サイバーセキュリティの置き薬　2020年　第２号

新型コロナウイルスに乗じた犯罪に注意を

JC3（日本サイバー犯罪対策センター）において、新型コロナウイルスに乗じた犯罪手口を把握しました。社会情勢に乗じた利用者の心理につけ込んだ手口ですので、十分に注意してください。

1　フィッシングに関する手口

運送系企業を装ったフィッシング手口により不正アプリがインストールされた感染端末を踏み台として、第三者にマスクを無料配付する旨のフィッシングメールをばらまき、運送系企業を騙ったフィッシングサイトに誘導する手口です。

2　悪質なショッピングサイトに関する手口

マスク販売の偽サイトであり、代金を支払っても商品が届かなかったり、会員登録時の個人情報やクレジットカード情報等を盗み取られる可能性がある手口です。

<ご注意ください！>

上記以外にも、様々なフィッシングメールが無差別かつ大量に送りつけられ、アプリのインストールや動画のダウンロードを要求するものがあります。

こうした手口ではアプリや動画を装って、知らない間にウイルスがインストールされ、スマートフォン等から個人情報（ネットバンク、クレジットカード情報等）が盗み取られ、金銭の被害にあう可能性がありますので、**「不審なメールは開かない・不審なファイルはインストールしない」**ようにしてください。

【参考サイト】
日本サイバー犯罪対策センター（ＪＣ３）
https://www.www.jc3.or.jp/