三重県立志摩病院　情報セキュリティポリシー（基本方針）

第 1 章　目的

本ポリシーは、三重県立志摩病院（以下「当院」という。）において取り扱うすべての情報資産を適切に保護し、患者の生命および安全、診療の継続性、社会的信頼を確保することを目的とする。

当院は、情報セキュリティ対策を単なる IT 管理の問題ではなく、医療安全および病院経営に直結する重要事項として位置づける。また、情報資産の機密性・完全性・可用性を適切に維持することを、情報セキュリティ対策の基本原則とする。

第 2 章　適用範囲

本ポリシーは、以下に掲げるすべての者に適用する。

- 当院の全職員（常勤・非常勤・派遣職員等を含む）
- 当院業務を受託する委託業者およびその従業者
- 当院情報システムを利用するすべての関係者

第 3 章　情報資産の定義

本ポリシーにおける情報資産とは、次に掲げるものをいう。

- 診療情報、個人情報
- 医療情報システムおよび関連機器
- 業務情報、経営情報
- ネットワーク、クラウドサービス等の情報基盤

第 4 章　役割と責任

1. 経営層の責任

経営層は、当院における情報セキュリティ確保の最終責任者として、必要な体制整備、資源配分、意思決定を行う責任を負う。

2. 最高情報セキュリティ責任者（CISO）

CISO は、当院の情報セキュリティに関する方針を統括し、予防、対応、再発防止に関する活動を監督する。

3. 職員および関係者の責任

すべての職員および関係者は、本ポリシーならびに関連規程を理解し、情報セキュリティ確保に主体的に取り組む責任を負う。

第 5 章　情報セキュリティの基本原則（平時）

当院は、平常時において以下の基本原則に基づき情報セキュリティ対策を実施する。

1. **必要最小限の原則**
    - 情報へのアクセスは、業務上必要な範囲に限定する。
2. **本人責任の原則**
    - ID・パスワード等の認証情報は本人のみが使用する。
3. **予防優先の原則**
    - 事故発生後の対処よりも、予防を優先する。
4. **異常は即報告の原則**
    - 異常や不審な事象を発見した場合は、速やかに報告する。

第 6 章　インシデント対応の基本姿勢（有事）

情報セキュリティインシデントが発生した場合、当院は以下の姿勢で対応する。

- 患者の安全および診療継続を最優先とする
- 被害拡大防止を最優先で実施する
- 個人の判断による独断対応を行わず、定められた体制による統制された対応を行う

具体的な対応手順については、「サイバー攻撃対応 BCP」に委ねるものとする。

第 7 章　関連規程との関係

本ポリシーは、以下の規程・内規・マニュアルの上位文書として位置づける。

- 事業継続計画（サイバー攻撃対応 BCP）
- 医療情報システム運用管理規程
- 各種情報セキュリティ関連内規
- CSIRT 対応マニュアル

これらの文書は、本ポリシーに基づいて整備・運用されるものとする。

また、本ポリシーの整備および運用にあたっては、「医療情報システムの安全管理に関するガイドライン」（厚生労働省）の趣旨および最新の動向を踏まえるものとする。

第 8 章　教育・見直し

当院は、情報セキュリティに関する教育および訓練を継続的に実施する。本ポリシーは、情報システム委員会および情報セキュリティ部会において定期的に点検を行い、社会情勢、技術動向およびインシデントの発生状況等を踏まえ、必要に応じて見直すものとする。

附　則

本ポリシーは、令和8年6月1日から施行する。