Emotet感染確認ツール「EmoCheck」の実行手順

エモテット感染を確認できる「EmoCheck」がJPCERT/CCから公開されています。「EmoCheck」は最新のエモテットに対応できるよう適宜更新されていますが、更新までの間、検出できないこともあります。最新のエモテットの検出が可能なバージョンであるかを確認してから使用しましょう。

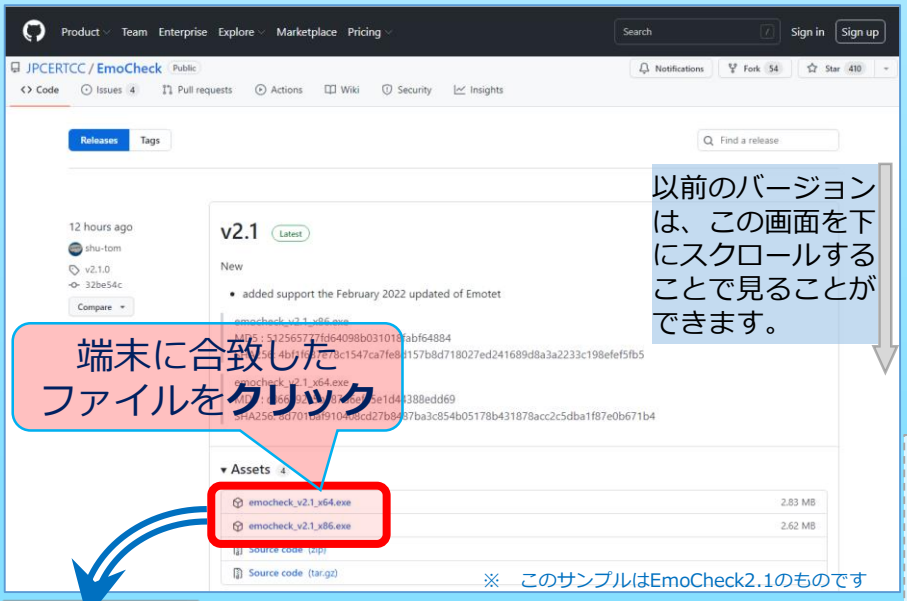
確認先はこちら⇒ JPCERT/CC「マルウェアEmotetの感染再拡大に関する注意喚起」

本資料では「EmoCheck2.1」で手順を説明します。

①　「EmoCheck」の入手（ダウンロード）

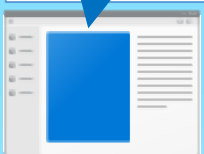
お使いのWebブラウザのアドレスバーに『**https://github.com/JPCERTCC/EmoCheck/releases**』と入力し、[Enter]キーを押してください

②　「EmoCheck」の実行

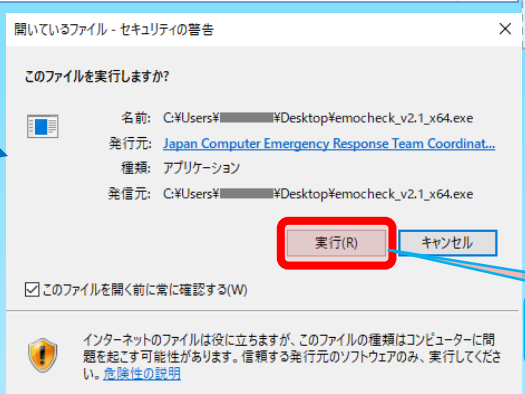


デスクトップに表示された英文表記のページ(左図)が表示されますので、スクロールして、「**▼Assets4**」の下にある表のうち、お使いのパソコンのビット数表示がある方の実行ファイル（exeファイル）をクリックして確認を実行してください。

※　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_2.1_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

※　今後も新しいバージョンが公開されることが予想されますので、定期的にこのページを閲覧してEmoCheckを実行するなどルール化に取り組んでください。

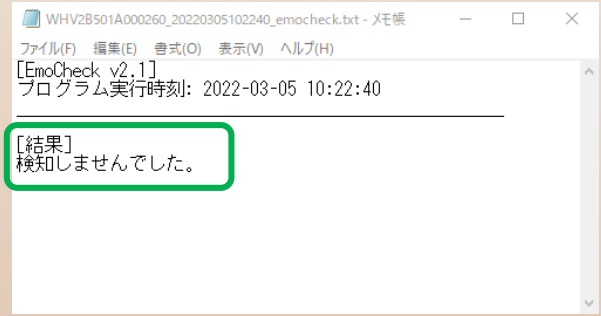
③　Emotet感染の確認

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。

黒色の画面が瞬時に消えてしまったとしても、メモ帳に検知しなかったと表示されれば、感染していないことが確認できます。

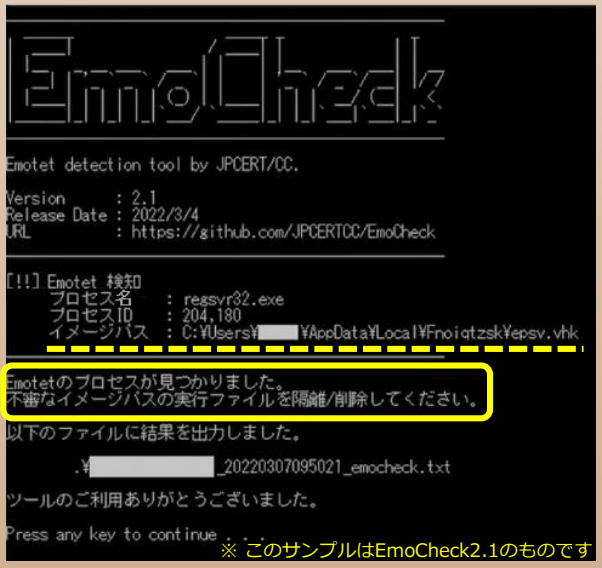


メモ帳を開いた際、感染していなかった場合は、「**検知しませんでした。**」と表示されます。

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。

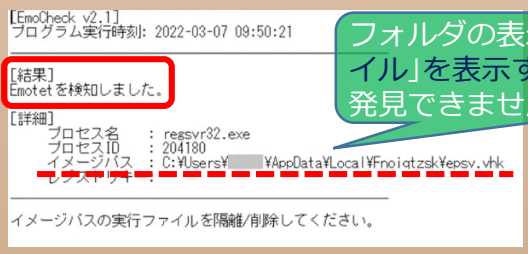
一度で終わらず、定期的にEmoCheckによる確認をお勧めします。

イ　感染していた場合



感染が確認された場合には、 EmoCheck実行後の黒色画面及びメモ帳に実線の囲み部分にある「**Emotetのプロセスが見つかりました。**」等と表示されます。

また、各画面の破線部分には、EmoCheckの実行によりEmotetとして認識されたものがイメージパスの項目に表示されます。



フォルダの表示設定で、「隠しファイル」を表示する設定にしないと、発見できません。ご注意ください。

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一読下さい

https://www.jpcert.or.jp/at/2022/at220006.html

JPCERT 注意喚起

警視庁サイバーセキュリティ対策本部