

## 公立鳥取環境大学情報システム運用基本規程

平成28年4月1日  
公立鳥取環境大学規程第53号

### (目的)

第1条 この規程は、公立鳥取環境大学（以下「本学」という。）における情報システムの運用及び管理について必要な事項を定め、もって本学の情報の保護と活用及び適切な情報セキュリティ対策を図ることを目的とする。

### (適用範囲)

第2条 本規程の適用範囲は、公立鳥取環境大学情報セキュリティ基本方針第4条に定めるものとする。

### (定義)

第3条 本規程における用語を以下に定める。

(1) 情報システム

公立鳥取環境大学情報セキュリティ基本方針第2条に定めるものとする。

(2) 情報資産

公立鳥取環境大学情報セキュリティ基本方針第3条に定めるものとする。

(3) ポリシー

本学が定める「情報セキュリティ基本方針」及び「情報システム運用基本規程」をいう。

(4) 実施規定

ポリシーに基づいて策定される規程、細則、内規等及び、基準、計画をいう。

(5) 手順

実施規定に基づいて策定される具体的な手順やマニュアル、ガイドラインを指す。

(6) 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。

(7) 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、全学情報システム総括責任者が認めた者をいう。

(8) 学生等

本学学則に定める学部学生、大学院学生、研究生、研究者等、その他、全学情報システム総括責任者が認めた者をいう。

(9) 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。

(10) 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をいう。

(1 1) 電磁的記録

電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、コンピュータによる情報処理の用に供されるものをいう。

(1 2) 情報セキュリティインシデント

情報セキュリティに関し、意図的または偶発的に生じる、本学規程または法律に反する事故あるいは事件、その他情報資産保全への障害を与えるものをいう。

(1 3) CSIRT (シーサート)

本学において発生した情報セキュリティインシデントに対処するため、本学に設置された体制をいう。Computer Security Incident Response Team の略。

(1 4) 明示等

情報を取り扱うすべての者が当該情報の格付けについて共通の認識となるように措置することをいう。

(15) 部局

学部、研究科、各センター、事務局をいう。

(全学情報システム総括責任者)

第4条 本学情報システムの運用に責任を持つ者として、本学に全学情報システム総括責任者を置く。全学情報システム総括責任者は、学長が指名する。

2 全学情報システム総括責任者は、ポリシー及びそれに基づく規程の決定や情報システム上での各種問題に対する処置を行う。

3 全学情報システム総括責任者は、全学の情報基盤として供される本学情報システムのうち情報セキュリティが侵害された場合の影響が特に大きいと評価される情報システムを指定することができる。この指定された情報システムを「全学情報システム」という。

4 全学情報システム総括責任者は、全学向け教育及び全学情報システムを担当する部局情報システム技術担当者向け教育を統括する。

5 全学情報システム総括責任者に事故があるときは、全学情報システム総括責任者があらかじめ指名する者が、その職務を代行する。

6 全学情報システム総括責任者は、情報セキュリティに関する専門的な知識及び経験を有した専門家を情報セキュリティアドバイザーとして置くことができる。

(全学情報システム実施責任者)

第5条 本学に全学情報システム実施責任者を置く。全学情報システム実施責任者は全学情報システム総括責任者が推挙し、学長が指名する。

2 全学情報システム実施責任者は、全学情報システム総括責任者の指示により、本学情報システムの整備と運用に関し、ポリシー及びそれに基づく実施規定並びに手順等の実施を行う。

3 全学情報システム実施責任者は、情報システムの運用に携わる者及び利用者に対して、情報

システムの運用並びに利用及び情報システムのセキュリティに関する教育を企画し、ポリシー及びそれに基づく実施規定並びに手順等の遵守を確実にするための教育を実施する。

- 4 全学情報システム実施責任者は、本学の情報システムのセキュリティに関する連絡と通報において本学情報システムを代表する。

(部局情報システム実施責任者)

第6条 各部局に部局情報システム実施責任者を置く。部局情報システム実施責任者は、部局長が指名する。

- 2 部局情報システム実施責任者は、全学情報システム実施責任者の指示に基づき部局における情報システム上での各種問題に対する処置を担当する。

(部局情報システム技術担当者)

第7条 部局情報システム実施責任者は、当該部局の情報システムの管理業務において必要な単位ごとに、部局情報システム技術担当者を置く。部局情報システム技術担当者は部局情報システム実施責任者が推挙し、部局長が任命する。なお、部局情報システム実施責任者自ら部局情報システム技術担当者を兼務することができる。

- 2 部局情報システム技術担当者は、部局情報システム実施責任者の指示により、部局の情報システムの運用の技術的実務を担当し、利用者への教育を補佐する。

(情報セキュリティ監査責任者)

第8条 本学に情報セキュリティ監査責任者を置く。学長がこれを任命する。

- 2 情報セキュリティ監査責任者は、本学の情報セキュリティの監査に関する事務を統括する。

(管理運営部局)

第9条 本学情報システムの管理運営部局を情報メディアセンターとする。

- 2 管理運営部局に管理運営部局長を置き、情報メディアセンター長をもって充てる。

(管理運営部局が行う事務)

第10条 管理運営部局は、全学情報システム実施責任者の指示により、以下の各号に定める事務を行う。

- (1) 全学情報システム運用委員会の運営に関する事務
- (2) 本学情報システムの運用と利用におけるポリシーの実施状況の取りまとめ
- (3) 講習計画、リスク管理及び非常時行動計画等の実施状況の取りまとめ
- (4) 本学の情報システムのセキュリティに関する連絡と通報

(全学情報システム運用委員会)

第11条 本学情報システムの円滑な運用のため、本学に全学情報システム運用委員会を置く。

2 全学情報システム運用委員会に関する規程は、別に定める。

(情報セキュリティインシデントに備えた体制の整備)

第12条 全学情報システム総括責任者は、CSIRTを整備し、その役割を明確化する。

- 2 全学情報システム総括責任者は、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。
- 3 全学情報システム総括責任者は、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。

(CSIRTの役割)

第13条 CSIRTの役割を次の各号のとおり定めるものとする。

- (1) 報告窓口からの情報セキュリティインシデントの報告の受付
  - (2) 情報セキュリティインシデントの全学情報システム総括責任者等への報告
  - (3) 対外的な連絡
  - (4) 被害の拡大防止を図るための応急措置の指示又は勧告
  - (5) その他全学情報システム総括責任者が必要と認める事項
- 2 CSIRT責任者の指示により実務を担当する者(CSIRT代表者(PoC(Point of Contact)))を置く。CSIRT代表者はCSIRT責任者が推挙し、全学情報システム総括責任者が指名する。

(役割の分離)

第14条 情報セキュリティ対策の運用において、承認又は許可事案の申請者とその承認又は許可を行う者(以下、本項において「承認権限者等」という。)若しくは監査を受ける者とその監査を実施する者は、その役割を同じ者が兼任してはならない。

- 2 前項の定めに係わらず、教職員等は、承認権限者等が有する職務上の権限等から、当該承認権限者等が承認又は許可(以下「承認等」という。)の可否の判断を行うことが不適切と認められる場合には、当該承認権限者等の上司に承認等の申請をする。この場合において、当該承認権限者等の上司の承認等を得たときは、当該承認権限者等の承認等を得ることを要しない。
- 3 教職員等は、前項の場合において承認等を与えたときは、承認権限者等に係る遵守事項に準じて、措置を講ずる。

(情報の格付け)

第15条 全学情報システム運用委員会は、情報システムで取り扱う情報について、電磁的記録については機密性、完全性及び可用性の観点から、書面については機密性の観点から当該情報の格付け及び取扱制限の指定並びに明示等の規定を整備する。

(本学外の情報セキュリティ水準の低下を招く行為の防止)

第16条 全学情報システム実施責任者は、本学外の情報セキュリティ水準の低下を招く行為の防止に関する措置について規定を整備する。

2 本学情報システムを運用・管理する者、並びに利用者及び臨時利用者は、本学外の情報セキュリティ水準の低下を招く行為の防止に関する措置を講ずる。

(情報システム運用の外部委託管理)

第17条 全学情報システム総括責任者は、本学情報システムの運用業務の全て又はその一部を第三者に委託する場合には、当該第三者による情報セキュリティの確保が徹底されるよう必要な措置を講じるものとする。

(情報セキュリティ監査)

第18条 情報セキュリティ監査責任者は、情報システムのセキュリティ対策がポリシーに基づく手順に従って実施されていることを監査する。情報セキュリティ監査に際しては、別途定める。

(見直し)

第19条 全学情報システム運用委員会は、ポリシー、実施規定及び手順等の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行う。

2 本学情報システムを運用・管理する者、並びに利用者及び臨時利用者は、自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には、当該事項の見直しを行う。

(諸規程等の準用)

第20条 この規程に定めるほか、必要な事項は、本学関係規則およびその他の諸規程を準用する。

(委任)

第21条 この規程に定めるもののほか、必要な事項は、学長が別に定める。

附 則

この規程は、平成28年4月1日から施行する。

附 則

この規程は、令和5年4月1日から施行する。