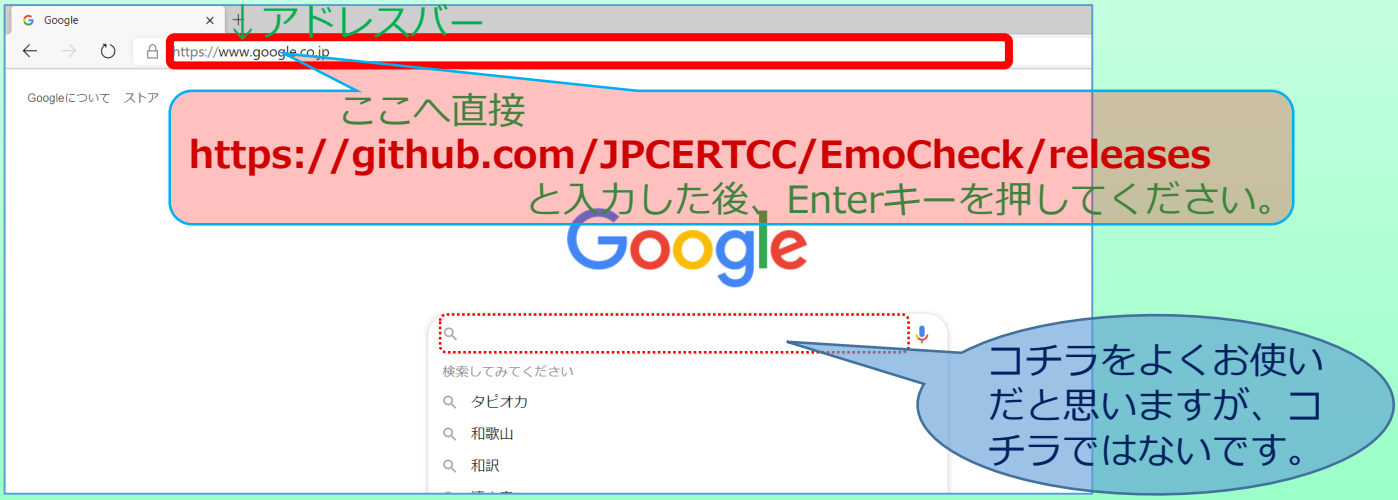
Emotet感染確認ツール「EmoCheck2.0」の実行手順

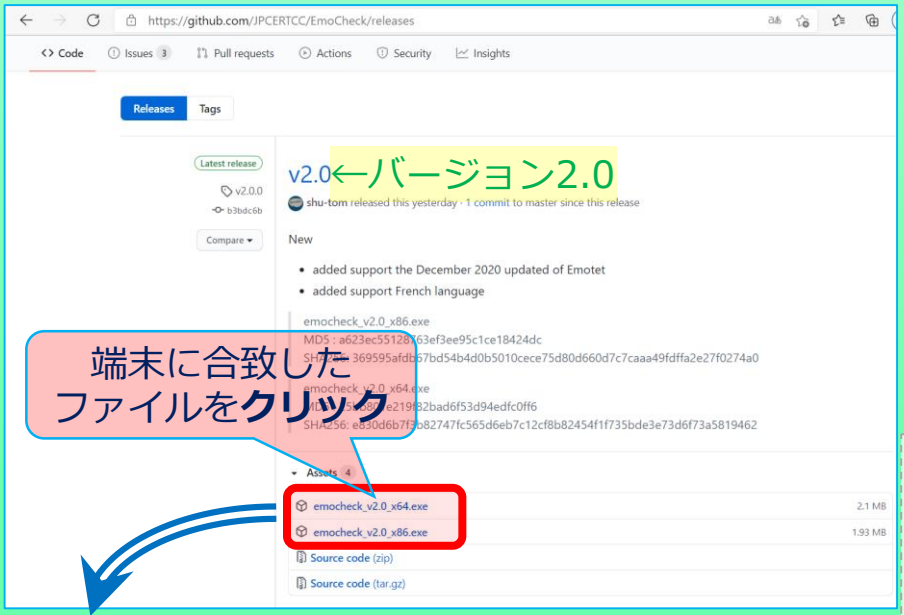
2021年1月に停止されたはずのマルウェア「Emotet（エモテット）」が、11月に入り再び稼働しています。
会社のパソコンが感染していないか、月に一度は感染の有無を確認してみましょう。

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

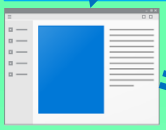


②　「EmoCheck2.0」の実行



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。

※　使っているパソコンが、x64かx86かわからない場合
調べる方法がわからないという方は、**x86**で実行してください。
（ちなみに、違っていたとしてもパソコンが壊れるということはありません。）

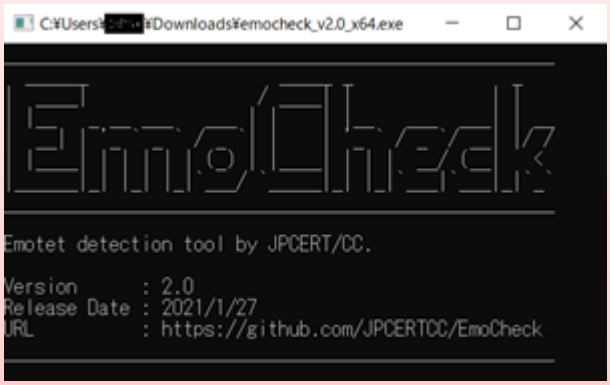


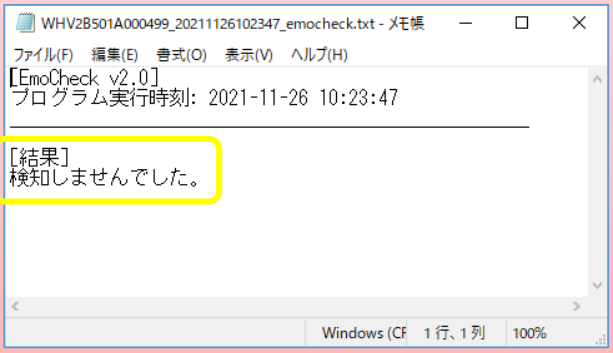
上記GitHubのウインドウの左下か、デスクトップ上にダウンロードされたこのアイコンのファイルをダブルクリック

[実行]ボタンを押してチェック開始

③　Emotet感染の確認

ア　感染していない場合





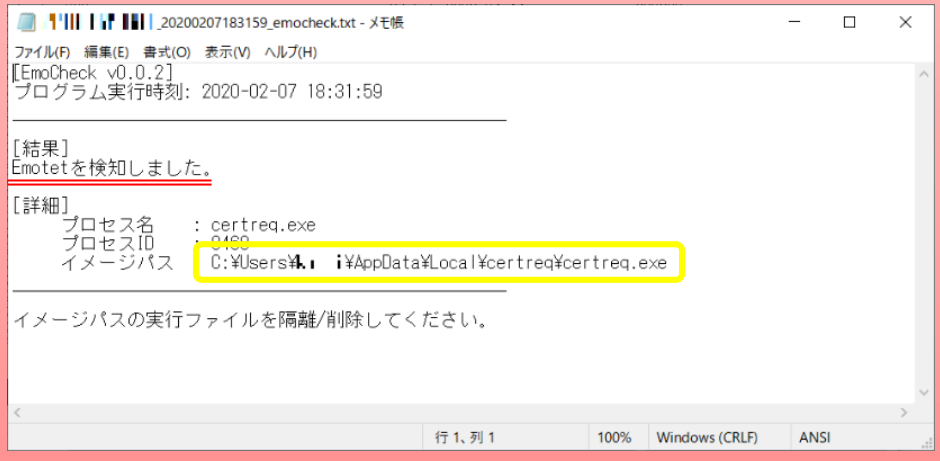
デスクトップ上には、左図のような黒色のウインドウが一旦立ち上がります。

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において、Emotetに感染していなかったことが確認できましたので、その後も定期的なEmoCheckによる確認をお勧めします。

イ　感染していた場合



メモ帳を開き、感染が確認された場合には、赤色下線部にあるように「**Emotetを検知しました。**」と表示されたものが表示されます。

黄色の枠の部分には、Emotetとして認識されたファイルそのものがある場所が表示されています。

ご自身で感染源の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。

もし、そのような駆除作業に自信がないという方にあっては、ご自身（または御社）で契約されているセキュリティベンダーに連絡をしていただくか、サイバーセキュリティに関して相談できる方がいらっしゃるようであれば、その方に駆除の方法等を確認しながら対応してください。

万が一、相談する先もないとおっしゃられる方にありましては、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