Ksisnetだより
発行:Ksisnet事務局
令和 2年 9月 9日
Vol.84

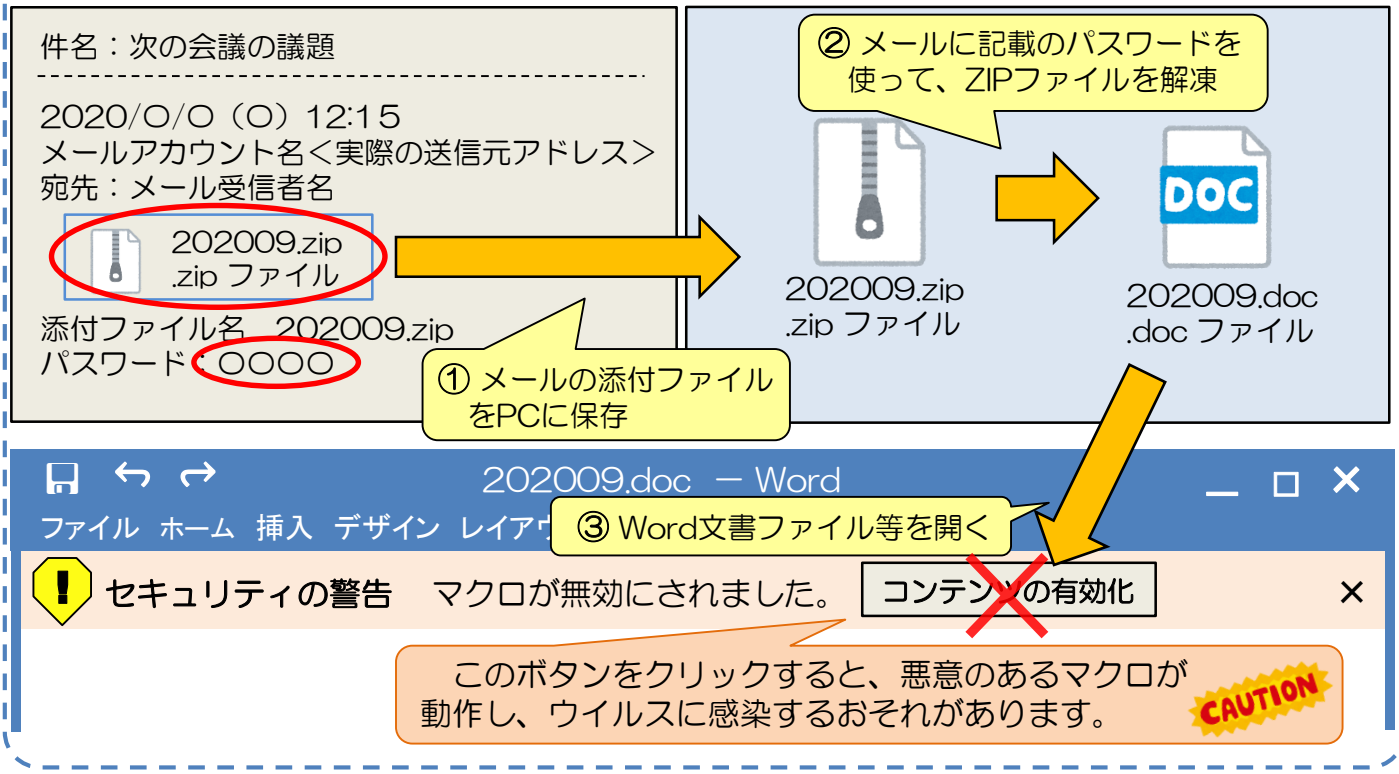
Emotetの感染拡大および新たな攻撃手法について

Emotetの感染に繋がる攻撃メールが急増するとともに手口が巧妙化していることから、組織内への注意喚起を行ってください。

【新たな攻撃手法】

新たに確認された手口として、
「パスワード付きZIPファイルを添付したEmotetの攻撃メール」
が確認されています。

・ パスワード付きZIPファイル受信からEmotet感染までの流れ



この手口では、添付ファイルが書庫ファイルであることから、メール配送経路上でのセキュリティ製品の検知・検疫をすり抜ける可能性があります。

信頼できるものと判断できない限りは「マクロやコンテンツを有効化」のボタンをクリックしないよう注意してください。

Emotetについては、Ksisnetだより 第70号、第75号、第83号においても情報提供しています。これらも参考に組織内への注意喚起を行ってください。

参考　ＩＰＡ（情報処理推進機構）・JPCERT/CC