

○学校法人東京電機大学情報セキュリティガイドライン（共通編）

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

目的

情報通信技術は、教育、研究及び法人運営を支える重要な基盤であり、近年のデジタル技術の発展に伴い、その活用の可能性はますます広がっている。一方で、サイバー攻撃や情報漏えい等の脅威は高度化・巧妙化しており、学校法人東京電機大学（以下「本法人」という。）が保有する情報資産を適切に保護し、安全かつ信頼性の高い教育・研究活動及び法人運営を維持するとともに、社会からの信頼を確保していくことが、これまで以上に重要となっている。

学校法人東京電機大学情報セキュリティガイドライン（以下「本ガイドライン」という。）は、その実現に向け、本法人の情報セキュリティ基本方針、情報セキュリティ基本規程及び情報セキュリティ対策規程を補完する利用者向けの指針である。本ガイドラインは、利用者が日常の教育、研究及び業務活動において実践すべき情報セキュリティ対策の基本的な考え方及び行動を明確に示すことにより、情報資産の適正な利用を促進することを目的とする。

適用範囲

本ガイドラインは、本法人が管理する情報資産及び情報システムを利用する役員、教職員、学生、生徒、研究員、派遣職員、委託事業者その他本法人が利用を認めた全ての利用者に適用する。

なお、本ガイドラインに定めのない事項については、本法人の情報セキュリティ基本規程及び情報セキュリティ対策規程による。

情報セキュリティインシデントの発見及び連絡

利用者は、情報セキュリティに関する異常、不審な事象又はインシデントの発生若しくはそのおそれを認知した場合は、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。

第2節 情報資産

概要

情報資産は、本法人の教育、研究及び法人運営を支える重要な経営資源である。一方で、不適切な利用や管理は、情報漏えいや法人の信用失墜などにつながるおそれがある。利用者は、情報資産の重要性及び公開区分を理解し、その目的や重要度に応じて適切に利用し、管理することが重要である。

なお、本ガイドラインにおいて、非公開情報資産、限定公開情報資産及び公開情報資産を、それぞれ「非公開情報」「限定公開情報」及び「公開情報」という。

利用者の行動基準

- 情報資産は、教育、研究及び業務上の正当な目的に限って利用すること。
- 情報資産の公開区分（公開情報・限定公開情報・非公開情報）を確認し、その区分に応じて取り扱うこと。
- 業務又は学修に必要な最小限の範囲で情報資産を利用すること。
- 限定公開情報及び非公開情報を、許可なく第三者へ提供しないこと。
- 情報資産を学外へ持ち出す場合は、本法人の定める手続及び承認に従うこと。
- 情報資産は適切な場所及び方法で保管し、紛失、盗難及び漏えいを防止すること。
- 不要となった情報資産は、復元できない方法で適切に廃棄又は消去すること。
- 個人所有の機器又はクラウドサービスへ、限定公開情報又は非公開情報を無断で保存しないこと。
- 委託先又は共同研究先へ情報資産を提供する場合は、契約及び本法人のルールを遵守すること。
- 情報資産の漏えい、紛失その他の異常を発見した場合は、第1節の定めに従い報告すること。

第3節 認証情報

概要

アカウント及びパスワードは、利用者本人を識別し、情報システムを安全に利用するための重要な認証情報である。一方で、不適切な管理は、不正アクセスや情報漏えいなどの原因となるおそれがある。利用者は、認証情報の重要性を理解し、自らの責任において適切に管理するとともに、安全な情報システムの利用に努めることが重要である。

利用者の行動基準

- アカウント及び認証情報は、第三者へ共有、貸与又は開示しないこと。
- 推測されやすい文字列や個人情報をパスワードに使用しないこと。
- 異なる情報システムで同一のパスワードを使い回さないこと。
- 多要素認証を利用できる場合は、積極的に利用すること。

- パスワードを付箋や机上など第三者が容易に確認できる場所へ記載しないこと。
- 離席時は画面をロックし、利用終了後はログアウトすること。
- 共用アカウントは、業務上やむを得ず本法人が認めた場合に限り、管理責任者を明確にし、定められた方法に従って使用すること。
- アカウントの不正利用又は漏えいの疑いを認めた場合は、直ちにパスワードを変更するとともに、第 1 節の定めに従い報告すること。
- 異動、退職、卒業等に伴うアカウント及びアクセス権限の変更手続に協力すること。

第 4 節 情報端末

概要

パソコンやモバイル端末は、本法人の情報資産を利用するための重要な機器である。紛失、盗難、マルウェア感染などは、情報漏えいや業務への支障につながるおそれがある。利用者は、端末を適切に管理し、安全な利用環境を維持するよう努めることが重要である。

利用者の行動基準

- 端末は教育、研究及び業務の目的に応じて適切に利用すること。
- OS、アプリケーション及びウイルス対策ソフトを最新の状態に維持すること。
- 画面ロック、パスワード又は生体認証を設定し、第三者による不正利用を防止すること。
- 端末を離れる際は画面をロックし、利用終了後はログアウト又は電源を切ること。
- ソフトウェアのインストールは、本法人が定めるルールに従い、安全性及び利用条件を確認した上で行うこと。
- 限定公開情報又は非公開情報を保存する場合は、本法人が定める方法に従い、必要に応じて暗号化すること。
- 端末を学外へ持ち出す場合は、紛失、盗難及び覗き見に十分注意すること。
- 私物端末を利用する場合は、本法人が定める利用条件及びセキュリティ対策を遵守すること。
- 端末の紛失、盗難、マルウェア感染又は不正利用の疑いを認めた場合は、第 1 節の定めに従い報告すること。
- 端末の廃棄又は譲渡を行う場合は、保存されている情報を復元できない方法で完全に消去すること。

第 5 節 外部記録媒体

概要

外部記録媒体は、情報を容易に持ち運べる便利な手段である。一方で、紛失や盗難、マルウェア感染などによる情報漏えいのリスクも高い。利用者は、利用の必要性を十分に判断し、情報の重要度に応じた適切な管理を行うことが重要である。

利用者の行動基準

- USB メモリ、外付け SSD・HDD、SD カードその他の外部記録媒体は、必要な場合に限って利用すること。
- 限定公開情報又は非公開情報を保存する場合は、本法人が認める方法により暗号化その他の保護措置を講じること。
- 外部記録媒体を学外へ持ち出す場合は、本法人の定める手続及び承認に従うこと。
- 利用中及び保管中は、紛失、盗難、置き忘れ及び第三者による閲覧を防止すること。
- 出所が不明な USB メモリその他の記録媒体を本法人の端末へ接続しないこと。
- 外部記録媒体を利用する前後には、必要に応じてマルウェア検査を実施すること。
- 利用終了後は、不要となった複製データを削除し、記録媒体内の情報を適切に管理すること。
- 外部記録媒体を廃棄又は譲渡する場合は、保存情報を復元できない方法で完全に消去すること。
- 外部記録媒体の紛失、盗難、破損又は情報漏えいのおそれを認めた場合は、第 1 節の定めに従い報告すること。

第 6 節 学内ネットワーク

概要

学内ネットワークは、本法人の教育、研究及び業務を支える重要な情報基盤である。不適切な利用や無許可の機器接続は、ネットワーク障害や情報漏えいの原因となるおそれがある。利用者は、運用ルールを理解し、他の利用者にも配慮しながら、安全かつ適切な利用に努めることが重要である。

利用者の行動基準

- 学内ネットワークは教育、研究及び業務目的に限って利用すること。
- 情報システム管理者の許可なく、ネットワーク機器又は通信設定を変更しないこと。
- 無許可のパソコン、サーバ、無線 LAN 機器その他の機器を学内ネットワークへ接続しないこと。

- 接続する端末には、OS 及びソフトウェアの更新並びにウイルス対策を適切に実施すること。
- 他の利用者又は情報システムの運用を妨げる行為を行わないこと。
- ネットワーク利用に必要な認証情報を適切に管理し、第三者へ貸与又は共有しないこと。
- 異常な通信、障害又は不正アクセスの疑いを発見した場合は、第 1 節の定めに従い報告すること。
- 学内ネットワークを経由した著作権侵害、不正アクセスその他法令又は規程に違反する行為を行わないこと。
- 学内無線 LAN は、本法人が提供又は承認したアクセスポイントを利用すること。
- 情報システム管理者による保守、点検及びセキュリティ対策に協力すること。

第 7 節 インターネット

概要

インターネットは、教育、研究及び業務に不可欠な情報基盤である。一方で、不正アクセスやフィッシング詐欺、誤情報など、様々なリスクが存在する。利用者は、情報の信頼性や安全性を確認するとともに、法令や本法人のルールを踏まえ、適切に活用することが重要である。

利用者の行動基準

- インターネットは教育、研究及び業務上の目的に沿って適切に利用すること。
- 不審な Web サイトへのアクセス又は不審なファイルのダウンロードを行わないこと。
- Web サイトへ ID、パスワード又は個人情報を入力する際は、接続先の真正性を十分確認すること。
- ソフトウェア、アプリケーション及びデータは、信頼できる提供元からのみ取得すること。
- 著作権、個人情報保護その他関係法令を遵守すること。
- 教育・研究・業務に支障を及ぼす過度な私的利用を行わないこと。
- ブラウザ及び利用ソフトウェアを最新の状態に保つこと。
- インターネット上で取得した情報を利用する際は、正確性及び信頼性を確認すること。
- 不審な Web サイト又はセキュリティインシデントを発見した場合は、第 1 節の定めに従い報告すること。
- 本法人の信用を損なう情報発信又は法令・規程に反する行為を行わないこと。

第 8 節 電子メール

概要

電子メールは、教育、研究及び業務を支える重要な連絡手段である。一方で、誤送信やフィッシング、マルウェア感染などのリスクも伴う。利用者は、その利便性と危険性を理解し、内容や送信先を十分確認するなど、安全で責任ある利用に努めることが重要である。

利用者の行動基準

- 送信前に宛先、件名、本文及び添付ファイルを確認すること。
- 限定公開情報又は非公開情報を送信する場合は、本法人が定める方法に従うこと。
- CC 及び BCC を適切に使い分け、不要な個人情報の開示を防止すること。
- 送信元が不明又は不審な電子メールは、添付ファイルを開いたり、リンクをクリックしたりしないこと。
- 電子メールを業務又は学修以外の不適切な目的で利用しないこと。
- チェーンメール、迷惑メール又は誤情報を拡散しないこと。
- 自動転送を設定する場合は、本法人のルールに従い、情報漏えいを防止すること。
- 誤送信した場合は、第 1 節の定めに従い報告し、必要な対応を行うこと。

第 9 節 クラウドサービス

概要

クラウドサービスは、教育、研究及び業務における情報共有や効率化を支える重要な基盤である。一方で、不適切な利用や設定は、情報漏えいや意図しない情報公開につながるおそれがある。利用者は、利便性とリスクを理解し、本法人が提供又は承認したサービスを適切に利用するとともに、保存する情報や共有範囲に応じた管理に努めることが重要である。

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を優先して利用すること。
- 限定公開情報又は非公開情報を個人契約のクラウドサービスへ無断で保存しないこと。
- 情報共有に当たっては、公開範囲、有効期限及びアクセス権限を適切に設定し、不要となった共有設定は速やかに削除すること。
- クラウドサービスへ保存した情報は、重要度に応じて適切にバックアップを実施すること。
- 共同研究又は外部機関との情報共有では、契約及び本法人のルールに従うこと。
- クラウドサービスへ保存する情報は、著作権、個人情報保護及び研究倫理等の関係法令・規程を遵守すること。

- クラウドサービスの異常、不正アクセス又は情報漏えいの疑いを認めた場合は、第 1 節の定めに従い報告すること。
- クラウドサービスの安全な利用方法について継続的に学び、適切な運用に努めること。

第 10 節 生成 AI

概要

生成 AI は、教育、研究及び業務の質と効率の向上が期待される有用な技術である。一方で、情報漏えい、著作権侵害、個人情報の取扱い及び生成結果の正確性などに留意する必要がある。利用者は、その特性と限界を理解し、法令及び本法人の規程を踏まえ、自らの責任において安全かつ効果的に活用することが重要である。

利用者の行動基準

- 生成 AI は、教育、研究及び業務の質の向上を目的として適切に活用すること。
- 本法人が提供又は承認した生成 AI サービスを優先して利用すること。
- 限定公開情報、非公開情報、個人情報及び未公表の研究成果等を、許可なく生成 AI へ入力しないこと。
- 生成 AI サービスの利用規約、学習利用設定及び保存設定を確認した上で利用すること。
- 生成 AI が生成した内容は、正確性、妥当性及び最新性を自ら確認して利用すること。
- 生成 AI による生成物を利用する場合は、著作権、研究倫理、引用ルールその他関係法令及び本法人の規程を遵守すること。
- 教育において生成 AI を利用する場合は、学修成果の真正性及び教育目的に配慮すること。
- 研究において生成 AI を利用する場合は、研究データの管理、研究倫理及び知的財産権に十分留意すること。
- 生成 AI の利用に関して情報漏えい、不適切な出力その他問題を認めた場合は、第 1 節の定めに従い報告すること。
- 生成 AI に関する知識及び活用方法を継続的に学び、安全かつ効果的な利用に努めること。

第 11 節 情報発信

概要

SNS 及び Web サイトは、教育、研究及び法人活動に関する情報を社会へ発信する重要な手段である。一方で、不適切な情報発信は、本法人の信用や関係者の権利利益に影

響を及ぼすおそれがある。利用者は、公開する情報の内容や影響を十分に考慮し、法令及び本法人のルールを踏まえ、責任ある情報発信に努めることが重要である。

利用者の行動基準

- 教育、研究及び業務に関する情報は、正確性を確認した上で発信すること。
- 公開情報、限定公開情報及び非公開情報の区分を確認し、限定公開情報又は非公開情報を無断で公開しないこと。
- 個人情報、肖像権、著作権及び知的財産権を尊重し、必要な同意又は許諾を得ること。
- 本法人を代表する情報発信は、定められた手続及び承認に従うこと。
- 誹謗中傷、差別的表現、虚偽又は誤解を招く情報を発信しないこと。
- 共同研究先、企業等との契約又は守秘義務に反する情報を公開しないこと。
- SNS の公開範囲及びプライバシー設定を適切に管理すること。
- 研究成果や教育活動を発信する場合は、社会的影響及び情報セキュリティに配慮すること。
- 不適切な公開又は情報漏えいを認めた場合は、第 1 節の定めに従い報告すること。
- SNS 及び Web サービスを活用し、本法人の教育・研究活動の適切な情報発信に努めること。

第 12 節 インシデント対応

概要

情報セキュリティインシデントへの迅速かつ適切な対応は、被害の拡大防止と早期復旧のために重要である。初動対応の遅れや不適切な対応は、教育、研究及び業務に大きな影響を及ぼすおそれがある。利用者は、異常やその疑いを認めた場合には速やかに報告し、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）並びに必要な応じて当該情報システムの情報システム管理責任者と連携して、適切に対応することが重要である。

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疑いを認めた場合は、速やかに TDU-CSIRT が定める窓口へ報告すること。また、必要な応じて、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。
- 被害拡大を防止するため、TDU-CSIRT 又は情報セキュリティ統括実施機関（総合メディアセンター）の指示に従い、必要な初動対応を行うこと。
- TDU-CSIRT による調査、分析、証拠保全、復旧及び再発防止策の実施に協力すること。
- インシデントに関する情報を、許可なく学外又は第三者へ公表しないこと。

- ログ、電子メールその他の関連情報を削除又は改変せず、証拠保全に協力すること。
- マルウェア感染等が疑われる端末は、TDU-CSIRT 又は情報セキュリティ統括実施機関（総合メディアセンター）の指示に従い、ネットワークから切り離すなど適切な措置を講じること。
- 復旧作業は、TDU-CSIRT 又は情報セキュリティ統括実施機関（総合メディアセンター）の指示に従って実施すること。
- インシデントの原因分析及び再発防止策の実施に協力すること。
- インシデント対応訓練及び教育に積極的に参加し、対応能力の向上に努めること。

第 13 節 教育・啓発及び継続的改善

概要

情報セキュリティは、技術的な対策だけでなく、利用者一人ひとりの理解と行動によって支えられる。また、デジタル技術や情報セキュリティを取り巻く環境は絶えず変化しており、継続的な学習と改善が欠かせない。利用者は、新たな知識や技術を積極的に学び、日常の教育、研究及び業務を通じて、安全かつ効果的な情報活用に努めることが重要である。

利用者の行動基準

- 本法人が実施する情報セキュリティ教育、研修及び訓練に積極的に参加すること。
- クラウドサービス、生成 AI その他の新しいデジタル技術について継続的に学び、安全かつ効果的な活用に努めること。
- 本ガイドライン及び関係規程を理解し、日常の教育・研究・業務において実践すること。
- インシデントやヒヤリ・ハット事例を共有し、再発防止及び未然防止に協力すること。
- 情報セキュリティ対策に関する改善提案や課題を積極的に所属部署へ伝えること。
- 監査、点検及び自己点検に協力し、必要な改善を実施すること。
- 教育・研究・業務における DX を推進するため、安全な情報活用を心掛けること。
- 法令、本法人の規程及び本ガイドラインを遵守し、情報セキュリティ文化の醸成に努めること。
- 利用者相互に情報セキュリティ意識を高め合い、安全な利用環境づくりに貢献すること。
- 継続的改善の考え方を共有し、本法人の情報セキュリティ水準の向上に主体的に取り組むこと。