# 最近のサイバー犯罪の手口について

令和２年２月５日（水）

市民の皆様の多くは、インターネットを利用されていると思います。

インターネットは非常に便利ですが、これを悪用した犯罪の手口は、日々、悪質化、巧妙化しています。

また、**２月１日から３月１８日**までの間は、政府が定めた**「サイバーセキュリティ月間」**でもありますので、本日は、市民の皆様に注意してほしい、最近のサイバー犯罪の、**２つの手口**について、説明させていただきたいと思います。

## １　フィッシング、スミッシングについて

先ず、１つ目の手口は、フィッシング、スミッシングによるものです。

**フィッシング**とは、**被害者のパソコンなどに、偽の電子メールを送りつけ、フィッシングサイトに誘導して、個人情報を窃取する行為**です。

**スミッシング**とは、フィッシングの一種で、**携帯電話機のショートメッセージサービスを利用したフィッシング**のことです。

フィッシングサイトに誘導されると、アカウントのID、パスワード、クレジットカードの情報等の入力を求められ、その後、知らないうちに、不正アクセスや商品の不正購入の被害に遭ってしまいます。

例としては、金融機関をかたり、「セキュリティ強化」などの名目でショートメッセージなどを送り付け、偽サイトへ誘導した後、「口座番号」等を入力させる手口があります。

また、宅配業者を装い、不在通知の偽メッセージを送って、フィッシングサイトへ誘導し、利用者に不正アプリをインストールさせ、ＩＤとパスワードを入力させて窃取するものもあります。

## ２　フィッシング、スミッシングの被害防止対策について

フィッシングや、スミッシングの被害に遭わないためには、次の３点に注意してください。

１点目は、**不審なｼｮｰﾄﾒｯｾｰｼﾞは無視し、ｼｮｰﾄﾒｯｾｰｼﾞに記載のＵＲＬを絶対タップしない**でください。

２点目は、また、**不審なアプリをインストールしない**でください。

３点目は、**ｼｮｰﾄﾒｯｾｰｼﾞに記載されているリンクからアクセスした先のサイトでは、ＩＤやパスワードなどを入力しない**でください。

万が一被害に遭った場合には、先ず、スマートフォンを機内モードに設定してください。

次に、不審アプリのアンインストール、スマートフォンの初期化、アカウントのパスワード変更などを行ってください。

## ３　Emotet（エモテット）について

２つ目の手口は、Emotet（エモテット）という、インターネットウイルスによるものです。

エモテットに感染されたら、情報を窃取されるほか、他のウイルスにも感染させられます。

エモテットへの感染を狙う攻撃メールには、攻撃メールの受信者が、『過去にメールのやり取りをしたことのある相手の氏名やメールアドレス、メール内容の一部』を流用されるなど、『正規のメールへの返信を装う手口』が使われ、『業務上開封してしまいそうな巧妙な文面』となっているものがあります。

感染経路は、主にメールに添付されたWord形式のファイルを実行し、「コンテンツの有効化」を実行することでエモテットに感染してしまいます。

## ４ Emotet(エモテット)の被害防止対策について

エモテット被害の防止対策として、次の３点に注意してください。

１点目は、身に覚えのないメールだけでなく、自分が送信したメールへの『返信』に見えるメールであっても、不自然な点があれば、添付ファイルは開かないでください。

２点目は、メールに添付されたＷｏｒｄ文書やＥｘｃｅｌファイルを開いた時に、『マクロやセキュリティに関する警告』が表示された場合、『コンテンツの有効化』のボタンは、クリックしないでください。

３点目は、ＯＳやアプリケーション、セキュリティソフトは、常に、最新の状態にしておいてください。

## ５ 最後に

**市民の皆様には、最近のサイバー犯罪の手口について知ってもらい、被害に遭わないようにしていただきたいと思います。**

**愛媛県警察本部のＨＰにも、注意事項を掲載していますので、ご覧になっていただきたいと思います。**

**よろしくお願いします。**