



ウイルスメール「エモテット」活動再開

「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、情報を盗まれるだけでなく、ランサムウェア等のウイルスにも感染するおそれがあります。

【ウイルスメールの例】

メールソフトに登録されている取引先等の知り合いを装う

よく使われる件名、返信を装う

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： 200901_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

【添付ファイルは様々】



ZIPファイル



ショートカット



Wordファイル



Excelファイル



PDFファイル

セキュリティの警告 マクロが無効にされました。

この表示が出たら要注意！
クリックせず送り主に確認を！



～ 被害に遭わないための注意～

- ・ 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！
- ・ 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！
- ・ ショートカットファイルやURLリンクをクリックしない！

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コードを御確認ください。

