FiNE-LINK + 社内セキュリティ研修プログラム

プログラムの目的

全従業員の情報セキュリティ意識と知識を向上させ、セキュリティ社内規定の遵守を徹底することで、利用者様の医療情報・個人情報を含む情報資産を保護し、安全かつ安定的なサービス提供に貢献します。

対象者

全従業員（新入社員、既存従業員、管理者層含む）

研修頻度

- **新入社員研修**: 入社時
- **既存従業員研修**: 年 1 回以上（全体研修、部署別研修）
- **管理者層向け研修**: 必要に応じて随時

研修内容

1. 基礎研修（全従業員対象）

- **情報セキュリティの重要性**:
    - 医療情報・個人情報の機微性と保護の重要性
    - 情報漏洩・改ざんが利用者様や会社に与える影響
    - 情報セキュリティ事故の事例と教訓
- **セキュリティ社内規定の理解**:
    - 本規定の目的と概要
    - 従業員一人ひとりの役割と責任
    - 禁止事項と罰則（社内規定に基づく）
- **パスワード管理の基本**:
    - 強力なパスワードの設定方法（複雑性、長さ）
    - パスワードの使い回し禁止、定期的な変更の奨励
    - パスワードの安全な保管方法
- **メールセキュリティ**:
    - フィッシング詐欺メールの見分け方と対策
    - 不審な添付ファイルや URL の取り扱い
    - スパムメール対策
- **マルウェア対策**:
    - マルウェアの種類と感染経路
    - アンチウイルスソフトの重要性と最新状態の維持
    - 不審なプログラムの実行禁止
- **情報持ち出し制限と外部記録媒体の利用**:
    - 機密情報の持ち出しルールの徹底
    - USB メモリ等の外部記録媒体の適切な利用方法
    - 私物端末での業務情報取り扱いに関する注意点
- **ソーシャルエンジニアリング対策**:
    - ソーシャルエンジニアリングの手口と対策
    - 電話や訪問者からの情報引き出しへの対応

- **インシデント発生時の対応**:
    - 不審な活動やセキュリティ問題の兆候を認識した場合の報告義務と手順
    - インシデント報告の重要性（早期発見と被害最小化）

2. 実践・応用研修（定期研修、部署別研修など）

- **フィッシングシミュレーション訓練**:
    - 定期的に実施し、従業員の対応能力を評価・向上させる
    - 訓練結果のフィードバックと改善点の共有
- **クラウドサービス利用のセキュリティ**:
    - LINE WORKS の責任共有モデルの再確認
    - 利用者側の責任範囲における具体的な対策（端末管理、共有情報の管理、アカウント・権限管理）
- **アクセス権限の適切な管理**:
    - 「最小権限の原則」の具体的な適用例
    - 異動・退職時のアカウント・権限管理の徹底
- **リモートワーク時のセキュリティ**:
    - VPN の利用と安全な接続方法
    - 公衆 Wi-Fi 利用時の注意点
    - デバイスの物理的セキュリティ確保
- **個人情報保護法・医療情報保護に関する法令の再確認**:
    - 福祉医療情報を取り扱う上での法令遵守と倫理意識の強化
    - 最新の法改正情報と対応
- **システム操作ログの重要性**:
    - ログがどのようにセキュリティ維持に役立っているか
    - 適切なシステム操作の励行

研修方法

- **座学**: 講義形式、質疑応答
- **実習・演習**: フィッシングシミュレーション、パスワード設定演習など
- **ディスカッション**: グループ討議によるケーススタディ
- **情報共有**: 社内ポータル、メーリングリストを通じた最新のセキュリティ脅威情報や事例の共有

研修効果測定と改善

- **フィッシングシミュレーション結果の分析**: 従業員の行動変容の確認
- **インシデント報告状況のモニタリング**: 報告意識の向上度合いの確認
- **監査結果のフィードバック**: 内部監査や外部評価の結果を研修内容に反映

担当部署

情報セキュリティ委員会（または担当者）が中心となり、プログラムの企画、実施、効果測定、改善を行います。