情報システムに関する規則

（目的）

第１条　この規則は、地方独立行政法人岐阜県立多治見病院（以下「法人」という。）における情報システム及び情報資産の安全性、信頼性及び可用性を確保するため、総務省、厚生労働省、および個人情報保護委員会の関係法令等に基づき、組織的かつ継続的な管理体制を整備し、もって法人の業務遂行及び診療提供の適正化並びに経営の健全性に資することを目的とする。

（定義）

第２条　情報システムとは、法人で利用する電子化された情報（以下「データ」という。）及びそのデータを処理・保管する仕組みをいう。

（情報セキュリティ責任体系）

第３条　法人に、情報セキュリティ統括責任者（CISO）を置く。

２　CISO は情報セキュリティの総括管理を行う。

３　法人は情報システム安全管理責任者、情報システム運用責任者、部門情報システム運用責任者を置き、それぞれの責務を明確にする。

（情報システム安全管理責任者）

第４条　情報システム安全管理責任者は、情報システムの構築、変更、保守に関する計画立案及び実施を統括し、CISO を補佐する。

（情報システム運用責任者）

第５条　情報システム運用責任者は、情報システムの運用、監視、障害対応、バックアップ等、日常の運用管理を統括させる。

２　情報システム運用責任者は、情報システム安全管理責任者と連携し、運用上の課題及び改善事項を報告する。

（部門情報システム運用責任者）

第６条　各部門の部門情報システム運用責任者は、当該部門における情報システムの利用に関する連絡調整及びインシデント発生時の初動連絡を行わせる。

２　部門システム運用責任者は、サーバ設定、ネットワーク設定、端末設定その他の技術的作業を行わないものとし、必要な事項を情報システム運用責任者に報告する。

（利用者の定義と責務）

第７条　利用者とは、法人の情報システム、情報資産又はネットワークを利用する職員、委託事業者職員その他法人が認めた者をいう。

２　利用者は、情報資産を適正に利用し、不正アクセス、データの不正取得又は漏えいにつながる行為をしてはならない。

３　利用者は、ID 及びパスワードを厳重に管理し、他者への貸与、譲渡又は共有をしてはならない。
４　利用者は、インシデント又は疑いがある事象を速やかに情報システム安全管理責任者に報告しなければならない。

（利用者の認証）
第８条　法人は、情報システムへのアクセスに当たり、ID 及びパスワードによる認証を原則としつつ、リスクに応じて二要素認証その他の多要素認証（以下「二要素認証等」という。）を導入する。
２　二要素認証等は、次に掲げる利用形態について必ず適用するものとする。
（１）院外からインターネットを経由した VPN 接続等を含むアクセス
（２）クラウドサービス、インターネット公開システムへの管理者権限によるアクセス
（３）サーバ、ネットワーク機器及び基幹システムの特権 ID によるアクセス
３　前項に定めるほか、CISO はリスク評価の結果に基づき、二要素認証等を適用すべきシステム及び利用形態を指定することができる。
４　技術的制約その他やむを得ない理由により二要素認証等を適用できない場合には、システム管理責任者は、CISO の承認を受けた上で、アクセス元の制限、利用時間帯の制限、ログ監視の強化等の代替措置を講じなければならない。

（情報資産管理）
第９条　法人は、情報資産の分類、リスク評価及び重要度評価を行い、情報資産台帳を整備するものとする。
２　情報資産には、個人情報、診療情報、システム管理情報等を含む。
３　外部ネットワークとの接続点について、必要な管理措置を講ずる。

（インシデント対応及び BCP）
第１０条　法人は、インシデント対応体制を整備し、初動、通報、封じ込め、復旧及び再発防止の手順を定める。
２　重大インシデントに対応するため、必要に応じて対策チーム（以下、「CSIRT」という。）を組織する。
（１）CSIRT の構成員は情報システム課員、関係ベンダー、必要な各部門責任者とする。
（２）サイバー攻撃等のインシデント発生時は、別途定める「医療総合情報システム障害対応マニュアル」にある「特別緊急会議」へ速やかに状況を報告し、指示を仰ぐものとする。
３　法人は事業継続計画（BCP）を策定し、定期的に訓練を行う。

（情報システム導入審査）
第１１条　法人は情報システム導入審査体制を整備し、導入の必要性、費用妥当性、リスク及び委託適合性等を審査する。

（情報システムの監査）
第１２条　法人は、情報システム及び情報セキュリティに関する内部監査を、毎年度、独立した組織により実施する。
２　内部監査のうち、技術的評価を要する事項については、必要に応じ外部の専門機関に委託することができる。
３　情報システム課は監査の実施には当たらず、監査に必要な資料の提供その他の協力を行う。

（外部委託の管理）
第１３条　法人は、委託先のセキュリティ水準、再委託体制、障害報告体制等を評価しなければならない。
２　契約に監査権限、再委託制限、事故通報義務等を明記する。

（情報セキュリティ教育）
第１４条　法人は、全職員に対し定期的な情報セキュリティ教育を実施し、記録を管理する。
２　標的型攻撃メール訓練等の実践的訓練を行い、管理職には高度研修を実施する。

（雑則）
第１５条　この規則に定めるもののほか、情報システムに関するコンプライアンスの推進に関し必要な事項は、理事長が定める。

附　則
この規則は、令和２年４月１日から施行する。
附　則
この規則は、令和８年２月１日から施行する。