はち丸ネットワーク

システム運用管理業務セキュリティポリシー

第一章　総則

(目的)

第1条　このセキュリティポリシーは、はち丸ネットワークの管理運営に関し、そのシステムの運用・管理に関する詳細を規定し、はち丸ネットワーク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ーは、はち丸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　はち丸ネットワークの運用・管理に係る委託契約事業者(以下「はち丸ネットワーク運用管理事業者」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「運用管理責任者」を選任する。

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。

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一般社団法人名古屋市医師会(以下「サービス運用者」という。) に届出する。

(教育・訓練)

第4条　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、はち丸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　運用管理責任者は、はち丸ネットワークの運用・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。

(準拠する法令・ガイドライン等)

第6条　はち丸ネットワークの提供にあたり、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 4.2 版(厚生労働省平成 25 年 10 月)

(資産台帳の整備、管理)

第 7 条　はち丸ネットワーク運用管理事業所は、はち丸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　はち丸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はち丸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、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 はち丸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、年 1 回 1 日間(24 時間)商用電源供給とする。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。

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　はち丸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①～⑤の業務をシステム運用業務とする。（図 1）

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 はち丸ネットワークの本番データの提供(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、はち丸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、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、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、上記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、サービス運用者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。

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。

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　はち丸ネットワークに関するシステム管理業務については、はち丸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①～⑦の業務をシステム管理業務とする。（図 2)

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 はち丸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 はち丸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 はち丸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

(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。

① システムの異常または不具合の状況を確認する。
② 原因を分析し、その復旧のため関係箇所(メーカ、ベンダー、システム構築など)と連係し、早期復旧に努める。
③ 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周知、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。
④ 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調整会議会を召集し、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、はち丸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。

(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。

① 利用者がはち丸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、はち丸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。

(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。

① システムの運転操作は自動となっているので、はち丸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。