主催 警視庁サイバーセキュリティ対策本部

警視庁

中小企業向け

体験型

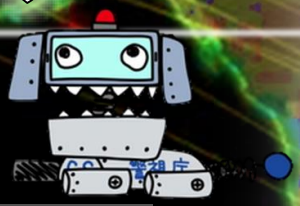
サイバーセキュリティセミナー

テレワーク勤務時代の今だからこそ知っておきたい

１人１台用意されたパソコンを使用し、実践的かつ臨場感のある被害体験と防御要領を解説

トップベンダー企業の講師が初心者にも分かりやすく解説！

セミナーで使用する冊子は、受講後にそのまま社内教養にも使用可能



日時場所

○　令和２年１１月５日（木）、６日（金）、９日（月）、１０日（火）
［於：文京区内］
※詳細な場所はおってご案内します。

○　令和２年１１月１２日（木）、１３日（金）
［於：立川商工会議所］

※　上記日程のうち、午前の部（９時～１２時）及び 午後の部（１４時～１７時）を選んでの受講となります。

講師

マカフィー株式会社　プロフェッショナルサービス本部シニアトレーナー

内容

・中小企業におけるサイバー犯罪、攻撃の情勢
・メールによるマルウェア感染、パソコンの乗っ取り体験
・サイバー犯罪、攻撃からの防御方法
・サイバー犯罪、攻撃を受けてしまった時の対処方法　等(予定)

受講無料

定員　各回１５名(合計１２０名)　**締切**　令和２年１０月８日まで

※　応募多数の場合、受講者の調整をさせていただきます。
　また、新型コロナウイルス感染拡大のためウェブにてセミナーを実施することもあります(裏面参照)。

申込方法

必要事項を明記したメール又は電話にて、下記問合せ先へお申込みください。
◎必要事項
・会社名(業種、従業員数、所在地、連絡先(電話、e-mail))
・受講者氏名、年代(○○歳代)、部署(役職)
・希望日時(日付及び午前午後の別、いずれか１つを選択)

※　記載していただいた個人情報は、本セミナー参加にかかる当選の有無やその他のご連絡及び新型コロナウイルス感染拡大防止対策以外の目的では使用しません。

お問合せ

警視庁サイバーセキュリティ対策本部　対策第二係（担当　児玉）
TEL　：03-3581-4321(内線7861-2234)
e-mail：cs-taio1＊keishicho.tokyo.jp（送信の際は＊を＠に変えてください）

※当セミナーにおける新型コロナウイルス感染症対策については、裏面をご覧ください。

●セミナーにおける新型コロナウイルス感染症対策について

新型コロナウイルス感染症対策のため、以下の対応の要領で、セミナーを開催いたします。ご理解の程、よろしくお願い申し上げます。

１　受講に際しての留意事項
- ○　過去２週間、発熱、咳、倦怠感、味覚嗅覚の異常などの新型コロナウイルス感染を疑われるような症状がないこと
- ○　同居家族や身近な知人などに新型コロナウイルス感染を疑われるような症状がないこと

２　セミナー当日における皆さまへのお願い
- ○　手指の殺菌消毒、マスクの着用をお願いいたします。なお、消毒液は会場に設置いたします。
- ○　非接触体温計を用いた検温をいたします。その際、３７．５度以上の発熱を確認した場合又は、検温に応じない場合は受講できません。

３　会場対策について
- ○　会場の窓・ドアを開放し、空調設備で換気を行います。
- ○　受講者ごとに、十分な座席空間（２メートル程度）を確保します。
- ○　講師・職員は、検温を実施し、マスク・手袋を着用いたします。また、講師と受講者の間には、遮蔽板を設置します。
- ○　毎回、会場内のパソコン・机・備品等の消毒をいたします。
- ○　配布資料は、予め机上に設置します。
- ○　終了後、他の受講者に感染が認められた場合は、速やかに受講者の方々に連絡いたします。

●Web セミナーを実施する場合について

今後、新型コロナウイルスの感染が拡大した場合は、インターネットを使用した Web セミナーを実施する場合があります。その際は、概ね２週間前までに連絡いたします。

Web セミナーは、マイクロソフト社のビデオ会議システム「Microsoft Teams（マイクロソフト　チームズ)」を使用しますので、以下のインターネット環境が必要になります。あらかじめご了承ください。

【パソコンを利用の場合】	【スマートフォンを利用の場合】
〈対応 OS〉 Windows8.1、macOS10.11 以上	App Store 又は Google Play で「Microsoft Teams」アプリをダウンロード
〈ブラウザ環境〉 ・Microsoft Edge（最新バージョンの２世代前までサポート） ・Google Chrome（最新バージョンの２世代前までサポート）	〈動作環境〉 ・iOS 端末（最新バージョンの１世代前までサポート） ・Android 端末（最新バージョンの３世代前までサポート）

※上記インターネット環境がなくても当セミナーに応募できます。

Emotet感染有無の確認ツールEmocheckの実行手順

簡略版

①

JPCERT/CCのホームページを開く。

②

JPCERT/CCのホームページを下にスクロールし、「おすすめ情報」欄にあるJPCERT/CC Eyes「マルウェアEmotetへの対応FAQ」感染チェックツールを追加をクリックする。

③

JPCERT/CC Eyes「マルウェアEmotetへの対応FAQ」のページの項目番号

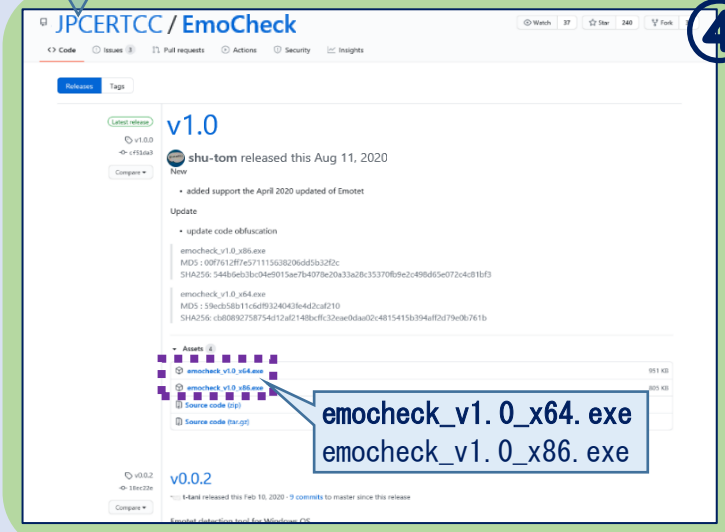
2-1-1　EmoCheckのダウンロード

まで移行し、項目番号2-1-2の直上にあるリンク（URL）

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

をクリックする。

④



JPCERTCC/EmoCheckのページに移行後、「v0.0.2」の直上にある「▼Assets④」の中から、お使いのパソコンが

64bitパソコンであれば

emocheck_v1.0_x64.exe

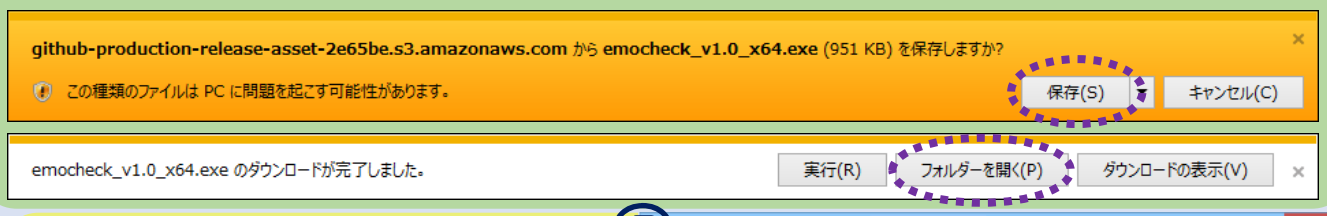
32bitパソコンであれば

emocheck_v1.0_x86.exe

をクリックする。

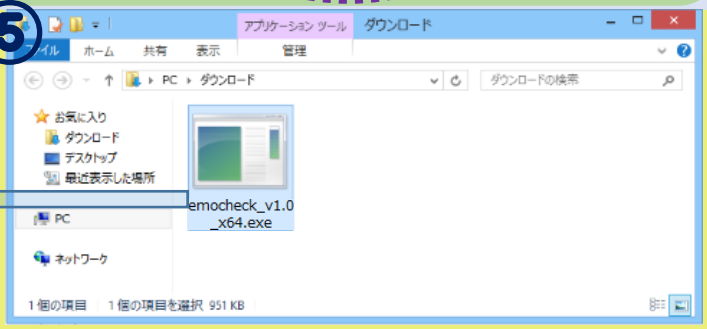
※ご使用のパソコンのビット数がわからない場合は「emocheck_v1.0_x86.exe」で実施してください。

前④の図内にあるファイル部分（.exe）をクリックしたとき、パソコンによっては下記のような警告が画面下部に表示されますが、手順どおりに進めている場合は、「保存(S)」をクリックし、ダウンロード完了の表示がでたら「フォルダーを開く(P)」をクリックしてください。ファイルは「ダウンロード」フォルダに保存されます。



⑤

「ダウンロード」フォルダ内に保存された「x64.exe」ファイルをクリックし、確認ツールを実行してください。

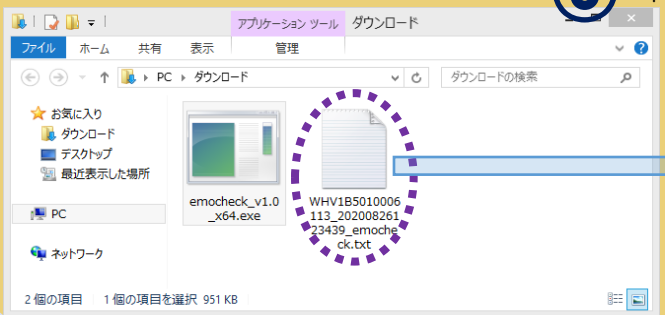


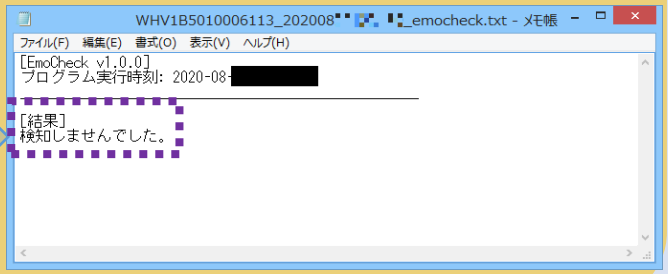
※ここでもセキュリティの警告画面が表示されますが、「実行(R)」をお選びください。

実行後に表示された画面を閉じ、再び「ダウンロード」フォルダを確認すると、新たにテキストファイルが作成されていますので、そのテキストファイルを開き、内容を確認してください。

感染の事実が確認できなかった場合には、「検知しませんでした。」と記載されます。

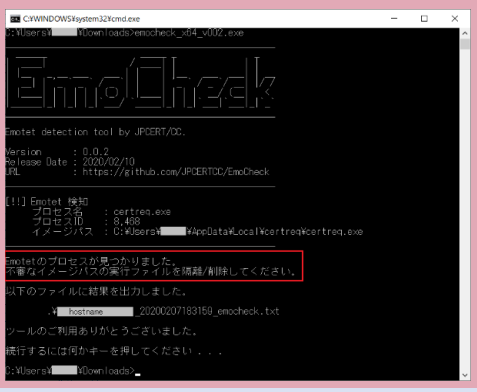
⑥





もし、**感染の事実が確認できてしまったら…**

テキストファイルに「Emotetを検知しました。」と記載されていた場合、早急に対応をする必要があります。詳しくは、③の**対応FAQ「2-1-3.感染時の対応」**をご確認いただきご自身で駆除していただくか、パソコンに精通している方（セキュリティベンダー等）にご相談ください。



2020年9月7日 第3版

一般社団法人ＪＰＣＥＲＴ（ジェーピーサート）コーディネーションセンターが公開したマルウェア「Ｅｍｏｔｅｔ（エモテット）」の感染確認ツール

ＥｍｏＣｈｅｃｋ（エモチェック） Ver1.0 の使用手順

警視庁サイバーセキュリティ対策本部

はじめに

2019年11月に報道されたマルウェア[1]「Emotet（エモテット）」を御存知ですか。

「Emotet」は、攻撃者が、日本で多く使われている**WindowsOSのパソコン**をマルウェア感染させるため、Microsoft Officeソフト（「Word」など）のマクロ（Macro：操作手順などを記録して自動的に実行する機能）を悪用したファイルをメールに添付して送信し、受信者がそのマクロを起動することによって感染[2]するマルウェアです。

「Emotet」に感染すると、会社のパソコン内のメールに関する情報の窃取に加え、更にその情報などを攻撃者が悪用し、他者に対する新たな攻撃メールの道具として知らぬ間に利用されてしまいます。

「Emotet」による脅威は、2020年２月以降休止状態であったものの、同年７月中旬から再び日本国内に向けて攻撃が開始されたことにより感染例が急増しております。

このような状況の中、インターネットによる不正アクセスの被害に対応するために設立された情報提供機関で、原因の分析や対処法を考案するなど、コンピュータセキュリティ関連情報の発信を行っている一般社団法人ＪＰＣＥＲＴ（ジェーピーサート）コーディネーションセンター（JPCERT/CC）が、2020年２月に「Emotet」の感染の有無をチェックする「EmoCheck（エモチェック）」を公開し、同年８月に更新しました。

「EmoCheck」は、インターネットの「GitHub（ギットハブ）」というサイトからお使いのパソコンに適合したものをダウンロードすれば、簡単に「Emotet」に感染しているか否かをチェックできるツールです。

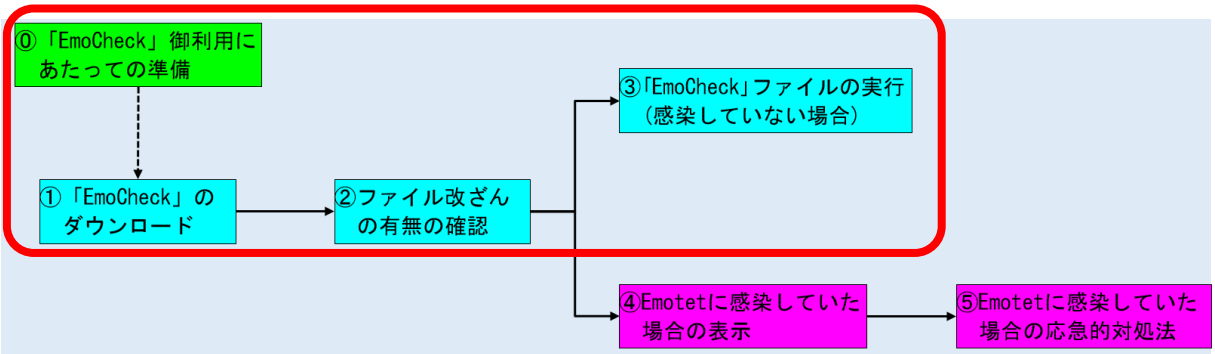
本資料は、「EmoCheck」を使って**誰もが感染の有無をチェックできる**よう、「Emocheck」のダウンロードから起動、「Emotet」の感染確認までの手順について、図を多く取り入れて説明したものです。

---

[1] マルウェアとは、「悪意のある不正ソフトウェア」、「有害なソフトウェア」、「不正プログラム」などと呼ばれる不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアや悪質なコードの総称。コンピュータウイルスやワームなどが含まれる。

[2] 日本における主な感染経路は、メールに添付されたOfficeファイルから感染させるものであるが、メール本文に付けられたURLから感染させる手法もある。いずれもOfficeファイルのマクロ機能を悪用してマルウェアに感染させるものである。

本資料は、次の図の番号どおりに「EmoCheck」の使用方法とそれぞれの表示画面について案内しており、特に⓪から③までの部分をメインに作成しています。



なお、マルウェア「Emotet」に関する情報や、図の④及び⑤について詳しい情報を入手する場合は、本資料を作成する元となった JPCERT/CC によって公開されている「マルウェア Emotet への対応 FAQ[3]」を御参照ください。

今回説明している「EmoCheck」は、2020 年８月に公開された「**v1.0**」というバージョンのものを使っており、今後もバージョンアップされていくものと思われます。

是非、**本資料をきっかけとして、新たに費用を掛けなくてもできるサイバーセキュリティ対策に取り組んでいただく方法を知っていただく**とともに、会社でお使いのパソコンだけでなく、御家庭のパソコンでも、このツールのバージョンが変わる度に一度はチェックをしていただき、より安全なインターネット環境下でパソコンをお使いいただければと思います。

本手順書では、皆様に当方から紹介するツールの改ざんによる被害を防ぐため、感染の有無を確認する作業以外の工程についても紹介しております。

感染の有無のみを確認する場合には、本資料

4 ページから始まる『①「EmoCheck」のダウンロード』及び

8 ページから始まる『③「EmoCheck」ファイルの実行』

を御参照ください。

[3] https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

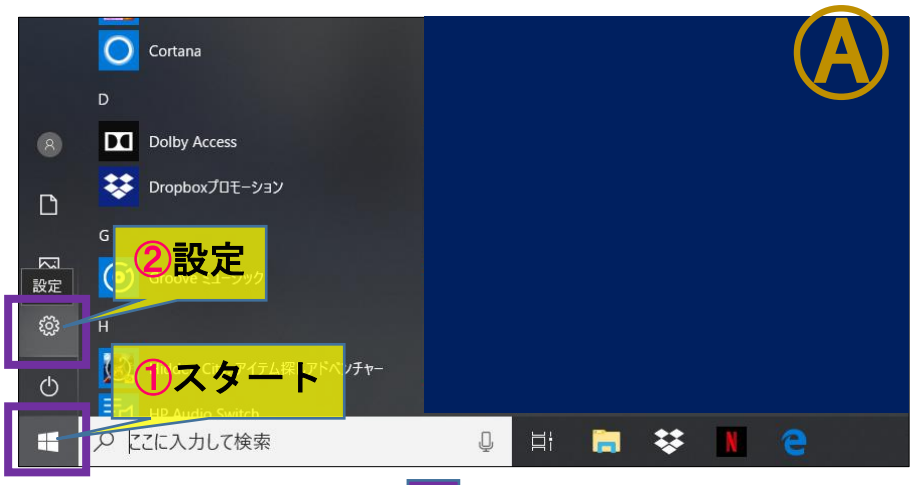
⓪「EmoCheck」御利用にあたっての準備

「EmoCheck」は**64 ビット版**と**それ以外版**があります。

どちらか分からない場合は、次の方法で確認することができます。なお、本資料においては、Windows10 の画面で説明します。

分かる場合は、①「EmoCheck」のダウンロードへお進みください。

デスクトップ画面左下にある**スタート①**ボタンをクリックし、スタートボタンの上に現れる歯車のマーク（**設定②**）をクリックする。



表示された「Windows の設定」画面で、「**システム③**」をクリックする。

開いた「システム」画面の左下に表示される「**バージョン情報④**」をクリックし、バージョン情報画面を表示させたところで、「デバイスの仕様」の下に表示される「**システムの種類⑤**」を確認してもらうことで、64 ビットか 64 ビット以外かが判別できる。

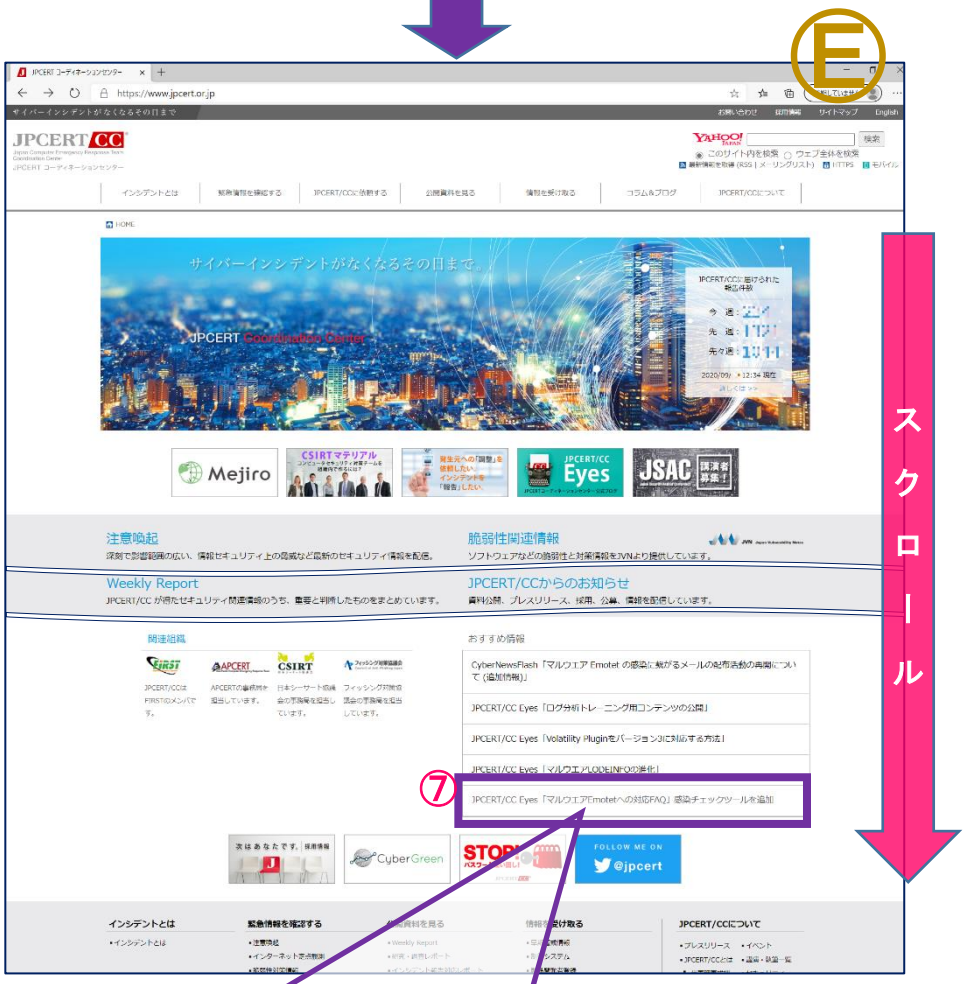
本資料では、Windows10 における 64 ビット版か否かの判別方法について説明をしていますが、Windows8.1 または Windows7 のパソコンをお使いの場合で、動作環境がわからないときは、NEC が提供している「121ware.com[4]」等を参照して御確認ください。

なお、上記の説明をお読みいただいた時点で、操作方法が分からない場合は、社内でシステムを担当されている方、または、パソコンの操作に慣れている方に依頼してください。

①「EmoCheck」のダウンロード

図Ⓓ「Google」等の検索サイトで、**JPCERT/CC の URL⑥**を入力し、ホームページを検索して表示する。

図ⒺJPCERT/CC のホームページの最下部にある「**おすすめ情報**」欄にある「**JPCERT･CC Eyes「マルウェア Emotet への対応 FAQ」感染チェックツールを追加⑦**」をクリックする。



JPCERT/CC Eyes「マルウエアEmotetへの対応FAQ」感染チェックツールを追加

[4] https://121ware.com/qasearch/1007/app/servlet/qadoc?QID=018406「インストールされている Windows が 32 ビットか 64 ビットか確認する方法」

表示された「マルウェア Emotet への対応 FAQ」画面Ⓕを下方向にスクロールし、「2.1.1 EmoCheck のダウンロード」とある項目の下に表示された URL⑧をクリックする。

※　なお、図Ⓕが掲載されているサイトのページには、攻撃者が「Emotet」に感染させようとして実際に送信したメールや、感染後の対処方法も記されているページ[5]となっているので、是非御覧ください。

リンク先である GitHub のページⒼに移動する（画面左上に「JPCERTCC/EmoCheck」と表題がある全文英文の画面が表示される）。
右画面の下部にある項目名「Assets 4」の部分にある表から、ダウンロードするアプリケーションを選択する。

[5] https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

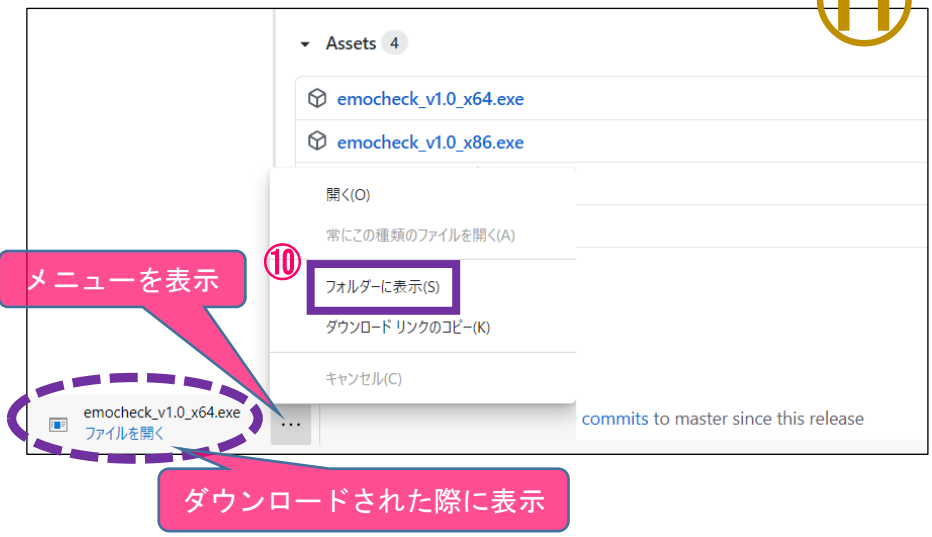
図Ⓖ部分拡大図

Ⓖ’

お使いのパソコンが64ビットであれば、「**emocheck_v1.0_x64.exe⑨**」を、それ以外であれば、その下にある「emocheck_v1.0_x86.exe」をクリックする。

Ⓗ

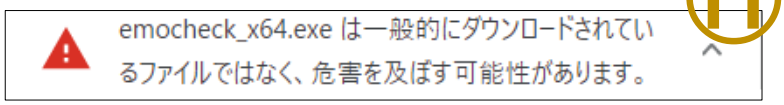
クリック後、ダウンロードするファイルの操作（処理）について確認されるので、「**フォルダーに表示(S)⑩**」を選択し「EmoCheck」ファイルをダウンロードする。



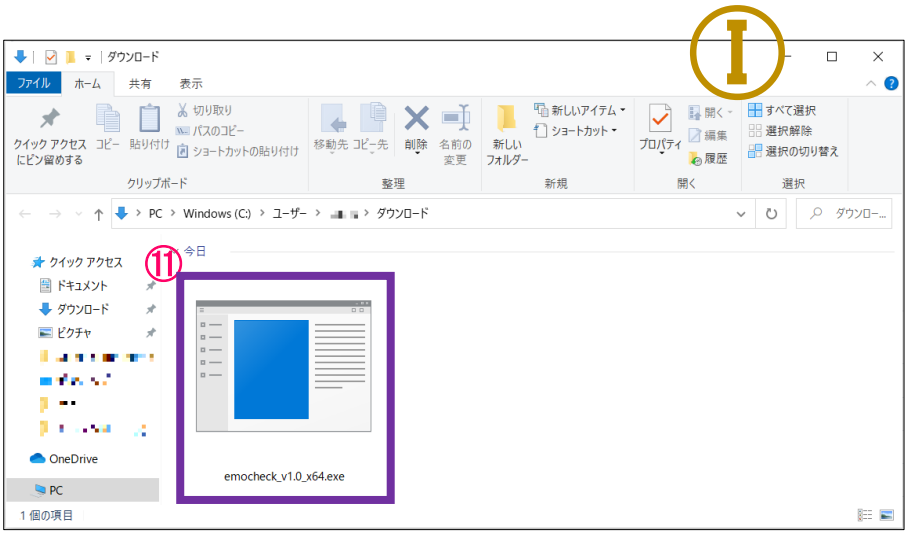
※　使用しているパソコンの環境により、図Ⓗと異なる表示がされた場合、できれば「EmoCheck」ファイルをそのまま実行させず、一旦「**保存**」する手続きをお取りいただき、「**フォルダーを開く**」などの順にクリックして、「EmoCheck」ファイルがパソコン内の「ダウンロード」フォルダー内等に保存されたことをご確認の上、お進めください。

※　お使いのブラウザがGoogle Chromeの場合、「Emocheck」ファイルをダウンロードする際に図Ⓗ’のような警告を発することがありますが、前記の手順で行っていれば、ダウンロードしてください。

Ⓗ’



図Ⓗの「**フォルダーに表示(S)⑩**」ボタンをクリックした後、デスクトップ画面上に、図Ⓘの「ダウンロード⑪」フォルダーが展開され、フォルダー内にファイルが保存されたことが確認できる。



②ファイル改ざんの有無の確認

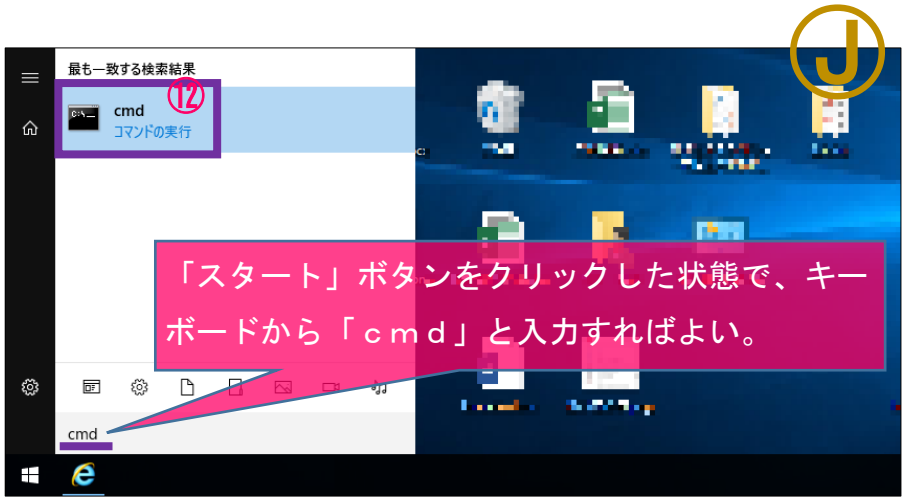
昨今、ネット上にアップロードされたサイトやファイルが改ざん（書き換え）される事案も多く発生しています。

そこで、ファイル改ざんの有無の確認などに使われるハッシュ値（ハッシュ関数を用いてファイルごとに付される固有の値）を使って確認作業をします。

※　ファイル改ざんの確認については、９月７日時点において、ハッシュ値が同一であることを確認しています。

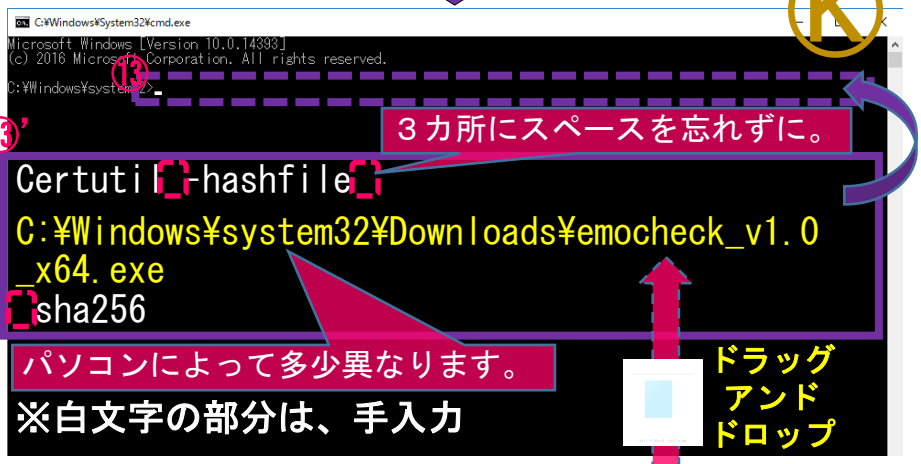
図Ⓖ中にある「SHA256」として記載された 64 文字の文字列がハッシュ値と呼ばれるもので、図Ⓗの手順により「ダウンロードした EmoCheck」ファイルが、JPCERT/CC が正規にサイト（GitHub）上に用意した「EmoCheck」ファイルと同一のものか否かを確認します。

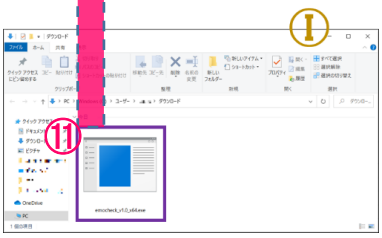
図Ⓙ画面左下のスタートボタンをクリックした後、続けて「検索入力」欄にキーボードから「ｃｍｄ」と入力し、現れた「**ｃｍｄ**[6]⑫」**をクリック**する。



[6] 「ｃｍｄ」とは、「**コマンドプロンプト**」と呼ばれる命令文（コマンド）を用いて Windows の操作や設定を行うためのツールの略号で、今回はファイルの同一性の確認と、「EmoCheck」ファイルを実行するために使用します。

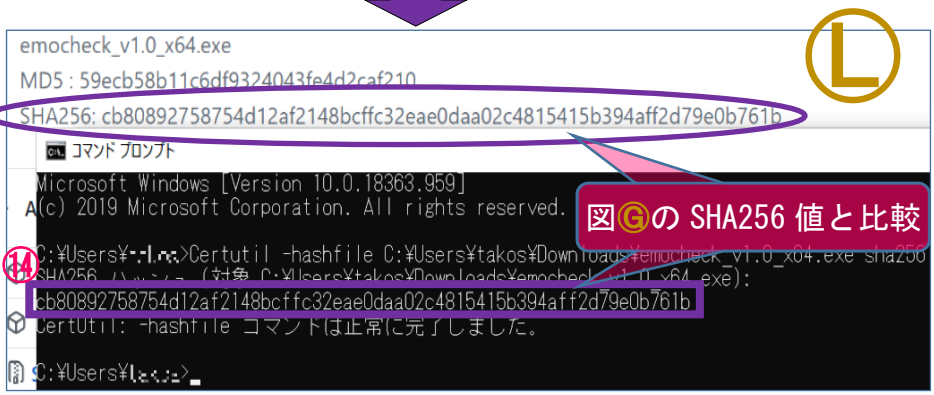
表示された図Ⓚのコマンドプロンプト画面（真っ黒なウインドウ）で、最終行に表示された「>」の後ろの点滅するカーソル「_」の位置⑬に、**⑬’の文字列を入力**しEnterキーを押す。





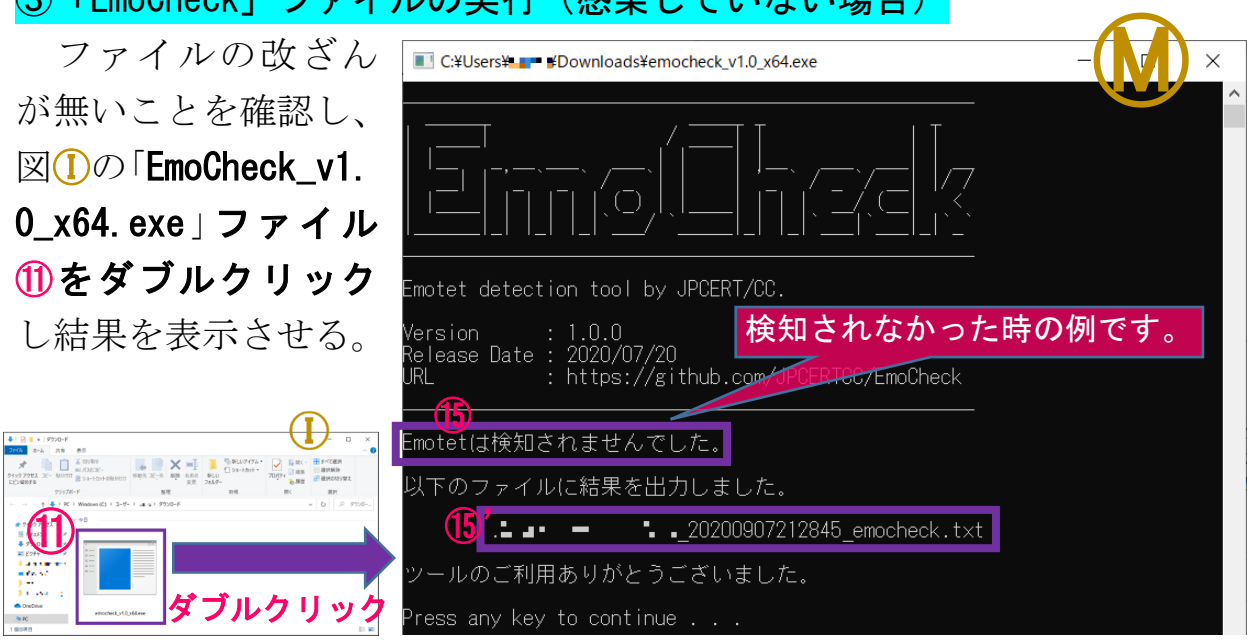
※⑬’内の黄色の文字部分は、前記図Ⓘの「EmoCheck」ファイルが置かれた場所を入力するのですが、手入力では手間がかかり、打ち間違いも生じやすいことから、同図Ⓘの**「EmoCheck」ファイル⑪をコマンドプロンプト画面上にドラッグアンドドロップ**することで、自動入力させることができます。

Enterキーを押した後「EmoCheck」ファイルのハッシュ値（SHA256）が⑭の位置に表示されるので、6頁図Ⓖや図Ⓖ’に表示されていたSHA256の文字列と同じであることを確認する。

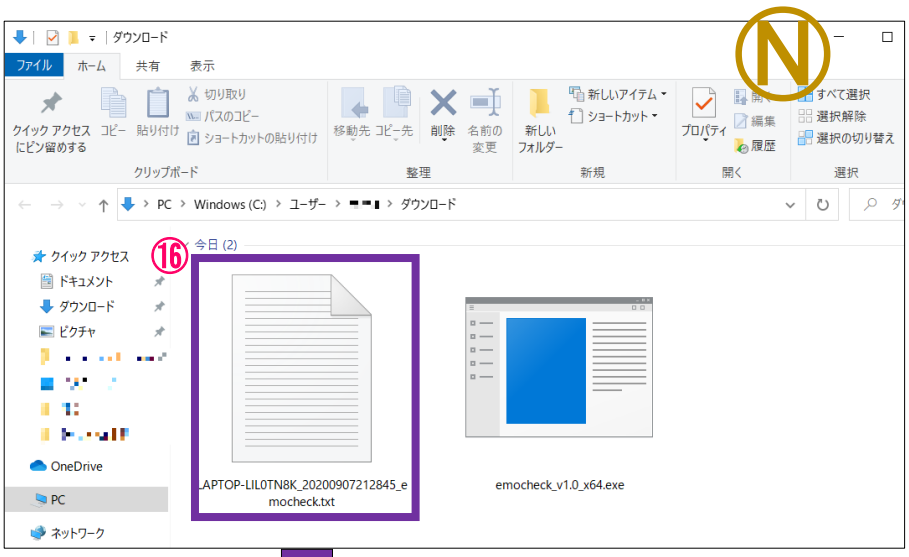


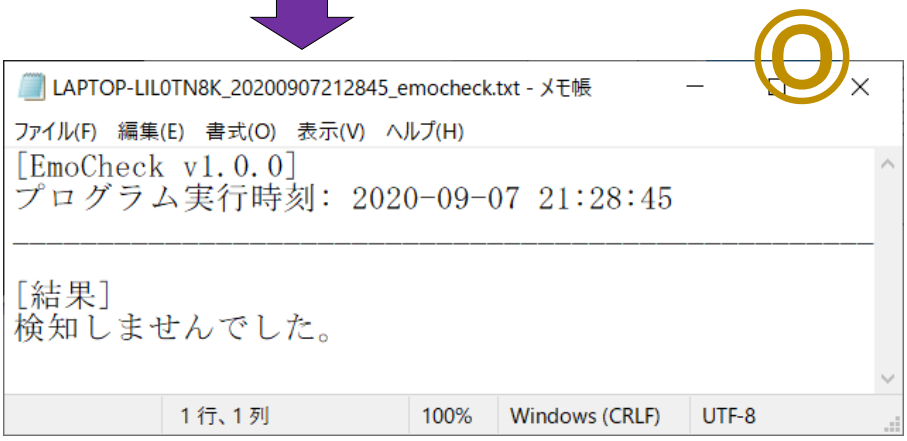
③「EmoCheck」ファイルの実行（感染していない場合）

ファイルの改ざんが無いことを確認し、図Ⓘの**「EmoCheck_v1.0_x64.exe」ファイル⑪をダブルクリック**し結果を表示させる。



前頁図Ⓜの下から４行目（⑮’部分）に新たに検索結果のテキストファイル（.txt）が出力された旨の記載があり、図Ⓝの**テキストファイル⑯が「EmoCheck」ファイルと同じフォルダーに作成**される（テキストの内容を開くと図Ⓞの文書が書かれていることが確認できる）。



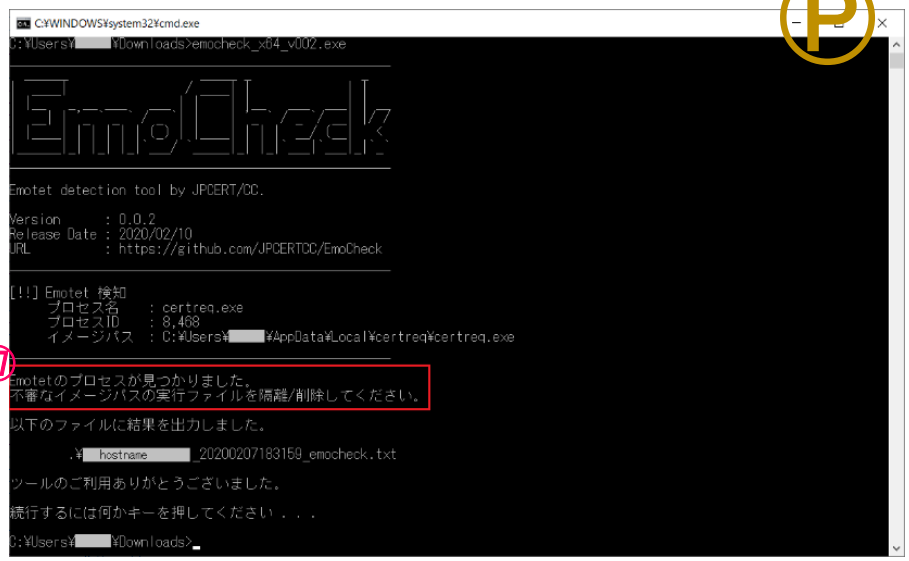


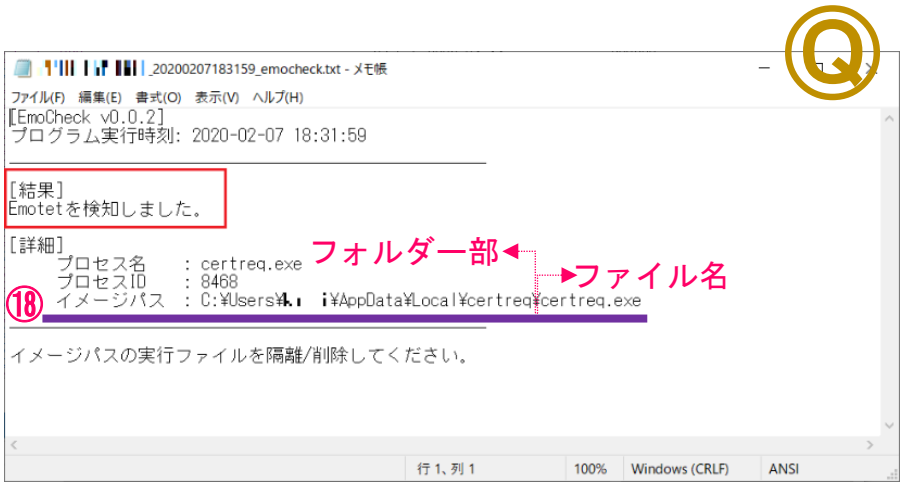
④Emotet に感染していた場合の表示

③までは、お使いのパソコンが「Emotet」に感染していないことを前提に図で説明してきました。

ここからは、前頁の図Ⓛまで作業が進み、チェックした結果、感染ありの場合について、６頁図Ⓕ「**マルウェア Emotet への対応 FAQ**」に掲載されている図を使って説明します。

感染したときの図Ⓟの⑰の部分と、感染なしのときの図Ⓜの⑮部分との比較でわかるように、見つかった旨の通知とともに、**Emotet と思われる不審なファイルを削除等するよう通知**される。





感染していなかったときと同様の手順で出力されたテキストファイルを確認すると、「EmoCheck」で**検知した不審なファイルがある場所**（図Ⓠの⑱「イメージパス」とある部分）を通知し、前頁図Ⓟと同じく、隔離や削除するように通知される。

※　もし、Emotet を検知した場合で、「イメージパス」の部分に何も表示されなかった場合は、**Emotet が管理者権限で動作している可能性がある**ため、「EmoCheck」を管理者権限で**大至急**実行してください。

⑤Emotet に感染していた場合の応急的対処法

万が一、「感染あり」と通知された場合には、JPCERT/CC によれば

⑴　タスクマネージャーを起動し、「詳細」タブから実行結果に表示された検出名のファイル（図Ⓠの⑱イメージパスの一番右にある「¥」マーク以降の文字列がファイル名）を選択して**タスクの終了を選択**する

⑵　（図Ⓠの⑱）イメージパスのうちフォルダー部をエクスプローラーで開き、表示されている「**exe**」**ファイルを削除**する

ことの２つの操作によって Emotet の無効化をします。

しかし、上記⑴、⑵の２項目を**読んだ時点で、意味が分からない場合や、どのように操作すればいいのか分からないときは、その時点でパソコンの操作を中断してください。**

中断する際には、**Emotet を検知したパソコンの LAN ケーブルを抜く、無線 LAN から切り離すなどしてインターネットの環境から検知したパソコン自体を隔離**し、直ちに社内でシステムを担当されている方、または、パソコンの操作に長けている方に隔離・削除作業を依頼するか、システムのセキュリティに関して契約しているセキュリティ会社があれば、連絡するなどして**早急に対応**してください。

Emotet に感染していた場合は、感染を確認したパソコン自体は、Emotet の削除という作業が必要となり、さらに、社内ネットワークのパソコンに感染が広がっていないかを確認しなければなりません。

Emotet に感染していると、不正送金をされて資産を失ったり、ランサムウェア[7]などの別のマルウェアに感染したりする可能性があるからです。

また、Emotet に感染していたことが判明した場合、その特性から

- 過去に送受信したメールアドレスと表示名
- 過去 180 日に送受信したメールのメール件名とメール本文（添付ファイルは除く）
- Web ブラウザに保存されていた認証情報

などが盗まれている（漏えいしている）可能性があります。

メールアカウント（メールアドレス等）が漏えいしてしまった場合、被害は自社内だけに留まらず、漏えいしたメールアカウントなどの情報が攻撃者に悪用されて、他社に向けてマルウェア感染を目的としたメールを送信する道具として使われているかもしれません。

感染を確認した際は、自社内での対応と同時に、他社への被害が拡散しないよう、早期に連絡して注意喚起を発するなどの対策をとり、感染拡大の防止に努める必要があります。

※　このような処理をしないで済むように、「Emotet」等のマルウェアに関して、日頃から意識を向けておく必要があります。

メールを悪用したサイバー攻撃の対処法としては

① 「何かおかしい」と感じた受信メールに添付されたファイルは、安易に開かない（特に、「**マクロを有効にする**」と表示されることがある **Word や Excel などの添付ファイル**）

② マルウェアが仕込まれたメールに気付けなかった場合でも、パソコンが検知して対処してくれるよう、セキュリティ対策ソフトの定義ファイルを常に新しいものに更新しておく[8]

という単純なことも、被害に遭わないためのセキュリティ対策の一つとなります。

被害に遭わないようにするための対策として、何ができるのかをこの機会に御検討いただければ幸いです。

---

[7] **ランサムウェア**に感染すると、パソコン内のデータが暗号化され、データがすぐには使えないように加工されてしまい業務が停滞します。データを元の状態に戻す場合、暗号資産(仮想通貨)で金銭を支払うように要求され、業務面だけでなく資産面でも被害を受けることになります。

[8] 自動更新に設定していれば考える必要がなくなりますので、自動更新の設定になっているか確認してください。

おわりに

以上で、JPCERT/CC から公開された「EmoCheck」の使い方についての説明は終わりとなります。

ところで、皆さまのパソコン内に常駐している「セキュリティ対策ソフトでは Emotet の検知ができないのか」というと、そんなことはありません。

ただし、セキュリティ対策ソフトが、マルウェアをマルウェアとして認識できるバージョンの定義ファイルが導入されていなければ検知できません。

常に最新の定義ファイルが自動的に更新される設定にしてパソコンを使うことで、早期に「Emotet」など新種のマルウェアを検知することが可能となりますので、設定の確認をしましょう。

今回紹介した「EmoCheck」は、はじめにも御案内しましたとおり、お使いのパソコンがマルウェア「Emotet」に感染している疑いがある場合に、**感染の有無を確認するために公開されたツール**です。

「感染の疑いがあった場合に実施するもの」という作りになっているとはいえ、**一度は操作してみなければ、有事の際に使うことができない**ことは明らかです。

「自分が使っているパソコンが「Emotet」に感染しているわけがない。」という場合でも、動作確認をしていただくことで、使い方を習得できるとともに、その時点における「Emotet」感染の有無も確認することができます。

今回は「v1.0」バージョンでの説明となりましたが、このバージョンだけで確認作業を終えることなく、本資料の元になっている JPCERT/CC の「EmoCheck」関連ページ（https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html）で、**バージョンの更新状況を確認し、「EmoCheck」のバージョンが新しくなるたびに確認**[9]していただき、安心してパソコンをお使いいただきたいと思います。

追記

「⑤Emotet に感染していた場合の応急的対処法」で感染後の対策として「直ちに社内でシステムを担当されている方、または、パソコンの操作に慣れている方に隔離・削除作業を依頼するか、システムのセキュリティに関して契約している会社があれば、相談する」とお伝えしましたが、相談する人や契約会社がない方は、東京都庁内に設置されている「Tcyss（ティーサイス）（東京中小企業サイバーセキュリティ支援ネットワーク）」の「**中小企業サイバーセキュリティ相談窓口**[10]」を活用いただくこともできます。

---

[9] 「EmoCheck」のバージョン更新の状況については、警視庁においてもツイッターでお知らせしていく予定です(警視庁ツイッター https://twitter.com/MPD_cybersec）。

[10] 電話番号：０３－５３２０－４７７３　＜相談料無料＞　ただし、都内の中小企業に限られますので御注意ください。