FiNE-LINK⁺情報セキュリティ内部監査規定

1. 目的

この規定は、FiNE-LINK⁺における情報セキュリティ対策が「FiNE-LINK⁺セキュリティ社内規定」および関連法令、ガイドラインに準拠しているか、またその対策が効果的に機能しているかを客観的に評価し、継続的な改善を促進するための情報セキュリティ内部監査の実施に関する事項を定めます。

2. 適用範囲

本規定は、FiNE-LINK⁺のすべての情報資産（デジタルデータ、物理文書、システム、ネットワーク、人的資源など）およびそれらを取り扱うすべての部署・従業員に適用されます。

3. 内部監査体制と役割

- **情報セキュリティ責任者**:
  - 内部監査の最終責任者であり、監査計画の承認、監査結果のレビュー、是正措置の決定を行います。
  - 監査チームが独立性と客観性を保てるよう必要なリソースを確保します。
- **情報セキュリティ委員会（または指定された監査担当者）**:
  - 監査計画の立案、監査の実施、監査結果の報告書作成、是正措置の進捗管理を担います。
  - 監査員は、監査対象業務から独立した者が担当し、客観的な視点で監査を実施します。
- **各部署の管理者**:
  - 内部監査への協力（資料提供、ヒアリング対応など）を確実に行います。
  - 指摘事項に対する是正措置計画を策定し、実行します。
- **全従業員**:
  - 内部監査に協力し、求められた情報提供やヒアリングに誠実に対応します。

4. 内部監査の実施

4.1. 監査計画の策定

情報セキュリティ委員会は、情報セキュリティ責任者の承認を得て、少なくとも
年1回以上の頻度で内部監査計画を策定します。計画には以下の事項を含めます。

- 監査の目的と範囲
- 監査対象部署および情報資産
- 監査実施期間
- 監査項目（セキュリティ社内規定の各項目に沿ったチェックリストなど）
- 監査体制（監査チーム、担当者）

4.2. 監査の実施

策定された計画に基づき、以下の方法で監査を実施します。

- **文書レビュー**: セキュリティ社内規定、関連規程、手順書、ログ記録、報告書などの確認。
- **ヒアリング**: 各部署の管理者や担当者への聞き取り。
- **現場確認**: 物理的セキュリティ対策（入退室管理など）やシステム設定、運用状況の確認。
- **ログ分析**: システムログ、アクセスログなどのレビュー。

4.3. 監査結果の評価

監査員は、収集した情報に基づき、以下の観点から情報セキュリティ対策の状況を評価します。

- セキュリティ社内規定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の実効性

- 潜在的な脆弱性や改善点の特定
- リスクアセスメントの実施状況と新たなリスク要因の特定

5. 監査結果の報告と是正措置

5.1. 監査報告

監査員は、監査結果を情報セキュリティ責任者および関係部署に報告書として提出します。報告書には以下の事項を含めます。

- 監査の概要
- 評価結果と発見された指摘事項（不適合、改善勧告など）
- 指摘事項の根拠
- 推奨される是正措置

5.2. 是正措置計画の策定と実施

指摘事項を受けた部署の管理者は、情報セキュリティ責任者と連携し、是正措置計画を策定します。計画には以下の事項を含めます。

- 指摘事項の内容
- 具体的な是正措置の内容
- 担当者
- 完了予定日

是正措置は、計画に基づき速やかに実施されます。

5.3. 是正措置の確認と評価

情報セキュリティ委員会は、是正措置の実施状況を定期的に確認し、その有効性を評価します。必要に応じて、再監査を実施することもあります。

6. 記録と保管

内部監査に関するすべての文書（監査計画、監査報告書、是正措置計画、確認記録など）は、適切な期間、安全に保管されます。

7. 継続的改善

本内部監査規定および内部監査のプロセス自体も、サイバー脅威の変化、技術の進歩、関連法令・ガイドラインの改定に対応するため、継続的に見直されます。