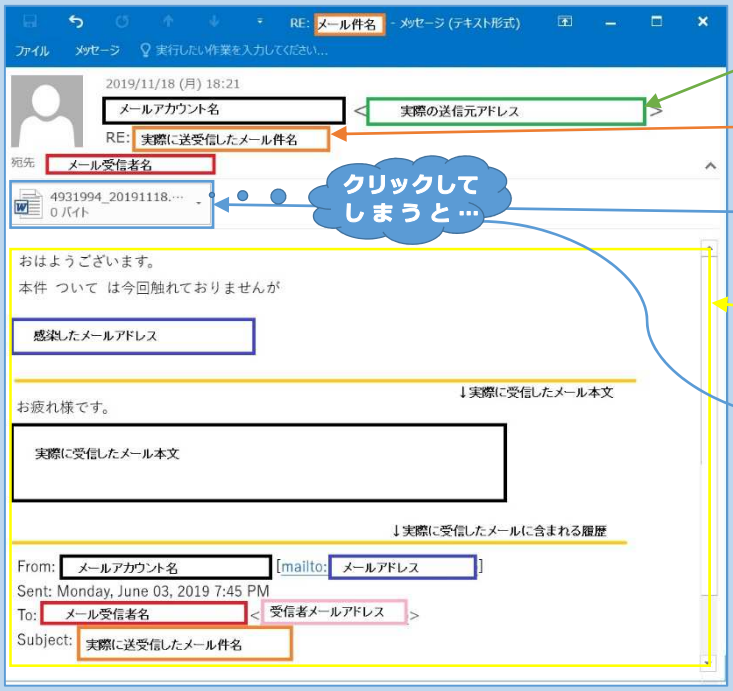
Word文書が添付されたメールに注意！

過去にやり取りした組織や人物になりすましたメールに添付されているWord文書ファイルを実行することで感染する**マルウェア「Emotet（エモテット）」**による被害が増加しています。感染すると端末に保存されたメール本文やアドレス帳、WEBブラウザに保存された認証情報等が流出するほか、ネットワークに接続されている他の端末にも感染が広がり、さらに感染した端末のメールアドレスを使って、アドレス帳やメール送受信記録に基づいて作り出された新たな「なりすましメール」が関係者に宛てて大量に送信され、被害が拡大します。

Emotet感染を狙ったメールの特徴



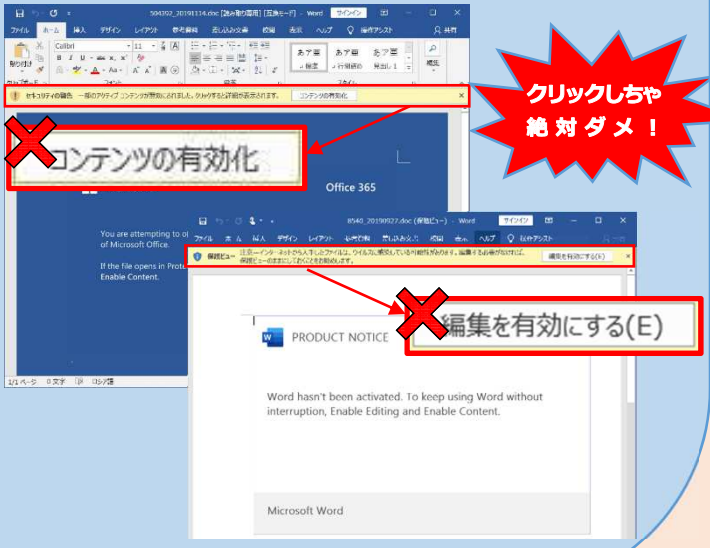
過去にメールで実際にやり取りした実在する組織や人物のメールアドレスで送信されます。

実際にやり取りしたメール件名が使われたり、返信を示す「RE:～」がつくケースもあります。

添付されたWord文書ファイルを実行するとマルウェア「Emotet」に感染してしまいます。

過去にやり取りした内容に基づいて本文が日本語で記載されているため、一見、不審だと感じない内容となっています。

「コンテンツの有効化」「編集を有効にする」クリックしてしまうとマルウェアに感染!!



クリックしちゃ 絶対ダメ！

感染被害防止対策として

- Word文書が添付された送信元への問合せ
- OS、アプリケーションのアップデート
- ウイルス対策ソフトの導入とパッチの更新
- Wordマクロの自動実行の無効化
- 組織内への注意喚起　など

参考：JPCERTコーディネーションセンター
URL　https://www.jpcert.or.jp/at/2019/at190044.html

最新セキュリティ情報はこちらから

2019年12月20日 発行

鳥取県警察本部
総合相談電話　☎　#9110
サイバー犯罪対策課　警部補　福井 貴
☎　0857-23-0110　（内線　3424）
URL　https://www.pref.tottori.lg.jp/police/