サイバーセキュリティ対策通信

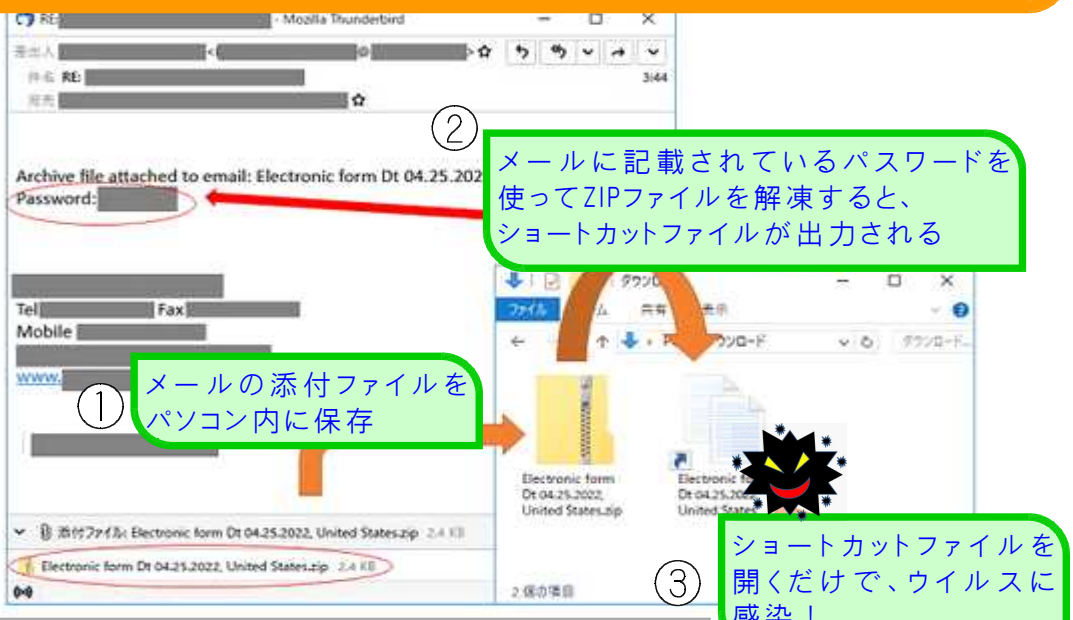
大阪府警察本部サイバーセキュリティ対策課

新たな手法によるEmotet攻撃に注意！

「Emotet」とは、実在の人物や取引先を装ったメールなどを介して感染を広げ、機密情報の漏洩やランサムウェアを引き込む等するマルウェア。これまでの手口として「Microsoft Office」製品のVBAマクロとして、送り付けられることが多く、対策としてマクロの無効化やブロックが有効だと考えられていました。

ところが！

メールに添付された「ショートカットファイル」を開くだけで感染する新たな手口が発生！！



【引用元】 ショートカットファイル型「Emotet」の動作原理（JPCERT/CCのWebサイト）

- **不用意にメールのショートカットファイルを開かない！**
- **以前にやり取りがある相手からのメールに見えても、タイミング等不自然な点があれば、電話で送信元に確認！**