SNS 利用時の脅威と対策

－企業・組織における情報セキュリティ対策－

出典

総務省　安心してインターネットを使うために

国民のための情報セキュリティサイト

※アンケート（巻末参照）の提出をもって、受講終了となります。

株式会社アクト・テクニカルサポート

SNS とは、ソーシャルネットワーキングサービス（Social Networking Service）の略で、登録された利用者同士が交流できる Web サイトの会員制サービスのことです。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するコミュニケーション手段として SNS が普及してきました。
友人同士や、同じ趣味を持つ人同士が集まったり、近隣地域の住民が集まったりと、ある程度閉ざされた世界にすることで、密接な利用者間のコミュニケーションを可能にしています。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。

ここでは SNS 利用時に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。

■発信内容は慎重に

SNS などのツールは、日常生活の中で、リアルタイムでの個人の思いなどを投稿できる点が大きな魅力です。しかし、その一方で、個人の何気ない発言でも、インターネット上の発言やふるまいは、多くの人の目に触れる可能性があり、場合によっては、現実世界に大きな影響を与えることがあります。

例えば、ある職員が勤務時間中にした SNS への投稿が、本来は秘密にするべき職務の内容を外部に漏らしてしまう結果となり、インターネット上で職員自身に非難が集中したり、その組織全体の問題として取り上げられる事例が発生しています。このような場合、しばしば、インターネット上のその問題に関心を持つ人の間で責任追及活動が行われ、その過程で、非難の対象となった個人の過剰な個人情報の特定・暴露や、誹謗中傷などの大量の書き込み（いわゆる「炎上」）などの行為が行われます。そして、インターネット上でこのような現象が発生した場合には、新聞やテレビなどのマスメディアで報道されることも珍しくありません。

こういった危険性を回避するためには、まずは自分のインターネット上での発信内容が、本来秘密にすべき事項を含んでいないか、現実世界でも非難を浴びるような内容でないかなど、毎回立ち止まって考える慎重さが必要です。

さらには、こうした個人の特定が行われるのは、SNS 上の情報発信だけではありません。悪ふざけのつもりで投稿された動画から、投稿者の個人情報の特定が行われ、現実世界での謝罪に至った事例も発生しています。今やインターネットは匿名の空間ではなく、インターネット上の行動は特定されてしまうものだといういことを自覚することが必要です。

■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。

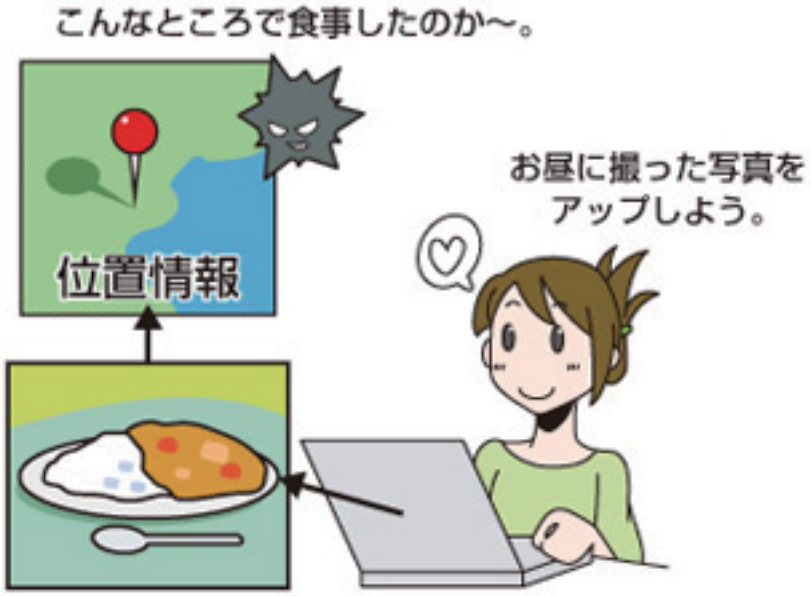
■プライバシー情報の書き込みに注意しましょう

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。

アンケートの提出をもって受講完了となります。
必ずご提出をお願いいたします。
下記のボタンをクリック、または QR コードを読み取り、アンケートにお答えください。

アンケートに回答する