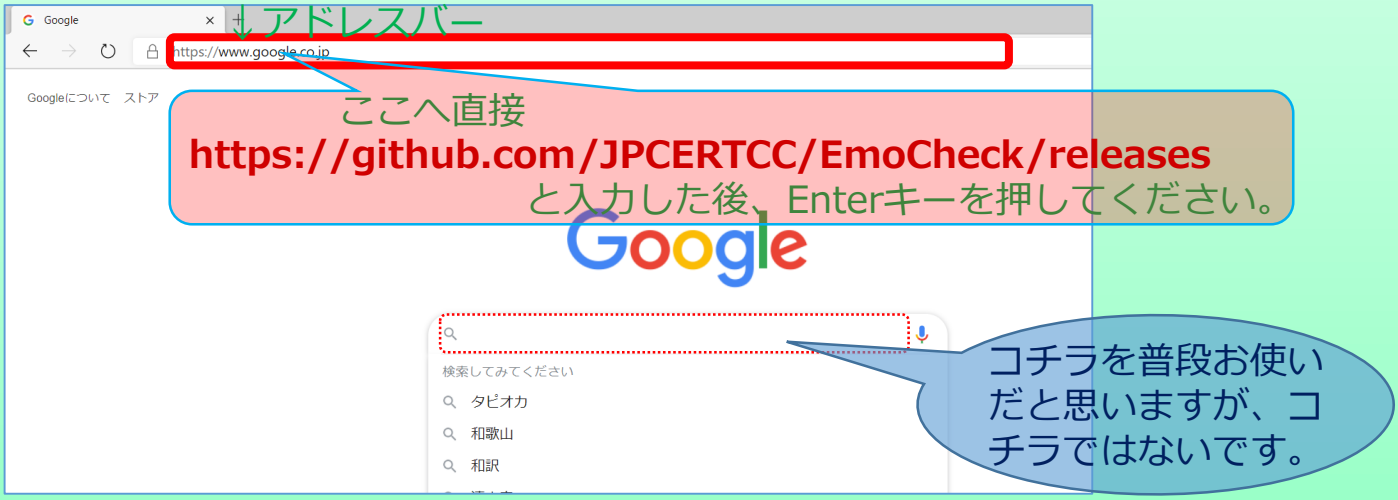
Emotet感染確認ツール「EmoCheck2.0」の実行手順

2022年3月4日に「v2.1」が公開されました!!

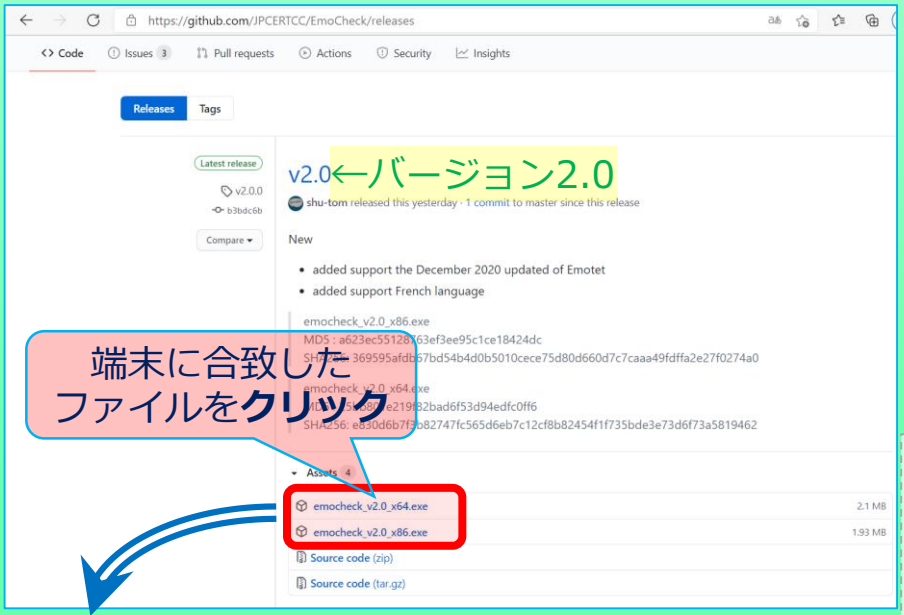
2022年に入り「Emotet（エモテット）」によるサイバー犯罪被害が激増しています。
エモテット感染を確認できる「EmoCheck」がJPCERT/CCから公開されており、昨年公開された「EmoCheck2.0」に加え、新たに「EmoCheck2.1」がアップされました。
本資料は「EmoCheck2.0」で手順を説明しますが、あわせて実行してみましょう。

①　「EmoCheck2.0」の入手（ダウンロード）

お使いのWebブラウザのアドレスバーに『**https://github.com/JPCERTCC/EmoCheck/releases**』と入力し、[Enter]キーを押してください

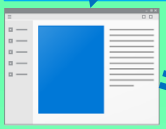


②　「EmoCheck2.0」の実行



デスクトップに表示された英文表記のページ(下図)が表示されますので、スクロールして、「**▼Assets4**」の下にある表のうち、お使いのパソコンのビット数表示がある方の実行ファイル（exeファイル）をクリックして確認を実行してください。

※　今お使いのパソコンの種類が、x64かx86かわからないという方は、**x86**で実行してください。
仮に違っていてもパソコンが壊れる等ということはありません。


emocheck_2.0_x64.exe

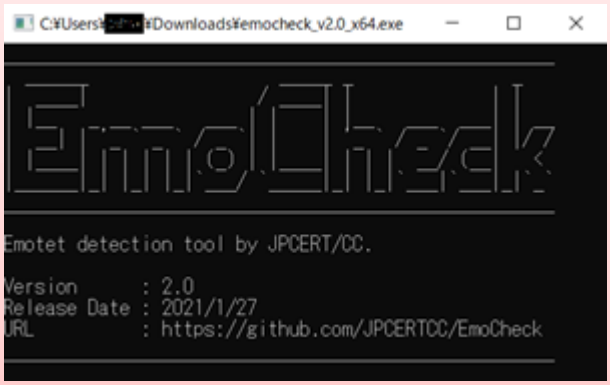
上記GitHubのウインドウの左下か、デスクトップ上にダウンロードされたこのアイコンのファイルをダブルクリック

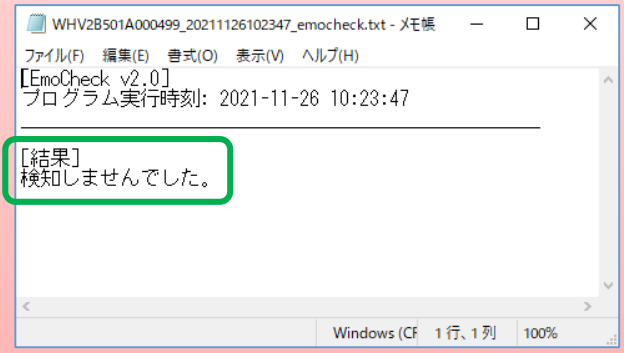
[実行]ボタンを押してチェック開始

※新たなバージョン「2.1」が更新されていますので、あわせて実行してください。

③　Emotet感染の確認

ア　感染していない場合





デスクトップ上には、左図のような黒色のウインドウが一旦立ち上がり結果が表示されます。

検索した結果は、デスクトップ上（またはEmoCheckがダウンロードされたファイル内）に新たに作成されたメモ帳（テキストファイル）にも記載されます。

メモ帳を開いた際、感染していなかった場合は、「**検知しませんでした。**」と表示されます。

この画面が表示された時点で、Emotetに感染していなかったことが確認できました。
一度で終わらず、定期的にEmoCheckによる確認をお勧めします。

イ　感染していた場合

感染が確認された場合には、EmoCheck実行後の黒色画面に黄色の囲み部分にある「**Emotetのプロセスが見つかりました。**」等と表示されます。
また、黄色の破線部分には、EmoCheck実行によりEmotetとして認識されたファイルそのものが存在する場所が表示されます。

ご自身でEmotetが駆除できるようであれば、駆除作業等が詳しく書かれている「**マルウェアEmotetへの対応FAQ**（JPCERT/CC Eyes　2019/12/02）」を参照して作業を行ってください。
駆除作業に自信がない方は、ご自身(または自社)で契約しているセキュリティベンダーに連絡するか、サイバーセキュリティの相談ができる方に駆除方法等を確認しながら対応してください。
万が一、相談する先がない方は、東京都で中小企業の方に対するサイバーセキュリティ支援を行っている機関の１つである
サイバーセキュリティ相談窓口（**０３-５３２０-４７７３**）
をご活用ください。

JPCERT FAQ

感染再拡大に関する注意喚起も是非ご覧下さい
https://www.jpcert.or.jp/at/2022/at220006.html
JPCERT 注意喚起