



本件照会先

石井 ヤニサ、池田 直紀、新井 雄太
帝国データバンク
東京支社情報統括部
03-5919-9343(直通)
情報統括部: keiki@mail.tdb.co.jp

発表日

2026/10/19

当レポートの著作権は株式会社帝国データバンクに帰属します。
当レポートはプレスリリース用資料として作成しております。著作権法の範囲内でご利用いただき、私的利用を超えた複製および転載を固く禁じます。

情報漏洩、 企業の16.2%で発生 背景に人為ミスやサイバー攻撃

「大企業」は3割が経験
「分からない」も約15%、発生有無の把握に課題

情報漏洩に関する企業アンケート

SUMMARY

情報漏洩(可能性のある事案を含む)が『発生したことがある』企業の割合は16.2%となり、直近1年以内の発生は5.5%だった。背景には、メールの誤送信などの人為ミスに加え、サイバー攻撃による被害もみられた。特に「大企業」では3割が経験しており、「中小企業」を上回った。一方で、「分からない」と回答した企業も14.8%存在し、発生有無を十分に把握できていない企業もみられた。また、「中小企業」からは、費用面や人材面の制約により十分な対策が難しいとの声もあがった。

株式会社帝国データバンクは、全国1,328社を対象に、情報漏洩(人為ミスやサイバー攻撃による漏洩等を含む)、または情報漏洩の可能性のある事案の発生状況についてアンケートを行った。

※調査期間:2026年10月9日~10月14日(インターネット調査)

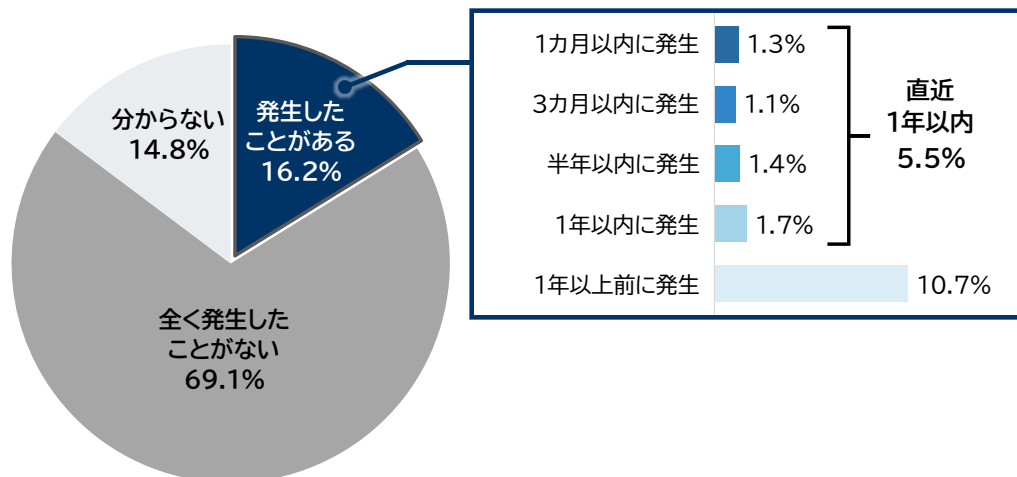
※有効回答企業:1,328社

情報漏洩、16.2%の企業で「発生したことがある」

情報漏洩(人為ミスやサイバー攻撃による漏洩等を含む)、または情報漏洩の可能性がある事案の発生状況について尋ねたところ、『発生したことがある』と回答した企業の割合は 16.2%だった。発生時期別にみると、「1カ月以内」が1.3%、「3カ月以内」が1.1%、「半年以内」が1.4%、「1年以内」が1.7%で、直近1年以内の発生は計 5.5%となった。また、「1年以上前に発生」は 10.7%だった。

企業からは、「メールの送信先を誤った」(建設、中小企業、3カ月以内に発生)といった人為ミスをあげる声が複数聞かれた。一方で、「他社担当者を装ったメールを受信し、緊急だと思い込んで電話確認を行わず情報を送付してしまった」(建設、小規模企業、1年以上前に発生)や、「外部からのサイバー攻撃を受けた痕跡がある。中小企業なので対策といっても大したことはできていないのが実情」(機械・器具卸売、中小企業、半年以内に発生)といった声も聞かれ、外部からの攻撃による被害も発生していることがうかがえた。

情報漏洩の発生経緯



注1:母数は、有効回答企業1,328社

注2:小数点以下第2位を四捨五入しているため、合計は必ずしも100とはならない

他方、『全く発生したことがない』企業は 69.1%、『分からない』企業は 14.8%だった。

『全く発生したことがない』と回答した企業からは、「情報漏洩を防ぐための教育と設備にお金をかけている」(建設、中小企業)といった声が聞かれた。一方で、「情報漏洩として問題になったことがないため、どのように対策をとるべきなのかが分からない」(建設、中小企業)のように、今後の対策に不安を抱く企業もみられた。

さらに、『分からない』と回答した企業からは、「コンピュータのデータ処理に関する専門家がいなかったため、情報漏洩があったのか、なかったのかが分からない」(不動産、小規模企業)といった声も複数聞かれた。情報漏洩の発生有無を十分に把握できていない企業もみられ、情報漏洩の実態把握や社内における共有、管理体制のあり方について課題がうかがえた。

一方で、「社内規程や訓練、インシデント対応手順の整備を進めるほか、不正アクセス対策、ウイルス対策、ログ管理、二要素認証、ファイアウォール、バックアップ体制などを導入し、高いセキュリティ環境を構築している。今後も継続的な強化を通じて社会的信頼の向上を図る」(専門サービス、小規模企業)のように、サイバーセキュリティ対策の強化に継続的に取り組む企業も少なくなかった。

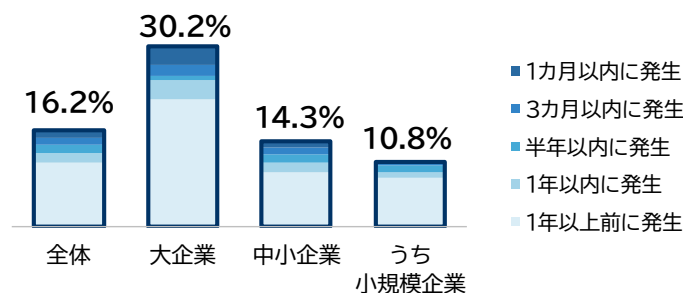
「大企業」では 3 割が情報漏洩経験あり

企業規模別に情報漏洩が『発生したことがある』と回答した企業の割合をみると、「大企業」は 30.2%と 3 割にのぼり、全体(16.2%)を 14.0 ポイント上回った。また、直近 1 年以内に発生した割合も、「大企業」の 8.8%に対し、「中小企業」は 5.0%と差がみられた。企業規模が大きいほど情報漏洩の発生経験の割合が高い背景には、取り扱う情報量やシステム数、情報にアクセスする従業員数、取引先数の多さに加え、情報漏洩や不正アクセスなどを検知・把握する体制が整備されていることなどがあると考えられる。「大企業」からは、「FAX や郵便などアナログ作業での人為的ミスが多く、デジタルに置き換えている」(金融、大企業、1 年以上前に発生)といった声が聞かれた。

一方で、「中小企業」からは、「それほど多くの情報を抱えていない」(専門サービス、小規模企業、全く発生したことがない)といったコメントが寄せられ、取り扱う情報量の違いが情報漏洩リスクに影響している可能性がうかがえた。しかし、「小規模企業なので、狙われる対象にもならないと思うが、昨今のサイバー攻撃のニュースを耳にすると他人事ではない気がする」(飲食店、小規模企業、全く発生したことがない)のように、情報漏洩の発生経験がない企業においても警戒感が高まりつつある。

また、「発生するかどうか分からないセキュリティ問題に対して、中小企業は多くのお金をかけられず、専門担当者も置けない状況にもかかわらず、業界大手の取引先からはしっかり対策するように指導がある。重要であるなら指導だけでなく金銭的、人的な協力もしてほしい」(化学品製造、中小企業、全く発生したことがない)といった声も聞かれた。大企業のサプライチェーンに組み込まれる企業ではセキュリティ対策の強化が求められるなか、費用面や人材面の制約が対策推進の課題となっている実態がうかがえた。

情報漏洩が『発生したことがある』企業の割合 ～規模別～



情報漏洩対策は「防止」だけでなく「早期把握」が重要に

本アンケートの結果、過去に情報漏洩を経験した企業は 16.2%となり、特に「大企業」では 3 割にのぼった。メールの誤送信などの人為ミスに加え、なりすましやサイバー攻撃など外部からの攻撃による被害もみられた。一方で、「分からない」と回答した企業も 14.8%存在し、情報漏洩の発生有無を十分に把握できていないケースもうかがえた。

昨今、国内企業で情報漏洩事案が相次ぎ、企業規模を問わずサイバー攻撃の脅威が高まるなか、中小企業からも警戒感を示す声が聞かれた。しかし、中小企業では費用面や人材面の制約から十分な対策が難しいとの声もあがっている。情報漏洩への対応には、技術的な対策だけでなく、従業員教育や組織内での情報共有、実態把握や兆候の早期発見、迅速に対応できる体制づくりを進めるとともに、中小企業が継続して対策に取り組める環境整備も求められる。情報漏洩を「起こさない」ための対策にとどまらず、発生時に迅速に把握し、「見逃さない」仕組みを備えることが、企業の信用を守るうえで一層重要となろう。

企業からの声	業種 51 分類	企業規模
情報漏洩が『発生したことがある』企業の声		
入社時と退職時には、秘密保持に関する説明を行うとともに、誓約書への署名を求めている。また、アンチウイルスソフトの導入など多面的なセキュリティ対策を講じている	建材・家具、 窯業・土石製品 製造	中小企業
取引先でサイバー攻撃による情報漏洩があり、現在自社内でも対策を検討している	機械・器具卸売	大企業
最近は大企業や自治体でも情報漏洩事案が多発しているが、AI を悪用したサイバー攻撃が要因であると考えている。自社でもサイバー攻撃への対策を講じる必要があるものの、多額の費用がかかるため十分な対応は容易ではない。国による支援や対策の強化を期待したい	専門商品小売	大企業
メールの CC で誤配信をしてしまった	運輸・倉庫 (一般貸切旅客 自動車運送)	大企業
メールやグループウェアの利用時に他社の資料を誤って添付したり、他社資料を参考に作成した資料から不要な情報を削除しきれなかったりするなど、人為的なミスが発生した。そのため、資料をメールに添付することを原則として避けるほか、資料の再利用を控え、テンプレートの利用を促進するなどの対策を講じている	専門サービス	小規模企業
情報漏洩が『全く発生したことがない』/『分からない』企業の声		
現在、大手各社の情報漏洩がニュースで報道されているが、中小零細企業では対策しても限界があり難しいと考える	不動産 (不動産代理業・ 仲介)	小規模企業
情報漏洩防止に向け、全社員に対して継続的な教育を実施している	機械製造	中小企業
外部と遮断された環境で業務を行い、機密情報や個人情報へのアクセスを厳格に制限している。個人情報を扱う部署も完全に隔離された環境で運用しており、現時点で重大な情報漏洩は発生していない	飲食料品小売	大企業
情報漏洩対策ツールを導入している	専門商品小売	中小企業
自社では顧客情報を主に紙媒体で管理しており、保有するデータは限定的である。一方で、取引のある OTA(オンライン旅行会社)事業者における情報漏洩リスクについては懸念している	旅館・ホテル	中小企業
情報漏洩やサイバー攻撃に気付いていないだけかもしれないが、現時点では発生していないと思う。なお、対策は行っている	専門サービス	小規模企業
情報管理業務は十分なスキルと安全意識を備えた担当者に限定している。従業員教育や業務フローの見直しに加え、メールや添付ファイルの取り扱いルールを厳格化し、情報漏洩防止に努めている	メンテナンス・ 警備・検査	中小企業

調査先企業の属性

1.有効回答企業:1,328 社

規模			業界			地域		
	大企業	159		農・林・水産	17		北海道	56
	中小企業	1,169		金融	12		東北	100
	うち小規模企業	461		建設	191		北関東	103
	全体	1,328		不動産	61		南関東	426
				製造	311		北陸	69
				卸売	262		東海	147
				小売	112		近畿	183
				運輸・倉庫	49		中国	89
				サービス	306		四国	32
				その他	7		九州	123
				全体	1,328		全体	1,328

2.企業規模区分

中小企業基本法に準拠するとともに、全国売上高ランキングデータを加え、下記のとおり区分。

業界	大企業	中小企業(小規模企業含む)	小規模企業
製造業その他の業界	「資本金 3 億円を超える」かつ 「従業員数 300 人を超える」	「資本金 3 億円以下」または 「従業員数 300 人以下」	「従業員数 20 人以下」
卸売業	「資本金 1 億円を超える」かつ 「従業員数 100 人を超える」	「資本金 1 億円以下」または 「従業員数 100 人以下」	「従業員数 5 人以下」
小売業	「資本金 5 千万円を超える」かつ 「従業員数 50 人を超える」	「資本金 5 千万円以下」または 「従業員数 50 人以下」	「従業員数 5 人以下」
サービス業	「資本金 5 千万円を超える」かつ 「従業員数 100 人を超える」	「資本金 5 千万円以下」または 「従業員数 100 人以下」	「従業員数 5 人以下」

注 1: 中小企業基本法で小規模企業を除く中小企業に分類される企業のなかで、業種別の全国売上高ランキングが上位 3% の企業を大企業として区分

注 2: 中小企業基本法で中小企業に分類されない企業のなかで、業種別の全国売上高ランキングが下位 50% の企業を中小企業として区分

注 3: 上記の業種別の全国売上高ランキングは、TDB 産業分類(1,359 業種)によるランキング