サイバー防犯通信

№ 58

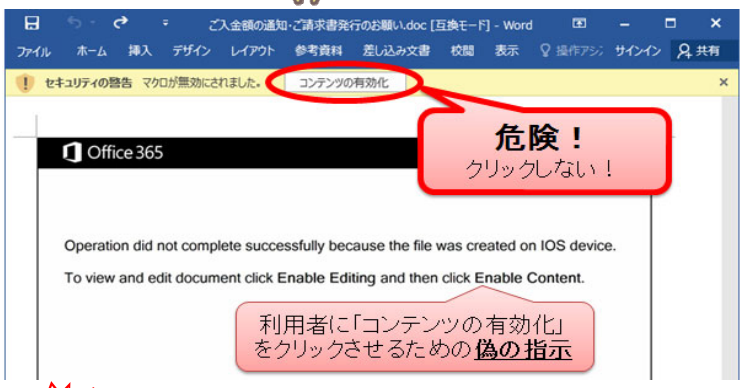
令和２年10月22日
兵庫県警察本部
サイバー犯罪対策課

～安易に開かないで！～
メールの添付ファイルには十分注意を

「Emotet」（エモテット）と呼ばれるウイルスへの感染を狙う攻撃メールが、国内の企業や法人等へ広く着信しています。メールの内容等の一部が、攻撃メールに流用され、「正規のメールへの返信を装う」内容となっている場合や、業務上開封してしまいそうな巧妙な文面となっている場合があり、注意が必要です。

右の図は攻撃メールのサンプルです。
正規メールと間違えてしまう様な内容で騙し、不正なコード（プログラム）が組み込まれた文書ファイルを添付して送信してきます。
添付される文書ファイルが「ZIPファイル」形式で添付して送信されるケースがみられます。

最近では、Microsoft社製「office」製品の更新を騙るものも認められます。
メール添付の文書ファイルは開かない様に注意してください。



もしメールを展開し、文書ファイルを開いても、左の図に示す「コンテンツの有効化」をクリックしなければ、マルウエアへの感染を防げます！！
「コンテンツの有効化」は正規メールと確認出来るまで絶対にクリックしないでください。

Check! ～～防犯ポイント～～

■ 被害に遭わないために、下記の点に留意してください。
- 「コンテンツの有効化」をクリックしない。
- 攻撃メールは正規のメールを装うケースが多いため、不審に感じた場合は発信元に確認する。
- 法人等の組織が攻撃対象になることが多いため、組織内で情報共有を行い対応策を検討しておく。
- 万が一「コンテンツの有効化」をクリックしてしまった場合、直ちにネットワークから切断し、組織内のセキュリティ担当に連絡する。

※図の出典・記事引用元
ＩＰＡ（独立行政法人情報処理推進機構）「Emotet」と呼ばれるウイルスへの感染を狙うメールについて