

○学校法人東京電機大学情報セキュリティガイドライン（教職員編）

発信 学校法人東京電機大学情報セキュリティ統括本部

所管 情報セキュリティ統括実施機関（総合メディアセンター）

第1節 はじめに

本編は、「情報セキュリティガイドライン（共通編）」を補完するものであり、教職員の諸活動において特に留意すべき事項を示す。なお、本編に定めのない事項については、「情報セキュリティガイドライン（共通編）」及び関係規程による。

また、諸活動において、情報セキュリティインシデント又はそのおそれを認めた場合は、速やかに第8節に定める方法により報告等を行うものとする。

第2節 教育活動

概要

教職員は、教育活動を通じて、学生情報、成績情報、教材、試験問題その他の重要な情報資産を取り扱う。これらの情報資産は適切に管理し、教育の公正性及び信頼性を確保しなければならない。また、教育支援システム等を利用する場合は、本法人のルールを遵守し、情報漏えい、著作権侵害その他の情報セキュリティ上のリスクに配慮して利用しなければならない。

利用者の行動基準

- 学生情報、成績情報、試験問題、答案その他教育上重要な情報資産を適切に管理すること。
- LMS その他の教育支援システムは、本法人が提供又は承認したものを利用すること。
- 教材、配付資料その他教育コンテンツを利用又は作成する際は、著作権その他関係法令及び本法人の規程を遵守すること。
- オンライン授業、授業録画及び授業配信を実施する場合は、学生の個人情報及び肖像権に十分配慮すること。
- 教育活動においてクラウドサービスを利用する場合は、公開範囲及びアクセス権限を適切に設定すること。
- 生成 AI を利用する場合は、限定公開情報、非公開情報、個人情報及び未公表の教育資料等を無断で入力しないこと。
- 学生に対し、情報モラル及び情報セキュリティに関する適切な指導及び助言に努めること。

第3節 研究活動

概要

教職員は、研究活動を通じて、研究データ、研究成果その他重要な研究情報を取り扱う。これらの情報は、研究活動の基盤であり、適切に管理しなければならない。また、共同研究その他学外との連携では、契約、守秘義務及び本法人のルールを遵守し、研究情報を適切に取り扱わなければならない。

利用者の行動基準

- 研究データ、未公表の研究成果その他重要な研究情報を適切に管理すること。
- 共同研究、受託研究その他外部機関との研究活動では、契約、守秘義務及び関係規程を遵守すること。
- 研究データをクラウドサービスへ保存又は共有する場合は、本法人が提供又は承認したサービスを利用し、適切なアクセス権限を設定すること。
- 生成 AI を利用する場合は、未公表の研究成果、契約上保護すべき情報その他機密性の高い情報を無断で入力しないこと。
- 研究成果を公表する際は、個人情報、知的財産権及び共同研究契約等に十分配慮すること。

第4節 学生情報・個人情報

概要

教職員は、教育、研究及び学生支援を通じて、学生情報、成績情報、その他の個人情報を取り扱う。これらの情報は適切に管理し、その機密性を確保しなければならない。個人情報を利用、保存又は提供する場合は、法令、本法人の規程及び利用目的を遵守し、適切な保護措置を講じなければならない。

利用者の行動基準

- 学生情報及び個人情報は、教育、研究及び業務上必要な範囲でのみ利用すること。
- 学生情報及び個人情報を第三者へ提供する場合は、法令及び本法人の規程に従い、必要な手続を行うこと。
- 成績情報、学生相談記録その他機密性の高い情報は、アクセス権限を適切に設定し、閲覧できる者を必要最小限とすること。
- 学生情報及び個人情報をクラウドサービスへ保存又は共有する場合は、本法人が提供又は承認したサービスを利用し、適切なアクセス管理を行うこと。
- 学生情報及び個人情報を電子メール又は外部記録媒体により送付又は持ち出す場合は、本法人の規程に従い必要な保護措置を講じること。

第 5 節 法人運営及び事務業務

概要

教職員は、人事、財務、契約、会議資料、各種申請書類その他法人運営に関する重要な情報資産を取り扱う。これらの情報は、その機密性を確保し、適切に管理しなければならない。業務で情報を共有又は持ち出す場合は、本法人のルールを遵守し、必要な情報セキュリティ対策を講じなければならない。

利用者の行動基準

- 人事、財務、契約その他法人運営に関する情報は、業務上必要な範囲でのみ利用すること。
- 会議資料、決裁文書その他重要文書は、適切なアクセス権限を設定し、関係者以外へ提供しないこと。
- 電子メール又はクラウドサービスを利用して法人情報を共有する場合は、本法人が提供又は承認したサービスを利用し、公開範囲及びアクセス権限を適切に設定すること。
- 限定公開情報及び非公開情報を学外へ送付又は持ち出す場合は、本法人の規程に従い必要な保護措置を講じること。
- 業務上知り得た情報を目的外に利用し、又は第三者へ漏らさないこと。

第 6 節 クラウドサービス及び生成 AI

概要

クラウドサービス及び生成 AI 等のデジタルサービスは、教育、研究及び法人運営に有効な手段である。一方で、情報漏えいその他のリスクを伴うことから、安全かつ適切な利用が求められる。利用に当たっては、本法人が提供又は承認したサービスを利用し、入力する情報及び生成された情報を適切に取り扱わなければならない。

利用者の行動基準

- 本法人が提供又は承認したクラウドサービス及び生成 AI サービスを利用すること。
- 限定公開情報、非公開情報、個人情報、未公表の研究成果その他機密性の高い情報を無断で入力しないこと。
- クラウドサービスを利用する場合は、公開範囲及びアクセス権限を適切に設定すること。
- 生成 AI による出力結果は、その内容の正確性及び適切性を確認した上で利用すること。
- 著作権その他第三者の権利を侵害しないよう十分配慮すること。

第 7 節 外部機関との連携

概要

教職員は、共同研究、委託業務その他外部機関との連携において、情報資産を適切に管理しなければならない。外部へ情報を提供する場合は、契約、本法人の規程及び守秘義務を遵守し、必要な保護措置を講じなければならない。

利用者の行動基準

- 共同研究、受託研究、業務委託その他外部機関との連携では、契約、守秘義務及び関係規程を遵守すること。
- 外部機関へ情報を提供する場合は、共有する情報を必要最小限とし、その重要度に応じた保護措置を講じること。
- 情報の共有には、本法人が提供又は承認した通信手段及びクラウドサービスを利用すること。
- 外部機関へ限定公開情報又は非公開情報を提供する場合は、必要な承認を得るとともに、アクセス権限を適切に設定すること。
- 連携終了後は、契約又は本法人の規程に従い、提供した情報及び媒体を適切に返却又は廃棄すること。

第 8 節 情報セキュリティインシデント対応

概要

教職員は、情報セキュリティインシデント又はそのおそれを認めた場合は、速やかに報告し、被害拡大防止に努めなければならない。また、情報セキュリティ実施責任者及び TDU-CSIRT による調査、復旧及び再発防止に協力しなければならない。

利用者の行動基準

- 情報セキュリティインシデント又はそのおそれを認めた場合は、速やかに TDU-CSIRT が定める窓口へ報告するとともに、TDU-CSIRT 及び情報セキュリティ統括実施機関（総合メディアセンター）の対応に協力すること。また、必要に応じて、当該情報システムの情報システム管理責任者にも報告すること。
- TDU-CSIRT による調査、証拠保全、原因究明及び復旧対応に協力すること。
- 感染拡大又は被害拡大を防止するため、情報セキュリティ実施責任者又は TDU-CSIRT の指示に従い適切な措置を講じること。
- 調査に必要な情報、機器、記録等を適切に保全し、無断で削除又は改変しないこと。
- 復旧後は、再発防止策の実施及び情報セキュリティ対策の改善に協力すること。
- インシデント対応を通じて得られた知見を教育、研究及び法人運営に活かし、情報セキュリティ水準の向上に努めること。