

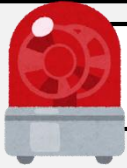
## マルウェア「Emotet」に注意!

電子メールにWordファイルを添付し、ウイルスを感染させるマルウェア「Emotet」。

新型コロナウイルスを題材にしたもの、パスワード付のZIPファイルを添付したものなど、様々な手口が確認されています。

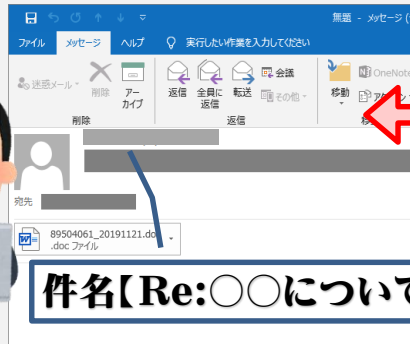


便乗詐欺にも注意!!!



令和3年2月から、警察庁、総務省、インターネットサービスプロバイダが連携して、Emotetに感染しているおそれのある利用者に対して、注意喚起を行っています。

取引先からのメールだ。件名に、“Re”が付いているから先週、話をした件の返信のメールかな。



実際に送信されていたメールを元に、メールのタイトルに“Re”を付け、送信することがあるので注意!

ん?セキュリティ警告? コンテンツの有効化? オッケー、オッケー! クリック!

件名【Re:〇〇について】

マクロ機能が有効化されることにより、ウイルスに感染してしまうので、“コンテンツの有効化”ボタンは押さない!

後日...



ちょっと!!! あなたからウイルス付きのメールが送られてきたわよ!



我が社の機密情報が漏れてしまった



- 情報が窃取される
- Emotetばらまきの踏み台にされる
- 社内の端末にEmotetを拡散させてしまう

### 対策!

- ✓ 電子メールに添付されたファイルは慎重に取り扱う
- ✓ マクロを自動実行しない設定にする
- ✓ OSを最新の状態にする

### 注意!

注意喚起を行っているインターネットサービスプロバイダから費用の請求や設定してるパスワードを聞き出すことはありません!

注意喚起に便乗した詐欺に注意をしてください!!

