

SNS などのネットサービスの発展や技術の進歩は、人々の生活を便利にする反面、新たなトラブルも生み出しています。インターネットを利用していけば誰もが巻き込まれる恐れのある問題について、どのようなものがあるのか、その危険性を学びましょう。

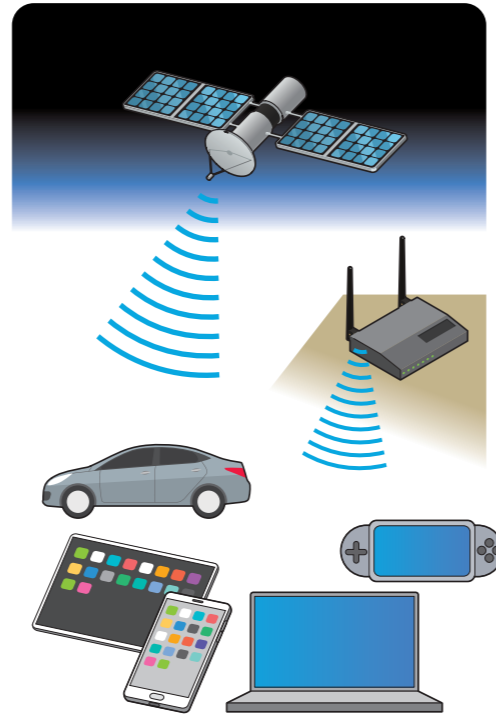
さまざまなものから得られる位置情報

スマートフォンを落としてしまったときに「探す」機能があることは知っていますか？これは、GPS システムを利用して、スマートフォンの現在位置を衛星から特定することで検索しています。最近では、インターネット上に位置情報を発信するゲームアプリもあります。

また、Wi-Fi で受け取った電波の強度や到達時間などの情報から現在位置の特定をすることもできます。こちらは GPS と異なり建物内でも使えるほか、Wi-Fi に接続していなくても Wi-Fi 機能がオンになっていれば利用できる機能です。

さらに、GPS や Wi-Fi をオフにしても、契約しているスマートフォンのキャリア（電気通信事業者）は、電波基地局を通じてある程度の位置情報を特定できます。この機能を利用して、新型コロナウイルス感染拡大時の繁華街の人出の計測などが行われています。

こうして測定された位置情報は、SNS への写真・動画の投稿時や、その他アプリの機能などで、自動的に取得されてしまうことがあります。不要な場合は、スマートフォンの全体設定だけでなく、個別の設定でもオフにしておきましょう。



瞳に写った個人情報



性能の良いカメラで撮影すると、写真には多くの情報が写りこみます。



人物写真の瞳に写った画像から、人物（対面者）や場所の特定ができてしまう場合があります。写真の背景に景色や物品が写りこんでいると、特定はさらに容易になります。

過去には、瞳に写った情報からアイドルの自宅を特定し、ストーカー行為をした男が逮捕されるという事件もありました。このケースでは、写真の投稿時間と差し込む光の角度などから、マンションの階数まで特定できたようです。

人物写真を SNS などにアップロードする場合は、個人の特定につながる情報が含まれていないか確認し、必要に応じて画像加工を行うなどして、個人情報を守りましょう。

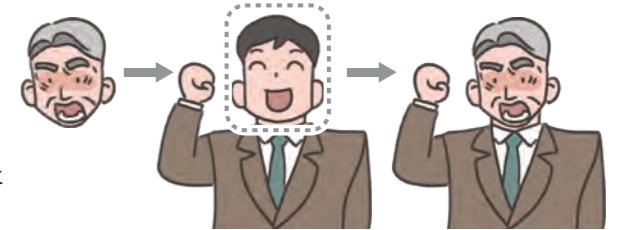
国立情報学研究所が 2016 年に行った実験では、顔の横でピースサインをした人物を 3m 先で撮影した写真から、指紋の解析に成功しています。これを元に人工指を作成したところ、指紋認証を突破できたそうです。

AI によるディープフェイク

コンピューターやスマートフォンのアプリを利用して、政治家や俳優などの著名人による「本人が言っていないことを発信している、人工で作られた架空の動画」などがアップロードされることがあります。

これは AI（人工知能）の機能であるディープラーニングを悪用してフェイク（偽）データを作り出すもので、「ディープフェイク」と呼ばれています。

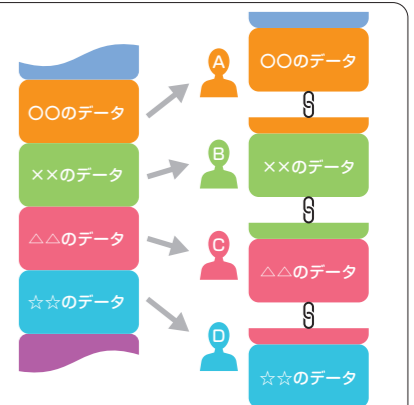
パロディならば問題ないという意見もありますが、データがコピーされてインターネット上に拡散されていくうちに、ディープフェイクであるという表記が失われてしまう危険性があります。内容を問わず、本人の許可なく作成された合成データを、ネット上にアップロードすることは許されません。



重要 技術的に「できる」ことと、それを面白がって「悪用してしまうこと」はまったく別物です。

ブロックチェーンをディープフェイク対策に？

ブロックチェーンとは、複数のメンバーで同一のデータを分散し、それぞれが保持することでデータの不正や改ざん、障害による停止を防ぐシステムです。通常、認証データなどの個人情報は暗号化され、サーバーに一括保管されていますが、これを直前のデータの一部を含んだ単位に切り分け、多くの人に分散して持たせます。そのデータが必要になったら、無関係の第三者が整合性を「承認」することで初めて利用できるようにします（「マイニング」）。データの改ざんが困難であること、データを分散するためトラブルに強いことなどのメリットがあり、現在は主に仮想通貨の取引記録に使われています。このシステムを本人の公式データであるかどうかの認証に応用すれば、ディープフェイクを防げるのではないかと期待されています。



デジタルタトゥー

インターネット上に書き込んだコメントやアップロードした画像は、半永久的にその痕跡が残ります。これを「デジタルタトゥー」といいます。

対面で消えていく言葉とは異なり、インターネットで一度発信した言葉は消えずに残ります。一度公開した情報のメンテナンス（アップデート）は不要なのでしょうか？

SNS に限らず、インターネット上に発信したデータはすべて記録（ログ）が採られています。それが元になる事件が発生し、警察が命じれば、捜査に必要な情報はすべて開示されてしまいます。匿名であるのをいいことに他人を誹謗・中傷すると、名誉毀損罪で訴えられる可能性もあるのです。

他にも、インターネット上にアップロードしたデータが勝手にコピーされ、海外のサーバーに置かれてしまったことで、日本の法律の手が及ばずに削除ができなくなるというケースもあります。



「危険だから使わない」ということではありません。「人が知りたいこと」、「見ていて楽しくなるもの」を発信するように心がけましょう。