マイナンバー監査サービス

NPO東京ITコーディネータ

1．マイナンバー対応監査の目的

付1.1　マイナンバー法制度対応の運用監査とは

付1.2　マイナンバー監査要件の確認

2．マイナンバー内部監査支援サービス

付2.1　マイナンバー内部監査の進め方

付2.2　マイナンバー監査チェックリスト例

3.マイナンバー外部監査サービス

付3.1　マイナンバー外部監査の進め方

付3.2　マイナンバー業務監査基準の考え方

付3.3　保証型マイナンバー運用監査

1 マイナンバー対応監査の目的

「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」においては、講ずべき安全管理措置の「C 組織的安全管理措置」として、以下の通り特定個人情報等の取扱状況の把握、安全管理措置の評価、見直し及び改善を求めている。

e 取扱状況の把握及び安全管理措置の見直し
特定個人情報等の**取扱状況を把握し、安全管理措置の評価、見直し及び改善**に取り組む。
≪手法の例示≫
＊ 特定個人情報等の取扱状況について、**定期的に自ら行う点検又は他部署等による監査**を実施する。

→ **内部監査の実施**

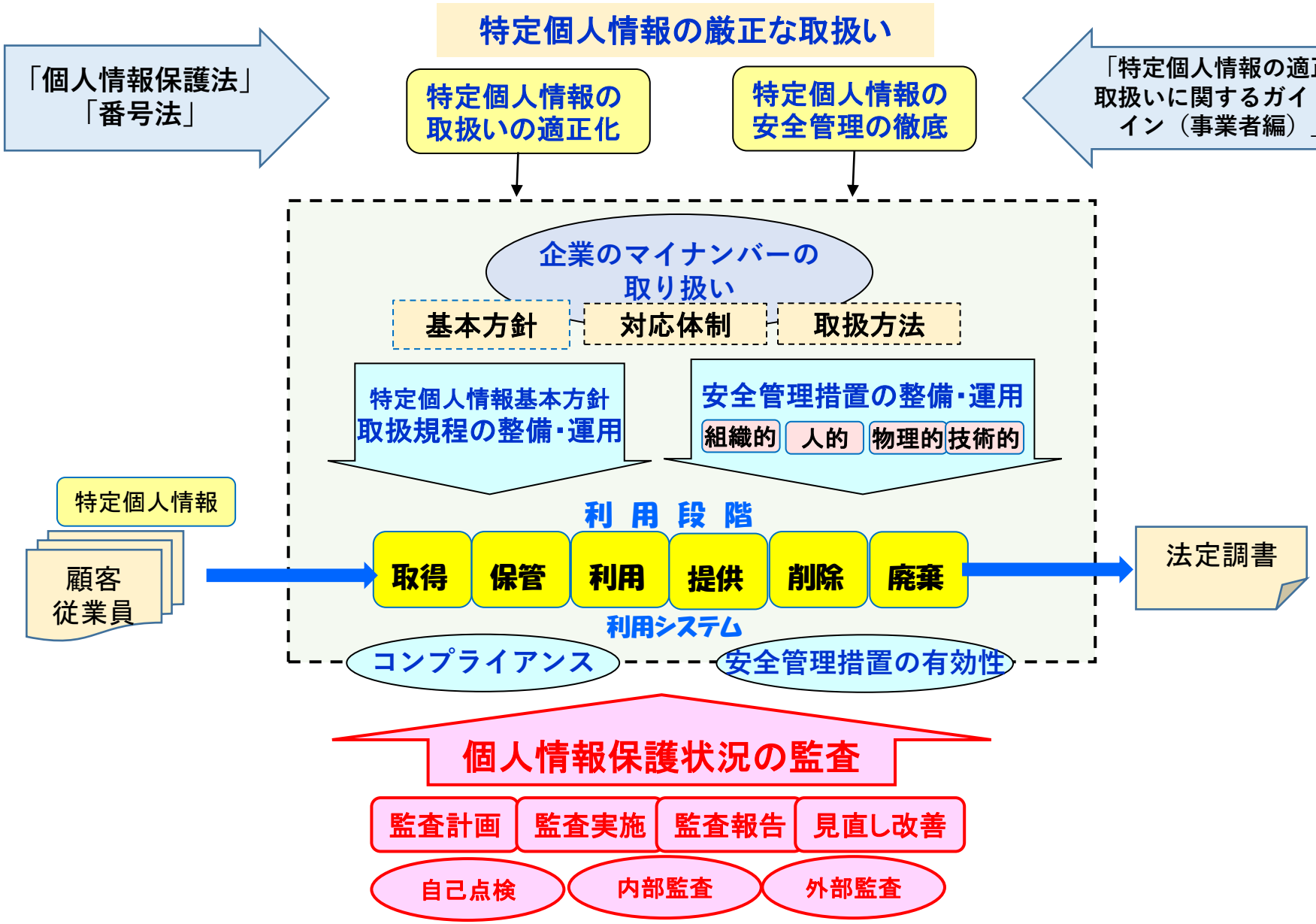
＊ **外部の主体**による他の監査活動と合わせて、**監査を実施**することも考えられる。

→ **外部監査の実施**

【中小規模事業者における対応方法】
○ 責任ある立場の者が、特定個人情報等の取扱状況について、**定期的に点検**を行う。

○中小規模事業者に対する特例措置が示されているがその定義は以下の通り。
「中小規模事業者」とは、事業者のうち**従業員の数が100人以下の事業者**であって、次に掲げる事業者を除く事業者をいう。
- **個人番号利用事務実施者**
- **委託**に基づいて個人番号関係事務又は個人番号利用事務を業務として行う事業者
- **金融分野**（金融庁作成の「金融分野における個人情報保護に関するガイドライン」第１条第１項に定義される金融分野）の事業者
- **個人情報取扱事業者**

付1.1 マイナンバー法制度対応の運用監査とは



付1.2　マイナンバー監査要件の確認

❶マイナンバー監査目的 と位置づけの確認

・経営上の番号法対応リスク認識とリスク管理状況確認
・監査目的の適合性・効率性・経済性・有効性確保

マイナンバー監査目的等

・目的の確認
- □特定個人情報の適正な取扱いの確保‥番号法
- □安全管理対策の有効性と残存リスクの把握

・安全管理措置に対する監査テーマ
- □特定テーマに係わる運用状況の監査
  - □セキュリティ（完全性、機密性、可用性）の確保状況
  - □サイバーセキュリティリスク管理状況
  - □情報環境資産の脆弱性評価
  - □脆弱性に対する脅威の評価
  - □リスクの影響度・発生可能性評価
  - □リスク対策・安全管理措置の整備・運用の有効性評価
  - □残存リスク評価
  - □業務委託管理状況‥選定基準・定期評価基準
  - □委託先クラウド運用の脆弱性診断
  - □自社運用プラットフォームの脆弱性診断

・監査業務としての位置づけ
- □内部監査・業務監査の一環として監査
- □内部統制の一環として監査
- □コンプライアンス監査の一環として監査

❷マイナンバー 監査対象の確認

□対象範囲と監査要件の確認
- 対象業務と対象部門の明確化
- 業務委託状況
- 関連システムの機能要件／非機能要件
- 関連システムの稼働環境と運用環境

□対象業務と対象フェーズ確認
- 取得・利用
- 保存・提供
- 運用・保守
- 削除・廃棄

❸マイナンバー監査手続 と手順の確認

・監査体制と被監査部門の負荷‥期間・工数
・費用対効果

❸-1マイナンバー監査手続

・監査目的の設定
- □内部目的‥助言型・業務改善
- □外部目的‥保証型・対外説明

・監査基準
- □「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」、業界編
- □各監督官庁ガイドライン
- □情報セキュリティガイドライン

・監査方法
- □面談‥チェックリスト
- □アンケート、自己点検・診断
- □運用記録閲覧、文書レビュー
- □記録のサンプリング評価
- □脆弱性評価

・監査結果評価
- □検出事項
- □指摘事項
- □改善助言

❸-2マイナンバー監査手順

1.経営計画による位置づけ確認
中期経営計画　/年度経営計画
情報化中期計画　/年度計画反映

中期業務監査計画
基本業務監査計画
個別セキュリティ監査計画

2.監査実施計画の策定
監査テーマと対象範囲
監査スケジュール
監査手順の明確化

3.予備調査
システム運用概況把握

4.本調査

5.分析・評価・結論
6.監査結果の報告
7.フォローアップの実施

❹ マイナンバー監査の有効性確保の前提

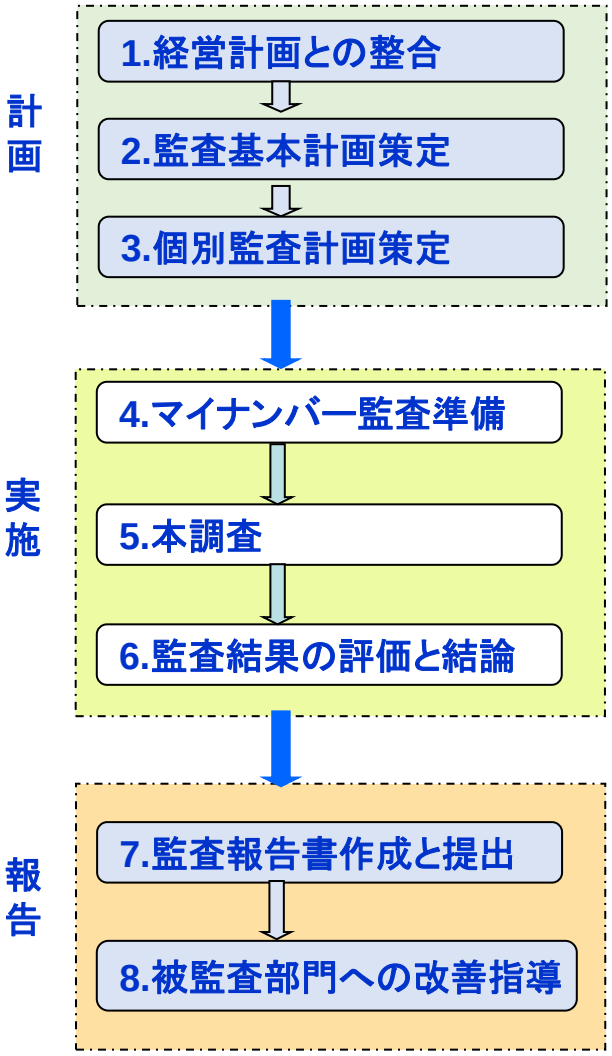
監査実施の前提等
- ■守秘契約締結
- □監査業務効率化のための協力体制
  - ・監査責任者および監査窓口と業務分担の決定
  - ・被監査部門責任者および担当者への周知
  - ・他の監査・検査との連携および調整
- □被監査部門への協力依頼
  - ・ヒアリング時間の確保、アンケート提出依頼
    - ・監査証跡提供依頼
      - 承認記録、議事録、運用記録等の閲覧

2 マイナンバー内部監査支援サービス

	企業における内部監査（任意監査）	マイナンバー内部監査支援サービス
監査目的	業務効率の向上 、コンプライアンスの遵守、従業員不正の防止等	同左
監査計画	経営者の要望を優先して、毎年度の監査 計画を立案しなければならない	①社内監査業務における位置づけの確認 ②社内の監査計画への組み入れを支援 中期監査計画、年度監査計画
監査専門性	業務監査の専門性が要求されるが、企業内では内部監査人の専門性の確保が困難な場合も多い	①番号法および安全管理措置（情報セキュリティ面）への対応状況の監査支援 ②検出事項に対する改善支援
監査独立性	経営者には直属し、経営者に対する独立性はない 経営者以外の部署からの独立性は確保される	①社内の内部監査部門の独立性確保支援 ②第三者として内部監査の一部受託可能
監査基準	法令・官公庁ガイドラインおよび社内規程。	同左準拠のチェックリスト提供
経営者と内部監査人との関係	経営者と主従関係がある 。監査対象から”独立かつ客観的”な立場のシステム監査人が、監査対象をを”総合的に点検および評価”し、経営者に助言または勧告するとともに”フォローアップ”する一連の活動	①内部監査部門支援方式 次年度以降の体制確立支援 自己点検方法 ②内部監査業務一部受託方式 内部監査工数・スキル不足支援
監査スタッフ体制	内部監査要員は質量とも不足しており、監査内容 を充実するために優先順位を決め、優先順位の高い監査テーマを選定して、 その年度のテーマとして実施することが多い	①監査スタッフの育成支援 ②PDCA管理によるリスク低減活動の改善支援

付2.1　マイナンバー内部監査支援の進め方

マイナンバー内部監査実施手順



マイナンバー内部監査支援サービス対象

経営方針、事業戦略、業務運営方針の把握、個人情報等への対応状況、業務上の課題確認、規程文書等の整備・運用状況、⇒監査対象・重点テーマの明確化。

経営基本計画や業務システムの全体最適化計画に対応し、中長期経営計画を踏まえた監査業務の年次方針や年間計画を明確にする。

個別監査対象の監査目的、監査項目、監査目標および監査手続を明確にし、個々のテーマ監査における各監査人の活動予定を明確にする。

監査の効率性および有効性向上のために、必要に応じて、被監査部門管理者へ事前ヒヤリングおよび資料を予備調査として実施し、監査チェックリストを準備する。

監査対象の実態を、監査実施計画および監査基準に準拠した監査項目や監査手続きに従い、ヒヤリングし、現場調査と資料や記録の確認する。必要に応じて事前に質問表を通じて調査。できるだけ監査証跡を確保する。

予備調査および本調査で収集した監査証拠を確認・分析・評価して、監査対象に対するコントロールが目的に照らして妥当であるか否かを評価する。検出事項に基づき監査の結論(総合評価、指摘事項、改善勧告)を出す。

各個別監査計画毎に個別監査報告書を作成する。監査調書をまとめ、監査責任者のレビューを受け、草案を作成する。被監査部門と意見交換を行い、監査内容に事実誤認がないことを確認し、個別監査報告書の最終作成と監査依頼者の承認を得る。

システム監査人として、監査報告の改善状況をモニタリングするとともに、改善の具現化をフォローアップする。

付2.2　マイナンバー監査チェックリスト例

マイナンバー対応整備・運用状況ヒアリングシート（委託先用）

特定個人情報の適正な取り扱いに関するガイドライン（事業者編）　H28 年 1 月版ベース

【委託内容・委託時期】	【評価者】	【評価日】	【評価判定】

評価項目		評価内容	確認	確認対象	備考
	契約書締結	□基本契約書締結日/改訂日（　.　.）、□秘密保持契約書　同（　.　.）		締結日・改訂日	
	基本方針	□特定個人情報の取扱いに係わる基本方針は策定されているか		基本方針作成日・改訂日	
	取扱規程	□委託業務に関する特定個人情報の取扱規程を策定しているか		取扱規程作成日・改訂日	
理措置	組織体制	□特定個人情報を取扱う社内組織体制、責任者、事務取扱担当者は明確か		体制図、担当者名	
	取扱状況	□当社の委託事務に係わる情報の台帳を整備し、正しく記録されているか		授受記録台帳	
		□当社の委託事務を処理するシステムの利用			
		□当社の委託事務の手順書・業務フローは作			
	漏洩時対応	□情報漏洩時の対応体制・手順を定めた規程			
	違反時対応	□情報の取扱いに違反があった場合の対応等			
	自己点検・監査	□取扱状況を自ら点検しているか、また、内部			
	見直し改善	□指摘事項を改善し、是正状況を確認してい			
措置	教育	□事務取扱担当者の教育を行っているか‥役			
	守秘契約	□事務取扱担当者と守秘契約を締結している			
	罰則規定	□取扱いに違反があった場合の罰則規定が定			
程	管理区域	□機器を設置している管理区域は入退室を管			
	取扱区域	□事務を行う取扱区域は壁・間仕切り等で隔			
	盗難対策	□特定個人情報記載書類、外部記録媒体、可			
		□当該システム機器に対し、盗難防止用ワイ			
	漏洩防止	□送付する場合、通信暗号化およびファイル			
		□当該書類の搬送時は、鍵付きカバン使用・			
	消去・廃棄	□削除または廃棄の記録（外部委託の場合は			

特定個人情報等の安全管理措置に係わる成熟度診断

特定個人情報の適正な取り扱いに関するガイドライン（事業者編）　H28 年 1 月改訂版ベース

自己診断結果　●：今回

ヒアリング日　　年　　月　　日

成熟度定義
- 5.最適化経営・業界ベストプラクティスのレベル
- 4.管理され、モニタリング・評価、継続的改善中【運用】
- 3.実施手順が定義され、標準化している【整備】
- 2.文書化は部分的、反復可能だが直観的・属人的
- 1.意識しているがその場対応している
- 0.管理項目として意識されていない

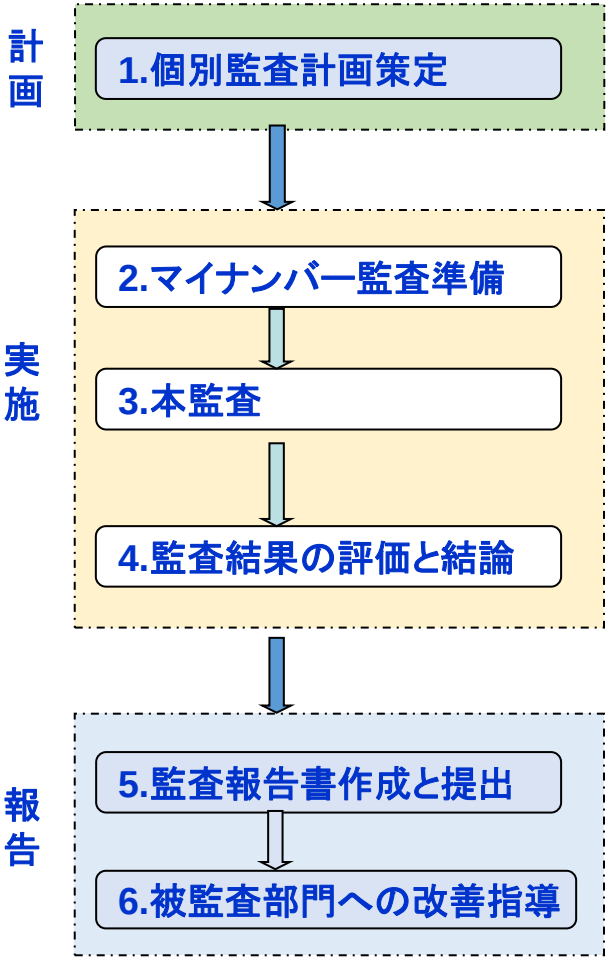
		必須項目	0	1	2	3	4	5	コメント
A	**基本方針の策定**								
(1)	**特定個人情報に関する方針の認識等**		0	1	2	3	4	5	コメント
	□特定個人情報等の扱いに関する「**基本方針**」が策定されているか	□							
	□特定個人情報等の**範囲**は明確にされているか	□							
	□関係者に特定個人情報の**収集・利用目的**について**周知**しているか	□							
B	**取扱規程等の策定**								
(2)	**特定個人情報の取扱いに関する要件**		0	1	2	3	4	5	
	□特定個人情報等の取扱いを定める「**取扱規程**」等を策定しているか	□							
	□個人番号を扱う**事務の範囲**(情報収集・法定調書・帳票類の作成の事務フロー等)は明確にされているか	□							
	□**管理段階**(取得・利用・保存・提供・削除・廃棄)ごとに**責任者・事務取扱担当者・任務**を定めているか	□							
(3)	**特定個人情報の保護措置の規定と周知**		0	1	2	3	4	5	
	□特定個人情報を利用できるのは、**社会保障、税及び災害対策**に関する特定の事務に**限定**されていることを従業員に**周知**しているか	□							
	□特定個人情報を前述の３つの目的以外のために**提供**したり、提供を求めてはならないこと	□							
	□**特定個人情報ファイル**を作成できるのは、個人番号関係事務および個人番号利用事務の**目的**の場合のみであること	□							
(4)	**特定個人情報の委託に係わる取扱い**		0	1	2	3	4	5	
	□個人データの取扱いを委託する場合、委託先選定基準の整備、委託契約書・秘密保持等契約書の締結とそれらに従った運用をおこなっているか	□							
	□個人番号関係事務の委託先の安全管理に関して社内と同等の**監督**を行っているか	□							
	□特定個人情報の規程、委託先の選定基準、等の経営層による承認および関係者への周知をおこなっているか	□							
	□委託先は、再委託の**許諾**等を行った場合のみが可能であり、委託先と同様に再委託先についての監督義務を果たしているか	□							
C	**組織的安全管理措置**								
(5)	**組織体制の整備**		0	1	2	3	4	5	
	□**個人番号関係事務**における「**責任者**」を定め、責任と権限を明確にしているか	□							
	□**事務取扱担当者**を定め、その役割を明確にしているか	□							
	□特定個人情報等を複数の部署で取り扱う場合、各部署間の**任務分担**および**責任範囲**を明確にしているか	□							
	□特定個人情報の取扱いに関する**規程等に違反**している事実、又は兆候を把握した場合、責任者等への**報告連絡体制**を確立しているか	□							
(6)	**取り扱い状況の確認手段の整備**		0	1	2	3	4	5	
	□**特定個人情報**等の**取扱い状況**(利用・出力・持出・削除・廃棄)の分かる**記録**(ログ、利用実績、システム利用状況)を**保存**しているか	□							
	□**特定個人情報ファイル**の種類、名称、責任者、取扱部署、利用目的等を記載した**台帳**を作成しているか	□							

3 マイナンバー外部監査サービス

	外部監査（法定監査または任意監査）	マイナンバー外部監査サービス
監査目的	会計監査の場合は、財務諸表の適正性に関する意見表明、会計不正の防止、内部統制報告書の監査等。 テーマ監査の場合は、当該分野の専門家による監査基準の準拠性監査等。	①番号法の準拠性監査 ②特定個人情報等の安全性管理措置の適用状況監査
監査計画	依頼者と協議して、監 査リスクの高いものから重点的に監査行うことを推奨する。想定されるリ スクをベースに監査計画を提案することになる。	①社内業務における番号法の位置づけの確認 ②社内の業務監査計画との整合性確認
監査専門性	管理すべきリスクに対するコントロールが、リスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的な立場のシステム監査人が検証又は評価することによって、保証を与えあるいは助言を行う。	番号法準拠性および安全管理措置（情報セキュリティ関係）への対応状況の監査 ①方針・規程・ルール等の整備状況 ②それらの運用状況と継続的改善状況
監査独立性	経営者や被監査部門からのからの独立性は確保される（精神的独立性、経済的独立性等）。	①第三者として外部監査業務の受託 ②社内の内部監査活動との調整
監査基準	法令・官公庁ガイドライン及び監査基準等。	同左準拠のチェックリスト使用
経営者と監査人との関係	主従関係はない。法定監査以外の専門的な監査では、社内に監査スキルが無い場合も多く外部に依頼する。 会計に係わる外部監査人は株主総会で選任されるが、経営者が実質 的には決定している。それ以外の特定テーマ監査については、企業の必要性に応じて外部に依頼される。	①経営者（監査委託者）との、監査目的監査対象範囲、監査方法についての合意。 ②契約範囲についての監査業務受託 内部監査工数・スキル不足支援 ③社内関連規程の確認
監査スタッフの外部活用	監査 部門からは独立して監査を実施し、被監査部門が直面しているビジネス、業界および戦略的リスクについて幅広い知識を有することが期待されている	継続的監査の契約による段階的な改善

付3.1　マイナンバー外部監査の進め方

マイナンバー外部監査実施手順



全体の監査方針や監査計画を確認し、個別監査対象の監査目的、監査項目、監査目標および監査手続を提案する。監査業務の年次方針や年間計画とも調整を行う。

監査の効率性および有効性向上のために、必要に応じて、被監査部門管理者へ事前ヒヤリングおよび資料等を閲覧し、事前に監査チェックリストを準備する。

監査対象の実態を、監査実施計画および監査基準に準拠した監査項目、監査手続に従い、ヒヤリング、現場調査、資料確認、アンケート質問表を通じて調査。
重要点は、検出事項についての監査証拠の確保

予備調査および本調査で収集した監査証拠を確認・分析・評価して、監査対象に存在するコントロールが目的に照らして妥当であるかどうかを評価する。
検出事項に基づき監査の結論(総合評価、指摘事項、改善勧告)を出す。

各個別監査計画毎に個別監査報告書を作成する。監査調書をまとめ、監査責任者のレビューを受け、草案を作成する。被監査部門と意見交換を行い、監査内容に事実誤認がないことを確認し、個別監査報告書の最終作成と承認を得る。

システム監査人として、監査報告の改善状況をモニタリングするとともに、改善の具現化を提案する。

付3.2　マイナンバー業務監査基準の考え方

システム監査および情報セキュリティ監査の経験を活かして監査基準を整備して監査を実施する。

監査基準

一般基準
1.目的、権限・責任の明確化
2.独立性、客観性・職業倫理の保持
3.専門能力の保持
4.業務上の注意・守秘義務
5.監査結果の品質維持

実施基準・・対象業務管理段階別
1.監査計画の立案
2.監査手順準拠
3.1監査証拠の入手と評価
3.2監査調書の作成と保存
4.監査業務の体制
5.他の専門職の利用
6.情報セキュリティ監査の方法
情報セキュリティ管理基準

報告基準
1.監査報告書の提出と開示
2.監査報告の合理的な根拠
3.監査報告の記載事項
監査対象
監査概要
保証意見・助言意見
制約・除外事項
指摘事項
改善勧告
特記事項
4.監査報告書についての責任
5.監査報告に基づく改善指導

■監査基準は、監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範である。

■監査基準は、監査人としての適格性及び監査業務上の遵守事項を規定 する「一般基準」、監査計画の立案及び監査手続の適用方法を中心に監査実施上に枠組みを規定する「実 施基準」、監査報告に係わる留意事項と監査報告書の記載方式を規定する「報告基準」からなっている。

■監査基準は、組織体の内部監査部門等が実施する監査だけでなく、組織体の外部者に 監査を依頼する監査においても利用できる。

■監査基準は、業務に保証を付与すること を目的とした監査であっても、業務の改善のための助言を行うことを目的とした監査であっても利用 できる。

マイナンバー業務管理基準

特定個人情報の適正な取扱いに関するガイドライン（事業者編）

（参考）情報セキュリティ管理基準

（参考）システム管理基準

■監査基準に従って監査を行う場合、原則とし て、監査人が監査上の判断の尺度として用いるべき基準となる。

■ただし、組織体が属する業界又は事業活動の特性等を考慮して、必要ある場合には、管理基準の主旨及び体系に則って、該当する関係機 関などにおいて、独自の管理基準を策定し活用することが望ましい。

■また、時々の関連技術動向、関連 法令、及び社会規範などを考慮し、それらを反映した詳細なサブコントロール項目を策定することが望ま しい。

付3.3　保証型マイナンバー運用監査