ニューノーマル処方箋（第59回）

サイバー攻撃による被害を防ぐために、企業が考えるべきセキュリティのポイント

2025.03.07

2025年2月13日、NTT西日本グループが開催したオンラインセミナー「【元防衛省のサイバーセキュリティ専門家が解説！】企業の考えるべきサイバーセキュリティのポイント」に、NTTチーフ・サイバーセキュリティ・ストラテジストの松原美穂子が登壇。サイバー攻撃の現状と事例、そして企業が考えるべきサイバーセキュリティのポイントについて解説した。

＜目次＞

◆被害増すランサムウエア攻撃、損害賠償につながる恐れも

増加の一途をたどるサイバー攻撃。その被害額はなんと世界全体のGDPの1割にも及ぶという。数字だけで見れば、日本のGDPを大きく上回るほどの金額が毎年、サイバー攻撃で失われているのだ。しかも、これはサイバー犯罪者による攻撃のみの損失であり、国家による妨害活動なども含めると被害額はさらに増大する。

こうしたサイバー攻撃をどこか人ごとのように捉えてはいないだろうか。企業の大小を問わず、サイバー犯罪者は常に私たちの隙を狙っている。甚大な被害を受ける前に、企業はサイバーセキュリティ対策を徹底しなければならない。

サイバー攻撃と一口にいってもさまざまな種類があるが、近年特に著しい増加を見せているのがランサムウエアによる被害だ。いわゆる身代金要求型ウイルスである。サイバー犯罪者はコンピューターウイルスなどを介して企業のデータを窃取したりシステムを乗っ取ったりして金銭を要求する。

国内事例としては、2024年5月に情報処理・印刷サービスを提供する企業がランサムウエア攻撃を受け、サービスの提供を停止する事態に陥った例がある。この企業は、業務が終了した際に顧客から預かったデータを削除する契約になっていたにもかかわらず、作業を効率化するためサーバーに保管していた。そのうえ、強固なサイバーセキュリティ対策をしていなかったため、攻撃によってデータを一気に盗まれ、委託元の個人情報が少なくとも150件以上漏えい。指名停止や損害賠償請求につながってしまった。

こうしたランサムウエア被害が多く発生しているのは、日本の基幹産業ともいえる製造業だ。他にも卸売業や小売業、サービス業、建設業など多方面が狙われている。最大の原因はVPN装置の脆弱性を突いたサイバー攻撃だ。例えばパスワードをデフォルトのまま放置し、被害に遭うケースが後を絶たない。

日本企業の場合、ランサムウエアに一旦感染してしまうと、平均して約2週間は業務停止が続くとされている。サイバー犯罪者に身代金を支払えば早急に解決するのかというと、そんなことはない。身代金を支払い、全データを復旧できた企業はわずか8%に過ぎない。さらに身代金を支払えば、犯罪者にとってその企業は「脅せば金を払ってくれる」対象と認識されてしまい、再び攻撃対象になるケースも多いのだ。

ランサムウエア攻撃により倒産に至った企業もある。とある物流企業はコロナ禍を機にデジタル化に着手し、リモートアクセスを可能にしたが、サイバーセキュリティ対策が行き届かず設定変更からわずか2日後に被害に遭ってしまった。その影響で復旧や再発防止にコストがかさみ、さらに一部の取引先から契約を解除されたことが原因で、1年後に倒産したのだ。

ランサムウエア以外で被害が多く発生している手口が、企業の公式SNSの乗っ取りだ。とある企業では公式アカウントが乗っ取られ、それまでの全投稿が削除された。そのうえ無関係の他国の企業の商品紹介が投稿されるようになった。SNSが乗っ取られるとブランドを毀損するような情報を発信される恐れがある他、DMを使ってフォロワーになりすましメッセージが送信されるリスクもある。SNSの乗っ取りは二要素認証を施す対策が有効なので、しっかりと行っておきたい。

さらに、サポート詐欺にも注意が必要だ。コンピューター上でサイトを閲覧中に偽の警告画面を表示し、サポート窓口に電話をかけてきた人にソフトをインストールさせる手口である。最近では大手ドラッグチェーンが被害に遭い、ユーザーや社員の個人情報を窃取されたケースもある。この他、取引先や自社の経営者を装って偽メールを送信し、入金などを促すビジネスメール詐欺も増えている。

◆サイバーセキュリティ重要5カ条、すべて実施できている企業は1割… 続きを読む