アカウントの乗っ取りに気をつけて！

近年、SNSや動画配信サービス、オンラインゲームなどのアカウントの乗っ取り被害が増加しています。突然、自分のアカウントが使用できなくなった、身に覚えのない投稿がされている、高額な請求が届いたといったことが起こりえます。こういった被害に遭わないためにどのような対策ができるか紹介します。

実際に起こったトラブルの事例

推しの名前をパスワードに使っていたら

Aさんは、推しのアイドル「Ren」の名前を使って「renlove2026」というパスワードを設定した。SNSで「Renが大好き！」と頻繁に投稿していたため、悪意のあるユーザーが「renlove2026」などを試したところ、見事にヒット。アカウントを乗っ取られた結果、Aさんの友達に向けて悪口のメッセージが勝手に送られ、トラブルに発展してしまった。

「ちょっと貸して」が大トラブルに

Bさんは友人から「その動画アプリのアカウント貸して！」と頼まれて、ついOKしてしまった。最初は一緒にアニメを観るだけだったけど、後日、自分のスマホに高額な請求が届いた。調べてみたら、友人が勝手に有料の映画をいくつも購入していたことがわかった。

被害に遭わないために

・IDやパスワードなどのアカウント情報を他人に教えないようにする

信頼できる人であってもアカウント情報を教えないようにしましょう。

・不審なメールやURLを開かない

身に覚えのないものや少しでも怪しいと思ったメールやURLは開かないようにしましょう。
偽サイトへの誘導やウイルス感染によりアカウント乗っ取りの原因になります。

・多要素認証を活用しましょう

顔認証や指紋認証などの生体認証、SMSやメールを使用した二段階認証を行うことも安全性を高めることに有効です。

・パスワードの設定を見直す

推測されづらいパスワードを使用しましょう。生年月日などの推測されやすいパスワードはアカウント乗っ取りの被害に遭う可能性が高まります。
パスワードを定期的に変更することも安全性を高めることに有効です。

被害に遭ってしまったときは

年々、アカウントの乗っ取り手口は巧妙になっています。もし被害に気づいたら、まずはパスワードを変更し、保護者に相談しましょう。そのうえで、ログイン履歴や不審な操作の記録を残し、警察やサイバー犯罪の窓口に相談することが大切です。