



福岡県警察からのお願い

令和4年4月

福岡県内企業でもEmotet(エモテット)の感染被害が多数発生

Emotet(エモテット)とは

- ▶ 電子メールの添付ファイル(Excel、Zipファイル等)を主な感染経路とするコンピュータウイルスで福岡県内企業でも感染被害が多数発生しています。
- ▶ 取引先などになりすましたメールの添付ファイルの開封を促し、開封するとメールアドレス、パスワード、メール本文等の情報が盗られ、さらに感染拡大を目的としたメールを取引先などに送信します。
- ▶ 感染を放置しておく、情報が盗られて感染が拡大するだけではなく、他のコンピュータウイルス(ランサムウェア等)に感染した例もあります。

【Emotetに感染誘導するメールの一例】

差出人：甲野乙男<qwertyuiop@xxxxxxx.com>
 件名：RE:書類の送付について 2022/3/8 15:37
 宛先：'福岡サイバー株式会社 fukuoka-cyber@xxxxxxx.jp

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：2022-03-08_1336.zip
 解凍パスワード：Yuod

株式会社エフシスネット
 甲野乙男
 TEL：092-641-1234 FAX：092-641-4321
 E-Mail：o-kouno@efushisu-net.co.jp

添付ファイル：
 2022-03-08_1336.zip
 .zipファイル 161KB

※この時点で感染します

福岡県内企業の実際の事例です！

① ○×社
 ▲■社のAさんからメールだ。なんか内容が変だけど… なにか急ぎの案件かな？ とりあえず添付ファイルを見てみるか。

② Zipを解凍して… Excelを開いて… コンテンツの有効化をクリックっと！ なにも出ないな…

③ 電話で確認したところ…
 エッ？ 送った添付ファイルを間違ってますか？
 ○×社にメールは送っていませんよ。

④ 翌日…(感染の影響)
 取引先企業 ガーン！
 ウイルスメールを送ってくるとはどういうことですか！！
 もう、おたくとは取引しません。
 申し訳ありません…

感染することでの影響

Emotetに感染すると自社の事業継続に支障があるだけではなく、取引先の業務の障害になるなど迷惑をかけることとなり、自社の業務や信用に影響します。



対策!!

Emotetへの対策は、一般的なセキュリティ対策に加え、**取引先等の名前で送信されていても不自然なメールは電話で確認する、添付ファイルを開かない**等といった従業員一人一人が注意することが重要です。もし、感染した疑いがある場合は、一般社団法人JPCERT/CCがインターネット上で公開している**Emotet感染確認ツール「EmoCheck」**でチェックしてみてください。【※注 全てのEmotetを検知するとは限りません。】

- ◆ 福岡県警察本部サイバー犯罪対策課では、最新のサイバー犯罪の手口や対策などをTwitterやホームページに掲載していますので、ぜひご覧ください。
- ◆ 万一、被害に遭われた場合は、管轄警察署宛てご一報ください。

【Twitter】

【HP】

