Ｆ－ＣＳＮＥＴ通信かわら版

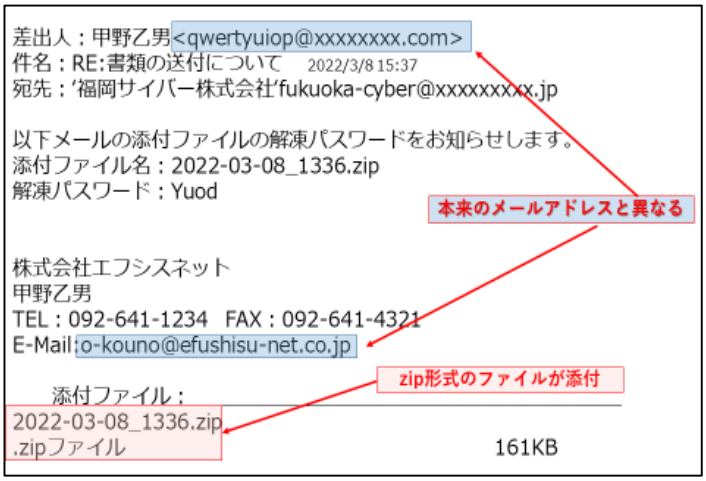
令和4年3月

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と、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】



福岡県内企業の実際の事例です！

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。】

◆ 福岡県中小事業者サイバーセキュリティ支援ネットワーク（通称：F-CSNET）とは、県内中小事業者のサイバー犯罪被害の未然防止･拡大防止を目的として、県内の中小企業支援団体と公的機関で構築したネットワークです。

◆ 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。

【Twitter】　【HP】