



あなたの情報が狙われています！

～攻撃の手口を知らなければ情報を奪われます～

Emotet（エモテット）と呼ばれるウイルス

受信したメールの添付ファイル（WordやExcelなど）を開き「コンテンツの有効化」をクリックすることでウイルスに感染します。

感染すれば、情報を盗まれるだけでなく、メールのアドレス帳が悪用され、関係先にウイルスメールがばらまかれて被害が広がります。

差出人には、過去にメールのやりとりをしたことのある相手の名前が使われることもあり、メールの内容も巧妙な文面になっています。

知人、取引先等を装っている	
差出人：	株式会社●●商事
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	

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

ウイルスに感染しないために

- 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
- 全ての受信メールに注意を払う！（安易に添付ファイルを開かない）
- 添付ファイルの「コンテンツの有効化」をクリックしない（有効化することでウイルスが作動します）
- 送信先にメールの送信の有無を直接確認する

参考：IPA情報処理推進機構（Emotetと呼ばれるウイルスへの感染を狙うメールについて）

< <https://www.ipa.go.jp/security/announce/20191202.html> >