

滋賀県医療介護情報連携ネットワーク
(びわ湖あさがおネット)

情報セキュリティ基本方針

特定非営利活動法人

滋賀県医療情報連携ネットワーク協議会

目次

1. 序説	1
1.1. 目的	1
1.2. 情報セキュリティポリシーの構成と位置づけ	1
1.3. 用語の定義	1
1.4. 適用範囲	1
1.5. 適用者	1
2. 情報の分類と管理	2
2.1. 情報の分類と対象	2
2.2. 情報の管理	2
2.3. 保管期間	2
3. 組織・体制	2
3.1. 体制	2
3.2. 管理者・責任者	2
3.3. 参加施設の窓口担当者	2
3.4. 委託先の管理	2
3.5. 情報セキュリティポリシーの公開	3
4. 物理的セキュリティ	3
4.1. 入退室管理	3
4.2. 災害・障害対策	3
4.3. 可搬型記録媒体、利用者端末（ノートPC、タブレット端末）の管理・取り扱い	3
5. 技術的セキュリティ	3
5.1. ネットワーク管理	3
5.2. システムの監視	3
5.3. アクセス管理	4
5.4. 情報システムのサービス継続	4
5.5. システムの更新・ウイルス対策	4
6. 人的セキュリティ	4
6.1. ID管理	4
6.2. パスワード管理	4
6.3. 利用者の責務	4
6.4. 教育・訓練	5

7. 監査・更新	5
7.1. 監査	5
7.2. 更新	5
7.3. 法令遵守	5
附則	5

1. 序説

1.1. 目的

滋賀県医療情報連携ネットワーク協議会（以下、「当協議会」という）では、滋賀県全域において、医療・介護・福祉等の関連諸機関が相互に医療情報等を活用できる環境を実現するため、「滋賀県医療介護情報連携ネットワークシステム」（以下、「本ネットワーク」という）の基盤整備および運用を主たる事業とし、全県にわたる機能的かつ安全な医療介護情報連携体制の構築に取り組む。また将来的には、蓄積された情報を疾病予防の情報解析に活用することを目指している。

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情報を、故意、過失、偶然の区別に関係なく、改ざん、破壊、漏洩から保護すると共に、情報を利用する当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、および個人情報の適切な取り扱いと保護についての認識を高め、連携基盤および連携基盤に接続する各連携システムを安全かつ効果的に運用することを目的として制定する。

1.2. 情報セキュリティポリシーの構成と位置づけ

情報セキュリティポリシー（以下、「ポリシー」）は、「情報セキュリティ基本方針」（本文書）、「運用管理規程」、「運用マニュアル」の3つの階層によって構成されている。

- ・ 「情報セキュリティ基本方針」
当協議会の情報セキュリティ管理における基本姿勢を示したもの
- ・ 「運用管理規定」
基本方針を受け、項目毎に遵守すべき事項について具体的にまとめたもの
- ・ 「運用マニュアル」
運用管理規程を受けて実際の運用方法、様式、操作手順について示したもの

1.3. 用語の定義

- ・ 「滋賀県医療介護情報連携ネットワークシステム」
連携基盤および連携基盤に接続する各連携システム（地域連携システム、小規模医療機関情報システム、在宅療養支援情報システム）

1.4. 適用範囲

ポリシーの適用範囲は、滋賀県医療介護情報連携ネットワークシステムに関連する人的・物理的・環境的リソースとする。

1.5. 適用者

本ポリシーの適用者は、当協議会の業務に関わるすべての構成員（役員、システム参加施設・利用者、運営事務局）とする。

2. 情報の分類と管理

2.1. 情報の分類と対象

本ポリシーの適用情報は、連携基盤および接続される各連携システムが取り扱う情報（診療情報、介護情報、利用者情報、利用者の診療情報や介護情報へのアクセスログなど）とする。また、情報システムへ入力する前の紙媒体の情報も含むものとする。

2.2. 情報の管理

本ネットワークで取り扱う情報に対しては、情報の取得から利用・保管・廃棄まで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」、「運用マニュアル」に規定し、適切に管理・運用する。

2.3. 保管期間

本ネットワーク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。

3. 組織・体制

3.1. 体制

本ポリシーに基づいた運営を実現するために、適切な管理体制・実施体制を構築する。本ポリシーの維持・管理は、本協議会が行う。

3.2. 管理者・責任者

本協議会の理事長を責任者とし、責任者が指名する管理者によって、ポリシー遵守状況の確認、改訂の検討を行う。また、責任者は、本ネットワークの安全管理に必要な、組織的、物理的、技術的、人的対策を実施し、維持し、かつ、改善するために不可欠な資源を用意する。

3.3. システム参加施設の窓口担当者

本協議会に所属する各参加施設は、協議会からの連絡窓口となる担当者を指名し、本ネットワークの業務に関わる連絡・依頼等への対応を行う。

3.4. 委託先の管理

本協議会から業務を委託する場合は、同等以上のセキュリティポリシーを遵守可能であることを確認したうえで契約し、契約締結後も適切に維持管理されているか定期

的に監査を行う。

3.5. 情報セキュリティポリシーの公開

本ポリシーは本協議会の全構成員に対して公開する。ICT が日々発展していることと社会環境が変化する事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、改訂後即時に全構成員に向けて公開する。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。

4. 物理的セキュリティ

4.1. 入退室管理

本ネットワークの機器が設置される場所については、業務上必要とする者以外が許可なく出入りしないように、入退室管理を実施する。なお、データセンター事業者等を利用する場合は、同等の管理レベルとなるようにする。

4.2. 災害・障害対策

本ネットワークでは、地震、火災等の災害や、断線、接触不良等の障害に備えて、機器、回線の冗長化等の必要な保安措置を講じる。

4.3. 可搬型記録媒体、利用者端末（ノートPC、タブレット端末）の管理・取り扱い

本ネットワークにおいて、盗難や紛失、不正使用等による情報漏洩を防止するため、可搬型記録媒体、利用者端末（ノートPC、タブレット端末）の管理方法を明確にし、適切に取り扱う。

5. 技術的セキュリティ

5.1. ネットワーク管理

本ネットワークを介して医療情報を交換するにあたり、交換する情報の機密度を考慮して適切な対策を講じる。対策を実施する際は、オブジェクトセキュリティとチャネルセキュリティの両面を考慮する。

5.2. システムの監視

本ネットワークでは、セキュリティ侵害およびその兆候の早期発見と対応のために、監視とその記録を行う。なおその際には、個人のプライバシーに配慮した上で、監視の目的を達成するために必要な範囲で行う。

各システムの情報セキュリティを侵害する行為ならびに機密情報の漏洩等を発見した場合は、所定の連絡体制に則り直ちに関係各所へ連絡することとし、管理者はすみやかに所要の措置をとる。

5.3. アクセス管理

本ネットワークの利用者は、情報または情報システムにアクセスするに先立ち、識別・認証後に情報にアクセスするための正当な権限をもっているか審査され、認可されなければならない。

管理者は、アクセス権限を設定し、利用者がアクセスに際して正当な権限を有しているか審査する仕組みを設けなければならない。

利用者の識別・認証に必要とされる情報は、本人しか知り得ない状態に保ち、漏えいには十分留意する。

5.4. 情報システムのサービス継続

本ネットワークのサービスの中断等により事業の継続が脅かされることを回避し、影響を極力軽減するため必要なセキュリティ対策を実施する。

5.5. システムの更新・ウィルス対策

本ネットワークの安全性を確認・維持するため、ウィルス対策を実施し、パターンファイルの更新を行う。また使用するソフトウェアのセキュリティホール等が確認された場合には、詳細を確認の上、すみやかに対策を講じる。

6. 人的セキュリティ

6.1. ID 管理

利用者は情報資産にアクセスするに先立ち、個人を一意に特定するために付与される識別子（ID）によって識別され、パスワード等によって認証される。自分に対して付与されたID以外のものを利用してはならない。

6.2. パスワード管理

本ネットワークの利用者は、推測が困難なパスワードを選択し、他人に漏れないように秘密に管理しなければならない。

6.3. 利用者の責務

本ネットワークの利用者は、システムの安全かつ適正な利用に努め、情報が保護されるようにしなければならない。

6.4. 教育・訓練

管理者は本ネットワークの利用に必要なマニュアル等を整備し、すべ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、および安全管理について意識面および技術面の向上を目的として、継続的な教育を行う。

7. 監査・更新

7.1. 監査

責任者は、本ネットワークを円滑に運用するため、本ネットワークに関する監査を担当する監査責任者を任命し、定期的な監査を実施させる。問題点が確認された場合は、ただちに必要な対策を講じる。

7.2. 更新

本ポリシーは、本協議会での議論・承認を経て変更する場合があります、その場合には、利用者の利用条件等について、変更後のポリシーで運用する。

7.3. 法令遵守

本協議会では、不正アクセス禁止法、個人情報保護法等の法令、国が定める指針その他の規範を遵守する。関係法令改正が行われた際には、整合性を維持するためにその内容に準拠した改訂を行う。

附則

本情報セキュリティ基本方針は、平成 26 年 7 月 1 日より適用する。

本情報セキュリティ基本方針は、令和 3 年 4 月 1 日より適用する。

本情報セキュリティ基本方針は、令和 4 年 7 月 14 日に改訂し、令和 4 年 7 月 28 日より適用する。