中小企業のセキュリティー対策

一般的な対策で被害防止は可能

独立行政法人情報処理推進機構（ＩＰＡ）では、経済産業省の告示に基づき、被害の状況把握や対策検討を目的とし、コンピュータウイルス・不正アクセスに関する届け出を受け付けている。２０２１年上半期（1～6月）に届け出のあった被害について全体を通して見ると、これまでと同様に、一般的によく知られたセキュリティー対策を実施していれば、被害を防ぐことができたと思われるものが多かった。

今回は届け出の中から特徴的な被害事例を二つ紹介する。

■事例①返信を装うメールによりウイルスに感染した被害

不審なメールを受信した従業員が利用している仮想デスクトップ環境がウイルスに感染した。調査したところ、メールに添付されていたＺＩＰファイルには、マクロ付きのＥｘｃｅｌのファイルが含まれていた。また、そのマクロにより外部からウイルスをダウンロードする動作が確認できたことから、感染が判明した。仮想デスクトップ環境をリセットすることで回復を図り、また再発防止策として従業員への教育を実施することとした。

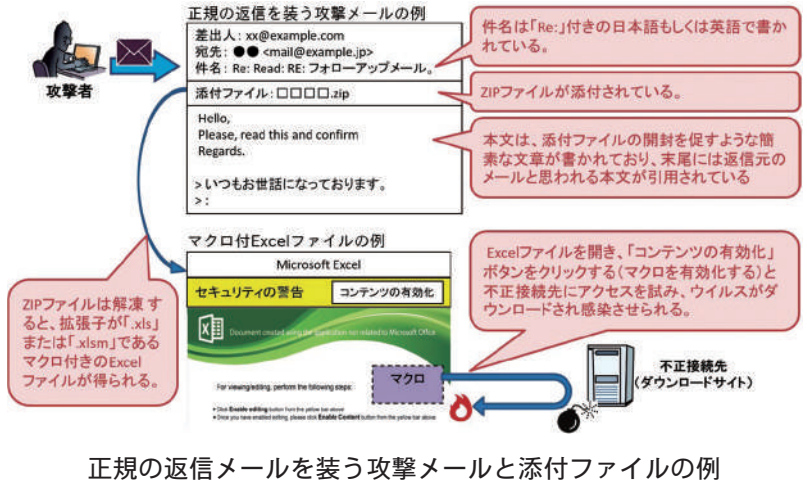
同事例では、正規の返信メールを装うことで受信者（攻撃対象）の警戒心を薄れさせて、添付ファイルを開かせようとする手口が使われており、今後も同様な手口による攻撃が行われることが懸念される。システム管理者が実施できる対策として、メールサーバやパソコンでのウイルス対策の徹底と、利用者に対する「不審なメール、ファイルは開かない」「Ｏｆｆｉｃｅ文書のマクロは安易に有効にしない」といった啓発が必要である。

これらを多層の防御策として実施しつつ、可能であれば、マクロ機能の無効化を標準の設定とすることや、ウェブゲートウェイのセキュリティー装置により、不審な外部サイトへの通信を遮断することも有効であると考える。

■事例②ＮＡＳの脆弱性を悪用されたランサムウェア感染

ＮＡＳ上の30万個以上のファイルが暗号化され、脅迫文が書かれたファイルが残されていた。調査したところ、ＮＡＳに脆弱（ぜいじゃく）性が存在しており、ＮＡＳを攻撃するランサムウェアに感染したと思われる状況であった。ベンダーから提供された駆除ツールとファイル復元ツールにより復旧を試みたが、一部のファイルは復元できなかった。最新のファームウェアに更新し、不要な機能を無効化して再発防止を図った。

同事例では、ＮＡＳをインターネットから直接アクセスできるように設定していた。外部からのアクセスを可能にすることは、攻撃者にとってもアクセスが容易になることを意味するため、より一層のセキュリティー対策が必要になる。また、ＮＡＳに限らず、ＶＰＮ装置やブロードバンドルータといったネットワーク機器についても同様のことがいえる。これらの機器への脆弱性情報を入手できるセキュリティー対策の重要性を認識し、随時手順やリソースなどを確立しておくことが重要である。



正規の返信メールを装う攻撃メールと添付ファイルの例

早期発見へ事例の詳細公表

各事例の詳細や、その他の被害事例については、ＩＰＡのホームページに報告書が掲載されているので確認してほしい。同様被害の早期発見や未然防止といったセキュリティー上の取り組みの促進につながることを期待する。

（独立行政法人情報処理推進機構・江島将和）

被害の届け出や事例はこちらを参照