地方独立行政法人岐阜県総合医療センター情報セキュリティ基本方針

（目的）

第１条　現在、地方独立行政法人岐阜県総合医療センター（以下「当センター」という。）において情報システムは医療現場を支える基盤設備として重要な役割を果たしている。そこで扱われる情報は患者様の個人情報であり、情報セキュリティ保護の重要性は言うまでもない。

しかし、医療スタッフにとって最も注力すべきは当然本来業務の医療行為であり、セキュリティ保護は重要だが、そのための過度の負担が本来業務を停滞させることがあってはならない。従って、情報セキュリティ保護の実現にあたっては、職員の必要最低限の注意と努力によって自然に必要かつ十分な情報セキュリティ対策をなし得るようにすることが求められ、情報セキュリティポリシーは、こうした情報セキュリティ対策を確立するための各種のルールを体系化・整理したものとして定義されねばならない。

こうした考えの下、地方独立行政法人岐阜県総合医療センター情報セキュリティ基本方針（以下「基本方針」という。）では、十分な患者様の個人情報保護を実現させ、同時に患者様本位の安全で良質な医療の提供、効率的な病院運営と職員の利便性確保を両立させることを目的として、情報セキュリティ対策について基本的な事項を定める。

（適用範囲）

第２条

１　機関

基本方針が適用される機関の範囲は、当センターとする。

２　情報資産の範囲

基本方針が対象とする情報資産は、次のとおりとする。

（１）ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

（２）ネットワーク及び情報システムで取り扱う情報

（３）情報システムの仕様書及びネットワーク図等のシステム関連文書

（用語の定義）

第３条　基本方針において、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）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（２）完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（３）可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（４）情報セキュリティ

情報の機密性、完全性及び可用性を維持することをいう。

（５）情報セキュリティポリシー

本基本方針及び第８条に規定する情報セキュリティ対策基準をいう。

（６）情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

（７）ネットワーク

コンピュータ等を相互に接続するための通信網､その構成機器(ハードウエア及びソフトウエア)をいう。

（８）電子カルテ系

電子カルテに関わる情報システム及びデータをいう。

（９）インターネット接続系

インターネットメール、インターネット閲覧システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(10) 通信経路の分割

電子カルテ系とインターネット接続系の両環境間の通信環境を分離したうえで、安全が確保された通信だけを許可できるようにすることをいう。

(職員等の遵守義務)

第４条　職員、非常勤職員、臨時職員（以下「職員等」という。）及び外部委託事業者は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たっては情報セキュリティポリシーを遵守しなければならない。

(対象とする脅威)

第５条　当センターは、情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（１）部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２）情報資産の無断持ち出し、無許可ソフトウエ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、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えい・破壊・消去等

（３）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

（４）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

（５）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

(情報セキュリティ対策)

第６条　前条の脅威から情報資産を保護するために､以下の情報セキュリティ対策を講じる。

（１）組織体制

当センターが保有する情報資産について、情報セキュリティ対策を推進・管理するための組織体制を確立する。

（２）情報資産の分類と管理

当センターが保有する情報資産を重要度に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

（３）情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の二段階の対策を行う。

① 電子カルテ系は、情報セキュリティポリシーで定める場合を除き、他の領域との通信を不可能とする。さらに、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、診療情報の流出を防ぐ。

② インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

（４）物理的セキュリティ

情報システムおよびその設置場所等の管理について、物理的な対策を講じる。

（５）人的セキュリティ

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必要な人的な対策を講じる。

（６）技術的セキュリティ

コンピュータの管理、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な対策を講じる。

（７）運用

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の対策を講じるものとする。また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を別途策定する。

（８）外部サービスの利用

外部委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を行う。

（９）評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、実施結果に基づき運用を改善することで情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

（情報セキュリティ監査及び自己点検の実施）

第７条　情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

（情報セキュリティ対策基準の策定）

第８条　この方針に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準（以下「対策基準」という。）を策定する。

（情報セキュリティポリシーの見直し）

第９条　情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

（情報セキュリティ対策実施手順の策定）

第１０条　対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ対策実施手順を策定するものとする。なお、情報セキュリティ対策実施手順は、公にすることにより当センターの業務運営に重大な支障を及ぼすおそれがあることから非公開とする。

附　則

この方針は、平成２２年４月１日から施行する。

附　則

この方針は、平成２３年４月１日から施行する。

附　則

この方針は、２０２３年４月１日から施行する。