

「Emotet」と呼ばれるウイルスへの感染を狙うメールについて

「Emotet」（エモテット）と呼ばれるウイルスメールが国内の組織へ広く発信され、被害が拡大しています。このメールは、お客様が過去にメールのやり取りをしたことのある、相手の氏名、メールアドレス、メールの内容等の一部を流用し、業務上開封してしまいそうな巧妙な文面となっている場合がありますので、ご注意ください。

なお、ウイルスメールの被害を避けるためには、以下の対応が有効ですので、是非ご検討ください。

- 身に覚えのないメールの添付ファイル、メール本文中の URL リンクはクリックしない。
- OS やアプリケーション、セキュリティソフトを常に最新の状態にする。
- 信頼できないメールに添付された Word 文書や Excel ファイルを開いた時に、マクロやセキュリティに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない。
- メールや文書ファイルの閲覧中、身に覚えのない警告ウインドウが表示された際、その警告の意味が分からない場合は、操作を中断する。
- 身に覚えのないメールや添付ファイルを開いてしまった場合は、すぐにシステム管理部門等へ連絡する。
- お客様 ID やログインパスワードを記載したファイルをパソコン上に保存しない。

IPA（情報処理推進機構）にて、詳細情報を公開しておりますので、詳しくは以下のアドレスをご参照下さい。

参照先：<https://www.ipa.go.jp/index.html>

以上