JPCERT Coordination Center

JPCERT CC®

日本中で感染が広がるマルウェアEmotet

2022年3月

一般社団法人JPCERTコーディネーションセンター

Emotetとは

1-1.マルウェア Emotet（エモテット）概要

- マルウェアとは
  - コンピュータに悪影響を与えるソフトウェア
  - いわゆるコンピューターウイルス

- Emotetの特徴
  - 知り合いになりすましたメールが送られてくる
    - 過去のメール本文が引用されることもある
  - 感染していないのに送信元名に悪用される

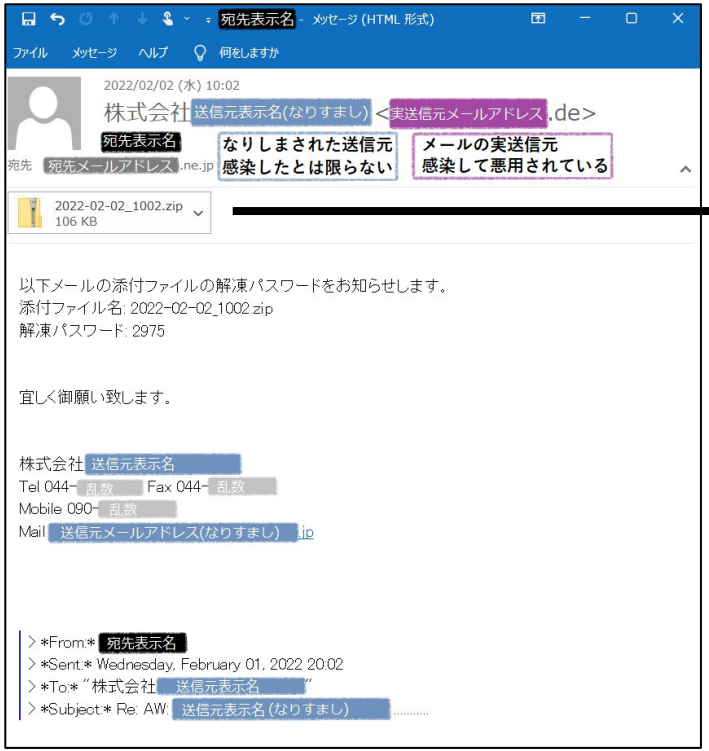
1-1.マルウェア Emotet（エモテット）概要

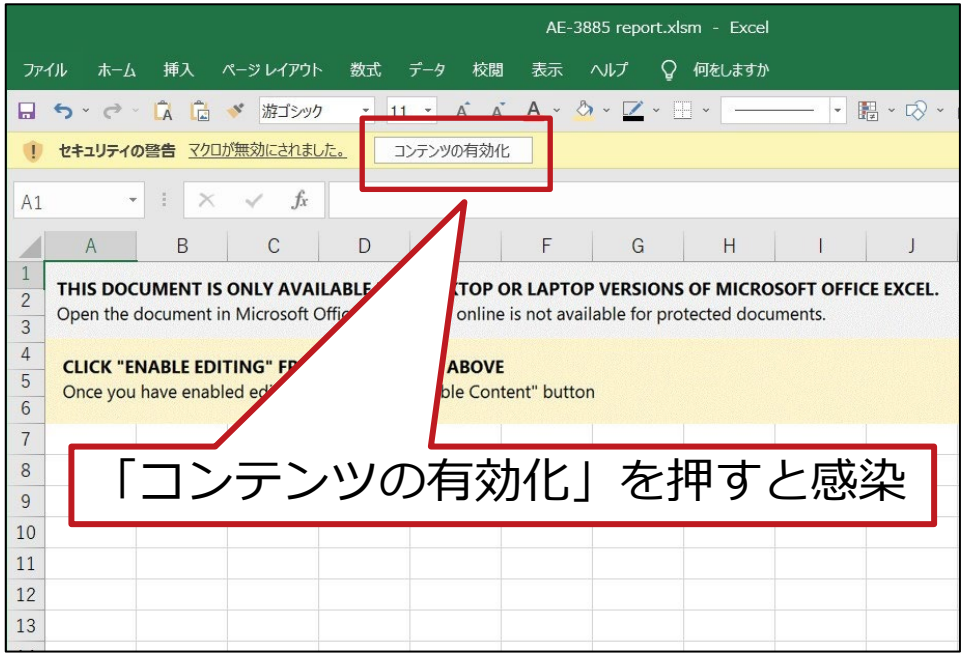
- Emotetの機能
  - メール関連情報を窃取
    - メールアカウント情報、メール本文、アドレス帳…
  - 感染を広げるメールを送信
  - 他のマルウェアに感染

- 感染により発生する被害
  - メール窃取による機微な情報の漏洩
  - 認証情報の漏洩
  - メールサーバが踏み台として悪用される
  - メール送受信者（取引先など）からの問い合わせ

1-2.Emotetに感染するまでの流れ

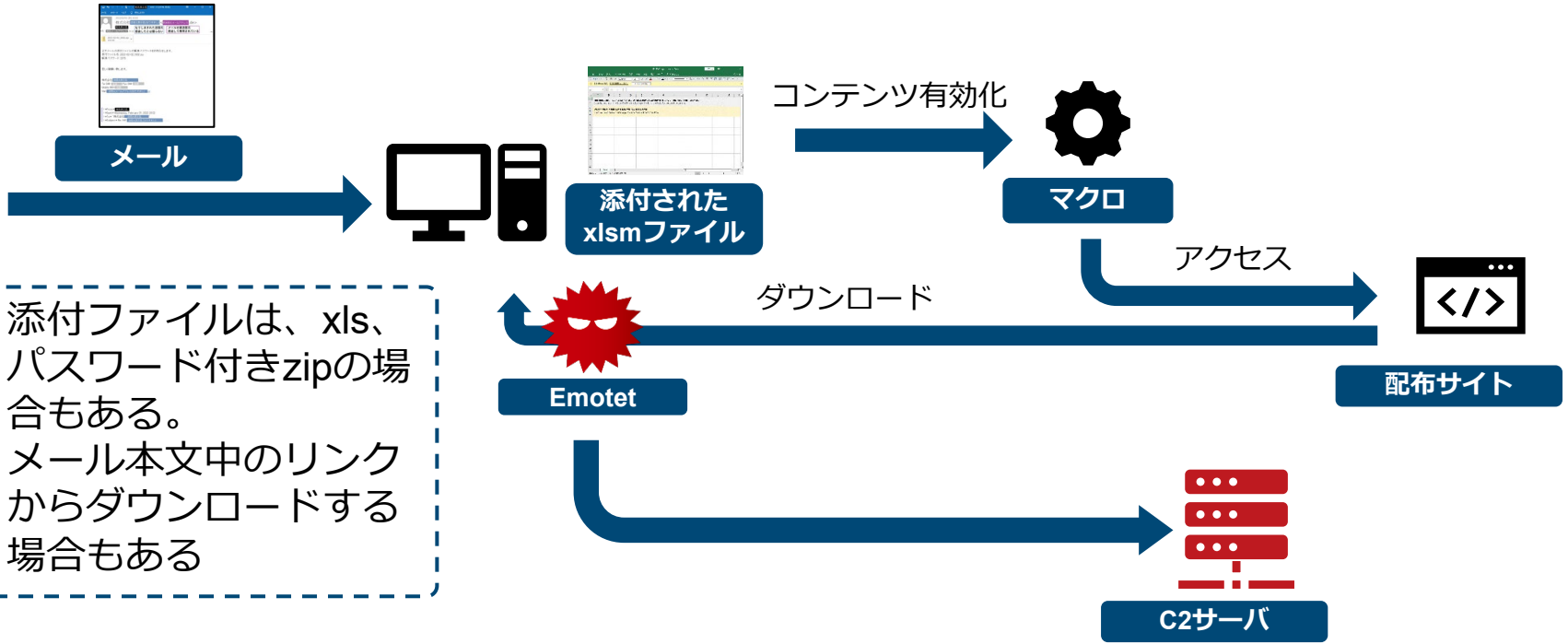
■Emotetはメールの添付ファイルから感染





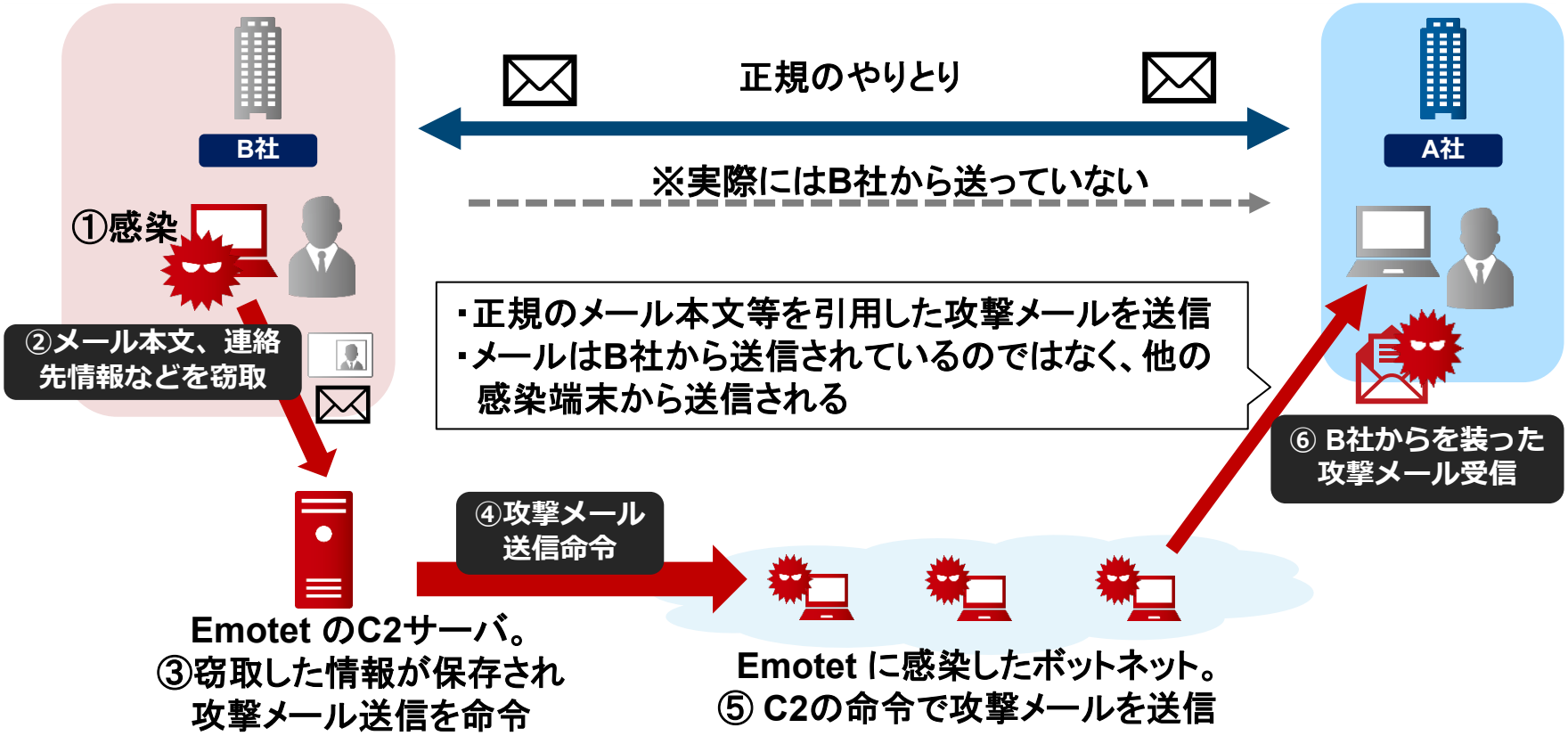
1-2.Emotetに感染するまでの流れ

- メールに添付されたxlsmを開きマクロが実行されると、インターネット経由でEmotetをダウンロードし感染



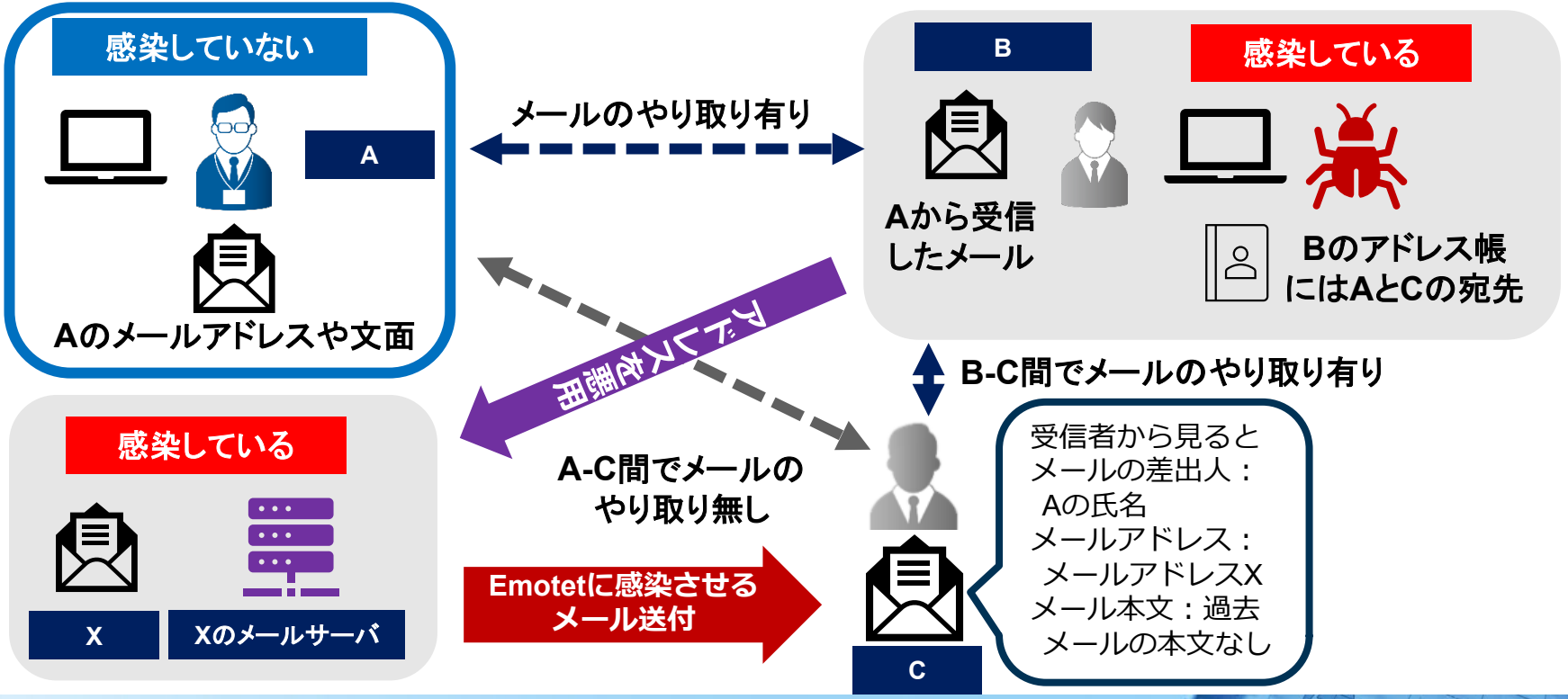
添付ファイルは、xls、パスワード付きzipの場合もある。
メール本文中のリンクからダウンロードする場合もある

1-3.Emotet感染によるなりすましメール送信



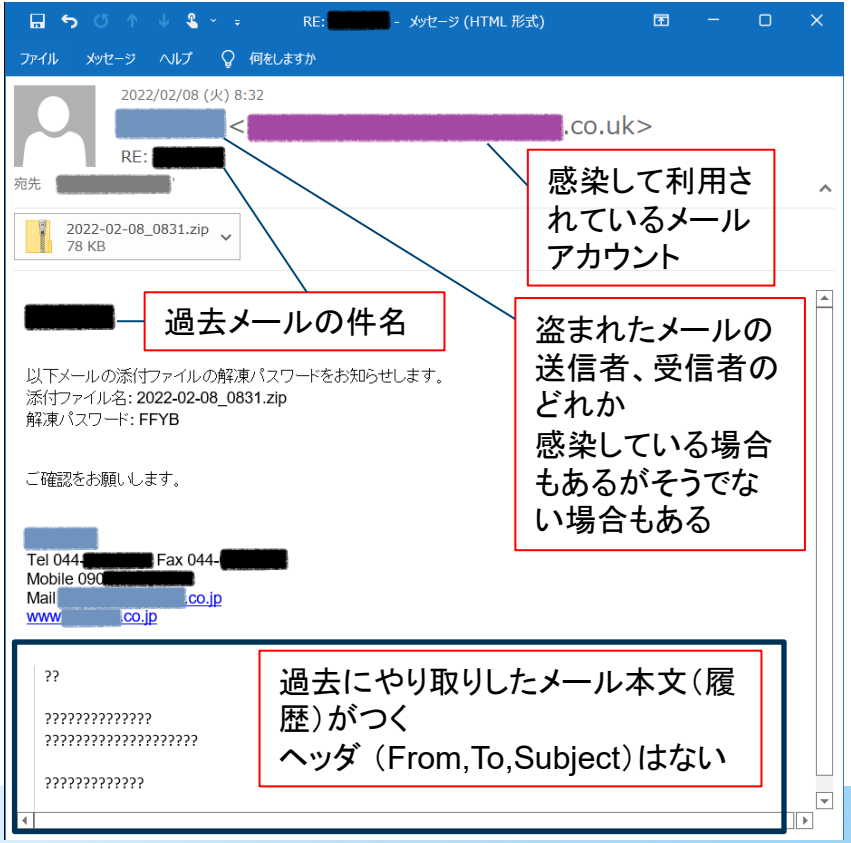
1-3.Emotet感染によるなりすましメール送信

■送信元がなりすまされているケース

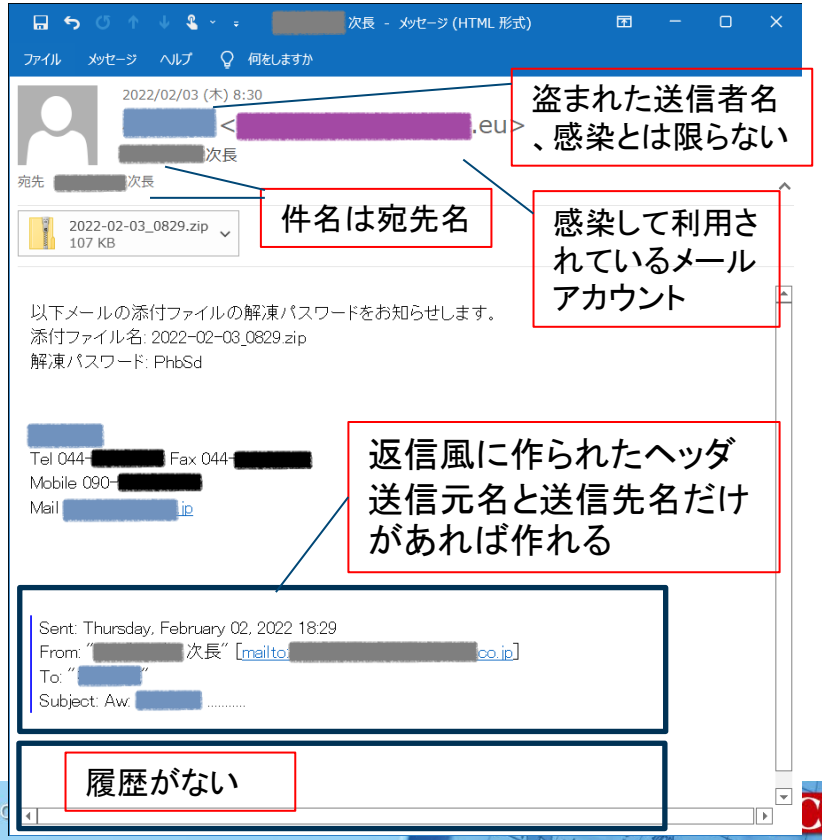


1-3.Emotet感染によるなりすましメール送信

感染した場合に送られるメール



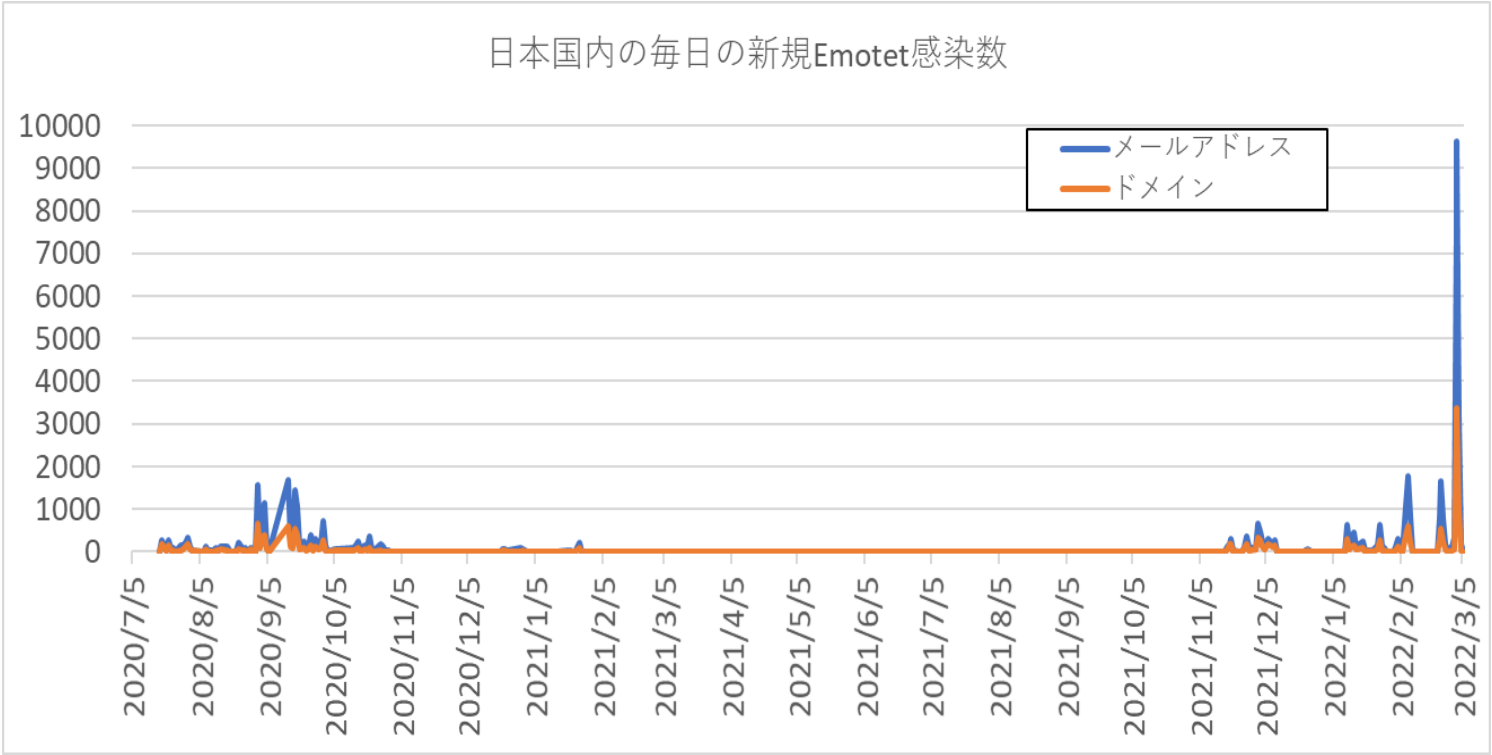
感染してなくても送られるメール



国内の被害状況

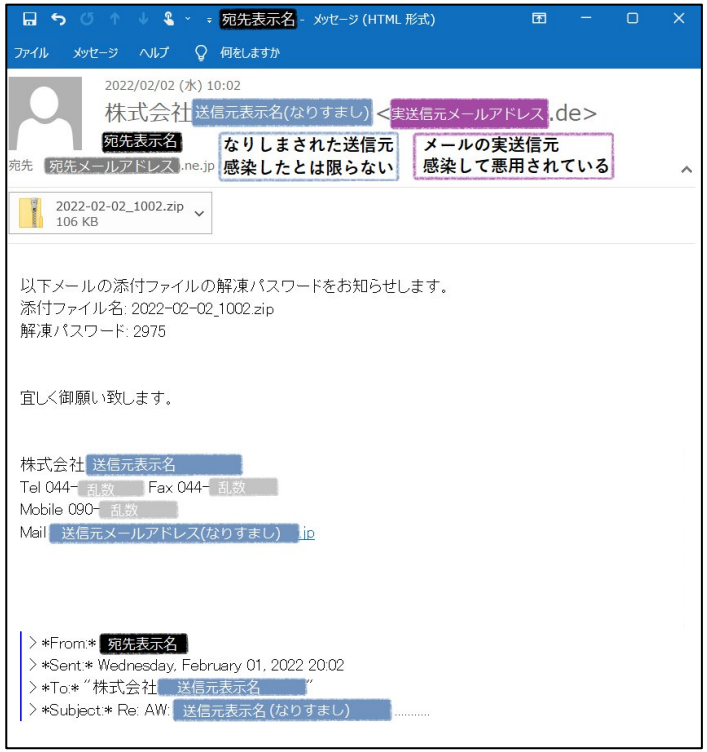
2-1. Emotetの国内感染状況

■2月から日本国内で感染が急増、3月に爆発



2-2. 感染が広がった要因

- 以下のメール文面が出てから感染が急増



お問合せ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form.html