

インターネットでのトラブルから身を守る



インターネットにアクセスすることは日常生活の一部となりましたが、同時に簡単にトラブルに巻き込まれたり、軽率な行為によって意図せずに加害者になってしまったりと、思わぬ落とし穴も増えています。

パスワードや個人情報は・・・

- パスワードとして、辞書にある単語や生年月日や名前など調べれば分かるものを含めてはいけません。パスワードは、英大文字、英小文字、数字、利用可能な記号を混ぜて作ると良いでしょう。
- パスワードは他人に知られてはいけません。パスワードを書いた紙や画面を他人の目に触れないように保護しましょう。もちろん、パスワードを他人に教えるはいけません。
- 同じパスワードを複数のサービスで使い回してはいけません。サービスごとに異なるパスワードを設定していれば、どれか1つのサービスでパスワードが流出したとしても、他のサービスには影響を与えません。いくつも覚えるのが大変なときは、パスワード管理ソフトを使いましょう。

SNS の利用

- SNS に公開した情報は閲覧制限をしても不特定多数に広まる可能性のあることを認識しましょう。面白がって投稿した不適切な動画や画像を、友人の誰かが面白がって他のサイトへアップすることも考えられます。SNS への投稿はあらゆる場所に拡散するということを留意して使用しましょう。
- SNS に投稿した内容は、「デジタルタトゥー」として、永久に残り続けることを認識しましょう。今後の人生（就職・結婚・評価など）に影響を及ぼし続ける可能性があります。
- 自分の発言・行動には常に責任が伴うことを認識しましょう。現実社会と同じで、SNS であっても個人や団体を侮辱すること、人種、性別、国籍、思想、宗教、外見、職業などについて差別的・排他的な発言することは厳禁です。

詐欺対策

- フィッシング詐欺メールに注意しましょう。「フィッシング詐欺」とは、実在のサイト（銀行・楽天・アマゾン・アップル・マイクロソフトなど）の管理者などを装い、本物に似せたサイトに呼び込んで、ID とパスワードを詐取しようとする行為です。まずは、銀行などがメールで個人情報（口座番号、パスワード、カード番号など）の入力や確認を求めることはありえないと考えてください。
- 不審な案内があった場合、受信したメールに書かれた連絡先ではなく、その会社の連絡先をインターネットで調べ問い合わせをするなど注意して対応しましょう。自分で理解できないこと、判断できないことがあれば、友人や教員に問い合わせるか、下記のようなサイトで調べ、不確実なことはせず、安易な解決を試みないことが肝心です。
 - ・ つくば市消費生活センター ・ 国民生活センター
 - ・ 警察庁インターネット安全・安心相談 <https://www.npa.go.jp/cybersafety/>



デバイス（PC, スマホなど）のウイルス対策

- デバイスの OS（Windows など）やブラウザ（Edge, firefox, chrome など）は、セキュリティに関する更新をこまめに行いましょう。
- ウィルス対策ソフトを必ずインストールし、ウィルス定義ファイルを常に最新の状態に保ちましょう。

学内のコンピュータやネットワークを利用する前に！

筑波大学の情報システム（ネットワークやコンピュータ等）を利用するときには、守らなくてはならないガイドラインがあります。必ず確認して、ガイドラインを守って利用してください。

- ・「情報システムを安心・安全に利用するために」（学内ネットワークから見られます）

<https://oii.tsukuba.ac.jp/oii-security/>

情報環境機構（情報基盤課） Tel.029-853-2070 E-mail:oii-security@oii.tsukuba.ac.jp

