IT-Report
2019 Spring

IT-REPORT

2019 Spring

Contents

JIPDEC
一般財団法人日本情報経済社会推進協会

本誌「JIPDEC IT-Report 2019 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、紹介しています。

本調査では、欧州（EU）域内に事業拠点または顧客を持つ回答者に対し、2018年５月25日に施行された「一般データ保護規則（GDPR）」への対応について調査していますが、「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」との回答が３割強となった一方で、「GDPRの存在は知っているが何も対応していない」「特に気にすることなく個人情報の移転を行っている」も３割を占めていました。

2017年に個人情報保護法やJIS Q 15001が改正されたことを受け、企業が法規制の何に関心を持っているかを調査したところ、「個人識別符号の定義と範囲、取扱い」に対し、過去の調査同様、関心が高いことがわかりました。

また、2018年に総務省による「パスワードの定期変更不要」見解への対応については、約５割がこれまでどおりパスワードの定期変更を行っており、パスワードから多要素認証に変更した割合が１割強にとどまっていることがわかりました。

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、2018年10月から2019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 2019 Spring

Contents

特 集

「企業IT利活用動向調査2019」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等に所属し、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2017年以降の調査結果と比較・分析して紹介する。

1 調査概要

1-1. 調査概要

・実査期間：2019年１月17日～２月４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、課長相当職以上の役職者約3,000人（2018年調査までは係長相当職以上を対象）。
・有効回答数：686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（29.6%）、次いでサービス業（24.5%）、情報通信（14.3%）、建設・不動産（9.5%）、卸売・小売（9.3%）、金融・保険（7.0%）となった。所属部門では情報システム部門が最も多く（34.1%）、役職は部長（43.3%）、課長（37.9%）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合いをみると、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、「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」（54.7%）、「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」（48.1%）とする回答が多く、前回調査と傾向はあまり変わっていない。

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」を一貫してメインテーマとしている。まずは経営課題の中での情報セキュリティの位置づけと、リスクの重視度合いを中心に調査結果をみる。

2-1. 重視する経営課題

経営課題として考えられる25項目に対し、複数回答で今後に向けて重視したいと考えられる項目を選んでもらった。「業務プロセスの効率化」がトップの58.0%、次いで「従業員の働き方改革」(45.9%)「情報セキュリティの強化」(38.5%)と続く(図1)。

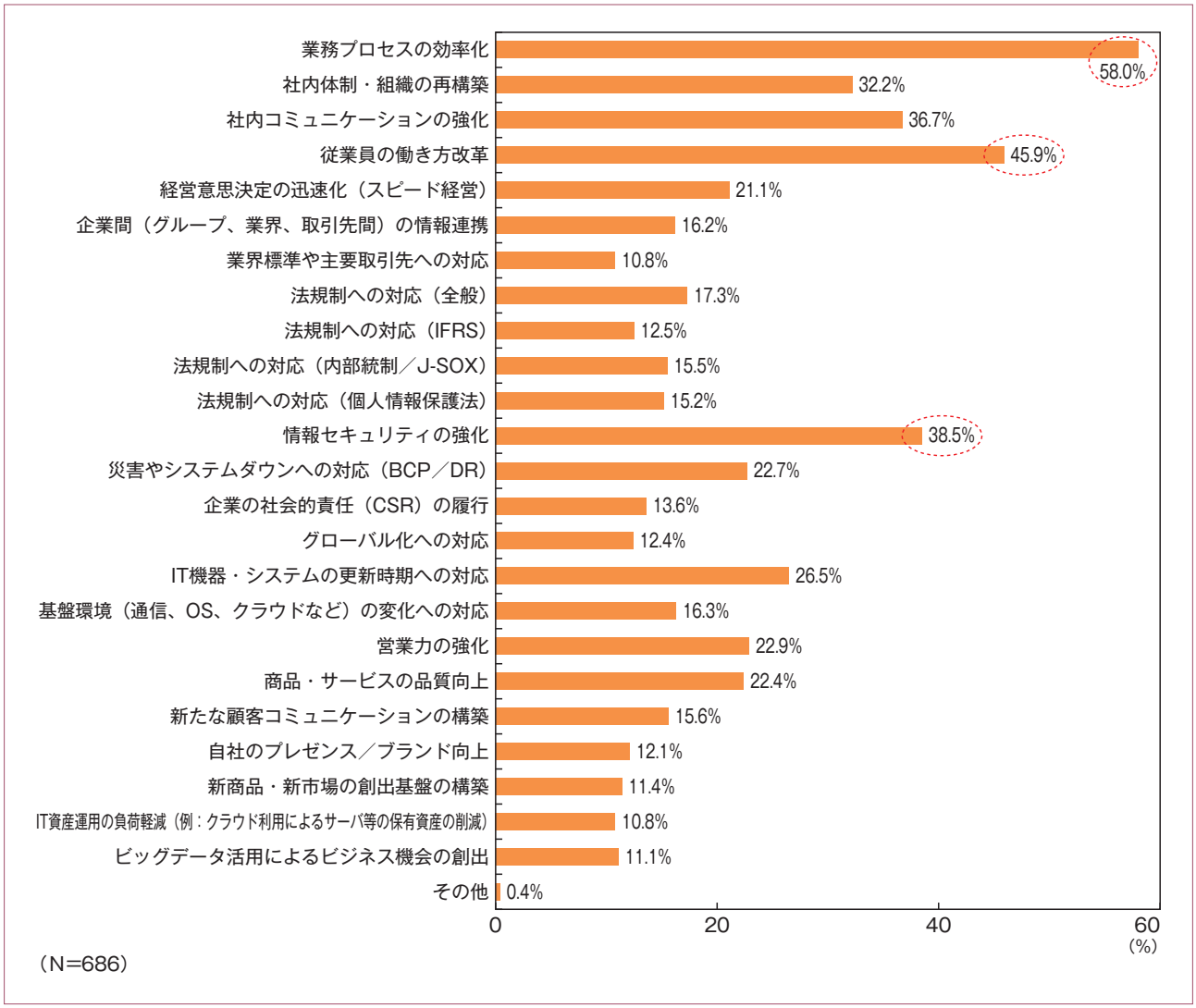


図1. 今後重視したい経営課題(複数回答)

過去3年間で比較すると、「従業員の働き方改革」への意識が2017年調査(35.8%)から約10ポイントの大幅増となっており、2018年の「働き方改革法」の成立を受け、意識が高まっていることがわかる。また、2014年調査以降減少傾向にあった「社内体制・組織の再構築」「社内コミュニケーションの強化」がそれぞれ前年調査より約5ポイント上昇した(図2)。

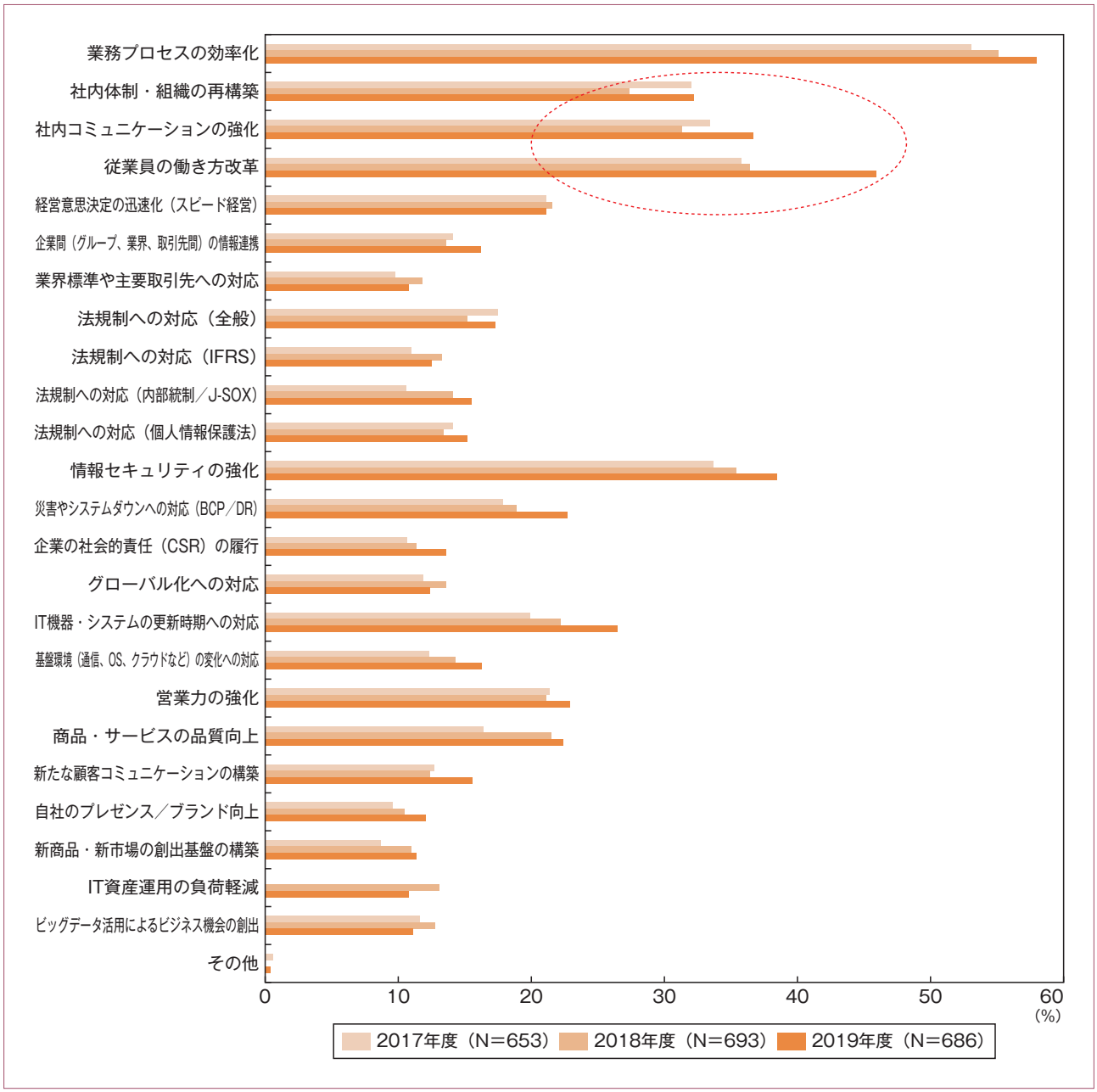


図２．主要経営課題に対する選択率（2017～2019年調査）

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で最も認知率が高かったのは「スマートフォン、携帯電話、タブレットの紛失・盗難」（26.1％）で、前回調査から６ポイント増となった。次いで「従業員によるデータ、情報機器の紛失・盗難」（24.1％）で、ともに紛失・盗難のインシデントであった。

過去３年間の経年変化に注目すると、「外部からのなりすましメールの受信」（10.7％→15.9％→17.8％）や「Webサイトへの不正アクセス」（8.7％→9.8％→13.1％）が目立って増加傾向にある。一方、前回調査で１位だった「社内PCのマルウェア感染」は減少している（27.3％→23.5％）。

これは、最近のサイバー攻撃が単純なバラマキ型の攻撃から複雑かつ巧妙な標的型攻撃やビジネスメール詐欺に移行しつつあることを裏付けていると考えられる（図３）。

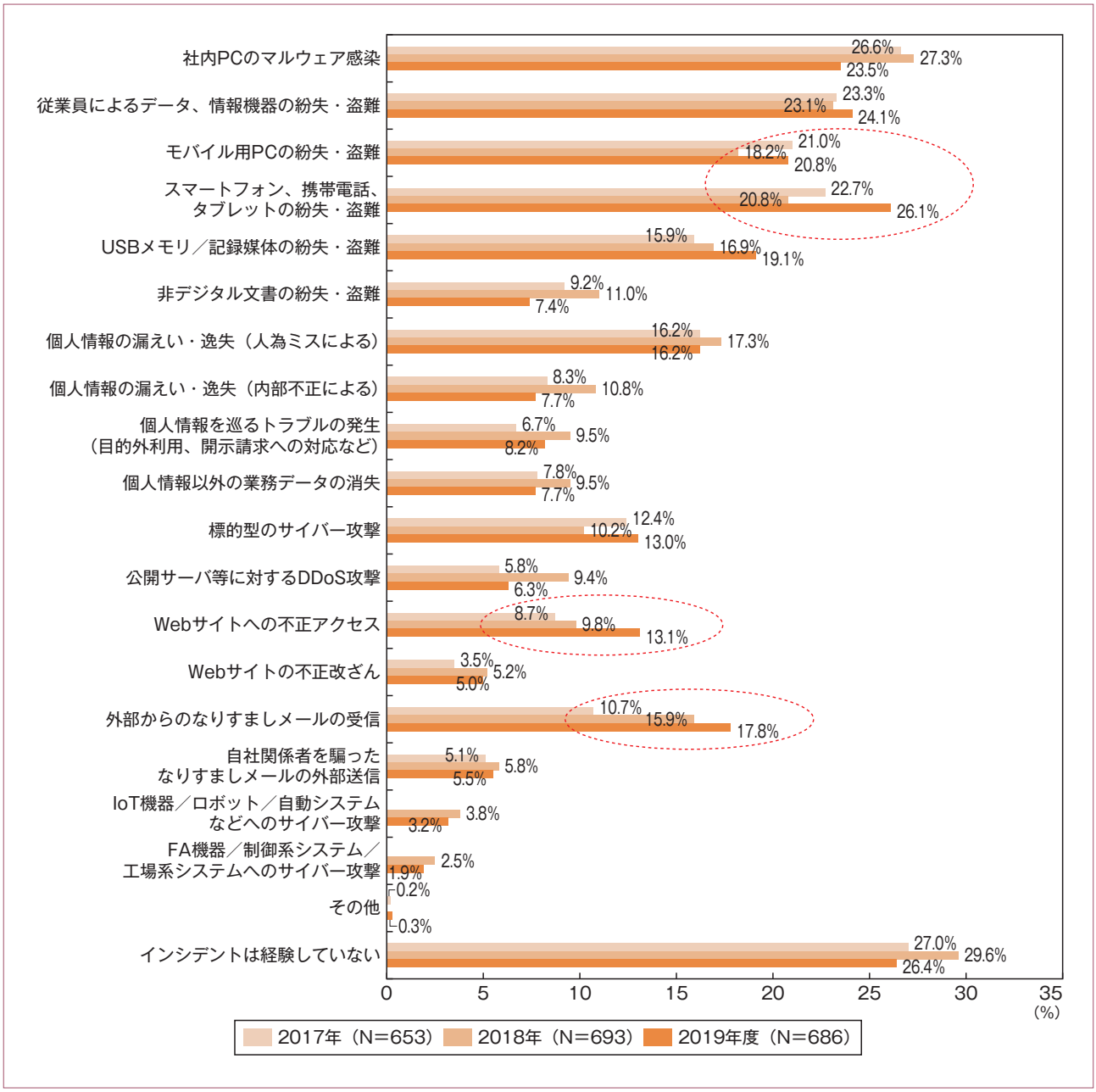


図３．セキュリティインシデント認知率（2017～2019年比較）

2-3. セキュリティリスクの重視度合い

本調査において、「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定点観測しているが、それぞれ「経営陣から最優先で対応するよう求められている」とした回答が約３割となっており、前回調査と同様の結果となった（図４）。

標的型サイバー攻撃に対する重視度合いについて業種別でみると、「最優先対応」の割合がいずれも高いのが「金融・保険」（50.0％）「卸売・小売」（43.8％）、さらに「重視しており、優先度が高い」までを含めれば８割前後を占めており、対応優先度の高いリスクとして認識されていることがわかる。また、従業員規模別にみると、5,000人以上の大企業での重視度合いが高い。

内部犯行による重要情報漏えい・消失に対する重視度合いについても、業種別、規模別ともに、同様の結果となった。

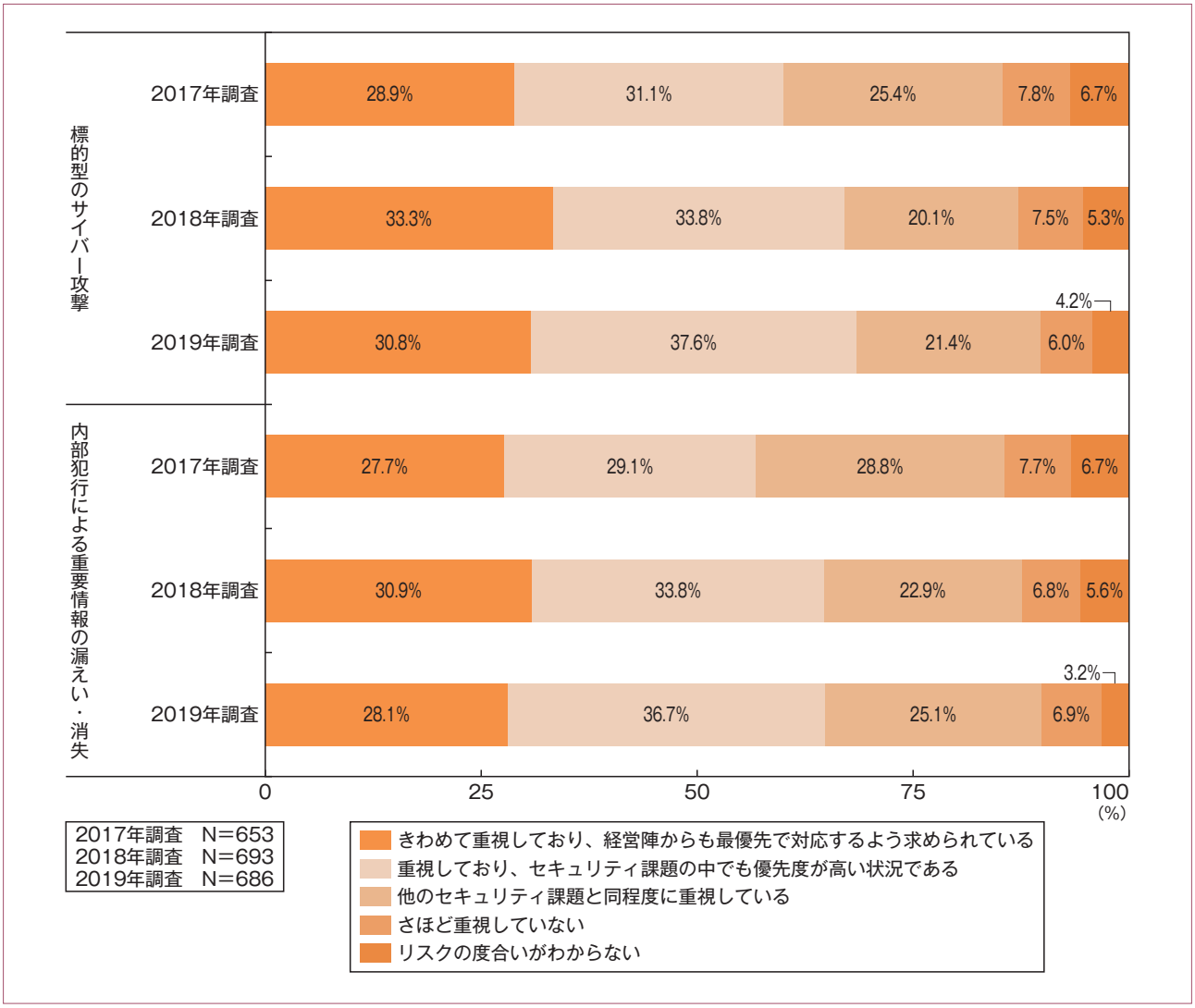


図4．セキュリティリスクの重視度合い（2017～2019年比較）

2-4. セキュリティ対策の実施状況

では、具体的なセキュリティ対策の実施状況はどのようになっているのか。ここでは「標的型のサイバー攻撃対策」「内部犯行対策」それぞれ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観測している。

「標的型サイバー攻撃対策」として最も実施率が高かったのが「PCの管理者権限の制御」（56.1％）、次いで昨年1位だった「重要システムのインターネットからの隔離」（55.0％）が続いた。また、今後の実施予定が高いのは「IoT／FA／制御システムへのセキュリティ対策」（28.7％）「CSIRTの立ち上げ」（27.5％）「インシデント発生時の対応手順の明確化」（26.5％）であった（図5）。

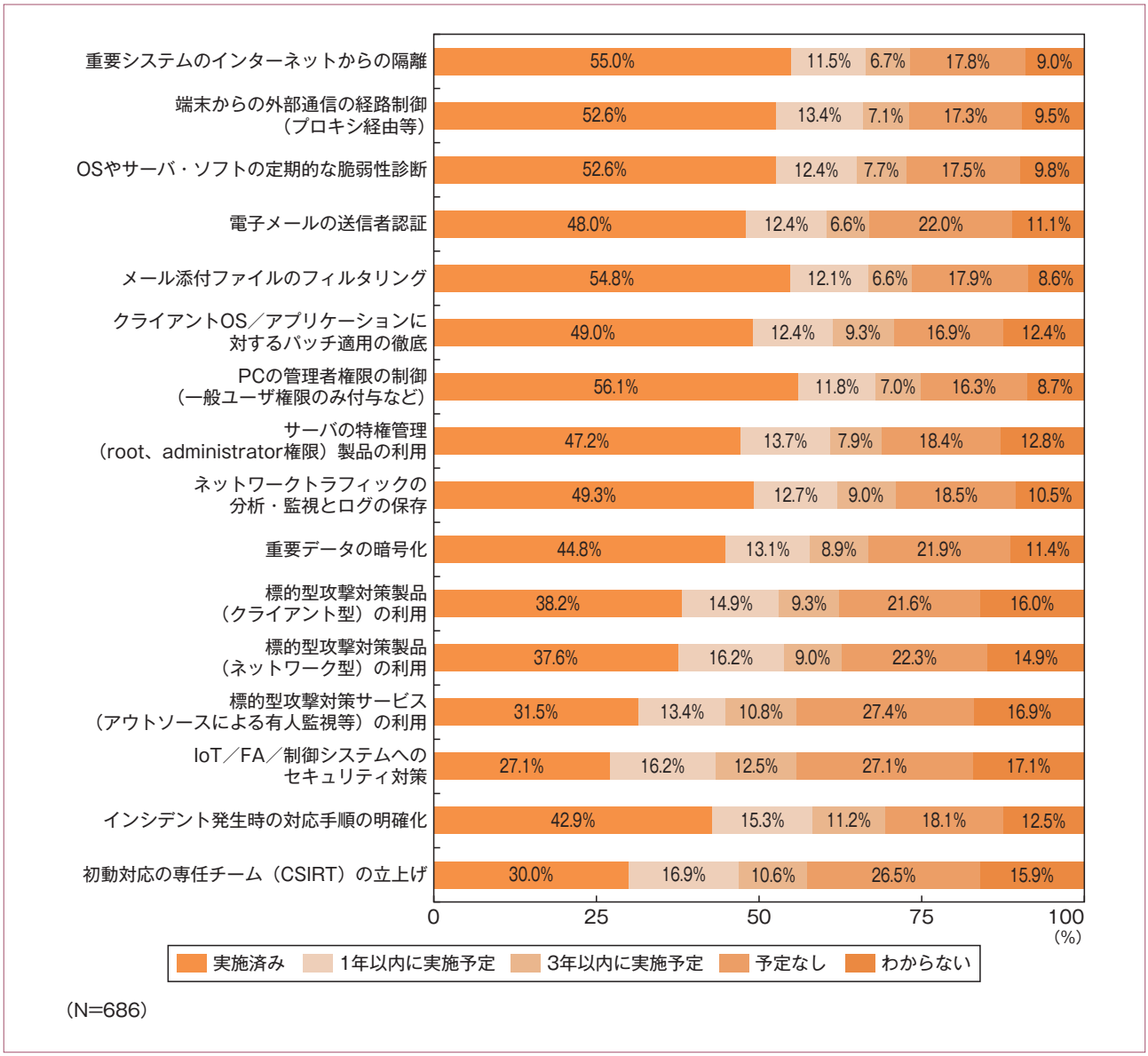
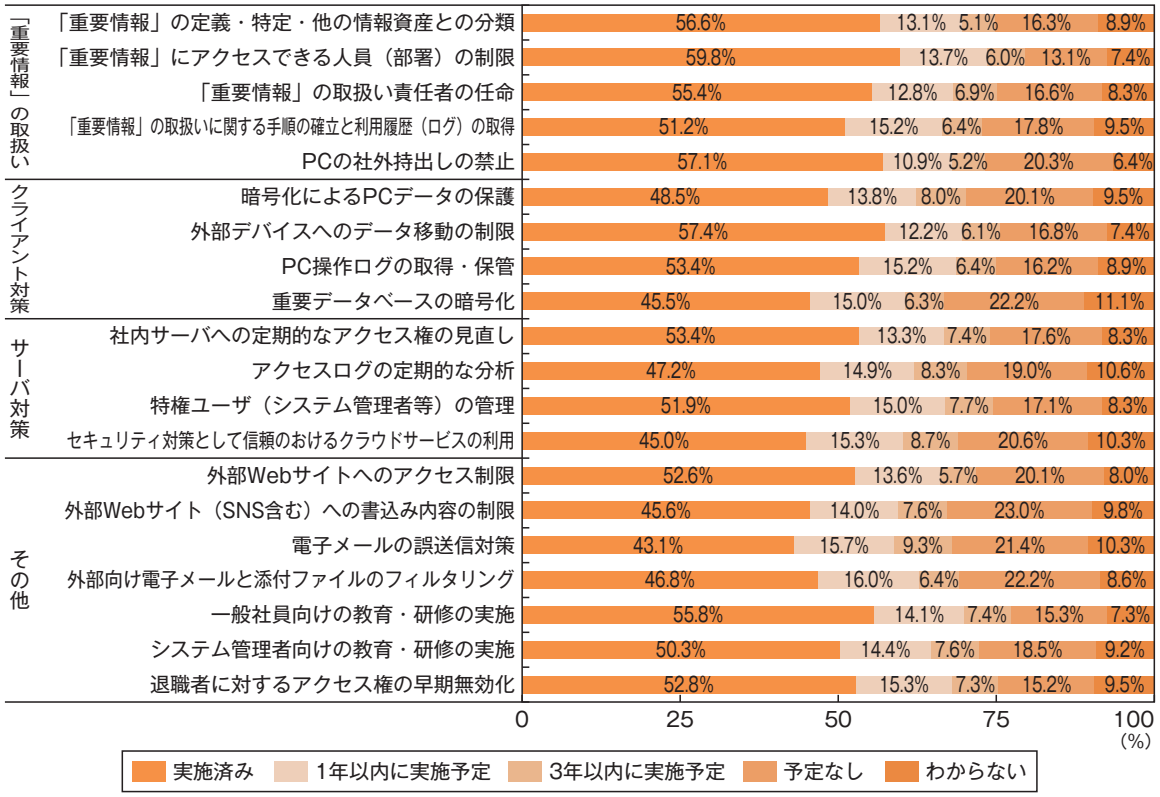


図５．主要な「標的型サイバー攻撃対策」の実施状況

一方、「内部犯行対策」としては、前回調査に続き「重要情報にアクセスできる人員（部署）の制限」（59.8％）の実施率が最も高く、「外部デバイスへのデータ移動の制限」（57.4％）が続いている（図６）。

また、「一般社員向けの教育・研修の実施」は、実施済は他の対策と大差はなかったが、今後１～３年以内の実施予定と合わせると、「重要情報へのアクセス制限」に続き高い結果となった。

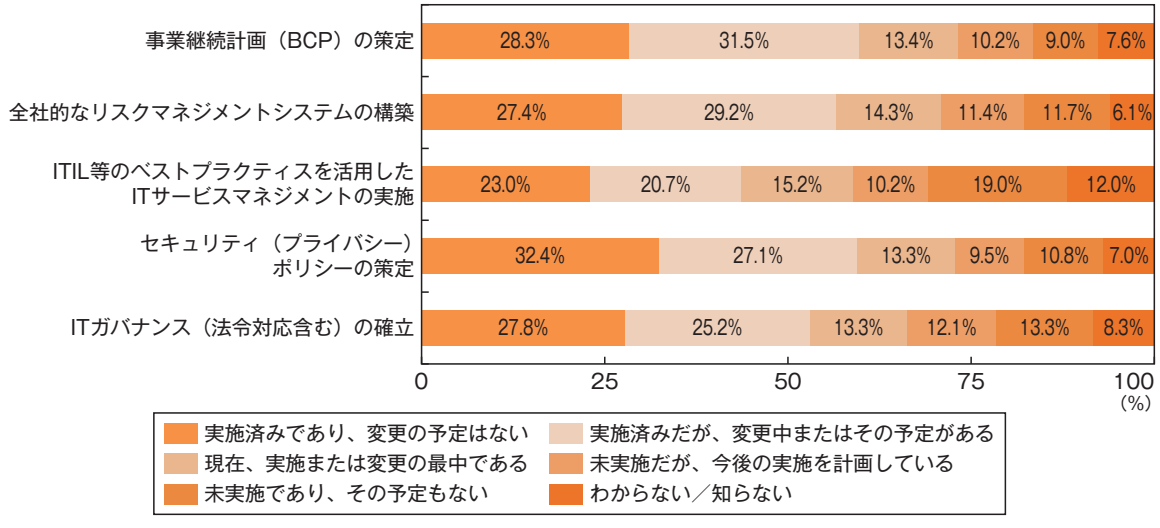


(N=686)

図6．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は、前回調査同様、「BCPの策定」「リスクマネジメントの構築」および「セキュリティポリシーの策定」の実施済が約６割となった。一方、「ITサービスマネジメントの実施」は実施済が約４割、予定なし・わからないが約３割であり、他の項目と比較して低い結果となった（図７）。



(N=686)

図7．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

セキュリティ支出の増減動向について、主要な支出内訳として15項目を取り上げ、それぞれについて2019年度の支出の増減見込み（対前年度比）を調査した。

「増加する見込み」と回答した企業の割合は、全項目とも15％を越えており、最も数値が大きかったのは「セキュリティ関連の認証取得に関する費用」（27.4％）となった。過去調査と比較するとほとんどの対策費用は「横ばい」で５割を占めている（図８）。なお、大きく変化があったのは「セキュリティ製品の利用・購入費（外部攻撃対策）」で、2017年調査時まで増加傾向にあったのが、前回調査で減少し、今回もほとんど差は見られなかった。これは、新たなサイバー攻撃対策費用の投入のピークが過ぎ、ある程度体制が整ったとも思われる。

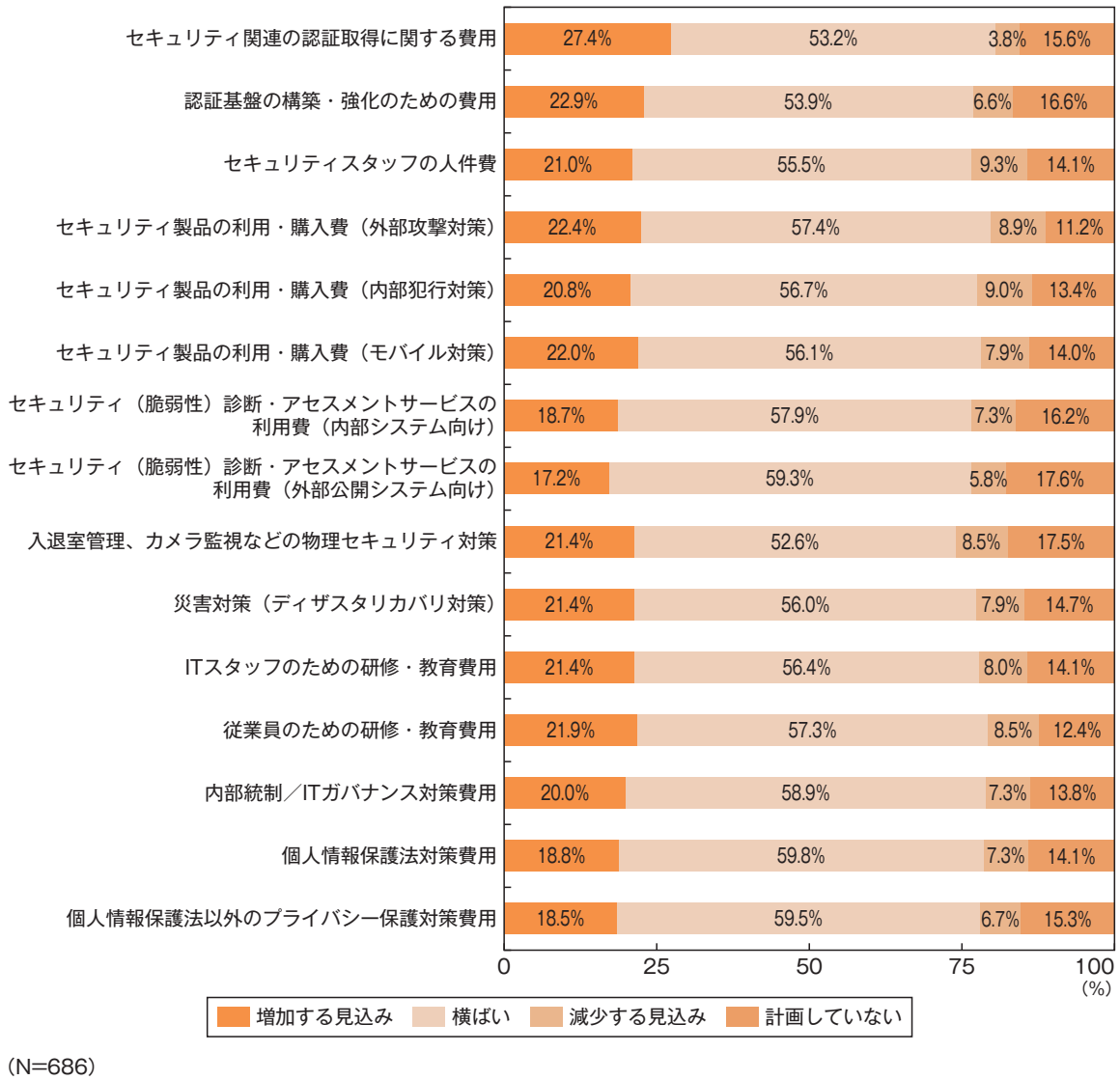


図8. 2019年度に想定されるセキュリティ支出の増減傾向

なお、「外部攻撃対策費用」を前回調査と企業規模別に比較すると、大企業ほど支出増加を見込んでいるのに対し、中小規模事業者の見込みは横ばいもしくは減少傾向にあることがわかった（図９）。

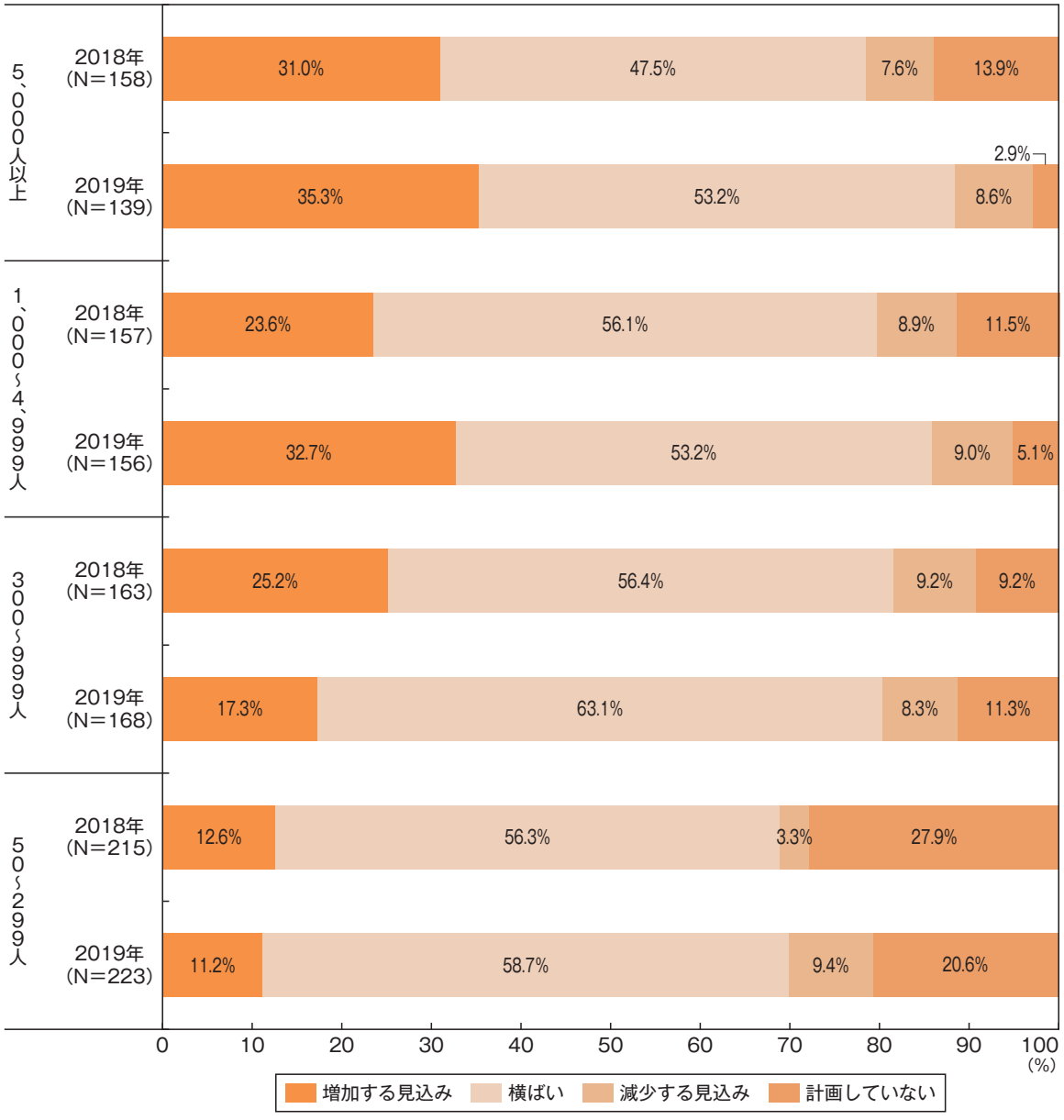


図９．企業規模別にみる外部攻撃対策委費用の増減傾向（2018～2019年比較）

3　情報セキュリティに関する認定／認証制度に対する意識

システムリスクの軽減策として「リスクマネジメントの構築」や「セキュリティポリシーの策定」があげられるが、リスク軽減強化策として主要なセキュリティ関連の認定／認証制度の取得がある。認定／認証を取得する目的には顧客が取引先から信頼を得ることも大きい。ここでは、情報セキュリティ関連の認定／認証制度に対する意識度合いを調査した。

3-1. 情報セキュリティに関する認定／認証制度の取組み状況

情報セキュリティの認定／認証制度の取組み状況については、「プライバシーマーク」と「ISMS」は取得済が約４割で、予定を含めると５割を超えている。一方、他の制度では「取得済」が約３割、「予定」を含めて４割強と、やや低い傾向にある（図10）。

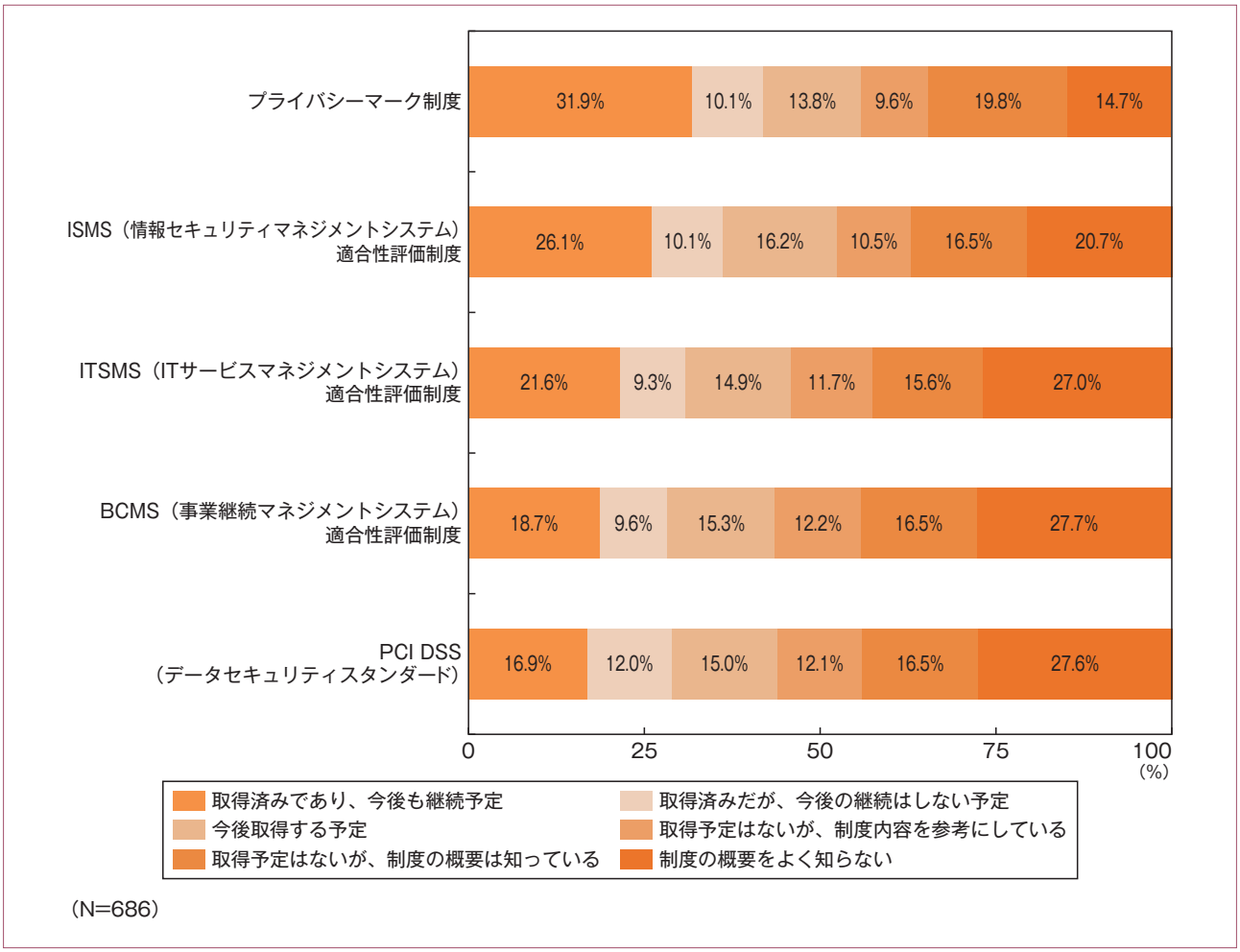


図10. 情報セキュリティの認定／認証制度への取組み

3-2. 認定／認証を取得する価値

2-6で示したとおり、セキュリティ関連認証取得費用の支出増加見込みは経年でみると割合自体は減少傾向にあった（2017年27.0％→2018年23.5％）が、今回、過去調査でも最も高い数値（27.4％）となった。理由としては、個人情報保護、セキュリティに関するニュースが多く取り上げられる中、消費者や取引先からの信頼を得るための根拠として、第三者認証の必要性が高まってきたと考えることができる。

では、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。

第三者から認定／認証を取得することの価値（効果）としては、「取引先から信頼を得るため」（59.3％）が最も多く、次に「社内の情報セキュリティ体制を高度化させるため」（44.0％）、「消費者からの信頼を得るため」（39.4％）が続いた（図11）。

なお、前回調査と比べ大きく変化がみられたのは「情報セキュリティ体制の高度化」と「コンプライアンスのため」で、それぞれ約７ポイントの増加となった。

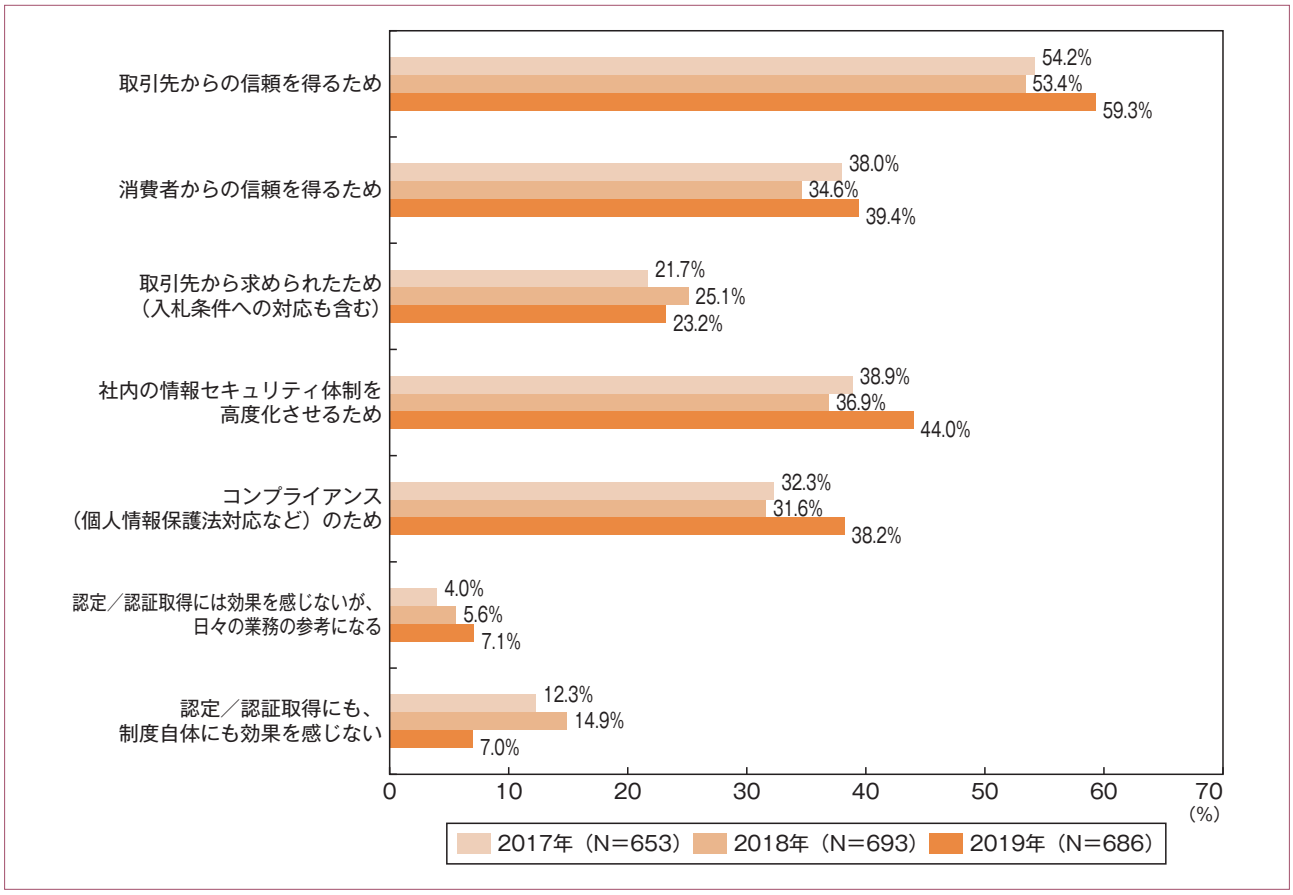


図11. 第三者から認定／認証を取得することの価値（効果）（2017～2019年比較）

次に、第三者認定／認証取得の有無により、どういう点に価値があると考えられているか、を比較した。

取得済み企業の場合、「取引先からの信頼を得るため」が約72％と、他と比べ突出して高くなっている。これは各種認定／認証取得により社内の取組みに対する適正管理が可視化され、取引先からの信頼確保に効果があったと受け止められた結果と考えられる。次に「社内の情報セキュリティ体制を高度化させるため」（48.9％）「消費者からの信頼を得るため」（46.0％）「コンプライアンス（個人情報保護法対応など）のため」（45.2％）が続いた。

一方、未取得企業についても取得済企業と同じ順位となったが、特に「取引先の信頼を得るため」（46.1％）は他と比べ７ポイント以上の差が見られており、認定／認証取得が取引先の信頼確保に効果があると考えられていることがわかる（図12）。

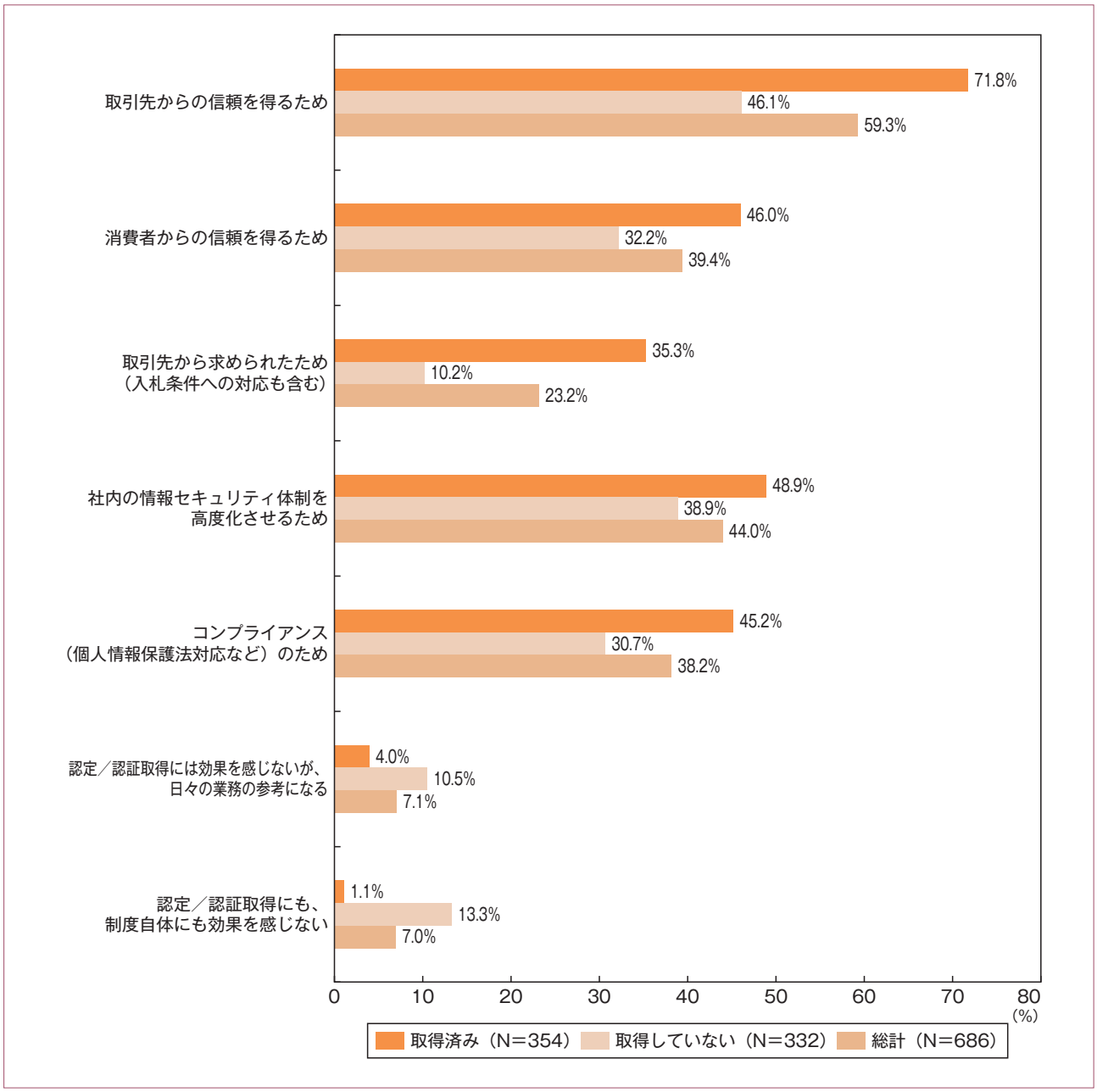


図12. 第三者から認証を取得することの価値（効果）（認定／認証取得の有無別）

4　グローバルセキュリティガバナンス

国内では2017年に個人情報保護法の改正とそれに対応したJIS Q15001の改正があった。またEUでは2018年５月に一般データ保護規則（GDPR）が施行されるなど、ここ数年の間に、グローバルにデータを流通・利用・保護するためのセキュリティ（プライバシー）法規制が整備されつつあり、日本企業もグローバルでのセキュリティガバナンスを確立しなければならない時期を迎えている。そのような状況において、日本企業の取組みは、まだ十分ではない状況が見えてきている。

4-1. 改正個人情報保護法およびJIS Q15001改正内容の関心事項

改正個人情報保護法と、それを受けたJIS Q15001の改正についての関心事項については、「個人識別符号の定義と範囲、取扱い」（39.9％）が最も高く、「要配慮個人情報の定義と範囲、取扱い」（30.5％）が続き、「匿名加工情報の定義と範囲、取扱い」（27.0％）は３位となった。マイナンバーをはじめとする個人を特定可能な識別符号は多く存在しており、該当の有無についての関心が高くなっていると思われる（図13）。直近３年の調査結果をみても「個人識別符号」への関心が高いことがわかる。

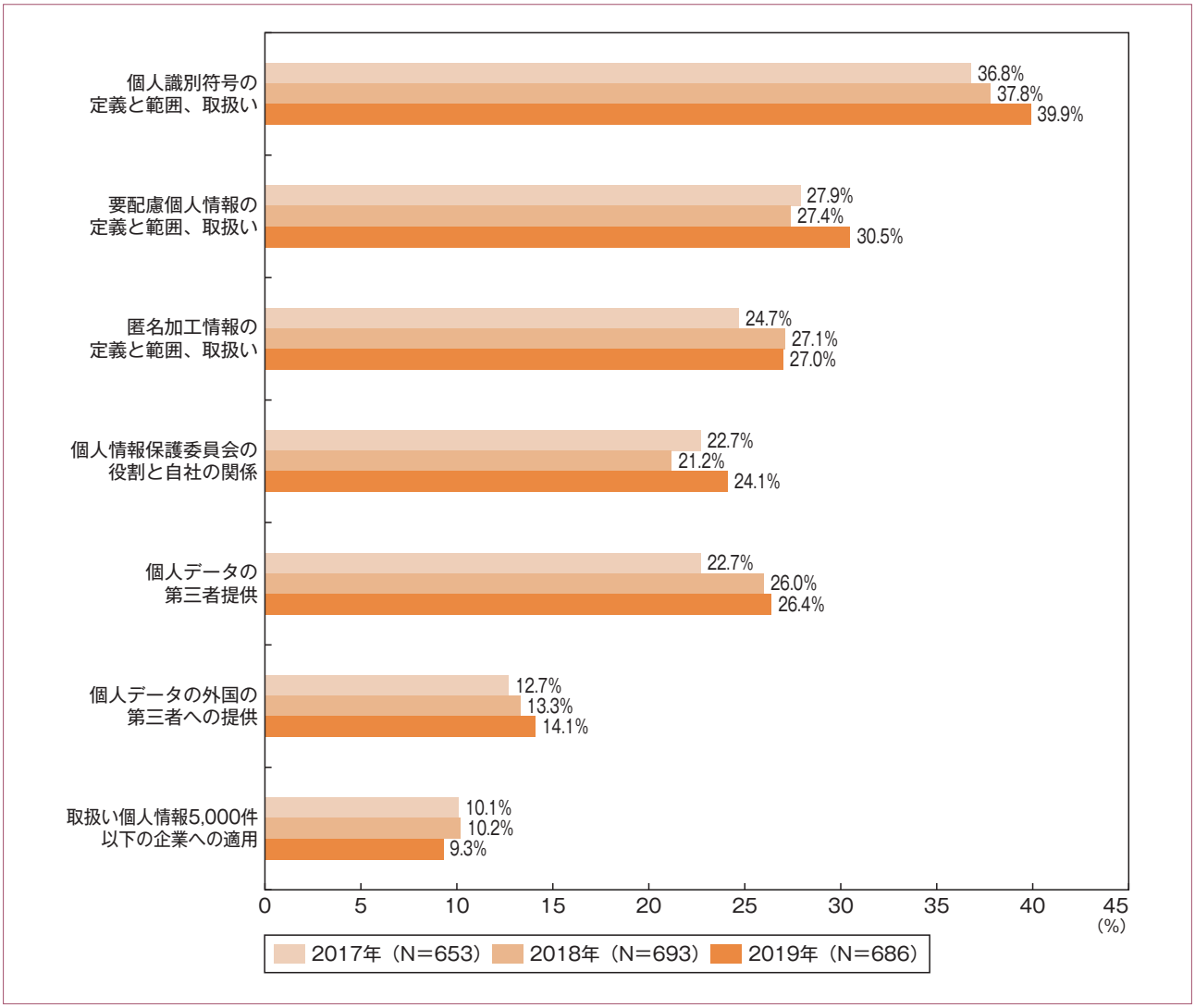


図13. 個人情報保護法およびJIS Q 15001の改正内容についての関心事項（2017～2019年比較）

4-2. 海外のプライバシー規制の認知度

各国で制定されているプライバシー規制の認知度について調べたところ、2018年５月に施行されたGDPRの認知度が約５割と最も高かったのに対し、その他のCBPR（APEC）、サイバーセキュリティ法（中国）、消費者プライバシー法（米国カリフォルニア州）の認知度は約３割にとどまっている（図14）。

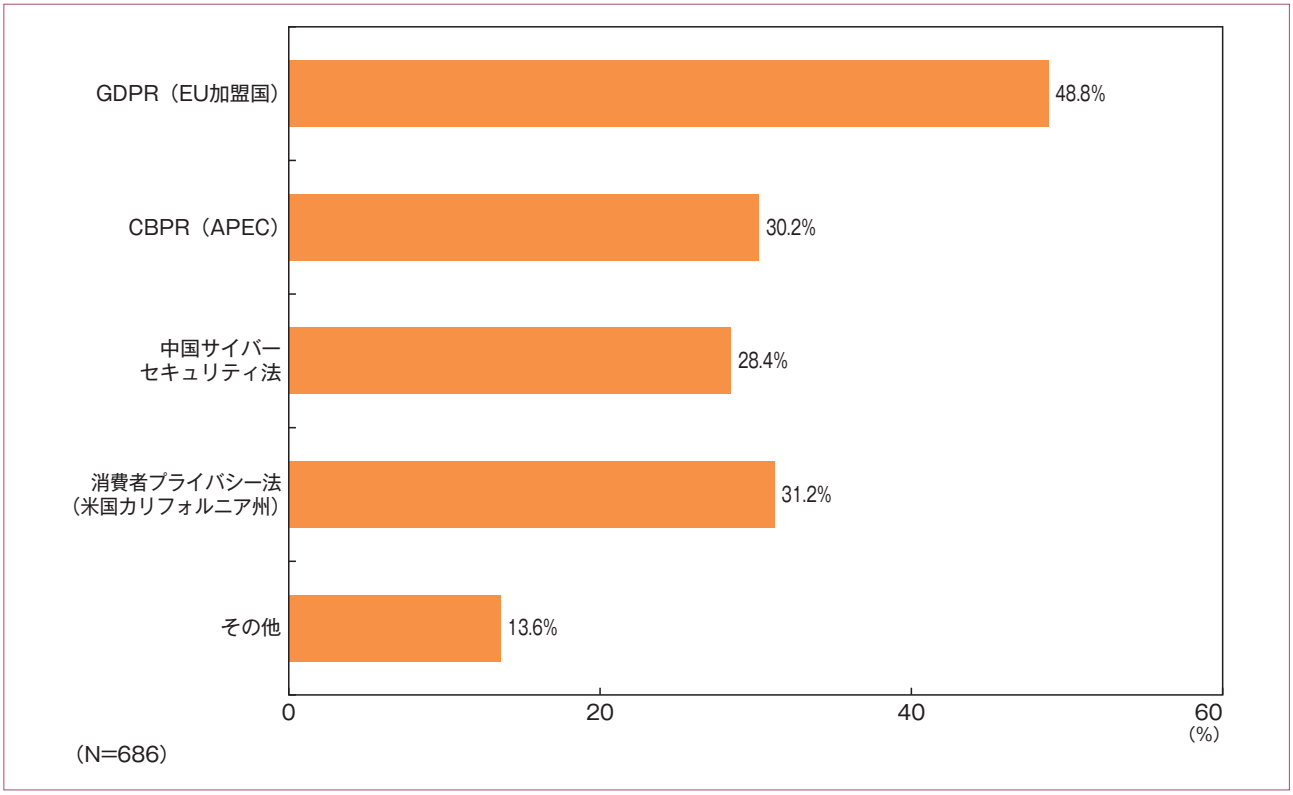


図14. 海外のプライバシー規制の認知度

4-3. GDPRの対応状況（施行前と施行後の対比）

EUにビジネス拠点または顧客を持つ企業に対し、GDPRへの対応状況を調査した。GDPRに対する認知度が高まっていることもあり、「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」が前回調査（2018年１月／施行前）の26.1％から34.4％へと約８ポイント増加した。一方、「何も対応していない」と「気にすることなく移転を行っている」については、前回調査よりも減少はしているが、３割強がいまだに未対応となった（図15）。

なお、本調査実施中の2019年１月下旬に日本とEU間における十分性認定の合意成立により、日－EU間での個人データ移転に際し、十分なデータ保護水準が保たれていることが認められ、個人データの移動が可能となったことから、国内企業にとって対応のハードルは下がったともいえる。ただし、EU側が条件とする「定期的な監査」により、日本側の保護水準に疑問が生じた場合、十分性認定撤回のリスクも残っていることから、該当の企業においては、今後もGDPR対応は重大な課題であり続けるといえよう。

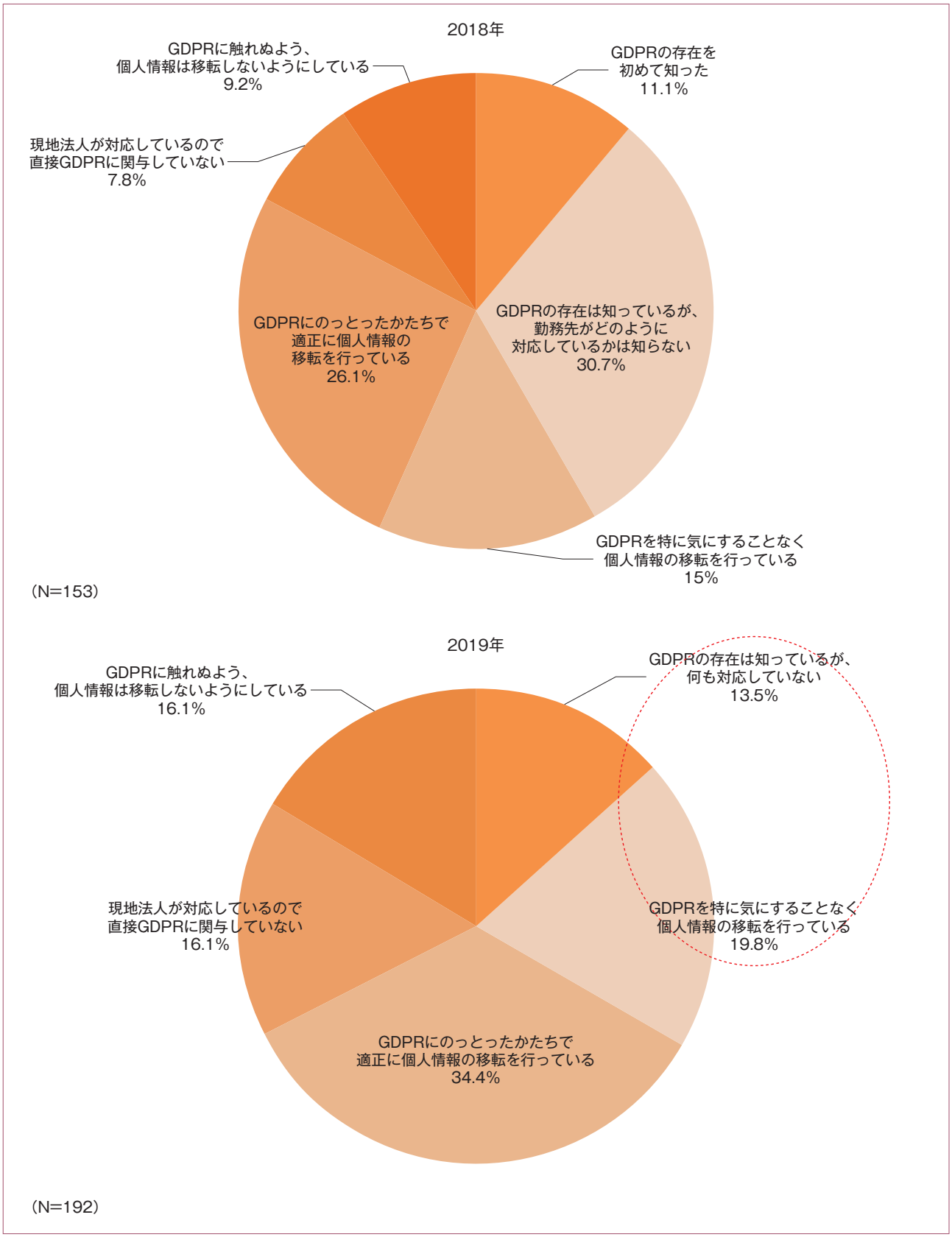


図15. GDPRの対応状況

5　セキュリティ製品／技術の利用動向

サイバー攻撃の巧妙化／複雑化とクラウド化の進行によって、対応するセキュリティ製品／技術も進化している。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調査した。調査結果から、実際の利用状況としては、新しい製品／技術の採用はまだ進んでいないことがわかった。

5-1. ネットワークセキュリティ製品の利用状況

ネットワーク系のセキュリティ製品は、これまで社内ネットワークとインターネットを隔てるファイアウォールや、インターネットから社内ネットワークに入るためのVPNが主流であったが、社内システムのクラウド環境への移行によってクラウドサービスへのアクセスを制御するCASB（Cloud Access Security Broker）のような新しいセキュリティ製品が登場してきている。ただし、今回の調査結果では、CASB（24.2%）よりも、いまだ現行のファイアウォール（79.7%）やVPN（56.0%）利用の方が多い、という結果となった（図16）。

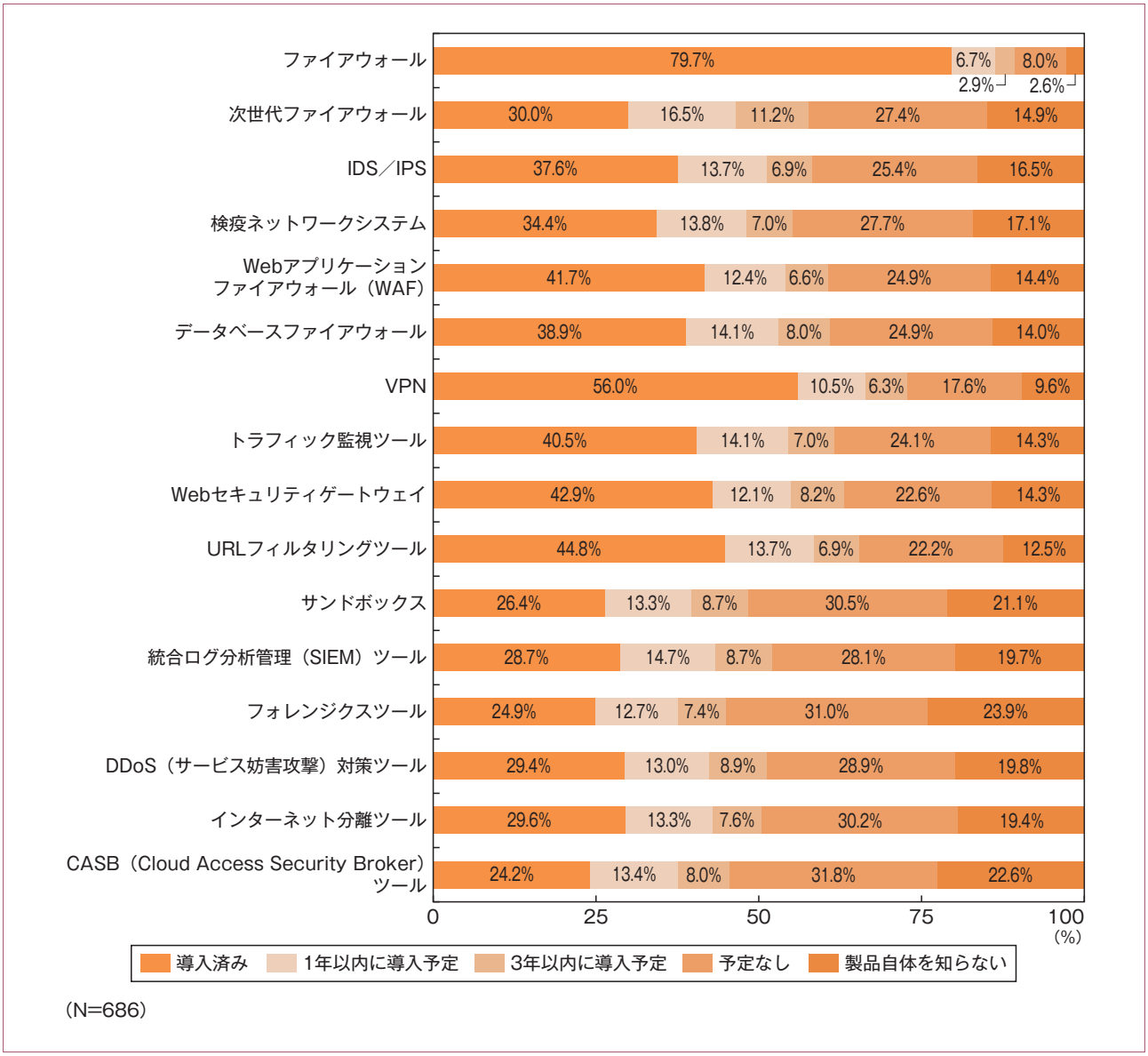


図16.　ネットワークセキュリティ製品の利用状況

企業規模別にみると、既存ネットワークセキュリティ製品の代表であるファイアウォールが中小規模から大規模までまんべんなく導入されているのに対し、次世代型ネットワークセキュリティ製品の代表であるCASBは企業規模別での導入に大きな差が出ており、大企業ほど新しいセキュリティ製品の導入に積極的であることがわかる（図17）。

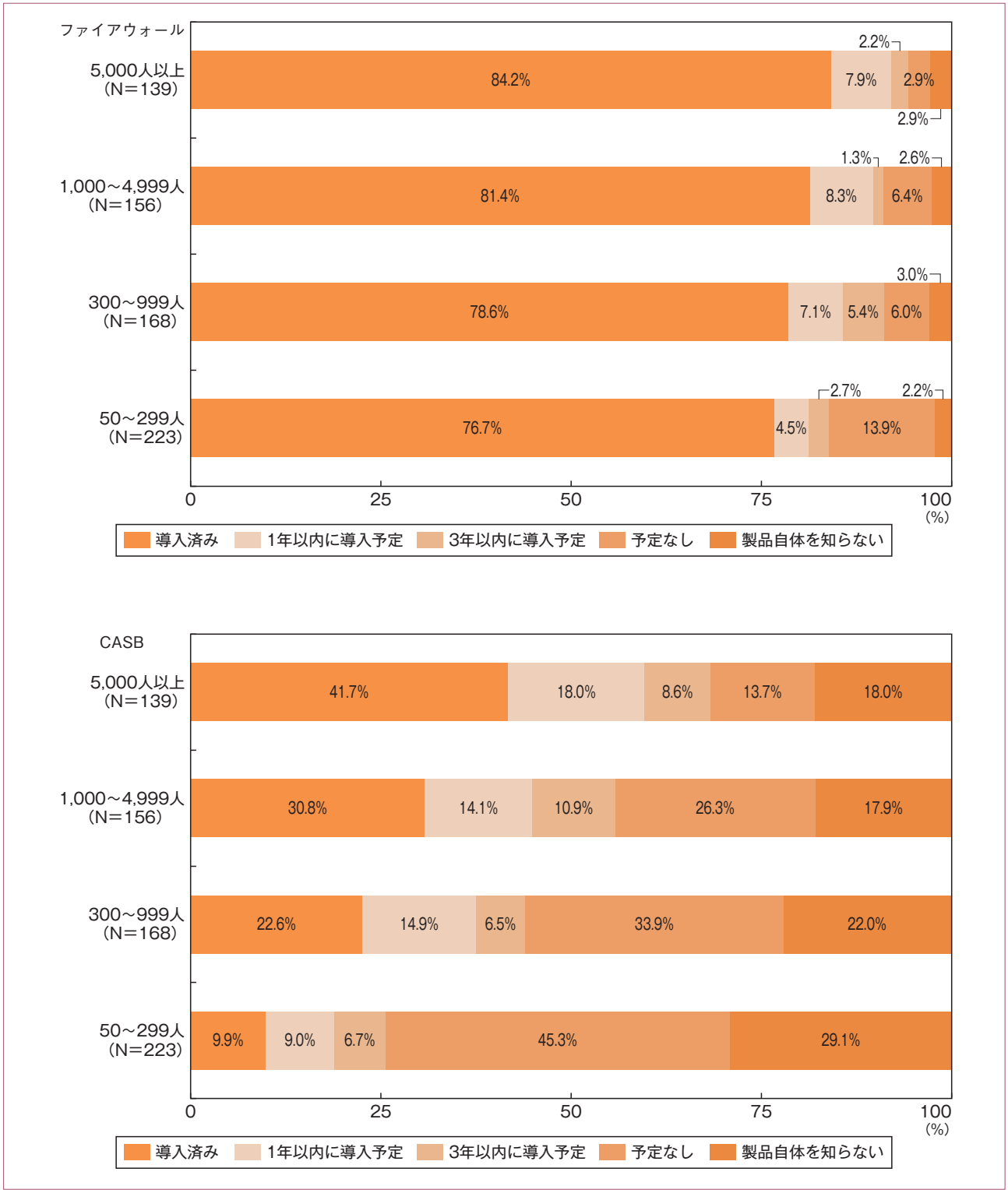


図17. ネットワークセキュリティ製品の利用状況（企業規模別）

5-2. エンドポイントセキュリティ製品の利用状況

エンドポイント（クライアント）系のセキュリティ製品についても、従来はウイルス対策ソフトが中心だったが、標的型攻撃やランサムウェアのような巧妙かつ複雑な攻撃に対応するため、振舞いや兆候の段階から検知して対応するEDR（Endpoint Detection and Response）やUEBA（User and Entity Behavior Analytics）等の次世代型のエンドポイントセキュリティ製品が登場してきている。しかし、実際の導入状況では現行のウイルス対策ソフト（79.4%）が中心であり、次世代型のEDRツール（27.1%）やUEBAツール（21.9%）の導入状況の割合は高くない（図18）。

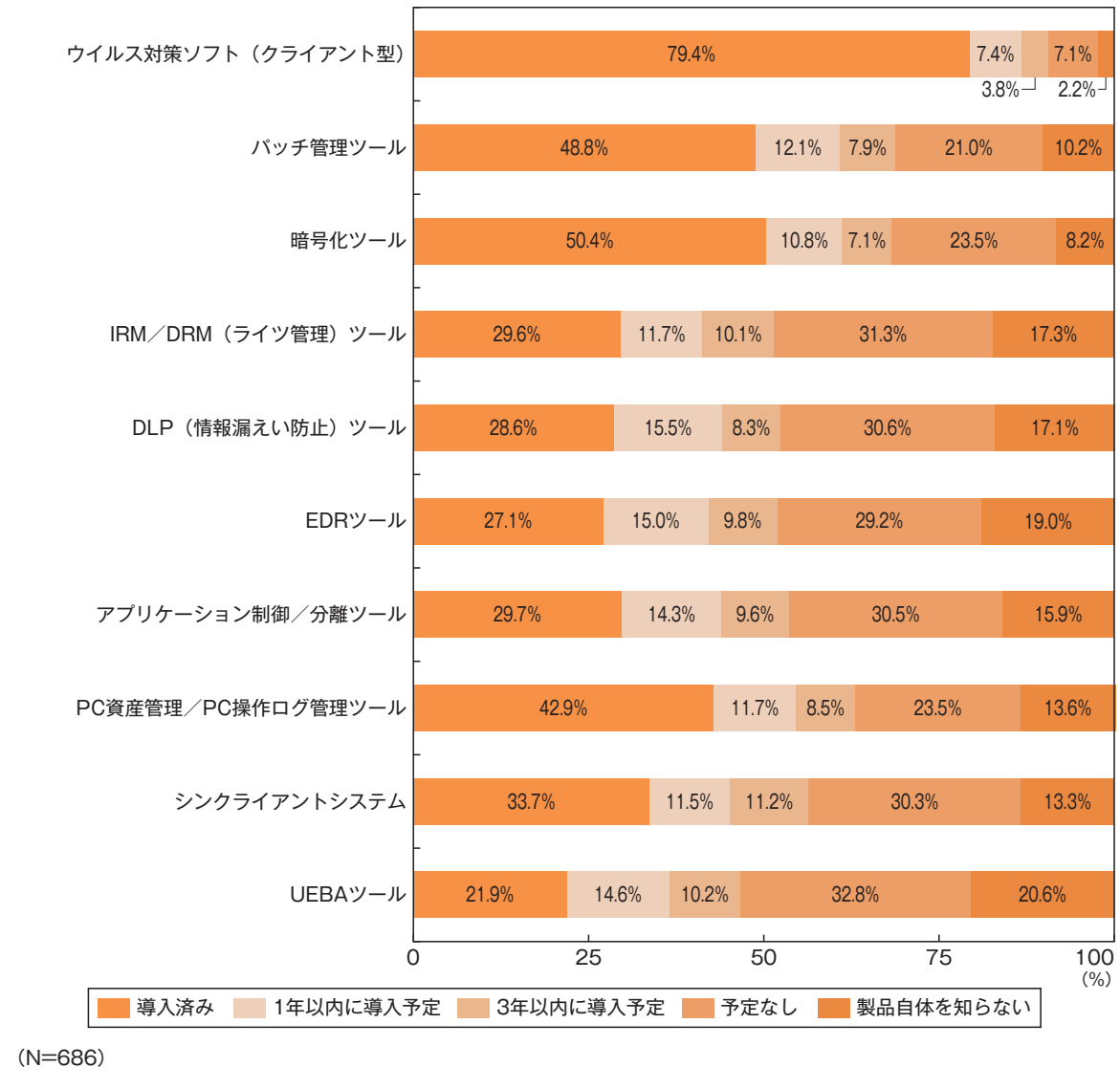


図18. エンドポイントセキュリティ製品の利用状況

企業規模別にみると、既存のエンドポイントセキュリティ製品の代表であるマルウェア対策ソフトが中小規模から大企業までまんべんなく導入されているのに対し、次世代型エンドポイントセキュリティ製品の代表であるEDRは企業規模によって導入状況に大きな差があり、大企業では約５割で導入されているのに対し、中小企業では１割程度であった（図19）。

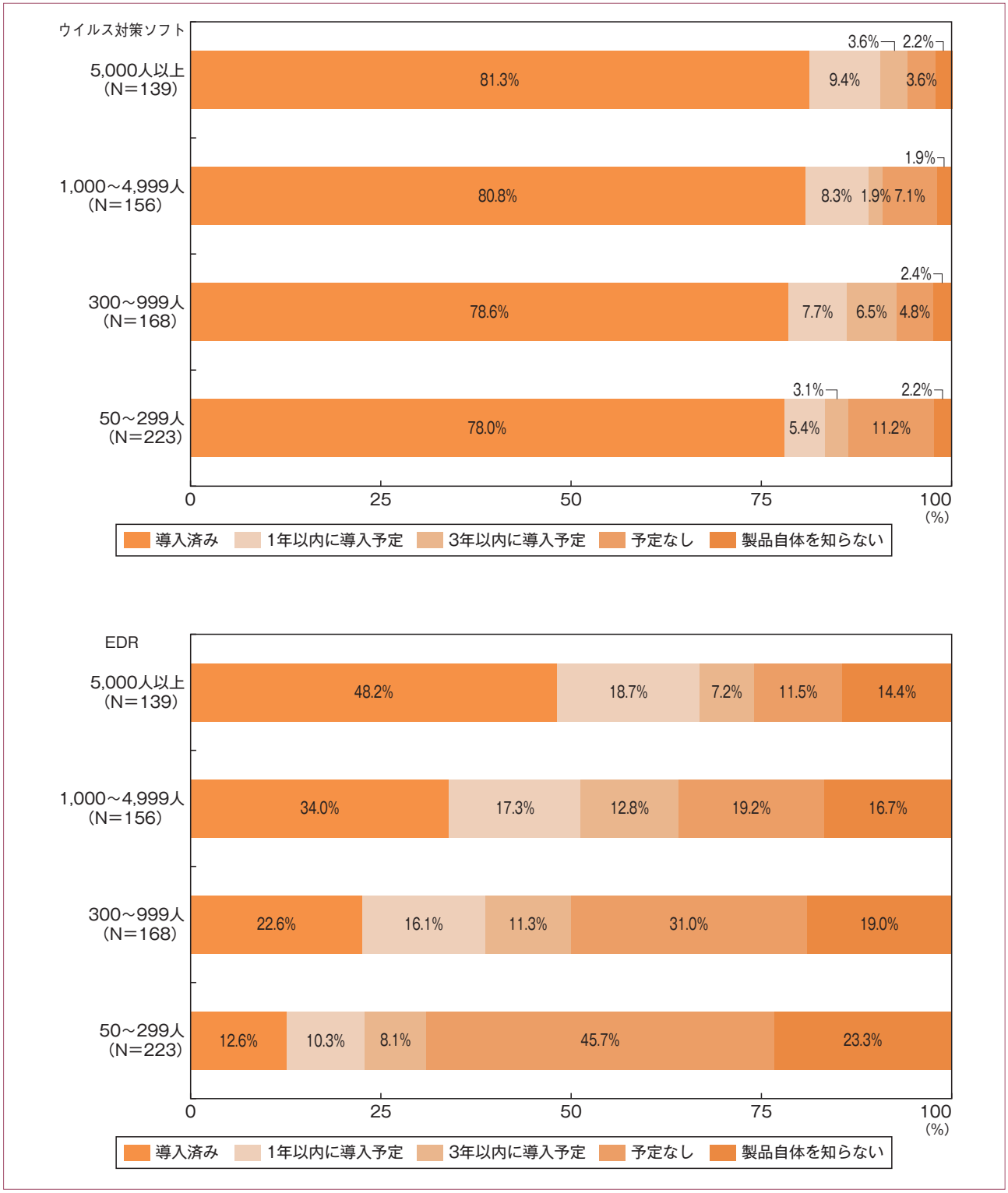


図19. エンドポイントセキュリティ製品の利用状況（企業規模別）

5-3. 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について、「導入済」が最も多かったのは脆弱性診断サービスと証明書サービスだったが、他にもWebサーバ攻撃対策サービスの導入率が高い。セキュリティ運用の外部アウトソーシングであるセキュリティオペレーションセンターの利用やサイバー攻撃の損害を補填するサイバー保険については約３割の導入率となった（図20）。

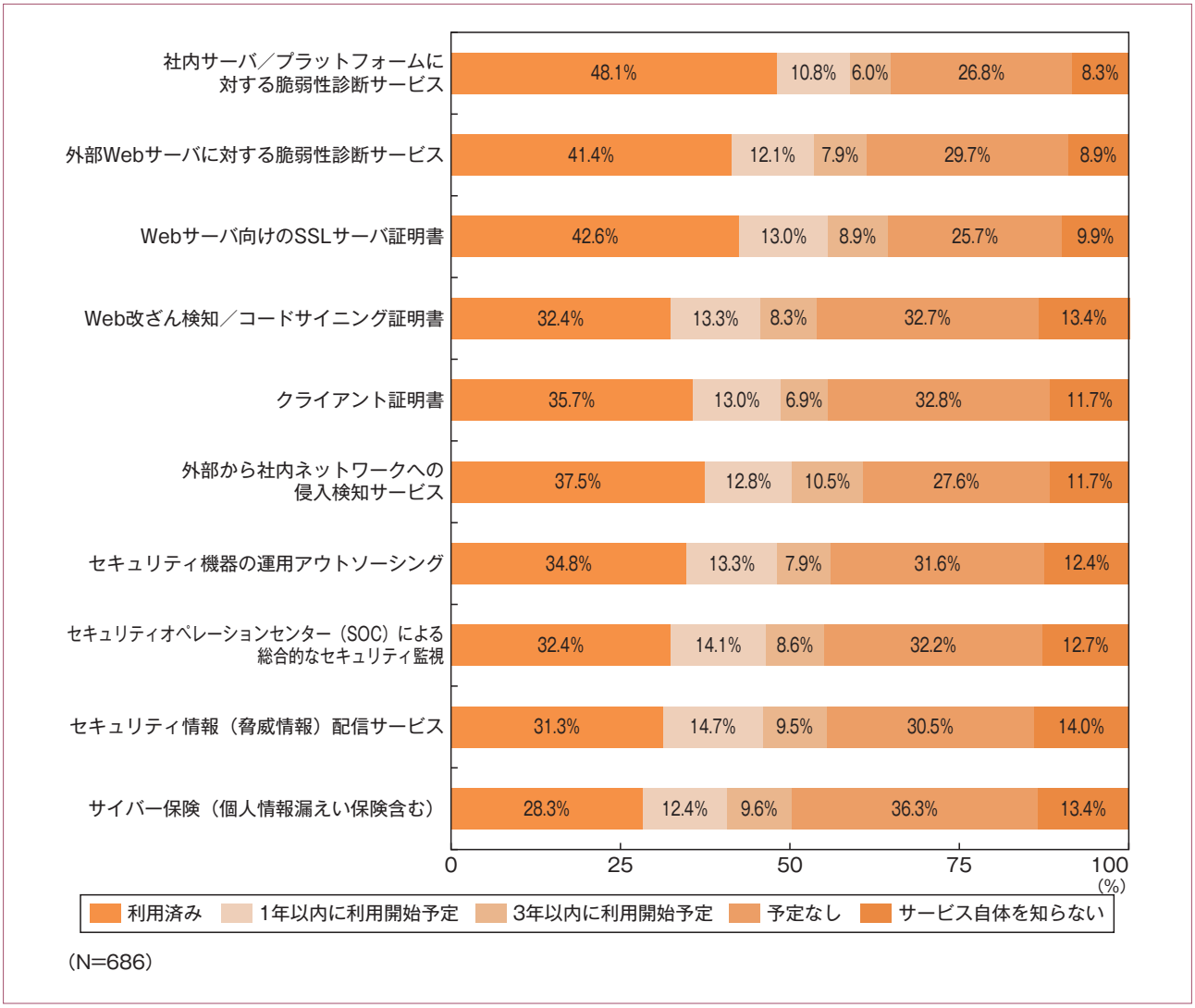
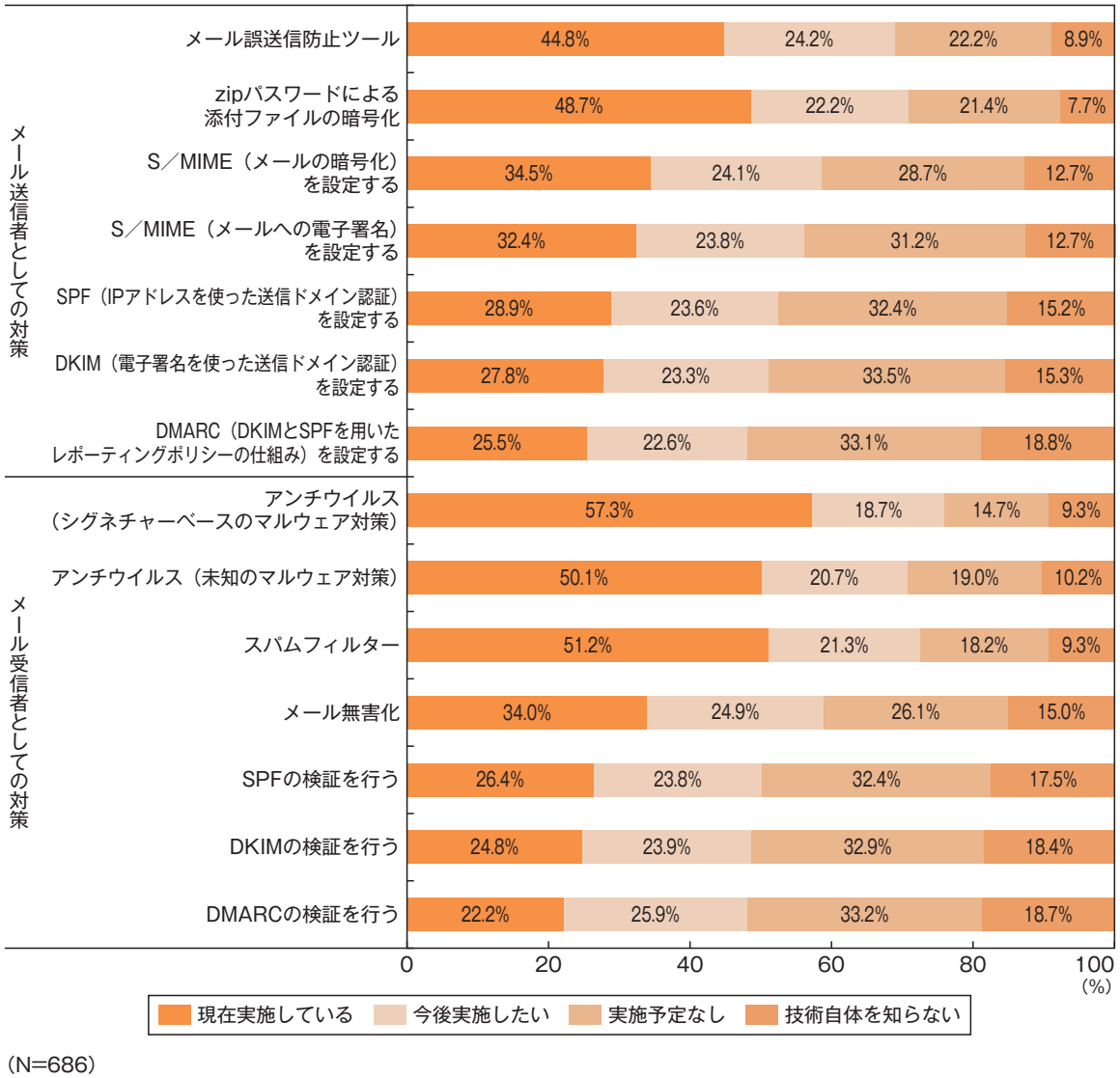


図20. セキュリティサービスの利用状況

5-4. 電子メールのセキュリティ対策の状況

電子メールのセキュリティ対策について、送信側対策では「添付ファイル暗号化」（48.7%）と「メール誤送信防止ツール」（44.8%）が多く、受信側対策としては「アンチウイルス（シグネチャベースのマルウェア対策）」（57.3%）「アンチウイルス（未知のマルウェア対策）」（50.1%）や「スパムフィルター」（51.2%）が多い（図21）。



(N=686)

図21. 電子メールのセキュリティ対策状況

5-5. 総務省パスワード変更不要見解への対応

2018年３月に総務省がパスワード定期変更不要の見解を公表したことを受け、どの程度の企業が定期変更を中止したかを調査した。

この見解公表は米国国立標準技術研究所（NIST）のレポートに基づくものであるが、もともとパスワードは単純な文字の羅列であるため、悪意のある第三者によりパスワードが解読され、不正アクセス被害にあう可能性は高い。これらのリスクを軽減するためには他の認証の仕組みへの変更や複数の認証の組合せ（多要素認証）を行うことが望ましい。ここでは、このような他の認証方式や複数認証の組合せの導入状況もあわせて聞いた。

その結果、定期変更不要の見解公表があったとはいえ、「これまでどおり定期変更を行っている」が５割を超えていた。一方、「他の認証への変更」や「複数認証の組合せに変更」したのが、合わせて13.2％と１割強にとどまっている。パスワードの強度は、これ以上強化されることは不可能であり、複数認証の組合せが広まることが望まれる（図22）。

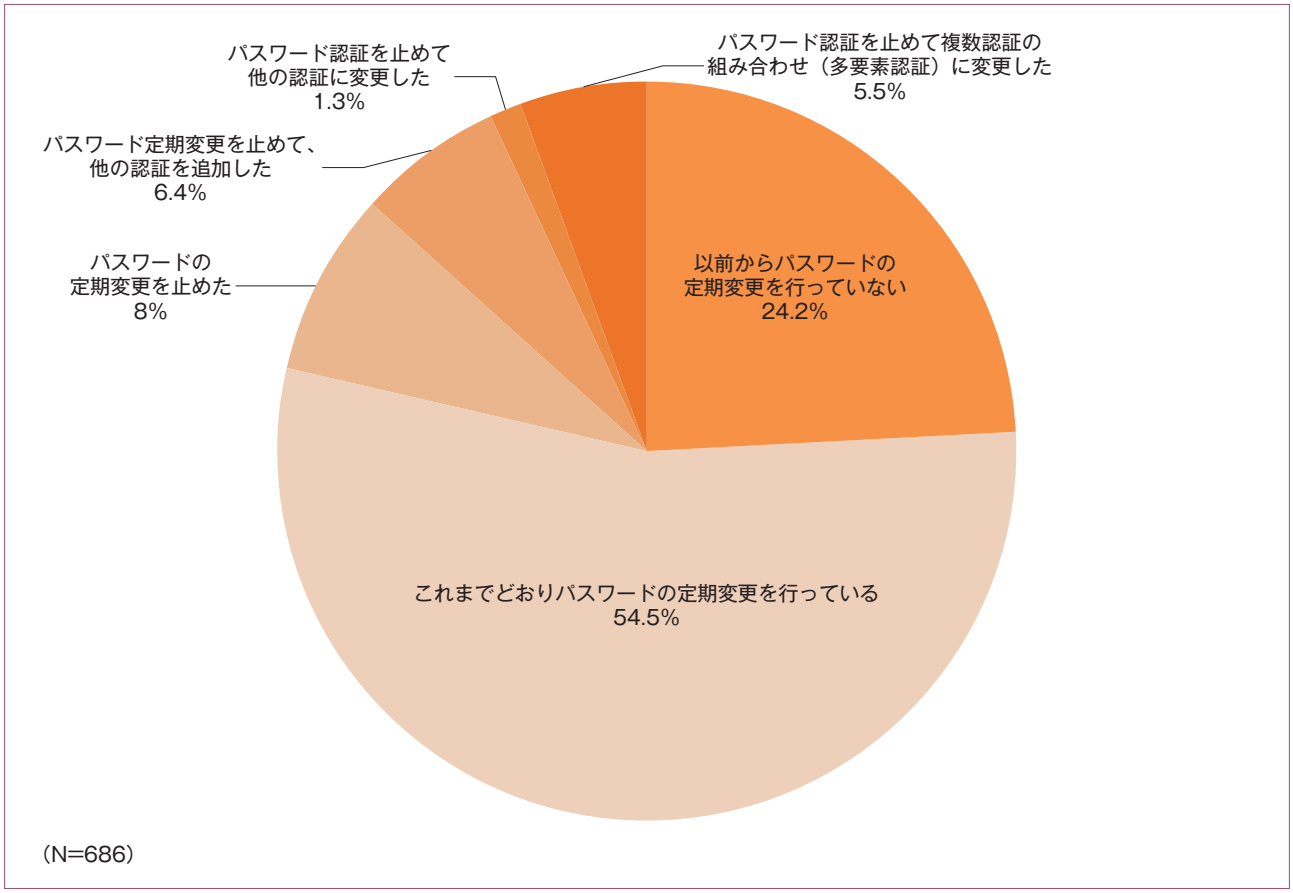


図22. 総務省パスワード変更不要見解への対応状況

5-6. 社内システムのアクセス認証手段

社内システムに対するアクセス認証手段としてなにが利用されているのかを調査した（図23）。

現在利用している認証手段としては、従来どおり「ID／パスワード」方式が圧倒的に高く８割を超え、次いでかなりの差があるが、「LDAP／Active Directory」（34.7％）「ハードウェアトークン（ICカード、RFID等）」（30.9％）と続く。

一方、今後利用したいと考えられている認証手段としては「生体認証」が37.3％と最も高かった。多要素認証の次世代の生体認証を実現するデファクトスタンダードであるFIDO認証については「現在利用中」が12.7％と低いのに対し、「今後利用したい」との回答は25.9％と、高い割合となった。

今後「ID／パスワード」方式からFIDO認証のような多要素認証の利用が一般的になることが期待される。

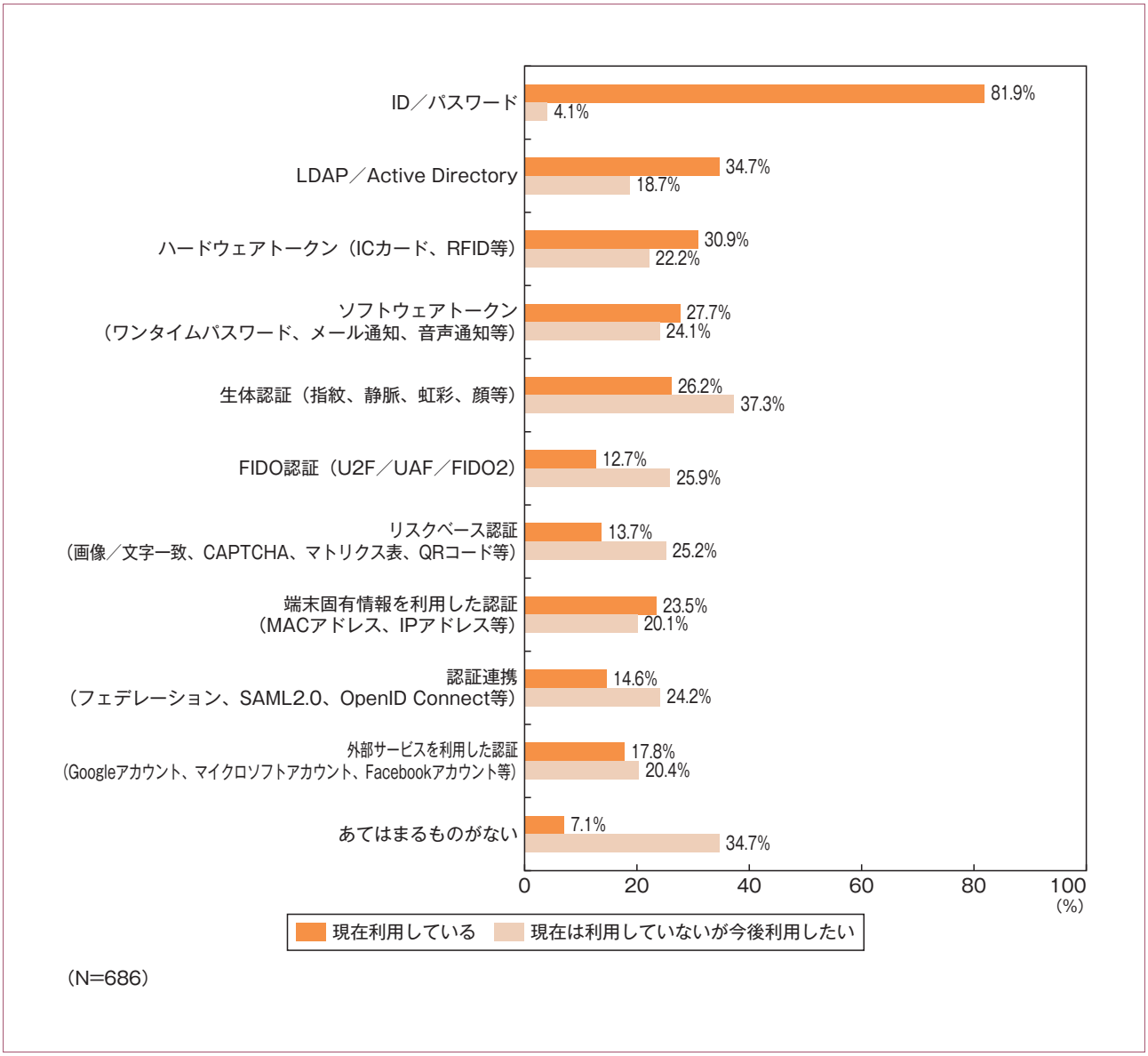


図23. 社内システムのアクセス認証手段

6 働き方改革とクラウドの動向

2018年６月に成立し、今年４月１日より順次施行されている働き方改革法について、企業の取組み状況を調査した。法律として施行されることを受け、取組み自体は加速してきているが、社内制度の整備や運用のためのシステムセキュリティ面の対策については、まだこれからの状況にある。

6-1. 働き方改革の取組み状況

４月の法施行を受けて企業における働き方改革に対する取組み状況は、すべての項目で「実施中」が増加傾向にあり、「検討中」とあわせて５割以上となっていることから、取組みが本格化していることがわかる（図24）。

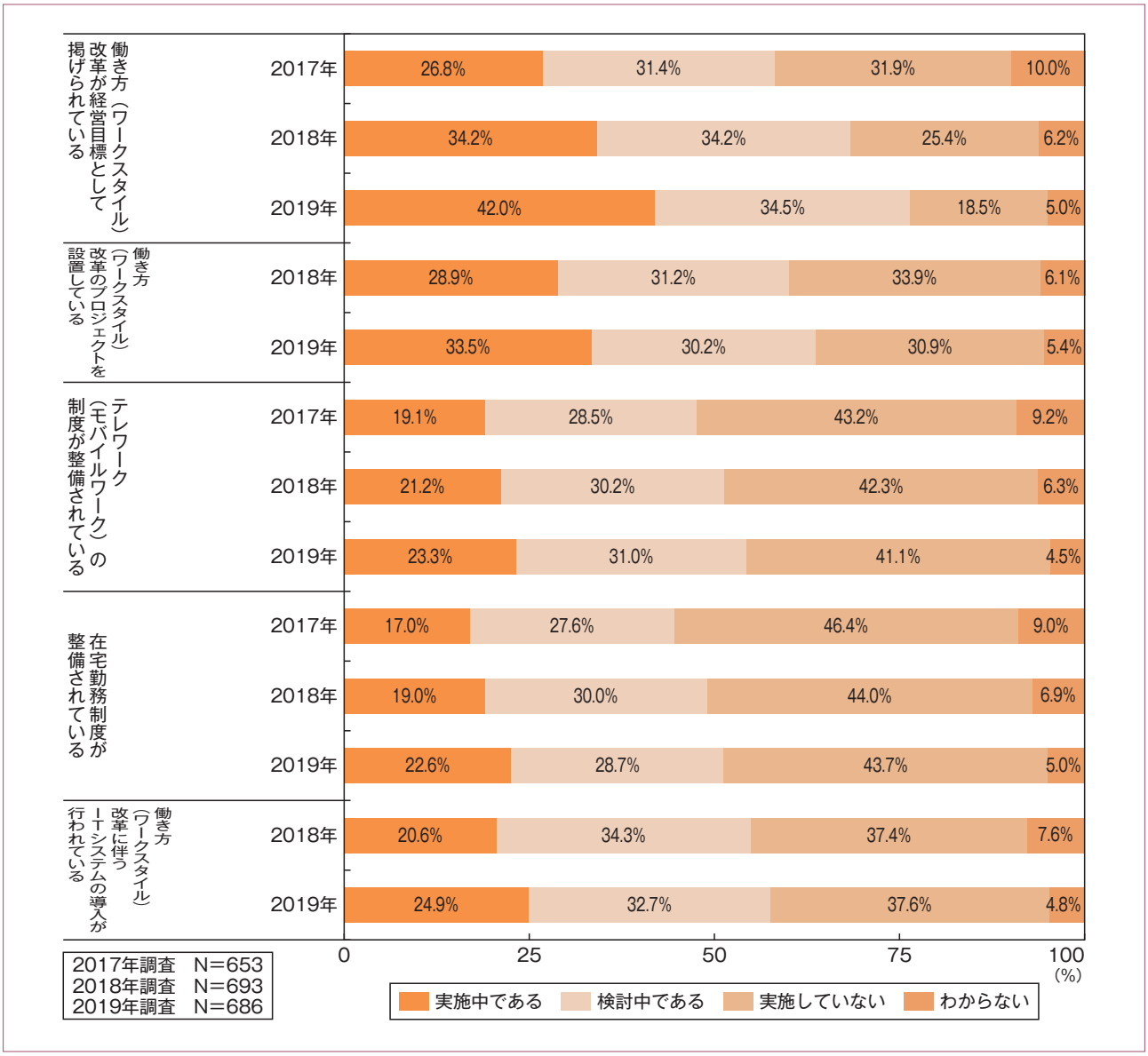


図24.「働き方改革」に関する取組み状況（2017～2019年比較）

6-2. 働き方改革実現のためのセキュリティ対策の実施状況

働き方改革を支えるシステムのセキュリティ対策状況については、「スマートデバイス向けのセキュリティ対策」（46.4%）「法人向けのクラウドサービス利用」（43.6%）「端末にデータを残さない環境整備」（40.1%）が実施されており（図25）、この傾向は前回調査とあまり変化はみられない。

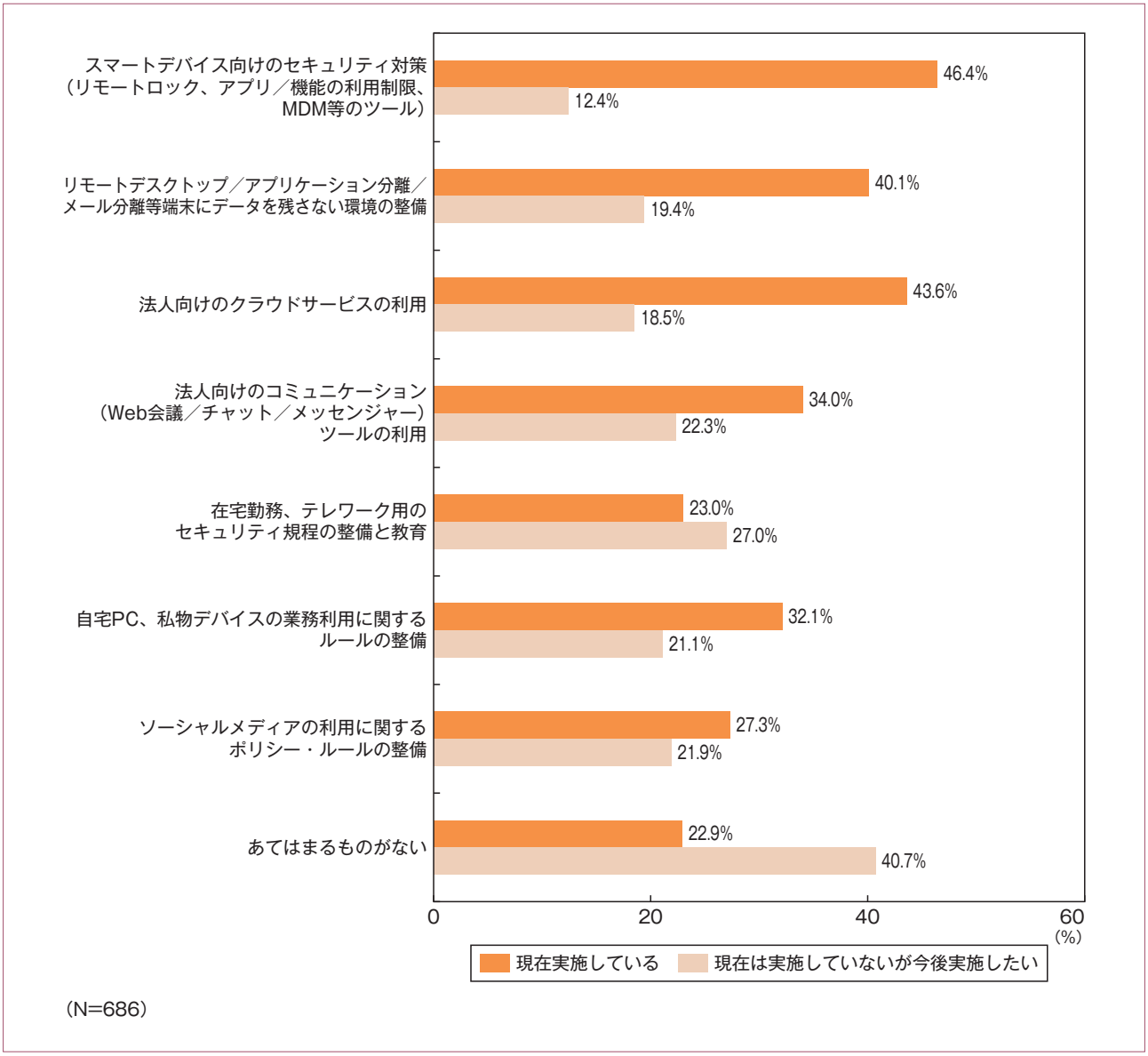


図25. 働き方改革実現のためのセキュリティ対策の取組み状況

6-3. クラウドサービスの選定ポイント

働き方改革を進めるうえで、法人向けクラウドサービスの利用は重要であることから、クラウドサービスの選定ポイントについて調査を行った。

ポイントとしては、前回調査に引き続き「コスト」（62.8%）が最も高く、「セキュリティ対策がしっかりしている」（51.5%）「サポート体制の充実」（41.5%）が続いている（図26）。

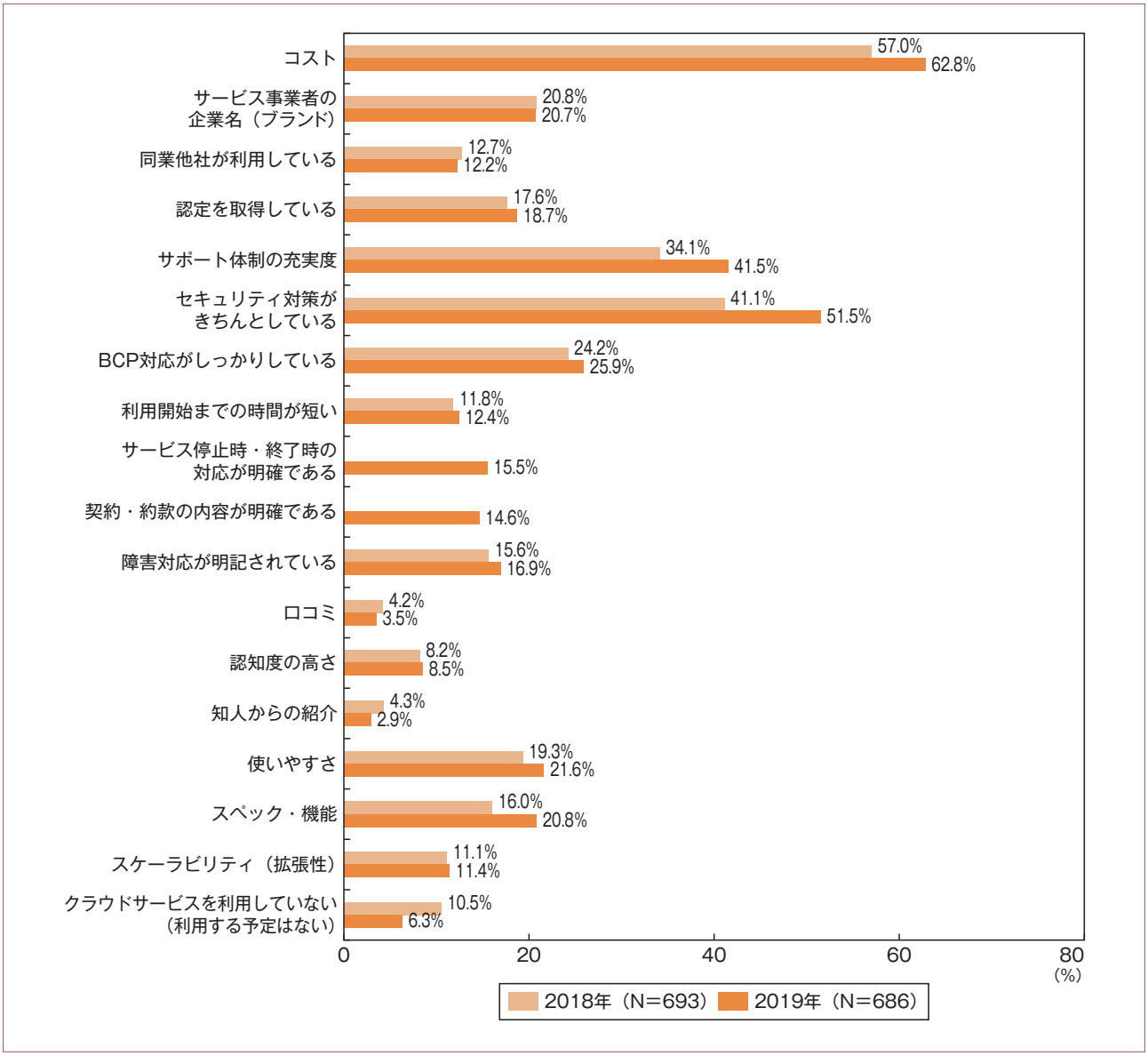


図26. クラウドサービス選定ポイント（2018～2019年比較）

6-4. 電子契約の利用状況

働き方改革と関連して、業務処理の時間短縮を図るため紙ベースで行っていた業務処理をデジタル化する動きがあるが、特に電子化したいと考える業務プロセスと電子契約の利用状況を調査した。

最も多いのは「経費精算（旅費、交通費）」（42.4%）、次いで「請求処理」（35.3%）「社内決裁処理」（35.1%）となった（図27）。

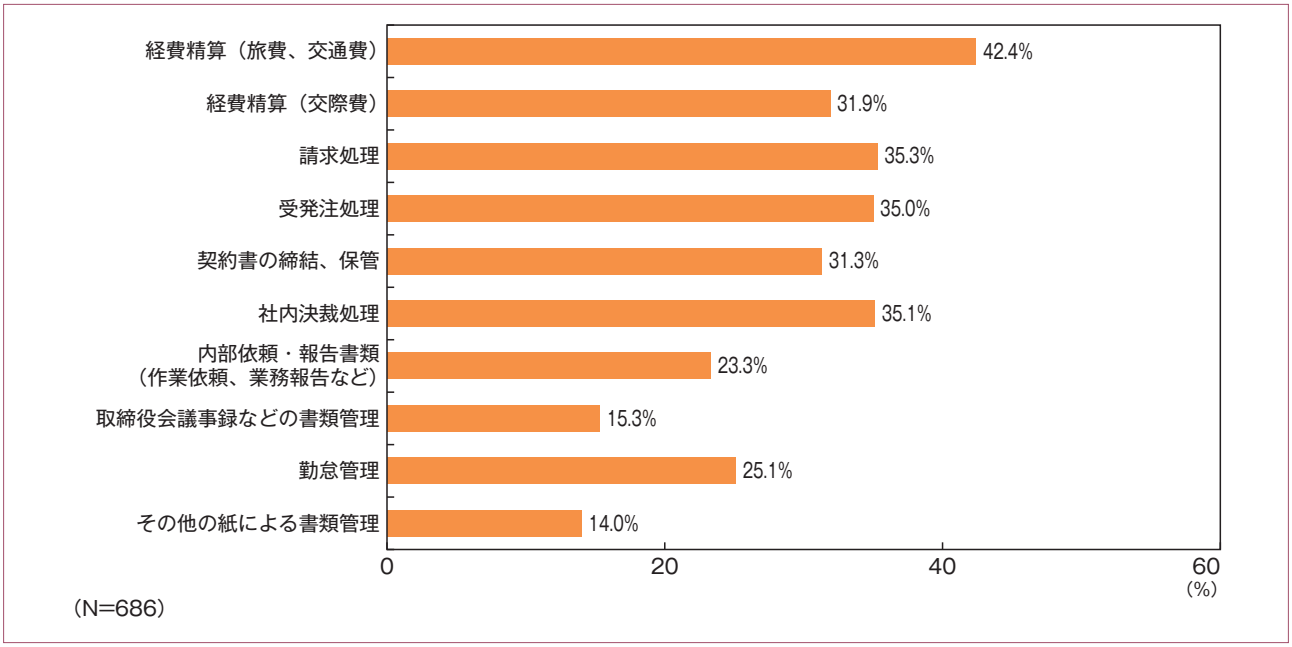


図27. 特に電子化したい業務プロセス

電子契約の利用状況については定点観測を行っているが、電子契約の利用状況について、すでに「複数部門での採用」（22.0%）と「一部の取引先間での採用」（22.2%）での利用で約４割、今後利用予定を含めると約７割に達しており、利用が進んでいる。過去３年間の傾向をみると、利用状況は徐々に増加傾向にあるが、特に大きな変化はみられない（図28）。

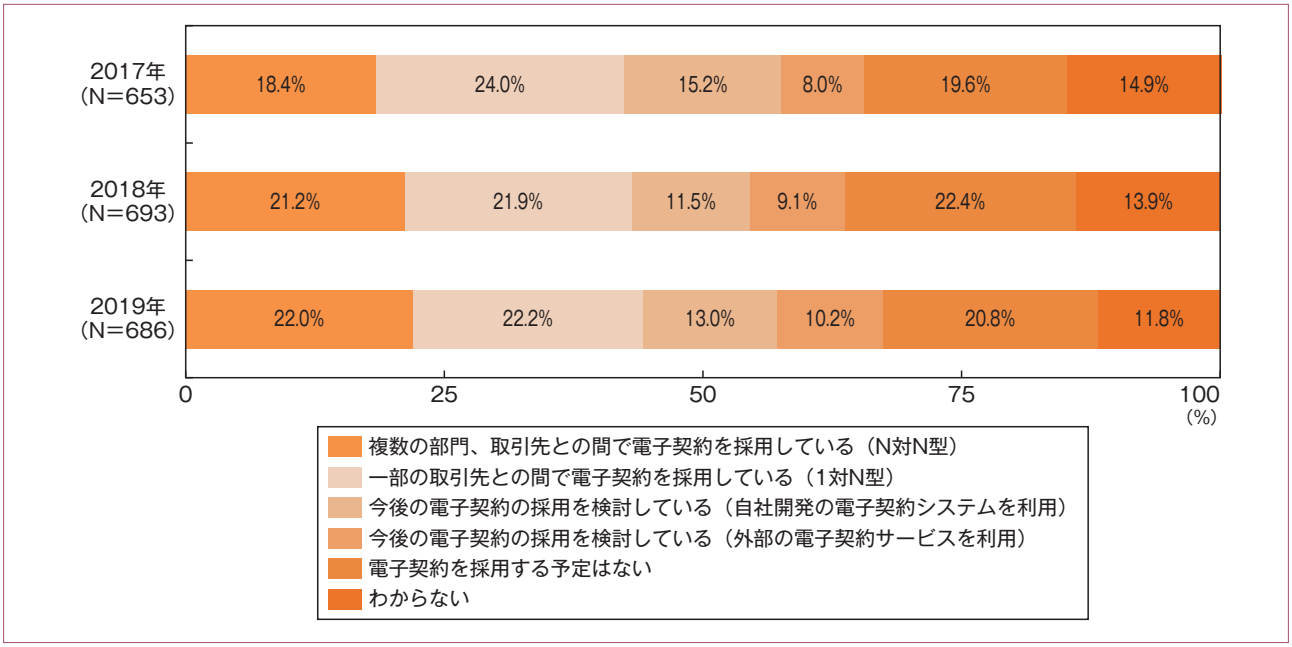


図28. 電子契約の利用状況（2017～2019年比較）

次に電子契約の採用、利用拡大を図るうえでの課題を調査したところ、「コスト（初期導入費用、保守・運用費用、電子証明書の取得・管理費用）」「サービス導入に係る手間（導入メリットの説明、システム導入）」を指摘する回答が５割を超えた。この傾向は前回調査とあまり変化はみられない（図29）。

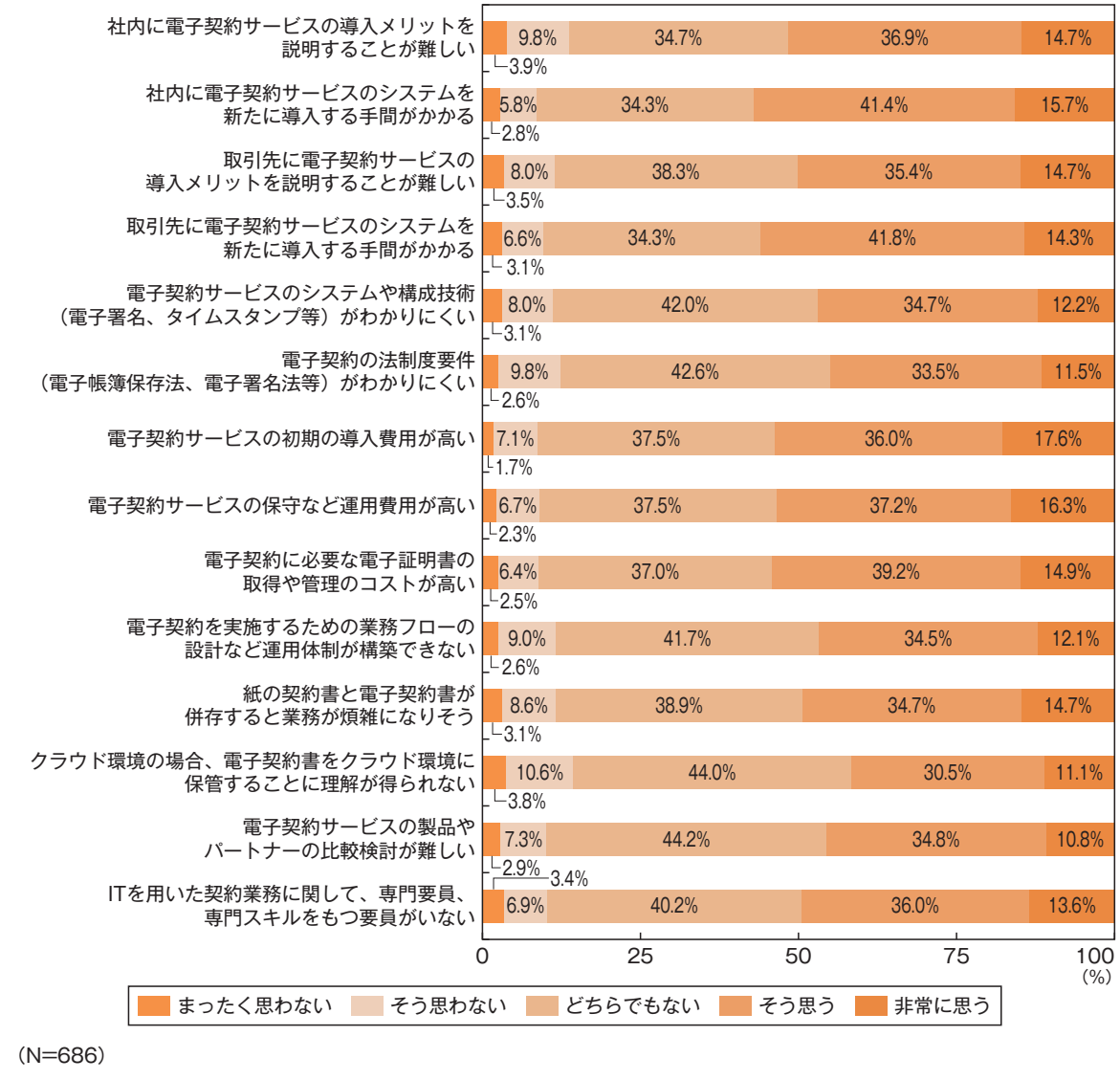


図29.　電子契約／電子契約サービス導入上の課題

7 電子署名／電子証明書の利用状況

セキュリティが担保されたシステムサービスを構築するためには電子署名／電子証明書、自社サイトのSSL化、情報セキュリティ監査の実施などが必要であることから、これらの利用／導入状況を調査した。

7-1. 電子署名／電子証明書の利用状況

電子署名／電子証明書の利用が最も多い分野は「電子メール」（74.5%）で、最近被害が多発している「なりすまし不正メール受信」（ビジネスメール詐欺）対策としての利用が考えられる。また、今後の利用増加が見込まれるのは「電子文書の保存（タイムスタンプ）」である（図30）。

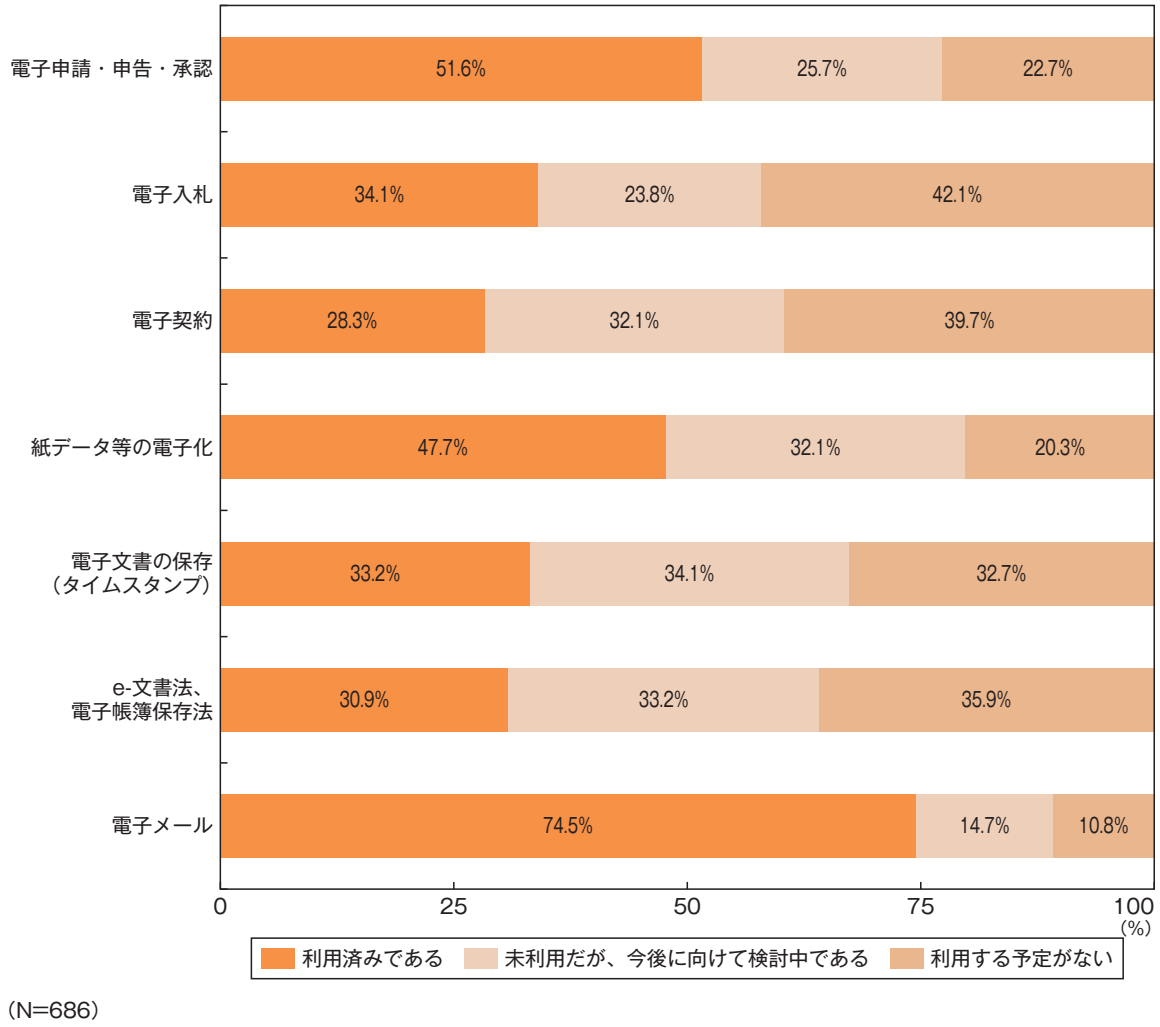


図30. 電子署名／電子証明書の利用状況

7-2. 自社Webサイトの常時SSL化

2018年４月に政府・サイバーセキュリティ戦略本部が発表した中央省庁のセキュリティ対策のための統一基準により、中央省庁の全Webサイトおよび電子メール通信の暗号化対策が義務付けられた。

Webサイトの暗号化対策のSSL化については民間企業にも浸透しており、すでにすべて常時SSL化設定済との回答が約４割、なんらかのSSL化を行っている企業が約８割となっている（図31）。

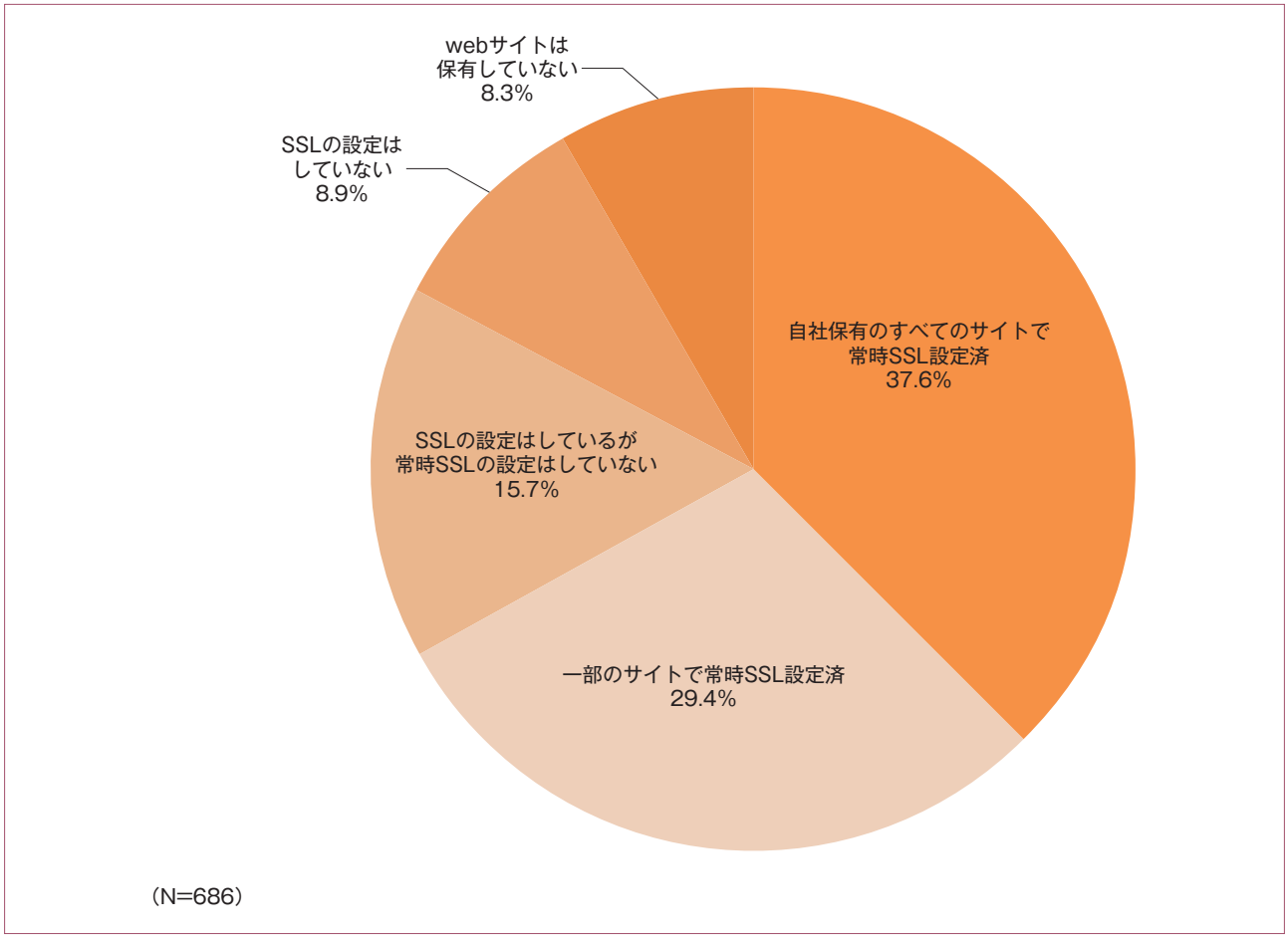


図31. 自社Webサイトの SSL化対応状況

7-3. 情報セキュリティ監査の実施状況

自社保有のシステムや利用しているクラウドサービスについて、必要な対策が実施されて十分なセキュリティが担保されているか客観的に検証するには情報セキュリティ監査が有効であることから、情報セキュリティ監査の実施状況について調査を行った。その結果、「外部委託による定期的な実施」（14.1％）「自社での定期的な実施」（20.8％）、と定期的な監査の実施率が３割強となり、あわせて会計監査等、他の監査の一環で行う簡易的なものや不定期の実施を含めると７割強で実施されている（図32）。

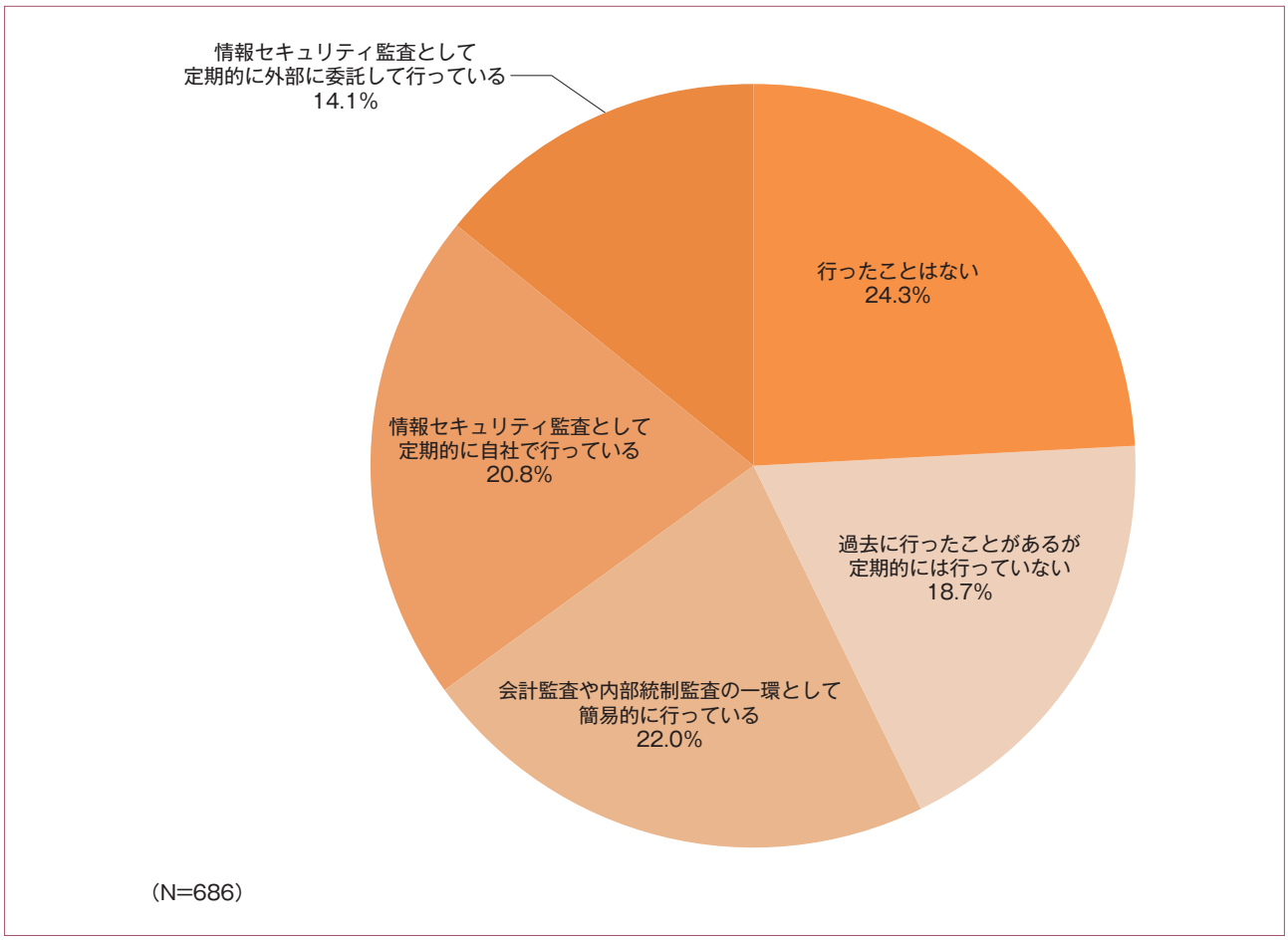


図32. 情報セキュリティ監査の実施状況

8 総　評

「企業IT利活用動向調査」は情報セキュリティをメインテーマとして、企業のIT利活用の状況を把握するため毎年行っている調査で、今年で８回目となった。

情報セキュリティインシデント認知率については、毎年「PC、スマートフォン等情報機器の紛失・盗難」や「PCのマルウェア感染」が多かったが、昨今の標的型攻撃やビジネスメール詐欺の増加を反映する形で「外部からのなりすましメール」や「Webサイトへの不正アクセス」のようなインシデントが年々増えて目立ってきている。

一方で企業のセキュリティ対策については、従来型のファイアウォールやマルウェア対策ソフトの導入に留まっており、このような新しい攻撃に対応できるセキュリティシステムの導入の比率はまだ低い。サイバー攻撃は日々巧妙化・複雑化してきていることから、新しい攻撃に対応できるセキュリティシステムの導入等対策を進めることが必要である。

国内では個人情報保護法改正およびJIS Q15001改正から１年以上が経過したが、「個人識別符号」についての関心が高いことがわかった。マイナンバーのみならず個人識別符号となり得る番号は業務に多く存在するため、これらの番号の適切な管理が改正個人情報保護法やJIS Q15001を遵守するうえで重要な意味を持つと思われる。一方で、2018年５月にEUで施行されたGDPRについては、未対応や気にせずにデータ移行を行っているという回答が約３割もあることがわかり、対応の遅れが明確になっている。GDPRはEU域内だけの法律ではなく、EU域外に対しても影響を及ぼす法律であり、日本の企業にも無関係ではない。グローバルではGDPRを契機に全世界のあらゆる地域で個人情報保護やセキュリティマネジメントの法律が整備されつ

つあり、これからは取引がある海外の国・地域の個人情報保護やセキュリティに関する法規制を考慮しながらビジネスを進めなければならなくなっており、企業には国内だけでなくグローバルでのセキュリティガバナンスが求められている。

働き方改革については2018年の「働き方改革関連法」の成立と今年４月からの順次施行により、各社とも取組みが進みだしており、今後在宅勤務やテレワーク等の勤務形態に合わせて信頼できるクラウドサービスの活用や、社内文書の電子化も進むと思われる。また、このような取組みには並行してセキュリティ対策が必要であり、状況をモニタリングして改善していくためにも情報セキュリティ監査の位置づけが重要になる。

回答者プロフィール

業種	回答数	%
製造	203	29.6
建設・不動産	65	9.5
卸売・小売	64	9.3
金融・保険	48	7.0
情報通信	98	14.3
サービス	168	24.5
公共・その他	40	5.8
全体	686	100.0

年間売上規模	回答数	%
1,000万円未満	5	0.7
1,000万円～１億円未満	3	0.4
１億～10億円未満	68	9.9
10億～100億円未満	201	29.3
100億～500億円未満	140	20.4
500億～1,000億円未満	72	10.5
1,000億～3,000億円未満	57	8.3
3,000億～5,000億円未満	32	4.7
5,000億円以上	108	15.7
全体	686	100.0

従業員規模	回答数	%
5,000人以上	139	20.3
1,000～4,999人	156	22.7
300～999人	168	24.5
50～299人	223	32.5
全体	686	100.0

業種別内訳

業種		回答数	%
製造	食品・飲料	14	2.0
	日用品・生活雑貨	4	0.6
	繊維	4	0.6
	パルプ・紙・印刷	10	1.5
	化学工業	17	2.5
	石油製品	3	0.4
	鉄鋼・金属	16	2.3
	プラスチック・ゴム	4	0.6
	機械	21	3.1
	電気機器	33	4.8
	情報通信機器	3	0.4
	電子部品・電子回路	20	2.9
	精密機器	15	2.2
	自動車・輸送機器	19	2.8
	医薬品	7	1.0
	その他の製造業	13	1.9
建設・不動産	建設	53	7.7
	不動産	11	1.6
	住宅	1	0.1
卸売・小売	卸売	21	3.1
	小売	23	3.4
	商社	20	2.9
金融・保険	銀行	22	3.2
	証券	7	1.0
	生命保険	4	0.6
	損害保険	7	1.0
	その他金融	8	1.2

業種		回答数	%
情報通信	通信	15	2.2
	ITベンダ/システムインテグレータ	57	8.3
	インターネットサービス	13	1.9
	情報システム子会社	13	1.9
サービス	電力・ガス・水道	6	0.9
	運輸	24	3.5
	倉庫	4	0.6
	宿泊	5	0.7
	飲食	9	1.3
	娯楽・レジャー	8	1.2
	メディア・出版・放送・広告	1	0.1
	生活関連サービス(旅行業など)	9	1.3
	医療	22	3.2
	福祉・介護	22	3.2
	教育（学校以外）	7	1.0
	人材派遣・業務委託	15	2.2
	その他サービス	36	5.2
公共・その他	学校	19	2.8
	官公庁	3	0.4
	地方自治体	9	1.3
	その他公共機関	9	1.3
全体		686	100.0

IT戦略／情報セキュリティへの関与度合（複数回答）	回答数	%
全社的なIT戦略に決定権をもっている	273	39.8
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	330	48.1
セキュリティ製品の導入、製品選定に関与している	375	54.7
セキュリティ対策の実務に関与している	240	35.0
全体	686	−

〈資料〉情報化に関する動向（2018年10月～2019年３月）

国　内	海　外
2018年10月	
・東京証券取引所、証券会社の大量電文送信の影響で、大規模システム障害。 ・全国銀行資金決済ネットワーク、他行に24時間365日振込可能な新システム「モアタイムシステム」稼働。約500行が参加。 ・ヤフー、個人の信用情報を数値化した「信用スコア」サービスの実証実験開始を発表。スコアを基に融資、審査サービスに活用。 ・東京大学、スマホ等の利用履歴を用いた認証技術「ライフスタイル認証」研究開発に着手。 ・個人情報保護委員会、Facebookによる数千万人分の個人情報流出問題で実態調査開始。行政指導も視野に。 ・情報通信研究機構（NICT）、日英中等８言語の識別技術開発。発話時間1.5秒の音声を0.15秒以内でリアルタイムに識別可能に。 ・総務省、GAFAを中心とするプラットフォーマー規制のあり方を検討する「プラットフォームサービスに関する研究会」初会合。個人情報保護規制強化を目指す。 ・総務省と日本IT団体連盟、「情報銀行」事業者認定説明会実施。金融機関等200社が参加。 ・日本政府、漫画等の無断掲載（海賊版）サイトへのアクセスブロッキングの法整備対策がまとまらず、議論は無期限延期に。 ・東京地裁、無料公開されたイラストの無断転載は違法と判断、まとめサイトに損害賠償命令。 ・ヤフー、なりすましメール対策で、正規メールに企業のブランドアイコン表示。送信元確認は送信ドメイン認証「DKIM」利用。	・カリフォルニア州、IoTデバイスを対象とするサイバーセキュリティ法成立、米州法では初。 ・英国保守党のモバイルアプリで、議員を含む党大会参加者の個人情報が漏えい。メールアドレス入力だけでプロフィール画面にアクセス可能。 ・中国企業調査、DNS書換えで不正サイトに誘導する「GhostDNS」で、70種類以上のルータ攻撃により端末10万台超が被害に。 ・FireEye調査、北朝鮮のハッキング集団「APT38」により、世界中の銀行で不正送金が続き、１億円以上の被害に。 ・Google、最大50万人の個人情報流出のおそれを受け、Google＋閉鎖を決定。2019年８月サービス終了を発表。 ・ロンドン高裁、Googleによる400万人超のiPhoneユーザの個人情報不正入手に対する集団訴訟を棄却。英データ保護法上の「損害」判断できず。 ・キャセイパシフィック航空、不正アクセスにより約940万人の顧客情報流出のおそれ。 ・ブリティッシュ・エアウェイズ、不正アクセスにより18.5万件のカード情報流出。９月の大量流出事件とあわせて42万件の被害。25万件が販売された可能性。 ・英情報コミッショナー事務局、Facebookの個人情報不正流出問題を受け、同社に50万ポンドの罰金徴収を発表。

国　内	海　外
2018年11月	
・日本版GPS「みちびき」の本格始動。世界最高精度の測位可能に。 ・経済産業省他、プラットフォーマー規制強化へ。有識者会議提言の「透明性・公正性確保」を受け、ルール整備に着手。プラットフォーマーへの聞取り調査で実態解明へ。 ・内閣府調査、ネット利用の不安事項のトップは「個人情報流出」で８割。「詐欺」「子ども・家族への危険」も。 ・LINE、信用スコア事業参入を発表。個人向けローンサービスを展開。	・Facebook、ハッカーにより8.1万件の個人的メッセージが売られた可能性。 ・Kaspersky調査、16カ国131大学がフィッシング攻撃の標的に。１年間で約1,000件を検知。 ・英下院、Facebook情報流出問題で９カ国の議会関係者参加の国際公聴会実施。 ・米司法省、総額700万ドル超のデジタル広告料金詐欺への関与で８人を訴追。詐欺に使用したbot解体。 ・ユーロポール、各国との連携により海賊版販売ドメイン約3.3万件を停止。12人を逮捕し、犯行で得た100万ユーロを凍結。 ・Uber、2016年のデータ流出問題で英国38.5万ポンド、オランダ60万ユーロの制裁金。GDPR施行前のため、旧規制に基づく制裁金額。

国　内	海　外
2018年12月	
・日本政府、改正サイバーセキュリティ基本法成立。2020年東京五輪・パラリンピックに向け、サイバーセキュリティ協議会発足準備。（2019年４月に発足） ・ソフトバンク、世界11カ国で大規模通信障害発生。交換機ソフトウェアの証明書の期限切れが原因。 ・日本政府、機密漏えい防止策の一環で初の政府調達指針策定。 ・経済産業省他、プラットフォーマー規制のための基本原則策定。独占禁止法運用の拡張やデータ移転ルールを整備。 ・経済産業省、デジタルトランスフォーメーション（DX）推進に向けガイドライン発表。 ・経済産業省他、「デジタルプラットフォーマー型ビジネスの台頭に対応したルール整備の基本原則」策定。 ・ベーシック社運営サイト、クラウドサービスへの不正アクセス攻撃で、約30万件の顧客情報流出のおそれ。	・マリオットホテルチェーン、不正アクセス被害によるデータ流出で最大５億人に影響のおそれ。 ・実名制Q＆AサイトのQuora、サイバー攻撃被害により、約１億人の個人情報に影響。 ・欧州連合、電子商取引での地理的制限を禁止するEU規則を施行。EU国民は同一条件で国外サイトでの買い物が可能に。 ・Google、Google＋のバグで新たに5,250万人の情報漏えいの可能性。Google＋の終了期限短縮を決定。 ・アイルランドデータ保護委員会、Facebookのプログラム不具合による写真情報流出を受け、GDPR全面施行後の法定調査を開始。 ・仏政府、プラットフォーマーを対象に2019年１月からデジタル課税の導入を発表。年間税収５億ユーロの見込み。 ・首都ワシントン、Cambridge Analytica事件で個人情報を保護しなかったとして、Facebookを提訴。 ・米司法省、ハッキング集団「APTIO」メンバーの中国人ハッカー起訴。偽メールでウイルスを感染させ、世界規模でハッキング行為。

国　内	海　外
2019年1月	
・カルチャー・コンビニエンス・クラブ、Tポイントカードの会員情報、ポイント履歴を捜査令状なしに捜査機関に提供。保護法上違反なし。 ・日－EU間、個人データ移転の例外措置を認める「十分性認定」発効。越境データ移転が円滑に。 ・オージス総研、個人向けファイル転送サービスへの不正アクセスで、約480万件の顧客情報流出。 ・鉄道総合技術研究所他、世界初、ミリ波（90GHz帯）無線通信システムにより時速240km走行列車と地上間でのデータ伝送に成功。 ・IPA 2018年の「サイバーセキュリティ10大脅威」発表、個人で最も影響が大きかったのはクレジット情報の不正利用、組織は標的型攻撃被害。	・ワールドワイドウェブ（WWW）、仕組み誕生から30年。 ・日米欧の貿易相、個人、企業の自由な越境データ流通を認める「データ流通圏」構築に向けた連携に向け合意。 ・メルケル首相他、ハッキング被害により政治家、著名人等数百人分の個人情報がtwitter上に流出。 ・マリオットホテルチェーン、2018年に発覚したサイバー攻撃で、最大3.8億件の個人情報流出を報告。うち、暗号化されていない旅券番号は525万件。 ・IBM、単体で動作可能な量子コンピュータ「IBM Q System One」発表。 ・仮想通貨取引所のコインベース発表、イーサリウムクラッシックへのハッカー攻撃で110億ドル相当の仮想通貨盗難被害。 ・Facebook、ベトナムサイバーセキュリティ法違反の可能性。違法コンテンツへの自社プラットフォーム投稿容認を問題に。 ・世界貿易機関、データ取引の国際ルール策定を目指す共同声明。国によるデータ管理をけん制し、安全なデータビジネス環境構築へ。 ・仏政府、GDPR違反第１号としてGoogleに5,000万ユーロの制裁金。 ・米司法省、中国華為に対し、企業機密搾取、詐欺容疑で起訴。米、EU、日本、台湾等の政府機関で中国ハイテク企業排除に向けた動きが活発化。

国　内	海　外
2019年2月	
・日EU経済連携協定（EPA）発効。電子商取引、データ流通、知的財産保護等のルール整備へ。 ・ソリトンシステムズ調査、27億件のアカウントデータ群「Collection#1」流出。うち2,002万レコードが国内関連。 ・総務省とNICT、サイバー攻撃に悪用されるおそれのあるIoT機器の特定調査と電気通信事業者に注意喚起を行う「NOTICE」開始。	・独研究施設HPI調査、過去10年分の流出アカウント情報数十億件がダークウェブ上で一括ダウンロード可能の状態に。 ・カナダ仮想通貨取引所、創設者死亡により、パスワードがわからず、1.9億米ドル分の仮想通貨が引き出せず。 ・独連邦カルテル庁、Facebookに利用者データの収集制限命令。 ・Apple仏子会社、仏当局と法人税未納分推計約５億ユーロの支払い合意。 ・TikTok、親の同意なしに子どもの個人情報の収集は児童オンラインプライバシー法に違反するとして、罰金570万ドルを支払い、米連邦取引委員会と和解合意。民事制裁金で最高額に。

国　内	海　外
2019年3月	
・NTTドコモ、「ｄポイント」会員情報を協業企業に有償提供するデータビジネスへの参入を発表。2019年度内実現へ。 ・東京地裁、野村HDと野村證券が2010年に日本IBMに対し委託業務不履行で訴えた損害賠償請求裁判で、日本IBMに約16億円の賠償支払い命令。 ・警視庁、約1,500万円相当の仮想通貨「モナコイン」を詐取した18歳のハッカー少年を電子計算機使用詐欺、犯罪収益隠匿の疑いで書類送検。ゲーム感覚での犯罪。 ・内閣府、Society5.0実現に向け「人間中心のAI社会原則」策定。	・仏政府、IT大手に対し、ネット上ビジネス売上高の３％を課すデジタル課税法案発表。EUとしては合意見送り。 ・国連安全保障理事会、対北朝鮮制裁履行状況報告書公開。北朝鮮によるサイバー攻撃で仮想通貨総額5.7億ドルの被害。 ・Google、最新のクラウドコンピュータにより円周率を小数点以下31.4兆桁まで計算し、世界記録更新。 ・欧州委員会、オンライン広告の不正慣行を理由にGoogleに14.9億ユーロの制裁金。独占禁止法違反での制裁金徴収は３年間で３度。 ・Facebook、数億人単位でのパスワードを非暗号化保管していたと発表。パスワードの社外流出、不正利用の形跡なし。 ・欧州委員会、次世代通信規格5Gのセキュリティ確保にむけ、EU各国共通の運営手順と施策に対する取組みを勧告。華為排除は求めず。 ・欧州議会、インターネットにも著作権を適用する著作権指令改正案を承認。 ・米住宅都市開発省、住宅関連広告表示において特定のユーザを差別しているとしてFacebookを提訴。同社は数日前に民間団体からの差別的広告裁判での和解を発表。

IT-REPORT

JIPDEC

JIPDEC IT-Report 2019 Spring
2019年5月31日発行（通巻第13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12階
TEL：03-5860-7555　FAX：03-5573-0561
制　作　株式会社ウィザップ