加害者にならないためのサイバー攻撃防止法（第7回）

狡猾なウイルスも捕獲する「サンドボックス」

2018.02.21

官公庁や大企業だけでなく、中堅・中小企業にも広がりつつあるサイバーセキュリティの脅威ーー。その典型ともいえる標的型攻撃メールの場合、日本語で書かれたごく普通の通知メールや照会メールが攻撃の発端となるケースが多い。「怪しいメールは開かない」といった注意喚起だけで防ぐのは、残念ながらほとんど不可能だ。

パターンで検知できるのは既知のウイルスだけ

もちろん、ほとんどの企業・団体は何年も前からセキュリティ対策製品を使っているはずだ。いまやウイルス対策ソフトやファイアウォールはほぼ普及しているといってよいし、ファイアウォールの上位版に当たるUTM（統合脅威管理）製品を導入する企業も増えてきた。

しかし、これら従来型の製品は、ウイルスなどのマルウエアの特徴を記した“パターン”を使って検知と処置をする仕組みを取る。セキュリティ対策製品のベンダーは、世の中に出回るマルウエアを収集するための体制を世界レベルで運用している。新しいマルウエアが発見されると、その特徴を調べてパターンに追加し、その製品のユーザーにインターネットを通じて配信してくれる。

新マルウエアの登場からパターン配信までの期間は場合によってまちまちだが、数時間から数日。この期間は“ゼロデイ”とも呼ばれ、従来型のセキュリティ対策製品では新マルウエアを検知できない。

また、“見つかっている数”という壁もある。いくら怪しいデータがインターネット上で見つかったとしても、世界で1例しかなければ、パターンに登録するセキュリティ対策製品ベンダーはない。ある程度の数が発見されないと、新パターンは配布されない。高価で高機能なウイルス対策ソフトであっても見落としは避けられないのだ。

そもそも、標的型攻撃メールの基本的な手口は、特定企業の特定部署といった、ごく限られた相手だけにマルウエアを送り付けること。見つかる可能性は低く、そこに使われているマルウエアがパターンに登録されなくてもまったく不思議はない。

高価な“サンドボックス”… 続きを読む