービス 契約数			2,634 万 3,956 契約 (2014 年 12 月末)	258 業者の合計契約数
				6,426 契約 (2015 年 12 月末)	
	BWA アクセスサービス 契約数			7,340 契約 (2014 年 12 月末)	46 事業者の合計契約数
				3,087 万 9,897 契約 (2015 年 12 月末)	
	3.9 世代携帯電話アクセス サービス契約数			1,491 万 9,380 契約 (2014 年 12 月末)	26 事業者の合計契約数
				8,274 万 9,785 契約 (2015 年 12 月末)	
携帯電話・PHS アクセスサー ビス契約数	6,187 万 2,640 契約 (2014 年 12 月末)	4 事業者の合計契約数			
	1 億 5,815 万 6,161 契約 (2015 年 12 月末)				
携帯電話契約数	1 億 5,451 万 1,501 契約 (2014 年 12 月末)	4 事業者の合計契約数			
	1 億 5,648 万 700 契約 (2016 年 3 月末)				
携帯電話契約数	1 億 4,783 万 9,700 契約 (2015 年 3 月末)	一般社団法人 電気通信事業者協会	3 事業者の合計契約数 PHS ユーザは含まない。		

<資料>各種公表資料より作成

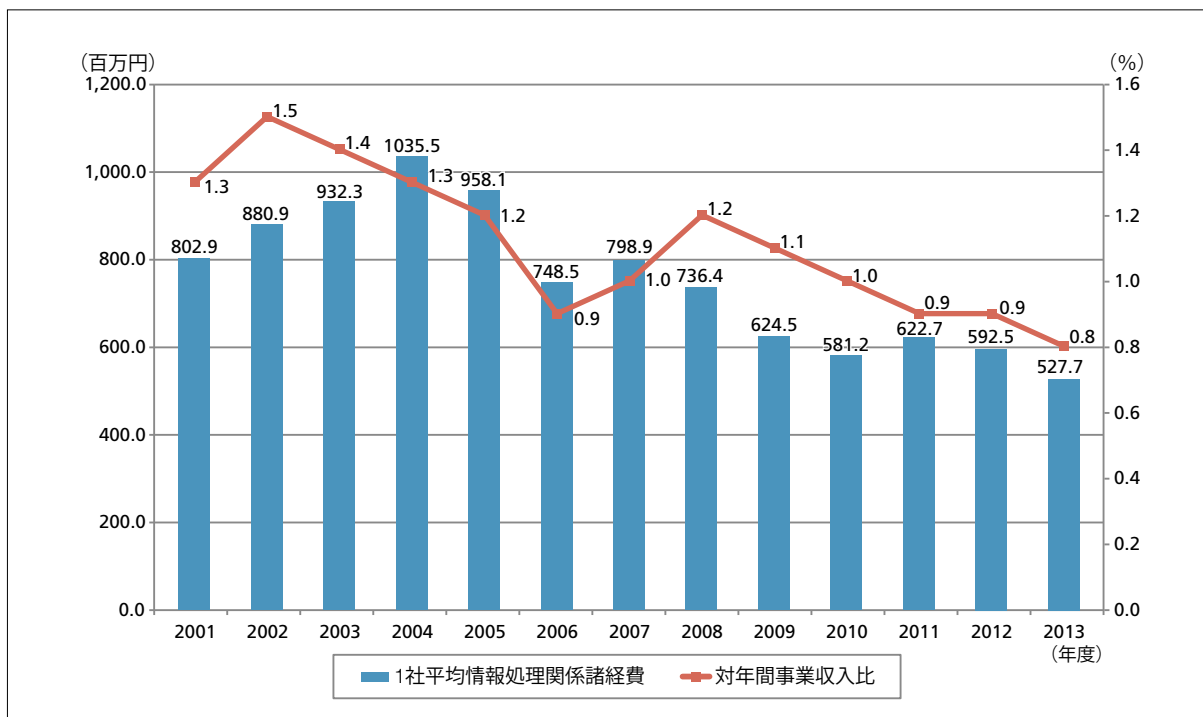
データ編/図表2-2.OECD各国の固定電話・ワイヤレスブロードバンド加入率(比較) (2015年第2四半期)



<資料> OECD「Broadband statistics」OECD (2016), Wireless mobile broadband subscriptions (indicator). doi: 10.1787/1277ddc6-en (Accessed on 15 April 2016)

## 2 情報処理実態調査

データ編/図表2-3.1社平均情報処理関係諸経費と対年間事業収入比



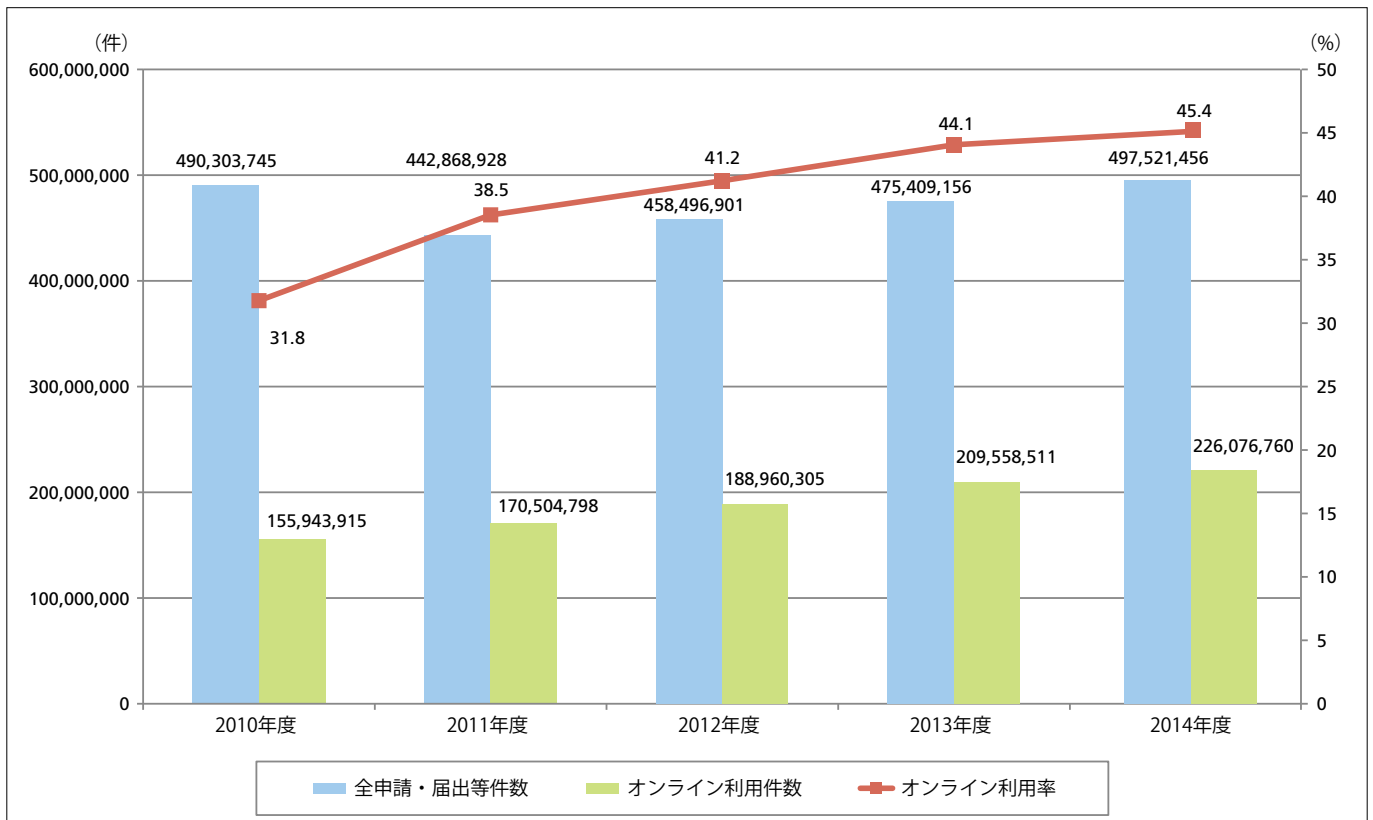
	1社平均情報処理関係諸経費 (百万円)	前年度比 (%)	対年間事業収入比 (%)
2001年度	802.9	85.1	1.3
2002年度	880.9	109.7	1.5
2003年度	932.3	105.8	1.4
2004年度	1,035.5	111.1	1.3
2005年度	958.1	92.5	1.2
2006年度	748.5	75.6	0.9
2007年度	798.9	106.7	1.0
2008年度	736.4	92.2	1.2
2009年度	624.5	84.8	1.1
2010年度	581.2	93.1	1.0
2011年度	622.7	107.1	0.9
2012年度	592.5	95.2	0.9
2013年度	527.7	89.1	0.8

(注) 1.一社平均情報処理関係諸経費については、小数点第2位以下を切捨て  
 2.2006年度以前は、情報処理関係諸経費とは、「コンピュータ・FAX・携帯情報端末関連費用計」+「ソフトウェア関連費用計」+「サービス関連費用計」+「その他費用」をいう。  
 3.2007年度より、情報処理関係諸経費とは、「コンピュータ・周辺機器関連費用計」+「通信機器関連費用計」+「その他の情報機器関連費用計」+「ソフトウェア関連費用計」+「サービス関連費用計」+「その他費用」をいう。

<資料>経済産業省 「情報処理実態調査」

# 3 行政の情報化

データ編/図表2-4.国の行政機関が扱う申請・届出等手続きのオンライン利用状況(オンライン利用促進対象手続)



「オンライン利用拡大行動計画」(平成20年9月12日IT戦略本部決定。以下「拡大行動計画」という。)において、「利用率が極めて低調である等の手続のオンライン化については見直しを図る」とされたことから、2010年度にオンライン利用の見直しが行われた。

<資料>総務省「平成26年度における行政手続オンライン化等の状況」(2015年12月)

データ編/図表2-5.国の行政機関が扱う手続き(オンライン利用状況)

	全申請・届出等件数 (件)		オンライン利用件数 (件)		オンライン利用率 (%)	
		うち重点手続		うち重点手続		うち重点手続
2010年度	490,303,745		155,943,915		31.8	
	(438,352,232)	403,819,006	(155,414,761)	149,920,227	(35.5)	37.1
2011年度	442,868,928	405,824,947	170,504,798	163,807,924	38.5	40.4
2012年度	458,496,901	421,297,165	188,960,305	181,479,301	41.2	43.1
2013年度	475,409,156	432,579,446	209,558,511	199,656,173	44.1	46.2
		うち改善促進手続		うち改善促進手続		うち改善促進手続
2014年度	497,521,456	394,918,846	226,076,760	162,577,184	45.4	41.2

「オンライン利用拡大行動計画」(平成20年9月12日IT戦略本部決定。以下「拡大行動計画」という。)において、「利用率が極めて低調である等の手続のオンライン化については見直しを図る」とされたことから、2010年度にオンライン利用の見直しが行われた。

- (注) 1.改善促進手続は、国民や企業による利用頻度が高い年間申請等件数が100万件以上の手続及び100万件未満であっても主として企業等が反復的又は継続的に利用する手続をいい、2014年度では、オンラインで利用が可能な申請・届出等手続の全申請・届出等件数の79.4%(2014年度、497,521,456件中394,918,846件)を占めている。  
 2.改善促進手続は、2013年度まで取り組んだ「新たなオンライン利用に関する計画」において選定した「重点手続」のうち利用率の高い分野(90%以上)の手続き等を除いている。  
 3.2010年度の( )内の数値は、国勢調査の件数を除いた申請等件数、オンライン利用件数及びオンライン利用率を示している。

<資料>総務省「平成26年度における行政手続オンライン化等の状況」(2015年12月)

# 4 コンピュータおよび関連装置の生産推移

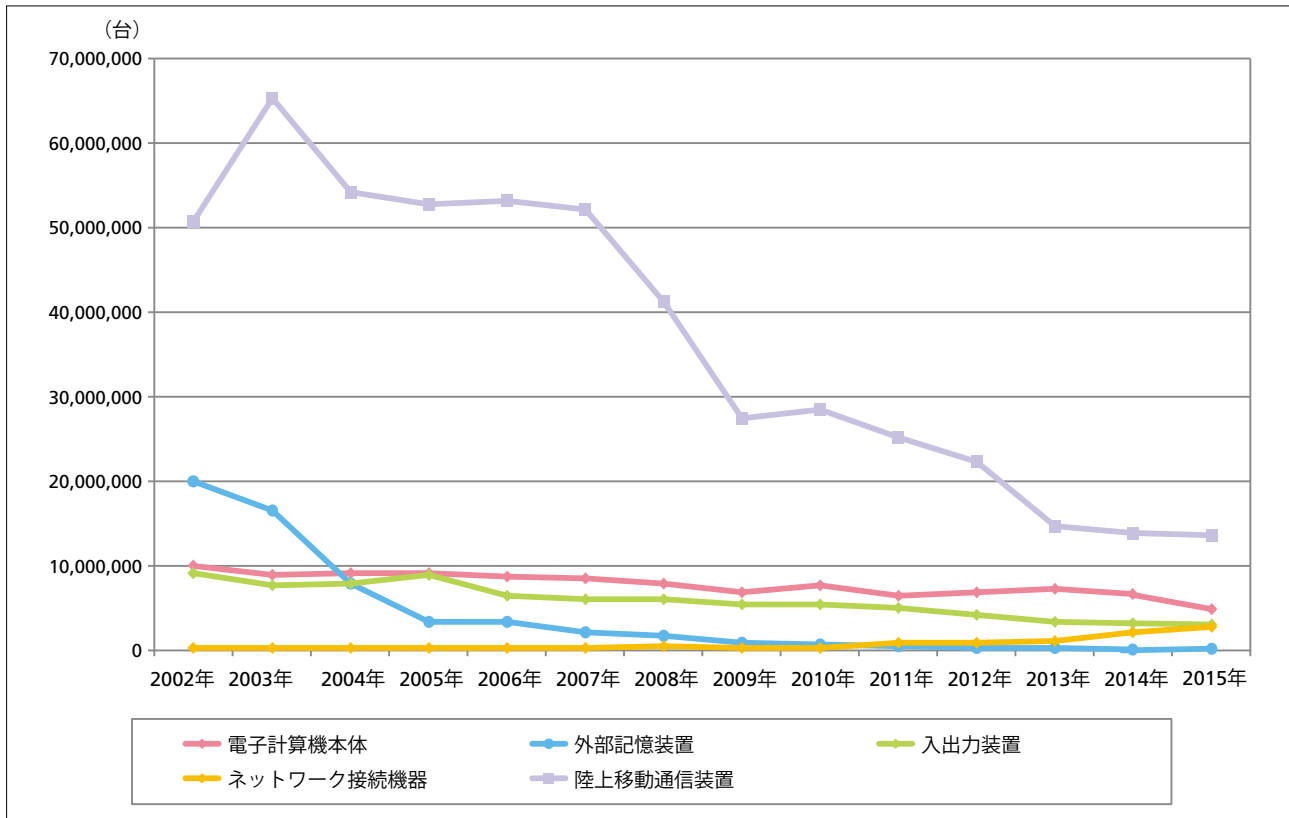
データ編/図表2-6.コンピュータおよび関連装置の生産推移

	2011年		2012年		2013年		2014年		2015年	
	数量(台)	金額(百万円)	数量(台)	金額(百万円)	数量(台)	金額(百万円)	数量(台)	金額(百万円)	数量(台)	金額(百万円)
電子計算機本体	6,386,237	720,658	6,823,572	713,883	7,357,375	735,021	6,619,607	726,046	4,458,707	592,894
汎用コンピュータ(メインフレーム)	342	25,563	290	40,976	312	40,342	223	41,647	203	27,928
ミッドレンジコンピュータ	166,408	114,330	168,113	98,695	139,631	83,044	124,672	82,436	119,114	82,951
パーソナルコンピュータ	6,219,487	580,765	6,655,169	574,212	7,217,432	611,635	6,494,712	601,963	4,339,390	482,015
サーバ用	142,685	58,617	152,070	54,327	158,091	60,268	149,938	62,051	149,454	73,223
デスクトップ型(タワー型および一体型を含む)	2,451,937	188,421	2,524,748	186,996	3,026,385	216,906	2,882,920	216,833	1,725,070	144,024
ノートブック型(タブレット型を含む)	3,624,865	333,727	3,978,351	332,889	4,032,956	334,461	3,461,854	323,079	2,464,866	264,768
周辺装置	5,534,218	340,615	4,531,161	337,861	3,554,526	327,185	3,304,498	315,282	3,210,173	301,486
外部記憶装置	446,188	181,280	306,139	190,066	233,231	185,424	110,013	169,028	119,582	162,550
磁気ディスク装置	—	—	—	—	—	—	—	—	—	—
光ディスク装置	67,688	1,270	43,975	824	27,211	518	—	—	—	—
ディスクアレイ装置	36,228	166,553	43,247	174,012	40,431	172,050	33,628	161,790	30,704	155,643
その他の外部記憶装置(※)	342,272	13,457	218,917	15,230	165,589	12,856	76,385	7,238	88,878	6,907
入出力装置	5,088,030	159,335	4,225,022	147,795	3,321,295	141,761	3,194,485	146,254	3,090,591	138,936
プリンタ	3,825,276	92,503	2,946,569	84,930	1,952,425	74,617	1,745,448	79,112	1,861,919	80,209
モニタ(電子計算機用)	1,236,157	58,599	1,260,518	55,155	1,354,557	58,628	1,449,037	67,142	1,228,672	58,727
その他の入出力装置	26,597	8,233	17,935	7,710	14,313	8,516	—	—	—	—
ネットワーク接続機器	971,256	39,844	842,364	41,914	1,124,088	41,459	2,710,127	45,013	2,807,415	44,887
陸上移動通信装置	25,087,431	648,782	22,239,438	636,612	14,670,834	410,381	13,831,198	235,966	13,555,258	263,042
携帯電話(スマートフォンを含む)	19,793,759	572,455	17,234,948	564,637	8,761,871	300,109	7,838,063	186,609	8,152,905	192,309
公衆用 PHS 端末	1,797,917	24,938	1,225,286	15,460	1,301,891	12,745	815,201	7,439	524,818	3,410
その他の陸上移動通信装置	3,495,755	51,389	3,779,204	56,515	4,607,072	97,527	5,177,934	41,918	4,877,535	67,323

(注) 1.調査の対象事業所が国内で実際に生産(受託生産を含む。)した製品が対象となる。  
 ただし、仕掛中の半製品は除く。なお、生産には調査対象で他の製品に加工又は消費するために生産したものも含む。  
 2.生産金額は契約価格又は生産者販売価格により評価した金額をいう。  
 3.一印:実績のないもの。×印:1または2事業所の数値であるため秘密の保護上、秘匿したもの。  
 4.調査対象事業所の見直し等により、発生年月以前の数値と発生年月以降の数値をそのまま比較できない品目がある。  
 ※2011年度以降、「磁気ディスク装置」は「その他の外部記憶装置」に含む。

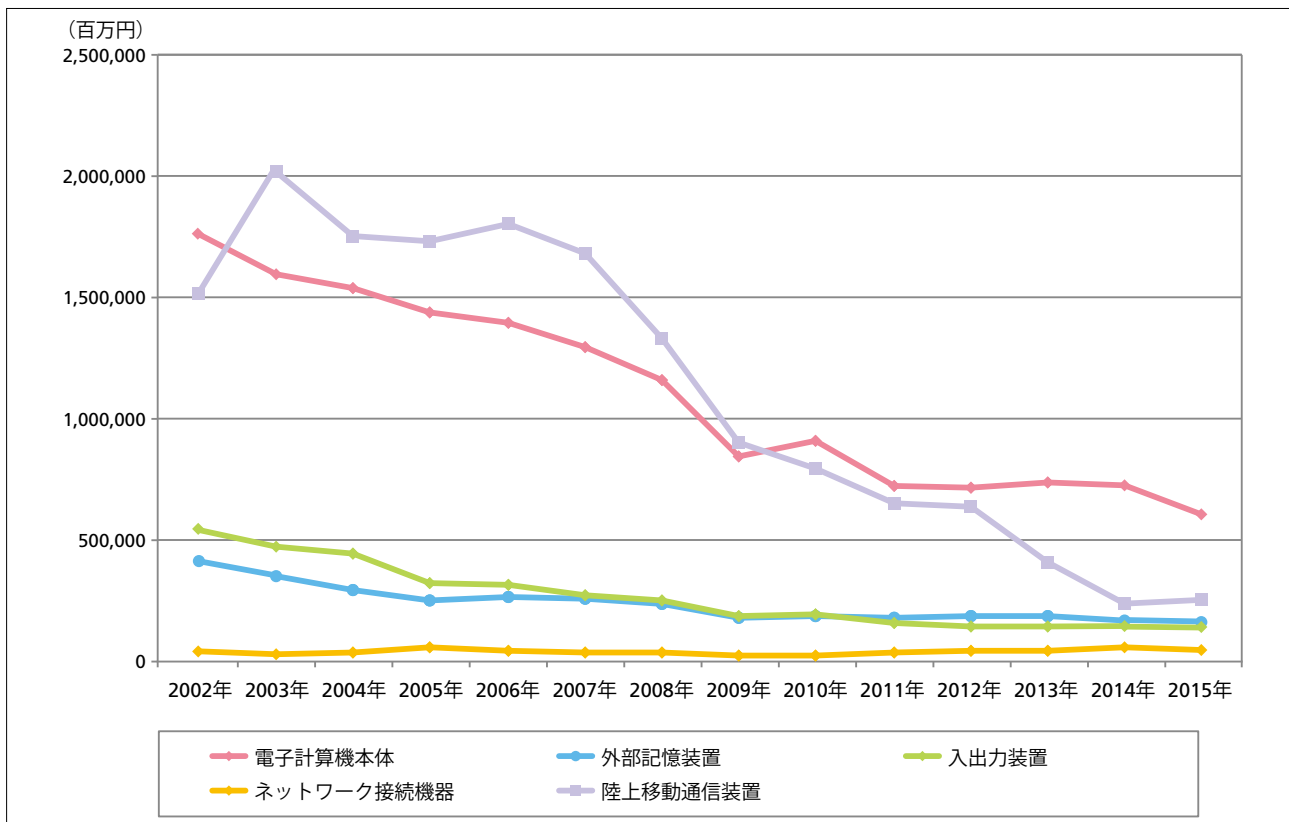


データ編/図表2-7. コンピュータおよび関連装置の生産推移(数量)



<資料> 経済産業省「機械統計年報」

データ編/図表2-8. コンピュータおよび関連装置の生産推移(金額)

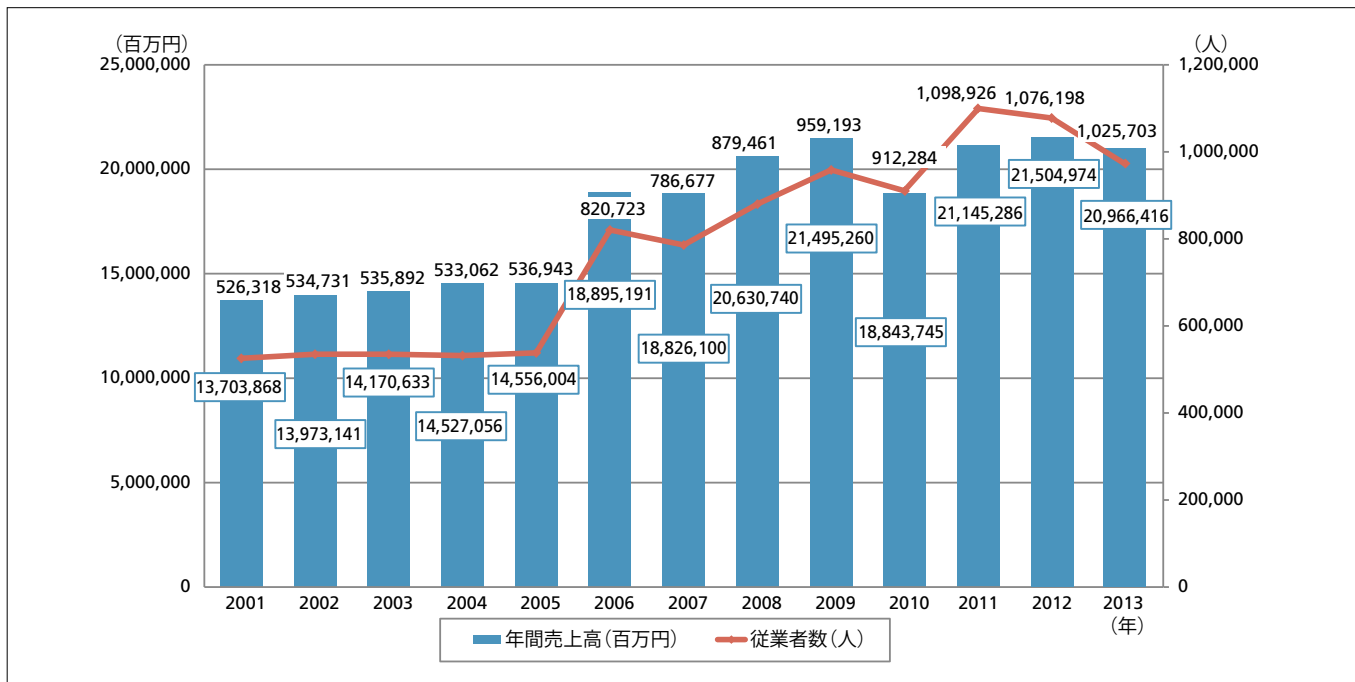


(注) 調査対象事業所の見直しにより、発生年月以前の数値と発生年月以降の数値をそのまま比較できない品目がある。

<資料> 経済産業省「機械統計年報」

# 5 情報サービス市場

データ編/図表2-9.情報サービス産業の年間売上高と常用従業員数

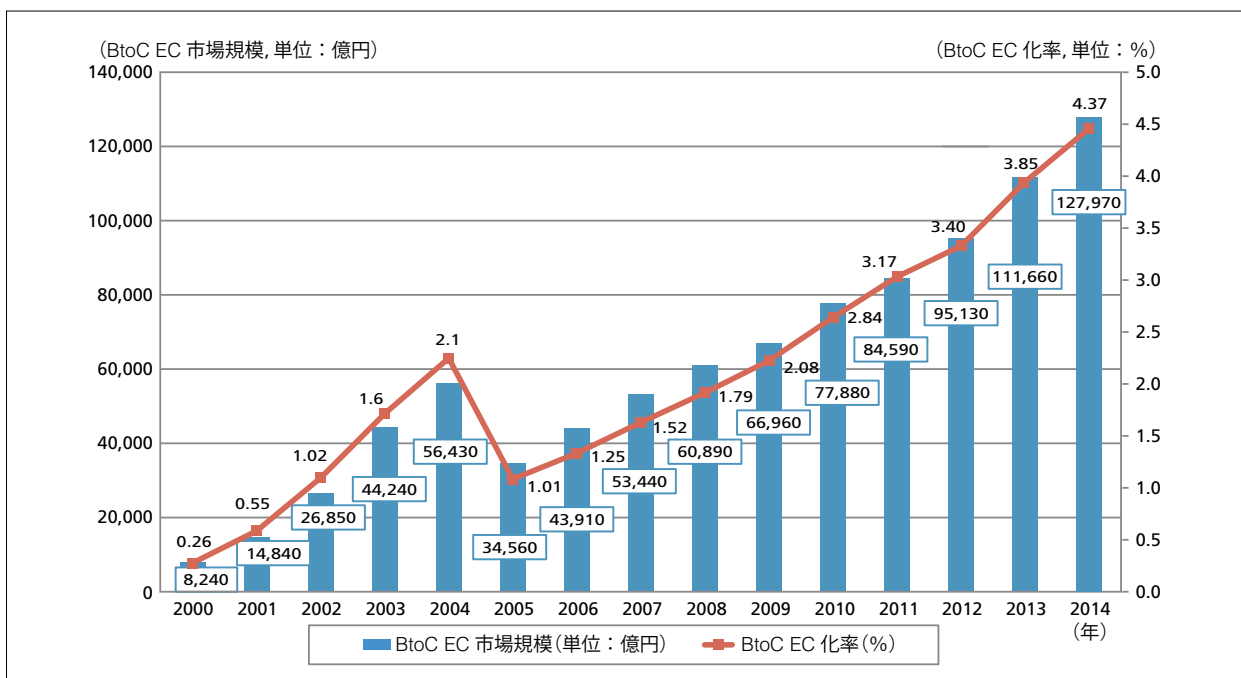


- (注) 1.2001、2006、2008、2009年は調査対象の見直し/拡大等があった。
- 2.2001～2005年の従業員数には「出向・派遣者(受入)」を含む。
- 3.2006～2013年の売上高には「情報サービス以外の売上げ」を含む。
- 4.2008～2009年は「インターネット付随サービス業」を含む。
- 5.2011年は「平成24年経済センサス-活動調査結果」の数値を使用

<資料>経済産業省・特定サービス産業実態調査および経済センサス-活動調査をもとに、一般社団法人情報サービス産業協会(JISA)で作成

# 6 電子商取引市場

データ編/図表2-10.日本の電子商取引市場規模推移(BtoC)

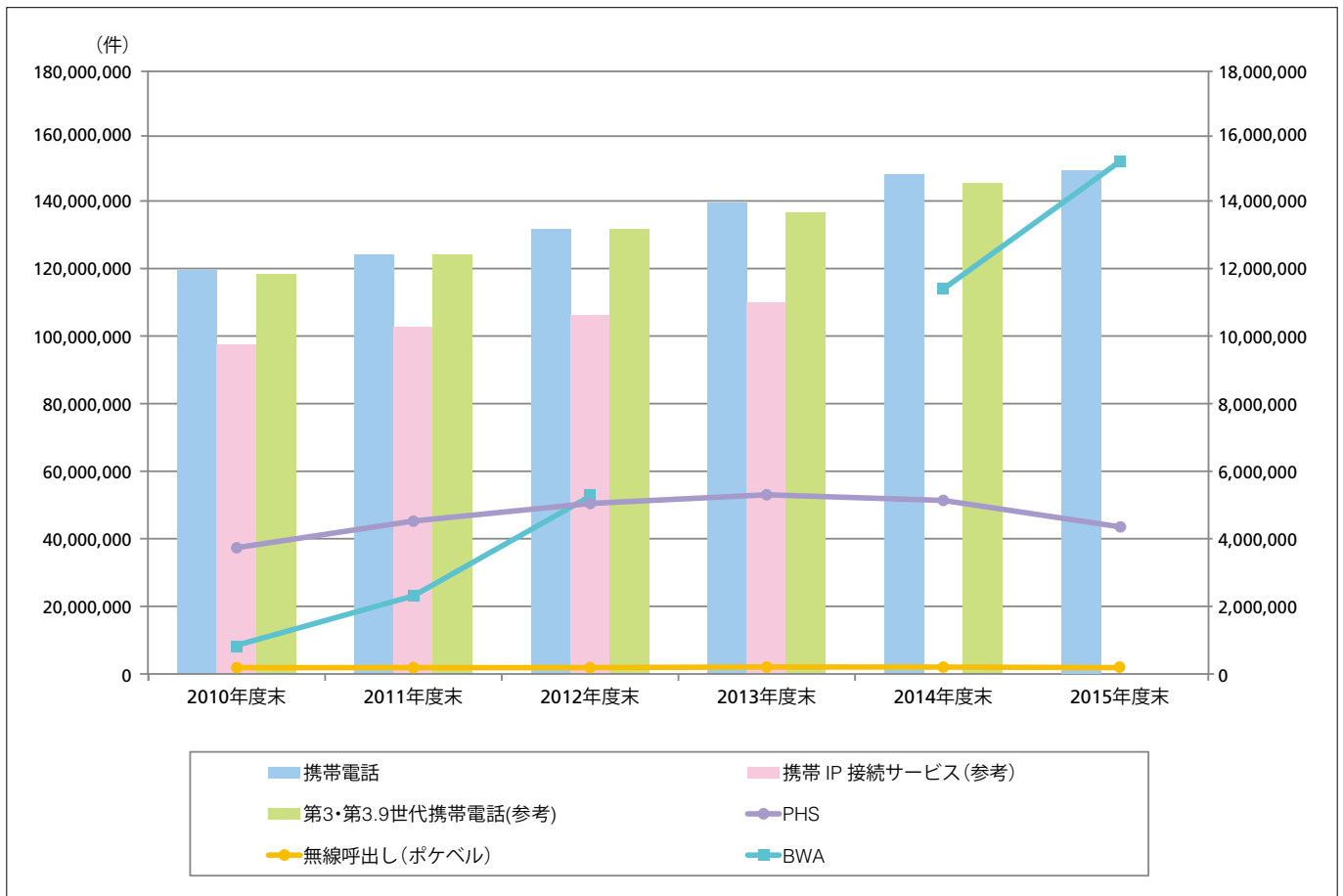


(注) 2005年より計測方法を変更

<資料>経済産業省「電子商取引に関する市場規模・実態調査」

# 7 電気通信市場

データ編/図表2-11. 携帯電話・PHS・無線呼出し・BWA累計契約数の推移



(件)

	2010 年度末	2011 年度末	2012 年度末	2013 年度末	2014 年度末	2015 年度末
携帯電話	119,535,344	128,204,758	136,043,361	144,014,699	152,697,747	154,419,395
携帯 IP 接続サービス (参考)	97,375,500	102,700,700	106,078,300	109,847,600	—	—
PHS	3,751,781	4,556,367	5,085,919	5,546,308	5,158,844	4,171,308
無線呼出し (ポケベル)	146,200	150,600	148,500	146,800	145,000	142,700
BWA	806,600	2,296,400	5,301,000	—	9,543,000	18,048,300
第3・第3.9世代携帯電話 (参考)	119,535,400	124,187,600	131,724,900	139,552,000	—	—

※1.イー・アクセスは2011.12末より契約数公表方法を変更し、TCAを通じた公表を行わないこととしているため、2011.12末以降の契約数には、イー・アクセス分は含まれておらず、「携帯電話・PHSの加入契約数の推移」において公表している契約数とは一致しない。

※2.2012年9月末以降KDDIおよびソフトバンクモバイルにおけるLTE契約数は、各社非公表としたためW-CDMA又はCDMA2000(第3世代)に計上されている。

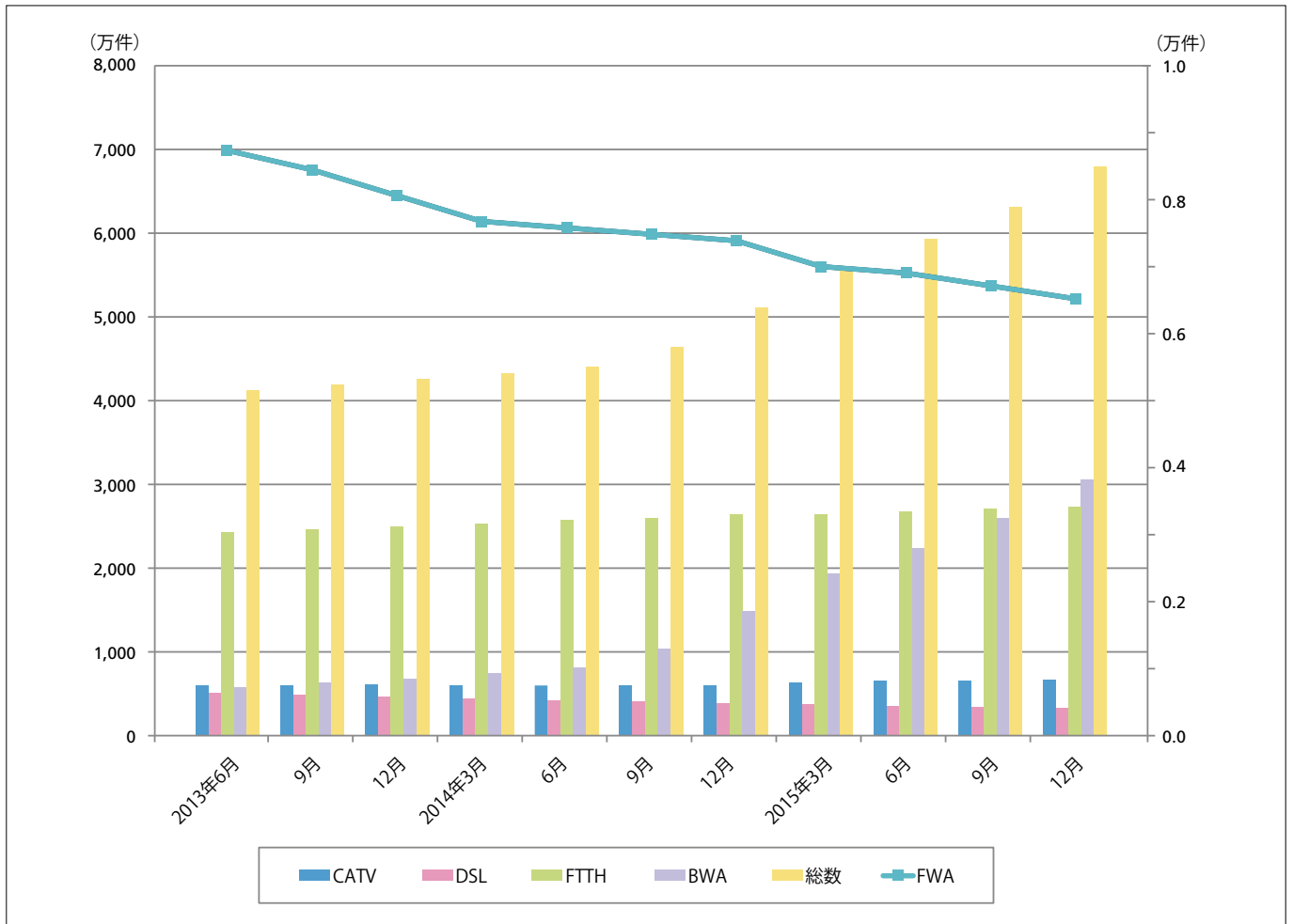
※3.2013年10月以降、PHSからの情報提供が取りやめられたため、契約数の掲載なし

※4.無線呼出し、BWAの最新加入数については、2015.12現在の加入数を計上

※5.第3・第3.9世代携帯電話の加入数については、TCAの公表項目が変更されたため、契約数の公開なし

<資料>一般社団法人電気通信事業者協会(TCA)、総務省 情報通信国際戦略局 「第3世代(3G)携帯電話の契約数の推移」

データ編/図表2-12.ブロードバンドサービス等の契約数の推移



(万件)

	2013年度				2014年度				2015年度		
	6月	9月	12月	3月	6月	9月	12月	3月	6月	9月	12月
CATV	604.2	604.7	606.4	622.5	622.6	623.5	630.8	643.0	661.5	665.4	671.0
DSL	515.7	492.4	470.2	447.0	423.8	407.1	392.2	375.3	357.7	343.6	331.8
FTTH	2,429.4	2,463.1	2,500.7	2,531.1	2,570.1	2,598.1	2,634.4	2,660.9	2,704.1	2,728.9	2,757.7
FWA	0.87	0.84	0.80	0.76	0.75	0.74	0.73	0.69	0.68	0.66	0.64
BWA	576.9	636.8	679.8	746.1	812.2	1,034.8	1,491.9	1,946.6	2,262.2	2,622.0	3,088.0
総数	4,127.1	4,197.8	4,257.9	4,347.5	4,429.5	4,664.2	5,150.0	5,626.5	5,986.2	6,360.6	6,849.1

(注) 1.FTTHアクセスサービスとは、光ファイバー回線でネットワークに接続するアクセスサービス(集合住宅内等において、一部に電話回線を利用するVDSL等を含む)  
 DSLアクセスサービスとは、電話回線(メタル回線)でネットワークに接続するアクセスサービス(ADSL等)  
 CATVアクセスサービスとは、固定された利用者端末を無線でネットワークに接続するアクセスサービス  
 FWAアクセスサービスとは、固定された利用者端末を無線でネットワークに接続するアクセスサービス  
 BWAアクセスサービスとは、2.5GHz帯を使用する広帯域移動無線アクセスシステム(WIMAX)でネットワークに接続するアクセスサービス  
 2.四捨五入しているため、内訳と総数が一致しない場合がある。

<資料>総務省 総合通信基盤局 「ブロードバンドサービス等の契約数の推移」

## 8

## 情報化に関する動向(2015年10月～2016年3月)

国内	海外
<b>2015年10月</b>	
<ul style="list-style-type: none"> <li>・セーフティーインターネット協会、2013年11月から2015年7月の間に4,254件の違法・有害サイトから、国内サイト約8割、国外サイト約7割の情報が要請を受けて削除されたと発表。</li> <li>・トレンドマイクロ、約3,000の国内正規サイト上に日本のユーザーを対象とした不正広告攻撃があったと発表。約50万人のユーザーを攻撃サイトに誘導。</li> <li>・ビデオリサーチインタラクティブ、初のオンライン「国勢調査」のアクセス状況を発表。9月1～20日間の接触者数は1,221.3万人。同期間ではヤフー、グーグルに次ぐ接触者率に。</li> <li>・厚生労働省改革推進本部、日本年金機構のサイバー攻撃被害を受け、セキュリティ強化に向け初会合。</li> <li>・マイナンバー法施行。社会保障・税の実務効率化をめざす。</li> <li>・7月に改正された不正競争防止法の一部を改正する法律の施行期日を2016年1月1日とする政令が閣議決定。</li> <li>・成田空港、ホームページが一時閲覧できず。</li> <li>・情報処理推進機構(IPA)、重要インフラ機器メーカーを中心とするサイバー情報共有イニシアティブ(J-CSIP)発足。</li> <li>・政府、あらゆるモノをインターネットでつなげる社会の実現に向け、産官学による「IoT推進コンソーシアム」設立。併せてIoT利用促進のための「IoT推進ラボ」と技術的課題に取り組む「IoT推進フォーラム」を発足。</li> <li>・情報通信研究機構、話しかけるだけで10以上の言語に翻訳可能なソフトウェア「VoiceTra」を開発。</li> <li>・富士通研究所他、手のひら静脈などの生体情報を安全に暗号鍵にする技術を開発。</li> <li>・ディー・ディー・エス、世界初、ウェアラブル型指紋認証機器「magatama」発表。Webにかざすだけで本人認証が可能に。</li> </ul>	<ul style="list-style-type: none"> <li>・GoogleとMicrosoft、米独で争っていた約20件の特許侵害訴訟を取り下げ、和解に同意。</li> <li>・米携帯電話会社T-Mobile US、信用調査業務委託先へのハッカー攻撃で、全顧客の約1/4にあたる1,500万人分の情報流出。</li> <li>・ロシア連邦独占禁止局、Googleが端末メーカーに自社製アプリをプリインストールさせていると判断し、独占禁止法違反に対する是正命令。</li> <li>・OECD、多国籍企業の行き過ぎた節税防止のため、2013年に公表された「税源浸食と利益移転(BEPS)」行動計画を受けた最終報告書を公表。</li> <li>・欧州連合(EU)司法裁判所、元CIA職員による米政府の情報収集問題を受け、2000年に取り決めたEU-米間の個人情報移転に関する「セーフハーバールール」を無効と判断。</li> <li>・米連邦航空局(FAA)、顧客向けにドローン空撮を無許可で27年間にわたり行ってきた不動産業者に対し、運行規則違反として約190万ドルの罰金を請求。</li> <li>・Yahoo!、検索エンジンにMicrosoftの技術採用契約を更新しつつ、Googleの検索エンジンも併用開始。</li> <li>・韓国Kakao、検察当局からの通信秘密保護法に基づく傍受令状による提出要請を受け、1年ぶりに通信記録の提供を再開。</li> <li>・英通信会社TalkTalk、サイバー攻撃被害により顧客約400万人のクレジットカード情報等流出の恐れ。金銭要求も。</li> <li>・欧州議会、EUが可決したEU加盟国でのローミング撤廃と「ネット中立性」に関する法案を承認。</li> <li>・米上院、サイバーセキュリティ法案(CISA)可決。米政府と企業間でサイバー攻撃の証拠情報が共有可能となる一方で、企業に対する市民のプライバシー侵害訴えが不可能に。</li> </ul>

国内	海外
<b>2015年11月</b>	
<ul style="list-style-type: none"> <li>・東京地検、マイナンバー制度関連事業発注に係る収賄容疑で厚生労働省幹部を起訴。</li> <li>・東京消防庁、23区内の119番通報がシステム障害で6分間不通に。過去にも同様の障害発生。</li> <li>・ソニー、ベータマックス方式のビデオカセットを2016年3月で出荷終了と発表。40年の歴史に幕。</li> <li>・マカフィー、2015年の情報セキュリティ事件の認知度ランキング発表。1位は日本年金機構情報流出事件。</li> <li>・文化審議会、著作権侵害の非親告罪の適用は海賊版のみ。オリジナル作品から派生した二次創作を対象外に。</li> <li>・国土交通省、9月の改正航空法を受け、ドローンの飛行範囲を規制。人や建物との距離を30m以上に設定。</li> <li>・特許庁、世界最大規模の無料商標DB「TMView」で日本の商標出願、登録情報提供を開始。</li> <li>・シマンテック、世界17カ国実施のインターネット犯罪調査結果発表。日本は過去1年間の犯罪被害率が最低、最高はインド。</li> <li>・プロキシサーバ運営業者による不正アクセス事件で、押収サーバから約12万4,000人分のクレジットカード情報発見。</li> <li>・東京地裁、過去の犯罪履歴の検索結果削除を求める仮処分申請を受け、Googleに削除命令を決定。Googleは「知る権利」を盾に争う見込み。</li> <li>・日本図書館協会、作家村上春樹氏が学生時代に借りた本の書名と図書カードを新聞社が承諾なく報道したことを「プライバシーの侵害」と見解。</li> </ul>	<ul style="list-style-type: none"> <li>・英政府、警察と諜報機関の情報収集活動に対する監視強化のため、インターネット関連企業ユーザーのWeb閲覧データの1年間保存を義務づける監視法「Investigatory Powers Bill」草案を公示。</li> <li>・スイスProton Technologies、暗号化電子メールサービス「ProtonMail」へのDDos攻撃犯に身代金15ビットコイン(6,000ドル)支払うも、攻撃止まらず。</li> <li>・フィラデルフィア控訴裁判所、GoogleがユーザーのCookieブロック設定を迂回して追跡可能にしたことが盗聴とコンピュータ不正行為に関する連邦法違反に当たる、とする集団訴訟を却下。</li> <li>・Microsoft、インターネット普及促進のため新基金設立。ネット接続環境不備地域向けソリューション開発企業を支援。</li> <li>・オックスフォード辞典、「今年の言葉」はうれし泣き顔の絵文字。絵文字採用は初めて。</li> <li>・インドの業界団体IAMA調査、インドのインターネットユーザー数が12月には4億200万人に達する見込み。アメリカを抜いて第2位に。1位は中国。</li> <li>・米国情報技術工業協議会、米法執行当局による携帯電話の通信内容の暗号化技術を迂回する「バックドア」へのアクセスを拒否。</li> <li>・Google、欧州での「忘れられる権利」削除要請を受け、全体の42%、約44万リンクを削除。</li> <li>・北朝鮮、インターネット通信局着工。</li> <li>・ASEAN加盟国、第10回ASEAN情報通信大臣級会合をベトナムで開催。日本はサイバー分野での人材育成協力強化を提案。</li> </ul>

国 内	海 外
<b>2015年12月</b>	
<ul style="list-style-type: none"> <li>・内閣サイバーセキュリティセンター、重要インフラ13分野を対象に、IT障害対応のための分野横断的演習を実施。</li> <li>・産業技術総合研究所、ICチップの偽造防止「ICの指紋」作製技術を開発。</li> <li>・札幌地裁、過去の逮捕歴がわかる検索結果削除を求めた仮処分申請を受け、グーグルに削除命令。</li> <li>・政府、「小型無人機に係る環境整備に向けた官民協議会」設立。ドローンの安全確保、利用促進、技術開発等の課題解決へ。</li> <li>・政府、ゲノム(全遺伝情報)を「個人情報」、ゲノムデータを「個人識別符号」とする方針を決定。2016年の政令で明確化。</li> <li>・堺市、有権者約68万人分の個人情報流出。職員が無断に持ち出し、レンタルサーバに保存、閲覧可能状態に。</li> <li>・東京地裁、名前検索で犯罪履歴があるような結果が表示されるとして、人格権侵害により検索結果削除を求めた仮処分申請を受け、ヤフーの一部削除命令。ヤフーに対する削除決定は国内初。</li> <li>・経済産業省、IPAと共同で「サイバーセキュリティ経営ガイドライン」策定。経営者の指揮下でのサイバーセキュリティ対策の推進を目指す。</li> <li>・健康保険証番号を含む全国約10万3,000人分のリスト流出。名簿業者による転売が発覚。</li> </ul>	<ul style="list-style-type: none"> <li>・香港玩具メーカーVtech、ハッキングにより20万人超の子供の個人データ流出。</li> <li>・Google、電子フロンティア財団からの「Google Chrome」の機能を使って学生の閲覧データ等を収集・分析・利用し、学生のプライバシーを侵害している、との非難を否定。</li> <li>・中国の米国に対するサイバー攻撃問題を受け、初の米中間僚級協議開催。サイバー犯罪指針作成へ。</li> <li>・EU議会と加盟国、EU域内初のサイバーセキュリティ法で合意。Google、Amazonなどネット関連企業がセキュリティ上深刻な事態が発生した場合に当局への報告を義務づけ。</li> <li>・Samsung、スマホやタブレット端末の知的財産権侵害訴訟で、Appleに約5億4,800万ドルの賠償金支払い。</li> <li>・IDC調査、世界ウェアラブル市場、第3四半期出荷台数が前年同期から197.6%増の2,100万台に。</li> <li>・Google、NASAと共同導入の量子コンピュータ「D-Wave 2X」の問題解析速度がシングルコアコンピュータの1億倍以上だったことを実証。</li> <li>・FAA、ホビー用ドローンの登録を義務づけ。商用目的でのドローン利用はFAAの特別な許可が必要に。</li> <li>・Samsung、Appleに対する知的財産権侵害訴訟で合意した損害賠償額の引下げを米最高裁判所に上訴。</li> <li>・欧州委員会、EU全加盟国に適用されるデジタルプライバシー関連法を承認。「忘れられる権利」を明確化。</li> </ul>

国 内	海 外
<b>2016年1月</b>	
<ul style="list-style-type: none"> <li>・マイナンバー法改正を受け、特定個人情報保護委員会が個人情報保護委員会に改組。これまで各主務大臣が行っていた勧告・命令等の権限が委員会に一元化。</li> <li>・個人情報保護委員会、「特定個人情報の適正な取扱いに関するガイドライン」改正。</li> <li>・朝日新聞調査、大学26校で設置のインターネット接続可能な複合機、プリンタの内部データが閲覧可能な状態に。ほとんどの大学でパスワード設定なし。</li> <li>・北海道大学、学内サーバの不正アクセス被害により、大学関係者11万人の個人情報流出の可能性。</li> <li>・情報通信研究機構、ビッグデータを暗号化したまま複数のグループに分類できる解析技術を開発。</li> <li>・東京都と警視庁、中小企業のサイバーセキュリティ対策支援のため、東京商工会議所等中小企業支援機関と協定締結。</li> <li>・IDC Japan調査、2015年の国内情報セキュリティ市場規模は、前年比4.9%増の2,699億円。2019年は15年比19%増、3,217億円と予測。</li> <li>・神奈川県警、岐阜県職員を県個人情報保護条例違反および不正アクセス禁止法違反容疑で逮捕。業務で管理していた県民の情報を不正に持ち出した疑い。</li> <li>・経済産業省、「APEC越境プライバシールールシステム」における国内初の認定団体として、JIPDECが認定されたと公表。</li> <li>・東京電力、81万世帯の顧客情報入りUSBメモリを紛失。</li> </ul>	<ul style="list-style-type: none"> <li>・米Time Warner Cable、加入者約32万人のメールアドレス、パスワードが流出の可能性。</li> <li>・米政府、Apple、GoogleらIT企業にテロ捜査に向け暗号通信解読協力を要請。プログラムの抜け穴「バックドア」使用を反対するAppleは協力拒否の姿勢。</li> <li>・欧州刑事警察機構、世界各国でDDos攻撃を繰り返し、身代金を要求・詐取していた犯罪組織「FF4BC」を逮捕。日本でもセブン銀行などが攻撃被害に。</li> <li>・IDC調査、PC世界出荷台数が前年比10.4%減、7,190万台と過去最大の落込み幅に。Appleの販売数は上向き。</li> <li>・米運輸省、トヨタ自動車など18メーカーと自動車の安全性向上をめざし協力体制。</li> <li>・米HYATT、決済処理システムへのサイバー攻撃により、世界54カ国、250店舗のクレジットカード情報漏えいの可能性。</li> <li>・パキスタン政府、宗教を冒涇するコンテンツの公開をきっかけに遮断が続いた「You Tube」へのアクセスを3年ぶりに承認。</li> <li>・Google、2015年に摘発した悪質広告7億8,000万件と、モバイルアプリに表示されるポリシー違反広告25,000件を遮断。</li> <li>・IDC調査、2015年の世界のスマホ出荷台数が前年比10.1%増の14億3,290万台に。Samsung、Appleに続き、中国Huaweiが3位に。</li> </ul>

国内	海外
<b>2016年2月</b>	
<ul style="list-style-type: none"> <li>・ラック、国内初のDNS通信を使った遠隔操作マルウェアを観測。ウイルス対策ソフトでの検知が難しく、深刻な脅威に位置づけ。</li> <li>・ヤフー、FX子会社の顧客情報約18万件がネット上で閲覧可能状態に。元従業員が持ち出し、ネット上に保存。うち12万件は個人情報含まれず。</li> <li>・政府、サイバーセキュリティ基本法を閣議決定。衆議院に提出。</li> <li>・日・米・カナダ他、環太平洋パートナーシップ(TPP)交渉参加12カ国、TPP協定に署名。ビジネス遂行のための越境データ移転が認められることに。</li> <li>・国土交通省、東京駅周辺でGPS電波が届かない地下、屋内での道案内アプリを使った実証実験開始。情報バリアフリーの具現化が目的。</li> <li>・経済産業省、IoT活用に向けた新事業選考会(IoT Lab Selection)で、16事業への出資決定。第1回グランプリはLiquidの「訪日観光客の滞在快適性向上おもてなしプロジェクト」。</li> <li>・経済産業省、企業の秘密情報漏えいを未然に防ぐための「秘密情報の保護ハンドブック」を初めて作成・公表。</li> <li>・総務省、マイナンバーカード活用の公的個人認証サービス利用の民間事業者3団体に対し、初の大規模認定。</li> <li>・陸上自衛隊のイラン派遣反対を訴える個人の個人情報収集に対するプライバシー侵害判決に対し、国は上告しない方針。</li> <li>・政府、2020年の東京五輪に向け、サイバー攻撃対策の一環として「オリンピック・パラリンピックCSIRT」創設。</li> <li>・金融庁、国内初の仮想通貨法規制案で仮想通貨に財産価値を定義づけ、貨幣と認定。決済や法定通貨との交換が可能に。</li> <li>・シャープ、鴻海精密工業の傘下で経営再建を目指すことを決定。4月に正式契約締結。</li> <li>・さいたま地裁、過去の逮捕事件の記事の削除要請の仮処分申請に対し「忘れられる権利」があると判断し、グーグルに削除命令。グーグルは決定取消しを求め異議申立て。</li> </ul>	<ul style="list-style-type: none"> <li>・中国最大P2P金融会社e租宝、投資詐欺により関係者21名逮捕。投資家90万人の被害総額は500億元(76億ドル)以上。被害額・規模ともに中国史上最大。</li> <li>・オバマ大統領、すべての子供たちにコンピュータ科学を学ばせる支援策「Computer Science for All」発表。3年間で40億ドルを拠出。</li> <li>・EU、米国企業のEU域内から米国への個人情報移転を認める新協定「プライバシーシールド」で米国と基本合意。前年10月に無効となった「セーフハーバー協定」の後継制度。</li> <li>・Apple、米特許保有会社VernetXの特許侵害で6億2,560万ドルの支払いを命じる陪審評決。Appleは控訴の方針。</li> <li>・Twitter、イスラム過激派組織ISIS等、テロ行為を助長する累計12万5,000件以上のアカウントを凍結。</li> <li>・米政府、サイバーセキュリティ対策のための「Cybersecurity National Action Plan(CNAP)」発表。2017年度に190億ドルの予算確保。</li> <li>・米運輸省道路交通安全局、Googleの自動自動車に搭載される人工知能を連邦法上「運転手」とみなす方針。</li> <li>・米連邦捜査局(FBI)、銃乱射犯所有のiPhoneの情報入手のため、Appleにセキュリティ機能解除やバックドア設定を要求。Appleは政府命令を拒否。</li> <li>・米Hollywood Presbyterian Medical Center、ランサムウェア感染により病院システムがダウン。身代金17,000ドルを支払い、復号鍵を入手。</li> <li>・米連邦巡回控訴裁判所、Samsungに対しAppleへの1億2,000万ドル支払いを命じた連邦地裁の評決を無効に。Appleに対するSamsungへの15万8,400万ドルの賠償支払い命令は支持。</li> <li>・米内国歳入庁、2015年5月に発生した納税者アカウントへの不正アクセス事件で、新たに39万人のアカウントが被害に遭っていたと発表。被害者数は72万人超。</li> <li>・Googleの自動運転車、走行試験中にバスと初の衝突事故。</li> </ul>

国内	海外
<b>2016年3月</b>	
<ul style="list-style-type: none"> <li>・経済産業省、セキュリティマネジメント国際規格ISO27001、27002改正を受け、情報セキュリティ管理基準を8年ぶりに改正。</li> <li>・大阪高裁、大阪地裁が違法性を指摘した令状なしのGPS捜査に対し、「重大な違法なし」と判断。</li> <li>・警察庁調査、2015年インターネットバンキング不正送金事件の被害額は前年比5.6%増の30億7,300万円。3年連続過去最悪を更新。</li> <li>・江崎グリコ、不正アクセスによりネット通販利用者の個人情報約83,000件流出の可能性。</li> <li>・総務省、自治体の情報セキュリティ強化対策に補助金約236億円交付を決定。自治体情報セキュリティクラウド構築に活用。</li> <li>・ドローン飛行規制強化法成立。国会議事堂、皇居、原発等重要施設とその周辺の上空を飛行禁止区域に。</li> <li>・警察庁、中央省庁対抗サイバー攻撃対処競技会で優勝。標的型メール着信に対する調査・対処の速さ、関係者とのコミュニケーションの適切さを重視。</li> <li>・警視庁、2015年11月摘発のプロキシサーバ不正アクセス事件の押収サーバから約1,800万件のID、パスワード発見。うち178万件で不正アクセス成功。</li> <li>・水戸地裁、令状なしのGPS捜査を「違法」と判断。</li> <li>・消費者庁、初の名簿業者実態調査実施。述べ3億件の個人情報保有業者も。</li> <li>・東京地裁、ベネッセの顧客情報流出事件で元SEに懲役3年6カ月、罰金300万円の判決。</li> <li>・全日本空輸、3月に2度起きた国内線のシステム障害は米Cisco Systems製スイッチの故障が原因。同製品発売以降世界初のトラブル。</li> </ul>	<ul style="list-style-type: none"> <li>・ニューヨーク連邦地裁、薬物事件に関わるiPhoneのロック解除を求める米政府の請求を棄却。</li> <li>・独連邦カルテル庁、FacebookがSNS市場において支配的地位を乱用し、データ保護法違反にあたるとして捜査を開始。</li> <li>・Facebook中南米部門幹部、麻薬密売事件捜査で対話アプリのデータ開示要求を拒否し続け、罰金と拘束。翌日釈放。</li> <li>・米国防総省、ISISを標的とするサイバー攻撃を開始。</li> <li>・米国防総省、ハッカーが侵入テストを試みる「Hack the Pentagon」プロジェクト発表。バグ発見者に奨励金支払い。</li> <li>・米連邦通信委員会(FCC)、低所得者向けブロードバンド接続支援プログラムの最終提案発表。</li> <li>・FCC、インターネット上の消費者プライバシー保護に関する規則の素案を公表。</li> <li>・Googleの「AlphaGO」、世界トップのプロ棋士との5番勝負を4勝1敗で征す。</li> <li>・米行政管理予算局、2015年の政府のサイバー案件は前年度比10%増の77,000件。大規模被害は連邦人事管理局の個人情報漏えい事案。</li> <li>・仏情報処理および自由に関する全国委員会、「忘れられる権利」の検索結果削除を拒否したGoogleに対し、10万ユーロの罰金。</li> <li>・FBI、Appleの支援なしにiPhoneのロック解除成功。</li> <li>・米自由人権協会、「All Writs Act(全令状法)」に基づき、AppleのほかGoogleも犯罪捜査のためデバイスロック解除命令を受けていた、との調査結果を発表。</li> </ul>



---

JIPDEC IT-Report2016 Spring

2016年5月31日発行(通巻第7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

禁・無断転載