

Emotet感染確認ツール「EmoCheck」について

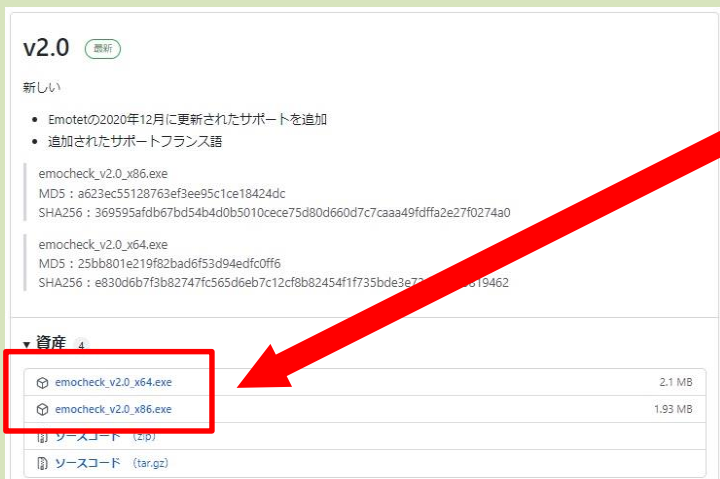
「Emotet」と呼ばれているウイルスの感染事案が発生しています。
今回は、Emotet感染確認ツール「EmoCheck」をご紹介します。

※「Emotet」については、令和3年12月発行のCyberNewsをご参照ください。

① EmoCheckのダウンロード

<https://github.com/JPCERTCC/EmoCheck/releases>

にアクセスします。



「Emocheck_v2.0_x64.exe」

又は

「Emocheck_v2.0_x86.exe」

のうち、使用しているパソコンのビット数の
実行ファイルをクリックします

※使用しているパソコンが、x64かx86が分から
ない方は、x64を試してください。

仮に間違ってもパソコンが壊れることはありません。

② Emotet感染確認



左図のようなウィンドウが立ち上がり、しばらくすると
EmoCheckの検索結果が表示されます。

感染していなかった場合は、左図のように
【Emotetは検知されませんでした。】
などと表示されます。

感染していた場合は、
【Emotetのプロセスが見つかりました。】
などと表示されます。
感染が確認された場合は、Emotetの駆除作業を行って
ください。

今回ご紹介しました「EmoCheck」は、JPCERT/CC（JPCERT
コーディネーションセンター）が作成・公開しているソフトウェアです。

「EmoCheck」は、定期的にバージョンアップがされますので、一度
だけではなく、頻繁にEmoCheckによる確認をお勧めします。

