News Release

2025年3月14日

一般財団法人日本情報経済社会推進協会（法人番号：1010405009403）
株式会社アイ・ティ・アール（法人番号：3011101047117）

企業の45%が生成AIを利用、日常業務では80%超の企業が利用成果を認識
ランサムウェア感染経験は48%、メールによる攻撃とリモートアクセス脆弱性が主な侵入経路

－JIPDECとITRが『企業IT利活用動向調査2025』の結果を発表－

一般財団法人日本情報経済社会推進協会（所在地：東京都港区、会長：杉山　秀二、以下、JIPDEC）と株式会社アイ・ティ・アール（所在地：東京都新宿区、代表取締役：三浦　元裕、以下、ITR）は本日、国内企業1,110社のIT戦略策定または情報セキュリティ施策の従事者を対象に、2025年1月に共同で実施した『企業IT利活用動向調査2025』の結果を発表いたします。

なお、本日15:00開催予定のJIPDECセミナーでは、本調査の詳細分析結果を報告予定です。
JIPDECセミナー「生成AIの活用成果の実態とセキュリティ課題への取り組み状況　～「企業IT利活用動向調査2025」結果報告」

今回の調査結果のポイントは、次の6点があげられます。

1．45%の企業が生成AIを利用。電子メールや資料作成など日常業務の利用では80%超が効果を認識している
2．生成AI利用のリスクとして、機密情報の漏えいとハルシネーション、倫理的問題が懸念されている
3．「内向きのDX」では業務のデジタル化で順調に成果が出ているが、企業文化の変革には課題が残り、「外向きのDX」では新しいビジネスの創出に向けた取り組みに遅れがみられる
4．テレワークと出社併用のハイブリッド勤務が主流であるが、最低出社日数を義務付ける企業やテレワーク制度がほとんど活用されていない企業もある
5．ランサムウェア感染経験は48%、メールによる攻撃とリモートアクセスの脆弱性が主な侵入経路
6．プライバシーガバナンスの取り組みは、従業員と顧客の双方のエンゲージメント向上に寄与

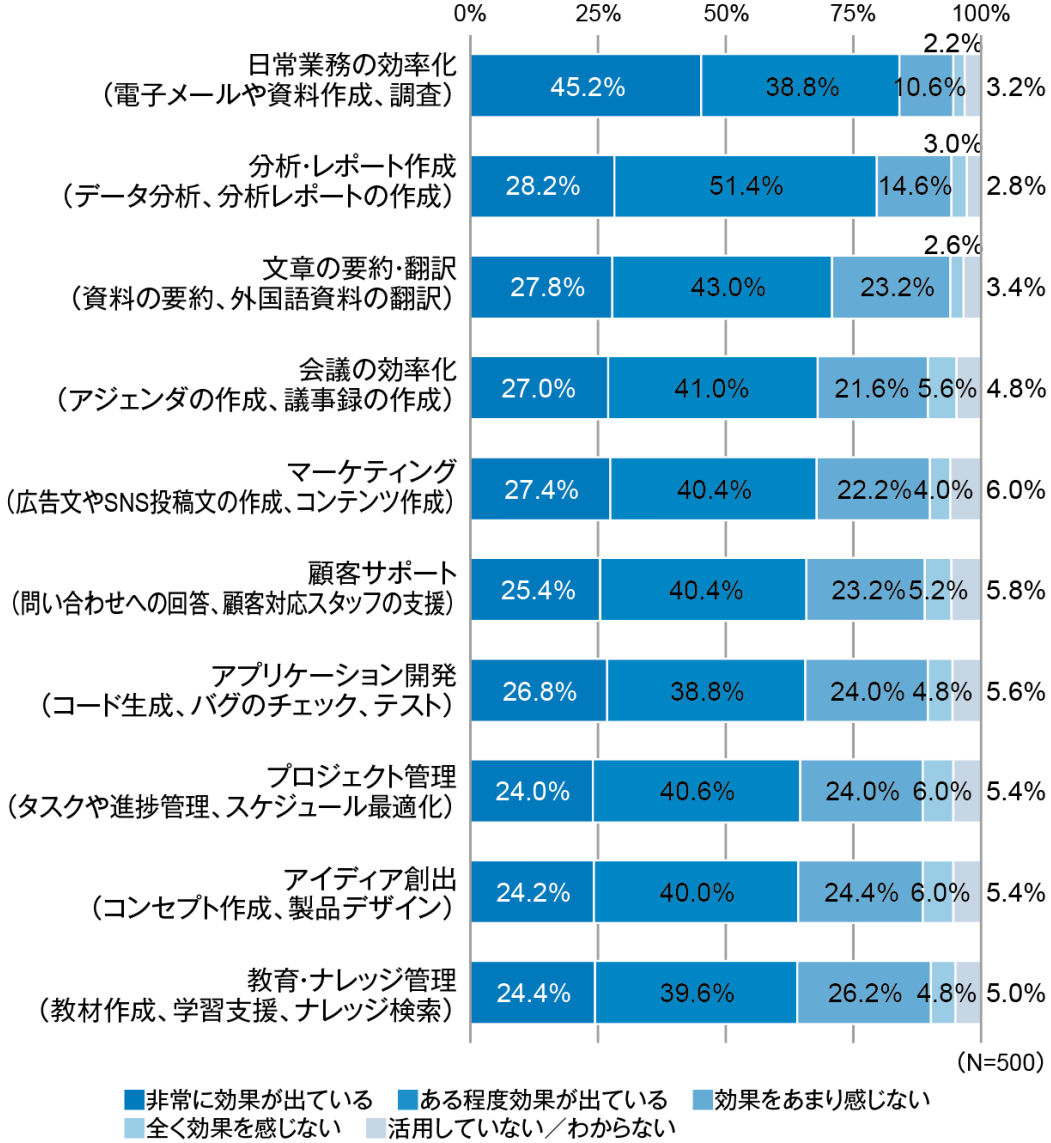
■45%の企業が生成AIを利用。電子メールや資料作成など日常業務の利用では80%超が効果を認識している

現在、生成AIへの関心が非常に高まっています。生成AIの利用状況について質問したところ、「全社的に利用が推奨され、幅広い業務で利用されている」が15.9%、「必要性の高い特定部門での利用に限定されている」が29.1%となり、合わせて45.0%の企業がすでに生成AIを利用している状況にあります。また、「一部のプロジェクトやチームで試験的に利用され、効果を検証している」は26.3%となり、生成AIを利用する企業がさらに増えていくとみられます。

次に、生成AIを全社的に利用している企業と特定部門で利用している企業を対象に、業務における生成AIの活用効果について質問したところ、「日常業務の効率化」については、45.2%が非常に効果が出ている、

38.8%がある程度効果が出ていると回答しました。この電子メール文や資料作成、データ入力、調査などの日常業務では、80%超の企業で生成AIの活用効果を認識していることが分かりました。次いで、「分析・レポート作成」も79.6%と多くの企業で活用効果が出ています。その他、「文章の要約・翻訳」「会議の効率化」「マーケティング」など、調査設問にあげたいずれの業務でも、効果が出ていると回答した企業が60%を超えました（図1）。生成AIを利用している企業の多くは、さまざまな業務で一定の活用効果をあげていることが読み取れます。

図1. 業務における生成AIの活用効果



出典：JIPDEC／ITR『企業IT利活用動向調査2025』

■生成AI利用のリスクとして、機密情報の漏えいとハルシネーション、倫理的問題が懸念されている

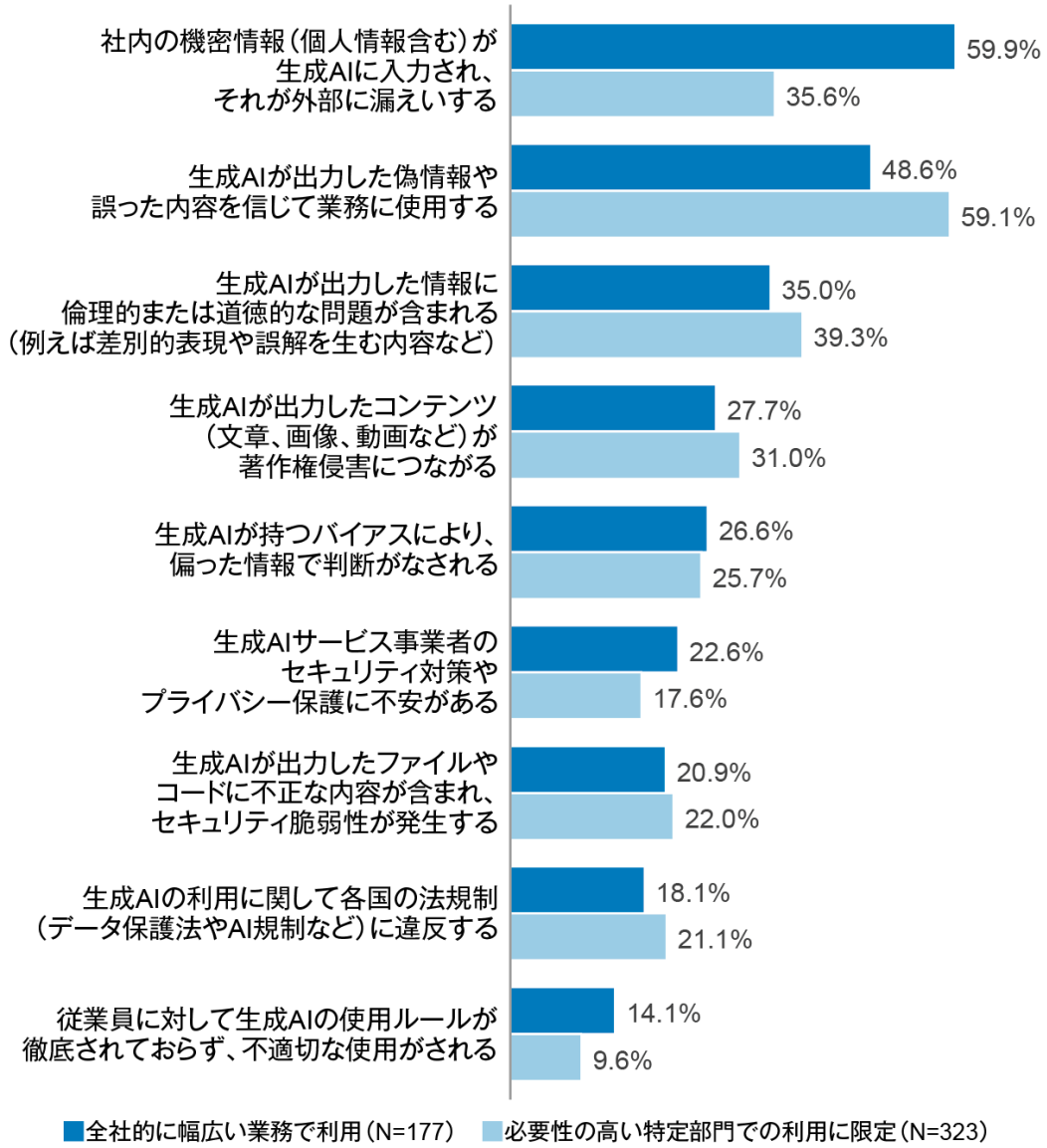
生成AIを利用していくうえでのセキュリティやプライバシーに関する不安や懸念点を質問したところ、生成AIを全社的に利用している企業では、「社内の機密情報（個人情報含む）が生成AIに入力され、それが外部に漏えいする」が最多の59.9%となりました（図2）。この結果から、生成AIの利用においては多くの企業が情報管理のリスクを強く意識していることが分かりました。特に、従業員が無意識のうちに機密情報を入力してしまうケ

ースや、適切なアクセス制御がされていないケースなどで、生成AIを利用することによる情報漏えいなどが懸念されています。この点は特定部門で利用している企業でも3番目に多い懸念点となっています。

特定部門で利用している企業での最多は、「生成AIが出力した偽情報や誤った内容を信じて業務に使用する」が59.1%に上り、ハルシネーション（AIが事実に基づかない情報を生成する現象）に対する懸念が大きいことが明らかになりました。ハルシネーションリスクは、意思決定や業務の正確性に大きな影響を及ぼす可能性があるため、十分に注意する必要があります。さらに「生成AIが出力した情報に倫理的または道徳的な問題が含まれる（例えば差別的表現や誤解を生む内容など）」の回答も多く、これらのリスクも重要な課題と認識されていることが分かりました。差別的な表現や誤解を招く内容が含まれることで、企業のブランドイメージの毀損や法的リスクにつながる可能性があります。

これらの懸念を踏まえると、生成AIの活用には慎重な運用が求められます。企業は、情報漏えいを防ぐための利用ルールを明確にし、従業員のリテラシー向上を図るとともに、AIの生成結果を適切に管理・監視する仕組みを整えることが不可欠となります。

図2．生成AIの利用におけるセキュリティ／プライバシー上の懸念点



出典：JIPDEC／ITR『企業IT利活用動向調査2025』

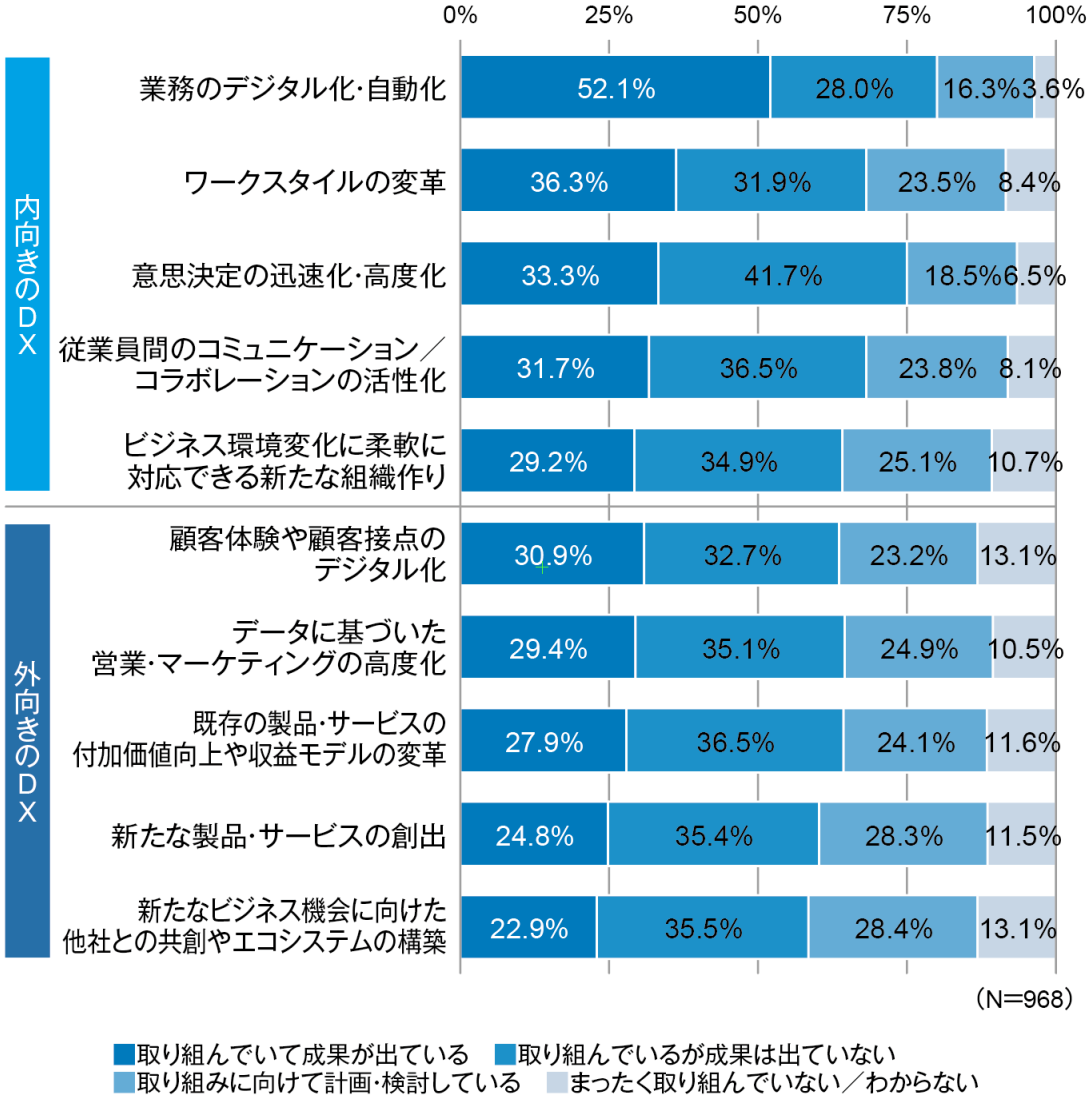
■「内向きのDX」では業務のデジタル化で順調に成果が出ているが、企業文化の変革には課題が残り、「外向きのDX」では新しいビジネスの創出に向けた取り組みに遅れがみられる

DX（デジタルトランスフォーメーション）を実践している企業に対して、具体的な取り組み内容とその成果について質問しました（図3）。社内の業務や働き方に関するDXを「内向きのDX」、顧客向けの新たな製品やサービス、マーケティングに関するDXを「外向きのDX」と分類しました。

「内向きのDX」で最も取り組みが進んでいるのは「業務のデジタル化・自動化」であり、52.1%の企業で成果が出ており、次いで「ワークスタイルの変革」では36.3%で成果が出ています。「意思決定の迅速化・高度化」では33.3%が成果が出ているとした一方で、まだ成果が出ていない企業は41.7%となりました。また、「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」と「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、まだ成果が出ていない企業の割合の方がより高い状況にあります。「内向きのDX」では、業務のデジタル化は比較的順調に進んでいるものの、意思決定の迅速化やコミュニケーションの活性化、組織の柔軟性向上といった、企業文化に関わる変革は依然として課題となっていることが分かりました。

一方、「外向きのDX」において最も成果が出ているのは、「顧客体験や顧客接点のデジタル化」で30.9%に、次いで「データに基づいた営業・マーケティングの高度化」が29.4%となり、顧客エンゲージメントを向上させるための取り組みが先行しています。「新たな製品・サービスの創出」や「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」といった、新しいビジネスの創出や機会に向けた取り組みはやや遅れていることが分かりました。「外向きのDX」の取り組みは、いずれも取り組んではいるが成果が出ていない割合の方がより高い結果が見て取れます。今後、成果を出していくためには、データの活用をさらに深化させ、デジタル技術を活用した新たな製品やサービスの開発に挑戦することが重要となります。

図3．DXの取り組み内容と成果の状況



出典：JIPDEC／ITR『企業IT利活用動向調査2025』

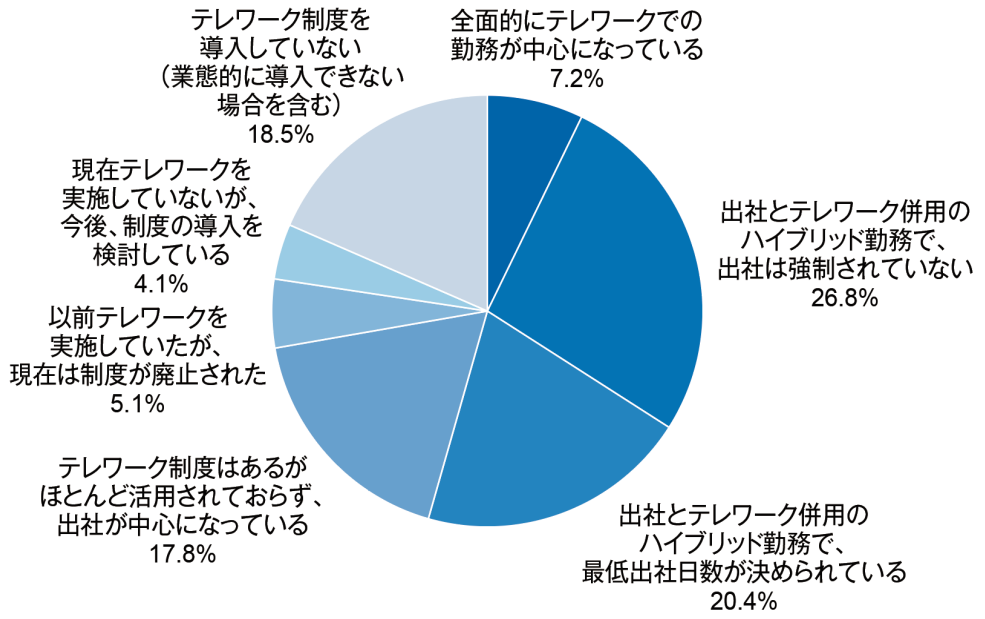
■テレワークと出社併用のハイブリッド勤務が主流であるが、最低出社日数を義務付ける企業やテレワーク制度がほとんど活用されていない企業もある

テレワークの実施状況について質問したところ、「全面的にテレワークでの勤務が中心になっている」は7.2%にとどまり、出社とテレワーク併用のハイブリッド勤務が主流になっていることが明らかになりました（図4）。その内訳は、「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」が26.8%、「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」が20.4%と半数近くを占めています。出社を強制しないハイブリッド勤務は、従業員の裁量を尊重し、業務内容や個々の事情に応じて柔軟に働ける環境を提供しているものと考えられます。一方、最低出社日数を定めるハイブリッド勤務は、オフィスでの対面コミュニケーションの重要性やチームワークの維持を考慮し、一定の頻度での出社を求めていると考えられます。

また、「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」は17.8%、「以前テレワークを実施していたが、現在は制度が廃止された」が5.1%と、完全な出社回帰の企業も一定層存在します。最近、欧米の企業では、対面コミュニケーションを重視し、完全リモートワークから出社中心の勤務へ回帰する動き

もみられます。コロナ禍によって大きく推し進められてきたテレワークですが、今後は企業文化や業務特性に応じて勤務体系のさらなる多様化が進んでいくと考えられます。その中で、テレワークと出社のバランスをどう取るかが、企業の生産性や従業員エンゲージメントに大きな影響を与えるとみています。

図4．テレワークの実施状況



（N=1,110）

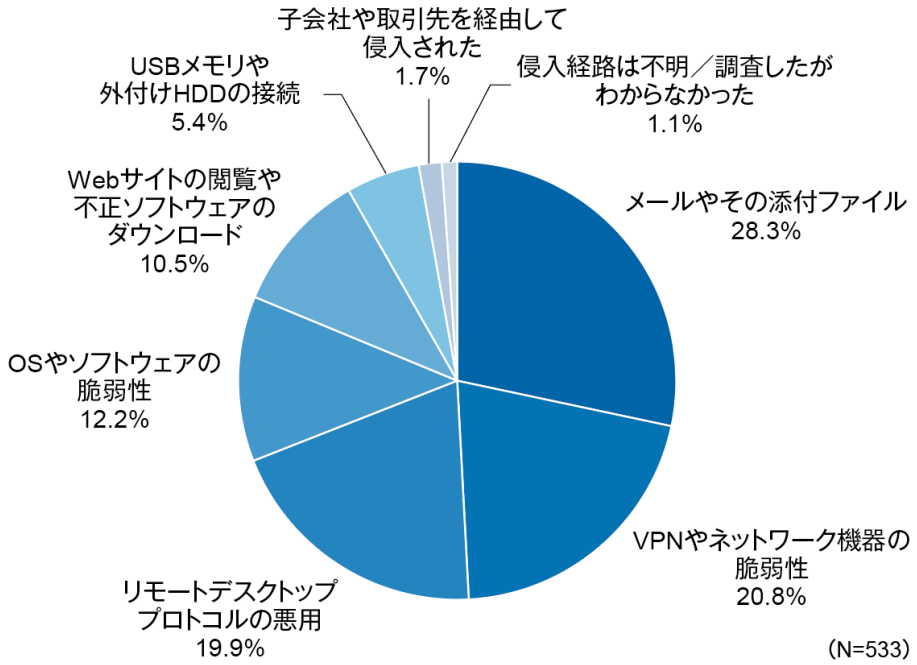
出典：JIPDEC／ITR『企業IT利活用動向調査2025』

■ランサムウェア感染経験は48%、メールによる攻撃とリモートアクセスの脆弱性が主な侵入経路

国内で拡大しているランサムウェア攻撃による感染被害の経験について質問したところ、48.0%がランサムウェアの感染経験があることが分かりました。うち約半数が身代金を支払ったとしており、全体の23.8%となりました。また、システムやデータを復旧できなかった企業は25.9%となり、半数以上が復旧できておらず、ランサムウェアに感染してしまうと、システムの復旧が難しいことが分かりました。

また、ランサムウェア感染企業に対して、ランサムウェアの侵入経路を質問しました（図5）。「メールやその添付ファイル」が28.3%と最多になりました。次いで、「VPNやネットワーク機器の脆弱性」が20.8%、「リモートデスクトッププロトコルの悪用」が19.9%になりました。この結果から、依然としてメールを利用した攻撃が続いている一方で、ネットワーク機器の脆弱性やリモートデスクトッププロトコルの悪用といった、リモートアクセス経由の脅威が高まっていることが分かりました。その他、「OSやソフトウェアの脆弱性」や「Webサイトの閲覧や不正ソフトウェアのダウンロード」も一定数あります。ランサムウェアの侵入経路は多様化していると考えられ、企業はゼロトラストアーキテクチャなどによる技術的対策と、従業員へのセキュリティ教育などの組織的な対策の両面から、セキュリティ戦略を講じることが求められます。

図5．ランサムウェアの侵入経路



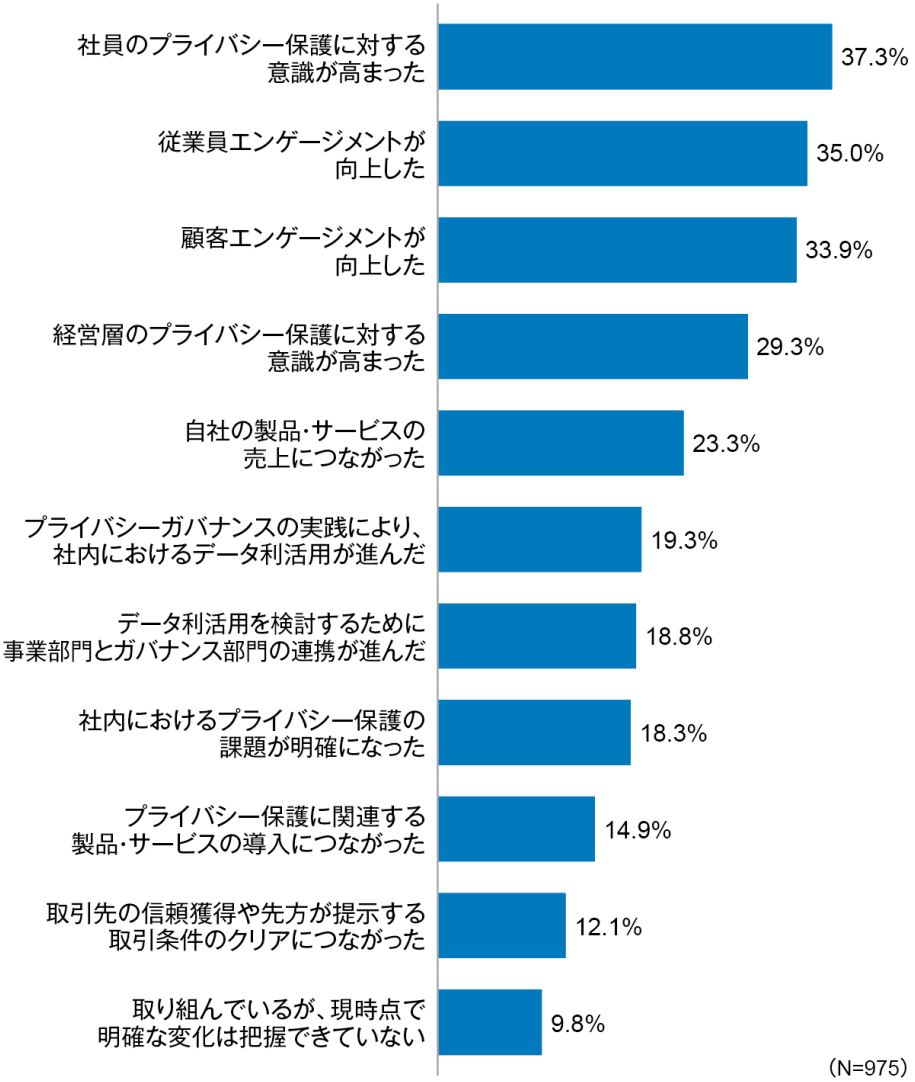
出典：JIPDEC／ITR『企業IT利活用動向調査2025』

■プライバシーガバナンスの取り組みは、従業員と顧客の双方のエンゲージメント向上に寄与

企業経営の重要事項として、組織全体でプライバシー問題の適切なリスク管理に能動的に取り組む体制を構築し、企業価値の向上につなげる「プライバシーガバナンス」の重要性が高まりつつあります。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したところ、「組織全体のプライバシー保護に関する責任者を任命」が37.9%と最も多く、次に「プライバシーガバナンスについての組織の姿勢を明文化」が32.9%、「プライバシー保護のための組織を設置」が32.4%で続きました。これらは、経済産業省／総務省が示した『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』で経営者が取り組むべき3要件として掲げられており、企業が要件に沿って適切に取り組んでいることがうかがえます。

さらに、プライバシーガバナンスに取り組んだことで生じた変化について質問しました（図6）。「社員のプライバシー保護に対する意識が高まった」が37.3%で最多となり、社内の意識改革に寄与していることが分かりました。次いで「従業員エンゲージメントが向上した」が35.0%、「顧客エンゲージメントが向上した」が33.9%で続きました。従業員エンゲージメントの向上は、組織全体でプライバシー保護を重視することが明示されることによって、従業員が企業への信頼を深めることにつながると考えられます。また、顧客エンゲージメントの向上は、プライバシーに配慮したデータ活用が企業のブランド価値を高め、顧客や取引先からの信頼を獲得する要因となることを示しています。

図6．プライバシーガバナンスに取り組んだことで生じた変化



出典：JIPDEC／ITR『企業IT利活用動向調査2025』

調査結果を受けて、ITRのシニア・アナリストである入谷　光浩氏は以下のようにコメントしています。

「企業は生成AIを導入する段階から、現在はいかにして活用するかという段階に移っており、さまざまな業務での活用が期待されています。資料作成など従業員の日常業務を中心に、すでに一定以上の成果が出ているという調査結果が示され、生成AIは活用効果の即時性が高いソリューションであることが分かりました。一方、生成AIの利用における情報漏えいやハルシネーションなどのリスクは、社内の利用範囲が広がるにつれて高くなるため、利用ルールの策定や従業員への教育、AIの管理・監視を適切に行っていくことが求められます。

ランサムウェア攻撃の脅威は続いており、すでに半数近い企業が感染経験をもち、その半数以上がデータやシステムを復旧できていません。また、主な侵入経路は、メールによる攻撃とリモートアクセスの脆弱性を狙った攻撃であることが分かりましたが、侵入経路は多様化しており、技術面と組織面でのセキュリティ対策が極めて重要となります。また、経営課題として重要性が高まっているプライバシーガバナンスに取り組んでいる企業では、従業員と顧客に対するエンゲージメントの向上において一定の効果がみられました。企業は、今後もプライバシーガバナンスに継続して取り組み、データの利活用の推進やビジネス拡大につなげていくことが重要となります。」

■本調査について

本調査は、JIPDECとITRが2025年1月17日から1月24日にかけて実施したものです。調査は、ITRの独自パネルに対するWebアンケート形式で実施し、従業員数50名以上の国内企業に勤務しIT戦略策定または情報セキュリティ施策に関わる係長職相当職以上の役職者約1万7,000名に対して回答を呼びかけ、1,110名の有効回答を得ました（1社1名）。

今回発表した動向だけでなく、企業の経営課題、情報セキュリティ対策の具体的な取り組み状況、認定／認証制度の取得状況、データ越境移転の状況、電子契約の導入状況など、広範にわたる調査を実施しています。

調査結果の詳細は後日公開予定の他、JIPDECが2025年5月下旬に発行予定の『JIPDEC IT-Report 2025 Spring』ではより詳細な分析結果を紹介する予定です。

■JIPDECについて

JIPDECは、1967年よりわが国の情報化推進の一翼を担い、技術的・制度的課題の解決に向けたさまざまな活動を展開しています。特に、安心安全な情報利活用環境の構築を図るため、プライバシーマーク制度の運営や、メールのなりすまし対策や電子証明書を発行する認証局等の信頼性を評価するトラストサービス評価事業等、個人情報の取扱いやプライバシーガバナンス等、情報の保護と活用に関する調査研究・政策提言等を行っています。

URL：https://www.jipdec.or.jp/

■ITRについて

ITRは、客観・中立を旨としたアナリストの活動をとおして、最新の情報技術（IT）を活かしたビジネスの成長とイノベーションの創出を支援する調査・コンサルティング会社です。戦略策定から、プロジェクトの側方支援、製品・サービスの選定に至るまで、豊富なデータとアナリストの知見と実績に裏打ちされた的確なアドバイスを提供します。2000年からは毎年、国内企業の情報システム責任者に対する『IT投資動向調査』を実施しています。ITRは1994年に設立、東京に本社を置いています。

URL：https://www.itr.co.jp/

■本件に関するお問い合わせ先
一般財団法人日本情報経済社会推進協会（JIPDEC）
広報室
問合わせフォーム https://www.jipdec.or.jp/jipdec_inquiry.html