サイバーセキュリティの置き薬

2022年 第4号

Emotetウイルス感染が再拡大中！

昨年11月中旬に活動再開が確認されたEmotetに関し、感染が疑われる事案が2月より急速に拡大しています。複数のセキュリティ機関から注意喚起が促されており、感染防止にご注意ください。

Emotetの特徴、不審点

○　確認されている主な特徴

- メール本文の内容が3行程度と短い
- ExcelやWordのマクロ機能を悪用して感染させる
- パスワード付きZIPファイルを悪用して感染させる

○　注意すべき主な不審点

- 送信元メールアドレスの偽装（日本語表記に騙されない！）
- メールの件名が返信メールを装っている（「Re:」に注意！）

※これらの特徴にとらわれることなく、不審に感じるメールには要注意です。

Emotetの感染メールには、一見すると業務に関係がありそうな内容等で取引先や知り合いからの送付にみえるよう偽装されているものがあります！

Emotetに感染しないための対策

1．不審なメールは開かない
2．添付ファイル、URLリンクに注意する
3．マクロ機能を有効にしない

※　このほか、ウイルス感染しないために、OSやアプリケーション、セキュリティ対策ソフトを常に最新の状態にするなど、必要な諸対策を講じてください。

【参考】　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
JPCERT/CC　：　マルウェアEmotetの感染拡大に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220006.html