# ＳＮＳ利用上の注意点

近年、短い文章を投稿したり、友人同士がメッセージや写真などを共有してコミュニケーション取ったりする、いわゆるソーシャルネットワーキングサービス(SNS)が普及してきました。しかし、安易な書込みがトラブルに発展したり、知り合い同士の空間であるという安心感を利用して詐欺やウイルスの配布を行う事例も急増しています。

いくつか想定される脅威と対策について紹介します。

## 偽アカウント、架空アカウントの作成

SNS には本人確認が徹底していないサービスもあり、実在の人物・組織の名前を使った偽のアカウントや、架空のアカウントで投稿されているケースもあります。偽のアカウントや架空のアカウントを悪用して、不正リンクの投稿などが行われる事例もありますので、SNS で関わるアカウントの相手が本物であるかどうかは、慎重に確認する必要があります。

SNS サービスによっては、本人確認が行われた上で公式アカウントとして登録されているものもあります。特に公的機関や企業、著名人などの情報を購読する場合には、まず公式アカウントが存在するかを、それぞれの機関のホームページなどで確認してみるとよいでしょう。直接の知人や公式アカウント以外のアカウントで、本人確認ができない場合には、安易にフォロー（購読）したり、友達になったりしないようにしましょう。

## 短縮 URL の悪用

短縮 URL は、SNS で文字数の制約上 URL を短縮して表示する外部のサービスです。本来の URL よりも文字列が短くなり、見た目にも扱いやすくなります。しかし、一見しただけではどのようなサイトにリンクされているかわからないことから、この機能を悪用してフィッシング詐欺やワンクリック詐欺などの悪性ホームページに誘導する手口が確認されていますので、短縮 URL をクリックする際には注意が必要です。心配な場合、短縮 URL を元の URL 表示に戻して確認することのできる Web サービスも提供されています。

## スパムアプリケーションに注意しましょう

SNS のアプリケーションの中には、インストールの際に、連絡先情報へアクセスする許可を求めてくるものがあります。このようなアプリケーションの中には、個人の連絡先情報を収集して、収集したメールアドレスに迷惑メールなどを送りつけることなどを目的としているものもあります。連絡先情報へアクセスするアプリケーションで、作成者の身元やその利用目的がよくわからないものは、使用を避けるようにした方が良いでしょう。

## プライバシー情報の書き込みに注意しましょう

友人間のコミュニケーションを目的として SNS を利用しているであっても、プライバシー設定が不十分であったり、友人から引用されることなどにより、書きこんだ情報が思わぬ形で拡散する危険性もあります。インターネット上に情報が公開されていることに変わりはないということを念頭に置いて、書き込む内容には十分注意をしながら利用することが大切です。

## SNS への写真掲載による意図しない位置情報の流出に注意しましょう

最近の GPS 機能のついたスマートフォンやデジタルカメラで撮影した写真には、設定によっては、目に見えない形で、撮影日時、撮影した場所の位置情報（GPS 情報）、カメラの機種名など、さまざまな情報が含まれている場合があります。SNS に、こうした位置情報付きの写真をよく確認せずに掲載してしまうと、自分の自宅や居場所が他人に特定されてしまう危険性があり、迷惑行為やストーカー被害などの犯罪の被害に遭う可能性もあるため、十分注意が必要です。

写真にどのような情報が含まれているか調べる方法はいくつかありますが、これらを表示するための専用のアプリケーションを利用すると、事前に確認ができます。写真に含まれている情報を編集・削除できるアプリケーションもあります。位置情報もプライバシー情報であるということを十分理解して、むやみに位置情報をつけて写真を投稿しないように心がけましょう。

## SNS の怪しい投稿のリンクに注意しましょう

SNS は誰でも投稿することができることから、怪しいリンク（ワンクリック詐欺、フィッシング詐欺など）に誘導される危険性があります。投稿した人が実在の信頼できる人であったとしても、他の人が投稿した内容をそのまま再投稿する場合もありますので、元々の情報の発信元の信頼性を意識することが大切です。