サイバーセキュリティ最前線

急拡大するリモートワークのスキをつく サイバー攻撃に要注意!!

経済産業省が昨年末、サイバー攻撃について注意喚起を行ったなかでも、「中小企業を巻き込んだサプライチェーン上での攻撃パターンの急激な拡がり」が大きな問題に。そこで、今号ではその最新事例を参照しつつ、有効な対策について考えてみたい。

サプライチェーン上での攻撃が拡大

「サプライチェーン」を通したセキュリティ管理の徹底が、中小企業にとって喫緊の課題となっている。たとえばこの3月、千葉県芝山町が総合計画策定支援業務を委託している業者のサーバーに対して、第三者による不正アクセスが行われたことが確認されたという。これにより、サーバーで保管されていた町民意識調査票を発送するために必要な氏名・住所などの個人情報が流出した可能性がある。また、同じ業者に業務委託していた総務省も、約6700人分の個人情報が流出していた可能性を公表した。

こうしたなか、情報処理推進機構（IPA）が「ニューノーマルにおけるテレワークとITサプライチェーンのセキュリティ実態調査」を実施、その最終報告が公開された。それによると「会社が許可していないアプリケーションやサービスの業務利用」についての設問に対する回答を区分した結果、規模が小さい企業ほど「一時的に『やむを得ず』認め、現在も認めている」という回答が多かったという。長年にわたってセキュリティシステムの提案をしてきた㈱ブロード（東京都千代田区）は「コロナ禍以前から、ITの発展に伴いセキュリティ管理の対象が増加・複雑化するなか、リモートワークを急ぐあまり多くの企業が業務優先でセキュリティ対策を二の次にせざるを得ない状況が、この調査結果に反映されたのではないか」と指摘する。

スキをつくらない対策を

この種の「スキの多さ」は世界的な企業にもみられる。たとえば最近、米国のクラウドベースの高機能なネットワーク監視カメラを販売するスタートアップのVerkada社のセキュリティが侵害され、15万台以上の監視カメラ映像が漏洩していたことが判明。しかも、この事件でのサイバー攻撃は先進的なマルウエアを使った攻撃でもなく、ITセキュリティ分野における基本原則を守っていれば防げたものだったそうだ。やはりコロナ禍での勤務形態の急な変化を背景に、こうした基本的な対策の実施が難しくなっているのではないか。

また、リモートワークを実践するためには当然、企業のネットワークへの接続や各種のクラウドサービスへの接続などの機会が増えるが、前出のブロードは「自分がアクセスできるログインページなどは、他人もまたアクセス可能だと認識しなければならない」と警告する。そこで、同社ではエンドポイント（PC端末）をサイバー攻撃から守り、安全な仕様を実現できるようにすることはもちろん、「厳重なパスワード管理の実施を重点的に提案している」という。

とはいえ、前年比4倍に増えたとされる詐欺メールの対策やパスワード管理などをヒトの判断や作業に委ねるには限界もある。そこで注目したいのが、ブロードが日本総代理店を務める米国発のセキュリティ製品「HP SCE（旧Bromium）」だ。これは仮想技術でパソコン本体から隔離された仮想環境でウェブサイトを閲覧したり、文書ファイルを安全に開いたりできるというもので、詐欺メールの対策にもつながることが特徴。また、同社はサーバーのセキュリティ対策にも長年取り組んできたとあって、もし侵害があっても自動化されたパスワード管理ツールで、実害を最小限に抑えることができるという。リモートワークのスキをつかれぬよう、こうしたシステムを軸としたセキュリティ環境の構築を検討してみるのも一案だ。