情報セキュリティ基本方針

東千葉メディカルセンター

2026/ 3/24　作成

1. 目的

電子カルテシステム等の情報システム（以下「情報システム」）の導入により、情報は一元管理され、診療効率及び事務効率が著しく向上したが、一方で、システム利用者は、情報及び情報を取り扱う情報システムを様々な脅威から防御しながらの利用が求められている。

また、地方独立行政法人東金九十九里地域医療センター（以下「当センター」）が扱う情報資産には、患者及び利用者等の個人情報のみならず病院運営上重要な情報など、外部への漏洩や破壊等が発生した場合には、極めて重大な被害を招く情報が数多く含まれている。

ついては、情報システムを安全かつ適切に運用するための基本方針を明示することにより、利用者が日頃から情報を守る情報セキュリティの重要性と責任を認識し、法令に則り情報を適切に管理・運用することを目的とする。

2. 定義

この基本方針において、次の各号に掲げる用語の定義はそれぞれ当該各号に定めるところによる。

(1)医療情報システム

診療録・検査結果など法令で保存義務のある情報を電子管理する機器、ソフトウェア及び運用に必要な仕組み全般をいう。

(2)一般情報システム

事務業務等で使用する外部ネットワーク接続型システムをいう。

(3)情報システム

医療情報システムと一般情報システムの総称をいう。

(4)ネットワーク

情報システムを相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

(5)情報資産

ネットワーク、情報システム及びこれらで取り扱う情報をいう。

(6)管理責任者

地方独立行政法人東金九十九里地域医療センターのセンター長を充てる。

(7)企画管理者

医療情報管理部長を充てる。

(8)運用担当者

企画管理者が指定する職員を充てる。

3. 対象とする脅威

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) 意図的脅威：不正アクセス、権限を越えた操作、ID・パスワードの不正使用、内部不正、ウイルス感染などによる情報漏えい・破壊・改ざん。

(2) 非意図的脅威：誤操作、設定ミス、機器故障、外部媒体の不適切利用などによる情報漏えい・破壊・消去。

(3) 災害による脅威：地震・火災・水害等の自然災害でシステムが停止するリスク。

(4) 人的要因の脅威：大規模な疾病流行、職員不足や担当者不在による運用低下。

(5) インフラ障害の脅威：停電・通信障害等によるシステム停止。

4. 適用範囲

(1) 対象となる利用者の範囲

①当センターに勤務する職員（常勤・非常勤を含む。）

②研修登録医

③契約業者から派遣された者

④企画管理者が特に認めた者

(2) 対象となる情報資産の範囲

①医療情報システム及び一般情報システム並びにこれらに関する機器、設備及び電磁的記録媒体

②医療情報システム及び一般情報システムで取り扱う情報（診療情報、検査情報、会計情報、事務情報等。これらを印刷した文書を含む。）

③情報システムに関する仕様書、ネットワーク構成図、運用マニュアル、障害時運用手順書等のシステム関連文書

5. 職員等の遵守義務

(1) 規程・手順に従い情報システムを適切に利用する。

(2) ID・パスワードを厳重に管理し、不正利用を防ぐ。

(3) 付与されたアクセス権の範囲で業務を行う。

(4) 個人情報・診療情報を適切に保護する。

(5) 異常や不正を発見した場合は速やかに企画管理者に連絡する。

(6) 外部記録媒体の使用は許可制とし、無断使用を禁止する。

(7) 必要な研修を受講し、知識を習得する。

6. セキュリティ対策

当センターの医療情報資産を先に掲げた脅威から保護するため、以下の情報セキュリティ対策を講ずるものとする。

(1) 物理的セキュリティ対策

最重要な情報システムを設置する施設（サーバー室）への不正な立ち入り、医療情報資産への損傷・妨害等を防ぐため、入退室や機器管理上の物理的な対策を講ずる。

(2) 人的セキュリティ対策

医療情報資産に接する職員等の情報セキュリティに関する権限や責任等を定めると共に、全ての職員等に情報セキュリティポリシーの内容を周知徹底するため、教育及び啓発が行われるよう必要な対策を講ずる。

(3) 技術的セキュリティ対策

医療情報資産を不正なアクセス等から適切に保護するため、医療情報資産へのアクセス制御、コンピュータウィルス対策等の技術的な対策を講ずる。またリモートアクセスの状態を管理する。

(4) 運用セキュリティ対策

情報セキュリティポリシーの実効性を確保するため、情報システム等の稼動状況の監視や情報セキュリティポリシーの遵守状況の確認のため、運用面における必要な対策を講ずる。また、緊急事態が発生した場合に迅速な対応を可能とするため、危機管理対策を講ずる。

7. 情報セキュリティ監査及び自己点検

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。

8. 情報セキュリティポリシーの見直し

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。