参考

特定個人情報保護評価書における共通・標準的なリスク対策について

令和７年度

個人情報保護委員会事務局

愛称：おサル博士

目　次

１．はじめに

（１）資料の位置付け

（２）想定する利用対象者

（３）見方

1．はじめに

（1）資料の位置付け

本資料は、毎年度、個人情報保護委員会（以下「委員会」）の年次報告で公表されている立入検査における不備事項のうち、上位を占めるカテゴリーについて、公表されている特定個人情報保護評価書（以下「評価書」）では、それらに対応するものとして、どのようなリスク対策が記載されているかをお示しする「参考情報」です。そのため、監査との関連性が分かるように、「地方公共団体等における監査のためのチェックリスト（令和６年12月最終改正）」に関連する確認項目についても示しています。

（2）想定する利用対象者

本資料は、地方公共団体等の実務担当者のうち、異動等により初めて特定個人情報保護評価（以下「保護評価」）の業務を担当する方などを想定しています。

＜本資料の活用例＞

事例から具体的なリスク対策を把握し、保護評価の実施に当たっての参考としたり、監査のチェックリストに基づき事務の内部監査を実施し、その際、該当するリスク対策が評価書のどこに記載されているかを確認し、評価書の見直しを検討することもできます。

＜ご注意＞

本資料に記載したリスク対策の具体例は、「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）」も踏まえ、公表されている評価書を元に、多くの評価実施機関にとって関連性が深いと考えられる内容を引用しています。評価実施機関の事務の性質や実情によってリスクの態様も様々と考えられるため、本資料に記載されたリスク対策の具体例が、必ずしも全ての評価実施機関に当てはまるものではなく、評価書に全て記載したことをもって、最適な評価書であることが保証されるものではないことに十分ご留意ください。

（3）見方

入手	使用	委託	提･移
NWS	保･消	その他	

XXXXX

不備が認められやすい安全管理措置の概要等を記載しています。

特定個人情報を取り扱うライフサイクル（次頁参照）のうち、どのフェーズと関連が強いかを示しています。

参考資料

監査チェックリスト

・項番XX

地方公共団体等における監査のためのチェックリストの関連番号を記載しています。

その他

・「XXXXX」
URL:

委員会が公表している参考資料を示しています。

リスク対策（例）

【○○○】

XXXXXXXX　Ⅲ.○.○

公表されている既存の評価書で記載されているリスク対策（参考）

全項目評価書の主な記載箇所

（参考）特定個人情報を取り扱うライフサイクル

○　保護評価の実施に当たっては、特定個人情報の取扱いを場面ごとに整理してリスクを識別・分析することが重要です。

（例）給付金の支給事務における特定個人情報を取り扱うライフサイクル

	本人	評価実施機関	他の行政機関	委託先
入手	窓口等で（個人番号、４情報、業務関係情報）の入力		情報提供ネットワークシステムによる照会（個人番号、税情報）	
使用		・登録簿の管理 ・給付金の支給		
委託				システムの運用
提供・移転			情報提供ネットワークシステムによる提供（個人番号、業務関連情報）	
NWS			情報提供ネットワークシステムによる照会・提供	
保管・消去		保存期間終了後、速やかに削除		

２．リスク対策

（１）ログの分析

（２）教育研修

（３）監査

（４）委託及び再委託

（５）電子媒体の管理及び使用

（１）ログの分析

○　令和６年度上半期における立入検査の結果、「ログの分析」に関して、９割の地方公共団体等で、技術的安全管理措置の不備事項が認められています。

○　特定個人情報等を不必要に閲覧・持ち出しをしていないか、不正アクセスを受けていないか等を確認するために、ログを定期に及び必要に応じ随時に分析等するための体制を整備する必要があります。記録については、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ずるとともに、分析等を行うことも重要です。

参考資料

監査チェックリスト

○項番13
（記録/保存/分析/改ざん等の防止）
https://www.ppc.go.jp/files/pdf//check_list_MN_2412.pdf

その他

○特定個人情報等の利用状況のログ分析・確認について
https://www.ppc.go.jp/files/pdf/log_bunseki.pdf

リスク対策（例）

事務に必要な各種情報の庁内連携機能からの入手については、「誰が」「いつ」「どのような操作をしたのか」、個人単位の操作ログを追跡可能な形式で管理している。	Ⅲ.2 Ⅲ.3
収集した操作ログについては完全性を担保し、容易に改ざんできない対策を施し、●年間保管している。	Ⅲ.2
個人単位の操作ログの収集については、周知することで不要な操作を抑止している。	Ⅲ.2
操作ログの記録は、毎月●回情報セキュリティ責任者が検査・分析を行い、不正なアクセスがないことを確認する。	Ⅲ.3

（２）教育研修 １/２

○　令和６年度上半期における立入検査の結果、「教育研修」に関して、８割の地方公共団体等で、人的安全管理措置の不備事項が認められました。
○　総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適正な取扱いについて理解を深め、特定個人情報等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教育研修を行うことが重要です。

参考資料

監査チェックリスト

○項番18
（教育研修/番号法に定められた研修）

その他

○特定個人情報の漏えい等の防止について
https://www.ppc.go.jp/files/pdf/rouei_boushi.pdf

リスク対策（例）

【教育・研修】

新規採用時の研修や各階層別等の研修において、個人情報保護・情報セキュリティを定めた規定等についての説明と周知を徹底している。	Ⅳ.２
毎年、情報セキュリティ対策強化月間を設定し、情報セキュリティや個人情報の取扱いに関する自己点検・職場研修を実施している。	Ⅳ.２
研修の未受講者に対しては、再受講の機会を付与している。	Ⅳ.２
委託先事業者においても、職員に対する情報セキュリティ研修を実施させている。	Ⅳ.１ .②

（2）教育研修 2/2

○　特定個人情報等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、特定個人情報等の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修を行うことも重要です。

参考資料

監査チェックリスト	その他
○項番18 （教育研修/番号法に定められた研修）	○特定個人情報の漏えい等の防止について https://www.ppc.go.jp/files/pdf/rouei_boushi.pdf

リスク対策（例）

【マニュアル等の整備・周知】

各システムの操作マニュアルにセキュリティの項目を設け、操作の際に特に注意を要する点を記載している。	Ⅳ.１.②
セキュリティ関連規程等に変更があった場合は、それに基づくシステムの情報セキュリティ対策実施手順についても適宜必要な見直しを行っている。 見直しを行った場合は利用部署等に周知し、情報セキュリティ対策の徹底を図るよう指導している。	Ⅳ.２

（3）監査

○　令和６年度上半期における立入検査の結果、「監査」に関して、７割の地方公共団体等で、組織的安全管理措置の不備事項が認められました。
○　監査責任者は、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（外部監査及び他部署等による点検を含む。）を行い、監査の結果等を踏まえ、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も重要です。

参考資料

監査チェックリスト

○項番16（点検/監査）
○項番17（事務取扱担当者の監督）

その他

○地方公共団体等における特定個人情報等に関する監査実施マニュアル ～はじめての監査のために～
https://www.ppc.go.jp/files/pdf/kansa_manual.pdf

リスク対策（例）

【監査】

紙媒体の保管状況や電子媒体の作業状況については、監査部門が定期的に漏えい・紛失がないかチェックしている。	Ⅲ.２.

【自己点検】

定期的に担当部署内において実施している自己点検に用いるチェック項目に、「評価書の記載内容通りの運用がなされていること」に係る内容を追加し、運用状況を確認する。	Ⅳ.１.①
所属長は部署の職員及び委託先事業者に対し、事務作業の中で遵守しなければならないルールを設定し、毎年●回又は必要に応じて自主点検を実施させることにより、情報セキュリティ対策の実施状況について確認するとともに、改善に取り組む。	Ⅳ.１.①

（４）委託及び再委託　1/3

○　令和６年度上半期における立入検査の結果、３割の地方公共団体等で、委託及び再委託に関する安全管理措置の不備事項が認められました。
○　委託先に安全管理措置を遵守させるために必要な委託契約の締結については、契約内容として、従業者に対する監督・教育、契約内容の遵守状況について報告を求める規定等を盛り込むことも重要です。

参考資料

監査チェックリスト

○項番７（委託先の監督）
○項番８（委託先の選定/契約内容/取扱状況の把握）
○項番９（再委託の要件）
○項番10（再委託の効果）
○項番11（再委託先の監督）

その他

○特定個人情報等のデータ入力業務の委託先に対する監督について
https://www.ppc.go.jp/files/pdf/itaku_kanntoku.pdf

リスク対策（例）【平時の管理・監督】

特定個人情報が記録されたサーバ等での作業については、事前に作業報告の提出を求める。	Ⅲ.４
委託業務は委託元の作業場所（庁舎内）のみで行うこととし、特定個人情報ファイルの外部への持ち出しを認めない。	Ⅲ.４
委託業者に特定個人情報を提供する際、日付・場所・担当者・数量等の情報を記録した受領管理簿に確認印を押印等させ、委託元の評価実施機関の管理者が確認する。委託業者から受領する場合も同様とする。記録は●年間保存する。	Ⅲ.４
運搬及び保管業務の委託の場合、庁舎の外部で特定個人情報を取り扱うことになるが、直接的に個人情報にアクセスすることはなく、また、基本的な個人情報の取扱いについて契約条項に定めている。	Ⅲ.４

（4）委託及び再委託　2/3

○　委託先に安全管理措置を遵守させるために必要な委託契約の締結については、契約内容として、従業者に対する監督・教育、契約内容の遵守状況について報告を求める規定を盛り込むとともに、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を盛り込むことも重要です。

参考資料

監査チェックリスト

○項番７（委託先の監督）
○項番８（委託先の選定/契約内容/取扱状況の把握）
○項番９（再委託の要件）
○項番10（再委託の効果）
○項番11（再委託先の監督）

その他

○特定個人情報等のデータ入力業務の委託先に対する監督について
https://www.ppc.go.jp/files/pdf/itaku_kanntoku.pdf

リスク対策（例）

【定期の管理・監督】

委託先において特定個人情報ファイルの管理状況の検査を年●回実施し、書面にて評価実施機関に報告する。	Ⅲ.4
必要に応じて、委託先への立入検査を実施する。	Ⅲ.4

【委託先における教育】

評価実施機関における独自例規等を含む個人情報の保護に関する関連法令に基づき、委託先においても個人情報の適正な取扱い及び罰則の内容並びに民事上の責任についての研修を実施させるとともに、個人情報保護に関する誓約書を委託先から提出させる。	Ⅲ.4

（４）委託及び再委託　3/3

○　委託先に安全管理措置を遵守させるために必要な委託契約の締結については、契約内容として、委託契約終了後の特定個人情報の返却又は廃棄に関する規定についても盛り込むことも重要です。

参考資料

監査チェックリスト

○項番７（委託先の監督）
○項番８（委託先の選定/契約内容/取扱状況の把握）
○項番９（再委託の要件）
○項番10（再委託の効果）
○項番11（再委託先の監督）

その他

○特定個人情報等のデータ入力業務の委託先に対する監督について
https://www.ppc.go.jp/files/pdf/itaku_kanntoku.pdf

リスク対策（例）

【契約終了時】

契約終了時、当該特定個人情報ファイルの使用が終了したとき若しくは委託元が指示したとき又はその他契約で定めたときに消去を行う。	Ⅲ．4
紙台帳は返却を義務付け、電子データは、消去申請の上、消去ソフト等を用いて消去し、その結果（消去証明）を書面にて提出させる。	Ⅲ．4

（５）電子媒体の管理及び使用　1/3

○　令和６年度上半期における立入検査の結果、「電子媒体の管理及び使用」に関して、３割の地方公共団体等で、物理的安全管理措置の不備事項が認められました。
○　特に、特定個人情報等の複製及び送信、特定個人情報等が保存されている電子媒体等の外部への送付及び持ち出し等については、責任者の指示に従い行うことを定めること等が重要です。

参考資料

監査チェックリスト

○項番21（機器及び電子媒体等の盗難等の防止）
○項番22（電子媒体等の取扱いにおける漏えい等の防止）
○項番23（個人番号の削除、機器及び電子媒体等の廃棄）

その他

―

リスク対策（例）【使用 1/2】

電子媒体の使用については、取扱いに関する実施手順書に従い、限定されたUSBメモリ等以外の利用を不可とし、施錠できるキャビネット等へ保管のうえ、USBメモリ等使用記録簿にて事前に責任者の承認を得た上で使用している。	Ⅲ.２
USBメモリやCD等の電子媒体への書き込みをシステム側で禁止する。	Ⅲ.２
電子媒体へ出力する必要がある場合には、逐一出力の記録が残される仕組みを構築する。	Ⅲ.２
提供を行う媒体の授受・運搬について手順を定め、提供元及び提供先において押印等により授受を確認する。	Ⅲ.２
委託先へ特定個人情報を提供する場合は暗号化した上で出力し、運搬の際は施錠可能なケースへ電子媒体を格納した上で実施することを義務づけている。	Ⅲ.２

（５）電子媒体の管理及び使用　2/3

○　管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するための物理的な安全管理措置を講ずることが重要です。

参考資料

監査チェックリスト

○項番21（機器及び電子媒体等の盗難等の防止）
○項番22（電子媒体等の取扱いにおける漏えい等の防止）
○項番23（個人番号の削除、機器及び電子媒体等の廃棄）

その他

―

リスク対策（例）

【使用 2/2】

職員等がサーバ室等へ入退室する際は、データの漏えい防止のために、電子媒体、携帯電話、パソコン類等の不要な機器の持込みがないかを確認する。	Ⅲ.2

【媒体内データの管理】

電子媒体で入手した情報は、入手後すぐに特定の権限者のみがアクセス可能な庁内連携システム内のフォルダに格納し、電子媒体内の情報はその時点で削除している。	Ⅲ.2
暗号化ソフトウェアを用いて暗号化処理を行わないと外部の電子媒体に書き込みができないよう、既存業務システムを設計する。	Ⅲ.5
電子媒体内のデータは暗号化する。	Ⅲ.3

（５）電子媒体の管理及び使用　3/3

○　特定個人情報等が記録された電子媒体等について、保存期間を経過した場合には、個人番号をできるだけ速やかに復元不可能な手段で削除又は廃棄し、その記録を保存することや、当該作業を委託した場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認することが重要です。

参考資料

監査チェックリスト

○項番21（機器及び電子媒体等の盗難等の防止）
○項番22（電子媒体等の取扱いにおける漏えい等の防止）
○項番23（個人番号の削除、機器及び電子媒体等の廃棄）

その他

―

リスク対策（例）

【廃棄】

特定個人情報保護管理者の指示に従い、当該特定個人情報等の復元又は判読ができない方法により当該保有特定個人情報等の消去又は当該電子媒体の廃棄を行う。	Ⅲ.７
電子媒体等の情報資産を廃棄する場合は、情報を復元できないように処置した上で廃棄する。機器リース終了による返却の場合も、同様とする。	Ⅲ.７
外部委託先が廃棄処理を行った場合は、業務が完了したことを書面（廃棄証明）にて報告させる。	Ⅲ.７

３．資料集

（１）特定個人情報保護評価に関する地方公共団体へのサポート強化の取組

（２）「Ⅳ リスク対策」において「２） 十分である」を選択できる水準

（３）「Ⅳ リスク対策」における措置状況の評価に係る「判断の根拠」の記載例

（４）保護評価の実施方法

【参考資料】⑴特定個人情報保護評価に関する地方公共団体へのサポート強化の取組

○　現在、委員会では、保護評価を実施するにあたっての参考資料を委員会HP上にて公表しています。
○　社会保障制度、税制及び災害対策の3分野以外の行政事務においてもマイナンバーの利用が可能となること等を踏まえ、当該評価に役立つ参考情報の提供などの地方公共団体へのサポート強化を検討中です。

現在委員会HPで公表中の参考情報

○特定個人情報保護評価とは
- 特定個人情報保護評価について（概要版/詳細版）

○特定個人情報保護評価の実施手順
- 特定個人情報保護評価の実施手順
- （参考）「特定個人情報保護評価の実施手順」の活用方法について

○特定個人情報保護評価の５年経過前の再実施について
- 特定個人情報保護評価 5年経過前の評価の再実施に係る留意事項について

○特定個人情報保護評価に関する規則・指針・解説
- 特定個人情報保護評価に関する規則
- 特定個人情報保護評価指針
- 特定個人情報保護評価指針の解説
  ※特定個人情報保護評価計画管理書、基礎項目評価書、重点項目評価書、全項目評価書の記載要領もあり。

【リンク先】
https://www.ppc.go.jp/legal/assessment/

今後予定している参考情報

○　地方公共団体が公表している評価書の記載内容を踏まえ、評価実施機関の担当者が評価を実施するに際して参考となるような情報の提供を検討中（具体的な内容及び提供時期は未定）。

【参考資料】⑵「Ⅳ リスク対策」において「２）十分である」を選択できる水準

○　基礎項目評価の実効性強化のため、基礎項目評価書中「Ⅳ　リスク対策」において記載する特定個人情報を保護するための主な措置の実施状況の評価について、「2)十分である」等を選択できる具体的水準を、特定個人情報保護評価指針の解説等（記載要領及び評価書様式）に掲載しています。
○　新様式移行の際には、この水準も参考に、実施状況の評価の見直しを行ってください。

【例】人為的ミスが発生するリスクへの対策は十分か

8．人手を介在させる作業	[　]人手を介在させる作業はない
人為的ミスが発生するリスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
判断の根拠	（自由記述）

リスク対策	「十分である」を選択できる水準
人為的ミスが発生するリスクへの対策は十分か	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 ＜典型的リスク対策（例）＞ ①「マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドライン」（令和５年12月18日デジタル庁）の次の留意事項等を遵守している。 （例） ・住基ネット照会によりマイナンバーを取得するのではなく、申請者からマイナンバーの提供を受け、その上で記載されたマイナンバーの真正性確認を行うこと。 ・申請者からマイナンバーが得られない場合にのみ行う住基ネット照会は、４情報又は住所を含む３情報による照会を原則とすること。 ・複数人での確認や上長による最終確認を行った上でマイナンバーの紐付けを行い、その記録を残すこと。 ・更新時には、本人から情報をマイナンバーを取得し、登録されているマイナンバーに誤りがないか、確認すること。 ②　特定個人情報の入手から保管・廃棄までのプロセスで、人手が介在する局面ごとに人為的ミスが発生するリスクへの対策を講じている。 ※　人為的ミス発生防止の着眼点等として、次の資料が参考となる（いずれも委員会HP公表資料：https://www.ppc.go.jp/legal/kensyuushiryou/）。 ・「特定個人情報を取り扱う際の注意ポイント」 ・「特定個人情報の漏えい等の防止について－地方公共団体における単純な事務ミスを防止するための着眼点－」

「典型的なリスク対策（例）」の位置付け

○「典型的なリスク対策（例）」は、あくまでも例示であり、**<u>１つでも実施していない対策があれば、「十分である」を選択できないというものではない</u>**。

○ **<u>「特に力を入れている」を選択できる水準</u>**は、「十分である」を選択できる水準を満たした上で、さらに、**<u>評価実施機関独自の取組を実施</u>**している場合に選択することができると考えられる。

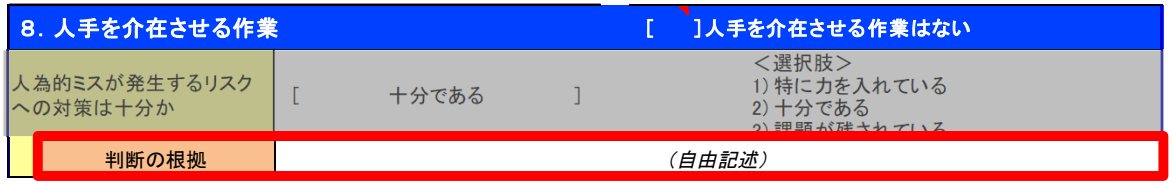
○「典型的なリスク対策（例）」には、**<u>組織的安全管理措置、人的安全管理措置</u>**については記載していないが、**<u>マイナンバーGLに則り、必要な措置を講ずる必要</u>**がある。

・組織的安全管理措置：
組織体制の整備、取扱規程等に基づく運用、取扱状況を確認する手段の整備、漏えい等事案に対応する体制等の整備、取扱状況の把握及び安全管理措置の見直し
・人的安全管理措置：
事務取扱担当者の監督、事務取扱担当者等の教育、法令・内部規程違反等に対する厳正な対処

【参考資料】⑶「Ⅳ リスク対策」における措置状況の評価に係る「判断の根拠」の記載例

○　新様式への円滑な移行に向けた支援のため、特定個人情報保護評価指針の解説において、基礎項目評価書中「Ⅳ　リスク対策」の各項目について、「判断の根拠」（自由記述）の記載例を掲載しています。

【例】8.人為的ミスが発生するリスクへの対策は十分か



8. 人手を介在させる作業	[　　]人手を介在させる作業はない
人為的ミスが発生するリスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
判断の根拠	（自由記述）

リスク対策	記載例
人為的ミスが発生するリスクへの対策は十分か	例①　マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドラインに従い、マイナンバー登録や副本登録の際には、本人からのマイナンバー取得の徹底や、住基ネット照会を行う際には４情報又は住所を含む３情報による照会を行うことを厳守している。また、●●事務では、上記のほか、下記の局面で特定個人情報の取扱いに関して手作業が介在するが、いずれの局面においても複数人での確認を行うようにしており、人為的ミスが発生するリスクへの対策は十分であると考えられる。 ・　申請書に記載された個人番号及び本人情報のデータベースへの入力 ・　特定個人情報の記載がある申請書等（USBメモリを含む。）の保管 ・　個人番号及び本人情報が記載された申請書の廃棄　　等
	例②　マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドラインに従い、マイナンバー登録や副本登録の際には、本人からのマイナンバー取得の徹底や、住基ネット照会を行う際には４情報又は住所を含む３情報による照会を行うことを厳守している。また、必ず複数人での確認を行った上で●●（上長）の最終確認を経ることとしている。 また、人手が介在する局面ごとに、人為的ミスが発生するリスクに対し、例えば次のような対策を講じている。 ・　人為的ミスを防止する対策を盛り込んだ事務処理手順をマニュアル化し、事務取扱担当者間で共有する。 ・　特定個人情報を受け渡す際（USBメモリを使用する場合を含む。）は、事前に、暗号化、パスワードによる保護、確実なマスキング処理等を行うとともに、これらの対策を確実に実施したことの確認を複数人で行う。 ・　マイナンバー入りの書類を郵送等する際は、宛先に間違いがないか、関係のない者の特定個人情報が含まれていないかなど、ダブルチェックを行う。 ・　特定個人情報を含む書類やUSBメモリは、施錠できる書棚等に保管することを徹底する。 ・　廃棄書類に特定個人情報が含まれていないか、ダブルチェックを行う。 これらの対策を講じていることから、人為的ミスが発生するリスクへの対策は「十分である」と考えられる。
	例③　（例②の内容に加え、）年に一度、業務プロセス全体について、漏えい等のリスクを軽減させるための仕組みを検討することとしており、令和●年度は、オンライン申請受付の導入を決定した（これにより、手作業が介在する申請数が減少することが期待される）。これらの対策を講じていることから、人為的ミスが発生するリスクへの対策は「特に力を入れている」と考えられる。

【参考資料】⑷保護評価の実施方法

何をする / 誰が	事前の準備	しきい値判断	リスク分析	リスク対策の検討	評価書の作成	評価書の確認	委員会への提出・公表
保護評価取りまとめ課	計画管理書を作成・更新	事務間の調整、情報の共有	情報の共有（番号法の規定やMNガイドライン等）	情報の共有（番号法の規定やMNガイドライン等）	評価書の記載方法の情報提供（作成を補助）	評価書の確認	計画管理書の提出 評価書の提出・公表作業の補助
事務担当部署	保護評価の対象となる事務の内容を明確化	しきい値判断に基づき、保護評価の種類を特定	事務手続面のリスク分析	事務手続面のリスク対策の検討	評価書の作成	必要に応じて総括部署へ根拠資料の提供等	評価書の提出・公表作業
システム担当部署	システム面の情報提供	―	システム面のリスク分析	システム面のリスク対策の検討	システム面の情報提供（作成を補助）	必要に応じて総括部署へ根拠資料の提供等	評価書の提出・公表作業の補助

※実施体制は、評価実施機関における部署間の役割分担などによっても異なるが、上記では推奨される例を示しています。

評価の実施方法に関する留意点

○ **全項目評価**を実施する場合、委員会への評価書の提出前に**30日以上の住民等からの意見聴取及び第三者点検が義務付けられます**。

○ 評価書の提出・公表は、新規事務の場合、**特定個人情報ファイルを保有する前（システム用ファイルを保有しようとする場合は、プログラミングの開始前）**に実施する必要があります。また、過去に保護評価を実施した事務について**「重要な変更」を加える場合は、「重要な変更」を加える前（システム開発を伴う場合は、プログラミングの開始前）に保護評価を再実施**（保護評価の実施手続の全てのプロセスを改めて実施）する必要があります。

○ 計画管理書・評価書の委員会への**提出**及び評価書の**公表作業は、マイナンバー保護評価システム**から行う必要があります。

※どのような事務の変更が「重要な変更」に該当するかについては、委員会HPで公表している「特定個人情報保護評価指針の解説」を参照ください。