「豊山レインボーネット」

システム運用管理業務セキュリティポリシ

第一章　総則

（目的）

第１条　このセキュリティポリシは、豊山レインボーネット（以下、「レインボーネット」という。）の管理運営に関し、そのシステムの運用・管理に関する詳細を規定し、レインボーネットの安定稼働と効果的な利用支援 を目的とする。

（適用範囲）

第２条　このセキュリティポリシは、レインボーネット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　レインボーネットの運用・管理に係る委託契約事業者（以下、「レインボーネット運用管理箇所」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「運用管理責任者」を選任するものとする。

２　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」を任命するものとする。

３　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「豊山レインボーネットサービス運用者 」（以下、「サービス運用者」という。）に届出するものとする。

（教育・訓練）

第４条　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、レインボーネット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・訓練を実施するものとする。

（管理規程などの提示）

第５条　運用管理責任者は、レインボーネットの運用・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、承認を得るものとする。

（準拠する法令・ガイドライン等）

第６条　レインボーネットの提供当たり、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。

・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）

・ASP・SaaS 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 1.1 版(総務省平成 22 年 10 月)
・ASP・SaaS における情報セキュリティ対策ガイドライン(総務省平成 20 年 1 月 30 日)
・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(平成 20 年 7 月 24 日経済産業省)

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。

・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ドライン(厚生労働省平成 16 年 12 月 24 日通達、平成 18 年 4 月 21 日改正)
・医療情報システムの安全管理に関するガイドライン第 4.1 版(厚生労働省平成 22 年 2 月)

(資産台帳の整備、管理)

第７条　レインボーネット運用管理箇所は、レインボーネット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ものとする。

第二章　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　レインボーネット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ものとする。

⑴　一般的な事務室との共用、または隣接を避けていること。
⑵　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こと。
⑶　設置場所の表示は最小限にとどめていること。
⑷　出入り口は原則 1 ヶ所とし、施錠設備を設けていること。
⑸　窓を設けることを避け、設ける場合は強化がラスの使用などの対策をしていること。
⑹　防犯カメラ、侵入報知器等の防犯設備を設置していること。
⑺　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こと。

⑻　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こと。

（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。

⑴　クラウド設備設置室及びレインボーネット用に隔離されたスペースは、不在時には施錠すること。

⑵　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こと。

⑶　入室制限を受けている者の入室に対しては、運用管理責任者が許可し、入室可能な者が同伴すること。

⑷　入退室履歴を記録すること。

⑸　クラウド設備設置室内では許可なしに撮影、録音をしないこと。

⑹　クラウド設備設置室内には、必要なもの以外を置かないこと。

⑺　レインボーネット用に隔離されたスペースの鍵は鍵管理者が管理すること。

（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、年１回１日間(24 時間)商用電源供給とするものとする。なお、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ものとする。

第三章　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　レインボーネット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、以下の業務をシステム運用業務とする。(図 1)

⑴　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)

⑵　ポータルサイト情報の登録・削除・変更(ポータル管理)

⑶　レインボーネットの本番データの提供(本番データの臨時使用)

⑷　利用者等の問合せ対応(問合せ対応)

⑸　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、「豊山レインボーネット利用規約」（以下、利用

規約という。)の１３条の２項による利用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。

⑴　利用者の追加に際しては、別紙１のユーザー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、利用施設管理者に封書で知らせるものとする。

⑵　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ものとする。

⑶　利用者の変更に際しては、上記⑴及び⑵の処理を行うものとする。

⑷　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ものとする。

(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。

⑴　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ものとする。

⑵　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、速やかに対応するものとする。

⑶　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ものとする。

(本番データの臨時使用)

第１４条　システム運用者は、運営委員会が承認した本番データ使用許可書(別紙２)が提示されたとき、以下のことを実施する。

⑴　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。

⑵　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。

⑶　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 9:00～18:00 の間、利用者からの以下の内容に答える体制(ヘルプデスク)を整えるものとする。

⑴　システム利用開始時の問合せ
⑵　システム仕様に関する問合せ
⑶　システム概要に関する問合せ
⑷　システム利用に関する問合せ
⑸　参加医療施設の案内
⑹　ユーザー情報の問合せ
⑺　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ものとする。

第四章　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１６条　レインボーネットに関するシステム管理業務については、レインボーネット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、以下の業務をシステム管理業務とする。(図 2)

⑴　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)
⑵　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)
⑶　レインボーネットの開発・構築・改修後のシステムの受け入れ(受け入れ)
⑷　レインボーネットのハードウェア、ソフトウェアの維持管理(維持管理)
⑸　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)
⑹　レインボーネットの運転・操作及び稼働監視(運転監視)
⑺　その他システム管理に関する事項

（トラブル対応）

第１７条　システム管理者は、システム管理業務の中で発見したシステムの異常、システム運用者から不具合の連絡を受けた場合、以下の事項を実施し、別紙３にその内容を記録するものとする。

⑴　システムの異常または不具合の状況を確認する。
⑵　原因を分析し、その復旧のため関係箇所(メーカ、ベンダー、システム構築箇所など)と連係し、早期復旧に努める。
⑶　利用者等の利用に影響が及ぶ場合は、状況に応じて広報サービスへの掲載、及び別紙４のとおり電話・FAX・e-mail 等により状況、復旧予定など

を報告する。

⑷　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運営委員会を召集し、事故防止の対策を検討する。

(セキュリティ区画管理)

第１８条　システム管理者は、レインボーネット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ものとする。

⑴　クラウド設備設置室への入退管理ルールに従うこと。

⑵　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ものとする。

⑶　鍵の管理は鍵管理者が実施するものとする。

(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ものとする。

⑴　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

⑵　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並びに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

⑶　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

⑷　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ものとする。

⑴　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。

⑵　ソフトウェアに対しては、メーカ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。

⑶　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。

⑷　システムデータについては、第１８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年間保管するものとする。

(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ものとする。

⑴　利用者がレインボーネット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。

⑵　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公開するものとする。

⑶　毎月１回のデータ・バックアップ作業時については、レインボーネット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、その内容を予めポータルサービスにより利用者に公開するものとする。

(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(生死監視など)を以下により実施する。

⑴　システムの運転操作は自動となっているので、レインボーネット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。

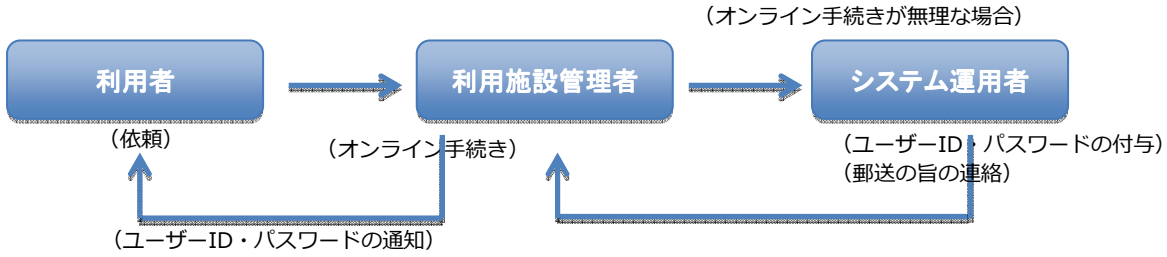
⑵　システムの稼働監視は、Ping による 5 分毎の生死監視、15 分毎のシステムアプリケーションの応答監視、さらにファイア・ウォールのアクセス・ログの定期的チェックとする。

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ものとする。

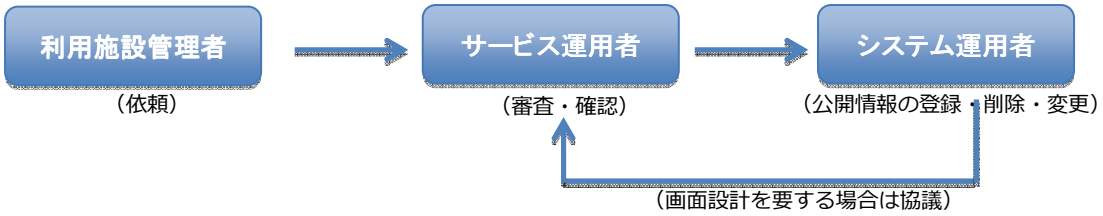
（図１）

システム運用業務

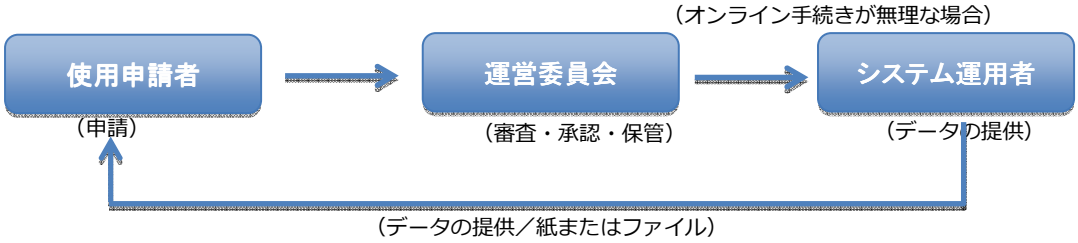
① ユーザーID・パスワードの付与とその登録・削除・変更



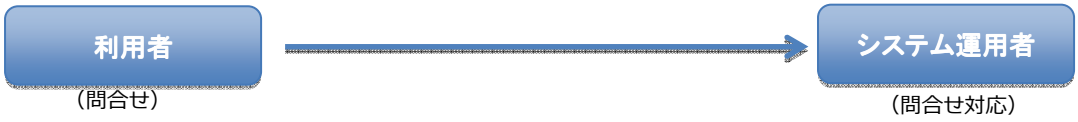
② ポータルサイト情報の登録・削除・変更（ポータル管理）



③ 本番データの臨時使用



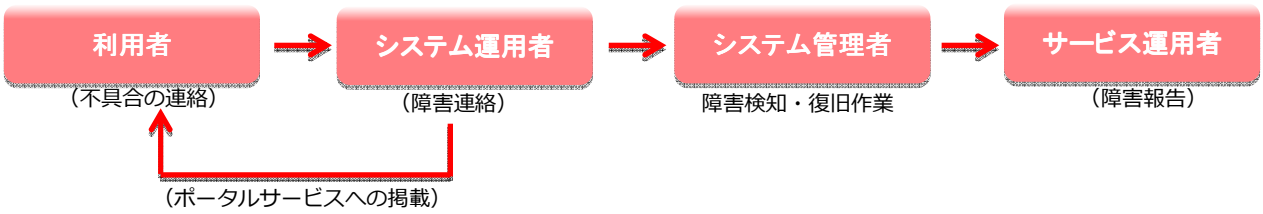
④ 利用者への問い合せ対応



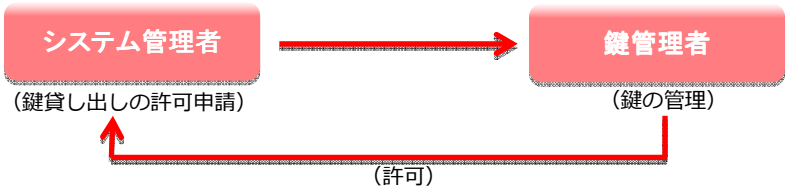
（図２）

システム管理業務

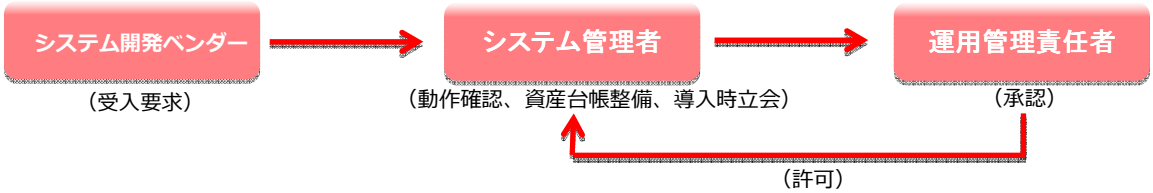
① セキュリティ上の問題、事故・故障等への対応



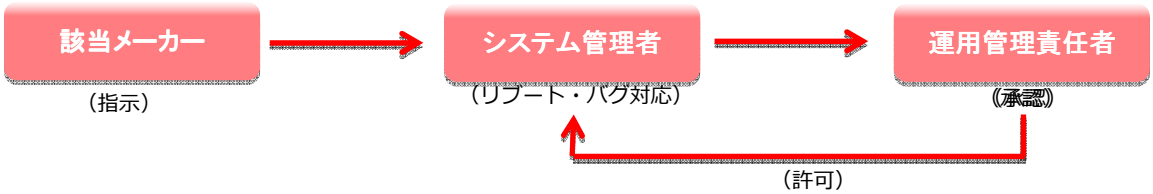
② セキュリティ区画の管理



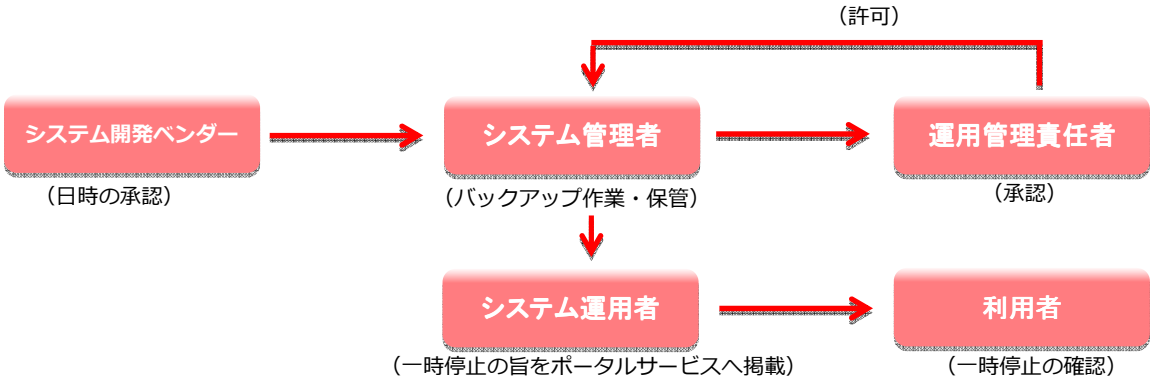
③ 新たなシステムの受け入れ



④ 維持管理



⑤ データ・バックアップ


（許可）
システム開発ベンダー
（日時の承認）
システム管理者
（バックアップ作業・保管）
運用管理責任者
（承認）
システム運用者
（一時停止の旨をポータルサービスへ掲載）
利用者
（一時停止の確認）

（別紙１）

利用者 ID 及びパスワードのコード要件

個人を特定できる利用者に対し、以下のユーザーID 及びパスワードを登録する。

利用者識別番号（ユーザーID）	１０桁の英数字
暗証番号（パスワード）	８桁の英数字

（別紙２）

本データ使用許可申請書

拝啓　時下ますますご清栄のこととお慶び申し上げます。

本データに記録されているデータの活用について次の通り申請させて頂きますので、ご査収を宜しくお願いいたします。

敬具

申　請　日	年　　月　　日
申　請　者	印
件　　名	
使 用 目 的	
処 理 内 容	
保 存 媒 体	□ＣＤ−Ｒ　□ＤＶＤ　□ＵＳＢメモリ　□ハードディスク □その他（　　）
使用後の措置	□自動保管　□返却　□消去　□その他（　　）
使 用 期 間	年　月　日～　　年　月　日
実　施　日	年　　月　　日
備　　考	
添 付 資 料	

（別紙３）

平成　　年　　月　　日

豊山町サービス運用者御中

中部テレコミュニケーション株式会社

障害報告書

拝啓　時下ますますご清栄のこととお慶び申し上げます。

平素は当社サービスをご利用いただき、厚く御礼申し上げます。

障害内容について次の通り報告させて頂きますので、ご査収を宜しくお願いいたします。

敬具

発見日時	
発見箇所	
発生日時	
障害内容	
影響範囲	
復旧日時	
経　　過	
原　　因	
処　　置	
備　　考	
添付資料	

（別紙４）

障害時などの連絡体制図