和歌山県立医科大学ネットワーク及び情報システムに関わる情報セキュリティ基本方針

制　　定　平成30年３月28日
最終改正　令和３年３月29日

序　文

和歌山県立医科大学は、医学、保健看護学及び薬学に関する学術知識について教育、研究するとともに、附属病院においては、質の高い安全な医療の提供、病院運営の効率化のために「総合医療情報システム」を活用して、高度医療を提供している。本学の研究・教育・診療・運営業務については、近年情報通信技術に対する依存度が高まる一方、本学が取り扱う情報には、附属病院の患者の個人情報のみならず大学運営上重要な情報が含まれており、漏洩、損壊等の事故があった場合に極めて重大な結果を招く可能性がある。

また、不正アクセス、マルウェアなどの外部からの脅威も高度化しており、さらに内部職員又は業務受託事業者等による機密情報又は個人情報の漏洩・悪用の可能性も皆無とはいえず、ネットワーク及び情報システムに関する情報セキュリティ管理の重要性がますます高まっているところである。

そこで、本学は、県民等が安心・信頼して本学の提供するサービスを利用することができるようにするとともに、本学における継続的かつ安定的な大学運営業務の実施を確保するために、情報セキュリティ管理に関する総合的、体系的かつ具体的な対策を和歌山県立医科大学ネットワーク及び情報システムに関わる情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）として定める。

情報セキュリティポリシーとは、情報資産の機密性（秘密を守る）、完全性（改ざんされない）、可用性（サービスが停まらない）という３つの情報セキュリティの要素を一定以上に保ち、維持するためのルールである。情報セキュリティポリシーは、本学の情報資産をさまざまな脅威から守るための基本的な考え方（基本方針）と基本方針を実現するために、組織的、技術的、物理的、人的に何をやらなければならないかという基準（管理要綱）から構成される。

本学構成員は、このルールを理解し、遵守するとともに、情報セキュリティ管理は本学構成員ひとりひとりの責任であることを自覚しなければならない。

第１章　和歌山県立医科大学ネットワーク及び情報システムに関わる情報セキュリティ基本方針の目的

第１節　基本方針の目的

和歌山県立医科大学ネットワーク及び情報システムに関わる情報セキュリティ基本方針（以下「基本方針」という。）は、情報セキュリティポリシーを構成し、和歌山県立医科大学（以下「大学」という。）の職員（非常勤職員、準職員及び臨時職員を含む。）及び学外受託者（大学の業務に従事する派遣会社社員、協力会社社員及び業務受託会社社員）など、情報資産を扱う者全員が従うべき、情報セキュリティを確保するための基本的な考え方であり、情報セキュリティポリシーの適用範囲や取扱い、人と組織の役割と責任、情報セキュリティ対策の基本的な方向性等を定めるものである。

第２節　適用範囲

第１項　組織

情報セキュリティポリシーの適用範囲は、大学の全ての部署とする。

第２項　ネットワーク

大学で使用されるコンピュータを接続する情報通信機器及び通信回線とする。

第３項　情報システム

大学で使用されるネットワーク、ハードウェア、ソフトウェア及び記憶媒体で構成された情報を処理する仕組みとする。

第４項　情報資産

情報セキュリティポリシーが適用される情報資産は以下のものとする。

⑴　大学で使用されるネットワーク及び情報システムの開発に関わる文書、図画、写真、フィルム並びに電磁的記録

⑵　大学で使用されるネットワーク及び情報システムで取り扱う電磁的記録

⑶　大学で使用されるネットワーク及び情報システムの運用に関わる文書及び図画で、和歌山県立医科大学文書処理規程第２条に規定するものを除く。

第２章　基本的な考え方

第１節　情報資産に対する脅威

情報資産に対する脅威の発生度合や発生した場合の影響を考慮し、特に備えるべき脅威を次のとおりとする。

⑴　情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏洩・破壊・消去等

⑵　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏洩・破壊・改ざん・消去、重要情報の詐取、内部不正等

⑶　地震、落雷、火災等の災害によるサービス及び業務の停止等

⑷　大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

⑸　電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

第２節　情報資産の保護

前節の脅威から情報資産を保護するため、以下の方策を講ずるものとする。

⑴　物理的方策

サーバ及びその設置エリア、通信回線等並びに職員の使用するパソコン等の管理について物理的に必要な方策を講じる。

⑵　人的方策

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的に必要な方策を講じる。

⑶　技術的方策

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的に必要な方策を講じる。

⑷　運用上の方策

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面で必要な方策を講じるものとする。

第３章　情報セキュリティポリシーの取扱い

第１節　基本方針

基本方針は、大学のネットワーク及び情報システム内の情報を安全に管理するために、全ての使用者が守るべき方針とする。

第２節　管理要綱

基本方針に基づいて情報セキュリティを確保するに当たり、遵守すべき行為、判断などの基準を統一的に定めるために、必要となる基本要件を明記した管理要綱を策定する。

要綱は、大学の情報資産を取り扱う全ての職員及び学外受託者に対し、周知徹底する。

第３節　点検

情報セキュリティ管理者等は、情報セキュリティポリシーに沿った情報セキュリティ対策が実施されているかどうか、定期的に点検を行う。

第４節　情報セキュリティポリシーの改正

情報セキュリティを取り巻く状況の変化に迅速に対応するため、情報セキュリティ点検の結果なども踏まえ、情報セキュリティポリシーは定期的に見直し、必要に応じて改正する。

第４章　人と組織

第１節　職掌上の役割と責任

第１項　学長の役割と責任

学長は、セキュリティに関する指針を明らかにし、職員及び学外受託者に対してセキュリティ意識を浸透させ、必要な指示をする役割と責任を持つ。

第２項　所属長の役割と責任

所属長は、セキュリティ確保の責任を負い、所属部署の職員及び業務関係者が、情報セキュリティポリシーを理解し遵守することを徹底し、かつ管理する。

また、所属長は、所属部署の職員が退職、転出又は業務変更する場合、利用する必要のなくなった全ての情報資産を回収する責任を持つ。また、学外受託者が契約終了した場合も同様である。

第３項　職員の役割と責任

職員は、法令、情報セキュリティポリシー及び所属長の指示等を遵守し、情報が不正な手段で取得されること又は不正に使用されることを防止する責任がある。

職員は、退職、転出又は業務変更する場合に利用する必要のなくなった全ての情報資産を大学に返却しなければならない。

職員は、自己責任の原則に基づいてネットワーク及び情報システムの利用を行うことを十分理解しなければならない。

第４項　職員以外の者（学外受託者等）の役割と責任

学外受託者は、業務委託契約等に反しない範囲で、前項の役割と責任を負う。

第２節　セキュリティの管理体制及び組織

大学の保有する情報資産について、統一的な情報セキュリティを確保するため、全学的な管理体制を以下のとおりとする。

第１項　管理体制

⑴　情報セキュリティ総括責任者

大学におけるセキュリティ責任者を総括し、セキュリティを含む情報管理全般に関する最高責任者であり、全ての責任及び権限を有する。学長がその任に当たる。

⑵　情報セキュリティ責任者

ア　各部署における情報セキュリティに関する責任と権限を有し、情報セキュリティ管理者に指示する。次の者がその任に当たる。

学生部長、医学部長、保健看護学部長、薬学部長、附属病院長、紀北分院長、産官学連携推進本部長、地域・国際貢献推進本部長及び事務局長

イ　各部署における情報セキュリティに関する責任と権限を有し、所属の職員に対し情報セキュリティ活動の指導及び監督を行う。次の者がその任に当たる。

教育研究開発センター長、入試・教育センター長、図書館長、共同利用施設長、助産学専攻科長、みらい医療推進センター長、健康管理センター長、ワークライフバランスセンター長、看護キャリア開発センター長及び危機対策室長

⑶　情報セキュリティ管理者

情報セキュリティ責任者の指示の下、各所属の職員に対し情報セキュリティ活動の指導及び監督を行う。各所属長がその任に当たる。

第２項　組織

⑴　情報管理委員会

ア　大学のネットワーク及び情報システムに係る情報セキュリティに関する重要な事項を調査、検討、審議し決定する。

イ　情報管理委員会は、和歌山県立医科大学情報管理委員会規程（以下、「情報管理委員会規程」という。）で定める者で構成する。

ウ　情報管理委員長は、情報セキュリティに関する重要な方針等を審議した場合、情報セキュリティ総括責任者に報告する。

⑵　情報管理委員会事務局

情報管理委員会事務局は、情報管理委員会規程に定める。

第３項　情報管理者

主管する業務において、情報収集、作成又は県民等から情報を預託された部署の所属長を情報管理者とする。

情報管理者は、自ら所有する情報資産の保護管理要件を定め、情報の使用者を決定する。

第３節　セキュリティに関する教育等

情報セキュリティ管理者等は、情報セキュリティポリシーの職員等への浸透と情報セキュリティ意識向上のため、情報セキュリティに関する教育・啓発を実施する。

第４節　第三者による情報資産使用に関する方針

大学の情報資産を、当該情報を大学に預託した本人以外の第三者に使用させる場合は、事前に当該情報の情報管理者の承認を必要とする。

情報資産のうち、特に個人情報の取扱いについては、個人情報保護法、和歌山県個人情報保護条例及び関係法令の規定を遵守すること。

第５章　情報資産の分類

第１節　セキュリティレベルの設定

情報セキュリティ管理者は、情報資産の重要度に応じて、機密性、完全性及び可用性を維持するために、セキュリティレベルを設定する。

セキュリティレベルごとに情報資産の保護管理要件を明確にし、想定されるリスク及びその対策を明確にする。

第２節　情報資産の分類

情報管理者は、自らが所管する情報資産を重要度に応じてセキュリティレベルに分類する。必要な場合は、追加の保護管理要件を設定することができる。

第６章　情報セキュリティの確保

情報セキュリティを確保するため、セキュリティレベルに応じて、情報の機密性、完全性及び可用性を維持するものとし、物理、技術及び運用の面から以下の方策を行う。

第１節　物理的方策

第１項　情報資産

セキュリティレベルに応じ、情報資産の保管等に関し必要な方策を講じなければならない。

第２項　情報システム

情報システム内で取り扱う情報資産のセキュリティレベルに応じ、情報システムを構成する機器の設置環境、物理的アクセス等に関し必要な方策を講じなければならない。

第３項　ネットワーク

ネットワーク内を通過する情報資産のセキュリティレベルに応じ、ネットワークを構成する機器の設置環境等に関し必要な方策を講じなければならない。

第２節　技術的方策

第１項　情報資産

セキュリティレベルに応じ、情報資産の保護のため、情報漏洩の防止等について必要な方策を講じなければならない。

第２項　情報システム

情報システム内で取り扱う情報資産のセキュリティレベルに応じ、利用者の識別方法、アクセス制御方法等に関し必要な方策を講じなければならない。また、システム開発及び保守に関するセキュリティ要件を明確にしなければならない。

第３項　ネットワーク

ネットワーク内を通過する情報資産のセキュリティレベルに応じ、ネットワークの経路制御等に関し必要な方策を講じなければならない。

第３節　運用上の方策

第１項　情報資産

情報資産のセキュリティレベルに応じ、データの取扱い、保管、使用、バックアップ等運用上の管理に関し必要な方策を講じなければならない。

第２項　情報システム

⑴　情報システム内で取り扱う情報資産のセキュリティレベルに応じて、操作手順書等を作成し、適切に管理運用しなければならない。

⑵　情報機器の設置、廃棄及び構成の変更について、管理手順を定め適切な管理を行わなければならない。

⑶　情報システムのセキュリティレベルに応じて、不正アクセスや障害検知等のための監視を行わなければならない。

⑷　情報セキュリティ管理者は、所管する情報システムのセキュリティを確保するための情報を収集し、必要な方策を講じなければならない。

第３項　ネットワーク

⑴　ネットワーク内を通過する情報資産のセキュリティレベルに応じて運用手順書等を作成し、適切に管理運用しなければならない。

⑵　ネットワーク機器の設置、廃棄及び構成の変更について、管理手順を定め適切な管理を行わなければならない。

⑶　ネットワーク内を通過する情報資産のセキュリティレベルに応じて、不正アクセスや障害検知等の監視を行わなければならない。

第７章　緊急時の対応

情報セキュリティ管理者は、主要業務毎にセキュリティレベルに基づいた緊急対応手順・緊急連絡体制・応急措置・バックアップ手順・業務再開手順等を含む情報セキュリティ事故対策マニュアルを作成する。

附　則

１　この基本方針は、平成30年４月１日から適用する。

２　和歌山県立医科大学ネットワーク及び情報システムに関わる情報セキュリティ基本方針（平成18年６月６日制定）は、廃止する。

附　則

この基本方針は、令和３年４月１日から適用する。