

おきなわ津梁ネットワーク「情報セキュリティ基本方針」

第 3.0 版

平成 30 年 2 月

一般社団法人 沖縄県医師会

改定履歴

版数	日付	内容
第 1.0 版	平成 24 年 10 月 9 日	新規制定
第 2.0 版	平成 28 年 1 月 12 日	参加機関拡充に伴う、文言の修正等
第 3.0 版	平成 30 年 2 月 6 日	機能拡充に伴う、文言の修正等

目 次

理 念	1
1. 目的	1
2. 構成と位置付け	1
3. 定義	2
4. セキュリティーの適用範囲	2
5. 基本原則	2
6. 適用対象者	2
7. 事故の予防と対応	2
8. 管理体制	3
9. 情報システムの運用責任者	3
10. 情報の管理	3
11. 保管期間	3
12. 利用者識別	3
13. 苦情・質問の受付	3
14. 公開基準	3
15. 標準規格・関連法令	4
16. 教育	4
17. 監査	4
18. 文書の改廃	4

理 念

おきなわ津梁ネットワーク（以下、「本ネットワーク」）では、厚生労働省が推進している医療情報の共有化を念頭に、正確な情報に基づいた高度で安全な医療を行うことを目的としております。充実した医療情報の共有には地域医療連携の体制づくりが必須であり、その手段として IT 活用が必要不可欠な時代となっております。

島嶼県である沖縄にとっては、遠隔地との連携手段として IT を利用した医療機関ネットワークの構築が急務とも言え、多くの情報がシステム化されることによりその利便性は計り知れないものがあります。しかしながら一方では、コンピュータウイルス、不正アクセス、過失などによる情報の改ざんや破壊、機密情報漏洩など、あらゆるリスクが点在し、IT 活用における医療連携体制の確立には様々な課題が考えられます。特に、医療機関のような医療・健康情報を取り扱う事業者では、万一漏洩事故が発生すると個人の人生に及ぼす影響は非常に大きく、一般の企業と比べ特に留意が求められます。

情報セキュリティポリシーは、本ネットワークで取り扱う個人情報等を、故意、過失、偶然の区別に関係なく、改ざん、破壊、漏洩から保護されることを目的とした方策をまとめたものです。本ネットワークに係わる、おきなわ津梁ネットワーク事務局、各医療機関や歯科診療所、保険薬局、医療保険者（以下「参加機関」という）は、情報セキュリティの重要性を認識し、安全で適切な取り扱いに努めるべく、下記の基本方針を元に運用致します。

1. 目的

情報セキュリティポリシー（以下、「ポリシー」という）とは、組織の中にある情報を、安全に運用するための規約を文書化したものをいう。

おきなわ津梁ネットワークに参加する全ての利用者が情報セキュリティの重要性を共通の認識として理解し、個人情報の取扱いに対して安全かつ適切な運用を行うことで社会的信頼性を保ち、安心しておきなわ津梁ネットワークに参加して頂けることを目的とします。

2. 構成と位置付け

本ポリシーは、情報セキュリティ基本方針、運用管理規程、利用者規程の 3 つの階層によって構成されます。

- ◆情報セキュリティ基本方針：おきなわ津梁ネットワークの情報システムに関する安全管理への取組みを指針として定めたもの
- ◆運用管理規程：基本方針を受け、それを各項目に遵守すべき事項について、組織的対策、

技術的対策、人的対策毎に具体的にまとめたもの

◆利用者規程：運用管理規程を受け、主にシステムの利用者である参加機関が遵守すべき事項について具体的にまとめたもの

3. 定義

本ポリシーで指す情報システムとは、本ネットワーク参加機関で得た個人情報、健康情報をシステム化したもの、あるいは参加機関のシステム並びに接続機器など健康情報を取り扱うシステム全般をいいます。また将来、他地域における同種の「地域医療介護ネットワーク」と連携または接続した場合には、それらの「地域医療介護ネットワーク」を取り扱うシステム全般（ネットワーク端末、デバイス等）を含みます。

4. セキュリティーの適用範囲

ポリシーの適用範囲は、本ネットワークの情報システムで取り扱う電子情報のみならず、本システムへ入出力する際に用いる紙媒体の情報も含むこととします。また将来、他地域における同種の「地域医療介護ネットワーク」と連携または接続した場合には、それらの「地域医療介護ネットワーク」を取り扱う情報全般（電子情報、紙媒体等）を含みます。

5. 基本原則

本ネットワークの情報システムは、下記に挙げる基本原則に則り運用します。

- ① 保存義務のある情報の電子媒体による保存については、情報の真正性、見読性、保存性を確保する。
- ② 情報システムの利用に当たっては、守秘義務を遵守し、患者個人の情報を保護する。
- ③ 情報システムへのコンピュータウイルスの侵入及び外部からの不正アクセスに対して必要な対策を講じる。原則、ソフトウェアのインストール及び USB メモリ等の外部記憶媒体の接続を禁止する。
- ④ 原則、BYOD（私的デバイス利用）での接続を禁止する。
- ⑤ 参加施設において購入または契約した端末について、本ネットワークの情報システムへの接続が認められた場合、業務使用デバイス利用同意書を提出し、承認を受けたうえで利用する。

6. 適用対象者

ポリシーは、職責に問わず、本ネットワーク参加機関に属する全ての利用者に対して適用する。ただし、ポリシーの対象となる業務を外部に委託する場合には、別途、本ポリシーに準拠した内容の外部委託契約を締結しなければならない。

7. 事故の予防と対応

おきなわ津梁ネットワーク運営協議会（以下「運営協議会」とする）は、ポリシーに基

づいた情報セキュリティ対策を講じ、指針を遵守することで事故の予防に務める。万一、事故が発生した場合には、その事実を速やかに公表し、再発防止策を含む適切な対策を速やかに講じる。

8. 管理体制

ポリシーの維持管理は、運営協議会が行う。各参加機関の長は、運営協議会の指示を受け、各参加機関に置いてポリシーが遵守されるように指導、教育を行う。

9. 情報システムの運用責任者

情報システム運用責任者（以下、「運用責任者」という）を置き、おきなわ津梁ネットワーク運営協議会委員長（以下、「運営協議会委員長」という）をもってこれに充てる。運用責任者は、医療情報システムの安全管理に必要な、組織的、人的、技術的、物理的対策を実施し、維持し、かつ、改善するために不可欠な資源を用意する。また、情報システムを円滑に運用するため、情報システムに関する運用を担当するシステム管理者を、運営協議会委員長は内部の者から指名することができる。

10. 情報の管理

情報システムで取り扱う情報の取り扱いは、情報の取得から利用・保管・廃棄までの情報の取扱いの流れに沿ったリスク分析を実施し、リスクに対応した適切な取り扱い方法を運用管理規程等に規定し、適切に管理・運用する。

11. 保管期間

情報システムで取り扱う情報の保管期間は、法令保管期間を基本として別途定める。また、情報システムへのアクセスログを記録し、その記録を最低 5 年保管するものとする。

12. 利用者識別

情報システムの利用者の登録を管理し、そのアクセス権限を定め、不正な利用を管理・防止する。

13. 苦情・質問の受付

運営協議会は、個人情報の取扱い及び情報システムの運用に関して、本人及びシステム利用者からの苦情及び質問を受け付け、適切かつ迅速な対応を行う。

14. 公開基準

ポリシーは全利用者に対して公開する。IT 技術が日々発展していることと社会環境が変化することを踏まえて適時改訂を行うことがあるが、改訂によって変更された箇所についても、改訂後即時に全利用者に向けて公開する。また、公開されたポリシーは重要機密情報である事を十分に認識した上で取り扱い、原則として外部に公開してはならない。

15. 標準規格・関連法令

運営協議会は、標準規格等についての改訂状況を確認し、改正が行われた際には、整合性を維持するためにはその内容に準拠した改訂を行う。

16. 教育

運営協議会は、個人情報を利用する全ての利用者に対して、情報セキュリティの重要性と、個人情報の適切な取り扱い、及び安全管理について意識面及び技術面の向上を目的として、継続的な教育を行う。

17. 監査

情報システムの適正な運用とその有効性を維持するために、毎年 1 回内部監査を実施する。但し、高度な技術を要する監査が必要な場合は、外部の専門家による外部監査を導入する。運用責任者は、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じる。

18. 文書の改廃

ポリシーを改訂する際は、運営協議会の議を経て、沖縄県医師会理事会の承認を必要とする。