JIPDECセミナー

クラウド時代のセキュリティ認証・インボイス制度・DXへの取組み～企業IT利活用動向調査2023報告～

2023年3月16日

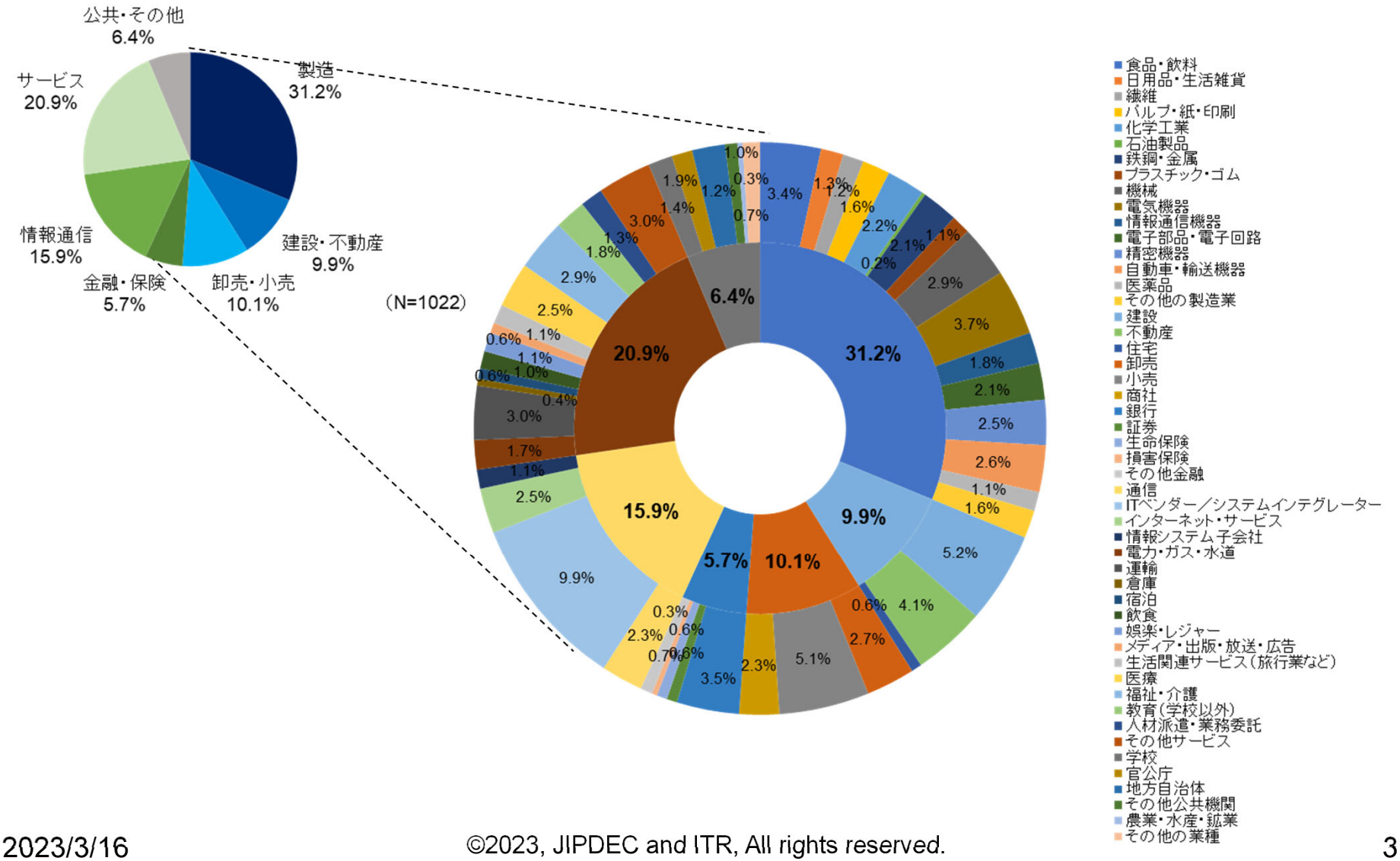
株式会社アイ・ティ・アール

調査概要

実査期間	：	2023年1月19日～1月20日
実施主体	：	一般財団法人日本情報経済社会推進協会 株式会社アイ・ティ・アール
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	：	以下の条件を満たす個人：**約17,000人** • 従業員２名以上の国内企業の勤務者であること • 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ていること • IT戦略策定または情報セキュリティの従事者であること • **係長相当職以上**の役職者であること
有効回答数	：	1,022件（1社1人）

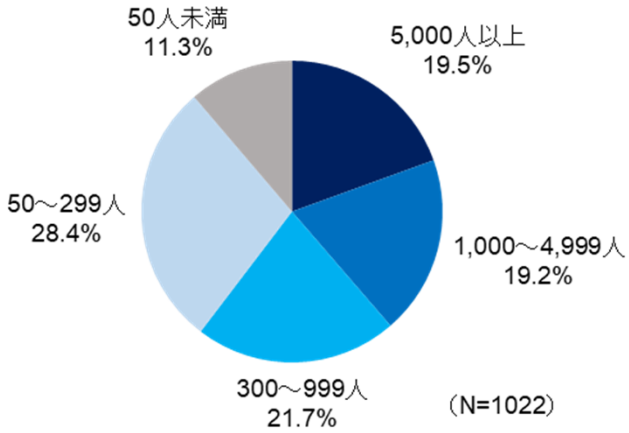
2023年調査：回答者プロフィール①

勤務先の業種

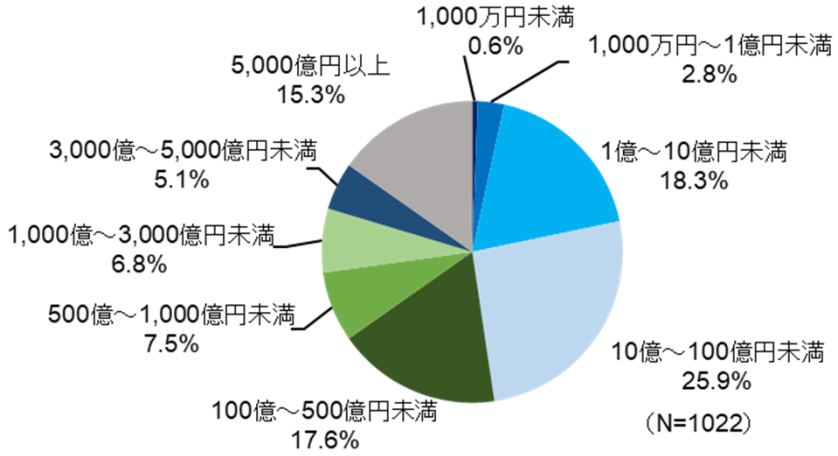


2023年調査：回答者プロフィール②

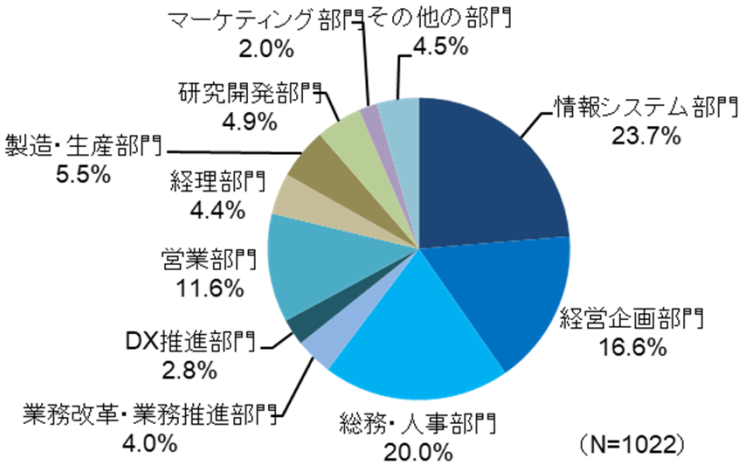
勤務先の従業員規模



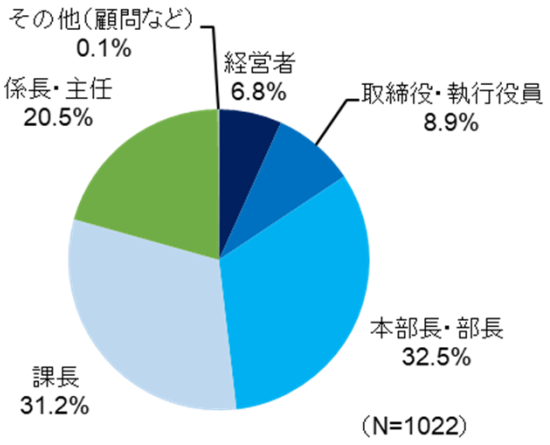
勤務先の売上規模



所属部門

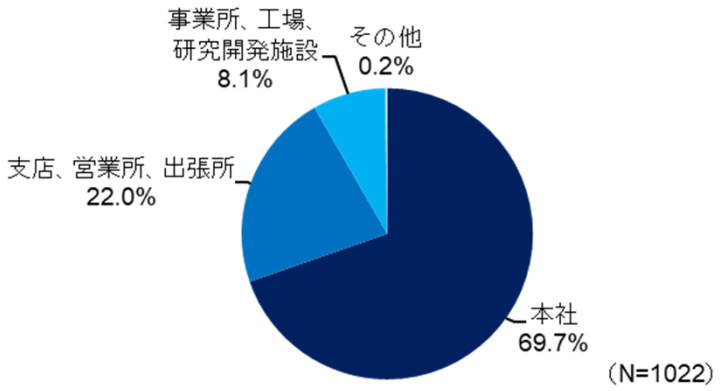


役職

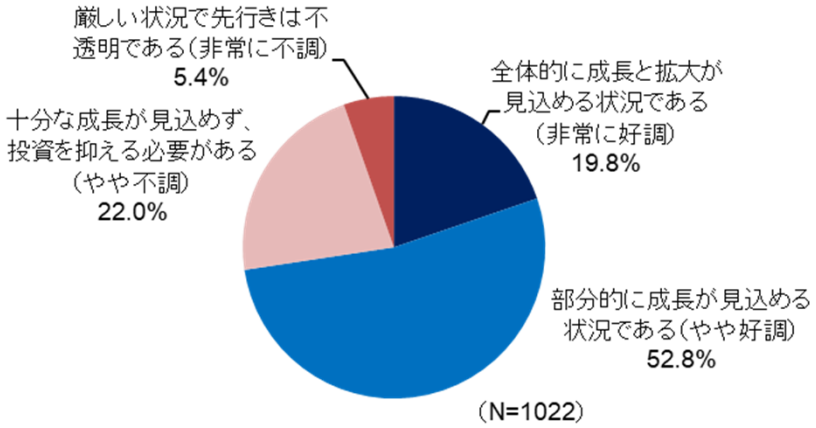


2023年調査：回答者プロフィール③

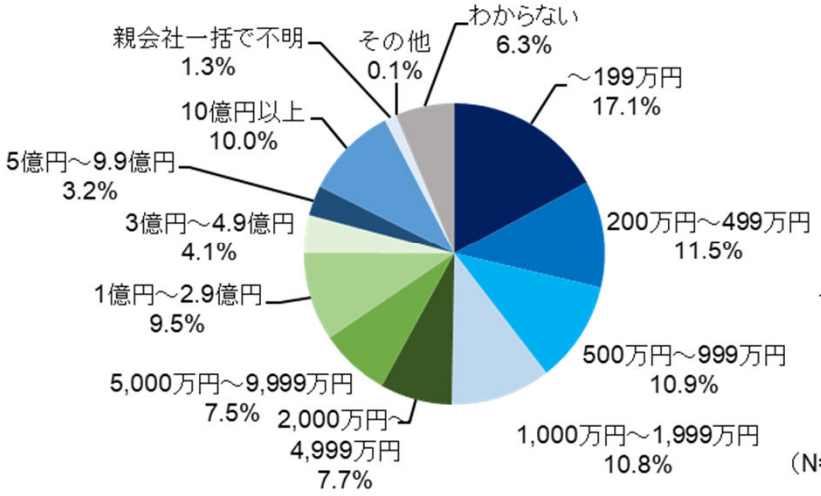
勤務先の組織形態



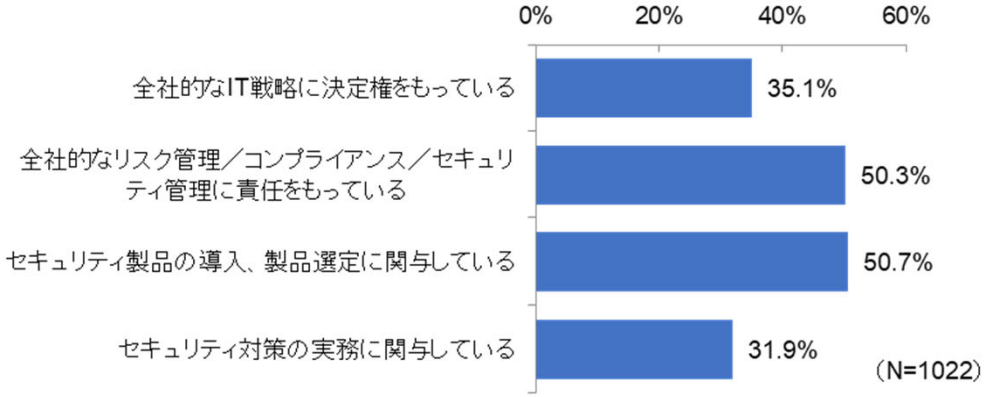
勤務先を取り巻くビジネス環境



年間セキュリティ投資額

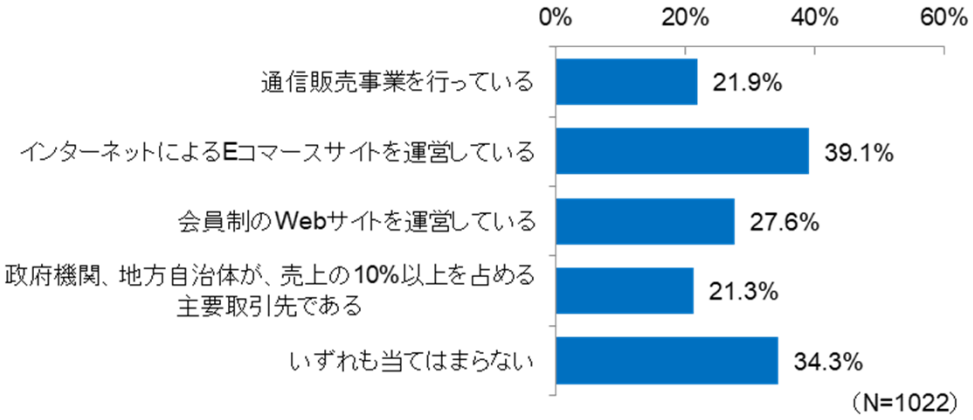


IT戦略/セキュリティへの関与度

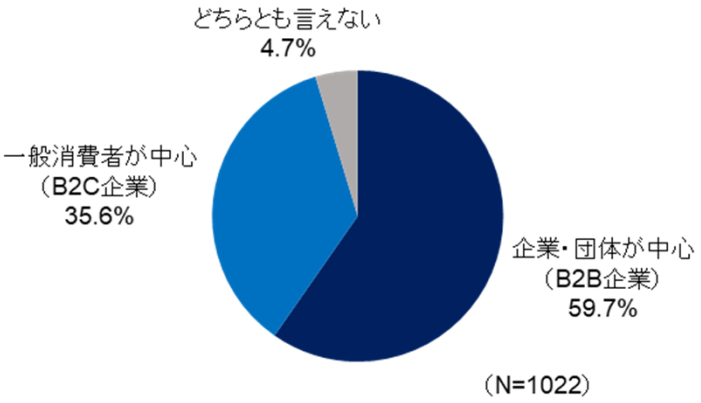


2023年調査：回答者プロフィール④

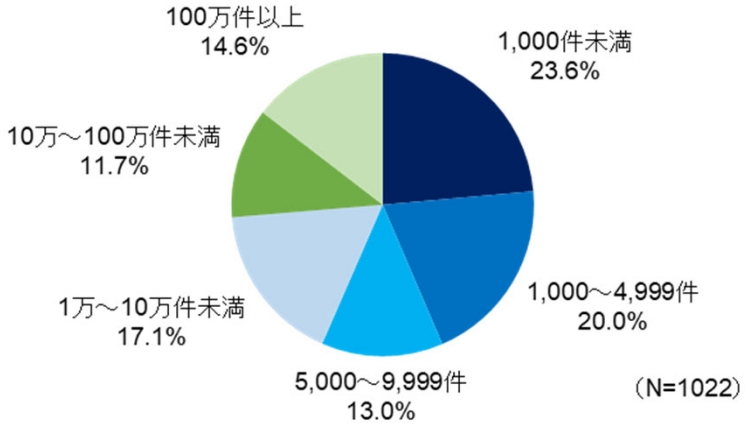
勤務先の事業形態



顧客・取引先のタイプ

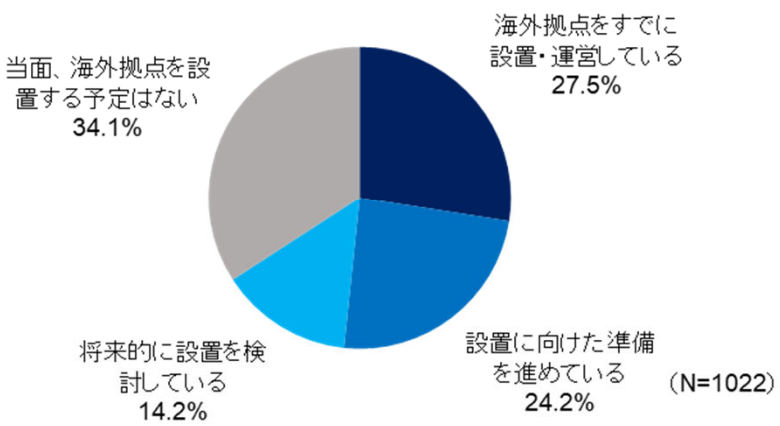


個人情報保有件数

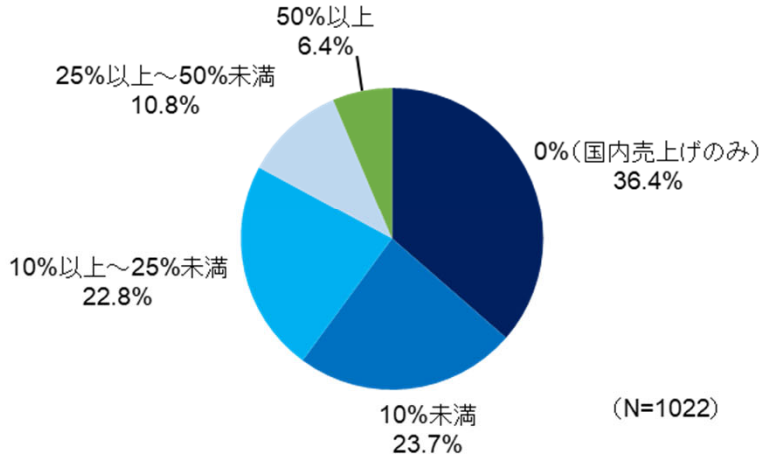


2023年調査：回答者プロフィール⑤

海外拠点の設置状況



海外売上比率



全体の所見

経営課題とセキュリティ

- 新しいワークスタイルに合わせた業務プロセスの見直しや働き方改革が経営課題として認識されており、セキュリティ面では内部不正対策が注目されてきている。

認定／認証制度に対する意識

- サイバーセキュリティの第三者認定／認証取得が少しずつ増加する傾向にあり、効果として、取引先の信頼向上が挙げられている。

個人情報保護・セキュリティ技術動向

- 個人情報保護の取り組みでは個人情報保護教育の実施の比率が高くなっている一方、セキュリティ技術動向ではクラウド対応の次世代型サービスへの移行が進みつつある。

新たなワークスタイルとクラウド化動向

- クラウドサービスの利用が少しずつ増加してきており、それに伴い、端末管理やクラウド上の情報管理が新たなワークスタイルのセキュリティ対策として重視されてきている。

電子帳簿保存法・電子契約・DX推進

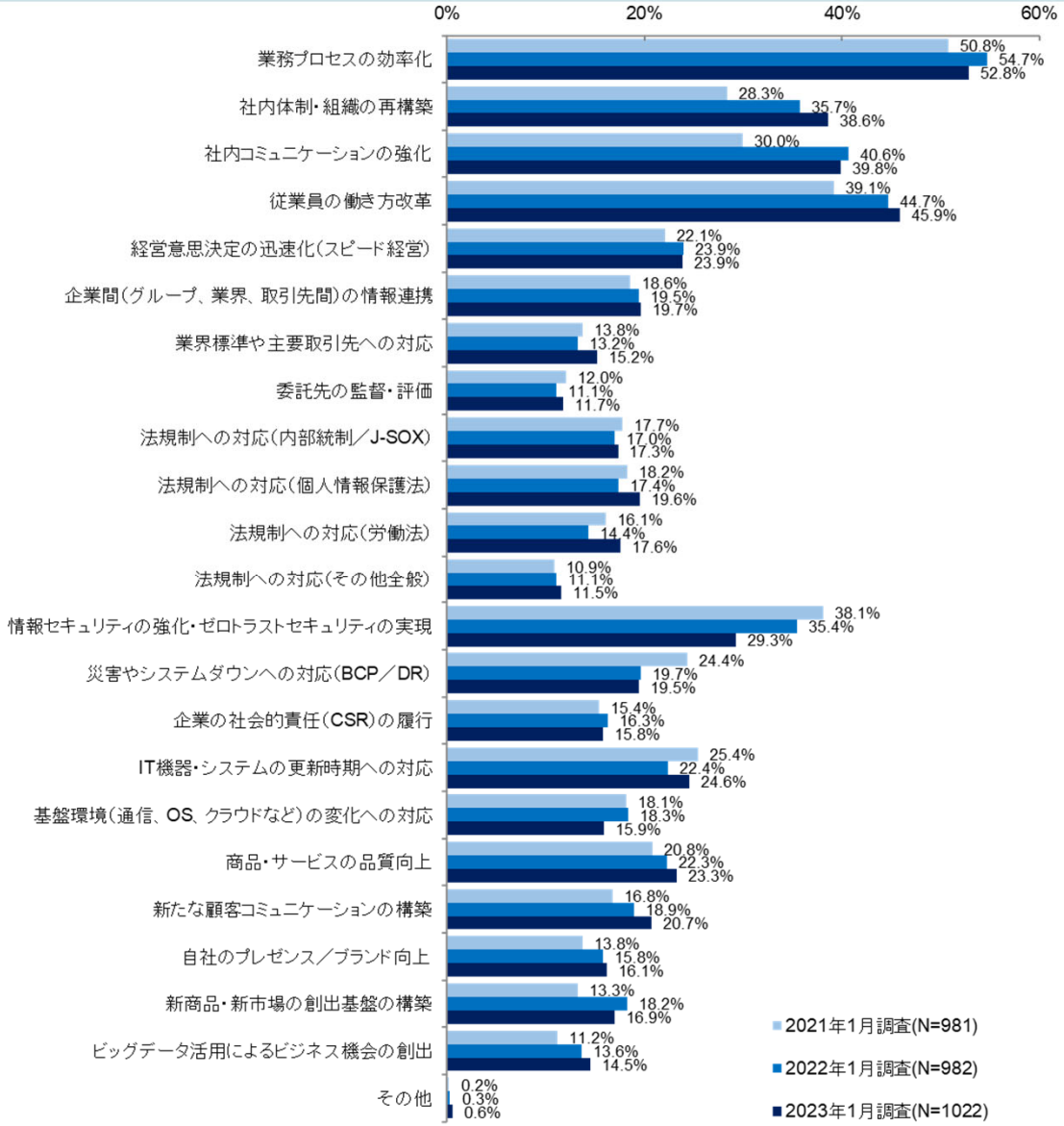
- 電子帳簿保存法の改訂とインボイス制度への対応が進んでおり、電子契約事業者選定ではクラウドセキュリティに関する認証取得が重要視されている。

1）経営課題におけるセキュリティの位置づけ

- Q1： 重視する経営課題
- Q2： セキュリティ・インシデントの認知状況
- Q3： セキュリティ・リスクの重視度合い

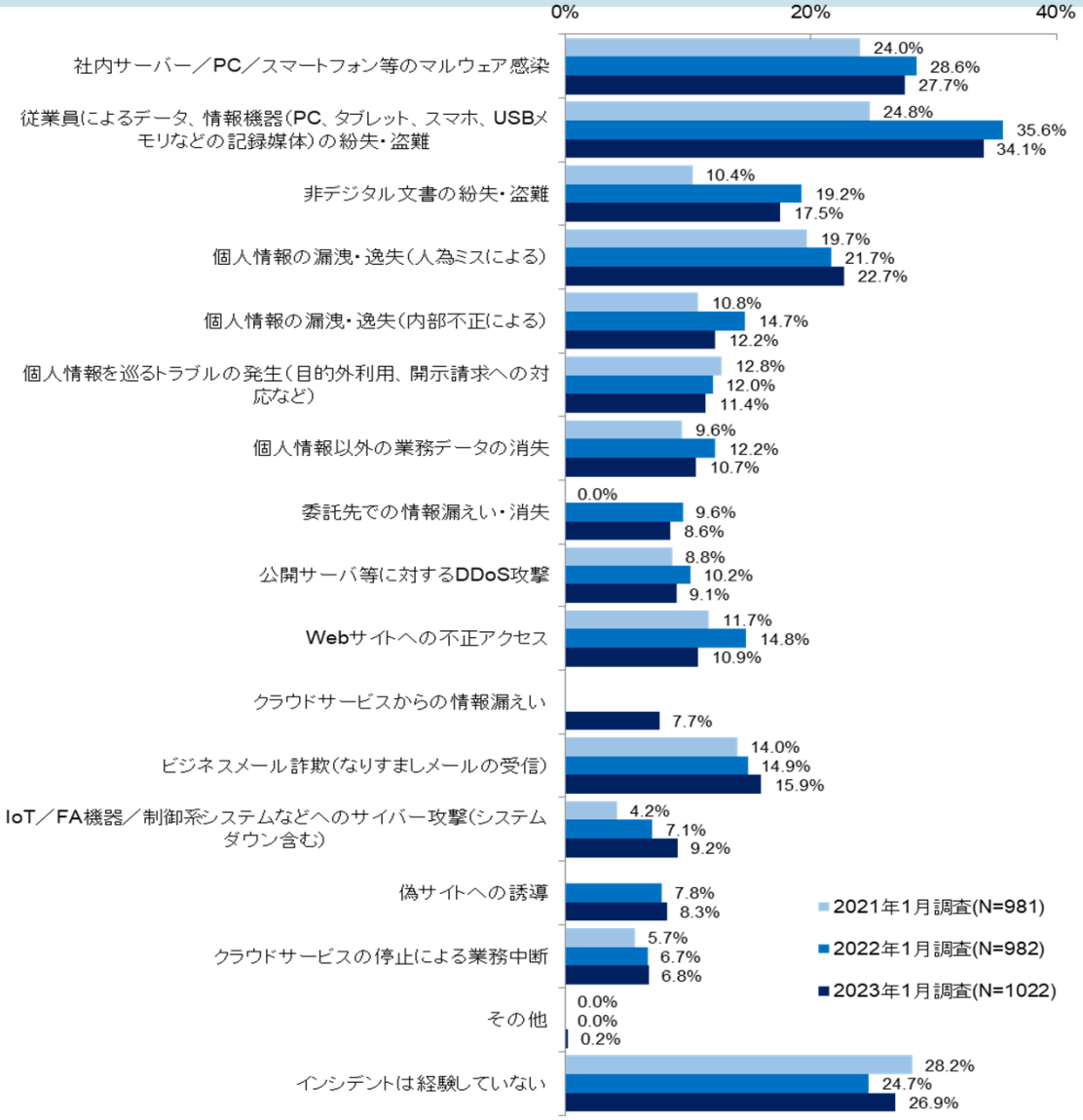
Q1：重視する経営課題（過去２回との比較）

■ 重視する経営課題としては「業務プロセスの効率化」、「従業員の働き方改革」が多く、過去２回との比較でも「従業員の働き方改革」は伸びている。



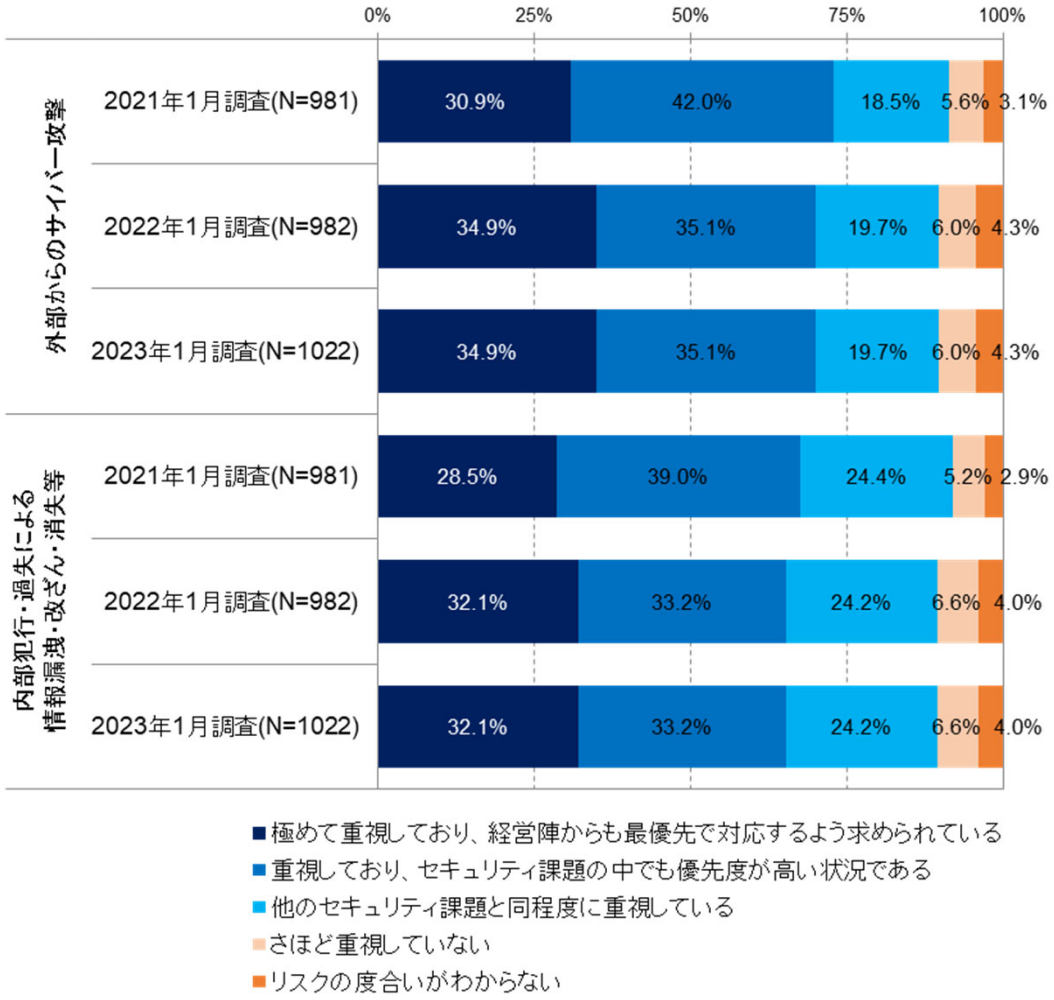
Q2：過去1年間に経験したセキュリティ・インシデント（過去２回との比較）

■ セキュリティ・インシデントとしては「従業員による紛失・盗難」がトップだが、過去２回との比較では「個人情報の漏洩・逸失（人為的）」と「ビジネスメール詐欺」が多くなっている。



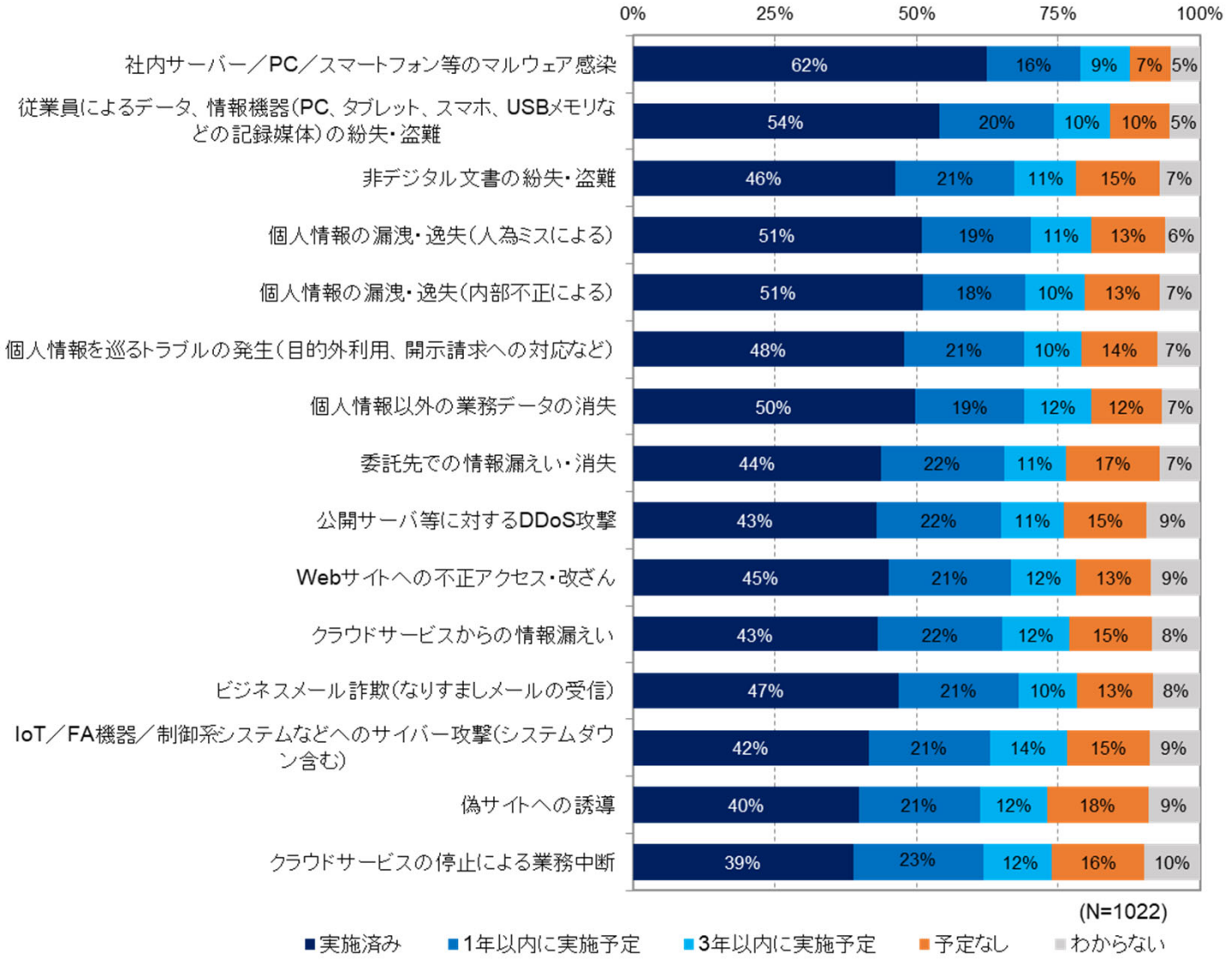
Q3_1：セキュリティ・リスクの重視度合い（過去２回との比較）

- 過去２回と比較して「外部からのサイバー攻撃」「内部犯行による重要情報の漏洩・消失」ともに重視の比率に変化はなく、約７割が重視していると回答している。



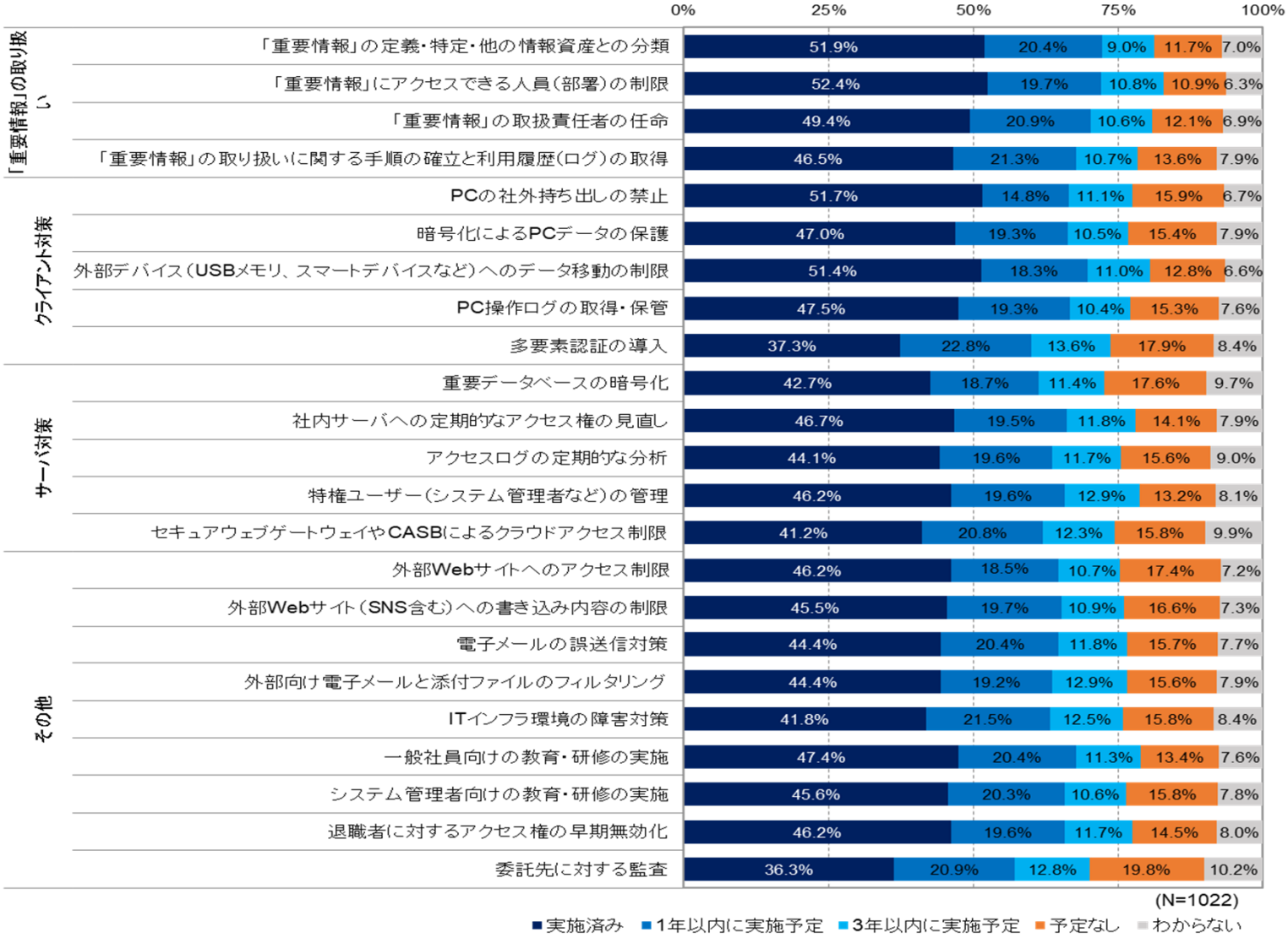
Q3_2：「外部からの攻撃対策」の実施状況（2023年）

■ 実施済の比率が高いのは、「マルウェア感染対策」で、次に「従業員による紛失・盗難対策」で５割を超えている。他の項目もほとんどが４割超である。



Q3_3：「情報漏洩対策」の実施状況（2023年）

■ 情報漏洩対策では、「重要情報へのアクセス制限」、「重要情報の定義」、「PC持ち出し禁止」、「外部デバイスへの移動制限」が５割を超えているが、他の項目も約４割が実施となっており、全般的な対策はされている。

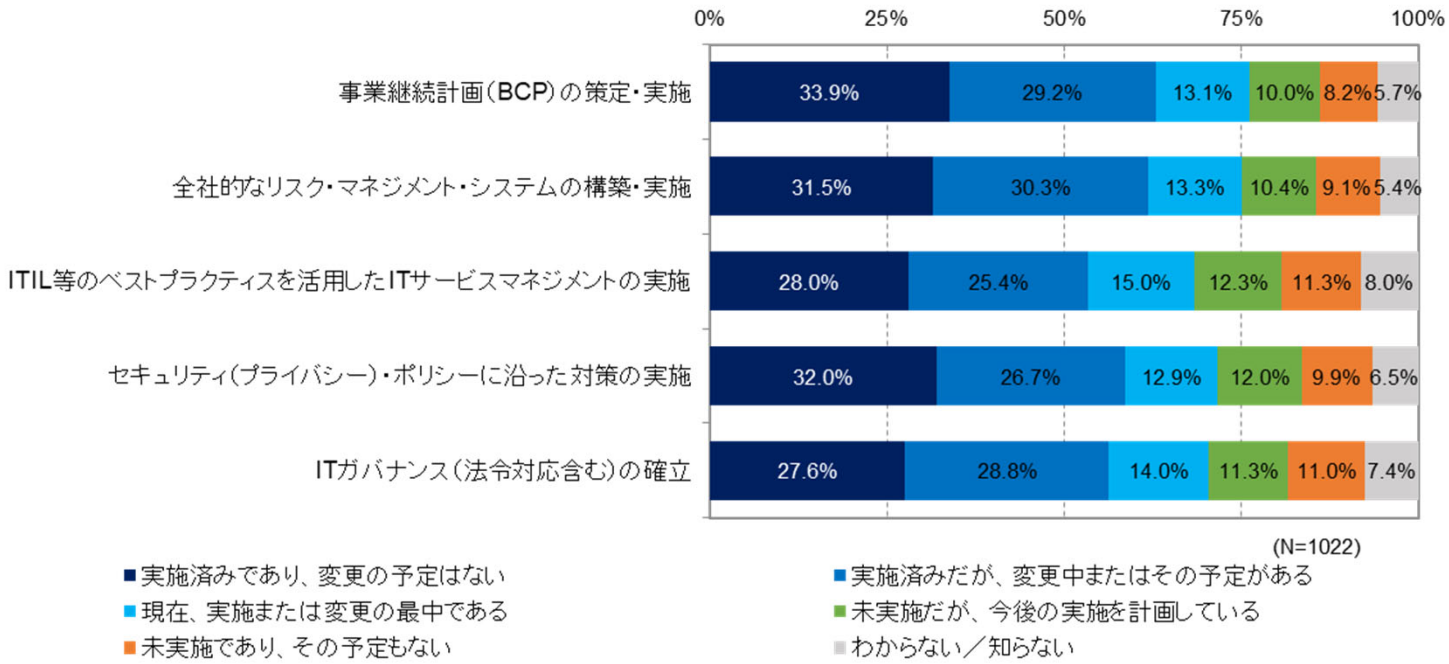


2）認定／認証制度に対する意識

- Q4_1：　システムリスク緩和策の取り組み状況
- Q4_2：　情報セキュリティ認定／認証制度への取り組み状況
- Q4_3：　取引選定時の認定／認証取得の重視度

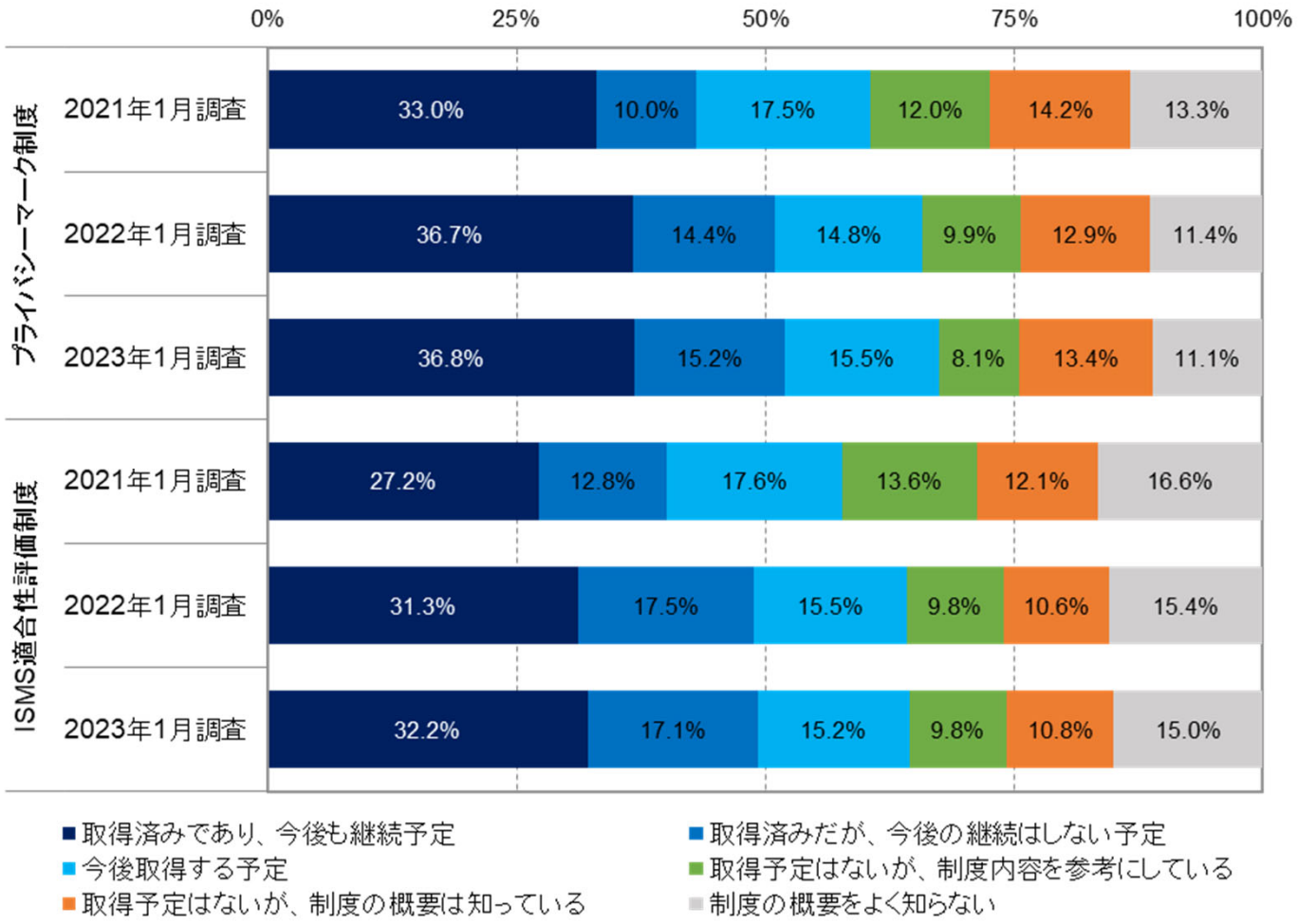
Q4_1：システムリスクの緩和策の取り組み状況（2023年）

■ システムリスクの緩和策では、すべての緩和策が５割以上実施済であり、実施予定を含めると約８割に達する。



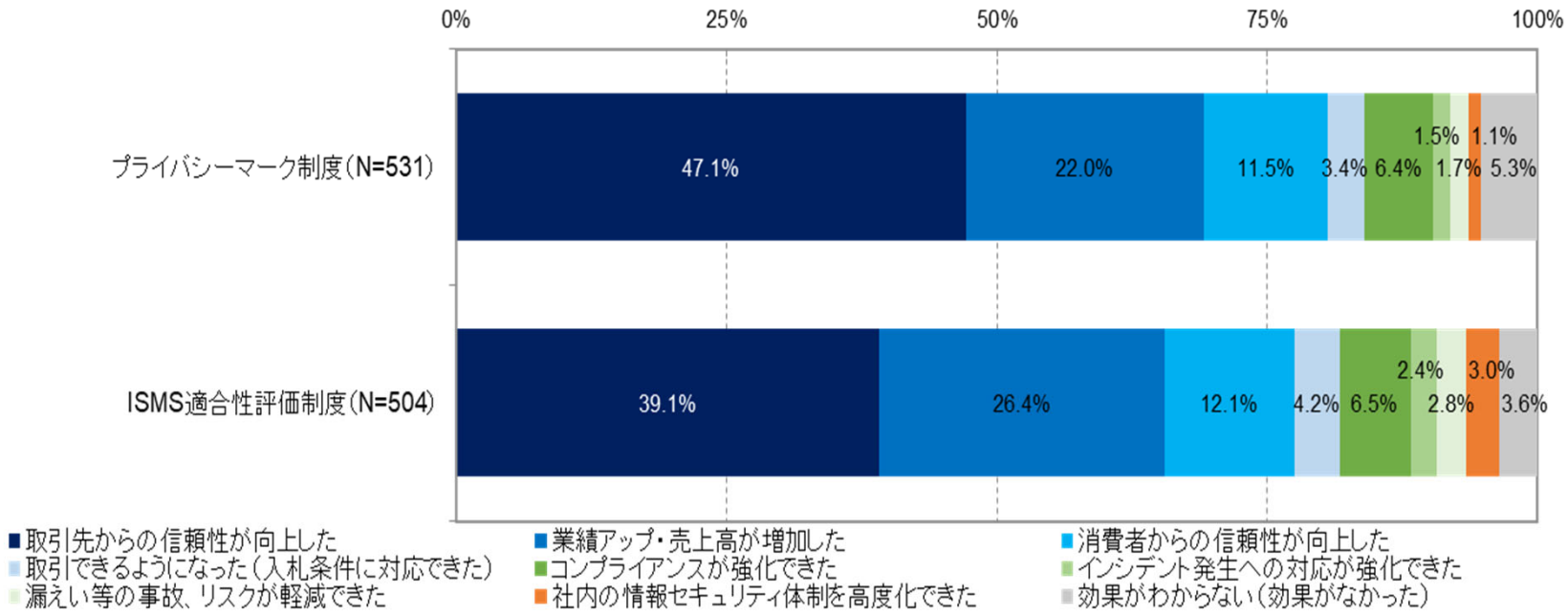
Q4_2：情報セキュリティ認定／認証制度への取り組み状況（過去２回との比較）

■ 過去２回との比較では、いずれも取得済の比率が少しずつ増加しており、「プライバシーマーク制度」と「ISMS適合性評価制度」は共に約５割に達した。



Q4_3：認定／認証取得したことの効果（2023年）

■ 取得したことによる効果は、「取引先からの信頼性向上」がトップで、プライバシーマークで約５割、ISMS認証でも約４割が回答している。続いて「業績アップ」、「消費者からの信頼性向上」が続く。

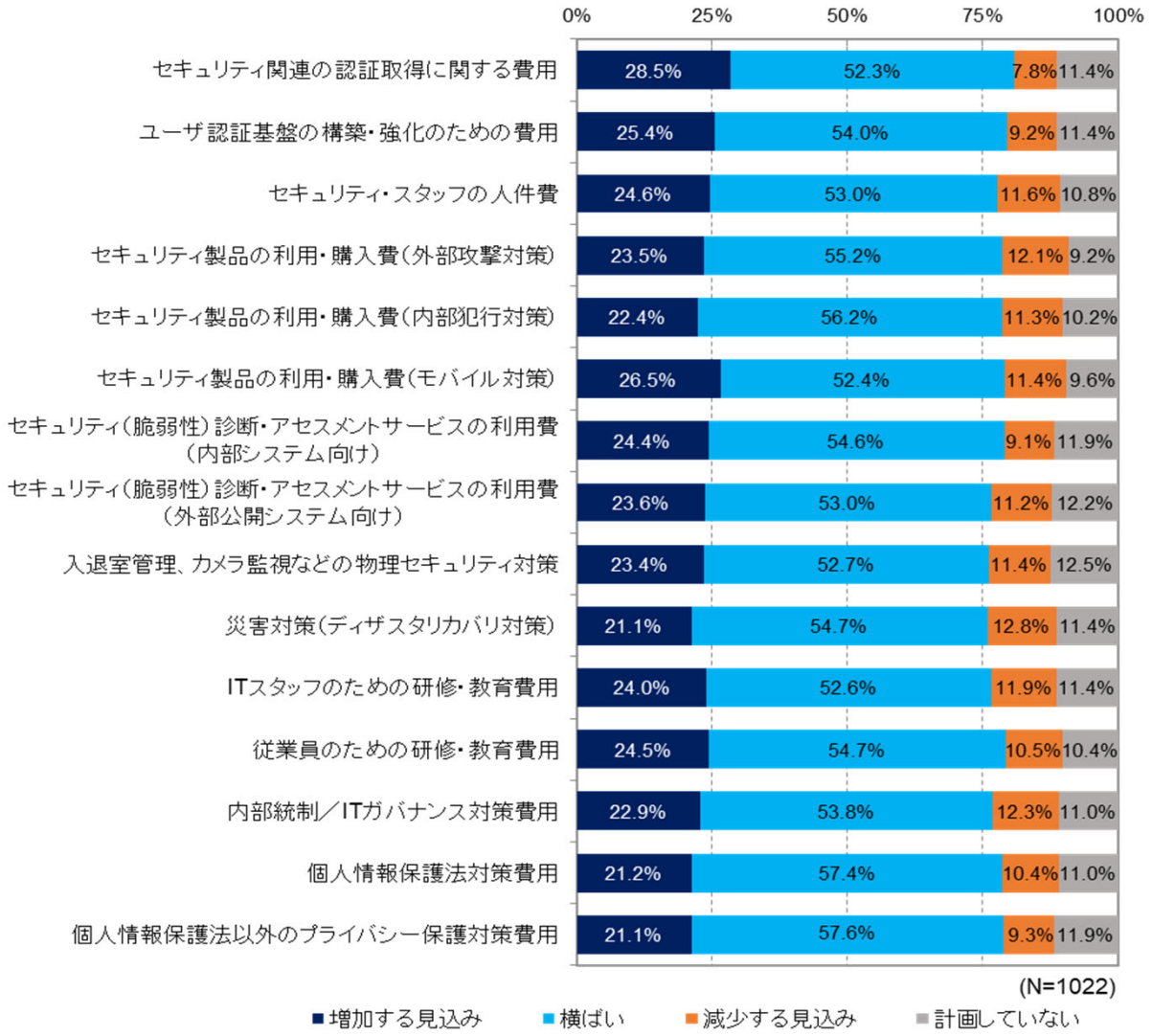


3）セキュリティ支出の動向

- Q５_1：　セキュリティ関連支出実績
- Q５_2：　セキュリティ関連支出の計画

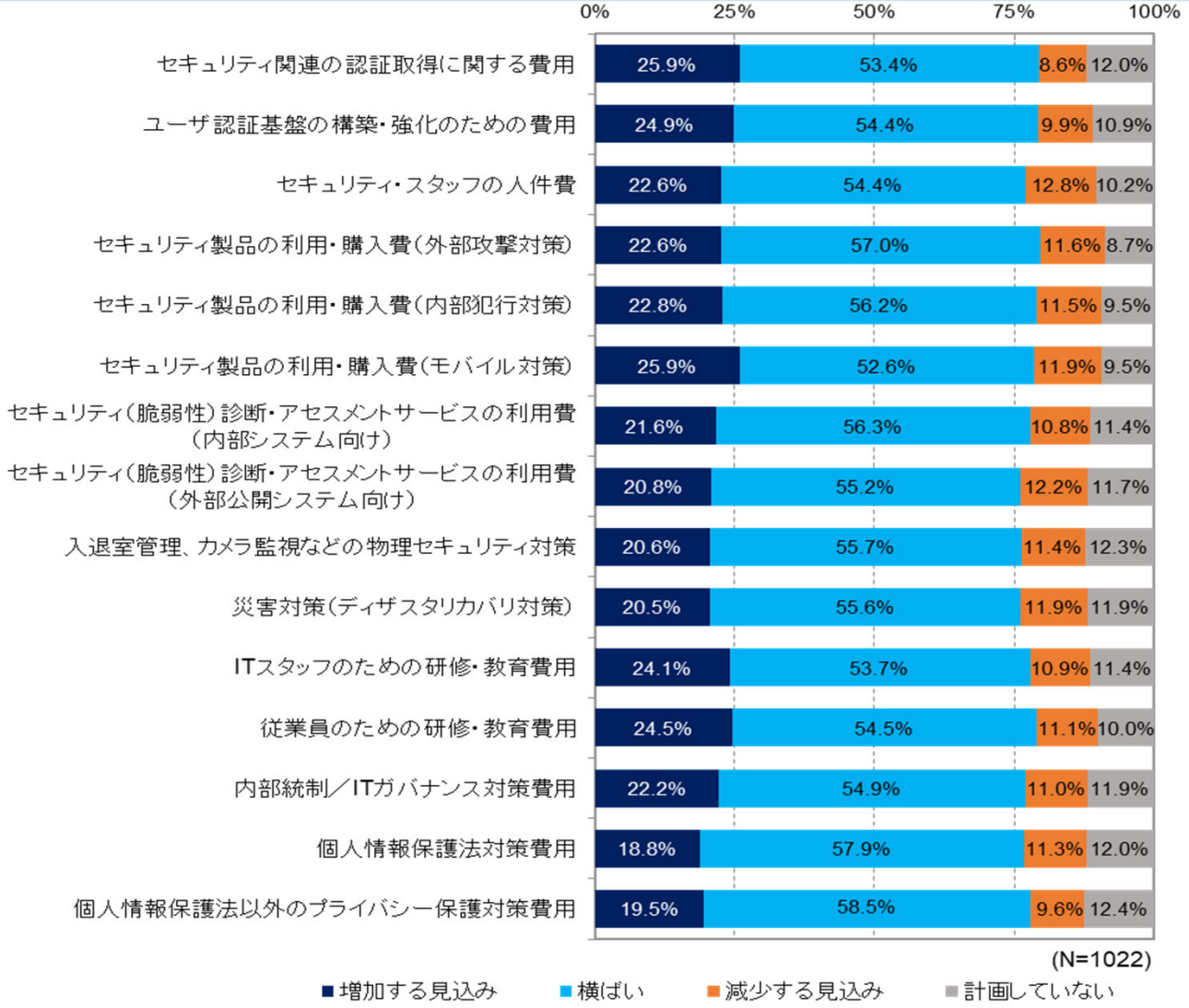
Q５_１ ：セキュリティ関連支出の実績（2023年）

■ 全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。



Q５_２：セキュリティ関連支出の計画（2023年）

- 支出計画についても、横ばいが５割超、増加が２割超となっているが、セキュリティ関連の費用の増加比率が若干高い。

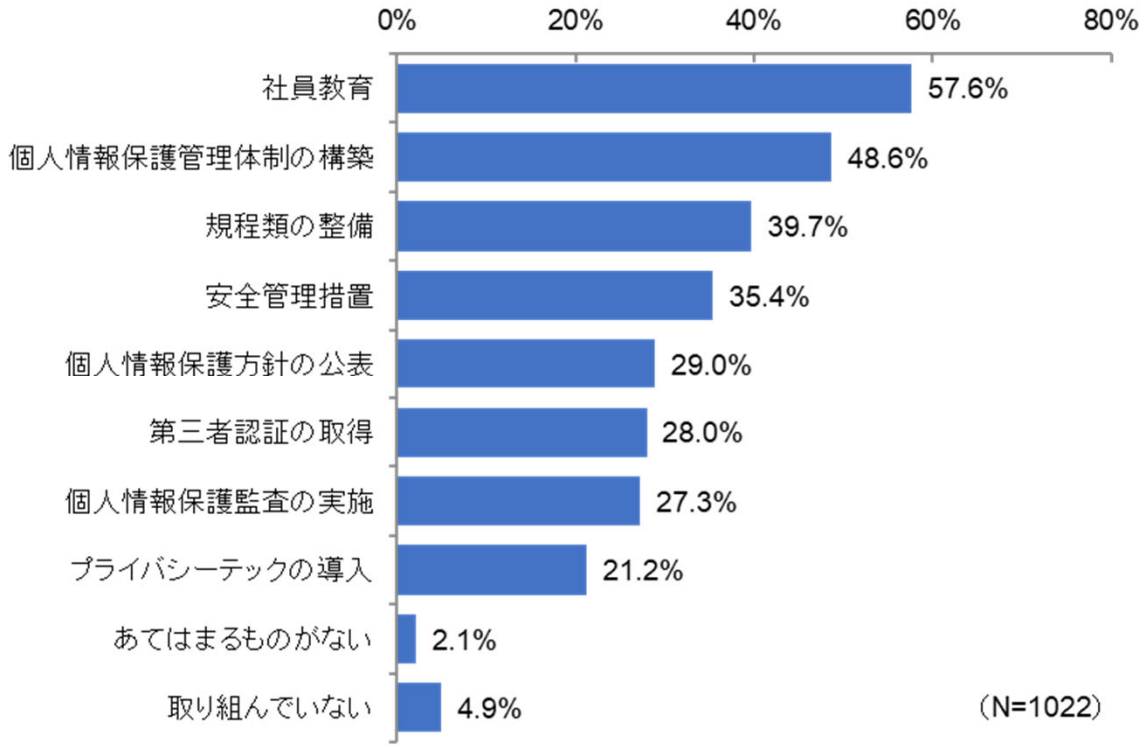


4）個人情報保護

- Q６_１：　個人情報保護についての取り組み
- Q６_２：　改正個人情報保護法施行にむけての取り組み
- Q６_３：　各国プライバシー保護規制の影響
- Q７　　：　プライバシーソリューション／テックの導入

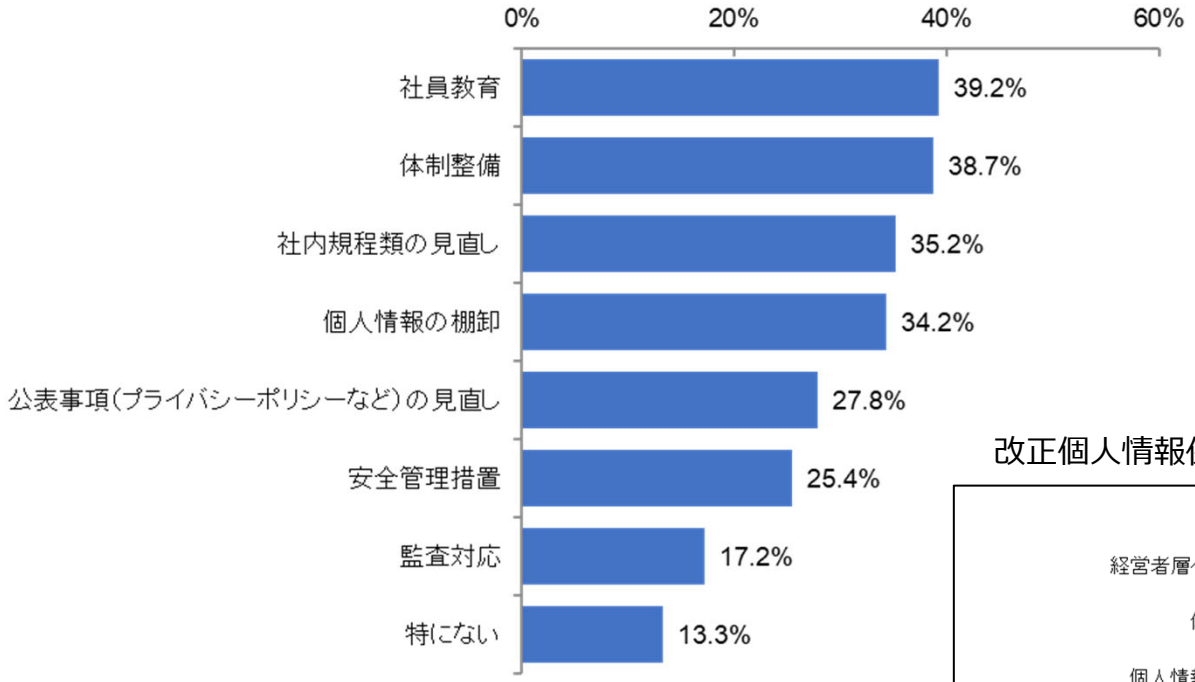
Q６_１：個人情報保護についての取り組み（2023年）

■ 個人情報保護についての取り組みでは、社員教育が最も多く、次いで管理体制の構築、規程類の整備と続く。安全管理措置や第三者認証はその次で実装面での取り組みはやや低い。

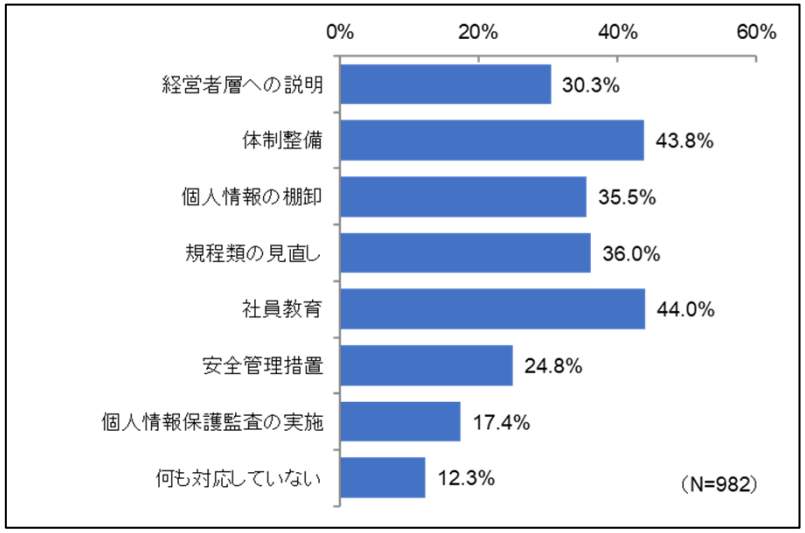


Q6_2：改正個人情報保護法遵守の課題（2023年）

■ 改正個人情報保護法遵守についても、社員教育と体制整備の比率が高く、昨年と同様となった。

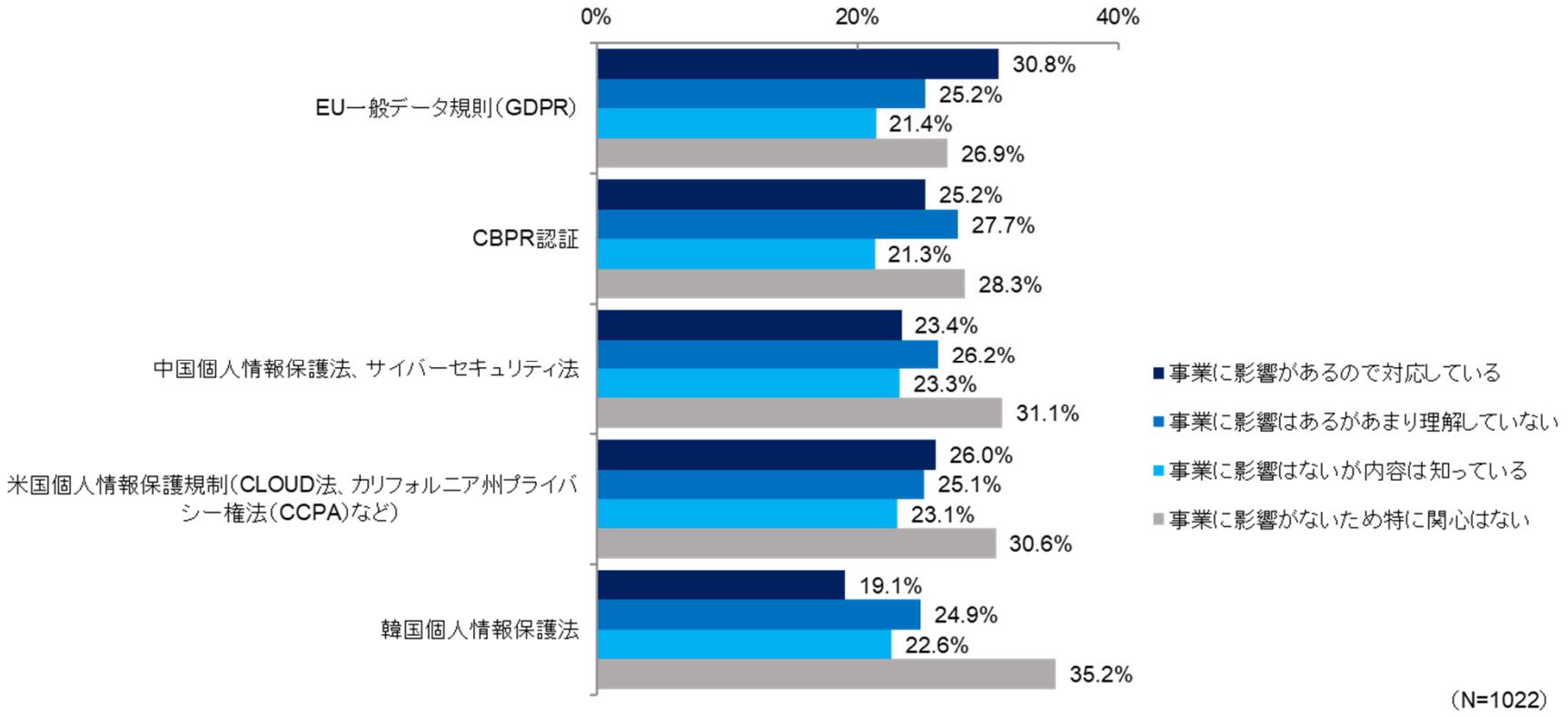


改正個人情報保護法施行向けた取り組み（2022年）



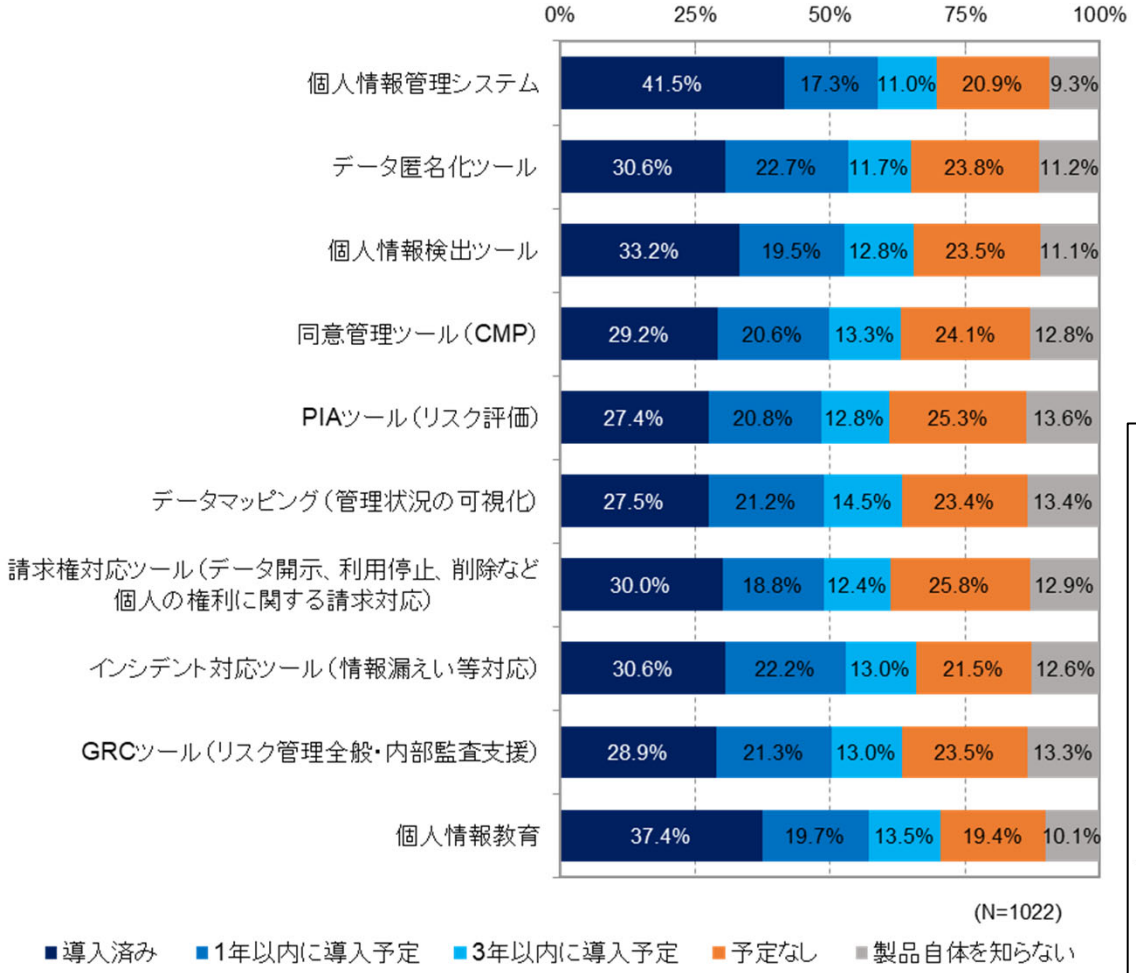
Q６_3：各国のプライバシー法規制の影響（2023年）

■ 各国のプライバシー法規制の影響については、影響があり対応しているが最も高いはEU GDPRで３割を超えている。逆に影響がなく関心もないのは韓国個人情報保護法となっている。

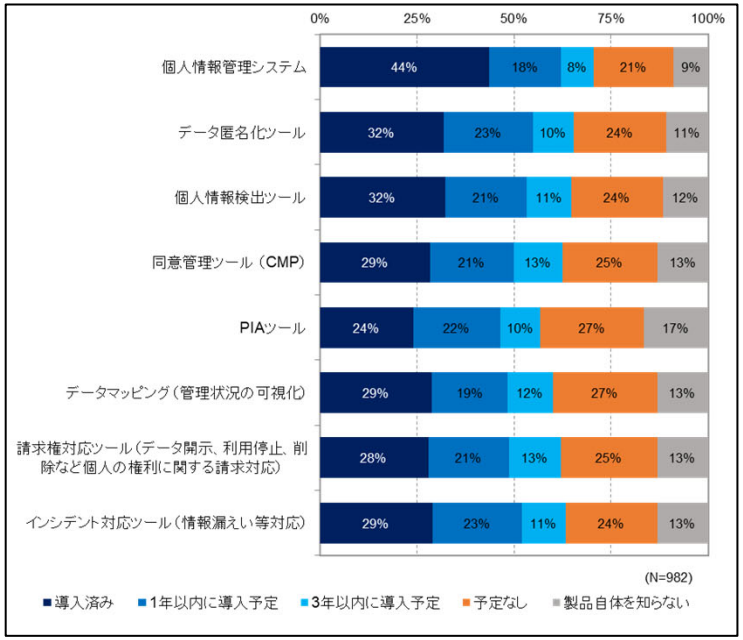


Q7：プライバシーソリューション／テックの導入状況（2023年）

■ 導入しているプライバシーソリューション／テックでは、個人情報管理システムが最も多く４割を超えており、個人情報教育サービスが続く。



プライバシーソリューション／テックの導入状況（2022年）

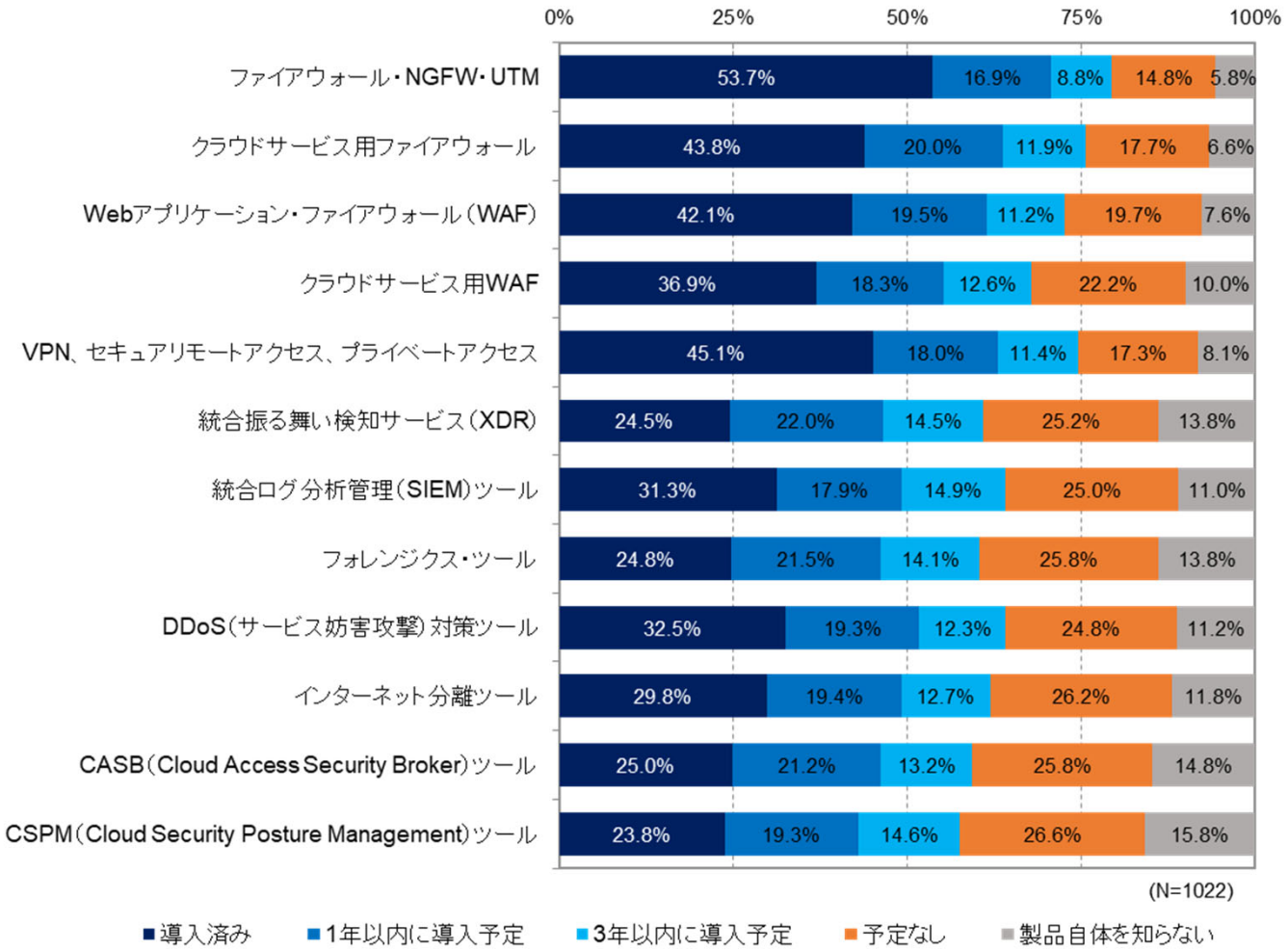


5）セキュリティ製品／技術の利用動向

- Q８_1　：セキュリティ製品・サービスの導入状況（ネットワーク／プラットフォーム）
- Q８_2　：セキュリティ製品・サービスの導入状況（クライアント）
- Q８_3　：セキュリティ製品・サービスの導入状況（サービス）
- Q９_1　：電子メールのセキュリティ対策状況
- Q９_2　：PPAPの送信時対応状況
- Q９_3　：PPAPのファイル受信への対応状況
- Q10　　：機密性の高いシステムのアクセス認証手段

Q８_１：セキュリティ製品の利用状況（ネットワーク/ゲートウェイ系）（2023年）

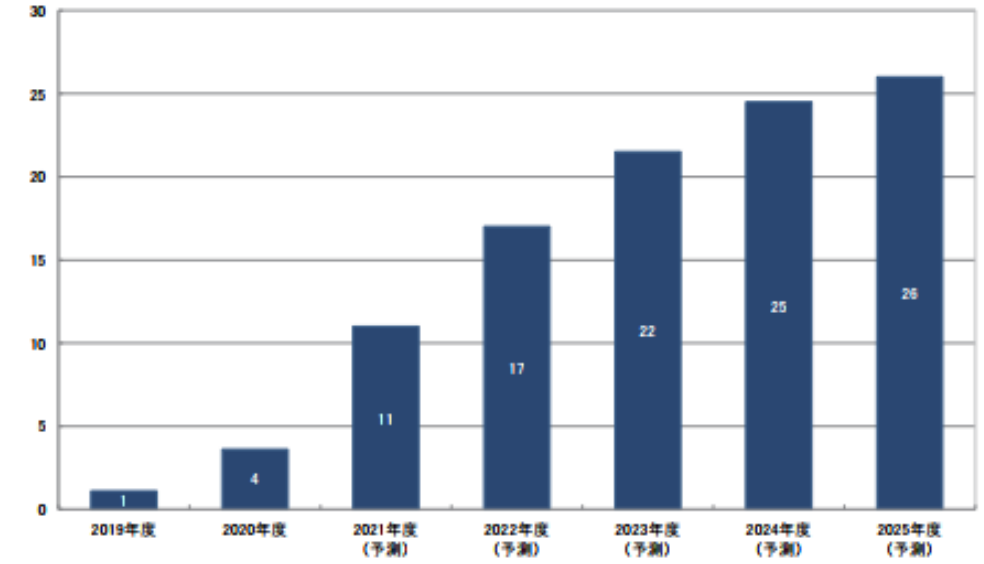
- 依然、従来型セキュリティ製品であるファイアウォールやVPNの導入比率が高いが、次世代型のクラウドファイアウォールやWAFも増加してきている。
- 最近注目されている、XDRやCSPMの導入比率は約２割強で、まだ低い。



【ご参考 】CSPM市場予測

- クラウドサービスの設定ミスや設定漏れを指摘するCSPMはクラウドサービスの利用拡大に伴い大きく伸びてきており、年平均市場成長率48.5%という驚異的な成長が見込まれる。

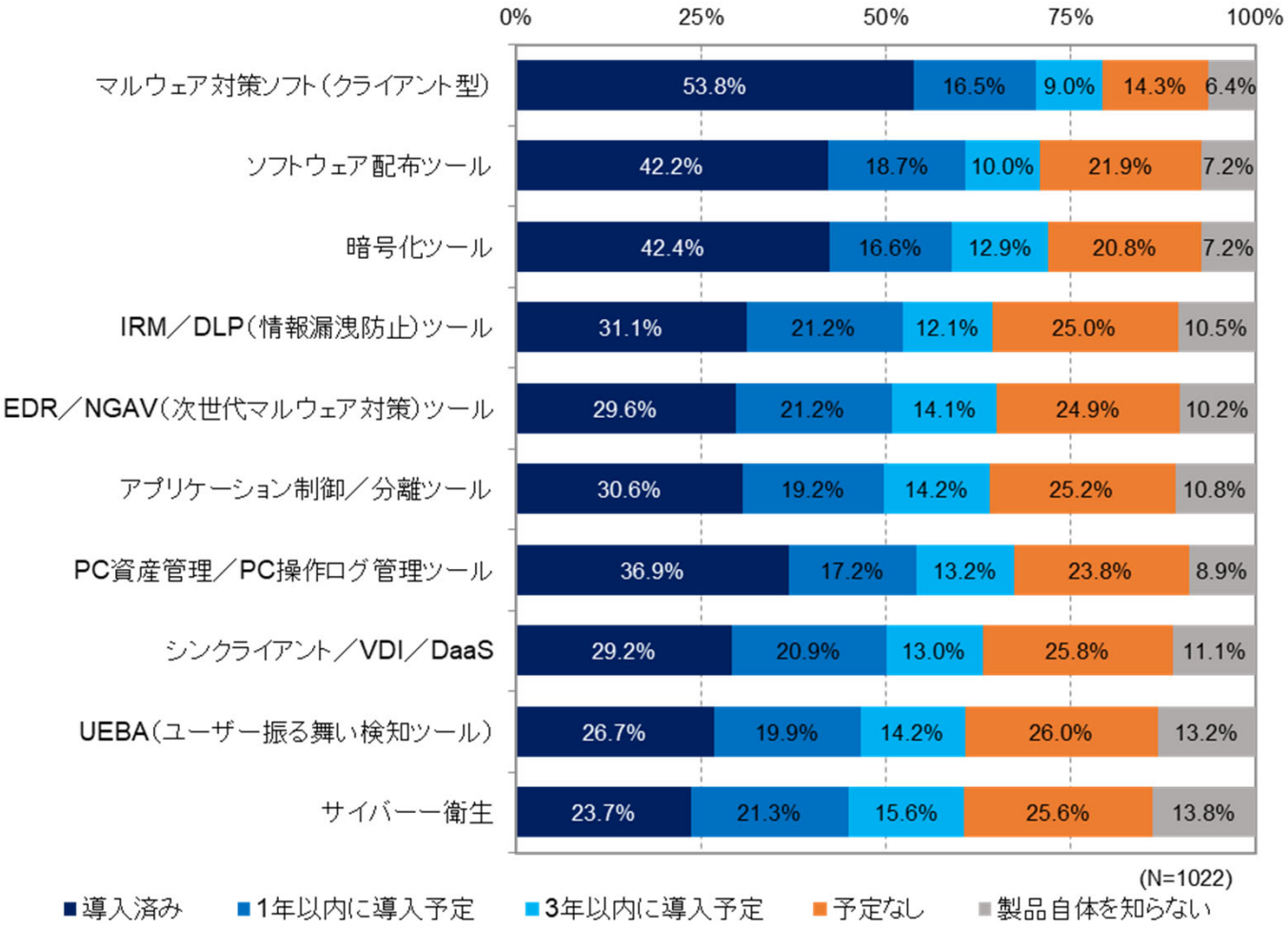
	2019年度	2020年度	2021年度（予測）	2022年度（予測）	2023年度（予測）	2024年度（予測）	2025年度（予測）	CAGR（2020～2025）
市場規模（単位：百万円）								
CSPM	110	360	1,100	1,700	2,150	2,450	2,600	48.5%
前年度比	—	327.3%	305.6%	154.5%	126.5%	114.0%	106.1%	



(出典：ITR Market View エンドポイント／無害化／Web分離／CASB／CSPM／CWPP／SOAR市場2022)

Q８_２：セキュリティ製品の利用状況（クライアント）（2023年）

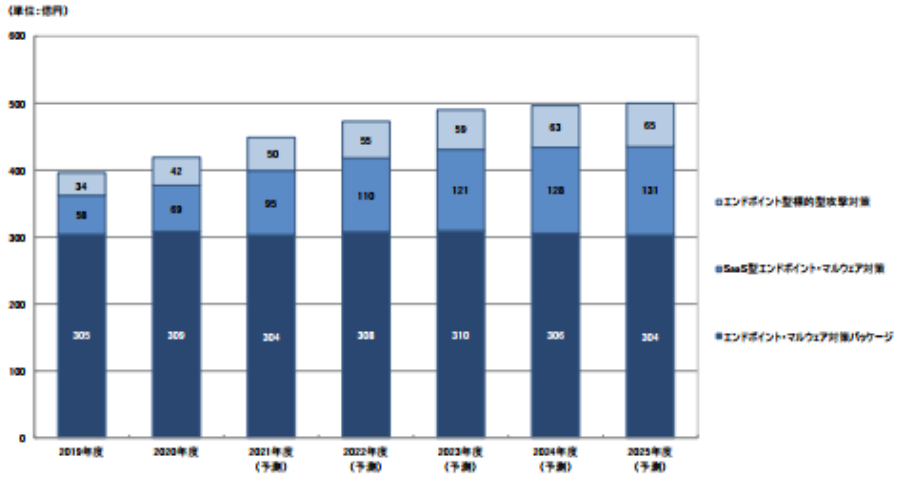
■ 依然、従来型のマルウェア対策ソフトの導入比率が約５割を占めているが、次世代型のEDR/NGAVも約３割を占めるようになっており、差は小さくなっている。



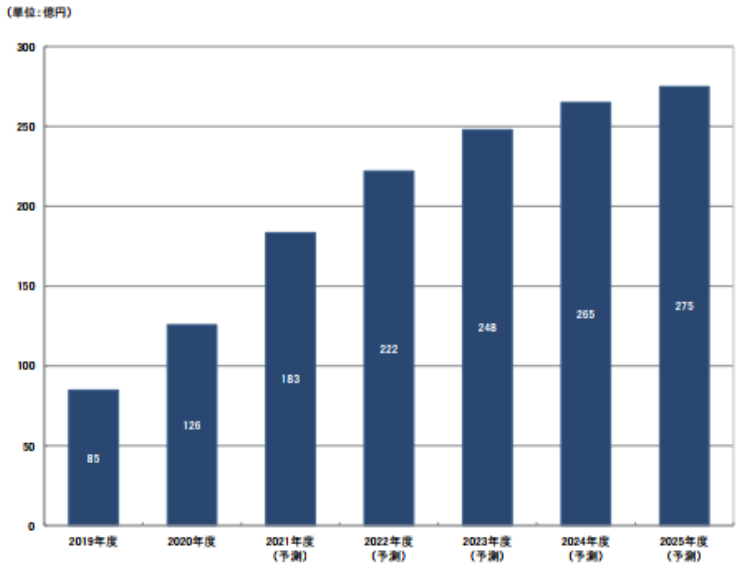
【ご参考 】従来型アンチウィルス（EPP）市場と次世代型EDR/NGAV市場予測

■ まだ、従来型の方が市場規模は大きいが、平均市場成長率は3.8%と低成長になってきている一方
次世代型は、平均市場成長率16.9%と高い伸びを示しており、いずれ市場が統合すると予測している。

従来型アンチウィルス市場



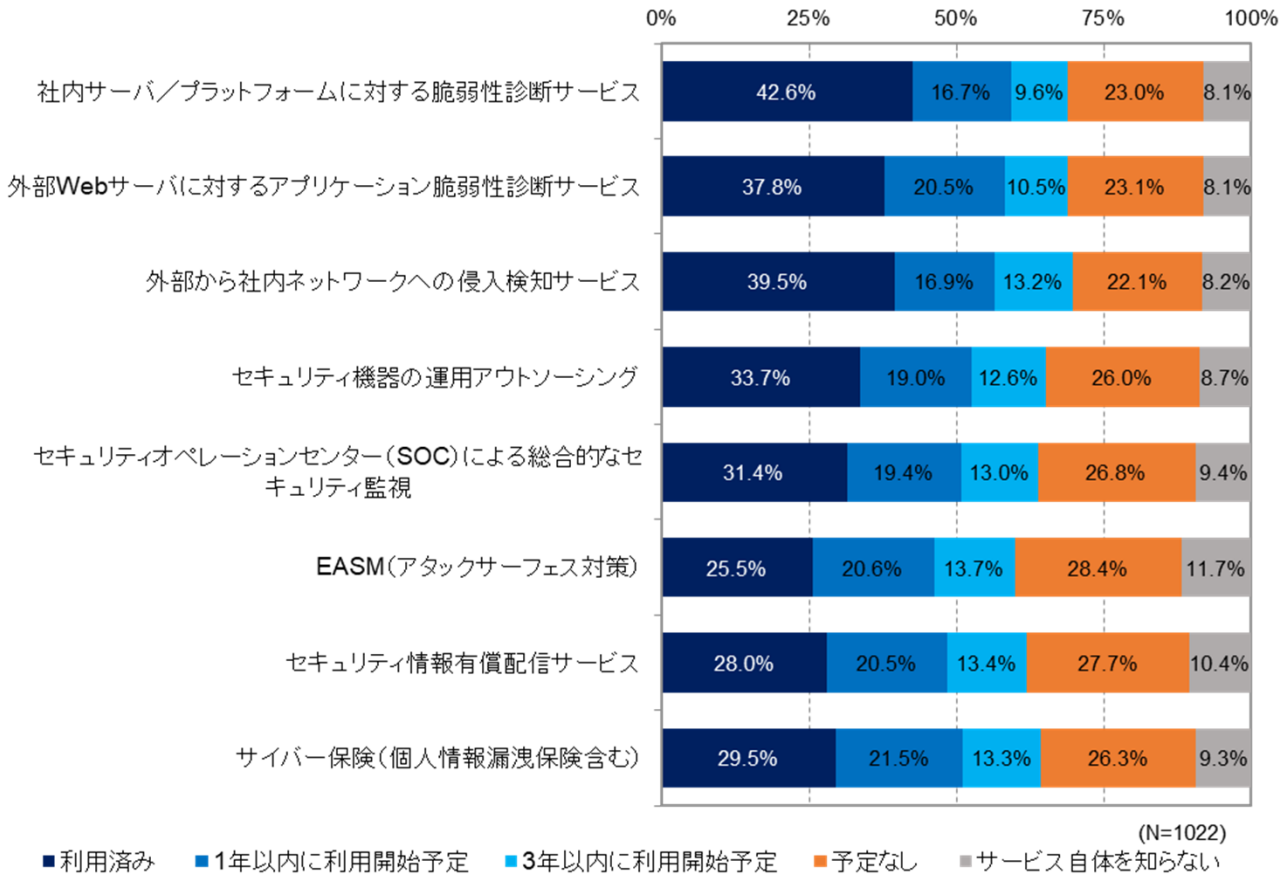
次世代型EDR/NGAV市場



(出典：ITR Market View エンドポイント／無害化／Web分離／CASB／CSPM／CWPP／SOAR市場2022)

Q８_３：セキュリティ製品の利用状況（セキュリティサービス）（2023年）

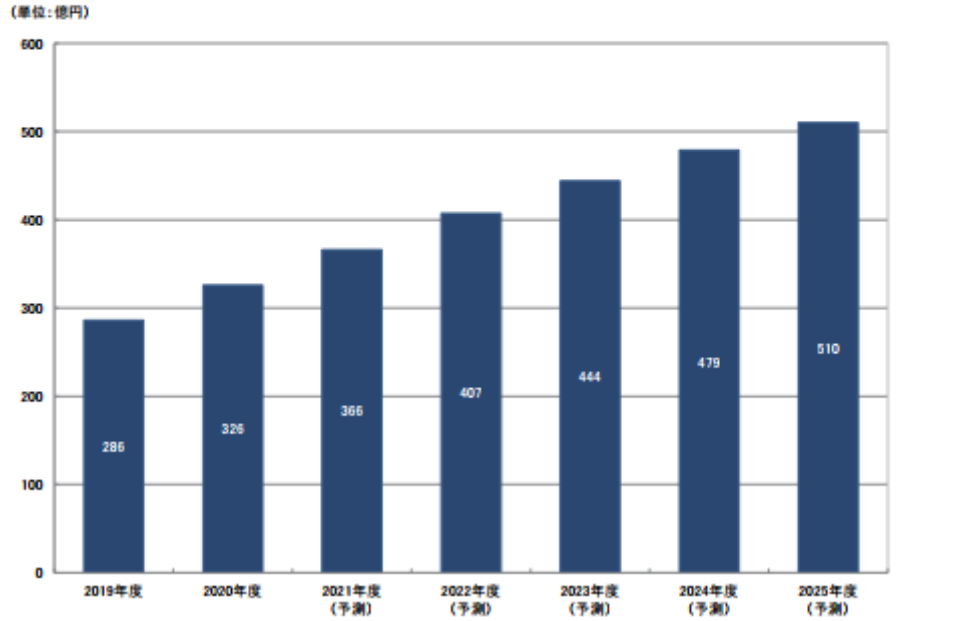
■ 脆弱性診断サービスや侵入検知サービスは導入済が約４割となっており、導入予定を含めると約７割に達しており、導入が一般化してきている。



【ご参考 】脆弱性診断サービス市場予測

- ランサムウェア等のサイバー攻撃の増加に伴い、自社システム・サービスの脆弱性を診断するサービスが伸びており、平均市場成長率 9.4%となっている。

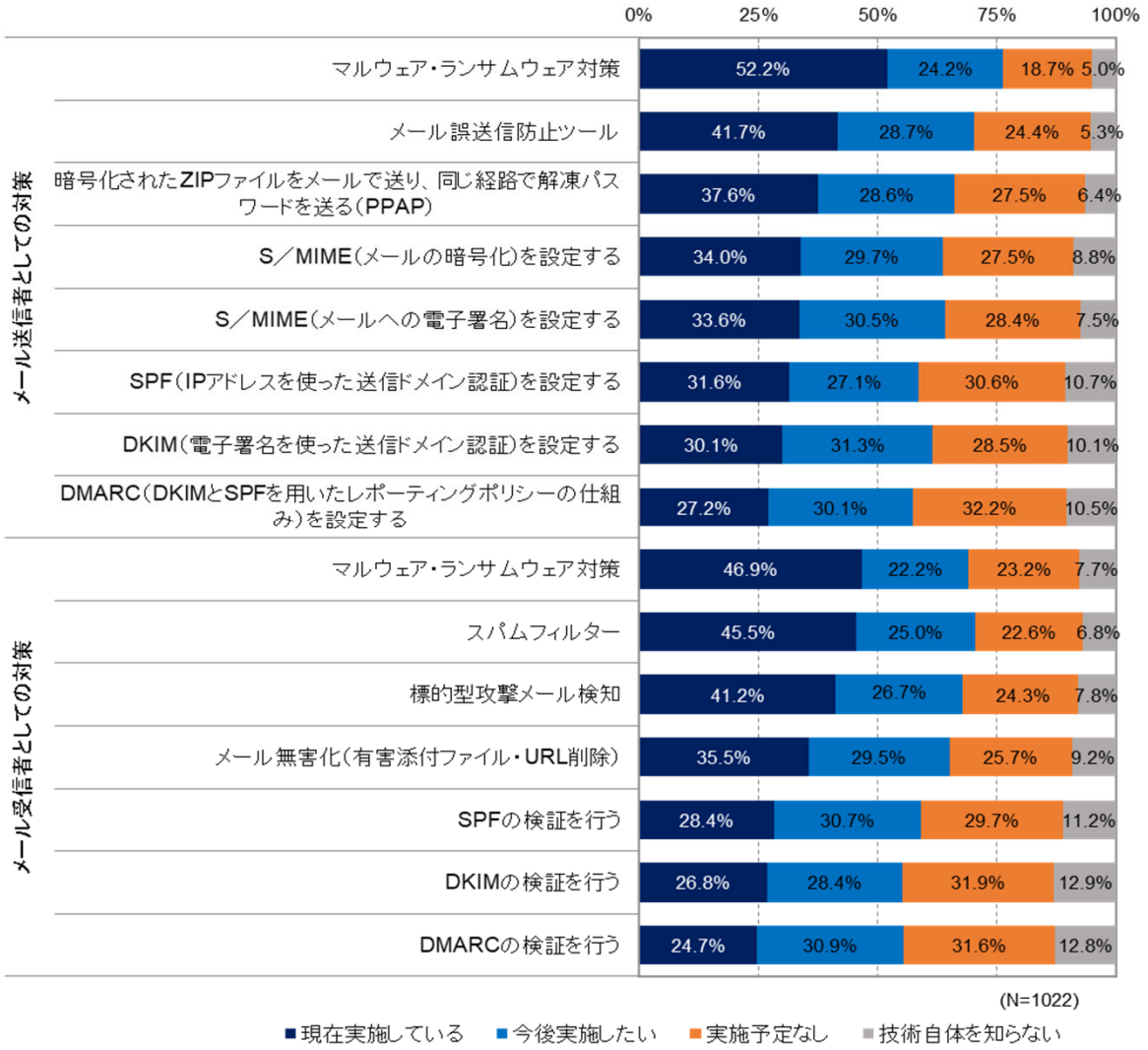
	2019年度	2020年度	2021年度（予測）	2022年度（予測）	2023年度（予測）	2024年度（予測）	2025年度（予測）	CAGR（2020～2025）
市場規模 （単位：百万円）								
セキュリティ脆弱性診断サービス	28,620	32,570	36,600	40,700	44,400	47,900	51,000	9.4%
前年度比	―	113.8%	112.4%	111.2%	109.1%	107.9%	106.5%	



(出典：ITR Market View サイバー・セキュリティ・コンサルティング・サービス市場2021)

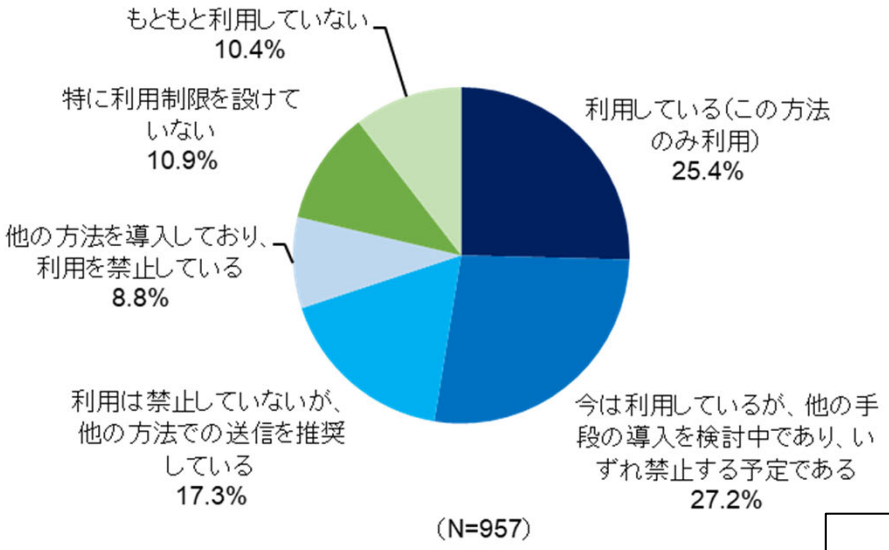
Q９_１：電子メールのセキュリティ対策状況（2023年）

■ 送信側・受信側共に実施済はマルウェア・ランサムウエア対策がトップで、メール経由での感染対策が重視されていることがわかる。

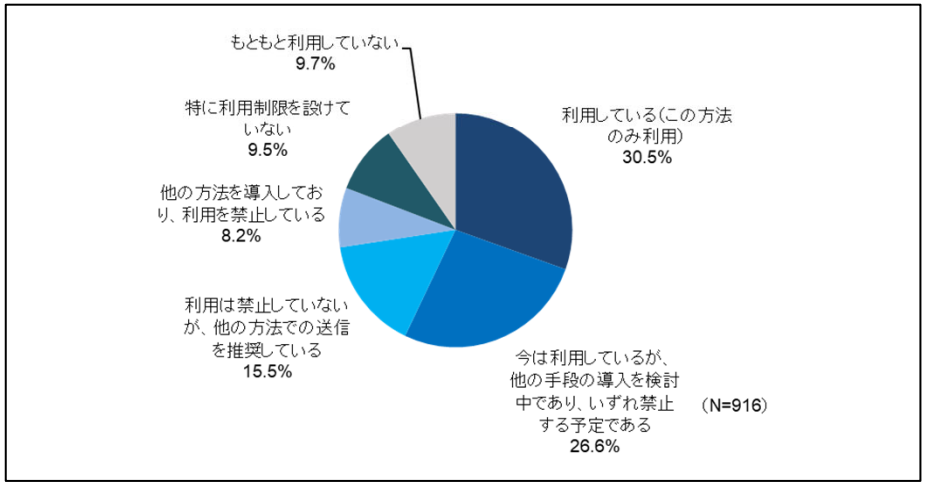


Q９_２：PPAP（Zip暗号化添付メール＆パスワード同一経路送付）への対応状況

- PPAP（送信系）をもともと利用していないが10.4%、利用を禁止しているが8.8%で、今後利用を禁止予定の27.2%を含めると約５割弱が禁止する方向となっている。

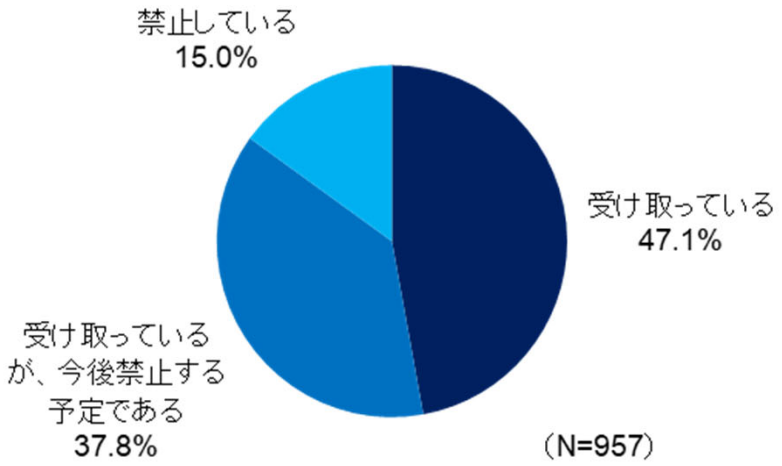


PPAP送信系対応状況（2022年）

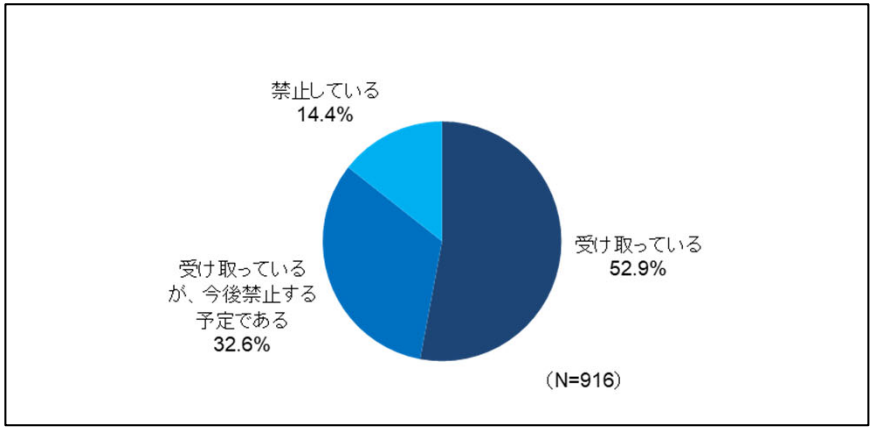


Q９_３：PPAP（Zip暗号化添付メール＆パスワード同一経路送付）での受信対応

- PPAPの受信側では、禁止しているが15.0%、今後禁止予定が37.8%で、約５割弱が禁止する方向である。

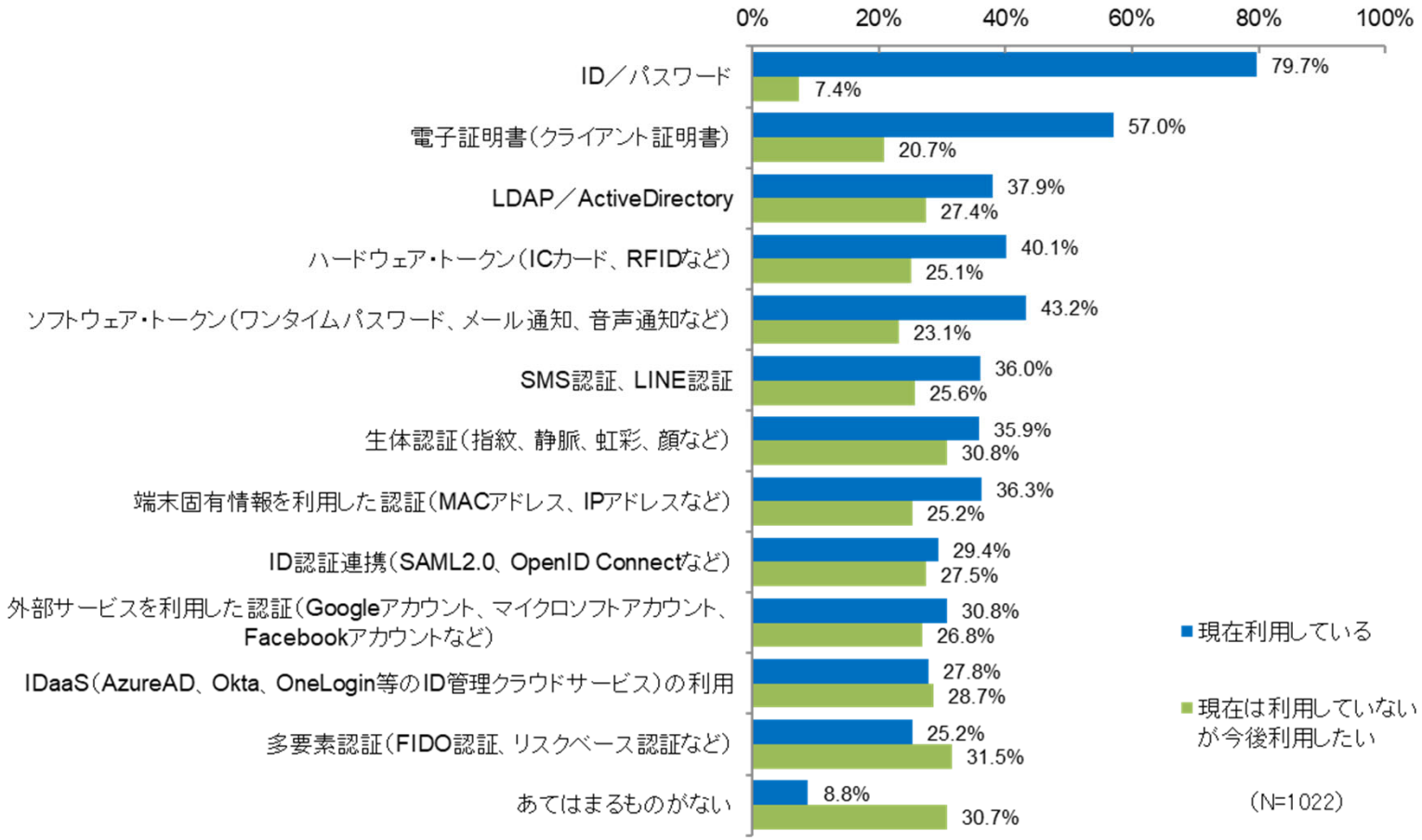


PPAP受信系対応状況（2022年）



Q10：高機密システムへのアクセス認証手段（2023年）

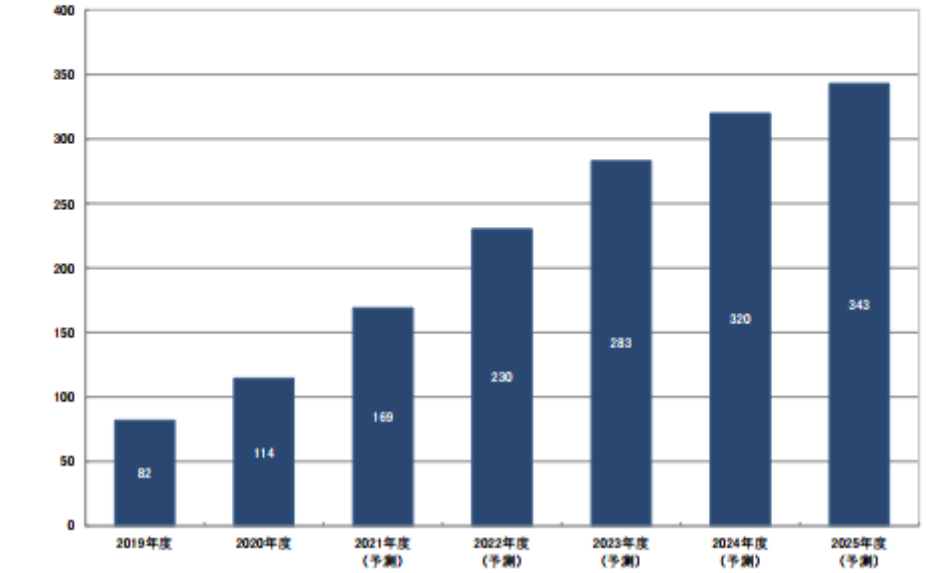
- 現在利用している認証手段としてはID・パスワードが最も多いが、採用予定は少ない。代わりに生体認証や多要素認証、IDaaSの採用予定が多くなっている。



【ご参考 】IDaaS市場予測

■ クラウドサービスの利用増加に伴い、クラウドサービスの統合認証・統合ID管理を行うIDaaSのニーズが拡大しており、年平均市場成長率 24.6%と驚異的な成長が見込まれる。

	2019年度	2020年度	2021年度（予測）	2022年度（予測）	2023年度（予測）	2024年度（予測）	2025年度（予測）	CAGR（2020～2025）
市場規模（単位：百万円）								
IDaaS	8,180	11,440	16,890	23,000	28,300	32,000	34,300	24.6%
前年度比	―	139.9%	147.6%	136.2%	123.0%	113.1%	107.2%	



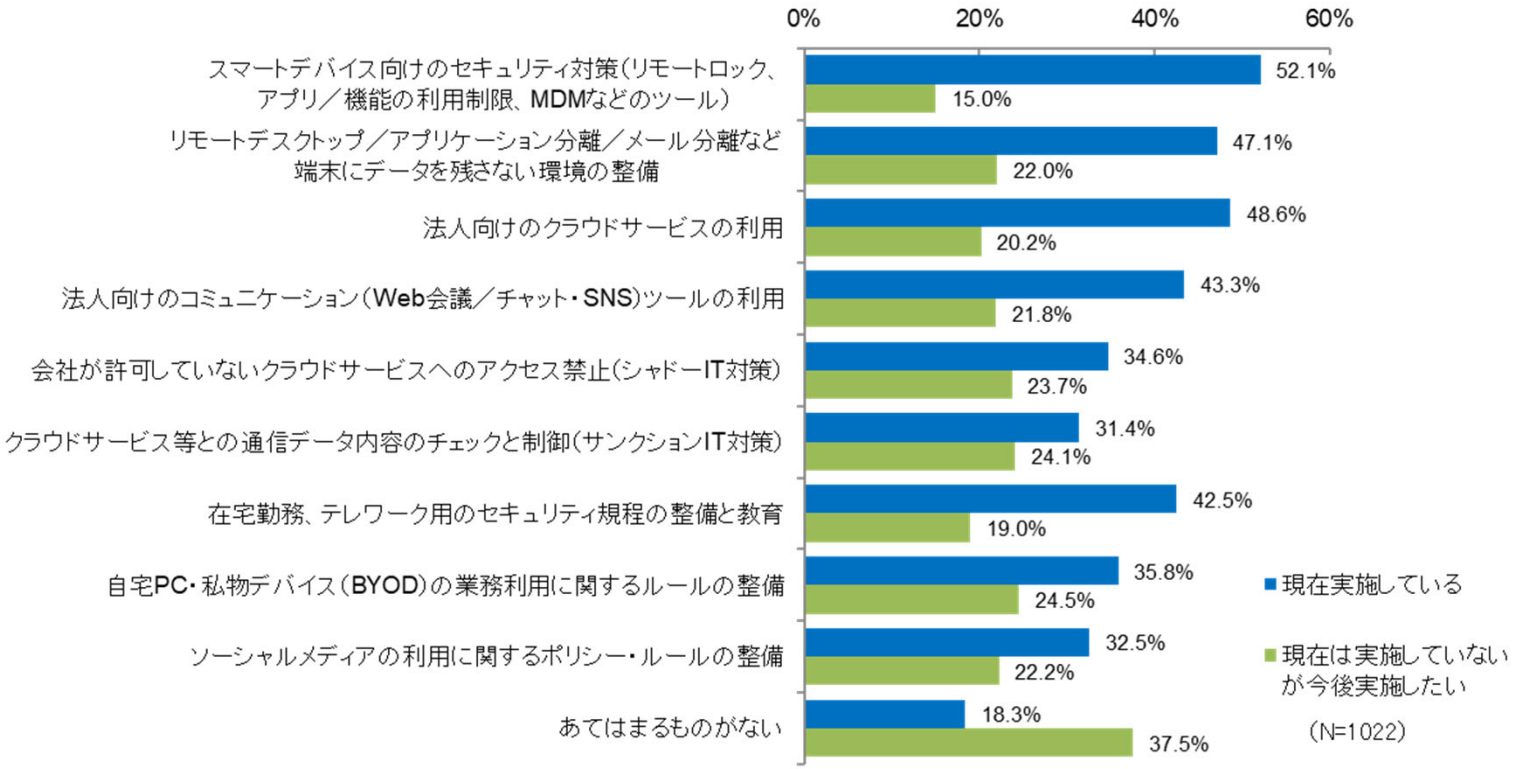
(出典：ITR Market View アイデンティティ・アクセス管理／個人認証型セキュリティ市場2022)

６） 新たなワークスタイルとクラウドの動向

- Q11： 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
- Q12： クラウドサービスの動向

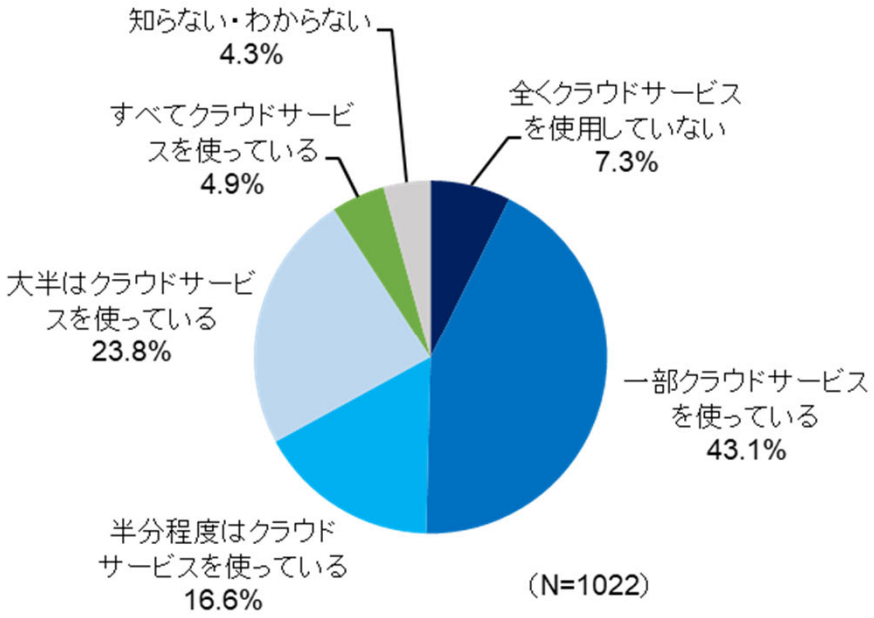
Q11：柔軟なワークスタイルを実現するためのセキュリティ対策（2023年）

- セキュリティ対策としては、「スマートデバイス向け対策」、「端末にデータを残さない環境整備」、「法人向けクラウドサービス利用」が約５割となっている。



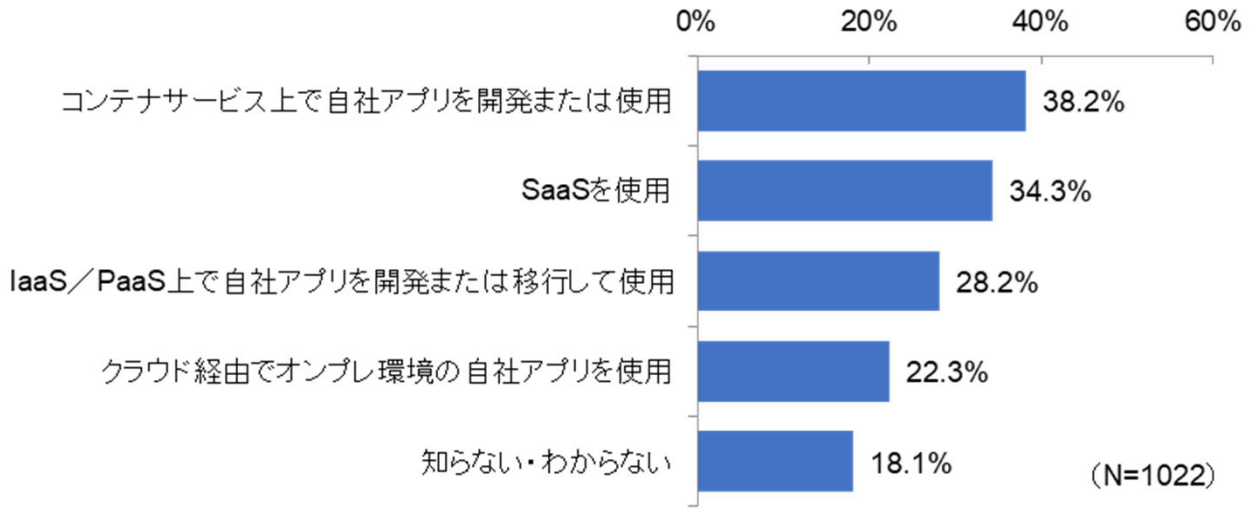
Q12_1：クラウドサービス利用状況（2023年）

- 半分以上クラウドサービスを使用している比率が約５割に近づいており、クラウドサービスの利用がすこしずつ増加している。



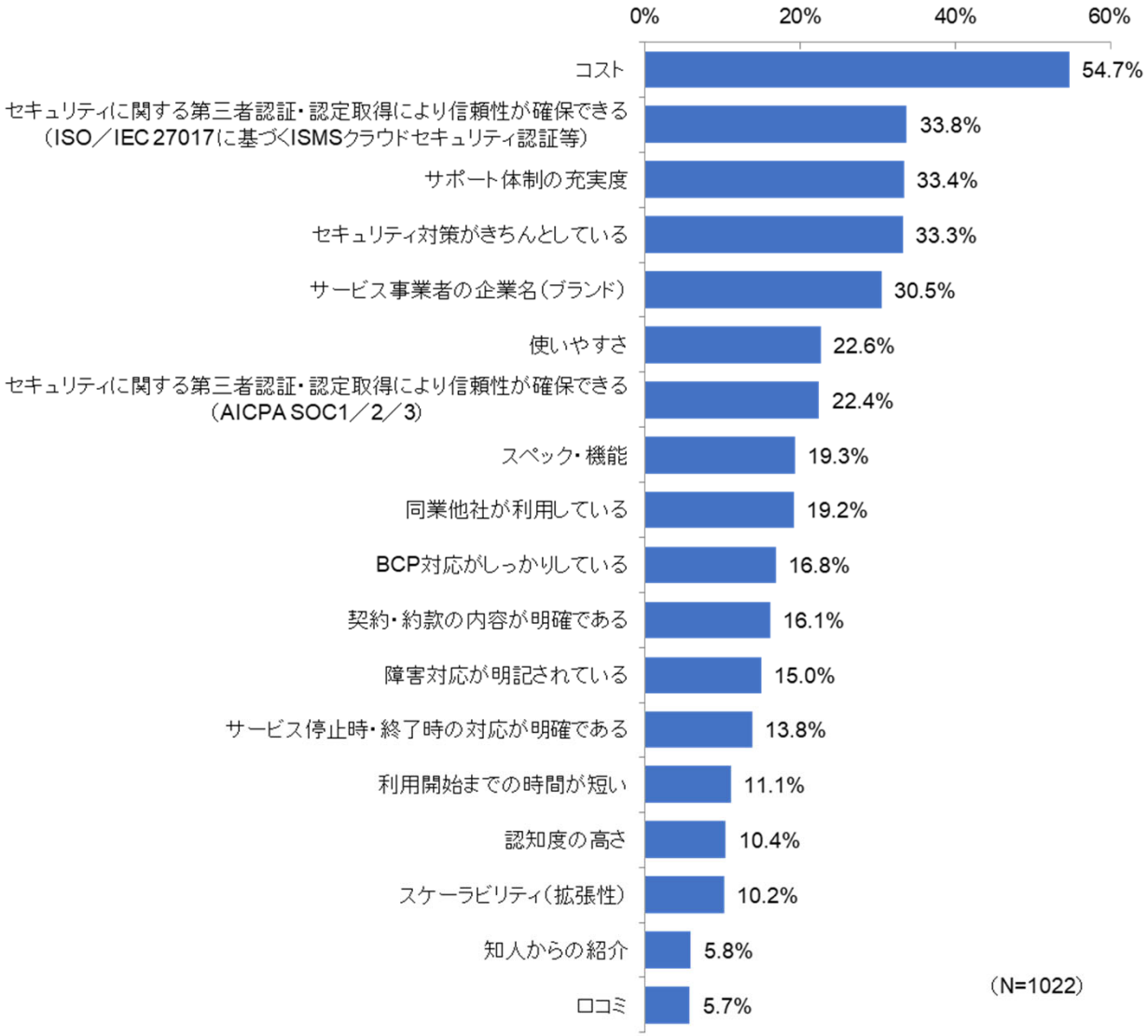
Q12_2：クラウドサービス利用方法（2023年）

- コンテナサービス上での開発の比率がトップで、SaaSの利用が続いており、IaaS/PaaS上の開発・移行の比率が若干低くなってきている。



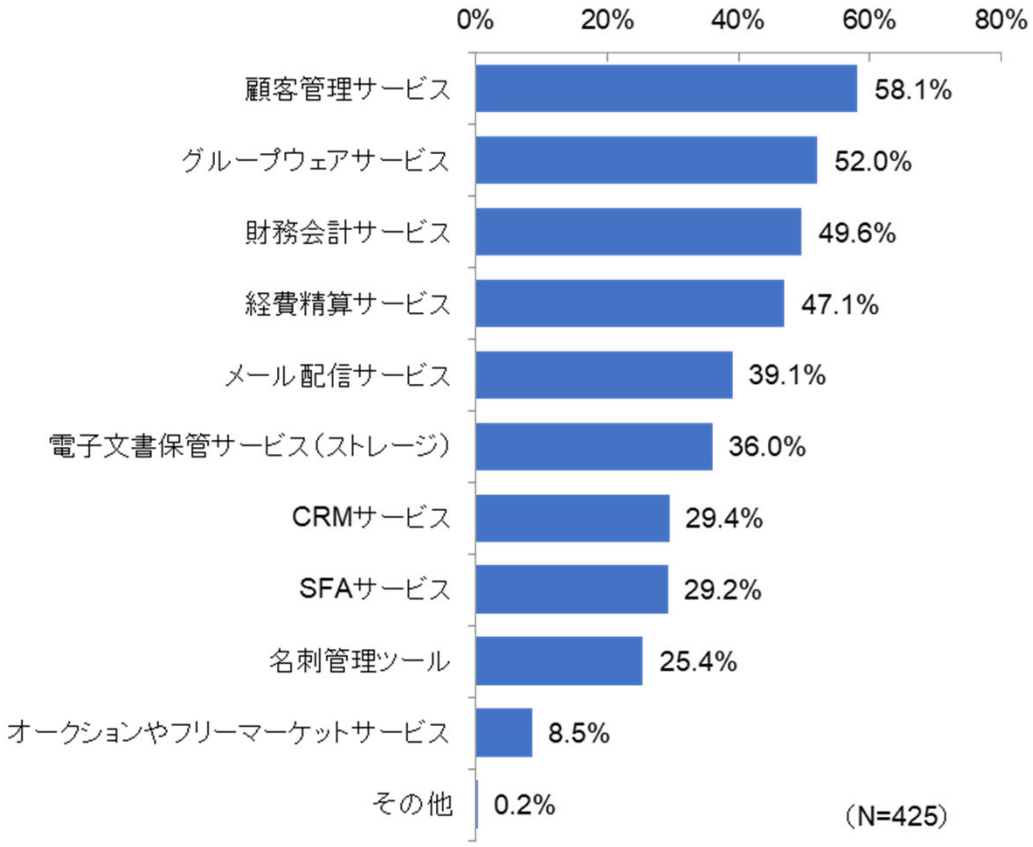
Q12_3：クラウドサービス選定する際のポイント（2023年）

■ クラウドサービス選定時のポイントは２位以下を大きく引き離して「コスト」で、「信頼性の確保」と「サポート体制の充実」、「セキュリティ対策」が続いている。



Q12_4：信頼性を重視して選ぶクラウドサービス（2023年）

■ 信頼性重視で選ばれるクラウドサービスとして、顧客管理がNo.1になり、グループウェア、財務会計サービスが続いている。

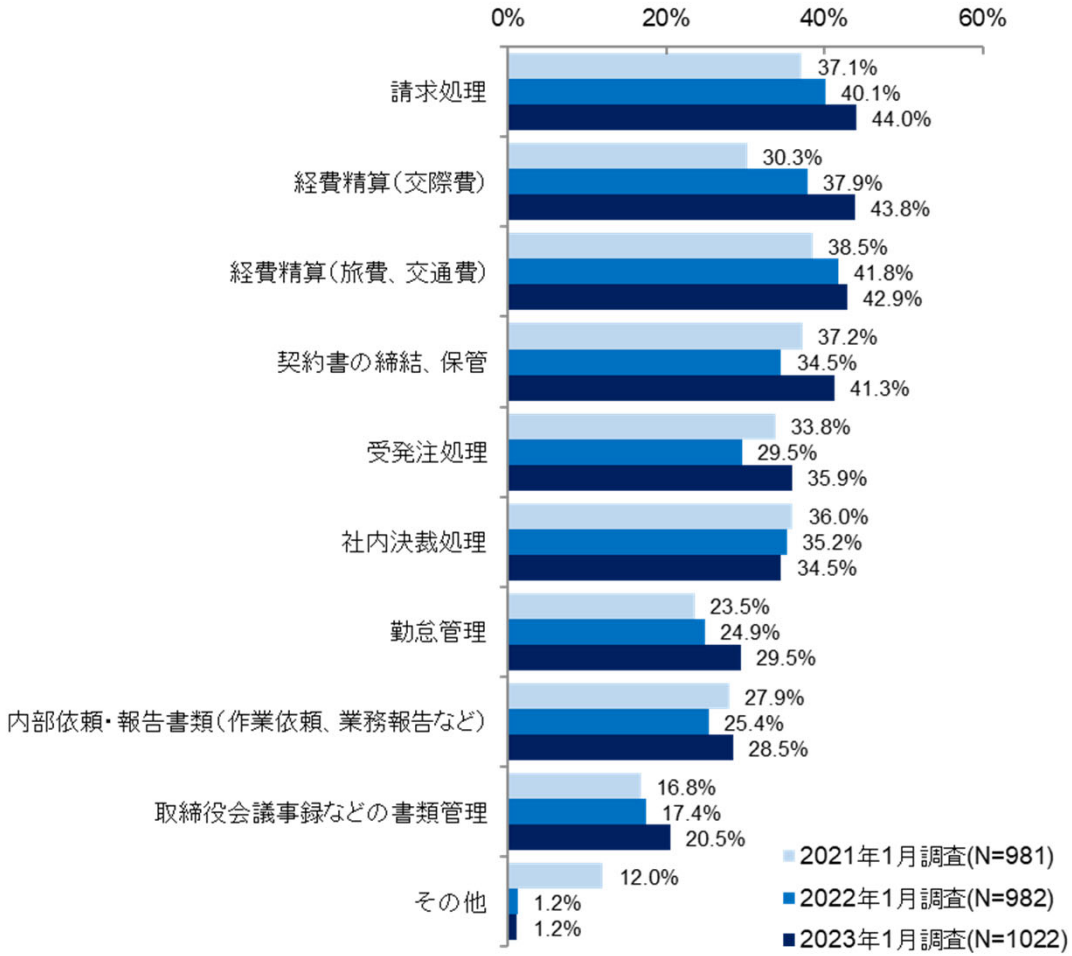


7）電子契約関連、ＤＸ推進

- Q13：電子インボイス・電子契約関連
- Q14：DX推進

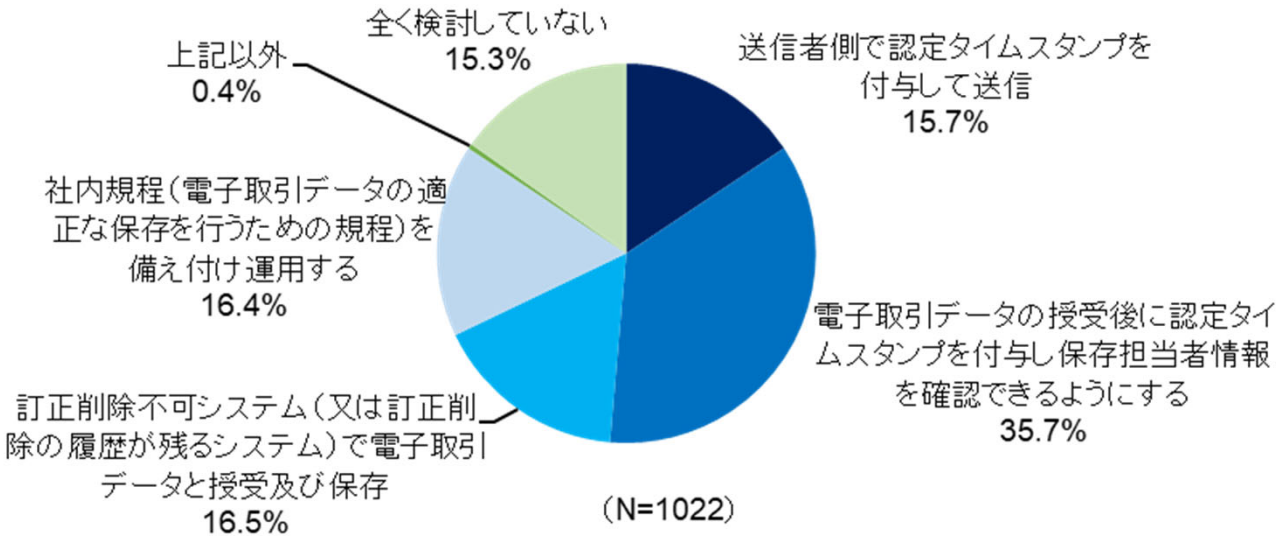
Q13_1：特に電子化したい業務プロセス（過去２回との比較）

■ 電子化したい業務プロセスでは、今回初めて請求処理がトップとなり、次いで経費精算（交際費）、経費精算（旅費、交通費）の順となった。



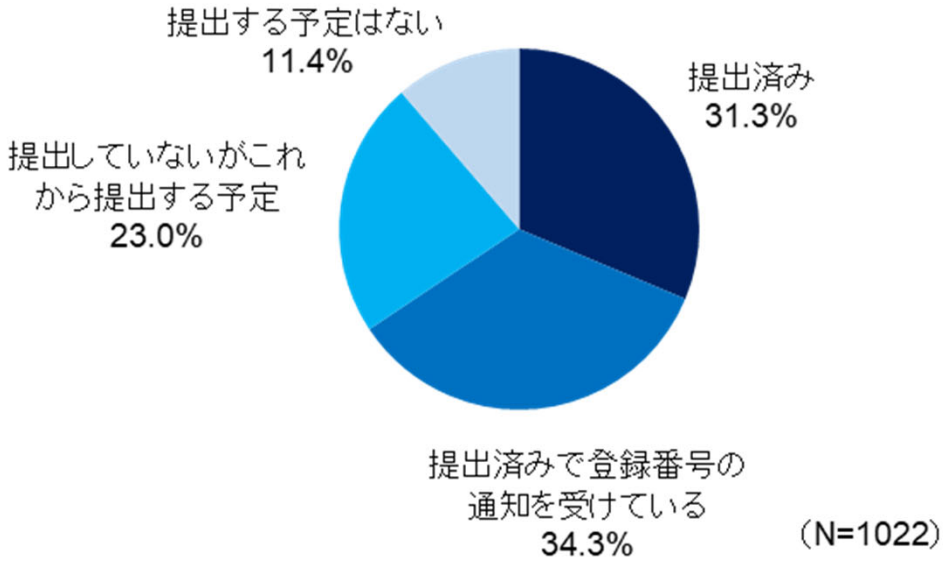
Q13_2：電子帳簿保存法の保存要件への対応方法（2023年）

- 電子帳簿保存法の保存要件への対応方法では「授受後のタイムスタンプ」がトップで、「訂正削除不可システムでの保存」、「社内規程での運用」が続く。



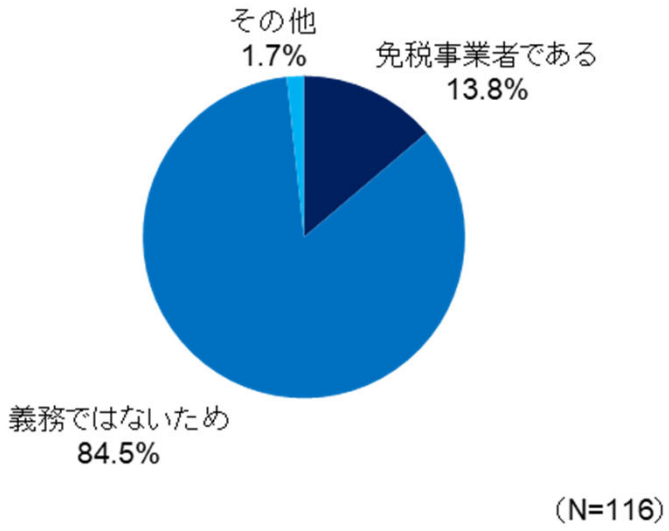
Q13_３：インボイス制度での登録申請書の提出状況（2023年）

■ インボイス制度の登録申請書は約2/3の事業者が提出済、提出予定を含めると約９割に達する。



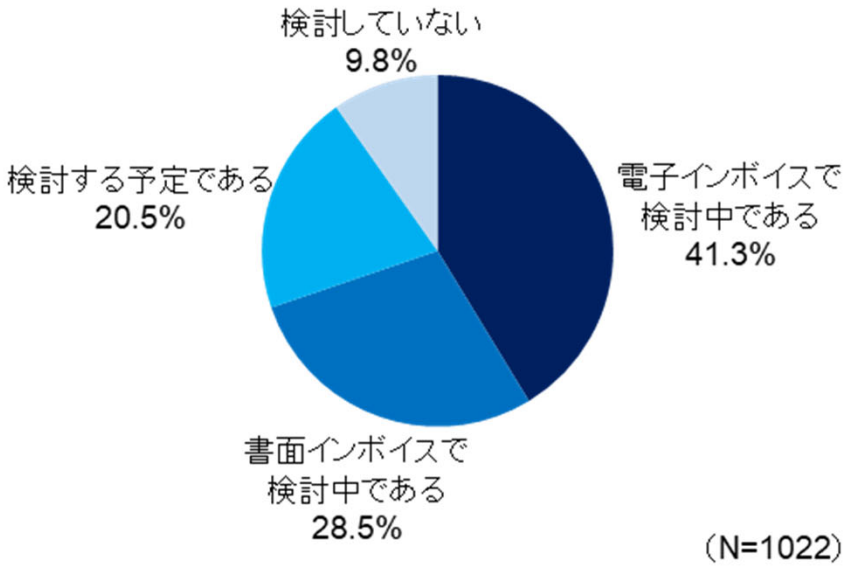
Q13_４：インボイス制度の登録申請書を提出しない理由（2023年）

■ 登録申請書を提出していない方の理由は「義務ではない」が８割超で圧倒的に多く、「免税事業者」が約１割強と回答。



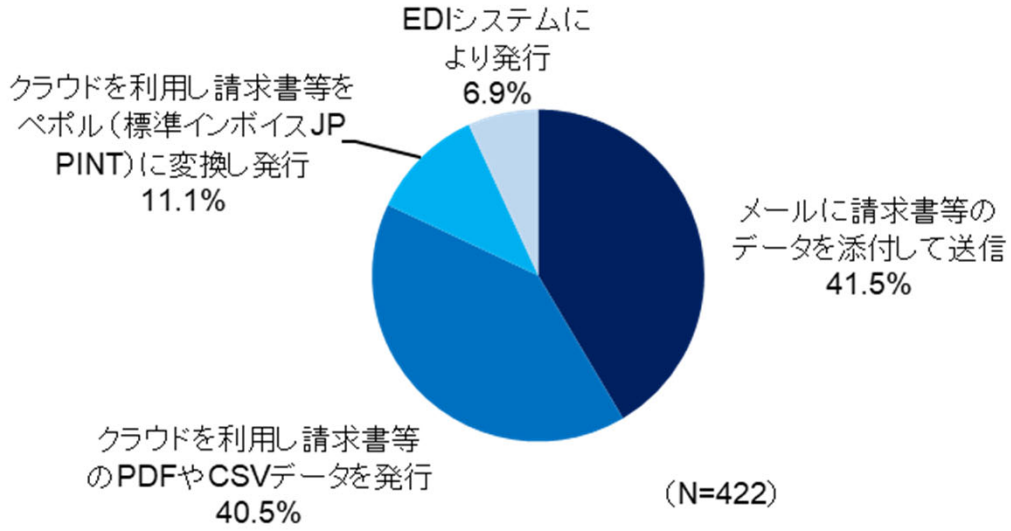
Q13_５：インボイスの作成・発行の検討状況（2023年）

- インボイスの検討状況では、「電子インボイスで検討中」が約４割、「書面インボイスで検討中」が約３割で検討予定を含めると約９割で検討または検討予定と回答。



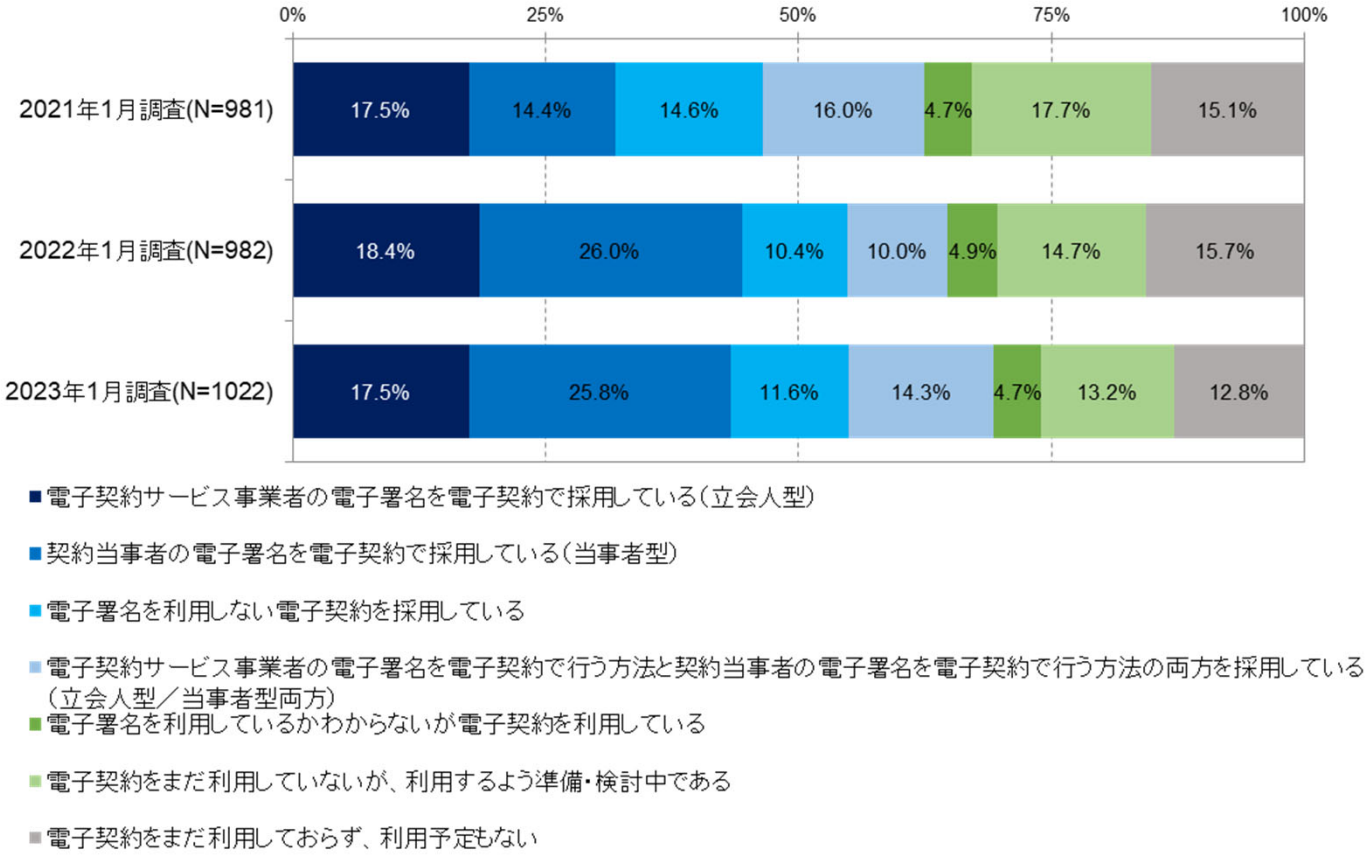
Q13_6：電子インボイスの発行方法（2023年）

- 電子インボイスの発行方法では、「メールに添付して送信」がトップで、「クラウドで請求書等のデータを発行」が続く。



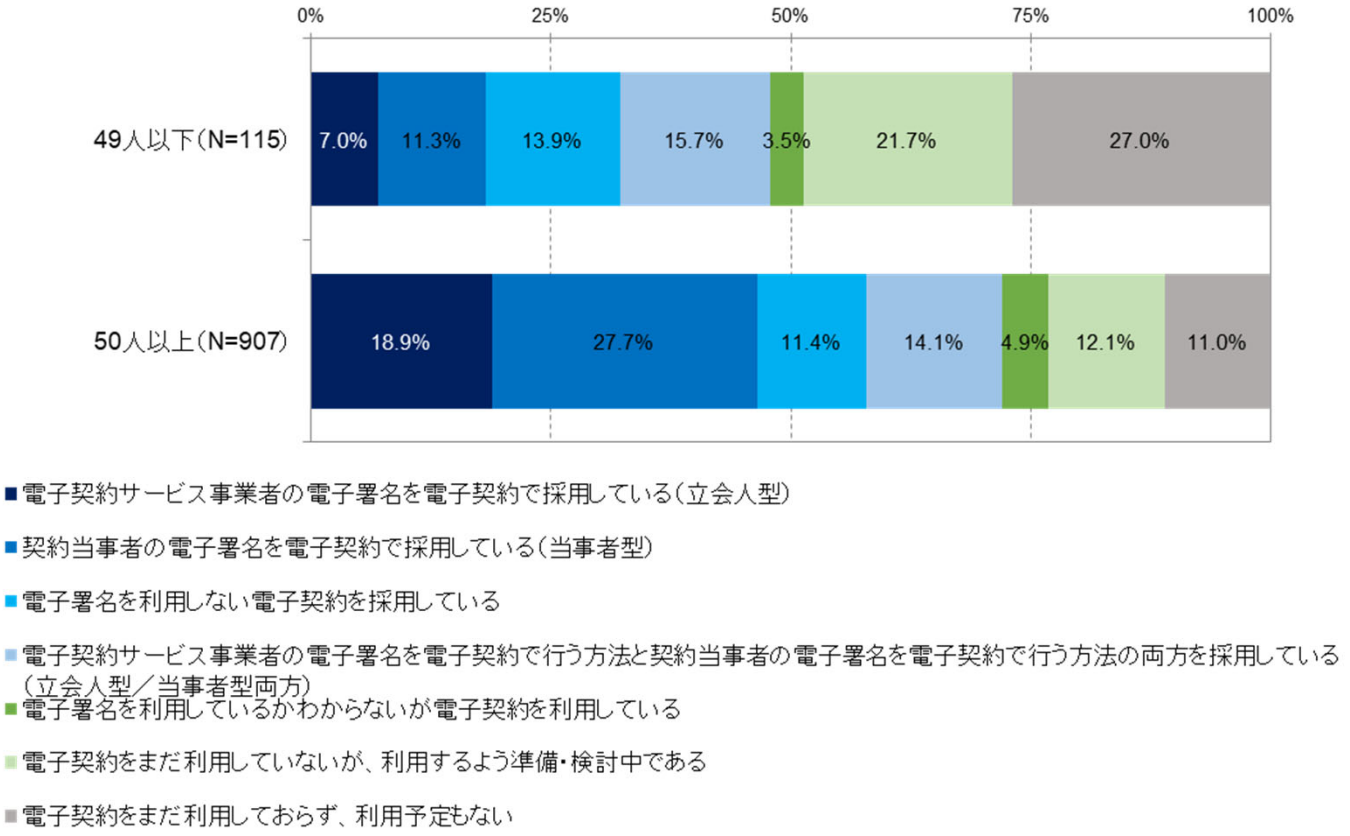
Q13_7：電子契約の利用状況（過去２回との比較）

■ 電子契約の利用状況では、採用している比率が毎回増加しており約７割に達している。内訳では当事者型が最も多い。



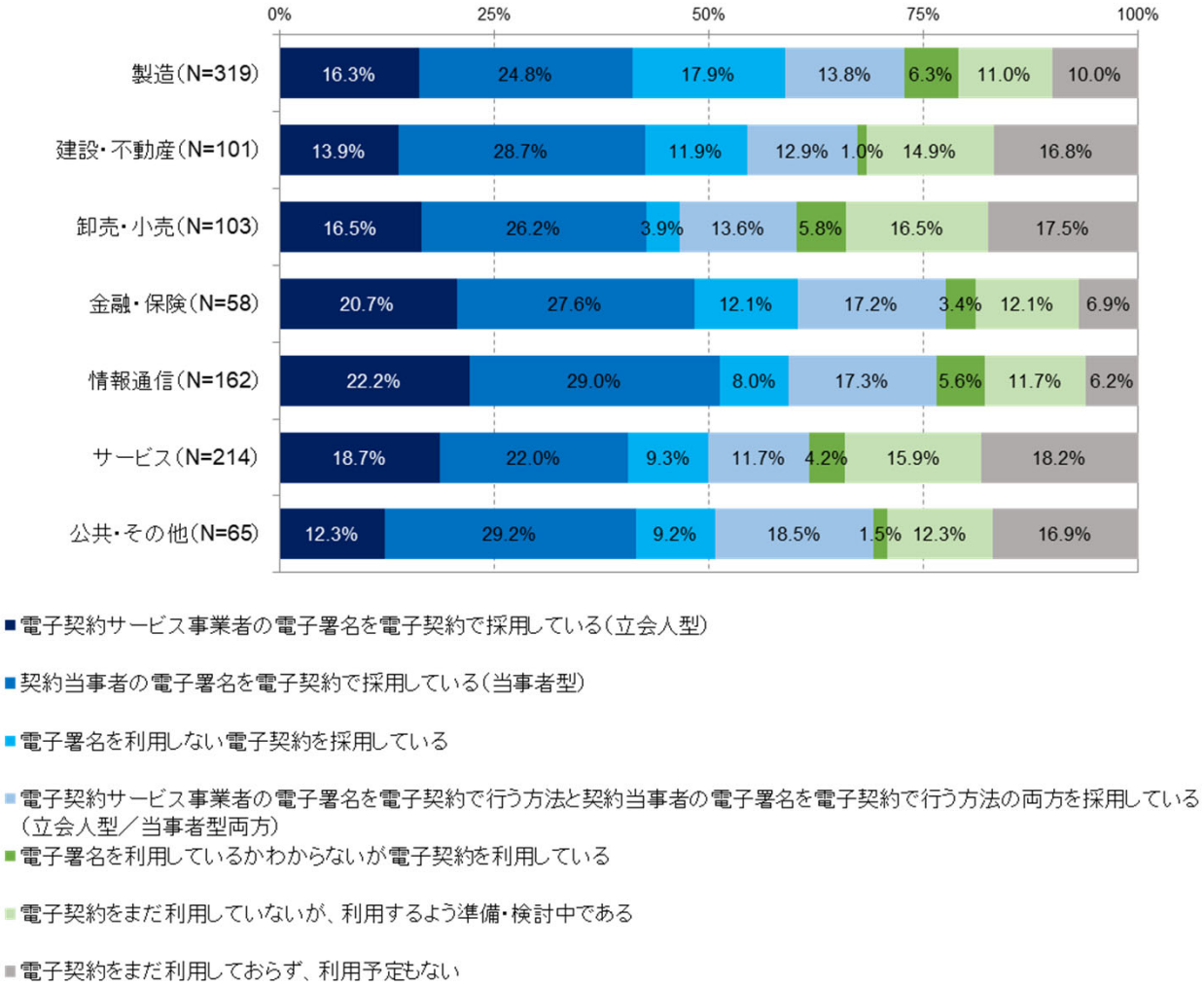
Q13_7：電子契約の利用状況（規模別）（2023年）

■ 小企業では、電子契約の利用率は約５割で、それ以上の企業の約８割を大きく下回る。



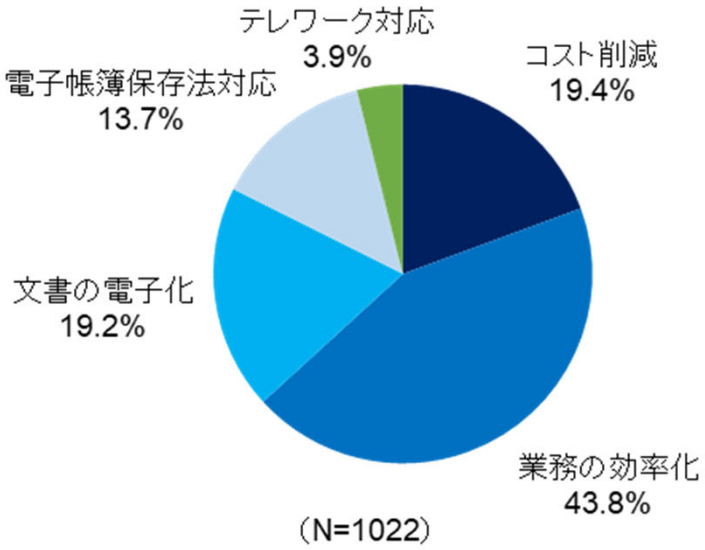
Q13_7：電子契約の利用状況（業種別）（2023年）

■ 業種別では、「金融・保険」、「情報通信」、「製造」で利用率が高く、内訳では全業種で「当事者型」が多い。



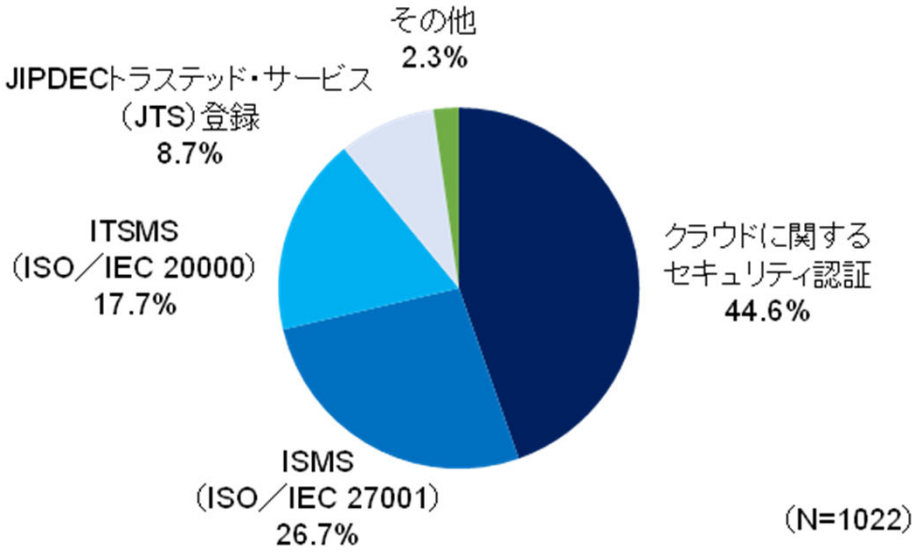
Q13_８：電子契約導入の目的（2023年）

■ 電子契約導入の目的としては、「業務の効率化」が約４割以上を占めトップ。「コスト削減」、「文書の電子化」が続く。



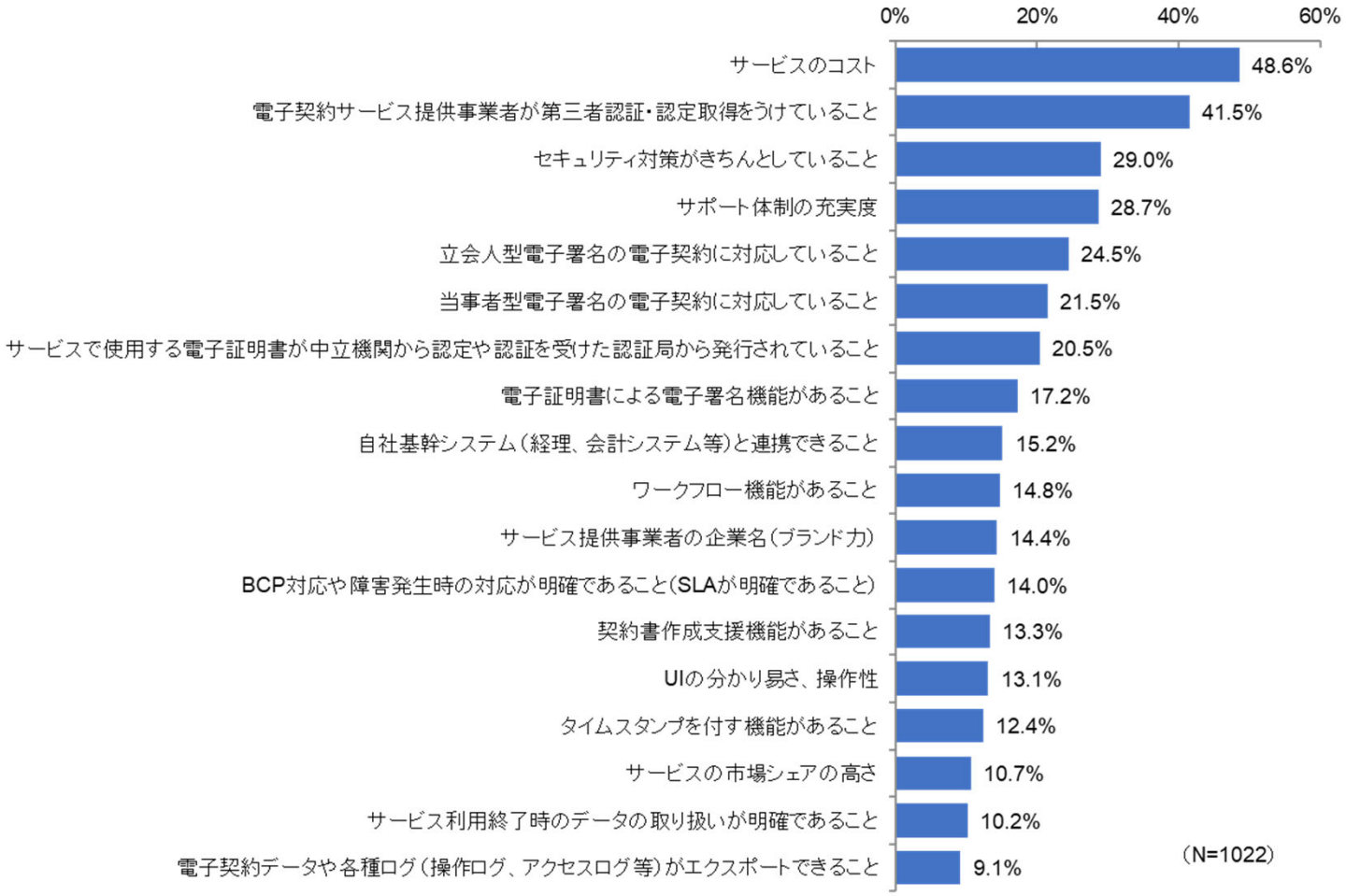
Q13_9：電子契約事業者を選定する場合の第三者認定・認証サービス（2023年）

■ 機密性の高いサービスでクラウドの利用が進む中で、「クラウドに関するセキュリティ認証」取得を参考にするとの回答が高い。



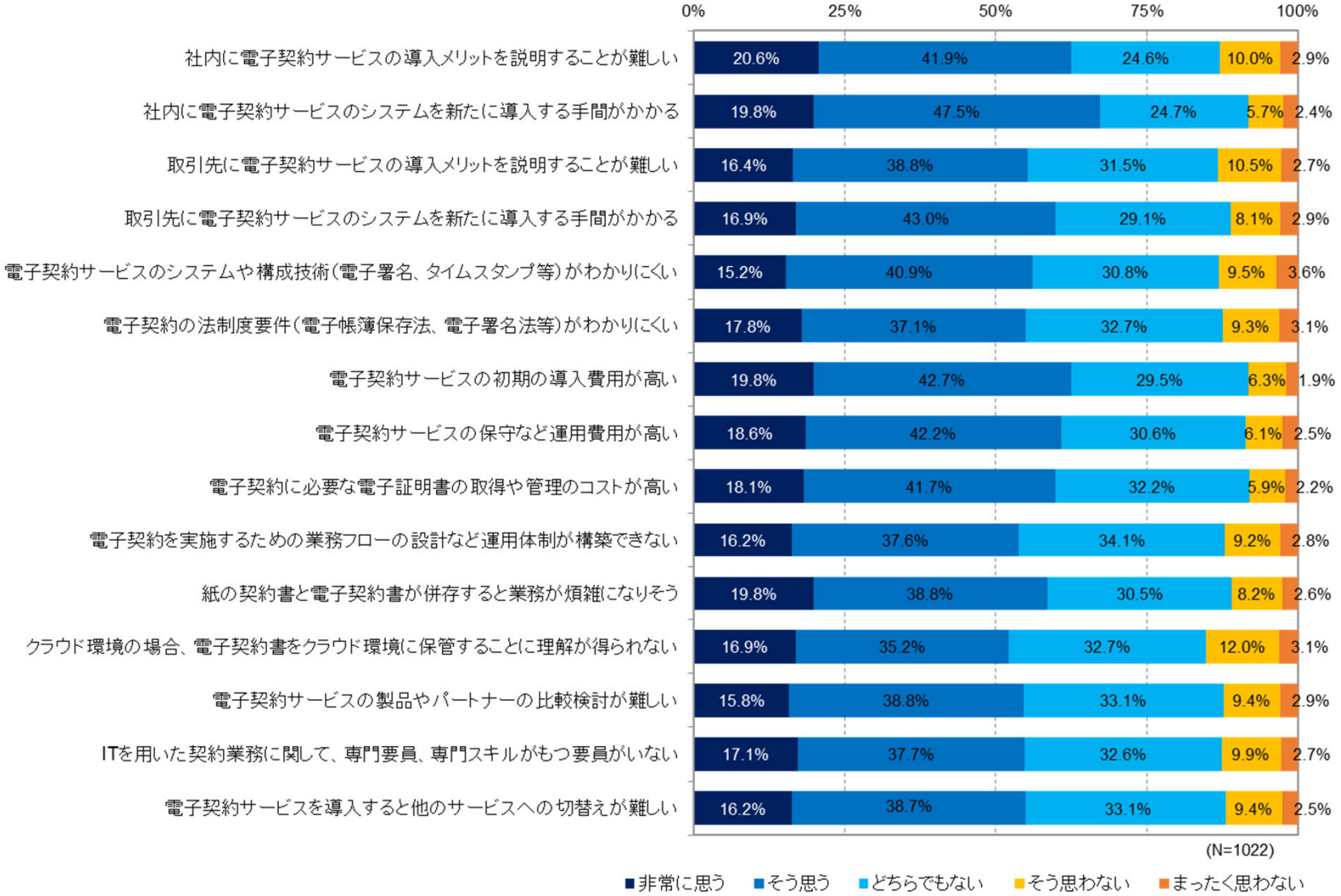
Q13_10：電子契約を選定する際に重視するポイント（2023年）

- 重視するポイントは「コスト」がトップで約５割。「第三者認証・認定を受けていること」、「セキュリティ対策」、「サポート体制」が続く。



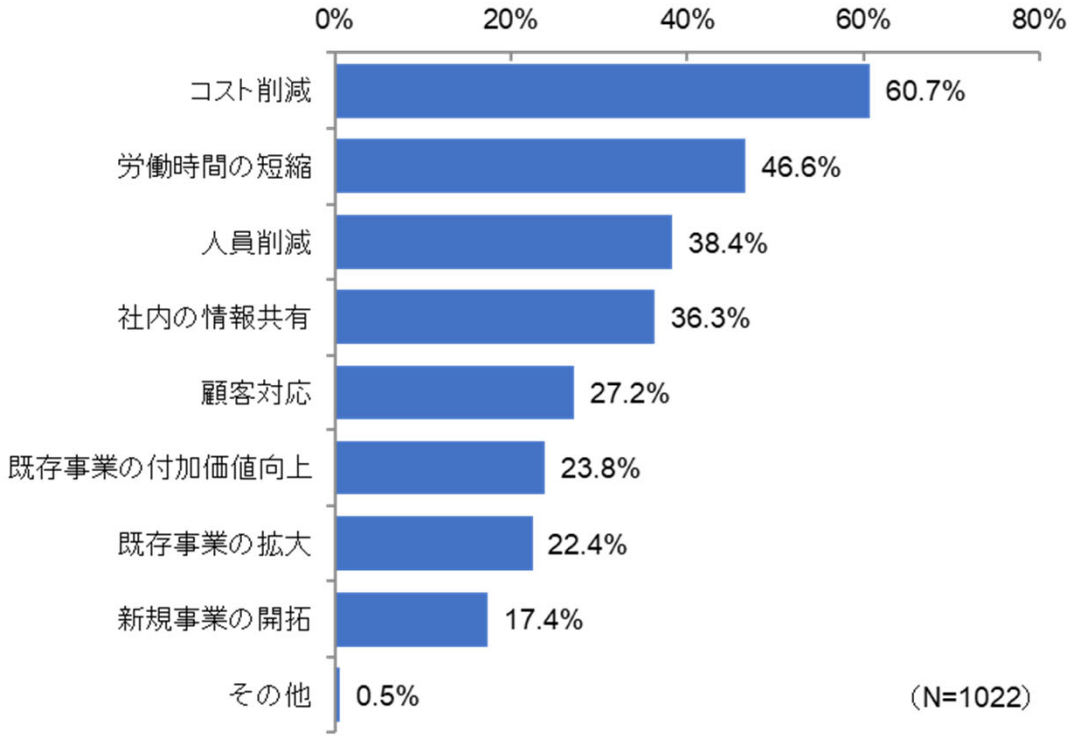
Q13_11：電子契約の利用拡大を図る上での課題（2023年）

- 利用拡大を図る上での課題として「そう思う」と「非常に思う」の合計が多いのは、「社内の導入の手間がかかる」が約７割でトップ。「導入のメリットの説明が難しい」、「初期導入コストが高い」が続く。



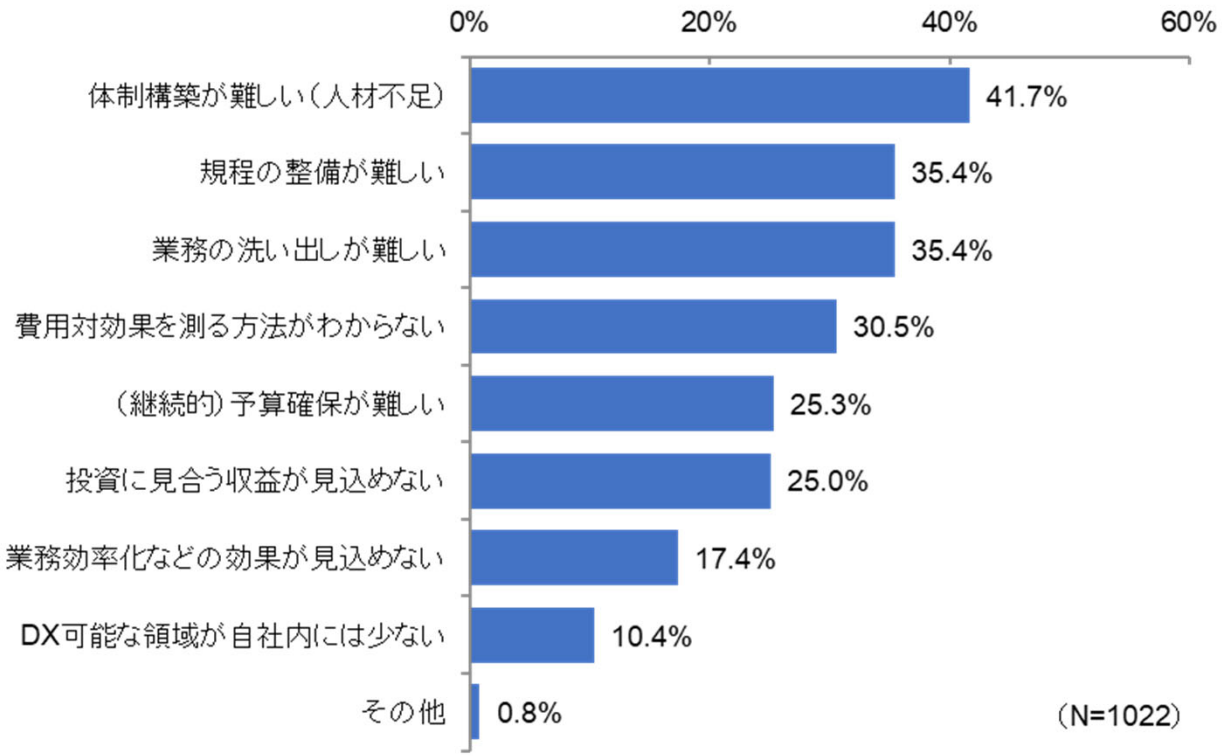
Q14_1：デジタルトランスフォーメーション（DX）の目的（2023年）

- DXの目的としては、「コスト削減」が最も多く約６割。「労働時間の短縮」、「人員削減」が続き、事業拡大というよりも事業の効率化の方が多い。



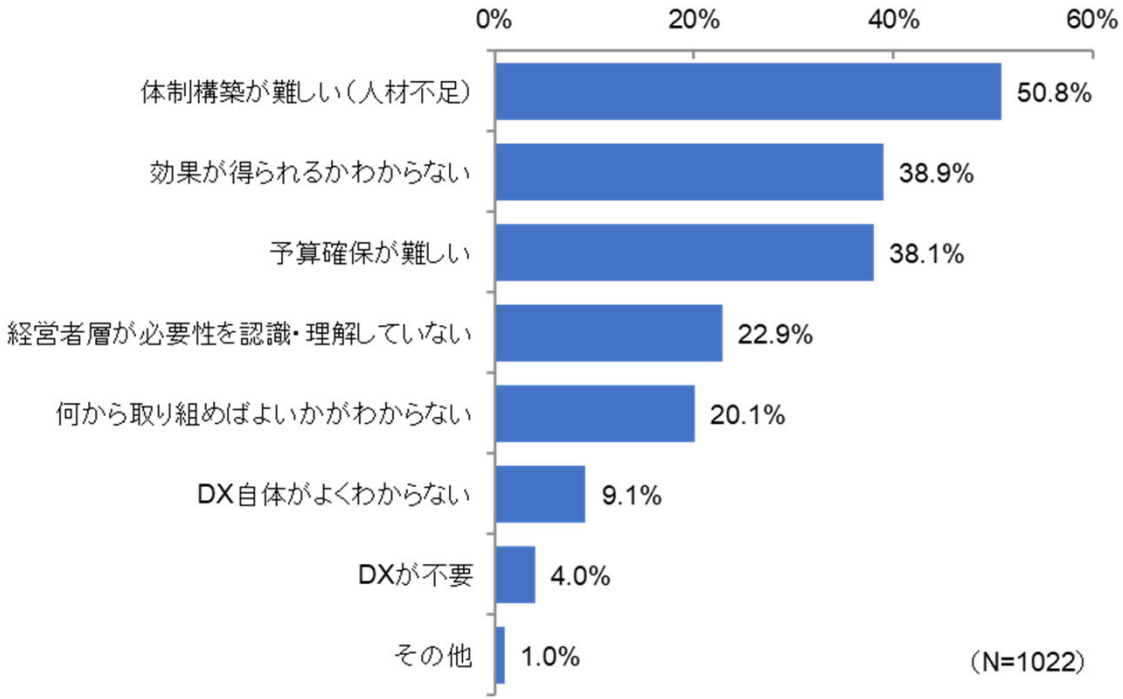
Q14_2：DXを推進するにあたっての課題（2023年）

- DX推進しようとしている企業の課題としては、「体制構築が難しい（人材不足）」が最も多く約４割、ついで「規程整備が難しい」、「業務の洗い出しが難しい」が続く。



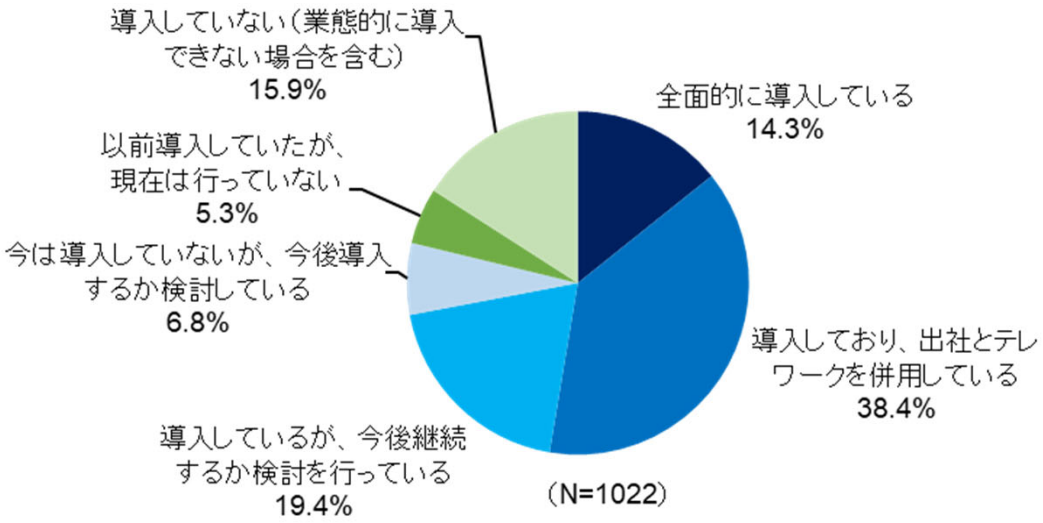
Q14_3：DXへの取り組みについての課題（2023年）

- DXを推進していない企業を含み、取り組みの課題としては「体制構築が難しい」、「効果が得られるかわからない」、「予算確保が難しい」、が３割を超えており、主な課題と言える。

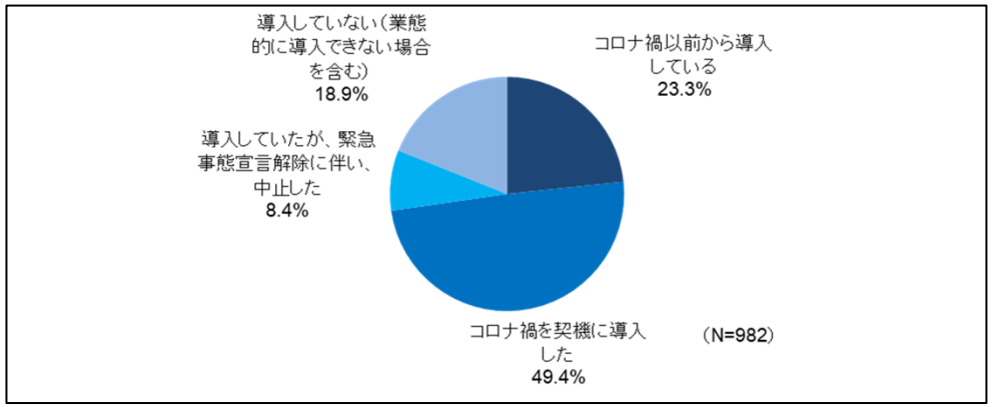


Q14_4：テレワークの導入状況（2023年）

- 併用や見直し検討中を含めるとテレワークの導入率は７割を超え、昨年と同レベルである。
  今後、新型コロナの状況によってテレワークの比率も変わっていくと思われる。



テレワーク導入状況（2022年）



総括・提言

テレワークやクラウド利用といった新しい作業環境が定着しつつあり、業務プロセスや働き方の変革が経営課題となりつつある。

セキュリティ面でも新たな作業環境・ワークスタイルに合わせたクラウドの情報漏洩対策・内部不正対策が必要とされてきている。

電子帳簿保存法やインボイス制度への対応が進み、電子契約は本格的に普及期に入ってきており、クラウド対応のセキュリティ認証が重要になっている。

DXについても、新たな作業環境・ワークスタイルを前提として、コスト・工数削減を目的とした取り組みがされているが、新たな環境に合わせた既存事業の拡大や新規事業の創出を進めることが望ましい。