管理番号：SEC-01

地方独立行政法人 佐賀県医療センター好生館

情報セキュリティポリシー

【初版】

制定日：2026 年 3 月 17 日

施行日：2026 年 4 月 1 日

【改訂履歴】

版数	改訂日	改訂者	改訂内容の概要
初版	2026 年 3 月 17 日	医療情報係	「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」（令和 7 年 3 月 28 日改定）の改正法施行日（令和 8 年 4 月 1 日）に準拠するため、新設制定。これに伴い既存の「地方独立行政法人佐賀県医療センター好生館病院情報システム運用管理要綱」は令和 8 年 3 月 31 日をもって廃止する。

目次

第Ⅰ部 情報セキュリティ基本方針

1. 目的

1.1. 策定の背景と目的

当館は、佐賀県における基幹的な急性期病院としての使命を果たすため、多くの情報システム及び医療機器を運用し、極めて機密性の高い診療情報を取り扱っている。これらの情報資産をサイバー攻撃、災害、及び過失等の脅威から保護し、診療業務を継続することは、患者の生命と健康を守るための最優先課題である。本情報セキュリティポリシーは、当館における情報セキュリティ対策の基本方針及び基準を定め、全職員等に遵守させることにより、情報資産の安全性、信頼性、及び可用性を確保することを目的とする。

1. 2. 準拠・参照すべき指針及び標準

本ポリシーの策定及び運用にあたっては、次に掲げる指針、手引き及び技術標準（以下「準拠指針等」という。） を根拠とするものとする。

（1） 行政による情報セキュリティ指針

①「医療情報システムの安全管理に関するガイドライン」

厚生労働省が策定し、当館が準拠すべき最上位の指針とするものとする。

②「サイバー攻撃を想定した BCP 策定の確認表のための手引き」

厚生労働省が定める「医療情報システムの安全管理に関するガイドライン」に関連する実務的手引きとするものとる。

③「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」

経済産業省及び総務省が策定した、外部事業者との連携において参照すべき指針とするものとする。

④「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」

総務省が策定し、本情報セキュリティポリシーを策定する際の根拠とするガイドラインとするものとする。

（2） 個人情報保護に関する指針

①「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」

個人情報保護委員会（厚生労働省） が策定した、個人情報保護法関連ガイドラインを補完し、具体化する実務的資料とするものとする。

（3） 業界団体による技術標準

①「リモートサービスセキュリティガイドライン」
一般社団法人保健医療福祉情報システム工業会（JAHIS） が策定した、リモートサービス等の技術的安全性に関して参照すべき標準とするものとする。
②「製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）」
一般社団法人保健医療福祉情報システム工業会（JAHIS） が策定した、医療情報システム及び医療機器の安全管理措置の状況を包括的に開示するための標準フォーマットとするものとする。

2. 定義

（1） ネットワーク

コンピュータ等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。

（2） 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(3) 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(4) 情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（5） 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（6） 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（7） 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（8） ネットワーク区分（NW レベル）

ネットワークは、情報の重要度とリスクに応じて Level0 から Level5 に区分し、分離・管理する。NW レベルの具体的な定義、ネットワーク構成上の扱い、及び取扱情報の詳細は、「APP-01 ネットワーク区分（NW レベル） 定義表」に定める。また、NW レベルに関する通信制御、例外接続（保守等） の許可条件、監査・記録等の具体的な運用は、情報セキュリティ対策基準に従う。なお、NW レベルのうち運用上の主要な三領域（HIS 系：Level5、外部連携系：Level4、インターネット接続系：Level3）を定義する。HIS 系（Level5） 及び外部連携系（Level4） は、同一の閉域網上に構築する場合であっても、NW レベルに基づき論理的に分離し、相互の通信は必要最小限に制御する。

また、当該閉域網上の業務利用は、原則として VDI（画面転送方式） を介して行い、二要素認証を適用する。具体的な運用要件は情報セキュリティ対策基準に定める。

統合閉域網（セキュアゾーン：Level5/Level4） の構成上の扱い（同一閉域網上での論理分離、外部接続点の位置づけ等） は APP-01 に定める。

また、統合閉域網に適用する共通セキュリティ統制（外部接続点の集約、許可通信の管理、VDI（画面転送方式） 、二要素認証（当館では二要素認証を必須とする。） 、端末制御、ログ取得・監視等） の詳細は、情報セキュリティ対策基準第 3 章、第 6 章及び第 7 章に定める。

（９） Level5（HIS 系）

電子カルテシステム及び部門システムを配置する領域。外部との通信を原則遮断し、当館の診療継続の根幹を成す最重要ネットワークをいう。

（１０） Level4（外部連携系）

HIS 系ネットワークと同じ閉域網にありながらも、特定の外部機関やプラットフォームとの通信を前提として運用するネットワークをいう。

（１１） Level3（インターネット系）

インターネットへの接続を前提とし、事務用システム、メール、及び Web 閲覧等を行う領域（Level3） 。病院経営及び一般的な事務運営を支援するネットワークをいう。

（１２） 通信経路の分割

HIS 系とインターネット系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

（１３） 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

（１４） 厚労省ガイドライン

「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） の略称。

（１５） ２省ガイドライン

「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（経済産業省・総務省） の略称。

（１６） ３省２ガイドライン

厚労省ガイドラインと２省ガイドラインの略称。

（１７） リモートガイドライン

「リモートサービスセキュリティガイドライン」（一般社団法人保健医療福祉情報システム工業会（JAHIS） ） の略称。

（１８） セキュリティ開示書（MDS/SDS）

「製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS） 」（一般社団法人保健医療福祉情報システム工業会（JAHIS） ） の略称。

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） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３） 地震、落雷、火災等の災害によるサービス及び業務の停止等

（４） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（５） 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4. 適用範囲

（１） 組織及び人的範囲

本基本方針が適用される範囲は、当館の全組織（病院、看護学院、総合教育研修センター、総合臨床研究所等を含む。） とする。対象者は、当館の役員、職員等（医師、看護師、薬剤師、コメディカル、事務職員等） 、臨時・非常勤職員、派遣職員、委託職員、並びに当館の情報資産を利用する実習生、研修生及び学生とする。

（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。

① 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

② 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。）

③ 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

5. 職員等の遵守義務

職員、臨時・非常勤職員、派遣職員、委託事業者の要員、研修医・実習生等、当館の情報資産を取り扱う可能性があるすべての者（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ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

6. 情報セキュリティ対策

上記３の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じる。

（１） 組織体制

当館の情報資産について、情報セキュリティ対策を推進する全館的な組織体制を確立する。

（２） 情報資産の分類と管理

当館の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（３） 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策（領域分離等） を踏まえ、NW レベルに基づきネットワークを分離・管理する。なお、運用上の主要領域として以下の三領域を定義する。HIS 系（Level5） 及び外部連携系（Level4） は同一の閉域網上に構築する場合であっても、NW レベルに基づき論理的に分離し、両領域には同等のセキュリティ統制（例：VDI（画面転送方式） を介した利用、二要素認証の必須化、端末からの情報持ち出し不可設定等） を適用する。ただし、外部通信の前提（許可範囲） は領域の目的に応じて異なるため、具体的な通信制御及び例外許可の要は情報セキュリティ対策基準に定める。

① Level5（HIS 系）

電子カルテシステム及び医療機器連携等、診療継続の根幹を成す最重要資産を配置する領域。外部との通信は原則として遮断し、診療・診察目的で不可避な医療機器・医療システムの通信、又はベンダーのリモート保守等、必要性が認められる場合に限り、対策基準に基づき限定して許可する。

② Level4（外部連携系）

オンライン資格確認、レセプト請求、電子カルテ情報共有プラットフォーム等の国の施策との通信、並びに PHR 系の情報提供等、外部通信を前提として運用する領域。HIS 系と同等のセキュリティ統制を適用した上で、接続先及び通信要件を必要最小限に限定し、対策基準に基づき管理する。

③ Level3（インターネット系）

インターネットへの接続を前提とし、事務用システム、及び Web 閲覧等を行う領域。

（４） 物理的セキュリティ

サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

（５） 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（６） 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（７） 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（8） 業務委託と外部サービス（クラウドサービス） の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

外部サービス（クラウドサービス） を利用する場合には、利用に係る規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（9） 評価・見直し

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し、その結果を踏まえて運用改善を行う。

具体的な実施方法、見直し手順及び改定判断は、第 7 章から第 9 章に定める。

7. 情報セキュリティ監査及び自己点検の実施

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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

9. 情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10. 情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するため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、情報セキュリティ対策基準および情報セキュリティ実施手順は、公にすることにより当館の診療継続及び病院運営に重大な支障を及ぼすおそれがあることから非公開とする。