サイバー防犯通信 No.38

平成30年5月15日
兵庫県警察本部
サイバー犯罪対策課

不正送金等の犯罪被害につながるメールに注意

現在、インターネットバンキングマルウェアの感染等を目的としたメールが大量に送信されています。

これらのメールの**添付ファイルを開いたり、本文中のリンクをクリックする**と、マルウェアの感染等につながり、インターネットバンキングの不正送金などの犯罪被害に遭う可能性があります。

例①【件名】注文内容のご確認（自動配信メール）

ご注文ありがとうございます

〇〇〇（サイト名）　**買い物かご　購入履歴　ヘルプ**

この度は〇〇ショップをご利用いただきまして、誠にありがとうございます。

本メールは、お客様のご注文を受け付けた時点で送信される自動配信メールです。ショップからの確認の連絡、または商品の発送をもってご購入についての契約が成立します。

ご注文内容
注文番号　20000-00×××-××××
注文日時　2018-05-00

お問い合わせ先
〇〇ショップ　✆052-600-××××
問い合わせフォームから連絡

〈！注意！〉

「買い物かご」「購入履歴」等の**リンクは不審なファイルへのリンクです！**

例②【件名】Re:注文書、請書及び請求書のご送付

いつもお世話になっております。
下記、注文請書・請求書をお送り致します。
ご査収の程、どうぞ宜しくお願い申し上げます。

【指定請求書】
請求書必着日までに原本を郵送にてご返信をお願い致します。

添付ファイル 00000.xls

〈！注意！〉

添付ファイルの確認を促すような文面ですが、添付ファイルは、**文書等を装ったマルウェアです！**

添付ファイルやリンクを安易にクリックしてはダメ！！

被害に遭わないために

〇ウイルス対策ソフトを利用するとともに更新を怠らないようにしましょう。
〇ＯＳやソフトウェアは最新の状態に保ちましょう。
〇メールの本文中のリンクや添付ファイルを安易に開かないようにしましょう。
〇メールソフトの迷惑メールフィルターを活用しましょう。
〇メールの送信元が実在する組織でも安易に開かず、電話等で確認しましょう。

※　このようなメールの注意喚起情報は、一般財団法人日本サイバー犯罪対策センター(JC3)のウェブサイトや、サイバー防犯通信に掲載中です。