学校法人愛知産業大学

情報セキュリティポリシー

施　行　令和２年２月26日

Ⅰ　情報セキュリティ基本方針

１　基本理念及び目的

学校法人愛知産業大学（以下「本法人」という。）において、健全な教育・研究活動を実践し、社会的責務を果たすためには、情報基盤の充実に加え、情報資産のセキュリティ確保が不可欠である。

そのために、本法人の教職員、学生その他本法人の構成員は、情報資産の価値を十分に認識し、本法人の情報資産を守るだけでなく、外部に対する不正な情報提供、情報資産の侵害等が行われないように努め、本法人における情報システムの信頼性を高めていかなければならない。

そこで、本法人においては、以下の（１）から（４）の実現を目的として「学校法人愛知産業大学情報セキュリティポリシー」（以下「本ポリシー」という。）を制定し、本法人の全構成員に周知を図ることとする。本法人の提供する情報資産に関連するサービスを利用する者は、本ポリシーを遵守する責任があり、意図の有無を問わず、本法人内部及び外部（以下「内外」という。）の情報資産に対する権限のないアクセス、改ざん、複写、破壊、漏えい等をしてはならない。

（１）本法人に対する情報セキュリティ侵害を阻止すること。

（２）内外の情報セキュリティを侵害する行為を抑止すること。

（３）情報資産の適切な管理・運用を行うこと。

（４）情報セキュリティ侵害の早期検出と迅速な対応を実現すること。

２　用語の定義

本ポリシーで使用する用語の定義は、以下のとおりとする。

（１）情報

本法人の教育・研究・管理運営に関わる者が作成し、又は収集及び取得した内容が記録された文書、電子文書、情報システム内のデータ、その他それに準ずるものをいう。

（２）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であり、本法人により所有又は管理されているもの及び本法人との契約又は他の協定に従って提供されるものをいい、本法人の情報ネットワークに接続される機器を含む。

（３）情報資産

情報及び情報を管理する仕組み（情報システム及びシステム開発、運用及び保守のための資料等）をいう。

（４）情報セキュリティ

情報資産の機密性、完全性及び可用性を維持すること。

① 機密性

情報資産にアクセスすることを許可された者だけが、情報資産にアクセスできることを確保すること。

② 完全性

情報資産が破壊、改ざん又は消去されていない状態を確保すること。

③ 可用性

情報資産にアクセスすることを許可された利用者が、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。

３ 対象範囲及び対象者

（１）本ポリシーの対象範囲は、次のとおりとする。

① 本法人が管理する情報資産

② 本法人の諸活動に伴い、業務委託先において取り扱われる情報資産

（２）本ポリシーの対象者は、本法人の情報資産を利用するすべての者（以下「利用者」という。）で、役員、教員（非常勤教員を含む。）、職員（嘱託職員、パート職員、派遣職員等を含む。）、共同研究者、学生（研究生、科目等履修生、特修生等を含む。）・生徒・園児等、委託業者、学外者等とする。

Ⅱ 情報セキュリティ対策基準

１ 趣旨

この対策基準は、基本方針の目的を達成するために、必要な体制、基準、指針等を定めるものとする。

２ 体制及び管理

（１）責任者、管理者等

本法人における情報セキュリティを確保するために、次のとおり定める。

① 情報セキュリティ最高責任者

本法人に情報セキュリティ最高責任者を置き、理事長をもって充てる。情報セキュリティ最高責任者は、本法人の情報セキュリティに関する総轄的な意思決定をし、内外に対する責任を負う。

② 情報セキュリティ実施責任者

本法人に情報セキュリティ実施責任者を置き、法人事務局においては法人事務

局長、設置校においては組織の長をもって充てる。情報セキュリティ実施責任者は、各部署の情報セキュリティに関する権限と責任を有する。

③　情報セキュリティ担当者

各部署に情報セキュリティ担当者を置き、次に掲げる者をもって充てる。情報セキュリティ担当者は、 個々の情報機器、ソフトウェア及び情報を管理・監督し、情報セキュリティを維持するための責任を負う。

ⅰ　大学・短期大学の教育研究組織

個々のクライアント機器により情報システムを利用する専任教員

ⅱ　大学・短期大学を除く設置校の教育研究組織

情報セキュリティ責任者が指名した者

ⅲ　事務組織

法人事務局及び大学は各課の長、大学以外の設置校は事務長

④　ネットワーク管理者

大学総務・広報部ＩＴサポート室にネットワーク管理者を置く。ネットワーク管理者は、基幹ネットワークと主要な業務用サーバを運用管理し、セキュリティを維持するための責任を負う。

⑤　研究室等において、利用者自らが直接管理する情報資産を持つ場合については、各利用者が、そのセキュリティに関する責任を負う。

（２）情報セキュリティ委員会

本法人における情報セキュリティ対策を推進し、本法人の情報システムの安全かつ適切な運用を図るため、情報セキュリティ委員会を置く。委員会は、情報セキュリティ最高責任者を委員長とし、委員は、情報セキュリティ実施責任者及びネットワーク管理者とする。

（３）情報の作成及び管理

①　情報を作成する者は、情報の作成時に当該情報の取扱制限を定めなければならない。

②　情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

③　情報資産が複製又は伝送された場合には、複製等された情報資産も管理しなければならない。

３　物理的セキュリティ

（１）情報システムの設置等

情報セキュリティ実施責任者は、サーバ機器等の重要な情報システム又は情報資産を、それぞれ設定された管理区域内に設置し、正当なアクセス権のない者が使用でき

ないよう、セキュリティ確保に努めなければならない。

（２）情報機器及び記録媒体の盗難対策

情報セキュリティ実施責任者は、情報機器及び記録媒体の盗難予防に努めなければならない。

（３）情報機器及び記録媒体の学外への持ち出し

利用者は、個人情報及び本法人の重要なデータが入った情報機器及び記録媒体を、原則として学外へ持ち出してはならない。情報セキュリティ実施責任者は、やむを得ず、情報機器又は記録媒体を学外へ持ち出すことを認める場合、情報の漏えいが発生しないよう、情報セキュリティ対策を講じなければならない。

（４）情報機器及び記録媒体の学内への持込み

利用者は、情報機器及び記録媒体を学内へ持ち込む場合は、ウィルスチェックを行う等の情報セキュリティ対策を講じなければならない。

（５）情報のバックアップ

利用者及びネットワーク管理者は、サーバ機器等に記録するデータを、必要に応じて定期的にバックアップしなければならない。

（６）情報機器及び記録媒体の処分

利用者は、情報機器及び記録媒体を破棄する場合、残存情報が第三者に読み取られることのないよう、情報セキュリティ対策を講じなければならない。

４　人的セキュリティ

（１）教育・研修

情報セキュリティ最高責任者は、情報セキュリティに関する啓発や教育を実施するため、必要な措置を講じるよう努めるものとする。

（２）利用者の義務

① 利用者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行にあたっては、本ポリシー及びその他関連法令等を遵守しなければならない。

② 利用者は、内外に対して、情報セキュリティを損ねる行為をしてはならない。

③ 利用者は、アクセス権限のない情報にアクセスしたり、許可されていない情報を利用してはならない。

（３）事故・障害時の報告・対応

① 利用者は、情報セキュリティに関する事故・障害及び公開情報の改ざん等を発見した場合には、直ちに情報セキュリティ実施責任者、情報セキュリティ担当者又はネットワーク管理者に報告しなければならない。

② ネットワーク管理者は、内外から情報システムの不正使用、情報資産の不正な利用等にかかわる苦情、通報等があった場合には、速やかに調査を行わなければならない。

③　ネットワーク管理者は、調査の結果、不正が確認されたときは、関係する通信の遮断、該当する情報システムの切離し等必要な措置を直ちに講じ、情報セキュリティ実施責任者に報告しなければならない。

④　情報セキュリティ実施責任者は、重大な事故が発生した場合は、情報セキュリティ最高責任者に報告しなければならない。

⑤　情報セキュリティ最高責任者は、重大な事故について審議する必要がある場合は、情報セキュリティ委員会を招集しなければならない。

（４）委託契約

情報システムの開発又は運用管理を外部委託する場合は、外部委託業者から再委託を受ける業者等も含め、 本ポリシーを遵守することを明記した契約を締結するものとする。

５　技術的セキュリティ

（１）不正アクセス等への対応

ネットワーク管理者は、不正アクセスの防止及び検出するための適切な手段を講じなければならない。

（２）アクセス制限

教育研究組織又は事務組織において、情報の内容に応じて、アクセス可能な利用者を定め、不正なアクセスを阻止するために必要なアクセス制限を行わなければならない。

（３）ログの保存

ネットワーク管理者は、システム等のアクセスログ、操作ログ等について、保存期間を定めて保存しなければならない。

（４）セキュリティの維持

ネットワーク管理者は、管理する機器・ソフトウェアについて、常にその構成を把握し、セキュリティに係る更新、ウィルス対策等適切なセキュリティの維持に努めなければならない。

６　違反者への措置

利用者が、本ポリシーに違反した場合には、法令、学校法人愛知産業大学就業規則、学則等に基づき、処分、その他の措置を行うことがある。

７　セキュリティポリシーの評価及び更新

セキュリティポリシーの実効性については、定期的に評価を行い、改善が必要と認められた場合は、セキュリティレベルの高い、かつ遵守可能なポリシーに更新しなければならない。