

現在、津田建築、津田建築社員の「なりすましメールの報告が相次いでおります。

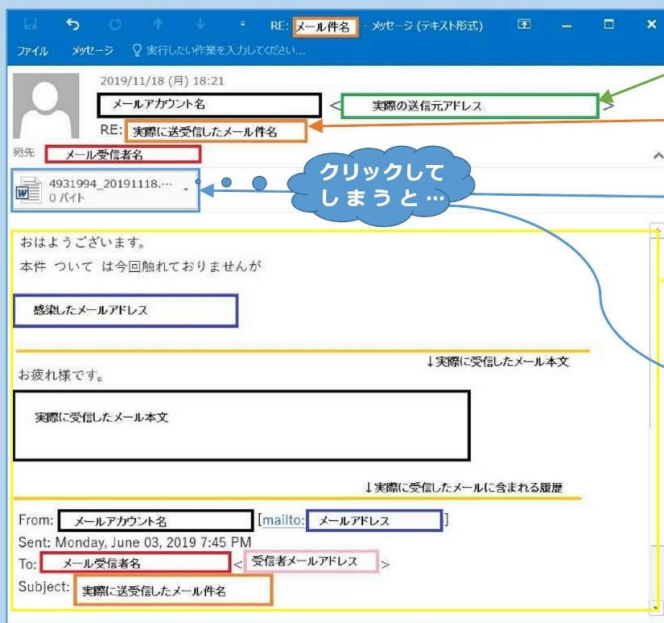
送信元の名前が津田建築もしくは津田建築社員名になっており、本来のアドレスとは異なるアドレスになっています。

協力業者様におかれましては、不明なメール或いは疑わしいメールにつきましては決して添付データを開封せずにメールを削除して頂きます様お願いします。

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



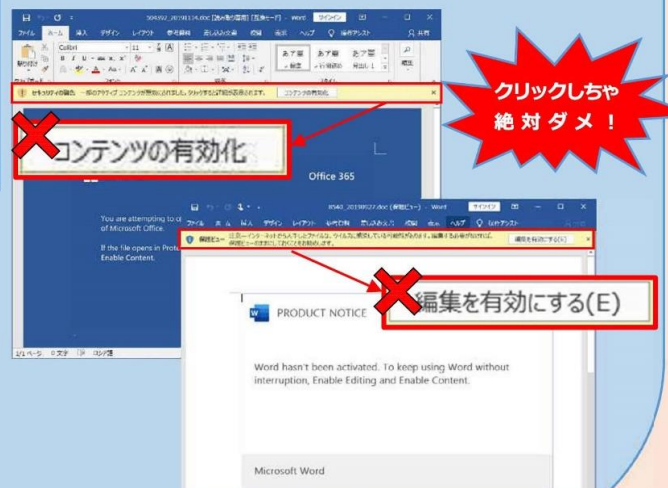
過去にメールで実際にやり取りした実在する組織や人物のメールアドレスで送信されます。

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」をクリックしてしまうとマルウェアに感染!!



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>