



ウイルスメール「エモテット」に注意！

「Emotet（エモテット）」と呼ばれるコンピュータウイルスを使ったメール攻撃が再び発生しています。

感染すると、パソコンを乗っ取られるだけでなく、メール情報が流出して、関係先にウイルスメールがばらまかれてしまいます。

【ウイルスメールの例】

送信者名は、取引先等になっているが、送信者メールアドレスが異なる

よく使われる件名、返信を装う

ワードまたはエクセルが添付されている！

よく使われる文面

差出人： 株式会社●●商事 <marumaru@xxxx.or.jp>
送信日時： 2020年9月1日 17:35
件名： Re:第●回定期会合の開催について
添付ファイル： 20200901_第●回定期会合次第.doc

関係会社各位
お世話になっております。
標記の件、例年とおりに開催することとなりましたので、式次第を送付します。
業務ご多忙中と存じますが、ご出席のほどよろしくお願いいたします。

株式会社●●商事
佐賀太郎

ちょっと待った！！



この表示が出たら要注意！



！ セキュリティの警告 マクロが無効にされました。

コンテンツの有効化

ウイルスに感染するので絶対にクリックしないでください！

～ 被害に遭わないために気をつけること ～

- ・ウイルス対策ソフトを導入し、最新の状態に更新して使用する！
- ・返信メールに見えても安易に添付ファイルやURLをクリックしない！
- ・添付ファイルの「コンテンツの有効化」をクリックしない！

参考：独立行政法人情報処理推進機構（IPA）
エモテットと呼ばれるウイルス 右のQRコードをご確認ください。

