FUKUOKA POLICE 70th ANNIVERSARY

F-CSNET通信かわら版

令和７年3月号

関係者からのメール？　それ本当ですか？

もしかしたら、標的型メール攻撃かも！

標的型メール攻撃の特徴

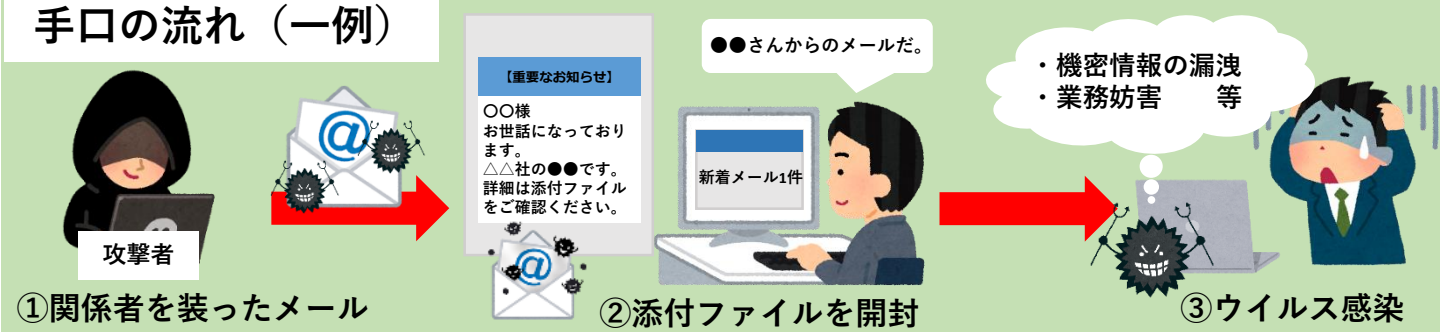
攻撃者はメール添付ファイルや本文に記載のリンク先にウイルスを仕込み、そのファイルを開封させたり、リンクにアクセスさせたりすることで、パソコンをウイルスに感染させます。

メール本文や件名、添付ファイル名は実在する組織名が使用される場合があります。

（例）　担当者様

お世話になっております。●●社の▲▲と申します。
現在ご使用中のPCに極めて深刻な脆弱性が発見されました。下記リンクを確認し、各自至急対応をお願いします。
https://www.●●●.jp:php?docid=●●●

手口の流れ（一例）



①関係者を装ったメール　②添付ファイルを開封　③ウイルス感染

不審なメールへの対応

〇　添付ファイルを開かない

安易に添付ファイルを開くと悪意のあるプラグラムが起動し、ウイルスに感染する恐れがある。

〇　リンクをクリックしない

不審なメールにはリンクをクリックさせる文面が多い。
リンクをクリックすると偽のサイトに誘導される危険性がある。

〇　メールの送信事実を確認する

送信者に対してメールの送信事実があるのか電話等で直接確認する。

◆　福岡県警察本部サイバー犯罪対策課では、最新のサイバー犯罪の手口や対策等を、ホームページやＸ（旧Twitter）に掲載していますのでぜひご覧ください。
◆　万一、被害に遭われた場合は、管轄警察署宛てご一報ください。

【X】　【HP】