CyberNews
サイバー犯罪対策課
広　報　用　資　料
令 和 元 年　第 ５ 号
佐賀県警察本部サイバー犯罪対策課

携帯電話事業者を装ったフィッシングメールに注意！

携帯電話事業者を装った偽メール（ＳＭＳ）で個人情報が盗まれる等の相談が増えています。

特に最近はメール本文にＵＲＬ（アドレス）が記載されたものが多く、アカウントのＩＤやパスワードを入力したためにキャリア決済（携帯電話料金での支払い）を不正に使用される被害も発生しています。

偽メッセージを見破るポイント（例）

差出人　XXXXXXXX　〉

お客様のアカウントに異常ログインの可能性があります。
下記ＵＲＬで確認をお願いします。

http:// www.●●●.com

URL が https で始まっていない。など。

注意！！

・差出人は、正規の携帯電話会社からのメッセージと同じ画面（フォルダ）に表示される場合がある。

・メッセージの内容は、「お客様がご利用のキャリア決済が不正利用の可能性があります」「ウェブページで二段階認証をお願いします」など。

被害に遭わないために

●　絶対にＵＲＬを開かないこと

メールやＳＭＳに記載されているＵＲＬが、正規のサイトであるか、公式ホームページなどで確認する。

万一、偽サイトでＩＤやパスワードを入力してしまった場合は、直ちに契約している携帯電話事業者に連絡する。

●　２段階認証の設定

ＩＤ、パスワード入力の他にセキュリティコードの入力を追加するなど、第三者が不正アクセスをすることを防止する設定を導入する。

●　迷惑メールフィルターの設定を導入する

契約している携帯電話事業者の公式サイトを確認し、例えばＵＲＬ付メールを拒否するなど迷惑メールフィルターの設定を導入する。