筑波大学
University of Tsukuba

情報システムを安心・安全に利用するために

筑波大学の情報システム（ネットワークやコンピュータなど）を利用するときに守らなくてはならないガイドラインがあります．本学の情報システムを使う前に，このガイドラインに関する以下のチェックリストを確認し，該当するものをチェックして下さい．該当しないものがあれば，パンフレット内の説明を読み，ガイドラインを守って情報システムを使って下さい．また，本パンフレットの詳しい説明が **http://www.oii.tsukuba.ac.jp/oii-security/** にあります．

☑Check！

- ☐ 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
  （著作権法が改正され，2012年10月から違法ダウンロードをすると罰せられるようになりました）
- ☐ 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の代表的な例として Xunlei, BitTorrent, µTorrent, LimeWire, Cabos, WinMX, Share, Winny などがあります．
- ☐ 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も頻繁に更新しています
- ☐ 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
- ☐ 個人情報等の管理を徹底し，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，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
- ☐ ネットワークを悪用した詐欺行為（フィッシング詐欺やワンクリック詐欺等）に注意して，ネットワークを利用しています
- ☐ 不審なメールは開かないように注意しています

情 報 環 境 機 構

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，著作者等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．また，著作権を侵害してアップロードされている音楽や映像などを，その事実を知りながらダウンロードする行為も罰せられるようになりました．

ファイル交換ソフトはインストールしてありません

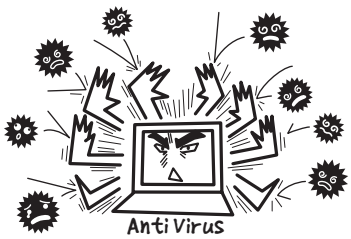
ファイル交換ソフトでは，コンピュータウィルスなど，悪意を持ったファイルも配布されていますのでその利用はとても危険です．また，ダウンロードしたファイルは自動的に他の人にアップロードされてしまいます．筑波大学では，個人のパソコンであっても，学内ネットワークでファイル交換ソフトを利用することを禁じています．ファイル交換ソフトによる通信を**遮断する体制を取っており，**利用者は学内処分されることがあります．
但し，正当な目的があって，学内でファイル交換ソフトを利用したい場合は，本パンフレット末尾の問い合わせ先まで御連絡下さい．

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（旧 Mac OS X）など）やよく利用されるソフトウェア（Microsoft Office，Adobe Flash Player，Adobe Reader，Java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（旧 Mac OS X）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．その他のソフトウェアも，常に最新版に更新しましょう．

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も頻繁に更新しています

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，ウェブページを見たり，USBメモリをパソコンにさしたりするだけで感染する等，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．筑波大学では，個人所有のPC等（Windows，Mac，モバイル端末）三台までにインストール可能なアンチウィルスソフトが利用できます．詳細については，**http://www.oii.tsukuba.ac.jp/oii-security/** をご覧下さい．



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や外付け無線LANカードを外す，内蔵無線LANの場合は無線LAN切り替えスイッチをオフにするなど），本パンフレット末尾の問い合わせ先に連絡・相談して下さい．

パスワードを他人に教えていません

筑波大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，筑波大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など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合う場合があります．パスワードは推測が難しいもの（６文字以上で，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下さい．

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さないで下さい．他所で漏洩したパスワードで学内のコンピュータが不正アクセスされ，迷惑メールが発信された事例も発生しています．たくさんのシステムを使う人は，パスワード管理ソフトを利用することもできます．

個人情報等の管理を徹底し，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を原則禁止とし，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等）の許可を得た後，暗号化等の安全保護措置を講じてから持ち出して下さい．また，個人情報は個人用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，暗号化等の安全保護措置を講じて下さい．

ソーシャル・ネットワーキング・サービス（SNS）など，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るなどの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．

ネットワークを悪用した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．以下では，学生生活支援室学生生活課が発行している「セーフティライフ～快適な学生生活を送るために～」から，ネットワークを利用する上で注意すべき詐欺行為について紹介します．**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，友人や教職員と相談するか，消費生活センター等に問い合わせて下さい．**

フィッシング（Phishing）詐欺

フィッシング詐欺とは，銀行やクレジットカード会社，携帯電話会社，ポータルサイトなどの信頼される会社から発信されたように見える虚偽の案内を電子メールなどで送り，ユーザをその会社のものに良く似たウェブページに誘導することで，ユーザの個人情報（クレジットカード番号や銀行の暗証番号，パスワードなど）を盗み出す詐欺です．銀行などが**電子メールで個人情報等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）大元の会社など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下さい．

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，電子メールやウェブページ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下さい．**
但し，裁判手続きを悪用した請求をされる場合があります．裁判所からの通知だった場合は無視せずに，（送られてきた通知に書いてある連絡先ではなく）電話帳などで確認した裁判所の連絡先に連絡をして下さい．

不審なメールは開かないように注意しています

メールシステム管理者を装った偽メールにより虚偽のページに誘導してアカウント情報を騙し取ろうとするフィッシング詐欺メールや，宅配業者を騙った配送通知など偽メールの添付ファイルを開封させウィルスに感染させようとするサイバー攻撃メールなどの不審メールが，本学でも多数確認されています．**件名や差出人，内容などに心当たりのない，また，疑問が感じられるメールについては安易に開かず削除し，添付ファイルの開封，本文中リンクへのアクセスは行わないで下さい．**
(参考) 全学計算機システム：フィッシングメールコレクション　https://www.u.tsukuba.ac.jp/phishing-collection/

問題を発見した場合は報告して下さい

筑波大学の情報システム上にセキュリティ上の脆弱性や不具合を見つけた場合や，著作権の侵害行為や機密情報や個人情報等が漏洩されている，または学外の情報システムで大学の機密情報や筑波大学構成員の個人情報等が公開されている，大学が権利を有するコンテンツが無断で使用されていることを見つけた場合は，速やかに右記問い合わせ先に連絡して下さい．

情報環境機構（学術情報部情報基盤課）
Tel ▶ 029-853-2070
e-mail ▶ oii-security@oii.tsukuba.ac.jp

詳細説明のページ：**http://www.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情報環境企画室が作成しました．　2018年3月発行