警察からパソコンをご利用の皆様へ

要注意！！

「Emotet」～メールの添付ファイルに気をつけて～

「Emotet」って何？？

特　徴

- Emotet（エモテット）は、主にメールの添付ファイルを感染経路とした不正プログラムです。
- 感染したパソコンからメールアカウント、パスワード、過去にやりとりしたメール本文等の情報を盗み、これらの情報を悪用して、感染拡大を目的としたメールを送信します。

メール例

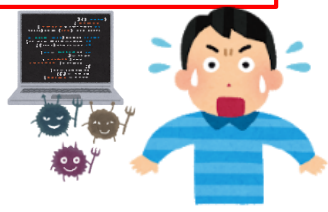
差出人	株式会社島根　才端太郎<cybertaro@shimane.co.jp>	過去にやりとりした相手のメールアドレス
件名	Re:見積もりの件について	実際に送信したメールの件名の返信など
本文	お世話になります。 下記の添付ファイルについて、確認願います。 パスワードは、123456になります。	
添付ファイル	見積書.zip	不正な添付ファイル

パスワード付きZIP形式で圧縮された文書ファイルが添付されています。
添付ファイルを開くと、ファイルに埋め込まれたマクロの実行を促す内容が表示され、実行するとEmotetに感染します。本文に記載されたURLリンクなどからEmotetに感染する事例もあります。

「コンテンツの有効化」ボタンをクリックすると、
Emotetに感染！！

感染すると…

- パソコン内の情報が盗まれて、組織内外で感染が拡大する。
- Emotet以外の他の不正プログラムにも感染する。



対　策

◎　送信したメールへの返信に見えるメールでも安易に添付ファイルは開かない、メール本文中のURLのリンクはクリックしない。
◎　メールに添付された文書ファイルを開いたときに、マクロを有効にしない。
◎　セキュリティの警告を無視した操作をせず、警告の意味が分からなければ操作を中断する。
◎　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。
◎　万が一、不審なメールや添付ファイルを開いた場合は、すぐにシステム管理部門等へ連絡の上、最寄りの警察署へ連絡する。

詳しくは、下記サイトにも掲載されています。
IPA（https://www.ipa.go.jp/security/announce/20191202.html）

島根県警察本部生活環境課サイバー対策室