

国立大学法人京都教育大学情報システム運用基本規程

平成20年 4月 9日 制定
令和 4年 3月 1日 最終改正

(目的)

第1条 本規程は、国立大学法人京都教育大学（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基本的事項を定め、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 本規程は、本学情報システムを運用・管理する全ての者及び利用者並びに間接利用者に適用する。

(定義)

第3条 本規程において、次の各号に掲げる用語の定義は、それぞれ当該各号の定めるところによる。

一 情報システム

情報処理及び情報ネットワークに係わるシステムで、次のものをいい、学内情報ネットワークに接続する機器を含む。

イ 本学により、所有又は管理されているもの

ロ 本学との契約あるいは他の協定に従って提供されるもの

二 情報

情報とは次のものをいう。

イ 情報システム内部に記録された情報

ロ 情報システム外部の電磁的記録媒体に記録された情報

ハ 情報システムに関係がある書面に記載された情報

三 情報ネットワーク

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情報ネットワークを総称したものをいう。情報ネットワークには、本学が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。

四 学内情報ネットワーク

本学が管理するサーバ装置又は端末の間の通信の用に供する情報ネットワークであって、本学の管理下でないサーバ装置又は端末が論理的に接続されていないものをいう。学内情報ネットワークには、物理的な回線を本学が管理していないもの（専用線やVPN等）も含まれる。

五 情報資産

情報システム並びに情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいう。

六 ポリシー

本学情報システム運用基本方針及び本規程をいう。

七 実施規程等

ポリシーに基づいて策定される規程，基準及び計画をいう。

八 手順

実施規程等に基づいて策定される具体的な手順，マニュアル及びガイドラインをいう。

九 利用者

役員，教職員等，学生等，特別利用者及び臨時利用者で，全学実施責任者の許可を受け，本学情報システムを利用する次のものをいう。

イ 役員とは，本学組織運営規則第4条に定める者をいう。

ロ 教職員等とは，本学組織運営規則第5条第1項に定める者及び派遣職員等それに準じる者をいう。

ハ 学生等とは，本学学則第4条第1項に定める組織に属する学生及び学内諸規定に定める学生等並びにそれに準じる者をいう。

ニ 特別利用者とは，本学に所属をしていないが，本学の活動に不可分な個人又は団体のうち，全学実施責任者が認めた者をいう。

ホ 臨時利用者とは，イ～ニに掲げる以外の者で，本学情報システムを臨時に利用するものをいう。

十 間接利用者

役員又は教職員等の監督下において本学情報システムを利用させることができるものをいう。

イ 外部委託契約等において委任等を受けた者

ロ 本学附属学校園に在籍する幼児，児童，生徒

ハ その他 全学実施責任者に予め許可を受けた者

十一 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。

十二 電磁的記録

電子的方式，磁氣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。

十三 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，学内諸規程または法律に反する事故あるいは事件をいう。

十四 CSIRT (Computer Security Incident Response Team)

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，本学に設置する体制をいう。

十五 例外措置

役員及び教職員等がその職務において，ポリシー，実施規程等及び手順を遵守することが困難な状況で，本学の教育及び研究並びに大学の業務において適正な遂行を継続するため，遵守事項とは異なる代替の方法を採用し，又は遵守事項を実施しないこ

とについて合理的理由がある場合に、そのことについて申請し許可を得た上で適用する行為をいう。

十六 外部委託

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

十七 約款による外部サービス

民間事業者等の学外の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものをいう。ただし、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除くものとする。

(全学総括責任者)

第4条 本学情報システムの運用に責任を持つ者として、本学に全学総括責任者を置き、情報化推進委員会の委員長をもって充てる。

- 2 全学総括責任者は、ポリシー及び実施規程等の策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 全学総括責任者は、情報セキュリティに関する教育を統括する。
- 4 全学総括責任者は、ポリシー及び実施規程等への違反行為への対処を行う。
- 5 全学総括責任者は、最高情報責任者（CIO）及び最高情報セキュリティ責任者（CISO）を兼ねる。
- 6 全学総括責任者は、前項の業務を補佐するため、最高情報責任者補佐及び最高情報セキュリティ責任者補佐を指名する。
- 7 全学総括責任者に事故があるときは、全学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。

(情報システム等に関する委員会)

第5条 本学情報システムの円滑な運用のため、情報化推進委員会において、情報システムの運用・管理及びセキュリティに関する決定を行う。

(全学実施責任者)

第6条 本学に全学実施責任者を置き、情報化推進委員会の副委員長をもって充てる。

- 2 全学実施責任者は、全学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、実施規程等及び手順を実施する。
- 3 全学実施責任者は、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、実施規程等及び手順の遵守を確実にするための教育を実施する。
- 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において本学情報システムを代表する者は、全学実施責任者とする。
- 5 全学実施責任者は、本学における情報セキュリティ対策に関する実施手順を整備し、整備状況について全学総括責任者に報告する。

(全学情報システム)

第7条 情報化推進委員会は、全学の情報基盤となる情報システムを指定し、その管理運営部局を定める。

(部局総括責任者)

第8条 部局及び部局総括責任者を次の各号のとおり定める。

- 一 事務局 事務情報化推進専門部会委員長
- 二 前号以外 情報処理センター運営委員会委員長

2 部局総括責任者は、前項に定める部局の運用方針の決定や情報システムに関する各種問題に対する処置を担当する。

(情報システム管理責任者)

第9条 各情報システムの管理運用を図るため学科、事務局等の管理組織ごとに情報システム管理責任者を置き、部局総括責任者が選任する。

2 情報システム管理責任者は、情報システムの構成、運用方針の決定や情報システム上での問題に対する処置を担当する。

(技術担当者)

第10条 情報システム管理責任者は、情報システムの管理業務において必要な単位ごとに、技術担当者を置く。技術担当者は情報システム管理責任者が選任し部局総括責任者に報告する。なお、情報システム管理責任者自ら技術担当者を兼務することができる。

2 技術担当者は、情報システム管理責任者の指示により、各情報システムの運用を担当する。

(区域情報セキュリティ責任者の設置)

第11条 全学総括責任者は、施設及び環境に係る対策を行う単位ごとの区域を定め、その区域ごとに、区域情報セキュリティ責任者を置く。それぞれ本学資産監守要領第3条に定める区分及び補助執行者をもって充てる。

2 区域情報セキュリティ責任者は、定められた区域における施設及び環境に係る情報セキュリティ対策を行う。

(職場情報セキュリティ責任者の設置)

第12条 全学総括責任者は、学科、事務局等の管理組織ごとに、職場情報セキュリティ責任者を置き、学科主任、連合教職実践研究科の系主任、本学組織運営規則第12条第1項一号、四～七号及び第2項並びに第3項各号の教育研究施設等の長、事務局長をもって充てる。

2 職場情報セキュリティ責任者は、学科、事務局等の管理組織における情報の取扱いその他の情報セキュリティ対策に関する事務を総括する。

(全学情報セキュリティアドバイザーの設置)

第13条 全学総括責任者は、情報システム及び情報セキュリティ等に関する専門的な知識及び経験を有する者を全学情報セキュリティアドバイザーとして選任する。

2 全学情報セキュリティアドバイザーは、全学総括責任者の求めに応じ、情報セキュリティ対策への助言又は支援等を行う。

(CSIRTの設置)

第14条 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とともに、情報セキュリティインシデントの発生時に迅速かつ円滑な対応を図るため、CSIRTを設置し、その役割を明確化する。また、CSIRTの活動が円滑に行えるよう、環境を整えるものとする。

(CSIRT の組織)

第15条 CSIRT は、次の各号により組織する。

- 一 CSIRT 責任者 全学総括責任者をもって充て、CSIRT の業務を統括するとともに、学内外の関係機関と情報共有に関する活動の責任者を務める。
 - 二 担当者 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し、委嘱する。
- 2** CSIRT 責任者は、必要があると認めるときは、前項第二号に掲げた以外の者を指名して担当者に加えることができる。
- 3** CSIRT 責任者は担当者の中から、1 名以上の CSIRT 副責任者を指名する。CSIRT 副責任者は CSIRT 責任者から委譲を受けた場合に CSIRT 責任者の業務を代行することができる。

(CSIRT の役割及び情報セキュリティインシデントへの対処)

第16条 CSIRT の役割及び情報セキュリティインシデントへの対処は、「情報システム運用・管理基準」及び「インシデント対応手順」による。

(役割の分離)

第17条 情報セキュリティ対策の運用において、次の各号に掲げる役割を同じ者が兼務しない。

- 一 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
- 二 監査を受ける者とその監査を実施する者

(情報の格付及び取扱いに係る基準)

第18条 全学総括責任者は、情報システムで取り扱う情報について、情報化推進委員会における審議のうえ、情報の格付及び取扱いに関する基準を整備する。

(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19条 全学総括責任者は、情報化推進委員会における審議のうえ、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関する「学外情報セキュリティ水準低下防止基準」を整備する。

(外部委託)

第20条 全学総括責任者は、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。

- 2** 全学総括責任者は、情報化推進委員会における審議のうえ、次の各号の外部委託に関する基準等を「情報システム運用・管理基準」において整備する。なお、定めのないものについては、情報化推進委員会において定める。
- 一 委託先によるアクセスを認める情報及び情報システムの範囲
 - 二 約款による外部サービスの利用
 - 三 ソーシャルメディアサービスによる情報発信
 - 四 クラウドサービス（民間事業者が提供するものに限らず、政府等が提供するものを含む。以下同じ。）の利用

(対策推進計画)

第21条 全学総括責任者は、情報化推進委員会における審議のうえ、情報セキュリティ対

策を総合的に推進するための計画（以下「対策推進計画」という。）を定める。また、対策推進計画には、本学の業務、取り扱う情報及び保有する情報システムに関する全体方針のほか、情報セキュリティ対策に関する教育、自己点検、監査、技術的取組、重要な取組の方針や時期を含める。

- 2 全学総括責任者は、情報セキュリティ対策の運用及び点検・監査等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、対策推進計画について定期的に、かつ必要に応じて見直しを行う。

（例外措置手続）

第22条 全学総括責任者は、例外措置の適用の申請を審査する者を選任する。

- 2 例外措置の運用等については、「情報システム運用・管理基準」による。

（情報セキュリティ対策に係る教育）

第23条 全学総括責任者は、利用者に対して、ポリシー、実施規程等及び手順に係る教育を適切に受講させなければならない。

- 2 全学実施責任者は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、その実施体制を整備しなければならない。
- 3 全学実施責任者は、CSIRT 構成員及びシステムを運用・管理する者に対して、教育を適切に受講させなければならない。
- 4 全学実施責任者は、全学総括責任者及び情報化推進委員会に対して、教育啓発対象者の情報セキュリティ対策の教育の実施状況について報告する。

（自己点検計画）

第24条 全学実施責任者は、対策推進計画に基づき年度自己点検計画を策定し、実施手順を整備しなければならない。

- 2 全学実施責任者は、年度自己点検計画に基づき、利用者に自己点検を実施させなければならない。
- 3 全学総括責任者は、自己点検結果の分析及び評価に基づき、明らかになった問題について、全学実施責任者や及び部局総括責任者に改善を指示し、改善結果の報告をさせなければならない。

（通信の監視）

第25条 情報システムを運用・管理する者及び利用者は、情報ネットワークを通じて行われる通信を傍受してはならない。なお、全学総括責任者又は当該情報ネットワークを管理する情報システム管理責任者は、セキュリティ確保のため、あらかじめ指定した者に、情報ネットワークを通じて行われる通信の監視を行わせることができる。

（情報セキュリティ監査責任者）

第26条 情報セキュリティ監査責任者を置き、内部監査室長をもって充てる。

（情報セキュリティ監査）

第27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は、国立大学法人京都教育大学内部監査規則に基づき行う。

- 2 全学総括責任者は、対策推進計画に基づき、情報セキュリティ監査責任者に対して、監査実施計画の策定及び実施を依頼することができる。

3 全学総括責任者は、情報セキュリティの状況変化に応じて必要と判断した場合、情報セキュリティ監査責任者に対して、対策推進計画で計画された以外の監査の実施を依頼することができる。

4 全学総括責任者は、情報セキュリティ監査責任者に情報セキュリティ監査についての報告を求めることができる。

(情報セキュリティ監査実施者)

第28条 情報セキュリティ監査責任者は、監査業務の実施において必要となる者を、情報セキュリティ監査実施者として、被監査部門から独立した者を選任する。

2 情報セキュリティ監査責任者は、必要に応じて、学外の者に監査の一部を請け負わせることができる。

(見直し)

第29条 全学総括責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、ポリシー、実施規程等及び手順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。

(その他)

第30条 その他、本学におけるシステムの運用管理及び情報システムを運用・管理する者に関する事項は、「情報システム運用・管理基準」において別に定める。

附 則

この規程は、令和2年 4月 1日から施行する。

附 則

この規程は、令和4年 4月 1日から施行する。