Emotet（エモテット）に気をつけて

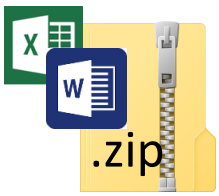
ウイルスへの感染を狙うメールが流行しています！！

電子メールの添付ファイルを主な感染経路とするEmotet(エモテット)と呼ばれるウイルス等への感染を狙う攻撃メールが流行しており、注意が必要です。

1　なりすましメールに注意！

攻撃メールは、受信者が過去にメールのやり取りをしたことのある、実在の相手・メールアドレス・メールの内容等の一部を流用し、実在の相手になりすました内容となっている場合があります。
※少しでも不自然な点があればメールを送った相手に直接確認してください。

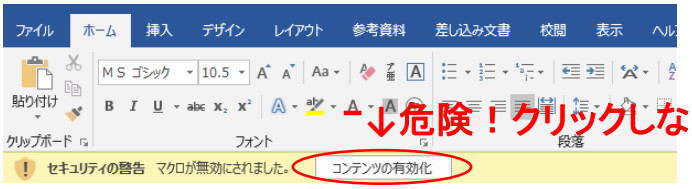
2　パスワード付きzipファイルにも注意



Emotetは、感染させるためにWordやExcelのファイルを送付しますが、ウイルス対策ソフトに検知されにくくするためにパスワード付きのzipファイルに圧縮している場合があります。
これらのファイルが添付されたメールには十分注意してください。

3　「コンテンツの有効化」ボタンを押さない！

WordやExcelのファイルを開いた時に、セキュリティに関する警告とともに表示される「コンテンツの有効化」というボタンを押すと感染します。間違いなく真正なメールと確認できた場合を除き、ボタンは押さないでください。



Emotetの概要

攻撃者が不正プログラムによってメールを窃取し、その関係者に窃取したメールを元に不審メールを送信して、ウイルス感染成功時にはまた情報を窃取するという手口を繰り返して攻撃対象を拡大する。