

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

件名：次の会議の議題

2020/0/0 (0) 12:15

メールアカウント名<実際の送信元アドレス>

宛先：メール受信者名

 202009.zip
zip ファイル

添付ファイル名 202009.zip

パスワード ○○○○

① メールの添付ファイルをPCに保存

② メールに記載のパスワードを使って、ZIPファイルを解凍

 202009.zip
zip ファイル

 202009.doc
.doc ファイル



202009.doc - Word

ファイル ホーム 挿入 デザイン レイア

③ Word文書ファイル等を開く



セキュリティの警告 マクロが無効にされました。

このボタンをクリックすると、悪意のあるマクロが動作し、ウイルスに感染するおそれがあります。

CAUTION

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。