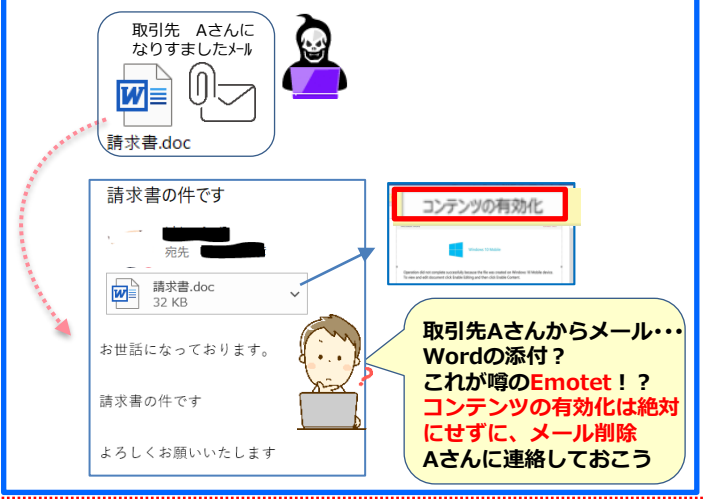
回覧 印 印 印 印 印 印 印 印 印 印 印 印

ASAMA Security News Letter Vol.68

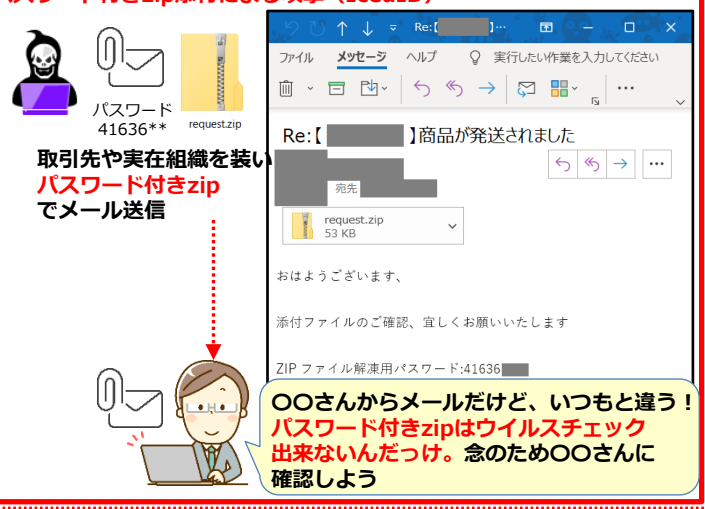
あさまセキュリティニュースレター

どこにいても、社内・取引先からのメールでも細心の注意を！ （2021年1月14日）

取引先のメールを悪用、主にWord添付による攻撃（Emotet）



パスワード付きzip添付による攻撃（IcedID）



攻撃のパターン

取引先、過去にやり取した相手先、実在する企業を装っている、本文もWordファイル内の文も日本語
ウイルスチェックをすり抜ける暗号化したZipファイルでの送信してくることもあり！
添付のWord等を開いてしまっても、コンテンツの有効化は絶対にしないように！！
本文に記載されたURLがあった場合もクリックしないように！！
『会議開催通知』・『賞与支払』等、時期に合わせて件名や添付ファイル名も変えてきます

被害

端末やブラウザに保存されたパスワード等の認証情報が窃取される
窃取されたパスワードを悪用され、社内ネットワーク内に感染が広がる
メールアカウントとパスワードが窃取される→メールサーバに直接アクセスされ、大量送信にも使われる
メール本文とアドレス帳の情報が窃取され、その情報を悪用し、取引先等感染を広げるメールが送信される
他のウイルスをダウンロードし、二次被害の恐れもあり！！（ランサムウェア・不正送金等被害）

対策

- **Wordのマクロの設定が、『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**
- **知っているメール送信者からでも不審な添付ファイル、URLリンクは開かない、相手先に確認する**
- **添付ファイルを開いてしまった場合でも、コンテンツの有効化はせず、ファイルを閉じ削除**
- **社員全員で最新の情報、脅威、手口を知る、ネット利用には社内外問わず、常に脅威が存在すると考える！**

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脅威も多いため、**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を**

情報源

IPA　https://www.ipa.go.jp/security/announce/20191202.html
JPCERT　Emotet などのマルウェア感染に繋がるメールに引き続き警戒を　https://www.jpcert.or.jp/newsflash/2020122201.html

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