パソコンをお使いの皆様へ
取引先からのメールの添付ファイルとURLは要注意

「Emotet」（エモテット）と呼ばれるコンピュータウイルスへの感染を狙う
不審なメールの増加が確認されています。
感染すると、送受信メールやアドレス帳の連絡先などの情報を盗まれ、
感染を広げるための材料として使われてしまいます。
全てのメールを疑えば業務が止まってしまい、本末転倒です。
以下に、不審なメールの特徴や対策を記載しますので参考にしてください。

不審なメールの特徴

「Emotet」は、メールに**添付された不審なファイルを開いたり**、メール本文内の**URLからファイルをダウンロードして開いてしまう**ことで感染します。
　メールの内容は様々なパターンがありますが、感染した端末から流出したメールを利用して、**正規のメールへの返信を装う内容**となっている場合は騙されやすいため、特に注意が必要です。

不審なメールの例

ファイル　メッセージ
○○ ○○<○○○○@○○○.○○○>　1　10/23(金)
×××××について

請求書_20201022…
200KB

○○ ○○ 様

お世話になっております。△△です。
取り急ぎご連絡いたします。

>△△ △△ 様
>
>いつもお世話になっております。
>　○○です……

不審な添付ファイル
パスワード付きのzipファイルの場合も確認されています

付け加えられた文章
ファイルをダウンロードするURLが付け加えられている場合もあります

返信を装うため、元々送信したメールの内容が引用されています

このボタンをクリックしてはいけません！ファイルのマクロが動作してウイルスに感染してしまいます

ファイルを開いてしまった場合

「マクロの自動実行」が有効 → 感染

「マクロの自動実行」が無効 → セキュリティの警告　一部のアクティブ コンテンツが無効にされました。クリックすると詳細が表示されます。　コンテンツの有効化

- 既に終わったはずの取引き、心当たりのない担当者など、**やり取り自体が不審なメール**には特に注意しましょう。
- **メールセキュリティソフト**を導入し、**OSなども最新の状態**にしておきましょう。
- メールの**添付ファイルやURLを安易に開かず**、送信元に確認しましょう。
- Wordファイル**「マクロの自動実行」の設定**を確認し、「有効」の場合は**「無効」**にしましょう。

一般社団法人JPCERTコーディネーションセンターが掲載している「マルウェアEmotetへの対応FAQ」（https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html）が更新されています。
感染予防対策や事後対策等について詳細に掲載されていますので参考にしてください。

埼玉県羽生警察署　☎０４８（５６２）０１１０