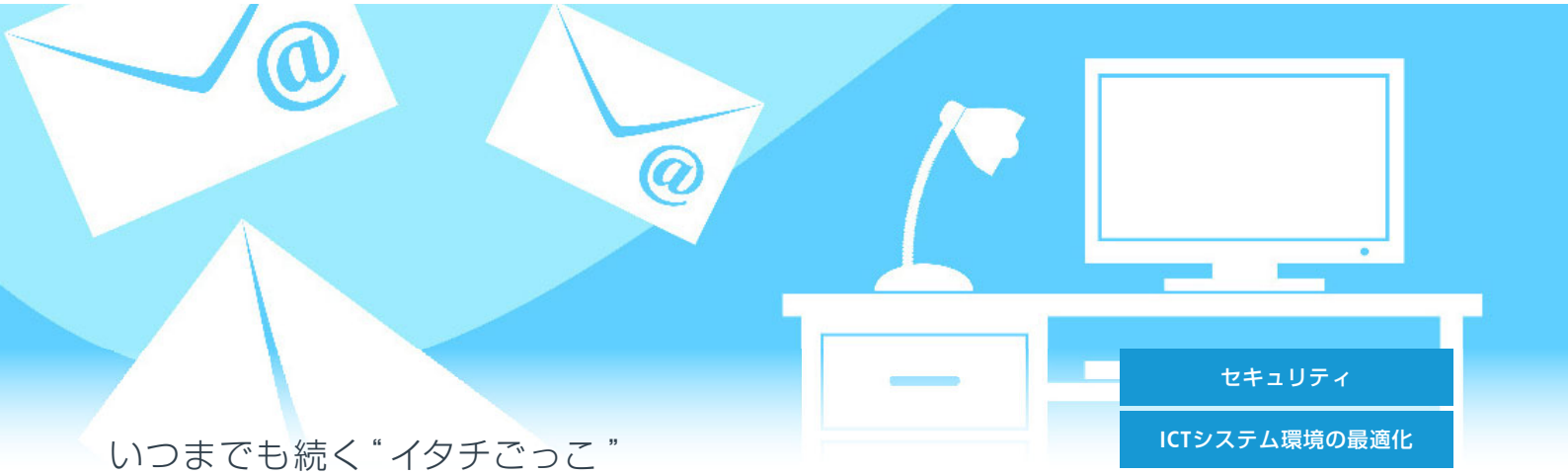

セキュリティ

ICTシステム環境の最適化

いつまでも続く“イタチごっこ”

メールのセキュリティ対策には多段・多層防御が有効

メールはビジネスの上で重要な連絡手段となっていますが、同時にマルウェアが企業へ侵入する経路にもなっています。マルウェア攻撃に使われるメールは日々進化しており、従来のセキュリティ対策ではすり抜けてしまうケースが増えています。さらにいえば、受信メールだけでなく送信メールも誤送信などのリスクが存在します。ここでは、メールにおけるセキュリティ対策のキーワード「自動化」とその手法について紹介します。

多くの脅威がメールを介してやってくる

メールにおけるセキュリティ対策は、エンドポイントとなるPCやゲートウェイで実施するケースが一般的ですが、サイバー攻撃者もその盲点を突くべくさまざまな工夫を行っており、長きにわたって“イタチごっこ”が続いてきました。

マルウェアそのものの特徴を見ていくと、1～2年で流行が変遷していることがわかります。2018年は、感染したPCのCPUやメモリの能力を勝手に仮想通貨の“発掘”へ使用する「マイニングマルウェア」が流行しました。その前の2017年は、感染したPCのファイルを暗号化して使えなくし、元通りにするために金銭を要求する「ランサムウェア」が流行しています。それより前となると、オンラインバンキングを悪用する「バンキングマルウェア」が主流でした。

このように、マルウェアには流行があるのですが、流行が過ぎたからといってなくなるわけではありません。スパムメールの添付ファイルや誘導先に仕込まれるなど、常套手段として今なお使われ続けています。また、新しいタイプのマルウェアが登場すると、その後を追って大量の亜種が作成されます。マルウェアの全体数は増える一方なのです。

マルウェアの種類が膨大になったことで、ウイルス対策ソフトがマルウェアを検知するためのパターンファイルも膨大になってしまいました。そこで、今ではパターンファイルの大半をクラウドに置くウイルス対策ソフトも多くなっています。しかしこうした対策もむなしく、近年はパターンファイルによる検知を回避するマルウェアが急増。現在では、従来型のウイルス対策ソフトの検知率は4割を切るまで低下したといわれています。

拡大する感染経路、ソーシャルエンジニアリングの手法も採用

検知を回避するマルウェアが増加した理由の1つに、アンダーグラウンドのマーケット(地下市場)の拡大が挙げられます。こうした地下市場は、インターネットの深淵にあり、検索にも引っかからず、専用のブラウザを使用しないとアクセスできません。サイバー攻撃者は、こうした地下市場でサイバー攻撃のための情報やツールを入手します。

地下市場は複数存在しており、それぞれが拡大傾向にあります。これらでは、最新のマルウェアや攻撃により入手した個人情報などが取引されているほか、マルウェアがセキュリティ対策ソフトで検出されるかどうかを試すことができるサービスもあるといわれます。また、ランサムウェアを簡単に作成できるクラウドサービスの存在も確認されています。つまり、最新のマルウェアが誰でも簡単に使用できる状態になっているのです。

最新のマルウェアが誰でも容易に入手できるようになったことで、サイバー攻撃者は「いかにメールや添付ファイルを開かせるか」に注力しています。脆弱性を悪用したシステム的な攻撃だけでなく、人間の心理的な隙を突くソーシャルエンジニアリングの手法も取り入れています。例えば、正規ファイルにマルウェアを忍ばせたり、マルウェアを正規のファイルそのものに見せかけたりします。これは心理の隙を突くことで受信したメールを開封させようとする手法であるため、「注意」や「マニュアル」によって見抜くのが難しいのが実情です。

感染経路や感染対象が増えていることも問題です。メール環境そのものをクラウドサービスに移行する企業が増えていますし、SNS(ソーシャルネットワークサービス)が普及したことで、SNSを経由してマルウェアに感染するケースが増えています。また、AndroidやiOSを搭載したスマートフォンなどのスマートデバイスを標的としたメール攻撃も増加しています。スマートデバイスの場合はウイルスではなく、マルウェアと同じような動作を行う不正アプリの形で侵入します。マルウェア対策には、ますます多段防御や多層防御が求められているのです。

関連サービス

Cloud App Security	Office 365標準セキュリティを強力にカバーするクラウド型セキュリティサービスです。 社外に置かれるメールやクラウド共有ストレージデータのセキュリティを補完し、クラウドサービスを安心してご使用いただくための新しいソリューションをご提供します。
メールセキュリティ	ウイルスチェック機能と迷惑メールフィルタリング機能をセットで提供する、「Bizメール＆ウェブ ビジネス」のオプションサービスです。 ウイルスメールや迷惑メール、フィッシングなどに対する最新のメールセキュリティ対策が可能となります。
テレワーク・スタートパック	ノートPCとモバイル通信、セキュリティサービスをパッケージ化したサービスです。 アンチウイルスソフトやファイアウォールから不正プログラムの実行阻止までテレワークを始めるためのセキュリティ対策が設定されたPCを納品します。面倒な設定作業が不要なので、最短10分でPCをご利用できます。