サイバーセキュリティ最前線

「情報セキュリティ10大脅威」を「仮想パソコン」で防ぐ!!

IPA（独立行政法人情報処理推進機構）は2月28日、「情報セキュリティ10大脅威 2023」の解説書（組織編）を公表した。今号ではその結果をもとに、サイバーセキュリティ最前線を検証!!

第1位は身代金を要求するランサムウェア

「情報セキュリティ10大脅威2023」において第1位となったのは「ランサムウェア」だった。「身代金」を意味する「ランサム」という言葉を含むランサムウェアは、データを「人質」にして金銭を要求する目的で使われるプログラムの総称。個人が使用するパソコンのデータを暗号化して使用できないようにして、これを元に戻すためのキーがほしければ金銭を支払えという手口が2015年頃から世界的に拡大し、しだいにより高額な身代金を狙える企業や組織をターゲットにした行為が増加していった。そして、近年では通信機能を使ってデータを外部（犯行者）に不正送信し、「盗んだ情報の開示」をあらたな人質とする手口まで増えてきている。

たとえば、従業員に脅迫メールを送付された武州製薬㈱では、VPN（仮想専用通信網）の脆弱性を突かれて個人情報が流出した可能性があるという。また、あるアパレル企業では、サーバーがサイバー攻撃を受けて、顧客情報が流出した結果、同社の顧客が2度にわたり「あなたの個人情報を入手しました。悪用されたくなければ～してください」といった脅迫メールを受信する事態が発生。さらにある高校では、教諭が自分の端末で業務用データを使いリモートワークをしていたところ、画面に「ウイルスに感染した」という文言とともに連絡先が表示され、金銭を支払ってしまったという。

10大脅威の2位は「サプライチェーンの弱点を悪用した攻撃」で、去年より順位をひとつ上げた。昨年下旬に大阪急性期・総合医療センターが患者の食事を納入していた事業者のシステムを経由してサイバー攻撃を受けたのもそういったケースのひとつだ。最近、このように大規模な企業や組織を直接狙う代わりに出入り業者や派遣、委託先などを経由して攻撃するというケースが多発しているので、中小企業もこれまで以上に注意を払う必要がある。

また「犯罪のビジネス化（アンダーグラウンドサービス）」という種別がはじめて取り上げられた点も興味深い。この点について、IPAは「犯罪に使用するためのサービスやツール、IDやパスワードの情報などがアンダーグラウンド市場で取り引きされ、これらを悪用した攻撃が行われている」と指摘。サイバー犯罪者の裾野が広がることで、サイバーリスクもさらに拡大していきそうだ。

仮想パソコンを立ち上げマルウェアを撃退

こうした点について、長年にわたってセキュリティシステムを手掛けてきた㈱ブロード（東京都千代田区）は「サイバー攻撃が多様化すればするほど、汎用的で長期的に使用できるツールが必要になる」と話す。そして、まずは「大多数のサイバー侵害の起点となるメール添付によるマルウェアの対策を最優先すべきだ」とも。

その対策の筆頭となるのが「HP Sure Click Enterprise（HP SCE）」（HP社）だ。このツールの特徴はメールなどの操作を行うパソコン上で「仮想パソコン」を立ち上げ、添付ファイルなどを隔離した状態で操作できること。そのため、マルウェアがどのような動作をしても、本体はまったく影響を受けず、確実に攻撃を防ぐことができるという。

また、VPNが起点になるケースについては、VPNを使用せずにリモート管理することができる「BeyondTrust Remote Support」（BeyondTrust社）が有効とのこと。さらに「BeyondTrust社は管理者の特権やパスワードの自動管理などの分野でも強みを持っているので、そのあたりの活用も有効だ」とブロードは太鼓判を押す。サイバー攻撃の多様化とともに、守りの多様化も必須に。ブロードはHP SCEやBeyondTrust社のツールの日本総代理店を務めているので、まずは気軽に相談してみてはどうか。