取引先のメールアドレスを装った
「なりすましメール」にご注意ください

「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙う攻撃メールが国内の組織へ広く発信され、「なりすましメール」被害が拡大しています。

一見すると正規の差出人からのメールであるかに思える場合であっても、心当たりのないメールを受信した場合は、添付ファイルを安易に開封したり、メール本文中に記載されたＵＲＬをクリックしたりせず、メールごと削除するようお願いいたします。

感染した場合、以下のような被害を受けることが報告されており、不正送金等の被害に発展する恐れがあります。

- ＩＤ・パスワード等の情報が窃取される
- メールやアドレス帳の情報が窃取される
- 窃取されたメールアカウントや本文などが悪用され、Emotet の感染を広げるメールが送信される（加害者になってしまう）

Emotet による感染を防ぐためには、以下の点に注意していただくことが有効です。

- メールの件名やメール本文が、メール受信者と全く関係ない内容となっていないこと等を確認する
- 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、内容や添付ファイル名等に、不自然な点がないことを確認する

もし、メールに添付された Word ファイルや 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は、安易に「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せず、システム管理者へ連絡し、指示を仰ぐことも有効です。

お客さまにおかれましても、被害に遭わないようご注意ください。

なお、JPCERT/CC や IPA（情報処理推進機構）が、手口や対策を公開しておりますので、詳しくは以下 URL をご参照ください。

- JPCERT/CC　マルウェア Emotet の感染拡大および新たな攻撃手法について
- IPA　「Emotet」と呼ばれるウイルスへの感染を狙うメールについて