中小企業の

セキュリティー対策

―33―

なりすましメールに注意

実在の氏名や文面流用

「Ｅｍｏｔｅｔ（エモテット）」と呼ばれるウイルスへの感染を狙う攻撃メールが、国内企業で広く着信している。Ｅｍｏｔｅｔは、情報の窃取に加え、別のウイルスに感染させるために悪用されるウイルスであり、攻撃者によって攻撃メールに添付されるなどして感染の拡大が試みられている。

Ｅｍｏｔｅｔへの感染を狙う攻撃メールの中には、正規のメールへの返信を装う手口が使われている場合がある。これは、攻撃対象者（攻撃メールの受信者）が過去にメールのやり取りをしたことのある実在する相手の氏名、メールアドレス、メール文面などの一部が流用された、あたかもその相手からの返信メールであるかのように見える巧妙な攻撃メールである。

このようなメールは、Ｅｍｏｔｅｔに感染してしまった企業から窃取された正規のメール文面やメールアドレスなどの情報が使われていると考えられる。すなわち、Ｅｍｏｔｅｔへの感染被害による情報窃取が、他者に対する新たな攻撃メールの材料とされてしまう悪循環が発生している恐れがある。

なお、正規のメールへの返信を装う手口の事例はこの他にもあり、例えば２０１８年11月、Ｅｍｏｔｅｔとは異なるウイルスへの感染を狙う日本語の攻撃メールでも悪用されたことを確認している。今後もこの手口は、正規のメールであっても、不自然な点があれば添付ファイルは開かない。

添付ファイルは不用意に開かない

Ｅｍｏｔｅｔへの感染を防ぐというためだけにとどまらず、一般的なウイルス対策として、次のような対応をすることを勧めたい。

■身に覚えのないメールの添付ファイルは開かない。メール本文中のＵＲＬリンクはクリックしない。

■自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない。

■ＯＳやアプリケーション、セキュリティーソフトを常に最新の状態にする。

■信頼できないメールに添付されているワード文書やエクセルファイルを開いた時に、マクロやセキュリティーに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない。

■メールや文書ファイルの閲覧中、身に覚えのない警告ウインドウが表示された際、その警告の意味が分からない場合は、すぐにシステム管理者へ連絡する。

■身に覚えのないメールや添付ファイルを開いてしまった場合は、すぐにシステム管理者へ連絡する。

Ｅｍｏｔｅｔへの感染を狙った攻撃メールの文面や添付されている不正なファイルの例、対策、関連情報については独立行政法人情報処理推進機構（ＩＰＡ）のウェブサイト（https://www.ipa.go.jp/security/announce/20191202.html）を参照してほしい。

また、ワードやエクセルのマクロ機能に関する設定の変更、Ｅｍｏｔｅｔに感染した場合の影響などについては、一般社団法人ＪＰＣＥＲＴコーディネーションセンターから公開されている注意喚起（https://www.jpcert.or.jp/at/2019/at190044.html）を併せて参照してほしい。

（独立行政法人情報処理推進機構・江島将和）

攻撃メールの文面の例

	事例１	事例２
受信日時	2019/11/28 15 時頃	2019/11/29 8 時頃
本　文	お世話になっております。 添付いたしますのでご確認ください。 内容に齟齬がございませんでしたら、 黒線太枠内をご記入いただき、 社判を捺印の上 下記、住所までご郵送くださいませ。 よろしくお願い致します。	いつもお世話になります。 11 月分の請求書を送信致します。 色々とお手数をおかけしますが、 宜しくお願い致します。
添付ファイル名	請求書の件です。【文字列】.doc	請求書送付のお願い【文字列】.doc