

令和4年3月7日

会員各位

岩見沢商工会議所

コンピュータウイルスへの感染を狙うメールにご注意ください！

～「エモテット」と呼ばれるコンピュータウイルスの相談・被害が増加しています～

独立行政法人情報処理推進機構(以下「IPA」)の発表によると、昨今、「エモテット(Emotet)」と呼ばれるコンピュータウイルスへの感染を狙うメールの相談・被害が増加しています。

エモテットの攻撃では、実際にメールのやり取りをしたことのある、実在の相手の氏名、メールアドレス、メールの内容等の一部が攻撃メールに流用され、ウイルスメールとして送られてくる場合があります(下記「1.」ご参照)。

重要な相手や取引先からのメールに見えても、すぐに添付ファイルや URL リンクは開かず、本物のメールであるか、落ち着いて確認してください。(下記「2.」ご参照)。

また、万一、コンピュータウイルス感染の被害が発生し、どのように対応したらよいか、お困りの場合は、専門の相談窓口もご利用ください(下記「3.」ご参照)。

記

1. 昨今急増しているエモテットの主な特徴・メール例

(その他の特徴やパターン、メール例については、(3)もご参照ください)

(1) 特徴

Excel ファイルや ZIP ファイル付きメールでいずれもファイルの開封や URL リンクのクリックを誘導する内容

(2) IPA で確認しているエモテットの攻撃メールの例(2022年2月)

(塗りつぶし部分は、実在の相手の連絡先や氏名、メールアドレス)

※メール例は以下の URL からご覧ください。

※IPA ウェブサイト

<https://www.ipa.go.jp/security/announce/20191202.html#L18>

(3) 上記以外の特徴やパターン、メール例等について

■「Emotet」(エモテット)と呼ばれるウイルスへの感染を狙うメールについて

<https://www.ipa.go.jp/security/announce/20191202.html>

(2022年2月9日付: IPA ウェブサイト)

2. 主な対応策（引用：IPA ウェブサイト）

- ・身に覚えのないメールの添付ファイルは開かない。メール本文中の URL リンクはクリックしない。
- ・自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない。
- ・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。

3. 相談窓口

- ・IPA 情報セキュリティ安心相談窓口
URL <https://www.ipa.go.jp/security/anshin/>
電話：03-5978-7509（受付時間は平日の 10:00～12:00 および 13:30～17:00）
E-mail：anshin@ipa.go.jp