豊川市民病院
情報セキュリティポリシー基本方針

平成 26 年 10 月　　策　　定
平成 27 年　4 月　　一部改定
令和 2 年 10 月　　一部改定
令和 5 年　4 月　　全部改定
令和 6 年　4 月　　一部改定

豊川市民病院

＜目次＞

第１章　情報セキュリティ基本方針 1

1. 目的 1
2. 用語の定義 1
3. 適用範囲 1
4. 情報セキュリティ対策 2
5. 標準規格・関連法令等の遵守 2
6. 情報セキュリティ監査 2
7. 情報セキュリティポリシーの見直し 3
8. 情報セキュリティ対策基準の策定 3
9. 情報セキュリティ実施手順の策定 3

第２章　情報セキュリティ対策基準 4

1. 組織体制 4
2. 情報資産の分類と管理 5

第 1 章　情報セキュリティ基本方針

1. 目的

当院が取り扱う情報資産には、個人情報や診療情報など機微な情報が多数存在しており、外部への漏えい、滅失、毀損等が発生した場合、重大な結果を招くこととなる。

そこで、基本方針では、安全かつ合理的な運用を図るための情報セキュリティの確保と法令で保存が義務付けられている診療録、診療諸記録など当院の情報資産の取扱いに関する基本的な事項について定めることを目的とするものである。

2. 用語の定義

情報セキュリティポリシーで使用する用語の定義は、以下のとおりとする。

(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

基本方針及び対策基準をいう。

(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。

3. 適用範囲

基本方針の適用範囲は、以下のとおりとする。

(1) 対象情報システムの範囲

実施手順の対象とする情報システムは、当院の運用する総合医療情報システムとする。

総合医療情報システムとは、電子カルテシステムが接続されたネットワーク（以下「HIS系LAN」という。）及びインターネット用グループウェアシステムが接続されたネットワーク（以下「INT系LAN」という。）を利用する情報システムとする。

(2) 対象情報資産の範囲

管理対象となる情報は、情報システムで取り扱う電子情報だけでなく、情報システムから出力された紙情報及び情報システム仕様書等システム関連文書もこれに含めるものとする。

(3) 適用対象者

適用対象者は、当院の情報資産及び情報システムを利用する全ての職員等（職員、非常勤、臨時職員）及び委託事業者とする。

4. 情報セキュリティ対策

当院の情報システムは、次に掲げる情報セキュリティ対策を考慮し、運用する。

(1) 組織体制

当院の情報システムについて、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

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

(3) 物理的安全対策

重要な情報を取り扱うサーバやネットワーク基幹機器等が設置される場所への鍵設置、パソコンへの盗難防止ワイヤー設置など、物理的な情報セキュリティ対策を講じる。

(4) 技術的安全対策

IT技術を活用し、コンピュータ等の管理、アクセス制御設定、不正プログラム対策等の技術的な情報セキュリティ対策を講じる。

(5) 人的安全対策

職員等が遵守すべき情報セキュリティ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情報セキュリティ対策を講じる。

5. 標準規格・関連法令等の遵守

情報システムの利用者は、標準規格及び関連法令を遵守し、これに従わなければならない。なお、システム変更・改定時の対象とするため、当院で遵守すべき法令及び標準規格の列挙を行い、変更状況を確認し、維持する。

6. 情報セキュリティ監査

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。

7. 情報セキュリティポリシーの見直し

情報セキュリティに関する標準規格・関連法令等の改正や情報セキュリティ監査等により是正が必要と判断される場合には、情報セキュリティポリシーの見直しを行う。

8. 情報セキュリティ対策基準の策定

上記 4、5、6 及び 7 に準ずる対策等を実施するために、基本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。

9. 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。情報セキュリティ実施手順はセキュリティの観点から非公開とする。なお、本文中の「運用管理規程」は、情報セキュリティ実施手順及び各種マニュアルのことを指すものとする。

第２章　情報セキュリティ対策基準

本対策策基準は、情報セキュリティ基本方針を実行に移すための、当院における情報資産に関する情報セキュリティ対策の基準を定めたものである。

1．組織体制

(1) 組織体制

ア　最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）

① 当院に最高情報セキュリティ責任者（以下「CISO」という。）を置き、病院長をもってこれに充てる。CISO は当院における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

② CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。

③ CISO は、情報セキュリティインシデントに対処するための体制（CSIRT Computer Security Incident Response Team 、以下「CSIRT」という。）を整備し、役割を明確化する。

イ　統括情報セキュリティ責任者

① 当院に統括情報セキュリティ責任者を置き、事務局長をもってこれに充てる。統括情報セキュリティ責任者は、CISO を補佐しなければならない。

② 統括情報セキュリティ責任者は、当院の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③ 統括情報セキュリティ責任者は、当院の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

④ 統括情報セキュリティ責任者は、情報セキュリティ責任者、情報セキュリティ管理者、医療情報システム安全管理責任者及び医療情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑤ 統括情報セキュリティ責任者は、当院の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISO の指示に従い、CISO が不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。

ウ　情報セキュリティ責任者

① 当院に情報セキュリティ責任者を置き、副院長、診療局長、看護局長、診療技術局長、薬局長をもってこれに充てる。

② 情報セキュリティ責任者は、その所管する局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

エ　情報セキュリティ管理者

① 当院に情報セキュリティ管理者を置き、各診療科の長、各看護科長、各部門主幹・科長・技師長、各センター主幹、事務局の課長・主幹をもってこれに充てる。

② 情報セキュリティ管理者は、その所管する各科（課）の等の情報セキュリティ対策に関する権限及び責任を有する。

オ　医療情報システム安全管理責任者

① 当院に医療情報システム安全管理責任者を置き、経営企画室主幹をもってこれに充てる。

② 医療情報システム安全管理責任者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③ 医療情報システム安全管理責任者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

④ 医療情報システム安全管理責任者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

カ　医療情報システム運用担当者

医療情報システム安全管理責任者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を医療情報システム運用担当者とする

キ　情報セキュリティ監査統括責任者

情報セキュリティ対策を円滑に運営するため、情報セキュリティ監査を担当する情報セキュリティ監査統括責任者を置き、医療情報管理委員会委員長をもってこれを充てる。

ク　医療情報管理委員会

情報セキュリティポリシーに関する取扱いに関し、以下のことを実施する組織として、医療情報管理委員会を設置する。

① 必要な事項を審議すること

② 定期的に監査すること

ケ　CSIRT

情報セキュリティインシデントに対して迅速かつ適正に対応するため、CSIRT（Computer Security Incident Response Team：シーサート）を設置する。CSIRT 要員は経営企画室職員をもってこれに充てる。

2. 情報資産の分類と管理

当院における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、リスクに応じた管理を行うものとする。

(1) 情報資産の分類

分類	分類基準	取扱制限
3	①個人情報または個人情報にアクセスすることが可能となる情報（情報システムに関する ID・パスワード情報等）が含まれる ②漏洩、改ざん、消去等が患者の生命・財産・プライバシーまたは医療事務の執行に重大な影響を及ぼすもの。個人情報は分類３に該当する。	・必要以上の複製及び配付禁止 ・パスワードによる操作権限設定 ・無許可外部記録媒体の利用制限 ・サーバ室への立ち入り制限 ・バックアップ ・外部記録媒体の施錠可能な場所への保管 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択
2	①当院の内部情報で、その漏洩、改ざん、消去等が医療事務の執行に影響を及ぼすもの。	
1	上記以外の情報資産	―

(2) 情報資産のリストアップ及びリスク分析

(1)の分類に基づき、各科（課）で取り扱う情報資産をリストアップし、それらの情報資産について、以下の脅威を想定したリスク分析を実施し、その結果を保管すること。

ア　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・重要情報の搾取・内部不正等

イ　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程違反、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

ウ　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

エ　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の運用の機能不全等

オ　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

(3) 情報資産を格納するシステムの管理

情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）及びシステム責任者一覧（設置事業者等含む）を作成し、常に最新の状態を維持しなければならない。また、情報システムベンダ及びサービス事業者から技術的対策等の情報を収集しなければならない。