サイバーセキュリティ通信 Vol.5

令和２年７月
【長崎県サイバーセキュリティに関する相互協力協定機関】

サイバァちゃん

偽サイトに御注意を！

インターネット上において、警察庁を騙るフィッシングが確認されています。
手口としては、リンクをクリックすると、認証を促すポップアップが表示され、警察庁の偽ウェブサイトが表示された後、自動的に銀行のフィッシングサイトへ誘導されます。
今後、警察庁に限らず長崎県警察などの官公庁のサイトを装った偽サイトが作成される可能性がありますので、**見慣れないトップレベルドメイン（ＵＲＬの末尾）ではないか、紛らわしいＵＲＬではないか、など、被害に遭わないように、ＵＲＬの確認**をお願いします。

URLの作りとトップレベルドメインについて

一般的なURL→ 通信方法 https :// ホスト名 www ドメイン名 .npa .go .jp ディレクトリ名 /cyber ファイル名 /index.html

ドメイン名→ 第３レベルドメイン npa　第２レベルドメイン go　トップレベルドメイン jp（ドメイン名を管理している国や組織を示す）

※　「jp」のトップレベルドメインについては株式会社日本レジストリサービス（通称ＪＰＲＳ）が管理しています。

ＵＲＬとは、「Uniform Resource Locator」の略で、インターネット上で、Webページの場所を特定するための文字列のことです。
「npa.go.jp」の部分は、「ドメイン名」と呼ばれ、組織等を表しており、例の場合では、「日本（jp）の政府機関(go)の警察庁(npa)」を意味しています。

被害に遭わないために、どうすればいいの？

○　被害に遭わないために知っておきたい3つのポイント
□　リンクからサイトに接続する際は、ＵＲＬを必ず確認しましょう
□　見慣れないトップレベルドメイン（.ml・.cf・.tk等）の場合は、安易にクリックせずに、検索等により本物のサイトのＵＲＬを確認しましょう
□　不審なサイトを開いてしまった場合は、そのページの何かをクリックしたりせずに、すぐにアクセスを中断しましょう

例えば、官公庁のサイトでＵＲＬの末尾が「.jp」でない場合は、特に注意が必要です！

長崎県警察本部サイバー犯罪対策課　095-820-0110（3451・3452）　ﾒｰﾙｱﾄﾞﾚｽ e103108@police.pref.nagasaki.jp