京都府立医科大学情報システム運用基本規程

平 成 ３ １ 年 ２ 月 ４ 日
京都府立医科大学規程第３７５号

（目的）
第１条　京都府立医科大学情報システム運用基本規程（以下、「本規程」という。）は、京都府立医科大学（以下、「本学」という。）におけるすべての情報システムの運用と管理について必要な事項を定め、本学の保有する情報資産の保護と活用を図ることを目的とする。

（定義）
第２条　本規程において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。
(1)　情報セキュリティ
　情報資産の機密性を保持し、正確性、完全性及び許可された利用者が必要なときに情報資産を利用できる状態が維持されていることをいう。
(2)　情報資産
　情報システム及び情報システムに関連するすべてのデータをいう。
(3)　アクセス制御
　特定の情報資産、あるいは特定の情報資産を扱う情報システムへの接続の可否について制御する機能をいう。
(4)　個別システム運用規程（以下、「運用規程」という。）
　基本方針及び本規程等で定められた内容を、個々の情報システム又は業務においてどのような手順で実施していくのかを示したものをいう。
(5)　情報セキュリティ監査
　情報セキュリティ対策が遵守されていることを検証するための監査をいう。
(6)　その他の用語の定義は、基本方針の定めるところによる。

（情報システム運用管理の組織・体制）
第３条　本学の情報システムの運用・管理に関する組織・体制を次の各号のとおり定める。
(1)　本学に総合情報センター（以下、「センター」という。）を設置する。センターは、本学における高度情報化の総合的かつ効率的な推進を図るものとする。

(2)　センターの運営に関する重要事項を審議するため、総合情報化推進委員会（以下、「推進委員会」という。）を置く。
(3)　センター業務の学内調整のため、総合情報化推進調整会議（以下、「調整会議」という。）を置く。
(4)　センター、推進委員会及び調整会議については、別に定める。
(5)　学内の情報システム総括責任者を定める。
ア　情報システム総括責任者を総合情報センター長とする。
イ　情報システム総括責任者は、情報システムの管理・運用と情報セキュリティ管理を総括する。
ウ　情報システム総括責任者は、大学の情報システムに障害が発生した際には、迅速に対応するものとする。
エ　情報システム総括責任者は、大学の情報システムに関する総括的、緊急的権限と責任を有する。
(6)　学内の情報セキュリティ管理者を定める。
ア　情報セキュリティ管理者を総合情報センター副センター長（情報リテラシー教育部門担当教員）とする。
イ　情報セキュリティ管理者は、大学の組織的な情報セキュリティが適正に管理されるために必要な情報セキュリティの啓発等を講じる。
ウ　情報セキュリティ管理者は、情報システム管理者から、大学の情報セキュリティに係る障害発生の報告があった場合は、速やかに、情報システム総括責任者に報告し、情報システム管理者と連携して障害復旧策を講じる。
なお、重大な障害の場合は、推進委員会に報告するものとする。
エ　情報セキュリティ管理者は、情報システム総括責任者と協議の上、大学の情報セキュリティに関する業務を実施する権限と責任を有する。
(7)　学内の情報システム管理者を定める。
ア　情報システム管理者を総合情報センター副センター長（企画・学内ＬＡＮ担当教員）とする。
イ　情報システム管理者は、大学全体の情報システムの適正な運用を図るため、個別システム管理者（本条（９）参照）に必要な運用規程の策定を指示し、適正に遂行されているかを管理する。
ウ　情報システム管理者は、情報システム総括責任者と協議の上、大学全体の情報システムに係る開発、設定の変更、運用、更新、個別システム導入の承認等を行う権限と責任を有する。
(8)　各所属の情報セキュリティ責任者を定める。
ア　各所属の長を当該組織の情報セキュリティに関する権限及び責任を有

する情報セキュリティ責任者とする。

イ　所属とは、各事務部門、各教室（部門のある場合は各部門）、各講座、中央研究室、附属病院の各部（中央部門を含む。）・各診療科並びに附属北部医療センター、最先端がん治療研究センター及び附属脳・血管系老化研究センター等、情報資産を保有する組織とする。

ウ　所属の長とは前号に規定する所属の教授、教室管理者、研究部門長、又は課長等の責任者をいう。

エ　情報セキュリティ責任者は、各所属において、対策基準及び運用規程が遵守されるよう必要な措置を講じるものとする。

(9)　学内の個別システム管理者を定める。

ア　各情報システムを所管する情報セキュリティ責任者を当該情報システムの個別システム管理者とする。

イ　個別システム管理者は、所管するシステムの適正な運用を図るために必要な運用規程を策定し、維持・管理するものとする。

ウ　個別システム管理者は、所管する情報システムに係る開発、設定の変更、運用、更新等を行う。

エ　個別システム管理者は、所管する情報システムに係る情報セキュリティに関する権限及び責任を有する。

（情報セキュリティ対策の推進）

第４条　センターは、センター長を最高情報セキュリティ責任者としてセキュリティ対策を推進することとし、重要事項については、学長を委員長とする推進委員会で協議する。

２　情報セキュリティ対策は、情報資産の重要度に応じ、次の各号に掲げる対策を講じるものとする。

(1)　人的セキュリティ対策

情報セキュリティに関する権限、責任を定めることや、すべての利用者等に対して情報セキュリティ対策の内容を周知徹底するための教育、啓発等の対策

(2)　物理的セキュリティ対策

情報システムの設置場所について、不正な立ち入り、損傷及び妨害から情報資産を保護するため、管理区域を設置するなどの物理的な対策

また、固定的に設置されている情報機器のほか、持ち運びを前提としたノートパソコン等の管理にも十分に配慮すること。

(3)　技術的セキュリティ対策

情報資産を不正なアクセス等から保護するため、情報資産へのアクセス

制御、ネットワーク管理等の対策

(4)　運用におけるセキュリティ対策

セキュリティ対策の遵守状況の確認、情報システムの監視等の対策

(5)　緊急時におけるセキュリティ対策

緊急事態が発生した際に、迅速な対応を可能とするための計画を定める等の危機管理対策

（情報セキュリティ対策基準の策定）

第５条　推進委員会は、本規程に基づき、情報セキュリティ対策を実施するに当たっての遵守すべき事項や判断等の統一的な基準として「対策基準」を定める。

（情報セキュリティ監査及び評価、見直しの実施）

第６条　推進委員会は、情報セキュリティ対策が遵守されていることを検証するため、定期及び随時の監査を実施し、その結果等を踏まえ、本方針等及び運用規程（以下、「基本方針等」という。）に定められた事項並びに情報セキュリティ対策について評価を行い、必要に応じて基本方針等の見直しを行う。

附　　則

（施行期日）

１　この規程は、平成 31 年 2 月 4 日から施行する。