地方独立行政法人三重県立総合医療センター
電子情報安全対策基準

情報セキュリティ基本方針

地方独立行政法人三重県立総合医療センター

目　　次

本規定は地方自治法第 244 条の６に基づく「サイバーセキュリティを確保するための方針」として取扱います。

第1章　目的

近年医療分野においても情報化の進展が望まれているなか、地方独立行政法人三重県立総合医療センター（以下「法人」という。）の各情報システムが取り扱う情報には、患者の個人情報のみならず運営上重要な情報など、外部に漏洩等した場合に極めて重大な結果を招く情報が多数含まれている。

これらの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、患者の財産、プライバシー等を守るとともに、事務の安定的な運営を行い、患者からの信頼の維持向上を図るため、地方独立行政法人三重県立総合医療センター電子情報安全対策基準（以下「本基準」という。）を定める。

このうち、本基準の対象、位置付け等基本的な事項について、地方独立行政法人三重県立総合医療センター情報セキュリティ基本方針に定めるものとする。

第2章　定義

本基準において、次の各項に掲げる用語の定義は、当該各項に定めるところによる。

1　ネットワーク

法人が組織として管理する通信網、通信関連機器、配線をいう。

2　情報システム

ハードウェア、ソフトウェア、ネットワーク、ネットワーク上で業務系並びにOA処理を行うために利用される機器及び記録媒体で構成されるものであって、これら全体で業務処理又は通信を行う仕組みをいう。

3　情報資産

ネットワーク及び情報システムの開発・運用にかかる全てのデータ並びにネットワーク及び情報システムで取り扱う全てのデータをいう。

4　機密性

許可された者のみが情報にアクセスできる状況を保持し、第三者に知られてはいけない情報の漏洩が防止されていることをいう。

5　完全性

情報の一部が欠如したり、全部又は一部が改ざんされることのない状態が保持されていることをいう。

6　可用性

許可された利用者が必要な情報にアクセスできる状態が保持されていることをいう。

7　情報セキュリティ

情報資産の機密性・完全性・可用性が維持されていることをいう。

第3章　情報資産への脅威

本基準を策定する上で、情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

脅威一覧

脅威の種類	脅威の詳細
サイバー攻撃	不正アクセス、ウイルス攻撃、サービス不能攻撃等
災害	火災、落雷、地震、風水害、その他災害等
インフラ障害	コンピュータシステム障害、諸設備の障害（電源設備への配慮、安定した電源供給)、ネットワーク障害、機器故障等
人的エラー	設計・開発の不備、プログラムの欠陥、操作ミス、メンテナンス不備、監査機能・委託管理の不備、マネジメントの欠陥、大規模・広範囲の疫病による要員不足等
不正・犯罪	情報資産の無断持ち出し、無許可ソフトウェアの使用、部外者の侵入、内部不正等

第4章　適用範囲

1　機関の範囲

本基本方針が適用される機関は、法人とする。

2　情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

ウ　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

第5章　本基準の位置付けと職員等の遵守義務

本基準は、法人が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、電子情報に関する情報セキュリティ対策の頂点に位置するものである。

したがって、地方独立行政法人三重県立総合医療センター理事長（以下「理事長」という。）をはじめ法人が所掌する情報資産に関する業務に携わる全ての職員及び外部委託事業者（以下「職員等」という。）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本基準を遵守する義務を負うものとする。

第6章　情報セキュリティ対策

1　情報セキュリティ組織体制の確立

法人の情報資産について、理事長が情報セキュリティ対策を推進・管理するための体制を確立するものとする。

2　情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

３　情報セキュリティ対策

上記第３章で示した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ずるものとする。

３－１　物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

３－２　人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員等に本基準の内容を周知徹底する等、教育及び啓発面において必要な対策を講ずる。

３－３　技術及び運用におけるセキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策、また、システム開発等の委託、ネットワークの監視、本基準の遵守状況の確認等の運用面の対策を講ずる。

また、緊急事態が発生した際に迅速な対応を可能とするための事後管理対策を講ずる。

第7章　情報セキュリティ監査の実施及び自己点検の実施

本基準が遵守されていることを検証するため、定期的に、又は必要に応じて情報セキュリティに関する監査及び自己点検を実施する。

第8章　評価及び見直しの実施

本基準が遵守されていることを定期的に検証し、本基準に定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティ等を取り巻く状況の変化に対応するために、本基準の見直しを実施する。

第9章　情報セキュリティ対策基準の策定

法人の様々な情報資産について、前章に規定する情報セキュリティ対策を講じるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

なお、情報セキュリティ対策基準は、公にすることにより法人の運営に重大な支障をきたすおそれがあることから非公開とする。

第10章 情報セキュリティ実施手順の策定

法人が組織として管理する情報システム及びネットワークの管理者は、当該情報システム等に関する情報セキュリティ対策の具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより法人の運営に重大な支障をきたすおそれがあることから非公開とする。

附則

本基準は、平成２４年４月１日から施行する。

附則

本基準は、令和８年４月１日から施行する。