地方公共団体等における
監査のためのチェックリスト
～保有個人情報の適正な取扱いのために～

令和６年 12 月
個人情報保護委員会

＜目次＞

はじめに

個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）第 66 条において、「行政機関の長等は、保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の安全管理のために必要かつ適切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、個人情報等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の機関及び地方独立行政法人（以下「地方公共団体等」という。）における個人情報等の適正な取扱いに関し、参考となる事項を整理したものとして、「個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）」（以下「事務対応ガイド」という。）等を示している。「監査」に関する部分については、事務対応ガイドの「４－８　（別添）行政機関等の保有する個人情報の適切な管理のための措置に関する指針」において、管理体制の整備として、監査責任者の設置及びその役割、監査の実施として、保有個人情報の適切な管理を検証するため、保有個人情報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い、その結果を総括保護管理者に報告すること、その結果等を踏まえ、保有個人情報の適切な管理のための措置について評価し、必要があると認めるときは、その見直し等の措置を講ずることなどが示されている。

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、個人情報保護法に基づく実地調査の結果や、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、既に公表している「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～」と同様に、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、事務対応ガイド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、保有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、保有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、事務対応ガイドに沿う形で作成しており、「大分類」において、「安全管理措置（4-8-1)」などのように、事務対応ガイド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。

・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」に記載している事務対応ガイドの見出し（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事務対応ガイド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」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２」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。

監査チェックリスト

番号	監査項目等			
	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個人情報保護に関する指針・考え方 （保有個人情報の取扱いに関する規程等の整備状況）
			□	③保有個人情報を取り扱う事務又は業務
			□	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総括保護管理者、保護管理者、保護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改正個人情報保護法施行による事務又は業務の変更点
			□	【地方公共団体のみ】改正個人情報保護法施行を反映した個人情報保護条例等の改正を行っているか
4－8－1　指針の意義				
2	安全管理措置（4-8-1） 指針の意義 ※個人情報保護基本方針の策定	※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。	□	個人情報保護基本方針を策定しているか
			□	職員（派遣労働者を含む。以下同じ）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
			□	職員が内容を理解しているか

番号	監査項目等			
	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
3	安全管理措置（4-8-1） 指針の意義 ※保有個人情報の適切な管理のために、保有個人情報の保護に関する取扱規程等を整備する		□	保有個人情報の適切な管理のための規程（管理規程、取扱規程）を整備しているか
			□	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、一覧化されているか
			□	職員に周知しているか 特に、容易にアクセスできるための措置を講じているか
			□	職員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（事務処理マニュアル、実施手順書等）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
			□	保有個人情報の漏えい、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 ※取得しようとする個人情報を含む
		利用	□	利用する際の規程（事務処理マニュアル、実施手順書等）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（事務処理マニュアル、実施手順書等）を整備しているか 特に、事務又は業務に見合う、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（事務処理マニュアル、実施手順書等）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（事務処理マニュアル、実施手順書等）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
4－8－2　管理体制				
4	安全管理措置（4-8-2） 管理体制			組織体制について、以下の点を整備しているか
			□	①総括保護管理者（各行政機関等に一人）の設置 ※官房長、総務担当役員等
			□	②保護管理者（保有個人情報を取り扱う各課室等に一人）の設置 ※当該課室等の長又はこれに代わる者
			□	③保護担当者（保有個人情報を取り扱う各課室等に一人又は複数人）の設置 ※当該課室等の保護管理者が指定
			□	④監査責任者（各行政機関等に一人）の設置 ※内部監査等を担当する部局の長、幹事等
			□	⑤保有個人情報の適切な管理のための委員会の設置 ※保有個人情報の管理に係る重要事項の決定、連絡・調整等を行うため必要があると認めるとき、関係職員を構成員とする委員会
			□	⑥保有個人情報の適切な管理のための委員会の開催 ※保有個人情報の管理に係る重要事項の決定、連絡・調整等を行うため必要があると認めるとき、定期又は随時に開催

番号	監査項目等			
	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
4－8－3　教育研修				
5	安全管理措置（4-8-3） 教育研修	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	□	保有個人情報の取扱いに関する教育研修に係る規定を整備しているか
			□	新規採用時や異動に伴う臨時の教育研修について、規定を整備しているか
			□	研修計画の策定について、規定を整備しているか
			□	研修計画を策定しているか
			□	保有個人情報の取扱い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）
			□	研修の内容は、保有個人情報の取扱いについて理解を深め、個人情報の保護に関する意識の高揚を図るための啓発その他必要な事項として、適切なものとなっているか
			□	保有個人情報を取り扱う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）
			□	研修の内容は、情報システムの管理、運用及びセキュリティ対策に関する事項として、適切なものとなっているか
			□	保護管理者及び保護担当者に対して、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）
			□	研修の内容は、課室等の現場における保有個人情報の適切な管理に関する事項として、適切なものとなっているか
			□	保護管理者及び保護担当者に対する教育研修を定期的に実施しているか
			□	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
4－8－4　職員の責務				
6	安全管理措置（4-8-4） 職員の責務		□	職員は、法の趣旨にのっとり、関連する法令及び規程等の定め並びに総括保護管理者、保護管理者及び保護担当者の指示に従い、保有個人情報を取り扱っているか
4－8－5　保有個人情報の取扱い				
7	安全管理措置（4-8-5） 保有個人情報を取り扱う事務又は業務の規模及び性質の把握	※事務フロー、システム概要図等に沿って事務又は業務の概況を確認すること		事務又は業務の概要について、以下の点を把握する。
			□	①保有個人情報を取り扱う事務又は業務の流れ（取得、利用、保存、提供、削除・廃棄の流れ）
			□	②所掌事務又は業務及び担当者等
			□	③各システム及びそのＩＤ管理の状況
			□	④改正個人情報保護法施行による事務又は業務の変更点
			□	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
8	安全管理措置（4-8-5） 事務又は業務において取り扱う保有個人情報の取扱状況（性質及び量を含む）の把握		□	保有個人情報の取扱いについて、規程を整備しているか
			□	保有個人情報の取扱件数等を把握しているか
9	安全管理措置（4-8-5(1)、(2)、(3)） アクセス制限	※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	□	アクセス権限の管理に関する規定を整備しているか
			□	アクセス権限の管理に関する手順書又はマニュアル等を整備しているか
			□	アクセス権限を管理しているか ※管理している場合、どのように管理しているか （職員、担当業務、課室等ごとに管理、人事異動期に確認しているなど）
			□	保有個人情報の秘匿性等その内容に応じて、当該保有個人情報にアクセスする権限を有する職員の範囲を、当該職員が業務を行う上で必要最小限の範囲に限定しているか
			□	保有個人情報の秘匿性等その内容に応じて、当該保有個人情報にアクセスする権限を有する職員の権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限定しているか
			□	アクセス権限を有しない職員が、保有個人情報にアクセスしていないか ※注意喚起しているか
			□	アクセス権限を有する職員が、業務上の目的以外の目的で保有個人情報にアクセスしていないか、アクセスは必要最小限としているか ※注意喚起しているか

番号	監査項目等			
	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
10	安全管理措置（4-8-5(4)） 複製等の制限		□	複製等の制限に関する規定を整備しているか
			□	複製等の制限に関する手順書又はマニュアル等を整備しているか
			□	保護管理者は、保有個人情報の複製については、当該行為を行うことができる場合を必要最小限に限定し、職員は、保護管理者の指示に従っているか。 ※行っている場合、どのように実施しているか（許可された外部記録媒体のみ接続を許可など）
			□	保護管理者は、保有個人情報の送信については、当該行為を行うことができる場合を必要最小限に限定し、職員は、保護管理者の指示に従っているか。 ※行っている場合、どのように実施しているか（送信する際には許可が必要、記録しているなど）
			□	保護管理者は、保有個人情報が記録されている媒体の外部への送付又は持ち出しについては、当該行為を行うことができる場合を必要最小限に限定し、職員は、保護管理者の指示に従っているか。 ※行っている場合、どのように実施しているか（持ち出しする際には許可が必要、記録しているなど）
			□	保護管理者は、上記の他保有個人情報の適切な管理に支障を及ぼすおそれのある行為については、当該行為を行うことができる場合を必要最小限に限定し、職員は、保護管理者の指示に従っているか。 ※行っている場合、どのように実施しているか
11	安全管理措置（4-8-5(5)） 誤りの訂正等		□	誤りの訂正等に関する規定を整備しているか
			□	誤りの訂正等に関する手順書又はマニュアル等を整備しているか
			□	職員は、保有個人情報の内容に誤り等を発見した場合には、保護管理者の指示に従い、訂正等を行っているか ※行っている場合、どのように実施しているか（上長の許可が必要など）
12	安全管理措置（4-8-5(6)） 媒体の管理等		□	媒体の管理等（保管、送付、持ち出し）に関する規定を整備しているか
			□	媒体の管理等に関する手順書又はマニュアル等を整備しているか
			□	職員は、保護管理者の指示に従い、保有個人情報が記録されている媒体を定められた場所に保管しているか、必要があると認めるときは、耐火金庫への保管、施錠等を行っているか ※行っている場合、どのように実施しているか（施錠できるキャビネットに保管など）
			□	保有個人情報が記録されている媒体を外部へ送付し又は持ち出す場合の運用はどのようになっているか 特に、外部への送付又は持ち出す場合の許可はどのようになっているか
			□	保有個人情報が記録されている媒体を外部へ送付し又は持ち出す場合の記録を作成しているか
			□	職員は、保有個人情報が記録されている媒体を外部へ送付し又は持ち出す場合には、パスワード等（パスワード、IC カード、生体情報等をいう。）を使用して権限を識別する機能を設定する等のアクセス制御のために必要な措置を講じているか ※行っている場合、どのように実施しているか（手動又は自動的にパスワードを設定など）
13	安全管理措置（4-8-5(7)） 誤送付等の防止		□	誤送付等の防止に関する規定を整備しているか
			□	誤送付等の防止に関する手順書又はマニュアル等を整備しているか
			□	職員は、保有個人情報を含む電磁的記録又は媒体の誤送信・誤送付、誤交付、又はウェブサイト等への誤掲載を防止するため、個別の事務・事業において取り扱う個人情報の秘匿性等その内容に応じ、複数の職員による確認やチェックリストの活用等の必要な措置を講じているか ※行っている場合、どのように実施しているか（ダブルチェックしている、一時保留されるなど）
14	安全管理措置（4-8-5(8)） 廃棄等		□	保有個人情報又は保有個人情報が記録されている書類・媒体の廃棄等に関する規定を整備しているか
			□	保有個人情報又は保有個人情報が記録されている書類・媒体の廃棄に関する手順書又はマニュアル等を整備しているか
			□	職員は、保有個人情報又は保有個人情報が記録されている媒体（端末及びサーバに内蔵されているものを含む。）が不要となった場合には、保護管理者の指示に従い、当該保有個人情報の復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行っているか ※行っている場合、どのように実施しているか（復元又は判読が不可能な方法を採用しているか）
			□	職員は、保有個人情報の消去又は保有個人情報が記録されている媒体の廃棄を行った場合、消去又は廃棄の記録を保存しているか
			□	保有個人情報の消去や保有個人情報が記録されている媒体の廃棄を委託する場合（二以上の段階にわたる委託を含む。）には、必要に応じて職員が消去及び廃棄に立ち会い、又は写真等を付した消去及び廃棄を証明する書類を受け取るなど、委託先において消去及び廃棄が確実に行われていることを確認しているか ※行っている場合、どのように実施しているか（証明書を受領、立ち会うなど）

番号	監査項目等			
	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
15	安全管理措置（4-8-5(9)） 保有個人情報の取扱状況の記録	記録	□	保有個人情報の取扱状況の記録に関する規定を整備しているか
			□	保有個人情報の取扱状況の記録に関する手順書又はマニュアル等を整備しているか
			□	保護管理者は、保有個人情報の秘匿性等その内容に応じて、台帳等を整備して、当該保有個人情報の利用及び保管等の取扱いの状況について記録しているか
16	安全管理措置（4-8-5(10)） 外的環境の把握		□	外的環境の把握に関する規定を整備しているか
			□	外的環境の把握に関する手順書又はマニュアル等を整備しているか
			□	保有個人情報が、外国において取り扱われる場合、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、保有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 ※行っている場合、どのように実施しているか（外部専門家に調査依頼、情報サービスの利用など）
4－8－6　情報システムにおける安全管理措置				
17	安全管理措置（4-8-6(1)、(2)） アクセス制御		□	情報システムにアクセスするための認証機能の設定等のアクセス制御に関する規定（ユーザID、パスワード、生体情報等の設定及び見直し等）を整備しているか
			□	情報システムにアクセスするための認証機能の設定等のアクセス制御に関する手順書又はマニュアル等を整備しているか
			□	保護管理者は、保有個人情報（情報システムで取り扱うものに限る。）の秘匿性等その内容に応じて、認証機能を設定する等のアクセス制御のために必要な措置を講じているか ※行っている場合、どのように実施しているか（二要素認証など）
			□	保護管理者は、アクセス制御のために必要な措置を講ずる場合、パスワード等の管理に関する定めを整備（その定期又は随時の見直しを含む。）しているか
			□	保護管理者は、アクセス制御のために必要な措置を講ずる場合、パスワード等の読取防止等を行うために必要な措置を講じているか ※行っている場合、どのように実施しているか（パスワードポリシーを策定し、運用しているなど）
18	安全管理措置（4-8-6(3)、(4)） アクセス記録		□	アクセス状況の記録、保存、分析に関する規定を整備しているか
			□	アクセス状況の記録、保存、分析に関する手順書又はマニュアル等を整備しているか
		記録	□	保有個人情報へのアクセス状況を記録しているか
		保存	□	保有個人情報へのアクセス状況の記録を保存しているか ※行っている場合、どのように実施しているか（自動的に保存している、記録の保存を委託しているなど）
			□	保有個人情報へのアクセス状況の記録を一定の期間保存しているか ※行っている場合、どの程度保存しているか（１年間以上保存など）
		分析	□	保有個人情報へのアクセス状況の記録について、分析しているか ※行っている場合、どのように実施しているか（システムによる分析、分析を委託しているなど）
			□	保有個人情報へのアクセス状況の記録について、定期的に分析しているか ※行っている場合、どの程度の頻度で実施しているか（おおむね●か月に一度行っているなど）
		改ざん等の防止	□	保有個人情報へのアクセス状況の記録の改ざん、窃取又は不正な消去の防止のために必要な措置を講じているか ※行っている場合、どのように実施しているか（アクセスできる者を限定するなど）
19	安全管理措置（4-8-6(5)） アクセス状況の監視		□	アクセス状況の監視に関する規定を整備しているか
			□	アクセス状況の監視に関する手順書又はマニュアル等を整備しているか
			□	保護管理者は、保有個人情報の秘匿性等その内容及びその量に応じて、当該保有個人情報への不適切なアクセスの監視のため、保有個人情報を含む又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合に警告表示がなされる機能の設定、当該設定の定期的確認等の必要な措置を講じているか ※行っている場合、どのように実施しているか（資産管理ソフトの使用、監視を委託しているなど）
20	安全管理措置（４-8-6(6)） 管理者権限の設定		□	管理者権限の設定に関する規定を整備しているか
			□	管理者権限の設定に関する手順書又はマニュアル等を整備しているか
			□	保護管理者は、保有個人情報の秘匿性等その内容に応じて、情報システムの管理者権限の特権を不正に窃取された際の被害の最小化及び内部からの不正操作等の防止のため、当該特権を最小限とする等の必要な措置を講じているか ※行っている場合、どのように実施しているか（限られた者に付与するなど）

番号	監査項目等			
	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
21	安全管理措置（4-8-6(7)） 外部からの不正アクセスの防止	※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	□	外部からの不正アクセスの防止に関する規定を整備しているか
			□	外部からの不正アクセスの防止に関する手順書又はマニュアル等を整備しているか
			□	保護管理者は、保有個人情報を取り扱う情報システムへの外部からの不正アクセスを防止するため、ファイアウォールの設定による経路制御等の必要な措置を講じているか ※行っている場合、どのように実施しているか（ファイアウォールの設置、ログ等の分析による検知など）
			□	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
22	安全管理措置（4-8-6(8)） 不正プログラムによる漏えい等の防止		□	不正プログラムによる漏えい等の防止に関する規定を整備しているか
			□	不正プログラムによる漏えい等の防止に関する手順書又はマニュアル等を整備しているか
			□	保護管理者は、不正プログラムによる保有個人情報の漏えい等の防止のため、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置（導入したソフトウェアを常に最新の状態に保つことを含む。）を講じているか ※行っている場合、どのように実施しているか（脆弱性情報の確認、セキュリティパッチの適用など）
23	安全管理措置（4-8-6(9)） 情報システムにおける保有個人情報の処理		□	情報システムにおける保有個人情報の処理に関する規定を整備しているか
			□	情報システムにおける保有個人情報の処理に関する手順書又はマニュアル等を整備しているか
			□	保有個人情報について、一時的に加工等の処理を行うため複製等を行う場合に、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去しているか ※行っている場合、どのように実施しているか（定期的なクリーンアップ、当日中にシュレッダーするなど）
			□	保護管理者は、当該保有個人情報の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認しているか ※行っている場合、どのように実施しているか（注意喚起している、定期的にフォルダ等を確認するなど）
24	安全管理措置（4-8-6(10)） 暗号化		□	暗号化に関する規定を整備しているか
			□	暗号化に関する手順書又はマニュアル等を整備しているか
			□	保護管理者は、保有個人情報の秘匿性等その内容に応じて、暗号化のために必要な措置を講じているか ※行っている場合、どのように実施しているか（HDDの暗号化、パスワードの設定など）
			□	職員は、その処理する保有個人情報について、当該保有個人情報の秘匿性等その内容に応じて、適切に暗号化を行なっているか ※行っている場合、どのように実施しているか（HDDの暗号化、パスワードの設定など）
25	安全管理措置（4-8-6(11)） 記録機能を有する機器・媒体の接続制限		□	記録機能を有する機器・媒体の接続制限に関する規定を整備しているか
			□	記録機能を有する機器・媒体の接続制限に関する手順書又はマニュアル等を整備しているか
			□	保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報の漏えい等の防止のため、スマートフォン、USBメモリ等の記録機能を有する機器・媒体の情報システム端末等への接続の制限（当該機器の更新への対応を含む。）等の必要な措置を講じているか ※行っている場合、どのように実施しているか（許可された媒体のみ接続可能とするなど）
26	安全管理措置（4-8-6(12)） 端末の限定		□	端末の限定に関する規定を整備しているか
			□	端末の限定に関する手順書又はマニュアル等を整備しているか
			□	保護管理者は、保有個人情報の秘匿性等その内容に応じて、その処理を行う端末を限定するために必要な措置を講じているか ※行っている場合、どのように実施しているか（専用端末の設置など）
27	安全管理措置（4-8-6(13)、(14)） 端末の盗難防止等		□	端末の盗難防止等に関する規定を整備しているか
			□	端末の盗難防止等に関する手順書又はマニュアル等を整備しているか
			□	保護管理者は、端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠等の必要な措置を講じているか ※行っている場合、どのように実施しているか（セキュリティワイヤによる固定、執務室の施錠など）
			□	職員は、保護管理者が必要であると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んでいないか ※行っている場合、どのように実施しているか（上長の許可、記録の作成など）

番号	監査項目等			
	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
28	安全管理措置（4-8-6(15)） 第三者の閲覧防止		□	第三者の閲覧防止に関する規定を整備しているか
			□	第三者の閲覧防止に関する手順書又はマニュアル等を整備しているか
			□	職員は、端末の使用に当たっては、保有個人情報が第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講じているか ※行っている場合、どのように実施しているか（覗き見防止フィルムの貼付など）
29	安全管理措置（4-8-6(16)） 入力情報の照合等		□	入力情報の照合等に関する規定を整備しているか
			□	入力情報の照合等に関する手順書又はマニュアル等を整備しているか
			□	職員は、情報システムで取り扱う保有個人情報の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報の内容の確認、既存の保有個人情報との照合等を行っているか ※行っている場合、どのように実施しているか（ダブルチェックなど）
30	安全管理措置（4-8-6(17)） バックアップ		□	バックアップに関する規定を整備しているか
			□	バックアップに関する手順書又はマニュアル等を整備しているか
			□	保護管理者は、保有個人情報の重要度に応じて、バックアップを作成し、分散保管するために必要な措置を講じているか ※行っている場合、どのように実施しているか（週一回フルバックアップを作成するなど）
31	安全管理措置（4-8-6(18)） 情報システム設計書等の管理		□	情報システム設計書等の管理に関する規定を整備しているか
			□	情報システム設計書等の管理に関する手順書又はマニュアル等を整備しているか
			□	保護管理者は、保有個人情報に係る情報システムの設計書、構成図等の文書について外部に知られることがないよう、その保管、複製、廃棄等について必要な措置を講じているか ※行っている場合、どのように実施しているか（耐火金庫に保管するなど）
4－8－7　情報システム室等の安全管理				
32	安全管理措置（4-8-7(1)、(2)、(3)） 入退管理	※必要に応じて、情報システム室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	□	保有個人情報を取り扱う基幹的なサーバ等の機器を設置する室その他の区域（以下「情報システム室等」という。）は明確になっているか
			□	入退管理に関する規定を整備しているか
			□	入退管理に関する手順書又はマニュアル等を整備しているか
			□	情報システム室等へ持ち込む機器等の制限等に関する規定を整備しているか
			□	情報システム室等へ持ち込む機器等の制限等に関する手順書又はマニュアル等を整備しているか
			□	保護管理者は、情報システム室等に立ち入る権限を有する者を定めているか ※行っている場合、どのように実施しているか（申請による許可制など）
			□	保護管理者は、用件の確認、入退の記録、部外者についての識別化、部外者が立ち入る場合の職員の立会い又は監視設備による監視、外部電磁的記録媒体等の持込み、利用及び持ち出しの制限又は検査等の措置を講じているか ※行っている場合、どのように実施しているか（ICカード等による入退室記録、立会いの実施、外部電磁的記録媒体等の持込制限の実施など）
			□	保護管理者は、保有個人情報を記録する媒体を保管するための施設を設けている場合において、必要があると認めるときは、同様の措置を講じているか ※行っている場合、どのように実施しているか（ICカード等による入退室記録、立会いの実施、外部電磁的記録媒体等の持込制限の実施など）
			□	保護管理者は、必要があると認めるときは、情報システム室等の出入口の特定化による入退の管理の容易化、所在表示の制限等の措置を講じているか ※行っている場合、どのように実施しているか（入り口の限定、所在は非表示など）
			□	保護管理者は、情報システム室等及び保管施設の入退の管理について、必要があると認めるときは、立入りに係る認証機能を設定しているか ※行っている場合、どのように実施しているか（ICカードによる認証など）
			□	保護管理者は、情報システム室等及び保管施設の入退の管理について、必要があると認めるときは、パスワード等の管理に関する定めを整備しているか
			□	保護管理者は、情報システム室等及び保管施設の入退の管理について、必要があると認めるときは、パスワード等の読取防止等を行うために必要な措置を講じているか ※行っている場合、どのように実施しているか（生体認証による認証など）

番号	監査項目等			
	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
33	安全管理措置（4-8-7(4)、(5)） 情報システム室等の管理		□	情報システム室等の管理に関する規定を整備しているか
			□	情報システム室等の管理に関する手順書又はマニュアル等を整備しているか
			□	保護管理者は、外部からの不正な侵入に備え、情報システム室等に施錠装置、警報装置及び監視設備の設置等の措置を講じているか ※行っている場合、どのように実施しているか（情報システム室等に施錠装置を設置するなど）
			□	保護管理者は、災害等に備え、情報システム室等に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、サーバ等の機器の予備電源の確保、配線の損傷防止等の措置を講じているか ※行っている場合、どのように実施しているか（予備電源の確保など）
4－8－8　保有個人情報の提供				
34	安全管理措置（4-8-8(1)、(2)、(3)） 保有個人情報の提供		□	保有個人情報の提供を受ける者に対する措置要求に関する規定を整備しているか
			□	保有個人情報の提供を受ける者に対する措置要求に関する手順書又はマニュアル等を整備しているか
			□	保護管理者は、利用目的のために又は法第 69 条第 2 項第 3 号及び第 4 号の規定に基づき行政機関等以外の者に保有個人情報を提供する場合には、法第 70 条の規定に基づき、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について提供先との間で書面（電磁的記録を含む。）を取り交わしているか
			□	保護管理者は、利用目的のために又は法第 69 条第 2 項第 3 号及び第 4 号の規定に基づき行政機関等以外の者に保有個人情報を提供する場合には、法第 70 条の規定に基づき、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況を確認してその結果を記録するとともに、改善要求等の措置を講じているか
			□	保護管理者は、法第 69 条第 2 項第 3 号の規定に基づき他の行政機関等に保有個人情報を提供する場合において、必要があると認めるときは、法第70 条の規定に基づき、上記の措置を講じているか
4－8－9　個人情報の取扱いの委託				
35	安全管理措置 個人情報の取扱いの委託		□	業務の委託等に関する規定を整備しているか
			□	業務の委託等に関する手順書又はマニュアル等を整備しているか
36	安全管理措置(4-3-1-1、4-3-1-2) 委託先の監督		□	行政機関等が保有個人情報の取扱いを委託する場合は、行政機関等として講ずべき安全管理措置として、サイバーセキュリティに関する対策の基準等を参考に委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準（保存された情報等に対して国内法令のみが適用されること等）や委託先の選定基準を整備しているか
			□	行政機関等が保有個人情報の取扱いを委託する場合は、個人情報保護法に基づき、行政機関等として講ずべき安全管理措置として、委託先に対して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
				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
			□	委託先が個人情報取扱事業者（法第 16 条第 2 項）に該当する場合には、委託先において、個人データに関する安全管理措置を講ずべき義務（法第 23 条）も負うことを認識しているか
			□	行政機関等から個人情報の取扱いの委託を受けた者は、当該委託を受けた業務を行う場合における個人情報の取扱いについて、行政機関等と同様の安全管理措置義務を負うことを認識しているか

番号	監査項目等			
	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
37	安全管理措置(4-8-9(1)) 業務の委託等	委託先の選定	□	個人情報の取扱いに係る業務を外部に委託する場合に、個人情報の適切な管理を行う能力を有しない者を選定することがないよう、必要な措置を講じているか
		明記する事項	□	委託契約書を締結しているか
				契約書に、次の事項を明記しているか
			□	① 個人情報に関する秘密保持、利用目的以外の目的のための利用の禁止等の義務
			□	② 再委託の制限又は事前承認等再委託に係る条件に関する事項
			□	③ 個人情報の複製等の制限に関する事項
			□	④ 個人情報の安全管理措置に関する事項
			□	⑤ 個人情報の漏えい等の事案の発生時における対応に関する事項
			□	⑥ 委託終了時における個人情報の消去及び媒体の返却に関する事項
			□	⑦ 法令及び契約に違反した場合における契約解除、損害賠償責任その他必要な事項
			□	⑧ 契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱状況を把握するための監査等に関する事項（再委託先の監査等に関する事項を含む。）
		書面確認	□	委託先における責任者及び業務従事者の管理体制及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認しているか
38	安全管理措置(4-8-9(2)) 業務の委託等	委託する個人情報の範囲	□	取扱いを委託する個人情報の範囲は、委託する業務内容に照らして必要最小限であるか
39	安全管理措置(4-8-9(3)) 業務の委託等	取扱状況の把握	□	委託する業務に係る保有個人情報の秘匿性等その内容やその量等に応じて、作業の管理体制及び実施体制や個人情報の管理の状況について、少なくとも年1回以上、原則として実地検査により確認しているか
40	安全管理措置(4-8-9(4)) 業務の委託等	再委託の要件	□	保有個人情報の取扱いに係る業務を再委託をしているか
			□	保有個人情報の取扱いに係る業務を再委託をしている場合、事前承認をしているか
		再委託の際の措置		保有個人情報の取扱いに係る業務を再委託している場合、委託先に以下の措置を講じさせているか
			□	個人情報の取扱いに係る業務を外部に委託する場合は、個人情報の適切な管理を行う能力を有しない者を選定することがないよう、必要な措置を講じているか
				再委託契約書に、次の事項を明記しているか
			□	① 個人情報に関する秘密保持、利用目的以外の目的のための利用の禁止等の義務
			□	② 再委託の制限又は事前承認等再委託に係る条件に関する事項
			□	③ 個人情報の複製等の制限に関する事項
			□	④ 個人情報の安全管理措置に関する事項
			□	⑤ 個人情報の漏えい等の事案の発生時における対応に関する事項
			□	⑥ 委託終了時における個人情報の消去及び媒体の返却に関する事項
			□	⑦ 法令及び契約に違反した場合における契約解除、損害賠償責任その他必要な事項
			□	⑧ 契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱状況を把握するための監査等に関する事項（再委託先の監査等に関する事項を含む。）
			□	委託先における責任者及び業務従事者の管理体制及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認しているか
		再委託先の監督	□	保有個人情報の取扱いに係る業務が再委託されている場合、再委託される業務に係る保有個人情報の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが委託する業務に係る保有個人情報の秘匿性等その内容やその量等に応じて、作業の管理体制及び実施体制や個人情報の管理の状況について、少なくとも年1回以上、原則として実地検査により確認しているか
			□	保有個人情報の取扱いに係る業務を再々委託等をしているか
			□	保有個人情報の取扱いに係る業務を再々委託等をしている場合、事前承認をしているか

番号	監査項目等			
	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
			□	保有個人情報の取扱いに係る業務について再委託先が再々委託等をしている場合、再委託先が同様の措置を講じているか
41	安全管理措置(4-8-9(5)) 業務の委託等		□	保有個人情報の取扱いに係る業務を派遣労働者によって行わせている場合、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記しているか
42	安全管理措置（4-8-9(6)) その他		□	保有個人情報を提供し、又は業務委託する場合、漏えい等による被害発生のリスクを低減する観点から、提供先の利用目的、委託する業務の内容、保有個人情報の秘匿性等その内容などを考慮し、必要に応じ、特定の個人を識別することができる記載の全部又は一部を削除し、又は別の記号等に置き換える等の措置を講じているか
4－8－10 サイバーセキュリティの確保				
43	安全管理措置(4-8-10(1)) サイバーセキュリティに関する対策		□	サイバーセキュリティに関する対策の基準等に関する規定を整備しているか
			□	サイバーセキュリティに関する対策の基準等に関する手順書又はマニュアル等を整備しているか
			□	個人情報を取り扱い、又は情報システムを構築し、若しくは利用するに当たっては、サイバーセキュリティ基本法第 26 条第 1 項第 2 号に掲げられたサイバーセキュリティに関する対策の基準等を参考として、取り扱う保有個人情報の性質等に照らして適正なサイバーセキュリティの水準を確保しているか
4－8－11 安全管理上の問題への対応				
44	安全管理措置 安全管理上の問題への対応	漏えい等事案に対応する体制等の整備	□	漏えい等事案への対応等に関する規定を整備しているか
			□	漏えい等事案への対応等に関する手順書又はマニュアル等を整備しているか
			□	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
		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
45	安全管理措置（4-8-11(1)) 事案の報告及び再発防止措置		□	保有個人情報の漏えい等安全管理の上で問題となる事案又は問題となる事案の発生のおそれを認識した場合に、その事案等を認識した職員は、直ちに当該保有個人情報を管理する保護管理者に報告しているか
46	安全管理措置（4-8-11(2)) 事案の報告及び再発防止措置		□	保護管理者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講じているか ※行っている場合、どのように実施してるか（体制の整備、研修の実施、訓練の実施等）
			□	保護管理者は、外部からの不正アクセスや不正プログラムの感染が疑われる当該端末等の LAN ケーブルを抜くなど、被害拡大防止のため直ちに行い得る措置については、直ちに行っているか（職員に行わせることを含む）
47	安全管理措置（4-8-11(3)) 事案の報告及び再発防止措置		□	保護管理者は、事案の発生した経緯、被害状況等を調査し、総括保護管理者に報告しているか
			□	保護管理者は、特に重大と認める事案が発生した場合には、直ちに総括保護管理者に当該事案の内容等について報告しているか
48	安全管理措置（4-8-11(4)) 事案の報告及び再発防止措置		□	総括保護管理者は、保護管理者による報告を受けた場合、事案の内容等に応じて、当該事案の内容、経緯、被害状況等を行政機関の長等（独立行政法人等にあっては法人の長、地方独立行政法人にあっては理事長）に速やかに報告しているか
49	安全管理措置（4-8-11(5)) 事案の報告及び再発防止措置		□	保護管理者は、事案の発生した原因を分析し、再発防止のために必要な措置を講じているか ※行っている場合、どのように実施しているか（規程類の見直し、部局内での共有など）
			□	保護管理者は、同種の業務を実施している部局等に再発防止措置を共有しているか
50	安全管理措置（4-8-11(6)) 法に基づく報告及び通知		□	漏えい等が生じた場合であって法第 68 条第 1 項の規定による個人情報保護委員会への報告及び同条第 2 項の規定による本人への通知を要する場合、速やかに所定の手続を行うとともに、個人情報保護委員会による事案の把握等に協力しているか

番号	監査項目等			
	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
51	安全管理措置（4-8-11(7)） 公表等		□	法第 68 条第 1 項の規定による個人情報保護委員会への報告及び同条第 2 項の規定による本人への通知を要しない場合であっても、事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る保有個人情報の本人への連絡等の措置を講じているか
			□	国民の不安を招きかねない事案（例えば、公表を行う漏えい等が発生したとき、個人情報保護に係る内部規程に対する違反があったとき、委託先において個人情報の適切な管理に関する契約条項等に対する違反があったとき等）については、当該事案の内容、経緯、被害状況等について、速やかに個人情報保護委員会へ情報提供を行っているか
4 － 8 － 12　監査及び点検の実施				
52	安全管理措置 監査及び点検の実施	※監査及び点検においては、他の機関から求められている監査及び点検がある場合があることから、当該項目を記載している。	□	監査に係る規定を整備しているか
			□	監査に係る手順書又はマニュアル等を整備しているか
			□	監査計画（監査の観点、監査周期等）は定めているか
53	安全管理措置（4-8-12(1)） 監査		□	監査責任者は、保有個人情報の適切な管理を検証するため、4-8-2（管理体制）から4-8-11（安全管理上の問題への対応）までに記載する措置の状況を含む当該行政機関等における保有個人情報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（外部監査を含む。以下同じ。）を行っているか
			□	監査の実施結果を記録しているか
			□	監査責任者は、監査の結果を総括保護管理者に報告しているか
54	安全管理措置(4-8-12(2)) 点検		□	点検に関する規定を整備しているか
			□	保護管理者は、各課室等における保有個人情報の記録媒体、処理経路、保管方法等について、定期に、及び必要に応じ随時に点検を行っているか
			□	保護管理者は、点検の結果を総括保護管理者に報告しているか
55	安全管理措置(4-8-12(3)) 評価及び見直し		□	総括保護管理者、保護管理者等は、監査又は点検の結果等を踏まえ、実効性等の観点から保有個人情報の適切な管理のための措置について評価し、必要があると認めるときは、その見直し等の措置を講じているか

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（保有個人情報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
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 (4-8-1)	保有個人情報の管理規程、取扱規程の前提となる規程（訓令）	①個人情報保護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
4	安全管理 (4-8-1)	保有個人情報の管理規程、取扱規程	①保有個人情報の具体的な取扱いを定めた管理規程、取扱規程（取得、利用、保存、提供、削除・廃棄の規程を含む。） ②（保有個人情報の）文書管理に関する規程
5	安全管理 (4-8-1)	保有個人情報を取り扱う事務又は業務の概要が分かる資料	保有個人情報を取り扱う事務又は業務に関する以下の規程等 ①事務又は業務の手順書 ②事務又は業務の処理手引き・マニュアル ③本省、地方支分部局（又は、本所、支所、分庁舎等）における事務又は業務の役割分担が分かる資料 ④事務又は業務の全体のフロー図 ⑤監査対象となる事務又は業務の所管課等のフロア図、座席表 ⑥事務連絡
6	安全管理 (4-8-1)	保有個人情報取扱件数が分かる資料 （前年度及び当年度）	①保有個人情報が記載される届出書、申請書等の取扱件数が分かる資料 （前年度及び当年度の同書類の取扱件数）
7	安全管理 (4-8-2)	組織体制の整備状況が分かる資料	①組織体制の整備状況が分かる資料 総括保護管理者・保護管理者・保護担当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
8	安全管理 (4-8-3)	保有個人情報の取扱いに従事する職員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教育研修に関する規定 ②教育（研修）計画 ③保有個人情報の取扱いに従事する職員に、教育を実施していることが分かる資料 ④保有個人情報を取り扱う情報システムの管理に関する事務に従事する職員に、教育を実施していることが分かる資料 ⑤保護管理者及び保護担当者に、教育を実施していることが分かる資料 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
9	安全管理 (4-8-5(1)、(2)、(3))	アクセス制限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、付与手順、人数が分かる資料 ③アクセス権限申請書、登録簿、付与簿等 ④情報システムのアクセスログの確認に関する規定及び手順書又はマニュアル等 ⑤アクセスログの記録
10	安全管理 (4-8-5(4))	複製等の制限措置状況が分かる資料	①複製等の制限に関する規定及び手順書又はマニュアル等 ②保有個人情報の複製の制限状況が分かる資料（記録簿を含む。） ③保有個人情報の送信の制限状況が分かる資料（記録簿を含む。） ④保有個人情報が記録されている媒体の外部への送付又は持ち出しの制限状況が分かる資料（記録簿を含む。）
11	安全管理 (4-8-5(5))	誤り等の訂正等の措置状況が分かる資料	①誤りの訂正等に関する規定及び手順書又はマニュアル等 ②誤りの訂正等を行なった場合の対応状況が分かる資料

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）
12	安全管理 (4-8-5(6))	媒体の管理等の措置状況が分かる資料	①媒体の管理・使用（使用許可等）に関する規定及び取扱規程（手順書又はマニュアル等） ②媒体の管理簿、運用管理台帳、貸出簿（管理者・使用者・期間・使用後のデータ消去等） ③媒体の登録申請、使用申請、利用申請、購入申請等に関する資料 ④媒体の管理・保管状況が分かる資料 ⑤保有個人情報が記録又は記載された媒体の外部への送付又は持ち運ぶ際の規定及び手順書又はマニュアル等 ⑥紛失、盗難防止等に関する周知文、指示文、研修資料等 ⑦紛失、盗難防止等の実施状況が分かる資料 ⑧媒体の使用簿、持出管理簿等（使用者・期間・使用後のデータ消去等）
13	安全管理 (4-8-5(7))	誤送付等の防止の措置状況が分かる資料	①誤送付等の防止に関する規定及び手順書又はマニュアル等 ②誤送付等の防止に関する職員向け周知資料（通知文、掲示文、研修資料等） ③誤送付等の防止の実施状況が分かる資料
14	安全管理 (4-8-5(8))	廃棄等が分かる資料	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・廃棄に関する規定及び手順書又はマニュアル等 ④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）
15	安全管理 (4-8-5(9))	保有個人情報の取扱状況の記録の状況が分かる資料	①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
16	安全管理 (4-8-5(10))	外的環境の把握状況が分かる資料	①外国における保有個人情報の取扱状況が分かる資料（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保有個人情報の取扱いを委託している場合は、当該委託先の選定基準、当該委託先に対する監督の実施状況が分かる資料
17	安全管理 (4-8-6(1)、(2))	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関する規定及び手順書又はマニュアル等（パスワードポリシーも含む） 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 ③ユーザID、パスワードの管理簿、管理台帳等
18	安全管理 (4-8-6(3)、(4))	アクセス記録を分析等していることが分かる資料	①アクセス記録の記録、保存、分析に関する規定及び手順書又はマニュアル等 ②アクセス状況を記録、保存していることが分かる資料 ③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 ④記録の改ざん、窃取又は不正な消去の防止の措置を講じていることが分かる資料
19	安全管理 (4-8-6(5))	アクセス状況の監視状況が分かる資料	①アクセス状況の監視に関する規定及び手順書又はマニュアル等 ②基盤運用設計書、基本設計書等 ③一定量以上の情報が情報システムからダウンロードされた場合に警告表示がなされる機能の設定状況、当該設定の定期的確認等の実施状況が分かる資料
20	安全管理 (4-8-6(6))	管理者権限の設定状況が分かる資料	①管理者権限の設定に関する規定及び手順書又はマニュアル等 ②管理者権限の設定状況が分かる資料

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 (4-8-6(7))	外部からの不正アクセスの防止の状況が分かる資料	①外部からの不正アクセスの防止に関する規定及び手順書又はマニュアル等 ②情報システムの構成図、接続状況や運用体制の整備状況が分かる資料 ③情報システムの概要・機能等の説明資料 ④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 ⑤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 ⑥情報提供ネットワークシステムの利用頻度（xx件/月など） ⑦情報システムの不正アクセスへの対策が分かる資料 ⑧アクセス状況の監視方法や警告機能等の設定状況が分かる資料 ⑨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
22	安全管理 (4-8-6(8))	不正プログラムによる漏えい等の防止の状況が分かる資料	①不正プログラムによる漏えい等の防止に関する規定及び手順書又はマニュアル等 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、ウイルススキャンの頻度、パターンファイルの更新頻度が分かる資料 ③セキュリティ対策情報（セキュリティパッチ、ソフトウェアアップデート情報等）の収集体制や適用方針が分かる資料、適用記録等
23	安全管理 (4-8-6(9))	情報システムにおける保有個人情報の処理の状況が分かる資料	①情報システムにおける保有個人情報の処理に関する規定及び手順書又はマニュアル等 ②職員への周知文、指示文、研修資料等 ③処理の実施状況を確認したことが分かる資料
24	安全管理 (4-8-6(10))	暗号化の状況が分かる資料	①暗号化に関する規定及び手順書又はマニュアル等 ②職員への周知文、指示文、研修資料等
25	安全管理 (4-8-6(11))	記録機能を有する機器・媒体の接続制限の状況が分かる資料	①記録機能を有する機器・媒体の接続制限に関する規定及び手順書又はマニュアル等 ②職員への周知文、指示文、研修資料等 ③接続制限の実施状況（技術的制限、物理的制限、運用による制限）が分かる資料
26	安全管理 (4-8-6(12))	端末の限定の状況が分かる資料	①端末の限定に関する規定及び手順書又はマニュアル等 ②保有個人情報を処理する端末を限定していることが分かる資料
27	安全管理 (4-8-6(13)、(14))	端末の盗難防止等の措置状況が分かる資料	①端末の盗難防止等に係る規定及び手順書又はマニュアル等 ②端末の固定、執務室の施錠等の実施状況が分かる資料 ③端末の外部への持ち出し、又は、外部から持ち込みの防止措置等の状況並びに記録
28	安全管理 (4-8-6(15))	第三者の閲覧防止の措置状況が分かる資料	①第三者の閲覧防止に関する規定及び手順書又はマニュアル等 ②職員への周知文、指示文、研修資料等 ③第三者の閲覧防止の措置状況が分かる資料
29	安全管理 (4-8-6(16))	入力情報の照合等の状況が分かる資料	①入力情報の照合等に関する規定及び手順書又はマニュアル等 ②職員への周知文、指示文、研修資料等 ③入力原票と入力内容との照合、処理前後の当該保有個人情報の内容の確認、既存の保有個人情報との照合等の実施状況が分かる資料
30	安全管理 (4-8-6(17))	バックアップの作成等の状況が分かる資料	①バックアップに関する規定及び手順書又はマニュアル等 ②バックアップの作成、分散保管の状況が分かる資料

番号	安全管理措置等の分類	資料（大分類）	資料（小分類）
31	安全管理 （4-8-6(18)）	情報システム設計書等の管理の状況が分かる資料	①情報システム設計書等の管理に係る規定及び手順書又はマニュアル等 ②保有個人情報に係る情報システムの設計書、構成図等の文書の保管、複製、廃棄等の状況が分かる資料
32	安全管理 （4-8-7(1)、(2)、(3)）	入退管理の状況が分かる資料	①情報システム室等の区域の設定に関する規定、又は、それぞれの区域が分かる資料 ②情報システム室等の入退室管理に関する規定及び手順書又はマニュアル等 【保有個人情報を取り扱う情報システムに係る入退出管理】 ③情報システム室等（システム設置場所）の概要図、配置図 ④情報システム室等の出入口の特定化の状況、所在表示の制限等の状況 ⑤情報システム室等に立ち入る者の基準及び指定状況が分かる資料 ⑥情報システム室等への入退室管理の状況が分かる資料（鍵の貸出を含む。） ⑦情報システム室等の立入りに係るID、パスワード認証の概要（パスワード等の読取防止等を行うための措置状況が分かる資料を含む。） ⑧入退室管理カード等の貸与、保管、貸出状況が分かる資料 情報システム室等に部外者が立ち入る場合の立会い又は監視設備による監視の状況が分かる資料 【外部電磁的記録媒体等の持込み等の制限等】 ⑨情報システム室等への外部電磁的記録媒体等の持込み等の制限等に関する規定及び手順書又はマニュアル等 ⑩情報システム室等への外部電磁的記録媒体等の持込み等の制限等の実施状況が分かる資料 【保有個人情報を記録する媒体を保管するための施設を設けている場合】 ⑪上記と同様の措置を講じていることが分かる資料
33	安全管理 （4-8-7(4)、(5)）	情報システム室等の管理状況が分かる資料	①情報システム室等の管理に関する規定及び手順書又はマニュアル等 ②情報システム室等の施錠・警報・監視設備の状況が分かる資料 ③情報システム室等に、耐震、防火、防煙、防水等の必要な措置を講じていることが分かる資料 ④サーバ等の機器の予備電源の確保、配線の損傷防止等の措置を講じていることが分かる資料
34	安全管理 （4-8-8(1)、(2)、(3)）	保有個人情報を提供する際の提供先の安全管理措置の確認の実施状況が分かる資料	①保有個人情報の提供に関する規定及び手順書又はマニュアル等 ②保有個人情報の提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について提供先との間で書面（電磁的記録を含む。）を取り交わしていることが分かる資料 ③行政機関等以外の者に保有個人情報を提供する場合に、安全確保の措置を要求していることが分かる資料 ④行政機関等以外の者に保有個人情報を提供する場合に、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況を確認してその結果を記録するとともに、改善要求等の措置を講じていることが分かる資料 ⑤他の行政機関等に保有個人情報を提供する場合に、必要があると認めるときは、上記②、③及び④の措置を講じていることが分かる資料

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）
35	安全管理 (4-8-9(1)、(2)、(3)、(4)、(5))	個人情報の取扱いの委託を行う際に講じている措置の状況が分かる資料	①業務の委託等に関する規定及び手順書又はマニュアル等 特に、委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準や委託先の選定基準を整備していることが分かる資料 ②委託契約書、仕様書等(必要な事項を明記していることが分かる資料、委託内容を示す資料) 特に、取扱いを委託する個人情報の範囲を委託する業務内容に照らして必要最小限にしていることが分かる資料 ③委託先を適切に選定していることが分かる書類 特に、委託先における責任者及び業務従事者の管理体制及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認していることが分かる資料 ④委託先に対する監督内容が分かる資料 (委託先の保有個人情報の取扱規程等を含む。) ⑤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） ⑥委託先における作業の管理体制及び実施体制や個人情報の管理の状況について、実地検査により確認していることが分かる資料 ⑦委託先における返却、廃棄、消去の台帳等 ⑧再委託等をしている場合の通知書、許諾書等 ⑨再委託等をしている場合、委託先が上記①、②、③、④及び⑥の措置を講じていること、委託先と再委託先との委託契約書に明記していることを確認していることや再委託先における責任者及び業務従事者の管理体制及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認していることが分かる資料 ⑩委託先を通じて又は委託元が再委託先等における作業の管理体制及び実施体制や個人情報の管理の状況について、実地検査により確認していることが分かる資料 ⑪労働者派遣契約書
36	安全管理 (4-8-9(6))	保有個人情報の提供又は業務委託する場合の提供する保有後人情報が分かる資料	①提供先の利用目的、委託する業務の内容、保有個人情報の秘匿性等その内容などを考慮し、必要に応じ、特定の個人を識別することができる記載の全部又は一部を削除し、又は別の記号等に置き換える等の措置を講じていることが分かる資料
37	安全管理 (4-8-10(1))	サイバーセキュリティに関する対策の実施状況が分かる資料	①サイバーセキュリティに関する対策に関する規定及び手順書又はマニュアル等 ②個人情報を取り扱い、又は情報システムを構築し、若しくは利用する場合に、サイバーセキュリティ基本法第 26 条第 1 項第 2 号に掲げられたサイバーセキュリティに関する対策の基準等を参考として、取り扱う保有個人情報の性質等に照らして適正なサイバーセキュリティの水準を確保していることが分かる資料
38	安全管理 (4-8-11(1)、(2)、(3)、(4)、(5)、(6)、(7))	安全管理上の問題への対応状況が分かる資料	①漏えい等の事案等が発覚した際の対応方法（報告・連絡、公表時期等）を定めた規定及び手順書又はマニュアル等 ②報告体制、報告様式、報告フロー図、連絡先一覧表等 ③対応・報告要領等の職員への周知文、指示文、研修資料等 ④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（事案の報告（内部及び外部（個人情報保護委員会を含む））、被害の拡大防止又は復旧等の措置、再発防止措置、本人への通知、公表等） ⑤標的型攻撃等を想定した確認・訓練の計画書 ⑥確認・訓練の実施状況が分かる資料等
39	安全管理 (4-8-12(1))	監査及び点検の実施状況が分かる資料 （監査に関する資料）	【監査】 ①監査に関する規定及び手順書又はマニュアル等 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、監査責任者が総括保護管理者に報告したことが分かる資料

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）
40	安全管理 (4-8-12(2))	監査及び点検の実施状況が分かる資料 （点検に関する資料）	【点検】 ①点検に関する規定及び手順書又はマニュアル等 ②点検の実施状況が分かる資料 ③点検結果について、保護管理者が総括保護管理者に報告したことが分かる資料
41	安全管理 (4-8-12(3))	監査及び点検の実施状況が分かる資料 （評価及び見直しに関する資料）	【評価及び見直し】 ①総括保護管理者、保護管理者等が、監査又は点検の結果等を踏まえ、保有個人情報の適切な管理のための措置について評価し、必要があると認めるときは、その見直し等の措置を講じていることが分かる資料

○　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。