医・歯・薬・介護連携ネットワーク
「TGP ネットワーク」

システム運用管理規程

（第 1.1 版）

平成 31 年２月 14 日

環岐阜地区医療介護情報共有協議会

第１章　総則

（目的）
第１条　このシステム運用管理規定（以下、「本規程」という。）は、医・歯・薬・介護連携ネットワーク「TGP ネットワーク」（以下、「TGP ネットワーク」という。）のシステムの運用・管理に関する詳細を規定し、TGP ネットワークの安全で安定な稼働を目的とする。

（適用範囲）
第２条　このシステム運用管理規定は、TGP ネットワークを構成するクラウド設備の管理業務（以下「システム管理業務」という。）、及びこのシステムの利用者支援業務並びに情報管理業務（以下「システム運用業務」という）に適用する。

（管理体制）
第３条　TGP ネットワークのシステムにおける運用・管理に係る委託契約事業者（以下「システム運用管理事業者」という。）は、前条のシステム管理業務及びシステム運用業務に関して責任を持つ「システム運用管理責任者」を選任する。
２ システム運用管理責任者は、その配下にシステム管理業務の実施管理を行う「システム管理者」、システム運用業務の実施管理を行う「システム運用者」、及びラック等の鍵管理を行う「鍵管理者」を任命する。
３ システム運用管理責任者は、第１項及び第２項により定めた管理体制を環岐阜地区医療介護情報共有協議会（以下「サービス運用者」という。）に届出する。

（教育・訓練）
第４条　システム運用管理責任者は、システム運用業務またはシステム管理業務に携わる要員に対し、TGP ネットワークに関する事項及び業務実施に関する事項について十分な教育・訓練を実施する。

（管理規程などの提示）
第５条　システム運用管理責任者は、TGP ネットワークのシステムにおける運用・管理業務に関係する社内管理規程及び手順をサービス運用者に提示し、承認を得る。

（準拠する法令・ガイドライン等）
第６条　TGP ネットワークの提供にあたり、システム運用管理責任者は、下記に示す法令及びガイドラインを遵守し、準拠度チェックリストをサービス運用者に提示し、承認を得るものとする。
(1)個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）
(2)クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン第１版（平成 30 年 7 月 総務省）
(3)医療情報を受託管理する情報処理事業者向けガイドライン第２版（平成 24 年 10 月 経済産業省）
なお、上記ガイドラインの遵守は、下記のガイドラインに記述された趣旨を理解した上で、実施する。
(4) 医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス（平成 29 年 4 月 14 日 個人情報保護委員会、厚生労働省）
(5)医療情報システムの安全管理に関するガイドライン第５版（平成 29 年 5 月 厚生労働省）

（資産台帳の整備、管理）
第７条　システム運用管理事業者は、TGP ネットワークを構成するクラウド設備システムに関係する情報資産を確実に保護し、その情報セキュリティ（機密性、完全性、可用性）を確保することを目的に、そのクラウド設備を構成するハードウェア、ソフトウェアについて資産台帳を整備管理する。

第２章　物理的及び環境的セキュリティ

（クラウド設備の設置場所）

第８条　TGP ネットワークを構成するクラウド設備は医療情報等を処理保管する重要機器が含まれることから、以下の条件を満たすセキュリティ区画に設置する。
(1) 一般的な事務室との共用、または隣接を避けている。
(2) 危険物保管場所、火気施設、水道設備等のリスクの大きい場所から離れている。
(3) 設置場所の表示は最小限にとどめている。
(4) 出入り口は原則１ヶ所とし、施錠設備を設けている。
(5) 窓を設けることを避け、設ける場合は強化ガラスの使用などの対策をしている。
(6) 防犯カメラ、侵入報知器等の防犯設備を設置している。
(7) コピー機、FAX など情報の複写、送信のための設備を設置していない。
(8) 外部の施設を利用する場合は、他組織の機器から隔離し、施錠できるようにしている。

(設置場所の運用)
第９条　センター設置場所の運用は次のとおりとする。
(1) クラウド設備設置室及び TGP ネットワーク用に隔離されたスペースは、不在時には施錠する。
(2) クラウド設備設置室への入室は、認証装置等により特定のものに制限する。
(3) 入室制限を受けている者の入室に対しては、システム運用管理責任者が許可し、入室可能な者が同伴する。
(4) 入退室履歴を記録する。
(5) クラウド設備設置室内では許可なしに撮影、録音をしない。
(6) クラウド設備設置室内には、必要なもの以外を置かない。
(7) TGP ネットワーク用に隔離されたスペースの鍵は鍵管理者が管理する。

(電源設備の点検)
第 10 条　システム管理者は、電源設備の点検作業のため、必要に応じ年 1 回 1 日間(24 時間)商用電源供給とする。なお、その場合システム管理者は予め点検日程をサービス運用者に連絡する。

第３章　システム運用業務とそのセキュリティ

(システム運用業務)
第 11 条　TGP ネットワークに関するシステム運用業務については、利用者等の的確な管理と利便性の向上を図ることを目的とし、以下の項目をシステム運用業務とする。
(1) 利用者識別番号(以下「ユーザーＩＤ」という。)、暗証番号(以下「パスワード」という。)の付与とその登録・削除・変更(ユーザー管理)
(2) ポータルサイト情報の登録・削除・変更(ポータル管理)
(3) TGP ネットワークの本番データ（TGP ネットワークで共有される実際の患者データ）の提供(本番データの臨時使用)
(4) 利用者等の問合せ対応(問合せ対応)
(5) その他、システム運用に関する事項

(ユーザー管理)
第 12 条　システム運用者は、TGP ネットワークを利用する施設の管理者（以下「施設管理者」）からの依頼で利用者のユーザーＩＤ利用停止と、新たなユーザーＩＤ及びパスワードの付与をする場合、以下のことを実施する。
(1) 利用者の追加に際しては、ユーザーＩＤ及びパスワードのコード要件に適合するユーザーＩＤ 及びパスワードを決定・登録する。そのユーザーＩＤ・パスワードを、施設管理者に通知する。
(2) 利用者の削除に際しては、その要求に対して速やかに削除する。
(3) 利用者の変更に際しては、(1)と(2)の処理を行う。
(4) 利用者に関する付随情報については、当該利用者の本人確認を確実に実施した上で要求に応じて変更する。

(ポータル管理)

第 13 条　システム運用者は、サービス運用者からポータルサイト情報の変更要求が送られてきた時、以下のことを実施する。
(1) ポータルサイト中に登録されている情報構成の変更など表示画面の設計を要する場合は、その設計について、サービス運用者と協議する。
(2) 表示画面の設計が不要で内容変更のみの場合は、その要求に対し、速やかに対応する。
(3) 新規追加情報、更新情報については、トップページで新規情報あるいは既存情報の更新が明記されるよう合わせて変更する。

(本番データの臨時使用)
第 14 条　システム運用者は、データ分析利用、障害対応時の原因究明作業、システム改修時の動作検証等、臨時的に本番データを使う場合において、サービス運用者が承認した本番データ使用許可書が提示されたとき、以下のことを実施する。
(1) 使用する本番データに個人情報が含まれる場合は、個人を特定できないように加工し出力する。
(2) 提供に当たって集計などの情報処理が必要なときは、その処理を行う。
(3) 提供方法は紙またはファイルとし、その送付先は本番データ使用申請者とする。

(問合せ対応)
第 15 条　システム運用者は、月曜日から金曜日(祝祭日と、12 月 29 日から 1 月 3 日までは除く)までの 9:00～17:00 の間､サービス運用者及び利用者からの以下の内容に答える体制(ヘルプデスク)を整える。
(1) システム利用開始時の問合せ
(2) システム仕様に関する問合せ
(3) システム概要に関する問合せ
(4) システム利用に関する問合せ
(5) 参加医療施設の案内
(6) ユーザー情報の問合せ
(7) 障害対応・復旧時間の問合せ対応 など
なお、システム運用者は、それぞれの問合せとその対応について記録する。

(トラブル対応)
第16条　システム運用者は、システム運用業務の中でシステムの異常を発見した場合及び情報漏えい事故が発生した場合、次の各号に示す事項を実施するものとする。
【システム異常の場合】
(1) システム管理者とシステム運用者は、システムの異常または不具合の状況把握を行う。
(2) 情報漏えい事案や利用者等の利用に影響が及ぶ場合、システム管理者は速やかにサービス運用者とシステム運用管理責任者に報告する。情報漏えい事案発生の場合は、後述の【情報漏洩事故の場合】の対応も合わせて行う。
(3) システム管理者とシステム運用者は､原因を分析し､その復旧のため関係箇所(メーカ､ベンダー、システム構築会社など)と連係し、早期復旧に努める。
(4) システム管理者とシステム運用者は、利用者等の利用に影響が及ぶ場合は、状況に応じて利用者へ通知し、電話・FAX・e-mail 等により状況、復旧予定などを報告する。
(5) システム運用管理責任者とシステム管理者は、システム管理業務の一環で対応できない再発防止策が必要と思われる場合は、その内容を整理しサービス運用者に報告する。それらを受け、サービス運用者は必要に応じて臨時の協議会を召集し、事故防止の対策を検討する。
(6) システム運用者は、障害等からの復旧対策の目的でシステム上に掲載された情報等にアクセスすることがある。その場合、医療機関等における診療録等の個人情報と同様の秘密保持を行なうと同時に、サービス運用者に許可を求めなければならない。
(7) システム運用者は、上記アクセスを行なう場合は必ず操作記録を取り、操作記録等をサービス運用者に提出するものとする。

【情報漏洩事故の場合】
(1) システム管理者とシステム運用者は、情報漏えい事案の状況把握を行う。
(2) システム管理者は、速やかにサービス運用者とシステム運用管理責任者に報告する。
(3) TGP ネットワーク事務局、参加施設、患者へ被害が発生する可能がある場合は、サービス運用者およびシステム運用管理責任者が必要と認める者を召集し、対応策を検討する。
(4) システム運用管理責任者とシステム管理者は、サービス運用者に今後の対応策を提案し、許可を得る。
(5) システム管理者は、関係者に対応を指示し、口頭と書面による報告を受ける。
(6) システム運用管理責任者は、対応の顛末を書面で、サービス運用者に提出し報告する。
(7) システム運用管理責任者は、影響の範囲に於いて、必要であれば然るべき監督官庁などへ報告を行う。

第４章　システム管理業務とそのセキュリティ

(システム管理業務)
第 17 条　TGP ネットワークに関するシステム管理業務については、TGP ネットワークを構成するクラウド設備システムに関係する情報資産を確実に保護し、その情報セキュリティ(機密性、完全性、可用性)を確保することを目的とし、以下の項目をシステム管理業務とする。
(1) セキュリティ上の問題、事故・故障等への対応(トラブル対応)
(2) セキュリティ区画の入退管理と施錠管理(セキュリティ区画の管理)
(3) TGP ネットワークの開発・構築・改修後のシステムの受け入れ(受け入れ)
(4) TGP ネットワークのハードウェア、ソフトウェアの維持管理(維持管理)
(5) システムデータ、アプリケーションデータのバックアップ(データ・バックアップ)
(6) TGP ネットワークの運転・操作及び稼働監視(運転監視)
(7) その他システム管理に関する事項

(セキュリティ区画管理)
第 18 条　システム管理者は、TGP ネットワークの維持管理等に伴って直接クラウド設備に対する作業を実施する必要がある場合、以下の事項を遵守する。
(1) クラウド設備設置室への入退管理ルールに従うこと。
(2) ラックは常時施錠し、作業に当たっては鍵管理者による鍵の貸し出し許可を受ける。
(3) 鍵の管理は鍵管理者が実施する。

(受け入れ)
第 19 条　システム管理者は、システムを新規に受け入れる場合または改善後に受け入れる場合、以下の事項を実施する。
(1) システム管理業務として規定された業務の具体的な実施方法またはその変更事項の確認。
(2) 受け入れるシステムが仕様通り正常に稼働することの確認及び改善の場合は既存システムへの悪影響がないことの確認。
(3) 受け入れる資産台帳(ハードウェア、ソフトウェア、アプリケーションプログラムなど)の整備。
(4) 受け入れるシステムについて、システムファイルのバックアップの確保。

(維持管理)
第 20 条　システム管理者は、受け入れたシステムのハードウェア及びソフトウェアに対する以下の維持管理を実施する。
(1) ハードウェアに対しては、メーカーの指示に従い定期的なリブートなどの維持管理を行い記録する。
(2) ソフトウェアに対しては、メーカー等からの指示に従い、バグ対応やセキュリティホール対応などの維持管理を行い記録する。
(3) ソフトウェアの維持管理を実施した時は、システムファイルのバックアップを確保する。

(4) システムデータについては、第 19 条に規定した受け入れ時及び変更時にバックアップを取り、１年間保管する。
(5) 個人情報を記した媒体の廃棄に当たっては、安全かつ確実に行われることを作業前後に確認し、結果を記録する。

(データ・バックアップ)
第 21 条　システム管理者は、システム内にて一時保管している利用者の複製診療情報(以下「アプリケーションデータ」という。)について以下のデータ・バックアップ処理を行う。バックアップ対象は、TGP ネットワークデータセンターの医療連携ツールサーバ及び、データ標準化サーバに記録・保存されたアプリケーションデータとし、TGP ネットワークデータセンターのバックアップ専用ストレージ内に保管する。
(1) 利用者が TGP ネットワークのシステム内へアプリケーションデータを発信した日から起算して１年間の保管に万全を期すために、毎日及び毎月定められた日時に自動データ・バックアップ処理を行う。
(2) 自動データ・バックアップ作業を行う日時については、予めサービス運用者の承認を受けるものとする。サービス運用者からの承認後、毎日及び毎月のデータ・バックアップの日時をポータルサービスにより予め利用者に周知する。
(3) 毎月 1 回のデータ・バックアップ作業時については、TGP ネットワークのすべて又はその一部のサービスを停止することができるものとする。また、システム停止を伴う作業が発生する場合は、その内容を予め利用者に周知する。
(4) データ・バックアップ先では暗号化して保管する。暗号化の方法はセキュリティ面を考慮して非公開とするが、AES-256bit と同等以上の、もしくは「電子政府における調達のために参照すべき暗号のリスト」に記載された暗号化方式を採用する。また、物理装置に分散保管を行い、部分的物理媒体盗難時でも情報の復号化を困難とする措置をもちいる。

(運転・監視)
第 22 条　システム管理者は、受け入れたシステムの運転操作(起動停止など)及びシステムの稼働監視(死活監視など)を以下により実施する。
(1) システムの運転操作は自動となっているので、TGP ネットワークのシステム内からアプリケーションデータの削除処理及びシステムの異常等によりシステム停止を要する時のみ、手動運転操作とする。
(2) システムの稼働監視は、Ping による５分毎の死活監視、15 分毎のシステムアプリケーションの応答監視とする。
(3) 外部からの不正アクセスを防止するため、ファイア・ウォールのアクセス・ログを常時チェックする。
２ 上記に必要な運転手順書はシステム管理者がいつでも参照できるよう常備する。
３ システム管理者は第１項により異常を検知した場合、速やかにサービス運用者へ通知する。

（個人情報へのアクセス）
第 23 条　システム運用管理事業者は、サービス運用者の許可なく TGP ネットワークが取り扱う個人情報にアクセスしてはならない。

（罰則）
第 24 条　システム運用管理事業者が本規程を遵守していない事実が判明した場合、サービス運用者は、相当期間を定めて書面により勧告し、是正報告を受けるものとする。
２　上記について書面により勧告したにも関わらず改善されていない場合、サービス運用者はシステム運用管理事業者との契約を解除するとともに、システム運用管理事業者はサービス運用者に対して、次項に定める違約金を支払うものとする。
３　違約金はシステムの移行に係る費用に相当する額として、サービス運用者が算定した金額とする。かかる違約金額についてサービス運用管理事業者は異議を述べないものとする。なお、違約金額の上

限額は別途取り決める１年間の契約金額とし、これを超えることは無いものとする。

附則

１　この規約は平成 30 年 2 月 28 日より実施します。

２　この規程はは平成 31 年２月 14 日より名称を「システム運用管理業務セキュリティポリシー」から「システム運用管理規程」へと変更・改訂し、実施いたします。