

峽南医療センター企業団

情報セキュリティ基本方針

制定 令和3年4月1日

改正 令和8年4月1日

理念	2
1. 目的	2
2. 構成と位置付け	2
3. 定義	3
4. 適用情報	3
5. 基本原則	3
6. 適用対象者	3
7. 事故の予防と対応	3
8. 管理体制	3
9. 情報システム運用責任者	4
10. 情報の管理	4
11. 保管期間	4
12. 利用者識別	4
13. 苦情・質問の窓口の設置	4
14. 公開基準	4
15. 標準規格・関連法令	5
16. 教育	5
17. 監査	5
18. 文書の改廃	5
19. 罰則規定	5

理念

近年の ICT（情報通信技術）の著しい進展により、医療分野においても電子化が急速に普及し、診療に ICT を活用することは、もはや当たり前の時代になってきている。峡南医療センター企業団（以下「企業団」という。）においても、電子カルテシステムを導入し、院内ネットワークにより円滑な業務遂行を推進してきた。

あらゆる情報が電子化、システム化、ネットワーク化されたことによる利便性の増大は計り知れないものがある。しかしその一方で、コンピュータウイルス、不正アクセス、内部犯行、過失などによる情報の改ざんや破壊、機密情報漏洩などの問題が多発している今日の社会の現状を見過ごすわけにはいかない。ICT 導入は大きなメリットをもたらすとともに、情報の漏洩リスクが飛躍的に高まることになり諸刃の剣と言える。病院のような医療・健康情報を主として取り扱う事業者では、万一漏洩事故が発生すると個人の人生に及ぼす影響は非常に大きく、一般の企業と比べ、特に留意が求められている。

本企業団は、改正地方自治法（令和 6 年法律第 65 号）及び総務省が定める「地方公共団体における情報セキュリティポリシーに関するガイドライン」に基づき、一部事務組合として情報セキュリティを確保するための基本的な方針を定め、これを公表するとともに、当該方針に基づく必要な措置を講ずるものとする。

情報セキュリティポリシーは、企業団で取り扱う個人情報と、故意、過失、偶然の区別に関係なく、改ざん、破壊、漏洩から保護されることを目的とした方策をまとめたものである。企業団の全職員は、情報セキュリティの重要性を認識し、その適切な取り扱いと保護に努めるべく、この情報セキュリティポリシーを遵守しなくてはならない。

1. 目的

情報セキュリティポリシー（以下、「ポリシー」という）とは、組織の中にある情報を、安全に運用するための規約を文書化したものをいう。

ポリシーは、企業団の取り扱う個人情報を、故意、過失、偶然の区別に関係なく、改ざん、破壊、漏洩から保護すると共に、個人情報を利用する職員に対して、情報システムに関する安全管理の重要性、及び個人情報の適切な取り扱いと保護についての認識を高め、医療機関としての信頼感と安心感の向上を図る事を目的として制定する。

2. 構成と位置付け

ポリシーは、峡南医療センター企業団情報セキュリティ基本方針（本文書、以下「基本方針」という。）、峡南医療センター企業団医療情報システム運用管理規程（以下「運用管理規程」という。）の 2 つの階層によって構成されている。

○基本方針：企業団の情報システムに関する安全管理についての基本姿勢を示したもの

○運用管理規程：基本方針を受け、項目毎に遵守すべき事項について、組織的対策、技術的対策、人的対策毎に具体的にまとめたもの

3. 定義

情報システムとは、企業団で運用する電子カルテシステム及び電子カルテシステムと接続する部門システム並びに接続機器など診療情報を取り扱うシステム、及び人事・労務管理システムなど職員情報等の個人情報を取り扱う全てのシステムのことをいう。

4. 適用情報

ポリシーを適用する情報は、情報システムで取り扱う電子情報だけでなく、情報システムへ入力する前の紙媒体の情報や、職員の履歴書等全ての個人情報を適用範囲とする。

5. 基本原則

企業団の情報システムは、次に掲げる基本原則により運用する。

- (1) 保存義務のある情報の電子媒体による保存については、情報の真正性、見読性、保存性を確保する。
- (2) 情報システムの利用に当たっては、守秘義務を遵守し、個人の情報を保護する。
- (3) 情報システムへのコンピュータウイルスの侵入及び外部からの不正アクセスに対して必要な対策を講じる。原則、ソフトウェアのインストール及び USB メモリ等の外部記憶媒体の接続を禁止する。

6. 適用対象者

ポリシーは、企業団の業務に携わる者（常勤職員、会計年度任用職員、ボランティア、実習生など）の雇用形態、職位、資格、勤務地を問わず、全職員等に対して適用するものとする。ただし、ポリシーの対象となる業務を外部に委託する場合には、別途、本ポリシーに準拠した内容の外部委託契約を締結しなければならない。

7. 事故の予防と対応

企業団は、ポリシーの遵守により、情報漏えい事故等の発生の予防に努める。万一、事故が発生した場合には、その事実を速やかに公表し、再発防止策を含む適切な対策を速やかに講じる。さらに、事業継続を確実にするため、災害なども含めた緊急事態を想定した事業継続計画の策定とその点検を推進する。

8. 管理体制

ポリシーの維持管理は、情報システム委員会（以下、「委員会」という）が行う。各部署の長は、委員会の指示を受け、各部署に置いてポリシーが遵守されるように指導、教育を

行う。

9. 情報システム運用責任者

情報システム運用責任者（以下、「運用責任者」という）を置き、企業長をもってこれに充てる。運用責任者は、医療情報システムの安全管理に必要な、組織的、人的、技術的、物理的対策を実施し、維持し、かつ、改善するために不可欠な資源を用意する。また、情報システムを円滑に運用するため、情報システムに関する運用を担当するシステム管理者を置き、院長をもってこれに充てる。

10. 情報の管理

情報システムで取り扱う情報は、情報の取得から利用・保管・廃棄まで流れに沿ったリスク分析を実施し、リスクに対応した適切な取り扱い方法を運用管理規程、各種手順書等に規定し、適切に管理・運用する。

11. 保管期間

情報システムで取り扱う情報の保管期間は、法令保管期間を基本とする。また、情報システムへのアクセスログを記録し、その記録を最低5年保管する。

12. 利用者識別

情報システム利用者の登録を管理し、そのアクセス権限を規定し、不正な利用を防止する。

13. 苦情・質問の窓口の設置

個人情報の取扱い及び情報システムの運用に関して、本人及びシステム利用者からの苦情及び質問を受け付け、適切かつ迅速な対応を行うために、苦情・質問を受け付ける窓口（ヘルプデスク）を設ける。

14. 公開基準

本基本方針は、改正地方自治法の規定に基づき、企業団における情報セキュリティに関する基本的な考え方を示すものとして、全職員等に周知するとともに、対外的に公表するものとする。

なお、本基本方針に基づき策定される運用管理規程、各種手順書その他詳細な運用に関する文書については、企業団の情報資産を保護する観点から非公開とし、適切に管理するものとする。

また、ICT技術の進展や社会環境の変化を踏まえ、本基本方針は必要に応じて見直しを行うものとし、改訂した場合には速やかに公表するものとする。

15. 標準規格・関連法令

委員会事務局は、標準規格等についての改訂状況を確認し、改正が行われた際には、整合性を維持するためにその内容に準拠した改訂を行う。

16. 教育

委員会は、個人情報を利用する全職員等に対して、情報セキュリティの重要性と、個人情報の適切な取り扱い、及び安全管理について意識面及び技術面の向上を目的として、継続的な教育を行う。

17. 監査

情報システムの適正な運用とその有効性を維持するために、毎年1回内部監査を実施する。ただし、高度な技術を要する監査が必要な場合は、外部の専門家による外部監査を導入する。運用責任者は、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じる。

18. 文書の改廃

ポリシーを改訂する際は、委員会決議・承認及び運用責任者の承認を必要とする。各部門で作成した運用規定については部門長の承認を経て改訂することができる。

19. 罰則規定

委員会は、上記に定める職員がポリシーに違反し、企業団の情報セキュリティに重大な影響を与えた場合、もしくはそれに準ずる悪質な行為などが認められた場合、企業長に対して、峽南医療センター企業団職員分限懲戒審査委員会要綱に基づいた審査の申請を行うことがある。

以上