されておらず、過去3年間にサイバー攻撃（インターネット犯罪）の被害に遭った中小企業のうち、約7割で取引先にも影響が及んだとされています。

セキュリティ対策が不十分なせいでサイバー攻撃の被害を受け、取引先にも大きな迷惑をかけてしまったら…。これが根拠のない杞憂とは言えないことが、調査で明らかになったのです。

以下に、実際に起きた事例を踏まえながら、サイバー攻撃の主な手口と今すぐ始められるセキュリティ対策を見ていくことにしましょう。

「うちは大丈夫」という油断が被害を招く

2024年6月、書籍や雑誌、ゲームなど幅広くコンテンツを提供している大手出版社のKADOKAWAが、ランサムウェア（身代金を要求するコンピュータウイルスの一種）を含む大規模なサイバー攻撃により、個人情報を含む機密情報が漏洩した旨を発表しました。これほど知名度の高い、恐らくセキュリティ対策にも相当な力を入れていたはずの企業ですら、こうしたサイバー攻撃を防ぎ切れなかった、しかも被害が広範囲に及んでしまったという事実は、多くの関係者に衝撃を与えました。

では、セキュリティ対策に潤沢な予算や人員を割けない中小企業が同様のサイバー攻撃を受けた場合、どうなるでしょうか。そう、対応に必要なリソースやノウハウが足りず、被害がより大きくなる可能性が高いのです。「うちは有名じゃないから大丈夫」という油断は、攻撃者にとってむしろ好都合かもしれません。

独立行政法人情報処理推進機構（IPA）の「情報セキュリティ10大脅威」など、中小企業が被害に遭った具体例は様々な媒体で紹介されています。例えば、地方にある従業員数十名規模の中小製造業がランサムウェアに感染し、社内サーバー上の設計図データや顧客情報が軒並み暗号化されてしまった事例。その結果、業務が2週間ほど停止し、納期が遅れ、多額の損失を被ったと報じられています。

調査を進めると、ウイルス対策ソフトこそ導入していたものの、ライセンスが切れたままで、定義ファイル（ウイルス情報）も古いままだったことが判明しました。さらに、クラウド上にデータを保管する仕組みもなく、バックアップが不十分だったため、復旧作業に膨大な時間とコストがかかったと言います。

経営者は、「もっと早くセキュリティ対策に注力していれば、このような事態は防げたかもしれない」と悔やんでいたそうです。

ビジネスメール詐欺で数百万円を振