

サイバーだより



令和2年1月8日

長野県警察本部
サイバー犯罪対策室

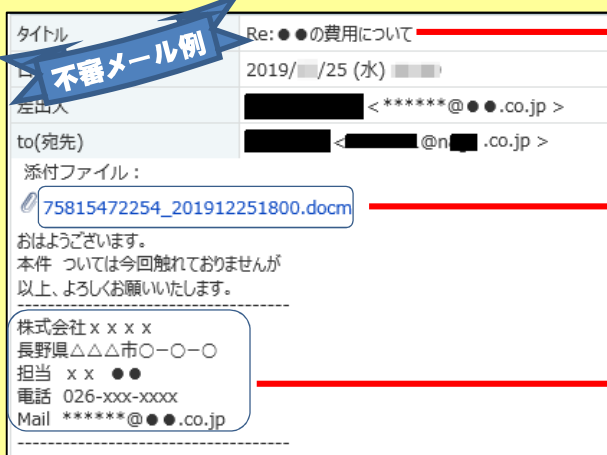
不審メールに注意!!! ~マルウェアEmotet被害が多発~

昨年10月頃から全国的にEmotetと呼ばれるマルウェアによる被害が多発しています。Emotetは、過去にメールのやり取りをした相手や実在の企業を装った者からのメールに添付されたマクロ付きのファイルを開くことで感染します。

このEmotetに感染すると、PC内に保存されたメール情報(メールのID・パスワード、メール内容等)を盗み見られ、そのメールが攻撃メールに流用されて他の者に送信して感染が拡大する特徴があります。

Emotetの感染を狙った不審メールの特徴的な例

- ・実在する企業等のメールを装う(文末に担当者名とメールアドレスを付ける等)
- ・件名に「Re:」をつけて返信メールを装う(過去に送受信した内容を引用している場合も)
- ・悪意あるマクロを埋め込んだWordやPDFファイルを添付する
- ・添付されたファイルを開くとマクロを実行させようとする
(マクロの自動実行になっていた場合、開いた時点で感染する)



返信メールを装う

ファイルを
クリックで感染

実在の人物及び
メールアドレスが記載

対 策

- ☑ 不用意に添付ファイルは開かない
- ☑ マクロの自動実行の無効化
- ☑ 組織内での注意喚起
- ☑ セキュリティソフトによる保護
- ☑ OSを最新の状態に維持

