JIPDECセミナー
「DX推進・生成AI利用とセキュリティ・プライバシー保護の実態
～「企業IT利活用動向調査2024」結果報告～」　講演資料

株式会社アイ・ティ・アール
シニア・アナリスト　　入谷　光浩　氏

2024年3月15日（金）

JIPDECセミナー

DX推進・生成AI利用と
セキュリティ・プライバシー保護の実態

～「企業IT利活用動向調査2024」結果報告～

2024年3月15日

株式会社アイ・ティ・アール

iTR

「企業IT利活用動向調査2024」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、クラウドサービス、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　：　2024年1月19日～1月23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

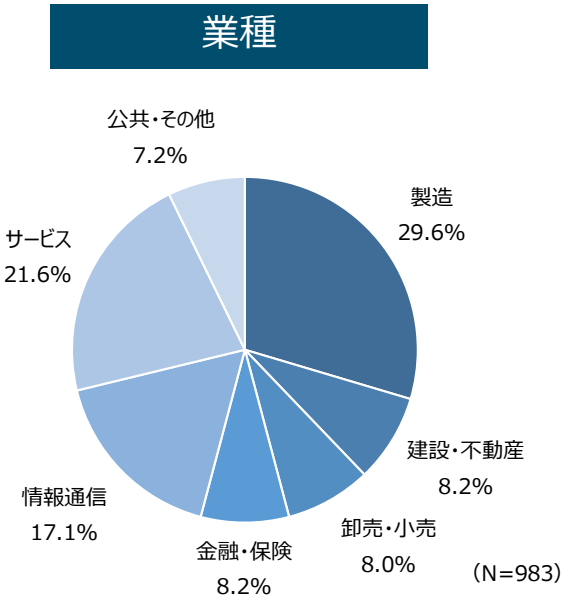
■調査対象　：　以下の条件を満たす個人：約17,000人
- 従業員50名以上の国内企業の勤務者
- 情報システム、経営企画、総務・人事、業務改革・業務推進関連、DX推進関連のいずれかに関する業務の担当者
- IT戦略策定または情報セキュリティの従事者
- 係長（主任）相当職以上の役職者

■有効回答数　：　983件（1社1回答）

調査結果における留意事項

- 2023年調査（企業IT利活用動向調査2023）、2022年調査（企業IT利活用動向調査2022）では、従業員2人以上の企業から調査対象としていた。今回調査では従業員50人以上を対象としたため、2023年調査と2022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

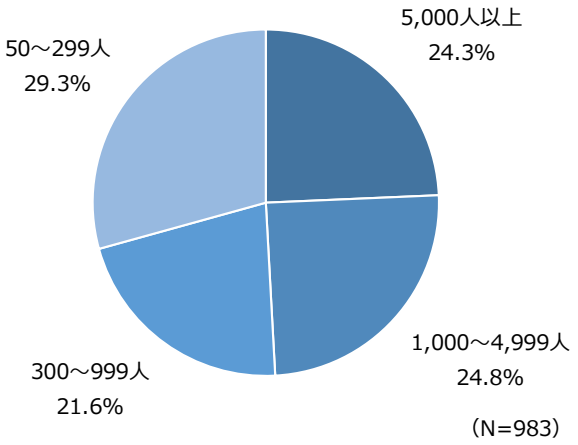


業種詳細

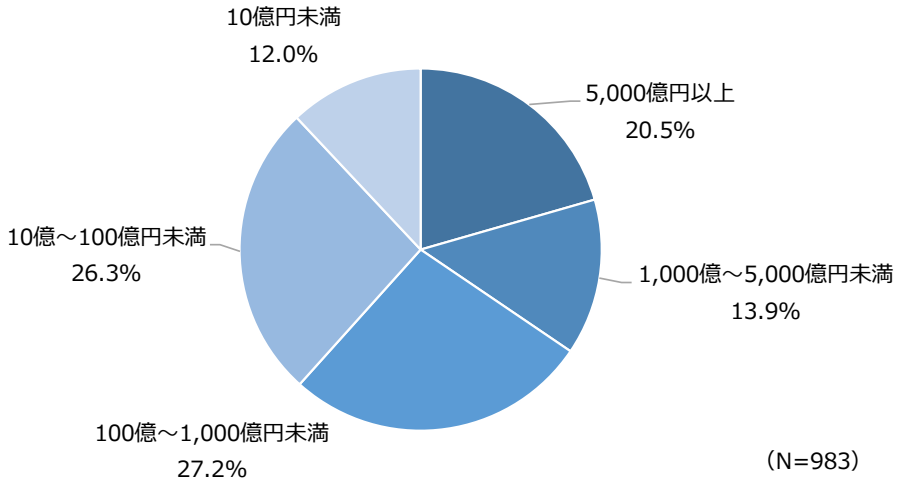
大分類	詳細	回答数	構成比
製造	食品・飲料	41	4.2%
	日用品・生活雑貨	18	1.8%
	繊維	11	1.1%
	パルプ・紙・印刷	15	1.5%
	化学工業	15	1.5%
	石油製品	5	0.5%
	鉄鋼・金属	21	2.1%
	プラスチック・ゴム	7	0.7%
	機械	23	2.3%
	電気機器	37	3.8%
	情報通信機器	10	1.0%
	電子部品・電子回路	16	1.6%
	精密機器	23	2.3%
	自動車・輸送機器	28	2.8%
	医薬品	8	0.8%
	その他の製造業	13	1.3%
建設・不動産	建設	45	4.6%
	不動産	36	3.7%
	住宅	0	0.0%
卸売・小売	卸売	19	1.9%
	小売	34	3.5%
	商社	26	2.6%
金融・保険	銀行	42	4.3%
	証券	7	0.7%
	生命保険	8	0.8%
	損害保険	14	1.4%
	その他金融	10	1.0%
情報通信	通信	26	2.6%
	ITベンダー／システムインテグレーター	114	11.6%
	インターネット・サービス	15	1.5%
	情報システム子会社	13	1.3%
サービス	電力・ガス・水道	22	2.2%
	運輸	33	3.4%
	倉庫	6	0.6%
	宿泊	5	0.5%
	飲食	6	0.6%
	娯楽・レジャー	13	1.3%
	メディア・出版・放送・広告	6	0.6%
	生活関連サービス（旅行業など）	10	1.0%
	医療	30	3.1%
	福祉・介護	28	2.8%
	教育（学校以外）	15	1.5%
	人材派遣・業務委託	17	1.7%
	その他サービス	21	2.1%
公共・その他	学校	12	1.2%
	官公庁	12	1.2%
	地方自治体	27	2.7%
	その他公共機関	9	0.9%
	農業・水産・鉱業	3	0.3%
	その他の業種	8	0.8%
合計		**983**	**100.0%**

回答者が所属する企業のプロフィール②

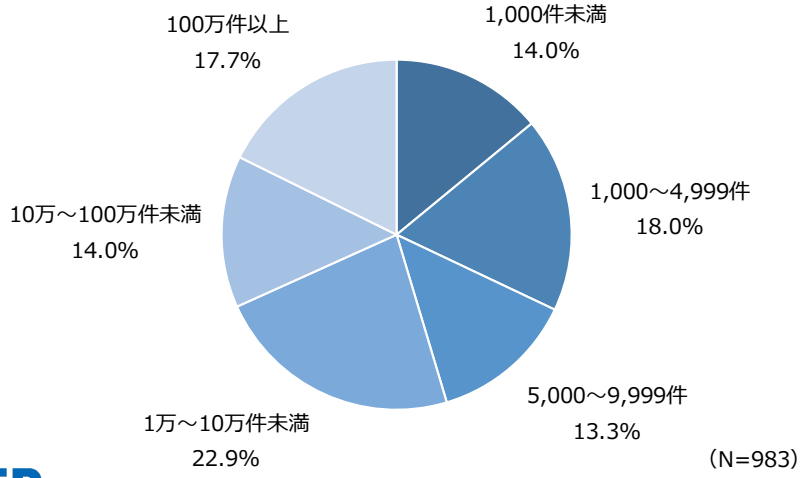
従業員規模



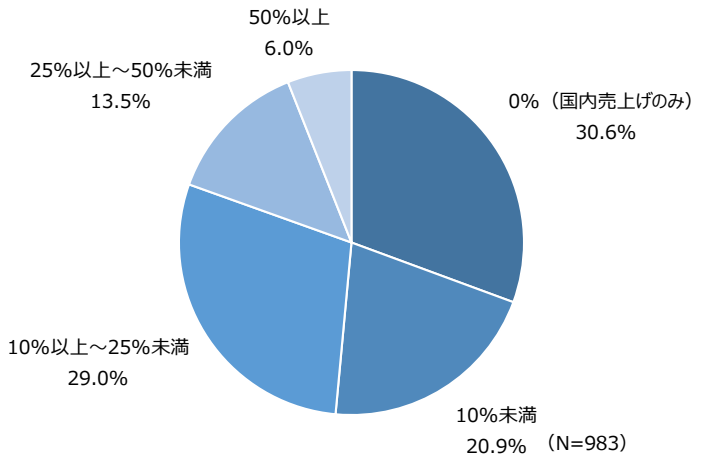
年間売上規模



個人情報保有件数



海外売上比率



報告する調査項目

1. DXの実践状況

2. 電子契約の利用状況

3. 生成AIの利用と課題

4. セキュリティのインシデントと対策

5. プライバシー保護に対する取り組み

6. 第三者認定／認証制度の取得状況

報告する調査項目

1. DXの実践状況

2. 電子契約の利用状況

3. 生成AIの利用と課題

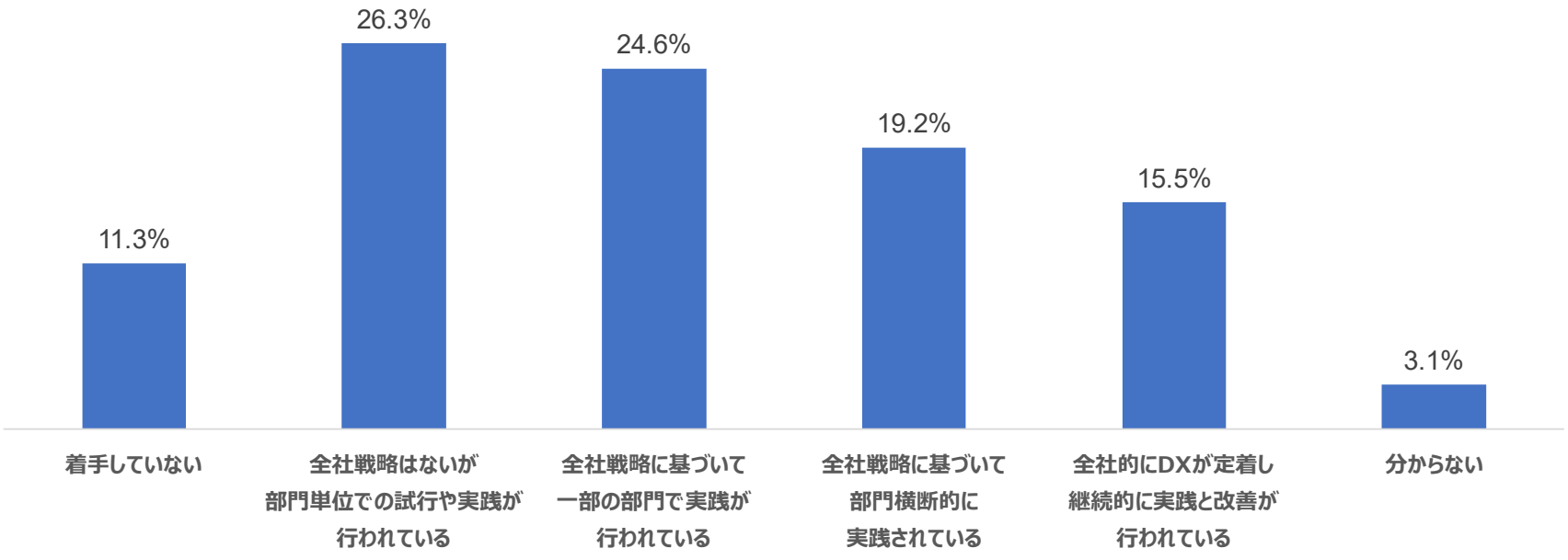
4. セキュリティのインシデントと対策

5. プライバシー保護に対する取り組み

6. 第三者認定／認証制度の取得状況

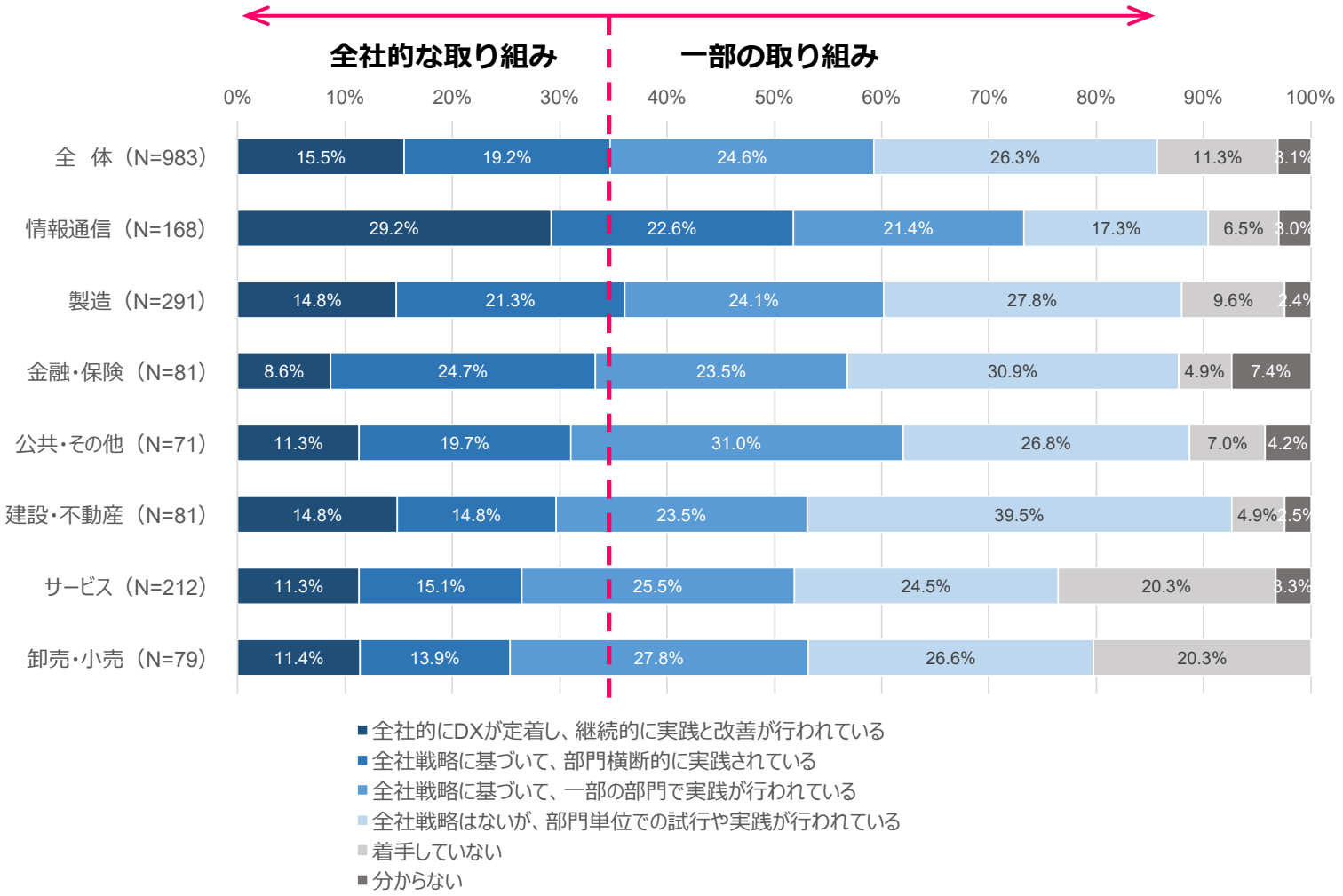
1.1　DXの実践段階の状況：全体

- ほとんどの企業でDXは実践されている状況にはあるが、約半数はPoCや一部での取り組みの段階にとどまっている状況にある。
- DXが全社的な取り組み（部門横断的取り組みも含む）となり、定着化が進んでいるのは約3分の1となっている。



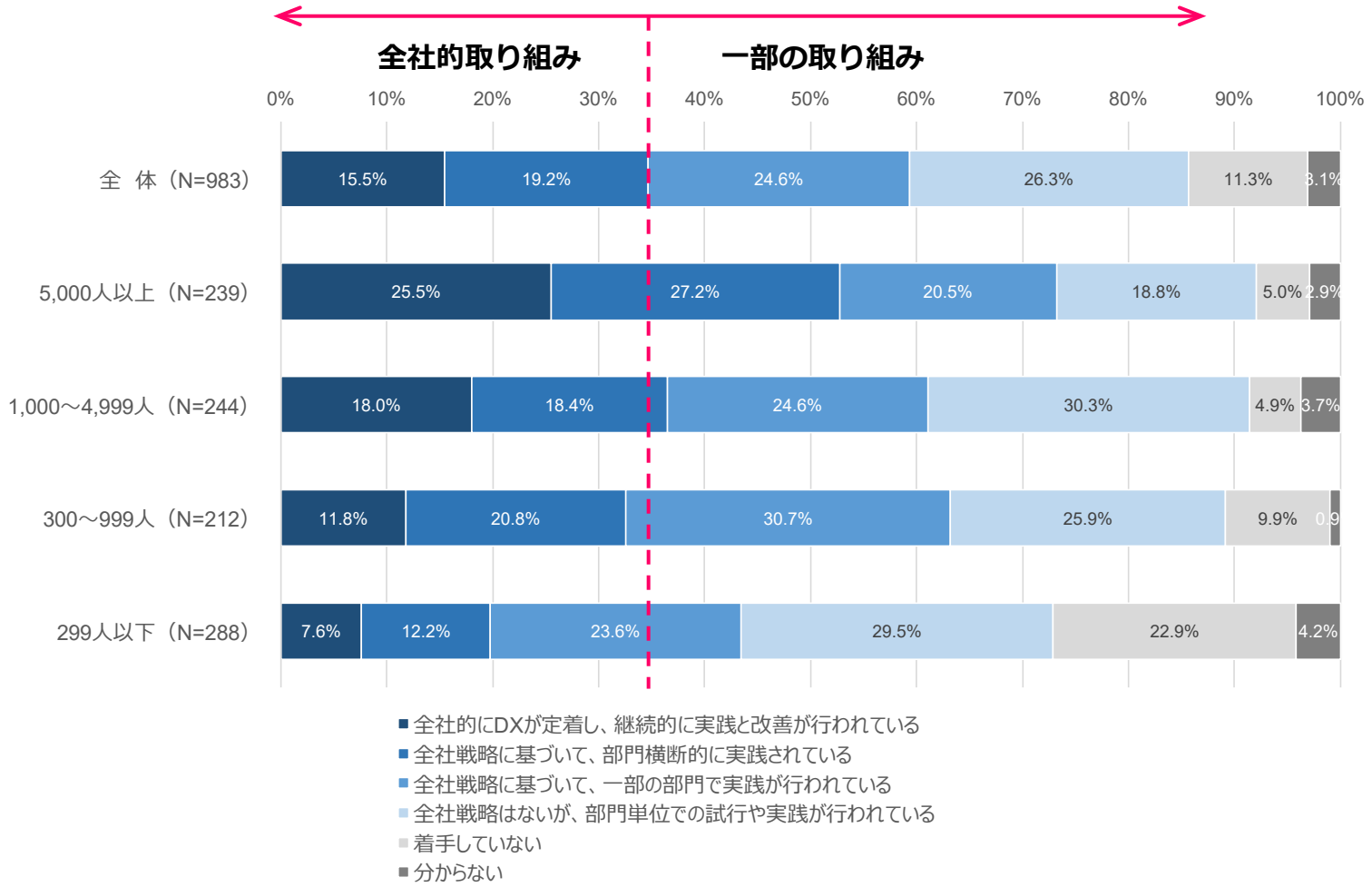
1.2　DXの実践段階の状況：業種別

- DXの全社的な取り組みは「情報通信」が大きく先行しており、「製造」と「金融・保険」が続く。
- 「卸売・小売」と「サービス」は取り組みが遅く、未着手の企業も20%程度いる。



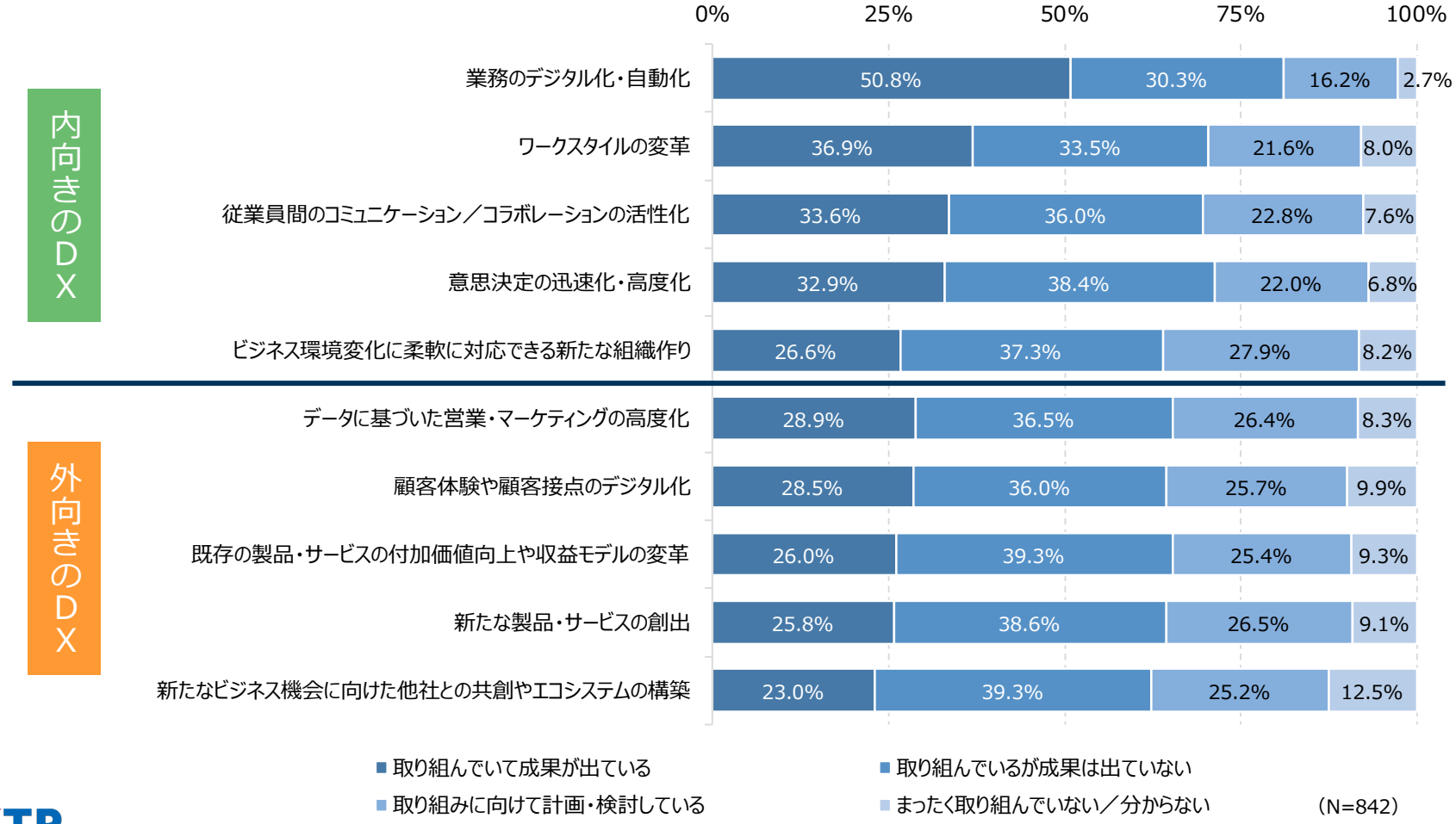
1.3　DXの実践段階の状況：従業員規模別

- 従業員規模が大きくになるにしたがいDXの取り組みも進んでいる傾向があり、「5,000人以上」では全社的に取り組んでいる企業が半数以上になっている。
- 「299人以下」ではDXの取り組みの遅れが顕著になり、未着手の割合も大きくなっている。



1.4　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。



1.5　DXの成果が出ている業種

- 内向きのDXと外向きのDXともに「情報通信」が最も成果が出ている。
- 「卸売・小売」は、各個別の取り組みでは成果を出している企業の割合が高い。
- それ以外の業種では、特に外向きのDXでの成果が出ていない状況にある。

		全　体 (N=842)	情報通信 (N=152)	製造 (N=256)	金融・保険 (N=71)	公共・その他 (N=63)	建設・不動産 (N=75)	サービス (N=162)	卸売・小売 (N=63)
内向きのDX	業務のデジタル化・自動化	50.8%	61.8%	47.3%	47.9%	42.9%	49.3%	48.1%	58.7%
	ワークスタイルの変革	36.9%	54.6%	30.5%	32.4%	30.2%	37.3%	30.2%	49.2%
	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	33.6%	44.7%	29.3%	32.4%	34.9%	29.3%	27.8%	44.4%
	意思決定の迅速化・高度化	32.9%	46.1%	23.8%	28.2%	31.7%	34.7%	34.0%	39.7%
	ビジネス環境変化に柔軟に対応できる新たな組織作り	32.9%	46.1%	23.8%	28.2%	31.7%	34.7%	34.0%	39.7%
	内向きのDX平均	**37.4%**	**50.7%**	**30.9%**	**33.8%**	**34.3%**	**37.1%**	**34.8%**	**46.3%**
外向きのDX	データに基づいた営業・マーケティングの高度化	28.9%	36.8%	22.3%	31.0%	27.0%	24.0%	29.0%	41.3%
	顧客体験や顧客接点のデジタル化	28.5%	40.8%	23.8%	23.9%	25.4%	29.3%	25.9%	31.7%
	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	26.0%	38.2%	21.9%	26.8%	22.2%	17.3%	22.2%	36.5%
	新たな製品・サービスの創出	25.8%	35.5%	24.6%	18.3%	27.0%	24.0%	19.1%	33.3%
	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	25.8%	35.5%	24.6%	18.3%	27.0%	24.0%	19.1%	33.3%
	外向きのDX平均	**27.0%**	**37.4%**	**23.4%**	**23.7%**	**25.7%**	**23.7%**	**23.1%**	**35.2%**

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

1.6　DX実践における課題

- どのDX実践段階においても「情報セキュリティ対策」が最も大きな課題となっている。
- DXの取り組み規模が大きくなってくるほど「DX人材の育成と獲得」の課題が深刻化している。
- 部門横断的な実践段階にある企業では、「投資対効果の測定」が定着化に向けた課題になっている。

	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）
情報セキュリティ対策	52.4%	55.9%	52.4%	48.3%	54.1%
DX人材の育成と獲得	38.8%	54.6%	43.9%	37.6%	27.0%
従業員のＤＸに対する理解や協力姿勢	38.1%	45.4%	39.7%	38.0%	32.8%
新しいデジタル技術の選定と導入	37.5%	51.3%	43.9%	30.6%	31.3%
継続的な予算確保	33.8%	40.8%	35.4%	35.5%	27.0%
経営層のリーダーシップ	33.4%	29.6%	33.9%	33.5%	35.1%
投資対効果の測定	30.3%	29.6%	42.9%	29.3%	22.4%
柔軟性のある組織や風通しの良い文化の構築	19.1%	28.3%	18.5%	16.5%	16.6%
法規制の遵守やコンプライアンスとの兼ね合い	17.3%	28.9%	21.2%	12.8%	12.0%
その他	0.1%	0.0%	0.5%	0.0%	0.0%
特に課題は出ていない	3.6%	5.3%	2.1%	3.7%	3.5%

1.7　DXの実践状況：調査結果からの考察

- ほとんどの企業がDXを実践しているが、試行段階や一部の限定的な取り組みの段階にある企業がまだ多く、国内企業全体のDXの定着化にはまだ時間を要する。しかし、全社的な取り組みとなった企業が3分の1となっていることは一定の評価ができる。

- 業種や企業規模でのDXの実践段階に差が出ている。デジタルリテラシーの高い情報通信や金融・保険が先行しているが、実践が遅れている業種や中小企業のDXを今後どのように後押ししていくかが国内のDX底上げの鍵になる。

- 業務効率化やコスト削減を優先する日本企業の特徴が「内向きのDX」に対する取り組み成果に表れている。今後はビジネス成長を目的とした「外向きのDX」の推進と強化が重要となり、日本企業のDXの真価が問われるようになっていく。

- DXにはクラウドから提供される様々なデジタルツールを駆使していくことになるが、そこでセキュリティとデジタル人材が大きな課題となっていることが明らかになった。業界全体で重点的に取り組み、課題を乗り越えていく必要がある。

報告する調査項目

1. DXの実践状況

2. 電子契約の利用状況

3. 生成AIの利用と課題

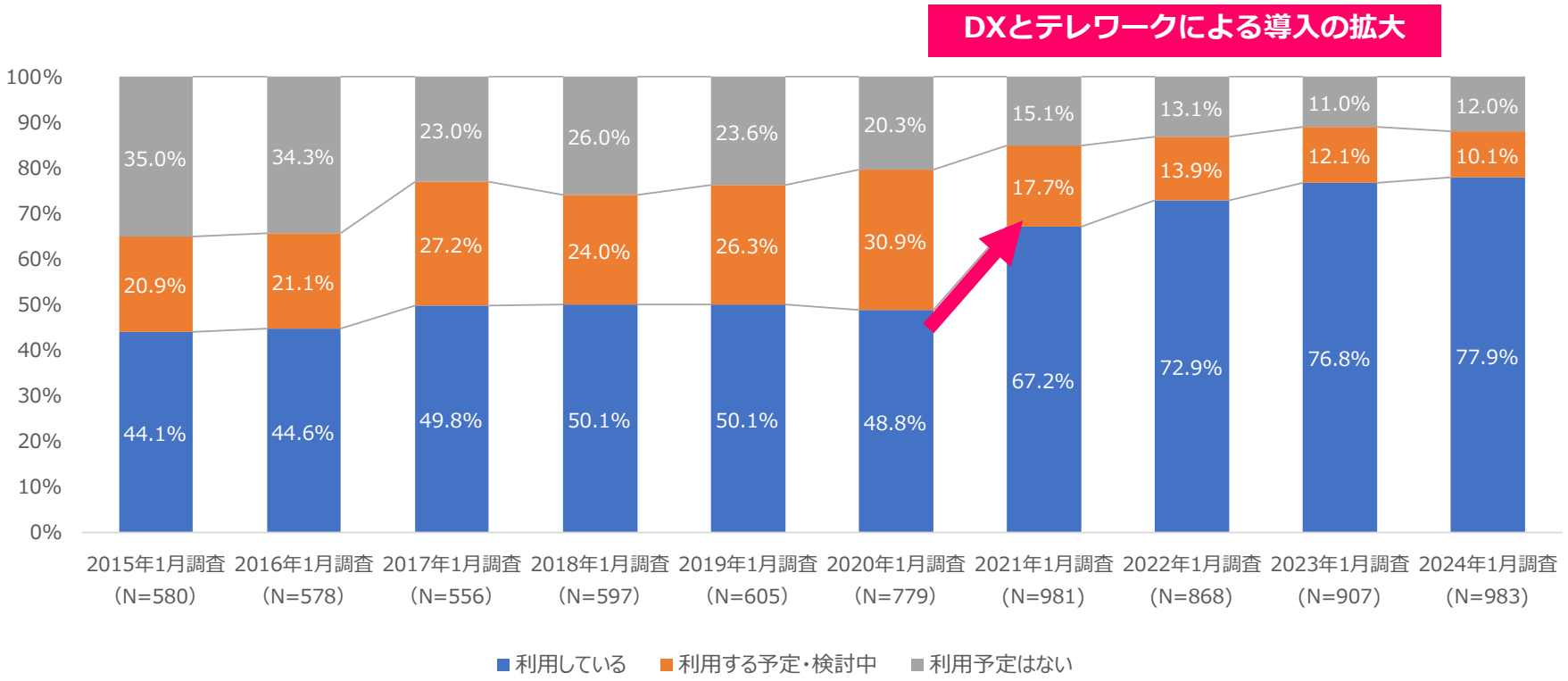
4. セキュリティのインシデントと対策

5. プライバシー保護に対する取り組み

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～2024年

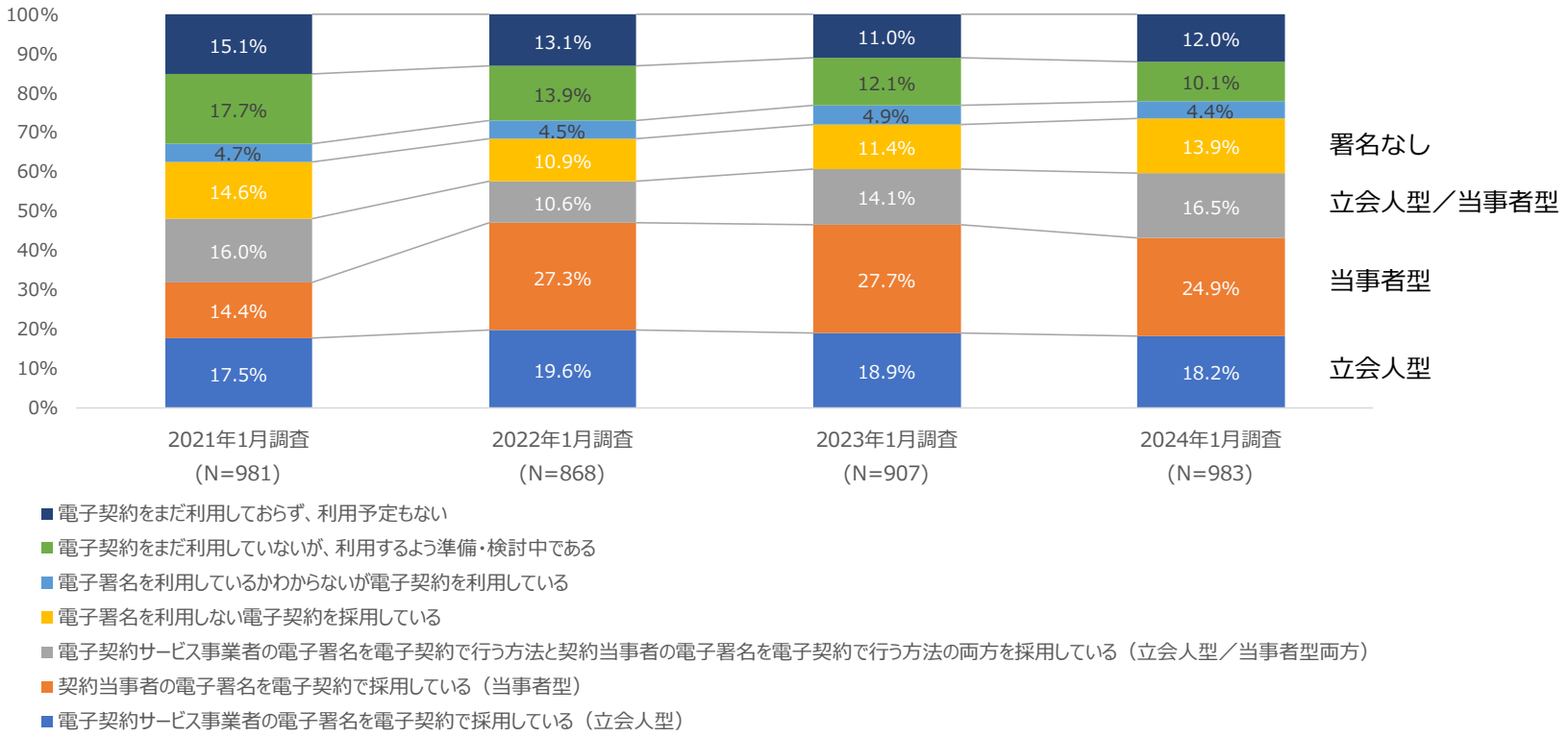
- 2020年1月調査までは電子契約の利用率が横ばいに推移していたが、2021年1月調査で大きく上昇している。DXによる業務のデジタル化の推進と、2020年からの新型コロナウイルス感染拡大によってテレワークが普及し、電子契約の需要が高まり2020年から2022年にかけて導入が拡大したとみられる。
- 2024年1月調査での利用率は77.9%であり、2023年調査からわずかな上昇にとどまった。すでに8割近い企業が利用していることもあり、導入がひと段落したとみることができる。



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（詳細）：2021年～2024年

- 「立会人型」は4年間で大きな変化は見られないが、「当事者型」は2022年1月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。
- 「立会型／当事者型両方」は、2022年1月調査で一度利用割合が小さくなったが、2023年1月調査から利用割合が大きくなっている傾向にある。契約相手によって、利便性の高い「立会人型」とガバナンスを利かせられる「当事者型」を使い分ける企業が増えているとみられる。



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

2.3　電子契約の利用による効果：全体と利用電子契約形態別

- 全体では「コスト削減」が導入効果として最も大きい。さらに「印紙税の節約」も上位にあがっており、費用の削減効果が出ている。特に立会人型ではコスト削減効果が非常に大きい。
- 「契約にかかる業務負荷の軽減」や「契約書管理の効率化」など業務効率化に対する効果も出ている。立会人型では約半数の企業で効果が出ている。
- 「契約時のセキュリティの強化」も3分の1以上の企業で効果が出ており、特に立会人型／当事者型の両方を利用している企業は40%を超えている。

	全　体 (N=865)	立会人型 (N=179)	当事者型 (N=245)	立会人型／当事者型の両方 (N=162)	電子署名を利用しないタイプ (N=137)	電子署名の利用有無は不明 (N=43)	利用を準備・検討中 (N=99)
コスト削減（印刷代、郵送費、保管費用など）	47.7%	75.4%	44.1%	40.7%	37.2%	27.9%	41.4%
契約にかかる業務負荷の軽減	40.6%	52.0%	40.4%	40.1%	34.3%	25.6%	36.4%
印紙税の節約	38.8%	44.1%	47.3%	33.3%	27.7%	39.5%	32.3%
契約書管理の効率化（探しやすい、整理しやすいなど）	37.9%	50.8%	41.6%	34.0%	29.9%	20.9%	30.3%
契約時のセキュリティの強化	34.0%	38.0%	38.4%	41.4%	29.9%	4.7%	22.2%
契約締結や取引完了までの期間の短縮	28.1%	31.8%	33.1%	32.7%	19.0%	16.3%	19.2%
テレワークや在宅勤務への対応	25.8%	32.4%	25.3%	32.7%	19.7%	23.3%	13.1%
取引先とのビジネス機会の増加	18.8%	24.0%	21.6%	20.4%	13.9%	7.0%	12.1%
企業の先進性やＤＸのアピール	12.5%	19.6%	12.7%	14.8%	4.4%	7.0%	9.1%
導入効果は特に出ていない／分からない	5.2%	2.2%	1.6%	2.5%	4.4%	4.7%	25.3%

注1：「利用を準備・検討中」は導入後に期待する効果について回答

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

- 全体では「立会人型に対応」と「当事者型に対応」、それぞれのタイプの対応が重視する点として上位に挙がっている。
- 「サービス事業者が第三者認証・認定取得を受けている」が全体で2番目となり、特に立会人型では60%以上が重視しており、第三者認証・認定の取得は立会人型サービスの選定に大きく影響する。
- 「EUのトラストリスに登録された電子証明書を利用」や「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」など、電子証明書も選定のポイントになっている。

	全 体 (N=766)	立会人型 (N=179)	当事者型 (N=245)	立会人型／当事者型の両方 (N=162)	電子署名を利用しないタイプ (N=137)	電子署名の利用有無は不明 (N=43)
立会人型電子署名の電子契約に対応している	39.3%	45.8%	42.4%	37.7%	30.7%	27.9%
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	37.7%	63.1%	37.6%	29.0%	21.2%	18.6%
当事者型電子署名の電子契約に対応している	36.6%	38.5%	42.4%	32.1%	35.8%	14.0%
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	30.7%	31.3%	32.2%	33.3%	30.7%	9.3%
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	28.1%	32.4%	32.2%	27.8%	20.4%	11.6%
サービス事業者からのサポート体制が充実している	22.7%	31.8%	21.2%	24.1%	16.1%	9.3%
サービスの知名度や市場シェアが高い	20.1%	26.8%	19.6%	24.1%	10.9%	9.3%
電子証明書による電子署名ができる機能がある	19.3%	24.0%	20.4%	20.4%	13.9%	7.0%
サービス利用終了時のデータの取り扱いが契約上明確になっている（データの完全消去など）	17.5%	25.7%	15.9%	16.7%	11.7%	14.0%
電子契約データや各種ログ（操作ログやアクセスログなど）をエクスポート（出力）できる機能がある	15.3%	19.6%	15.5%	15.4%	11.7%	7.0%
タイムスタンプを付与する機能がある	14.0%	18.4%	13.5%	17.9%	7.3%	4.7%
自社の基幹業務システム（会計や経理システムなど）と連携ができる	12.9%	22.3%	10.2%	14.2%	5.1%	9.3%
分からない	4.0%	4.5%	1.6%	3.1%	4.4%	18.6%

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、導入がひと段落したとみられる。当事者型の利用が依然として多いが、立会人型と当事者型の両方を利用する企業が増加傾向にあり、電子契約の柔軟な運用を行う企業が増えてきていると考えられる。

- 電子契約の大きな効果は、コスト削減と業務効率化である。特に利便性の高い立会人型はコスト削減効果が大きいことが示されている。また、契約時のセキュリティの強化が図られることも電子契約の効果として重要な点である。

- 電子契約サービスを選定する際は、利用したい契約形態のサービスが提供されているかどうかと、電子証明書の信頼性が主に重視される。さらに、サービス事業者が、ISMS認証のような第三者機関の認証・認定を取得しているかどうかも選定に（立会人型サービスの選定では特に）強く影響していることも明らかになった。

報告する調査項目

1. DXの実践状況

2. 電子契約の利用状況

3. 生成AIの利用と課題

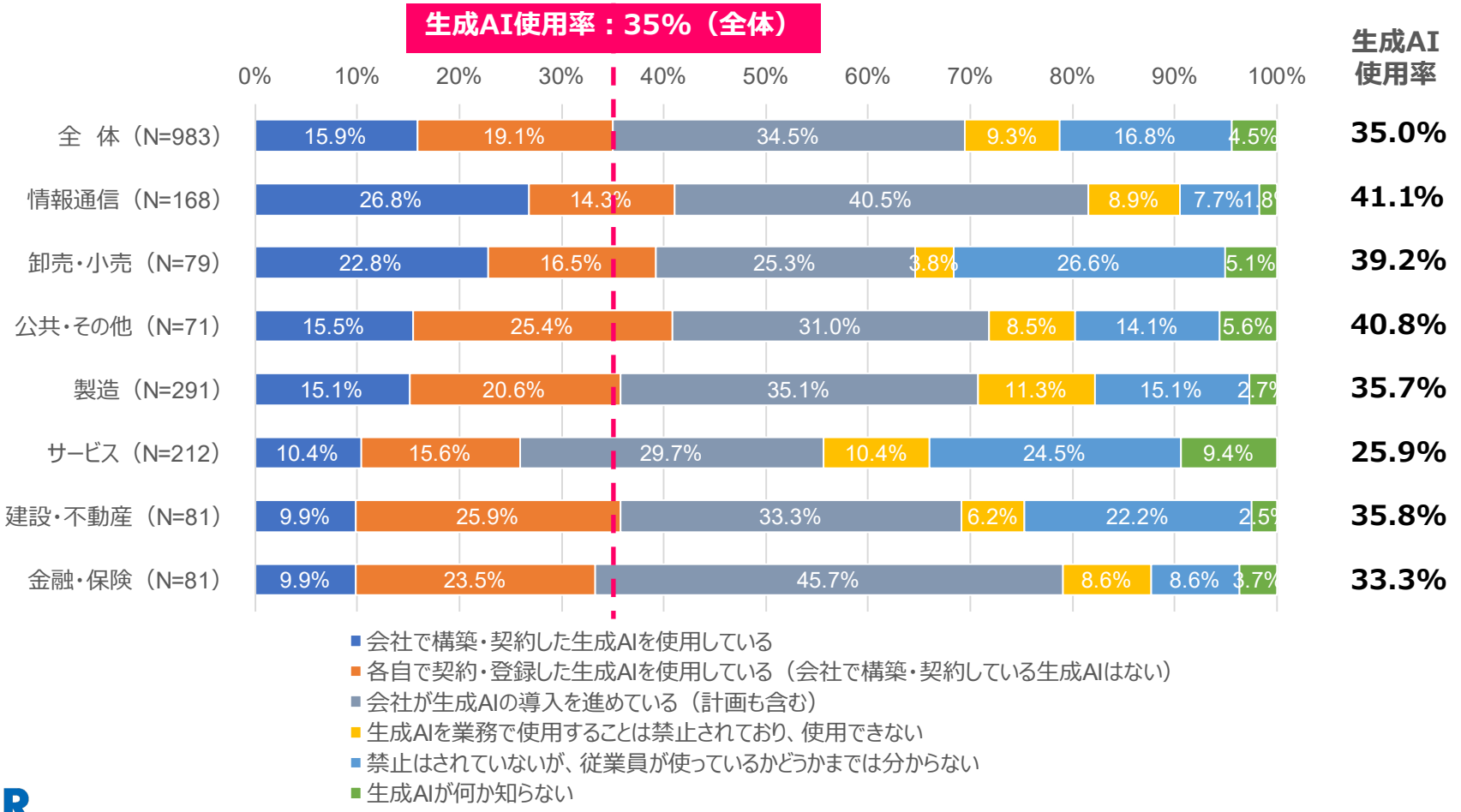
4. セキュリティのインシデントと対策

5. プライバシー保護に対する取り組み

6. 第三者認定／認証制度の取得状況

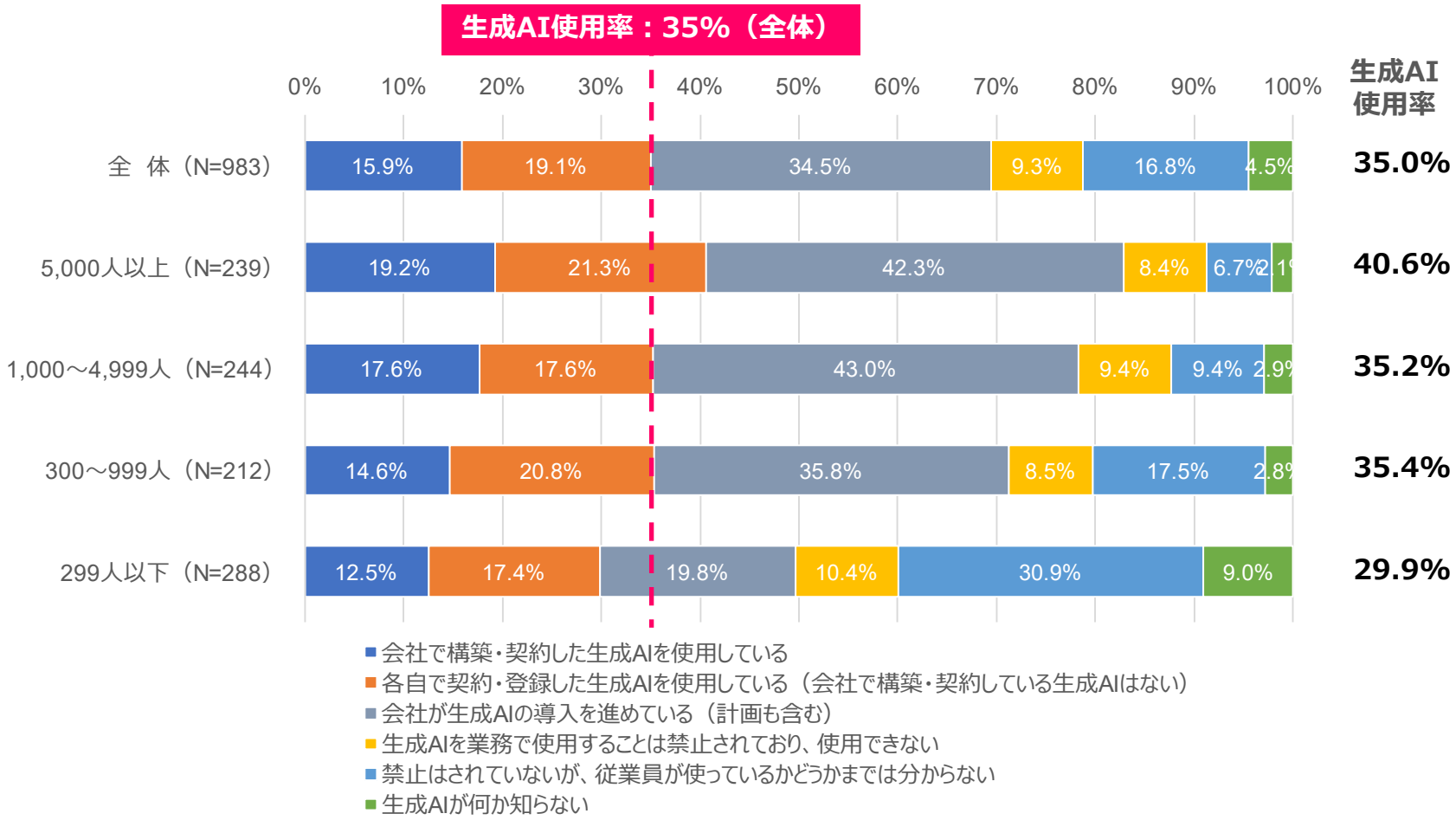
3.1　業務における生成AIの使用状況：全体と業種別

- 業務での生成AI使用率は35.0%、導入を進めているのは34.5%となり今後の急拡大が見込まれる。
- 会社で構築・契約した生成AIよりも各自が契約・登録した生成AIの使用割合の方が大きい状況にある。
- 「情報通信」と「卸売・小売」は会社で構築・契約した生成AIの使用割合が20%以上と大きい。
- 「金融・保険」は現状の使用率はやや低いが、会社で導入を進めているのは45.7%と非常に高い。



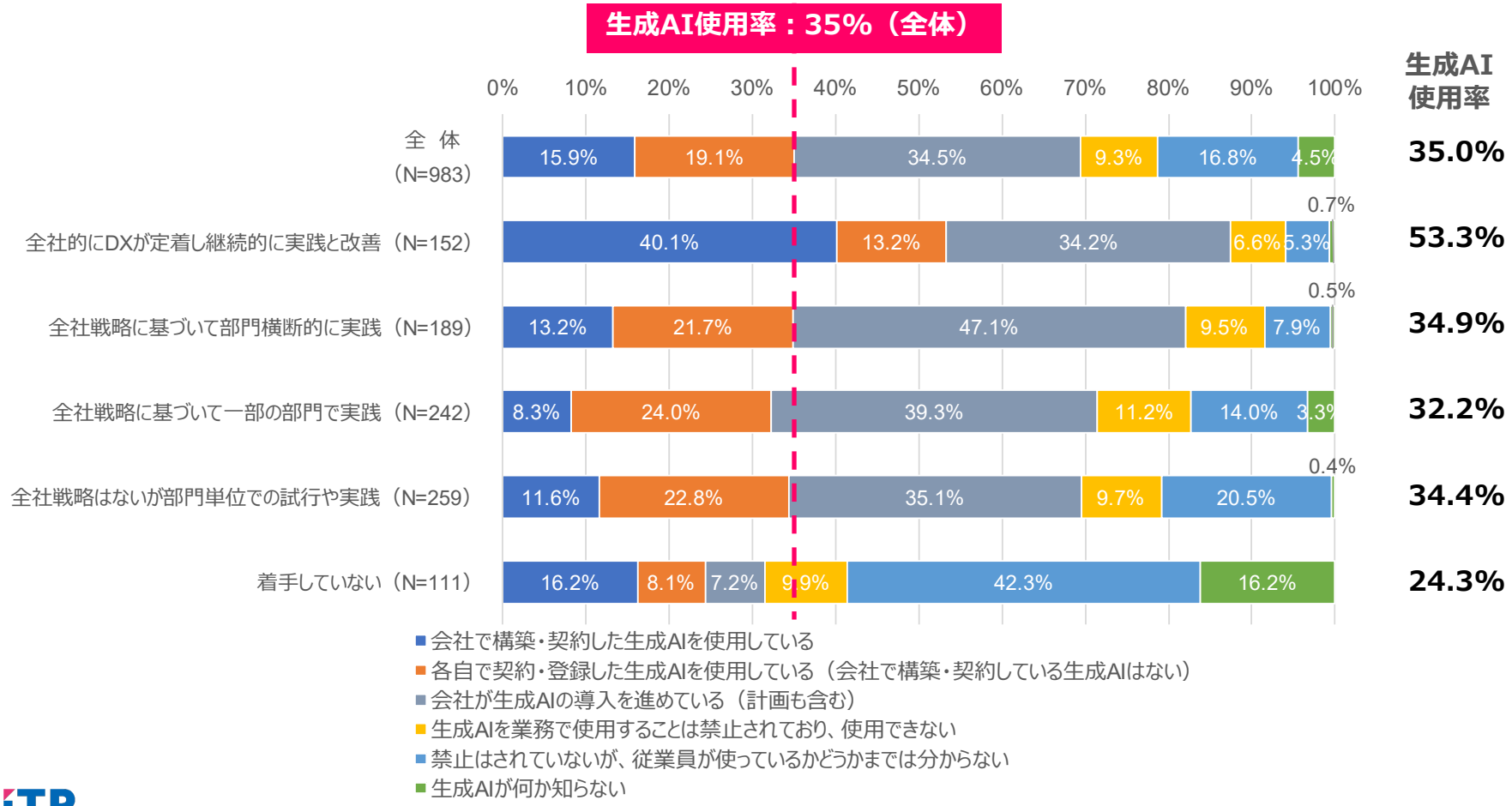
3.2　業務における生成AIの使用状況：従業員規模別

- 従業員規模が大きくなるにしたがい、生成AIの使用率も上昇していく。
- 「999人以下」では、会社で構築・契約した生成AIよりも各自が契約・登録した生成AIの使用割合の方が大きくなっていることが顕著に見られる。



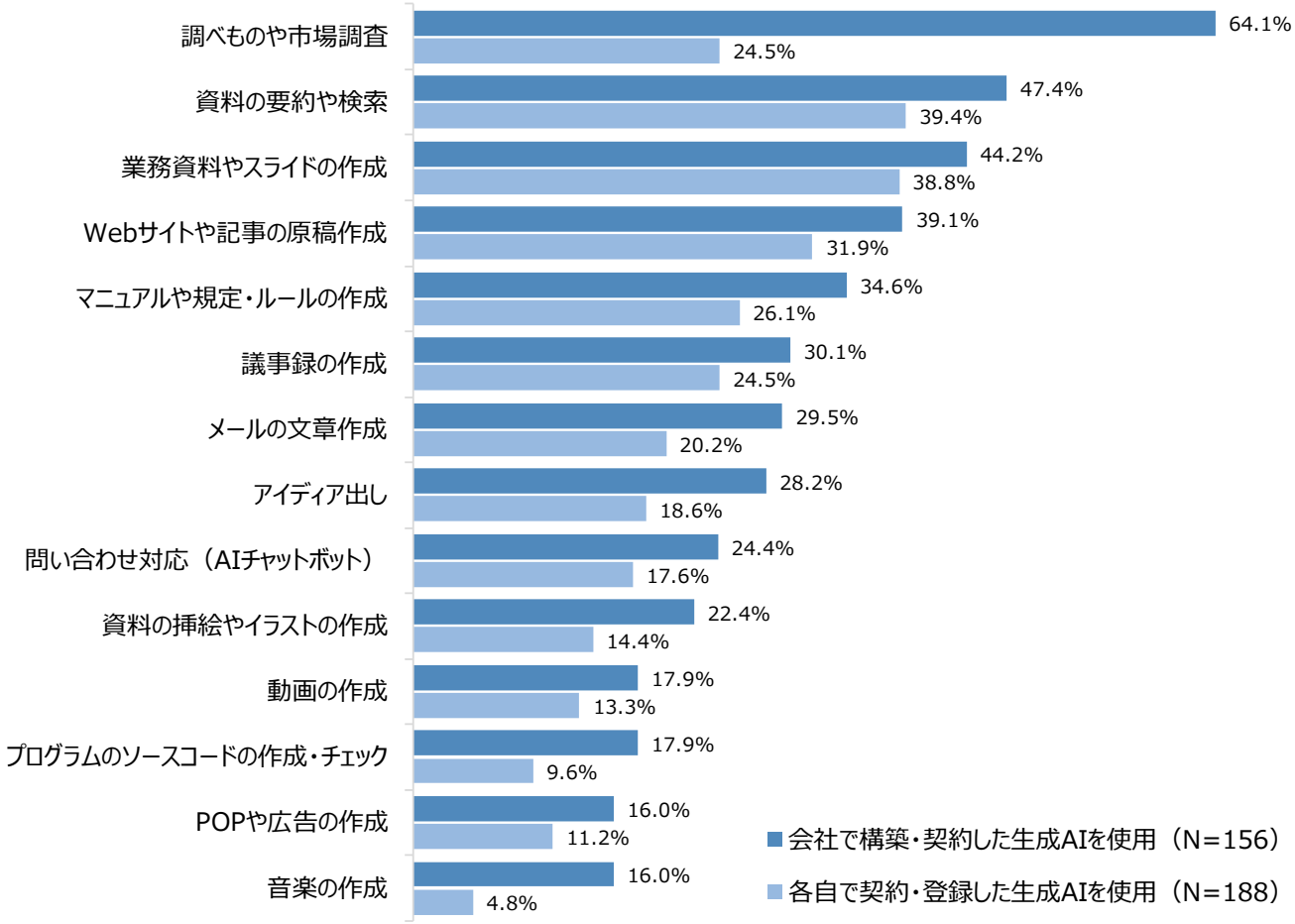
3.3　業務における生成AIの使用状況：DX実践段階別

- 「DX定着」企業は生成AIの使用率が50%以上、さらに会社で構築・契約した使用が40.1%と非常に割合が大きく、会社として戦略的に生成AIを利用している状況がうかがえる。
- それ以外の段階の企業は、現時点では各自で契約・登録した使用割合の方が大きく、場当たり的な利用となっている。しかし、導入を進めている企業が多く、今後は戦略的な利用にシフトしていく。



3.4　生成AIを使用している業務

- 会社で構築・契約して使用している企業は、「調べものや市場調査」が最も多いが、各自が契約・登録して使用している企業はそれほどではない。
- その他の主な用途としては「資料の要約や検索」や「業務資料やスライドの作成」など資料作成業務、「Webサイトや記事の原稿作成」などがある。



3.5　生成AIを使用している業務：業種別

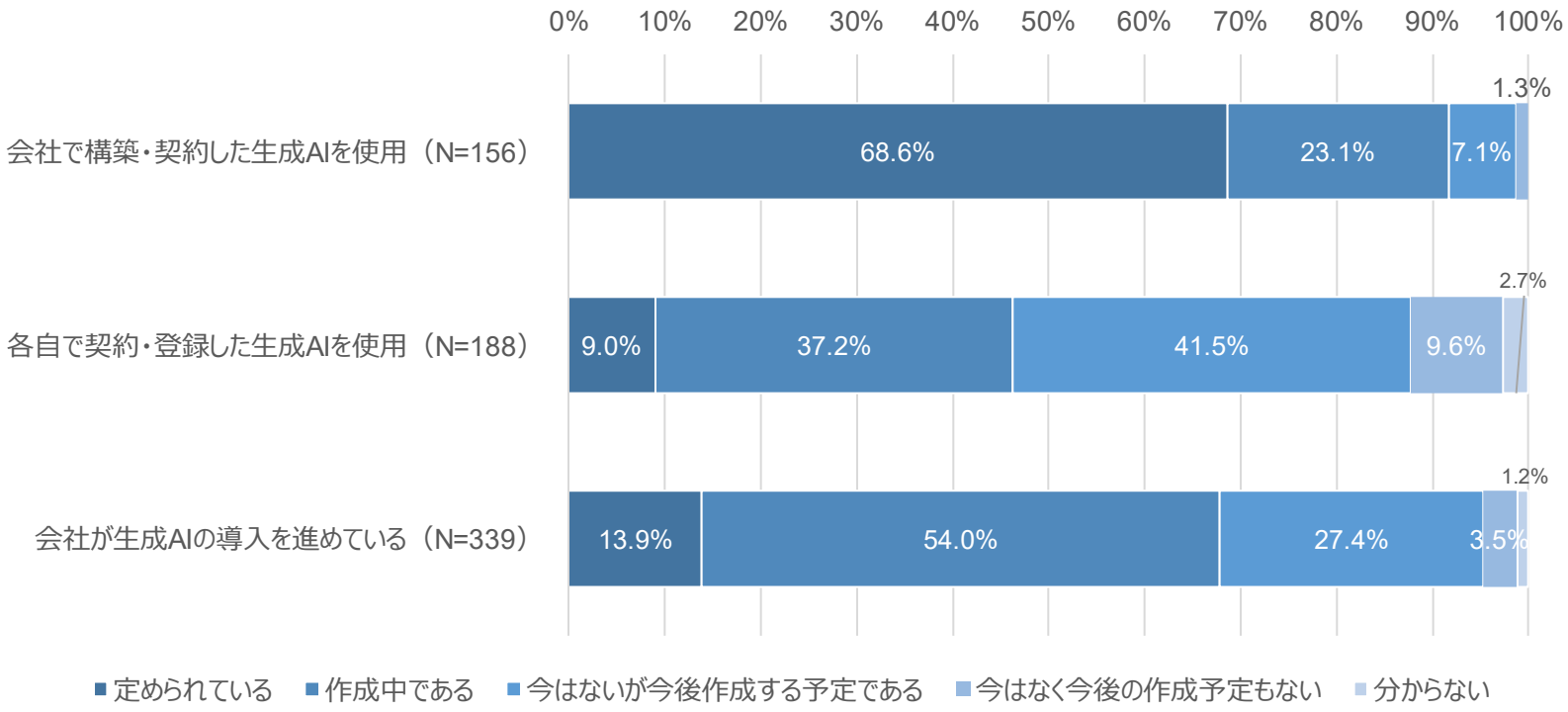
- 「卸売・小売」は、メール文章作成やアイディア出し、問い合わせ対応、イラストの作成など、他の業種よりも用途が多様である。
- IT業務において期待されている生成AIによるソースコードの作成やチェックは、まだそれほど適用されていないという状況が見てとれる。情報通信でも18.9%の使用率にとどまっている。

	全 体 (N=363)	情報通信 (N=74)	卸売・小売 (N=32)	公共・その他 (N=30)	製造 (N=110)	サービス (N=59)	建設・不動産 (N=29)	金融・保険 (N=29)
調べものや市場調査	42.4%	60.8%	46.9%	40.0%	37.3%	42.4%	31.0%	24.1%
資料の要約や検索	42.4%	45.9%	46.9%	63.3%	29.1%	52.5%	48.3%	31.0%
業務資料やスライドの作成	40.5%	32.4%	37.5%	40.0%	42.7%	39.0%	48.3%	51.7%
Webサイトや記事の原稿作成	34.7%	31.1%	37.5%	46.7%	31.8%	42.4%	37.9%	20.7%
マニュアルや規定・ルールの作成	28.9%	32.4%	31.3%	26.7%	26.4%	22.0%	41.4%	31.0%
議事録の作成	26.7%	25.7%	28.1%	23.3%	21.8%	35.6%	37.9%	20.7%
メールの文章作成	24.2%	21.6%	43.8%	26.7%	16.4%	30.5%	34.5%	13.8%
アイディア出し	22.3%	28.4%	37.5%	23.3%	17.3%	20.3%	27.6%	6.9%
問い合わせ対応（AIチャットボット）	20.1%	17.6%	28.1%	20.0%	15.5%	30.5%	20.7%	13.8%
資料の挿絵やイラストの作成	17.4%	14.9%	28.1%	23.3%	13.6%	20.3%	17.2%	13.8%
動画の作成	14.9%	8.1%	25.0%	23.3%	13.6%	16.9%	20.7%	6.9%
POPや広告の作成	13.2%	16.2%	15.6%	20.0%	8.2%	11.9%	17.2%	13.8%
プログラムのソースコードの作成・チェック	13.2%	18.9%	15.6%	13.3%	12.7%	10.2%	13.8%	3.4%
音楽の作成	10.2%	5.4%	15.6%	30.0%	8.2%	11.9%	3.4%	6.9%

※「会社で構築・契約した生成AIを使用」もしくは「各自で契約・登録した生成AIを使用」の回答者

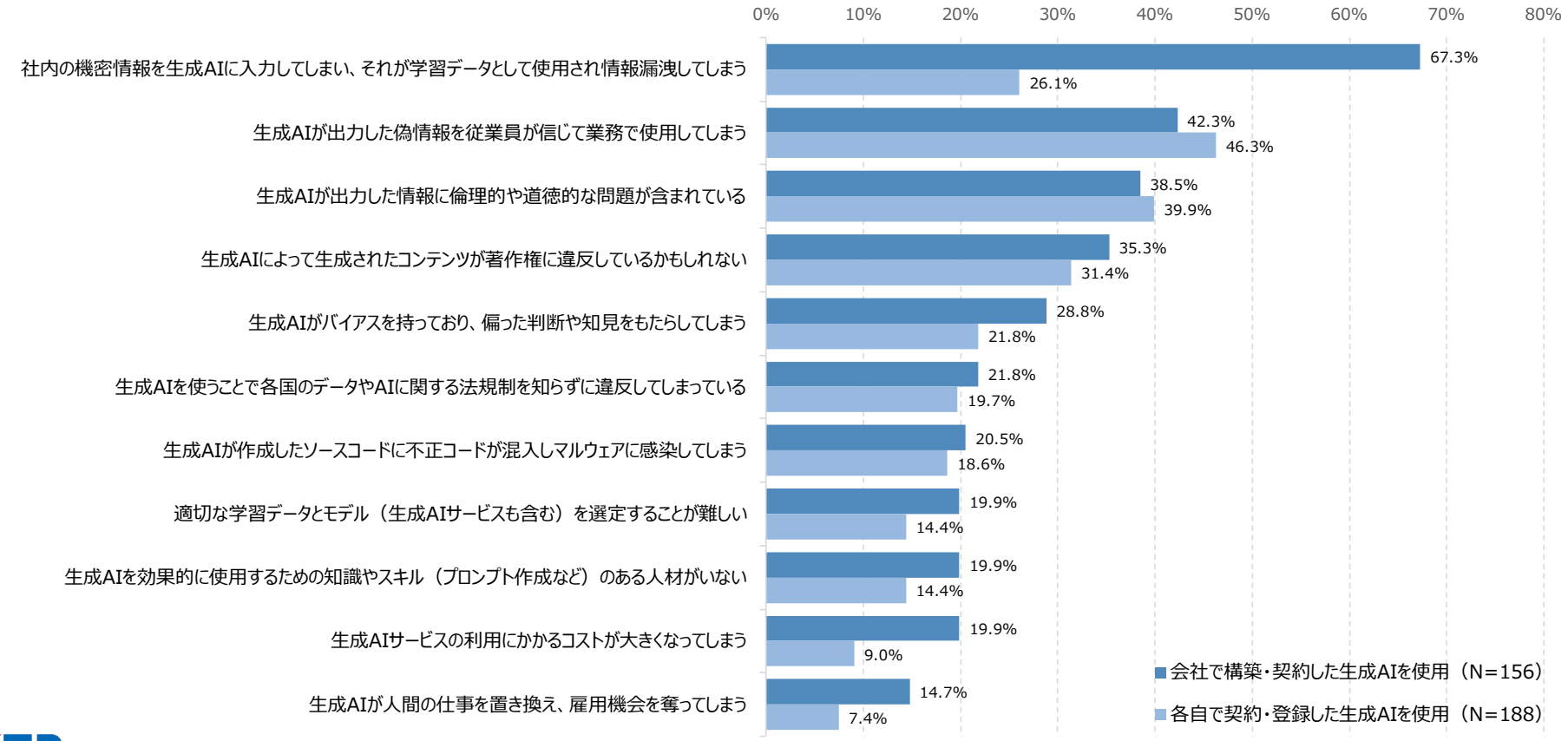
3.6　生成AIに関する利用規定・ガイドラインの策定状況

- 会社で構築・契約して使用している企業の3分の2以上は、生成AI使用時のプロンプト入力の際の情報の取り扱いのルールや禁止事項などを利用規定・ガイドラインで定めている。
- 一方、各自で契約・登録して使用している企業のほとんどは利用規定・ガイドラインを定めておらず、ほとんどが作成中・作成予定となっている。
- 現在生成AIの導入を進めている企業の約半数は、導入に合わせて作成を進めている。



3.7　生成AIの業務使用における懸念点

- 会社で構築・契約して使用している企業における「社内機密情報の入力による情報漏洩」への懸念は大きい。一方で、各自で契約・登録して使用している企業はさほどでもなく、危機感が薄い。
- 「生成AIが出力した偽情報を信じて使用」を懸念している企業も多い。AIは事実と異なる情報を生成することがあり（ハルシネーション）、誤った意思決定や顧客からの信頼性低下を招く恐れがある。
- その他、「倫理的や道徳的な問題（差別的な表現の生成など）」、「生成したコンテンツの著作権違反」、「バイアスを持った情報の生成」などへの懸念が出ている。



3.8　生成AIの利用と課題：調査結果からの考察

- これから企業における生成AIの利用は、急速に拡大するとみられる。現状においては、従業員個人で登録した生成AIを使用する企業の方が多いという状況にあるが、それは一時的であり、今後は生成AIサービスを法人契約する企業が多くなるであろう。

- 現状における生成AIの主な用途は調査や資料作成であるが、メールの文章作成やアイディア出し、問い合わせ対応など多様な業務への適用が見込まれる。ただし、ソースコードの自動生成への適用にはある程度の時間がかかるとみられる。

- 生成AIを使用する上で懸念が多いリスクは、情報漏洩とハルシネーションとなっている。特にプロンプト入力の際における機密情報の取り扱いは十分に注意する必要がある。また、差別的表現と著作権侵害についてのリスク意識も高くなっている。

- 生成AIで想定されるリスクを軽減し安全に利用するためには、利用規定やガイドラインの策定が必須である。特に個人で登録した生成AIを業務で使用させている企業は、策定が進んでおらずリスクに晒されており、早急に対応すべきである。

（参考）生成AIの利用規定・ガイドライン策定の必要性

■ 生成AIには様々なリスクが存在し、企業の評判を大きく低下させる結果を招く恐れがある。

生成AIを利用する際のリスク

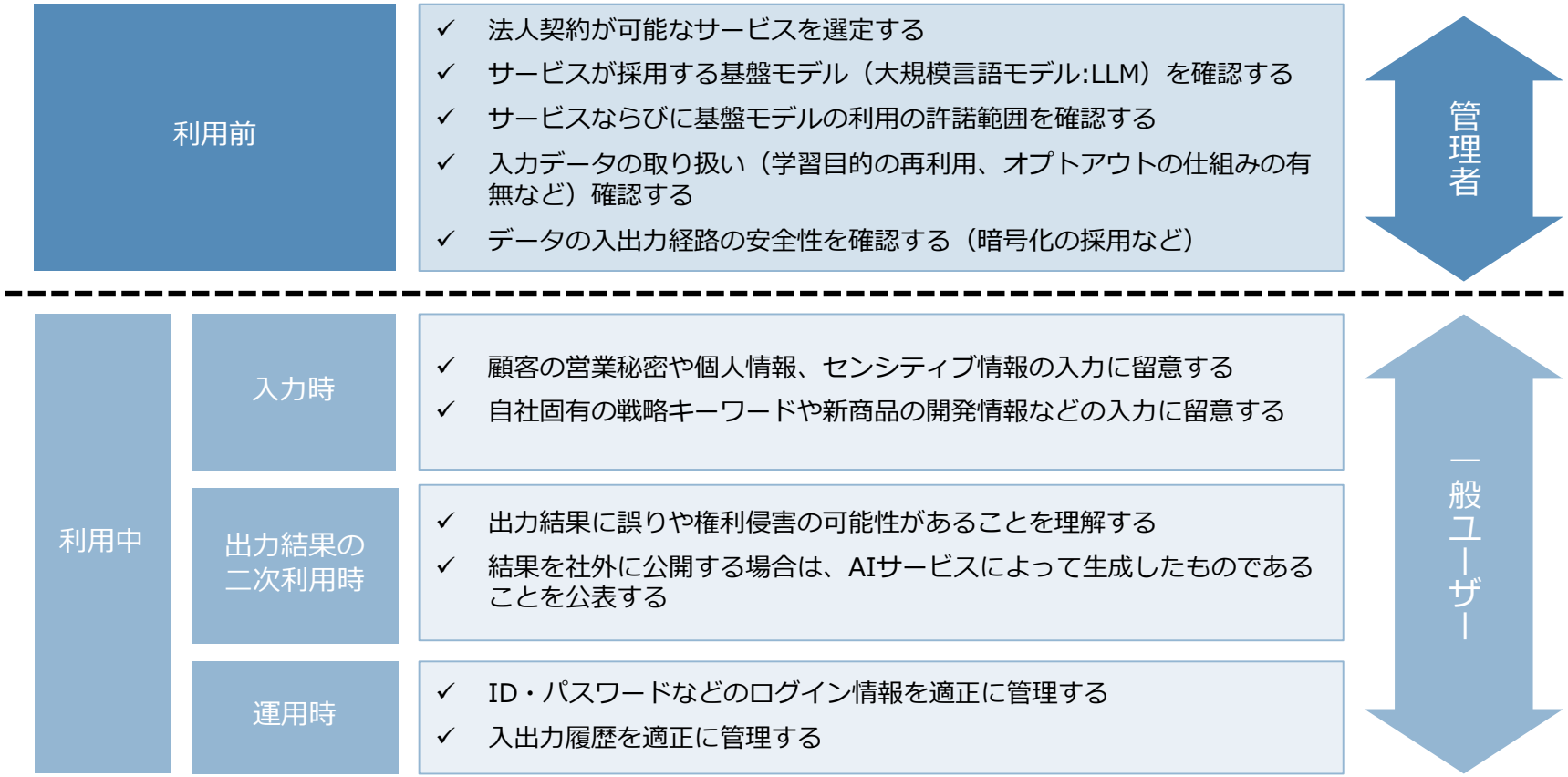
分類		概要
1	機密性	• プロンプト入力を通じた個人情報、営業秘密情報の漏洩 • アカウント情報の漏洩による企業戦略の流出 • 中間者攻撃や不正アプリケーションなどによる情報漏洩
2	正確性	• 不正確なコンテンツの生成（ハルシネーション） • バイアス（偏り）のある表現の生成
3	倫理性	• 不公平や差別的な表現の生成 • 攻撃的な表現の生成
4	法適合性	• 生成コンテンツの2次利用による権利侵害
5	透明性	• モデルのブラックボックス化による説明責任の欠如
6	コスト	• 導入費用／ライセンス費用の増大 • 教育・トレーニング費用の増大
7	組織風土・文化	• 少数意見が無視されることによる多様性の低下 • 生成コンテンツを介したコミュニケーションに依存することによる関係性の悪化

出典：ITR

（参考）生成AIの利用規定・ガイドライン策定の必要性

■ リスクを低減するためには、生成AIの利用に関する規定やガイドラインを策定することが望ましい。

生成AIのガイドライン策定に向けたチェックリストの例



出典：ITR

報告する調査項目

1. DXの実践状況

2. 電子契約の利用状況

3. 生成AIの利用と課題

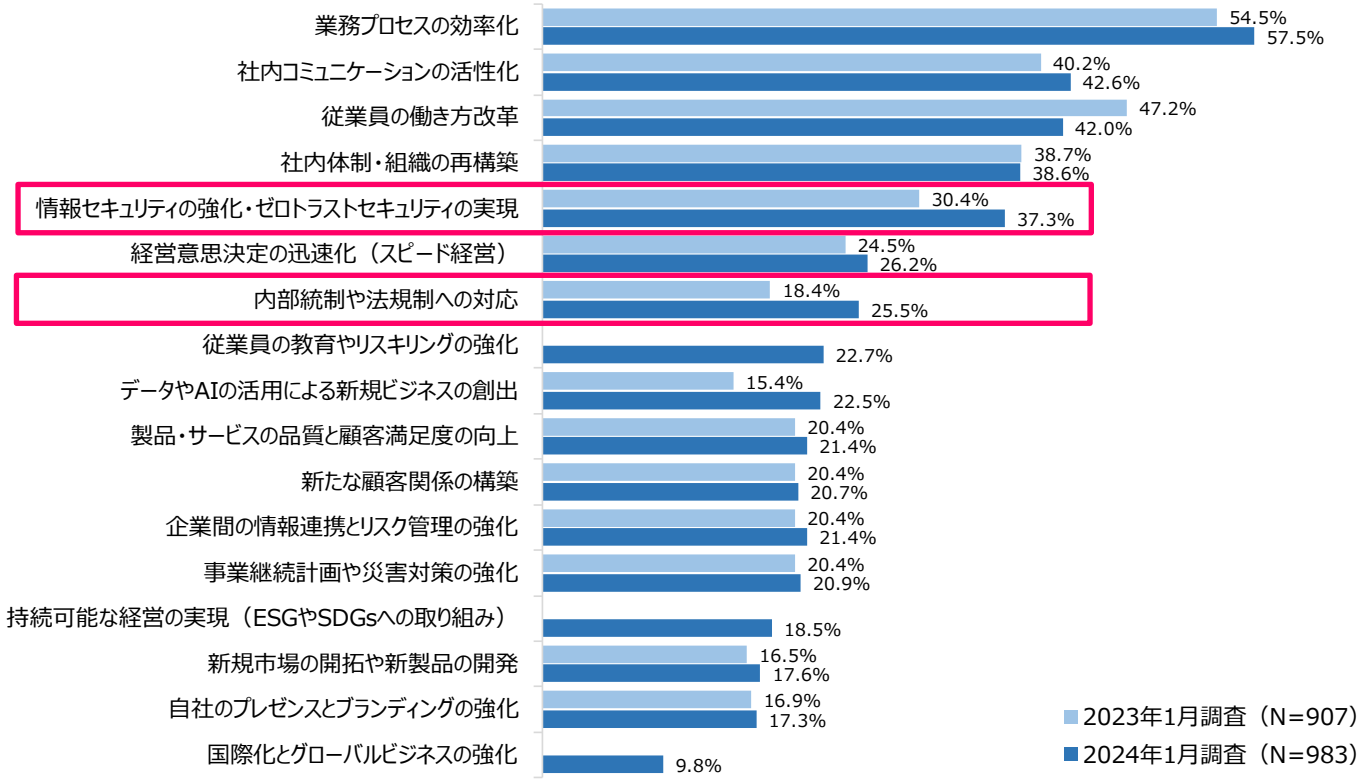
4. セキュリティのインシデントと対策

5. プライバシー保護に対する取り組み

6. 第三者認定／認証制度の取得状況

4.1　今後に向けて重視していく経営課題

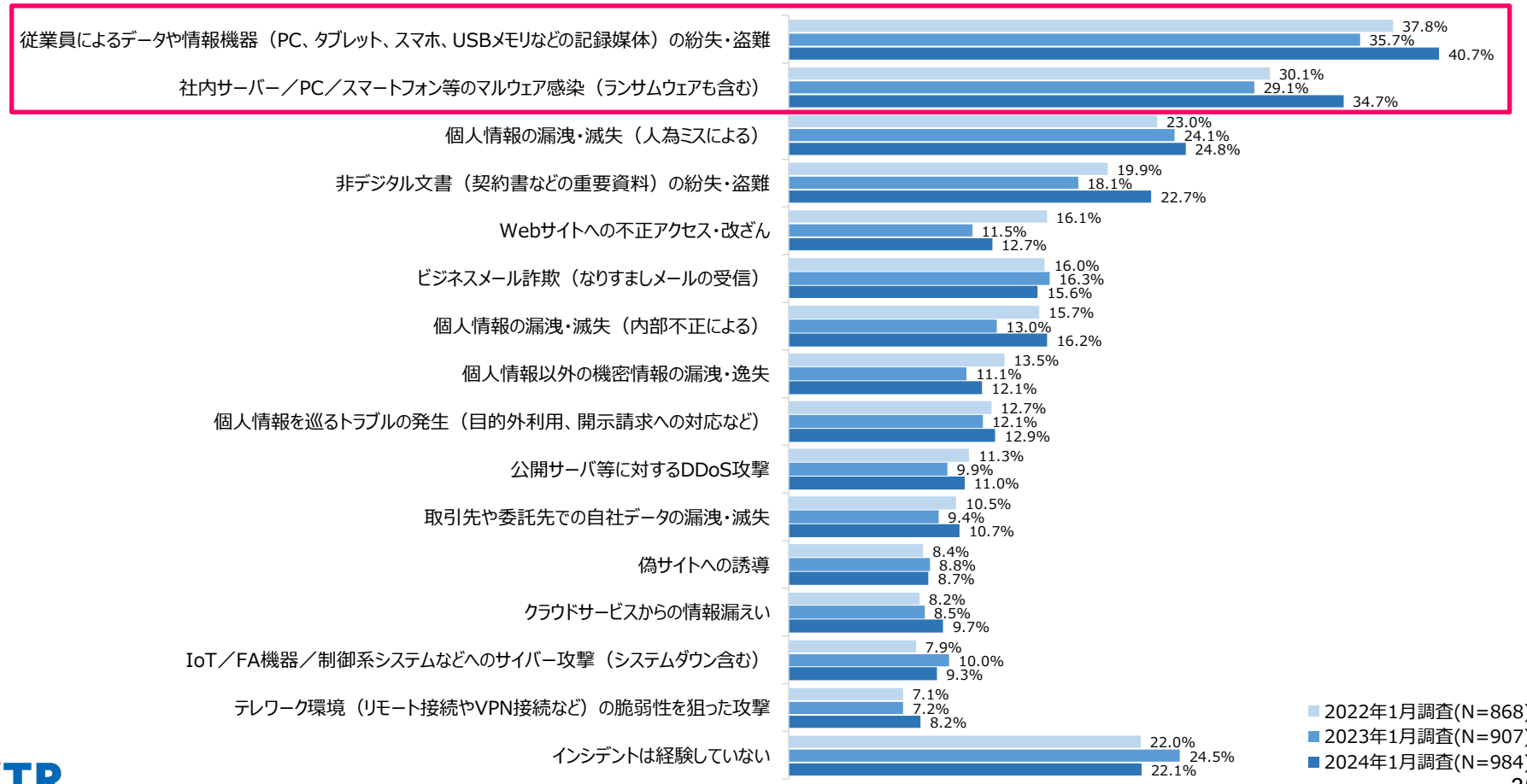
- 「情報セキュリティの強化・ゼロトラストセキュリティの実現」が前回調査から大きく上昇し、上位3つの課題に迫っている。これからの経営においてセキュリティの重要性がより高まっていく。
- 「内部統制や法規制への対応」も上昇し、コンプライアンス対応の重要性も高まっている。



注1：「従業員の教育やリスキリングの強化」「持続可能な経営の実現（ESGやSDGsへの取り組み）」「国際化とグローバルビジネスの強化」は2024年1月調査で新たに選択肢に追加
注2：「内部統制や法規制への対応」は2023年1月調査では「法規制への対応（内部統制／J-SOX）」としている
注3：「データやAIの活用による新規ビジネスの創出」は2023年1月調査では「ビッグデータ活用によるビジネス機会の創出」としている
注4：上記の他にも2023年1月調査から選択肢の内容は変わらない程度の変更を行った選択肢がある

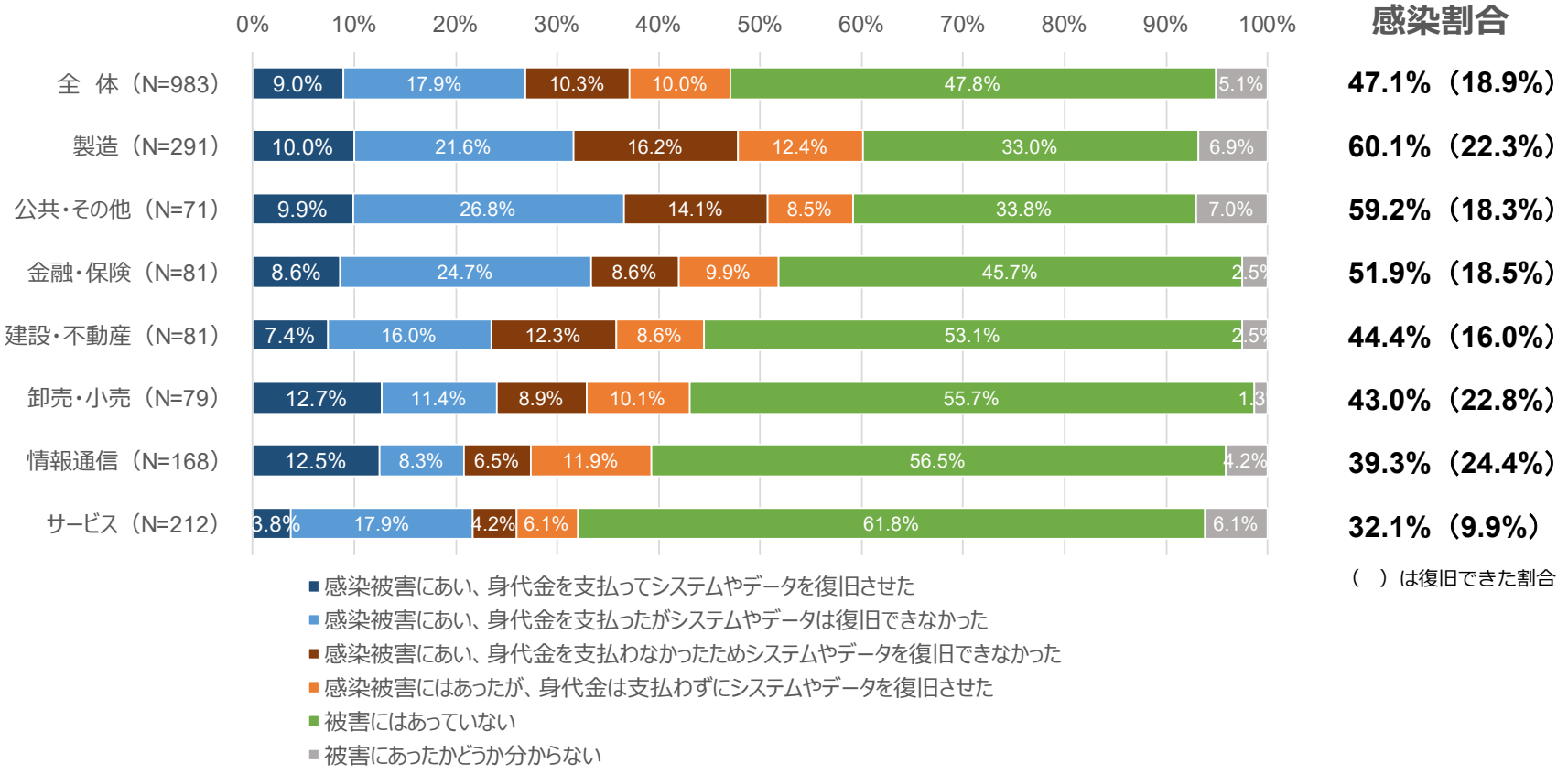
4.2　過去1年間のセキュリティ・インシデントの発生状況

- 「従業員によるデータや情報機器の紛失・盗難」が最も多く、前回調査から5ポイント上昇し40%を超えた。「個人情報の漏洩・滅失（人為ミスと内部不正の両方）」や「非デジタル文書の紛失・盗難」も含め、従業員に起因するインシデントが増加している状況にある。
- 「マルウェア感染（ランサムウェア含む）」も前回調査から5ポイント以上も上昇しており、外部攻撃によるインシデントも増加している。内部・外部双方のインシデントが拡大している状況にある。



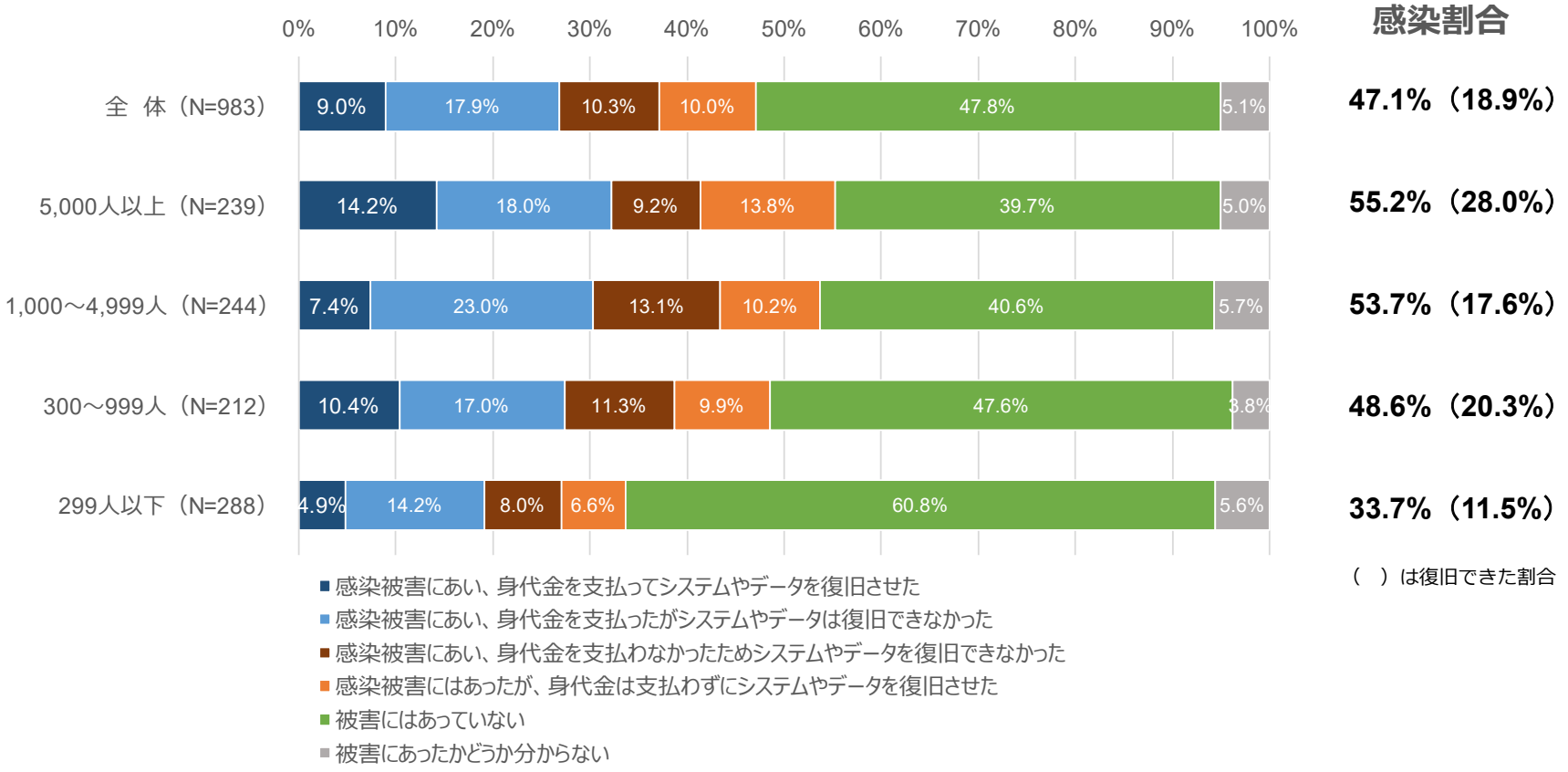
4.3　ランサムウェアの感染被害の経験：全体と業種別

- ランサムウェアの感染被害を経験した企業は47.1%。そのうち身代金を支払った企業は26.9%であるが、システムやデータを復旧できたのは18.9%にとどまっている。身代金を支払ったものの復旧できなかった企業は17.9%となった。感染すると身代金の支払い有無によらず復旧は困難な状態になる。
- 最も感染割合が高いのは「製造」で60.1%、その次に「公共・その他」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。この3つの業種はおよそ3分の1程度しか復旧できていない。



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。「1,000人～4,999人」と「5,000人以上」では感染割合が50%以上であり、特に「1,000人～4,999人」は復旧できた割合が低い。
- 「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。



（参考）ランサムウェアの感染事例

- 報告されているランサムウェアの感染経路の多くは、VPN機器の脆弱性や強度の弱い認証情報が悪用されている。（警察庁調査[注1]によると感染経路の71%がVPN機器からの侵入）
- 子会社や取引先から侵入されて社内ネットワークにまで侵入されるサプライチェーン攻撃も増加。
- バックアップデータも暗号化されると復旧が困難になる。

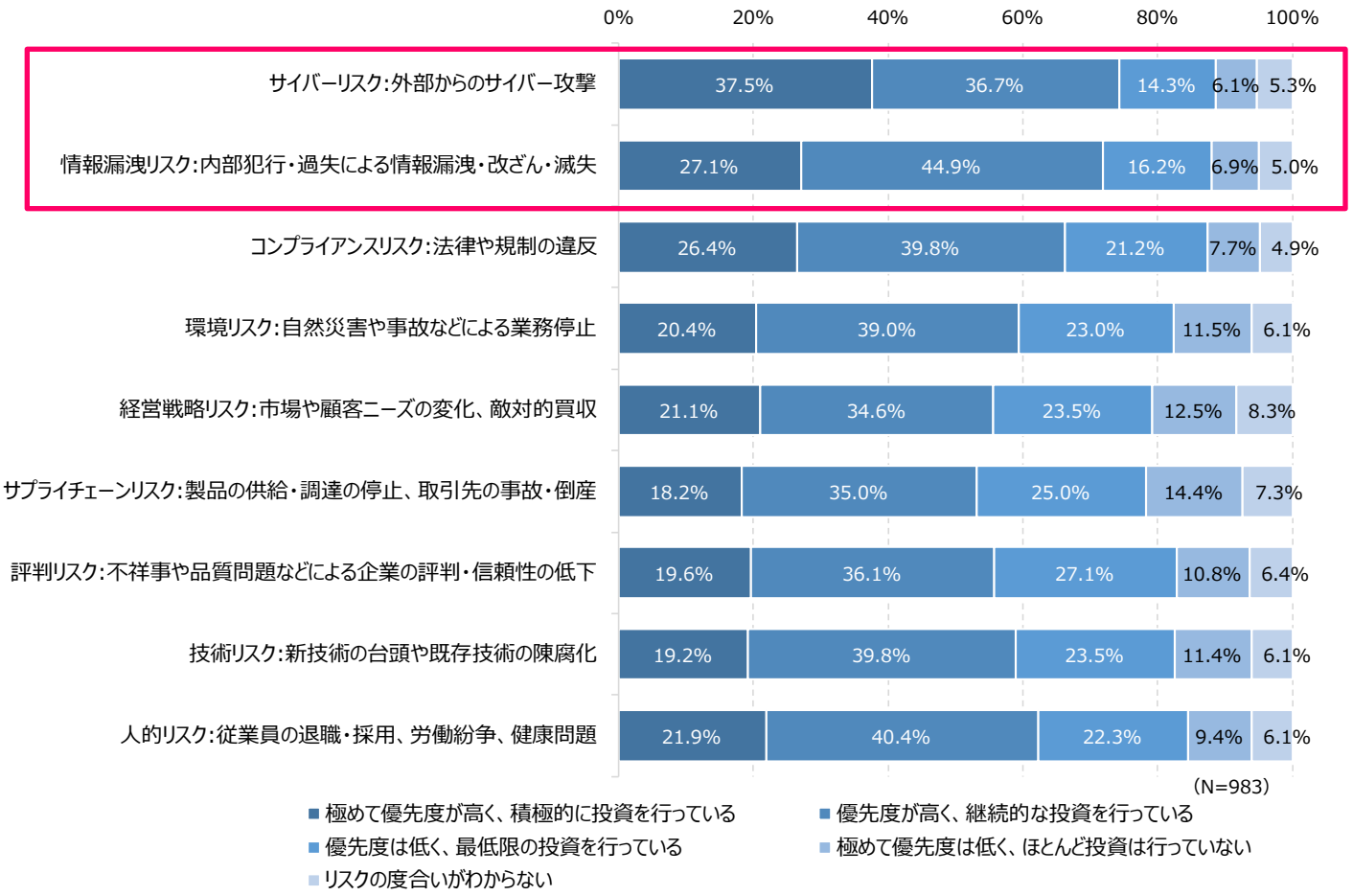
注1：警察庁「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」

A社	A社の子会社が利用するリモート接続機器の脆弱性が悪用され、子会社の社内ネットワークに侵入され、そこからさらにA社の社内ネットワークに侵入され、サーバやPCに保存されていたデータが暗号化された。給与システムや受発注システムにまで被害が及び、A社が関連する工場が全て停止された。
B病院	B病院に給食を提供している事業者のデータセンターにあるVPNの脆弱性または漏洩により公開されていた認証情報を悪用し、データセンターへ侵入。さらに給食事業者のサーバーからB病院のサーバーに侵入され（給食事業者のサーバーからB病院のサーバーに常時リモートデスクトップによる接続があった）、サーバーのファイルが暗号化された。手術や外来診療の停止を余儀なくされた。
C社	VPN機器の脆弱性を悪用して認証情報が窃取され、社内ネットワークに侵入された。攻撃者が何らかの方法で、認証サーバー（Active Directory）の管理者情報を乗っ取り、ドメイン管理下でPCやサーバに対して感染被害を広げたことで、数百台が暗号化の被害を受けた。
D社	VPN接続において、多要素認証などの不正ログイン対策が不十分であり、さらにパスワードの設定がが英数字や数字のみといった脆弱な状態で運用していたことから、総当たり攻撃などの方法で認証を突破されて侵入され、サーバーとPC、NASが暗号化された。また、Windowsのリモートプログラム実行ツールであるPSexec が悪用されて、被害が拡大した。
E社	VPN装置の脆弱性の悪用により侵入され、サーバ内のファイルが暗号化された。サーバ内の数万件の個人情報も流出した。さらに、データが暗号化された状態でバックアップ処理をしていたため、バックアップサーバにも影響が及んだ。

出典：企業が公開したランサムウェア被害調査報告書や「コンピュータウイルス・不正アクセスの届出事例（IPA）」の情報を基にITRが作成

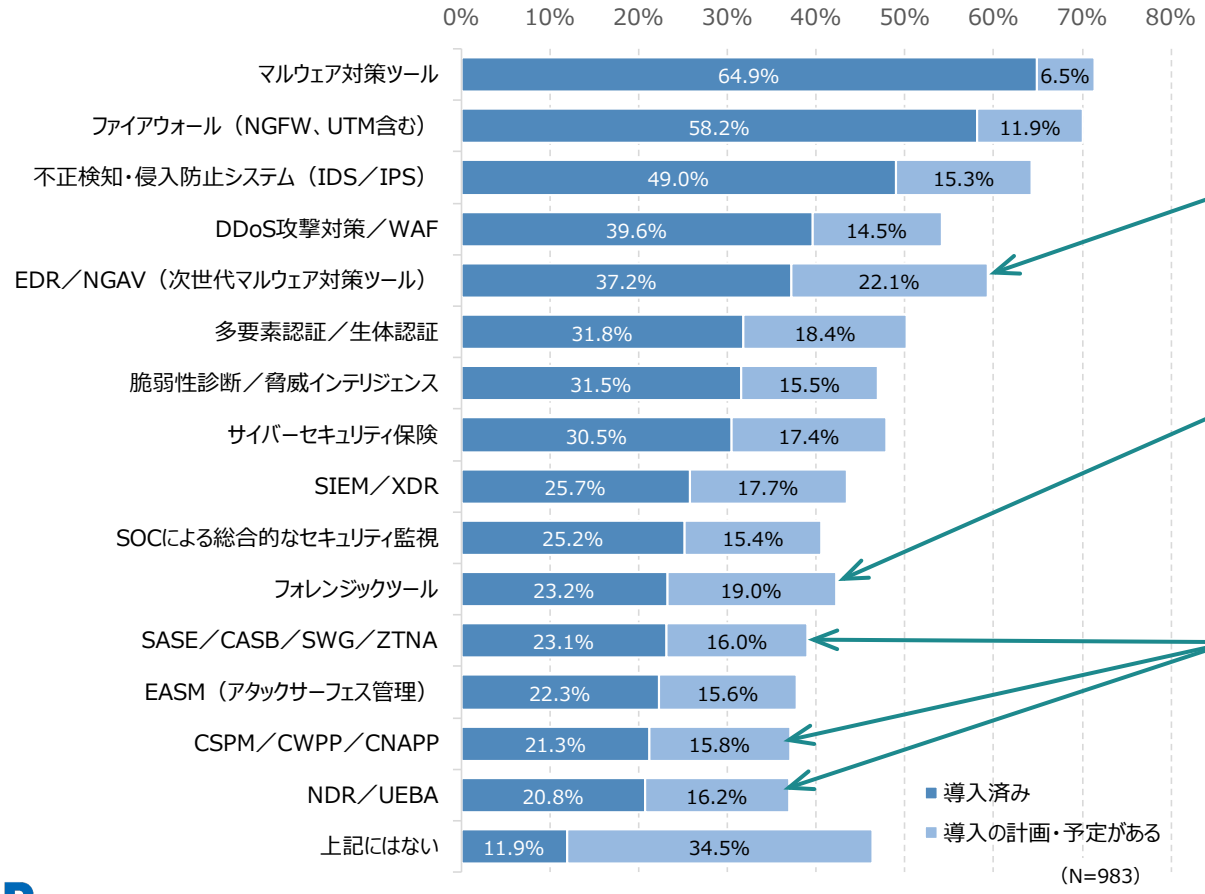
4.5　経営リスク対策への投資優先度

- ランサムウェアなどサイバー攻撃による「サイバーリスク」の対策について、約75%が優先的に投資を行っていると回答し、そのうちの約半数は積極的に投資を行っているとしている。
- 内部の不正や過失による「情報漏洩リスク」の対策についても約70%が優先的に投資を行っている。
- 企業では、内部・外部双方に対するセキュリティ対策への投資の優先度が高まってる状況にある。



4.6　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」にような次世代型ツールの導入も進んでいる。
- インシデント発見後の調査を行う「フォレンジックツール」に対するニーズの高まりがみられる。
- 「SASE／CASB／SWG／ZTNA」や「CSPM／CWPP／CNAPP」などゼロトラスト・セキュリティを実現するためのツールも徐々に導入が進んでいくとみられる。



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ふるまい検知が可能なEDRやNGAVの導入が進んでいる

サイバー攻撃による被害範囲の調査・特定や不正行為の原因究明を行うデジタルフォレンジックのニーズが高まりつつある

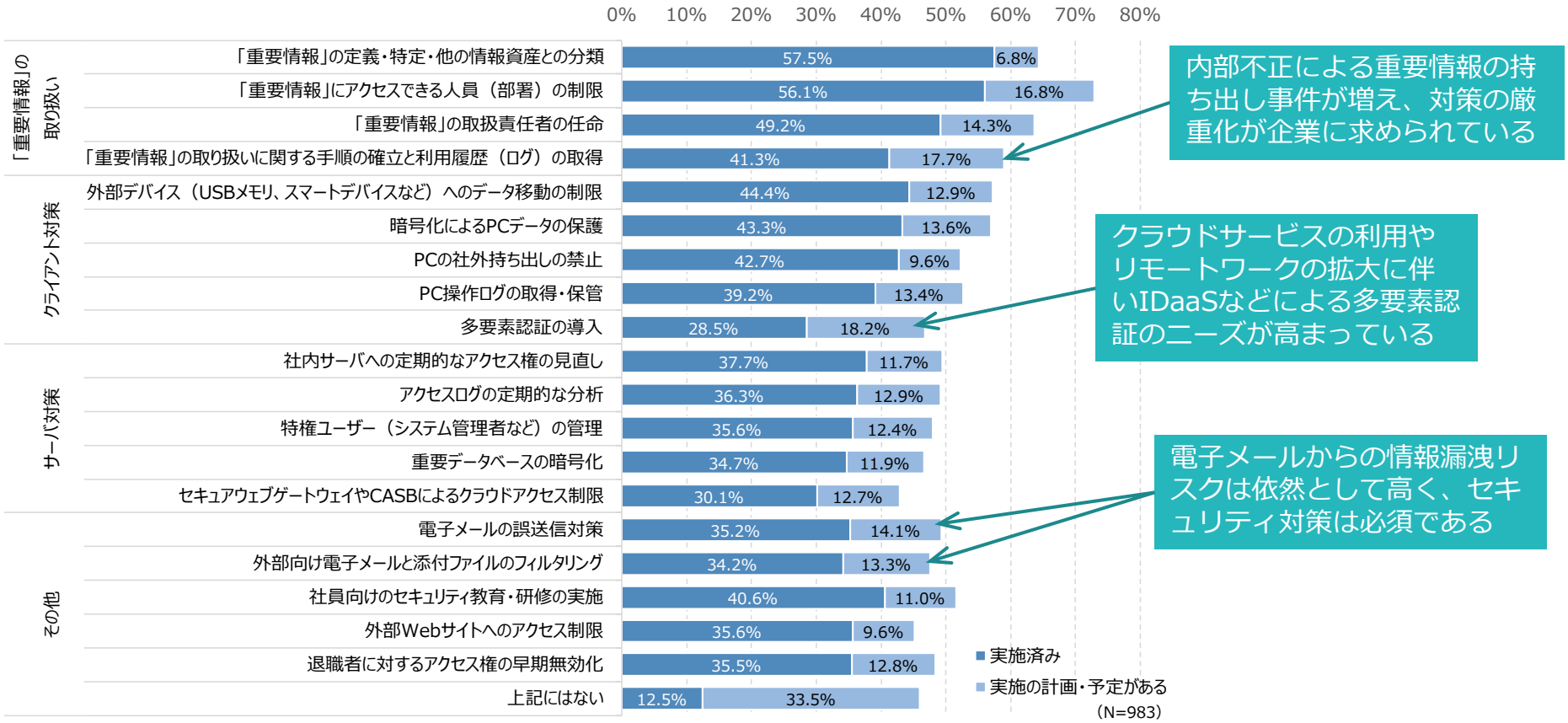
ゼロトラスト・セキュリティを構成するツール

（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

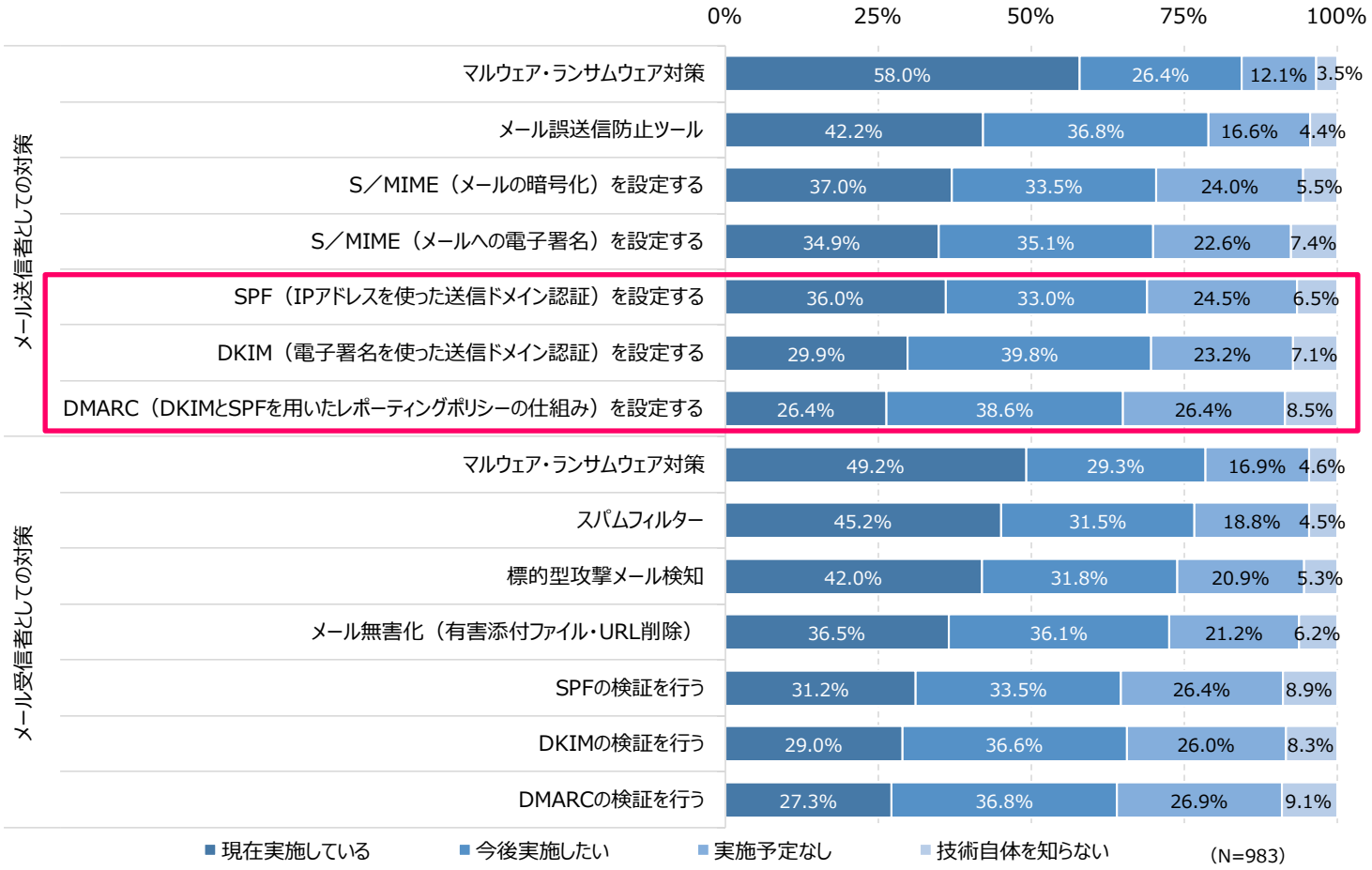
4.7　内部からの情報漏洩対策として実施している項目

- 「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増えつつある。
- クライアント対策では「多要素認証の導入」の実施率が30%未満となり最も低いが、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。



4.8　内部からの情報漏洩対策として実施している項目

- 受信者としての対策としては、「マルウェア・ランサムウェア対策」の実施率が58.0%で最も高く、「メール誤送信防止ツール」が42.2%、「S／MIME（暗号化）」が37.0%で続いている。
- 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」においては、「SPF」の実施率が36.0%と最も高く。「DKIM」と「DMARC」は、今後実施したい割合が40%近くあり、今後、対策が進んでいくことが期待できる。



4.9　セキュリティのインシデントと対策：調査結果からの考察

- ランサムウェアをはじめとするサイバー攻撃や内部からの情報漏洩などセキュリティのインシデントは増加傾向にある。特にランサムウェアは半数近い企業で感染被害の経験があるという驚くべき結果が出ている。脅威は身近に潜んでいる。

- 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ことが調査結果から明らかになった。このようなセキュリティリスクに対して、優先して対策への投資を行い、さらにそれを継続的に行わなければならない。

- アンチウイルスやファイアウォールなどによる境界防御型対策では限界があり、ランサムウェアや未知のマルウェアを防ぐのは難しい。EDRやSASEなど次世代型ソリューションを導入し、ゼロトラストセキュリティを実現することが求められる。

- 情報漏洩対策も引き続き重要な投資領域である。クラウドサービスやリモートワークの利用が拡大した今、多要素認証やCASBなどアクセス時のセキュリティ対策は重要であるが、まだ普及には至ってない状況にある。早急な対応が必要である。

報告する調査項目

1. DXの実践状況

2. 電子契約の利用状況

3. 生成AIの利用と課題

4. セキュリティのインシデントと対策

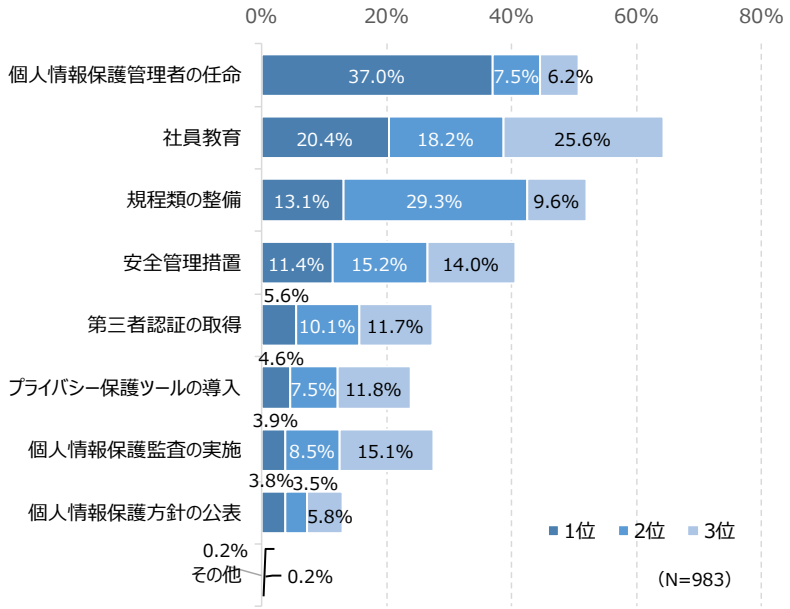
5. プライバシー保護に対する取り組み

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

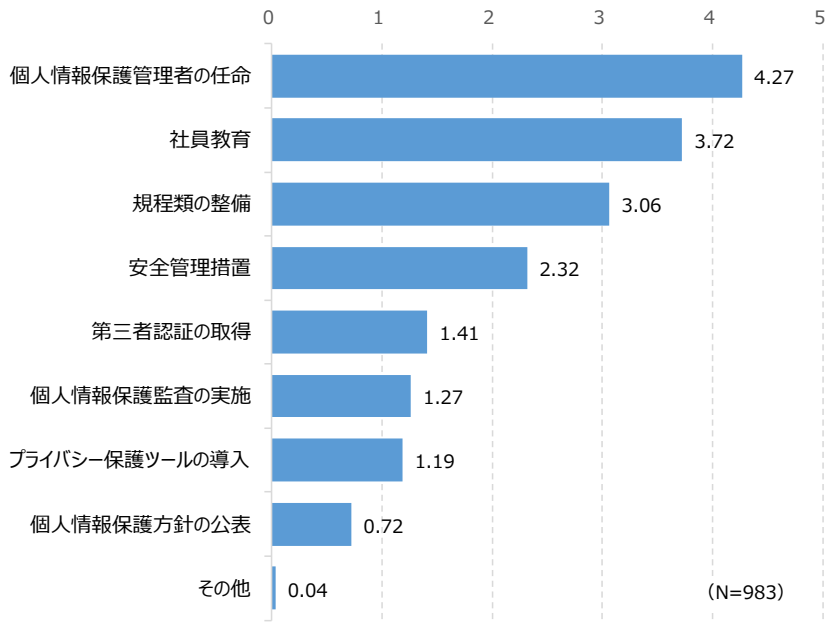
- 個人情報保護において注力している取り組みとして、「個人情報保護管理者の任命」を1位にしたのが37.0%と最も多く、重み付けでも最もポイントが高くなっている。
- 「社員教育」は順位付けでは1位、2位、3位と満遍なく回答率が高く、重み付けでも2番目のポイントになっており、おしなべて取り組まれている項目となっている。

順位付けした結果



注1：特に注力している取り組みについて1位～3位までを順位付けしている

重み付けした結果



注1：1位を10点、2位を5点、3位を3点とし、加重平均による重み付けを行っている

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

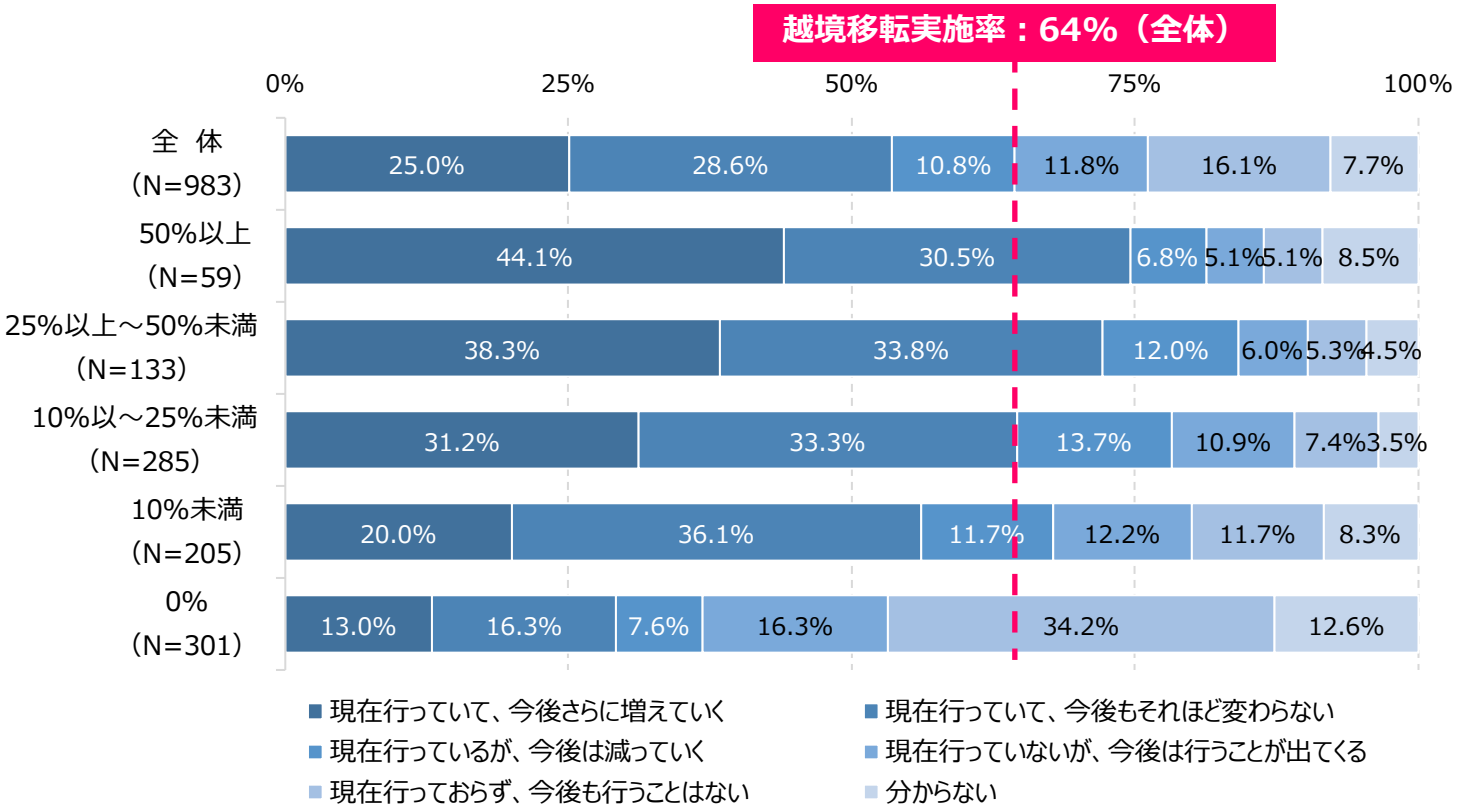
- 全体では「予算が確保ができない」が最も多く、保有件数別に見てもいずれの規模も回答率が高い。
- 「社内の運用体制が整備できていない」が全体で2番目に多く、特に1千～10万件未満での回答率が高い。この保有件数企業は「特に問題はない」の回答率は低く、対応すべき問題が多いとみられる。
- 1万件以上では、「変更点が抽出・整理できていない」と「公表事項の見直し・更新ができていない」の回答率が比較的高くなっており、制度の変更に対する対応が主な問題となっている。

	全 体 (N=983)	100万件以上 (N=174)	10万～100万件未満 (N=138)	1万～10万件未満 (N=225)	5千～1万件未満 (N=131)	1千～5千件未満 (N=177)	千件未満 (N=138)
改正された事項に対応するための予算が確保できない	31.2%	31.6%	30.4%	32.9%	36.6%	29.9%	25.4%
法改正に対応した社内の運用体制が整備できていない	28.6%	21.8%	26.8%	30.2%	32.1%	34.5%	25.4%
法改正による変更点が抽出・整理できていない	25.2%	27.6%	29.7%	27.1%	22.9%	20.3%	23.2%
公表事項（プライバシーポリシーや利用規約など）の見直し・更新ができていない	22.6%	26.4%	24.6%	27.1%	24.4%	16.4%	14.5%
社員向けの周知や教育が十分にできていない	21.5%	23.6%	17.4%	24.4%	19.8%	23.2%	17.4%
社内規定の見直し・更新ができていない	19.9%	17.2%	15.9%	23.1%	23.7%	22.0%	15.9%
情報漏洩時の報告・通知手順の見直しができていない	13.9%	13.8%	13.8%	18.7%	11.5%	14.1%	8.7%
第三者への情報提供時の対応が十分にできていない（Cookie情報の第三者提供の本人同意など）	11.6%	12.1%	17.4%	11.1%	10.7%	11.3%	7.2%
外国の第三者への情報提供の対応が十分にできていない	11.1%	13.8%	13.8%	12.9%	13.0%	8.5%	3.6%
本人からの開示請求への対応が十分にできていない	6.8%	10.3%	4.3%	6.7%	7.6%	7.3%	3.6%
特に問題はない	19.8%	23.6%	24.6%	14.2%	13.7%	18.6%	26.8%

5.3　データの越境移転の状況：全体と海外売上比率別

- 全体では、現在データの越境移転を行っているのは64.4%。そのうち「今後さらに増えていく」としているのは25.0%となり、越境移転はこれからも拡大していく傾向にある
- 企業の海外売上比率が高まるほど越境移転の実施率が高くなり、さらに「今後さらに増えていく」の割合も高まっている傾向にある。
- 海外売上比率50%以上では、データの越境移転の実施率が80%以上あり、そのうちの半数以上が「今後さらに増えていく」と回答している。

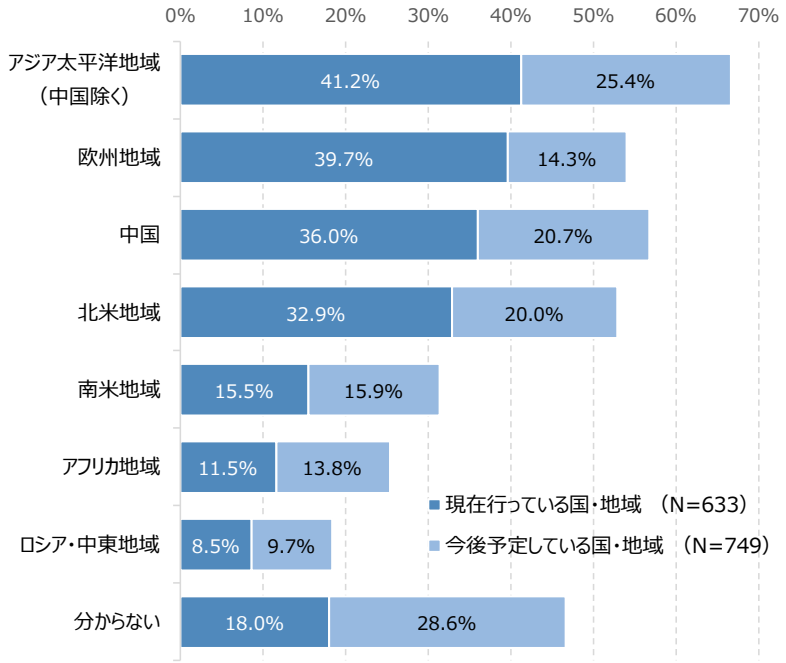
※データの越境移転：個人情報を海外の第三者に提供すること。プライバシー保護の観点から、各国・地域が規制を設けるなどの対応が行われている



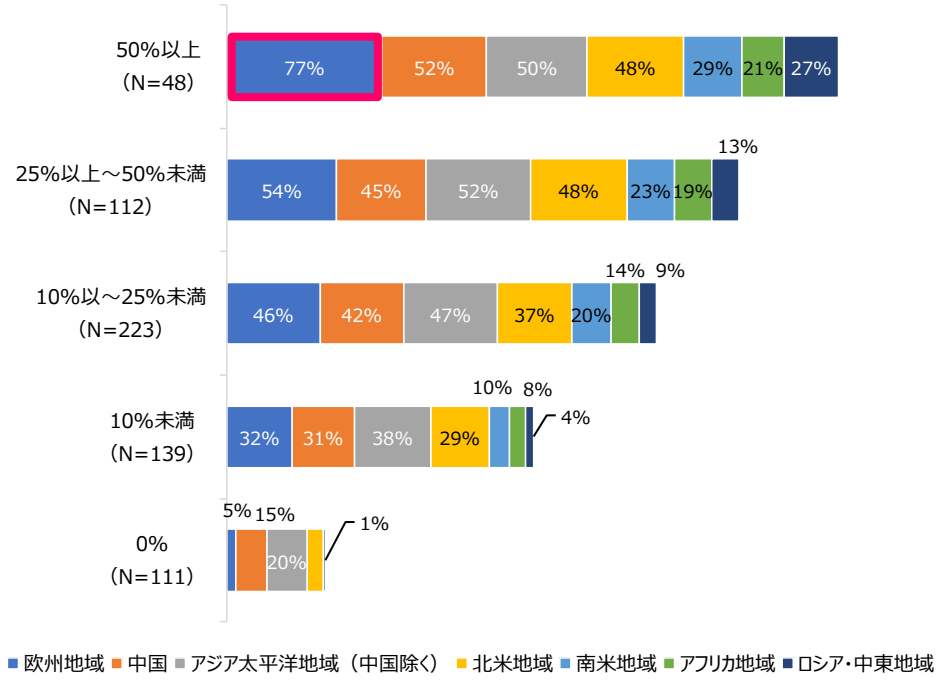
5.4　データの越境移転先の国・地域

- 現在のデータの主な越境移転先としては、「アジア太平洋地域（中国除く）」、「欧州地域」、「中国」、「北米地域」となっている。
- 海外売上比率50%以上の企業では、欧州が77%と非常に多いことが特徴としてみられる。
- 今後の移転先として、中国を含むアジア太平洋地域がさらに増えていくとみられる。

全体（現在実施と今後予定の国・地域）

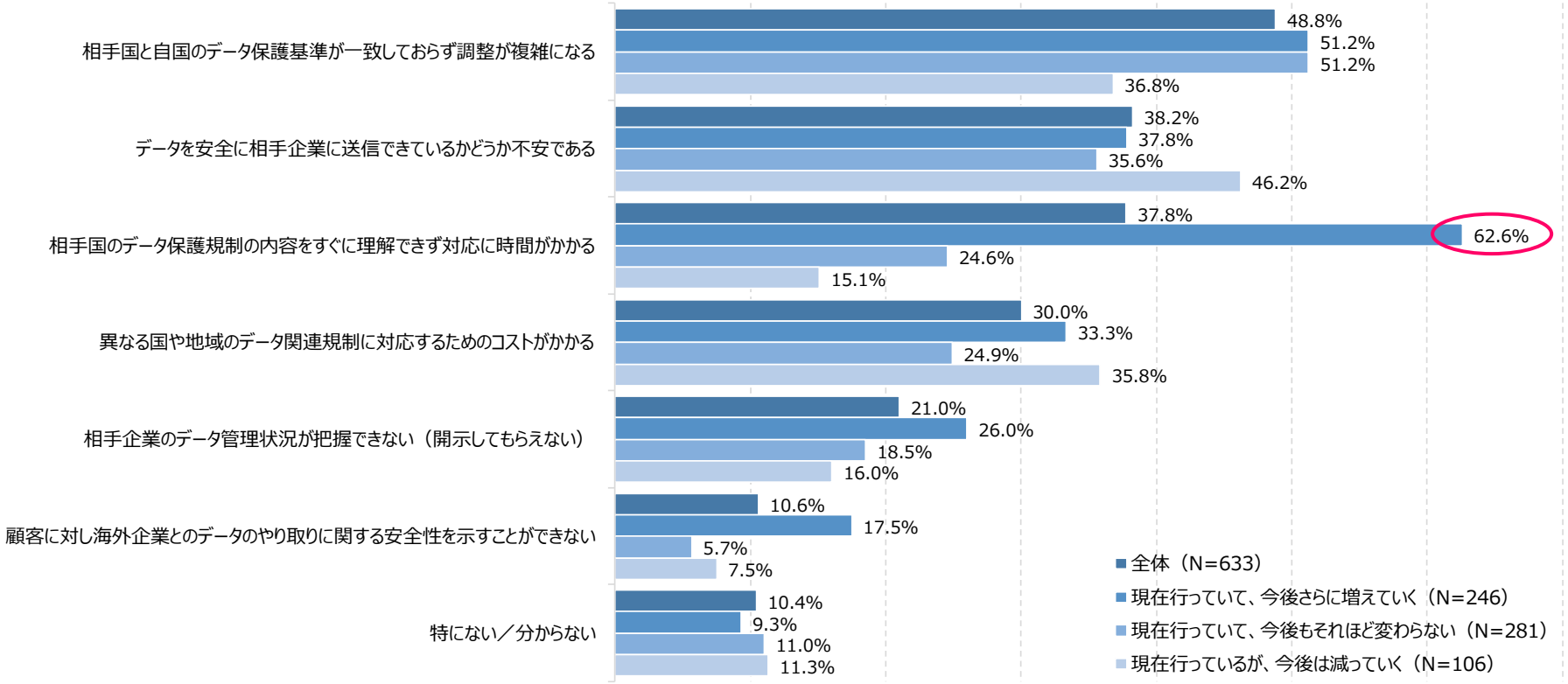


海外売上比率別（現在実施している国・地域）



5.5　海外企業とのデータのやり取りにおける課題

- 全体では「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」が最も多い。
- その次に「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」が続き、特に越境移転が今後減っていく企業で多くなっている。越境移転に消極的な理由のひとつとして考えられる。
- 越境移転が今後増えていく企業は、「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62.2%と非常に多くなっている。各国で異なるデータ保護規制への対応に苦慮していることがうかがえる。



5.6 プライバシーガバナンスに関する取り組み状況：全体と個人情報保有件数別

- 全体では「責任者を任命している」が最も多く、「組織の姿勢が明文化されている」、「リスクマネジメントを行っている」、「プライバシー保護組織の設置」が続いている。
- 個人情報の保有件数が多くなるほど、プライバシーガバナンスへの取り組み範囲が広がっていく傾向がある。特に100万件以上保有企業では「取り組みについて対外的にわかりやすく開示している」や「取引先に対して取り組みを促している」など、対外的な取り組みもみられる。

	全 体 (N=983)	100万件以上 (N=174)	10万～100万件未満 (N=138)	1万～10万件未満 (N=225)	5千～1万件未満 (N=131)	1千～5千件未満 (N=177)	1千件未満 (N=138)
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	37.5%	44.8%	37.7%	38.7%	42.0%	35.6%	24.6%
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	34.3%	53.4%	41.3%	31.1%	33.6%	26.6%	18.8%
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	31.4%	37.9%	31.9%	31.6%	35.9%	28.8%	21.7%
プライバシー保護のための組織を設置している	30.4%	43.7%	30.4%	26.7%	31.3%	32.2%	16.7%
運用ルールを策定し、組織全体に周知・徹底している	26.1%	32.2%	21.7%	28.0%	27.5%	27.1%	17.4%
内部監査部門やアドバイザリボードなど第三者的な組織を設置している	22.4%	32.2%	28.3%	20.9%	26.7%	15.3%	11.6%
従業員一人一人が当事者意識をもつような企業文化の醸成に取り組んでいる	20.1%	29.3%	21.7%	20.9%	16.0%	16.4%	14.5%
自社の取り組みについて、対外的にわかりやすく開示している	15.4%	24.7%	15.2%	12.9%	10.7%	16.9%	10.1%
取引先に対し、プライバシー保護に関する取り組み実施を促している	14.5%	25.9%	17.4%	12.4%	12.2%	10.2%	8.7%
規約・機能の変更や追加時に迅速に通知または公表している	14.2%	23.6%	15.9%	12.0%	11.5%	13.6%	8.0%
何も取り組んでいない	14.9%	9.2%	15.2%	12.4%	8.4%	14.1%	32.6%

5.7　プライバシーガバナンスにおける課題：全体と個人情報保有件数別

- 全体では「社内の体制整備が不十分である」が最も多く、「社内のルール策定が不十分である」が続いている。特に個人情報1千～1万件未満において、不十分な体制とルールの課題が多くみられる。
- 「経営層が十分に重要性を認識していない」も主要課題のひとつに含まれ、特に1万～10万未満において経営課題としての認識の低さがみられる。
- 100万件以上では、他の保有件数規模と比較して特に際立つような課題はない。また、27.0%が課題意識はなく、着実に対応している企業が多いとみられる。

	全　体 (N=983)	100万件以上 (N=174)	10万～100万件 未満 (N=138)	1万～10万件 未満 (N=225)	5千～1万件 未満 (N=131)	1千～5千件 未満 (N=177)	1千件未満 (N=138)
社内の体制整備が不十分である	32.8%	25.3%	31.2%	32.4%	38.9%	38.4%	31.2%
社内のルール策定が不十分である	30.0%	25.3%	28.3%	29.3%	33.6%	37.3%	26.1%
経営層が十分に重要性を認識していない	28.1%	26.4%	29.7%	34.2%	27.5%	25.4%	22.5%
企業文化の醸成が不十分である	20.0%	18.4%	21.7%	25.8%	18.3%	18.6%	14.5%
プライバシーガバナンスという考え方をそもそも知らなかった	18.9%	22.4%	23.2%	21.3%	19.1%	15.3%	10.9%
消費者とのコミュニケーションが不十分である	14.6%	12.6%	18.8%	17.3%	18.3%	12.4%	8.0%
ステークホルダーとのコミュニケーションが不十分である	11.3%	14.4%	9.4%	12.4%	13.0%	10.2%	7.2%
特に課題意識はない	22.2%	27.0%	23.9%	18.7%	14.5%	18.6%	31.9%

5.8　プライバシー保護の取り組み：調査結果からの考察

- 2022年4月から施行された改正個人情報保護法の対応においては、予算確保と運用体制整備を中心に問題が生じている。さらに個人情報の保有件数が多い企業では、改正に伴う変更点が自社にどう影響するかの整理とそのの対応にも難しさがみられる。

- データの越境移転を行う企業は今後も増加し、さらに越境移転先も欧米からアジアへと拡大していくとみられる。その一方で、各国・地域の規制は厳格化され、それぞれ異なることから、取引相手国の規制の理解と調整がより複雑になっていく。

- 経済産業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素のうち、責任者の任命と姿勢の明文化が進められている。個人情報を保有件数が多い企業から、プライバシー保護組織や第三者組織の設置など、リソースの投入が図られている。

- プライバシーガバナンスへの取り組みは、企業内でのプライバシー保護に取り組むだけではなく、プライバシーデータを扱う企業として消費者や取引先にも取り組みを公表することが重要である。それによって企業の信頼性が高まっていき、ビジネスにおいても優位性が高まっていく。企業の経営者はそうした認識を強く持つ必要がある。

報告する調査項目

1. DXの実践状況

2. 電子契約の利用状況

3. 生成AIの利用と課題

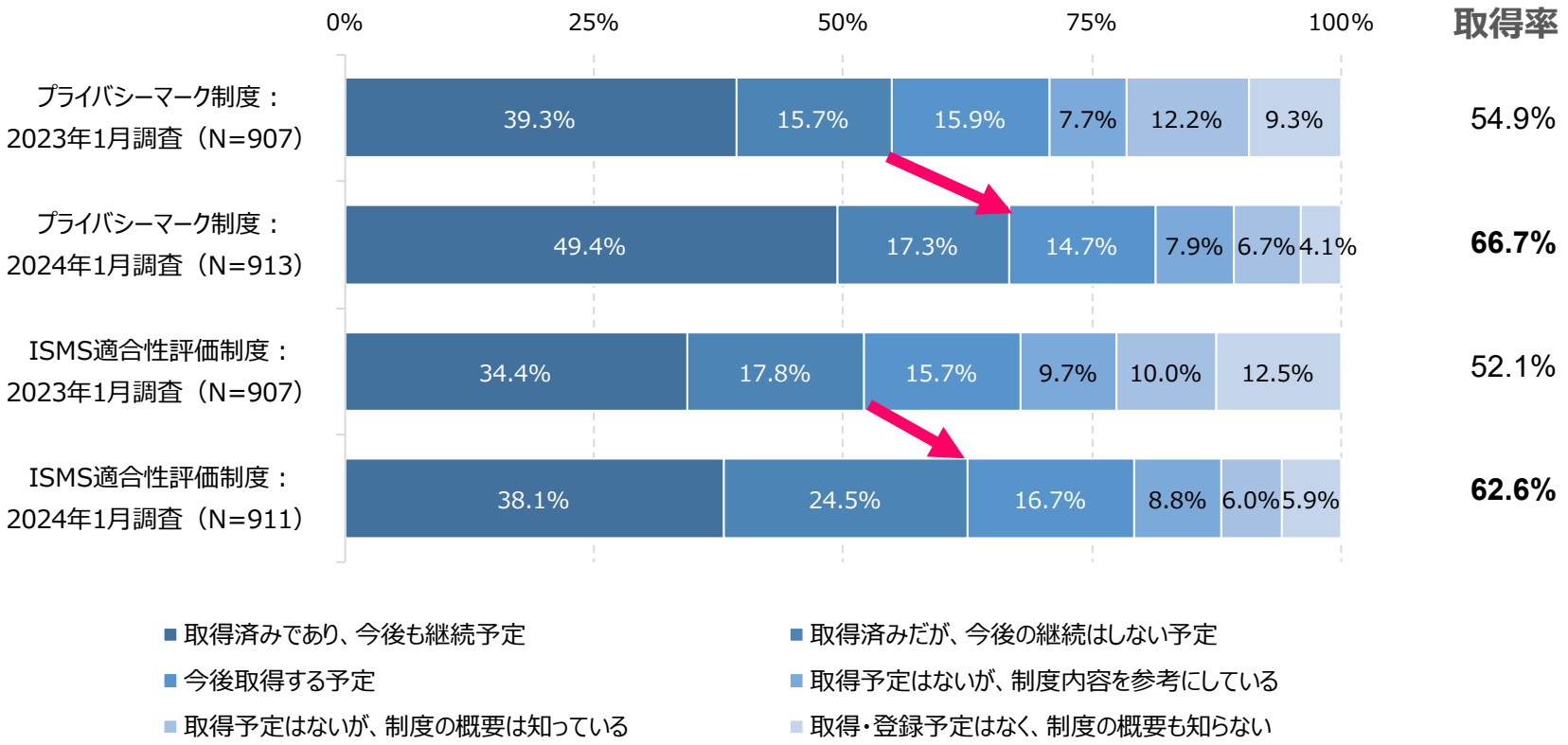
4. セキュリティのインシデントと対策

5. プライバシー保護に対する取り組み

6. 第三者認定／認証制度の取得状況

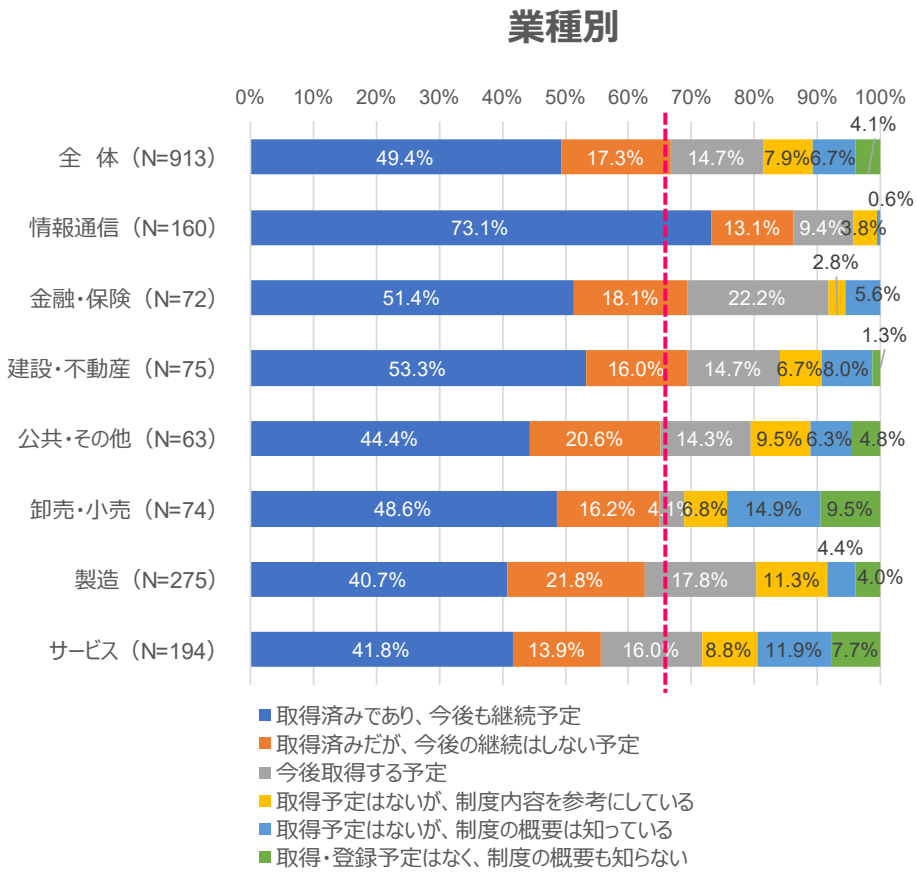
6.1　プライバシーマーク／ISMSの取得状況：2023年～2024年

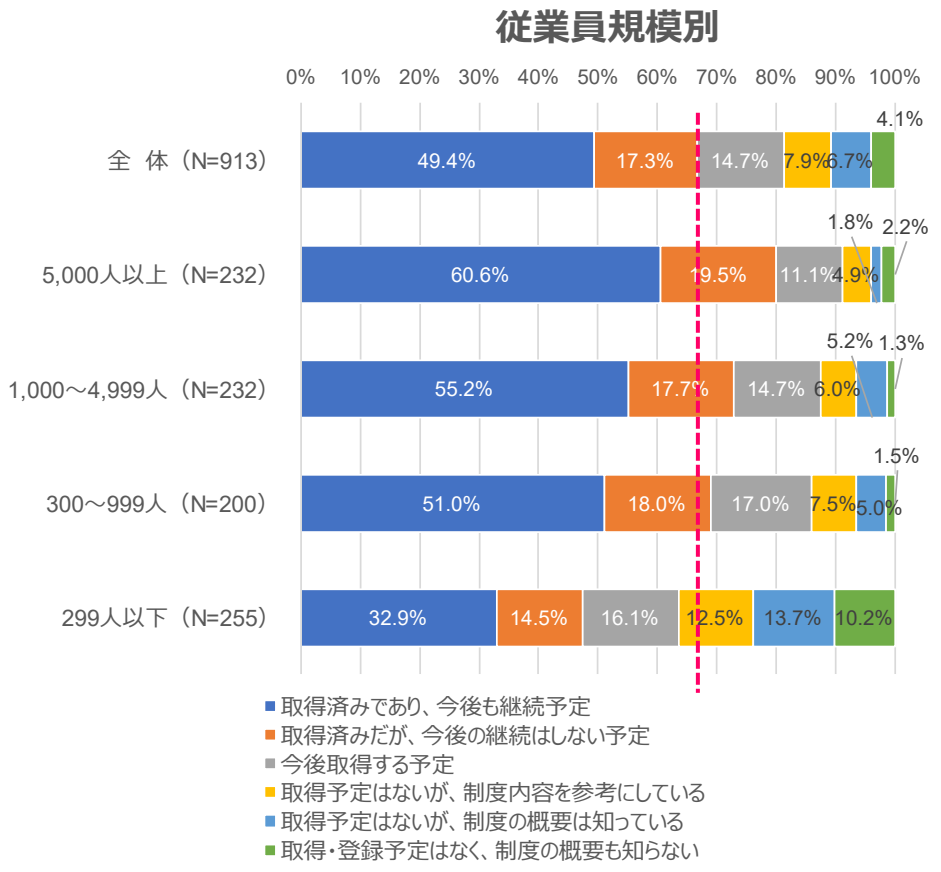
- 2024年調査のプライバシーマークの取得率は66.7%、2023年調査から10ポイント以上も上昇している。特に「取得済み・今後も継続予定」が大きく上昇している。
- 2024年のISMSの取得率は62.6%となり、こちらも2023年調査から10ポイント以上も上昇している。ただ、「取得済み・今後継続しない予定」が24.5%となっており、ISMSは継続性に不安がみられる。



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

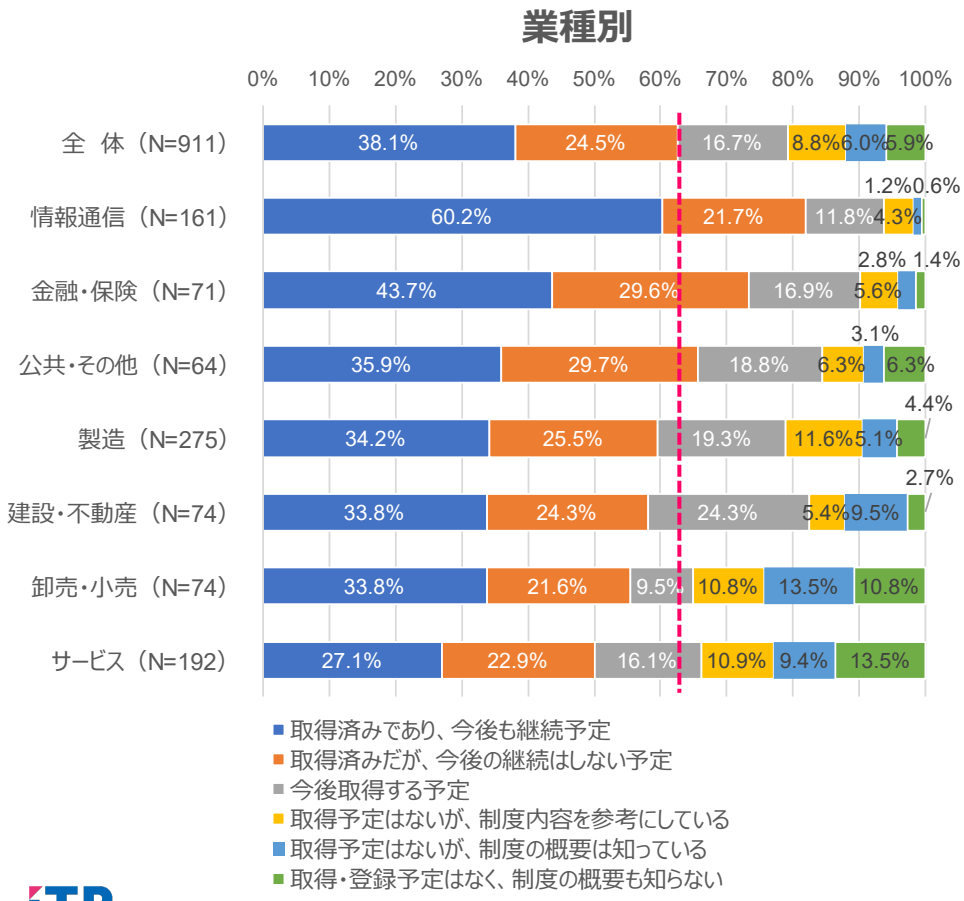
- 業種別で取得率が最も高いのは「情報通信」で85%を超えている。次に「金融・保険」と「建設・不動産」が続く。製造は「取得済み・今後継続しない予定」が21.8%と他の業種に比べて高くなっている。取得率が最も低いのはサービスである。
- 従業員規模別では、規模が大きくなるにしたがい取得率が高くなっていき、「5,000人以上」では80%が取得している。一方、「299人以下」では取得率が50%に達していない。

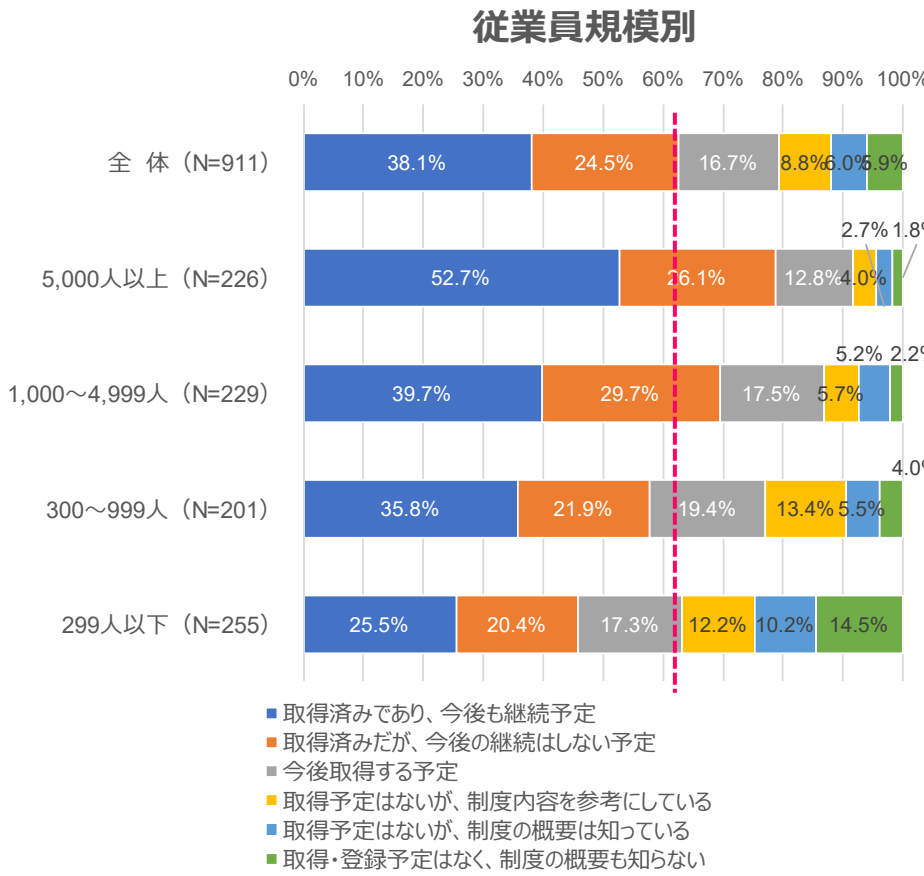




6.3　ISMSの取得状況：業種別と従業員規模別

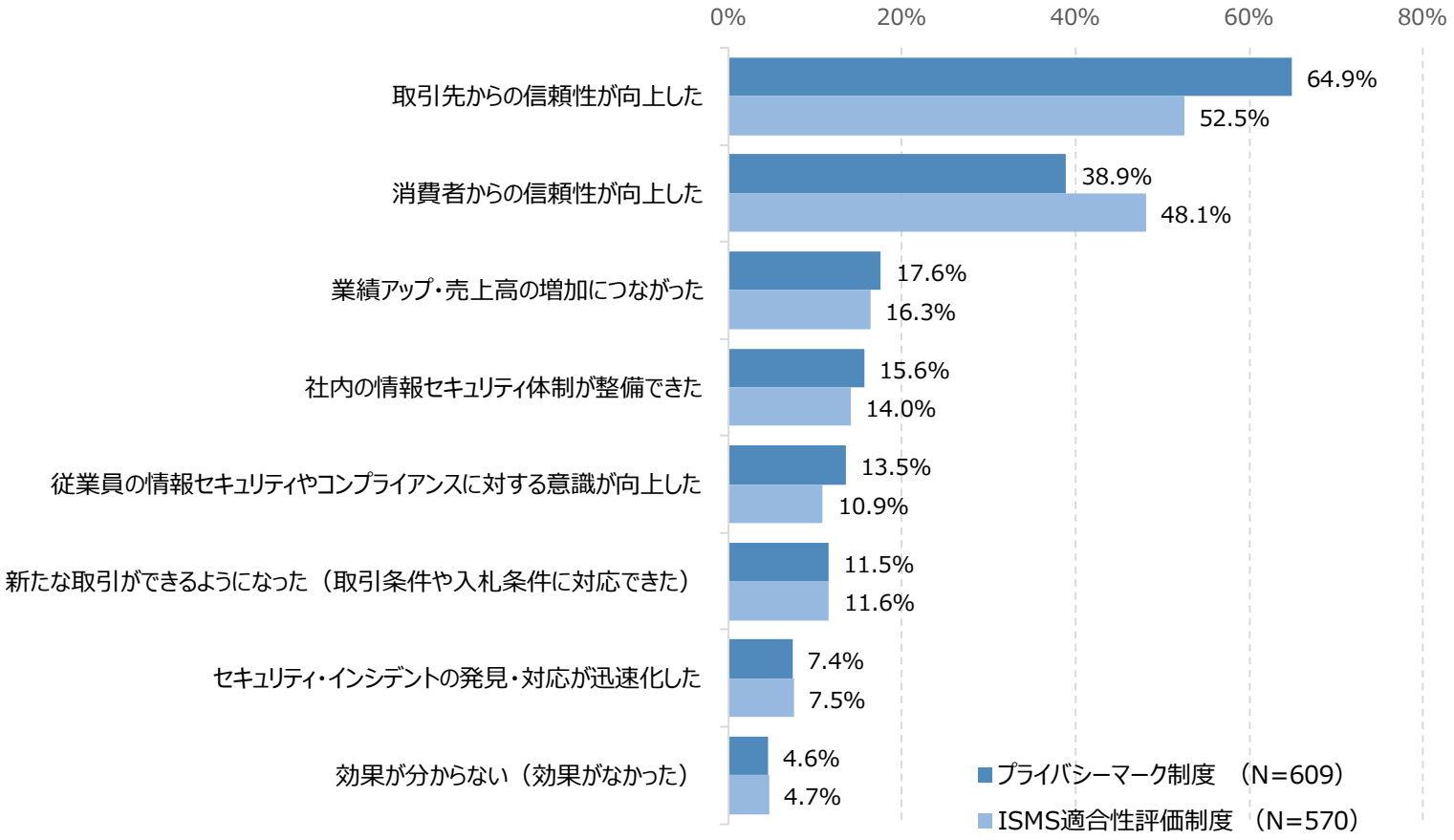
- 業種別で取得率が最も高いのは「情報通信」となり、80%を超えている。次に「金融・保険」が続く。「取得済み・今後継続しない予定」が高いのは、「公共・その他」、「金融・保険（29.6%）」である。取得率が最も低いのはサービスである。
- 従業員規模別では、規模が大きくなるにしたがい取得率が高くなっていき、「5,000人以上」では約80%が取得している。一方、「299人以下」では取得率が50%に達していない。





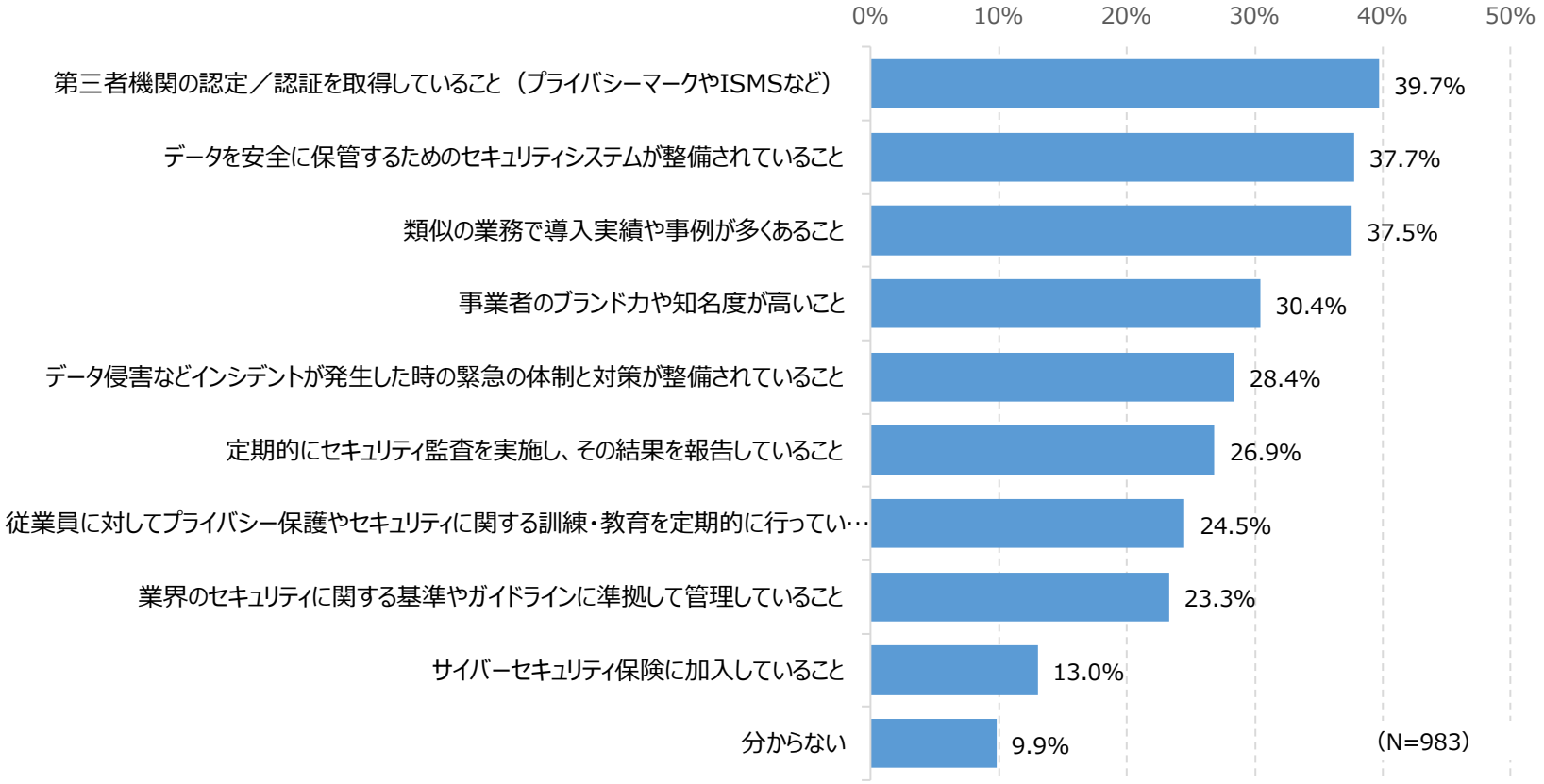
6.4 プライバシーマーク／ISMSの取得による効果

■ 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」が最も多い効果となった。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の方がやや多い。



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、業務委託事業者の選定において第三者認定／認証の取得有無が与える影響が大きいと考えられる。
- 「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2番目にあがっており、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。
- 「類似の業務で導入実績や事例が多くあること」と「事業者のブランド力や知名度が高いこと」のようなセキュリティ面以外も選定要因として重視されている。



6.6　第三者認定／認証制度取得に関する取り組み：調査結果からの考察

- プライバシーマーク、ISMSともに取得率が上がっている。ただし、ISMSにおいて、現在取得しているが今後は継続しないという回答が目立っており、継続する難しさがみられる。また、全体の取得率を現状からさらに押し上げるためには、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。

- 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／認証の取得が重視されている。事業者はデータセキュリティへの取り組みとあわせて第三者機関の認定／認証を取得することで、選定における優位性を高めていくことができる。

7　総括・提言

企業は既存ビジネスの拡大や新たなビジネスの創出に向けて、DXへの取り組みや生成AIの活用をさらに加速させていくであろう。その中において、経営者やIT／セキュリティ責任者は、同時にセキュリティリスクが高まっていくことを強く認識すべきである。

ランサムウェアに代表されるように、サイバー攻撃は巧妙化・高度化しており、どの企業（公的機関）にも攻撃被害が及ぶ可能性がある。自社のセキュリティ対策への継続的な投資を行いながら、最新の技術・ツールにアップデートを行うことが重要である。

DXによるクラウドやAIを活用したデジタルサービスは、個人情報の収集と活用が増え、プライバシーガバナンスへの取り組みが重要となる。ビジネスがグローバル化すれば、さらにその重要性は増す。自社のDXの価値と信頼性を高めるためにも、経営者がリーダーシップを取り、プライバシーガバナンスへの取り組みを推進していくべきである。

問いを、答えに。

ITR