２０２２年3月9日

マルウェア「Emotet」にご注意ください

「Emotet」(エモテット)と呼ばれるマルウェアへの感染を狙う不審メールが国内で急増しており、数多くの感染被害が確認されています。「Emotet」は、感染した端末のメール情報を盗み、その情報を悪用してさらに攻撃メールをばらまく特徴があり、感染被害が連鎖的に拡大していきます。

見知った相手からのメールに見えても、感染を狙った攻撃メールの可能性があるため注意が必要です。

取引先や知人などから、自社や自身の名前を詐称した不審メールが送られているとの連絡を受けた場合、「Emotet」に感染している可能性があります。万が一感染していた場合、インターネットバンキングのお取引をお控えいただいた上、直ちにウイルスチェックを行うなどの対策を実施してください。

また「Emotet」に限らず、一般的なウィルス対策として次のような対応をすることをお勧めします。

・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。
・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」というボタンは安易にクリックしない。
・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。

独立行政法人情報処理推進機構
「Emotet（エモテット）」と呼ばれるウィルスへの感染を狙うメールについて」より抜粋

■インターネットバンキングに関するお問い合わせ先

０１２０－２７５－２０１

受付時間　平日９：00～17：00（※12 月 31 日～1 月 3 日および、土日祝日は除きます）

・「Emotet」の手口や対策

IPA（情報処理推進機構）

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

・「Emotet」への感染が疑われる場合、または、感染してしまった場合の対応

JPCERT コーディネーションセンター

→マルウェア Emotet への対応 FAQ

以上

千葉信用金庫