CyberNews
佐賀県警察本部サイバー犯罪対策課

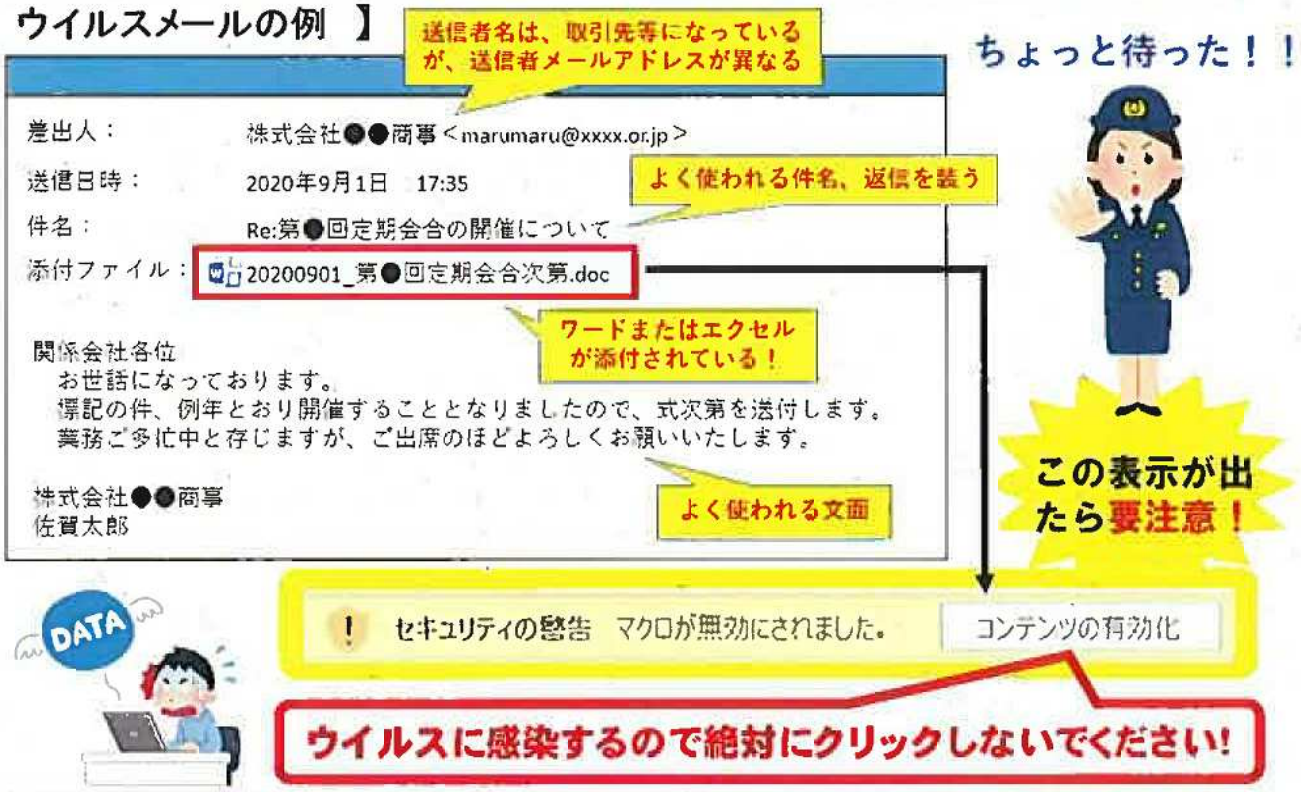
広報用資料
令和３年第１７号
サイバー犯罪対策課

ウイルスメール「エモテット」に注意！

「Ｅｍｏｔｅｔ（エモテット）」と呼ばれるコンピュータウイルスを使ったメール攻撃が再び発生しています。

感染すると、パソコンを乗っ取られるだけでなく、メール情報が流出して、関係先にウイルスメールがばらまかれてしまいます。

【 ウイルスメールの例 】



ウイルスに感染するので絶対にクリックしないでください!

～　被害に遭わないために気をつけること　～

・ウイルス対策ソフトを導入し、最新の状態に更新して使用する！

・返信メールに見えても安易に添付ファイルやＵＲＬをクリックしない！

・添付ファイルの「コンテンツの有効化」をクリックしない！

参考：独立行政法人情報処理推進機構（ＩＰＡ）
エモテットと呼ばれるウイルス　右のＱＲコードをご確認ください。

CyberNews
サイバー犯罪対策課

広報用資料
令和３年第１３号
サイバー犯罪対策課

サポート詐欺に騙されないで！！

サポート詐欺とは「パソコンがウイルスに感染している」など偽の警告画面を表示させてユーザーの不安をあおり、画面に表示された電話番号に電話をかけさせ、パソコンを遠隔操作するソフトをインストールするように促し、有償のサービス契約に誘導する詐欺の手口です。

～ 被害に遭わないために気をつけること ～

- 警告画面や警告音が出ても慌てず、電源を切る
- サポート窓口に電話をしない
- 電子マネーの支払いやクレジットカード情報の入力には応じない
- ソフトをインストールしてしまった場合には、アンインストール、システムの復元を検討する（メーカーへ相談をする）

参考：一般社団法人日本サイバー犯罪対策センター（ＪＣ３）
サポート詐欺の手口（動画解説）右のＱＲコードをご確認ください

CyberNews サイバー犯罪対策課

広報用資料
令和３年第１２号
サイバー犯罪対策課

料金確認の偽メールに注意！

【 偽メールの例 】

< 050-XXXX-XXXX

SMS/MMS
10月1日(月)12:30

〇〇〇お客様センターです。
ご利用料金のお支払い確認
が取れておりません。
ご確認が必要です。

偽サイト

https://〇〇〇.net/index.html

携帯電話会社を装ってメールを送り、偽サイトに誘導してＩＤ・パスワード等の情報をを入力させてだまし取る手口です。

情報を入力してしまうと、利用しているサイト、サービスに不正ログインされ、ネットで高額な買い物をされるなどの被害につながります。

被害に遭わないための対策

・メール添付のＵＲＬをクリックしない
・ウイルス対策ソフトを導入する
・サービスごとのパスワードと多要素認証を設定する

偽メール、偽サイトは、実在の企業名とロゴを使っており、見分けるのは困難です。全ての受信メールに注意を払い、安易にＵＲＬに接続しないようにしましょう！

参考 ： 日本サイバー犯罪対策センター （ＪＣ３）
最新の脅威具体例 <https://www.jc3.or.jp/threats/>