サイバーセキュリティだより

発行：愛媛県警察本部生活安全部サイバー犯罪対策課

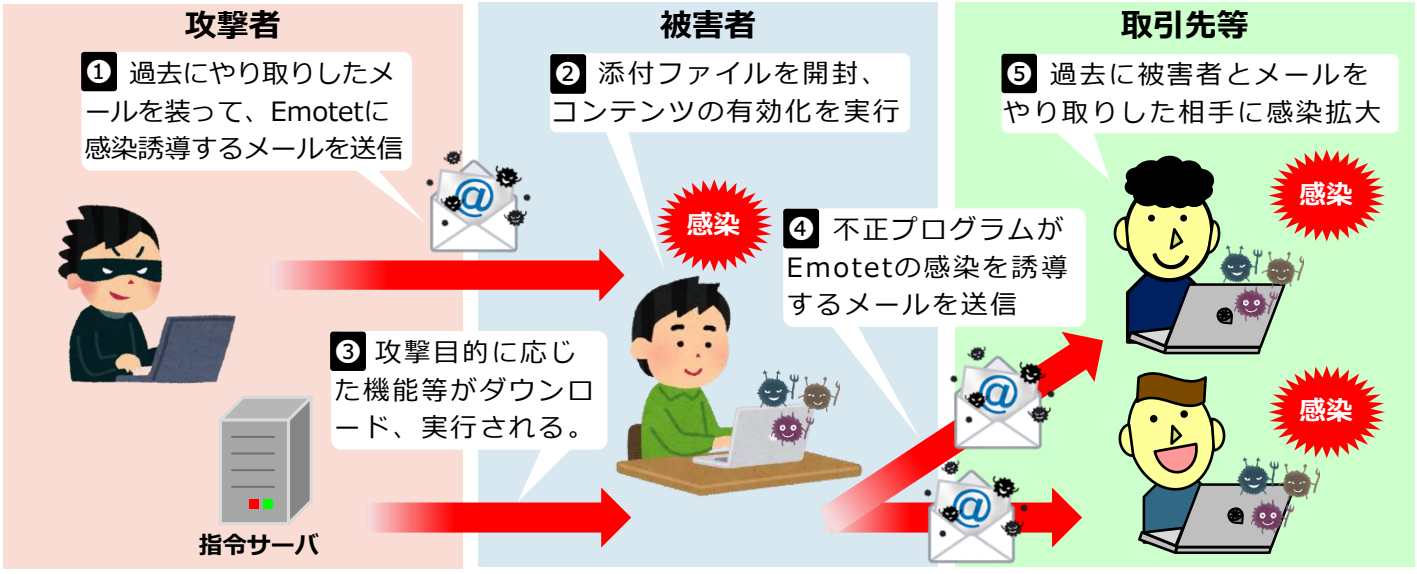
令和4年
6月30日
Vol.78

手口が巧妙化する Emotet に注意

Emotet（エモテット）は、主にメールを介して感染するマルウェアで、過去にやり取りしたメールの返信を装ったメールを送り付け、添付ファイル※の開封を促します。

添付ファイルには、**Emotetに感染するプログラム**が埋め込まれており、この**ファイルを開封しただけで、Emotetに感染**するおそれがあります。

※WordやExcelファイルの他、ショートカットファイル（LNKファイル）を添付する手口も確認されています。



Emotetに感染すると・・・

- **過去にやり取りしたメールの本文やメールアドレス、メールソフトやブラウザに記録したパスワード等の情報が盗み取られる。**
  - ⚠ **ウェブブラウザ「Google Chrome」に保存されたクレジットカード情報を盗み取る手口も新たに確認されています。**
- **盗み取られたメールに関連する情報が悪用され、感染拡大を目的としたメールが送信される。**
- **バンキングトロイ、ランサムウェア等、他の不正プログラムに感染する。**
- **ネットワーク内の他のパソコンに感染拡大する。**

Emotetの被害に遭わないための対策

- **自分が送信したメールへの返信に見えるメールを受信しても、添付ファイルを不用意に開いたり、メール本文中のURLリンクをクリックしたりしない。**
- **添付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には、不用意にマクロを有効にしたり、セキュリティ警告を無視しない。**
- **マクロの自動実行機能を備えたソフトウェアについて、当該機能を無効化する。**
- **ウイルス対策ソフトやOS、その他ソフトウェアを常に最新の状態に更新する。**
- **メールセキュリティ製品を導入する。**
- **不正通信ブロックサービスを導入する。**

相談窓口　愛媛県警察本部サイバー犯罪対策課 TEL089-934-0110(代)