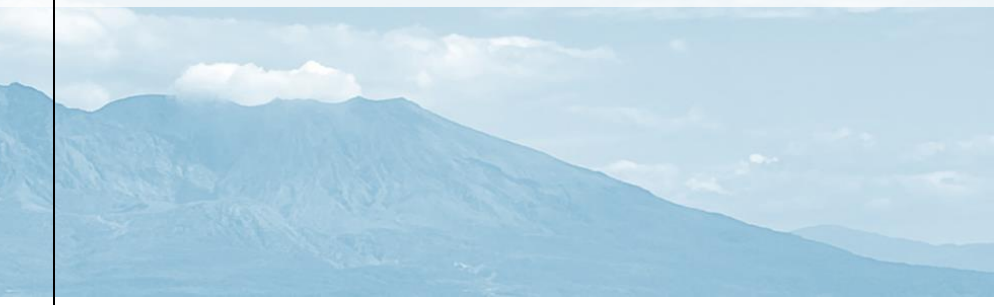
TDB Business View
2025/07/22

サイバー攻撃 企業の 32.3%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

鹿児島県・サイバー攻撃に関する実態調査（2025 年）



帝国データバンク

本件照会先

日比生　秀一（支店長）
帝国データバンク
鹿児島支店
099-223-8208
info.kagoshima@mail.tdb.co.jp

発表日

2025/07/22

SUMMARY

鹿児島県内で過去にサイバー攻撃を受けたことが『ある』企業の割合は 32.3%だった。規模別では、「大企業」が 57.1%で最も多く、「中小企業」が 30.3%、うち「小規模企業」が 25.0%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。

＊事業継続計画（BCP）とは、自然災害・感染症等の不測の事態が発生した場合に備えるために、身体、生命の安全確保に加え、重要な事業を中断させない、また中断しても可能な限り短い期間で復旧させるための方針・体制・手順を示した計画。

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：鹿児島県企業 303 社、有効回答企業数は 96 社（回答率 31.7%）

サイバー攻撃、
企業の 32.3%で経験あり　大企業への攻撃目立つ

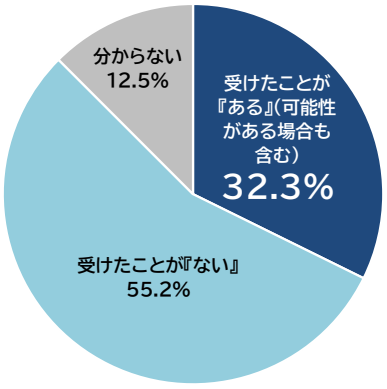
過去にサイバー攻撃を受けたことがあるか尋ねたところ、受けたことが『ある』(「1カ月以内に受けた(可能性がある場合も含む)」「3カ月以内に受けた(同)」「半年以内に受けた(同)」「1年以内に受けた(同)」「過去に受けたが、1年以内に受けていない」の合計)と回答した企業の割合は 32.3%だった。他方、過去に受けたことが『ない』企業は 55.2%、『分からない』企業は 12.5%だった。

規模別では、「大企業」が 57.1%、「中小企業」が 30.3%、うち「小規模企業」が 25.0%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 24.8 ポイント高く、規模が大きいほど割合が高くなっている。

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 4.2%であったが、「中小企業」は 4.5%、うち「小規模企業」は 2.5%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」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。

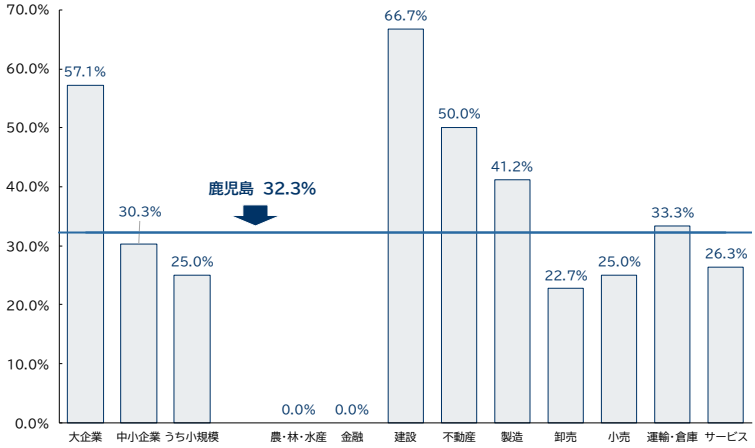
サイバー攻撃の有無と「規模別」「業界別」のサイバー攻撃の経験割合

サイバー攻撃の有無

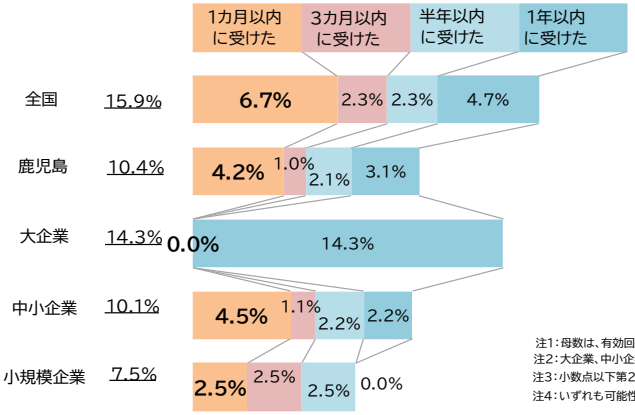


注1:母数は、有効回答企業96社
注2:小数点以下第2位を四捨五入しているため、合計は必ずしも100とはならない
また、内訳も必ずしも一致しない

「規模別」「業界別」サイバー攻撃の経験割合



「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、鹿児島96社、大企業7社、中小企業89社、小規模企業40社
注2:大企業、中小企業、小規模企業は、鹿児島の企業
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

まとめ

本調査の結果、鹿児島県において過去にサイバー攻撃を受けたことがある企業の割合は 32.3%であった。規模別でみると、大企業で 57.1%、中小企業で 30.3%と、大企業への攻撃が目立ったものの、直近では中小企業への攻撃の割合が伸びており、規模を問わず、サイバー攻撃に対するリスクが高まっていることが分かった。

企業からは、「サイバー攻撃によるシステムダウンに備え、紙媒体などアナログ対応で業務を乗り切るシミュレーションが必要」や「緊急時の対策構築に万全を期すことに超したことはないと思う」「事前に準備をしておくことで、有事の際にスムーズに対応出来る」など、対策に前向きな声があがった。

「商工会議所の支援を受けている」や「専門業者に依頼してウイルス対策を実施している」など、実際に対策を講じている企業もある一方で、「策定した方が良いとは思うが、時間・費用面に余裕がない」など、対策が後回しになっている企業も多い。また、「少人数の企業なので、その都度の判断で対応できると感じている」など、小規模企業では特段の対策の必要は感じていない向きも多かった。

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。

＜参考＞企業からの声（全国の回答から抜粋）

企業からの声	業種 51 分類
サイバー攻撃への対策や内容	
サイバー攻撃によるシステムダウンが発生すると、業務を中断せざるを得ない。現状の対策に加え、万が一に備え、紙媒体などアナログ対応で業務を乗り切るシミュレーションが必要	建材・家具、窯業・土石製品卸売
特に、サイバー攻撃は実務的にも会社の評価的にも多大な影響を及ぼすことがあるため、対策は必須と思われる。従業員が少しでも意識するためにも BCP 対策は必要	化学品卸売
商工会議所の支援を受けている。3月頃、異常を検知したとの報告があり、社内の総点検を行い、検知された PC の切断を行った	機械・器具卸売
弊社は間接受注の業務が多い専門分野のため、元請会社に対してのサイバー攻撃によるコンピューターウイルス感染は絶対に避けなければならず、専門業者に依頼してウイルス対策を実施している	専門サービス
サイバーテロについては、専門部署がないため十分な情報収集ができないが、対策は親会社から実施、展開してもらっている	メンテナンス・警備・検査
自然災害やサイバー攻撃など多様化する時代に会社存続のため出来うることを共有することは、一企業だけではなく業界内での対策も必要だと感じる	飲食料品小売
小規模企業のため、BCP は人材の安全確認とネットワーク・サイバーセキュリティに尽きる。ネットワーク・サイバーセキュリティは一定の備えを実施しているが、通信会社のネットワークが寸断されたら対処のしようがない	建材・家具、窯業・土石製品卸売
ランサムウェアを停止させ暗号化データを即時復旧させる自社製品の導入、UTM などによる防御、クラウドバックアップからの復旧と万全を期している	機械・器具卸売
サイバー攻撃に関する BCP 策定の予定がない理由や課題	
個人スキル（知財）かつ数人の会社であり、各人が活動可能であれば良く、また、個別のリスク対策（セキュリティ強化、サイバー保険加入等）を実施しており、あえて BCP を策定する必要を感じない	専門サービス
サイバー攻撃を受けたことがなく、その費用対効果が感じられないため	電気・ガス・水道・熱供給
必要性は感じるが、 地震、火災、感染症、サイバー攻撃、テロ、軍事紛争など対象が多岐にわたるため作成が非常に困難	繊維・繊維製品・服飾品小売