国立大学法人東京農工大学情報システム管理規程

平成１８年１２月２６日
１８　規程第３８号

（目的）

第 1 条　この規程は、国立大学法人東京農工大学（以下「本学」という。）情報システムの総合的な管理、運用及び利用について必要な事項を定めることにより、情報資産の安全性及び信頼性を確保し、もって本学の教育研究の充実及び事務の効率化に資することを目的とする。

（定義）

第 2 条　この規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

一　「情報資産」とは、情報及び情報を管理する仕組み（情報システム並びにシステム開発、運用及び保守のための資料等）を総称していう。

二　「情報システム」とは、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、これら全体で業務処理を行うものをいう。

三　「情報セキュリティ」とは、情報資産の機密性、安全性及び可用性を維持することをいう。

四　「情報セキュリティポリシー」とは、本学が所有する情報資産の情報セキュリティ対策について、総合的・体系的かつ具体的にとりまとめ、どのような情報資産をどのような脅威から、どのようにして守るかについての基本的な考え方並びに情報セキュリティを確保するための体制、組織及び運用を含めた規定をいう。

五　「最適化」とは、情報システムをその目的、性格等に応じて、最も効率的、合理的なものになるように見直すことをいう。

（管理）

第 3 条　本学情報システムの総合的な管理については、総合情報メディアセンターがこの任に当たる。

2　前項の規定にかかわらず、事務系情報システムの管理は、学術情報チームの協力を得て、当該事務系情報システムを主として運用する部署がその任に当たる。

（責任者）

第 4 条　本学の情報システムの分析、評価、最適化計画を策定する責任者として情報化統括責任者（以下「CIO」という。）を置き、CIO は学術研究担当副学長をもって充てる。

２　CIO は情報セキュリティ最高責任者（以下「CISO」という。）を兼ねる。

３　CIO を補佐する者として CIO 補佐を置き、CIO 補佐は総合情報メディアセンター長をもって充てる。

（情報セキュリティ対策）

第 5 条　CISO は、不正アクセス等により情報資産に被害が及ぶと判断した時ときは、緊急に情報システムの運用を停止または制限することができる。

２　情報セキュリティ対策の詳細は、別途定める本学情報セキュリティポリシーによるものとする。

（利用者の範囲）

第 6 条　本学の情報システムを利用することができる者（以下「利用者という。」）は、次の各号に掲げる者とする。

一　本学の役員

二　本学の教職員（非常勤を含む。）

三　本学の学生（研究生、聴講生、科目等履修生を含む。）

四　本学の来学者

五　前号に掲げる者の他、CIO が必要と認めた者

（利用者の自己管理）

第 7 条　利用者は次の各号に掲げる事態の発生を考慮し、情報のバックアップ、ウィルス対策及び修正プログラムの適用等、並びに情報機器の紛失防止対策等、自己の責任において適宜実行するものとする。

一　情報システム障害による情報の消失

二　ウィルス感染等による情報の消失、漏洩等

三　情報機器の盗難、紛失

（利用停止等）

第 8 条　CISO は利用者が次の各号に掲げるいずれかに該当するときは、利用資格の取消し若しくは使用の停止、又は制限等の措置を講じることができる。

一　本規程及び本学情報セキュリティポリシーを遵守しない者

二　その他本学情報システムの利用者として不適格であると認められる者

（事故・障害の連絡）

第９条　利用者は次の各号に掲げる状況に遭遇したときには、すみやかに CISO に連絡しなければならない。

一　本学情報システムの障害

二　データの盗聴及び改ざん

三　使用する情報機器の不審な動作

四　利用者でない者による情報システムへの接続

五　その他本規程に違反する行為等の発見

（その他）

第 10 条　本規程に定めのない事項については、本学大学情報委員会で協議して定めることとする。