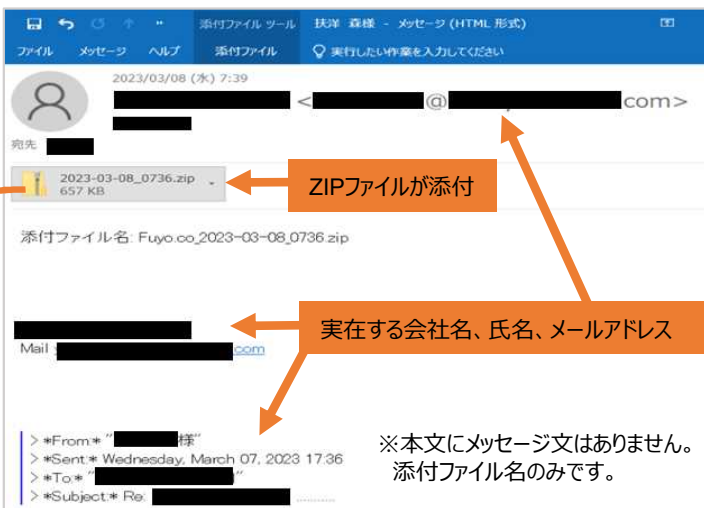


新手口 「Emotet」 滋賀県内で発生 メールの添付ファイルにご注意願います。

今月（2023年3月）に入り、滋賀県内で「Emotet」の新たな手口による被害が発生しました。Emotetは、感染すると端末からメール情報を盗み出したうえ、盗んだメールを使ってさらに感染を広げるウイルスです。Emotetの活動は、休止と再開を繰り返しており、再開が確認されました。新手口は、大容量のWordファイルをZIPファイルに圧縮してメールに添付しています。業務でメールを使用される方は、特に添付ファイルの取扱には注意してください。



実際に確認されたEmotet



「Emotet（エモテット）」とは

主にメールに添付された「Wordファイル」等を開いたうえ、「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。

滋賀県内で確認されたEmotetメール

今回確認されたEmotetは、ZIPファイルに圧縮したWordファイルが使用されています。Wordファイルのサイズが約500MBで、大きなサイズになっているのが特徴です。ファイルサイズを大きくすることと圧縮ファイルにすることでウイルス対策ソフトに検知されにくくしているものと思われます。



編集を有効にする(E)

編集を有効にすると、次に「コンテンツの有効化」が表示される

コンテンツの有効化



新手口でも最終的には「コンテンツの有効化」を押さないと感染はしません。
「コンテンツの有効化」は安易に押さないでください。

«CS情報SHIG@» クレジットカードの不正利用に注意。カード番号等を安易に入力しないで。

滋賀県警察本部 サイバー犯罪対策課 077-522-1231（代表） 県警webページ →

