掛川市・袋井市病院企業団　情報セキュリティ基本方針

（目的）

第１条　本基本方針は、掛川市・袋井市病院企業団（以下「企業団」という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、企業団が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

（定義）

第２条　本基本方針における用語の定義は、以下のとおりとする。

(1) 情報セキュリティ

情報資産の機密性、完全性、可用性を維持することをいう（真正性、責任追跡性等を含む）。

(2) 機密性

許可さ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。

(3) 完全性

情報が破壊、改ざん、又は消去されていない正確な状態を確保することをいう。

(4) 可用性

許可された者が、必要なときに中断されることなく情報やシステムを利用できる状態を確保することをいう。

(5) 情報資産

企業団が保有又は管理する全ての情報（診療録、看護記録、検査データ、事務文書、職員情報等）及びそれらを処理・保存・伝送する情報システム（電子カルテ、部門システム、医療機器、ネットワーク機器、記録媒体等）をいう。

(6) 医療情報系

電子カルテや部門システム等の患者情報を取り扱う情報システム及びデータをいう。

(7) インターネット系

インターネットに接続された情報システム及びその情報システムで取扱うデータをいう。

(8) 通信経路の分割

医療情報系（以下「HIS 系」という。）、インターネット系の両環境間を分離したうえで、安全が確保された通信のみを許可できるようにすることをいう。

(9) 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。

(10) 職員等

企業団に勤務する全ての職員（会計年度任用職員等を含む）、及び企業団の情報資産を利用する外部委託事業者、実習生、研究員等をいう。

（適用範囲）

第３条　本基本方針は、企業団の管理下にある全ての情報資産、及びそれらを利用する全ての職員等に適用する。なお、外部委託事業者に対しては、契約に基づき本基本方針に準拠したセキュリティ対策の実施を義務付けるとともに、必要に応じて監査を実施する権限を留保する。

（法令等の遵守）

第４条　企業団及び職員等は、情報セキュリティに関する法令、個人情報の保護に関する法律、国が定める指針（総務省「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」、厚生労働省「医療情報システムの安全管理に関するガイドライン」等）、及び企業団が別途定める規定を遵守しなければならない。

（対象とする脅威）

第５条　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、外部委託管理の不備、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

（情報セキュリティ対策）

第６条　企業団が所掌する情報資産を脅威から保護するため、以下の対策を講ずる。

(1) 組織体制

情報セキュリティ対策を推進する組織体制を確立する。

(2) 情報資産の分類と管理

企業団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、以下の対策を講じる。

ア　医療情報系

他の領域との通信ができないようにした上で、端末の持出及び患者情報の流出対策を行う。

イ　インターネット系

必要に応じて不正接続及び不正通信の監視機能の強化等の情報セキュリティ対策を実施する。

ウ　オンライン資格確認系

原則として他の領域との通信をできないようにした上で、データの持出及び物理的な持出対策等の実施により患者情報の流出対策を行う。

(4) 物理的セキュリティ対策

ア　情報システムを設置する施設への不正な立ち入り、情報資産の損傷や妨害等を防ぐため、入退室や機器管理上の物理的な対策を講ずる。

イ　情報システムの利用を企業団職員及び申請の後、承認された者のみに制限する。

(5) 人的セキュリティ対策

情報資産に接する職員について権限と責任を明確にするとともに、全ての職員が情報セキュリティの考え方や意識を共有するための教育や啓発が行われるよう、必要な措置を講ずる。

(6) 技術的セキュリティ対策

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) 運用セキュリティ対策

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。また、外部サービスの利用においては、企業団、利用者、外部サービス提供者の役割及び責任分担を明確にし、十分なセキュリティ要件を満たすよう対策を講じる。

⑼ 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、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

（情報セキュリティ監査及び自己点検の実施）

第７条　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。

（情報セキュリティポリシーの見直し）

第８条　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。

（情報セキュリティ対策基準の策定）

第９条　情報セキュリティ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。

（情報セキュリティ対実施手順の策定）

第 10 条　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別途策定する。

附　則

この規程は、令和８年４月１日から施行する。