情報システムを安心・安全に利用するために

このパンフレットは、筑波大学の情報システム（ネットワークやコンピュータなど）を利用する際に守らなくてはならないルールや重要なポイントを記載しています。本学の情報システムを使用する前に、パンフレットの内容をよく読み、確認した後、以下の項目にチェックを入れてください。
また、本パンフレットのさらに詳しい補足説明が https://oii.tsukuba.ac.jp/oii-security/details/ にあります。
正しい知識を身につけて、本学の情報システムを安心・安全に活用しましょう。

筑波大学
University of Tsukuba

☑Check!

- □「INFOSS 情報倫理」を受講しています
- □Windows Update などを定期的に行い、ソフトウェアを最新の状態で使っています
- □アンチウィルスソフトをインストールしています。また、最新のコンピュータウィルスに対応するため、ウィルスの定義ファイルが自動更新になっていることを確認しています
- □詐欺行為に注意して、ネットワークを利用しています
- □パスワードを他人に教えていません
- □他人のユーザ名とパスワードを使用していません
- □簡単なパスワードを設定していません
- □個人情報などの管理を徹底し、情報漏えいの対策を講じています
- □ソーシャル・ネットワーキング・サービス（SNS）など、インターネットへの情報発信は、筑波大学構成員としての自覚をもち、モラルをもって行っています
- □他者の著作物を違法にコピーしたり、ネットワークで第三者が閲覧可能な状態にしたりしていません
- □ファイル交換ソフトはインストールしてありません
- □出所が不明なソフトウェアはダウンロードしません

情報環境機構

情報システムを安心・安全に利用するために

「INFOSS 情報倫理」を受講しています

情報環境機構では、大学の様々な活動を進める上で欠かせない ICT（情報通信技術）に関する知識や法律、マナーなどを身に付け、ネットワーク社会で被害を受けたりトラブルを起こしたりしないよう、情報セキュリティを学ぶためのｅラーニング教材を用意しています。学生の方は在学中に少なくとも１回（学籍番号が変わるごとに１回以上）受講しなくてはいけません。まだ受講していない場合は、必ず受講してください。

詳細については、https://oii.tsukuba.ac.jp/infoss/ をご覧ください。

Windows Update などを定期的に行い、ソフトウェアを最新の状態で使っています

コンピュータウィルスは、OS（Microsoft Windows や macOS など）やよく利用されるソフトウェア（Microsoft Office、Adobe Reader、ブラウザなど）の欠陥を悪用して感染します。Microsoft Windows の場合は Windows Update や Microsoft Update を、macOS の場合はソフトウェア･アップデートを定期的に行い、常に最新の状態に保ちましょう。また、サポートが終了した古いバージョンの OS は、使用を中止してください。最新のバージョンへのアップグレードが必要です。その他のソフトウェアも、常に最新版に更新しましょう。

詳細については、https://oii.tsukuba.ac.jp/oii-security/details/ をご覧ください。

アンチウィルスソフトをインストールしています。また、最新のコンピュータウィルスに対応するため、ウィルスの定義ファイルが自動更新になっていることを確認しています

コンピュータウィルスに感染すると、パソコンのデータが破壊されるだけでなく、パソコン自体が乗っ取られ、迷惑メールの配信や他のパソコンへの攻撃に利用されてしまいます。コンピュータウィルスは、メールなどで送られてくるだけでなく、Web サイトを見たり、USB メモリをパソコンにさしたりするだけで感染するなど、感染経路が多様化しています。不注意な操作でコンピュータウィルスに感染しないよう、アンチウィルスソフトをインストールし、ウィルスの定義ファイルも定期的に更新しましょう。

本学では、３台までの個人所有端末（Windows、Mac、モバイル端末）にインストール可能なアンチウィルスソフトを提供しています。まだインストールしていない場合はもちろん、既にインストールされているアンチウィルスソフトのライセンス料を支払っているか不明な場合は、これをインストールしてください。

詳細については、https://oii.tsukuba.ac.jp/oiisecurity/details/ をご覧ください。

Q コンピュータウィルスに感染してしまったら？

更なる感染を防止するため、当該コンピュータをネットワークから切り離し（ネットワークケーブルを外す、機内モードにする、Wi-Fi とモバイル通信をオフにするなど）、本パンフレット末尾の問い合わせ先に連絡・相談してください。

詐欺行為に注意して、ネットワークを利用しています

ネットワークを利用すると便利な半面、思わぬトラブルに巻き込まれることがあります。
問題に直面し自分で判断できないときは、安易な解決を試みる前に、友人や教職員に相談するか、消費生活センターなどに問い合わせてください。

フィッシング（Phishing）詐欺

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 Web サイトに呼び込んで、ID やパスワードなどの個人情報を詐取しようとする行為です。銀行などが電子メールで個人情報の入力や確認を求めることはありません。不審な案内があった場合は、（送られてきた案内に書いてある連絡先ではなく）大元の会社に問い合わせるなどして、安易に個人情報を入力しないでください。

（参考）情報環境機構 Web サイト：本学に届いたフィッシングメール・詐欺メール　※学内限定
https://oii.tsukuba.ac.jp/security/information/suspiciousmail/

サポート詐欺

サポート詐欺とは、Web サイト閲覧中に突然ウィルスに感染したかのような嘘の警告画面を表示させるなどして不安を煽り、画面に記載された連絡先に電話をかけさせ、遠隔操作ソフトをインストールさせたり、金銭を詐取したりするものです。Web サイト閲覧中のポップアップ画面は安易に信じ込んではいけません。突然セキュリティ警告画面が表示されても、決して表示された電話番号には電話をかけずに、まずはサポート詐欺の可能性を疑ってください。ブラウザを強制終了したりコンピュータを再起動したりしても症状が改善されない場合は、本パンフレット補足説明のページに記載した対処方法を試してください。その後、ウィルスチェックを実施してコンピュータの安全を確認すると良いでしょう。

ワンクリック詐欺（ワンクリック商法）

ワンクリック詐欺とは、電子メールや Web サイトに記載されたリンクを 1 回クリックしただけで、一方的に契約に合意したことにされてしまい、料金の支払いを請求される詐欺です。このような請求は無視し、見覚えのない相手に連絡しない、住所や氏名を教えない、利用した覚えのない請求には現金を振り込まないなどの対策をしてください。
また、裁判手続きを悪用した請求をされる場合があります。裁判所からの通知は無視せずに、（送られてきた通知に書いてある連絡先ではなく）裁判所のホームページ（https://www.courts.go.jp/）
などで確認した連絡先に連絡をしてください。

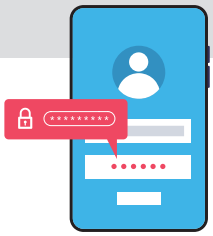
パスワードを他人に教えていません

本学の情報システムで使うユーザ名とパスワードは、コンピュータを利用している個人を特定する大事な情報です。あなたのユーザ名とパスワードを他人に教えて、本学の情報システムを使わせ、その人が問題を起こした場合、その責任はパスワードを教えたあなたにもあります。逆に、他人から教えてもらったユーザ名とパスワードを使ってもいけません。

他人のユーザ名とパスワードを使用していません

他人のユーザ名とパスワードを何らかの方法で知り、その人に成りすましてログインした場合や、セキュリティホール（プログラムの不具合）などを利用し、ユーザ名やパスワードの確認を回避してログインした場合は、不正アクセス行為の禁止等に関する法律に違反します。

簡単なパスワードを設定していません



パスワードを容易に推測できるもの（ユーザ名や自分の名前、誕生日や電話番号と同じにする、同じ文字を繰り返す、英単語を 1 つ以上繰り返したものにする、キーボードの並び（qwerty など）にする、以上のものを逆順にするなど）にしていると、不正アクセスの被害に遭う場合があります。パスワードは推測が難しいもの（最低 8 文字、12 文字以上推奨、英語の大文字と小文字、記号、数字を組み合わせたもの）に設定し、定期的に変更しましょう。難しいパスワードにしても、メモなどに書いて、他人が容易に見える状態にしないでください。
また、同じパスワードを複数のインターネットサービスで使い回すのはやめましょう。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。個人の端末であれば、パスワード管理ソフトを利用することもできます。
多要素認証も活用しましょう。万が一パスワードを盗まれてしまっても、不正アクセスを防ぐことができます。

個人情報などの管理を徹底し、情報漏えいの対策を講じています

教職員はもちろん、学生であっても、講義や実習でのアンケート調査などを通じて得られた個人情報や診療情報などを取り扱う場合があります。このような情報は、ネットワーク上で公開してはならず、また、学外に持ち出すことは原則禁止です。やむを得ず持ち出す場合も、当該情報の管理者あるいは管理者の委任を受けた者（講義や実習などの場合は、授業担当教員や研究室の指導教員など）の許可を得た後、暗号化などの安全保護措置を講じてから持ち出してください。また、個人情報は個人で管理するパソコンに保存しないように努め、やむを得ず保存する場合も、暗号化などの安全保護措置を講じてください。

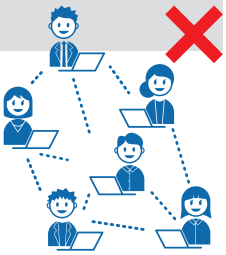
ソーシャル・ネットワーキング・サービス（SNS）など、インターネットへの情報発信は、筑波大学構成員としての自覚をもち、モラルをもって行っています

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、個人の安易な書き込みからトラブルが引き起こされたり、本学や本学構成員の良識が疑われたりする事態が起こりかねません。本来秘密にすべき事項や公序良俗に反する内容の書き込みなど不適切な情報発信を行わないように注意してください。

他者の著作物を違法にコピーしたり、ネットワークで第三者が閲覧可能な状態にしたりしていません

著作権法とは、「著作物並びに実演、レコード、放送及び有線放送に関し著作者の権利及びこれに隣接する権利を定め、これらの文化的所産の公平な利用に留意しつつ、著作者などの権利の保護を図り、もって文化の発展に寄与することを目的とする」法律です。著作権者の許諾なしに、法律で許されている範囲外で著作物を複製したり、ネットワークで第三者が閲覧可能な状態にしたりすると、罰せられます。さらに、著作権を侵害してアップロードされた事実を知りながら、その著作物（音楽、映像以外も含む）をダウンロードしても罰せられます。

ファイル交換ソフトはインストールしてありません



ファイル交換ソフトでは、コンピュータウィルスなど悪意を持ったファイルも配布されていますので、その利用はとても危険です。また、ダウンロードしたファイルは自動的に他の人にアップロードされてしまいます。本学では、個人のパソコンであっても、学内ネットワークでファイル交換ソフトを利用することを禁じています。ファイル交換ソフトによる通信を遮断する体制を取っており、利用者は学内処分されることがあります。正当な目的があって、学内でファイル交換ソフトを利用したい場合は、情報環境機構までご連絡ください。学生の場合、目的によって指導教員またはクラス担任の承認が必要となります。

出所が不明なソフトウェアはダウンロードしません

高額なソフトウェアが、無償、もしくは極めて安価に配布されている出所不明な Web サイトを見つけても、決してダウンロードしてはいけません。多くの場合、これらは許諾なしに配布されており、著作権を侵害するだけでなく、ソフトウェアが改変されているためコンピュータウィルスに感染する危険性があります。本学では、出所不明なソフトウェアのダウンロードを監視しており、対象者は学内処分されることがあります。

問題を発見した場合は報告してください

以下のような問題を発見した場合や、コンピュータウィルス感染など情報セキュリティに関するトラブルに直面した場合は、速やかに下記の問い合わせ先に連絡してください。

●著作権の侵害行為　●本学の機密情報や構成員の個人情報などの漏えい　●本学の情報システムのセキュリティ上の脆弱性や不具合

筑波大学 ISIRT　　Tel ❯ 029-853-2070　　e-mail ❯ incident@cc.tsukuba.ac.jp

このパンフレットの PDF 版・補足説明ページはこちら：https://oii.tsukuba.ac.jp/oii-security/

このパンフレットは、筑波大学情報環境機構が作成しました。　　2024 年 3 月発行