

JIPDECセミナー

デジタルワークスタイル実現に向けた企業の IT利活用とセキュリティ対策の現状と課題 ～企業IT利活用動向調査2022報告～

2022年3月17日

禁無断転載

引用・転載をご希望の方は
JIPDEC引用・転載申請フォーム
から申請をお願いいたします。



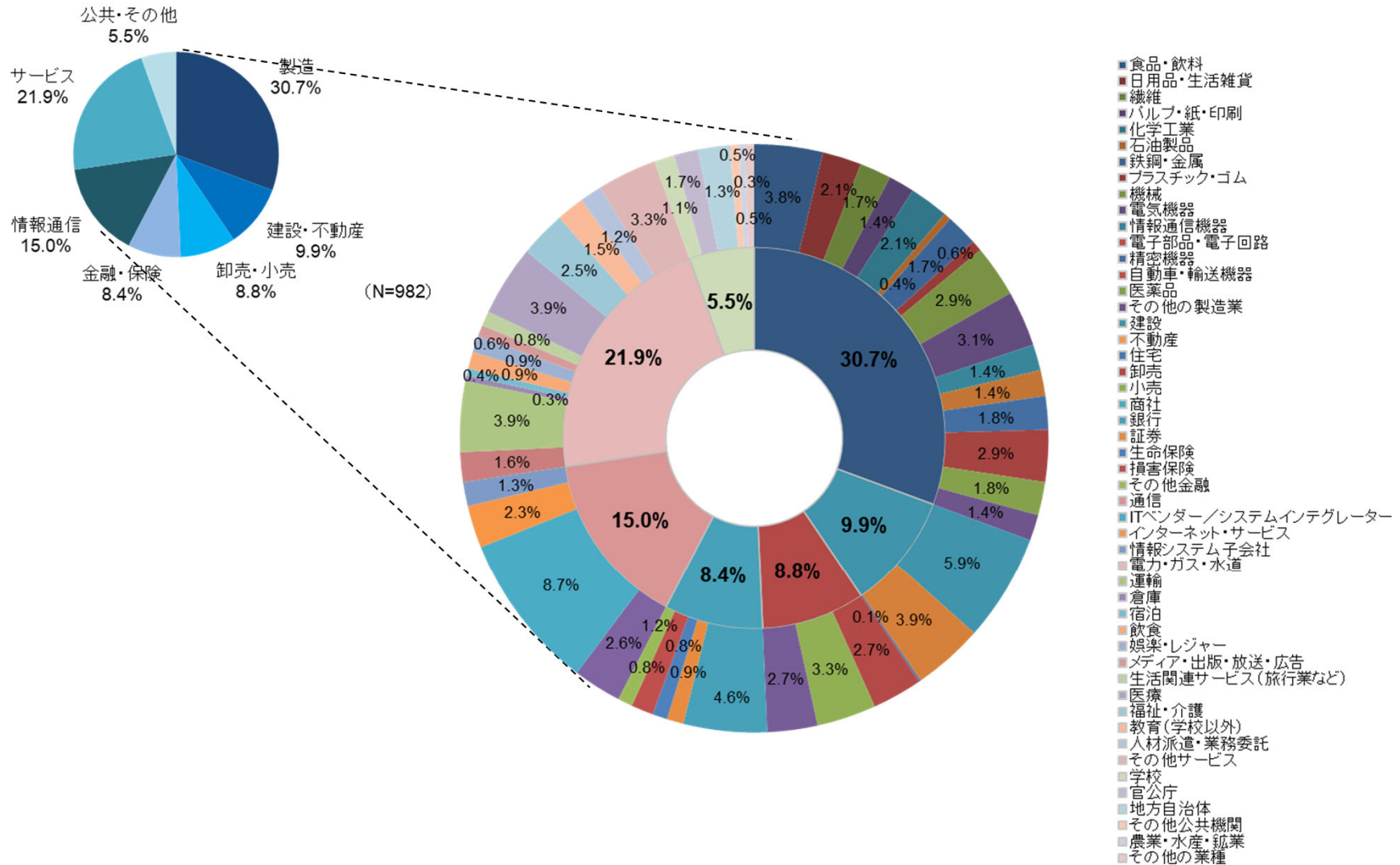
株式会社アイ・ティ・アール

調査概要

- 実査期間 : 2022年1月15日～1月17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14,000人**
- 従業員2名以上の国内企業の勤務者であること
(**今回から小規模事業者も対象に含めた**)
 - 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 : 982件 (1社1人)

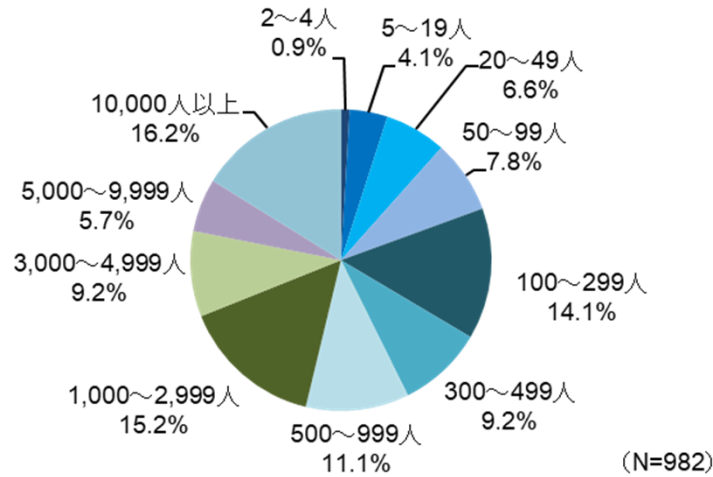
2022年調査：回答者プロフィール①

勤務先の業種

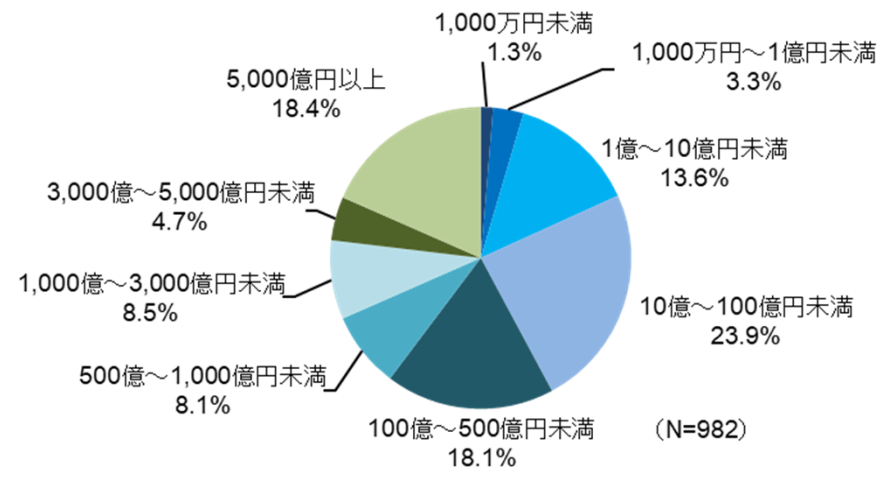


2022年調査：回答者プロフィール②

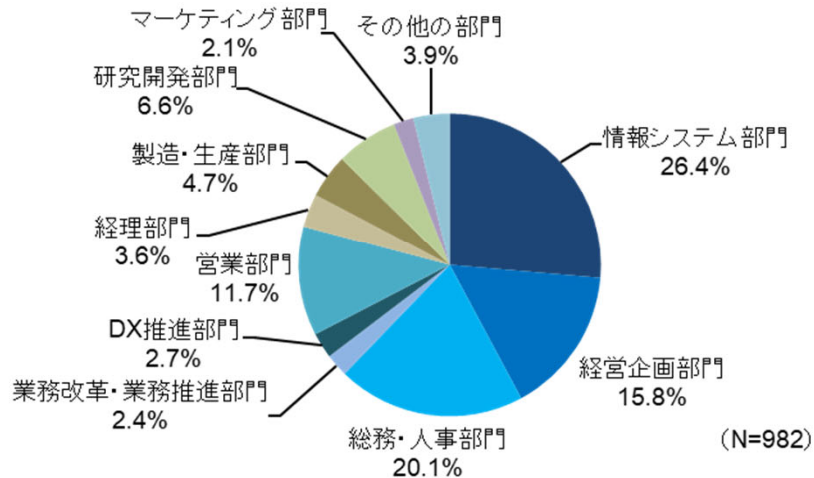
勤務先の従業員規模



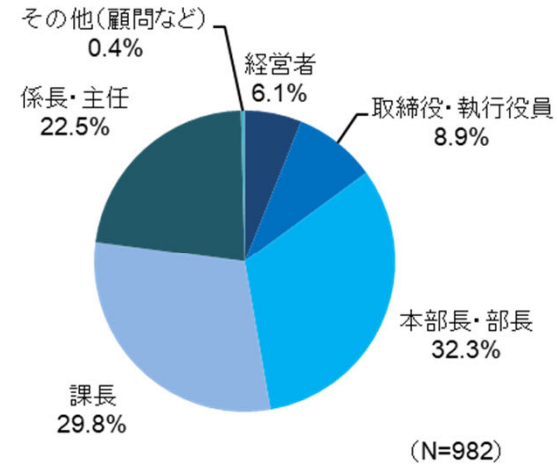
勤務先の売上規模



所属部門

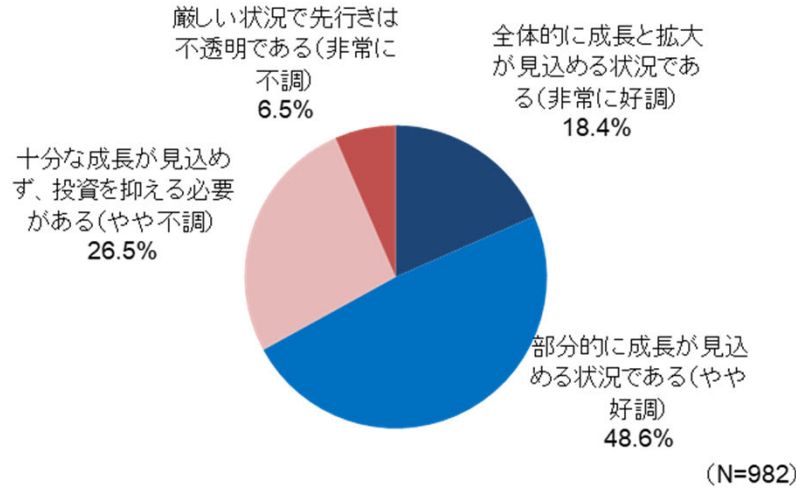


役職

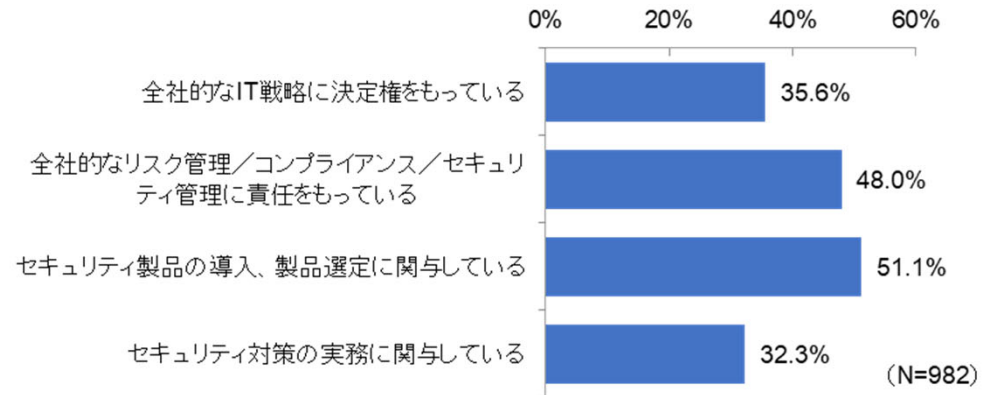


2022年調査：回答者プロフィール③

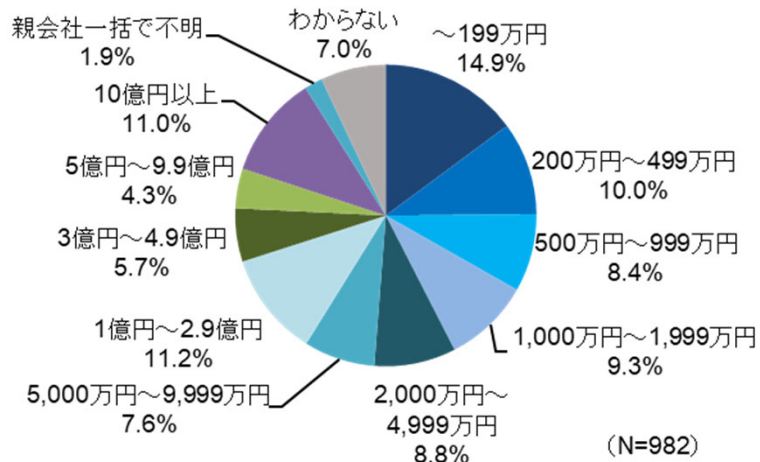
勤務先を取り巻くビジネス環境



IT戦略/セキュリティへの関与度

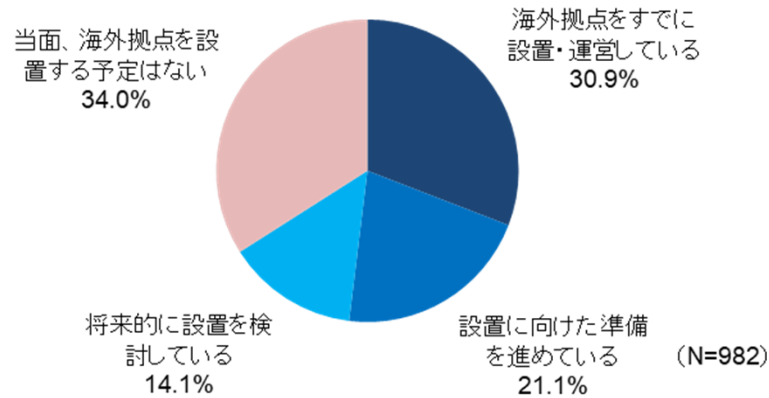


年間セキュリティ投資額

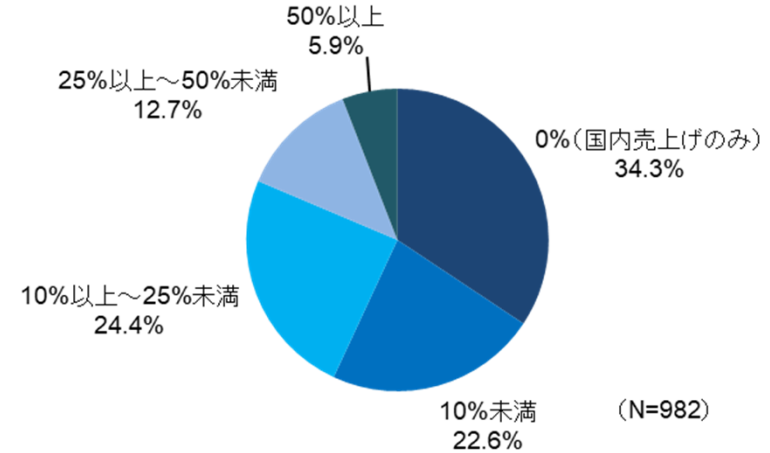


2022年調査：回答者プロフィール④

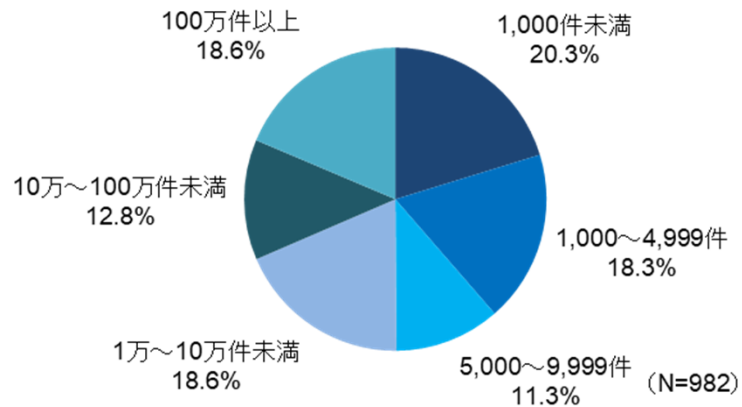
海外拠点の設置状況



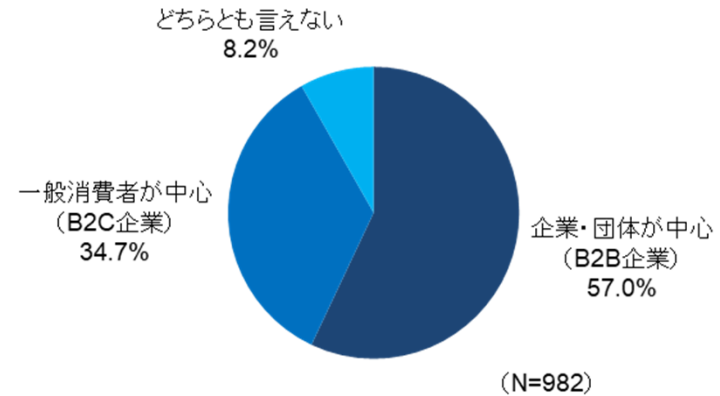
海外売上比率



個人情報保有件数



顧客・取引先のタイプ



全体の所見

経営課題とセキュリティ

- 長期間のコロナ禍に対応して企業において、社内組織の変革と共に新規事業の創出が新たな経営課題として認識されてきている。

認定／認証制度に対する意識

- 取引先や顧客から信頼を得るためにセキュリティの第三者認定／認証を取得・維持する傾向があるが、一方で維持のための工数・費用がかかるとの指摘も。

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教育の実施や個人情報保護システムの導入の比率が高く、セキュリティ技術動向ではクラウド対応サービスへの移行が進んでいる。

テレワークとクラウド化動向

- コロナ禍によりテレワークは勤務形態の7割超が採用しており、クラウドサービスも約9割が利用し、新たなデジタルワークスタイルが確立。

電子帳簿保存法・電子契約・DX推進

- 電子インボイスの対応はまだ定着していないが、電子契約は約7割が対応で定着してきている。またDXも取り組みは開始しているが成果はまだ出ていない企業が多い。

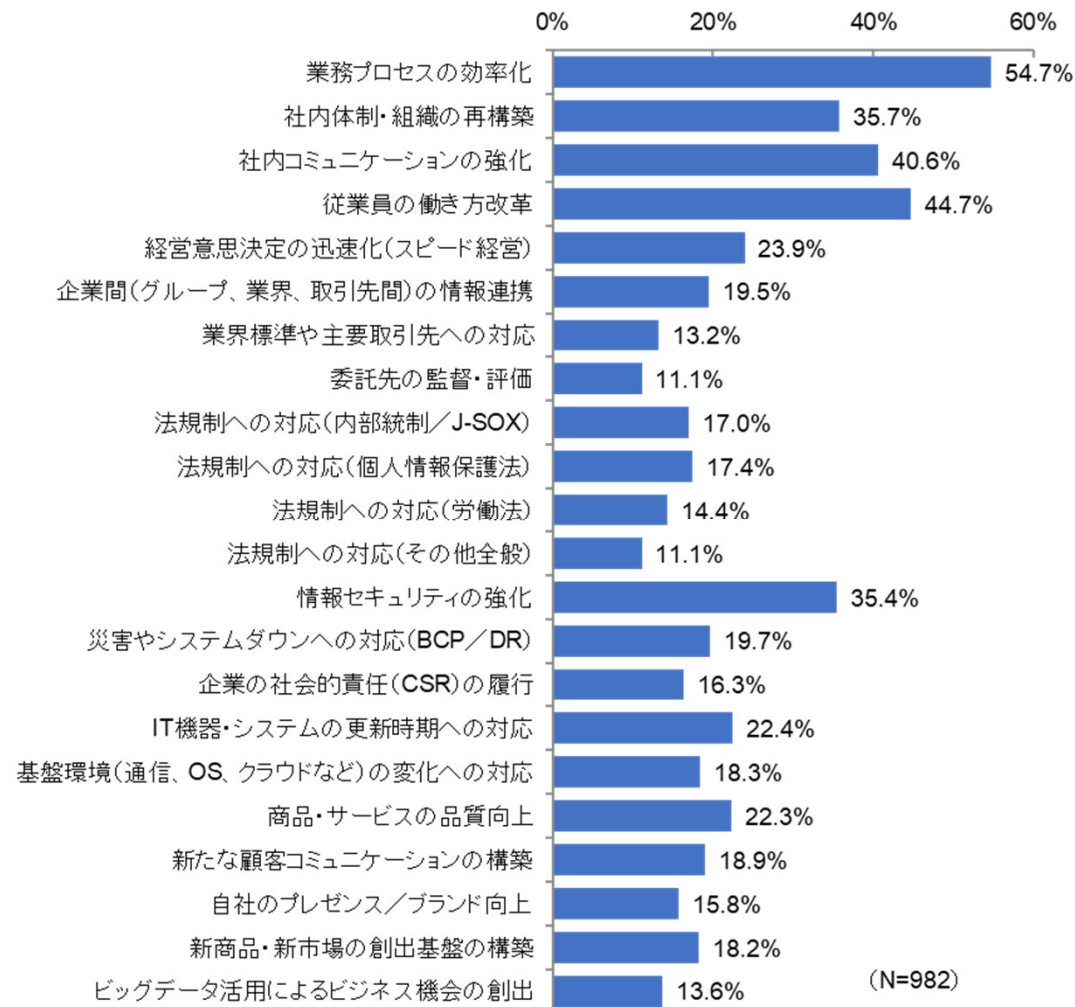
1) 経営課題におけるセキュリティの位置づけ

- 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（2022年調査）

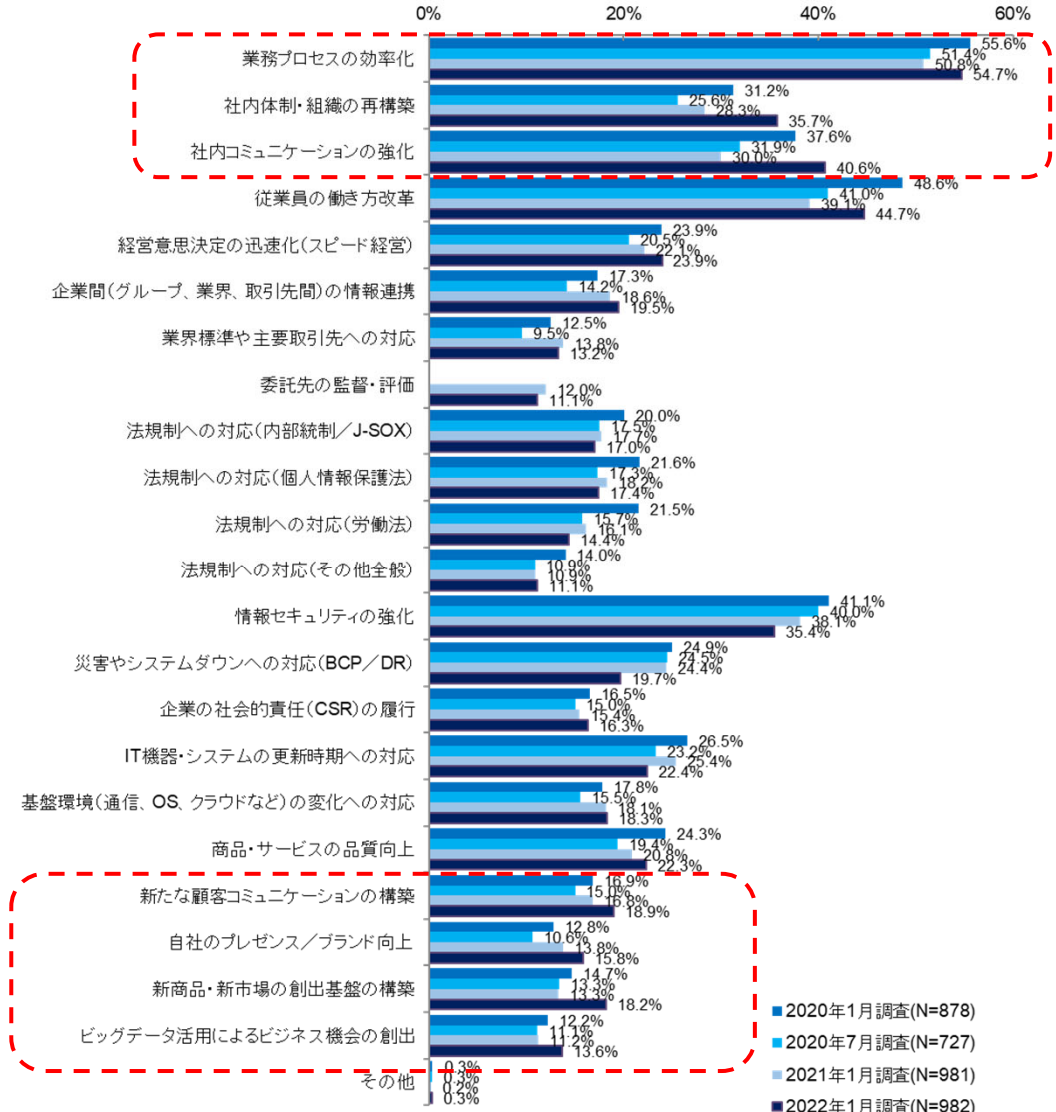
質問：あなたの勤務先において、以下の経営課題のうち、今後に向けて重視したいものは何ですか？

- 「業務プロセスの効率化」、「従業員の働き方改革」、「情報セキュリティの強化」の順で、大きな傾向の変化は見られない。



Q1：重視する経営課題（過去3回との比較）

■ 過去3回との比較では「社内体制・組織の再構築」や「社内コミュニケーションの強化」のような社内組織関連の変革と「顧客コミュニケーションの構築」や「自社プレゼンス/ブランド向上」、「新商品・新市場の創出基盤の構築」、「ビッグデータ活用によるビジネス機会の創出」のような新規事業創出・拡大が最も高くなっている。



Q1：重視する経営課題（2022年/業種別）

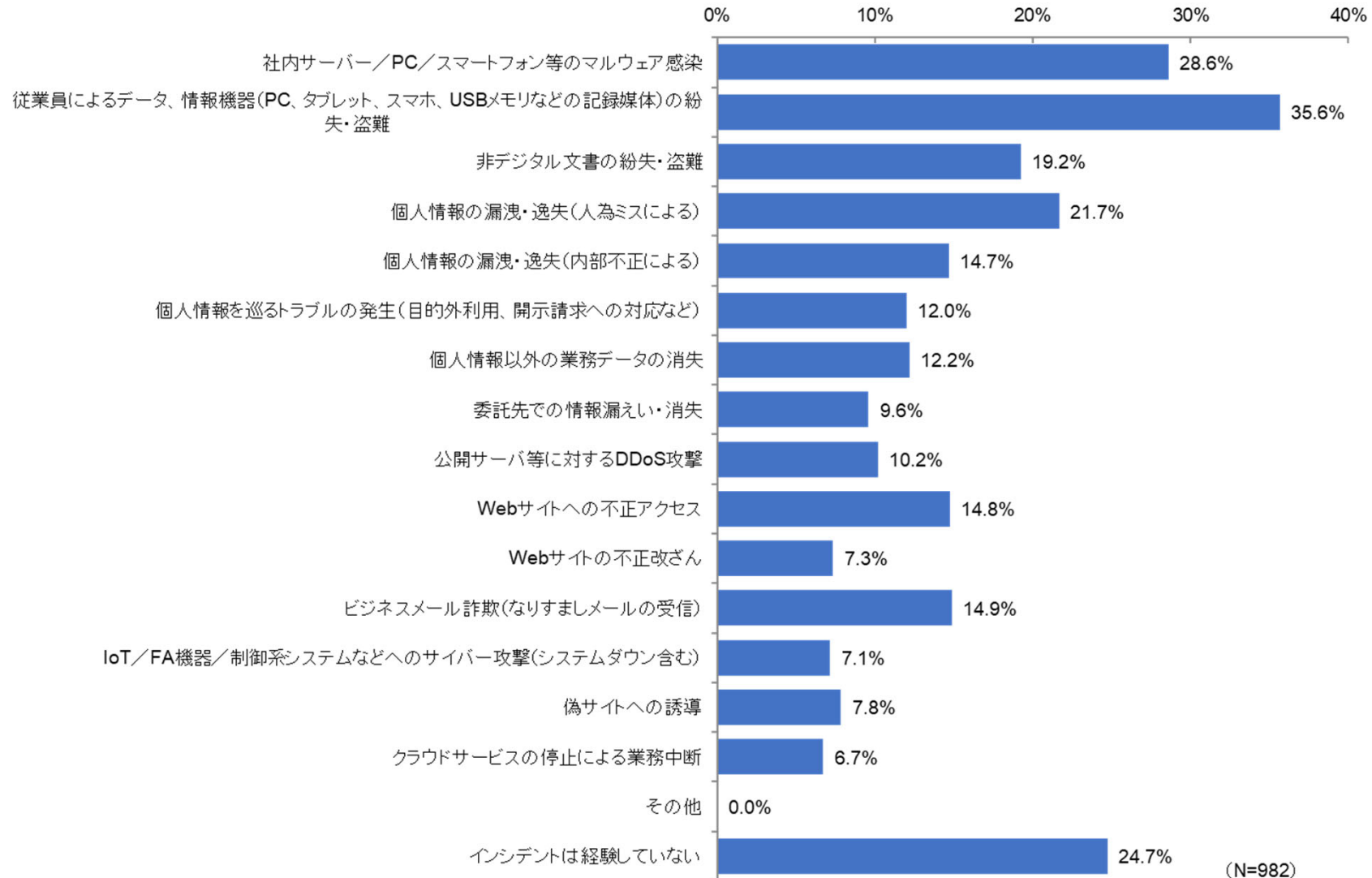
- 「金融・保険」では業務プロセスの他、セキュリティ&システム関連の課題が高くなっており、「卸売・小売」では、顧客拡大・新規事業創出関連の課題が高くなっている。また「建設・不動産」では社内組織体制・働き方関連の課題が高くなっている。

	製造 (N=301)	建設・不動産 (N=97)	卸売・小売 (N=86)	金融・保険 (N=82)	情報通信 (N=147)	サービス (N=215)	公共・その他 (N=54)	全体 (N=982)
業務プロセスの効率化	55.8%	57.7%	55.8%	61.0%	57.8%	47.0%	53.7%	54.7%
社内体制・組織の再構築	37.2%	43.3%	33.7%	37.8%	32.7%	33.0%	33.3%	35.7%
社内コミュニケーションの強化	42.2%	41.2%	38.4%	42.7%	42.2%	38.1%	37.0%	40.6%
従業員の働き方改革	40.9%	52.6%	44.2%	48.8%	40.1%	47.9%	46.3%	44.7%
経営意思決定の迅速化(スピード経営)	28.2%	24.7%	27.9%	22.0%	19.0%	21.4%	18.5%	23.9%
企業間(グループ、業界、取引先間)の情報連携	21.6%	19.6%	19.8%	20.7%	21.8%	15.8%	13.0%	19.5%
業界標準や主要取引先への対応	16.6%	13.4%	17.4%	8.5%	11.6%	10.7%	9.3%	13.2%
委託先の監督・評価	12.0%	11.3%	12.8%	13.4%	12.2%	7.9%	9.3%	11.1%
法規制への対応(内部統制/J-SOX)	18.9%	18.6%	17.4%	19.5%	14.3%	15.8%	11.1%	17.0%
法規制への対応(個人情報保護法)	16.9%	18.6%	14.0%	25.6%	19.0%	15.3%	14.8%	17.4%
法規制への対応(労働法)	12.3%	19.6%	17.4%	12.2%	12.2%	16.3%	13.0%	14.4%
法規制への対応(その他全般)	10.3%	12.4%	16.3%	12.2%	8.8%	10.2%	13.0%	11.1%
情報セキュリティの強化	35.2%	33.0%	30.2%	41.5%	40.1%	32.1%	40.7%	35.4%
災害やシステムダウンへの対応(BCP/DR)	21.6%	17.5%	19.8%	28.0%	16.3%	17.7%	16.7%	19.7%
企業の社会的責任(CSR)の履行	18.6%	19.6%	17.4%	19.5%	15.0%	12.1%	11.1%	16.3%
IT機器・システムの更新時期への対応	20.3%	15.5%	26.7%	29.3%	27.9%	20.9%	20.4%	22.4%
基盤環境(通信、OS、クラウドなど)の変化への対応	19.6%	17.5%	17.4%	17.1%	20.4%	16.3%	18.5%	18.3%
商品・サービスの品質向上	20.9%	17.5%	23.3%	23.2%	19.0%	27.9%	22.2%	22.3%
新たな顧客コミュニケーションの構築	16.6%	19.6%	25.6%	22.0%	17.0%	20.5%	14.8%	18.9%
自社のプレゼンス/ブランド向上	15.0%	12.4%	15.1%	15.9%	20.4%	15.3%	16.7%	15.8%
新商品・新市場の創出基盤の構築	22.3%	15.5%	23.3%	19.5%	14.3%	15.8%	11.1%	18.2%
ビッグデータ活用によるビジネス機会の創出	12.6%	14.4%	11.6%	14.6%	20.4%	11.6%	9.3%	13.6%
その他	0.0%	1.0%	0.0%	1.2%	0.0%	0.5%	0.0%	0.3%

Q2：過去1年間に経験したセキュリティ・インシデント（2022年調査）

質問：あなたの勤務先において、過去1年間に経験した情報セキュリティ・インシデントは何ですか？

- 従業員による紛失・盗難がトップで、マルウェア感染が2位となっており、大きな傾向に変化はない。



Q2：過去1年間に経験したセキュリティ・インシデント（2022年/業種別）

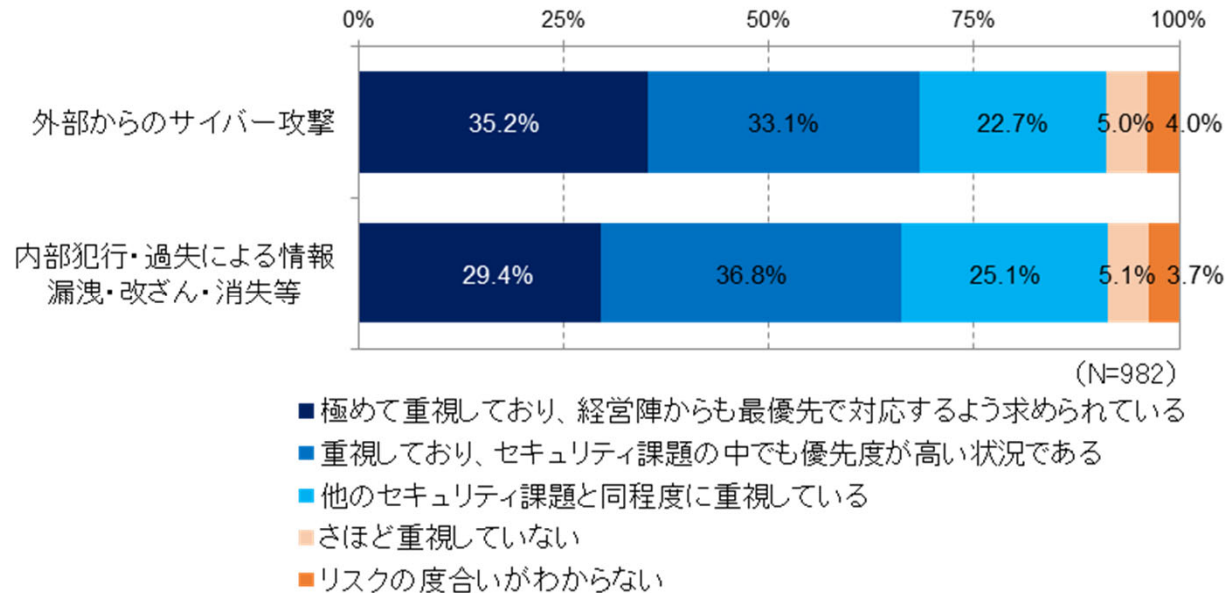
- 「金融・保険」では非デジタル文書の紛失・盗難と人為ミスによる個人情報の漏洩・逸失、ビジネスメール詐欺が増加、「公共その他」ではWEBサイトへの不正アクセス・改ざんと偽サイトへの誘導が増加している。

	製造 (N=301)	建設・不動産 (N=97)	卸売・小売 (N=86)	金融・保険 (N=82)	情報通信 (N=147)	サービス (N=215)	公共・その他 (N=54)	全体 (N=982)
社内サーバー／PC／スマートフォン等のマルウェア感染	35.2%	28.9%	27.9%	26.8%	25.2%	23.7%	24.1%	28.6%
従業員によるデータ、情報機器(PC、タブレット、スマホ、USBメモリなどの記録)	40.9%	37.1%	27.9%	36.6%	32.0%	32.1%	38.9%	35.6%
非デジタル文書の紛失・盗難	16.3%	25.8%	19.8%	29.3%	20.4%	15.8%	18.5%	19.2%
個人情報の漏洩・逸失(人為ミスによる)	18.6%	21.6%	17.4%	37.8%	21.8%	20.9%	24.1%	21.7%
個人情報の漏洩・逸失(内部不正による)	16.9%	13.4%	19.8%	8.5%	11.6%	14.4%	14.8%	14.7%
個人情報を巡るトラブルの発生(目的外利用、開示請求への対応など)	14.0%	10.3%	11.6%	14.6%	10.9%	8.8%	16.7%	12.0%
個人情報以外の業務データの消失	12.3%	14.4%	15.1%	12.2%	11.6%	9.8%	14.8%	12.2%
委託先での情報漏えい・消失	8.6%	7.2%	7.0%	13.4%	10.9%	10.2%	11.1%	9.6%
公開サーバー等に対するDDoS攻撃	10.0%	9.3%	7.0%	15.9%	12.9%	7.0%	14.8%	10.2%
Webサイトへの不正アクセス	17.3%	12.4%	12.8%	15.9%	17.0%	9.8%	20.4%	14.8%
Webサイトの不正改ざん	8.6%	7.2%	3.5%	8.5%	6.1%	6.0%	13.0%	7.3%
ビジネスメール詐欺(なりすましメールの受信)	16.9%	11.3%	16.3%	23.2%	14.3%	11.2%	11.1%	14.9%
IoT／FA機器／制御系システムなどへのサイバー攻撃(システムダウン含む)	12.0%	7.2%	4.7%	7.3%	4.8%	3.7%	3.7%	7.1%
偽サイトへの誘導	7.3%	5.2%	11.6%	6.1%	9.5%	5.6%	16.7%	7.8%
クラウドサービスの停止による業務中断	6.3%	6.2%	7.0%	7.3%	8.8%	4.7%	11.1%	6.7%
その他	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
インシデントは経験していない	16.9%	28.9%	32.6%	14.6%	25.9%	34.4%	22.2%	24.7%

Q3_1：セキュリティ・リスクの重視度合い（2022年）

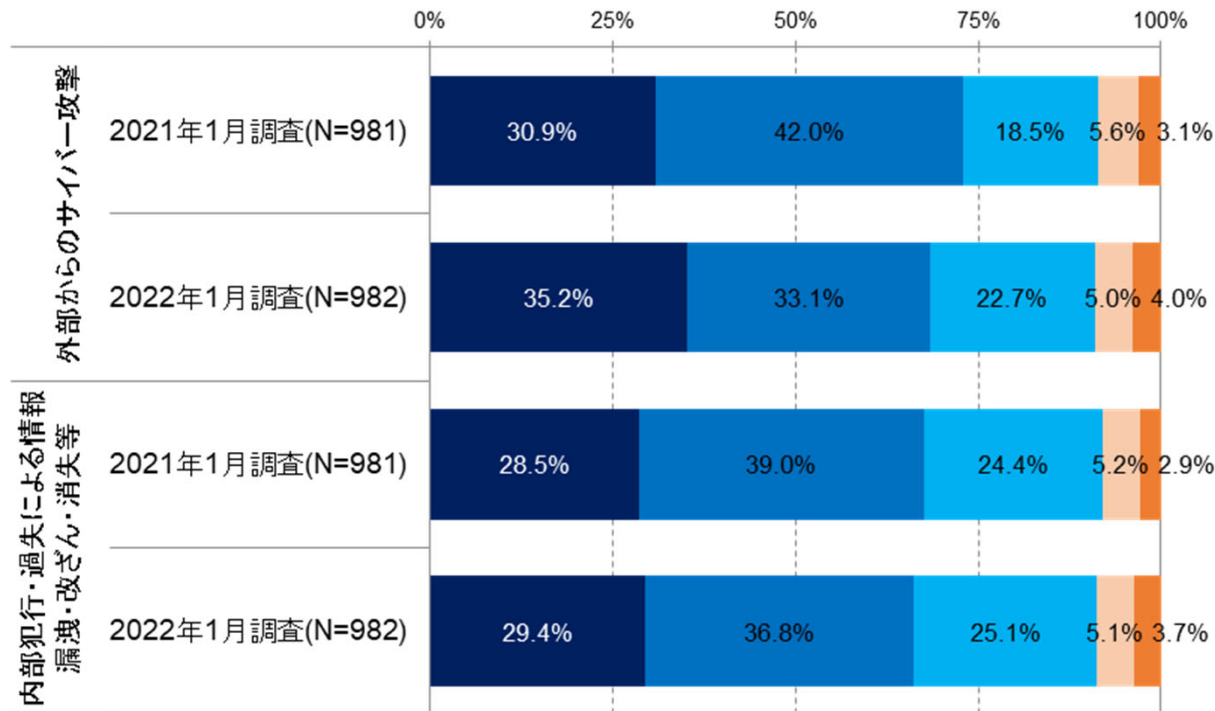
質問：あなたの勤務先において、以下の情報セキュリティ・リスクはどの程度重視されていますか？

- 「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」ともに重視しているが6割超となっている。特に「外部からのサイバー攻撃」を経営陣から最優先で対応するように求められているのは35%となっており、「内部犯行・過失による情報漏洩・改ざん・消失等」よりも高くなっている。



Q3_1 : セキュリティ・リスクの重視度合い (昨年との比較)

- 「外部からのサイバー攻撃」については、極めて重視しており経営陣からも最優先で対応するように求められている比率が増加している。

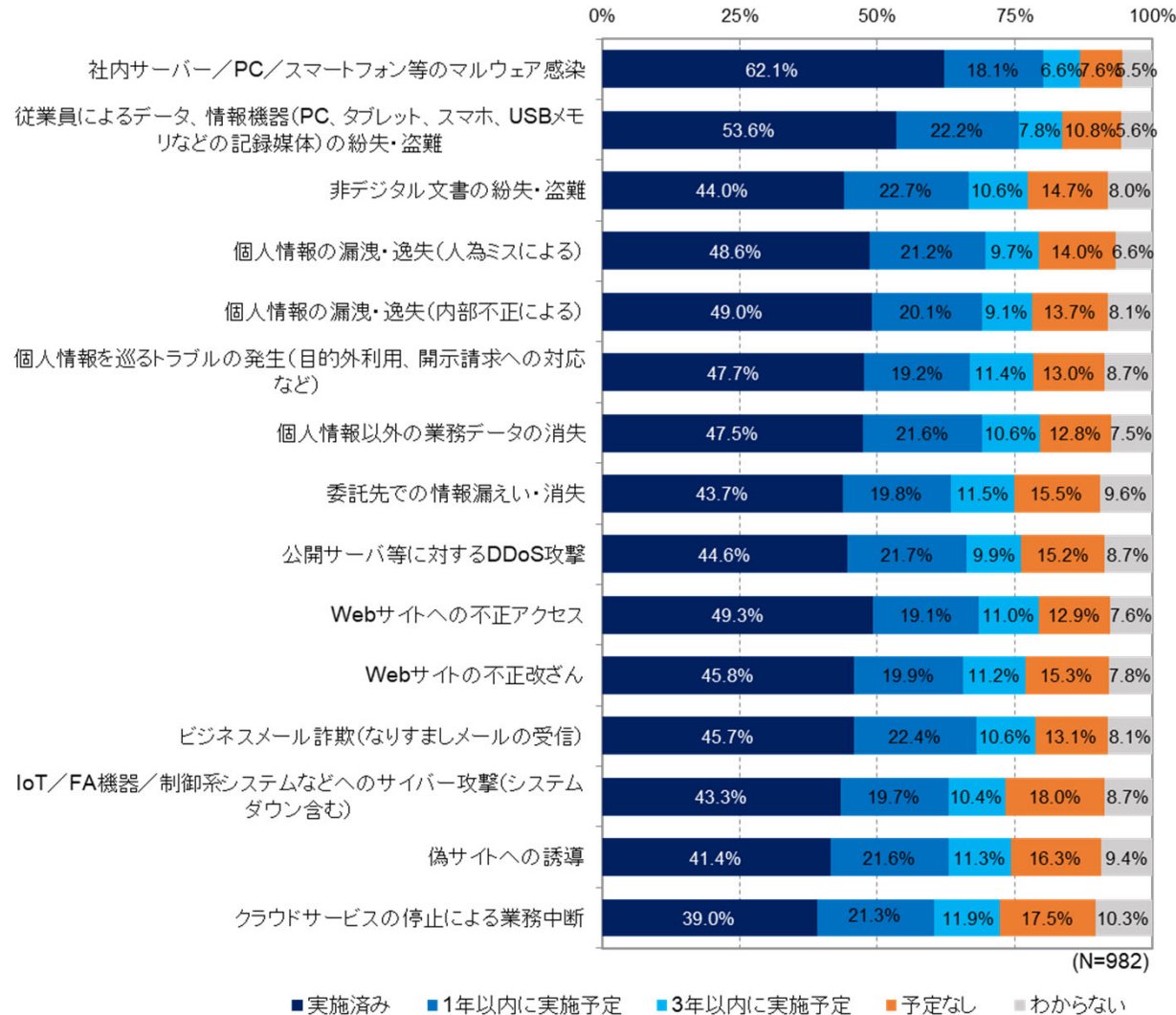


- 極めて重視しており、経営陣からも最優先で対応するように求められている
- 重視しており、セキュリティ課題の中でも優先度が高い状況である
- 他のセキュリティ課題と同程度に重視している
- さほど重視していない
- リスクの度合いがわからない

Q3_2：「外部からの攻撃対策」の実施状況（2022年）

質問：あなたの勤務先において、「外部からのサイバー攻撃対策」として実施しているものは、以下のうちどれですか？ また、今後実施を計画しているものはどれですか？

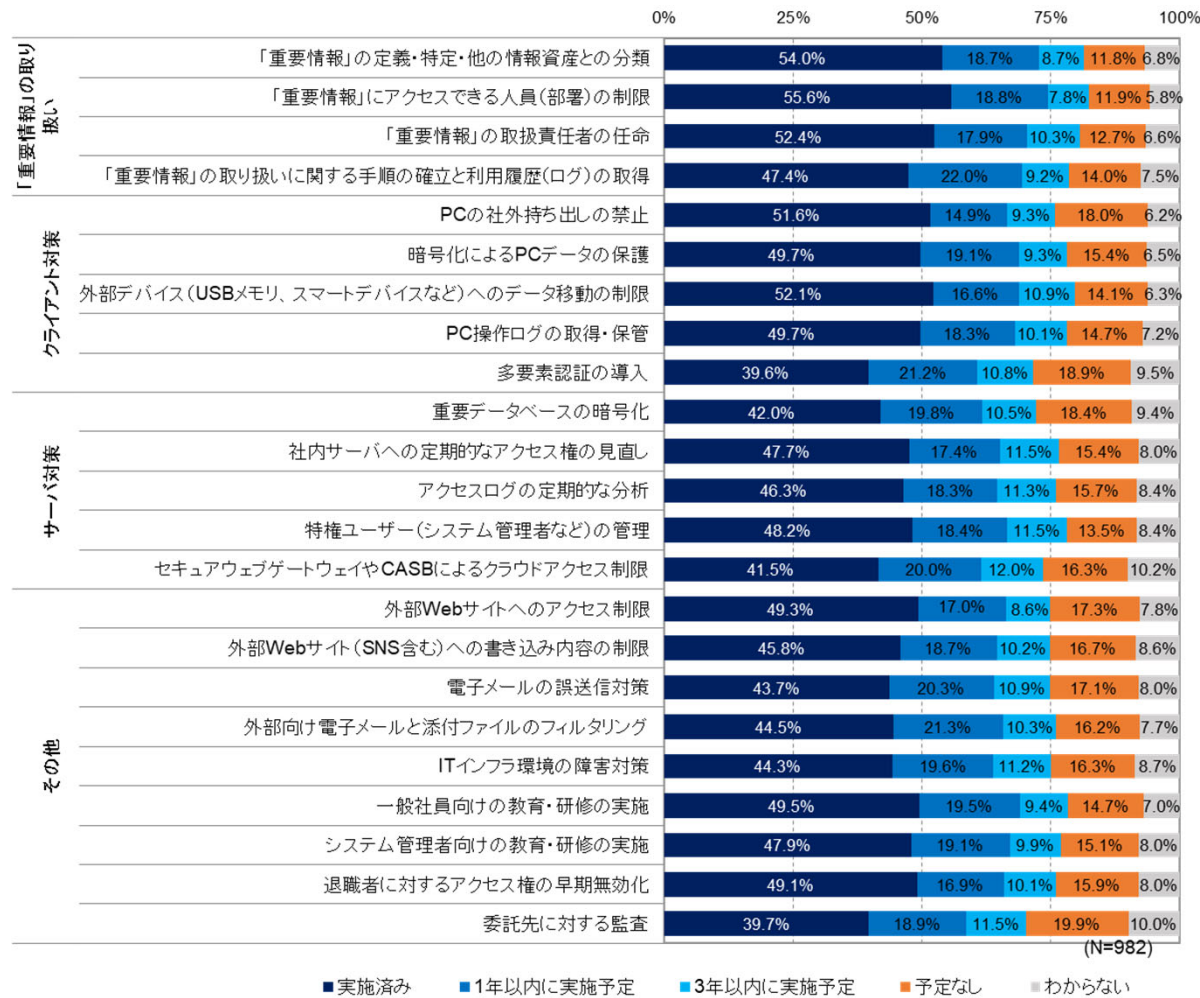
- 実施済の比率が高いのは、「マルウェア感染対策」で、次に「従業員のによる紛失・盗難対策」で5割を超えている。他の項目もほとんどが4割超である。



Q3_3 : 「情報漏洩対策」の実施状況 (2022年)

質問 : あなたの勤務先において、「内部犯行・過失対策」として実施しているものは、以下のうちどれですか？ また、今後実施を計画しているものはどれですか？

■ 実施済の比率が高いのは「重要情報の取り扱い」についての項目で、4項目中3項目が5割を超えている。次が「クライアント対策」で6項目中2項目が5割を超えている。



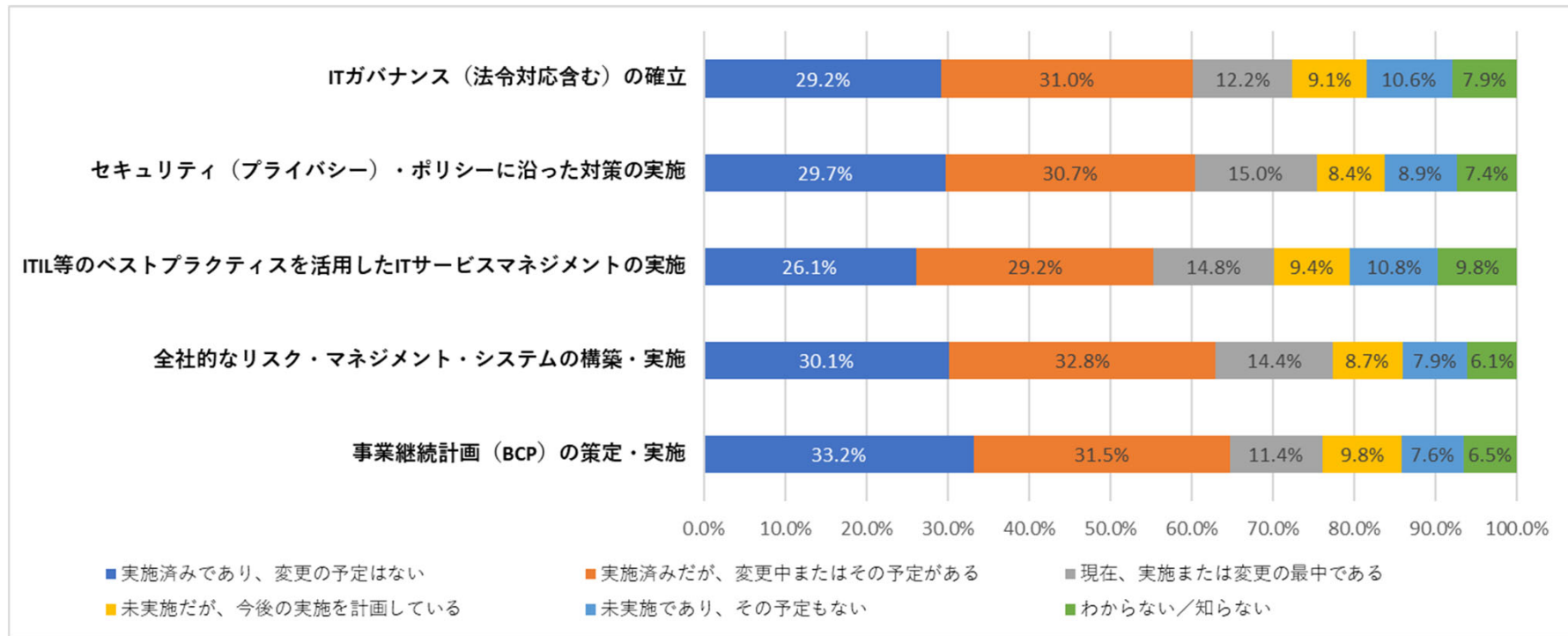
2) 認定／認証制度に対する意識

- 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 : 情報セキュリティの第三者認定／認証取得の価値（効果）
- Q4_4 : 取引選定時の認定／認証取得の重視度
- Q4_5 : 第三者認定／認証取得に消極的な理由

Q4_1：システムリスクの軽減策の取り組み状況（2022年）

質問：あなたの勤務先において、以下のテーマに対する取り組みの現状をお答えください。

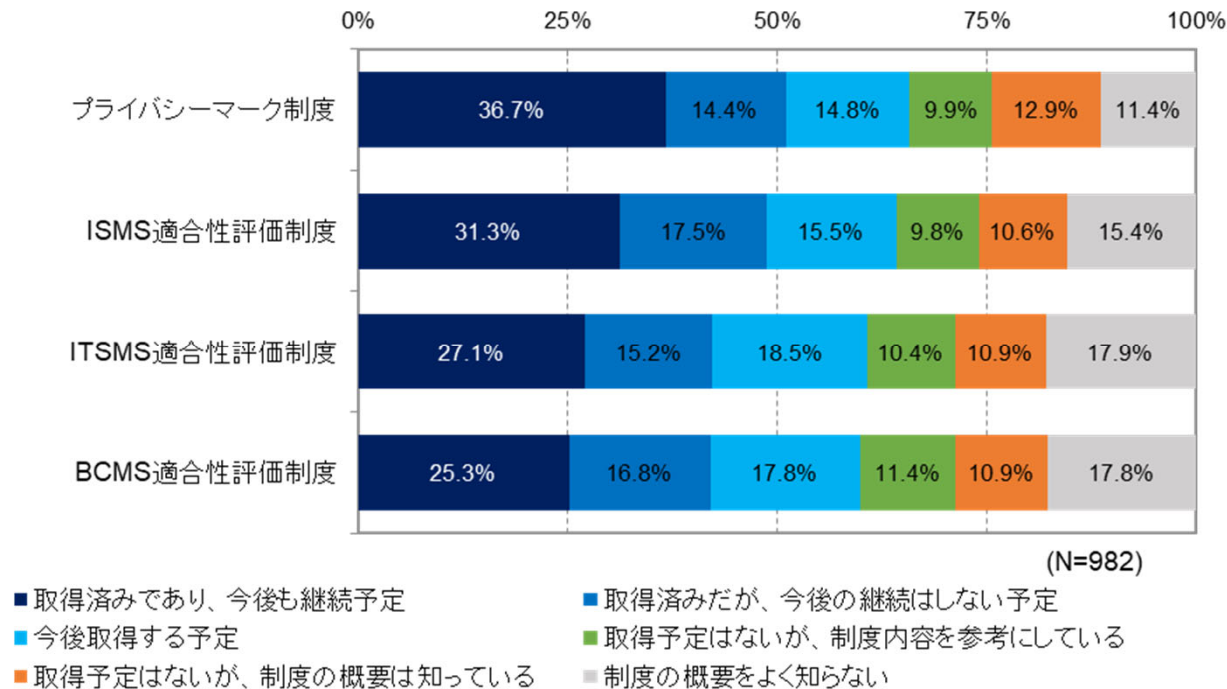
- 「ITサービスマネジメントの実施」以外は実施済が6割を超えて、かつ「ITサービスマネジメント」も6割に近づいており、全ての項目について半数が実施済になっている。



Q4_2：情報セキュリティ認定／認証制度への取り組み状況(2022年)

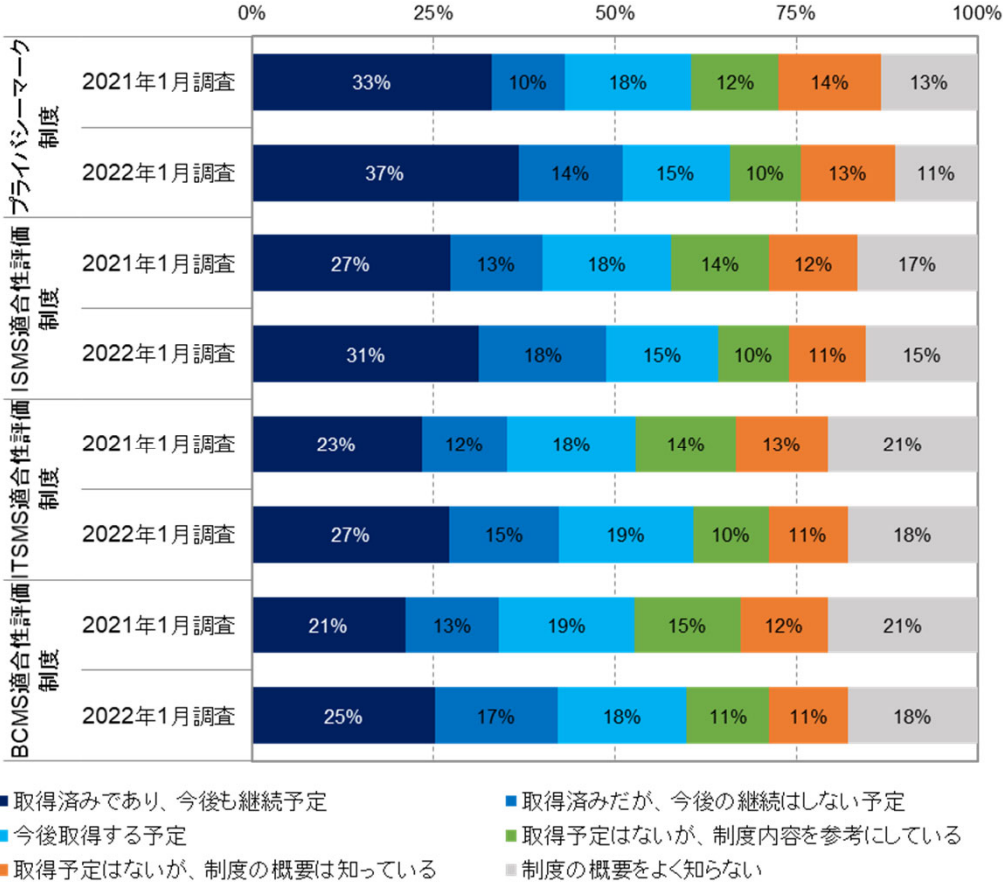
質問：情報セキュリティに関する以下の認定／認証制度に対して、あなたの勤務先の取り組み状況はどのようになっていますか？最も近いと思うものを1つずつお選びください。

- プライバシーマーク制度とISMS適合性評価制度は取得済が約 5 割、ITSMS適合性評価制度とBCMS適合性評価制度は約 4 割となっている。



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

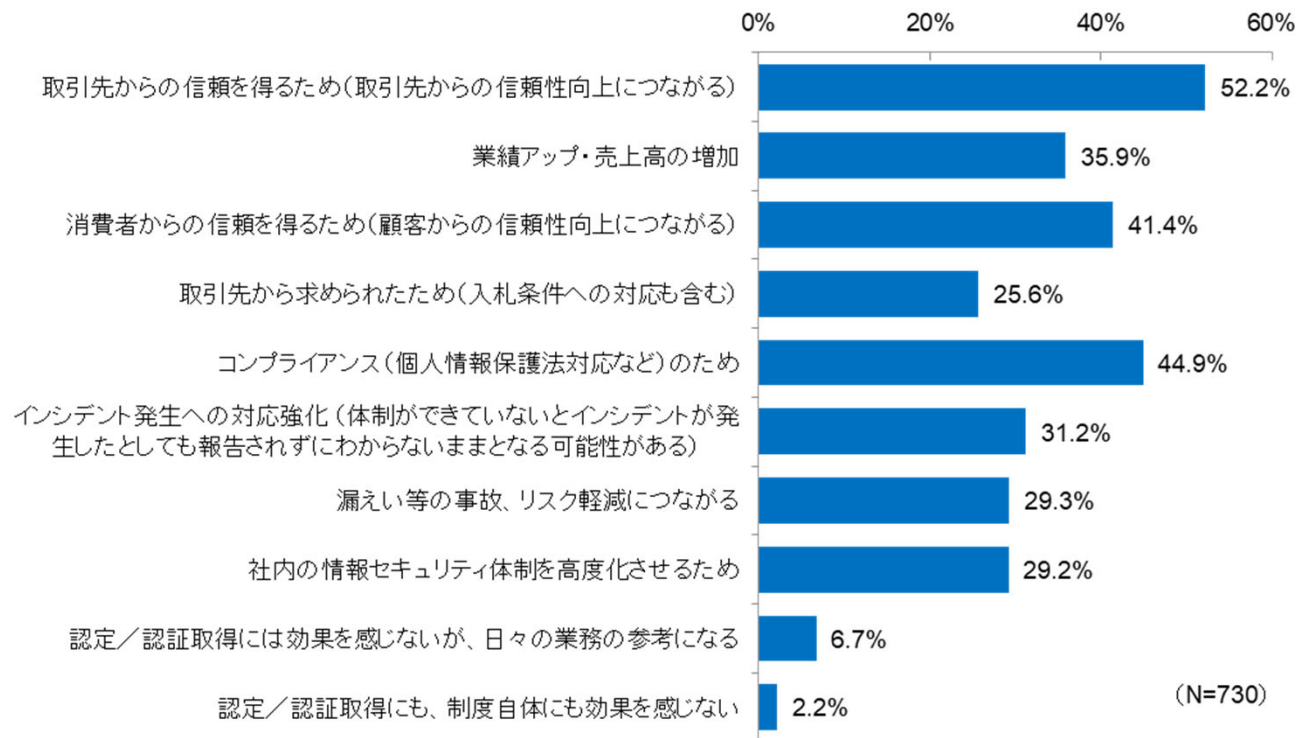
- 全ての認定／認証制度で取得済が増加している。
- 取得済で継続しないと今後取得予定が拮抗しており、取得率の伸びは鈍化するとと思われる。



Q4_3：情報セキュリティの第三者認定／認証取得の価値（効果）

質問：あなたの勤務先が第三者からの認定／認証を取得することの価値（効果）は何だとお考えですか？

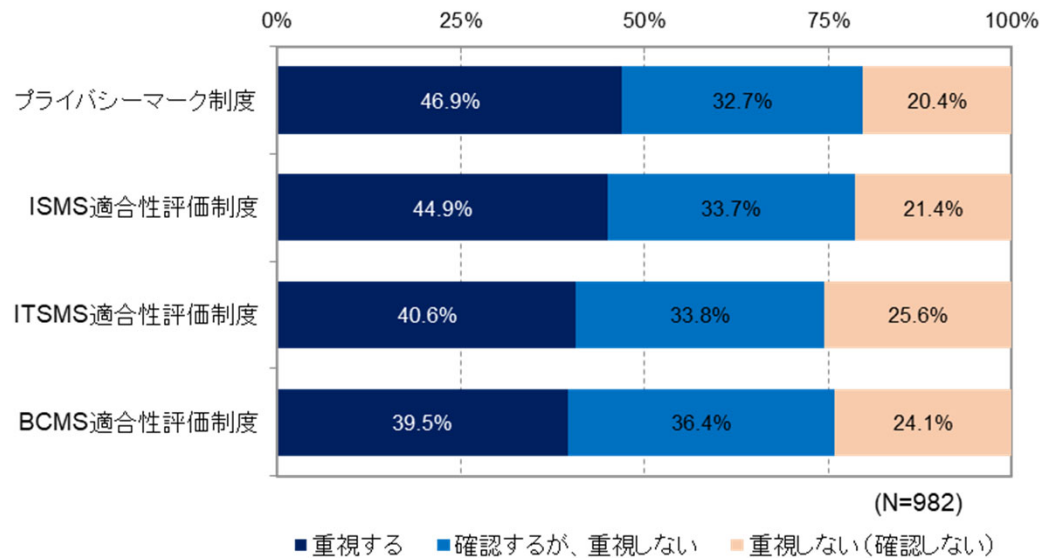
- トップは取引先からの信頼を得るため、続いてコンプライアンスのため、顧客からの信頼を得るためとなっており、対外的な理由が大きいことがわかる。



Q4_4：取引選定時の認定／認証取得の重視度(2022年)

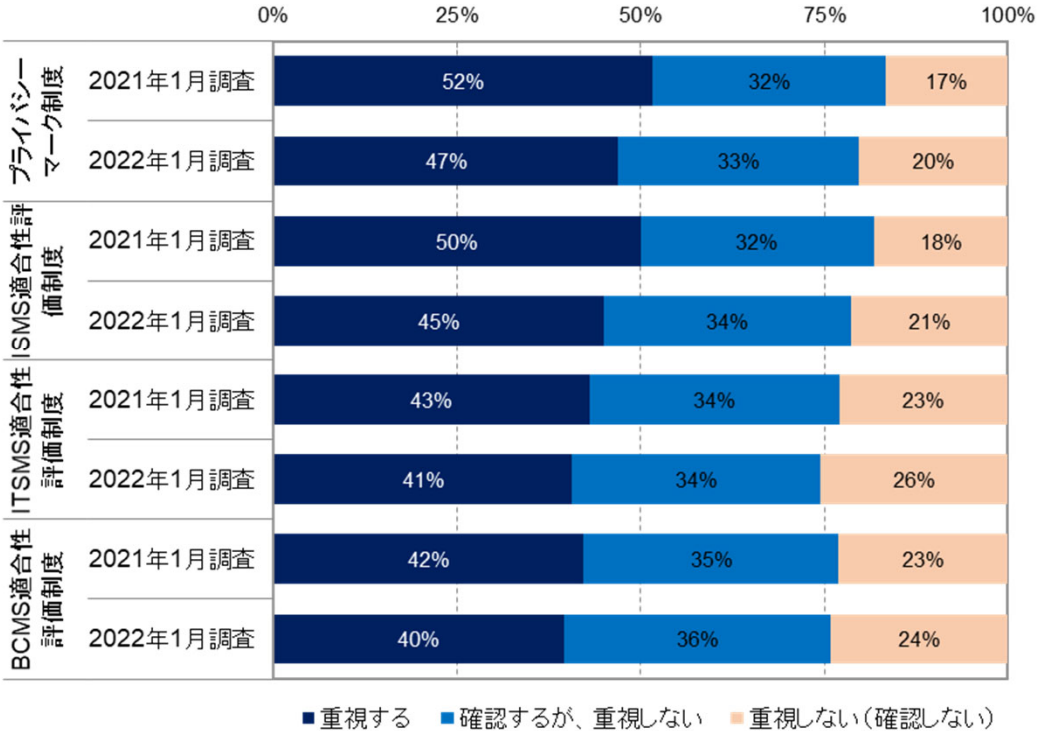
質問：あなたの勤務先では取引相手先を選定する際に以下の認定／認証制度を重視しますか？

- プライバシーマーク制度が約47%が重視するで最も高く、次いでISMS適合性評価制度が約45%、ITSMS適合性評価制度が約41%、BCMS適合性評価制度が約40%となっており、制度によって大きな差はないことがわかる。



Q4_4：取引選定時の認定／認証取得の重視度(昨年との比較)

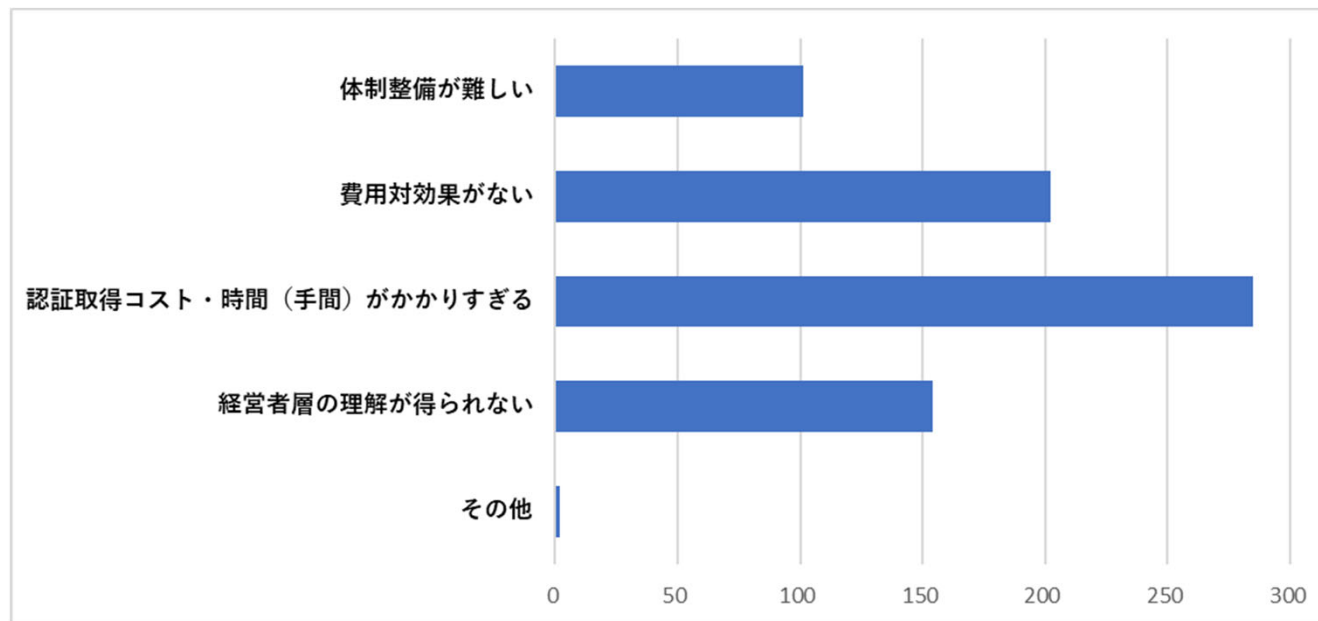
■ 前回と比較して大きな変化はないが、重視しないが若干増加している。



Q4_5：第三者認定／認証取得に消極的な理由(2022年)

質問：あなたの勤務先が第三者認証取得に消極的な理由は何ですか

- 取得に消極的な理由は、コスト・時間がかかりすぎるが最も多く、次いで費用対効果がないと回答されている。



3) セキュリティ支出の動向

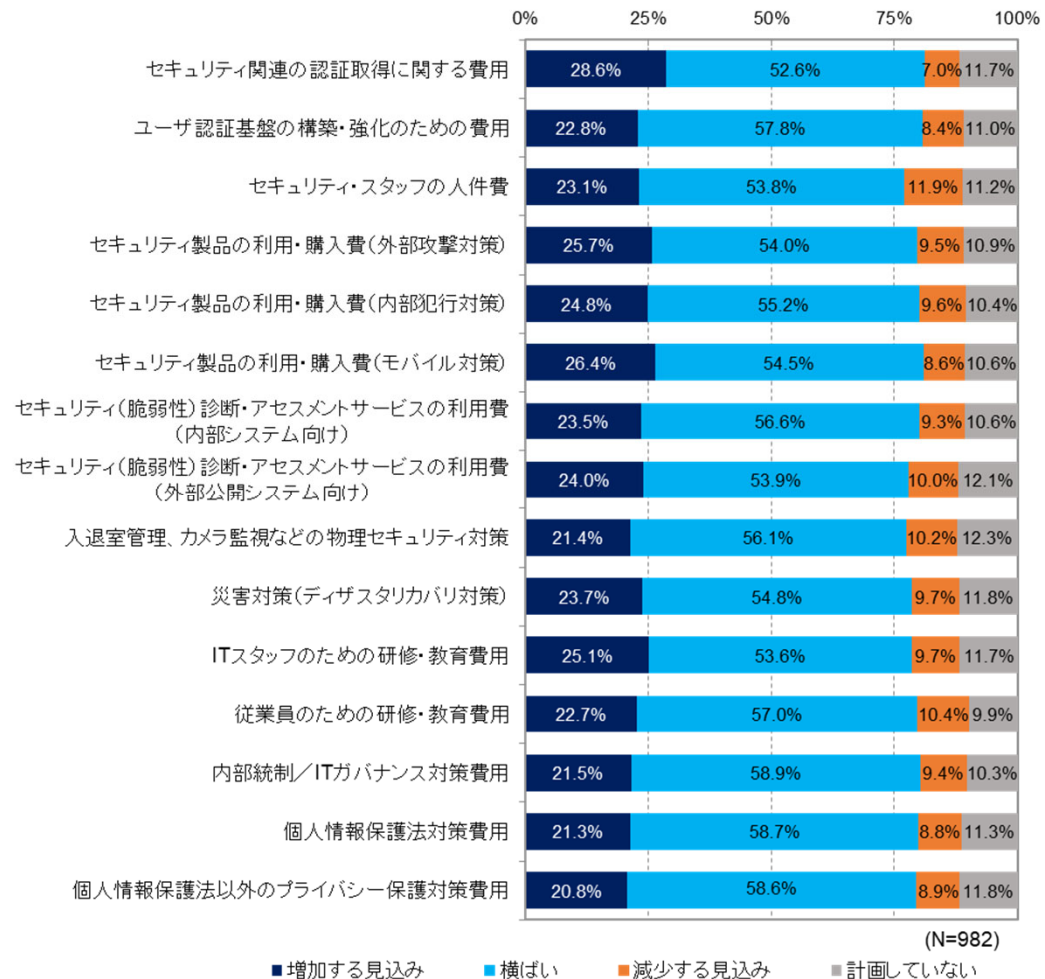
- Q5_1 : セキュリティ関連支出実績
- Q5_2 : セキュリティ関連支出の計画

Q5_1 : セキュリティ関連支出の実績 (2022年)

質問：以下の対策に対する2021年度の支出は、2020年度と比べてどのように変化する見込みですか？

それぞれについて、あてはまるものを1つずつお選びください。それぞれについて、あてはまるものを1つずつお選びください。

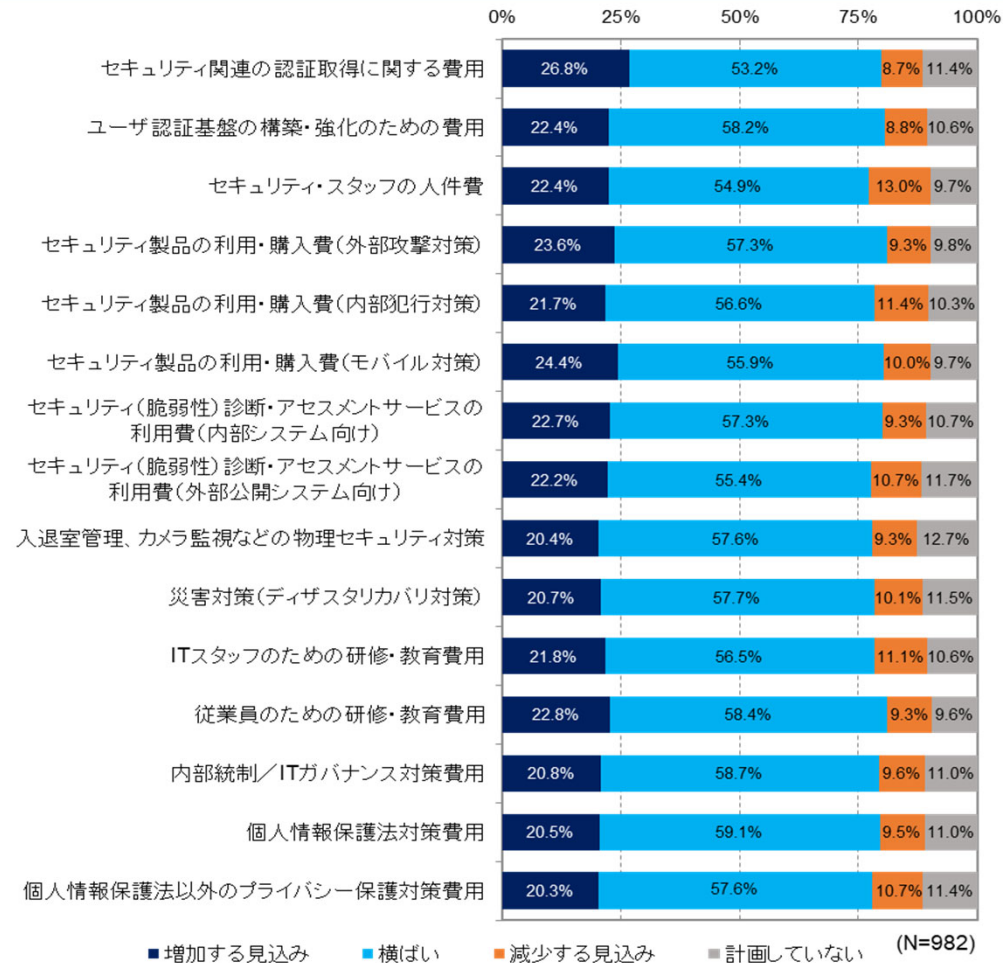
- 全ての支出項目において横ばいが5割を超えているが、増加と回答している比率も2割を超えている。特にセキュリティ関連の認証取得費用が増加と回答している比率が約3割と高くなっている。



Q5_2：セキュリティ関連支出の計画

質問：以下の対策に対する2022年度の支出予算は、2021年度と比べてどのように変化する見込みですか？それぞれについて、あてはまるものを1つずつお選びください。

- 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、実績と同様にセキュリティ関連の認証取得費用が高くなっている。



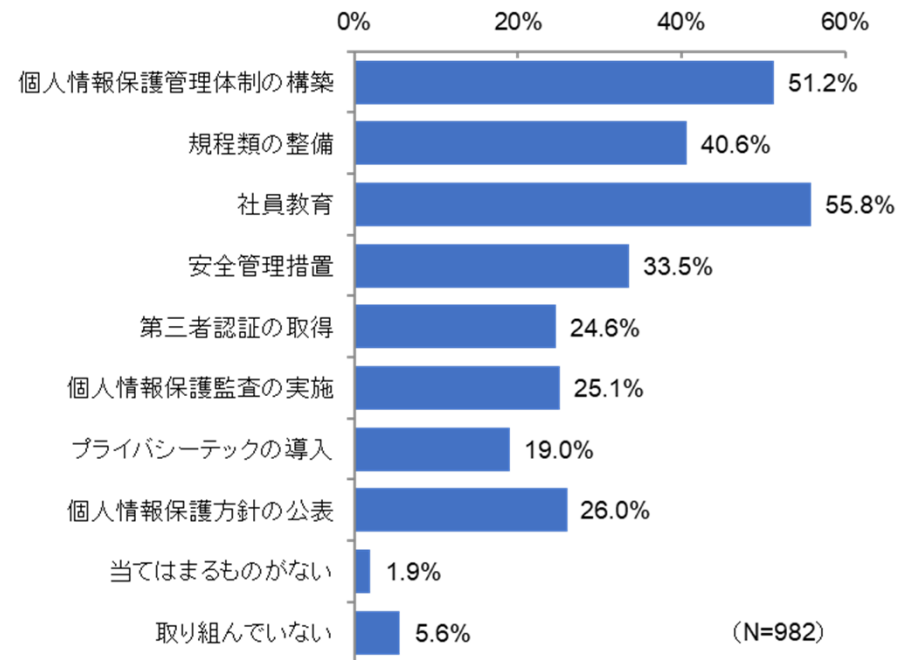
4) 個人情報保護

- 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(2022年)

質問：あなたの勤務先では個人情報保護についてどのような取り組みを行っていますか？

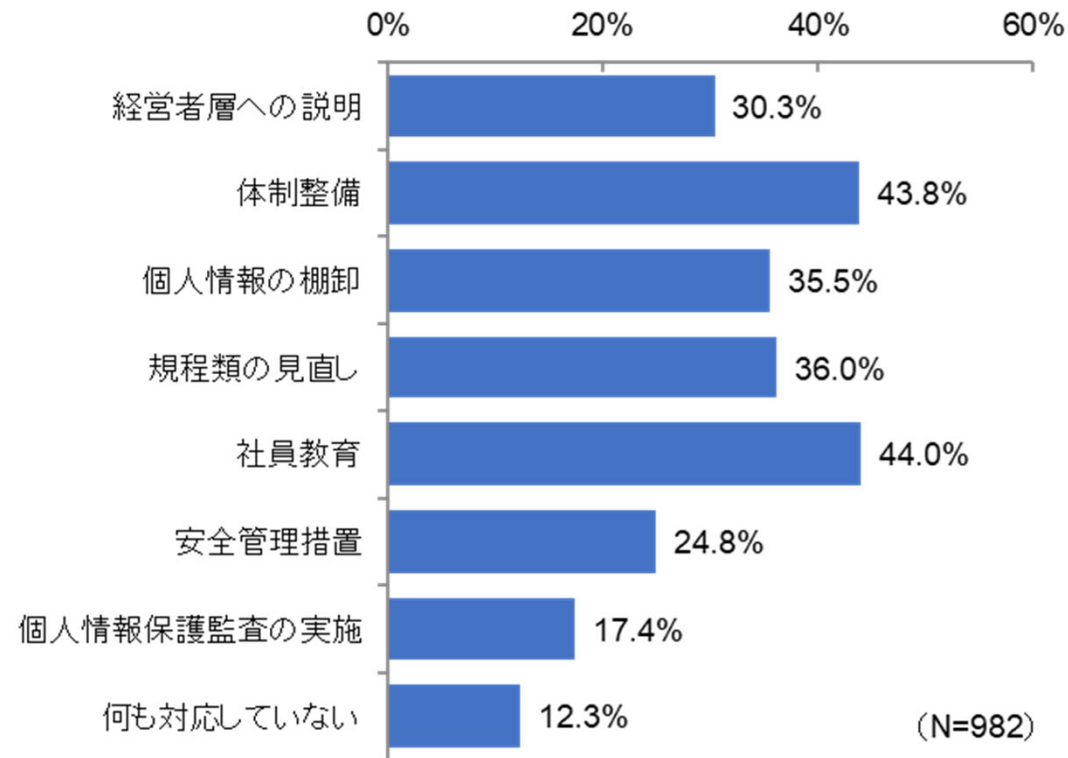
- 個人情報保護についての取り組みでは、社員教育が最も多く、次いで管理体制の構築、規程類の整備と続く。安全管理措置や第三者認証はその次で実装面での取り組みはやや低い。



Q6_2：改正個人情報保護法施行に向けての取り組み(2022年)

質問：あなたの勤務先では4月の改正個人情報保護法施行に向け、どのような取り組みを行っていますか。

- 改正個人情報保護法施行に向けても、現行の取り組み同様、社員教育と体制整備の比率が高い。



Q6_3：各国のプライバシー法規制の影響

質問：あなたの勤務先は、EUをはじめとする各国のプライバシー保護規制の影響を受けますか？

- 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APEC CBPRとなっている。

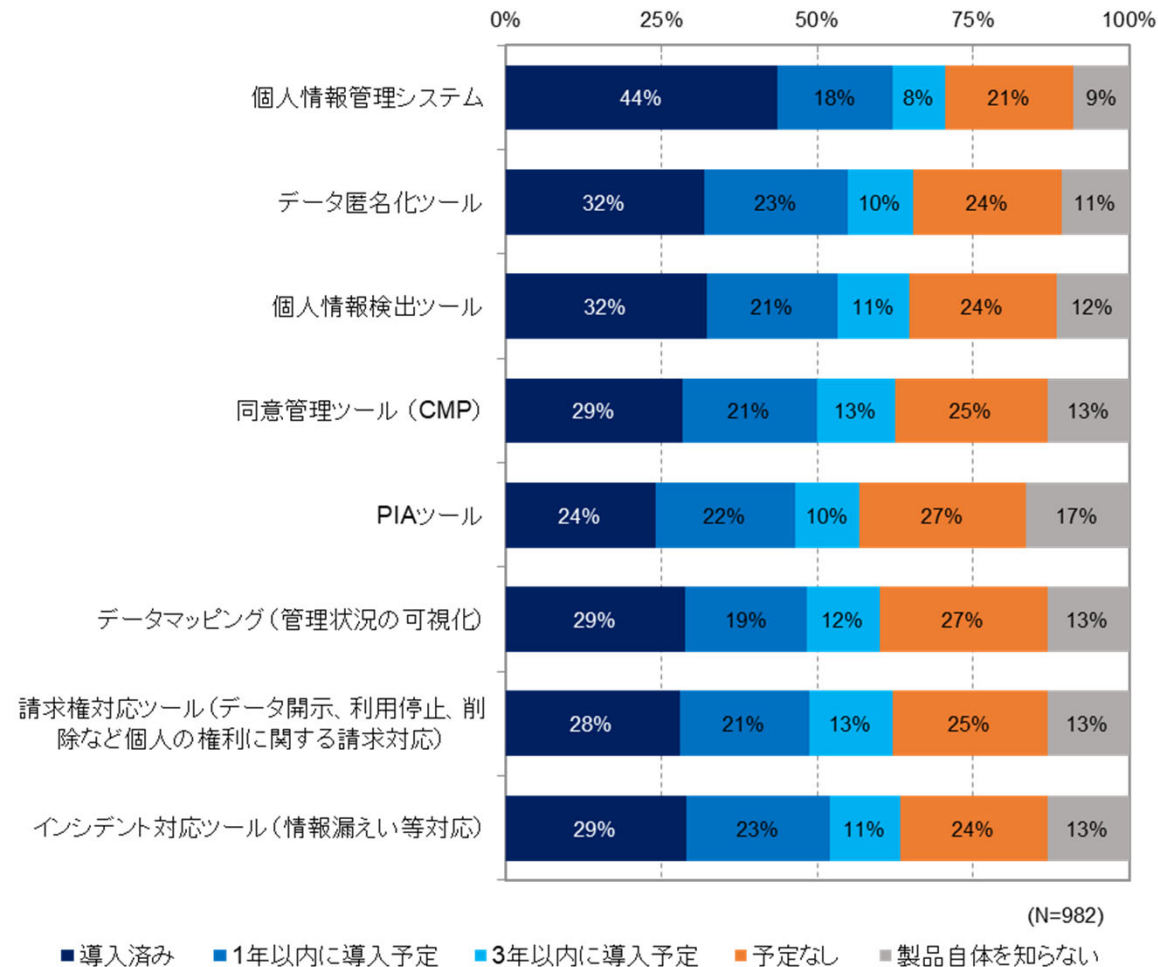
	EU一般データ規則 (GDPR)	CBPR認証	中国個人情報保護法、サイバーセキュリティ法	米国個人情報保護規制 (CLOUD法、カリフォルニア州プライバシー権法 (CCPA) など)	韓国個人情報保護法
事業に影響があるので対応している	30.9%	24.4%	23.4%	24.5%	18.6%
事業に影響はあるがあまり理解していない	24.6%	26.5%	24.9%	25.1%	25.5%
事業に影響はないが内容は知っている	18.8%	20.7%	23.5%	22.6%	19.7%
事業に影響がないため特に関心はない	29.2%	31.0%	32.4%	32.2%	37.9%

(N=982)

Q7：プライバシーソリューション／テックの導入状況

質問：あなたの勤務先ではプライバシーソリューション／テックを導入していますか？

- 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、導入予定を含めると7割に達する。



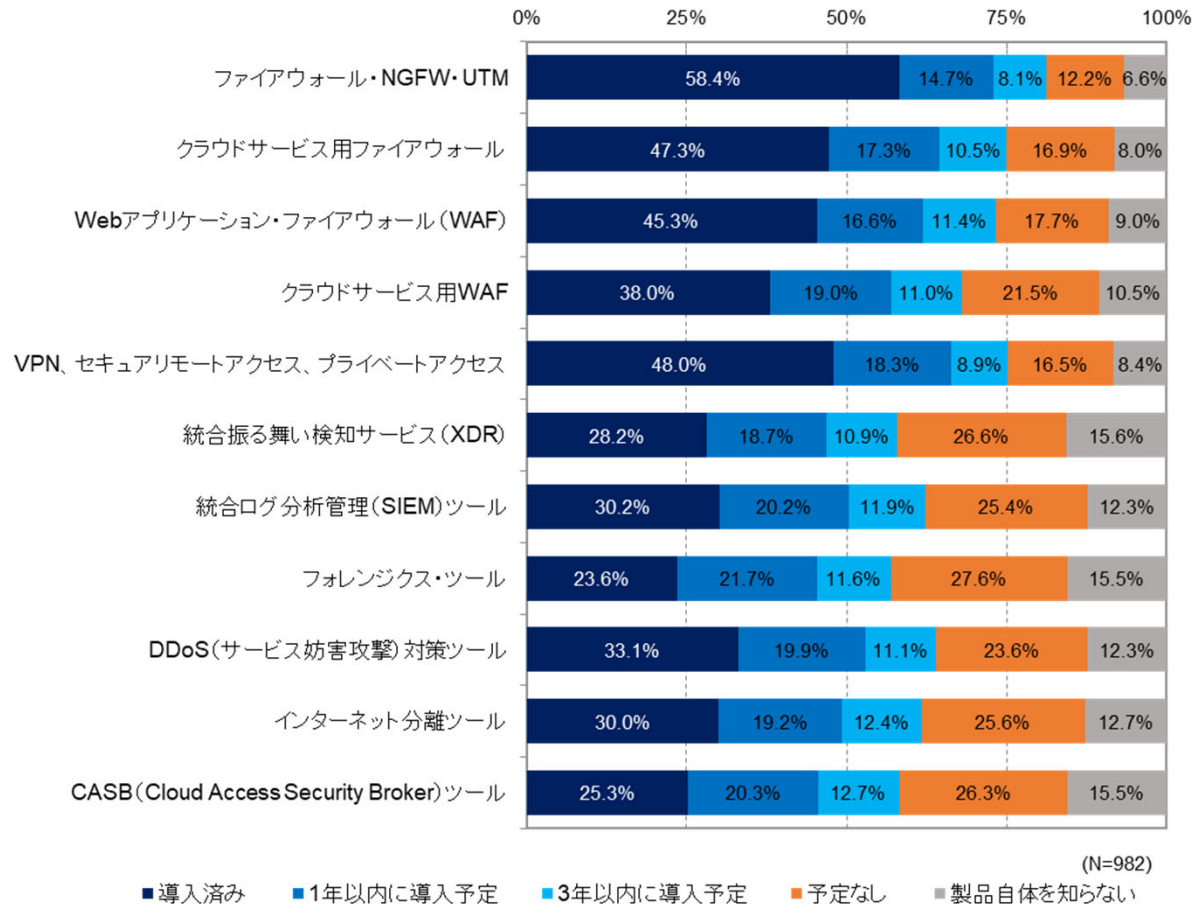
5) セキュリティ製品／技術の利用動向

- 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 : P P A P の対応状況
- Q9_3 : P P A P 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）

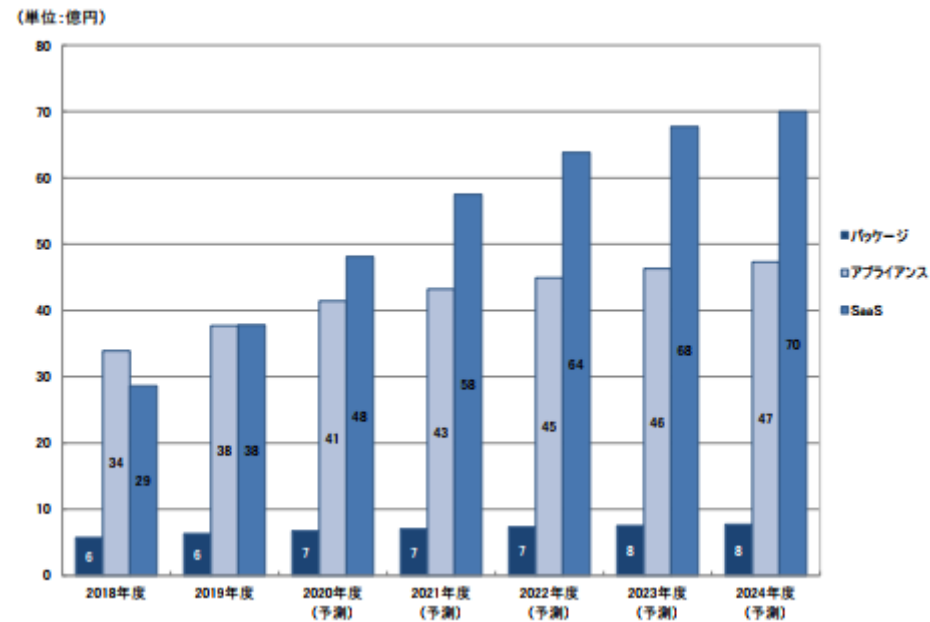
質問：以下のセキュリティ製品の利用について、あなたの勤務先での現在の実施状況と今後の計画について教えてください。

- クラウドファイアウォールやWAFなどのクラウド用のセキュリティサービスが伸びてきているが、オンプレ用の機器と交代するまでにはなっていない。
- セキュリティベンダーが注力しているXDRはSIEMにならびつつある。



【ご参考】ITR 国内WAF市場予測

- 国内のWAF市場は、年平均8.9%の伸びで、特にSaaS(クラウド)型は13.1%と驚異的な伸びが予測されている。

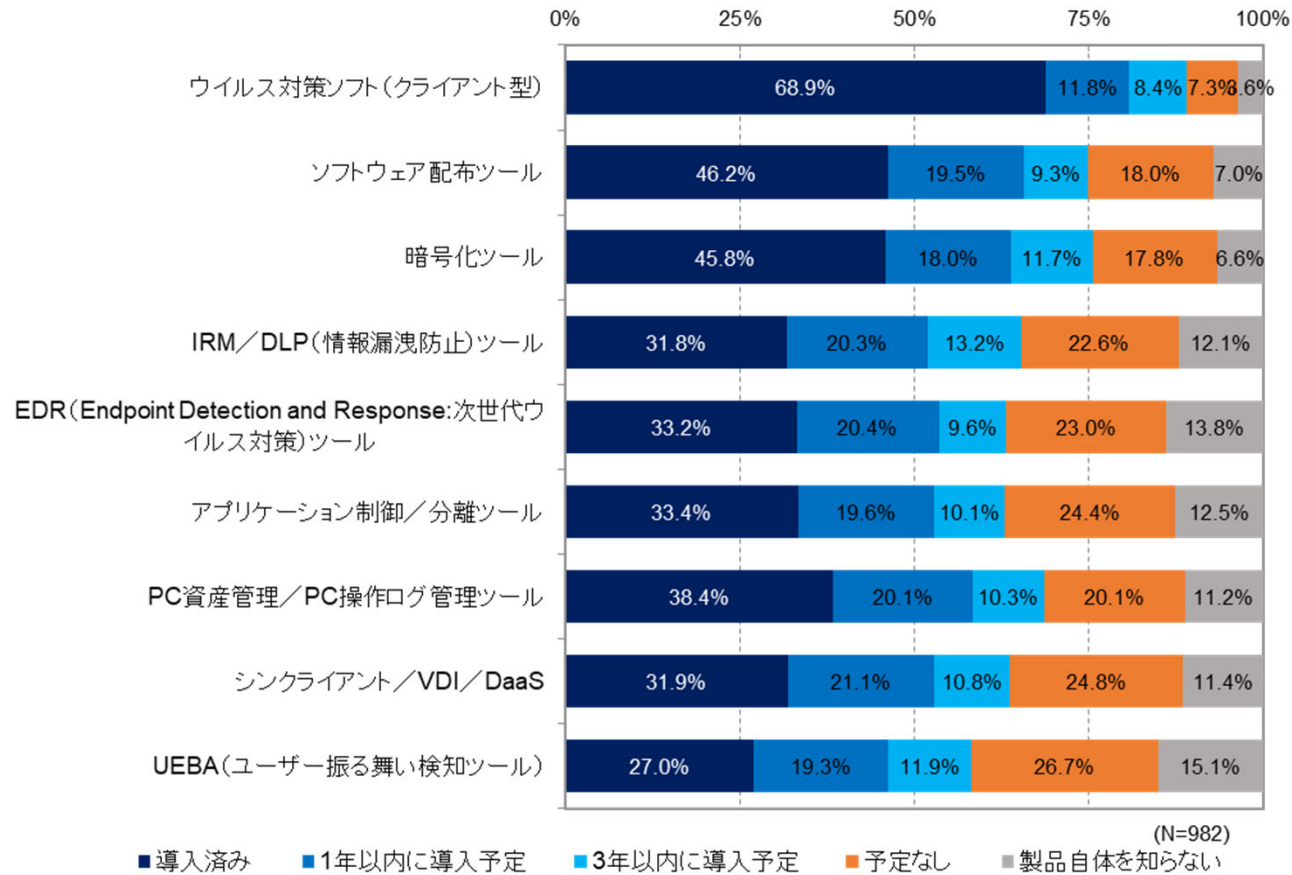


(出典：ITR Market View：サイバー・セキュリティ対策市場2021)

Q8_2：セキュリティ製品の利用状況（クライアント）

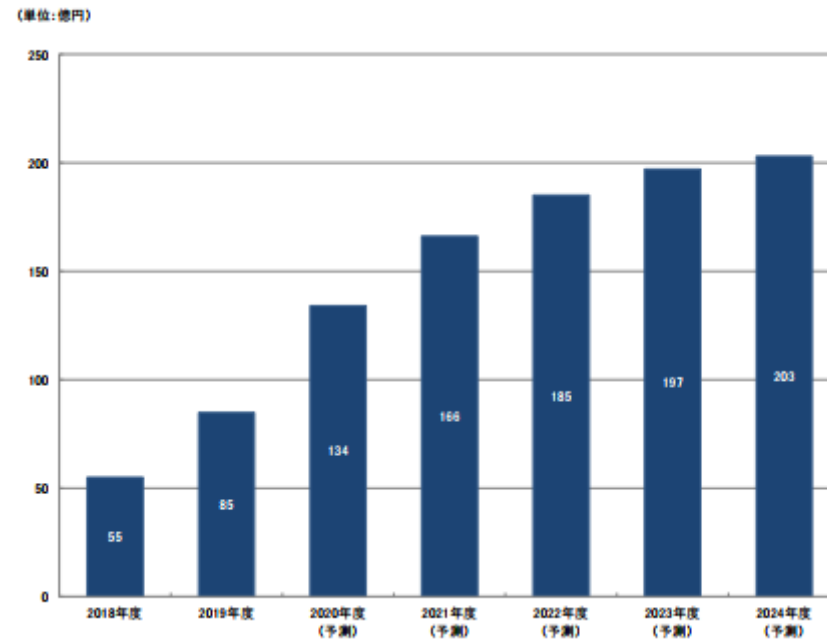
質問：以下のセキュリティ製品の利用について、あなたの勤務先での現在の実施状況と今後の計画について教えてください。

- 次世代型ウイルス対策ソフトであるEDRは導入済が約3割で予定を含めると6割に達しており、本格的な導入時期を迎えようとしている。



【ご参考】ITR 国内EDR市場予測

- 国内のEDR（NGAV含む）市場は、年平均19.1%の伸びで、驚異的な伸びが予測されている。

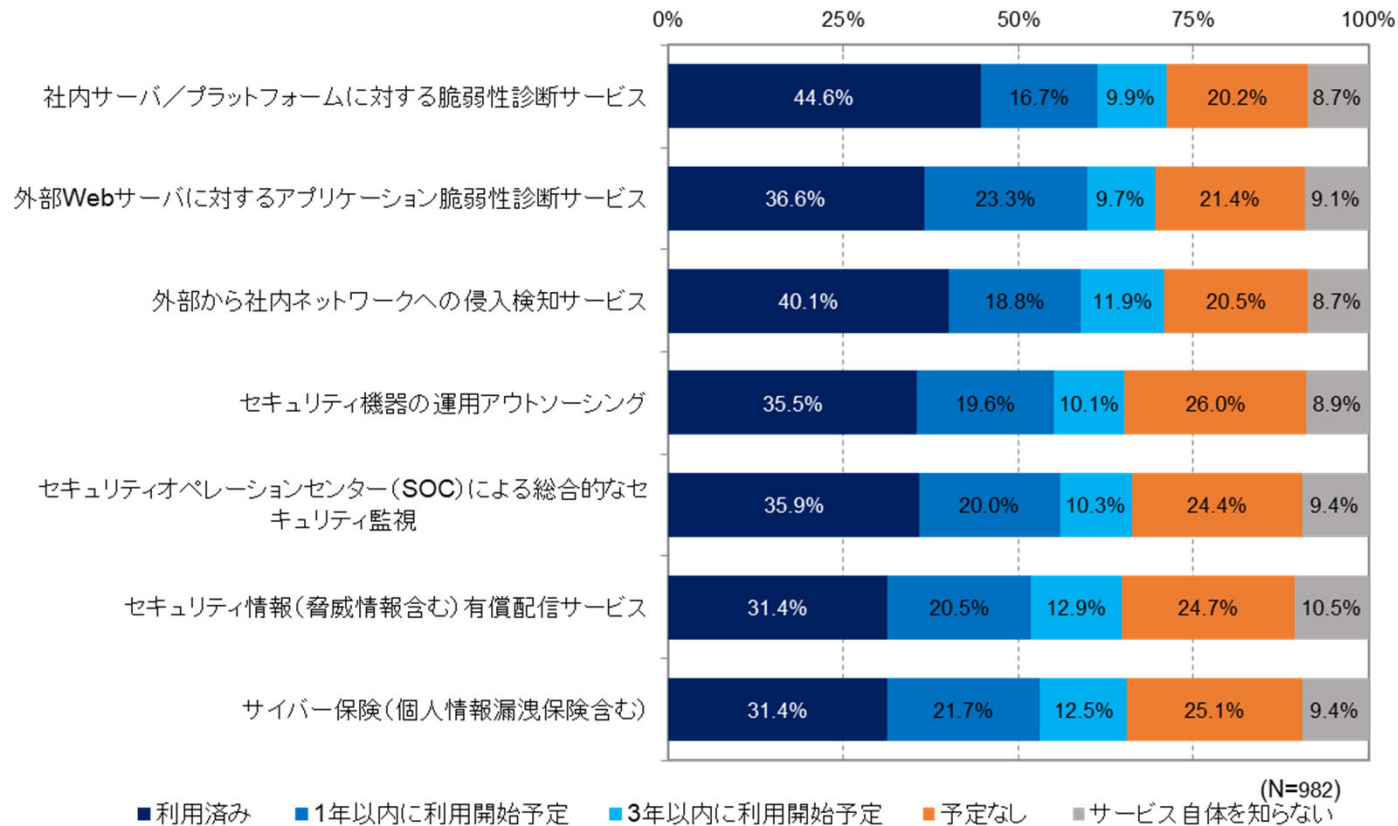


(出典：ITR Market View：エンドポイント／無害化／Web分離／CASB／CSPM／SOAR市場2021)

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）

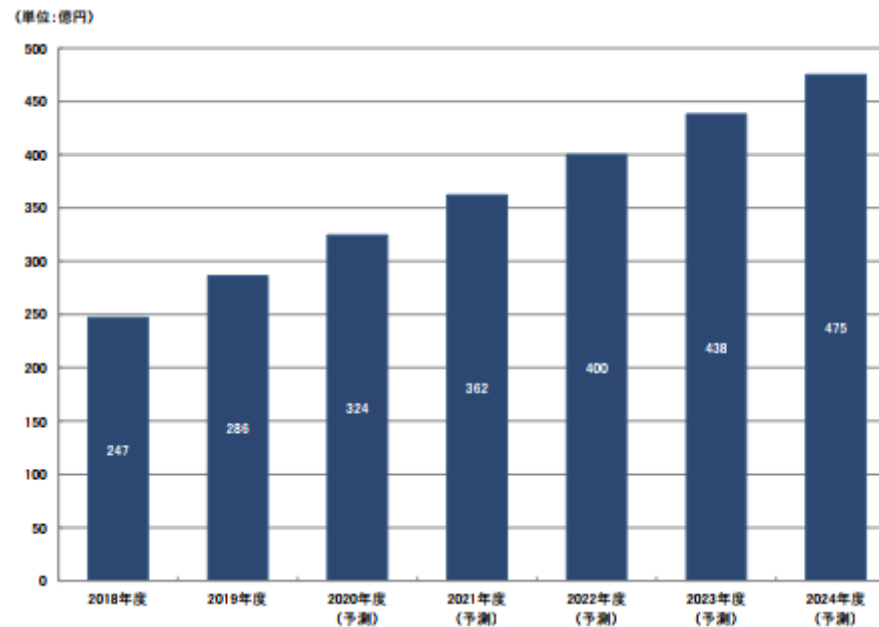
質問：以下のセキュリティ製品・サービスの利用について、あなたの勤務先での現在の実施状況と今後の計画について教えてください。

- 脆弱性診断サービスや侵入検知サービスは導入済が4割を超え、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】ITR 国内セキュリティ脆弱性診断市場予測

- 国内のセキュリティ脆弱性診断市場は、年平均10.7%の伸びで、大きな伸びが予測されている。

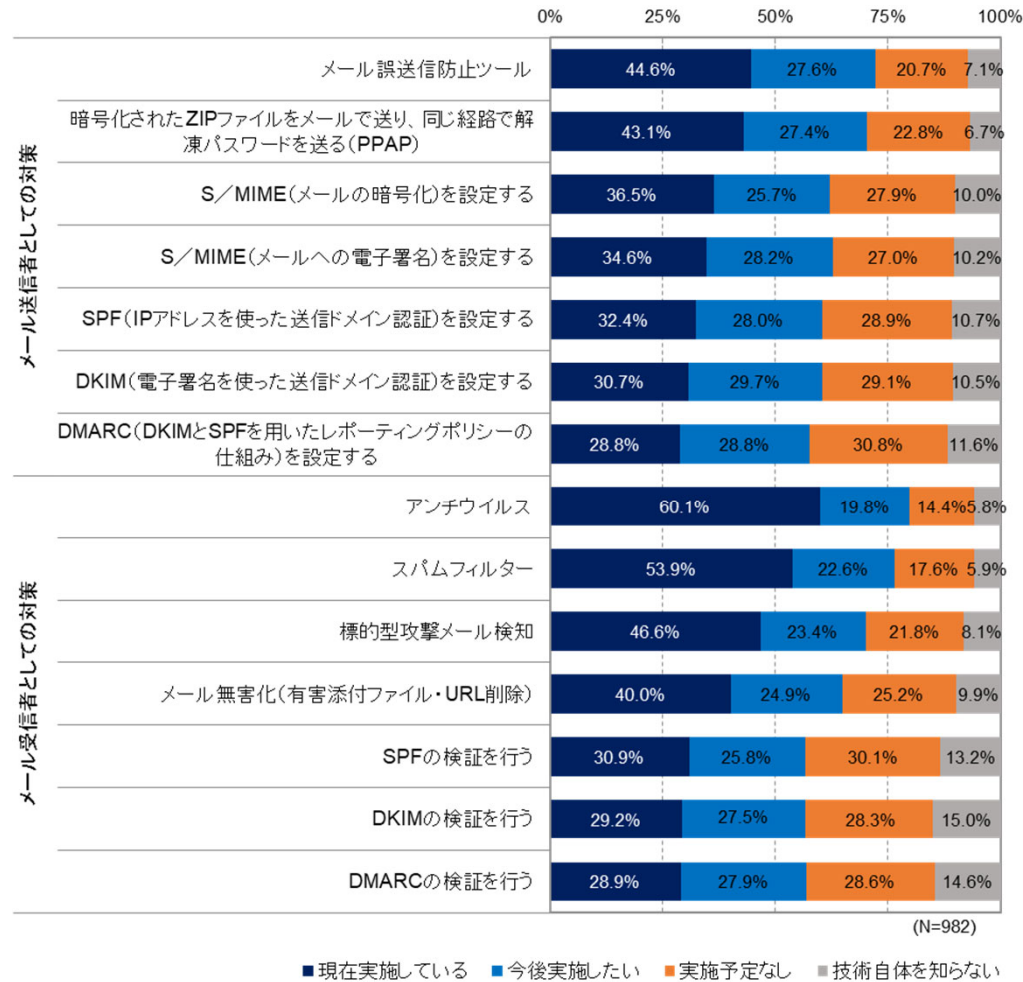


(出典 : ITR Market View : サイバー・セキュリティ・コンサルティング・サービス市場2020)

Q9_1：電子メールのセキュリティ対策状況(2022年)

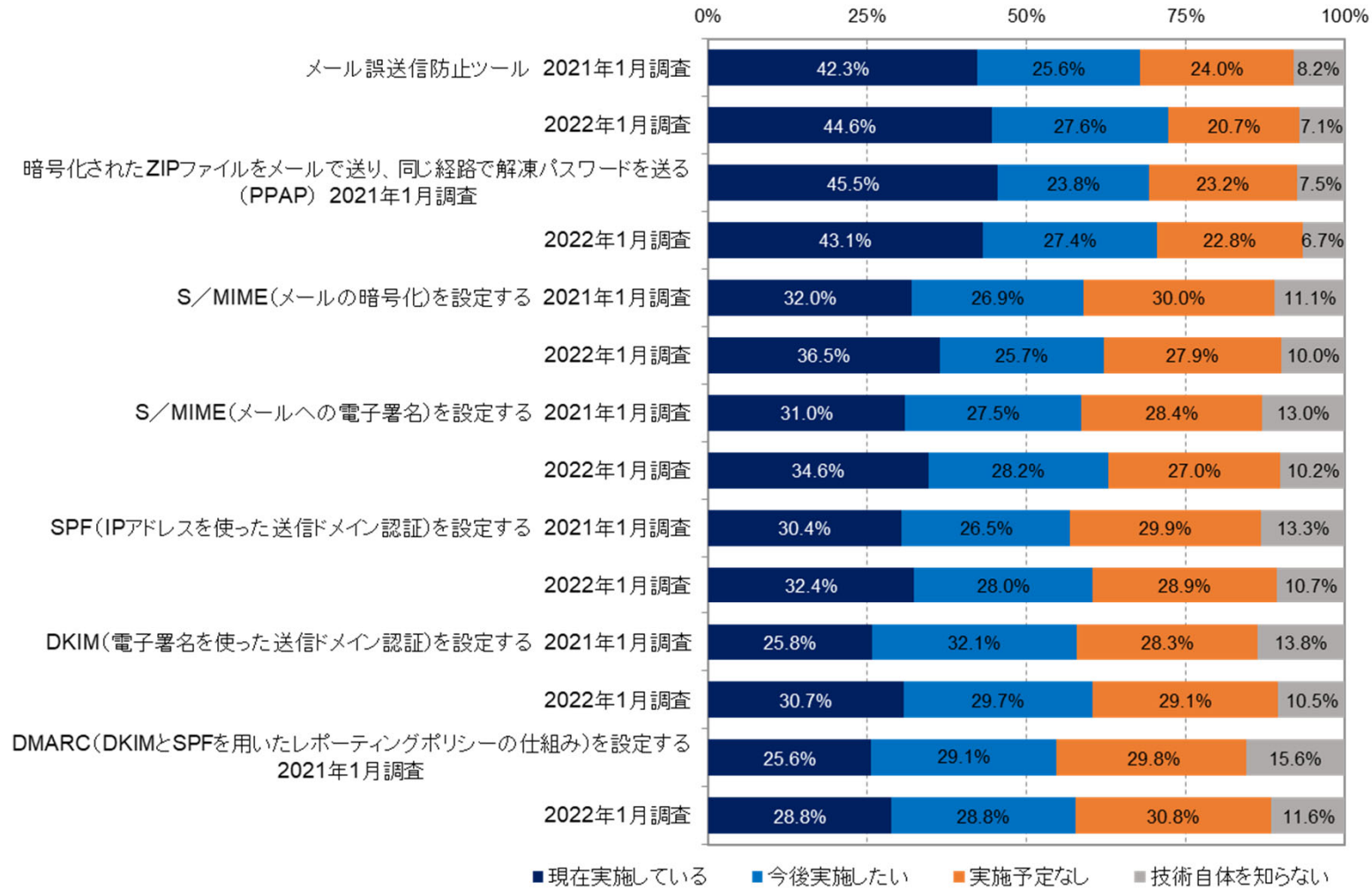
質問：あなたの勤務先での電子メールのセキュリティ対策について、現在の実施状況などについて教えてください。

- 送信側については誤送信防止ツールで予定を含めると7割に達する。受信側はアンチウィルスがトップで約8割となっている。



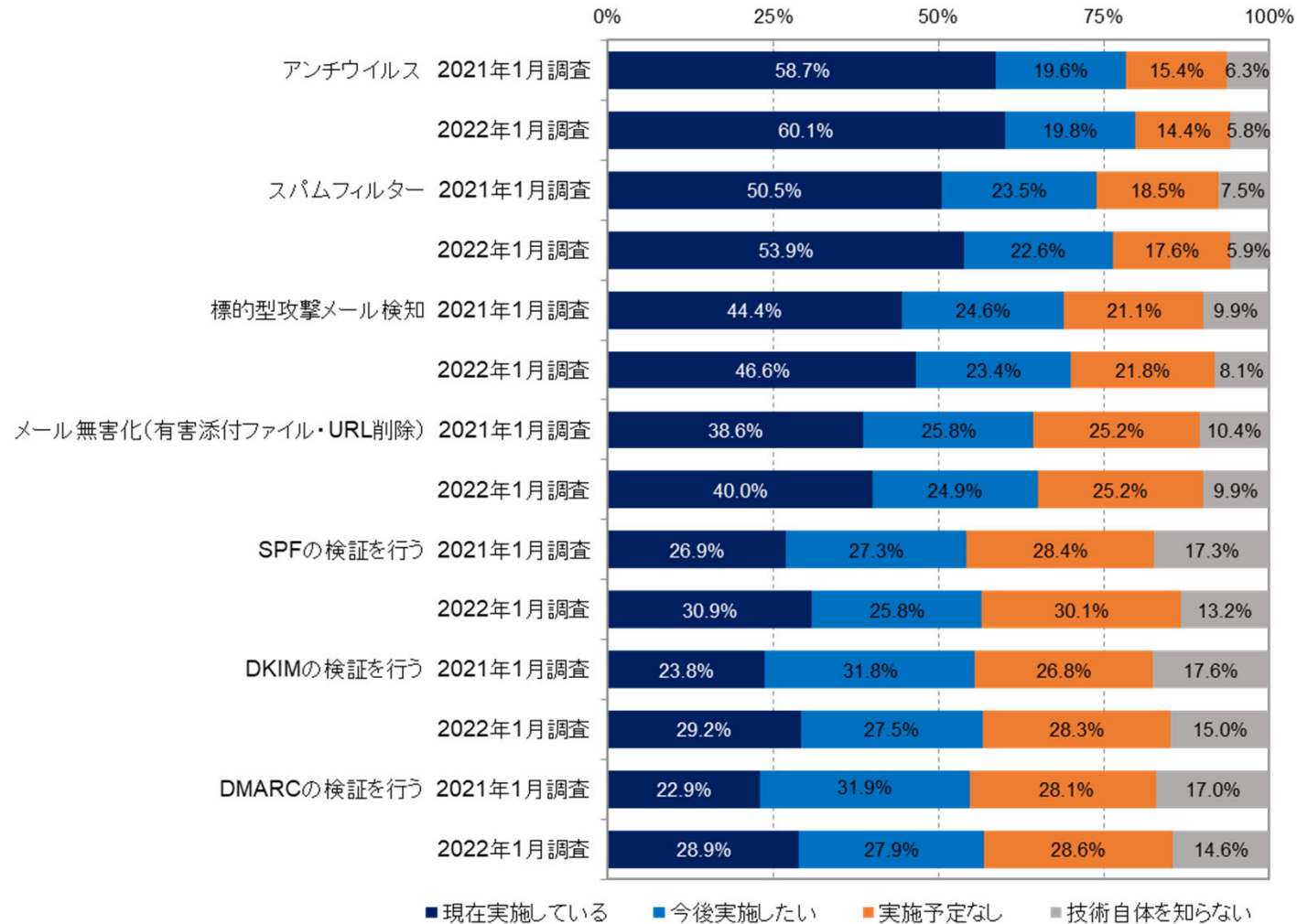
Q9_1：電子メールのセキュリティ対策状況（送信側、昨年との比較）

- 送信側は、昨年のPPAPからメール誤送信防止ツールにトップが入れ替わった。他の項目についてはいずれも昨年よりも実施比率がアップしている。



Q9_1：電子メールのセキュリティ対策状況（受信側、昨年との比較）

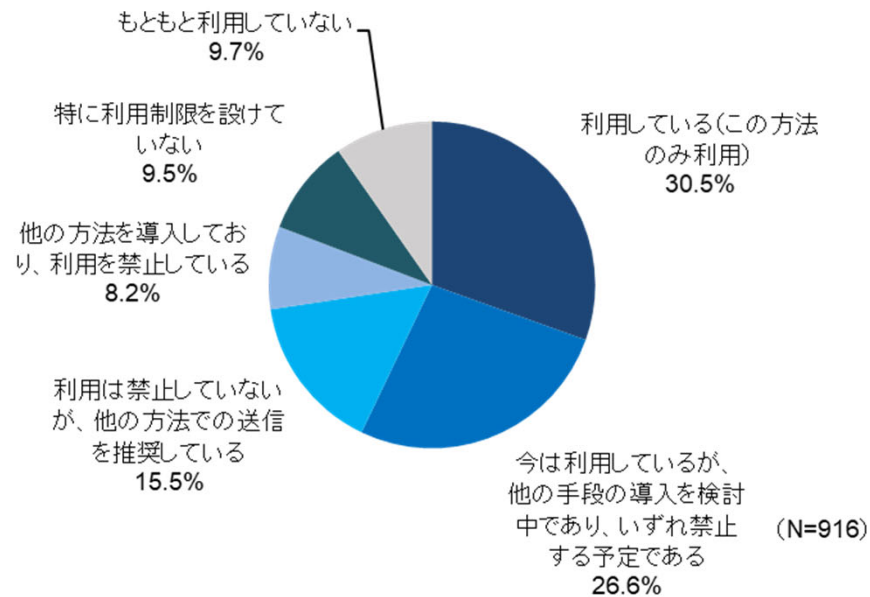
■ 受信側も、予定を含めると全項目について昨年よりも比率がアップしている。



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

質問：あなたの勤務先ではPPAP送信をどう対応していますか？

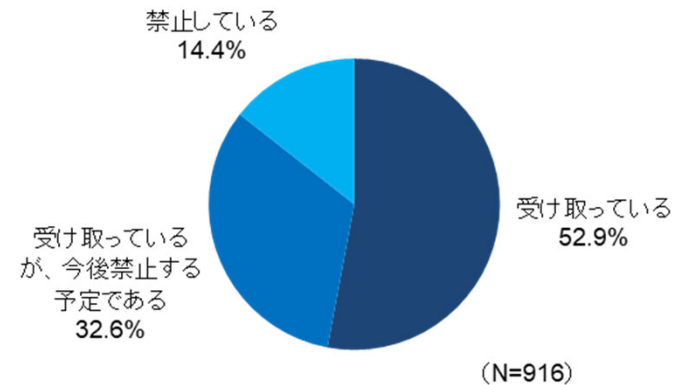
- PPAP(送信系)をもともと利用していないが9.7%、利用を禁止しているが8.2%で、今後利用を禁止予定の26.6%を含めると約5割弱が禁止する方向となっている。



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

質問 : あなたの勤務先ではPPAPによるファイル受信にどう対応していますか。

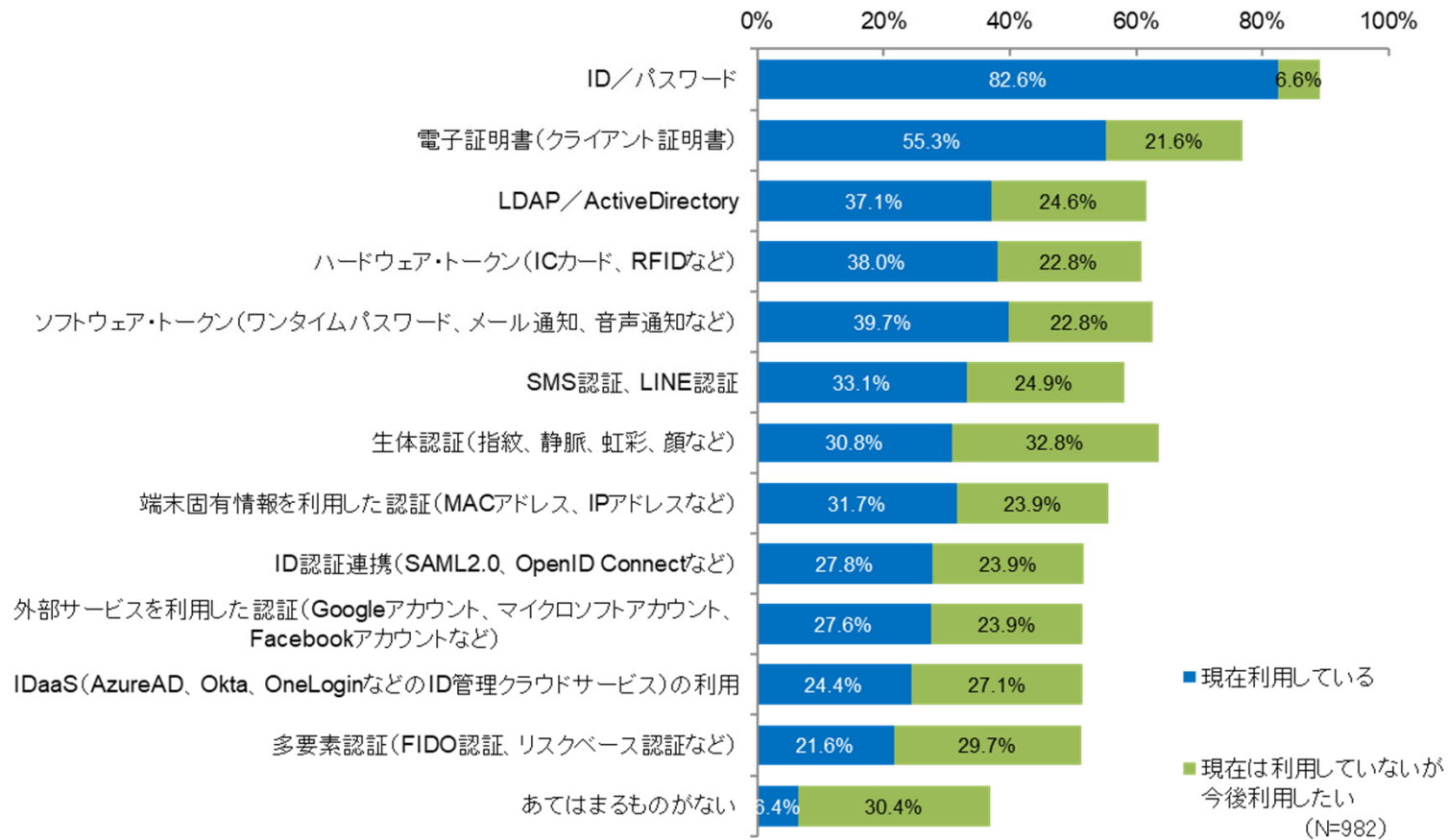
- PPAPの受信側では、禁止しているが14.4%、今後禁止予定が32.6%で、約5割弱が禁止する方向である。



Q10：高機密システムへのアクセス認証手段

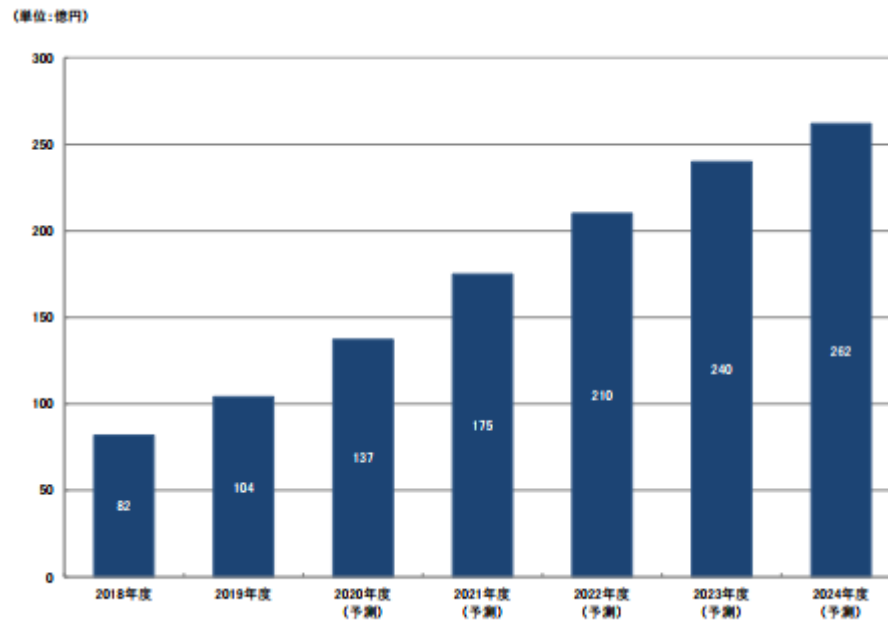
質問：機密性の高い情報を扱うシステムのアクセス認証手段として、あなたの勤務先で現在利用しているものと、現在は利用していないが今後利用したいと考えているものをそれぞれお選びください。

- 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】ITR IDaaS市場予測

- 国内のIDaaS市場の年平均市場成長率は20.3%で、クラウド化の進行に伴い、驚異的に成長することが予測される。



(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2021)

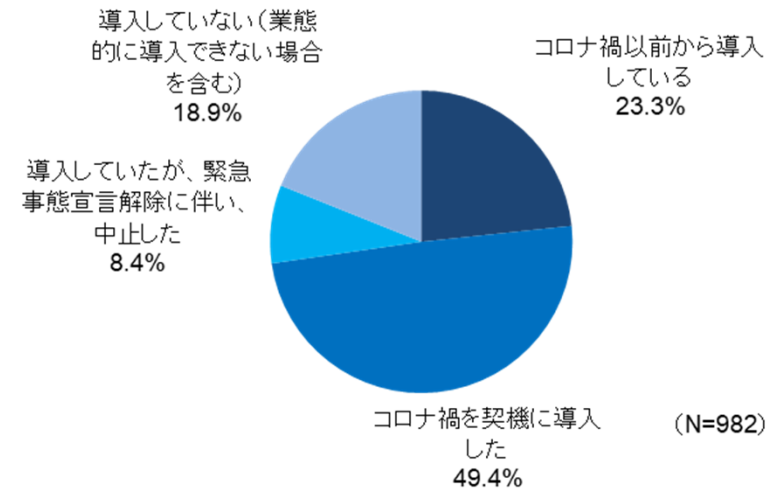
6) テレワークとクラウドの動向

- Q11_1 : テレワークの導入状況
- Q11_2 : テレワークシステム環境 (方式)
- Q11_3 : テレワークの実施場所
- Q11_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
- Q12_1 : システムのクラウド化の状況
- Q12_2 : クラウドサービスの利用方法
- Q12_3 : クラウドサービスの選定ポイント
- Q12_4 : 信頼性重視のクラウドサービス機能

Q11_1：テレワークの導入状況

質問：あなたの勤務先ではテレワークを導入していますか。

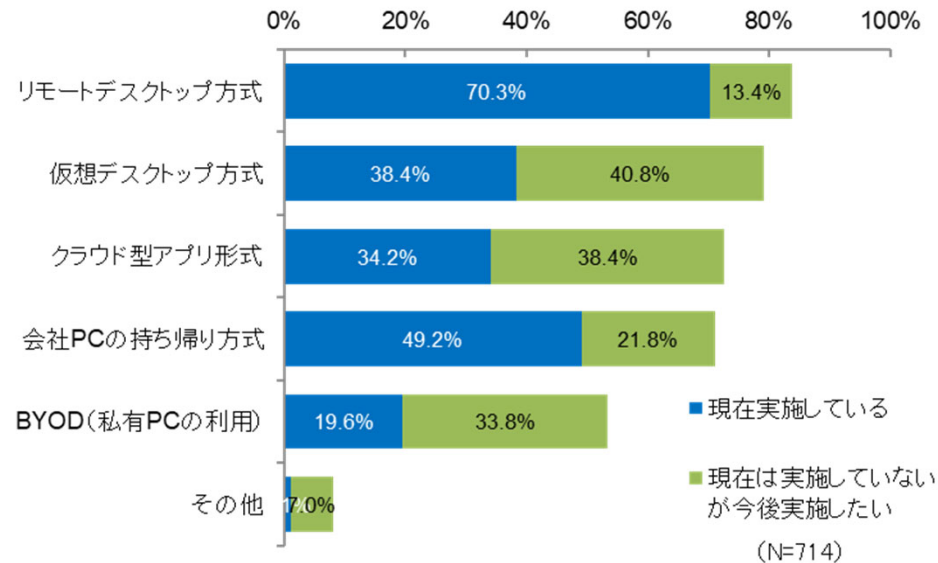
- コロナ禍をきっかけに導入しているが約5割で、以前から導入しているを合わせると7割超がテレワークを導入しており、ワークスタイルのメインとなってきている。



Q11_2：テレワークのシステム環境（方式）

質問：あなたの勤務先が採用しているテレワークシステム環境（方式）を教えてください

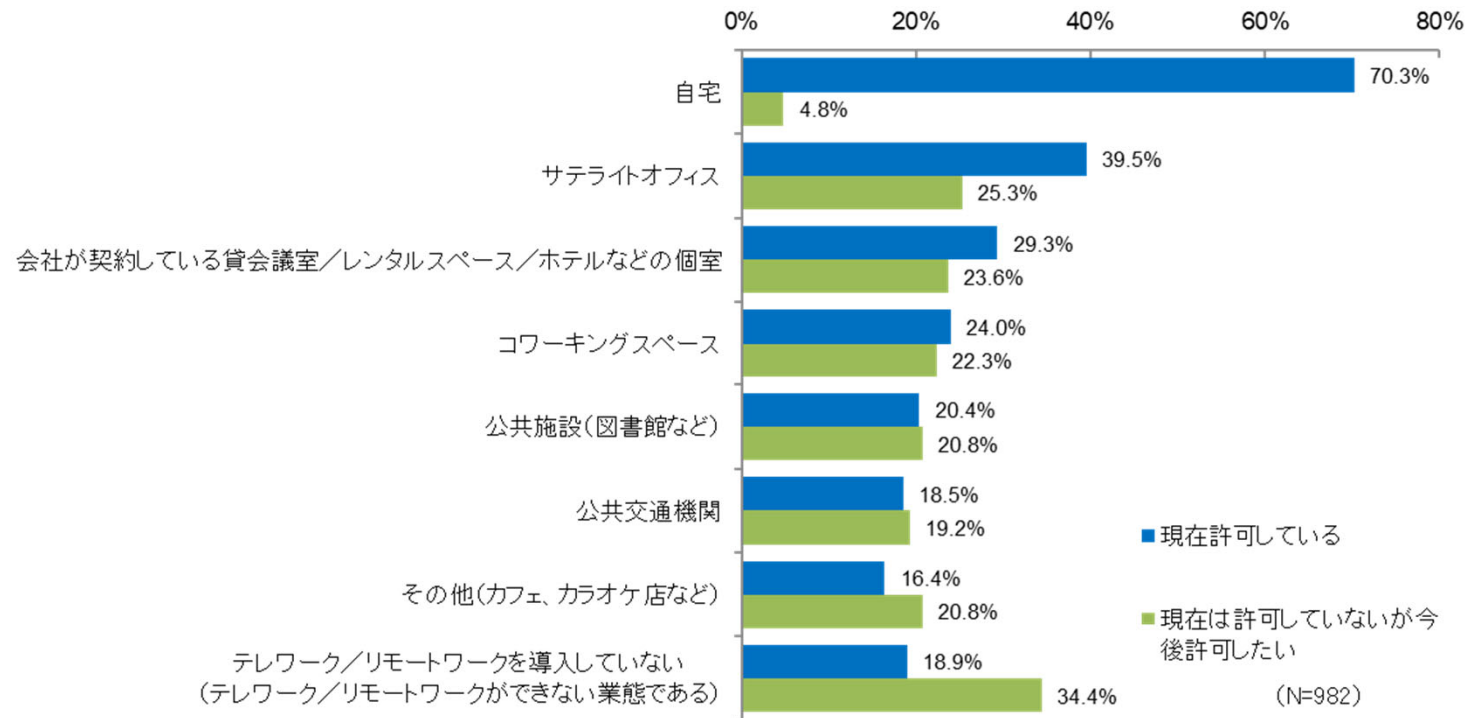
- テレワークの方式としてはリモートデスクトップ方式が最も多く、次いで会社PCの持ち帰り方式だが、今後実施したい方式としては仮想デスクトップやクラウド型アプリ、BYODが挙げられている。



Q11_3：テレワークの場所

質問：あなたの勤務先ではテレワーク／リモートワークの実施場所としてどのような場所を使用していますか？

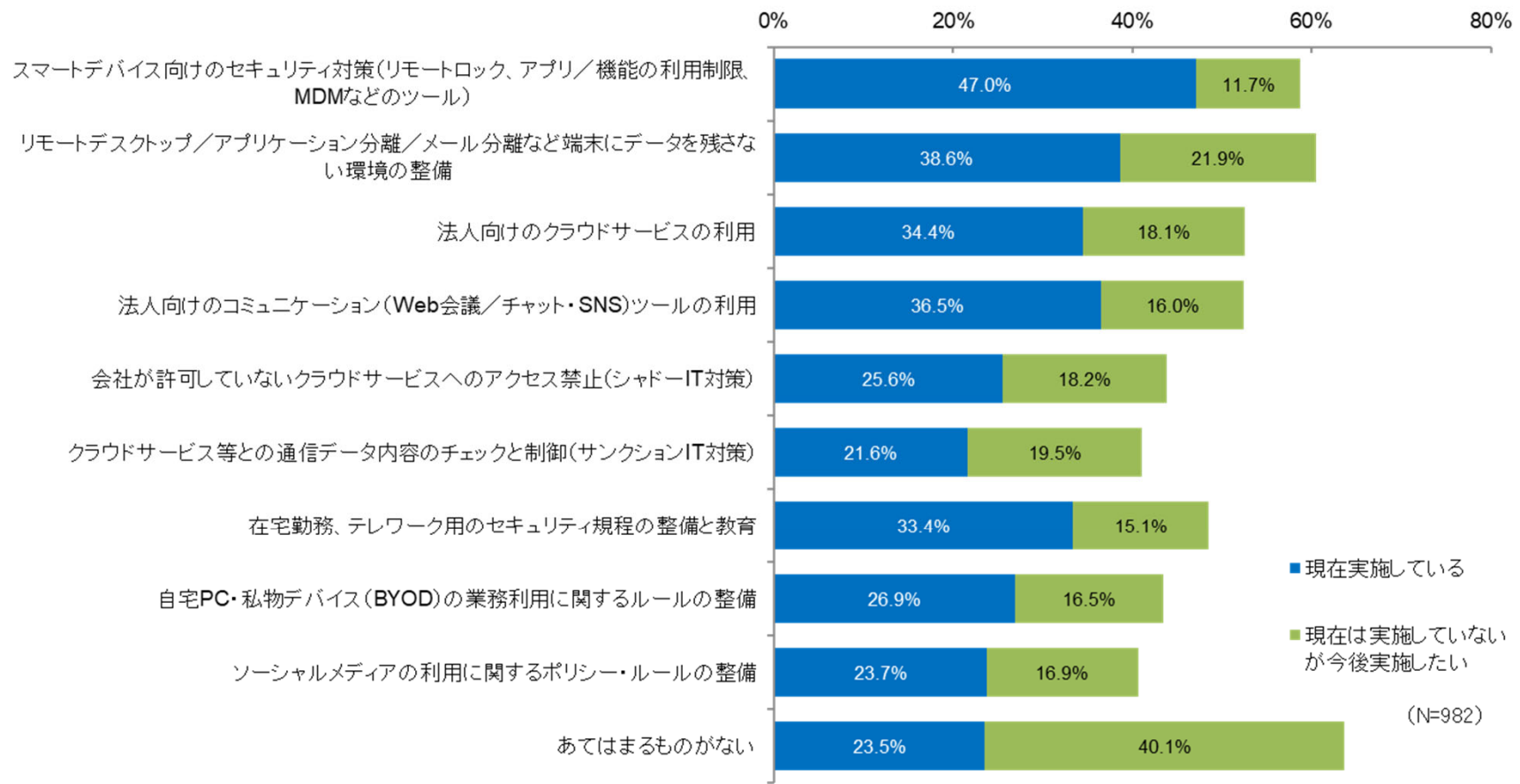
- テレワークの場所は、現状では自宅が最も多く、サテライトオフィスが続くが、今後会社契約の貸会議室やコワーキングスペース、公共施設など多様化する動きがみられる。



Q11_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

質問：以下の項目について、あなたの勤務先ですでに実施していること、現在は実施していないが今後実施したいと考えていることはそれぞれ何ですか？

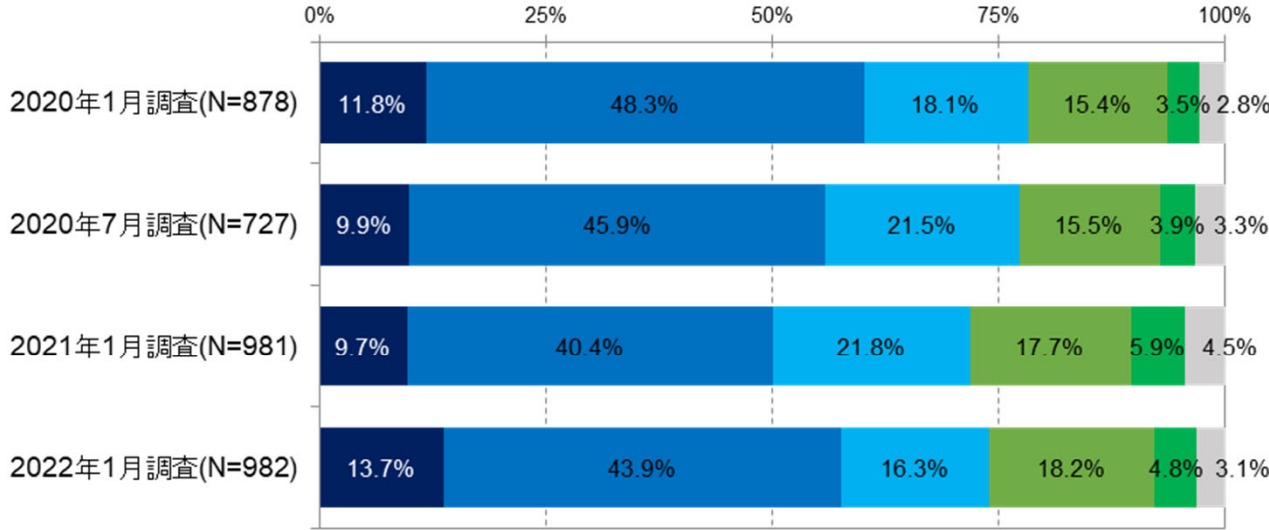
- 実施済の対策についてはスマートデバイスのセキュリティ対策が約 5 割、端末にデータを残さないが約 4 割で、他の施策は 2 ～ 3 割となっている。



Q12_1：クラウドサービス利用状況（過去3回との比較）

質問：あなたの勤務先のシステムではどの程度クラウド化が進んでいますか？

■ 今回小規模事業者を対象にしたことで、クラウド利用状況は若干減少したが、約9割はなんらかクラウドサービスを利用している。

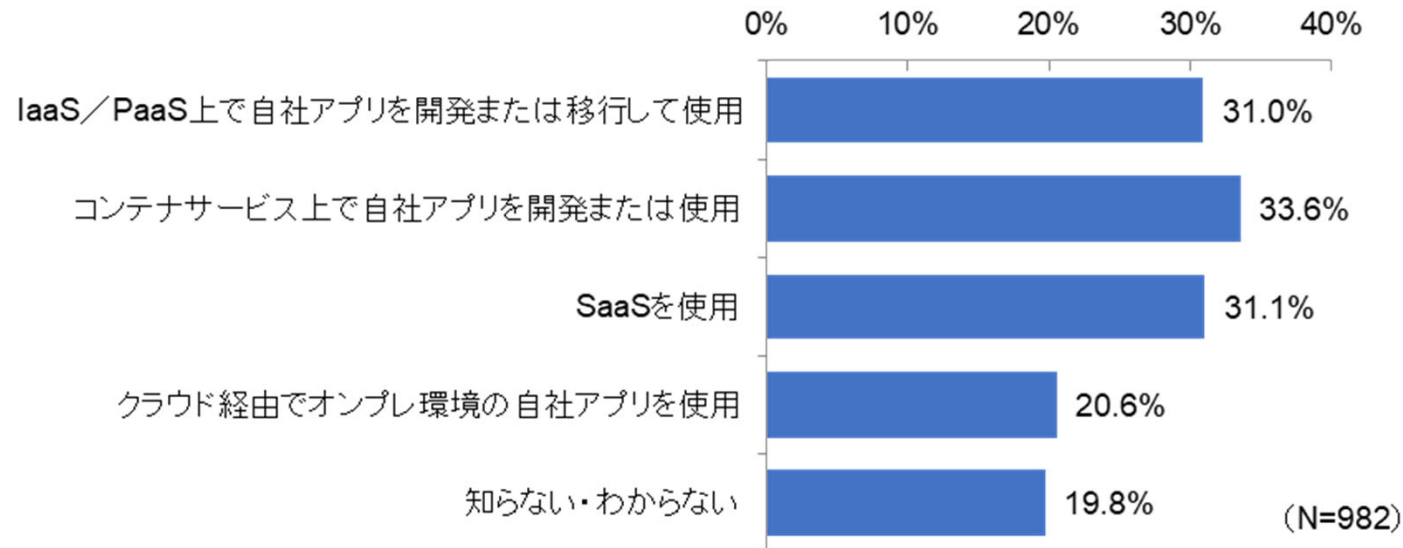


- 全くクラウドサービスを使用していない
- 一部クラウドサービスを使っている
- 半分程度はクラウドサービスを使っている
- 大半はクラウドサービスを使っている
- すべてクラウドサービスを使っている
- 知らない・わからない

Q12_2：クラウドサービス利用方法

質問：あなたの勤務先でのクラウドサービスの利用方法を教えてください？

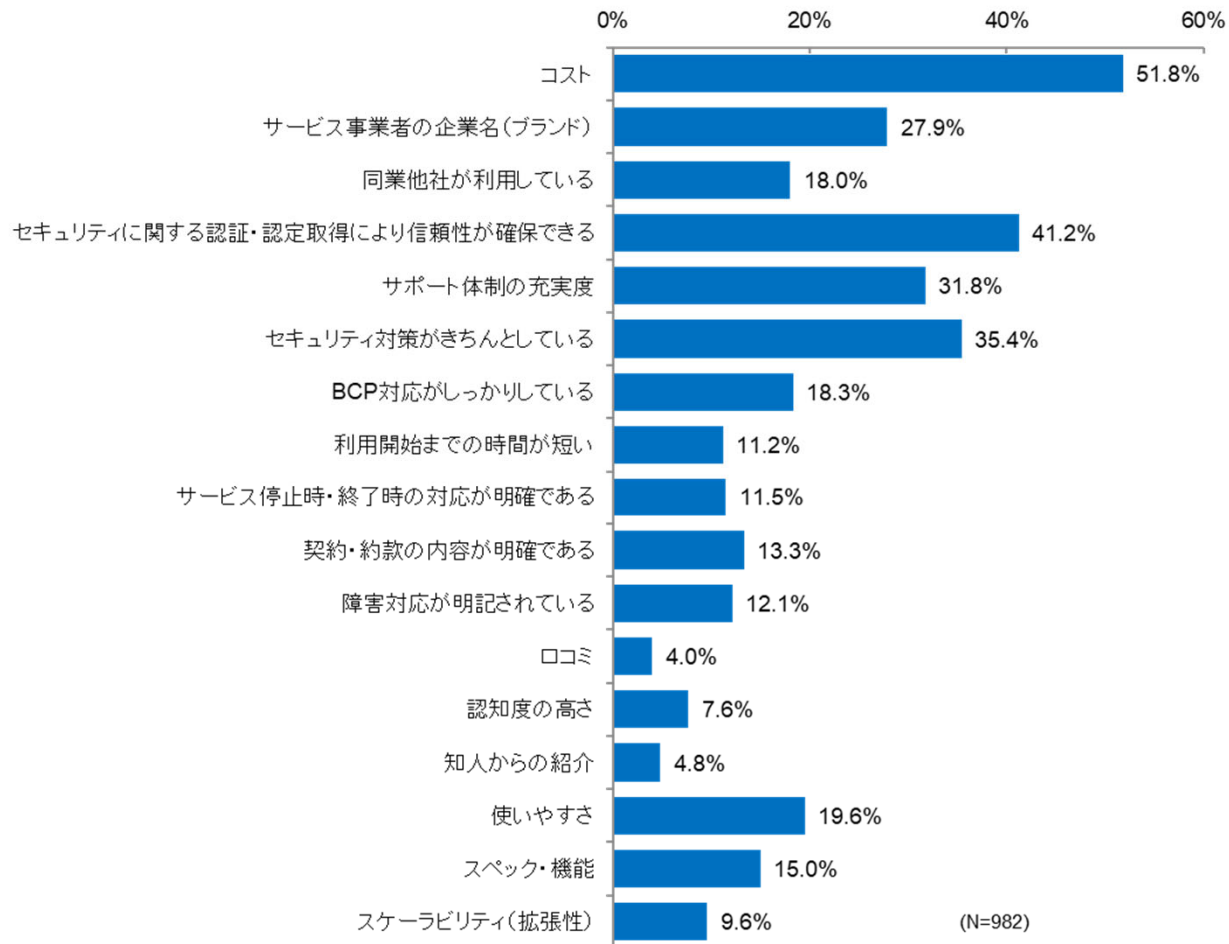
- コンテナサービス上での開発がトップとなっており、SaaSの利用、IaaS/PaaS上での開発がほぼ同率でコンテナサービスが普及してきている。



Q12_3：クラウドサービス選定する際のポイント

質問：あなたの勤務先がクラウドサービスを選定する際のポイントは何ですか？

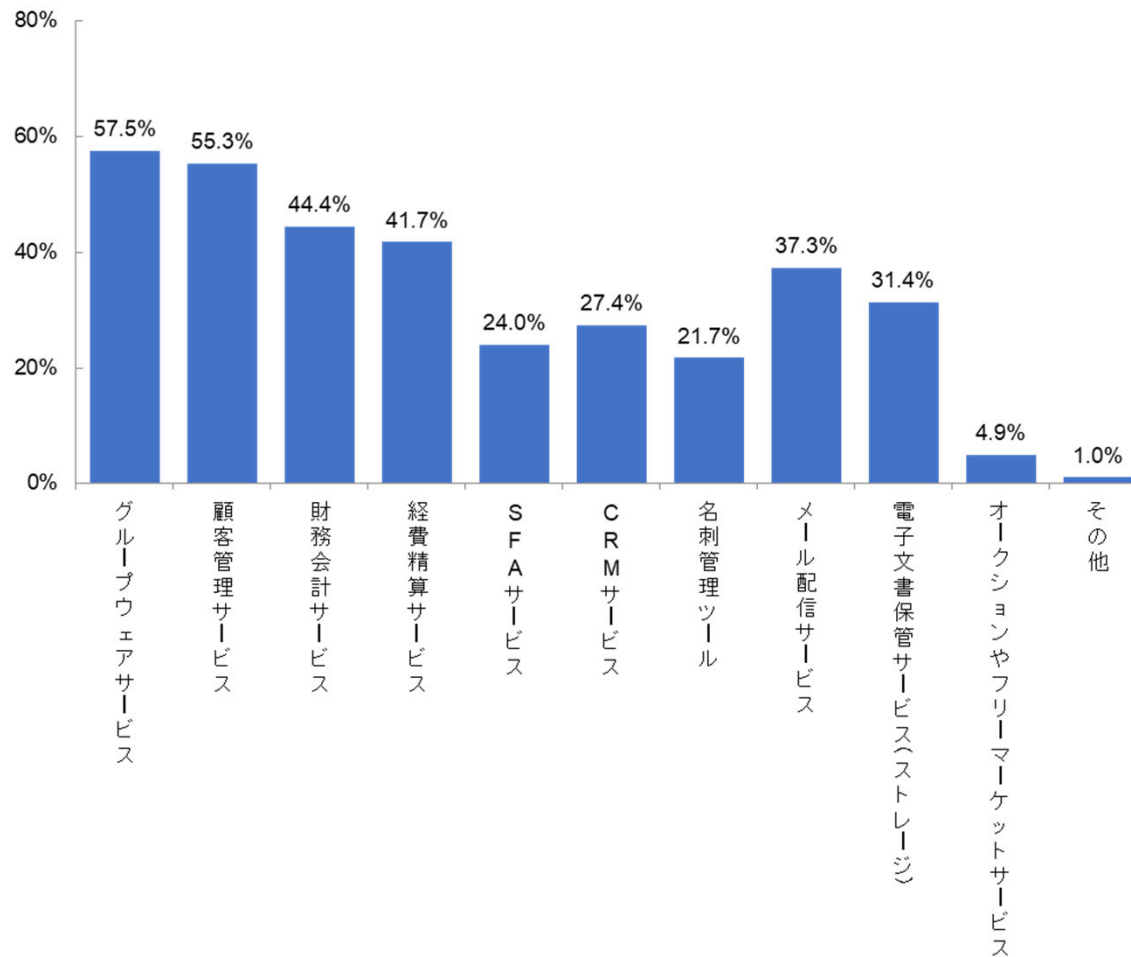
- クラウドサービス選定時のポイントの1位はコストで、信頼性の確保とセキュリティ対策が続いている。



Q12_4：信頼性を重視して選ぶクラウドサービスはどれですか？

質問：あなたの勤務先がクラウドサービス選定の際に信頼性を重視して選ぶ機能はどれですか？

- 信頼性重視で選ばれるクラウドサービスとして、グループウェアがNo.1で、顧客管理サービス、財務管理サービスが続いている。



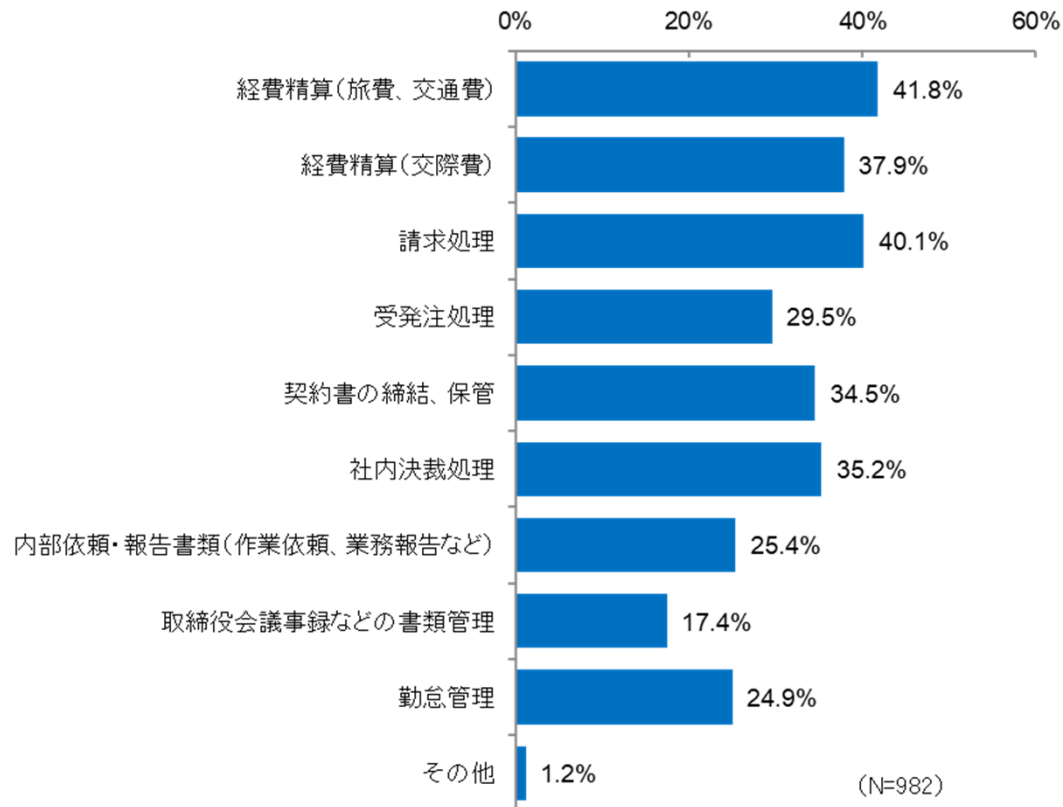
7) 電子契約関連、DX推進

- 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(2022年)

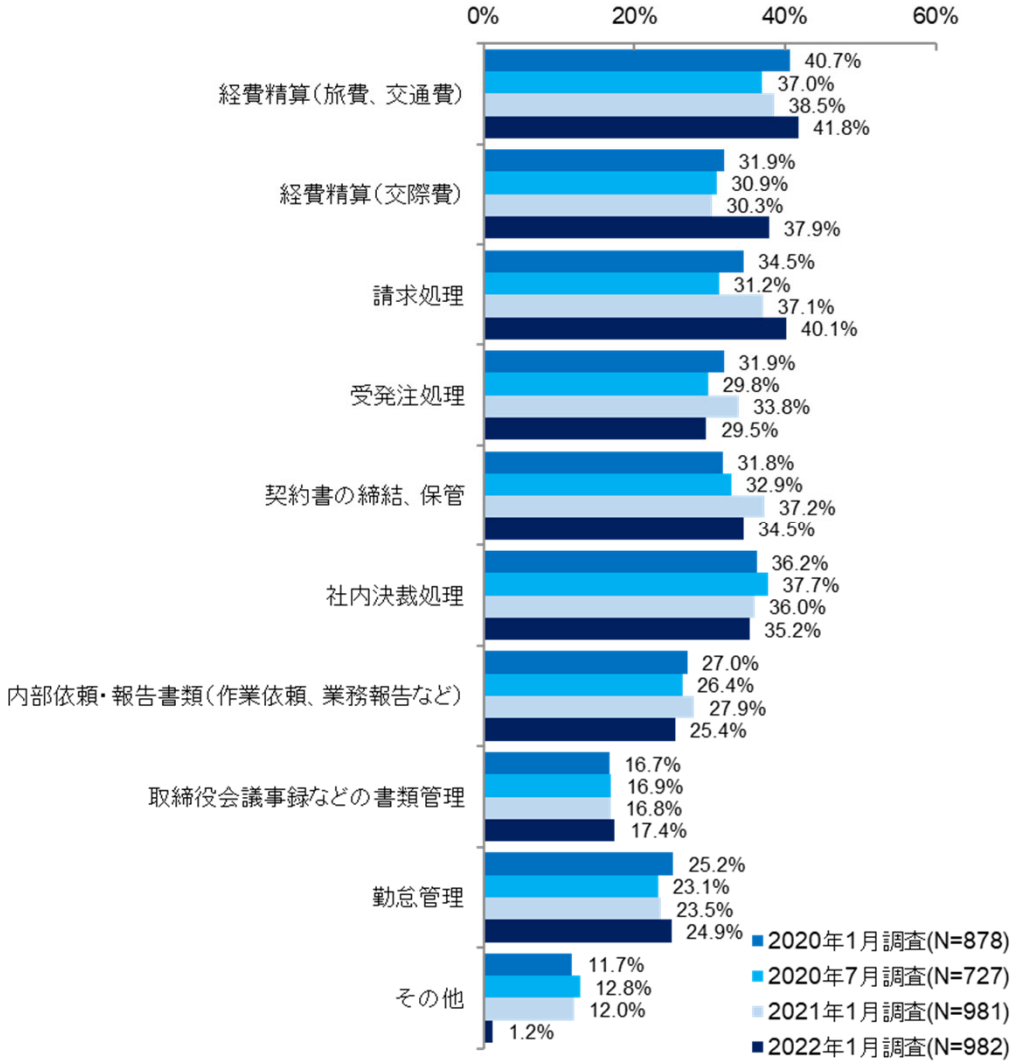
質問：あなたの勤務先で、特に電子化したいと考えている業務プロセスは何ですか？

- 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）で、次いで請求処理、経費精算（交際費）と続く



Q13_1 : 特に電子化したい業務プロセス(過去3回との比較)

- 過去3回との比較でも経費精算（旅費、交通費）が最も多く、請求処理も同様である。経費精算（交際費）が今回多くなっている一方、逆に社内決裁処理が減っている。



Q13_1 : 特に電子化したい業務プロセス(業種別・規模別)

- 業種別では建設・不動産で経費精算、請求処理が高い傾向にある
- 規模別では規模が大きいほどニーズが高い傾向があるが、勤怠処理は全規模で平均して高い。

業種別

	製造 (N=301)	建設・不動 産(N=97)	卸売・小売 (N=86)	金融・保険 (N=82)	情報通信 (N=147)	サービス (N=215)	公共・その 他(N=54)	全体 (N=982)
経費精算(旅費、交通費)	39.9%	52.6%	40.7%	46.3%	40.1%	38.1%	46.3%	41.8%
経費精算(交際費)	43.5%	42.3%	34.9%	46.3%	36.7%	28.4%	31.5%	37.9%
請求処理	38.5%	49.5%	39.5%	31.7%	38.8%	42.3%	40.7%	40.1%
受発注処理	32.9%	36.1%	32.6%	15.9%	28.6%	27.4%	25.9%	29.5%
契約書の締結、保管	34.6%	42.3%	33.7%	41.5%	30.6%	33.0%	27.8%	34.5%
社内決裁処理	33.2%	29.9%	29.1%	42.7%	37.4%	37.7%	38.9%	35.2%
内部依頼・報告書類(作業依頼、業務報告など)	24.6%	23.7%	30.2%	24.4%	21.1%	26.0%	35.2%	25.4%
取締役会議事録などの書類管理	16.6%	19.6%	20.9%	18.3%	17.7%	16.3%	14.8%	17.4%
勤怠管理	20.6%	30.9%	27.9%	19.5%	22.4%	28.8%	33.3%	24.9%
その他の紙による書類管理	1.3%	2.1%	1.2%	0.0%	0.7%	1.9%	0.0%	1.2%

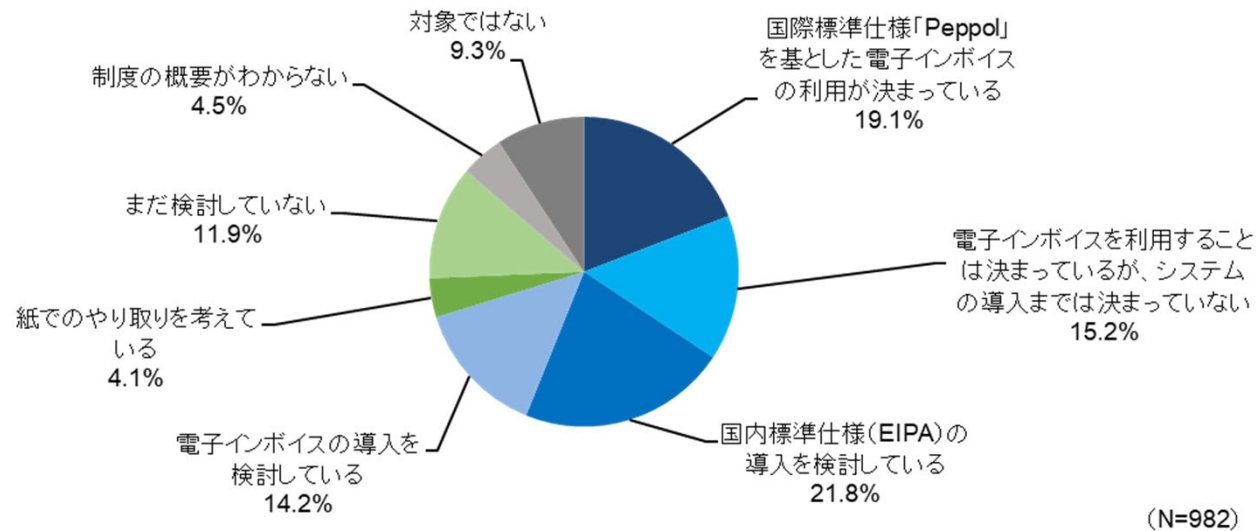
規模別

	5,000人 以上 (N=215)	1,000~ 4,999人 (N=239)	300~999 人 (N=199)	50~299人 (N=215)	50人未 満 (N=114)	全体 (N=982)
経費精算(旅費、交通費)	41.9%	43.1%	48.7%	40.5%	28.9%	41.8%
経費精算(交際費)	39.5%	42.3%	43.2%	32.6%	26.3%	37.9%
請求処理	38.6%	40.6%	43.7%	40.0%	36.0%	40.1%
受発注処理	29.8%	30.5%	32.7%	28.8%	22.8%	29.5%
契約書の締結、保管	35.8%	35.1%	40.2%	32.1%	25.4%	34.5%
社内決裁処理	38.6%	33.5%	40.7%	33.5%	26.3%	35.2%
内部依頼・報告書類(作業依頼、業務報告など)	29.8%	24.7%	27.6%	24.2%	16.7%	25.4%
取締役会議事録などの書類管理	17.2%	18.4%	20.6%	16.7%	11.4%	17.4%
勤怠管理	20.9%	23.0%	27.6%	29.8%	22.8%	24.9%
その他の紙による書類管理	1.4%	0.4%	0.0%	1.4%	4.4%	1.2%

Q13_2：電子インボイスへの対応状況

質問：あなたの勤務先では、消費税インボイス制度への対応について検討を進めていますか？

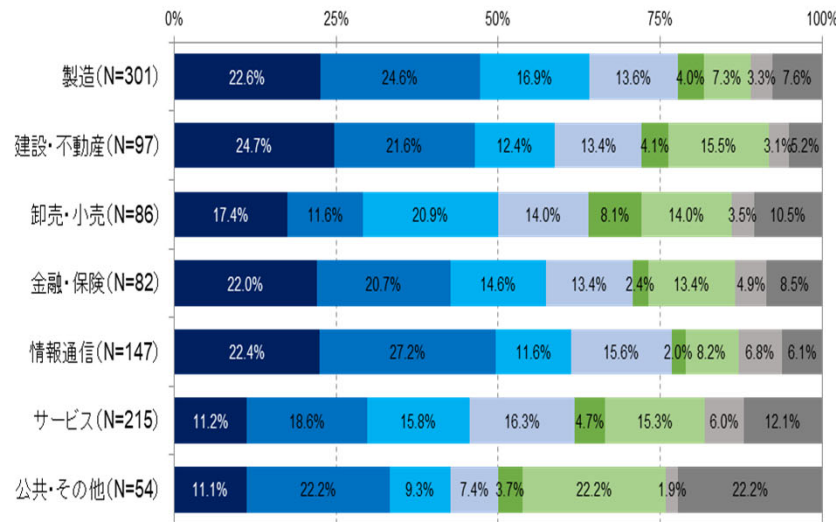
- 電子インボイスについては、国際標準仕様適用が約2割、国内標準仕様検討が約2割となっているが、利用は決まっているがシステムは決まっていないと導入検討中も1割以上あり、まだ対応はバラバラで収束傾向にはなっていない。



Q13_2 : 電子インボイスへの対応状況 (業種別・規模別)

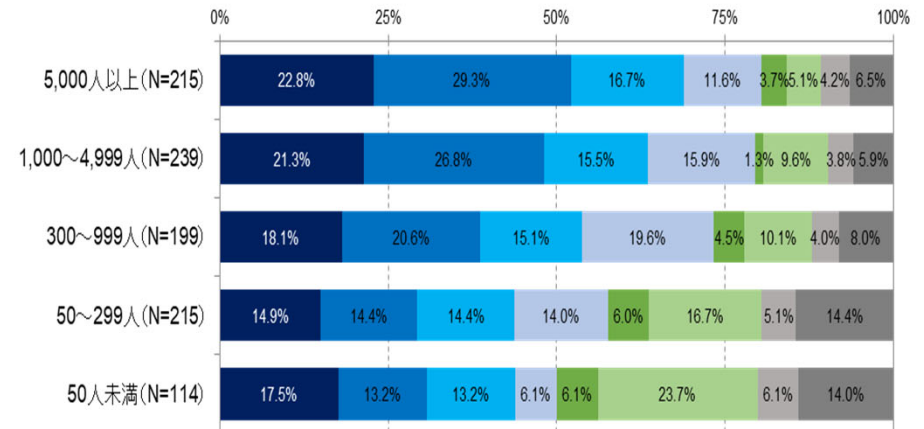
- 業種別では、電子インボイスを導入しようとしている比率は製造、情報通信が高い
- 規模別では規模が小さくなると紙での対応の比率が高くなる

業種別



- 電子インボイスの利用が決まっており、(国際標準仕様「Peppol」を基とした)
- 国内標準仕様(EIPA)の導入を検討している
- 電子インボイスの利用は決まっているが、システムの導入までは決まっていない
- 電子インボイスの導入を検討している
- 紙でのやり取りを考えている
- まだ検討していない
- 制度の概要がわからない
- 対象ではない

規模別

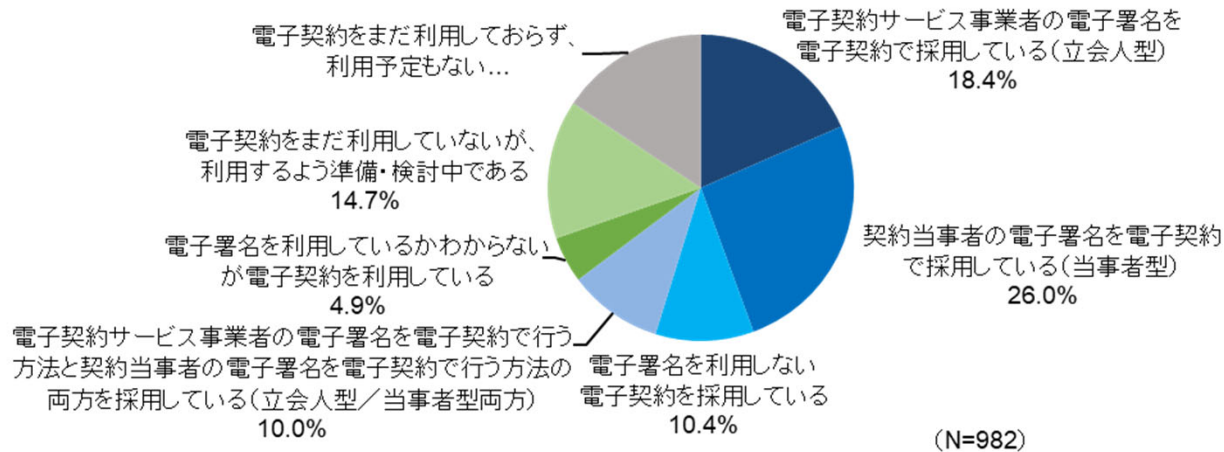


- 電子インボイスの利用が決まっており、(国際標準仕様「Peppol」を基とした)
- 国内標準仕様(EIPA)の導入を検討している
- 電子インボイスの利用は決まっているが、システムの導入までは決まっていない
- 電子インボイスの導入を検討している
- 紙でのやり取りを考えている
- まだ検討していない
- 制度の概要がわからない
- 対象ではない

Q13_3：取引文書に関する電子契約を利用状況(2022年)

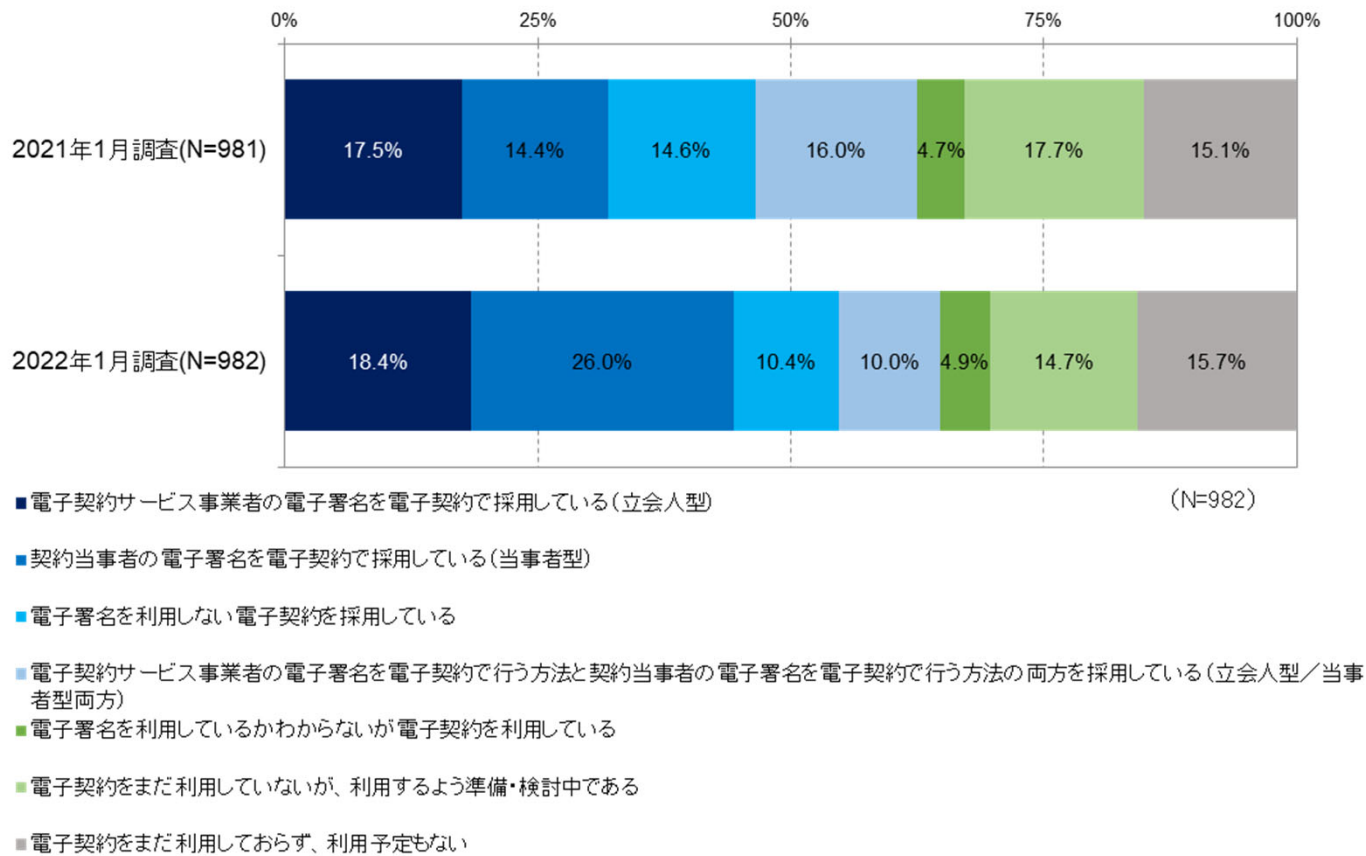
質問：あなたの勤務先における電子契約の利用状況はどのようになっていますか？

- 電子契約の利用状況では、電子署名の当事者型が最も多く、電子署名の立会人型が続き、両方利用や電子署名利用せず、不明を入れると約 7 割が利用している。



Q13_3 : 取引文書に関する電子契約を利用状況(前回との比較)

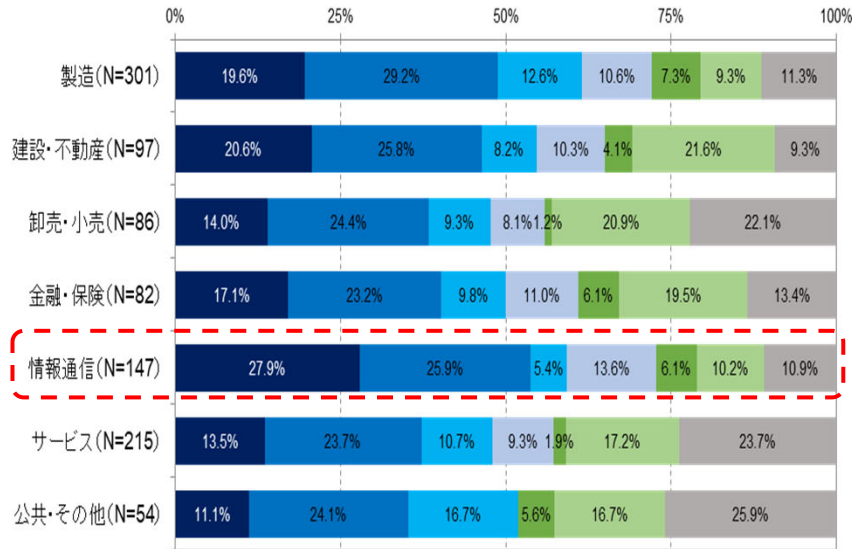
■ 前回との比較では、電子署名の当事者型が1割以上増加しているが、利用率としては微増である。



Q13_3 : 取引文書に関する電子契約を利用状況(業種別・規模別)

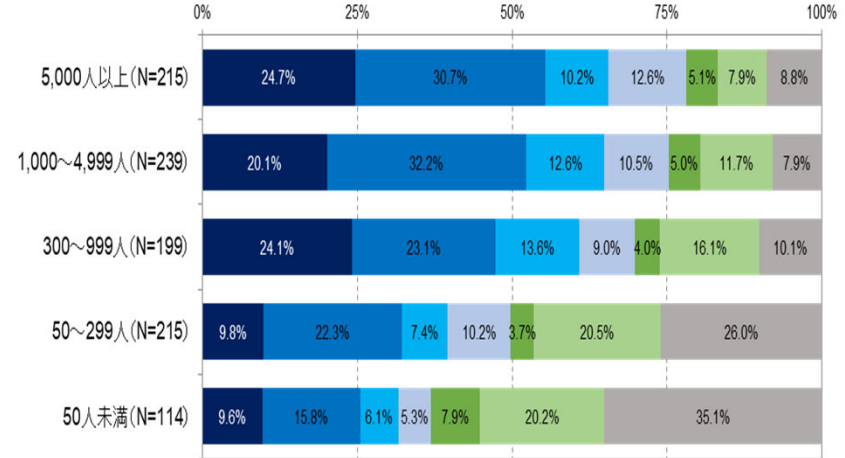
- 業種別では、情報通信は電子署名立会人型が多く、利用率としては製造と情報通信が高い
- 規模別では、規模が大きいほど利用率が高くなっている

業種別



- 電子契約サービス事業者の電子署名を電子契約で採用している (立会人型)
- 契約当事者の電子署名を電子契約で採用している (当事者型)
- 電子署名を利用しない電子契約を採用している
- 電子契約サービス事業者の電子署名を電子契約で行う方法と契約当事者の電子署名を電子契約で行う方法の両方を採用している (立会人型/当事者型両方)
- 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
- 電子契約をまだ利用していないが、利用するよう準備・検討中である
- 電子契約をまだ利用しておらず、利用予定もない

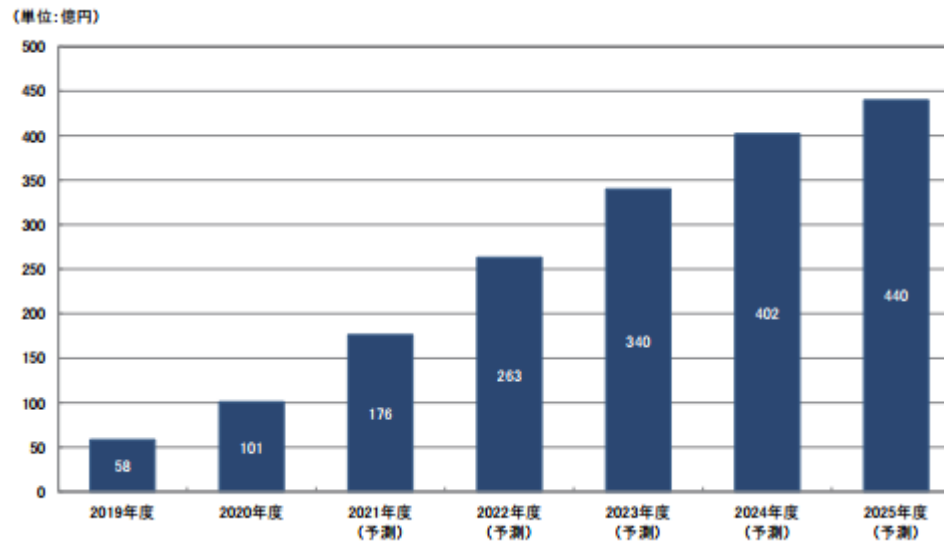
規模別



- 電子契約サービス事業者の電子署名を電子契約で採用している (立会人型)
- 契約当事者の電子署名を電子契約で採用している (当事者型)
- 電子署名を利用しない電子契約を採用している
- 電子契約サービス事業者の電子署名を電子契約で行う方法と契約当事者の電子署名を電子契約で行う方法の両方を採用している (立会人型/当事者型両方)
- 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
- 電子契約をまだ利用していないが、利用するよう準備・検討中である
- 電子契約をまだ利用しておらず、利用予定もない

【ご参考】ITR 電子契約市場予測

- 国内の電子契約市場は政府の後押しもあり、年平均市場成長率は34.3%と驚異的な伸びが予測されている。

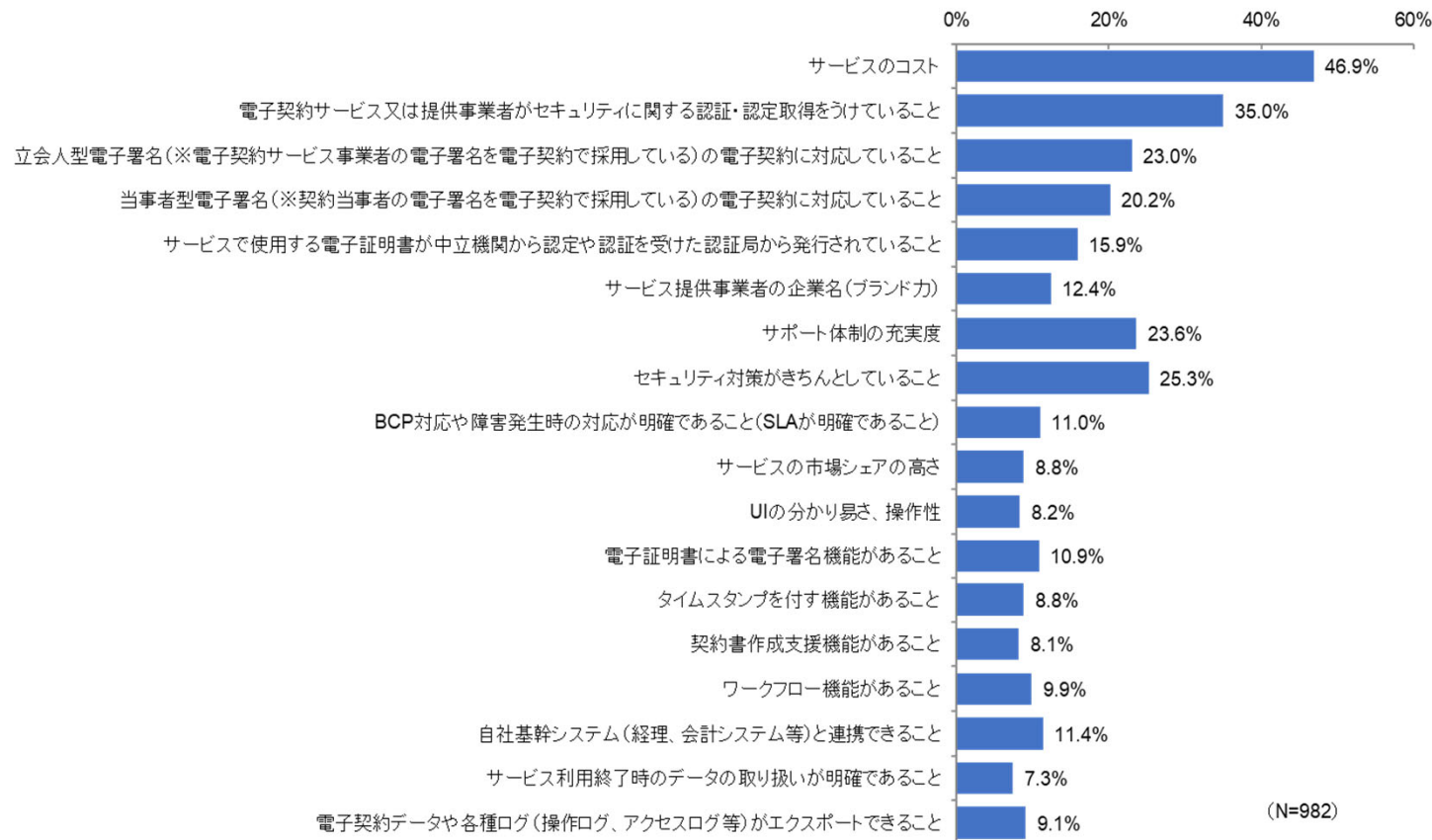


(出典：ITR Market View：ECサイト構築／CMS／SMS送信サービス／CLM／電子契約サービス市場2021)

Q13_4：電子契約を導入する際に重視するポイント

質問：あなたの勤務先で電子契約サービスを選定、導入する際に重視するポイントで当てはまるものをすべて選んでください。

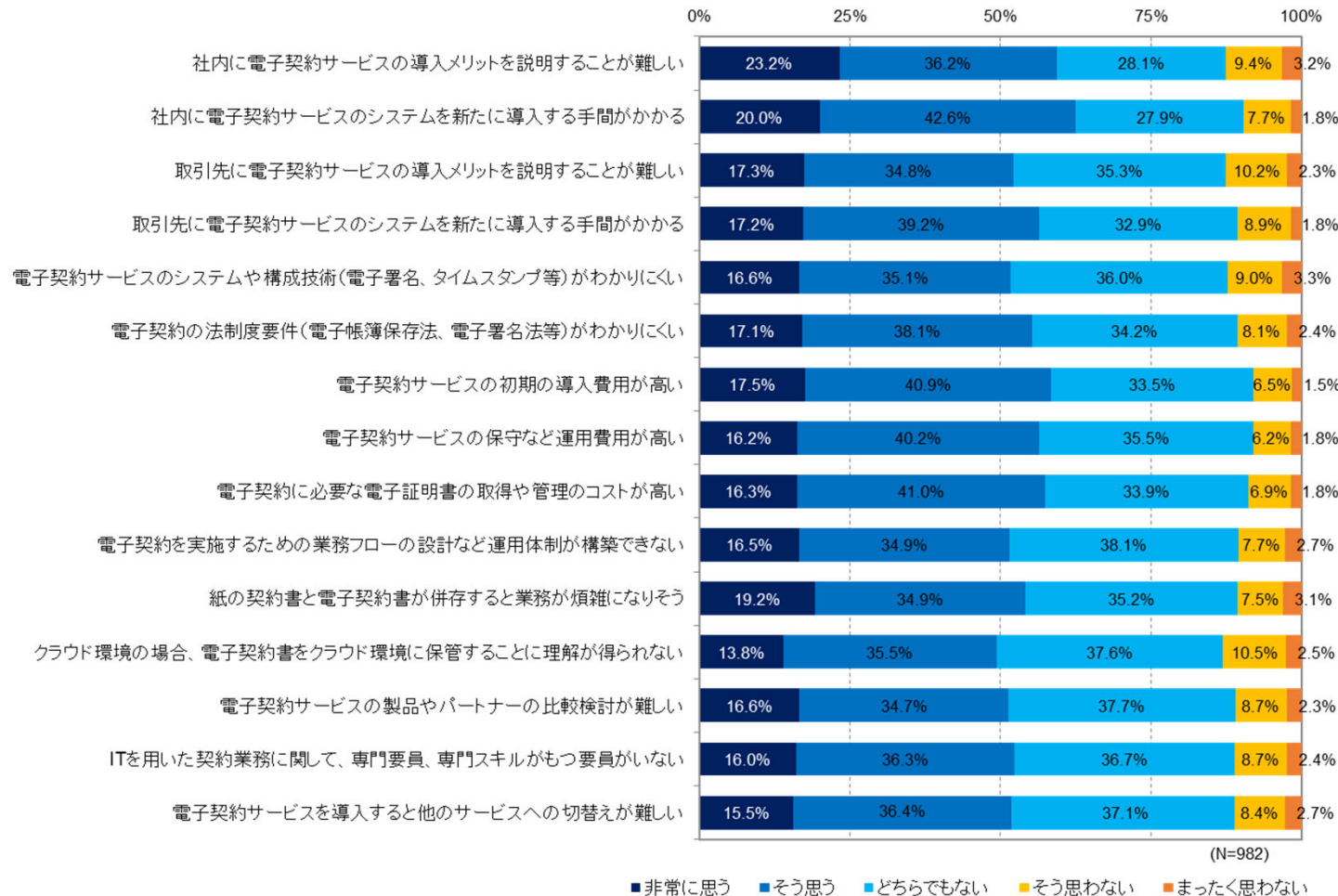
- 電子契約を導入する際に重視するポイントとしてサービスコストが一番で、サービス事業者がセキュリティ認証・認定の取得しているかセキュリティ対策が行われているかが続き、次はサポート体制の充実度があげられている。



Q13_5：電子契約の利用拡大図る上での課題

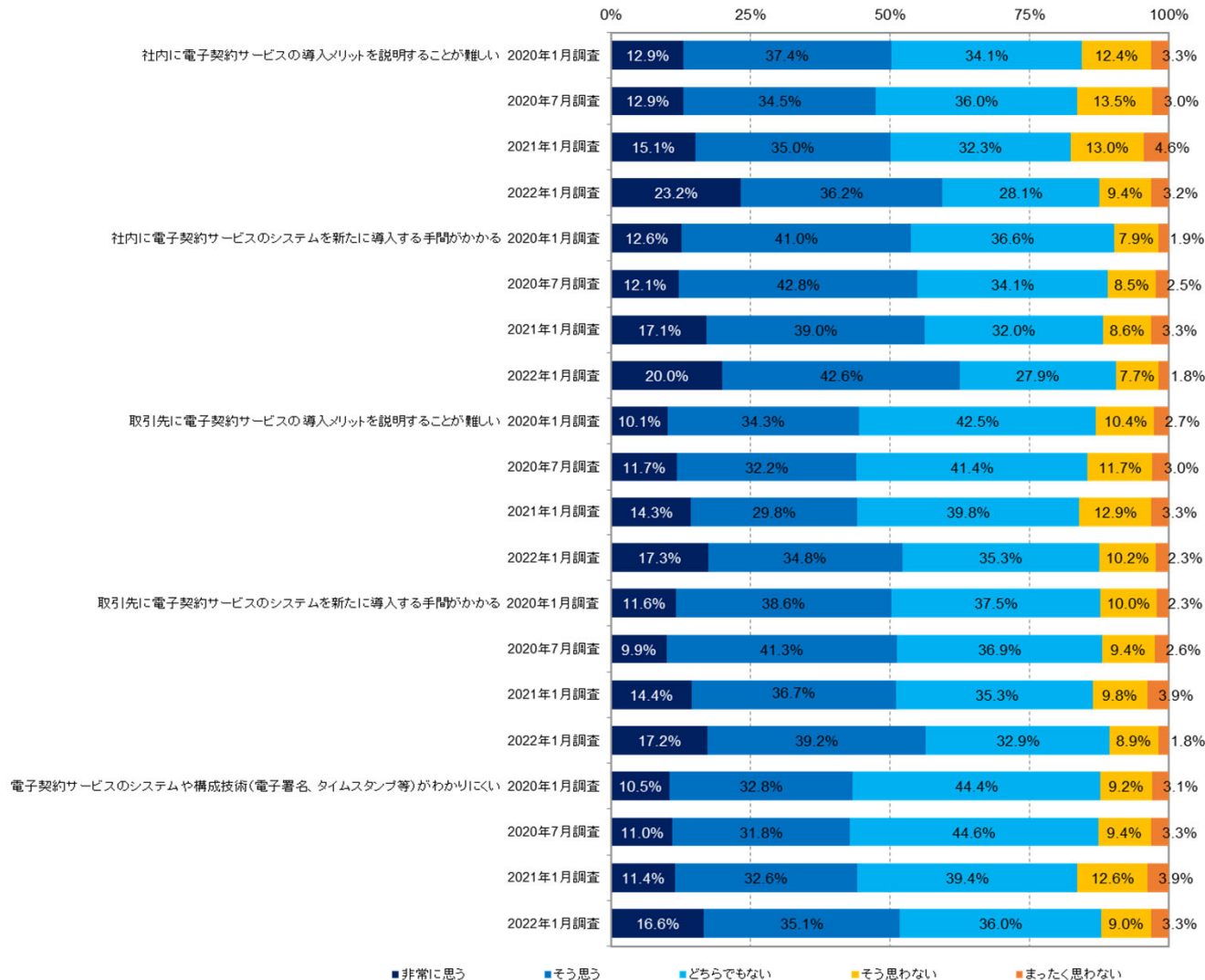
質問：あなたの勤務先において、電子契約の採用や利用拡大を図るうえで課題だと思うものは何ですか？

- 課題として非常に思うが多かったのは、導入メリットを説明することが難しいことと手間がかかることが2割を超えているが全体的には分散している。そう思うを含めても分散傾向があり突出した課題は見られない。



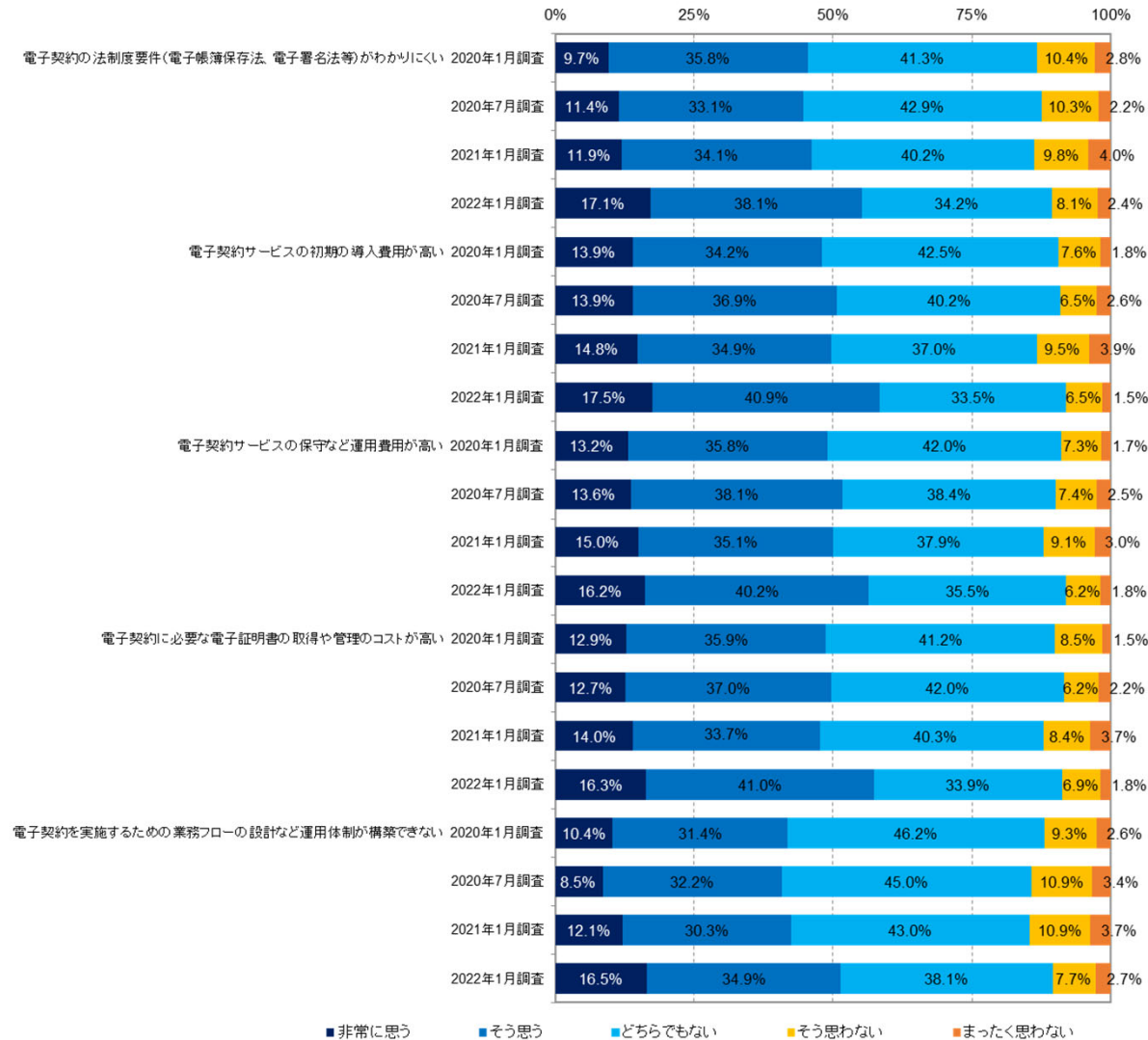
Q13_5 : 電子契約の利用拡大図る上での課題 (過去3回との比較、1/3)

- 過去3回との比較では、導入メリットを説明することが難しいが大きく伸びており、手間がかかるも伸びており、導入検討のケースが増えていることが推測される。



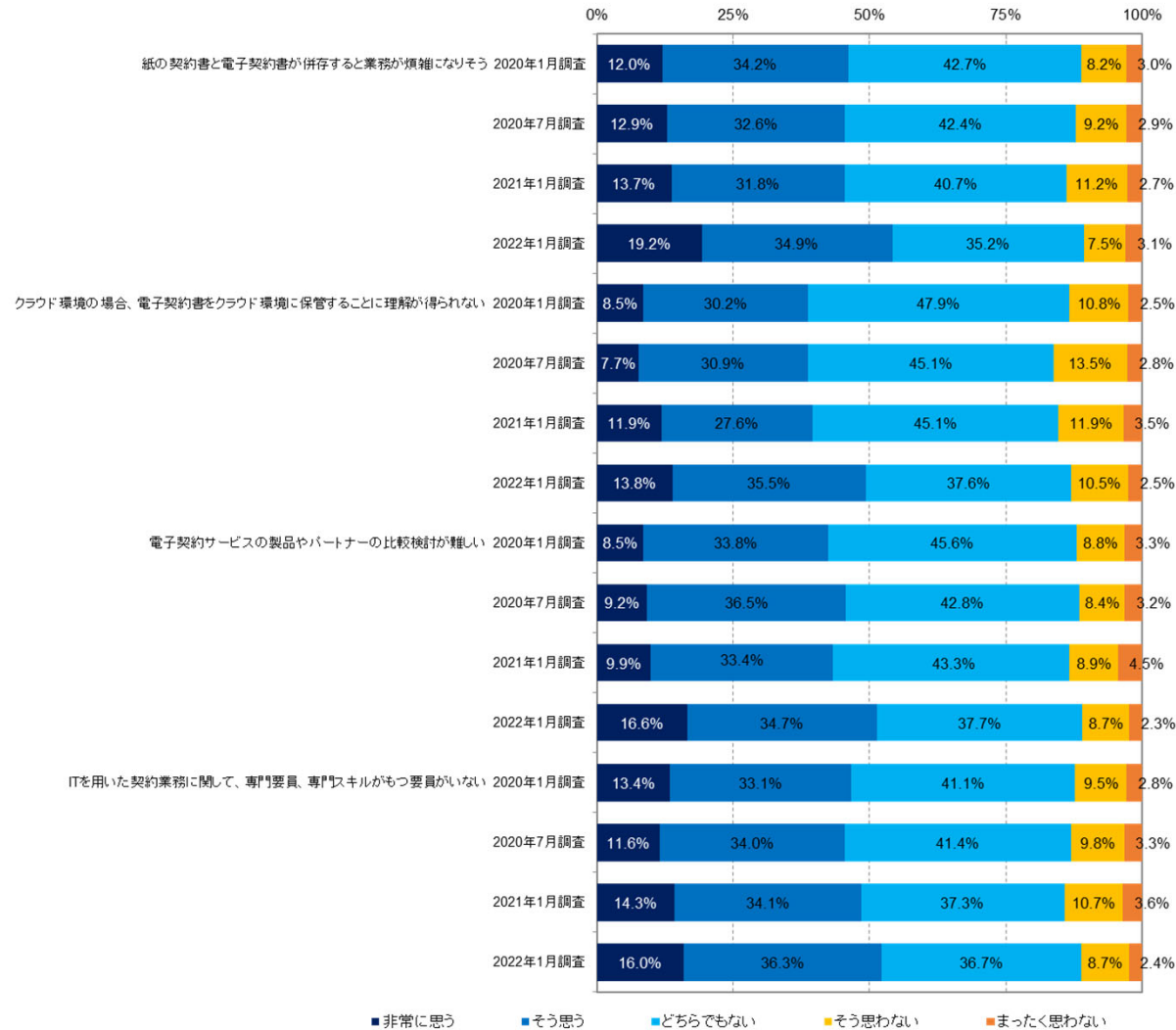
Q13_5 : 電子契約の利用拡大を図る上での課題（過去3回との比較、2/3）

- 過去3回との比較では、法制度要件がわかりにくい、コストが高い、運用体制が構築できないが、いずれも伸びており、導入検討のケースが増えていることが推測される。



Q13_5 : 電子契約の利用拡大図る上での課題 (過去3回との比較、3/3)

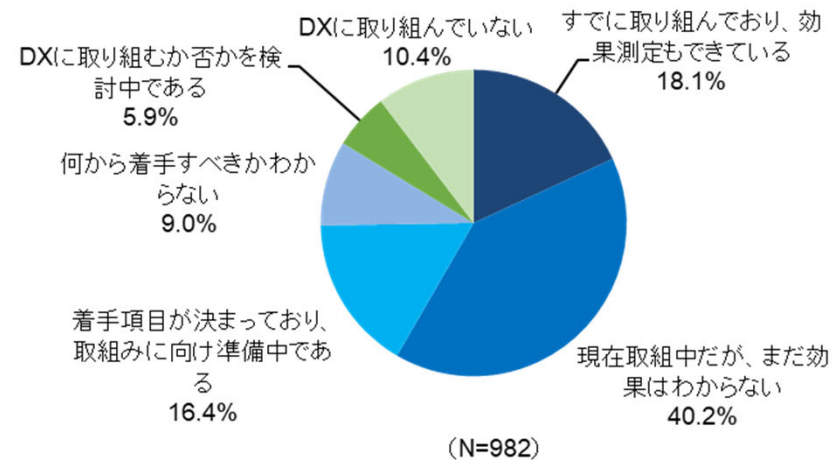
■ 過去3回との比較では、いずれも非常に思うやそう思うが増えており、導入検討が進んでいると推測される。



Q14_1: デジタルトランスフォーメーション (DX) の推進状況

質問：あなたの勤務先ではデジタルトランスフォーメーション (DX) 推進に向けて取り組んでいますか

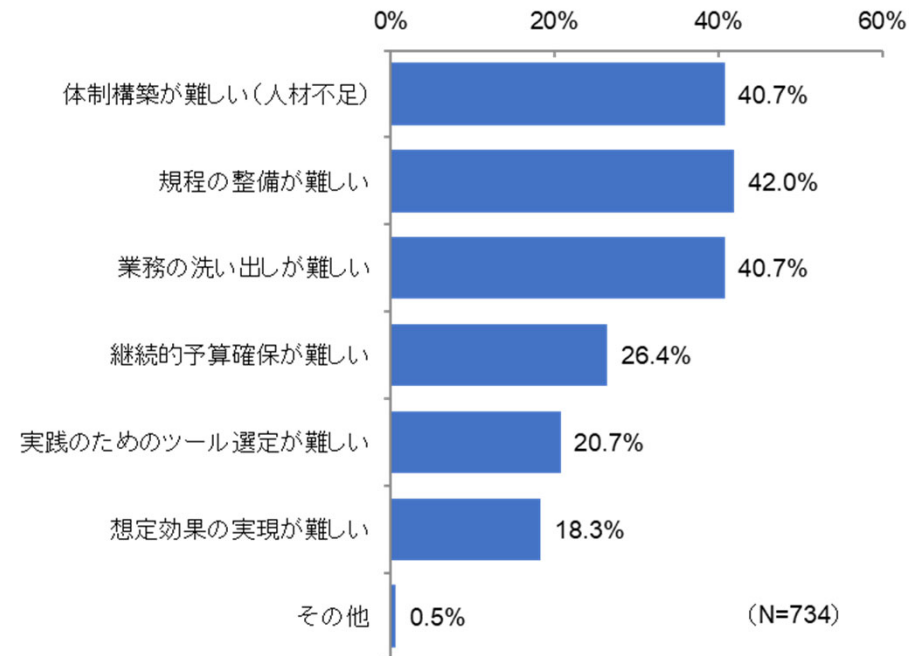
- 取り組みは開始しているが効果は不明が最も多く、効果がでている、着手準備中が続く。



Q14_2:DXを推進するにあたっての課題

質問：あなたの勤務先でのDX推進にあたっての課題は何ですか？

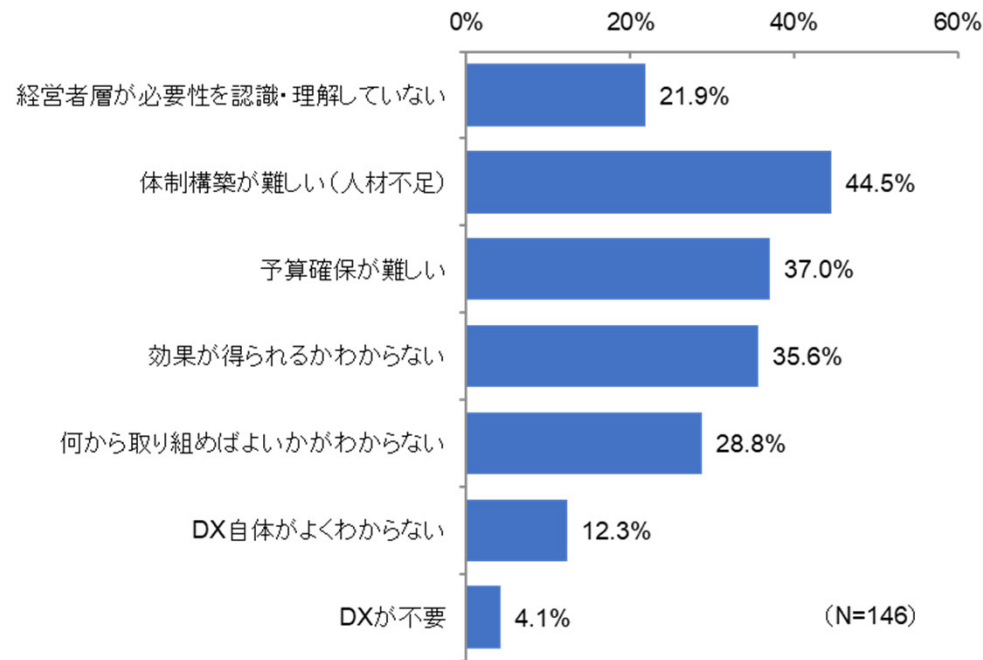
- DX推進しようとしている企業の課題としては、規程の整備が難しい、体制構築が難しい、業務の洗い出しが難しいが4割を超えており、主な推進課題と言える。



Q14_3:DXへの取り組みについての課題

質問： DX取組みにあたっての課題は何ですか？

- 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、予算確保が難しい、効果が得られるかわからないが3割を超えており、主な課題と言える。



総括

コロナ禍も3年目を迎え、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が確立してきており、新しい環境下での新事業創出が課題とされてきている。

新たなデジタルワークスタイルにおいて取引先や顧客の信頼を得るためにはセキュリティの第三者認定／認証の取得維持がますます重要になってくる。

長期間のコロナ禍に対応して企業ではテレワークとクラウド利用が通常勤務形態となり、クラウド利用のためのセキュリティ対策が進めなければならない。

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になり、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。

