

# 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

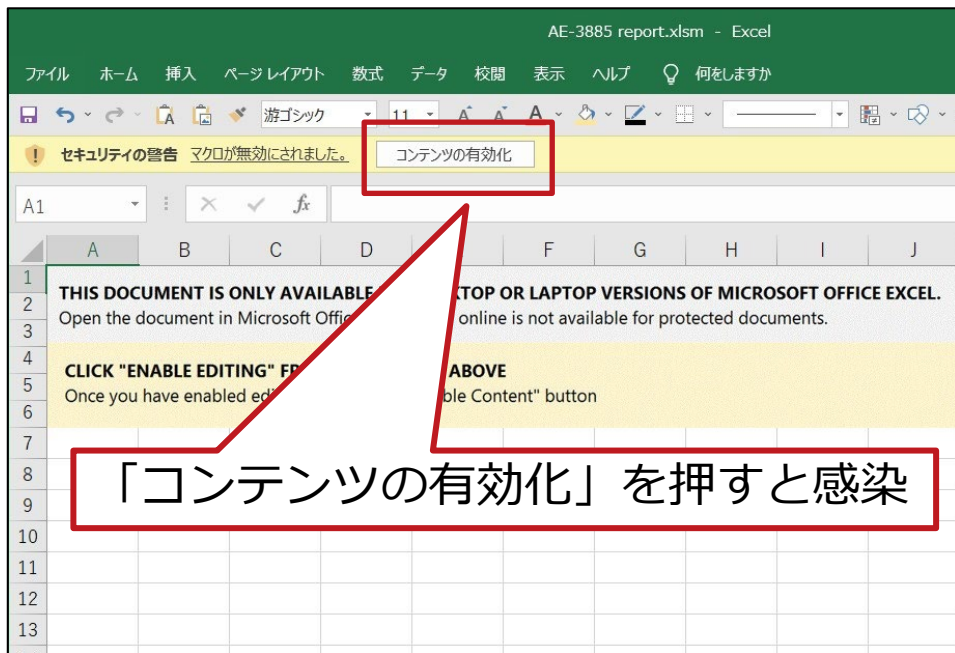
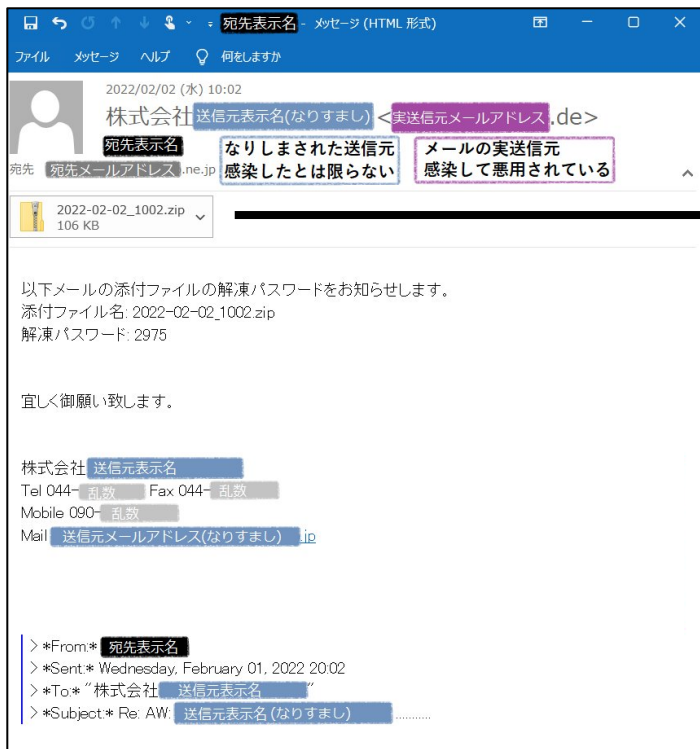
- メール関連情報を窃取
  - メールアカウント情報、メール本文、アドレス帳…
- 感染を広げるメールを送信
- 他のマルウェアに感染

## ■ 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

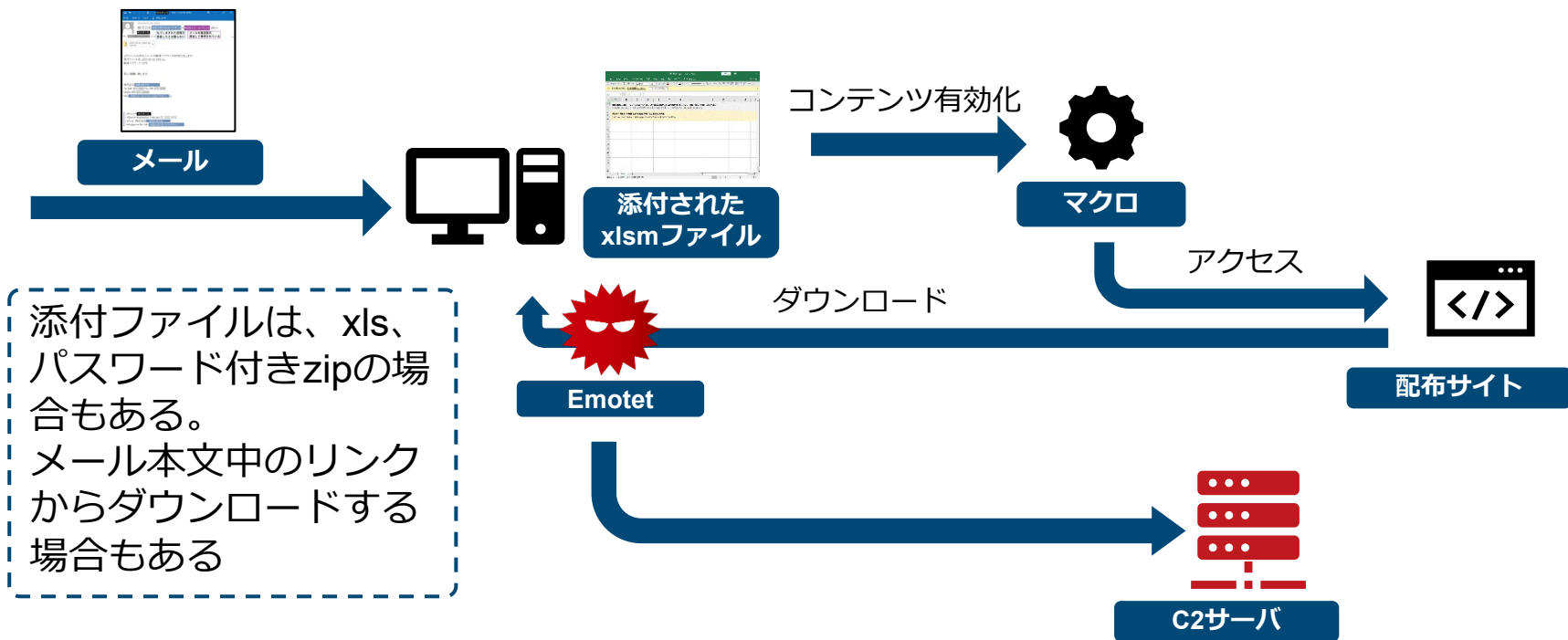
# 1-2.Emotetに感染するまでの流れ

## ■ Emotetはメールの添付ファイルから感染

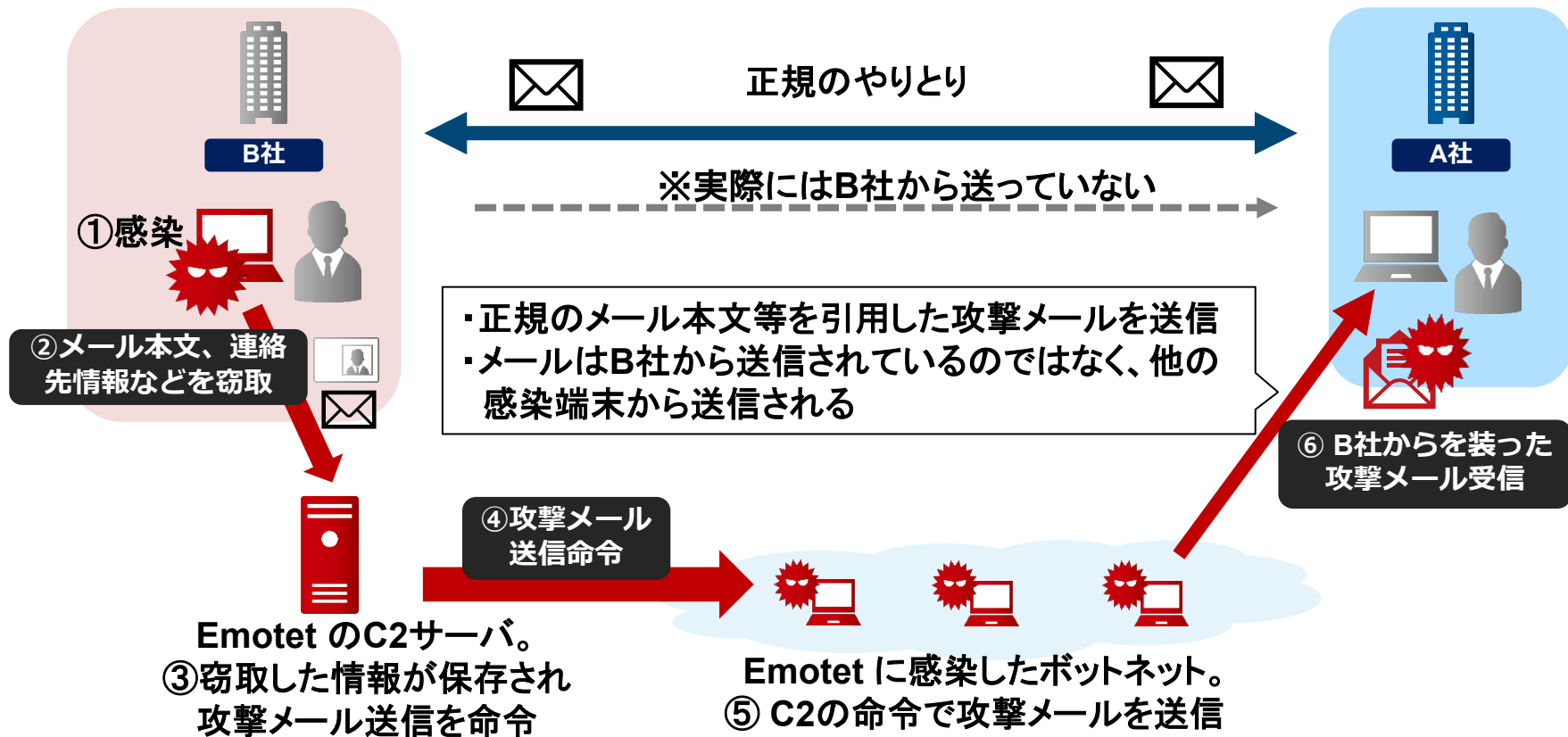


# 1-2.Emotetに感染するまでの流れ

- 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

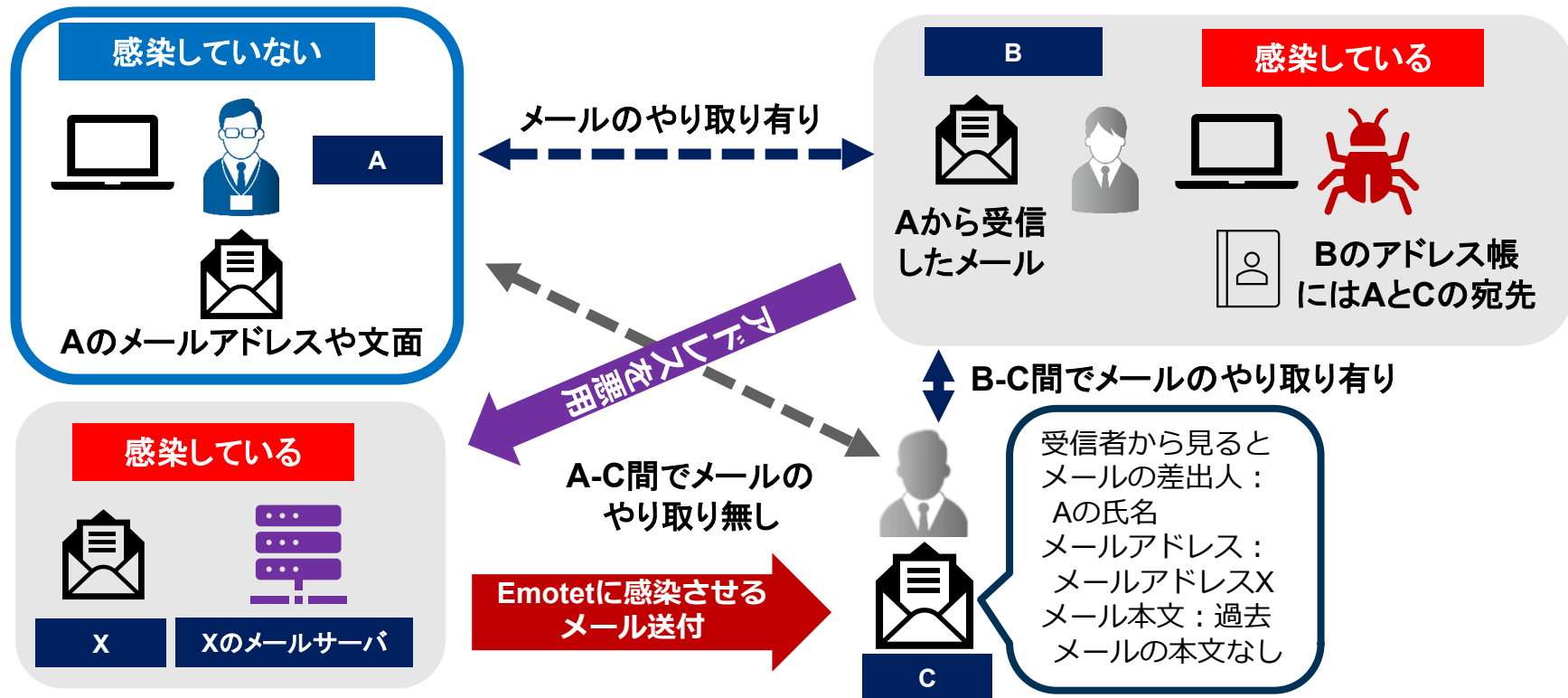


# 1-3. Emotet感染によるなりすましメール送信



# 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

2022/02/08 (火) 8:32  
[Redacted] <[Redacted].co.uk>  
宛先 [Redacted]  
2022-02-08\_0831.zip  
78 KB  
[Redacted] 過去メールの件名  
以下メールの添付ファイルの解凍パスワードをお知らせします。  
添付ファイル名: 2022-02-08\_0831.zip  
解凍パスワード: FFYB  
ご確認をお願いします。  
Tel 044-[Redacted] Fax 044-[Redacted]  
Mobile 090-[Redacted]  
Mail [Redacted].co.jp  
www [Redacted].co.jp  
??  
????????????  
????????????????  
????????????

感染して利用されているメールアカウント  
盗まれたメールの送信者、受信者のどちらか  
感染している場合もあるがそうでない場合もある  
過去にやり取りしたメール本文(履歴)がつく  
ヘッダ (From,To,Subject)はない

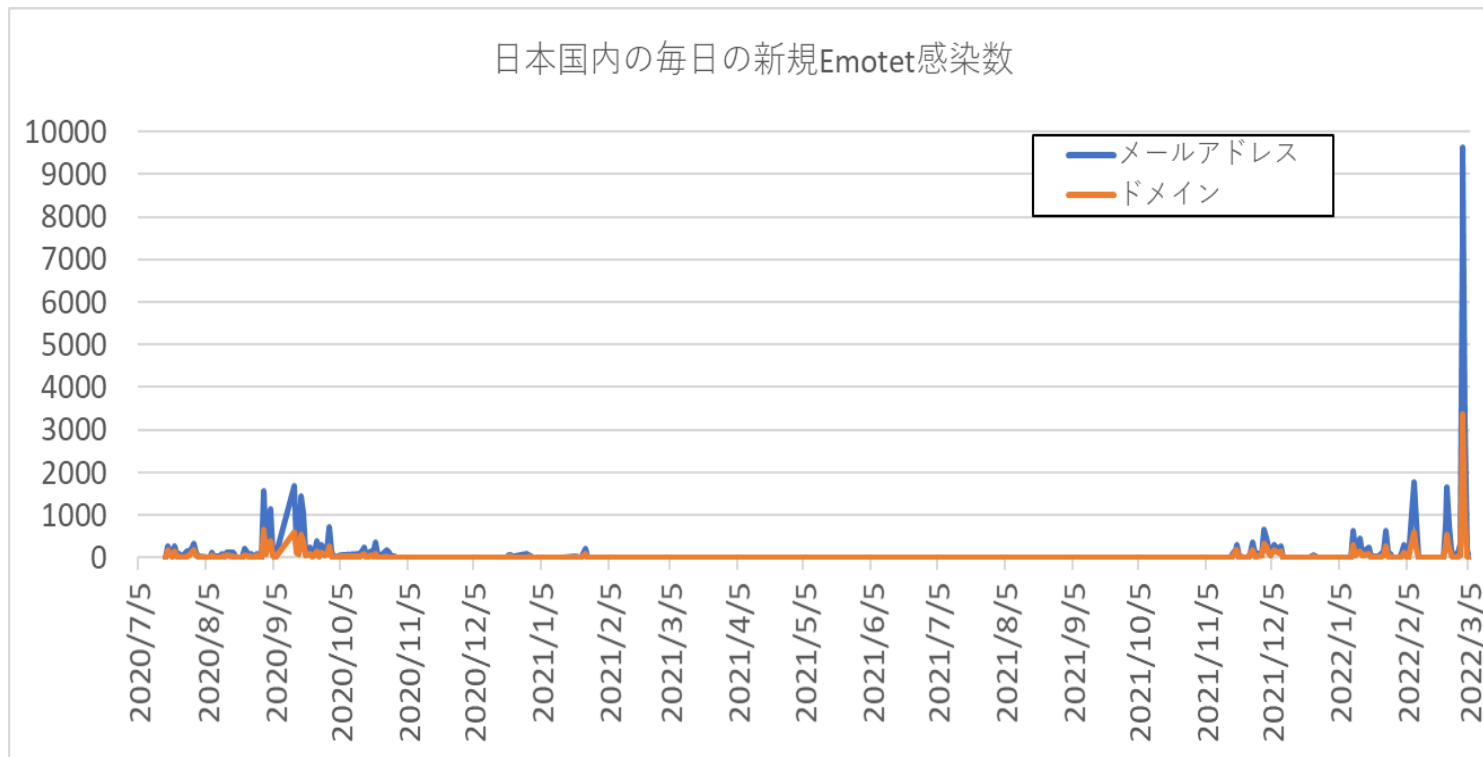
## 感染してなくても送られるメール

2022/02/03 (木) 8:30  
[Redacted] <[Redacted].eu>  
宛先 [Redacted] 次長  
2022-02-03\_0829.zip  
107 KB  
件名は宛先名  
盗まれた送信者名、感染とは限らない  
感染して利用されているメールアカウント  
以下メールの添付ファイルの解凍パスワードをお知らせします。  
添付ファイル名: 2022-02-03\_0829.zip  
解凍パスワード: PhbSd  
[Redacted]  
Tel 044-[Redacted] Fax 044-[Redacted]  
Mobile 090-[Redacted]  
Mail [Redacted].jp  
返信風に作られたヘッダ  
送信元名と送信先名だけが  
あれば作れる  
Sent: Thursday, February 02, 2022 18:29  
From: "[Redacted] 次長" [mailto:[Redacted].co.jp]  
To: "[Redacted]"  
Subject: Aw: [Redacted] .....  
履歴がない

# 国内の被害状況

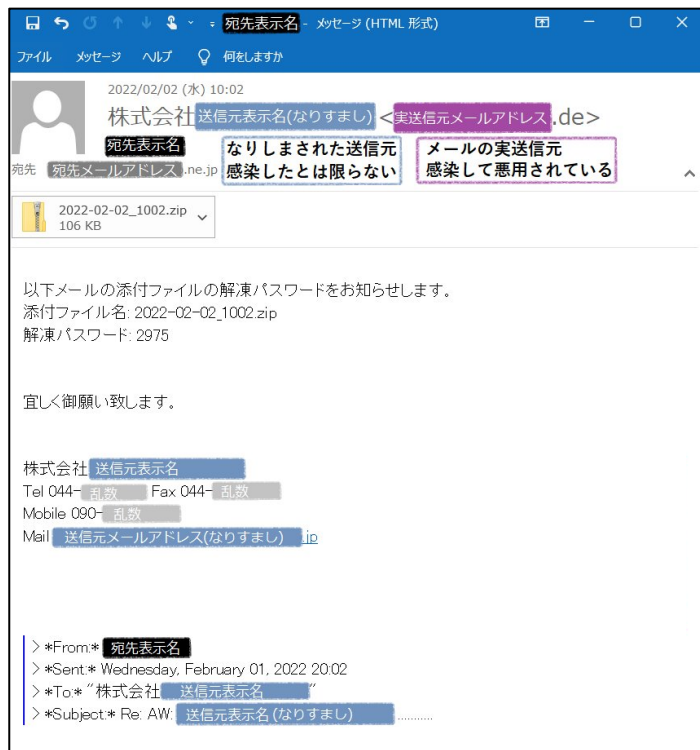
## 2-1. Emotetの国内感染状況

■ 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](mailto:pr@jpcert.or.jp)
- <https://www.jpcert.or.jp/>

## インシデント報告

- Email : [info@jpcert.or.jp](mailto: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](mailto:icsr-ir@jpcert.or.jp)
- <https://www.jpcert.or.jp/ics/ics-form.html>

