２０２２年１１月１６日
Ｋビジョン株式会社

【注意喚起】マルウェア Emotet の感染再拡大について

メール感染型マルウェア Emotet（エモテット）（※）について、１１月に入り国内において改めて不審なメールの受信が確認されたとの連絡を受けたことから、Ｋネットをご利用のお客様へ注意喚起します。

不審なメールの添付ファイルは開かない、メール本文中の不審な URL リンクはクリックしないようにするなど、以下の対策を行ってマルウェアに感染しないよう注意してください。

【対策】

- **○ 見知った相手からの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**
- **○ 本物のメールか判断がつかない場合は、添付ファイルを開く前に電話等確実な手段でメールの差出人に問い合わせる**
- **○ OS、セキュリティ対策ソフト、その他ソフトウェアを最新の状態に更新する**
- **○ マクロの自動実行機能を備えたソフトウェア（ワード、エクセル等）について、当該機能を無効化する**
- **○ 添付ファイルを開いて「コンテンツの有効化」や「マクロを有効にする」という指示が画面上に表示されている場合、信頼できるファイルと判断できなければクリックしない**

（※）Emotet（エモテット）は主にメールを感染経路としたマルウェア（不正なプログラム）です。
メールソフトに登録している連絡先メールアドレスを盗んで使うなどして、知り合い本人が作成したメールであると信じ込ませ、不審に思わず開封してしまいそうなメールを装うなど巧妙化が進んでいます。このメールにはエクセルファイル（.xls）やショートカットファイル（.lnk）またはこれらを含むパスワード付きの ZIP ファイルが添付されていることが確認されています。安易にこれらの添付ファイルを実行してしまうと Emotet に感染し、パソコン内の情報が盗まれたり、ランサムウェア等の他のマルウェアにも感染するといった被害に遭う恐れがあります。**また、対策としてマクロ機能を無効化に設定している場合でも添付ファイルの指示どおりに Templates フォルダにコピーして開くとマクロが強制的に実行され感染します。**

詳しくは下記のサイトを参考になさってください。

・参考 URL（IPA：情報処理推進機構　Emotet と呼ばれるウィ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

以上