

【重要】「Emotet（エモテット）」と呼ばれるマルウェアへの感染を誘導する攻撃メールにご注意ください

平素はインターネットマンションシステムをご利用いただき誠にありがとうございます。

2022年2月以降、「Emotet（エモテット）」と呼ばれるマルウェアへの感染を誘導する攻撃メールが国内外の組織へ広く着信しております。「Emotet（エモテット）」およびマルウェアに感染すると、端末からお客様の情報が漏洩する被害に加えて、ご利用中のメール情報（ID/パスワードやアドレス帳）が悪意のある第三者に不正利用され、お客様になりすました攻撃メールを別の方に送信されてしまう恐れがあります。

不正利用の被害にあわれないよう、お客様におかれましては、以下の対策の実施をお願いいたします。

<対策>

- ・不審なメールの添付ファイルは開かない
- ※以前にやり取りしたメールに対し、「返信」や「転送」の形式で送信者をなりすました新たな手法にご注意ください。
- ・不審なメール本文中のURLリンクやアプリケーションのインストールリンクはクリックしない
- ・OSやアプリケーション、セキュリティアプリを最新の状態にする
- ・重要データやメールのバックアップを取っておく

なお、Emotetへの感染確認については、一般社団法人 JPCERTコーディネーションセンター（JPCERT/CC）が無償公開しているチェックツール「EmoCheck」をご活用ください。

<JPCERT/CC>

<https://www.jpccert.or.jp/at/2022/at220006.html>

<マルウェアEmotetへの対応FAQ>

<https://blogs.jpccert.or.jp/ja/2019/12/emotetfaq.html>

<Emotet感染有無確認ツールEmoCheck>

<https://github.com/JPCERTCC/EmoCheck/releases>

感染が確認された場合は、ネットワークから遮断していただき、ウイルス対策ソフト等での駆除をおすすめいたします。

ご不明な点は [インターネットマンションヘルプデスク] までお問合せください。