資料３（和歌山）

医療情報連携基盤の全国展開に向けた
EHR ミニマム基盤モデルの実証事業
（和歌山県）

青洲リンク接続インタフェースに係るセキュリティ要件

Ver.1.0

平成　26 年　12 月　22 日

青洲リンク協議会

目次

１．概要

１．１ 件名

きのくに医療連携システム青洲リンク接続インタフェースに係るセキュリティ要件

１．２ 現システムの概要

きのくに医療連携システム青洲リンク（以下「青洲リンク」という。）は、南海トラフ巨大地震による津波に備えるため厚生労働省「医療情報連携・保全基盤推進事業」に基づき、公立大学法人和歌山県立医科大学（以下「県立医大」という。）が「平成24年度医療情報・保全システム構築業務」として株式会社サイバーリンクスに委託し構築したシステムであり、各病院は標準的な診療情報形式SS-MIX2（Standardized Structured Medical Information Exchange)、診療所はレセプト電算データで連携している。

平成 25 年度 4 月より、和歌山県内の和歌山県立医科大学附属病院とともに国立病院機構南和歌山医療センター、新宮市立医療センター、紀南病院、白浜医療福祉財団白浜はまゆう病院、国保すさみ病院、くしもと町立病院、那智勝浦温泉病院（以下「参加病院」という。）、が青洲リンクに参加し、その参加病院は青洲リンクの運用を株式会社サイバーリンクスに委託し、クラウド型医療情報連携システムが運用されている。

また、青洲リンクは医療再生基金に基づき平成２５年度より３ヵ年計画で県立医大が「きのくに医療連携システム青洲リンク機能拡張業務」として、調剤薬局は NSIPS、検査センターは SS-MIX2 拡張ストレージで連携、参加病院医用画像の連携等、順次サービス機能の拡充を行うとともに参加病院、診療所の拡大に取組んでいる。

さらに、今般、青洲リンクは総務省「平成２５年度医療情報連携基盤の全国展開に向けたＥＨＲミニマム基盤モデルの実証事業」の実証フィールド和歌山のシステムとして参加し、地域包括ケアシステムとして歯科医院、訪問看護ステーション、調剤薬局、介護事業所等との連携を行い、医療情報連携基盤の運営事例として取り組み、ミニマムの求められる機能について検討することになった。

このため、きのくに医療連携システム青洲リンクの接続インタフェースで必要となるセキュリティ要件を満たすための方法について、安全性や妥当性の観点から検討を行うものである。

１．３ 範囲

きのくに医療連携システム「青洲リンク」の接続インタフェースに係るセキュリティ要件の範囲は、和歌山県全域における病・病・診・在宅医療/介護に関する医療・介護情報連携、及び地域医療再生基金を活用したその他のＩＣＴ関連事業に関するシステムの情報連携を実現するために必要な次のものを対象範囲とする。

(1)各医療圏内での病・病・診・在宅医療/介護連携を実現するための接続インタフェース

(2) 各医療圏を越えた病・病・診・在宅医療/介護連携を実現し、さらに関連するその他のＩＣＴ関連事業システムとの情報連携を実現するための接続インタフェース

２．セキュリティ要件

２．１ ネットワークに関する要件

(1) 医療機関・薬局は IPSec＋IKE 方式の VPN ネットワークを利用し、介護事業所・訪問看護ステーションは SSL 暗号化通信を利用する。

(2) データセンターと青洲リンクに参加している病院との間で診療情報保全を行う場合、セキュアなネットワークを利用する。

(3) 病院間で通信を行わないようにする。

２．２ システムアクセスに関する要件

(1) システムの利用者等は、ID・パスワードを用いてシステム利用者の認証を行う。

(2) パスワード再入力に伴う回数制限、認証不成功時の対応を設定する。

(3) システム利用者のアクセスコントロールを行い、必要最低限の操作に制限する。

２．３ システムアクセスに使用する機器に関する要件

(1) 参加施設の責任者が保有する利用者情報を取り扱う機器等について、自己の責任により厳重な管理を行う。

(2) 本システムと接続する機器等と外部との接続には、厳重なセキュリティ対策を講じる。

(3) 本システムと接続するパソコン等は、OS 等のセキュリティ対策のアップグレードを行い、ウイルス対策ソフトウェアをインストールし、常に最新の定義ファイルに更新する。

(4) システムの構成機器は、セキュリティ区画に設置する。

(5) Winny、P2P ファイル交換ソフトウェア等をインストールしない。

(6) OS のログイン認証にはパスワード認証を設定し、定期的に変更を行う。

２．４ データセンターに関する要件

(1) 安全な稼働をするため、システム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) ファイアーウォールのアクセスログの定期的チェックを行うものとする。

(3) 本システムの構成機器は、データセンター内のセキュリティ区画内に設置されるものとする。

(4) データセンターは安定した電源供給設備を有し、非常用電源設備（UPS）を備え、停電時のシステム稼働に備える。

(5) サーバーのハードディスクの冗長性を向上させ、機器故障時にシステムが停止しないように備える。

(6) サービス稼働率については、以下の目標値を設定する。

通常業務時間帯　　９９．９５％
その他の時間帯　　９９．９５％

２．５ システム運用管理者に関する要件

(1) システム運用管理者は、安全な稼働をするため、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) システム運用管理者は、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) システム管理者、ネットワーク管理者のアクセス制限をする。

(4) リモートメンテナンスのために行うリモートログインは、必要最小限の範囲で実施する。