

福岡県・サイバー攻撃 32.5%で「経験あり」 大企業への攻撃目立つ

直近で中小企業の被害が急拡大



本件照会先

秋山進（調査担当）
帝国データバンク
福岡支店 情報部
092-738-7779（直通）
tdb.fukuoka@mail.tdb.co.jp

発表日

2025/07/15

福岡県・サイバー攻撃に関する実態調査(2025 年)

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。

SUMMARY

過去にサイバー攻撃を受けたことが『ある』企業の割合は 32.5%だった。規模別では、「大企業」が 53.3%で最も多く、「中小企業」が 28.1%、うち「小規模企業」が 25.7%だった。最近では、大企業よりも対策が比較的手薄な中小企業の被害増加が顕著になっている。企業は、サイバー攻撃を他人事と捉えず、BCP の一環として対策を整備していくことが重要である。

※株式会社帝国データバンク福岡支店は、福岡県 2,592 社を対象に「サイバー攻撃」に関するアンケート調査を実施した。

調査期間：2025 年 5 月 19 日～5 月 31 日（インターネット調査）

調査対象：福岡県 2,592 社、有効回答企業数は 910 社

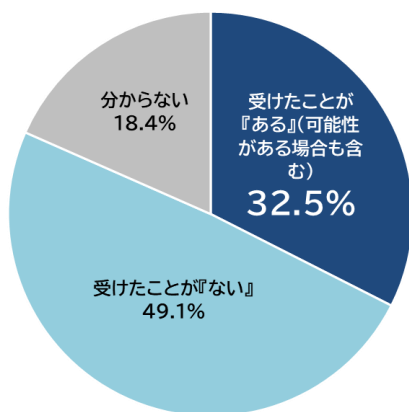
サイバー攻撃、 32.5%で「経験あり」 大企業への攻撃目立つ

過去にサイバー攻撃を受けたことがあるか尋ねたところ、受けたことが『ある』（「1カ月以内に受けた（可能性がある場合も含む）」「3カ月以内に受けた（同）」「半年以内に受けた（同）」「1年以内に受けた（同）」「過去に受けたが、1年以内に受けていない」の合計）と回答した企業の割合は32.5%だった。

他方、過去に受けたことが『ない』企業は49.1%、『分からない』企業は18.4%だった。

サイバー攻撃の有無と「規模別」「業界別」のサイバー攻撃の経験割合

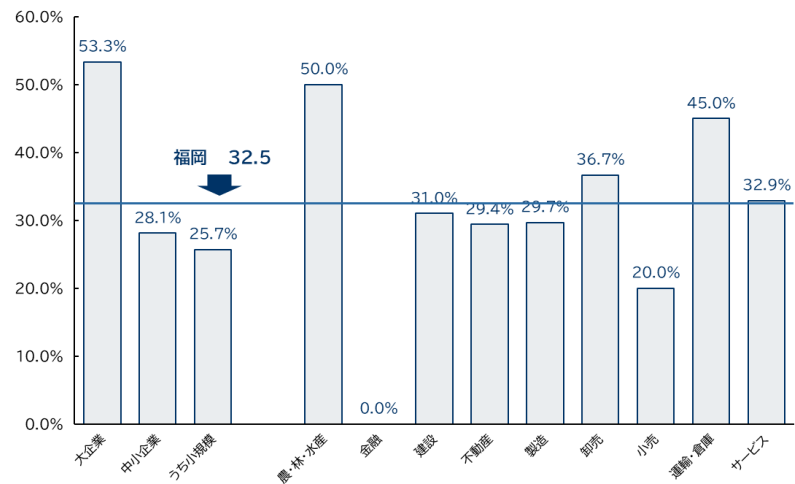
サイバー攻撃の有無



注1:母数は、有効回答企業348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。

「規模別」「業界別」サイバー攻撃の経験割合

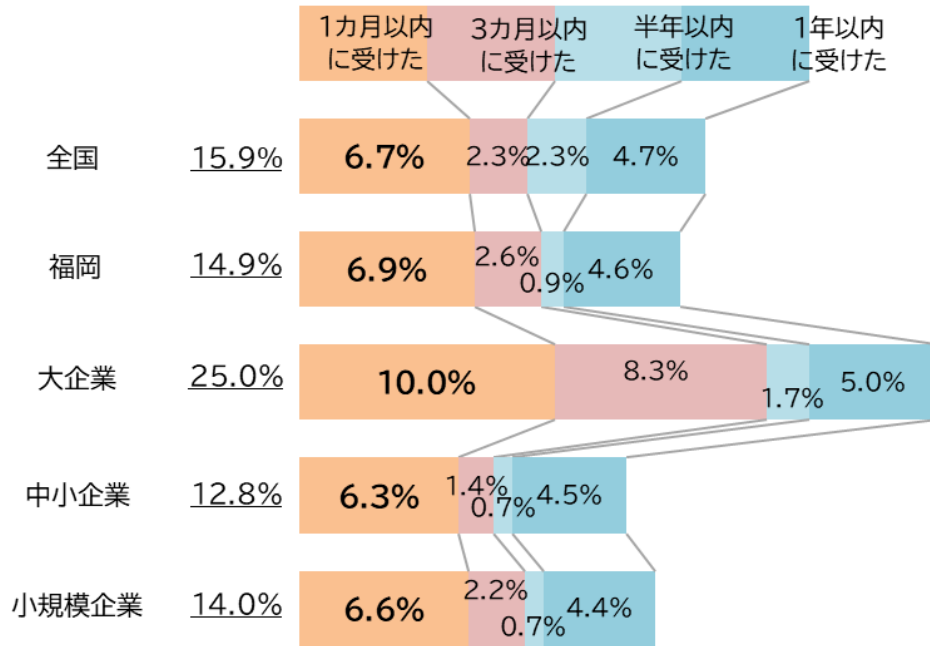


規模別では、「大企業」が53.3%、「中小企業」が28.1%、うち「小規模企業」が25.7%となった。とりわけ、「大企業」のサイバー攻撃を受けている割合は、全体より20ポイント以上高く、規模が大きいほど割合が高くなっている。

また、サイバー攻撃を「1カ月以内に受けた（可能性がある場合も含む）」企業は全体で6.7%であったが、「中小企業」は6.9%、うち「小規模企業」は7.9%だった。また、「1カ月以内に受けた（可能性がある場合も含む）」と回答した「中小企業」と「小規模企業」の割合は「1年以内の他の期間に受けた」とする回答より高く、足元では中小企業のサイバー攻撃に対するリスクが急速に高まっている。

2025年3月13日に警察庁が発表した「令和6年におけるサイバー空間をめぐる脅威の情勢等について」によると、2024年の中小企業のランサムウェア被害件数は2023年より37%増加した。また、この被害による事業への影響も長期化・高額化している。近年、ランサムウェアの攻撃が多様化しているなか、対策が比較的手薄な中小企業の被害増加が顕著になっている。企業は、サイバー攻撃を他人事と捉えず、BCP（事業継続計画）の一環として対策を整備していくことが重要である。

「規模別」1年以内のサイバー攻撃の経験割合



注1:母数は、有効回答企業のうち、全国1万645社、福岡348社、大企業60社、中小企業288社、小規模企業136社

注2:大企業、中小企業、小規模企業は、福岡の企業

注3:小数点以下第2位を四捨五入しているため、内訳と合計は必ずしも一致しない

注4:いずれも可能性がある場合も含む

<参考> 企業からの声

企業からの声	業種 51 分類
サイバー攻撃への対策や内容	
BCP は必須外部環境変化が激しいなか、企業の持続性を鑑みて事前の準備は必要という認識	包装用品卸売業
外的要因に不確定要素が大きくなっている現状では策定は急務と感じている	その他の卸売業
自社の経営課題抽出の機会と捉え、前向きに取り組む必要がある	機械製造業
サイバー攻撃に関する BCP 策定の予定がない理由や課題	
少人数なので、その場の判断で対応できると見込んでいる。	鉄鋼・非鉄・鋳業
自前のサーバーを持っている為)火災や水害で焼失、水没しない限り復元可能なため。	運輸・倉庫
なにをどこから策定していいのか、わからない。	各種商品小売業