令和××年××月××日

**情報セキュリティ監査実施計画書**

|  |  |  |
| --- | --- | --- |
| № | 項目名 | 内　容 |
| １ | 監査目的 | 特定個人情報取扱規程の運用状況を点検・評価し、情報セキュリティ水準の向上に寄与することを目的とする。 |
| ２ | 監査テーマ | 特定個人情報を取扱う情報システムの利用に係るセキュリティ対策の実施状況を把握する。 |
| ３ | 監査範囲 | 対象事務：介護保険事務  対象システム：介護保険システム  場所：本庁舎、〇〇出張所 |
| ４ | 被監査部門 | 介護保険課 |
| ５ | 監査方法 | (1)インタビュー（ヒアリング、聞き取り）：口頭による質問  (2)閲覧（レビュー）：文書類・規程類・記録類の確認  (3)視察（サイトレビュー）：情報システム・サーバ室・執務室などの現場視察 |
| ６ | 監査実施日程 | (1)監査実施  本庁舎　：令和××年××月××日　9:30～12:00  A出張所：令和××年××月××日　13:30～15:00  (タイムスケジュール)  ・監査実施についての説明・・・・・・・・・・・・ 5分  ・担当者へのヒアリング、規程類・記録類の閲覧・・90分  ・執務室等の観察、他職員へのヒアリング・・・・・30分  ・監査チーム内協議・・・・・・・・・・・・・・・15分  ・監査結果の中間報告・・・・・・・・・・・・・・10分  (2)監査報告会  平成××年××月××日　13:00～14:00 |
| ７ | 監査実施体制 | 情報セキュリティ監査統括責任者：企画部　○○部長  内部監査人：情報システム課　　◇◇課長補佐  内部監査人：保険福祉課　　△△主任 |
| ８ | 監査項目 | (1)特定個人情報の分類と管理方法  (2)機器等の持ち出し、持込み  (3)研修・訓練  (4)ＩＤ及びパスワードの管理  (5)不正プログラム対策 |
| ９ | 適用基準 | (1)○○市管理基準  (2)〇〇市特定個人情報取扱規程  (3)〇〇市特定個人情報取扱マニュアル |

|  |
| --- |
| 情報セキュリティ監査実施計画書策定のポイント  １　監査目的の決定  年度計画に基づいた監査目的を記載する。  ２　監査テーマの決定  監査目的を達成するための具体的なテーマや目標を記載する。  　　　〔監査テーマの例〕  　　　　・情報システムの利用に係るセキュリティ対策の実施状況の把握  　　　　・情報システムの管理に係るセキュリティ対策の実施状況の確認  　　　　・個人情報の適切な運用管理の点検と改善  ３　監査範囲の決定  　　　　今回の監査対象となる情報システムを記載する。監査範囲が部門単位となる場合  は「○○部門保有の情報システム」などの記載でもよい。  ４　被監査部門の決定  今回の監査対象となる被監査部門を記載する。  ５　監査方法の決定  　　適用する監査技法を記載する。  〔監査技法の種類〕  　　・インタビュー（ヒアリング、聞き取り）：口頭による質問  　　・閲覧（レビュー）：文書類・規程類・記録類の確認  　　・視察（サイトレビュー）：情報システム・サーバ室・執務室などの現場確認  　　・アンケート：文書・セルフチェックシートによる質問や自己点検  　　・再実施（テスト）：監査人自らが操作や運用を行って確認  ※適用する監査技法はすべて記載する。  　　６　監査実施日程の決定  　　　　・監査を実施する日時を記載する。  　　　　・被監査部門に関連する事項を中心に記載する。  　　　　・監査報告会を行う場合はその予定も記載する。  　　　　・タイムスケジュールを記載してもよい。  　　７　監査実施体制の決定  　　　　・監査統括責任者、監査チームリーダー、監査人を記載する。  ・技術的監査を行う専門家や外部のアドバイザーなどを記載してもよい。  　　８　監査項目  　　　　・実施する監査項目の概要を記載する。  ・予定している監査項目はすべて記載する。  　　９　適用基準  　　　　監査指摘の判断基準として適用する基準を記載する。  　　　　具体的な基準が定められていない場合は、総務省「地方公共団体における情報  セキュリティ監査に関するガイドライン」でもよい。  以上 |