東京医療保健大学情報セキュリティ対策基本方針

（目的）

第１条 東京医療保健大学（以下「本学」という。）は、本学の理念と使命を実現するため、本学で扱う情報及び情報システムを対象に情報セキュリティ対策を実施する。

（方針）

第２条　前条の目的を達するため、本学は情報セキュリティ対策基本規程（以下、「対策基本規程」という。）及びその他の規程等の定めるところにより、以下の対策を行う。

（１）情報セキュリティ対策の実施体制の整備
（２）情報及び情報システムの保護
（３）情報システムや情報サービスの管理・運用
（４）インシデントへの対処
（５）利用者への啓発・教育
（６）（１）～（５）を含む情報セキュリティマネジメントの実施

（義務）

第３条　本学の情報及び本学で扱う情報システムを利用する者、管理・運用の業務に携わる者は、本方針、対策基本規程及びその他の規程等を遵守しなければならない。

（罰則）

第４条　本方針に基づき定められる規程等に違反した場合の利用の制限及び罰則は、本学が定める大学学則及び大学院学則並びに就業規則に則って行うほか、それぞれの規程に定めるところによる。

附則　　この方針は、令和５年４月１日から施行する。

東京医療保健大学情報セキュリティ対策基本規程

（目的）

第１条 本規程は、東京医療保健大学（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・管理するすべての者、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）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（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、教職員等が職務上取り扱う情報

（３）前各号のほか、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 本規程における用語の定義は、次のとおりとする。

（１）情報システムを運用・管理するすべての者

本規程第４条以下に規定する、最高情報セキュリティ責任者、最高情報セキュリティ責任者補佐、情報セキュリティ委員会委員、総括実施責任者、運営事務局に所属する職員、キャンパス統括管理者、情報セキュリティ監査責任者、その他本学の情報システムを運用・管理する教職員等をいう。

（２）利用者

教職員等（前号に定める教職員等を除く）及び学生で、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。

（３）臨時利用者

教職員等及び学生以外の者で、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。

（４）教職員等

本学を設置する法人の役員及び本学の職員（常勤・非常勤を問わず、派遣契約その他の契約に基づき本学の業務に従事する者を含む。）をいう。

（５）学生

大学において修学するすべての者（留学生、科目履修生等を含む。）をいう。

（６）情報

本規程第２条第２項に定めるものをいう。

（７）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。）若しくは本学情報ネットワークに接続されるものをいう。

（８）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、電子計算機による情報処理用に供されるもの（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、電子計算機や通信回線装置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。

（９）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。

ア　機密性とは、アクセス権をもつ者だけが情報にアクセスできる状態を確保することをいう。

イ　完全性とは、情報及び処理方法が正確であること及び完全な状態であることを確保することをいう。

ウ　可用性とは、認可された利用者が必要なときに情報及び関連資産にアクセスできる状態を確保することをいう。

（１０）ポリシー

本学が定める「情報セキュリティ対策基本方針」及び本規程をいう。

（１１）インシデント

情報管理やシステム運用に関して保安上の脅威となる現象や事案（ウイルス感染、不正アクセス、情報漏えい、迷惑メール送信、サービス拒否攻撃(DoS アタック)等を指す。)が発生し、又はその発生の可能性がある状態をいう。

（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、本学に設置された組織をいう（Computer Security Incident Response Team の略)。

（最高情報セキュリティ責任者）

第４条 本学に、最高情報セキュリティ責任者（Chief Information Security Officer。以下、「CISO」という。）を置く。

２ CISO は、医療情報学科長をもって充てる。

３ CISO は、本学の情報セキュリティに関する総括的な意思決定を行う。

４ CISO は、情報セキュリティ委員会に対し、情報セキュリティポリシーの策定及びその周知徹底を指示する。

（最高情報セキュリティ責任者補佐）

第５条 本学に、CISO を補佐し情報セキュリティに係る技術的支援を行う最高情報セキュリティ責任者補佐（以下、「CISO 補佐」という。）を置く。

２ CISO 補佐は、CISO が指名する専任教員をもって充てる。

（情報セキュリティ委員会の設置）

第６条 本学における情報セキュリティに関する事項を審議し、必要な事項を決定して周知するため、東京医療保健大学情報セキュリティ委員会（以下、「情報セキュリティ委員会」という。）を設置する。

２ 情報セキュリティ委員会に委員長を置き、CISO をもって充てる。

３ 情報セキュリティ委員会の運営に関し必要な事項は別に定める。

（総括実施責任者）

第７条 本学に、総括実施責任者を置く。

２ 総括実施責任者は、事務局長をもって充てる。

３ 総括実施責任者は、本学における情報セキュリティ対策の実施に関する事項を総括する。

（運営事務局）
第８条 本学に、運営事務局を置き、総務人事部が担当する。
２　運営事務局は，総括実施責任者の指示の下，次に掲げる事項を処理する。
（１）情報セキュリティ委員会の運営に関すること。
（２）情報セキュリティに関する連絡と通報に関すること。
（３）情報セキュリティポリシーの遵守励行に関すること。
（４）情報セキュリティポリシーの周知及び教育に関すること。
（５）その他情報セキュリティに関し必要な事項に関すること。

（キャンパス統括管理者）
第９条 各キャンパスに、キャンパス統括管理者を置く。
２　キャンパス統括管理者は、キャンパス事務部長をもって充てる。
３　キャンパス統括管理者は、情報システムの利用者に対して、情報システムの運用及び利用に関し、ポリシー及びそれに基づく基準並びに手順等の遵守を確実にするための教育実施を支援する。

（情報セキュリティ監査責任者）
第１０条　本学に、情報セキュリティ監査責任者１人を置く。
２　情報セキュリティ監査責任者は、内部監査室長をもって充てる。
３　情報セキュリティ監査責任者は、CISO の指示に基づき、監査に関する事務を総括する。

（CSIRT）
第１１条　本学に、情報セキュリティ対策の実施及びインシデント対応のための組織として、平常時の情報収集やインシデント時の迅速な初動対応を行う CSIRT を置く。
２　CSIRT に関し必要な事項は、別に定める。

（雑則）
第１２条　この規程に定めるもののほか、情報セキュリティ対策に関し必要な事項は、別に定める。

（規程の改廃）
第１３条　この規程の改廃は、大学経営会議において決定する。

附則　　この規程は、令和５年４月１日から施行する。

東京医療保健大学情報セキュリティインシデント対応チーム細則

（趣旨）

第１条 本細則は、東京医療保健大学情報セキュリティ対策基本規程（以下、「規定」という。）第１１条第２項の規定に基づき、東京医療保健大学セキュリティインシデント対応チーム（以下、「CSIRT」という。）に関し必要な事項を定める。

（目的）

第２条 CSIRT は、東京医療保健大学情報セキュリティ対策基本方針（以下、「方針」という。）第２条第４号に規定するインシデントへの対処を技術的に支援することにより、インシデント発生時の影響を最小限に抑制し、情報資産の安全を確保することを目的とする。

（業務）

第３条 CSIRT は、次に掲げる業務を行う。

（１）インシデントの通報受付及び関係者との連絡調整に関すること。
（２）インシデントの拡大防止措置に関すること。
（３）インシデントの復旧措置に関すること。
（４）インシデントの原因究明及び再発防止措置に関すること。
（５）インシデントに関する学外関係機関への連絡・報告に関すること。
（６）インシデントに関する報告書作成及び作成支援に関すること。
（７）インシデントに関する情報収集、学内への注意喚起に関すること。
（８）その他インシデントに関すること。

（組織）

第４条 CSIRT は、次に掲げる者をもって組織する。

（１）CSIRT 長
（２）インシデントマネージャー
（３）チーム員

（CSIRT 長）

第５条 CSIRT 長は、システム部長をもって充てる。

（インシデントマネージャー）

第６条 インシデントマネージャーは、システム部に所属する職員のうちから CSIRT 長が指名する者をもって充てる。

２ インシデントマネージャーは、CSIRT 長の命を受け、インシデント対応の指揮を行う。

３ CSIRT 長に事故があるときは、インシデントマネージャーがその職務を代行する。

（チーム員）
第７条　チーム員は、医療情報学科に所属する教員、ＰＣサポートセンターに所属する職員をもって充てる。
２　チーム員は、CSIRT 長の命を受け、インシデント対応業務を行う。

（事務）
第８条　CSIRT の事務は、システム部において処理する。

（雑則）
第９条　この細則に定めるほか、CSIRT に関して必要な事項は、東京医療保健大学セキュリティポリシーによる。

附則　　この細則は、令和５年４月１日より施行する。

＜補足資料＞　CSIRT 業務の流れ（イメージ）