「企業IT利活用動向調査2026」から見る日本企業のDX、AI活用、ランサムウェア被害の実態

集計結果分析レポート

株式会社アイ・ティ・アール
取締役 / プリンシパル・アナリスト　　入谷　光浩氏

【要約】
本レポートでは、JIPDEC「企業IT利活用動向調査2026」の国内企業1,100社超の調査データを基に、DX、AI活用、サイバーセキュリティの実態を多角的に分析した。
全社戦略に基づくDX推進は65.1%に達する一方、AIを事業レベルで活用できている企業は36%にとどまる。
本調査は、DXの定着と外向きDXへの転換、ならびにリスク管理高度化が今後の競争力を左右することを示唆している。

本レポートでは、一般財団法人日本情報経済社会推進協会（以下、JIPDEC）が2026年1月に実施した「企業IT利活用動向調査2026」（調査協力：株式会社アイ・ティ・アール）集計結果の中から特徴的な傾向をピックアップし、日本国内におけるIT利活用とセキュリティの実態について概説する。

目次

経営課題とDXの実践状況

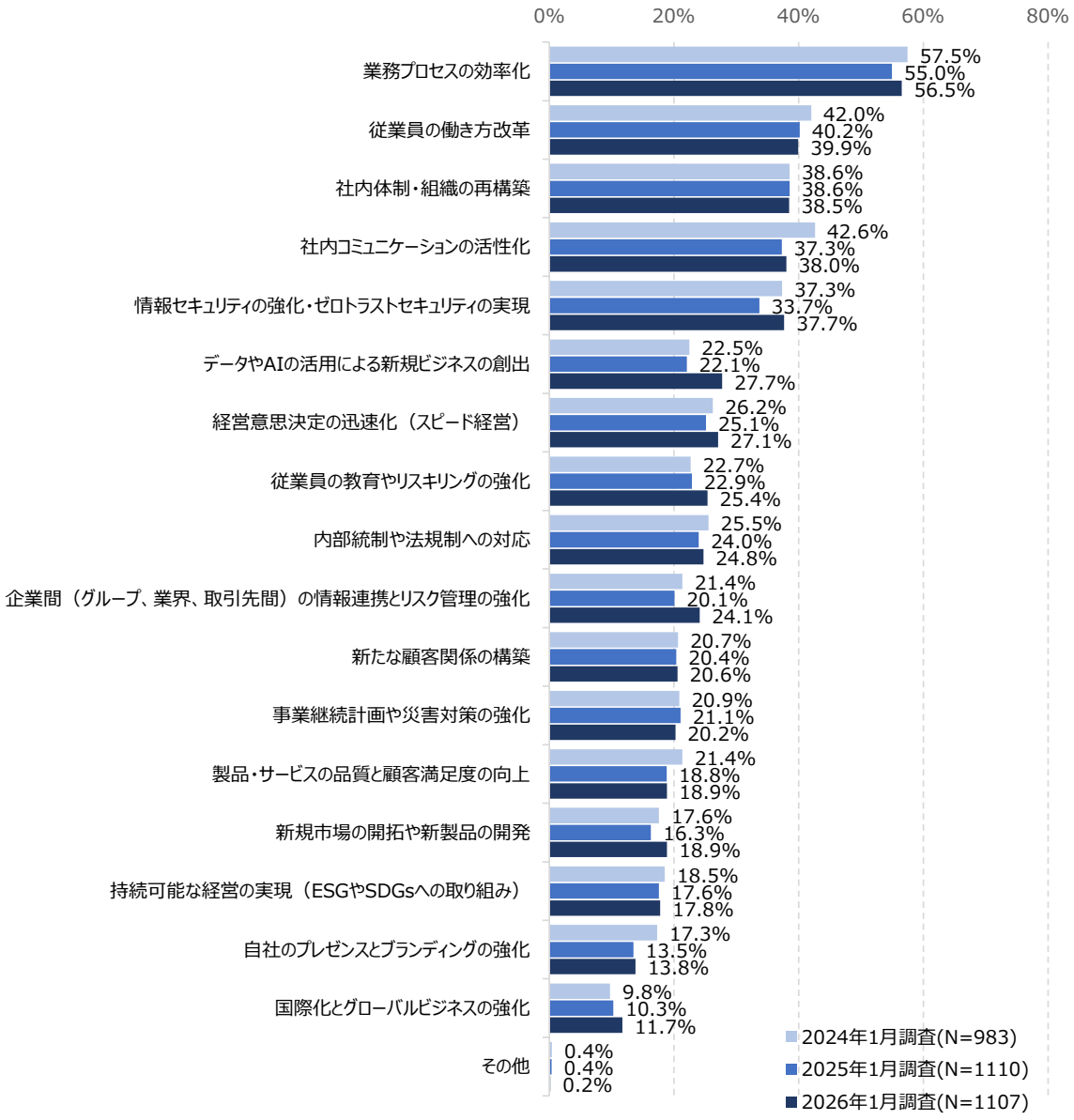
本章では、企業における経営課題とDX（デジタルトランスフォーメーション）の実践状況について調査した結果を分析している。

経営課題と施策への投資状況

企業が今後に向けて重視していく経営課題について質問を行った（図1）。「業務プロセスの効率化」は2025年調査から微増し、引き続き最上位を維持している。また、「従業員の働き方改革」や「社内体制・組織の再構築」、「社内コミュニケーションの活性化」も前年同様上位となるなど課題に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、2025年調査から回答率が上昇している。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施策にとどまらず、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。

一方、「データやAIの活用による新規ビジネスの創出」は、2025年調査から5ポイント以上の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、効率化やリスク対応と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。

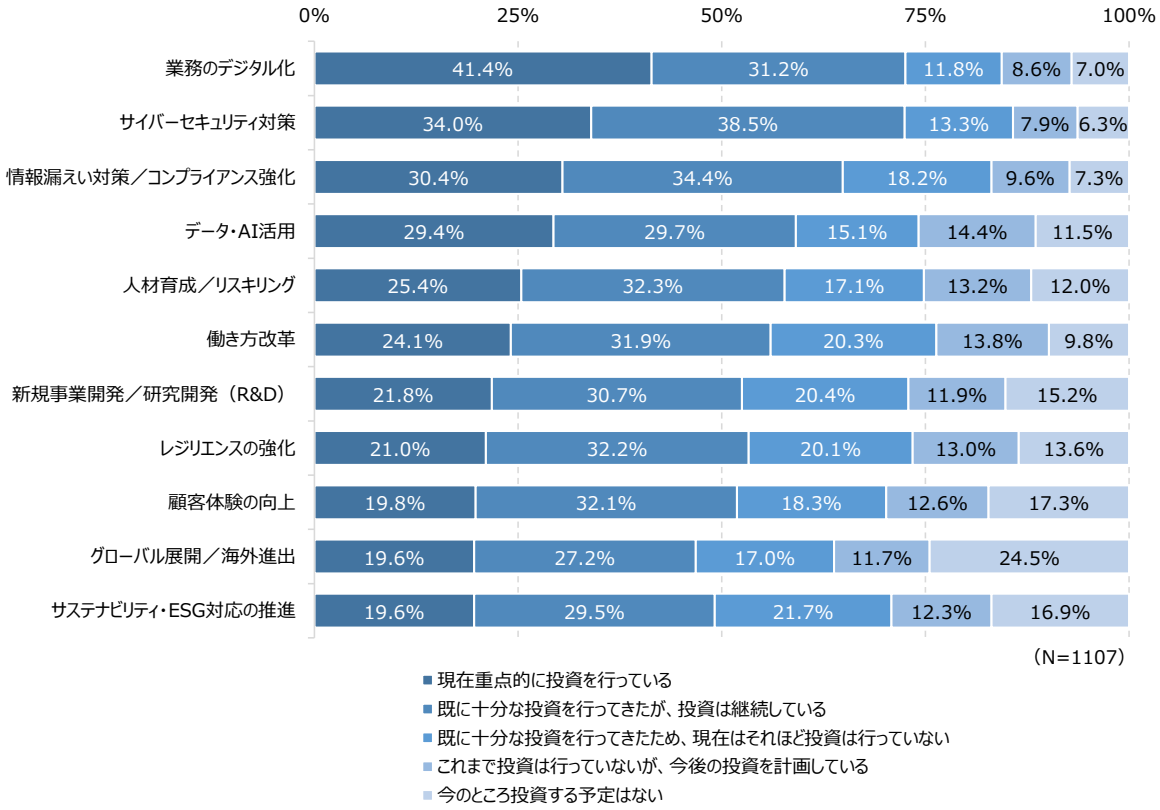


出典：JIPDEC『企業IT利活用動向調査2026』

図1 今後に向けて重視していく経営課題

では、経営課題に向けて策定した経営施策の投資はどのような状況にあるのだろうか。ここでは10個の経営施策を提示し、各施策への投資状況について質問している（図2）。「業務のデジタル化」や「サイバーセキュリティ対策」、「情報漏えい対策／コンプライアンス強化」では、重点的に投資を行っている割合と投資を継続している割合の合計が60%を超えている。企業運営に不可欠な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／リスキリング」も重点的に投資を行っている割合が比較的高く、中長期的な競争力強化を見据え、将来の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。



出典：JIPDEC『企業IT利活用動向調査2026』

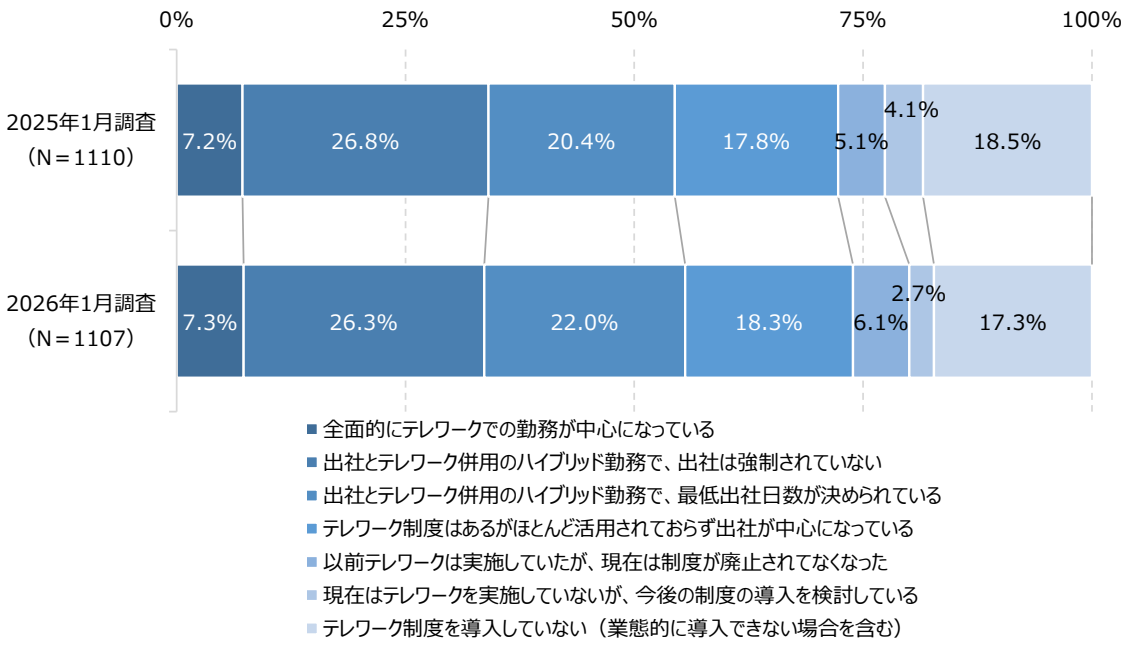
図2 経営施策に対する投資状況

テレワークの実施状況

重要な経営施策のひとつである働き方改革の取り組みにおいて、テレワークの推進が重要になっている。そこで、テレワークの実施状況について質問を行った（図3）。「全面的にテレワークでの勤務が中心になっている」（7.3%）と「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」（26.3%）の合計は33.6%と、2025年調査（34.0%）とほぼ同水準で推移している。約3社に1社では、テレワークが一時的な対応にとどまらず、働き方の一つとして定着していることがうかがえる。

「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」は2025年調査の20.4%から22.0%へ微増している。業務効率やマネジメント、社内コミュニケーションの維持を重視し、出社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広がっている。

一方、「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」（18.3%）と「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」（6.1%）の合計は24.4%と2025年調査（22.9%）からわずかに上昇しており、テレワーク制度が実質的に機能しなくなっている企業も緩やかに増加しつつある。



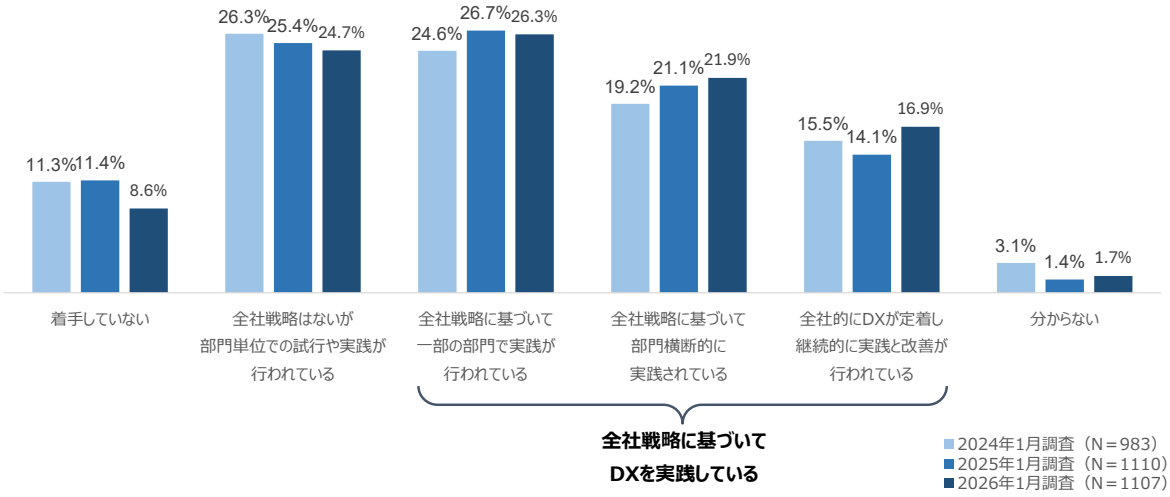
出典：JIPDEC『企業IT利活用動向調査2026』

図3　テレワークの実施状況

DXの実践段階の状況

現在、企業のDXがどの実践段階にいるかについて質問を行った（図4）。「全社戦略に基づいてDXを実践している」（「一部の部門で実践」「部門横断的に実践」「全社的に定着し継続的に実践・改善」の合計）は、2024年調査の59.3%から2026年調査では65.1%へと拡大しており、過半数の企業がすでに全社戦略に基づくDX推進の段階に移行していることがわかる。その内訳を見ると、「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」は15.5%（2024調査）から16.9%（2026年調査）へと上昇しており、DXを一過性のプロジェクトではなく、継続的な経営改善サイクルとして組み込む段階に達した企業が着実に増えつつある。

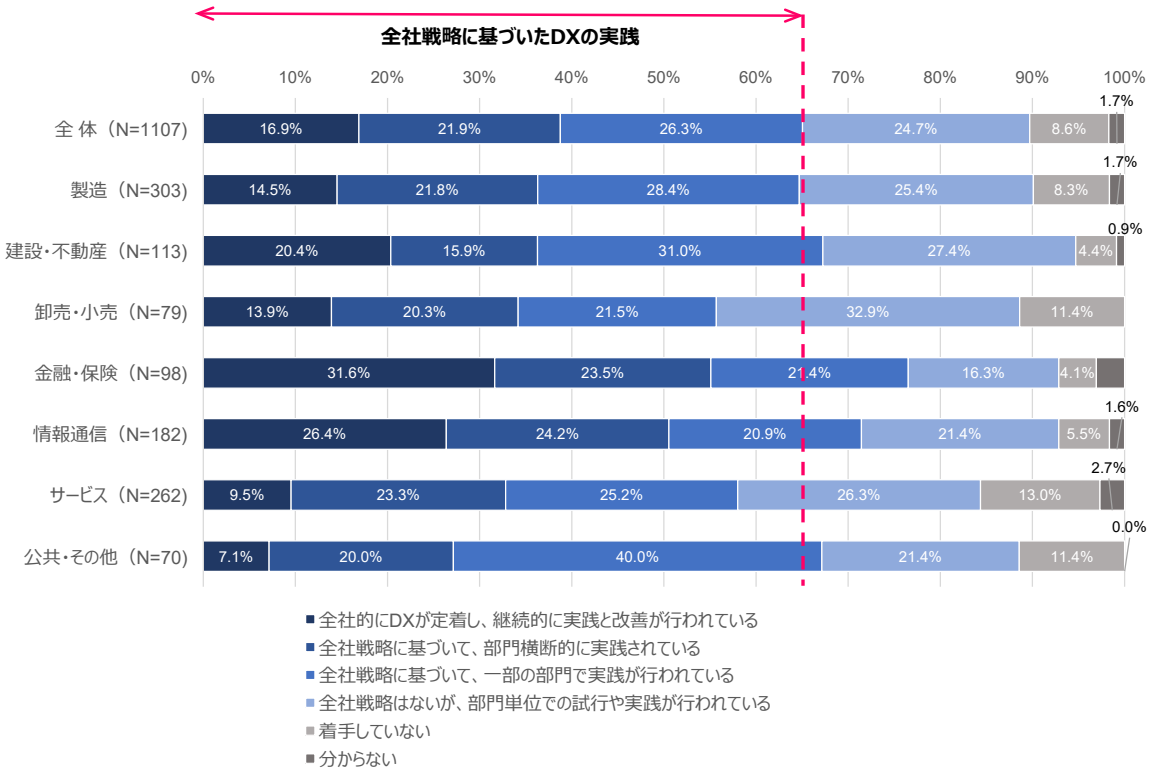
一方、「着手していない」企業は2024年調査の11.3%から2026年調査では8.6%へと減少し、「全社戦略はないが部門単位での試行や実践が行われている」も26.3%から24.7%へと微減している。部門単位の取り組みにとどまる企業や未着手の企業が縮小しており、DXへの取り組みが企業全体に着実に広がっていることが確認できる。



出典：JIPDEC『企業IT利活用動向調査2026』

図4 DXの実践段階

次に業種別にDXの実践段階を見てみると、全社戦略に基づいたDXの実践では、金融・保険と情報通信が先行している（図5）。一方で、卸売・小売とサービスが遅れをとっている。サービスは「着手していない」が13.0%と高く、最も遅れている業種といえる。

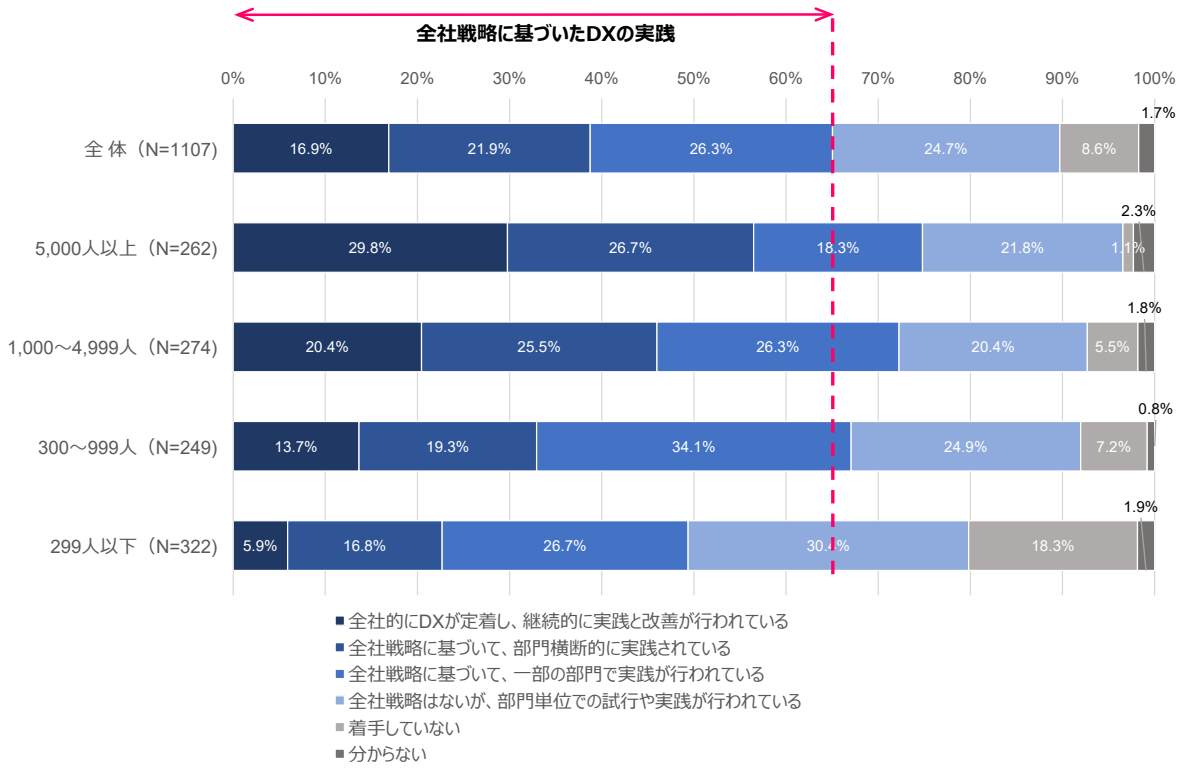


出典：JIPDEC『企業IT利活用動向調査2026』

図5 DXの実践段階：業種別

さらに従業員規模別にDXの実践段階を見てみる（図6）。従業員規模が大きくなるにしたがってDXの実践も進んでいる傾向があり、従業員5,000人以上では「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」が29.8%と非常に高い。一方、従業員299人以下では、約半数が「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」もしくは「着手していない」の段階であり、中小企業におけるDXの実践が遅れている状況が色濃く出ている。



出典：JIPDEC『企業IT利活用動向調査2026』

図6 DXの実践段階：従業員規模別

DXの取り組み内容と成果の状況

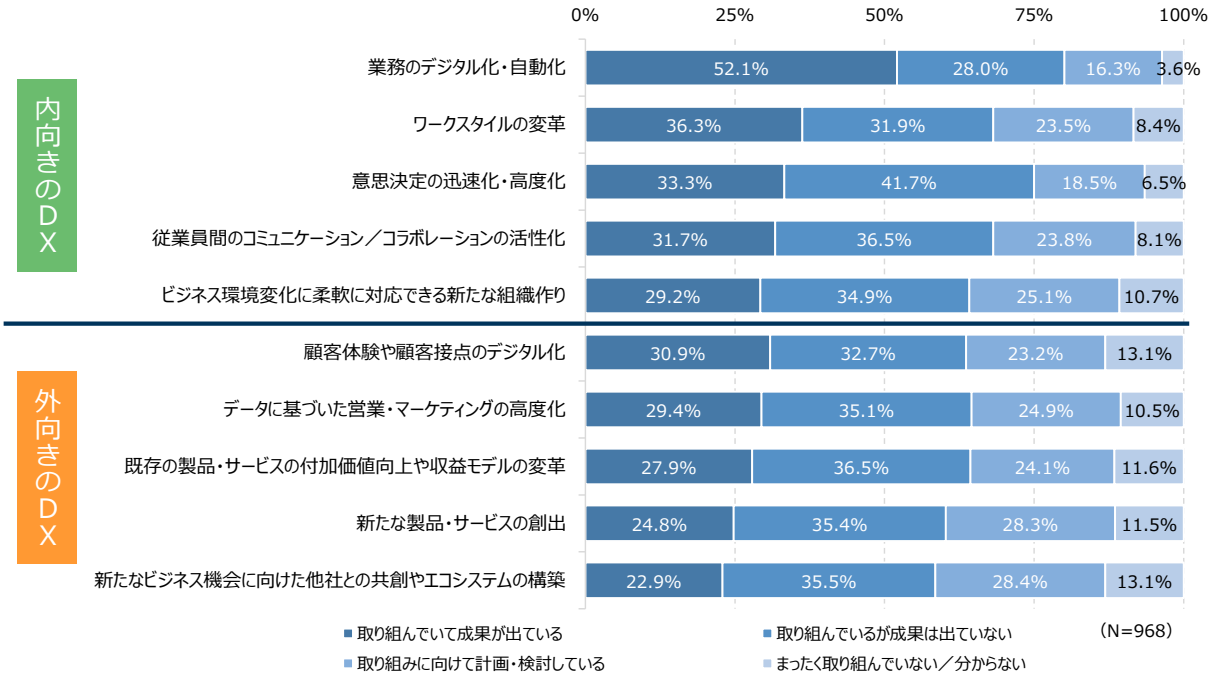
DXには、様々な取り組みがある。そこで、DXの取り組み内容について10項目を示し、その取り組み状況と成果について質問を行った（図7）。ここでは、DXの取り組みを大きく2つに分類している。ひとつは「内向きのDX」で、社内を対象に業務のデジタル化や従業員体験を向上させる取り組みである。もうひとつは「外向きのDX」で、顧客や市場に新たな価値を提供する取り組みである。

内向きのDXでは、「業務のデジタル化・自動化」が最も取り組まれており、「取り組んでいて成果が出ている」の割合が52.1%と、半数以上の企業で成果が確認されている。「ワークスタイルの変革」（36.3%）がこれに続き、この2項目は成果が出ている割合が成果の出ていない割合を上回っている。一方、「意思決定の迅速化・高度化」では成果が出ていない割合が41.7%と高く、取り組みの難度の高さがうかがえる。「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」や「ビジネス環境変化に柔軟に対応できる新たな組織作り」においても、成果が出ていない割合の方が大きく、組織・人材に関わる取り組みでは成果創出に時間を要する傾向がある。

外向きのDXでは、「顧客体験や顧客接点のデジタル化」（30.9%）と「データに基づいた営業・マーケティングの高度化」（29.4%）が成果の出ている割合で上位に位置する。しかし、外向きのDX全10項目のいずれにおいても、成果が出ていない割合が成果の出ている割合を上回っており、取り組みの本格化はこれからの段階にある。「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」は取り組んでいる企業自体がまだ少なく、外向きのDXの推進にはさらなる取り組みの加速が求め

られる。

内向きのDXと外向きのDXを比較すると、現時点では両者の間に明確な成熟度の差がある。内向きのDXは業務効率化を中心に成果創出が進み、一定の定着段階に入りつつある。一方、外向きのDXは取り組み自体が広がっているものの、成果につながっている企業はまだ少なく、試行・模索の段階にとどまっている。

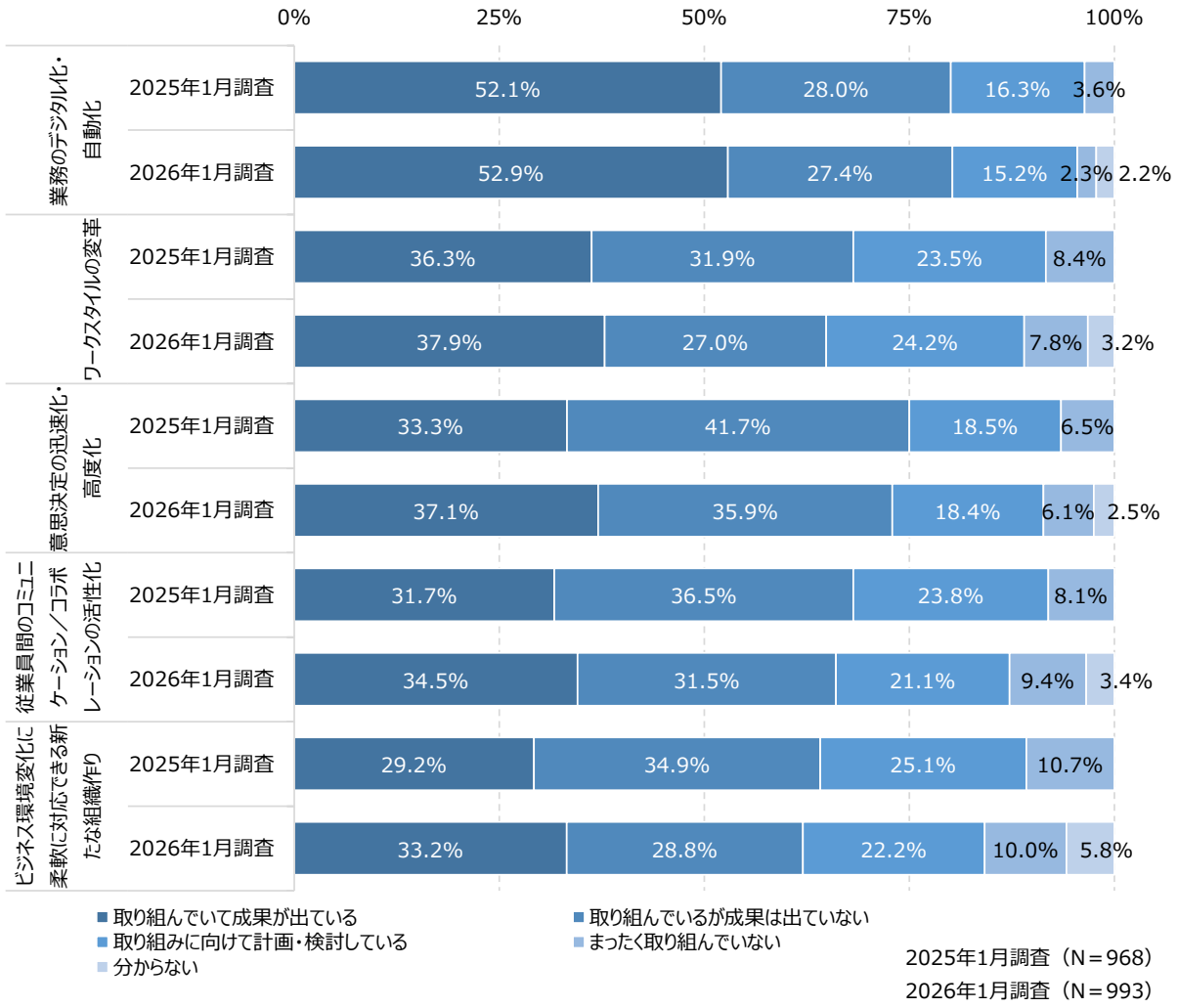


出典：JIPDEC『企業IT利活用動向調査2026』

図7　DXの取り組み内容と成果の状況

次に、内向きのDXにおける2025年調査との比較を見てみる（図8）。全5項目で「取り組んでいて成果が出ている」の割合が上昇しており、内向きのDX全体として成果創出が着実に進んでいることがわかる。「業務のデジタル化・自動化」は2025年調査の52.1%から2026年調査では52.9%とほぼ横ばいで推移しており、すでに高い成果率を維持したまま定着の段階に入っている。「ワークスタイルの変革」も36.3%から37.9%へと微増しており、働き方改革に関する取り組みが引き続き成果につながっている。

注目されるのは「意思決定の迅速化・高度化」で、前回調査では成果が出ていない割合が41.7%と高く課題として指摘されていたが、今回調査では成果が出ている割合が33.3%から37.1%へと3.8ポイント上昇し、成果が出ていない割合も35.9%へと改善が見られる。データ活用やAIの導入が意思決定の高度化に寄与し始めている可能性がある。「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」および「ビジネス環境変化に柔軟に対応できる新たな組織作り」も成果が出ている割合が上昇している。組織・人材に関わるこれらの取り組みは成果創出に時間を要する傾向があるが、継続的な取り組みが実を結び始めていることがうかがえる。



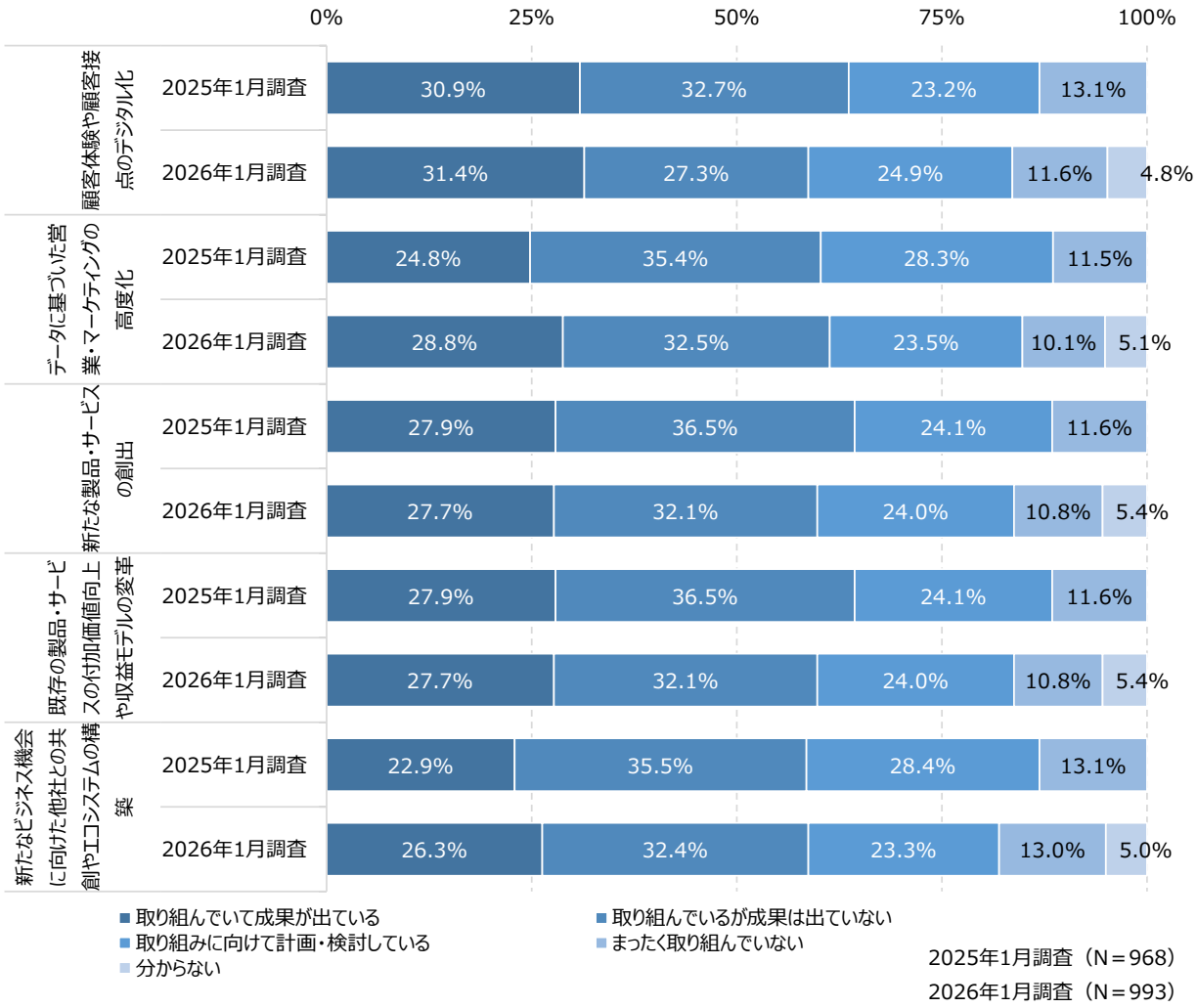
出典：JIPDEC『企業IT利活用動向調査2026』

図8　内向きDXの取り組み内容と成果の状況：2025年調査との比較

さらに、外向きのDXにおける2025年調査との比較も見てみる（図9）。全5項目のうち、成果が出ている割合が上昇したのは「顧客体験や顧客接点のデジタル化」、「データに基づいた営業・マーケティングの高度化」、「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」の3項目にとどまり、「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」と「新たな製品・サービスの創出」はいずれもわずかに低下している。

成果が出ている割合で最も高いのは「顧客体験や顧客接点のデジタル化」（31.4%）であり、顧客接点のデジタル化は外向きのDXの中では比較的取り組みが進んでいる領域といえる。また、「データに基づいた営業・マーケティングの高度化」は4.0ポイントの上昇と、外向きのDXの中では最も改善幅が大きく、データ活用による営業・マーケティング高度化への取り組みが成果につながり始めている。

しかし、外向きのDX全項目において依然として成果が出ていない割合が成果の出ている割合を上回っており、前回調査から大きな構造的変化は見られない。内向きのDXが成果創出の面で着実に進展しているのと対照的に、外向きのDXは取り組みの拡大と成果創出の両面でいまだ課題が多く、本格的な成果獲得に向けてはさらなる時間と投資の継続が必要な段階にあると考えられる。



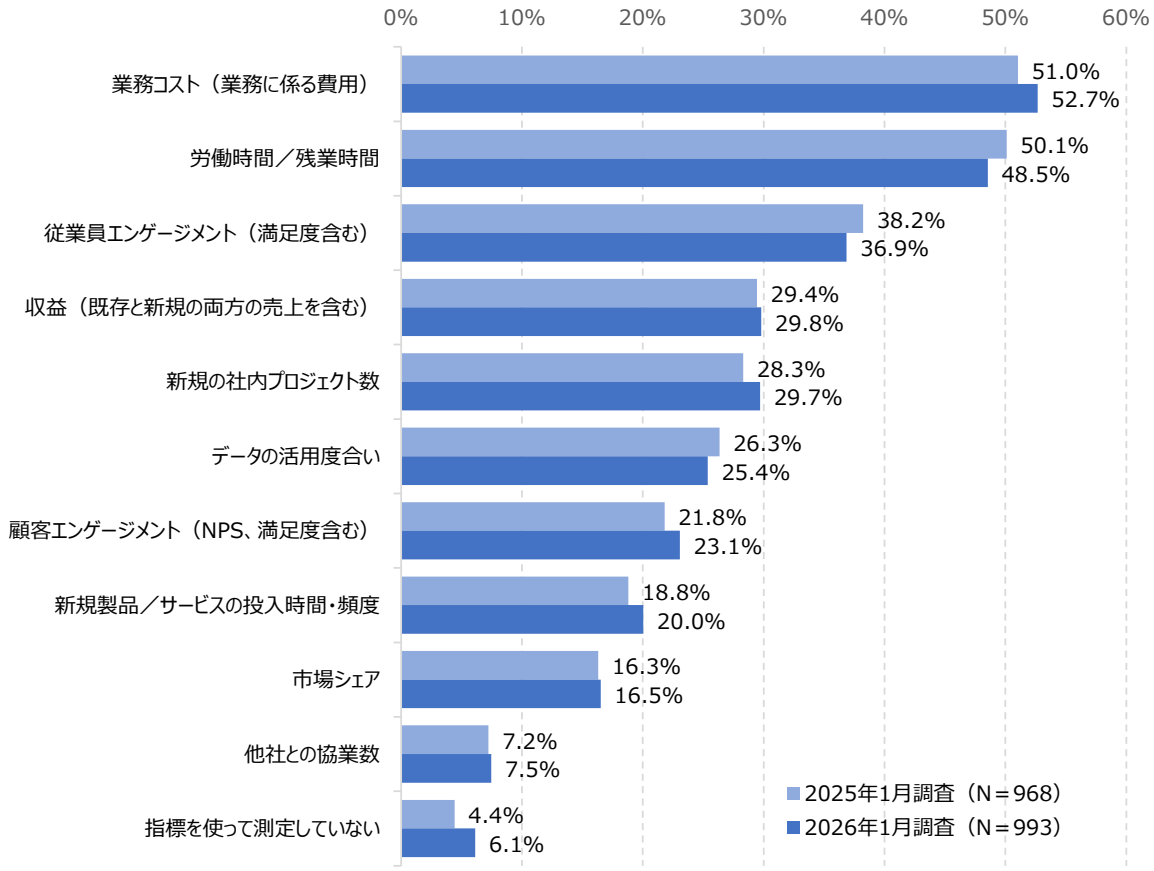
出典：JIPDEC『企業IT利活用動向調査2026』

図9　外向きDXの取り組み内容と成果の状況：2025年調査との比較

DX成果の測定指標

DXの成果測定にはどのような指標が用いられているだろうか。「業務コスト（業務に係る費用）」と「労働時間／残業時間」が最も多く、2社に1社がコスト削減や業務効率化に関連する指標でDXの成果を測定している（図10）。これは、内向きのDXが成果創出の面で先行しているという傾向と一致しており、企業がDXの効果をまず効率化の観点から評価していることを示している。

一方、「収益（既存と新規の両方の売上を含む）」や「顧客エンゲージメント（NPS、満足度含む）」、「新規製品／サービスの投入時間・頻度」といった外向きのDXに関連する指標の活用も一定程度見られる。ただし、2025年調査との比較では、これらの項目はほぼ横ばいか微増にとどまっており、外向きのDXの成果測定が本格化するにはいまだ至っていない。



出典：JIPDEC『企業IT利活用動向調査2026』

図10　DX成果の測定指標

次に、DX成果の測定指標をDX実践段階別に見ると、実践段階が進むほど多様な指標を活用してDXの成果を測定する傾向が明確に表れている（図11）。全社的にDXが定着している企業では、「業務コスト」や「労働時間／残業時間」といった効率化指標が高水準を維持するとともに、「従業員エンゲージメント」、「収益」、「顧客エンゲージメント」、「データの活用度合い」など、成長や価値創出に関連する指標の活用割合も他の段階と比べて際立って高い。DXが定着している企業では、効率化にとどまらず、事業成果や組織能力の向上を多面的に測定する仕組みが整いつつあることがうかがえる。

一方、部門単位での試行や実践にとどまっている企業では、「業務コスト」や「収益」、「顧客エンゲージメント」といった指標の活用割合が全体平均を下回っている。また、「指標を使って測定していない」が9.9%と全段階中最も高く、取り組みの成果を適切に評価・管理できていない企業が相対的に多いことが示されている。

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

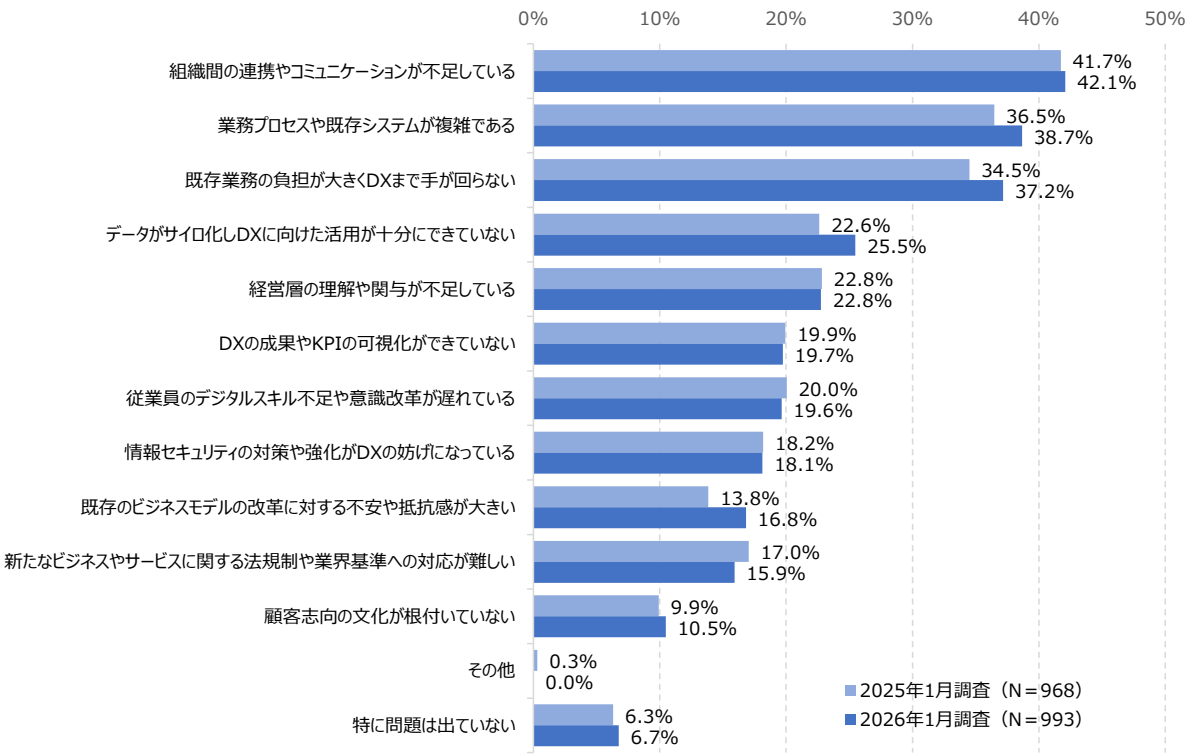
出典：JIPDEC『企業IT利活用動向調査2026』

図11　DX成果の測定指標：DX実践段階別

DX実践における問題

DXを実践している中でどのような問題が生じているだろうか。調査結果を見ると、「組織間の連携やコミュニケーションが不足している」が42.1%と最も高く、2025年調査（41.7%）からさらに上昇している（図12）。次いで「業務プロセスや既存システムが複雑である」、「既存業務の負担が大きくDXまで手が回らない」が続いており、この上位3項目はいずれも2025年調査から増加している。さらに、「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」も22.6%から25.5%へと2.9ポイント上昇しており、データ活用やAI活用への関心が高まるなかで、データ基盤の整備が追いついていない実態が浮かび上がっている。

「経営層の理解や関与が不足している」と「DXの成果やKPIの可視化ができていない」はほぼ横ばいで推移している。経営層の関与不足や成果の見えにくさは引き続き課題として認識されているものの、改善があまり進んでいない状況がうかがえる。また、「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」は13.8%から16.8%へと上昇しており、外向きのDXを本格化させていくうえでの心理的・文化的障壁が顕在化しつつあることがうかがえる。



出典：JIPDEC『企業IT利活用動向調査2026』

図12　DXの実践で生じている問題

次に、DXの実践で生じている問題をDX実践段階別に見ると、段階によって課題の構造が異なることがわかる（図13）。部門単位での試行や実践にとどまっている層では、「組織間の連携やコミュニケーションが不足している」が最も高く、全社的な戦略や推進体制が整っていないことによる組織間の分断が、DX推進の最大の障壁となっている。全社戦略に基づいて一部の部門で実践が行われている層では、「既存業務の負担が大きくDXまで手が回らない」と「組織間の連携やコミュニケーションが不足している」が突出して高い。全社戦略は存在するものの、実行段階での現場負荷と部門間連携の不足が、取り組みの横展開を妨げている状況が読み取れる。

全社戦略に基づいて部門横断的に実践されている層では、「業務プロセスや既存システムが複雑である」と「経営層の理解や関与が不足している」が相対的に高い。取り組みが部門横断的に広がるなかで、既存システムや業務プロセスの複雑さが障壁となるとともに、経営層の継続的な関与の重要性が改めて意識されている。一方、全社的にDXが定着している層では、「組織間の連携やコミュニケーションが不足している」や「既存業務の負担が大きくDXまで手が回らない」、「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」がいずれも全体平均を下回っており、組織・データ面での課題が相対的に解消されつつある。しかし、「業務プロセスや既存システムが複雑である」は全体平均とほぼ同水準で残存しており、DXが定着した段階においても既存システムの複雑さは継続的な課題として残ることが示されている。

	全 体 (N=993)	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=187)	全社戦略に基づいて、部門横断的に実践されている (N=242)	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=291)	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=273)
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%	32.6%	40.5%	44.7%	47.3%
業務プロセスや既存システムが複雑である	38.7%	39.6%	41.7%	35.4%	38.8%
既存業務の負担が大きくDXまで手が回らない	37.2%	27.8%	39.3%	45.0%	33.3%
経営層の理解や関与が不足している	25.5%	24.1%	32.6%	25.8%	19.8%
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	22.8%	14.4%	24.4%	27.5%	22.0%
従業員のデジタルスキル不足や意識改革が遅れている	19.7%	21.4%	22.7%	21.6%	13.9%
DXの成果やKPIの可視化ができていない	19.6%	20.9%	21.9%	18.9%	17.6%
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%	21.9%	19.0%	17.9%	15.0%
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	16.8%	17.6%	19.4%	16.8%	13.9%
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	15.9%	15.0%	18.6%	14.8%	15.4%
顧客志向の文化が根付いていない	10.5%	14.4%	7.9%	13.4%	7.0%

出典：JIPDEC『企業IT利活用動向調査2026』

図13　DXの実践で生じている問題：DX実践段階別

調査結果の考察

本章では、DXの実践状況とその課題について調査結果を分析した。そこから得られた考察を以下にまとめる。

1. **経営の安定基盤とDX推進が両輪で進んでいる**： 最も重視されている経営課題は引き続き業務プロセスの効率化であり、業務のデジタル化・自動化は半数以上の企業で成果が出ている。一方、セキュリティ対策への投資も拡大しており、効率化とリスク管理という経営の安定基盤を固めながら、DXを着実に前進させている企業の姿が浮かび上がっている。
2. **DXの全社展開が進む一方、外向きのDXへの転換が次の課題となる**： 全社戦略に基づいてDXを実践している企業は過半数を超え、内向きのDXでは全項目で成果率が向上するなど、DXの定着が着実に進んでいる。しかし、外向きのDXは依然として成果が出ていない割合が高く、効率化で培ったデータ・デジタル基盤を事業成長や新たな価値創出へと活かす取り組みへの転換が、次の重要なステップとなる。
3. **データ・AIへの関心の高まりが、DXの次フェーズを牽引する**： データやAIの活用による新規ビジネスの創出を経営課題として挙げる企業が2025年調査から大きく増加しており、データ・AI活用への投資を本格化させる企業も増え始めている。DXが定着している企業ほど収益や顧客エンゲージメントなど多面的な指標で成果を測定しており、データ・AIの活用がDXの深化と事業変革を加速させる原動力となることが期待される。
4. **DX推進の障壁は技術よりも組織・プロセス・文化にある：** DXの実践で生じている問題の上位は、組織間の連携不足、既存システムや業務プロセスの複雑さ、既存業務による現場の負荷であり、いずれも2025年調査から悪化している。テクノロジーの導入だけでなく、組織横断的な推進

体制の整備、業務プロセスの抜本的な見直し、そして変革を受け入れる企業文化の醸成を一体的に進めることが、DXをさらに高度化させるための鍵となる。

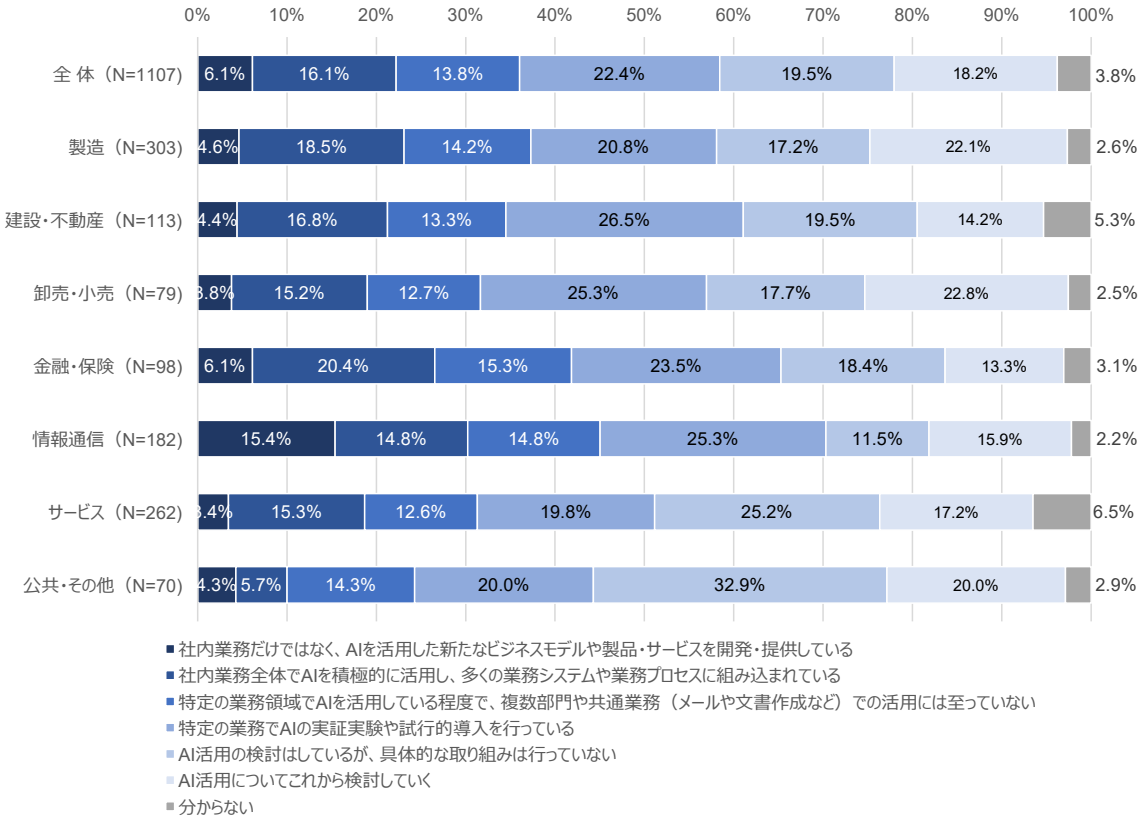
AIの活用状況と課題

本章では、AIの活用状況とその効果、活用における課題について調査した結果を分析している。

AIの活用状況

企業の業務におけるAIの活用状況について質問を行った（図14）。全体の結果を見ると、AIを実践・活用している企業（「社内業務だけでなく新たなビジネスモデルや製品・サービスを開発・提供」「社内業務全体で積極的に活用」「特定業務領域で活用」の合計）は36%にとどまっており、本格的な活用に至っている企業はまだ少ない。まだ、試行段階や検討段階にとどまっている企業が多く、業務全体への本格的な組み込みや新たなビジネス創出への活用という観点ではまだ発展途上にある。

業種別に見ると、業種間で活用の進展度合いに明確な差が生じていることがわかる。情報通信は社内業務全体でAIを積極的に活用している割合が最も高く、AI活用が最も進んでいる業種といえる。また、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・提供している割合も他業種を大きく上回っており、AIをビジネス創出にまで結びつけている企業が多い。金融・保険も積極的な活用層の割合が高く、情報通信と並んでAI活用の先行業種として位置づけられる。



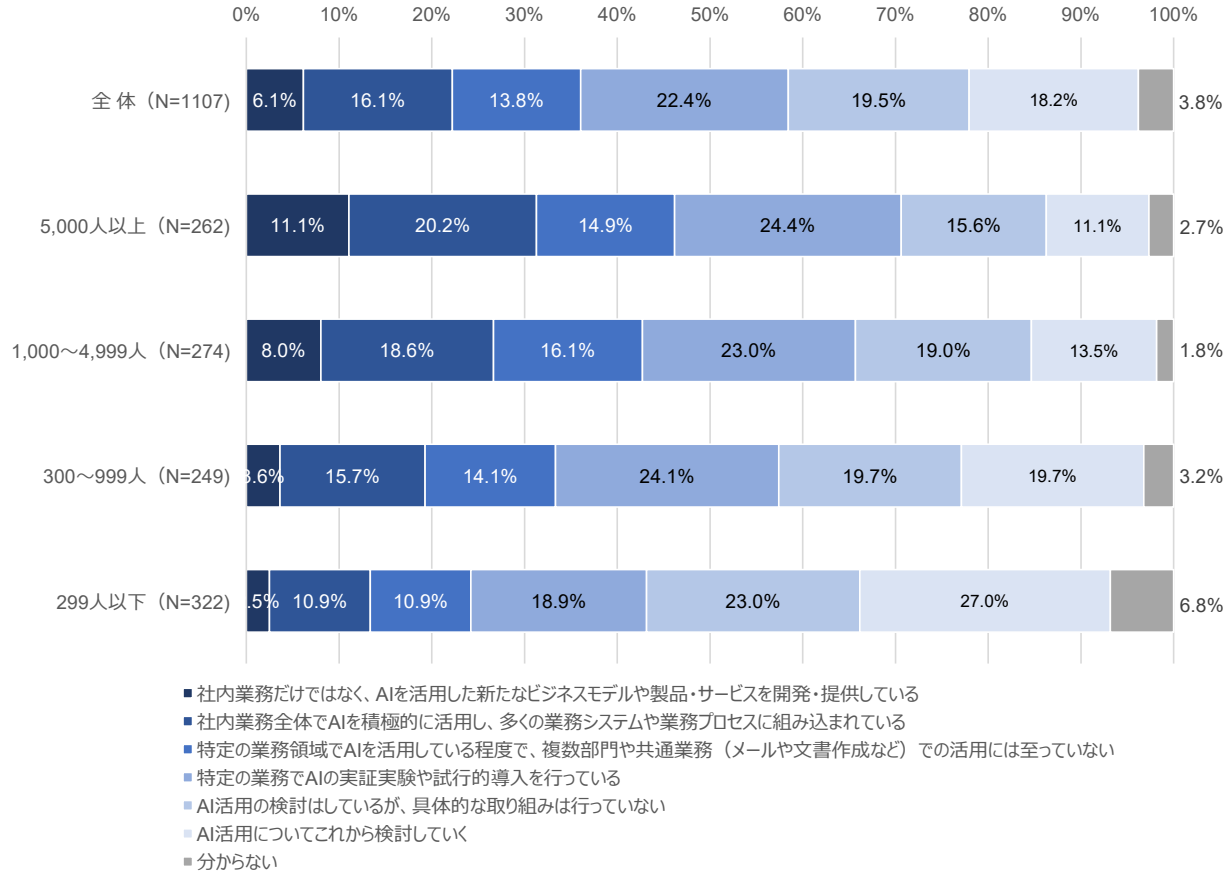
出典：JIPDEC『企業IT利活用動向調査2026』

図14　AIの活用状況：業種別

次に従業員規模別に見てみる（図15）。規模が大きくなるほどAI活用が進んでいる傾向が明確に表れている。5,000人以上の企業では、社内業務全体でAIを積極的に活用している割合と新たなビジネスモデルや製品・サービスを開発・提供している割合の合計が他の規模を大きく上回っており、AIが業

務プロセスへの組み込みにとどまらず、事業創出にまで活用されている企業が相対的に多い。1,000～4,999人もこれに次ぐ水準にあり、大企業ほどAI活用の深度が高い傾向がうかがえる。

一方、50～299人の企業では、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割合とAI活用についてこれから検討していく割合の合計が全規模中最も高く、本格的な取り組みはこれからの段階にある企業が多い。

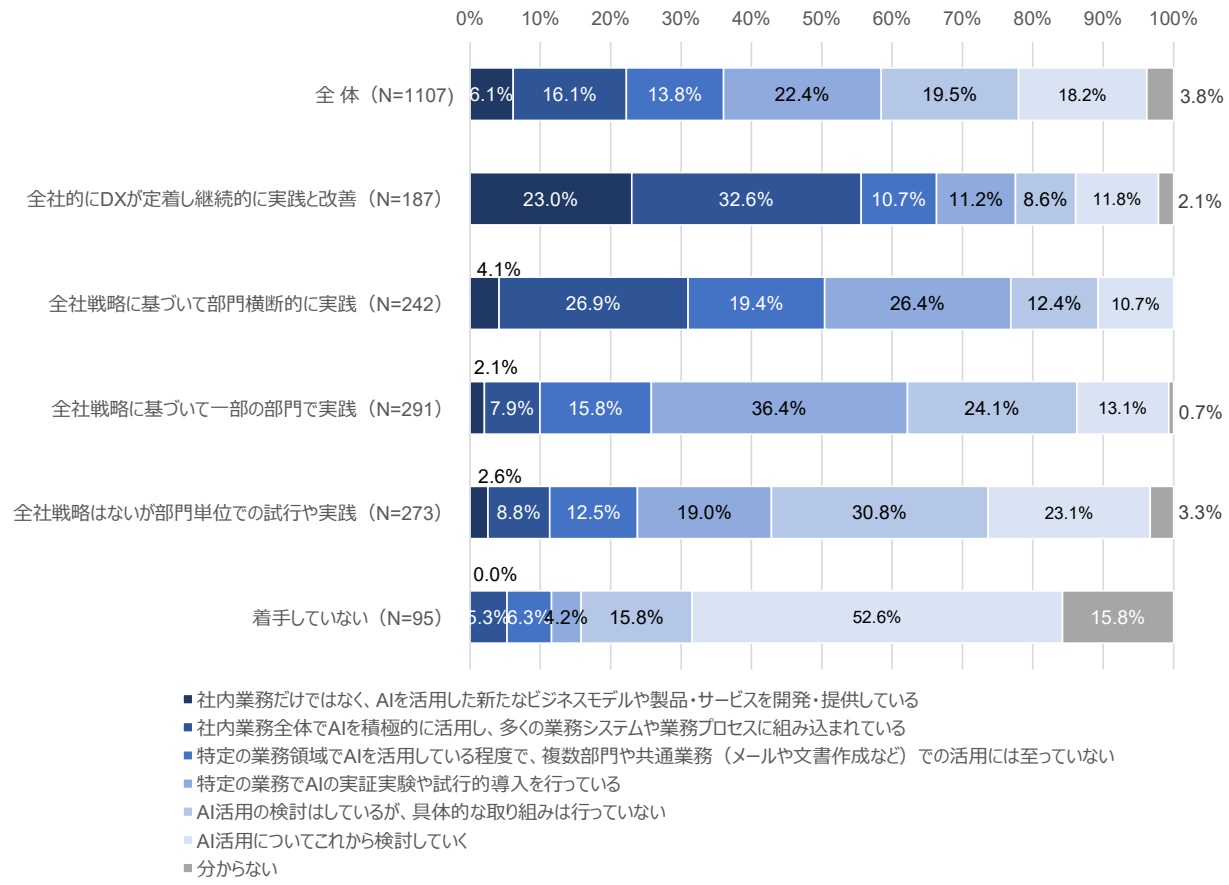


出典：JIPDEC『企業IT利活用動向調査2026』

図15　AIの活用状況：従業員規模別

さらにDX実践段階別に見てみる（図16）。DXの実践段階が進むほどAI活用も深化している傾向が明確に表れており、DXの推進とAI活用の間には強い相関関係があることがわかる。全社的にDXが定着している企業では、社内業務全体でAIを積極的に活用している割合と新たなビジネスモデルや製品・サービスを開発・提供している割合の合計が全段階中最も高く、AIが業務効率化にとどまらず事業創出にまで活用されている企業が多い。DXの定着がAI活用の深化を促す土台となっていることがうかがえる。

全社戦略に基づいて部門横断的に実践されている企業でも積極的な活用層の割合が比較的高い。一方、全社戦略に基づいて一部の部門で実践している企業および部門単位での試行や実践にとどまっている企業では、実証実験・試行的導入やAI活用の検討はしている段階の割合が高く、AI活用が特定部門や試行段階にとどまっている企業が多い。さらに、DXに着手していない企業では、AI活用をこれから検討していくが過半数を占めており、DXの基盤が整っていない企業においてはAI活用も難しい状況が浮かび上がっている。



出典：JIPDEC『企業IT利活用動向調査2026』

図16　AIの活用状況：DX実践段階別

AIの活用効果

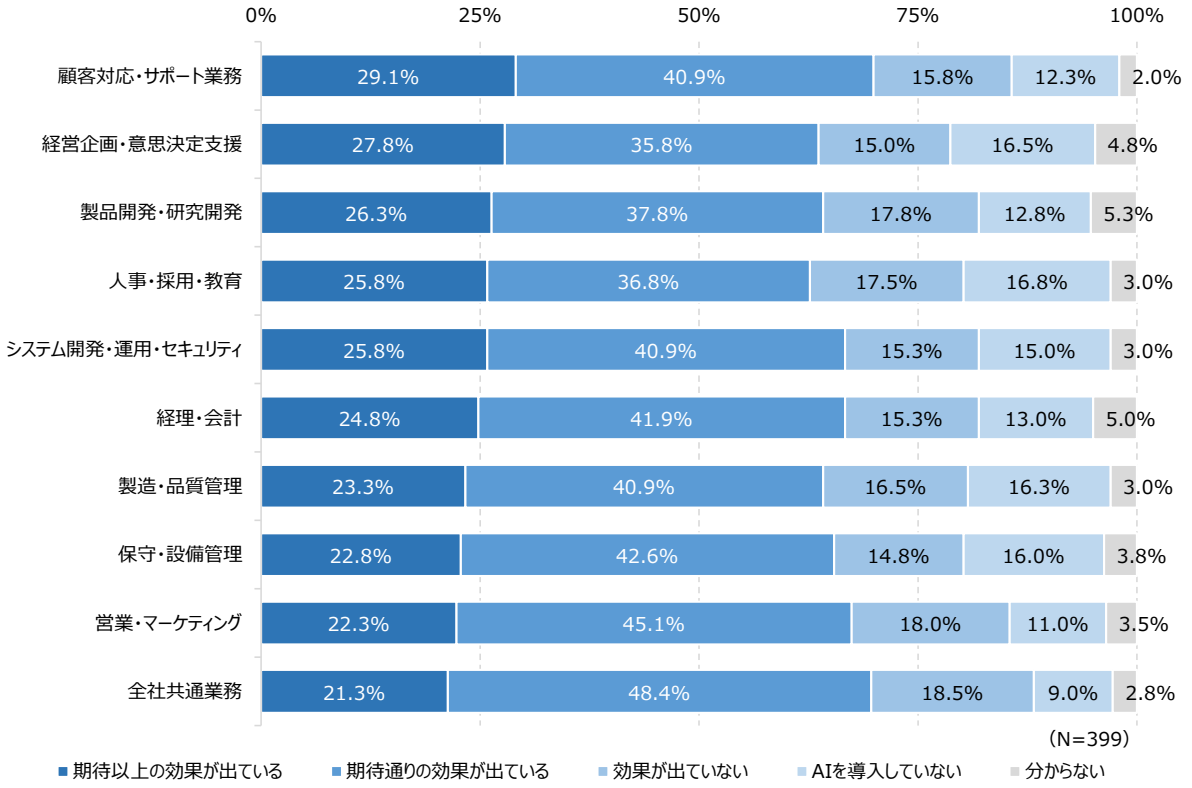
AIは業務でどの程度の活用効果が出ているのだろうか。AIを活用している企業に対し、活用効果について質問を行った（図17）。設定した業務項目は以下の通りである。

① 全社共通業務（文書作成・要約、情報検索、ナレッジ共有など）
② 営業・マーケティング（顧客分析、レコメンド、広告最適化、需要予測など）
③ 顧客対応・サポート業務（チャットボット、音声認識、問い合わせ対応など）
④ 経営企画・意思決定支援（経営ダッシュボード、予算策定支援、経営分析など）
⑤ 経理・会計（請求書処理、経費精算、仕訳自動化など）
⑥ 人事・採用・教育（スキル分析、面接支援、教育コンテンツ生成など）
⑦ 製造・品質管理（画像検査、異常検知、品質予測など）
⑧ 保守・設備管理（予兆保全、稼働分析、点検記録自動化など）
⑨ システム開発・運用・セキュリティ（プログラミング支援、異常・脅威検知、運用自動化など）
⑩ 製品開発・研究開発（製品企画、設計支援、デザイン支援など）

全ての業務項目において、期待以上の効果が出ている割合と期待通りの効果が出ている割合の合計が60%を超えており、AIを導入した企業の多くで一定の効果が確認されていることがわかる。期待以上の効果が出ている割合が最も高いのは「顧客対応・サポート業務」であり、チャットボットや自動応答などAI活用が比較的早くから進んできた領域で、高い効果が実感されている。「経営企画・意思決

定支援」や「製品開発・研究開発」もこれに続いており、高度な判断や創造的な業務において高い効果が出ていることがうかがえる。

一方、「全社共通業務」は、期待以上の効果が出ている割合は最も低いものの、期待通りの効果が出ている割合は最も高くなっている。これは、文書作成や要約、情報検索など定型業務での活用が中心であるため、効率化は図れるものの、業務そのものを大きく変えたり、付加価値を出すまでには至らず、期待を大きく上回る効果は得られにくいためだと考えられる。「営業・マーケティング」も同様である。

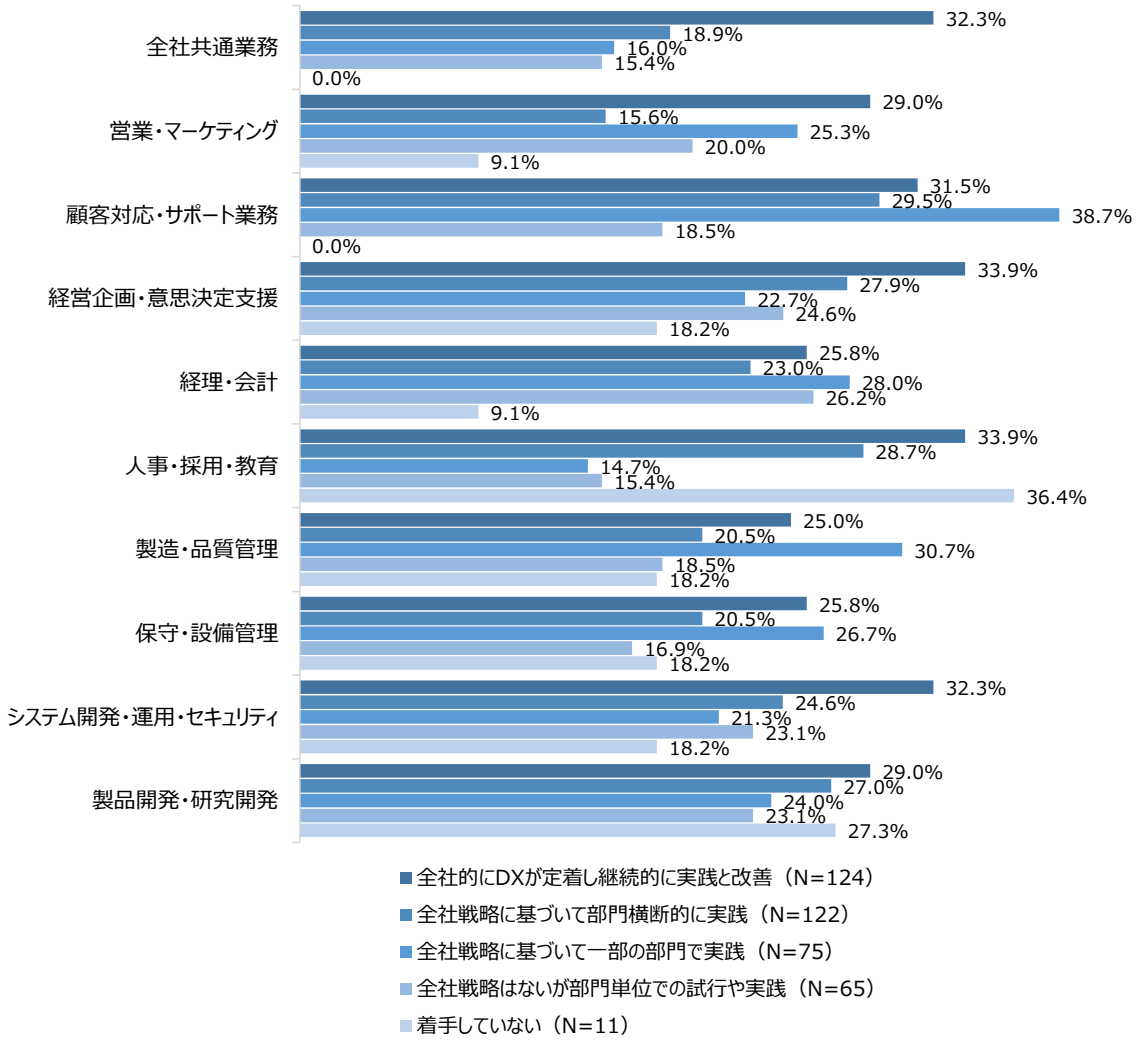


出典：JIPDEC『企業IT利活用動向調査2026』

図17　AIの活用効果

次に、各業務で期待以上の効果が出ている割合を各DX実践段階別に分析を行った（図18）。その結果、DXが定着している企業ほど多くの業務領域で期待以上の効果を得ている傾向が見られ、DXの推進がAI活用の効果創出にも直結していることがわかる。特に「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」「経営企画・意思決定支援」の領域では、DXの実践段階が上がるほど期待以上の効果が出ている割合が高くなる傾向が見られる。これらは部門横断的に関わる業務であり、DXによる業務の標準化やデジタル化が進むことで、AIが活用できるデータや業務プロセスの質が高まり、効果創出につながりやすくなると考えられる。

一方、「人事・採用・教育」「製造・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」といった専門性の高い業務領域では、DXの実践段階と期待以上の効果が出ている割合の間に明確な相関関係は見られない。これらの領域では、DXの推進度合いよりも、業務固有のノウハウやナレッジがAI活用の効果に影響している可能性が高いと考えられる。



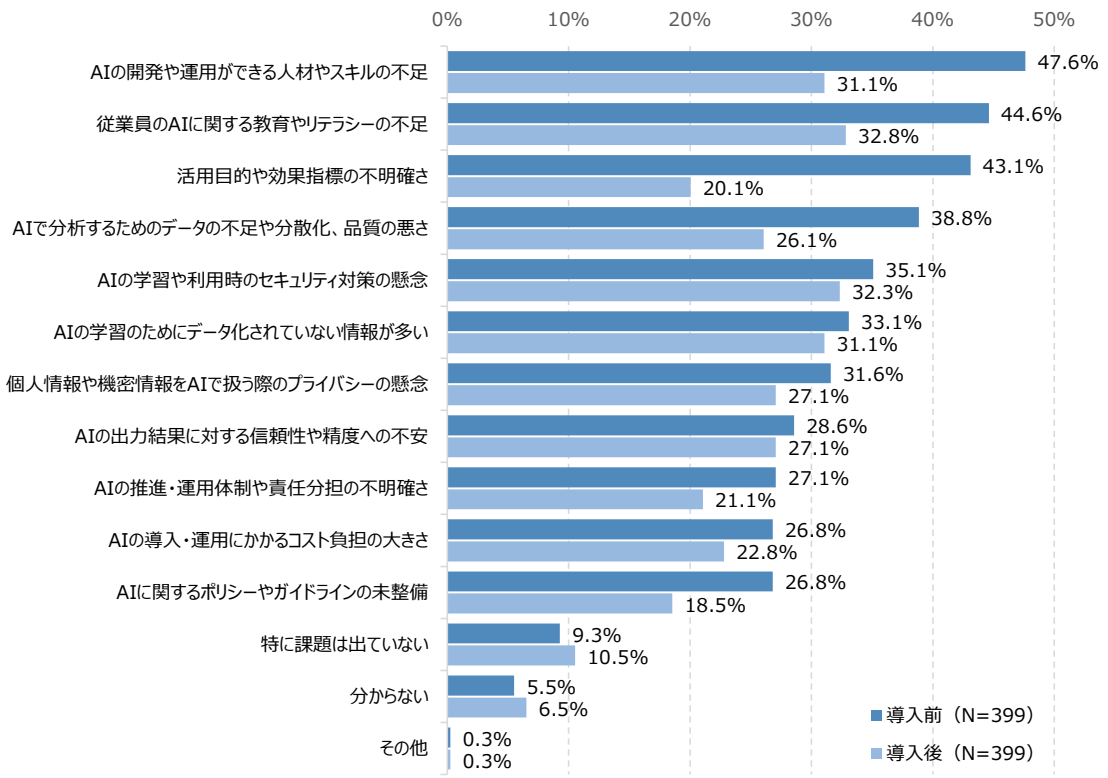
出典：JIPDEC『企業IT利活用動向調査2026』

図18　AI活用で期待以上の効果が出ている業務：DX実践段階別

AI活用の課題

AI活用を進める上でどのような課題が出ているだろうか。AIの導入前と導入後の課題について質問を行った（図19）。導入前の課題として最も多く挙げられているのは「AIの開発や運用ができる人材やスキルの不足」であり、次いで「従業員のAIに関する教育やリテラシーの不足」「活用目的や効果指標の不明確さ」が続いている。導入前の段階では、人材・スキル面の不安と、何をどう活用するかという目的・指標の不明確さが主な障壁となっていることがうかがえる。

導入後になると、これらの課題は全般的に割合が低下する傾向にある。特に「活用目的や効果指標の不明確さ」は導入前から大幅に低下しており、実際に導入することで活用の方向性が明確になるケースが多いことが示されている。一方、「AIの学習や利用時のセキュリティ対策の懸念」「AIの学習のためにデータ化されていない情報が多い」「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」「AIの出力結果に対する信頼性や精度への不安」は、導入前後での低下幅が小さく、導入後も引き続き課題として残存している。データ基盤の整備やセキュリティ対策・プライバシー保護は、導入後も継続的な対応が求められる。



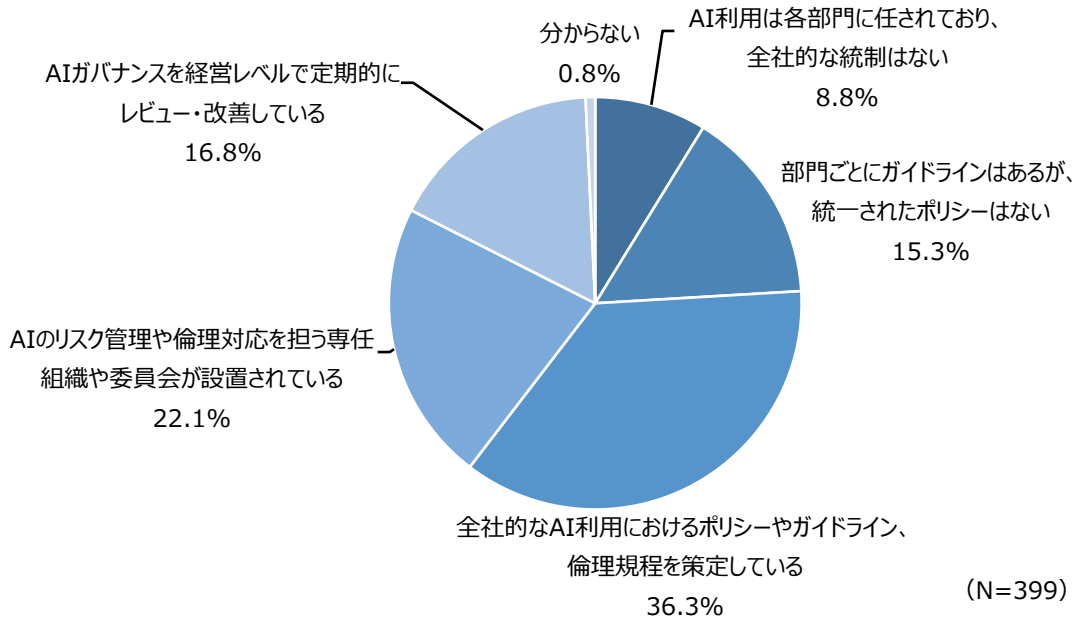
出典：JIPDEC『企業IT利活用動向調査2026』

図19　AI活用を進める上での課題：AIの導入前と導入後の課題

AIのガバナンス体制

AI活用におけるガバナンス体制はどのようになっているだろうか（図20）。「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」が最も多く、3分の1以上の企業がポリシーやガイドラインの整備に取り組んでいる状況にある。さらに「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」と「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」を合わせると、全社レベルでの組織的なガバナンス体制を整えている企業は全体の約7割に達しており、AI活用の拡大に伴いガバナンスへの意識が高まっていることがうかがえる。

一方、「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」と「AI利用は各部門に任されており、全社的な統制はない」が合わせて2割以上となっており、全社横断的なガバナンスが整備されていない企業も一定数残っている。



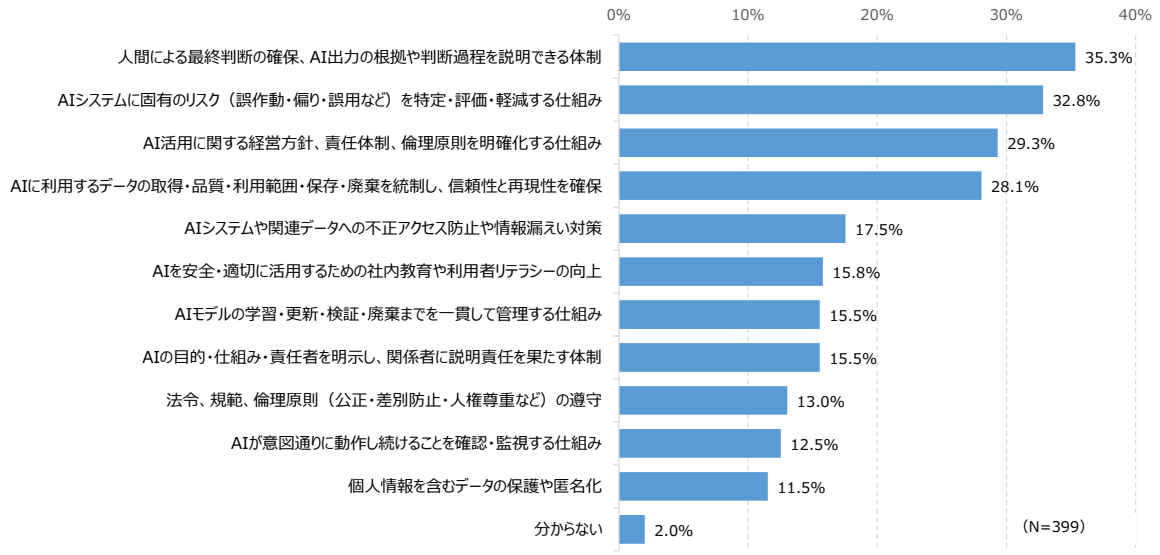
出典：JIPDEC『企業IT利活用動向調査2026』

図20　AI活用におけるガバナンス体制

次に、AIガバナンスにおいて、特に強化が必要と感じる領域について質問を行った（図21）。「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」が最も高く、次いで「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」が続いている。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、最大の強化領域として認識されていることがわかる。

次いで、「AI活用に関する経営方針や責任体制、倫理原則を明確化する仕組み」と「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」が上位に挙げられている。技術的な管理にとどまらず、経営レベルでの方針整備やデータガバナンスを含む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。

一方、「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」「社内教育や利用者リテラシーの向上」「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」といった個別の技術・運用領域は相対的に低い水準にとどまっている。これらはすでに既存のセキュリティ対策やIT管理の延長として取り組まれているケースが多く、AI固有の課題としての優先度が相対的に低く評価されている可能性がある。



出典：JIPDEC『企業IT利活用動向調査2026』

図21　強化が必要なガバナンス領域

調査結果の考察

本章では、生成AIの利用状況と活用効果、活用における課題について調査結果を分析した。そこから得られた考察を以下にまとめる。

1. **AI活用はまだ試行段階にあり、本格活用に向けた取り組みの加速が求められる**： AIを実践・活用している企業は全体の3分の1強にとどまっており、業種・規模によって活用の深度に大きな格差が生じている。情報通信や大企業がAI活用を牽引する一方、サービス業や中小企業では検討・試行段階にとどまる企業が多く、AI活用の裾野を広げるための支援や環境整備が重要な課題となっている。
2. **DXの推進がAI活用の効果を高める土台となる**： DXの実践段階が進むほどAI活用も深化し、より広い業務領域で期待以上の効果が得られる傾向が明確に表れている。特に部門横断的な業務においては、DXによる業務の標準化やデジタル化がAI活用の効果創出に直結している。一方、専門性の高い業務領域ではDXよりも業務固有のノウハウがAI活用の効果に影響しており、業務特性に応じた活用戦略が求められる。
3. **AI導入後も続く課題への継続的な対応が不可欠となる**： AI導入によって活用目的や効果指標の不明確さは解消される傾向にある一方、セキュリティ対策、データ基盤の整備、プライバシー保護、出力結果の信頼性への不安は導入後も課題として残存している。AIを業務に本格的に組み込んでいくためには、ツールの導入にとどまらず、データ基盤の整備やセキュリティ対策、従業員リテラシーの向上を継続的に推進することが不可欠である。
4. **AI活用の拡大に伴い、実効性あるガバナンス体制の構築が急務となる**： 組織的なガバナンス体制を整えている企業は約7割に達しているものの、強化が求められる領域として、人間による最終判断の確保と説明可能性、AI固有リスクの管理、経営レベルでの方針整備、データガバナンスが上

位に挙げられている。ポリシーの策定にとどまらず、包括的なガバナンスを実効性あるものとして機能させることが、AI活用を安全かつ持続的に推進するうえで重要な取り組みとなる。

セキュリティのインシデントと対策の状況

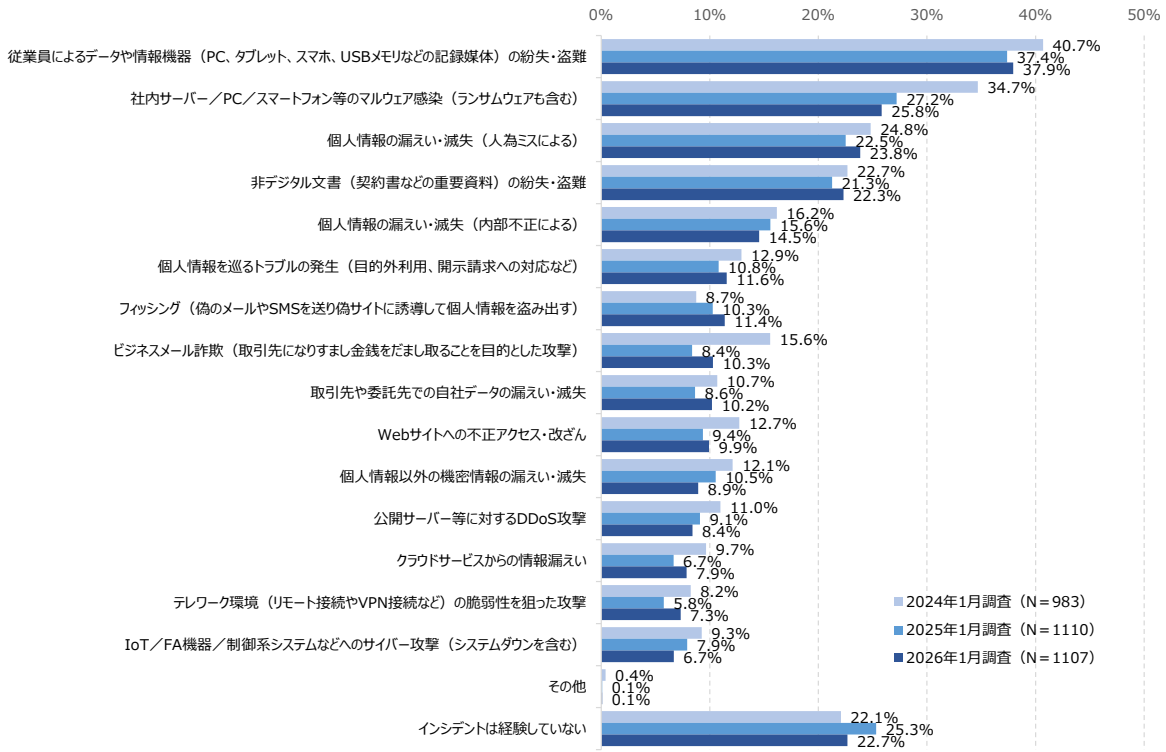
本章では、企業におけるランサムウェア感染被害の状況とセキュリティ対策について調査した結果を分析している。

過去1年に経験したセキュリティインシデント

過去1年に経験したセキュリティインシデントについて質問を行った（図22）。「インシデントは経験していない」が2024年調査の22.1%から2026年調査では22.7%とほぼ横ばいで推移しており、依然として約8割の企業が何らかのセキュリティインシデントを経験していることがわかる。

最も多く経験されているインシデントは「従業員によるデータや情報機器の紛失・盗難」であり、3年連続で最上位を維持している。2024年調査から2026年調査にかけて割合が低下傾向にあるものの、依然として約3社に1社が経験しており、人的要因によるセキュリティリスクが根強く残っていることがうかがえる。

「社内サーバー／PC／スマートフォン等のマルウェア感染」は2024年調査から2026年調査にかけて低下しているものの、依然として高い水準にある。一方、「ビジネスメール詐欺」は2024年調査の8.4%から2026年調査では10.3%へと上昇しており、取引先になりすました金銭詐取を狙った攻撃が急増していることが注目される。「フィッシング」も同様に上昇傾向にあり、巧妙化するソーシャルエンジニアリング攻撃への対策強化が急務となっている。また、「取引先や委託先での自社データの漏えい・滅失」も上昇傾向にあり、自社だけでなくサプライチェーン全体を視野に入れたセキュリティ対策の必要性が高まっている。



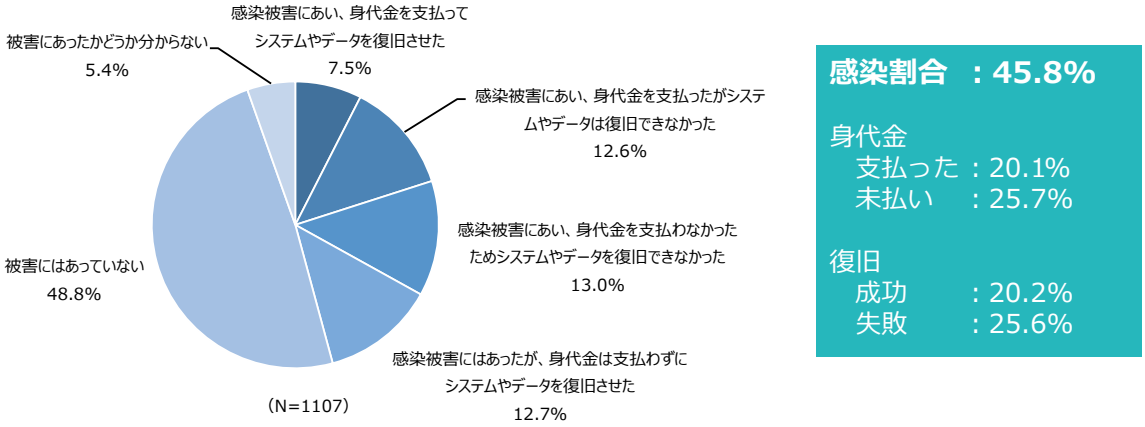
出典：JIPDEC『企業IT利活用動向調査2026』

図22　過去1年に経験したセキュリティインシデント

ランサムウェアの感染状況

近年、ランサムウェアによるサイバー攻撃の脅威が高まっている。そこで、国内企業でのランサムウェア感染被害の経験について質問を行った（図23）。ランサムウェアの感染割合は45.8%と約2社に1社がランサムウェアの被害を経験しており、ランサムウェアが企業にとって極めて現実的な脅威となっていることが示されている。

身代金の支払い状況を見ると、感染被害にあった企業のうち身代金を支払った割合は20.1%、支払わなかった割合は25.7%となっている。注目されるのは復旧の成否であり、身代金を支払っても復旧に成功した割合は20.2%にとどまる一方、復旧に失敗した割合は25.6%に上っている。身代金を支払ったとしてもシステムやデータの復旧が保証されないことを示しており、身代金の支払いがリスク回避の有効な手段とはならないことがうかがえる。



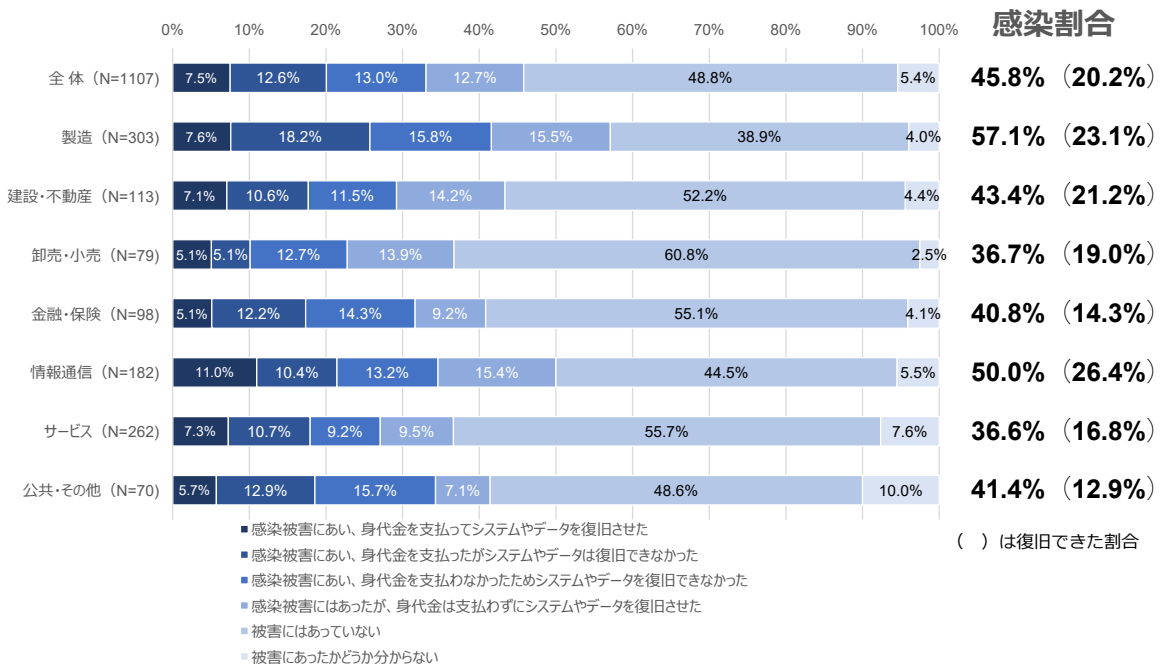
出典：JIPDEC『企業IT利活用動向調査2026』

図23　ランサムウェアの感染被害の経験

次に、業種別に見てみる（図24）。最も感染割合が高いのは製造業の57.1%であり、全体平均の45.8%を大きく上回っている。情報通信も50.0%と高く、この2業種では約2社に1社以上がランサムウェアの被害を経験していることになる。製造業はサプライチェーンの複雑さや生産システムとITシステムの連携が攻撃者に狙われやすい背景があり、情報通信は保有するデータの価値の高さが標的となりやすい要因と考えられる。

一方、サービス業（36.6%）と卸売・小売（36.7%）は感染割合が相対的に低い。ただし、感染割合が低いことがセキュリティ対策の充実を意味するわけではなく、攻撃の標的になりにくい業務特性や、被害を把握できていないケースも含まれる可能性がある点には留意が必要である。

復旧できた割合に着目すると、業種間でのばらつきが大きい。情報通信は感染割合が高い一方で復旧割合も26.4%と比較的高く、セキュリティ対策や復旧体制が他業種より整っていることがうかがえる。一方、公共・その他は復旧割合が12.9%と全業種中最も低く、感染した場合のダメージが特に大きい業種といえる。

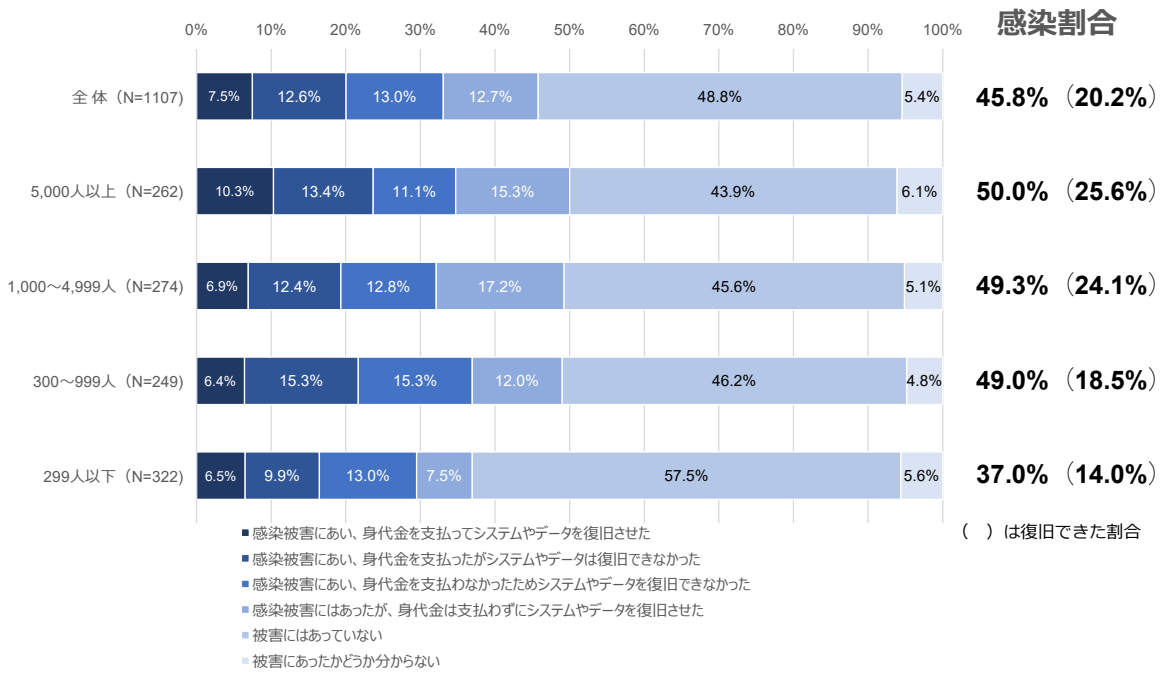


出典：JIPDEC『企業IT利活用動向調査2026』

図24　ランサムウェアの感染被害の経験：業種別

今度は従業員規模別に見てみると、規模が大きいほど感染割合が高い傾向が見られる。（図25）。5,000人以上では50.0%、1,000～4,999人では49.3%、300～999人では49.0%と、300人以上の企業では約半数がランサムウェアの被害を経験している。一方、299人以下では37.0%と他の規模と比べて低くなっており、大企業ほど攻撃者の標的になりやすい傾向がうかがえる。保有するデータの価値や社会的影響力の大きさ、システムの複雑さが、大企業が狙われやすい背景にあると考えられる。ただし、中小企業は、被害を把握できていないケースが含まれている可能性もある。セキュリティが脆弱な中小企業から侵入され、ネットワークを経由して大企業のシステムが攻撃されるサプライチェーン攻撃も増えており、中小企業も決して油断してはならない。

復旧できた割合に着目すると、規模による差が顕著に表れている。5,000人以上では25.6%、1,000～4,999人では24.1%と、大企業ほど復旧割合が高い傾向にある。セキュリティ専門人材やインシデント対応体制など、大企業が持つリソースの優位性が復旧力に反映されていると考えられる。一方、299人以下の中小企業では感染割合は相対的に低いものの、復旧割合も14.0%と全規模中最も低く、ひとたび感染した場合のダメージが特に大きいことが示されている。中小企業はセキュリティ対策に充てられる人材や予算が限られており、感染後の対応力にも課題があることがうかがえる。



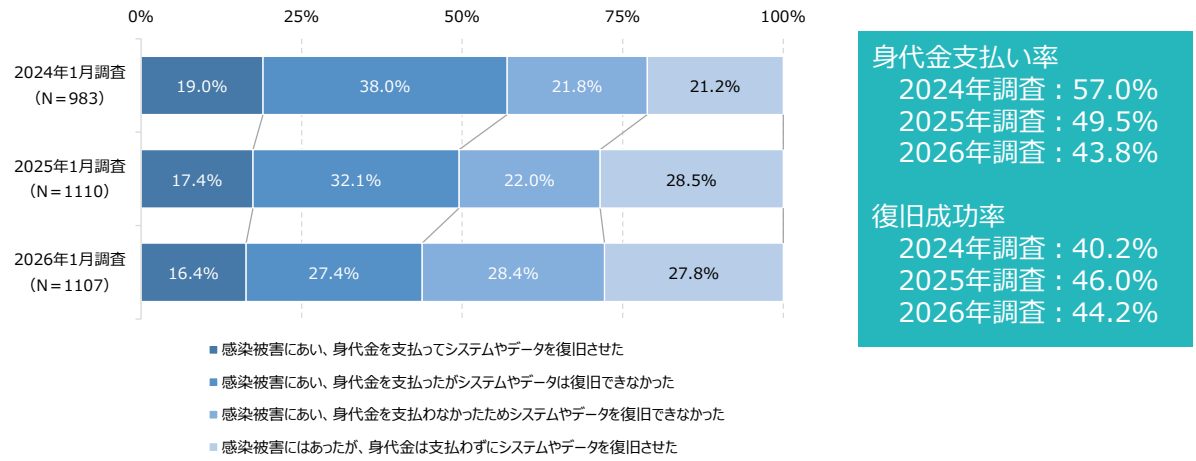
出典：JIPDEC『企業IT利活用動向調査2026』

図25　ランサムウェアの感染被害の経験：従業員規模別

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年調査から2026年調査までの比較を行った（図26）。身代金支払い率は2024年調査の57.0%から2026年調査では43.8%へと3年連続で低下しており、身代金を支払わない企業が着実に増えていることがわかる。

一方、「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」割合は2024年調査の21.8%から2026年調査では28.4%へと上昇している。身代金を支払わない選択をする企業が増えた結果として、復旧できないケースも増加している。

復旧成功率は2024年調査の40.2%から2025年調査の46.0%へと上昇したものの、2026年調査では44.2%へとわずかに低下している。ランサムウェアの攻撃手法が高度化・巧妙化するなかで、復旧成功率の改善が頭打ちになりつつある状況がうかがえる。



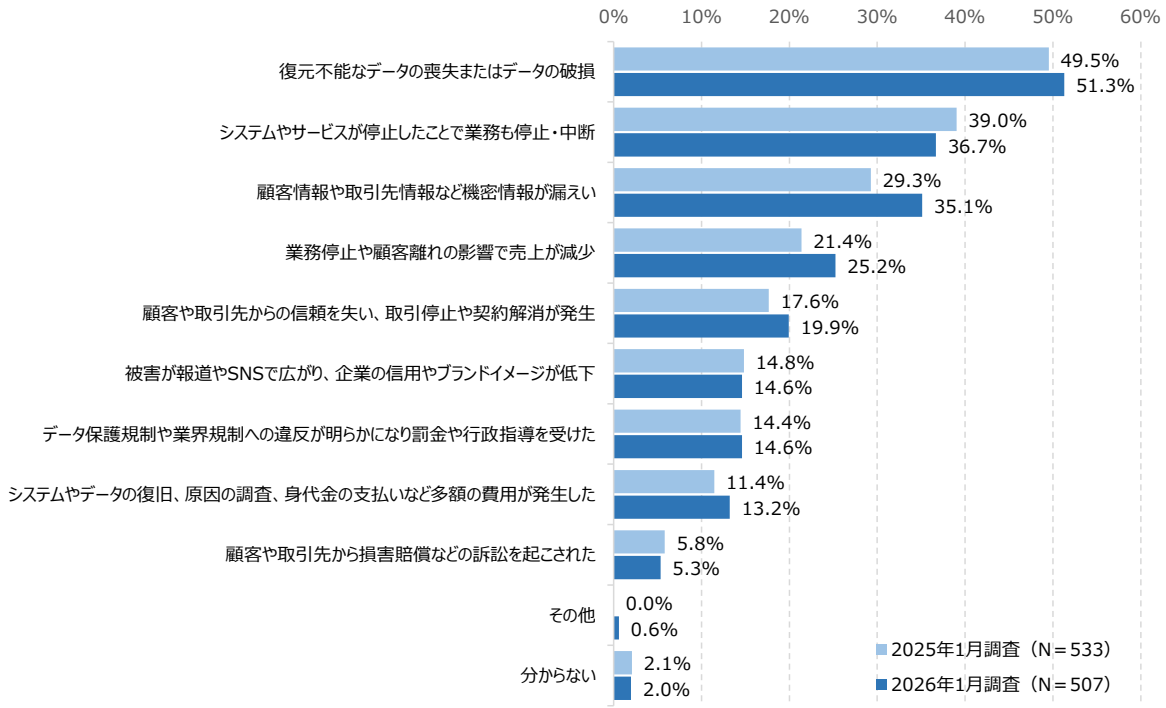
出典：JIPDEC『企業IT利活用動向調査2026』

図26　ランサムウェア感染での身代金支払いと復旧の変化

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企業はどのような影響を受けているのだろうか。ランサムウェア感染被害の影響について質問を行った（図27）。「復元不能なデータの喪失またはデータの破損」が最も高く、2025年調査からさらに上昇しており、データの損失がランサムウェア感染の最大の被害として引き続き深刻な問題となっていることがわかる。「システムやサービスが停止したことで業務も停止・中断」も高い水準にあり、感染による事業活動への直接的な打撃が広く経験されていることがうかがえる。

注目されるのは「顧客情報や取引先情報など機密情報が漏えい」が、29.3%から35.1%へと大幅に上昇している点である。単なるシステム障害にとどまらず、機密情報の外部流出を伴うケースが増加しており、感染被害の質的な深刻化が進んでいることが示されている。「業務停止や顧客離れの影響で売上が減少」や「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」も上昇傾向にあり、ランサムウェア感染が直接的な経営損失や取引関係の毀損にまで波及するケースが増えていることがうかがえる。また、「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」も前回調査から上昇しており、感染後の対応コストの増大も企業経営への打撃として無視できない水準となっている。



出典：JIPDEC『企業IT利活用動向調査2026』

図27　ランサムウェア感染被害の影響

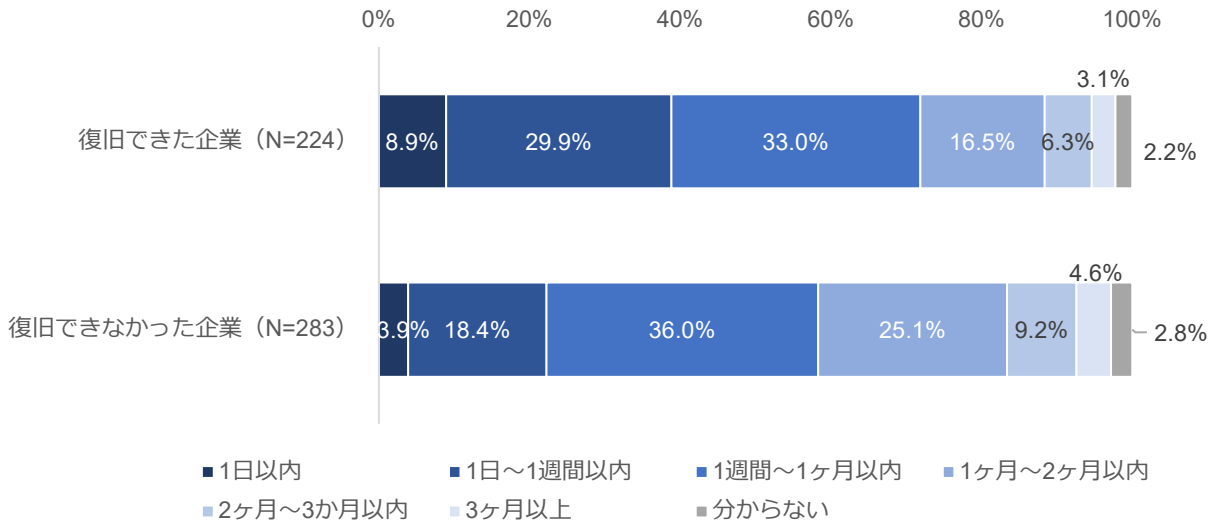
ランサムウェア感染からの復旧期間

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ているのだろうか。ランサムウェア感染企業に対し、復旧期間について質問を行った（図28）。復旧できなかった企業に対しては、復旧をあきらめた時点での期間を質問している。復旧できた企業では、「1日以内」

「1日～1週間以内」「1週間～1ヶ月以内」を合わせると7割以上の企業が1ヶ月以内に復旧している。しかし、「1ヶ月～2ヶ月以内」（16.5%）、「2ヶ月～3ヶ月以内」（6.3%）、「3ヶ月以上」（3.1%）と、復旧に長期間を要した企業も約4分の1に上っており、復旧には相当の時間とリソースが必要となることがうかがえる。

復旧できなかった企業（復旧をあきらめた時点での期間）では、「1週間～1ヶ月以内」が36.0%と最も高く、「1ヶ月～2ヶ月以内」（25.1%）、「1日～1週間以内」（18.4%）が続いている。相当の時間と労力を費やした末に復旧を断念しているケースが多く、感染後の対応が長期化するほど事業への影響が深刻になることが示されている。

復旧できた企業と復旧できなかった企業を比較すると、復旧できた企業のほうが短期間での対応割合が高い傾向にある。感染後の初動対応の迅速さが復旧の成否を左右する重要な要因であることがうかがえる。



注1）復旧できなかった企業は復旧をあきらめた時点での期間を回答

出典：JIPDEC『企業IT利活用動向調査2026』

図28　ランサムウェア感染からの復旧期間

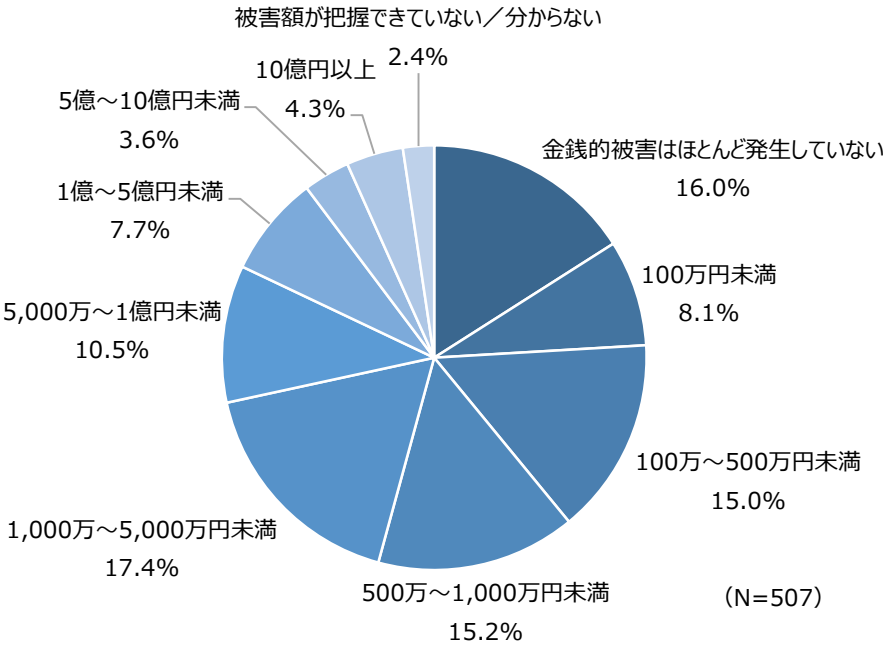
ランサムウェア感染の被害額

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ているだろうか。ランサムウェア感染企業に対し、その被害額について質問を行った（図29）。被害額に含む項目は以下の通りとした。

- 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

「金銭的被害はほとんど発生していない」が16.0%にとどまり、感染した企業の約8割以上が何らかの金銭的被害を受けていることがわかる。被害額の分布を見ると、「1,000万～5,000万円未満」が最も多く、「500万～1,000万円未満」「100万～500万円未満」がこれに続いており、数百万円から数千

万円規模の被害を受けた企業が多いことがうかがえる。一方、「1億～5億円未満」（7.7%）、「5億～10億円未満」（3.6%）、「10億円以上」（4.3%）と、億円規模の大きな被害を受けた企業も相当数存在しており、ランサムウェア感染が企業経営に与える財務的インパクトの深刻さが改めて浮き彫りとなっている。



出典：JIPDEC『企業IT利活用動向調査2026』

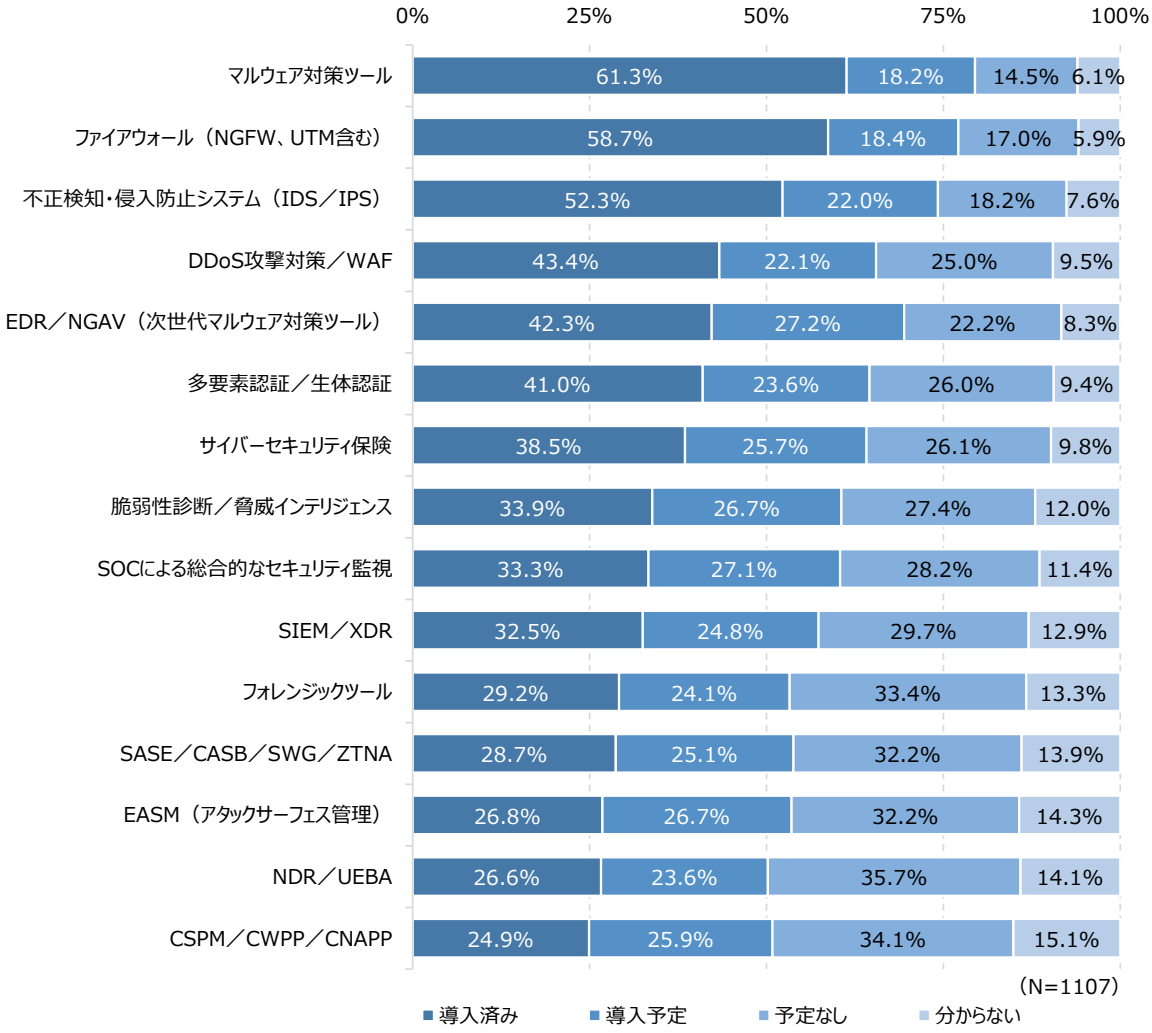
図29　ランサムウェア感染による被害額

サイバー攻撃対策向けのセキュリティツール・サービスの導入状況

外部からのサイバー攻撃対策としてどのようなセキュリティツール・サービスが導入されているのだろうか（図30）。「マルウェア対策ツール」と「ファイアウォール」が導入済み割合で上位にあり、過半数の企業が導入済みである。「不正検知・侵入防止システム（IDS／IPS）」もこれに続いており、これらの従来型セキュリティ対策は企業のセキュリティ基盤として広く普及していることがうかがえる。

一方、より高度な脅威に対応するための製品・サービスについては、導入済み割合が相対的に低い。「EDR／NGAV（次世代マルウェア対策ツール）」や「多要素認証／生体認証」は4割超の企業が導入済みであるものの、「脆弱性診断／脅威インテリジェンス」「SOCによる総合的なセキュリティ監視」「SIEM／XDR」はいずれも導入済みが3割台にとどまっており、高度な監視・検知体制の整備はまだ途上にある企業が多い。

ゼロトラストセキュリティの実現に向けた製品群である「SASE／CASB／SWG／ZTNA」や「EASM（アタックサーフェス管理）」「NDR／UEBA」「CSPM／CWPP／CNAPP」といった製品は導入済み割合が3割未満にとどまっており、ゼロトラストへの移行はまだ緒についた段階にある企業が多いことが示されている。ただし、「導入予定」の割合も一定程度あり、今後の普及が見込まれる。



出典：JIPDEC『企業IT利活用動向調査2026』

図30　外部からのサイバー攻撃対策として導入しているセキュリティ製品・サービス

情報漏えい対策の実施状況

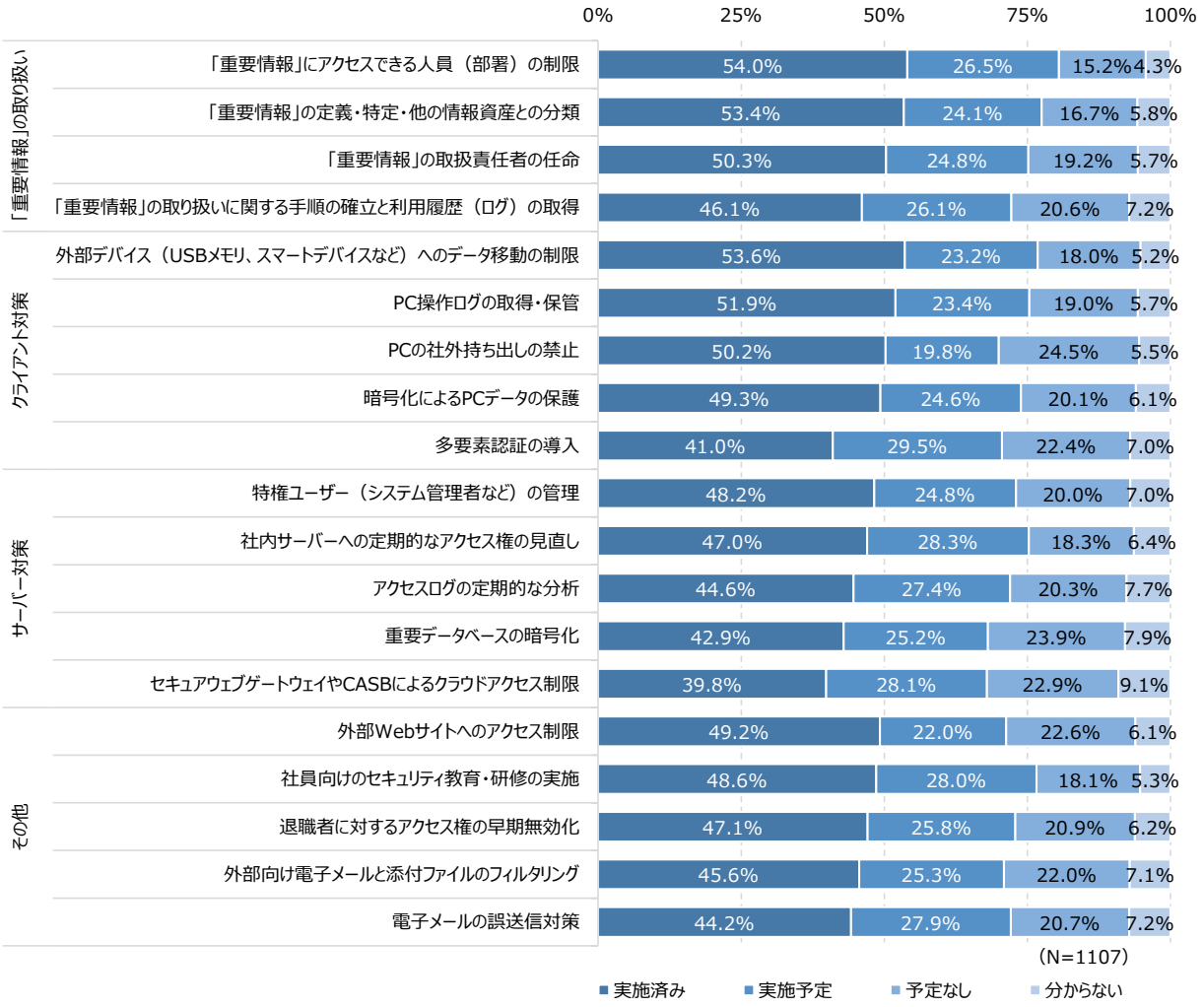
次に、内部からの情報漏えい対策の実施状況について質問を行った（図31）。「重要情報」の取り扱い、クライアント対策、サーバー対策、その他の各領域において、過半数前後の企業が主要な対策を実施済みであり、内部脅威への対策が広く浸透していることがわかる。

「重要情報」の取り扱い領域では、「重要情報にアクセスできる人員（部署）の制限」と「重要情報の定義・特定・他の情報資産との分類」が最も高い実施率となっており、情報資産の適切な管理とアクセス制御が内部対策の基本として定着していることがうかがえる。一方、「重要情報の取り扱いに関する手順の確立と利用履歴（ログ）の取得」は他の項目と比べて実施率がやや低く、操作履歴の可視化・追跡体制の整備が遅れている企業が一定数残っている。

クライアント対策では、「外部デバイスへのデータ移動の制限」や「PC操作ログの取得・保管」「PCの社外持ち出しの禁止」が高い実施率を示している。一方、「多要素認証の導入」は実施率が相対的に低く、内部不正やなりすましへの対策としてさらなる普及が求められる。

サーバー対策では、「特権ユーザーの管理」や「社内サーバーへの定期的なアクセス権の見直し」

の実施率が高い一方、「重要データベースの暗号化」や「セキュアウェブゲートウェイやCASBによるクラウドアクセス制限」は相対的に低く、クラウド環境の普及に対応したデータ保護の取り組みが追いついていない実態がうかがえる。



出典：JIPDEC『企業IT利活用動向調査2026』

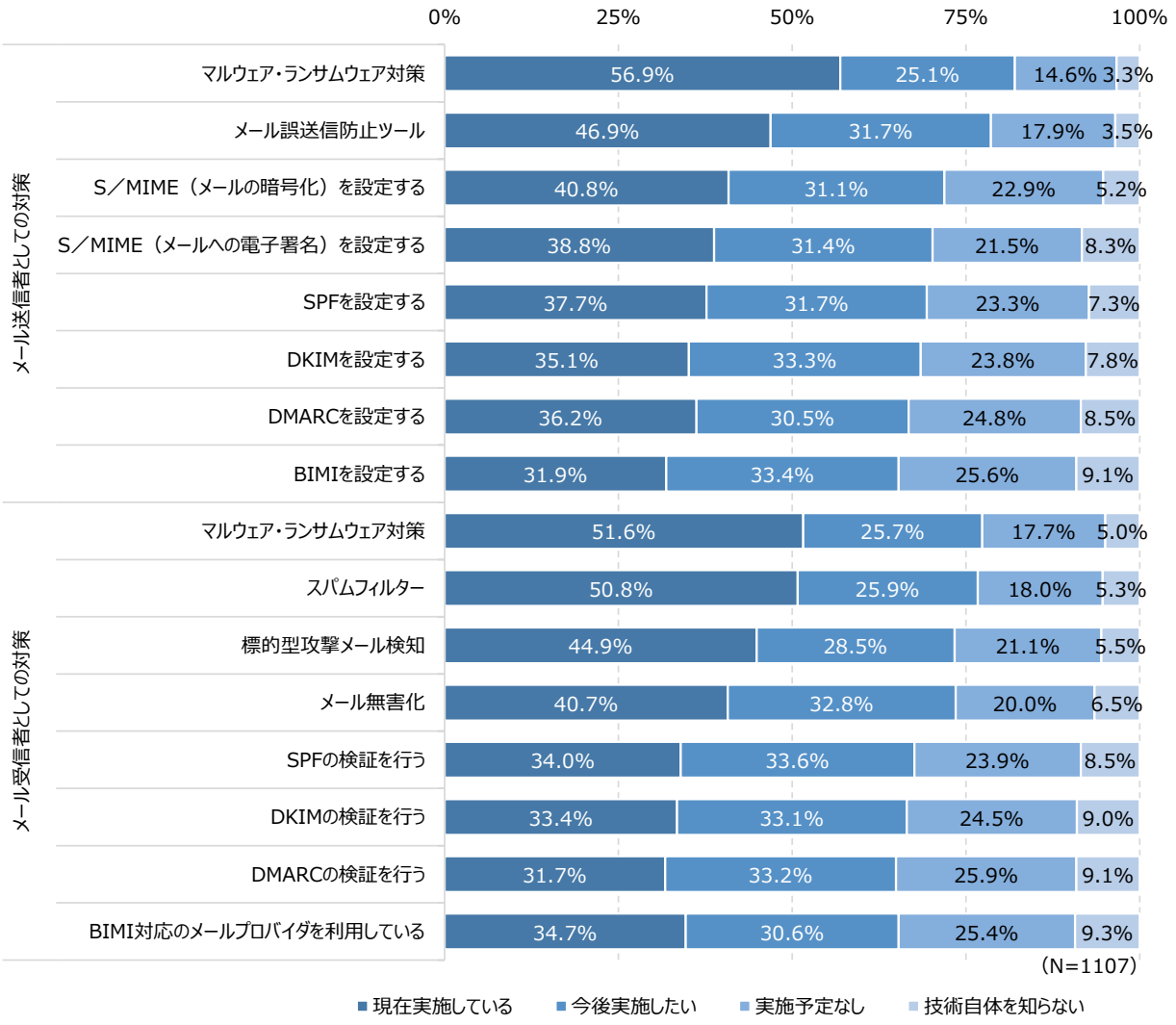
図31　内部からの情報漏えい対策として実施している項目

電子メール向けセキュリティ対策の実施状況

電子メール向けのセキュリティ対策の実施状況について質問を行った（図32）。メール送信者としての対策とメール受信者としての対策の両面から見ると、全体的に基本的な対策は一定程度普及しているものの、より高度な対策の導入は道半ばにある企業が多いことがわかる。

メール送信者としての対策では、「マルウェア・ランサムウェア対策」が最も高い実施率を示しており、「メール誤送信防止ツール」がこれに続いている。一方、なりすましメール対策として有効なSPF・DKIM・DMARCの設定は、実施率がいずれも3割台にとどまっている。ビジネスメール詐欺やフィッシング攻撃が急増するなかで、送信ドメイン認証の普及が急務であることが示されている。BIMIの実施率は最も低く、ブランド保護と受信者の視覚的な信頼確保に向けた取り組みはまだ緒についた段階にある。

メール受信者としての対策では、「マルウェア・ランサムウェア対策」と「スパムフィルター」が過半数の企業で実施されており、基本的な受信対策は比較的広く普及している。「標的型攻撃メール検知」や「メール無害化」も4割前後の企業が実施しているものの、SPF・DKIM・DMARCの検証については実施率が3割台にとどまっており、送信者側の認証対策と同様に受信者側の検証体制も十分に整備されていない企業が多い。



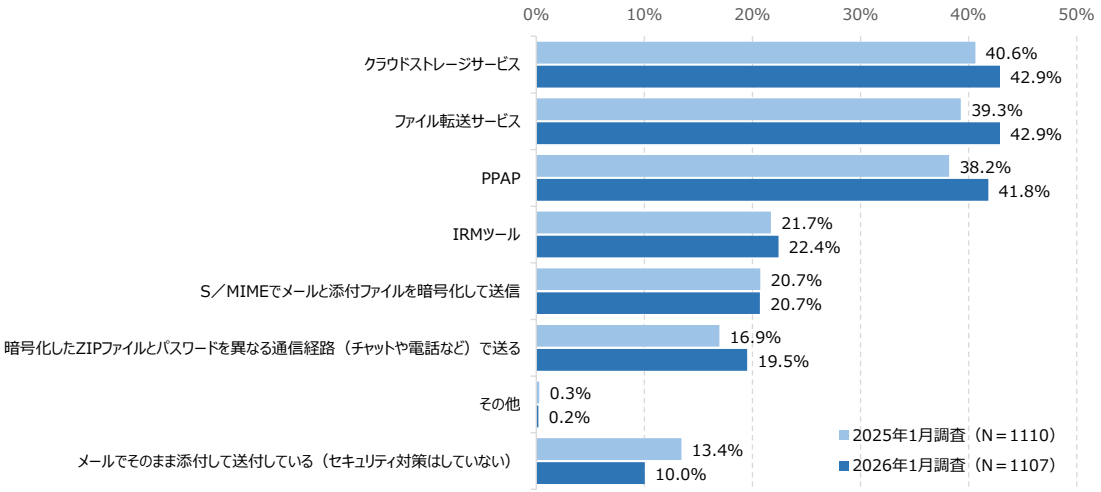
出典：JIPDEC『企業IT利活用動向調査2026』

図32　電子メールのセキュリティ対策の実施状況

電子メールからランサムウェアなどのマルウェアに感染する要因として、マルウェアを含んだ添付ファイルを開いてしまうことがある。そこで、電子メールのファイル送付手段として社内で標準としている手段について質問を行った（図33）。2025年調査と比較すると、「クラウドストレージサービス」と「ファイル転送サービス」はいずれも上昇しており、より安全なファイル送付手段への移行が着実に進んでいることがわかる。

一方、PPAPも38.2%から41.8%へと上昇しており、セキュリティ上の問題が広く認識されているにもかかわらず利用率が増加している点は看過できない。PPAPはパスワード付きZIPファイルとパスワードを同一経路で送信するため、マルウェアの検知を回避できず実質的なセキュリティ効果がないこ

とが知られており、政府機関も廃止を呼び掛けている。それでもなお約4割の企業が社内標準として使用し続けているのは、長年の慣習からの脱却が進んでいない実態を示している。



注1：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手段

出典：JIPDEC『企業IT利活用動向調査2026』

図33　社内で標準としている電子メールのファイル送付手段

調査結果の考察

本章では、企業におけるランサムウェア感染被害の状況とセキュリティ対策についての調査結果を分析した。そこから得られた考察を以下にまとめる。

1. **ランサムウェアはすべての企業が備えるべき経営リスクである**：約2社に1社がランサムウェアの被害を経験しており、業種・規模を問わず現実的な脅威となっている。感染した企業の約8割以上が金銭的被害を受けており、数千万円から億円規模の損失に至るケースも少なくない。身代金を支払っても復旧が保証されない現実を踏まえると、感染を未然に防ぐ予防的な対策と、感染後に迅速に復旧できるバックアップ体制やBCPの整備を経営課題として優先的に位置付けることが不可欠である。
2. **サイバー攻撃の巧妙化に対応した多層的なセキュリティ体制への移行が急務となる**：ビジネスメール詐欺やフィッシングなどのソーシャルエンジニアリング攻撃が増加しており、サイバー攻撃の手口は年々高度化・多様化している。マルウェア対策ツールやファイアウォールなど従来型の境界防御は広く普及しているものの、高度な監視・検知体制やゼロトラストセキュリティに向けた製品の導入はまだ途上にある企業が多い。侵入を前提とした検知・対応・復旧までを包括する多層的なセキュリティ体制への移行が求められる。
3. **内部脅威対策とメールセキュリティの深化が引き続き重要な課題となる**：内部からの情報漏えい対策は基本的な取り組みが広く普及している一方、ログの活用や多要素認証、クラウド環境に対応したデータ保護など、対策の深化が遅れている領域が残っている。また、メールセキュリティ

ではSPF・DKIM・DMARCなどの送受信ドメイン認証の導入が3割台にとどまっており、ビジネスメール詐欺やフィッシング対策の観点から普及の加速が急務となっている。

4. **セキュリティ対策は技術的対応だけでなく人的・組織的な取り組みとの一体推進が必要となる**：最も多く経験されているインシデントは従業員によるデータや情報機器の紛失・盗難であり、人的要因によるリスクが根強く残っている。PPAPの利用率が前回調査から上昇しているように、技術的な問題が認識されていても慣習からの脱却が進まないケースも多い。技術的対策の整備と並行して、社員へのセキュリティ教育・研修の継続的な実施と、経営層が主導する組織全体のセキュリティ文化の醸成が、インシデントを減らすための重要な鍵となる。

プライバシー/個人情報保護に対する取り組み

本章では、プライバシー/個人情報保護に対する取り組み状況について調査した結果を分析している。

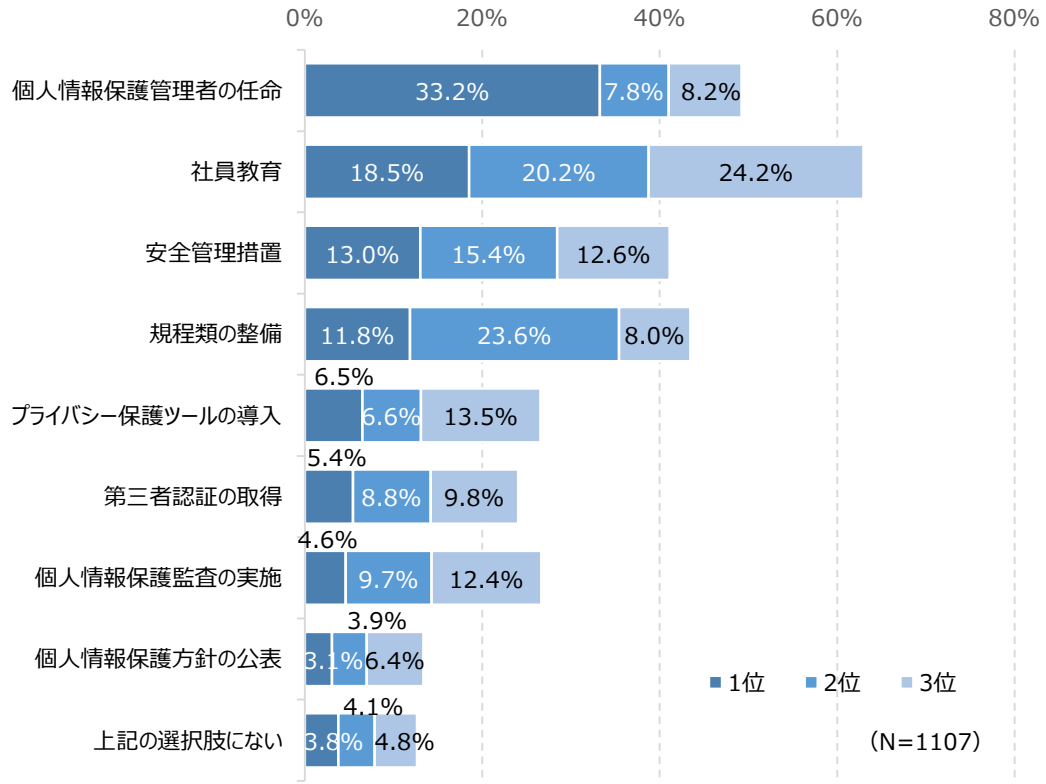
個人情報保護において注力している取り組み

個人情報保護に対する取り組みにおいて、特に注力している取り組みについて質問を行った（図34）。ここでは、特に注力している取り組みについて、1位～3位までを順位付けをして回答している。その結果、「個人情報保護管理者の任命」が1位に挙げた割合で最も高く、責任体制の明確化が個人情報保護の最優先事項として広く認識されていることがわかる。

「社員教育」は1位こそ「個人情報保護管理者の任命」に次ぐ水準にとどまるものの、2位と3位への回答割合が全項目中最も高く、1位から3位の合計では最上位となっている。個人情報漏えいの多くが人的ミスや内部不正に起因することを踏まえると、従業員への継続的な教育・啓発活動が個人情報保護の根幹として広く重視されていることがうかがえる。

「安全管理措置」と「規程類の整備」も上位に位置しており、技術的・物理的な対策の整備と社内ルールの策定が個人情報保護の基盤として重要視されていることが示されている。特に「規程類の整備」は2位への回答割合が高く、管理者の任命や教育と並んで組織的な取り組みの土台として位置付けられていることがうかがえる。

一方、「プライバシー保護ツールの導入」「第三者認証の取得」「個人情報保護監査の実施」「個人情報保護方針の公表」は相対的に低い水準にとどまっている。プライバシー保護ツールの活用や外部認証・監査といった高度な取り組みの普及はまだ限定的であり、個人情報保護の実効性をさらに高めるうえでの課題として残っている。



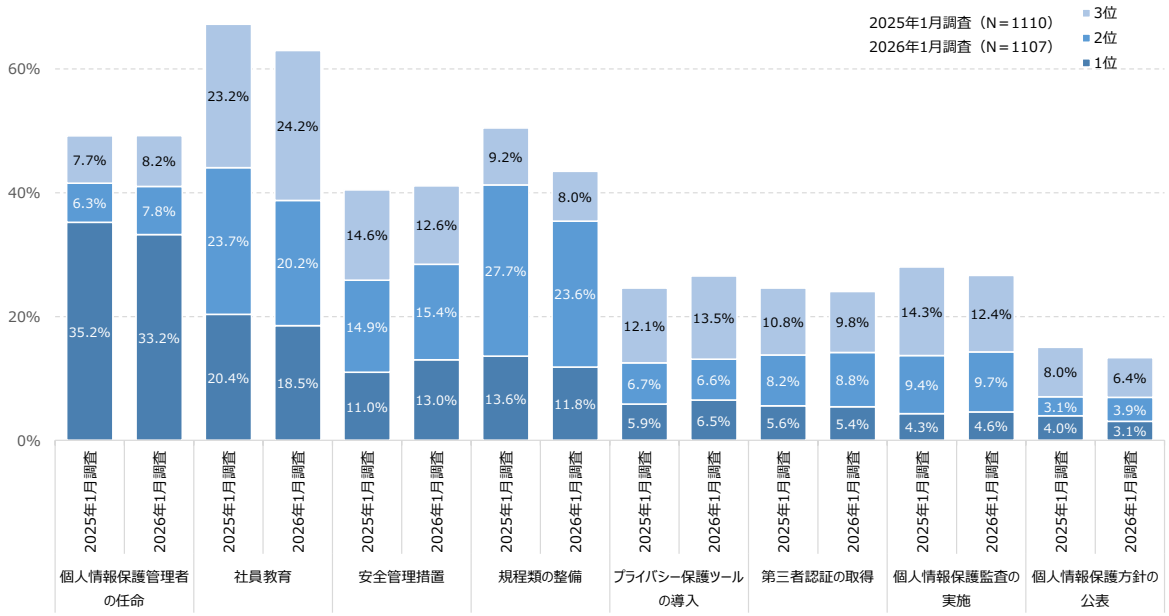
注1：特に注力している取り組みについて1位～3位までを順位付けしている

出典：JIPDEC『企業IT利活用動向調査2026』

図34　個人情報保護において注力している取り組み：順位付け

次に、2025年調査と比較を行った（図35）。「個人情報保護管理者の任命」は1位に挙げた割合が35.2%から33.2%へとわずかに低下しており、責任体制の整備がすでに一定程度定着し、他の取り組みへの関心が相対的に高まっていることが背景にあると考えられる。また、「社員教育」も1位への回答割合が20.4%から18.5%へと低下しており、最優先事項として位置付ける企業がわずかに減少している。一方で2位と3位への回答割合は増加しており、最優先ではないものの重要な取り組みとして継続的に重視する企業は引き続き多い。

「規程類の整備」も1位から3位の合計が前回調査から増加しており、社内ルールの整備・見直しへの関心が高まっている。一方、「安全管理措置」は前回調査とほぼ横ばいで推移しており、技術的・物理的な対策の整備については取り組みが一定程度定着した段階にあることがうかがえる。



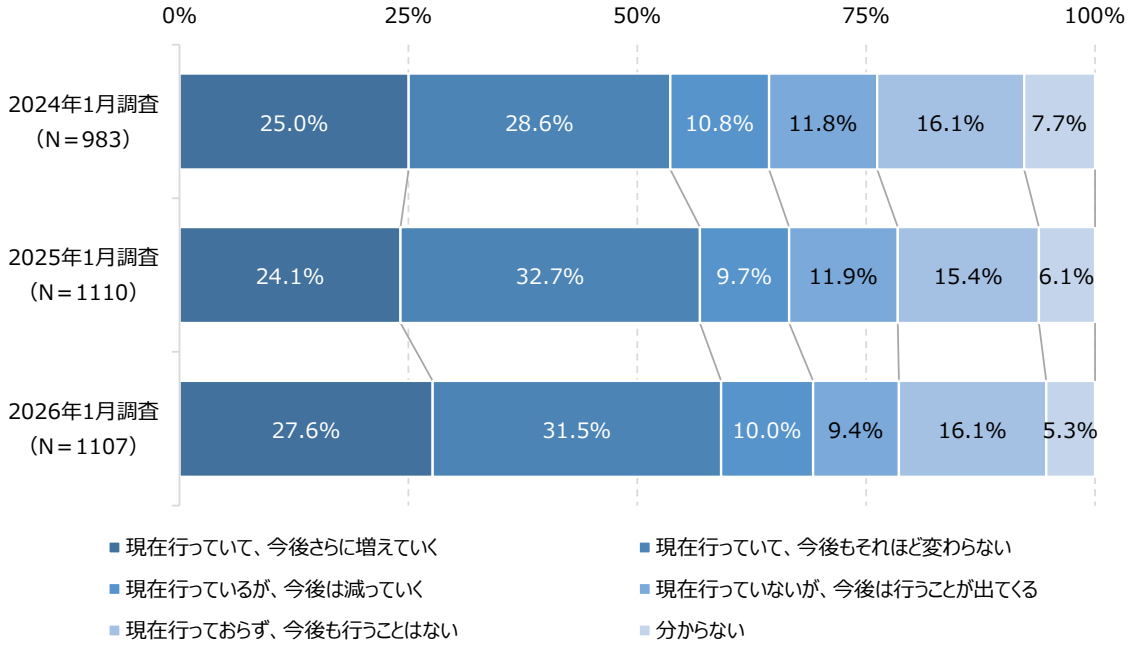
出典：JIPDEC『企業IT利活用動向調査2026』

図35　個人情報保護において注力している取り組み：2025年調査との比較

データの越境移転の状況

データの越境移転の状況について質問を行った（図36）。データの越境移転とは、個人情報を海外の第三者に提供することである。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。ここでは2024年調査、2025年調査との比較を行っている。現在越境移転を行っている企業（「今後さらに増えていく」「今後もそれほど変わらない」「今後は減っていく」の合計）は2026年調査で69.1%と、2024年調査（64.4%）から増加しており、データの越境移転がより広く行われるようになっていることがわかる。

なかでも「現在行っていて、今後さらに増えていく」の割合が2025年調査の24.1%から2026年調査では27.6%へと上昇しており、越境移転をさらに拡大させる意向を持つ企業が着実に増えていることが示されている。この背景には、グローバルなビジネス展開やクラウドサービスの活用拡大があると考えられる。

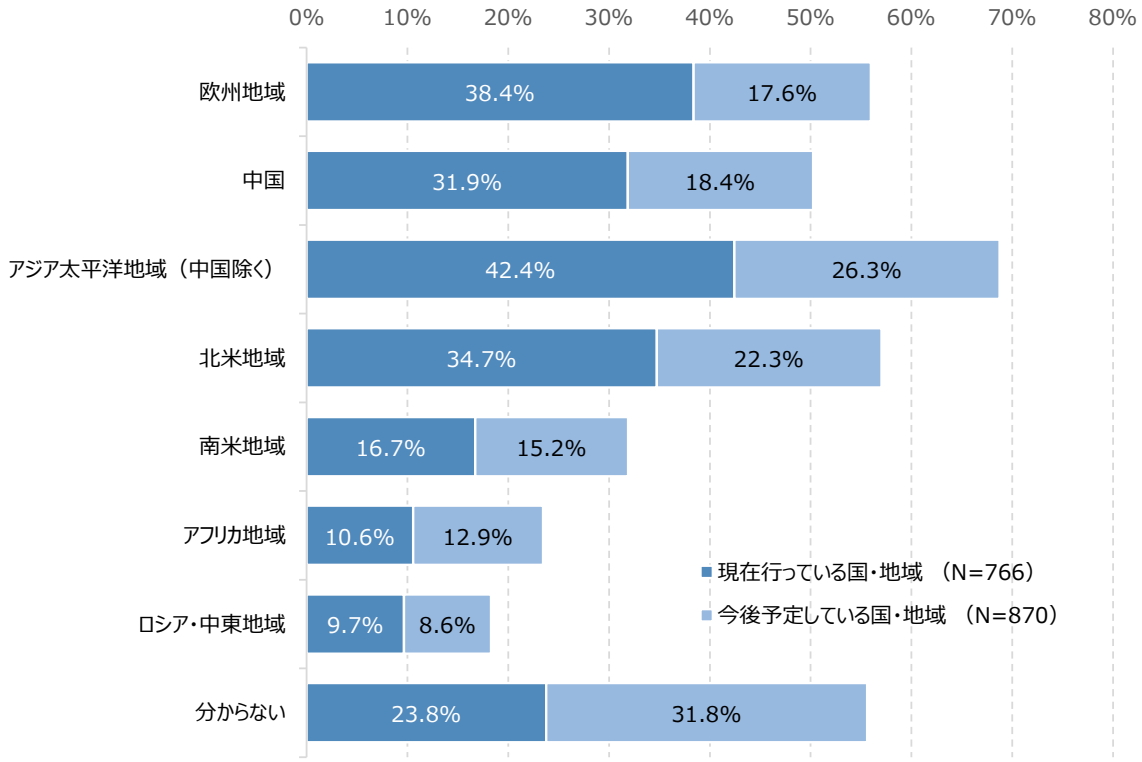


出典：JIPDEC『企業IT利活用動向調査2026』

図36　データの越境移転の状況

それでは、データの越境移転先はどのような国・地域になっているのだろうか（図37）。「アジア太平洋地域（中国除く）」が現在の移転先として最も多く、「欧州地域」「中国」「北米地域」がこれに続いている。日本企業にとってアジア太平洋地域が最大のデータ越境移転先となっており、製造業やサービス業を中心とした域内のビジネス展開の広がりが背景にあると考えられる。

今後予定している移転先を見ると、「アジア太平洋地域（中国除く）」が最も多く、「北米地域」が続いている。「アフリカ地域」は現在の10.6%から今後予定では12.9%へと上昇しており、新興市場への越境移転が徐々に広がりつつある。



出典：JIPDEC『企業IT利活用動向調査2026』

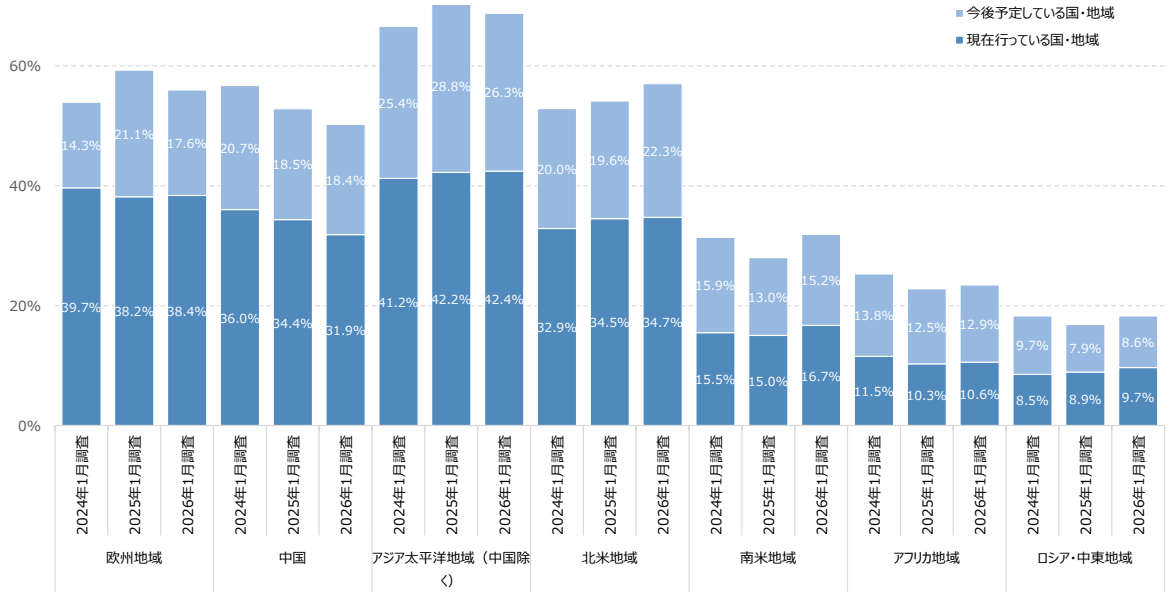
図37　データの越境移転先

次に、2024年調査から2026年調査までの3年間の経年変化を見てみる（図38）。「欧州地域」への現在の越境移転は39.7%（2024年調査）から38.4%（2026年調査）へとわずかに低下しているものの、ほぼ横ばいで推移しており、引き続き主要な移転先として位置付けられている。

「中国」への越境移転は36.0%（2024年調査）から31.9%（2026年調査）へと低下傾向が続いている。中国のデータセキュリティ法や個人情報保護法の施行・強化を受け、リスク管理の観点から中国へのデータ移転を慎重に見直す企業が増えていることが背景にあると考えられる。

「アジア太平洋地域（中国除く）」は3年間を通じて最も高い現在の移転割合を維持しており、日本企業にとってアジア太平洋地域が引き続き最大のデータ越境移転先となっている。今後予定している移転先としても最上位を維持しており、域内ビジネスの拡大に伴いデータの流通がさらに活発化することが見込まれる。

「北米地域」は現在の移転割合が32.9%（2024年調査）から34.7%（2026年調査）へと上昇傾向にあり、クラウドサービスの活用拡大やデジタルビジネスの深化を背景に、北米との間のデータ流通が拡大していることがうかがえる。「南米地域」「アフリカ地域」「ロシア・中東地域」は絶対的な水準は低いものの、3年間で緩やかな上昇傾向が見られ、新興地域へのビジネス展開に伴うデータ越境移転が徐々に広がりつつある。



出典：JIPDEC『企業IT利活用動向調査2026』

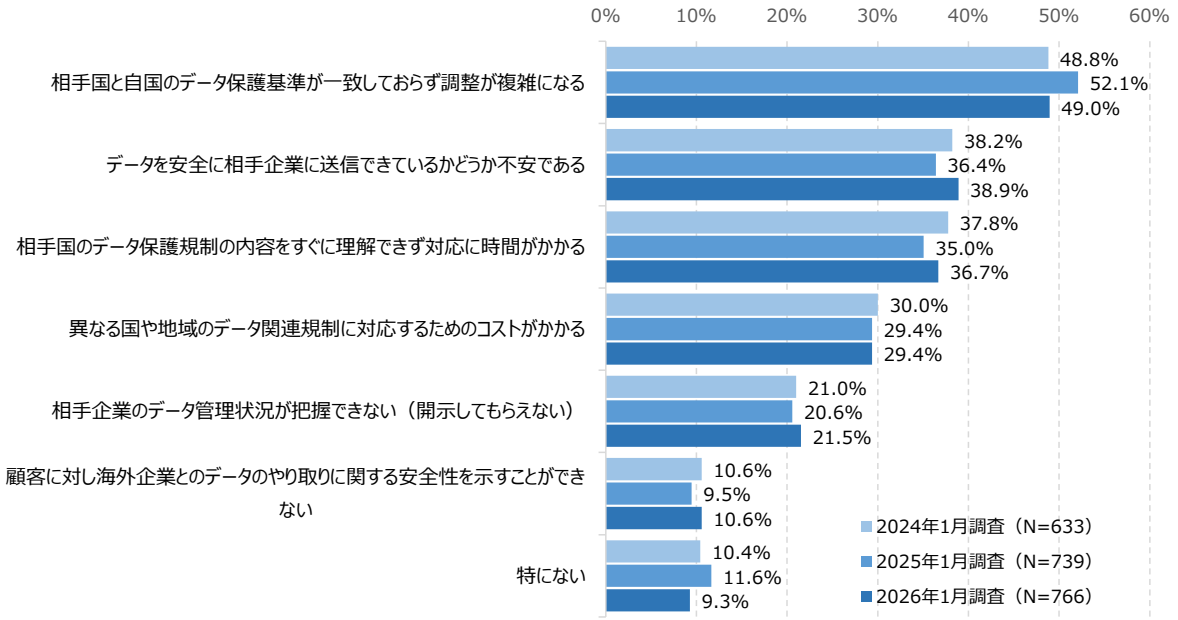
図38　データの越境移転先：2024年調査、2025年調査との比較

海外とのデータのやり取りにおける課題

海外企業とデータをやり取りする際、どのような問題が生じているだろうか。2024年調査から2026年調査までの3年間の経年変化を見てみる（図39）。最も多く挙げられているのは「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」であり、3年間を通じて最上位を維持している。2026年調査では49.0%と約半数の企業が課題として認識しており、各国・地域のデータ保護規制の複雑さが越境データ流通の最大の障壁となっていることが示されている。

「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」は2025年調査の36.4%から2026年調査では38.9%へと上昇しており、データ送信時のセキュリティへの不安が高まっていることがうかがえる。「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」も高い水準で推移しており、各国の規制動向を継続的に把握・対応するための体制整備が課題となっている。

「異なる国や地域のデータ関連規制に対応するためのコストがかかる」はほぼ横ばいで推移しており、規制対応コストが慢性的な負担として定着していることがうかがえる。「相手企業のデータ管理状況が把握できない」も一定程度存在しており、サプライチェーン全体を通じたデータガバナンスの確保が難しい実態が浮かび上がっている。



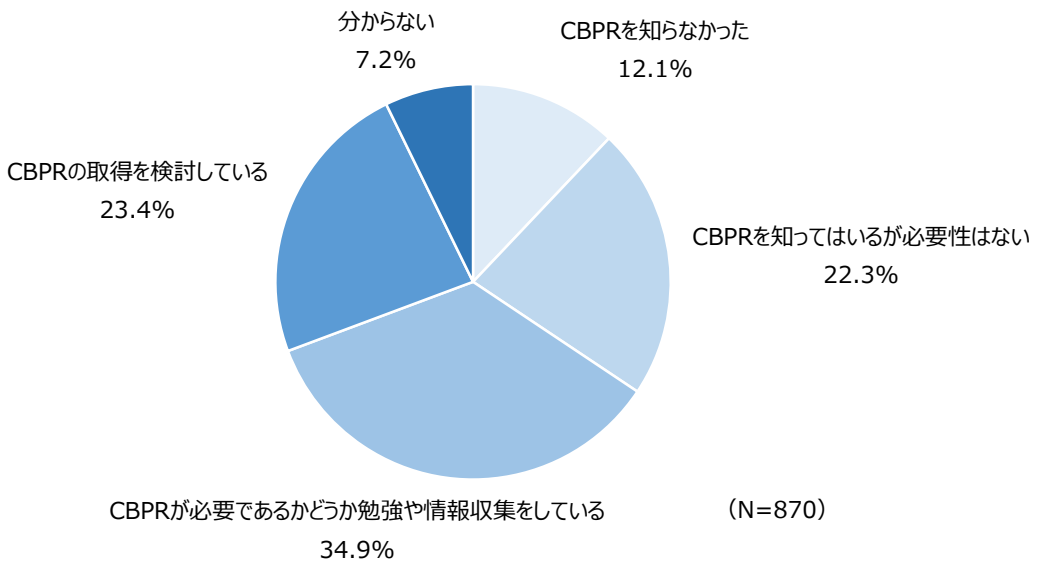
出典：JIPDEC『企業IT利活用動向調査2026』

図39　海外企業とのデータのやり取りにおいて生じている課題

CBPRの取得状況

越境する個人データに関して企業等が一定の保護要件を満たしていることを国際的に認証する枠組みとして、CBPRがある。これは、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となる。まず、CBPRを取得検討状況について質問を行った（図40）。「CBPRが必要であるかどうか勉強や情報収集をしている」が34.9%と最も多く、「CBPRの取得を検討している」（23.4%）と合わせると約6割の企業がCBPRへの関心を持ち、何らかの形で前向きに検討していることがわかる。

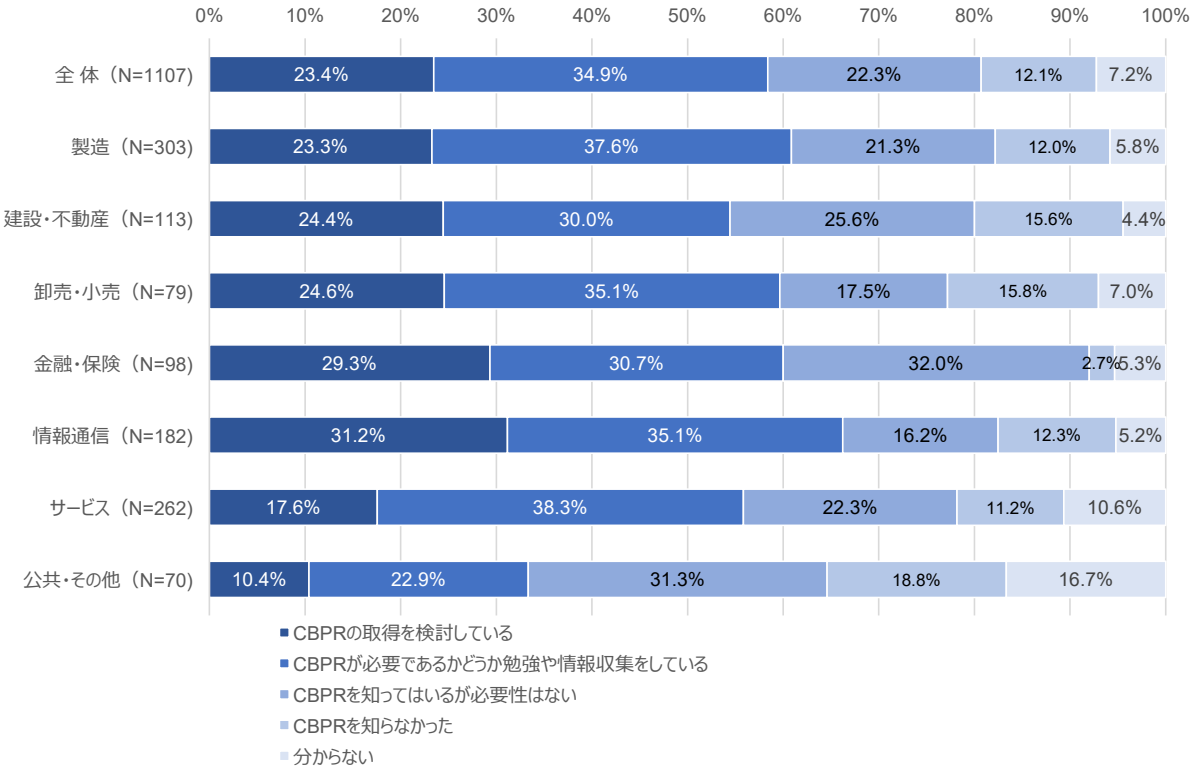
一方、「CBPRを知ってはいるが必要性はない」が22.3%、「CBPRを知らなかった」が12.1%存在しており、認知はしているものの自社への必要性を感じていない企業や、そもそも認知が及んでいない企業も相当数残っている。CBPRは越境データ移転の安全性を第三者が認証する仕組みであり、取引先や顧客に対するデータ保護への信頼性を示すうえで有効な手段であることの認識が、まだ十分に浸透していない状況がうかがえる。



出典：JIPDEC『企業IT利活用動向調査2026』

図40　CBPRの取得検討状況

次に、業種別に見てみる（図41）。「CBPRの取得を検討している」割合が最も高いのは情報通信（31.2%）と金融・保険（29.3%）であり、いずれも全体平均（23.4%）を大きく上回っている。情報通信はデータの越境移転が事業の根幹に関わる業種であり、金融・保険は顧客の機密情報を大量に扱うことから、データ保護への信頼性を対外的に示す手段としてCBPRへの関心が高いと考えられる。この2つの業種は「CBPRの取得を検討している」と「CBPRが必要かどうか勉強や情報収集をしている」の合計も高く、越境データ移転への対応が最も進んでいる業種群として位置づけられる。

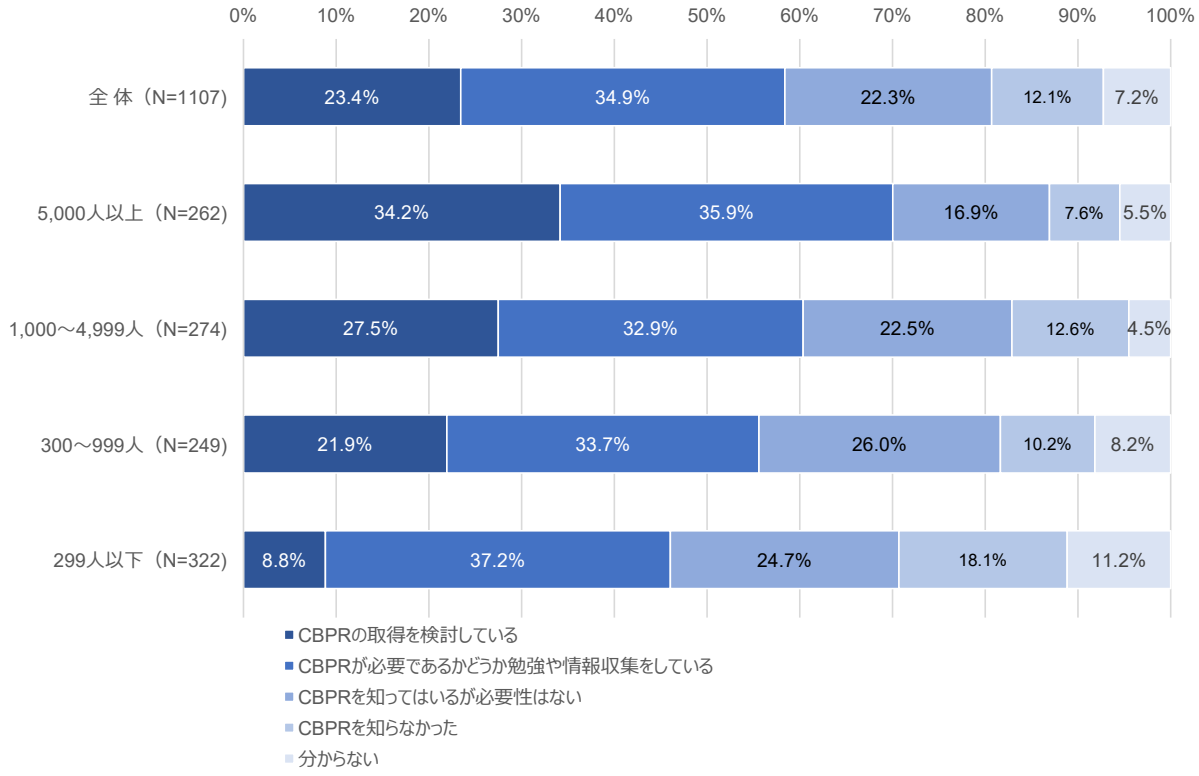


出典：JIPDEC『企業IT利活用動向調査2026』

図41　CBPRの取得検討状況：業種別

さらに、従業員規模別に見てみる（図42）。「CBPRの取得を検討している」割合は5,000人以上で34.2%と最も高く、1,000～4,999人（27.5%）、300～999人（21.9%）と規模が小さくなるにつれて低下し、299人以下では8.8%と全規模中最も低い。大企業ほどグローバルなビジネス展開が広く、越境データ移転への対応が事業上の必要性として強く認識されていることが背景にあると考えられる。

299人以下の中小企業では「CBPRの取得を検討している」は8.8%にとどまる一方、「CBPRが必要かどうか勉強や情報収集をしている」が37.2%と全規模中最も高い。取得検討には至っていないものの、必要性を探りながら情報収集を進めている企業が多い。



出典：JIPDEC『企業IT利活用動向調査2026』

図42　CBPRの取得検討状況：従業員規模別

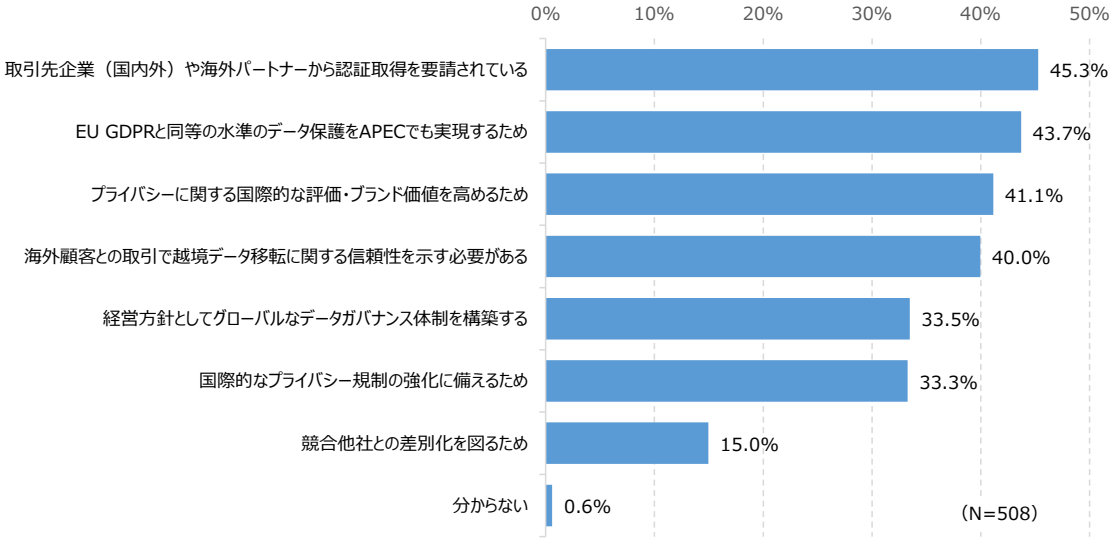
CBPRの取得検討の動機

CBPRを取得検討や情報収集を行っている企業に対し、その背景や動機について質問を行った（図43）。「取引先企業（国内外）や海外パートナーから認証取得を要請されている」が最も高く、外部からの要請がCBPR取得検討の最大の契機となっていることがわかる。自社の自発的な判断よりも、取引関係における要件充足がCBPR取得を後押しする主要因となっている実態が浮かび上がっている。

「EU GDPRと同等の水準のデータ保護をAPECでも実現するため」と「プライバシーに関する国際的な評価・ブランド価値を高めるため」がこれに続いており、GDPRへの対応経験を持つ企業がCBPRをGDPRと同等水準のデータ保護の枠組みとして位置付けていることや、データ保護の取り組みを対外的な信頼性向上に結びつけようとする意識が高いことがうかがえる。

「海外顧客との取引で越境データ移転に関する信頼性を示す必要がある」も高い水準にあり、顧客との信頼関係構築においてCBPRが有効な手段として認識されていることが示されている。「経営方針

としてグローバルなデータガバナンス体制を構築する」や「国際的なプライバシー規制の強化に備えるため」も一定程度挙げられており、取引上の要件対応にとどまらず、経営レベルでの戦略的な取り組みとしてCBPRを位置付けている企業も存在していることがわかる。



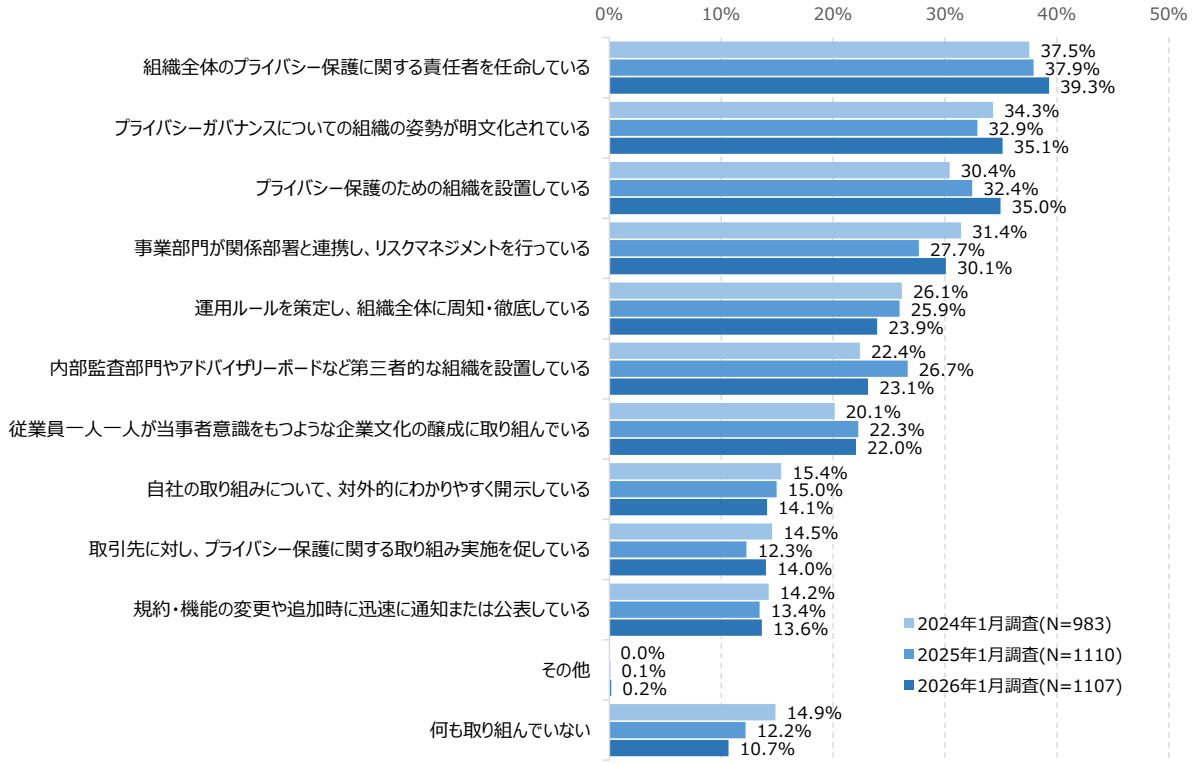
出典：JIPDEC『企業IT利活用動向調査2026』

図43　CBPRの取得を検討する動機

プライバシーガバナンスに関する取り組み状況

近年、経営上の重要事項として、必ずしも法令遵守に留まらない形で、組織全体でプライバシー問題の適切なリスク管理に対して能動的に取り組むための体制を構築し、企業価値向上につなげるプライバシーガバナンスの重要性が高まりつつある。そこで、プライバシーガバナンスの取り組み状況について質問を行った（図44）。「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3年連続で最上位を維持しており、2026年調査では39.3%へと上昇している。責任体制の明確化がプライバシーガバナンスの基盤として定着しつつある一方、「プライバシー保護のための組織を設置している」（35.0%）や「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」（35.1%）も上昇傾向にあり、責任者の任命にとどまらず、組織体制の整備や方針の明文化へと取り組みが深化していることがうかがえる。

「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」は2025年調査の27.7%から2026年調査では30.1%へと上昇しており、プライバシーリスクへの対応が特定部門の責任にとどまらず、事業部門を巻き込んだ横断的な取り組みへと発展しつつあると考えられる。



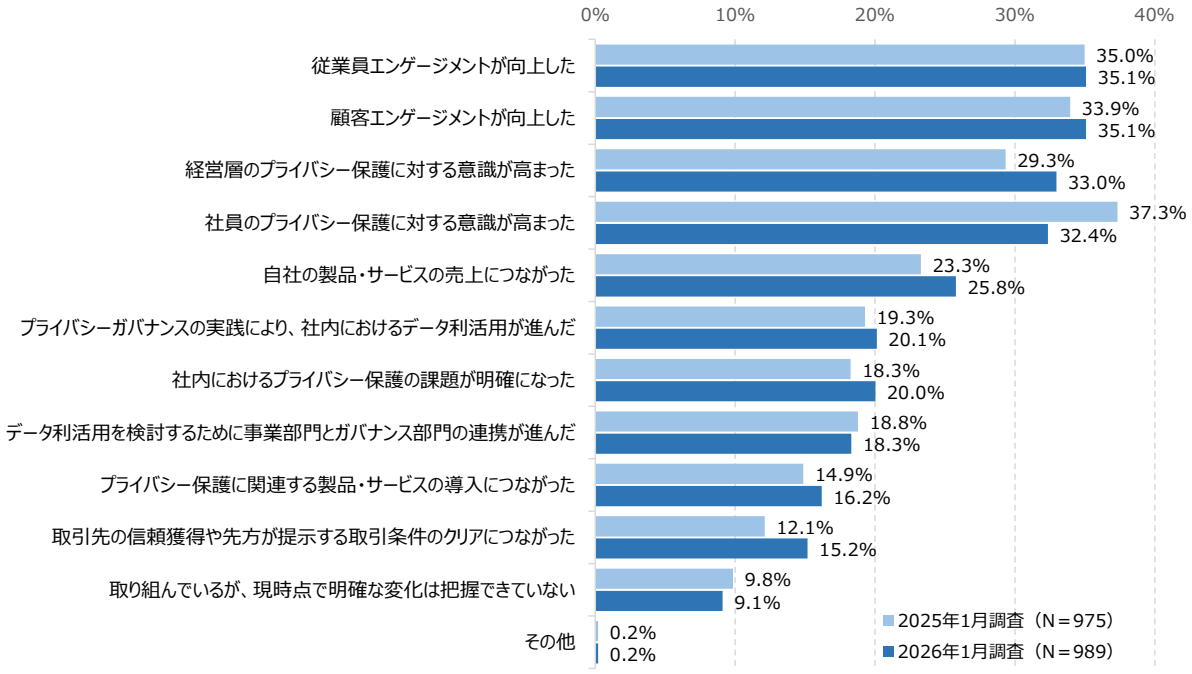
出典：JIPDEC『企業IT利活用動向調査2026』

図44　プライバシーガバナンスに関する取り組み状況

プライバシーガバナンスに取り組んだことで、どのような変化が出ているのだろうか（図45）。「従業員エンゲージメントが向上した」と「顧客エンゲージメントが向上した」はいずれも2025年調査とほぼ同水準で最上位を維持しており、プライバシーガバナンスへの取り組みが従業員・顧客双方の信頼や満足度の向上に継続的に貢献していることが示されている。

2025年調査から最も変化が大きいのは「経営層のプライバシー保護に対する意識が高まった」であり、29.3%から33.0%へと上昇している。プライバシーガバナンスが現場レベルの取り組みにとどまらず、経営課題として意識される傾向が強まっていることがうかがえる。一方、「社員のプライバシー保護に対する意識が高まった」は37.3%から32.4%へと低下しており、社員の意識向上効果が一定程度定着してきた段階にある可能性が考えられる。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。

「自社の製品・サービスの売上につながった」は23.3%から25.8%へと上昇しており、プライバシーガバナンスへの取り組みが事業成果に直結するケースが増えていることは注目される。「取引先の信頼獲得や先方が提示する取引条件のクリアにつながった」も12.1%から15.2%へと上昇しており、プライバシーガバナンスがビジネス上の競争力や取引要件の充足において実質的な効果をもたらしていることが示されている。



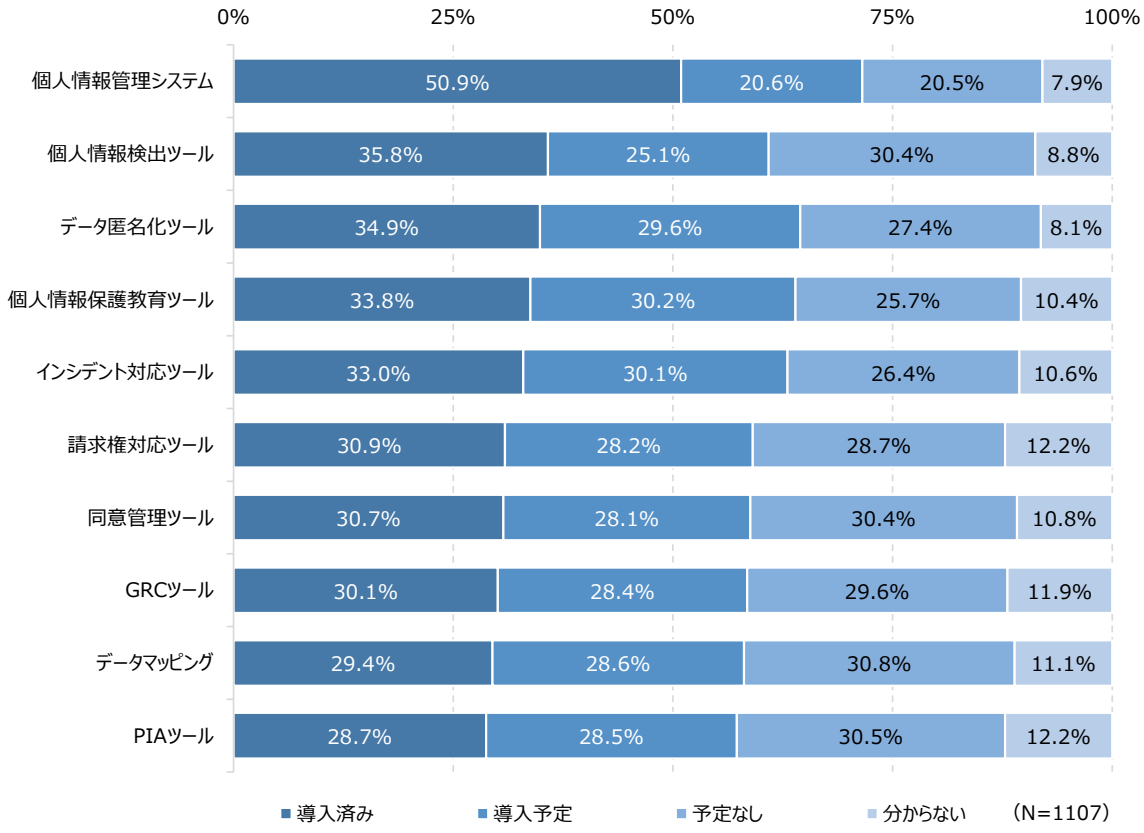
出典：JIPDEC『企業IT利活用動向調査2026』

図45　プライバシーガバナンスに取り組んだことによる変化

プライバシー保護関連ツールの導入状況

プライバシー保護に関するツールやシステムの導入状況について質問を行った（図46）。「個人情報管理システム」が唯一導入済みの割合が50%を超えており、個人情報の一元管理を目的としたシステムの導入が最も広く普及していることがわかる。個人情報保護法への対応を基盤として、個人情報の所在・取り扱いを管理するシステムの整備が先行して進んできた状況が反映されていると考えられる。

「個人情報検出ツール」と「データ匿名化ツール」がこれに続いており、個人情報の特定・保護に関わる基本的なツールの導入も一定程度進んでいる。「個人情報保護教育ツール」や「インシデント対応ツール」も30%台の導入率を示しており、人材育成や事故対応の面でもツールを活用する企業が増えていることがうかがえる。

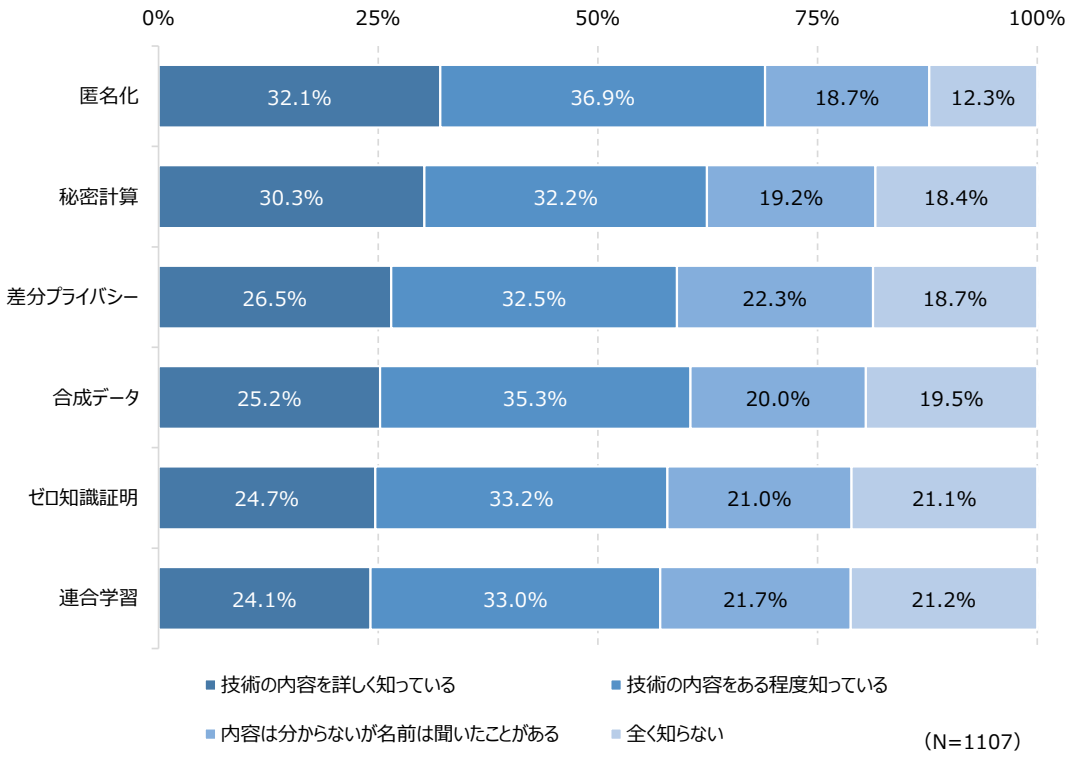


出典：JIPDEC『企業IT利活用動向調査2026』

図46　プライバシー保護関連ツール・システムの導入状況

次に、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）の認知状況について質問を行った（図47）。最も認知度が高いのは「匿名化」であり、「技術の内容を詳しく知っている」と「技術の内容をある程度知っている」の合計が約7割に達している。匿名化はデータ保護の基本的な手法として長年活用されてきた経緯があり、他の技術と比べて認知・理解が進んでいることが背景にあると考えられる。「秘密計算」もこれに次ぐ認知度を示しており、データを暗号化したまま処理できる技術として注目が高まっていることがうかがえる。

一方、「差分プライバシー」「合成データ」「ゼロ知識証明」「連合学習」は「技術の内容を詳しく知っている」割合が20%台にとどまっており、名前は聞いたことがあるものの内容の理解が浸透していない層が相当数存在している。特に「ゼロ知識証明」と「連合学習」は「全く知らない」の割合が20%を超えており、認知自体がまだ限定的な段階にある。



出典：JIPDEC『企業IT利活用動向調査2026』

図47　プライバシーテック（PETs）の認知状況

調査結果の考察

本章では、プライバシー保護に関する取り組み状況について調査結果を分析した。そこから得られた考察を以下にまとめる。

1. **個人情報保護の取り組みは基盤整備から実効性の強化へと移行が求められる**：個人情報保護管理者の任命や社員教育、規程類の整備といった基盤的な取り組みは広く定着しつつある。一方、プライバシー保護ツールの活用や外部認証・監査といった高度な取り組みの普及はまだ限定的であり、責任体制の構築にとどまらず、技術的対策や継続的な監査を通じた実効性の強化が今後の重要な課題となっている。
2. **データの越境移転が拡大するなかで、規制対応とデータガバナンスの整備が急務となる**：越境移転を行っている企業は増加傾向にあり、アジア太平洋地域と北米地域を中心にデータの国際的な流通がさらに拡大していく見通しにある。しかし、相手国とのデータ保護基準の不一致や規制対応の複雑さ、送信時のセキュリティへの不安が慢性的な課題として残っており、移転先ごとの法令対応と包括的なデータガバナンス体制の整備が不可欠となっている。
3. **CBPRは越境データ移転の信頼基盤として重要性が高まっている**：CBPRへの関心は高まっており、特に情報通信、金融・保険、大企業での取得検討が進んでいる。取得の主な動機は取引先からの要請やGDPRと同等の水準の実現であり、ビジネス上の信頼確保に向けた手段として位置付けられている。

4. **プライバシーガバナンスは法令遵守を超えた経営課題として定着しつつある**：プライバシーガバナンスへの取り組みが従業員・顧客エンゲージメントの向上や売上増加、取引条件のクリアといった具体的な事業成果に結びついている企業が増えており、経営層の意識向上も進んでいる。プライバシーテック（PETs）の認知はまだ限定的であるものの、データ活用とプライバシー保護の両立に向けて、ツールの活用や新技術の理解を深めながら、プライバシーガバナンスを企業価値向上につなげる取り組みを継続的に推進していくことが重要となる。

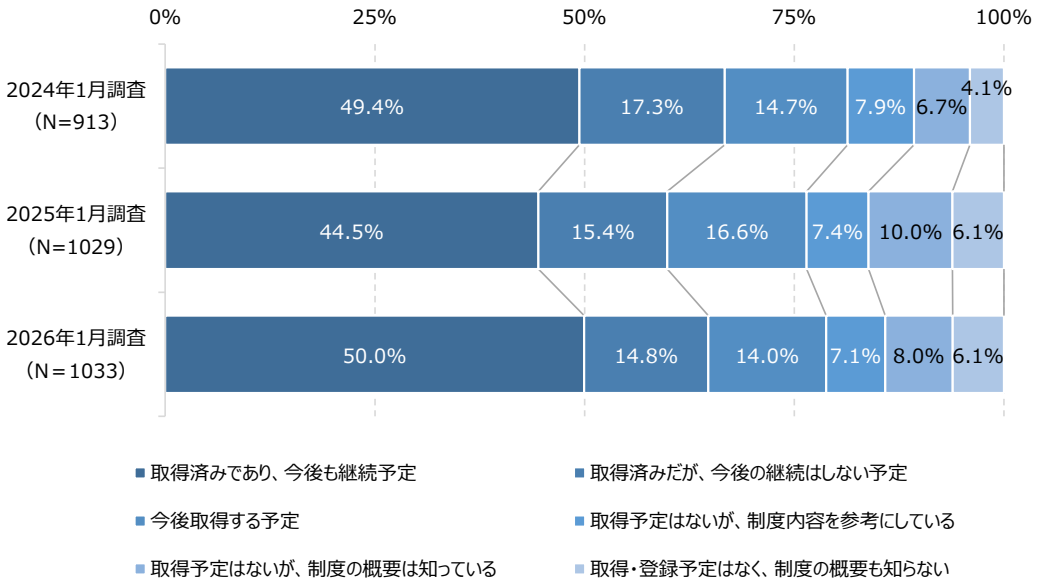
第三者認証の取得状況

本章では、プライバシーマークとISMS認証を中心に第三者機関による認証の取得状況について調査した結果を分析している。

プライバシーマーク／ISMS認証の取得状況

プライバシーマークとISMS認証の取得状況について質問を行った。まず、2024年調査から2026年調査までのプライバシーマークの取得状況を見てみる（図48）。「取得済みであり、今後も継続予定」の割合は2024年調査の49.4%から2025年調査では44.5%へと低下したものの、2026年調査では50.0%へと回復している。約2社に1社が取得済みで継続を予定しており、プライバシーマークが企業における個人情報保護への取り組みの証明として定着していることが示されている。

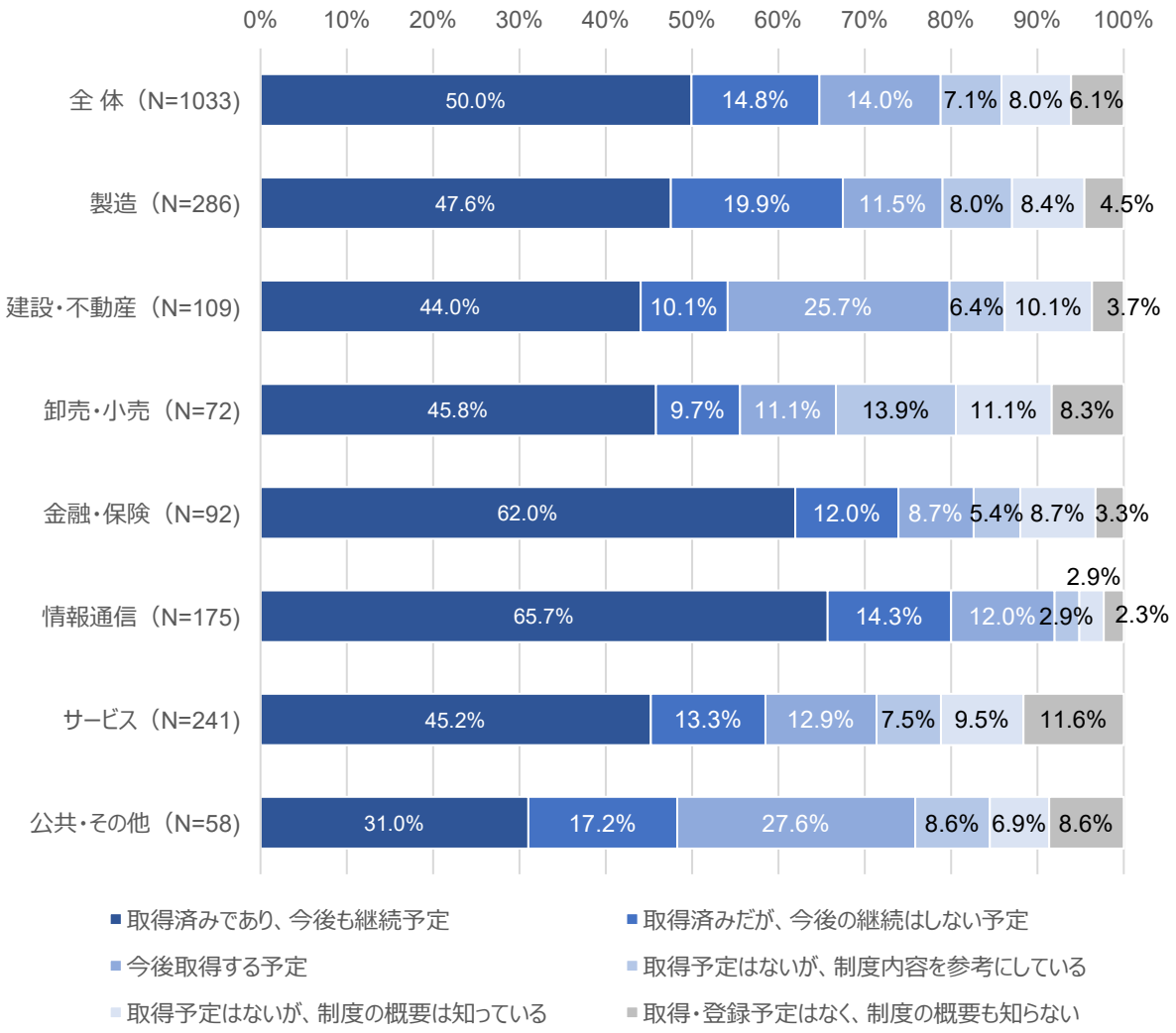
「取得済みだが、今後の継続はしない予定」は2024年調査の17.3%から2026年調査では14.8%へと低下傾向にあり、取得を維持する企業の割合が相対的に安定していることがうかがえる。「今後取得する予定」は14.0%と一定程度存在しており、新規取得を目指す企業も引き続き見られる。



注1：「取得・登録予定が分かる立場にない」の回答者は除いている
出典：JIPDEC『企業IT利活用動向調査2026』

図48　プライバシーマークの取得状況

プライバシーマークの取得状況について業種別に見てみる（図49）。「取得済みであり、今後も継続予定」の割合が最も高いのは情報通信（65.7%）であり、金融・保険（62.0%）がこれに続いている。この2つの業種は全体平均（50.0%）を大きく上回っており、個人情報を大量に取り扱う業務特性や、顧客・取引先からの信頼確保の必要性が、プライバシーマーク取得を強く後押ししていると考えられる。

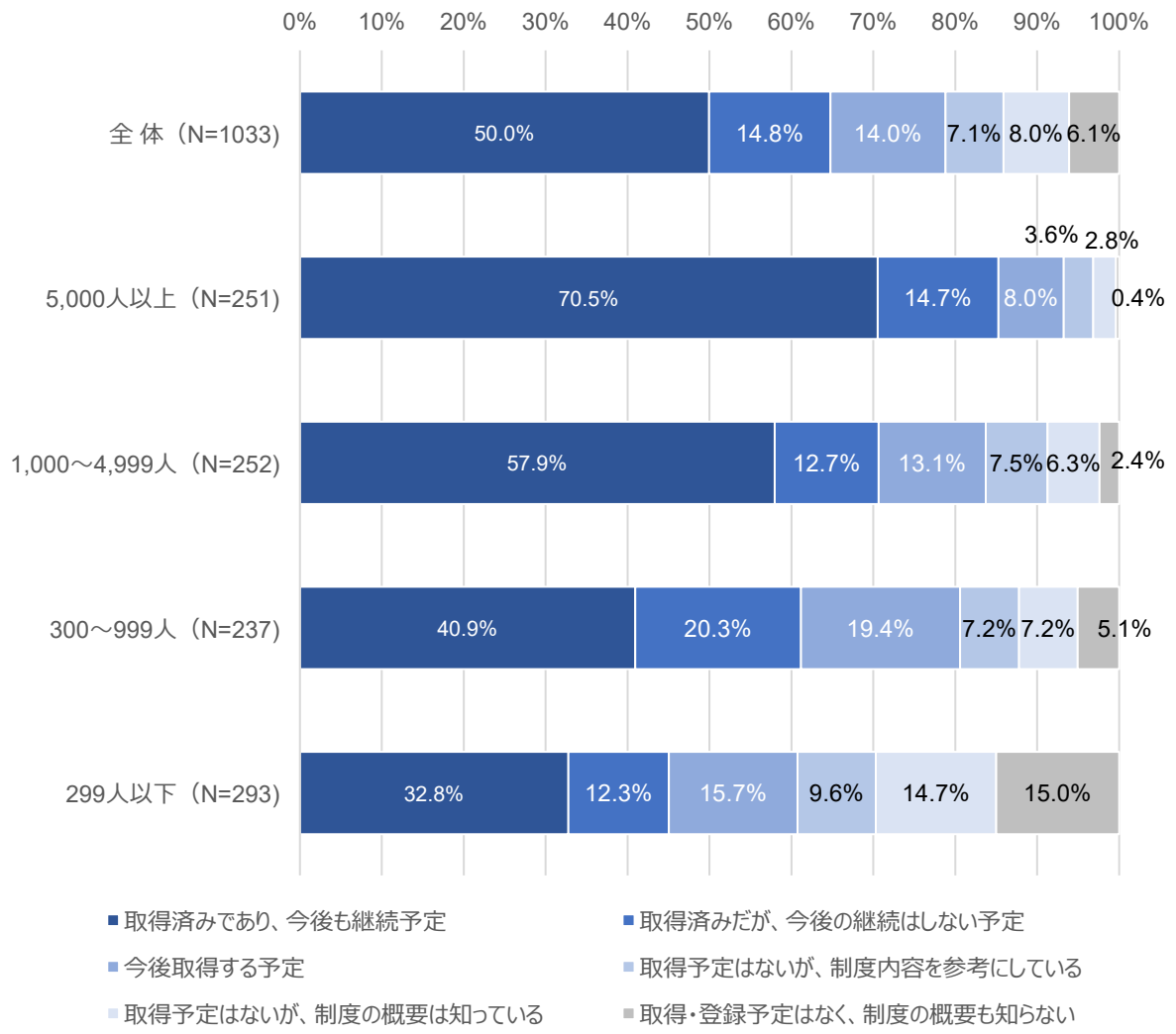


注1：「取得・登録予定が分かる立場にない」の回答者は除いている

出典：JIPDEC『企業IT利活用動向調査2026』

図49　プライバシーマークの取得状況：業種別

プライバシーマークの取得状況について従業員規模別に見てみる（図50）。「取得済みであり、今後も継続予定」の割合は5,000人以上で70.5%と最も高く、1,000～4,999人（57.9%）がこれに続いており、大企業ではプライバシーマークが個人情報保護の基盤的な認証として広く定着していることがわかる。一方、300～999人では40.9%、299人以下では32.8%と、規模が小さくなるにつれて取得済み継続割合が大きく低下している。

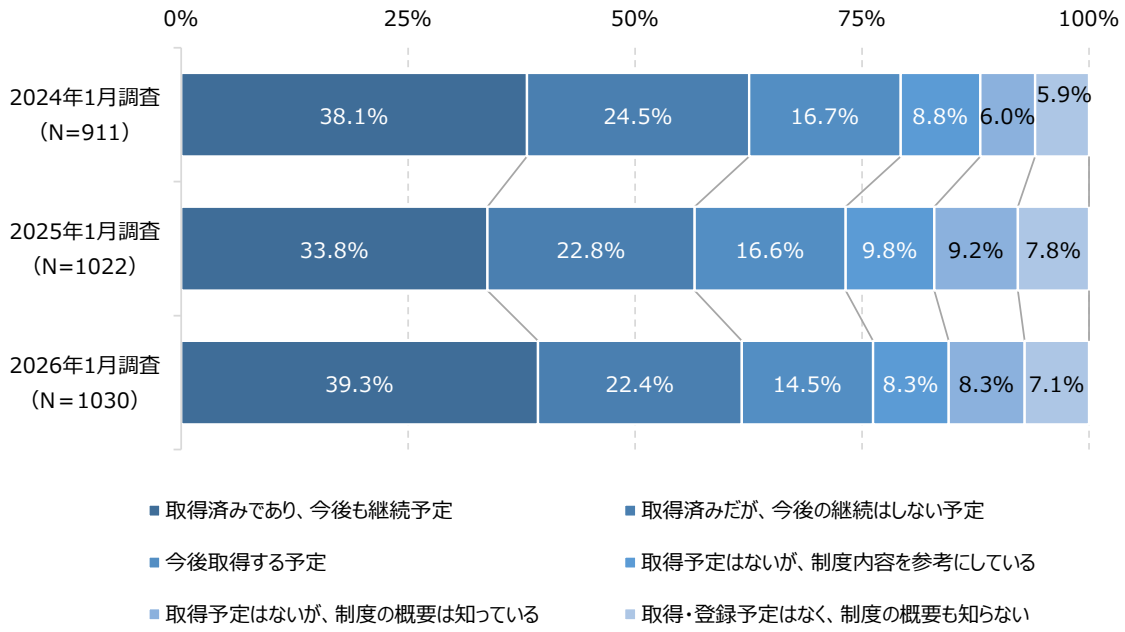


注1：「取得・登録予定が分かる立場にない」の回答者は除いている

出典：JIPDEC『企業IT利活用動向調査2026』

図50　プライバシーマークの取得状況：従業員規模別

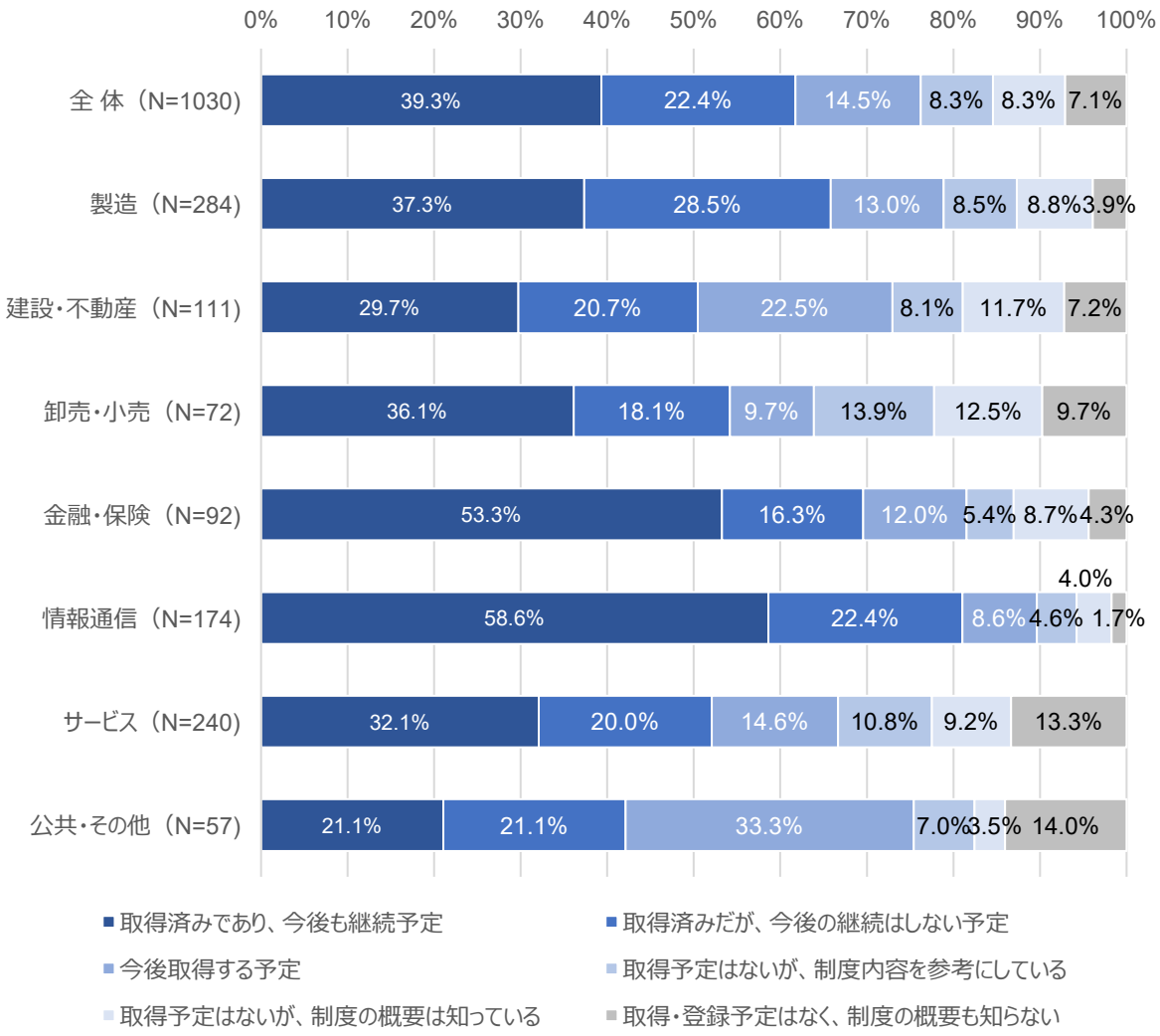
次に、2024年調査から2026年調査までのISMS認証の取得状況を見てみる（図51）。「取得済みであり、今後も継続予定」の割合は2024年調査の38.1%から2025年調査では33.8%へと低下したものの、2026年調査では39.3%へと回復しており、プライバシーマークと同様に情報セキュリティマネジメントの基盤的な認証として一定の水準を維持していることがわかる。「取得済みだが、今後の継続はしない予定」は2024年調査の24.5%から2026年調査では22.4%へと低下傾向にあり、取得を維持する企業の割合が相対的に安定していることがうかがえる。



注1：「取得・登録予定が分かる立場にない」の回答者は除いている
出典：JIPDEC『企業IT利活用動向調査2026』

図51　ISMS認証の取得状況

次にISMS認証の取得状況について業種別に見てみる（図52）。「取得済みであり、今後も継続予定」の割合が最も高いのは情報通信（58.6%）であり、金融・保険（53.3%）がこれに続いている。この2つの業種は全体平均（39.3%）を大きく上回っており、情報資産の保護が事業の根幹に関わる業種特性や、顧客・取引先からの信頼確保の必要性がISMS認証取得を強く後押ししていると考えられる。プライバシーマークでも同様の傾向が見られており、この2つの業種が情報セキュリティ・プライバシー保護の両面で先行していることが改めて示されている。

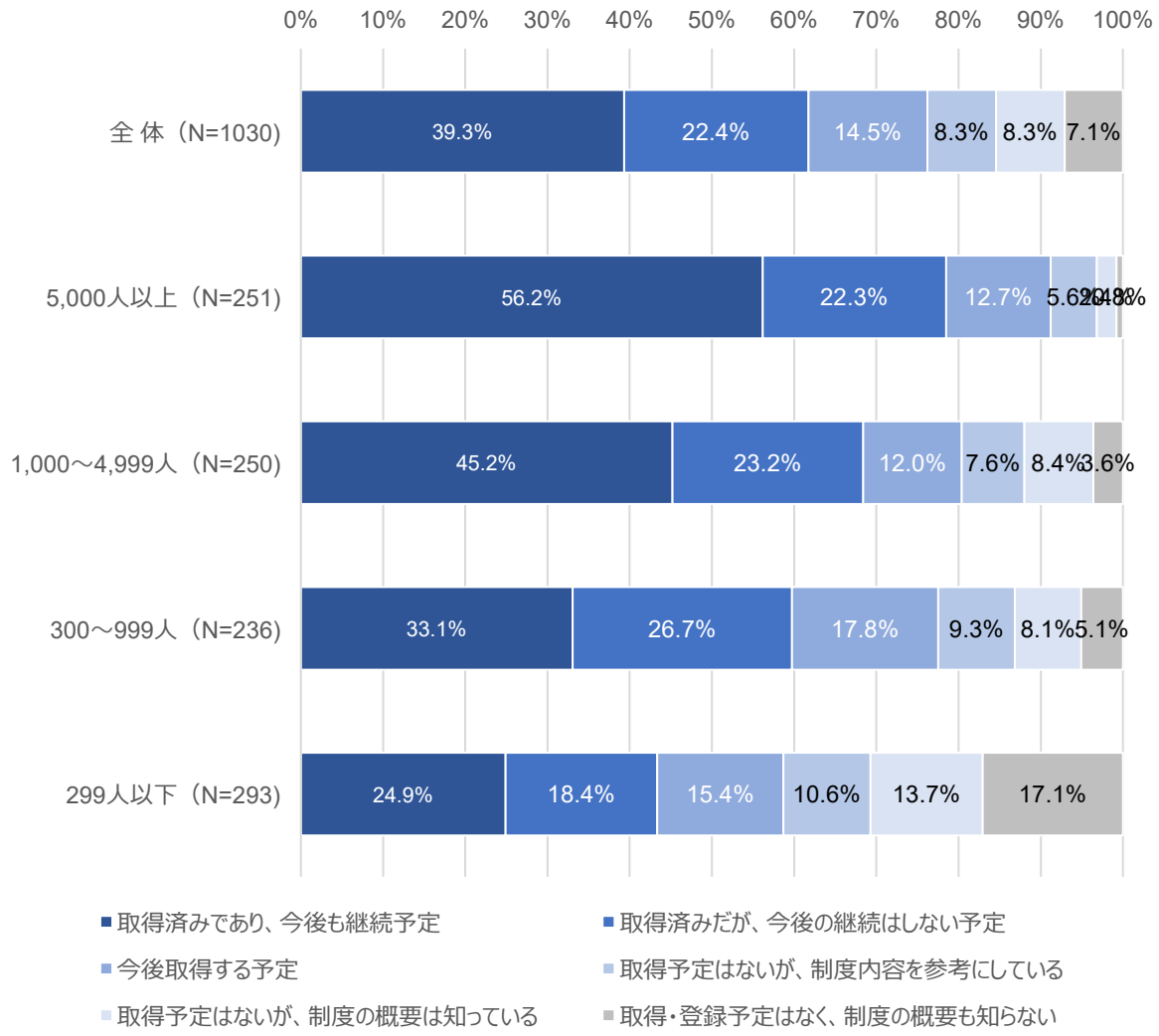


注1：「取得・登録予定が分かる立場にない」の回答者は除いている

出典：JIPDEC『企業IT利活用動向調査2026』

図52　ISMS認証の取得状況：業種別

ISMS認証の取得状況について、従業員規模別に見てみる（図53）。「取得済みであり、今後も継続予定」の割合は5,000人以上で56.2%と最も高く、1,000～4,999人（45.2%）がこれに続いており、大企業ではISMS認証が情報セキュリティマネジメントの基盤的な認証として広く定着していることがわかる。一方、300～999人では33.1%、299人以下では24.9%と、規模が小さくなるにつれて「取得済みであり、今後も継続予定」の割合が大きく低下している。



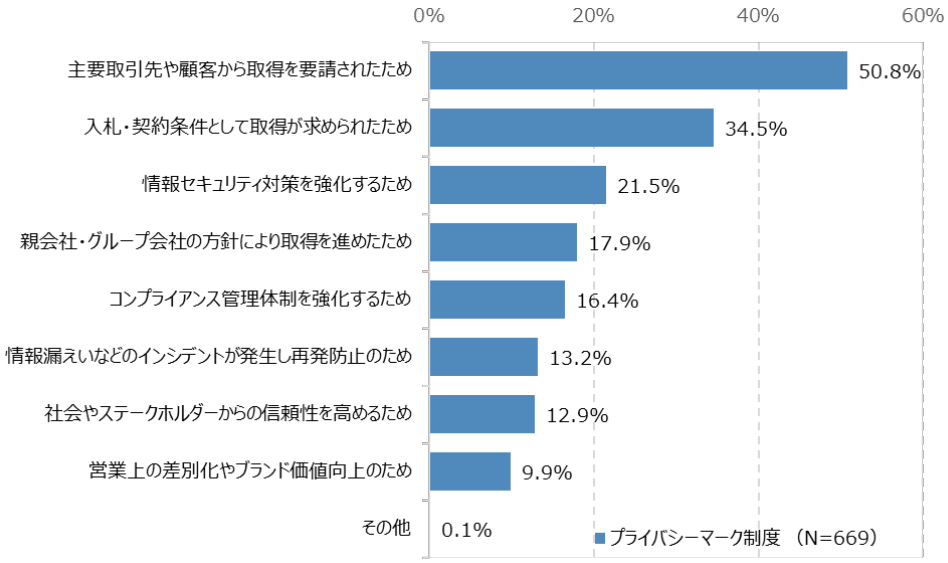
注1：「取得・登録予定が分かる立場にない」の回答者は除いている

出典：JIPDEC『企業IT利活用動向調査2026』

図53　ISMS認証の取得状況：従業員規模別

プライバシーマーク／ISMS認証取得の動機

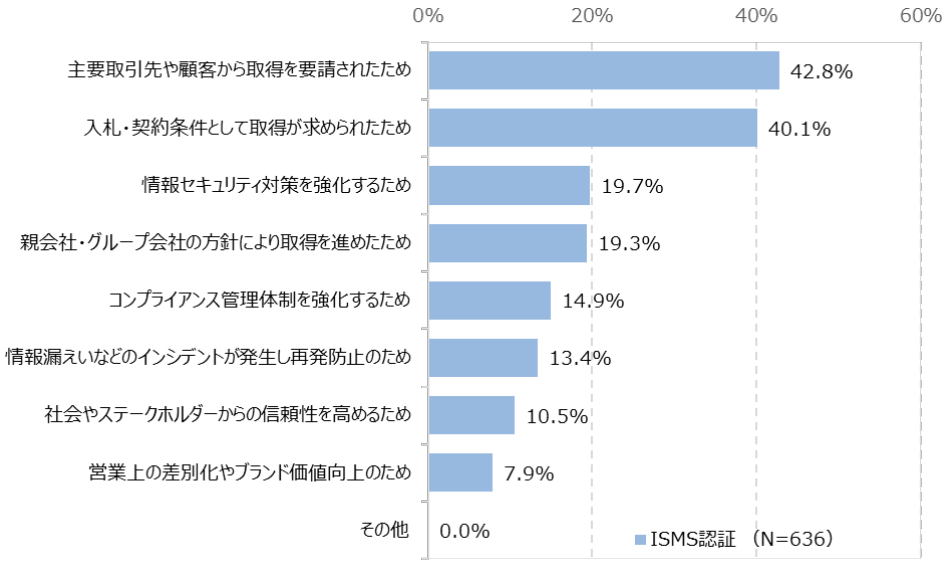
プライバシーマークとISMS認証はどのような背景や動機があって取得しているのだろうか。プライバシーマークでは「主要取引先や顧客から取得を要請されたため」が最も高く、「入札・契約条件として取得が求められたため」がこれに続いている。取引関係における要件充足が取得の主要動機となっており、自発的な取り組みよりも外部からの要請に応じる形で取得が進んでいる実態が浮かび上がっている（図54）。



出典：JIPDEC『企業IT利活用動向調査2026』

図54　プライバシーマーク認証取得の動機

ISMS認証も同様の傾向にあるが、「入札・契約条件として取得が求められたため」がプライバシーマークを上回っており、公的な入札案件や企業間取引においてISMS認証が契約要件として位置付けられているケースが多いことがうかがえる（図55）。



出典：JIPDEC『企業IT利活用動向調査2026』

図55　ISMS認証取得の動機

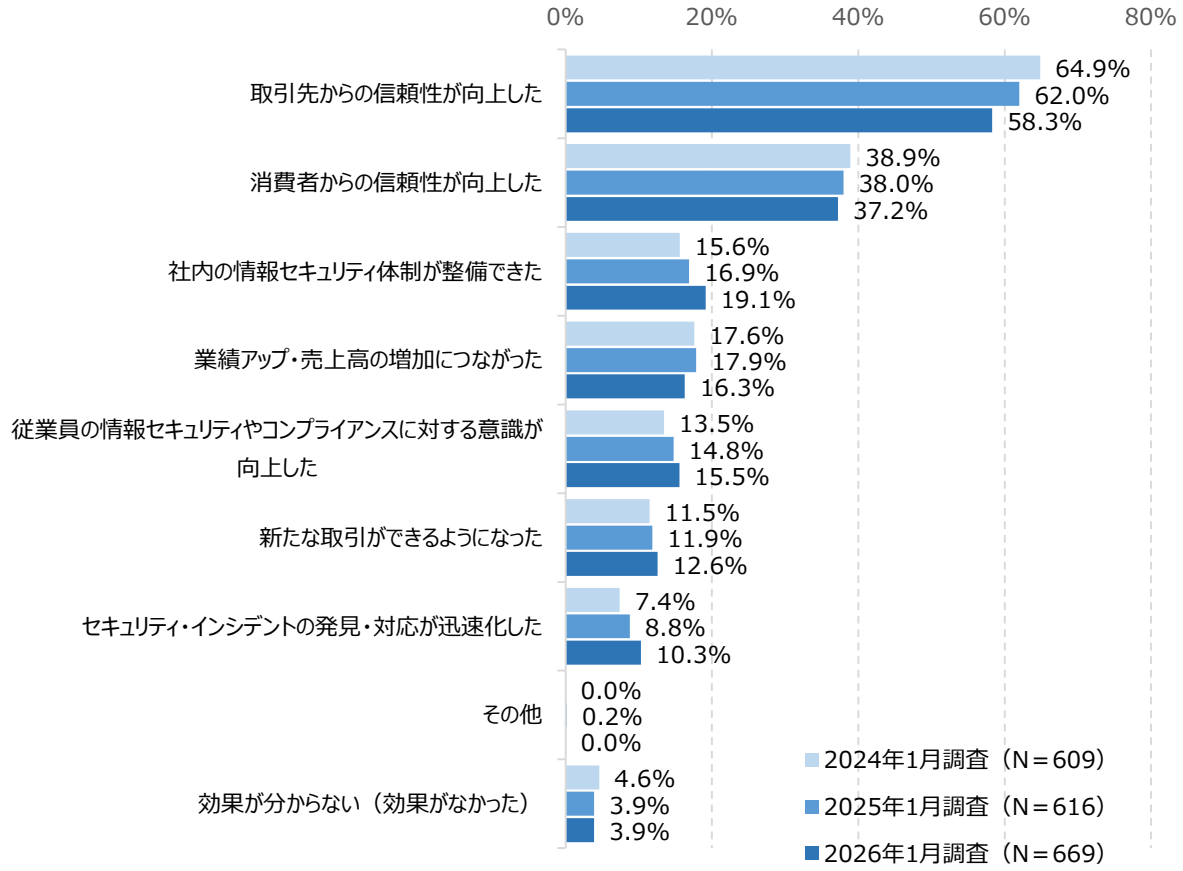
プライバシーマーク/ISMS認証ともに、「情報セキュリティ対策を強化するため」や「コンプライアンス管理体制を強化するため」も一定程度挙げられており、外部要請への対応だけでなく、自社の内部管理体制の強化を目的とした取得も見られる。一方、「社会やステークホルダーからの信頼性を高めるため」や「営業上の差別化やブランド価値向上のため」は相対的に低い水準にとどまっており、両認証の取得がまだ外部要件への受動的な対応にとどまり、戦略的な価値創出として位置付けて

いる企業は限定的であることが示されている。

プライバシーマーク／ISMS認証の取得による効果

プライバシーマークとISMS認証を取得したことでどのような効果が出ているのだろうか。まず、2024年調査から2026年調査までのプライバシーマークの取得による効果を見てみる（図56）。「取引先からの信頼性が向上した」が3年連続で最上位を維持しているものの、2024年調査の64.9%から2026年調査では58.3%へと低下傾向にある。「消費者からの信頼性が向上した」も同様に緩やかな低下傾向が見られる。

一方、上昇傾向にある項目も複数見られる。「社内の情報セキュリティ体制が整備できた」は15.6%から19.1%へと年々上昇しており、プライバシーマーク取得が対外的な信頼向上にとどまらず、社内のセキュリティ管理体制の整備にも寄与していることがうかがえる。「従業員の情報セキュリティやコンプライアンスに対する意識が向上した」や「セキュリティインシデントの発見・対応が迅速化した」も上昇しており、セキュリティ強化にも寄与していることが示されている。



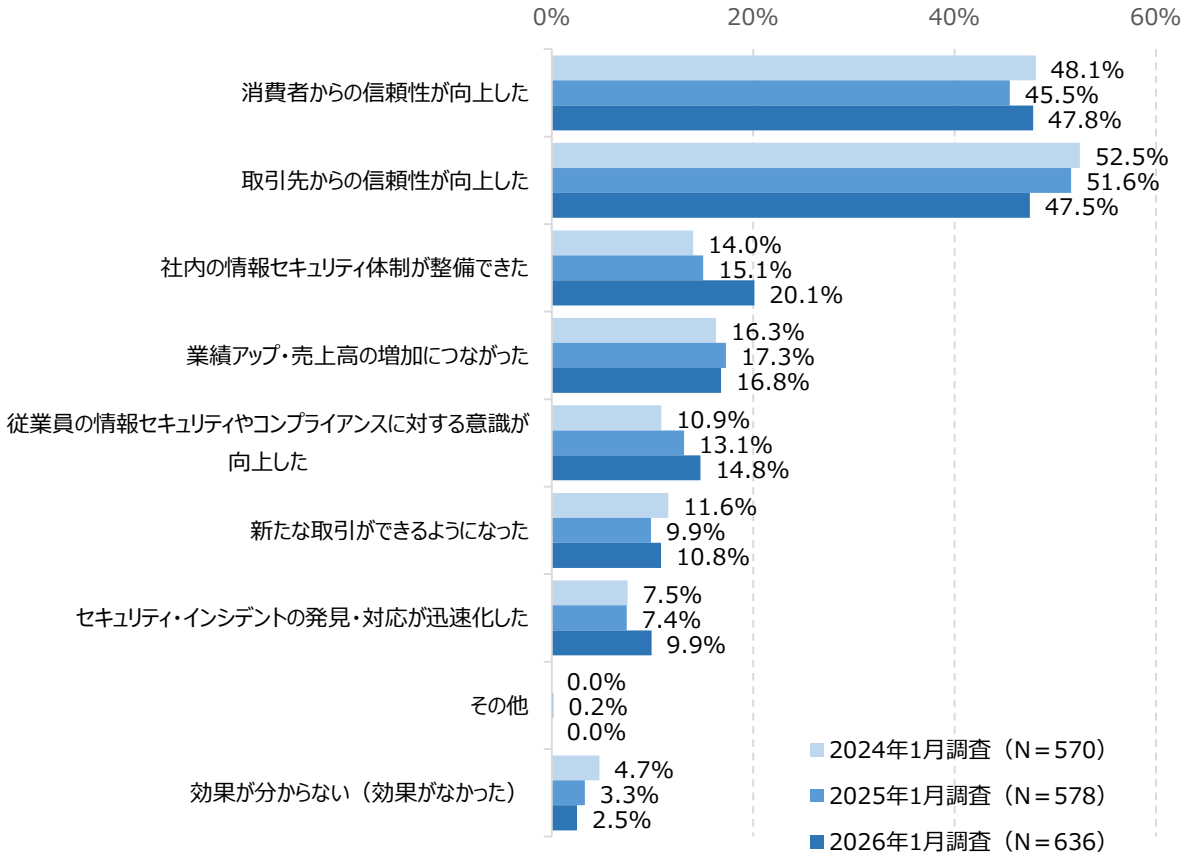
出典：JIPDEC『企業IT利活用動向調査2026』

図56　プライバシーマークの取得による効果

次に、2024年調査から2026年調査までのISMS認証の取得による効果を見てみる（図57）。プライバシーマークと同様に「取引先からの信頼性が向上した」が高い水準にあるものの、2024年調査の52.5%から2026年調査では47.5%へと低下傾向にある。「消費者からの信頼性が向上した」も同様の傾向を示しており、対外的な信頼向上効果は一定程度定着した段階にあると考えられる。

一方、上昇傾向にある項目も複数見られる。「社内の情報セキュリティ体制が整備できた」は14.0%

から20.1%へと大幅に上昇しており、ISMS認証取得が社内のセキュリティ管理体制の整備に寄与していることが明確に示されている。「従業員の情報セキュリティやコンプライアンスに対する意識が向上した」や「セキュリティインシデントの発見・対応が迅速化した」も上昇しており、社内の実効的なセキュリティ強化へと広がっていることがうかがえる。この傾向はプライバシーマークと共通しており、両制度とも社内への波及効果が高まっていることが示されている。



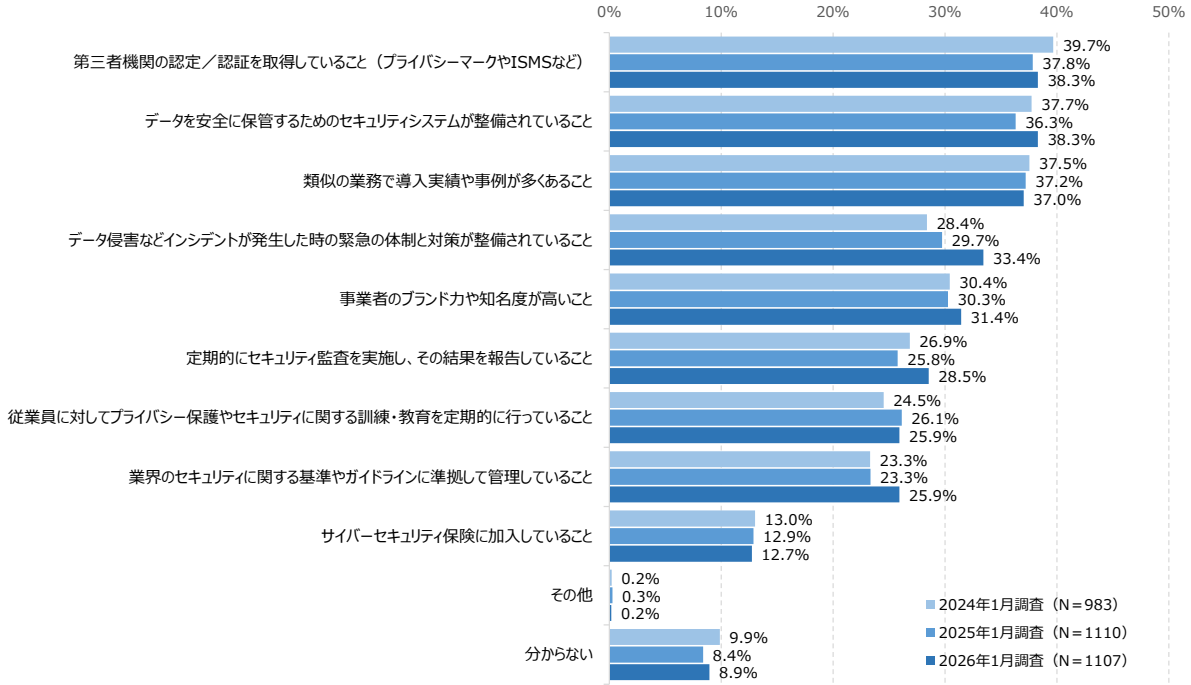
出典：JIPDEC『企業IT利活用動向調査2026』

図57　ISMS認証の取得による効果

業務委託事業者の選定で重視する点

機密情報を扱う業務の委託事業者を選定する際に重視する点について質問を行った（図58）。「第三者機関の認定／認証を取得していること（プライバシーマークやISMS認証など）」は3年連続で最上位を維持しており、委託先選定においてプライバシーマークやISMS認証などの第三者認証が最も重視される基準として定着していることがわかる。約4割の企業が最重要基準として位置付けており、認証取得が委託事業者としての信頼性確保に直結していることが改めて示されている。

「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」は28.4%から33.4%へと大幅に上昇しており、ランサムウェアをはじめとするサイバー攻撃リスクの高まりを背景に、委託先のインシデント対応体制の整備を重視する企業が着実に増えていることがうかがえる。「業界のセキュリティに関する基準やガイドラインに準拠して管理していること」も23.3%から25.9%へと上昇しており、業界固有のセキュリティ基準への適合を委託先選定の条件として重視する傾向が強まっている。



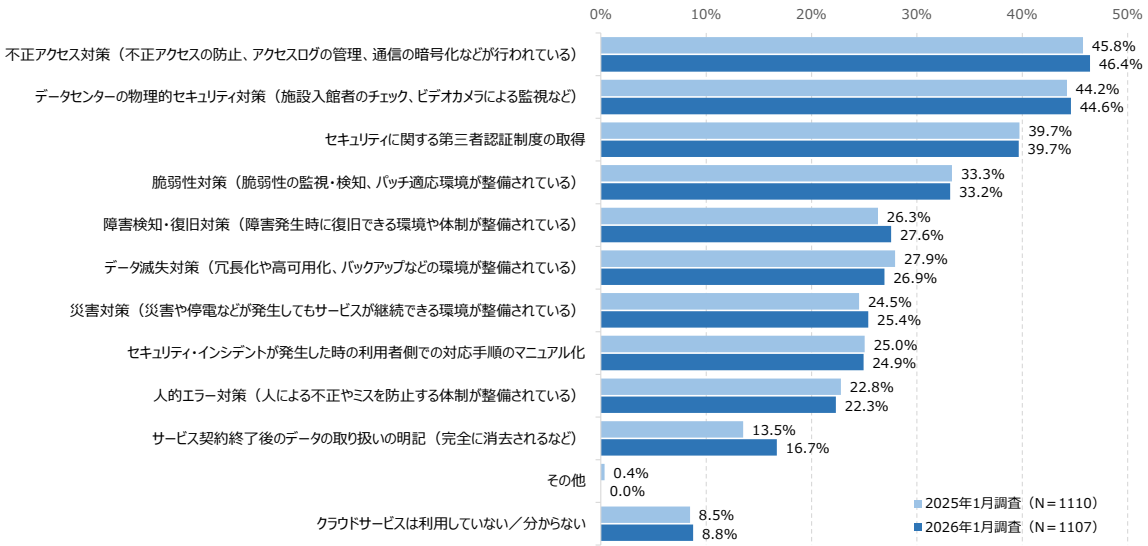
出典：JIPDEC『企業IT利活用動向調査2026』

図58　機密情報を扱う業務の委託事業者の選定で重視する点

クラウドサービスの選定における第三者による評価の重視度

クラウドサービスを選定する際に、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について質問を行った（図59）。「不正アクセス対策」が最も重視される項目として最上位を維持しており、「データセンターの物理的セキュリティ対策」「セキュリティに関する第三者認証制度の取得」がこれに続いている。クラウドサービス選定においても、委託事業者の選定と同様に第三者認証が重要な選定基準として広く認識されていることがわかる。

ランサムウェアをはじめとするサイバー攻撃によるシステム障害やデータ暗号化のインシデントが増加していることもあり、「障害検知・復旧対策」や「データ滅失対策」、「セキュリティインシデントが発生した時の利用者側での対応手順のマニュアル化」など、インシデントからの復旧対策も重視されるようになっている。

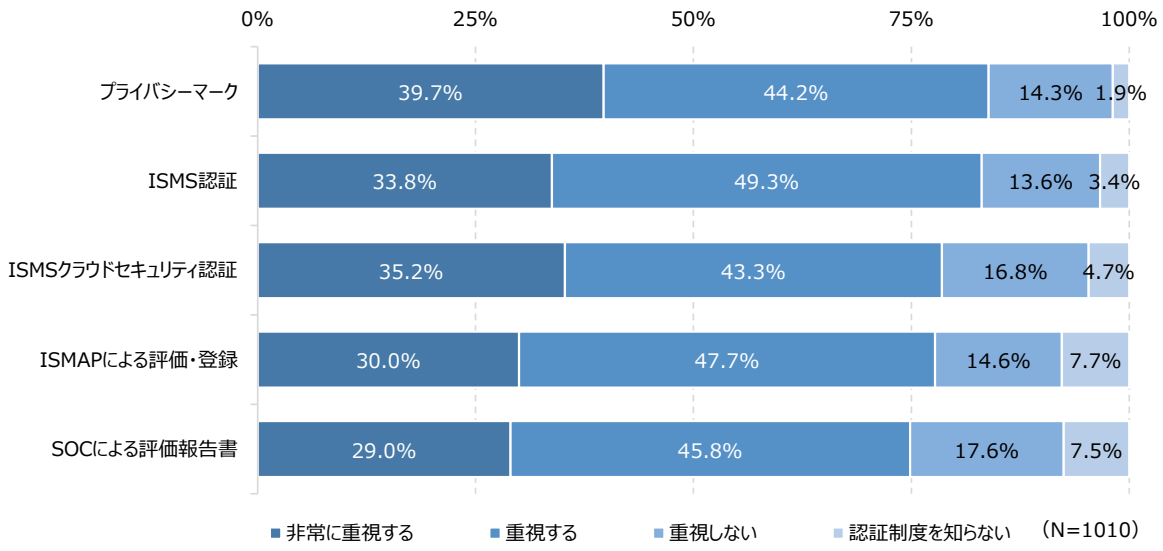


出典：JIPDEC『企業IT利活用動向調査2026』

図59　クラウドサービスの選定で重視するサービス提供事業者のセキュリティに対する取り組み

次に、クラウドサービスを選定する際、サービス提供事業者が取得している第三者評価をどの程度重視するかを、5つの第三者評価について質問を行った（図60）。すべての第三者評価において「非常に重視する」と「重視する」の合計が80%前後に達しており、クラウドサービス選定において第三者評価・認証が広く重視されていることがわかる。

「非常に重視する」の割合が最も高いのはプライバシーマーク（39.7%）であり、ISMSクラウドセキュリティ認証（35.2%）、ISMS認証（33.8%）がこれに続いている。プライバシーマークはクラウドサービスの選定においても個人情報保護への対応を示す指標として最も強く重視されており、個人データを扱うクラウドサービスにおけるプライバシー保護への関心の高さが反映されていると考えられる。ISMS認証は「非常に重視する」の割合こそプライバシーマークを下回るものの、「重視する」の割合が49.3%と全項目中最も高く、「非常に重視する」と「重視する」の合計では83.1%に達している。情報セキュリティマネジメントの基盤的な認証として、クラウドサービス選定における幅広い層での重視度が高いことがうかがえる。



出典：JIPDEC『企業IT利活用動向調査2026』

図60　クラウドサービスの選定における第三者評価の重視度

調査結果の考察

本章では、第三者認証制度の取得状況について調査結果を分析した。そこから得られた考察を以下にまとめる。

1. **プライバシーマークとISMS認証は裾野を広げていくことが求められる**：プライバシーマークとISMS認証の両制度ともに取得済み継続割合が回復傾向にあり、大企業を中心に広く普及している。一方、中小企業や一部の業種では取得率が低く、認知・活用の格差が残っており、認証取得の裾野を広げていくことが重要な課題となっている。
2. **認証取得の動機は外部要請への対応が主であり、戦略的活用への転換が求められる**：プライバシーマーク、ISMS認証ともに、取引先や顧客からの要請、入札・契約条件への対応が取得の主要動機となっており、自発的・戦略的な取り組みとして位置付けている企業はまだ限定的である。一方、取得による効果として社内のセキュリティ体制整備や従業員意識の向上が着実に上昇しており、認証取得を単なる要件充足にとどめず、組織能力の強化や企業価値向上につなげる視点を持つことが今後の重要な方向性となっている。
3. **委託先・クラウド事業者の選定において第三者認証が最重要基準として定着している**：機密情報を扱う業務委託先の選定でも、クラウドサービスの選定においても、第三者認証の取得が最も重視される基準として定着している。加えて、インシデント対応体制の整備を重視する企業が増加傾向にあり、サイバー攻撃リスクの高まりを背景にサプライチェーン全体でのセキュリティ水準の確保に対する要求が高まっていることが示されている。
4. **認証の対外的な信頼向上効果は定着しつつあり、社内への実効的な波及効果の拡大が次の課題となる**：プライバシーマークとISMS認証の両制度において取引先からの信頼性の向上という対外的な効果の割合は緩やかに低下している一方、社内の情報セキュリティ体制の整備やインシデント

対応の迅速化といった社内への実効的な波及効果が着実に上昇している。認証取得を契機に、組織全体のセキュリティ文化の醸成と継続的な改善サイクルの定着へとつなげていくことが、今後の重要な取り組みとなっている。

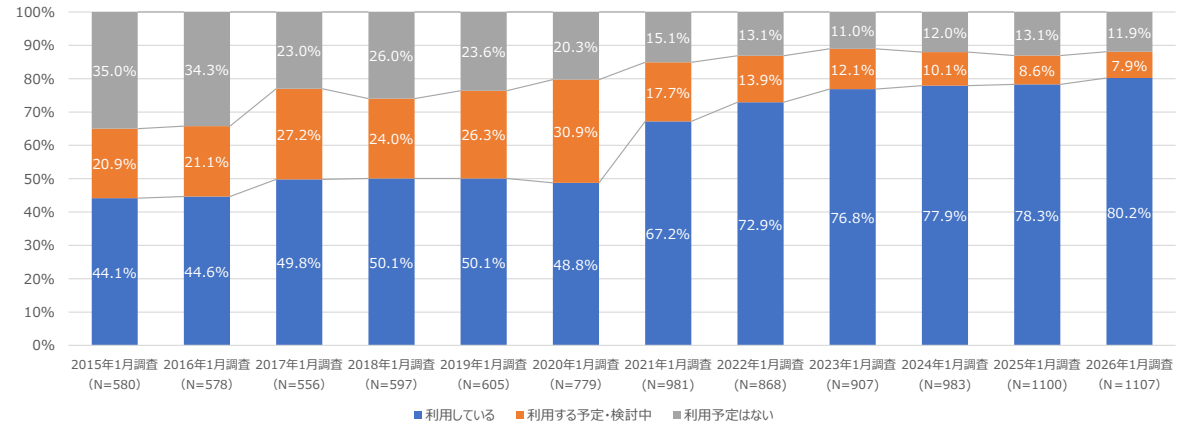
電子契約の利用状況

本章では、電子契約の利用状況について調査した結果を分析している。

電子契約の利用状況

これまでの「企業IT利活用動向調査」における電子契約の利用状況に関する調査結果を基に算出した、電子契約の利用状況の推移を示す（図61）。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によって業務のデジタル化が推進され、さらに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たことで電子契約の需要が高まり、2020年から2022年にかけて導入が急速に拡大したと見ている。

2026年調査での利用率は80.2%と、2025年調査（78.3%）から上昇し、初めて8割を超えた。2023年調査以降の推移を見ると、利用率の上昇幅は緩やかになっており、電子契約の導入がひと段落し定着段階に入っていることがうかがえる。一方、「利用する予定・検討中」の割合は7.9%と2025年調査（9.6%）から低下しており、今後の新規導入の伸びは限定的になる可能性がある。

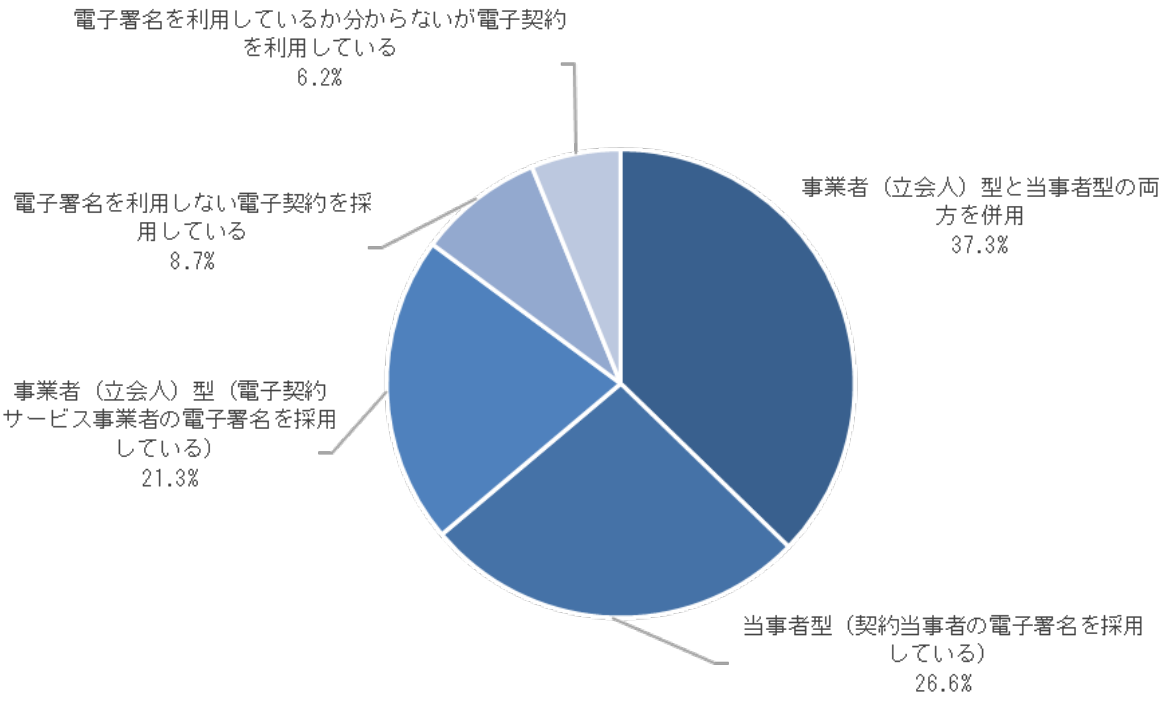


注1：2020年以前は質問が異なり、「わからない」の回答を除いていて再集計している
注2：2022～2023年調査は従業員2名企業の企業を対象としていたが、他の年度の調査と母集団を統一するため従業員数50名以上の回答者に限定し再集計している

出典：JIPDEC『企業IT利活用動向調査2026』

図61 電子契約の利用状況の推移：2015年～2026年

次に、利用している電子契約を方式別に分類している（図62）。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%）が最も大きく、契約方式を一つに限定しない運用が広がっているとみられる。「当事者型を利用」「事業者（立会人）型」の利用企業を含めると、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。



出典：JIPDEC『企業IT利活用動向調査2026』

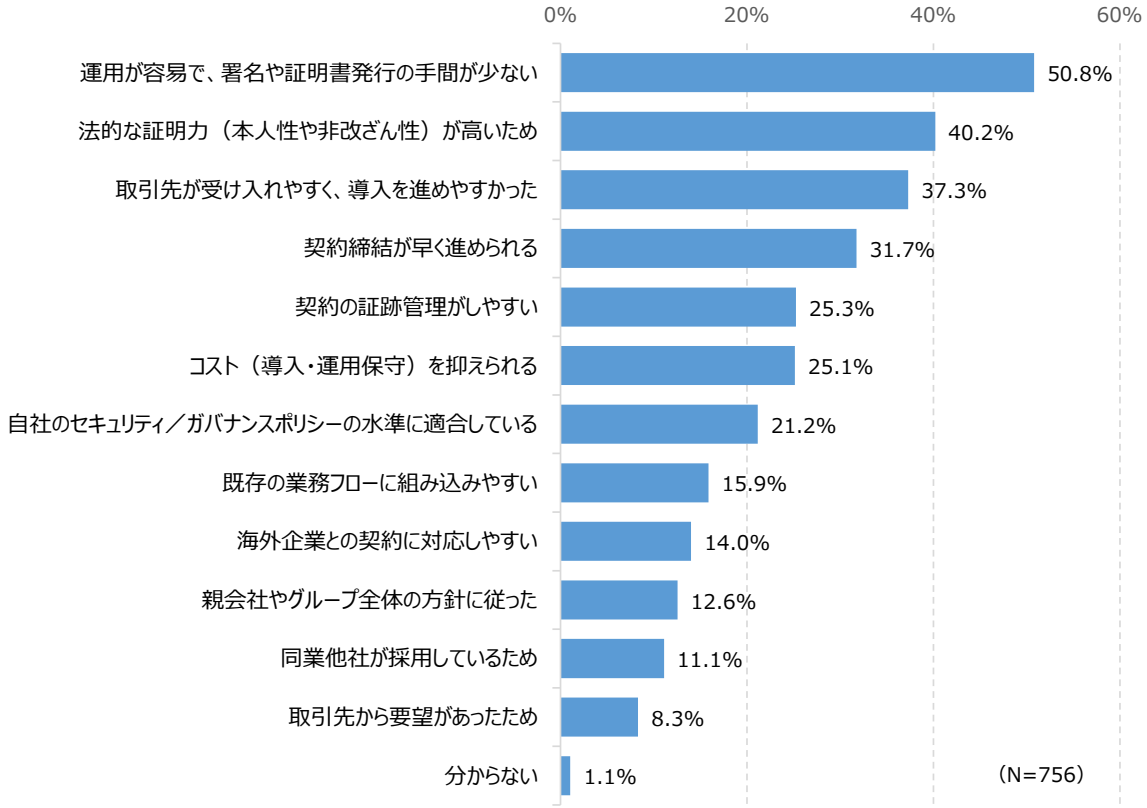
図62 電子契約の利用状況

電子契約方式を選んだ理由

次に、電子契約方式を選んだ理由について質問を行った（図63）。「運用が容易で、署名や証明書発行の手間が少ない」が最も高く、過半数の企業が運用の簡便さを選定の最大の理由として挙げている。電子契約の導入において、実務上の使いやすさが優先される傾向が示されている。

「法的な証明力（本人性や非改ざん性）が高いため」が2位に挙げられており、法的信頼性も電子契約方式の選定において重視されていることがわかる。「取引先が受け入れやすく、導入を進めやすかった」も高い水準にあり、自社内での判断だけでなく取引先との関係性が方式選定に大きく影響していることがうかがえる。電子契約はひとたび利用が始まれば取引先との間で標準化が進みやすく、取引先の受け入れやすさが普及を後押しする重要な要因となっていることが示されている。

「契約締結が早く進められる」や「コスト（導入・運用保守）を抑えられる」も一定程度挙げられており、業務効率化とコスト削減という電子契約の基本的なメリットが理由として認識されていることがわかる。また、「自社のセキュリティ／ガバナンスポリシーの水準に合致している」も約2割の企業が挙げており、電子契約の選定においてセキュリティやガバナンスの観点も一定程度考慮されていることがうかがえる。



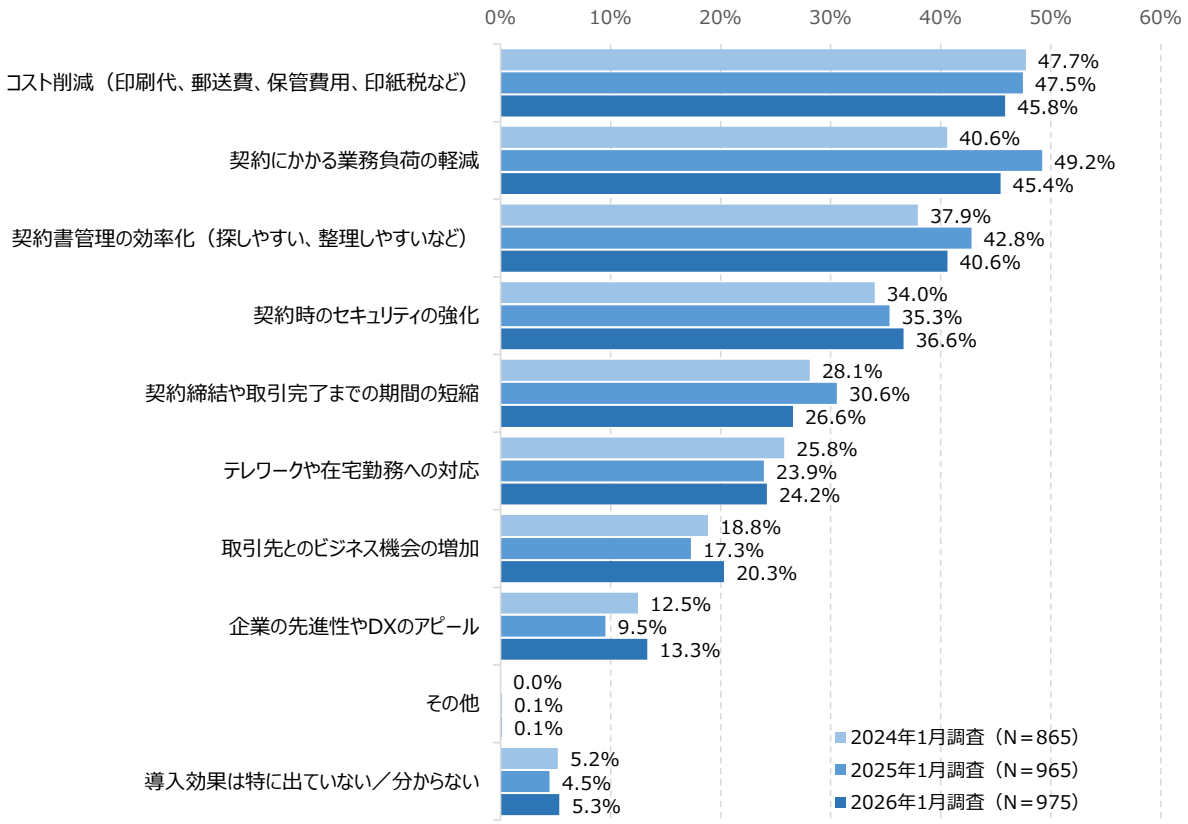
出典：JIPDEC『企業IT利活用動向調査2026』

図63　利用している電子契約方式を選んだ理由

電子契約の利用による効果

次に、電子契約を利用したことによる効果を見てみる（図64）。「コスト削減（印刷代、郵送費、保管費用、印紙税など）」は3年間を通じて最上位を維持しているものの、やや低下傾向にある。電子契約の定着により、コスト削減効果が当然のものとして認識されるようになってきたことが背景にあると考えられる。「契約にかかる業務負荷の軽減」は、2024年調査の40.6%から2025年調査では49.2%へと大幅に上昇したものの、2026年調査では45.4%へと低下している。電子契約の活用範囲が広がり業務負荷軽減効果が広く実感された時期を経て、一定の水準に落ち着いてきていることがうかがえる。

「契約時のセキュリティの強化」は34.0%から36.6%へと上昇傾向にあり、サイバー攻撃リスクへの意識の高まりを背景に、電子契約のセキュリティ面での効果を重視する企業が増えていることが示されている。「取引先とのビジネス機会の増加」や「企業の先進性やDXのアピール」も上昇しており、電子契約が業務効率化にとどまらず、事業拡大やブランド価値向上にも寄与していることがうかがえる。



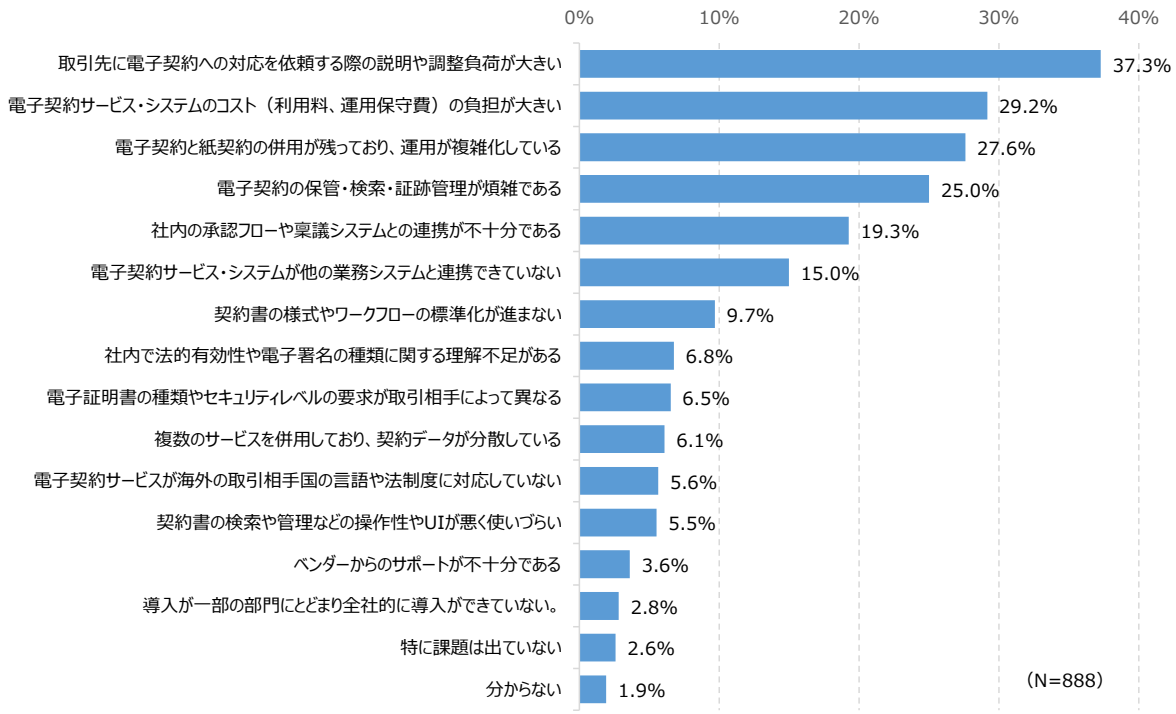
出典：JIPDEC『企業IT利活用動向調査2026』

図64　電子契約の利用による効果

電子契約の導入後における課題

電子契約を導入した後に、どのような課題があるのだろうか（図65）。最も多く挙げられているのは「取引先に電子契約への対応を依頼する際の説明や調整負荷が大きい」であり、約4割の企業が課題として認識している。電子契約の普及が進む一方で、取引先によって電子契約への対応状況や理解度が異なるため、導入・運用における取引先との調整コストが最大の障壁となっていることが示されている。

「電子契約サービス・システムのコスト（利用料、運用保守費）の負担が大きい」と「電子契約と紙契約の併用が残っており、運用が複雑化している」も上位に挙げられており、コスト負担と移行期の運用複雑化が導入定着の障壁となっていることがうかがえる。「電子契約の保管・検索・証跡管理が煩雑である」も高い水準にあり、契約締結後のライフサイクル管理における課題も根強く残っている。また、「社内の承認フローや稟議システムとの連携が不十分である」や「電子契約サービス・システムが他の業務システムと連携できていない」も一定程度存在しており、既存の社内システムとのシームレスな連携が課題となっていることが示されている。



出典：JIPDEC『企業IT利活用動向調査2026』

図65　電子契約の導入における課題

調査結果の考察

本章では、電子契約の利用状況とその効果、課題について調査結果を分析した。そこから得られた考察を以下にまとめる。

1. **電子契約は企業活動の標準的な基盤として定着段階に入っている**：電子契約の利用率は初めて8割を超え、コロナ禍を契機とした急速な普及期を経て定着段階に入っていることが明確に示されている。事業者（立会人）型と当事者型を契約の性質や重要度に応じて使い分ける運用が広がっており、電子契約の活用が単なる紙契約の代替にとどまらず、契約業務の最適化へと深化しつつある。
2. **電子契約の効果はコスト削減・業務効率化から事業価値創出へと広がりつつある**：コスト削減や業務負荷軽減という基本的な効果は定着した一方で、契約時のセキュリティ強化、取引先とのビジネス機会の増加、企業の先進性やDXのアピールといった事業価値に関わる効果が上昇傾向にある。電子契約が業務効率化のツールとしてだけでなく、競争力強化や事業拡大に寄与する戦略的な手段として位置付けられるようになってきていることがうかがえる。
3. **取引先との調整コストと運用の複雑化が電子契約定着の最大の障壁となっている**：電子契約が広く普及しているにもかかわらず、取引先への対応依頼における説明・調整負荷が最大の課題として残っている。また、紙契約との併用による運用の複雑化や、社内システムとの連携不足も根強

い課題であり、電子契約の効果を最大化するためには、業界全体での標準化の推進と社内外のシステム連携の深化が不可欠となっている。

総括・提言

企業を取り巻く経営環境は、デジタル化の加速、サイバー脅威の深刻化、グローバルな規制強化、そしてAIの急速な普及など、かつてないスピードで変化し続けている。こうした環境のなかで、多くの企業は人材不足やコスト増を背景に、既存業務の効率化や組織基盤の安定化を最優先課題として位置付け続けている。一方で、セキュリティ強化への関心が年々高まるとともに、AIによる新規ビジネスの創出を重要課題として挙げる企業も着実に増加している。企業は現在、足元の経営基盤を守りながら、同時にDXとAIによる将来の競争力強化という二つの命題に向き合う局面にある。この両立をどう実現するかが、今後の企業経営における最大の問いである。

DXを実践している企業は着実に増えており、全社戦略に基づくDX推進が過半数の企業に広がっている。内向きのDXでは全項目で成果が出ている割合が上昇するなど定着が進む一方、外向きのDXは依然として成果が出ていない割合が高く、国内DXの大きな課題として残っている。効率化で培ったデータ・デジタル基盤を活かして外向きのDXへと軸足を移し、顧客や市場に新たな価値を提供する取り組みを本格化させることが次の重要なステップとなる。一方、DX推進の障壁として組織間の連携不足や既存システムの複雑さ、現場の業務負荷が課題として顕在化している。テクノロジーの導入と並行して、組織横断的な推進体制の整備と企業文化の変革を一体的に進めることが、DXをさらに高度化させるための鍵となる。

AIの活用は試行・検討段階にとどまっている企業がまだ多く、業種や規模間の格差も大きい。一方で、AIを導入した企業では業務領域を問わず一定の効果が確認されており、DXが定着した企業ほどAI活用の深度が高い傾向も明らかになっている。AI活用を本格化させるためには、DX推進との連動を意識しながら、データ基盤の整備、セキュリティ対策、従業員リテラシーの向上を継続的に推進することが不可欠である。加えて、AIガバナンスの整備が急務となっており、人間による最終判断の確保と説明可能性、AI固有リスクの管理、データガバナンスを柱とした包括的なガバナンス体制を実効性あるものとして機能させることが求められる。

ランサムウェアをはじめとするサイバー攻撃の脅威は深刻さを増しており、約2社に1社が感染を経験している。身代金を支払っても復旧が保証されない現実や、機密情報漏えいを伴うケースの増加、億円規模に及ぶ被害額は、ランサムウェアが経営に直結するリスクであることが、今回の調査結果から改めて示された。また、ビジネスメール詐欺やフィッシングといったソーシャルエンジニアリング攻撃の増加も見過ごすことができない。従来型の境界防御にとどまらず、ゼロトラストの考え方に基づく多層的なセキュリティ体制への移行と、感染を前提としたバックアップ体制やBCPの整備を経営課題として優先的に位置付けることが不可欠である。技術的対策と並行して、社員教育と組織全体のセキュリティ文化の醸成も徹底して進めていく必要がある。

プライバシーガバナンスへの取り組みが事業成果に直結するケースが増えており、経営層の意識向上も進んでいる。プライバシーマークやISMS認証の取得による社内への実効的な波及効果も着実に広がっており、認証取得を単なる要件充足にとどめず、組織能力の強化や企業価値向上につなげる視点が重要となっている。データの越境移転が拡大するなかで、各国規制への対応やCBPRを活用した越境データ流通の信頼基盤の整備も急務となっている。プライバシーガバナンスを法令遵守の枠を超えた経営上の重要課題として位置付け、データ活用とプライバシー保護の両立を推進していくことが、企業の持続的な成長と競争力強化につながっていくと考えられる。

Appendix

調査概要

調査名：　企業IT利活用動向調査2026

実施期間：　2026年1月16日～1月20日

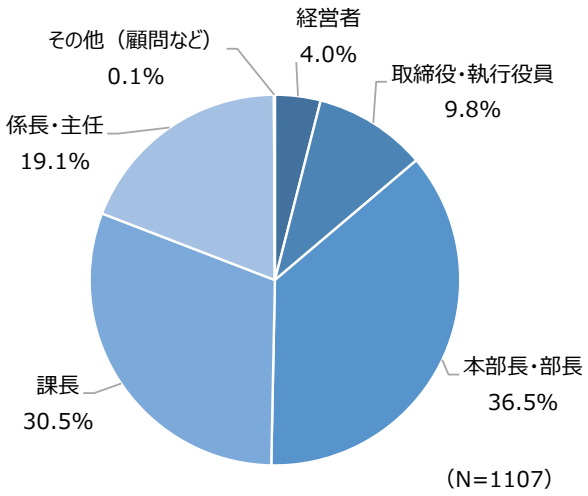
調査方法：　ITRの独自パネルを対象としたインターネット調査

調査対象：　国内企業に勤務し、以下の条件に該当する個人
・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

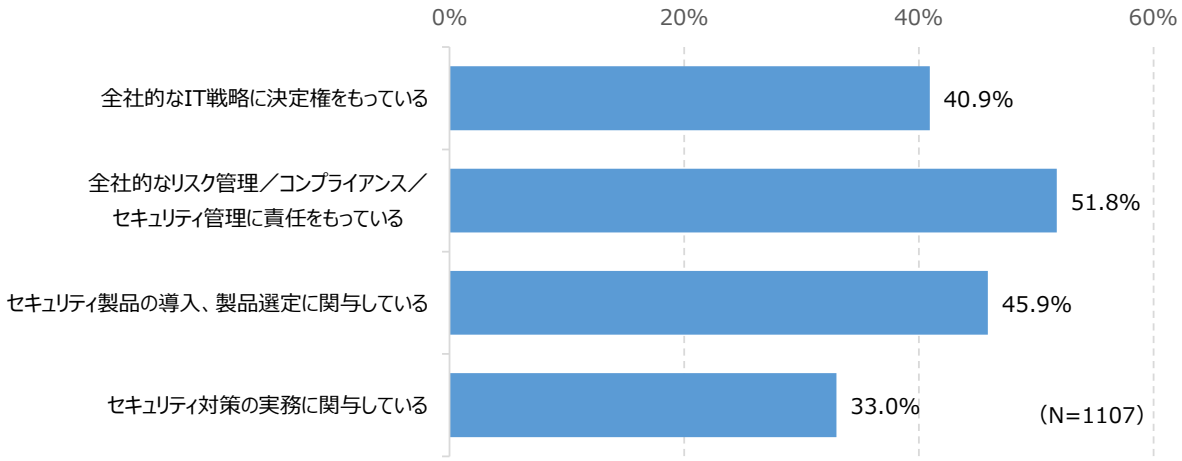
有効回答数：　1,107件（1社1回答）

回答者プロフィール

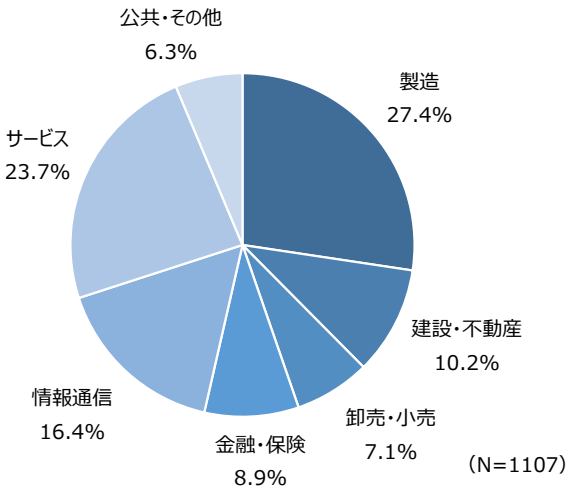
（1）回答者の役職



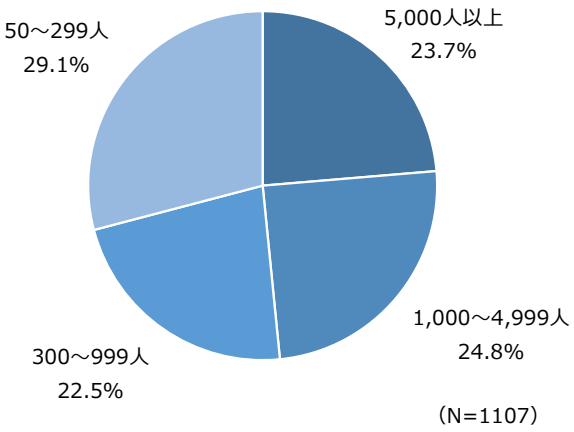
(2) 回答者のIT戦略／セキュリティ戦略への関与



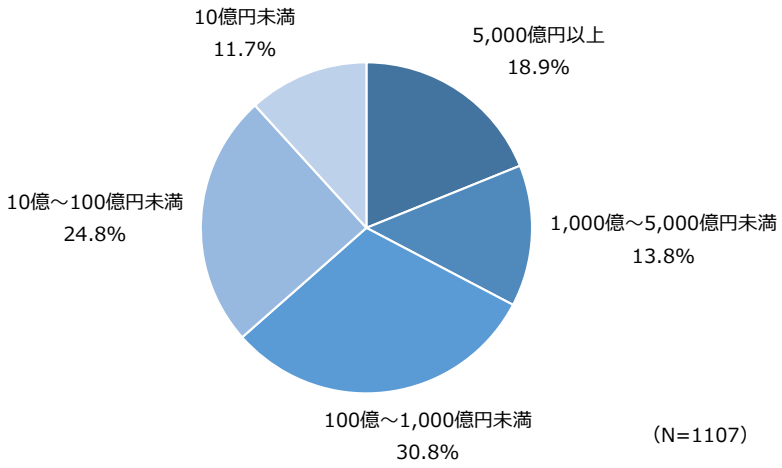
(3) 勤務先の業種



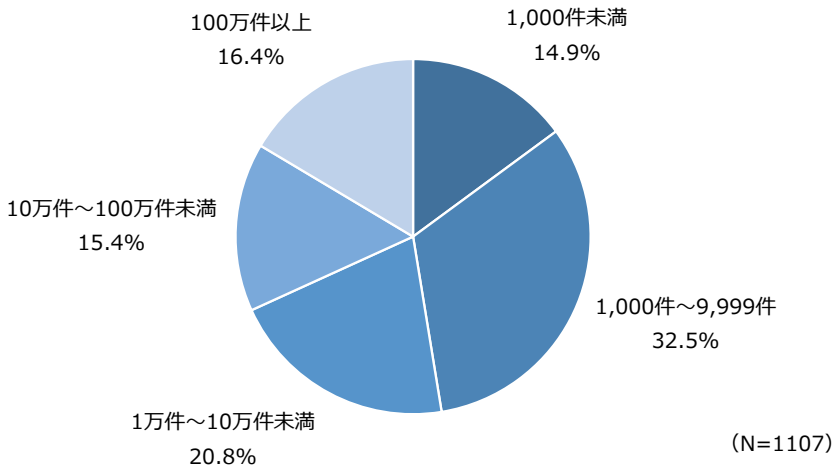
(4) 勤務先の従業員規模



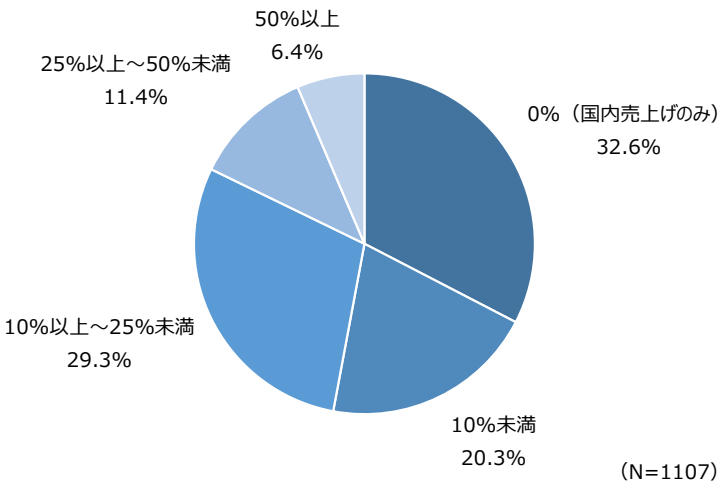
（5）勤務先の年間売上規模



（6）勤務先の個人情報保有件数



（7）勤務先の海外売上比率



本内容は、筆者自身の調査分析に基づく個人的見解で、JIPDECの公式見解を述べたものではありません。

株式会社アイ・ティ・アール

取締役 / プリンシパル・アナリスト　　入谷　光浩氏

ITRにおいて、システム運用とセキュリティに関する市場・技術動向調査と企業向けのコンサルティング・アドバイザリーを担当。
ITR以前は、グローバルIT調査会社IDCにて、15年以上ソフトウェアとクラウドサービスの調査・コンサルティングを担当し、日本における調査責任者も務める。
その他、複数の外資系大手ITベンダーにおいて、事業戦略の立案や新規事業調査を担当。