

横浜町田関節脊椎病院

病院情報システム

運用管理規程

【第3版】

改訂履歴

- | | | |
|---|------------|------|
| 1 | 2020年6月1日 | 新規作成 |
| 2 | 2020年8月1日 | 第2版 |
| 3 | 2024年8月14日 | 第3版 |

目次

第1章 目的

- 1 電子カルテ運用開始日

第2章 管理組織

- 1 情報システム管理者
- 2 情報システム委員会

第3章 情報システムに関する理念

- 1 理念

第4章 電子保存する情報の範囲

- 1 保存範囲
- 2 保存情報の保護

第5章 利用者

- 1 情報システム利用者
- 2 利用者管理者
- 3 情報システムの機能要件

第6章 情報システム安全管理基準

- 1 機器の管理
- 2 記録媒体の管理
- 3 ソフトウェアの管理
- 4 資源管理
- 5 ドキュメント管理
- 6 ネットワーク管理
- 7 事故対策

第7章 情報システムのセキュリティ方針書

- 1 方針
- 2 目的
- 3 修正
- 4 適用範囲
- 5 配布

- 6 情報システム
- 7 リスク管理
- 8 プライバシー情報
- 9 セキュリティ管理
- 10 責任の分散
- 11 違反者に対する処置
- 12 診療に関わる情報のアクセス
- 13 電子カルテへのアクセス
- 14 物理的なセキュリティ管理
- 15 情報セキュリティ管理
- 16 運用管理
- 17 スタッフセキュリティ

第8章 管理者マニュアル

- 1 はじめに
- 2 管理者及び情報システム委員会
- 3 義務と罰則
- 4 利用者への指導及び構成の管理
- 5 システムの利用
- 6 ネットワークの利用及び構成の管理
- 7 院外接続管理
- 8 利用環境面におけるセキュリティについての管理者の義務
- 9 運用管理面におけるセキュリティについてのシステム資源管理
- 10 情報システムの利用時のセキュリティ
- 11 法的に利用される電子カルテ情報を出力する装置の管理
- 12 コンピュータウイルス対策
- 13 事件又は異常現象の報告
- 14 教育・訓練

第9章 利用者マニュアル

- 1 はじめに
- 2 情報システムの利用
- 3 義務と罰則
- 4 情報システムの利用時のセキュリティ
- 5 情報システム運用管理面でのセキュリティ
- 6 ドキュメント管理

- 7 電子カルテシステムの利用時のパスワードセキュリティ
- 8 法的に利用される電子カルテ情報の管理
- 9 コンピュータウィルス対策
- 10 事件又は異常現象の報告
- 11 教育・訓練

第10章 情報システムダウン対策マニュアル

- 1 はじめに
- 2 目的
- 3 システム障害の対策対象
- 4 システムダウン障害区分
- 5 システムダウン時の基本姿勢
- 6 システムダウン障害時の対応

(別紙)

- ・可搬記憶媒体使用申請書兼診療データ二次利用申請書（案）
- ・電子カルテ修正依頼票（案）

第1章 目的

この規程は、当病院において、法令に保護義務が規定されている診療録および診療諸記録（以下「保存義務のある情報」という）の電子媒体による保存のために使用される機器、ソフトウェア、ソフトウェアサービス、及び運用に必要な仕組み全般（以下「情報システム」という）について、その取扱いおよび管理に関する事項を定め、当病院において保存義務のある情報を適正に保存するとともに、適正に利用することに資することを目的とする。また、ここに規定する原則とそれに基づく各種運用マニュアル等は、すべて院外の専用線等を含むネットワークを介して行われる業務を前提としている。

1 電子カルテ運用開始日

○電子カルテシステム使用開始日：2020年06月01日

稼働日以前の移行データについては紙カルテを正とする。

第2章 管理組織

1 情報システム管理者

1) 情報システム管理者の情報管理に関する責務

- (1) 当病院に情報システム管理者（以下「システム管理者」という）を置き、病院長をもってこれに充てる。
- (2) システム管理者は、電子保存に用いる機器、ソフトウェア、及びソフトウェアサービスを導入するに当たって、システムの機能を確認し、これらの機能が「法令に保存義務が規定されている診療記録及び診療諸記録の電子媒体による保存に関するガイドライン」に示される各項目に適合するよう留意すること。
- (3) システム管理者は、「情報システム安全管理基準」と「セキュリティ方針書」を作成し、さらに効率的に運用するために「情報管理をする組織」を設けなければならない。
- (4) システム管理者は、情報の共有化を図るとともに、共有化によって起こる各種情報の漏洩防止のためにその「セキュリティ権限付与」を設定し常に管理しなければならない。
- (5) システム管理者は、情報システムを利用するために必要な「運用規程」を設けなければならない。
- (6) システム管理者は、情報システムを円滑に運営し、情報システム全体の管理状況を把握しなければならない。
- (7) システム管理者は、情報システムが常に業務の効率化と円滑化ができるように情報収集し、合理的運営を指針するために適切に、病院情報システム運営委員会（以下「情報システム委員会」という）に諮問しなければならない。
- (8) システム管理者は、情報システム委員会の責任者等を選任あるいは承認し、同委員会から答申あるいは協議内容について報告を受けなければならない。

2 情報システム委員会

1) 情報セキュリティ管理

- (1) 情報システムに関する取扱いおよび管理に関し必要な事項を審議し、システム管理者のもとに情報システムを管理するものとする。
- (2) 画面ハードコピーをとった資料など、不要となった診療情報等を安全な方法で、速やかに廃棄・消去することを各部門に指導しなければならない。

2) 情報マスタ管理

- (1) 情報システムに関する取扱いおよび管理に関し必要な事項を審議し、システム管理者のもとに情報システムを管理するものとする。
- (2) システム導入業者及びシステム保守管理業者と強調してマスタ管理を行う。

3) 情報システムダウン管理

- (1) 情報システムが機能しなくなった時でも診療に大きな混乱を来さないための方策を検討し、各部門の詳細な対応を定める。

4) ネットワーク管理

- (1) 外部および内部ネットワークを利用して各種情報を病院利用あるいは院内職員に提供する内容について検討し、編集する。
- (2) 外部ネットワークの院内利用者についてその利用者権限を管理し、特に臨床研究情報を個人の端末に保存する職員については、その端末のセキュリティ管理について指導する。

5) 情報システム教育

- (1) 情報システムの使用について効率的な使用ができるように、利用者あるいは利用者になるものに対して、診療情報等を保護する目的とその必要性を十分に理解させ、その対策を推進するために、教育研修を行うものとし、情報システム担当（以下「情報システム担当」という）がその実務を担当する。

6) システム企画協議

- (1) 情報システムの適正な管理・運用を図るため、中長期に係る情報システムの改善や随時発生する小規模なシステム改善等を計画的に実行できるよう全体調整を行う。

7) 監査の実施

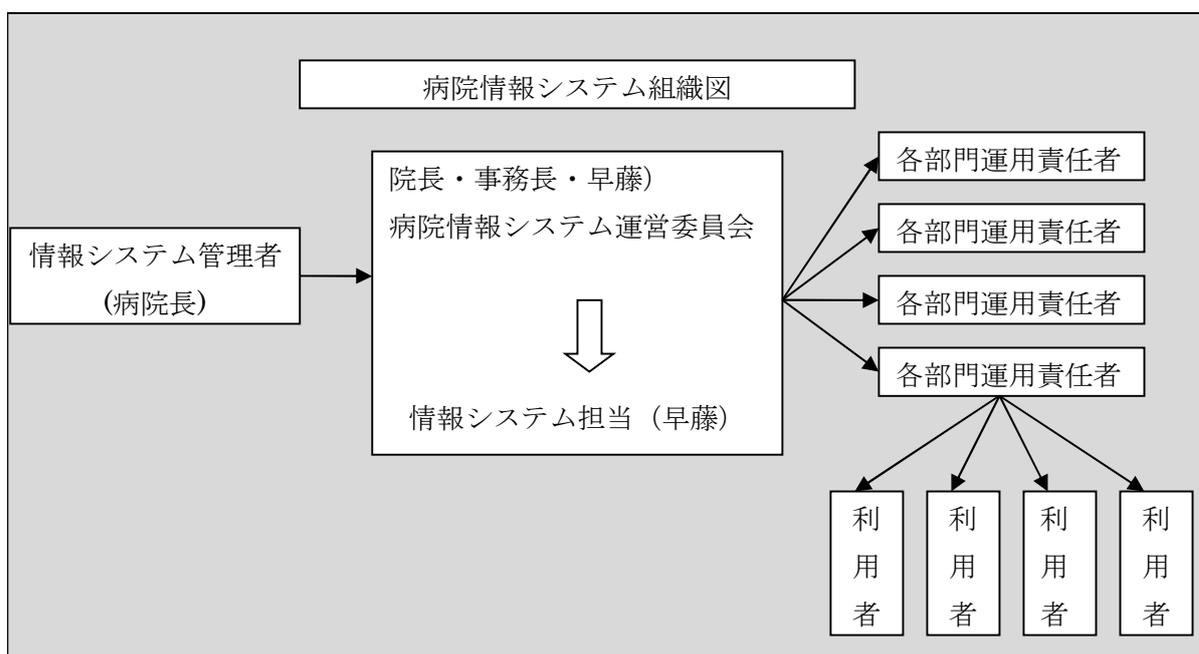
- (1) 情報システムの利用者の端末利用状況を管理するため、端末利用状況をログ情報等によって毎年4回定期的にチェックし、これを広報する。なお、問題点の指摘等がある場合には、直ちに必要な措置を講じなければならない。
- (2) 監査内容については、システム管理者がこれを定める。
- (3) システム管理者から要請があった場合、定期監査以外に臨時の監査を行うものとする。

8) 情報システム担当

- (1) 情報システム委員会の実務については、情報システム委員会の責任の下に情報システム担当が行う。

【ログ】

ログとは、電子カルテシステムを中心とした情報システムの処理内容や利用状況を、時間の流れに沿って記録したもの、あるいは記録すること。



第3章 情報システムに関する理念

1 理念

- 1) 情報システムの管理者及び利用者は、保存義務のある情報の電子媒体による保存が、自己責任の原則に基づいて行われることをよく理解しておかなければならない。
- 2) 電子保存された保存義務のある情報の真正性、見読性、保存性を確保し、かつ、情報が患者の診療や病院の管理運営上必要とされるときに信頼性のある情報を迅速に提供できるよう、協力して環境を整え、適正な運営に努めなければならない。
- 3) 情報システムの管理者及び利用者は、診療情報の二次的利用(診療や病院管理を目的としない利用)についても、患者のプライバシーが侵害されることのないように注意しなければならない。

【自己責任の原則】

自己責任とは、当病院が運用する情報システムについて、どういう方法によって電子保存のための条件を満たしているか第三者にわかるように示す『説明責任』、運用方法が決められたとおり、実行できるように運用管理を行う『管理責任』、決められた運用方法が後になって、電子保存のための条件を満たしていなかった、又は適切に運用できていなかったことによる第三者に対して損失を与えた場合の責任を当病院が負う『結果責任』を果たすことを意味する。

【真正性・見読性・保存性の原則】

『真正性』とは、正当な人が記録し確認された情報に関し、第三者から見て作成の責任と所在が明確であり、かつ、故意又は過失による、虚偽入力、書き換え、消去、及び混同が防止されていることである。“混同”とは、患者を取り違えた記録がなされたり、記録された情報間での関連性の記録内容を誤ったりすることをいう。

『見読性』とは、電子媒体に保存された内容を必要に応じて肉眼で見読可能な状態に容易にできることである。なお、“必要に応じて”とは「診療、患者への説明、監査、訴訟等に際して、その目的に応じて」という意味であり、“容易に”とは、「目的にあった速度、操作で見読を可能にすること」を意味する。

『保存性』とは記録された情報が、法令等で定められた期間にわたって、真正性を保ち、見読可能にできる状態で保存されることをいう。

第4章 電子保存する情報の範囲

1 保存範囲

- 1) 当病院において、保存義務のある情報を電子保存する際に対象とする情報の範囲については、「第2章 管理組織 2 情報システム委員会」に規定する情報システム委員会の審議を経て、システム管理者がこれを定めるものとする。

2 保存情報の保護

- 1) 情報システムの運用並びにそれに関する責任を定めることにより、診療情報等の不適切な取扱いに起因する患者の権利・利益の侵害の防止および基本的人権の保護と同時に、利用者の情報の共同利用に関する保護を図る。
- 2) 当病院の情報システムのデータは、別に定める「第7章 情報システムのセキュリティ方針（以下「セキュリティ方針」という）」、「第8章 管理者マニュアル（以下「管理者マニュアル」という）」及び「第9章 利用者マニュアル（以下「利用者マニュアル」という）」により保護されるものとし、ここに規定する情報システムのデータの保護の規程等の内容は、以下のとおりとする。
 - ① 「セキュリティ方針」
 - ・ 情報の管理や保護のための技術的な対策
 - ・ システムの利用者や管理者への教育の実施等を定めた「セキュリティガイドライン」として規定
 - ② 「管理者マニュアル」
 - ・ 情報システムの管理者が注意すべき事項を規定
 - ③ 「利用者マニュアル」
 - ・ 情報システムの利用者が注意すべき事項を規定
- 3) 電子カルテを中心とした情報システムの診療情報を含むデータおよび秘密情報は、機密性、一貫性、可用性の欠如に起因する危害から保護されなければならない。

【機密性】

利用者に対して、その利用者が権限行使できる責任範囲に限り、その権限の条件に従ってデータ及び情報が書き換えられ、あるいは見読できること。

【一貫性】

データ及び情報が正確で完全であり、かつその真正性、保存性が維持されること。

【可用性】

データ、情報、計算システムが、適時に必要な様式に従い、アクセスでき、利用できること。

4) 電子媒体による保存を認める文書等(法律の適用)

- ① 医師法(昭和 23 年法律第 201 号)第 24 条に規定されている診療録
- ② 医療法(昭和 23 年法律第 205 号)第 21 条、第 22 条及び第 22 条の 2 に規定されている診療に関する諸記録及び同法第 22 条及び第 22 条の 2 に規定されている病院の管理及び運営に関する諸記録
- ③ 薬剤師法(昭和 35 年法律第 146 号)第 28 条に規定されている調剤録
- ④ 救急救命士法(平成 3 年法律第 36 号)第 46 条に規定されている救急救命処置録
- ⑤ 保健医療機関及び保健医療養担当規則(昭和 32 年厚生省令第 15 号)第 9 条に規定されている診療録等
- ⑥ 保健薬局及び保険薬剤師療養担当規則(昭和 32 年厚生省令第 16 号)第 6 条に規定されている調剤録
- ⑦ 診療放射線技師法(昭和 26 年法律第 226 号)第 8 条に規定されている照射録

5) 利用者は情報システムへの信頼を高めるために、診療情報等の保護対策、手続き、規定等の存在及びその範囲について適切な知識を得ることができ、管理者はこれらについて周知を図る。

6) 情報システムの保護対策は、他の者の権利および利益を尊重して提供され、利用されるべきである。

7) 診療情報等の保護のための対策、手続き、規則には、技術、管理、組織、運営、教育、法律を含めた範囲での関連する考え方を考慮に入れて院内の対策、手続き、規則の調和を図るべきである。

8) 情報システムの保護施策の要求は、運用形態、利用形態及び技術と共に変化するため、診療情報等の保護のための対策、手続き、規則は定期的に再評価する。

第5章 利用者

1 情報システム利用者

1) 利用者の責務

- (1) 利用者自身の認証番号やパスワードを管理し、これを他者に利用させないこと。
- (2) 情報システムの情報の参照や入力（以下「アクセス」という）に際して、認証番号やパスワード等によって、システムに利用者自身を認証させること。
- (3) 情報システムの情報入力に際して、確定操作(入力情報が正しいことを確認する操作)を行って、入力情報に対する責任を明示すること。
- (4) 与えられたアクセス権限を越えた操作を行わないこと。
- (5) 参照した情報を、目的外に利用しないこと。
- (6) 患者のプライバシーを侵害しないこと。
- (7) システムの異常を発見した場合、速やかに情報システム担当に連絡し、その指示に従うこと。
- (8) 不正アクセスを発見した場合、速やかに情報システム担当に連絡し、その指示に従うこと。

2 利用者管理

1) 利用者管理の目的

利用者権限は、情報システムを利用する上で、利用資格の識別およびプログラムやデータファイル等への不正アクセスを制御し、データの変更等において利用者の真正性を高めることを目的とし、利用者情報区分によりアクセス権を設定するものである。

2) 利用者権限の管理

新規	・当病院で採用(病院に着任)した時点
変更	・院内の部署が変わった時点 ・氏名が変更になった時点 ・業務が変更され、権限の内容が変更された時点
非表示(中止)	・退職又は移動などで情報システムに関係の無くなった時
利用者権限変更	・基本的に、医師、看護師、検査技師等の設定がされているが、業務上、必要な区分が変更になる時

※ 後利用等でデータを作成する際、利用者の関連付けができなくなる為に、登録された利用者 ID は削除しない。

3) 利用者権限の分類・権限範囲区分

利用者権限は、利用者の職種による分類・権限範囲区分を原則とし、情報システム委員会において別途定める。

4) 申請・登録・交付・非表示

(1) 利用者権限の交付は、運用管理者が情報システム委員会に利用者の申請を提出し、承認を得る必要がある。また、利用者の異動に伴って運用管理者から非表示申請が出た場合は、事後報告として情報システム委員会に非表示の依頼を出すものとする。ただし、当病院職員に対する利用者権限の交付等については、その者の人事異動に伴い、システム管理者の責任において設定を行うため申請を必要としない。

(2) 利用者の登録設定・非表示手続きは、運用管理者が『利用者登録管理表』に次の項目を記入し、情報システム委員会へ提出する。

①依頼者名

②利用者所属、職種、氏名、性別

③適用開始日

④権限付与に関する理由等

(3) 情報システム委員会は、申請に基づき利用者 ID、利用者区分を記入する。ただし、非表示申請は、運用管理者の異動連絡で情報システム担当に依頼し、事後報告とする。

(4) 情報システム委員会で承認されれば、申請に基づき交付を行う。

(5) 運用管理者は、人事異動・退職その他の事由により、当該システムの使用に関係なくなった時、速やかに情報システム担当に連絡し、非表示処理をする。

情報システム担当は、申請の通り登録を行い、利用者登録管理表を保管する。

5) 利用者 ID のパスワードの登録あるいは運用管理については、パスワード管理をする者にあっては「管理者マニュアル」、システムを利用するものにあっては、「利用者マニュアル」に詳述する。

6) 利用者ログの監査

(1) 不正アクセスの防止

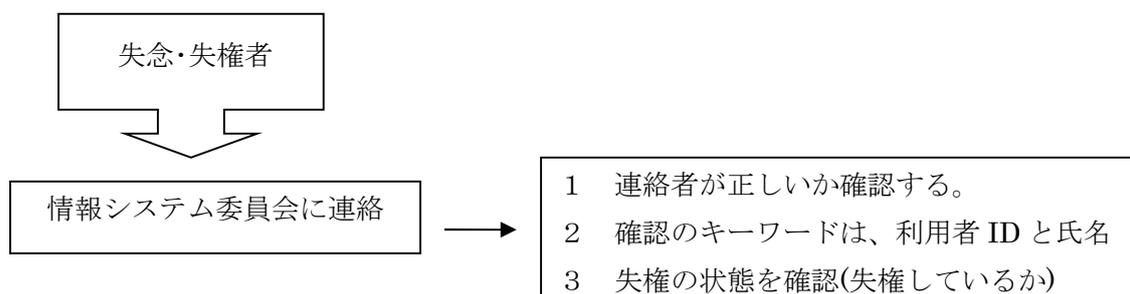
情報システム担当は、不正アクセスを防止する為、以下の点を監視する。

・アクセス権の無い者によるデータアクセス

・パスワードの失権状況

(2) 点検の結果、異常がある場合は、その対象の ID・パスワードを使用不可とし、不正使用の防止に努める。

7) 失念・失権者の復旧手順



3 情報システムの機能要件

- (1) システム内の情報にアクセスしようとする者の識別と認証
- (2) 情報の機密度に応じた利用者のアクセス権限の設定と不正なアクセスを排除する機能
- (3) 利用者入力した情報について確定操作を行うことができる機能
- (4) 利用者が確定操作を行った情報を正確に保存する機能
- (5) 利用者が確定操作を行った情報の記録及びその更新に際し、その日時並びに実施者をこれらの情報に関連付けて記録する機能
- (6) 管理上又は診療上の必要がある場合、記録されている情報を速やかに出力する機能
- (7) 複数の機器や媒体に記録されている情報の所在を一元的に管理できる機能
- (8) 情報の利用範囲、更新履歴、機密度等に応じた管理区分を設定できる機能
- (9) 利用者が情報にアクセスした記録を保存し、これを追加調査できる機能
- (10) 記録された情報のバックアップを作成する機能

第6章 情報システム安全管理基準

1 機器の管理

- 1) 電子保存された情報システムの記録媒体を含む主要機器は独立した施設管理が可能なコンピュータ室に設置する。ただし、コンピュータ室への設置が困難な理由が明白な場合に限り、当病院職員が24時間常駐することを条件として、他の部屋への設置を可能とする。
- 2) コンピュータ室の出入り口は常時施錠し、ICカード等による入退出管理機能を備える。なお、システム機器の搬入出等により、一定時間入退出を繰り返す場合には、当病院職員が必ず作業に立ち会うものとする。
- 3) 万が一の災害等発生を考慮して、コンピュータ室には無水消火装置、漏電防止装置、無停電電源装置等を備える。
- 4) 設置するシステム機器は定期的に点検を行う。

2 記録媒体の管理

- 1) 品質の劣化が予想される記録媒体は、あらかじめ別の媒体に複写し、媒体品質の劣化に伴う記録喪失等の発生を防ぐ。
- 2) 記録媒体は、利用者権限で施錠管理された場所において厳重保管し、機密保護に努める。
- 3) 破棄データの取扱い
 - (1) 記録媒体は、読取り不能の状態にした後に破棄する。
 - (2) 業務運用上発生する廃棄帳票は、シュレッダーにかけ廃棄する。

3 ソフトウェアの管理

- 1) 情報システム担当は、情報システムで使用されるソフトウェア、及びソフトウェアサービスを使用の前に審査を行い、情報の安全性に支障が無いことを確認する。
- 2) 情報システム担当は、ネットワークや可変型媒体によって情報を受け取る機器につい

て、必要に応じてこれを限定する。

- 3) 情報システム担当は、定期的にソフトウェアのウイルスチェックを行い、感染の防止に努める。

4 データ管理

- 1) システムバックアップ／復元手順

機器障害や災害などに備えて、システムのバックアップの取得を義務付ける。併せてバックアップからの復旧手順書を作成する。

- (1) バックアップの種類

- ①データベース
- ②システム本体(OS、アプリケーションプログラム、各種設定情報)
- ③ジャーナル、ログ等

- (2) バックアップ対象は、運用に係るすべてのサーバとする。

- (3) バックアップのタイミング

- ①新規のアプリケーションが発生した場合
- ②業務のアプリケーションに変更があった場合
- ③オンライン終了時、又はコンピュータ利用が低い時間帯

- 2) システムバックアップ媒体の管理手順

- (1) バックアップする媒体には、ボリューム(論理的な格納領域)管理を行う。
- (2) 媒体の保存管理は、2節で示すデータ管理手順に順ずる。

- 3) システムデータの容量チェック手順

- (1) システムデータの管理対象

情報システムデータを保存する媒体(格納領域)は、容量不足に陥るとシステムダウンと同等の重大な影響を及ぼしかねない障害に結びつくため、情報システム委員会は、次の項目について日常の利用頻度の確認をしなければならない。

- ①データベース格納率の管理
- ②格納先ディスク使用率の管理

5 ドキュメント管理

- 1) 取扱い対象

取扱いドキュメントとは、システムプログラム・ユーザズプログラム・電子カルテ

を中心とした情報システムの医療情報を含むデータ及び機密情報が記述されている全てのドキュメントである。なお、申請手続きの無いドキュメントは管理対象外とする。

2) ドキュメントの保管・管理

(1) 媒体の場合

磁気媒体に記録されたプログラムドキュメントは、施錠可能な場所に格納し保管する。

※ 磁気媒体は、毎年定期的に利用確認を行い、媒体劣化等の恐れがある場合には、必要に応じて複写を行う。なお、媒体の管理については、2節で述べた管理手順に従う。

(2) 帳票の場合

紙に記述されたドキュメントは、施錠可能な場所にファイリングして保管する。

※ ドキュメント類を格納する保管ロッカーは、常時鍵を閉めて管理する。

6 ネットワーク管理

- 1) 情報システム委員会は定期的にシステムの利用履歴やネットワーク負荷等进行检查し、通信環境の効率的な運用を維持するとともに、不正に利用された形跡がないか確認する。
- 2) 運用責任者はネットワークの不正な利用を発見した場合には、直ちに情報システム担当に報告するとともに、情報システム担当と連携してその原因を追求し、再発防止対策を実施する。

7 事故対策

- 1) システム管理者は、緊急時及び災害時の連絡、復旧体制並びに回復手順を定め、非常時においても参照できるような媒体に保存し管理する。
- 2) 情報システムのいずれかに障害が発生した場合は、「情報システムダウン対策マニュアル」により対応する。

第7章 情報システムのセキュリティ方針書

1 方針

当病院において運用する情報システムが取扱う情報は不当に暴露されたり、不当に内容が改ざんされたり、不当に処理が妨害されたりしないように管理および保護されなければならない。

情報システムで処理、保管されているデータに関するいかなる情報も、このシステムに関係のない者には公表しないことを原則とする。

2 目的

本章「第7章 情報システムのセキュリティ方針（以下「セキュリティ方針」という）」は、上記1の方針に基づき、情報の管理や保護のための技術的な対策及びシステムの利用者や管理者への教育の実施等を定めた「セキュリティガイドライン」を定めることを目的とする。

3 修正

情報システム委員会は、「セキュリティ方針」に定められた事項について修正の必要が生じた場合には、速やかに見直しを行うものとする。

4 適用範囲

本セキュリティ方針は、情報システムを構成する全ての部分（コンピュータシステムに関連する装置、システムの運用に携わる人、システムの利用者等を言う。以下同じ）に適用する。

特に、プライバシー情報（診療情報等を含む）を扱う全ての部分に対しては、運用時の必須要件として本セキュリティ方針を適用する。

5 配布

本セキュリティ方針は、情報システムに関係する全ての者が閲覧可能な場所に保管する。

6 情報システム委員会

- 1) セキュリティ方針を実施するため、その実施方法について、その評価や問題点などを検討し、情報セキュリティの保護、管理を行うとともに、病院内で実施される情報セキュリティ対策に矛盾が生じないよう調整を行う。
- 2) 業務内容

- (1) 病院のデータ保護に関する「セキュリティ方針書」の適切な運用とそれに関する責任についての検討
- (2) 病院の情報財産に対する脅威についての監視と予防対策の検討
- (3) セキュリティ対策を実践するための病院長への提言

3) 業務の実務については、情報システム委員会の責任の下に情報システム担当が行う。

7 リスク管理

セキュリティ管理は、セキュリティ対策と保護対象となる情報の価値とのバランスを維持するために、下記の点に留意して方針が決定される。

- (1) 情報システムのセキュリティ上の想定脅威(発生が懸念される不正暴露、改ざん、処理妨害等)
- (2) 想定脅威に対して、その発生が及ぼす損失とそのセキュリティ対策費用及び利便性を考慮した有効な対策とその速やかな実施

8 プライバシー情報

医療機関に関しては、「個人情報保護に関する法律についてのガイドライン（通則編、国にある第三者への提供編、第三者提供時の確認・記録義務編及び匿名加工情報編）」とその通則編を基礎とした、医療・介護関係事業者に対する「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」が適用されます。

他人の財産を管理し、しかも、一度暴露等の事故が発生する、取り戻すことができないという情報固有の特性（機微性）を鑑み、委託先民間企業も含めた情報システムに関与するすべての利用者は、その保護に最優先で取り組まなければならないものとする。

9 セキュリティ管理

病院長は、情報システムのセキュリティ確保のために各部門から運用責任者を指名し、情報システム委員会に報告する。

10 責任の分散

セキュリティ管理の責任を分散し、特定の個人に権限と責任が集中して、矛盾を引き起こさないように配慮する。

11 違反者に対する処置

本セキュリティ方針を含む組織、機関の定めた情報セキュリティに違反した者には、罰則を科する。

1.2 診療にかかわる情報のアクセス

診療にかかわる情報にアクセスできる者は、医師及び関連する医療スタッフ施設運営に関わる委託業者とし、患者による直接アクセスは行えないこととする。ただし、医師の判断により診療に必要であると認められた情報を当該患者に開示する場合は、担当医師の責任において行うこととする。

また、患者の要請に基づく全カルテの開示を行う場合は、別に定める「カルテ開示規定」によるものとする。

なお、診療の準備、症例研究、カンファレンス等の目的で診療にかかわる情報にアクセスする場合も同様に、医師の責任において行うこととする。

1.3 電子カルテへのアクセス

- 1) 通常時の電子カルテへのアクセスは、外来・入院を問わず、受診を希望する旨の根拠となる情報が患者又は患者の代理人の意思により表明され、かつ、患者の登録手続きが済まされていなければ行うことができない。受診者が本人であることが判明しない場合には、患者の診療券の磁気テープ部分もしくはバーコード部分を電子カルテ端末に認識させることにより、確認しなければならない。
- 2) 緊急時の電子カルテへのアクセス
 - (1) 患者氏名が不詳の場合は、新たに診察券(患者 ID)を作成する。
 - (2) この診察券は、新規の ID で作成されるため、患者の重複登録にならないよう作成にあたっては、万全の配慮をしなければならない。
 - (3) 患者名が確認できた場合で、従来 ID が存在していたときは、その ID と新規 ID の融合方法を関係部門と調整するための方法を勘案しなければならない。

1.4 物理的なセキュリティ管理

自然災害や装置の故障、盗難、破壊等から情報システムを保護するために以下の対策を実施する。

- (1) コンピュータ装置本体、ネットワーク管理装置等、電子カルテシステムの処理に重大な影響を与える装置は盗難や破壊、関係者外の利用から保護するための物理的な対策を実施する。
- (2) 全装置の一覧表を維持管理し、不正な持ち出し等が発生しないようにする。
- (3) システム診断用のハードウェア、及びソフトウェアの使用は利用目的を限定し、その使用を管理する。
- (4) ネットワーク回線は全ての部分で物理的に保護されることとし、定期的に検査する。
- (5) 電源設備の故障による停電等の場合でも、無停電電源供給装置 (UPS) 等の別系統電源供給によって電力の供給を可能とする。
- (6) 重大な故障又は災害時の業務継続計画(「情報システムダウン対策マニュアル」)は、

別途定める。

1.5 情報セキュリティ管理

1) 利用者の識別と認証

- (1) 個々の情報に対し、権限を持っている利用者に対して、その権限の範囲内でのみ利用させるようにするため、利用者一覧を作成し、運用責任者にて管理する。
- (2) 利用者は、利用者 ID によって識別し、本人の確認は、パスワードによって行う。

2) ファイル管理

- (1) ファイル（データベースを含む）やプログラムを管理しているシステム（以下「管理システム」という）あるいは業務上特別な条件下で必要なツールさらに、後利用データベースにおいて患者のプライバシーに影響を与えるデータなどは、特別に権限を付与された利用者のみ利用できる。
- (2) システム運用関連、及びファイル（データベース含む）管理関連のプログラムやデータの変更は、特別な権限を付与された者のみが事前に関係者に情報共有を行った後に、行うことができる。
- (3) 管理システムは、運用中は常時、管理者が管理できる状態にしておく。

3) ネットワークセキュリティ管理

- (1) ネットワークの利用及びネットワークの構成の登録・変更には、事前の手続きを規定し、その規定に基づき実施するようにする。
- (2) 内部ネットワーク（業務で使用するサーバ、無線 LAN 及び端末が接続された病院情報システム専用ネットワーク）から部門システム等を介して外部と通信する場合（リモートメンテナンスに限る）には、院外のリモートメンテナンス端末の管理方法も把握して許可を与えなければならない。
- (3) 院内に敷設された外部ネットワークは、内部ネットワークを接続しないものとする。
- (4) 特に許可された者以外は、院外回線を通じて内部ネットワークを利用できない。
- (5) 各部門システムを通じて直接院外の回線を結びつけてダイアルアップネットワークを構築する場合は、必ずその機能に関する仕様書を情報システム担当に提出して承認を受けるとともに、定期的にその安全性の維持を確認できる場を設ける。
- (6) プライバシーに関係するような重要なデータをネットワーク上で使用する場合は、ネットワーク環境がセキュリティの確保上完全ではないことを考慮した上で使用しなければならない。

4) 分散管理

- (1) システムを構成する部門サーバ間のセキュリティレベルを統一する。
- (2) 部門サーバ間で一貫したセキュリティ属性の解釈が行えるように管理する。

5) 電子メール管理

- (1) プライバシーに関係するような重要なデータを、電子メールで送信する場合は、データを暗号化する等、その送信方法について考慮されなければならない。

6) 監査

- (1) 情報セキュリティの管理のため監査情報を収集し、それらを監査し、その結果をシステム管理者に報告する。
- (2) 管理責任者は、常に第三者的立場を堅持して公正にシステムの不正あるいは改ざんあるいは混同の存在について指摘しなければならない。
- (3) 監査情報には、利用者(利用者 ID)、利用場所、日時、アクセスした資源名、利用事象のタイプ、アクセスの可否結果を記録しておく。
- (4) 監査情報が収められているファイルは、保護されなければならない。
- (5) 監査責任者は、監査情報を少なくとも月 1 回、チェックする。
- (6) 違反に関する監査記録は、少なくとも 60 日間は保存しておく。
- (7) 監査ツールの使用は、監査者のみに限る。

7) データ保存とコンピュータウイルス

- (1) 利用者が持ち込むデータや、システム運用に直接関連するプログラム等重要なプログラムを扱う場合には、利用前にウイルスチェックを実施する。
- (2) ウィルス対策プログラムサーバでの一括管理とし、ウィルス対策ソフトウェアメーカーから新しいプログラムが提供された場合には、各端末に配信するものとする。
- (3) 利用者は、使用中にウイルス感染の疑いが生じた場合は、情報システム担当に連絡するとともに、その指示に従って端末隔離等の処理を行わなければならない。
- (4) 情報システム担当は、障害の状況を分析しウイルスが確認された場合は、その旨を全利用者へ通知して注意を喚起し、同時に情報システム委員会に報告しなければならない。
- (5) メディアの管理は、業務の責任者が負うものとする。

8) 法的に使用される情報の管理

- (1) 法的に使用される電子カルテ情報は、その真正性を確保するように講じられていること。

- (2) 法的に使用される電子カルテ情報の真正性は、操作を行う者の利用者 ID とパスワードで認識させて、操作を行う者が入力した確定情報は、確定入力を動機付けできる画面で構成し、その修正は原本を保存しながら修正データが見読できるように講じられていること。
- (3) 法的に使用される電子カルテ情報は、法的に求められる期間中保存でき、機器等の新調によるデータの互換性は保持できるように講じられていること。
- (4) 法的に使用される電子カルテ情報を、保存及び出力するシステムは、法的に求められる期間内は常に稼動しているように講じられていること
- (5) 法的に使用される電子カルテ情報の所在を明確にし、法的保存期間の情報の開示を求められた場合、速やかに開示できるように講じられていること。
- (6) 紙面での保存が法的に必要な情報は、その法的根拠が保たれる状態で保存するように講じられていること。

1 6 運用管理

1) 運用管理

- (1) システムは、以下の条件に従って適切に管理されなければならない。
 - ① システムが災害にあった場合の対処方法と復旧方法について手順を明確にし、必要に応じて情報システム担当で見直しを実施すること。
 - ② システムのバックアップを定期的の実施するとともに、バックアップ媒体は、安全な場所に保管されること。
 - ③ 機密性の高いバックアップデータは、厳重に保管されること。
 - ④ 可搬媒体(テープ、ディスク、カセット、及びプリントしたレポート等)に関する管理手順を明確にし、利用者に遵守させること。
 - ⑤ システムデータの容量を定期的を確認し、容量不足が予想される場合には速やかに対処すること。

2) システム管理

- (1) 利用者の本人確認は、システムの利用を開始する時点で実施する。
 - (2) 不正なシステム利用は、許可しない。
- 3) システムの運用を適切に管理するために、「管理者マニュアル」及び「利用者マニュアル」を定めるものとする。
 - 4) 各部門別において、利用者マニュアルに基づき使用する事を定める。

1.7 スタッフセキュリティ

1) 外部委託管理

- (1) 情報システムを利用することのできる職員を雇用する委託業者は、当病院で作業する職員に対して十分な利用者教育を行わなければならない。
- (2) 情報システムの利用者は、守秘義務と同時に、情報システムの構造を熟知して、院外からのアクセスに注意を払わなければならない。
- (3) 部門システムに対して院外からのアクセス手段を有する委託業者は、その構造(仕組み)について事前に情報システム担当の許可を得なければならない。
- (4) 部門システムは、部門内でログ管理をし、定められた内容で情報システム担当に報告、もしくは情報システム担当が必要に応じてログを確認できるようにしなければならない。
- (5) 委託契約の締結に際しては、契約上に職員の情報セキュリティに関する項目を盛り込まなければならない。

2) 教育・訓練

- (1) 情報システムの利用者は、情報システムの利用を許可される前にセキュリティ方針及びセキュリティ対策、運用の教育を受けなければならない。
- (2) セキュリティに理解の乏しい利用者は、セキュリティ方針及びセキュリティ対策の研修を受けなければならない。
- (3) 教育内容には、以下の項目が盛り込まなければならない。

①情報システムの利用者に対する教育

- ア. セキュリティ侵害や情報の漏洩が何によって起きるかを含めた、プライバシー、機密性、完全性、可用性、情報公開及び情報セキュリティの概念
- イ. 利用者のセキュリティ管理における個人の責任及び立場による責任範囲の違い
- ウ. 診療情報の重要性と、その利用者および使用用途
- エ. 利用者情報の重要性
- オ. 情報セキュリティに対する想定脅威の種類
- カ. データの保護の方式
- キ. セキュリティ違反の重大さと罰則
- ク. セキュリティに対する定期的な評価と改良

②管理者に対する教育

- 初めて管理者になった者に対する教育は、利用者に対する教育に加えて以下の項目を履修しなければならない。
- ア. 情報セキュリティ教育のプログラムを確立するための管理責任
 - イ. 「セキュリティ方針書」とその実践を実現、監視、評価するための戦略

- ウ. 全ての利用者に対する情報の取扱い方法・内容
 - エ. 情報セキュリティに影響を与える新技術や、セキュリティ計画に影響を与える規制・規則について熟知する責任
 - オ. 不適切な情報の漏洩によって発生する法律上の要件や罰則
 - カ. セキュリティ侵害時の一貫した対応と訓練
- (4) 情報システムを利用するすべてのスタッフは、教育・訓練を受けなければならない。

第8章 管理者マニュアル

1 はじめに

- 1) 本章は、情報システムを安全に管理、運用するため、システム管理者が定めた病院情報システム運用管理規程（以下「運用管理規程」という）、及び「第7章 情報システムのセキュリティ方針（以下「セキュリティ方針」という）」を基に、当病院の情報システムの管理者が注意すべき事項を定めたものである。
- 2) 情報システムの管理者は、本章ならびに「運用管理規程」及び「セキュリティ方針」を遵守して、診療情報等の漏洩、改ざん、破壊などが発生しないように、安全に情報システムを管理運用しなければならない。

2 管理者及び情報システム委員会

- 1) 本章で規定する管理者及びその職務内容は、以下のとおりとする。
 - (1) 情報システム委員会
 - ① 情報システムに関するすべてを統括する。
 - ② 情報システムを利用する可能性のあるすべての職員を把握し、必要に応じて利用者の異動・職種・勤務形態等の登録情報を運用責任者に通知する。
 - (2) 運用責任者: 各部門の登録申請あるいは異動情報を受けて情報システムへのアクセス権限の登録及び変更許可を情報システム委員会に報告する。
 - (3) 情報システム担当: 情報システム委員会の責任の下に、ハードウェア及びソフトウェアの資源管理、特にハッキング等によるシステム障害の防止のための情報収集と各種メディアの感染防止に関する調査、検証を行う。
- 2) 各担当者は、権限分散のため兼務しないことを原則とする。
- 3) 各構成委員が一利用者として情報システムを利用する場合には、「セキュリティ方針」及び「利用者マニュアル」を遵守し、診療情報の漏洩、改ざん、破壊などが発生しないよう、安全に情報システムを利用し、また他の職員にも啓蒙しなければならない。

3 義務と罰則

各構成委員は、本ガイドラインに則って情報システムを管理、運用しなければならない。また、情報システム上の情報について守秘義務を負わなければならない。違反した場合には、罰則を科されるものとする。

4 利用者への指導及び管理

各構成委員は、情報システムの利用者に対して、「セキュリティ方針」及び「利用者マニュアル」を遵守するよう指導、管理し、その徹底を図らなければならない。

5 システムの利用

- 1) 情報システム委員会は、内部ネットワーク及び外部ネットワークを利用する可能性のあるすべての職員を把握し、利用者の異動、退職時には、システム管理者に速やかに利用者権限の設定、変更の依頼を行う。
- 2) システム管理者は、利用者権限の基盤となるものを作成し、情報システム委員会に提出し、規定に基づき情報システムに利用者権限を設定する。

6 ネットワークの利用及び構成の管理

1) 利用者の管理

- (1) 内部ネットワーク及び外部ネットワークの利用者の申請・登録・変更については、事前に手続きを規定し、その手続きに則って実施するようにする。
- (2) 外部インターネットからの転送情報は、特別な理由がない限り内部ネットワークのサーバに保存しない。
- (3) 内部ネットワークから外部インターネットに対してアクセスすることはできない。
- (4) 定期的に利用者の利用レベルの妥当性のチェックを行う。
- (5) 利用者は、運用責任者を通じて情報システム委員会へ報告され、利用者権限が付与された後、登録されるものとする。ただし、失念による処理についてはこの限りでない。

2) ネットワーク構成の管理

- (1) ネットワーク構成の登録・変更については、事前に手続きを規定し、その手続きに則って実施するようにする。
- (2) 情報システム委員会は定期的にシステム運用状況をチェックし、必要と判断した場合には、「情報システムダウン対策マニュアル」の構成部分の追加・変更・破棄を関係者と協議する。

7 院外接続管理

1) 共通事項

- (1) 内部ネットワークへの院外からインターネットを通じた直接アクセスを禁止する。
- (2) 内部ネットワークに対して、院外からインターネットを通じてアクセスできる経路を設けることを禁止する。
- (3) 部門システム等のリモートメンテナンスを含め、院外と接続する場合には、事前に情報システム担当と協議し、その構造について許可を得るとともに、管理者の適切な指示のもとに設置しなければならない。

8 利用環境面におけるセキュリティについての管理者の業務

1) 入退室管理

- (1) 休日・夜間には通常使用されない設置場所の端末については、休日・夜間における情報システム利用情報をいつでも確認出来る様にする。
- (2) ログは6ヶ月保存する。

2) 名札の着用管理

名札の有無により、権限のない者が情報システムを利用していないかどうか確認する。

3) ノートブック型端末の管理

- (1) ノートブック型端末の設置してある部署の業務の管理者は、常に配置台数と使用状況について管理する。
- (2) ノートブック型端末は、原則として業務の管理者の管理区域を越えて使用することができない。

9 運用管理面におけるセキュリティについてのシステムデータ管理

1) 設備についての管理

- (1) 重要なデータが、どの装置に格納されているのか明確に定める。
- (2) インフォメーションあるいは情報開示用端末以外は、人の通行の多い場所に設置しない。
- (3) 定期的にチェックし、機器を厳重に管理する。

2) 可搬記憶媒体の管理

- (1) 可搬記録媒体（専用ドライブやカードリーダー等の装置を含む）は、情報システム担当者が予め許可したもの以外の使用を禁止する。

- (2) 可搬記録媒体の使用にあたって、利用者にウィルス感染を防止するなどの自己管理について十分に指導する。
 - (3) 情報システムで利用するCD及びUSBメモリ等のデータの格納媒体で患者のプライバシー及び病院運営上重要なものは、施錠したキャビネット又は施錠した部屋（保管庫も含む）で管理しなければならない。
- 3) ノートブック型端末の管理
ノートブック型端末は運搬が容易なため、可搬記録媒体と同様に管理を行う。
- 4) ドキュメント管理
- (1) 患者のプライバシー及び、病院運営に危害が及ぶ情報が記述されている重要なドキュメントは、暗号化する等の処置を考慮する。
 - (2) 重要なドキュメントや帳票のコピーや持ち出しについて管理を行わなければならない。

10 情報システムの利用時のセキュリティ

- 1) システム管理者
- (1) 端末の利用状況
 - ①情報システムの利用者の端末利用状況を管理しなければならない。
 - ②端末利用状況をチェックし、情報システム委員会に報告しなければならない。
 - (2) アクセスログの管理あるいは利用者からの報告を受けてセキュリティの侵害、又はそのおそれがある場合には速やかに調査の上その状況をシステム管理者に報告しなければならない。
 - (3) 特別な権限の利用は、制限されなければならない。
- 2) 運用責任者の責任
- (1) 情報システムのサービスへのアクセスは、システム担当者が正式な利用者登録及び登録解除(非表示)手続きがなされるよう管理しなければならない。
 - (2) 利用者のパスワードは、暗号化されたパスワードによって安全に管理されなければならない。
 - (3) 利用者は、パスワード受理時もしくは直近の変更時から60日間の間にパスワードの変更をしなければならない。ガイドラインに則って、13ケタ以上の場合はその限りではない。
 - (4) システム管理者は、利用者の登録状況及び情報システムの利用状況を管理し、異動等で利用者外になった者は、速やかに、また、60日以上利用のない利用者の権

限を失権(非表示)させなければならない。また、1年以上利用のない場合「利用者マスタ登録」を抹消(非表示)しなければならない。

- (5) 漏洩した可能性がある旨の届出があった場合、速やかに当該利用者のパスワードを通常の再発行の手続きで再発行するとともに、当該利用者パスワードによる利用履歴のチェック等の調査を情報システム委員会に依頼しなければならない。
- (6) 運用責任者は、利用者の再発行履歴を情報システム委員会から報告を受けなければならない。
- (7) 情報システムのサービスとデータへのアクセス範囲は、業務要件に基づいて管理されるとともに、その利用者の権限付与は業務の管理者が申請し、情報システム委員会が決定し、その管理は、運用責任者が行う。

3) 利用者 ID とパスワード管理

- (1) 通常システムにログインする際には、パスワードを利用する。
- (2) 自分のパスワードは、決して他人又は他のグループに口外しない。
- (3) パスワードを紙などに記述して記録しない。
- (4) パスワードをファンクションキーなどに登録しない。
- (5) 自分の利用者 ID とパスワードを他の者に教えることにより、システムの利用権限を他人に貸与しない。
- (6) パスワードは、アルファベット(小文字・大文字)と数字のそれぞれを最低 1 文字以上用い、最低 8 文字以上で構成しなければならない。

- (7) パスワードには、以下のような推測可能な用語を設定してはならない。(パスワードの禁則)
 - ①年月日、曜日、その他日付に関すること
 - ②姓名、名字、イニシャル、ニックネームなど
 - ③医療機関名、部署名、それらに関するもの
 - ④電話番号やそれに類似するもの
 - ⑤ユーザ識別子、ユーザネーム、グループ ID、他のシステムの識別子
- (8) 利用者のパスワードは、登録してから 60 日が経過する日まで新しいパスワードに変更する。
- (9) 再登録したパスワードで使用中的のものは、継続して使用することができない。
- (10) 利用者パスワードは、一方的に暗号化し認証情報を保護する。

1 1 法的に利用される電子カルテ情報を出力する装置の管理

- 1) 法的に利用される電子カルテ情報を出力するシステムは、常に情報が出力されるように管理する。
- 2) 少なくとも法的に要求される期間は、電子カルテ情報の出力が保証されるように維持、管理する。

1 2 コンピュータウイルス対策

情報システム委員会は、ウイルスに感染した旨の届けがあった場合、現状と感染ルートを調査し、速やかに、これへの対処及び予防策を検討、実施し、システム管理者に報告しなければならない。

1 3 事件又は異常事象の報告

- 1) 情報システム委員会は、情報システムの異常が報告された場合あるいは確認された場合は、速やかに異常事象への対応措置を取り、システム管理者に報告しなければならない。
- 2) 情報システム委員会は、事件又は異常事象の発生の状況・原因・対応措置に関する報告資料を作成し、システム管理者に報告しなければならない。

1 4 教育・訓練

- 1) 情報システム委員会は、新たに情報システムを利用することになった利用者に対し、使用方法についてカリキュラムを編成し、各部門と協調して操作方法の習熟に努めなければならない。
- 2) 情報システムの利用者に対し、毎年1回、セキュリティ研修を実施し、受講させなければならない。

第9章 利用者マニュアル

1 はじめに

本マニュアルは、情報システムを安全に管理、運用するため、システム管理者が定めた病院情報システム運用管理規程（以下「運用管理規程」という）、及び「第7章 情報システムのセキュリティ方針（以下「セキュリティ方針」という）」を基に、当病院の情報システムの利用者が注意すべき事項を定めたものである。

従って、情報システムの利用者は、本マニュアル並びに「運用管理規程」及び「セキュリティ方針」を遵守して、診療情報等の漏洩、改ざん、破壊などが発生しないように、安全に情報システムを利用しなければならない。

利用者権限は、情報システムを利用する上で、利用資格の識別及びプログラムやデータファイル等への不正アクセスを制御し、データの変更等において利用者の真正性を高めることを目的とし、利用者情報区分によりアクセス権を設定するものである。

2 情報システムの利用

情報システムは、利用者管理者が作成した職員登録の中から、業務の責任者が利用者登録申請を提出したものを情報システム委員会が承認し、情報システム担当もしくは利用者情報とアクセス権限を登録した者のみ利用できるものとする。

3 義務と罰則

情報システムの利用者は、本ガイドラインに従って情報システムを利用しなければならない。また、情報システム上の情報について守秘義務を負わなければならない。

違反した場合には、別途定めるところにより、罰則を科されるものとする。

4 情報システムの利用時のセキュリティ

1) 利用時の画面管理及び就業時間外の情報システムの利用内容報告

- (1) 端末利用中に席を外す場合には、他の者にそのまま自分の権限で端末を利用されないよう、必ずログオフする。ログオフせずに席を外した場合、その間に行われた不正行為については、ログオフせずに席を外した利用者の責任とする。
- (2) 利用者は、端末の利用を終了する場合には業務終了処理を行い、初期画面をログオフに移行しなければならない。

2) 名札の着用

- (1) 情報システムを利用できる端末が設置してある場所では、必ず名札を誰もが見える所に着用しなければならない。
- (2) 身近に非着用者がいた場合、ただちに運用責任者に連絡し指示を受ける。

5 情報システム運用管理画面でのセキュリティ

1) 設備の利用

利用者は、業務の管理者が許可した装置以外で情報システムを利用してはならない。

2) 可搬記憶媒体の管理

- (1) 可搬記憶媒体（専用ドライブやカードリーダー等の装置を含む）は、情報システム担当者が予め許可したもの以外の使用を禁止する。
- (2) 利用者は、業務上必要な理由(検査機器からのデータ取り込み、他院への診療情報提供など)を除き、可搬記憶媒体を使用して情報システムからデータ(臨床研究用画像など)を取得する必要がある場合には、予め業務の管理者の許可を受けなければならない。また、本記憶媒体を当病院外に持ち出してはならない。
- (3) 可搬記憶媒体により取得したデータを当病院における診療以外の目的(臨床研究等)で使用する場合には、データの中の個人情報特定部分は削除しなければならない。また、可搬記憶媒体の使用後は、データを消去して速やかに返却(CD 等メディアの場合には再利用できないよう裁断等処分)しなければならない。
- (4) 情報システムで利用する CD 及び USB メモリ等のデータの格納媒体で患者のプライバシー及び病院運営上重要なものは、施錠したキャビネット又は施錠した部屋（保管庫も含む）で管理しなければならない。

3) ノートブック型端末の管理

- (1) ノートブック型端末は運搬が容易なため、可搬記憶媒体と同様の取扱いによって管理を行う。
- (2) 利用者個人の専用端末は、内部ネットワークでは使用できない。

6 ドキュメント管理

- (1) 重要度の高いドキュメントや帳票のコピーや持ち出しは、業務の管理者の許可を得なければならない。
- (2) 診療記録のハードコピーなど重要度の高いドキュメントや帳票が不要になった場合には、速やかにシュレッダーで破砕する。
- (3) 重要度の高いドキュメントや帳票は、鍵付きのキャビネットに保管する。

7 電子カルテシステムの利用時のパスワードセキュリティ

1) パスワードセキュリティ

情報システムの利用者は、パスワードセキュリティの侵害又はその恐れがある場合には、規定された手順に基づき、運用責任者に報告しなければならない。

2) パスワードの利用者の責任

- (1) 利用者は、パスワードの選定及び使用に際しては、本マニュアルに従わなければならない。
- (2) パスワードの変更を要請した後もパスワードの変更を行わない利用者は、システム管理者によってその利用権限を停止される。
- (3) 利用権限が停止された利用者は、失念時再登録と同様の登録方法をとる。
- (4) パスワードを失念した場合あるいは漏洩した可能性がある場合には、電話で速やかに運用責任者に届け出なければならない。
- (5) 利用者からパスワードの失念の届を受けた運用責任者は、情報システム担当に連絡をしてパスワードの利用を有効(もしくは再発行)とする。

3) 利用者 ID とパスワード管理

- (1) 通常システムにログインする際に、パスワードを利用する。
- (2) パスワードを紙などに記述して記録しない。
- (3) パスワードをファンクションキーなどに登録しない。
- (4) 自分の利用者 ID と第 1 パスワードを他の者に教えることにより、システムの利用権限を他人に貸与しない。
- (5) パスワードは、アルファベット(小文字・大文字)と数字のそれぞれを最低 1 文字以上用い、8 文字以上で構成しなければならない。
- (6) パスワードは、以下のような推測可能な用語を設定してはならない。(パスワードの禁則)
 - ①年月日、曜日、その他日付に関すること
 - ②姓名、名、イニシャル、ニックネームなど
 - ③医療機関名、部署名、それらに関するもの
 - ④電話番号やそれに類似するもの
 - ⑤ユーザ識別子、ユーザネーム、グループ ID、他のシステムの識別子
- (7) 利用者のパスワードは、登録してから 60 日が経過する日までに新しいパスワードに変更する。ただし、(6) に則って 13 文字以上の PW はその限りではない。
- (8) 再登録したパスワードで使用中のものは、継続して使用することができない。
- (9) 利用者パスワードは、一方的に暗号化し認証情報を保護する。

4) パスワードの利用に関する一般的注意事項

- (1) 自分のパスワードは、決して他人又は他のグループに口外しない。
- (2) パスワードを紙などに記述して記録しない。
- (3) パスワードをファンクションキーなどに登録しない。
- (4) 自動化されたログオンプロセスにパスワードを含めない。
- (5) 自分の利用者 ID とパスワードを他の者に教えることにより、システムの利用権限を他人に貸与しない。

8 法的に利用される電子カルテ情報の管理

- 1) 法的に利用されるデータについては、法的に求められる期間保管しておく。
- 2) 法的に利用されるデータを、可搬記憶媒体で保管する場合には、鍵付の保管庫に入れるなどして管理すること。また、用紙で保管する場合は、患者毎にファイルして保管庫に保管する。
- 3) 情報システムの操作を誤ることにより、目的と異なるデータが登録された場合には、電子カルテ修正依頼票により、その訂正を実施しなければならない。その際には、訂正前後のデータを履歴管理するとともに訂正理由を記録しなければならない。また、電子カルテ修正依頼票は、他の紙書類(原本)と同様に患者毎にファイルして保管しなければならない。

9 コンピュータウイルス対策

- 1) 外部から持ち込んだ CD やフロッピーディスク等の記憶媒体は、フォーマットするかウイルス検査後使用する。
- 2) 市販ソフトウェアは、必ず使用許諾に従って使用する。
- 3) フリーソフトウェアは、情報システム担当によって入手経路を確認し、ウイルス検査及び情報システムへの影響有無を検査し、検査に合格したもののみを使用する。
- 4) オリジナルプログラムは、ライトプロテクトを施し安全な場所に保管する。
- 5) 外部から持ち込んだハードウェア及びは、ウイルス検査を行うか初期化してから使用する。
- 6) ハードウェアや USB メモリ等記憶媒体を共用する場合は、使用者及び利用状況の管理を確実にを行う。

- 7) 利用者は、端末の再起動もしくはウイルス対策システムの機能によってウイルス対策ソフトウェアの更新を行う。
- 8) ウィルスに感染した可能性がある場合(ウイルス対策ソフトウェアメーカーから通知があった場合等)には、個人で駆除せず、運用管理者を通じて直ちに、情報システム担当に通知して指示を仰ぐ。
- 9) ウィルス感染の可能性がある場合は、直ぐにその端末の使用を中止する。
- 10) 情報システム担当は、解析結果を情報システム委員会とシステム管理者に報告する。

1 0 事件又は異常事象の報告

- 1) 情報システムに何らかの異常が検出あるいは疑われた場合は、直ちに情報システム担当に報告するとともに、遅滞なく異常事象に関する報告書を作成して、情報システム担当に提出しなければならない。

1 1 教育・訓練

- 1) 新たに情報システムを利用することになった者は、情報システムを利用する前に、情報システム担当の教育研修を受けなければならない。
- 2) 情報システムの利用者は、毎年 1 回、セキュリティ研修を受講しなければならない。

第10章 情報システムダウン対策マニュアル

1 はじめに

診療録の電子媒体による保存については、真正性、見読性、保存性の三原則を条件に、病院長の責任（説明責任、管理責任、結果責任）において実施する。その際留意事項として「運用管理規程」を定めることとしており、端末とサーバ（ソフトウェアサービス）、及びネットワークシステムダウン対策を定めることが要求されている。

診療情報の全てが電子カルテに搭載されるため、情報システムのダウンには障害の発生部位により大小の違いはあるもの、予期せざる病院運用麻痺の発生という想定脅威を常に念頭において対応する必要がある。このため、情報システムのダウンに備えて、システムダウン対策のマニュアル化を行う必要がある。

2 目的

当病院に導入されている病院情報システムは、ネットワークを経路として端末とサーバ（ソフトウェアサービス）間で通信するものであり、電子機器を用いたシステムである以上、システムダウンの発生を想定する必要がある。本マニュアルの作成はシステムダウン時に受診者がスムーズに受診を完了でき、診察情報が滞りなく記載され、伝達されることを目的とする。

3 システム障害の対策対象

システムダウンはメンテナンス、情報システム担当の対応等により一定時間後に復旧する。3時間を越えるシステムダウンは實際上極めて特殊な状況と考えられる。

システムダウン時間内には外来診療、手術部門診療、病棟診療、リハビリテーション部門診療が対策上の対象業務となるが、上記時間内のシステムダウンを考えたとき、手術部門診療は口頭指示をベースにした運用と事後入力に対応可能である。病棟診療は参照カルテシステムにより、指示情報の確認、及び予定された指示は日常診療と同様に運用可能であり、緊急時の指示は口頭支持並びに紙運用と事後入力に対応可能である。

従って、問題とすべき主たる対象は、緊急性を要し、短時間で対応を要求される外来診療とそれに伴う部門診療である。

4 システムダウン障害区分

1) 障害区分

システムダウンをその障害箇所により、以下の5通りに分類する。

- ①電子カルテシステムのダウン
- ②部門システムのダウン

- ③参照カルテシステムのダウン
- ④ネットワークシステムのダウン
- ⑤端末のダウン

2) トラブルレベルの規定

診療業務に及ぼす影響の強いトラブルで、レベルを設定する。

レベル	内容	主な対応
0	運用系サーバがダウンし、待機系サーバに切り換わり、サーバ（ソフトウェアサービス）が短時間（10分前後が目安）で復旧する見込みの場合	一時待機し、復旧後にオンラインアプリケーションを再起動
1	運用系サーバと待機系サーバがともダウンし、サーバ（ソフトウェアサービス）が短時間で復旧する見込みがない場合で、参照カルテシステムが稼働している場合	参照カルテシステムより過去カルテを参照し、紙伝票運用に切り替えて診察を行う
2	ネットワークシステムがダウンしている場合など、復旧にかなりの時間を要する場合	参照カルテシステムより過去カルテを印刷し、紙カルテ及び紙伝票運用に切り替えて診察を行う

※ 部門システムダウンについては、診療に及ぼす影響の程度が低い、あるいは範囲が狭いため、紙運用を要求される場合もあるが、診療全体に及ぼす影響は少ないため全てレベル0を基本とし、復旧見込み等の状況を判断してレベル1を適用する。また、端末ダウン(瞬断、停電など)については、システムダウンとは異なるため、後述する。

※ レベル判断は情報システム担当にて行ない、システムダウン時に各関連部署に連絡をする。

5 システムダウン時の基本姿勢

- 1) システムダウンは病院機能の突然の運用麻痺をもたらす非常事態であり、本来の持ち場に必要最小限の人員を残し、とりわけ短時間の早急な対応を要する外来診療を集中的に対応することを原則とする。
- 2) 本来提供すべきサービスが、当院で発生したトラブルのため遅延あるいは提供できな

い状態にあることを十分に理解し、患者に対して、『ご迷惑をおかけしていますが、全職員が誠意をもって対応していますのでご理解をいただきたい』という心構えで接する。

- 3) レベル 2 のシステムダウンが発生した場合は、病院長を本部長とする対策本部を設置し、本部長、情報システム委員会、管理局長、看護部長及び医事課長の協議のもとにマニュアルに沿った指示を決定・発令し、統率のとれた対応を行なう。
- 4) 迅速な対応と患者への声掛けが混乱を避ける方法であり、対策本部設置と指示系統の確立、速やかな連絡を徹底する。
- 5) 外来への動員体制
 - (1) 対策本部の指示を受けた動員可能な病棟看護師は、外来への稼動を行い、外来看護師とともに患者対応(状況説明、患者整理)を行なうものとする。
 - (2) 対策本部の指示を受けた動員可能な管理局職員は、外来への稼動を行い、患者対応や対患者用物品(机、椅子)など準備し、患者誘導を行なう。

6 システム障害時の対応

- 1) カルテシステムサーバ及びネットワークシステムの障害
 - (1) 通常、カルテサーバがダウン状態に陥っても、閲覧サーバへの切替えによりサーバ(ソフトウェアサービス)は稼動しており、運用通常の診察が継続できるため、切替え時間以上の影響を受けることはない。ただし、両サーバともにダウンし、サーバ(ソフトウェアサービス)が稼動していない場合は、電子カルテへの記載を中断して、情報システム担当からの連絡を待つ。情報システム担当の確認と判断によってレベル 0 と判断された場合は、10 分前後にて再稼動可能となるため、再度、情報システム担当からの復旧の連絡を待ち、復旧後に電子カルテシステムを再起動する。また、レベル 1 以上の連絡があった場合は、紙カルテ運用に切り替え、診療業務を再開する。
 - (2) システムダウンの情報が入ったら、情報システム使用者は、その時点からシステムが復旧するまでの間、システムダウンのレベルにかかわらず端末の使用は中止する。カルテ保存やシステム終了などの処置も一切加えないで待機する。(原因究明のために必要となる)
 - (3) レベル 0 の場合、診療業務については、電子カルテシステムの復旧待ちの体制であり、基本的に外来患者への説明のみで対応をする。
 - (4) レベル 1 の場合、診療業務については、参照カルテシステムにより過去カルテを参照にし、紙カルテ運用にて診療業務を再開し、復旧後、紙カルテにて診察した

患者データを事後入力する。

- (5) レベル 2 の場合、各サーバ（ソフトウェアサービス）自体はシステムダウンをしていないが、それを結ぶネットワークに障害があるため各システムの使用はできない状態に陥る障害である。従って、診療業務については、参照カルテシステムにより過去カルテを印刷(コンピュータ室内で印刷)し、出力した過去カルテを参照して診療業務を再開し、復旧後、紙カルテにて診察した患者データを事後入力する。なお、レベル 2 の場合は、対策本部が設置されるので、対策本部の指示やマニュアルに沿って初動対応を行なうものとする。
- (6) 画像系ネットワークダウンの場合は、装置に直接、患者 ID 等必要な情報を入力、撮影を行ない、直ちにフィルム化し診療に使用する。その際、画像は撮影を行なった各機器に保存し、復旧後、画像サーバに送信し保存する。
- (7) 医事課は、システムダウンに備えて紙運用に必要な物品を各部署に配布し、いつでも運用できるよう準備しておく。

準備すべき物品　：　紙カルテ(患者情報・受診歴・診察内容・過去処方)
カルテ記載用紙、事後入力のための記録紙
検査依頼指示伝票(検体検査、生理検査、放射線検査)
処置伝票
処方せん・麻薬処方せん
手書き用検体ラベル　等
- (8) レベル 1 以上の段階で受付に到着した患者については、紙による受付を総合受付にて行ない、診察室、担当医、受付時間を明示する受付票を手渡し、診察受付へ誘導する。
- (9) 情報システム担当よりシステム復旧の連絡を受けた後に、紙カルテ運用にて行なった診療業務分のデータは当日中に入力を完了する。ダウン時に入力され電子カルテシステム上指示が伝達されていない事項については、調査の上、指示入力依頼があるのでこの点も事後入力する。
- (10) システムダウン時に使用した紙(カルテ 2 号紙、伝票等)については、当該紙が原本となるため、カルテ庫にて厳重に保管する。

2) 端末の障害

- (1) 端末レベルで全端末が同時に使用不可能になる状態としては瞬断や停電が考えられる。停電が発生すると全ての端末において一旦電源が切れる状態になる。しかし、サーバ（ソフトウェアサービス）側は無停電対応となっており、電源が切れることなく稼動しているため、自家発電が起動(1 分以内)して端末への給電が開始された際には、端末の電源を投入し、サーバとの再接続を行う。
- (2) 個別端末レベルで使用不可能になる状態としては、ハードウェア障害や画面のフ

リーズが考えられる。この状態の時は、情報システム担当に速やかに連絡をし、端末交換等を含めた復旧作業後に診療業務を再開する。

※ 白色コンセントは商用電源のみの系統であり、停電時に自家発電に切り換わらない。一般的には端末やプリンタの電源を白色非常用（常時）と赤色コンセントに接続して設置してあるが、移設や他医療機器利用のために接続コンセントを変更する場合には注意が必要となる。

緑コンセントは非常時（常時）で一番の優先である。

3) 外部ネットワーク由来の障害対応

インターネットアクセスが存在する外部ネットワークは、電子カルテシステムとは接続のないシステムであり、その障害が診療自体になんら影響を与えない為、本マニュアルでは取扱わない。