Emotet（エモテット）に注意!

～ウイルスメールに気をつけて～

和歌山県警察マスコット
きしゅう君

県内でEmotet（エモテット）による被害が発生

県内で、情報の窃取・感染拡大するコンピュータウイルス「Emotet （エモテット）」と思われる被害が確認されました。

Emotetは令和元年10月以降、全国でも被害が多数報告されており、感染が拡大しています。

Emotetの特徴として、**感染したパソコンからメールアドレスを窃取し、更に偽装メールを送信し感染をより広げていく**ことがあげられます。

また、感染したパソコン内のメーリングリストから過去に送受信したメールを引用するなど、**その人があたかも送っているかのような偽装メール**が送られてきます。

Emotet（エモテット）とは

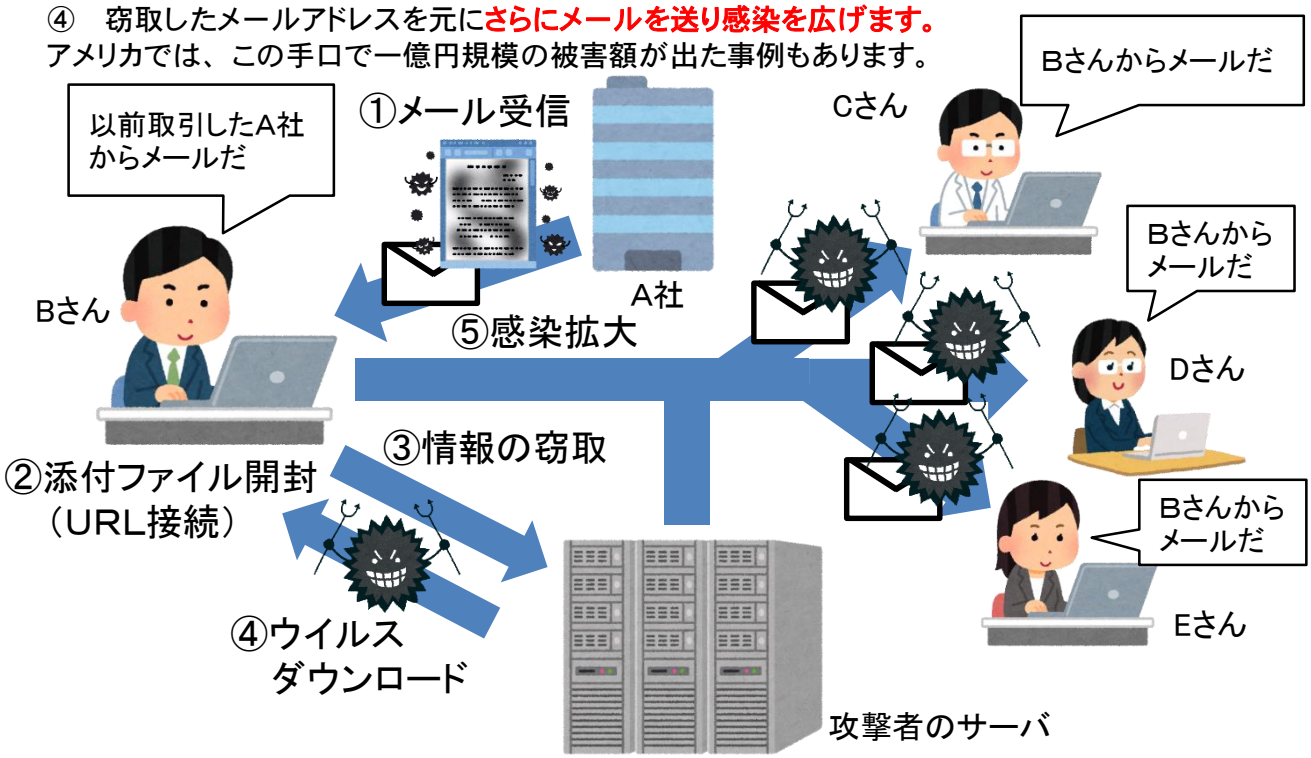
① 主に攻撃者からの**メールに添付されているファイル（WordやExcel等）**から**感染**します。
※メール本文のリンクURLに接続し、感染してしまう場合もあります。

② 感染すると、感染したパソコンにある**メールアドレスやメールアカウントのパスワード等が窃取**されます。

③ 添付ファイルに設定されたプログラムにより、**新たなウイルスがダウンロード**されます。

④ 窃取したメールアドレスを元に**さらにメールを送り感染を広げます。**

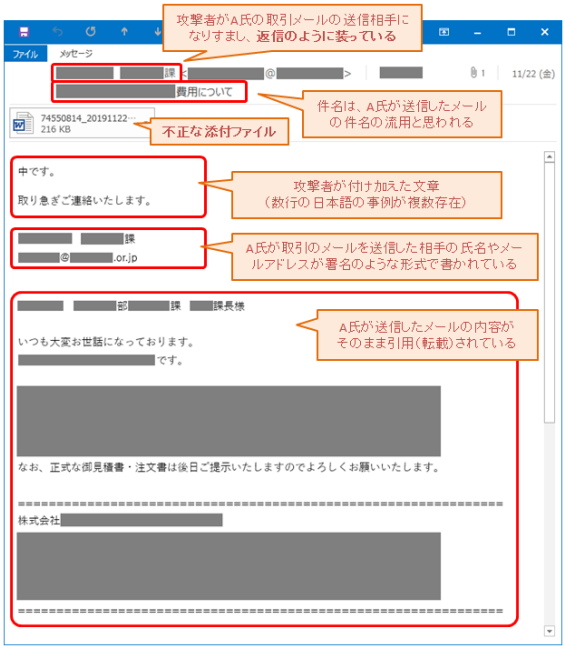
アメリカでは、この手口で一億円規模の被害額が出た事例もあります。



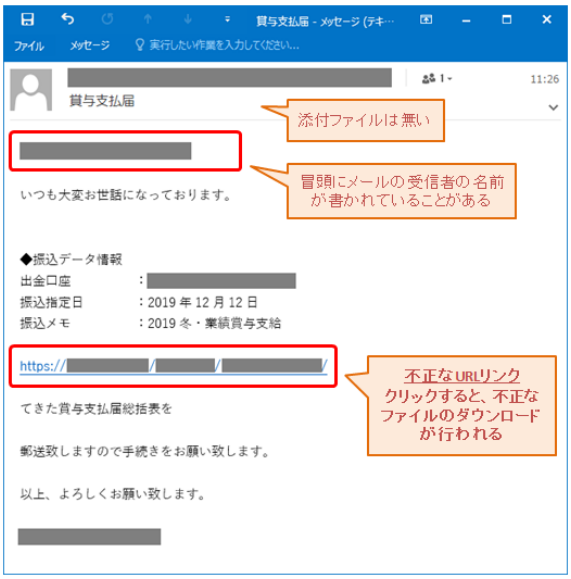
知人や取引先からのメールであっても、偽装されているかも知れません!!

ウイルスメールの例

添付ファイルを開くことで感染が起こるメール



リンク先を開くことで感染が起こるメール



出典　独立行政法人情報処理推進機構ホームページ

対策

☆　メールを受信したとき

- OS、セキュリティソフトやメールソフトは**常に最新の状態**にする。
- 身に覚えのないメールの添付ファイル（リンクURL）は開かない。
- 返信メールであっても、不審な点があれば添付ファイル（リンクURL）は開かない。

☆　添付ファイル（リンクURL）を開いてしまったとき

- メールに添付のWordやExcelファイルを開いてしまい、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」というボタンはクリックしない。**

- リンク先でダウンロードが始まってしまったら、**通信を切りパソコンをネットワークから隔離してください。**

☆　感染が疑われる場合

- パソコンを**ネットワークから隔離する。**
- メールアカウント等の**パスワードを変更する。**
- 過去に送受信した相手やメーリングリストに登録している人へウイルスメールが届いているのであれば**メールを開かないように注意喚起する。**
- ウイルス対策ソフトによる**ウイルスチェックを実行する。**

実際に感染した場合や感染が疑われる場合は、**お近くの警察署又はサイバー犯罪対策課にご相談ください。**

【発行元】　和歌山県警察本部サイバー犯罪対策課　　073-423-0110㈹