地方独立行政法人山形県・酒田市病院機構
情報セキュリティ基本方針
第１版

（基本理念）

近年の IT 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 IT を活用することは、もはや当たり前の時代になっている。当機構においても、平成 19 年 3 月に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が、その一方で、コンピュータウィルス、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。IT 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。

情報セキュリティポリシーは、当機構で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、漏洩から保護されることを目的とした方策をまとめたものである。当機構の全従業者は、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。

（目的）

第１条　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、当機構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従業者に対して、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。

（構成と位置付け）

第２条　ポリシーは、基本方針（本文書）、運用管理要綱、運用手順の３つの階層によって構成する。

〇基本方針：当機構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

〇運用管理要綱：基本方針を受け、運営する組織ごとに遵守すべき事項について、組織的対策、技術的対策、人的対策を具体的にまとめたもの

〇運用マニュアル：運用管理要綱を受けて、情報システムごとに実際の運用方法について示したもの

（定義）

第３条　情報システムとは、当機構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・給与・就業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。

（適用範囲）

第４条　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、従業者（役職員、派遣職員、嘱託職員、日々雇用職員、ボランティア、

実習生など）の履歴書等全ての個人情報を適用範囲とする。

（基本原則）

第５条　当機構の情報システムは、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、患者および職員の個人情報を保護する。

（３）情報システムへのコンピュータウィルスの侵入及び内部または外部からの不正アクセスに対して必要な対策を講じる。原則として許可されていない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。

（適用対象者）

第６条　ポリシーは、従業者の雇用形態、職位、資格、勤務地を問わず、全従業者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。

（事故の予防と対応）

第７条　当機構は、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。

（管理者、責任者の任命）

第８条　最高情報セキュリティ責任者（以下、「CISO」という。）を置き、日本海総合病院病院長をもって充てる。CISOは、ポリシーの策定およびセキュリティ施策の策定を行い、セキュリティインシデント発生時の体制を整備する。

２　総括保護管理者を置き、法人管理部長をもって充てる。総括保護管理者は保有個人情報の管理に関する事務を総括する。

（情報の管理）

第９条　情報システムで取り扱う情報の取扱は、情報の取得から利用・保管・廃棄までの情報の取り扱いの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要綱、各種運用マニュアル等に規定し、適切に管理・運用する。

（保管期間）

第１０条　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して別途定める。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。

（利用者識別）

第１１条　情報システムの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。

（苦情・質問の窓口の設置）

第１２条　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、運営する組織ごとに苦情・質問を受け付ける窓口（ヘルプデスク）を設ける。

（公開基準）

第１３条　ポリシーは当機構の Web サイト上で公開する。IT 技術が日々発展していることと社会環境が変化する事を踏まえて適時改訂を行うことがあるが、改訂によって変更された箇所についても、改訂後即時に公開する。

（標準規格・関連法令）

第１４条　情報システムの運営に際し、標準規格や関係法令等の改訂状況を確認し、改訂が行われた際には、整合性を維持するためにその内容に準拠したシステム改修を行う。

（教育）

第１５条　統括保護管理者は、個人情報を利用する全ての従業者に対して、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。

（監査）

第１６条　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。総括保護管理者は、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。

（文書の改廃）

第１７条　ポリシーを改訂する際は、CISO 及び統括保護管理者の承認を必要とする。各部門で作成した運用マニュアルについては部門長の承認を経て改訂することができる。

（罰則）

第１８条　従業者がポリシーに違反し、当機構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、就業規則に基づいた処罰の申請を行うことができる。

改 訂 履 歴

版数	改訂年月日	改訂内容
1.0	令和 8 年 3 月 31 日	新規制定

※ 版数は新規制定を第 1.0 版とし、改訂が発生した際は第 1.1 版とする。

※ 改訂があった場合は、必ず改訂内容を記載すること。