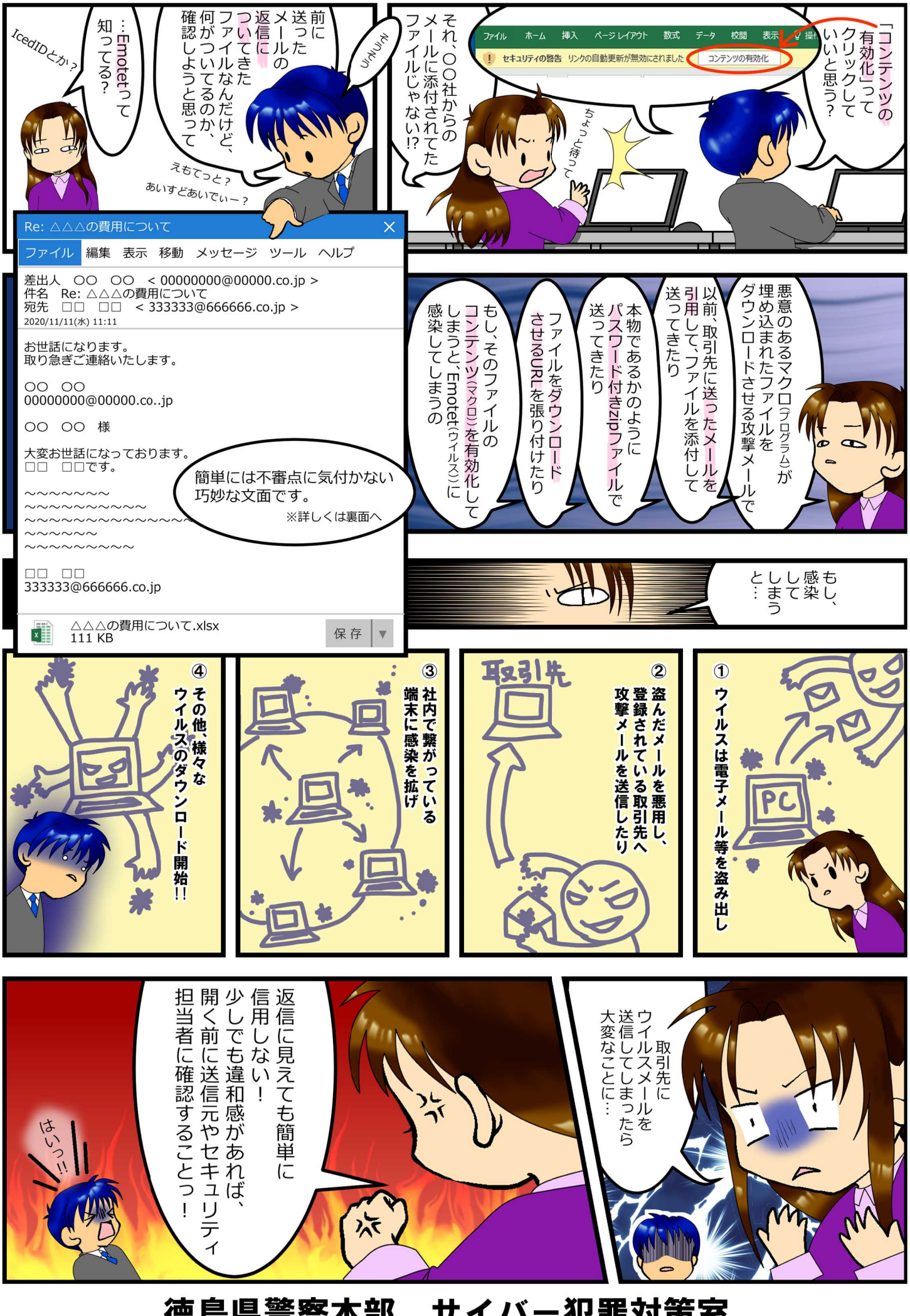
そのメール、本当に開いて大丈夫？



徳島県警察本部　サイバー犯罪対策室

返信を装って不正な添付ファイル等を開かせようとするメールについて

「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙ったメールが、国内の様々な組織に着信しています。特に、過去にメールをやり取りしたことがある相手からの返信を装うなど、一見して不審を認めにくい巧妙なメールが増えており、注意が必要です。

○平素から必要な対策
- 組織内へ注意喚起を実施する。
- Ｗｏｒｄ等のマクロを無効にしておく。
- メールセキュリティ製品を導入して不正な添付ファイルを検知する。
- 基本ソフトを最新の状態に保つ。
- 定期的にバックアップをとって安全な場所に保管する。

○メールを扱う際に必要な対策
- 添付ファイルのマクロは必要性を確認できるまで有効化しない。
- 安全を確認できないリンクやＵＲＬは開かない。

○組織内での感染を示唆する兆候
- ウイルス対策ソフトがEmotetの感染を発見した。
- 自組織のメールアドレスをかたって、Word形式のファイルを添付したメールが届いたと外部組織から連絡を受けた。
- 自組織のメールサーバから、Word形式のファイルを添付したメールや、なりすましメールが大量に送信されていることが判明した。

○感染が確認された時の初期対応
- 感染した端末をネットワークから隔離する。
- 感染した端末で利用していたメールアカウントのパスワードを変更する。

詳しくは以下のページ等を参照してください。

独立行政法人情報処理推進機構
「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

一般社団法人JPCERTコーティネーションセンター
マルウエアEmotetの感染に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190044.html

徳島県警察本部
徳島県徳島市万代町２丁目５番地１　電話 088-622-3101