滋賀県警からのサイバーセキュリティに関するお知らせ

「新型コロナウイルス」に便乗した偽メールに要注意
マルウェア「Emotet」に感染させる手口が発生

新型コロナウイルスの感染拡大に便乗し、実在する保健所を装ってマルウェア「Emotet（エモテット）」を送り付けるメールが全国的に発生しています。

Emotet に感染するとメールアドレスやメール本文の情報が窃取されるほか、実在する組織や人物になりすましたメールの送信元にされます。

「新型コロナウイルス感染拡大に関するメール」には十分注意してください。

新型コロナウイルス感染拡大に便乗した偽メールの例

差出人　　：■■■■保健所福祉室 <■■■■■■@■■■■.jp>
件　名　　：通知2020Jan29
添付ファイル：instruction Jan 2020.doc

お世話になっております。

新型コロナウイルス肺炎関連については、・・・・・・・・・・・・・感染が報告され、
国内でも■■県で患者が報告されているところであり、

つきましては、別添通知をご確認いただき、
感染予防対策についてよろしくお願いします。
なお、・・・・・・・・・・・・・準備をしております

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊
■■■■保健所福祉室（担当：■■）
〒■■■■■■■■■■■■■■■■
電話：■■■-■■■-■■■■
＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊　（※メール内容は一部編集しています。）

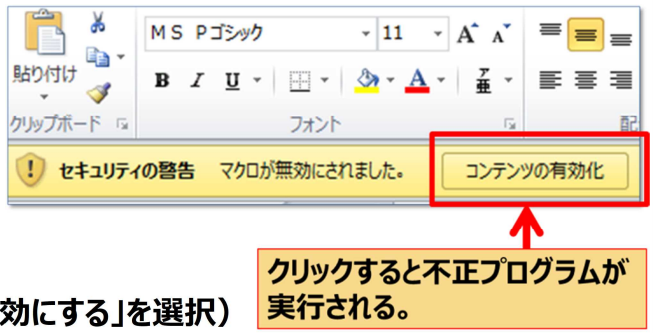
参照：IPA「Emotet」と呼ばれるウイルスへの感染を狙うメールについて
https://www.ipa.go.jp/security/announce/20191202.html

←標的型メール攻撃は、実在する組織名やメールアドレスが使われるなど、かなり巧妙化しており、不審点を見抜くことが困難になっています。（※メール内容は一部編集しています。）

Emotet 感染予防対策

Emotet は、主にメールに添付された Word 形式のファイルを開き、コンテンツの有効化を実行することで感染するので、コンテンツを有効化する場合は、注意してください。

Word マクロ設定を「自動実行の無効化」にしておきましょう。
（マクロの設定で「警告を表示してすべてのマクロを無効にする」を選択）



JPCERT コーディネーションセンター（JPCERT/CC）では、Emotet 感染有無を確認するツール情報を公開しています。無料で利用できますので、詳しくは、下記 JPCERT/CC のウェブサイトをご覧ください。

参照：JPCERT/CC Eyes「マルウェア Emotet への対応 FAQ」
https://blogs.jpcert.or.jp/ja/2019/12/emtetfaq.html

[お知らせ] 毎年 2 月 1 日から 3 月 18 日まではサイバーセキュリティ月間です。

滋賀県警察本部サイバー犯罪対策課　（代表）077-522-1231