



# 企業IT利活用動向調査2026 集計結果

2026年4月15日

一般財団法人日本情報経済社会推進協会

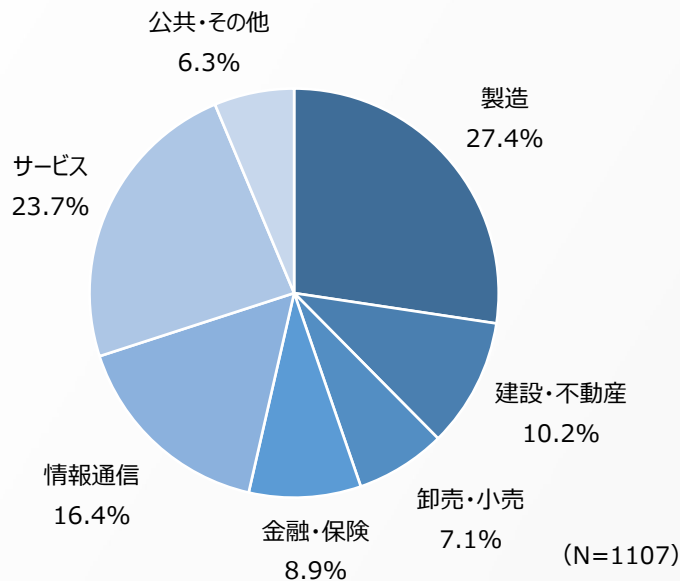
調査協力：株式会社アイ・ティ・アール

# 調査概要

- 調査名 : 企業IT利活用動向調査2026
- 調査期間 : 2026年1月16日～1月20日
- 調査方法 : ITR独自パネルユーザーに対する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50名以上の国内企業の勤務者
  - 情報システム、経営企画、総務・人事、業務改革・業務推進関連、DX推進関連のいずれかに関する業務の担当者
  - IT戦略策定または情報セキュリティの従事者
  - 係長（主任）相当職以上の役職者
- 有効回答数 : 1,107件（1社1回答）

# 回答者プロフィール①

## 業種（大分類）

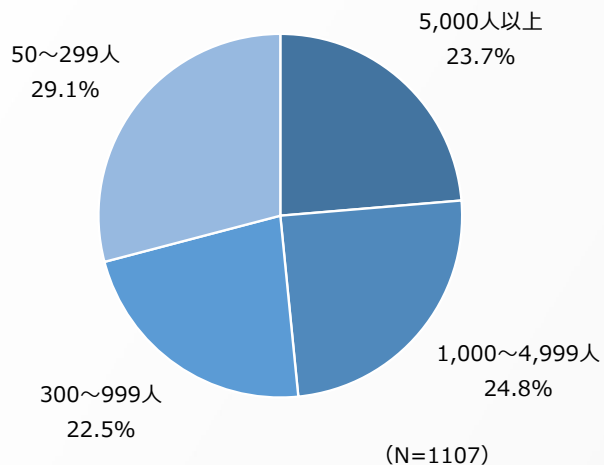


## 業種詳細

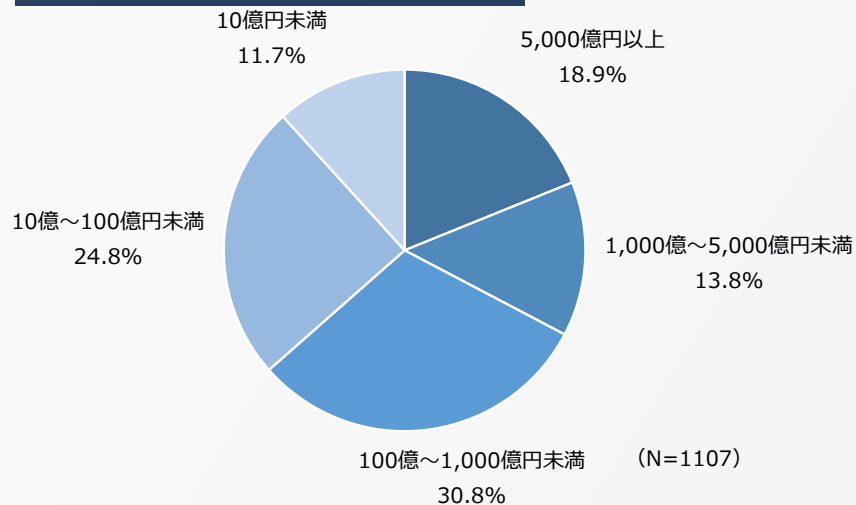
大分類	詳細	回答数	構成比	
製造	食品・飲料	42	3.8%	
	日用品・生活雑貨	19	1.7%	
	繊維	13	1.2%	
	パルプ・紙・印刷	13	1.2%	
	化学工業	10	0.9%	
	石油製品	5	0.5%	
	鉄鋼・金属	28	2.5%	
	プラスチック・ゴム	4	0.4%	
	機械	22	2.0%	
	電気機器	32	2.9%	
	情報通信機器	14	1.3%	
	電子部品・電子回路	18	1.6%	
	精密機器	16	1.4%	
	自動車・輸送機器	42	3.8%	
医薬品	12	1.1%		
その他の製造業	13	1.2%		
建設・不動産	建設	61	5.5%	
	不動産	46	4.2%	
	住宅	6	0.5%	
卸売・小売	卸売	28	2.5%	
	小売	25	2.3%	
	商社	26	2.3%	
金融・保険	銀行	61	5.5%	
	証券	5	0.5%	
	生命保険	10	0.9%	
	損害保険	11	1.0%	
	その他金融	11	1.0%	
情報通信	通信	26	2.3%	
	ITベンダー／システムインテグレーター	115	10.4%	
	インターネット・サービス	27	2.4%	
	情報システム子会社	14	1.3%	
サービス	電力・ガス・水道	26	2.3%	
	運輸	38	3.4%	
	倉庫	8	0.7%	
	宿泊	4	0.4%	
	飲食	14	1.3%	
	娯楽・レジャー	11	1.0%	
	メディア・出版・放送・広告	6	0.5%	
	生活関連サービス（旅行業など）	7	0.6%	
	医療	46	4.2%	
	福祉・介護	32	2.9%	
	教育（学校以外）	21	1.9%	
	人材派遣・業務委託	19	1.7%	
	その他サービス	30	2.7%	
	公共・その他	学校	19	1.7%
		官公庁	14	1.3%
地方自治体		24	2.2%	
その他公共機関		5	0.5%	
農業・水産・鉱業		3	0.3%	
その他の業種		5	0.5%	
合計			1,107	100.0%

# 回答者プロフィール②

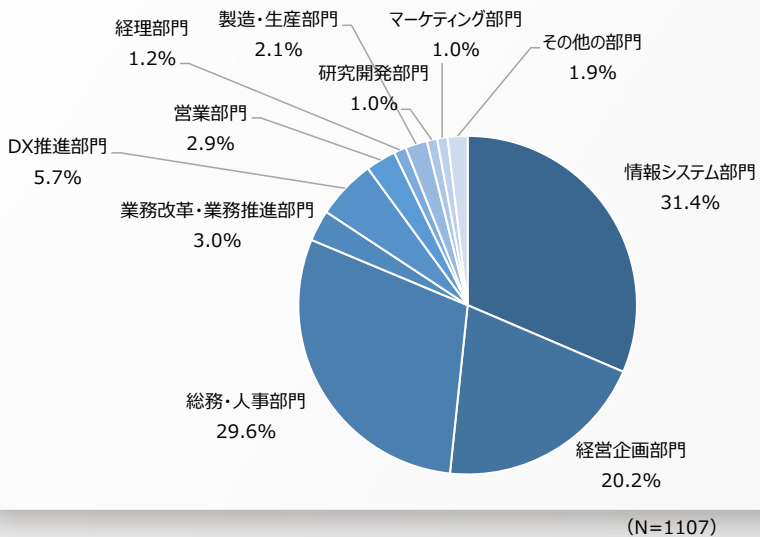
## 従業員規模



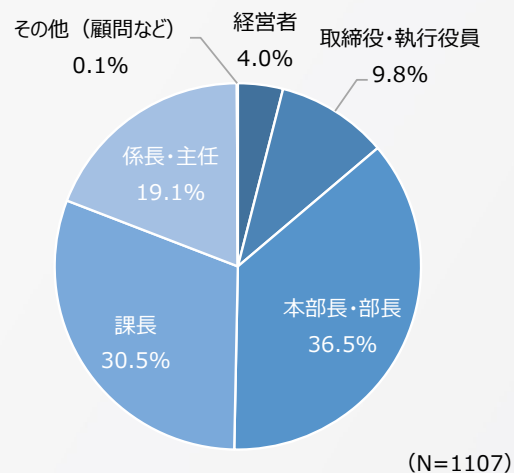
## 年間売上規模



## 所属部門

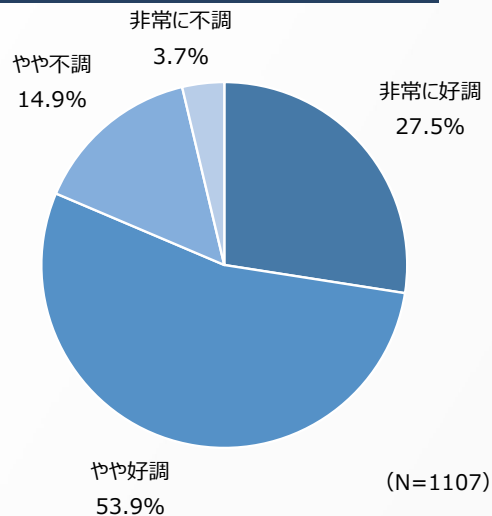


## 役職

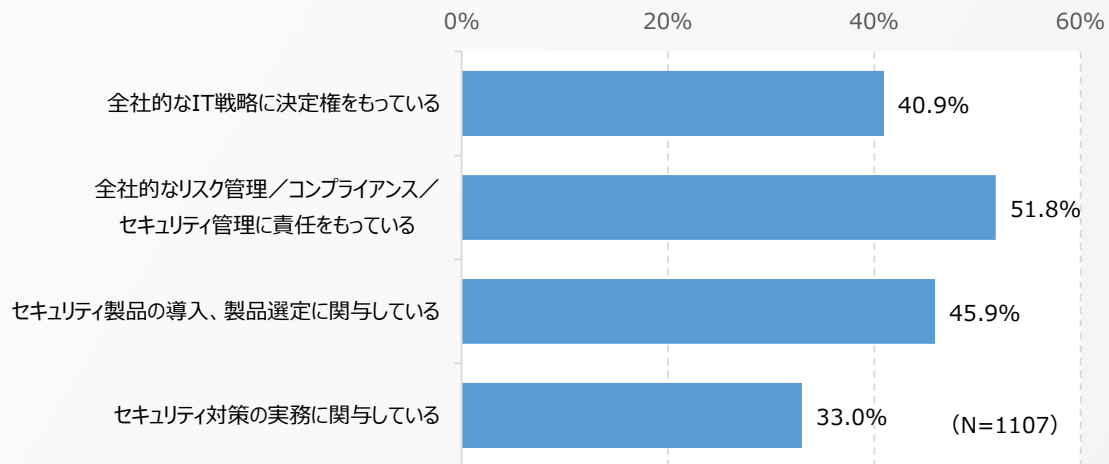


# 回答者プロフィール③

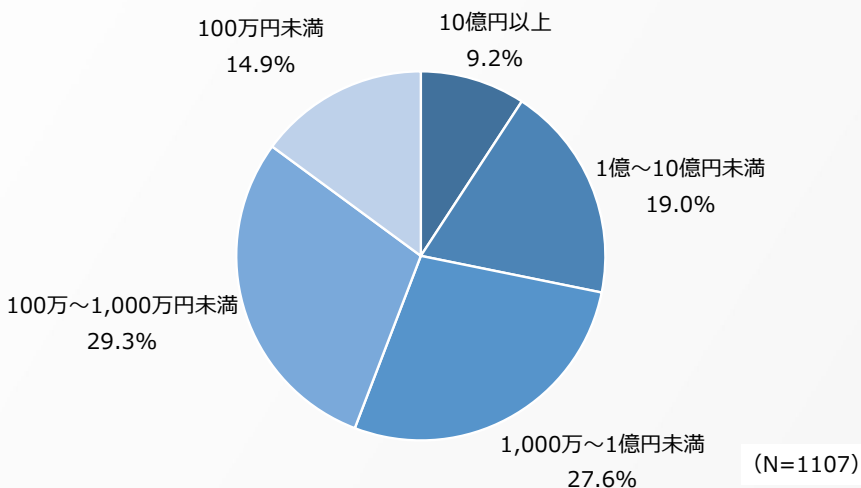
## ビジネス環境



## IT戦略／セキュリティへの関与度

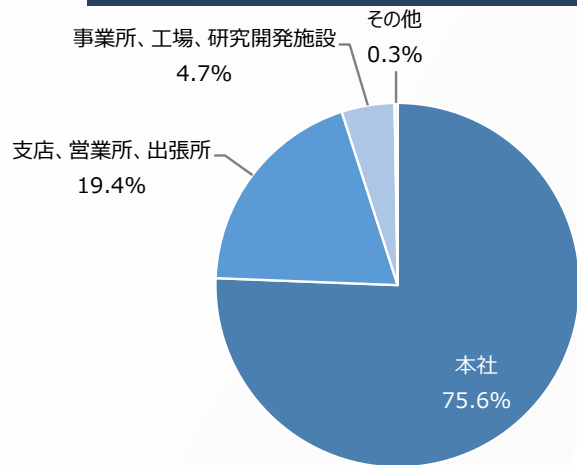


## 年間セキュリティ投資額



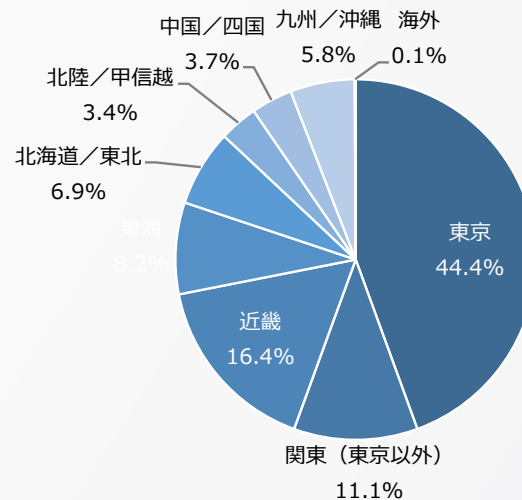
# 回答者プロフィール④

## 勤務している組織形態



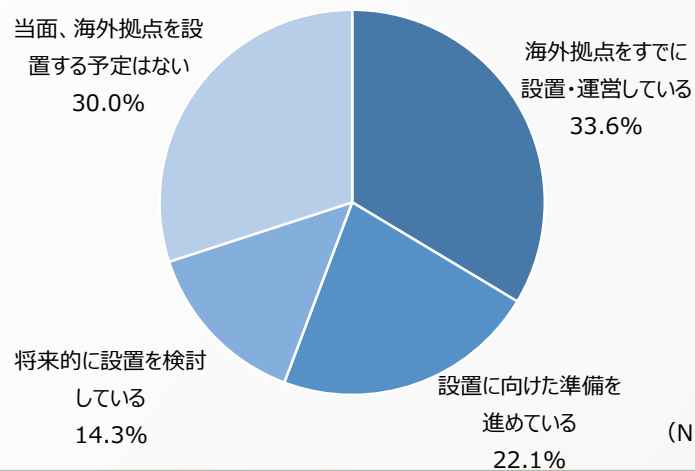
(N=1107)

## 本社の所在地



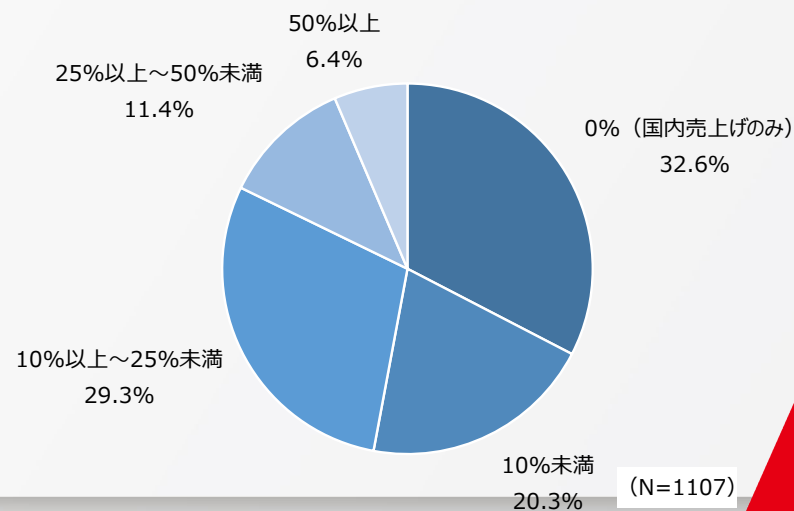
(N=1107)

## 海外拠点の設置状況



(N=1107)

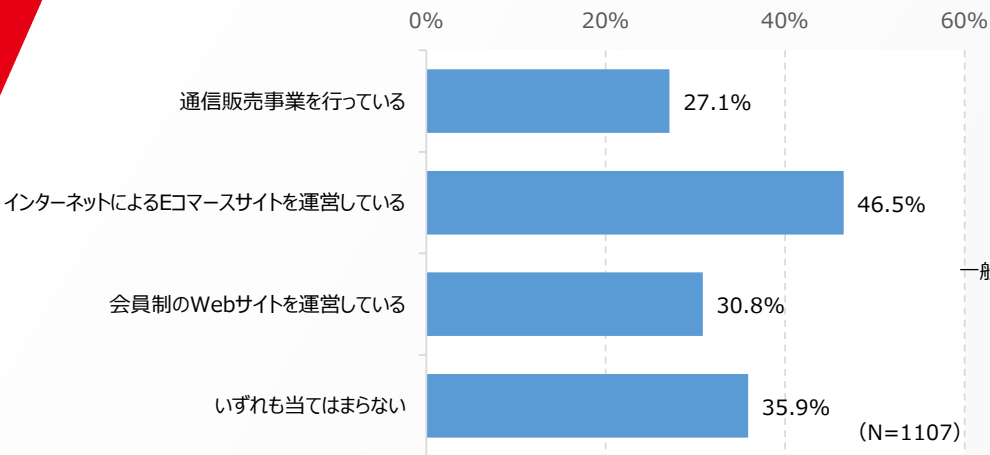
## 海外売上比率



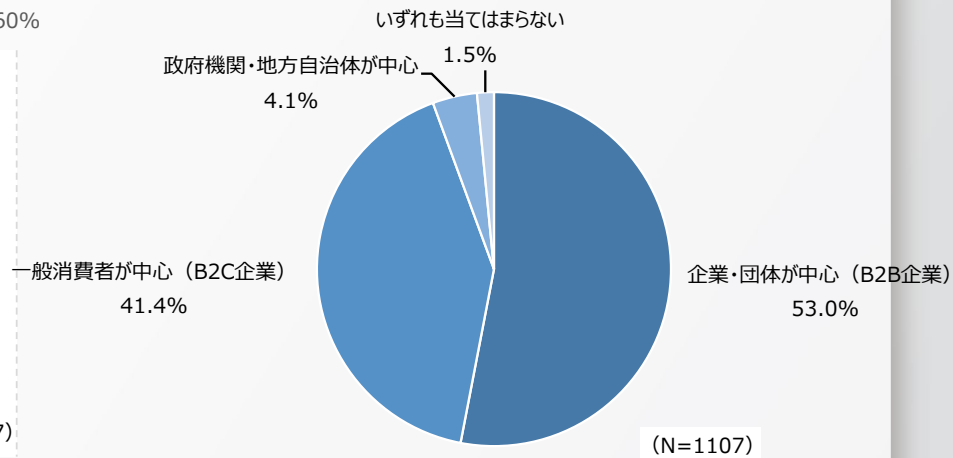
(N=1107)

# 回答者プロフィール⑤

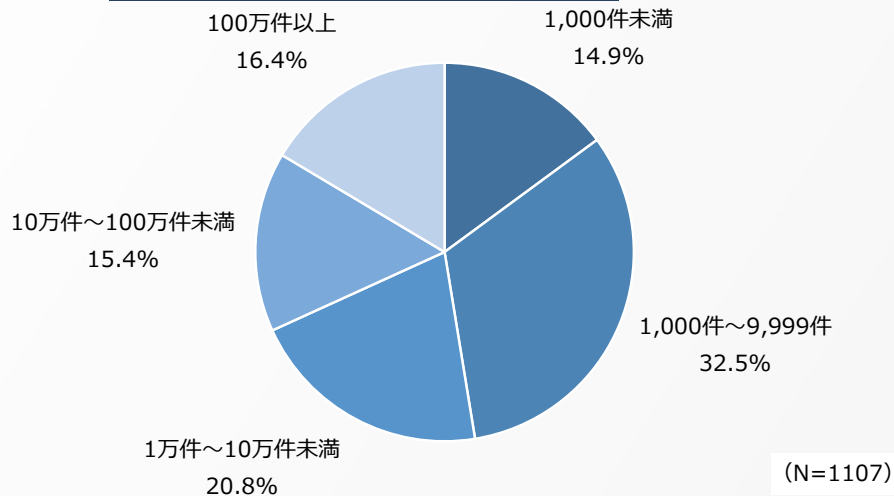
## 事業形態



## 顧客・取引先



## 個人情報の保有件数



# 1

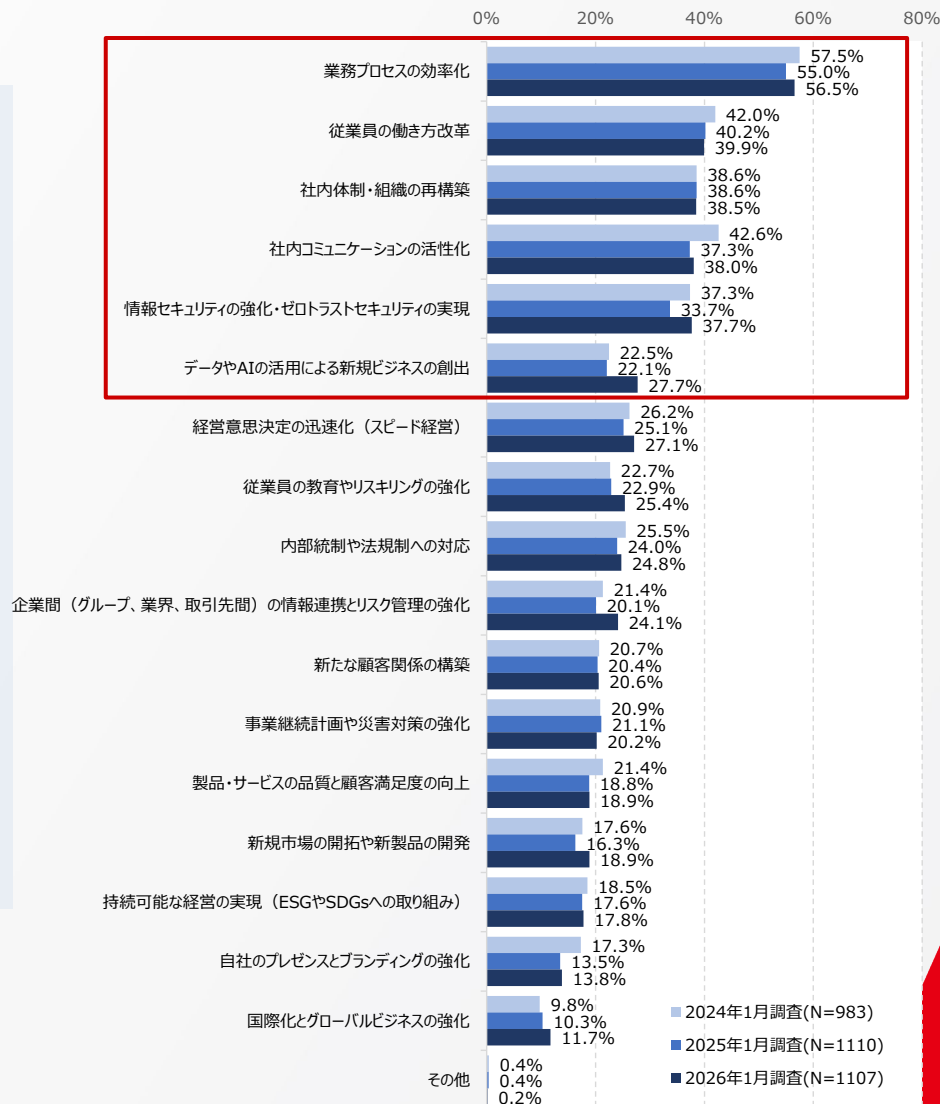
## 企業の経営課題

- Q1\_1 重視する経営課題
- Q1\_2 経営施策に対する投資状況
- Q1\_3 テレワークの実施状況

# Q1\_1 重視する経営課題

Q：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。当てはまるものをすべてお答えください。（MA）

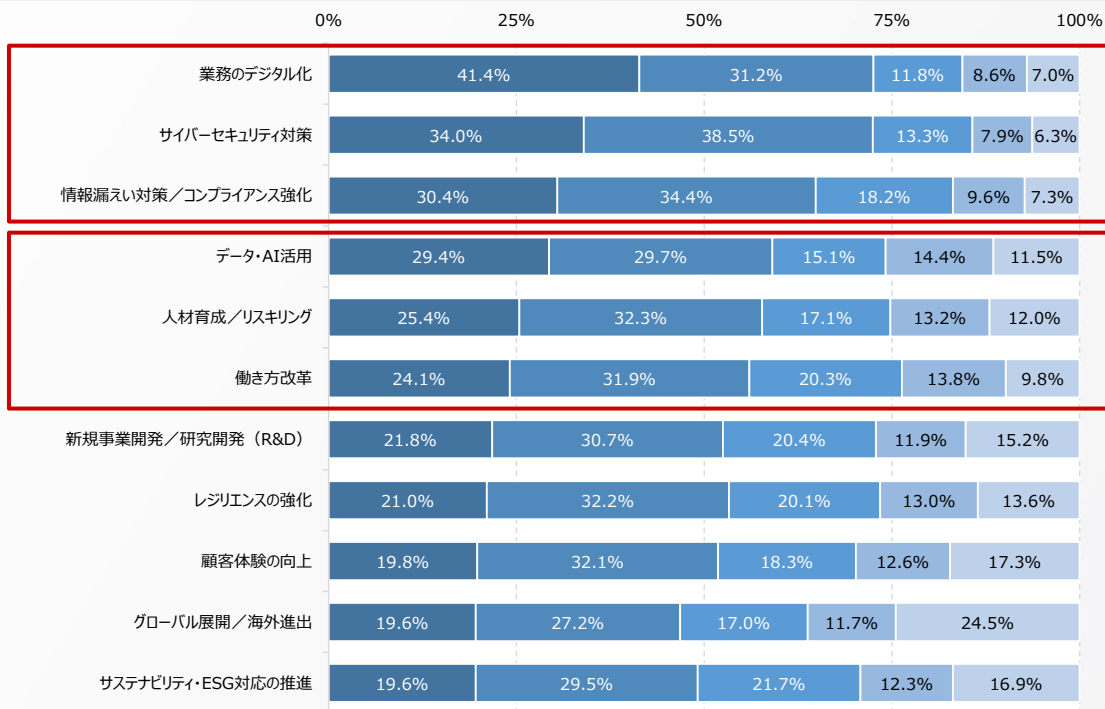
- 業務プロセスの効率化は前回調査から微増し、引き続き最上位を維持している。働き方改革や組織再構築、社内コミュニケーションも大きな変動は見られず、多くの企業が成長投資よりも、人材不足やコスト増を背景とした既存業務・組織基盤の安定化を継続的に重視していることがうかがえる。
- 情報セキュリティの強化・ゼロトラストセキュリティの実現は、前回調査から上昇している。サイバー攻撃や情報漏えいリスクの高まりを受け、セキュリティ対策が個別のIT施策ではなく、事業継続や企業価値を守るための恒常的な経営課題として位置付けられつつある。
- データやAIの活用による新規ビジネスの創出は、前回調査から伸びが見られるものの、依然として中位にとどまっている。関心は着実に高まっている一方で、効率化やリスク対応に比べると優先度は相対的に低く、収益化・事業化に向けた本格的な取り組みはこれからの段階にあることが示唆される。



# Q1\_2 経営施策に対する投資状況

Q：あなたの勤務先において、以下の各経営施策に対する投資状況について最も当てはまるものをお答えください。  
(SA)

- 業務のデジタル化やサイバーセキュリティ、情報漏えい対策では「重点的投資」と「投資継続」の合計が60%を超えており、企業活動の前提となる基盤領域への投資が広く定着し、成熟フェーズに入りつつあることがうかがえる。
- データ・AI活用と人材育成／リスクリングも「重点的投資」割合が高く、中長期的な競争力強化を見据え、将来価値創出に向けた投資を本格化させる企業が増え始めている。

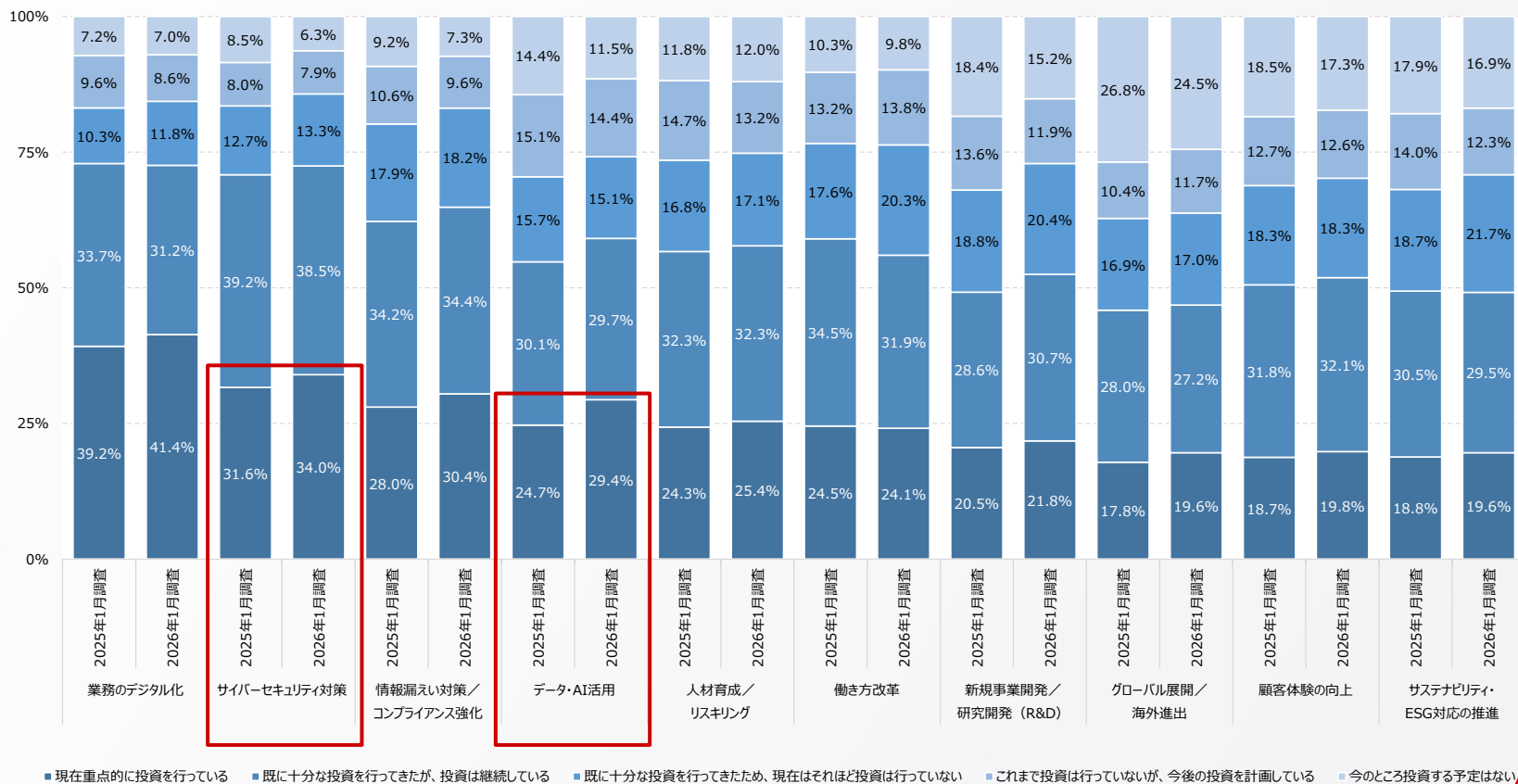


- 現在重点的に投資を行っている
  - 既に十分な投資を行ってきたが、投資は継続している
  - 既に十分な投資を行ってきたため、現在はそれほど投資は行っていない
  - これまで投資は行っていないが、今後の投資を計画している
  - 今のところ投資する予定はない
- (N=1107)

# Q1\_2 経営施策に対する投資状況：前回調査との比較

Q：あなたの勤務先において、以下の各経営施策に対する投資状況について、最も当てはまるものをお答えください。（SA）

- サイバーセキュリティ対策は、「重点的投資」が前回調査より上昇している。2025年はランサムウェア攻撃による被害が社会問題へと発展したこともあり、投資を強化する企業が増えていると見られる。
- データ・AI活用は、全施策の中で「重点的投資」が最も上昇している。AIに対して、競争力強化や将来成長を見据えた本格投資に踏み出す企業が増えていることが示されている。

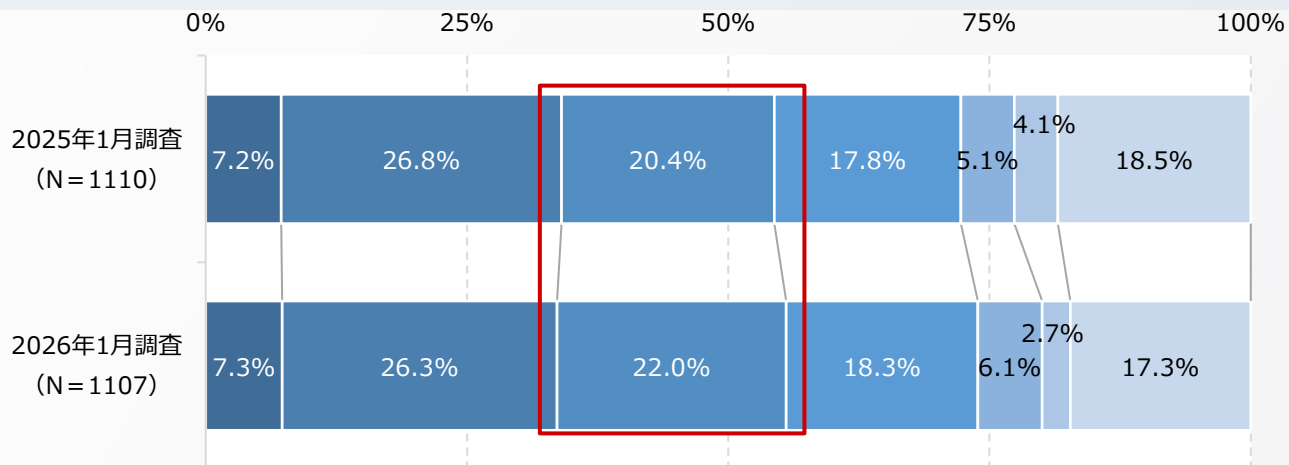


■ 現在重点的に投資を行っている ■ 既に十分な投資を行ってきたが、投資は継続している ■ 既に十分な投資を行ってきたため、現在はそれほど投資は行っていない ■ これまで投資は行っていないが、今後の投資を計画している ■ 今のところ投資する予定はない

# Q1\_3 テレワークの実施状況

Q：あなたの勤務先におけるテレワークの実施状況をお答えください。（SA）

- 「全面的にテレワークが中心」「出社とテレワーク併用（出社比率は強制されない）」は前回調査とほぼ同水準で推移しており、3分の1の企業では、テレワークは一時的対応ではなく、働き方の一つとして定着していることがうかがえる。
- 「併用だが出社日数が決められている」は前回から微増しており、企業側が業務効率やマネジメント、コミュニケーションを重視し、ルールを明確化したハイブリッドワークへ移行する動きが徐々に進んでいる。
- 一方で、「テレワーク制度が活用されておらず出社中心になっている」と「テレワーク制度が廃止されてなくなった」もともに微動しており、テレワーク制度が機能しなくなっている企業も徐々に増えつつある。

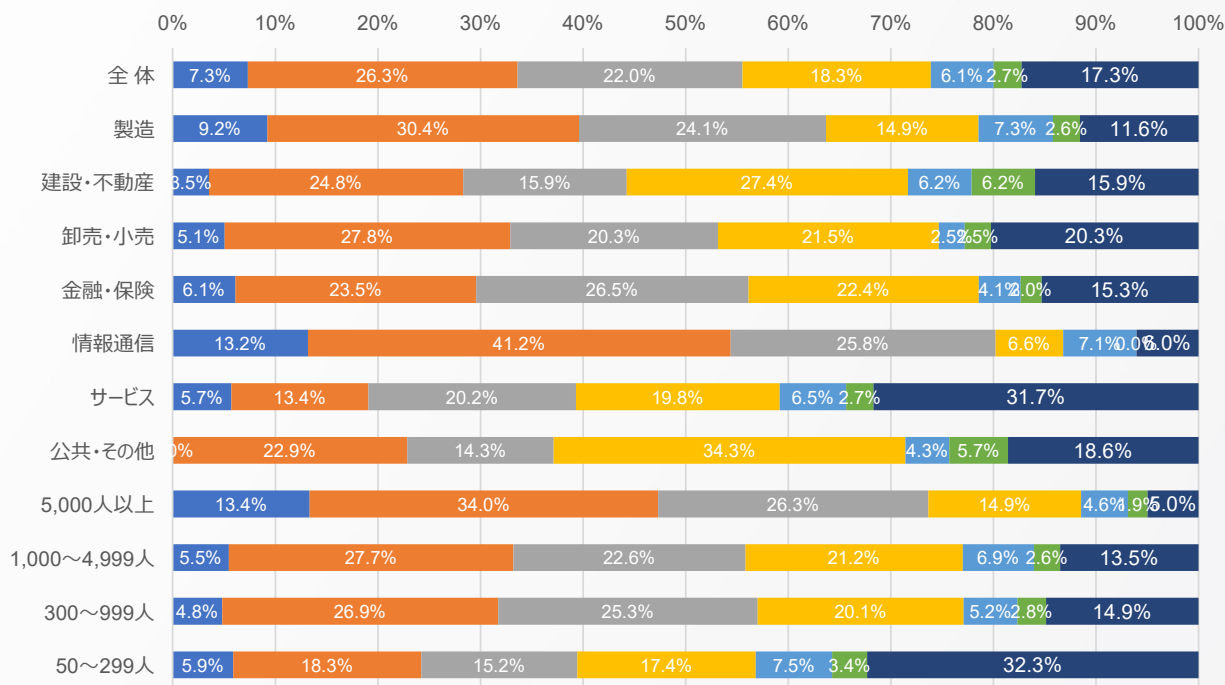


- 全面的にテレワークでの勤務が中心になっている
- 出社とテレワーク併用のハイブリッド勤務で、出社は強制されていない
- 出社とテレワーク併用のハイブリッド勤務で、最低出社日数が決められている
- テレワーク制度はあるがほとんど活用されておらず出社が中心になっている
- 以前テレワークは実施していたが、現在は制度が廃止されてなくなった
- 現在はテレワークを実施していないが、今後の制度の導入を検討している
- テレワーク制度を導入していない（業態的に導入できない場合を含む）

# Q1\_3 テレワークの実施状況：企業属性別

Q：あなたの勤務先におけるテレワークの実施状況をお答えください。（SA）

- 業種別：情報通信はハイブリッド勤務を含めテレワークが主流の働き方になっている。一方、サービスは最もテレワークの実施率が低く、テレワーク制度を導入していない企業も30%を超えている。
- 従業員規模別：規模が大きくなるほどテレワークの実施率が上昇し、5,000人以上では約75%で実施している。



- 全面的にテレワークでの勤務が中心になっている
- 出社とテレワーク併用のハイブリッド勤務で、出社は強制されていない
- 出社とテレワーク併用のハイブリッド勤務で、最低出社日数が決められている
- テレワーク制度はあるがほとんど活用されておらず出社が中心になっている
- 以前テレワークは実施していたが、現在は制度が廃止されてなくなった
- 現在はテレワークを実施していないが、今後の制度の導入を検討している
- テレワーク制度を導入していない（業態的に導入できない場合を含む）

# 2

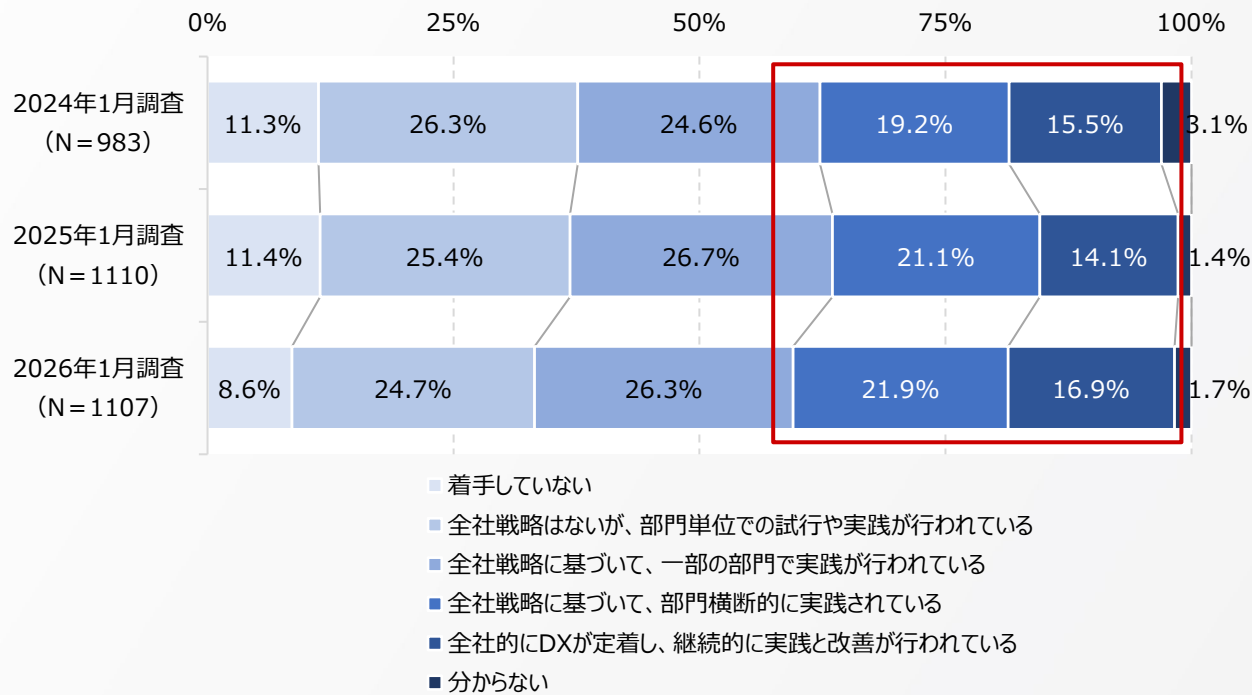
## DXの実践状況

- Q2\_1 DXの実践状況
- Q2\_2 DX成果の測定指標
- Q2\_3 DXの取り組み内容
- Q2\_4 DX実践上の問題

## Q2\_1 DXの実践状況

Q：あなたの勤務先のデジタルトランスフォーメーション（DX）の実践状況について、最も当てはまるものをお答えください。（SA）

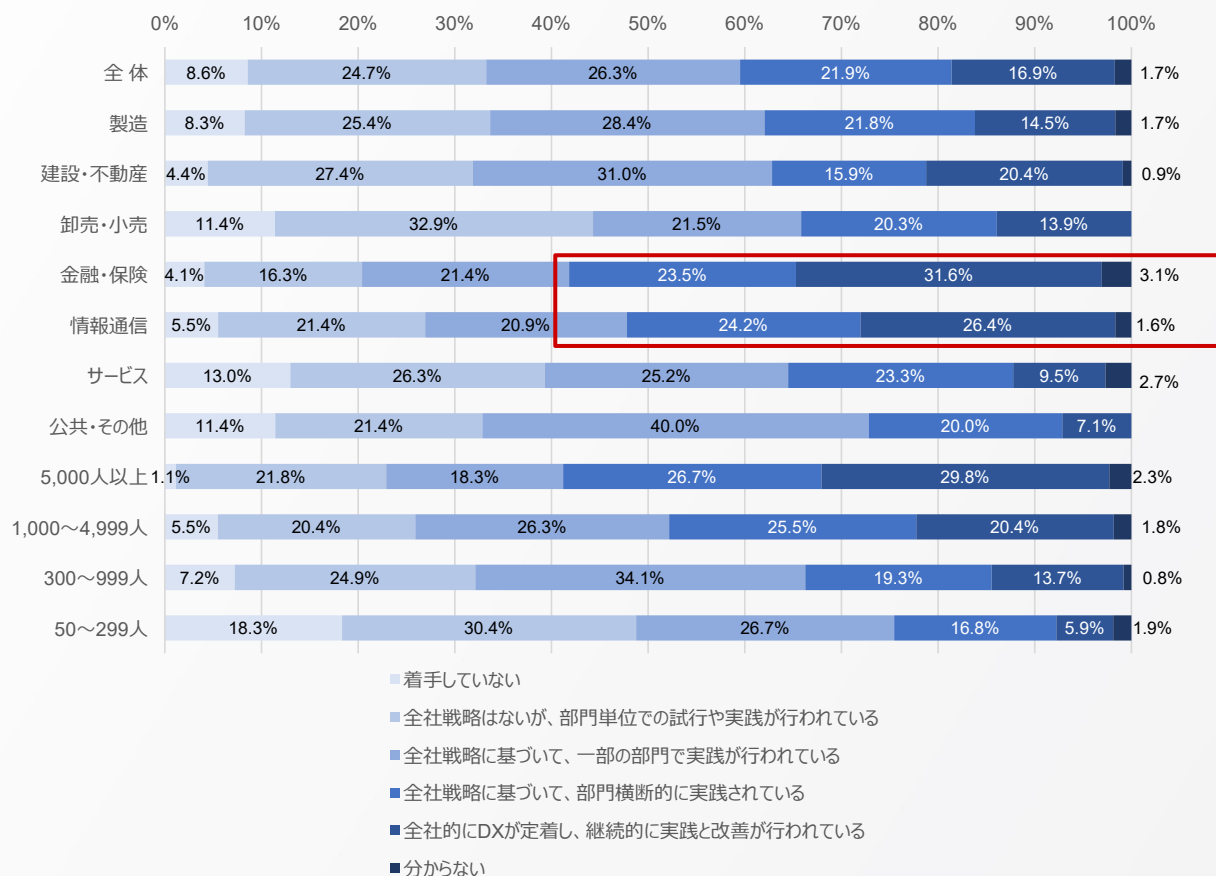
- 「**全社戦略に基づき、部門横断的に実践**」と「**全社的にDXが定着**」の合計比率は2024年から2026年にかけて着実に上昇しており、DXが試行段階から全社展開・定着フェーズへと徐々に進展している状況がうかがえる。
- 一方で、「**着手していない**」「**部門単位での試行・実践**」に該当する企業の割合は徐々に低下しているものの30%は超えており、DXの取り組み状況には企業間でのばらつきが残っている。



## Q2\_1 DXの実践状況：企業属性別

Q：あなたの勤務先のデジタルトランスフォーメーション（DX）の実践状況について、最も当てはまるものをお答えください。（SA）

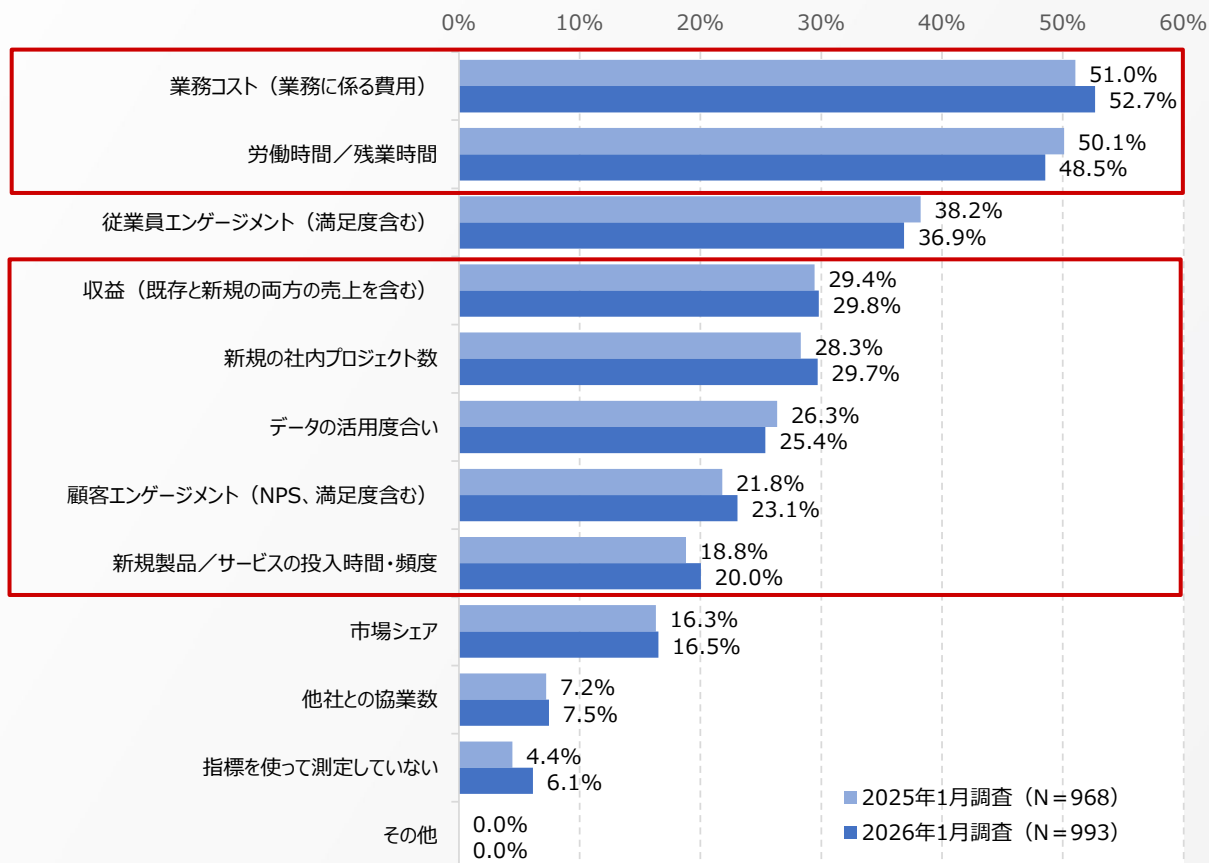
- 業種別：全社的にDXが定着している割合が大きいのは、金融・保険と情報通信となり、DXの実践段階が高い業種となっている。その一方で、サービスと卸売・小売は、遅れをとっている傾向が見られる。
- 従業員規模別：規模に比例して実践段階が上がる傾向にあり、5,000人以上では約30%でDXが定着している。一方、50～299人では、半数弱が未着手か部門単位での試行・実践にとどまっている。



## Q2\_2 DX成果の測定指標

Q：あなたの勤務先ではDXの成果をどのような指標で測定していますか。当てはまるものをすべてお答えください。  
(MA)

- 業務コストや労働時間といった効率性指標は前回調査に引き続き最上位となっている。DXの成果測定は、売上拡大よりも省力化・コスト削減といった短期的かつ定量化しやすい指標に重心が置かれている傾向にある。
- 収益や新規プロジェクト数、顧客エンゲージメント、新製品／サービスの投入時間など、ビジネス成長に直接関わる指標は、微増ながらも上昇傾向が見られる。



## Q2\_2 DX成果の測定指標：DX実践状況別

Q：あなたの勤務先ではDXの成果をどのような指標で測定していますか。当てはまるものをすべてお答えください。  
(MA)

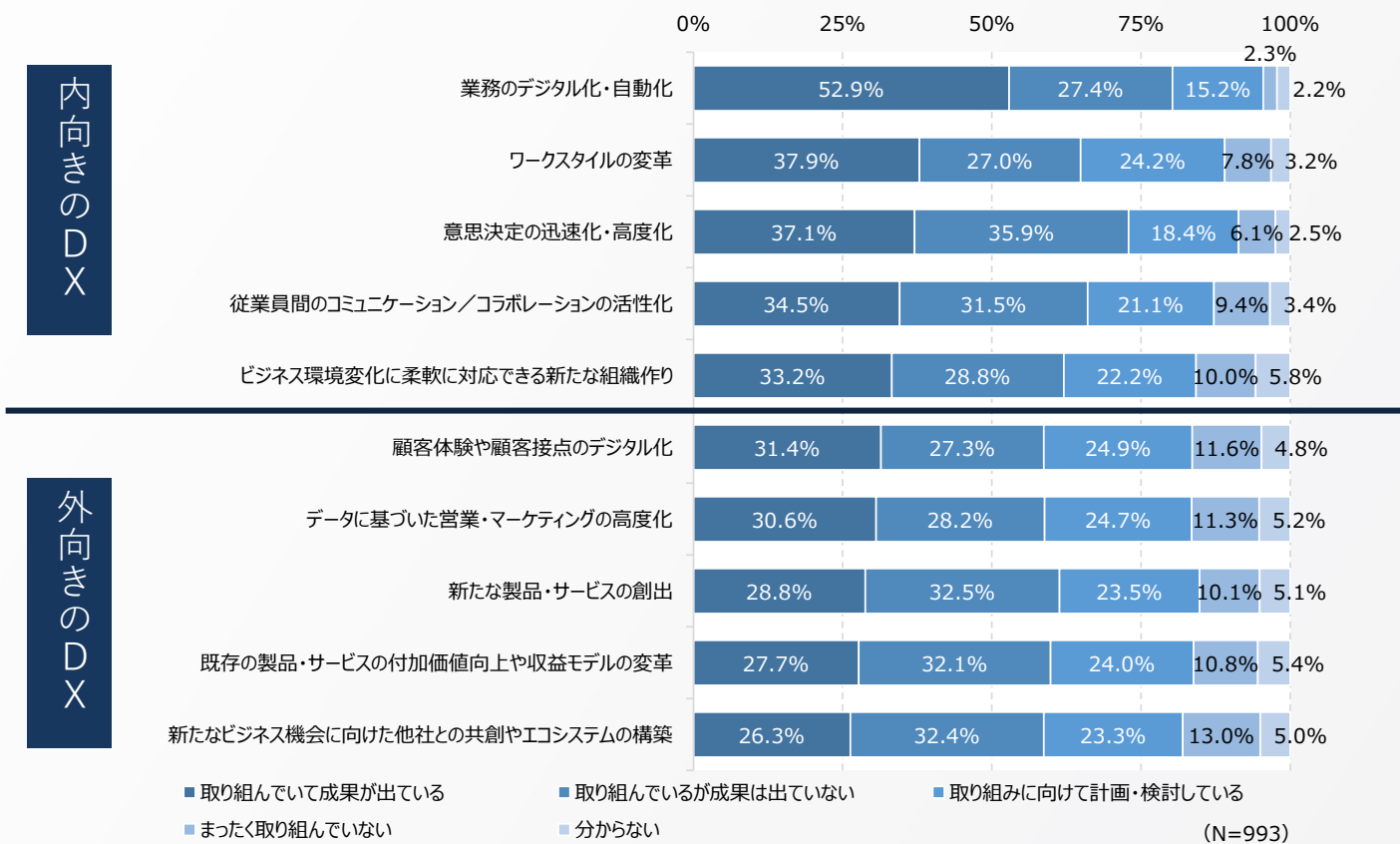
- DXの実践度が高まるにつれて、成果指標は業務コストや労働時間といった効率性指標に加え、収益、顧客エンゲージメント、市場シェアなど事業成果に近い指標へと広がっており、DXが業務改善からビジネス創出フェーズへ進展していることが分かる。
- 一方で、全社戦略を持たない、または部門単位にとどまる企業では、指標未設定や限定的な指標に依存する傾向が強く、DXの進展度合いが成果測定の設計力にも表れている。

	全 体	DX実践状況			
		全社戦略はないが、部門単位での試行や実践が行われている	全社戦略に基づいて、一部の部門で実践が行われている	全社戦略に基づいて、部門横断的に実践されている	全社的にDXが定着し、継続的に実践と改善が行われている
該当数	993	273	291	242	187
業務コスト（業務に係る費用）	52.7	42.1	46.4	60.7	67.4
労働時間／残業時間	48.5	50.2	46.7	47.5	50.3
従業員エンゲージメント（満足度含む）	36.9	27.8	35.7	37.6	50.8
収益（既存と新規の両方の売上を含む）	29.8	20.5	30.2	34.3	36.9
新規の社内プロジェクト数	29.7	27.8	32.3	28.5	29.9
データの活用度合い	25.4	17.9	22.0	32.6	32.1
顧客エンゲージメント（NPS、満足度含む）	23.1	15.4	17.5	27.7	36.9
新規製品／サービスの投入時間・頻度	20.0	10.6	19.6	24.4	28.9
市場シェア	16.5	12.1	13.7	19.0	24.1
他社との協業数	7.5	5.5	5.2	7.4	13.9
指標を使って測定していない	6.1	9.9	4.5	4.5	5.3

## Q2\_3 DXの取り組み内容

Q：あなたの勤務先で実践しているDXは、どのようなことに取り組んでいますか。以下の項目について、それぞれ取り組み状況として当てはまるものをお答えください。（SA）

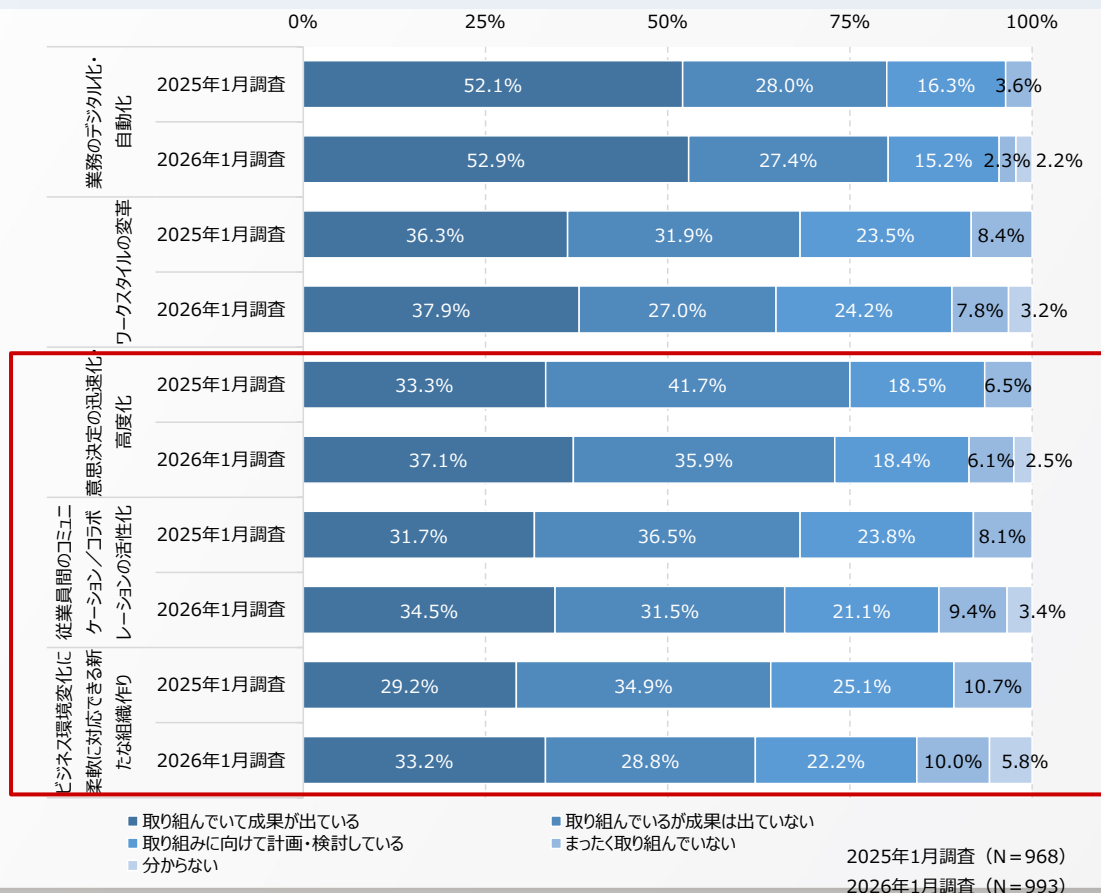
- 「内向きのDX」では業務のデジタル化・自動化が最も進展しており、成果が出ている割合も高い。一方で、意思決定の高度化やコラボレーション活性化は、成果は出ていないとする層も多く、実践の難しさがうかがえる。
- 「外向きのDX」では、顧客接点のデジタル化やデータ活用、新たな製品・サービスの創出などの取り組みは進みつつあるものの、成果が出ている割合は内向きDXより低い状況にある。



# Q2\_3 DXの取り組み内容：前回調査との比較（内向きのDX）

Q：あなたの勤務先で実践しているDXは、どのようなことに取り組んでいますか。以下の項目について、それぞれ取り組み状況として当てはまるものをお答えください。（SA）

- 業務のデジタル化・自動化とワークスタイルの変革は、成果が出ている割合ではほとんど変化は見られない。
- ワークスタイルの変革、意思決定の迅速化、コラボ／コミュニケーション活性化、新たな組織作りは、前回調査から成果が出ている割合が上昇している。ツール導入だけでなく、組織面や文化面の変革も着実に進んでいる状況がうかがえる。

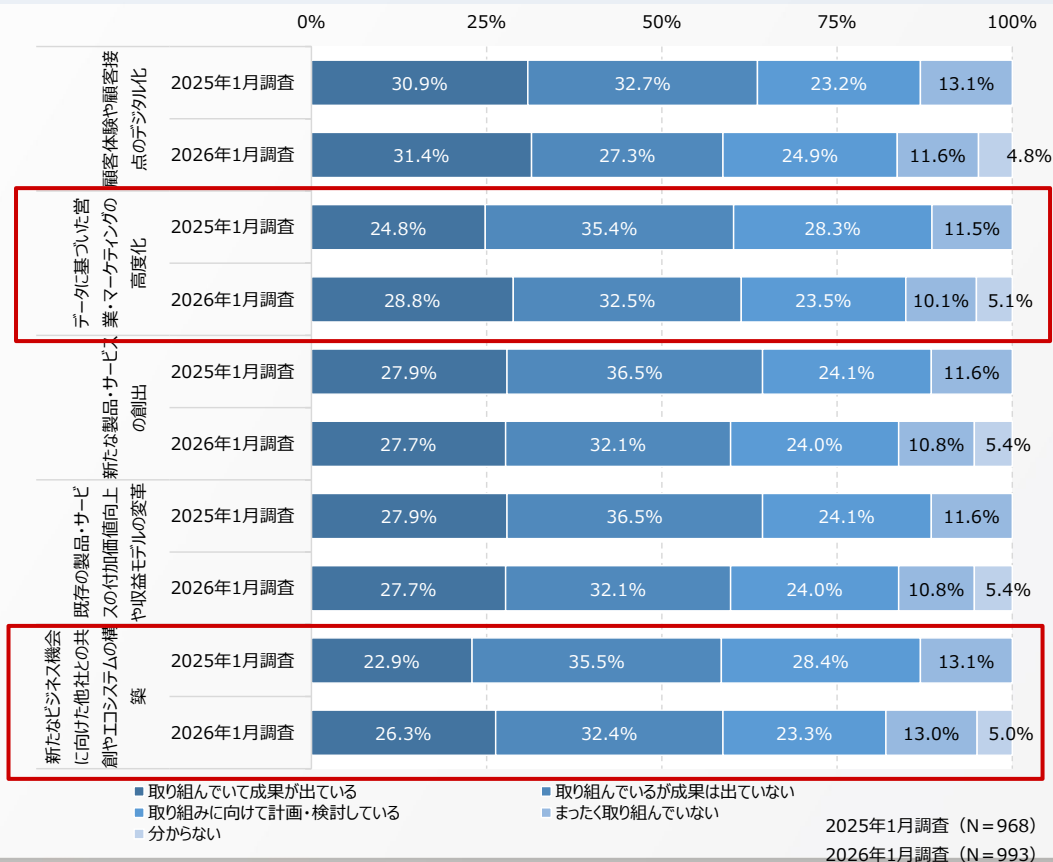


※2025年調査は「まったく取り組んでいない／分からない」、2026年調査では「まったく取り組んでいない」と「分からない」を分割している

# Q2\_3 DXの取り組み内容：前回調査との比較（外向きのDX）

Q：あなたの勤務先で実践しているDXは、どのようなことに取り組んでいますか。以下の項目について、それぞれ取り組み状況として当てはまるものをお答えください。（SA）

- データに基づく営業・マーケティング高度化は、成果が出ている割合が前回調査からの上昇率が最も大きく、データ活用が実際の営業活動やマーケティング施策の改善に結び付き始めている企業が増えていることがうかがえる。
- 新たなビジネス機会に向けたエコシステム構築でも、成果が出ている割合が上昇している。取り組みの難易度は高いものの、パートナー連携や共創モデルが成果につながり始めた企業が一定数現れていることがうかがえる。

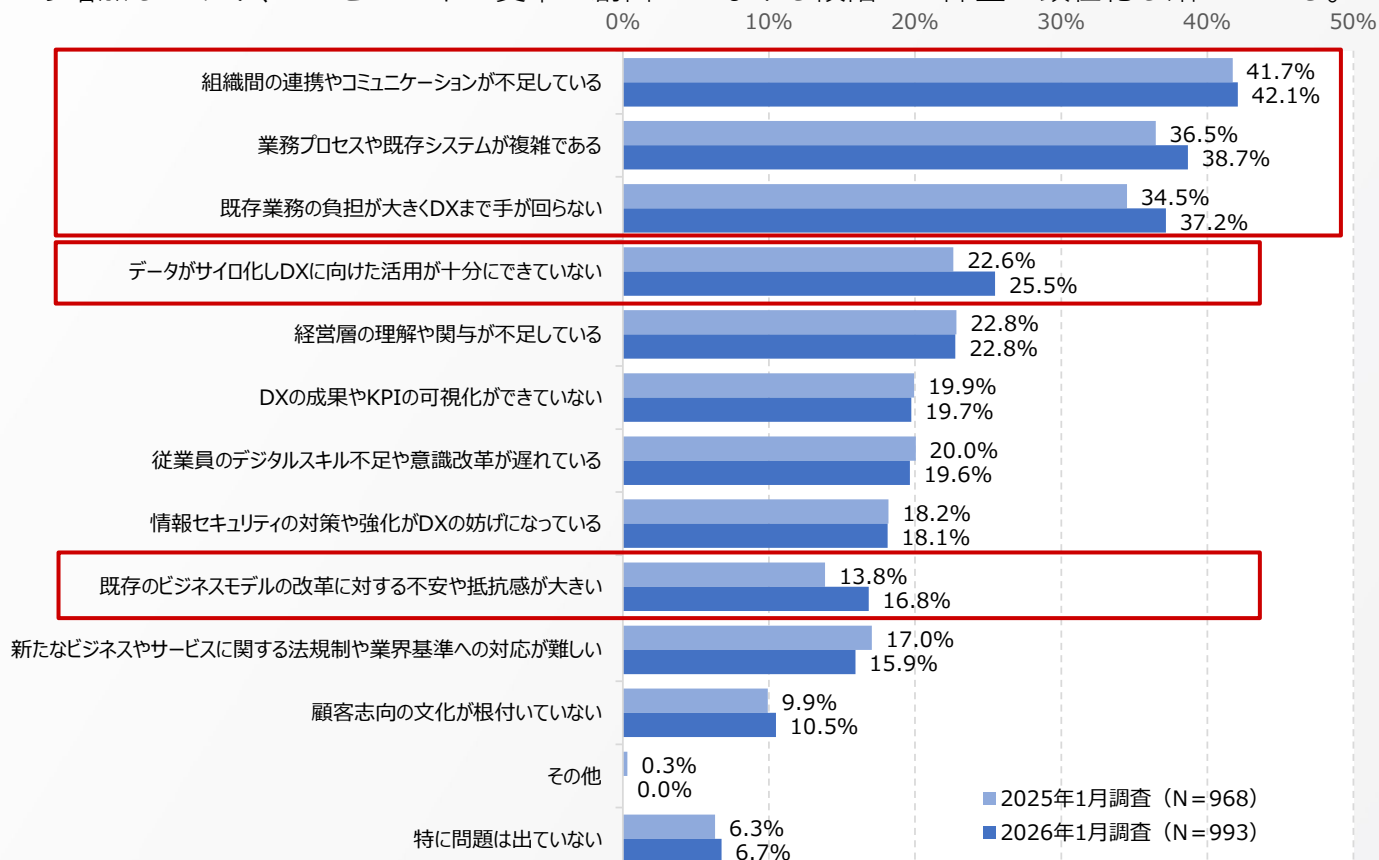


※2025年調査は「まったく取り組んでいない/分からない」、2026年調査では「まったく取り組んでいない」と「分からない」を分割している

## Q2\_4 DX実践上の問題

Q：あなたの勤務先で、DXを実践していく上でどのような問題が生じていますか?当てはまるものを全てお答えください。(MA)

- 組織間の連携・コミュニケーション不足、業務プロセス・既存システムの複雑さ、既存業務の負担といった上位項目はいずれも前回調査から増加しており、DX推進の阻害要因が技術よりも組織や業務の硬直性に集中している状況が改めて浮き彫りになっている。
- データがサイロ化し十分に活用できていないことや、既存のビジネスモデル変革に対する不安・抵抗感も前回調査から増加しており、DXをビジネス変革・創出へつなげる段階での障壁が顕在化し始めている。



## Q2\_4 DX実践上の問題：DX実践状況別

Q：あなたの勤務先で、DXを実践していく上でどのような問題が生じていますか?当てはまるものを全てお答えください。(MA)

- DXの実践度が高まるほど、組織間の連携・コミュニケーション不足や既存業務の負担が大きいといった課題は低下しており、全社的にDXが定着している企業ほど、組織・業務面の初期的な障壁を乗り越えていることがうかがえる。
- 一方で、業務プロセスや既存システムの複雑さやDXの成果・KPIの可視化不足は、全社戦略を持つ企業でも一定割合残っている。DXが進展するにつれ、技術的負債や成果測定の難しさといった、より本質的な課題が顕在化していることが分かる。

	DX実践状況				
	全体	全社戦略はないが、部門単位での試行や実践が行われている	全社戦略に基づいて、一部の部門で実践が行われている	全社戦略に基づいて、部門横断的に実践されている	全社的にDXが定着し、継続的に実践と改善が行われている
該当数	993	273	291	242	187
組織間の連携やコミュニケーションが不足している	42.1	47.3	44.7	40.5	32.6
業務プロセスや既存システムが複雑である	38.7	38.8	35.4	41.7	39.6
既存業務の負担が大きくDXまで手が回らない	37.2	33.3	45.0	39.3	27.8
データがサイロ化しDXに向けた活用が十分にできていない	25.5	19.8	25.8	32.6	24.1
経営層の理解や関与が不足している	22.8	22.0	27.5	24.4	14.4
DXの成果やKPIの可視化ができていない	19.7	13.9	21.6	22.7	21.4
従業員のデジタルスキル不足や意識改革が遅れている	19.6	17.6	18.9	21.9	20.9
情報セキュリティの対策や強化がDXの妨げになっている	18.1	15.0	17.9	19.0	21.9
既存のビジネスモデルの改革に対する不安や抵抗感が大きい	16.8	13.9	16.8	19.4	17.6
新たなビジネスやサービスに関する法規制や業界基準への対応が難しい	15.9	15.4	14.8	18.6	15.0
顧客志向の文化が根付いていない	10.5	7.0	13.4	7.9	14.4
特に問題は出ていない	6.7	4.4	3.4	4.5	18.2

# 3

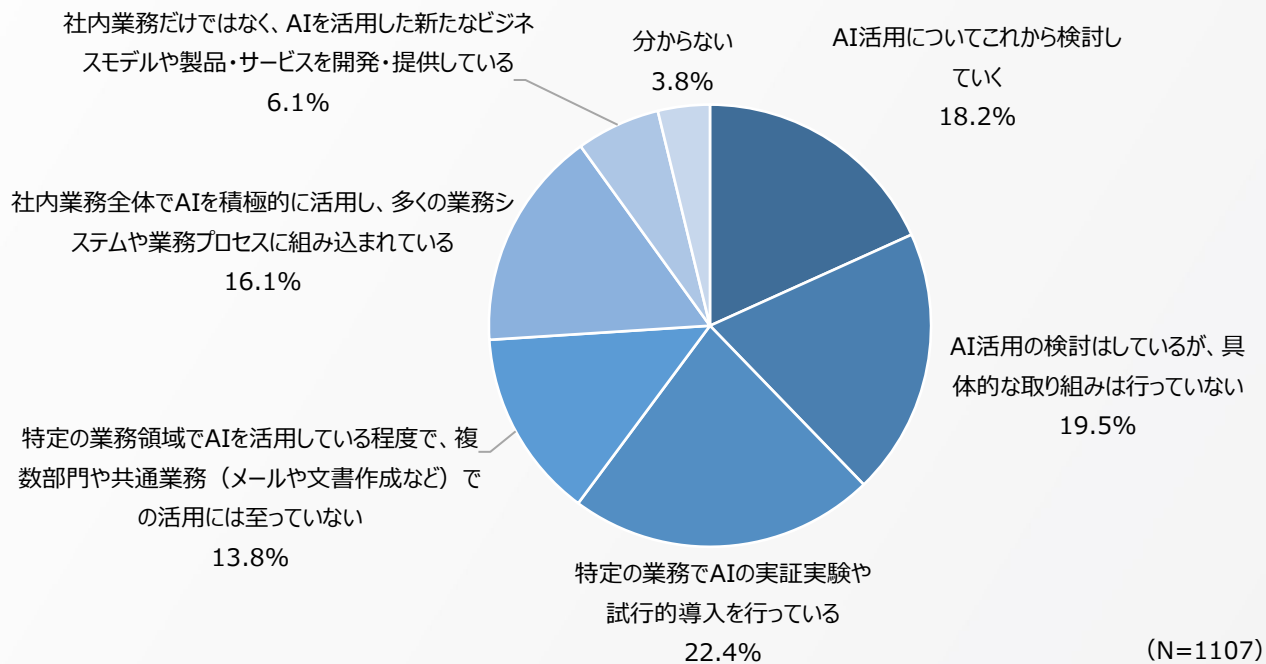
## AIの活用状況

- Q3\_1 AIの活用状況
- Q3\_2 AIの活用効果
- Q3\_3 AI活用の課題
- Q3\_4 AI活用のガバナンス体制
- Q3\_5 強化が必要なAIガバナンス領域

## Q3\_1 AIの活用状況

Q：あなたの勤務先でのAIの活用状況はどのような段階にありますか。最も近いものをお答えください。ここでは、会社標準としてのAI活用を対象としており、個人で個別契約した生成AIを利用などの個人でのAI利用は対象としていません。（SA）

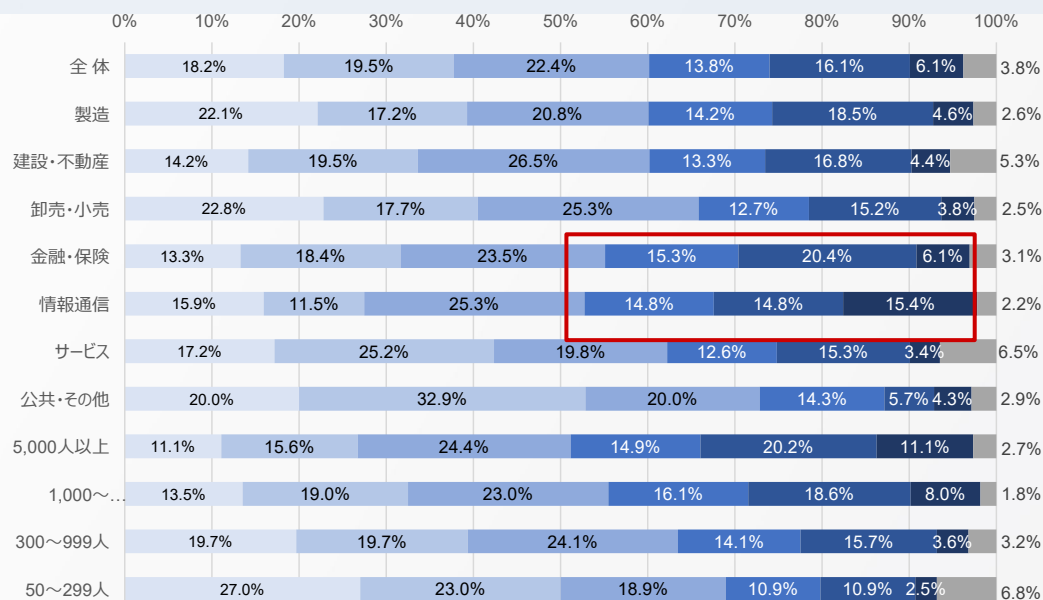
- 会社標準としてのAI活用は「これから検討（18.2%）」 「検討はしているが具体的な取り組みはない（19.5%）」 「実証実験・試行導入（22.4%）」が合計で60%を占めており、多くの企業が準備段階にとどまっている。
- 「社内業務全体での積極活用（16.1%）」や「AIを活用した新たなビジネスモデル・製品提供（6.1%）」まで進んでいる企業は約2割強にとどまっている。AIをビジネス競争力や事業創出に直結させられている企業はまだ少数である。
- AI活用の成熟度にバラつきが見られ、企業間で明確な差が生じていることがうかがえる。



# Q3\_1 AIの活用状況：企業属性別

Q：あなたの勤務先でのAIの活用状況はどのような段階にありますか。最も近いものをお答えください。ここでは、会社標準としてのAI活用を対象としており、個人で個別契約した生成AIを利用などの個人でのAI利用は対象としていません。（SA）

- 業種別：情報通信と金融・保険においてAI活用の成熟度が高い傾向が見られる。特に情報通信はAIを利用し製品・サービスを開発している割合が高い。一方、卸売・小売やサービス、公共・その他において活用の遅れが見られる。
- 従業員規模別：従業員数が多い企業ほど、AI活用度が上昇していく傾向が顕著に見らる。一方、50～299人の企業では半数が取り組みに至っておらず、リソースや投資余力の差がAI活用の成熟度に反映されていると見てとれる。

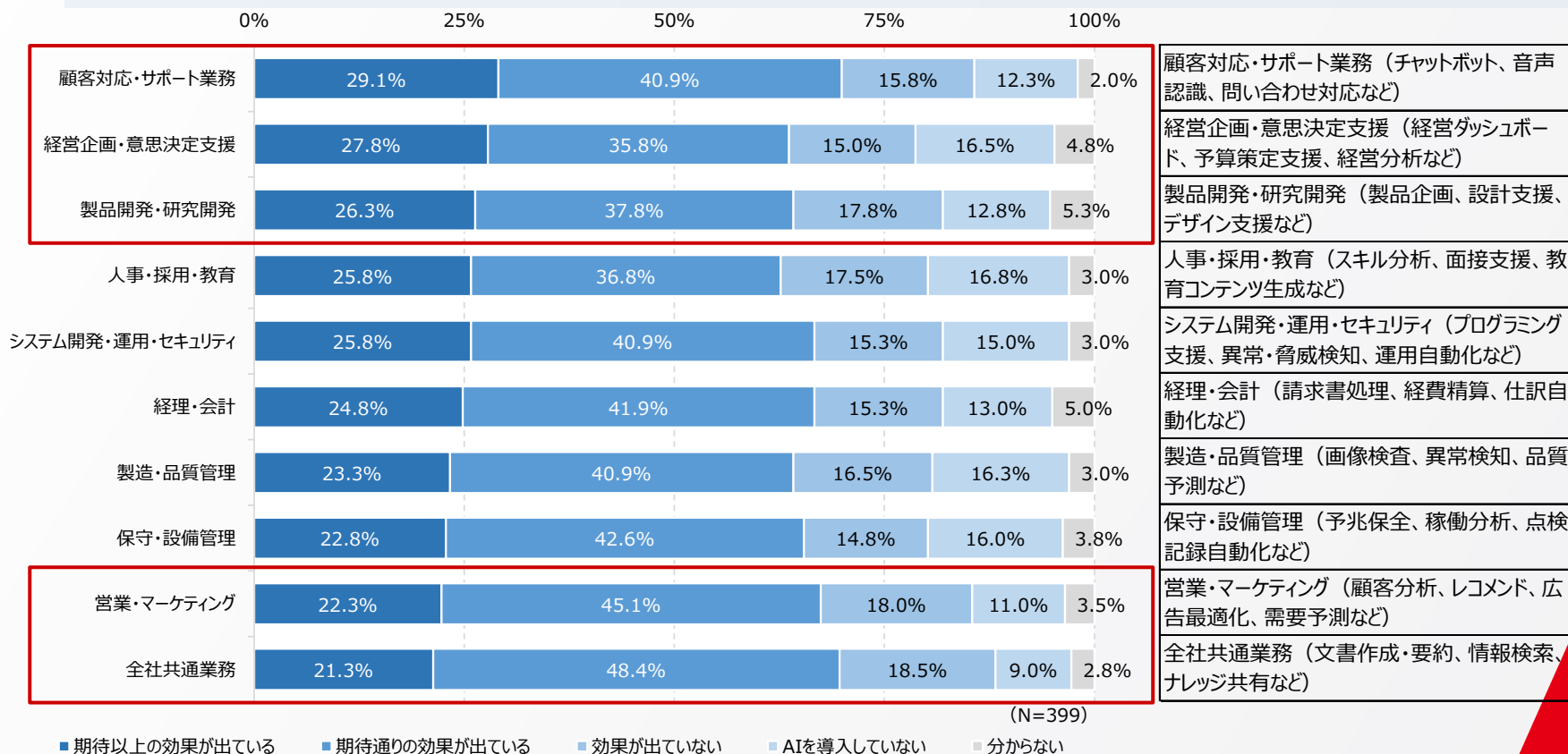


- AI活用についてこれから検討していく
- AI活用の検討はしているが、具体的な取り組みは行っていない
- 特定の業務でAIの実証実験や試行的導入を行っている
- 特定の業務領域でAIを活用している程度で、複数部門や共通業務（メールや文書作成など）での活用には至っていない
- 社内業務全体でAIを積極的に活用し、多くの業務システムや業務プロセスに組み込まれている
- 社内業務だけでなく、AIを活用した新たなビジネスモデルや製品・サービスを開発・提供している
- 分からない

# Q3\_2 AIの活用効果

Q：あなたの勤務先で活用しているAIはどの程度の効果が出ていますか。各業務項目に対する効果の割合をお答えください。（SA）

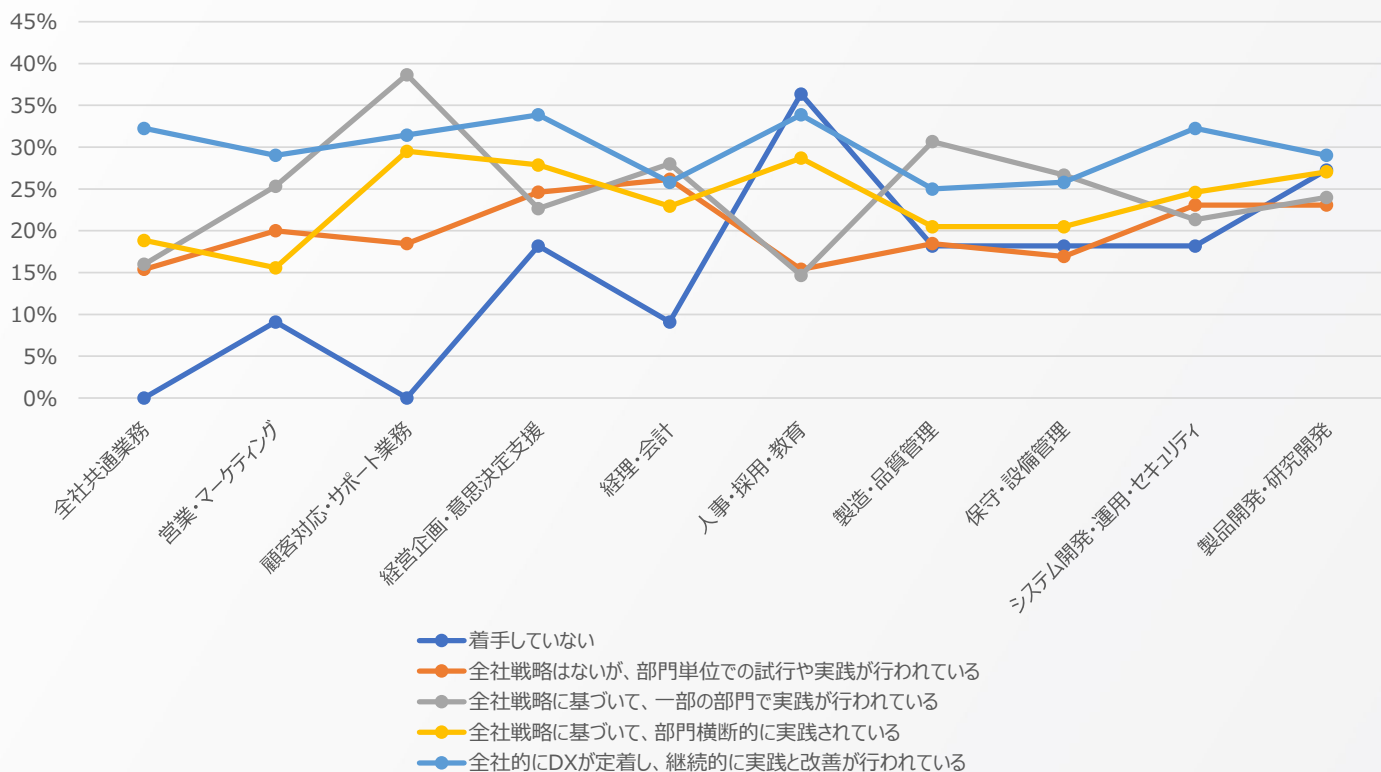
- 顧客対応・サポート、経営企画・意思決定支援、製品開発・研究開発などでは「期待以上」の効果が相対的に高く、AIが人の判断支援や対応スピード向上に寄与しやすい業務ほど、高い効果を実感しやすい傾向が見られる。
- 一方、全社共通業務と営業・マーケティングでは「想定通り」の効果は相対的に高いものの「期待以上」の効果の割合は相対的に低くなっている。業務の汎用性が高いがゆえに、高い効果実感にはつながりにくいとも考えられる。



## Q3\_2 AIで期待以上の効果が出ている業務：DX実践状況別

Q：あなたの勤務先で活用しているAIはどの程度の効果が出ていますか。各業務項目に対する効果の度合いをお答えください。（SA） ー 期待以上の効果が出ている

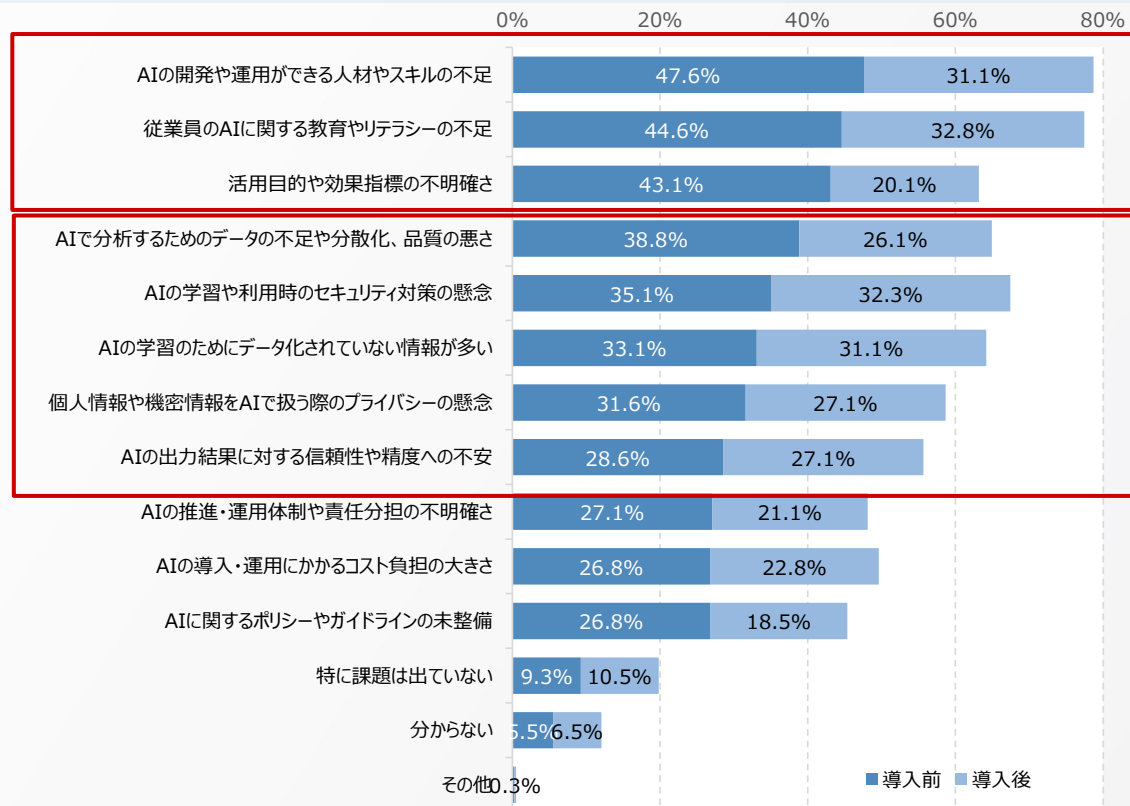
- 全社共通業務、営業・マーケティング、顧客対応・サポート業務などでは、DXの実践レベルが上がると期待以上の効果が出ている割合が高くなる傾向がある。部門横断的な業務でのAI活用で効果を出すためには、DXによる業務の標準化やデジタル化が重要となっている。
- 一方、人事・採用・教育、製品・品質管理、保守・設備管理、システム開発・運用・セキュリティ、製品開発・研究開発など専門性の高い業務になると、DXの実践レベルとAIによる効果の相関関係は見られない。DXよりも業務特有のノウハウやナレッジなどが、AI活用で効果を出すことに関係している可能性が考えられる。



## Q3\_3 AI活用の課題

Q：あなたの勤務先では、AI活用を進める上でどのような課題が挙がりましたか。AIの導入前と導入後、それぞれについて当てはまるものをすべてお答えください。

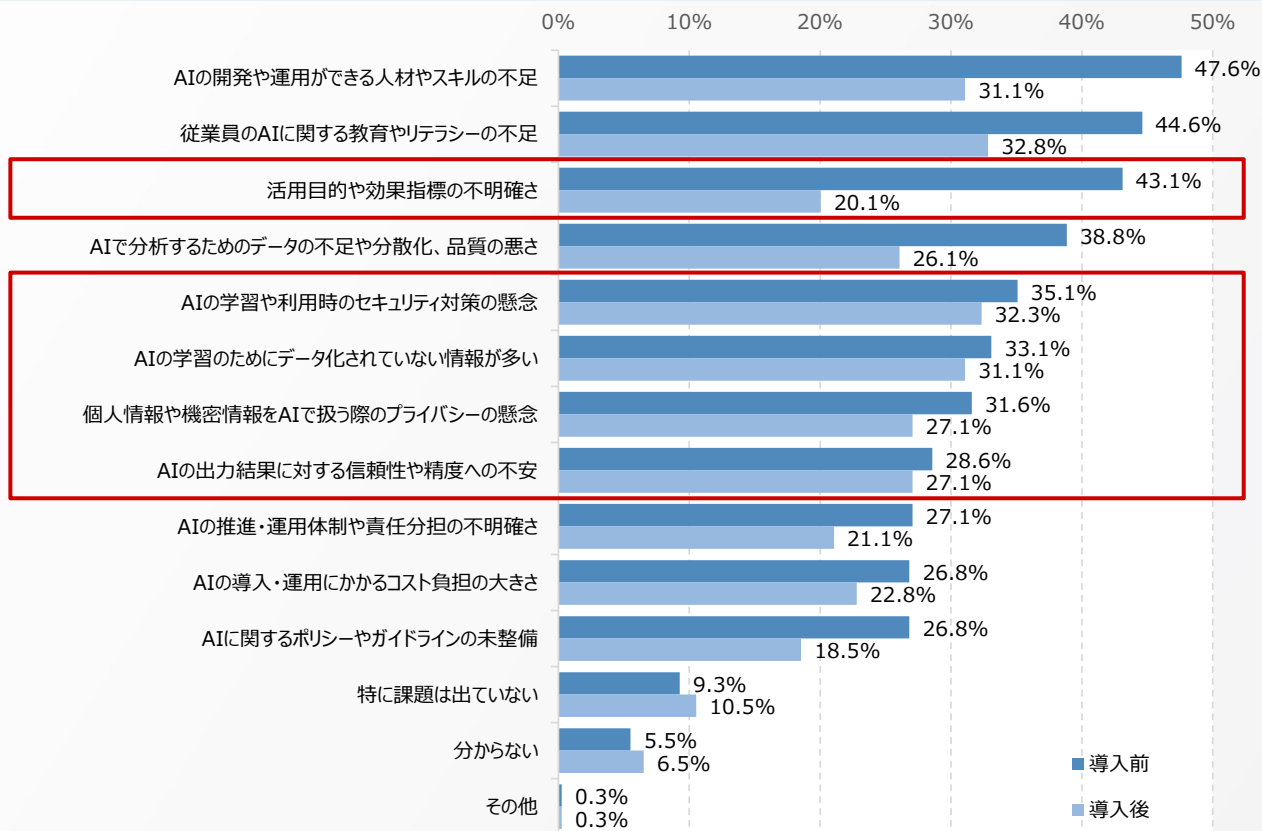
- 導入前の課題では、AIを開発・運用できる人材・スキル不足、従業員のAIリテラシー不足、活用目的や効果指標の不明確さが上位を占めており、AI活用に踏み出す前段階では人材やスキル、目的設計が大きな障壁になっていることが分かる。
- 導入後の課題では、AI活用におけるセキュリティやプライバシーへの懸念、AIの出力結果に対する信頼性への不安が相対的に目立つ。活用フェーズに入ることによって、セキュリティやガバナンス、信頼性といったAIリスクの課題が顕在化していることが示されている。また、AI活用のためのデータ整備の課題も見られる。



## Q3\_3 AI活用の課題：導入前と導入後の比較

Q：あなたの勤務先では、AI活用を進める上でどのような課題が挙がりましたか。AIの導入前と導入後、それぞれについて当てはまるものをすべてお答えください。

- 活用目的や効果指標の不明確さは、導入前では高い割合を占めていたが、導入後は大きく低下しており、実際にAI活用を進める中で目的やKPIの設定が具体化・明確化されたことがうかがえる。
- AIの学習・利用時のセキュリティ対策の懸念や学習のためにデータ化されていない情報の多さ、個人情報や機密情報を扱う際のプライバシーへの懸念、AIの出力結果に対する信頼性や精度への不安は、導入前後で大きな変化が見られず、継続的な対応が求められる。



# Q3\_3 AI活用の課題（導入前）：AI活用状況別

Q：あなたの勤務先では、AI活用を進める上でどのような課題が挙がりましたか。AIの導入前と導入後、それぞれについて当てはまるものをすべてお答えください。

- AI活用の成熟度にかかわらず、人材・スキル不足、従業員のAIリテラシー不足、活用目的や効果指標の不明確さが高水準で挙がっており、AI導入前段階では人材・教育と目的設計が共通のボトルネックになっていることが分かる。
- データ不足・分散や未整備、セキュリティやプライバシーへの懸念も認識されており、AI活用の検討段階からデータ基盤整備とガバナンス設計も重点課題となっている。

	全体	AI活用状況		
		特定の業務領域でAIを活用している程度で、複数部門や共通業務（メールや文書作成など）での活用には至っていない	社内業務全体でAIを積極的に活用し、多くの業務システムや業務プロセスに組み込まれている	社内業務だけではなく、AIを活用した新たなビジネスモデルや製品・サービスを開発・提供している
該当数	399	153	178	68
AIの開発や運用ができる人材やスキルの不足	47.6	43.8	51.1	47.1
従業員のAIに関する教育やリテラシーの不足	44.6	45.8	43.3	45.6
活用目的や効果指標の不明確さ	43.1	42.5	41.0	50.0
AIで分析するためのデータの不足や分散化、品質の悪さ	38.8	41.8	37.1	36.8
AIの学習や利用時のセキュリティ対策の懸念	35.1	34.0	37.1	32.4
AIの学習のためにデータ化されていない情報が多い	33.1	32.0	33.1	35.3
個人情報や機密情報をAIで扱う際のプライバシーの懸念	31.6	31.4	31.5	32.4
AIの出力結果に対する信頼性や精度への不安	28.6	23.5	34.3	25.0
AIの推進・運用体制や責任分担の不明確さ	27.1	24.2	30.9	23.5
AIの導入・運用にかかるコスト負担の大きさ	26.8	21.6	30.3	29.4
AIに関するポリシーやガイドラインの未整備	26.8	25.5	28.7	25.0
その他	0.3	0.0	0.6	0.0
特に課題は出ていない	9.3	6.5	10.1	13.2
分からない	5.5	5.2	4.5	8.8

# Q3\_3 AI活用の課題（導入後）：AI活用状況別

Q：あなたの勤務先では、AI活用を進める上でどのような課題が挙がりましたか。AIの導入前と導入後、それぞれについて当てはまるものをすべてお答えください。

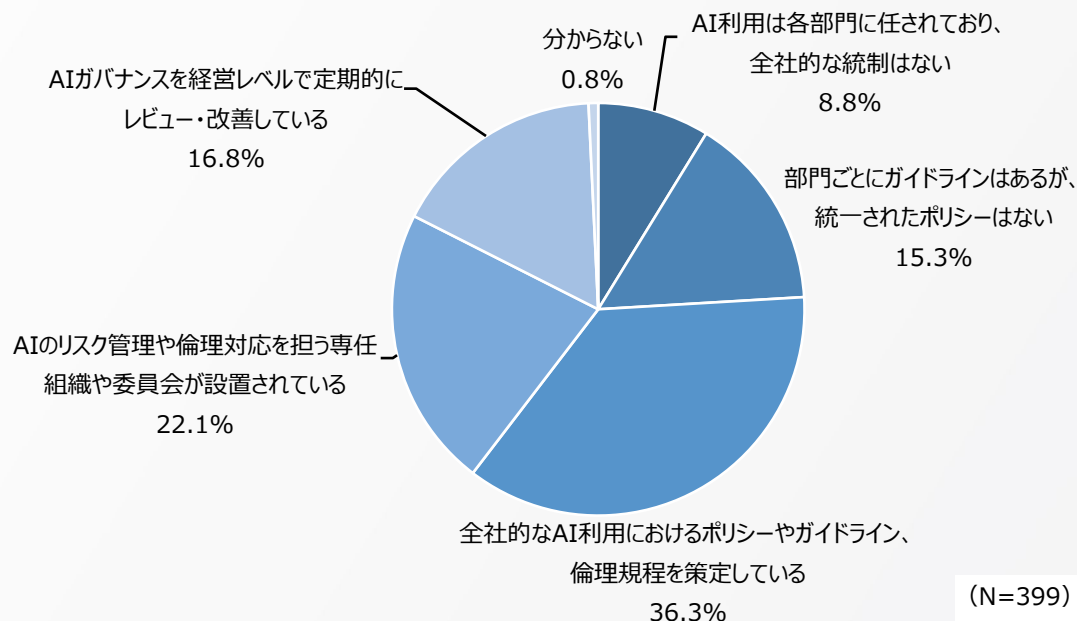
- AI活用の成熟度が低い企業ほど、従業員のAIリテラシー不足の割合が高く、従業員のAIに関する基礎理解の不足がAI活用の最大の課題となっていることがうかがえる。
- AIを業務全体や新規ビジネスに活用している企業では、セキュリティ・プライバシーへの懸念、データの未整備、人材・スキ不足など課題が多様化しており、導入後の運用の難しさが見えてくる。

	全体	AI活用状況		
		特定の業務領域でAIを活用している程度で、複数部門や共通業務（メールや文書作成など）での活用には至っていない	社内業務全体でAIを積極的に活用し、多くの業務システムや業務プロセスに組み込まれている	社内業務だけではなく、AIを活用した新たなビジネスモデルや製品・サービスを開発・提供している
該当数	399	153	178	68
従業員のAIに関する教育やリテラシーの不足	32.8	41.2	28.1	26.5
AIの学習や利用時のセキュリティ対策の懸念	32.3	31.4	32.0	35.3
AIの開発や運用ができる人材やスキルの不足	31.1	30.1	29.8	36.8
AIの学習のためにデータ化されていない情報が多い	31.1	30.7	30.3	33.8
個人情報や機密情報をAIで扱う際のプライバシーの懸念	27.1	23.5	27.0	35.3
AIの出力結果に対する信頼性や精度への不安	27.1	26.1	28.1	26.5
AIで分析するためのデータの不足や分散化、品質の悪さ	26.1	26.8	23.6	30.9
AIの導入・運用にかかるコスト負担の大きさ	22.8	20.3	21.9	30.9
AIの推進・運用体制や責任分担の不明確さ	21.1	16.3	25.8	19.1
活用目的や効果指標の不明確さ	20.1	20.9	19.1	20.6
AIに関するポリシーやガイドラインの未整備	18.5	16.3	19.7	20.6
その他	0.3	0.0	0.6	0.0
特に課題は出ていない	10.5	7.2	12.4	13.2
分からない	6.5	7.8	4.5	8.8

## Q3\_4 AI活用のガバナンス体制

Q：あなたの勤務先では、AI活用におけるガバナンス体制はどのようになっていますか。最も近いものをお答えください。（SA）

- 全社的なポリシーやガイドライン、倫理規程を策定している企業は36%、さらに専門組織や委員会の設置、経営レベルでの定期レビューまで含めると、一定のガバナンスを構築している企業は約75%を占める。AI活用が本格化する中で、ガバナンスの必要性を認識する企業は多い。
- その一方で、部門任せや部門別ガイドラインにとどまる企業も2割超存在しており、全社的に統一されたガバナンスが未整備な企業が依然として残っている。



## Q3\_4 AI活用のガバナンス体制：AI活用状況別

Q：あなたの勤務先では、AI活用におけるガバナンス体制はどのようになっていますか。最も近いものをお答えください。（SA）

- AI活用が特定業務にとどまる企業では、部門任せや部門別ガイドラインに依存する割合が高く、全社的なガバナンスが相対的に弱い。一方、社内業務全体にAIを組み込んでいる企業では、全社ポリシーやガイドラインを整備する動きが進み、ガバナンスの標準化が進展している。
- AIを製品・サービスの開発に活用している企業では、経営レベルでの定期的なレビュー/改善を過半数以上が行っており、AIガバナンスが現場から経営での統制へと格上げされている。AI活用の高度化に伴い、AIガバナンスに対する経営関与が強まっていることがうかがえる。

	全 体	AI活用状況		
		特定の業務領域でAIを活用している程度で、複数部門や共通業務（メールや文書作成など）での活用には至っていない	社内業務全体でAIを積極的に活用し、多くの業務システムや業務プロセスに組み込まれている	社内業務だけではなく、AIを活用した新たなビジネスモデルや製品・サービスを開発・提供している
該当数	399	153	178	68
AI利用は各部門に任せられており、全社的な統制はない	8.8	11.8	6.7	7.4
部門ごとにガイドラインはあるが、統一されたポリシーはない	15.3	27.5	9.6	2.9
全社的なAI利用におけるポリシーやガイドライン、倫理規程を策定している	36.3	41.8	40.4	13.2
AIのリスク管理や倫理対応を担う専任組織や委員会が設置されている	22.1	15.0	28.7	20.6
AIガバナンスを経営レベルで定期的にレビュー・改善している	16.8	3.9	13.5	54.4
分からない	0.8	0.0	1.1	1.5

## Q3\_4 AI活用のガバナンス体制：DX実践状況別

Q：あなたの勤務先では、AI活用におけるガバナンス体制はどのようになっていますか。最も近いものをお答えください。（SA）

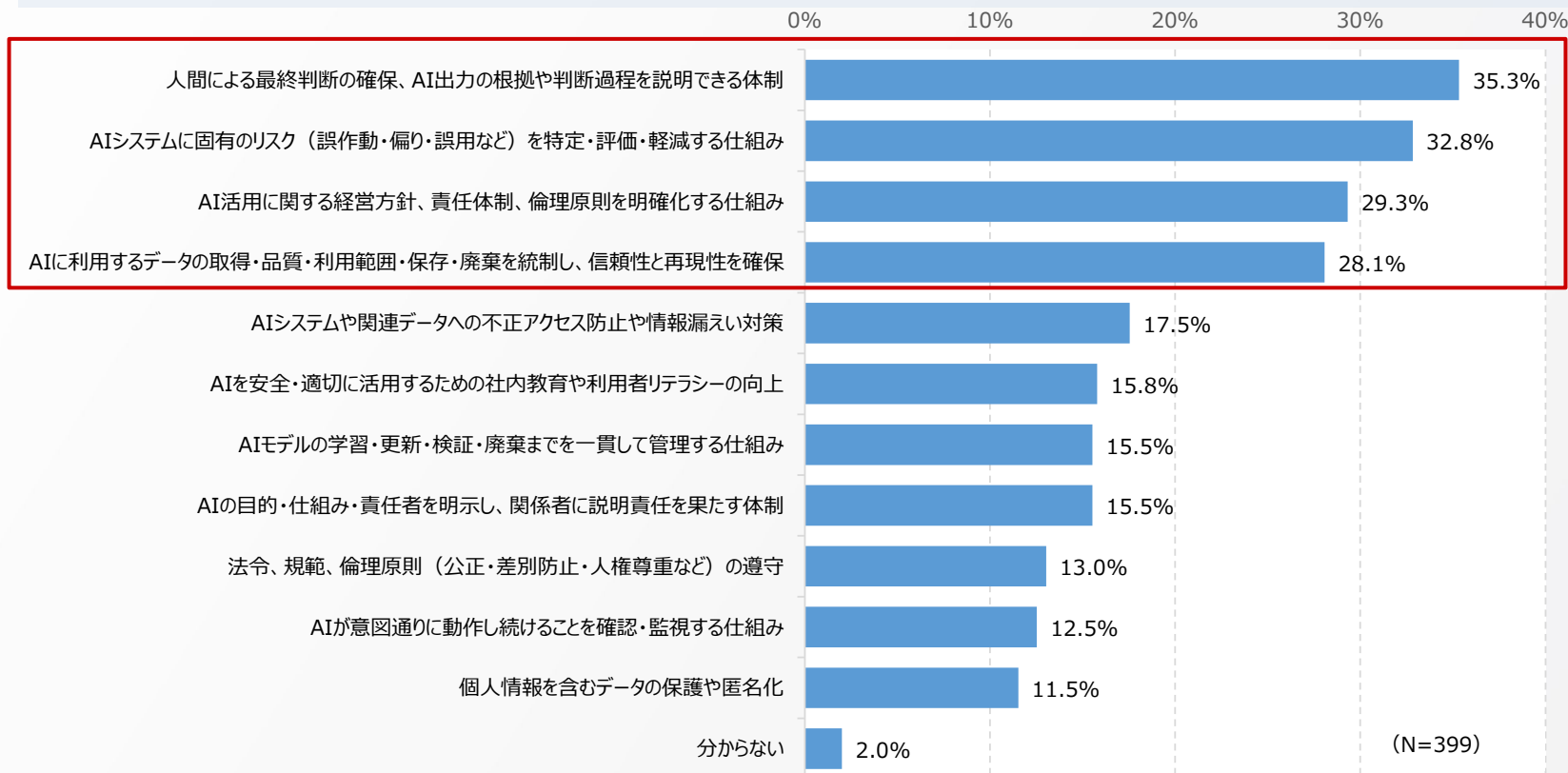
- DXの実践レベルが高いほど、全社的なポリシー・倫理規程の策定が進んでいる。部門横断での実践や定着企業では、大部分が全社的なポリシーやガイドラインを策定している。一方、DX未着手企業では部門任せや統一ポリシーがない割合が高い。
- 全社的にDXが定着している企業では、経営レベルでの定期的レビューが突出して高く、AI統制が現場レベルから経営アジェンダへ昇格していることがうかがえる。

	全体	DX実践状況				
		着手していない	全社戦略はないが、部門単位での試行や実践が行われている	全社戦略に基づいて、一部の部門で実践が行われている	全社戦略に基づいて、部門横断的に実践されている	全社的にDXが定着し、継続的に実践と改善が行われている
該当数	399	11	65	75	122	124
AI利用は各部門に任されており、全社的な統制はない	8.8	27.3	15.4	9.3	8.2	4.0
部門ごとにガイドラインはあるが、統一されたポリシーはない	15.3	18.2	21.5	30.7	14.8	2.4
全社的なAI利用におけるポリシーやガイドライン、倫理規程を策定している	36.3	18.2	44.6	41.3	41.0	26.6
AIのリスク管理や倫理対応を担う専任組織や委員会が設置されている	22.1	9.1	13.8	16.0	27.9	25.0
AIガバナンスを経営レベルで定期的にレビュー・改善している	16.8	18.2	4.6	2.7	6.6	41.9
分からない	0.8	9.1	0.0	0.0	1.6	0.0

## Q3\_5 強化が必要なAIガバナンス領域

Q：AIガバナンスにおいて、特に強化が必要と感じる領域はどこですか。最大3つまでお答えください。（MA）

- 強化が最も求められているのは、人による最終判断の確保とAI出力の根拠・判断過程の説明可能性（人間中心設計・説明可能性）、およびAI固有リスクの特定・評価・軽減（リスク管理）であり、AIを業務や意思決定に組み込むうえでの信頼性と説明責任の確保が最大の強化領域になっている。
- 次いで、AI活用に関する経営方針・責任体制・倫理原則の明確化（ガバナンス体制）やデータ取得・品質・利用範囲・保管の統制（データガバナンス）が必要とされており、技術管理にとどまらず、包括的なガバナンスの必要性が強く認識されていることがうかがえる。



# Q3\_5 強化が必要なAIガバナンス領域：AI活用状況別

Q：AIガバナンスにおいて、特に強化が必要と感じる領域はどこですか。最大3つまでお答えください。（MA）

- AI活用が特定業務にとどまる企業では、人による最終判断の確保やAI固有リスクの特定・評価・軽減といった利用時の安全性・説明責任に直結する領域への関心が高く、まずはAIを安全に使うことを重視している傾向が見られる。
- 一方、製品・サービスの開発にAIを活用している企業では、経営方針・責任体制・倫理原則の明確化や教育・リテラシー向上の比率も高くなっており、AI活用を継続的に拡張する前提として、経営・組織レベルでのガバナンスやリテラシー強化が重要になっていることがうかがえる。

	全体	AI活用状況		
		特定の業務領域でAIを活用している程度で、複数部門や共通業務（メールや文書作成など）での活用には至っていない	社内業務全体でAIを積極的に活用し、多くの業務システムや業務プロセスに組み込まれている	社内業務だけではなく、AIを活用した新たなビジネスモデルや製品・サービスを開発・提供している
該当数	399	153	178	68
人間による最終判断の確保、AI出力の根拠や判断過程を説明できる体制	35.3	37.3	36.5	27.9
AIシステムに固有のリスク（誤作動・偏り・誤用など）を特定・評価・軽減する仕組み	32.8	33.3	33.1	30.9
AI活用に関する経営方針、責任体制、倫理原則を明確化する仕組み	29.3	21.6	32.6	38.2
AIに利用するデータの取得・品質・利用範囲・保存・廃棄を統制し、信頼性と再現性を確保	28.1	30.7	29.8	17.6
AIシステムや関連データへの不正アクセス防止や情報漏えい対策	17.5	15.0	21.9	11.8
AIを安全・適切に活用するための社内教育や利用者リテラシーの向上	15.8	15.0	12.4	26.5
AIモデルの学習・更新・検証・廃棄までを一貫して管理する仕組み	15.5	17.6	12.9	17.6
AIの目的・仕組み・責任者を明示し、関係者に説明責任を果たす体制	15.5	17.0	14.6	14.7
法令、規範、倫理原則（公正・差別防止・人権尊重など）の遵守	13.0	12.4	12.9	14.7
AIが意図通りに動作し続けることを確認・監視する仕組み	12.5	7.8	15.7	14.7
個人情報を含むデータの保護や匿名化	11.5	11.1	12.4	10.3
分からない	2.0	1.3	2.8	1.5

# 4

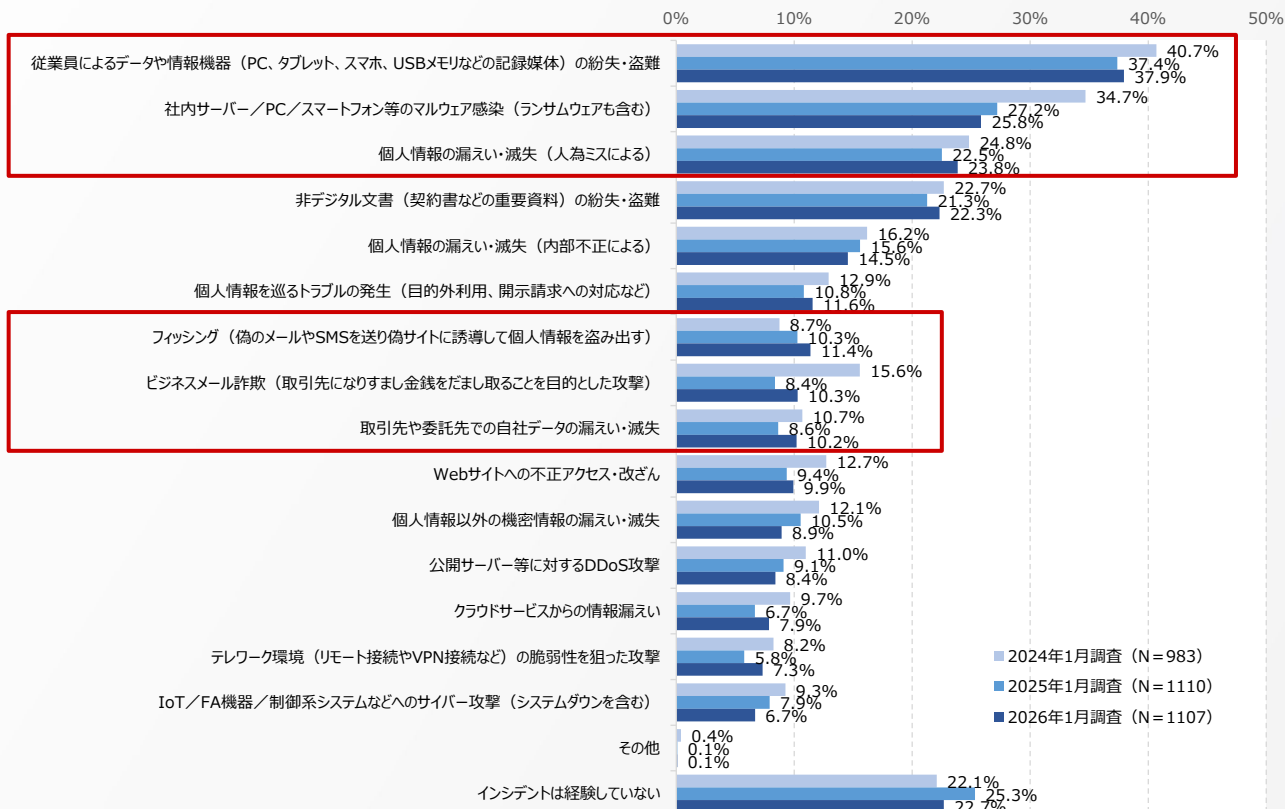
## 企業のセキュリティ対策

- Q4\_1 セキュリティ・インシデントの状況
- Q4\_2 ランサムウェア感染被害の経験
- Q4\_3 ランサムウェア感染からの復旧期間
- Q4\_4 ランサムウェア感染被害による影響
- Q4\_5 ランサムウェア感染被害による被害額
- Q4\_6 サイバー攻撃対策の実施状況
- Q4\_7 情報漏えい対策の実施状況
- Q4\_8 電子メールのセキュリティ対策状況
- Q4\_9 電子メールでのファイル送付手段

# Q4\_1 セキュリティ・インシデントの経験

Q：あなたの勤務先において、過去1年間に経験したセキュリティ・インシデントは何ですか。当てはまるものをすべてお答えください。（MA）

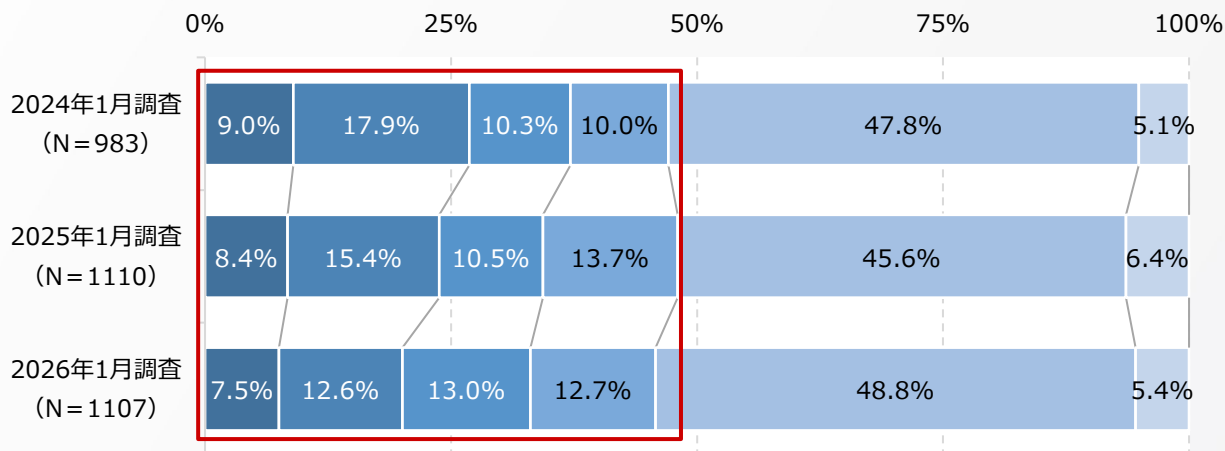
- 従業員による記録媒体の紛失・盗難、マルウェア感染、人的ミスによる個人情報漏えいは、2024年調査以降一貫して上位に挙がっており、今回調査でも高水準を維持している。人や端末を起点とするリスクは依然として大きいと言える。
- フィッシングやビジネスメール詐欺、取引先・委託先を起点とした情報漏えいは、前回から今回にかけて徐々に比率が高まっている。攻撃の焦点が社外接点やサプライチェーンへ拡大している傾向がうかがえ、境界防御に依存しない対策や取引先を含めた管理強化の重要性が増している。



## Q4\_2 ランサムウェア感染被害の経験

Q：あなたの勤務先で、ランサムウェア感染による被害を経験したことがありますか。（SA）

- 何らかの形でランサムウェア感染被害を経験した企業は毎年5割前後存在しており、ランサムウェアは特定企業でのインシデントではなく、どの企業でも被害にあう可能性のあるインシデントになっている。
- 2024年から2026年にかけて身代金を支払った企業の割合は減少傾向にあり、2026年では身代金を支払わなかった企業の割合の方が大きい。
- 2024年から2026年にかけて、システムを復旧できなかった企業の割合は復旧できた企業より大きいものの減少傾向にあり、2024年と比較し2026年では復旧できなかった割合は2.6ポイント減少している。

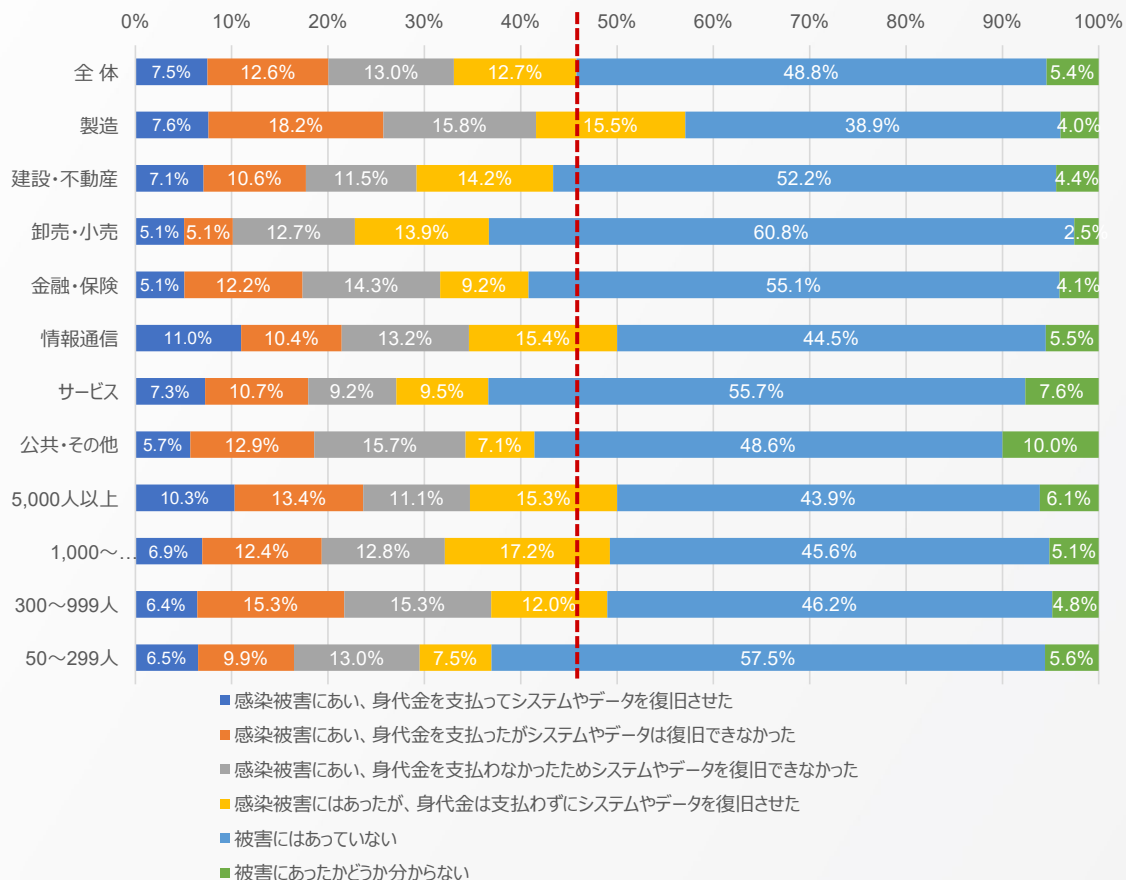


- 感染被害にあい、身代金を支払ってシステムやデータを復旧させた
- 感染被害にあい、身代金を支払ったがシステムやデータは復旧できなかった
- 感染被害にあい、身代金を支払わなかったためシステムやデータを復旧できなかった
- 感染被害にはあったが、身代金は支払わずにシステムやデータを復旧させた
- 被害にはあっていない
- 被害にあったかどうか分からない

## Q4\_2 ランサムウェア感染被害の経験：企業属性別

Q：あなたの勤務先で、ランサムウェア感染による被害を経験したことがありますか。（SA）

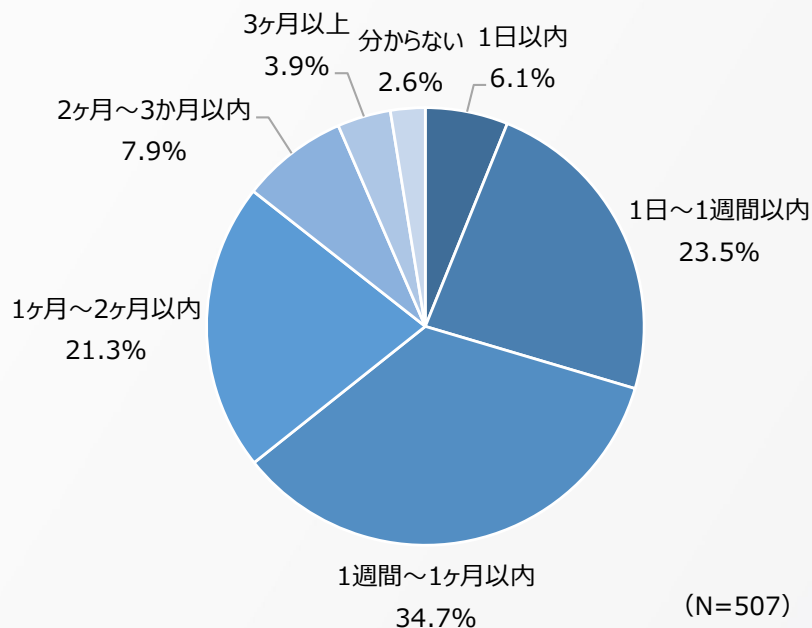
- 業種別：製造の感染率が最も高い（57.1%）。それに続くのが、情報通信（50.0%）となっている。製造は、身代金を支払ったがシステム・データを復旧できなかった割合も高くなっている。
- 従業員規模別：300人以上での感染率はそれほど変わらず、ほぼ半数で感染を経験している。また、50～299人での感染率は37.0%となっており、中小企業でも攻撃対象になっていることが分かる。



## Q4\_3 ランサムウェア感染からの復旧期間

Q：ランサムウェア感染を検知後、データやシステムの復旧までにどの程度の期間を要しましたか。Q4\_2で復旧できなかったと回答した方は、復旧作業を行っていた期間についてお答えください。（SA）

- 復旧までに1週間以内だった割合は約30%、1週間～1か月以内は約35%、合計で約65%が1か月以内で復旧、もしくは作業を終了している。
- 一方で、1か月以上要した企業も約3割存在しており、被害の深刻度やシステムの複雑さによって復旧に長期間を要するケースが少なくない。



## Q4\_3 ランサムウェア感染からの復旧期間：感染状況別

Q：ランサムウェア感染を検知後、データやシステムの復旧までにどの程度の期間を要しましたか。Q4\_2で復旧できなかったと回答した方は、復旧作業を行っていた期間についてお答えください。（SA）

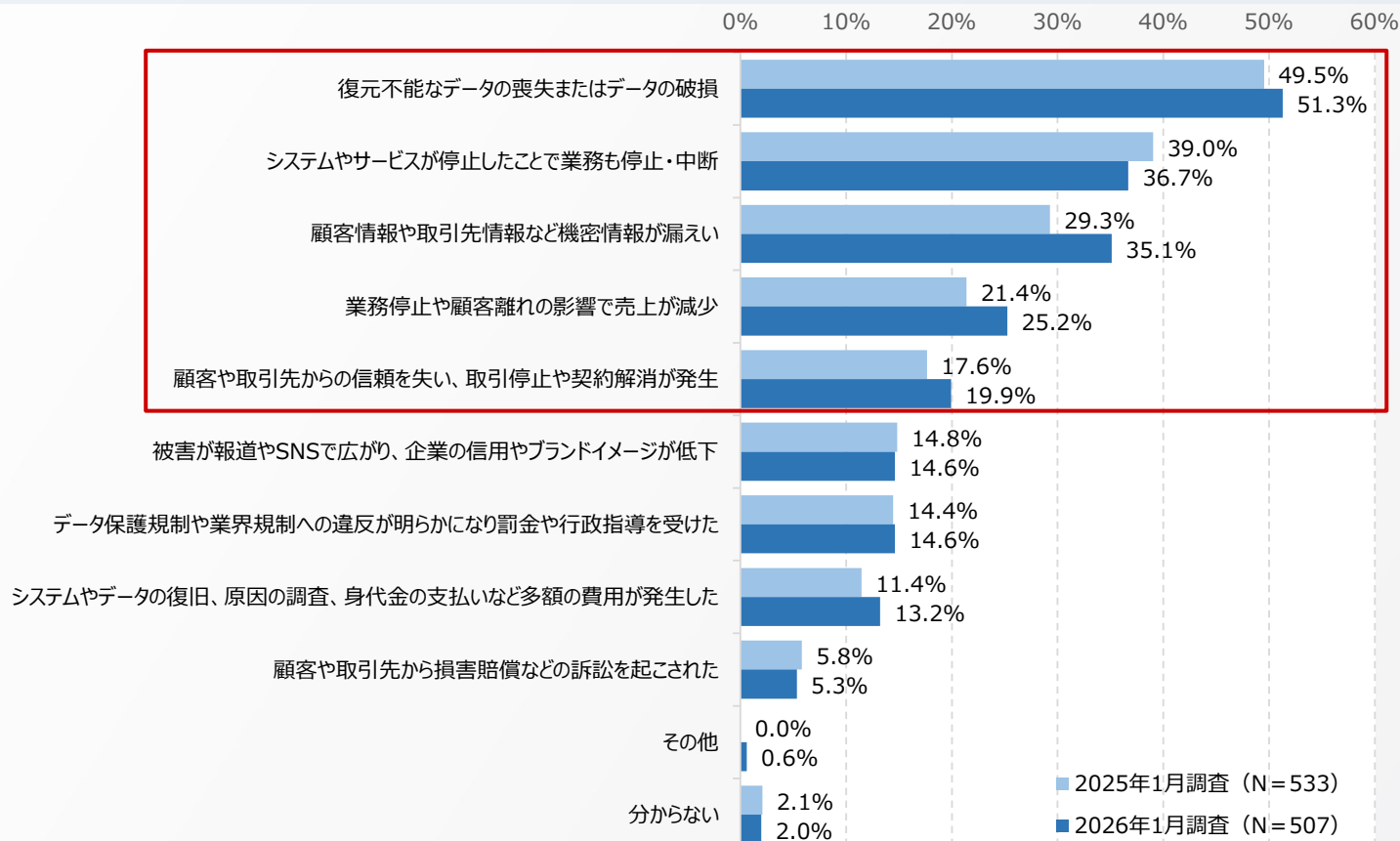
- 身代金を支払って復旧した企業では、1週間以内の割合が相対的に高く、復旧スピードは最も速い。
- 身代金を支払わずに復旧できた企業では、1カ月以内で6割以上が復旧している。
- 身代金を支払ったが復旧できなかった企業、支払わずに復旧できなかった企業は、約4割が1カ月以上を費やし、復旧できずに作業を終了している。

	全 体	ランサムウェア感染状況			
		感染被害にあい、身代金を支払ってシステムやデータを復旧させた	感染被害にあい、身代金を支払ったがシステムやデータは復旧できなかった	感染被害にあい、身代金を支払わなかったためシステムやデータを復旧できなかった	感染被害にはあったが、身代金は支払わずにシステムやデータを復旧させた
該当数	507	83	139	144	141
1日以内	6.1	16.9	5.0	2.8	4.3
1日～1週間以内	23.5	26.5	21.6	15.3	31.9
1週間～1ヶ月以内	34.7	33.7	33.8	38.2	32.6
1ヶ月～2ヶ月以内	21.3	16.9	21.6	28.5	16.3
2ヶ月～3か月以内	7.9	2.4	10.1	8.3	8.5
3ヶ月以上	3.9	2.4	5.0	4.2	3.5
分からない	2.6	1.2	2.9	2.8	2.8

# Q4\_4 ランサムウェア感染被害による影響

Q：ランサムウェア被害によってどのような影響を受けましたか。当てはまるものをすべてお答えください。  
(MA)

- 復元不能なデータの喪失・破損とシステム停止による業務中断は前回調査から変わらず上位に挙がっており、業務やデータへの影響は依然として大きい状況にある。
- 顧客・取引先情報の漏えいや売上減少、取引停止・契約解除といった項目が前回調査より上昇しており、ビジネスへの直接的ダメージや顧客・社会に対する信頼の低下にまで波及している傾向が強まっている。



# Q4\_4 ランサムウェア感染被害による影響：感染状況別

Q：ランサムウェア被害によってどのような影響を受けましたか。当てはまるものをすべてお答えください。  
(MA)

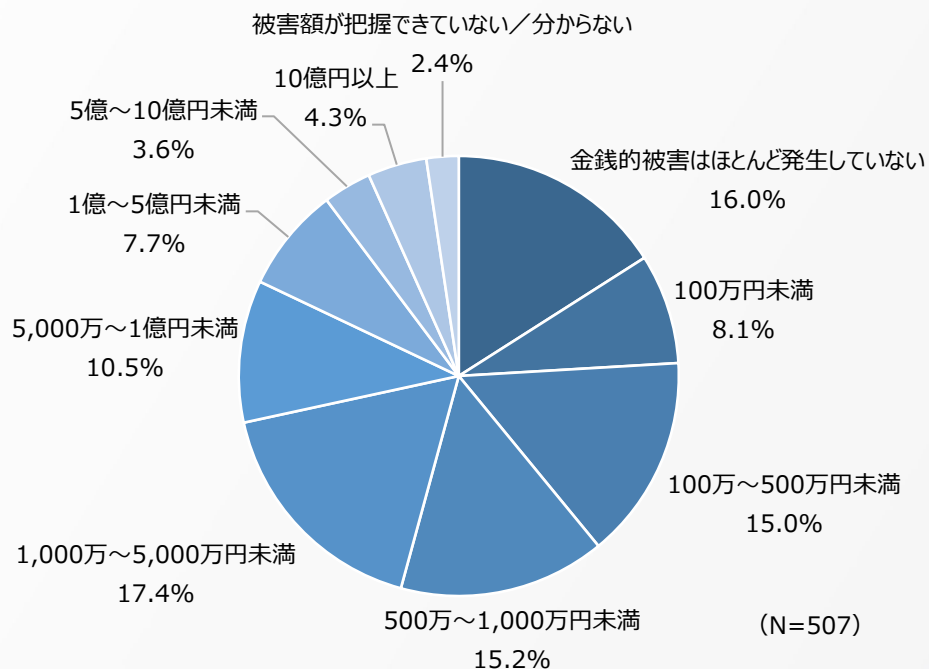
- 身代金を支払って復旧した企業では、システム停止による業務中断が高く、早期復旧を優先する判断に至った背景として、業務停止のインパクトが極めて大きかったことがうかがえる。一方で、データ喪失や情報漏えいも多くの企業で発生している。
- 身代金を支払っても復旧できなかった企業では、復元不能なデータの喪失・破損が最も高く、加えて売上減少やブランド低下、規制対応など影響が広範に及んでいる。身代金支払いが被害軽減につながっていない。
- 身代金を支払わなかった企業は、情報漏えいや売上減少、取引停止・契約解除の割合が相対的に高く、ビジネスへの直接的な影響が大きくなりやすい傾向が見られる。

	全体	ランサムウェア感染状況			
		感染被害にあり、身代金を支払ってシステムやデータを復旧させた	感染被害にあり、身代金を支払ったがシステムやデータは復旧できなかった	感染被害にあり、身代金を支払わなかったためシステムやデータを復旧できなかった	感染被害にはあつたが、身代金は支払わずにシステムやデータを復旧させた
該当数	507	83	139	144	141
復元不能なデータの喪失またはデータの破損	51.3	50.6	59.0	45.8	49.6
システムやサービスが停止したことで業務も停止・中断	36.7	61.4	30.9	19.4	45.4
顧客情報や取引先情報など機密情報が漏えい	35.1	37.3	29.5	36.1	38.3
業務停止や顧客離れの影響で売上が減少	25.2	21.7	23.7	27.1	27.0
顧客や取引先からの信頼を失い、取引停止や契約解消が発生	19.9	20.5	13.7	23.6	22.0
被害が報道やSNSで広がり、企業の信用やブランドイメージが低下	14.6	9.6	18.0	11.8	17.0
データ保護規制や業界規制への違反が明らかになり罰金や行政指導を受けた	14.6	20.5	13.7	13.2	13.5
システムやデータの復旧、原因の調査、身代金の支払いなど多額の費用が発生した	13.2	10.8	12.2	14.6	14.2
顧客や取引先から損害賠償などの訴訟を起こされた	5.3	7.2	2.9	5.6	6.4
分からない	2.0	2.4	2.9	0.7	2.1

## Q4\_5 ランサムウェア感染被害による被害額

Q：ランサムウェア攻撃によって、どの程度の金銭的被害が発生しましたか。最も近い金額の範囲をお選びください。(SA)

- 被害額は、100～5000万円の範囲で半数近くとなっている。
- 特に1000万～5000万円が最も割合が大きい層となっている。
- 1億円以上の被害も約15%あり、被害額の分布は広い。



※被害額に含む項目

- 事故調査
- 被害範囲調査
- 身代金支払い額
- データやシステムの復旧・再構築
- 再発防止のためのセキュリティ対策費用

# Q4\_5 ランサムウェア感染被害による被害額：感染状況別

Q：ランサムウェア攻撃によって、どの程度の金銭的被害が発生しましたか。最も近い金額の範囲をお選びください。  
(SA)

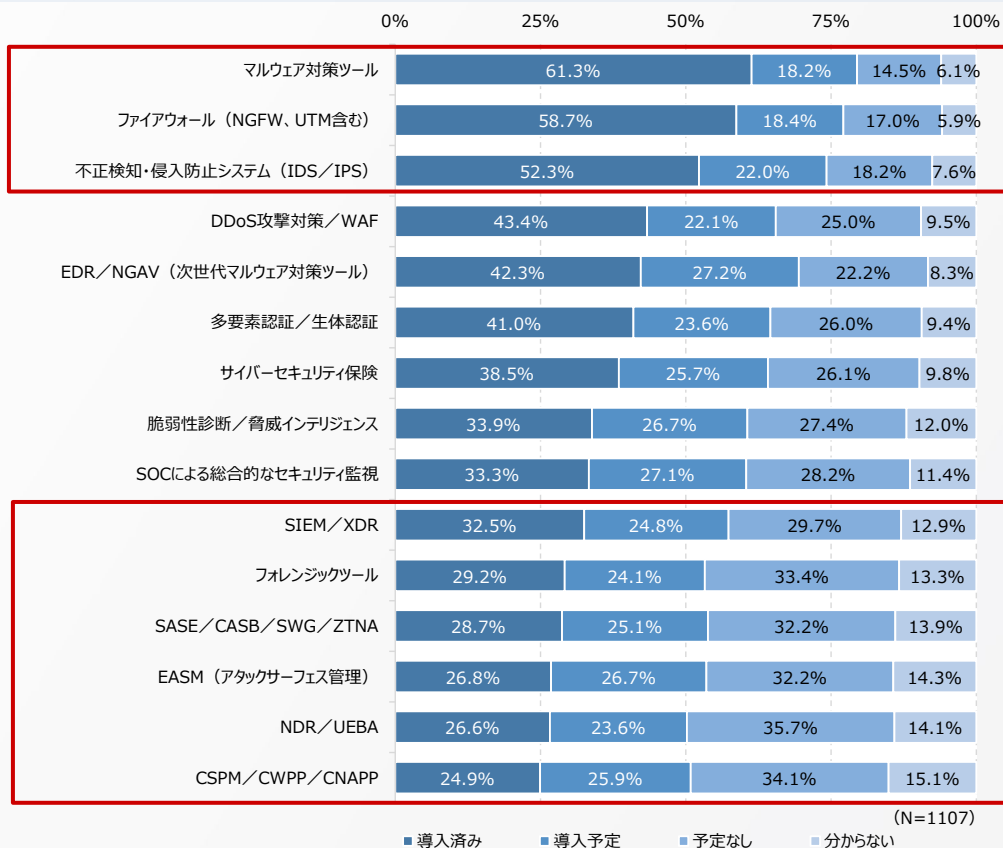
- 身代金を支払って復旧した企業：被害額は1,000万～5,000万円未満が中心だが、1億円以上も一定数存在する。早期復旧はできたものの、身代金や復旧・再発防止費用が積み上がり、結果として被害額が膨らんだケースが多いと考えられる。
- 身代金を支払ったが復旧できなかった企業：5,000万円以上の割合が相対的に高く、被害額が大きくなりやすい。支払いに加え、復旧失敗による再構築や事業影響が重なり、最もコストインパクトが大きい層となっている。
- 身代金を支払わず復旧できなかった企業：ほとんどが100万～1億円未満のレンジで分布している。
- 身代金を支払わず復旧できた企業：金銭的被害はほとんど発生していない企業や1,000万円未満の割合が相対的に高く、最も被害額を抑制できている。

	全 体	ランサムウェア感染状況			
		感染被害にあい、身代金を支払ってシステムやデータを復旧させた	感染被害にあい、身代金を支払ったがシステムやデータは復旧できなかった	感染被害にあい、身代金を支払わなかったためシステムやデータを復旧できなかった	感染被害にはあったが、身代金は支払わずにシステムやデータを復旧させた
該当数	507	83	139	144	141
金銭的被害はほとんど発生していない	16.0	18.1	12.9	11.1	22.7
100万円未満	8.1	9.6	10.8	4.9	7.8
100万～500万円未満	15.0	12.0	10.8	22.2	13.5
500万～1,000万円未満	15.2	12.0	13.7	18.1	15.6
1,000万～5,000万円未満	17.4	19.3	17.3	18.8	14.9
5,000万～1億円未満	10.5	4.8	10.8	14.6	9.2
1億～5億円未満	7.7	10.8	10.1	4.2	7.1
5億～10億円未満	3.6	3.6	5.8	2.8	2.1
10億円以上	4.3	7.2	5.0	1.4	5.0
被害額が把握できていない／分からない	2.4	2.4	2.9	2.1	2.1

# Q4\_6 サイバー攻撃対策の導入状況

Q：あなたの勤務先において、「外部からのサイバー攻撃対策」として導入しているものは何ですか。それぞれについて導入状況をお答えください。（SA）

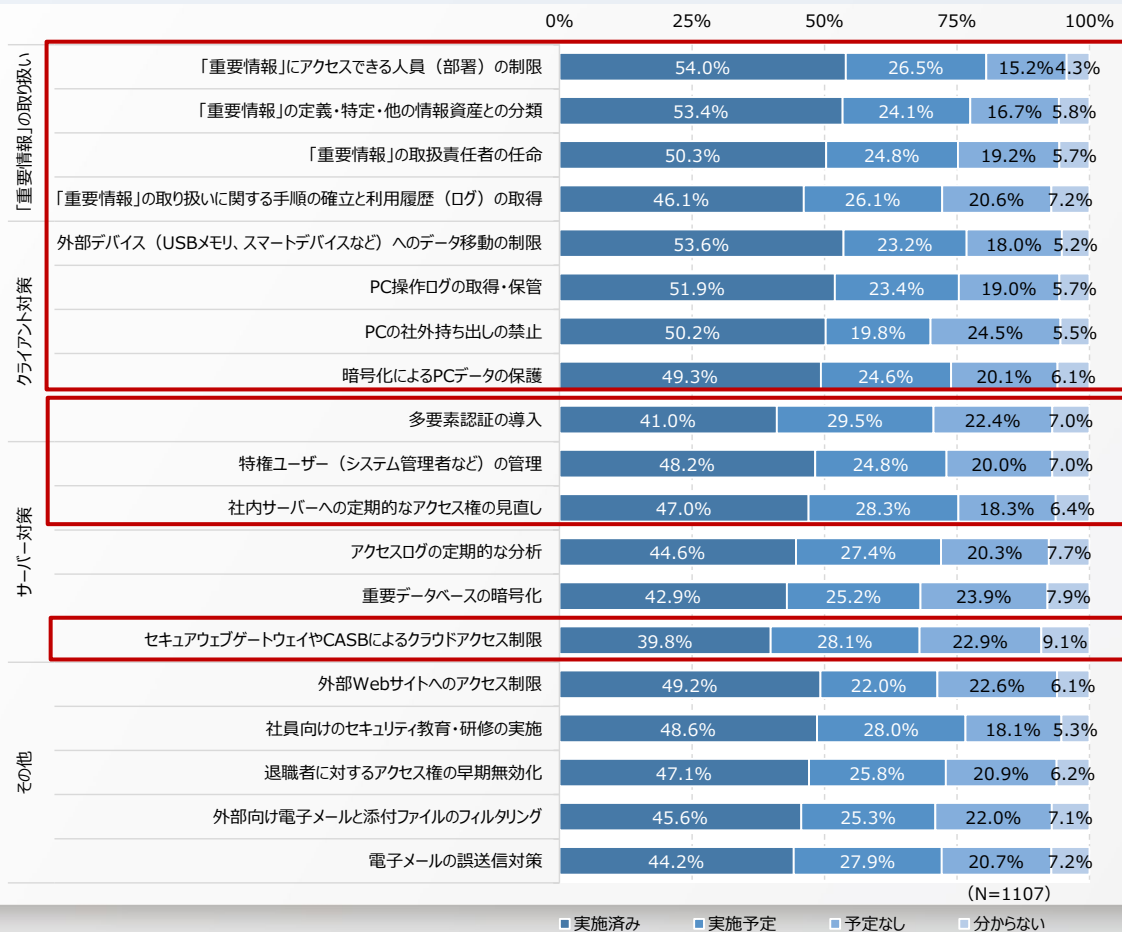
- マルウェア対策、ファイアウォール、IDS/IPSといった従来型の境界防御・エンドポイント対策は導入済みが過半を占めており、外部攻撃対策のベースラインとして広く定着している。
- SIEM/XDR、SASE/CASB/SWG/ZTNA、EASM、NDR/UEBA、CSPM/CWPP/CNAPPなどのゼロトラスト型セキュリティツールは、導入済みの割合は低いものの、導入予定は比較的高い。サーバー攻撃の高度化やクラウド環境の拡大を背景に、今後導入が拡大していくと見られる。



# Q4\_7 情報漏えい対策の導入状況

Q：あなたの勤務先において、「内部からの情報漏えい対策」として実施しているものは何ですか。それぞれについて実施状況をお答えください。（SA）

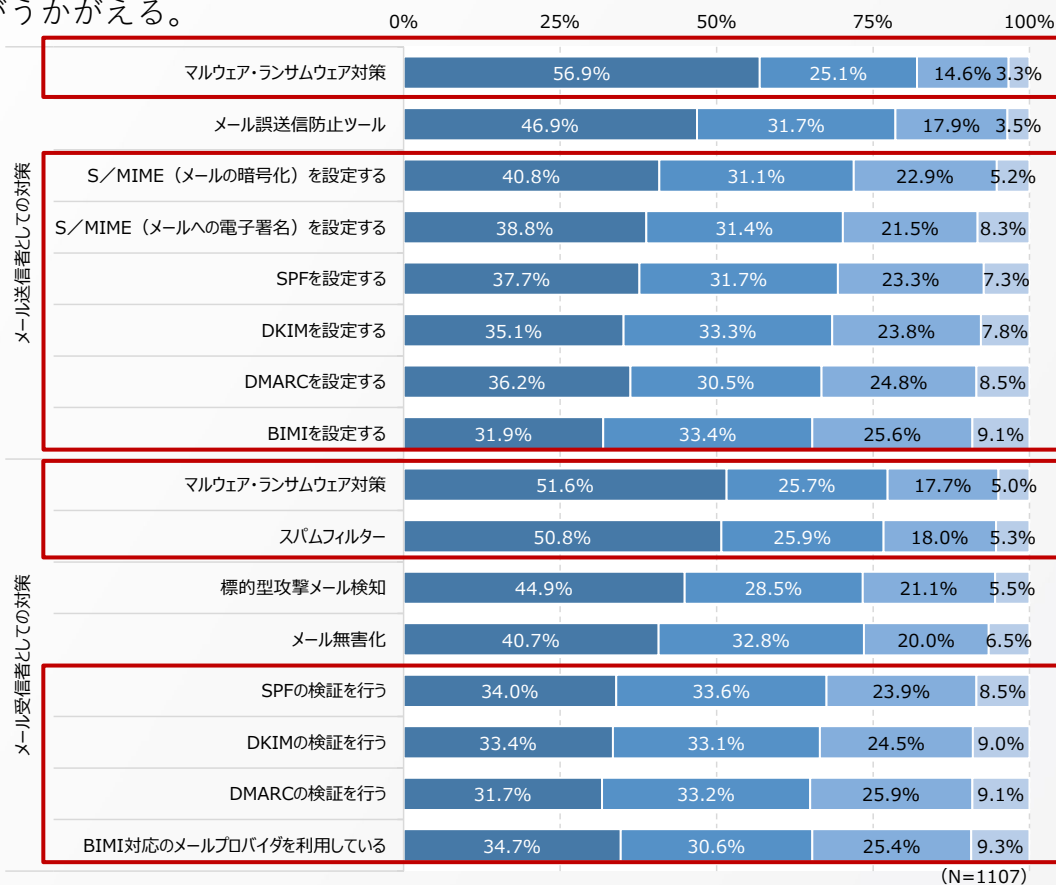
- 重要情報の取り扱いとクライアント対策のような、人の行動と端末を管理する基本的な内部不正・誤操作対策の多くで実施済みが過半を占めており、内部情報漏えい対策のベースラインとして定着している。
- 多要素認証、特権ユーザー管理、アクセス権の定期的な見直し、CASBによるクラウドアクセス制御などは実施予定も多く、ゼロトラストやID中心の統制へ移行しつつある過渡期にあることがうかがえる。



# Q4\_8 電子メールのセキュリティ対策状況

Q：あなたの勤務先の電子メールのセキュリティ対策について、以下の各対策について現在の実施状況をそれぞれお答えください。（SA）

- マルウェア・ランサムウェア対策やスパムフィルタといった基本的なメール防御策は、実施している企業が過半を占めており、対策が標準装備化している。
- S/MIME、SPF、DKIM、DMARC、BIMIといった送信ドメイン認証・真正性確保の仕組みは、今後実施したい企業の割合が高い。なりすまし・フィッシング対策として重要性は理解されつつあり、徐々に導入が進んでいる状況がうかがえる。



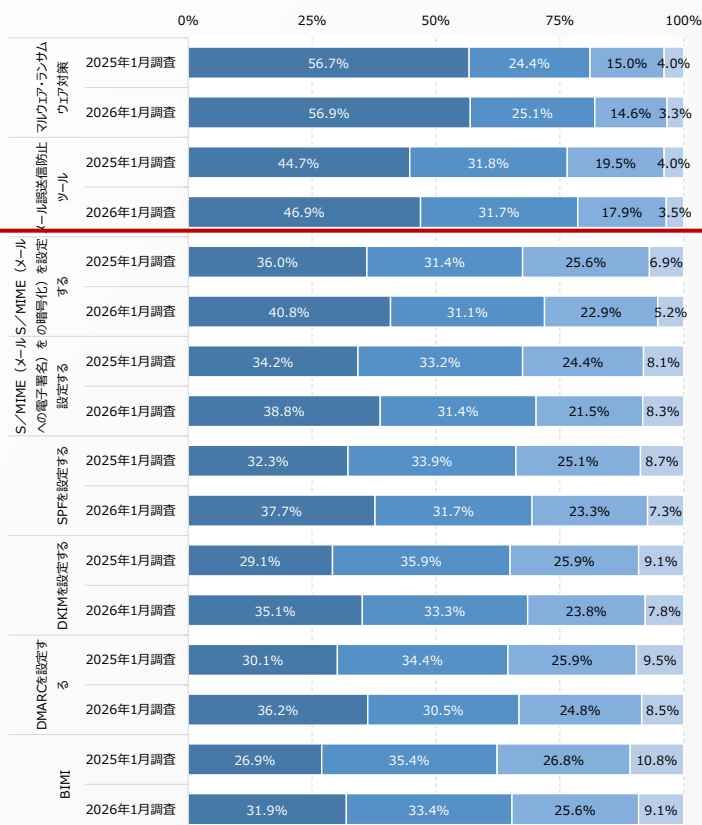
■ 現在実施している ■ 今後実施したい □ 実施予定なし □ 技術自体を知らない

# Q4\_8 電子メールのセキュリティ対策状況：前回調査との比較

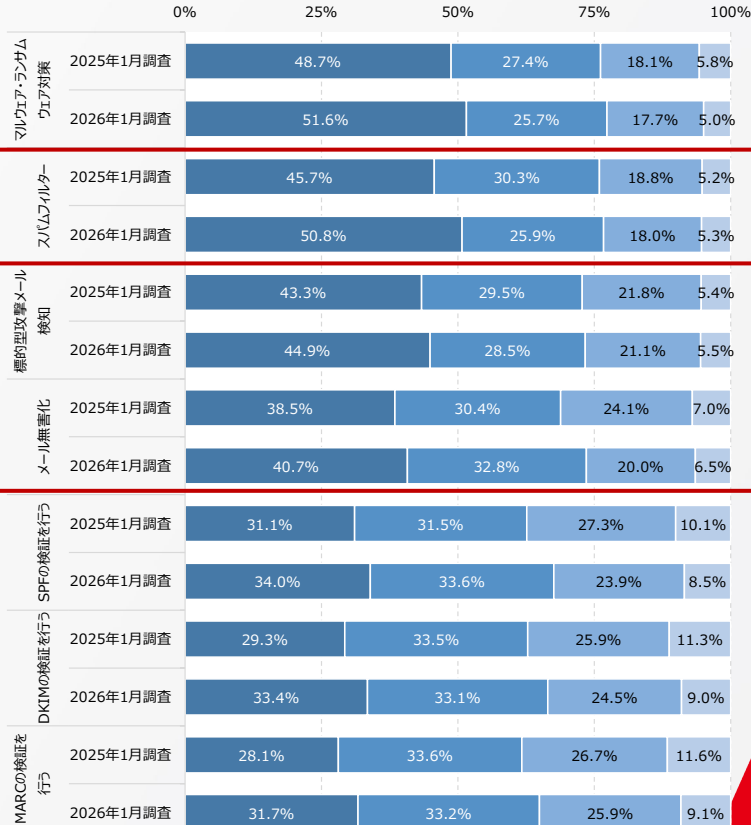
Q：あなたの勤務先の電子メールのセキュリティ対策について、以下の各対策について現在の実施状況をそれぞれお答えください。（SA）

- ・ 送信者としての対策：S/MIME、SPF、DKIM、DMARC、BIMIといった送信ドメイン認証・真正性確保は前回調査より実施率が向上している。
- ・ 受信者としての対策：スパムフィルターの実施率が大きく上昇し、過半数に達している。また、送信者対策と同様に、S/MIME、SPF、DKIM、DMARCの実施率も上昇している。

【メール送信者としての対策】



【メール受信者としての対策】



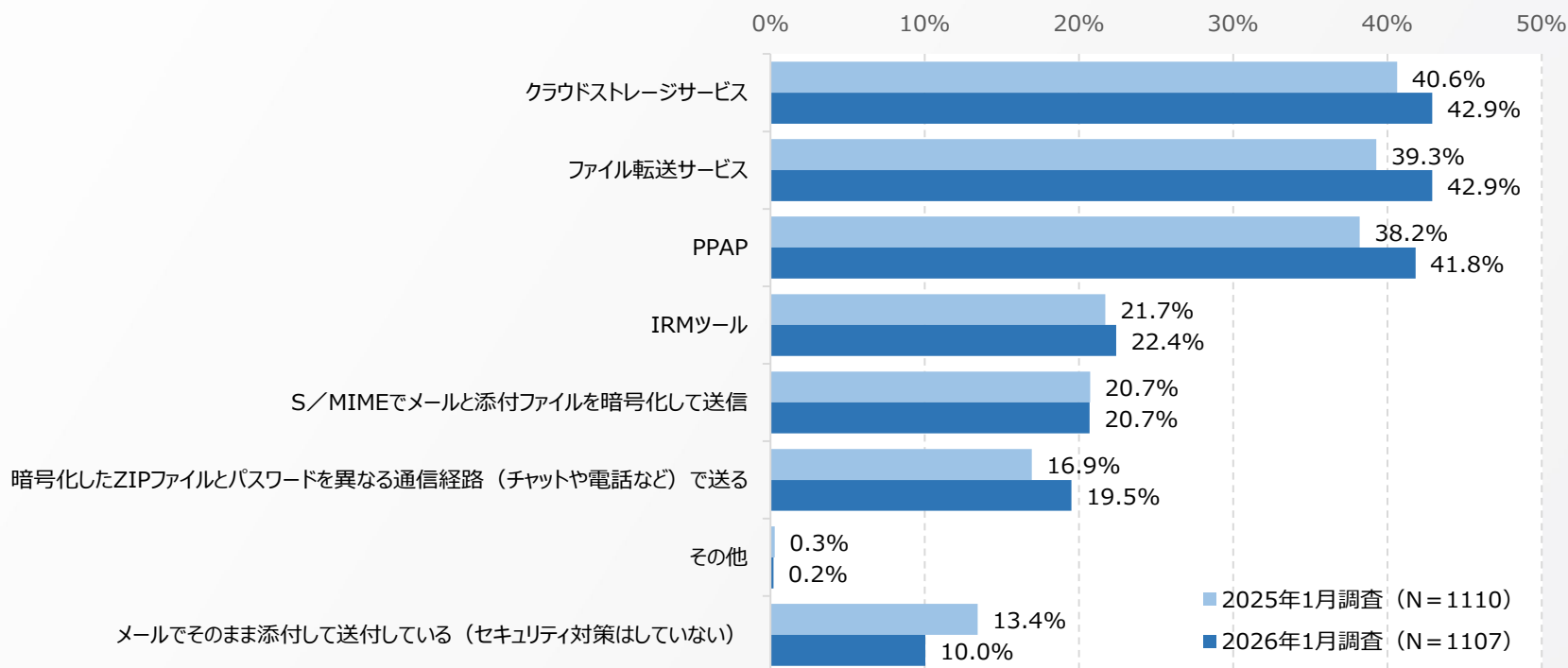
■ 現在実施している ■ 今後実施したい ■ 実施予定なし ■ 技術自体を知らない  
2025年1月調査 (N=1110)  
2026年1月調査 (N=1107)

■ 現在実施している ■ 今後実施したい ■ 実施予定なし ■ 技術自体を知らない  
2025年1月調査 (N=1110)  
2026年1月調査 (N=1107)

## Q4\_9 電子メールでのファイル送付手段

Q：外部の取引先に電子メールでファイルを送付する際に、社内の標準として採用しているファイル送付の手段は何ですか。当てはまるものをすべてお答えください。（MA）

- クラウドストレージ、ファイル転送サービス、PPAPの3つの手段が主流となっており、前回調査からも上昇している。PPAPは、その脆弱性が指摘されているが、依然として主要な手段として利用されている。
- 一方で、IRMやS/MIMEといったファイル自体の制御・暗号化を前提とした仕組みの採用は20%程度にとどまっている。利便性を優先した代替手段が広がる中で、情報の二次利用防止や持ち出し制御まで踏み込んでいる企業は限定的である。



※PPAP：メールでパスワード付きのZIPファイルを送信し、その後メールでパスワードを別送する方法

※IRM：添付ファイルを暗号化しアクセス権限を制御するツール

# 5

## 第三者認証制度取得に関する取り組み

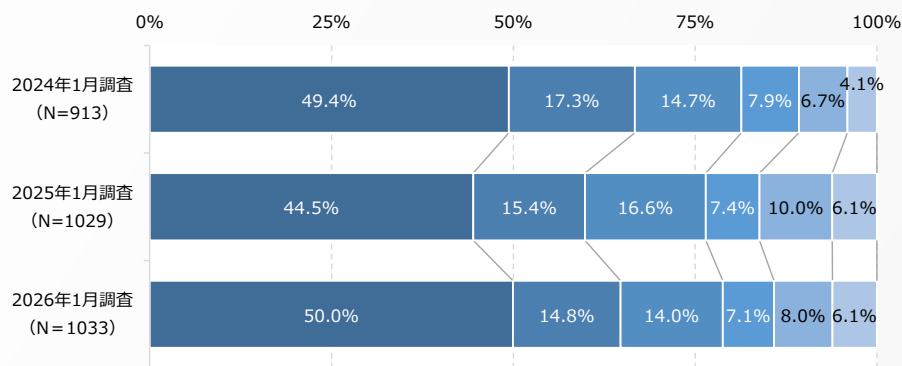
- Q5\_1 プライバシーマーク／ISMS認証の取得状況
- Q5\_2 プライバシーマーク／ISMS認証取得の背景
- Q5\_3 プライバシーマーク／ISMS認証取得による効果
- Q5\_4 業務委託事業者の選定で重視する点
- Q5\_5 クラウドサービス選定において重視するセキュリティの取り組み
- Q5\_6 クラウドサービス選定で重視する第三者評価
- Q5\_7 提供するITサービスの品質向上に向けた取り組み

# Q5\_1 プライバシーマーク／ISMS認証の取得状況

Q：情報セキュリティに関する以下の認証制度に対して、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。

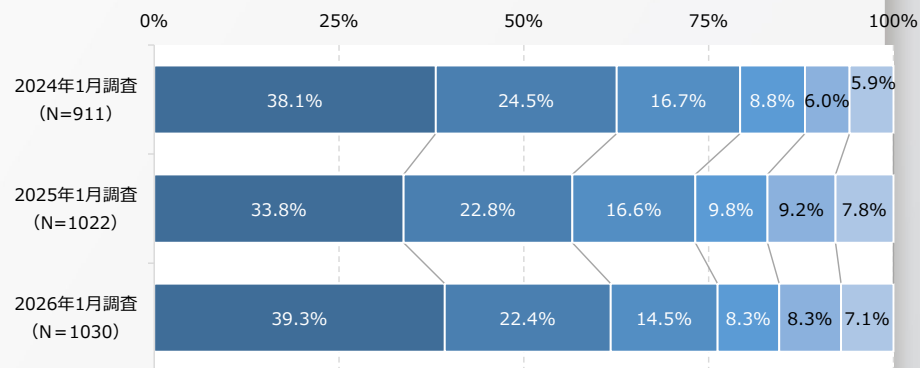
- プライバシーマークは、「取得済み・継続予定」の割合が2025年から上昇し、2024年調査を上回った。「取得済みだが継続しない予定」は年々低下しており、取得企業が拡大する流れが見られる。
- ISMS認証も、「取得済み・継続予定」の割合が2025年から上昇し、2024年調査を上回った。「取得済みだが継続しない予定」は22.4%あるものの、年々、徐々に低下している。

【プライバシーマーク】



- 取得済みであり、今後も継続予定
- 取得済みだが、今後の継続はしない予定
- 今後取得する予定
- 取得予定はないが、制度内容を参考している
- 取得・登録予定はなく、制度の概要も知らない
- 取得予定はないが、制度の概要は知っている

【ISMS認証】



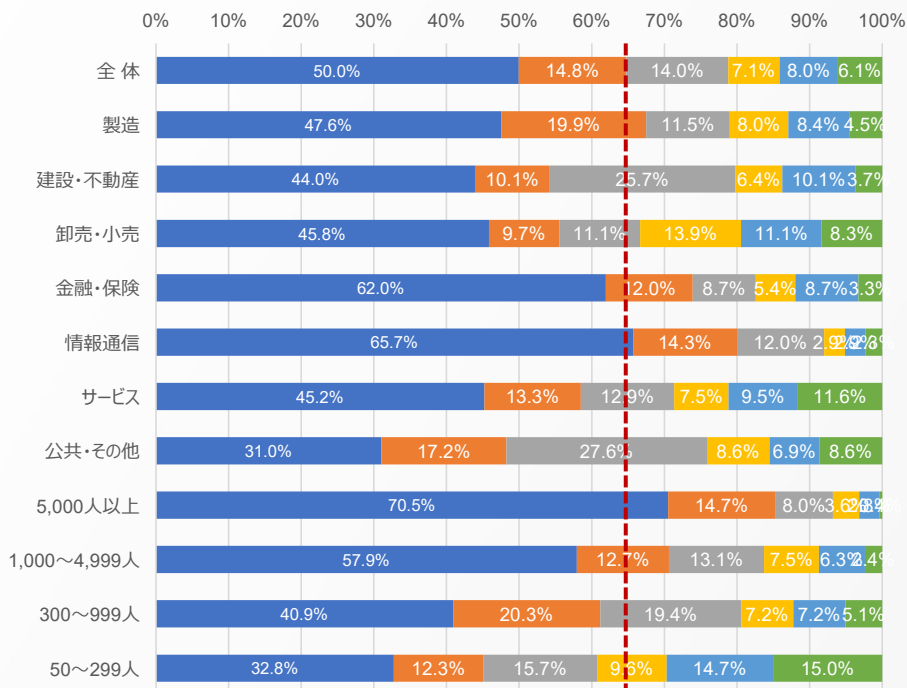
- 取得済みであり、今後も継続予定
- 取得済みだが、今後の継続はしない予定
- 今後取得する予定
- 取得予定はないが、制度内容を参考している
- 取得・登録予定はなく、制度の概要も知らない
- 取得予定はないが、制度の概要は知っている

# Q5\_1 プライバシーマーク／ISMS認証の取得状況：企業属性別

Q：情報セキュリティに関する以下の認証制度に対して、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。

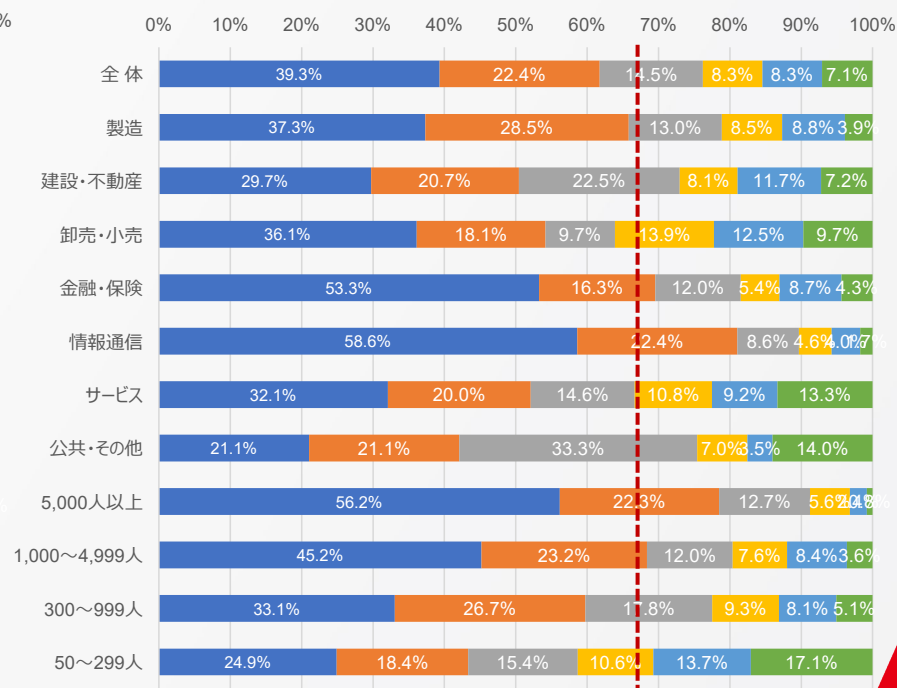
- プライバシーマーク：業種別では、取得率が最も高いのは情報通信、次に金融・保険、製造が続く。公共・その他は現在の取得率は低いものの、今後取得予定の割合は非常に高い。
- ISMS認証：業種別では、取得率が最も高いのは情報通信、次に金融・保険、製造が続く。ただし、製造は取得済み・継続なし予定の割合が高い。公共・その他は取得率は低いものの、今後取得予定の割合は非常に高い。

### 【プライバシーマーク】



- 取得済みであり、今後も継続予定
- 取得済みだが、今後の継続はしない予定
- 今後取得する予定
- 取得予定はないが、制度内容を参考している
- 取得予定はないが、制度の概要は知っている
- 取得・登録予定はなく、制度の概要も知らない

### 【ISMS認証】



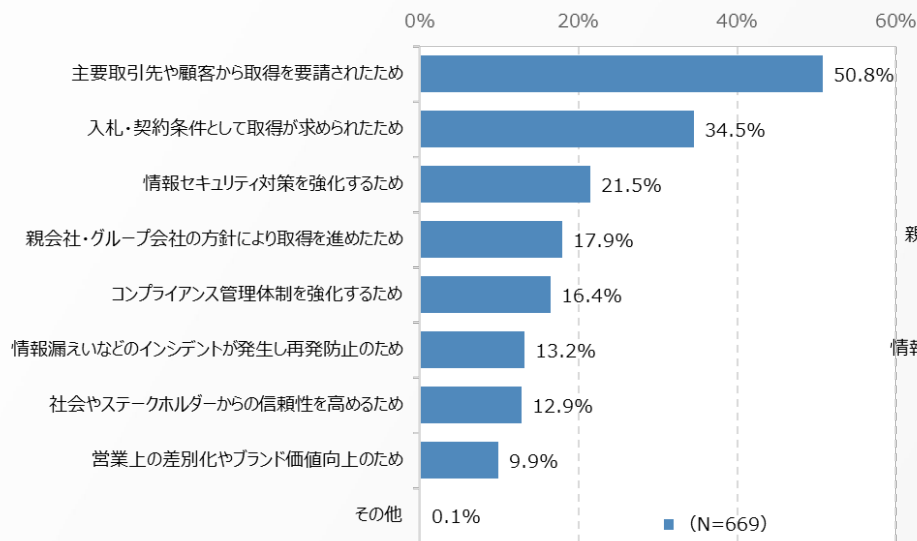
- 取得済みであり、今後も継続予定
- 取得済みだが、今後の継続はしない予定
- 今後取得する予定
- 取得予定はないが、制度内容を参考している
- 取得予定はないが、制度の概要は知っている
- 取得・登録予定はなく、制度の概要も知らない

## Q5\_2 プライバシーマーク／ISMS認証取得の背景

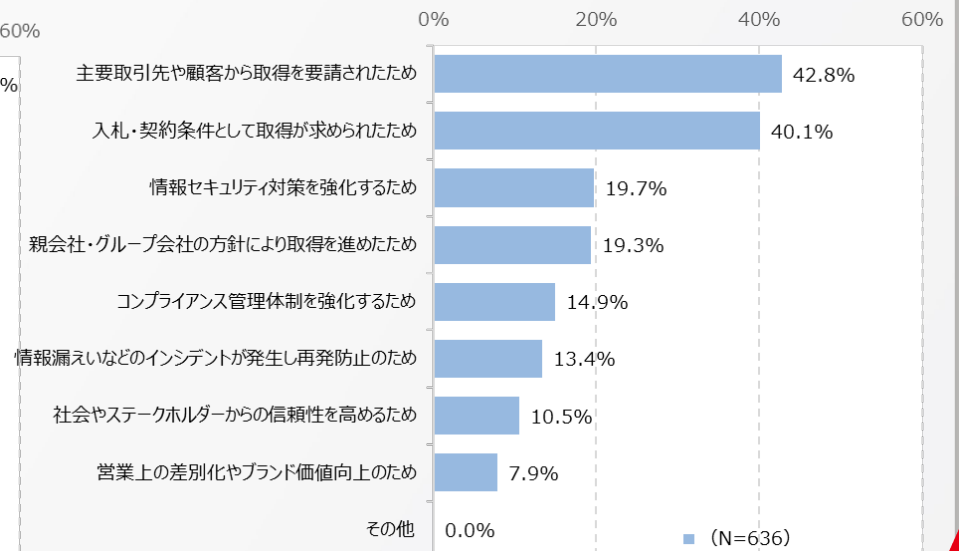
Q：あなたの勤務先が以下の第三者認証を取得した背景や動機は何でしたか？それぞれについて当てはまるものすべてをお答えください。（MA）

- プライバシーマーク、ISMS認証ともに、主要取引先・顧客からの要請、入札・契約条件として求められたことが上位にあり、取引や契約の前提条件となるような外部要請からの取得が強いことが分かる。
- 一方で、情報セキュリティ対策やコンプライアンス管理体制の強化、グループ方針への対応といった内部要因も一定割合を占めており、外部からの要請を契機にしつつ、社内統制や信頼性向上を目的としたガバナンス強化へつなげている企業も少なくないことがうかがえる。

【プライバシーマーク】



【ISMS認証】



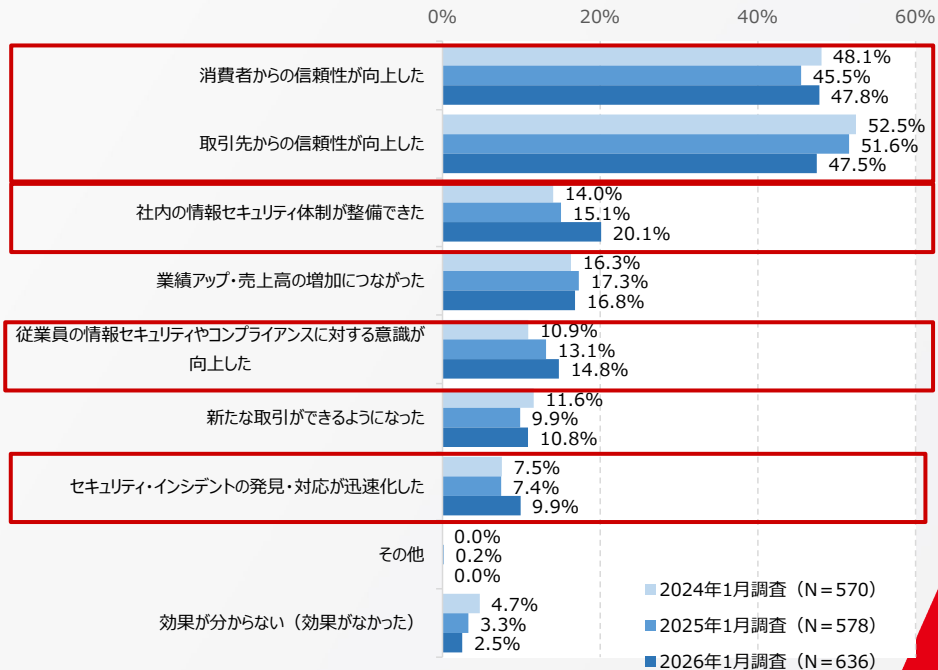
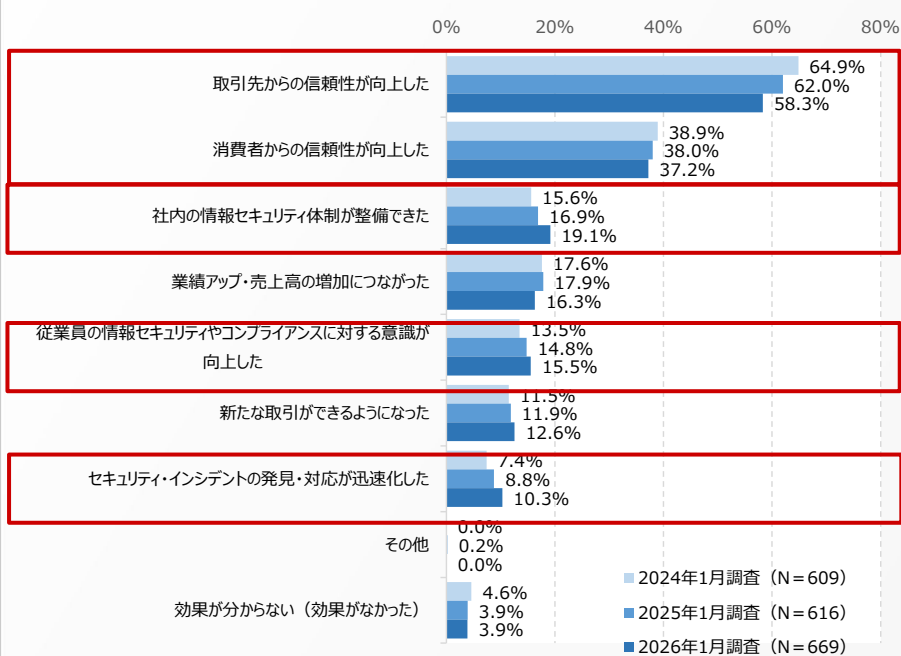
# Q5\_3 プライバシーマーク／ISMS認証取得による効果

Q：あなたの勤務先が以下の第三者認証を取得したことによる効果はどのようなことがありますか。それぞれについて当てはまるものすべてをお答えください。（MA）

- プライバシーマーク、ISMS認証ともに、取引先と消費者からの信頼性向上が最も多い効果となっているが、比率が下がる傾向にある。
- 一方で、セキュリティ体制の整備や従業員のコンプライアンス意識の向上、さらにセキュリティ・インシデントの発見・対応の迅速化の比率が年々上昇しており、セキュリティ・コンプライアンスの実効性強化につながっている。

【プライバシーマーク】

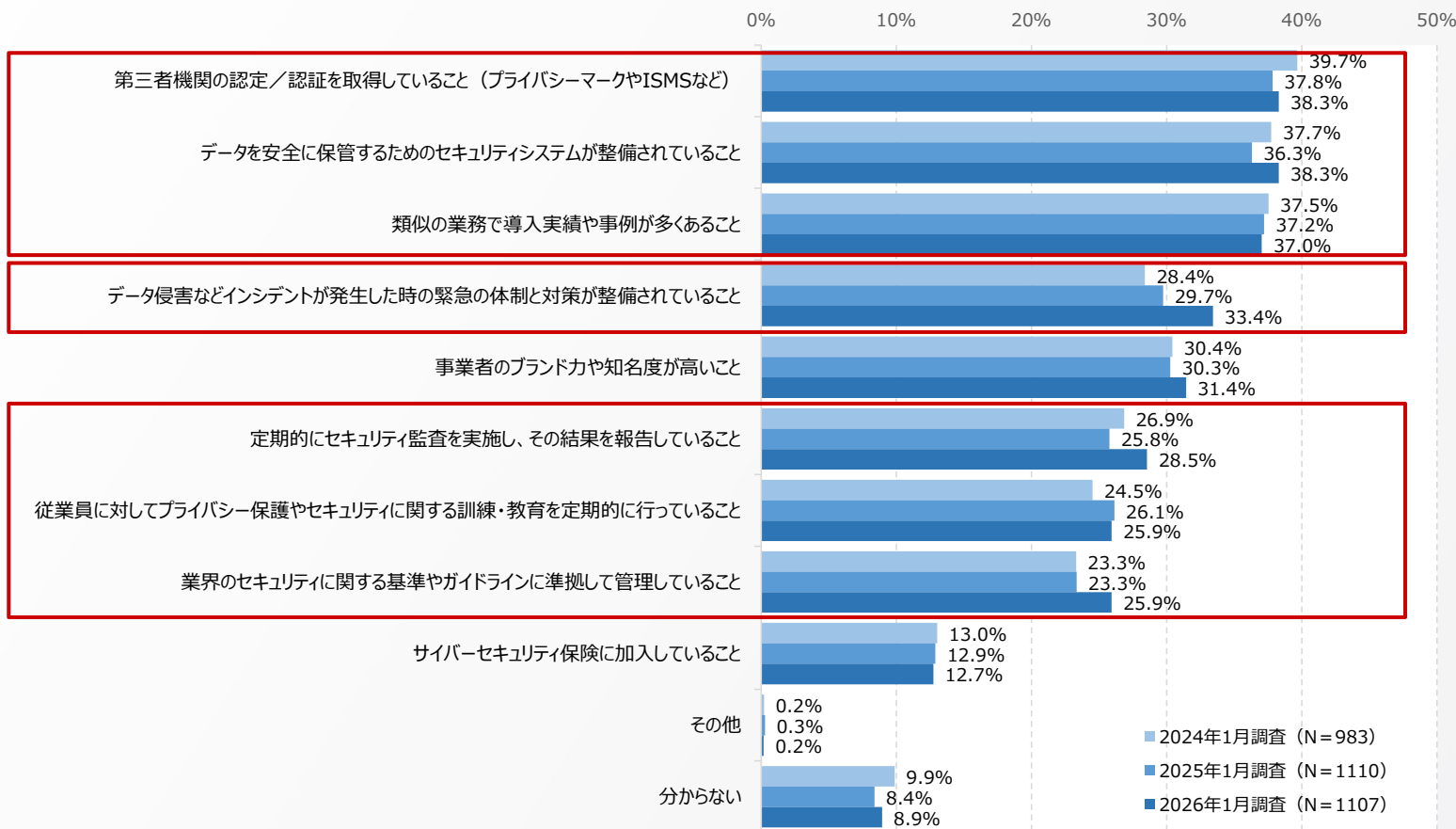
【ISMS認証】



# Q5\_4 業務委託事業者の選定で重視する点

Q：個人情報など機密情報を扱う業務の委託事業者を選定する際、どのような点を重視していますか。当てはまるものをお答えください。（MA）

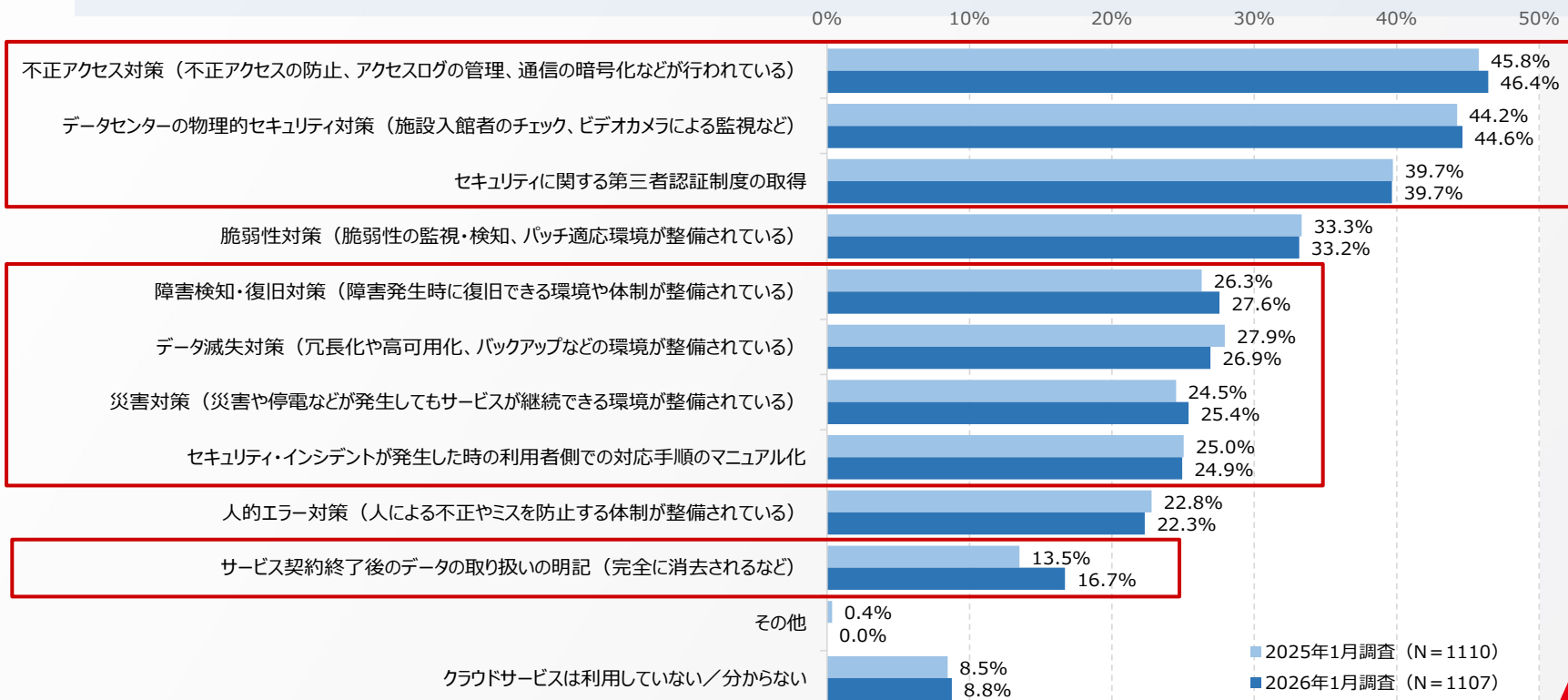
- プライバシーマークやISMSなどの第三者認証は最も重視されており、過去の調査から変わっていない。さらに、セキュリティシステムの整備状況と導入実績も重視される傾向にも変わらない。
- インシデント発生時の対応体制の整備、セキュリティ監査の実施、従業員へのセキュリティ訓練・教育に実施、ガイドラインへの準拠といった実運用レベルでの事業者の対策や対応力を重視する傾向が強まっている。



## Q5\_5 クラウドサービスの選定において重視するセキュリティの取り組み

Q：あなたの勤務先がクラウドサービスを選定する際、重視するサービス提供事業者のセキュリティやデータ保護に関する取り組みは何ですか。当てはまるものすべてお答えください。（MA）

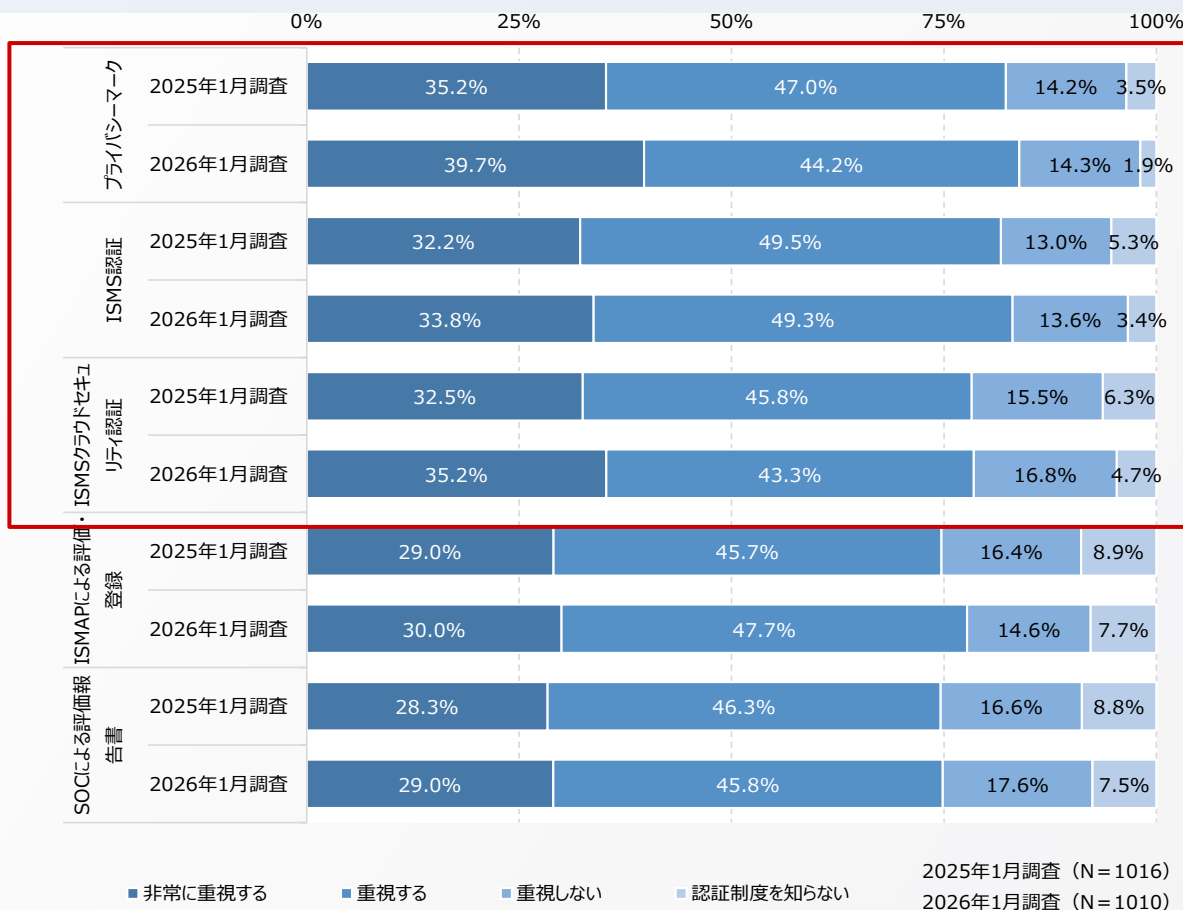
- 不正アクセス対策やデータセンターの物理的セキュリティ、第三者認証の取得は前回調査から引き続き上位であり、クラウド選定における最低条件としてのセキュリティ要件となっている。
- 障害検知・復旧、データ消失対策、災害対策、インシデント発生時の利用者対応手順といったレジリエンスや運用面の取り組みも前回調査と同様に一定数はあり、事故発生を前提とした継続性・復旧力まで含めた評価が定着し始めている。
- サービス契約終了後のデータ取り扱い明記は前回調査から上昇し、徐々に重視されてきている傾向にある。



# Q5\_6 クラウドサービスの選定で重視する第三者評価

Q：あなたの勤務先がクラウドサービスを選定する際、以下の第三者による評価をどの程度重視しますか?それぞれ当てはまるものをお答えください。（SA）

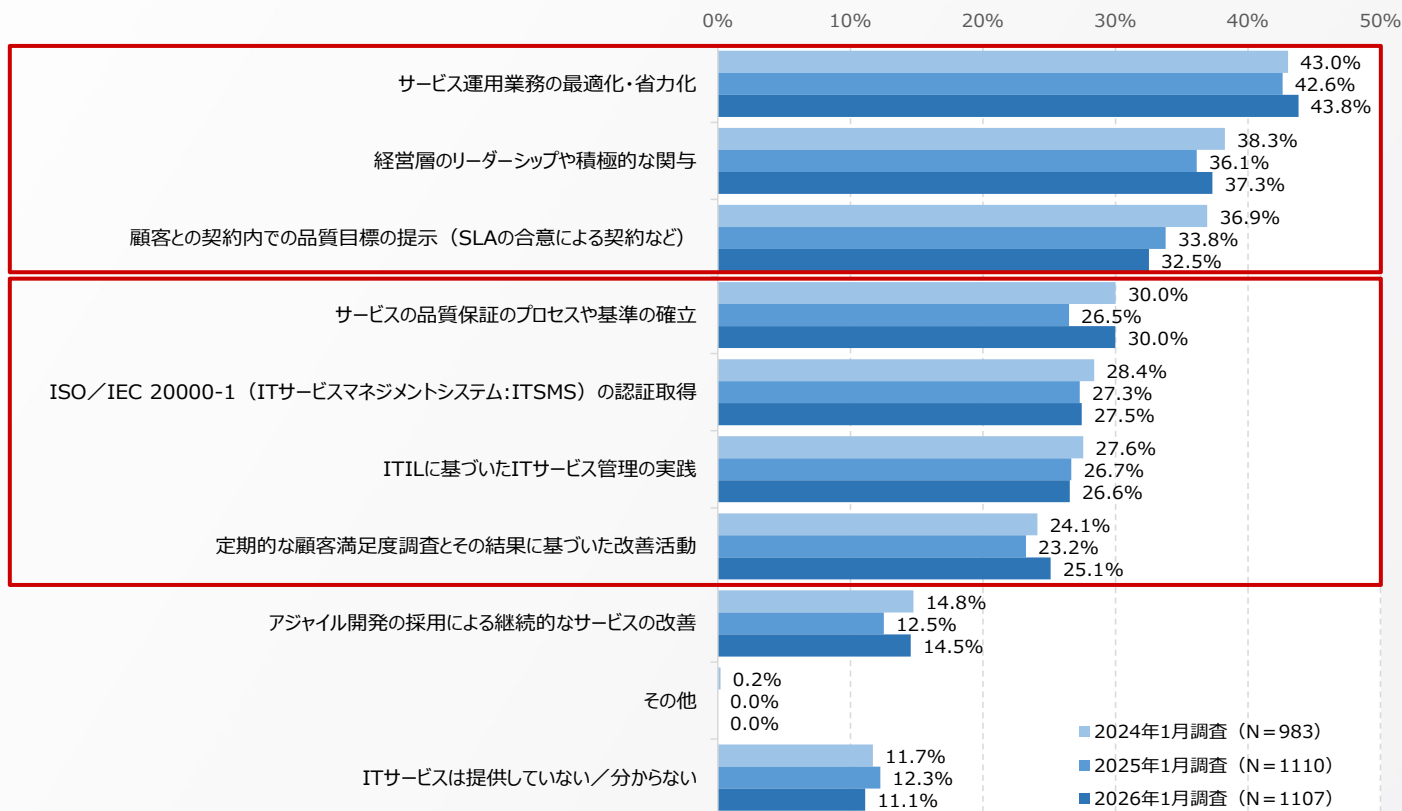
- いずれの第三者評価も前回調査から重視される割合が大きくなっている。
- 特にプライバシーマークとISMSクラウドセキュリティ認証は、非常に重視されている割合の上昇が顕著に見られる。



# Q5\_7 提供するITサービスの品質向上に向けた取り組み

Q：自社で提供するITサービスの品質の確保・向上を図る上で効果的と考える取り組みは何ですか。当てはまるものをすべてお答えください。（MA）

- サービス運用業務の最適化・省力化、経営層のリーダーシップといった項目は変わらず上位に挙がっており、品質向上は経営関与と運用成熟の両輪で実現するものという認識が定着していることがうかがえる。
- SLAを含む契約上の品質目標設定は、上位に挙がっていないものの年々比率は低下している。その一方で、品質保証プロセスの確立や顧客満足度調査に基づいた改善活動は前回調査から上昇している。
- ISO/IEC 20000-1とITILのフレームワーク活用は、年次で大きな変動はないものの安定的に支持されている。



# 6

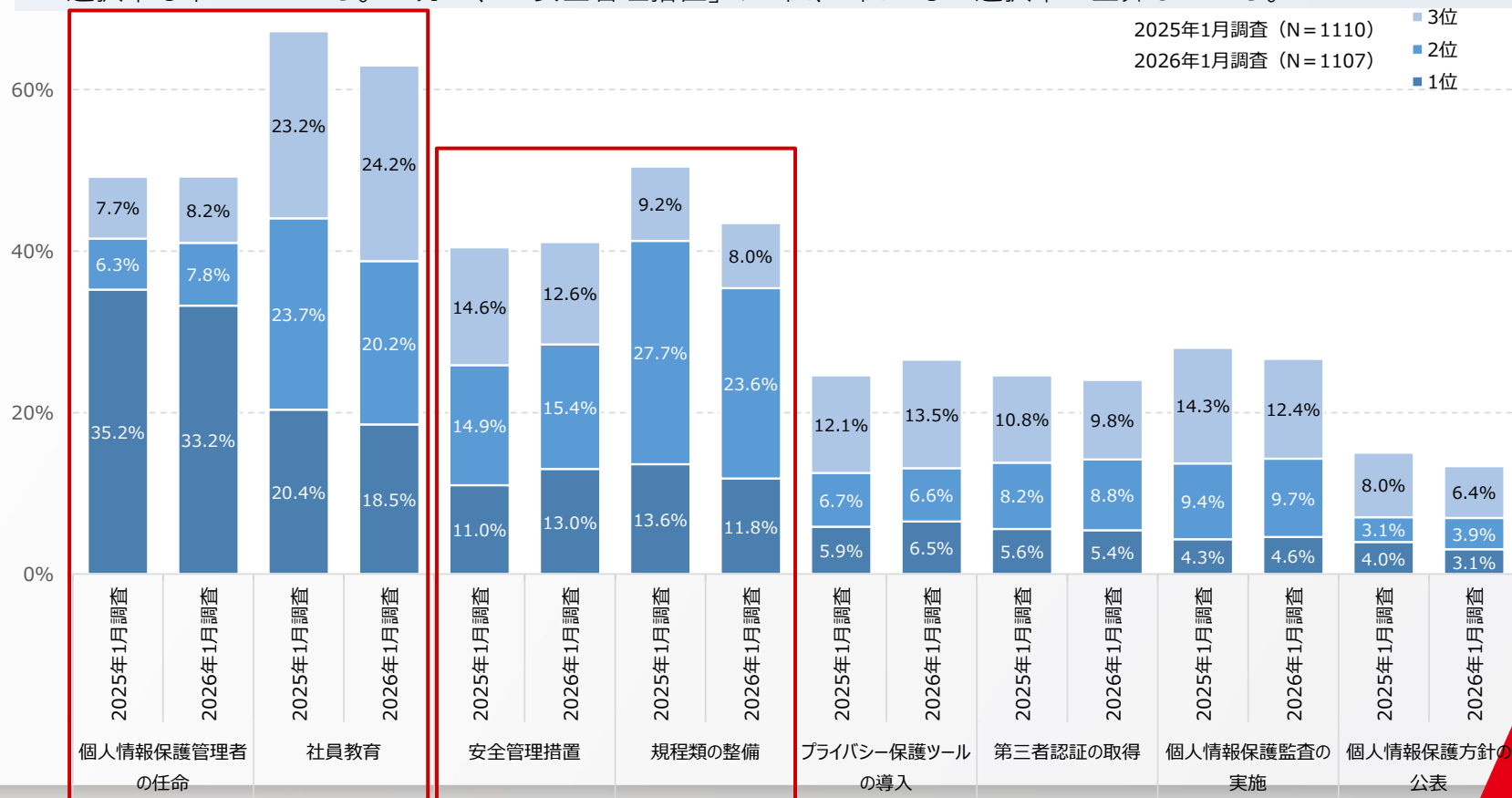
## プライバシー／個人情報保護への取り組み

- Q6\_1 個人情報保護に対する取り組み
- Q6\_2 データの越境移転の状況
- Q6\_3 データの越境移転先の国・地域
- Q6\_4 海外企業とのデータ送受信における課題
- Q6\_5 CBPRの取得検討状況
- Q6\_6 CBPRを取得検討する動機
- Q6\_7 プライバシーガバナンスに関する取り組み
- Q6\_8 プライバシーガバナンスに取り組んだことによる変化
- Q6\_9 プライバシー保護ツール・システムの導入状況
- Q6\_10 プライバシー保護技術（PETs）の認知度

# Q6\_1 個人情報保護に対する取り組み

Q：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。特に注力している取り組みについて、1～3位まで順位を付けてそれぞれ選択してください。（SA）

- 前回調査と同じく「個人情報保護管理者の任命」が1位の比率で最も多い結果となり、責任所在の明確化が中核施策として定着している。ただし、前回調査から1位の選択率はやや下がっている。
- 「社員教育」は1位、2位、3位と満遍なく回答率が高く、教育は不可欠な取り組みとなっている。
- 「規程類の整備」が2位で最も高い選択率となっているが、前回調査から比率は下がっている。さらに、1位選択率も下がっている。一方で、「安全管理措置」は1位、2位ともに選択率が上昇している。



# Q6\_1 個人情報保護に対する取り組み(1位)：個人情報保有件数別

Q：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。特に注力している取り組みについて、1～3位まで順位を付けてそれぞれ選択してください。（SA）

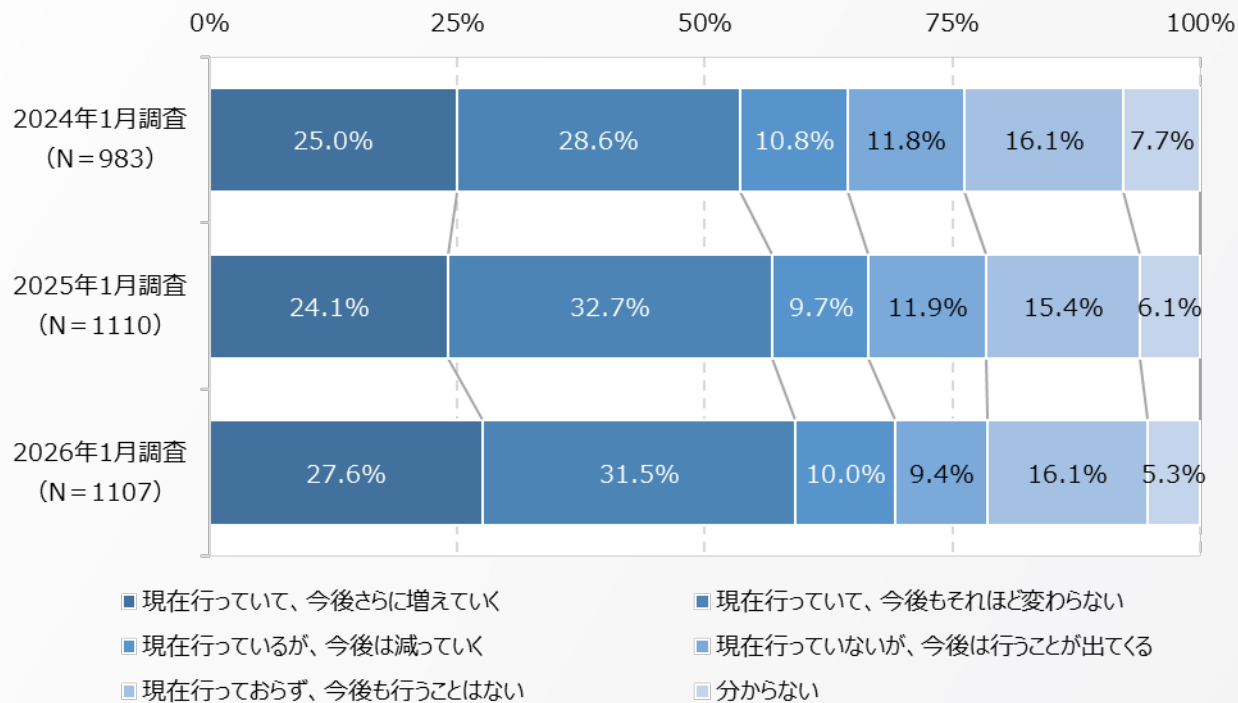
- 1位の選択結果を個人情報保有件数別に集計した結果を示す。
- いずれの個人情報保有件数においても個人情報保護管理者の任命の比率が高く、特に100万件以上で最も高くなっている。保有量の増加に伴い、責任の所在を明確化するガバナンス重視の姿勢が強まっていることがうかがえる。
- 社員教育、安全管理措置、規程類の整備は、いずれの保有件数でも一定水準の比率となっており、個人情報の量にかかわらず、基本的な運用・教育は共通施策として実施されている。
- プライバシー保護ツール導入や第三者認証の取得は大規模保有企業ほど進みやすい傾向が見られる。

	全 体	個人情報保有件数				
		1,000件未 満	1,000件～ 9,999件	1万件～10 万件未満	10万件～ 100万件未 満	100万件以 上
該当数	1107	165	360	230	170	182
個人情報保護管理者の任命	33.2	27.9	33.6	34.3	30.6	38.5
社員教育	18.5	27.3	17.2	14.8	21.8	14.8
安全管理措置	13.0	17.6	10.3	15.7	12.9	11.0
規程類の整備	11.8	9.7	13.6	11.3	12.4	10.4
プライバシー保護ツールの導入	6.5	3.6	5.8	7.8	7.1	8.2
第三者認証の取得	5.4	2.4	6.4	4.8	7.1	5.5
個人情報保護監査の実施	4.6	3.0	6.7	3.5	1.8	6.0
個人情報保護方針の公表	3.1	1.2	2.5	4.3	3.5	3.8
上記の選択肢にない	3.8	7.3	3.9	3.5	2.9	1.6

## Q6\_2 データの越境移転の状況

Q：あなたの勤務先でのデータの越境移転を行う頻度はどのようになっていくと考えていますか。（SA）

- データ越境移転を行っている企業は年々増加している傾向が見られる。特に今回調査では、今後さらに増えていく企業の比率が上昇しており、データ越境移転はさらに増加していくと見られる。



## Q6\_2 データの越境移転の状況：海外売上比率別

Q：あなたの勤務先でのデータの越境移転を行う頻度はどのようになっていくと考えていますか。（SA）

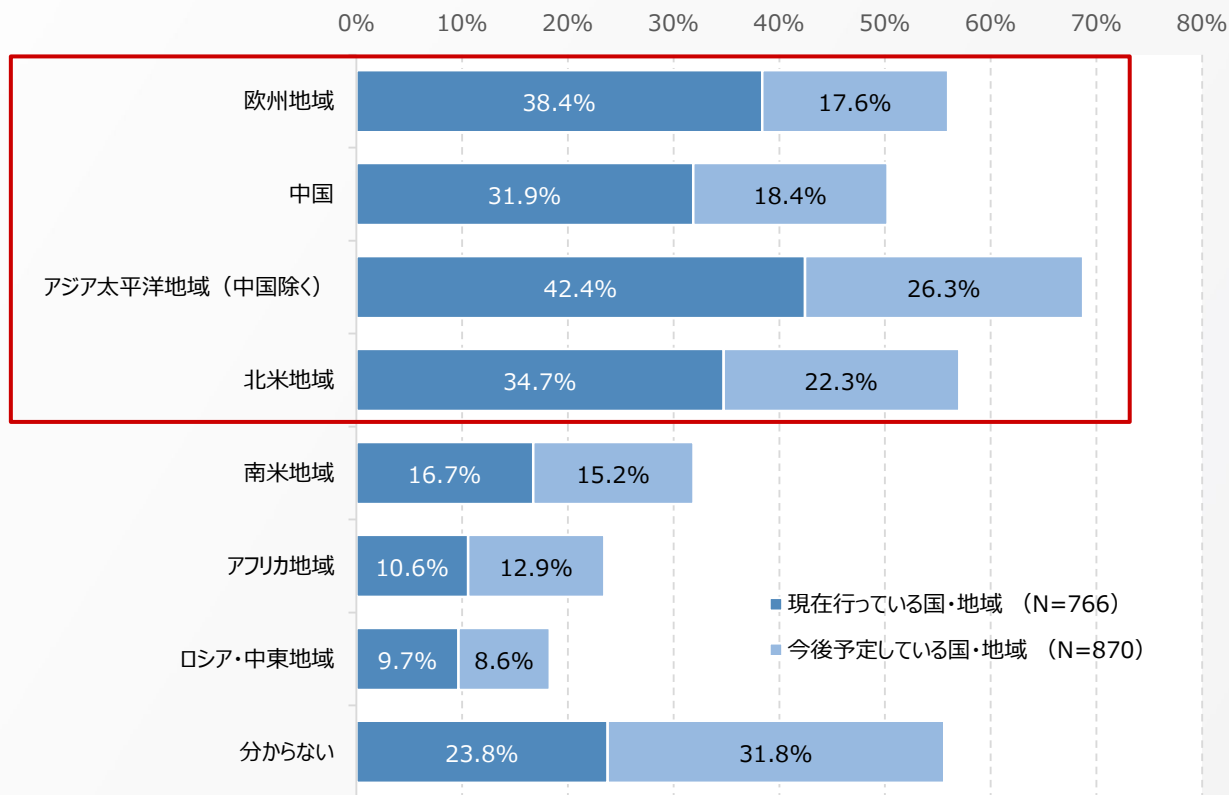
- 海外売上比率が大きくなるほどデータ越境移転の実施率は高くなる。
- 今後さらに増えていく割合が高いのは海外売上比率25%以上の企業で、約50%が増えていくと回答している。

	全 体	海外売上比率				
		0%（国内 売上げのみ）	10%未満	10%以上～ 25%未満	25%以上～ 50%未満	50%以上
該当数	1107	361	225	324	126	71
現在行っていて、今後さらに増えていく	27.6	13.9	25.3	30.6	51.6	49.3
現在行っていて、今後もそれほど変わらない	31.5	22.2	39.1	40.7	20.6	32.4
現在行っているが、今後は減っていく	10.0	5.8	11.6	14.2	12.7	2.8
現在行っていないが、今後は行うことが出てくる	9.4	11.9	10.2	8.0	4.8	8.5
現在行っておらず、今後行うことはない	16.1	36.8	9.8	4.3	5.6	2.8
分からない	5.3	9.4	4.0	2.2	4.8	4.2

## Q6\_3 データの越境移転先の国・地域

Q：あなたの勤務先で行っているデータの越境移転は、どの国や地域と行っていますか。現在行っている国・地域と今後行う予定がある国・地域についてそれぞれお答えください。（MA）

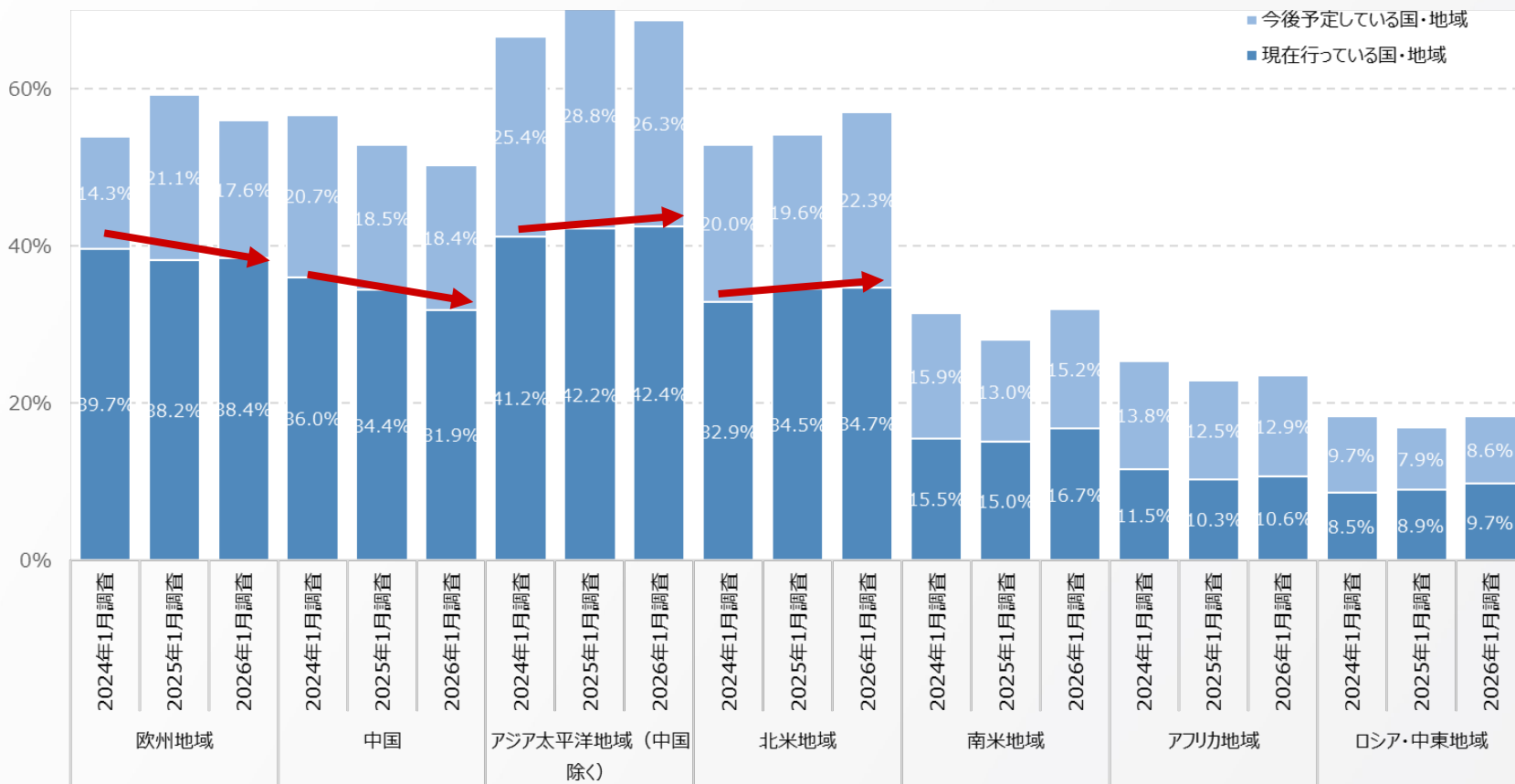
- アジア太平洋地域（中国除く）と中国、北米、欧州が主要な越境移転先となっており、現在実施・今後予定のいずれにおいても比率が高い。特に今後予定されている地域として、アジア太平洋地域（中国除く）と北米の比率が高くなっている。
- 一方で、南米、アフリカ、ロシア・中東は比率が相対的に低く、越境移転先は限定的である。



# Q6\_3 データの越境移転先の国・地域：過去調査との比較

Q：あなたの勤務先で行っているデータの越境移転は、どの国や地域と行っていますか。現在行っている国・地域と今後行う予定がある国・地域についてそれぞれお答えください。（MA）

- ・ 欧州および中国は、データ越境移転先としての比率が年々低下傾向にある。規制対応の複雑さや地政学リスクなどを背景に、越境移転先として慎重な判断が進んでいることがうかがえる。
- ・ 一方、アジア太平洋地域（中国除く）と北米は、比率が年々上昇している。ビジネス進出の拡大に伴う取引先の増加やクラウドの利用拡大など、データ越境移転を行う機会が増加していると考えられる。



## Q6\_3 データの越境移転先の国・地域：海外売上比率別

Q：あなたの勤務先で行っているデータの越境移転は、どの国や地域と移転を行っていますか。現在行っている国・地域と今後行う予定がある国・地域についてそれぞれお答えください。（MA）

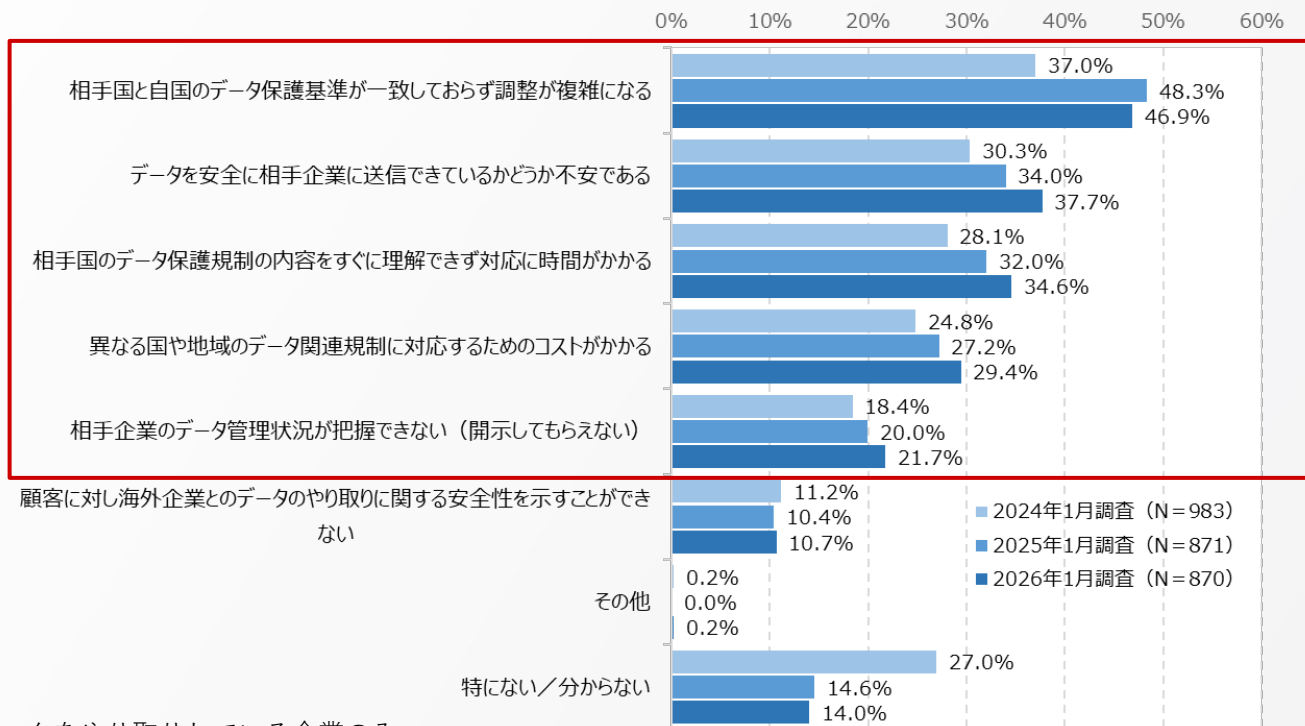
- 海外売上比率50%以上では欧州地域の比率が最も高い。また、中国、アジア太平洋地域、北米地域も6割を超えている。
- 海外売上比率25%以上～50%未満でも欧州地域とアジア太平洋地域は6割を超えている。
- 海外売上比率10%未満になると、アジア太平洋地域の比率が他の国・地域と比較して高くなっている。

	全 体	海外売上比率				
		0%（国内 売上げのみ）	10%未満	10%以上～ 25%未満	25%以上～ 50%未満	50%以上
該当数	766	151	171	277	107	60
欧州地域	38.4	6.0	28.1	45.1	66.4	68.3
中国	31.9	7.9	28.1	37.9	39.3	61.7
アジア太平洋地域（中国除く）	42.4	15.2	42.1	44.8	62.6	65.0
北米地域	34.7	5.3	28.7	40.4	54.2	65.0
南米地域	16.7	2.0	8.2	19.5	29.9	41.7
アフリカ地域	10.6	1.3	6.4	9.0	18.7	38.3
ロシア・中東地域	9.7	1.3	7.0	9.0	19.6	23.3
分からない／予定がない	23.8	74.8	15.8	12.3	5.6	3.3

## Q6\_4 海外企業とのデータ送受信における課題

Q：あなたの勤務先において、海外企業との取引の際にデータをやり取りする際に困っている点や課題はありますか。当てはまるものをすべてお答えください。今後やり取りする予定がある場合には、懸念される点をお答えください。（MA）

- データ保護基準が一致しておらず調整が複雑になることや相手国の規制内容を理解・対応するのに時間がかかるといった制度・法規制の差異に起因する課題が上位に挙がっていることに変化はない。また、対応コストの課題も一定数挙がっている。
- 相手企業に安全にデータを送信できているか不安になるといった技術的な課題も上位に挙がり、比率が高くなる傾向が見られる。

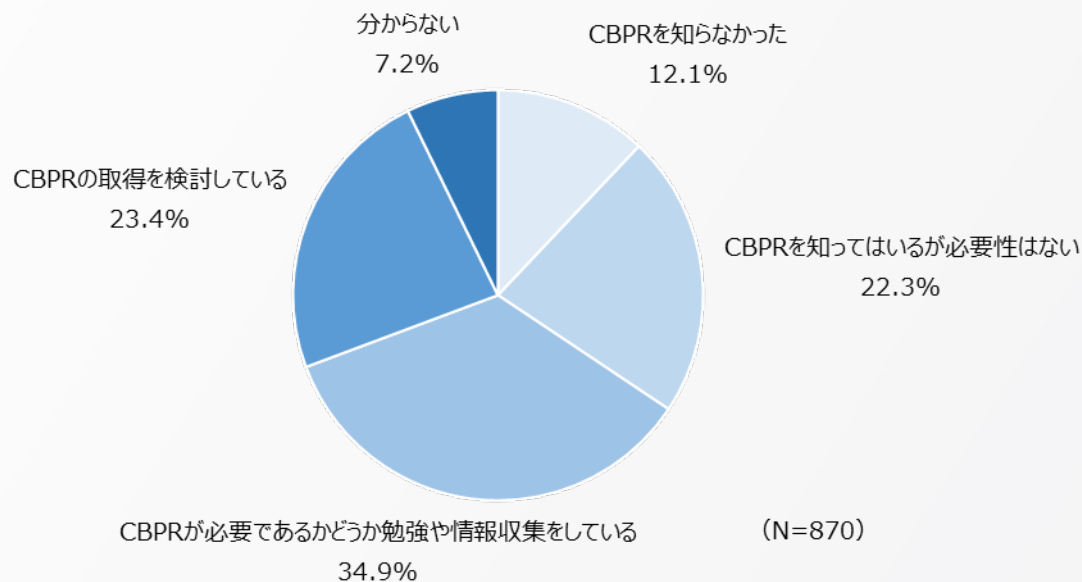


※現在データをやり取りしている企業のみ

## Q6\_5 CBPRの取得検討状況

Q：あなたの勤務先では、CBPRの取得を検討していますか。（SA）

- 「取得を検討している」は23.4%、「必要性であるかどうか情報収集している」を合わせると50%以上となっており、CBPRの関心が高まりつつあることがうかがえる



## Q6\_5 CBPRの取得検討状況：企業属性別

Q：あなたの勤務先では、CBPR認証の取得を検討していますか。（SA）

- 業種別：情報通信と金融／保険において、取得を検討している企業の割合が高くなっている。特に情報通信は勉強・情報収集を合わせると65%以上でCBPRに関する議論が行われている。
- 従業員規模別：規模が大きい企業ほど取得を検討している企業の割合が高くなる傾向が見られる。特に5,000人以上は勉強・情報収集を合わせると70%でCBPRに関する議論が行われている。

	全体	業種							従業員規模			
		製造	建設・不動産	卸売・小売	金融・保険	情報通信	サービス	公共・その他	5,000人以上	1,000～4,999人	300～999人	50～299人
該当数	870	258	90	57	75	154	188	48	237	222	196	215
CBPRを知らなかった	12.1	12.0	15.6	15.8	2.7	12.3	11.2	18.8	7.6	12.6	10.2	18.1
CBPRを知ってはいるが必要性はない	22.3	21.3	25.6	17.5	32.0	16.2	22.3	31.3	16.9	22.5	26.0	24.7
CBPRが必要であるかどうか勉強や情報収集をしている	34.9	37.6	30.0	35.1	30.7	35.1	38.3	22.9	35.9	32.9	33.7	37.2
CBPRの取得を検討している	23.4	23.3	24.4	24.6	29.3	31.2	17.6	10.4	34.2	27.5	21.9	8.8
分からない	7.2	5.8	4.4	7.0	5.3	5.2	10.6	16.7	5.5	4.5	8.2	11.2

## Q6\_5 CBPRの取得検討状況：データ越境移転状況別

Q：あなたの勤務先では、CBPRの取得を検討していますか。（SA）

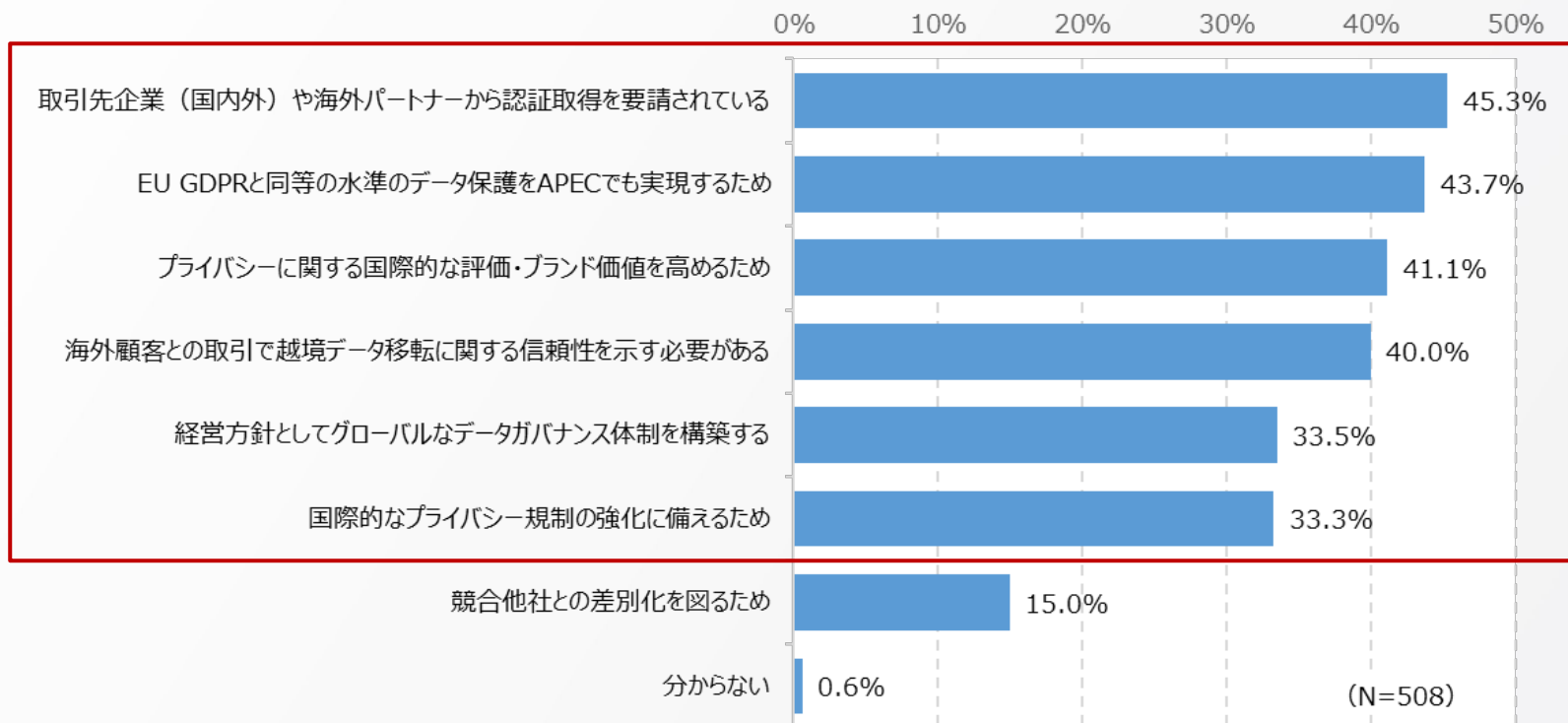
- データ越境移転が今後さらに増えていく企業は、CBPRを検討している割合が高く40%を超えている。越境データの拡大とCBPRへの本格対応が強く連動している。
- 今後も変わらないや減っていくとしている企業、もしくは現在行っていない企業でも、CBPRを知らないとする企業の割合は低く、認知度はある。その中では、必要であるかどうかの情報収集を行っている企業が多い。

	全 体	データ越境移転			
		現在行っていて、 今後さらに増えてい く	現在行っていて、 今後もそれほど変 わらない	現在行っているが、 今後は減っていく	現在行っていない が、今後は行うこと が出てくる
該当数	870	306	349	111	104
CBPRを知らなかった	12.1	13.1	12.0	5.4	16.3
CBPRを知ってはいるが必要性はない	22.3	10.8	32.1	26.1	19.2
CBPRが必要であるかどうか勉強や情報収集をしている	34.9	28.4	33.5	47.7	45.2
CBPRの取得を検討している	23.4	43.5	13.2	12.6	10.6
分からない	7.2	4.2	9.2	8.1	8.7

## Q6\_6 CBPR認証を取得検討する動機

Q：CBPR認証の取得を検討している、もしくは情報収集を行っている背景や動機は何ですか。当てはまるものをすべてお答えください。（MA）

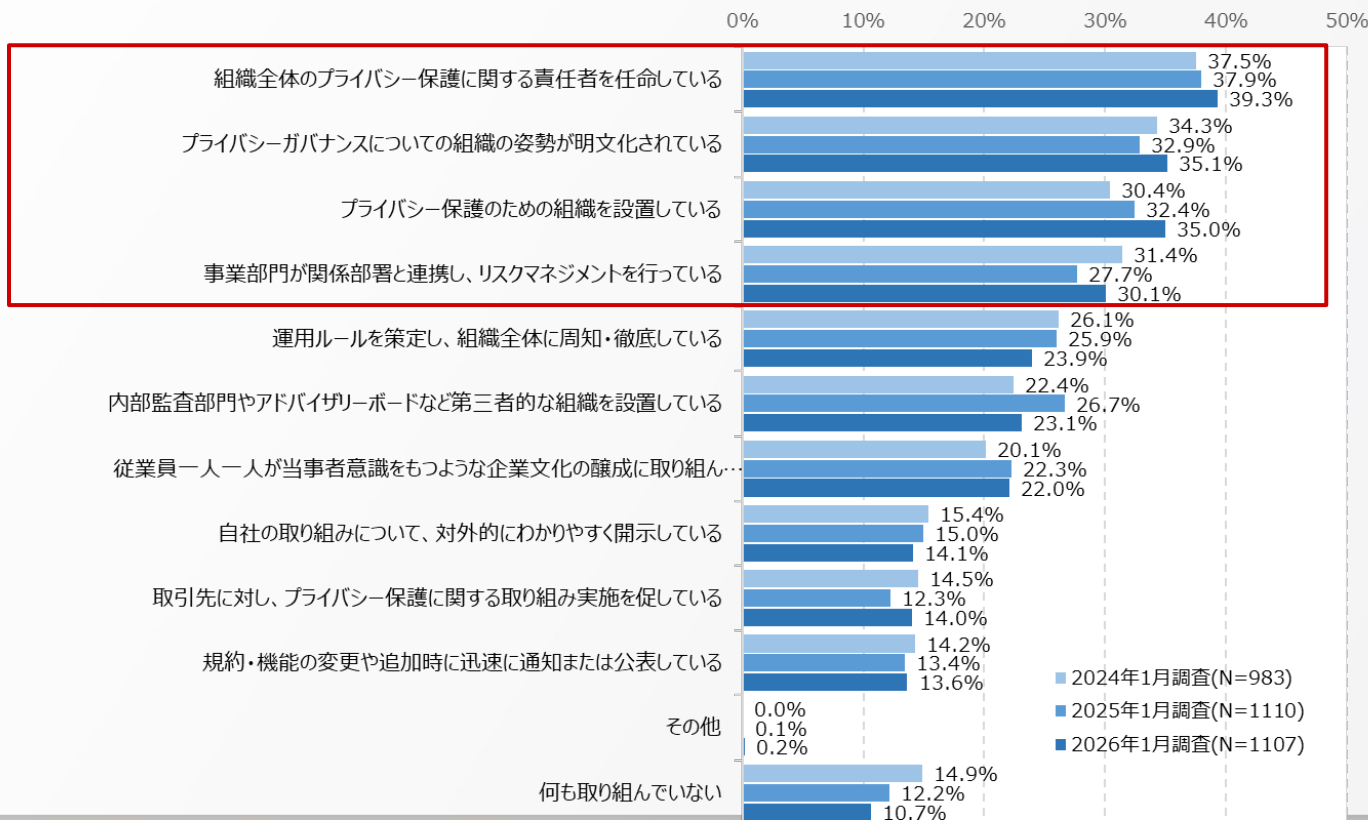
- 取引先や海外パートナーからの要請、EU GDPRと同等水準のデータ保護実現、海外顧客との取引における信頼性確保といった項目が上位にあり、CBPRは越境ビジネスを継続・拡大するために検討されていることが分かる。
- また、国際的な評価やブランド価値の向上、グローバルなデータガバナンス体制の構築、プライバシー規制強化への備えといった回答も3割以上あり、中長期的な経営・ガバナンス戦略の一環として位置付ける企業もある。



# Q6\_7 プライバシーガバナンスに関する取り組み

Q：あなたの勤務先では、プライバシーガバナンスに関する取り組みを行っていますか。当てはまるものをすべて選択してください。（MA）

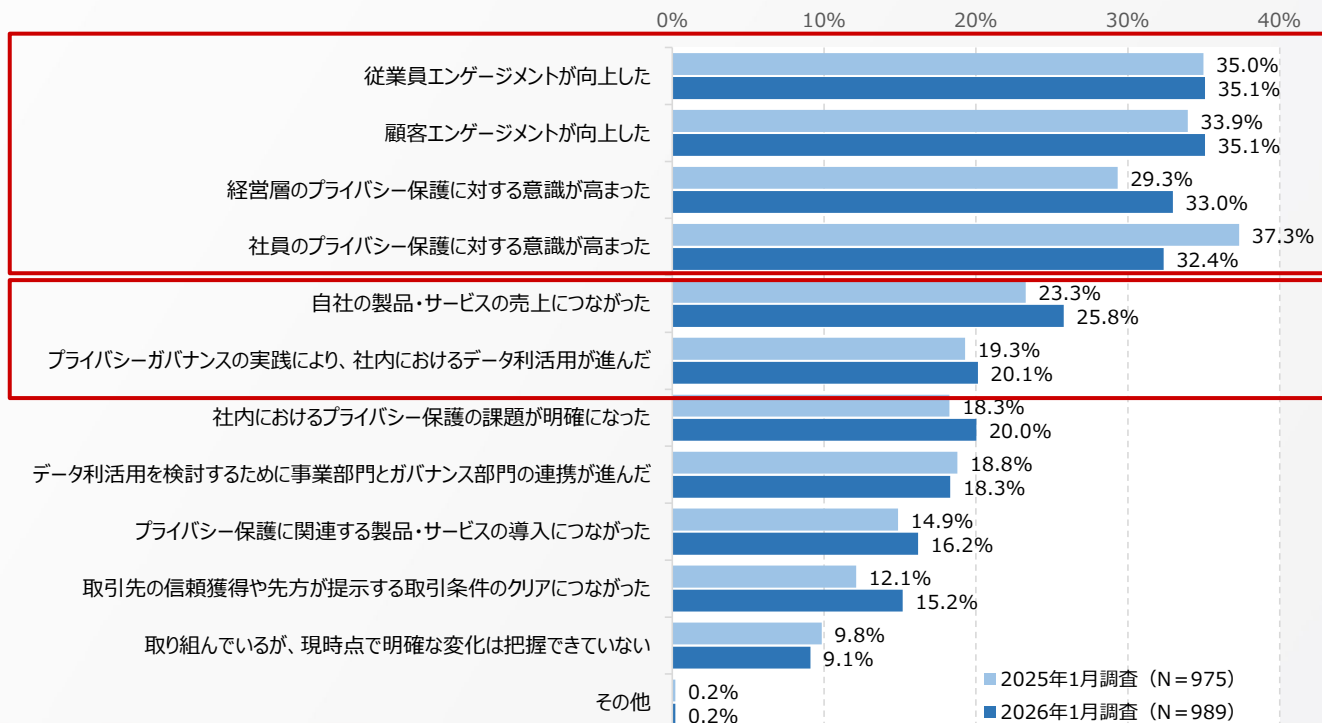
- 「組織全体のプライバシー保護に関する責任者を任命している」が前回調査に続き最も多く、「プライバシーガバナンスについての組織の姿勢が明文化されている」も前回調査と同様に2番目に続いている。責任者の任命と社内への明文化が最も取り組まれている状況に変わりはない。
- 3番目の「プライバシー保護のための組織を設置している」が年々上昇している傾向が顕著に見られる。また4番目の「事業部門が関係部署と連携し、リスクマネジメントを行っている」も前回調査から上昇している。組織づくりを行い、各部門が連携して取り組む体制を整備している企業が増えていると見られる。



# Q6\_8 プライバシーガバナンスに取り組んだことによる変化

Q：あなたの勤務先では、プライバシーガバナンスに取り組んだ（取り組んでいる）結果として、どのような変化がありましたか。当てはまるものをすべてお答えください。（MA）

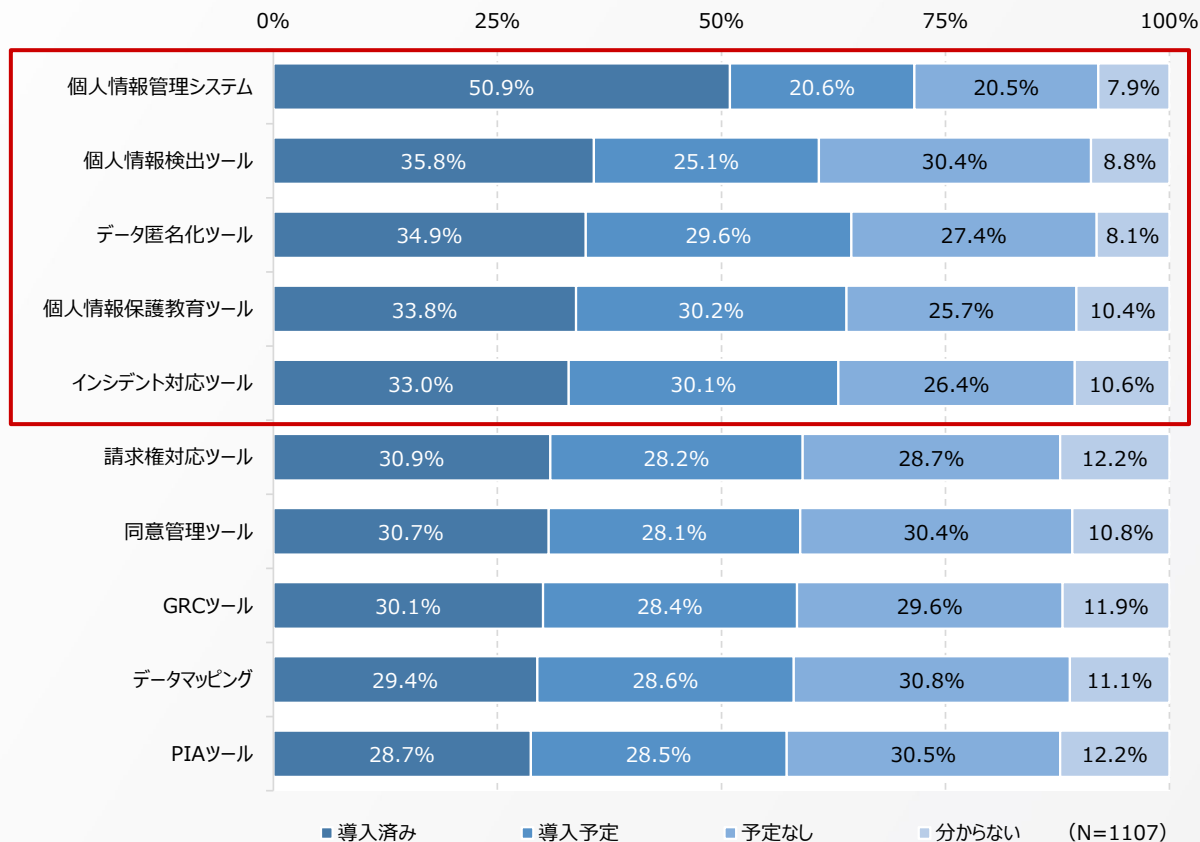
- 従業員・顧客エンゲージメントの向上が上位に挙がっており、プライバシーガバナンスはリスク対策にとどまらず、社内外の信頼関係に寄与する取り組みとして定着していることがうかがえる。
- 経営層の意識向上の回答率が前回調査から上昇している。一方、従業員の意識向上は低下している。これは、既に前回調査で社員の意識が既に向上していた企業は、今回調査では選択しなかったとも見ることができる。また、社員の意識向上が、今回調査での経営層の意識向上を促したと考えることもできる。総じて社内全体での意識は確実に向上している。
- 自社製品・サービスの売上につながった、データ利活用が進んだといったビジネスやデータ活用面での効果が前回調査よりやや増加しており、守りの効果だけではなく、攻めの効果も徐々に始めていることがうかがえる。



# Q6\_9 プライバシー保護ツール・システムの導入状況

Q：あなたの勤務先ではプライバシー保護に関するツールやシステムを導入していますか。それぞれのツール・システムについて当てはまるものをお答えください。（SA）

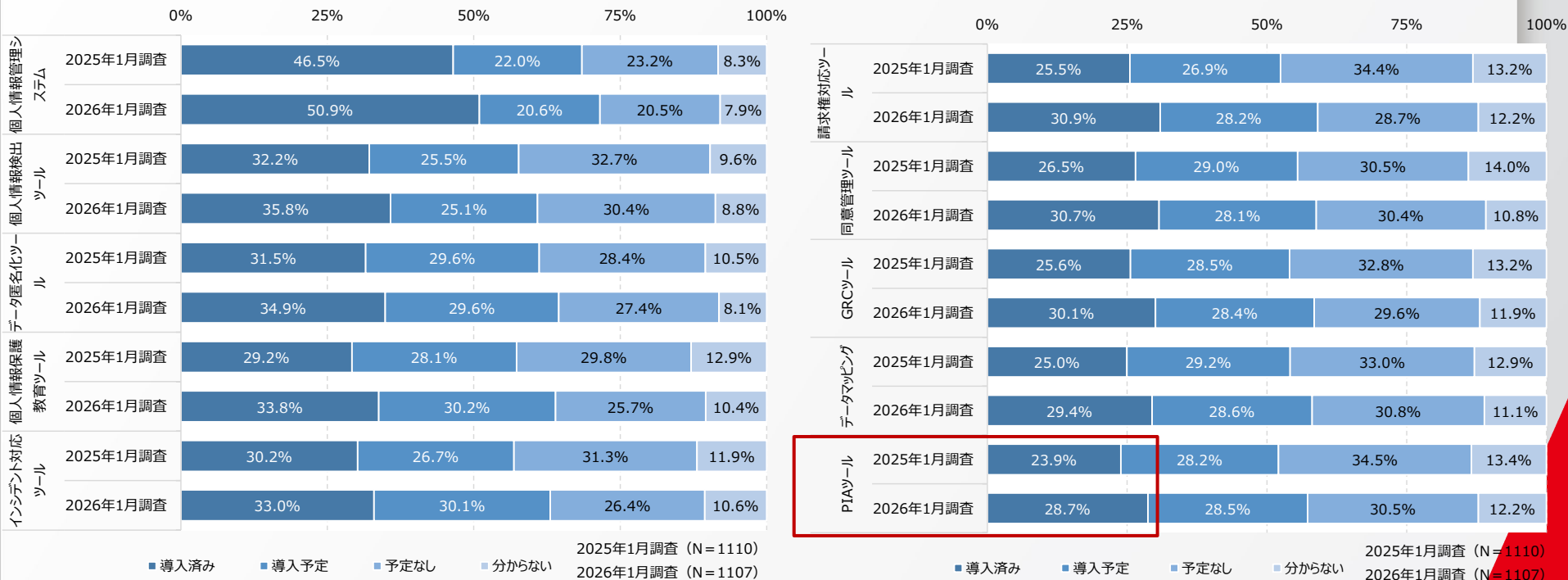
- 「個人情報管理システム」が最も導入率が高く、他のツールとの差が大きい。
- 次に「個人情報検出ツール」「データ匿名化ツール」「個人情報保護教育ツール」「インシデント対応ツール」と続いている。



# Q6\_9 プライバシー保護ツール・システムの導入状況：前回調査との比較

Q：あなたの勤務先ではプライバシー保護に関するツールやシステムを導入していますか。それぞれのツール・システムについて当てはまるものをお答えください。（SA）

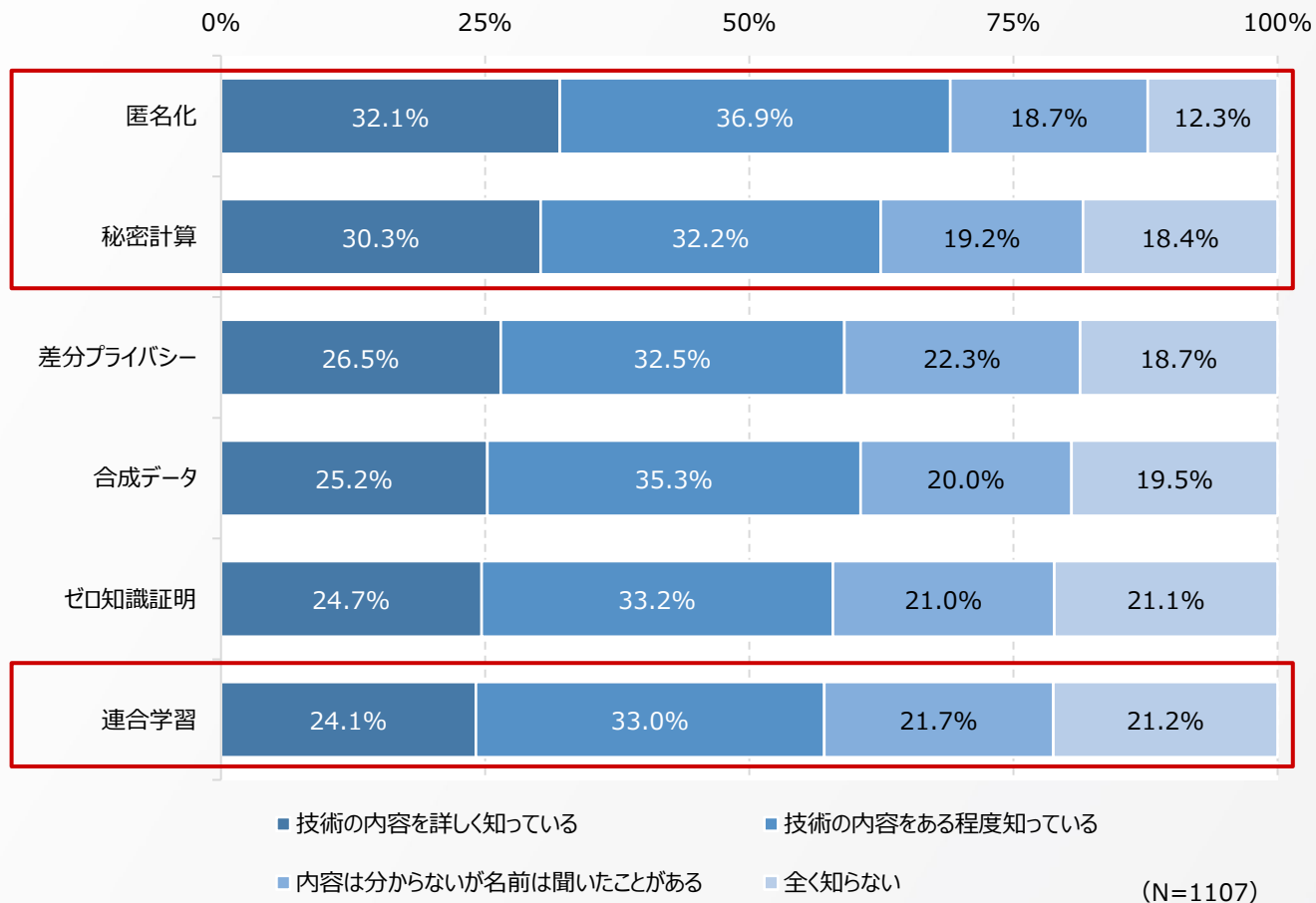
- すべてのツール・システムにおいて、前回調査から導入率が上昇している。技術的なプライバシー保護対策の必要性や重要性が浸透し、具体的な対策に動いている企業が増えていると見られる。
- 請求権対応ツール、同意管理ツール、GRCツール、データマッピングツール、PIAツールの上昇率が高くなっている。属人的管理から脱し、専用ツールの導入が進み始めている。



# Q6\_10 プライバシー保護技術（PETs）の認知度

Q：プライバシー保護を強化する技術であるプライバシーテック（PETs）を知っていますか。それぞれの技術について当てはまるものをお答えください。（SA）

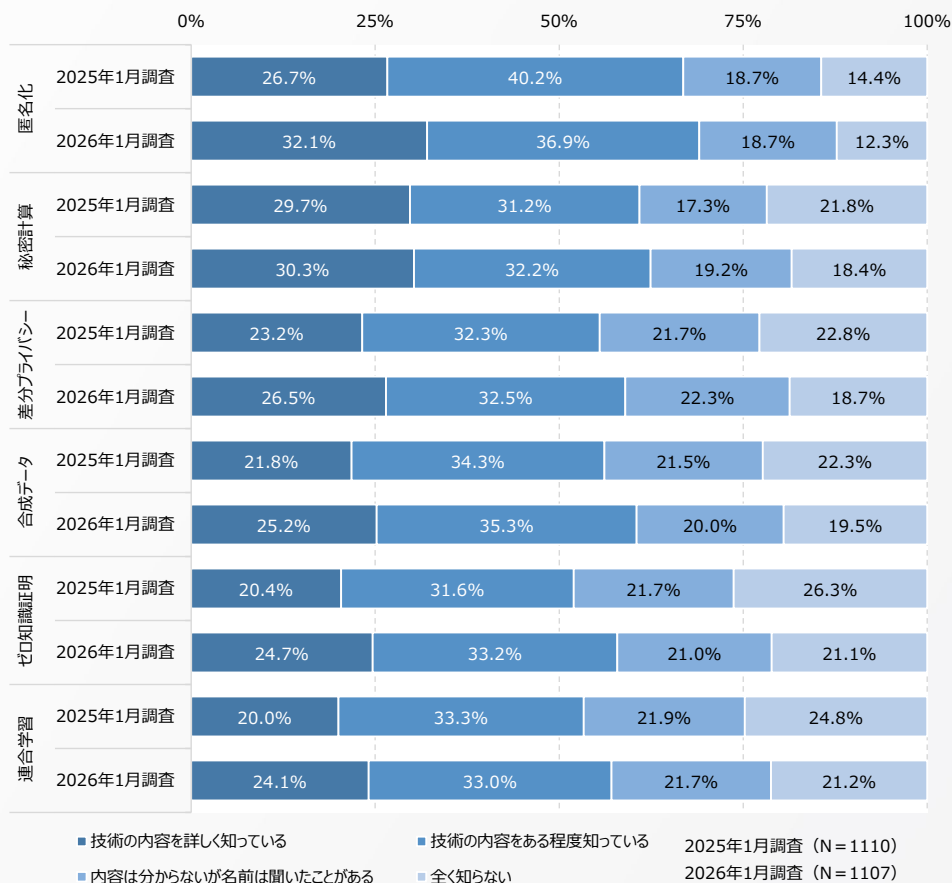
- 「匿名化」と「秘密計算」は、詳しく知っているとある程度知っているとを合わせると60%以上が認知している。
- 最も認知度が低いのは「連合学習」ではあるが、各技術の認知度に大きな差はない。



# Q6\_10 プライバシー保護技術（PETs）の認知度：前回調査との比較

Q：プライバシー保護を強化する技術であるプライバシーテック（PETs）を知っていますか。それぞれの技術について当てはまるものをお答えください。（SA）

- いずれの技術も前回調査から認知度が上昇している。生成AIや高度なデータ利活用が進む中で、プライバシーデータを「使わない／制限する」ではなく「保護しながら使う」アプローチが求められ、セキュリティ・規制対応とデータ活用を両立できるPETsの認知度が高まっていると見られる。



# 7

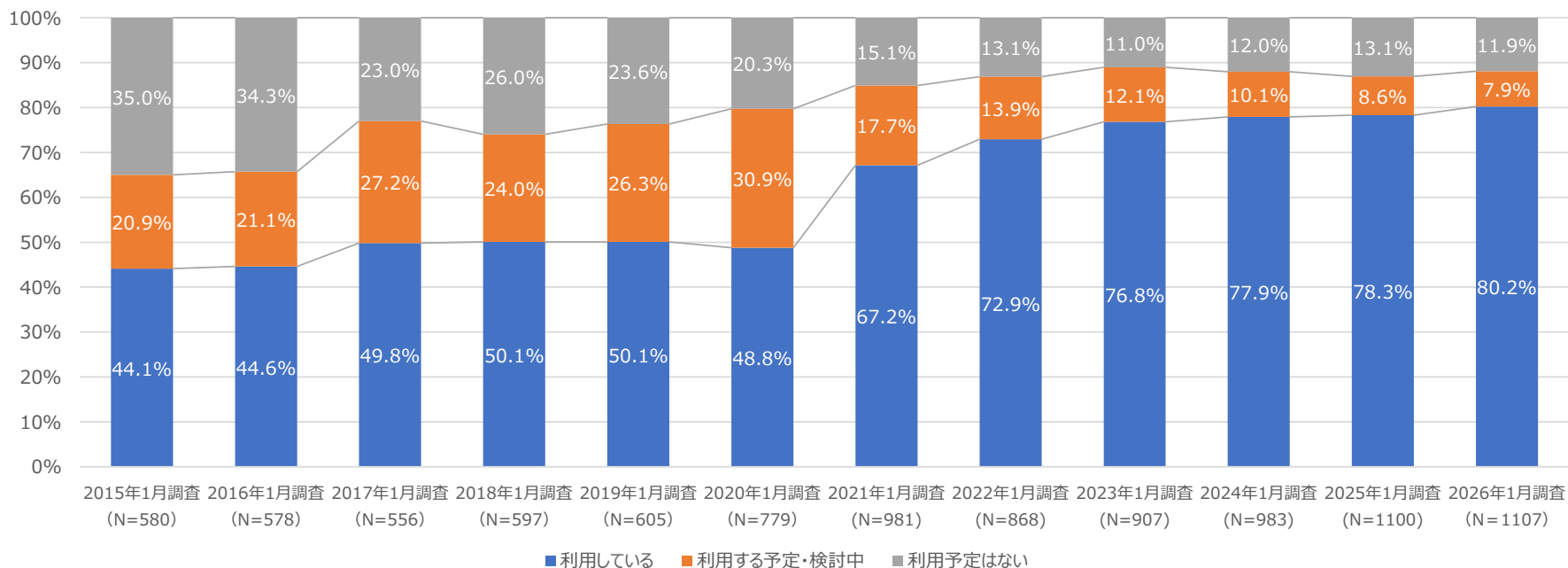
## 電子契約の実施状況

- Q7\_1 電子契約の実施状況
- Q7\_2 電子契約サービスの選択理由
- Q7\_3 電子契約の導入効果
- Q7\_4 電子契約の導入後の課題

# Q7\_1 電子契約の利用状況：利用率の推移

Q:あなたの勤務先で利用している電子契約はどのような方法ですか。以下から当てはまるものをお答えください。(SA)

- JIPDECでは2015年より企業における電子契約の普及状況を調査している。
- 2021年から電子契約の利用率が大きく上昇している。2017年から利用率が横ばいで推移していたが、2020年から新型コロナによる緊急事態宣言で入社制限が出るなど紙や対面での契約に支障が出たため、2020年中に電子契約の導入を進めた企業が急増したとみられる。
- 2023年からは利用率の上昇が落ち着きを見せているが、着実に上昇し続けており、2026年では初めて80%を超えた。

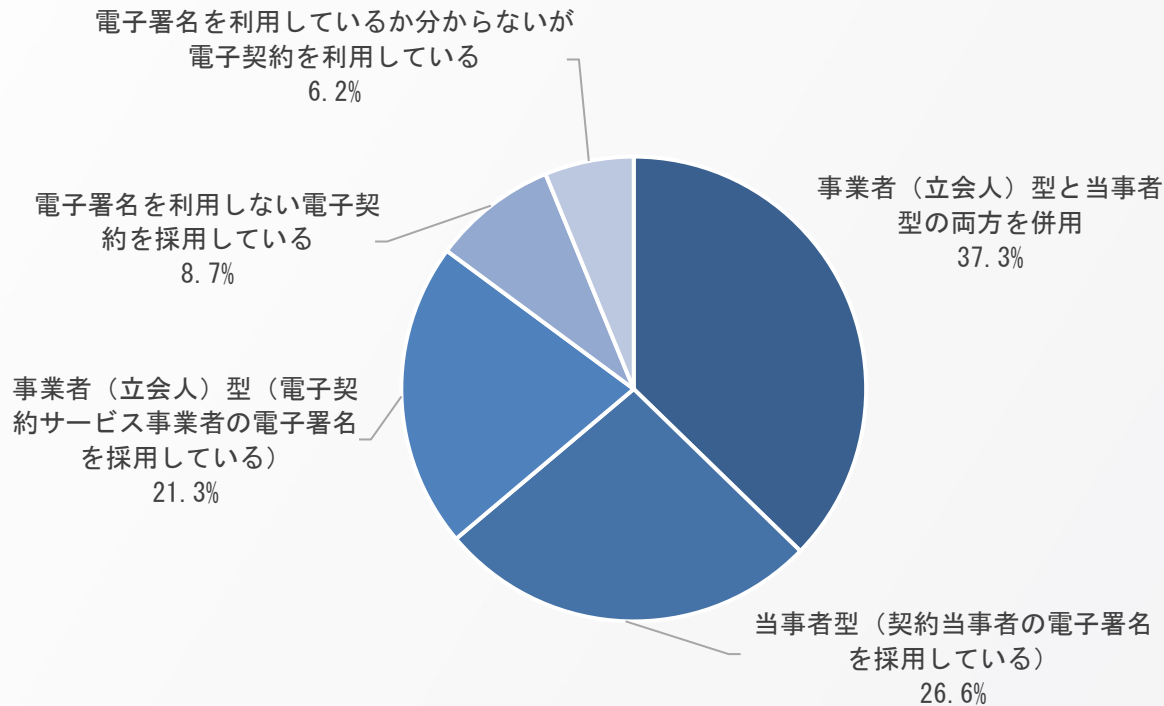


※2020年以前は質問が異なり、「わからない」の回答を除いている

# Q7\_1 電子契約の利用状況：利用方式

Q：あなたの勤務先で利用している電子契約はどのような方法ですか。以下から当てはまるものをお答えください。  
(SA)

- 電子契約の利用企業では、事業者（立会人）型と当事者型を併用している企業の割合（37.3%）が最も大きい。
- 電子契約の利用企業のうち、85.2%が契約書類の信頼性を確保するため電子署名あり電子契約サービスを採用している。

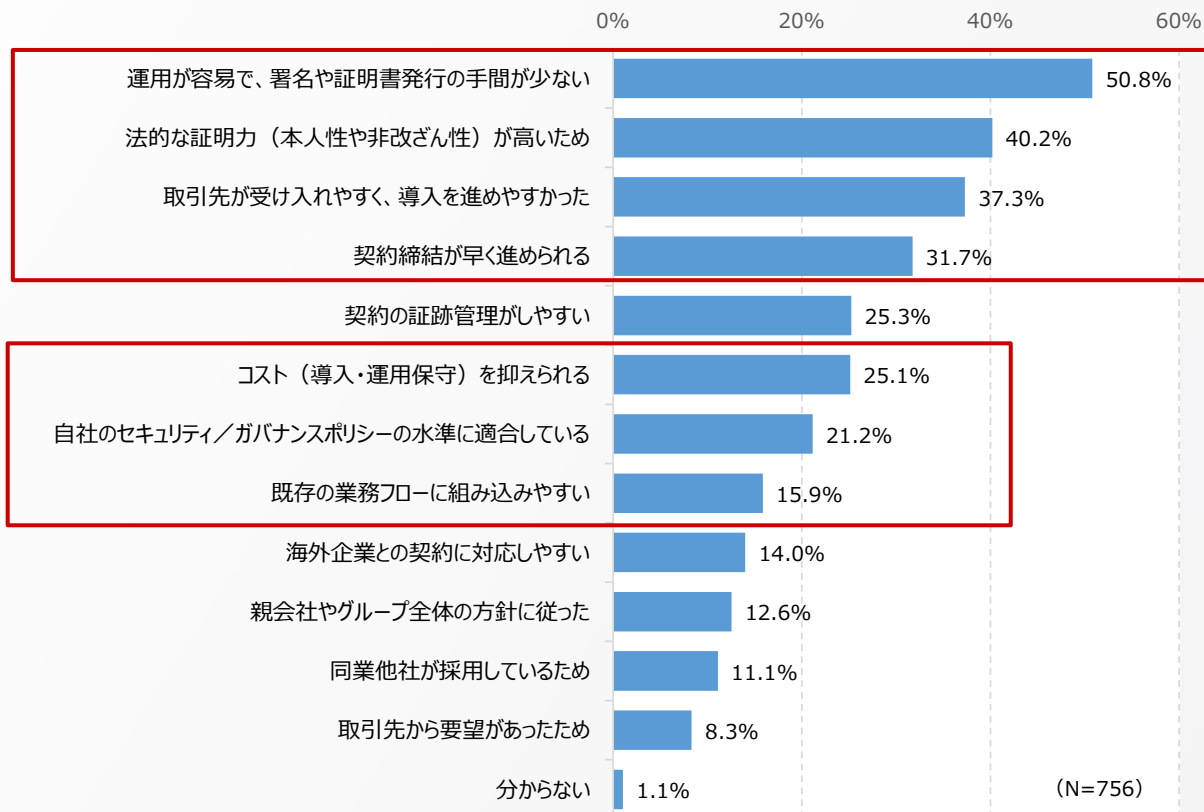


(N=888)

## Q7\_2 電子契約方式の選択理由

Q：Q7\_1で回答した電子契約方式を選んだ理由は何ですか。当てはまるものをすべてお答えください。導入時のご担当ではない場合、想定でお答えください。（MA）

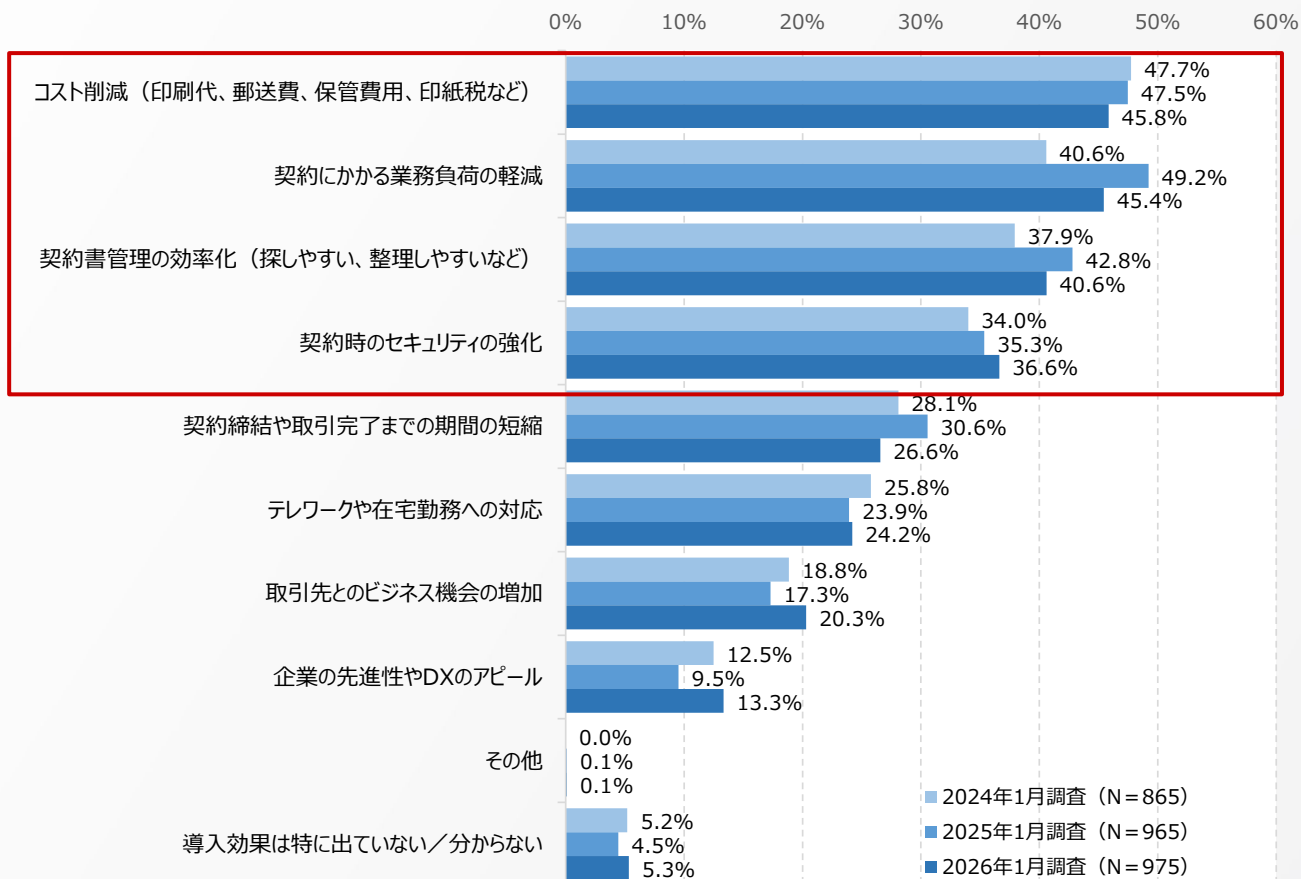
- 運用の容易性、法的な証明力の高さ、取引先が受け入れやすい、契約締結が早く進められることが上位に挙がっている。電子契約方式の選定においては、法的な信頼性と契約業務の回しやすさを両立できる点が最も重視されていることが分かる。
- 一方で、コストや既存業務フローへの組み込みやすさといった項目は中位以下にとどまっており、サービスの戦略的な差別化よりも、まずは確実に・円滑に契約を成立させることが優先されている傾向がうかがえる。



## Q7\_3 電子契約の導入効果

Q：あなたの勤務先が電子契約を利用することで、どのような効果が得られましたか。当てはまるものをすべてお答えください。これから電子契約を利用する場合は、期待する効果についてお答えください。（MA）

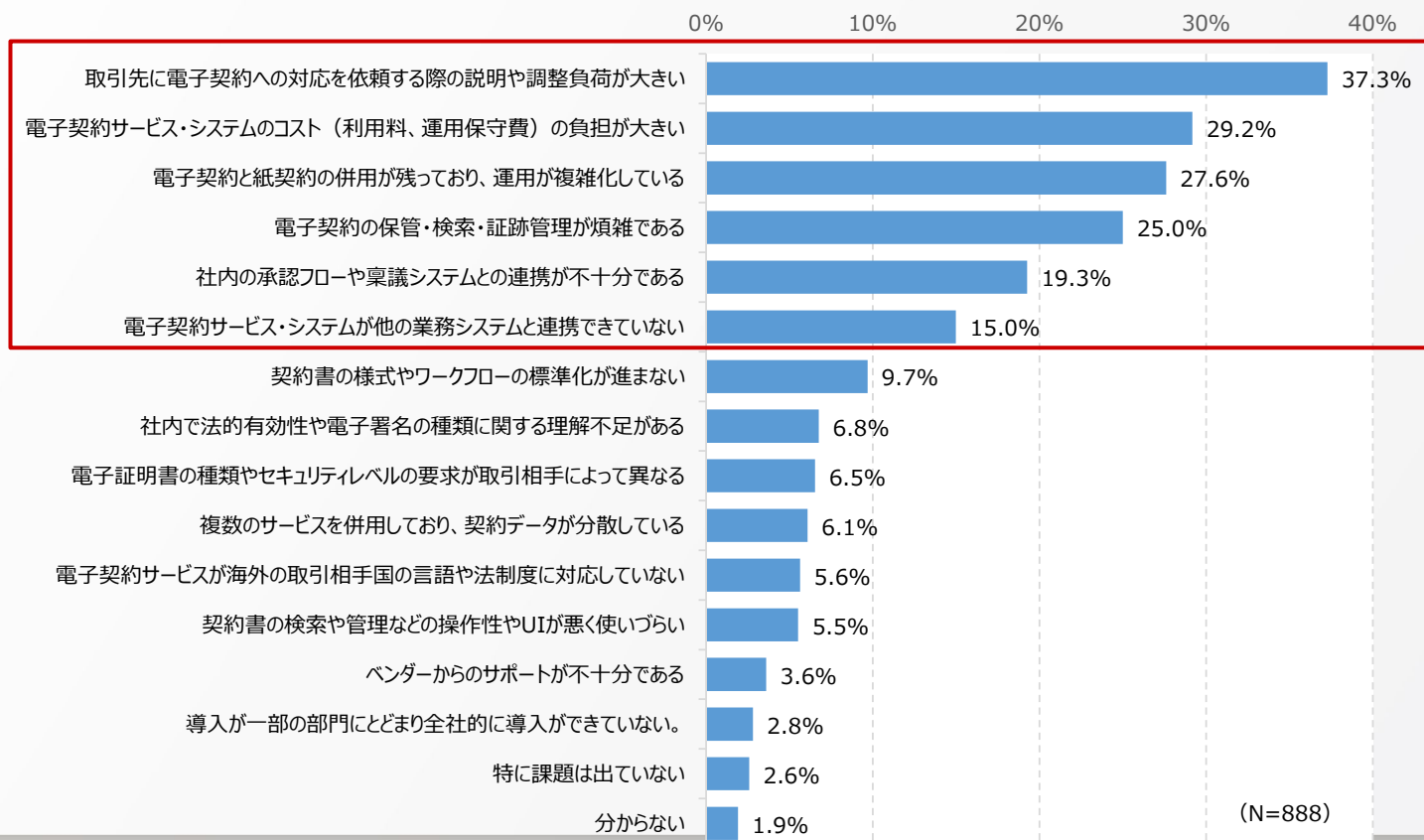
- コスト削減、契約業務負荷の軽減、契約書管理の効率化が一貫して上位に挙がっており、電子契約は業務効率化・省力化の即効性が高い施策として定着している。ただ、回答率は前回調査からやや低下している。
- 契約時のセキュリティ強化が、年々上昇している。電子契約が単なる効率化手段から、契約の真正性・改ざん防止・証跡確保を重視するセキュリティ対策の手段としても評価されるようになってきている。



## Q7\_4 電子契約導入後の課題

Q：電子契約の導入後、どのような点で課題を感じますか。特に深刻な課題を3つまでお答えください。（MA）

- 最も深刻な課題は取引先への説明・調整にかかる負荷であり、電子契約そのものよりも、相手先の理解を得ることに苦労している状況がうかがえる。電子契約で自社内の効率化が進む一方、社外との調整が課題になっている。
- 次いで、コスト負担や紙契約との併存による運用の複雑化、保管・検索・証跡管理の煩雑さ、社内システムとの連携が不十分であることが挙がっており、電子契約は導入したものの、業務全体の最適化に至っていないことが顕在化している。



The logo for JIPDEC features the word "JIPDEC" in a bold, black, sans-serif font. A solid red circle is positioned above the letter "I", serving as a distinctive graphic element.

**JIPDEC**