2026 年 9 月 9 日
新潟国際情報大学
情報センター運営委員会

ICT を活用するための教育環境の整備計画について

1. 目的

ICT の利活用による教育の質向上を目的として、「ICT 環境の整備」「教職員への技術・教育支援体制の構築」「情報セキュリティへの対応」を本学の全体方針として継続し、本年度の具体的な施策を推進する。

2. ICT を活用した教育の質の向上（現状と課題）

これまで、PC 必携化やネットワーク強化、サポート体制の整備により、ICT 活用の基盤は確立された。現在、昨年度からの課題である「利便性の向上（SSO・ポータル構築）」および「認証基盤の強化（多要素認証）」の導入作業を進行中である。

一方で、生成 AI の急速な普及と高度化により、サイバー攻撃（特にフィッシングメール等）の脅威が新たな局面を迎えている。AI によって自然な日本語を用いた詐欺メールが生成されるようになり、従来の「不自然な日本語を見分ける」といった個人の注意喚起だけでは防ぎきれないリスクが増大している。

3. 継続・進行中の計画（利便性と安全性の両立）

昨年度より着手している以下のプロジェクトについて、順次開始し、定着化を目指す。

- サービスポータルの運用開始と拡充
  学内の各サービスへ一ヶ所からアクセスできるポータルサイトを本稼働させ、利用者の利便性を最大化する。
- シングルサインオン（SSO）の対象拡大
  複数の学内システムの認証を統合し、パスワード管理の負担軽減と安全性の確保を両立させる。
- 学外アクセス時における多要素認証（MFA）の導入
  文部科学省の指針に基づき、成績入力のみならず学外からの全アクセスに対して多要素認証を適用する。これにより、パスワード漏えい時の不正アクセスを物理的に遮断する。

4. 重点取り組み事項（AI による高度化するフィッシング攻撃への対策啓発）

生成 AI を悪用した攻撃が巧妙化し、システム的な防御をすり抜けてくるものに対応するため、学生・教職員が「自分事」として捉え、行動を変えることで被害を最小化できるよう啓発活動を強化する。

- **“判別不可能”を前提とした行動へ**
  「AI が作成したメールは本物と区別がつきづらい」という現状を学生・教職員に周知する。
  メール内のリンクを無条件にクリックしたりするのではなく、遷移先の URL が適切なドメインかを必ず確認する。特に、パスワードの入力を求める通知に対しては最大限注意するよう指導する。

- **最新の AI 悪用事例を用いた注意喚起**
  生成 AI による精巧ななりすましメールや、公式サイトを模倣した偽ログイン画面の事例を収集し、ガイダンスや学内掲示板を通じて速やかに共有する。
- **多要素認証（MFA）による実害阻止の重要性周知**
  多要素認証の導入に合わせ、「フィッシングでパスワードが漏洩しても、MFA があればアカウントを乗っ取られない」というメリットを強調する。MFA を「手間の増加」ではなく「情報の安全を守る最後の砦」として前向きに捉えてもらえるよう啓発する。
- **被害発生時の速やかな報告の徹底**
  巧妙な攻撃に対し、100%の防御は不可能であることを共有する。万が一フィッシングサイトに情報を入力してしまった際に、躊躇なく報告し、即座にパスワード変更等の対処ができる文化・体制を整備する。

5. 今年度及び次年度以降の計画

- PC 教室 AV 設備の更新（令和 8 年 9 月実施）
  修理が困難になった 351 および 352 教室のプロジェクター設備の更新を行う。
- 次年度以降の計画
  全教室に整備されている ICT 機器の状況を継続的に把握し、計画的な更新を検討する。

以上