JIPDEC

IT-Report

2018 Spring

特集 「企業IT利活用動向調査2018」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

本誌「JIPDEC IT-Report2018 Spring」では、JIPDECが2011年から継続して行っているIT利活用にかかわる独自調査の結果をとりまとめ、ご紹介しています。

2017年５月30日に全面施行された「改正個人情報保護法」について、2016年調査以降の対応状況や自社に与える影響を調査していますが、「改正法が与える自社への影響」に関しては、「システムやプライバシーポリシーの大幅な変更・修正の必要性」「変更・修正は必要だが、範囲は限定的」とする回答が、昨年に比べそれぞれ約５ポイント減少しました。

なお、改正法への対応状況については７割以上が「すでに完了している」「2017年度中に対応完了見込み」（今年１月時点）となった一方で、２割が、「いつまでに完了できるかわからない」という結果となりました。

また、欧州連合（EU）域内に事業拠点または顧客を持つ回答者に対し、今年５月25日に施行された欧州連合（EU）の「一般データ保護規則（GDPR）」への対応についても調査していますが、「GDPRの存在を知らない」または「自社がどう対応しているかを把握していない」との回答が４割を占めていました。

このほか、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、働き方改革とクラウドの動向、情報セキュリティ製品の導入状況など、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、2017年10月から2018年３月の情報化動向をとりまとめ、紹介していますので、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-Report 2018 Spring

Contents

特 集

「企業IT利活用動向調査2018」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2016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：2018年１月17日～１月29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、業務改革系部門のいずれかに所属し、IT戦略策定または情報セキュリティ従事者で、係長相当職以上の役職者約2,000人
・有効回答数：693件（１社１人）

1-2. 回答者のプロフィール

回答者の業種で最も多かったのは製造業（28.3%）、次いでサービス業（23.1%）、情報通信（16.2%）、金融・保険、卸売・小売（8.7%）となった。所属部門では情報システム部門が最も多く（45.9%）、役職は部長（36.9%）、課長（28.4%）、係長・主任（19.6%）が回答の８割強を占めている。

IT戦略や情報セキュリティへの関与度をみると、回答者に情報システム部門所属が多いことも関係しているからか半数以上が、「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」（62.6%）、「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」（53.2%）。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

本調査では、企業における重要テーマである「情報セキュリティ」をメインテーマとしている。ここでは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みる。

2-1. 重視する経営課題

経営課題としてあげた24項目に対し、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調べた（図１）。「業務プロセスの効率化」が６年連続で首位となり、昨年同様、「従業員の働き方改革」が２位に続いた。「情報セキュリティの強化」は３位となった。

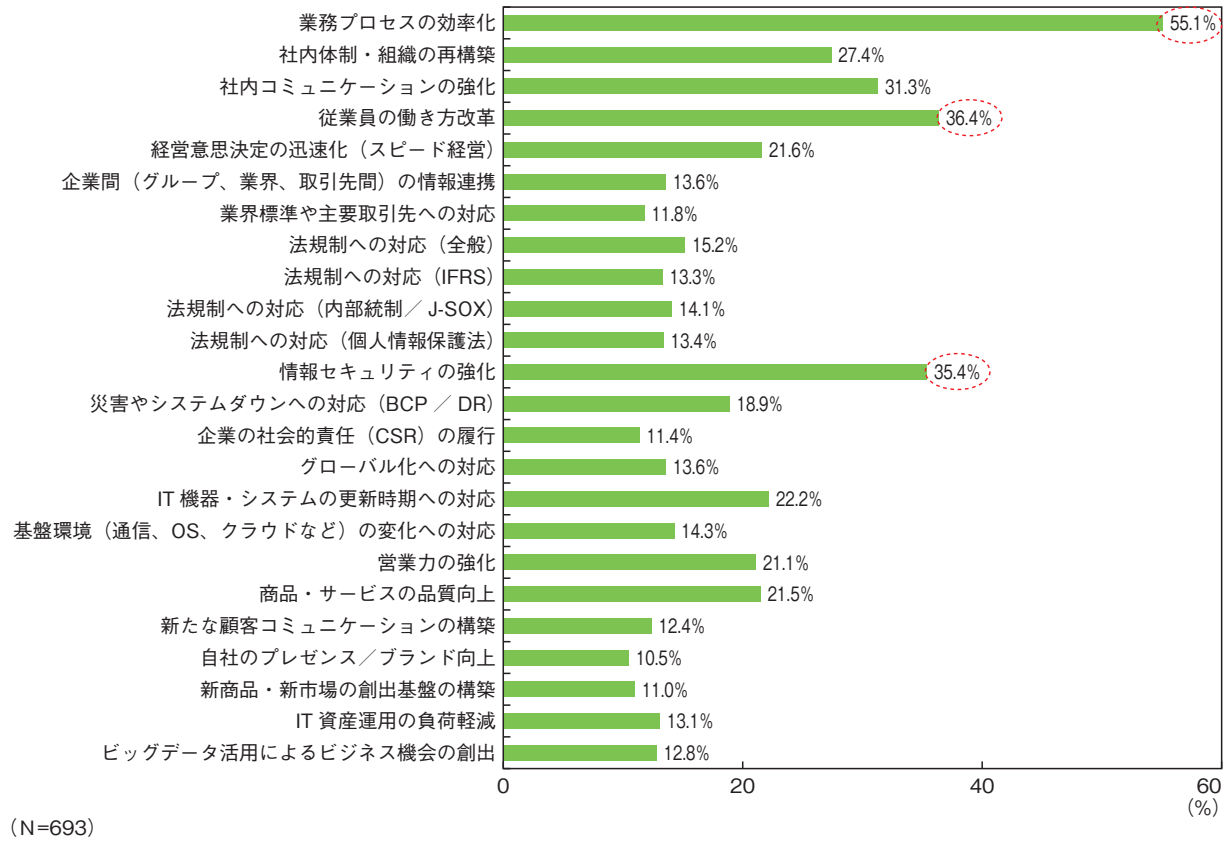


図１．今後重視したい経営課題（複数回答）

さらに、今年の調査結果の上位18項目について、過去２回の調査結果と比較すると、2016年調査から右肩上がりで上昇傾向にある項目は「システム更新への対応」「基盤環境の変化への対応」「ビッグデータ活用」であり、前年から大きく上昇した項目は「商品・サービスの品質向上」「内部統制／J-SOXへの対応」であった（図２）。

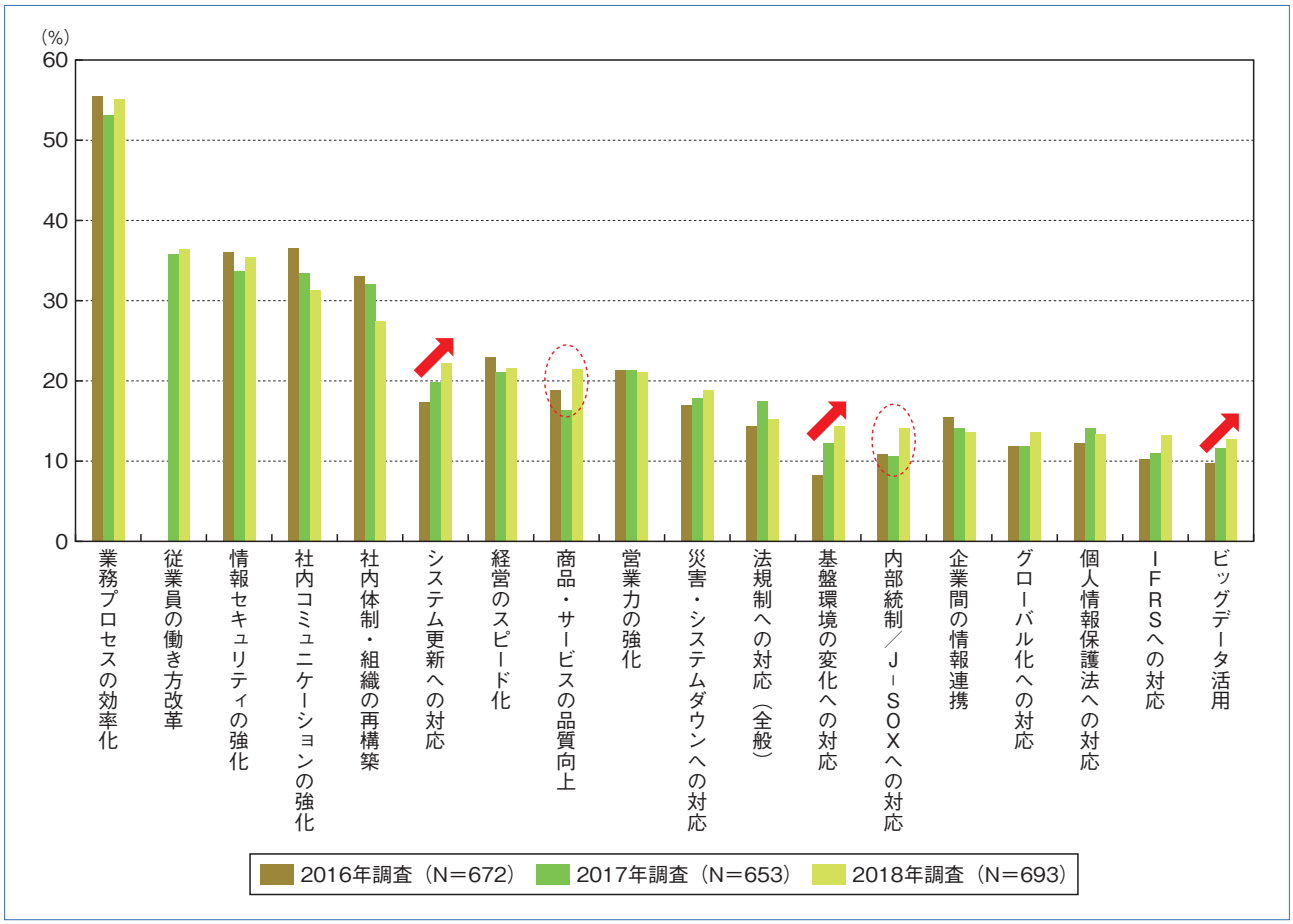


図2. 主要経営課題に対する選択率の経年変化（2016年～2018年調査）

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をみると、認知率が最も高かったのは「社内PCのマルウェア感染」であった。続いて多いのが、データや機器の紛失・盗難で、「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」が20％台となった（図３）。

「個人情報の漏えい・逸失」については、人為ミスによるインシデントの認知率が高く（17.3％）、内部不正によるものも10％を超えた。

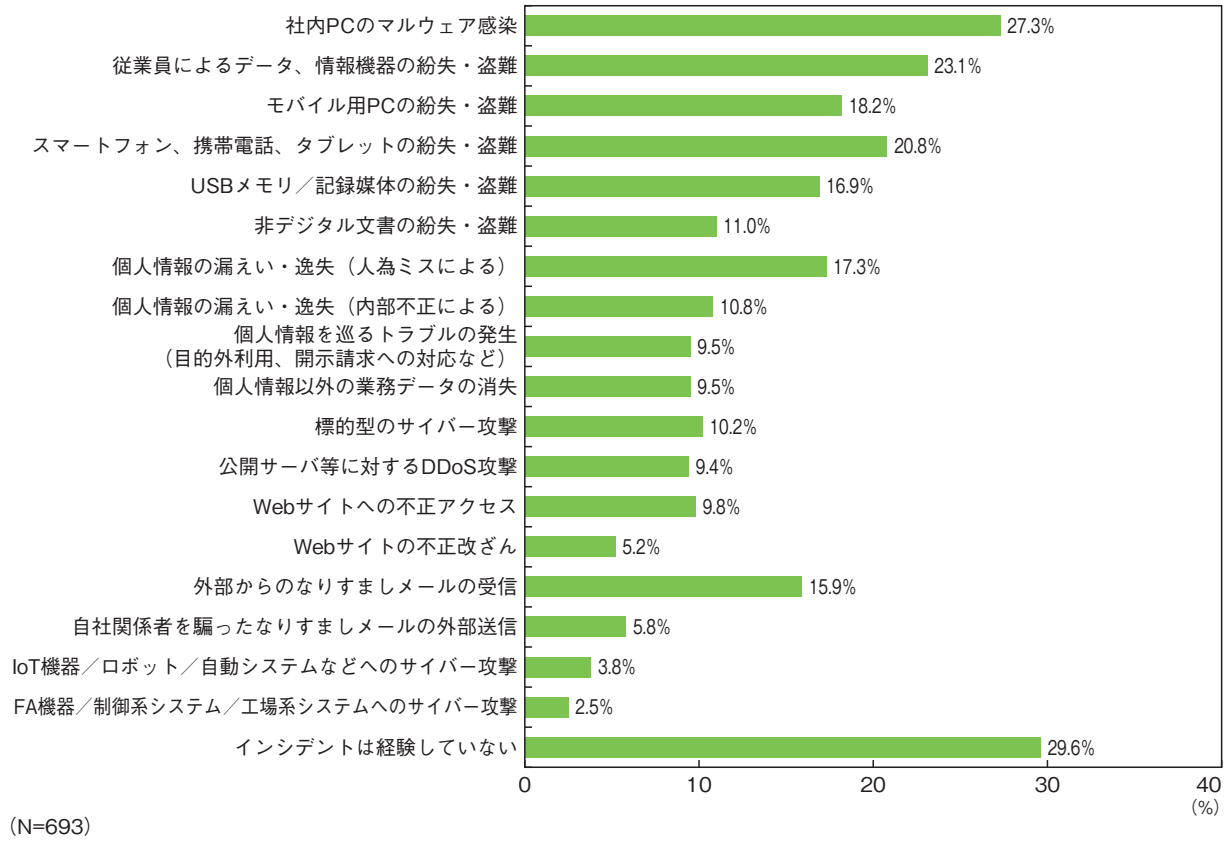


図3. 過去1年間に認知したセキュリティインシデント（複数回答）

過去の調査結果と比較すると、特徴的なインシデントの認知率が上昇傾向にある。たとえば「外部からのなりすましメールの受信」は前年調査結果から５ポイント以上と大幅に上昇した（10.7%→15.9%）。また、「公開サーバ等に対するDDoS攻撃」も３ポイント以上上昇した（5.8%→9.4%）。さらに「内部不正による個人情報の漏えい・逸失」や「個人情報を巡るトラブルの発生」など、個人情報に関わるインシデントも年々上昇している（図４）。

特に「外部からのなりすましメールの受信」と「公開サーバ等に対するDDoS攻撃」について、従業員規模別にみると、限られた一部の企業で認知されているものではなく、中堅・中小企業においても増加している点にも注目されたい（図５）。2017年から国内において金銭をだまし取るビジネスメール詐欺（BEC：Business E-mail Compromise）による被害が確認されていることから、早急な対応が求められるといえる。

また「公開サーバ等に対するDDoS攻撃」もすべての従業員規模で増加しており、２年後の2020年東京五輪に向け、今後さらに攻撃被害が増加することが予想される。

被害が増加傾向にあるなか、依然として「インシデントは経験していない」とする割合も約３割（29.6%）の回答があったことから、インシデントの検知および発見ができていない企業も多く存在している可能性があることが危惧される。企業においては、セキュリティインシデントは、もはや「起こさない」ことよりも、「起こることを前提として対策をたてる」ことが経営層の責務として求められている。

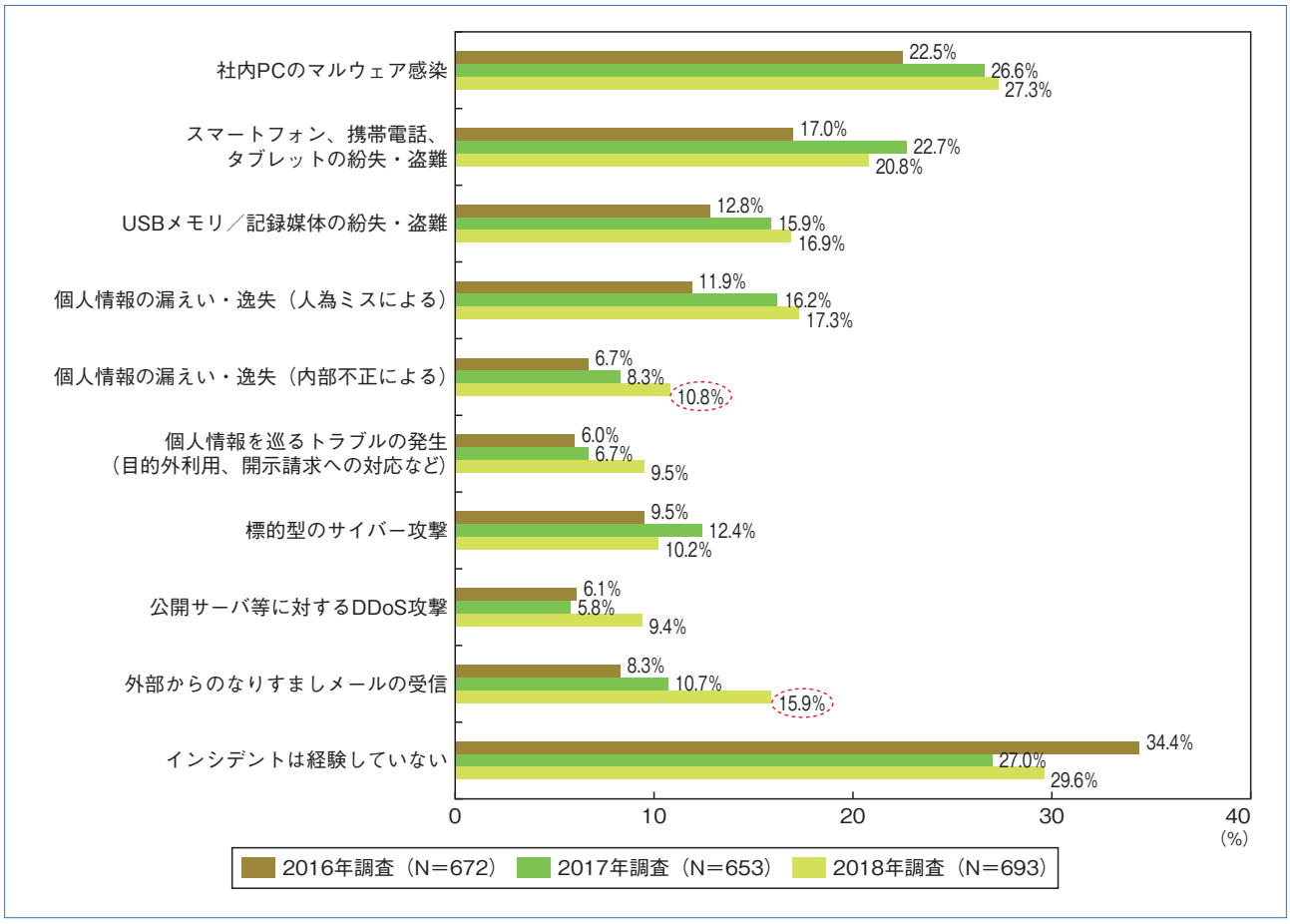
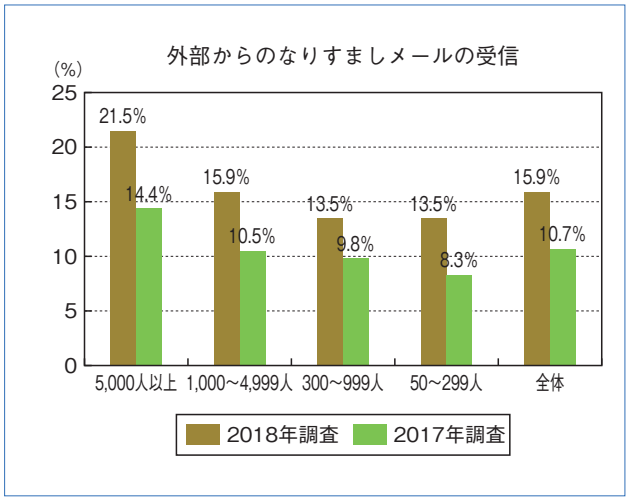


図4. 主要なセキュリティインシデント認知率の経年変化（2016年～2018年調査）



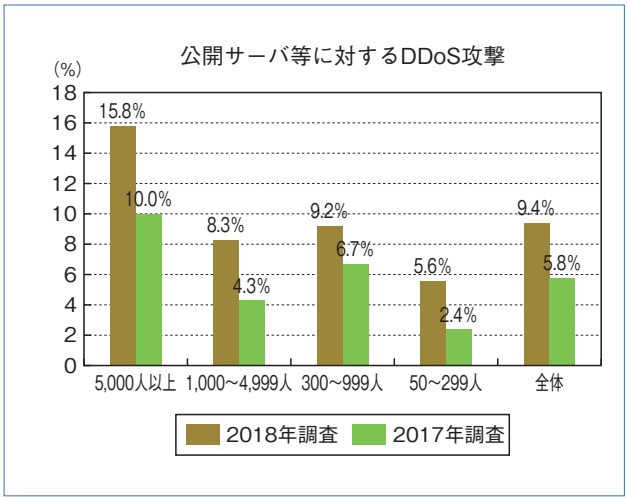


図5. セキュリティインシデントの認知状況（従業員規模別／2017年～2018年調査）

2-3.「標的型攻撃」と「内部犯行」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」のリスクに対する重視度合いをそれぞれ定点観測しているが、今回の調査ではいずれも「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、直近３回の調査の中で最多となった（図６）。特に「サイバー攻撃」に対する危機感は年々増大しており、６割以上の企業が重要課題として認識し、対応の優先度を高めている。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、サイバー攻撃をしかける側がAIを活用するなど、巧妙化が進んでいることから、サイバーインシデントの潮流を理解することは企業のリスク管理として重要である。今後は局所的なツールの導入対策（サイロ型セキュリティ対策）にとどまらず、ITインフラ全体のセキュリティレベルのベースラインを包括的に高めることに注力することが求められるであろう。

さらに昨今の社会的な情勢から、ITガバナンスや内部統制として、データ改ざん防止も含めた重要情報の保護や内部犯行による情報漏えいなどのセキュリティインシデントの防止は、企業の社会的な責務として重要なテーマとなると予測できる。

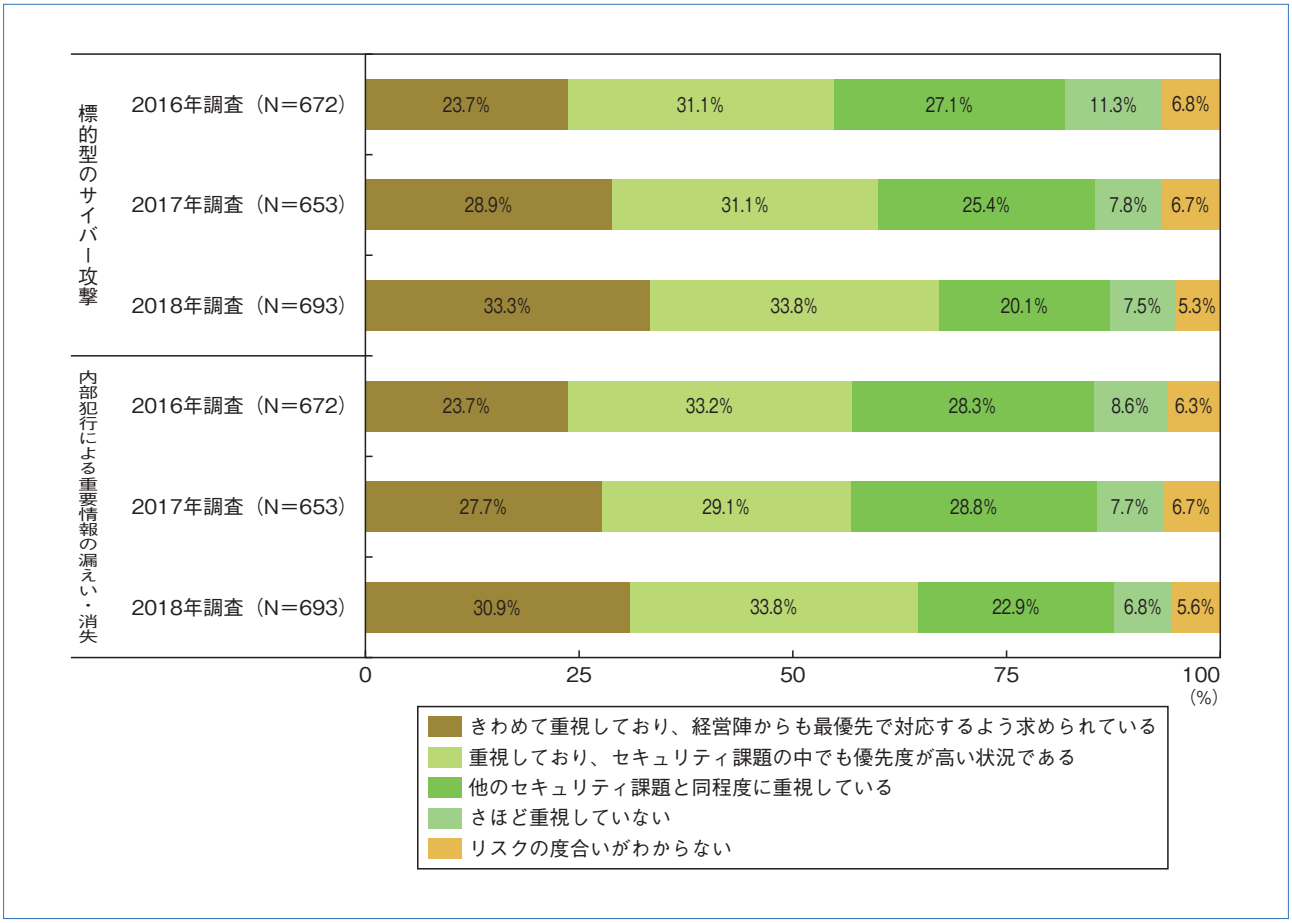


図6.「標的型のサイバー攻撃」および「内部犯行による重要情報の漏えい・消失」
リスクに対する重視度合いの経年変化（2016年～2018年調査）

2-4. セキュリティ対策の実施状況

では、具体的にどのようなセキュリティ対策が実施されているのか。この調査では、「標的型のサイバー攻撃対策」「内部犯行対策」として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観測している。

「標的型攻撃対策」として最も実施率が高いのは「重要システムのインターネットからの隔離」であった（図7）。なお、前年調査で最も実施率が高かった「メール添付ファイルのフィルタリング」は51.6%から47.0%へと減少し、今回調査では第５位となった。

また、今後の実施予定が高かったのは「標的型攻撃対策（クライアント型）／（ネットワーク型）／（アウトソースによる有人監視等）」「IoT／FA／制御システムへのセキュリティ対策」「CSIRTの立上げ」であった。

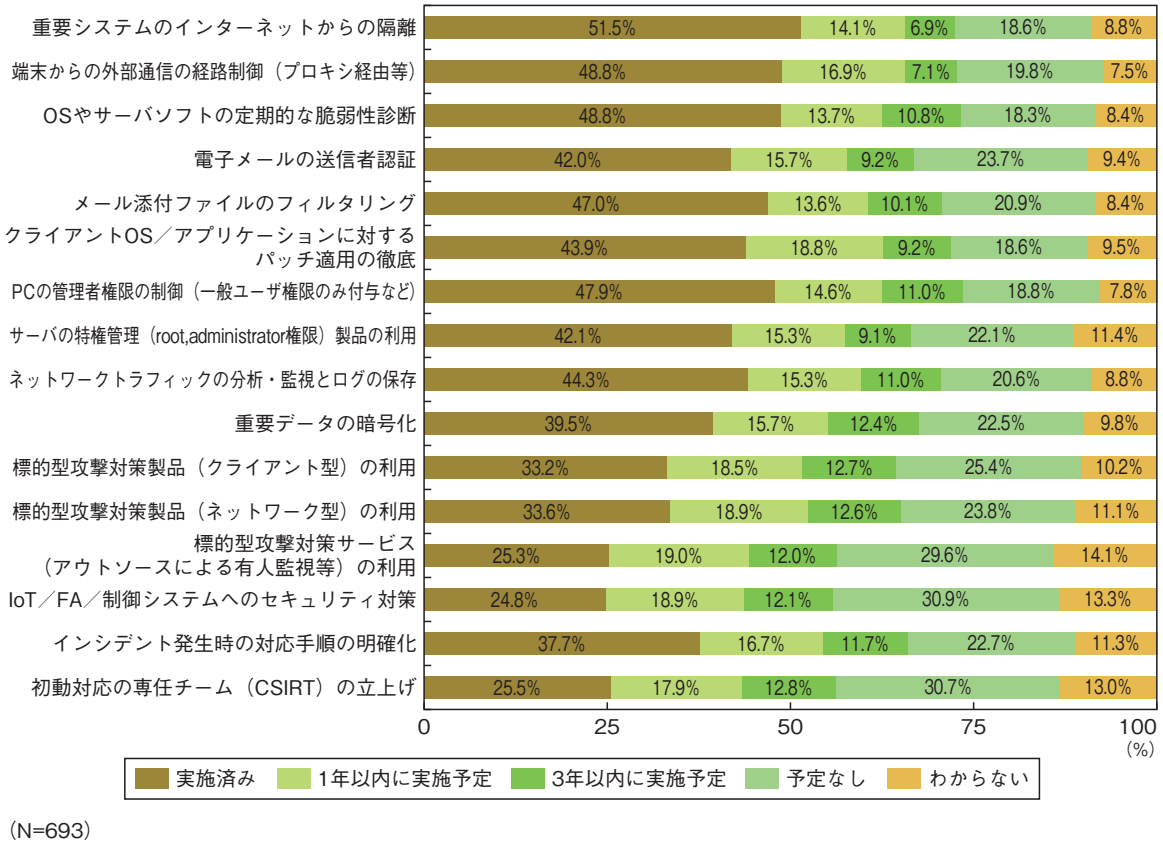


図7. 主要な「標的型サイバー攻撃対策」の実施状況

一方、「内部犯行対策」としては「重要情報にアクセスできる人員（部署）の制限」の実施率が最も高く（50.8％）、「外部デバイスへのデータ移動の制限」が次に続いている。なお、「PCの社外持出しの禁止」は、54.5％から47.0％へと大きく減少した。

また、今後実施予定が高かったのは「セキュリティ対策としてクラウドの利用」「システム管理者向けの教育・研修の実施」であった（図８）。

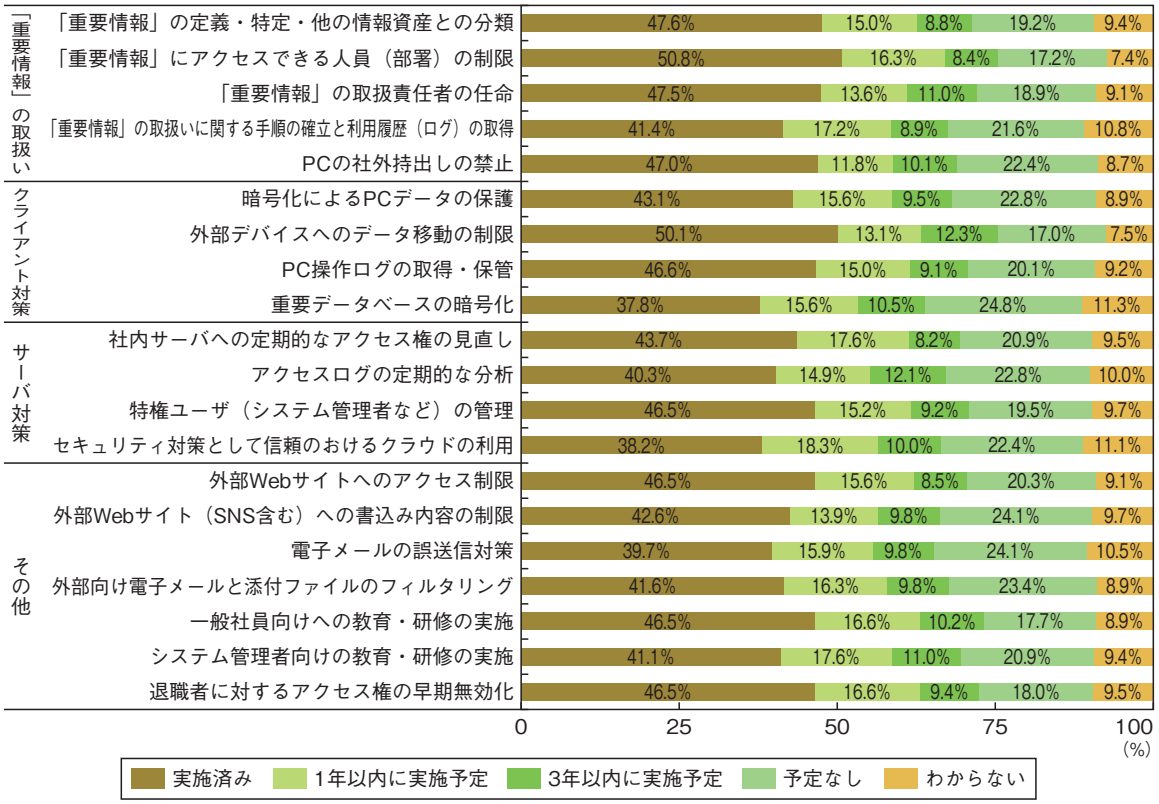


図8. 主要な「内部犯行対策」の実施状況

2-5. システムリスク軽減策への取組み状況

システムリスク軽減策への取組み状況について調査した。「BCPの策定」「全社的なリスクマネジメントシステムの構築」および「セキュリティ（プライバシー）ポリシーの策定」の実施率（実施済）が５割強となったのに対し、「ITサービスマネジメント」の実施率は低く、約４割であった（図９）。

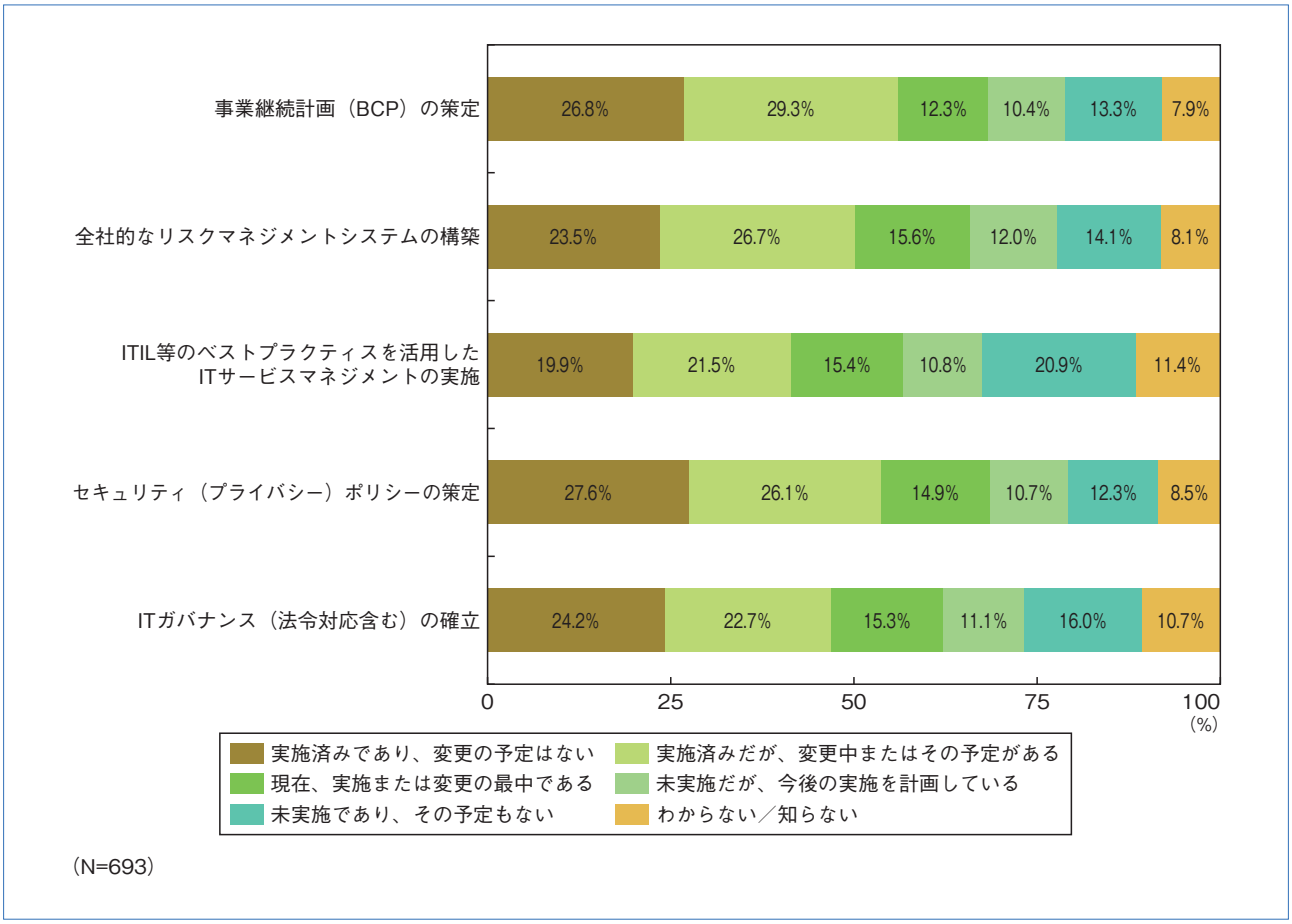


図9. システムリスクの軽減策の取組み状況

2-6. セキュリティ支出の増減傾向

主要なセキュリティ支出15項目について、2018年度の支出の増減見込み（対前年度比）を調査した（図10）。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」「セキュリティ製品の利用・購入費」「従業員研修・教育」など９項目が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。

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（モバイル対策）」が上位となっている。

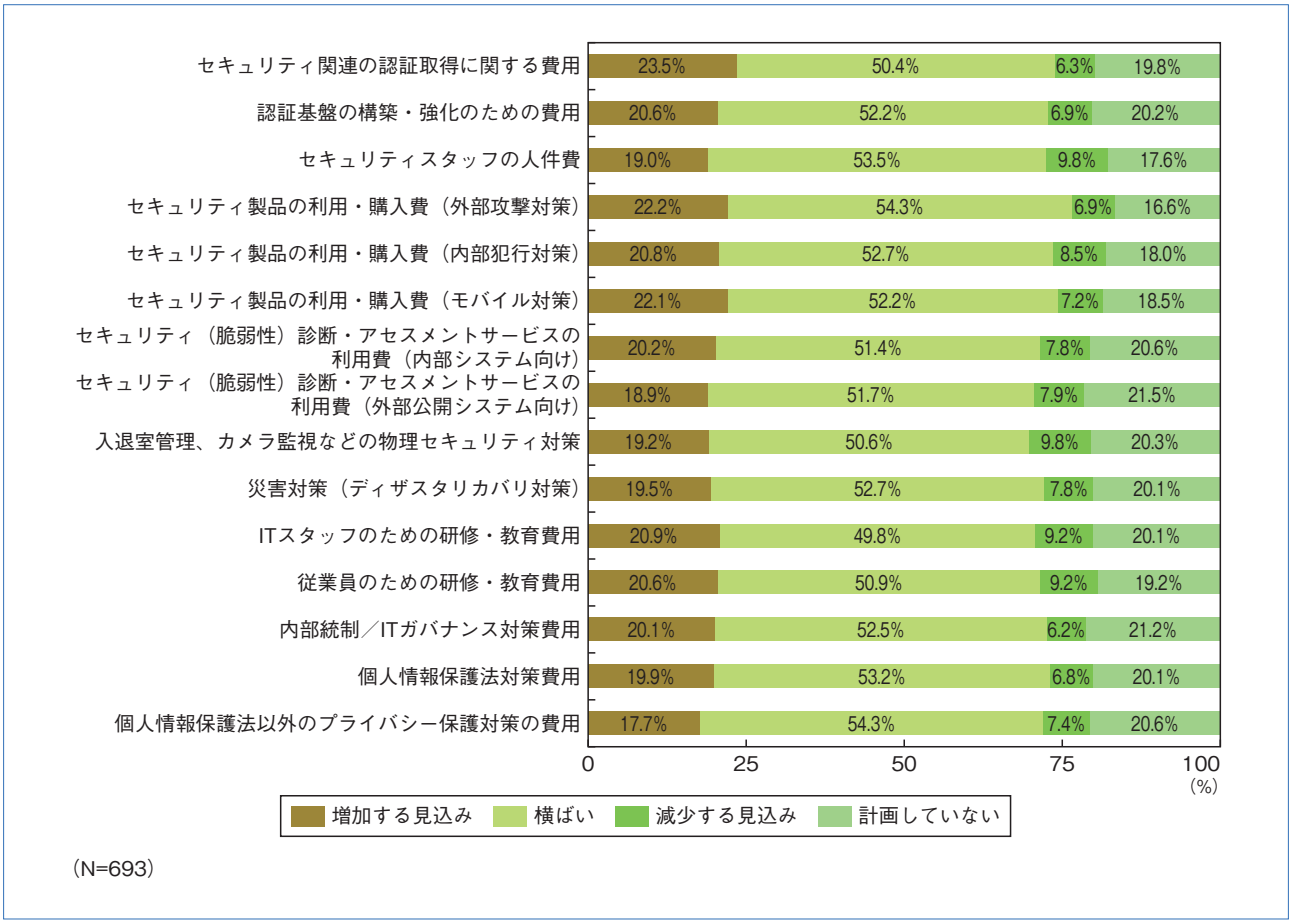


図10. 2018年度に想定されるセキュリティ支出の増減傾向

こうしたセキュリティ支出の増大傾向は大企業だけでなく、これまで比較的支出に消極的であった中堅企業にも広がっていることがわかった。特に「ITガバナンス・内部統制対策に関する費用」および「個人情報保護法対策に関する費用」は顕著であるといえる（図11、図12）。

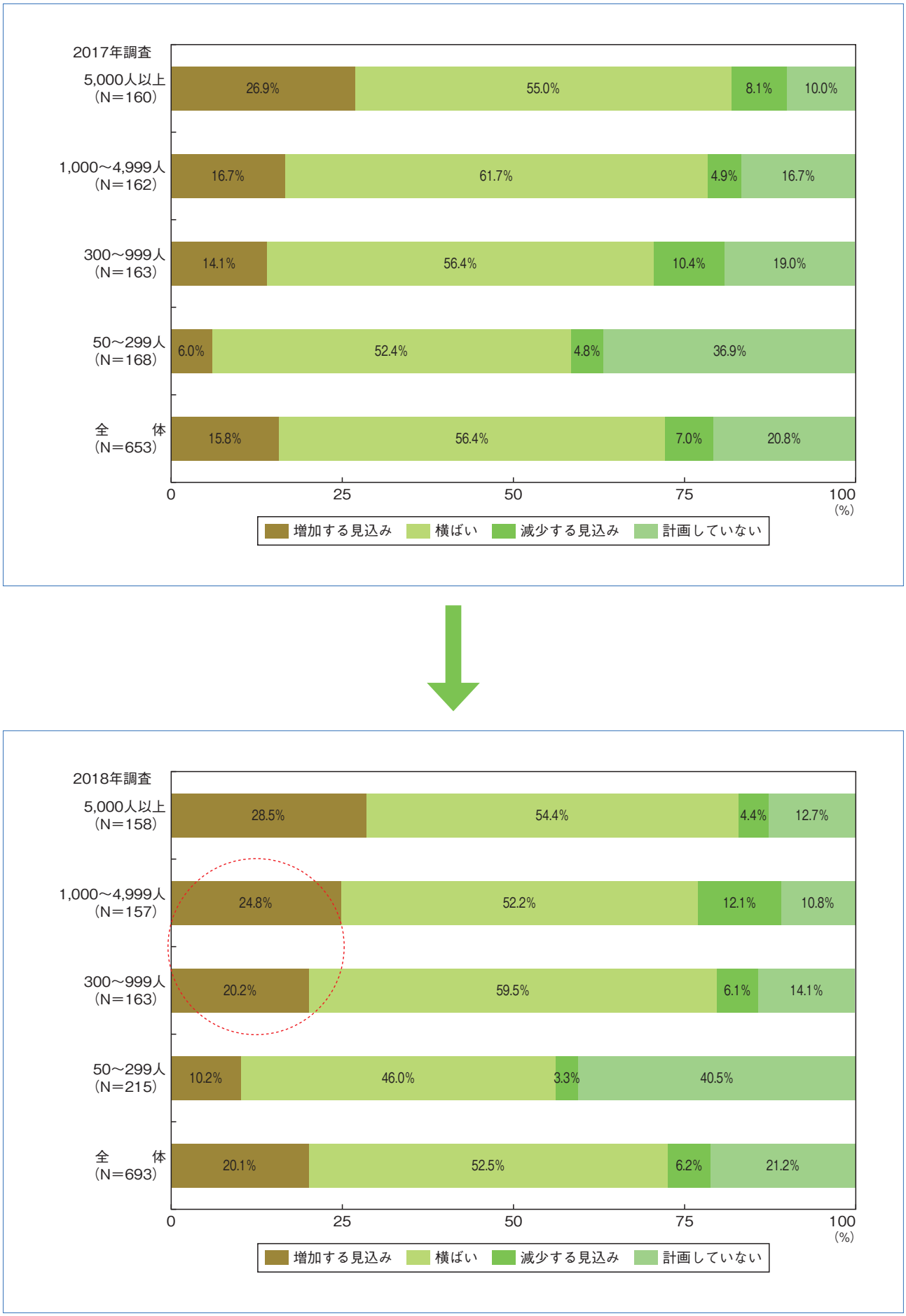


図11．ITガバナンス・内部統制対策に関する費用（従業員規模別/2017年～2018年比較）

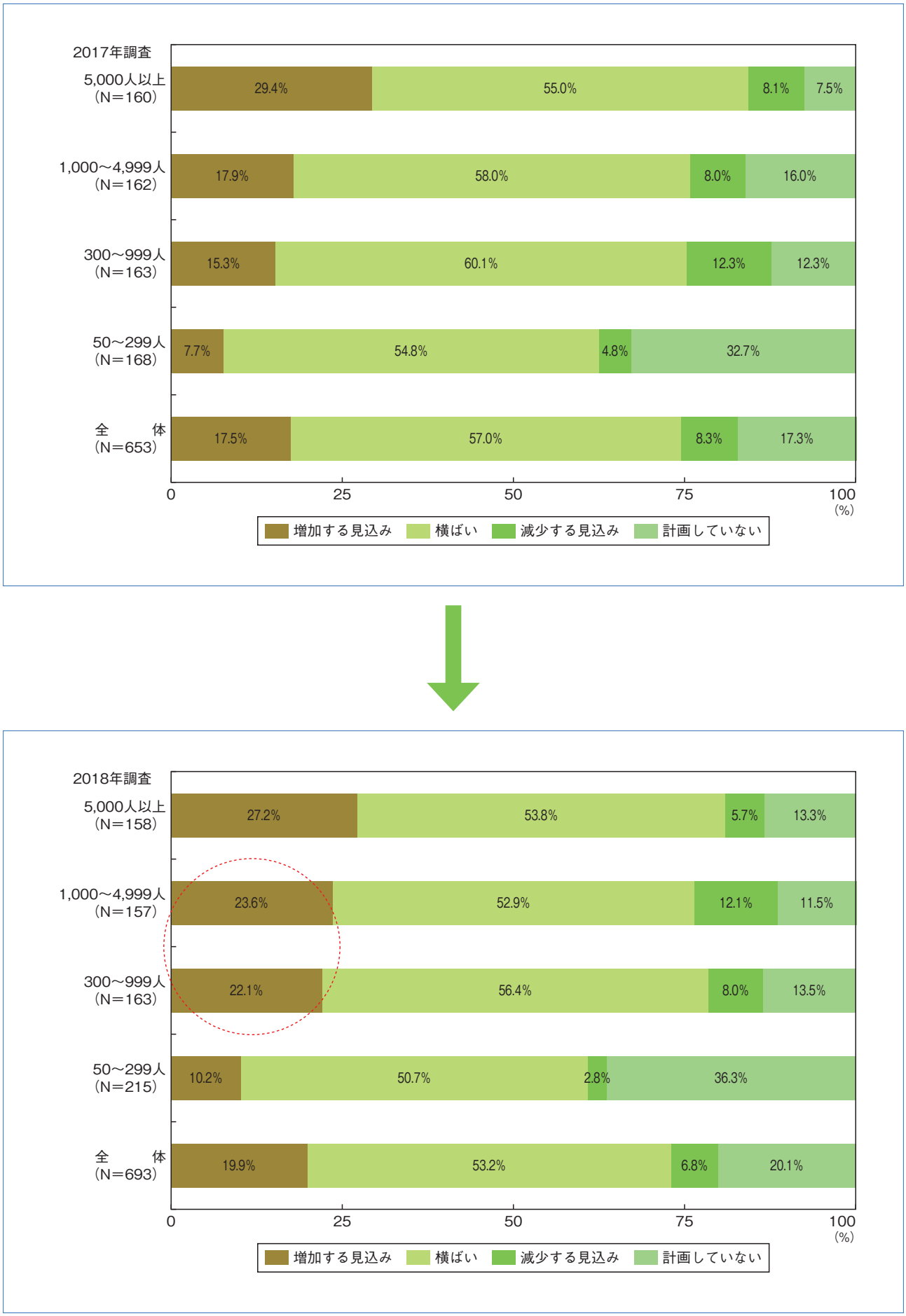


図12.　個人情報保護法対策に関する費用（従業員規模別/2017年～2018年比較）

3 情報セキュリティに関する認定／評価制度の動向

情報セキュリティに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／認証制度の重要性は広く認知されている。本調査では、主要な制度について、現在の取得状況と今後の取得意欲について定点観測している。

3-1. 情報セキュリティ関連の認証制度の取組み状況

国内において取得可能である代表的な認定／認証制度５項目について、それぞれの取得状況と今後の取得意欲について調査した。最も取得率が高かったのは「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り、依然としてこの２つの制度の認知度が高いことを物語っている（図13）。

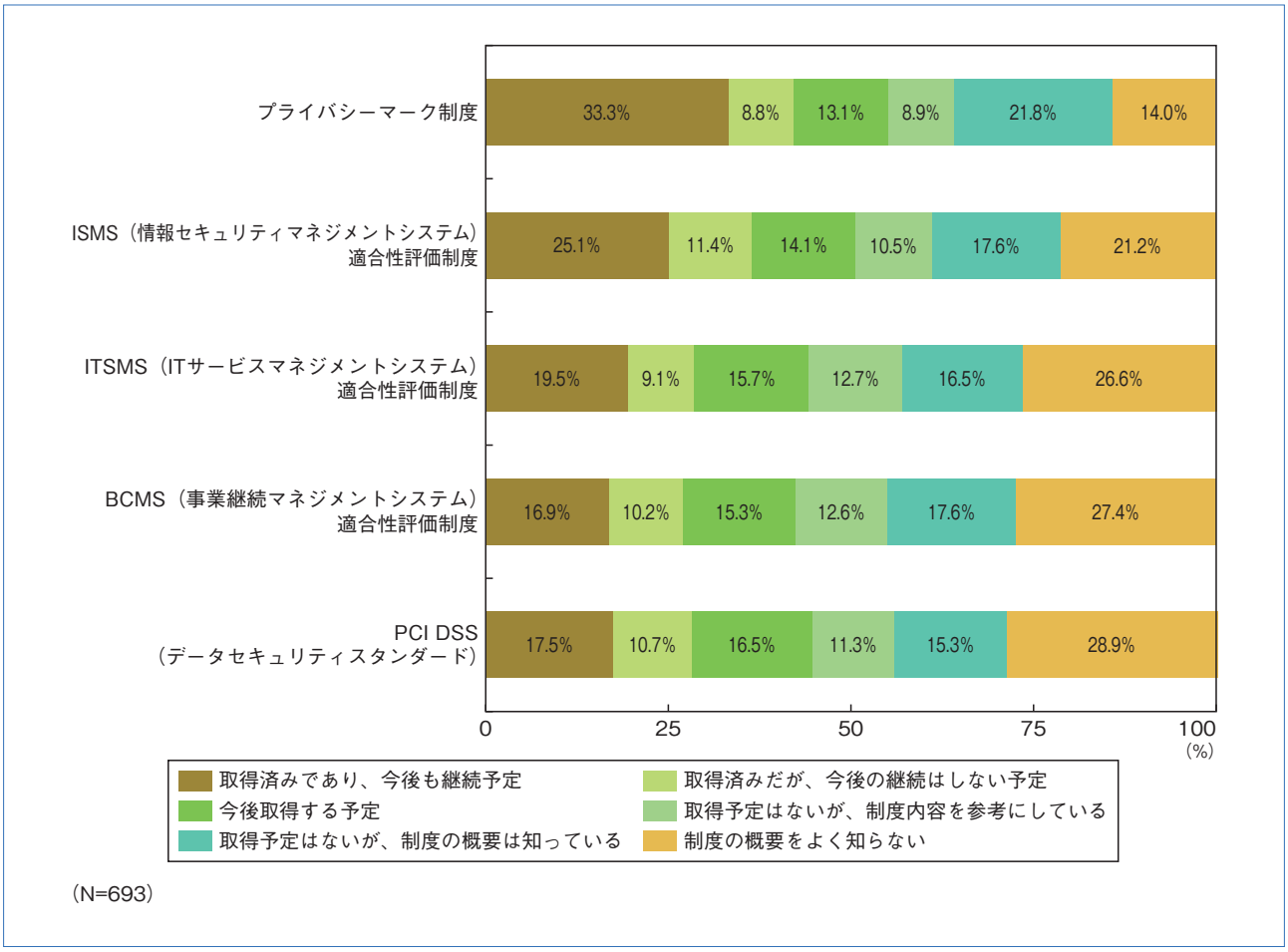


図13. 情報セキュリティに関わる認定／認証制度の取組み状況

3-2. 認定／認証を取得する価値

2-6で示したセキュリティ支出の見込みでも、認定／認証の取得にかかわる支出の増加が見込まれているが、実際、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であろうか。

今回、ISMS認証を例に第三者の認定／認証を取得することの価値について調査した。図14はISMS認証の「取得済みの企業」と「今後取得を予定している企業」「いずれにもあてはまらないその他の企業」に分けて集計した結果である。取得済みの企業の場合、「取引先からの信頼を得るため」が約76％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」「消費者からの信頼を得るため」が続いている。

それに対して、今後取得を予定している企業では、「取引先からの信頼を得るため」「社内の情報セキュリティ体制を高度化させるため」の順位は取得済み企業と同じ傾向となっているが、「取引先から求められたため」が次に続いている。契約や入札の際、第三者認証取得が条件となっている場合も多く、第三者認証取得の重要性がより増している背景があるといえる。

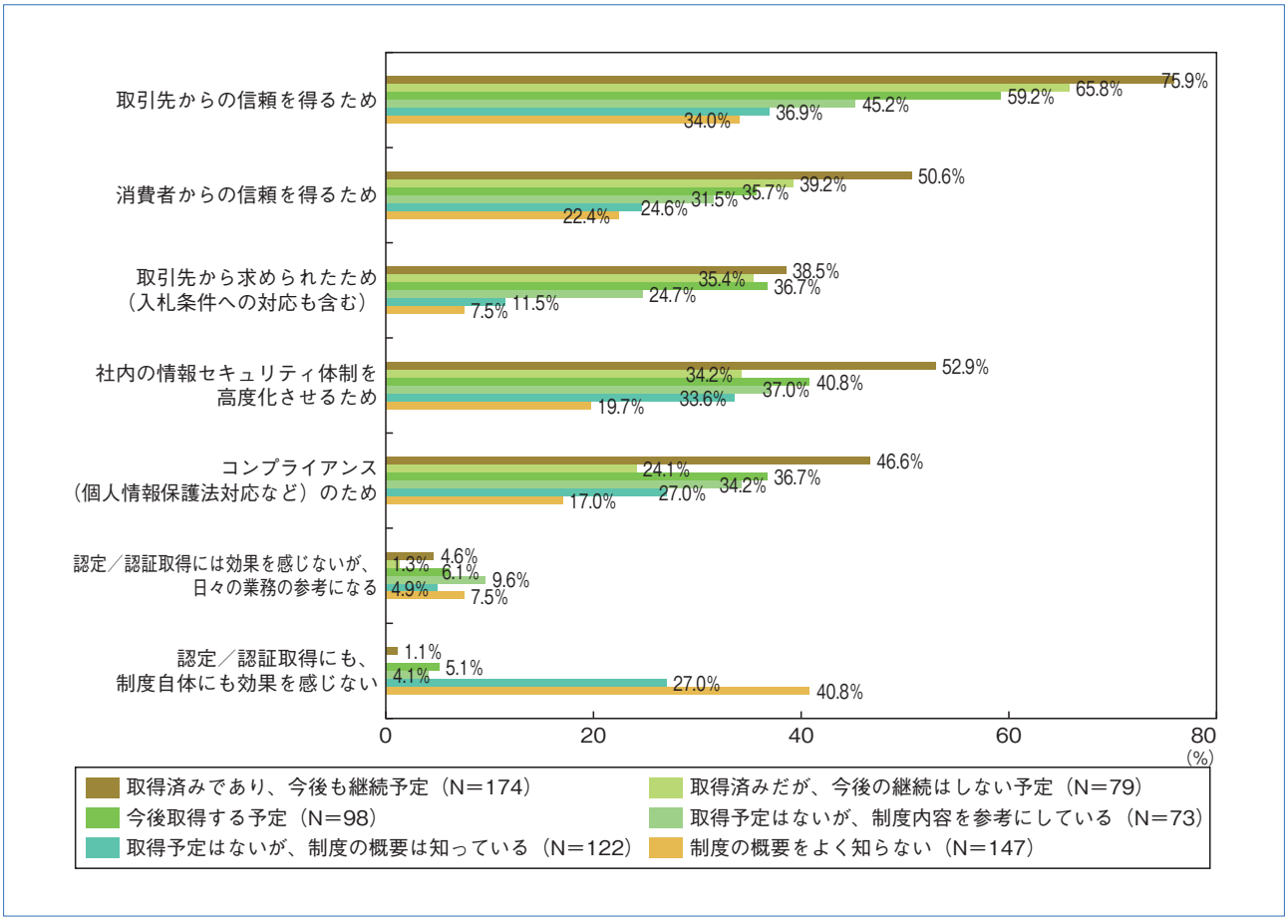


図14. 認定／認証を取得することの価値（ISMS取得状況別）

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。今回の調査では、2017年５月30日に施行された改正個人情報保護法、ならびに2018年５月25日に施行されたEUの一般データ保護規則（GDPR）への対応に焦点をあてた。

4-1. 改正個人情報保護法のインパクト

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」「システム、プライバシーポリシー両方の変更・修正が必要になったがその範囲は限定的だった」と回答した割合が前年から減少し、各企業とも改正法に対して対策のめどが立ったといえる（図15）。しかしながら、「現状の個人情報保護のあり方を変更する必要はなかった」とする回答者が増加しており、実施している対策内容について法令に正しく準拠しているかは第三者による判断が必要な可能性もある。さらに依然として「改正法の内容をよく知らないので答えられない」との回答も13%存在しており、情報システム／情報セキュリティ担当者の中にも、法改正の動向に対する関心に温度差があることがみてとれた。

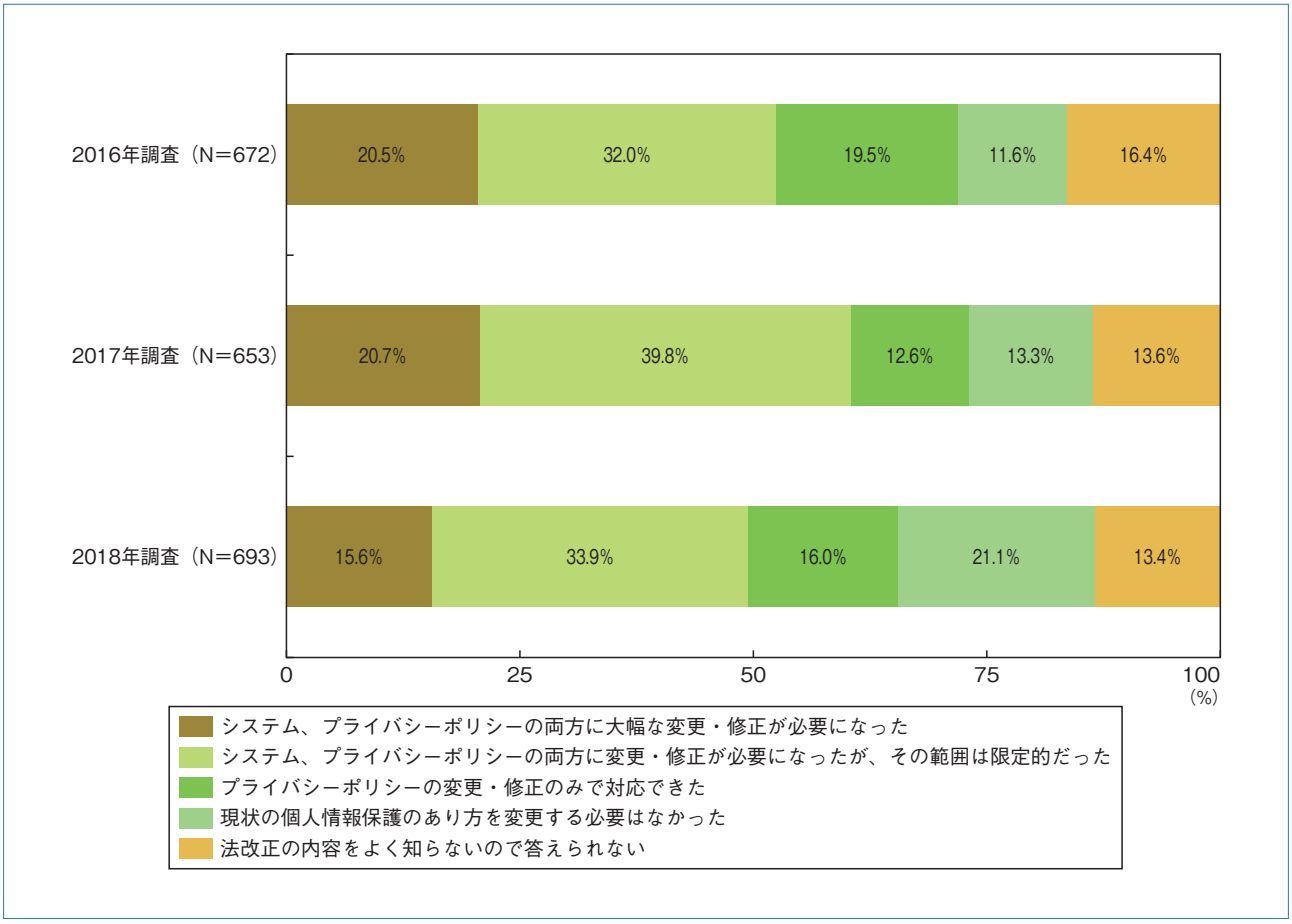


図15. 個人情報保護法改正が及ぼすインパクトの経年比較（2016年～2018年調査）

法の改正内容で注目している点を調査した結果、「匿名加工情報の定義と範囲、取扱い」「個人データの第三者提供」が年々増加傾向となった（図16）。改正個人情報保護法への対応が終了した企業は、次に匿名加工情報を利用したビジネスへの貢献に注力が向いていると予測される。

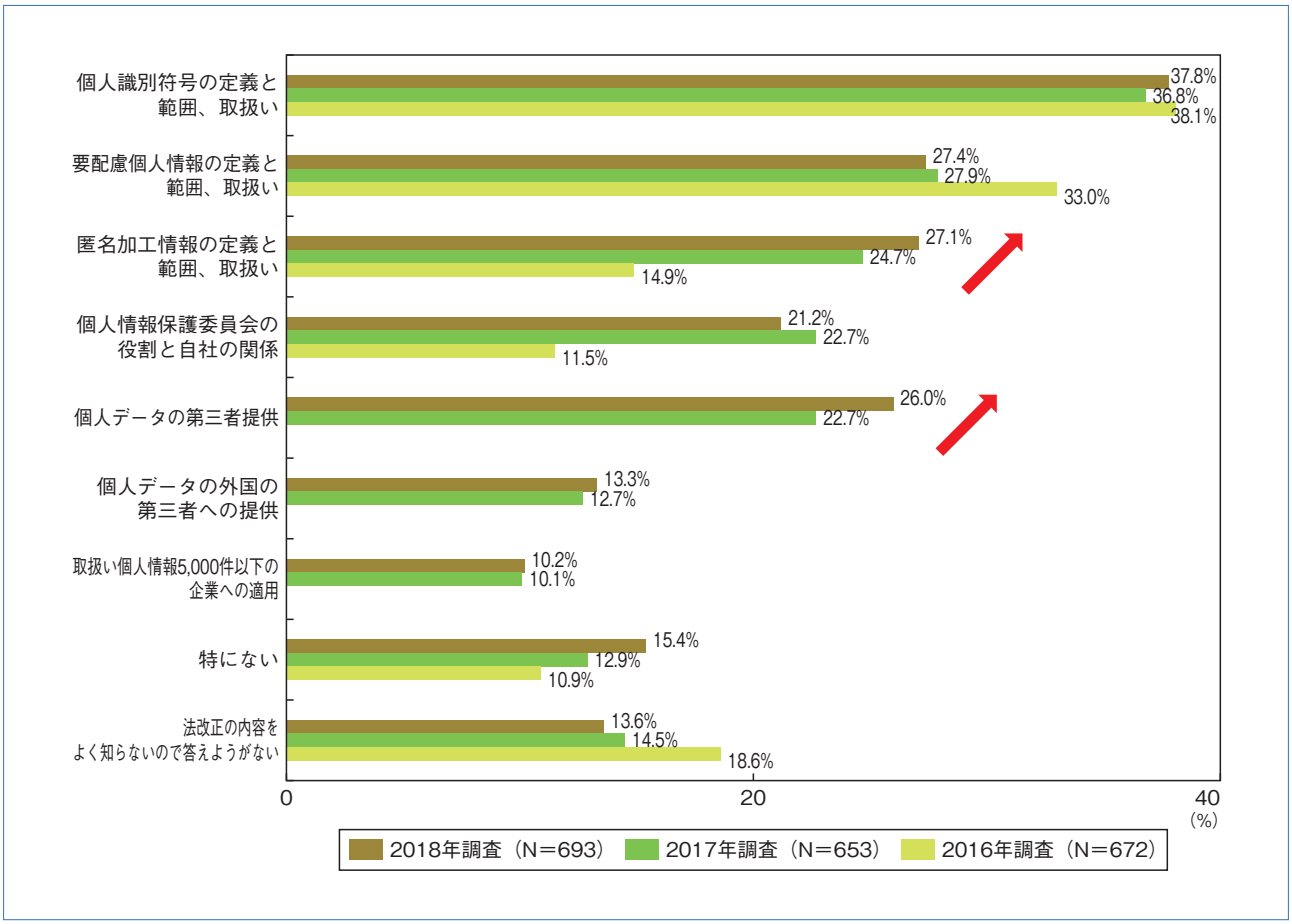


図16. 改正個人情報保護法の改正内容の関心度の経年比較（2016年～2018年調査）

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、改正法への対応状況について調査したところ、８割弱の企業が「すでに対応済み」もしくは「2017年度（2018年３月）までに対応を完了させる見込み」と回答した（図17）。その一方で、依然として「いつまでに完了できるかわからない」とする回答も約２割あり、今後の対応が課題といえる。なお、個人情報保有件数別にみると、法改正前は規制対象外であった「5,000件未満」の企業の約３割が「対応完了時期がわからない」と回答した。

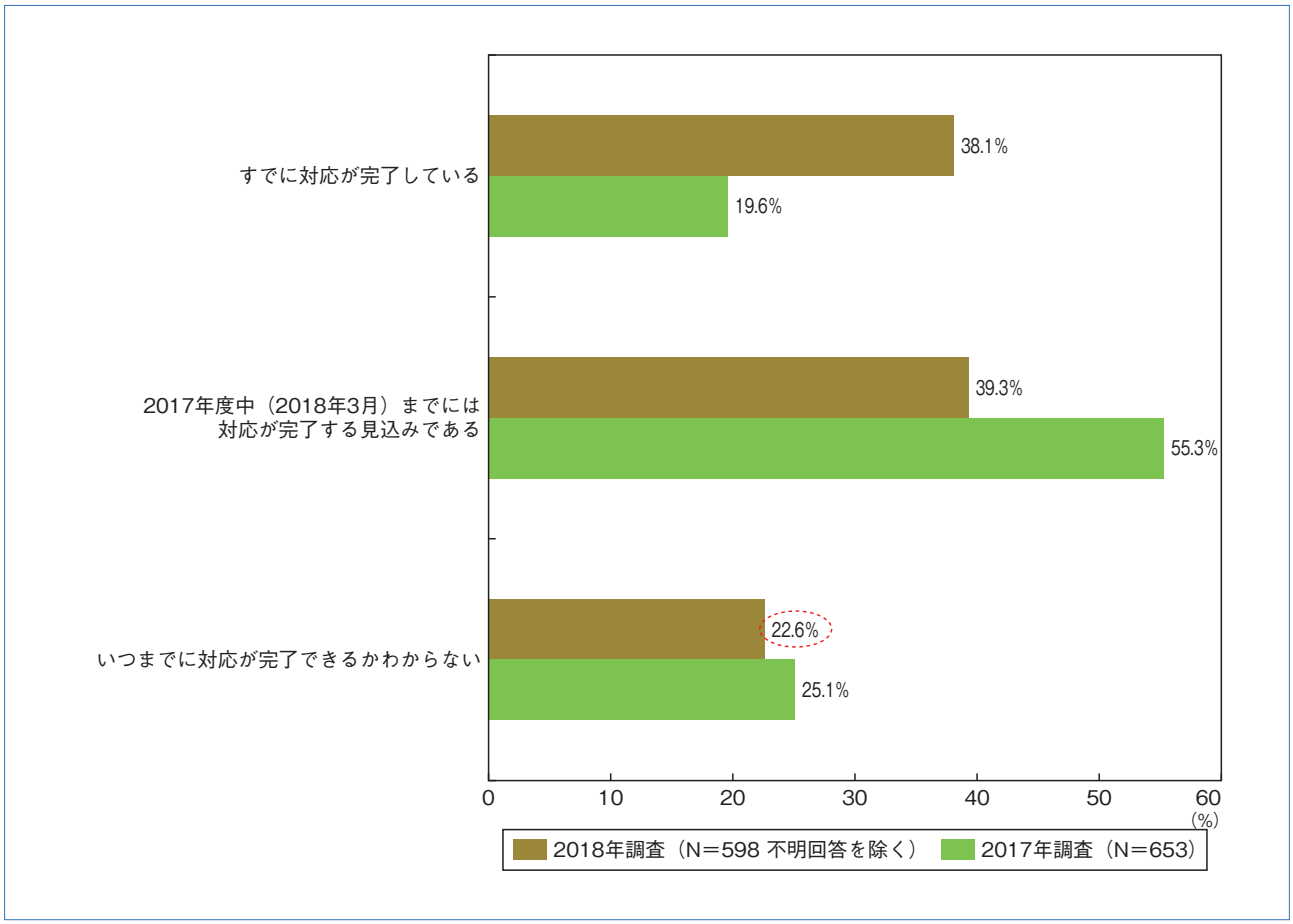


図17. 改正個人情報保護法の対応期間の状況（2017年～2018年調査）

4-3. EUプライバシー規制への対応状況

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、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欧州連合（EU）域内に事業拠点または顧客をもつとする回答者（153件）に対して、2018年５月25日から施行されるEU（EEA）からの個人情報の域外への移転を制限する「EUデータ保護規則（GDPR）」への対応状況を調査した。

施行約４か月前となる今年１月時点で、未だ４割以上が「規制の存在を初めて知った」または「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」と回答し、規制対応にIT／セキュリティ責任者が十分に関与していない実態が明らかとなった。

また、「GDPRに触れぬよう、個人情報は移転しないようにしている」が9.2％、「GDPRを特に気にすることなく個人情報の移転を行っている」との回答が15.0％存在し、「GDPR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」は26.1％にとどまった（図18）。

同規則ではインシデントが発生した場合には、72時間以内の報告義務があることなどから、対象となる企業では早急な対応が求められる。

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、ということを自覚すべきであろう。

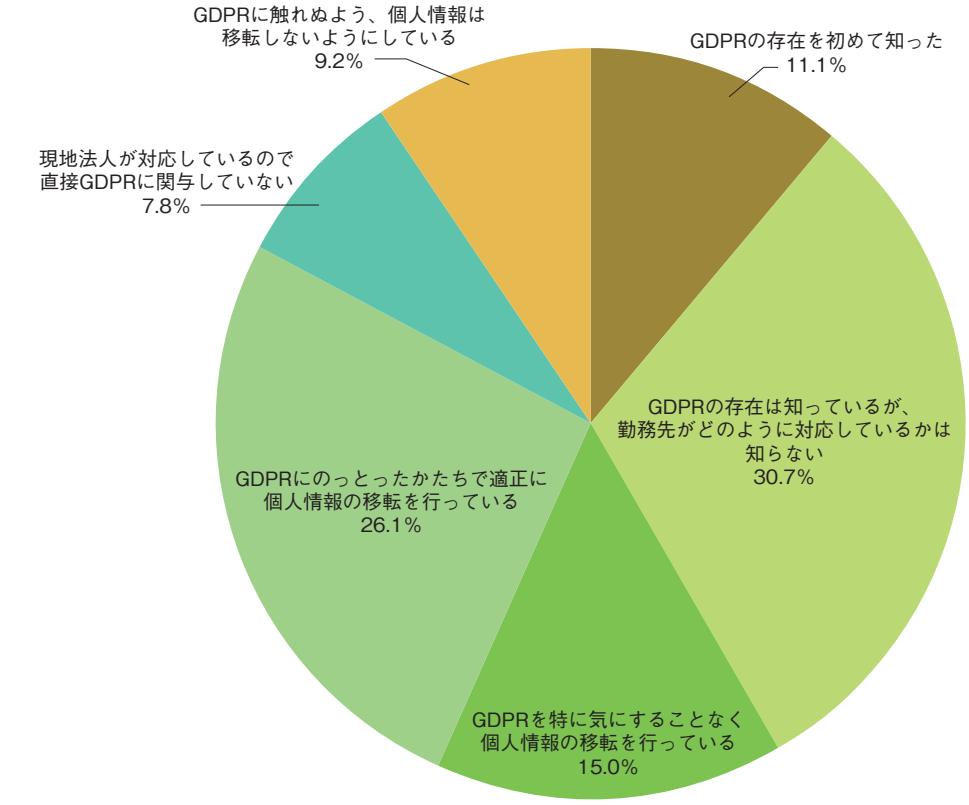


図18. EUのプライバシー規制への対応状況

5 働き方改革とクラウドの動向

安倍政権も重要政策の１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、昨年同様、この働き方改革の推進状況と、今年は新たにクラウドの動向に着目して調査した。

5-1. 働き方改革の取組み状況

政府が推進する「働き方改革」の取組み状況について、従業員の「働き方変革が経営目標として掲げられている」企業の割合は2017年の26.8％から2018年は34.2％と、約７ポイントの増加がみられた。しかしながら、「テレワークの制度が整備されている」および「在宅勤務制度が整備されている」企業の割合は微増にとどまった。「働き方改革」の取組みについて経営課題として経営層の関心は高まりつつあるが、対策の整備は進んでいない状況も浮彫りとなった。(図19)。

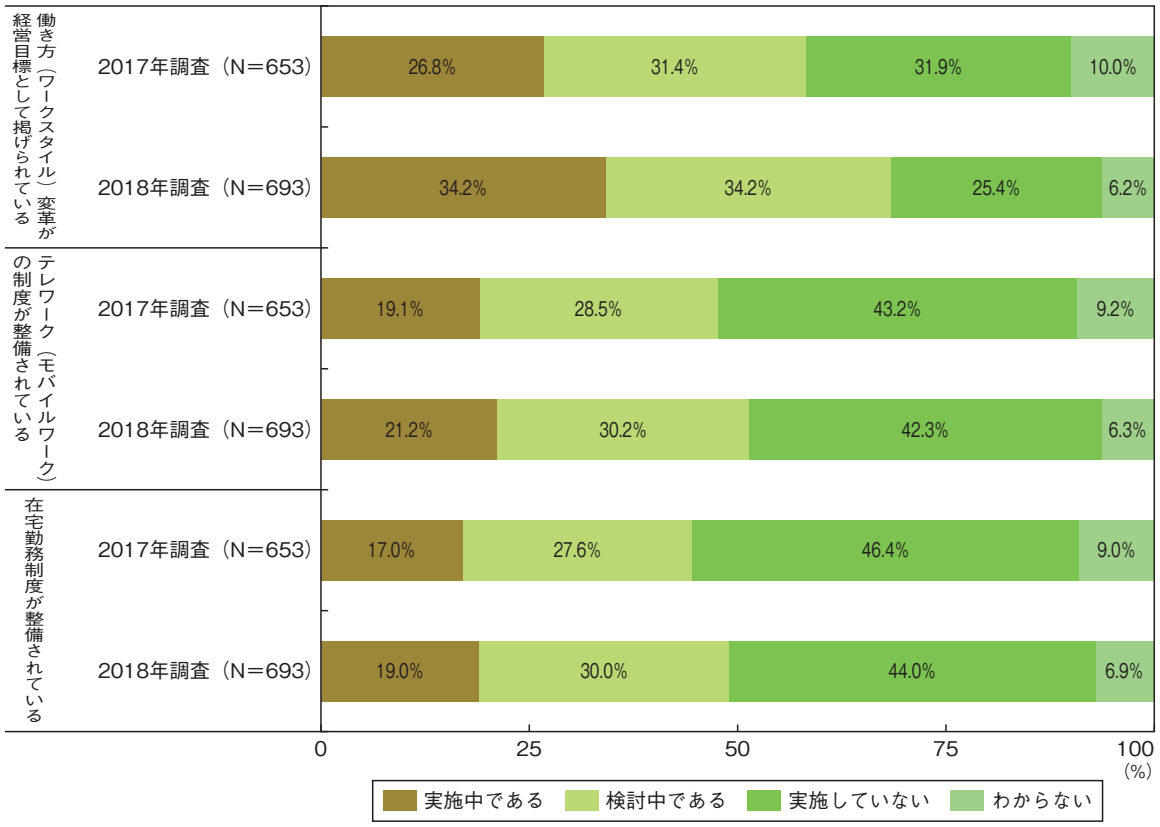


図19.「働き方改革」に関する取組み状況の経年変化（2017年～2018年調査）

5-2. 働き方改革と関わるセキュリティ対策の実施状況

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７項目選び、現在の実施率と今後の計画について調査した（図20）。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、「スマートデバイスのセキュリティ対策」が44.4％の企業で実施されており、続いて「クラウドサービスの利用」が40.8％であった。

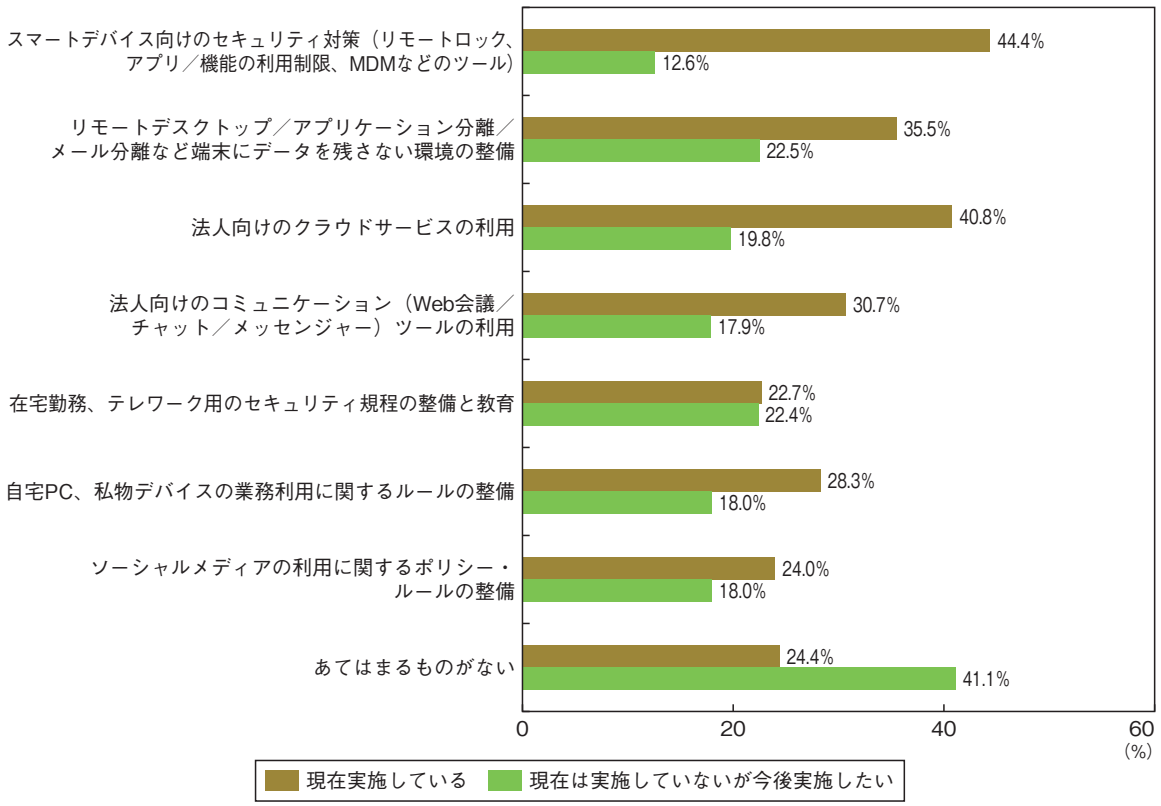


図20. 働き方改革と関わるセキュリティ対策の取組み状況

5-3. クラウドの動向

現在、クラウドがさまざまな分野で本格的な普及期に入りつつあることから、クラウドサービスを選定する際のポイントについて調査した（図21）。「コスト」が57.0％で首位となり、次に「セキュリティ対策がきちんとしている」が41.1％、「サポート体制の充実度」が34.1％であった。

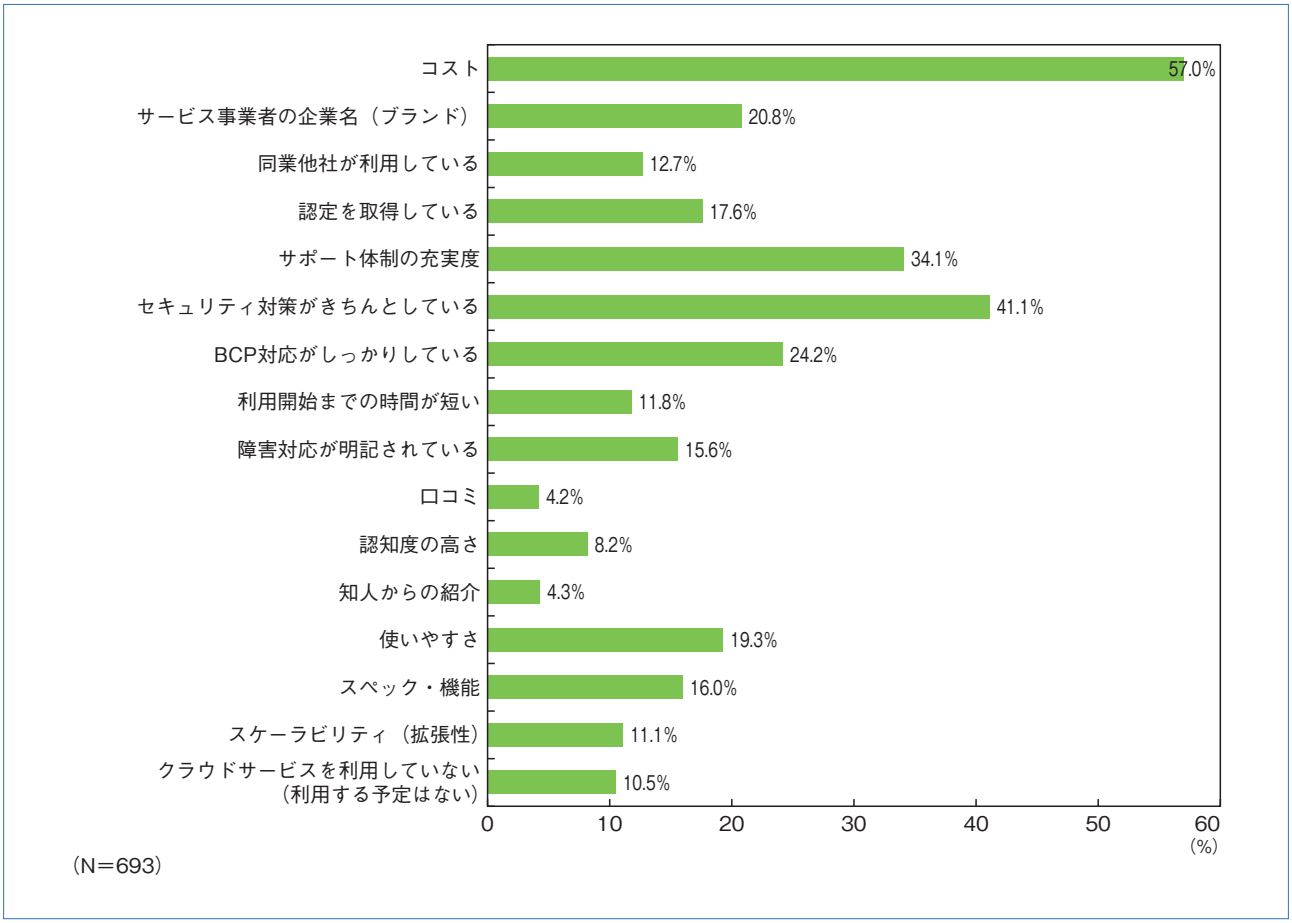


図21. クラウドサービスを選定する際のポイント（複数回答）

5-4. 電子契約の導入状況

働き方改革と関連して、企業はこれまで紙ベースで行っていた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。そこで、特に電子化したい業務プロセスについて調査した（図22）。

「経費精算（旅費、交通費）」が37.7％で最も多く、次に「請求処理」33.9％であった。今後は改正電子帳簿保存法に適応する企業の増加が見込まれることから、経費精算の電子化の需要が増すことが予測される。

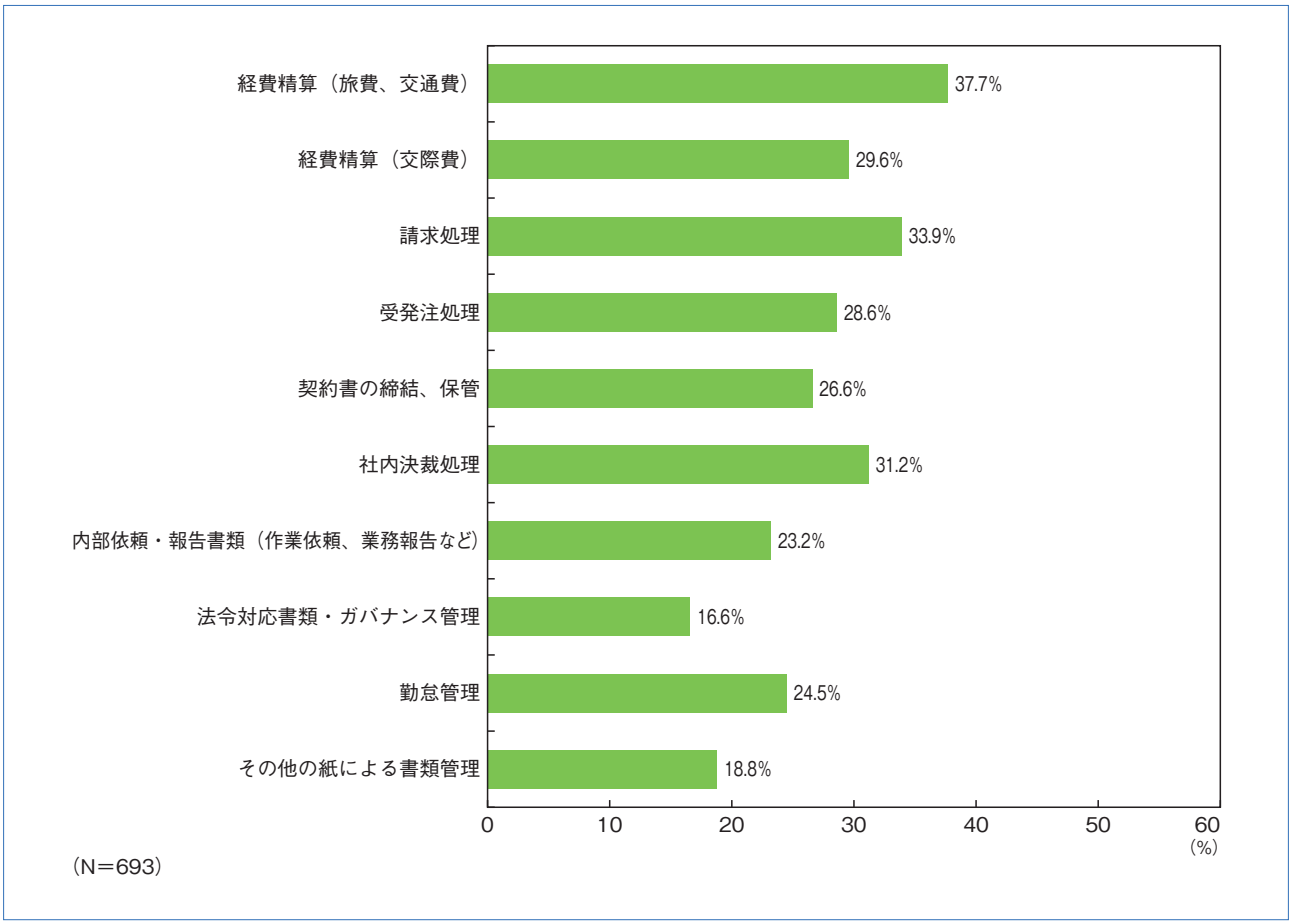


図22. 特に電子化したい業務プロセス（複数回答）

電子契約の利用状況について定点観測を行っているが、今回の調査では、利用率の内容について若干変化がみられた（図23）。

電子契約の実現手段として、これまでは１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」のシステム環境が優位であったが、今回の調査では１対Ｎ型が減少し、複数の組織、部門間で電子契約を行える「Ｎ対Ｎ型」システムの利用が増加した。さらに、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では、昨年までは自社開発の電子契約システムを利用する割合が多かったが、今年は外部の電子契約サービスを利用する割合が増加しており、ここでもクラウドの利用が増加することが予測される。

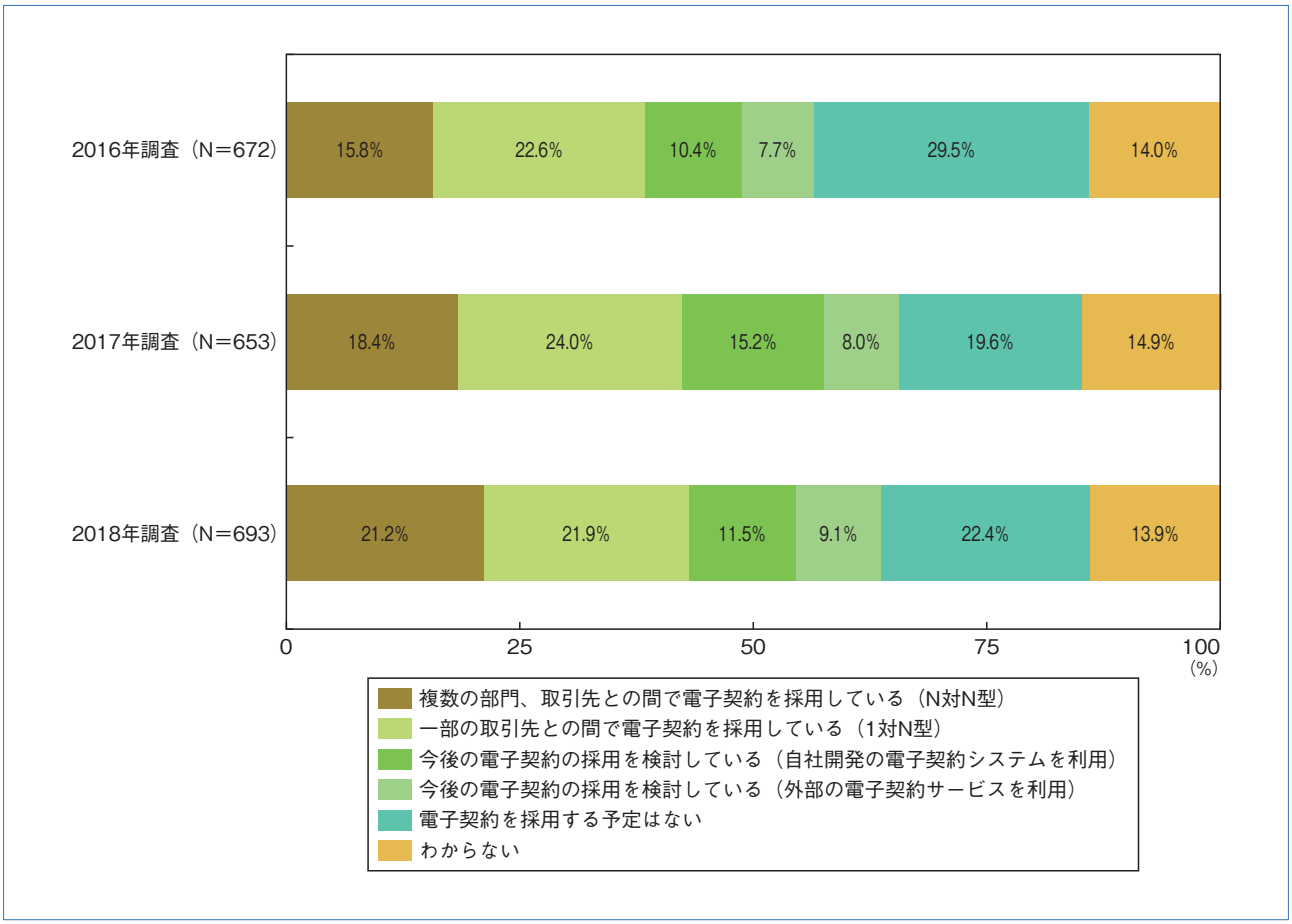


図23. 電子契約の利用状況の経年比較（2016年～2018年調査）

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別にみる。

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。項目別にみると、「ファイアウォール」の導入率が最も高く、次いで「VPN」「Webセキュリティゲートウェイ」「URLフィルタリングツール」が続いている。また、今後３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」、クラウド／アプリケーションを保護するための「CASB（Cloud Application/Access Security Broker）ツール」「インターネット分離ツール」「サンドボックス」「DDoS対策」があげられる（図24）。

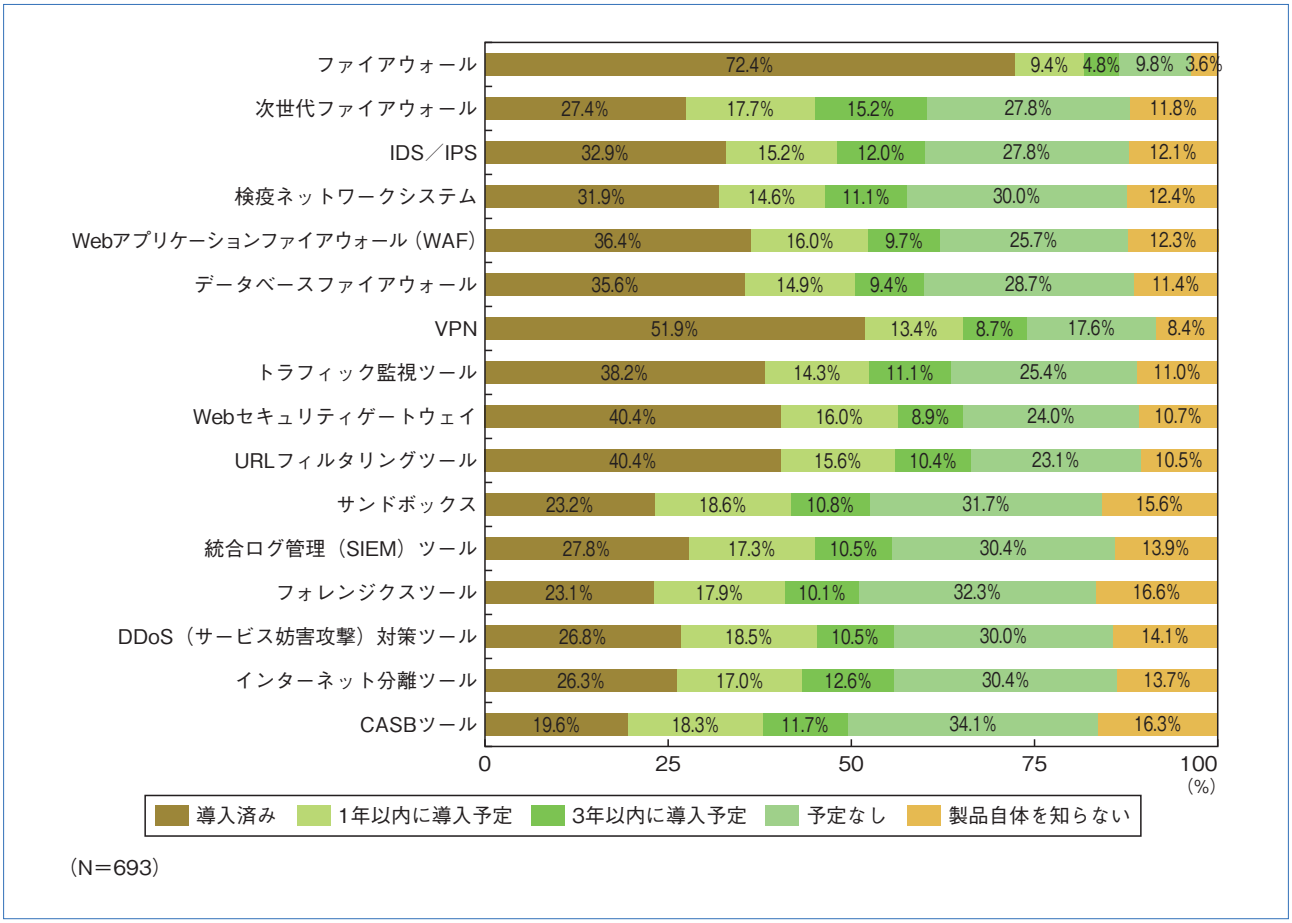


図24. セキュリティ製品の導入率（ネットワークセキュリティ）

6-2. クライアントセキュリティ製品の導入状況

主としてクライアントPCの保護を目的に利用される製品としては、「ウイルス対策ソフト（クライアント型）」の導入率が際立って高い傾向に変化はない。今後に向けては、「UEBA（User Entity Behavior Analytics）」「シンクライアントシステム」「PC資産管理／PC操作ログ管理」や新しい技術であるEDR（Endpoint Detection and Response）の導入意欲が高い（図25）。

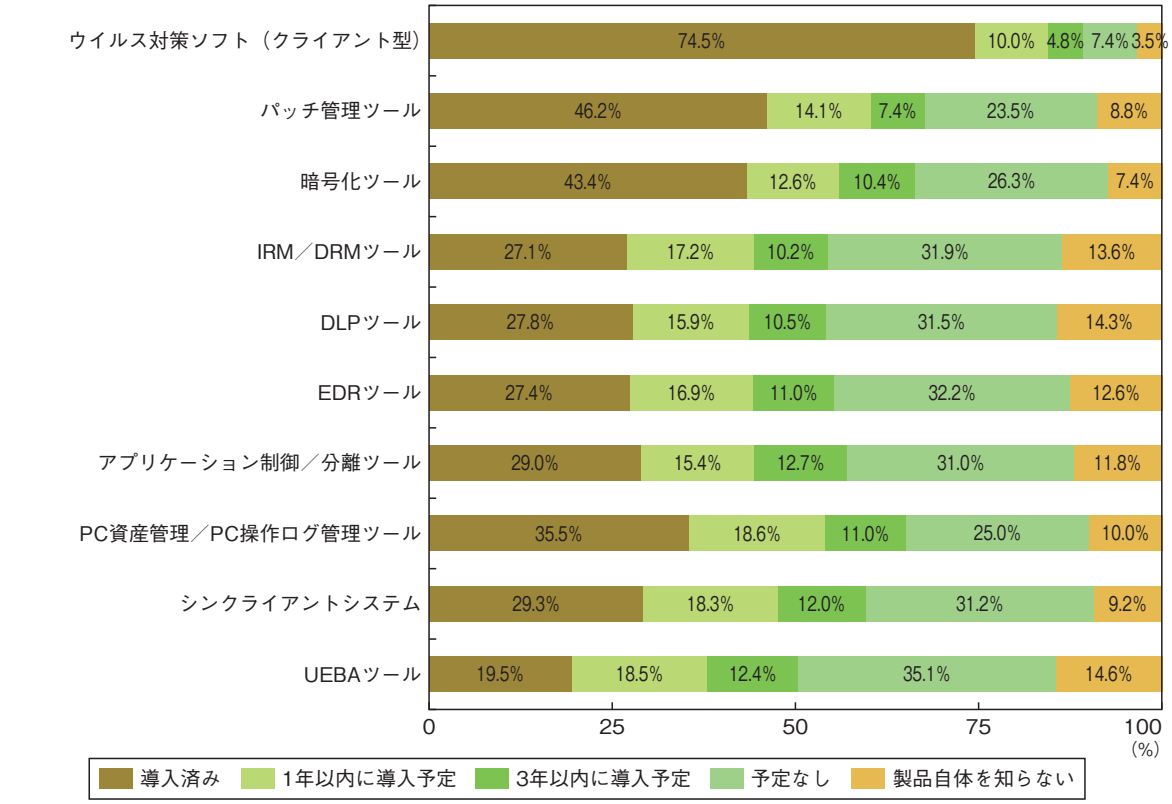


図25. セキュリティ製品の導入率（クライアントセキュリティ）

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。今回の調査では、「社内サーバ／プラットフォームに対する脆弱性診断サービス」の利用率が最も高い結果であった（図26）。今後に向けては「セキュリティオペレーションセンタによる総合的なセキュリティ監視」「サイバー保険（個人情報漏えい保険含む）」に対する導入意欲が高い。投資対効果が見えにくいセキュリティ対策の中で、今後はサイバー保険により、セキュリティリスクを移転する戦略も需要が増す可能性もある。

また、肥大化の一途をたどる各種セキュリティ機器の運用アウトソーシングや、セキュリティ情報（脅威情報）配信サービスも今後に向けて注目が高まると予想される。

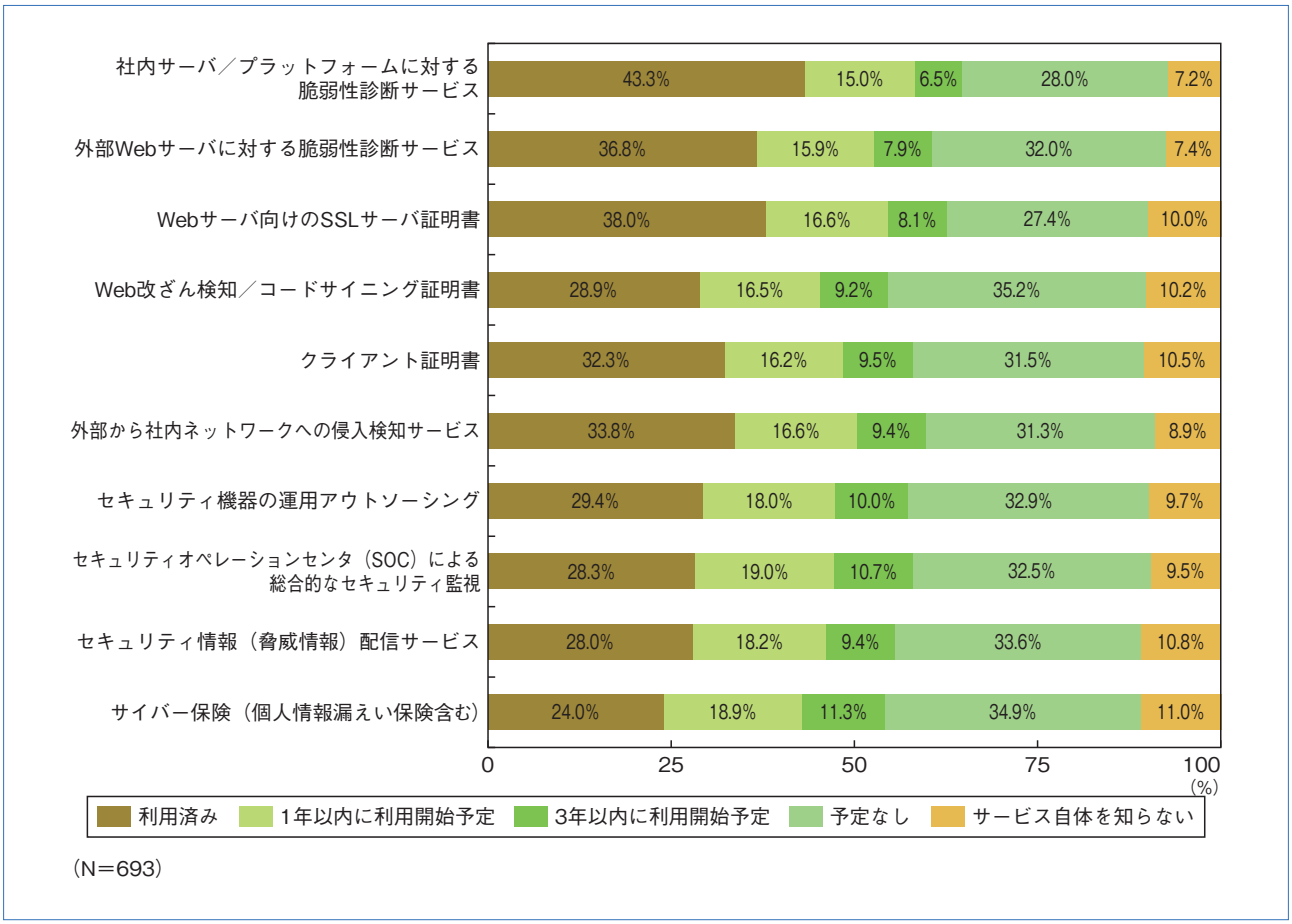


図26. セキュリティ製品の導入率（セキュリティサービス）

6-4. 電子メールのセキュリティ対策の実施状況

電子メールのセキュリティ対策について、昨年同様送信者、受信者別に考えられる主要な対策を選び、その実施状況を調査した。

送信者側の対策としては「メール誤送信防止ツール」「zipパスワードによる添付ファイルの暗号化」が、受信者側の対策としては「アンチウイルス」「スパムフィルター」「メール無害化」の導入／実施率が高いとの結果が示された（図27）。特にグローバルの潮流と比較して「zipパスワードによる添付ファイルの暗号化」は日本独特のセキュリティ対策といえる。なお、「メールの無害化」については前年調査の27.7％から20ポイント以上の増加がみられた。

ビジネスメール詐欺対策として有効な手段の１つである送信者認証は、今後に向けて関心が高まっているものといえる。SPF、DKIMといった認証手段の利用率も、送信者側、受信者側ともに２割を超えており、今後の導入意欲も高い。

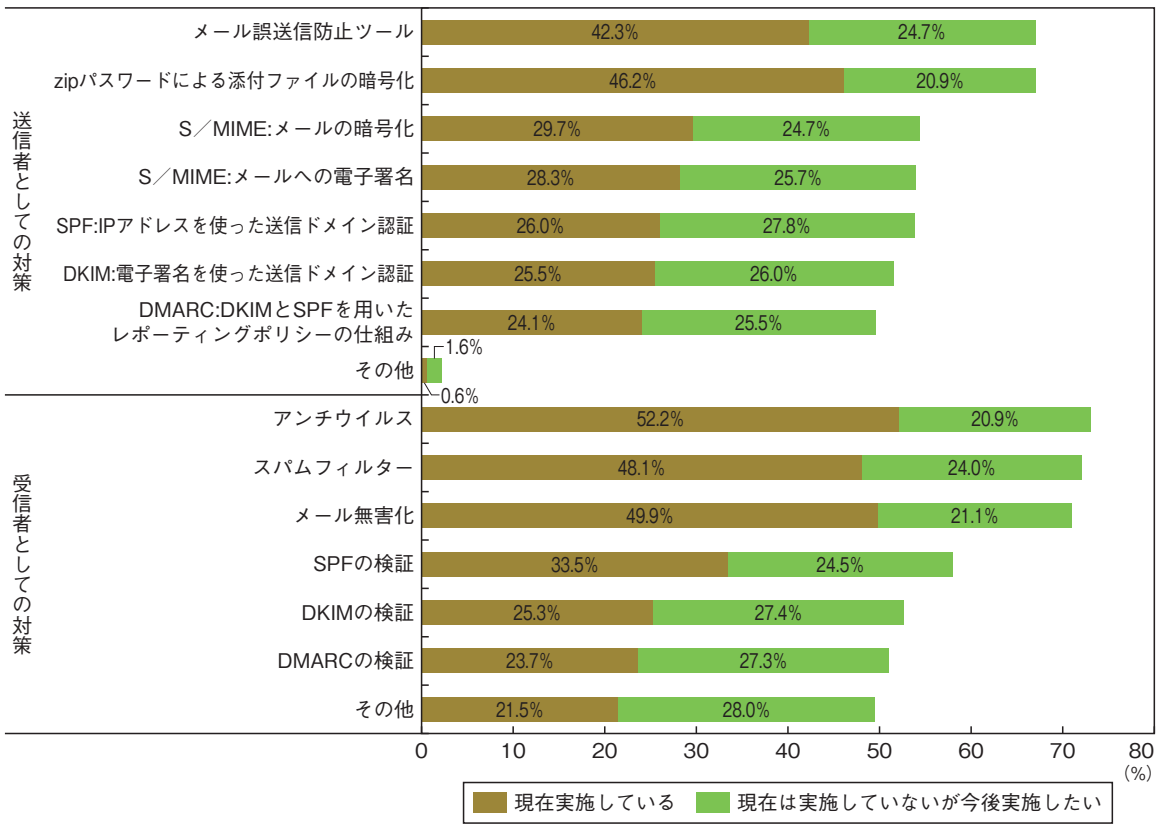


図27. 電子メールのセキュリティ対策の実施状況

6-5. 社内システムのアクセス認証手段の導入状況

社内システムのアクセス認証手段の導入状況について、ID／パスワードの導入率が高いのは当然であるが、LDAP／Active Directoryの導入は39.5％に止まっている（図28）。一方で、導入意欲が高い認証手段に「生体認証」「FIDO認証」があげられる。今後、クラウドの利用が増えれば、オンプレミスの環境とクラウド環境をシームレスに認証可能とする手段の需要がより一層高まると予測される。

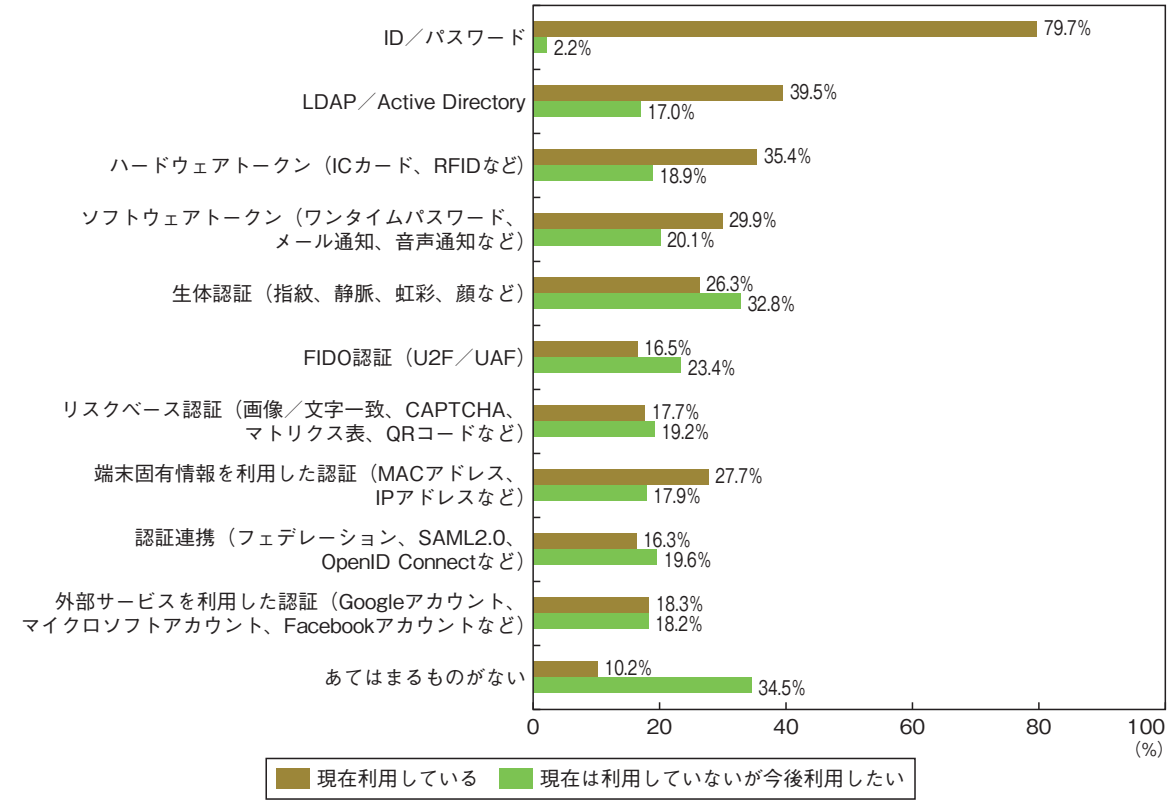


図28. 社内システムへのアクセス認証手段の導入状況

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実施しており、今回で7回目となった。回を重ねるなかでみえてくるのは、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、多様化しているという現実である。サイバー攻撃はAIの活用などで高度化し、IoT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デバイスに依存したサイロ型のセキュリティツールの導入および対策（マルウェア感染／Web対策、USBデバイス対策など）に重きが置かれている。今後は、クラウド環境を含め企業間を超えた重要情報の保護、つまり企業責務としてサプライチェーンを含めた包括的なセキュリティ対策を強化する必要があろう。さらにはデータの改ざん防止を含め、ITガバナンスや内部統制といった内部不正対策もより強化が求められる。

改正個人情報保護法への対応については、一部の企業でまだ完了していないが、８割の企業で対応のめどが立ったことから、今後は匿名加工情報などのビジネスの利用に向けた施策に関心が推移していくだろう。ただし、海外法への対応は多くの対象企業が早急な対策が必要である。今後は、国境を越えたプライバシー保護への対策不足がビジネスに影響を与えかねない、ということを認識しておく必要がある。特に2018年５月25日に施行されたGDPRは、インシデントが発生した場合に72時間以内の報告義務があることや、罰金が科されるため、対象となる企業は早急な対応が求められる。

国内企業においては、2017年11月に経済産業省から出された「サイバーセキュリティ経営ガイドライン」への準拠を通じて経営層を巻き込み、全社的なリスクマネジメントの一環として、情報セキュリティへの投資を行う必要がある。特にインシデントの検知・復旧での能力を向上させるために、多様化と複雑化が進む現在のリスクについて改めて捉え直すことから始めることが求められるといえる。

安倍政権も積極的に推進している「働き方改革」は、経営層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なかでも昨年同様２位となった。しかし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に対応している企業はまだ少なく、これからの動向を見守る必要があるといえる。今後はクラウドの活用と合わせ、働き方改革とセキュリティ対策について、利便性と安全性の両立がこれまで以上に求められるであろう。

回答者プロフィール

業種	回答数	%
製造	196	28.3
建設・不動産	55	7.9
卸売・小売	60	8.7
金融・保険	60	8.7
情報通信	112	16.2
サービス	160	23.1
公共・その他	50	7.2
全体	693	100.0

年間売上規模	回答数	%
1,000万円未満	4	0.6
1,000万円～1億円未満	2	0.3
1億～10億円未満	69	10.0
10億～100億円未満	204	29.4
100億～500億円未満	144	20.8
500億～1,000億円未満	62	8.9
1,000億～3,000億円未満	61	8.8
3,000億～5,000億円未満	36	5.2
5,000億円以上	111	16.0
全体	693	100.0

従業員規模	回答数	%
5,000人以上	158	22.8
1,000～4,999人	157	22.7
300～999人	163	23.5
50～299人	215	31.0
全体	693	100.0

業種別内訳

業種		回答数	%
製造	食品・飲料	12	1.7
	日用品・生活雑貨	5	0.7
	繊維	7	1.0
	パルプ・紙・印刷	5	0.7
	化学工業	14	2.0
	石油製品	3	0.4
	鉄鋼・金属	15	2.2
	プラスチック・ゴム	5	0.7
	機械	20	2.9
	電気機器	32	4.6
	情報通信機器	10	1.4
	電子部品・電子回路	17	2.5
	精密機器	13	1.9
	自動車・輸送機器	17	2.5
	医薬品	4	0.6
	その他の製造業	17	2.5
建設・不動産	建設	36	5.2
	不動産	17	2.5
	住宅	2	0.3
卸売・小売	卸売	24	3.5
	小売	15	2.2
	商社	21	3.0
金融・保険	銀行	33	4.8
	証券	9	1.3
	生命保険	2	0.3
	損害保険	7	1.0
	その他金融	9	1.3

業種		回答数	%
情報通信	通信	22	3.2
	ITベンダ/システムインテグレータ	67	9.7
	インターネットサービス	8	1.2
	情報システム子会社	15	2.2
サービス	電力・ガス・水道	7	1.0
	運輸	17	2.5
	倉庫	8	1.2
	宿泊	1	0.1
	飲食	10	1.4
	娯楽・レジャー	7	1.0
	メディア・出版・放送・広告	4	0.6
	生活関連サービス(旅行業など)	7	1.0
	医療	27	3.9
	福祉・介護	24	3.5
	教育（学校以外）	7	1.0
	人材派遣・業務委託	10	1.4
	その他サービス	31	4.5
公共・その他	学校	13	1.9
	官公庁	6	0.9
	地方自治体	22	3.2
	その他公共機関	9	1.3
	全体	693	100.0

IT戦略／情報セキュリティへの関与度合	回答数	%
全社的なIT戦略に決定権をもっている	297	42.9
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	369	53.2
セキュリティ製品の導入、製品選定に関与している	434	62.6
セキュリティ対策の実務に関与している	294	42.4
全体	693	100.0

〈資料〉情報化に関する動向（2017年10月～2018年３月）

国　内	海　外
2017年10月	
・総務省サイバーセキュリティタスクフォース、「IoTセキュリティ総合対策」発表。脆弱性対策整備、民間企業のセキュリティ対策推進、人材育成など５項目の施策を推進。 ・日本ディープラーニング協会設立。深層学習の技術者育成を目指す。 ・日立製作所、生体情報から電子署名を生成する技術を応用し、ブロックチェーン上でIoT決済や自動取引を安全に行える連携技術を開発。 ・トレンドマイクロ調査、「パスワード使いまわし」85.2%。 ・情報処理推進機構（IPA）、他社との比較で自社のセキュリティ対策の取組み状況のレベルを把握できる「情報セキュリティ対策ベンチマーク　バージョン4.6」サービス開始。	・米Oath調査、2013年に発生した米Yahoo! へのサイバー攻撃で流出したアカウントは30億件に。 ・米国土安全保障省（DHS）と連邦捜査局、政府機関、エネルギー、電子力、水道等重要インフラへの不正侵入被害の分析結果を公表・警告。 ・ロシア他、ランサムウェア「Bad Rabbit」感染拡大。 ・米Google、メディア専門教育研究機関The Poynter Instituteが運営する事実検証フォーラムと連携し、フェイクニュース対策強化。

国　内	海　外
2017年11月	
・マイナポータル、11月13日から本格運用開始。 ・厚生労働省、2020年度までに健康保険証番号を個人に割当て。健診情報の一元化を目指す。 ・産業技術総合研究所、２種類のパスワードで相互認証する「AISTパスワード認証方式」と、匿名で認証可能な「AIST匿名パスワード方式」が国際標準化。 ・政府、日本年金機構がマイナンバー制度で情報連携可能とする政令を閣議決定。 ・経済産業省、サイバーセキュリティ経営ガイドライン改訂。	・米ミズーリ州司法当局、Googleの個人情報の収集・利用が消費者保護に反するとして調査を開始。Googleは強固な個人情報保護実施を訴え。 ・米連邦通信委員会（FCC）、「ネットの中立性」原則撤廃を発表。 ・米Uber、2016年10月に約5,700万件の個人情報が漏えいしたことを1年以上経過して発表。

国　内	海　外
2017年12月	
・千代田区立図書館、サイバー攻撃で約1か月閲覧不能に。 ・警察庁、インターネットバンキングで不正送金させるウイルス「ドリームボット」感染被害急増を発表。 ・日本経済団体連合会、サイバーセキュリティ対策強化に向け、経営者層の意識改革、人材育成急務を提言。 ・NEC、日立製作所、富士通、2020東京五輪に向けて2,000人のセキュリティ専門家の共同育成を発表。 ・個人情報保護委員会、EUデータ保護移転をテーマに欧州委員会のヨウロバー委員と会談。最終合意を目指し今後も会談実施へ。 ・個人情報保護マネジメントシステム－要求事項「JIS Q 15001:2017」改正。	・Google、ユーザの同意なくデータ収集するアプリの取締り強化。アプリや誘導サイトに警告表示。 ・中国政府、インターネット管理・統制を強いる方針策定。 ・スロベニアの仮想通貨マイニング事業者NiceHash、ハッキング被害で仮想ウォレットコンテンツ約4,700ビットコイン（約6,000万ドル超相当）の盗難被害に。 ・加Nissan Canada Finance、ローン利用者、約113万人の個人情報流出。 ・中国政府のインターネット規制、2015年以降に13,000超のサイト閉鎖。SNSアカウント閉鎖は1,000万件。

国　内	海　外
2018年1月	
・情報通信研究機構、量子コンピュータでも解読困難な暗号技術開発。 ・トレンドマイクロ調査、2017年のサイバー攻撃被害はランサムウェアが圧倒的。ビジネスメール詐欺も増加傾向に。 ・東京高裁、ヤフー検索結果の偽り情報に対し名誉棄損を認め、削除命令。 ・仮想通貨取引所コインチェック、不正アクセス被害で580億円相当の仮想通貨「NEM」流出。2月に全額返金。 ・IPA、「情報セキュリティ10大脅威2018」公開。1位は標的型攻撃被害(組織)、インターネットバンキング・クレジットカード情報の不正利用（個人)。 ・東京地裁、Google検索による自社の虚偽情報表示削除を求める訴訟に対し、検索結果が真実か否かの証明ができないとして、請求棄却。	・DHS、不正アクセスで現・元職員約24万人の個人情報が漏えい。 ・米Intel、49量子ビットの量子コンピューティングテストチップ「Tangle Lake」開発成功。 ・米Facebook、GDPR対応でプライバシーポリシーを初公開。 ・Facebook、仮想通貨、ICO関連の広告掲載を全世界で禁止。

国　内	海　外
2018年2月	
・NEC、毎秒10万件の記録可能な世界最速のブロックチェーン向け合意形成アルゴリズム開発。 ・トレンドマイクロ調査、日本での仮想通貨を不正採掘する「コインマイナー」のデバイス検出件数は、2017年10-12月期に13万件で、前期の16倍。 ・政府、「不正競争防止法の一部を改正する法律案」閣議決定。IoT、AI環境下でのデータ利活用促進環境整備へ。第196回国会で成立。 ・経済産業省、情報セキュリティサービスを安心に利用できる環境醸成に向け、セキュリティサービス基準、情報セキュリティサービスに関する審査登録機関基準策定。	・仮想通貨「Monero」を採掘するマルウェア「ADB.Miner」、中国、韓国で感染拡大。 ・伊BitGrail、1,700万XRB（200億円相当）の仮想通貨「Nano」流出。 ・仮想通貨を不正採掘するマルウェア「Coinhive」、世界4,000以上のサイトが改ざん被害。 ・平昌オリンピック公式サイト、サイバー攻撃被害で12時間システムダウン。 ・独ベルリン裁判所、Facebookのデータ保護指針とサービス条件を違法と判断。 ・欧州委員会、TwitterとFacebookの消費者保護対策に是正要求。Googleの改善策は評価。 ・米大統領経済諮問委員会、2016年の米国に対するサイバー攻撃被害額が570～1,090億ドルだったと報告。 ・ベルギー裁判所、Facebookの個人情報収集・保管方法がプライバシー侵害に当たると判決。「いいね！」ボタン設置だけで個人情報収集。 ・FCC、「ネット中立性」規定廃止規則公布。 ・米McAfee&戦略国際問題研究所調査、サイバー犯罪が世界経済にもたらす損失は6,000億ドルと予測。2014年調査から約1,500億ドル増加。

国　内	海　外
2018年3月	
・政府、「サイバーセキュリティ基本法の一部を改正する法律案」閣議決定。内閣セキュリティサイバーセンターが事務局となり、サイバーセキュリティ協議会創設へ。 ・警察庁調査、2017年の仮想通貨業者等を狙った不正アクセス被害は149件、被害額約６億6,240万円相当に。 ・個人情報保護委員会、SNSの「いいね！」ボタン押下での非ユーザデータ収集の可能性について注意喚起。 ・IoT推進コンソーシアム、「カメラ画像利活用ガイドブックVer2.0」策定。特定空間での設置カメラのリピート分析時の配慮事項を整理。	・米信用情報会社Equifax、2017年5-7月に受けたサイバー攻撃被害により、14,550万人の個人情報の流出を報告。昨年９月の報告時より約240万人増加し、2017年最大規模の流出事件に。 ・Uber、自動運転車試行運転中に初の歩行者死亡事故。 ・Facebook、トランプ陣営が契約した英調査分析会社Cambridge Analyticaによる5,000万人分の個人情報が不正利用されたことに対し、アプリによる個人情報収集対策を発表。その後の調査で流出は8,700万件に。

JIPDEC

JIPDEC IT-Report 2018 Spring

2018年5月31日発行（通巻第11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　株式会社ウィザップ