ATTENTION

■情報倫理とセキュリティ

担当部署
・情報基盤課

学内の情報と情報システム（ネットワークとコンピュータ等）の利用に当たっては，以下の点に注意を払い，利用者としての自覚と責任を持って行動して下さい。これらに違反した場合，注意や処罰の対象になります。

■倫理的・法的な規則

●メール・インターネットサイトの閲覧

インターネット上の情報交換では，意識せずに犯罪行為や違法行為を行ってしまうことが少なくありません。違法薬物の取引，賭博行為，ネズミ講等は，刑事罰を伴う違法行為です。また，ハラスメントのように，相手が嫌がることもしてはいけません。情報の発信元，発信先は十分確認をしましょう。

●ＳＮＳやブログの利用

X（旧 Twitter）や LINE などの SNS や，ブログで発信する情報には，利用者の生活に密接な情報が多く含まれます。そのため，思いもよらず自分の個人情報が公開されたり，発信した情報によっては，ひどい場合炎上することもあります。また，大学の授業の講義動画，板書された内容，試験問題などを発信することは，著作権侵害にあたる可能性もあります。これらのサービスは便利ですが，利用する場合には，十分な注意を払いましょう。

●個人情報・プライバシー・人格権の保護

個人を特定する情報を公開することは，『なりすまし行為』をされる可能性や，ストーカー被害等のきっかけになる危険性があります。また，自分の情報を扱う以上に，他人の情報の取り扱いには注意が必要です。動画投稿サイトに，他人を撮影したものを無断で投稿すると，肖像権という人格権の侵害が問題になる場合があります。自分と他人のプライバシーを守りましょう。

●研究者の倫理

学生も研究活動を担う一員として，研究者の倫理を守るようにしなければなりません。適切に引用せず他人の文書等を利用することや，研究データの改ざんは研究者の倫理に反します。

●情報と知的財産の保護

紙の印刷物ばかりでなく，インターネット上の電子的情報も著作物として保護されます。それらの著作権を侵さないように十分注意して下さい。講義の動画，板書内容，試験問題にも著作権があります。また，商用アプリ，ソフトウェアには，利用にライセンスが必要なものも多くあります。このような権利保護されている情報などを，許可，ライセンスなく利用（発信）することは違法です。 また，友人やインターネットで得たライセンス情報，利用情報は，間違っていたり，古くなっていたり，元々許可を得ていないこともあります。利用許可やライセンスを，自分できちんと確認できない場合，利用しないようにしましょう。

ATTENTION

【検知サービス】

●ファイル共有ソフトウェアの不使用徹底

著作権侵害や情報流出など事件で利用されることも多いファイル共有ソフトウェアの利用は禁止されています。共有型のダウンロードソフトウェアや，無許可の音楽映像配信ソフトウェアの多くも該当します。大学ではファイアウォールで検知遮断していますが，自宅や出先での利用でも事件には巻き込まれることがあります。インストールしないようにしましょう。

【ファイル交換ソフトウェア検知サービス】

https://www.noc.titech.ac.jp/service/policy_violation.shtml

●ソフトウェアライセンス

ソフトウェアは一般にライセンス契約（使用許諾の形）で取引されますが，その使用許諾により，勝手に複数のコンピュータにインストールして使用することは禁じられています。必要数のライセンス契約を結ぶようにしましょう。なお，大学では，研究や業務で使用するソフトウェアによっては包括契約（Ｐ３６『ソフトウェア包括ライセンス』を参照）を結んでいるものがあります。

Attention!!

本学では不正ライセンスによるソフトウェア利用は違法行為として厳に禁止しています。違法行為は必ず発覚します。不正ライセンスによるソフトウェアの利用者が特定された場合には，当該利用者本人が法的及び社会的責任を負うことを認識して下さい。

≪参考≫

「東工大情報基盤利用ガイドライン」
東工大ポータルhttps://portal.titech.ac.jp/**に掲載**
「情報基盤利用に関する誓約・同意書」
https://portal.titech.ac.jp/guide/doc/yoshiki18.pdf
「国立大学法人東京工業大学情報倫理ポリシー」
http://www.jyoho.jim.titech.ac.jp/news/policy_1.pdf
「国立大学法人東京工業大学情報倫理規則」
http://www.somuka.titech.ac.jp/reiki_int/reiki_honbun/x385RG00000462.html?id=j3

●問題が起きたとき

具体的な問題が発生したときは，情報倫理委員会にお知らせ下さい。

【情報倫理委員会連絡先】

メールアドレス： cce@jim.titech.ac.jp

■情報セキュリティに関する注意

●モバイル機器の利用

スマートフォンやノート PC 等のモバイル機器を使うのが一般的になっていますが，大事な内容が保存された機器を紛失したり盗難されると，個人情報や機密情報が漏えいする危険があります。紛失等しないよう注意するとともに，パスワード設定等により，紛失等した場合でも不正なアクセスがされないように注意しましょう。

ATTENTION

●バックアップ

ユーザ各自のデータは貴重な個人の財産です。定期的に自らの責任でバックアップを取りましょう。

●ウイルス対策

各自の PC には，大学が包括契約したウイルス対策ソフトウェア（Ｐ３６『ソフトウェア包括ライセンス』を参照），もしくは，各自で用意したウイルス対策ソフトウェアをインストールして下さい。

●セキュリティアップデート

各自の PC にインストールされている OS やアプリケーションソフトウェアのセキュリティアップデートは，必ず行って下さい。PC 起動時に確認する習慣を身に付けたり，自動更新ができるソフトウェアは，その機能を有効にして下さい。

●パスワード管理

パスワードは情報システムを利用する際の鍵のようなものです。これが漏洩してしまうと，利用権のない第三者に無断で情報システムが利用されてしまいます。PC 以外のプリンタ複合機，ネットワークカメラにも適切なパスワード設定が必要です。パスワード管理には十分に注意を払って下さい。また，ID やパスワードの共用を避ける注意も必要です。

●共有設定やネットワーク管理

PC の共有は情報漏えいの危険がありますので，なるべく避けましょう。ID やパスワードの共有は決して行わないで下さい。またパスワードの使いまわしも止めましょう。共有ファイル設定には十分に注意を払って，不必要にファイルを共有にしておかないよう気を付けましょう。また，外部からのアクセスに対するポートは，必要のない限り，できるだけ閉じておく習慣を付けましょう。

●障害時の対応

意図的に情報システムや情報資産への破壊行為を行うことは論外ですが，操作ミス等，意図しない行為や悪意はなくとも興味本位の行為が，結果的に情報システムの障害や他人の情報資産へ損害を与えることがあり得ることに注意して下さい。万が一，そのような事態になった場合，決して隠したりせずに，即座にシステム管理者に連絡し，被害が拡大しないように努めて下さい。

【情報セキュリティガイド】

●情報倫理とセキュリティのためのガイド

このガイドは，本学の学生および教職員を対象として平易にまとめた小冊子です。必ず，読んで下さい。

【問い合わせ先】

研究推進部情報基盤課情報セキュリティ対策グループ

（学術国際情報センター２Ｆ）

E-mail：kib.sec@jim.titech.ac.jp

ATTENTION

【CERT】

URL：https://www.titech.ac.jp/guidelines-j.pdf

●情報セキュリティに係る事案発生時の緊急対応

本学には情報セキュリティに対応する専門チーム（CERT：Computer Emergency Response Team）が設置されています。

CERTはウイルス感染やWebサービスの不正利用などの情報セキュリティに係る事案が発生した時に緊急対応を行うほか，セキュリティ情報の発信，学内の脆弱性調査などの事前対応にも重きを置いた活動を行っています。近年は本学に向けた攻撃も一層高度化，多様化する傾向にあり，日常的に学内のマシンを狙った攻撃にさらされています。

ウイルスに感染するなどの情報セキュリティに係る事案に巻き込まれた場合は，CERTに問い合わせをして下さい。また，CERTのWebページ等も確認をして日頃から情報収集にも努めて下さい。

【問い合わせ先】

情報システム緊急対応チーム［東工大CERT（サート）］

URL：https://cert.titech.ac.jp　　X(旧 Twitter)：@T2CERT

E-mail：contact@cert.titech.ac.jp

電　話：03－5734－3272