筑波大学
University of Tsukuba

筑波大学 情報環境機構
（学術情報部情報基盤課）

情報システムを安心・安全に利用するためのチェックポイント

（教職員向け）

筑波大学における情報システム（ネットワークやコンピュータなど）の利用においては、以下の各ポイントに目を通し、高いセキュリティ意識を持つように心がけましょう。

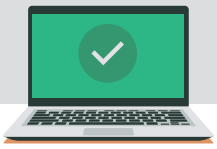
1 「INFOSS 情報倫理」を受講しましたか？

情報環境機構では、学生・教職員を対象に、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。本学教職員は少なくとも 3 年度に 1 回以上は受講しなければなりません。まだ受講していない方は、早めに受講するようお願いします。詳しくはこちら▶ https://oii.tsukuba.ac.jp/infoss/ をご覧ください。

なお、「e ラーニング受講管理システム」から自分の受講状況を確認することができます。

▶ https://lms4el.sec.tsukuba.ac.jp/

2 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か？



コンピュータウィルスは、OS 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 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。

3 不審なメールは開かないようにしましょう

システム管理者や宅配業者を騙って ID やパスワードなどの個人情報を盗み取ろうとするフィッシングメールや、添付ファイルを開かせコンピュータウィルスに感染させようとする迷惑メールが、本学でも多数確認されています。次の点に特に注意し、不明な場合は本学の管理者に確認するようにしましょう。

❶ 本学（tsukuba.ac.jp）以外のドメインからのメール

❷ 本学（tsukuba.ac.jp）以外のドメインの URL へのアクセス指示

❸ パスワードを記載するような指示（管理者がパスワードを聞くことは一切ありません）
（本学に届いたフィッシングメールの例 ▶ https://oii.tsukuba.ac.jp/security/information/suspiciousmail/）

4 パスワードの管理・パスワードの設定について

情報システムのパスワードは、適切な管理の徹底が必要です。特に、統一認証システムのパスワードは、manaba、TWINS など重要な情報を扱っているシステムで使用しますので、十分に注意してください。

❶ 他者には絶対に知らせない。学生や秘書などに作業を代行させない。

❷ パスワードは、難解で他者から類推しにくいものを設定する。
（英大文字・小文字・数字・記号をランダムに使い、最低 8 桁、12 桁以上を推奨）

❸ 統一認証システムの ID やパスワードを、他のシステムやサービスに使い回さない。
近年、パスワードクラッキング（悪意ある者がプログラムなどを用いて力ずくでパスワードを盗み出すこと）の被害に遭ったと思われる案件が複数発生しています。
OS 標準などのパスワード管理ソフトを利用することもできます。

❹ 多要素認証を活用しましょう。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。

5 個人情報・機密情報の適切な管理の徹底について

適切な取り扱いがなされていない場合、重大な情報セキュリティインシデントを招く可能性があります。下記のとおり、個人情報･機密情報の適切な管理の徹底をお願いします。

❶ 個人情報・機密情報を保有する機器が複数ある場合はできるだけ一つに集約する。また、不要な個人情報・機密情報は削除する。

❷ 個人情報･機密情報を保有する可搬型機器(ノートPCなど)、外部記憶装置(USBメモリなど)は、学外に持ち出さない。やむを得ず持ち出す場合は、個人情報保護管理者の許可を得たうえで必要最小限に絞り、パスワードの設定やデータの暗号化など、盗難・紛失時の対策を確実に行う。また、使用後は情報を確実に削除する。

❸ 本学では、情報の格付け及び取扱制限に関するルールを定めています。
▶ https://oii.tsukuba.ac.jp/regulation/kakuduke/ によって適切に取り扱ってください。

❹ 本学では、本学教職員が学内外の情報端末からファイルに安全にアクセスでき、閲覧・編集可能な環境としてオンラインストレージシステム（UTOS）を導入していますので、ご活用ください。
▶ https://utos.tsukuba.ac.jp/

❺ 個人情報・機密情報を取扱う情報システムを、外部クラウドサービスを利用して構築・運用・契約する場合は、「クラウドサービス利用のためのガイドライン」を参照してください。▶ https://oii.tsukuba.ac.jp/regulation/

❻ メールアドレスは個人情報です。面識のない相手や不特定多数にメールを送る場合などは､BCC を使いましょう。また、送信前に宛先に不要な相手のアドレスが含まれていないか、BCC で送るべきアドレスが TO や CC に入っていないかを確認しましょう。

6 民間企業のグループメールサービスやオンラインストレージサービスの利用上の注意点

Google Groups、OneDrive、Google Drive、Dropbox などを使用していませんか。このようなオンラインストレージサービスなどのインターネット上のサービスは、意図せず世界中に情報を公開してしまう恐れがあります。例えば、不注意なセキュリティ設定によって第三者の閲覧が可能となってしまう、ファイル同期機能により、公開フォルダに意図せず機密情報のファイルをアップロードしてしまうなどです。

意図したセキュリティ設定になっているか、周囲の人に確認してもらいましょう。また、強固なパスワード、多要素認証などの設定により、セキュリティを強化しましょう。

7 ソーシャル・ネットワーキング・サービス（SNS）などのネットへの情報発信について

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ます。個人の安易な書き込みによりトラブルとなり、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。機密情報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注意してください。
（筑波大学ソーシャルメディア利用ガイドライン▶ https://oii.tsukuba.ac.jp/regulation/）

8 参考情報

・学術情報メディアセンターのソフトウェアライセンスの提供

❶ EES：https://www.cc.tsukuba.ac.jp/wp/service/sl/ees/
本学では、Microsoft 社の教育機関向け総合契約（EES: Enrollment for Education Solutions）を締結しています。本学教職員は、Windows や Office などの製品を利用できます。

❷ アンチウィルスソフト：https://www.cc.tsukuba.ac.jp/wp/service/sl/trendmicro/
本学では、アンチウィルスソフトのサイトライセンス契約を締結しています。本学教職員は無償でアンチウィルスソフトを利用できますので、ぜひ活用してください。

❸ その他のライセンスソフト：https://www.cc.tsukuba.ac.jp/wp/service/sl/

・筑波大学情報環境機構 Web サイト：https://oii.tsukuba.ac.jp/

・筑波大学における情報システム利用のガイドライン：https://oii.tsukuba.ac.jp/regulation/

情報セキュリティインシデントが発生した場合は下記へ連絡してください。

連絡先：筑波大学 ISIRT　TEL：029-853-2070　e-mail：incident@cc.tsukuba.ac.jp

2026年3月発行