

# 「ASTONE通信」



第 169 号  
2022 年 4 月 21 日発行

担当：小東 康人

## Emotet (エモテット)

Emotet は 2019 年 9 月に日本国内で大規模な拡散が発生した最怖のウイルスです。

その後は落ち着きをみせていましたが、2022 年 3 月に初回被害の約 5 倍の 1 日当たり約 1 万台のウイルス感染がありました。

Emotet の感染源は主にメールであり、感染力が高い理由はウイルスセキュリティソフトでは感染を防げないことにあります。

感染経路も巧妙であり、まず知り合いや仕事上の取引先から今までのメールでやりとりしていた文章に返信する形で送られてきます。

今までの会話履歴がメール本文にある状態で送信されてきて、添付ファイル「以下、メール添付ファイルの解凍パスワードをお知らせします。」と記載された添付ファイルや圧縮ファイル、或いは直接 Excel や Word が添付されている場合などがあり、それらをクリックして開き『コンテンツの有効化』をクリックすると Emotet に感染してしまいます。

Emotet 対策は各サイトや YouTube などに説明ありますが、怪しい添付ファイルには十分にご注意お願い致します。



### Emotet 被害 (例)

- ・メール関連の情報 (メールアドレス、本文、アカウント) が洩れる。
- ・他のブラウザで記憶されている ID やパスワードなどの情報が盗まれる。(Amazon、ヤフオク、ネットバンクなど) これは結構痛いです…
- ・パソコンが感染したら、その他マルウェアにも感染しやすい。

### 感染するとすぐに異変に気付きます！

- ・送信した覚えのないエラーメールが大量に受信される。
- ・メールの送受信が頻繁にフリーズする。

悪意をもって感染の拡大をさせるため、本人の知らないところで大量のメールを拡散送信しており、サーバーが重くなってしまいうほどの大量のメールを送信しているようです。

Emotet に感染しているかどうか確認する方法として、感染を調べるフリーソフト『EmoCheck』にてすぐにチェックできます。



＊「今月の名言」・・・目が覚めたら、まずは今日の生命に感謝する事である！