サイバーセキュリティ最前線

アメリカで多発する「ランサムウェア」（身代金要求）と「EMOTET（エモテット）」の脅威
日本にもあらたなサイバーセキュリティが必要

日本でも多発する情報漏洩などのサイバーセキュリティ問題。だが、アメリカではそれよりも高いレベル、規模のサイバー攻撃が頻繁に発生している。東京2020大会を目前に控え、日本はどのような対策を講じるべきだろうか。

2019年12月6日、『朝日新聞』で㈱ブロードリンク（東京都中央区）の元社員が廃棄を依頼されたHDD（ハードディスクドライブ）などを転売し、情報漏洩していたことが大きく報じられた。転売されたHDDのなかには神奈川県の行政データが入った18個のHDDもあり、大量の個人情報や非公開情報が漏洩することになってしまった。依然として回収されていないHDDも残っており、さらに情報漏洩が拡大する恐れもある。また、12月12日には青森県弘前市などの職員約2700分の個人情報が記されたデータが、匿名の人物から東奥日報社にメールで送付されるという事案が発生。そのデータには氏名や住所、生年月日だけでなく、給与支給額や最終学歴といった情報まで入っていたという。弘前市は現在、このデータの出所について調査中だそうだが、いずれにしてもどこからかこれらの個人情報が漏洩したことは間違いない。

このようなレベルのサイバー攻撃にも満足に対応できていない日本だが、アメリカではそれよりもはるかに高いレベルのサイバー攻撃が頻発している。事実、アメリカのITニュースサイト『ZDNet』は2010年代を締めくくるコラムのなかで、19年の象徴的な出来事のひとつとしてランサムウェアを用いた「大物狩り」に言及。これは感染するとパソコン上のデータが暗号化されて使用できなくなり、画面に表示される指示に従い「ランサム」（身代金）を支払えば、暗号化を解除するパスワードが送られる、という手口のマルウェア（悪意のあるソフトウェア）のこと。近年はその標的が個人から企業や組織に移ってきており、19年にはITサービス業者、教育機関、米国地方自治体、さらに最近では欧州の企業なども被害を被ったことから「大物狩り」と称されるようになったのだ。

その象徴的なものがフロリダ州レイクシティ市の事件だ。この事件の経緯はつぎのとおりだ。職員が市に送られてきたメールのリンクを開いたことを機に、市のITネットワークがランサムウェアに感染。市のほぼ全システムが完全に乗っ取られ、市は最終的にランサムウェアの攻撃者に対し、50万ドル相当の身代金を支払ったという。

なお、このレイクシティ市の事件の特徴としては、19年に頻繁に報じられるようになった「EMOTET（エモテット）」が使用されていることがあげられる。セキュリティ会社である㈱ブロードによると「エモテットは約5年前からネットバンキング分野で知られるようになったマルウェアで、それ自体が動作するというよりも、別の種類のマルウェアをインターネット経由でダウンロードする機能に優れており、一般的なウイルス対策ソフトで検知することが非常に難しい。しかも、昨今のマルウェアはOSやセキュリティソフトで検知することが難しくなっているため、さらにリスクは拡大している」という。

このようなレベルや規模のサイバー攻撃はまだ日本では顕在化していないが、東京2020大会は世界の注目を集めるだけに、今後はそういった攻撃が発生するリスクも十分にある。そこで、注目したいのが一般的なセキュリティソフトのようにマルウェアやウイルスなどを検知・判定してブロックするのではなく、いったんマイクロVM（仮想パソコン）にすべてを取り込み、使用後に仮想パソコンごと削除するという超斬新なソフト「Bromium（ブロミアム）」（発売元は前出のブロード）だ。米国発のこのソフトは比較的安価であるにもかかわらず、日本のサイバーセキュリティのレベルを一気に向上させる可能性を持っているとは識者の弁、あらためてこの種のサイバーセキュリティについて検証してみてはどうか。