JIPDECセミナー
「生成AIの活用成果の実態とセキュリティ課題への取り組み状況
～「企業IT利活用動向調査2025」結果報告」　講演資料

2025年3月14日（金）

JIPDECセミナー

生成AIの活用成果の実態と セキュリティ課題への取り組み状況

～「企業IT利活用動向調査2025」結果報告～

2025年3月14日

株式会社アイ・ティ・アール

iTR

「企業IT利活用動向調査2025」調査概要

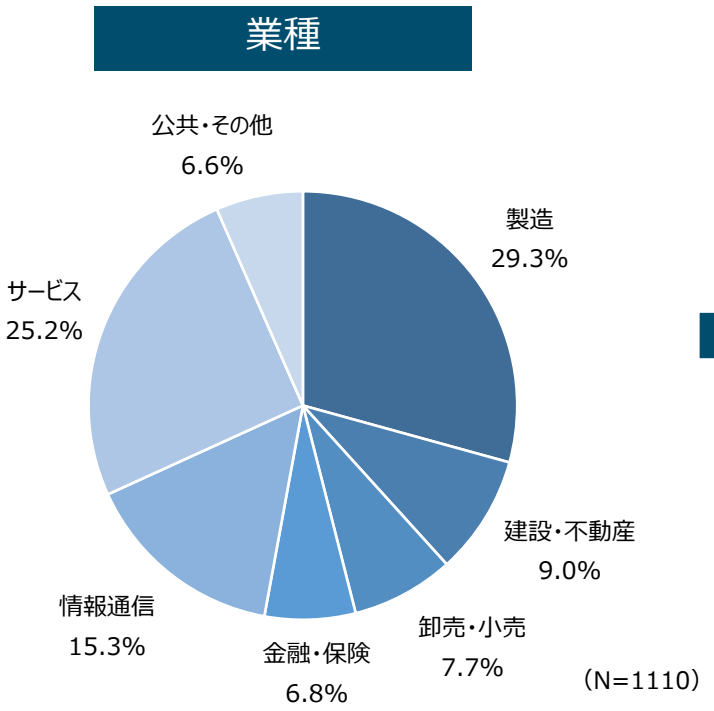
国内企業の情報セキュリティに重点を置いたIT動向調査。事業継続のための経営戦略、セキュリティ技術の導入状況、セキュリティ関連認証制度の取得状況、プライバシー保護対応などセキュリティの実態を調査するとともに、DXや生成AI、テレワーク、電子契約など最新ITの導入状況も調査している。

■調査期間	：	2025年1月17日～1月24日
■調査主体	：	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	：	1,110件（1社1回答）

調査結果における留意事項

- 本調査について、2022年～2023年実施時は、従業員2人以上の企業から調査対象としていた。2024年調査から従業員50人以上を対象としたため、同年調査との結果を比較する際には、従業員50名以上に統一して比較している。
- グラフに表記されている数値を合計しても100%にならない場合や、グラフの数値を足し合わせて数値が文章中の数値と合わない場合がある。グラフは小数点以下1位までを四捨五入した数値を示しているが、集計上はそれより下位の小数点まで計算しているため差異が生じている。

回答者が所属する企業のプロフィール①

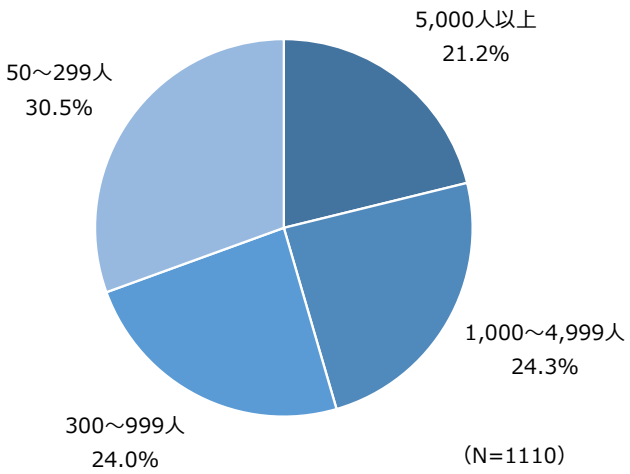


業種詳細

大分類	詳細	回答数	構成比
製造	食品・飲料	36	3.2%
	日用品・生活雑貨	22	2.0%
	繊維	16	1.4%
	パルプ・紙・印刷	14	1.3%
	化学工業	21	1.9%
	石油製品	8	0.7%
	鉄鋼・金属	22	2.0%
	プラスチック・ゴム	9	0.8%
	機械	29	2.6%
	電気機器	42	3.8%
	情報通信機器	15	1.4%
	電子部品・電子回路	17	1.5%
	精密機器	15	1.4%
	自動車・輸送機器	39	3.5%
	医薬品	10	0.9%
	その他の製造業	10	0.9%
建設・不動産	建設	53	4.8%
	不動産	44	4.0%
	住宅	3	0.3%
卸売・小売	卸売	22	2.0%
	小売	31	2.8%
	商社	33	3.0%
金融・保険	銀行	45	4.1%
	証券	9	0.8%
	生命保険	6	0.5%
	損害保険	7	0.6%
	その他金融	9	0.8%
情報通信	通信	28	2.5%
	ITベンダー／システムインテグレーター	113	10.2%
	インターネット・サービス	17	1.5%
	情報システム子会社	12	1.1%
サービス	電力・ガス・水道	29	2.6%
	運輸	39	3.5%
	倉庫	10	0.9%
	宿泊	10	0.9%
	飲食	15	1.4%
	娯楽・レジャー	12	1.1%
	メディア・出版・放送・広告	3	0.3%
	生活関連サービス（旅行業など）	9	0.8%
	医療	39	3.5%
	福祉・介護	50	4.5%
	教育（学校以外）	16	1.4%
	人材派遣・業務委託	17	1.5%
	その他サービス	31	2.8%
公共・その他	学校	15	1.4%
	官公庁	11	1.0%
	地方自治体	30	2.7%
	その他公共機関	3	0.3%
	農業・水産・鉱業	3	0.3%
	その他の業種	11	1.0%
合計		1,110	100.0%

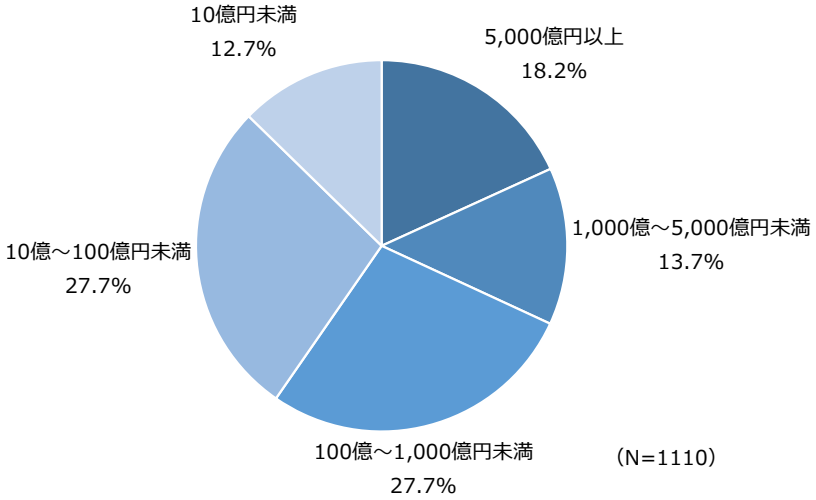
回答者が所属する企業のプロフィール②

従業員規模



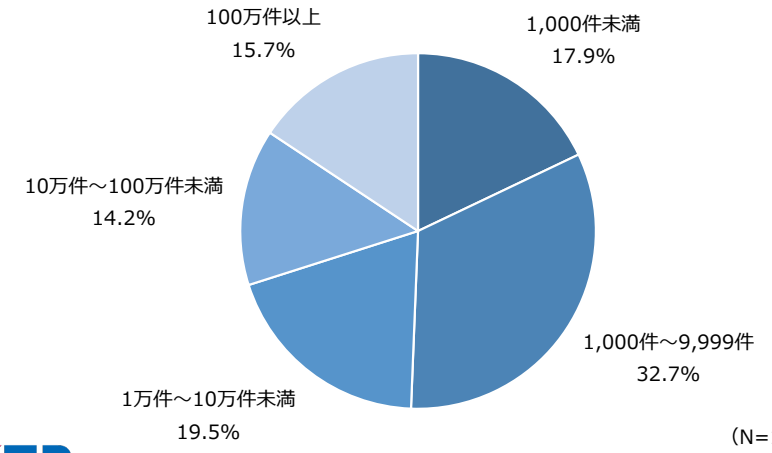
（N=1110）

年間売上規模



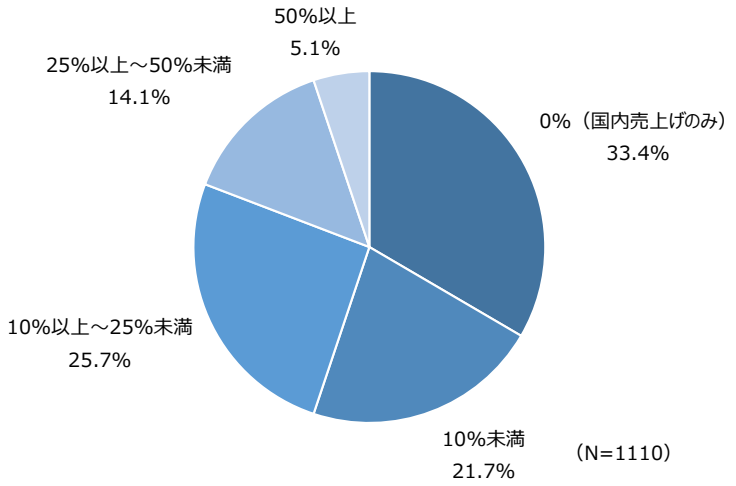
（N=1110）

個人情報保有件数



（N=1110）

海外売上比率



（N=1110）

報告する調査項目

1. 経営課題とDX実践状況

2. 電子契約の利用状況

3. 生成AIの活用状況と課題

4. ランサムウェアとセキュリティ対策の実態

5. プライバシー保護に対する取り組み状況

6. 第三者認定／認証制度の取得状況

報告する調査項目

1. 経営課題とDX実践状況

2. 電子契約の利用状況

3. 生成AIの活用状況と課題

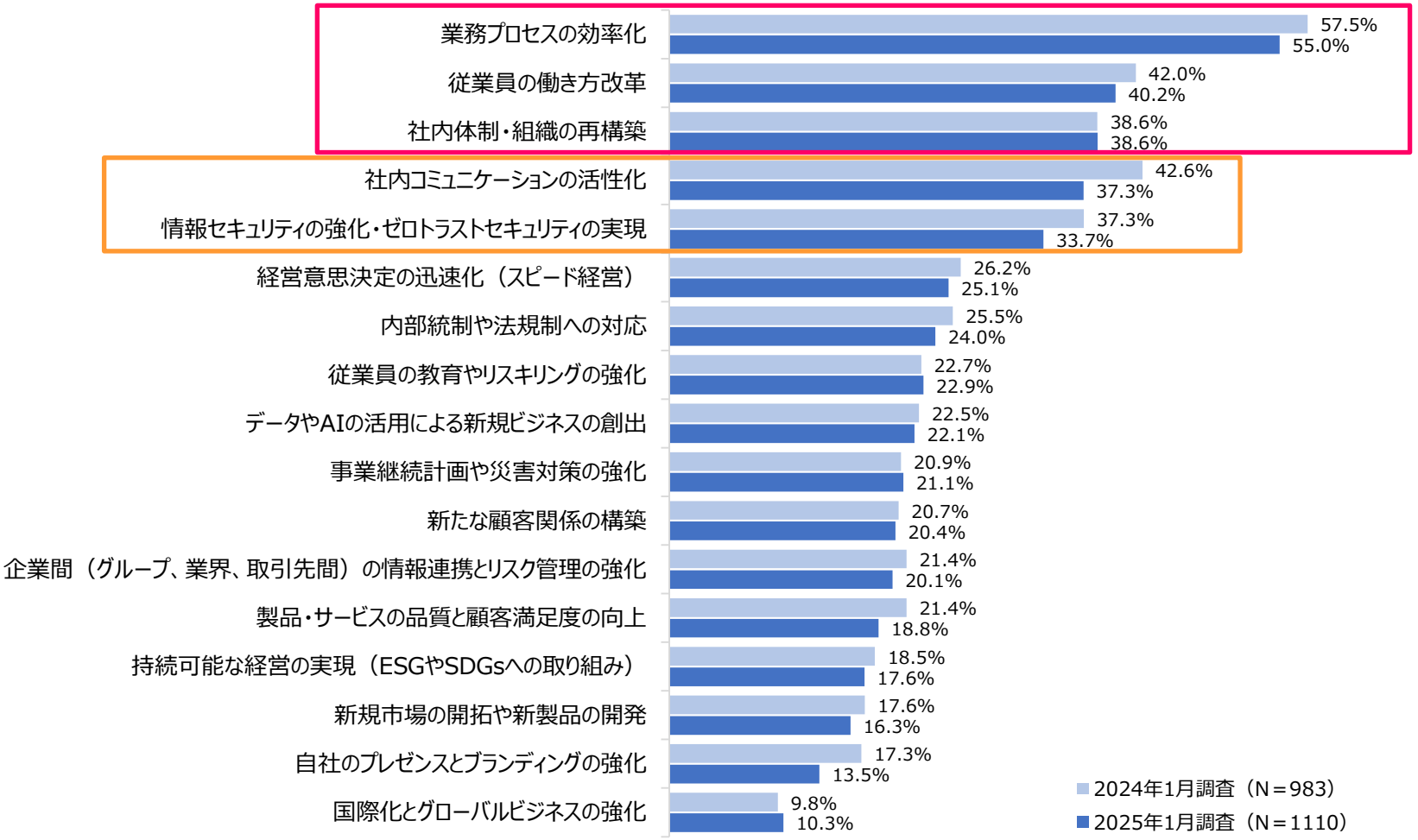
4. ランサムウェアとセキュリティ対策の実態

5. プライバシー保護に対する取り組み状況

6. 第三者認定／認証制度の取得状況

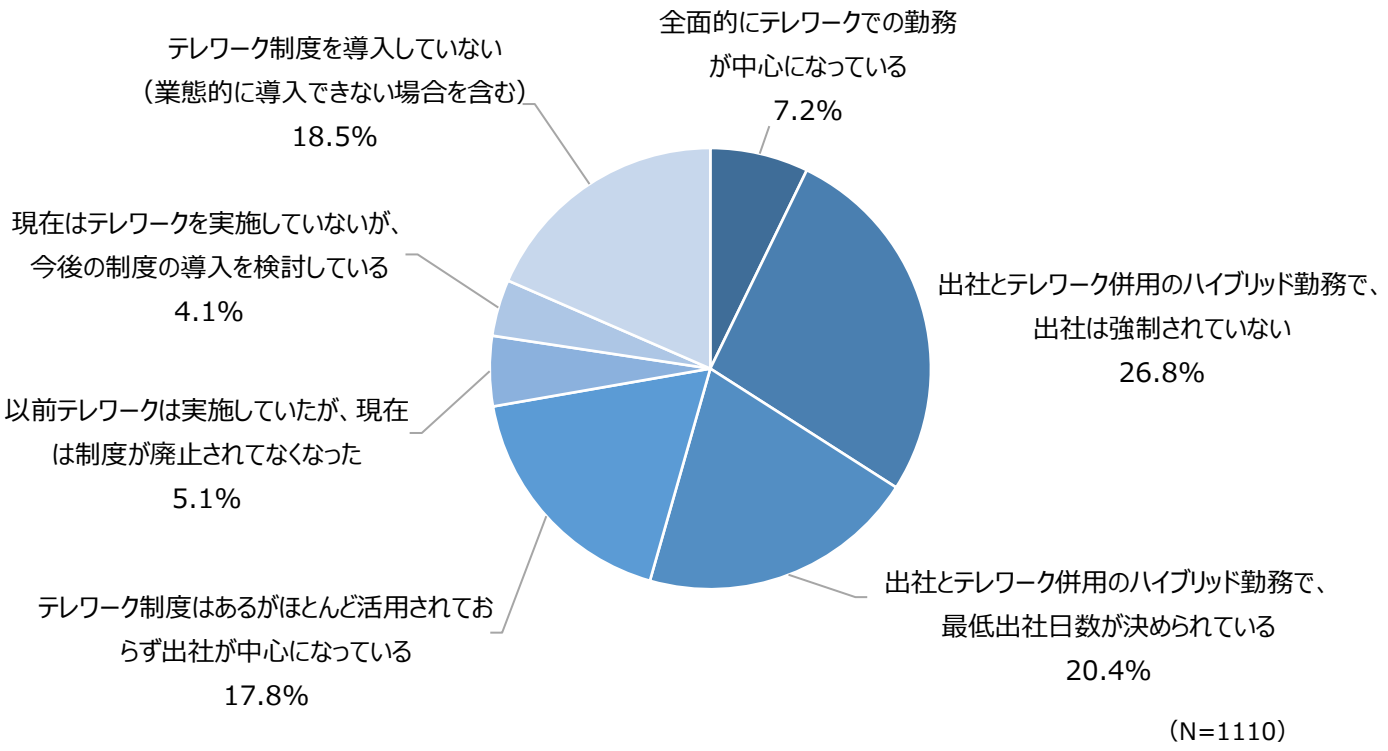
1.1　今後に向けて重視していく経営課題

- 2024年調査と同様に「業務プロセスの効率化」が最も多く、「従業員の働き方改革」「社内体制・組織の再構築」が続く。業務効率化や働き方改革は引き続き重点課題となっている。
- 「社内コミュニケーションの活性化」と「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」のポイントの減少が目立つが、重視される経営課題の上位5項目には入っている。



1.2　テレワークの実施状況

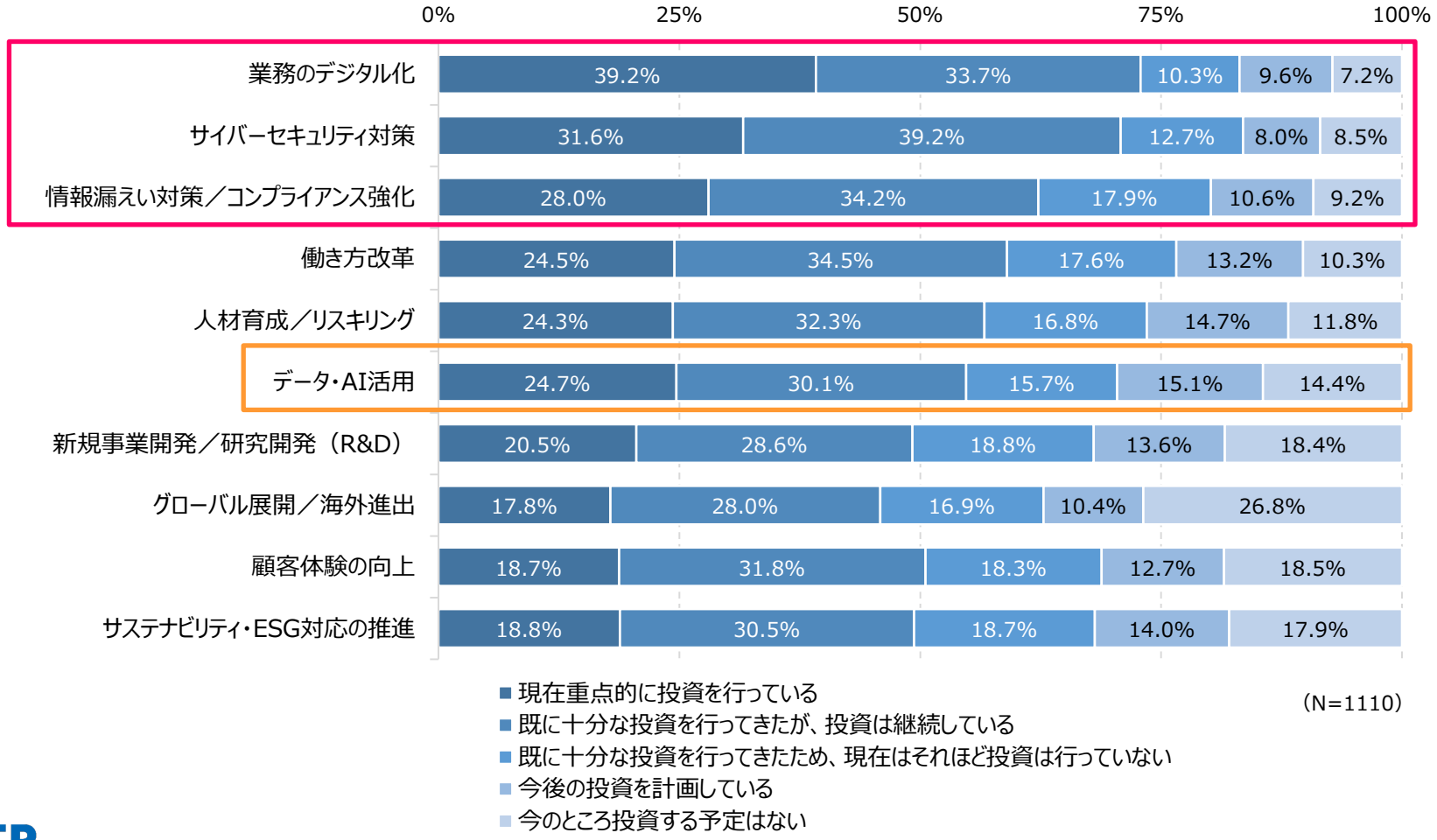
- 「全面的にテレワーク勤務が中心」は7.2%（2024年調査は10.9%）にとどまり、テレワークと出社のハイブリッド勤務（47.2%）が主流となっている。
- ハイブリッド勤務の中では「最低出社日数が決められている」が20.4%もあり、対面コミュニケーションを考慮するなど出社を義務付けたテレワークがみられる。
- 「ほとんど活用されていない」が17.8%、「制度が廃止された」が5.1%となり、テレワークが有効に機能していない企業も20%以上いるという状況にある。



（N=1110）

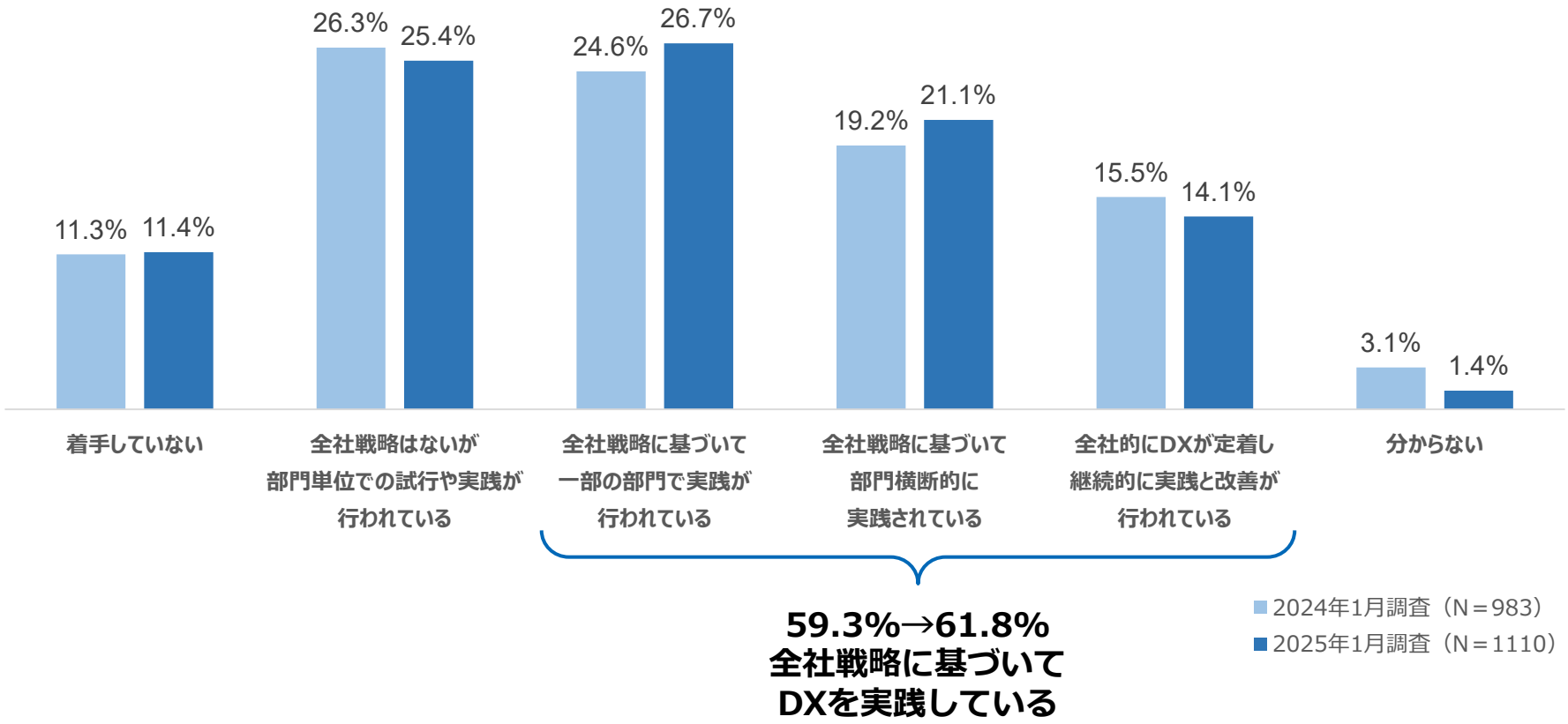
1.3　経営施策に対する投資状況

- 最も重点的に投資されている施策は「業務のデジタル化」となり、39%が重点投資対象である。
- 次に「サイバーセキュリティ対策」と「情報漏えい対策／コンプライアンス強化」が重点的に投資されており、セキュリティ・コンプライアンスに対する投資の優先度は高い。
- 注目度の高い「データ・AI活用」は、半数以上が重点的もしくは継続的に投資を行っている。



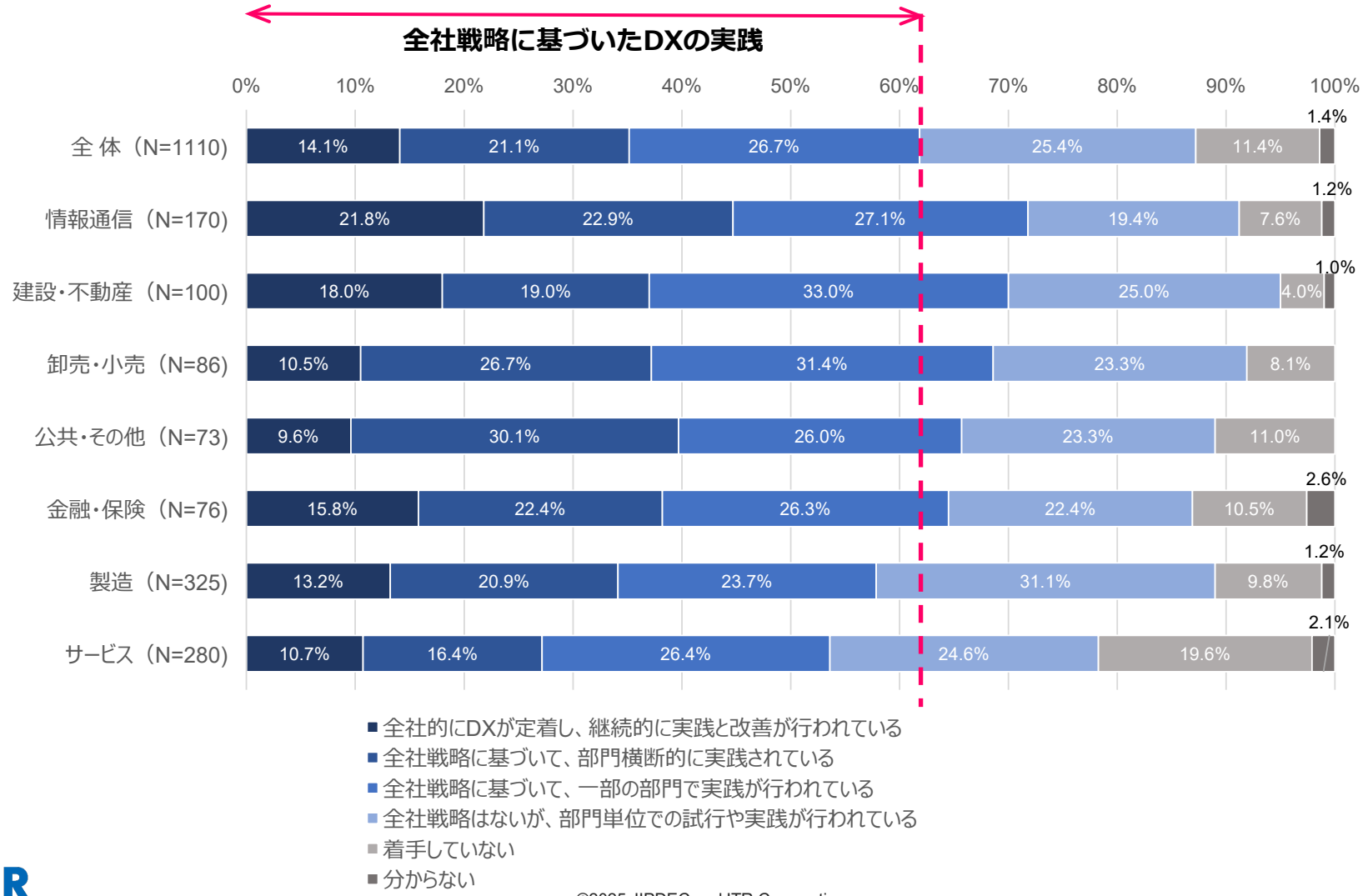
1.4　DXの実践段階の状況：全体

- 全社戦略に基づいてDXを実践している企業の割合は2024年調査から上昇しており、DXを企業戦略として推進している企業は拡大している。
- DXが定着している企業の割合は2024年調査からやや減少しており、定着化の難しさもうかがえる。



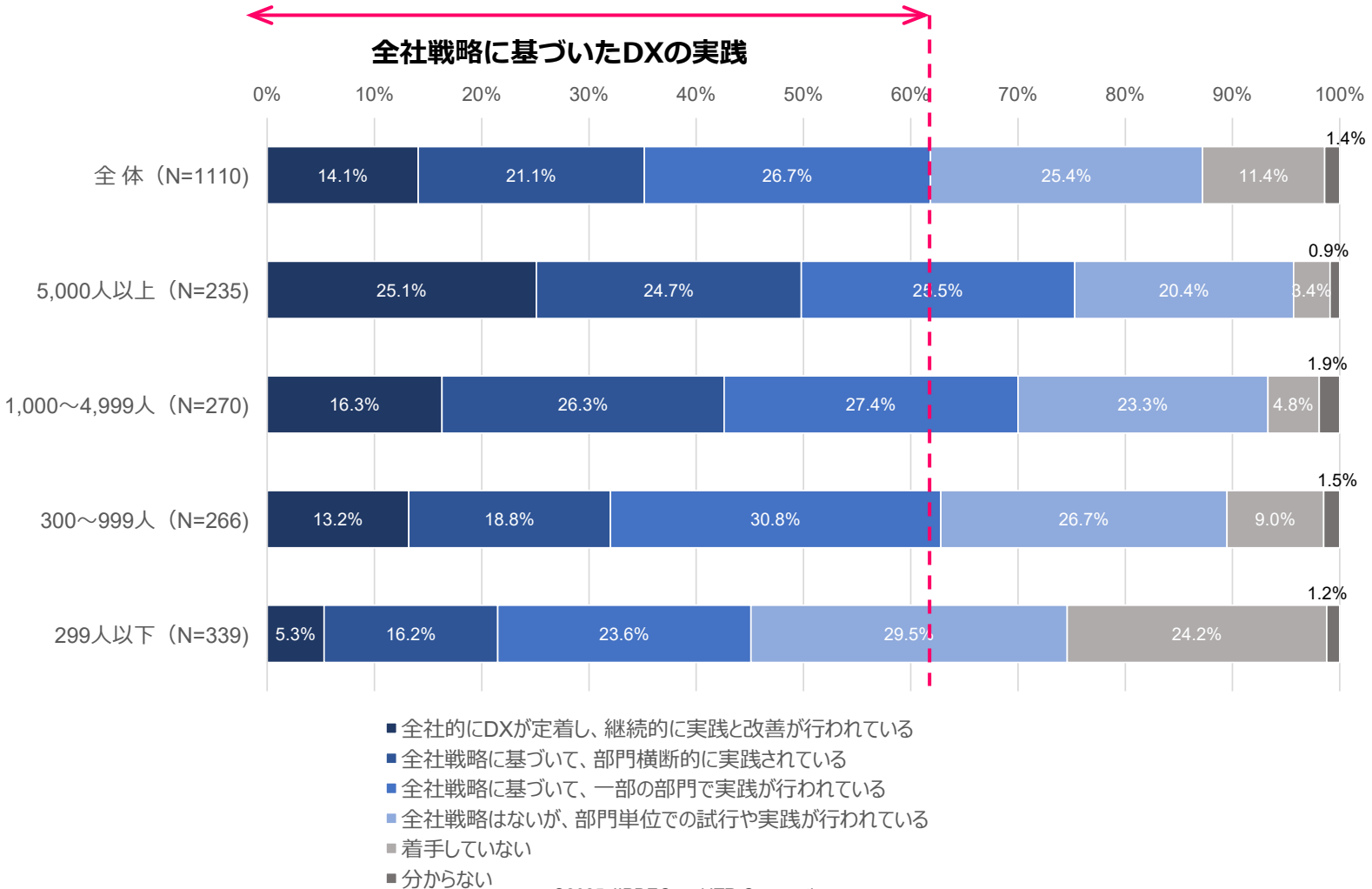
1.5　DXの実践段階の状況：業種別

- 全社戦略に基づいた実践は「情報通信」が最も進んでおり「建設・不動産」「卸売・小売」が続く。
- 「製造」と「サービス」が遅れをとっており、特に「サービス」は未着手が20%と最も遅れている。



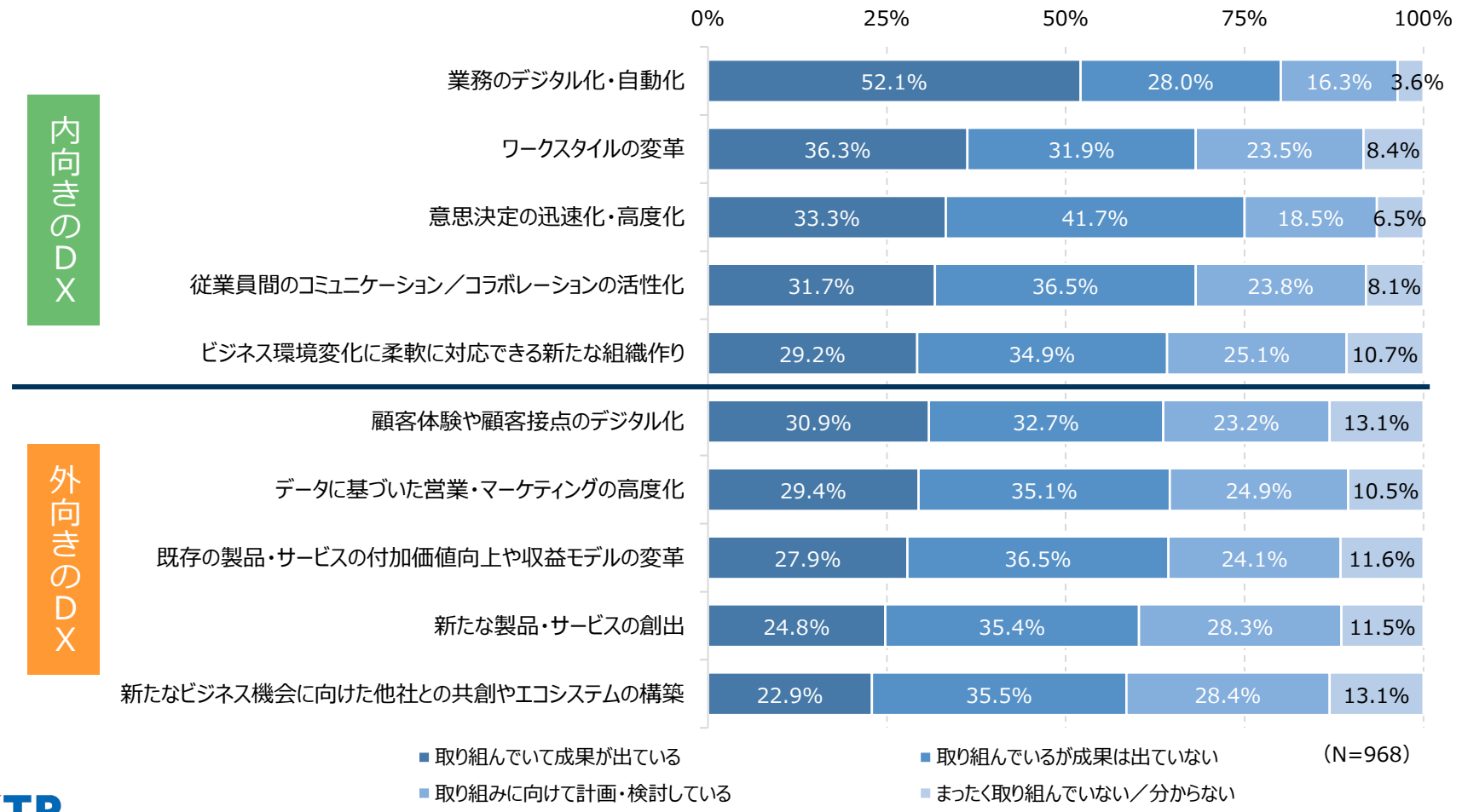
1.6　DXの実践段階の状況：従業員規模別

- 従業員規模が大きくになるにしたがいDXの実践が進んでいる傾向があり、「5,000人以上」ではDXが定着している企業が25%にもなっている。
- 「299人以下」ではDXの実践の遅れが顕著になり、未着手の割合も24%と大きい。



1.7　DXの取り組み内容と成果の状況

- **内向きのDX**（社内を対象に業務のデジタル化や従業員体験を向上させるDX）の方が、**外向きのDX**（顧客や市場に新たな価値を提供するDX）よりも取り組みが進み成果が出ている企業が多い。
- 内向きのDXでは「業務のデジタル化・自動化」が最も進んでおり、50%以上で成果が出ている。
- 外向きのDXでは、いずれの取り組みにおいても、まだ成果が出ていない企業の割合の方が大きい。



1.8　DXの成果が出ている業種

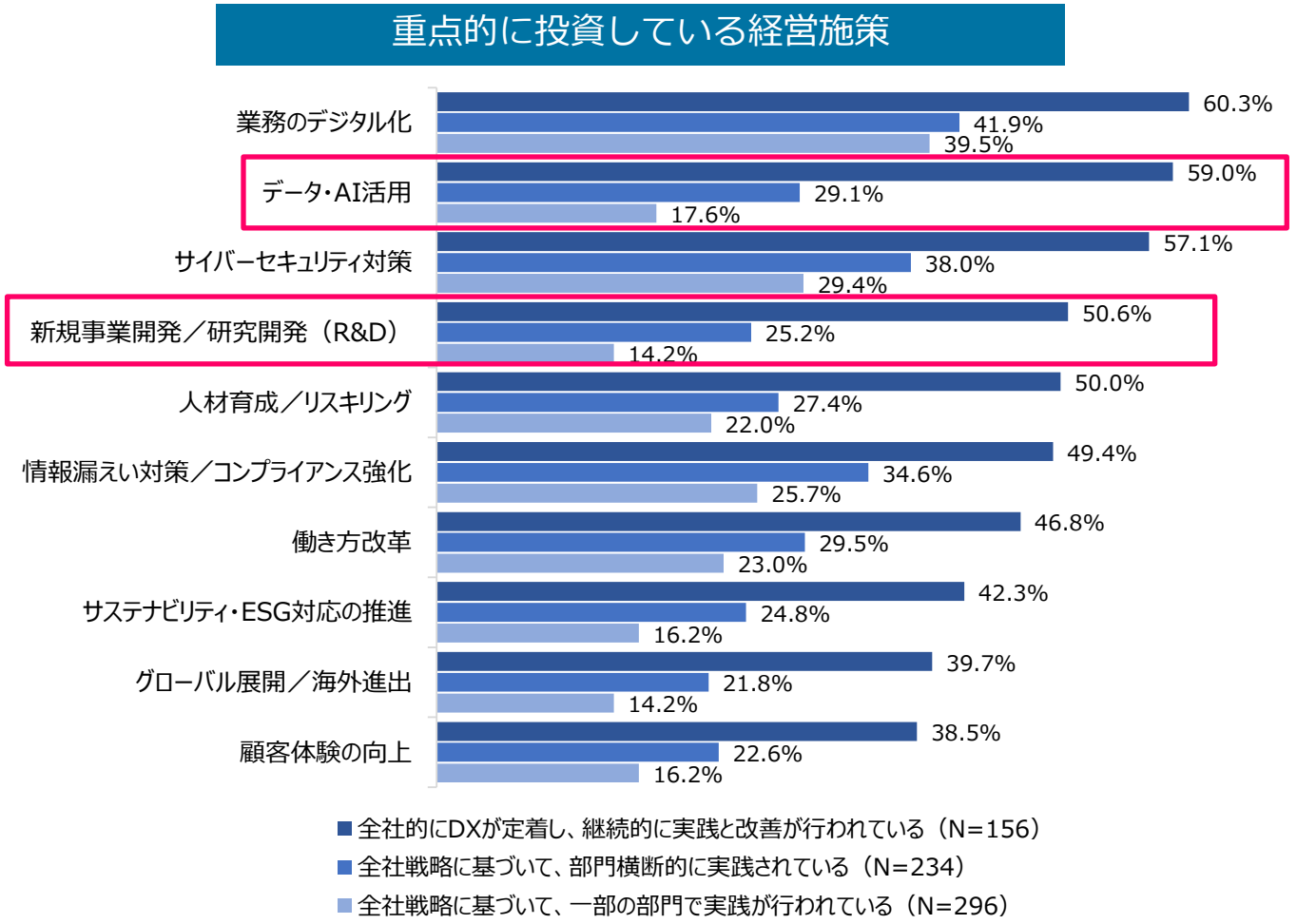
- 「情報通信」が最も成果が出ている。内向きでは業務のデジタル化・自動化が61%、外向きでは顧客体験・接点のデジタル化が41%で効果が出ている。
- 次いで「卸売・小売」も成果の割合が大きい。意思決定の迅速化は43%で成果が出ている。

		全　体 (N=968)	情報通信 (N=155)	卸売・小売 (N=79)	建設・不動産 (N=95)	金融・保険 (N=66)	サービス (N=219)	製造 (N=289)	公共・その他 (N=65)
内向きのDX	業務のデジタル化・自動化	52.1%	60.6%	58.2%	50.5%	48.5%	50.7%	47.4%	55.4%
	ワークスタイルの変革	36.3%	46.5%	39.2%	44.2%	39.4%	32.9%	31.5%	26.2%
	意思決定の迅速化・高度化	33.3%	35.5%	43.0%	32.6%	30.3%	31.5%	33.6%	24.6%
	従業員間のコミュニケーション／コラボレーションの活性化	31.7%	37.4%	32.9%	32.6%	34.8%	31.5%	29.4%	23.1%
	ビジネス環境変化に柔軟に対応できる新たな組織作り	31.7%	37.4%	32.9%	32.6%	34.8%	31.5%	29.4%	23.1%
	内向きのDX平均	**37.0%**	**43.5%**	**41.2%**	**38.5%**	**37.6%**	**35.6%**	**34.3%**	**30.5%**
外向きのDX	顧客体験や顧客接点のデジタル化	30.9%	40.6%	39.2%	31.6%	36.4%	25.6%	29.1%	16.9%
	データに基づいた営業・マーケティングの高度化	29.4%	38.7%	34.2%	27.4%	27.3%	27.9%	28.0%	18.5%
	既存の製品・サービスの付加価値向上や収益モデルの変革	27.9%	39.4%	27.8%	25.3%	30.3%	26.5%	24.9%	20.0%
	新たな製品・サービスの創出	24.8%	31.0%	25.3%	25.3%	19.7%	26.0%	22.1%	21.5%
	新たなビジネス機会に向けた他社との共創やエコシステムの構築	24.8%	31.0%	25.3%	25.3%	19.7%	26.0%	22.1%	21.5%
	外向きのDX平均	**27.6%**	**36.1%**	**30.4%**	**27.0%**	**26.7%**	**26.4%**	**25.2%**	**19.7%**

注1：「取り組んでいて成果が出ている」と回答した企業の回答率

1.9　経営施策への投資状況とDX実践段階の関係

- DX定着企業は、各経営施策に対して重点的に投資を行っている企業が多い。
- 「データ・AI活用」と「新規事業開発／研究開発」は、DX定着企業とそれより低い実践段階の企業との差が大きく開いている。DX定着企業は、AIに積極的に投資を行い、新しい事業を創出していこうという姿勢が色濃く見られ、DXが定着しない企業との差が出ている。



1.10　DXの実践で生じている問題：DX実践段階別

- 「組織間の連携やコミュニケーションが不足」がDXを実践する上で最も大きな問題となっている。特に部門横断的に取り組むことの難しさがうかがえる。
- DXの実践が一部や試行に留まっている企業は「業務プロセスや既存システムが複雑」「データの活用が十分にできていない」「従業員のデジタルスキル不足」が定着化もしくは部門横断的な実践企業よりも問題が生じている。

	全　体 (N=842)	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 (N=152)	全社戦略に基づいて、部門横断的に実践されている (N=189)	全社戦略に基づいて、一部の部門で実践が行われている (N=242)	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 (N=259)
組織間の連携やコミュニケーションが不足している	41.7%	41.8%	45.3%	40.2%	37.2%
業務プロセスや既存システムが複雑である	36.5%	33.7%	31.1%	37.6%	50.0%
既存業務の負担が大きくDXまで手が回らない	34.5%	32.6%	35.1%	37.2%	32.7%
経営層の理解や関与が不足している	22.8%	21.6%	26.0%	23.5%	17.9%
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	22.6%	16.7%	23.6%	24.4%	28.8%
従業員のデジタルスキル不足や意識改革が遅れている	20.0%	18.1%	18.2%	23.1%	22.4%
DXの成果やKPIの可視化ができていない	19.9%	16.0%	18.9%	21.4%	26.9%
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	18.2%	9.2%	18.6%	22.6%	26.9%
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	17.0%	11.7%	17.9%	20.5%	19.9%
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	13.8%	7.8%	13.5%	18.4%	18.6%
顧客志向の文化が根付いていない	9.9%	8.5%	10.1%	9.4%	12.8%
特に課題は出ていない	6.3%	3.5%	5.4%	6.4%	12.8%

1.11　経営課題とDX実践状況：調査結果からの考察

- 最も重視されている経営課題は業務プロセスの効率化である。その課題に対する取り組みとして、DXの中で業務のデジタル化・自動化が最も実践されており、高い効果が出ている。経営課題とDXがしっかり紐づいた例となっている。

- 働き方改革も経営課題とDXの実践が伴った取り組みとなっている。ただし、働き方改革の中心を担ってきたテレワークでは、出社を義務付ける企業や活用できていない企業も一定層みられることから、より多様な働き方を模索していく必要がある。

- 「外向きのDX」の遅れは国内DXの課題である。DX定着企業のようにデータやAIの投資・活用を積極的に進め、デジタル技術を活用した新しい製品やサービスの開発に挑戦し続けることが重要となる。

- DXの実践段階が低い企業の主な課題として、組織間の連携やコミュニケーションの不足、従業員の意識やデジタルスキルの不足がある。テクノロジーだけではなく、企業文化や組織体制の改革を併せて取り組んでいくことが、DXを全社に浸透させていくための重要なポイントになる。

報告する調査項目

1. 経営課題とDX実践状況

2. 電子契約の利用状況

3. 生成AIの活用状況と課題

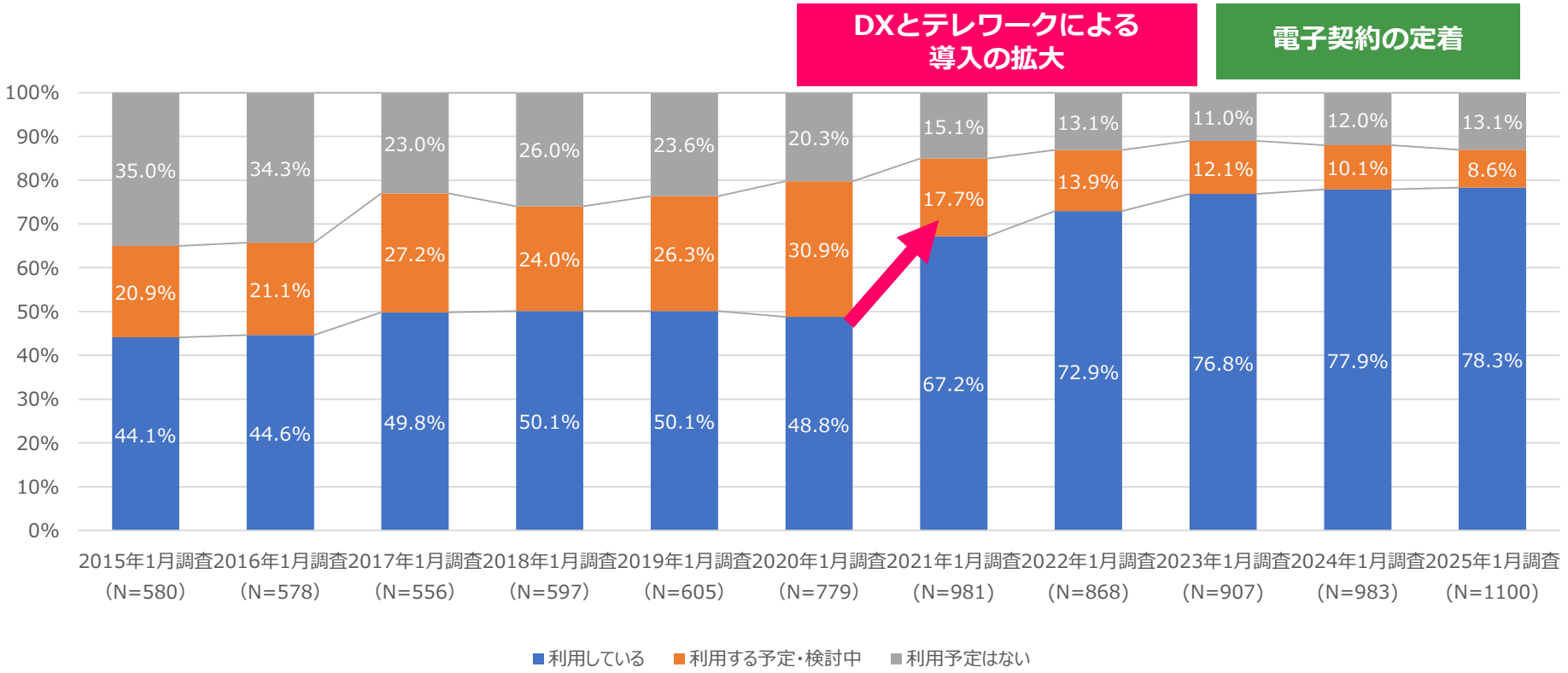
4. ランサムウェアとセキュリティ対策の実態

5. プライバシー保護に対する取り組み状況

6. 第三者認定／認証制度の取得状況

2.1　電子契約の利用状況の推移：2015年～2025年

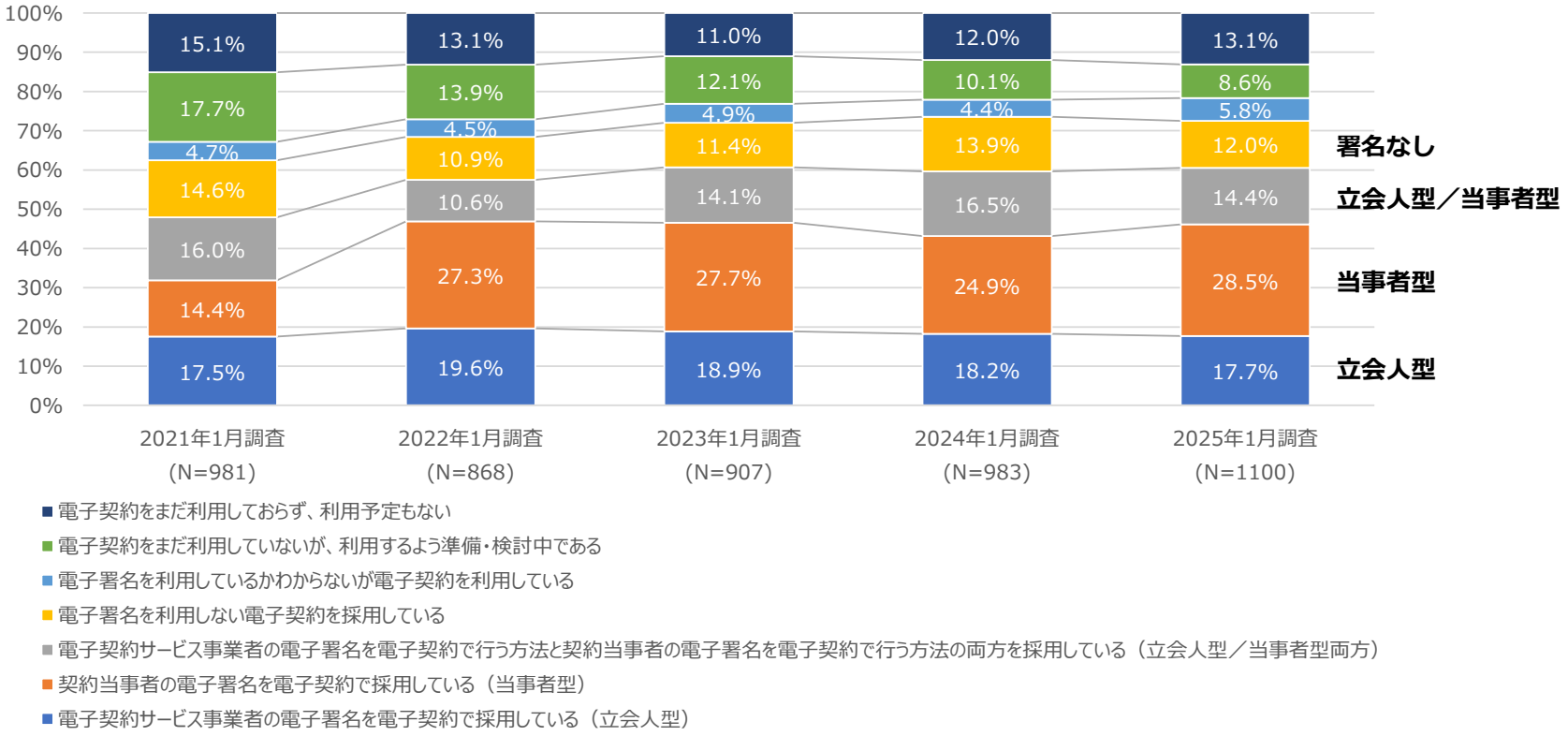
- 2020年調査までは電子契約の利用率が横ばいに推移していたが、2021年調査で大きく上昇している。DXによる業務のデジタル化の推進と、2020年からの新型コロナウイルス感染拡大によってテレワークが普及し、電子契約の需要が高まり2020年から2022年にかけて導入が拡大したとみられる。
- 2025年調査での利用率は78.3%であり、2023年調査からほぼ横ばいで推移している。すでに8割近い企業が利用しており、導入がひと段落し、電子契約が定着したと考えられる。



注1：2020年以前は質問が異なり、「わからない」の回答を除いている
注2：2022～2023年調査は、他の調査と母集団を統一するため従業員数50名以上の回答者に限定し再集計

2.2　電子契約の利用状況の推移（契約タイプ別）：2021年～2025年

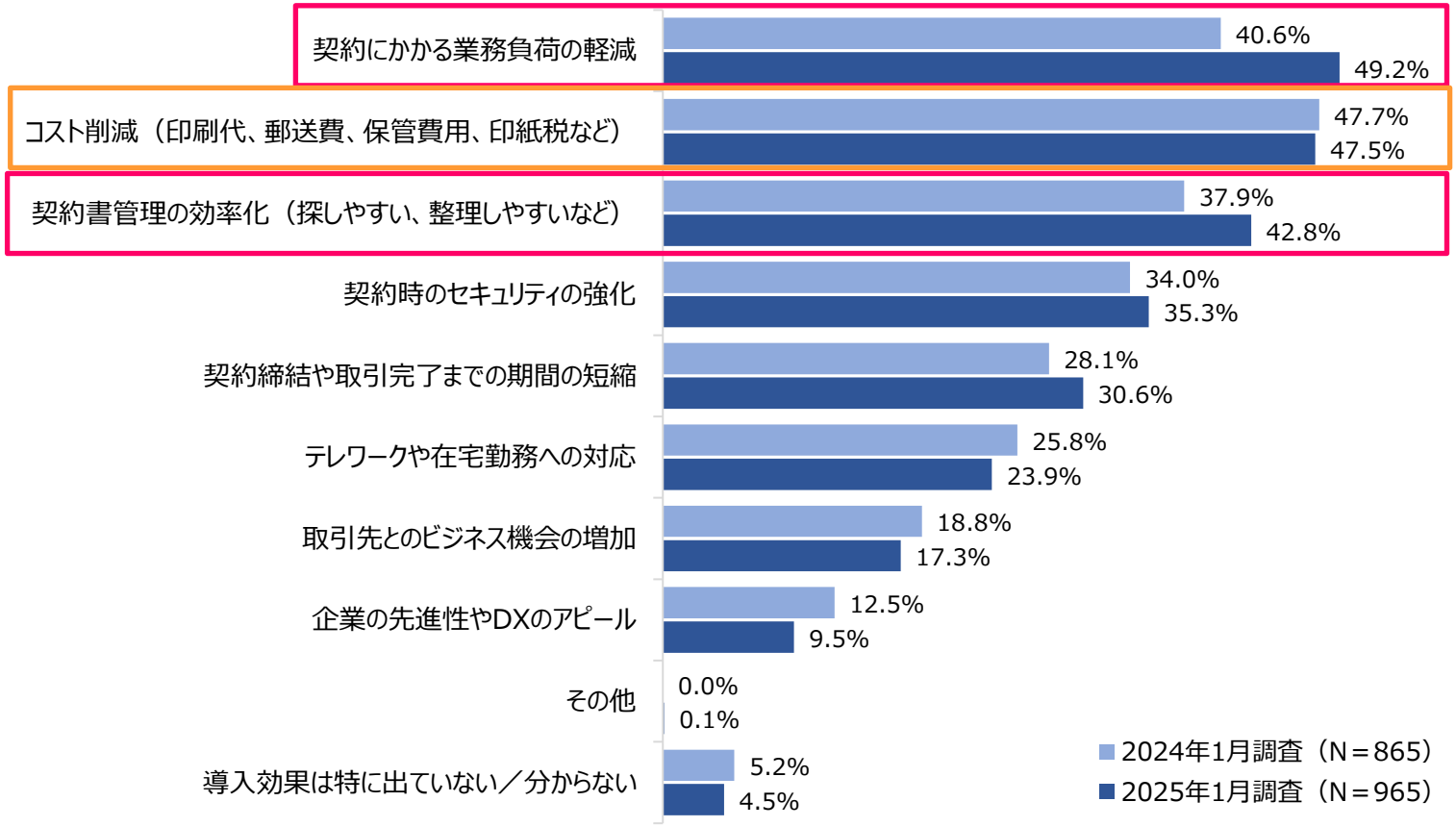
- 「立会人型」は4年間で大きな変化は見られないが、徐々に割合が低くなっている。
- 「当事者型」は2022年調査で利用割合が大きく拡大し、それ以降で利用割合が最も大きい署名タイプとなっている。2025年調査では最も大きな割合を占めている。
- 「立会型／当事者型両方」は、2024年調査で一度割合が大きくなったが、2025年調査では2023年調査の水準に戻っている。



注1：2020年以前は質問が異なり、「わからない」の回答を除いている
注2：2022～2023年調査は、他の調査と母集団を統一するため従業員数50名以上の回答者に限定し再集計

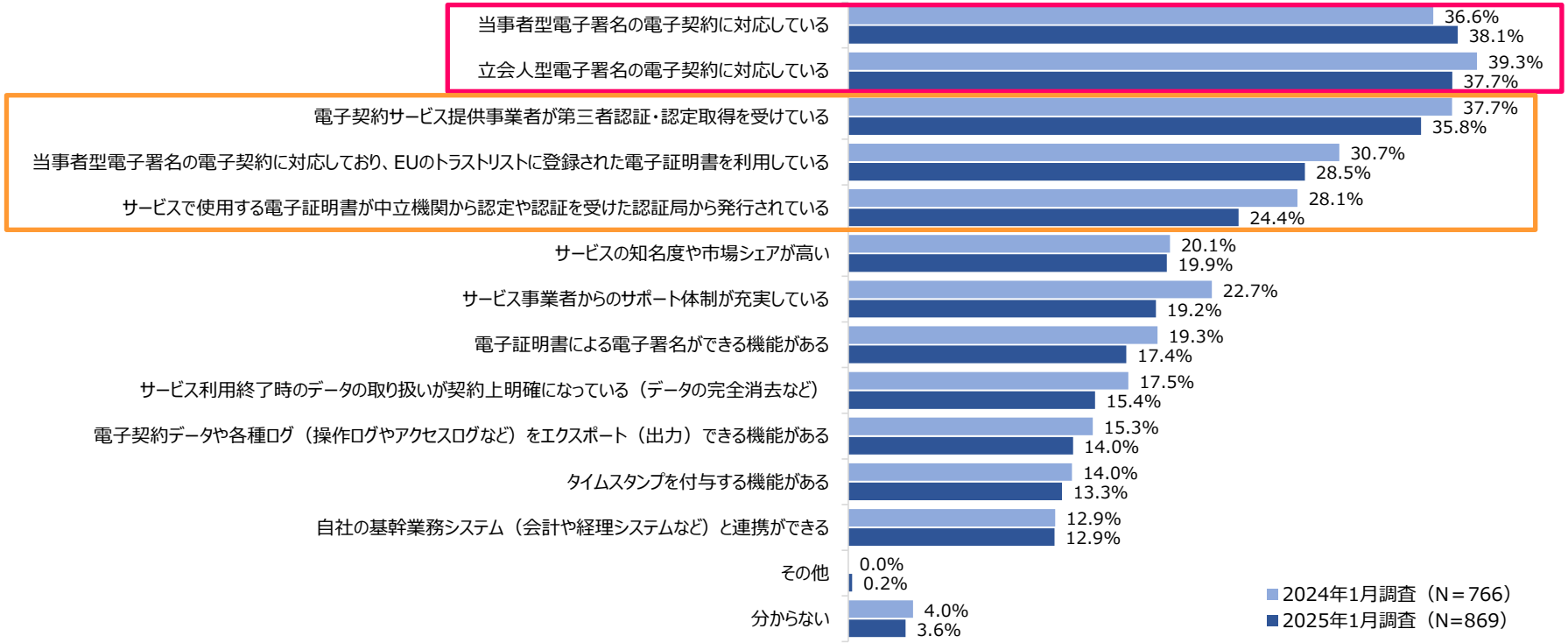
2.3　電子契約の利用による効果

- 「契約にかかる業務負荷の軽減」が最も多く、2024年調査から大きく上昇している。3番目の「契約書管理の効率化（探しやすい、整理しやすいなど）」も前回調査から上昇しており、契約にかかる業務負荷や管理の効率化での導入効果が出ている企業が増えている傾向にある。
- 2番目には「コスト削減」が挙がっており、印刷代や郵送費、印紙税など契約にかかるコストの削減に大きな効果が出ている。



2.4　電子契約サービスの選定で重視する点：全体と利用電子契約形態別

- 「当事者型電子署名の電子契約に対応している」と「立会人型電子署名の電子契約に対応している」、それぞれの契約タイプでの対応が重視する点として上位に挙がっている。
- 「電子契約サービス提供事業者が第三者認証・認定取得を受けている」が3番目に重視されており、サービス事業者が第三者認証を所得していることも重要な選定ポイントになっている。
- 「当事者型電子署名の電子契約に対応しており、EUのトラストリストに登録された電子証明書を利用している」と「サービスで使用する電子証明書が中立機関から認定や認証を受けた認証局から発行されている」が上位に挙がっていることから、信頼性の高い電子証明書の利用も重視されている。



2.5　電子契約の利用状況：調査結果からの考察

- 電子契約の利用率は8割近くに達している。コロナ禍以降急速に導入拡大が続いていたが、導入がひと段落し、商習慣として電子契約が定着したとみられる。

- 電子契約のタイプは、当事者型の利用が拡大傾向にある。当事者型は仲介者を必要とせずに契約を締結できるため、契約締結までの時間が短縮できるという利点がある。契約の種類や相手方の環境によっては、立会人型との使い分けも必要になる。

- 電子契約の大きな導入効果は、契約の締結や契約書の管理などの業務効率化である。さらに、印刷代や印紙税などのコスト削減効果も出ている。

- 電子契約サービスの選定要因として、サービス事業者が、プライバシーマークやISMS認証のような第三者機関の認証・認定を取得していることが重視されている。また、電子証明書の信頼性も重要な選定ポイントとなっている。

報告する調査項目

1. 経営課題とDX実践状況

2. 電子契約の利用状況

3. 生成AIの活用状況と課題

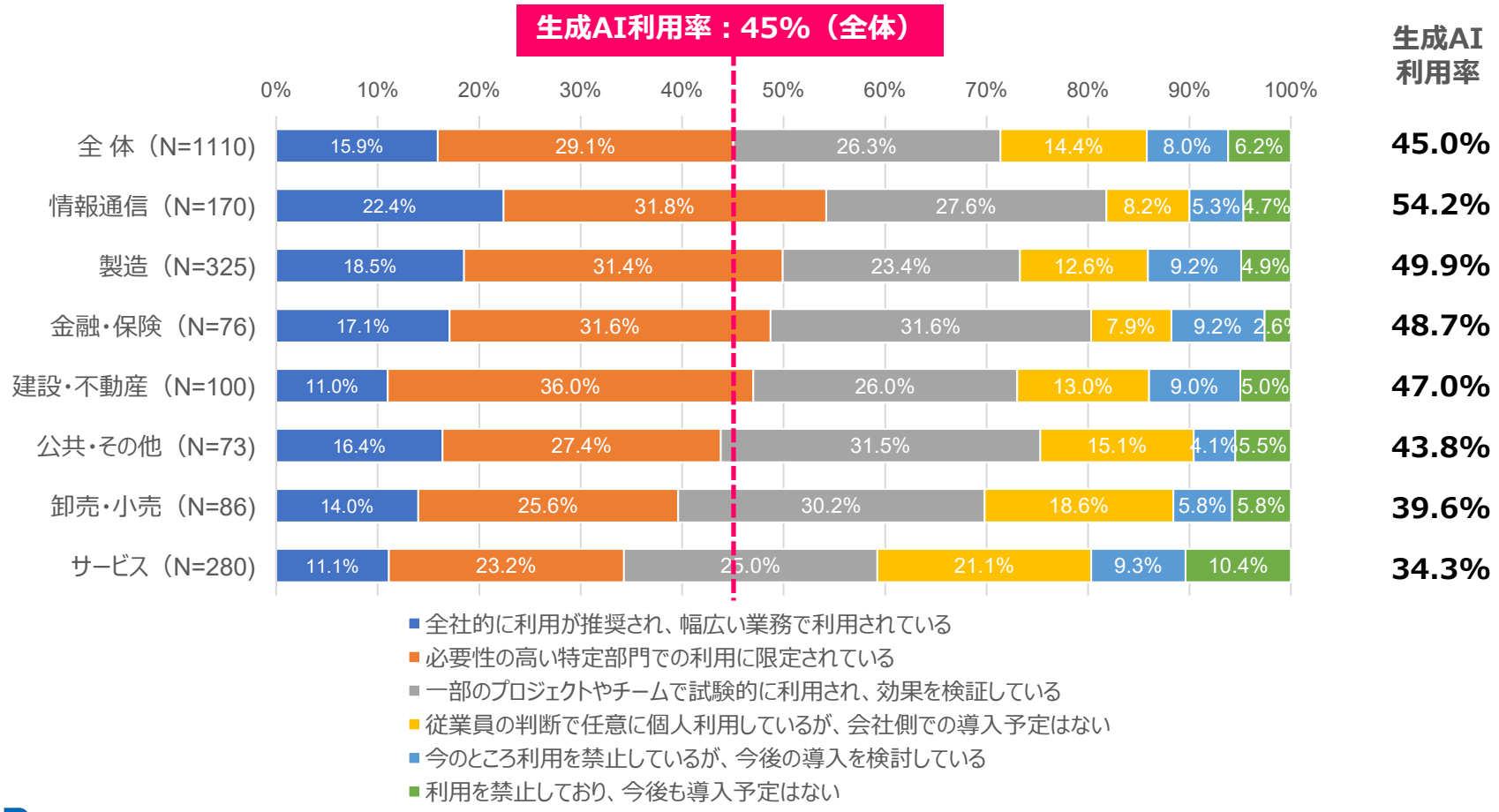
4. ランサムウェアとセキュリティ対策の実態

5. プライバシー保護に対する取り組み状況

6. 第三者認定／認証制度の取得状況

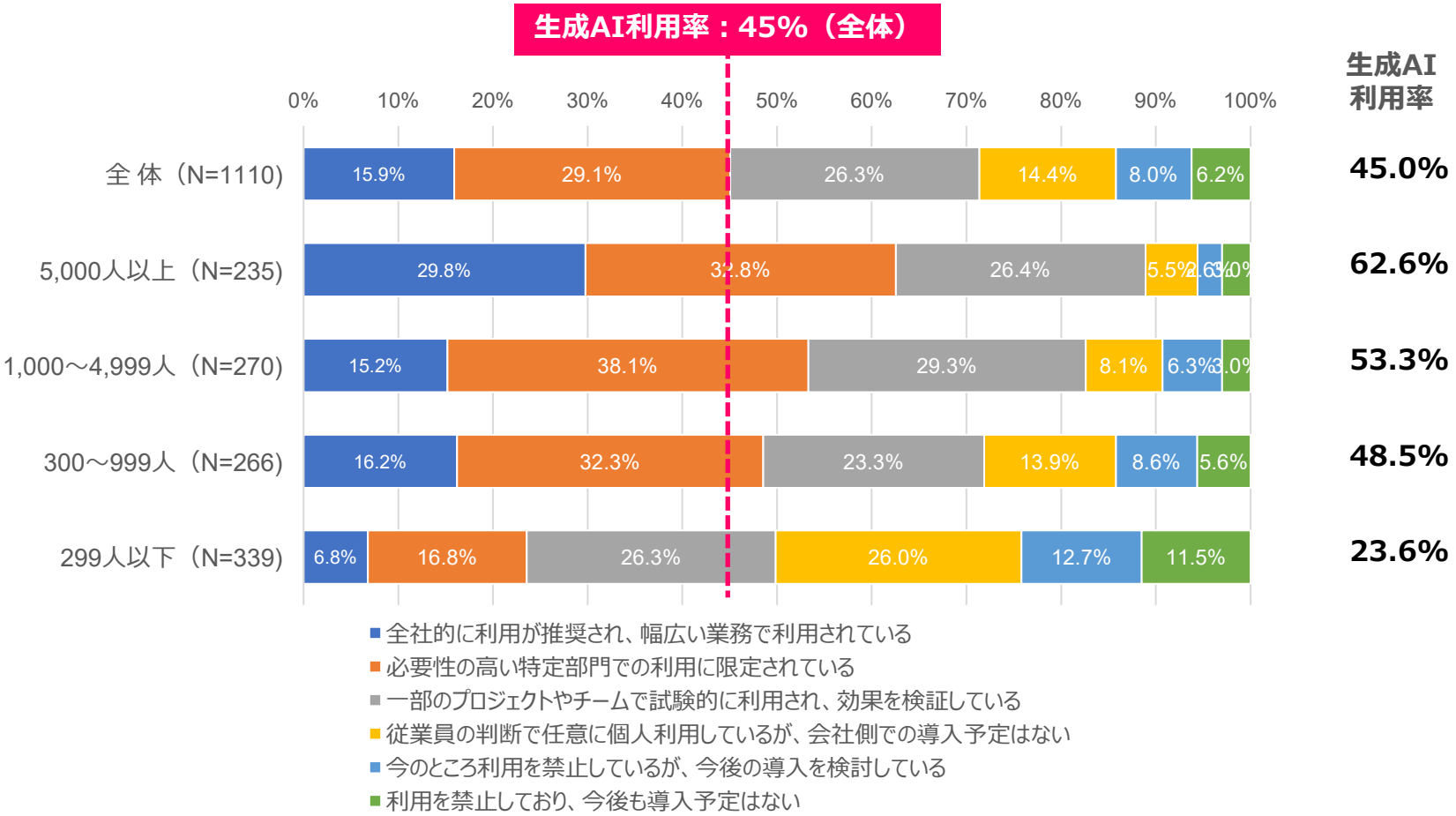
3.1　生成AIの利用状況：全体と業種別

- 生成AIの利用率は45.0%、その中で全社利用は15.9%にとどまり、まだ特定部門での利用が多い。
- 検証している企業は26.3%、今後のさらなる利用拡大が見込まれる。
- 利用率では「情報通信」が50%を超え、「製造」「金融・保険」「卸売・小売」が続く。一方、「卸売・小売」と「サービス」は40%未満と低い。



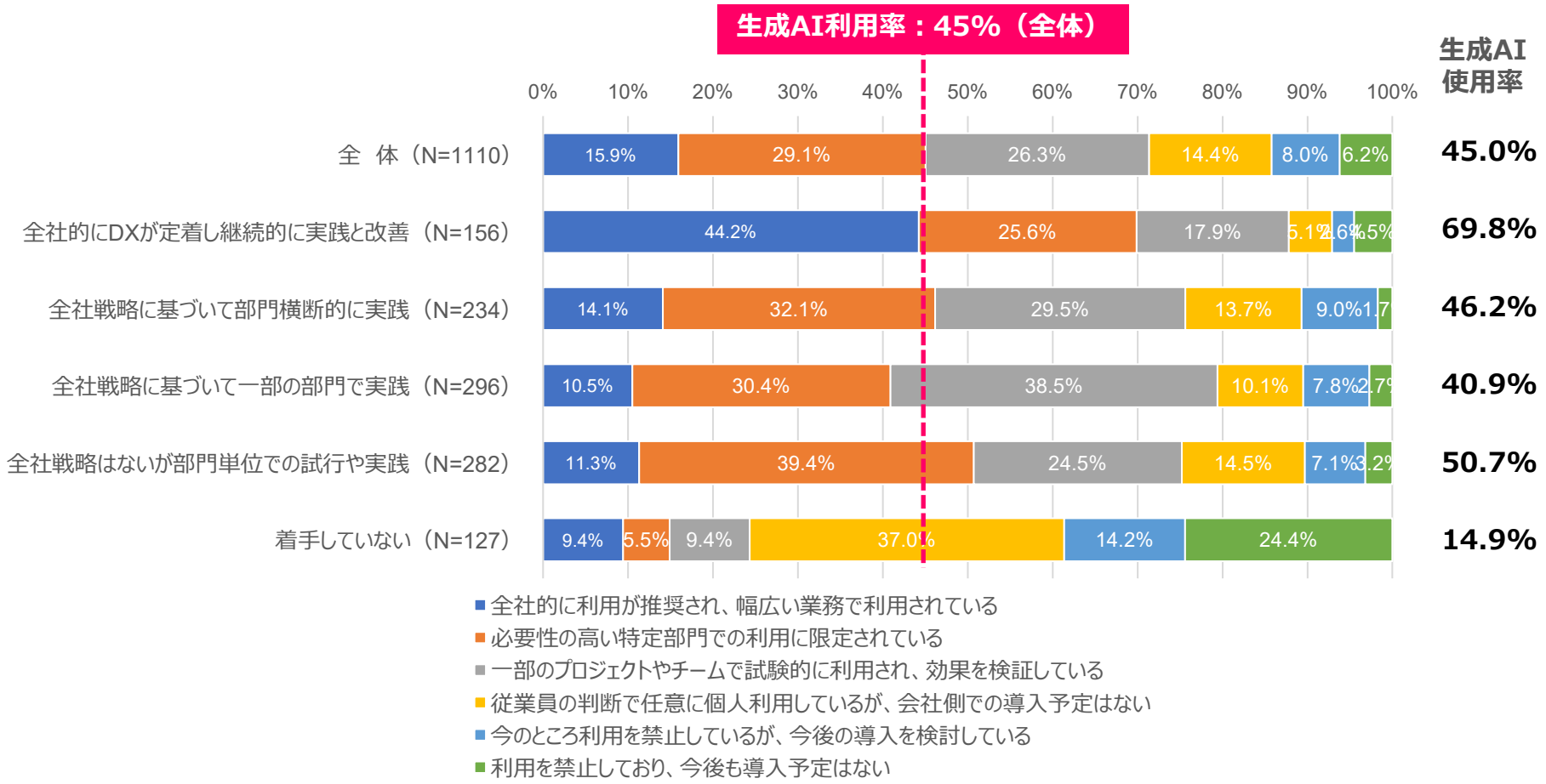
3.2　生成AIの利用状況：従業員規模別

- 従業員規模が大きくなるにしたがい、生成AIの利用率が上昇している。「5,000人以上」では60%以上で利用されている。また、全社利用の割合についても他の規模と比べ大きい。
- 「299人以下」になると、利用率が23.6%と大きく下がっている。



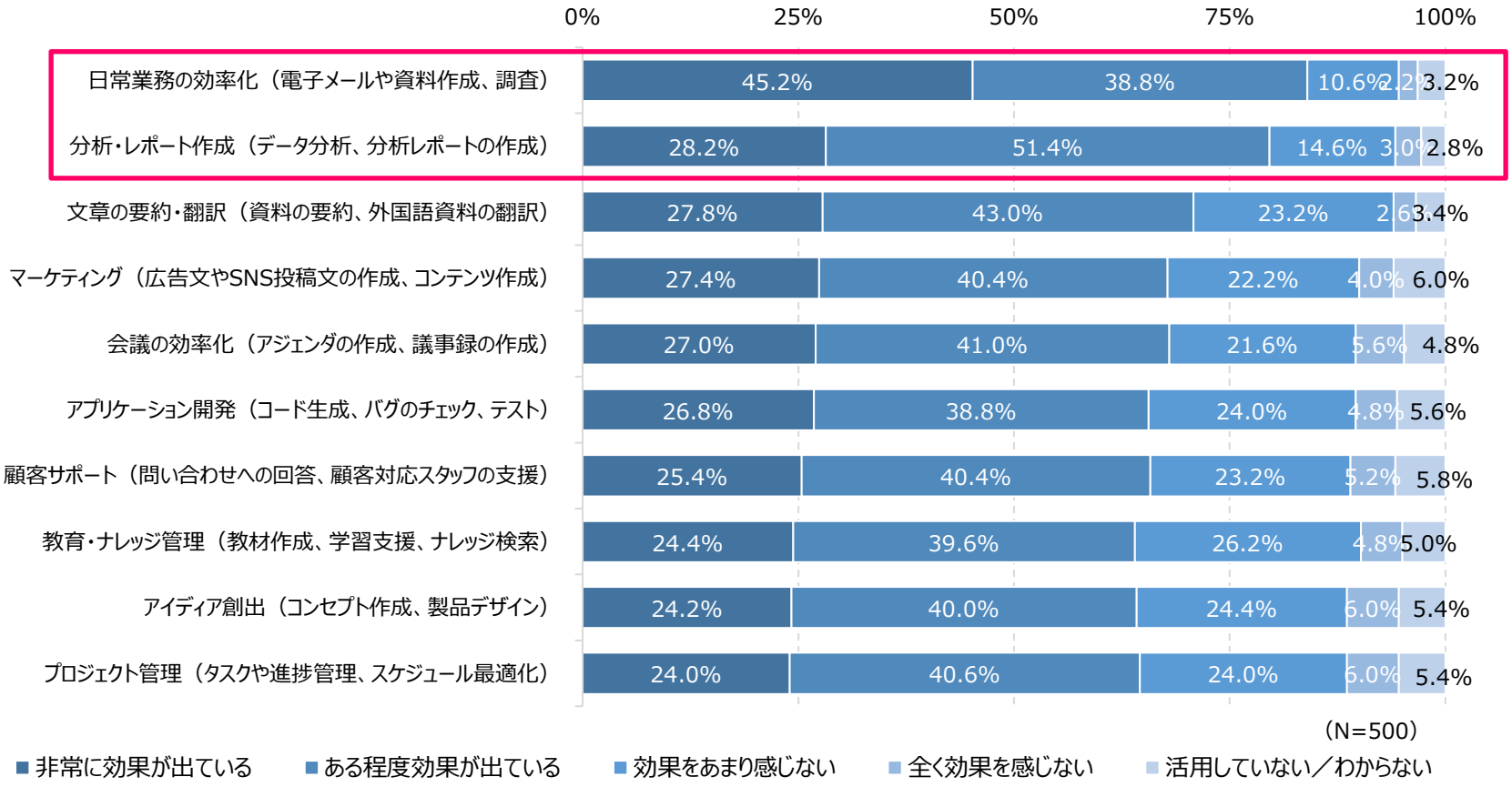
3.3　生成AIの利用状況：DX実践段階別

- 「DX定着企業」は生成AIの利用率が約70%と非常に利用が進んでいる。さらに全社利用の割合の方が大きい。DX戦略として生成AIを積極的に活用していく姿勢がうかがえる。
- それ以外の段階の企業は特定部門での利用が多い。生成AI利用において、DX定着企業とそれ以外の企業との差が大きく開いている状況にある。



3.4 生成AIの活用効果

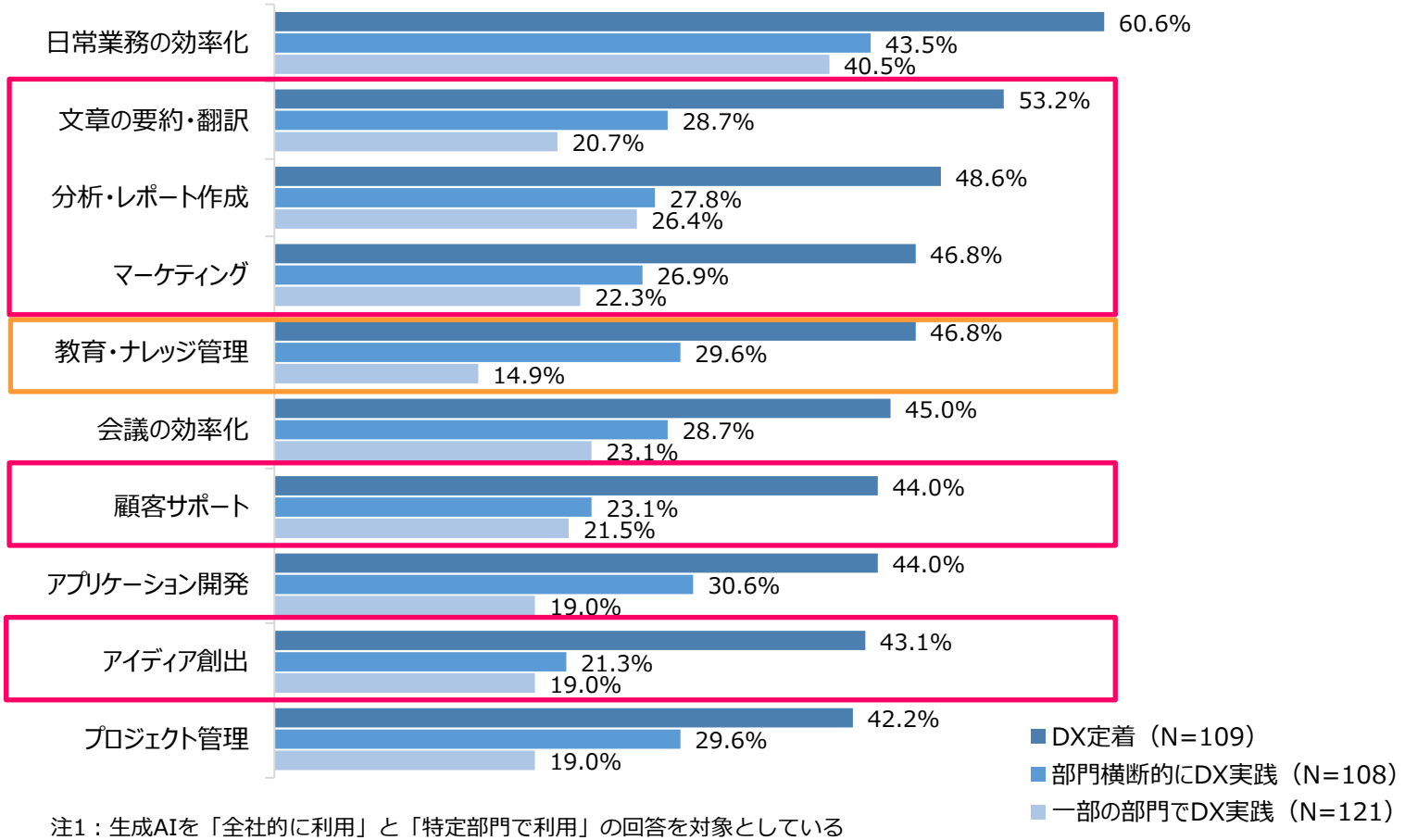
- 「日常業務の効率化」は45.2%が非常に効果が出ているとしており、ある程度の効果を含めると84%で活用効果を認識している。「分析・レポート作成」も活用効果が出ている企業が79.6%と非常に多い。
- その他、「文章の要約・翻訳」「会議の効率化」「マーケティング」など、調査設問にあげたいずれの業務でも、効果が出ていると回答した企業が60%を超えている。生成AIを利用している企業の多くは、さまざまな業務で一定の活用効果をあげていることがうかがえる。



注1：生成AIを「全社的に利用」と「特定部門で利用」の回答を対象としている

3.5　活用効果の高い業務：DX実践段階別

- 各業務で生成AIを活用して非常に効果が出ている割合をDX実践段階別で示している。
- DX定着企業はいずれの業務でも高い値を示し、「日常業務」は60%で非常に効果が出ている。
- DX定着企業と部門横断で実践している企業との差が大きいのは（20ポイント以上の差）、「文章の要約・翻訳」「分析・レポート」「マーケティング」「顧客サポート」「アイディア創出」である。
- 「教育・ナレッジ管理」は一部の部門で実践している企業が非常に低くなっている。



注1：生成AIを「全社的に利用」と「特定部門で利用」の回答を対象としている

3.6　活用効果の高い業務：業種別

- 各業務で生成AIを活用して非常に効果が出ている割合を業種別で示している。
- 効果の平均値が最も高いのは卸売・小売で35.3%となった。特に「顧客サポート」において他の業種よりも高い割合を示しており、消費者や取引先からの問い合わせ対応で高い活用効果が出ている。
- 公共・その他では「教育・ナレッジ管理」が高く、学校での活用効果が出ていることがうかがえる。

	全　体 (N=500)	卸売・小売 (N=34)	サービス (N=96)	公共・その他 (N=32)	情報通信 (N=92)	製造 (N=162)	金融・保険 (N=37)	建設・不動産 (N=47)
効果の平均値	**28.0%**	**35.3%**	**31.6%**	**28.4%**	**28.4%**	**26.3%**	**24.3%**	**23.6%**
日常業務の効率化	45.2%	55.9%	53.1%	56.3%	44.6%	40.7%	37.8%	36.2%
分析・レポート作成	28.2%	38.2%	33.3%	18.8%	26.1%	29.0%	24.3%	21.3%
文章の要約・翻訳	27.8%	38.2%	32.3%	18.8%	26.1%	26.5%	27.0%	25.5%
マーケティング	27.4%	35.3%	29.2%	21.9%	32.6%	25.3%	24.3%	21.3%
会議の効率化	27.0%	41.2%	30.2%	37.5%	22.8%	22.2%	24.3%	29.8%
アプリケーション開発	26.8%	26.5%	27.1%	21.9%	28.3%	28.4%	29.7%	19.1%
顧客サポート	25.4%	38.2%	27.1%	18.8%	28.3%	24.1%	18.9%	21.3%
教育・ナレッジ管理	24.4%	23.5%	25.0%	37.5%	30.4%	21.6%	13.5%	21.3%
アイディア創出	24.2%	29.4%	29.2%	25.0%	20.7%	22.2%	24.3%	23.4%
プロジェクト管理	24.0%	26.5%	29.2%	28.1%	23.9%	22.8%	18.9%	17.0%

注1：生成AIを「全社的に利用」と「特定部門で利用」の回答を対象としている
注2：効果の平均は業種ごとに10個の業務の割合の平均値である

3.7　活用効果の高い業務：従業員規模別

- 各業務で生成AIを活用して非常に効果が出ている割合を従業員規模別で示している。
- 効果の平均値が最も高いのは5,000人以上で33.7%となった。その次に高いのが300～999人となっており、1,000～4,999人はそれよりも低い結果となった。効果は規模に比例しているわけではない。
- 5,000人以上では「マーケティング」と「顧客サポート」が他の従業員規模より高い割合を示している。
- 300～999人では「アプリケーション開発」が他の従業員規模より高い割合を示している。

	全　体 (N=500)	5,000人以上 (N=147)	1,000～4,999人 (N=144)	300～999人 (N=129)	299人以下 (N=80)
効果の平均値	**28.0%**	**33.7%**	**23.5%**	**29.5%**	**23.5%**
日常業務の効率化	45.2%	51.0%	38.9%	47.3%	42.5%
分析・レポート作成	28.2%	34.7%	22.9%	31.0%	21.3%
文章の要約・翻訳	27.8%	33.3%	24.3%	28.7%	22.5%
マーケティング	27.4%	34.7%	24.3%	25.6%	22.5%
会議の効率化	27.0%	31.3%	21.5%	32.6%	20.0%
アプリケーション開発	26.8%	31.3%	18.8%	33.3%	22.5%
顧客サポート	25.4%	32.0%	20.8%	24.8%	22.5%
教育・ナレッジ管理	24.4%	31.3%	19.4%	21.7%	25.0%
アイディア創出	24.2%	29.3%	20.1%	27.1%	17.5%
プロジェクト管理	24.0%	27.9%	24.3%	22.5%	18.8%

注1：生成AIを「全社的に利用」と「特定部門で利用」の回答を対象としている
注2：効果の平均は従業員規模ごとに10個の業務の割合の平均値である

（参考）生成AIの導入形態と効果

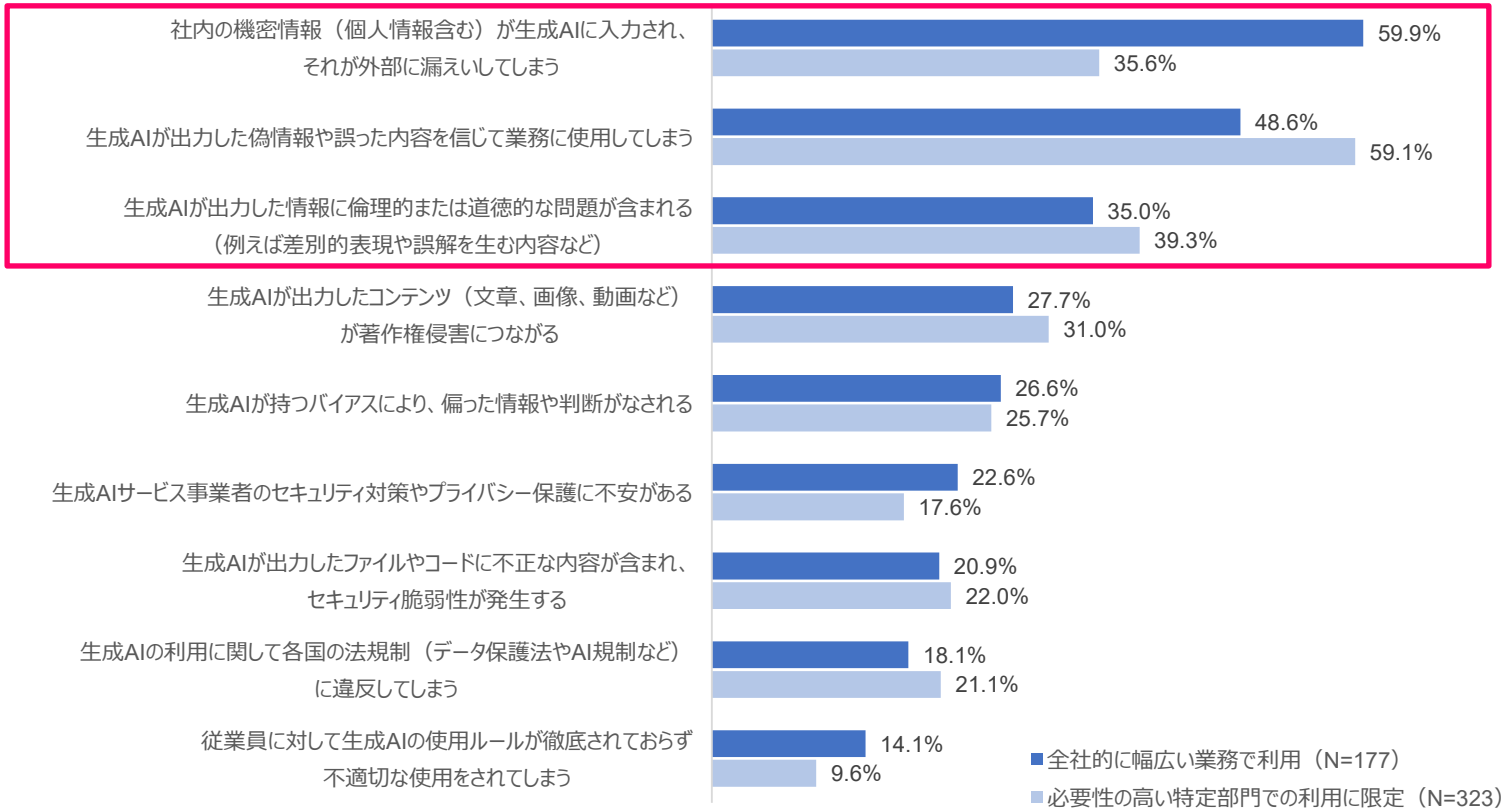
- ChatGPTのような生成AIサービスを利用することによって、短期間かつ低コストで業務の効率化や自動化の効果を出すことができるのが大きなメリットである。
- 他社と差別化を図るような効果、新たな製品やサービスを創出するような効果を出すためには、ファインチューニング（生成AIに追加学習を行う手法）やRAG（LLMに外部の情報ソースを与えてより精度の高い回答を生成させる手法）によるカスタマイズ、さらにはLLMの独自開発を行うという高度な実装を必要とする。

Use（利用）	• 生成AI機能が組み込まれた市販サービスを利用 • 多くの従業員が共通して行う汎用的なタスクに適用 • 情報収集、調査、文書・資料作成、汎用コンテンツ作成など
Build（構築）	• APIなどにより生成AI機能を組み込んだアプリケーションを作成して利用 • 特定の業務ワークフローに関わるタスクに適用 • 汎用チャットボット、ナレッジ検索、コード生成など
Custom（特製）	• 用途向けにLLMをカスタマイズしてアプリケーションに実装して利用 • RAG環境の構築やファインチューニングの実施 • 専門性が高く複雑な問題解決が求められるタスクに適用 • 専門チャットボット、高度な情報分析、専門分野のレポート作成など
Develop（開発）	• LLMを独自開発しアプリケーションに実装して利用 • 既存LLMが未学習の特殊用途や将来の革新につながるタスクに適用 • 新製品・サービス開発、研究開発、高度な意思決定など

出典：ITR

3.8　生成AIの利用におけるセキュリティ／プライバシー上の懸念点

- 全社利用企業では「社内の機密情報が生成AIに入力され、それが外部に漏えいする」が最も多い懸念点となった。特に全社利用では様々なリテラシーの従業員が利用するため、機密情報をプロンプトに入力してしまうことなどによる情報漏えいリスクへの懸念が大きくなっている。
- 特定部門利用企業では「生成AIが出力した偽情報や誤った内容を信じて業務に使用する」が最も多く、ハルシネーション（AIが事実に基づかない情報を生成する現象）に対する懸念が大きい。また、「生成AIが出力した情報に倫理的または道徳的な問題が含まれる」が続いている。AIガバナンスへの取り組みが強く求められる。



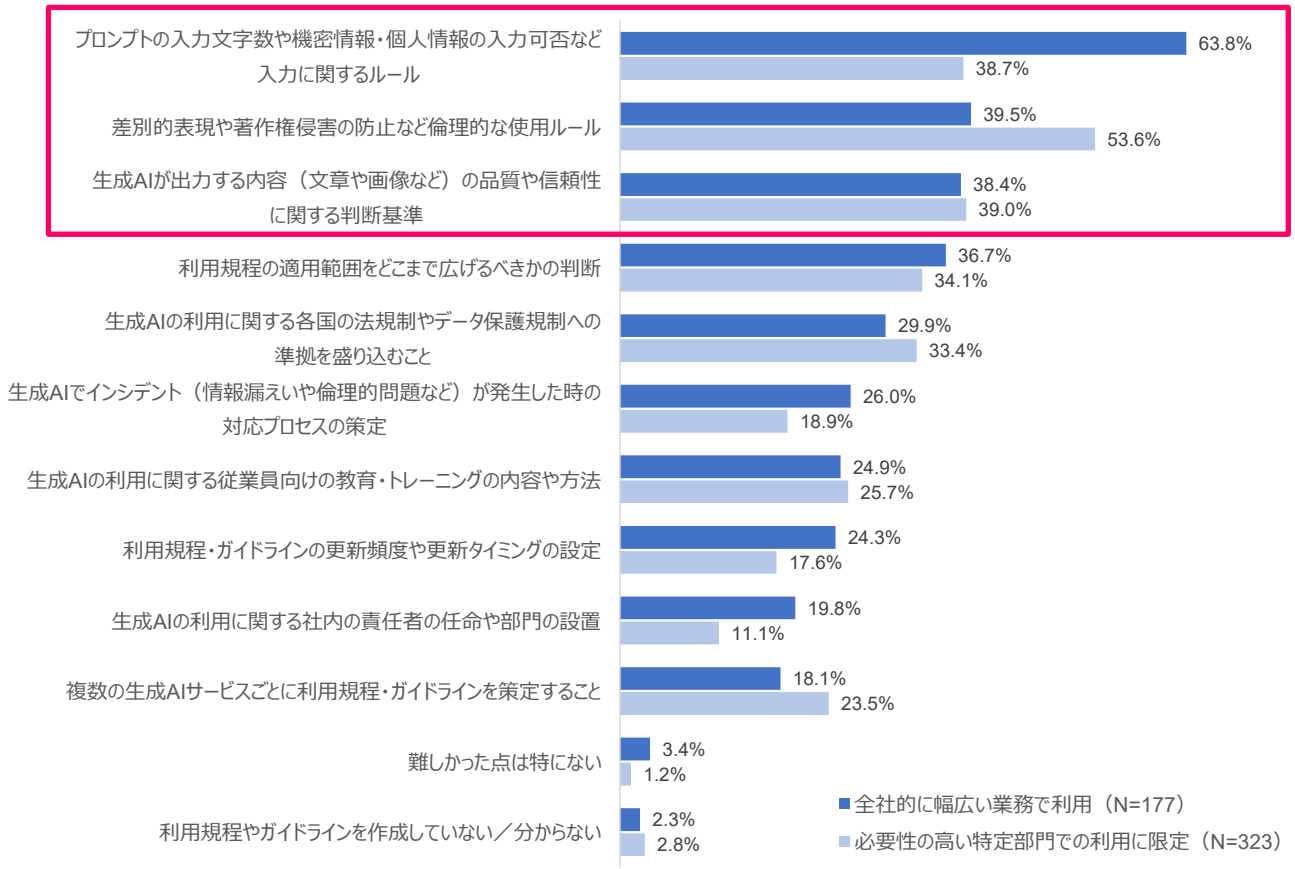
（参考）生成AI利用におけるリスクとその回避手段の例

リスク	回避手段の例
機密情報が学習対象となり情報が漏えい	• 機密情報や個人情報を入力禁止とするルールの策定・周知徹底 • 専用のプライベート生成AI環境の構築（機密データを扱う専用モデルを運用） • データ漏えい検知のためのログ監査・モニタリングの導入
生成された偽情報や誤った情報を業務で利用	• 学習データの鮮度維持・LLMの定期的なアップデート • AIの回答には参考情報や出典元を明示させ、利用者が検証できるようにする • 重要な判断にはAIだけでなく、必ず人間の確認プロセスを入れる
偏見や差別など不適切な回答を生成	• 不適切な表現を学習データから除外・再学習させる • 定期的な出力サンプルの評価とレビュー体制の整備 • 人間による適切なフィードバックを行い、継続的にモデルを調整
著作権侵害につながるコンテンツを生成	• 著作権上問題ない、クリアなデータセットのみで学習させる • AIの生成結果に対し、著作権チェックを行うルールを策定する • 著作権侵害検知ツール・サービスを利用する

出典：ITR

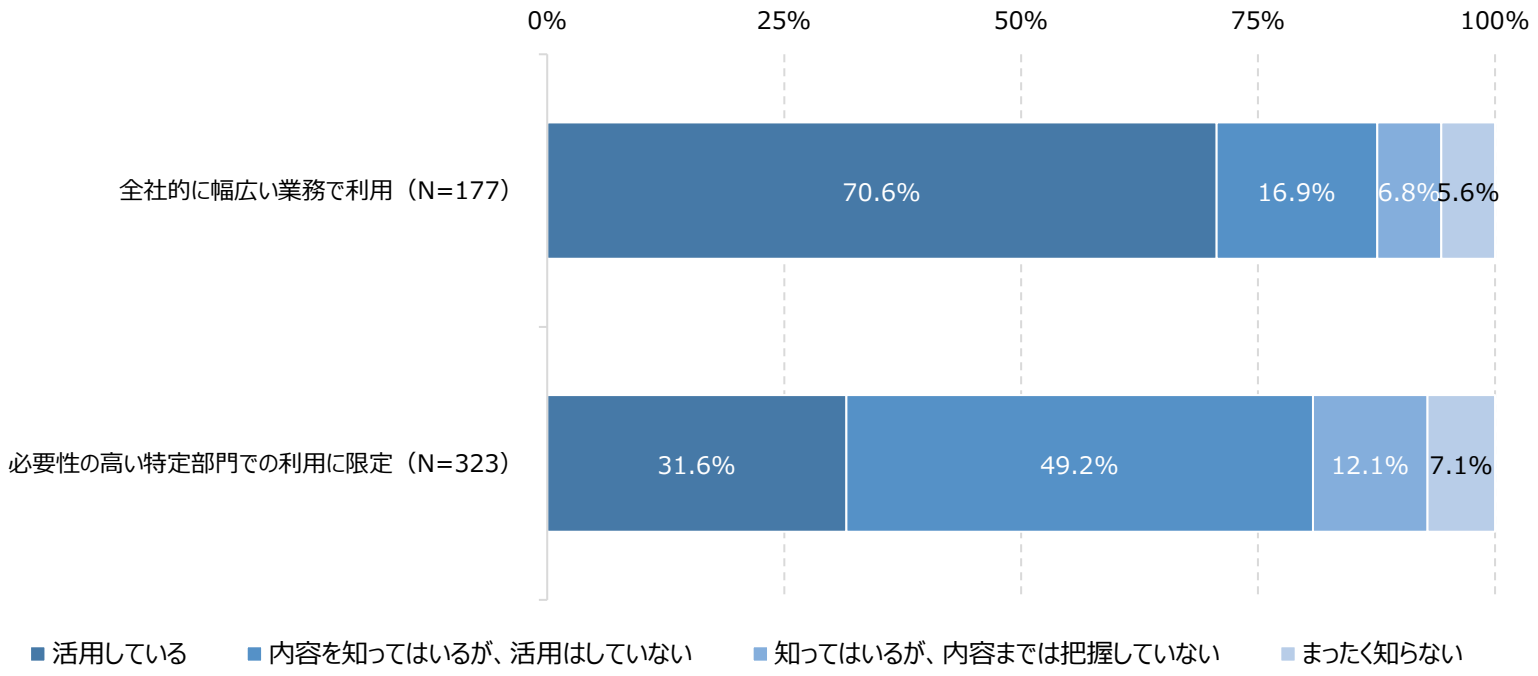
3.9　生成AIガイドラインの策定における難しさ

- 全社利用企業の60%以上が「プロンプトの入力文字数や機密情報・個人情報の入力可否などのルール」と回答しており、プロンプトの入力ルールを作成する難しさを感じている。全従業員が利用するとなるとスキルや知識に幅があるため、入力時の様々なリスクを想定した上での策定になる。
- 特定部門利用企業では「差別的表現や著作権侵害の防止など倫理的な使用ルール」が最も多い。
- 「生成AIが出力する内容の品質や信頼性に関する判断基準」も多く、ハルシネーションにどのように対応していくかもガイドラインを作成する上で課題となってくる。



3.10　AI事業者ガイドラインの活用状況

- 経済産業省と総務省は、 AIを活用する事業者が安全安心なAIの活用のための望ましい行動につながる指針として「AI事業者ガイドライン」を2024年4月に発表している。
- 全社利用企業の70.6%は既にAI事業者ガイドラインを活用し、AIを運用している。一方、特定部門利用企業では31.6%にとどまる結果となっている。



（参考）AIを活用する全ての人が守るべき10の原則：AI事業者ガイドラインより

1. 人間中心	AI システム・サービスの開発・提供・利用において、後述する各事項を含む全ての取り組むべき事項が導出される土台として、少なくとも憲法が保障する又は国際的に認められた人権を侵すことがないようにすべきである。また、AI が人々の能力を拡張し、多様な人々の多様な幸せ（well-being）の追求が可能となるように行動することが重要である。
2. 安全性	AI システム・サービスの開発・提供・利用を通じ、ステークホルダーの生命・身体・財産に危害を及ぼすことがないようにすべきである。加えて、精神及び環境に危害を及ぼすことがないようにすることが重要である。
3. 公平性	AI システム・サービスの開発・提供・利用において、特定の個人ないし集団への人種、性別、国籍、年齢、政治的信念、宗教等の多様な背景を理由とした不当で有害な偏見及び差別をなくすよう努めることが重要である。また、各主体は、それでも回避できないバイアスがあることを認識しつつ、この回避できないバイアスが人権及び多様な文化を尊重する観点から許容可能か評価した上で、AI システム・サービスの開発・提供・利用を行うことが重要である。
4. プライバシー保護	AI システム・サービスの開発・提供・利用において、その重要性に応じ、プライバシーを尊重し、保護することが重要である。その際、関係法令を遵守すべきである。
5. セキュリティ確保	AI システム・サービスの開発・提供・利用において、不正操作によって AI の振る舞いに意図せぬ変更又は停止が生じることのないように、セキュリティを確保することが重要である。
6. 透明性	AI システム・サービスの開発・提供・利用において、AI システム・サービスを活用する際の社会的文脈を踏まえ、AI システム・サービスの検証可能性を確保しながら、必要かつ技術的に可能な範囲で、ステークホルダーに対し合理的な範囲で情報を提供することが重要である。
7. アカウンタビリティ	AI システム・サービスの開発・提供・利用において、トレーサビリティの確保、「共通の指針」の対応状況等について、ステークホルダーに対して、各主体の役割及び開発・提供・利用する AI システム・サービスのもたらすリスクの程度を踏まえ、合理的な範囲でアカウンタビリティを果たすことが重要である。
8. 教育・リテラシー	主体内の AI に関わる者が、AI の正しい理解及び社会的に正しい利用ができる知識・リテラシー・倫理感を持つために、必要な教育を行うことが期待される。また、各主体は、AI の複雑性、誤情報といった特性及び意図的な悪用の可能性もあることを勘案して、ステークホルダーに対しても教育を行うことが期待される。
9.公正競争確保	AI を活用した新たなビジネス・サービスが創出され、持続的な経済成長の維持及び社会課題の解決策の提示がなされるよう、AI をめぐる公正な競争環境の維持に努めることが期待される。
10. イノベーション	社会全体のイノベーションの促進に貢献するよう努めることが期待される。

出典：経済産業省／総務省『AI事業者ガイドライン（第1.0版）』

3.11　生成AIの活用状況と課題：調査結果からの考察

- 約半数近い企業が生成AIを業務で利用しており、試験利用フェーズにある企業も多いことから、大部分の企業で利用が進むことが予想される。5,000人以上の大手企業では、既に半数近くが全社利用しているが、中堅・中小企業ではそこまでになっていないことから、生成AI利用の格差が生じてくる可能性も考えられる。

- 生成AIの活用効果は高く、電子メールや資料作成などの日常業務では既に約80%で効果が出ている。その他、分析・レポート作成や文章の要約・翻訳などでも効果が出ており、生成AIの強みである文章生成を伴う業務での効果が高いことがわかる。

- DX定着企業では、マーケティングや顧客サポート、アイディア創出など、顧客体験や製品・サービス企画での活用効果が高くなっている。社内業務の効率化にとどまらず、ビジネスの成長や新たな創出に向けた活用が拡大することを期待したい。

- 生成AI利用における大きな課題は、情報漏えいとハルシネーションのリスクを如何に回避するかにある。これは利用する従業員が多くなればなるほど、高いリスクを伴う。生成AIの活用推進と併せて、ガイドラインの策定も進めることが重要となる。その際、「AI事業者ガイドライン」や他社が公開しているガイドラインなどの外部資料を参照することを推奨する。

報告する調査項目

1. 経営課題とDX実践状況

2. 電子契約の利用状況

3. 生成AIの活用状況と課題

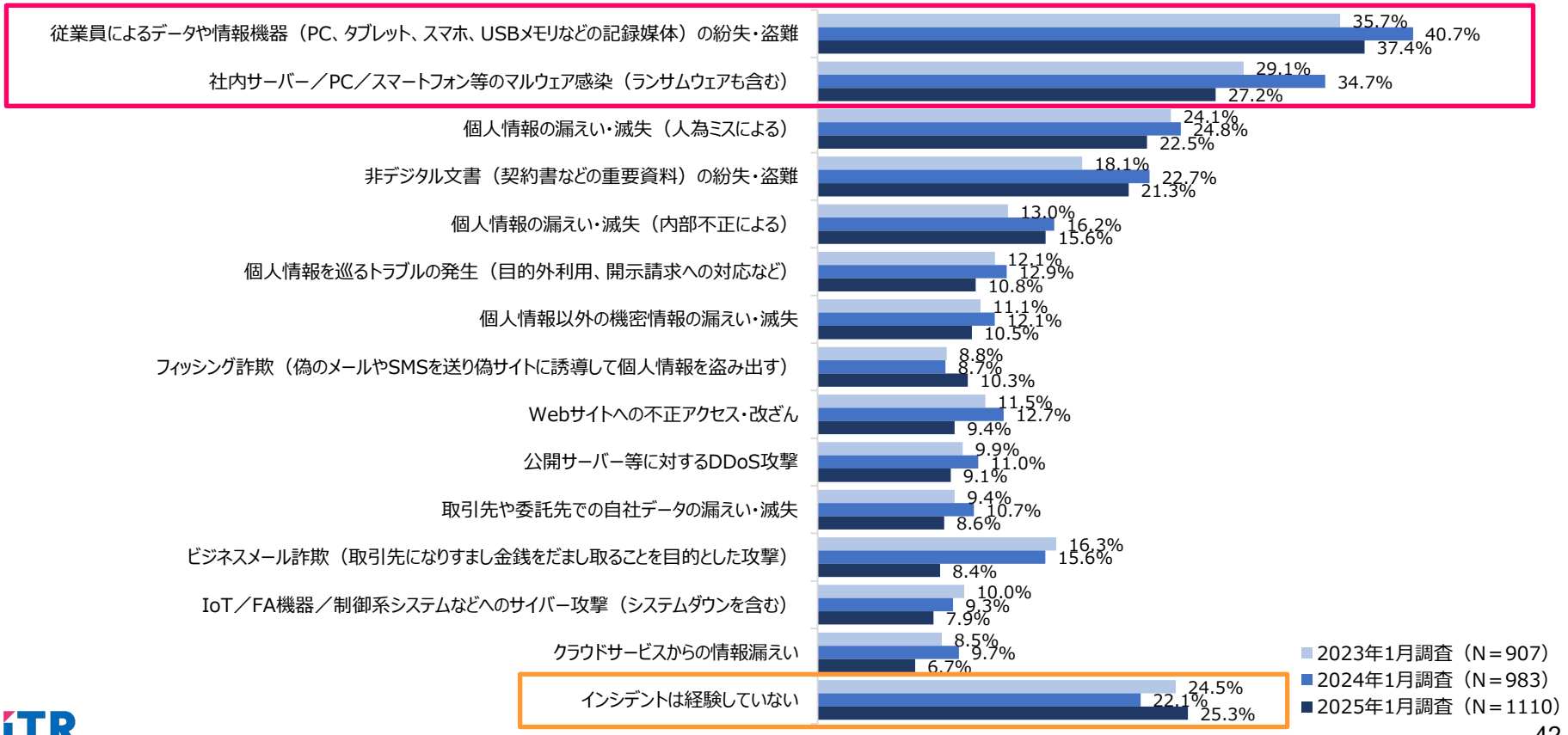
4. ランサムウェアとセキュリティ対策の実態

5. プライバシー保護に対する取り組み状況

6. 第三者認定／認証制度の取得状況

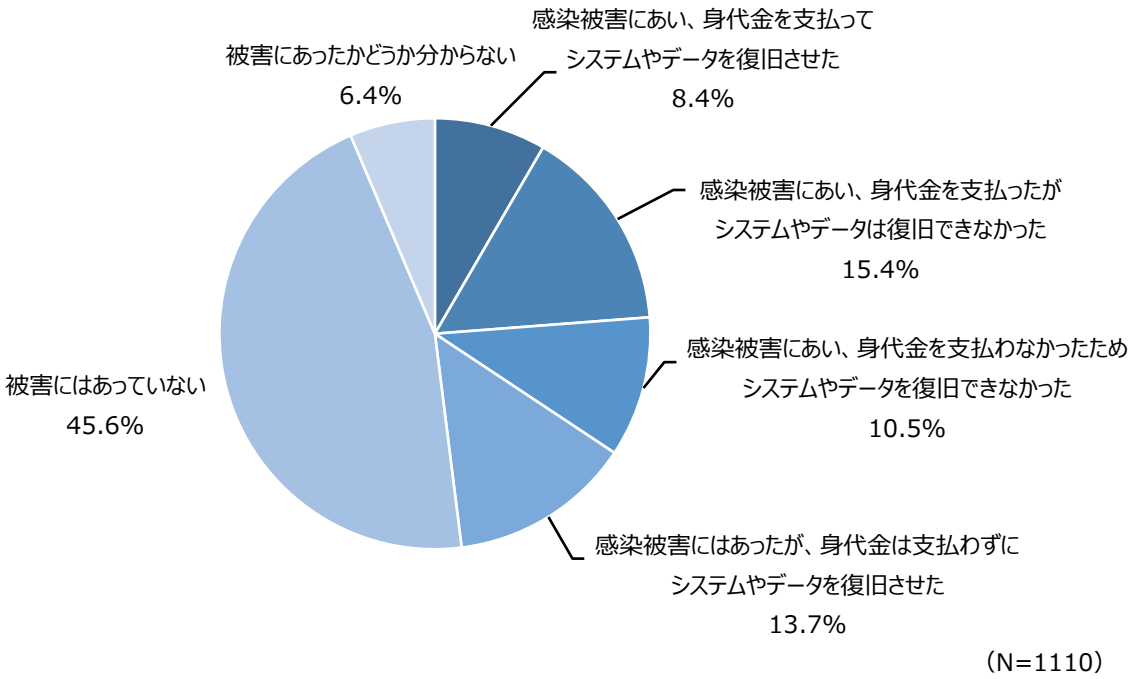
4.1　過去1年間のセキュリティ・インシデントの発生状況

- 「従業員によるデータや情報機器の紛失・盗難」が最も多い。2024年調査からはやや減少しているが、2023年調査よりは多い状況にある。
- 「マルウェア感染」は前回調査から大きく減少している。ランサムウェアへの注意喚起がなされていることもあり、適切な対策が実施されていることが寄与している可能性も考えられる。
- また、「インシデントは経験していない」が2024年調査から増加していることからも、直近1年間でのセキュリティ対策が強化された結果とみてとれる。



4.2　ランサムウェアの感染被害の経験

- ランサムウェアの感染被害を経験した企業は48.0%となり、約半数が感染を経験している。
- 身代金を支払った企業は23.8%となり、未払い（24.2%）とほぼ変わらず、約半数は支払っている。
- システムやデータを復旧できなかった企業は25.9%となり、半数以上が復旧できていない。ランサムウェアに感染してしまうと、システムの復旧が難しいことが分かる。



（N=1110）

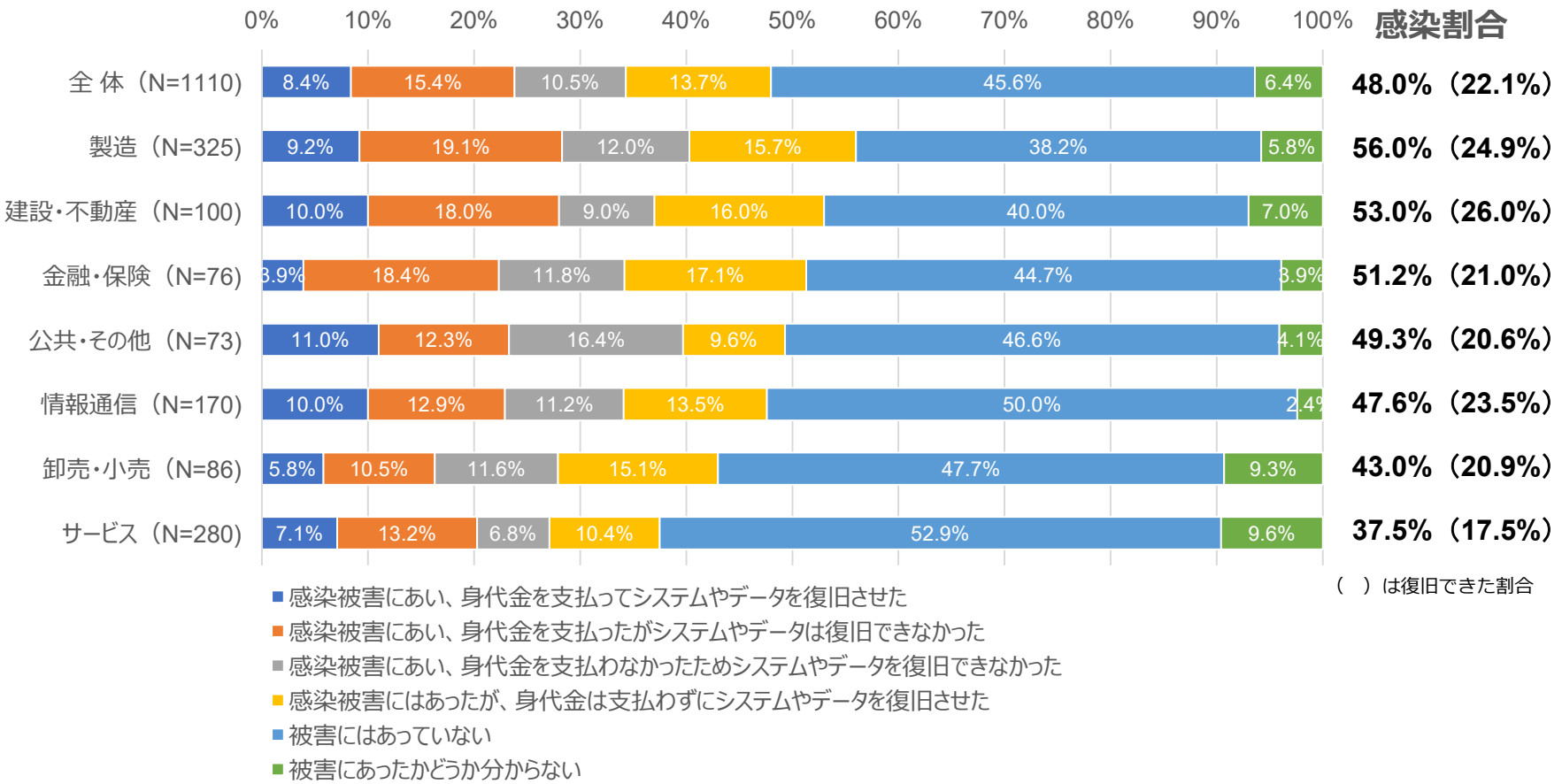
感染割合　：48.0%

身代金
　支払った：23.8%
　未払い　：24.2%

復旧
　成功　　：22.1%
　失敗　　：25.9%

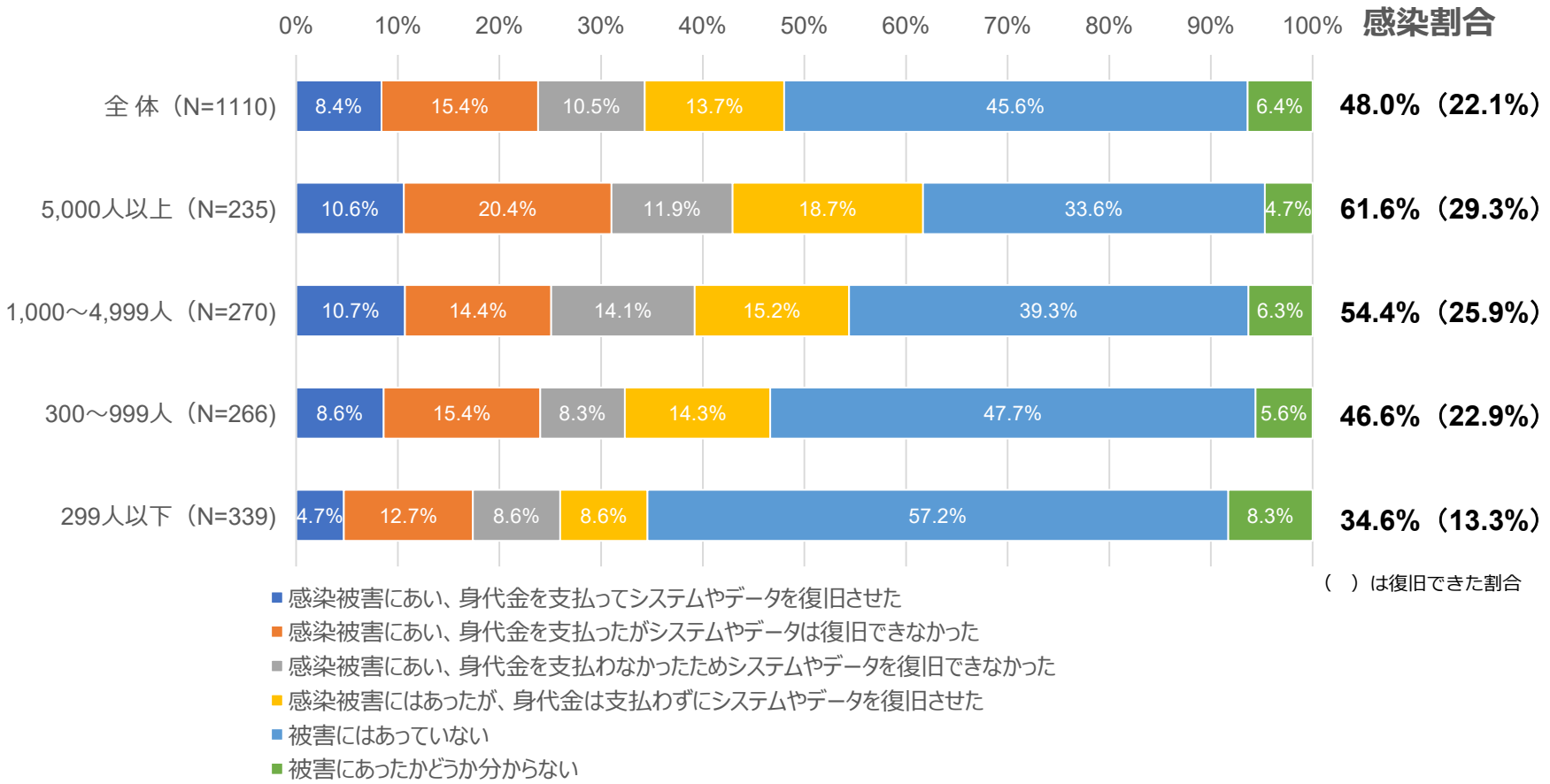
4.3　ランサムウェアの感染被害の経験：業種別

- 最も感染割合が高いのは「製造」で56.0%、その次に「建設・不動産」と「金融・保険」が続き、いずれも50%以上の感染割合となっている。いずれも復旧できた割合は半分に満たない。
- 最も感染割合が低いのは「サービス」で37.5%となった。それでも3分の1以上は感染経験がある。どの業種においても、ランサムウェア攻撃を受ける可能性は十分にある。



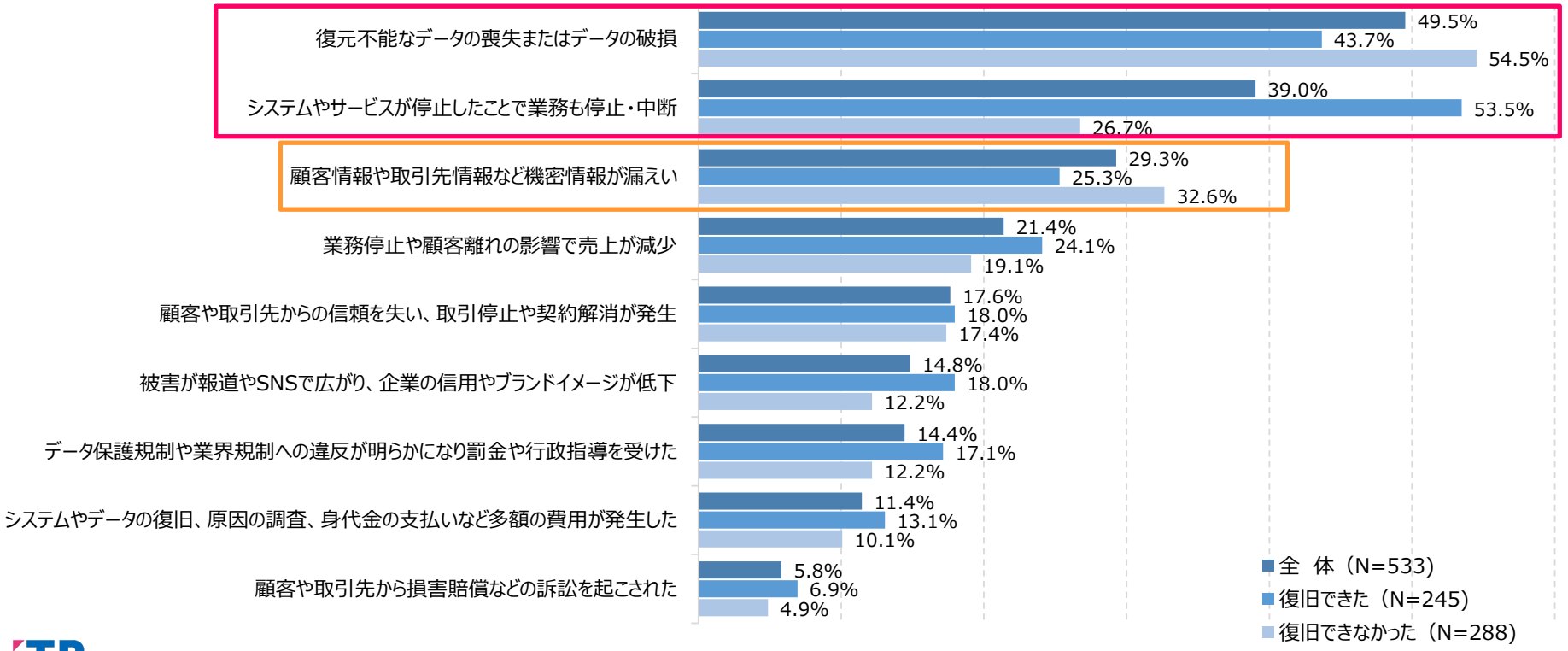
4.4　ランサムウェアの感染被害の経験：従業員規模別

- 従業員規模が大きくなるにしたがい感染割合が高まる傾向がある。「5,000人以上」では61.6%、「1,000人～4,999人」では54.4%と感染割合が50%以上となっている。
- 「299人以下」でも3分の1の企業で感染を経験しており、企業規模に依らずランサムウェア攻撃を受ける可能性は十分にある。「中小企業だから狙われないだろう」という先入観を持ってはならない。



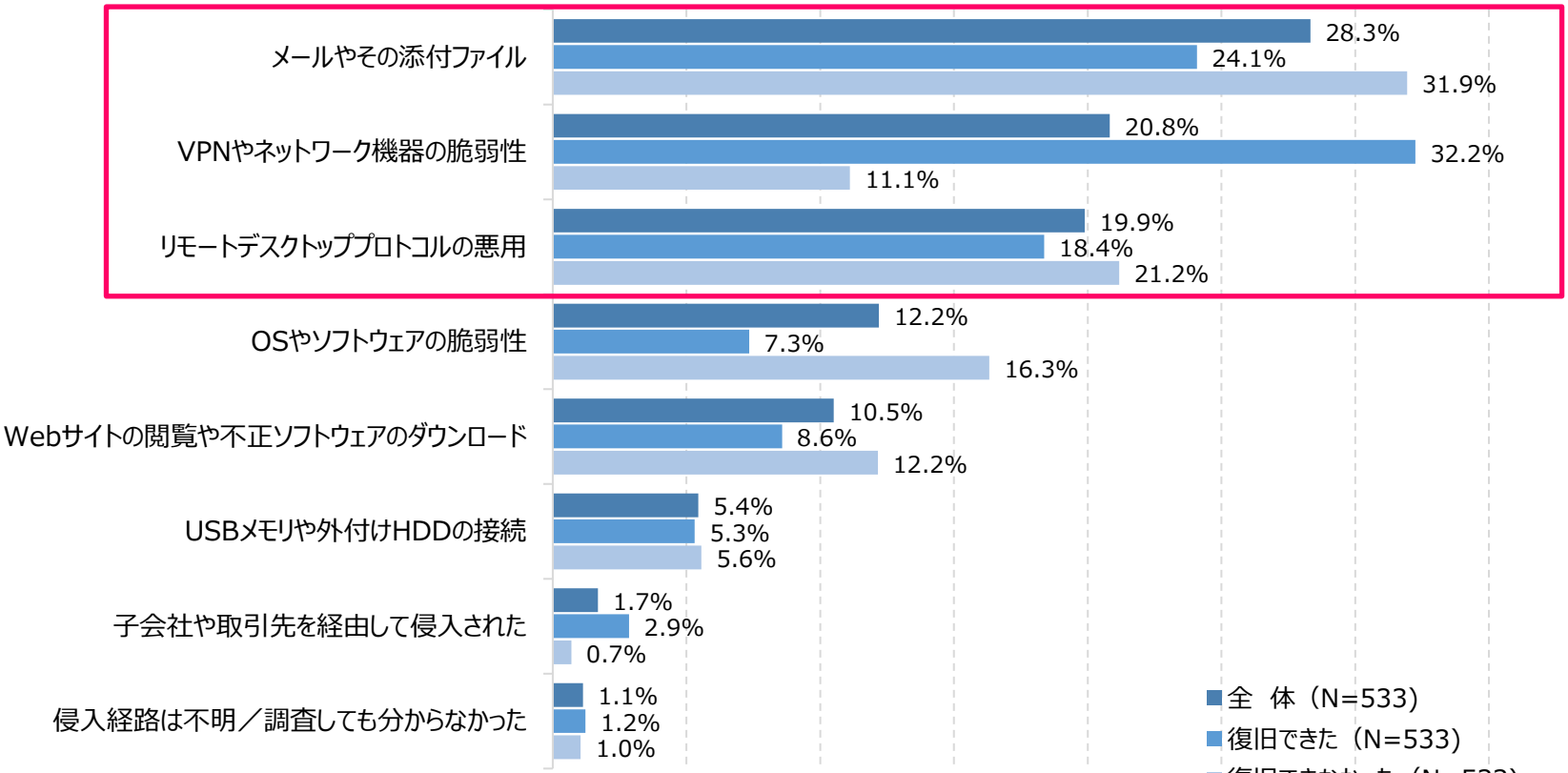
4.5　ランサムウェア感染被害の影響

- ランサムウェアに感染した結果、「復元不能なデータの喪失またはデータの破損」と「システムやサービスが停止したことで業務も停止・中断」を中心に影響が出ている。特に復旧できなかった企業は、データが暗号化されて開けなくなるなどの損害が出ている。
- 影響はシステムの停止やデータの喪失だけではなく「顧客情報や取引先情報など機密情報が漏えい」の被害も受けている企業が約3割出ている。攻撃者がデータを抜き取り、顧客情報などの機密情報をダークサイトで公開することを強迫してくる攻撃者が増加傾向にある。これによって、顧客や取引先からの信頼を失い、顧客離れや売上減少にもつながっていく恐れがあるため、非常に悪質な攻撃と言える。



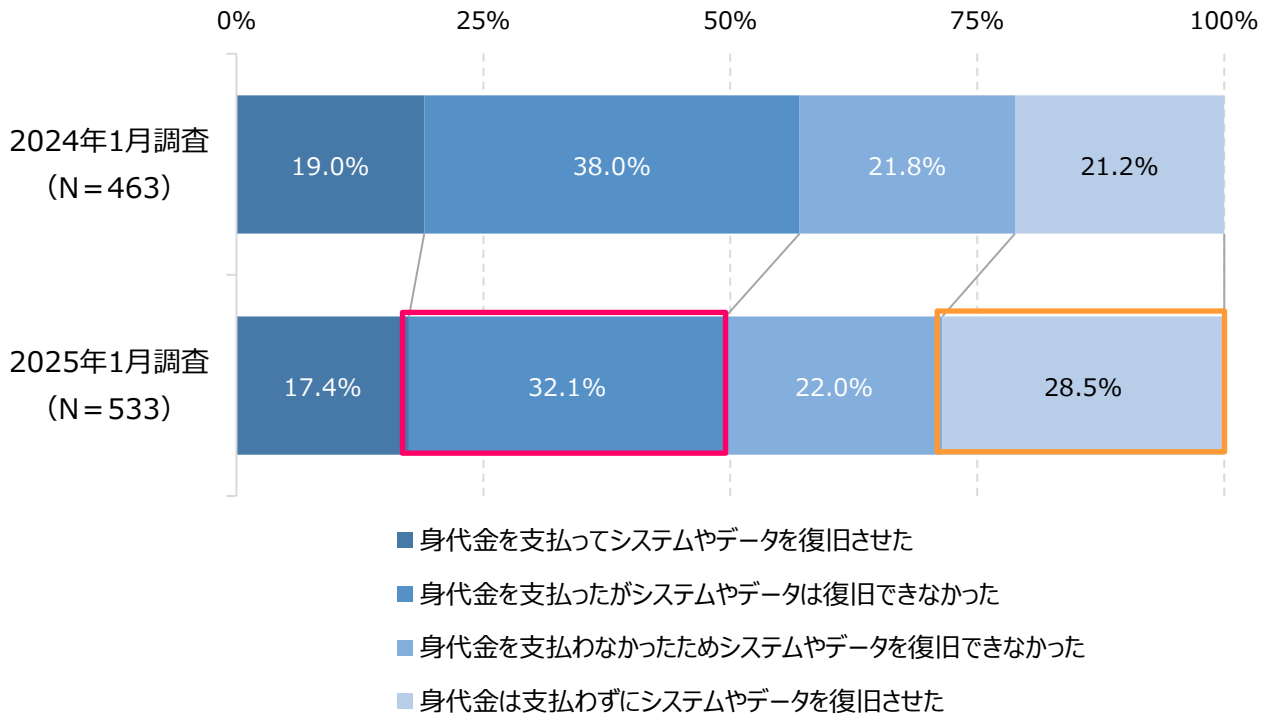
4.6　ランサムウェアの感染経路

- ランサムウェアの主な感染経路のひとつに「メールやその添付ファイル」がある。依然としてメールを利用した攻撃は続いている。特に復旧できなかった企業で多い傾向があり、感染の根本原因の特定が難しい。 ばらまきメールやフィッシングメールなど攻撃が多様化しており、注意が必要である。
- もうひとつの主な感染経路として、 「VPNやネットワーク機器の脆弱性」と「リモートデスクトッププロトコルの悪用」がある。これらは、テレワークなどにおけるリモートアクセス環境の脆弱性が狙われている事例が多い。比較的復旧できた企業に多い傾向があり、侵入起点が明確であり、感染の根本原因が特定しやすいことが想定される。



4.7　ランサムウェア感染での身代金と復旧の状況

- ランサムウェア感染経験のある企業における、身代金の支払いとシステム・データの復旧結果について、2024年調査と2025年調査を比較している。
- 身代金を支払った企業は57.0%（2024年調査）から49.5%（2025年調査）に下がっている。2025年調査では、支払ったが復旧できなかった企業の割合が大きく減少している。
- 復旧に成功した企業は40.2%（2024年調査）から46.0%（2025年調査）に上昇している。2025年調査では、支払わずに復旧できた企業の割合が大きく上昇している。感染後の復旧対応を適切に行っている企業が増えている傾向にある。

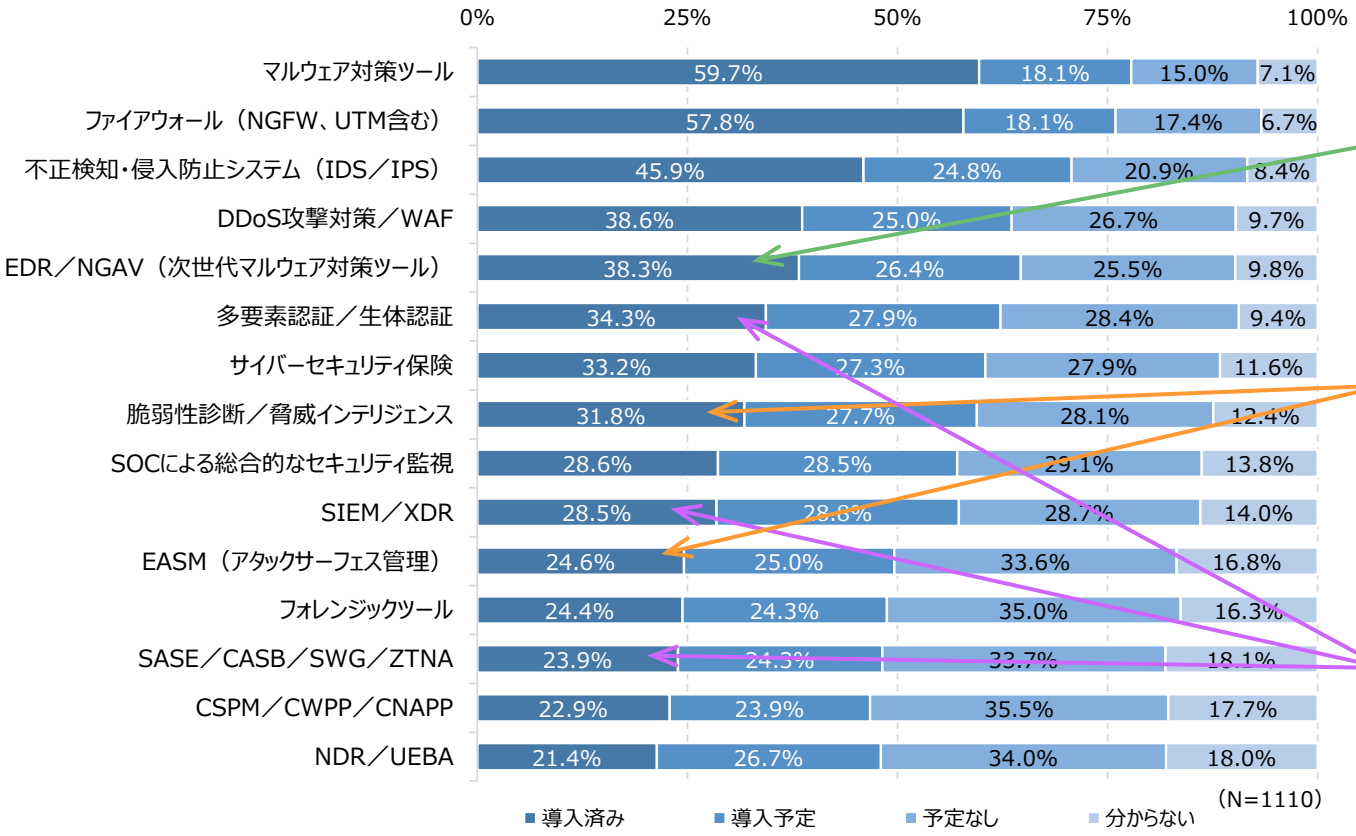


身代金支払い率
2024年調査：57.0%
2025年調査：49.5%

復旧成功率
2024年調査：40.2%
2025年調査：46.0%

4.8　外部からのサイバー攻撃対策として導入しているツール・サービス

- 現状では「マルウェア対策ツール」、「ファイアウォール」、「IDS/IPS」のような従来型のセキュリティ対策ツールの導入が多いが、「EDR／NGAV」のような次世代型ツールの導入も進んでいる。
- ランサムウェアは脆弱性を狙った攻撃が多いため、「脆弱性診断／脅威インテリジェンス」や「 EASM（アタックサーフェス管理）」によって脆弱性を診断・管理することが求められる。
- セキュリティ対策の考え方が、境界防御型からゼロトラスト型へ移行しており、これから「多要素認証／生体認証」「SIEM／XDR」「 SASE／CASB／SWG／ZTNA」の導入が見込まれる。



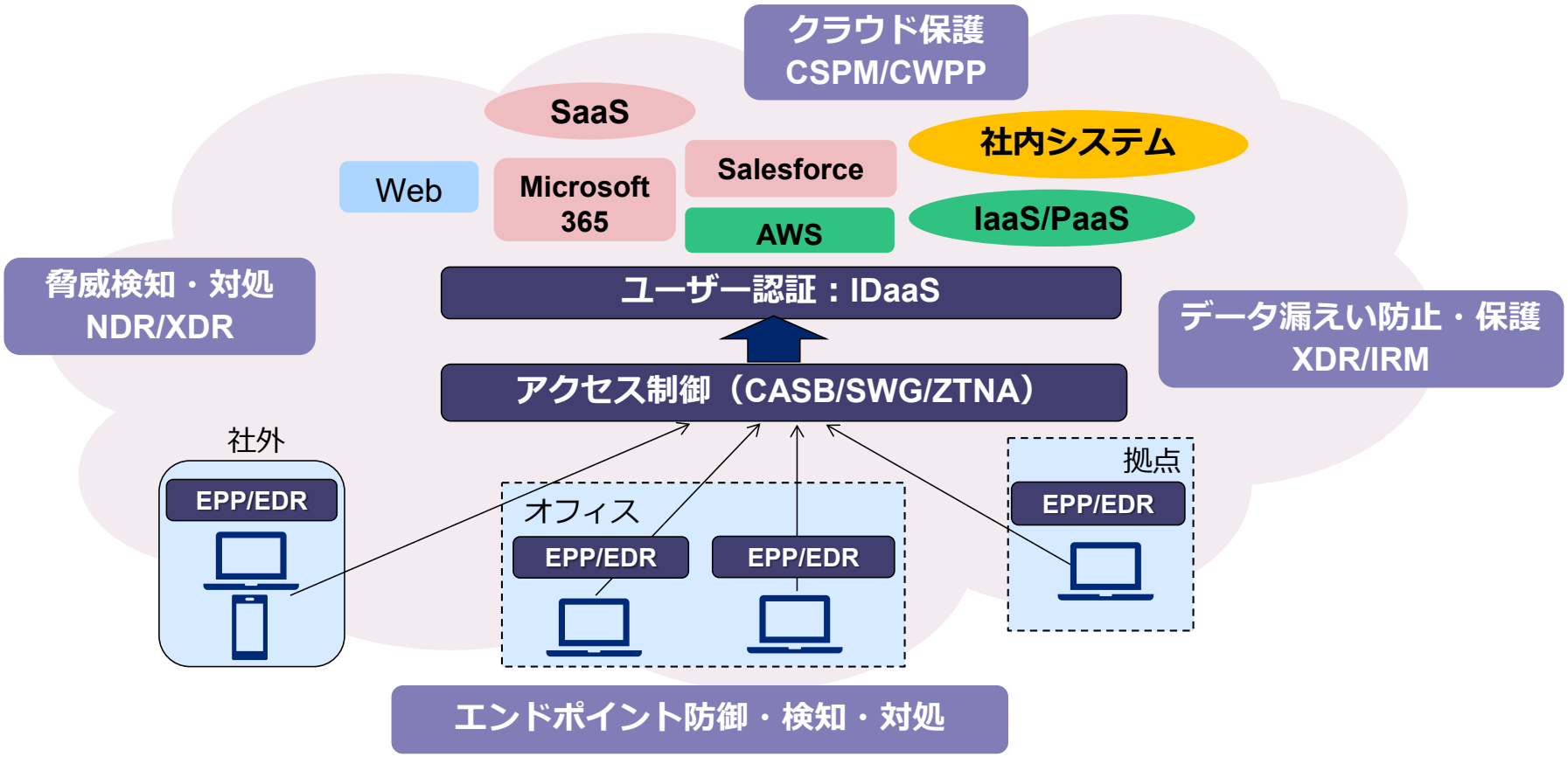
ランサムウェアや未知のマルウェア対策として侵入検知や振る舞い検知が可能なEDRやNGAVの導入が進んでいる

IT環境の脆弱性を診断し、攻撃対象になる可能性の高いIT資産や設定を特定して、未然に対応を図っていく

次世代セキュリティモデルであるゼロトラストを構成するために多要素認証、SASE、XDRなどが不可欠

（参考）ゼロトラストセキュリティのアーキテクチャ

- ネットワークの内部と外部を区別することなく守るべき資産にアクセスするものは全て信用しないという前提で監視と認証を行い、さらに不正な振る舞いを検知することで脅威を防ぐ

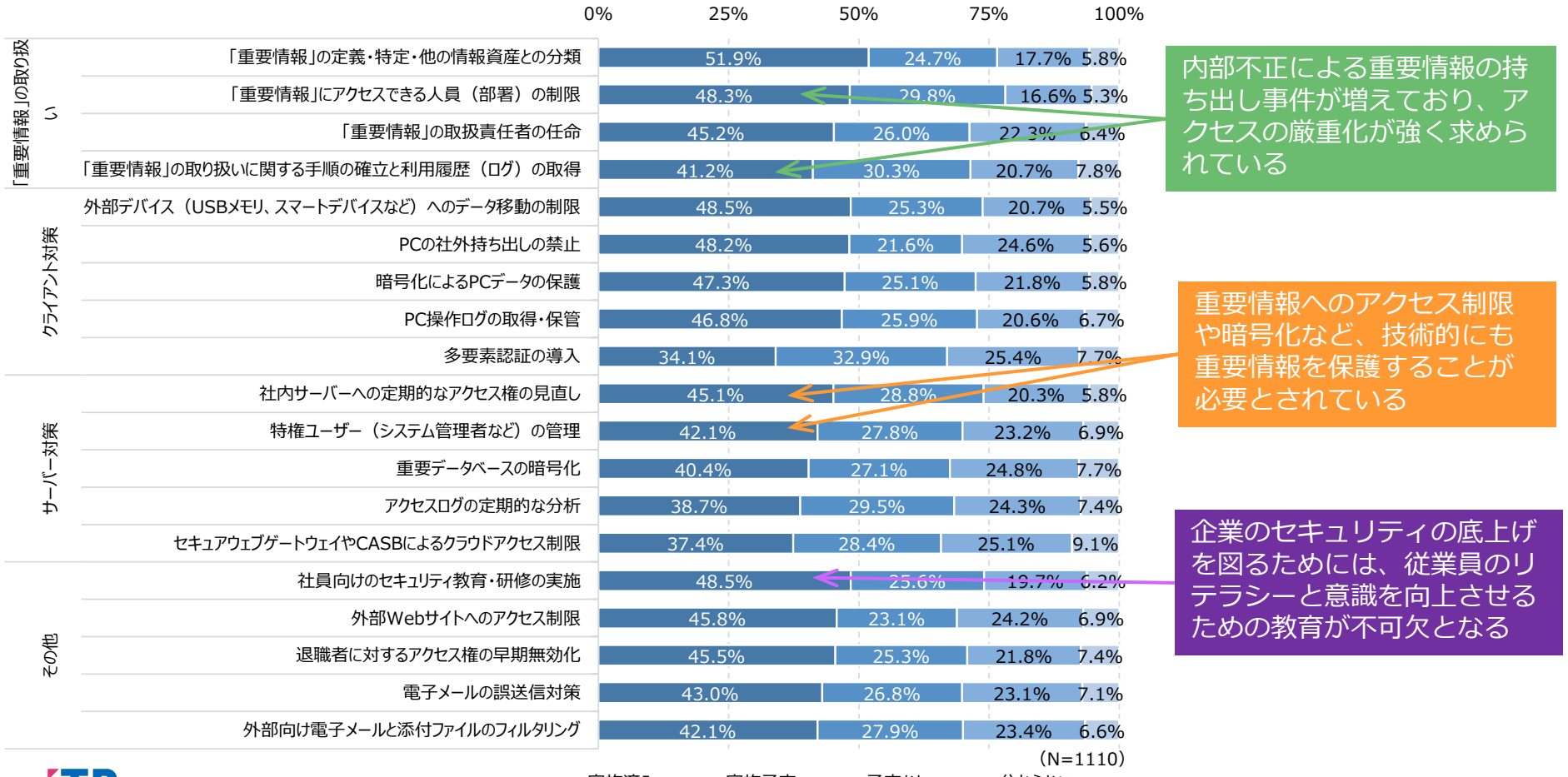


（参考）主なゼロトラストセキュリティ関連ソリューション

EDR	EDR（Endpoint Detection and Response）。マルウェアの感染、サイバー攻撃によるインシデント後の迅速な対応を行うことを目的とし、エンドポイントのアクティビティ情報（振る舞いやリスクの高い動作など）を収集し、データを活用した機械学習やAIなどによるマルウェアやサイバー攻撃の検知を行い、対処や回復を行う
SIEM	SIEM（Security Information and Event Management）。各種ログを一元的に収集・管理する統合ログ管理の機能に加え、相関分析機能などにより、あらかじめ定めたポリシーに従って脅威を検出し、自動的にアラートを出す
XDR	XDR（Extended Detection and Response）。エンドポイントやネットワーク、クラウドなど複数の場所に分散するログを一元的に監視することで、複数の領域に渡ってインシデントやエラーの検知、調査、対応などを自動化する
NGAV	NGAV（Next Generation Anti-Virus）。機械学習やAI、振る舞い検知などの技術を活用し、シグネチャ、パターンマッチングでは検知できない未知の脅威の検知・防御だけではなく、ダメージコントロールなどの脅威への対処・回復といったEDR機能をシングルエージェント、単一管理コンソールで提供する製品
SASE	SASE（Secure Access service Edge）。ネットワークの機能とセキュリティの機能を1つのクラウドサービスに統合させるという新たなセキュリティフレームワークに基づいた考え方・概念。CASB、WSG、ZTNA、SD-WANなどから構成される
CASB	CASB（Cloud Access Security Broker）企業が利用するクラウドサービスに対し、認証やアクセスコントロール、クラウドおよび外部ストレージのデータ保護や暗号化、シャドーITの防止と可視化、モニタリングやサンクションITの保護などを行い、利用企業のセキュリティポリシーの適用を実現させるクラウドに特化したセキュリティソリューション
WSG	WSG（Web Secure Gateway）ユーザーが社外ネットワークへのアクセスを安全に行うために、不正アクセスやウイルスの検知と除去を行う。さらに、URLフィルタリングやWeb トラフィックを監視し、悪意のあるサイトやコンテンツへのアクセスをブロックする
ZTNA	ZTNA（Zero Trust Network Access）。特定のデータやアプリケーションへのアクセスを許可するソリューションであり、ユーザーがアクセスを行う度にID、アクセス権限、端末などを検証し、都度、認証を行い、事前に定義されたポリシーに基づいたアクセス制御を行う
CSPM／CWPP／CNAPP	CNAPP（Cloud Native Application Protection Platform）は、クラウドアプリケーションのセキュリティを確保するためのフレームワーク。クラウドの設定やクラウドの利用状況などを監視するCSPM（Cloud Security Posture Management）、クラウドワークロード（クラウド上のサーバ、アプリケーション、仮想マシンなど）の監視と保護を行うCWPP（Cloud Workload Protection Platform）、コンテナセキュリティなどのクラウドセキュリティ機能を統合した包括的なソリューション
NDR	NDR（Network Detection and Response）。網羅的にネットワーク全体を可視化し、ネットワーク上のさまざまなログを収集・分析することで、不審なトラフィックを見つけ出し、既知、未知の脅威を検知する。そして、ネットワーク状況をリアルタイムに把握し、リアルタイムでの対処を可能にする製品・サービス
UEBA	UEBA（User and Entity Behavior Analytics）。AI、機械学習、ディープラーニングなどを用いて、ネットワーク内のユーザーやシステムの振る舞いを分析し、疑わしい行動、異常行動、異常なトラフィック、未知のマルウェアなどを検知し、セキュリティ上どのような影響をもたらすかを判断する製品・サービス

4.9　内部からの情報漏えい対策として実施している項目

- 「重要情報」の取り扱いでは「手順の確立とログの取得」の実施予定とする企業が30%以上と高い。
- クライアント対策の中では「多要素認証の導入」の実施率が最も低いが、実施予定とする企業の割合が最も高いため、今後の導入拡大が期待される。
- 「社員向けセキュリティ教育の実施」は半数以下となり、セキュリティ意識の甘さが露呈している。



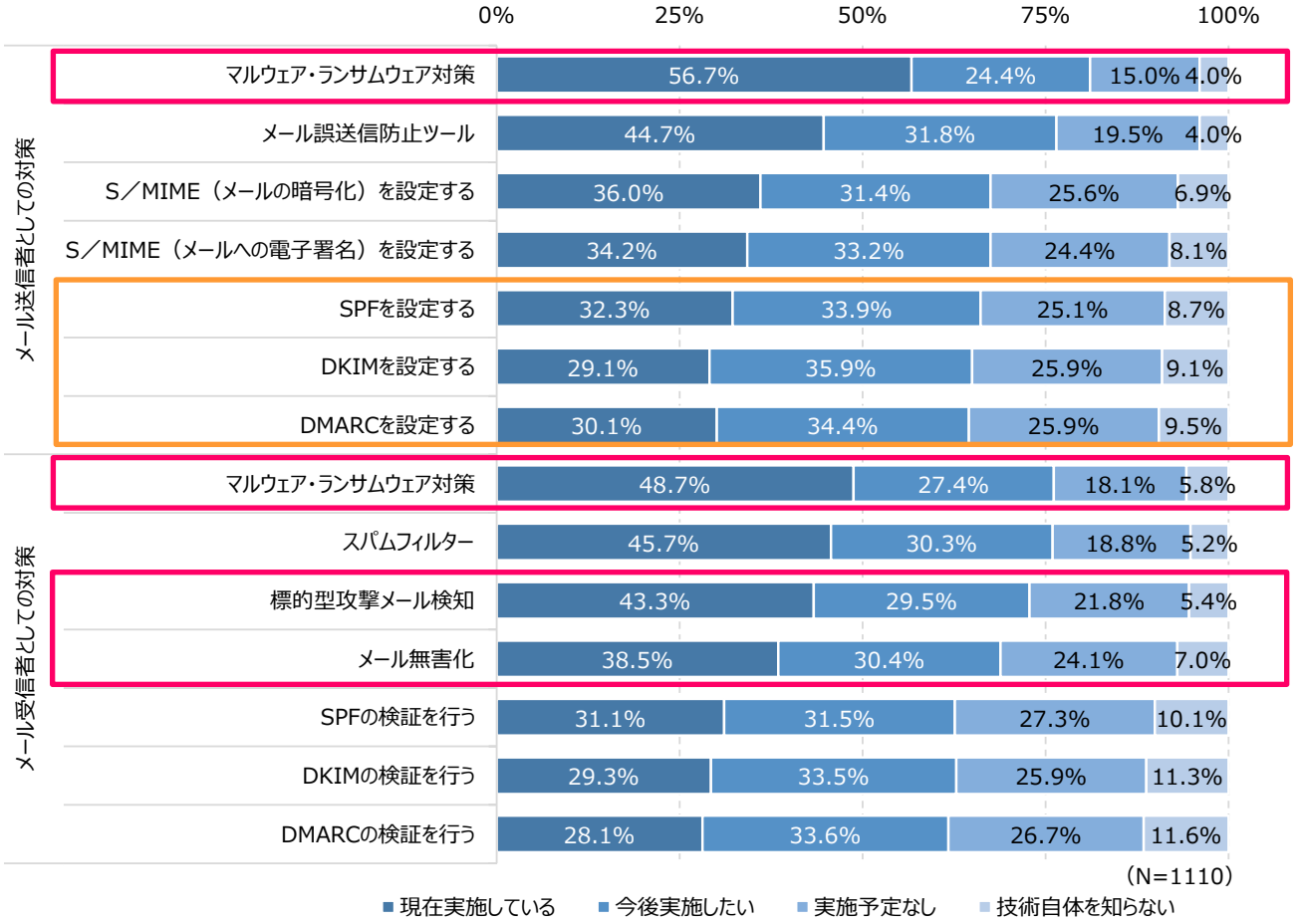
内部不正による重要情報の持ち出し事件が増えており、アクセスの厳重化が強く求められている

重要情報へのアクセス制限や暗号化など、技術的にも重要情報を保護することが必要とされている

企業のセキュリティの底上げを図るためには、従業員のリテラシーと意識を向上させるための教育が不可欠となる

4.10　電子メールのセキュリティ対策として実施している項目

- 電子メールからのランサムウェア攻撃対策としては、「マルウェア・ランサムウェア対策」「標的型攻撃メール検知」「メール無害化」が挙げられるが、より高い実施率が求められる。
- なりすましメール対策として期待されているメール認証の仕組みである「SPF／DKIM／DMARC」は30%程度の実施率にとどまっているが、今後実施したい割合が30%以上あり、これから対策が進んでいくことが期待される。



4.11　ランサムウェアとセキュリティ対策の実態：調査結果からの考察

- ランサムウェアは業種、企業規模問わず、どの企業でも攻撃される可能性が十分にあると考えるべきである。感染すると復旧成功率は50%にも満たない状況にあり、業務やシステム、データに大きな影響が出ることを覚悟しなくてはならない。

- データの暗号化による身代金要求に加え、窃取した機密情報の公開や顧客への脅迫を迫る多重脅迫型のランサムウェアが増加している。調査結果からも情報漏えいやそれによる顧客離れや企業の信頼性の失墜などの影響もみられる。サイバー攻撃は巧妙化が進んでいるため、継続して常に最新の対策とそれに向けた投資を行う必要がある。

- ランサムウェア対策として、電子メールからの攻撃やリモートアクセス環境の脆弱性を悪用した攻撃に対する対策は不可欠である。脆弱性の診断・管理、電子メールセキュリティ、ゼロトラスト・セキュリティの導入が求められる。

- セキュリティ対策は、ツールや技術などのハード面だけではなく、手順やルール、体制などソフト面の対策と強化も必要である。それとあわせて従業員のセキュリティに関するリテラシーや意識の向上を図り、組織全体のセキュリティの底上げを行っていくことが重要である。

（参考）ランサムウェア対策としてのバックアップの重要性

- ランサムウェアを完全に防御できる保証はない。感染した時にバックアップデータが残っていれば復旧はできるが、バックアップデータまで感染し暗号化されるケースが増えている。
- バックアップデータをランサムウェアから保護するために、バックアップの基本原則である「3-2-1ルール」徹底の重要性が高まっている。

3 バックアップデータを3つ作成
1つのデータが暗号化されても他のデータで復元

2 2つの異なるメディアで保存
特定のデバイスが感染しても他のメディアのデータで復元

1 1つはオフサイト（遠隔地）で保存
ネットワーク全体が感染しても隔離されたサイトのデータで復元

＋

1 1つは不変ストレージで保存
データの改変、削除、暗号化を防止するストレージで対策

NASや外付けHDD

クラウドストレージ

テープストレージ

不変ストレージ
（イミュータブルストレージ）

報告する調査項目

1. 経営課題とDX実践状況

2. 電子契約の利用状況

3. 生成AIの活用状況と課題

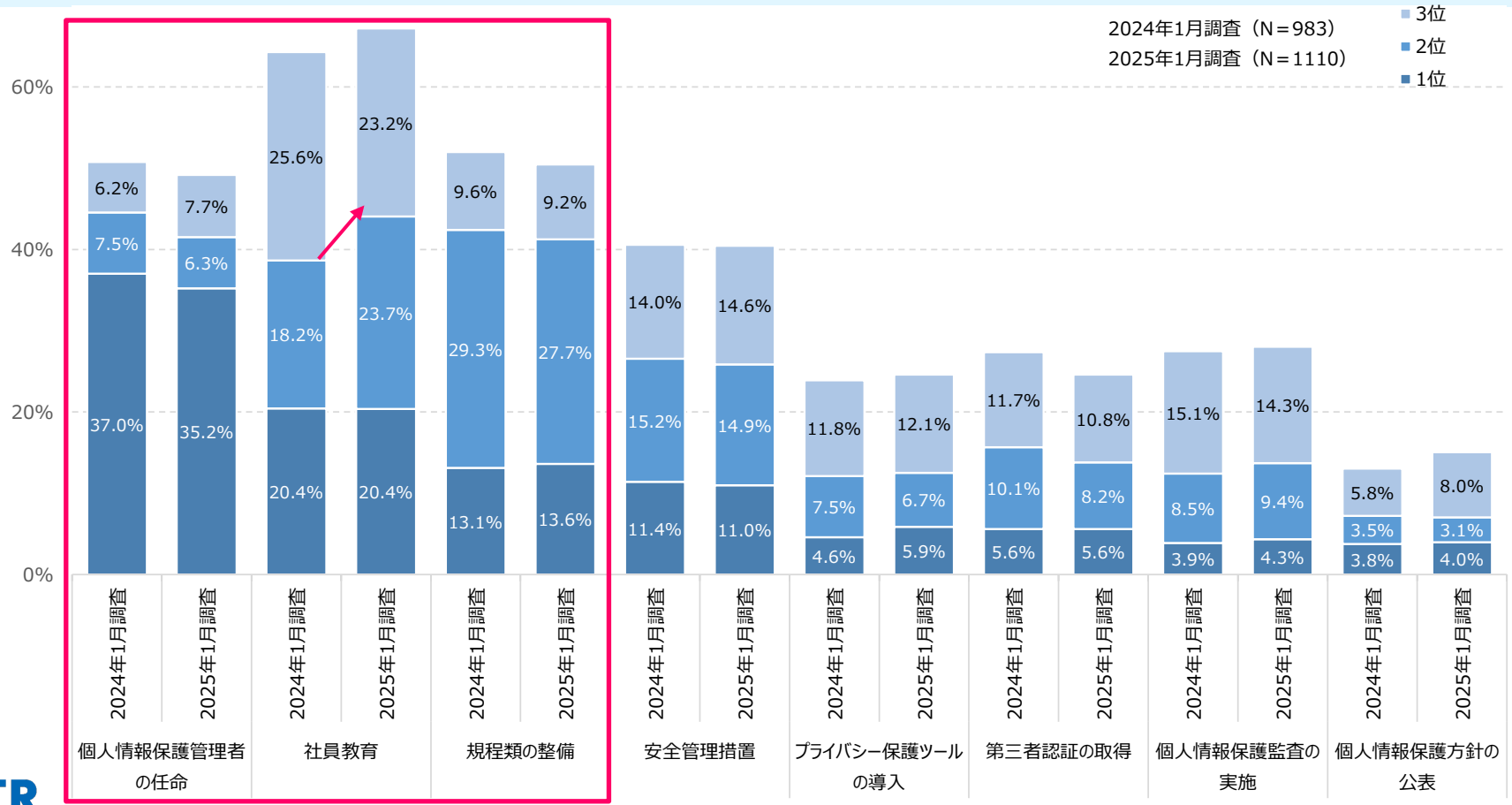
4. ランサムウェアとセキュリティ対策の実態

5. プライバシー保護に対する取り組み状況

6. 第三者認定／認証制度の取得状況

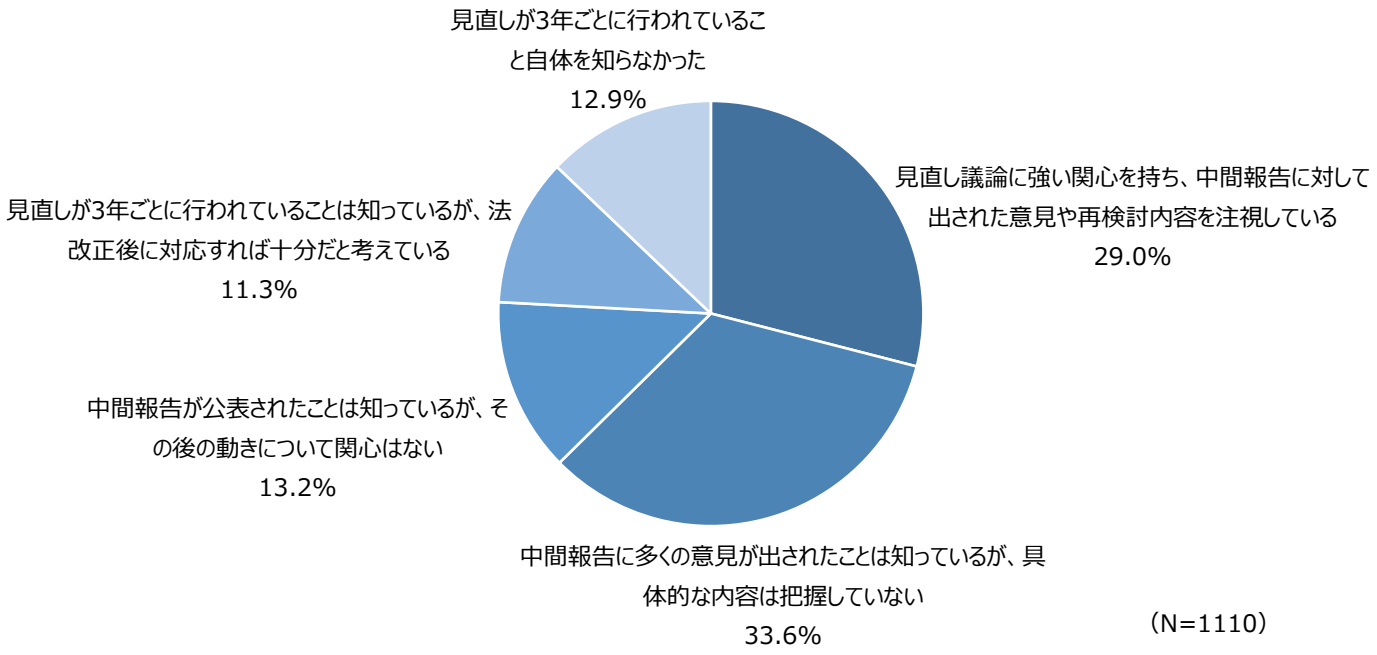
5.1　個人情報保護において注力している取り組み

- 個人情報保護に対して注力している取り組みを、1位～3位まで順位付けしている。
- 1位の取り組みとして最も回答率が高いのは「個人情報保護管理者の任命」となった。ただ、2024年調査から回答率は減少し、その他の取り組みの回答率が上昇している傾向が出ている。
- 「社員教育」は1位、2位、3位と満遍なく回答率が高く、多くの企業が注力していることがうかがえる。特に2位としての回答率が2024年調査から上昇している。
- 「規程類の整備」が2位で最も高い回答率となっている。



5.2　改正個人情報保護法の対応における問題：全体と個人情報保有件数別

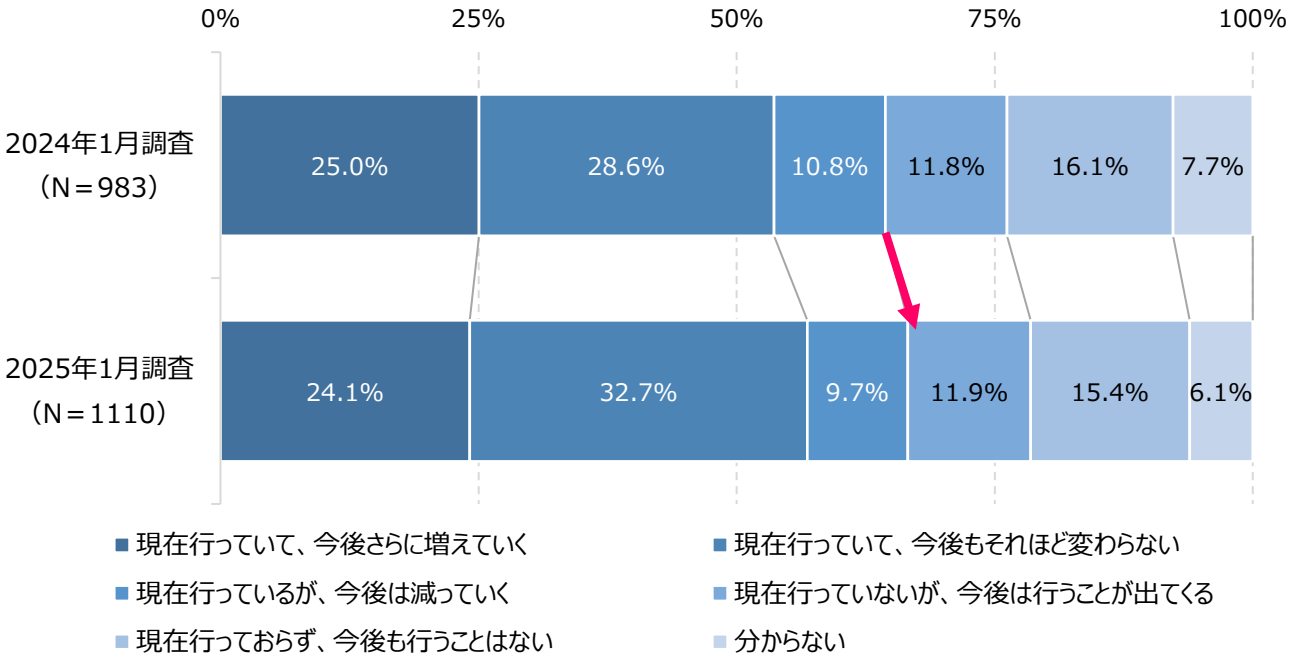
- 現在、個人情報保護法の改正に向けた検討が行われている。2024年6月に出された「個人情報保護法いわゆる3年ごと見直しに係る検討の中間整理」（9月に意見結果公表）に対し、「見直し議論に強い関心を持ち、中間報告に対して出された意見や再検討内容を注視している」は29.0%となった。
- 最も多い層は「中間報告に多くの意見が出されたことは知っているが、具体的な内容は把握していない」で33.6%となった。残りの3分の1は関心がない、または知らないということになる。



5.3　データの越境移転の状況

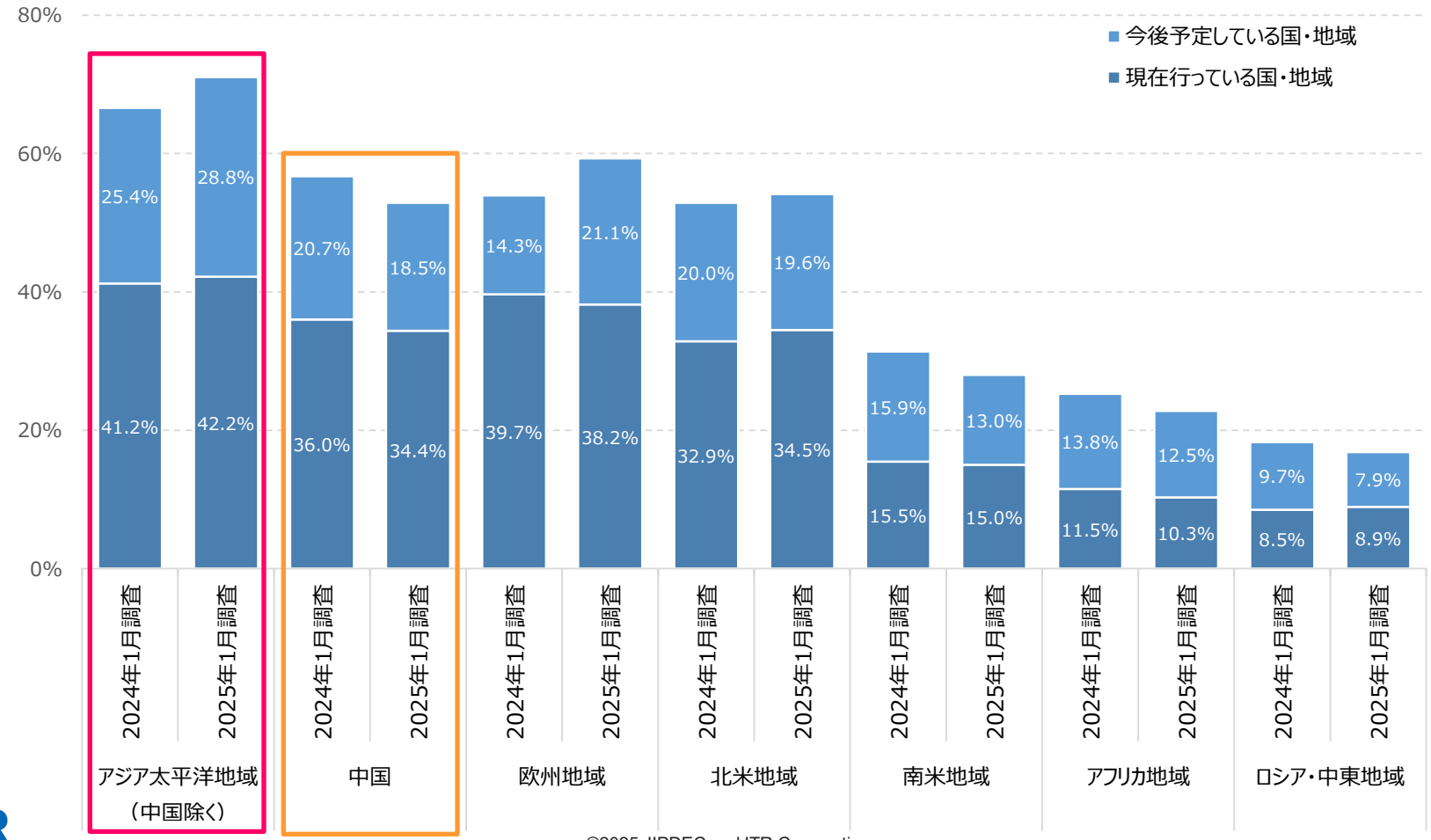
- 現在データの越境移転を行っている企業は66.6%となり、2024年調査（64.4%）よりも増加している。
- 「今後さらに増えていく」と「今後は減っていく」の割合はやや減少し、「今後もそれほど変わらない」の割合が増えている。

※データの越境移転：個人情報を海外の第三者に提供すること。プライバシー保護の観点から、各国・地域が規制を設けるなどの対応が行われている



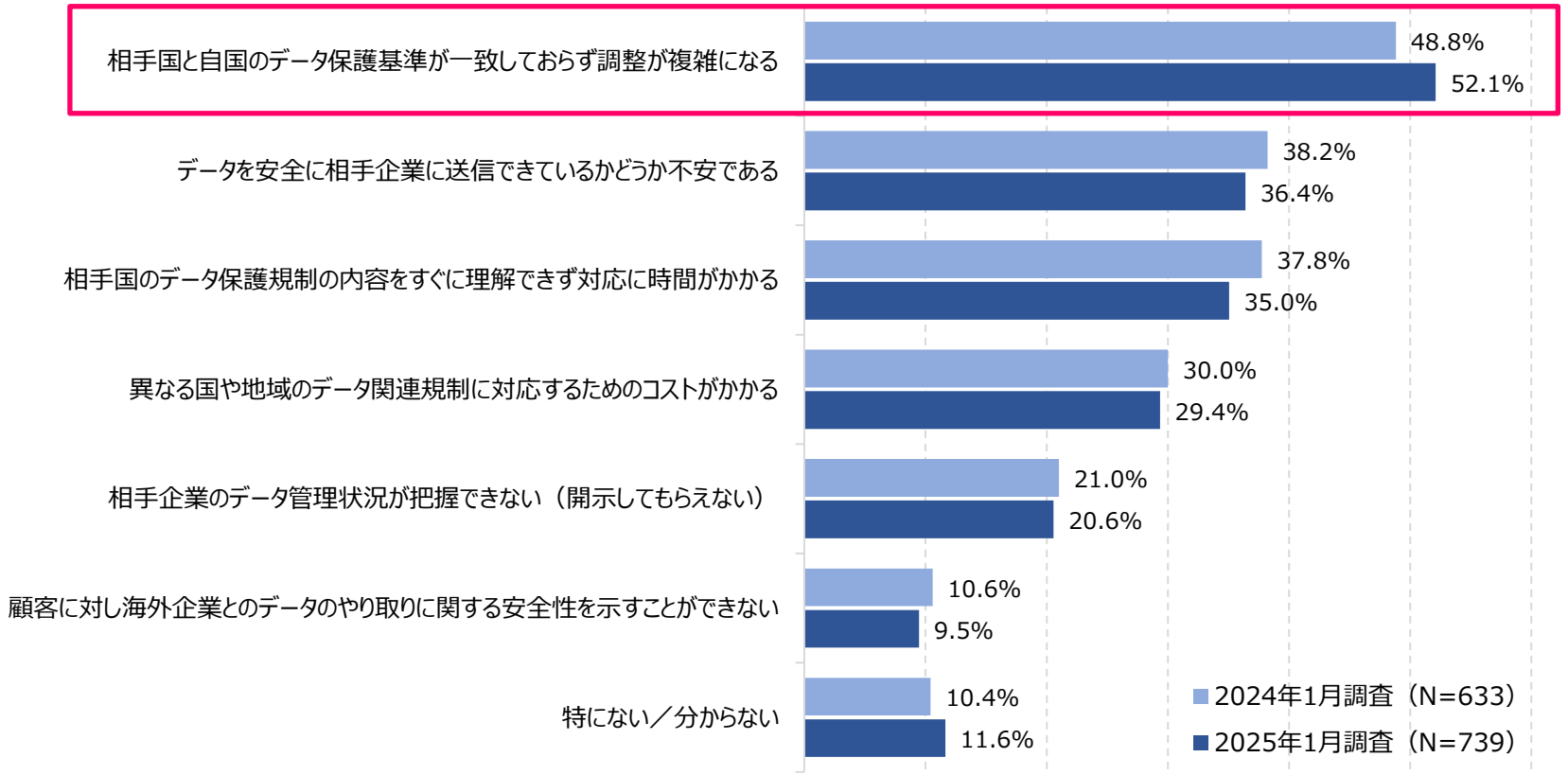
5.4　データの越境移転先の国・地域

- 現在データ越境移転を行っている国・地域としては「アジア太平洋地域（中国除く）」が最も多い。今後行う予定としても多く、どちらも2024年調査から増加している。
- その他の主なデータ越境移転先としては「欧州地域」「中国」「北米地域」となっている。「中国」は現在と今後両方で減少している。



5.5　海外企業とのデータのやり取りにおける課題

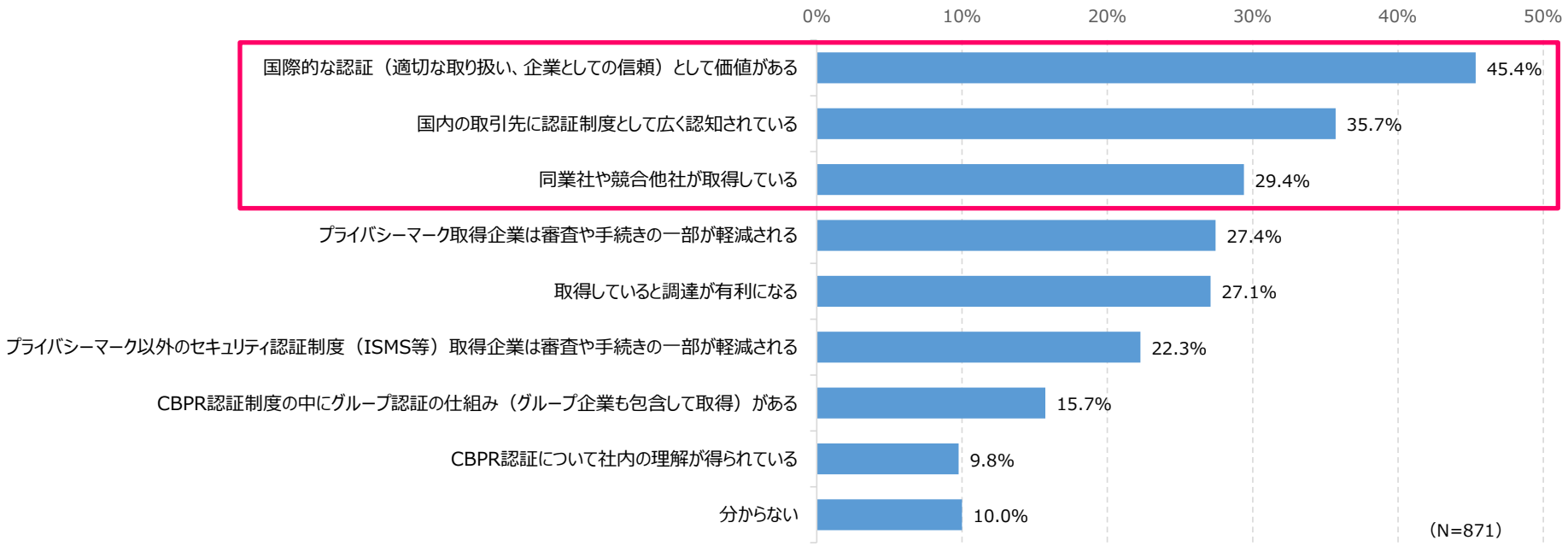
- 「相手国と自国のデータ保護基準が一致しておらず調整が複雑になる」が最も多く、50%を超え、2024年調査よりも増加している。両国のデータ保護基準が一致せず、調整が複雑化している企業が多いことがうかがえる。
- 2番目には「データを安全に相手企業に送信できているかどうか不安である」、3番目に「相手国のデータ保護規制の内容をすぐに理解できず対応に時間がかかる」が続いている。



5.6　CBPR認証取得に向けて動機となること

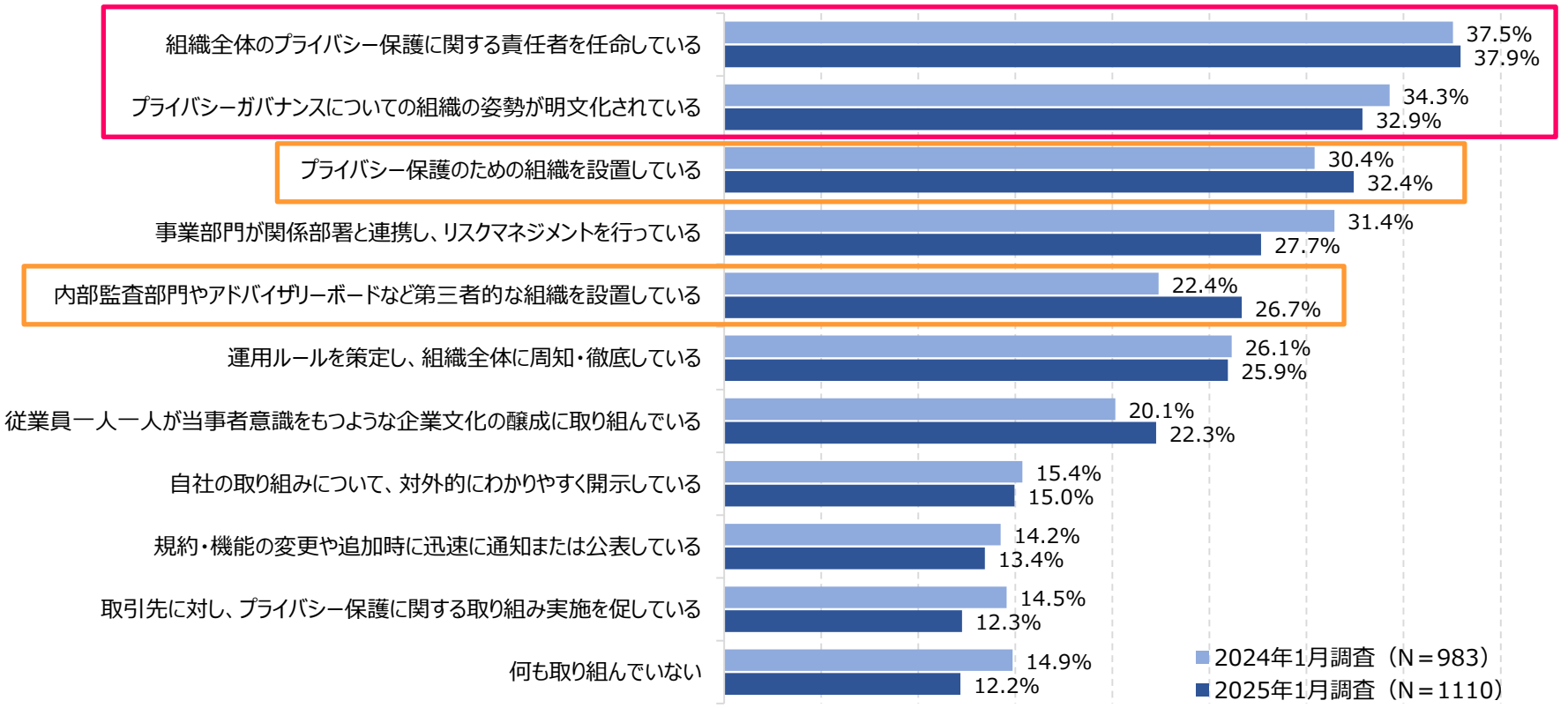
- 「国際的な認証（適切な取り扱い、企業としての信頼）として価値がある」が最も多い。CBRPの国際的な認知度や重要度が高まってくると取得企業は増えてくるものと考えられる。
- 2番目は「国内の取引先に認証制度として広く認知されている」、3番目は「同業社や競合他社が取得している」が続いている。国内でのCBPRの認知度が高まることも、取得企業を増やす上で必要になってくる。

CBPR認証：APEC域内において国境を越えて流通する個人情報に対し、消費者や事業者、行政機関における信用を構築するシステム



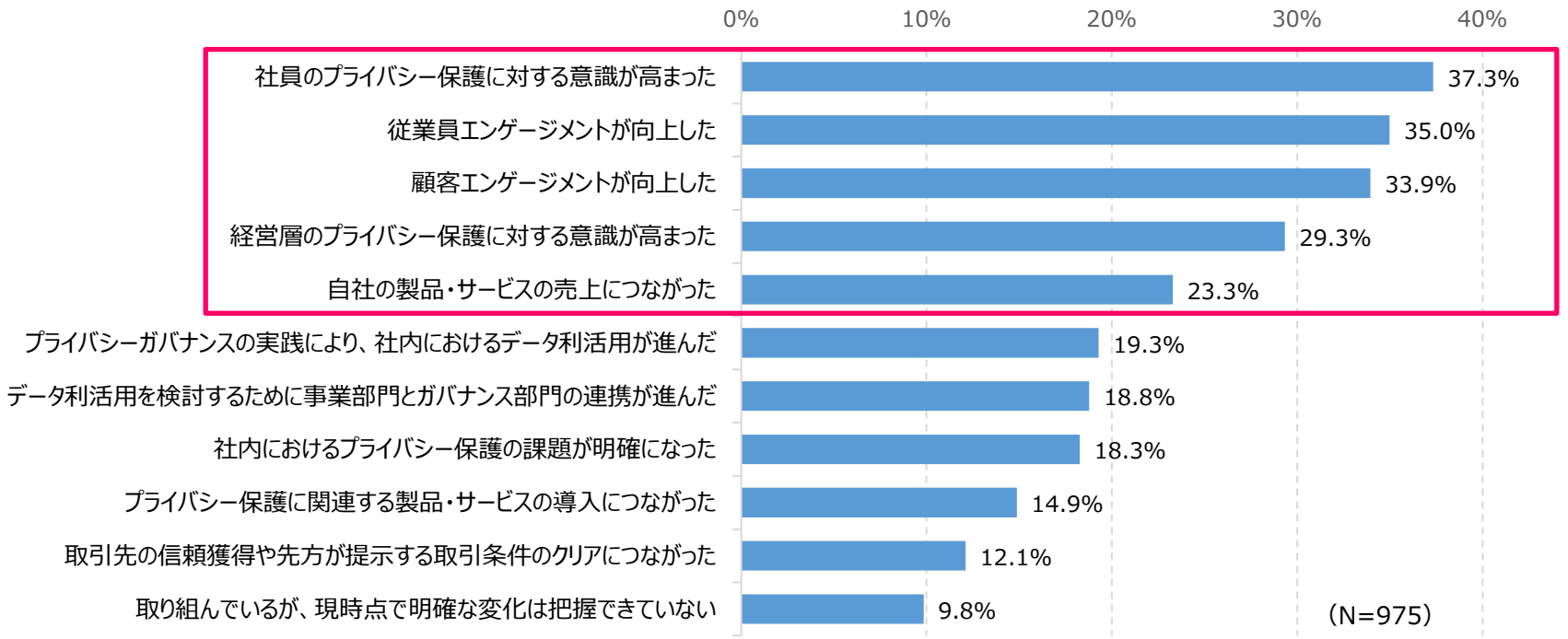
5.7　プライバシーガバナンスに関する取り組み状況

- 「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」が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は変わっていない。
- 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」と5番目の「内部監査部門やアドバイザリーボードなど第三者的な組織を設置している」が前回調査から上昇している。プライバシー保護関連の組織を設置する企業が増加している傾向がみられる。



5.8　プライバシーガバナンスに取り組んだことによる変化

- 「社員のプライバシー保護に対する意識が高まった」が37.3%で最多となり、「経営層のプライバシー保護に対する意識が高まった」も29.3%となっている。プライバシーガバナンスの取り組みが、社内全体の意識改革に寄与していることがうかがえる。
- 2番目は「従業員エンゲージメントが向上した」となった。組織全体でプライバシー保護を重視することが明示されることによって、従業員が企業への信頼を深めることにつながると考えられる。
- 3番目は「顧客エンゲージメントが向上した」が挙がっている。プライバシーに配慮したデータ活用が企業のブランド価値を高め、顧客や取引先からの信頼を獲得する要因になると考えられる。その結果、4分の1が製品・サービスの売上につながっている。



5.9　プライバシー保護の取り組み状況：調査結果からの考察

- 個人情報保護法の改正に関する検討内容に関心を示しているのは約3割にとどまっている。このままだと、多くの企業が改正後に慌てて対応することになるので、今から検討内容を把握し、改正後に迅速かつ円滑に対応できるよう準備を進めて頂きたい。

- データの越境移転を行う企業は増加し、移転先はアジアに拡大している。一方で、各国のデータ保護基準が異なることから、調整に難航している企業が増えている。CBPR認証の取得など、データ移転の円滑化を図るための施策を検討すべきである。

- 経済産業省／総務省が提示するプライバシーガバナンスの取り組むべき三要件（プライバシーガバナンス姿勢の明文化、プライバシー保護責任者の指名、取り組みに対するリソースの投入）に沿って進めている企業が増えており、このまま継続した取り組みとなっていくことを期待したい。

- プライバシーガバナンスに取り組んだ成果が見えてきている。社内の意識の高まりだけではなく、顧客など外部のステークホルダーにも良い影響が出ているという調査結果が示されたことは、今後のさらなる推進につながっていくと考えられる。

報告する調査項目

1. 経営課題とDX実践状況

2. 電子契約の利用状況

3. 生成AIの活用状況と課題

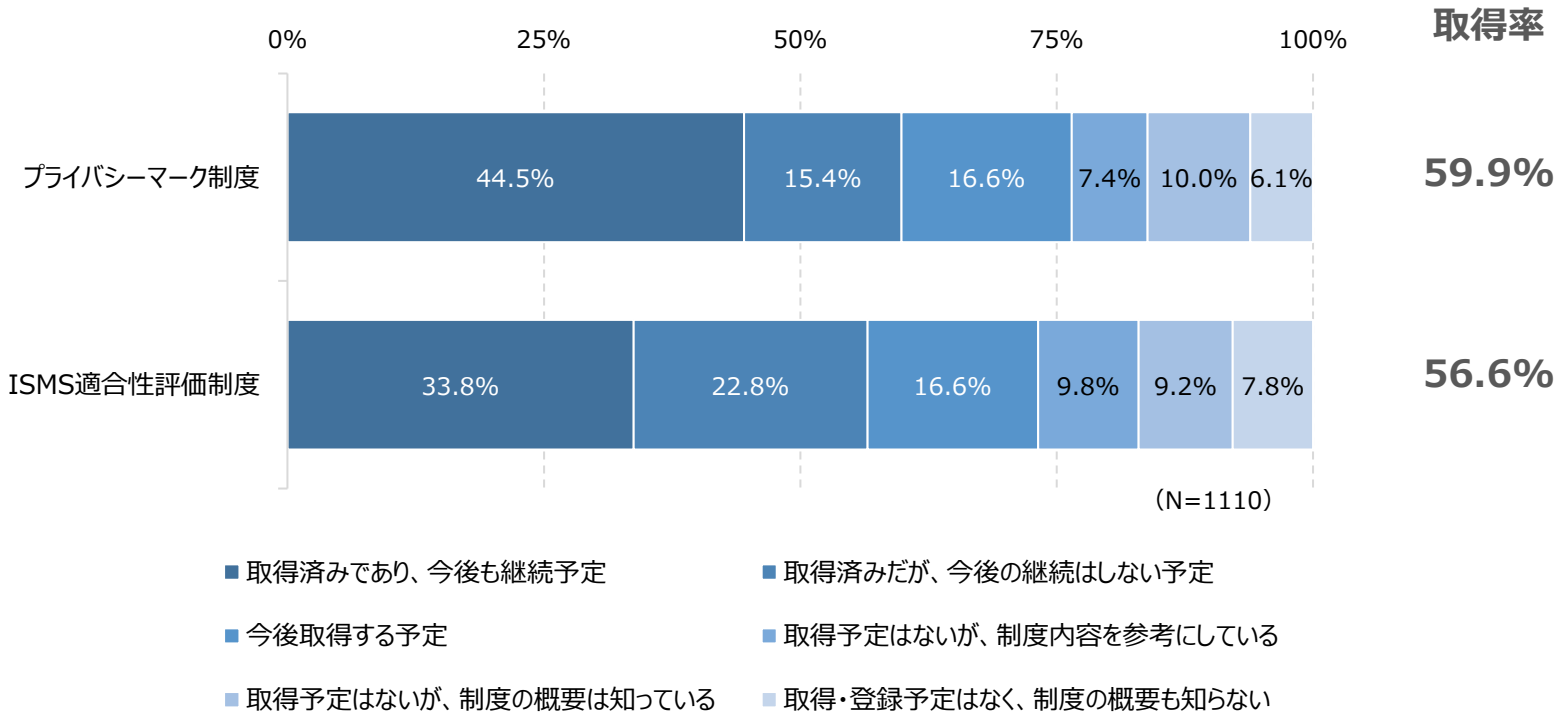
4. ランサムウェアとセキュリティ対策の実態

5. プライバシー保護に対する取り組み状況

6. 第三者認定／認証制度の取得状況

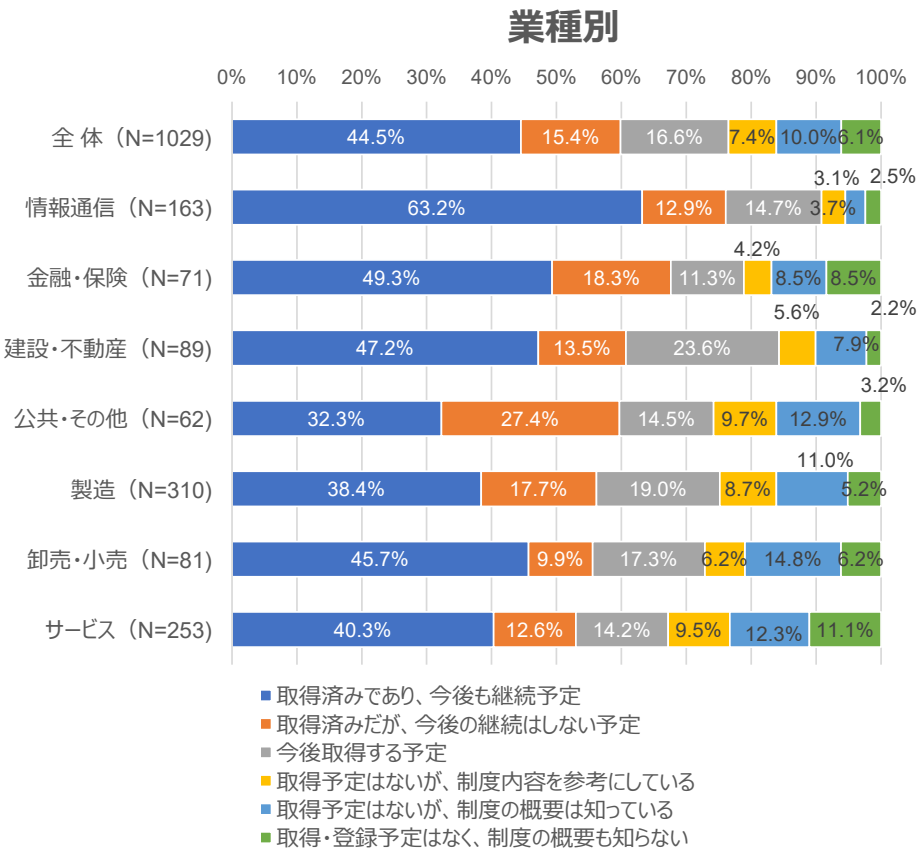
6.1 プライバシーマーク／ISMSの取得状況

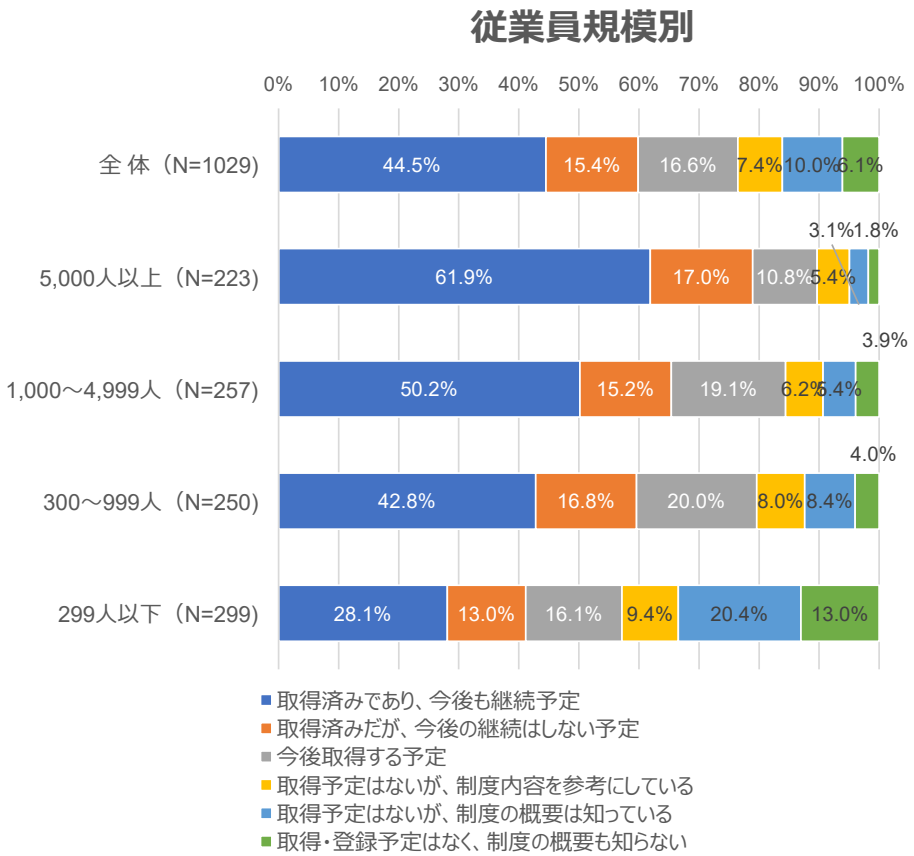
- プライバシーマークの取得率は59.9%となった。そのうち「取得済みであり、今後も継続予定」は44.5%となっている。
- ISMSの取得率は56.6%となった。そのうち「取得済みであり、今後も継続予定」は33.8%とやや低く、今後の継続に課題が残る結果となった。



6.2　プライバシーマークの取得状況：業種別と従業員規模別

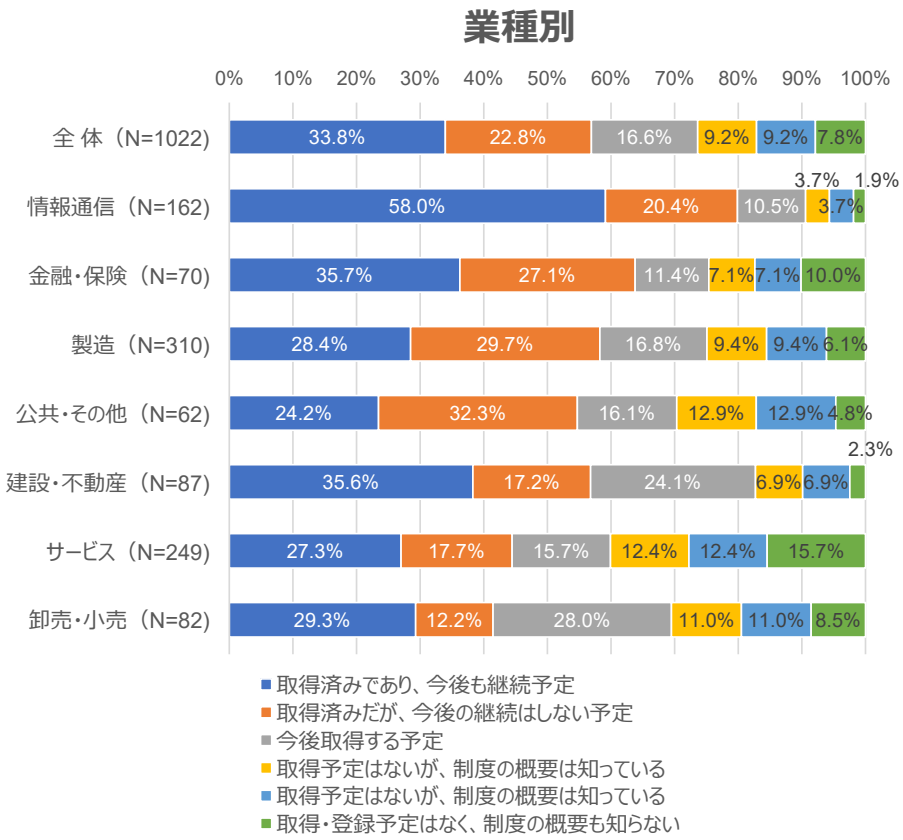
- 業種別で取得率が最も高いのは「情報通信」で75%を超えている。次に「金融・保険」と「建設・不動産」が続く。「公共・その他」は今後継続しない予定が27.4%と他の業種に比べて高くなっている。取得率が最も低いのは「サービス」である。
- 従業員規模別では規模が大きくなるにしたがい取得率が高くなっていき、「5,000人以上」では約8割が取得している。一方、「299人以下」では取得率が約4割にとどまっている。

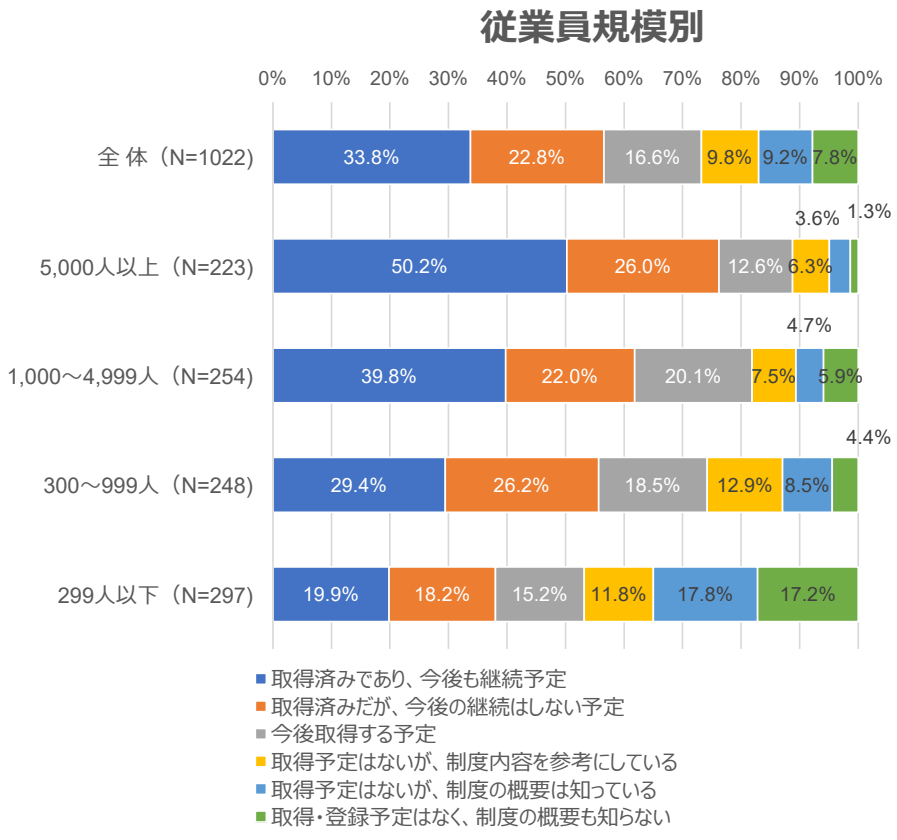




6.3 ISMSの取得状況：業種別と従業員規模別

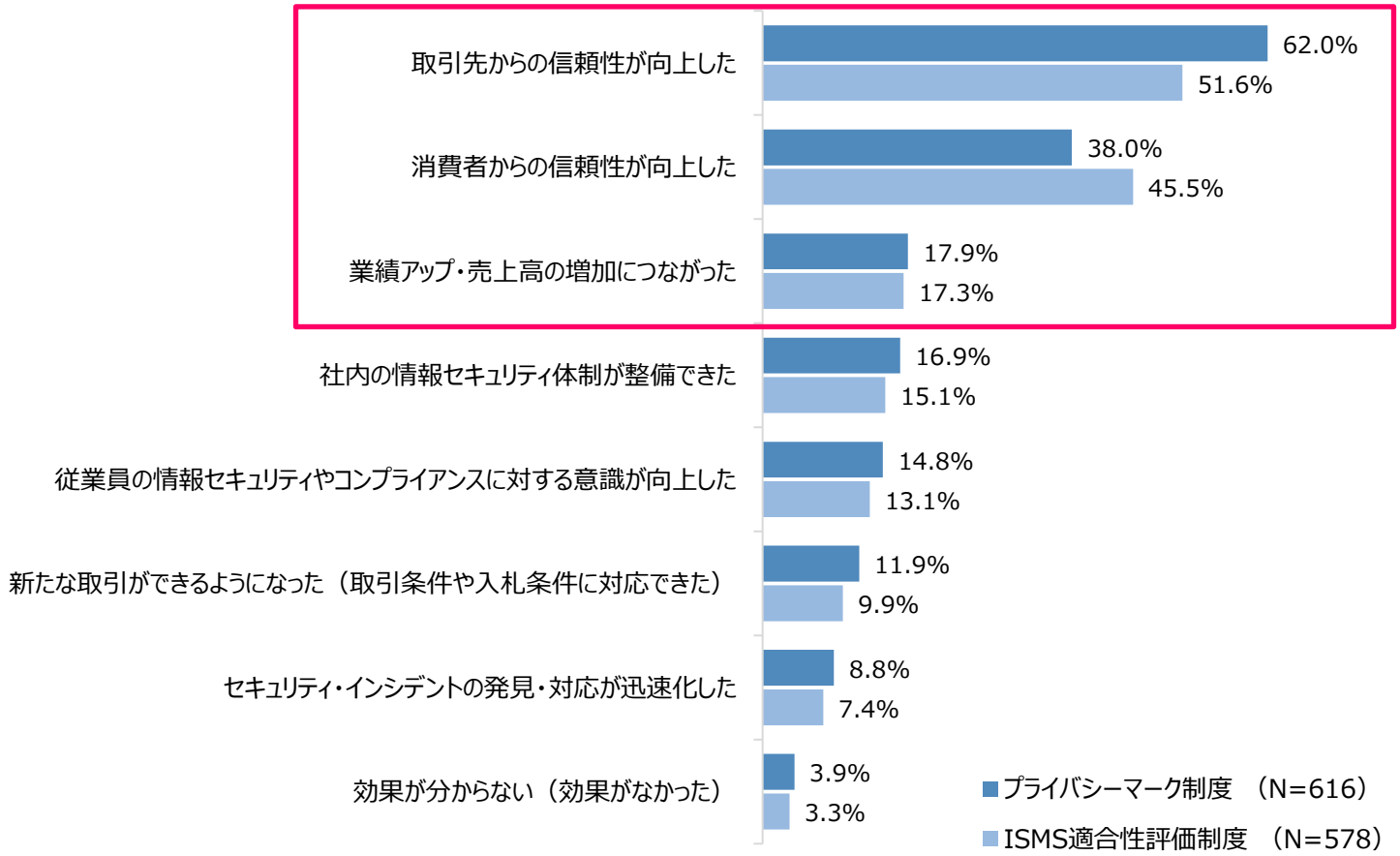
- 業種別で取得率が最も高いのは「情報通信」となり約8割が取得している。次に「金融・保険」が続く。「公共・その他」「製造」「金融・保険」で、今後継続しない予定が比較的高い。取得率が最も低いのは「サービス」である。
- 従業員規模別では規模が大きくなるにしたがい取得率が高くなっていき、「5,000人以上」では75%以上が取得している。一方、「299人以下」では取得率が約4割にとどまっている。





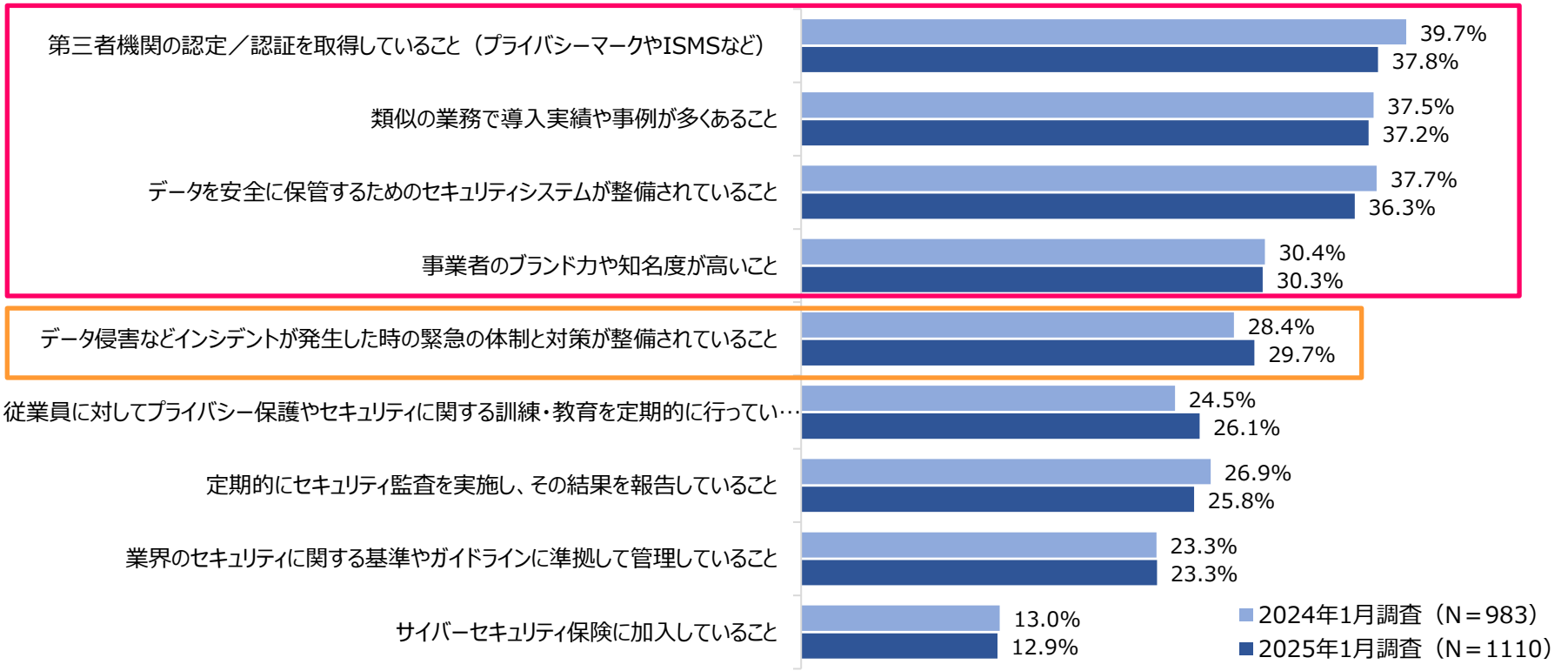
6.4 プライバシーマーク／ISMSの取得による効果

- プライバシーマーク、ISMSともに「取引先からの信頼性が向上した」が最も多く回答された効果となった。プライバシーマークの方がより多くなっている。
- その次は「消費者からの信頼性が向上した」となっているが、ISMSの方が多くなっている。
- 「業績アップ・売上高の増加につながった」が3番目に挙がっており、ビジネスに寄与している企業も一定数ある。



6.5　機密情報を扱う業務の委託事業者の選定で重視する点

- 「第三者機関の認定／認証を取得していること」が最も多く、選定に与える影響は大きい。
- 2番目に「類似の業務で導入実績や事例が多くあること」、4番目には「事業者のブランド力や知名度が高いこと」が挙がっており、セキュリティ面以外も選定要因として重視されている。
- 「データを安全に保管するためのセキュリティシステムが整備されていること」が3番目に挙がっており、事業者におけるデータセキュリティへの取り組みが選定において重要となっている。
- 「データ侵害などインシデントが発生した時の緊急の体制と対策が整備されていること」が2024年調査から上昇している。インシデント発生時の復旧体制がより重視されるようになっている。



6.6　第三者認定／認証制度の取得状況：調査結果からの考察

- プライバシーマーク、ISMSともに取得率は50%を超えている。ただし、ISMSにおいて、今後は継続しないという回答率が目立つため、継続する難しさがうかがえる。また、全体の取得率をさらに押し上げるためには、サービス業や中小企業での取得率を向上させる必要がある。

- プライバシーマークとISMSの取得による主な効果は、消費者や取引先からの信頼性が向上することである。さらに売上の増加につなっがている企業も一定数ある。

- 機密情報を扱う業務の委託事業者の選定においては、プライバシーマークとISMSのような第三者機関の認定／認証の取得が最も重視されている。さらに、事業者がランサムウェアに感染する事例も出ていることから、セキュリティシステムや復旧体制の整備状況も重視される傾向が強まっていると考えられる。

7　総括・提言

生成AIは、評価・導入する段階から、活用して効果を出していくという段階に移っており、そのスピードはこれまでに経験したことのない速さである。一方で、情報漏えいやハルシネーションなどのリスクは、社内の利用範囲が広がるにつれて高くなるため、ガイドラインの策定や従業員への教育、AIの適切な管理を行うことが不可欠となる。

ランサムウェア攻撃の脅威は続いており、すでに半数近い企業が感染経験をもち、その半数以上がデータやシステムを復旧できていない。現時点での主な侵入経路は、メールによる攻撃とリモートアクセスの脆弱性を狙った攻撃であるが、攻撃は日々巧妙化し、侵入経路も多様化していくであろう。徹底かつ継続的なセキュリティ対策が強く求められる。

企業におけるプライバシーガバナンスの重要性が高まっている。取り組んでいる企業において、従業員と顧客に対するエンゲージメントの向上、さらには収益増加という一定の効果がみられたことは評価すべき点である。今後も継続して取り組み、データの利活用の推進やビジネス拡大につなげていくことが重要となる。

問いを、答えに。

ITR