医療情報システム
運用管理規程

第１版

牧野リハビリテーション病院

変更履歴

Rev	日　付	内　容	担　当	備　考
１	２０１８年4月１日	新規作成	システム管理委員会	

目次

第1章　　目的

本規程は、牧野リハビリテーション病院（以下「当院」という。）において、法令に保存義務が規定されている診療録、及び、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、ソフトウェアおよび運用に必要な仕組み全般（以下「医療情報システム」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、該当施設において、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、すべてネットワークを介して行なわれる業務を前提とし、今後院外の専用線等を介して持ち込まれる医療関連情報も綴集・付加されるものである。

第2章　　管理組織

1．医療情報システム管理者

1）医療情報システム管理者の情報管理に関する責務

（1）当院に医療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、電子保存に用いる器機及びソフトウェアを導入するに当って、システムの機能を確認し、これらの機能は厚生労働省が発行する「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、医療職種間で情報を共有する環境を提供するために、その基本をなす「データ保護に関する規程」を作成し、全職員に周知しなければならない。

（5）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。

（6）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。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、システム管理委員会に諮問しなければならない。

（8）システム管理者は、システム管理委員会の責任者等（委員長）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．システム管理委員会

（1）医療情報システムを安全かつ効率的に運用するためにシステム管理委員会を設置する。

（2）委員会については別紙「システム管理委員会規程」の定める通りとする。

（3）委員会名称については同様の機能を有するものであれば問わない。

3．監査委員会

1）監査委員会の責務

（1）医療情報システムを円滑に運用するため、医療情報システムに関する監査を担当する責任者（以下「監査責任者」という。）を置くこと。

（2）監査責任者の責務は本規程に定めるものの他、「医療情報システム監査規程」の定める通りとする。

（3）システム管理者は、監査責任者に毎年１回、医療情報システムの監査を実施させ、監査結果の報告を受け、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ること。

（4）システム管理者は必要な場合、臨時の監査を監査責任者に命ずること。

（5）委員会名称については同様の機能を有するものであれば問わない。

第3章　　情報システムに関する理念

１．理念

１）医療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、該当施設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通り、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該当施設が負う『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。なお、“混同”とは、患者を取り違えた記録や記録された情報間での関連性の記録内容を誤ることをいう。
『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１章に規定するシステム管理委員会の審議を経て、病院長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）当院の情報システムのデータは、別に定める「セキュリティ方針書」、「管理者マニュアル」及び「利用者マニュアル」により保護されるものとする。ここに規定する情報システムのデータ保護の規程等の内容は、以下のとおりとする。
（１）「セキュリティ方針書」
① 情報の管理や保護のための技術的な対策。
② 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。
（4）電子カルテを中心とした情報システムの診療情報等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。

3）民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について（医療分野に係る文書に限る）
（1）電磁的記録の保存、作成及び交付等を行うことができる文書
1. 医師法（昭和２３年法律第２０１号）第２４条の診療録
2. 歯科医師法（昭和２３年法律第２０２号）第２３条の診療録
3. 保健師助産師看護師法（昭和２３年法律第２０３号）第４２条の助産録
4. 医療法（昭和２３年法律第２０５号）第５２条の財産目録及び貸借対照表並びに損益計算書
5. 歯科技工士法（昭和３０年法律第１６８号）第１９条の指示書
6. 薬剤師法（昭和３５年法律第１４６号）第２８条の調剤録
7. 外国医師又は外国歯科医師が行う臨床修練に係る医師法第十七条及び歯科医師法第十七条の特例等に関する法律（昭和６２年法律第２９号）第１１条の診療録
8. 救急救命士法（平成３年法律第３６号）第４６条の救急救命処置録
9. 医療法施行規則（昭和２３年厚生省令第５０号）第３０条の２３第１項及び第２項の帳簿
10. 保険医療機関及び保険医療養担当規則（昭和３２年厚生省令第１５号）第９条の診療録等（作成については、同規則第２２条）
11. 保険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条の調剤録（作成については、同規則第５条）
12. 臨床検査技師、衛生検査技師等に関する法律施行規則（昭和３３年厚生省令第２４号）第１２条の３の書類（作成については、同規則第１２条第１４号及び第１５号）
13. 医療法（昭和２３年法律第２０５号）第２１条第１項の記録（同項第９号に規定する診療に関する諸記録のうち医療法施行規則第２０条第１０号に規定する処方せんに限る。）、同法第２２条の記録（同条第２号に規定する診療に関する諸記録のうち医療法施行規則第２１条の５第２号に規定する処方せんに限る。）、同法第２２条の２の記録（同条第３号に規定する診療に関する諸記録のうち医療法施行規則第２２条の３第２号に規定する処方せんに限る。）及び同法第２２条の３の記録（同条第３号に規定する診療及び臨床研究に関する諸記録のうち医療法施行規則第２２条の７第２号に規定する処方せんに限る。）（第二２（４）を参照のこと）
14. 薬剤師法（昭和３５年法律第１４６号）第２６条、第２７条の処方せん（第二２（４）を参照のこと。）
15. 保険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条の処方せん（第二２（４）を参照のこと。）
16. 医療法（昭和３２年法律第２０５号）第２１条第１項の記録（医療法施行規則第２０条第１０号に規定する処方せんを除く。）、同法第２２条の記録（医療法施行規則第２１条の５第２号に規定する処方せんを除く。）、同法第２２条の２の記録（医療法施行規則第２２条の３第２号に規定する処方せんを除く。）及び同法第２２条の３の記録（医療法施行規則第２２条の７第２号に規定する処方せ

んを除く。）
17. 麻薬及び向精神薬取締法（昭和２８年法律第１４号）第２７条第６項の処方せん
18. 歯科衛生士法施行規則（平成元年厚生省令第４６号）第１８条の歯科衛生士の業務記録
19. 医師法（昭和２３年法律第２０１号）第２２条の処方せん
20. 歯科医師法（昭和２３年法律第２０２号）第２１条の処方せん
21. 健康保険法施行規則（大正１５年内務省令第３６号）第５４条の処方せん
22. 船員保険法施行規則（昭和１５年厚生省令第５号）第４５条第１項の処方せん
23. 保険医療機関及び保険医療養担当規則（昭和３２年厚生省令第１５号）第２３条第１項の処方せ
24. 国民健康保険法施行規則（昭和３３年厚生省令第５３号）第２５条の処方せん
25. 高齢者の医療の確保に関する法律施行規則（平成１９年厚生労働省令第１２９号）第３０条の処方せん

4）保管期間は5年間とする。

第5章　　利用者

1．医療情報システム利用者

1）利用者の責務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）医療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）医療情報システムの情報入力に際して、確定操作（入力情報が正しい事を確認する操作）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、速やかにシステム管理者に連絡し、その指示に従うこと。
8）不正アクセスを発見した場合、速やかにシステム管理者に連絡し、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	・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	・退職又は異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・師長・技師・看護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）申請・登録・交付・非表示
（1）利用者権限の交付は、各部署における責任者（以下「運用管理者」という。）がシステム管理者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、事後報告としてシステム管理者に非表示の依頼を出す。

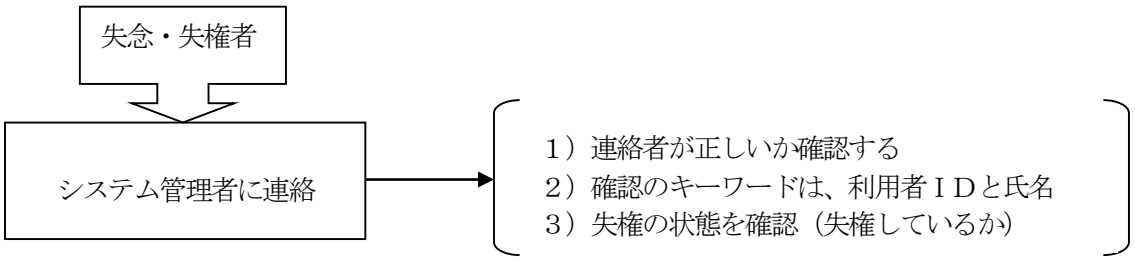
（2）利用者の登録設定・非表示手続きは、運用管理者がシステム管理者へ申請書を提出する。
① 所属部署（職種・役職）
② 利用者氏名（漢字、カナ）
③ 生年月日（和暦）
④ 性別
⑤ その他登録上必要となる項目
（3）システム管理者は、申請書に基づき利用者ＩＤ、利用者情報を登録する。
（4）運用管理者は、緊急を要する場合には口頭または紙連絡にてシステム管理者に依頼し、申請については事後とする。
（5）運用管理者は、人事異動・退職その他の事由により、当該システムの使用に関係なくなった時、速やかにシステム管理者に連絡し、非表示処理をする。
（6）システム管理者は、申請書の通り登録を行い、申請書を保管する。

4）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。

3．利用者ログの監査

実施可能な範囲内にて下記の措置を講じる必要がある。

1）不正アクセスの防止
（1）システム管理者は、不正アクセスを防止する為、以下の点を監視する。
（2）アクセス権の無い者によるデータアクセス
（3）パスワードの失権状況
2）点検の結果、異常がある場合は、その対象パスワードを使用不可とし、不正使用の防止に努める。
3）失念・失権者の復旧手順
4）失念・失権者



4．情報システムの機能要件

実施可能な範囲内にて下記の要件を満たす必要がある。

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）利用者が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器機は独立した電算室に設置する。
２）電算室の出入り口は常時施錠し、システム管理者がその入退出を管理する。
３）電算室には無水消化装置、漏電防止装置、無停電電源装置等を備える。
４）設置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する。
２）記録媒体は、利用者権限で施錠監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を定め実施する。
４）媒体の破棄は、読取り不能の状態にした後、破棄する。
５）業務運用上発生する廃棄帳票は、シュレッダーにかけ破棄する。

３．ソフトウェアの管理

１）システム管理者は、医療情報システムで使用されるソフトウェアを、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）システム管理者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）システム管理者は、定期的にソフトウェアのウィルスチェックを行い、感染の防止に努める。

４．資源管理

１）システムバックアップ／復元手順
（１）機器障害や災害などに備えて、システムのバックアップをとる事を義務付ける。
（２）バックアップの種類
① ＤＢジャーナルのバックアップ
② データベース
③ システム本体（ＯＳ）
２）バックアップ対象は、原則として運用に係るすべてのサーバとする。運用上での理由がある場合にはこの限りではない。
（１）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 業務のデータに変更があった場合。
④ 他必要と判断された場合。
⑤ オンライン終了時、又はコンピュータ利用が低い時間帯に行う。
３）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、ボリューム管理を行う。
（２）媒体には、世代管理を行い少なくとも３世代の媒体管理を行うこと。
（３）媒体の保存管理は、２節で示すデータ管理手順に順ずる。
４）システム資源の容量チェック手順
（１）システム資源の管理対象
システム管理者は、システム資源を保存する媒体は、パンク状態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、日常の利用頻度の確認をしなければならない。

① ＤＢ格納率の管理。
② 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・ユーザーズプログラム・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。

6．ドキュメントの保管・管理

1）媒体の場合
（1）磁気媒体に記憶されたプログラムドキュメントは、システム管理者の媒体保管ロッカーに格納し保管する。この際、ドキュメント管理台帳を作成し、ドキュメントの保存管理を行う。長期間保管される磁気媒体は、定期的に複写を行い消失に備える。なお、媒体の管理については、2.記録媒体の管理で述べた管理手順に従う。
（2）ファイルは消失を前提にした保存方法を施し管理を行う。

2）帳票の場合
（1）紙に記述されたドキュメントは、システム管理者のデータ保管用ロッカー等にファイリングして保管する。
（2）保管ロッカーは、常時鍵を閉めて管理する。

7．ネットワーク管理

1）システム管理者は定期的に利用履歴やネットワーク負荷等を検査し、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を確認する。
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、直ちにその原因を追求し対策を実施する

8．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。
1）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。

9．問合せ・苦情の受付窓口の設置

1）患者又は利用者からの、電子カルテシステムについての問合せ・苦情を受け付ける窓口を設けること。
2）苦情受け付け後は、その内容を検討し、直ちに必要な措置を講じること。

１０．事故対策

システム管理者、各部署において緊急時に連絡が取れるよう「院内連絡網」や「電子カルテシステム非常時運用規定」定め、非常時においても参照できるような媒体に保存し保管すること。

１１．利用者への周知法

1）システム管理者は、電子カルテシステムの取扱いについてマニュアルを整備し、利用者に周知の上、常に

利用可能な状態におくこと。

2）システム管理者は、電子カルテシステムの利用者に対し、電子カルテシステムの取扱いを説明すること。

第8章　　セキュリティ方針書

１．方針

医療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

本セキュリティ方針書は、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

システム管理委員会は、本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、医療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いう。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書は、医療情報システムに関係する全ての者が確認できる場所に配置する。

６．システム管理委員会

１）情報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情報セキュリティ方針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、委員長の責任のもとに委員会所属者及びシステム管理者が行う。

７．リスク管理

１）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）医療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

行政機関の保有するプライバシー情報は「行政機関の保有する電子計算機処理に係わる個人情報の保護に関する法律 」（１９８８年１２月施行）によって法的に保護が義務づけられている。民間の機関に対しては本法律の適用はなされないが、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と、取り戻すことができないという情報固有の特性を考え、委託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、医療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、システム管理委員会の承認を得る。

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、院内規定の定めるところにより、罰則を科されるものとする。

１２．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。ただし、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

１３．情報の共有アクセス

施設外での診療情報の共有アクセスは、事前に院長及び患者本人（あるいは代理人）の承認を得た場合にのみ共有可能とする。

１４．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志により表明され、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。なお、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）患者氏名が不祥の場合は、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。

１５．物理的なセキュリティ管理

１）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。
（２）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。
（３）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。
（４）システム診断用のハードおよびソフトの使用は利用目的を限定し、その使用を管理する。
（５）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。
（６）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。
（７）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。

１６．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、利用者権限チェック表を作成し、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変更手続き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など）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）院内の外部ネットワークは、内部ネットワークと直接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システム管理者に提出し、定期的にその安全性の維持について通信ログを報告しなければならない。
（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）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データを、電子メールで送信する場合は、その送信方法について考慮されなければならない。
（２）メール発信者、メール内容、メール受信者についての許可範囲は、「利用者マニュアル」に明確に定めるものとする。
６）監査
（１）監査責任者は、「電子カルテシステム監査基準」に照らし合わせ「電子カルテ監査規程」に則した監査を実施する。

（2）監査責任者は、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。
（3）監査責任者は、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。

7）データ保全とコンピュータウィルス
（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、利用前にウィルスチェックを実施する。
（2）ウィルスワクチンプログラムは、サーバでの一括管理とする。
（3）利用者は、使用中にウィルス感染の疑いが生じた場合は、システム管理者に連絡する。
（4）システム管理者は、障害の状況を分析しウィルスが確認された場合は、その旨を全利用者に通知して注意を喚起し、同時に病院長及びシステム管理委員会に報告しなければならない。
（5）持ち込みメディアの管理は、業務の責任者が管理する。

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設計されている。
（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ものである。
（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、常に稼動できる状態にしておく。
（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する。
（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しなければならない。

１７．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、必要に応じてシステム管理者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に実施するとともに、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 システム資源の容量を定期的に確認し、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、許可しない旨の通知を行う。

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、システム運用実施細則を定める。

１８．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企業は、職員に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）部門システムに院外アクセスを持つ委託企業は、その構造について医療シスシテム科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、定期的に、定められた内容でシステム管理者に報告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）必要に応じて、セキュリティ方針及びセキュリティ対策の研修を実施すること。
（3）教育内容には、以下の項目が盛り込まれることが望ましい。
① 情報システムの利用者に対する教育
- 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
- プライバシー、機密性及びセキュリティに影響を与える情報技術
- 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
- 診療情報の重要性と、その利用者および使用用途
- 利用者情報の重要性
- 情報セキュリティに対する想定脅威の種類
- データ保護の方式
- セキュリティ違反の重大さと罰則
- 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することが望ましい
- 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
- 情報セキュリティ方針とその実践を実現、監視、評価するための戦略
- 全ての利用者に対する情報の取扱い方法・内容
- 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
- 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
- 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、操作について教育・訓練を受けなければならない。

第9章　　管理者マニュアル

1．はじめに

1）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、病院長及びシステム管理委員会が定めた医療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「セキュリティ方針書」を基に、該当施設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、本マニュアルならびに「運用管理規程」及び「セキュリティ方針書」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．管理者及びシステム管理者

1）本マニュアル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）システム管理者

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。

③ 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システム管理者に報告する。

④ システム管理者：システム管理者の責任のもとに、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。また、院内の内部ネットワーク及び外部ネットワーク（インターネット）の利用を管理する。

⑤ 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。

⑥ 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、「セキュリティ方針書」 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、院内規定の定めるところにより、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、「セキュリティ方針書」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）システム管理者は、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登録し、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、利用者管理者から新規登録者名簿を受けて業務の管理者と協議し、利用者権限の基盤となるものを作成し、システム管理者に提出し、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）院外からの転送情報は、外部ネットワークのサーバに保存される。

（3）内部ネットワークから外部ネットワークに対してアクセスすることはできない。

（4）利用者は、運用責任者を通じてシステム管理者へ報告され、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）システム管理者は、定期的にネットワーク構成をチェックし、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 」の障害時連絡網に従って対策本部責任者に確認を取り構成部分を追

加・変更・破棄する。

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の直接のアクセスを禁止する。

（2）内部ネットワークに対して、直接院外から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、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）入退出管理

（1）休日・夜間等の利用者が制限される部署での端末利用では、運用部署での入退室記録を管理し保管することが望ましい。

（2）管理簿を保管する場合には保管期間について運用部署にて規定する。

2）名札の着用管理

（1）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）端末の管理

（1）システム管理者は、常に端末情報について把握しておくこと。

（2）管理区域外への端末の移動については、システム管理者の指示により行うことができる。

（3）端末設置及び撤去の承認は、病院長及びシステム管理委員会にて承認される。

（4）端末の設置及び撤去の実施は、システム管理者の指示により行うことができる。

4）ノートブック型端末の管理

（1）ノートブック型端末の配置してある部署の業務の管理者は、移動端末の特性上、常に配置台数と使用状況について把握しておくこと。

（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はできない。

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資源管理

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）可搬記憶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。

（2）ウィルス管理は、内部ネットワークに接続されている情報システムの端末機については自動チェックがかかる。ウィルスの感染アラームの表示された媒体は、業務の管理者がシステム管理者に連絡し共に対応を検討後処置する。

（3）情報システム上で使用する可搬記憶媒体は、定期的にウィルスチェックを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な管理を行う。

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）監査責任者の責任

（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 端末利用状況をログ情報によって定期的にチェックし、システム管理者に報告し、これを広報する。

（2）監査責任者は、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委員長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には、運用責任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）利用者パスワードの有効期間は６０日間とし、利用者は、有効期間内に速やかにパスワードの変更をしなければならない。

（3）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、一定期間利用のない利用者の権限を失権（非表示）あるいは抹消させなければならない。

（4）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手続き（期限前のパスワード更新）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、システム管理者に依頼しなければならない。

（5）運用責任者は、利用者の再発行履歴をシステム管理者から報告を受けなければならない。

（6）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、システム管理者が決定し、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）管理を行う過程で運用上支障が発生すると懸念される場合には、運用管理者と各部署長の協議により一時運用を行うことがある。

（2）利用者は、初期登録時において運用責任者より紙で配布された中の初期パスワードを一時利用し、有効期限までに自身でパスワードをシステムで推奨されているパスワード変更方法にて変更する。

（3）システム導入時において配布されている初期パスワードについては、円滑な運用を考慮し、稼働後１ヶ月以内に利用者自身でのパスワード変更を実施することとする。

（4）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。

（5）パスワードを他人が容易に閲覧できる紙などに記述して記録しない。

（6）パスワードを辞書登録やキー割り当てなど簡易に入力できる仕組みに登録しない。

（7）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、システム利用権限を他人に貸与しない。

（8）パスワードは、以下の条件で付与する。

① パスワードに使用するキャラクタは、アルファベット（大文字）、アルファベット（小文字）、数字それぞれ最低限１文字以上用い８文字以上で使用する。

② 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。

（9）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

（１０） 利用者のパスワードは、通知してから有効期限の１０日が経過する日までに新しいパスワードに変更する。

（１１） 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。

（１２） パスワードの失念再発行は以下の手順による。

① システム管理者にパスワード初期化の申請書を提出する。

② システム管理者担当者は、失念者のパスワードを初期化し通知する。
③ 急を要する場合は口頭での指示でも可能とするが、後日、申請書処理を行うこと。

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

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。

１２．コンピュータウィルス対策

1）システム管理者は、ウィルスに感染した旨の届けがあった場合、現状及び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。

１３．事件又は異常事象の報告

1）システム管理者は、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処措置を取り、システム管理者に報告しなければならない。
2）システム管理者は、事件又は異常事象の発生の状況･原因･対応措置に関するレポートを作成し、システム管理者に報告しなければならない。

１４．教育・訓練

1）システム管理者は、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、各局と協調して操作方法の習熟に努めなければならない。
2）必要に応じて情報セキュリティについての教育を実施し、受講させること。

第10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運用管理規程（以下「運用管理規程」という。）及び「セキュリティ方針書」を基に、該当施設の医療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「セキュリティ方針書」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運用責任者に提出したものをシステム管理者が利用者権限の付与を決定し、運用責任者がアクセス権限を登録された者のみ利用できるものとする。

３．義務と罰則

医療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、院内規定の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。ログオフ処理を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、ログオフ処理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。

（3）部屋から全員がいなくなる場合、最終退室者は端末の電源を切らなければならない。また、部屋の施錠をしなければならない。

（4）利用者は、就業時間外に情報システムを利用した場合、利用内容の報告を業務の管理者に行わなければならない。

（5）利用内容の報告をしない場合には、院内規定の定めるところにより、罰則を科されるものとする。

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、ただちに利用者管理者に連絡し指示をうける。

5．情報システム運用管理面でのセキュリティ

1）設備について

（1）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）利用者は、業務上必要な理由により、情報システムで可搬記憶媒体を利用する場合には、業務の管理者の許可を受けなければならない。

（2）情報システムで利用する磁気テープ（MT）及びフロッピーディスク等の可搬可能な外部記憶媒体にて保管されるデータは、患者のプライバシー及び病院運営上重要なものを含む場合、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許可なく使用できない。

（3）ログイン ID は管理者と利用者で権限を分けて設定すること。

（4）利用者の識別が可能となる様にログイン管理を行うこと。

（5）利用者は利用者専用の ID にてログインを行うこと。

（6）盗難、紛失を考慮し、内部データの暗号化等の秘匿化を検討すること。

4）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。

6．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

（1）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、速かに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、システム管理者に通知をしてパスワードの利用を有効とする。

3）利用者ＩＤとパスワード管理

（1）管理を行う過程で運用上支障が発生すると懸念される場合には、運用管理者と各部署長の協議により一時運用を行うことがある。

（2）利用者は、初期登録時において運用責任者より紙で配布された中の初期パスワードを一時利用し、有効期限までに自身で初期パスワードを所定のパスワード変更ツールにて変更すること。

（3）システム導入時において配布されている初期パスワードについては、円滑な運用を考慮し、稼働後１ヶ月以内に利用者自身でのパスワード変更を実施することとする。

（4）パスワードを他人が容易に閲覧できる紙などに記述して記録しない

（5）パスワードを辞書登録やキー割り当てなど簡易に入力できる仕組みに登録しない。

（6）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。

（7）パスワードは、以下の条件で付与する。

① パスワードに使用するキャラクタは、アルファベット（大文字・小文字 ）、数字のそれぞれを最低限１文字以上用い８文字以上で使用する。

② 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。

（8）パスワードは、以下のような推測可能な用語を設定しない。(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

（9）利用者のパスワードは、登録してから有効期限の６０日が経過する日までに新しいパスワードに変更する。

（１０） 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。

（１１） パスワードの通常変更は、以下の手順による。

① 通常は、パスワード変更ボタンによる操作で変更を可能にする。

② 有効期限が経過するまでに変更を行う必要がある。

（１２） パスワードの失念再発行は以下の手順による。

① システム管理者にパスワード初期化の申請書を提出する。

② システム管理者担当者は、失念者のパスワードを初期化し通知する。

③ 急を要する場合は口頭での指示でも可能とするが、後日、申請書処理を行うこと。

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）パスワードを他人が容易に閲覧できる紙などに記述して記録しない。

（3）パスワードを辞書登録やキー割り当てなど簡易に入力できる仕組みに登録しない。

（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。

7．法的に利用される電子カルテ情報の管理

1）データ入力後、遅滞なく証明装置により署名する。
2）法的に利用されるデータと署名データについては、法的に求められる期間保管しておく。
3）法的に利用されるデータと署名データを、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。

8．コンピュータウィルス対策

1）身元不明の記憶媒体は、フォーマットするかウィ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、入手経路を確認し、ウィルス検査後使用する。
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は、ウィルス検査を行うか初期化してから使用する。
6）ハードウェアや外部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行う。
7）内部ネットワークに繋がる端末機器は、ウィルスワクチンソフトウェアを常駐させる。
8）利用者は、端末の再起動によってウィルスワクチンソフトの更新を行う。
9）ウィルスに感染した可能性がある場合（ウィルスワクチンソフト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、システム管理者に通知して指示を仰ぐ。
１０）　システム管理者は、解析結果をシステム管理者とシステム管理者に報告する。

9．事件又は異常事象の報告

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、直ちにシステム管理者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、システム管理者に提出しなければならない。

１０．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、システム管理者の開催する教育スケジュールで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、セキュリティセミナーを受講しなければならない。

第11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、「情報システム安全管理基準」として、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、システム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生じる。このため、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

医療情報システムは、病院内高速ネットワークＬＡＮを経路としたクライアント・サーバシステムであり、電気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、システム管理者の対応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実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、部門診療、救急及び手術部門診療、病棟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、救急及び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で対応可能である。病棟診療は緊急時参照用カルテシステムより、指示情報を確認できるため、予定された指示は取得まで時間を要するが運用可能である。緊急時の指示は口頭指示並びに紙運用と事後入力で対応可能である。従って、問題とすべき主たる対象は、緊急性を要し、短時間での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．非常時運用手順書

１）システム停止が発生した場合の非常時運用を定めた「非常時運用手順書」を作成すること。
２）「非常時運用手順書」は病院全体を考慮し作成すること。
３）各部署で手順が必要な場合「非常時運用手順書」にまとめて記載されること。

５．システムダウン障害区分

１）障害区分
（１）システムダウンはその障害部位により、以下の５通りに分類される。
① 電子カルテシステム（電子カルテ、医事システム）ダウン
② 部門システムダウン（放射線、薬剤など）
③ ネットワークシステムダウン
④ 緊急時参照用カルテシステムダウン
⑤ 端末ダウン（瞬断、停電など）
２）トラブルレベルの規定
（１）システムダウンは全体範囲に影響を与える場合と特定範囲に影響を与える場合がある。
（２）影響度によりシステム対応を変える必要がある。
（３）レベル設定・・・情報システムダウンが最も診療業務に及ぼす影響の強いトラブルであり、基本的には情報システムダウンの復旧見込み時間によりレベル設定する。

レベル	内　容	主な対応
0	対象システムは継続稼働しており、すぐには影響が発生しない状況を指す。	縮退運転、予備機への自動切り替えなど 継続稼働しているので事後対応
1	対象システムに関わらず、システムが一時的に停止、あるいは、正常に稼働していないが３０分程度で再稼働が行える状況を指す	ケーブル抜け、自動的な再起動、部門サーバの再起動 再稼働を確認し事後対応
2	一部対象システム（部門サーバーなど）が完全に停止、あるいは関連システムの影響により３０分以上正常なシステム稼働が行えない状況を指す	部門サーバの停止、電子カルテサーバーの停止など 状況により非常時運用を行う
3	電子カルテシステムが完全に停止、あるいは関連システムの影響により３０分以上正常なシステム稼働が行えない状況を指す	電子カルテサーバーの停止 非常時運用を行う

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とする。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。

レベル判断はシステム管理者にて行ない、システムダウン時に各関係部署に連絡をする。

6．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、当方が引き起こ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、システム管理者、事務局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、外来への移動を行い、外来看護師とともに　患者対応（状況説明、患者整理など）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事務局の職員は、外来への移動を行い、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。

7．システム障害時の対応

1）障害対応
（1）状況に応じ、病院長、事務長の判断を仰ぐこと。
（2）非常時運用が判断された場合には、運用の手順に沿って対応を行う。
2）システムの障害
（1）通常、主サーバがダウン状態に陥っても、従サーバの稼動により通常の診察が継続できるため、従サーバの稼動中に主サーバを復旧することが可能であり、なんら影響を受けない。ただし、主・従サーバともにダウンした場合は、電子カルテへの記載を中断して、医療情報システム室からの連絡を待つ。システム管理者の確認と判断により、レベル０と判断された場合は、３０分以内に再稼動可能なので、再度、システム管理者からの復旧の連絡を待ち、復旧後、電子カルテシステムを再起動する。また、レベル２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。カルテを閉じること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)
（3）レベル０、１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２以上の場合、診療業務については、緊急時参照用カルテシステムにより過去カルテを参照し、以下の運用を行う。
① 過去カルテを参照し、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とする。
② 過去カルテを印刷し、打出し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。
（5）レベル２以上の場合、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）システムダウンに備え、紙運用に必要な物品を各部署に配付し、いつでも運用できるよう準備しておく。
① 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）
② カルテ記載用紙、事後入力のための記録紙

③　検査依頼指示伝票（検体検査、生理検査、放射線検査）
④　処置伝票
⑤　処方せん・麻薬処方せん
⑥　再診予約記載用紙
⑦　コピー用カーボン紙
⑧　手書きの検体ラベル等

（7）システム復帰の判断
① 代替手段を持って運用されたデータ（紙、写真。ファイルなど）と、復帰したデータの整合性が確認されシステム利用に支障がないことを確認する。
② 利用開始に必要な関連システムとの整合性についてシステム利用に支障がないことを確認する。
③ 電子カルテシステムの使用開始について、各部署の責任者による事前利用確認の上判断され、病院長（不在時には代行者）が指令を行う。
④ 病院長（不在時には代行者）による解除宣言により非常時運用から通常運用に切り替えること。
⑤ 復帰後、全利用者はシステムの稼働状況に注意を払い、システムやデータにおいて異常と思われる場合には即時システム管理者へ連絡すること。

（8）代替運用のデータ
① システムが正常復帰した後、代替手段を持って運用した間のデータ（紙、写真。ファイルなど）との整合性を取ること。
② 代替手段を持って運用されたデータ（紙、写真。ファイルなど）は、整合性の確認が取れるまで保存しておくこと。
③ 代替手段を持って運用されたデータ（紙、写真。ファイルなど）の破棄については個人情報、漏洩について注意すること。

（9）システムダウン時に使用した紙カルテについては、当該紙カルテが原本となるため、カルテ庫にて厳重に保管する。

3）端末ダウン（瞬断、停電など）
（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。サーバ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。
（2）個別端末レベルで使用不可能になる状態としては、短絡や画面のフリーズが考えられる。この状態の時は、システム管理者に速やかに連絡をし、復旧後、診療業務を再開する。

8．その他

1）運用管理規程の公開について規程
本運用管理規程は２０１８年４月より実施される。