秀明大学情報セキュリティポリシー

令和３年５月２６日

学校法人　秀明学園

１．目的

秀明大学（以下「本学」という。）は、本学が保有する情報資産を適正に運用するため、本学で扱う情報及び情報システムを対象とした情報セキュリティ対策を実施する。

２．方針

前条の目的を達するため、本学は情報セキュリティ対策基本規程（以下、「対策基本規程」という。）及びその他の規定等の定めるところにより、以下の対策を行う。

(1) 情報セキュリティ対策の実施体制の整備

(2) 情報及び情報システムの保護

(3) 情報システムや情報サービスの管理・運用

(4) 情報セキュリティインシデントへの対処

(5) 利用者への啓発・教育

(6) (1)～(5)を含む情報セキュリティマネジメントの実施

３．義務

本学の情報及び本学で扱う情報システムを利用する者、管理・運用の業務に携わる者は、本方針、対策基本規程及びその他の規程等を遵守しなければならない。

４．罰則

本方針に基づき定められる規程等に違反した場合の利用の制限および罰則は、秀明大学学則及び本学が定める就業規則に則って行うほか、それぞれの規程に定めるところによる。

以　上

秀明大学情報セキュリティ対策基本規程

第一条　（目的）

本規程は、秀明大学（以下「本学」という。）における情報及び情報システムの情報セキュリティ対策について基本的な事項を定め、本学の保有する情報の保護と活用及び情報セキュリティ水準の適切な維持向上を図ることを目的とする。

第二条　（適応範囲）

本規程において適用対象とする者は、本学情報システムを運用・管理するすべての者、並びに利用者及び臨時利用者とする。

２　本規程において適用対象とする情報は、以下とする。

一 教職員等が職務上使用することを目的として本学が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）

二 その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、教職員等が職務上取り扱う情報

三 第一号及び及び第二号のほか、本学が調達し、又は開発した情報システムの設計又は運用管理に関する情報

３　本規程において適用対象とする情報システムは、本規程の適用対象となる情報を取り扱う全ての情報システムとする。

第三条　（用語定義）

本規程において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

一 外部委託

本学の情報処理業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。

二 学生等

本学学則に定める学生、研究生、研究員、研修員並びに研究者等、その他、部局総括責任者が認めた者をいう。

三　教職員等

本学を設置する法人の役員及び、本学に勤務する常勤又は非常勤の教職員（派遣職員を含む）その他、部局総括責任者が認めた者をいう。教職員等には、個々の勤務条件にもよるが、例えば、派遣労働者、一時的に受け入れる研修生等も含まれるものとする。

四　情報システム

ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、本学が調達又は開発するもの（管理を外部委託しているシステムを含む。）若しくは本学情報ネットワークに接続されるものをいう。

五　端末

情報システムの構成要素である機器のうち、利用者が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。端末には、モバイル端末も含まれる。

六　通信回線

複数の情報システム又は機器等（本学が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、本学の情報システムにおいて利用される通信回線を総称したものをいう。

七　通信回線装置

通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。

八　利用者

教職員等及び学生等で、本学情報システムを利用する許可を受けて利用するものをいう。

九　臨時利用者

教職員等及び学生等以外の者で、本学情報システムを臨時に利用する許可を受けて利用するものをいう。

第四条　（全学総括責任者）

本学における情報セキュリティに関する事務を統括する全学総括責任者を置く。学長がこれを任命する。

二　全学総括責任者は、全学総括責任者を助けて本学における情報セキュリティに関する事務を整理し、全学総括責任者の命を受けて本学の情報セキュリティに関する事務を統括する全学総括副責任者１人を必要に応じて置くことができる。

三　全学総括責任者は、次に掲げる事務を統括する。

1 情報セキュリティ対策推進のための組織・体制の整備

2 情報セキュリティ対策基準の決定、見直し

3 対策推進計画の決定、見直し

4 情報セキュリティインシデントに対処するために必要な指示その他の措置

5 前各号に掲げるもののほか、情報セキュリティに関する重要事項

第五条　（全学実施責任者・部局総括責任者の設置）

全学総括責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、情報セキュリティ対策に関する事務を統括する者として、部局総括責任者１人を置く。そのうち、部局総括責任者を統括し、全学総括責任者及び全学総括副責任を補佐する者として、全学実施責任者１人を選任する。

二　全学実施責任者は、命を受け、次の事務を統括すること。

1 要管理対策区域の決定並びに当該区域における施設及び環境に係る対策の決定

2 情報セキュリティ対策に関する実施手順の整備及び見直し並びに実施手順に関する事務の取りまとめ

3 情報セキュリティ対策に係る教育実施計画の策定及び当該実施体制の整備

4 例外措置の適用審査記録の台帳整備等

5 情報セキュリティインシデントに対処するための緊急連絡窓口の整備等

6 前各号に掲げるもののほか、情報セキュリティ対策に係る事務

三 部局総括責任者は、命を受け、管理を行う組織のまとまりにおける情報セキュリティ対策を推進するため、次の事務を統括する。

1 必要な場合、定められた区域ごとの区域部局総括責任者の設置

2 情報システムごとの部局技術責任者の設置

3 情報セキュリティインシデントの原因調査、再発防止策等の実施

4 情報セキュリティに係る自己点検計画の策定及び実施手順の整備

5 前各号に掲げるもののほか、管理を行う組織のまとまりの情報セキュリティ対策に関する事務

第六条 （情報セキュリティインシデントに備えた体制の整備）

全学総括責任者は、CSIRT(Computer Security Incident Response Team)を整備し、その役割を明確化する。

二 全学総括責任者は、教職員等のうちから CSIRT に属する職員として専門的な知識又は適性を有すると認められる者を選任する。そのうち、本学における情報セキュリティインシデントに対処するための責任者として CSIRT 責任者を置くこと。また、CSIRT 内の業務統括及び外部との連携等を行う教職員等を定めること

三 全学総括責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備すること。

四 全学総括責任者は、以下を含む CSIRT の役割を規定する。

1 本学に関わる情報セキュリティインシデント発生時の対処の一元管理

・全学における情報セキュリティインシデント対処の管理

・情報セキュリティインシデントの可能性の報告受付

・本学における情報セキュリティインシデントに関する情報の集約

・情報セキュリティインシデントの全学総括責任者等への報告

・情報セキュリティインシデントへの対処に関する指示系統の一本化

2 情報セキュリティインシデントへの迅速かつ的確な対処

・情報セキュリティインシデントであるかの評価

・被害の拡大防止を図るための応急措置の指示又は勧告を含む情報セキュリティインシデントへの対処全般に関する指示、勧告又は助言

・文部科学省への連絡

・外部専門機関等からの情報セキュリティインシデントに係る情報の収集

・他の機関等への情報セキュリティインシデントに係る情報の共有

・情報セキュリティインシデントへの対処に係る専門的知見の提供、対処作業の実施

以上

令和 3 年 5 月 26 日施行