ご注意ください！！

Ｅｍｏｔｅｔ（エモテット）と呼ばれるウイルスへの感染を狙うメールについて

「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、国内で多く着信しています。
非常に感染力・拡散力が強いマルウェアの一種であり、また、自分の送ったメールの返信を装うなど、
気付きにくく悪質で危険なウイルスです。

Ｅｍｏｔｅｔに感染すると・・・

- 感染したＰＣの様々な電子メールのパスワードとアカウント関連情報・メッセージの送信者とそのメールアドレスを搾取されます。
- 感染したＰＣの現在ログオンしているシステムに保存されているすべてのネットワークパスワードを搾取されます。

**感染した結果、社内だけに限らず、取引先等へ
自分のメールアドレスを使い、次の攻撃が行われます。
つまり、自分と登録のあるアドレスのＰＣすべてのデータが
奪われるといっても過言ではありません。**

主な対策方法

裏面に感染例を記載しております

- 身に覚えのないメールの添付ファイルは開かない。
  メール本文中のＵＲＬリンクはクリックしない。
- 自分が送信したメールへ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は開かない。
- ＯＳやアプリケーション、セキュリティソフトを常に最新の状態にする。
- メールに添付されたＷｏｒｄ文書やＥｘｃｅｌファイルを開いた時に、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない。
- メールや文書ファイルの閲覧中、身に覚えのない警告ウインドウが表示された際、その警告の意味が分からない場合は、捜査を中断する。

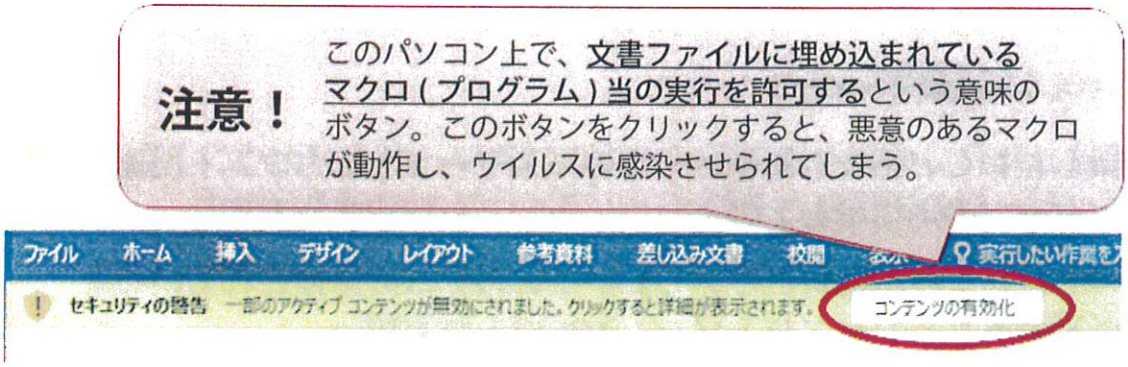
※万が一、添付ファイルを開いてしまったり、
ＵＲＬリンクをクリックしたことで
パソコンが不可解な挙動を始めた場合は、
すぐにＬＡＮケーブルを抜いて、当社へご一報ください。

株式会社 ティ・エス・エス
〒001-0034
札幌市北区北３４条西５丁目２－１５　ニュートーアビル３Ｆ
TEL：011-727-3450　FAX：011-727-3483
URL：https://www.tss-web.co.jp/

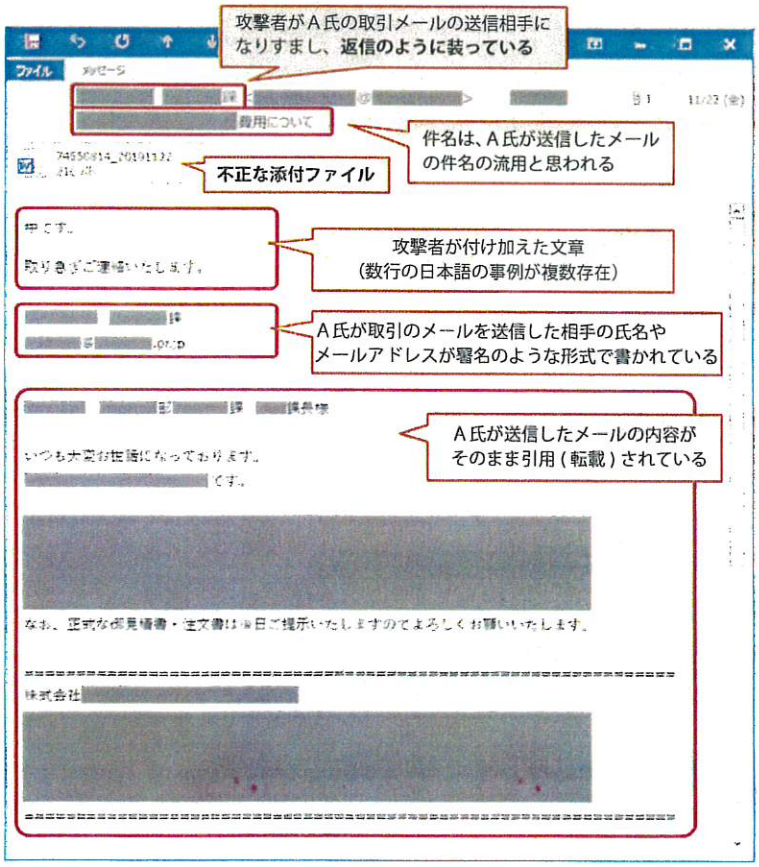
自分のメールアドレスや、過去にメールのやり取りをしたことのある実在の相手の氏名・メールアドレス・メールの内容等が流用され、あたかもその相手から返信メールであるかのように見える手口です。

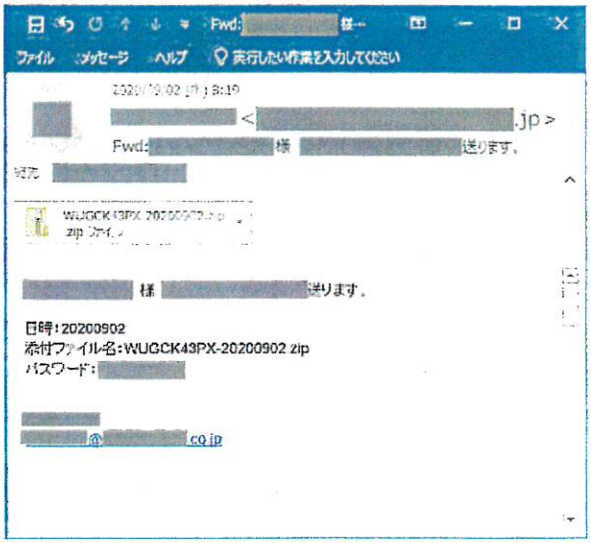
知っているメールアドレスから、「請求書送付のお知らせ」「ご請求明細」といった内容で送信されていたり、以前にやり取りをしていたメール内容を丸々送信されたりと、「なりすましメール」や「ウィルス添付メール」とは違い、非常に分かりにくいという特徴があります。

2020年9月には、トレンドマイクロを騙ったり、をパスワード付きＺＩＰファイルを使った攻撃も急増しており、悪質化が進んでいるため、対策が非常に難しくなっております。



添付ファイルによるＥｍｏｔｅｔ感染を狙うメール例





最新情報はＩＰＡ（情報処理推進機構）のＨＰでご確認ください。
https://www.ipa.go.jp/security/announce/20191202.html

株式会社 ティ・エス・エス
〒001-0034
札幌市北区北３４条西５丁目２－１５　ニュートーアビル３Ｆ
TEL：011-727-3450　FAX：011-727-3483
URL：https://www.tss-web.co.jp/