サイバーセキュリティ最前線

多様化する「ランサムウェア」と「WEBサイトの改ざん」への対策

2025年下半期に国内の企業・組織が公表したサイバーインシデント事例（ランサムウェア、不正アクセス、不審メール、WEBサイト改ざんなど悪意ある第三者による攻撃など／編集部調べ）が145件もあった。そこで、今号ではその傾向と対策について紹介したい。

多様化するサイバー被害

2025年下半期に国内で企業・組織がみずから公表したサイバーインシデント事例を分析すると、図表の通り、上半期と同様にランサムウェアおよび不正アクセスが依然として大きな割合を占めていた。

なかでも、注目すべき点は「ランサムウェア」の範囲が広がりつつあることだ。ランサムウェアといえば「身代金型ウイルス」といわれる通り、攻撃者側が身代金を得るための特定のマルウェアプログラム※1であることが一般的だったが、最近はその他の方法でデータを詐取し、リークサイト※2などで公開することを脅迫材料にするケースも増加している。さらに、下半期も継続して目立っている傾向として、WEBサイトへの不正アクセスおよび改ざん（悪意による変更）の多様化がある。従来、WEBサイトの改ざんといえば、表示内容を書き換える、政治的主張やいたずら目的のものなどが多かったが、最近は海外の不審な通販サイトに誘導されるといった被害が相次いでいるのだ。また、技術的には本来のページと見分けがつかない「偽のページ」に誘導され、認証情報が詐取されるなどのケースも想定される。サイトの管理者自身でも注意しなければ異変に気づきにくい可能性があり、細心の注意が必要だ。

技術的な傾向に加え、近年は社会的な環境の変化も無視できない。個人情報漏えいに関する報告義務の厳格化のほか、大手企業が取引先に対してセキュリティ対策状況を評価する動きなどが活発化しており、サイバー侵害が発生した際の「ペナルティ」やそれを回避しなければならないというプレッシャーが年々大きくなっているのだ。こうした変化によって「攻撃者にとっても詐取したデータが以前にも増して大きな〝人質価値〟を持つようになってきている」とセキュリティ会社の㈱ブロード（東京都千代田区）は解説する。

セキュリティの最適化を

では、こうした状況にいかに対応すればいいのか。ブロードがまず導入をすすめるのが「RidgeBot」だ。攻撃者側の主な侵入経路になりがちな社内およびWEBシステムの脆弱性を横断的に把握し、さらに実際に侵害可能なポイントをAIが自動検証するというもので、まさに転ばぬ先の杖となる。また、パソコンでのメールやインターネット閲覧のリスクを100ゼロトラスト隔離するエンドポイント対策「HP SCE（Sure Click Enterprise）」も、攻撃者側による日々の情報収集などを回避するうえで大いに役に立つだろう。さらに特権アクセスを制御し、誤操作・内部不正を防ぐ「BeyondTrust」の製品群も社内からの情報漏洩リスクを防ぐうえで有用だ。これらのソリューションを組み合わせることで、自社の現状にマッチしたセキュリティ環境を構築してほしい。

図表 2025年下半期のサイバーインシデントの分類と傾向

種類	上期	下期	増減とサイバー攻撃の特徴
不正アクセス	86	104	+18
WEB系	63	60	−3（WEBサイトの旧URL、新URLに自動転送するリダイレクト型改ざん）
内部	24	46	+22（業務システムが侵害される事例が増加）
ランサムウェア	39	27	−12（初期公表時とは違い、後続調査でランサムウェアと判明するケースが多い）
不審メール	11	6	−5（単独事象としての不審メールは減少したが、不正アクセスやアカウント侵害の一部として扱われるケースが増加）
その他	12	12	インサイダー、サポート詐欺など

※複数の項目にまたがるサイバーインシデントも含まれる

※1 電子メールやホームページなどを閲覧した際にコンピュータに侵入する悪意のある特殊プログラム
※2 インターネット上で不正に取得された機密情報、データが公開されるWEBサイト