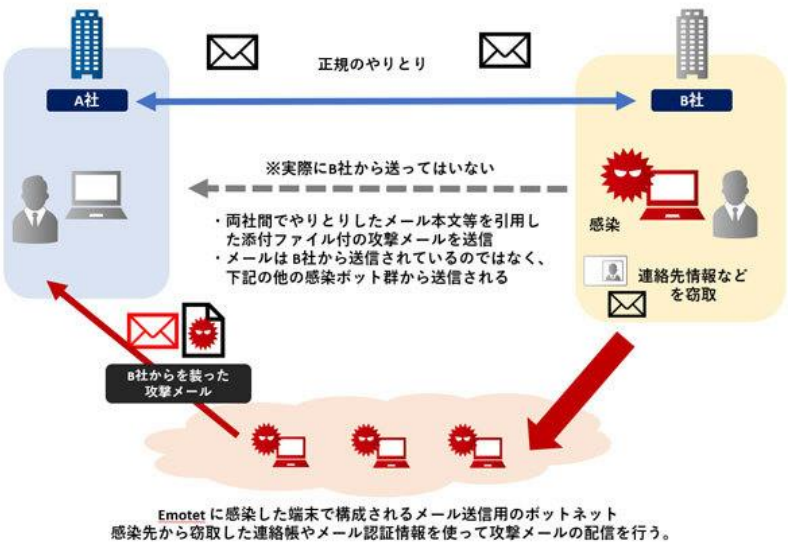
Ksisnetだより
発行:Ksisnet事務局
令和4年 2月 28日
Vol.103

活動を再開したEmotetに注意！

注意！

2021年末から活動を再開したEmotetの攻撃活動が２月に入り急増しています！！



実在の組織や人物になりすましたメールに、**マクロ付きのExcelやWordファイル、パスワード付ZIPファイル**が添付される形式で配信されており、これら添付ファイルを開封後に**「マクロを有効化する」**ことでEmotetに感染します。

また、メール本文中のリンクをクリックすることで悪性なExcelやWordファイルがダウンロードされたり、アプリケーションのインストールを装いEmotet感染をねらうケースも確認されています。

出典　JPCERT/CC

対　策

- ○　身に覚えのないメールの添付ファイルを開いたり、本文中のURLをクリックしたりしない
- ○　自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない
- ○　定期的にOSやセキュリティソフトをアップデートして最新の状態にする
- ○　信頼できないメールに添付の文書ファイルを開いた時に、セキュリティに関する警告が表示された場合「マクロ（コンテンツ）の有効化」ボタンはクリックしない
- ○　メールや文書ファイルの閲覧中、身に覚えのない警告ウインドウが表示された際、その警告の意味がわからない場合は操作を中断する
- ○　身に覚えのないメールや添付ファイルを開いてしまった場合は、システム担当者に連絡する

Emotetについては、**Ksisnetだより 第70号、第75号、第83号、第84号、第100号**においても情報提供しています。これらも参考にしてください。

IPA、JPCERT/CCが注意喚起しています。
下記のURLから詳細を確認してください

https://www.ipa.go.jp/security/announce/20191202.html#L18
https://www.jpcert.or.jp/at/2022/at220006.html