介護医療地域ネットワーク FiNE-LINK⁺

における安全管理規程

医療情報システムの安全管理に関するガイドライン（第 6.0 版）準拠

発行元:：株式会社 AGEN　FiNE-LINK⁺ サービス提供事業者

LINE WORKS 共同プロジェクト

1. はじめに

本セキュリティポリシーは、介護医療地域ネットワーク FiNE-LINK⁺（以下、「本サービス」という。）において、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厳格に保護し、安全かつ安定的なサービスを提供するための揺るぎない基本指針を定めるものです。医療情報は、その性質上、極めて機微な個人情報であり、その漏洩や改ざんは、利用者様の尊厳を著しく損ねるだけでなく、社会的な信頼を失墜させる重大な事態を招きかねません。

このため、本ポリシーは、厚生労働省が定める「医療情報システムの安全管理に関するガイドライン」に厳密に準拠し、さらにシステムのセキュリティ基盤においては、LINE WORKS の最新のセキュリティホワイトペーパー（2023 年 7 月版を参照）に示される先進的なセキュリティ思想と実践的な対策を深く取り入れ、策定されました。FiNE-LINK⁺は、介護・医療・障害事業者の皆様が、安心して情報連携を行えるセキュアな環境を提供することを最優先事項とし、情報セキュリティを継続的に向上させるため、技術的・組織的側面から常に最新の対策を講じてまいります。これにより、利用者様への高品質なケアの提供に貢献するとともに、地域医療・介護連携の信頼性を確固たるものとします。

2. 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かつ実効的に推進するため、本サービスでは以下の多層的な管理体制を構築し、役割と責任を明確化します。

- **情報セキュリティ責任者**:
    - 本ポリシーの策定、定期的な改訂、実施、運用、監査、および継続的改善のすべてを統括する最高責任者です。
    - 情報セキュリティに関するあらゆる意思決定（例えば、新規セキュリティ技術の導入判断や予算配分）と必要なリソースの確保を主導します。
    - 万が一セキュリティインシデントが発生した場合、その対応における最終的な責任を負い、組織全体を指揮します。定期的なリスク評価を通じて、常に最新の脅威に対応できる体制を維持します。
- **情報セキュリティ委員会（または担当者）**:
    - 情報セキュリティ責任者の強力なリーダーシップのもと、具体的なセキュリティ対策の立案、計画、実行、およびその効果測定を担います。
    - 全従業員を対象とした情報セキュリティ教育・訓練（例: フィッシング詐欺対策訓練）を企画・実施し、従業員全体のセキュリティ意識向上を図ります。
    - 定期的に内部セキュリティ監査を実施し、本ポリシーおよび関連規定の遵守状況、セキュリティ対策の実効性を客観的に評価し、改善点を特定・是正します。
- **全従業員**:
    - 本ポリシーおよび情報セキュリティに関する全ての関連規定、手順書を深く理解し、日常業務において厳密に遵守する義務を負います。
    - 情報セキュリティに関する最新の知識と意識を維持するため、定期的に実施される教育・訓練を積極的に受講します。
    - システム上の不審な活動、セキュリティ上の問題、またはインシデントの兆候を認識した場合（例: 未知のメールの添付ファイル、不審なログイン試行など）、速やかに情報セキュリティ責任者または指定された担当者に報告し、初期対応に協力します。この報告義務の徹底は、インシデントの早期発見と被害最小化に不可欠です。

3. 対象となる情報資産と情報の分類

本ポリシーが対象とする情報資産は、本サービスの提供・運用に関わるすべての有形・無形の情報（デジタルデータ、物理的な文書、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）を包含します。これらの情報資産は、その重要度に応じて「機密性（Confidentiality)」「完全性（Integrity)」「可用性（Availability)」の 3 つの側面から分類され、それぞれに最適な管理措置が講じられます。

- **福祉医療情報・個人情報**:
    - 利用者様の氏名、生年月日、連絡先、保険情報、病歴、診断結果、治療内容、処方薬剤情報、介護記録、身体機能評価、家族構成など、個人の特定に繋がり得る情報および医療・介護サービスの提供に直接関わる機微な情報がこれに該当します。
    - これらの情報は、最高レベルの機密性を要求し、厳格なアクセス管理（必要最小限の担当者のみがアクセス可能)、高度な暗号化（通信経路および保存データの双方)、詳細な操作ログの記録、および定期的なセキュリティ監査体制を適用することで、不正なアクセス、漏洩、改ざんから最大限に保護されます。
- **営業秘密・企業情報**:
    - 本サービスの運営に関わる独自のノウハウ、技術情報、システム設計書、サービス仕様、ビジネス戦略、顧客リスト、契約情報、財務情報、従業員情報などが該当します。
    - これらは高い機密性を要求し、厳密なアクセス制限、情報持ち出しの制限、電子メールやファイル共有における漏洩防止対策、契約による秘密保持義務の徹底を講じます。不正競争防止法等の関連法令も考慮し、その保護を徹底します。
- **公開情報**:
    - 本サービスの公式ウェブサイトや広報資料などで一般に公開されている情報（サービス概要、料金体系、ニュースリリース、お問い合わせ先など）がこれに該当します。
    - これらの情報は、その完全性（情報が正確で、改ざんされていないこと）と可用性（必要な時に確実にアクセスできること）を確保することが重要です。ウェブサイトの改ざん防止対策、コンテンツ管理システムのセキュリティ強化、サービス停止を防ぐための冗長化構成などを講じます。

4. アクセス管理

情報資産への不正アクセスを未然に防止するため、以下のアクセス管理策を多層的に徹底します。

- **認証**:
    - LINEWORKS または、それに付帯するシステムに関して、ユーザー名と強固なパスワードの組み合わせによる認証を基本とします。パスワードは、複雑性（英小文字、数字、の組み合わせ)、十分な長さ（最低 8 文字以上を推奨)、履歴管理（過去のパスワードの再利用禁止）を義務付け、定期的な変更を促します。
    - 不正なログイン試行や総当たり攻撃に対する防御として、アカウントロックアウトポリシー（一定回数の失敗で一時的にアカウントをロックする）を導入します。
    - 利用者様の利便性とセキュリティを両立させるため、多要素認証（MFA）の導入を推進します。
- **認可（権限管理）**:
    - 「最小権限の原則」に基づき、利用者の役割（例: 医師、看護師、ケアマネージャー、システム管理者など）およびそれぞれの業務内容に応じて、情報資産へのアクセス権限を厳密に最小限に推進します。

- アクセス権限は、従業員の異動や退職、業務内容の変更が発生した場合、速やかに見直し、不要な権限は即座に削除します。

- **ログ管理と監視（テナント管理者）**:
  - システムへのログイン（成功・失敗)、情報へのアクセス（発信、受信、削除)、重要なシステム操作（設定変更など）を含む、すべての活動について、詳細なログを時系列で把握し追跡することができます。
  - ログは、改ざん防止措置（ハッシュ化、デジタル署名など）を講じた上で、法令（例: 個人情報保護法）および「医療情報システムの安全管理に関するガイドライン」で定められた期間（最低でも数年間）安全に保存され、インシデント発生時の原因究明や法的証拠として利用されます。

5. ネットワークセキュリティ

LINE WORKS のセキュリティホワイトペーパーに示される高度なインフラストラクチャセキュリティの概念を参照し、本サービスにおいても以下の多層的なネットワークセキュリティ対策を講じます。

- **ファイアウォール**:
  - 外部からの不正な侵入を防ぐため、ネットワークの境界に多層的なファイアウォールを設置します。これには、パケットフィルタリング型、ステートフルインスペクション型、アプリケーションレベルゲートウェイ型など、複数の種類を組み合わせることで、より高度な防御を実現します。
  - 必要な通信のみを許可し、それ以外の不要なポートやプロトコルは厳しく制限または遮断する設定を行います。ファイアウォールルールは、定期的に見直され、最新の脅威やサービス要件に合わせて更新されます。
- **VPN（Virtual Private Network）**:
  - 外部の拠点（例: 自宅からのリモートアクセス、提携医療機関からの接続）から本サービスシステムへアクセスする際には、VPN などの暗号化された安全な通信経路を必須とします。
  - VPN は、公衆ネットワーク上に仮想的な専用回線を構築し、データが盗聴や改ざんから保護されることを保証します。認証されたユーザーのみが VPN 接続を確立でき、これによりセキュアなリモートワーク環境を提供します。
- **IDS/IPS（不正侵入検知・防御システム）**:
  - ネットワークトラフィックを常時監視し、既知のサイバー攻撃パターン（シグネチャベース）や異常な振る舞い（アノマリベース）をリアルタイムで検知する不正侵入検知システム（IDS）とそれを自動的に防御する不正侵入防御システム（IPS）を導入します。
  - これにより、SQL インジェクション、クロスサイトスクリプティング（XSS)、DDoS 攻撃などの多様な攻撃手法を早期に発見し、システムへの到達前に遮断することで、被害を未然に防ぎます。
- **ネットワークセグメンテーション**:
  - 本サービスのネットワークを論理的または物理的に複数のセグメント（区画）に分割します。例えば、Web サーバー、データベースサーバー、管理用サーバーなど、機能や重要度に応じてネットワークを分離します。
  - これにより、万が一、あるセグメントが攻撃を受けた場合でも、他のセグメントへの被害拡大を限定し、システム全体の可用性と安全性を高めます。セグメント間の通信は厳格なアクセス制御リスト（ACL）によって管理されます。

6. システムセキュリティ

LINE WORKS の高度なセキュリティ実装の考え方に基づき、本サービスのシステム（サーバー、アプリケーション、データベース、OS、ミドルウェアなど）のセキュリティを包括的に確保します。

- **脆弱性管理とパッチ適用:**
    - システムに使用されているすべてのソフトウェア（OS、ミドルウェア、アプリケーション）について、既知の脆弱性情報を常に収集・監視します。
    - 定期的に専門ツールを用いた脆弱性診断（外部からのペネトレーションテスト、内部からの脆弱性スキャン）を実施し、潜在的な弱点を特定します。
    - 発見された脆弱性に対しては、ベンダーから提供されるセキュリティパッチを速やかに適用するか、または、それが不可能な場合は代替の対策（回避策、アクセス制限強化など）を講じ、リスクを最小化します。パッチ適用は、システムの安定稼働に影響を与えないよう、計画的に実施されます。
- **マルウェア対策:**
    - サーバーおよびクライアント端末に、AI を活用した振る舞い検知機能も備えた最新のアンチウイルスソフトウェアおよび EDR（Endpoint Detection and Response）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。
    - 定義ファイルは常に最新の状態に自動更新されるように設定し、ランサムウェア、スパイウェア、ボットなどの多様なマルウェアや、標的型攻撃（APT）などの高度な脅威に対しても防御力を維持します。定期的なフルスキャンも実施します。
- **設定管理:**
    - システムの構築および運用にあたり、セキュリティガイドラインや CIS Benchmarks 等の業界標準に基づく安全な設定を標準化し、すべてのシステムに適用します。
    - 初期設定のパスワードの即時変更、不要なサービスやポートの無効化、最小権限でのプロセス実行など、セキュリティを考慮したベースライン設定を徹底します。
    - 設定変更は、変更管理プロセスに従い、厳格な承認フローと変更履歴の記録を義務付けます。設定の「ドリフト」（設定の意図しない変更）を定期的に検出し、是正する仕組みを導入します。
- **ログ管理:**
    - システムの稼働状況、エラー、セキュリティイベント、ユーザー操作に関する詳細なログ（例: どのユーザーが、いつ、どのファイルにアクセスしたか、どのコマンドを実行したかなど）を一元的に取得し、集中型ログ管理システム（SIEM: Security Information and Event Management）に集約します。
    - ログは、リアルタイムで分析され、異常なパターンや潜在的な脅威（例: 複数のシステムにおける不審なログイン試行の相関関係）の特定に利用されます。これにより、インシデントの早期発見とプロアクティブな脅威ハンティングが可能となります。
- **セキュリティ監査:**
    - システムの設定、ログ、運用手順、アクセス制御リストなどについて、定期的に内部監査を実施し、本ポリシーおよび関連規定の遵守状況、セキュリティ対策の実効性を評価します。
    - 監査結果に基づき、発見された脆弱性や改善点を特定し、是正措置計画を策定・実施します。監査は、セキュリティ対策の継続的な改善サイクルの一部として不可欠です。

7. データ保護

利用者様の医療情報および個人情報という極めて重要なデータを安全に保護するため、以下の包括的な対策を講じます。

- **データの暗号化**:
    - **通信経路上のデータ**: 本サービスと利用者端末間の通信、または内部システム間の通信は、TLS（Transport Layer Security）1.2 以降などの業界標準の強力な暗号化技術を用いて保護されます。これにより、データがインターネット経由で送信される際に、盗聴や改ざんから守られます。
    - **保存データ（データ at Rest）**: データベース、ファイルストレージ、バックアップメディアなどに保存されるデータは、AES 256 ビットなどの高度な暗号化アルゴリズムを用いて暗号化されます。これにより、万が一、物理的なストレージが不正に持ち出された場合でも、データの内容が保護されます。
    - 暗号鍵の管理は厳格に行い、鍵の生成、配布、保管、失効、破棄のライフサイクル全体を通じて、鍵の機密性と完全性を確保します。鍵管理システム（KMS）の利用を推進し、セキュアな運用を実現します。
- **バックアップと復旧**:
    - 全ての重要データについて、定期的に完全バックアップおよび差分/増分バックアップを取得します。バックアップ頻度は、データの重要度と変更頻度に応じて適切に設定されます（例: 毎日、毎週）。
    - バックアップデータは、運用環境とは物理的に分離されたセキュアなオフサイト環境に保管され、災害や大規模システム障害が発生した場合でも、データの損失を防ぎます。
    - 迅速なデータ復旧が可能なように、バックアップからの復旧手順を明確に確立し、定期的にテストを実施します。これにより、ビジネス継続計画（BCP）および災害復旧計画（DRP）の実効性を高め、サービス中断時間を最小限に抑えます。
- **データの廃棄**:
    - 本サービスから退会した利用者様のデータや、サービス利用終了により不要となったデータは、法令（例: 医療情報保護に関する法令、個人情報保護法）および「医療情報システムの安全管理に関するガイドライン」に基づき、完全に復元不可能な方法で安全に廃棄します。
    - デジタルデータについては、データ消去ソフトウェアによる上書き消去、または物理的な破壊（シュレッダー、磁気消去器（デガウザー）など）といった確実な方法を用います。物理的な記録媒体（HDD、SSD、USB メモリなど）の廃棄においても、データ消去の確実性を第三者機関が保証するような措置を講じます。

8. 物理的セキュリティ

本サービスに関連するサーバー、ネットワーク機器、データ、および従業員が利用する情報機器が設置されているデータセンターやオフィスに対し、多層的で厳格な物理的セキュリティ対策を講じます。

- **入退室管理**:
    - データセンターやサーバー室、重要な情報を取り扱うオフィスエリアへの入退室は、生体認証（指紋認証）、IC カード、物理鍵の組み合わせなど、厳格な認証メカニズムによって管理されます。
    - 許可された者のみが立ち入りを認められ、入退室の履歴は詳細に記録され、不審な活動がないか常時監視されます。訪問者には、一時的な入館証の発行と、常時監視下の入室を義務付けます。

- **監視**
    - 施設内には、24 時間体制で稼働する高性能な監視カメラを多数設置し、死角がないように徹底します。
    - 監視記録は、一定期間保存され、必要に応じて証拠として利用されます。
- **環境管理**:
    - サーバー機器の安定稼働と長期的な信頼性を確保するため、データセンター内では、適切な温度・湿度管理（空調システム）、安定した電力供給（UPS: 無停電電源装置、非常用発電機）、および高度な防火対策（ガス消火設備など）を講じます。
    - これにより、機器の故障やデータ破損のリスクを最小限に抑え、サービスの継続性を確保します。

9. インシデント管理

セキュリティインシデント（情報漏洩、不正アクセス、マルウェア感染、システム障害、サービス停止など）が発生した際の迅速かつ適切な対応体制を確立し、被害の最小化と早期復旧を目指します。

- **検知と報告**:
    - セキュリティ監視システム（SIEM、IDS/IPS、EDR など）やログ分析ツールを常時稼働させ、異常な活動やセキュリティ脅威の兆候を早期に検知します。
    - 従業員は、システムエラー、不審なメール、不審な外部からの連絡、またはインシデントの兆候を認識した場合、社内の定められた手順に従い、速やかに情報セキュリティ責任者または指定されたインシデント対応チームに報告することを義務付けます。報告を怠った場合には、厳正な社内規程に基づき適切に対処します。
- **対応と復旧**:
    - インシデント発生時には、情報セキュリティ責任者の指揮のもと、事前に策定されたインシデント対応計画（IRP: Incident Response Plan）に基づき、インシデント対応チームが迅速に行動します。
    - 対応フェーズには、被害の拡大防止（システムの隔離、サービスの停止）、原因究明、根絶（マルウェアの駆除、脆弱性の修正）、復旧（システムの再構築、データ復元）、そして最終的な正常運用への移行が含まれます。
    - 関連法令（個人情報保護法、医療情報保護に関する法令など）およびガイドラインに従い、必要に応じて、管轄の監督官庁、警察、関係者（利用者様、取引先など）への適切な情報公開や報告を、速やかかつ正確に行います。
- **原因究明と再発防止**:
    - インシデント対応完了後、その原因を詳細に分析し、根本的な問題点やセキュリティ対策の不備を特定します。
    - 分析結果に基づき、再発防止策（システム改修、セキュリティ強化、運用手順の見直し、従業員教育の強化など）を立案し、確実に実施します。このプロセスは、組織のセキュリティ成熟度を高めるための重要なフィードバックループとなります。

10. 従業員のセキュリティ意識向上

情報セキュリティ対策の実効性を高める上で、最も重要な要素の一つは、組織全体の従業員一人ひとりのセキュリティ意識と行動です。このため、全従業員に対し、情報セキュリティに関する継続的な教育・研修を実施します。

- **情報セキュリティ研修**:
    - 新入社員研修では、情報セキュリティの基本原則、本ポリシーの内容、個人情報保護の

重要性を徹底的に教育します。
    - 既存従業員に対しては、年一回以上の定期的な全体研修に加え、部署や業務内容に応じた専門的な研修を実施します。
    - 研修内容は、パスワード管理のベストプラクティス、フィッシング詐欺や標的型攻撃メールの見分け方、ソーシャルエンジニアリングの手口と対策、USB メモリ等の外部記録媒体の適切な利用方法、情報持ち出し制限など、実践的で具体的な内容を含みます。定期的なフィッシングシミュレーション訓練も実施し、従業員の対応能力を評価・向上させます。
    - 福祉医療情報を取り扱う特性を考慮し、特に機密性の高い情報の取り扱いに関する法令遵守と倫理意識を強化する教育を行います。
- **情報共有と啓発**:
    - 最新のセキュリティ脅威情報（例: 新たな脆弱性、流行しているサイバー攻撃の手法）、セキュリティインシデント事例、およびそれらに対する対策に関する情報を、社内ポータルやメーリングリストなどを通じて定期的に共有します。
    - ポスター掲示やセキュリティ月間などのキャンペーンを通じて、セキュリティ意識を常に高く保つための啓発活動を継続的に行い、従業員がセキュリティを「自分ごと」として捉える文化を醸成します。

11. 継続的改善

本セキュリティポリシーおよび関連するセキュリティ対策は、サイバー脅威の進化、技術の進歩、そして関連法令・ガイドラインの改定に対応するため、継続的に見直し、改善を行います。

- **内部監査**:
    - 情報セキュリティ委員会が、定期的に内部監査を実施します。この監査では、本ポリシーおよび関連規定の遵守状況、策定されたセキュリティ対策が適切に実施されているか、その効果は十分か、といった点を多角的に評価します。
    - リスクアセスメントを定期的に行い、新たなリスク要因や既存リスクの変化を特定し、それらに対応するための対策を立案します。監査結果に基づき、発見された脆弱性や改善点を明確にし、具体的な是正措置計画を策定・実施します。
- **外部評価**:
    - 客観的な視点からのセキュリティ対策の評価と改善点の特定のため、必要に応じて外部の専門機関によるセキュリティ診断（ペネトレーションテスト、脆弱性診断など）や、ISO 27001 などの国際的な情報セキュリティマネジメントシステム認証の取得、または第三者認証機関による監査を積極的に受入れます。
    - これらの外部評価を通じて得られた知見や指摘事項は、本サービスのセキュリティレベルをさらに向上させるための重要なインプットとして活用し、継続的な改善サイクルに組み込みます。

12. LINE WORKS セキュリティ責任共有モデルと FiNE-LINK⁺における対応

LINE WORKS のホワイトペーパーで示されている「責任共有モデル」は、クラウドサービスにおけるセキュリティの責任範囲を明確にする上で非常に重要です。FiNE-LINK⁺においても、この考え方に基づき、サービス提供者としての責任と、利用者様（事業者）にご協力いただく責任を明確にします。

LINE WORKS のセキュリティ責任共有モデルでは、SaaS（Software as a Service）の特性に応じて、以下の責任分担が図られています。

LINE WORKS（サービス提供者）の責任範囲: LINE WORKS は、サービスの基盤となるインフラスト

クチャ（ハードウェア、ネットワーク、施設・電源、仮想化環境、OS、ミドルウェア）、およびアプリケーション層のセキュリティ確保に責任を負います。これには、アプリケーションの機能提供、アカウント・権限機能の運用管理、サービス処理やサービスデータに対する脅威からの情報セキュリティ保護が含まれます。

- **サービス処理に対する脅威への保護**:
    - **機能不備の防止**: LINE WORKS は、常に機能改善を行い、セキュリティ上の不備があった場合には迅速に対応しています。強制アップデート機能により、古いバージョンの利用を防止し、常に安全な最新バージョンを利用できるようにしています。
    - **脆弱性を狙う攻撃への対応**: 不正侵入検知システム（IDS）による不正アクセス検知・防御、24 時間 365 日体制でのサイバー脅威モニタリング、定期的な脆弱性チェック、迅速な脆弱性対応（緊急修正パッチの適用など）、定期的な模擬攻撃（ペネトレーションテスト）を実施し、サービスのセキュリティ強度を継続的に確認しています。
- **サービスデータに対する脅威への保護**:
    - **データ分離の徹底**: LINE WORKS の契約単位で論理的に独立した「テナント」を割り当て、他のテナントからのデータアクセスを厳しく制限しています。これにより、利用者様のデータが他の利用者から不正にアクセスされることを防止します。
    - **不正アクセス防止**: サービス内部のデータに対する不正アクセスを防ぐため、データ保存場所の物理的・ネットワーク的な防御強化、データの厳格な暗号化（ハッシュアルゴリズム、対称鍵アルゴリズムの適切な利用と鍵の厳重管理）、データ改ざん・破壊のリアルタイム検知とブロックを行っています。
    - **改ざん・破壊からの復旧**: 万が一、データが改ざん・破壊された場合でも迅速に復旧できるよう、重要度に応じたサービスデータの定期的なバックアップ取得と、迅速な復旧のための手順および体制を整備し、定期的な復旧演習を実施しています。
- **データセンターや拠点に対する脅威への保護**:
    - **自然災害・事故への備え**: データセンターや業務拠点の多重化、災害復旧（DR）システムの構築により、単一の障害発生時でもサービス提供を継続できる体制を確保しています。
    - **不正侵入の防止**: データセンター・拠点への物理的セキュリティ対策として、厳格な入退室管理（生体認証、二重認証など）、24 時間 365 日の監視カメラによる映像セキュリティシステム、所在地非公開化などの措置を講じています。定期的な監査により、物理的セキュリティの有効性を確認しています。

FiNE-LINK⁺と FiNE-LINK⁺サービス利用者側の責任範囲: 本サービスの利用者である事業者様には、主に以下の領域においてセキュリティ確保にご協力いただきます。

- **利用者に対する脅威への対応**:
    - **端末の適切な管理**: 本サービスに接続するモバイル端末や PC 端末は、常に OS やアプリケーションを最新の状態に保ち、信頼できないアプリケーションをインストールしないなど、端末の安全を確保する責任があります。
    - **共有情報の適切な管理**: サービス内で共有される社外秘情報が意図せず公開されたり、漏洩したりしないよう、共有機能の設定を正しく行い、ユーザー自身が情報取り扱いに関する高い意識を持つ必要があります。FiNE-LINK⁺は、情報流出リスク軽減を支援します。
    - **フィッシング・詐欺対策**: 利用者自身が、フィッシングメールや詐欺メッセージに騙さ

れ、ログイン情報や個人情報を詐取されないよう、信頼できないサイトへの接続を避け、個人情報入力時には必ず入力先の正当性を確認する責任があります。FiNE-LINK⁺は、利用者側のセキュリティ意識向上を支援します。

- **通信に対する脅威への対応**:
    - **パブリックネットワークの適切な管理**: 海外からの不正アクセスや盗聴、偽サイトへの誘導などから情報を保護するため、FiNE-LINK⁺は、利用者側のセキュリティ意識向上を支援します。
- **アカウント・権限に対する脅威への対応**:
    - **アカウント情報の適切な管理**: パスワードの強度を高め、多要素認証を可能な限り活用し、連続ログイン失敗時のアカウント一時停止ポリシーなどを適用することで、アカウント乗っ取りのリスクを低減する責任があります。FiNE-LINK⁺は、パスワードポリシー、ログインポリシーで（2 段階認証を可能な限り、自動ログアウト設定など）強固な認証を実現します。
    - **権限の適切な管理**: 各アカウントには必要最小限の権限のみを付与し、退職者や異動者のアカウント管理を徹底することで、万一アカウントが乗っ取られた際の被害を最小限に抑える責任があります。FiNE-LINK⁺は、利用者側からの申告を受け、随時アカウントの作成及び削除、名称変更などきめ細やかな管理を支援します。

FiNE-LINK⁺は、この責任共有モデルに基づき、サービス提供者としての責任を完全に果たしつつ、利用者様がそれぞれの責任範囲において適切なセキュリティ対策を講じられるよう、必要な機能提供、情報公開、サポートを継続的に行ってまいります。この協力体制により、地域医療・介護連携における情報セキュリティの信頼性を最大限に高めます。

参考資料：LINE WORKS セキュリティホワイトペーパー

LINE-WORKS-Security-White-Paper_ver1.03.pdf