今月の特集

中小企業のセキュリティ対策

ランサムウエア対策強化を

（独立行政法人情報処理推進機構・江島将和）

25年も被害が多発　3分の2は中小企業

ランサムウエアが猛威を振るっている。ランサムウエアとは、パソコンやサーバーに感染後、端末のロックやデータの窃取、暗号化を行い、これらを取引材料としたさまざまな脅迫により金銭を要求するマルウエア（悪意のあるソフトウエア）の一種である。2025年の主な被害報道としては、２月に大手保険企業がランサムウエア攻撃を受けて、データサーバーの一部で保管しているファイルが暗号化されるとともに、保険契約に関する個人情報など約510万件が流出した可能性を発表した。

４月には、大手物流企業にてサーバーがランサムウエア攻撃を受けて、業務にシステム障害が発生し、国内外の物流に影響を及ぼした。９月には、大手飲料企業がランサムウエア攻撃を受け、システム障害の影響で、国内工場の生産を停止するなどの被害が発生し、今も調査・対応が続いている。

警察庁の発表によると、25年上半期におけるランサムウエアの被害報告件数は116件であり、半期の件数として22年下半期と並び最多となった。組織規模別の被害件数で見ると、中小企業からの被害報告は77件となっており、全体の３分の２を占めている。大手企業の被害報道が目につくが、依然として中小企業が狙われている状況が続いている。

ランサム攻撃による被害のイメージ

基本対策を確実に　バックアップも重要

ランサムウエア対策としては、基本的な情報セキュリティ対策を確実に実施することが重要である。基本的な情報セキュリティ対策とは、①ソフトウエアの更新を行う②セキュリティソフトを利用する③パスワードの管理・認証強化を行う④設定の見直しを行う⑤脅威・手口を知る――ことであり、独立行政法人情報処理推進機構（IPA）では「情報セキュリティ５か条」と呼び実施を推奨している。

近年のランサムウエア攻撃は、VPN（仮想専用線）やリモートデスクトップ用の機器からの侵入が大半を占めている。その原因としては、当該機器の脆弱（ぜいじゃく）性を放置していたことや、ID・パスワードが安易であったこと、不必要なアカウントが適切に管理されずに存在していたことなどが挙げられる。このような手口を知り、ソフトウエアの更新や認証強化、設定の見直しを行うことで、被害に遭う確率は大幅に低減することが期待できる。

基本的な情報セキュリティ対策に加えて、データのバックアップも実施していただきたい。暗号化されたデータは金銭を支払っても確実に復旧できるとは限らない。従って、バックアップは最後のとりでとなる。バックアップをとる際は、ランサムウエアの感染拡大の影響を受けないように、ネットワークから隔離して保管することを推奨する。また、バックアップから問題なくデータを復元できるかテストを行っておくことも推奨する。

IPAではランサムウエア対策特設ページを公開し、対策情報や従業員教育用のコンテンツ、外部参考サイトなどを紹介している。自社の対策強化のために活用いただきたい。

（会議所ニュース10月21日号（日本商工会議所発行）より転載）

「ランサムウエア対策特設ページ」についてはこちら