情報セキュリティ実施手順

（公益財団法人ハイパーネットワーク社会研究所）

情報セキュリティ対策標準に基づき、具体的な実施手順を以下に示す。

1. アクセス制御

1.1 アクセス権限の管理手順

- 新規所員が配属した際、情報セキュリティ担当者（情報セキュリティ委員会にて任命）がアクセス権限を設定する。
- 所員の離職時は情報セキュリティ担当者がアクセス権削を直ちに削除する。
- 毎年情報セキュリティ担当者はアクセス権限のレビューを行い、不要な権限があれば削除する。

1.2 認証手順

- 業務端末における多要素認証の設定を全ての所員に対して義務付ける。
- セッションが一定時間アクティブでない場合に自動でログアウトする設定を施行する。

2. データ保護

2.1 データの分類手順

情報セキュリティ担当者は、所内のデータを機密性に基づいて分類し、取り扱い基準を設定する。

2.2 暗号化手順

機密データを扱う際は、暗号化を推奨する。

2.3 バックアップ

情報セキュリティ担当者は、年に 1 回程度、重要データのバックアップスケジュールを定め、実行する。

3. セキュリティインシデントの管理

3.1 インシデント検知手順

- 異常検知時、直ちに情報セキュリティ委員会に報告する。

3.2 インシデント対応手順

- インシデント発生時、情報セキュリティ委員会は直ちに緊急会議を開催する。
- 対応計画を策定し、必要に応じて所長に報告する。

3.3 インシデント後のレビュー手順

- インシデント解決後、情報セキュリティ委員会はレビュー会議を開催する。
- 原因分析を行い、再発防止策を策定する。

4. リスク管理

4.1 リスク評価手順

- 年に一度、情報セキュリティ委員会はリスク評価会議を開催する。
- 評価結果をもとに、リスク対応計画を策定し、所長に報告する。

5. 教育と意識向上

5.1 定期的な教育プログラム実施手順

- 全所員は、毎年指定された情報関連のセミナーまたは研修に参加する。
- 新入所員に対しては、情報セキュリティセミナーの参加を奨励する。

5.2 意識向上活動実施手順

- 情報セキュリティ担当者は、セキュリティセミナーを年に 1 回以上 実施し、全所員にセミナーの開催案内を通知する。