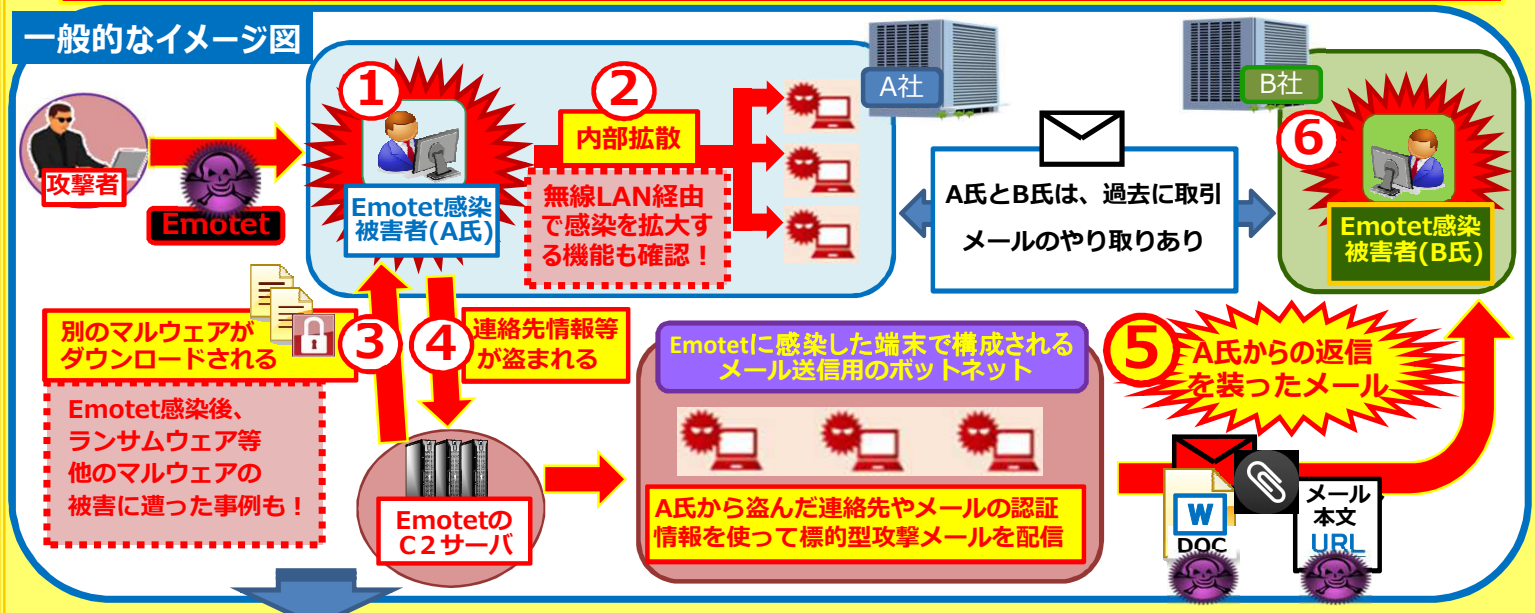
CyberCrime Control Project

令和２年第１号

広島県警察本部
サイバー犯罪対策課
082-228-0110
（内線　705-586）

マルウェア「エモテット（Emotet）」感染被害拡大中！

一般的なイメージ図



イメージ図の説明

① A氏のPCが何らかの原因で「Emotet」に感染する。

② A氏のPCからA社内の他のPCに感染が拡散する。
（無線LAN経由で感染を拡大する機能も確認）

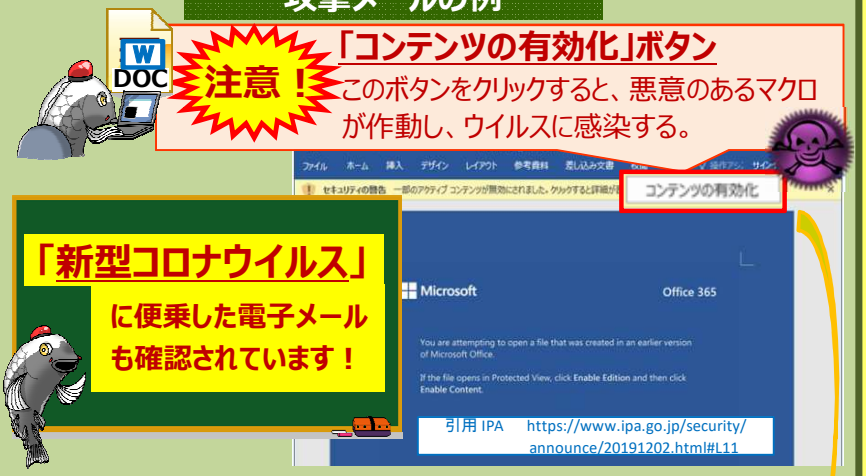
③ A氏のPCに別のマルウェアがダウンロードされる。
「Emotet」感染後、**ランサムウェアに感染**させられた事例もある。

④ A氏のPCから連絡先・メールの認証情報等が窃取される。

⑤ 「Emotet」に感染したボットネットから、**A氏からの返信を装ったメール**がB氏宛に送信される。

⑥ B氏がメールの添付された**ワードファイルを開き、マクロを有効にする**あるいは、メール本文の**URLをクリック**することで「Emotet」に感染する。

攻撃メールの例



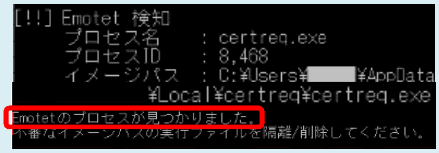
「Emotet」感染有無の確認と削除

～ JPCERT/CCよりリリースされた「EmoCheck」で確認できます ～

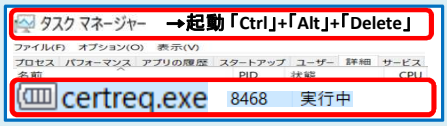
① 「EmoCheck」をダウンロード

② 「EmoCheck」の実行
コマンドプロンプトまたはPowerShellで実行

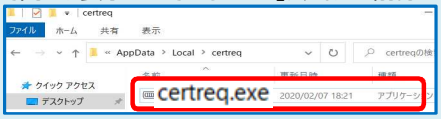
③ Emotetのプロセスが見つかりました



④ Emotetのタスクを終了
タスクマネージャーを起動し、実行結果に表示されている「プロセスID」を選択し、タスクを終了。



⑤ Emotetを削除
「イメージパス」のフォルダ部をエクスプローラーで開き、表示されている「exe」ファイルを削除。



⑥ EmoCheckを再実行し検知なしを確認

引用 JPCERT/CC
https://blogs.jpcert.or.jp/ja/2019/emotetfaq.html

感染予防、感染被害最小化のための対策

- 組織内への注意喚起の実施
- Word**マクロの自動実行の無効化**
（Wordのセキュリティセンターのマクロの設定で「警告を表示してすべてのマクロを無効にする」を選択）
- メールセキュリティ製品の導入によるマルウェア付きメールの検知
- メールの監査ログの有効化
- OSに定期的にパッチを適用
- 定期的なオフラインバックアップの取得
（標的型ランサムウェア攻撃への対策）

引用 JPCERT/CC
https://www.jpcert.or.jp/at/2019/at190044.html