

アカウントの乗っ取りについて

SNSや無料通話アプリなどのサービスで、アカウント(※)を乗っ取られる被害が相次いでいます。アカウントを乗っ取られると、自分になりすまされ、アカウントを悪用されてしまいます。今回は、アカウントの乗っ取りについてお話ししたいと思います。

※アカウントとは……コンピューターや、インターネット上のサービスを利用するための権利のこと。通常、IDとパスワードがセットになっている。

アカウントの乗っ取り被害にあう原因について

アカウントの乗っ取り被害にあう主な原因が、パスワードの漏洩です。パスワードの漏洩には、以下のようなケースがあります。

- ・名前や生年月日などのわかりやすいパスワードを設定していて、推測されてしまう
- ・スマートフォンなどのインターネット機器がウイルス感染し、パスワードが流出してしまう
- ・詐欺サイトに誘導され、自身でパスワードを入力してしまう



同じパスワードを複数のサービスで使っていると、パスワードが漏洩した際、複数のサービスで乗っ取りの被害にあう可能性があります。

また、SNSのアプリ連携が原因となることもあります。アプリ連携とは、本来アカウントの所有者しか行えない操作の権限を、外部のアプリに与える機能です。アカウントの乗っ取り犯は、SNS上の投稿や広告、それからダイレクトメッセージなどを使って、SNSの利用者に不正なアプリへの連携を促しており、利用者がうっかり連携を許可してしまうと、SNSの操作権限を乗っ取り犯に与えてしまうこととなります。

アカウントを乗っ取られると、こんな被害が……

SNSや無料通話アプリなどのアカウントを乗っ取られると、自分になりすまされ、嫌がらせ目的で不適切な投稿をされることがあります。また、SNS上で友だちとなっている利用者に対して、外部サービスへの登録や商品購入を促すメッセージを送られてしまうこともあります。

アカウントの乗っ取り被害は、自分だけでなく友だちにまで及んでしまう可能性があるのです。



SNSや無料通話アプリなどのアカウントの乗っ取り被害を防ぐために、以下のような点に気をつけるよう、子どもたちに指導していくことが必要です。

- ・名前や生年月日、連番や連続の英数字（11111、98765、abcdefなど）のような推測されやすいパスワードは使わない
- ・パスワードを使いまわさない（サービスごとに違うパスワードを設定する）
- ・提供元不明のアプリや、何のためにその権限を必要とするかわからないアプリに対しては、アプリ連携をしない
- ・SNS上の投稿や広告、ダイレクトメッセージ内のURLリンクを不用意に開かない