阿波あいネット情報セキュリティ規約
第３版

令和４年２月

一般社団法人阿波あいネット

改定履歴

版数	日付	内容
第 1.0 版	平成 30 年 8 月 1 日	新規制定
第 2.0 版	令和 2 年 11 月 2 日	対象となるシステム、情報機器及び情報の明確化（1.1.1.2 対処システム、情報機器及び情報） 総務省及び経済産業省の 3 ガイドラインが 1 つに統廃合されたことに伴う改正（1.1.1.3 法令及び標準規格対応）管理体制の改正（2.1.1 管理体制） 教育及び研修体制の改正（2.1.8 教育及び研修） その他、文言の改正及び他の規約との整合性一致
第 3.0 版	令和 4 年 2 月 21 日	文言の改正

目　次

1　総則

1.1　総則

1.1.1　総則

1.1.1.1　（目的）

本規約は、一般社団法人阿波あいネット（以下、当法人とういう。）で運用する健康・医療・介護（以下、医療等という。）に関する情報連携システム（以下、「当システム」という。）の安全かつ合理的な運用を図り、併せてカルテ情報、レセプト情報、院外処方箋、放射線・内視鏡及び検査結果等の電子情報をデータセンターに収集・蓄積し、利用者が参照するための運用にあたって、必要事項を定義し、適正なセキュリティ管理を行うとともに、当システム及び取り扱う情報の適正利用に資することを目的とする。

1.1.1.2　（対象システム、情報機器及び情報）

対象となるシステムは、当システムそれに接続する利用施設等の情報機器や周辺装置等及び医療等の情報を保存した情報記録可搬媒体（以下、可搬媒体という。）とする。

2　対象となる情報は、当システムで取り扱う電子情報だけでなく、対象機器へ入力する前の紙媒体の情報や全ての個人情報にも適用する。

3　対象機器の扱う情報の定義、安全管理上の分類及びリスク分析は台帳等に情報を記入し維持する。

4　将来、他地域における同種の情報連携システムと連携する場合には、これも対象機器及び対象情報として取扱い、対象機器の扱う情報の定義、安全管理上の分類及びリスク分析は台帳に情報を記入し維持する。

1.1.1.3　（法令及び標準規格対応）

システム管理統括責任者は、システム変更・改定時の対象とするため、当法人で対応すべき法令及び標準規格を列挙し、変更状況を確認するともに対応に必要な措置を講じる。

2　法令に準じたガイドラインとして、以下の各号に対応する。また、対応するガイドラインは最新のものとする。

（1）厚生労働省　医療情報システムの安全管理に関するガイドライン

（2）総務省・経済産業省　医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン

3　国内において定められた標準規格として、厚生労働省標準規格に対応する。また、対応する標準規格は最新のものとする。

1.1.1.4　（利用施設）

利用施設は、当システムを利用するにあたって事業管理者に施設参加申込書を提出し、参加の許諾を受けた医療・介護施設をいう。

1.1.1.5　（利用者）

利用者は、当法人社員及び職員並びに利用施設に所属する職員で、本規約に定める識別番号（以下「ID 番号」という。）及びパスワードの登録を完了した当システムを利用する者のことをいう。

2　一般社団法人阿波あいネット及び利用施設における規約

2.1　システム運用における管理

2.1.1　管理体制

2.1.1.1　（管理体制）

当システムの安全かつ合理的な運用を図るため設置されたシステム管理委員会及び個人情報保護委員会において、必要な管理体制を整備する。

2　当システムを管理するため、次の各号に掲げる責任者等を置く。

（1）当法人に当システム及び個人情報の運用・管理を統括する運用責任者を設置する。

（2）当法人にシステム管理統括責任者を設置し、システム管理委員長を持って充てる。

（3）当法人に個人情報取扱統括責任者を設置し、個人情報保護委員長を持って充てる。

（4）利用施設にシステム管理施設責任者及び個人情報取扱施設責任者を設置する。

（5）システム管理統括責任者及びシステム管理施設責任者の実務を代行する担当者として、必要に応じシステム管理担当者を設置する。

2.1.1.2　（マニュアル、契約書等の文書管理体制）

各種規約、様式、契約書、マニュアル等の文書の管理については別途定める規約による。

2.1.1.3　（監査体制と監査責任者）

監査責任者は、情報システムを円滑に運用するため、監査の実施及び報告を行う責任及び権限を他の責任にかかわりなく行い、業務を遂行する。

2.1.1.4　（苦情及び質問等の受付体制）

個人情報の取扱いについて地域住民、医療・介護施設から苦情や質問を受け付ける相談窓口を設置するものとする。また、情報システムの運用に関して利用者から質問を受け付けるヘルプデスクを設置するものとする。

2.1.1.5　（事故対策体制）

システム管理統括責任者は、緊急時及び災害時の連絡、復旧体制及び回復手順を定め文書化し、利用者に周知の上、常に利用可能な状態にする。

2.1.1.6　（教育及び研修体制）

システム管理統括責任者は、当システムの利用について利用者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する。

2　システム管理統括責任者は、当システムの利用者に対し、定期的に当システムの利用及び情報セキュリティに関する教育又は周知等を行うものとする。

3　個人情報取扱統括責任者は、当システムの利用者に対し、定期的に個人情報保護に関する教育又は周知等を行うものとする。

2.1.2　責任者及び利用者の責務

2.1.2.1　（運用責任者の責務）

運用責任者は、本規約に基づき次の各号に掲げる責務を負う。

（1）当システムの機能要件に挙げられている機能が支障なく運用される環境を整備する。

（2）当法人が設置した、住民、参加同意者及び利用施設等から当システムにおける個人情報の取扱いについての問い合せ、相談及び苦情を受け付ける問い合せ窓口を設ける。

（3）当システムの利用者を認定する。

（4）監査責任者の監査結果に基づき、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。

2.1.2.2 （システム管理統括責任者の責務）

システム管理統括責任者は、本規約に基づき次の各号に掲げる責務を負う。

（1）当システムに用いるハードウェア等の情報機器及びソフトウェアを導入するに当たって、システムの機能を確認するとともに、ガイドラインで定める安全性を確認するものとする。

（2）情報機器、ソフトウェア構成及び構成管理の内容について、利用施設と相互確認するとともに、その文書化を行い、システム管理施設責任者へ通知することができるものとする。

（3）医療等の情報の安全性を確保し、常に利用可能な状態に置くこと。

（4）システム管理統括責任者は、安全かつ正常な稼働を確保するため、ネットワークの稼働状態を常に監視する対策を実施し、異常な動作、不適切なシステムへのアクセス等の検知に努めるものとする。

（5）システム管理統括責任者は、定期的にログの収集を行い、ログを保管するものとする。

（6）情報機器やソフトウェアに変更があった場合においても、情報が継続的に使用できるよう維持・管理する。

（7）当システムの利用者及び利用端末の登録は、各利用施設のシステム管理施設責任者が届け出及び利用端末の所在管理を行うこととする。さらに、そのアクセス権限を規定し、不正な利用を防止する。

（8）当システムを正しく利用させるため、作業手順書の整備を行い利用者の教育等を行う。

（9）当システムの安全管理の見直し及び改善の基礎として、運用責任者に当システムの運用状況を報告する。

（１０）システム管理統括責任者は、当システムの取扱い利用についてマニュアルを整備し、運用責任者及びシステム管理施設責任者に通知し、利用者が常に利用可能な状態に置くものとする。

2.1.2.3 （個人情報取扱統括責任者の責務）

個人情報取扱責任者は、本規約に基づき次の各号に掲げる責務を負う。

（1）個人情報取扱統括責任者は、各利用施設の個人情報取扱施設責任者と協力しながら、当法人の個人情報保護体制を構築・運用する。

（2）個人情報取扱統括責任者は、個人情報保護の運用状況に関して定期的な確認を行い、常に最良の状態を維持する。

（3）個人情報取扱統括責任者は、必要に応じて個人情報保護体制の見直しを行う。

2.1.2.4 （監査責任者の責務）

監査責任者は、本規約に基づき次の各号に掲げる責務を負う。

（1）監査責任者は、監査計画を立案し、監査を指揮し、監査報告書を作成し、運用責任者に報告する。

（2）監査責任者は、当システムの監査を円滑に実施するため、情報システムに関する監査を担当

する監査員を置くことができる。

（3）監査員の選定及び監査の実施においては、監査の客観性及び公平性を確保する。

2.1.2.5　（システム管理担当者の設置）

システム管理統括責任者は、作業を代行する担当者として、システム管理担当者を設置できる。

2　システム管理統括責任者は、システム管理担当者に対し当システムの運用管理に必要な教育を実施する。

3　システム管理担当者は、システム管理統括責任者の指示に基づき、必要な作業を実施する。

2.1.2.6　（システム管理施設責任者の責務）

システム管理施設責任者は、本規約に基づき次の各号に掲げる責務を負う。

（1）システム管理施設責任者は自施設における当システムの運用管理に責任を持つ。

（2）システム管理施設責任者は当システムの利用者及び利用端末の届け出及び利用端末の所在管理を行うこととし、人事異動や退職等による利用者の変更も併せて管理する。

（3）システム管理施設責任者はシステム管理統括責任者からの通知を遅滞なく自施設の利用者へ通知し、利用マニュアルを自施設の利用者が常に利用可能な状態に置くものとする。

（4）当システムの脆弱性や情報セキュリティのインシデント及びアクシデントについて、どのようなものでも記録し、速やかにシステム管理統括責任者に報告する。

2.1.2.7　（個人情報取扱施設責任者の責務）

個人情報取扱施設責任者は、本規約に基づき次の各号に掲げる責務を負う。

（1）個人情報取扱施設責任者は、各部門の責任者と協力しながら、施設内の個人情報保護体制を構築・運用する。

（2）個人情報取扱統括責任者は、施設内の個人情報保護の運用状況に関して定期的な確認を行い、常に最良の状態を維持する。

（3）当システムの個人情報取扱のインシデント、及びアクシデントについて、どのようなものでも記録し、速やかに個人情報取扱統括責任者に報告する。

2.1.2.8　（利用施設におけるシステム管理施設担当者の設置）

システム管理施設責任者は、システム管理統括責任者の許諾を得て、作業を代行する担当者として、システム管理施設担当者を設置できる。

2　システム管理施設責任者は、システム管理統括責任者の指導の下、システム管理施設担当者に対し当システムの運用管理に必要な教育を実施する。

3　システム管理施設担当者は、システム管理施設責任者の指示に基づき、必要な作業を実施する。

4　システム管理施設責任者は、必要作業の実施終了後にシステム管理統括責任者にその内容を報告する。

2.1.2.9　（利用者の責務）

利用者は、本規約に基づき次の各号に掲げる責務を負う。

（1）利用者は、当システムの参照や入力（以下「アクセス」という。）に際して、ID 番号やパスワード等によって、システムに自身を認識させる。

（2）利用者は、自身の ID 番号やパスワードを管理し、これを他者に利用させない。
（3）利用者が、正当な ID 番号及びパスワード等の管理を行わないために生じた事故や障害に対しては、その利用者が責任を負う。
（4）利用者は、情報システムへ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。
（5）利用者は、与えられたアクセス権限を越えた操作を行わない。
（6）利用者は、情報システム及び参照した情報を、目的外に利用しない。
（7）利用者は、患者等のプライバシーを尊重し、職務上知ることが必要な情報以外の情報にアクセスしてはならない。
（8）利用者は、法令上の守秘義務の有無に関わらず、アクセスにより知り得た情報を目的外に利用し、又は正当な理由なしに漏らしてはならない。異動、退職等により職務を離れた場合においても同様である。
（9）利用者は、システムの異常を発見した場合、速やかに自施設のシステム管理施設責任者に連絡し、その指示に従う。
（１０）利用者は、不正アクセスを発見した場合、速やかに自施設のシステム管理施設責任者に連絡し、その指示に従う。
（１１）利用者は、離席の際などを考慮し、ログアウトまたはスクリーンロック等の情報漏えい対策を実施する。持ち運び端末に関しては、これに加え持ち運ぶ際は画面を覆うカバーを付ける等の対策を行い、情報漏えい対策を実施する。
（１２）ウイルスに感染又はその恐れを発見した場合は、ネットワークから端末を切り離すとともに、自施設のシステム管理施設責任者へ連絡し、指示に従って必要な対応を実施する。
（１３）当システム利用に際して発生したインシデント、アクシデントについて、どのようなものでも記録し、速やかに自施設のシステム管理施設責任者に報告する。
（１４）個人情報取扱において発生したインシデント、アクシデントについて、どのようなものでも記録し、速やかに自施設の個人情報取扱施設責任者に報告する。
（１５）利用者は、年 1 回以上、研修を受講しなければならない。

2.1.3　システム管理における管理事項

2.1.3.1　（利用者の登録・認証）

利用者の ID 番号及びパスワード等の登録・認証は次の各号に基づいて行うこととする。
（1）利用者のユーザ認証は、ID 番号とパスワードを用いることを基本とする。
（2）ID 番号の付与は原則個人単位とし、複数人で共有することはない。
（3）パスワードは 8 文字以上の英数文字を組み合わせたものとする。
（4）利用者ごとに、アカウント取得の申請書を利用施設の長から当法人の理事長へ提出する。
（5）アカウント取得の申請書をシステムヘルプデスク（事務局）で受付する。
（6）システム管理統括責任者は、アカウント取得の申請を受理し、確認の上、アカウント発行を承認する。
（7）システムヘルプデスク（事務局）が ID 番号を発行する。

（8）システム管理施設責任者は、利用施設に属する職員等の採用時、異動時及び退職時に合わせ、各利用施設の長から書面による申請を受けた際に、速やかに利用者の登録、変更及び削除の措置を講じる。

（9）利用者の登録処理時はシステムにより発行された初期値のパスワードとし、その後速やかに利用者が個々のパスワードへ変更する手順とする。また、システム管理統括責任者又はシステム管理施設責任者であってもパスワードを確認できない仕組みとする。

（１０）パスワードの有効期限は、原則２ヶ月以内とし、利用者が更新する。

（１１）利用者が、パスワードを紛失し、当システムの利用ができなくなった場合は、システム管理統括責任者へパスワードの初期化依頼を提出する。

（１２）システム管理統括責任者は、利用者からのパスワード紛失の申請書を受け、ユーザ登録の確認後、パスワードの初期化を行ない、利用者へ知らせることとする。この場合、利用者は、速やかにパスワードを変更することとする。

（１３）利用者 ID には原則として管理者権限は付与しない。

2.1.3.2　（利用者の資格）

当システムの利用者は、年１回以上、当システムの研修を修了している者でなければならない。また、アカウント取得の申請時において、研修を修了していなければならない。

２　当システムの利用者は、以下の各号いずれかを満たす者でなければならない。

（1）利用施設に所属する医師又は歯科医師

（2）別表に定める医療職、介護職の有資格者のうち、所属する利用施設の長からの推薦があった者

（3）システム管理統括責任者又はシステム管理施設責任者

（4）システム管理統括責任者又はシステム管理施設責任者から、システム管理の実務作業を代行するシステム管理担当者として推薦があった者

（5）個人情報取扱統括責任者又は個人情報取扱施設責任者

2.1.3.3　（利用者の資格喪失）

当システムの利用者の資格を喪失した場合、システム管理統括責任者は、当該利用者のアカウントの凍結処理を実施するとともに、利用者の資格喪失について通知する。また、利用者の資格を喪失したものは、利用者の資格を得るために必要な措置を講じることでアカウントの凍結処理の解除を受けることができる。

２　システム管理施設責任者は、必要な措置を講じたことを確認し、アカウントの凍結処理の解除をシステム管理統括責任者へ申請する。

３　システム管理統括責任者は、システム管理施設責任者からの申請を受け、必要な措置が講じられたことを確認し、アカウントの凍結処理の解除を実施する。

2.1.3.4　（利用者の資格永久停止）

利用者が以下の各号の何れかに該当する場合、運用責任者は利用者の資格を永久停止し、システム管理統括責任者がそのアカウントの利用停止処理を実施することができる。

（1）本規約に違反し、違反が意図的であると認定された場合

（2）システム管理統括責任者又はシステム管理施設責任者の指示に違反し、違反が意図的である

と認定された場合

（3）教育又はシステム管理統括責任者及びシステム管理施設責任者からの指導を受けても、違反再発を防止できないと認定された場合

（4）その他、当システム又は当法人に意図的に損害を与えようとしたと認定された場合

2　違反、及び意図等の認定は、システム管理委員会にて違反事実を確認し、理事会で意図等の認定を行う。

3　利用者の資格永久停止は個人への処置とし、当該個人の人事異動や退職等があっても継続する。

2.1.3.5　（入退室管理）

参加同意書等の個人情報が記載された原本の保管場所については常時施錠し、入退室者については名簿に記録を残すものとする。

2　入退室の記録の内容は、定期的にチェックを行うものとする。

3　入退室管理について、利用施設が求める内容に対して不足がある場合、必要な措置を個人情報保護委員会又はシステム管理委員会で協議すること。

2.1.3.6　（アクセス管理）

システム管理統括責任者は、職務や担当業務等に定められた権限によるアクセス範囲を定め、必要に応じてアクセス権限の設定を行うものとする。

2　当システムの利用者の資格・職種に応じて参照できる項目を制限する。

3　自施設に受診歴のない患者又は受診予約のない患者の医療等の情報は、原則参照できない。ただし以下の各号に該当する緊急時の場合はこの限りでない。

（1）　救急医療の場合

（2）　災害時の場合

（3）　その他緊急時に該当すると認められた場合

4　職務や担当業務等に定められた権限によるアクセス範囲は、別途一覧表で定める。

5　システム管理統括責任者は、アクセス権限の設定に関して実際に設定する作業に関する役割も含めてたマニュアルを整備すること。

6　システム管理統括責任者は、アクセス権限に沿ってアクセス状況の確認を行い、監査責任者に報告をしなければならない。

7　アクセス範囲について、利用施設が求める内容に対して不足がある場合、アクセス範囲の定めを個人情報保護委員会又はシステム管理委員会で協議すること。

2.1.3.7　（個人情報を含む記録媒体の管理）その作業の記録を

保管及びバックアップの作業に当たる者は、既定の手順に従って行い、その作業の記録を残し、システム管理統括責任者の承認を得なければならない。

2.1.3.8　（個人情報を含む記録媒体の廃棄管理）

個人情報を記した媒体の廃棄にあたっては、安全かつ確実に行われることを、システム管理統括責任者が作業前後に確認し、結果を記録に残すものとする。

2.1.3.9　（リスクに対する予防と発生時の対応）

システム管理統括責任者は、業務上において情報漏洩等のリスクが予想されるものに対し、

本規約の見直しを行うものとする。

2　システム管理統括責任者は、事故発生に対しては、直ちに運用責任者に報告し利用者に周知しなければならない。

2.1.4　業務委託の安全管理措置

2.1.4.1　（業務委託の安全管理措置）

当法人の社員若しくは職員又は利用施設に所属する職員以外に業務を委託する場合は、守秘事項を含む業務委託契約を結ぶものとする。

2　個人情報保護取扱統括責任者は、委託作業内容が個人情報保護の観点から適正かつ安全に行われていることを確認しなければならない。

3　業務委託の契約書には、個人情報の保護水準を担保する事項を規定することとする。

4　個人情報の取り扱いを委託する場合、委託契約において安全管理に関する条項を含めること。

5　業務委託事業者と守秘義務契約を締結し、これを遵守させること。

6　システム管理統括責任者は、業務委託先における作業の作業者及び作業内容について報告を求め、適切であることを確認し、必要と認めた場合は、適時監査を行うものとする。

7　業務委託事業者の作業者が、医療等の情報の要配慮個人情報にアクセスする場合は、罰則のある就業規則等で裏付けられた守秘契約等の秘密保持の対策を行うこと。

8　当法人が医療等の情報の外部保存を委託する場合、外部保存業務を受託する業務委託事業者（以下、「外部保存受託事業者」という。）と、その管理者や電子保存作業を実施する作業者等に対する守秘に関連した事項や、これに違反した場合のペナルティも含めた委託契約を取り交わし、外部保存した医療等の情報の取扱いについて監督する。

9　外部保存受託事業者と契約の際には、ガイドラインを遵守することを明確に定める。

１０　外部保存受託事業者は、外部保存した医療等の情報の分析、解析等を実施してはならない。また、医療等の情報を当法人の許可なく匿名化してはならない。これらの事項を委託契約に明記する。

１１　外部保存された医療等の情報を、外部保存受託事業者が独自に提供しないように、委託契約に明記する。また、外部保存受託事業者が医療等の情報の提供に係るアクセス権の設定作業を実施する場合は、適切なアクセス権を設計し、情報漏えいや、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った提供が起こらないようにさせること。

2.1.5　情報機器及び情報機器の管理

2.1.5.1　（情報機器の管理及び持ち出し）

システム管理統括責任者は、当システムに関わる情報機器の管理及び持出しに関してリスク分析を行い、対象となる情報機器をシステム管理施設責任者及び利用者に公開することとする。

2　システム管理施設責任者は、情報が格納された可搬媒体及び情報機器の所在について台帳に記録し、その内容を定期的にチェックし、所在状況を把握しなければならない。

3　情報を持ち出す場合は、申請書を利用者がシステム管理施設責任者に届け出て、承認を得なけ

ればならない。

4　持ち出す情報ききは、以下の取り扱うものとする。

（1）情報機器にはパスワードを設定すること。

（2）パスワードは、推定しやすいものを避け、また定期的に変更すること。

（3）情報機器について、ウイルス対策ソフトをインストールしておくこと。

（4）情報機器には、許可無くアプリケーションソフトをインストールしないこと。

5　持ち出す情報機器の盗難及び紛失時には、直ちにシステム管理施設責任者に届け出なければならない。届け出を受け付けたシステム管理施設責任者は、その情報と情報機器の重要度に従って対応する。

6　システム管理施設責任者は、利用者に対し、情報機器の管理及び持ち出しについて教育又は周知を行うものとする。

7　利用者以外に当システムの情報機器を貸与又は譲渡する場合には、情報機器内部の阿波あいネットにかかわる情報全てを消去することとする。

2.1.5.2　（モバイル端末の管理及び持出し）

モバイル端末を、患者の診療目的以外で自施設外に持ち出すことは原則禁止する。

2　診療目的でモバイル端末を持ち出す際には、当該端末の有するモバイル通信網を使用する。

3　当該端末の有するモバイル通信網が電波圏外又は電波が微弱で運用に耐えない通信状況において、以下の各号に掲げる要件を満たす場合、モバイル端末の持出しを許可する。

（1）専用アプリケーションを用いる以外にアクセス不可能とすること。

（2）専用アプリケーションのログインには、利用者のアカウントによる認証を必要とすること。

（3）専用アプリケーションは、無操作の時間が一定時間経過すると、再度認証を求めること。

（4）持ち出し端末内に保存される医療等の情報を暗号化すること

（5）通信が再開され、持ち出し端末内に医療等の情報を保存する必要がなくなった場合、保存されている医療・介護情報を削除すること。

（6）持ち出し端末紛失時に備え、遠隔操作で端末ロック及び保存されている医療等の情報の削除又は破壊ができること。

2.1.5.3　（情報機器の共同利用）

当システムに関わる情報機器を、利用者以外の者と共同利用する場合は、システム管理施設責任者は該当する情報機器を把握し、管理しなければならない。

2　利用者は、当システムに関わる情報機器を、利用者以外の者と共同利用する場合、システム管理施設責任者へ届け出て、承認を得なければならない。

2.1.5.4　（情報の管理及び持ち出し）

当システムの医療等の情報を当システム以外の情報機器又は可搬媒体に保存し持ち出すことを原則禁止する。

2　診療、看護及び介護等の実務のために必要な医療等の情報を、利用施設の診療録等に引用することは情報の持出しに含まないものとする。

2.1.6 外部システムと接続する場合の措置

2.1.6.1 （利用施設が運用するシステムとの接続）

当システムと、利用施設が運用する電子カルテシステム及び医事会計システム等のシステムをネットワークで接続し、医療等の情報の収集を行う場合は、基本方針において定める必要な情報セキュリティ対策を講じる。

2 必要な情報セキュリティ対策を講じるにあたって、全利用施設で一定以上のセキュリティレベルを担保するため、基本方針を別途定める。また、各利用施設の情報セキュリティ対策の具体的な実装は、基本方針に従う。

3 基本方針を定めるにあたって、システム管理統括責任者は、想定される利用施設が運用するシステムと、ネットワークで接続するセキュリティリスクについて、リスク分析を行い、技術的及び運用上の対策を設計すること。

4 システム管理統括責任者は、利用施設が運用するシステムとの接続について設計されたネットワーク構成図、機器設定諸元等を確認し、基本方針に従っているか確認すること。また、確認結果についてシステム管理委員会において報告するとともに、当該利用施設のシステム管理施設責任者へ通知すること。

5 システム管理施設責任者は、システム管理統括責任者から通知されたネットワーク構成図、機器設定諸元等を確認、保管すること。また、情報セキュリティに関する規則等を利用施設が有する場合は、これに適合していることを確認し、システム管理統括責任者へ報告すること。

6 システム管理施設責任者は、利用施設が運用する電子カルテシステム、医事会計システム等のシステム、及びネットワークに変更が生じた場合、変更点を速やかにシステム管理統括責任者へ報告し、システム管理統括責任者と協働し影響について評価、基本方針の遵守に必要な対策を講じること。

7 システム管理施設責任者は、利用施設が定める情報セキュリティに関する規則等に変更が生じた場合、変更点を速やかにシステム管理統括責任者へ報告するとともに、対応のために必要な措置を講じること。

2.1.6.2 （外部機関が運用するシステムとの接続）

当システムと、外注検査会社が運用する検査システム等の外部機関が運用するシステムをネットワークで接続し、医療等の情報の収集を行う場合は、基本方針において定める必要な情報セキュリティ対策を講じる。

2 外部機関からネットワークを通じて医療等の情報を収集する場合、外部機関との間で、責任分界点や責任の所在を明確にするものとする。

3 必要な情報セキュリティ対策を講じるにあたって、全外部機関との接続において一定以上のセキュリティレベルを担保するため、基本方針を別途定める。また、各外部機関との接続における情報セキュリティ対策の具体的な実装は、基本方針に従う。

4 基本方針を定めるにあたって、システム管理統括責任者は、想定される外部機関が運用するシステムと、ネットワークで接続するセキュリティリスクについて、リスク分析を行い、技術的及び運用上の対策を設計すること。

5 システム管理統括責任者は、外部機関が運用するシステムとの接続について設計されたネット

ワーク構成図、機器設定諸元等を確認し、基本方針に従っているか確認すること。また、確認結果についてシステム管理委員会において報告する。

2.1.6.3 （運用保守サービス事業者との接続）

リモートメンテナンス及び運用保守における監視を目的として、当システムと運用保守サービス事業者間をネットワークで接続する場合は、基本方針において定める必要な情報セキュリティ対策を講じる。

2 システム管理統括責任者は、運用保守サービス事業者からリモートメンテナンスを受ける場合、運用保守サービス事業者、及び使用する回線の通信事業者との間で、責任分界点や責任の所在を明確にするものとする。

3 必要な情報セキュリティ対策を講じるにあたって、運用保守サービス事業者との接続において一定以上のセキュリティレベルを担保するため、基本方針を別途定める。また、各運用保守サービス事業者との接続における情報セキュリティ対策の具体的な実装は、基本方針に従う。

4 基本方針を定めるにあたって、システム管理統括責任者は、想定される運用保守サービス事業者とネットワークで接続するセキュリティリスクについて、リスク分析を行い、技術的及び運用上の対策を設計すること。

5 リモートメンテナンスによるシステムの改造や保守が行われた場合には、必ずアクセスログを収集するとともに、当該作業結果をシステム管理統括責任者、及び当該作業の対象となったシステム管理施設責任者が確認すること。

6 システム管理統括責任者は上記の契約状態が適切に維持管理されているか、定期的に監査を行なって確認しなければならない。

7 システム管理統括責任者は、外部からアクセスする情報機器については許可した物に限定し、その情報機器が許可された際の状態を保持していることを定期的に確認しなければならない。

2.1.7 災害等の非常時の対策

2.1.7.1 （災害等の非常時対策）

バックアップ施設は自然災害の影響を同時に受けないよう、徳島県から十分離れた地点に構築すること。

2 バックアップ施設に対しては、物理的安全対策がなされていることを確認すること。

（1）建物に関する安全対策

（2）入退館、入退室等に関する安全対策

（3）情報処理装置のセキュリティに関する安全対策

（4）情報処理装置の廃棄及び再利用に関する安全対策

（5）情報処理装置の外部への持ち出しに関する安全対策

3 見読性の要求から、医療等の情報について当システムとバックアップ施設の間で同期を取ること。

4 同期をとるための回線は、基本方針において定める必要な情報セキュリティ対策を講じること。

5 バックアップ施設及びバックアップ装置は、当システムが委託するバックアップ事業者が自ら

管理することを原則とする。なお、緊急時の対応が遅れる等の事態を避けるため、パックアップ事業者が緊急時対応を再委託する場合には、再委託先事業者の安全管理基準を事務局に通知し、承認を受けること。

6　バックアップ施設におけるサービス等については、事前に当ネットに説明し、承認を得ること。

7　災害、サイバー攻撃などによりサービス提供体制に支障が発生する非常時の運用は、以下の通りとする。

（1）システム管理統括責任者は、発災後速やかにシステムの被害状況を確認し、被災状況及び復旧見込みを運用責任者に報告、利用施設へ周知する。

（2）運用保守サービス事業者による被害状況確認後、システムの切替・復旧作業を行う。

2.1.8　教育及び研修

2.1.8.1　（教育及び研修会）

システム管理統括責任者は、システム管理施設責任者と利用者に対し、定期的に当システムの利用、情報セキュリティ及び個人情報保護に関する教育又は周知を行うものとする。

2　システム管理施設責任者はシステム管理統括責任者と協働し、自施設の利用者に対し定期的に当システムの利用、情報セキュリティ及び個人情報保護に関する教育又は周知を行うものとする。

3　システム統括管理責任者とシステム管理施設責任者は、利用者の資格を得るために必要な教育を実施する研修会を協働して開催する。

4　研修会における教育内容は、システム統括管理責任者が別途定める。

5　システム統括管理責任者は、研修会において教育を実施する教育実施者を認定し、その実務を代行させることができる。

6　当システムの利用者は、システム統括管理責任者又はシステム管理施設責任者の開催する研修会を年1回以上受講し、当システムの利用資格を維持するものとする。

7　個人情報保護に関する教育に関しては、個人情報取扱施設責任者の認める個人情報研修会等が自施設で開催される場合、利用者は研修を受講したものとする。

8　利用者は、利用施設在職中のみならず、退職後においても当システムを利用することで知った個人情報及び情報セキュリティに関する情報について守秘義務を負うものとする。

2.1.9　監査

2.1.9.1　（監査）

監査責任者は、当システムが不正な改ざんを受けていないことの検証、本規約への準拠状況の検証、及びシステム構成やソフトウェアの動作状況の検証のため、定期的に監査を実施する。

2　アクセスログは最低 3 年以上保存すること。また、保存期間が 3 年を超えた場合、システム統括管理責任者が運用状況を踏まえ、これを廃棄することができる。10 年を超えた場合は全て廃棄する。

3　システム管理統括責任者は毎月 1 回以上アクセスログを分析し、不審なアクセスの有無について確認すること。

4　システム管理統括責任者はアクセスログの分析結果を監査責任者、及びシステム管理施設責任

者へ提供すること。

5　システム管理施設責任者はアクセスログの分析結果を確認し、把握する自施設の運用状況と照らし合わせ、不審なアクセスの有無について確認すること。また、不審なアクセスを確認した場合は直ちにシステム管理統括責任者へ報告すること。

6　システム管理統括責任者、及びシステム管理施設責任者は、監査責任者の求めに応じ監査に必要な記録の提出、及び調査を行うこと。また、利用者本人への確認が必要な事項が生じた場合、これにシステム管理施設責任者は協力すること。

7　監査責任者は、監査結果を事業管理者へ報告すること。事業管理者は、監査結果を確認し、監査結果を運用責任者へ通知するとともに、問題点等の指摘がある場合、必要な措置を命じることができる。

8　運用責任者は、事業管理者からの監査結果の通知を受け、問題点の指摘等がある場合は、直ちに必要な措置を講じること。

9　監査の内容については、監査責任者が計画を立案し、事業責任者が承認する。

１０　監査結果及び記録等を利用施設に開示する情報の範囲・条件等については監査責任者が定める。

１１　事業管理者は必要な場合、計画に定める監査の他、臨時の監査を監査責任者に命ずることができる。

2.2　情報保存に関するシステムの運用管理

2.2.1　電子保存におけるシステムの運用管理

2.2.1.1　（相互運用性の確保）

システム管理統括責任者は、情報機器やソフトウェアを変更した場合に、電子保存された情報が継続的に使用できるよう維持する。

2.2.1.2　（スキャナ読み取り書類の運用）

スキャナにより電子保存する対象文書は以下の通りとする。

（1）患者や利用施設以外の施設から持ち込まれた文書等（例：検査結果、診療録）

（2）患者や医師の署名・記載が必要な文書等（例：同意書、問診票）

（3）やむ得ない事情で生じる紙媒体文書等（例：システムダウン時の診療記録等）

2　スキャナにより電子保存された医療等の情報の管理は各施設の責とするが、必要に応じて以下の対策をとることができる。

（1）スキャナ（スキャナ機能を有す複合機を含む）設置部署においては、スキャナ読み取りを円滑に運用するため、スキャナ読み取り電子情報と原本との同一性を担保する情報作成管理者（以下、「作成管理者」という。）を置く。

（2）作成管理者は、システム管理施設責任者が指名する。

（3）作成管理者は、スキャン読み取りの運用について職員を指導し、監督する責任を有し、適正な手続きで確実に運用が実施される措置を講じる。

3　スキャン業務の運用は以下の通りとする。

（1）改ざんを防止するため、情報が作成されてから又は情報を入手してから一定期間以内にスキ

ャナによる読み取り作業を行う。

（2）作業における個人情報の適切な保護を図るため、スキャンする体制は複数で執り行う等、作業実施・終了後の監査を確保する。

（3）スキャン等を行う前に、対象文書に他の文書を重ねて貼り付けない、電子化可能な範囲外に情報が存在する等、スキャンによる電子化で情報が欠落することがないことを確認する。

4　システム管理施設責任者は、適宜業務において本規約どおりの運用がなされていることを確認するものとする。

2.2.2　可搬媒体を用いて外部保存を行う場合における運用管理

2.2.2.1　（可搬媒体が搬送される際の個人情報の保護）

運用保守や監査等において可搬媒体を用いて個人情報を搬送する必要性が生じた場合、システム管理統括責任者は次の各号に掲げる措置が取られることを確認すること。

（1）可搬媒体の紛失防止措置

（2）可搬媒体と他の搬送物との混合の防止措置

（3）搬送時の個人情報漏洩等の守秘義務の遵守

2.2.2.2　（可搬媒体が外部保存される際の個人情報の保護）

運用保守や監査等において可搬媒体を用いて個人情報を外部保存する必要性が生じた場合、システム管理統括責任者は次の各号に掲げる措置が取られることを確認すること。

（1）外部保存の受託業者の管理者であっても正当な理由なく可搬媒体内の医療等の情報へアクセスすることの禁止

（2）外部保存している可搬媒体に障害が発生した場合で、やむを得ず可搬媒体に保存されている個人情報にアクセスする場合の通知と許可

（3）外部保存の受託業者、及び可搬媒体を搬送する搬送業者との責任分界点の明確化と守秘義務の遵守

（4）外部保存の受託業者、及び可搬媒体を搬送する搬送業における個人情報保護対策の実施状況の監査

2.2.2.3　（可搬媒体が外部保存される際の事後責任の明確化）

運用保守や監査等において可搬媒体を用いて個人情報を外部保存する必要性が生じた場合、システム管理統括責任者は次の各号に掲げる管理体制、及び責任体制に関する事項を契約上明記するものとする。

（1）可搬媒体を受託業者に授受するタイミングと外部保存に関連する一連の操作

（2）当法人と搬送業者との間で可搬媒体を授受する方法及び管理方法

（3）事故等で可搬媒体の搬送に支障が生じた場合の対処法

（4）搬送中に情報漏洩があった場合の対処方法

（5）搬送業者と外部保存の受託業者との間で可搬媒体を授受する方法及び管理方法

（6）受託機関が当法人の求めに応じて可搬媒体を返送することができなくなった場合の対処方法

2.2.3 外部保存を行う場合全般における運用管理

2.2.3.1 （通常運用における責任の明確化）

運用責任者は、外部保存を行なっていることを参加同意者へ周知するものとする。

2 システム管理統括責任者、及びシステム管理施設責任者は、可搬媒体への記録、保存等に用いる装置の運用及び管理を適正に行うものとする。

3 システム管理統括責任者は、外部保存の運用管理状況を定期的に監査するものとする。

2.2.3.2 （外部保存終了時の処理）

外部保存終了時のデータ返却処理又はデータ消去方法について、当法人と外部保存の受託業者間の契約に明記するものとする。

2.3 雑則

2.3.1 その他

2.3.1.1 （開発・実験目的での医療等の情報の利用）

システム開発、新規導入検証等において、当システムの医療等の情報を直接利用しない。個人が特定できる情報の消去、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他のデータと入れ替える等のデータ操作をしたテストデータを作成し、これを用いることとする。

2.3.1.2 （再委託）

再委託が行われる場合は、再委託する事業者にも再委託元の事業者の責任で同等の義務を課すこと。

3 委託事業者に求める規約

3.1 一般管理における運用管理

3.1.1 管理体制

3.1.1.1 （管理体制）

委託業者（以下「事業者」という）において、情報システム運用責任者が明確に定められていること。

2 当法人の体制に対応した事業者の体制を定めること。

3 当法人、及び利用施設と利用者からの問い合わせ窓口を設けること。また、問い合わせ受付の時間帯等を定めること。

3.1.1.2 （運用管理規程）

事業者が定める情報機器の管理等の運用管理の規程、及び個人情報保護を記録した媒体の規程等は、当法人が求める内容を含むものとし、不足があれば事業者がとるべき対応について定めること。

2 各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、本運用管理規程に則り正しく確実に実施されるよう、定期的にレビュー及び見直しを行う。

3 遵守すべきガイドラインの範囲及びこれを遵守している旨の報告につき、その内容・範囲等を定めること。

3.1.2 事業者の責務

3.1.2.1 （事業者の責務）

当法人と施設において発生する参加同意者等に対する説明責任、管理責任等、各種責任に関し、事業者が負う責任の範囲、役割等について定めること。

2 サービスを提供する際に用いる回線の管理責任、品質等に対する事業者の責任の範囲、役割等について定めること。

3.1.3 情報セキュリティ方針

3.1.3.1 （情報セキュリティ組織運営）

事業者は情報セキュリティに関する組織的取組についての基本的な方針を定めた文書を作成することとする。また、当該文書には経営陣が承認の署名を行い、情報セキュリティに関する経営陣の責任が明確になされていること。

2 上記文書は定期的にサービス提供に係る重大な変更が生じた場合には見直しを行うこと。この見直しの結果、変更の必要性が生じた場合は、経営陣の承認の下で改定等を実施すること。

3 事業者の経営陣は情報セキュリティに関する取組についての責任と関与を明示し、人員・資産・予算の面での積極的な支援・支持を行う。

4 事業者の従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は定期的又はサービス提供に係る重大な変更が生じた場合に見直しを行う。

5 雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。

6 全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・研修を実施すること。

7 従業員が情報セキュリティポリシー又はサービス提供上の契約に違反した場合の対応手順を備えること。

8 全ての従業員に対し、業務において発見あるいは疑いを持った情報システムの脆弱性や情報セキュリティインシデントについて、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるような手続きを定め、実施を要求すること。

3.1.3.2 （情報セキュリティ基本方針）

情報セキュリティ対策における具体的な実施基準や手順等を明文化し、文書化すること。当該文書は定期的又はサービス提供に係る重大な変更が生じた場合に見直しを行う。

2 事業者が定める情報セキュリティ基本方針に基づいて委託業務を実施すること。

3 事業者が定める情報セキュリティ基本方針は、当法人が求める内容を含むものとし、不足があれば事業者がとるべき対応について定めること。

4 事業者が提供するサービスの利用に際して、利用施設が無線 LAN を利用する場合は、次の各号に準拠してセキュリティ対策を行うこと。また、事業者の役割と責任の範囲を定めること。

（1）利用者以外に無線 LAN の利用を特定されないようにすること。例えば、ステルスモード、ANY 接続拒否等の対策を行うこと。

（2）不正アクセスの対策を施すこと。少なくとも SSID や MAC アドレスによるアクセス制限を

行うこと。

（3） 不正な情報の取得を防止すること。例えば WPA2/AES 等により、通信を暗号化し情報を保護すること。

（4） 電波を発する情報機器（携帯ゲーム機等）によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合には留意すること。

5 サービス提供に際して、当法人と守秘義務契約を締結すること。

6 守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わすこと。

7 事業者で講じるネットワークの安全対策が、当法人が求めるネットワーク回線の安全性に関する規準を満たしていること。また、当法人の求めに応じて資料を提出すること。

8 個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を講じること。

3.1.3.3 （情報セキュリティ要求事項）

委託事業者は、次の各号に掲げる情報セキュリティ要求事項について対策を講じること。また、これらの対策における事業者の役割の範囲を定めること。

（1）ネットワーク構成図を作成すること。

（2）利用者及び管理者等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。なお、認証方法の詳細については別紙にて定めることとする。

（3）外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。

（4）不正な通過パケットを自動的に発見又は遮断する措置（IDS/IPS の導入等）を講じること。

（5）外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。なお、情報交換の実施基準・手順等の詳細については別紙にて定めることとする。

（6）外部ネットワークを利用した情報交換において、又はクラウドサービスにおいて送受信されるデータに対して、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、電子政府推奨の暗号を用いた通信の暗号化を行うこと。

（7）暗号化によるセキュリティ対策が当法人が求める水準であることを確認し、不足があれば事業者がとるべき対応を追加すること。

（8）第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。

（9）医療機関等がクラウドサービスを利用するネットワークにつき、ウイルスや不正なメッセージの混入等による改ざんに対する防止措置についての事業者の役割の範囲を定めること。

（１０）利用者及び管理者（情報システム管理者、ネットワーク管理者等）等 のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。

（１２）クラウドサービスを利用するネットワークで用いられる利用施設の送受信の拠点の出入

り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、利用施設から事業者までの確認を行うこと。

（１３）クラウドサービスを利用するネットワークで用いられるルータ等のネットワーク機器がガイドラインで求める安全性が確認されているものであること、クラウドサービスを利用するネットワークで用いられる利用施設内のルータについて、これを経由して利用施設間を結ぶ VPN の間で送受信ができないように経路設定されていること等に関して、事業者の役割、範囲を定めること。

（１４）情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。

（１５）個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。

（１６）クラウドサービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び本規程が定める要求事項に従って、適切に管理すること。

（１７）利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。

（１８）通常運用時、緊急時の医療機関等と事業者との起点から終点までの通信手順を明確にし、事業者の負う責任の範囲、役割等を定めること。なお、通信手順及び責任分界点の詳細については別紙にて定めることとする。

（１９）利用施設の管理者において発生する患者等に対する説明責任、管理責任等、各種責任に関し、事業者が負う責任の範囲、役割等について定めること。

3.1.4 一般管理における運用管理事項

3.1.4.1 （情報の開示）

事業者が定める規程類は、その開示する範囲と条件等を定めること。

２　個人情報等の外部保存など患者等への説明及び同意を得る際に、事業者から提供される情報の種類、事業者の役割を定めること。

３　マニュアル等の文書管理に関して、開示できる文書等の範囲、事業者の役割等を定めること。

４　監査記録等に関して、開示できる文書等の範囲・条件等を定めること。

５　契約に先立ち、当法人の管理者から、選定に必要な情報の提供を求められた場合に、速やかに提出すること。

3.1.4.2 （情報の破棄）

事業者が定めた情報破棄手順は、当法人が求める内容を含むものとし、不足があれば事業者がとるべき対応を定めること。

２　情報の破棄を実施した場合に、報告の内容・範囲・提出すべき資料等を定めること。

３　電磁記録媒体の消磁、物理的破壊等、情報の削除方法を含む実施内容を、当法人に対して報告し、破棄記録等を提出する。

3.1.4.3 （個人情報保護指針）

事業者が定める個人情報保護指針に基づいて委託業務を実施すること。

2　個人情報保護法の対象外（死者に関する情報）等であっても、個人情報保護法における運用に準じて取扱い、当法人の求めに応じて資料を提出すること。

3　事業者が定める個人情報保護指針は、当法人が求める内容を含むものとし、不足があれば事業者がとるべき対応を追加すること。

4　事業者が定める個人情報を記録した媒体の運用管理の規程等は、当法人が求める内容を含むものとし、不足があれば事業者がとるべき対応を追加すること。

3.1.4.4　（認証方式）

採用する認証手段・方式について定めること。

2　事業者が定めるパスワードポリシーが、当法人が求める内容を含むものとし、不足があれば事業者がとるべき対応を追加すること。

3　利用者のパスワード発行等に関する手続き及び業務範囲を定めること。

4　事業者は、利用施設が採用する通信方式認証手段が妥当であることを確認することについて、事業者の役割と範囲を定めること。採用する認証手段については、容易に解読されない次の各号の方法を推奨する。

（1）PKI による認証

（2）Kerberos 等の鍵配布

（3）事前配布された共通鍵の利用

（4）ワンタイムパスワード

3.1.4.5　（入退室管理）

個人情報が保管されている主要機器の設置場所及び記録媒体の保管場所については常時施錠し、入退室者については名簿に記録を残すものとする。

2　入退室の記録の内容は、定期的にチェックを行うものとする。

3　入退室管理のルールは、当法人が求める内容を含むものとし、不足があれば事業者がとるべき対応について定めること。

3.1.4.6　（事業者内におけるアクセス管理）

事業者におけるアクセス管理は、職務や担当業務等に定められた権限によってデータアクセス範囲が定められていることとする

2　事業者が運用しているアクセス管理に関する規程類は、当法人が求める内容を含むものとし、不足があれば事業者がとるべき対応を定めること。

3.1.4.7　（提供サービスにおけるアクセス管理）

提供するサービスにおいて、利用施設等の利用者の職種、担当業務等に応じてアクセス制御が可能な機能を含めること。

2　利用施設等の利用者の職種等に応じたアクセス制御の設定に関しては、当法人の管理者と協議の上、実際に設定する作業に関する役割も含めて定めること。

3　当法人のアクセス管理に関する運用管理規程の内容に従った運用を行い、当法人の求めに応じて資料の提出を行う。

4　データアクセスの制限の方法を定めること。

3.1.4.8　（保守）

保守体制に変更が生じた場合に、当法人に行う報告の範囲、内容等を定めること。

2　サービス提供に必要な保守業務を行うに際して、当法人の管理者に対して、書面等により作業の事前及び事後に通知を行うこと。また、事前の了解を必要とする作業等を定めること。

3　サービス提供に必要なシステム保守をリモートメンテナンスで行う場合の、当法人に対する報告対象となるシステムの範囲、そのシステムに対するリモートメンテナンスの実施条件、報告内容、承認等を定めること。

4　サービス提供に必要な保守業務を利用施設内で行う際に、利用施設等の立会の下で実施する旨を定めること。

5　受託した医療情報を、保守作業に必要な範囲での閲覧を超えて閲覧しないこと。

6　許可されていない受託データの閲覧を禁止することにつき、その方法を含め定めること。

3.1.4.9　（リスクに対する予防と発生時の対応）

事業者が定めるリスク等に対する予防措置及び事故等の発生時の対応等が、当法人が求める内容を含むものとし、不足があれば事業者がとるべき対応を追加すること。

3.1.5　提供サービスにおける運用管理事項

3.1.5.1　（標準規格対応）

入出力するデータ項目の形式、及びデータの交換方法について、厚生労働省標準規格に採用された各標準規格を採用する。対象とするデータ項目又は交換方法に標準形式が存在しない場合は、妥当なデータ項目の形式又はデータ交換方法を提示すること。

2　データを保存する際に用いるデータ項目の形式又はデータ交換方法を変更する場合、変更前の方式との互換性を確保すること。

3.1.5.2　（データの更新）

入力された内容が記録の確定前に作成責任者によって確認できる仕様を確保すること。

2　更新管理の仕様を定めること。

3.1.5.3　（データの移行）

マスタテーブルの変更に際してのレコード管理方法・とるべき措置等について、移行に際して情報内容の変更が生じない機能及び検証方法を備えることとする。

3.1.5.4　（インターフェースの構築）

電子カルテシステム、臨床検査システム、医用画像ファイリングシステム等との連携におけるインターフェースの構築に関し、事業者の役割、責任の範囲、役割等を定めること。

3.1.5.5　（構成管理）

情報機器、ソフトウェア構成について定めること。

2　情報機器、ソフトウェア構成について文書化を行い、当法人の管理者に対して報告できる内容とすること。

3　システムの構成管理内容を示す資料の開示内容・範囲・条件について、当法人の管理者に対して報告できる内容とすること。

3.1.5.6　（サービスレベル）

見読性を保証するサービス仕様として次の各号を定めること。

（1）情報の所在管理

（2）見読化手段の管理

（3）見読目的に応じた応答時間

（4）システム障害対策としての冗長性の確保

2　障害等が生じた場合を想定し、冗長性を確保する仕様等を定めること。

3　サービス提供に用いる回線又は施設等のサービスレベル維持を満足するための更新計画を定めること。

3.1.5.7　（サービスの終了）

事業者の都合によりサービス提供を終了する場合の事前通知の方法、終了が認められる理由、及び終了に向けての対応を定めること。

2　サービスの提供を終了する場合に、受託しているデータ、及びこれに関連する資料の内容、範囲、条件等を定めること。

3　受託データを当法人に引き渡す際には、次の各号に従って定めること。

（1）厚生労働省標準規格への準拠

（2）学会や業界団体で定められた基本データセットや標準的な用語集、コードセットの利用

（3）データ交換のための国際的な標準規格への準拠

3.1.5.8　（教育と研修）

運用・操作に関する利用者教育における事業者の役割、範囲等を定めること。

3.1.6　情報及び情報機器の持ち出しについて

3.1.6.1　（情報及び情報機器の持ち出し）

事業者が定める情報及び情報機器の持出しに関する運用管理の規程が、当法人が求める内容を含むものとし、不足があれば事業者がとるべき対応を追加すること。

2　個人情報を含むデータ又は情報機器を事業者外に持ち出さなければならない場合には、当法人の管理者による監査の内容、範囲を定めること。

3　事業者が定めた情報機器又は可搬媒体の盗難、紛失が生じた際の対応についての手順等が、当法人が求める内容を含むものとし、不足があれば事業者がとるべき対応を追加すること。

4　受託した情報を可搬媒体により外部に持ち出し、受託情報の処理を行わない旨を、事業者が定める運用管理規程に含め、不足があれば事業者がとるべき対応を追加すること。

3.1.7　災害等の非常時の対策

3.1.7.1　（非常時対策）

事業者において定めた非常時における BCP 対策に関する運用手順等が、当法人が求める内容を含むものとし、不足があれば事業者がとるべき対応を追加すること。

2　事業者において定めた非常時におけるアクセス管理の対応方法の内容が、当法人が求める内容を含むものとし、不足があれば事業者がとるべき対応を追加すること。

3　バックアップの毀損箇所の確認に関する仕様、方法等を定めること。なお、仕様、方法の技術的詳細を含めること。

3.1.8 監査

3.1.8.1 （監査）

事業者において実施するシステム監査等が、当法人が求める内容を含むものとし、不足があれば事業者がとるべき対応を追加すること。

2 システム構成やソフトウェアの動作状況に関する内部監査について、事業者の役割、範囲等を定めること。

3 サービス提供に用いる情報システムが、本情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に点検・監査を行う。

3.2 雑則

3.2.1 その他

3.2.1.1 （開発・試験・研究目的での個人情報の利用）

受託した情報処理に必要なシステムに関する動作確認に際し、個人情報を含むデータを使用せず、テスト用のデータを使用すること。

2 システムに関する動作確認に際し、やむを得ず受託した個人情報を使用する場合には、当法人の管理者と十分な協議の上、必要な措置を講じて使用すること。

3 受託した医療情報は、匿名化されたものを含めて、当法人、及び利用施設との契約に基づくことなく、分析、解析等を実施しないこと。

4 当法人、及び利用施設との契約に基づくことなく、受託したデータの分析・解析等を実施しないことにつき、その方法等を含め定めること。

3.2.1.2 （再委託）

事業者が外部組織に対して再委託を行う場合には、事前に当法人の管理者に対して説明を行い、契約において体制を明確にすること。

2 外部組織においても、本規程の「情報セキュリティ要求事項」に示す事項を遵守すること。

4 附則

（平成 30 年 8 月 1 日制定）

本規程は、平成 30 年 8 月 1 日から施行する。

（令和 2 年 11 月 2 日改正）

本規程は、令和 2 年 11 月 2 日から施行する。