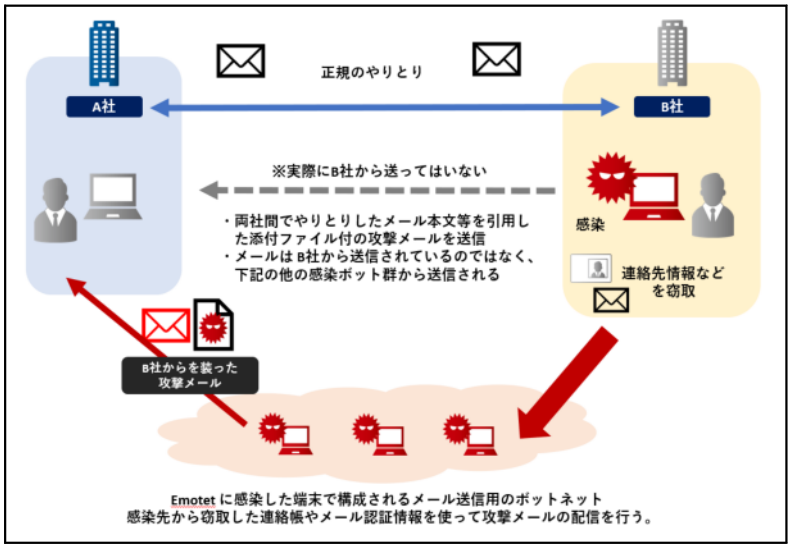
メール情報を盗み出すマルウエア（Emotet）に注意!!

昨年１０月以降、国内においてEmotet（エモテット）と呼ばれるウイルスへの感染が拡がっています。

感染経路は主にメールで、実在の送信者を装ったメールを送りつけられ、受信者がその添付ファイルを開くことによって、マクロが自動実行するというものです。

本県でも発生が確認されています。



一般社団法人 JPCERT コーディネーションセンターより

☆　感染すると・・・

○　端末やブラウザに保存されたパスワード等の認証情報が盗まれる。

○　メールアカウントやパスワード、メール本文、アドレス帳の情報が盗まれる。

○　盗まれたメールアカウントや本文が悪用され、Emotetの感染を広げるメールが送信される。等々

※　また、自己拡散機能や拡張機能を持っていることから、不正送金マルウエアやランサムウエア等に２次感染するおそれもあります。

☆　感染しないために

○　不審なメールのリンクや添付ファイルを開かない。

○　WordやExcelのマクロの自動実行が無効になっていることを確認する。（ファイル→オプション→セキュリティセンター→「警告を表示してすべてのマクロを無効にする」をチェック）

○　OSを常に最新状態に更新する。

○　メール攻撃対策製品を導入する。

※　一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）、独立行政法人情報処理推進機構（IPA）のサイトにおいて、詳しい情報が掲載されています。参考にしてください。

福島県警察本部生活安全部生活環境課
サイバー犯罪対策室
情報提供メール：fp-hitec@police.pref.fukushima.jp

福島県警サイバー防犯キャラクター
ダ メ ポ チ く ん