かがわ医療情報ネットワーク協議会セキュリティポリシー

１．総則

１．１目的

このセキュリティポリシーは、かがわ医療情報ネットワーク（以下「K-MIX R」という。）を活用した医療情報等連携事業に係る事業運営主体である、かがわ医療情報ネットワーク協議会（以下「協議会」という。）が、K-MIX R で取り扱う情報を改ざん、破壊、漏洩から保護すると共に、情報を利用する協議会の構成員に対して、情報システムに関する安全管理の重要性及び個人情報の適切な取扱いと保護についての認識を高め、K-MIX R の安全かつ適正な管理を図ることを目的として定めるものとする。

１．２適用範囲

このセキュリティポリシーは、情報連携基盤である K-MIX R のポータルシステムに接続する各システムの利用者支援業務並びに運用管理業務等に適用する。接続システム名は下表の通りである。

＜K-MIXR ポータルシステム接続システム一覧＞

接続システム名
K-MIX R BASIC
地域患者情報システム
K-MIX＋
遠隔読影システム
地域連携クリティカルパスシステム

令和３年４月１日現在

２．管理体制

２．１責任者の選任と管理体制

（１）事業管理者

かがわ医療情報ネットワーク協議会会長をこれに充てる。

事業管理者は、K-MIX R の円滑な推進を目的とし、本事業の統括・管理を行う。

（２）事業実施責任者の設置

かがわ医療情報ネットワーク運営委員会運営委員長をこれに充てる。

事業実施責任者は、正副の任命を妨げない。

事業実施責任者は、K-MIX R の運営が円滑に執り行われるよう各種調整業務を行う。

事業実施責任者は、参加機関の登録に関する事務取扱を実施し、登録状況について事業管理者に報告する。

（３）運用管理責任者の設置

かがわ医療情報ネットワーク協議会事務局長をこれに充てる。

運用管理責任者は、正副の任命を妨げない。

（４）システム管理者の設置

運用管理責任者は、本システムの安全かつ円滑な運用の実施責任をもつシステム管理者を任命するものとする。

システム管理者は、正副もしくは複数の任命を妨げない。

（５）その他の責任者の設置

運用管理責任者は、本システムの安全かつ円滑な運用の実施を行う、その他の責任者を任命するものとする。

その他の責任者は、各々正副もしくは複数の任命を妨げない。

責任分担の詳細については、運用管理規程にて別途定める。

２．２サポートデスクの設置

（１）運用管理責任者は、個人情報の取扱いおよび本システムの運営等に関して、利用者等からの相談、苦情を受け付け、適切かつ迅速な対応を行うためサポートデスクを設置し、運営するものとする。

（２）サポートデスクは、以下のサポート業務を行うものとする。

①　以下の問合せへの対応

・本システムの利用に関する事項
・本システムの内容に関する事項
・本システムの利用者登録、変更、解消に関する事項
・本システムの障害に関する事項
・本システムの操作に関する事項
・個人情報の保護、取扱いに関する事項

②以下の実施

・本システムの利用者登録、変更、解消
・利用者向け個人情報の保護、安全管理に関する教育
・利用者向けシステム利用に関する教育

（３）サポートデスクの問い合わせ対応日時は、以下のとおりとする。
平日９：００～１７：００
（土日祝日および年末年始を除く）

（４）サポートデスクの場所等

相談窓口	かがわ医療情報ネットワーク協議会サポートデスク
住所	〒760-8534　高松市浜ノ町 73 番 4 号
Web サイト	https://kmix-r.jp
電話番号	080-6373-9180
FAX	087-883-0202
メール	support@kmix-r.jp

２．３災害・事故対策体制

運用管理責任者は、緊急時および災害時の連絡、復旧体制等を定め、文書化し、運用管理に携わる関係者に周知をするものとする。

２．４教育・訓練

（１）運用管理責任者は、本システムの取扱いについてマニュアルを整備し、運用管理に携わる関係者に周知を行うものとする。

（２）運用管理責任者は、本システムの運用に携わる関係者に個人情報の保護に関する教育を行うものとする。

（３）運用管理責任者は、本システムを利用する病院、診療所、歯科診療所、薬局（以下これらを「医療機関等」という。）の責任者がその所属員に行う個人情報保護および安全管理に関する教育に関し、協力の依頼があった場合はこれに協力するものとする。

２．５運用管理規程などの整備

運用管理責任者は、本システムに係わる運用について運用管理規程などを整備し、安全かつ円滑な運用を図るものとする。

事業全体に係わる運用管理規程などについては、別途定めるものとする。

３．本システムの安全管理事項

３．１各システム設備の設置場所

K-MIX R のポータルシステムに接続する各システムに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。

① 一般的な事務室との共用、または隣接を避けていること。
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こと。
③ 設置場所の表示は最小限にとどめていること。
④ 出入り口は原則１ヶ所とし、施錠設備を設けていること。
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こと。
⑥ 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。
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こと。
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こと。

３．２設置場所の運用

各システム設備の設置場所の運用は次のとおりとする。

① 各システム設備設置室及び本システム用に隔離されたスペースは、不在時には施錠すること。
② 各システム設備設置室への入室は、認証装置等により特定の者に制限すること。
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、入室可能なものが同伴すること。
④ 入退室履歴を記録すること。
⑤ 各システム設備設置室内では許可なしに撮影、録音をしないこと。
⑥ 各システム設備設置室内には、必要なもの以外を置かないこと。
⑦ 本システム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。

３．３各システム設備の保守点検

保守点検のため、本システムの利用に影響が生じる場合は、予め日程と時間を本システムの利用者に伝えるものとする。

３．４各システムの運用監視

（１）安全かつ正常な稼働を確保するため、システムの運転状態を常に監視する対策を実施し、異常なシステムの動作、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。

（２）システムの稼働監視は、死活監視、システムアプリケーション応答監視を行うものとする。

（３）ファイアーウォール等のアクセスログの定期的チェックを行うものとする。

３．５ネットワークの管理

（１）システム管理者は、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。

（２）システム管理者は、定期的にログの収集を行い、ログを保管するものとする。

（３）利用するネットワークは、以下のものとする。

○ IP-VPN 方式の VPN ネットワーク

○ IPsec+IKE 方式の VPN ネットワーク

○ 通信経路の暗号化およびクライアント証明書を利用した認証に基づく、TLS 1.2（「CRYPTREC TLS 暗号設定ガイドライン：高セキュリティ型」） 方式の通信ネットワーク

３．６利用者のアクセス管理

（１）本システムへアクセスする場合は、診療で使用している端末を用いることとする。医療機関等のポリシーにより、診療で使用する端末とは別の端末を用いることも可とする。

（２）利用者は、運営管理責任者の指示の下、サポートデスクが発行した ID・パスワードを利用し、システム管理者は、アクセス管理を行うものとする。

３．７保守・運用者の電子記録媒体の管理

（１）システム管理者の許可を得た場合を除き、CD、DVD、USB メモリ、磁気テープ等（以下「可搬型記録媒体」）という。）への個人情報の複写を禁止するものとする。

（2） 可搬型記録媒体を利用する場合は、事前に利用方法を明確化した上で、システム管理者の許可を得ることとし、確認した方法以外での利用を禁止するものとする。

（3）システム管理者から許可を得た場合において、個人情報が格納された可搬型記録媒体は、施錠付キャビネット等に保管し、システム管理者は、台帳に記録し、管理するものとする。

3．8保守・運用者の情報の廃棄

（1） 紙媒体の廃棄は、原則シュレッダーによる粉砕処理によるものとする。大量廃棄する場合は、溶融廃棄証明書を受領することで、外部業者に委託することができるものとする。

（2） 電子媒体の廃棄は、原則粉砕処理によるものとする。

（3）粉砕処理をしない PC 等は、データの再生ができない方法で消去するものとする。なお、消去証明書を受領することで、データの消去処理を外部業者に委託することができるものとする。

（4）事業管理者が指定した重要な情報を廃棄する場合は、廃棄の結果の報告受け、運用管理責任者が確認するものとする。

3．9データのバックアップ

（1）サーバのシステムファイルおよびデータのバックアップを自動または手動で実施するものとする。

（2） バックアップの作業に当たる者は、その作業の記録を残すものとする。

4．本システムでの情報の取扱い

（1） 本システムが保存する情報は、複製情報として取り扱うものとし、情報の原本は情報を作成した医療機関等が法令に従い別途管理するものとする。

（2）本システムが取り扱う複製情報の内容は、事業管理者、事業実施責任者、医療機関等において、その完全性、正確性、適用性、有用性等のいかなる面からの保証をするものではないものとする。

５．業務委託の安全管理

５．１委託契約における安全管理

業務を外部に委託する場合は、委託契約書に以下の措置を実施するものとする。

①委託契約書には、守秘事項を含むものとし、契約先の契約署名者は代表者とするものとする。

②委託契約書には、再委託先に関する事項を加えるものとする。

③委託契約書の付帯条件として、サービス提供にあたって保障する品質と、事故・障害等が発生した際の補償について明確にするものとする。

５．２再委託先の安全管理

委託先が委託業務を外部に再委託する場合は、本ポリシーと同等の個人情報保護、安全管理に関する対策および契約がなされるものとする。

６．セキュリティポリシーの公開

本セキュリティポリシーは、本事業に参加する医療機関等および K-MIX R の利用者、患者等及び本システムの運営と構築等に係わる団体、法人等とその関係者に公開するものとする。

７．セキュリティポリシーの見直し

事業管理者は、システムの機能、運用状況等に問題がある場合には、必要な是正の実施および予防の実施を行うため、事前の了解なく本セキュリティポリシーを見直しすることができるものとする。

８．セキュリティポリシーの施行日

本セキュリティポリシーは、令和３年４月１日より施行する。

以上