FiNE-LINK⁺ セキュリティ社内規定

1. 目的

この規定は、介護医療地域ネットワーク FiNE-LINK⁺（以下、「本サービス」という）における利用者様の医療情報、個人情報、および関連するすべての情報資産を保護し、安全かつ安定的なサービス提供を行うための基本的なルールを定めるものです。

2. 対象となる情報資産

本サービスに関連するすべての有形・無形の情報（デジタルデータ、物理文書、システム、サーバー、ネットワーク機器、ソフトウェア、知的財産、人的資源など）を対象とします。これらの情報資産は、「機密性」「完全性」「可用性」の観点から分類され、適切に管理されます。

3. セキュリティ管理体制

情報セキュリティ対策を組織的に推進するため、以下の体制と役割を定めます。

- **情報セキュリティ責任者**: セキュリティポリシーの策定、改訂、運用、監査、改善を統括し、インシデント発生時の最終責任を負います。
- **情報セキュリティ委員会（または担当者）**：セキュリティ対策の立案、実行、効果測定、全従業員への教育・訓練、内部セキュリティ監査を実施します。
- **全従業員**: 本規定および関連規定を遵守し、情報セキュリティ教育・訓練を積極的に受講します。不審な活動やセキュリティ問題を発見した場合は、速やかに情報セキュリティ責任者または担当者に報告します。

4. アクセス管理

情報資産への不正アクセスを防止するため、以下の措置を講じます。

- **認証**: LINE WORKS または付帯システムへのアクセスは、ユーザー名と強固なパスワードによる認証を基本とし、多要素認証（MFA）の導入を推進します。不正ログイン試行に対してはアカウントロックアウトポリシーを導入します。
- **認可（権限管理）**：「最小権限の原則」に基づき、業務内容に応じた必要最小限のアクセス権限を付与し、異動・退職時には速やかに見直します。
- **ログ管理と監視**: システムへのログイン、情報へのアクセス、重要なシステム操作など、すべての活動の詳細なログを取得し、改ざん防止措置を講じた上で法令に基づき安全に保存します。

5. ネットワークセキュリティ

LINE WORKS のセキュリティ思想に基づき、以下の対策を講じます。

- **ファイアウォール**: 外部からの不正侵入を防ぐため、ネットワーク境界に多層的なファイアウォールを設置し、必要な通信のみを許可します。
- **VPN**: 外部からのアクセスには、VPN などの暗号化された安全な通信経路を必須とします。
- **IDS/IPS**: 不正侵入検知・防御システムを導入し、サイバー攻撃パターンや異常な振る舞いをリアルタイムで検知・遮断します。
- **ネットワークセグメンテーション**: ネットワークを複数のセグメントに分割し、被害拡大を限定します。

6. システムセキュリティ

システム（サーバー、アプリケーション、データベース、OS など）のセキュリティを確保するため、以下の対策を講じます。

- **脆弱性管理とパッチ適用**: ソフトウェアの脆弱性情報を常に監視し、定期的な脆弱性診断を行

い、セキュリティパッチを速やかに適用します。

- **マルウェア対策**: サーバーおよびクライアント端末に最新のアンチウイルスソフトウェアおよび EDR ソリューションを導入し、リアルタイムスキャンを有効にします。
- **設定管理**: 業界標準に基づいた安全な設定を標準化し、厳格な変更管理プロセスに従って運用します。
- **ログ管理**: システムの詳細なログを一元的に取得し、SIEM に集約してリアルタイム分析を行い、脅威の早期発見に活用します。
- **セキュリティ監査**: 定期的に内部監査を実施し、セキュリティ対策の実効性を評価・改善します。

7. データ保護

利用者様の医療情報および個人情報を保護するため、以下の対策を講じます。

- **データの暗号化**: 通信経路上のデータ（TLS 1.2 以降）と保存データ（AES 256 ビットなど）の双方で強力な暗号化を適用し、暗号鍵を厳格に管理します。
- **バックアップと復旧**: 全ての重要データを定期的にバックアップし、運用環境とは物理的に分離されたセキュアな環境に保管します 。迅速なデータ復旧のため、復旧手順を確立し定期的にテストします。
- **データの廃棄**: 不要となったデータは、法令およびガイドラインに基づき、完全に復元不可能な方法で安全に廃棄します。