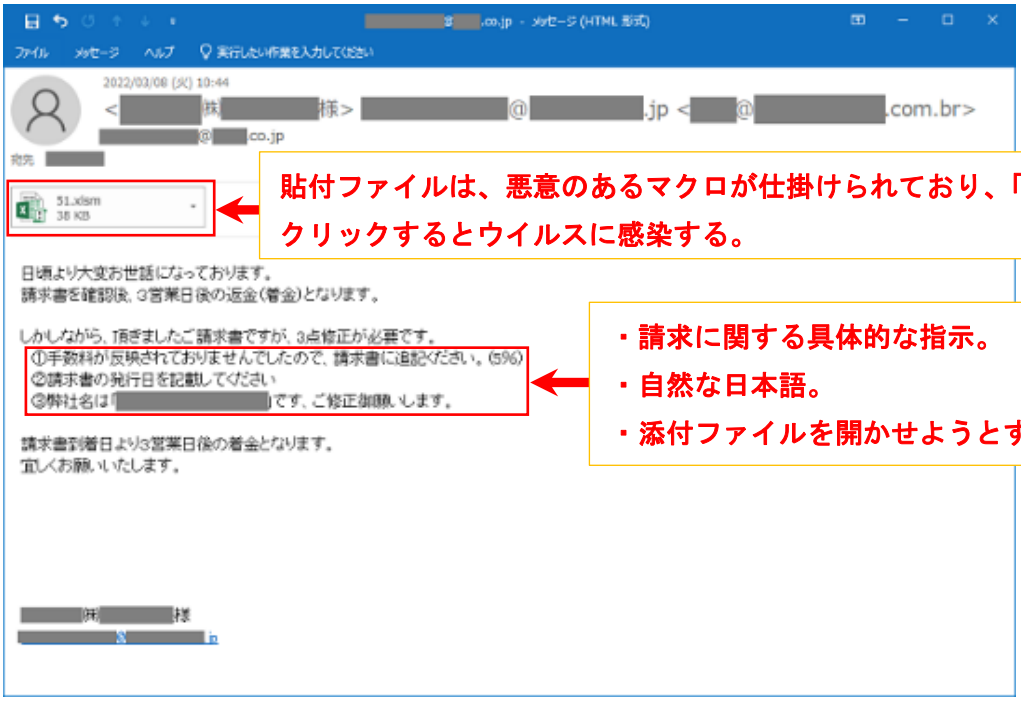
# Emotet（エモテット）への感染に注意！！

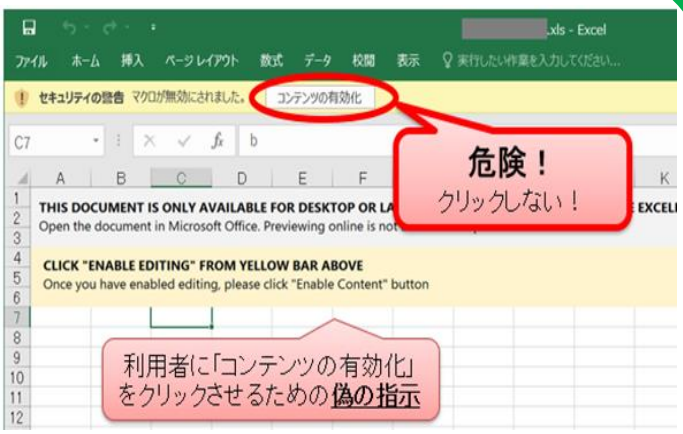
全国的にコンピュータウイルス Emotet（エモテット）への感染が拡大しています。
Emotet が添付された攻撃メールの特徴は、過去にやり取りをしたことのある、実在の相手の氏名、メールアドレス、メール内容等の一部が流用されて、「正規メールへの返信を装う内容」や、「業務上開封してしまいそうな巧妙な文面」となっています。

## 攻撃メールの例




## 対策

- メールに添付されたファイルは、送信元にかかわらず警戒し、不審に思ったら差出人に確認する。
- OS やアプリケーション、セキュリティソフトを常に最新の状態にする。
- メールに添付された Word や Excel ファイルを開いたときに、マクロやセキュリティに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない。




- メールや文書ファイルの閲覧中に警告ウィンドウが表示された際、その警告の意味が分からない場合は、操作を中断する。
- 不審な添付ファイルを開いてしまった場合は、すぐにシステム管理担当者などへ連絡する。

【出典】IPA 独立行政法人情報処理推進機構（「Emotet（エモテット）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

岩手県警察本部サイバー犯罪対策課の公式Twitterは QR コードから！！
サイバー空間を悪用した犯罪の手口やサイバー犯罪の被害に遭わないための情報をお知らせしています。

**岩手県警察本部生活安全部サイバー犯罪対策課**
**令和4年3月 28 日発行**

@Iwate_cyber