サイバーセキュリティ最前線

コロニアル・パイプラインの被害からランサムウェアの進化を学ぶ

2021年2月号の本コーナーで、経済産業省が公表したサイバー攻撃に関する注意喚起について紹介した。それは大きく①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増②大企業、中小企業などを問わないランサムウェア（身代金要求型ウイルス）による被害③機微性の高い情報の窃取などを目的としたと考えられる海外拠点を経由した攻撃の深刻化に大別されていたが、最近はそれらに該当する被害が日本の企業や組織で実際に発生している。今号ではそのあたりの動向を検証したい。

拡大するランサムウェア被害

2021年は日本でもリモートワークの増加にともなってサイバー攻撃が増加したが、まず①については、今年4月のランドブレイン㈱への不正アクセスによるランサムウェア被害がそれに当たる。情報流出の可能性を公表したのは同社に業務を委託した総務省、内閣官房国土強靱化推進室、東京都、兵庫県など広範におよんだ。もちろん、②や③についても多くの企業が被害を受けており、今年だけでも②については富士フイルム㈱や徳島県のつるぎ町立半田病院など、③については㈱キーエンスや東芝テック㈱などがサイバー攻撃を受けたことを公表している。

数あるサイバー攻撃のなかでも目立ったのはランサムウェア被害だ。警察庁の調べによると、今年1～6月のランサムウェア被害の件数は61件に達したという。これは半年前の3倍の水準であり、いかに急速にその被害が拡大しているかがわかる。

もっとも、ランサムウェア被害の拡大は日本だけの問題ではない。たとえば、米国のコロニアル・パイプラインの被害は請求された身代金が4440万ドル（約4億8000万円）と巨額であったこと、米国における石油供給に広く影響を与えたことから、日本でも話題になった。

多様化する攻撃方法

では、コロニアル・パイプラインへの攻撃の背景にはどんな問題があったのだろうか。その点について、長年にわたってセキュリティシステムの提案を行ってきた㈱ブロード（東京都千代田区）は「外部の専門家が調査した結果、①事件発生前の時点でVPN（外部からのリモート接続に設けられたネットワーク）に誰も使用していない『休眠アカウント』が使用可能な状態で存在していたこと②ネット上の闇市場でそのパスワードのひとつが流通していたことなどが判明した」一方で「最初の侵害の痕跡は見つからなかった」と指摘。また、痕跡がなかった点については、そのマルウェアから発見された①自動バックアップの情報を削除して、容易に復旧できなくする②マルウェアにとって望ましくないOSのセキュリティ機構や主要セキュリティ製品を停止（無効化）する③ネットワークを通してアクセス可能なデータを探索した後、マルウェア自身を削除して痕跡を消すといった機能が働いていたものと思われる。

こういった被害が相ついだことから、今年の間にランサムウェアの知名度は高くなったが、つぎつぎと新種が誕生しているため、イタチごっこは当面、つづきそうだ。また、最近ではハードの制御プログラムなどに侵入し、OSをクリーンインストール（再設定）しても除去できないマルウェアまで誕生しているという。まさに、事態は日増しに深刻になっている感じだ。

だが、そういった状況に力を発揮するセキュリティシステムがある。それが「HP Sure Click Enterprise」だ。「このシステムなら信頼できないファイルを最初から仮想のパソコンで開くことができるため、ランサムウェアを含むマルウェア全般に対して抜本的な対策になる。巧妙なマルウェアがセキュリティ機構をすり抜けるといったこともない」と前出のブロードも太鼓判を押す。22年はこのシステムを導入し、安心・安全なセキュリティを確立してみてはどうか。