公立大学法人静岡社会健康医学大学院大学情報セキュリティ対策基本規程

令和３年４月１日　規則第 50 号

（目的）

第１条　本規程は、静岡社会健康医学大学院大学（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、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　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・管理する全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。

(1)　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。）

(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（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、職員等が職務上取り扱う情報

(3)　第１号及び第２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。

（用語定義）

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

(1)　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。

(2)　学生等　本学通則に定める大学院学生、研究生、委託生、科目等履修生、社会人聴講生、社会人専門講座受講生、特別聴講学生その他情報セキュリティ実施責任者が認めた者をいう。

(3)　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。

(4)　職員等　本学を設置する法人の役員、本学に勤務する常勤又は非常勤の

職員（派遣職員を含む）その他情報セキュリティ実施責任者が認めた者をいう。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ている。

(5)　記録媒体　情報が記録され、又は記載される有体物をいう。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記載された紙その他の有体物（以下「書面」という。）と、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、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。）に係る記録媒体（以下「電磁的記録媒体」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。

(6)　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、本学が調達又は開発するものをいう。

(7)　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。

(8)　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。

(9)　情報　第２条第２項に定めるものをいう。

(10)　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、本学が調達若しくは開発するもの（管理を外部委託しているシステムを含む。）又は本学情報ネットワークに接続されるものをいう。

(11)　情報セキュリティインシデント　JIS Q 27000:2014 における情報セキュリティインシデントをいう。

(12)　情報セキュリティ関連規程　ポリシーに基づいて策定される規程、基準及び計画を総称したものをいう。

(13)　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。

(14)　対策基準　本学が定める静岡社会健康医学大学院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。

(15)　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。特に断りを入れた例としては、本学が調達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。

(16)　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。

(17)　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。

(18)　ポリシー　本学が定める静岡社会健康医学大学院大学情報セキュリティ対策基本方針及び本規程をいう。

(19)　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。

(20)　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。

(21)　利用者　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者をいう。

(22)　臨時利用者　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。

（最高情報セキュリティ責任者）

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最高情報セキュリティ責任者を置き、理事長をもって充てる。

２　最高情報セキュリティ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、最高情報セキュリティ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最高情報セキュリティ副責任者１人を置き、理事（総務担当）をもって充てる。

３　最高情報セキュリティ責任者は、次に掲げる事務を統括すること。
(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
４　最高情報セキュリティ責任者は、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。

（情報セキュリティ対策に関する審議）

第５条　対策基準及び対策推進計画の審議、その他情報セキュリティ対策の推進に関する事項については、静岡社会健康医学大学院大学図書館情報委員会の所管とする。

（情報セキュリティ監査責任者）

第６条　最高情報セキュリティ責任者の指示に基づき実施する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１人を置き、監査課長をもって充てる。

（管理運営部局）

第７条　本学情報システムの管理運営は、事務局で行う。

（管理運営部局が行う事務）

第８条　管理運営部局は、最高情報セキュリティ責任者の指示により、以下の各号に定める事務を行う。
(1)　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
(2)　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
(3)　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

（情報セキュリティ実施責任者の設置）

第９条　最高情報セキュリティ責任者を補佐する者として、情報セキュリティ実施責任者１人を置き、事務局長をもって充てる。
２　情報セキュリティ実施責任者は、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)　定められた区域ごとの区域情報セキュリティ責任者の設置
(7)　職場情報セキュリティ責任者の設置
(8)　情報システムごとの情報システム技術責任者の設置
(9)　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
(10)　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
(11)　前各号に掲げるもののほか、情報セキュリティ対策に関する事務

（区域情報セキュリティ責任者の設置）

第10条　情報セキュリティ実施責任者は、静岡社会健康医学大学院大学情報セキュリティ対策基準で定める区域ごとに、当該区域における情報セキュリティ対策の事務を統括する区域情報セキュリティ責任者１人を置くこと。

（職場情報セキュリティ責任者の設置）

第11条　情報セキュリティ実施責任者は、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人を置くこと。

２　職場情報セキュリティ責任者は、命を受け、管理組織単位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統括すること。

（情報システム技術責任者の設置）

第12条　情報セキュリティ実施責任者は、情報システムごとの情報セキュリティ対策に関する事務の責任者として、情報システム技術責任者を、当該情報システムの企画に着手するまでに選任すること。

２　情報システム技術責任者は、命を受け、情報システムにおける情報セキュリティ対策に関する事務を担うこと。

３　情報システム技術責任者は、所管する情報システムの管理業務において必要な単位ごとに情報システム技術担当者を置くこと。

（情報セキュリティアドバイザーの設置）

第13条　最高情報セキュリティ責任者は、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情報セキュリティアドバイザーとして置くものとし、図書館情報委員会委員長をもって充てる。

２　情報セキュリティアドバイザーは、最高情報セキュリティ責任者に対し、情報セキュリティに関する技術的な助言を行うことができる。

（情報セキュリティ対策推進体制の整備）

第14条　最高情報セキュリティ責任者は、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　最高情報セキュリティ責任者は、情報セキュリティ対策推進体制の責任者を定めるものとする。

3　最高情報セキュリティ責任者は、以下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

4　最高情報セキュリティ責任者は、以下を含む CSIRT の役割を規定するものとする。

(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最高情報セキュリティ責任者等への報告
- 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

5　最高情報セキュリティ責任者は、実務担当者を含めた実効性のある CSIRT 体制を構築するものとする。

6　最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際に、情報セキュリティインシデント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。

7　最高情報セキュリティ責任者は、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組織及び

その他関連組織の役割分担を規定するものとする。

（兼務を禁止する役割）

第 15 条　職員等は、情報セキュリティ対策の運用において、以下の役割を兼務してはならない。

(1)　承認又は許可の申請者と当該承認を行う者

(2)　監査を受ける者とその監査を実施する者

（対策基準の策定）

第 16 条　最高情報セキュリティ責任者は、サイバーセキュリティ戦略本部決定「政府機関等の情報セキュリティ対策のための統一基準」に準拠した対策基準を定めなければならない。また、対策基準は、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リスク評価の結果を踏まえた上で定めるものとする。

（規程の改廃）

第 17 条　この規程の改廃は、公立大学法人静岡社会健康医学大学院大学理事会の議決を経て行うものとする。

附　則

この規則は、令和３年４月１日から施行する。