地方公共団体等における
監査のためのチェックリスト
～マイナンバーの適正な取扱いのために～

平成 29 年 6 月
（令和６年 12 月最終改正）
個人情報保護委員会

＜目次＞

はじめに

行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号。以下「番号法」という。）第 12 条において、「個人番号利用事務実施者及び個人番号関係事務実施者は、個人番号の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために必要な措置を講じなければならない」とされている。

そして、当委員会は、個人番号を取り扱う行政機関及び独立行政法人等（以下「行政機関等」という。）並びに地方公共団体及び地方独立行政法人（以下「地方公共団体等」という。）が特定個人情報の適正な取扱いを確保するための具体的な指針として、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）」（以下「ガイドライン」という。）等を定めている。「監査」に関する部分については、ガイドラインの「（別添１）特定個人情報に関する安全管理措置」の組織的安全管理措置において、組織体制の整備として、監査責任者の設置及び責任の明確化、取扱状況の把握及び安全管理措置の見直しとして、特定個人情報等の管理の状況について、定期に及び必要に応じ随時に監査を行うこと、その結果等を踏まえ、必要があると認めるときは、取扱規程等の見直し等の措置を講ずることなどが示されている。

保護措置の１つである特定個人情報保護評価書（基礎項目評価書は除く。）においても、「監査」の項目について、リスク対策の記載を求めている。

また、情報セキュリティの確保に当たっては、組織的・体系的に取り組む必要があり、そのような中で、監査の位置付けは、重要なものとなっている。

監査を行うに当たっては、専門的知識を有する者を配置するなど人員等の適切な資源配分を行うとともに、組織において権限と責任を有する者に対して、監査結果等を報告する仕組みを確立するなど、組織的に取り組む必要がある。さらに、監査において把握した問題点等の改善のみに留まるのではなく、監査結果等を踏まえて、当該事務や作業方法の見直しを行うなど、事務等を効率的に行うために、監査結果等を活用することが重要である。

今般、番号法に基づく立入検査の結果や、どのような項目を監査すればよいのかなどの意見が寄せられたことなどを踏まえ、監査のためのチェックリスト（以下「監査チェックリスト」という。）を策定・公表することとした。

監査チェックリストは、ガイドライン等を基にした確認項目を示すとともに、監査を行うに当たり、どのような資料を求めれば良いのかが分かるよう、監査資料及び監査チェックリストの活用方法の参考例についても併せて示している。

なお、監査チェックリストは、行政機関等及び地方公共団体等が監査を行うに当たり、あくまでも参考として示したものであるため、当該監査チェックリストに基づき監査を行わなければならないということではない点、また、事務の特性等を踏まえて、監査項目を追加するなどして監査を行うことを妨げるものでもない点には注意願いたい。

監査チェックリストの策定・公表を通じて、特定個人情報の適正な取扱いの確保に資することになれば幸いである。

○　監査チェックリスト及び監査資料の留意事項

監査チェックリスト及び監査資料の利用に当たっては、以下の点について、留意されたい。

（１）監査チェックリスト

・監査は、どの事務を対象として、どのような方針で監査を行うのかなどの監査計画を立て、当該計画に基づいて監査を行い、監査の結果等に基づいて規程等の見直しを行う必要がある。監査チェックリストは、事務単位での監査を前提に作成したものであるが、監査計画を立てるに当たっては、特定個人情報がどこでどのように取り扱われているか機関全体の事務等を把握する必要があるため、監査チェックリストの「番号１　機関の概要」の「確認項目」を設けている。

・「番号２」以降は、事務単位での確認項目としている。

・「確認項目」は、主として、ガイドラインに沿う形で作成しており、「大分類」において、「安全管理措置（1_A)」などのように、ガイドラインの記載箇所が分かるように見出し（項番）を付している。

・「確認項目」は、網羅的に記載しているため、一部重複する項目がある。

・監査を行うに当たっては、客観的な事実を基に検証する必要があることから、資料等に基づいて監査を行うことになるが、特に、注意すべき項目については、「～を記録しているか」などと記載をしている。

・「確認項目」の「～運用はどのようになっているか」の箇所については、規程に沿った運用をしているのか、又は、規程にない運用をしており、規程を整備する必要があるのかなどを確認する必要がある。

・「番号 16　取扱状況の把握及び安全管理措置の見直し」は、当該監査ではなく、他の監査における状況を確認するために記載している。

・確認する資料については、監査資料の「安全管理措置等の分類」に記載しているガイドラインの見出し（項番）を参考にしてほしい。

（２）監査資料

・監査資料についても、監査チェックリストと同様にガイドラインの記載箇所がわかるように見出し（項番）を付している。

・「番号１」及び「番号２」の「機関の概要」は、機関全体の内容を把握するための資料であり、「番号３」以降は、事務単位での監査資料である。

・本省、地方支分部局、本所、支所、分庁舎等ごとに規程がある場合や取扱いが異なる場合は、それぞれの規程等を確認する必要がある。

・「番号 15」は、当該監査ではなく、他の監査における状況を把握するために記載している。

監査チェックリスト

番号	大分類	小分類 （※は、確認ポイントを示している）	チェック	確認項目
1	機関の概要	※組織、情報システムに関して全体の概要を確認すること		機関の概要について、以下の点を把握する。
			□	①組織体制、出先機関、所掌事務等
			□	②特定個人情報保護に関する指針・考え方 （個人番号の取扱いに関する規程等の整備状況）
			□	③個人番号を取り扱う事務
			□	④情報システムセキュリティ対策
			□	⑤サーバ室の状況
			□	⑥ＰＣの設置状況、管理状況
			□	⑦総括責任者、保護責任者、事務取扱担当者及び情報システム管理者
			□	⑧文書管理規程
				庁舎の文書管理の状況について、以下の点を把握する。
			□	①窓口収受及び郵便受領から関係各課への回付の流れ
			□	②保管、廃棄の状況
			□	③番号制度導入による事務の変更点
			□	【地方公共団体のみ】法改正を反映した個人情報保護条例等の改正を行っているか
			□	【地方公共団体のみ】番号法第９条第２項に基づく条例を整備しているか
			□	【地方公共団体のみ】独自利用事務の内容が法定事務の内容と類似しているか
2	安全管理措置（1_A） 個人番号利用事務等の範囲の明確化	※個人番号利用事務は、番号法別表に記載又は条例に規定されている事務であること ※事務フロー、システム概要図等に沿って事務の概況を確認すること		事務の概要について、以下の点を把握する。
			□	①個人番号利用事務等の流れ（取得、利用、保存、提供、削除・廃棄の流れ）
			□	②所掌分担及び事務取扱担当者等
			□	③各システム及びそのＩＤ管理の状況
			□	④番号制度導入による事務の変更点
			□	⑤独自施策の実施状況
			□	執務室内等（職員の動線、機器設置等）の状況はどのようになっているか
			□	【地方公共団体のみ】団体内統合宛名システムの整備状況はどのようになっているか
3	安全管理措置（1_B） 明確化した事務において取り扱う特定個人情報等の範囲の明確化		□	個人番号と関連付ける個人情報の範囲について、規程を整備しているか
			□	特定個人情報の取扱い件数を把握しているか
4	安全管理措置（1_C） 明確化した事務に従事する事務取扱担当者の明確化	※指定の方法について、部署名、事務名、担当者名かの違いにも留意すること	□	事務取扱担当者の指定について、規程を整備しているか
			□	事務取扱担当者を指定しているか 特に、事務取扱担当者の指定に漏れはないか
5	安全管理措置（1_D,2_A） 基本方針の策定	※周知していることを確認する場合は、実際に周知された者に対して確認をすることも有用である。	□	基本方針を策定しているか
			□	事務取扱担当者等の関係者に周知しているか 特に、容易にアクセスできるための措置を講じているか
			□	事務取扱担当者等の関係者が内容を理解しているか

番号	大分類	小分類 （※は、確認ポイントを示している）	チェック	確認項目
6	安全管理措置（1_E,2_B） 特定個人情報等の適正な取扱いを確保するために、特定個人情報の保護に関する取扱規程等の見直し等を行う	※規程の見直しについて、版数を確認することも一つの方法である。 ※「特定個人情報の取扱いに関する管理規程の考え方（個人情報の保護に関する管理規程の見直し等のポイント）」（平成27年4月　特定個人情報保護委員会事務連絡）を参照すること	□	特定個人情報を取り扱うための規程の策定・見直しをしているか
			□	情報セキュリティの規程について、相互の関連を示す文書管理体系となっているか また、一覧化されてるか
			□	事務取扱担当者等の関係者に周知しているか 特に、容易にアクセスできるための措置を講じているか
			□	事務取扱担当者等の関係者が内容を理解しているか
		取得 ※紙媒体、電子データ、それぞれの規程類と運用を確認すること	□	取得する際の規程を整備しているか 特に、取得手順を整備しているか
			□	取得に係る運用はどのようになっているか 特に、取得方法は適切か、台帳等に記録しているか
			□	目的外の取得についてのリスク対策を講じているか 特に、情報提供ネットワークシステムを利用して目的外の取得をしないためのリスク対策を講じているか
			□	個人番号の漏えい、滅失又は毀損等（以下「漏えい等」という。）事案についてのリスク対策を講じているか
		利用	□	利用する際の規程を整備しているか 特に、利用手順を整備しているか
			□	利用に係る運用はどのようになっているか
			□	不正利用についてのリスク対策を講じているか
			□	アクセス権限の管理をしているか
		保存	□	保存する際の規程を整備しているか 特に、業務に見合う、保存期間を定めた規定を整備しているか
			□	保存に係る運用はどのようになっているか 特に、台帳等に記録しているか
		提供	□	提供する際の規程を整備しているか 特に、提供手順を整備しているか
			□	提供に係る運用はどのようになっているか 特に、台帳等に記録しているか
		削除・廃棄	□	削除、廃棄する際の規程を整備しているか 特に、削除、廃棄手順を整備しているか
			□	削除、廃棄に係る運用はどのようになっているか 特に、台帳等に記録しているか
7	委託の取扱い(第４-２(1)) 1.委託先の監督 A 委託先における安全管理措置		□	委託先に対して、番号法に基づき個人番号利用事務等を行う行政機関等及び地方公共団体等が果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行わなければならないことを認識しているか
8	委託の取扱い(第４-２(1)) 1.委託先の監督 B 必要かつ適切な監督	委託先の選定		委託先の選定時、果たすべき安全管理措置と同等の措置が講じられていることについて、以下の点を確認しているか
			□	①委託先の設備
			□	②技術水準
			□	③従業者に対する監督・教育の状況
			□	④経営環境
			□	⑤漏えい等事案に対応する体制等の整備状況

監査チェックリスト

番号	大分類	小分類 （※は、確認ポイントを示している）	チェック	確認項目
		契約内容	□	委託契約書を締結しているか
				委託契約書の内容について、以下の項目を含んでいるか
			□	①秘密保持義務
			□	②事業所内からの特定個人情報の持ち出しの禁止
			□	③特定個人情報の目的外利用の禁止
			□	④再委託における条件
			□	⑤漏えい等事案が発生した場合の委託先の責任
			□	⑥委託契約終了後の特定個人情報の返却又は廃棄
			□	⑦特定個人情報を取り扱う従業者の明確化
			□	⑧従業者に対する監督・教育
			□	⑨契約内容の遵守状況について報告を求める規定
			□	⑩必要があると認めるときは委託先に対して、実地の監査、調査等を行うことができる規定等
		取扱状況の把握	□	委託先から定期的な報告をさせているか
			□	委託先から受けた報告書の取扱いはどのようになっているか
9	委託の取扱い(第４-２(1)) 2.再委託 A 再委託の要件		□	再委託をしているか
			□	再委託をしている場合、許諾をしているか
10	委託の取扱い(第４-２(1)) 2.再委託 B 再委託の効果		□	再委託に当たっては、特定個人情報の適切な安全管理が図られることを確認した上で再委託の諾否を判断しているか
11	委託の取扱い(第４-２(1)) 2.再委託 C 再委託先の監督		□	委託先が再委託先について監督していることを把握しているか
12	安全管理措置（2_Ca） 組織的安全管理措置 -組織体制の整備			組織体制について、以下の点を整備しているか
			□	①総括責任者（行政機関等に各１名）の設置及び責任の明確化
			□	②保護責任者（個人番号利用事務等を実施する課室等に各１名）の設置及び責任の明確化
			□	③監査責任者の設置及び責任の明確化
			□	④事務取扱担当者及びその役割の明確化
			□	⑤事務取扱担当者が取り扱う特定個人情報等の範囲の明確化
			□	⑥取扱規程等に違反している事実又は兆候を把握した場合の責任者への報告連絡体制の整備
			□	⑦漏えい等事案の発生又は兆候を把握した場合の報告連絡体制の整備
			□	⑧特定個人情報等を複数の部署で取り扱う場合の各部署の任務分担及び責任の明確化

監査チェックリスト

番号	大分類	小分類 （※は、確認ポイントを示している）	チェック	確認項目
13	安全管理措置（2_Cb） 組織的安全管理措置 -取扱規程等に基づく運用	記録		以下の項目を記録しているか
			□	①特定個人情報ファイルの利用・出力状況の記録
			□	②書類・媒体等の持ち運びの記録
			□	③特定個人情報ファイルの削除・廃棄記録
			□	④削除・廃棄を委託した場合、これを証明する記録等
			□	⑤特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況（ログイン実績、アクセスログ等）の記録
		保存	□	記録を一定の期間保存しているか
		分析	□	記録について、定期及び必要に応じ随時に分析等しているか
		改ざん等の防止	□	記録の改ざん、窃取又は不正な削除の防止のために必要な措置を講じているか
14	安全管理措置（2_Cc） 組織的安全管理措置 -取扱状況を確認する手段の整備			特定個人情報ファイルの取扱状況を確認するための手段について、以下の点を記録しているか
			□	①特定個人情報ファイルの名称
			□	②行政機関等の名称及び特定個人情報ファイルが利用に供される事務をつかさどる組織の名称
			□	③特定個人情報ファイルの利用目的
			□	④特定個人情報ファイルに記録される項目及び本人として特定個人情報ファイルに記録される個人の範囲
			□	⑤特定個人情報ファイルに記録される特定個人情報等の収集方法
			□	取扱状況を確認するための記録等に、特定個人情報等を記載していないか
15	安全管理措置（2_Cd） 組織的安全管理措置 -漏えい等事案に対応する体制等の整備	漏えい等事案に対応する体制等の整備		漏えい等事案等に対応するための体制及び手順等について、以下の点を整備しているか
			□	①漏えい等事案が発覚した際の報告・連絡等
			□	②事実関係の調査及び原因の究明
			□	③影響範囲の特定
			□	④影響を受ける可能性のある本人への連絡
			□	⑤個人情報保護委員会への報告
			□	⑥関係機関への報告
			□	⑦再発防止策の検討及び決定
			□	⑧事実関係及び再発防止策等の公表
		漏えい等事案の実績	□	漏えい等事案が過去に発生しているか
			□	漏えい等事案が発生していた場合の運用はどのようになっているか
			□	漏えい等事案が発生していた場合、規程類の見直し等を行っているか
		訓練	□	不正アクセス、ウイルス感染の事案、標的型攻撃等の被害を受けた場合の対応について、関係者において定期的に確認又は訓練等を実施しているか
16	安全管理措置（2_Ce） 組織的安全管理措置 -取扱状況の把握及び安全管理措置の見直し	※点検及び監査においては、他の機関から求められている点検及び監査がある場合があることから、当該項目を記載している。	□	監査に係る規程を整備しているか
			□	監査計画（監査の観点、監査周期等）は定めているか
			□	監査を実施しているか（運用はどのようになっているか）
			□	監査の実施結果を記録しているか
			□	総括責任者に報告しているか
			□	監査の結果等を踏まえ、取扱規程等の見直し等をしているか

番号	大分類	小分類 （※は、確認ポイントを示している）	チェック	確認項目
17	安全管理措置（2_Da） 人的安全管理措置 -事務取扱担当者の監督	※事務連絡の発出等を確認することが考えられる。	□	総括責任者及び保護責任者が事務取扱担当者に対して必要かつ適切な監督をしているか
18	安全管理措置（2_Db） 人的安全管理措置 -事務取扱担当者等の教育	教育研修 ※誰が、どの研修を受講したかを記録等により確認すること	□	特定個人情報等の保護に関する教育研修に係る規程を整備しているか
			□	新規採用時や異動に伴う臨時の教育研修について、規程を整備しているか
			□	事務取扱担当者に対して、教育研修を実施しているか（運用はどのようになっているか）
			□	情報システムの管理に関する事務に従事する職員に対して、教育研修を実施しているか（運用はどのようになっているか）
			□	保護責任者に対して、教育研修を実施しているか（運用はどのようになっているか）
			□	教育研修への参加の機会を付与する等の措置を講じているか
			□	未受講者に対して再度の教育研修を実施するなどのフォローを行っているか 特に、フォローの実施について、記録しているか
		番号法に定められた研修	□	サイバーセキュリティの確保に関する事項その他の事項に関する研修を行っているか
			□	研修の計画をあらかじめ策定し、これに沿ったものとなっているか
			□	研修の内容は、サイバーセキュリティの確保に関する事項として、適切なものとなっているか
			□	特定個人情報ファイルを取り扱う事務に従事する者の全てに対して研修を実施しているか
			□	おおむね一年ごとに研修を実施しているか
19	安全管理措置（2_Dc） 人的安全管理措置 -法令・内部規程等の違反に対する厳正な対処	※行政機関の職員は、人事院規則「懲戒処分の指針について」という国家公務員の処分基準（平成28年９月30日改正で秘密漏えいにかかる標準例が新たに追加され、情報セキュリティ対策を怠ったことによる職員の処分について基準が明記された。）	□	法令又は内部規程等に違反した場合の対処の規程を整備しているか
			□	法令又は内部規程等に違反した職員がいた場合、厳正に対処しているか
20	安全管理措置（2_Ea） 物理的安全管理措置 -特定個人情報等を取り扱う区域の管理	※必要に応じて、管理区域等に立ち入る際の手続に沿って実際に現場にて確認すること	□	特定個人情報等を取り扱う事務を実施する区域（取扱区域）では、事務取扱担当者等以外の者が特定個人情報等を容易に閲覧等できないように留意しているか
			□	特定個人情報ファイルを取り扱う情報システムを管理する区域（管理区域）は明確になっているか
			□	入退室管理の規程を整備しているか
			□	入退室管理に係る運用はどのようになっているか
			□	管理区域へ持ち込む機器等の制限等の規程を整備しているか
			□	管理区域へ持ち込む機器等の制限等に係る運用はどのようになっているか
21	安全管理措置（2_Eb） 物理的安全管理措置 -機器及び電子媒体等の盗難等の防止		□	機器、電子媒体の盗難等の防止に係る規程を整備しているか
			□	機器、電子媒体の盗難等の防止に係る運用はどのようになっているか
			□	書類等の盗難等の防止に係る規程を整備しているか
			□	書類等の盗難等の防止に係る運用はどのようになっているか
22	安全管理措置（2_Ec） 物理的安全管理措置 -電子媒体等の取扱いにおける漏えい等の防止		□	電子媒体又は機器等の使用（暗号化・パスワード設定、使用許可等）に係る規程を整備しているか
			□	電子媒体又は機器等を使用する際の運用はどのようになっているか 特に、接続制限、使用の許可はどのようになっているか
			□	電子媒体又は書類等を持ち運ぶ際の規程（暗号化・パスワード設定、封緘、目隠しシール、施錠できる搬送容器の使用等）を整備しているか
			□	持ち運ぶ際の運用はどのようになっているか 特に、書類送付の担当者が事務取扱者でない場合は特定個人情報が閲覧できないような工夫をしているか

番号	大分類	小分類 （※は、確認ポイントを示している）	チェック	確認項目
23	安全管理措置（2_Ed） 物理的安全管理措置 -個人番号の削除、機器及び電子媒体等の廃棄		□	削除又は廃棄の規程を整備しているか
			□	削除又は廃棄の運用はどのようになっているか 特に、復元不可能な手段を採用しているか、削除又は廃棄の記録を保存しているか
			□	委託している場合は、委託先が確実に削除又は廃棄したことについて、証明書等を取得して確認しているか
24	安全管理措置（2_Fa） 技術的安全管理措置 -アクセス制御	※人事異動等があった場合は、特にアクセス権の削除について確認すること	□	情報システムを使用する場合、使用可能な端末、事務取扱担当者、特定個人情報ファイルの範囲を限定しているか 特に、アクセス権の付与を最小化しているか 特に、アクセス権を有する者に付与する権限を最小化しているか
25	安全管理措置（2_Fb） 技術的安全管理措置 -アクセス者の識別と認証		□	情報システムにアクセスするための識別・認証の規程（ユーザID、パスワード、生体情報等）を整備しているか
			□	識別・認証に係る運用はどのようになっているか
26	安全管理措置（2_Fc） 技術的安全管理措置 -不正アクセス等による被害の防止等	※情報システムの不正アクセス又は不正ソフトウェアから保護する仕組み等を確認すること	□	外部等からの不正アクセス又は不正ソフトウェアから保護する仕組み等を導入しているか 特に、ファイアウォール等の不正アクセス対策はできているか 特に、セキュリティ対策ソフトウェア等によりウイルス等への対策はできているか 特に、ログ等の分析を行い、不正アクセス等を検知する体制をとっているか
			□	情報提供ネットワークシステム等の接続規程等が示す安全管理措置を遵守しているか
			□	個人番号利用事務において使用する情報システムについて、インターネットから独立する等の高いセキュリティ対策を踏まえたシステム構築や運用体制整備を行っているか
			□	【地方公共団体のみ】自治体情報システム強靭性向上モデルへの対応（ＬＧＷＡＮを活用する業務システムとインターネットメール等のシステムとの通信経路を分割、端末への二要素認証の導入、端末からの情報持出しの不可設定、無害化通信）は、どのようになっているか
27	安全管理措置（2_Fd） 技術的安全管理措置 -漏えい等の防止		□	特定個人情報等をインターネット等により外部に送信する場合、通信経路における漏えい等を防止するための措置を講じているか
			□	外部送信する場合の規程を整備しているか
			□	特定個人情報等を外部送信した実績はあるか
			□	特定個人情報ファイルを機器又は電子媒体等に保存する場合の規程を整備しているか
			□	特定個人情報ファイルを機器又は電子媒体等に保存する場合、暗号化、パスワード等を設定しているか
28	安全管理措置（2_G） 外的環境の把握		□	【外国にある拠点・委託・クラウドサービスの利用等により外国において特定個人情報等を取り扱っている場合】 当該外国の個人情報の保護に関する制度等を把握した上で、特定個人情報等の安全管理のために必要かつ適切な措置を講じているか。
			□	【外国にある第三者に特定個人情報の取扱いを委託している場合】 当該委託先に対し７～11で示す事項を確認し、当該委託先における安全管理措置について必要かつ適切な監督を行っているか。

監査資料

番号	安全管理措置等の分類	資料（大分類）	資料（小分類）
1	機関の概要	機関の概要が分かる資料	①機関の事務（個人番号を取り扱わない事務を含む。）、規模、部署、人員が分かる資料 ②情報システムの状況（情報システムセキュリティ対策、サーバ室、ＰＣの設置状況等）が分かる資料 ③本省、地方支分部局（又は、本所、支所、分庁舎等）の活動内容が分かる資料 ④条例で定める事務（独自利用事務）の内容が分かる資料
2	機関の概要	文書管理体系が分かる資料	①文書管理規程 ②情報セキュリティ関連の文書の一覧が分かる資料
3	安全管理 （1_A）	個人番号を取り扱う事務の範囲・概要が分かる資料	個人番号を取り扱う事務に関する以下の規程等 ①事務手順書 ②事務処理手引き・マニュアル ③本省、地方支分部局（又は、本所、支所、分庁舎等）における事務の役割分担が分かる資料 ④事務全体のフロー図 ⑤監査対象となる事務の所管課等のフロア図、座席表 ⑥事務連絡
4	安全管理 （1_B）	特定個人情報等の範囲が分かる資料	事務において使用される個人番号及び個人番号と関連付けて管理される個人情報の範囲が分かる資料
5	安全管理 （1_B）	個人番号取扱件数が分かる資料 （前年度（当年度がある場合は当年度も含む。）））	個人番号が記載される届出書、申告書等の取扱件数が分かる資料 （前年度の同書類の取扱件数及び内数として実際に個人番号が記載されている書類の取扱件数）
6	安全管理 （1_C）	事務取扱担当者の明確化が分かる資料	事務取扱担当者を定めた資料（規程を含む。）
7	安全管理 （1_D、2_A）	特定個人情報等の取扱規程の前提となる規程（訓令）	①番号制度に関係する規程（基本方針を含む。） ②情報セキュリティポリシー ③情報システムの運用規程
8	安全管理 （1_E、2_B）	特定個人情報等の取扱規程	①特定個人情報等の具体的な取扱いを定めた取扱規程（取得、利用、保存、提供、削除・廃棄の規程を含む。） ②（特定個人情報等の）文書管理に関する規程
9	委託の取扱い 第４－２（１）	委託先の監督に関する資料	①委託契約書、仕様書等(委託内容を示す資料) ②委託先を適切に選定していることが分かる書類 ③委託先に対する監督内容が分かる資料 （委託先の特定個人情報の取扱規程等を含む。） ④委託先から受けた報告書（作業管理表、業務報告書、月次レポート等） ⑤委託先における廃棄、消去の台帳等 ⑥再委託をしている場合の通知書、許諾書等
10	【組織的安全管理措置】 安全管理 （2_Ca）	組織体制の整備状況が分かる資料	①組織体制の整備が分かる資料 総括責任者・保護責任者などを明記している資料 ②漏えい等事案に対応するための報告連絡体制が分かる資料
11	安全管理 （2_Cb）	取扱規程等に基づく運用が分かる資料	①特定個人情報ファイルの利用状況、削除・廃棄状況などが分かる台帳等 ②定期に及び必要に応じ随時に分析等していることが分かる資料
12	安全管理 （2_Cc）	取扱状況の確認のための手段の整備状況が分かる資料	特定個人情報ファイルの取扱状況を確認するための手段の整備状況が分かる資料 （個人情報ファイル簿に記載している事項が分かる資料）

監査資料

番号	安全管理措置等の分類	資料（大分類）	資料（小分類）
13	安全管理 （2_Cd）	漏えい等事案に係る体制等の整備状況が分かる資料	①漏えい等の事案が発覚した際の対応方法（報告・連絡、公表時期等）を定めた規程 ②漏えい等の事案の発生状況とその対応状況が分かる資料
14	安全管理 （2_Cd）	標的型攻撃等を想定した定期的な確認・訓練の状況が分かる資料	①標的型攻撃等を想定した確認・訓練の計画書 ②確認・訓練の実施状況が分かる記録
15	安全管理 （2_Ce）	取扱状況の把握及び見直しが分かる資料 （監査に関する資料）	①監査の規程 ②監査計画及び実施状況が分かる資料 ③監査結果について、監査責任者が定期に及び必要に応じ随時に総括責任者に報告した記録 ④総括責任者が、監査結果を踏まえ取扱規程類の見直し措置の有無を判断した記録
16	【人的安全管理措置】 安全管理 （2_Da）	事務取扱担当者への監督状況が分かる資料	総括責任者及び保護責任者の事務取扱担当者に対する監督状況が分かる資料
17	安全管理 （2_Db）	事務取扱担当者等への教育状況が分かる資料（職員に対する教育・啓発に関する資料）	①教育研修に係る規程 ②教育（研修）計画 ③事務取扱担当者に、教育を実施していることが確認できる資料 ④特定個人情報等を取り扱う情報システムを管理する職員に、教育を実施していることが確認できる資料 ⑤保護責任者に、教育を実施していることが確認できる資料 ⑥教育の結果が一定水準を満たさない場合の対応状況が分かる資料 例）情報システムを使用できなくしているなどの予防措置を実施 ⑦番号法に定められたサイバーセキュリティの研修が分かる資料
18	安全管理 （2_Dc）	法令違反等に対する規程	①法令又は内部規定等に違反した職員に対する対処規程 ②違反した職員数及びその対処状況が分かる資料
19	【物理的安全管理措置】 安全管理 （2_Ea①②）	入退室管理等の状況が分かる資料	①管理区域、情報システム室等の区域の設定の規程、又は、それぞれの区域が分かる資料 ②管理区域の入退室管理の規程 【特定個人情報ファイルを取り扱う情報システムに係る入退出管理】 ③サーバ室（システム設置場所）の概要図 ④サーバ室への入退室管理の状況が分かる資料（鍵の貸出を含む。） ⑤サーバへアクセスするためのID、パスワード認証の概要 ⑥入退室管理カードの貸与、保管、貸出状況が分かる資料 ⑦サーバ室の施錠・警報・監視設備の状況が分かる資料 【個人番号利用事務等に係る居室の入退出管理】（※該当がある場合のみ） ⑧事務居室の概要図 ⑨事務居室への入退室の管理状況が分かる資料（鍵の貸出を含む。） ⑩職員のID、パスワード認証の概要 ⑪職員以外（臨時入室等）の入退室管理カードの貸与、保管、貸出状況が分かる資料 【持ち込む機器等の制限等】 ⑫管理区域へ持ち込む機器等の制限等の規程
20	安全管理 （2_Eb）	電子媒体等の盗難等の防止の措置が分かる資料	①電子媒体等の盗難等の防止に係る規程 ②特定個人情報等（紙媒体）の保管状況（耐火金庫等へ施錠）が分かる資料 ③特定個人情報等を取り扱う機器、電子媒体の保管状況が分かる資料

監査資料

番号	安全管理措置等の分類	資料（大分類）	資料（小分類）
21	安全管理 （2_Ec）	使用制限、接続制限の規程	電子媒体又は機器等の使用の制限、接続の制限の規程
22	安全管理 （2_Ec）	持ち運びに係る規程等	①特定個人情報等が記録された電子媒体又は機器等の持ち運ぶ際の規程 ②電子媒体(USBメモリ・CD・DVD・カメラ等)の取扱規程 ③電子媒体の運用管理台帳等（使用者・期間・使用後のデータ消去等） ④特定個人情報等が申告書等の紙媒体からシステム入力される場合、入力後の紙媒体の管理状況が分かる資料
23	安全管理 （2_Ｅｄ）	個人番号の削除、電子媒体等の廃棄の規程等	①保存期間が分かる資料 ②保存期間の妥当性を示す資料 ③保存期間を経過した場合の削除・廃棄の規程 ④書類・媒体を廃棄した場合の記録（委託している場合は証明書等）
24	【技術的安全管理措置】 安全管理 （2_Fa）	アクセス制御の措置状況が分かる資料	①ユーザーID等の発行管理の状況が分かる資料 （アクセス権限の権限と事務の対応表など） ②権限付与者の基準、人数が分かる資料 ③情報システムのアクセスログを確認する規程 ④アクセスログの記録
25	安全管理 （2_Ｆｂ）	アクセス者の識別方法が分かる資料	①職員の識別と認証に係る規程 ②情報システムのアクセス者の識別方法（ユーザーID、パスワード等）等が分かる資料
26	安全管理 （2_Fc）	個人番号利用事務等で使用するシステムの概要が分かる資料	①情報システムの概要・機能等の説明資料 ②ネットワーク構成図（以下の内容が分かる資料） a)サーバ等の物理的な配置状況、ファイアウォール等の設置状況 b)システムとクライアントPC（ユーザー端末等）との接続状況 c)他のシステム（外部機関のシステムを含む）との接続状況（予定を含む） d)インターネット網との接続・分離状況 e)インターネット網から分離していない場合、又は論理的分離の場合の高いセキュリティ対策を踏まえたシステム構築状況 ③【地方公共団体のみ】団体内統合宛名システムと業務システム、中間サーバー等との接続を示す資料及び個人番号を管理する仕組みが確認できる資料
27	安全管理 （2_Fc）	不正アクセスの防止等の状況が分かる資料	①情報システムの不正アクセスへの対策が分かる資料 ②情報システムのセキュリティ対策ソフトウェア等の導入、更新頻度が分かる資料 ③ログ等の分析を行うなど、不正アクセス等を検知する手順が分かる資料
28	安全管理 （2_Fc）	情報提供ネットワークシステムとの接続に係る規程	情報提供ネットワークシステムの接続に関する以下の規程 ①目的外入手の防止に係る規程 ②不適切な方法での入手防止に係る規程 ③漏えいや紛失等の防止に係る規程 ④提供時に適切な措置を講じる規程 ⑤誤提供の防止に係る規程
29	安全管理 （2_Fc）	情報提供ネットワークシステムによる提供の状況が分かる資料	①情報提供ネットワークシステムを用いて提供する情報の内容 ②情報提供ネットワークシステムの利用頻度（xx件/月など）
30	安全管理 （2_Fd）	漏えい等の防止に係る規程	①特定個人情報等の外部送信に係る規程 ②外部送信の実績 ③漏えい等防止策（暗号化・パスワード等）が分かる資料

監査資料

番号	安全管理措置等の分類	資料（大分類）	資料（小分類）
31	【外的環境の把握】 安全管理 （2_G）	外的環境の把握状況に関する資料	①外国における特定個人情報等の取扱い状況が分かる資料（契約書、利用規約、事業者に関する資料等） ②当該外国の個人情報の保護に関する制度等の把握状況が分かる資料（当該外国の法令に関する資料等） ③当該外国の個人情報の保護に関する制度等をふまえて特に講じている安全管理措置の内容が分かる資料 ④外国にある第三者に特定個人情報の取扱いを委託している場合は、当該委託先に対する監督の実施状況が分かる資料

○　監査チェックリストの活用方法の参考例

番号	監査項目等				監査手法・手続			確認対象	監査実施後の対応			
	大分類	小分類	チェック	確認項目 （確認のポイント）	ヒアリング	資料閲覧	現場視察・実機確認	監査資料 （文書、記録、台帳等）	監査確認結果 （実態の姿、発見事項等）	監査結果の評価 （軽微な指摘、重大な指摘、観察事項）	指摘事項 （発見事項に対する助言）	改善案
○-○-○												
1												
2												
3												

監査チェックリストで
示している範囲

監査チェックリストの
活用方法

※それぞれ、各組織において、実務に即してカスタマイズして活用してください。