2024 Spring

IT-REPORT

「企業IT利活用動向調査2024」結果分析
（生成AI、DXへの対応状況等）

Contents

Ⅰ.「企業IT利活用動向調査2024」の概要

Ⅱ. 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」調査レポート～
株式会社アイ・ティ・アール　シニア・アナリスト　入谷　光浩氏

Ⅲ. コラム

・DXの現在地と成果の活用
JIPDEC 電子情報利活用研究部調査研究グループ グループリーダ　松下　尚史

・生成AIと個人情報
JIPDEC　電子情報利活用研究部　主席研究員　手嶋　洋一

・電子メールの安全な未来：
セキュリティガイドラインの最新動向
JIPDEC　セキュリティマネジメント推進室　主幹　佐藤　桂史郎

・データ越境移転ツールの最新動向
－APEC CBPRsからグローバルCBPRへ
JIPDEC　認定個人情報保護団体事務局　事務局長　奥原　早苗

・プライバシーガバナンスをめぐる動き
JIPDEC　電子情報利活用研究部　主幹　恩田　さくら

・「eシール」とは～「シール」本来の意味を入り口に～
JIPDEC　デジタルトラスト評価センター　曾我部　倭玄

〈資料〉情報化に関する動向

JIPDEC
一般財団法人日本情報経済社会推進協会

JIPDEC IT-Report 2024 Spring

Contents

Ⅰ.「企業IT利活用動向調査2024」の概要…… 01
Ⅱ. 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」調査レポート～
株式会社アイ・ティ・アール　シニア・アナリスト
入谷　光浩氏 …… 04
1. DXの実践と成果 …… 04
2. 生成AIの利用と課題 …… 12
3. セキュリティのインシデントと対策の状況 …… 21
4. プライバシー保護に対する取り組み …… 34
5. 第三者認証の取得状況 …… 44
6. 電子契約の利用状況 …… 55
7. 総括・提言 …… 61
Ⅲ. コラム
・DXの現在地と成果の活用
JIPDEC　電子情報利活用研究部　調査研究グループ
グループリーダ　松下　尚史 …… 62
・生成AIと個人情報
JIPDEC　電子情報利活用研究部　主席研究員
手嶋　洋一 …… 63
・電子メールの安全な未来：セキュリティガイドラインの最新動向
JIPDEC　セキュリティマネジメント推進室　主幹
佐藤　桂史郎 …… 64
・データ越境移転ツールの最新動向
－APEC CBPRsからグローバルCBPRへ
JIPDEC　認定個人情報保護団体事務局　事務局長
奥原　早苗 …… 65
・プライバシーガバナンスをめぐる動き
JIPDEC　電子情報利活用研究部　主幹
恩田　さくら …… 66
・「eシール」とは～「シール」本来の意味を入り口に～
JIPDEC　デジタルトラスト評価センター
曾我部　倭玄 …… 68

〈資料〉情報化に関する動向（2023年10月～2024年3月） …… 69

Ⅰ.「企業IT利活用動向調査2024」の概要

JIPDECは、調査会社の株式会社アイ・ティ・アール（ITR）の協力を得て、国内企業の情報システム、経営企画、総務・人事、業務改革部門等に所属し、IT投資と製品選定、もしくは情報セキュリティ管理に携わる役職者を対象に、2010年から情報セキュリティ対策に重点を置いた「企業IT利活用動向調査」を実施している。

2020年に発生したコロナ禍の影響により、ワークスタイルは大きく変化した。政府による緊急事態宣言を契機に業務の効率化を図るためクラウドサービスや電子契約などのデジタル技術を導入・活用し、DX（デジタルトランスフォーメーション）に取り組む企業が増えてきている。さらに今後は生成AI技術を活用したビジネスが増えてくることが予想されるが、一方で生成AI利用・結果が原因で法的問題に発展しかねないリスクも共存している。

そこで、今回の調査では、DXの導入状況や生成AIの導入と利用状況、業務利用に伴う懸念点について企業がどう捉えているか調査を行った。また、セキュリテインシデントの中で、昨今、高度化・巧妙化し、被害が増えている身代金支払いを要求するランサムウェア攻撃について、被害の状況、身代金支払いの有無、被害後のシステム復活の可否なども調査項目に加えた。

その他、第三者認証制度の取得状況、プライバシー保護への取り組み、海外取引先とのデータ越境移転の状況、電子契約の利用状況など、企業の取組状況について調査を行った。

以下、調査の概要と、ITR　シニア・アナリスト　入谷　光浩氏による分析・考察結果を紹介する。

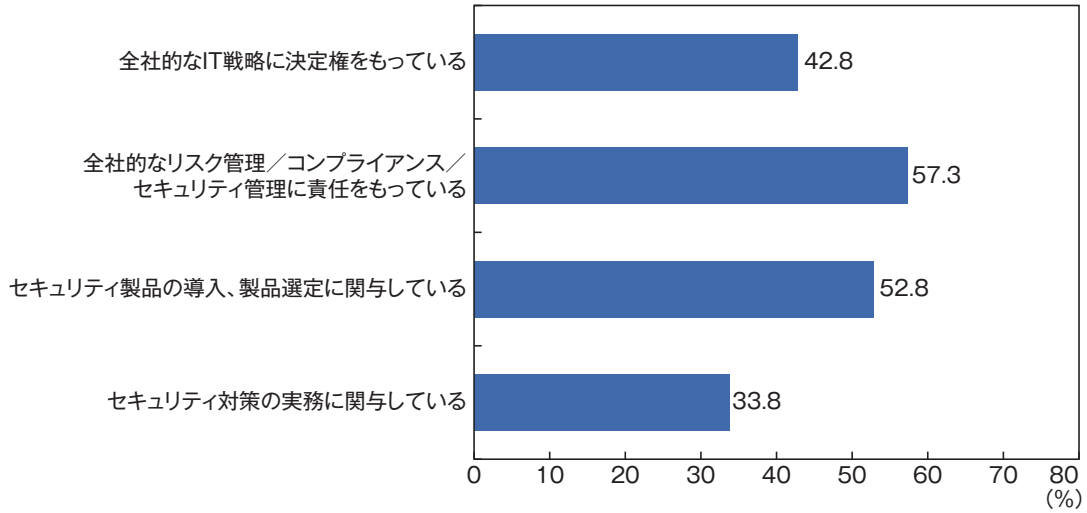
調査概要

・実査期間：2024年１月19日～１月23日
・調査方式：ITRの独自のパネルを利用したWebアンケート
・調査対象：従業員50名以上※の国内企業に勤務し、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推進関連部門のいずれかに所属し、IT戦略策定または情報セキュリティ従事者で、係長（主任）相当職以上の役職者、17,000人
・有効回答数：983件（１社１人）

※本調査では、従業員50名以上の企業を対象としているが、過去２回（2022～2023年）の調査では従業員２人以上の企業を対象としていたため、今回、過去２回分の調査結果と比較をする際には、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。

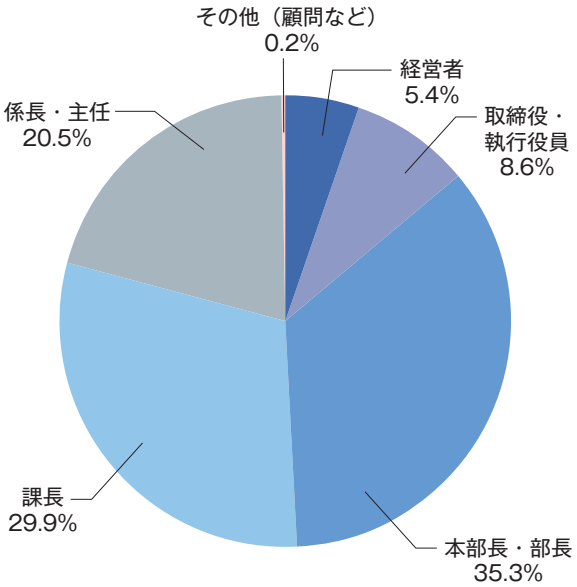
回答者プロフィール

（1）回答者のIT戦略／セキュリティ戦略への関与



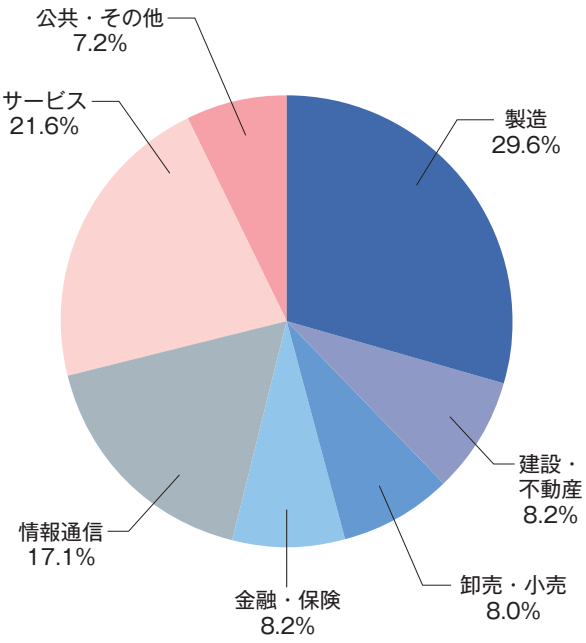
（N=983）

（2）回答者の役職



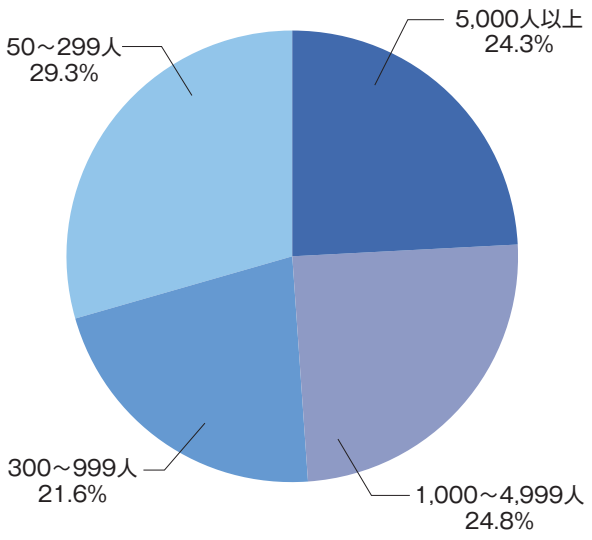
（N=983）

（3）勤務先の業種

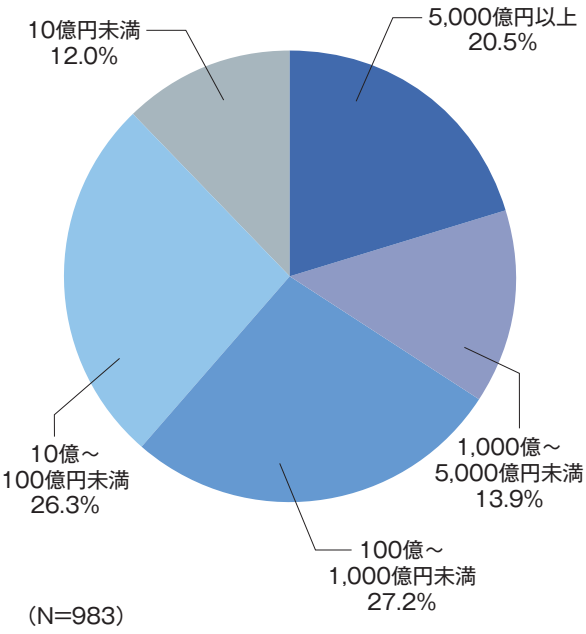


（N=983）

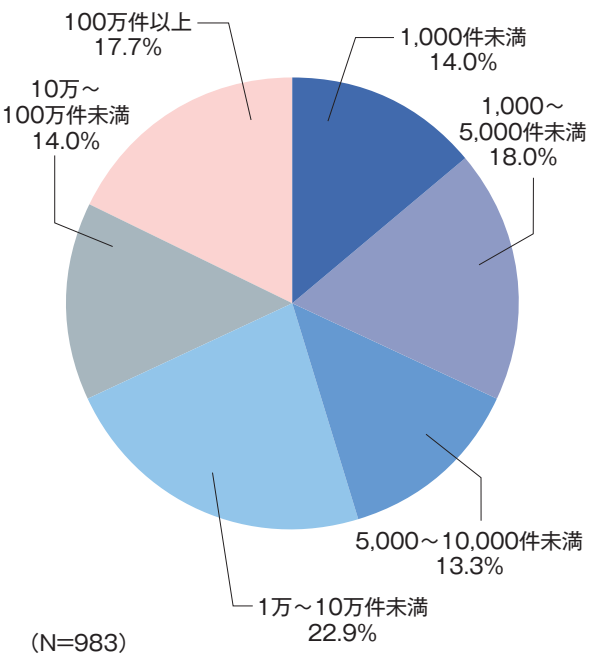
（4）勤務先の従業員規模



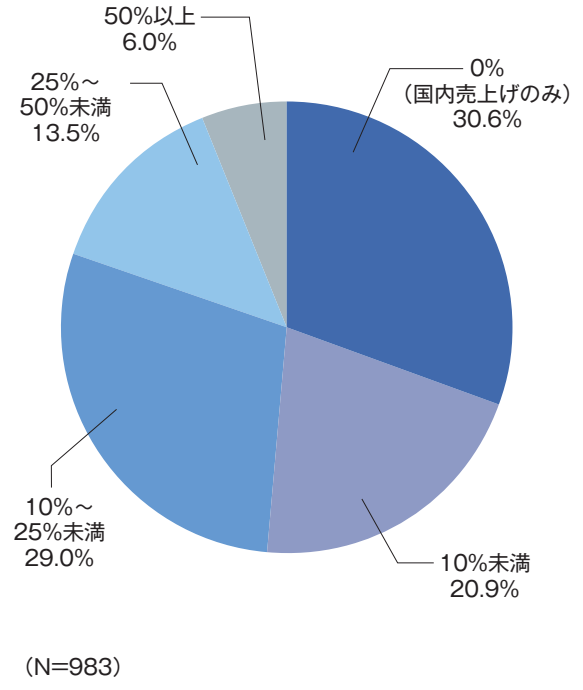
（5）勤務先の年間売上規模



（6）勤務先の個人情報保有件数



（7）勤務先の海外売上比率



Ⅱ．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」調査レポート～

株式会社アイ・ティ・アール　シニア・アナリスト　　入谷　光浩氏

1　DX の実践と成果

本章では、企業におけるDX（デジタルトランスフォーメーション）の実践状況と課題について調査した結果を分析している。多くの企業がDXを実践しているが、業種や企業規模によって実践段階に差があり、さらに成果が出ている取り組みとそうではない取り組みにも差が見られる。今後、DXを進めていく上での課題も明らかになっている。

DXの実践段階の状況

現在、企業のDXがどの実践段階にあるかについて質問を行った（図１）。「着手していない」と「分からない」を除いた85.7%の企業がDXを実践している。そのうち「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」と「全社戦略に基づいて、一部の部門で実践が行われている」を合わせた50.7%は、PoC（Proof of Concept）または一部の部門での取り組みの段階にとどまっている。まだDXの実践は限定的である企業が約半数ということになる。それに対して、「全社戦略に基づいて、部門横断的に実践されている」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」を合わせた34.7%は、DXが全社的な取り組みになり定着化が進んでいる段階にある。

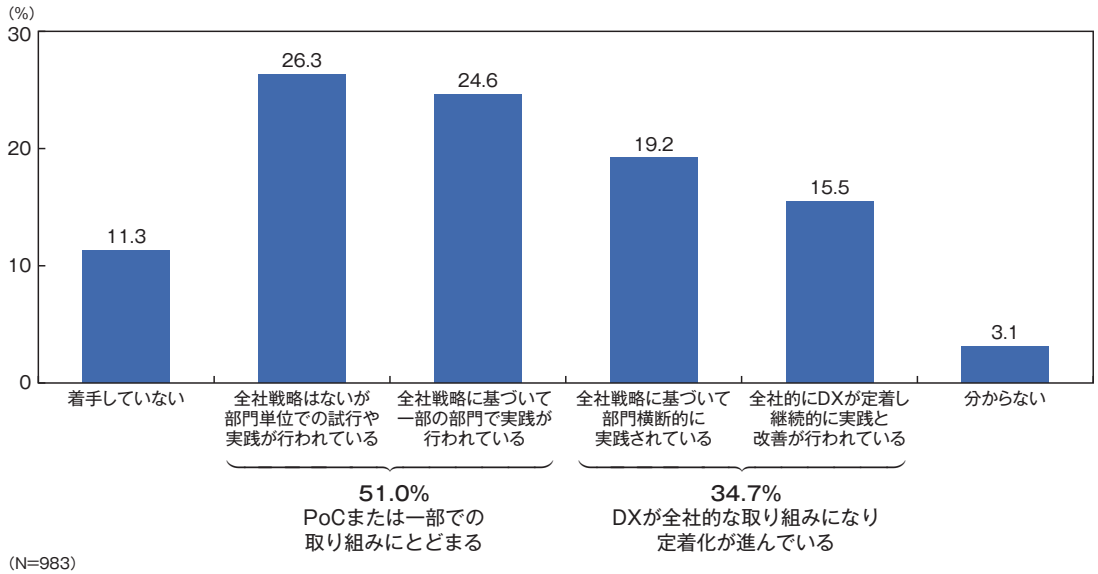


図１　DXの実践段階

次に業種別にDXの実践段階を見てみると、情報通信が全社的な取り組みにおいて先行している（図２）。特に「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29.2%となり、他の業種と比較して高い割合を示している。情報通信はクラウドサービスのようなデジタル技術と親和性が高く、DXが進んでいるのが分かる。その次に、製造と金融・保険が続いている。一方、サービスと卸売・小売は取り組みがやや遅れをとっており、「着手していない」も約20%となっている。

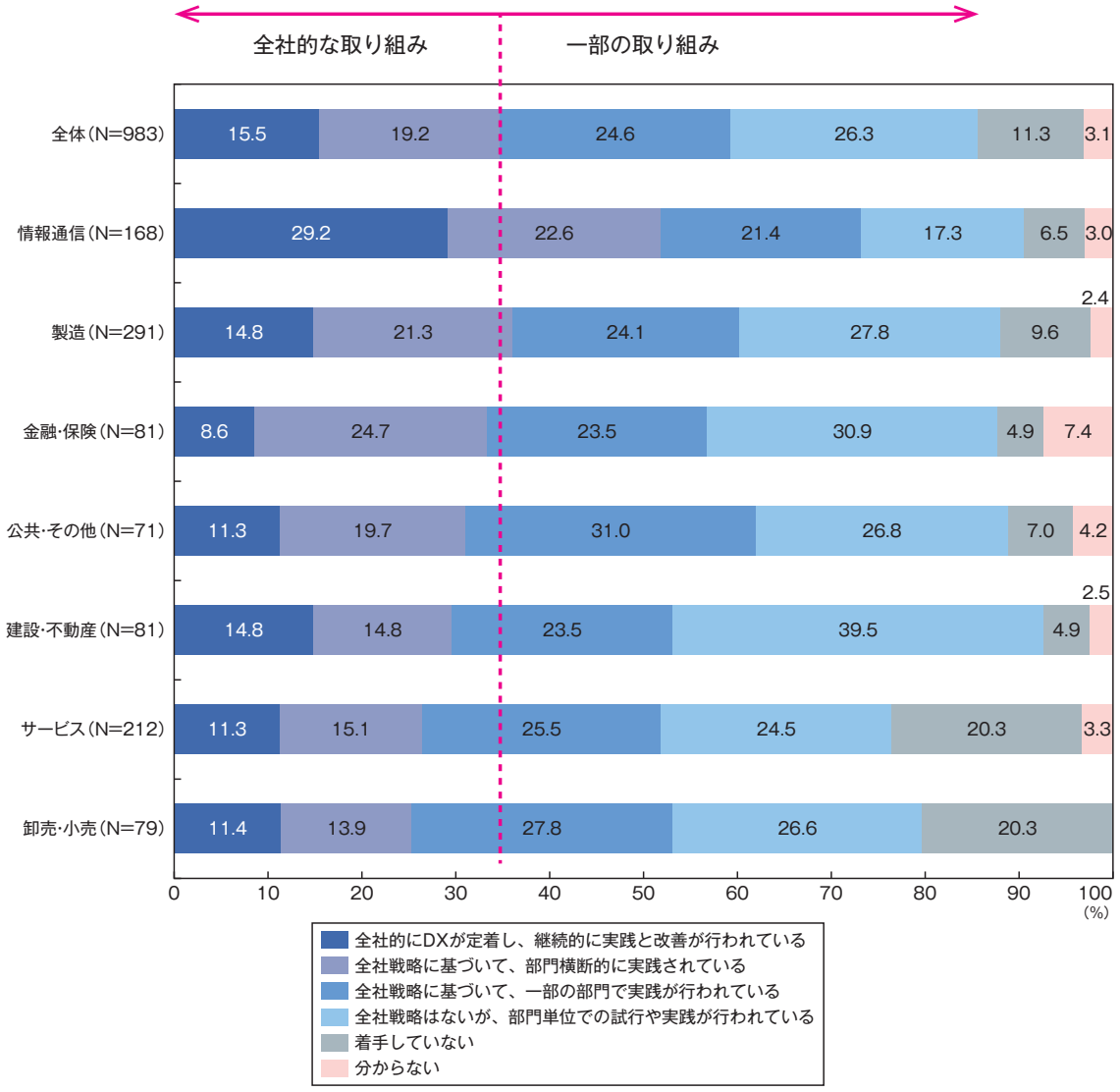


図２　DXの実践段階：業種別

さらに従業員規模別にDXの実践段階を見てみる（図３）。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取り組んでいる企業が半数を超えている。一方、従業員299人以下では、「着手していない」が20%以上となっており、中小企業でのDX実践の遅れが示されている。

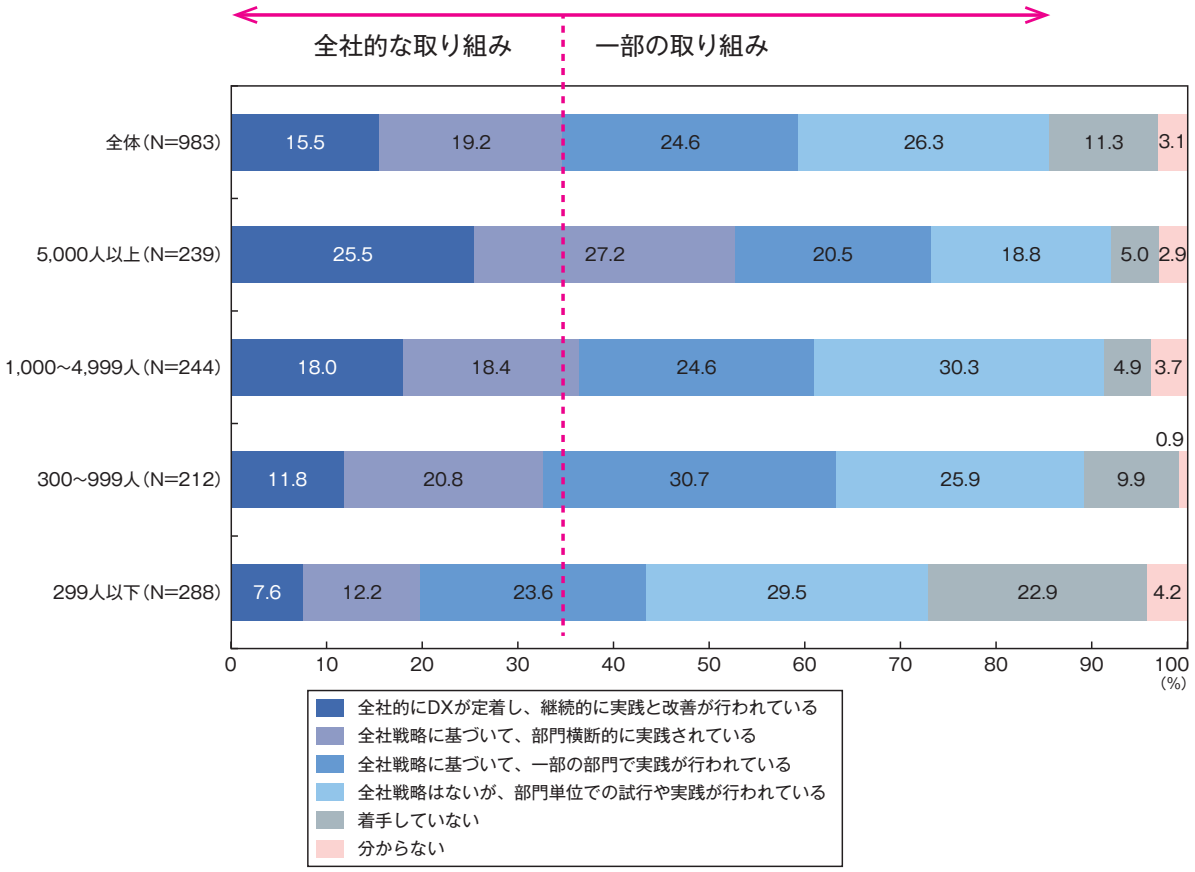


図３　DXの実践段階：従業員規模別

DXの取り組み内容と成果の状況

DXには、さまざまな取り組みがある。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４）。ここでは、DXの取り組みを大きく二つに分類している。一つは「内向きのDX」である。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への取り組みである。もう一つは「外向きのDX」である。顧客や市場に新たな価値を提供するDXへの取り組みである。

最も取り組まれているのは「業務のデジタル化・自動化」であり、半数の企業で成果が出ている。次に「ワークスタイルの変革」が続いている。いずれも内向きのDXであり、外向きのDXに比べて成果が出ている割合が高い。ただし、上記の二つ以外の内向きのDXへの取り組みは、成果が出ているよりも成果が出ていない割合の方が大きい状況にある。

外向きのDXでは、「データに基づいた営業・マーケティングの高度化」と「顧客体験や顧客接点のデジタル化」において成果が出ている割合はやや大きいが、それでも外向きのDXはいずれの取り組みにおいても、まだ成果が出ていない割合の方が大きい。外向きのDXは、ビジネスの成長や変革のために必要となる取り組みとなるので、企業におけるさらなる推進が必要になる。

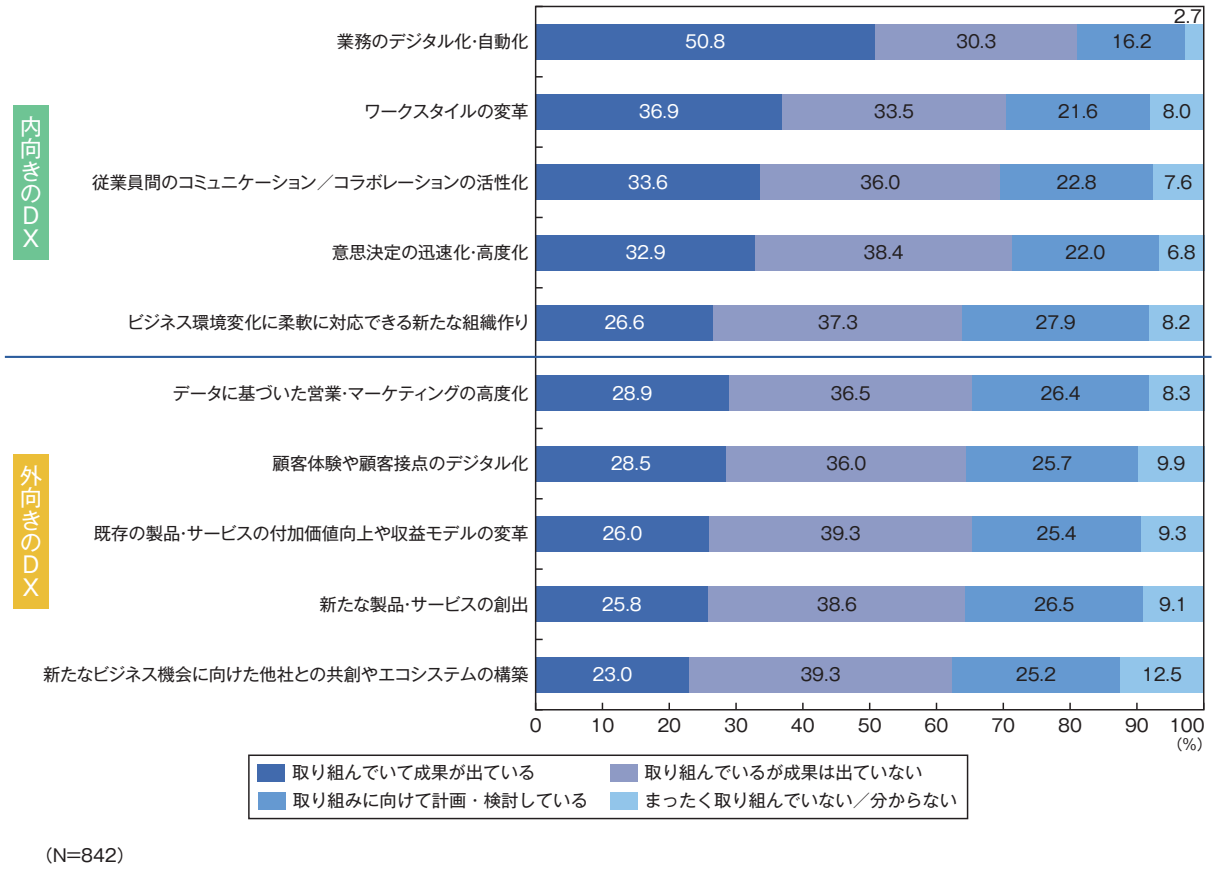


図４　DXの取り組み内容と成果の状況

次に、DXの各取り組みで成果が出ている割合を業種別に見てみる（図５）。情報通信が、「内向きのDX」と「外向きのDX」の両方の平均が大きく、最も成果が出ている業種である。その次に成果が出ている業種が、卸売・小売である。卸売・小売は、DXの実践段階（図２）では、全体的な取り組みとなっている割合はまだ低いが、個々の取り組みでは成果を出している企業の割合が大きい。特に外向きのDXの「データに基づいた営業・マーケティングの高度化」は40%を超えている。変化の激しい消費者のニーズを的確に捉える必要があるため、営業やマーケティングにおける高度なデータ活用が進んでいると見られる。

		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：DXに「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
注２：「内向きのDX平均」と「外向きのDX平均」は、それぞれの取り組み成果の回答率を平均した数値

図５　DXの取り組み成果の状況：業種別

テレワークの実施状況

テレワークの推進は、コロナ禍で急遽対応を迫られたが、DXにおけるワークスタイルの変革の取り組みとしても重要である。そこで、テレワークの実施状況について質問を行った（図６）。全体では、「出社とテレワークを併用しながらのハイブリッド型勤務になっている」が38.5%で現在の主流となっている。「全面的にテレワークでの勤務が中心になっている」は10.9%にとどまっている。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」が23.9%、「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」が6.5%でこれらを合わせると約30%となった。テレワークから出社中心へ回帰している兆候が見られる。

業種別では情報通信が最もテレワークを活用している。一方、建設・不動産や金融・保険ではテレワーク制度がありながらも活用されていない割合が高い。また、従業員規模別では、企業規模が小さいとテレワークの実施率は低くなり、従業員299人以下では、30.9%がテレワーク制度を導入していない状況にある。

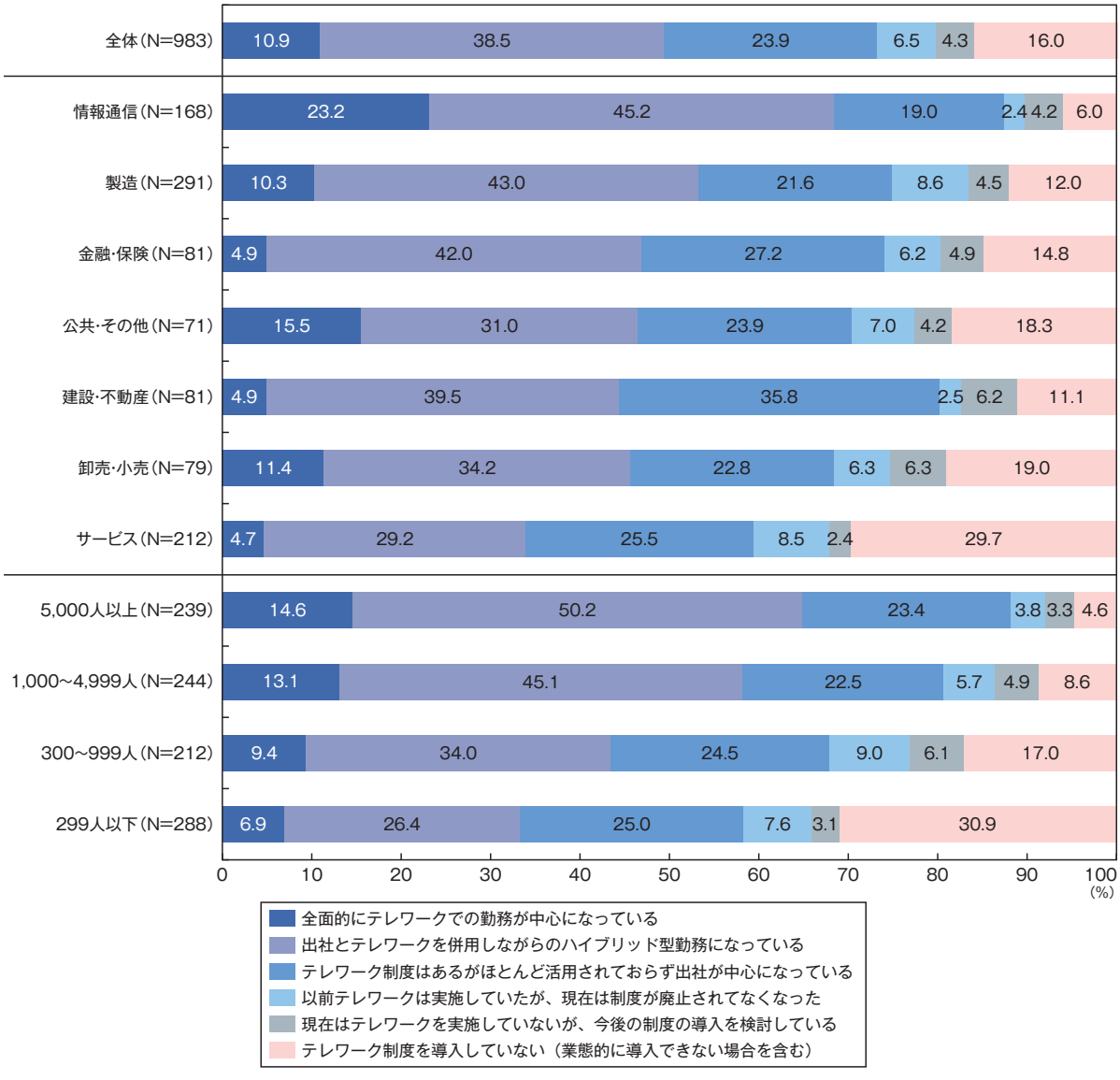


図６　テレワークの実施状況：業種別と従業員規模別

DXを実践していく上での課題：DX実践段階別

DXを実践していく上でどのような課題が出ているのだろうか。最も多い課題は、「情報セキュリティ対策」となった（図７）。どの実践段階においても主要な課題となっている。DXに取り組んでいくためには、さまざまなクラウドサービスを活用することになるが、クラウドへアクセスする際やデータを送受信する際には、どうしてもセキュリティリスクを抱えることになる。そのためにセキュリティ対策は必要不可欠となる。

２番目に大きい課題は、「DX人材の育成と獲得」である。特にDXの実践段階が進むほど企業の回答率が高くなり、全社的にDXが定着している企業では、半数以上がこの課題を回答している。DXが全社的な取り組み、もしくはより高度な取り組みになると、デジタルスキルを有するDX人材が多く必要になってくるため、育成と採用がDXを継続していく上でより重要になる。また、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」の回答率が42.9%と高い。この段階にある企業は、DXの定着化に向けて、これまで投資してきたDXがどのくらいの効果が出ているのかを見極めることが多く、投資対効果をどのように測定するかが重要なポイントになっている。

	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%

図７　DXを実践していく上での課題：DX実践段階別

調査結果の考察

DXの実践状況とその課題についての分析結果から得られた考察を以下にまとめる。

1．**国内企業全体のDXの定着化には時間を要する**：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い状況にあり、国内企業全体のDXの定着化にはまだ時間を要すると考えられる。しかし、全社的な取り組みを行っている企業が３分の１あることから、政府や業界によるDX推進施策の影響が表れていることには、一定の評価ができる。

2．**中小企業のDX推進が鍵となる**：業種や従業員規模でDXの実践段階に差が見られる。デジタル技術と親和性が高い情報通信や金融・保険、そして大手企業でのDXが先行している。一方、サービス業や中小企業では実践が遅れている。特に中小企業のDXを今後どのように後押ししていくかが、国内のDX全体の底上げの鍵になる。

3．**外向きのDXの推進と強化が重要となる**：内向きのDXを優先して取り組み、そこから成果を出しているという調査結果は、業務効率化やコスト削減を優先する日本企業の特徴が示されている。しかし、デジタル化でより一層競争が激しくなっている世界のビジネス環境において、国内企業はビジネスの変革が迫られている。今後は外向きのDXの推進と強化がより重要となり、日本企業のDXの真価が問われるようになっていく。

4．**セキュリティと人材が大きな課題になっている**：DXにはインターネットやクラウドなどを活用したさまざま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DX人材が大きな課題となっていることが明らかになった。特に高度なデジタル技術を要する外向きのDXに取り組んでいく上において、この二つの課題は大きく立ちはだかる。各業界で重点的に取り組み、この課題を乗り越えていく必要がある。

2 生成 AI の利用と課題

本章では、生成AIの利用状況について調査した結果を分析している。生成AIは非常に注目が高まっており、さまざまな業務での活用が期待されている。その一方で、利用していく上でのリスクも指摘されており、安全に利用するための利用規程やガイドラインの策定も重要になっている。

生成AIの使用状況

企業の業務における生成AIの使用状況について質問を行った（図８）。その結果、全体では「会社で構築・契約した生成AIを使用している」が15.9%、「各自で契約・登録した生成AIを使用している（会社で構築・契約している生成AIはない）」が19.1%、合わせて35.0%が生成AIを使用していることが分かった。現状においては、生成AIサービスの法人契約を結ぶなど、会社で構築・契約した生成AIを従業員が使用するというよりも、従業員各自が生成AIサービスを契約・登録して業務で使用している割合の方が大きいという状況にある。一方で、「会社が生成AIの導入を進めている（計画も含む）」という企業が34.5%となり、今後、生成AIの導入が急速に拡大していくと見られる。

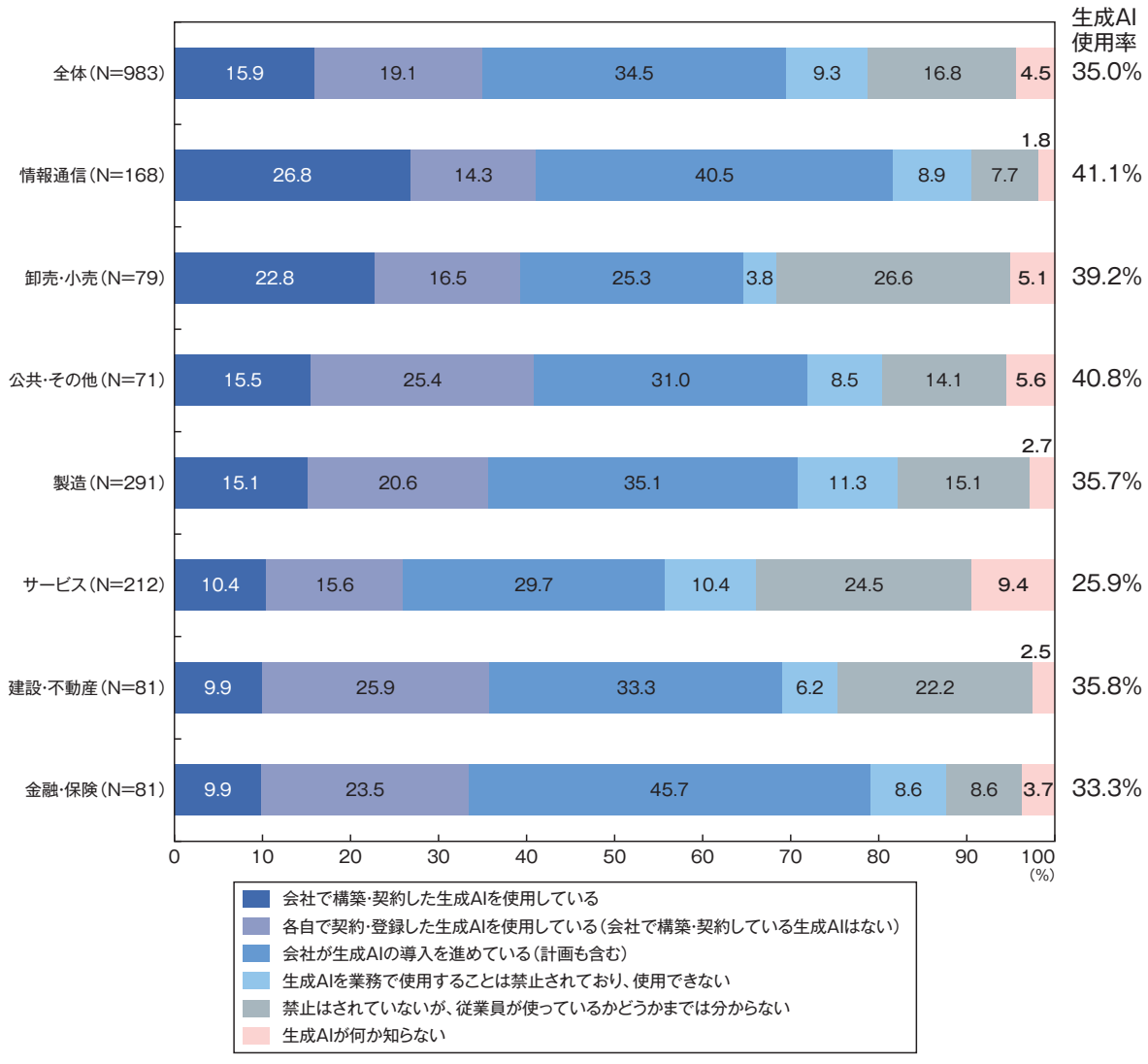


図８　生成AIの使用状況：業種別

業種別に見ると、情報通信、卸売・小売、公共・その他での使用率が40%前後と高くなっている。そのうち、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%以上と高い。金融・保険は現状の使用率は最も低いが、会社で導入を進めているのは45.7%と非常に高く、今後の導入の拡大が期待される。

次に従業員規模別に見てみる（図９）。従業員規模が大きくなるに従い、生成AIの使用率も上昇していき、従業員5,000人以上の企業では、使用率が40%を超えている。

前述のとおり、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利用の割合が高いが、特に従業員999人以下では、その割合が高くなっている傾向が見られる。

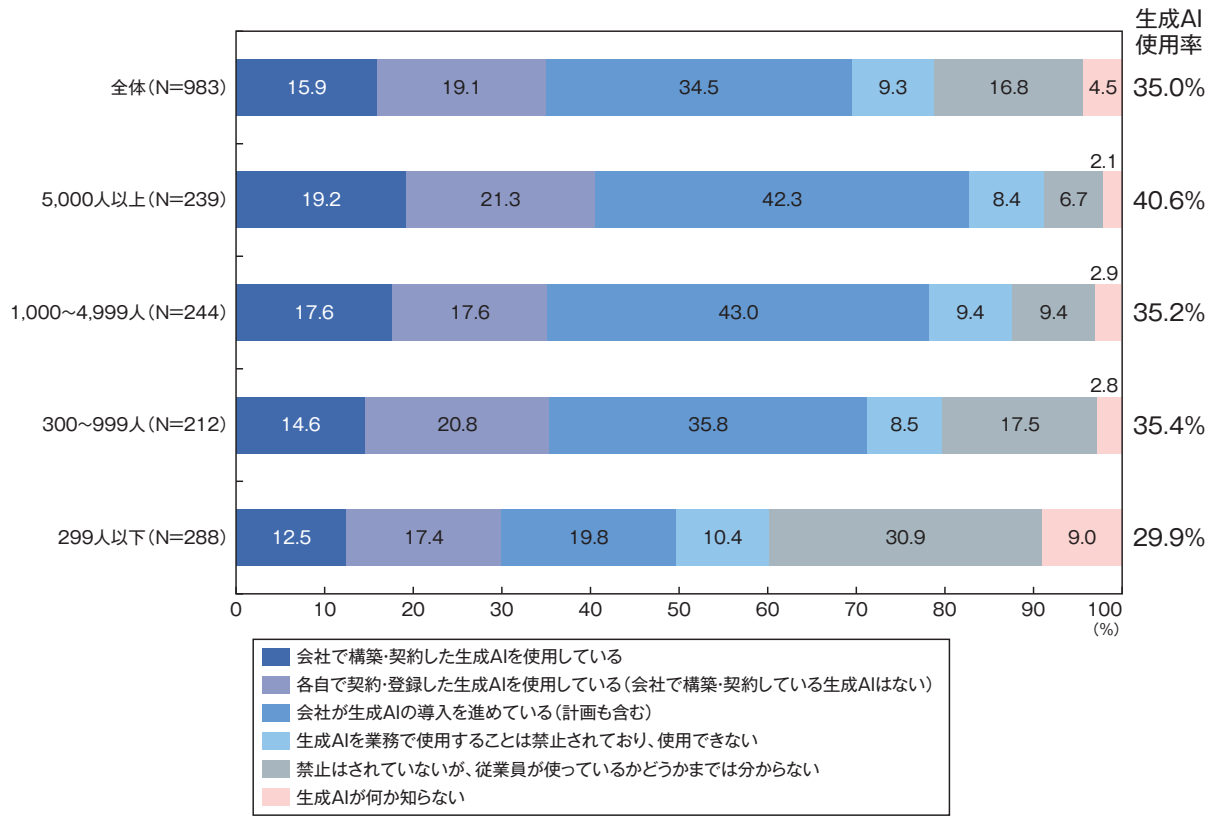


図９　生成AIの使用状況：従業員規模別

さらにDX実践段階別に見てみる（図10）。DXが定着して継続的に実践している企業は、生成AIの使用率が50%以上となり、さらに会社で構築・契約した使用が40.1%と非常に割合が高く、会社として戦略的に生成AIを利用している状況をうかがうことができる。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高く、生成AIは場当たり的な利用となっている。しかし、現在、導入を進めている企業は多く、今後は戦略的な利用にシフトしていくと考えられる。

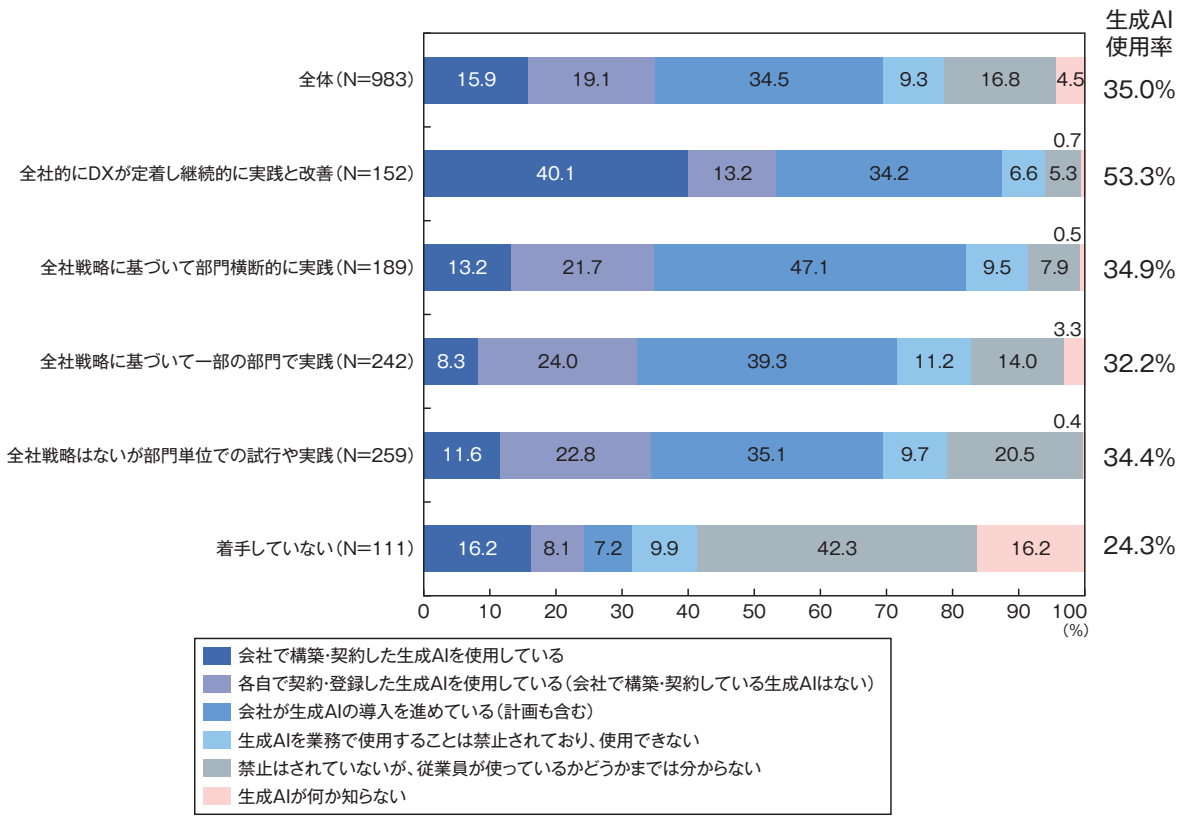


図10　生成AIの使用状況：DX実践段階別

生成AIを使用している業務

生成AIはどのような業務で使用されているのだろうか（図11）。会社で構築・契約した生成AIを使用している企業は、「調べものや市場調査」が64.1%と非常に多いが、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」、「Webサイトや記事の原稿作成」、「マニュアルや規程・ルールの作成」などがある。

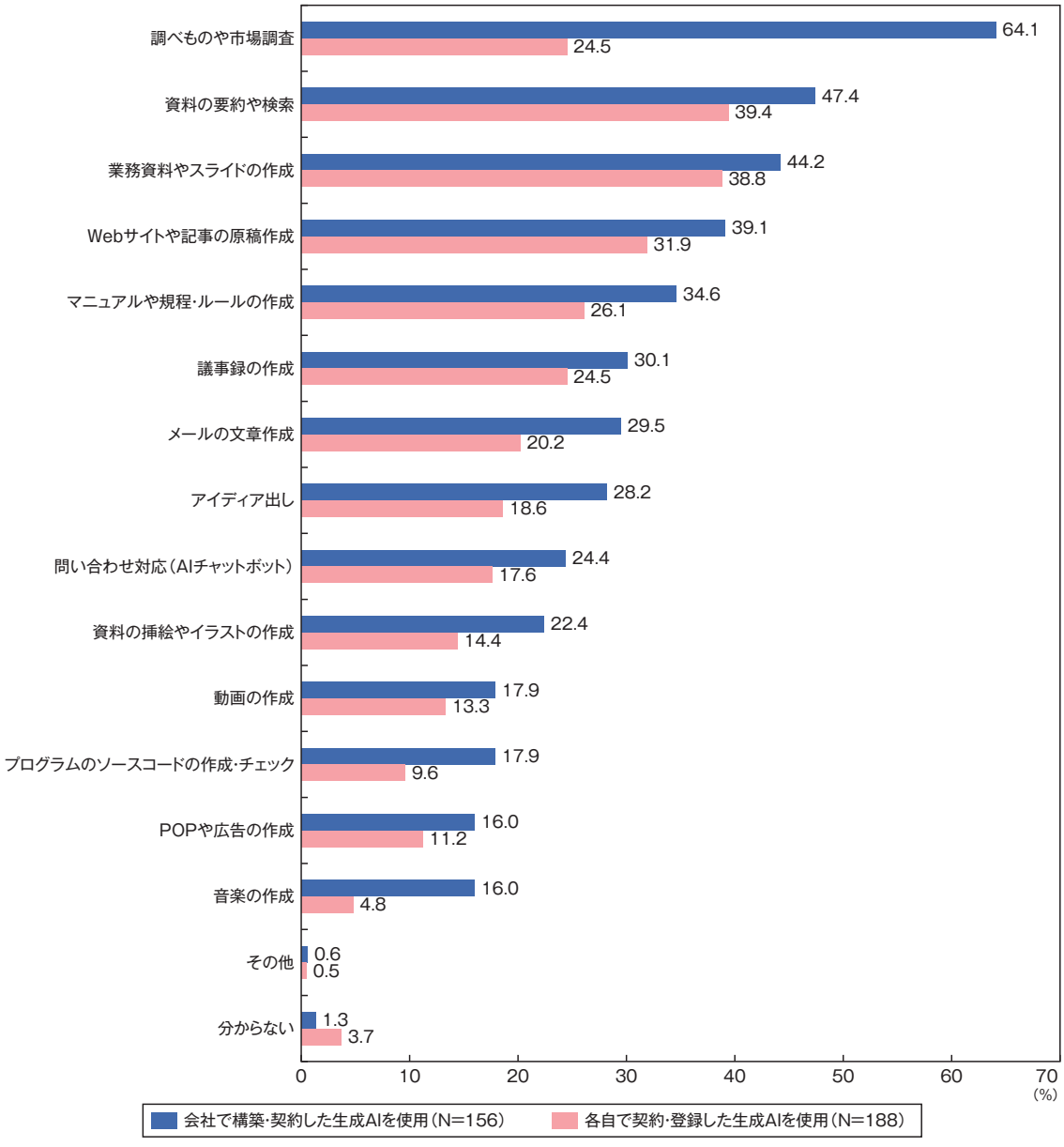


図11　生成AIを使用している業務

次に業種別に見てみる（図12）。ここでは、「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」の回答者を合わせて集計している。特徴的な結果としては、卸売・小売において、「メールの文章作成」や「アイディア出し」、「問い合わせ対応（AIチャットボット）」、「資料の挿絵やイラストの作成」など、他の業種よりも多様な用途で活用している。また、IT業務において活用が期待されている生成AIによる「プログラムのソースコードの作成・チェック」は、情報通信でも18.9%の使用率にとどまっており、まだそれほど活用が進んでいない状況が見てとれる。

	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 規程・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%

注：「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

図12　生成AIを使用している業務：業種別

生成AIの業務使用における懸念点

生成AIを業務で使用していく上で、どのような懸念点があると考えられているのだろうか（図13）。会社で構築・契約した生成AIを使用している企業は、「社内の機密情報を生成AIに入力してしまい、それが学習データとして使用され情報漏えいしてしまう」に対する懸念が大きい。例えば、A社の従業員が生成AIに開発中の製品に関する情報をプロンプトに含めて入力してしまい、それが学習され、競合となるB社の従業員が生成AIを使用してA社の調査をしたところ、A社の開発中の製品情報が出力されてしまうということが想定される。これはA社にとって大きなリスクとなる。一方、各自で契約・登録して使用している企業の回答率はそこまで高くなく、情報漏えいリスクへの危機感が薄いと考えられる。

次の大きな懸念点として、「生成AIが出力した偽情報を従業員が信じて業務で使用してしまう」があがっている。生成AIは事実と異なる情報を生成することがある。これをハルシネーションと呼ぶ。生成AIが出力した偽情報をそのまま鵜呑みにしたことで、誤った意思決定や顧客からの信頼低下を招く恐れがある。その他、「生成AIが出力した情報に倫理的や道徳的な問題が含まれている」、「生成AIによって生成されたコンテンツが著作権に違反しているかもしれない」、「生成AIがバイアスを持っており、偏った判断や知見をもたらしてしまう」などの懸念が出ている。生成AIはまだ発展途上の技術であり、上記のようなさまざまなリスクがあることを理解した上で使用しなければならない。

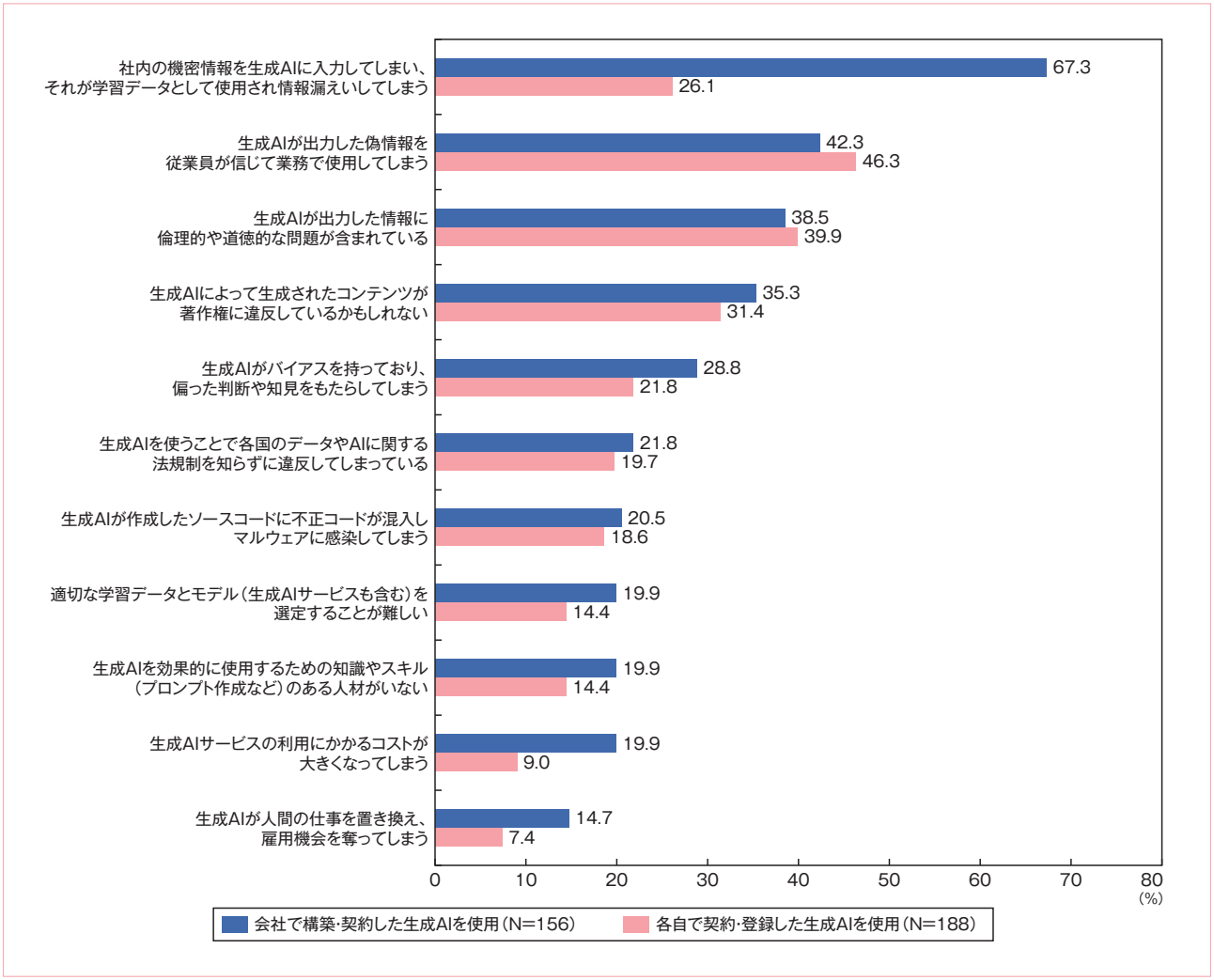


図13　生成AIの業務利用における懸念点

生成AIに関する利用規程・ガイドラインの策定状況

前述した生成AIの使用で生じるリスクに対応するために、プロンプト入力の際の機密情報の取り扱いのルールや禁止事項などのような利用規程もしくはガイドラインを定めている企業はどの程度いるのだろうか（図14）。会社で構築・契約した生成AIを使用している企業の約３分の２は、利用規程・ガイドラインを定めている。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、現状で利用規程・ガイドラインを定めておらず、多くが作成中あるいは作成予定という状況にある。これは非常に危険である。また、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。

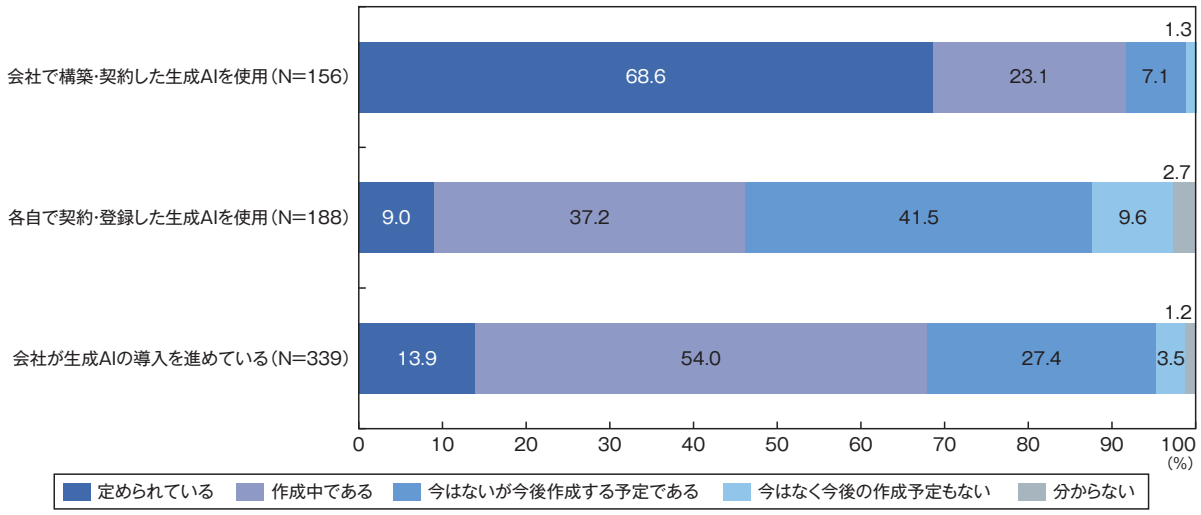


図14　生成AIに関する利用規程・ガイドラインの策定状況

調査結果の考察

生成AIの利用状況と課題についての分析結果から得られた考察を以下にまとめる。

1．**生成AIの利用は急拡大していく**：調査結果から、現時点ではまだ生成AIをビジネスに取り入れている企業は多いとは言えないが、これから急速に拡大することが予測される。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増えていくだろう。

2．**多様な業務の適用が見込まれる**：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、今後は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見られる。

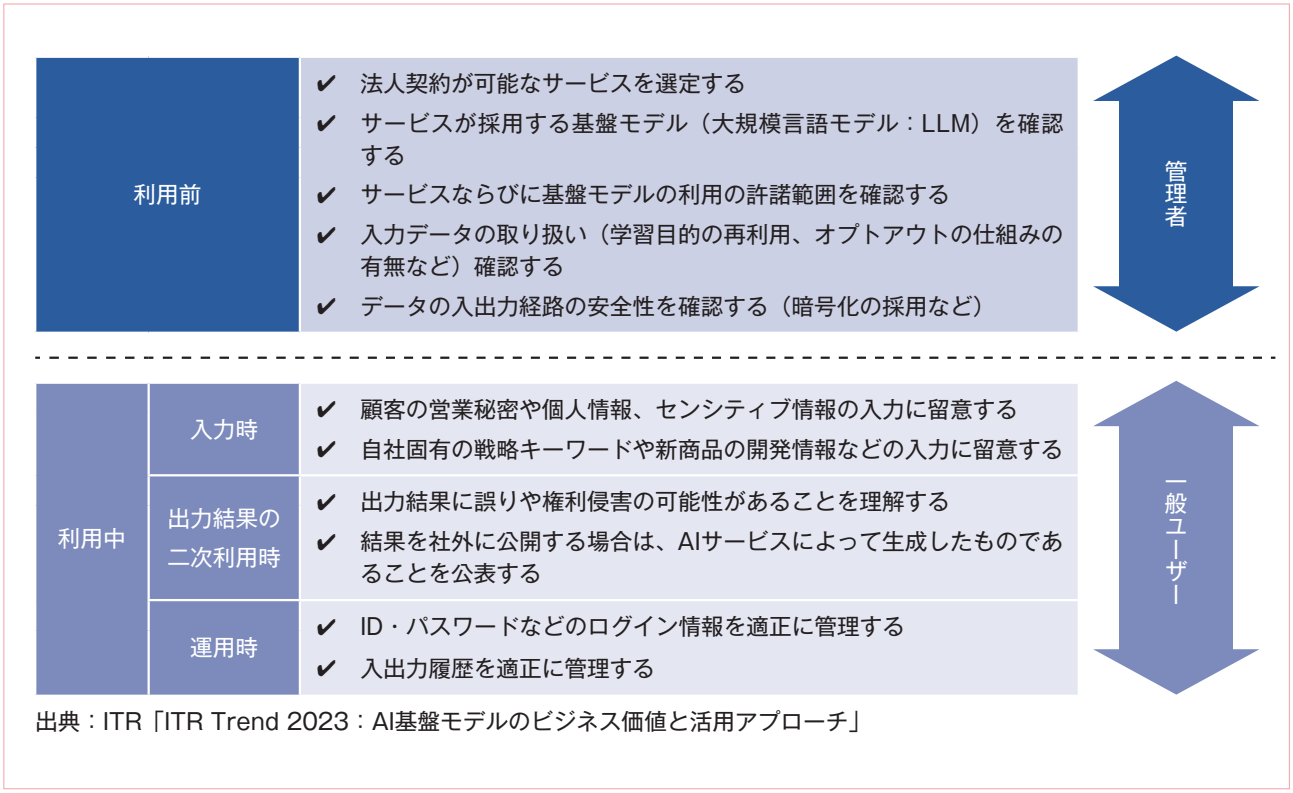
3．**さまざまなリスクがあることを認識すべきである**：生成AIを使用する上で懸念が多いリスクは、情報漏えいとハルシネーションとなっている。特にプロンプト入力の際における機密情報の取り扱いは十分に注意する必要がある。また、倫理に反する情報の生成、生成されたコンテンツの著作権侵害など、さまざまなリスクがあることを認識した上で生成AIを利用することが重要である（図15）。

分類		概要
1	機密性	・プロンプト入力を通じた個人情報、営業秘密情報の漏えい ・アカウント情報の漏えい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えい
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「ITR Trend 2023：AI基盤モデルのビジネス価値と活用アプローチ」

図15　生成AIを利用する際のリスク

4．**利用規程・ガイドラインの策定は必須である**：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、利用規程やガイドラインの策定が必須である。特に従業員各自で登録した生成AIを業務で使用させている企業の多くは、策定が進んでおらずリスクに晒されている状況にある。チェックリスト例（図16）を参考に、早急に利用規程・ガイドラインを策定すべきである。



出典：ITR「ITR Trend 2023：AI基盤モデルのビジネス価値と活用アプローチ」

図16　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

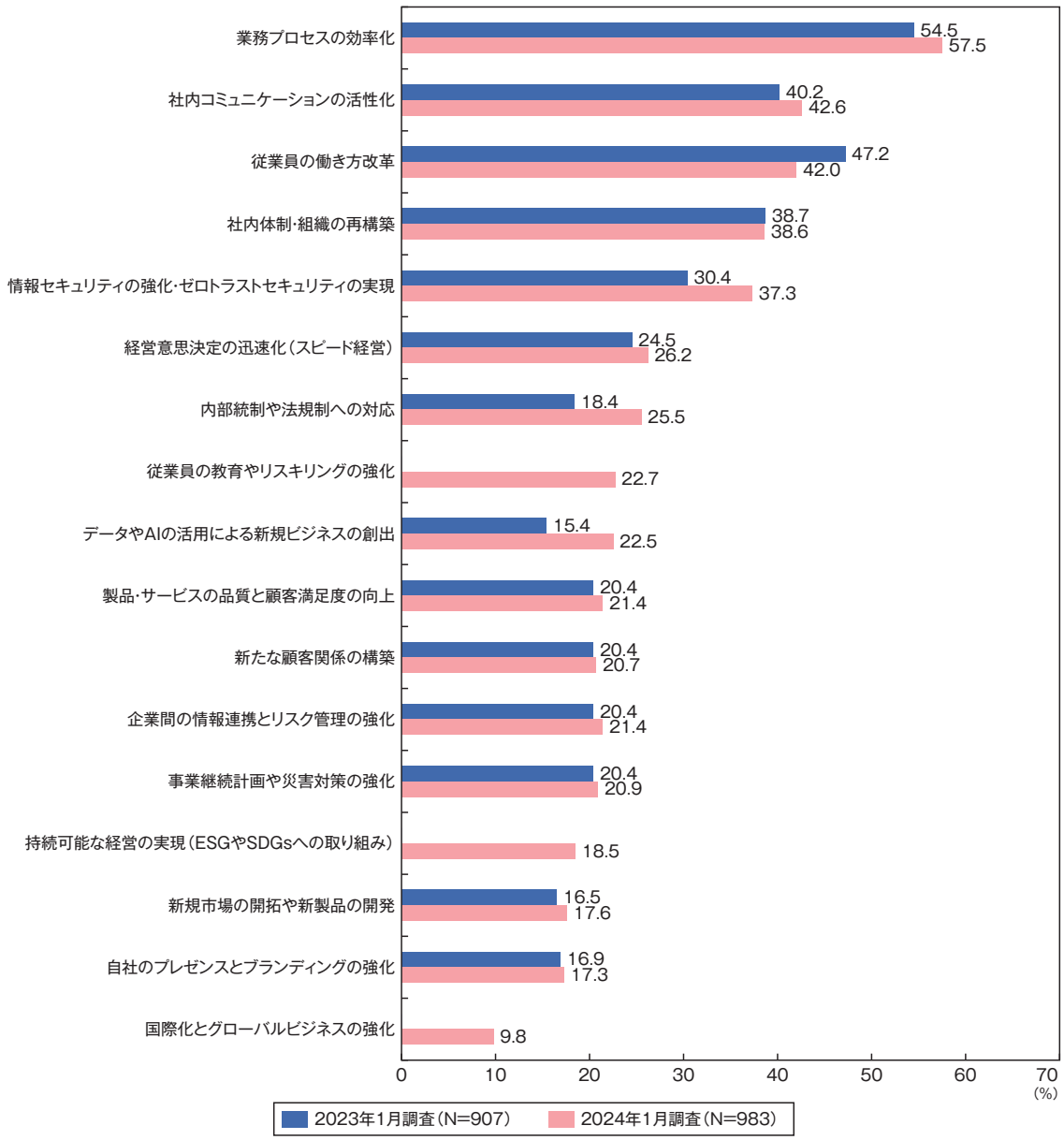
3 セキュリティのインシデントと対策の状況

本章では、企業におけるセキュリティインシデントの状況とそれに対する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。ランサムウェアに代表されるサイバー攻撃はますます巧妙化と高度化が進んでいることから、セキュリティリスクの中でも、特にサイバーリスク対策の実施・継続のための投資が経営戦略の中で重要性が高まっている。それと同時に、人為的なミス、あるいは悪意のある不正行為による情報漏えいの対策への投資も重要性が高まっている。

経営課題におけるセキュリティの位置づけ

企業が今後に向けて取り組みを重視していく経営課題について質問を行った（図17)。「業務プロセスの効率化」、「社内コミュニケーションの活性化」、「従業員の働き方改革」、「社内体制・組織の再構築」は2023年調査と同様、回答率が高く主要な課題となっている。それに続くのが「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」となっているが、2023年調査から大きく上昇し、上位４つの主要課題に迫ってきている。これからの経営において、セキュリティへの取り組みがこれまで以上に重要となっていくと見られる。また、「内部統制や法規制への対応」も2023年調査から大きく上昇しており、コンプライアンス対応の重要性も高まっていくであろう。

その他、「経営意思決定の迅速化（スピード経営)」、「従業員の教育やリスキリングの強化」、「データやAIの活用による新規ビジネスの創出」が上位にあがっている。これらはDXの取り組みにも通ずるところがある。特に「従業員の教育やリスキリングの強化」は、DX人材の育成につながっていく。



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している
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

図17　今後に向けて重視していく経営課題

過去１年に経験したセキュリティインシデント

次に、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18）。「従業員によるデータや情報機器（PC、タブレット、スマホ、USBメモリなどの記録媒体）の紛失・盗難」が40.7%と最も多く、過去２回の調査よりも上昇している。さらに、「個人情報の漏えい・滅失（人為ミスによる）」、「非デジタル文書（契約書などの重要資料）の紛失・盗難」、「個人情報の漏えい・滅失（内部不正による）」も上位にあがっており、過去２回の調査よりも上昇している。これらは、従業員によって引き起こされる内部のインシデントである。

２番目に多い「社内サーバー／PC／スマートフォン等のマルウェア感染（ランサムウェアも含む）」も過去２回の調査から大きく上昇しており、外部攻撃によるインシデントも増加していることが分かる。内部・外部双方のセキュリティインシデントが拡大している状況にある。

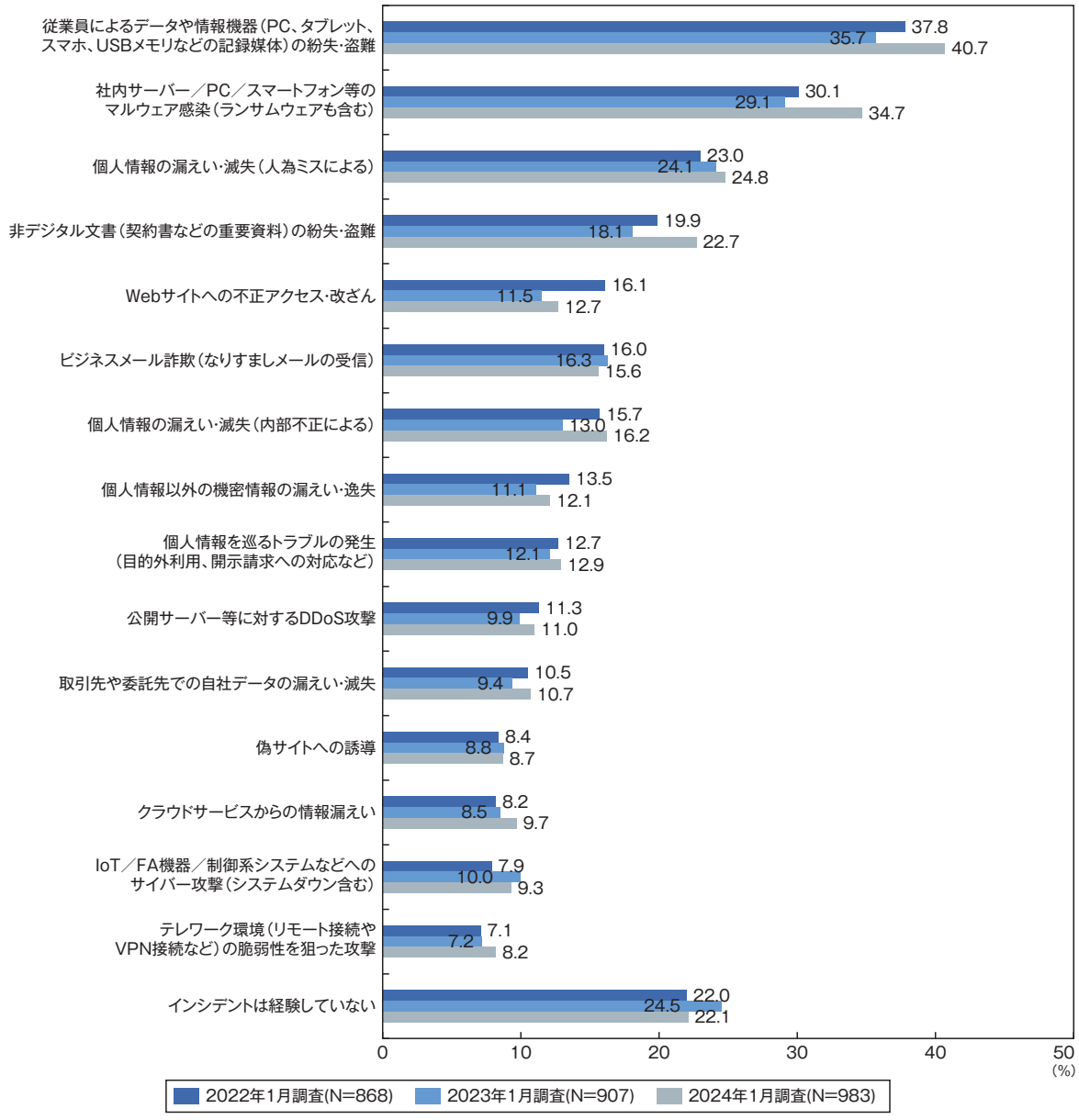


図18　過去１年に経験したセキュリティインシデント

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19）。ランサムウェアの感染被害を経験した企業は47.1%となった。そのうち、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。身代金を支払った企業は26.9%であるものの、それでも復旧できなかった企業は17.9%となっている。ランサムウェアに感染すると、身代金の支払い有無に関わらず復旧は困難な状態になるということが調査結果からうかがえる。

業種別に見ると、最も感染割合が高いのは製造で60.1%、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。この三つの業種では、感染した企業のうちおよそ３分の１程度しか復旧できていない。最も感染割合が低いサービスでも30%以上の感染経験がある。いずれの業種においても、ランサムウェアの感染リスクがあると認識する必要がある。

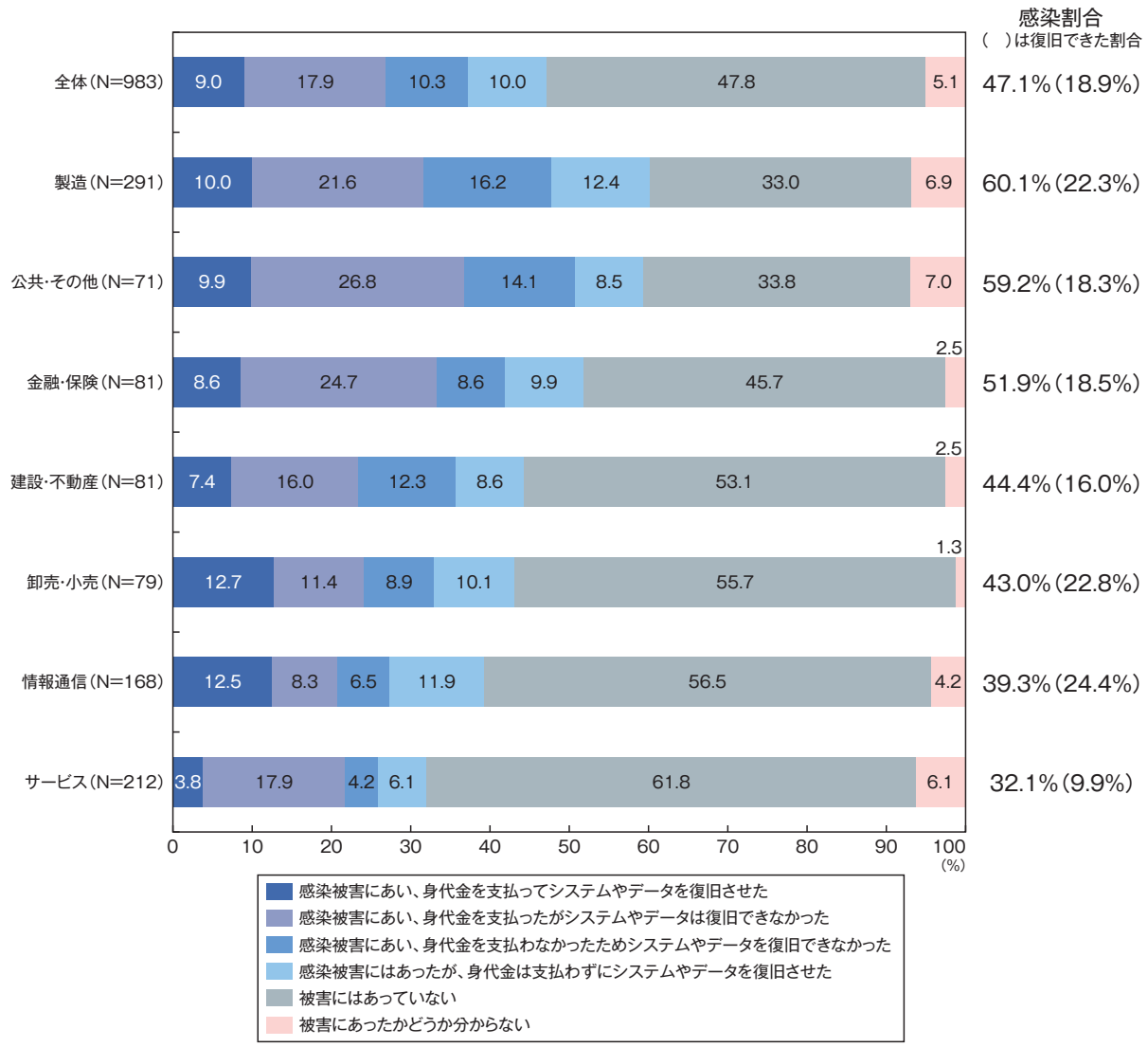


図19　ランサムウェアの感染被害の経験：業種別

従業員規模別に見ると、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（図20）。1,000人～4,999人と5,000人以上では感染割合が50%以上となっており、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30%以上の企業で感染経験があり、中小企業でもランサムウェア攻撃のターゲットになってしまう可能性は十分にある。

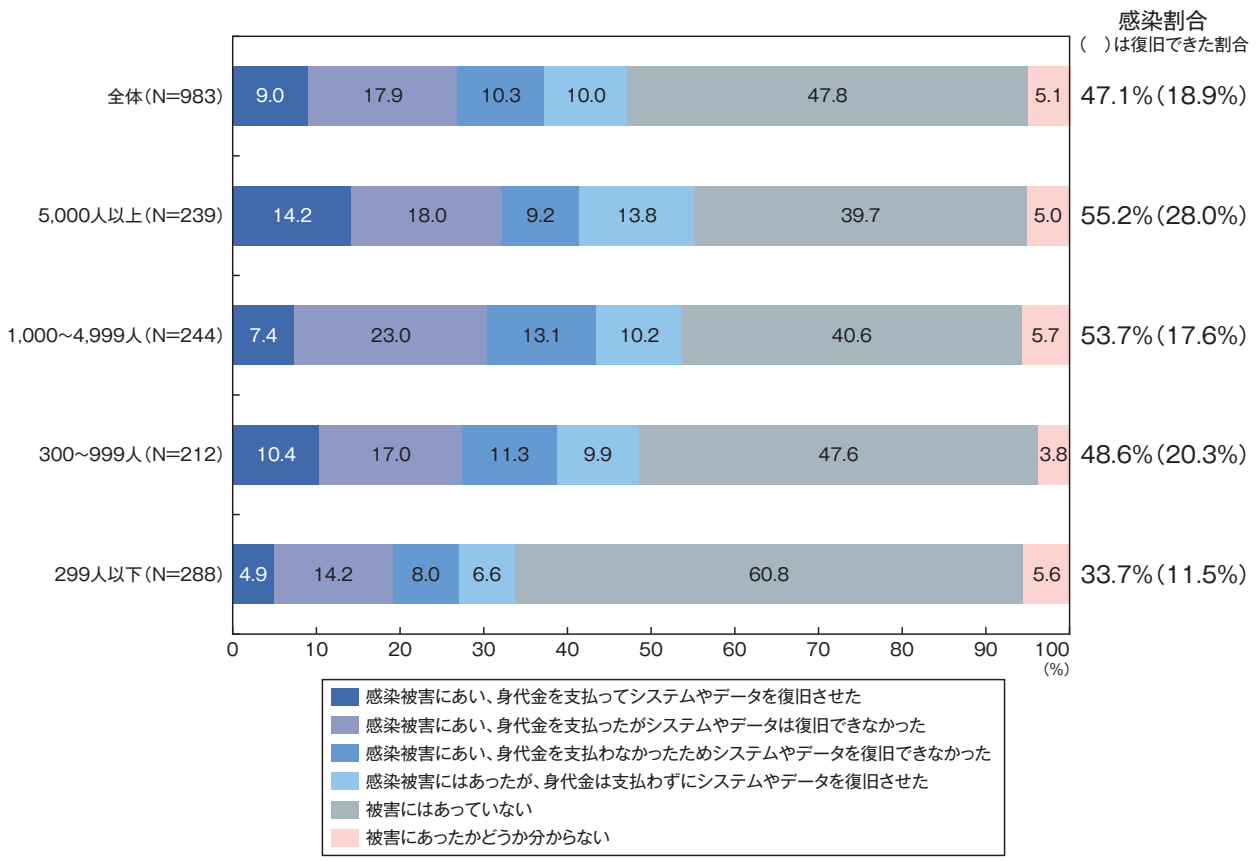
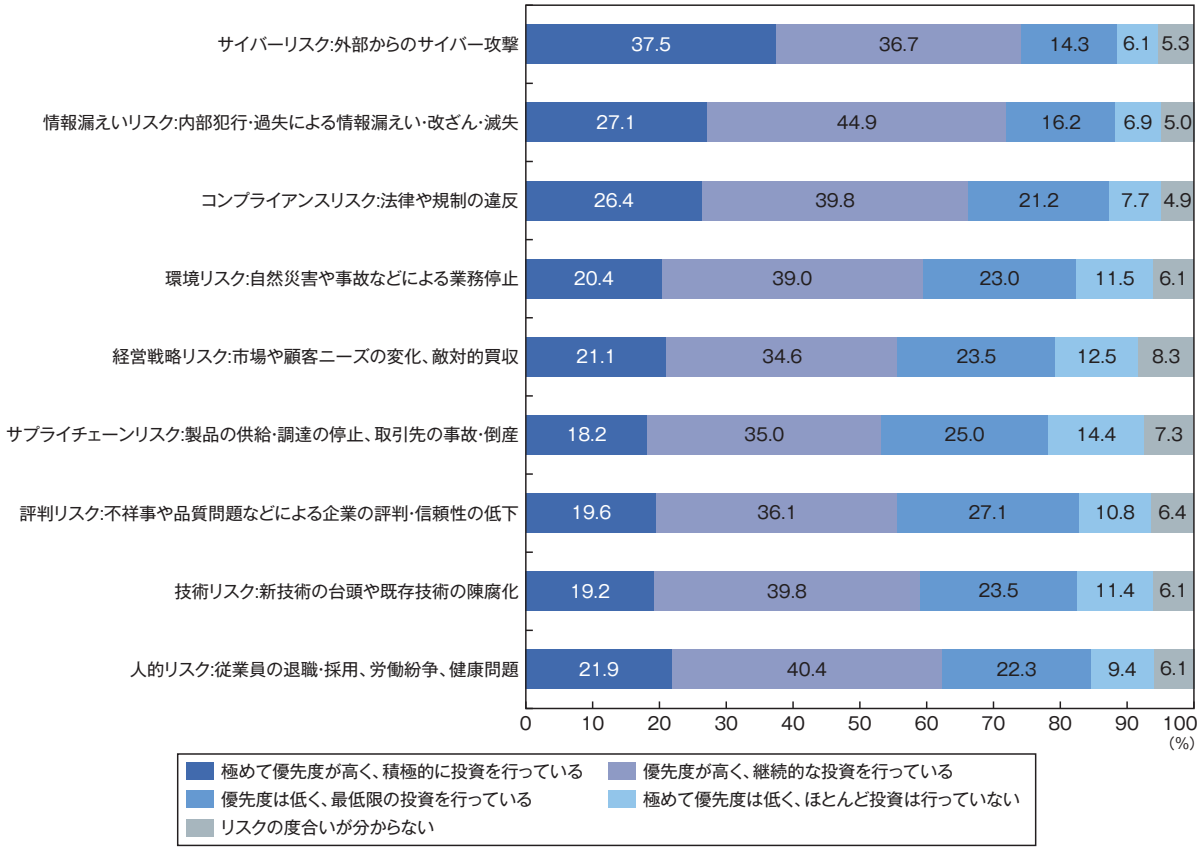


図20　ランサムウェアの感染被害の経験：従業員規模別

経営リスクにおけるセキュリティ対策の投資優先度

企業を経営していく上で、さまざまなリスクが存在する。その中で、セキュリティリスクへの対策はどのくらい優先されているのだろうか。そこで、経営に関するリスクを10項目示し、それらに対する対策への投資の優先度について質問を行った（図21）。その結果、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」への対策が最も優先して投資が行われていることが分かった。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。また、内部の不正や過失による「情報漏えいリスク」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・外部双方のセキュリティリスクへの対策の投資優先度が高まってる状況にあることが、調査結果から示された。



(N=983)

図21　経営リスクにおけるセキュリティ対策の投資優先度

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22）。現状では「マルウェア対策ツール」、「ファイアウォール（NGFW、UTM含む）」、「不正検知・侵入防止システム（IDS／IPS）」のような従来の境界防御型セキュリティ対策ツールの導入が多い。導入の計画・予定があるものとしては、「EDR／NGAV（次世代マルウェア対策ツール）」が最も多くなっている。EDRは、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、それを機械学習やAIによって分析することで、未知のマルウェアやサイバー攻撃を検知し、対処や回復を行うことができる、次世代型のマルウェア対策ツールとして注目されている。また、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も見られる。

ゼロトラストセキュリティを実現するためのツールとして期待されている「SASE／CASB／SWG／ZTNA」や「CSPM／CWPP／CNAPP」については、現状ではまだ導入率が低いが、導入の計画・予定がある企業も出てきており、これから徐々に導入が進んでいくものと見られる。

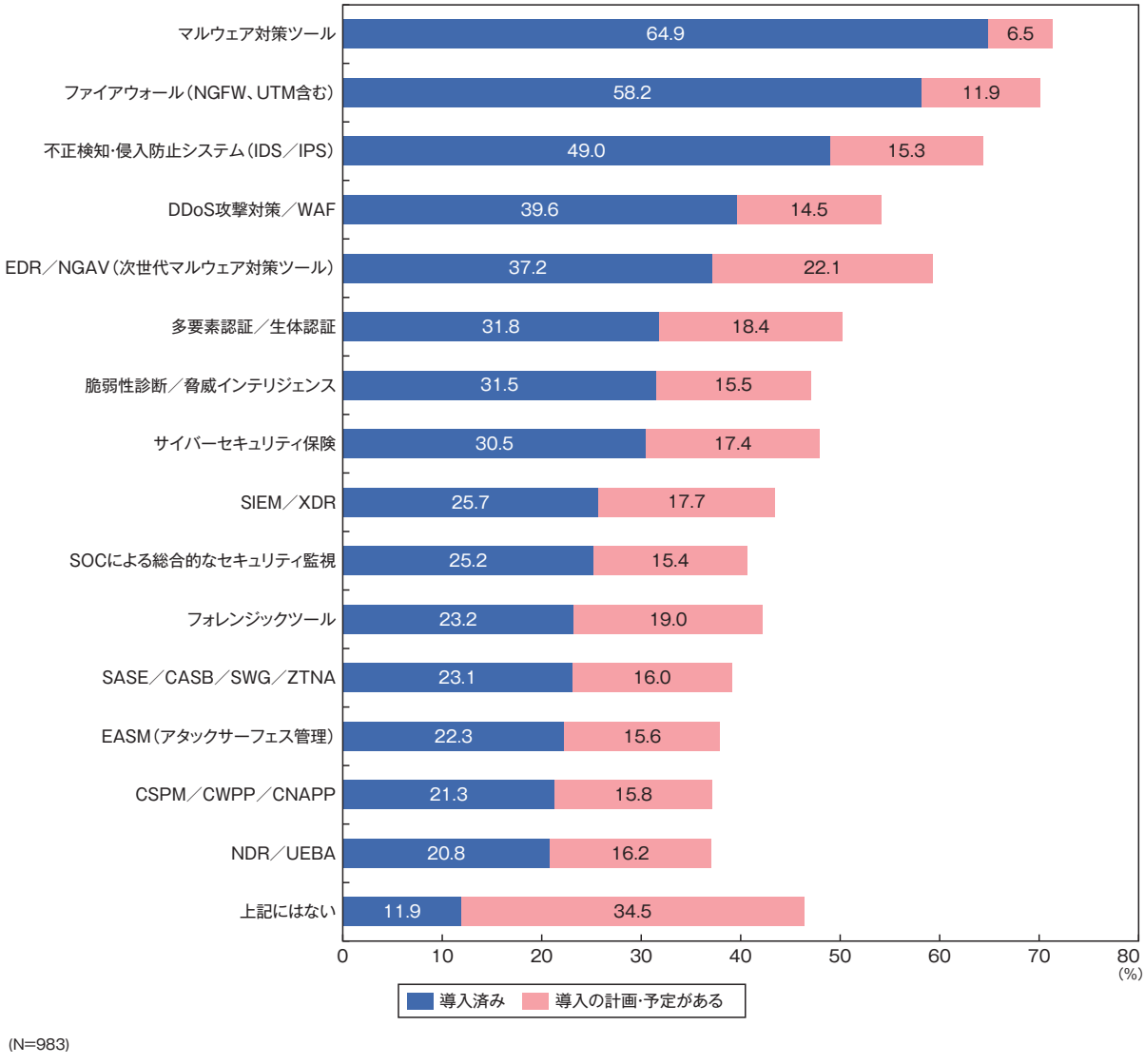


図22　外部からのサイバー攻撃対策として導入しているセキュリティツール・サービス

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としてはどのようなことが実施されているのだろうか（図23）。「重要情報」の取り扱いでは、「「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」を実施予定とする企業が増えつつある。内部不正による重要情報の持ち出しに備え、対策の厳重化が企業に求められるようになっている。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、実施計画・予定とする企業の割合は最も高い。クラウドサービスの利用やリモートワークの拡大に伴い、IDaaSなどによる多要素認証のニーズが高まっていると考えられる。

その他、「電子メールの誤送信対策」と「外部向け電子メールと添付ファイルのフィルタリング」は実施計画・予定とする企業の割合が比較的高くなっている。電子メールからの情報漏えいリスクは依然として高く、メールセキュリティ対策は重要である。その一方で、「社員向けセキュリティ教育・研修の実施」は実施率が半数以下となっており、国内企業におけるセキュリティ意識の甘さが露呈している。

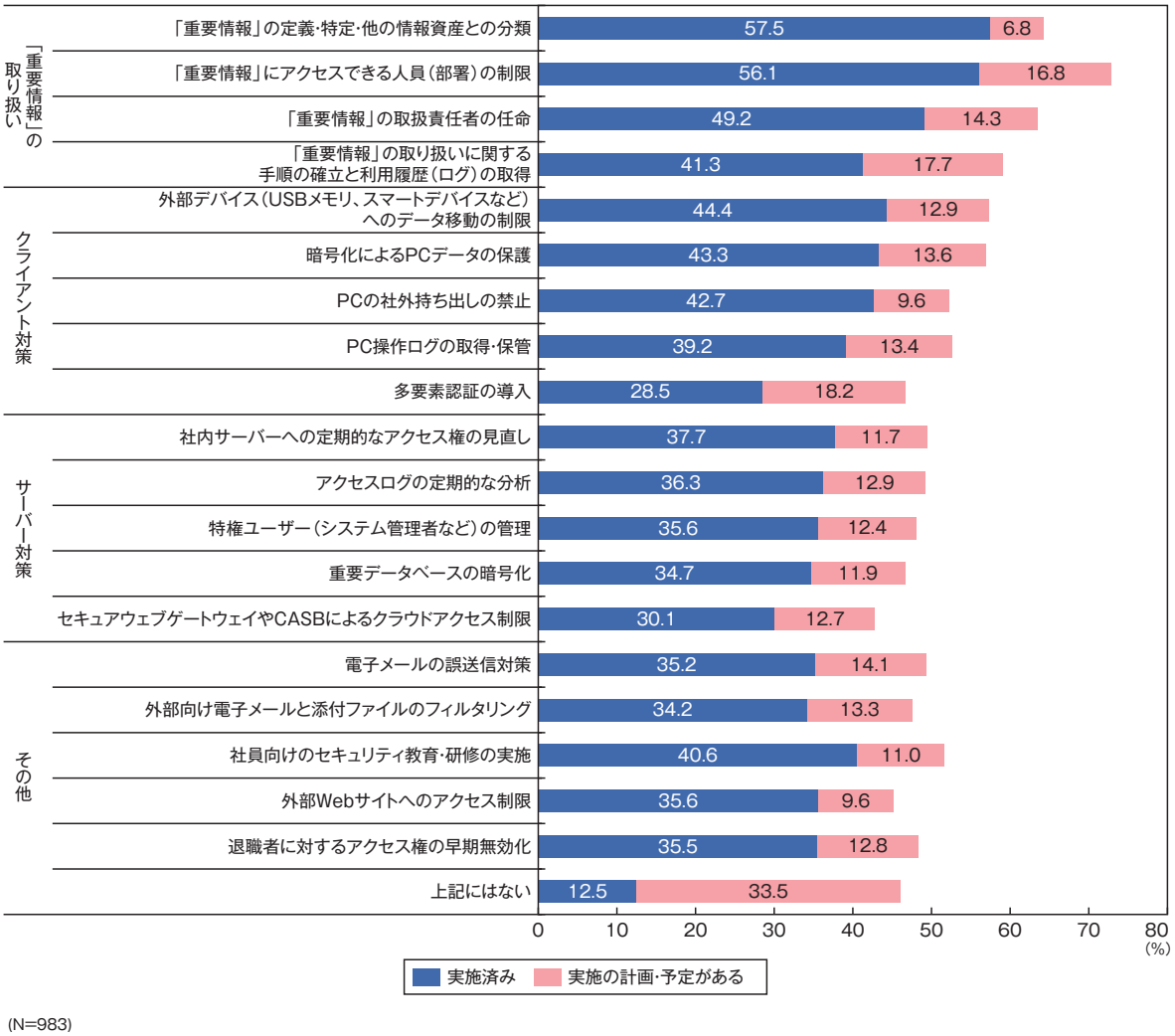
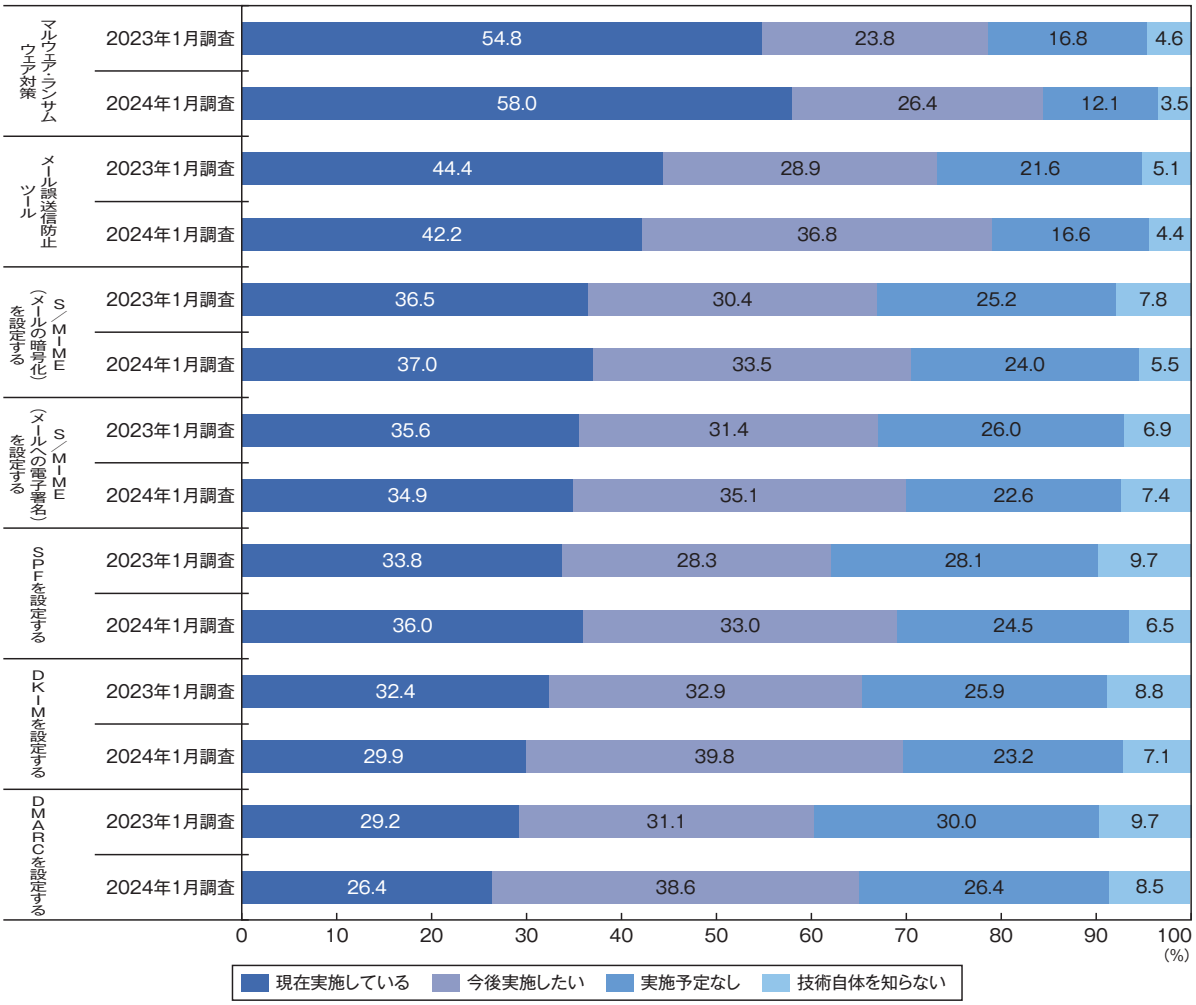


図23　内部からの情報漏えい対策として実施している項目

電子メール向けセキュリティ対策の実施状況

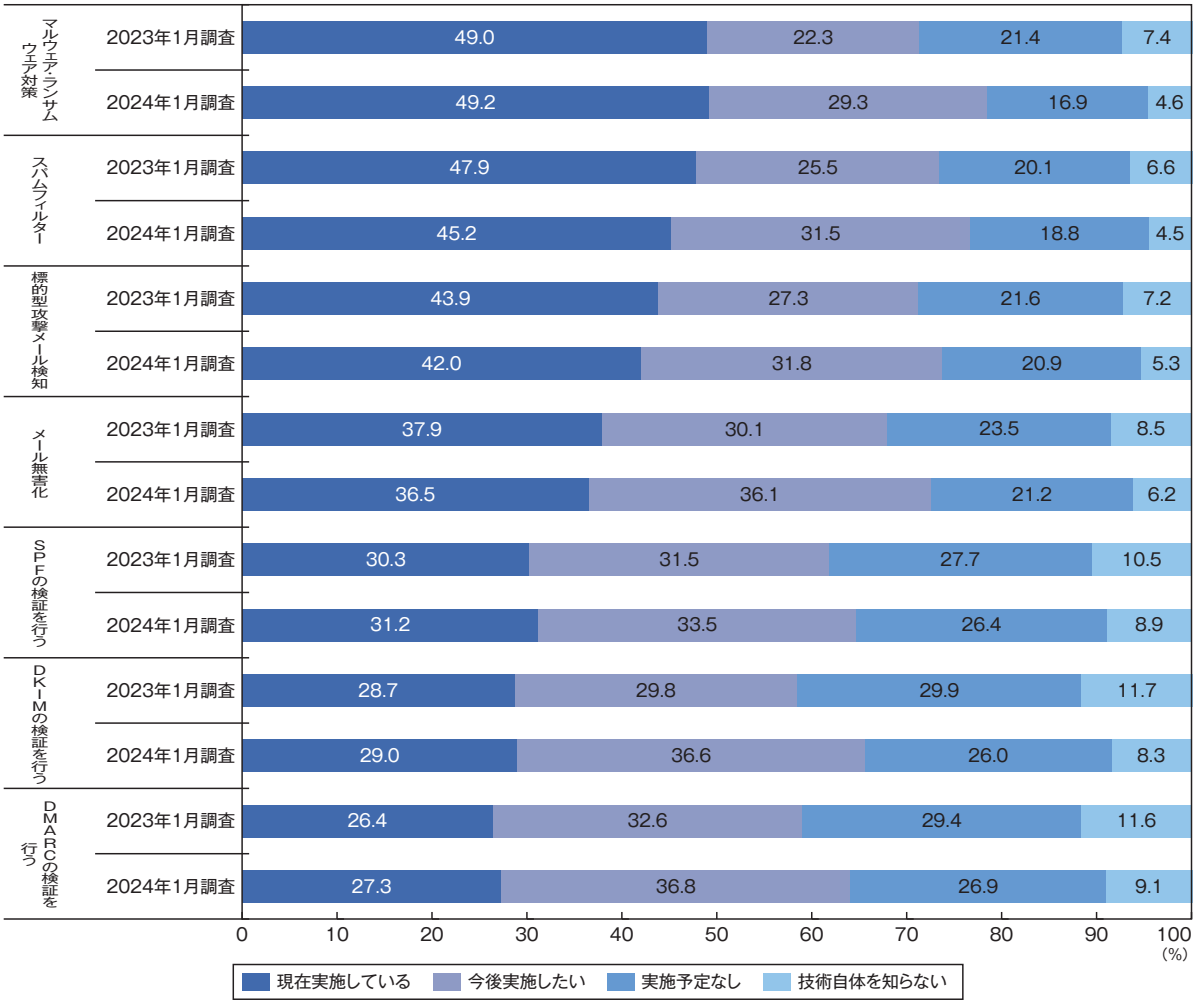
では、電子メール向けのセキュリティ対策はどのような状況になっているのだろうか。まず送信者としての対策状況を見てみる（図24）。「マルウェア・ランサムウェア対策」の実施率が58.0%で最も高く、前回調査よりも上昇している。「メール誤送信防止ツール」が42.2%、「S/MIME（メールの暗号化）を設定する」が37.0%で続いている。なりすましメール対策として期待されているメール認証の仕組みである「SPFを設定する」、「DKIMを設定する」、「DMARCを設定する」については、「SPF」は前回調査から実施率が上昇している。「DKIM」と「DMARC」は今後実施したいという割合が前回調査よりも大きく上昇している。2023年10月に、Google社がGmailに対してこれらのメール認証に対応するよう新たなガイドラインを発表したこともあり、今後、メール認証に対応する企業が増えていくと見られる。



2023年1月調査（N=907）
2024年1月調査（N=983）

図24　電子メールのセキュリティ対策の実施状況：送信者としての対策

次に、受信者としての対策状況を見てみる（図25）。ランサムウェアによる攻撃を想定してか、「マルウェア・ランサムウェア対策」、「スパムフィルター」、「標的型攻撃メール検知」、「メール無害化」について、今後実施したいという企業の割合が増えている。さらに、メール認証の「SPF」、「DKIM」、「DMARC」も同じく今後実施したいという企業が増えている。



2023年1月調査（N=907）
2024年1月調査（N=983）

図25　電子メールのセキュリティ対策の実施状況：受信者としての対策

PPAPの利用状況

近年、取引先とファイルを共有する際、PPAP（暗号化されたZIPファイルをメールで添付して送り、同じ経路で解凍パスワードを送る手法）を使用することによるリスクが指摘されている。2020年11月には、当時のデジタル改革担当大臣が政府でのPPAP廃止の方針を発表している。では、企業におけるPPAPの利用状況はどのようになっているのだろうか（図26）。「利用している（PPAPのみ利用）」が27.1%となり、前回調査とあまり変わっていない。「今は利用しているが、他の手段の導入を検討中であり、いずれ禁止する予定である」が29.1%となり、これも前回調査からはそれほど変化は見られない。「利用は禁止していないが、他の方法での送信を推奨している」は前回調査からやや減少している。前回調査から、PPAPを利用している企業の割合はほとんど変わっていない状況にある。

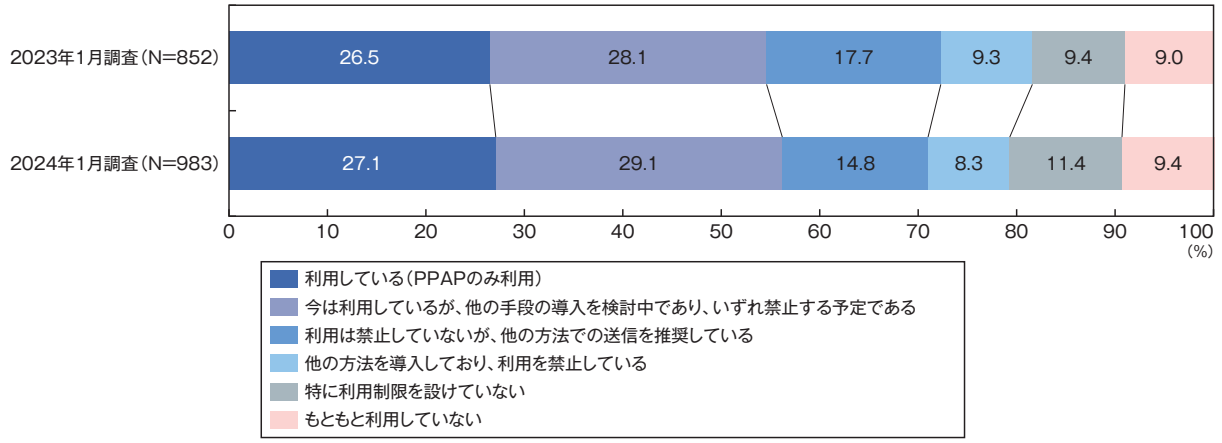


図26　PPAPの実施状況

PPAP以外で採用しているファイル送付の手段について質問を行った（図27）。ここでは、今後採用する予定の手段も含めて回答しているが、「クラウドストレージサービス」の採用が最も多く52.4%となった。それに、「ファイル転送サービス」と「IRMツール（添付ファイルを暗号化しアクセス権限を制御するツール）」が続いている。

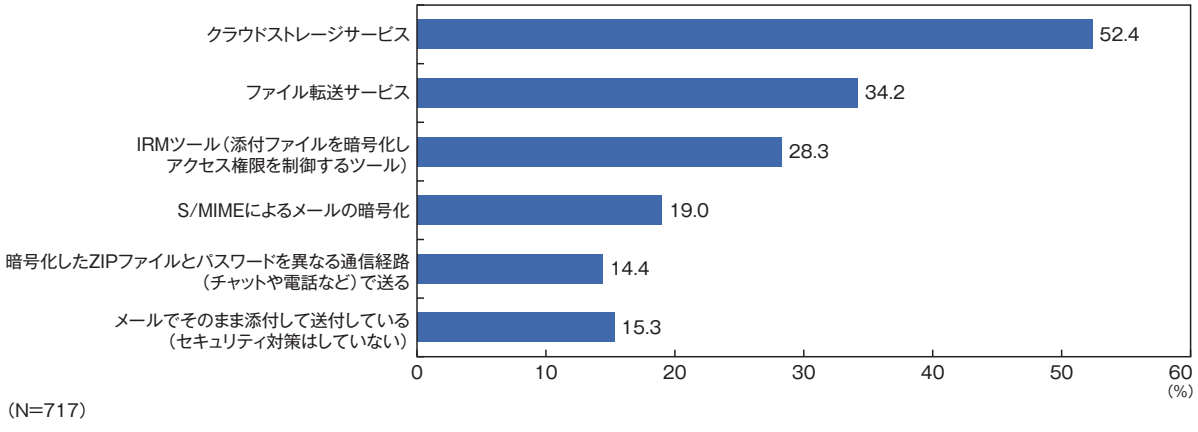
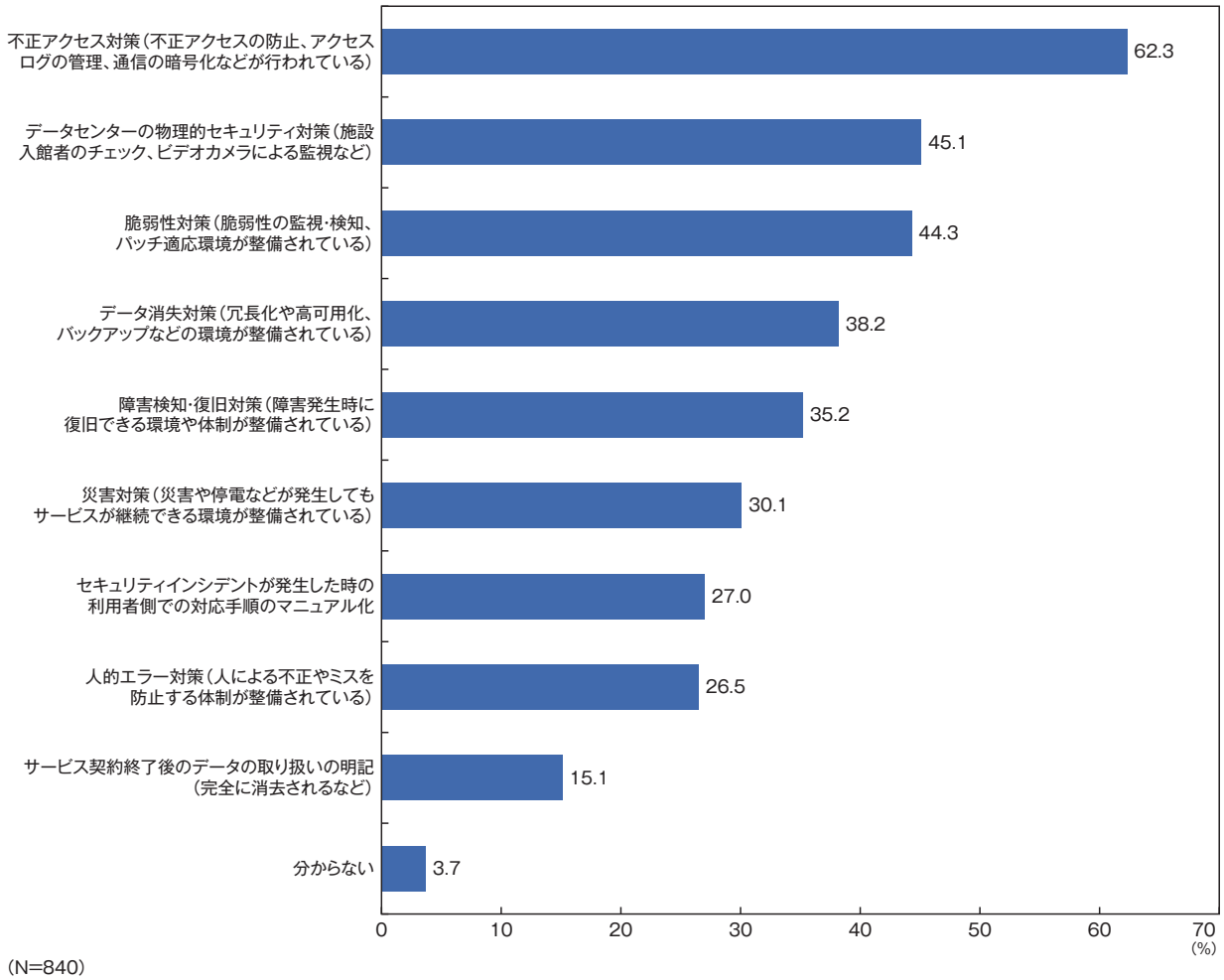


図27　PPAP以外で採用している（採用を予定している）ファイル送付の手段

クラウドサービスの選定で重視する事業者のセキュリティ対策

クラウドサービスの利用が拡大している。企業がクラウドサービスを選定する際、サービス事業者のどのようなセキュリティ対策・体制を重視しているのだろうか（図28）。「不正アクセス対策（不正アクセスの防止、アクセスログの管理、通信の暗号化などが行われている）」が62.3%と非常に多く、クラウドサービスのアクセスや通信に対するセキュリティ対策が選定時に最も重視されている。次に「データセンターの物理的セキュリティ対策（施設入館者のチェック、ビデオカメラによる監視など）」が２番目に多く、データセンターへの入館管理や室内の監視など物理的なセキュリティ対策も重視されている。その他、「脆弱性対策（脆弱性の監視・検知、パッチ適応環境が整備されている）」や「データ消失対策（冗長化や高可用化、バックアップなどの環境が整備されている）」などがあがっている。



（N=840）

注：クラウドサービスを利用している回答者

図28　クラウドサービスを選定する際、重視するサービス事業者のセキュリティ対策・体制

調査結果の考察

本章では、セキュリティインシデントとその対策の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．**セキュリティ脅威は常に身近に潜んでいる**：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えい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。経営者やIT・セキュリティの責任者は、セキュリティの脅威は常に身近に潜んでいると認識しておく必要がある。

2．**セキュリティへの継続的な投資が必要となる**：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、経営者は優先してセキュリティ対策への投資を行い、さらにそれを継続的に行っていかなければならない。

3．**ゼロトラストセキュリティを実現していく**：アンチウイルスやファイアウォールなどによる従来の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。次世代型のセキュリティ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。

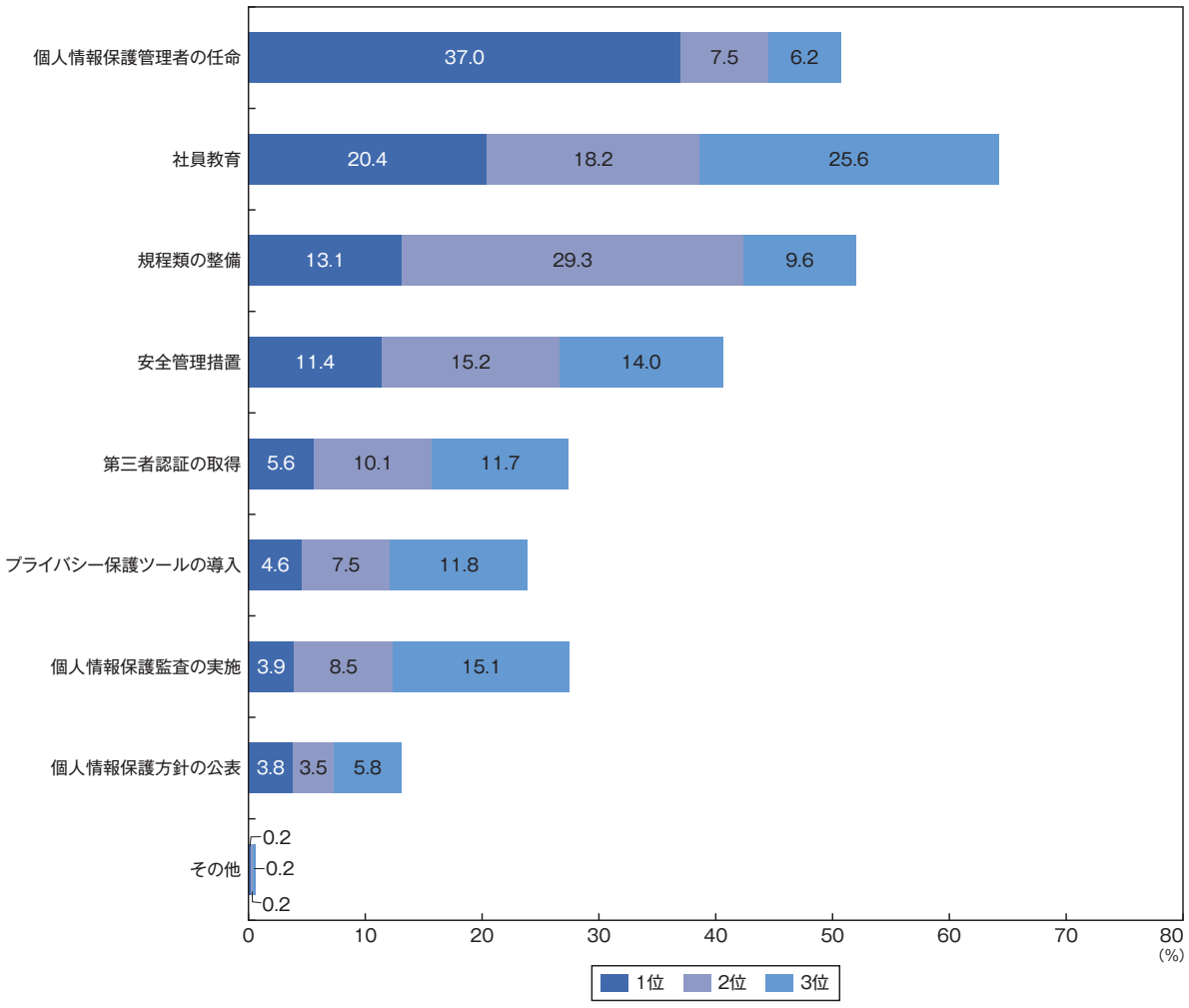
4．**多様な働き方を実現するための情報漏えい対策が必要となる**：情報漏えい対策も引き続き重要な投資領域である。クラウドサービスやテレワークの利用が拡大した今、多要素認証やCASBなどアクセス時のセキュリティ対策は重要であるが、まだ普及には至っていない状況にある。安全で多様な働き方を推進するためにも、早急な対応が必要である。

4　プライバシー保護に対する取り組み

本章では、プライバシー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。個人情報保護法やデータの越境移転のような法規制への対応に加え、企業の信頼性や価値を高めるために、プライバシーガバナンスにも取り組むことが求められるようになっている。

個人情報保護において注力している取り組み

個人情報保護で特に注力している取り組みについて質問を行った（図29）。ここでは、特に注力している取り組みについて、１位～３位までを順位付けして回答している。「個人情報保護管理者の任命」を１位にした企業が37.0%と最も高い。２位の回答が最も多いのが「規程類の整備」となっている。管理者の任命を行い、その次に社内規程の策定を行うという流れが見て取れる。「社員教育」は、１位、２位、３位と満遍なく回答率が高く、おしなべて取り組まれている項目となっている。

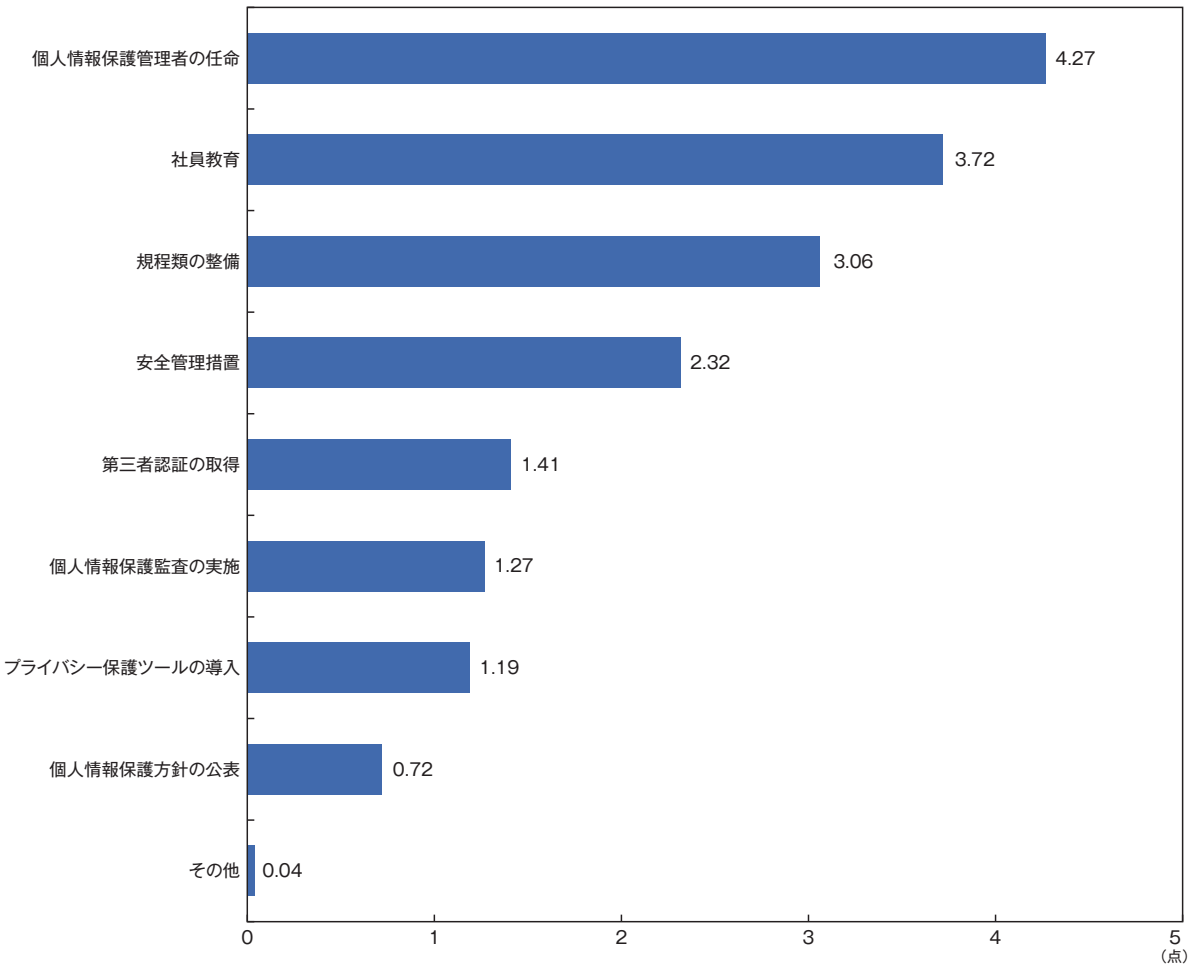


(N=983)

注：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

図29　個人情報保護において注力している取り組み：順位付け

ここではさらに、１位の回答を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た（図30）。「個人情報保護管理者の任命」、「社員教育」、「規程類の整備」の次に、「安全管理措置」と「第三者認証の取得」が続いている。



(N=983)

注：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

図30　個人情報保護において注力している取り組み：順位付け

改正個人情報保護法の対応における問題点

2022年4月に施行された改正個人情報保護法に対応していく中で生じている問題について質問を行った（図31）。ここでは企業の個人情報保有件数別に分析を行っている。全体では「改正された事項に対応するための予算が確保できない」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。次に「法改正に対応した社内の運用体制が整備できていない」が多く、特に保有件数１千～10万件未満での回答率が高い。この保有件数の規模を持つ企業は、「特に問題はない」の回答率が低く、対応すべき問題が多いと見られる。保有件数１万件以上では、「法改正による変更点が抽出・整理できていない」と「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」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%
社内規程の見直し・更新ができていない	19.9%	17.2%	15.9%	23.1%	23.7%	22.0%	15.9%
情報漏えい時の報告・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%

図31　改正個人情報保護法の対応における問題：個人情報保有件数別

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32）。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・地域で規制を設けるなどの対応が行われている。ここでは企業の海外売上比率別に分析を行っている。全体では、現在データの越境移転を行っている企業は64.4%となった。そのうち「現在行っていて、今後さらに増えていく」と回答している企業は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別に見ると、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」という割合も高まる傾向にある。特に、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%以上となっており、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。

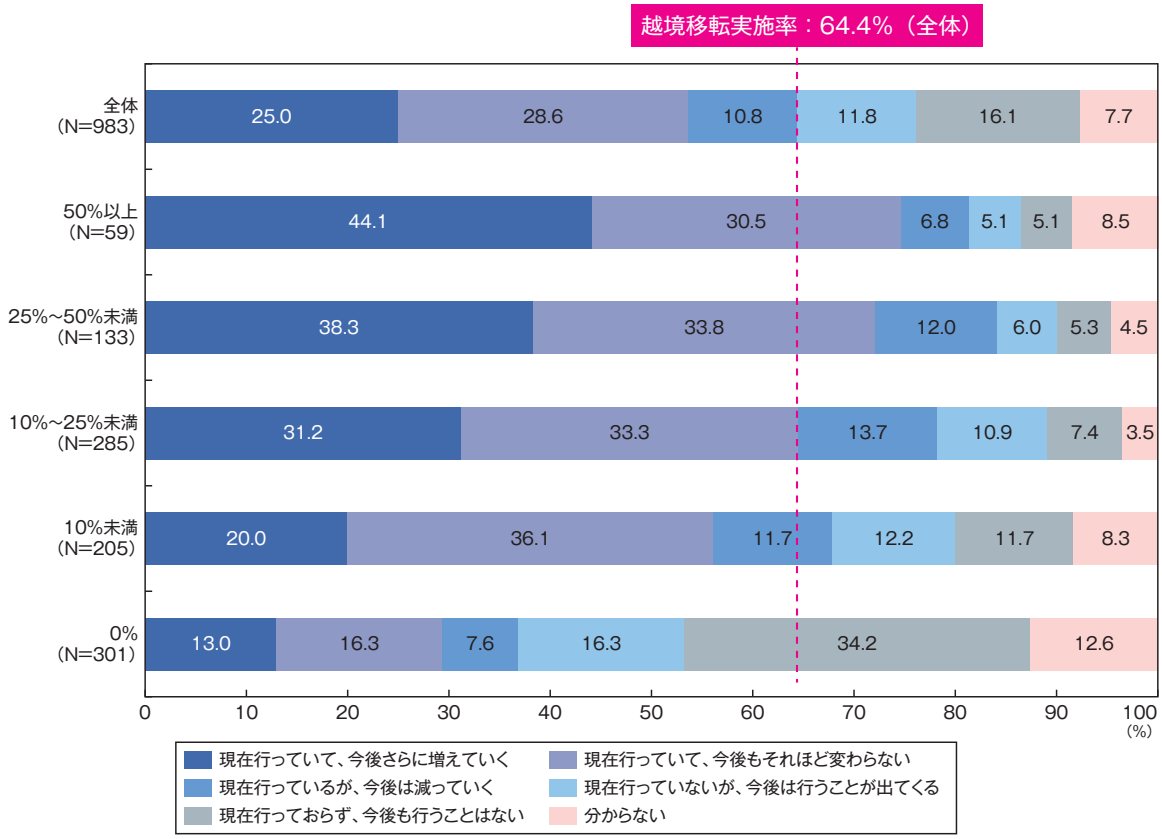


図32　データの越境移転の状況：海外売上比率別

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33）。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。今後の移転先としては、「アジア太平洋地域（中国除く）」と「中国」がさらに増えていくと見られる。

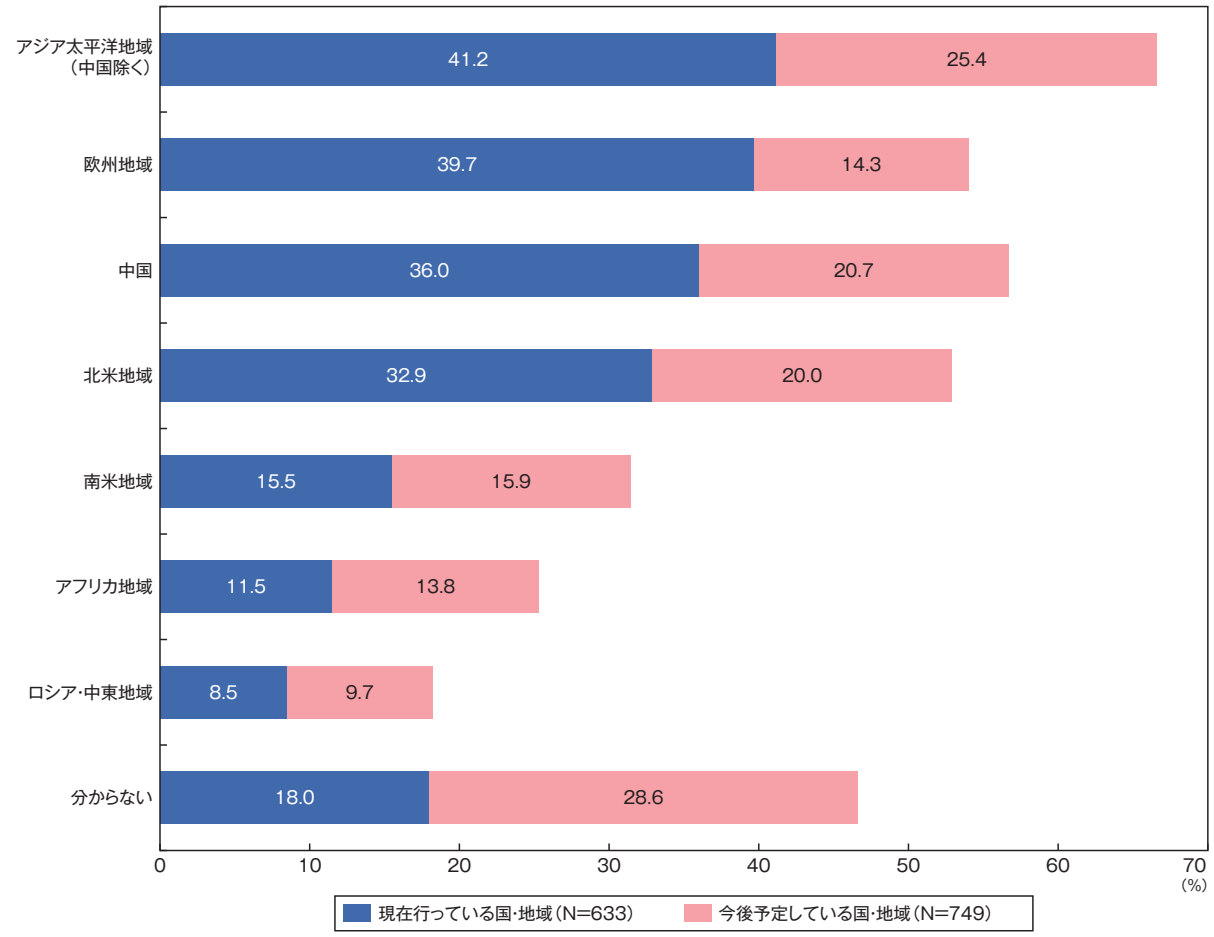
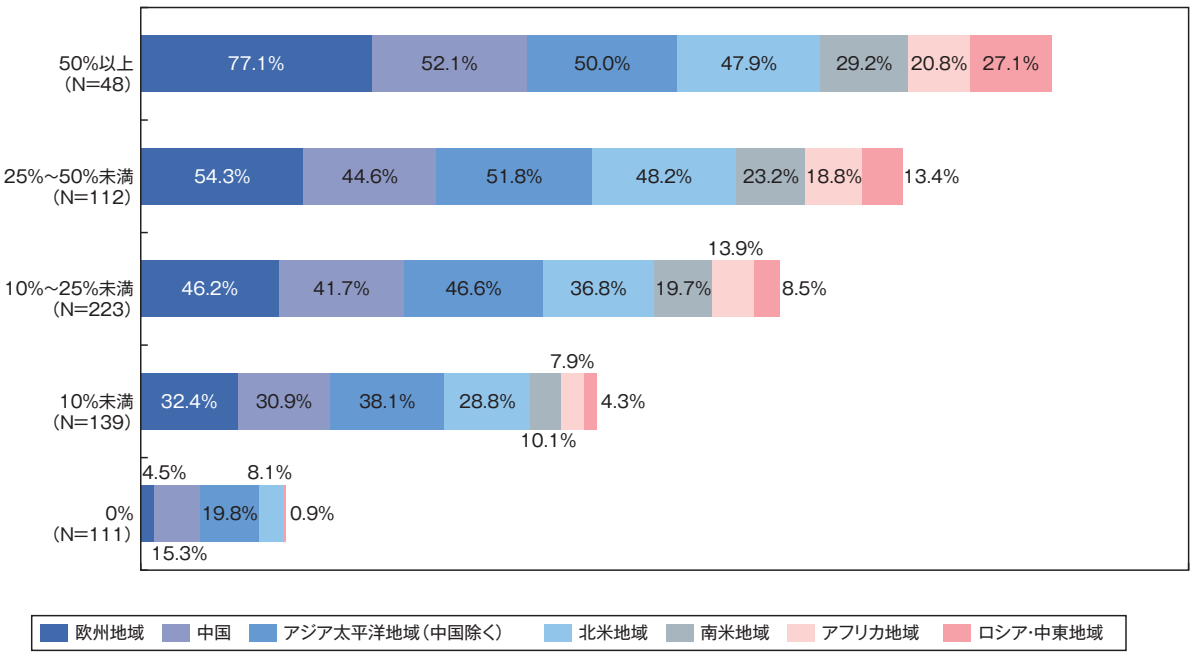


図33　データの越境移転先

次に、現在のデータ越境移転先を海外売上比率別に見てみる（図34）。海外売上比率50%以上の企業では、欧州が77.1%と非常に多いことが特徴として見られる。



注：現在データ越境移転を行っている国・地域について回答していない者を除く

図34　データの越境移転先：海外売上比率別

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のだろうか（図35）。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」が最も多く、データの越境移転の状況に関わらず共通した課題となっている。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」が続いている。特に越境移転が今後減っていく企業で多くなっており、越境移転に消極的な理由の一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62.6%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。

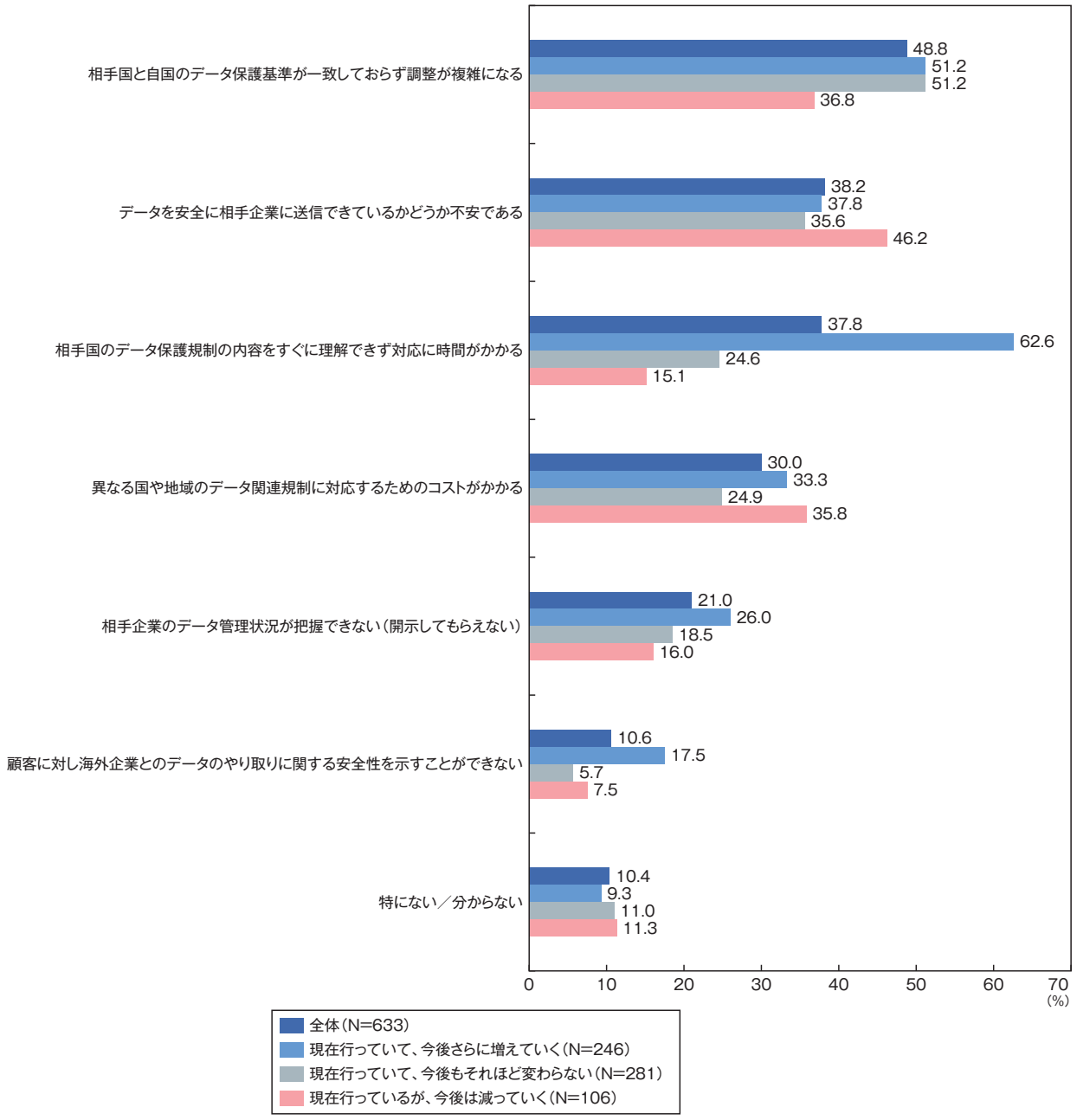


図35　海外企業とのデータのやり取りにおいて生じている課題

プライバシーガバナンスに関する取り組み状況

近年、組織経営において、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36）。全体では「組織全体のプライバシー保護に関する責任者を任命している」が最も多く、「プライバシーガバナンスについての組織の姿勢が明文化されている」が続き、それぞれ３分の１の企業が取り組んでる。それに、「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」と「プライバシー保護のための組織を設置している」が30%以上で続いている。

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100万件以上の保有企業では、「自社の取り組みについて、対外的に分かりやすく開示している」や「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」など、対外的な取り組みも見られるようになっている。

	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)	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、対外的に分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%

図36　プライバシーガバナンスに関する取り組み状況：個人情報保有件数別

プライバシーガバナンスにおける課題

プライバシーガバナンスに取り組んでいく上での課題はどのようなものがあるのだろうか（図37）。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見られる。また、「経営層が十分に重要性を認識していない」も主要課題の一つに含まれる。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見られる。一方、保有件数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%がプライバシーガバナンスに対する課題意識はなく、着実に対応している企業が多いと見られる。

	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%

図37　プライバシーガバナンスにおける課題：個人情報保有件数別

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．**改正個人情報保護法への対応課題は予算と運用体制となる**：2022年４月に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対応にも難しさが見られる。

2．**データの越境移転は拡大するも各国の規制の理解と調整が課題となる**：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見られる。その一方で、プライバシー保護に関する各国・地域の規制は厳格化され、それぞれで異なることから、取引相手国の規制の理解と調整がより複雑になっている。

3．**プライバシーガバナンスは責任者の任命と姿勢の明文化から取り組まれている**：経済産業省／総務省が提示するプライバシーガバナンスの取り組むべき三要素のうち、責任者の任命と姿勢の明文化への取り組みが行われている。そして、個人情報の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。

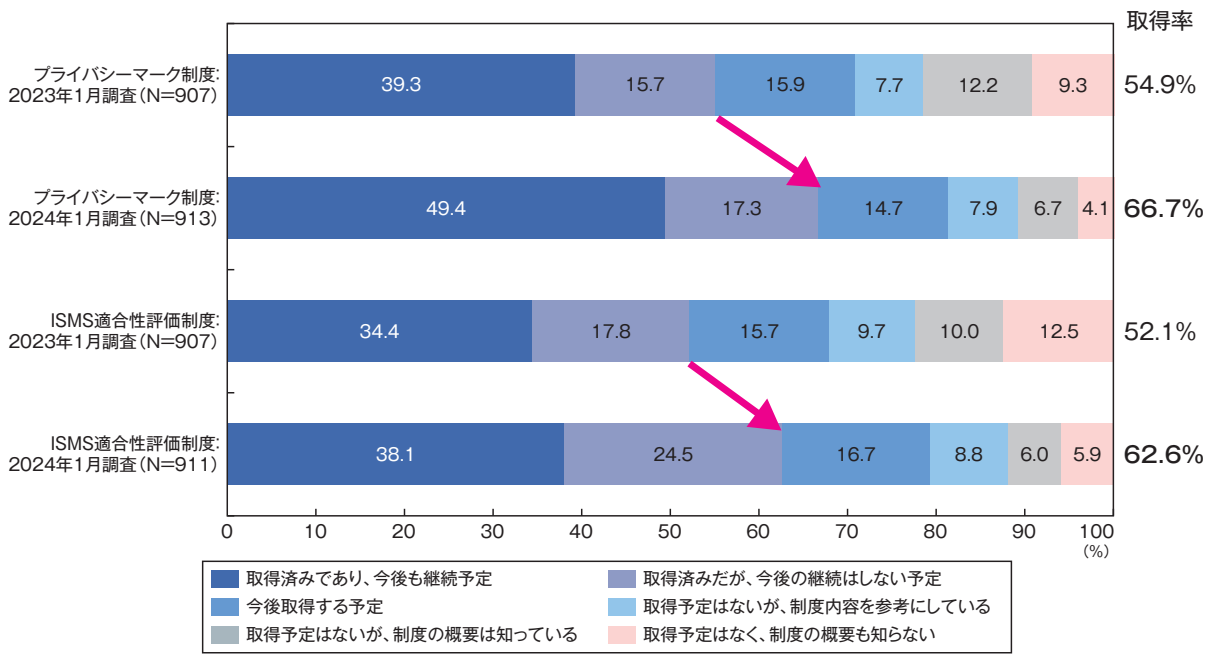
4．**プライバシーガバナンスの取り組みを公表し、企業価値と信頼性を高めていくことが重要となる**：プライバシーガバナンスへの取り組みは、企業内で取り組むだけではなく、データを扱う企業として消費者や取引先にも取り組みを公表することが重要である。それによって企業の価値と信頼性が高まっていき、ビジネスにおいても優位性が高まっていく。企業の経営者は、そのような認識を強く持つ必要がある。

5 第三者認証の取得状況

本章では、第三者機関による認証の取得状況、効果、事業者選定ポイントについて調査した結果を分析している。企業は顧客と取引先からの信頼性を高めるために、個人情報保護やセキュリティ対策を講じていることを対外的に示すことが重要になっており、客観的な立場による評価を得られる第三者機関の認証を取得する企業は増加している。

プライバシーマーク／ISMSの取得状況

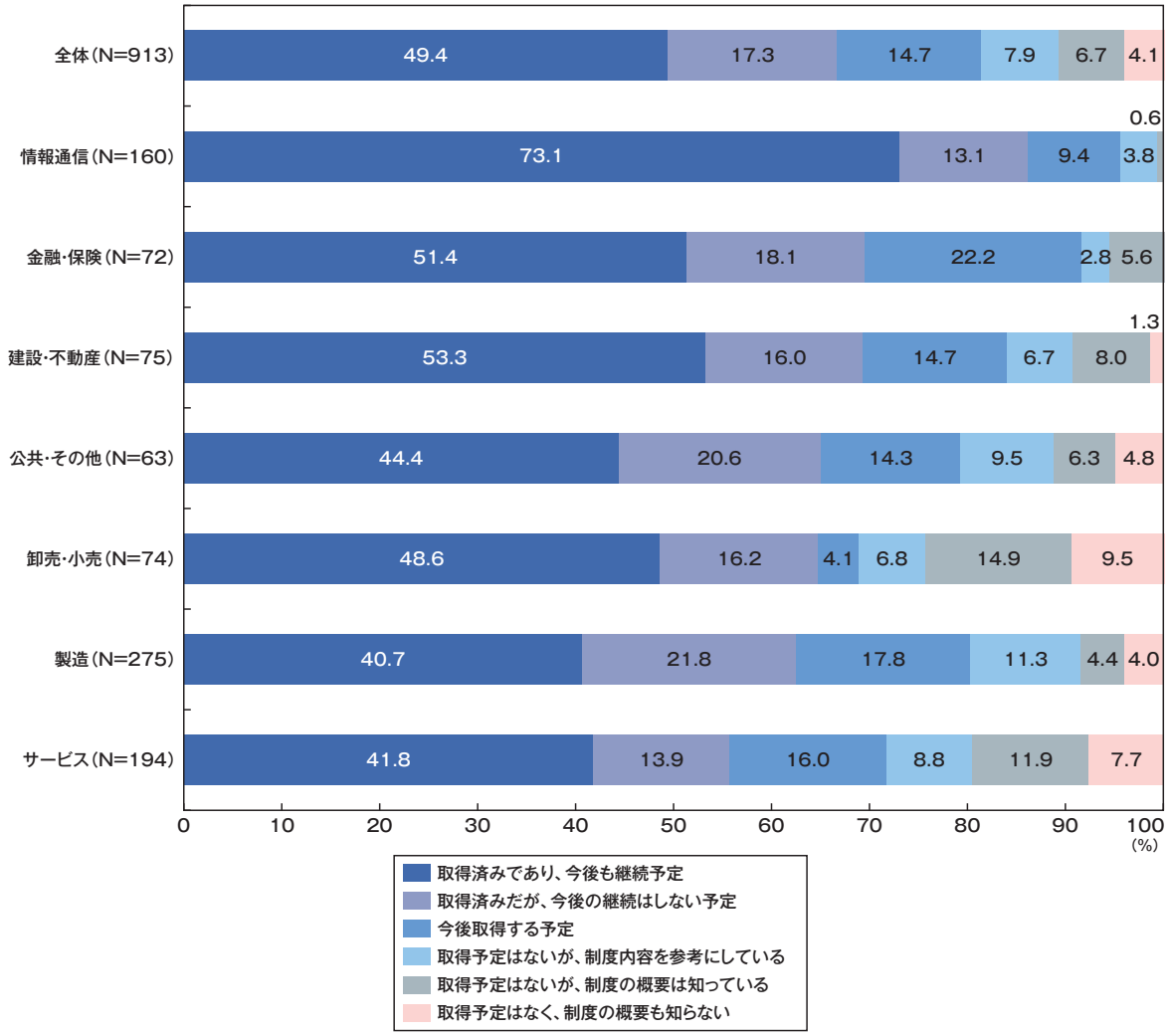
プライバシーマーク制度（以下、プライバシーマークという）とISMS適合性評価制度（以下、ISMSという）の認証取得状況について質問を行った（図38）。プライバシーマークの取得率は66.7%となり、前回調査から10ポイント以上も上昇している。特に「取得済みであり、今後も継続予定」が大きく上昇している。ISMSの取得率は62.6%となり、こちらも前回調査から10ポイント以上も上昇している。ただし、「取得済みだが、今後の継続はしない予定」が24.5%と前回調査から大きく上昇している。



注：「取得予定が分かる立場にない」の回答者は除いている

図38　プライバシーマーク／ISMSの取得状況

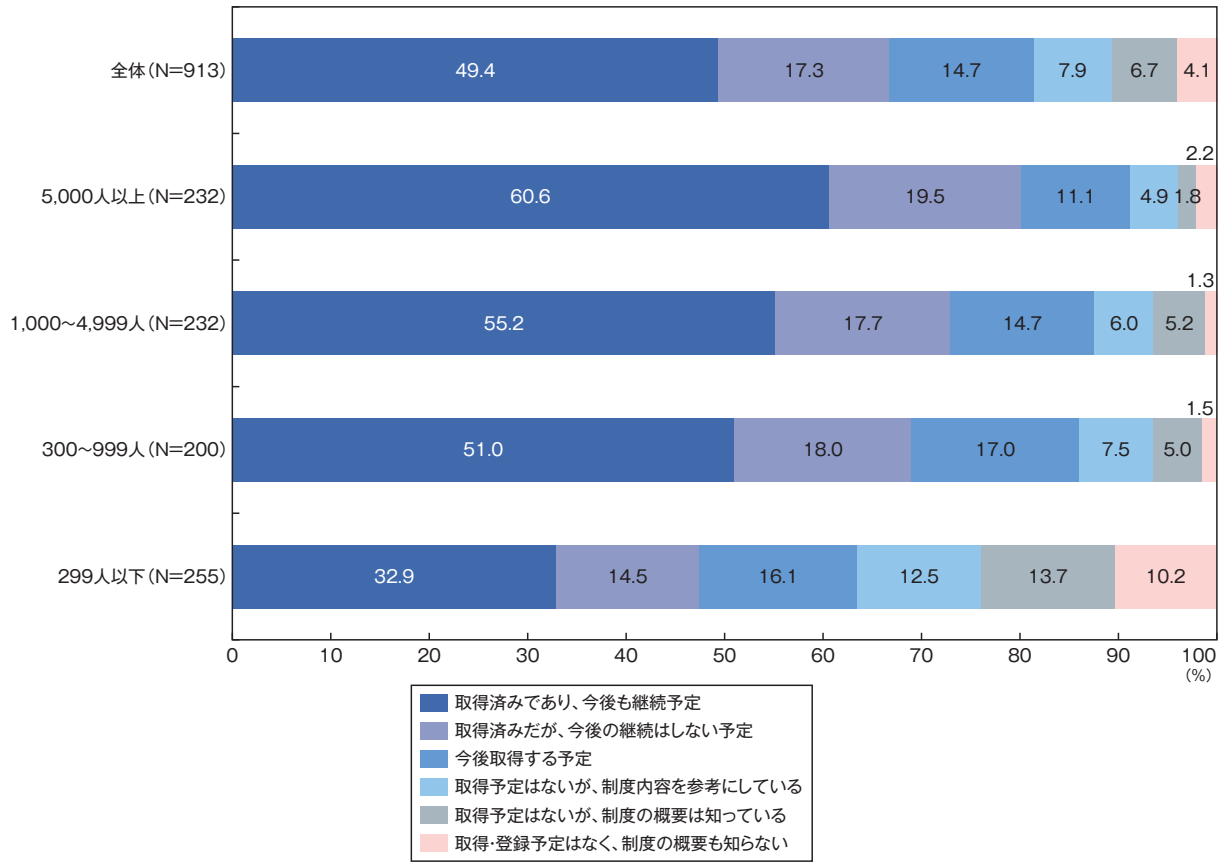
プライバシーマークの取得状況について業種別に見てみる（図39）。取得率が最も高いのは情報通信で85%を超えている。次に金融・保険と建設・不動産が続いている。取得率が最も低いのはサービスであった。



注：「取得予定が分かる立場にない」の回答者は除いている

図39　プライバシーマークの取得状況：業種別

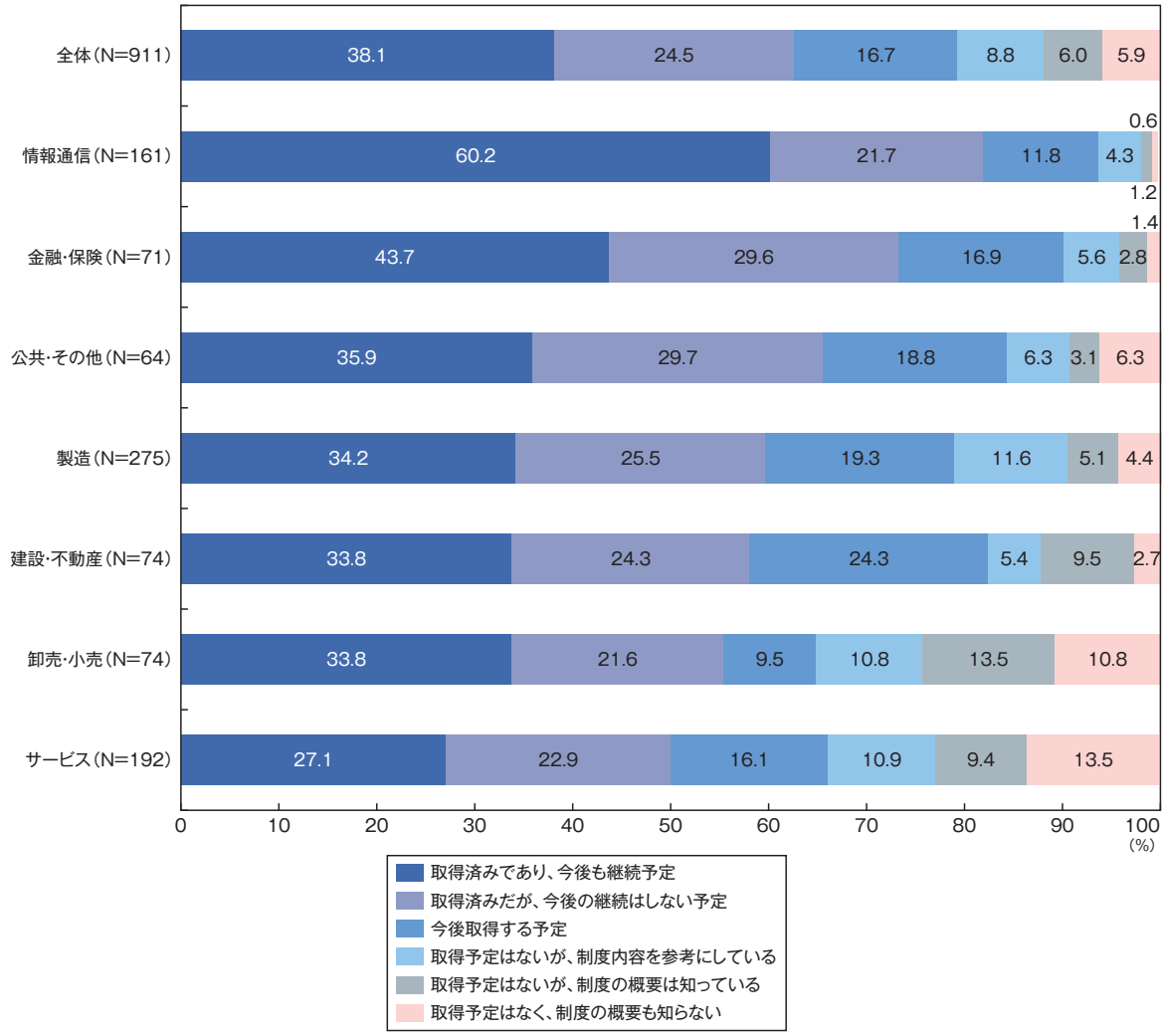
プライバシーマークの取得状況について従業員規模別に見てみる（図40）。従業員規模が大きくなるにしたがい取得率が高くなっていき、従業員5,000人以上では80%が取得している。一方、299人以下では取得率が50%に達していない状況にある。



注：「取得予定が分かる立場にない」の回答者は除いている

図40　プライバシーマークの取得状況：従業員規模別

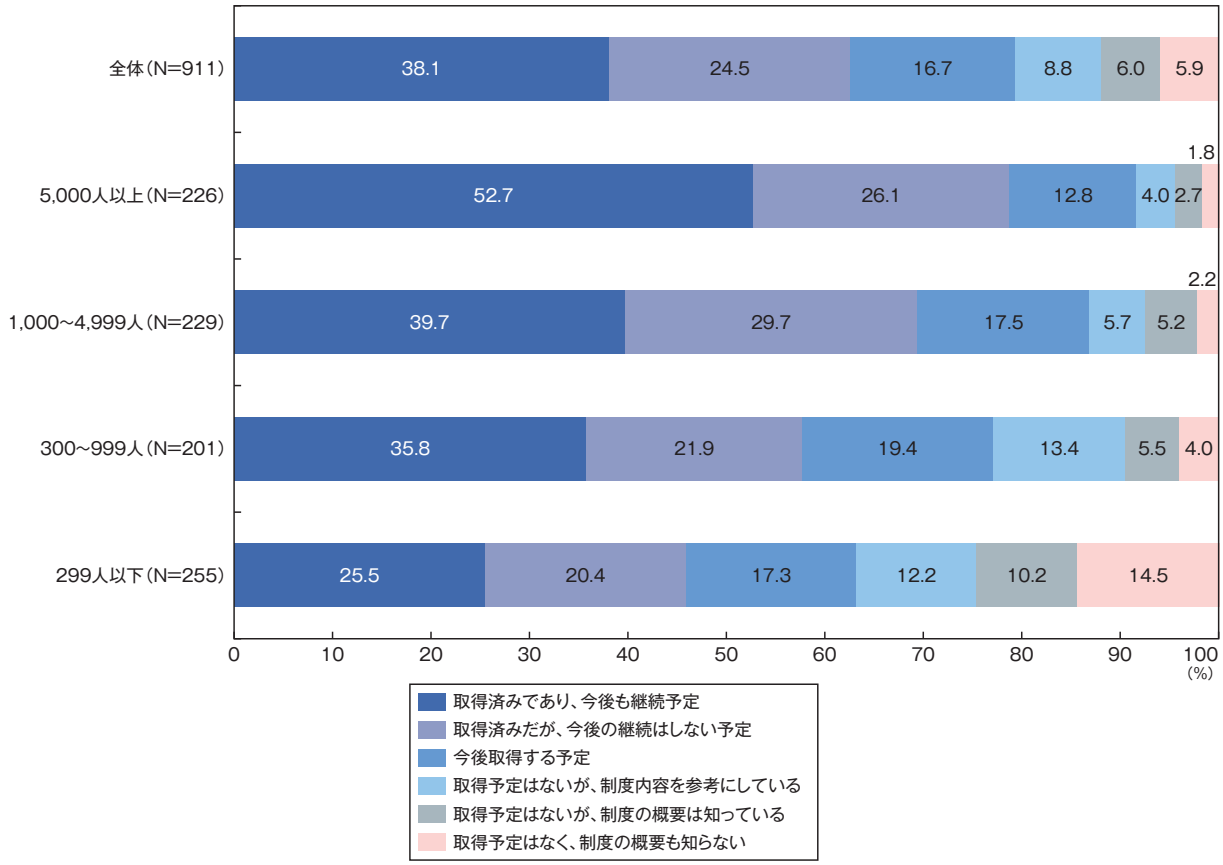
次にISMSの取得状況について業種別に見てみる（図41）。取得率が最も高いのは情報通信となり、80%を超えている。次に金融・保険が続く。「取得済みだが、今後継続しない予定」の割合が比較的大きいのは、「公共・その他」と「金融・保険」である。



注：「取得予定が分かる立場にない」の回答者は除いている

図41　ISMSの取得状況：業種別

ISMSの取得状況について従業員規模別に見てみる（図42）。従業員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。



注：「取得予定が分かる立場にない」の回答者は除いている

図42　ISMSの取得状況：従業員規模別

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とISMS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（図43）。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。その次に「消費者からの信頼性が向上した」となっており、ISMSの方がやや多い。

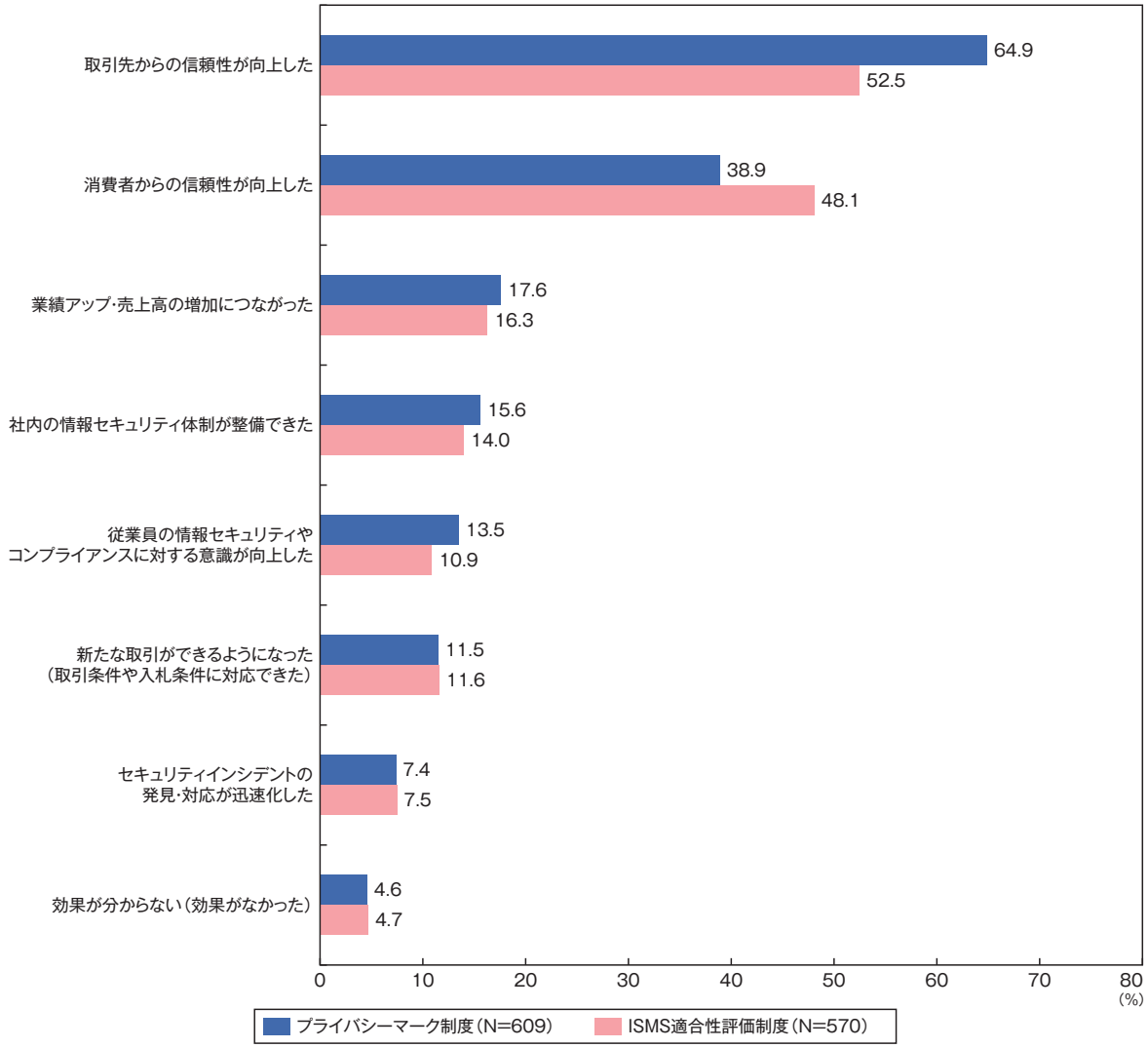


図43　プライバシーマーク／ISMSの取得による効果

プライバシーマーク／ISMSの継続・取得に消極的な理由

プライバシーマークの継続もしくは取得に消極的な理由について質問を行った（図44）。取得済みだが継続は予定しない企業は、「取得のための人員を確保できない」が64.6%と非常に多い。取得による効果は認められているものの、人員不足が継続の大きな障壁になっていることがうかがえる。取得予定がないが制度内容は参考にしている企業については、人員不足の他、「取得後の審査対応や情報管理などの業務負担が大きくなる」と「認証取得のコストがかかる」が主な理由としてあがっている。

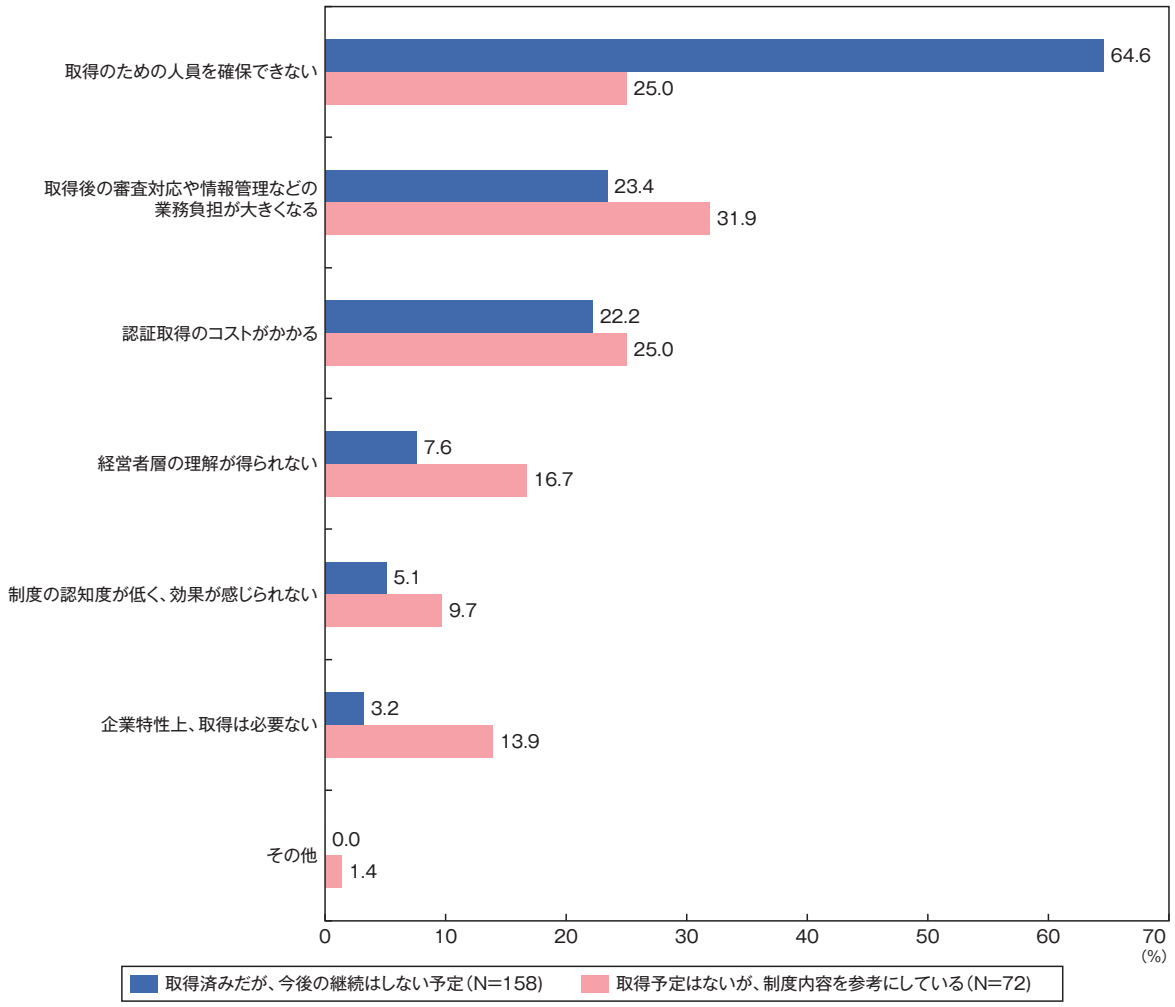


図44　プライバシーマークの継続・取得に消極的な理由

ISMSの継続もしくは取得に消極的な理由について質問を行った（図45）。取得済みだが継続予定がない企業は、「取得のための人員を確保できない」が45.8%で最も多く、「認証取得のコストがかかる」が次に続いている。ISMSでは、人員不足に加えて取得コスト負担が継続の大きな障壁になっていることがうかがえる。取得予定がないが制度内容は参考にしている企業については、人員不足とコストの他、「取得後の審査対応や情報管理などの業務負担が大きくなる」が主な理由としてあがっている。

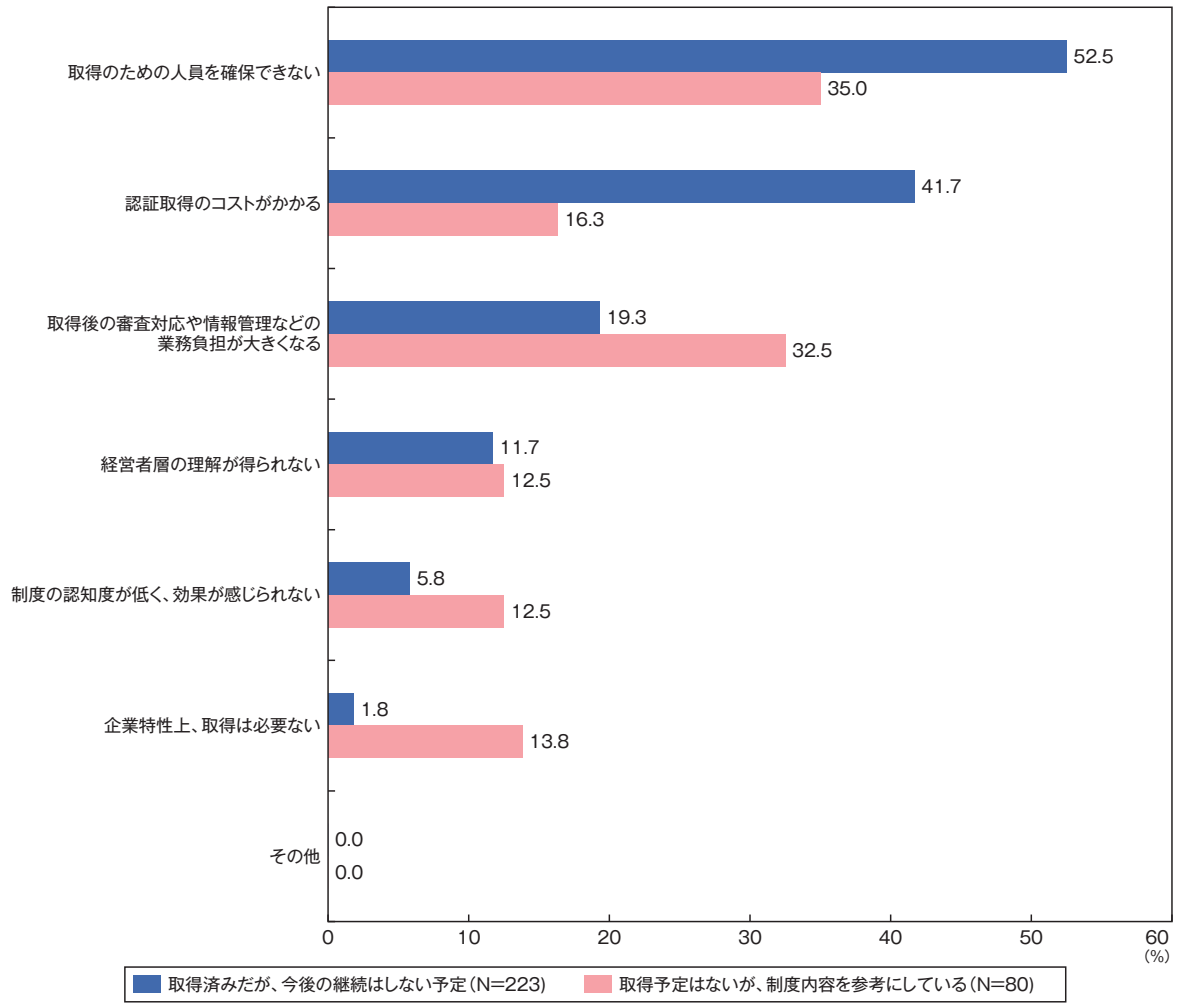


図45　ISMSの継続・取得に消極的な理由

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46）。「第三者機関の認証を取得していること（プライバシーマークやISMSなど）」が最も多く、業務委託事業者の選定において第三者認証の取得有無の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番目に多く、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ことが分かる。また、「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。

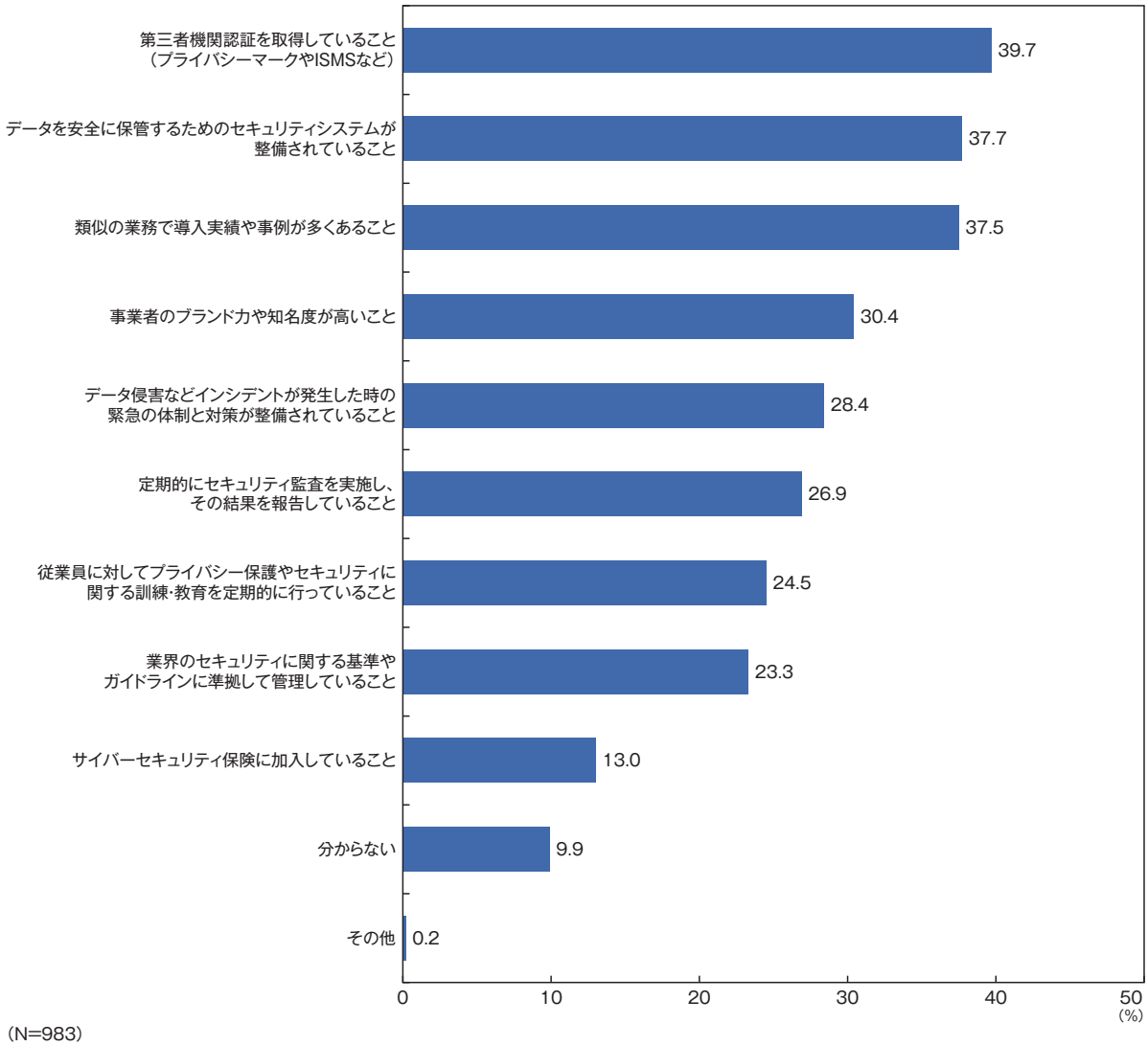


図46　機密情報を扱う業務の委託事業者の選定で重視する点

クラウドサービスの選定における第三者評価の重視度

クラウドサービスを選定する際、サービス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について、五つの評価制度について質問を行った（図47）。「プライバシーマーク」を非常に重視するが40.0%となり最も重視されている第三者評価になっている。それに「ISMSクラウドセキュリティ認証」と「ISMS認証」が続いている。

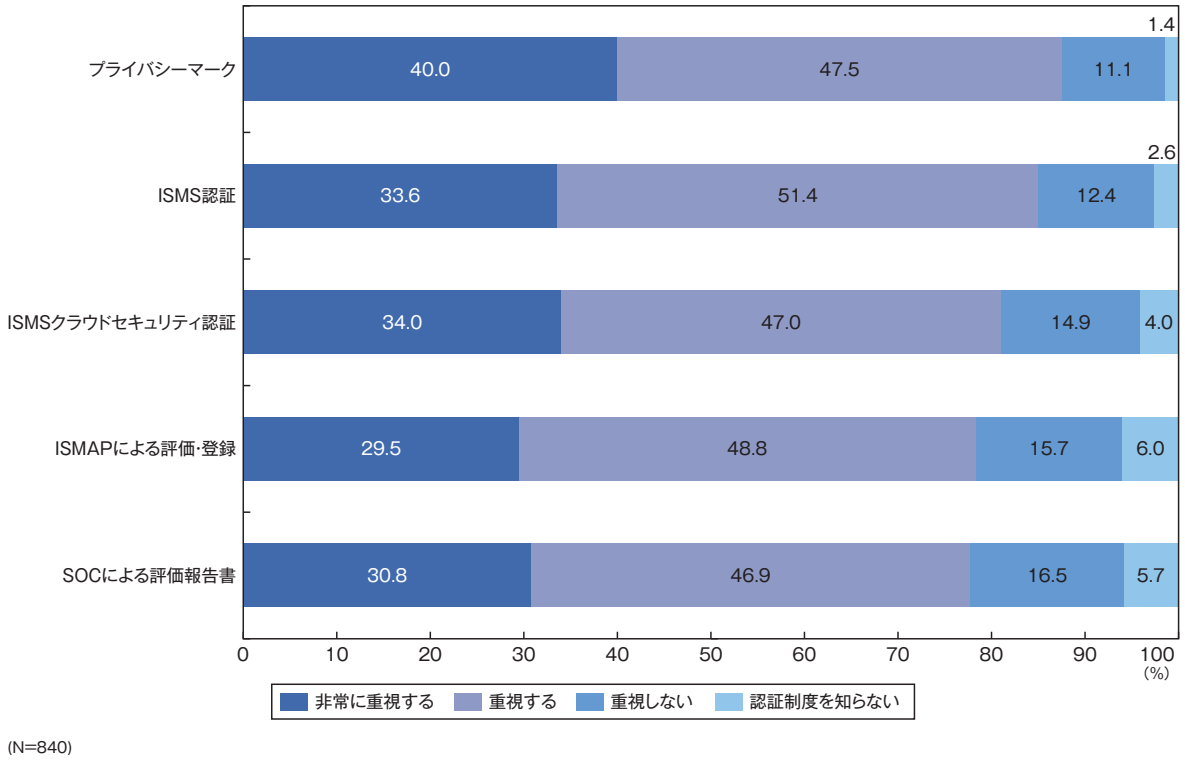


図47　クラウドサービスの選定における第三者評価の重視度

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／ISMSの取得率は上昇している**：プライバシーマーク、ISMSともに取得率が上昇している。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。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。

2．**取得効果は消費者や取引先からの信頼向上である**：プライバシーマークとISMSの取得による主な効果は、特に消費者や取引先からの信頼が向上したことと認識されている。一方、継続や取得に消極的な主な理由は、取得や運用に関する人員不足とコスト負担となっている。

3．**業務委託事業者の選定には第三者認証取得が重視されている**：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やISMSのような第三者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。

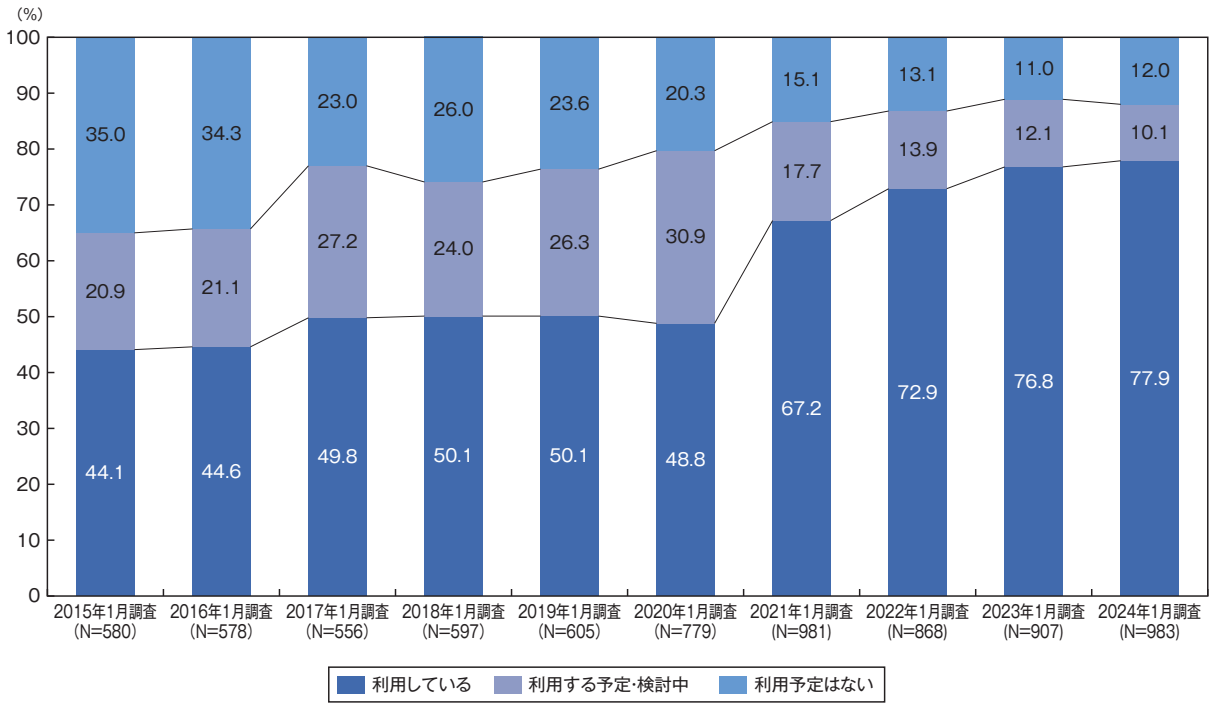
6 電子契約の利用状況

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。ここ数年、新型コロナウイルスの感染拡大が契機となり、電子契約の利用が拡大してきていたが、落ち着きが見られるようになった。利用による効果や電子契約サービスの選定で重視されている点についても分析を行っている。

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48）。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たことで、電子契約の需要が急速に高まり、2020年から2022年にかけて導入が拡大している。

2024年１月調査での最新の利用率は77.9%となり、2023年１月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、導入が一段落したと見ることができる。



注1：2020年以前は選択肢が異なるため、「分からない」の回答を除いて再集計している
注2：2022~2023年調査は従業員2名以上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名以上の企業に限定し再集計している

図48　電子契約の利用状況の推移：2015年～2024年

さらに詳細に電子契約の利用状況を見てみる（図49）。ここでは契約時に付与する電子署名のタイプ別に分類している。電子契約サービス事業者を通して電子署名を行う「立会人型」は４年間で大きな変化は見られないが、電子証明書を発行して当事者同士が電子署名をする「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高い署名タイプとなっている。「立会人型／当事者型両方」は、2022年１月調査で一度利用割合が低くなったが、2024年１月調査では、2021年調査時点とほぼ同じ割合に戻っている。契約の内容や相手によって、利便性の高い「立会人型」と本人性の担保力の強い「当事者型」を使い分ける企業が増えていると見られる。

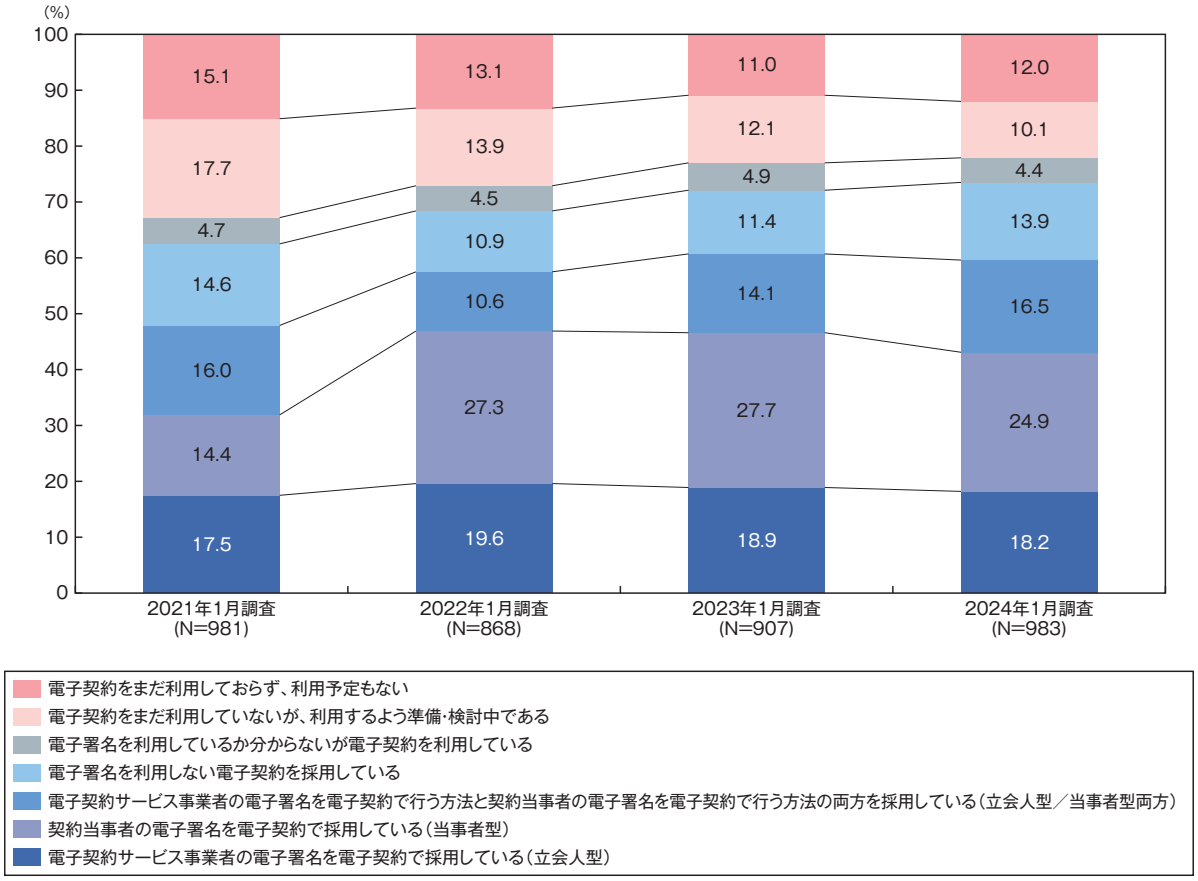


図49　電子契約の利用状況の推移（詳細）：2021年～2024年

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50）。全体では、「コスト削減（印刷代、郵送費、保管費用など）」の回答が最も多かった。さらに「印紙税の節約」も上位にあがっており、契約にかかる費用の削減効果が見られる。特に立会人型では、「コスト削減（印刷代、郵送費、保管費用など）」の効果が非常に大きくなっている。

全体で２番目に多い回答は、「契約にかかる業務負荷の軽減」となった。さらに「契約書管理の効率化（探しやすい、整理しやすいなど）」も上位にあがっており、契約業務の効率化に対する効果も見られる。特に、利便性の高い立会人型では約半数の企業で効果が出ており、なかでも費用削減と業務効率化に対する効果が大きくなっている。また、「契約時のセキュリティの強化」も上記に次いで効果が見られる。立会人型／当事者型の両方を利用している企業の回答率は、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：「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している

図50　電子契約の利用による効果：電子署名タイプ別

電子契約の導入における課題

では、電子契約を導入するにあたり、どのような課題があるのだろうか（図51）。まず主な課題として、「社内に電子契約サービスのシステムを新たに導入する手間がかかる」と「取引先に電子契約サービスのシステムを新たに導入する手間がかかる」という回答が多く、電子契約サービスの導入の手間があがっている。特に当事者型の利用企業では、社内に導入する手間の回答が半数近くなっている。

もう一つは、「取引先に電子契約サービスの導入目的の説明や同意を得ることが難しい」と「社内に電子契約サービスの導入目的の説明や同意を得ることが難しい」という、電子契約サービスを導入することについて、社内や取引先からの同意を得ることにある。特に立会人型を利用する企業では、社内の同意を得ることが大きな課題になっている。

	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）
社内に電子契約サービスのシステムを新たに導入する手間がかかる	37.0%	35.8%	46.9%	34.0%	32.1%	23.3%	32.3%
取引先に電子契約サービスの導入目的の説明や同意を得ることが難しい	33.8%	34.1%	38.0%	36.4%	37.2%	20.9%	19.2%
取引先に電子契約サービスのシステムを新たに導入する手間がかかる	29.9%	29.1%	35.9%	33.3%	24.8%	23.3%	21.2%
社内に電子契約サービスの導入目的の説明や同意を得ることが難しい	26.5%	48.0%	25.3%	16.0%	17.5%	23.3%	21.2%
電子契約サービスのシステム構成や機能（電子署名やタイムスタンプなど）が分かる要員が社内にいない	22.3%	25.1%	23.3%	20.4%	21.2%	30.2%	16.2%
電子契約の法制度要件（電子帳簿保存法や電子署名法など）が分かる要員が社内にいない	18.6%	16.8%	19.2%	21.6%	21.2%	11.6%	15.2%
電子契約サービス関連のコストが高い（初期導入コスト、運用保守コスト、電子証明書取得コストなど）	16.5%	16.8%	13.5%	17.3%	12.4%	14.0%	29.3%
紙の契約書と電子契約書が併存していて業務が煩雑になっている	14.7%	17.3%	12.2%	19.8%	10.2%	9.3%	16.2%
電子契約の業務プロセス（申請・承認フローなど）の設計が難しい	12.5%	15.6%	12.7%	12.3%	10.2%	7.0%	12.1%
電子契約サービスの製品や導入パートナーの比較検討が難しい	9.1%	13.4%	6.5%	11.7%	4.4%	4.7%	12.1%
電子契約書をクラウド環境に保管することに理解が得られない	8.2%	11.7%	6.5%	9.9%	5.8%	7.0%	7.1%
特に問題はない	8.9%	16.2%	7.8%	6.2%	3.6%	2.3%	13.1%

図51　電子契約の導入における課題：電子署名タイプ別

電子契約サービスの選定で重視する点

企業が電子契約サービスを選定する際に、どのような点を重視するのだろうか（図52）。「立会人型電子署名の電子契約に対応している」と「当事者型電子署名の電子契約に対応している」は、それぞれの署名タイプへの対応が重視する点として上位にあがっている。次に、「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番目の回答率となっている。特に立会人型を利用する企業では、60%以上が重視しており、第三者認証・認定の取得が立会人型電子契約サービスの選定に大きく影響していることが分かる。また、「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」や「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」など、信頼性のある電子証明書の発行も選定の重要な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%

図52　電子契約サービスの選定で重視する点：電子署名タイプ別

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．**電子契約の柔軟な運用が増えている**：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、導入が一段落したとみられる。利用されている電子署名のタイプとしては、当事者型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る。契約の内容や相手によって、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。

2．**コスト削減と業務効率化の効果が得られている**：電子契約の利用における大きな効果は、契約に係る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。

3．**電子契約サービス選定には事業者の第三者機関の認証・認定の取得が影響している**：電子契約サービスを選定する際は、利用したい電子署名タイプのサービスが提供されているのかと、信頼性のある電子証明書が発行されているかが重視される。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を取得しているのかも選定に強く影響していることも明らかになった。立会人型サービスの選定では、特に強く影響している。

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をさらに加速させていくだろう。「内向きのDX」から「外向きのDX」へ取り組みがさらに拡大していくと、高度なデジタル技術や大量のデータを活用することが増えていくと同時に、セキュリティリスクも高まっていくことになる。経営者やIT／セキュリティ責任者は、DXの推進とともに、セキュリティ戦略の見直しと強化を図っていくことが重要となる。

生成AIが社会全体で注目を集めている。企業での生成AI活用も、これから急速に拡大していくことが予想される。生成AIは劇的な業務の効率化を期待できる一方、情報漏えいやハルシネーションなど、さまざまなリスクが想定される。生成AIサービスは発展途上であるため、リスクへの技術的な対策が十分にできているとは言い難い状況にある。当面は、ユーザーである企業自身が生成AIの利用規程やガイドラインを策定し、業務で活用していく上でのリスクを減らしていく取り組みが不可欠となる。

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。本調査結果から、ランサムウェアは、常に身近に潜んでいるセキュリティ脅威であることが明らかになった。ランサムウェアは、感染すると影響が広範囲に及ぶため、対策を徹底していく必要がある。経営者やIT／セキュリティ責任者は、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、ゼロトラストセキュリティの実現に向けて、最新の技術・ツールにアップデートを行うことが求められている。

DXによるクラウドやAIを活用したデジタルサービスは、データの収集と活用が増えるため、プライバシーガバナンスへの取り組みが重要になってくる。ビジネスがグローバル化すれば、さらにその重要性は増していく。そこでは、日本も含む各国・地域のデータプライバシーに関する法規制に準拠することが強く求められる。特にこれからはAIに関する法規制の動向も注視しなければならない。さらに、プライバシーガバナンスへの取り組みも重要になってくる。これは、法規制への対応のみならず、自社の価値と信頼性を高めていくことを目的として、経営者がリーダーシップを取って推進していくべきである。

株式会社アイ・ティ・アール　シニア・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。

Ⅲ. コラム

DXの現在地と成果の活用

JIPDEC　電子情報利活用研究部　調査研究グループ　グループリーダ　**松下 尚史**

2000年にIT革命が流行語大賞となって以降、わが国においても急速にデジタル化・IT化が推進され、現在はDX[1]として多くの企業がその取り組みを進めています。「企業IT利活用動向調査2024」においても、85.6%の回答企業が何かしらのDXに関する取り組みを行っていることが明らかになりました。業種としては「金融・保険」「情報通信」が、従業員規模別としては従業員規模の大きい方がDXに関する取り組みを進めていることは調査結果のとおりです。事業の特性や資金力などの影響を考慮すると妥当な結果と言えます。

DX成果の測定指標に関する結果を見ると、全社的にDXが定着している企業が「顧客エンゲージメント」「新規製品／サービスの投入時間・頻度」「市場シェア」を測定指標として用いている点は非常に興味深いと言えます。IPAはDX実践手引書において、社内のデジタル化およびサプライチェーンまでの範囲のデジタル化を推進している状態をデジタルオプティマイゼーションと定義しており、顧客体験の変革・市場での立ち位置の変革・社会の変革などを推進している状態をDXと定義しています。この定義に従うと、本調査で全社的にDXが定着している企業のうちでも、社外（顧客や市場）に目を向けた測定指標を用いた企業をDX段階の企業と捉えることができ、部門横断的に取り組んでいる状態の企業、一部の部門で取り組んでいる企業、全社的にDXが定着しているが社外に測定指標と持たない企業はデジタルオプティマイゼーション段階の企業と捉えることができます。上記の捉え方から、本調査の集計結果を再整理すると、DX段階にある企業は12.0%、デジタルオプティマイゼーション段階にある企業は73.6%、DXに関する取り組みを行っていない、もしくは分からない企業が14.4%であるという結果がDXの現在地ということになります。

また、DXがどの段階にあるかに関わらず、過半数近くの回答企業が「業務コスト」「労働時間／残業時間」をDX成果の測定指標として挙げていますが、これらの指標は、一般論として、企業のコスト削減につながりますし、過半数近くの企業がコスト削減のためにDXに取り組んできたことを示していると考えられます。2000年以降、消費者物価や物価指数は下がり続け[2]、企業保有の現預金は2000年比259.7%となる一方で、人件費は2000年比135.0%にとどまっています[3]。今後、企業がDXの目標としたコスト削減の成果を、顧客への利益還元だけでなく従業員の賃上げにも充当することで、従業員は職場を出れば消費者であることから、消費が促進され、国内経済の好循環につながるものと考えられます。このような取り組みはDX段階にある企業でも、デジタルオプティマイゼーション段階にある企業でも取り組むことが可能です。

DXの成果を売価の引き下げと賃上げに同時に還元するDXを推進する企業が増えれば、消費者の購買力が向上し、企業はより多くの自社の製品・サービスを購入してもらえるよう、さらにDXを推進するという好循環が実現します。このような好循環を実現する企業の取り組みは、政府が掲げる「成長と分配の好循環[4]」の一面をなす取り組みであり、より多くの企業がこのような取り組みを推進することが求められています。

1　DXは、経済産業省が2020年11月9日に策定したデジタルガバナンス・コード2.0において、「企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること」と定義されている。
2　GDPデフレーターは消費税などの間接税を含む指標です。内閣府の国民経済計算（GDP統計）によると、2023年のGDPデフレーターは2000年比で、消費税が5%から10%に引き上げられているにもかかわらず、約4.5%低下しています。
3　財務省　法人企業統計調査
4　経済財政運営と改革の基本方針2023

生成AIと個人情報

JIPDEC　電子情報利活用研究部　主席研究員　**手嶋 洋一**

2022年11月にOpenAI社からChatGPTが公開されたのを皮切りに、生成AIブームが巻き起こっています。ChatGPTは、当時では最速となるサービス開始後2週間で全世界100万ユーザーを獲得しており、日本でも、国別の利用状況で第三位[1]となっているほど利用のすそ野は広がっています。

今回の調査（企業IT利活用動向調査2024）でも、すでに35.0%の企業が生成AIを利用し、「生成AIの導入を進めている」企業も34.5%と、今後の企業における生成AIの導入は急速に拡大していくとみられます。

一方、生成AIサービスの利用においては、使い方次第では個人情報の漏えいにつながる危険性をはらんでいます。2023年3月にイタリア当局が個人情報処理の問題を理由にChatGPTの一時禁止命令を行ったことが話題になったほか（現在は解除済み）、日本の個人情報保護委員会も、2023年6月2日に「生成AIサービスの利用に関する注意喚起等」[2]を行っています。

では、なぜ生成AIサービスを利用すると、個人情報が漏えいしてしまうのでしょうか？ ChatGPTをはじめとする生成AIでは、プロンプトに質問や作業指示を入力します。このプロンプトに個人情報を入力してしまうと、生成AIの精度を向上させるために利用されるデータ（これを学習データと呼びます）としてサービス事業者（＝第三者）に収集されてしまう場合があります。一旦学習データとして収集されてしまうと、他の利用者の質問の回答に利用されてしまい、予期せぬ機会に漏えいしてしまうこととなります。

生成AIサービスを利用する場合、個人情報保護の観点から、注意しなければならない点は大きく三つ挙げられます。一点目は、個人情報の利用目的の範囲内かという点、二点目は第三者提供の同意を得ているかという点、これら二つについて、個人情報収集時に同意を得ていた場合でも、生成AIサービスの提供者（例えばOpenAIなど）が海外企業の場合には越境移転規制をクリアしているかという点に注意しなければなりません。

企業や団体で生成AIサービスを利用する場合は、生成AIサービスを提供する事業者の利用規約やプライバシーポリシー等を十分に確認し、入力する情報の内容等を踏まえ、生成AIサービスの利用について適切に判断する必要があります。まずは、生成AIへの個人情報の入力は慎重に行うことを利用者に徹底することが得策だと思われます。

1　日本のChatGPT利用動向（2023年6月時点）（野村総合研究所）
2　生成AIサービスの利用に関する注意喚起等について（個人情報保護委員会Webページ）

電子メールの安全な未来：セキュリティガイドラインの最新動向

JIPDEC　セキュリティマネジメント推進室　主幹　**佐藤　桂史郎**

2023年10月にGoogle社がGmailに係る「メール送信者のガイドライン」を公表し、メール送信者（メール配信事業者等）は、DMARC等の送信元のなりすまし対策等への対応が必要となりました。2024年2月1日以降、当該ガイドラインに準拠しないメール送信者は、送信レートが制限されたり、メールがブロックされたりし、Gmailアカウントにメールが届かないような措置を取るとGoogle社が発表しています。また2024年5月に同じくGoogle社がGmailにおいて、送信ドメイン認証技術とは別の仕組みであるS/MIME（メール送信者のなりすまし防止／メールの改ざん検知／メールの暗号化技術）に必要な電子証明書の発行者（ルートCA）情報リストのアップデートが行われています。

DMARC等の送信ドメイン認証技術については、総務省のサイバーセキュリティタスクフォースのICTサイバーセキュリティ政策分科会の中でも議論がなされ、送信ドメイン認証技術導入に係るガイドラインが公表される予定です。当該ガイドラインは、メールの送信者側と受信者側のそれぞれで導入対応をするための、最低限必要な知識と設定にフォーカスした内容となっています。第5回ICTサイバーセキュリティ政策分科会[1]のWebサイトにガイドラインの案が公表されています。

内閣官房 内閣サイバーセキュリティセンターでは「政府機関等の対策基準策定のためのガイドライン（令和5年度版）」[2]を2023年7月4日付けで公表しています。こちらのガイドラインは、国の行政機関、独立行政法人および指定法人がサイバーセキュリティ対策のための統一基準の規定を遵守するための対策基準を策定する際に参照されるもので、当該統一基準の遵守事項を満たすためにとるべき基本的な対策事項が規定されています。電子メールのセキュリティ対策事項としては、DMARC等の送信ドメイン認証技術や、S/MIMEによる対策が示されています。特に、DMARC等の送信ドメイン認証技術については、前回令和3年度版のガイドラインでは電子メールのセキュリティ対策例の一つとして示されているだけでしたが、令和5年度版では、当該技術を導入する必要があるという表現に変わり、各政府機関に対して強く導入を求める内容となっています。

DMARCやS/MIME等のメールのセキュリティに対する取り組みを強化することで、なりすましメールによるサイバー犯罪による被害が軽減される効果が期待できます。政府機関や企業が安全で信頼性の高いメール環境を整備することは、国民の安心・安全な生活を支える重要な対策と言えるでしょう。

1　ICTサイバーセキュリティ政策分科会（第5回：2024年4月5日開催）
2　政府機関等のサイバーセキュリティ対策のための統一基準群

データ越境移転ツールの最新動向－APEC CBPRsからグローバルCBPRへ

JIPDEC　認定個人情報保護団体事務局　事務局長　**奥原 早苗**

これまで、個人データの越境移転ツール（認証制度）として運用されている仕組みとしては、APECのCBPRs一択と言っても良い状況でした。そのAPEC CBPRsも本格的に稼働したのは2013年のため、比較的歴史の浅い制度と言えます。そうしたことも要因の一つとして考えられますが、国際的な会合の場等で課題として挙げられてきたのは、制度自体の認知度が低いこと、認証を取得している企業が思うように伸びていないこと等です。

APEC域内においても、全エコノミー（以下、「国や地域」）が21ある中で、全てがこの制度に参加しているのかと言えばCBPRsに参加する国や地域は9と全体の半数に及ばず、さらに認証制度を適正に運用するために必要となるアカウンタビリティ・エージェント（AA）と呼ばれる認証審査機関を設置できている国や地域は5に留まります。そこで、APECに複数設置される委員会の中で「デジタルエコノミー運営グループ（DESG）」およびDESG内でCBPRsの活動を推進する「データプライバシーサブグループ（DPS）」では、参加する国や地域の拡大、認知度の向上、制度の改善他、さまざまな取り組みを行ってきました。

近年、わが国のみならず個人データの越境移転は世界的に拡大しており、「企業IT利活用動向調査2024」の結果でも「データの越境移転を行っている」と回答した企業は66.4％となっており、「今後さらに増えていく」と答えた企業はそのうちの1/4を占めています。ただし、自社が取り扱う個人データが越境しているかどうかを正しく把握できている企業はどれ位でしょうか。当協会は、2016年にAPEC CBPR認証制度における日本の審査機関として認定を受けてから、さまざまな情報流を審査する中で、クラウド等外部サービスの利用増大も相まって、複雑化するビジネススキームに紐づく業務フローを読み解き情報の棚卸しとマッピングすることの難しさを実感するところです。

国際的な動きとしては、2023年6月にわが国で開催された「G7データ保護・プライバシー機関（DPA）ラウンドテーブル」において、G7 DPA行動計画[1]が公表され、データ移転ツールがDFFTの重要な手段であると認識された2022年の前回会合における結論に基づき、移転ツールに対する取り組みがコミットされました。

ここで注目すべきは、安全かつ信頼性のある移転ツールに関する知識を共有するため、グローバル越境プライバシールール（グローバルCBPR）およびEU認証の要件の比較や、既存のモデル契約条項の比較を行うことが取り決められた点です。このグローバルCBPRは、CBPRsをAPECから独立させ、グローバル化するための新たな運営組織として、2022年4月21日に設立が宣言されたグローバルCBPRフォーラムが運営する制度であり、本格的な運用開始が待ち望まれています。この組織には、APEC CBPRに参加する九つの国と地域（米国、日本、カナダ、韓国、シンガポール、チャイニーズタイペイ、フィリピン、メキシコおよびオーストラリア）が参加しており、2023年6月にはAPEC域外で初めて英国が準会員として参加することが承認され、正にグローバルな展開を見せています。2024年4月30日には、全てのシステム文書がグローバルCBPRフォーラムのWebサイトに公開され、当協会もこの新しいCBPR認証制度の審査機関として認定を受けたばかりです。

APECと並び移転ツールの選択肢として新たな国際水準の認証制度が動き始めることは、事業者や規制当局だけでなく、データの提供主体である利用者にとっても安全かつ信頼性のあるデータの取り扱いが行われていることを示す指標の一つとなり得るため、今後さまざまなステークホルダーに注目していただきたいと思います。

1　G7 DPA行動計画（仮訳）（個人情報保護委員会）

プライバシーガバナンスをめぐる動き

JIPDEC　電子情報利活用研究部　主幹　**恩田 さくら**

デジタル化の加速を背景に、パーソナルデータの利活用におけるプライバシーへの配慮はますます重要になってきています。企業が社会から信頼を獲得するためのプライバシーガバナンスの構築に向けて取り組むべきことを取りまとめた「DX時代における企業のプライバシーガバナンスガイドブック」（以下、ガイドブック）は、経済産業省、総務省より2020年8月に発表され、2023年4月に最新のver1.3が公表されました[1]。

このガイドブックや付属資料においても、企業のプライバシーガバナンスに関する実践例が紹介されてきたところですが、2023年度も、プライバシーに関係する主要な団体のイベント[2]や、学会[3]、ビジネス法専門誌[4]など[5]においても、引き続き、プライバシーガバナンスの重要性、実効性の確保や定着、組織のデータ活用とコミュニケーションの在り方などについて議論が深められるとともに、各企業のプライバシーガバナンスに係るプラクティスの共有が図られました。業界団体におけるセミナーや勉強会も開催されました。

プライバシーガバナンスをより強固にするものとして、プライバシー影響評価（PIA）を実施し、その結果を発信する事例も見られるようになりました。株式会社NTTドコモは、「NTTドコモグループ サステナビリティレポート2023」の中でPIA制度や、評価件数、事例を紹介しています。また利用者向けのWebサイトからもPIAの取り組みを発信しています。

2024年4月19日に、経済産業省と総務省は「AI事業者ガイドライン（第1.0版）」[6]（以下、ガイドライン）を公表しました。ガイドラインの共通の指針の1項目として、プライバシーを尊重し、保護することが重要であるとされています。ガイドラインの別添資料の中では、プライバシーガバナンスの重要性も指摘されています。例えば、AIシステムをアプリケーション、製品、システムなどに組み込んだサービスを提供する事業者に対して、プライバシー侵害への対策として、常に関連する情報を収集し、有識者との関係性を構築して相談することなどが期待されるとされており、具体的な手法として、プライバシー保護組織による対応が紹介されています。また、AIシステムまたはAIサービスを利用する事業者向けにも、個人情報の不適切入力及びプライバシー保護組織を中核として、新規事業部門を含むAIシステム・サービスを利用する部門の密なコミュニケーションを醸成したり、関連情報を社外有識者から収集したり、多角的に対応策を検討する等を実質的に行うことができる、との記述もされています。

現在、個人情報保護法の3年ごと見直しの検討が進んでいますが、個人情報保護委員会による経済団体等に対するヒアリングの中でも、プライバシーガバナンス等の民間の自主的な取り組みの推進につい

1　「DX時代における企業のプライバシーガバナンスガイドブックver1.3」
2　MyDataJapan CONFERENCE 2023（2023年7月14日開催）、NIKKEI PRIVACY CONFERENCE 2023（2023年10月30日開催）、Privacy by Design Conference 2024（2024年1月24日開催）等。
3　情報ネットワーク法学会（2024年12月9日開催）等。
4　NBL1257（2024.1.1）号「データガバナンス／プライバシーガバナンスの要諦と課題（上）」、NBL1258（2024.1.15）号「データガバナンス／プライバシーガバナンスの要諦と課題（下）」
5　IT-Report2023 Winter座談会「「今考えるプライバシーガバナンス」～生成AIをはじめデータの高度な利用が進む中で～」
6　「AI事業者ガイドライン（第1.0版）」

ては言及されています。一般社団法人日本経済団体連合会のヒアリングの資料[7]においては、データ主体や社会からの信頼獲得のために、アジャイル・ガバナンスの考え方の採用、プライバシーガバナンスの促進等によるPDCAサイクルの構築と事業者の主体的取り組みの推進が求められています。また、実効性のある監視・監督の在り方として、事業者の主体的な取り組みや適切な対応を促す仕組みとして、プライバシーガバナンスやデータガバナンス体制を促す仕組みや、PIAの普及への支援などが挙げられています。

今後もプライバシーガバナンスに対する理解が進み、企業の自主的な取り組みが広がるとともに、その取り組みが社会からのその企業の信頼の獲得につながるような環境整備が進んでいくことが望まれます。

7　第270回個人情報保護委員会（2024年1月31日）「個人情報保護法の3年ごと見直しに対する意見（日本経済団体連合会）」（https://www.ppc.go.jp/aboutus/minutes/2023/20240131/）

「eシール」とは～「シール」本来の意味を入り口に～

JIPDEC　デジタルトラスト評価センター　**曾我部 倭玄**

皆さんは「シール」の意味をご存知でしょうか。本来は文書の真正性や発信元の証明として利用されるものを指し、実は「印章（印鑑）」もその一例に含まれます。他には、手紙が未開封であることの証明として使われる「封蠟」が馴染み深いかもしれません。

文書の真正性や発信元を保証・証明するための「シール」ですが、デジタル社会で「シール」の役割を担っているのが「eシール」[1]です。請求書、資格証明書、電化製品への保証書だけにとどまらず、IoTデバイスから出力されるデータ等、クラウド環境で取り交わされるデータにもeシールの付与が考えられます[2]。

この「eシール」、全く新しい技術ではなくPKI[3]に基づく技術であり、電子署名と仕組みは同じです[4]。電子署名と同じように、電子データにeシールを付けるには電子証明書が必要で、eシールの情報には、電子証明書内の記載事項（法人・団体名やその所在地等）も、その一部として記録されています。

ただ、eシールの情報、すなわち電子証明書の情報が不正確・不正なものであった場合はどうでしょうか。eシールを付けたデータの信頼性に疑いが生じます。このため、電子証明書を発行するサービスが「安心・安全」なものか、第三者による認証が重要です。その点において、JIPDECでは、電子証明書を発行するサービス等を審査し、その信頼性を公表する「JIPDECトラステッド・サービス登録」（JTS登録）を行っています[5]。登録基準も公開しているため、ぜひご確認ください[6]。

さらに総務省から、国によるeシールに係る認定制度が2024年度中にスタートすることが公表されています[7]。国の認定制度が始まることにより、eシール関連の市場がどのように変化するのか、注目されるところです。

今後、実社会での認印や実印と同様に、「行政への申請書類には国の認定を取得した電子証明書でeシール、一方、請求書には民間の第三者認証を取得した電子証明書でeシール」といった、eシールを使い分ける未来がくるのではないでしょうか。

最後に、eシールの用途は大量発行を前提としたものが多く、卒業証明書に至っては、何万単位となり、その枚数に応じたeシールの付与が必要となります。この時に「リモート署名サービス」との組み合わせが重要ですが、「リモート署名サービス」についても、JTS登録で審査・評価をしています[8]。

JIPDECは、JTS登録を通じて安心・安全なデジタル社会の実現に貢献していきます。

1　eシール（eSeal）：電子データ／文書の起源と完全性を保証するもの。日本国内におけるeシールの定義については、総務省「eシールに係る指針（第2版）」、「1.1 eシールの定義」も併せてご覧ください。
2　eシールの用途については、総務省「eシールに係る指針（第2版）」、「1.4 eシールのユースケース」も併せてご覧ください。
3　PKI（Public Key Infrastructure：公開鍵基盤）：公開鍵暗号技術に基づいて、電子署名や相手認証等を実現するための技術基盤。
4　共通点としては、電子署名、eシール共に改ざんされていないことが分かる仕組みであることが挙げられます。異なる点としては、電子署名をした場合は電子署名をした者（自然人）の意思が含まれますが、eシールを付けた場合は意思が介在せず、発信元の証明（＝主に組織等から発行されたことの証明）のみにとどまります。総務省「eシールに係る指針（第2版）」、「1.2 eシールと電子署名の異同」も併せてご覧ください。
5　JIPDECトラステッド・サービス登録（JTS登録）
6　JTS登録では現在、以下の登録基準を公開しています。
・JIPDECトラステッド・サービス登録（認証局）登録基準
・JIPDECトラステッド・サービス登録（リモート署名サービス）登録基準
7　総務省HP報道資料「eシールに係る検討会 最終取りまとめ」、「eシールに係る指針（第2版）」及び意見募集の結果の公表」（令和6年4月16日）の概要より
8　JIPDECトラステッド・サービス登録（リモート署名サービス）

〈資料〉情報化に関する動向（2023年10月～2024年３月）

【国内／国際連携】

2023年10月

- 広告であることを隠して宣伝・表示するステルスマーケティング、内閣府告示第19号（施行：2023年10月１日）により景品表示法違反の規制対象に。
- 全国銀行資金決済ネットワーク、システム障害で２日にわたり10行での振込みできず、約506万件に影響。システム稼働50年目にして初の大規模障害。
- NTT西日本グループ会社、元派遣社員が10年にわたり全国各地の複数企業のコールセンター業務に係る顧客情報約120万件を不正持ち出し発覚。その後の調査で928万件に。2024年１月に個人情報保護委員会（PPC）、２月に総務省が行政措置。
- PPC、英国データ保護機関（ICO）と個人情報保護に関する法令施行や情報交換の促進を図る協力覚書を締結。
- 公正取引委員会、スマートフォン端末の初期設定で自社検索サービスの優遇が独占禁止法に当たるとしてGoogleの審査開始。第三者からの情報・意見募集も。
- G７首脳、「広島AIプロセス」に関する声明発出。生成AI開発者向けリスク軽減策事例を示した行動規範、指針公表。

2023年11月

- 米中日等28か国とEU、AI安全サミット（主催：英）でAIのリスクを認識し安全で倫理的なAI開発を約束する「ブレッチリー宣言」に共同署名。
- 経済協力開発機構（OECD）／G20、国際社会におけるデジタル化とグローバル化から生じる巨大IT企業を対象とする税務課税に関する多国間条約を発表。
- 日米欧等50か国・地域、「カウンターランサムウェア・イニシアティブ会合」にてランサムウェア攻撃に対し身代金を払わないと共同誓約。
- G７競争当局等、巨大IT企業による市場独占を阻止するための会合を開催。「デジタル競争コミュニケ」採択。
- 日米英等18か国、AIの不正利用防止のための安全なAI開発・活用を促す「セキュアAIシステム開発ガイドライン」に共同署名し、公表。設計段階でのセキュリティ確保を要請。
- LINEヤフー、韓国関連会社経由でサイバー攻撃を受け、約44万件の個人情報流出。その後の調査で被害は52万件に拡大。2024年３月にPPCが是正勧告。
- デジタル庁、初の国内ガバメントクラウド提供事業者として「さくらインターネット」を採択。2025年度中の運用・提供開始の条件付き。

2023年12月

- G７デジタル・技術大臣会合、AI開発者向け行動規範等を示す「広島AIプロセス包括的政策枠組み」および「広島AIプロセス推進作業計画」と、国境を越えたデータ流通や信頼性のあるデータ流通の育成を目指す「DFFTの具体化に関する閣僚声明」を採択
- 日米政府、偽情報流布対処で連携する協力文書に署名。
- 国際電気通信、12月の決議で１日の長さに１秒を加える「うるう秒」の調整廃止を決定。
- 政府、紙の健康保険証廃止を24年12月２日に決定。マイナ保険証に一本化。
- 財務省、海外スマホゲームの消費税納付を巨大IT企業に課すこと等を盛り込んだ、今後の課税方法・導入に向けた検討結果を含む令和６年度税制改正大綱を閣議決定。
- PPC、個人情報保護法規則とガイドライン改正。ECサイトのスキミング被害、マルウェア感染被害による漏えいも報告対象に。

2024年１月

・日米他９か国、AI使用に関するガイダンス「Engaging with Artificial Intelligence（AI）」に共同署名。
・日EU、日・EU間のデータの自由な流通に関する規定を追加した「経済連携協定改正議定書」に署名。

2024年２月

・日本政府、IPA内にAIの安全性評価手法の検討等を行う機関「AIセーフティ・インスティテュート（AISI）」設置。米英のAIセーフティ・インスティテュートや、諸外国機関と連携へ。
・日米欧、被害規模世界最大級のランサムウェア攻撃グループLockBit摘発。2023年の被害は1,000件超。

2024年３月

・日韓等６か国、米国主導で商用スパイウェアの拡散・悪用対策に取り組む国際協定に参加。17か国が加盟。
・国連総会、各国に安全で安心、信頼できるAIシステムの開発・利用に向けた取り組みを求める決議案採択。日本等120以上の国・地域が共同提案国に。
・日本DPO協会とJIPDEC、個人情報保護力量検定試験制度と教育制度創設。
・旭川地裁、探偵によるGPS機器を使っての素行調査はプライバシーの違法侵害と判決。

【海外】

2023年10月

・米国家安全保障局、AIの開発と統合を監督する「AI Security Center」創設。防衛基盤強化を目指す。
・米ユタ州、ユーザーからの収集データが中国政府と共有され、さらには中毒性のあるアプリ設計が子どもたちに害を及ぼすとして、TikTokに賠償と慣行変更を求め提訴。
・欧州委員会（EC）、違法コンテンツや偽情報の排除を義務付けたデジタルサービス法（DSA）準拠確認のため、X（旧Twitter）の調査開始。12月に本格調査。
・Google、生成AIユーザーが生成した著作物に対し、著作権者からの訴訟リスク補償を表明。
・EC、加盟国に対し、テロや違法コンテンツによる深刻な脅威からユーザーを守るため、DSAに基づき大手プラットフォーマーに義務を執行させるよう勧告。
・EC、DSA施行支援のため、フランスとアイルランドのメディア規制当局と管理協定締結。
・米カリフォルニア州等42州・地域、若者ユーザーに有害コンテンツを提供したとして、Metaを提訴。Metaは安全に配慮した利用環境を提供しているとコメント。
・米政府、中国向けAI用半導体の輸出規制を予定前倒しで発効。
・英政府、オンライン上での子どもの安全確保のためにプラットフォームへの対応を義務付ける「オンライン安全法」成立。
・バイデン大統領、「安全・安心・信頼できるAIの開発と利用に関する大統領令」に署名。

2023年11月

- 欧州データ保護委員会、EUと欧州経済地域30か国でのMetaのターゲティング広告配信禁止を発表。個人データ収集方法を問題視し、アイルランドデータ保護委員会（IE DPC）に２週間以内に処理を課すよう指示。その後、IE DPCがデータ処理の禁止命令。
- ネパール政府、ヘイトスピーチ、偽情報、プライバシー侵害の増加を受けTikTok利用禁止発表。
- Meta、TikTokとApple、ECがデジタル市場法（DMA）のゲートキーパーに指定したことに対し、異議申し立て。
- Microsoft、AI向け半導体、クラウドコンピューティング用プロセッサを初めて自社開発。
- 米司法省、世界最大の仮想通貨取引所Binanceへの違反行為調査終結で、40億ドル超の支払い要求。2024年２月に43億ドル支払いで和解成立。
- カナダ政府とGoogle、６月成立のオンラインニュース法に則り、国内報道機関への対価として年間１億カナダドル支払いで合意。
- 米モンタナ州、2024年１月１日施行予定のTikTok禁止法について、アプリ禁止が言論の自由を損なうとのTikTok側や利用者からの不当提訴を受け、連邦地裁が仮差し止め。
- Meta、連邦取引委員会（FTC）が５月に提示した18歳未満ユーザーからの収集データの広告利用規制案を違憲として、FTCを提訴。

2023年12月

- 米遺伝子計算ツール会社の23andMe、サイバー攻撃で90万件の遺伝的データ漏えいを報告。
- IBMとMeta、安全で責任のあるAI推進に焦点を当てたコミュニティ「AI Alliance」設立。世界50以上の企業・大学等が創設メンバーとして参画。
- Epic Games、ゲームアプリ内課金手数料をGoogleが徴収するのは独禁法違反としてG社を提訴した連邦地裁裁判で勝訴。地裁はG社に対する差し止め命令案提出をE社に要請。
- 欧州司法裁判所、ルクセンブルクによるAmazonへの税優遇措置を不当としてECが2.5億ユーロの徴収命令を科した裁判で、21年の下級裁判所の無効判決を支持し、上告を棄却。
- Google、2018年に提訴されたアプリストア利用者への過大請求を巡る裁判で、消費者と米50州・地域への合計７億ドルの和解金で合意。G社は自社アプリストア以外からのダウンロードの簡略化など対応。
- 英最高裁判所、AIシステム考案の発明品の特許登録認めず。「発明者は人間か企業でなければならない」とする英知的財産庁の見解を支持。
- Google、位置情報履歴の保存とアクセス方法変更。法執行機関によるユーザーの位置情報の強制提出を求めるジオフェンス令状が無効に。
- EC、世界最大級の３アダルトサイトをDSA規制対象に指定。利用者保護対策等の報告義務。
- FTC、オンラインでの子どもの個人情報保護を強化する児童オンラインプライバシー保護法（COPPA）変更提案。データセキュリティ強化や子ども向けターゲティング広告制限盛り込み。
- 中国ネット通販大手の京東集団、Alibabaへの独禁法違反訴訟の一審判決で勝訴。A社に10億元賠償金支払い命令。

2024年１月

- 米証券取引委員会、暗号資産最大手Bitcoinの現物投資型の上場投資信託の上場申請を初承認。
- 米最高裁判所、Epic Games対Appleの独禁法違反訴訟に関する両社の審理請求を却下。iOS開放を求めたE社の主張は認められず。
- Microsoft、AI使い全個体電池向け新素材を発見。２年かかる研究が２週間で成果。
- ロシア連邦独占禁止局、Appleが独占的地位乱用に対し12億ルーブルの制裁金を支払ったと発表。
- 米ニュージャージー州、消費者プライバシー法成立。2025年１月施行。事業者に個人データの処理目的、開示先第三者情報など消費者への通知を義務付け。
- 伊データ保護機関（GPDP）、OpenAIに対し、2023年３月にユーザーデータの違法処理で一時使用禁止となり翌月使用再開されたChatGPTについて、GDPR違反があったと通知。

2024年２月

- MetaとByteDance、EUのDSAで義務付けられたプラットフォーム監視費用の負担配分を不服として、それぞれ異議申し立て。
- EC、DMAで指定したゲートキーパー６社のうち、Microsoft、Appleの一部サービスを規制対象から除外。
- Google等IT企業20社、2024年予定の各国選挙に向け、AI生成の偽コンテンツ排除に向けた協定締結。

2024年３月

- EC、音楽ストリーミング市場における競争法違反でAppleに18.4億ユーロの制裁金。A社は不服申し立てを表明。
- GPDP、OpenAIのAI動画自動生成技術Soraの個人データ処理に関する調査を開始。
- EU、DMAの全面適用開始。規制対象のゲートキーパーはApple、Google、Amazon、Microsoft、Meta、TikTokの６社、22サービス。
- 欧州データ保護監察機関、ECによるMicrosoft365使用は個人情報保護規則違反と指摘。EU域外への移転データの保護措置の不備を指摘し、ECにM社のデータ移転停止を命令。
- 米下院、外国の敵対者が制御するアプリの配布、維持、提供を禁止する法案可決。中国ByteDance運営のTikTok利用禁止へ。
- 欧州議会、世界初のAI包括規制法案「EU AI Act」可決。AI製明示など透明性担保を要求。2026年運用開始予定。
- 仏競争委員会、GoogleによるAI開発へのメディア記事の無断使用、対価支払いへの不誠実な対応に、2.5億ユーロの制裁金。2021年に続き２度目。
- 米司法省、iPhone等の寡占的地位乱用を問題視し、Appleを反トラスト法違反で提訴。
- EC、アプリストアからのアプリ取得の制約や、検索結果への自社サービスの優先的表示がDMA違反に当たるとして、Apple、Google、Metaに対しDMA正式適用後初の調査を開始。
- 欧州理事会と欧州議会、全加盟国間で電子ヘルスデータのやり取りとアクセスを容易に行うための「欧州ヘルスデータスペース規則案」について、暫定的政治合意。研究開発目的での利用が可能に。
- EC、巨大IT企業に対しDSAに基づく選挙関連の偽情報対策措置の指針を発表。
- 米フロリダ州、14歳未満の子どものSNSアカウント取得禁止法成立。14～15歳アカウントは保護者の同意必須。同意ない場合は運営会社が停止・削除処置。
- 米政府、公共サービスでのAI利用の安全性を確保するため、全政府機関に最高AI責任者任命を義務化。
- AT＆T、顧客情報7,300万件がダークウェブに流出。社会保障番号等も含まれる。

JIPDEC IT-Report 2024 Spring
2024年5月31日発行（通巻第23号）
発行所　一般財団法人日本情報経済社会推進協会
〒106-0032 東京都港区六本木1-9-9
六本木ファーストビル12階
TEL：03-5860-7555
制　作　株式会社ウィザップ