

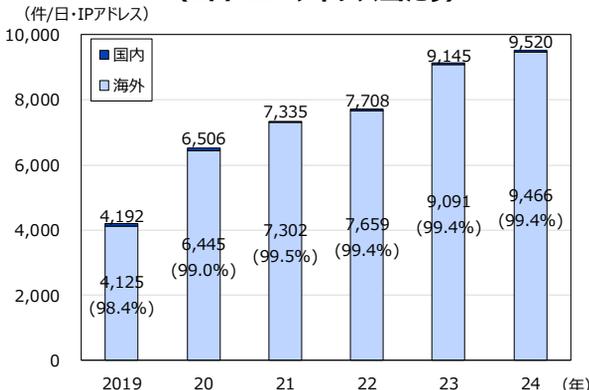
中小企業に求められるサイバーセキュリティ対策 ～組織的対応を行っていない中小企業は7割～

不審なアクセスは過去5年で倍増

情報通信技術の進展に伴い、サイバーセキュリティの重要性がますます高まっています。サイバー攻撃前にシステム中の攻撃可能な部分を探す「脆弱性探索行為」等の不審アクセス件数は、2024年には9,520件（1日・1IPアドレスあたり）と過去5年間で倍増しており、その大半が海外を送信元としています（図表1）。

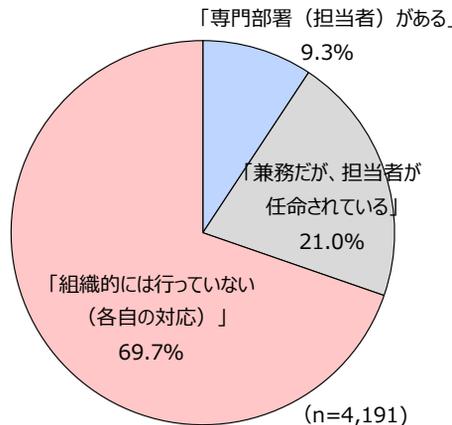
そして、こうしたサイバー攻撃は、対策が手薄な中小企業を標的にするケースが増えていますが、情報処理推進機構が2024年に実施した調査によると、セキュリティ対策を「組織的には行っていない（各自の対応としている）」中小企業は約7割に達しています（図表2）。

図表1 警察庁が検知した不審なアクセス件数
(1日・1IPアドレスあたり)



(資料) 警察庁「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」より、ひろぎんHD経済産業調査部作成

図表2 自社のセキュリティ対策状況



(資料) 情報処理推進機構「2024年度中小企業における情報セキュリティ対策の実態調査報告書」より、ひろぎんHD経済産業調査部作成

「予防」と「被害抑制」両面の対策を

サイバー攻撃被害のリスクを低減するためには、「予防」と「被害抑制」の両面について対策することが重要です（図表3）。まず、「予防」体制の構築には、社員教育に加えて、初期投資を抑えつつ高度なセキュリティ機能を利用できるクラウドサービスの活用などが有効です。

また、攻撃を受けた後の初動対応が遅れると、復旧に時間や費用を要するため、「被害抑制」も不可欠です。これには、事業継続計画（BCP）を策定して対応手順を明確化し、定期的に訓練することが重要です。

上記調査では、サイバー被害を受けた中小企業のうち約7割が「取引先にも影響があった」としています。サイバーセキュリティ対策は各社員の対応ではなく、補助金等の政府支援を活用しつつ、効果的かつ組織的に取り組むことが急務となっています。

図表3 中小企業のサイバーセキュリティ対策例

予防	<ul style="list-style-type: none"> ✓ セキュリティ教育とトレーニング ✓ インターネットアクセスルールの制定 ✓ クラウドサービスの活用 ✓ 定期的なバックアップ 等
被害抑制	<ul style="list-style-type: none"> ✓ 事業継続計画（BCP）の策定 ✓ 対応手順の明確化 ✓ 定期的な訓練 ✓ ログの監視と分析 等

(資料) 各種資料より、ひろぎんHD経済産業調査部作成

- ◆ 本資料は情報提供のみを目的として作成されたものであり、何らかの行動を勧誘するものではありません。
- ◆ 本資料は、信頼できるとされる情報に基づいて作成されていますが、その正確性を保証するものではありません。また、本資料に記載された内容等は作成時点のものであり、今後予告なく修正、変更されることがあります。資料のご利用に関しては、お客さまご自身の責任において判断なされますよう、お願い申し上げます。
- ◆ 本資料に関連して生じた一切の損害については、責任を負いません。その他、専門的知識に係る問題については、必ず弁護士、税理士、公認会計士等の専門家にご相談のうえ、ご確認ください。
- ◆ 本資料の一部または全部を、当社の事前の了承なく複製または転送等を行うことを禁じます。
- ◆ 本件に関するご照会は、ひろぎんHD経済産業調査部 担当：古谷（TEL082-247-4958）までお願いします。