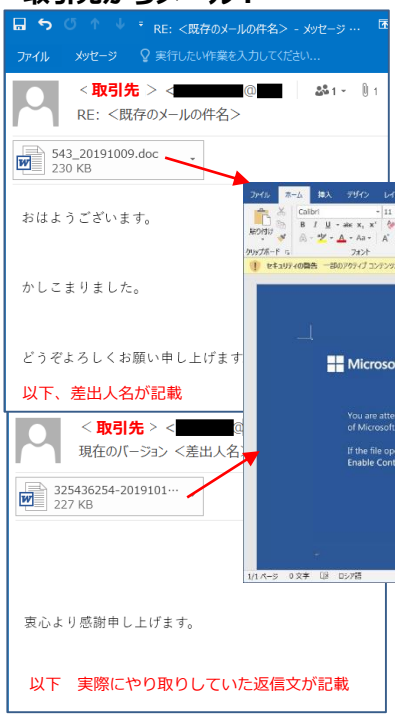
回覧 印 印 印 印 印 印 印 印 印 印 印 印

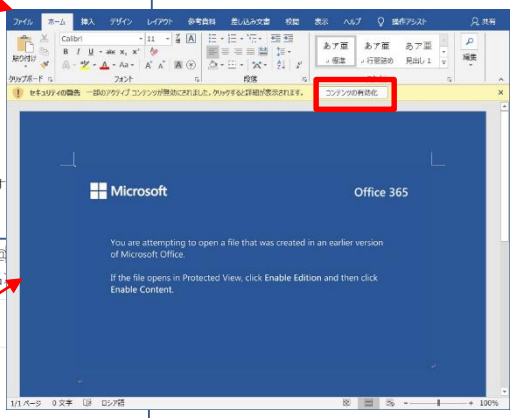
ASAMA Security News Letter Vol.55

あさまセキュリティニュースレター

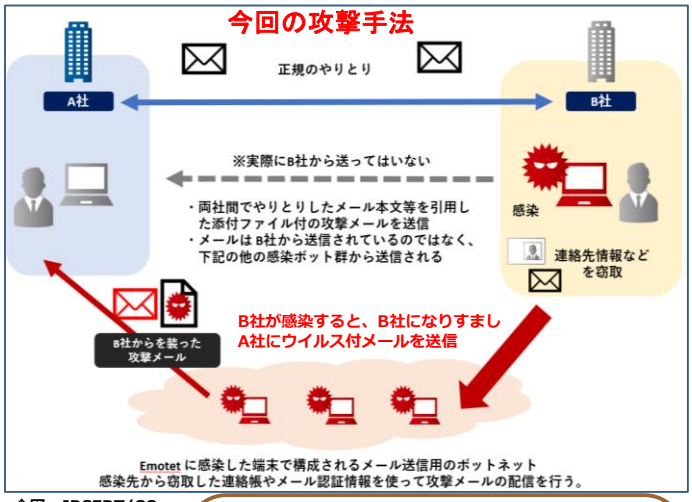
取引先とのやり取りメールに紛れ込むウイルスが大流行！！ (2019年12月11日)

取引先からメール？





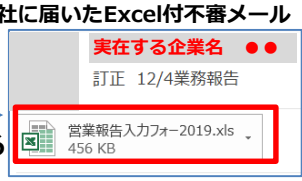
添付ファイルの中身一例
コンテンツの有効化をすると不正プログラムがダウンロードされ、ウイルス感染



↑図　JPCERT/CC

取引先とのやり取りメールに紛れ込む添付のWordファイルに要注意！！
・取引先や顧客の連絡先とメール内容が窃取され外部に送信
・（取引先以外の）外部の組織に大量の不審メールを送信
・他のマルウエアに感染する恐れ

12月弊社に届いたExcel付不審メール



攻撃のパターン

- 取引先からのメールと思わせ、WordやExcelファイルを開かせる
- コンテンツの有効化をするように誘導し、裏でウイルスをダウンロード・感染させる
- メール、ネットバンキング、カード情報、WEBサービスのID・パスワードを窃取し、不正利用
- 盗んだメール・パスワード、アドレス情報を元に、他社へ感染を広げる

被害

メール・パスワード・アドレス帳情報搾取、不正利用
ネットバンキング不正利用・ランサムウェア被害
社外に同様のメール配信

対策

- 知っているメール送信者からでも不審な添付ファイルは開かない、相手先に確認する
- 添付ファイルを開き、Office製品の警告が表示されても、安易にコンテンツの有効化をしない
- 社員全員で最新の情報を得る、最新の脅威を知る、手口を知る、セキュリティに対し常に意識をもつ

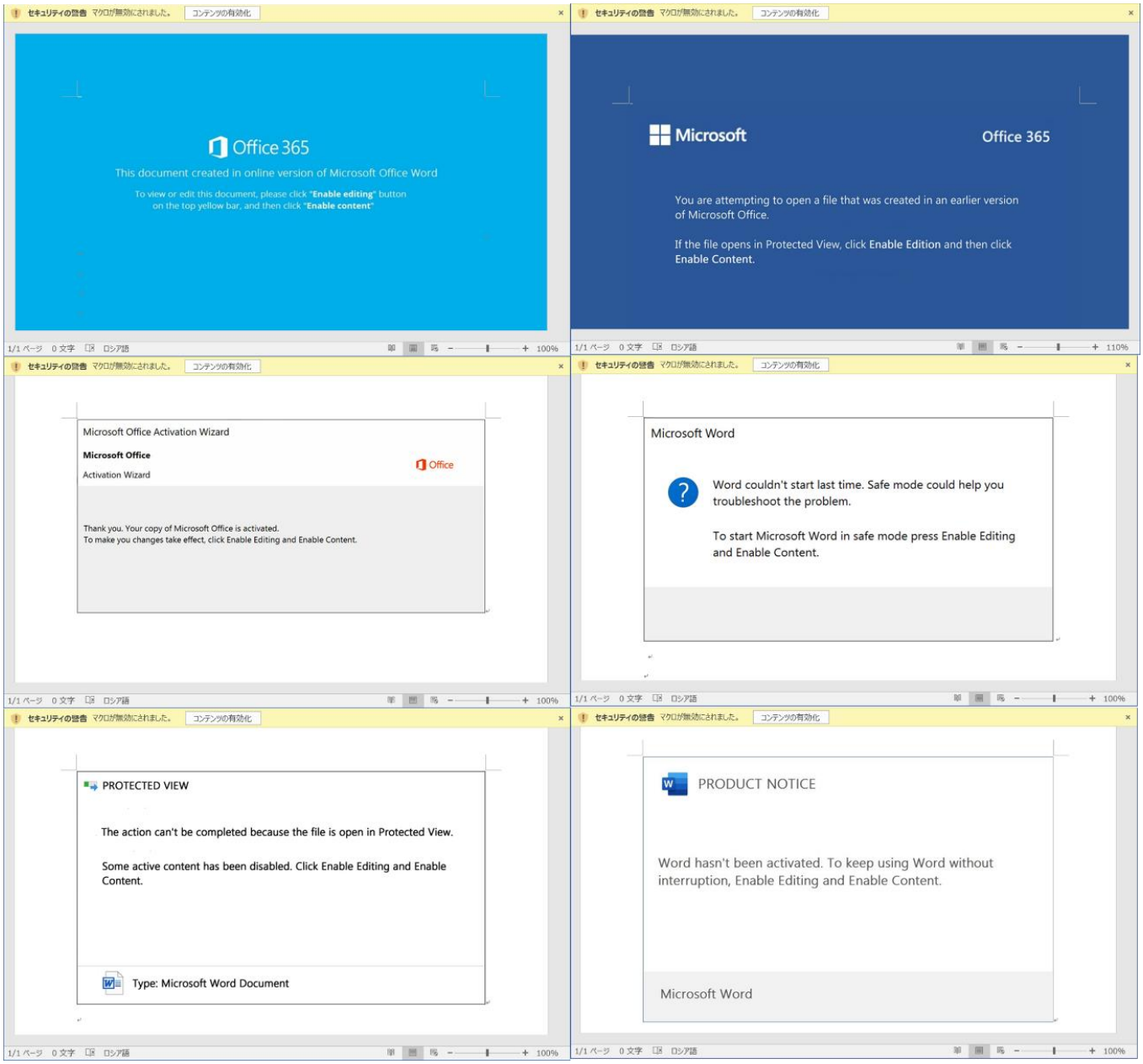
情報源

IPA　https://www.ipa.go.jp/security/announce/20191202.html　**JPCERT/CC**　https://www.jpcert.or.jp/newsflash/2019112701.html
マルウェア情報局　https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1910.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

10月にEmotetの感染を狙ったダウンローダー(Word)の表示画面

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のクリックは押さないでください



https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1910.html