

中小企業  
の皆様へ

さいばーどうねっとニュース 第30号

# Cyber-道net News

発行日  
令和2年2月4日

発行元  
北海道中小企業  
サイバーセキュリティ  
支援ネットワーク事務局

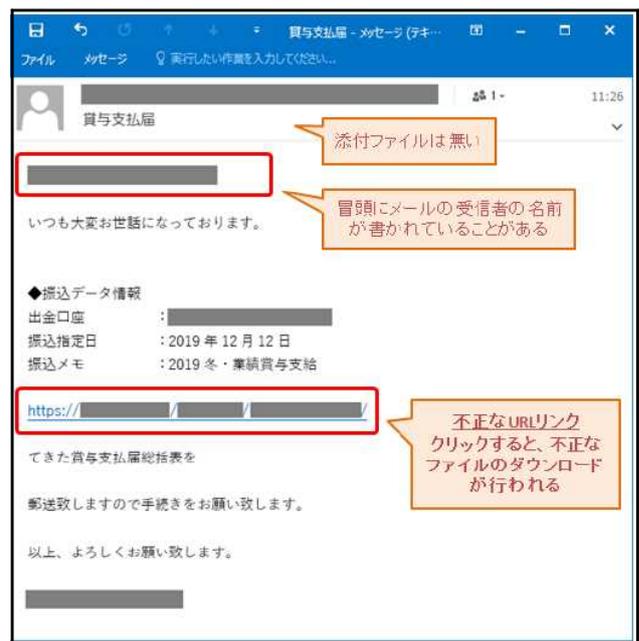
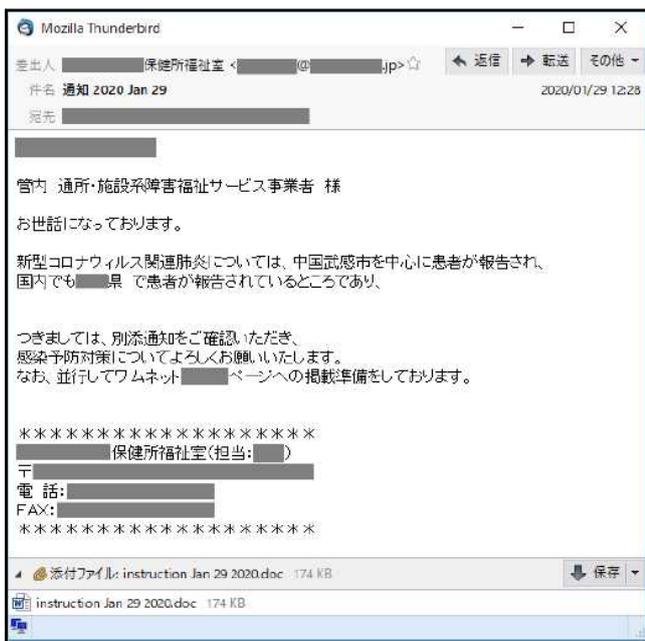


## メールを感染源とするウイルス 「エモテット」に対する注意喚起

エモテット (Emotet) と呼ばれる、ウイルス感染を狙うメールが昨年引き続き猛威を振るっています。

今後も同様の手口による攻撃メールが出回り続ける可能性もあり、今回は具体的な攻撃メールの文面及びその対策例を紹介します。

### 手口のパターンは大きく分けて2つあります

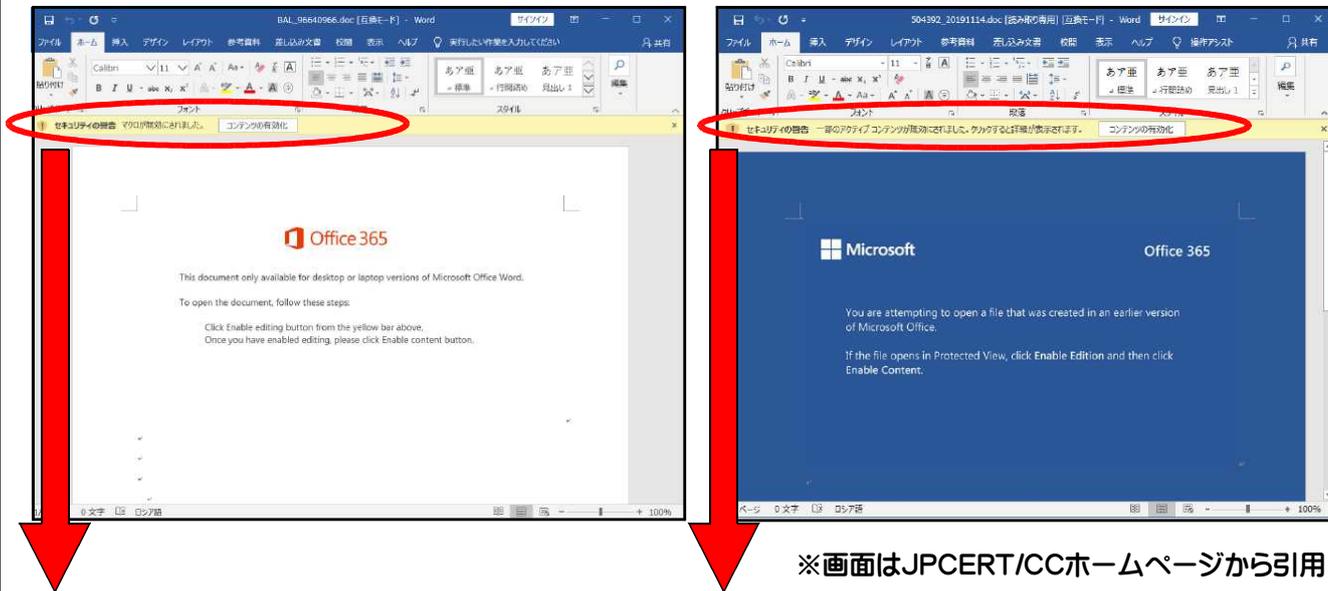


左：ウイルスが添付されている例 右：本文に不正なURLが記載されている例 ※いずれもIPA林-IA°-ヅ から引用

### 攻撃者は皆さんの興味・関心を惹く内容とタイミングを計り狙ってきます！

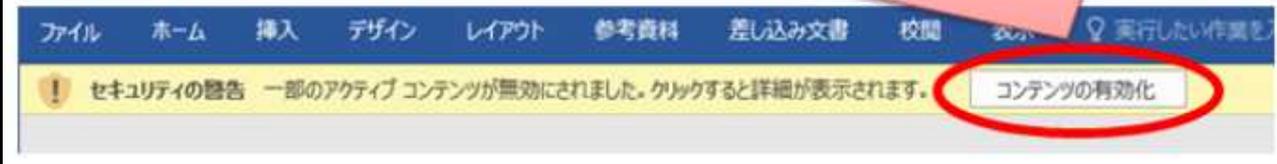
- 自分が送信したメールの返信に見えるメールであっても、不自然な点があれば添付ファイルを開かない (URLをクリックしない)
- 信頼できないメールの添付ファイル等をクリックしてしまい「マクロを有効にする」「コンテンツの有効化」というボタンが表示されてもクリックしない
- メールや文書ファイルの閲覧中、自分では判断できない警告画面が表示された場合は作業を中断する

①添付ファイルを開いてしまった場合の画面例及び注意点



※画面はJPCERT/CCホームページから引用

**注意！** このパソコン上で、文書ファイルに埋め込まれているマクロ(プログラム)等の実行を許可するという意味のボタン。このボタンをクリックすると、悪意のあるマクロが動作し、ウイルスに感染させられてしまう。



※IPAホームページから引用

②「業務上開封してしまいそうな本文」の事例

	事例1	事例2
受信日時	2019/11/28 15時頃	2019/11/29 8時頃
本文	お世話になっております。  添付いたしますのでご確認ください。 内容に齟齬がございませんでしたら、 黒線太枠内をご記入いただき、社刊を捺印の上下記、住所までご郵送くださいませ。  よろしく申し上げます。	いつもお世話になります。  11月分の請求書を送信致します。  色々とお手数をおかけしますが、宜しく申し上げます。
添付ファイル名	請求書の件です。【文字列】.doc	請求書送付のお願い【文字列】.doc

※IPAホームページから引用