地域医療介護連携ネットワークシステム

「さくらネット協議会運用管理規程」

2024 年 6 月 13 日

一般社団法人　さくらネット協議会

第１章　一般管理における運用管理

第１節　総則

第１条（目的）

この規程は、一般社団法人さくらネット協議会（以下「協議会」という）において、地域医療介護連携ネットワークシステム（以下、「さくらネット」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、処方箋情報、放射線・内視鏡、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、適正な管理を図るための必要事項の定義を目的とする。

第２条（対象情報）

（１）対象システムは、協議会で運用する本ネットワークシステム及び本ネットワークに接続する参加機関等にて接続する機器や周辺装置など、医療・介護情報を取り扱うシステムをいう。

（２）管理対象となる情報は、本ネットワークシステムで取り扱う電子情報だけでなく、同システムへ入力する前の紙媒体の情報や全ての個人情報を適用対象とする。

（３）対象システムの扱う情報の定義、安全管理上の分類及びリスク分析を行い文書化しし維持する。

（４）将来、他地域における同種の「地域医療介護ネットワーク」と連携する場合には、これも対象システム及び対象情報として取扱い、（３）と同様に文書化し維持する。

第２節　管理体制

第４条（管理体制）

本ネットワークシステムの安全かつ合理的な運用を図るため、協議会を置く。協議会に関する事項は別に定める。

２　本ネットワークシステムを管理するため、次の各号に掲げる管理者等を置く。

（１）協議会にさくらネット運用責任者（以下、「運用責任者」という）および個人情報保護管理者を置き、理事長の指名をもってこれに充てる。

（２）さくらネットを円滑に運用するため、システムを担当する管理者（以下「システム管理者」という）及びネット管理責任者を置き、理事長の指名をもってこれに充てる。

第５条（マニュアル、契約書等の文書管理体制）

各種規程、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程による。

第６条（監査体制と監査責任者）

理事長は、情報システムを円滑に運用するため、公平、かつ、客観的な立場に

ある監査責任者を内部の者から指名し、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与え、業務を行わせる。

第７条（苦情及び質問等の受付体制）

協議会は、個人情報の取扱いや情報システムの運用に関して、本事業に参加する住民及び各参加施設等からの苦情や質問を受け付けるものとする。また、適切で迅速な対応を行う手順を確立し、これを維持する。

第８条（事故対策体制）

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文書化し、参加施設等に周知の上、常に利用可能な状態にする。

第９条（教育、訓練体制）

システム管理者は、本ネットワークシステムの取扱いについてシステム運用マニュアルを整備し、参加施設等に周知の上、常に利用可能な状態にする。

２　システム管理者は、本ネットワークシステムの参加施設等に対し、定期的に本ネットワークシステムの取扱い及び個人情報保護に関する研修又は周知等を行うものとする。

第３節　管理者及び利用者の責務

第１０条（運用責任者の責務）

運用責任者は、協議会運用管理規程に基づき次の各号に掲げる責務を負う。

（１）本ネットワーク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）本事業に参加する住民又は参加機関等からの本ネットワークシステムについての苦情を受け付ける窓口を設ける。

（３）監査責任者に監査を実施させ、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。

第１１条（システム管理者の責務）

システム管理者は、協議会運用管理規程に基づき次の各号に掲げる責務を負う。

（１）本ネットワークシステムに用いるハードウェア等の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。

（２）診療情報や健康情報の安全性を確保し、常に利用可能な状態に置いておく。

（３）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。

（４）本ネットワークシステムの利用者（参加施設等の所属員）の登録を、人事異動や退職等による利用者の変更等に併せて管理する。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。

（５）本ネットワーク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。

（6）本ネットワークシステムの安全管理の見直し及び改善の基礎として、運用責任者に本ネットワークシステムの運用状況を報告する。

（7）本ネットワークシステムに接続する機器について、BYOD デバイスからの利用者は原則禁止とする。事前に配布された、あるいは申請または通告されていない機器を接続することを防ぐ。さらに、機器の接続を規定し、不正な機器利用を防ぐ。

（8）やむを得ない事情があるとシステム管理者が判断した場合には、BYOD デバイス利用同意書を提出し、不正利用を防止した上での接続を認める。

（9）本ネットワークシステムの利用者の利用状況の確認として、不正アクセス監視を行う。不正アクセス監視の方法については、「不正アクセス監視手順」に従う。

第１２条（個人情報保護管理者の責務）

個人情報保護管理者は、協議会運用管理規程に基づき次の各号に掲げる責務を負う。

（1）個人情報保護管理者は、個人情報保護管理運用手順を策定、実施、維持し継続的改善を推進する。

（2）個人情報保護管理運用手順の見直し及び改善の基礎として、運用状況を協議会へ報告する。

（3）個人情報保護にかかわる教育計画と実施の責務を負う。教育の実施においては補佐する担当者を任命することができる。

第１３条（監査責任者の責務）

監査責任者は、協議会運用管理規程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、本ネットワーク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。

第１４条（参加施設の定義）

参加施設とは、本ネットワークを利用するにあたって理事長に施設参加申請書を提出し、利用の許諾を受けた機関をいう。

第１５条（参加施設の管理責務）

本ネットワークに参加する参加施設の長は、その管理責任を負うものとする。また、利用にあたっては施設管理者を配置し安全かつ適切な管理・運用に努めなければならない。参加施設の管理責務については「施設利用規約」

で定める。

第１５条（施設管理者の責務）

施設管理者は、自施設における本ネットワークシステムの運用管理に責任を持つ。施設管理者の管理責務については「施設利用規約」で定める。

第１６条（利用者の定義）

利用者とは、本ネットワークへの参加申請があった施設のうち本規程に定める識別番号（以下「ID 番号」という）及び、パスワードの登録を完了した本ネットワーク利用者のことをいう。

第１７条（利用者の責務）

利用者は、「施設利用規約」に基づき利用する。

第４節　一般管理における運用管理事項

第１８条（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、個人単位とし共有することはない。

（３）パスワードは８桁以上の英数を組み合わせたものとする。

（４）ネット管理責任者は、利用者から本ネットワークの参加利用申請を書面にて受理した後、システム管理者へ受け渡しを行う。システム管理者は、参加利用申請に従って、ユーザ登録を実施する。

（５）システム管理者は、参加施設に属する職員等の採用時、異動時、退職時にあわせ、各参加施設の長から書面による申請を受けた際に、速やかにユーザの登録、変更、削除の措置を取る。

（６）ユーザ登録時は、システム管理者の登録処理による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し、システム管理者であってもパスワードを推定できない仕組みとする。

（７）パスワードの有効期限は、原則６ヶ月以内とし、利用者が更新する。システム管理者またはネット管理責任者は、６ヶ月以上パスワードを更新しない利用者に対し、警告を与え、速やかに更新させるものとする。

（８）利用者が、パスワードを紛失し、本ネットワークシステムの利用ができなくなった場合は、ネット管理責任者を介してシステム管理者へパスワードの初期化依頼を提出する。

（９）ネット管理責任者は、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、システム管理者へ申請書の受け渡しを行う。システム管理者は、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。

（１０）利用者が、ネットワークへのログインの際にパスワードの入力を１０回連続で間違えた場合は、ロックアウトされるものとする。ロックの解除は事務局にて電話で受け付けるものとする。

（１１）利用者 ID には原則として管理者権限は付与しない（ユーザ権限とする）。

第１９条（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。

第２０条（アクセス管理）

システム管理者は、職務に定められた権限によるデータ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　システム管理者は、その内容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。

３　不正アクセス監視として、利用者のアクセスログを「不正アクセス監視手順」に従って監視し、「不正アクセス監視手順」で設定された閾値を超える不正が発生した場合、監査責任者に報告をしなければならない。

第２１条（個人情報を含む記録媒体の管理）

保管、バックアップの作業に当たる者は、手順に従って実施し、その作業の記録を残し、システム管理者の承認を得なければならない。

第２２条（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、システム管理者が作業前後に確認し、結果を記録に残すものとする。

第２３条（リスクに対する予防と発生時の対応）

システム管理者は、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、この規程の見直しを行うものとする。

２　システム管理者は、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。

第２４条（タイムスタンプ）

時刻調整された各サーバーからシステムに付与された時刻情報をタイムスタンプとみなすものとする。

第５節　業務委託の安全管理措置

第２５条（業務委託の安全管理措置）

業務を協議会以外の所属者に委託する場合は、守秘事項を含む業務委託契約を結ぶものとする。

２　システム管理者は、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、次に示す事項を規定し、十分な個人情報の保護水準を担保する。

（１）委託者及び受託者の責任の明確化
（２）個人情報の安全管理に関する事項
（３）再委託に関する事項（再委託する事業者にも委託先と同等の義務を課すこと）
（４）個人情報の取扱状況に関する委託者への報告の内容及び頻度
（５）契約内容が遵守されていることを委託者が確認できる事項
（６）契約内容が遵守されなかった場合の措置
（７）事件・事故が発生した場合の報告・連絡に関する事項
（８）一連の委託業務終了後に関する事項（終了報告、確実にデータを消去する等）
（９）保守要員のアカウント情報の管理に関する事項（適切に管理することを求める）

４　システム管理者は、保守会社における保守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。

第６節　情報及び情報機器の持ち出しについて

第２６条（情報及び情報機器の持ち出し）

ネットワークシステムに関わる情報及び情報機器の持ち出しに関するリスク分析並びに持ち出し対象となる情報及び情報機器の規程は、別に定めるものとする。

２　持ち出し対象となる情報及び情報機器は、本システムへ接続が可能な端末及び、その端末で利用する電子媒体とする。

３　持ち出し対象となる情報機器を、施設内またはその他の環境にあるデスクトップ PC またはノート PC などの USB ポートを利用して充電をすることを禁止する。

４　情報及び情報機器を持ち出す場合は、「情報機器外部持ち出し許可申請書」を利用者がネット管理責任者に届け出て、承認を得なければならない。ただし、その都度ではなく、１回申請後の有効期間を 6 か月間とする。

５　ネット管理責任者は、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。

6　持ち出す情報機器は、以下の通り扱うものとする。

（1）情報機器には起動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）持ち出すPCまたはノートPC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）持ち出した情報を、許可されていないアプリケーションがインストールされた情報機器で取り扱わないこと。

（5）持ち出した情報機器には、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。

7　持ち出した情報及び情報機器の盗難及び紛失時には、直ちにネット管理責任者に届け出なければならない。届け出を受け付けたネット管理責任者は、その情報および情報機器の重要度に従って対応する。

8　ネット管理責任者は情報及び情報機器の持ち出しについてシステム運用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置くものとする。

9　ネット管理責任者は、利用者に対し、情報機器の持ち出しについて研修又は周知を行うものとする。

第７節　外部の機関と医療情報を交換する場合の措置

第２７条（外部機関との医療情報の交換）

本ネットワークシステムと外部各種システムとのデータ連携は、予め協議会理事会にて審議を行い、決裁を受けるものとする。

2　外部の機関とネットワークを通じて医療情報を交換する場合は、リスク分析を行い、安全に運用されるように別途定める技術的及び運用的なリスク対策を講じるものとする。

3　外部の機関と本ネットワークを通じて医療情報を交換する場合、相手の医療機関、通信事業者及び運用委託業者との間で、責任分界点や責任の所在を契約書等で明確にするものとする。

4　システム管理者は、外部の保守会社からリモートメンテナンスを受ける場合、相手の保守会社、通信事業者及び運用委託業者等との間で、責任分界点や責任の所在を契約書等で明確にするものとする。

5　システム管理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。

6　システム管理者は、外部からアクセスする機器については許可した物に限定し、その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するものとする。

第８節　災害等の非常時の対策

第２８条（災害等の非常時対策）

災害、サイバー攻撃などにより一部ネットワークサービス提供体制に支障が発生する非常時の運用は、別に定める「災害時マニュアル」に従って運用を行う。

第９節　教育と訓練

第２９条（教育と講習会）

システム管理者は、情報システムの取扱いについてシステム運用マニュアルを整備し、ネット管理責任者及び利用者に周知の上、常に利用可能な状態に置くものとする。

２　システム管理者は、本ネットワークシステムの利用者に対し、定期的にネットワークシステムの取扱い及びプライバシー保護に関する教育又は周知を行うものとする。

３　本ネットワークの業務従事者は、在職中のみならず、退職後においても業務中に知った個人情報に関する守秘義務を負うものとする。

第１０節　監査

第３０条（監査）

本ネットワークシステムを円滑に運用するために、ネットワーク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。

２　監査責任者は理事長が指名する。

３　監査責任者はさくらネットの協議会運用管理規程への準拠状況及びさくらネットの運用状況を毎年３月に監査する。

４　運用責任者は、監査責任者から監査結果の報告を受け、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。

５　監査責任者の責務は本規程に定めるものの他、別に定める。

６　監査の内容については、監査責任者が定める。

７　運用責任者は必要な場合、臨時の監査を監査責任者に命ずることができる。

第１１節　是正処置及び予防処置

第３１条（是正処置及び予防処置）

本ネットワークでは、本事業に参加する住民やシステム利用者等からの苦情、緊急事態の発生、監査報告、外部審査機関等からの指摘で、システムの機能、運用状況等に問題がある場合には、問題に対する是正処置及び予防処置を確実に実施するための責任及び権限を定める手順を確立し、実施し、かつ、維持する。その手順には、次の事項を含める。

（１）問題の内容を確認する。

（２）問題の原因を特定し、是正処置及び予防処置を立案する。

（３）期限を定め、立案された処置を実施する。
（４）実施された是正処置及び予防処置の結果を記録する。
（５）実施された是正処置及び予防処置の有効性を確認する。

第２章　電子保存における運用管理

第１２節　電子保存３原則の確保

第３２条（真正性の確保）

システム管理者及び利用者は、次の各号のとおり真正性を確保するものとする。
（１）システム管理者は、電子保存システムの利用者の登録を管理し、そのアクセス権限を規定し、不正な利用を防止する。
（２）パスワードの最低文字数と有効期間、認証の有効回数と超過した場合の対処等については別途システム運用マニュアルの「利用者 ID とパスワード」に定めるものとする。
（３）利用者は、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。
（４）利用者は、ネットワークシステムの情報のアクセスに際して、認証番号、パスワード等によって、ネットワークシステムに自身を認識させること。
（５）システム管理者は、ネットワークシステムを正しく利用させるため、講習会を開催し、利用者の教育を行うこと。
（６）利用者は、離席する際にネットワークシステムからログアウトすること。
（７）ネットワークシステムに保存されている情報の作成責任は、ログオン利用者にあるものとする。
（８）利用者は、ネットワークシステムへの情報入力に際して、確定操作を行い、入力情報に対する責任を明示し、及びその更新履歴を保存すること。
（９）代行入力の場合、入力権限を持つ者が最終的に確定操作を行い、入力情報に対する責任を明示し、及びその更新履歴を保存すること。
（１０）システム管理者は、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をネット管理責任者の協力の元、定期的に実施することとする。

第３３条（見読性の確保）

システム管理者は、次の各号のとおり見読性を確保するものとする。
（１）情報機器及び媒体のリストを作成し、定期的に情報の所在確認を行うこと。
（２）電子保存に用いる機器及びソフトウェアを導入するにあたって、保存義務のある情報として電子保存された情報ごとに、見読用機器（モニタ、プリンタ、ネットワーク機器等）を常に利用可能な状態に置くこと。
（３）応答時間の劣化がないように維持に努め、必要な対策をとること。
（４）障害時の対応体制が最新のものであるように管理すること。また、データバッ

クアップ作業が適切に行われていることを確認すること。

第３４条（保存性の確保）

システム管理者は、次の各号のとおり保存性を確保するものとする。

（１）本ネットワークシステムで使用されるソフトウェアについて、使用の前に審査を行い、情報の安全性に支障がないことを確認すること。

（２）ネットワークシステムの記録媒体を含む主要機器を、入退室管理された場所に設置すること。

（３）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こと。

第３５条（相互運用性の確保）

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

第３６条（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）患者や他院・他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、また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　システム管理者は、適宜業務において本規程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。

第３章　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

第１３節　外部保存における電子保存３原則の確保

第３７条（外部保存）

ネットワークシステムサーバのバックアップ情報は、可搬媒体を用いて外部保存するものとする。

２　可搬媒体の搬送及び保管は、業務委託するものとする。

第３８条（真正性の確保）

システム管理者は、次の各号のとおり真正性を確保するものとする。

（１）搬送時や外部保存を受託する機関の障害等に対する対策として、可搬媒体の教授記録を行うこと。

（２）システム管理者は、可搬媒体を変更したり、更新したりする際には、明確な記録を行うこと。

第３９条（見読性の確保）

システム管理者は、緊急時の診療への対応又は監査等への対応に支障が出ないように、可搬媒体と同等の内容を持つ情報を事務局内部に保存するものとする。

第４０条（保存性の確保）

システム管理者は、次の各号のとおり保存性を確保するものとする。

（１）システムの更新等に伴う相互運用性を確保するために、可能な限り標準的なデータ形式を用いて可搬媒体に記録すること。

（２）可搬媒体の劣化対策を行うこと。

（３）可搬媒体や読み出し機器の陳腐化対策を行うこと。

第４１条（可搬媒体が搬送される際の個人情報の保護）

システム管理者は、次の各号に掲げる、可搬媒体が搬送される際の個人情報保護に関わる事項を契約上明記するものとする。

（１）パスシート等を記録した可搬媒体の遺失防止措置

（２）パスシート等を記録した可搬媒体と他の搬送物との混合の防止措置

（３）搬送時の情報漏洩等の守秘義務の遵守

第４２条（可搬媒体が外部保存される際の個人情報の保護）

システム管理者は、次の各号に掲げる、可搬媒体が外部保存される際の個人情報保護に関わる事項を契約上明記するものとする。

（１）受託業者が可搬媒体内の医療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の事務局への通知

（３）外部保存時の守秘義務の遵守

（４）受託業者の個人情報保護対策の実施状況の監査

第４３条（通常運用における責任の明確化）

システム管理者は、外部保存を行なっていることを患者へ周知するものとする。

２　システム管理者は、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。

第４４条（事後責任の明確化）

システム管理者は、次号に掲げる、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保存するタイミングと外部保存に関連する一連の操作

（２）事務局と搬送業者との間で可搬媒体を教授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業者との間で可搬媒体を教授する方法及び管理方法

（６）受託機関が事務局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

第４５条（外部保存契約終了時の処理）

システム管理者は、外部保存契約修了時のデータ返却処理について、契約上明記するものとする。

第４章　雑則

第１４節　その他

第４６条（本事業に参加する住民への説明）

運用責任者は、外部保存を行なっていることを本事業に参加する住民へ周知するものとする。

第４７条（実験・開発目的の利用）

各種研究・開発、新規技術導入検証等においてネットワークを実証実験に利用する場合、協議会にて審議を行う必要がある。

附則

（施行期日）

１．本規程は、２０２４年６月１３日から施行する。