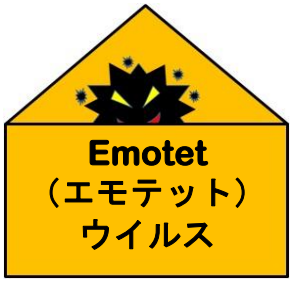
それウイルスメールかも！

Emotet（エモテット）の感染が急拡大しています



メールに添付されたファイルを開封したり、メール本文中のリンク先に接続することで「Ｅｍｏｔｅｔ（エモテット）」と呼ばれるウイルスに感染します。

エモテットに感染すると

- 感染した端末のメールアカウント、パスワード、メール本文などが盗まれる
- 取引先関係者などを装って、感染を広げる攻撃メールを送信する
- 別の不正プログラムに感染しやすくする

などの被害が発生するおそれがあります。

被害を防止するために、次のことに注意してください。

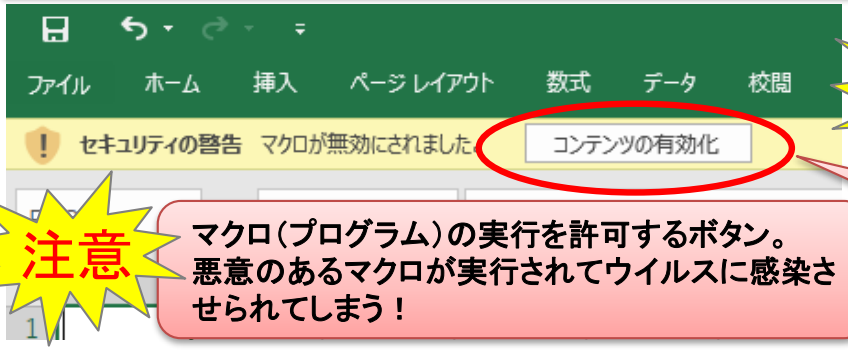
被害防止対策

送信者が知人や取引相手の名前でも、以下の点に注意し、不用意に添付ファイルを開封したり、本文中のリンク先にアクセスしない

本文に不自然なところはありませんか？
本当に知人や取引相手からの必要な内容が記載されたメールなのか、しっかり確認しましょう。

★ウイルスメールでよく使用される文面
「取り急ぎご連絡いたします。添付ファイル（リンク先）をご確認ください。」

添付ファイルやリンク先からファイルを開いてしまい、警告画面が表示されても、「コンテンツの有効化」などのボタンをクリックしない



危険

クリックしないで！！

注意

マクロ（プログラム）の実行を許可するボタン。
悪意のあるマクロが実行されてウイルスに感染させられてしまう！

OSやウイルス対策ソフトは常に最新の状態にする

古いとセキュリティが弱くなって、サイバー攻撃の被害に遭うリスクが高くなるよ。

もし感染が疑われる場合は・・・

- 感染したパソコンのネットワークをインターネットから遮断する
- ウイルス対策ソフトでウイルスチェックを行う
- 関係者に連絡し、メールを開封しないように注意喚起する
- 最寄りの警察署に相談する

熊本県警察本部サイバー犯罪対策課