



サイバーセキュリティの置き薬

2019年
第13号

“Emotet (エモテット)” ウイルス感染を狙う攻撃メールに注意!

Emotet ウイルスへの感染を狙った攻撃メールが増加しています。攻撃メールは、知人や取引先といった過去にやり取りしたことのあるメールアドレスが用いられ、さらには返信メールを装って件名に「Re:」の表記が付くなど、巧妙な手口となっています。

また、メール本文には実際のメール内容の一部が引用される場合もあり、注意が必要です。

＜ウイルス感染しないための注意点＞



1. 不審なメールは開かない
2. 添付ファイル、メール本文中の URL リンクに注意
3. マクロ動作を有効にしない

攻撃メールに添付された Word ファイルを開くだけでは、一般的には Emotet ウイルスに感染しません。マクロ動作を有効にすることで、外部サイトから Emotet ウイルスがダウンロードされ、感染するものです。マクロを有効にする旨のメッセージには従わないようにしてください。

⇒ Word や Excel 等のマクロの設定（セキュリティセンター）を確認し、「すべてのマクロを有効にする」が選択されている場合は、マクロが自動実行される設定です。“マクロを無効にする”設定を選択してください。

注意：攻撃メール、感染手段には複数のパターンがある模様です。今後、これらは変化することも考えられます。



【参考サイト】

独立行政法人情報推進機構セキュリティセンター（IPA）

<https://www.ipa.go.jp/security/announce/20191202.html>