きのくに医療連携システム青洲リンク情報セキュリティポリシー

1. 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、和歌山県地域における医療機関の医療情報を標準的な形式で外部保存し、連携する医療機関で相互参照することにより緊密な医療連携の促進を図るとともに、災害などの非常時に情報参照として活用することで地域住民への質の高い安全な診療を提供することを目的としている。

各医療機関から集められた医療情報は慎重な取扱いを要する要配慮個人情報であり、漏洩、損傷等の事故があった場合に極めて重大な結果を招くおそれがある。

そこで、青洲リンク協議会（以下「協議会」という。）では、地域住民が安心、信頼して青洲リンクを利用できるよう、青洲リンク情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）を定める。

青洲リンク利用者（以下「利用者」という。）は、このルールを理解し、遵守しなければならない。

2. 適用範囲

(1) 組織

情報セキュリティポリシーの適用範囲は、青洲リンクを利用する全ての利用者とする。

(2) ネットワーク

青洲リンクで使用される情報通信機器及び通信回線とする。

(3) 情報システム

青洲リンクで使用されるネットワーク、ハードウェア、ソフトウェア及び記憶媒体で構成された情報を処理する仕組みとする。

(4) 情報資産

情報セキュリティポリシーが適用される情報資産は以下のものとする。

- 青洲リンクで使用されるネットワーク及び情報システムの開発、保守及び運用に係る全ての文書、図画、写真並びに電磁的記録
- 青洲リンクで扱う全ての電磁的記録

3. 情報資産に対する脅威とその対策

(1) 情報資産に対する脅威

情報資産に対する脅威の発生度合や発生した場合の影響を考慮すると、特

に認識すべき脅威は以下のとおりである。

・不正アクセス又は不正操作によるデータ又はプログラムの持ち出し、盗聴、改ざん、消去、機器及び媒体の盗難、規定外の端末接続によるデータ漏洩等
・利用者及び部外受託者による誤操作
・地震、落雷、火災、風水害等の災害によるサービスの停止
・事故、故障、障害などによるサービスの停止

(2) 情報セキュリティ対策

前項で示した脅威から情報資産を保護するために、以下のセキュリティ対策を講ずる。

ア. 物理的対策

情報システム及びネットワークを設置する施設への不正な立ち入り、並びに情報システム、ネットワーク及び情報資産への損傷・妨害等から保護するための物理的な対策に努める。

イ. 人的対策

情報セキュリティに関する権限及び責任を定め、職員等に基本方針、情報セキュリティに関する法令などの内容を周知徹底する等、十分な教育及び啓発が行われるよう必要な対策を講ずる。

ウ. 技術的対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策を講ずる。また、情報システム及びネットワークの可用性を確保するために、必要な技術面の対策を講ずる。

エ. 運用上の対策

システム開発の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等、運用面の対策を講ずる。

4. 情報セキュリティポリシーの取扱い

情報セキュリティポリシーは、地域住民から預かっている情報の管理方針と位置づけ、広く公開するものとする。また、青洲リンクの情報資産を取扱うすべての利用者に対し、周知徹底する。

5. 職掌上の役割と責任

(1) 協議会長

協議会長は、セキュリティに関する指針を明らかにし、利用者及び部外受託者に対してセキュリティ意識を浸透させ、必要な支援をする役割と責任を持

つ。

(2) 各医療機関における青洲リンクシステム運用責任者

各医療機関における青洲リンクシステム運用責任者（以下「システム運用責任者」という。）は、セキュリティ確保の責任を負い、職員及び業務関係者が、情報セキュリティポリシー及びそれに基づく実施手順等を理解し遵守することを徹底し、かつ管理する。また、システム運用責任者は、部外受託者が契約終了した場合に、青洲リンクから取得させた情報資産がある場合は、当該情報資産をすべて再利用できない状態にして廃棄させなければならない。

(3) 利用者

利用者は、情報セキュリティポリシー及びそれに基づく実施手順等及びシステム運用責任者の指示を遵守し、情報が不正な手段で取得されること又は不正に使用されることを防止する責任を負う。利用者は、青洲リンクの利用資格を喪失するなど青洲リンク情報資産の取扱いができなくなった時点で、青洲リンクから取得した情報資産がある場合は、当該情報資産をすべて再利用できない状態にして廃棄しなければならない。

(4) 部外受託者

部外受託者は、契約に基づき情報セキュリティポリシー及びそれに基づく実施手順等及びシステム運用責任者の指示を遵守し、情報を不正に取得又は不正に使用してはならない。部外受託者は、契約終了その他を原因として、青洲リンク情報資産の取扱いができなくなった時点で、青洲リンクから取得した情報資産がある場合は、当該情報資産をすべて再利用できない状態にして廃棄しなければならない。

6. セキュリティの管理体制及び組織

(1) 管理体制

ア. 最高統括責任者（CIO）

青洲リンクにおけるセキュリティを含む情報管理全般に関する最高責任者であり、全ての責任及び権限を有し、協議会長がその任に当たる。

イ. 情報セキュリティ統括責任者（CISO）

青洲リンクにおける情報セキュリティに関する責任と権限を有し、協議会事務局長がその任に当たる。

ウ. 情報セキュリティ管理責任者

各医療機関における情報セキュリティに関する責任と権限を有し、システム運用責任者がその任に当たる。

(2) 組織

ア. 情報セキュリティ委員会

情報セキュリティに関する重要な事項を審議し決定する。また、業務遂行上やむを得ず情報セキュリティポリシーを適用できない事態についての判断を行う。

イ. 情報セキュリティ委員長

情報セキュリティ統括責任者がその任に当たる。

(3) セキュリティに関する教育

情報セキュリティ管理責任者は、情報セキュリティポリシーの職員等への浸透と情報セキュリティ意識向上のため、情報セキュリティに関する教育プログラムを策定し、それを実施する。

7. 関係法令の遵守

青洲リンクを利用する際には、使用する情報資産について、関連する法令を遵守し、これに従わなければならない。