湘南工科大学ネットワーク利用ガイドライン

制定　令和4年7月13日

1. 趣旨
   (1) 本ガイドラインは湘南工科大学の構成員（教職員・学生等）がコンピュータ、携帯情報端末やネットワークを利用するに当たって遵守すべき事項をまとめたものである。

2. 用語の定義
   (1) ネットワークはコンピュータを相互に接続する通信網のことをいう。
   (2) 情報システムはコンピュータ、ネットワーク、記憶媒体等で構成され、業務を処理する仕組みのことをいう。
   (3) 情報資産は以下のいずれかに該当するものをいう。
      ① ネットワーク及び情報システム
      ② ネットワーク及び情報システムで取り扱う情報
   (4) 情報端末はスマートフォン、タブレット端末、IoT 機器などネットワークへ接続が可能な機器のことをいう。

3. 一般利用
   (1) ネットワークの利用において、やりとりする情報の内容については、本学は基本的に関知せず、利用者が良識を持って判断しなければならない。
   (2) 利用者 ID を他人に譲渡または貸与してはならない。また、他の利用者 ID を用い、なりすましを行ってはならない。
   (3) OS やアプリケーションなどのソフトウェアのサポート期限が切れている状態では、ネットワークへ接続してはならない。
   (4) 掲示板、SNS、Web ページなどネットワーク上で学内から意見を表明するときは、関与者の人権やプライバシーを尊重すると共に、知的所有権（著作権、商標権、特許権等）に配慮しなければならない。
   (5) 大学設置の情報資産を本来の目的以外に使ってはならず、特に商用目的に使ってはならない。
   (6) 個人情報やアカウント情報（ID とパスワード）は適切に管理しなければならない。
   (7) 卒業等により利用資格を失った場合、それまで使用していた利用者 ID を使用してはならない。

4. 電子メールの利用
   (1) 第三者のプライバシーや知的所有権は十分尊重しなければならない。
   (2) ネズミ講やマルチ商法・チェーンメールなどに加担してはならない。
   (3) 送信先や転送先のメールアドレスは十分に確認しなければならない。
   (4) ファイルサイズの大きな添付ファイルをメール送信したい場合は、オンラインストレージサービス（Box、Google Drive 等）にファイルをアップロードして URL を共有すること。
   (5) 添付ファイルにマルウェアが内在する可能性を考慮しなければならない。
   (6) 安全を確保するためには暗号メールを必要に応じ使用することが望ましい。
   (7) メール中の URL を不用意にクリックしてはならない。
   (8) 送信元が不確かなメールは送信者へ確認するか無視しなければならない。

5. Web サイトへのアクセス
   (1) 不適切なサイトへのアクセスは行ってはならない。 信頼できないサイトへのアクセスは、取引時のトラブルなどに十分注意しなければならない。
   (2) 信頼できないサイトへ個人情報等の入力は行ってはならない。
   (3) Web ブラウザや OS のアップデートを常に行い、最新の状態に保たなければならない。
   (4) Web サイトで禁止されている行為をしてはならない。 例えば、Web サイトのスクレイピング、電子ジャーナル等のサイトでの機械的なダウンロードは禁止されていることがある。
   (5) 教育・研究・業務以外の用途による動画サイトの閲覧、ファイルサイズが巨大なファイルのダウンロードなどネットワークへ特に負荷がかかる利用を行ってはならない。学内ネットワークの通信容量は有限であり、その容量は学内で共有しているためである。

6. ソーシャルメディアの利用・情報の公開
   (1) 利用するソーシャルメディアの利用規約、仕組み、安全な利用に必要な設定などを事前に充分に確認してから利用しなければならない。
   (2) 第三者のプライバシーや知的所有権を十分尊重しなければならない。特に個人情報、肖像、プライバシー等に関わる内容の情報発信を行う場合は、事前に関係者の同意を得ておくなど、必要な手続きを行うこと。それができない場合には、発信をしないこと。もしも事実に反する情報発信や、他人に対して不快または嫌な思いをさせるような情報の発信、その他の不適切な情報の発信を行ったことを自覚した場合には、その発信を削除するだけでなく、訂正しお詫びをするなど誠実な対応を心がけること。
   (3) 公序良俗に反する情報、個人や組織に対する誹謗中傷、不当な批判など、不快な思いをさせる情報の発信を行ってはならない。また、自分が、それらの情報発信を受けた場合であっても、感情的に対応しないよう心がけること。内容によっては、ソーシャルメディア上でやりとりすることが望ましくない場合や、返答そのものをするべきでない場合もあることを理解し、ソーシャルメディア上でのやりとりにはこだわらないこと。
   (4) 細心の注意を払う必要のある事柄（思想信条や宗教、衝突を招きやすい事柄等）を話

題とする場合には、特に慎重に内容を検討することを心がけなければならない。

(5) 事実であるかどうかの裏づけを得ていない情報に基づく発信や、不確かな内容の発信は行うことを控えるとともに、情報発信を行う場合にはその旨を明らかにして行わなければならない。また事実に反する情報や単なる噂を拡散させる行為を行わないこと。

(6) 研究内容等を含む発信は十分注意し、機密が漏洩しないようにしなければならない。

(7) 公開した情報は多くの人に閲覧されることを想定しなければならない。

(8) 公開範囲を常に意識しなければならない。特に面識のない人からソーシャルメディア上の交流の申し出を受けた場合には、安易に了承しないこと。自分の情報の開示対象者を一定の範囲の人たちに限定している場合であっても、この申し出に応じることで情報が漏えいする危険性が高まることに充分気をつけること。

(9) 完全な匿名性は存在しないことを認識しなければならない。

(10) 一度公開した内容を完全に削除できないことを認識しなければならない。

(11) 情報は正確に記述するよう努め、誤解を招かないよう注意しなければならない。

(12) サービス登録・利用時には利用規程を確認しなければならない。

(13) 講義等における教材、作品、パフォーマンスを撮影・録音・録画したい場合は、その講義等の担当者（教員、製作者など）に事前に了承を得なくてはならない。了承がない場合の撮影・録音・録画は禁止する。また、撮影が許可された場合でも、それは個人のみの利用に限定した許可であり、ソーシャルメディア等にアップロードすることは著作権に違反する行為であり、これを行わないこと。特に講義等の担当者が掲載した講義録画データや資料などについては知的所有権の観点からソーシャルメディアなどへアップロードしてはならない。

7. ファイルの扱い

(1) 知的所有権（著作権、商標権、特許権等）を犯すなど違法なファイルを取り扱ってはならない。

(2) 法令により所持が禁止されているファイルを自己の意志に基づいて所持してはならない。

(3) 出所が不明なファイルや内容に確証が持てないファイルをダウンロードしてはならない。特に送信元が不確かなメールに含まれる Web サイトへのリンクや添付ファイルは開いてはならない。

(4) 大きなサイズのファイルをネットワークでやりとりするときは、他の利用者への影響を考慮しなければならない。

8. パソコン、情報機器のセキュリティ管理

(1) OS やアプリケーションなどのソフトウェアには常にセキュリティパッチを適用し最新の状態を保たなければならない。

(2) マルウェア（ウイルス）対策ソフトウェアを適時使用しなければならない。対策ソフトウェアは常に最新の状態に保ち有効な状態にしなければならない。

(3) 外部から取得した（ダウンロード、メールの添付、USB メモリや光学ディスクなどのメディアでのコピー）ファイルは、マルウェア対策ソフトウェアなどでスキャンしてから使用しなければならない。

(4) マルウェアの稼働を確認した場合は速やかに無効化し、無効化出来ない場合コンピュータをネットワークへ接続してはならない。また、学内で発生した場合はメディア情報センターに即時連絡しなければならない。

(5) データの改ざんや破損に備え、重要な情報は常にバックアップを行わなければならない。

9. 罰則

(1) このガイドラインに違反する場合、メディア情報センターの管理するコンピュータやネットワーク利用停止、違反者のメディア情報センター利用アカウントを停止する場合がある。さらに悪質な場合には学則に定めるところに従い処罰する場合がある。

附則

- 本ガイドラインの改定は情報セキュリティ委員会で協議する。