

沢辺税理士事務所通信

令和 8 年 11 月 1 日号
NO. 153

※※※　AI時代のサイバー攻撃と情報防衛　※※※

2026 年 9 月頃から、日本での不正アクセス・サイバー攻撃による大規模な情報流出が相次いでおります。特に件数の多かったものでは佐川急便「お荷物問い合わせサービス」5,323 万件、無印良品「ＭＵＪＩアプリ」2,726 万件、タイムズカー660 万件など、かなり衝撃的な件数になっています。またタイムズカーでは漏洩した情報の質も重く、うち 146 万件は本人確認書類画像まで外部送信された痕跡がある、とされています（私の情報も含む・・）。

またＧＭＯグループでは情報漏洩に加えて、ＦＸ口座内で勝手に不正な取引が行われ金銭被害が発生し、さらに犯人側が身代金 5,000 万ドル（約 80 億円）を要求、これに応じなかった場合は毎日正午に取得した情報を順次公開していくと宣言し、実際に 10 月 27 日に 1 件の個人情報が公開されました（情報の真偽については不明）。もっとも、その後攻撃者側のサイトがアクセス不能になったことによりそれ以上の情報は現時点では公開されていないようです。

このような話は中小企業や個人の一般生活者にも全く例外ではなく、サイバー攻撃被害の 6 割は中小企業であり、被害にあった際にはその約 7 割で取引先にも影響が及んでいると言われています。ではこのような被害に合わないために、どのような対策を行っていけばいいでしょうか。

個人のパスワードに関しては使いまわしすることをやめ、パスワードマネージャーを使う方法があります。異なるサイトごとに予測不可能な複雑なパスワードを自動で作成してくれ、次回にアクセスした際にはパスワードマネージャーが自動で各サイトごとのログイン情報を入力してくれます。

また今年の春先に証券口座の乗っ取りが多発しましたが、それ以降くらいから特にパスキーが使われることが増えてきました。これはスマホの生体認証などを使ってログインするため、攻撃者が盗み出す「パスワードという文字列」そのものが存在しません。さらに正規サイトのドメインと認証情報が結びついているため、うっかり偽サイトに誘導されてしまっても認証情報を盗まれることがありません。そのためフィッシング詐欺（偽サイトにパスワードを打ち込ませて盗む手口）に特に有効と言われています。

中小企業・事業者がすべき対策は、3-2-1 ルールに基づくバックアップ体制の点検です。データを 3 つ（原本＋バックアップ 2 つ）保持する、2 種類の異なる媒体・方式で保存する、1 つはネットワークから切り離したオフライン環境や、外部から改ざん・削除できない環境に保管する、という体制を構築することです。また社内のネットワーク機器が古くなっていないかの確認も大切です。その脆弱性を突いて社内ネットワークに侵入される可能性があるので、必要に応じて最新版への更新や機器の交換などの措置を取ります。

これらの攻撃の激増は、ＡＩの発展と密接につながっています。ＡＩが、今まで人間が見つけられていなかったシステムの脆弱性を見つけ出したり、攻撃を効率化させているからです。さらに人間の操作なしにＡＩが攻撃を行っている事例も出始めています。これがＡＩによる「2030 年人類滅亡論」を荒唐無稽な話では無くさせているのです。

沢辺税理士事務所　　株式会社沢辺会計コンサルタント
〒732-0811　広島市南区段原三丁目3番27号　段原メディカルビル3階
TEL 082-236-3935　FAX 082-236-3936　HP: http://www.sawabe-ac.jp