サイバーセキュリティパートナーシップだより

No.6

令和4年3月28日　山口県警察本部生活環境課

不正プログラム「Emotet」への感染を狙う山口県警をかたった不審メールに注意!!

現在、山口県警の部署名をかたった不審メールの送りつけ事案の発生を確認しています。

今回の不審メールは、本年２月頃から多発している不正プログラム「Emotet（エモテット）」への感染を狙った添付ファイル付きのメールとなります。

下記のようなメールを受信した場合は、添付ファイルを開かないようにしてください。

※　Emotet～情報の窃取や、更に他のウイルスへの感染のために悪用されるウイルスの名称

【確認されている不審メール（２件分）の特徴】

差出人：〇〇課＜●●●●●@×××××××＞
件名：RE:●●●●●●
添付ファイル：2022-03-19_xxxx.zip

差出人名は、山口県警の部署名

件名は返信メールを装う。（Re）が頭に付く。

以下のメールの添付ファイルの解凍パスワード
添付ファイル名　2022-03-19_xxxx.zip
解凍パスワード　xxxxxxxxxx

圧縮ファイル内には、ワードやエクセルファイルが格納。ファイルを開いてマクロを実行してしまうと、不正プログラムに感染

〇〇課
Tel ●●●-●●●-●●●●　Fax ●●●-●●●-●●●●
Moblie　●●●-●●●-●●●●

署名情報には、上記の差出人名と正規アドレス等の記載あり。
※署名情報を信用しないこと！

差出人：〇〇課＜●●●●●@×××××××＞
件名：Fw:テストメールの送信について
添付ファイル：〇〇〇〇〇〇〇.xlsm

差出人名は、山口県警の部署名

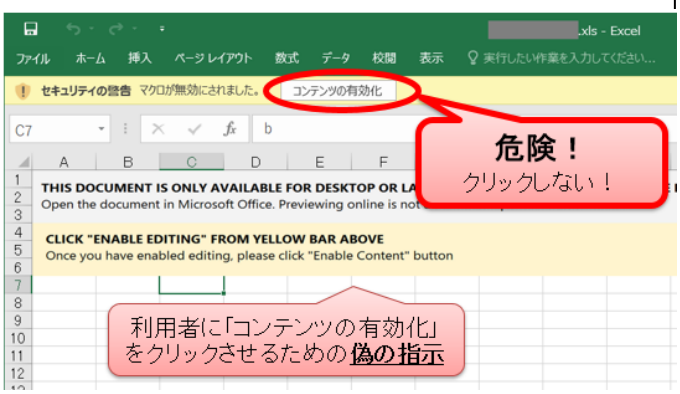
件名はテストメールを装う。（Fw）が頭につく。

テストメールの送信について
ご確認をお願いします。
宜しく御願い致します。

添付ファイルは、zip の圧縮ファイルだけでなくエクセルファイルの場合もある。解凍作業がないだけであり、上記と同様、ファイルを開いてマクロを実行すると不正プログラムに感染

〇〇課
Tel ●●●-●●●-●●●●　Fax ●●●-●●●-●●●●
Moblie　●●●-●●●-●●●●

～Office 製品のファイルを開いた際の画面例～
（右記画像の引用元：IPA 情報処理推進機構）



マクロやセキュリティに関する警告とともに、コンテンツの有効化を促すような注意書きがあるが、不正プログラムに感染させるための偽の表示であるため、クリックしてはいけない。

Emotet の感染被害に遭わないためには

● メールに添付ファイルやリンクの記載がある場合は、十分に注意する。
～ 過去にやり取りしたメールの返信や転送メールを装うため、うっかり添付ファイルを開いてしまうケースが多い。
また、添付ファイル型の手口の他、リンクにアクセスさせ、不正プログラムをダウンロードさせる手口もある。

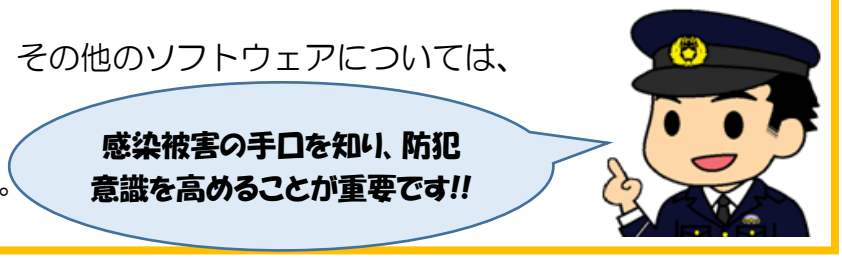
● 本物のメールか判断がつかない場合は、ファイルを開く前（マクロを実行する前）に、電話などの確実な手段でメールの差出人に問い合わせる。

● Office 製品（ワードやエクセル）で「コンテンツの有効化」や「編集を有効にする」を画面上で指示されている場合、信頼できるファイルと判断できなければクリックしない。

● セキュリティ対策ソフトを導入し、定期的なウイルスチェックや更新を行う。また、不要データの削除を定期的に行う。

● OS、セキュリティ対策ソフト、その他のソフトウェアについては、常に最新の状態に更新する。

● 組織内への注意喚起を徹底する。



～Emotet に感染しているか確認する方法の一例～

一般社団法人 JPCERT/CC から無料で公開されている
Emotet 感染有無確認ツール「EmoCheck」（エモチェック）
（https://github.com/JPCERTCC/EmoCheck/releases）
を利用する。

注１）使用する場合は、Emotet 感染に繋がる可能性が考えられるメールを開いた PC のアカウントで端末にログインした状態でツールを実行すること

注２）２０２２年３月１４日付けで、EmoCheck の最新バージョン v2.1 を公開

【使い方】
JPCERT/CC 解説動画～Emotet 感染の確認方法と対策
https://www.youtube.com/watch?v=nqxikr1x2ag

【感染していた場合の対応】
JPCERT/CC～マルウェア Emotet への対応 FAQ
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

【その他関連サイト】
○ JPCERT/CC 解説動画～日本中で感染が広がるマルウェア Emotet
https://www.youtube.com/watch?v=wvu9sWiB2_U
○ 情報処理推進機構（IPA）～Emotet の攻撃活動の急増
https://www.ipa.go.jp/security/announce/20191202.html#L18
○ 警察庁（@police）～Emotet の解析結果について
https://www.npa.go.jp/cyberpolice/important/2020/202012111.html

山口県警察サイバー犯罪相談窓口
TEL ０８３－９２２－８９８３
mail cyber.soudan@police.pref.yamaguchi.lg.jp