愛知工業大学　情報セキュリティガイドライン（管理者編）

１．目的

このガイドラインは、名古屋電気学園（以降 学園）の情報セキュリティーポリシーに基づき、サイバー攻撃、不正アクセス等から愛知工業大学（以降 本学）の情報資産を保護するため、情報資産及び情報ネットワークの管理者に対するガイドラインを設けて、一定の情報セキュリティを確保することを目的とする。

２．適応対象者

本学の情報資産及び情報システムを管理する者（教職員、本学の情報資産及び情報ネットワークを管理するすべての者）

３．用語の定義

⑴情報セキュリティ

情報の機密性、完全性、可用性を維持すること

・機密性：情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保すること

・完全性：情報が破壊、改ざん又は消去されていない状態を確保すること

・可用性：情報へのアクセスを認められた者が、必要なときに情報にアクセスできる状態を確保すること

⑵情報システム

ハードウェア、ソフトウェア、ネットワーク、記録媒体で構成されるものであって情報処理を行う仕組み

⑶情報機器

情報を処理したり伝達・加工するための機器、コンピュータとその周辺機器、IoT 機器

例：サーバ、パソコン、ロボット、ドローン、スマート家電、ファクシミリ・複写機等

⑷情報資産

情報システムに記録された情報および情報を管理する仕組み（情報システム、システム開発・運用・保守に関する資料等）の総称

⑸情報セキュリティインシデント（以降、インシデント）

情報セキュリティの確保が困難な事象、その恐れのある事象

⑹本学構成員

本学の学生、教職員及び学内において業務を行うことが認められている者

⑺その他

必要に応じ、本文に※表示して記載

４．アクセス制限

(1) アクセス者の取決め

情報へのアクセスコントロールについては、本学が正当と認める利用者が教育・研究・業務上の必要性に応じて確実に必要な情報へアクセスできるとともに、教育・研究・業務上の必要性がなく、情報を利用する権限のない者への情報へのアクセスを防止するため、教育・研究・業務上必要な情報へのアクセス者を明確に定め、その定めにそって情報へのアクセス権限を付与しなければならない。

※アクセスコントロール：情報の内容に応じて、情報に対するアクセスを制限すること

(2) アクセス権限の厳格な管理

必要な利用者に情報へのアクセスが確実に行えるよう、情報の利用者の登録及び権限の付与を行わなければならない。特にシステムを管理するための権限等、権限の及ぶ範囲の広い権限を保有する利用者に対しては、厳格な管理を実施しなければならない。

(3) 学外利用者に対するアクセス制限

学外の者が利用する情報システムについては、本学構成員のみで利用する情報システムに比べ、情報システムの無断使用や情報漏えい・改ざん等が発生しやすいことが懸念されるため、アクセスコントロールを厳格に実施しなければならない。また、利用者に対し契約上の利用制限を明記しなければならない。

(4) ネットワークに関するアクセスコントロール

ネットワークを利用した不正アクセスを防止するため、ネットワーク利用者の特定によるアクセスコントロールを講じるとともに、利用場所や接続機器の特定によるアクセスコントロールを可能な限り実施しなければならない。

(5) ソフトウェア等各種アクセスコントロール

情報システムの不正利用を防止するため、ネットワーク・オペレーティングシステムのアクセスコントロール、情報システムのアプリケーション毎のアクセスコントロールを可能な限り実施しなければならない。

(6) 物理的なアクセス制限

情報資産及び情報資産の設置場所は、盗難及び物理的な破壊等による被害を防止するため、物理的なアクセスコントロールを実施し、アクセスは必要最低限の要員に限定しなければならない。

(7) 端末のアクセスコントロール

情報システムの不正利用を防止するため、情報システムは教育・研究・業務上必要な者のみが利用できるように利用者権限による論理的なアクセスコントロールに加え、必要に応じて端末の設置場所に物理的なアクセスコントロールを実施しなければならない。

５．情報資産の管理（学外持ち出し、学内持ち込み）

(1) 電子媒体の管理

装置及び電子記録媒体に記録されている情報の漏えい、改ざん、破壊を防止するため、電子記録媒体の利用、保管、破棄、持ち出しについて管理を実施しなければならない。

(2) 学外持ち出し手続、適切な取り扱い

学外への重要な情報資産の持ち出しについては、持ち出し手続きを定め、学外へ持ち出した情報資産が適切に取り扱われるようにしなければならない。

(3) 持出状況の把握・管理

情報の利用権限の無い者への情報の開示、情報の利用権限の無い者による情報の変更・窃盗を防止するため、情報資産の持出状況について把握し、管理しなければならない。

(4) 学外組織との情報のやり取り管理

情報資産の紛失、改ざん、誤用を防止するため、学外の組織との情報（ソフトウェア、電子記録媒体、電子商取引、情報公開等）のやり取りを管理しなければならない。

(5) 学内持込状況の把握・管理

情報の利用権限の無い者への情報の開示、情報の利用権限の無い者による情報の変更・窃盗を防止するため、個人・企業等が所有するコンピュータ機器及び可搬媒体の学外から事務室・研究室への持ち込みについて把握し、管理しなければならない。

(6) 個人所有ソフトウェア導入・利用の把握・管理

不正なソフトウェアの利用、コンピュータの誤動作を防止するため、個人所有するソフトウェアを学内のコンピュータへ導入、利用すること（原則禁止）を把握し、管理しなければならない。なお、実習室パソコンは、個人所有するソフトウェアを導入されても、電源オフ時に消去される。

6．情報システムの開発・運用・管理

(1) セキュリティ要件の明確化

新規に開発、あるいは変更を加える情報システムにおいて、必要な情報セキュリティを確保するため、業務要件定義の際、機能要件だけでなく、必要なセキュリティ要件を明確にし、その要件を確実にシステムへ反映しなければならない。

(2) 入力・処理・出力時の情報の完全性確保

情報システムの開発にあたっては、情報システムで取り扱う情報の完全性を確保するため、データ入力、処理、出力時に完全性を可能な限り確認しなければならない。

(3) コンピュータウィルス感染防止

コンピュータウィルスが情報システムで取り扱う情報の完全性を損なうことを防止するため、コンピュータウィルスに感染することを防止しなければならない。

(4) バックアップの取得・管理

インシデントが発生した場合、直ぐに情報システムのデータを戻して復旧できるようにするため、情報のバックアップを取得しなければならない。

(5) ネットワーク管理

公共のネットワークに接続する場合、通過するデータの機密性及び完全性を保護するため、ネットワーク機器の適切な設定・運用・管理を行わなければならない。

(6) 利用状況の記録・監視

情報システムの不正利用を早期に発見し、不正利用に起因する悪影響を最小化するため、情報

システムの利用状況を正しく記録し、監視を実施しなければならない。また、記録された利用状況は、定期的に確認しなければならない。規程に定めた情報セキュリティ組織より求めがあった場合、利用状況を報告しなければならない。

7．外部委託先の情報の取り扱い

外部委託先の情報セキュリティが確保されていないことに起因して、預託した情報が委託先から漏えいすること、及び、預託先で無断使用されることを防止するため、本学情報を預託する委託先に対しては、必要な対策を契約書に明記し、業務委託先での情報の取り扱い状況を監視しなければならない。

8．コンプライアンス

情報資産保護に関する法的要求事項及び本学規程等に準拠しなければならない。

9．啓発、教育

情報資産保護への認識不足から情報が漏えい、改ざん、破壊されることを防止するため、本学構成員への情報資産保護に関わる教育、訓練を実施しなければならない。

10. 自主点検

情報資産に対する保護対策が実施され有効に機能していることを確認するため、情報資産の所管責任者は、定期的に自主的な点検を実施しなければならない。

11. 例外事項

本学で定める情報資産保護対策の実施が、費用面、技術面で困難となるような例外的な事項が発生する場合、関係する情報資産の所管責任者が、計算センターへ報告しなければならない。計算センターは情報資産保護対策から逸脱した例外事項を取り纏めて整理しなければならない。

12. 評価・見直し

このガイドラインは、情報技術の発展、制定したガイドラインの実効性を評価し、遵守可能な内容を保持するため、定期的に見直し、改定を行う。

以上

平成 30 年 11 月 12 日制定

附　則

この規定は、令和 4 年 10 月 1 日から施行する。