国立大学法人滋賀医科大学情報セキュリティ対策基本規程

令和５年４月１日制定
令和５年７月 28 日改正

（目的）

第１条　この規程は，国立大学法人滋賀医科大学（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の基本的な事項を定め，もって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。

（適用範囲）

第２条　この規程において適用対象とする者は，すべての教職員等，並びに本学の情報システムの利用者及び臨時利用者とする。

２　この規程において適用対象とする情報は，次の各号に掲げるとおりとする。

(1)　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

(2)　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であって，教職員等が職務上取り扱う情報

(3)　前２号に規定するもののほか，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　この規程において適用対象とする情報システムは，この規程の適用対象となる情報を取り扱うすべての情報システムとする。

（用語定義）

第３条　この規程において，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。

(1)　外部サービス

学外の者が一般向けに情報システムの一部又は全部の機能を提供するものをいう。ただし，当該機能において本学の情報が取り扱われる場合に限る。

(2)　外部サービス管理者

外部サービスの利用における利用申請の許可権限者から利用承認時に指名された当該外部サービスに係る管理を行う者をいう。

(3)　外部サービス提供者

外部サービスを提供する事業者をいう。外部サービスを利用して本学に向けて独自のサービスを提供する事業者は含まれない。

(4)　外部サービス利用者

外部サービスを利用する本学の利用者等又は業務委託した委託先において外部サービスを利用する場合の委託先の従業員をいう。

(5) 学生等

学部学生，大学院学生，研究生，研究員，研修員並びに研究者等，その他全学実施責任者が認めた者をいう。

(6) 機器等

情報システムの構成要素（サーバ装置，端末，通信回線装置，複合機，特定用途機器等，ソフトウェア等），外部電磁的記録媒体等の総称をいう。

(7) 教職員等

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），その他全学実施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。

(8) 業務委託

本学の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。ただし，当該業務において本学の情報を取り扱わせる場合に限る。

(9) 記録媒体

情報が電磁的に記録されるものをいう。記録媒体には，文字，図形等人の知覚によって認識することができる情報が電子的方式，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記録され，情報システムによる情報処理の用に供されるもの（以下「電磁的記録」という。）がある。また，電磁的記録媒体には，サーバ装置，端末，通信回線装置等に内蔵される内蔵電磁的記録媒体と，ＵＳＢメモリ，外付けハードディスクドライブ，ＤＶＤ－Ｒ等の外部電磁的記録媒体がある。

(10) サーバ装置

情報システムの構成要素である機器のうち，通信回線等を経由して接続してきた端末等に対して，自らが保持しているサービスを提供するもの（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，本学が調達し，又は開発するものをいう。

(11) ＣＩＳＯ（シーアイエスオー）

最高情報セキュリティ責任者（Chief Information Security Officer）の略で，職務は「国立大学法人滋賀医科大学情報化統括責任者等に関する規程」に定めるものとする。

(12) 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。

(13) 実施手順

対策基準に定められた対策内容を個別の情報システムや業務において実施するため，あらかじめ定める必要のある具体的な手順をいう。

(14) 情報

この規程の第２条第２項に定めるものをいう。

(15) 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，本学が調達し，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。）をいう。

(16) 情報セキュリティインシデント

JIS Q 27000:2019 で定義されている，「望まない単独若しくは一連の情報セキュリティ事象，又は予期しない単独若しくは一連の情報セキュリティ事象であって，事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの」をいう。

(17) 情報セキュリティ関係規程

ポリシーに基づいて策定される規程，対策基準，計画及び実施手順を総称したものをいう。

(18) 情報セキュリティ対策推進体制

本学の情報セキュリティ対策の推進に係る事務を遂行するため，学内に設置された体制をいう。

(19) 対策基準

本学における情報及び情報システムの情報セキュリティを確保するための対策の基準として定める「国立大学法人滋賀医科大学情報セキュリティ対策基準」及び同基準から参照される関連基準をいう。

(20) 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，本学が調達し，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。特に断りを入れるような例としては，本学が調達し，又は開発するもの以外を指す「本学支給以外の端末」がある。また，本学が調達し，又は開発した端末と本学支給以外の端末の双方を合わせて「端末（支給外端末を含む)」という。

(21) 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。通信回線には，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。

(22) 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。

(23) ポリシー

本学が定める「国立大学法人滋賀医科大学情報セキュリティ対策基本方針」及びこの規程をいう。

(24) モバイル端末

端末のうち，必要に応じて移動させて使用することを目的としたものをいい，端末の形態は問わない。

(25) 要管理対策区域

本学の管理下にある区域（学外組織から借用している施設等における区域を含む。）であって，取り扱う情報を保護するために，施設及び執務環境に係る対策が必要な区域をいう。

(26) 利用者

本学情報システムを利用する許可を受けて利用する者をいう。

(27) 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者をいう。

（全学総括責任者）

第４条　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き，ＣＩＳＯをもって充てる。

２　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

３　全学総括責任者は，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　全学総括責任者に事故があるとき，第７条に規定する全学実施責任者が，その職務を代行する。

（情報統括・セキュリティ委員会の設置）

第５条　情報セキュリティに関する事項を統括し，ポリシーの承認策定等重要事項の決定を行い，重要事項に関する関係部署との連絡及び調整を行うため，情報統括・セキュリティ委員会（以下，「委員会」という。）を置く。委員会の組織及び運営等については，「滋賀医科大学情報統括・セキュリティ委員会規程」に定める。

（情報セキュリティ監査責任者）

第６条　情報セキュリティの監査に関する事務を統括する者として，情報セキュリティ監査責任者を置き，学長が指名する監事をもって充てる。

（全学実施責任者の設置）

第７条　情報セキュリティ対策に関する事務を統括し，全学総括責任者を補佐する者として，全学実施責任者１名を置き，情報総合センター長をもって充てる。

２　全学実施責任者は，次の事務を統括する。

(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

３　全学実施責任者に事故があるとき，「国立大学法人滋賀医科大学情報化統括責任者等に関する規程」に定めるＣＩＳＯ補佐が，その職務を代行する。

（職場情報セキュリティ責任者の設置）

第８条　講座，事務局の課・室等の管理組織単位ごとに情報セキュリティ対策に関する事務を統括する職場情報セキュリティ責任者１名を置き，各所属の長をもって充てる。

２　職場情報セキュリティ責任者は，情報セキュリティに関する事務を整理・統括する職場情報セキュリティ担当者１名を必要に応じて置くことができる。

（全学情報セキュリティアドバイザーの設置）

第９条　全学総括責任者は，情報セキュリティについて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置くことができる。

２　全学総括責任者は，次に掲げるものを例とする全学情報セキュリティアドバイザーの業務内容を定めるものとする。

(1)　全学の情報セキュリティ対策の推進に係る全学総括責任者への助言

(2)　情報セキュリティ関係規程の整備に係る助言

(3)　対策推進計画の策定に係る助言

(4)　教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援

(5)　情報システムに係る技術的事項に係る助言

(6)　情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言
(7)　利用者に対する日常的な相談対応
(8)　情報セキュリティインシデントへの対処の支援
(9)　前各号に掲げるもののほか，情報セキュリティ対策への助言又は支援

（情報セキュリティ対策推進体制の整備）

第 10 条　全学総括責任者は，本学の情報セキュリティ対策推進体制を整備し，その役割を規定するものとする。

2　全学総括責任者は，情報セキュリティ対策推進体制の責任者を定める。

3　全学総括責任者は，次に掲げるものを含む情報セキュリティ対策推進体制の役割を規定するものとする。
(1)　情報セキュリティ関係規程及び対策推進計画の策定に係る事務
(2)　情報セキュリティ関係規程の運用に係る事務
(3)　例外措置に係る事務
(4)　情報セキュリティ対策の教育の実施に係る事務
(5)　情報セキュリティ対策の自己点検に係る事務
(6)　情報セキュリティ関係規程及び対策推進計画の見直しに係る事務

（情報セキュリティインシデントに備えた体制の整備）

第 11 条　委員会にＣＳＩＲＴを置き，ＣＳＩＲＴは本学情報システムのセキュリティに関する業務，情報セキュリティの維持，情報セキュリティインシデント対応に必要な措置を実施するものとし，その他ＣＳＩＲＴに必要な事項は「滋賀医科大学情報セキュリティインシデント対策チーム内規」に定める。

2　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。

3　情報セキュリティインシデントへの対応及び対策として，ＣＳＩＲＴが行う事項は「滋賀医科大学情報セキュリティインシデント対策チーム内規」に定める。

4　全学総括責任者は，実務担当者を含めた実効性のあるＣＳＩＲＴ体制を構築する。

5　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に，その対処に関する知見を有する外部の専門家等による必要な支援を速やかに得られる体制を構築しておくものとする。

6　全学総括責任者は，全学における情報セキュリティインシデント対処について，ＣＳＩＲＴ，情報セキュリティインシデントの当事者部局及びその他関連部局の役割分担を規定するものとする。

（ＢＣＰとの整合）

第 12 条　全学実施責任者は，情報セキュリティ関係規程の整備又は見直しを指示するに際し，当該規程が満たすべき要件として国立大学法人滋賀医科大学事業継続計画

（ＢＣＰ）との整合性の確保を含めるものとする。

（兼務を禁止する役割）

第 13 条　教職員等は，情報セキュリティ対策の運用において，次に掲げる役割を兼務しないこと。

(1)　承認又は許可（以下，本条において「承認等」という。）の申請者と当該承認等を行う者

(2)　監査を受ける者とその監査を実施する者

２　教職員等は，承認等を申請する場合において，自らが承認権限者等であるとき，その他承認権限者等が承認等の可否の判断をすることが不適切と認められるときは，当該承認権限者等の上司又は適切な者に承認等を申請し，承認等を得ること。

（情報の分類と管理）

第 14 条　本学の情報システムにおいて取扱う情報について，重要な情報を重点管理する考え方から，情報格付けに応じた情報分類の定義，情報の管理責任，管理の方法を定めるものとする。

（見直し）

第 15 条　本学のポリシー及び情報セキュリティ規程の内容を適時検討し，必要があると認めた場合にはその見直しを行うものとする。

（対策基準の策定）

第 16 条　全学総括責任者は，委員会における審議を経て，サイバーセキュリティ戦略本部決定「政府機関等のサイバーセキュリティ対策のための統一基準群」に準拠した対策基準を定めるものとする。

２　前項の対策基準は，本学の業務，取扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえたうえで定めるものとする。

附　則

この規程は，令和５年４月１日から施行する。

附　則

この規程は，令和５年８月１日から施行する。