中小企業の

セキュリティー対策

―57―

Emotetに再び警戒を

エモテット

攻撃再開の兆候 従業員へ注意喚起を

2021年11月14日頃から「Emotet（エモテット）」の攻撃活動再開の兆候が確認されたという情報がある。Emotetとは、情報の窃取に加え、さらにほかのウイルスへ感染させるために悪用されるウイルスのことで、本連載vol・33（19年12月11日号）とvol・43（20年10月21日号）にて注意喚起を行っている（文末のQRコードを参照）。

21年1月27日、EUROPOL（欧州刑事警察機構）が、欧米8カ国の法執行機関・司法当局の協力により、Emotetの攻撃基盤（ウイルスメールをばらまいたり、感染したマシンを操作したりするための機器など）を停止させたと発表し、独立行政法人情報処理推進機構（IPA）でも、Emotetによる攻撃や被害が停止、あるいは大幅に減少したことを確認していた。

IPAでは今回、攻撃メールに添付されていたと思われるWordファイルとExcelファイルを入手し、確認を行った。これらは悪意のあるマクロ（プログラム）が仕込まれたもので、21年1月までの攻撃と同様の手口である。被害に遭わないために、システム管理部門などにおいては、Emotetの攻撃メールを警戒するとともに、改めて従業員へ、不審なメールへの注意喚起を実施してほしい。

実施すべき対策

Emotetへの感染を防ぐというためだけにとどまらず、メールを介したサイバー攻撃への対策として、次のような対応をすることを勧める。

■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。

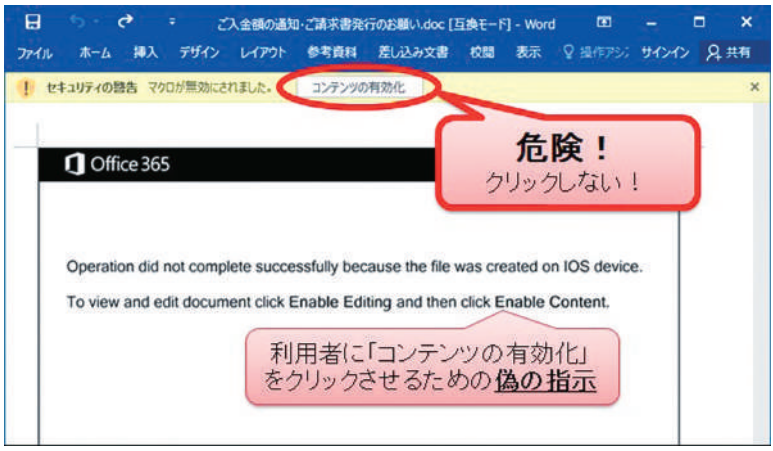
■信頼できないメールに添付されたWord文書やExcelファイルを開いたときに、マクロやセキュリティーに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない。

■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（メッセージ）が表示された際、その警告の意味が分からない場合は、操作を中断する。

■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部門などへ連絡する。

IPAなどが発する関連情報を参考に

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、IPAのウェブサイトを参照してほしい。また、WordやExcel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（JPCERT／CC）から公開されている注意喚起を併せて参照してほしい（文末のQRコードを参照）。



悪意のあるマクロを仕込んだWord文書ファイルの例（2020年7月）

今後、Emotetの攻撃メールは大規模なばらまきに発展する可能性もある。19年から20年にかけ、多くの企業・組織が被害に遭っている。念のため、警戒することをお願いしたい。

（独立行政法人情報処理推進機構・江島将和）

IPAの注意喚起

JPCERT／CCの注意喚起

※本連載vol・33と43はこちらを参照

日商ASSIST BIZ