中小企業 と サイバーセキュリティ

第6回「ランサムウェアの主な被害者は中小企業です」

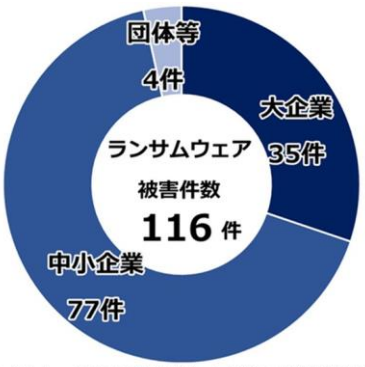
前回までは「お手軽サイバー防犯対策」として身近な予防策を紹介してきましたが、今回はランサムウェアという深刻な脅威に焦点を当てます。

昨年秋、大手飲料メーカーがランサムウェアの被害を受け、受注や出荷業務が停止する事態となり、多くの方に衝撃を与えました。大企業でも被害を免れないのですから、中小企業にとっても決して他人事ではありません。実際、警察庁の統計によれば、被害の多くは中小企業なのです。

被害に遭えば、納品遅延や信用失墜、収益減少、復旧費用など連鎖的な影響は避けられません。

大企業の事例は「自分たちも同じ状況に陥り得る」という現実を示しています。

特に注意すべきは、VPNの脆弱性です。警察庁の統計では、ランサムウェア被害の多くがVPN経由で発生しています。アップデートや修正パッチが適用されず、既知の欠陥を抱えたまま使われていることが原因で、攻撃者に侵入の糸口を与えてしまいます。対策としては、最新のファームウェアやセキュリティパッチの適用、不要な機器の停止、利用状況の監視が有効です。

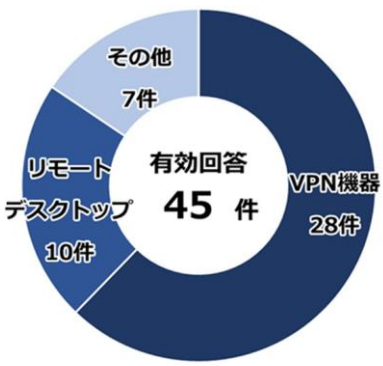


ランサムウェア被害の被害企業・団体等の規模別報告件数
警察庁「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について」より

次に重要なのが、BCP（事業継続計画）の整備です。災害は短期で復旧できる場合もありますが、サイバー事案では数か月以上かかることもあります。

長期戦を想定したBCPを整えておくことで、事業停止の影響を最小限に抑えられます。

さらに、事業者同士の共助関係の構築をはかると良いでしょう。不審メールの共有や合同研修など、簡単な取り組みでも効果があり、費用や人材不足を補えます。競争相手であっても、事案の前では同じ立場です。地域や業界で協力し合うことが、事業活動を維持する力になります。



ランサムウェアの感染経路
警察庁「令和7年上半期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

ランサムウェアは特別なものではなく、日常的なリスクです。中小企業が自社を守ることは、取引先や地域社会を守ることにもつながります。

ぜひ「VPN脆弱性への対策」、「BCPの整備」、「共助助の関係づくり」を意識して、現実的な一歩を踏み出しましょう。

神奈川県警察サイバーセキュリティ対策本部

※ この記事は川崎市産業振興財団機関紙「産業情報かわさき(2026年2月号)」に掲載されたコラムを再編集したものです。