

「デジタルタトゥー」 という考え方を知る

軽い気持ちでアップした画像などが、タトゥーのように、消すことが難しいままネット上に残ってしまうことがあります。ネットにアップするのは、それだけ重い行動なのです。

投稿がネット上にずっと残ってしまうことの危険

13ページで説明したように、ネット上にアップされた投稿や画像などは、一度拡散されると、いくらもとの投稿を取り消したり削除したりしても、その投稿が引用されたりスクリーンショットで撮影されたりすることで、半永久的にインターネット上に残ってしまい

ます。その結果、人に知られたくない情報などが広がってしまい、不利益を被ることもあるのです。

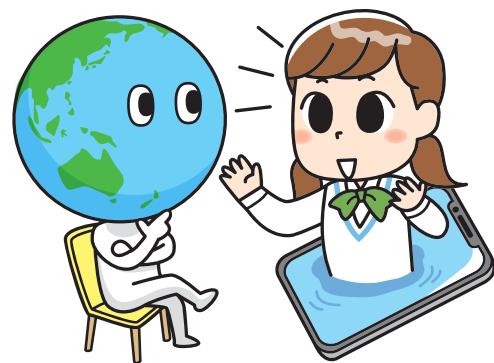
このことを、デジタルタトゥーといいます。「digital」（デジタルの）と、「tattoo」（刺青、タトゥー）を組み合わせた言葉です。

世界中の人が見ているという自覚をもつ

SNSの普及により、誰もが情報を受け取ったり拡散したりできるようになった今、デジタルタトゥーの問題が深刻化しています。

投稿など、何か情報発信をするさいは、誰もがスクリーンショットなどでその投稿を保存できることを意識しましょう。そして、「本当に発信しているか」「その情報は本当に残すべきか」を考えることが大切です。その結果、

投稿に悩むような場合は、まず家族や周囲の大人に相談しましょう。

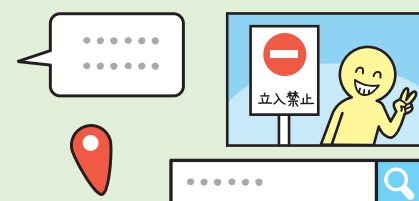


デジタルタトゥーの具体的な例

ケース01

個人情報

ネット上のコメントや画像、位置や顔認識情報、検索履歴、閲覧・視聴履歴など（20～21ページで解説します）。



ケース02

誹謗中傷・デマ

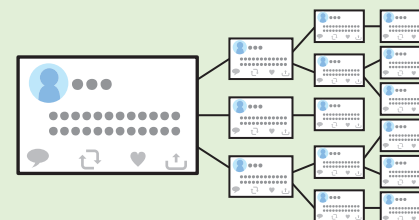
事実とは異なる情報や、悪意のある編集された画像、動画。



ケース03

ネットに書きこんだ文章

とくにTwitterなどでは瞬く間に拡散されてしまい、消せない情報がどんどん広がります。



ケース04

悪ふざけ・いたずら

SNSにアップされる、仕事現場での過剰な悪ふざけや、立入禁止区域へ入り込んだ違法行為など。



ケース05

リベンジポルノ

以前の交際相手や結婚相手などとの間で撮影された、性的な画像や動画が拡散されること。リベンジポルノ防止法という法律でとくに規制されています。

ケース06

逮捕歴・前科

たとえ警察に逮捕されても、不起訴になれば有罪ではありません。しかし逮捕の時点でニュースが公開され、それが拡散されることで、人の名誉および信用が深刻に損なわれます。

個人情報 の 取り扱い は慎重に

個人情報の取り扱いは、スマホでコミュニケーションを取るときにいちばん気をつけるべきもののひとつです。流出によってトラブルが多く起こっています。個人情報について注意すべきことを確認しておきましょう。

個人情報はどこからどこまで？

名前や電話番号、住所がすべてわかれば、その人のことが特定できます。このように特定の人にたどりつける情報を、個人情報といいます。情報ももれても、情報がひとつだけでは、個人の特定は難しいものです。複数の情報を組み合わせて、個人を特定できる状態になってはじめて個人情報となります。



個人情報が流出するとどうなる？

たとえば、あなたの個人情報が流出して誰にでも見られるようになったとします。そうすると、知らない人から電話がかかってくる、メールが届いたりします。ときには、もれた情報をもとにあなたしか知らないような趣味や趣向などの情報を調べて、広告を送ってきたり、その情報をネタに脅迫したりされることもあります。

個人情報の流出による被害の例

- 勧誘の電話がかかってくる
- 入会案内が山のように届く
- 勝手に有料サービスに登録されてしまい、課金される
- 誰かがあなたの名前を使って、ウェブ上の情報を書きこむ
- つきまといや嫌がらせを受ける

他人の個人情報をもらしてしまうことも

自分の個人情報と同じように、家族や友だちの個人情報についても気をつけなくてはなりません。

家族や友だちの許可なく勝手に画像をアップしたり、名前や学校名などを書きこんだりすると、その人の個人情報もれてしまいます。「自分が知っている、他人の個人情報はもらさない」という態度が大切です。



自分で情報をもらしていることも

SNSのプロフィール欄に電話番号や住所を書いたり、実際に会ったことのない相手に学校や名前などを教えたりしてはいけません。このような形で、自分から個人情報をもらしてしまうこともあるので、十分に気をつけましょう。巧妙に個人情報を引き出そうとする悪意のある人もいます。22～23ページを読んで、どんな危険があるかを把握してください。



人が写っている写真も個人情報なの？

人物が写っている写真データは、個人情報となります。なぜなら、写っている人を知っている人が見れば、それが、どの誰なのかということ特定でき、識別できるからです。

個人情報保護法という法律では、「特定の個人とわかるような画像、音声データなども個人情報である」と明確に定義されています。

写真に写っている背景などからも、その人がどこで何をしていたのか、どこに住んでいるかという情報まで読み取れることもあります。SNSなどに写真を投稿するさいは、とくに気をつけましょう。

写真に写っている背景などからも、その人がどこで何をしていたのか、どこに住んでいるかという情報まで読み取れることもあります。SNSなどに写真を投稿するさいは、とくに気をつけましょう。

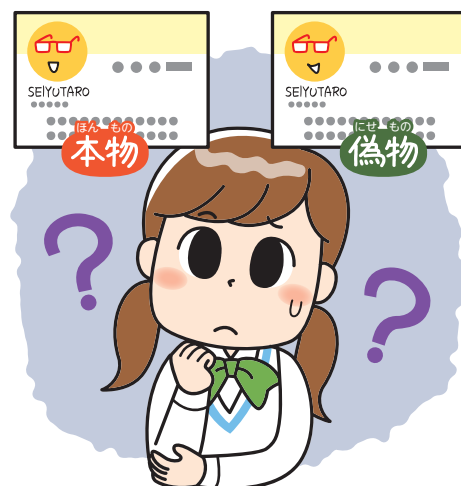
SNSアプリの危険性を知っておこう

エスエヌエス SNSが普及する中、知り合い同士の空間であるという安心感を利用した詐欺やウイルスを流す事件も起こっています。ここでは、そういったトラブルに巻き込まれないために知っておきたいことを紹介します。

キケン01 偽アカウントや架空アカウントの可能性

多くのSNSでは、アプリ運営会社が利用者の本人確認をしますが、それをすり抜けて「なりすまし」といわれる偽者がまぎれ込むこともあります。

SNS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。直接の知人や公式アカウント以外は、安易にフォロー（購読）したり、友だちになったりしないようにしましょう。



キケン02 フリマアプリでのやり取り

メルカリやラクマなどの「フリマアプリ」には年齢制限がありませんが（未成年は親の承諾があれば利用可能）、お金や商品の受け渡しを伴うものなので、とくに注意が必要です。フリマアプリには、お金や商品をだまし取ろうと考える悪意をもった参加者もいます。アプリが決めたルールからはみ出てしまふ、普通ではない決済方法や架空の取

り引きに応じてしまつて、トラブルになるケースが多くあります。また、商品を送ってもらうために住所や氏名を相手に伝えるので、そこから個人情報もれることもあります。

基本的にネットでの買い物子どもだけで行うのは避け、お金のやり取りが発生するアプリは、大人といっしょに利用しましょう。

キケン03 SNS投稿の怪しいリンク

SNSには、基本的には誰でも投稿することができます。だからこそ、投稿された文章にある怪しそうなリンク先のURLには注意しましょう。それらをクリックするだけで不当な料金を請求される「ワンクリック詐欺」や、偽のウェブサイトにアクセスさせ、そのサ

イトでIDやパスワード、クレジットカードの番号などを入力させて情報を盗み取る「フィッシング詐欺」などに誘導される危険性があるからです。怪しい情報の見分け方については、このシリーズの3巻で詳しく紹介していますので、参考にしてください。



キケン04 メールアドレスの入力や送信

ブログやウェブサイトの問い合わせ先として公開しているメールアドレスには、大量の迷惑メールが送られることがあります。これは、公開されているメールアドレスを自動的に検索・収集するプログラムがあって、悪用されているためです。

これを防ぐために、ブログなどの問い合わせ先として、ふだん利用しているメールアドレスとは別の専用のアドレスを用意するとよいでしょう。また、ブログ上では、「@」を「atmark」などに変えて表記する、メールアドレスを画像ファイルとして表示する、などの対策が有効です。

