IT-REPORT

IT-REPORT 2021 Spring

特集 コロナ禍にみるIT化の現状―「企業IT利活用動向調査2021」結果から

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 2021 Spring」では、JIPDECが2011年から継続して行っている「企業IT利活用動向調査2021」の結果をとりまとめ、紹介しています。

2020年に世界規模で拡大した新型コロナウイルス感染はわが国をはじめ、世界各国に大きな影響を及ぼし、人々の生活様式、ビジネス環境も大きく変化させました。

本調査では、毎年「働き方改革」への取組み状況について、経営課題上の重視度合いや、具体的な取組状況について調査を実施していますが、ここでもコロナ禍の影響により、働き方改革に沿った体制の整備、テレワーク導入に関連したIT環境、クラウドサービスの利用状況などに変化が見られました。

働き方改革を支えるシステムのセキュリティ対策についてはスマートデバイス向けのセキュリティ対策の実施や法人向けクラウドサービスや法人向けコミュニケーションツールの利用が増えており、特に、働き方改革の実現に重要な役割を示すクラウドサービスの利用に関しては、何らかの形でクラウドサービスを利用している割合が８割を超え、さらにそのうちの半数は半分以上の社内システムにクラウドを利用しています。

コロナ禍で勤務形態が変わってきていることにより、事務手続きの電子化も進んでいます。今回の調査では、６割以上の企業が電子契約を利用しており、今後も増加していくであろうことが推測されます。また、企業がセキュリティ対策を重視する中、十分なセキュリティ対策が講じられているかを第三者の立場で客観的に判断する手段として、認定／認証制度や、セキュリティ監査の実施が有効と考えられますが、情報セキュリティ監査の実施率は、約９割が定期的または不定期に実施していることがわかりました。

このほか、過去１年間に受けたセキュリティインシデントの状況、セキュリティ支出の動向、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、2020年10月から2021年３月の国内外の情報化動向をとりまとめていますので、今後のIT環境整備の参考にしていただければ幸いです。

2021年５月

一般財団法人日本情報経済社会推進協会

JIPDEC IT-Report 2021 Spring

Contents

特集

コロナ禍にみるIT化の現状 ―「企業IT利活用動向調査2021」結果から

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、経営企画系、総務・人事、業務改革系部門等に所属し、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。

本調査は、毎年１月に、その時のIT動向を反映しつつ調査項目を見直し実施しているが、昨年は、世界規模で急激に拡大した新型コロナウイルス感染症が社会のさまざまな場面に大きく影響を与えた状況を鑑み、コロナ禍において企業の考え方や行動にどのような変化が生じたかを把握するため、2020年７月に一部の項目について追跡調査を行った。

本誌では、2021年１月の調査結果について、これまでの調査結果との経年比較を含め、コロナ禍における企業の取組みについて、特徴的な傾向をピックアップして紹介する。

1 「企業 IT 利活用動向調査」10 年の変化

企業IT利活用動向調査は東日本大震災後の2011年５月に第１回目の調査を実施してから10年が経過した。震災後も大規模なサイバー攻撃事件や個人情報漏えい事件、システム障害、そして2020年の世界規模でのコロナウイルス感染拡大という大きな災禍に見舞われたこの10年で、IT環境、セキュリティ製品等の技術面に著しい進化が見られた。

しかしその一方で、サイバー攻撃や情報漏えいなどのセキュリティインシデントも複雑化、巧妙化するとともに、規模が拡大化し、これらの環境下において、企業・事業の存続を図るため、経営課題の見直し、最新IT技術の導入、ビジネスへの取組み方の見直し、労働体制の見直しを余儀なくされるようになった。

●働き方改革は常に経営課題に挙がるも、取組みは課題から実践へ

2016年、安倍政権下に発足された「働き方改革実現会議」で、働く人の視点に立った労働環境や処遇改善を見直すための13の実行計画が策定された。このなかで「柔軟な働き方がしやすい環境整備」としてテレワークの導入が挙げられた。

働き方改革は2017年の調査開始以降、重視する経営課題の第２位となっていたが、今回調査では割合が減少した（図１）。これは、働き方改革関連法が2019年４月から順次施行されたことで、机上の課題から実際の取組みに移行したとみることができる。実際、働き方改革の実行計画公表後の2017年とコロナ禍直前の2020年１月、そして2021年の取組み状況を比較すると、テレワーク制度や在宅勤務制度の整備が進んでいることがわかる。2020年以降の数度にわたる緊急事態宣言下で在宅勤務やテレワークを導入せざるを得ない状況となったことから、早急な環境整備・実践に繋がったものと考えられる。

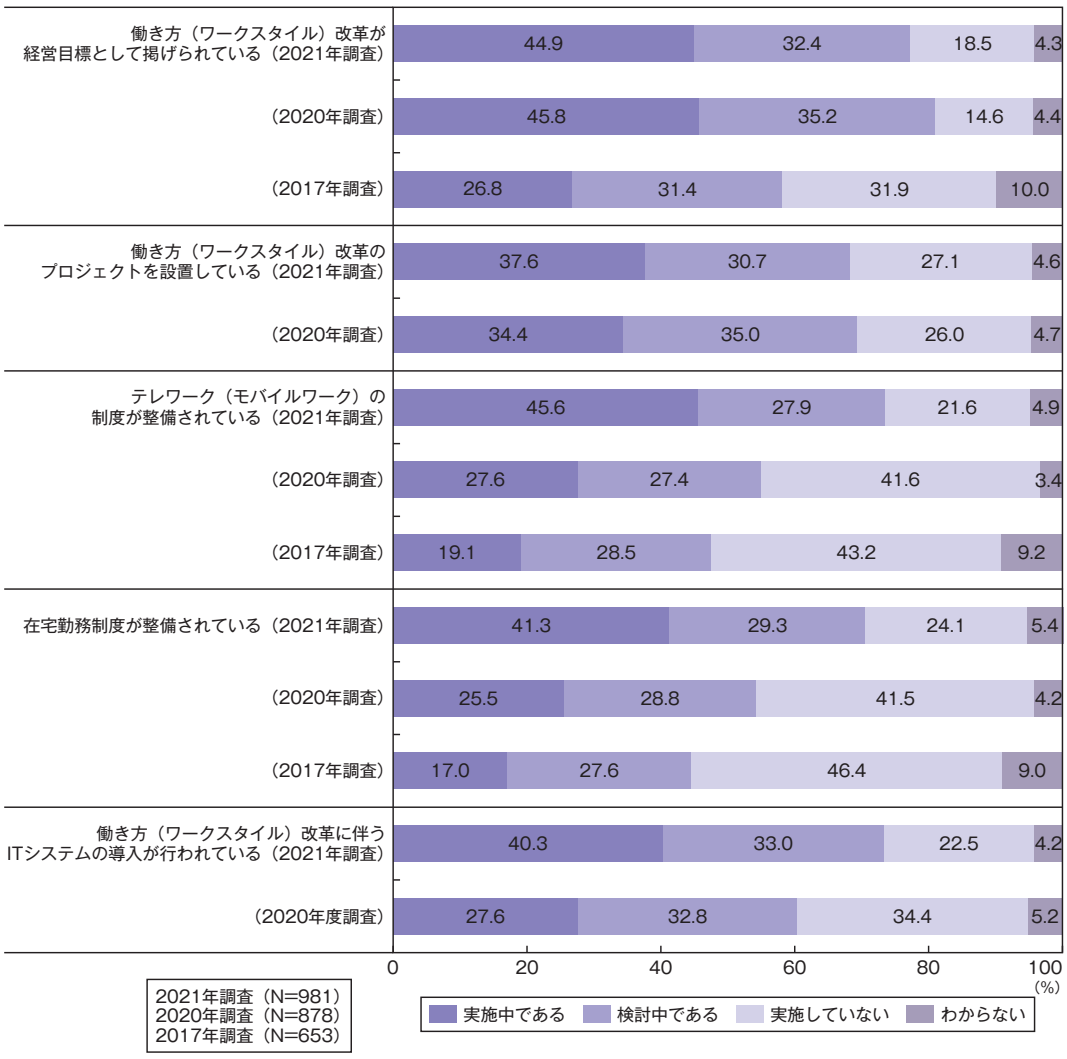


図１．働き方改革への取組み状況（2017、2020、2021年調査比較）

●オンプレミスからクラウドへ―テレワークで活用増大

勤務体制の変更・整備や、テレワークのためのネットワーク環境が整備される中、システムのクラウド利用も急速に進んでいる。2011年はまだ自社で情報システムを保有・管理・運用するオンプレミスが主流で、クラウドサービスの利用は少なく、プライベートクラウドや、パブリッククラウド（IaaS/HaaS、PaaS、SaaS）も低い導入率であった（図２）。しかし、2021年調査では、社内システムの半分以上にクラウドサービスを利用する企業が増加した（図３）。

オンプレミスに比べ、クラウドシステムの方が導入コスト、運用管理負荷の軽減などの面から導入しやすい点、さらにはコロナ禍で在宅勤務、テレワーク環境下でのWeb会議やチャット、ファイル共有などのコミュニケーション基盤整備が急務となったことから利用が増えたと考えられる。

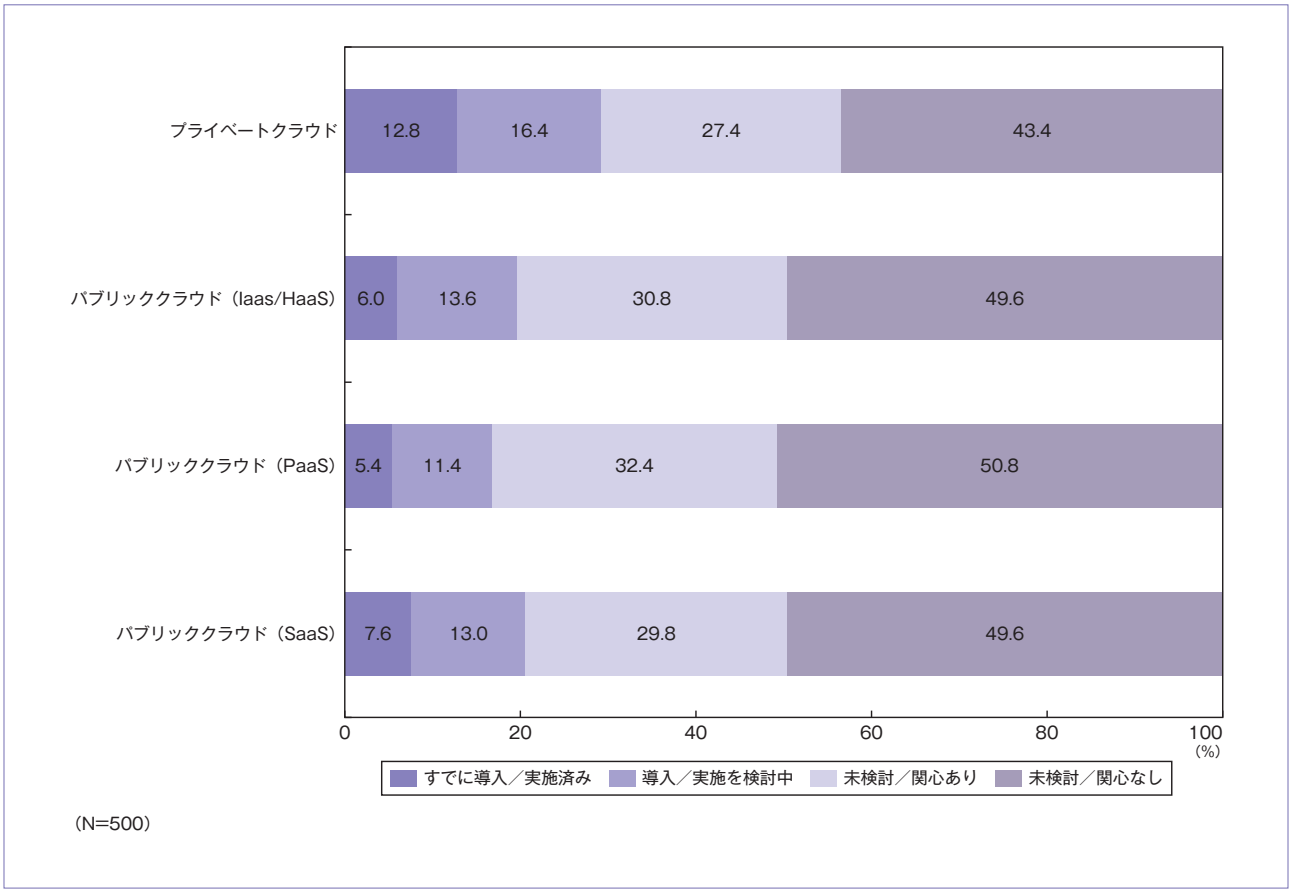


図２．クラウドサービスの利用状況（2011年調査）

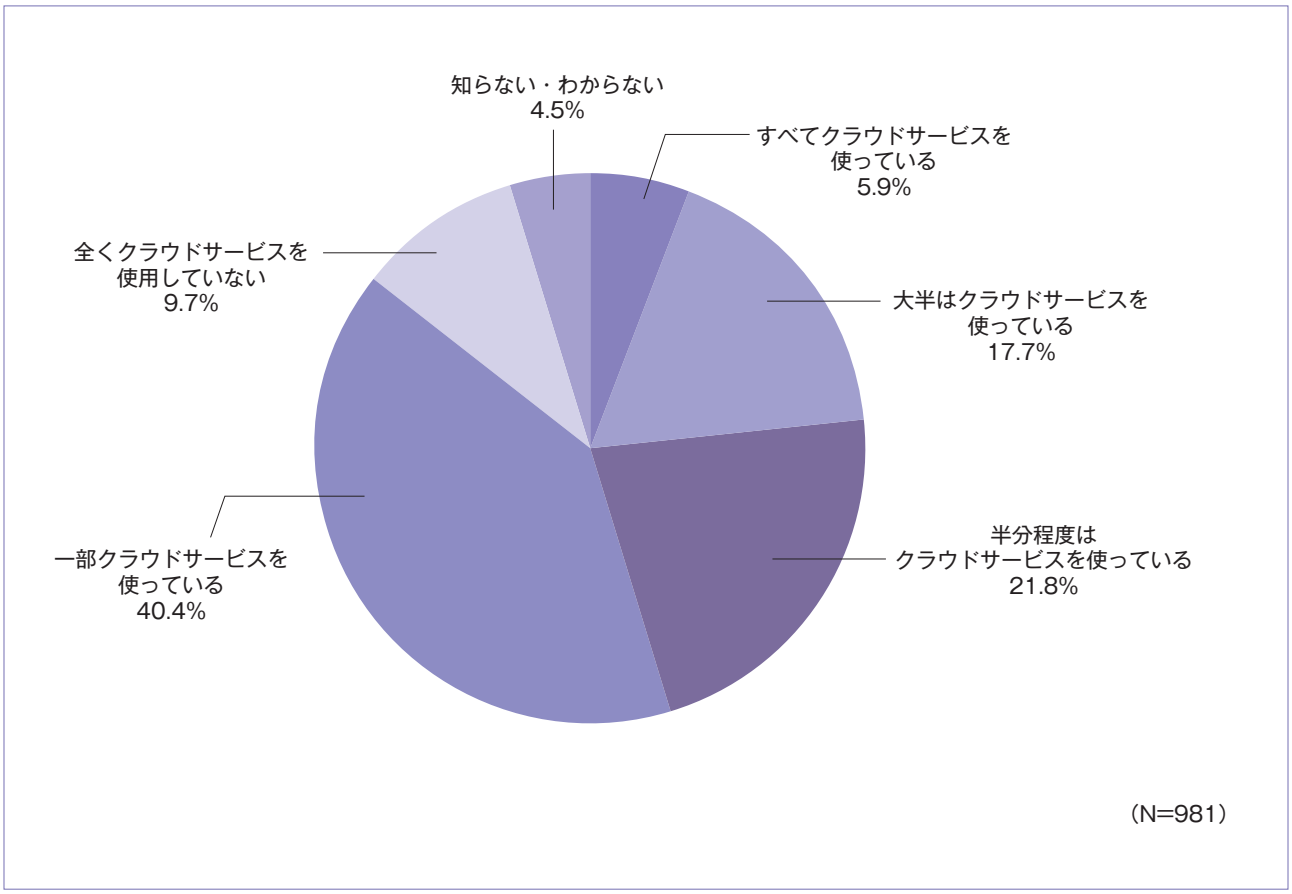


図３．クラウドサービスの利用状況（2021年調査）

●テレワーク導入で電子契約利用が増加

コロナ禍において在宅勤務やテレワークが必須の経営課題となる中、内閣府が2020年７月に策定した規制改革実施計画には電子署名の活用促進や国、地方公共団体の押印手続きの見直しが盛り込まれており、民間企業においても、働き方改革の一環として、事務処理の電子化、押印廃止の動きが進み、電子契約普及の後押しになっている。

2000年に成立したIT関連法で公共調達や公共入札で電子署名が活用されるようになり、建設工事の請負契約に電子契約が利用され、さらに2014年にJIPDEC他による「電子契約元年プロジェクト」が始動した。

電子契約の利用は、調査開始の2015年から徐々に増加傾向となり、今回、特に在宅勤務、テレワークの影響から、電子署名の利用の有無を問わない何らかの方法で電子契約を利用している割合が拡大した（図４、５）。

電子契約導入にあたってはコスト、システム導入の手間、社内や取引先との調整などの課題が挙げられているが、いろいろな形態の電子契約サービスが出始めたことから、今後、電子契約の利用割合はさらに高まることが期待される。

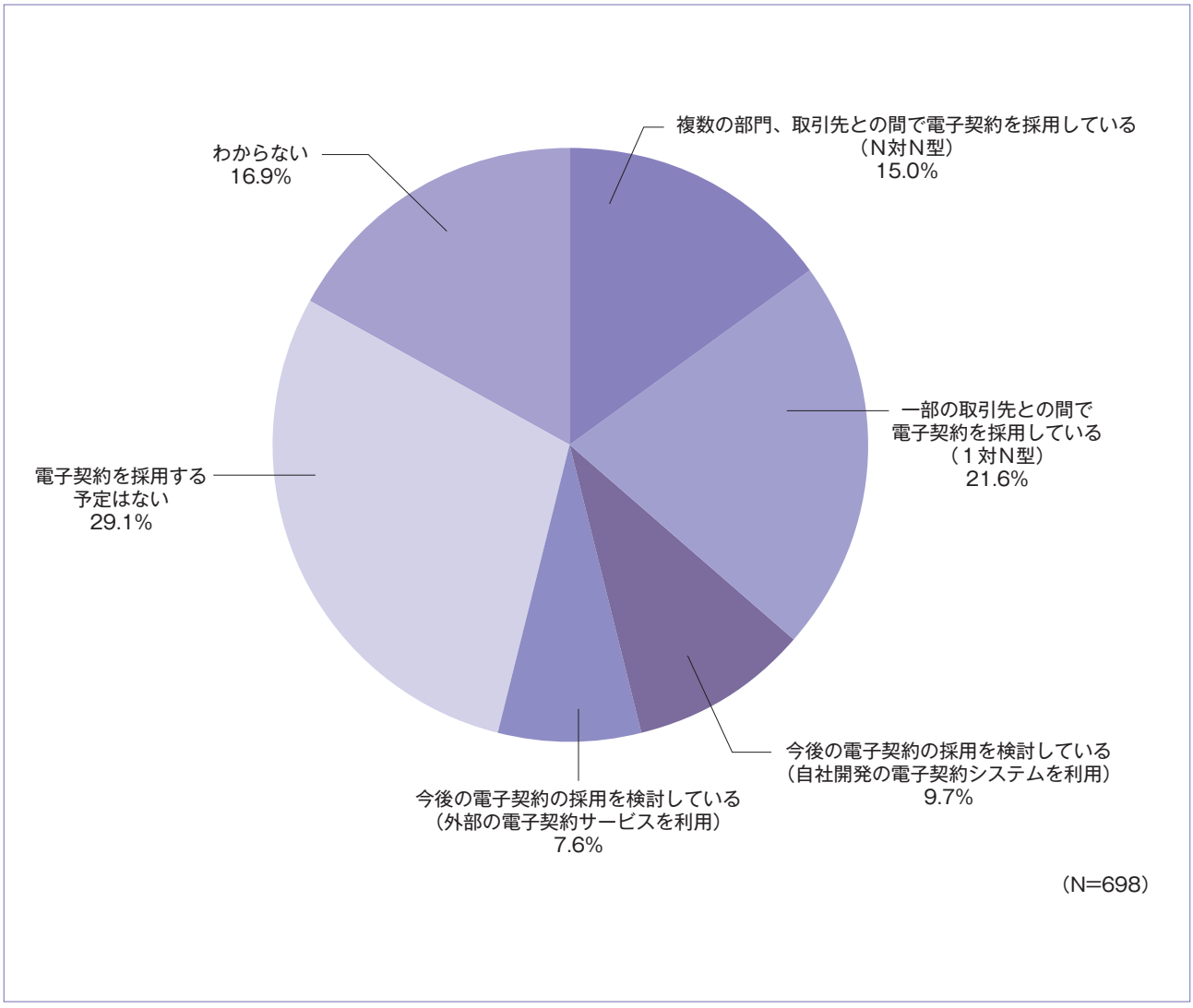


図４．電子契約の利用状況（2015年調査）

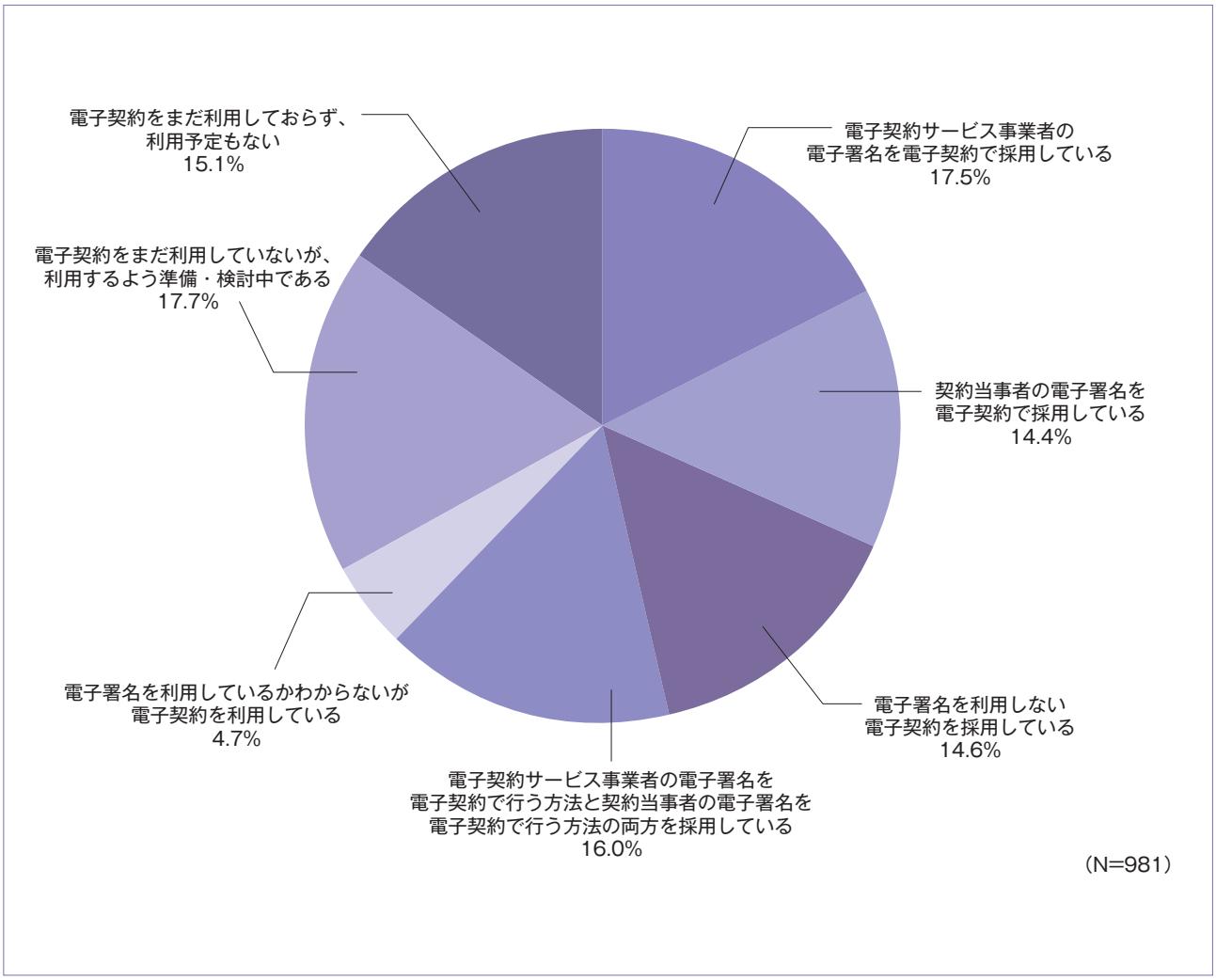


図５．電子契約の利用状況（2021年調査）

●外部へのファイル送信はPPAPが未だ主流

2020年以降、世界中で流行しているマルウェア「Emotet」がZipファイル内の文書に仕掛けられ、感染被害が拡大したことが一つの契機となり、外部への電子ファイル送信手段として長年利用されてきた、パスワード付きZipファイルを送付して別途パスワードをメールで連絡する、いわゆる「PPAP」のセキュリティリスクが問題視されるようになった。

政府が設置した「デジタル改革アイデアボックス」への国民からの多くの意見を契機に、2020年11月、平井卓也デジタル改革担当大臣が中央省庁でのPPAP廃止を宣言し、また大手ベンダ各社をはじめ民間企業でも廃止の動きが出てきている。しかし、政府が非推奨とした後の2021年調査においても未だ多くの企業が引き続き利用している結果となった（図６）。

今後、簡便で安全性の高いクラウド／オンラインストレージを利用したファイル共有などの代替手段が普及すれば、PPAPの利用をやめるなど利用状況にも変化が現れることだろう。今後の動向を引き続き注視していきたい。

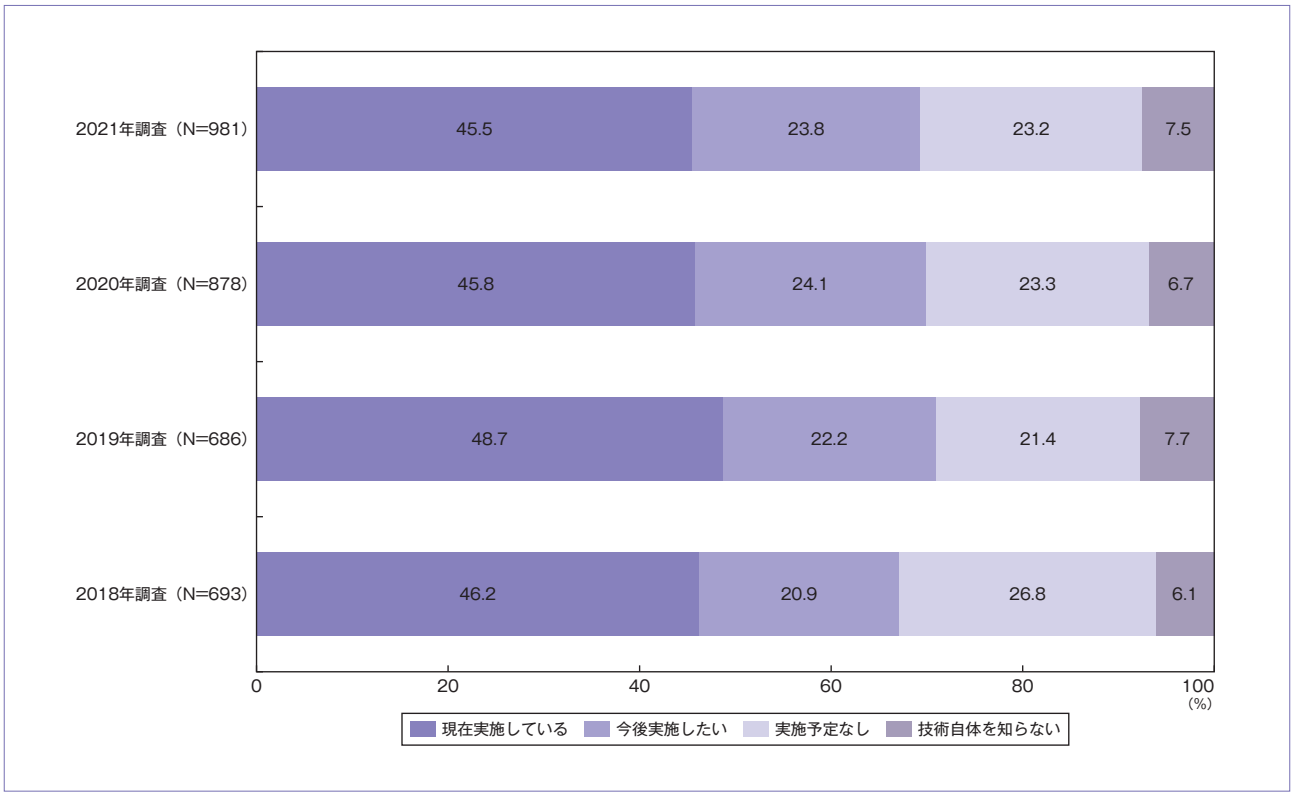


図6．電子メールの送信側セキュリティ対策－PPAP利用状況（2018-2021年比較）

2 2021年調査の概要

2-1. 調査概要

・実査期間：2021年1月13日～1月15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、営業、経理、製造・生産、研究開発、マーケティング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9,000人
・有効回答数：981件（1社1人）

2-2. 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（29.0%）、次いでサービス業（22.9%）、情報通信（15.5%）、建設・不動産（9.8%）、金融・保険（8.1%）、卸売・小売（8.0%）となった。所属部門では情報システム部門（26.3%）が最も多く、役職は課長（33.1%）、本部長・部長（32.4%）が回答の約6割を占めている。

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・製品選定に関与している」（51.3%）、「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」（46.6%）とする回答が多く、2020年調査と傾向はあまり変わっていない（巻末に詳細データ掲載）。

以下、各テーマ別に分析結果を紹介する。

3　経営における情報セキュリティの位置づけ

3-1．重視する経営課題

重視する経営課題については、全24項目の経営課題を取り上げ、今後１～３年で何を重視しようとしているかを調べた（図７）。2020年調査および追跡調査結果同様、「業務プロセスの効率化」（50.8％）がトップとなり、「従業員の働き方改革」（39.1％）が２位、「情報セキュリティの強化」（38.1％）がわずかな差で３位となった。

今回調査で大きく変化があったのは「従業員の働き方改革」で、2020年調査の48.6％から39.1％へと約10ポイントの減少となった。2020年調査時点では、これから働き方改革に取り組もうとして経営課題に掲げていた企業が、コロナ禍により、課題として挙げていたテレワークの導入などを早急に実践にシフトした結果によるものと思われる。

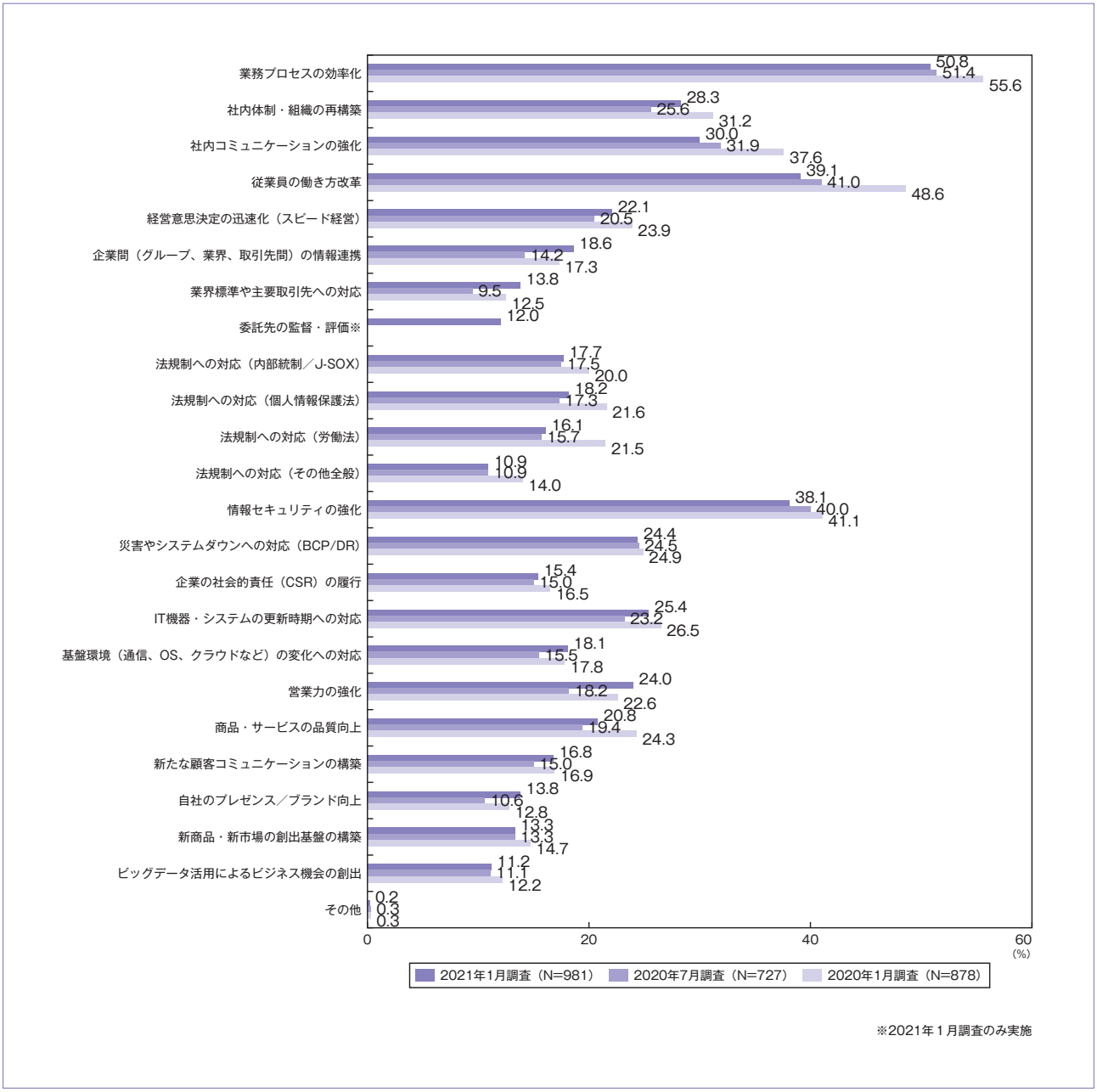


図７．今後重視したい経営課題（2020－2021年比較）（複数回答）

3-2. 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は、最も高かったのは「社内サーバー／PC／スマートフォン等のマルウェア感染」（24.3％）で、２位は「従業員によるデータ・情報の紛失・盗難」（23.2％）であった。過去２回の調査と比較すると、マルウェア感染、DDoS攻撃、クラウドサービス停止による業務中断など、セキュリティインシデントが増加傾向となった。

なお、「インシデントは経験していない」（24.2％）は過去最低となり、インシデントが増加していることを示している（図８）。

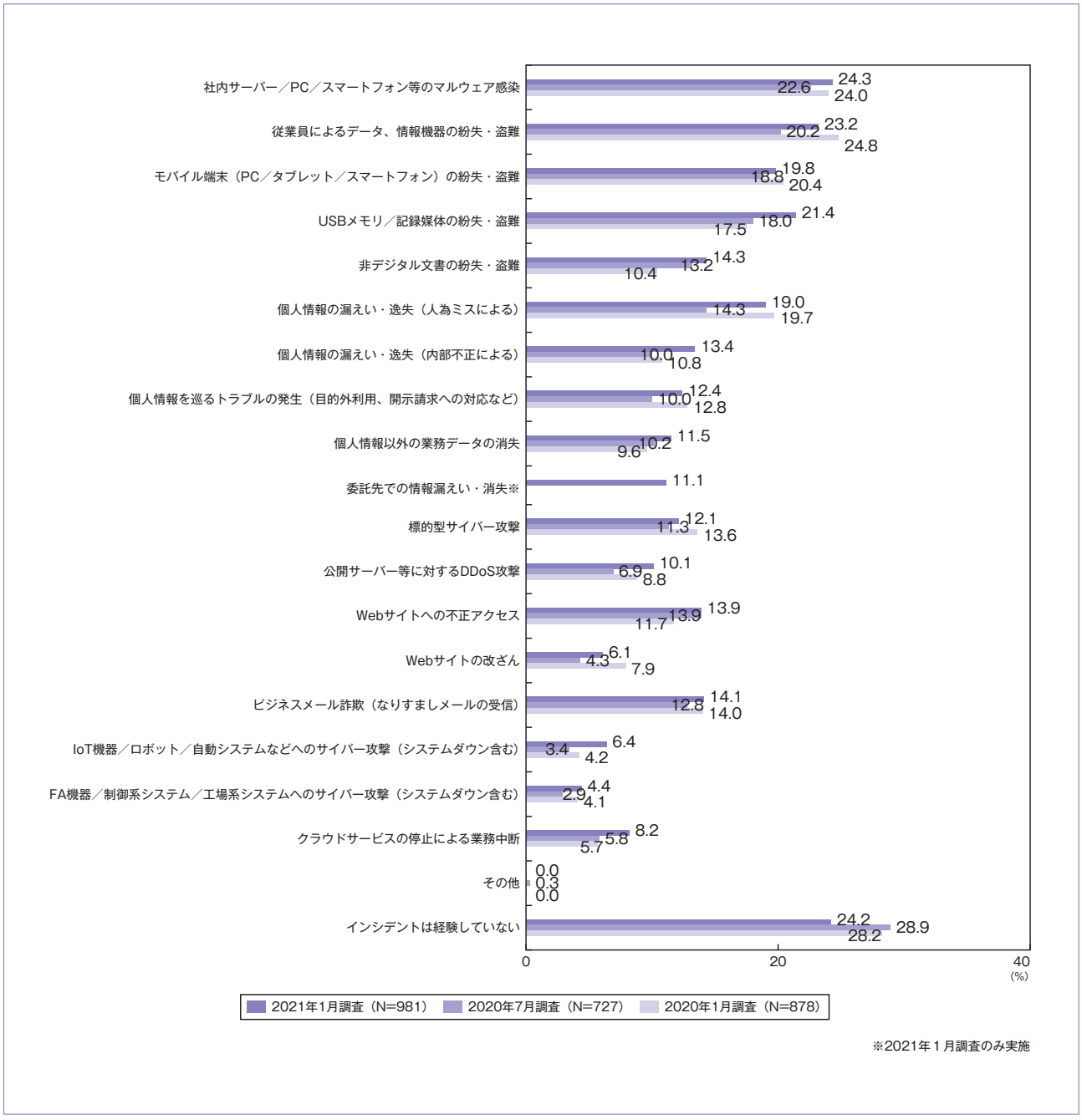
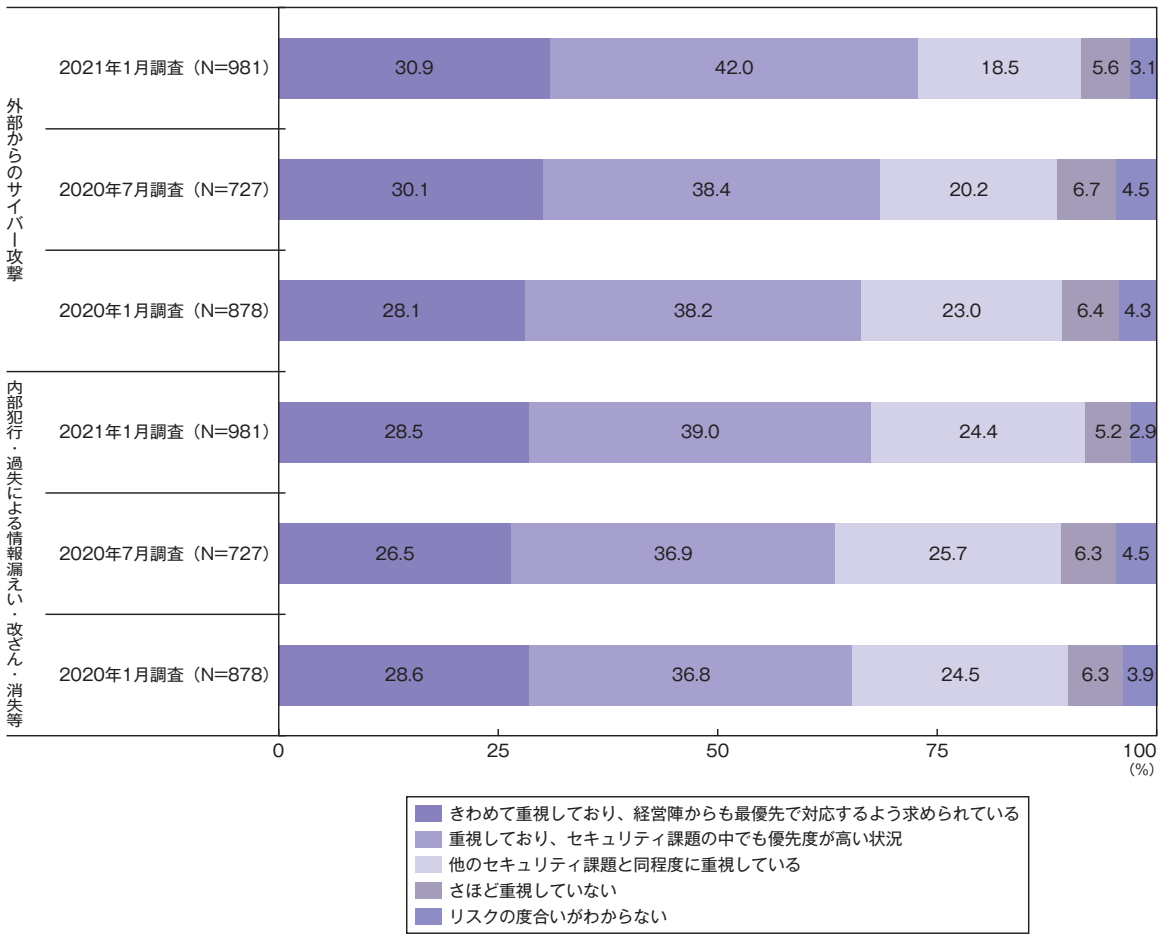


図８．過去１年間に経験したセキュリティインシデント（2020-2021年比較）

3-3. セキュリティリスクの重視度合い

本調査において、「外部からのサイバー攻撃」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、昨年同様の結果となった（図９）。

なお、外部からのサイバー攻撃については、「重視しており、優先度が高い」までを含めると、初めて７割を超え、対応優先度が高いリスクとして認識されていることがわかる。国内外を問わず、毎年標的型サイバー攻撃による大規模情報漏えい事件が発生し、その影響により業務停止、信用失墜に発展しかねない状況において、企業全体として外部からのサイバー攻撃対応を重視し、優先的に対応すべきとの考えが浸透してきていると考えられる。



注）2020年は「標的型サイバー攻撃」に対する回答

図９．セキュリティリスクの重視度合い（2020-2021年比較）

3-4. セキュリティ対策の実施状況

具体的なセキュリティ対策はどのように実施されているのか。この調査では、「外部からの攻撃対策」「情報漏えい対策」として、代表的な取組みを取り上げ、その実施率についても観測している。

「外部からの攻撃対策」として最も実施率が高かったのは「重要なシステムのインターネットからの隔離」（47.9%）で、２位は「PCの管理者権限の制御」（47.7%）であった（図10）。

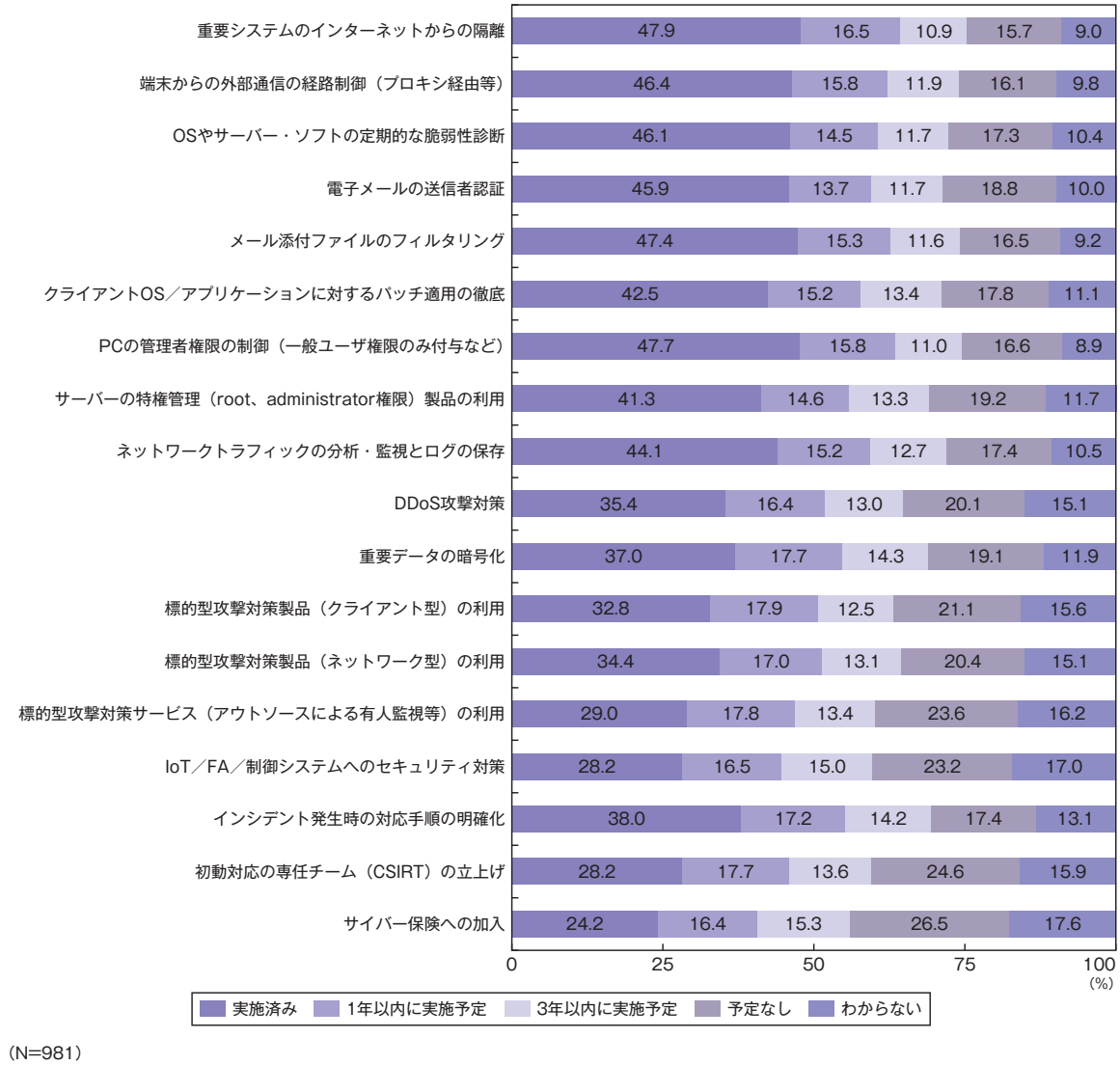


図10. 主要な「外部からの攻撃対策」の実施状況

一方、「情報漏えい対策」としては、昨年に続き「重要情報にアクセスできる人員（部署）の制限」（50.6%）の実施率が最も高く、「重要情報の取扱責任者の任命」（49.7%）、「重要情報の定義・特定、他の情報資産との分類」（49.3%）が続いている（図11）。

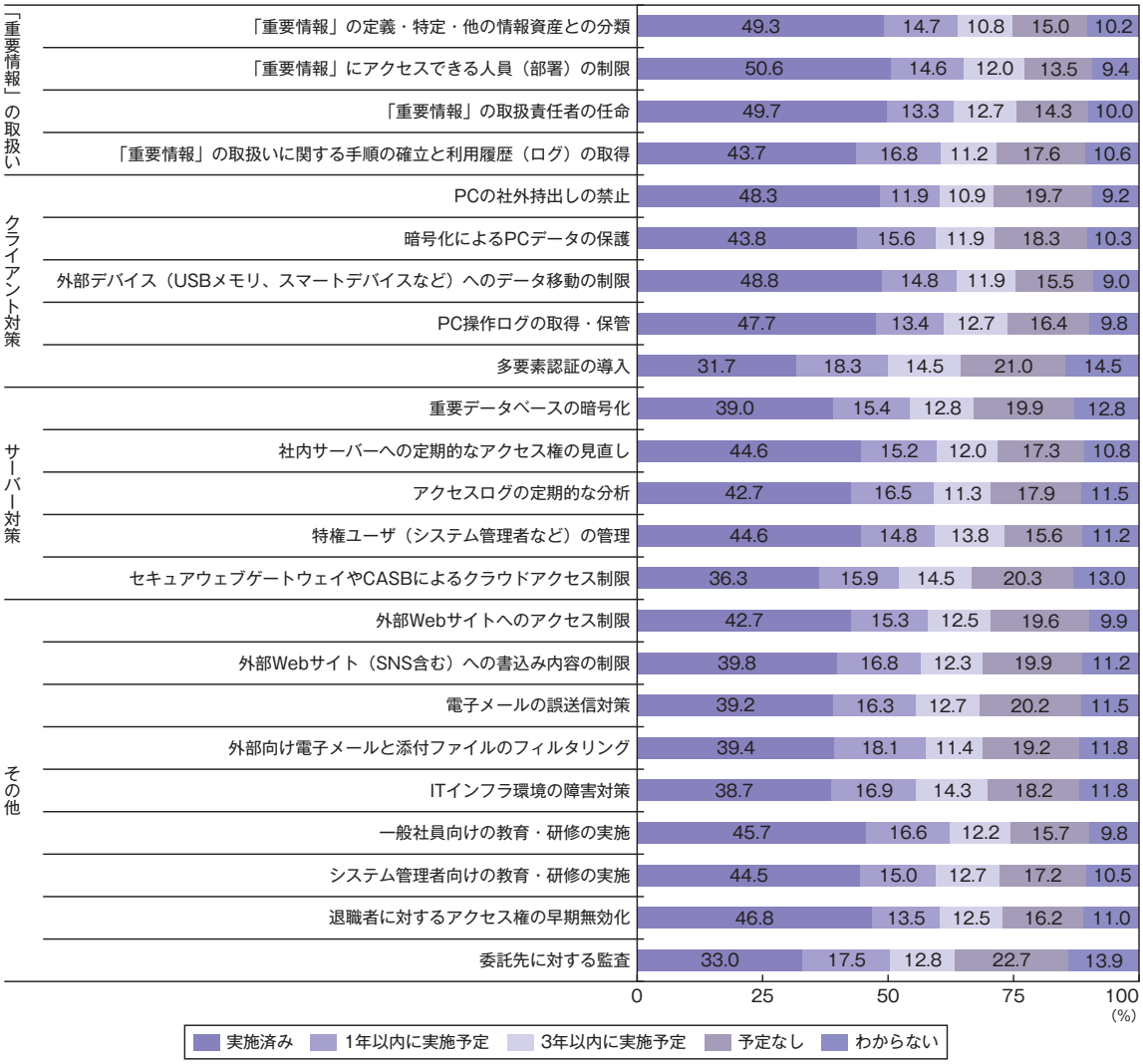


図11．主要な「情報漏えい対策」の実施状況

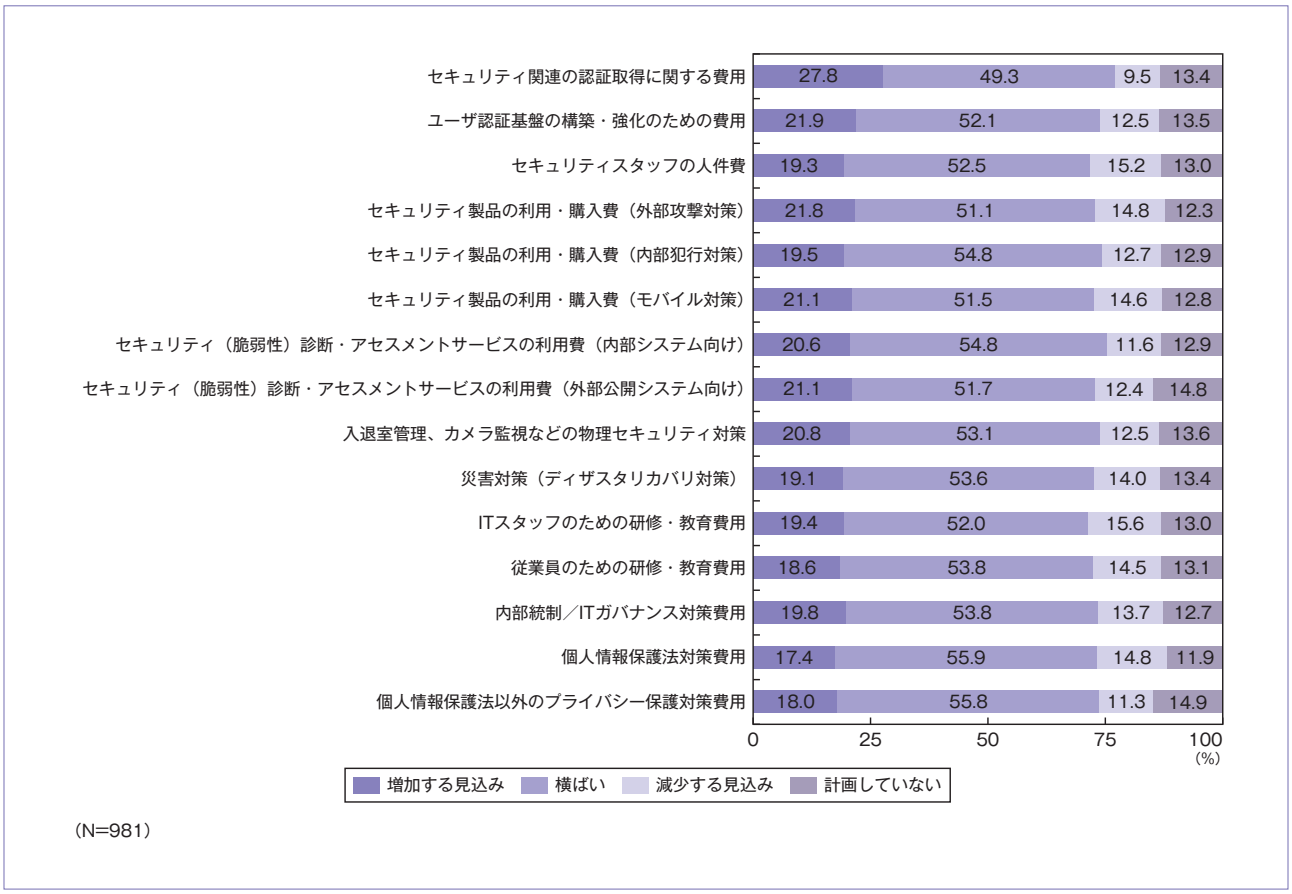
3-5．セキュリティ支出の動向

セキュリティ支出の増減動向については、例年同様、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、コロナ禍の影響によるセキュリティ関連費用の実績と、2020年度と比較した2021年度支出計画の状況を調査した（図12）。

コロナ禍対策に伴い、実績・計画ともに各項目において若干の増加傾向となり、「増加する見込み」と回答した企業の割合は全項目とも17％を越えている。支出実績で最も高かったのは「セキュリティ関連の認証取得に関する費用」（27.8％）で、次いで「ユーザ認証基盤の構築・強化のための費用」（21.9％）であった。

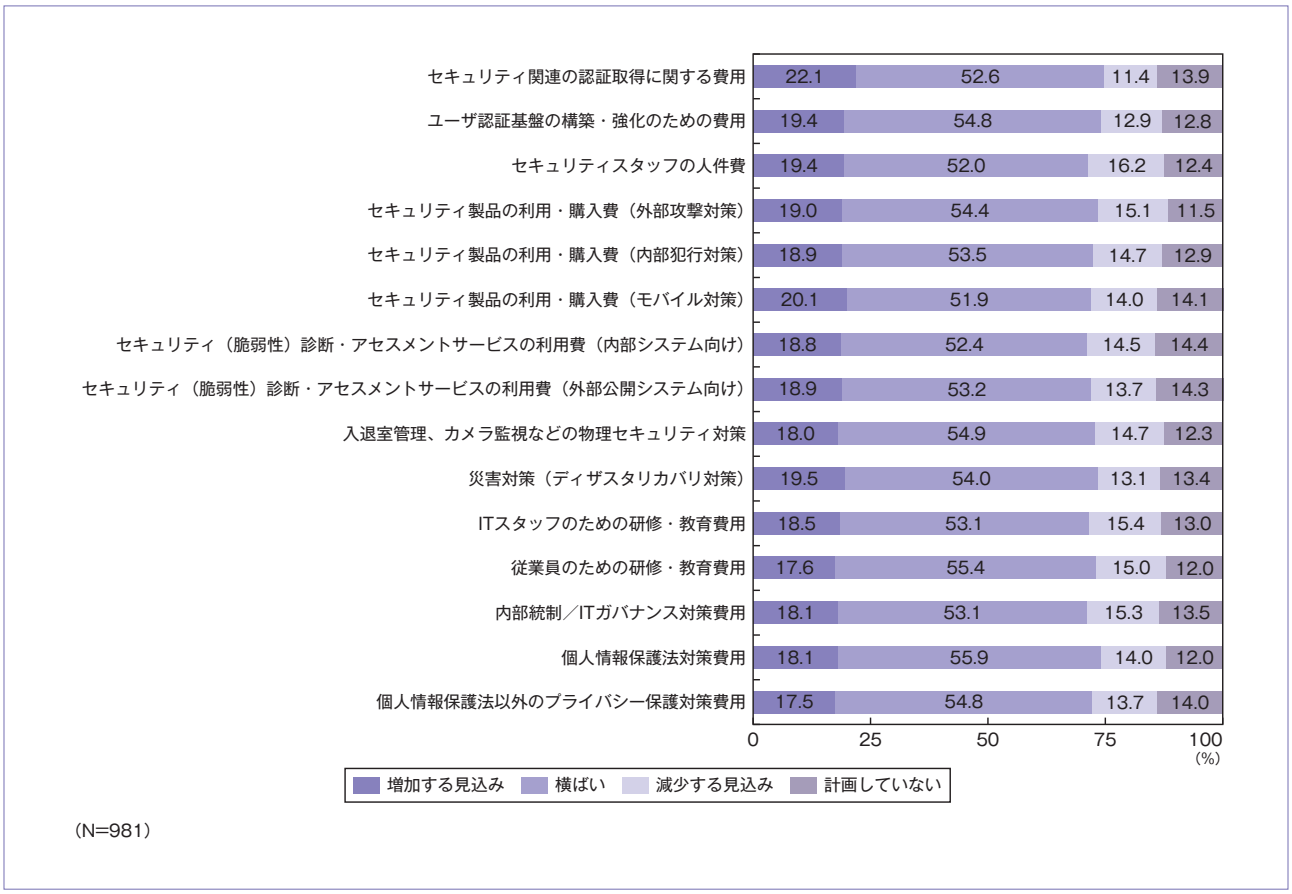
また、全項目ともに「横ばい」がほぼ５割を占め、「減少」が１割前後となっており、横ばいが多い中で認証取得とセキュリティ製品の導入が増加する傾向となっている。

一方、2020年度と比較した支出計画については、全項目で増加が約２割、横ばいが約５割となった（図13）。



(N=981)

図12.　コロナ禍による2021年度のセキュリティ関連費用支出実績



(N=981)

図13.　2020年度と比較した2021年度のセキュリティ関連費用支出計画

4　認定／認証制度に対する意識

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」があり、その一環として、第三者による客観的な視点により自社の取組み状況を確認できる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や取引先から信頼を得ることも大きい。そこで、本章では、システムリスク軽減策への取組み状況、認定／認証制度の取得目的、価値と、コロナ禍が認証取得にどのように影響を与えたかを調査した。

4-1. 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、実施済みで５割を超えたのは、昨年同様、「リスクマネジメントの構築」（56.4％）、「事業継続計画（BCP）の策定」（54.5％）、「セキュリティポリシーの策定」（53.0％）、「ITガバナンスの確立」（50.4％）となり、「ITサービスマネジメントの実施」は44.6％が実施済となった（図14）。

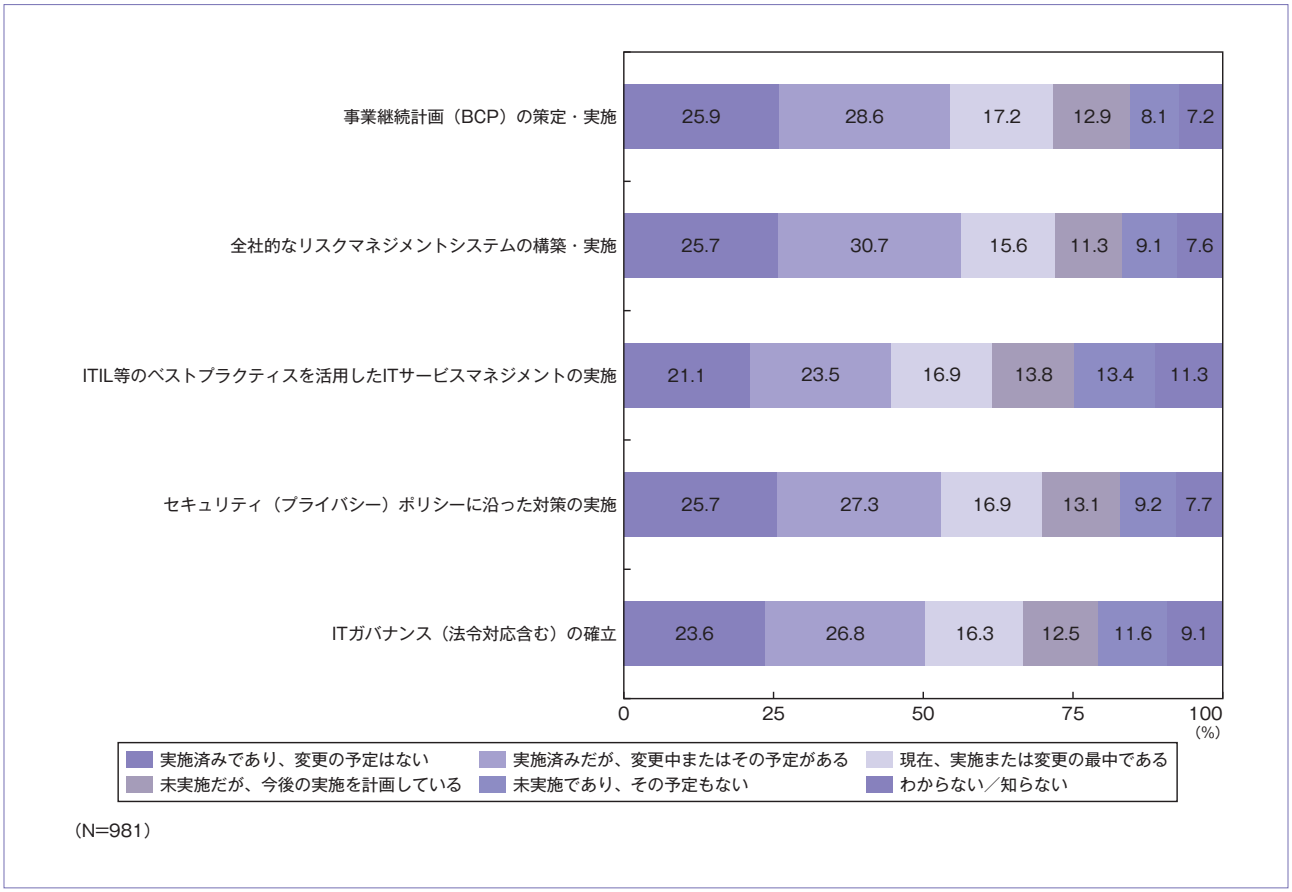


図14.　システムリスク軽減策の取組み状況

4-2. 第三者から認定／認証を取得することの価値・効果

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」（51.2％）が最も多かった。次は「社内の情報セキュリティ体制を高度化させるため」（45.0％）で、「消費者からの信頼を得るため」（38.2％）が続いている（図15）。

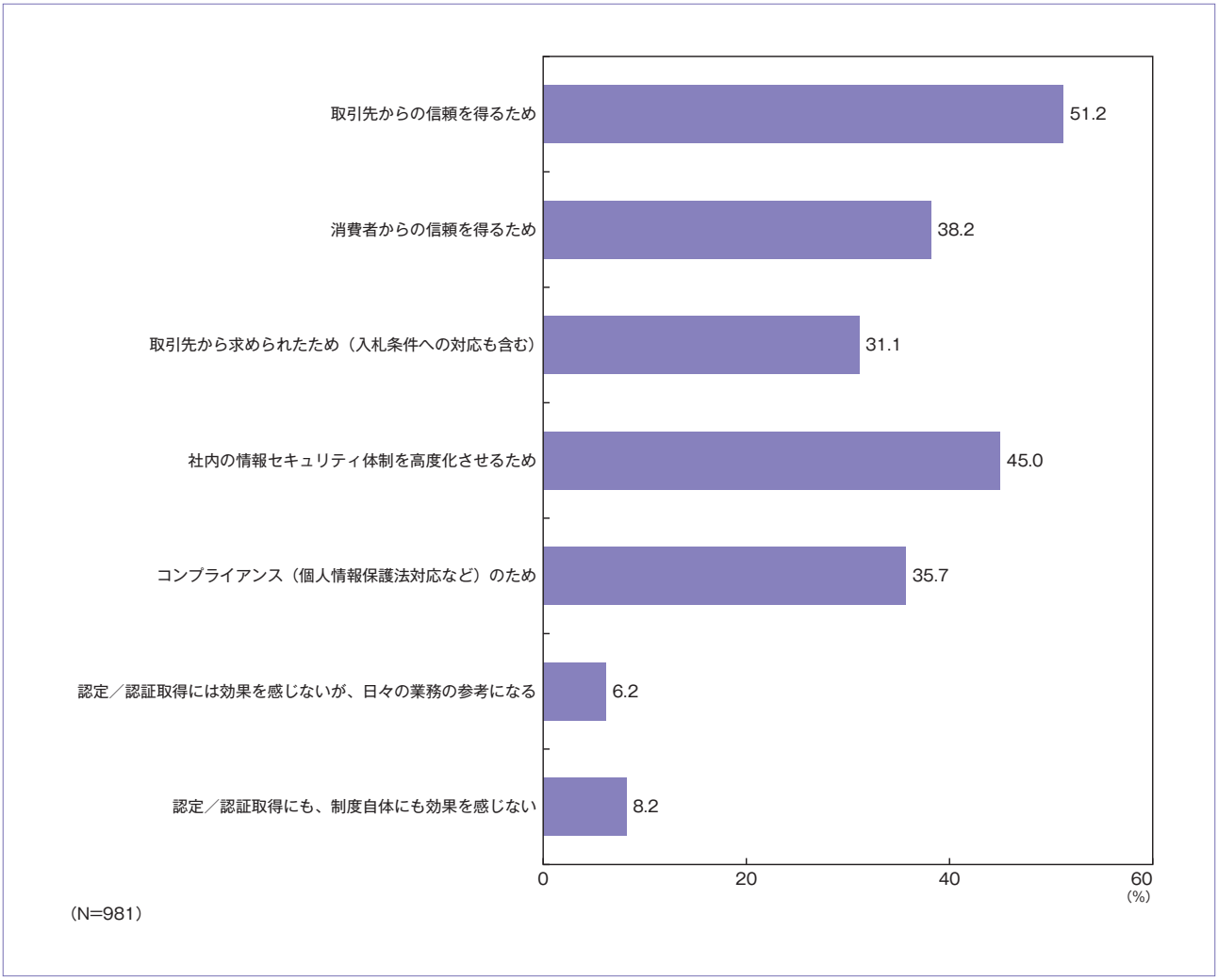


図15. 第三者から認定／認証を取得することの価値・効果

4-3. コロナ禍対策に伴うプライバシーマーク制度／ISMS評価制度の取引先評価時の重視度

コロナ禍により業務体制に変化が見られ、これまで社内でのみ処理していた業務を在宅勤務やクラウドサービスを利用するなどで従来の業務体制が変わった企業も増えてきている中、セキュリティ面を重視して取引先選定を行う際、プライバシーマークを取得していることを６割超の企業が重視していることがわかった（図16）。

また、ISMS評価制度についても６割近い企業が重視していることがわかった（図17）。

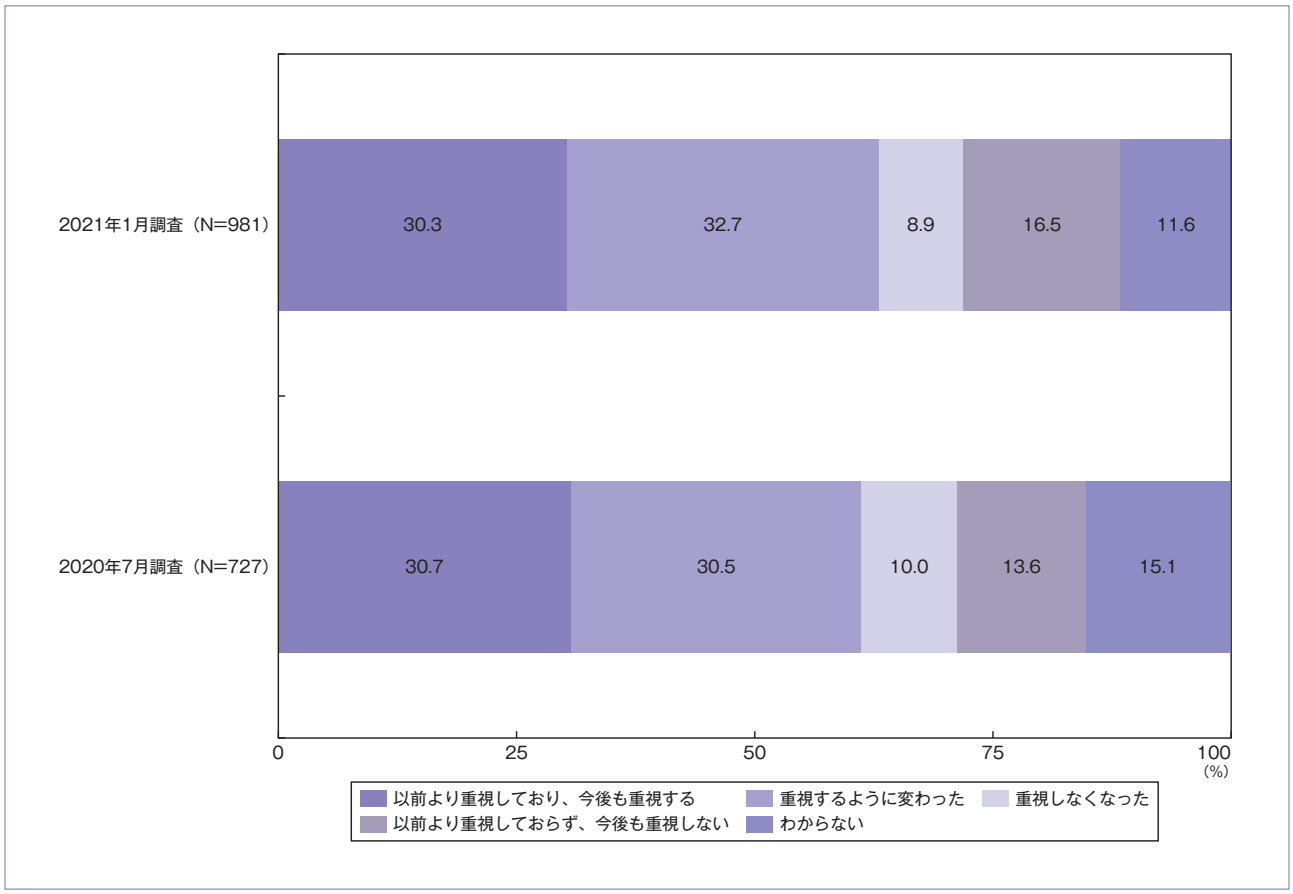


図16.　コロナ禍に伴うプライバシーマーク制度の取引先評価時の重視度

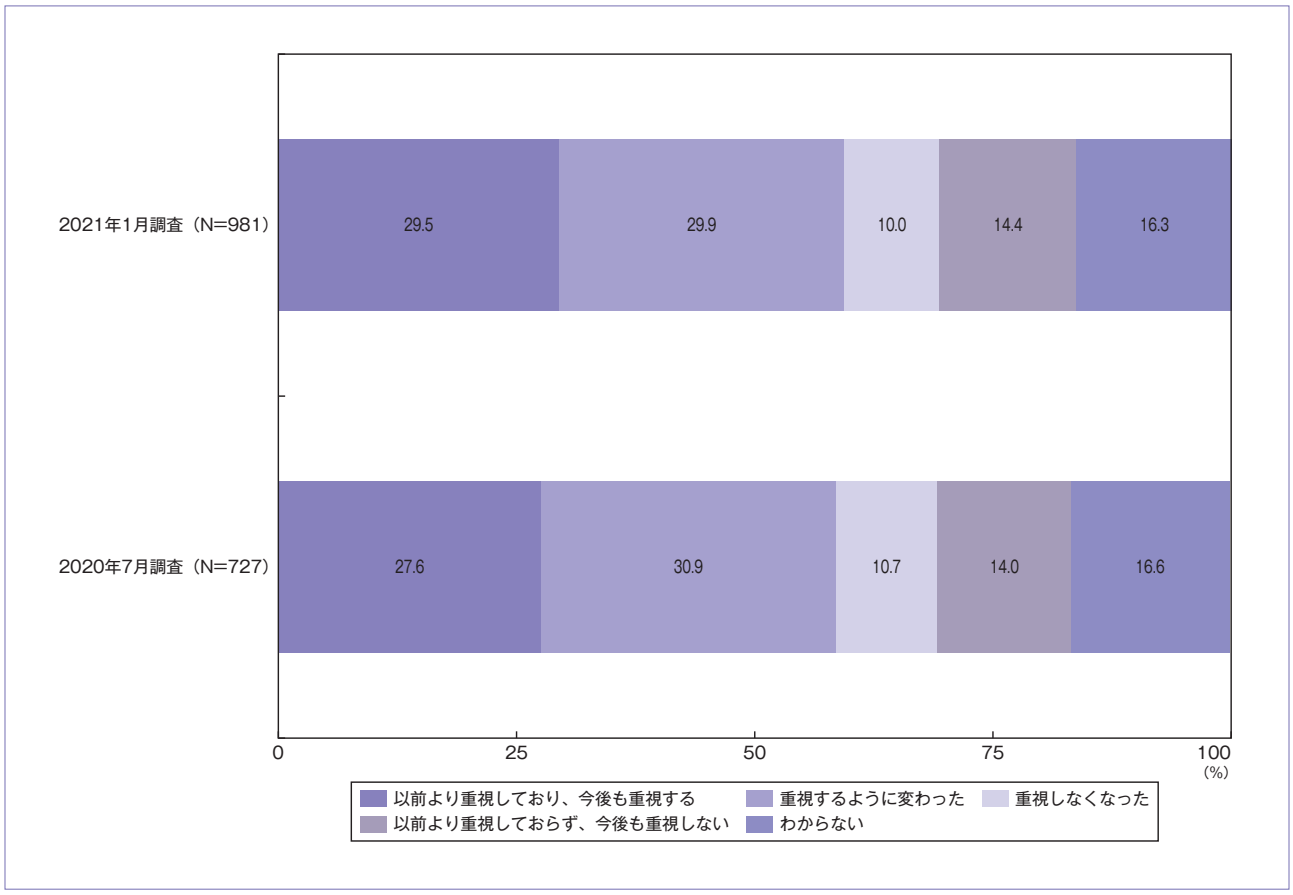


図17.　コロナ禍に伴うISMS評価制度の取引先評価時の重視度

5　プライバシーガバナンス

EUが2018年５月からGDPRを運用開始し、2019年１月には日本とEU間での十分性認定合意により、個人情報保護法とGDPR補完ルールを遵守することで、日－EU間のデータ移転が可能となった。今回の調査では、現在の日本企業のGDPRへの対応状況、および2020年８月に経済産業省と総務省から公表された「プライバシーガバナンスガイドブック Ver1.0」の認知度を調査した。

5-1．国内におけるGDPR対応状況

国内法規制以外でEU圏の法を準拠する立場にある企業のGDPR対応状況は、「現在、個人データを移転できるようGDPR対応中（対応検討中を含む）」が26.1％、「GDPRの存在は知っているが、EU（EEA）との個人データの移転がないので対応していない」（19.0％）、「現地法人が対応しているので日本法人とのデータ移転はない」（13.4％）となっており、標準契約条項（SCC）や拘束的企業準則（BCR）を締結するケースは少ない（図18）。

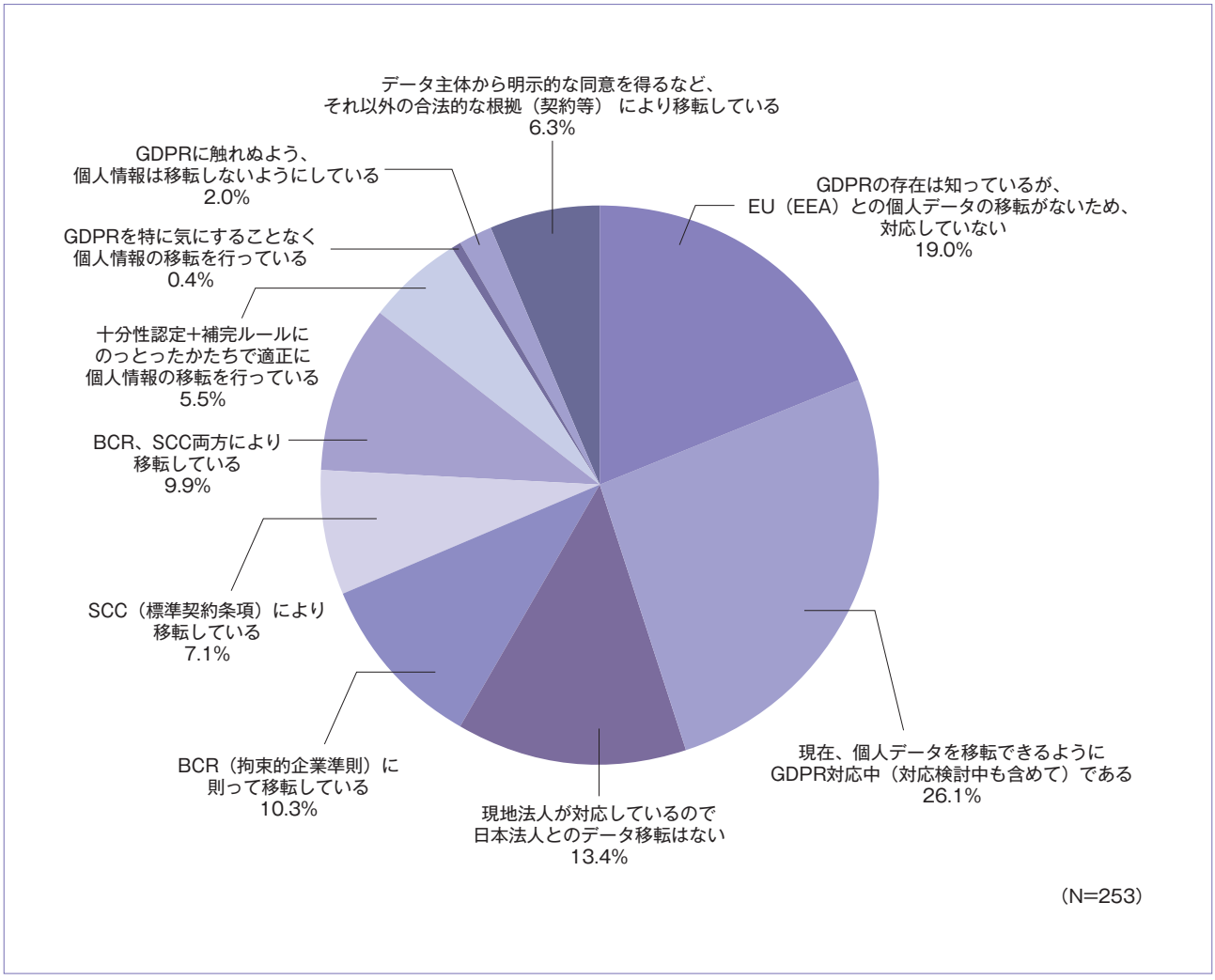


図18．国内のGDPR対応状況

5-2. プライバシーガバナンスについての課題認識

プライバシーガバナンスの課題として認識されているのは、「企業内の体制構築が不十分」（32.3%）、次いで「企業内のルール策定が不十分」（29.9%）と、企業内でのプライバシーガバナンスの仕組みがまだ十分に構築されていないことがわかった（図19）。

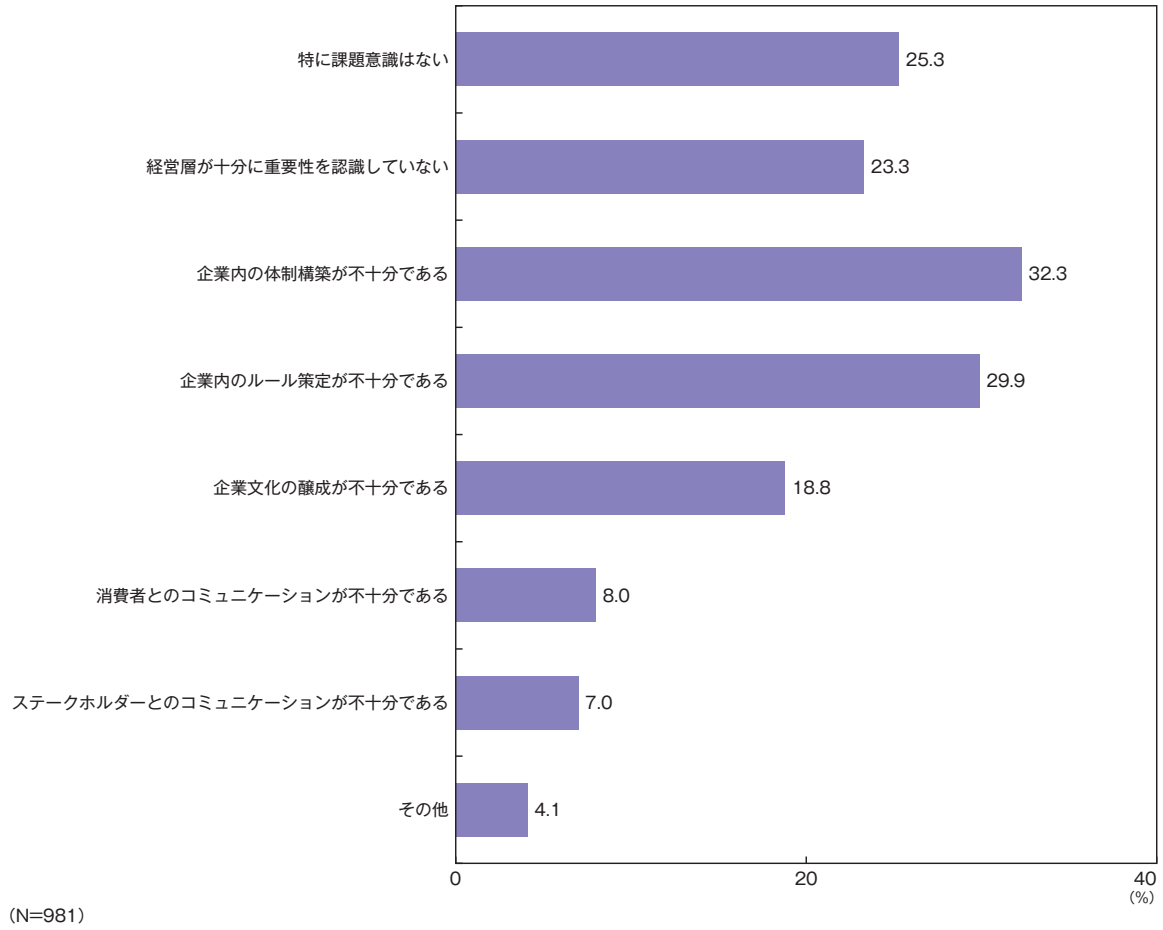


図19. プライバシーガバナンスについての課題認識

5-3. プライバシーガバナンスガイドブックの認知度

2020年８月に経済産業省／総務省が公表した「DX時代における企業のプライバシーガバナンスガイドブックver1.0」の認知度について、「知っている」が60.6％となったが、このうち、約４割が「活用している」または「活用予定」と回答した（図20）。

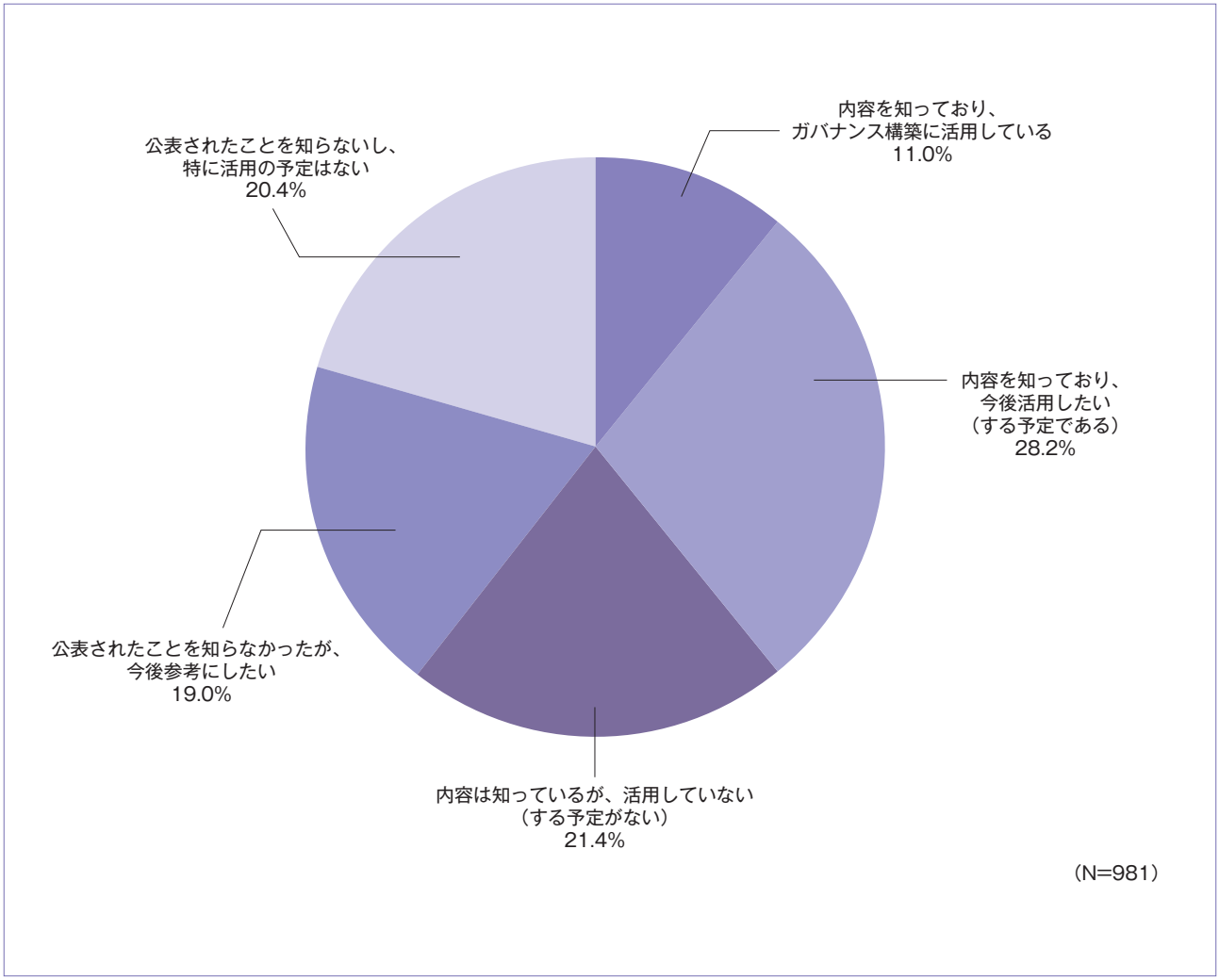


図20.「プライバシーガバナンスガイドブックver.1.0」の認知度

6　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／技術も進化してきており、利用シーンにおいても従来のオンプレミス用製品からクラウド用製品への移行が始まっている。

6-1．ネットワーク／ゲートウェイ製品の利用状況

ネットワーク／ゲートウェイ系のセキュリティ製品では、これまで境界防御型のオンプレミス製品だったが、社内システムのクラウド環境への移行に伴い、ゼロトラストネットワーク向けのクラウド製品に移行が始まっている（図21）。

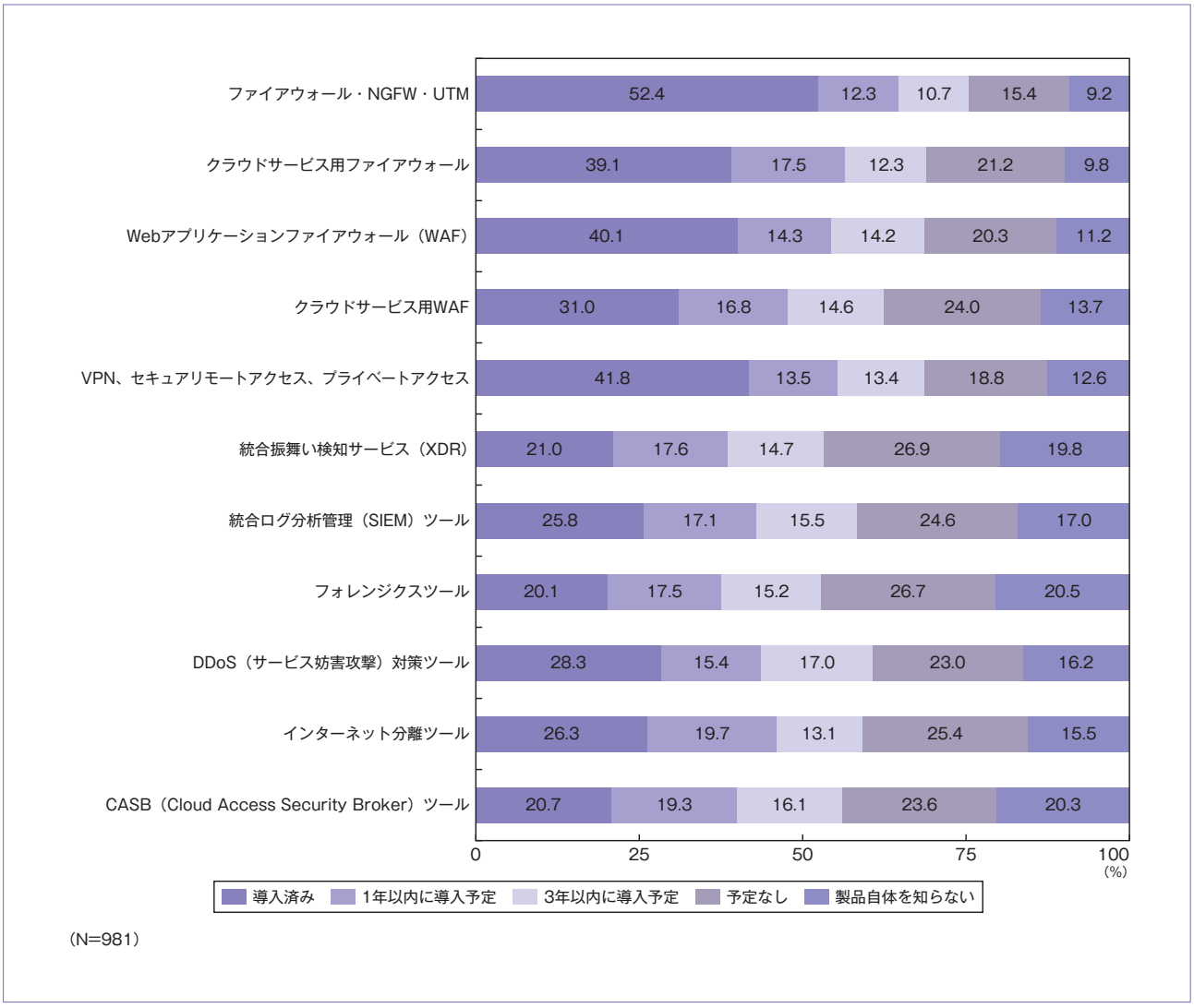


図21．ネットワーク／ゲートウェイセキュリティ製品の利用状況

6-2. 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、従来のウイルス対策ソフトの導入比率が低下する一方、次世代型ウイルス対策ソフトであるEDRが少しずつ伸びてきており、世代交代が進みつつある（図22）。

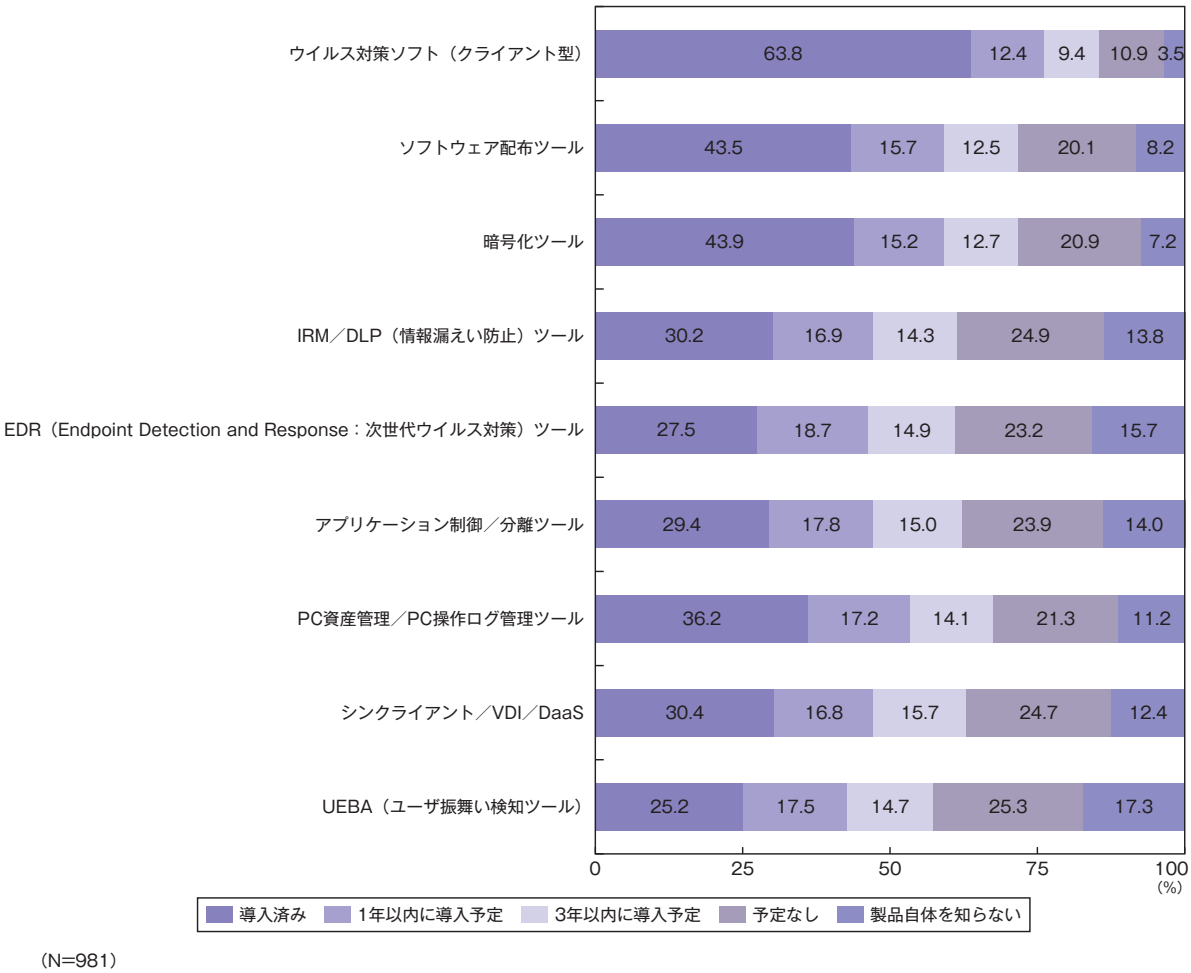


図22. エンドポイントセキュリティ製品の利用状況

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については、サイバー攻撃が増加していることを受けて、「脆弱性診断サービス」や「侵入検知サービス」の増加が見られた。また攻撃の高度化・複雑化を反映してセキュリティ運用を専門の業者にアウトソーシングする「SOCサービス」や、被害が発生した時のための「サイバー保険」への加入が増加している（図23）。

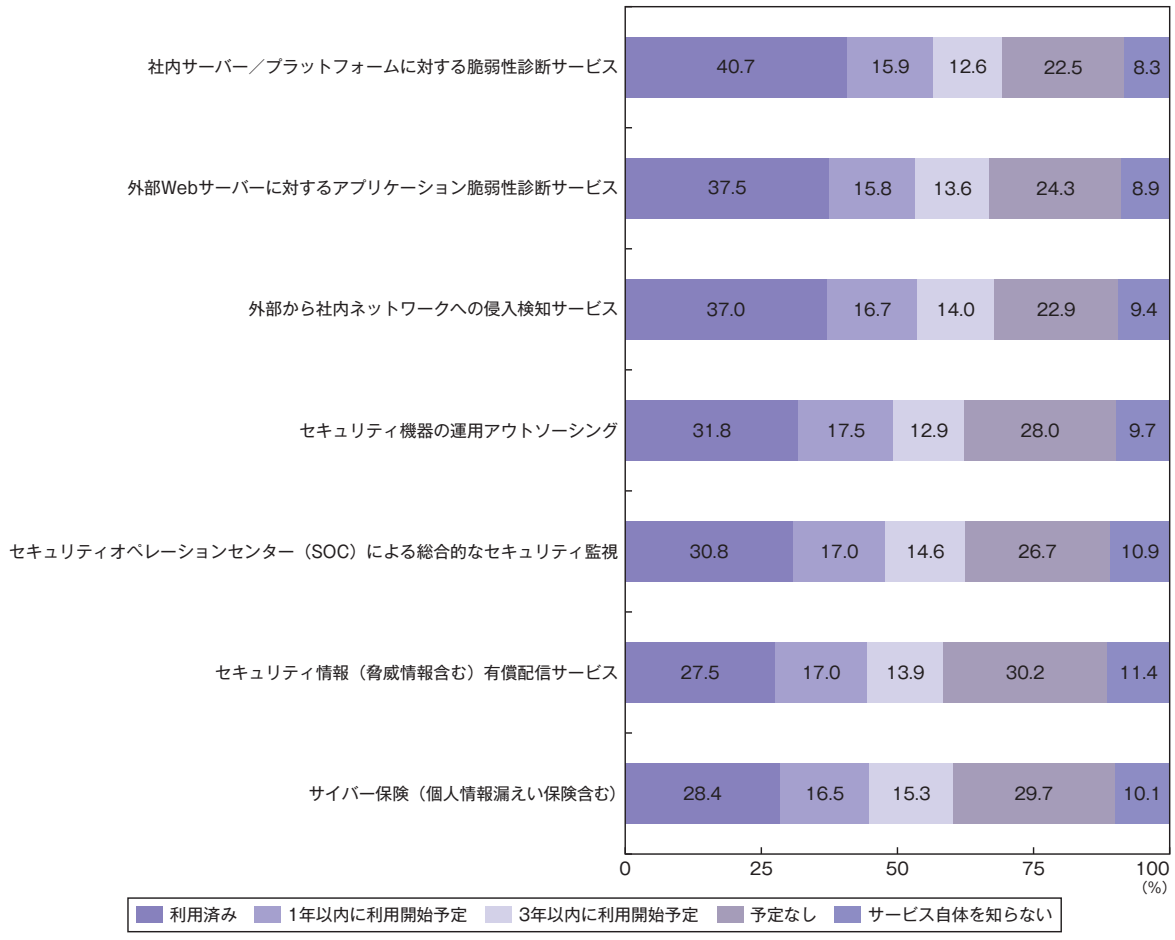
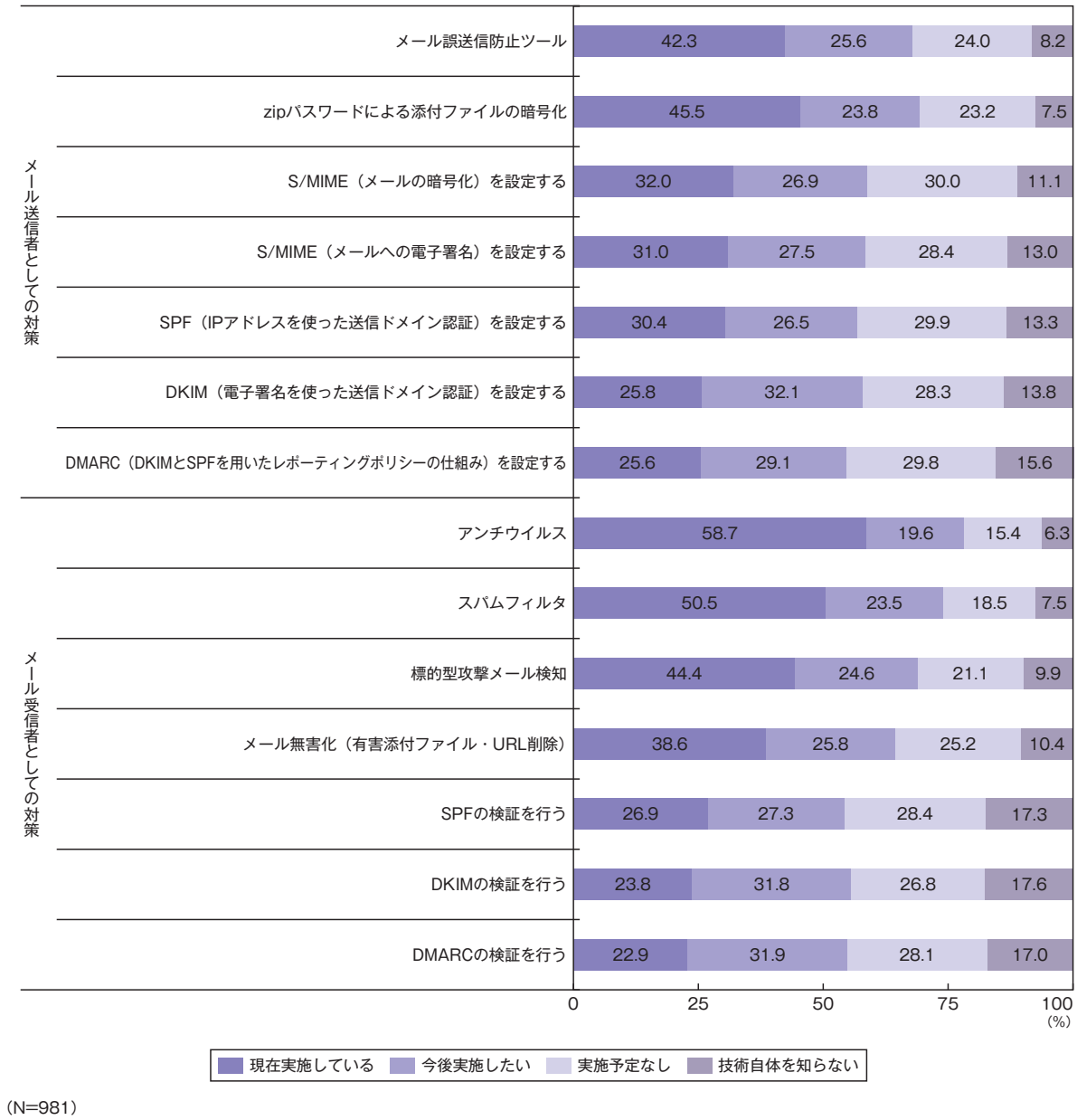


図23. セキュリティサービスの利用状況

6-5. 電子メールのセキュリティ対策

電子メールのセキュリティ対策は、送信側については政府非推奨となった「Zipパスワードによる暗号化添付ファイル」（45.5%）が最も多く、次が「メール誤送信防止ツール」（42.3%）で、受信側では「アンチウイルス」（58.7%）と「スパムフィルタ」（50.5%）となり、前回同様の結果となっている（図24）。



（N=981）

図24. 電子メールのセキュリティ対策状況

6-6. 高機密システムへのアクセス認証手段

現在利用している認証手段としては「ID・パスワード」（81.4%）が最も多いが、減少に転じつつある。代わりに今後利用したい手段としては「生体認証」（30.4%）や「多要素認証」（27.7%）、「IDaaS（クラウドID認証サービス）」（24.6%）が増えつつある（図25）。

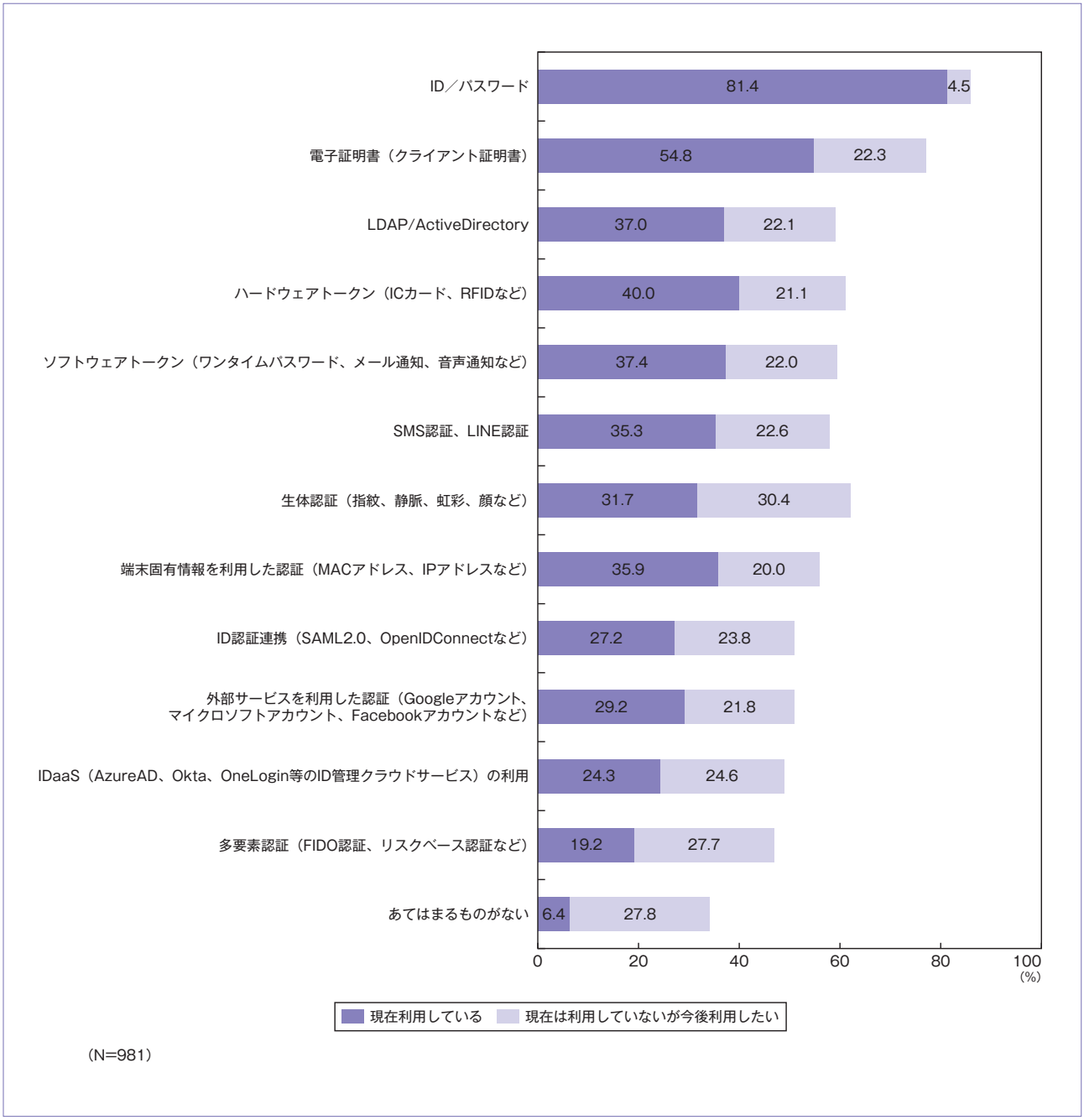


図25. 高機密性システムへのアクセス認証手段

7　働き方改革とクラウドの動向

2019年の働き方改革法の成立によって本格化した働き方改革は、コロナ禍におけるテレワーク常態化によって、勤務制度や関連するシステムの整備が大きく進み、クラウドサービス利用も増加した。

7-1. 働き方改革の取組み状況

働き方改革は、すべての項目で「実施中」と「検討中」が増加し、あわせて５割を超えており、取組みは本格化している（図26）。

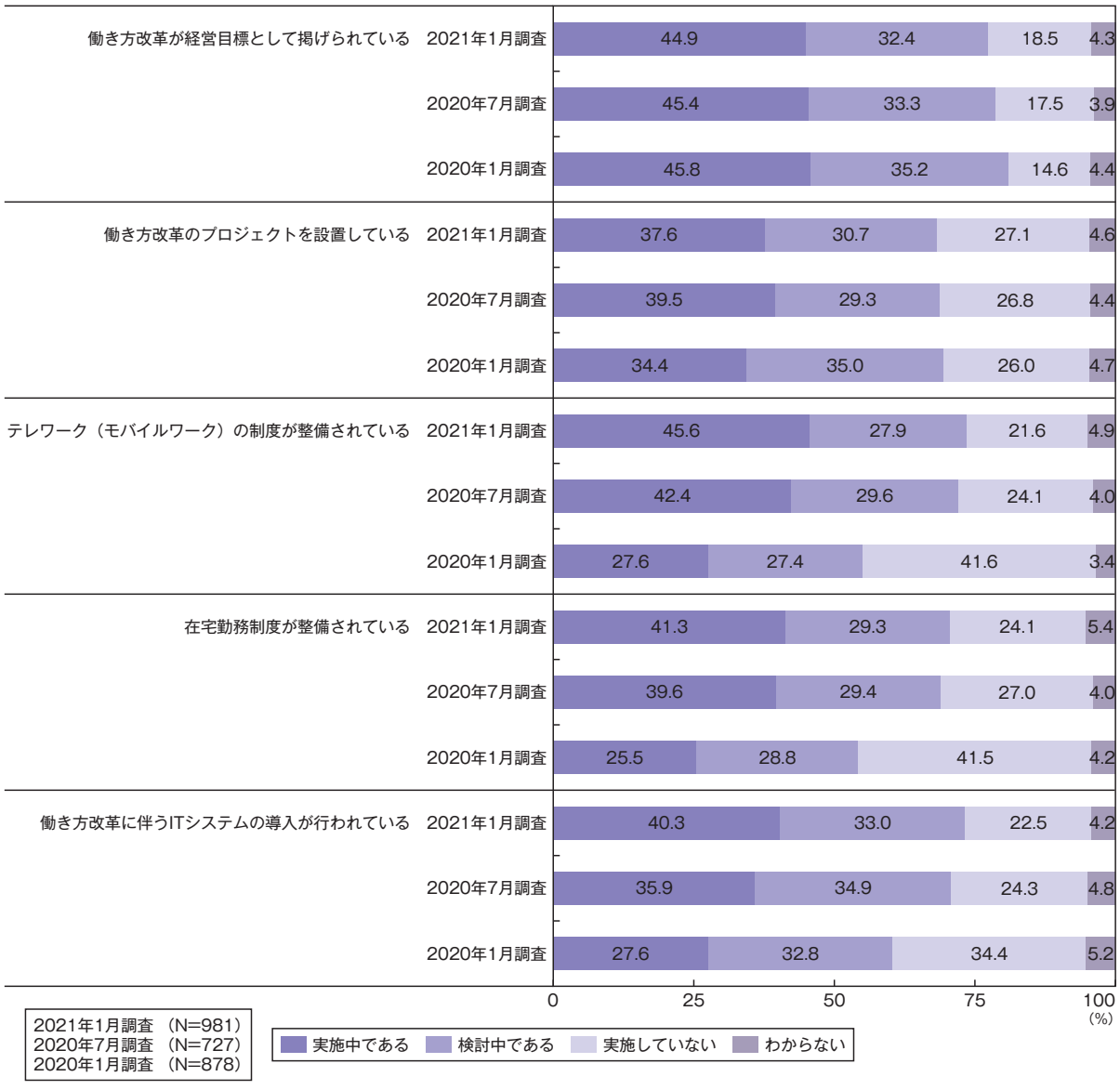


図26.「働き方改革」に関する取組み状況（2020-2021年比較）

7-2. ワークスタイルに関連する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セキュリティ面の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」（50.8%）がトップで、「法人向けクラウドサービスの利用」（44.4%）や「法人向けコミュニケーションツールの利用」（44.3%）が続いている（図27）。

なお、「法人向けコミュニケーションツールの利用」や「在宅勤務、テレワーク用のセキュリティ規程の整備と教育」は、2020年１月調査から７月調査に大幅に増加したが、今回調査ではほとんど変化が見られなかった。

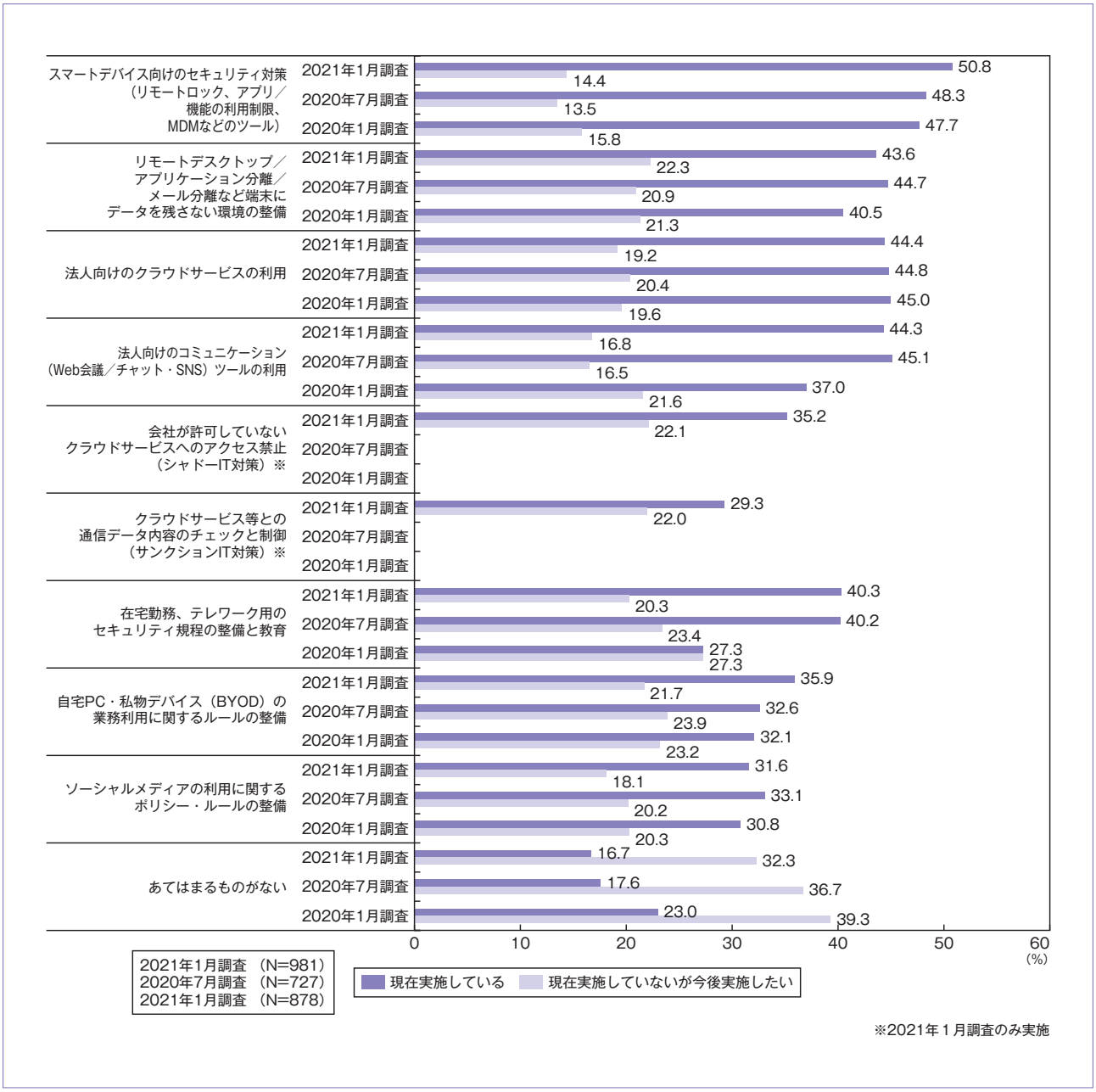


図27. ワークスタイルに関連するセキュリティ対策の取組み状況（2020-2021年比較）

7-3. クラウドサービスの利用状況

働き方改革を進めるうえで、重要なポイントとなるクラウドサービスの利用状況について調査を行った。

クラウドサービスの利用率は年々増加傾向にあり、今回調査では85.8％がクラウドサービスを利用していると回答し、そのうち、半分以上クラウドサービスを利用している比率が５割に近づきつつある（図28）。

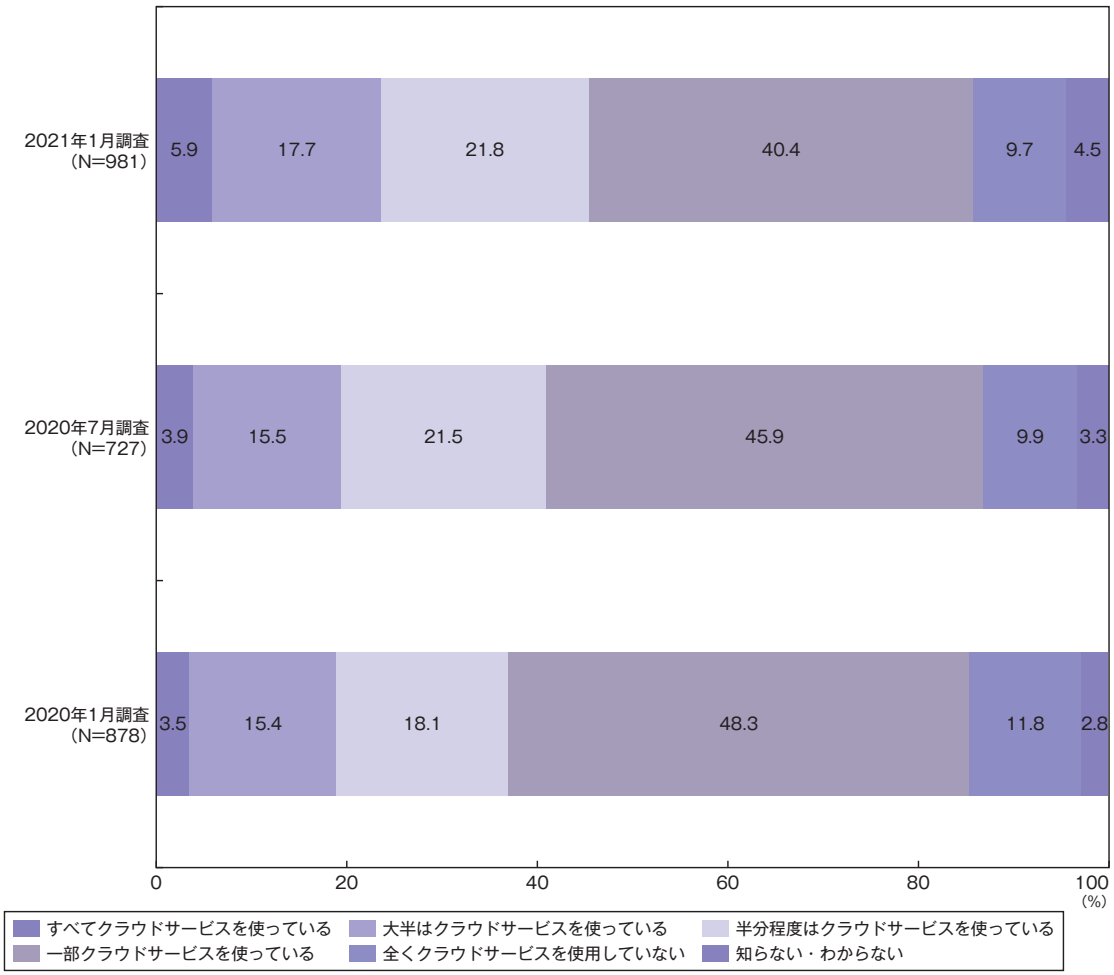


図28. クラウドサービスの利用状況（2020-2021年比較）

7-4. クラウドサービスの選定ポイント

クラウドサービスを選定する場合、どのような点に重点を置くのか調査した結果では、2020年に引き続き「コスト」（49.2%）が１位となり、次いで「セキュリティ認証・認定取得による信頼性の確保」（41.6%）、「セキュリティの対策」（41.3%）となった。各年で割合に差は生じているが、選定の際に重視するポイントの順位に変化は見られなかった（ここでは上位10項目について紹介している）。

なお、2020年１月調査と比較すると、「BCP対応がしっかりしている」「障害対応が明記されている」がいずれも約４ポイント増加、「コスト」が６ポイント減少した（図29）。

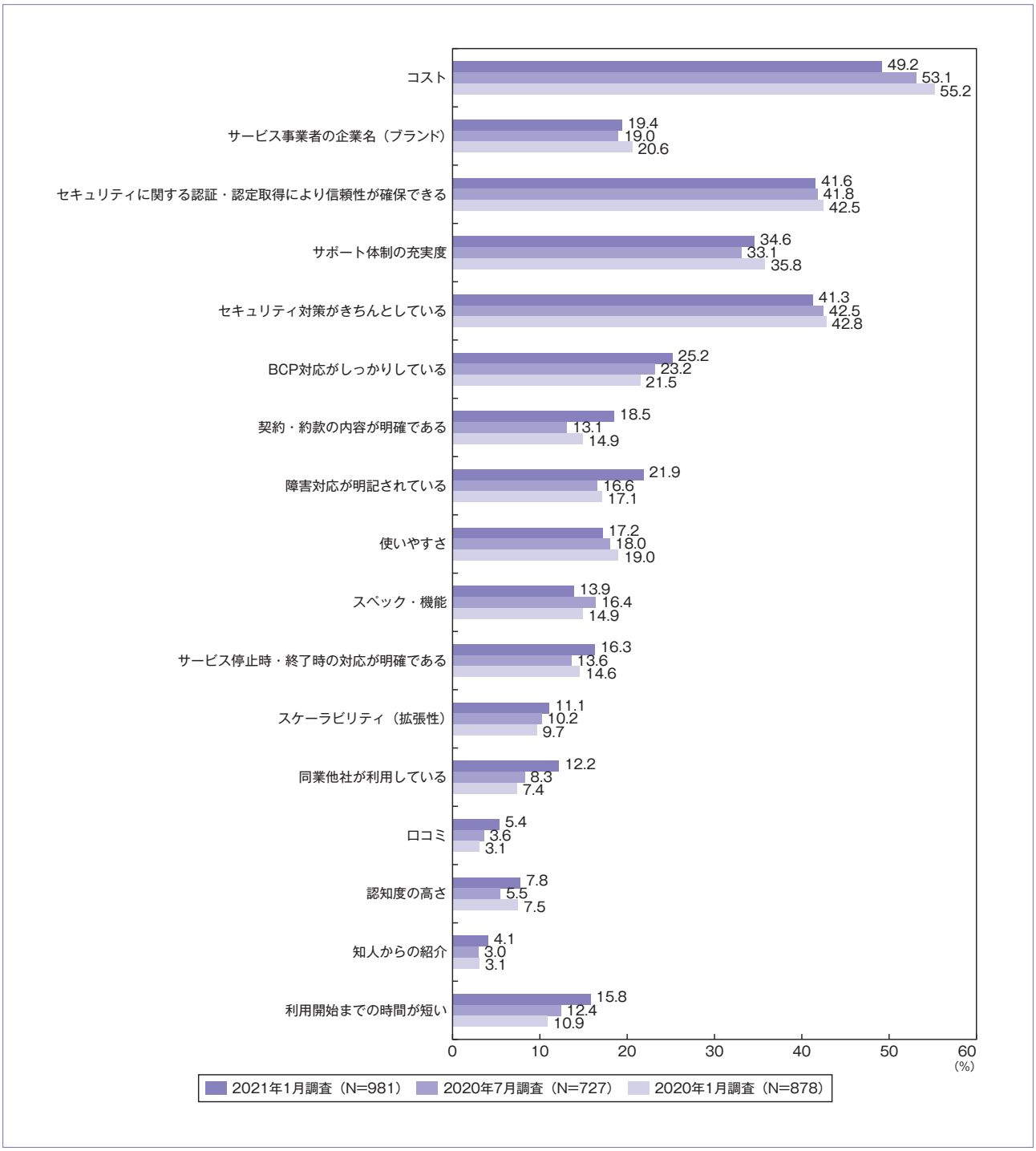


図29. クラウドサービスを選定する際のポイント（2020-2021年比較）

次に、「セキュリティに関する認証・認定制度により信頼性が確保できる」と選択した事業者が実際にサービスを選定する際、信頼性を重視して選んでいるサービスが何かを調査したところ、「グループウェアサービス」（61.8％）が他を引き離してトップで、「顧客管理サービス」（49.5％）、「財務会計サービス」（47.5％）、「経費精算サービス（42.9％）が続く（図30）。

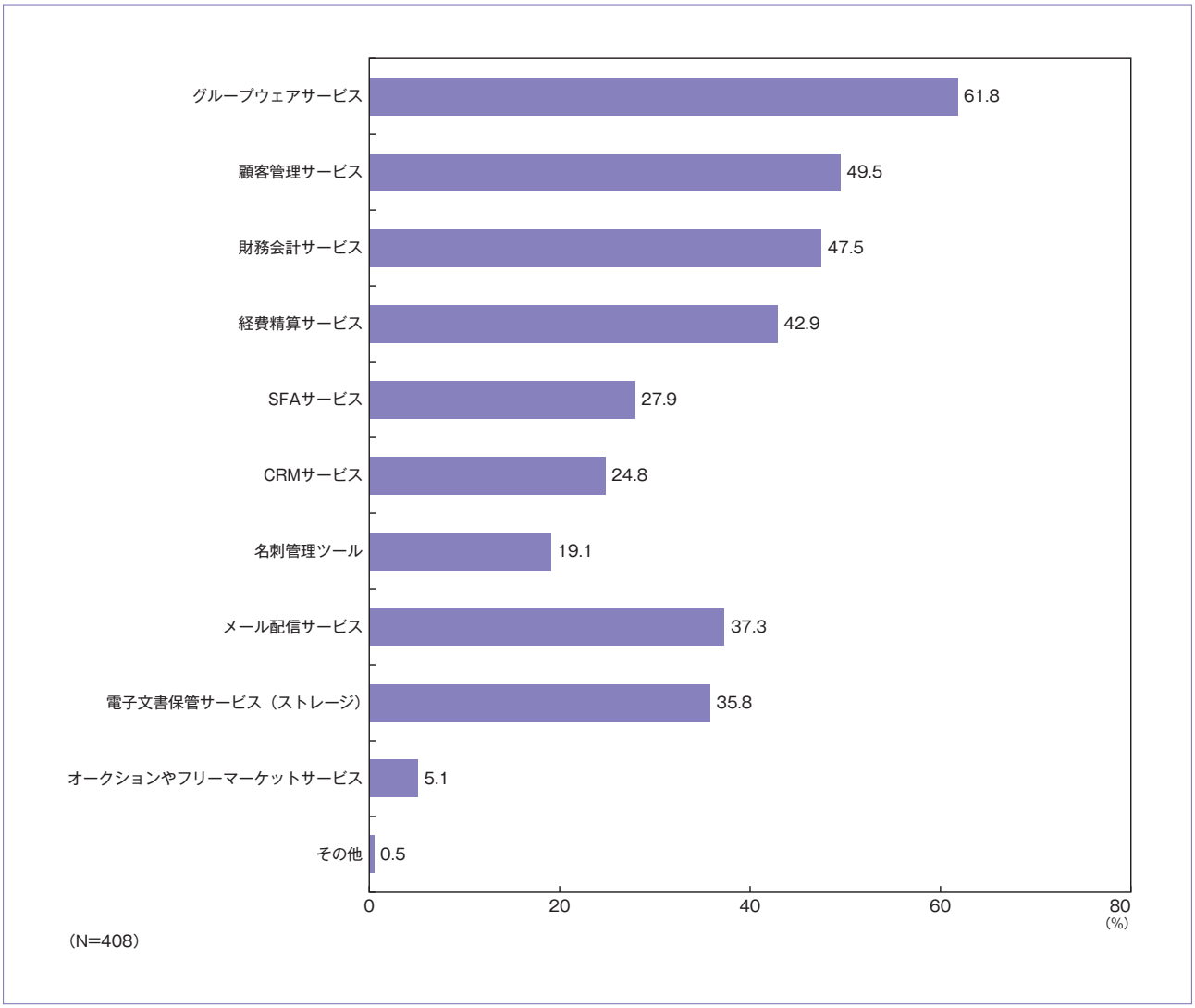


図30. 選定時に信頼性を重視して選ぶクラウドサービス機能

8 電子契約、情報セキュリティ監査

コロナ禍によるテレワーク常態化における電子契約、情報セキュリティ監査について調査を行った。特に電子契約については前回（2020年７月調査）と比較して大きく変化が見られた。

8-1. 電子化したい業務プロセス

業務プロセスの中で電子化したいと回答が最も多かったのは「経費精算（旅費・交通費）」（38.5%）で、「契約書の締結・保管」が徐々に増加傾向にあり、2020年１月調査から約６ポイント増加して２位（37.2%）となった（図31）。

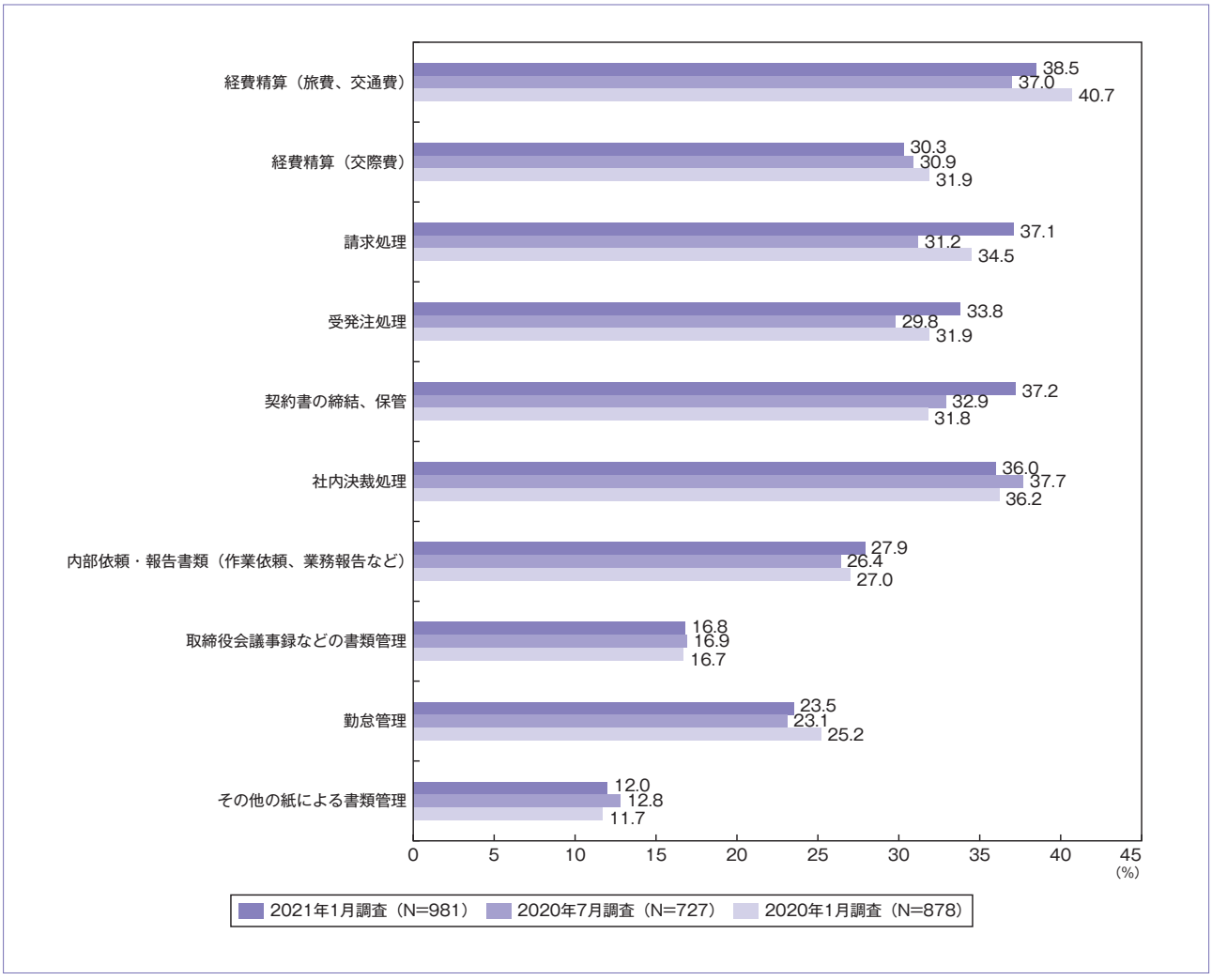


図31. 電子化したい業務プロセス（2020-2021年比較）

8-2. 電子契約の利用状況

電子契約については、コロナ禍の勤務形態の変化に対応し、電子契約を利用している比率は合計で67.2％となった。

今回の調査では質問項目を変えているため単純に比較はできないが、2020年調査では約４割の利用率であったことから、大幅な増加が見られた。調査時点では「採用していないが、利用するよう準備・検討している」割合が17.7％となり、今後８割以上の利用が見込まれる（図４参照）。

なお、業種別では大きなばらつきが見られ、情報通信、金融・保険業、製造業での利用割合が高い（図32）。

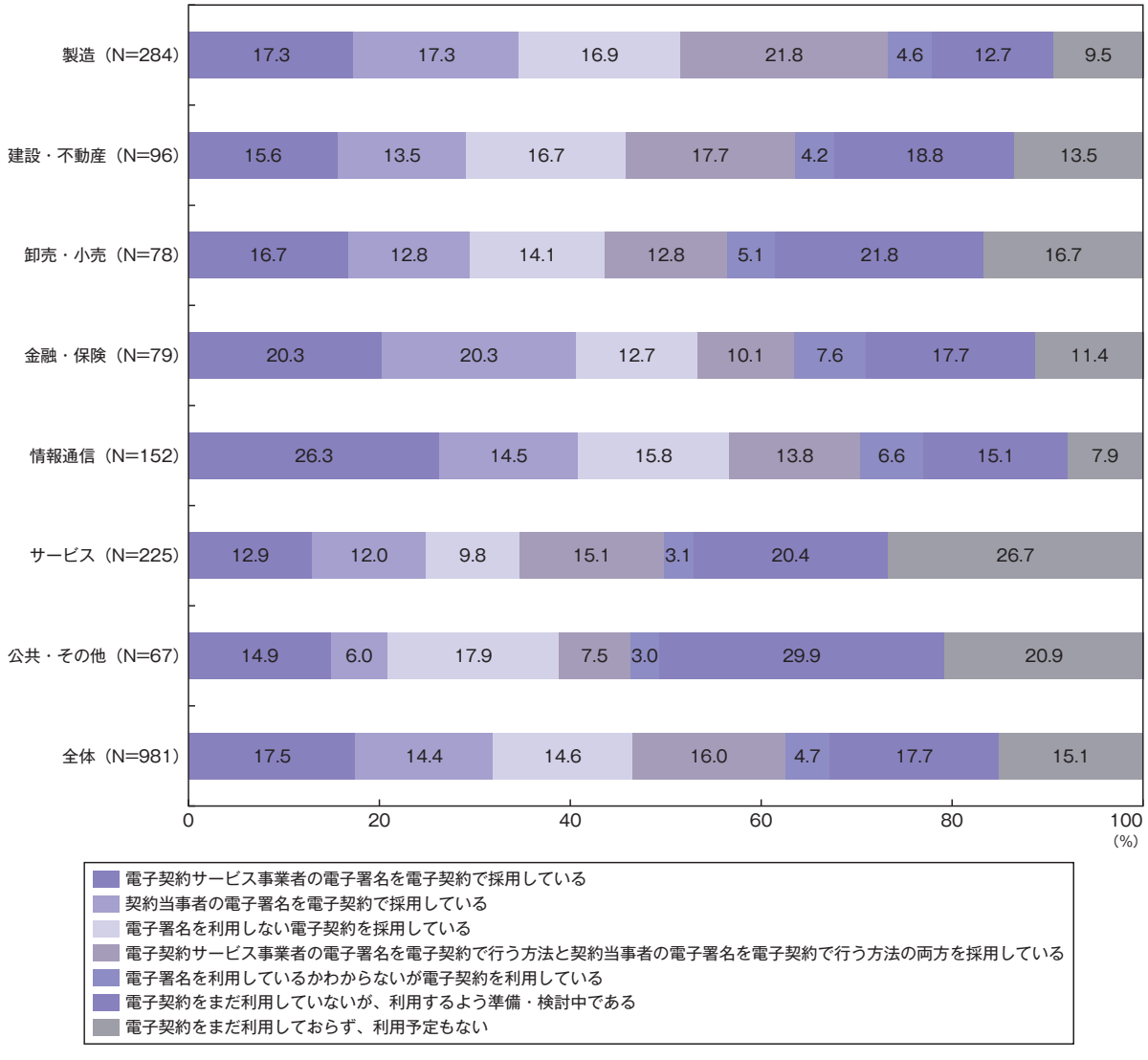


図32. 電子契約の利用状況（業種別）

8-3. 電子契約の採用または利用拡大に向けての課題

電子契約を採用または利用拡大するための課題について「非常に思う」「そう思う」の合計が多いのは、「社内または取引先に新たに導入する手間がかかる」で、次に「導入費用または運用費用が高い」が挙げられている（図33）。なお本調査は2020年１月、７月調査でも実施しているが、あまり変化が見られなかった。

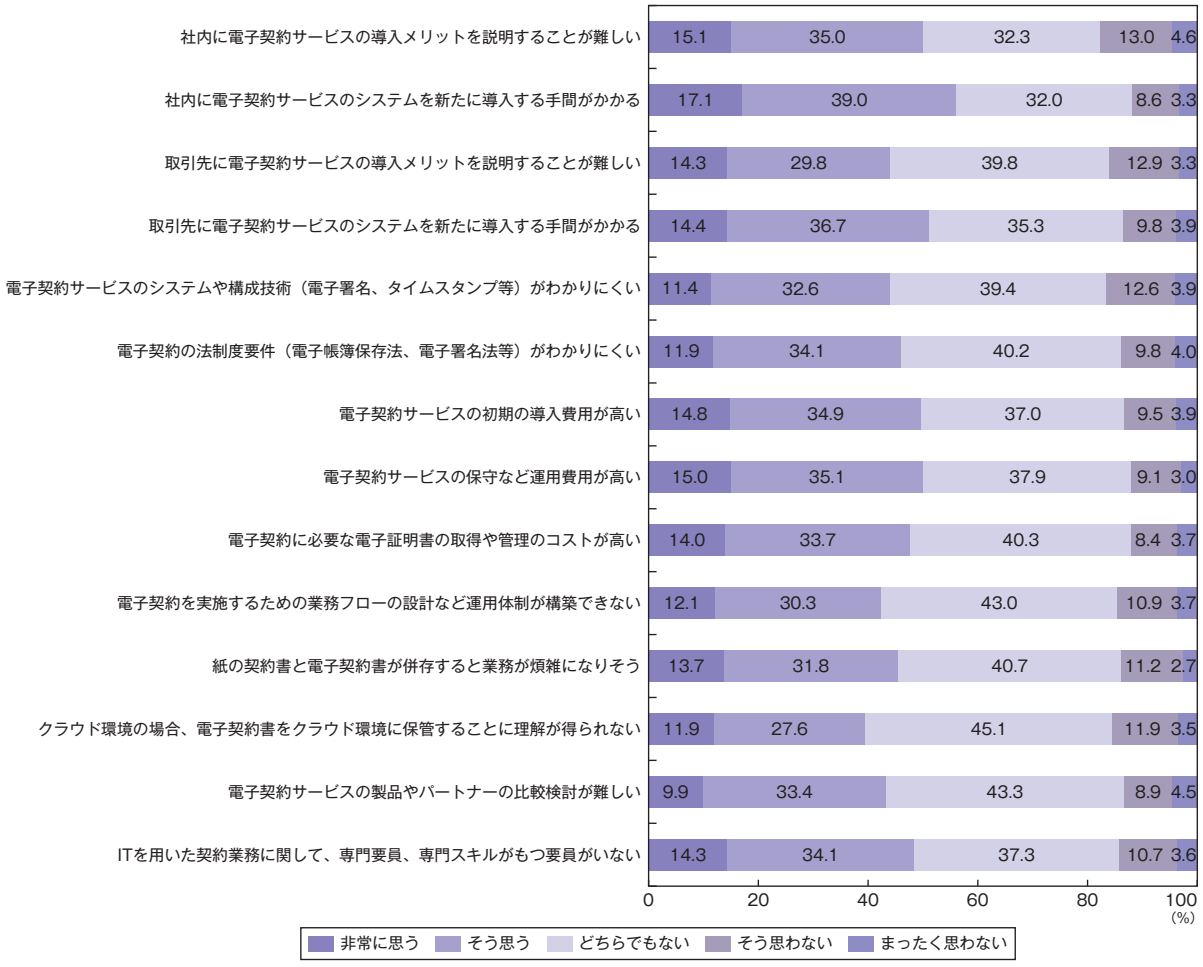


図33. 電子契約拡大に向けての課題

8-4. 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否かを検証する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。2019年と2020年を比較すると、自社、外部委託双方で「定期的に実施している」状況が大きく増加したが、今回はあまり変化は見られなかった。しかし、「定期的に実施している」が約７割、「過去に行ったことがある」を含めれば約９割が実施していることから、情報セキュリティ監査が必要とされているものであることが伺える（図34）。

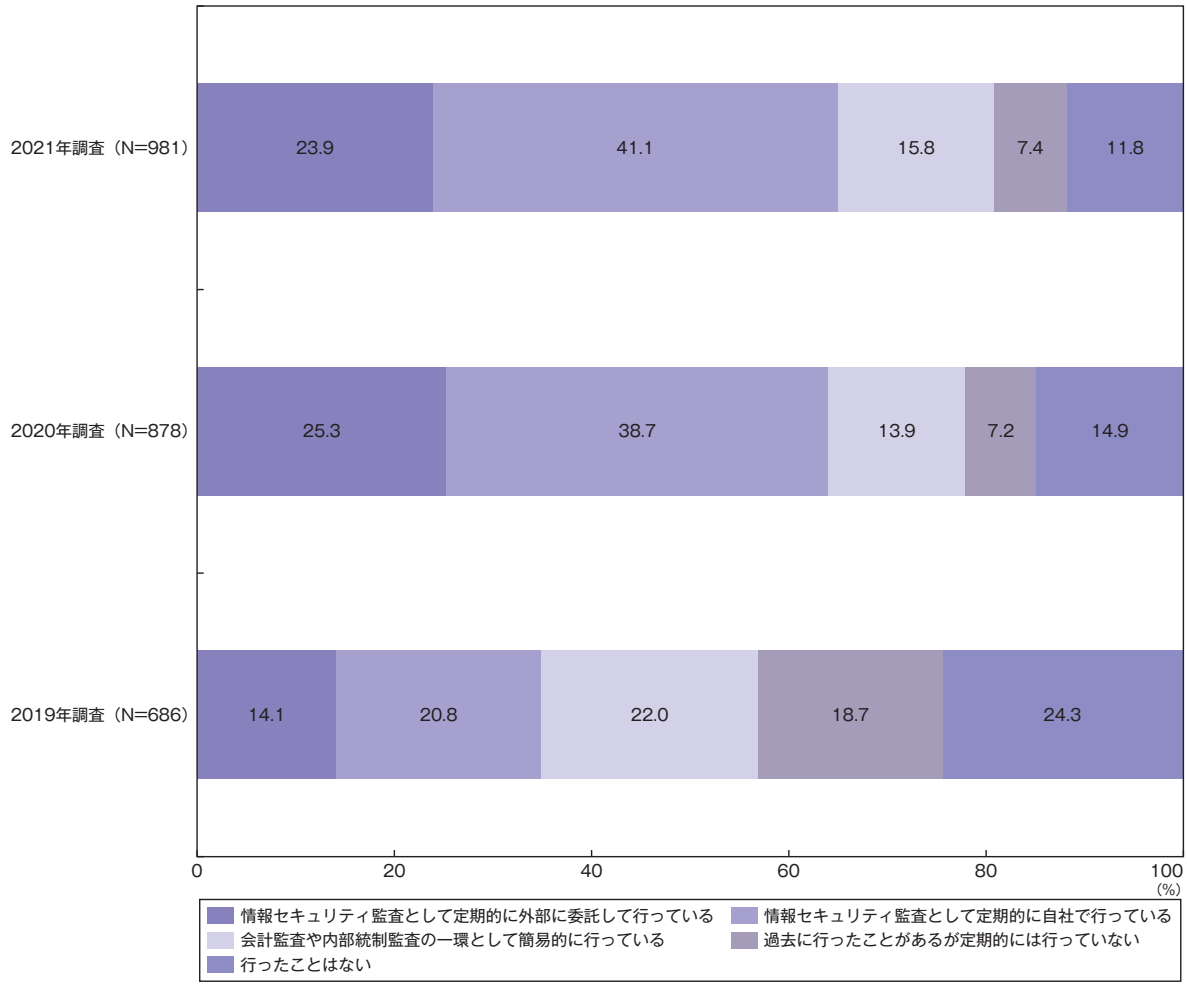


図34. 情報セキュリティ監査の実施状況（2019-2021年比較）

9 総評

2020年初めからのコロナ禍に対応して企業の勤務形態がテレワークに移行したことにより、システム面・セキュリティ面の対応のみならず、営業力の強化や自社プレゼンス／ブランドの向上が経営課題になってきている。

情報セキュリティインシデントはテレワーク勤務に移行したことによって増加傾向になっている。「マルウェア感染」や「従業員によるデータ・情報の紛失・盗難」が依然多いが、「Webサイトへの不正攻撃」や「公開サーバー等に対するDDoS攻撃」のようなサイバー攻撃が増加している。一方で企業のセキュリティ対策についても従来型のファイアウォールやマルウェア対策ソフトのような境界防御型のツールから、ゼロトラストネットワークに対応したCASBやEDRのような次世代型のセキュリティシステムへ移りつつある。サイバー攻撃は日々巧妙化・複雑化してきており、今後、従来型から次世代型への移行が加速すると思われる。

個人情報保護関連では、2020年８月に経済産業省と総務省が「プライバシーガバナンスブック Ver1.0」を公表したが、認知度は高く、個人情報関連のガバナンスへの関心が高いことが伺える。

働き方改革については、一昨年の法令施行後もあまり対応が進んでいなかったが、コロナ禍によってテレワーク勤務にせざるを得なくなり、勤務制度の変更やテレワークのためのネットワーク整備およびシステムのクラウド化が一気に進んだ。

この流れを受けて、電子契約の利用が2020年７月時点で約４割だったものが、半年で７割近くまでに増加しているのは、テレワーク勤務での典型的なデジタル化の事例といえよう。

回答者プロフィール

業種	回答数	%
製造	284	29.0
建設・不動産	96	9.8
卸売・小売	78	8.0
金融・保険	79	8.1
情報通信	152	15.5
サービス	225	22.9
公共・その他	67	6.8
全体	981	100.0

従業員規模	回答数	%
5,000人以上	216	22.0
1,000～4,999人	222	22.6
300～999人	232	23.6
50～299人	311	31.7
全体	981	100.0

資本金規模	回答数	%
5,000億円以上	174	17.7
3,000億～5,000億円未満	54	5.5
1,000億～3,000億円未満	89	9.1
500億～1,000億円未満	98	10.0
100億～500億円未満	203	20.7
10億～100億円未満	270	27.5
1億～10億円未満	88	9.0
1,000万円～1億円未満	5	0.5
全体	981	100.0

業種別内訳

業種		回答数	%
製造	食品・飲料	26	2.7
	日用品・生活雑貨	6	0.6
	繊維	10	1.0
	パルプ・紙・印刷	16	1.6
	化学工業	30	3.1
	石油製品	11	1.1
	鉄鋼・金属	27	2.8
	プラスチック・ゴム	12	1.2
	機械	24	2.4
	電気機器	36	3.7
	情報通信機器	11	1.1
	電子部品・電子回路	18	1.8
	精密機器	15	1.5
	自動車・輸送機器	18	1.8
	医薬品	10	1.0
	その他の製造業	14	1.4
建設・不動産	建設	54	5.5
	不動産	39	4.0
	住宅	3	0.3
卸売・商社	卸売	27	2.8
	小売	33	3.4
	商社	18	1.8
金融・保険	銀行	44	4.5
	証券	6	0.6
	生命保険	9	0.9
	損害保険	10	1.0
	その他金融	10	1.0

業種		回答数	%
情報通信	通信	27	2.8
	ITベンダ/システムインテグレータ	91	9.3
	インターネット・サービス	19	1.9
	情報システム子会社	15	1.5
サービス	電力・ガス・水道	16	1.6
	運輸	36	3.7
	倉庫	8	0.8
	宿泊	7	0.7
	飲食	8	0.8
	娯楽・レジャー	9	0.9
	メディア・出版・放送・広告	8	0.8
	生活関連サービス(旅行業など)	5	0.5
	医療	22	2.2
	福祉・介護	35	3.6
	教育（学校以外）	17	1.7
	人材派遣・業務委託	13	1.3
	その他サービス	41	4.2
公共・その他	学校	13	1.3
	官公庁	16	1.6
	地方自治体	21	2.1
	農業・水産・鉱業	4	0.4
	その他の業種	7	0.7
	その他公共機関	6	0.6
全体		981	100.0

IT戦略・情報セキュリティへの関与度合い	回答数	%
全社的なIT戦略に決定権をもっている	311	31.7
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もっている	457	46.6
セキュリティ製品の導入、製品選定に関与している	503	51.3
セキュリティ対策の実務に関与している	336	34.3
全体	981	100.0

〈資料〉情報化に関する動向（2020年10月～2021年３月）

国　内	海　外
2020年10月	
・東京証券取引所、自動切換え用設定ミスによるシステムダウンで終日取引できず。マニュアル不備が原因。 ・規制改革推進会議、押印廃止に向け関連法案改正へ着手。11月、官庁の事務手続き99％の押印廃止を公表。 ・政府、「Trusted Web推進協議会」設置。DX推進に必要となるデータガバナンスの構造設計と技術の抽出、課題検証など官民連携で検討。 ・情報通信研究機構（NICT）他、電子データを量子暗号で秘匿化、秘密分散技術でデータの管理、復元に成功。	・日米英など７カ国、Facebookの対話アプリメッセージの暗号化が犯罪捜査に支障をきたすとして、プライバシーを配慮した見直し要請。 ・アルゼンチン政府、犯罪容疑者DBに未成年登録。顔認識システムで追跡も。 ・英情報コミッショナー事務局、2018年に発生したBritish Airwayの大規模個人情報流出事件で2,000万ポンドの制裁金。 ・米司法省（DOJ）と11州、Googleを検索エンジン、インターネット広告市場における反トラスト法違反で提訴。 ・Google、自社のデータ保護ポリシーに抵触する子供向けアプリを削除。 ・カリフォルニア州、2020年１月施行の消費者プライバシー保護法（CCPA）の補正修正を巡り国民投票実施。11月に可決。

国　内	海　外
2020年11月	
・サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）設立。官民連携でサプライチェーン全体のセキュリティ対策に着手。 ・ゲーム大手カプコン、ランサムウェア被害で最大35万件の個人情報流出の恐れ。身代金要求には応じず。ロシア周辺国の関与浮上。１月には累計39万件に拡大。 ・イベントプラットフォームPeatix、不正アクセスで最大677万件の個人情報流出。その後の調査でも侵入方法特定できず。 ・東建コーポレーション、不正アクセス被害で最大65万件流出の可能性。 ・平井デジタル改革相、中央省庁でのパスワード付きZipファイルによるデータ送信（PPAP）廃止発表。まずは内閣府と内閣官房で実施。	・米ポートランド、法執行機関での顔認識と監視技術の利用を禁じる法律可決。2019年以降、サンフランシスコ他多数の地域で禁止に。 ・仏広告団体、デバイス搭載の広告識別子（IDFA）へのアクセス、ユーザ追跡へのユーザ同意義務づけをめぐりAppleを独占禁止法違反で提訴。 ・Zoom、米連邦取引委員会（FTC）からの録画データの暗号化設定不備指摘に対処し、和解合意。 ・中国国家市場監督管理総局、自国ネット大手の独占を抑止する規則案公表。 ・Apple、旧型iPhoneバッテリー老朽化による動作不良の影響非開示に対する集団訴訟で、米34州・地区の司法当局に1.1億ドルの和解金支払い。 ・Microsoft、プライバシーシールド無効に伴う欧米間のデータ送信に関する欧州連合司法裁判所からの勧告への対応方針発表。方針発表は対象企業として初。 ・欧州委員会（EC）、データ戦略の一環として、データ共有のメカニズム強化のためのデータガバナンス法案公表。 ・英政府、2021年４月に競争・市場庁（CMA）内に巨大IT企業の独占を監視・規制する専門組織「デジタル市場ユニット」設置を発表。

国　内	海　外
2020年12月	
・PayPay、加盟店データベースアクセス権限設定不備で加盟260万店2,007万件に不正アクセス発覚。 ・NICT他、世界初、IBM製量子コンピュータで、暗号技術の安全性の根拠の一つである離散対数問題の求解実験に成功。 ・NICT他、マルチモード光ファイバ伝送容量、毎秒１ペタビット伝送成功で世界記録。 ・公正取引委員会、企業合併審査等書類手続きでの押印廃止。 ・楽天、2016年以降４年10カ月にわたり外部のクラウド型の顧客情報管理システムが閲覧可能状態に。148万件のユーザ情報流出の可能性。 ・経済産業省、コロナ禍を踏まえて明らかになったDXの本質、企業・政府が変革のために取るべきアクションをまとめた「DXレポート２（中間取りまとめ）」公表。	・中国政府、モバイルアプリの個人情報収集内容の通知と利用同意を必須とする規制案公表。 ・仏データ保護機関、GoogleにCookie利用規則違反で１億ユーロの制裁金。 ・FTC、InstagramやWhatsAppの買収は市場独占を脅かす企業排除のためとして、Facebookを反トラスト法違反で提訴、買収解消を要求。同週に全米46州も提訴。 ・Apple、全180万アプリの個人情報取扱い開示開始。アプリ開発事業者に利用情報通知義務づけ。 ・欧州連合、企業買収時の当局への事前通知を課す「デジタル市場法」と、SNSの違法コンテンツの迅速な削除を義務づける「デジタルサービス法」公表。英国もSNS企業向け同様の法案公表。 ・米テキサス州など10州、広告枠の売買取引操作でネット広告市場競争を妨げたとして、反トラスト法違反でGoogleを提訴。その後も検索事業での独占を理由にコロラド州他38州が提訴。 ・米英他40超の政府機関や企業、SolarWinds社のネットワーク製品を経由した大規模サイバー攻撃被害。米国務長官がロシア関与を断定。 ・ニューヨーク州知事、全公・私立学校で生体認証技術を2022年７月まで使用禁止とする法案署名。

国　内	海　外
2021年１月	
・東京商工リサーチ調査、上場企業・子会社の個人情報漏えい・紛失事故公表88社の流出件数は2,515万件。事故原因の多くはウイルス感染・不正アクセス被害。 ・「JIS X 9251 情報技術－セキュリティ技術－プライバシー影響評価のためのガイドライン」制定。潜在的なプライバシーへの影響を事前に評価する（PIA）ための有効な方法／手段を示した国際標準。 ・警視庁、2018年に580億円相当が流出した仮想通貨NEMを約188億円分不正交換した疑いで31名を摘発。流出の首謀者は特定できず。 ・内閣サイバーセキュリティセンター、Salesforce製品設定不備による顧客情報流出の可能性を注意喚起。楽天、PayPay、バンダイなど複数企業に影響。	・シンガポール政府、コロナ感染追跡アプリのデータを犯罪捜査に利用する可能性を発表。国民８割弱に無料配布済。 ・CMA、Chromeから3rd Party Cookieとその多機能排除方針を受け、競合他社のデジタル広告抑制とならないか調査に着手。 ・中国政府、「インターネット情報サービス管理弁法」の改正草案を公開。国家安全に危害を与える情報やデマの発信者に最高100万元の罰金。 ・Googleと仏報道各社、G社サービスへのニュース表示時の記事使用料支払いで合意。 ・スコットランド環境保護庁、ランサムウェア攻撃の身代金支払い拒否でハッカーグループが全ファイル公開。

国　内	海　外
2021年２月	
・ヤフー、スマホ向け本人確認をID／パスワード入力から生体認証対応へ。2021年春完了を発表。 ・「特定デジタルプラットフォームの透明性及び公正性の向上に関する法律」施行。規制対象企業には取引先、消費者への契約条件の開示や変更時の事前通知義務と経済産業省への定期的な取引内容の報告義務。（４月に対象企業６社発表。） ・接触確認アプリ「COCOA」、2020年９月のバージョンアップ後、Androidで４カ月間通知されず。その後iPhoneも不具合。その後の調査で動作確認未実施など発覚。 ・政府、デジタル庁設置法案等、デジタル改革関連６法案を閣議決定、国会提出へ。行政システムの標準化、行政手続きのオンライン化等に着手。 ・公正取引委員会、デジタル広告分野におけるデジタルプラットフォーム事業者の取引実態調査結果報告。 ・政府、「プロバイダ責任制限法」改正案を閣議決定。ネット上での誹謗中傷投稿者情報開示の可否を裁判所が判断し、被害者の負担軽減へ。	・米メリーランド州、全米初とされるネット広告税制度導入。デジタル広告収入に最大10％の課税。米国商工会議所とAmazon等業界団体が連邦法に反すると提訴。 ・米ミネアポリス市、全米各地での反人種差別デモの発端となった警察機関での顔認証ソフト使用禁止条例案可決。 ・DOJ、2014年のソニーエンタテインメント攻撃をはじめ、世界規模のサイバー攻撃で13億ドルを摂取した３名の北朝鮮ハッカーを起訴。 ・EC、英国との個人データ移転承認で手続き着手。承認後４年間は自由に流通可能に。 ・米ファイル共有サービス提供企業Accellion、システムの脆弱性を突いたサイバー攻撃で、複数の政府機関、企業の個人情報数百万件が漏えい。 ・TikTok、アプリ利用者の生体認証データと個人情報収集問題に関する集団訴訟に9,200万ドル支払い和解へ。双方の主張の食違いよりもサービス提供を優先。

国　内	海　外
2021年３月	
・日本航空、複数の航空会社に予約システムを提供するスイスSITA社への不正アクセスにより、92万人の情報流出。全日空は100万人。 ・LINE、システム開発委託先の中国スタッフが利用者情報にアクセス可能に。個人情報保護委員会が立入り調査実施。プライバシーポリシーに第三国からのアクセス説明不足。政府、自治体は一時LINE使用休止措置。 ・IBM、EC分野で利用可能な技術利用のライセンス契約に応じない楽天を特許侵害で提訴。	・Facebook、同意なき生体認証データ収集がイリノイ州法違反にあたるとした160万人による集団訴訟に対し、約6.5億ドル支払いで和解合意。 ・CMA、アプリ開発者向け利用規約が反競争的として、Appleを独占禁止法違反の疑いで調査開始。 ・米ネットワーク監視カメラ提供企業Verkad、15万台の監視カメラデータをハッカー集団が不正取得。流出企業には警察、刑務所、学校、大手電気自動車メーカーなど。 ・台湾Acer、ランサムウェア攻撃被害で過去最高の5,000万ドルの身代金要求。ハッカーは支払期限を過ぎたら金額倍増と通告。 ・米ニューヨーク州、コロナワクチン接種証明書アプリ無料公開。IBM開発のブロックチェーンを採用し、利用者のプライバシー保護。州によるアプリ提供は米国初。

JIPDEC IT-Report 2021 Spring

2021年5月31日発行（通巻第17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