統合情報管理システムの情報セキュリティ方針書

第１章　総論

１ 方 針

島根県立こころの医療センター統合情報管理システム（ 以下「統合情報管理システム」という。）が取り扱う情報は不当に暴かれたり、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及び保護されなければならない。

統合情報管理システムで処理、保管されているデータに関するいかなる情報もこの統合情報管理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

本方針書は、「統合情報管理システムのデータ保護に関する倫理規程」と上記１の方針に則って、情報の管理や保護のための技術的な対策及び統合情報管理システムの利用者や業務の管理者への教育の実施等の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

統合情報管理システム管理委員会（以下「管理委員会」という。）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、統合情報管理システムを構成する全ての部分（統合情報管理システムに関連する装置、統合情報管理システムの運用に携わる人、統合情報管理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

本方針書は、統合情報管理システムに関係する全ての者に配布する。

６　リスク管理

情報セキュリティ管理は、情報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する。

1）統合情報管理システムの情報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

７ 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）及び、民間機関に対しては「個人情報保護法」（２００５年４月１日施行)によって法的に保護が義務づけられている。当院では、漏えい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、委託業者も含めた統合情報管理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むこと。

８　責任

1）病院長は、統合情報管理システムの統括責任者として管理委員会委員長と各部署から推薦された者の中から委員を任命する。

2）管理委員会委員長は、少なくとも毎年一回、「統合情報管理システムの情報セキュリティ方針書」に基づいて、統合情報管理システムの情報セキュリティ管理状況を調査し、必要に応じて、その内容の見直しを病院長に提言する。

９ 統合情報システム管理委員会

1）管理委員会は、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、当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）管理委員会は、次のような事項を担当する。
（1）当院の「統合情報システムのデータ保護に関する倫理規程」に基づいた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）当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）当院内で発生した情報セキュリティ事件の検討及び監視
（4）情報セキュリティを強化するためのイニシアティブ
（5）情報セキュリティ対策を実践するための病院長への提言

10　情報セキュリティ管理組織

管理委員会委員長は、統合情報管理システムの情報セキュリティ管理のため、各当該部門から推薦された以下の管理者及び責任者を指名する。病院長は、これを承認する。
1）利用者管理者（総務企画課）
2）医療情報システム安全管理責任者
3）システム資源管理者（業務の管理者及び総務企画課）
4）ネットワーク管理者（業務の管理者及び総務企画課）

11　監査

（1）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、その結果を情管理委員会に報告する。
（2）監査責任者は、常に第三者的立場を堅持して公正に統合情報管理システムの運用管理、個人情報保護及び電子保存基準の確保等に関し監査を行う。
（3）監査の実施方法等詳細については、監査責任者が管理委員会の承認を得て別に定める。

12　責任の分散

情報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。

13　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対し、管理委員会は厳格な措置をとることとする。

第２章　システム・情報の利用・保存に関する基本原則

１　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、原則医師及び関連する医療スタッフ（権限付与者）とし、患者等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かかわる情報を患者等に開示する場合は、医師の責任において行うこととする。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は、医師及び看護師の責任において行うこととする。

２　統合情報管理システムへのアクセス

1）通常時の統合情報管理システムへのアクセスは、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また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統合情報管理システム端末に認識させることにより、確認すること。
2）緊急時の統合情報管理システムへのアクセス
（1）患者氏名が不祥の場合は、新たに診療カードを作成する。

（2）このカードは、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と作成後の重複検索の標準化を構築すること。
（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との融合方法を関係部門と調整するための方法を構築すること。

3　情報の管理

1)データ保全

（1）管理委員会は、「統含情報管理システムのデータ保護に関する倫理規定」に定めるデータ及び秘密情報の保護原則に沿った適切なデータの保全を図るために必要な手続き等を定めるものとする。
（2）統合情報管理システムに保存されたデータは、その真正性を保つために、統合情報管理システムの利用者が通常の操作により正当な権限で修正する場合を除き、変更してはならない。ただし、データの一貫性を保つことを目的として別に定められた手続きにより修正が認められた場合においては、この限りではない。

2）法的に使用される情報の管理・保存期間

（1）統合情報管理システム内に保存される情報のうち、法的に使用される情報（以下「法定情報」という。）は、その真正性を確保するための措置を講ずること。
具体的には、操作を行う者を厳密に認証すること、確定情報は確定入力を動機付けできる画面で入力すること、確定入力した情報の修正は、見え消し（修正前情報が削除されていることを示す削除線を重ねた状態で表示すること）により表示し、修正履歴と併せて保存され、見読できるようにされていることなど、運用上及び設計上の措置が講じられていること。
（2）法定情報は、法的に求められる期間（以下「法的保存期間」という。）保存し、見読可能な状態にしておくこと。
具体的には、変更前システムで保存したデータを変更後システムで見読可能とする又は変更又は廃止したシステムで保存した情報を見読可能な状態で維持すること。
（3）法定情報は、その所在を明確にし、開示請求に対して速やかに対応できること。
（4）紙面での保存が法的に必要であって、統合情報管理システム内にデータとして保存される情報は、法的保存期間に紙面の開示を求められた場合、速やかに開示できる状態で保存し、統合情報管理システム内データの法的正当性を担保すること。

第３章　分野別の情報セキュリティ管理対策

Ⅰ　物理的な情報セキュリティ管理

1　施設の管理

1）業務管理者は、管理する各室においては、島根県庁舎等管理規定によるほか、以下の管理策を実施する。
（1）職員以外の者が立ち入ることができる範囲を明確にすること。
（2）情報セキュリティの重要度により室内を区分する必要がある場合は、それぞれの区分の範囲及び立ち入ることができる職員を明確にすること
（3）職員のみが利用する区画において、職員が不在となる場合及び業務時間外は施錠を行うこと

2）サーバ室においては、上記に加え、以下の管理策を実施する。
（1）サーバ室の管理担当者は総務企画課長とする。
（2）サーバ室の存在を示す案内板や標識等は建物の内外を問わず表示しない。
（3）コンピュータ室は、以下の設備を有するものとする。

ア. 火災に備えるための火災検知、消火、保護設備
イ. 地震に備えるための固定器具設置等による転倒防止設備
ウ. 温度による動作異常・結露を防止するための空調設備
エ. 外者の侵入に備えるための施錠・入退室管理設備
オ. 電源の安定供給を行うための電源設備

（4）サーバ室は、常に施錠管理する。
（5）サーバ室への入退室の際は、認証を行う。
（6）サーバ室への入退室を記録し、定期的に確認する。
（7）サーバ室内は、管理担当者が許可した場合を除き、以下の行為を禁止する。
ア. 危険物の持ち込み
イ. 複写機及びFAXの設置
ウ. 撮影及び録音
エ. 喫煙及び飲食
オ. 情報通信システム機器及び記録媒体の持ち込み
（8）サーバ室へ入室する際には、必ず名札等の着用をする。

2　情報通信システム機器の管理

1）管理責任
（1）統合情報管理システムを構成する全ての機器等は、台帳に記載するとともに、その管理者（システム資源管理者）を明らかにすること。
（2）管理委員会は、自然災害や装置の故障、盗難、破壊等から統合情報管理システムを保護するために「統合情報管理システム機器等の管理規程」により、システム資源管理者等が実施すべき物理的対策を定めるものとする。

3　記録媒体の管理

（1）統合情報管理システムの医療情報及び機密情報を保存した外部記憶媒体及びそれが記載された帳票等は、業務の管理者が管理する。
（2）統合情報管理システムの医療情報又は機密情報を保存した外部記憶媒体及びそれが記載された帳票等は、利用者権限で施錠管理された場所あるいは施錠管理のできる所定の保管ロッカーに厳重保管し、機密保護に努めること。
（3）医療情報又は機密情報を保存した外部記憶媒体を、患者又は院外の機関等から受理したときは、データ授受台帳により日付、データ名称、媒体名、数量、相手担当者名を管理するとともに、定められた保管場所に前条に準じて保管すること。
（4）外部記憶媒体には、保存されている情報の重要度に応じてラベル表示すること。(統合情報管理システムの医療情報及び密情報を保存した場合には、「情報区分Ⅰ」と表示すること。)
（5）医療情報又は機密情報を保存した外部記憶媒体及び帳票及びそれが記載された帳票等を利用するときは常に職員の管理下に置き、放置しないこと。
（6）業務の管理者は、外部記憶媒体の老朽化等によりデータの品質劣化が予想される場合には、あらかじめ別の媒体に複写すること。
（7）データが記録された外部記録媒体を今までの使用目的と違う用途で再利用する場合は、データを物理的に消去（消去プログラムが有る場合にはそれを利用し、無い場合には通常フォーマットし、消去されていることを確認）すること。
（8）外部記録媒体を破棄するときは、読み取り不能の状態にした後、指定の廃棄置き場に廃棄すること。
（9）業務運用上発生する廃棄帳票は、シュレッダーにかけ、廃棄置き場に廃棄すること。

Ⅱ　人的情報セキュリティ対策

1　利用者への情報セキュリティ対策

1）責任
（1）管理委員会委員長は、統合情報管理システムの利用者の正当性を確保するとともに、診療情報等の不適切な取り扱いに起因する患者の権利・利益の侵害を防止し、基本的人権を保

護するために、利用者・が遵守しなければならない事項について利用者マニュアルとして定め、利用者に周知すること。

2）利用者の教育・研修

（1）統合情報管理システムの利用者は、統合情報管理システムの利用を許可される前に本セキュリティ方針及び情報セキュリティ対策、運用の教育を受け、これを遵守すること。

（2）情報セキュリティに理解の乏しい利用者は、1 年に一度、本セキュリティ方針及び情報セキュリティ対策の研修を受けること。

（3）教育を実施した場合は、その実施日、受講者及び内容について記録を作成すること。また、内容や受講者の理解度等を確認、評価し、常に改善を図ること。

（4）教育内容には、以下の項目が盛り込まれなければならない。

①統合情報管理システムの利用者に対する教育

ア　情報セキュリティ侵害や情報の漏えい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　プライバシー、機密性及び情報セキュリティに影響を与える情報技術
ウ　利用者の情報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
エ　診療情報の重要性と、その利用者及び使用用途
オ　利用者情報の重要性
カ　情報セキュリティに対する想定脅威の種類
キ　データ保護の方式
ク　情報セキュリティ違反の重大さとペナルティ
ケ　情報セキュリティに対する定期的な評価と改良
コ　個人情報取扱時の注意事項
サ　ＩＤ、パスワードの管理方法
シ　情報の安全性を侵害する事故発生時の対応方法

②業務の管理者に対する教育

初めて業務の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。

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業務の管理責任
イ　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
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、情報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　利用者への適切な動機付けや報奨を与えること
カ　情報の漏えいによって科される法律上の罰則
キ　情報セキュリティ侵害時の一貫した対応と訓練

Ⅲ　技術的情報セキュリティ対策

1　ネットワークセキュリティ管理

1）管理責任

（1）ネットワークは、そのセキュリティレベル及び管理者毎に分割し、その境界上に責任分界点を設けること。

（2）責任分界点で区切られた範囲毎にネットワーク管理者を選任する。

（3）統合情報管理システム管理委員会委員長は、ネットワーク管理者を統括し、ネットワーク相互の接続におけるセキュリティレベルの整合性を確保するものとする。

（4）統合情報管理システム管理委員会委員長は、ネットワークを脅威から保護するためにネットワーク管理者が実施すべき対策を定めるものとする。

2）基本原則

（1）患者の個人情報を含む秘匿すべき重要情報は、原則として内部ＬＡＮ上で管理する。

（2）重要情報を保護し、業務を安定的に継続するため、内部ＬＡＮにおいては特に許可された利用者の許可された方法による通信のみを認めるものとし、許可を得ない利用者又は通信方法による通信を禁止する。

2　利用者及び権限管理

1）利用者の識別と認証

（1）利用者権限の管理に関しては、「統合情報管理システムのデータ保護に関する倫理規定」に定めるもののほか、以下に定める。

（2）管理委員会は、利用者及び利用者権限の適切な管理のために必要な手続き等を定めるものとする。
（3）管理委員会は、利用者のなりすましの防止のために必要な措置を講じるものとする。
（4）利用者に関する情報は、統合情報管理システムを構成する全てのシステムで統一する。

3　システム管理

1）プログラム管理

（1）統合情報管理システムのプログラムやマスタの変更は、特別に権限を付与された利用者に限定する。
（2）上記（1）の変更については、事前に定めた変更手続きに則って実施する。
（3）利用されるソフトウェアは、ライセンス契約に準拠したものであることが保証できるようにしておく。
（4）バックグラウンドで動作している不要なソフトウェア及びサービスは可能な限り停止し、統合情報管理システムのブログラムに影響が出ないよう対策を講じること。

2）システム管理

（1）システム資源管理者は、システムの状況を定期的に点検し、障害防止のために必要な措置を講じること。
（2）システム資源管理者は、システムの処理領域や保存領域などの容量を定期的に確認し、容量不足等が予想される場合には速やかに対処すること。
（3）システム資源管理者は、システムに障害が発生したときに速やかに検知するための対策を実施すること
（4）システム資源管理者は、障害の検知及び障害復旧方法について、手順を明確にし、早期の復旧に努めること。

3）時刻管理

（1）システム資源管理者は、情報システム処理結果の証拠性、信頼性を確保するために、情報システム機器の時間をタイムサーバと同期させること。

4　コンピュータウイルス対策の一般原則

1）ウィルス対策

（1）全ての情報資源管理者は、原則として全ての機器にウィルス対策ソフトを導入するとともに、ウィルス定義ファイルを最新に保つこと。
（2）管理委員会は、USBメモリ等の外部記憶媒体の利用手順を定めるとともに、外部記憶媒体の利用状況について監視するものとする。
（3）管理委員会は、ウィルス感染防止及びデータ保全のため、USBメモリ等の外部記憶媒体の利用を制限することができる。

2）ウィルス感染事故の取り扱い

（1）管理委員会は、感染による被害の拡大防止と、再発の防止を図るため、統合情報管理シス

テムがコンピュータウイルスに感染した場合の取り扱いを定めるものとする。

5　データ保全

1）バックアップ

（1）システム資源管理者は、統合情報管理システムを構成する全ての機器等により管理される電磁的記録（診療記録などのデータ、プログラム及び設定情報等の全てを含む。以下同じ。）は、自然災害や装置の故障、盗難、不正アクセスやシステム障害による棄損、改ざんから保護し、早期の復旧を可能とするため、常にバックアップデータを取得しておくこと。

（2）システム資源管理者は、バックアップの取得方法・手続きについて、当該データの重要度に応じて個別に定めるものとする。ただし、診療情報及び法定情報については、自然災害等から保護するため、院外においてバックアップデータの保管を行うこと。また、改ざんから保護するために、３世代以上のバックアップデータの保存に配慮すること。

（3）システム資源管理者は、外部記憶媒体にバックアップデータを保存する場合においては、第３章Ⅰの３の規程準じて、施錠管理された場所あるいは施錠管理のできる所定の保管庫に厳重保管し、機密保護に努めること。

Ⅳ　緊急時の情報セキュリティ対策

1　情報の安全性を侵害する事故発生時の取り扱い

（1）管理委員会は、統合情報管理システムで管理する情報の漏洩、改ざん、破壊等が発生した場合の取り扱いについて別に定めるものとする。

2　障害時の取り扱い

（1）システム資源管理者は、その管理するシステムに異常が生じるまたは生じる恐れがある場合には、速やかに医療情報システム安全管理責任者に連絡し、連携して対応を行うこと。

（2）システム資源管理者は、システム復旧後速やかに原因を調査するとともに、管理委員会に諮って再発防止策及び未然防止策を策定すること。

3　業務継続計画

（1）統合情報管理システムに重大な障害が発生した場合においても、業務を継続するための手順を「情報システムに関する事業継続計画（ＩＴ－ＢＣＰ統括）」に定め、必要に応じてＣＳＩＲＴ及び医療業務継続対策チームで見直しを実施する。

（2）災害による統合情報管理システムの棄損に対して、業務を速やかに再開するための対策を検討する。