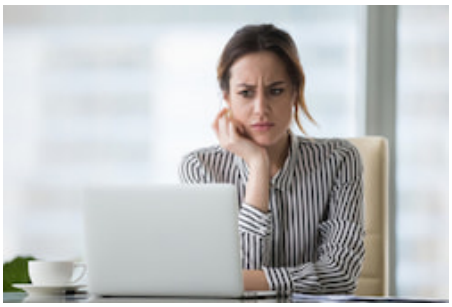
潜行するサイバー攻撃（第8回）

FBIから届いた「偽メール」の正体

2022.01.05



ビジネスはもちろん、プライベートでも広く利用されている便利な電子メール。しかし最近、その安全性を揺るがす事件が発生して話題になった。舞台となったのは米国FBI（連邦捜査局）。同局の正式なメールアカウントから大量の偽メールが送信された。なぜこのようなことが起きたのか、これまでに判明した情報から考えてみたい。

2021年11月13日（現地時間）、米国FBIから「公式メールアカウントが乗っ取られ、偽の電子メールが送信された」との発表があった。メールの内容は某セキュリティ関連企業の創業者を非難する類のものだった。送信元のアドレス末尾はFBIを示す「fbi.gov」。正規のメールサーバーを通じて送信され、世界各国10万件以上のメールアドレスに偽メールが送り付けられる事態になった。FBIは問題発覚後、直ちに当該サーバーを停止するとともに、被害状況の把握と原因究明に乗り出した。

その後、攻撃者とみられる人物からジャーナリストに連絡が入り、自らの行為を説明する異例の展開となった。「Pompompurin」と名乗る攻撃者は、FBIのシステムの脆弱性を指摘するのが攻撃の目的だとし、FBIが関係機関に提供するポータルサービス「Law Enforcement Enterprise Portal（LEEP）」の設定の問題を悪用してシステムに侵入、偽メールを送信したと語った。続いて11月15日にFBIからも同様の内容が発表され、図らずも攻撃者の解説を追認する形となった。

偽メールは確かにFBIのメールサーバーから送信されていたが、このサーバーはLEEP専用に使われるもので、データの窃取や機密情報漏えいにつながる恐れはないとFBIは発表している。この事件は個人のハッカーが引き起こした愉快犯的犯罪に分類されるが、これまで偽メールを見抜く手段として一般的だった「正規のドメインか確認する」という方法が、攻撃者がサーバーを乗っ取ることで簡単に破られてしまう問題を明らかにした。

巧妙化する「なりすまし」「フィッシング」

この事件ではFBIという公的機関のメールサーバーが乗っ取られるショッキングな部分に注目されがちだが、電子メールを利用する上での原則である名前（メールアドレス）が第三者によって書き換えられサイバー攻撃に使われる可能性を、リアルな警告として世に示した。

「なりすまし」「フィッシング」と呼ばれるこのような行為は、電子メールが使われ始めた1990年代から問題視されている。電子メールは、送信時に特定のメールサーバーを使用し、その際にドメイン（@以降の文字列：△△.com／△△.jpなど）情報が記録され、受信側はその情報から送信元を確認する。昨今のサイバー攻撃では、システム侵入のきっかけとしてターゲットに社員や取引先を装った偽のメールを送り付け、そこに添付されたファイル（マルウエア）を実行させてシステムに「穴（セキュリティホール）」を空ける行為が頻発している。

偽メールは送信者のアドレス、ドメインの文字列を確認することで、ある程度見分けられる。例えば、取引先からのメールなのに通常とドメインが違っている場合は開封せず、不審な点があれば職場のシステム担当者に連絡するといった対処が必要だ（例：@△△□□.jp→@△△□□.netなど）。

セキュリティ対策で「ガード固め」

このような偽メール、なりすましの被害を未然に防ぐには、何よりもユーザーが危険性を意識し、メールが正しいものかを都度確認することが基本だ。ただし周到に身を隠し、かつ高度な技術を持った攻撃者に対抗するのは難しい。そこで、ITベンダー各社から提供されるセキュリティ対策サービスを導入し、必要に応じてプロに助力を求める方法を検討してもよいだろう。

セキュリティ対策サービスには、添付ファイルに仕込まれたマルウエアを排除する「アンチウイルス」をはじめ、送信元サーバーやアドレスから迷惑メールを見分ける「アンチスパム」、情報を窃取するWebサイトへの接続を防ぐ「Webフィルタリング」など、さまざまな種類がある。これらはいずれもUTM（統合脅威管理）の機能として提供されており、メールの扱いに不安を抱えている場合は心強い備えになる。

また、日本データ通信協会が運営する「迷惑メール相談センター」では、判断が難しいメールに関する相談を受け付けるほか、迷惑メール送信者の情報提供を実施している。同センターでは迷惑メールにだまされないコツ「ゼロトラスト」をはじめ、迷惑メール・詐欺メールの事例や注意点、スマホ・パソコンでの受信時の対処法などをまとめた資料「撃退！迷惑メール」が公開されているので、こちらも対策の参考にしてみてはいかがだろうか。