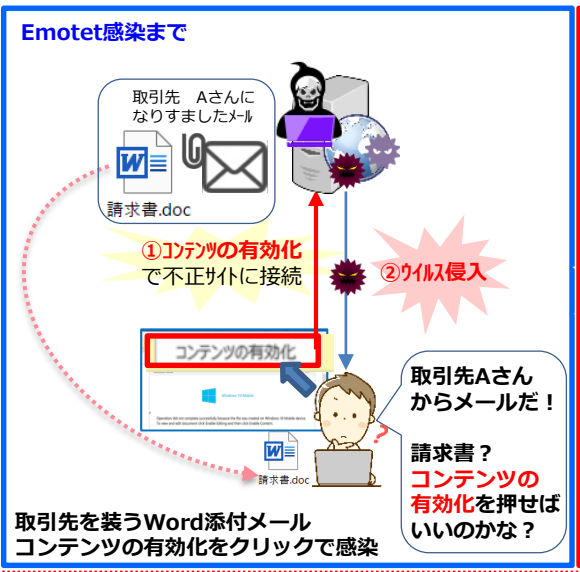
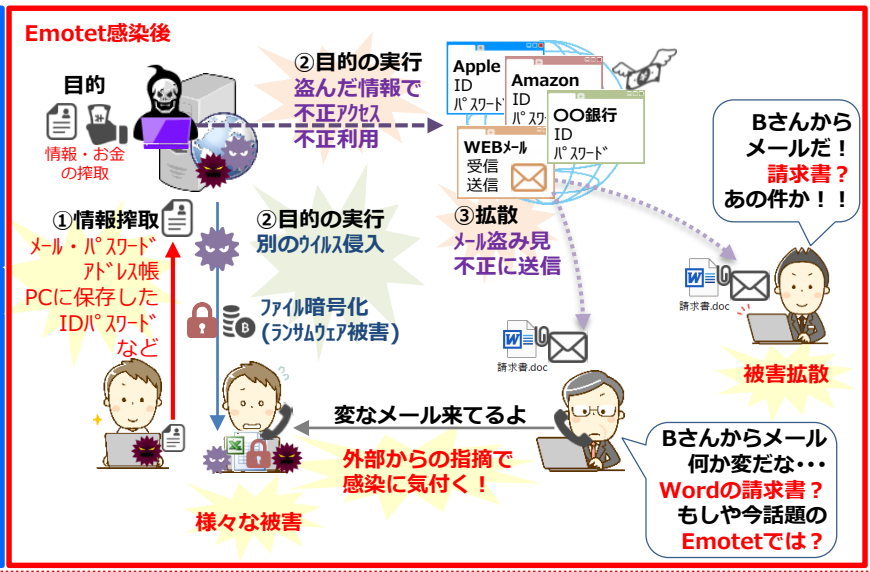
回覧 印 印 印 印 印 印 印 印 印 印 印 印

ASAMA Security News Letter Vol.65

あさまセキュリティニュースレター

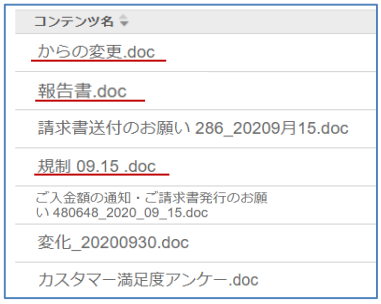
被害にあったら取引先にも･･･Emotetの脅威と対策について！ （2020年10月12日）





攻撃のパターン

不正なプログラムを組み込んだ、Wordの添付ファイル付きメールによる攻撃（取引先になりすまし、成功率が高い）



←実際に添付されていたWordのファイル名（高度なウイルスチェック機能による検知）
その他、シンプルなファイル名の検知が増えています。下記の添付も開かずに削除！
注文.doc 注文書.doc 変化.doc 追加分も.doc 資料.doc 給与.doc ビル.doc 2020.doc
契約する.doc 作業計画.doc テスト結果.doc アンケート.doc 総会 2020 09.doc

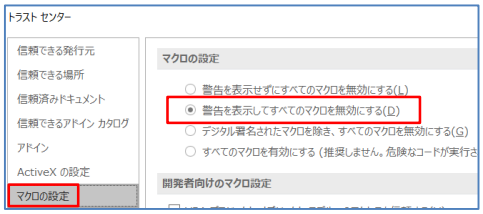
下記のケースも要注意！
添付がExcel形式、PDF形式、圧縮された形式（.zip .lzh .gz等）の場合あり
パスワード付きフォルダで届いたファイル（ウイルス検知をすり抜けています）
メール本文内のURLリンク（リンク先が不正サイトになっているの可能性）

感染が疑われる場合の対処

メールの添付を開きコンテンツの有効化をした、取引先からEmotetと思われる内容の連絡を受けた場合、
下記サイトの感染確認ツール『EmoCheck』で確認を行い、手順従い対処しましょう
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html（JPCERT/CC マルウエアEmotetへの対応FAQ）

対策

・Wordを起動、オプション→セキュリティ（またはトラスト）センターの設定
→マクロの設定が『警告を表示してすべてのマクロを無効にする』（デフォルト設定）になっているか確認



サイバー攻撃は高度化し脅威は増える一方、**テレワーク等でセキュリティが行き届いていない環境でのネット利用が増え**、社内で直接情報共有・相談できる場も減り、**リスクは格段に増えて**います！
どこにいても、社内・取引先からでも、常にリスクがあると考え、安易に開かず必ず確認を！
知っていれば防げるため、**全社員へ注意喚起、OSやソフト、機器のアップデートも忘れずに対策しましょう**

迷惑メール相談センター https://www.dekyo.or.jp/soudan/index.html IPA https://www.ipa.go.jp/security/announce/20191202.html#L13

浅間商事株式会社 〒110-0005 東京都台東区上野7-15-70 浅間第一ビル 0120-830-414