安全管理規定

－ 文書情報 －

□制定日：２０１２年7月２０日
□更新日：２０１８年2月２７日
□管理元：事務局
□作成　：事務局
□審査　：
□承認　：事務局長（２０１８年2月２７日）

改　訂　履　歴

版数	制定・改訂日	作成	審査	承認	内　　容
1.0	2012 年 7 月 20 日	事務局		事務局長	新規作成
2.0	2015 年 3 月 24 日	事務局		事務局長	第 3 条、第 9 条、第 10 条、第 11 条、第 16 条、第 17 条、第 23 条修正、追記
2.1	2016 年 2 月 1 日	事務局		事務局長	第 26 条パスワードの更新期限を 60 日に修正
2.2	2017 年 2 月 17 日	事務局		事務局長	第 21 条ログ保存期間 13 ヶ月に修正
2.3	2018 年 2 月 27 日	事務局		事務局長	第 11 条追記、第 27 条 6 項追記

目次

安全管理規定

第１章　総則

（目的）

第１条　この安全管理規定（以下、「本規定」という。）は、「島根県医療情報ネットワーク基本要綱」（平成 24 年 2 月 7 日）に基づき、特定非営利活動法人しまね医療情報ネットワーク協会（以下、「当協会」という）が、「島根県医療情報ネットワーク」（以下、「医療情報ネットワーク」という）で取り扱う個人情報を含む医療情報を安全に管理し、漏えい、き損、改ざん等の物理的、技術的、人的被害から守り、その機密性、完全性、可用性を確保し、当協会が提供するサービスの効率性及び信頼性を確立し、かつ、維持することを目的とする。

（用語の定義）

第２条　本規定で用いる用語の定義は以下のとおりとする。

（１）システム運用管理責任者
　　理事長が選任し、安全管理に対する施策、権限を有する。

（２）医療情報ネットワーク管理機器
　　参加団体とアプリケーション・サービス提供者が医療情報ネットワークに接続するための接続装置、全県 IDC に設置されたサーバ、それらを結ぶアクセス回線およびルータ・ファイアウォール等の通信管理機器

（３）医療情報サービス提供機器
　　当協会がアプリケーション・サービス提供者として提供するサービスを稼働させるサーバ・アプリケーションソフトおよび関連端末

（４）医療情報処理システム
　　医療情報ネットワーク管理機器および医療情報サービス提供機器の総称

（５）医療情報処理施設
　　医療情報処理システムを設置する部屋

（適用範囲）

第３条　本規定の人的適用範囲は、役員、正職員、契約社員、派遣職員、パート･アルバイトを含む全ての従業者及び、委託契約を行っている委託先において、委託業務に携わる全ての従業者を範囲とする。

（管理対象）

第４条　本規定は、医療情報処理システムを構成するすべての機器を管理対象とする。

２　本規定によらず、医療情報ネットワークを安全に運用管理するために必要な機器類を

管理する場合は、本規定を遵守するものとする。

第２章　物理的安全管理措置

（医療情報処理システムを設置する建物）

第５条　医療情報処理システムを配置する場所（以後、「医療情報処理施設」という。）は、当協会の専有する建物、あるいは当協会が全体を専有するフロア、あるいは十分に安全性が確保された外部事業者のデータセンター内に設置された医療情報処理システム専用のサーバラックとすること。

２　外部事業者のデータセンターを利用する場合には、医療情報処理システムを構成する全ての機器を十分な強度を持った専用のラックに納め、同じデータセンターを利用する他事業者からの不正なアクセスに対する保護対策を施すこと。

３　部屋を区切る壁面、天井、床部分においては、傍受、盗撮等の不正な行為を防止するための十分な厚みがあり、部屋に対する物理的な不正侵入を抑止・検知するための侵入検知装置を導入されていること。監視カメラ等による常時監視が実施されていることが望ましい。

（医療情報処理施設の入退室管理）

第６条　医療情報処理施設は、有人受付・IC カード・生体認証・暗証番号等のうち、二要素以上の組合せによる認証により入退館、入退室者を制限し管理する。

２　認証を受けた要員に続いて認証を受けずに入退室する行為、及び、認証を受けて入退室した要員から認証装置越しに認証デバイスを受け取り同じデバイスで再度入退室を行うこと等の不正行為を防ぐ装置を設置する。

３　有人受付・機械式入退管理は、いずれも履歴を取得し、定期的に履歴を点検すること。

４　職務中においては、要員の職員証を外部から目視で確認できる状態で携帯するとともに、医療情報施設内への個人的所有物の持ち込みは禁止する。

５　職員証を紛失あるいは不正利用された疑いを持った際には、ただちにシステム運用管理責任者に連絡すること。また、職員の退職時には確実に職員証を回収・廃棄すること。

６　医療情報処理施設内へは、外部媒体（MO、USB、CD-ROM 等）を、原則、持ち込んではならない。但し、ソフトウェアのインストール等の理由で外部媒体を利用する場合は、予めシステム運用管理責任者の許可を得た上で職員が同伴することで利用できるものとする。なおこの場合、外部媒体は、施設への入室前に同伴する職員に手渡しで預け、退室するまでの間は、同伴する職員が外部媒体の抜き差しおよび利用を管理しなければならない。

（事務所の入退管理）

第７条　当協会の事務所（以後、単に「事務所」という。）は、夜間休日は施錠し、鍵は事務局および事務局が許可した者が管理する。

２　事務局が許可した者は、事務所の鍵の利用状況を記録し、定期的に事務局に報告すること。

３　事務所を最終退出する際は、「点検簿」に従い室内を点検し、記録すること。なお、前２項の記録および「点検簿」は、事務局が毎月点検すること。

（医療情報処理装置のセキュリティ）

第８条　医療情報処理システムを構成する装置（以後、「医療情報処理装置」という。）は、製造元又は供給元が指定する間隔及び仕様に従って保守点検を行うこと。

２　火災発生時の消火設備が医療情報処理装置に損傷を与えないよう配慮すること。また、機器を設置するサーバラックは、震災時に転倒することが無いよう確実に設置するとともに、十分な換気・空調を施すこと。

３　保守点検で障害不良等が発見された際は、当協会が管理する領域で対応作業を行うこととし、外部に持ち出すことが無いようにすること。ただし、必要により外部に持ち出しての作業が必要な場合には、装置内の電磁的記録を確実に消去した場合に限り持出しを許可するが、記憶装置等、障害により情報の消去が不可能となっている装置については補修ではなく物理的に破壊し廃棄すること。

４　医療情報処理システムにつながる端末は、離席時には画面の電源を切るか、パスワード付きスクリーンセーバ（起動時間：5 分以内）を設定すること。

（廃棄・再利用）

第９条　個人情報（不要になった個人情報を含む）及び機密情報が格納された機器等を廃棄する場合は、事務局長が選任した者が以下の方法で廃棄し、廃棄した記録を残しておくこと。

１.サーバ･PC 等を廃棄する場合､ハードディスクは確実な方法でデータを完全消去するか、物理的に破壊し廃棄すること

２．CD、USB 等の外部媒体は、物理的に破壊し、廃棄すること。

３．紙媒体は、シュレッダーで裁断し廃棄すること。

４．上記いずれにおいても、外部の事業者に廃棄を委託する場合には、廃棄方法を確認するとともに、確実に廃棄したことを証する証明等の証跡を取得すること。

（医療情報処理装置及び事務所内機器の外部への持ち出し）

第１０条　医療情報処理装置は、第８条３項に依る以外、外部へ持ち出してはならない。

２　事務所内機器は、持ち出しが許可されている機器以外は原則禁止とする。ただし、やむを得ず許可のない機器を持ち出す場合は、個人情報が格納されていないか、格納されていればＰＷの設定等安全確認を行った上、システム運用管理責任者の許可を得ること。

（情報システムの安全に関する技術的と運用的対策の分担を定めた文書の管理規定）

第１１条　各システムはその設計時、運用開始時に技術的対策と運用による対策を、基準適合チェックリストに記載し、必要時には第三者への説明に使える状態で保存する

２　システムの保守時には基準適合チェックリスト記載にしたがっていることを確認する。

３　システム改造時は最新の基準適合チェックリストに従って、技術的対策と運用による対策の分担を見直す。

第３章　技術的安全管理措置

（医療情報処理装置およびソフトウェアの保守）

第１２条　保守に伴う医療情報処理装置及びソフトウェアの変更がもたらす影響を考慮し、影響を最小限に抑える方策を検討すること。

２　医療情報処理装置及びソフトウェアの保守作業については、業務の停止時間を最小限に留めるように計画を立てるとともに、次の様な内容を含む変更手順を整理し実施すること。

関係者への通知、変更申請および承認（申請者情報、承認者情報、対象機器情報、変更作業開始日時、変更作業期間、変更理由、機器に納められている情報の概要、変更に伴うリスク評価の結果、機器が損傷した場合の対応策、等）、変更後の試験方法、変更作業に支障が発生した場合の復旧手順、変更終了の承認、変更に伴う影響の監視、等。

３　潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（パッチ適用、設定変更等）を決定すること。

４　メーカー等から提供されるセキュリティパッチは、原則自動適用とする。なお、サーバ等は、パッチを適用することによるアプリケーション等への不具合がない事を確認した上で適用するものとする。

５　保守作業を外部事業者に委託する場合には、上記要件を満たしていることを確認すること。

６　情報システムで扱う情報資産について、リスク分析を行い、その対応方法について文書で保存しておくこと。対応方法については、技術的対応と運用的対応を適切に分担すること。

（開発・試験施設と運用施設の分離）

第１３条　ソフトウェア開発を行う際には、ソフトウェア障害の影響を避けるため、運用施設とは直接に接続されていない開発用の情報処理施設を用いて行うこと。

２　運用施設に保存されている医療情報を開発施設及び試験施設にコピーならびに試験用データとして直接利用してはならない。利用する場合には、個人情報の消去及び元のデータを復元できないように一部データをランダムに置き換える等の処置をした上で、

医療機関の了解を得た上で利用する。

（悪意あるコードからの保護）

第１４条　最新の脅威についての情報収集に努め、導入している悪意のあるコード対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認すること。脅威の例としては、コンピュータウイルス（ワーム）、バックドア（トロイの木馬）、スパイウェア（キーロガー）、ボットプログラム（ダウンローダー）等がある。

２　悪意のあるコード対策ソフトウェアでは、リアルタイムスキャン（ディスク書き出し・読み込み）、定期的な自動スキャン（週 1 回以上）、外部記憶媒体へのデータ書き出し・読み込み時におけるオンデマンドスキャンを設定すること。

３　定義ファイル、スキャンエンジンは自動アップデートとするか、少なくとも週 1 回以上定期的な更新を行うこと。

（外部事業者が提供するサービス）

第１５条　外部事業者により提供されるサービスを特定し、サービスレベルを確認するとともに、サービスの実施、運用、維持について定期的に検証すること。

２　サービス実施について事前、事後報告を義務づけ、報告内容を点検確認すること。

３　サービスを実施する人員は予め届け出を受けサービス実施時に確認するとともに、原則、職員が監督している状況で作業を実施すること。

４　サービス実施にともなう処理施設内への立ち入り手順に関しては、職員の入室、退室手順に準ずること。

（ネットワークの管理）

第１６条　セキュリティゲートウェイ（ネットワーク境界に設置したファイアウォール、ルータ）では、接続先の限定、接続時間の限定等のアクセス制御を行うこと。

２　ネットワーク機器及びサーバ、端末の空いているネットワークポートへの接続を制限すること。

３　医療機関等との接続ネットワーク境界には侵入検知システム（IDS）及び侵入防止システム（IPS）などを導入し、ネットワーク上の不正なイベントの検出、あるいは不正なトラフィックの遮断を行うこと。

４　侵入検知システムが、緊急度の高い攻撃・不正アクセス行為を検知した際は、監視端末への出力や電子メール等を用いて直ちに管理者に通知する設定にしていること。

５　専用回線等のクローズネットワークを介して情報処理設備に接続する場合においても適切な認証を用いること。

６　ネットワーク経由で直接、特権ユーザとしてログオンする行為を禁止すること。

７　VPN 接続を行う場合には VPN 装置間で相互に認証を行うこと。

８　VPN 接続を含むネットワーク接続のログ（認証ログ及び接続ログ）を記録し、毎月定期的に点検すること。なお、不正なアクセスの兆候を検出した場合は、システム管理者

に通知するとともに、実態を把握するとともに、必要に応じ是正・予防処置を講じること。

９　無線 LAN の使用は原則禁止する。なお、業務上、使用せざるを得ない場合は、システム運用管理責任者の承認を得た後に、WPA2-AES 以上の暗号化を行った上で、期間を限定し利用する。

（媒体の取扱い）

第１７条　医療情報処理システムのデータを記録した可搬型の記憶媒体は、システム運用管理責任者の許可を受けない限りは持ち出してはならない。

２　情報交換、情報保管以外の目的で記憶媒体を用いないこと。またその場合、媒体内のデータにパスワードによるアクセス制限又は暗号化を施すこと。

３　媒体は、施錠可能なキャビネット等で保管するとともに、一覧表を作成し、所在管理を行うこと。なお、未使用の媒体は、事務局が保管し、払い出し等を管理すること。

４　媒体を配送する際は、配送物と宛先に間違いがないかを十分確認した上で配送すること。

５　配送業者から媒体を受け取る時は、情報処理設備とは別の搬入・搬出専用の区域で正規職員が直接受け取ること。

６　CD、DVD 等の光学メディア、MT（磁気テープ）等の媒体を廃棄する場合には、物理的に破壊し（高温による融解、裁断等）廃棄する。なお、媒体の破壊は、協会自身で行うが、破壊した媒体の処理は外部の専門事業者に依頼することが可能である。

７　ハードディスク等の固定記憶装置の扱いについては第９条（廃棄・再利用）に従う。

（配送時のセキュリティ）

第１８条　物理的に情報を搬送する場合には、以下の対策を実施すること。

ただし、以下の対策を実施する事が困難な場合は、別の安全対策方法を示しシステム運用管理責任者の許可が得られた場合は、以下の対策以外の方法で搬送する事ができる。

(1) 予め評価選定された配送業者に依頼し、配送伝票を１ヵ月以上保管する。

(2) 配送時の作業者については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐこと

(3) 交換する記憶媒体の数と種類について、予め情報交換して受領時に欠損が無いことを確認すること

(4) 不正な開封を検出することのできるコンテナ等を利用すること

２　電子的に情報を転送する際には以下の対策を実施すること。

(1) ファイル転送等による送受信を行う際は、送信者、受信者は相互に電子的に認証を行い相手の正当性を検証すること。

(2) 送受信する経路は適切な方法（VPN、SSL 等）で傍受のリスクから保護されていること。

(3) 送受信に失敗する時には、三回を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施すること。
(4) 電子メールに添付する場合は、必ず暗号化し、復号のためのパスワードは送信メールとは別の手段で確実に相手先に伝えること。

（医療情報処理システムに対するセキュリティ）

第１９条　開発用コード又はコンパイラ等の開発ツール類および作業者個人のファイル、情報処理に不必要なファイル等は、運用システム上に置いてはならない。

２　業務に供するソフトウェア及びオペレーティングシステムソフトウェアについて、十分な試験を行った上で導入すること

３　運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得すること。

４　システム運用情報（システム及びサービス設定ファイル等）の複製及び利用については監査証跡とするためにログを取得すること。

（アプリケーションに対するセキュリティ）

第２０条　アプリケーションでのデータ入力は、データ範囲・データタイプの制限・入力文字種及び長さの制限の設定など、自動的な誤り検出を行う機構を導入すること。

２　Web を通じてデータの入力・閲覧を行う場合、クロスサイトスクリプト対策、SQL インジェクション対策等が実施されていることを確認すること。

３　アプリケーション及びアプリケーション稼動に利用する第三者のソフトウェア（ライブラリ、サーバプロセス等）については、公開される最新の脆弱性情報を参照し、迅速に対応策をとること。

４　アプリケーションにて情報の登録、編集、削除等を行う際には、ユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行うこと。

（暗号の管理）

第２１条　電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとすること。

２　医療機関等から受け付けるデータを検証するための認証機関の公開鍵証明書は安全な経路で入手し、別の経路で入手したフィンガープリント(※)と比較して、正確性を検証すること。

※公開鍵証明書のハッシュ値のこと。証明書とフィンガープリントを別々の経路で入手し、比較することで証明書の正しさを確認する。

（ログの管理）

第２２条　以下に示すシステム使用状況等について監査ログに記録し、不正な行為・システム異常等の有無について毎月初にシステム管理者が点検する。

・作業者情報（作業者 ID、ログオンの可否、利用時刻及び時間、実行作業内容等）
・ファイル及びデータへのアクセス、変更、削除記録
・データベース操作記録
・修正パッチの適用作業（作業者 ID、変更されたファイル）
・特権操作（特権取得者 ID、特権取得の可否、利用時刻及び時間、実行作業内容）
・システム起動、停止イベント
・ログ取得機能の開始、終了イベント
・外部デバイスの取り外し
・IDS・IPS 等のセキュリティ装置のイベントログ
・サービス及びアプリケーションの動作により生成されたログ

２　サーバの時刻が適切となるよう、時刻サーバの導入・定期的な点検・再設定などの手段を講じること。

３　ログデータのアクセス権限者を制限し、ログを保護すること。また、最低限１３カ月程度のログを保存すること。

（バックアップ）

第２３条　バックアップを取得するサーバ等を特定し、原則、毎日バックアップし 3 世代以上の世代管理を行う。

２　バックアップ媒体は、アクセスが制限された室・キャビネット等で確実に保管する。

（アクセス制御）

第２４条　情報処理に用いる情報処理機器、ソフトウェアおよびデータに関するアクセスポリシーを定め、アクセス権限者を明確にすること。リモートメンテナンスを行う場合も同様とする。

２　アクセス権限は、システム管理者に申請し、それに基づき適切にアクセス権限を付与し、その状況を記録すること。

３　アクセス権限者を定める際は、業務内容等を考慮し、作業者を最小限にするとともに、必要最小限の権限とするよう考慮すること。

４　作業者に与えられた権限外の情報や権限外の操作画面を表示しないよう権限管理を行うことが望ましい。

５　定められたアクセス制御方針がファイル、ディレクトリパーミッション、データベースアクセス等のアクセス制御機構として適切に反映されていることを定期的に検証し、記録すること。

（ID の管理）

第２５条　作業者にはユニークな ID を付与し、ID の共有は原則不可とする。

２　やむを得ない理由で共有 ID を使用する場合は、同 ID を使ったものが特定できるよう別途作業日誌等により作業開始日時・終了日時等を記録すること。

３　作業者が変更もしくは退職した際には、直ちに当該 ID を利用停止すること。
４　不要な ID やアカウントが残っていないことを毎月定期的に確認すること。
５　情報処理装置及びソフトウェアを使用する前に、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等、必要のないアカウントについては削除あるいはパスワード変更を行うこと。

（特権 ID の管理）
第２６条　特権の使用時には作業実施内容を記録すること。
２　システムとして可能であれば、特権の種類に応じてアカウントを分離し、ファイルやディレクトリに対するアクセスを制限すること。また、特権 ID で使用可能なコマンド及びユーティリティについて業務上必要な最低限の範囲に制限し、重要なコマンド、ユーティリティ及びログについて改ざん、削除など不正な行為を防止すること。

（パスワードの管理）
第２７条　システム管理者が設定した初期パスワードは、使用する前に変更すること。
２　パスワードは、英数混合８ケタ以上とすること。
３　パスワードは、定期的に６０日毎に変更する。なお、過去に利用したパスワードは再利用せず、付箋・張り紙等に記録し張り付けるなどをしてはならない。
４　パスワード変更時には変更前のパスワードの入力を要求し、一定回数以上間違えた場合には、そのアカウントを一時的に使用できなくするなどの措置を講じること。
５　連続したログオンの失敗回数を制限するアカウントロック機能を有効とすること。また可能であれば、ログオンの連続した失敗が許容限度回数に達した場合には警告メッセージをシステムの管理者に送出する仕組みを導入すること。
６　類推しやすいパスワードの使用や類似のパスワードを繰り返し使用しないこと。

第４章　人的安全管理措置

（要員の管理）
第２８条　医療情報を操作する可能性のある要員の全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約あるいは守秘義務契約への署名を求めること。
２　派遣従業員については機密保持義務及び継続的な情報セキュリティ教育を課すことを条件に選定、派遣することを求めること。
３　医療情報を操作する可能性のある要員の全てに情報セキュリティに関する教育を行い、一定水準の理解を得たものだけを選定すること。派遣従業員に関しては、派遣元に対し、情報セキュリティに関する一定水準の知識、理解を持つ、あるいは持つことができる人員を選定、派遣することを求め、受入れ後に正規職員同等の教育を行うこと。

４　医療情報を操作する要員が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳及び返却確認手続きを予め規定しておくこと。

５　業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求めること。派遣従業員については、派遣契約解除時に同等の合意書への署名を求めること。

以上