滋賀県警察からのお知らせ

サイバーセキュリティ情報 CSI

事業者の皆さまに、注目のサイバーセキュリティに関する情報をお届けします。

R３年度No.12

「Emotet」ウイルスの感染が拡大
メールの添付ファイルに注意してください。

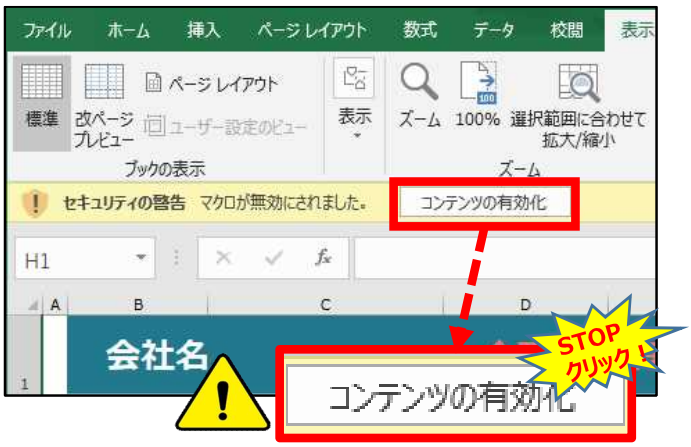
IPA（独立行政法人情報処理推進機構）によりますと、「**Emotet（エモテット）**」と呼ばれるウイルスへの感染を狙う攻撃メールが、国内の組織に広く送付されているとのことです。

「Emotet」は、MicrosoftのWordやExcelに悪意のあるマクロプログラムが仕込まれていて、利用者に「コンテンツの有効化」ボタンをクリックさせることで、ウイルスをダウンロードさせて、感染させる手口です。

ウイルス感染すると、メールや重要情報が盗まれたり、それを悪用して別の人に攻撃が行われたりします。

メールの添付ファイルには注意してください。

また、「コンテンツの有効化」ボタンは、信用できるファイル以外はクリックしないでください。



ウイルス感染のおそれがあります。メールに添付されたOfficeソフトの「コンテンツの有効化」ボタンを安易にクリックしないでください。

「Emotet（エモテット）」とは

Emotetは、情報の窃取に加え、更に、他のウイルス感染のために悪用されるウイルスです。

主にメールに添付された「Wordファイル」を開いたうえ、「コンテンツの有効化」又は「編集を有効にする」ボタンを押すことで、マクロプログラムが実行され、外部サーバから不正プログラム（Emotet）がダウンロードされます。

Emotetに感染すると、PCに保存されている送受信メールの情報が盗まれるため、実在する人物の氏名やメールアドレスを使用することが可能となり、正規のメールへの返信を装って、別の人（取引先等）へ、標的型メールが送られます。

特にパスワード付きのZIPファイルに注意してください

攻撃者は、パスワード付きZIPファイル（圧縮ファイル）に、Word等のファイルを入れて送ってくる場合があります。

パスワードはメール本文に記されており、ZIPファイルを開くとWord等のファイルが入っているというものです。パスワードにより暗号化されているため、メール配送経路上でセキュリティ製品の検知・検疫をすり抜ける可能性が高いので注意が必要です。

※ Emotetは、2019年ころに世界的に感染が拡大しましたが、外国機関の摘発により収束していました。
滋賀県内でも感染が確認されていました。

パスワード付きzipファイルが添付されたメールの例

対策のポイント

- 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リンクをクリックしない。
- 自分が送ったメールの返信でも不自然な点があれば添付ファイルは開かない。
- 「Word」や「Excel」ファイルを開いたときに、マクロやセキュリティに関する警告が表示された場合、「マクロを有効化する」「コンテンツの有効化」というボタンはクリックしない。
- 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に連絡する。

参照：IPA「Emotetと呼ばれるウイルスへの感染を狙うメールについて」
https://www.ipa.go.jp/security/announce/20191202.html

【受付随時】体験型サイバーセキュリティセミナーを実施しています。詳細は下記まで。

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）