



エモテット マルウェア「Emotet」活動再開!!

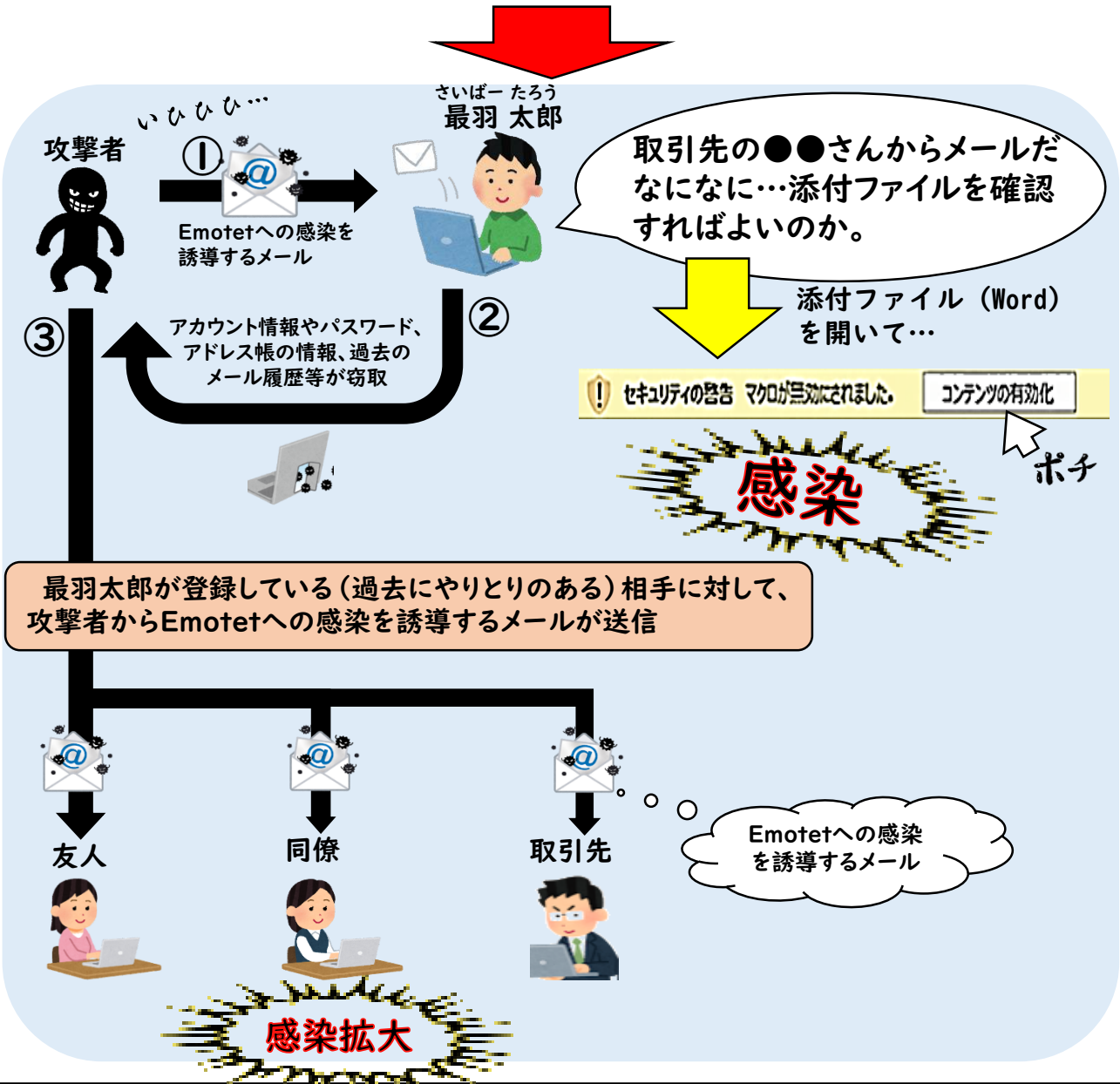
エモテット
Emotetは、主にメールを感染経路としたマルウェアウイルス（不正プログラム）の名前です。

これまで幾度となく世界中で猛威をふるってきましたが、令和4年7月頃から活動を停止していました。

要注意

しかし!警察庁によると、本年11月、国内でEmotetメールが複数見つかリ、その活動が再開したことが確認されました。

Emotetに感染するまでの流れ





サンプルメールを基に チェックポイントを見ていきましょう！



2022/11/22 (火) 11:24

奈良県警察株式会社_総務部_奈良太郎 <emotet.emotet@.jp>

RE: 見積書の作成依頼について

宛先

- 攻撃者が取引メールの送信相手に偽装
- 見慣れない（不審な）メールアドレス



765543_202211.docx.rtf
154 KB

不正な添付ファイル

おはようございます。

謄本及び公図のデータを送ります。

どうぞよろしくお願い申し上げます。

- 攻撃側が付け加えた文章
- 返信メールにも関わらず、全く関係のない内容が記載されている場合も

>奈良県警察株式会社 総務部 奈良 太郎様

>お世話になっております。サイバー株式会社の最羽太郎です。

>先日、ご相談させていただいた件について、見積書の作成をお願いいたします。

>-----

>サイバー株式会社 総務部 最羽 太郎

>TEL 0742-23-0110

> @ .jp

>-----

取引相手に送信した正規のメールの内容



メールサンプルのように、一見して過去にやりとりのある相手方から送信されたメールであっても、メール本文の内容をよく確認して不自然な点があれば、添付ファイルは開かず、一旦、相手方に確認するよう心掛けてください！

Emotetへの対策

STOP! サイバー犯罪!

- 身に覚えのないメールの添付ファイルは開かない！本文中のURLリンクもクリックしない！
- 添付されたファイル（WordやExcel）を開いたとき、「マクロを有効にする」「コンテンツの有効化」というボタンは絶対にクリックしない！
- メールや文書ファイルの閲覧中、身に覚えのない警告ウィンドウが表示された時は、操作を中断する！
- ウイルス対策ソフト、OSを更新して、常に最新の状態を保つ！



参照 独立行政法人 情報処理推進機構（IPA）

「Emotet（エモテット）と呼ばれるウイルスへの感染を狙うメールについて」

URL:<https://www.ipa.go.jp/security/announce/20191202.html>