



## 官公庁になりすました偽メールに注意！

本年3月以降、Emotetに感染させるメールが増加しています。

メールのなかには、送信元情報を偽装したものもあり、官公庁の担当者を名乗った偽メールも送信されています。

なお、長崎県警担当者になりすました偽メールも確認されています。

官公庁を名乗るメールに十分に注意をし、添付されたファイルを不用意に開かないようにしてください。

### 1 Emotetとは？

- 感染したパソコンからメールアドレスやログイン情報などを盗み出すマルウェアです。
- メール添付ファイルから感染させる手法が主流です。
- Emotetに感染後、さらにランサムウェアに感染する事例もあります。ランサムウェアに感染した端末は、データが暗号化されてしまいます。

### 2 Emotetの感染経路と特徴

- 現在主流となっている感染経路は以下のとおりです。
  - ①パスワード付ZIPファイルが添付されているメールを受信
  - ②ZIPファイルを展開するとExcelファイルなどのOfficeファイルが保存されている
  - ③Officeファイルを開き、「マクロを有効化する」とEmotetに感染する
- 返信メールを装った件名、文字化けした引用文などの特徴があります。

### 3 Emotetによる悪影響は？

- Emotetに感染することで、自組織になりすました偽メールが配信される
- さらに、自組織の端末に記録しているメーリングリストをもとに、関係者になりすました偽メールが配信される

※自組織の端末が感染していなくても、関係者からメール情報等が流出することで、なりすまされることがあります。

### 【 注 意 事 項 】

- 従業員に対し、添付ファイル付きのメールには特に注意するよう、繰り返し注意喚起をお願いします。
- 関係者からのメールであっても、不用意にファイルを開き、マクロを有効化しないで下さい。
- 感染が判明した際は、端末をネットワークから切り離して下さい。
- 自組織がなりすまされてしまった場合に対する備えも必要です。関係者への注意喚起のほか、広報についても日頃から検討しておく必要があります。

長崎県警察本部サイバー犯罪対策課  
095-820-0110 (3451・3452)  
メールで e103107@police.pref.nagasaki.jp

サイバー犯罪対策課  
公式LINEアカウントで  
情報配信中！

@387ojopi

