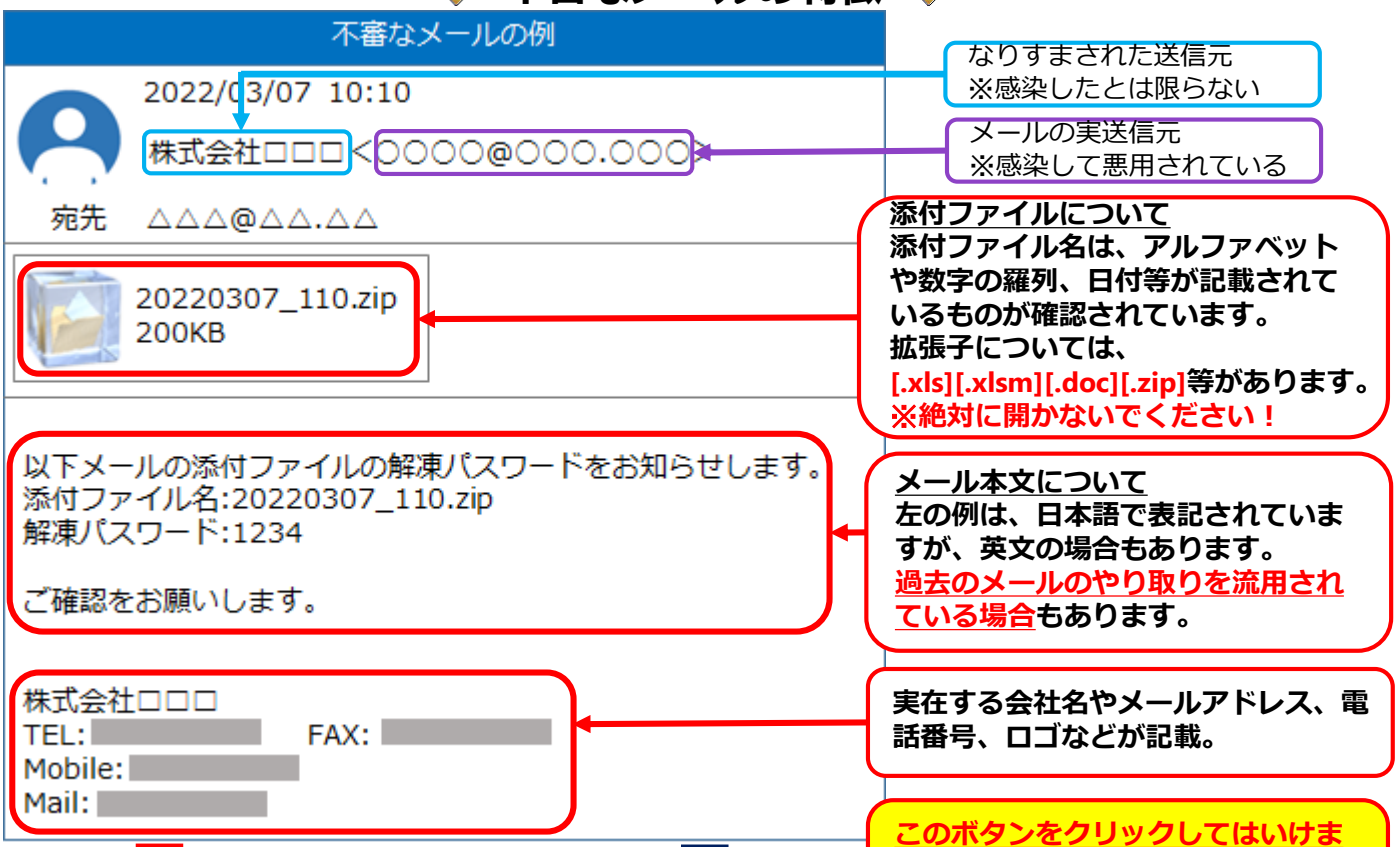
Emotet感染拡大中！
取引先からのメールの添付ファイルに要注意

Emotet（エモテット）は、主にメールに**添付された文書ファイルや圧縮ファイルを開くことで感染**する不正プログラムです。過去にやり取りしたメールへの**返信を装ったメール**を送信し、添付ファイルの開封を求めてきます。
感染すると、メールアカウント、パスワード、メール本文等の情報を窃取し、これらの情報を悪用して、**取引先等に感染を拡散**させたり、ランサムウェア等、**他のマルウェアに感染する恐れ**があります。

不審なメールの特徴



なりすまされた送信元
※感染したとは限らない

メールの実送信元
※感染して悪用されている

添付ファイルについて
添付ファイル名は、アルファベットや数字の羅列、日付等が記載されているものが確認されています。
拡張子については、[.xls][.xlsm][.doc][.zip]等があります。
※絶対に開かないでください！

メール本文について
左の例は、日本語で表記されていますが、英文の場合もあります。
過去のメールのやり取りを流用されている場合もあります。

実在する会社名やメールアドレス、電話番号、ロゴなどが記載。

ファイルを開いてしまった場合

「マクロの自動実行」が有効

「マクロの自動実行」が無効

このボタンをクリックしてはいけません！ファイルのマクロが動作してウイルスに感染してしまいます

感染が確認された場合、被害拡大防止の観点より次の初期対応をお願いします。

- 感染した端末の**ネットワークからの隔離**
- 感染した端末が利用していた**メールアカウントのパスワード変更**
- 感染端末が接続していた組織内ネットワークの**ウイルス対策ソフトによるフルスキャン**
- 感染した端末が利用していた**アカウントのパスワード変更**
- ネットワークトラフィックログの監視
- 被害を受ける（攻撃者に窃取されたメールアドレス）可能性のある関係者への**注意喚起**
- 調査後の**感染した端末の初期化**

警察への通報もお願いします！

参考：一般社団法人JPCERT/CC「マルウェアEmotetへの対応FAQ」https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html）

埼玉県警察本部サイバー対策課