2022 SPRING

IT-REPORT

特集

コロナ禍で加速するデジタルワークスタイルへのシフト
―「企業IT利活用動向調査2022」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 2022 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2022」の結果をとりまとめ、紹介しています。

新型コロナウイルス感染拡大防止にあたり、ビジネススタイルも大きく変化していますが、コロナ禍を契機にテレワークを導入した企業は約５割、コロナ以前から導入している場合とあわせ７割の企業でテレワークが常態化し、スマートデバイスやリモート環境で利用する機器、アプリケーションなどに対するセキュリティ対策が実施されています。また、クラウドサービスの利用動向については、９割以上の企業が全部または一部でクラウドサービスを利用していることがわかりました。

今年は毎年実施している過去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の他、新たに４月に全面施行となった「改正個人情報保護法」に対する事前対応やプライバシーテックの利用状況、DXや電子インボイスの取組状況や、昨今、標的型メール被害拡大の影響を受け、政府や大手企業で利用禁止の傾向が高まっているPPAP対応についても調査するなど、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。

なお、今号では、調査分析結果を踏まえ、「プライバシーテック」「電子契約」「メールのなりすまし対策」の最新動向をテーマに、当協会職員によるコラムも掲載しています。

あわせて、2021年10月から2022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。

2022年５月

一般財団法人日本情報経済社会推進協会

JIPDEC IT-Report 2022 Spring

Contents

特 集

コロナ禍で加速するデジタルワークスタイルへのシフト ―「企業IT利活用動向調査2022」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、経営企画、総務・人事、業務改革部門等に所属し、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、2011年から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」を実施している。

2020年からは社会のさまざまな場面に大きく影響を与えているコロナ禍において、企業の考え方や行動にどのような変化が生じたかについても調査を行っている。

本誌では、2022年１月実施の調査結果をもとに、過去の調査結果との経年比較を含め、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 2022年調査の概要

1-1. 調査概要

・実査期間：2022年１月15日～17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２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14,000人
・有効回答数：982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（30.7%）、次いでサービス業（21.9%）、情報通信（15.0%）、建設・不動産（9.9%）、卸売・小売（8.8%）、金融・保険（8.4%）となった。

所属部門では情報システム部門（26.4%）が最も多く、役職は、本部長・部長（32.3%）、課長（29.8%）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から、「セキュリティ製品の導入・製品選定に関与している」（51.1%）、「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」（48.0%）とする回答が多く、2021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、テーマ別に分析結果を紹介する。

2 経営課題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として定着しつつある「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見る。

2-1. 重視する経営課題

全24項目の経営課題について、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調査した。（図１）前回調査同様、「業務プロセスの効率化」（54.7％）がトップとなり、「従業員の働き方改革」（44.7%）が２位、「社内コミュニケ―ションの強化」（40.6％）は３位となった。

2020年以降の調査結果を比較して特に大きな変化が見られたのは「社内コミュニケーションの強化」で、2020年１月調査で37.6％だったのが、コロナ禍の影響を受けた後の２回の調査は大きく減少したものの、今回調査では10ポイント以上の増加がみられた。その他、「社内体制・組織の再構築」（35.7％）、「従業員の働き方改革」（44.7％）などの社内組織関連の変革も、コロナ前の数値にV字回復している。また、「新商品・新市場の創出基盤の構築」（18.2％）が前回と比較して高くなっている。

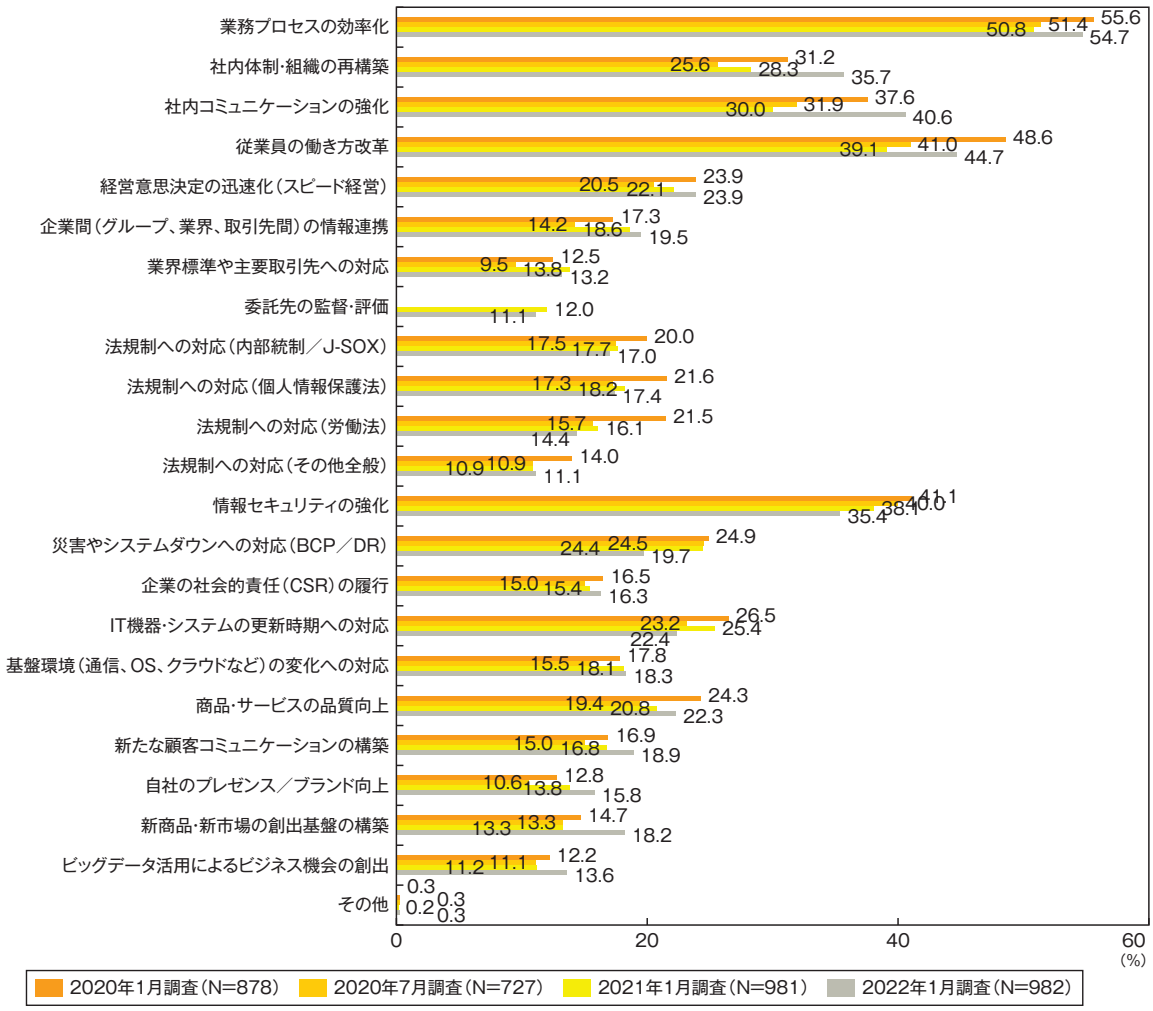
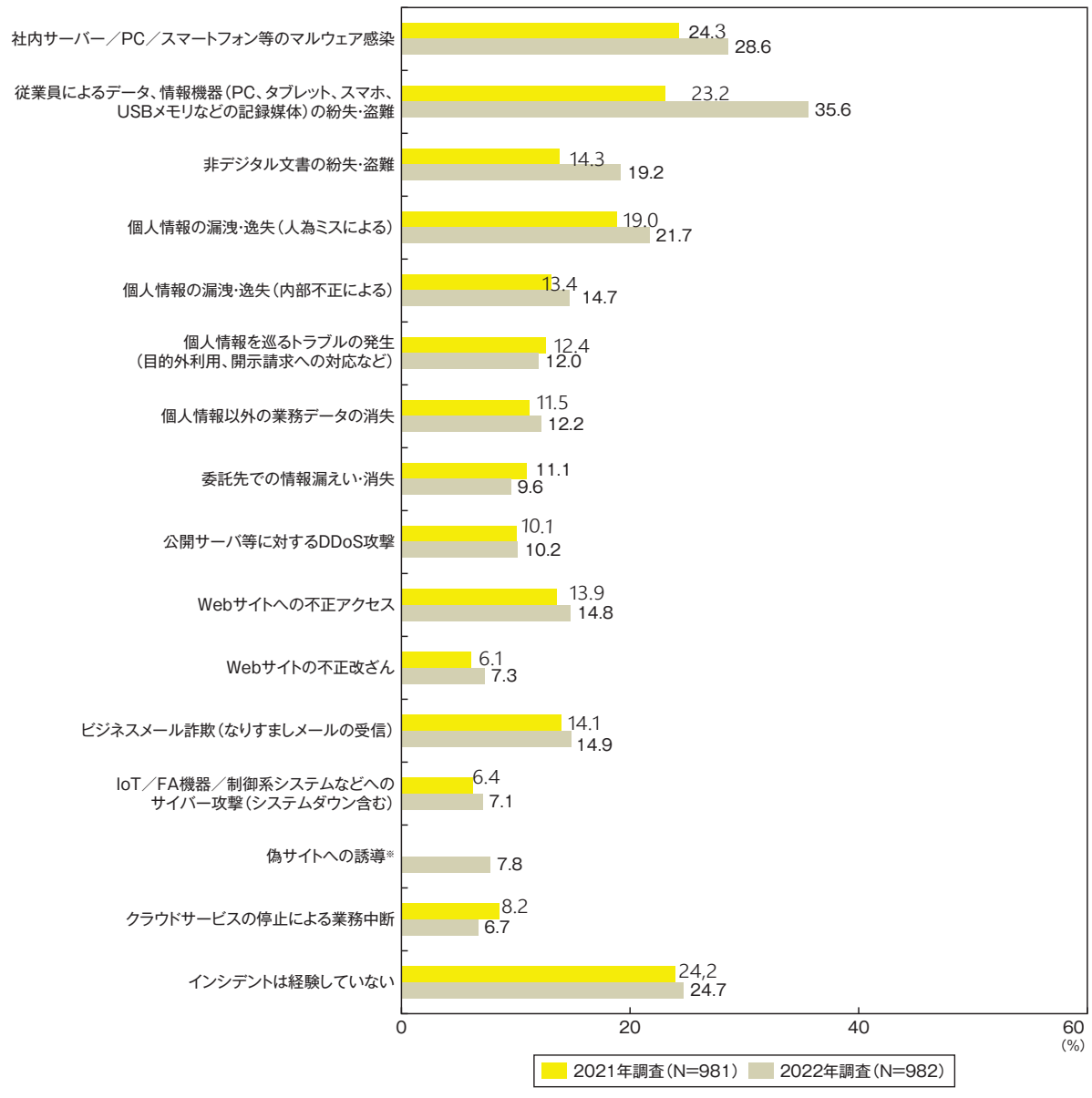


図１．今後重視したい経営課題（複数回答）（2020年１月～2022年比較）

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、最も高かったのは「従業員によるデータ・情報の紛失・盗難」（35.6%）で、前回調査から10ポイント以上増加した。２位は「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%から28.6%に増加）となり、前回調査から１位と２位が入れ替わった。（図２）



※偽サイトへの誘導は2022年調査のみ

図２．過去１年間に認知したセキュリティインシデント（2021-2022年比較）（複数回答）

2-3. セキュリティリスクの重視度合い

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に関しては、外部からのサイバー攻撃に対し、「経営陣から最優先で対応するよう求められている」とした回答が前回調査の30.9%から約５ポイント増えて35.2%となった。世界的にマルウェア「Emotet」が再び猛威を奮っており、サイバー攻撃被害の影響から自社業務の停止や取引先や顧客からの信用失墜を避けるためにも、企業全体でサイバー攻撃対応が重視された結果と考えられる。

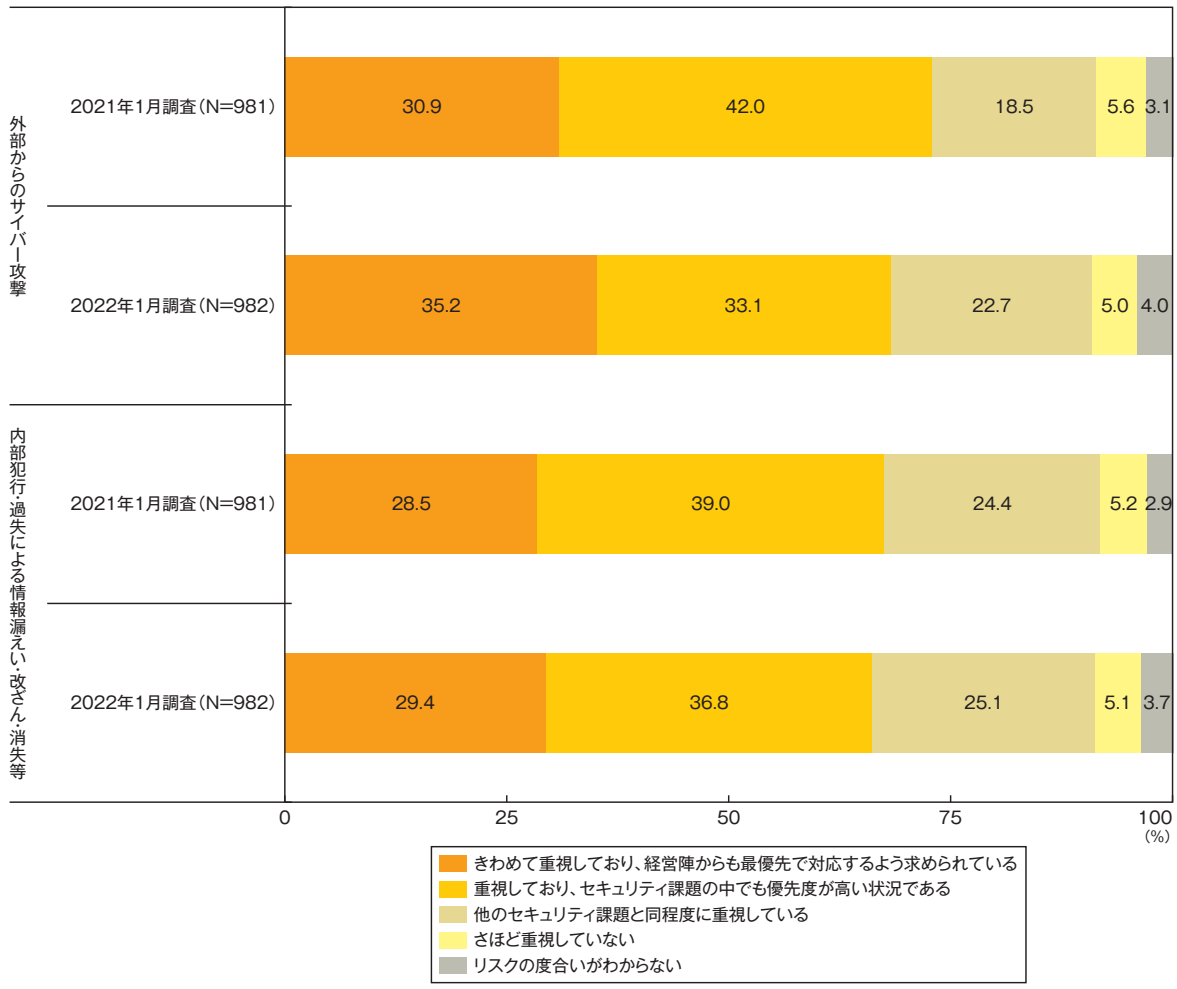


図３．セキュリティリスクの重視度合い（2021-2022年比較）

2-4. 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の実施はどのようになっているのか。今回調査では、「過去１年間に経験したセキュリティインシデント」で取り上げたインシデントに対し、「外部からのサイバー攻撃対策」「内部犯行の情報漏えい対策」の実施率について調査を行った。

「外部からのサイバー攻撃対策」として最も実施率が高かったのが「マルウェア感染対策」（62.1%）、２位は「従業員による紛失・盗難対策」（53.6%）と５割を超えたが、「クラウドサービスの停止による中断」以外はいずれも実施済みが４割となった。（図４）

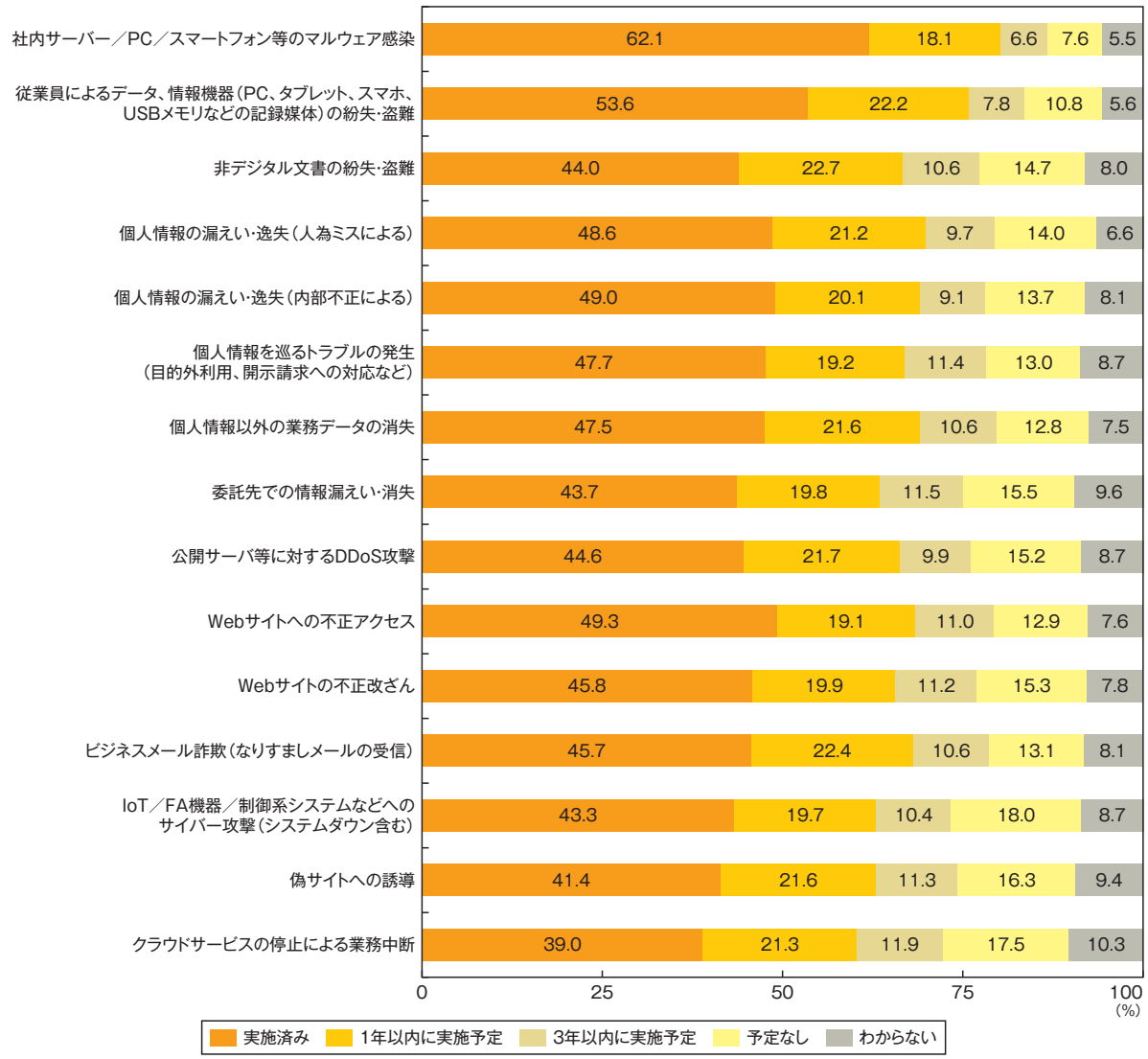


図４．主要な「外部からのサイバー攻撃対策」の実施状況

一方、「内部犯行による情報漏えい対策」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」（55.6%）の実施率が最も高く、「重要情報の定義・特定・他の情報資産との分類」（54.0%）、「重要情報の取扱責任者の任命」（52.4%）が、いずれも５割を超えている。（図５）

実際に経験したセキュリティインシデントで「委託先での情報漏えい・消失」が9.6%であった（図２）が、「委託先に対する監査」の実施状況が最も低い結果となった。委託先でのインシデントが自社の業務や信用失墜に与える影響を考慮すれば、委託先のセキュリティ対策の実施状況を把握することは重要であり、定期的な監査の実施が望まれる。

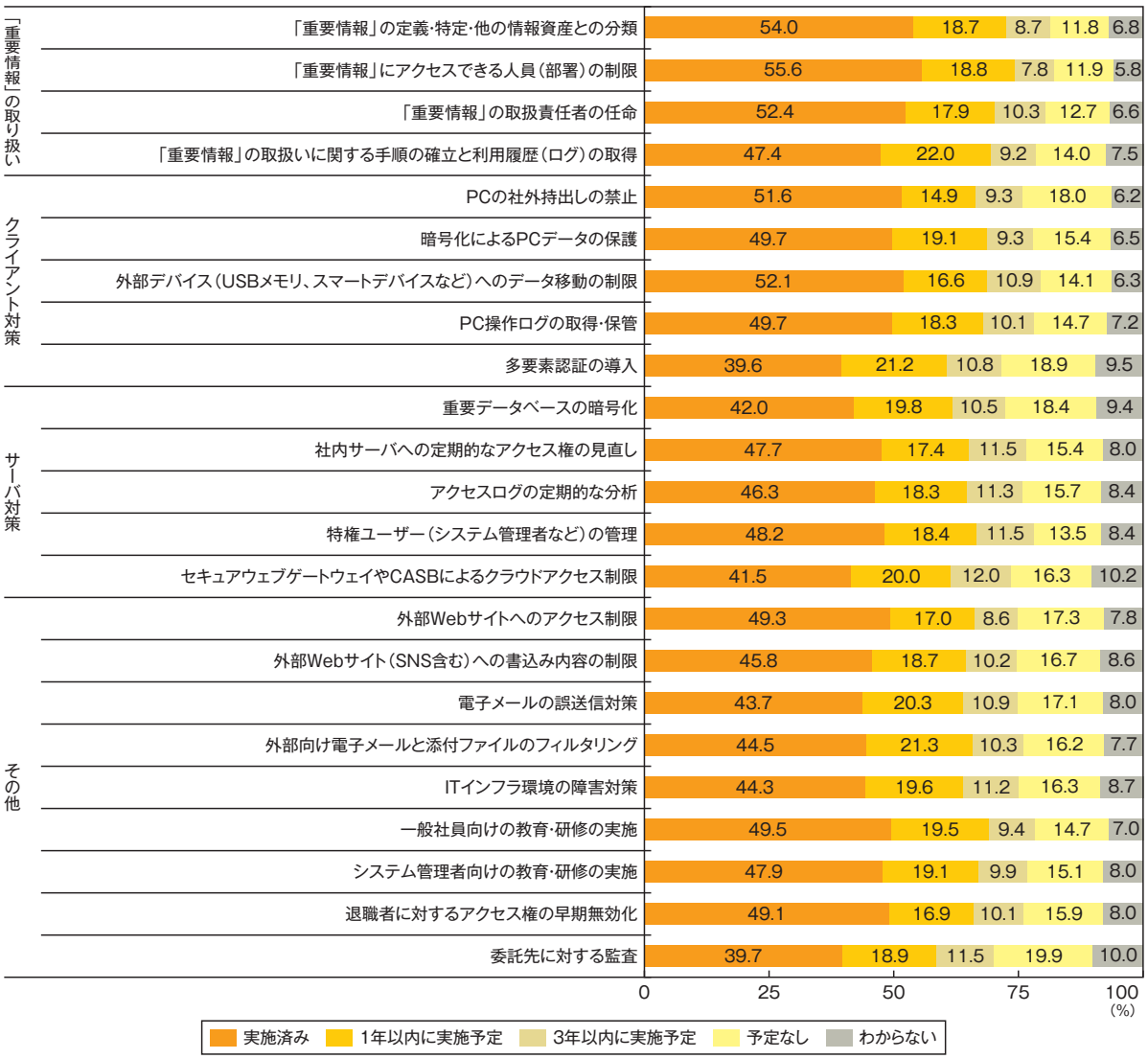


図５．主要な「内部犯行による情報漏えい対策」の実施状況（2022年）

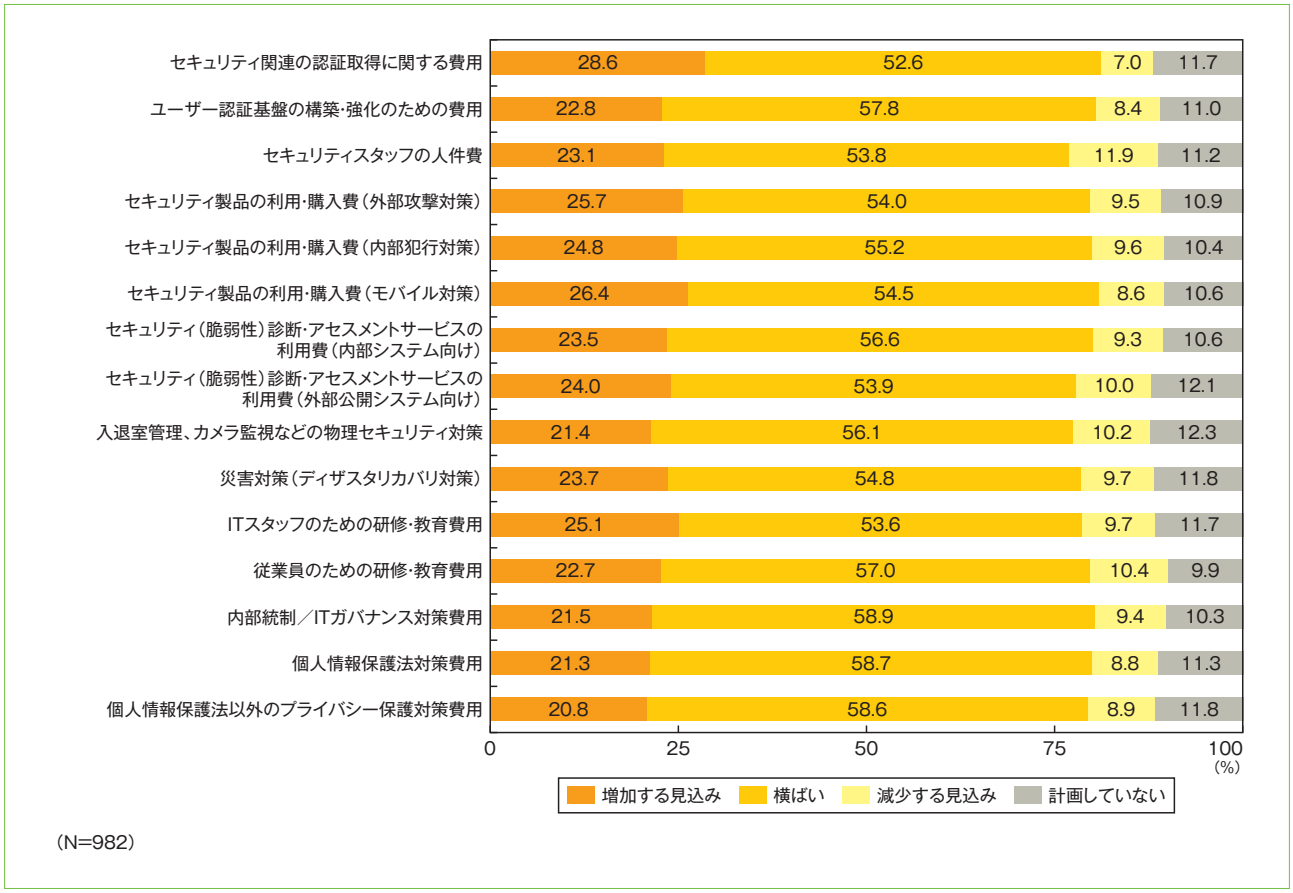
2-5. セキュリティ支出（実績／計画）の動向

コロナ禍によりリモートワークやクラウドサービスの利用が増えてきている中、2021年度のセキュリティ関連費用の扱いについて、実績と、次年度の支出計画について調査を行った。

実績・計画ともにセキュリティ関連認証取得費用について、若干ではあるが増加傾向にあり、新規認証取得や認証維持に費用を充当する企業が増えていると考えられる。

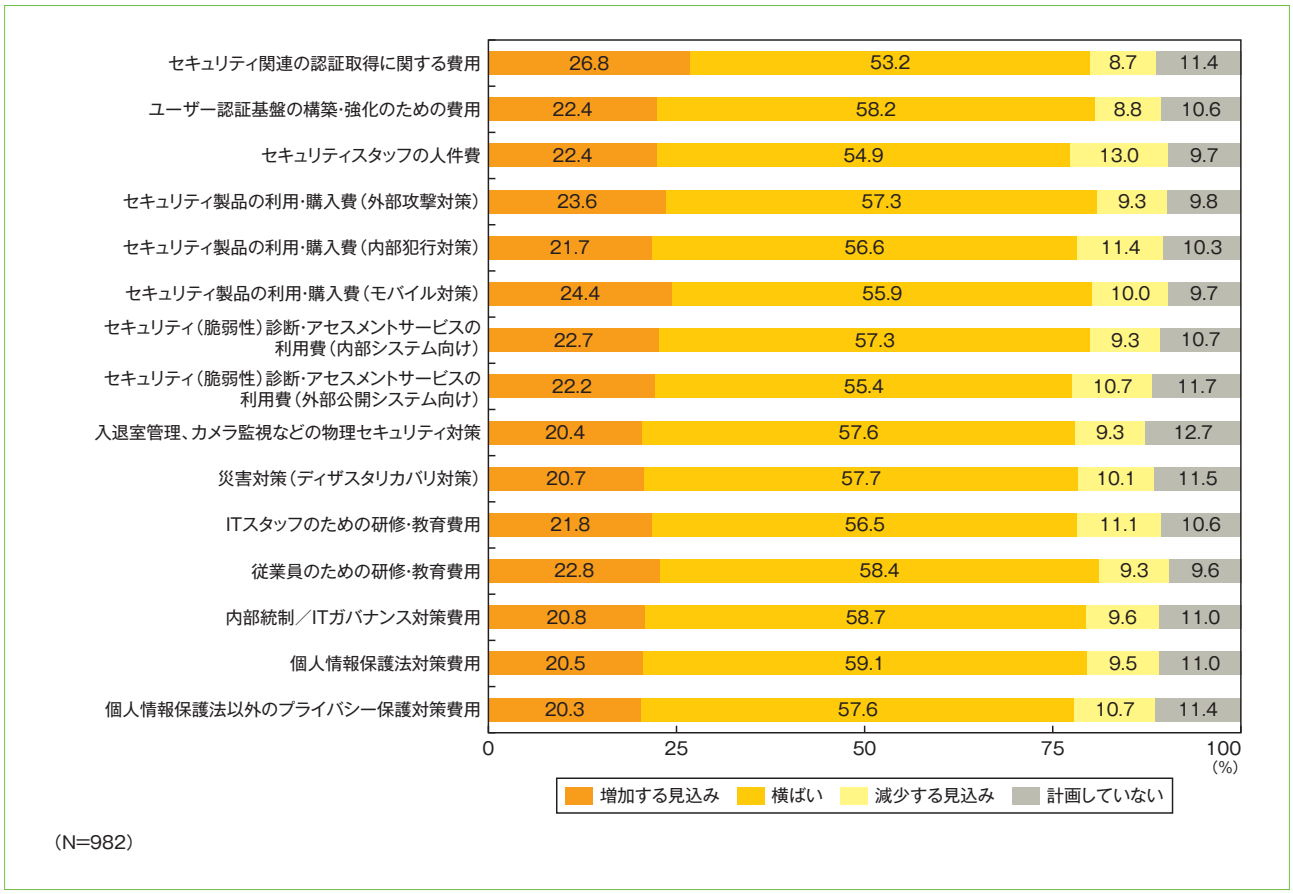
セキュリティ支出の増減動向については、すべての支出項目において「横ばい」が５割を超えているが、「増加」と回答している比率も２割を超えている。特にセキュリティ関連の認証取得費用が「増加」と回答している比率が約３割と高くなっている。（図６）

一方、2022年度支出計画については、2021年度の支出と比べ、全項目で「増加」が約２割、「横ばい」が約５割となった。（図７）



(N=982)

図6．セキュリティ支出実績の増減傾向



(N=982)

図7．セキュリティ支出計画の増減傾向

3　第三者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で自社の取組み状況を確認するとともに、取組みの結果を顧客や取引先に「見える化」することができるセキュリティ関連の認証制度の取得がある。

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／認証制度の取得の価値・効果と、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。

3-1. 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、「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」を除く４つの項目で実施済みが６割を超えている。ただし、「ITサービスマネジメントの実施」についても５割を超えていることから、前回調査からすべてにおいて取組みが進んでいることがわかる。（図８）

前年調査との比較で大きく変化が見られたのは「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」（前回44.6％から55.3％へ）と「事業継続計画（BCP）の策定・実施」（54.5％から64.7％）で、いずれも約10ポイント増加している。

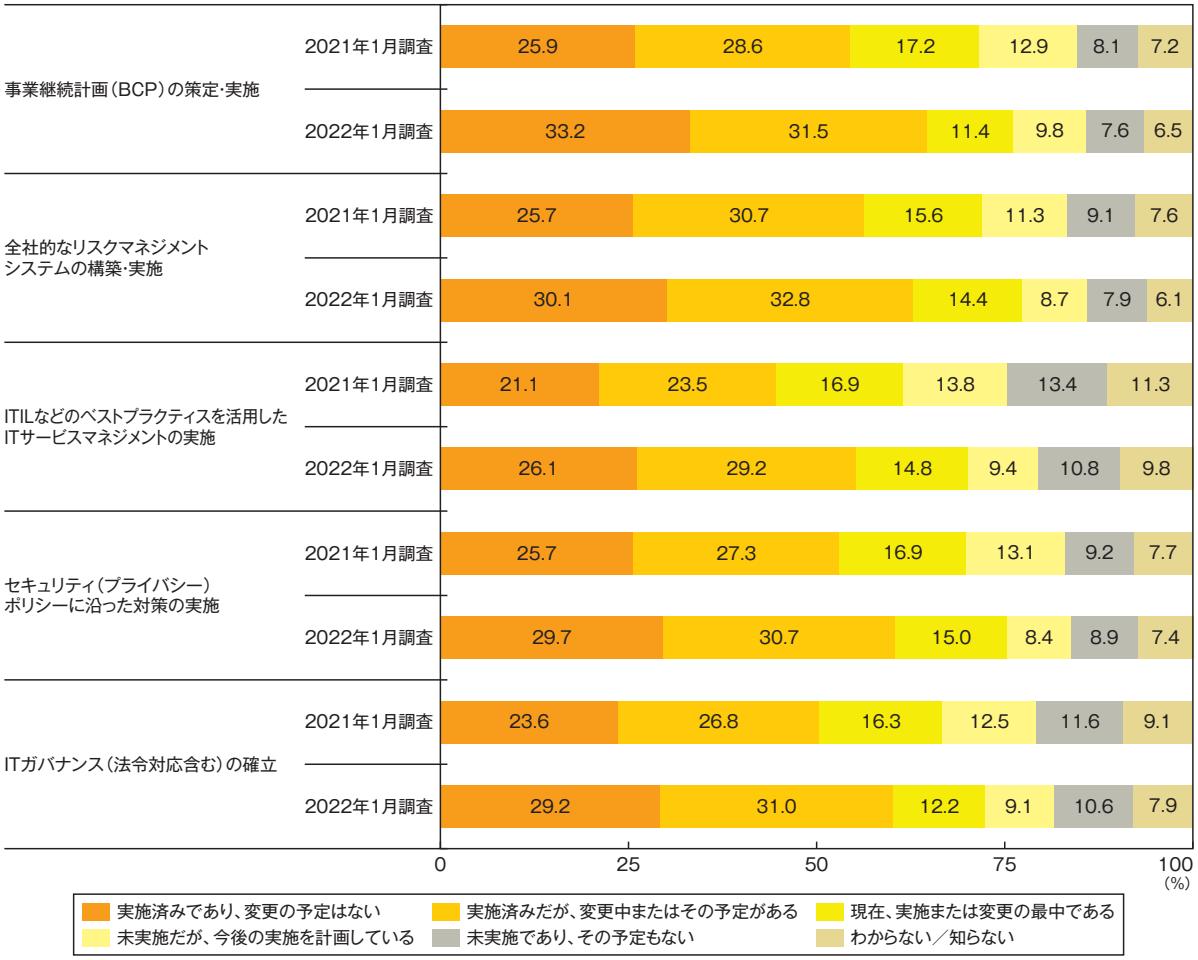
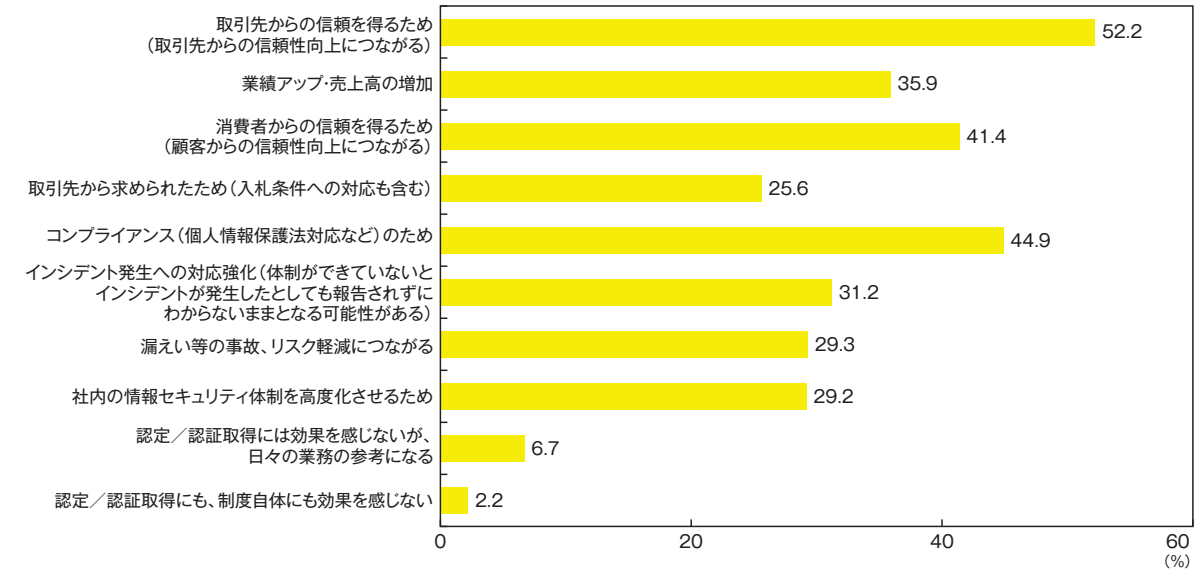


図８．システムリスクの軽減策の取組み状況（2021-2022年比較）

3-2. 情報セキュリティの第三者認証取得の価値

第三者から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」（52.2%）が最も多かった。次いで「コンプライアンスのため」（44.9%）、「消費者からの信頼を得るため」（41.4%）と続いており、対外的な理由から第三者認証取得に価値を感じていることがわかる。（図９）

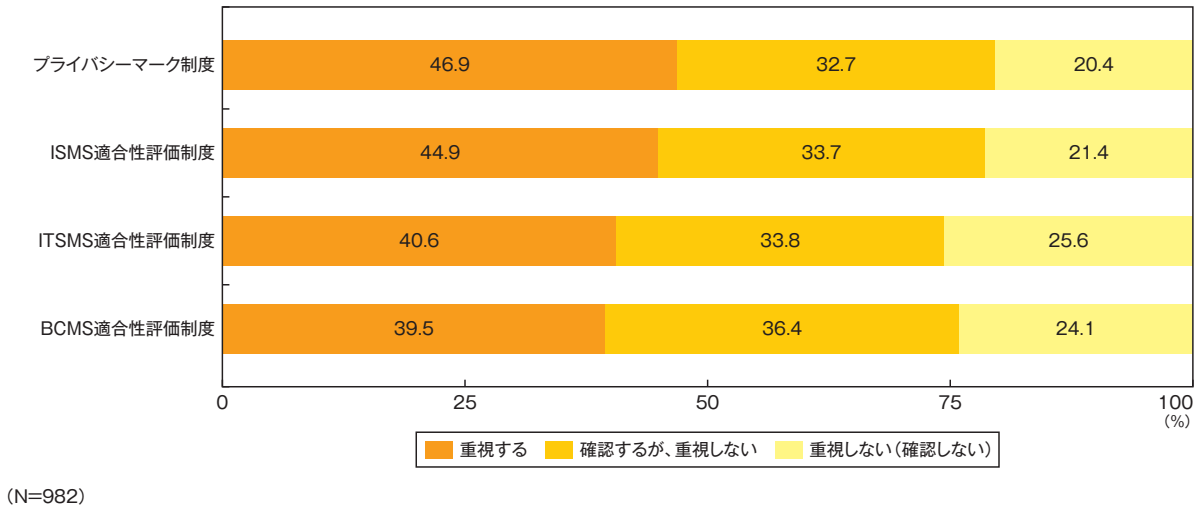


（N=730）
※第三者認証を「取得済」／「取得予定」／「制度を参考にしている」と回答した730件

図９．情報セキュリティの第三者認定／認証取得の価値

3-3. 取引先選定時の第三者認証取得の重視度

取引先選定時の認証取得の重視度では、「プライバシーマーク制度」（46.9%）が最も高く、次いで「ISMS適合性評価制度」（44.9%）、「ITSMS適合性評価制度」（40.6%）、「BCMS適合性評価制度」（39.5%）となっている。（図10）



（N=982）

図10．取引先選定時の認証取得の重視度

4　個人情報保護への取組み

2018年５月にEU一般データ保護規則（GDPR）が適用され、2022年４月１日にわが国で改正個人情報保護法が施行、その他、米国、中国など各国でプライバシー法制が整備されつつある。

ここでは改正個人情報保護法に対する取組みや、海外でプライバシー強化に向け導入が著しいプライバシーテックについて、わが国の現状を調査した。

4-1．個人情報保護についての取組み

個人情報保護についての取組みでは、「社員教育」（55.8%）が最も多く、次いで「管理体制の構築」（51.2%）、「規程類の整備」（40.6%）と続く。（図11）

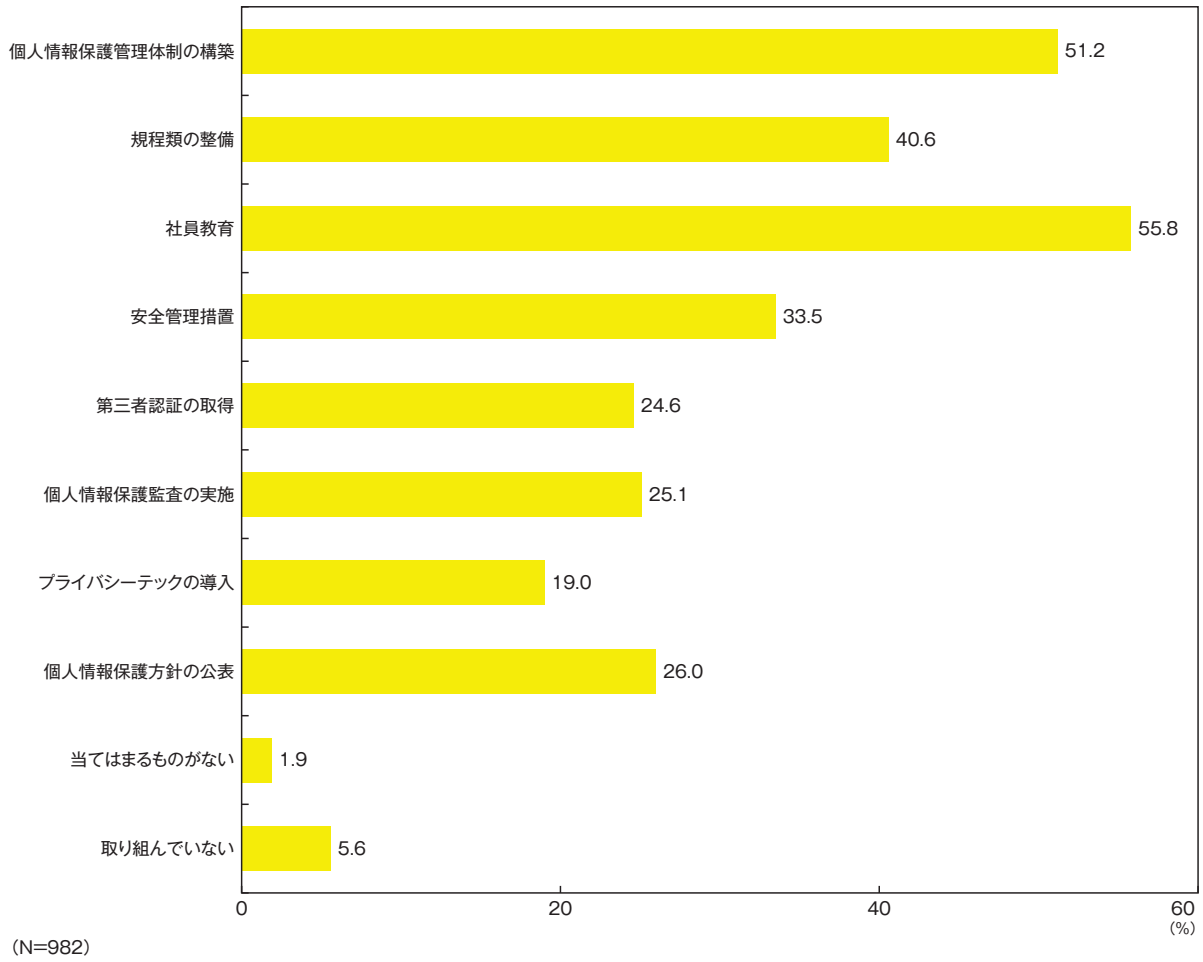


図11．個人情報保護についての取組み

4-2. 改正個人情報保護法施行に向けての取組み

改正個人情報保護法施行３カ月前時点での法対応の取組み状況を調査した。前項目の取組み同様、「社員教育」（44.0%）と「体制整備」（43.8%）の比率が高い。（図12）

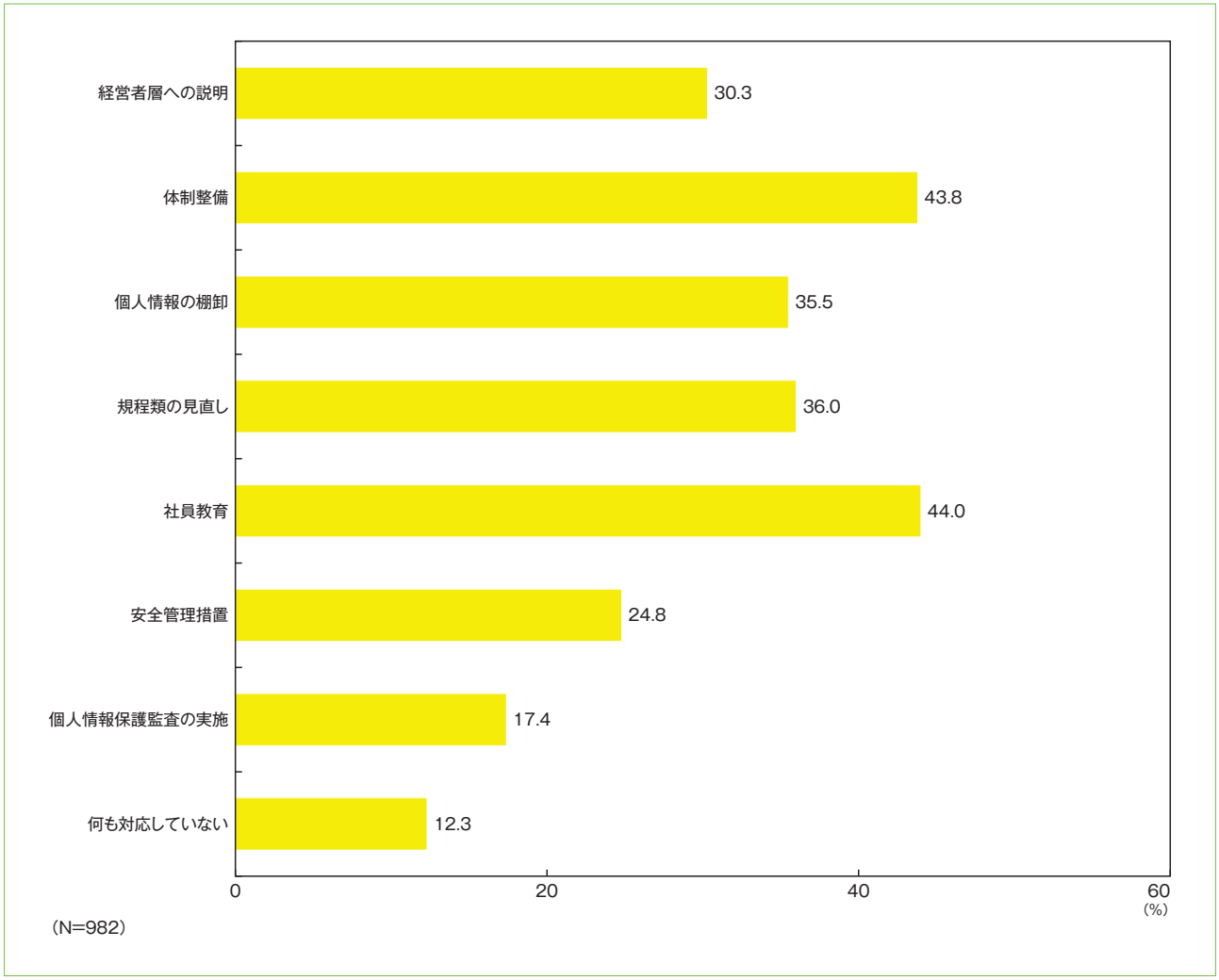


図12. 改正個人情報保護法施行に向けての取組み

4-3. プライバシーテックの導入状況

プライバシーテックの導入状況としては個人情報管理システム（44.0%）が最も多く、導入予定を含めると７割に達する。（図13）

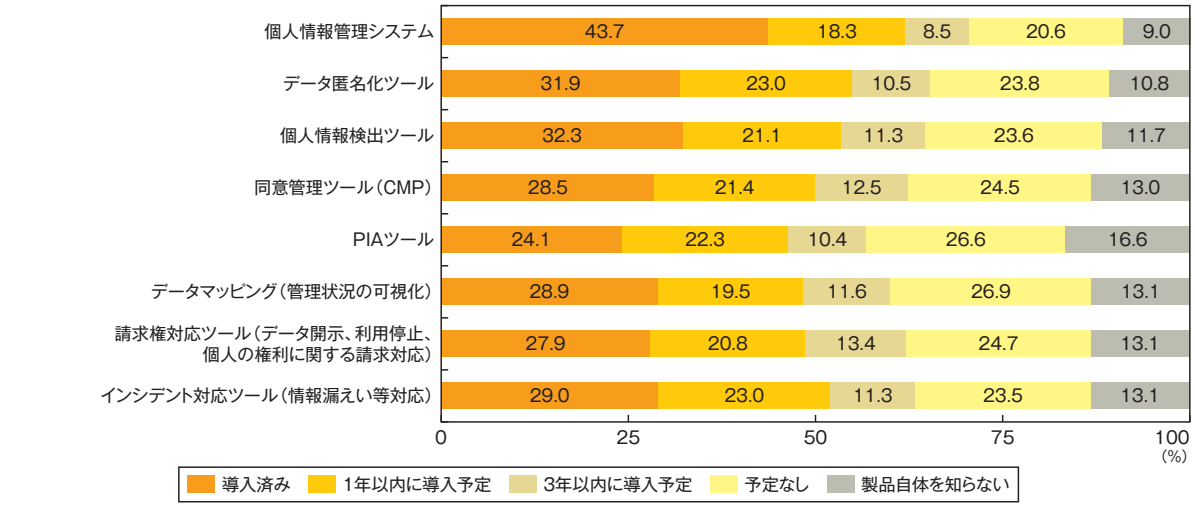


図13. プライバシーテックの導入状況

【コラム】プライバシーテックの概要と国内外のプライバシーテック市場の状況

国際プライバシー専門家協会（International Association of Privacy Professionals：IAPP）は、2017 年からプライバシーテック企業の調査を行い Privacy Tech Vendor Report を公開しています。Privacy Tech Vendor Report では、プライバシーテックは２つの主要なカテゴリに大別されるとしています。一つは、プライバシー担当部署向けに設計されたプライバシープログラム管理ソリューション（PPM：Privacy Program Management）、もう一つはプライバシー担当部署の要求と組織全体のビジネスニーズを同時に満たすように設計されたエンタープライズプライバシー管理ソリューション（EPM：Enterprise Privacy Management）です。PPM には、自動化されたプライバシー影響評価、同意管理ツール、データマッピングなどのプライバシープログラム実施のためのフレームワーク、開示・訂正・利用停止等の本人の権利に関連する要求を含む個人データに関する権利の行使を希望する個人からの問合せ対応を容易にするデータサブジェクト（本人）リクエストソリューション、インシデント発生時の対応に関して情報を提供するツール、世界の最新のプライバシー関連法に関する広範な情報を自動で提供する情報ツール、Cookie 規制遵守のためのウェブサイトスキャンツールなどがよく含まれます。EPM には、企業のデータ資産をスキャンしてマッピングする自動化技術や人工知能技術、データアクセスやデータフローを監視、管理、制御、監査するツールが含まれます。その他、これらをすべてのタスクを引き受けるように設計されたプラットフォームも登場しています。

近年、海外においては、プライバシーテック市場が急速に拡大しています。その理由として、GDPR の施行によりデータ保護への厳しい要件と違反行為に対して高額な賠償金が求められるようになったこと、データ利用環境が高度化と複雑化により企業がスケーラブルで効率的な技術ソリューションを求めるようになったことが挙げられます。IAPP によると、2017 年の調査開始時に 44 社だったプライバシーテック企業数は、2021 年には 365 社まで増加しており、多額の投資資金を集めるようになっています。

わが国でも、2022 年４月１日に改正個人情報保護法が施行され、個人に関する情報の取扱いは複雑さを増しており、多くの企業でプライバシーテックの導入および導入検討が進んでいることが、今回の調査で明らかになりました。海外同様に、わが国においてもプライバシーテックの導入が進み、プライバシーテック市場は拡大していくのではないかと考えられます。

JIPDEC　電子情報利活用研究部　調査研究グループリーダー　松下 尚史

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移行が進行している。

5-1. 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、昨今のゼロトラストセキュリティ化の流れで、「クラウドサービス用ファイアウォール」（39.1％から47.3%、約８ポイント増）や「クラウドサービス用WAF」（31.0％から38.0％、７ポイント増）などのクラウド用セキュリティサービス製品の利用が増えている。（図14）

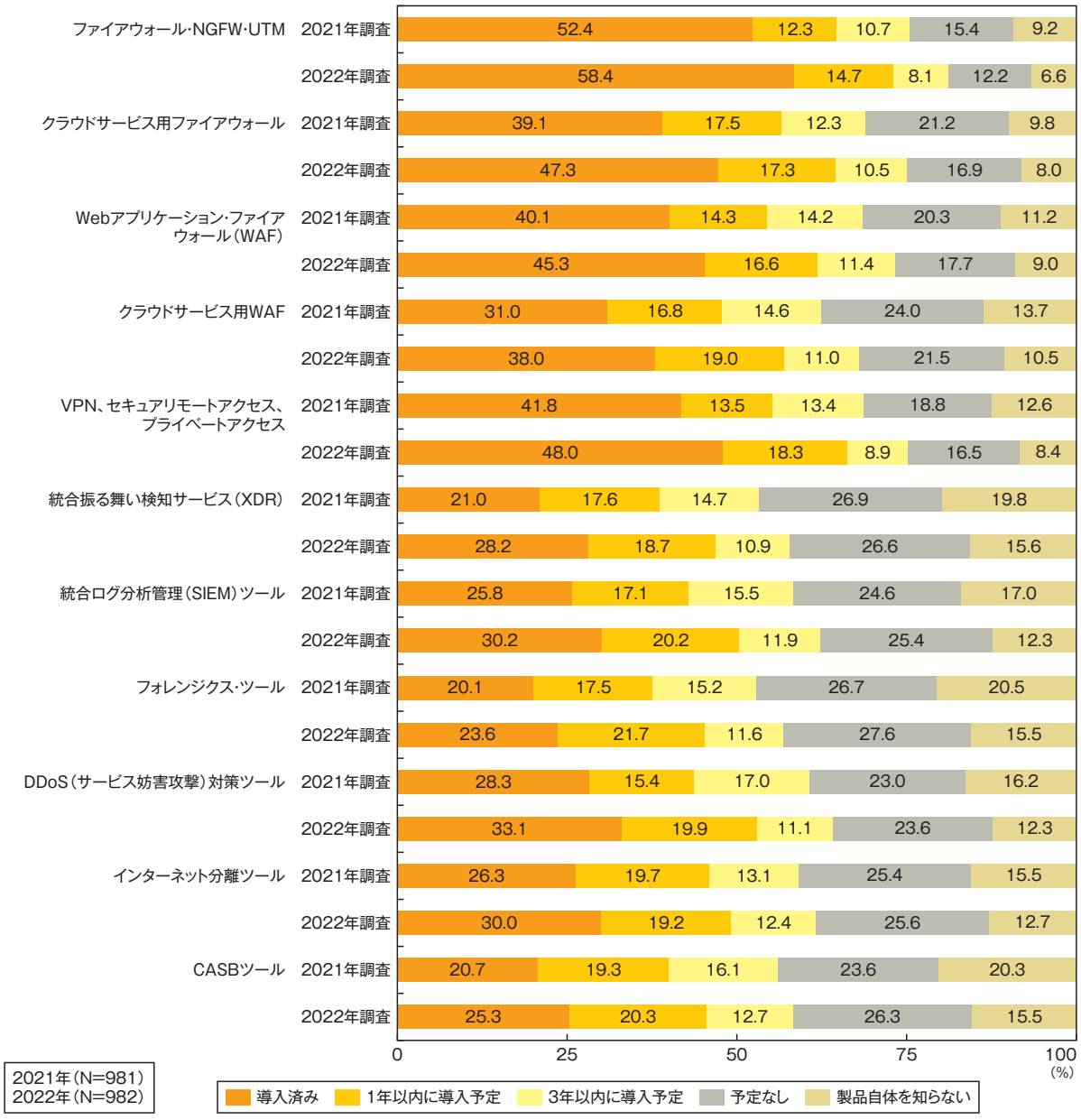


図14.　ネットワーク／ゲートウェイセキュリティ製品の利用状況（2021-2022年比較）

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は、従来の事前にウイルスを検知して感染を防止する「ウイルス対策ソフト」が最も導入割合が高いが、ウイルス感染後の不審な動きを検知し、被害の拡散を抑えることを主目的とした次世代型ウイルス対策ソフトである「EDRツール」の導入率が、前回調査の25.5％から33.2%へと、約６ポイント増加している。（図15）

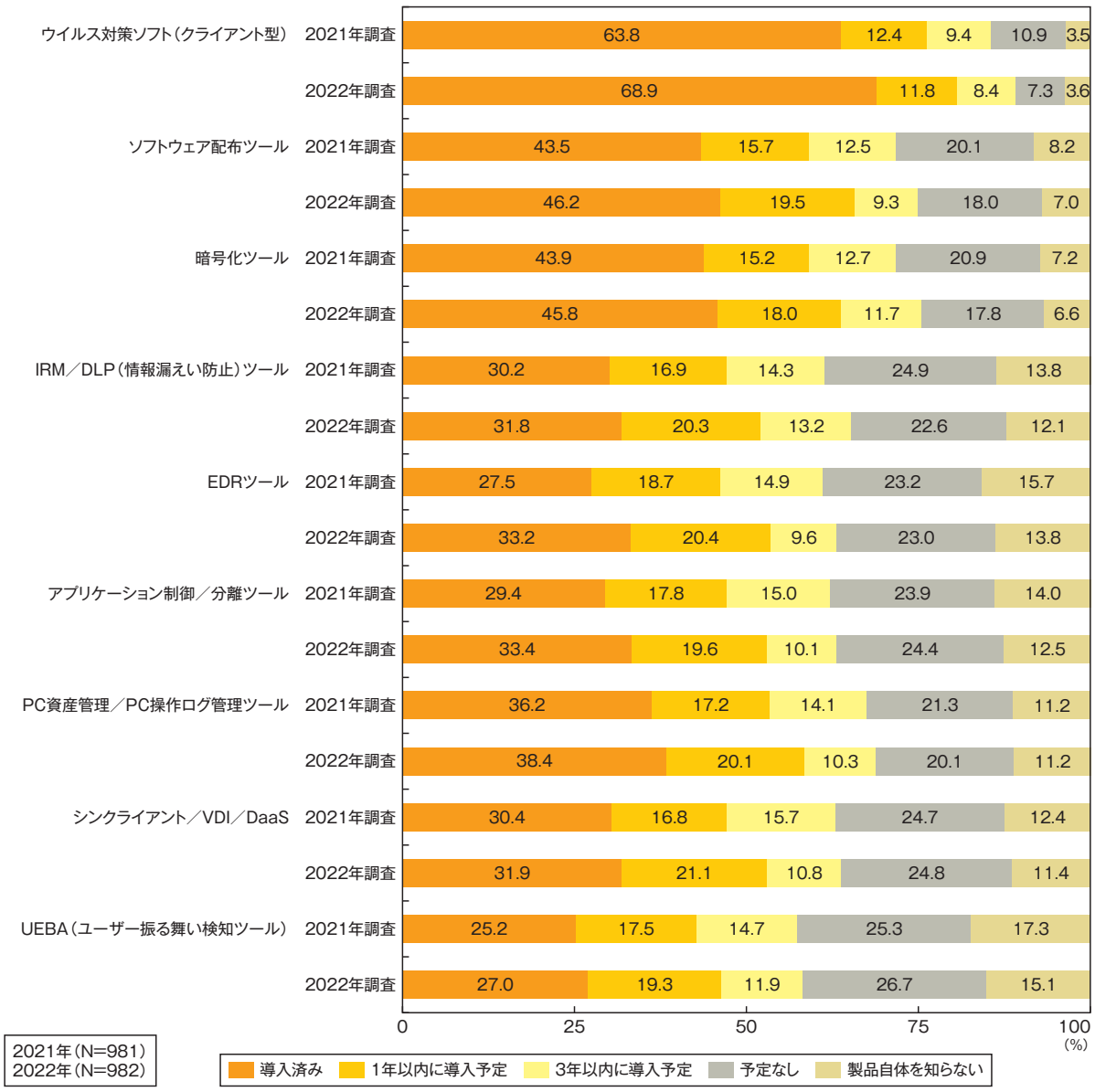


図15. エンドポイントセキュリティ製品の利用状況

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は、前年調査と大きな変化は見られていないが、マルウェア「Emotet」など、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」（44.6％）や「侵入検知サービス」（40.1％）の導入比率が４割を超え、導入予定を含めると約７割に近づいており、サービス利用が一般化しつつある。（図16）

利用済みのサービスについて前回調査と比べると、「セキュリティオペレーションセンターによる総合的なセキュリティ監視」が30.8％から35.9％と５ポイント増加している。

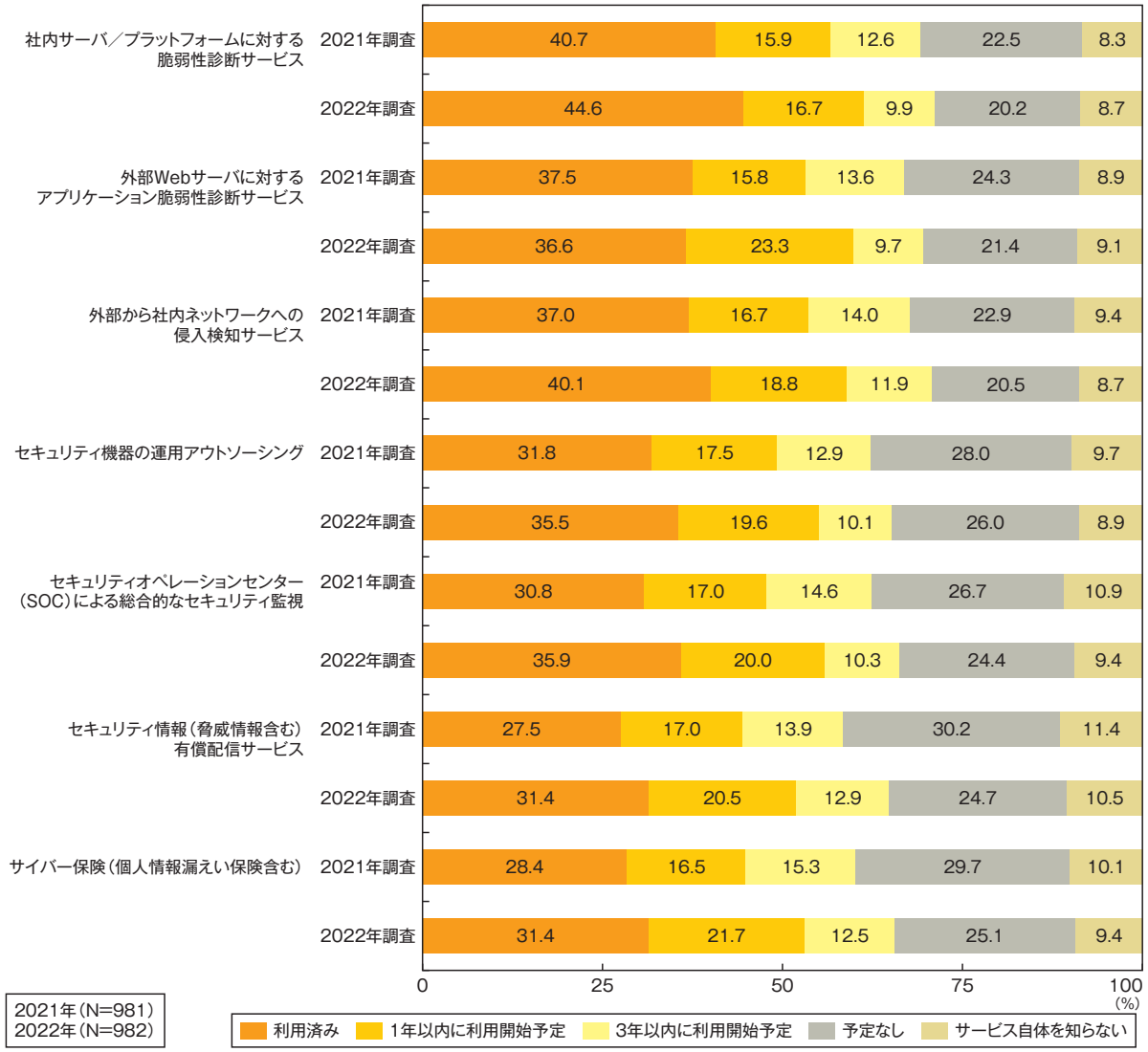
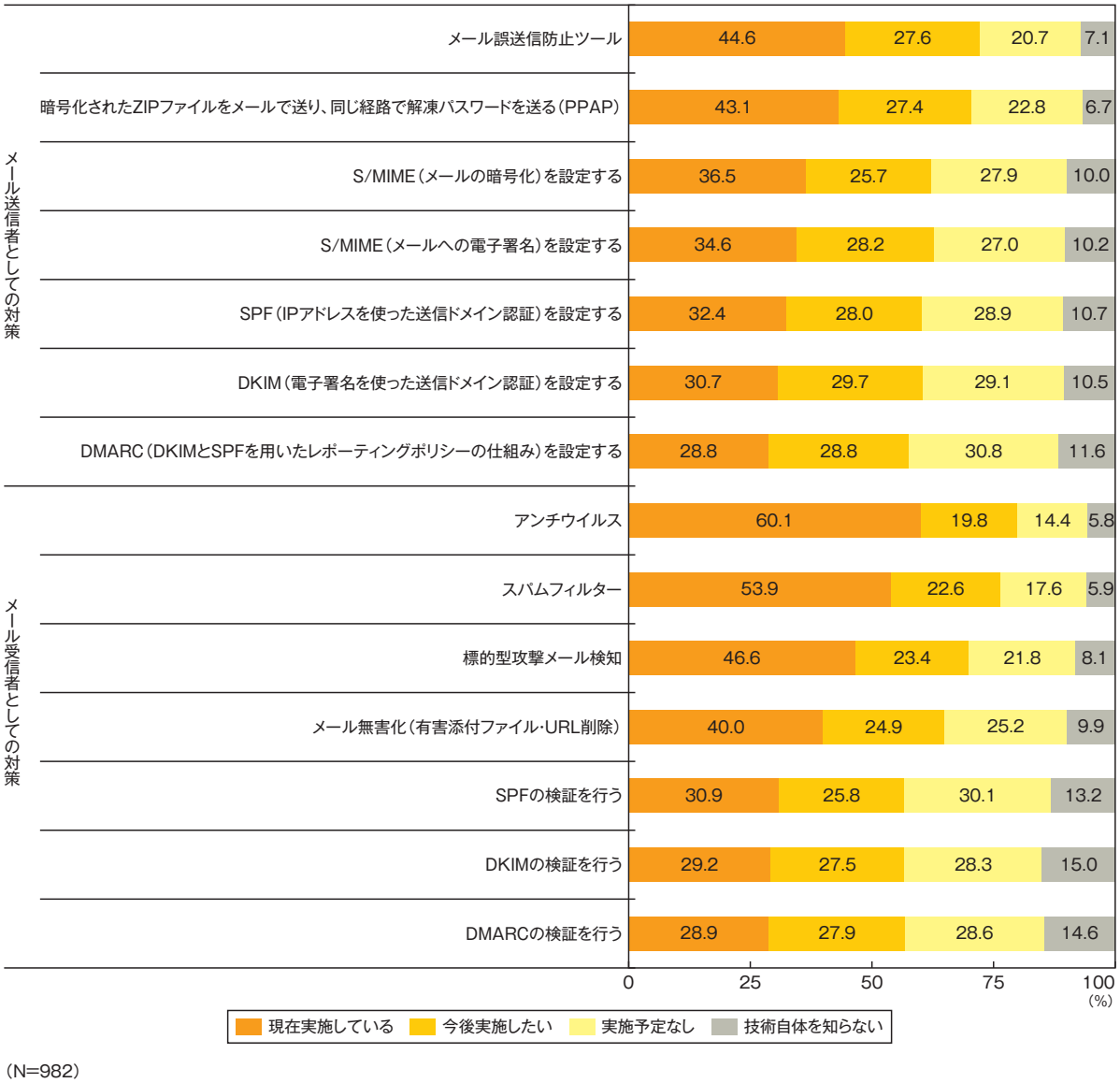


図16. セキュリティサービスの利用状況

5-4. 電子メールのセキュリティ対策状況

電子メールのセキュリティ対策状況は、送信側については「誤送信防止ツール」（44.6%）がトップで実施予定を含めると７割に達する。受信側は「アンチウイルス」（60.1%）がトップで、実施予定を含めると８割に達する。（図17）



（N=982）

図17. 電子メールのセキュリティ対策状況

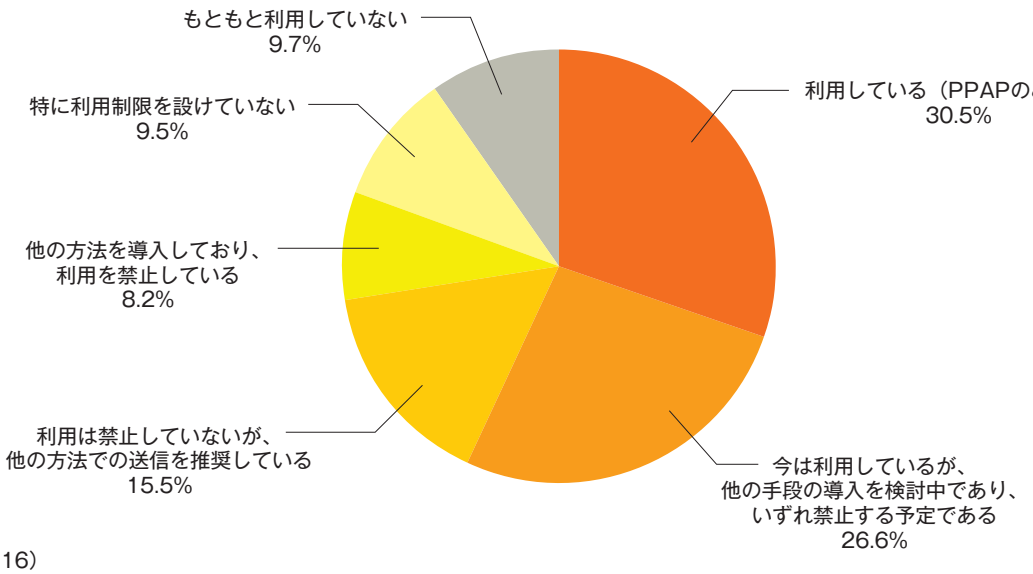
5-5. PPAPへの対応状況

Zipファイルを暗号化して添付ファイルで送り、同一経路でパスワードを知らせる送信方法、いわゆる「PPAP」について、送信／受信側それぞれの対応状況を調査した。

PPAPを「利用していない」、または「禁止している」企業は、送信側で17.9％となった。（図18）

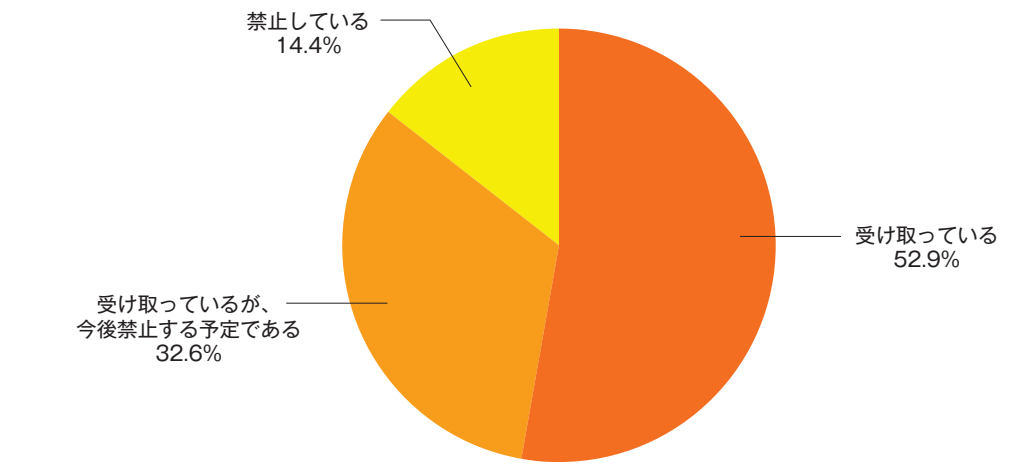
一方、受信側では暗号化Zipファイルを添付したなりすましメールの爆発的な流行などを受けて、「受け取っているが、今後禁止する予定である」が32.6％となった。（図19）

受信禁止の動きに伴い、送信時の対策の必要性が高まるため、「送信禁止を予定」する企業（26.6％）、「他の方法での送信を推奨する」企業（15.5％）の割合は、今後さらに高まる可能性があると考えられる。



（N=916）
※電子メールのセキュリティ対策状況で「技術自体を知らない」と回答した66件を除く

図18. PPAP（送信系）の状況



（N=916）
※電子メールのセキュリティ対策状況で「技術自体を知らない」と回答した66件を除く

図19. PPAP（受信系）の状況

【コラム】PPAP対策やなりすまし対策にS/MIME

カード会社や銀行、運送会社、通販会社など、いろいろな組織を騙ったなりすましメールも珍しくなくなってきました。ひと昔前だと、「文章で見抜ける」と言われていましたが、今はメールの本文を見ても、なかなか区別がつきません。「メールアドレスを見ろ、ドメインで判断しろ」と言われても、一般の人はなかなかピンときません。

そこで、「S/MIME※を使いましょう」とお話しています。近年は多くのメーラーが対応するようになりました。S/MIMEとは、電子証明書を用いたなりすまし対策技術の一つで、“電子署名”と“暗号化”機能を提供するものです。S/MIMEを使うのに必要な電子証明書も昔ほど取得費用が高くなくなったので、徐々に広まっているようです。

最近はマルウェア「Emotet」が飛び交っているのをよく見聞きするようになりました。Emotetによるなりすましメールでは実際にその相手とのやり取りで使われている文章が件名やメール本文に使われるので、騙されやすいようです。Emotetは暗号化されたZIPファイルで送られてくることが多いことでも知られています。

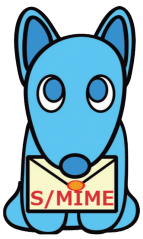
日本では、暗号化されたZIPファイルをメール送信したあとにパスワードをメールする方式はPPAPと呼ばれ、よく使われているようですが、暗号化されたZIPファイルにはウイルス対策ソフトのスキャンが機能しないため、PPAPを利用する習慣のある日本ではより被害が拡大しているようです。よって、最近ではPPAPのメールを受け取らない、送らないと宣言する企業も少しずつ増えているようです。

S/MIMEは、電子署名に加えて、暗号化されたメールのやり取りにも使えますので、有力なPPAP対策となります。S/MIME以外のPPAP対策としては、クラウドを利用したデータ授受の方式を検討されるところもあるようです。

※ S/MIME（Secure / Multipurpose Internet Mail Extensions）
電子証明書を使って、メールが改ざんされていないことや送信元がなりすまされていないことを保証したり、暗号化ができる仕組み

なりすましメール対策キャラクター「エスマいぬ」

メールのなりすまし対策や暗号化ができるS/MIMEを使うんだわんっ！



1999年6月の港区生まれ。性格は社交的。
中身を見られないように封筒で送る。

エスマいぬはJIPDECの登録商標®です。

JIPDEC　セキュリティマネジメント推進室　主査　高倉 万記子

5-6. 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は「ID・パスワード」（82.6%）が最も多いが、今後の利用予定は少ない（6.6%）。今後の利用予定が多いのは、「生体認証」（32.8%）や「多要素認証」（29.7%）、「IDaaS」（27.1%）となっている。（図20）

なお、現在利用している手段は前回調査と比較しても大きな変化は見られなかった。

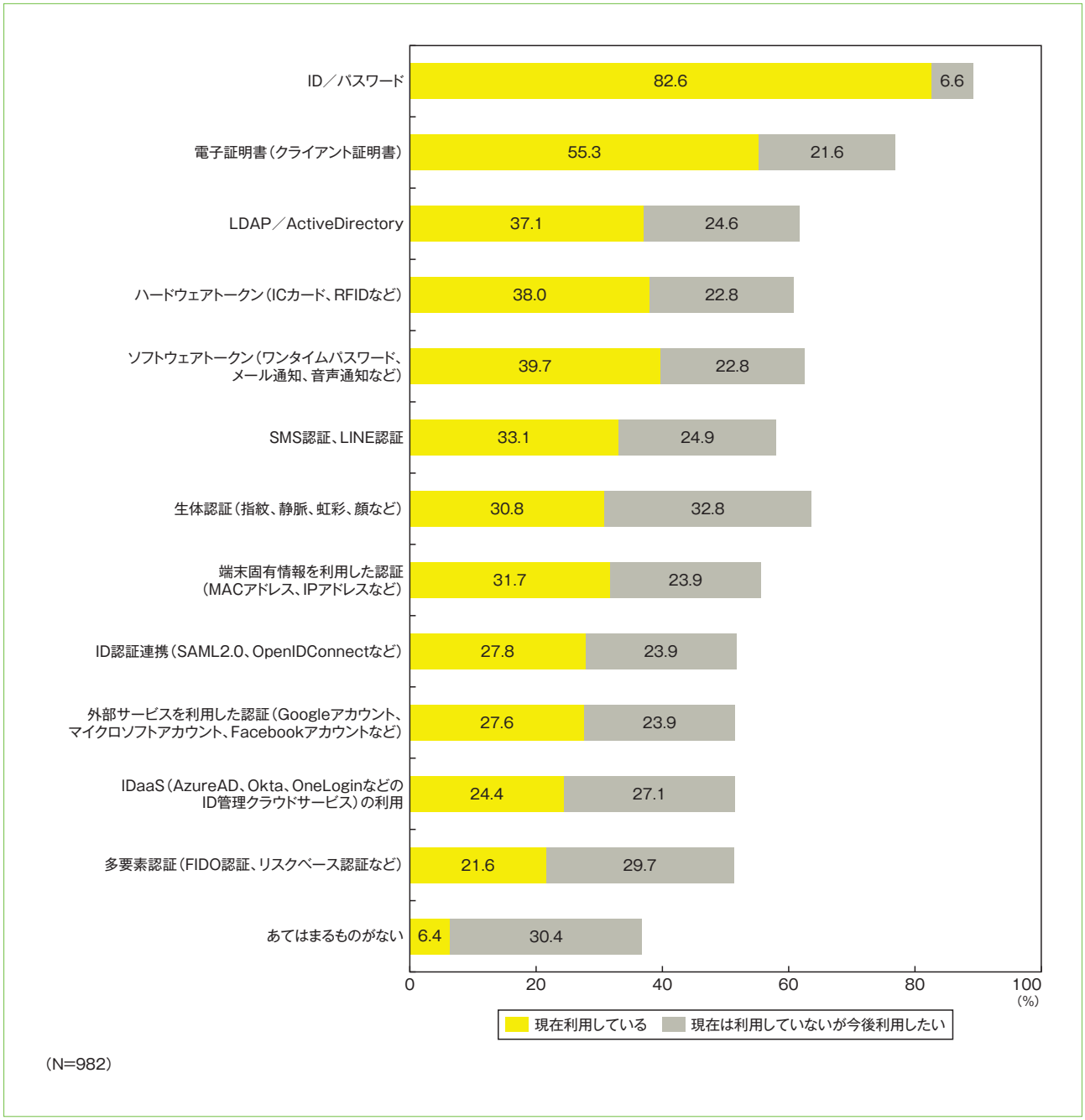


図20. 高機密性システムへのアクセス認証手段

6　テレワークとクラウドの動向

コロナ禍も３年目を迎えたことで、テレワークが通常の勤務形態となり、クラウドサービスの利用も増加している。一方で、リモート環境下でのセキュリティ対策強化が必須となることから、テレワークの導入状況、クラウドサービスの利用状況、セキュリティ対策の現状を調査した。

6-1. テレワークの導入状況

「コロナ禍を契機にテレワークを導入した」企業が49.4%で、「以前から導入している」（23.3%）を合わせると７割超がテレワークを導入しており、ワークスタイルの一つとして定着しつつある。（図21）

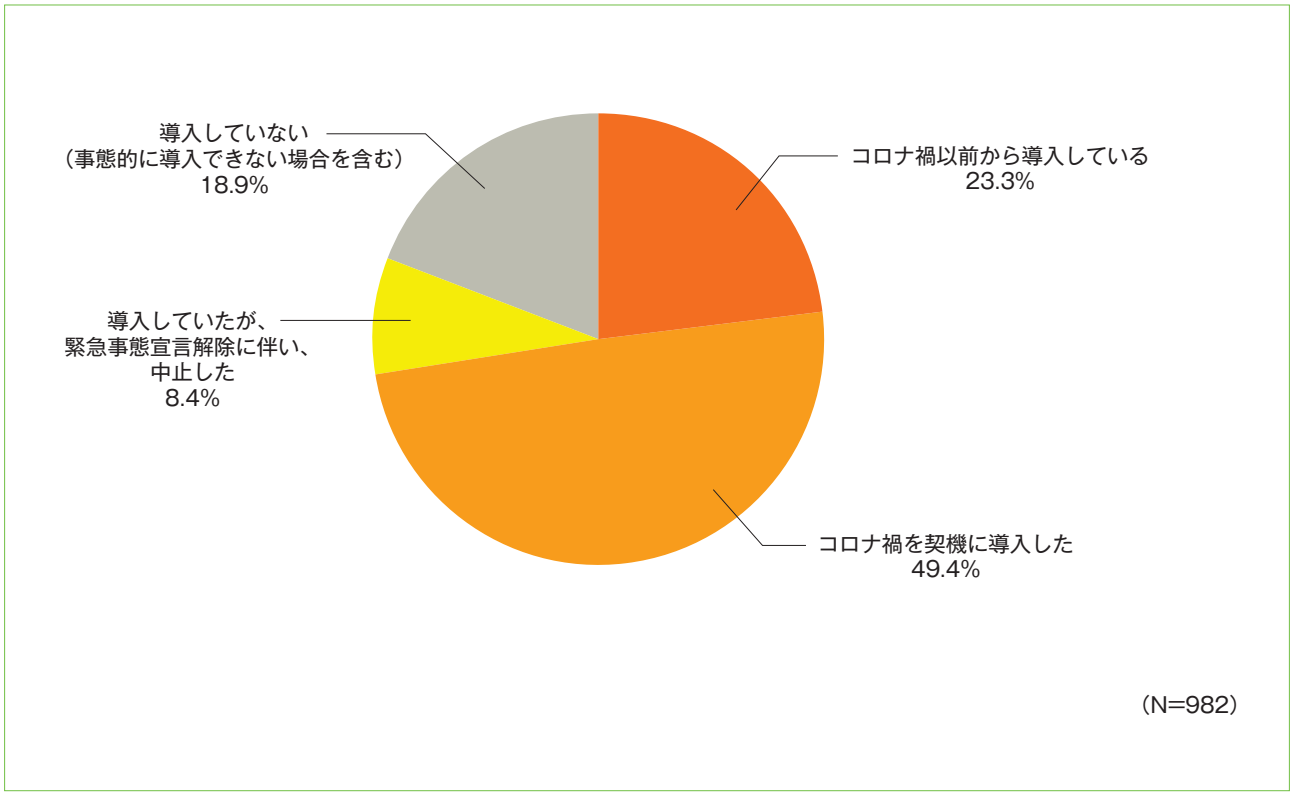
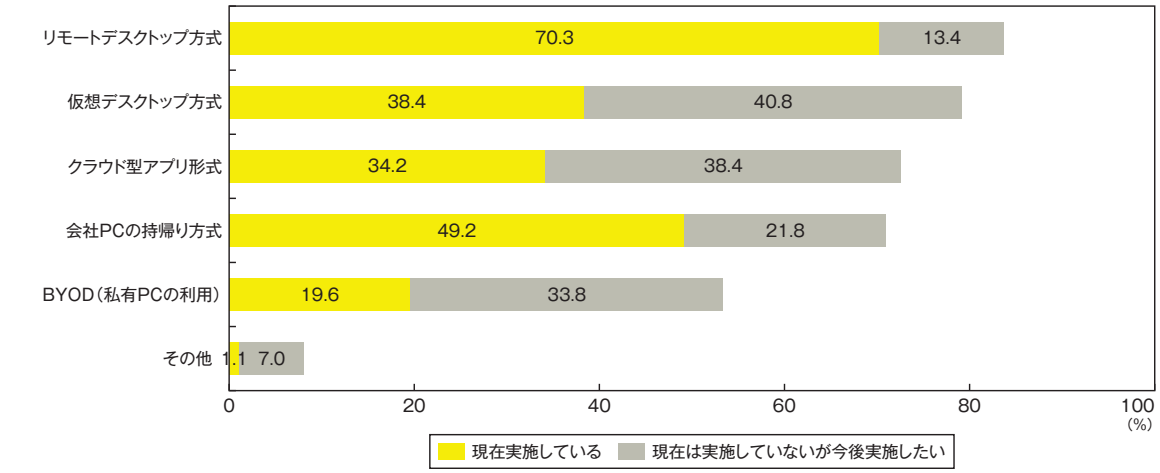


図21．テレワークの導入状況

6-2. テレワークのシステム環境（方式）

テレワークの方式としては「リモートデスクトップ方式」（70.3%）が最も多く、次いで「会社PCの持帰り方式」（49.2%）となった。今後実施したい方式としては「仮想デスクトップ」や「クラウド型アプリ」、「BYOD」が挙げられている。（図22）

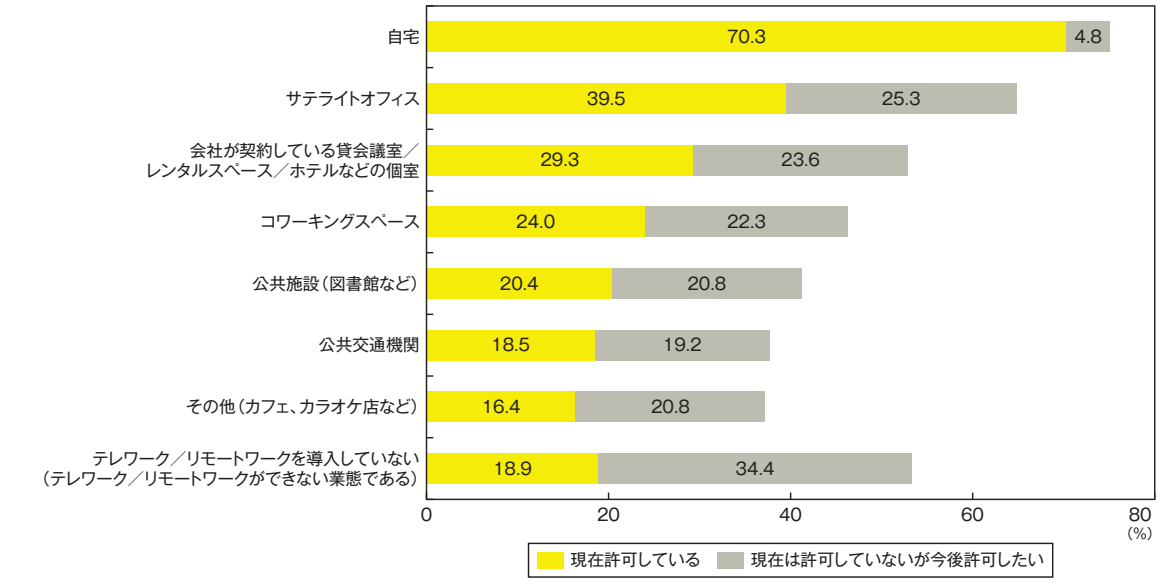


(N=714)
※テレワークの導入状況で「テレワークを導入している」と回答した714件

図22. テレワークのシステム環境

6-3. テレワークの場所

テレワークの場所は、現状では「自宅」（70.3%）が最も多く、「サテライトオフィス」（39.5%）が続くが、今後については「会社契約の貸会議室」「コワーキングスペース」「公共施設」など多様化する可能性がみられる。（図23）



(N=982)

図23. テレワークのシステム場所

6-4. 柔軟なワークスタイルを実現するためのセキュリティ対策

柔軟なワークスタイルを実現するためのセキュリティ対策としては、「スマートデバイスのセキュリティ対策」が47.0%、「端末にデータを残さない」が38.6%で、他の対策は２～３割となっている。（図24）

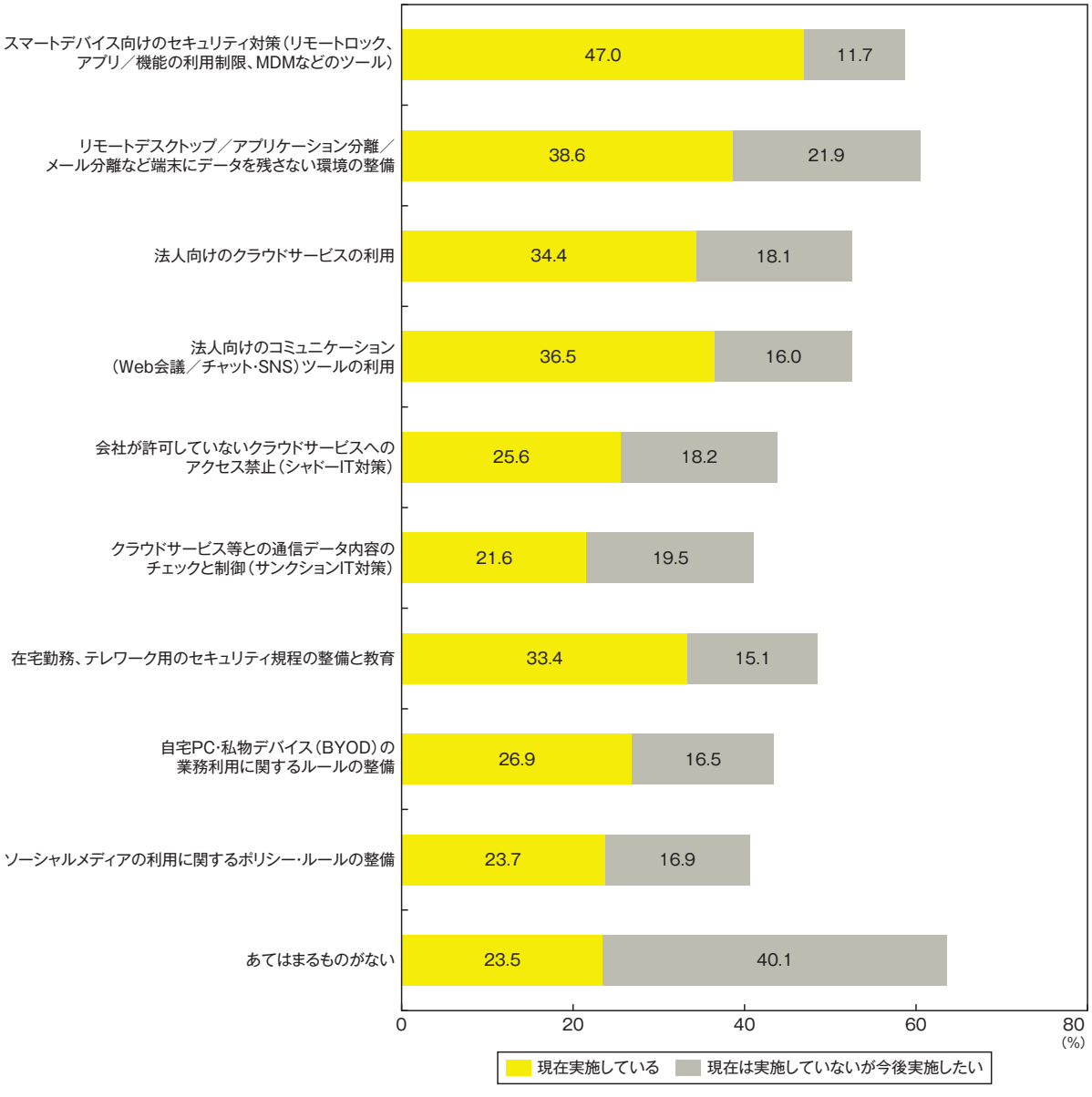


図24. 柔軟なワークスタイルを実現するためのセキュリティ対策

6-5. クラウドサービス利用状況

働き方改革を進めるうえで、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利用状況について調査を行った。

今回小規模事業者も対象にしたことで、クラウド利用状況は若干減少したが、約９割はなんらかのクラウドサービスを利用している。（図25）

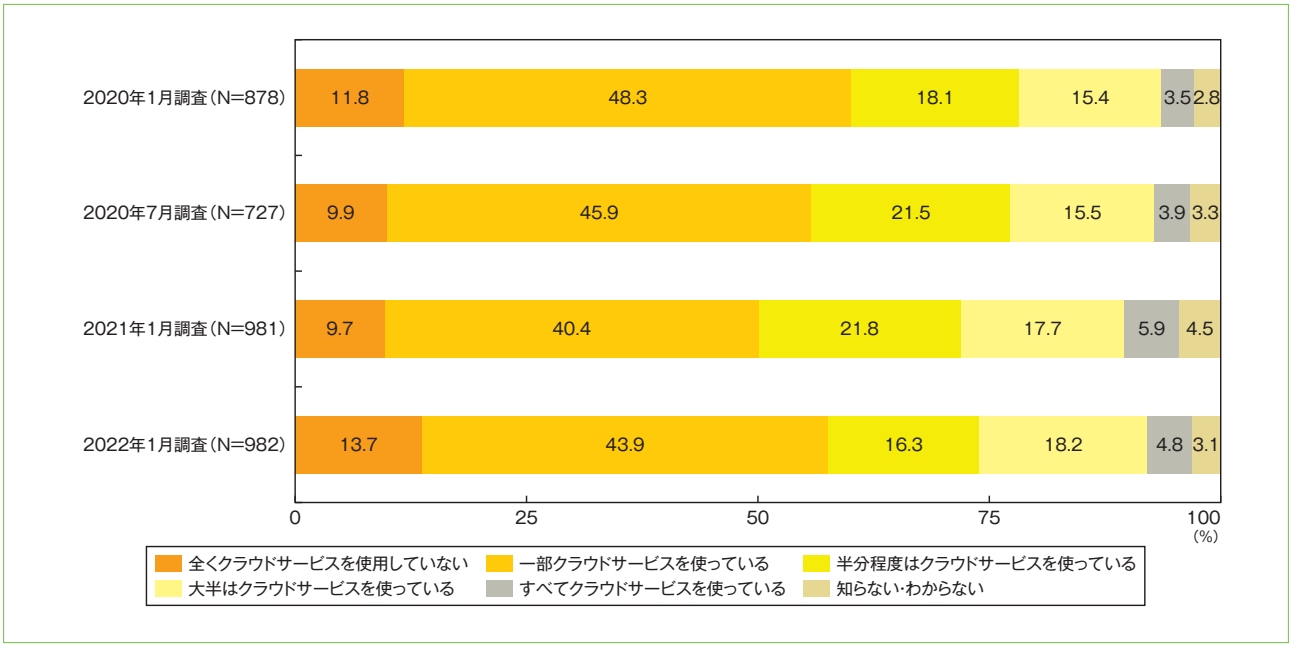


図25. クラウドサービスの利用状況（2020-2022年比較）

6-6. クラウドサービスの利用方法

クラウドサービスの利用方法としては、「コンテナサービス上で自社アプリを開発または使用」（33.6%）がトップとなっており、「SaaSを利用」（31.1%）、「IaaS/PaaS上で自社アプリを開発または移行して使用」（31.0%）がほぼ同率となり、コンテナサービスが普及してきている。（図26）

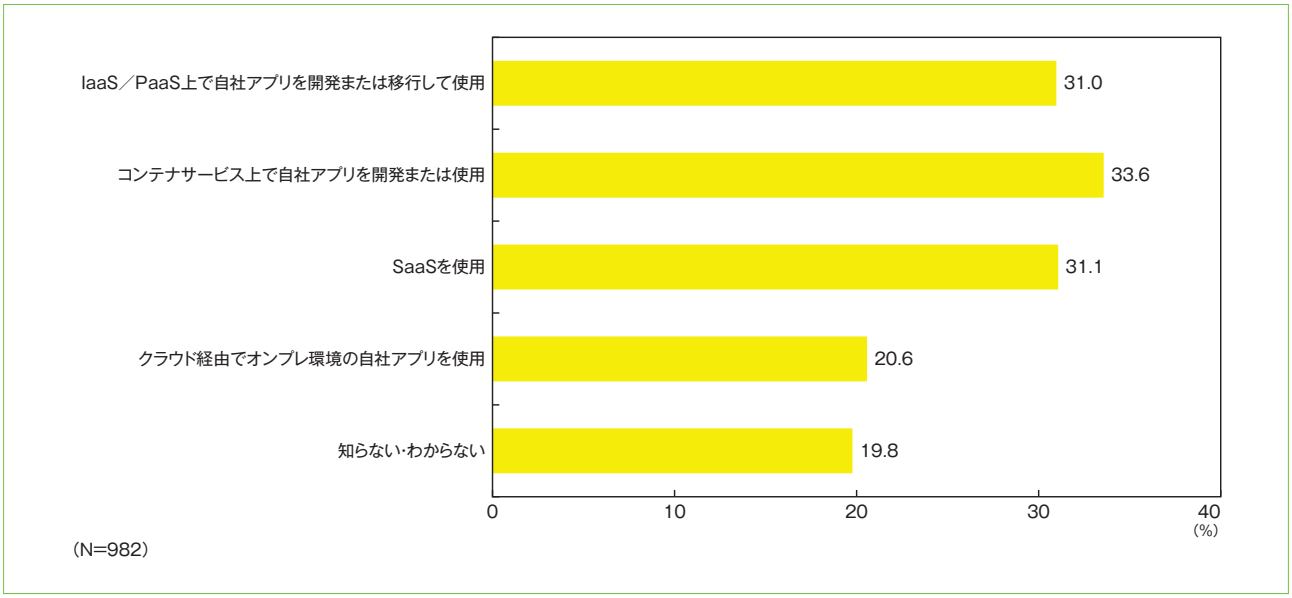


図26. クラウドサービスの利用方法

6-7. クラウドサービスの選定ポイント

クラウドサービス選定のポイントとしては、前回調査に引き続き「コスト」（51.8%）が１位、次いで「セキュリティに関する認証・認定取得による信頼性の確保」（41.2%）と「セキュリティの対策がきちんとしている」（35.4%）が続いている。（図27）

前回調査と比較すると、「サービス事業者の企業名（ブランド）」が19.4％から27.9％と8.5ポイント増加、「同業他社が利用している」が12.2％から18.0％と約６ポイント増加したのに対し、「セキュリティ対策」や「BCP対応」については６～７ポイント減少した。

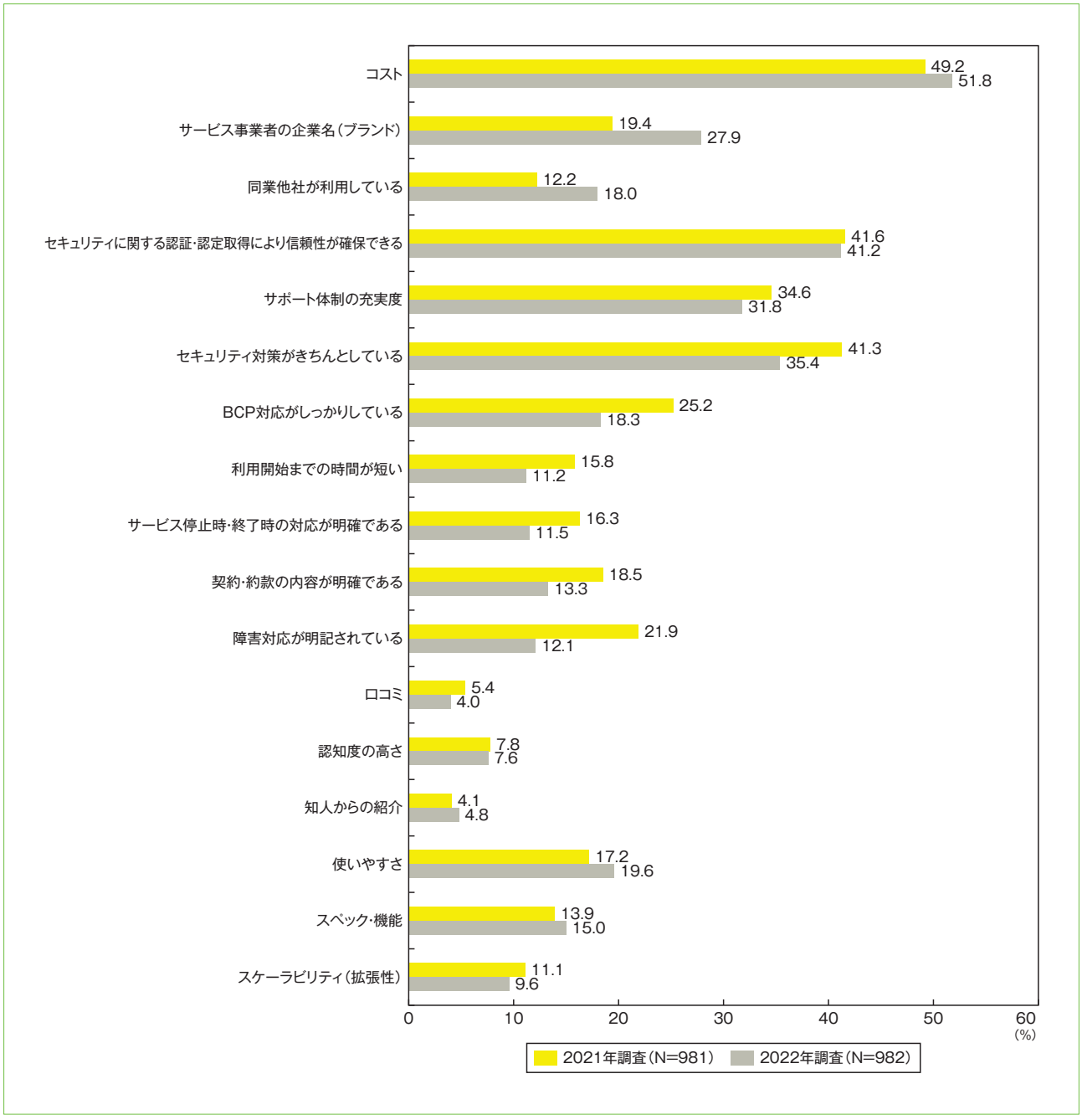
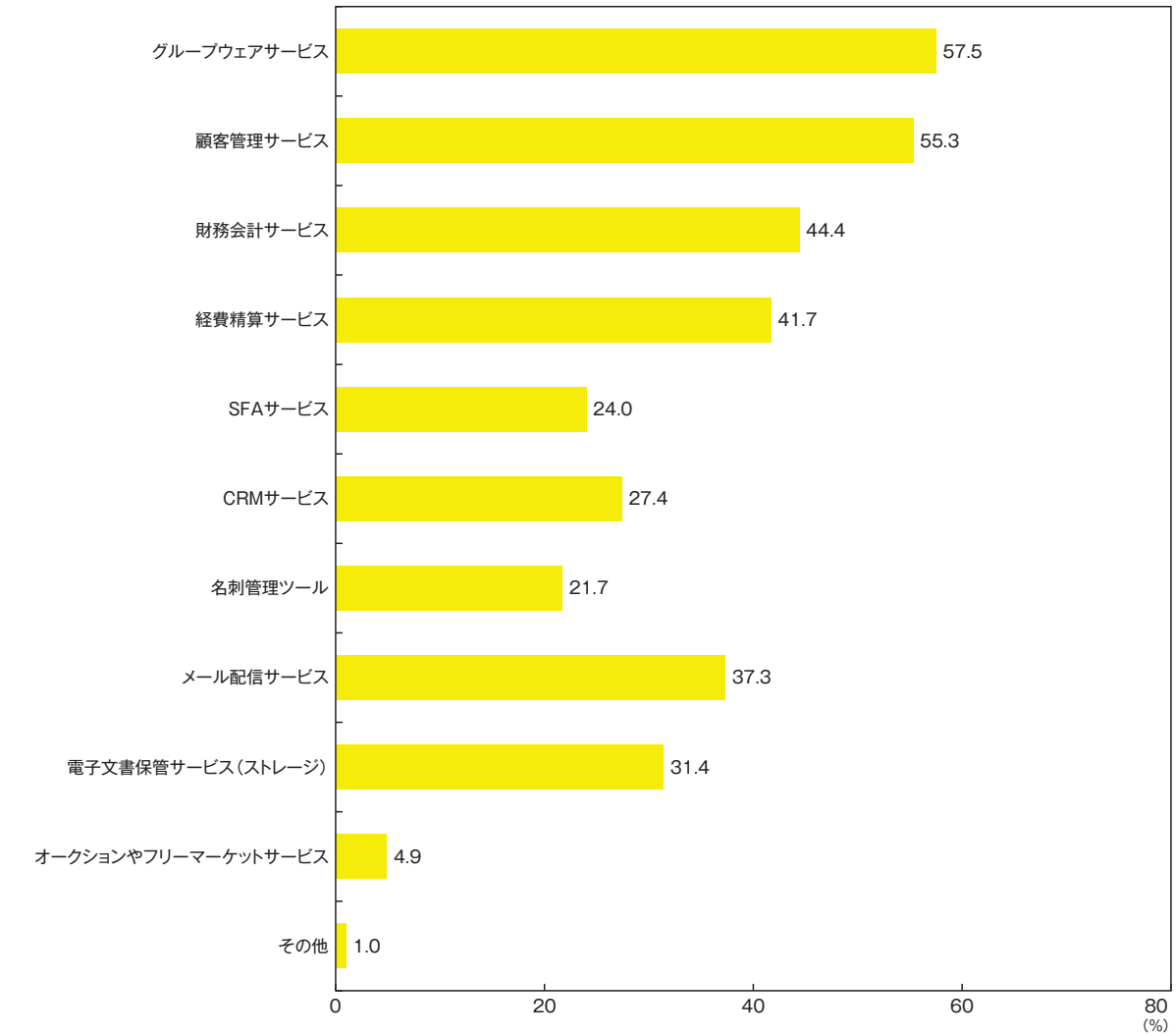


図27. クラウドサービスを選定する際のポイント

6-8. 信頼性を重視するクラウドサービス

クラウドサービス選定のポイントとして、「セキュリティに関する認証・認定取得により信頼性が確保できる」を選択した事業者が実際に信頼性を重視して選定するクラウドサービスは、1位が「グループウェア」（57.5%）、次いで「顧客管理サービス」（55.3%）、「財務管理サービス」（44.4%）となった。（図28）



（N=405）
※「セキュリティに関する認証・認定取得により信頼性が確保できる」を選択した405件

図28. 信頼性を重視するクラウドサービス

7　電子契約関連、DX 推進

政府によるデジタル化推進や３年目を迎えるコロナ禍によりデジタルワークスタイルが進んできている。本章では、デジタルワークスタイルを支える電子契約、DX推進、電子インボイスの導入状況について調査した。

7-1. 電子化したい業務プロセス

電子化したいとの回答が最も多かったのは、「経費精算（旅費・交通費）」（41.8%）で、次いで、「請求処理」（40.1%）、「経費精算（交際費）」（37.9%）と続いている。（図29）

過去３年間との比較で大きく変化が見られたのは「経費精算（交際費）」で、過去３回の調査では、３割程度だったのが、前回調査から７ポイント増加となった。

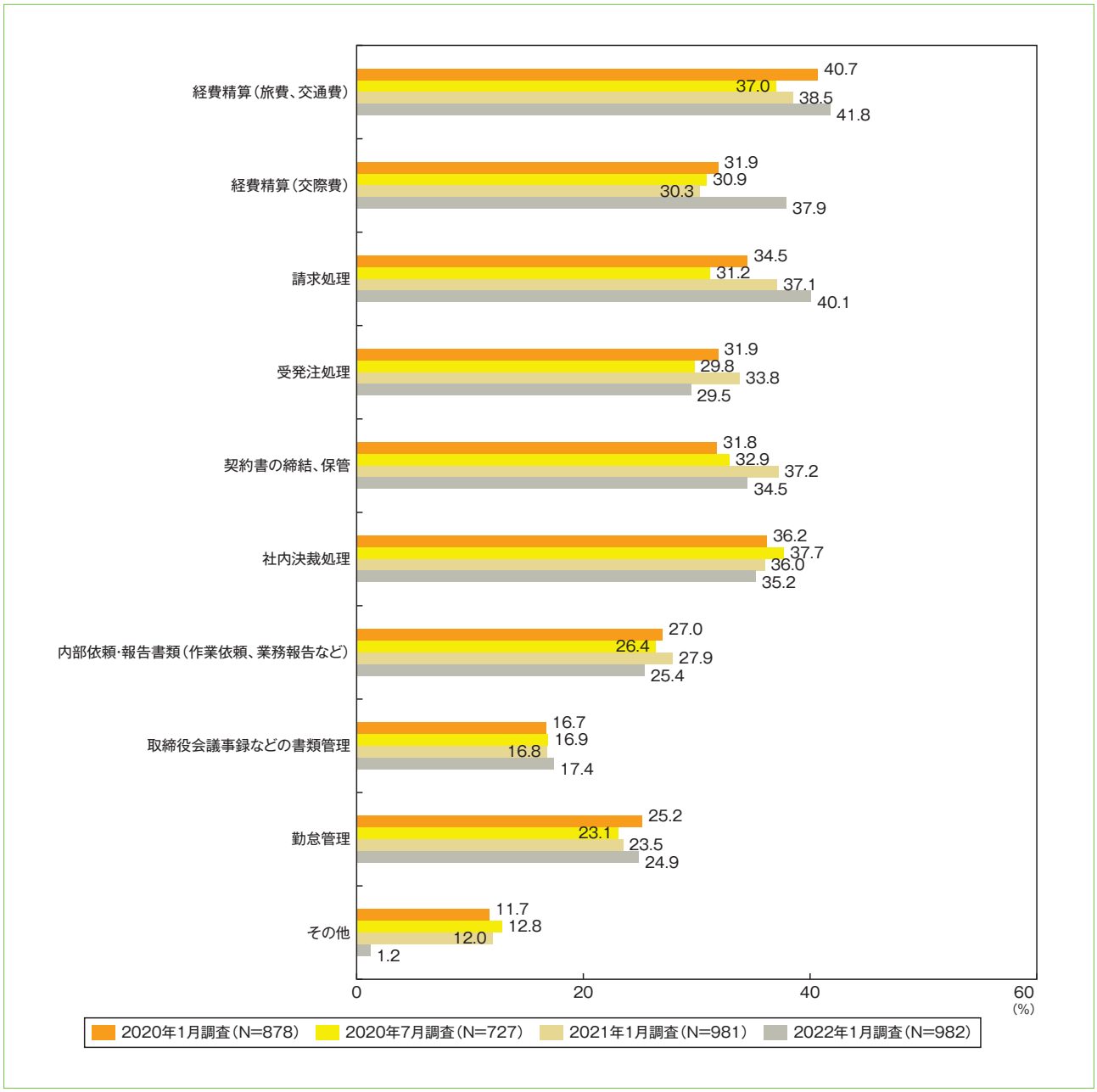


図29.　電子化したい業務プロセス

7-2. 電子インボイスへの対応

2023年10月に導入される適格請求書保存方式（インボイス制度）への対応として、買手が仕入税額控除の適用を受けるために必要となる「適格請求書」を電子化した「電子インボイス」への対応状況を調査した。

「国際標準仕様（Peppol）を基とした電子インボイスの利用が決まっている」が19.1%、「国内標準仕様（EIPA）の導入を検討している」が21.8%となっているが、「利用は決まっているがシステムは決まっていない」と「導入検討中」も１割以上あり、まだ対応はさまざまで収束傾向にはなっていない。（図30）

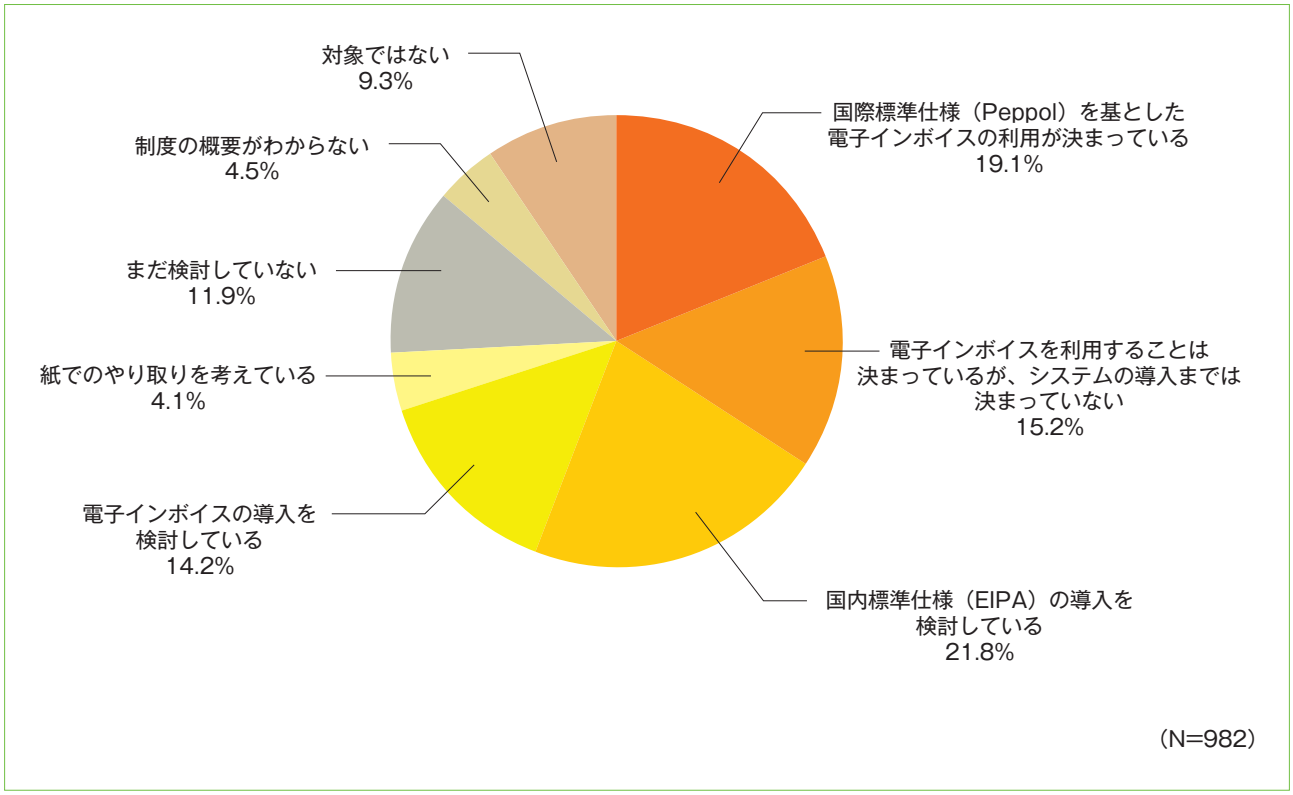


図30. 電子インボイスへの対応

7-3. 電子契約の利用状況

電子契約の利用状況では「当事者型電子署名」(26.0%) が最も多く、「立会人型電子署名」(18.4%) が続き、「両方利用」や「電子署名を利用しない電子契約」、「電子署名を利用しているかわからないが電子契約を利用している」を入れると、約７割が何らかの電子契約を利用している。(図31)

何らかの方法で電子契約を利用している割合は前回調査の67.2%から69.7%へ若干ではあるが増加しており、その中で、「当事者型」が14.4%から26.0%と、10ポイント以上の増加が見られた。

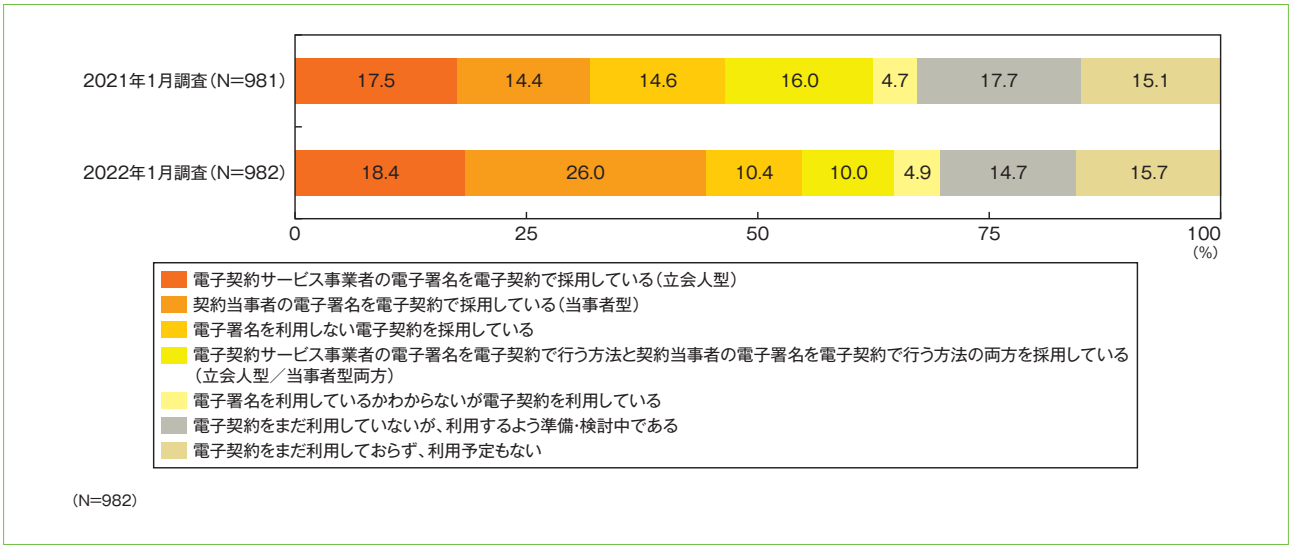


図31. 電子契約の利用状況（2021-2022比較）

7-4. 電子契約導入時に重視するポイント

電子契約を導入する際に重視するポイントとして「サービスコスト」(46.9%) が１位で、次いで「サービス事業者がセキュリティ認証・認定を取得している」(35.0%) があげられている。(図32)

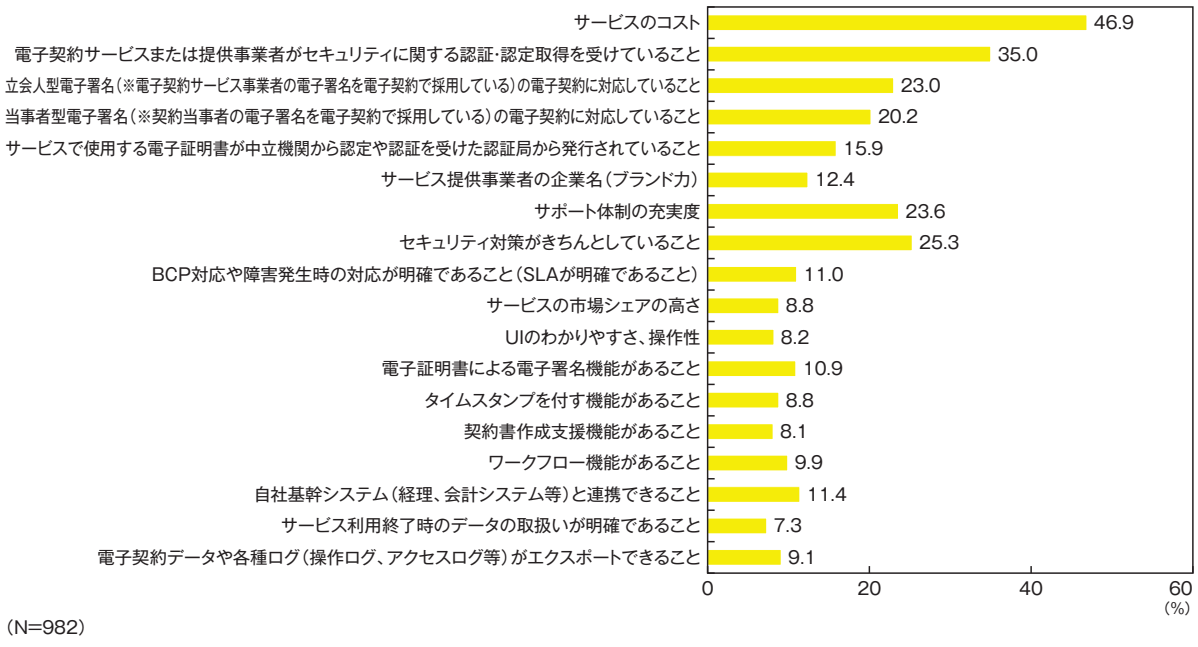
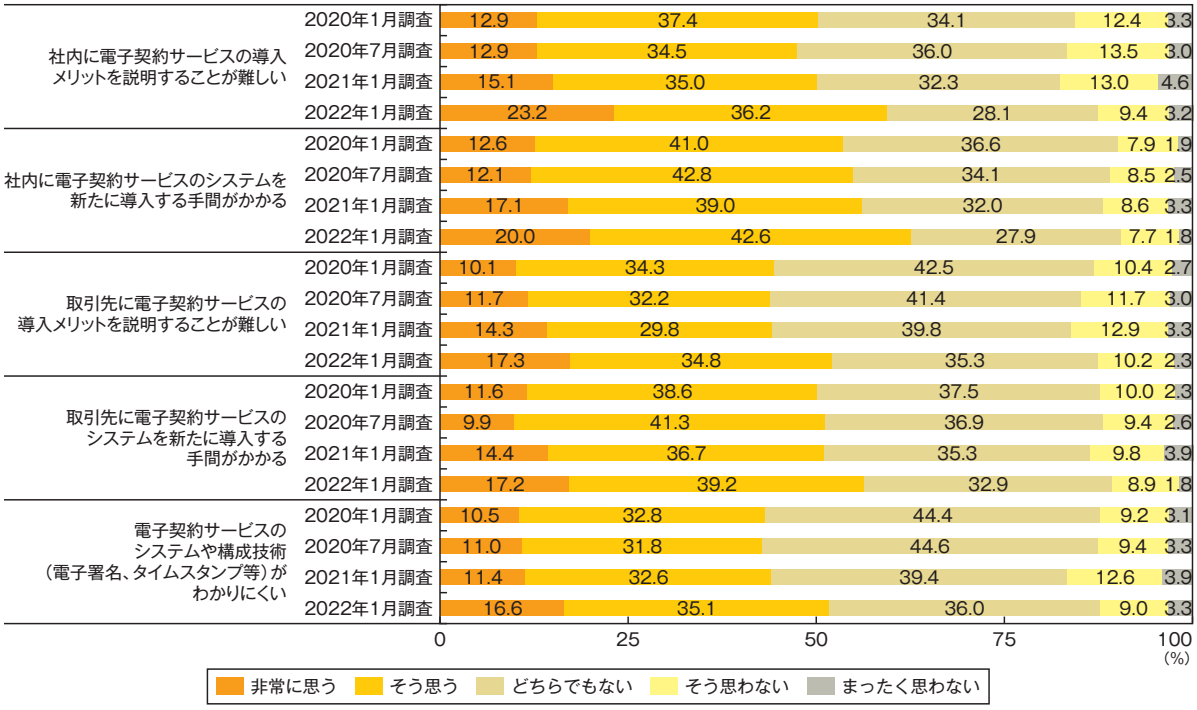


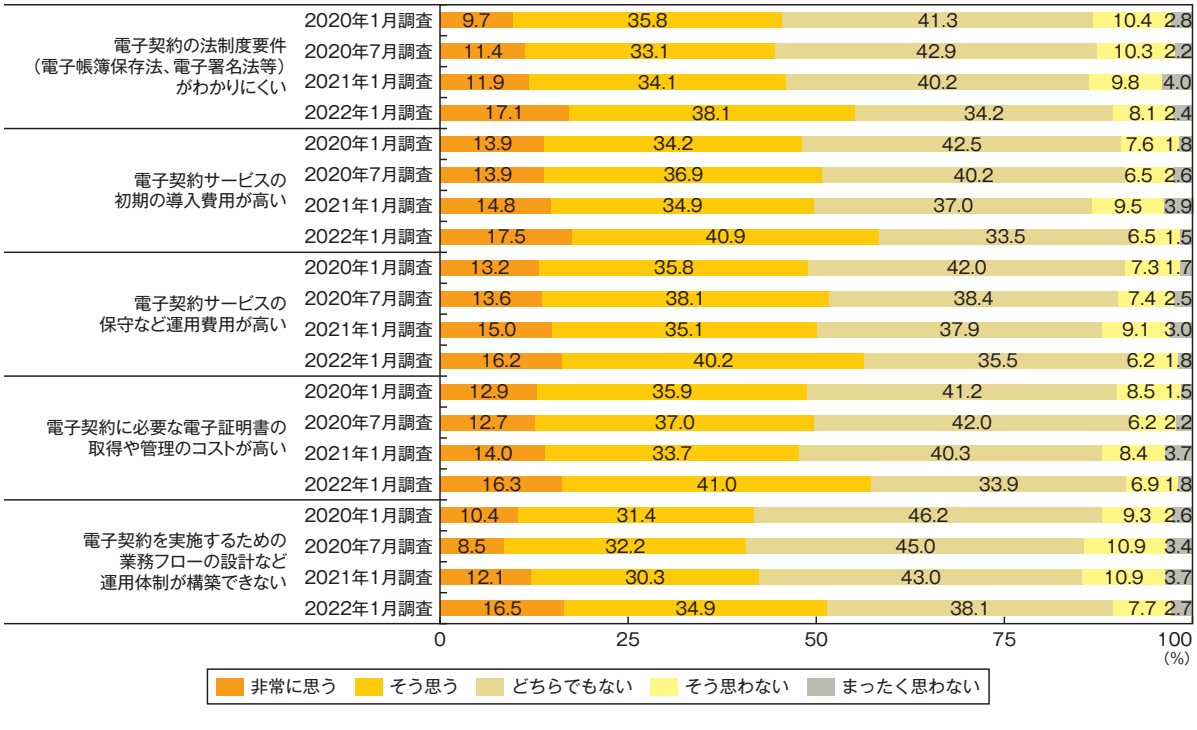
図32. 電子契約を導入する際に重視するポイント

7-5. 電子契約の利用拡大に向けての課題

電子契約の利用拡大のための課題では、「導入メリットを説明することが難しい」（23.2%）と「手間がかかる」（20.0%）について、２割が「非常に思う」と回答しているが、全体的には分散しており、突出した課題は見られない。（図33）

過去３年との比較では、「導入メリットを説明することが難しい」「法制度要件がわかりにくい」「導入費用が高い」「運用体制が構築できない」が特に増加傾向にある。





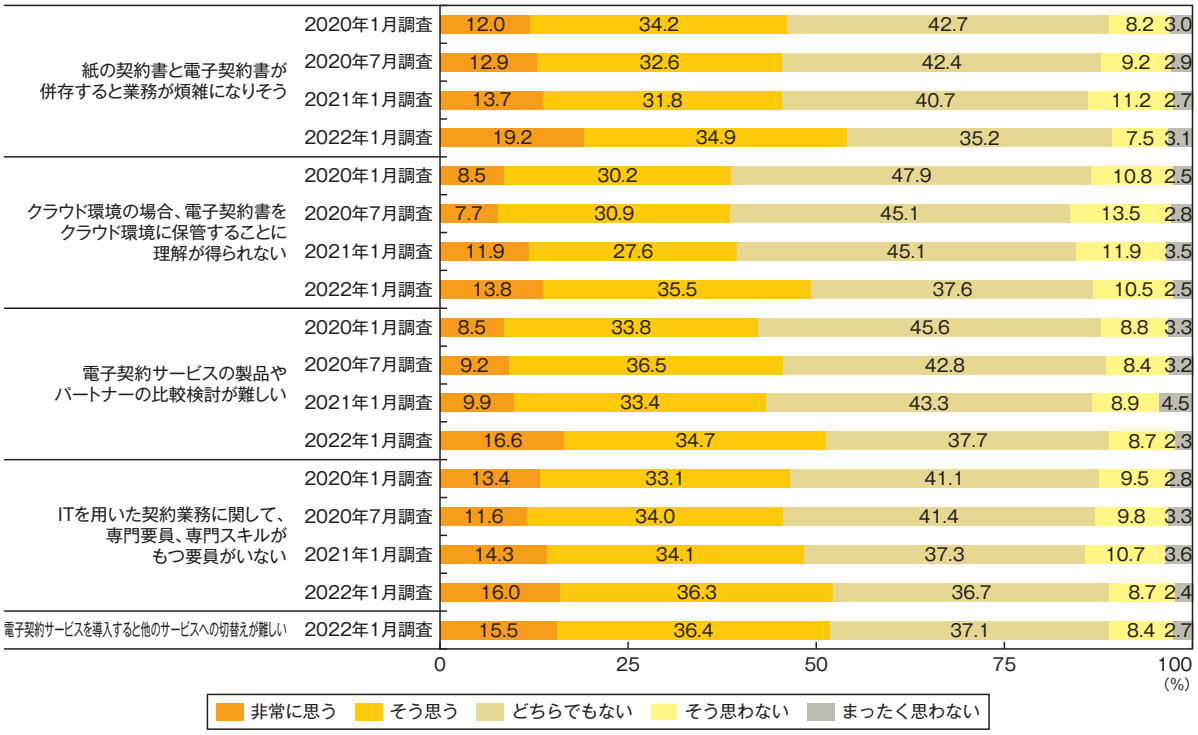


図33. 電子契約の利用拡大に向けての課題（2020-2022年比較）

【コラム】電子契約の動向について

電子契約の利用状況について、本調査結果から、取引文書に関する電子契約の導入企業が約７割となり、多くの企業が何らかの形で電子契約を利用していることがわかります。

電子契約のタイプ別の利用状況については、①当事者型電子契約※1の採用が 26.0%、②立会人型電子契約※2の採用が 18.4%、③電子署名を利用しない電子契約※3の採用が 10.4%、④当事者型と立会人型のハイブリットな電子契約の採用が 10.0% となっています。

※1 契約当事者自身で電子署名に使われる電子証明書を持ち、それを用いて契約書に電子署名を行う電子契約のこと
※2 電子契約サービス事業者の電子証明書で、契約書に電子署名を行う電子契約のこと
※3 電子署名やタイムスタンプを利用せず、単に電子契約サービス上で契約書を交換したり、電子メールで交換したりする電子契約のこと

調査結果から、電子契約を導入している企業のうち、電子署名の技術を利用した電子契約（上記①②④）を採用している企業が８割以上となり、信頼性の高い電子契約サービスを選択し、導入していることが伺えます。

また、電子契約を導入する際に重視するポイントとして、「サービスのコスト」が 46.9% で一番ですが、その次に、「サービス事業者がセキュリティに関する認証・認定を取得しているか」が 35.0% で二番目に付けていることから、やはり電子契約サービスに対する信頼性について重視していることが読み取れます。

最近では、電子契約市場へ参入するサービス提供事業者も増えており、多種多様な電子契約サービスが展開されている状況です。また民間企業だけでなく自治体でも電子契約導入が進んでいることから、さらに電子契約の普及が進むものと思います。

JIPDEC は、信頼性の高い電子契約等トラストサービスの普及を目指しています。「JIPDEC トラステッド・サービス登録※4」は電子契約サービスや、電子証明書を発行する認証局の第三者評価も行っておりますので、ご興味がありましたらお問い合わせいただければ幸いです。

※4 JIPDEC トラステッド・サービス登録　https://www.jipdec.or.jp/project/jtsr.html

JIPDEC　デジタルトラスト評価センター　主査　佐藤 桂史郎

7-6. デジタルトランスフォーメーション（DX）の推進状況

DXの推進状況については、「取組みは開始しているが効果は不明」（40.2%）が最も多く、「効果がでている」（18.1%）、「着手準備中」（16.4%）と続いている。（図34）

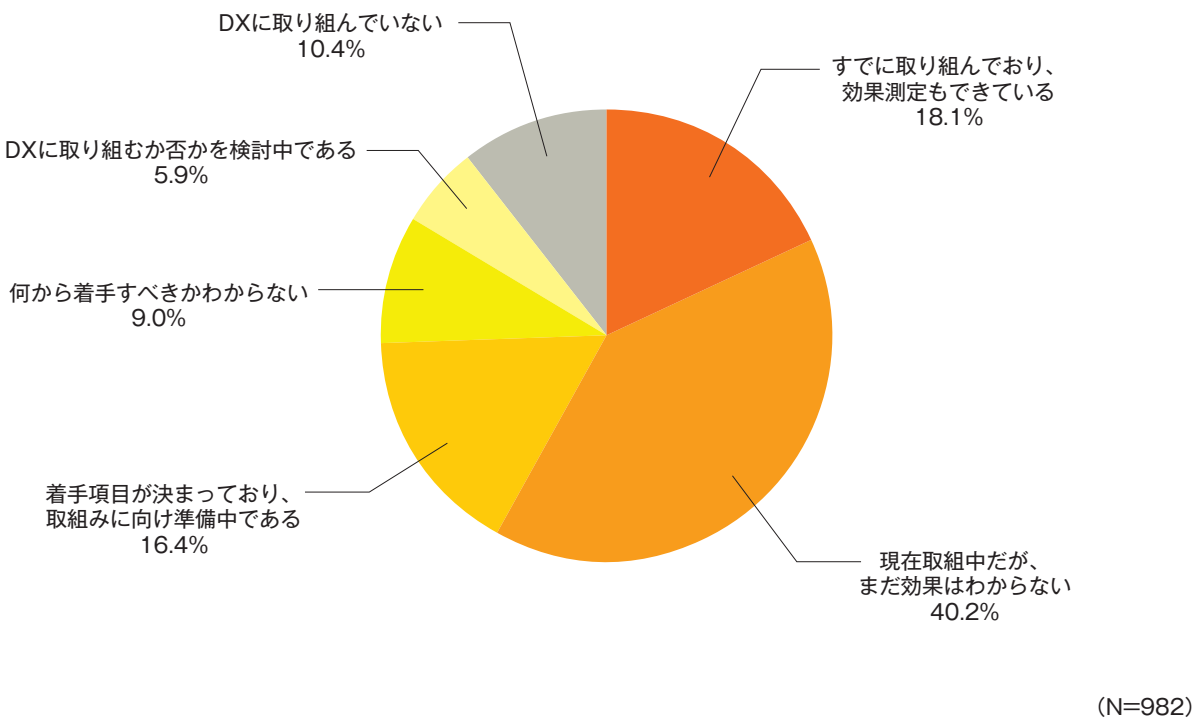


図34. DXの推進状況

7-7. DXを推進するにあたっての課題

DXを推進しようとしている企業の課題では、「規程の整備が難しい」（42.0%）、「体制構築が難しい」（40.7%）、「業務の洗い出しが難しい」（40.7%）が４割を超えており、主な推進課題と言える。（図35）

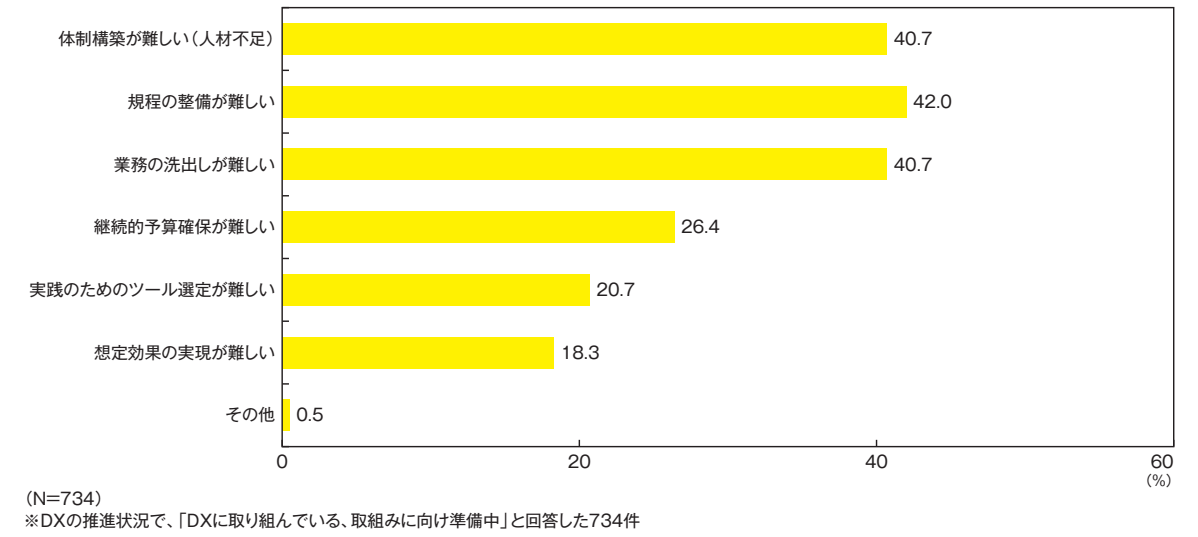
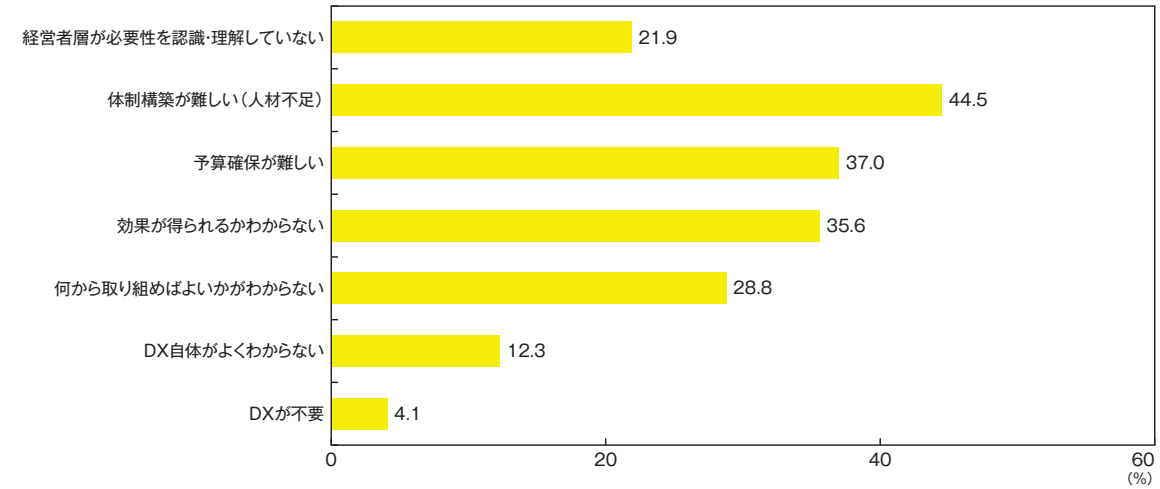


図35. DXの推進課題

7-8. DXへの取組みについての課題

DXの推進にあたり、「何に着手すればよいかがわからない」、または「取り組むか否かを検討中」の企業では、「体制構築が難しい（人材不足）」（44.5%）、「予算確保が難しい」（37.0%）、「効果が得られるかわからない」（35.6%）が３割を超えており、主な課題と言える。（図36）



(N=146)
※DXの推進状況で「何から着手すべきかわからない」「DXに取り組むか否かを検討中である」と回答した146件

図36. DXの取組み課題

8 総評

コロナ禍も３年目を迎え、企業はテレワークとクラウド利用を中心とした新たなデジタルワークスタイルを確立しつつあり、システム面・セキュリティ面の対応のみならず、新たな環境下における新事業の創出が課題となってきている。

情報セキュリティインシデントは「マルウェア感染」と「従業員によるデータ・情報の紛失・盗難」が依然多く、外部からの攻撃と内部からの情報漏えいと両方のリスクを抱えている。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ような境界防御型のツールから、クラウド環境に適したゼロトラスト型に対応したCASBやEDRのような次世代型のセキュリティサービスへ移りつつある。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していくことが予測される。

個人情報保護関連では、国内は2022年４月より改正個人情報保護法が施行され、海外ではEU GDPRの影響を受けて各国でプライバシー法制が施行されてきている。それを受けて企業ではプライバシーテックの導入が進みつつある。

新たなデジタルワークスタイルでは、電子契約の利用が普通となり、電子インボイスへの対応も進むと思われる。DXについて取り組む企業も増えており、新たな環境下で成果を出していくことが期待される。

回答者プロフィール

業種	回答数	%
製造	301	30.7
建設・不動産	97	9.9
卸売・小売	86	8.8
金融・保険	82	8.4
情報通信	147	15.0
サービス	215	21.9
公共・その他	54	5.5
全体	982	100.0

従業員規模	回答数	%
5,000人以上	215	21.9
1,000～4,999人	239	24.3
300～999人	199	20.3
50～299人	215	21.9
50人未満	114	11.6
全体	982	100.0

資本金規模	回答数	%
5,000億円以上	181	18.4
3,000億～5,000億円未満	46	4.7
1,000億～3,000億円未満	83	8.5
500億～1,000億円未満	80	8.1
100億～500億円未満	178	18.1
10億～100億円未満	235	23.9
1億～10億円未満	134	13.6
1,000万円～1億円未満	32	3.3
1,000万円未満	13	1.3
全体	982	100.0

業種別内訳		回答数	%
製造	食品・飲料	37	3.8
	日用品・生活雑貨	21	2.1
	繊維	17	1.7
	パルプ・紙・印刷	14	1.4
	化学工業	21	2.1
	石油製品	4	0.4
	鉄鋼・金属	17	1.7
	プラスチック・ゴム	6	0.6
	機械	28	2.9
	電気機器	30	3.1
	情報通信機器	14	1.4
	電子部品・電子回路	14	1.4
	精密機器	18	1.8
	自動車・輸送機器	28	2.9
	医薬品	18	1.8
	その他の製造業	14	1.4
建設・不動産	建設	58	5.9
	不動産	38	3.9
	住宅	1	0.1
卸売・商社	卸売	27	2.7
	小売	32	3.3
	商社	27	2.7
金融・保険	銀行	45	4.6
	証券	9	0.9
	生命保険	8	0.8
	損害保険	12	1.2
	その他金融	8	0.8

業種別内訳		回答数	%
情報通信	通信	26	2.6
	ITベンダ／システムインテグレータ	85	8.7
	インターネット・サービス	23	2.3
	情報システム子会社	13	1.3
サービス	電力・ガス・水道	16	1.6
	運輸	38	3.9
	倉庫	3	0.3
	宿泊	4	0.4
	飲食	9	0.9
	娯楽・レジャー	9	0.9
	メディア・出版・放送・広告	6	0.6
	生活関連サービス（旅行業など）	8	0.8
	医療	38	3.9
	福祉・介護	25	2.5
	教育（学校以外）	15	1.5
	人材派遣・業務委託	12	1.2
	その他サービス	32	3.3
公共・その他	学校	11	1.1
	官公庁	13	1.3
	地方自治体	17	1.7
	農業・水産・鉱業	5	0.5
	その他の業種	3	0.3
	その他公共機関	5	0.5
	全体	982	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	350	35.6
全社的なリスク管理／コンプライアンス／セキュリティ管理に責任をもっている	471	48.0
セキュリティ製品の導入、製品選定に関与している	502	51.1
セキュリティ対策の実務に関与している	317	32.3
全体	982	100.0

〈資料〉情報化に関する動向（2021年10月～2022年３月）

国　内	海　外
2021年10月	
・NTTドコモ、スマホ利用者へのフィッシング詐欺による不正なギフトカード購入などで１億円の被害。 ・東京五輪・パラリンピック、大会期間中に組織委員会システム、公式サイトが受けたサイバー攻撃4.5億回、大会への影響なし。 ・公正取引委員会、スマホ向けOS市場実態調査実施を発表。Apple、Googleの市場寡占状況把握へ。 ・NTTドコモ、IoT位置情報サーバ切替え時の不具合で大規模通信障害発生。全面復旧回復までの２日間で、約200万人に影響。その後の調査で、音声利用者460万人、データ利用者830万人に影響。 ・Zホールディングス、LINE社のデータガバナンス他を検証・評価する、特別委員会最終報告書公表。中国関連会社での個人情報閲覧、韓国サーバ保管は経済安全保障上配慮できず。 ・マイナ保険証、本格運用開始。利用可能な医療機関は全体の１割未満。 ・東芝、世界初、量子暗号機器の小型化に成功。 ・三菱電機、サイバー攻撃被害により、子会社の保有する複数顧客情報の一部流出。	・Facebook、約６時間にわたるシステム障害発生。世界中でインスタグラム他サービス使用できず。原因はネットワーク通信調整のためのバックボーンルーターの設定ミス。 ・欧州議会、法執行機関によるAIを用いた顔認識技術、犯罪を予見する技術を禁止。AIアルゴリズムの偏りによる差別助長をけん制。 ・アイルランド政府、OECDの法人税に関する包括的枠組みに参加。プラットフォーマーの租税回避に対応。 ・Microsoft調査、2020年７月から21年６月に起きたサイバー攻撃の58％がロシア国家支援によるものと報告。 ・韓国、「データ産業振興および利用促進に関する基本法」制定。データ産業の競争力確保を目指し、生産、取引、活用促進のための必要事項を規定。2022年４月施行予定。 ・米商務省、ハッキングツールの輸出、再輸出、国内移転抑制のための輸出規制導入発表。 ・豪政府、オンラインプライバシー法案発表。16歳未満のSNS利用に保護者同意義務付け。 ・Facebook、「Meta」に社名変更。メタバースを創造する企業ビジョンをアピール。 ・中国政府、「データ海外越境安全評価弁法」草案発表。個人情報持出しに審査義務付け。

国　内	海　外
2021年11月	
・my FinTech株式会社、秘密鍵と電子証明書を搭載する「my電子証明書」サービスが電子署名法に基づく特定認証業務の認定取得。 ・LegalForce調査、DXが進んでいるのは２割程度。課題は推進者不在、予算不足で６割。 ・金融庁、2021年２月～９月に８度にわたるシステム障害を起こしたみずほ銀行、みずほFGに業務改善命令。再発防止策、業務改善計画策定と経営責任の明確化を要求。 ・東大・九州大学・NTT他、量子コンピュータでも解読困難なデジタル署名技術「QR-UOV 署名」開発。	・中国、個人情報の収集、使用、保管に関する基本原則を定めた個人情報保護法施行。中国拠点企業のデータ処理要件規定。違反時には高額な制裁金。 ・Facebook、利用者間のプライバシー侵害への懸念を受け、顔認識技術の利用中止へ。 ・米Yahoo、中国でのサービス提供撤退。中国個人情報保護法施行による規制強化で事業継続困難と判断。 ・豪情報コミッショナー事務所、顔認識アプリClearview AIをプライバシー法違反と判断。 ・Google、韓国「反Google法」9月成立を受け、韓国公式アプリストアで代替アプリ内課金システム容認へ。 ・欧州裁判所、Googleへの競争法を巡る24億ユーロ超の制裁金命令に対し、EUを支持、Google敗訴。 ・欧州委員会（EC）、未成年者に対する行動ターゲティング禁止、意図的にユーザーをだますダークパターンを禁止する「デジタル市場法（DSA）」承認。 ・Deloitte Global調査、年間売上高５億ドル以上の企業で、７割が2020年にインシデント、侵害経験。 ・UNESCO、AI倫理の国際規範策定。プライバシー保護や透明性確保など守るべき10原則を規定し、加盟国に勧告。国際合意は世界初。

国　内	海　外
2021年12月	
・NEC、顔情報を暗号化したまま認証できる「秘匿生体認証技術」開発。悪用リスク軽減を目指す。 ・個人情報保護委員会、顔認識データ利用規制に関する有識者会議設置。データ利用目的の公表義務に加え、データ保存期間の明示などを検討。 ・トレンドマイクロ調査、全世界でビジネスメール詐欺被害増加。2021年７～９月の検出件数５万件。19年同時期の約3.5倍に。	・米Cisco調査、マルウェア感染、フィッシング攻撃を受けた中小企業、回答の５割が50万ドル超の被害。 ・中国政府、2008年独占禁止法改正に着手。合併・買収などの企業結合審査の届け出義務違反による制裁金引上げ。 ・イタリア競争局、Amazonの市場における優越的地位乱用に対し11.3億ユーロの罰金。 ・米・豪政府、重大犯罪時に法執行機関が国境を越えてデータを共有できる「海外データ合法的使用明確化法（CLOUD法）」協定締結。

国　内	海　外
2022年１月	
・フィッシング対策協議会調査、2021年12月のフィッシング報告件数が11月の1.3倍。Amazonを騙るフィッシングが最多。 ・東芝他、金融取引における量子暗号通信利用の実証実験成功。 ・最高裁、不正指令電磁的記録保管罪を問われた「Coinhive」の無断設置事件、東京高裁の有罪判決を棄却し無罪判決。	・仏データ保護機関（CNIL）、Cookie拒否が容易にできないとして、Googleに1.5億ユーロ、Facebookに6,000万ユーロの制裁金。３カ月の猶予設定。未対応なら１日あたり10万ユーロのペナルティ。 ・北朝鮮ハッカー、2020-2021年のサイバー攻撃で暗号資産４億ドルを盗取。 ・ロシア政府、米企業にランサム攻撃をした自国のハッカー集団メンバー14人を拘束・起訴。資産4.2億ルーブル差押さえ。 ・中国、「サイバーセキュリティ審査弁法」改正。100万件超の個人データを処理する中国企業を海外上場審査対象に。２月15日施行。 ・欧州議会、11月にECが承認した「デジタルサービス法（DSA）」承認。違法コンテンツや製品の削除をプラットフォーム企業に義務付け。違反企業には年間売上高の最大６％の制裁金。

国　内	海　外
2022年２月	
・ヤフー、2022年４月以降の欧州でのサービス提供中止を公表。同地域でのヤフーサイトの閲覧不可へ。 ・JPCERT/CC調査、マルウェア「Emotet」感染急拡大。2021年１月頃に一時停滞するも、11月頃から活動再開。 ・ソフトバンク、積水ハウス、ワコール他大手企業、Emotet感染被害防止に向け、PPAP廃止の動き。 ・国立極地研究所他、南極昭和基地でローカル5Gシステムの試験運用開始。南極域で世界初の運用。	・米上院司法委員会、Apple、Googleによるアプリ開発会社に対する自社決済システムの強制使用を禁じる「開かれたアプリ市場法案」可決。 ・国連安全保障理事会北朝鮮制裁委員会発表、北朝鮮による暗号資産交換事業者へのサイバー攻撃で5,000万ドルの被害。 ・米国土安全保障省、国内セキュリティ事件の検証機関「Cyber Safety Review Board（CSRB)」新設。Log4jの脆弱性検証実施へ。 ・米国税庁、納税者のプライバシーとセキュリティを重要視し、利用契約料２年間で8,600万ドルのサードパーティ顔認証システムの使用取りやめ。 ・EC、EU独自の衛星通信網構築計画策定のための規則案公表。2028年までに全サービス提供へ。 ・CNIL、Googleアナリティクスの解析データを米国に送信するのはGDPRおよび仏国内法違反と声明。GDPR準拠または使用中止を要求。 ・英歳入関税庁、脱税事件捜査で、ブロックチェーン上で発行された代替不可能なトークンNFTを押収、英国内初。

国　内	海　外
2022年３月	
・トヨタ自動車、取引企業へのサイバー攻撃の影響を受け、国内全工場の製造ラインを１日全停止。翌日再開。 ・政府、インターネット利用者の情報の適正な取扱いを規制する「電気通信事業法改正案」を閣議決定。利用者情報の第三者提供時は本人通知・公表、同意取得、オプトアウトいずれかを義務付け。 ・政府、「道路交通法改正案」閣議決定。マイナンバーカードと運転免許情報一本化へ。 ・防衛省、陸・海・空自衛隊共同の「サイバー防衛隊」発足。 ・個人情報保護委員会調査、ECサイトの不正アクセス被害４割。外部委託先に任せきりの現状明るみに。 ・総務省、「電気通信事業における個人情報保護に関するガイドライン」改正。	・米加州他、子どもへの心理的影響が消費者保護法に違反するか、「TikTok」調査へ。 ・アイルランド人権保護団体ICCL、Googleによる個人情報侵害への対応を怠ったとして同国データ保護委員会（DPC）を提訴。 ・ワシントンDC上級裁判所、Amazonに対する反トラスト法訴訟に対し、ワシントンDCの司法長官の訴えを棄却。 ・欧州連合、EC が 2020 年 12 月に発表した「ゲートキーパー」とみなされた巨大プラットフォームを規制する「デジタル市場法（DMA)」法案に合意。企業買収時の当局への事前通知、自社製品の優遇禁止などを規定。 ・米・EU、個人データの移転ルールで基本合意。2020年７月のプライバシーシールド無効判断後の新ルール。

JIPDEC IT-Report 2022 Spring
2022年5月31日発行（通巻第19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
制　作　株式会社ウィザップ