令和　年　月　日

情報セキュリティ監査統括責任者：企画部長　○○　○○

**情報セキュリティ監査中期計画書**

**１　目的**

計画期間内に特定個人情報を取り扱う全ての事務に対する監査を着実に達成することを目的とする。

**２　監査方針**

〇〇においては、特定個人情報に対する情報セキュリティ管理策の実効性を確保するため、情報セキュリティマネジメントサイクルの確立を目標に、特定個人情報を取り扱う全ての事務に対し、情報セキュリティ管理策の改善の方向性を助言する助言型監査を繰り返し実施する。

その結果、情報セキュリティマネジメントが一定のレベルに達した段階で、外部の専門家による外部監査を受け、必要に応じ情報セキュリティの水準を保証することを目的とする保証型監査も検討することとする。

**３　実施目標**

地方公共団体を取り巻く情報セキュリティリスクは多様化しているが、法令に基づき住民の個人情報を取り扱う責任に鑑みれば、事故を未然に防止する対策を十分に講じる必要がある。そこで、本市では番号法ならびに個人情報保護委員会が公表した特定個人情報保護に関連する指針やガイドラインに基づき、情報セキュリティの管理策の整備状況及び運用状況を点検・評価するため、内部監査を実施する。

さらに、内部監査の実務を通じて職員に情報セキュリティに関する知識やノウハウが浸透し、将来的には各部門が相互に監査を実施できるよう、内部監査人の育成を図る。

**４　対象範囲**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | 監査対象事務 | システム名 | 所管部署 | 備考 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**５　活動計画**

(1)計画期間

令和XX年度から令和XX年度の３ヵ年

(2)計画内容と実施時期

|  |  |  |  |
| --- | --- | --- | --- |
| **年　度** | **被監査部門**  **（　）内は実施予定時期** | **対象事務** | **自己点検** |
| 令和XX年度 | ○○○○課（XX月～XX月）  ○○○○課（XX月～XX月）  ○○○○課（XX月～XX月）  ○○○○課（XX月～XX月） | 住民基本台帳 | 庁内全課  実施予定時期  XX月頃 |
| 令和XX年度 | ○○○○課（XX月～XX月）  ○○○○課（XX月～XX月）  ○○○○課（XX月～XX月）  ○○○○課（XX月～XX月） | 固定資産税 | 庁内全課  実施予定時期  XX月頃 |
| 令和XX年度 | ○○○○課（XX月～XX月）  ○○○○課（XX月～XX月）  ○○○○課（XX月～XX月）  ○○○○課（XX月～XX月） | 介護保険 | 庁内全課  実施予定時期  XX月頃 |

**６　監査実施手順**

　　情報セキュリティ監査実施指針に基づき、以下の手順で実施する。

1. 準　　備　：　体制の整備、実施要綱の策定、協力体制の整備等
2. 監査計画　：　中期計画・年度計画の策定等
3. 監査実施　：　監査実施計画の策定、監査実施、監査結果の取りまとめ等
4. 監査報告　：　監査報告書の作成、監査結果の報告等
5. 監査結果への対応　：　改善計画書の作成等
6. フォローアップ監査　：　改善対応状況の確認

|  |
| --- |
| 情報セキュリティ監査中期計画書策定のポイント  １　監査方針の明確化  組織として情報セキュリティ内部監査の実施により何をどこまで目指すのかという  監査の基本方針（目的）を明確にする。  　　　〔基本方針の例〕  　　　　・情報セキュリティ対策の妥当性確認  　　　　・情報セキュリティ対策の準拠性確認  　　　　・継続的な助言型監査の実施による改善  　　・将来的な保証型監査への展開  ２　実施目標の明確化  基本方針（目的）を実現するために目指す実施目標を明確にする。  　　　〔実施目標の例〕  　　　　・全庁的な情報セキュリティレベルの底上げ  　　　　・重要情報資産を取扱う部門のセキュリティ確保  　　　　・情報セキュリティ対策の準拠性確保  　　　　・内部監査人の育成  　　　　・相互監査の実施  　　　　・保証型監査実施の事前準備  ３　監査範囲の決定  　　　 実施目標を達成するために対象となる被監査部門や監査対象システムを決定する。  　　　〔監査範囲の例〕  　　　　・特定個人情報を取り扱う全部門  　　　　・重要情報資産を取扱う部門  　　　　・特定管理項目（外部媒体利用やアクセス制御など）の対象となる部門  　　・保証型監査対象部門  ４　活動計画の決定  ３年から５年程度の中期における大まかな監査計画を決定する。  　　　〔活動計画の例〕  ・開始年度と中期計画期間  ・各年度の監査対象部門（監査対象システム）と実施予定時期  ・自己点検の実施時期  ５　監査実施手順の決定  　監査実施プロセスを情報セキュリティ監査実施指針に基づいて決定する。    以上 |