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

令和元年９月
（令和６年５月一部改訂）
個人情報保護委員会事務局

はじめに（当資料の趣旨）

平成26年４月に特定個人情報保護評価制度が施行され、その後各評価実施機関において順次、特定個人情報保護評価（以下「保護評価」という。）が実施されてきました。

特定個人情報保護評価に関する規則（平成26年特定個人情報保護委員会規則第１号）第15条及び特定個人情報保護評価指針（平成26年特定個人情報保護委員会告示第４号）により、特定個人情報保護評価書（以下「評価書」という。）の直近の公表日から５年を経過する前に保護評価を再実施するよう努めることとされております。

また、個人情報保護委員会では、立入検査の結果や、各種説明会等における問合せ内容を踏まえ、特定個人情報の適正な取扱いに関するガイドライン（以下「マイナンバーガイドライン」という。）の改正、「委託先に対する監督」、「ログの分析・確認手法」等に関する参考資料の公表、注意喚起等を行ってきました。

これらと合わせて、今回、各評価実施機関が５年経過前の再実施を行うに当たって参考となるよう、５年経過前の再実施の留意事項（チェックポイント）を公表することとしました。
本留意事項が、各評価実施機関における事務の特性や情報システムの構成等を踏まえた、より充実した保護評価の再実施の一助となれば幸いです。

５年経過前の保護評価の再実施の意義

５年経過前の保護評価の再実施には、 各評価実施機関において、５年間の個人情報の保護に関する情報技術の進歩や社会情勢の変化を考慮し、改めて事務の特性や情報システムの構成等を踏まえ、評価書に記載する事務の内容や流れを確認し、特定個人情報ファイルの取扱いについてのリスク及びリスク対策を検討するという重要な意義があります。

また、保護評価制度の目的に照らし、特定個人情報ファイルの取扱い等について、国民・住民に対する説明責任を果たし、信頼を確保をするために、評価書の記載内容を分かりやすく工夫する機会ともなります。

５年経過前の保護評価の再実施を機に、各評価実施機関が保護評価の基本理念・目的について再認識し、自らの取組について積極的、体系的に評価し、継続的改善に努めていくことが望まれます。

（参考）「５年を経過する前の保護評価の再実施」と「１年ごとの見直し」について

	５年を経過する前の保護評価の再実施（努力義務）	１年ごとの見直し（努力義務）
委員会規則	特定個人情報保護評価に関する規則　第15条	特定個人情報保護評価に関する規則　第14条
特定個人情報 保護評価指針（抄）	【第６の２の（４）　一定期間経過】 　評価実施機関は、規則15条の規定に基づき、直近の特定個人情報保護評価書を公表してから５年を経過する前に、特定個人情報保護評価を再実施するよう努めるものとする。	【第５の４　特定個人情報保護評価書の見直し】 　評価実施機関は、少なくとも1年に１回、公表した特定個人情報保護評価書の記載事項を実態に照らして見直し、変更が必要か否かを検討するよう努めるものとする。
特定個人情報 保護評価指針の解説（抄）	○　保護評価を実施してからある程度の期間が経過すると、個人情報の保護に関する情報技術の進歩や社会情勢の変化が生じ、保護評価を再実施することが望ましい状況となることが考えられます。 ○　昨今の情報通信技術の進歩の早さを踏まえると、５年を経過すればリスク対策を見直す必要性が高くなっていることが想定されます。	○　保護評価の再実施が義務付けられない程度の比較的軽微な変更・変化であっても、国民・住民からの信頼を確保するという観点から、記載内容が実態と齟齬がないように見直しておく必要があります。 ○　見直した結果、しきい値判断項目の対象人数又は取扱者数の増加に伴いしきい値判断結果が変わる場合は、保護評価の再実施が必要になります。それ以外の場合は、評価書の修正が必要になります。

５年経過前の保護評価の再実施の手順

５年経過前の保護評価の再実施のための手順はおおむね以下のとおりです。

注意！

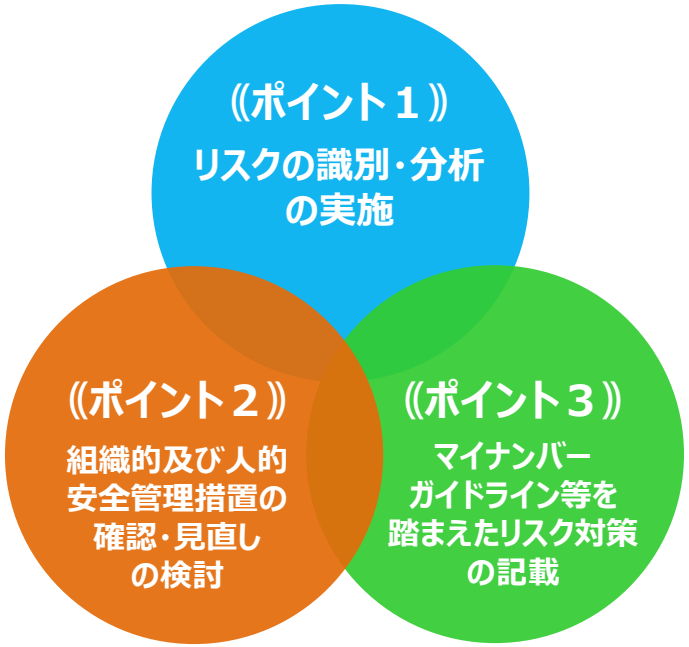
仮に記載内容に変更が生じない場合でも、国民・住民の信頼の確保という保護評価制度の目的に照らし、 特定個人情報の取扱い状況を周知するために、評価書の種類に応じた手続（パブコメ、第三者点検等）を経て、評価書の公表まで行う必要があります。

	全項目評価書	重点項目評価書	基礎項目評価書
１．再実施の対象となる評価書の特定	計画管理書やマイナンバー保護評価システムを確認し、評価書の直近の公表日（※）以降、一度も保護評価の再実施をせずに、５年を迎える評価書を特定します。 ※ ここに記載している「公表日」とは、保護評価の実施又は再実施に伴い公表した日です。軽微な修正に伴い評価書を修正し、公表した日を除きますので御注意ください。		
２．記載内容の確認・変更	今後、変更が生じ得る事務の流れ、事務において使用するシステム、特定個人情報ファイルの内容等について、評価書の記載内容を確認し、必要に応じて評価書を変更します。 ポイント１：リスクの識別・分析を改めて実施 ポイント２：組織的及び人的安全管理措置の確認・見直し ポイント３：マイナンバーガイドライン等を踏まえたリスク対策の記載 様式中「Ⅳリスク対策」を中心として、左記の観点も踏まえつつ、指針の解説に掲載の「『十分である』を選択できる水準」も参考に、評価の見直しを行ってください。		
３．パブコメ・第三者点検	必須	任意	任意
４．公表	評価書を個人情報保護委員会に提出、公表します。記載内容に変更がない場合でも、今回の評価実施日、公表日の日付で、評価書を提出、公表することが必要です。		

記載内容の確認・変更のポイント

記載内容の確認・変更の参考として、３つのポイントを御紹介します。

当資料はあくまでも参考として示したものです。各評価書の事務の実態や特性等を踏まえ、対応してください。



《ポイント１》　リスクの識別・分析を改めて実施

評価書を作成したときの想定と実際の事務が異なる可能性がある場合、現在の評価書をそのまま使うのではなく、実際の事務を確認した上で、リスク識別・分析を改めて実施することが重要です。

リスクの識別・分析では、「入手」、「使用」、「委託」、「提供・移転」、「保管・消去」等の特定個人情報ファイルの取扱いの各場面を整理し、想定されるリスクを識別・分析することで、現状のリスク対策が十分か、リスク対策の追加や変更が必要かを検討することが重要です。

《ポイント２》　組織的及び人的安全管理措置の確認・見直し

「組織体制の整備」、「自己点検・監査」、「教育・啓発」等の組織的及び人的安全管理措置は、各評価実施機関の組織体制や事務運営の特性により異なります。改めて、組織の特性にあったリスク対策を確認・見直して、記載の追加や変更が必要かを検討することが重要です。

《ポイント３》　マイナンバーガイドライン等を踏まえたリスク対策の記載

「委託先に対する適切な監督」、「ログの記録・分析」等、マイナンバーガイドラインに対応したリスク対策が現状の評価書に記載されているかを確認し、記載の追加や変更が必要かを検討することが重要です。

次のページ以降、詳しく説明していきます。

《ポイント１》リスクの識別・分析を改めて実施

評価対象の事務におけるリスクの識別・分析の実施手順を御紹介します。

リスクの識別・分析については、（１）～（３）の順番で実施していきます。

（１）評価対象事務の実態整理

例えば、特定個人情報ファイルの取扱いについて、「入手」、「使用」、「委託」、「提供・移転」、「保管・消去」等の取扱いの場面ごとに、項目を立て、表形式に整理すると効果的です。

【評価対象事務の整理表（例）】

事務の実施主体/システム等			使用		入手		提供・移転		保管・消去		委託
「誰」が	どの「特定個人情報ファイル」を	何の「システム」を使用し	どの事務でどのように**「使用」**するのか		誰から特定個人情報ファイルを**「入手」**し		誰に特定個人情報ファイルを**「提供・移転」**するのか		どのように特定個人情報ファイルを**「保管・消去」**するのか		何を**「委託」**するのか
取扱部署名	特定個人情報ファイル名	システム名	主な事務	電子記録媒体の使用場面	入手元	入手方法	提供先	提供方法	保管場所 保管方法	消去方法 廃棄方法	委託内容

（２）想定されるリスクの識別・分析

特定個人情報ファイルの取扱いの場面ごとに、事務等の追加や変更の予定はないか、現状の評価書に記載しているリスク対策が十分であるかという観点から、想定されるリスクを識別・分析します。さらに、保護評価は、事務を行う前の事前評価であることから、制度の性質上、現状の評価書に実際の事務に対応していないリスク対策が記載されている場合も想定されます。そうした観点からの見直しも検討します。

（３）リスク対策等の追加・変更

（２）で識別した想定リスクについて、事務の実態を踏まえて検討し、改めてリスク対策を確定します。その上で、評価書の該当箇所へリスク対策を追加・変更します。

《ポイント１》リスクの識別・分析を改めて実施

評価対象の事務におけるリスクの識別・分析の手法を御紹介します。

【リスクの識別・分析の実施（例）】 事務の実態を踏まえ、リスク対策を検討し、評価書への追加・変更を行います。

（１）評価対象事務の実態整理

項番	「誰」が	どの「特定個人情報ファイル」を	何の「システム」を使用し	どの事務でどのように**「使用」**するのか		誰から特定個人情報ファイルを**「入手」**し		誰に特定個人情報ファイルを**「提供・移転」**するのか		どのように特定個人情報ファイルを**「保管・消去」**するのか		何を**「委託」**するのか
	取扱部署名	特定個人情報ファイル名	システム名	主な事務	電子記録媒体の使用場面	入手元	入手方法	提供先	提供方法	保管場所 保管方法	消去方法 廃棄方法	委託内容
1	○○○部 △△課 （10人～50人）	住基ファイル	既存住基システム	① 住基台帳の管理 ② 住基情報の照会 ③ 各種証明書の交付 ④ ・・・ ⑤ ・・・	① 住基情報を健康増進課へ提供する時に、電子記録媒体（DVD）を使用する ② パンチ入力業者から納品物を受領する時に、電子記録媒体（DVD）を使用する ③ ・・・	本人	紙（対面、郵送）	住民	紙	＜紙＞ ・ 保管庫に保管している ＜電子記録媒体＞ ・ 保管庫に保管している ・ 媒体管理子で管理している ＜サーバ等＞ ・ マシンルームに設置している	＜紙＞ ・ シュレッダー又は溶解処理 ＜電子記録媒体＞ ・ 専用ソフトによる完全消去 ・ 物理的破壊	①「使用」に関する委託 ・ システム運用保守 ②「入手」に関する委託 ・ パンチ入力 ③・・・
						他部署	庁内連携（庁内LAN）	市町村	住民基本台帳ネットワーク			
						市町村	住民基本台帳ネットワーク	行政機関等	情報提供ネットワークシステム			
						地方公共団体情報システム機構	住民基本台帳ネットワーク	課税課 納税課	庁内連携（庁内LAN）			
						委託先（パンチ入力業者）	電子記録媒体（DVD）	健康増進課	電子記録媒体（DVD）			
						・・・	・・・	教育委員会	紙			

各場面等における、特定個人情報ファイルの取扱いに関する事項の追加・変更の予定の確認

（２）想定リスクの識別・分析

システムにおいて、アクセス権限の発行・失効の管理方法を変更予定
⇒想定されるリスク
「権限のない者によって不正に使用されるリスク」を識別
- ユーザIDの不正使用
- 不正照会・出力など

① 新たに、他部署から電子記録媒体で特定個人情報ファイルを入手する予定
② 健康増進課への電子記録媒体の提供について、現状の評価書の記載が不十分
⇒想定されるリスク
① 「漏えい・紛失のリスク」を識別
② 「電子記録媒体」の提供のリスク対策を検討

保管場所を変更する予定
⇒想定されるリスク
「漏えい・紛失のリスク」等を識別
- 収集・保管違反
- 盗難・紛失など

委託事項を追加する予定
⇒想定されるリスク
「委託に関するリスク」を識別
- 未許諾の再委託
- 不適切な取扱いなど

（３）リスク対策等の追加・変更

- 事務の従事者のみに限定されたユーザIDの発行
- ユーザIDに対して必要最小限のアクセス権限の付与
- 職員の採用、異動、退職に伴い必要となるユーザIDの発行・失効の管理及び適切なアクセス権限の追加・削除など

- 利用する電子記録媒体の限定
- 媒体管理簿等による管理
- 電子記録媒体内のデータの暗号化等
- 施錠可能なキャビネット等への保管など

- 保管場所への入退室管理装置の設置
- 入室の際の制御など

- 委託先の管理体制の確認
- 実地の監査・調査等の権限を契約書に規定
- 監査・調査の実施など

《ポイント１》リスクの識別・分析を改めて実施

リスクの識別・分析の実施結果による、評価書の記載内容の追加・変更例を御紹介します。

リスクの識別・分析の実施結果から、評価書のリスク対策等の追加や変更が必要となりえる記載項目、記載内容について、例示します。

※評価書の該当箇所については、全項目評価書を前提としています。重点項目評価書については、こちらを参考に対応する項目に読み替えてください。

場面	リスク識別・分析の結果	記載の追加や変更が必要となり得る評価書項目（例）	主な追加・変更内容（例）
入手	新たに他部署から電子記録媒体を用いた特定個人情報ファイルの入手を行う予定である。	Ⅱ３．特定個人情報の入手・使用 ①入手元 ②入手方法	①入手元 [○]評価実施機関内の他部署（ ○○部△△課 ） ②入手方法 [○]電子記録媒体
		Ⅲ２．特定個人情報の入手 Ⅲ３．特定個人情報の使用 Ⅲ７．特定個人情報の保管・消去	・ 利用する電子記録媒体については、管理者等が許可・承認をしたものに限定し、担当者が私物の機器等を利用することを防止する。 ・ 電子記録媒体の利用に際は、媒体管理簿等で管理する。 ・ 持ち運ぶ際は、電子記録媒体内のデータの暗号化、パスワードによる保護をする。 ・ 電子記録媒体を施錠できるキャビネット等に保管する。 ・ 電子記録媒体を廃棄する際は、専用データ削除ソフトウエア等により、復元不可能な手段を採用する。 ・ 削除・廃棄した記録の保存を行う。
使用	特定個人情報を取扱うシステムにおいて、アクセス権限の発行・失効の管理方法を変更する。	Ⅲ３．特定個人情報の使用 アクセス権限の発行・失効の管理 アクセス権限の管理	＜発行・失効管理＞ ・ ○○システムにおけるユーザIDの発行・失効については、人事システムと連動し、職員の採用、異動、退職等に伴い自動的にユーザIDの発行・権限の付与及び削除がおこなわれる仕組みとしている。 ・ 事務の必要性によりユーザID権限を変更する際は、所属長から人事へ変更申請を提出し、承認された場合のみ変更がなされる。 ＜アクセス権限管理＞ ・ 業務内容と業務担当者に対応したアクセス制御リストを作成し、業務に対して必要最小限の権限が付与されていることを人事担当とともに確認している。

《ポイント１》リスクの識別・分析を改めて実施

場面	リスク識別・分析の結果	記載の追加や変更が必要となり得る評価書項目（例）	主な追加・変更内容（例）
委託	特定個人情報ファイルの取扱いの委託に該当する委託事項を増やす予定である。	Ⅱ４．特定個人情報ファイルの委託 Ⅲ４．特定個人情報ファイルの委託	※「特定個人情報保護評価指針の解説の別添（記載要領）」、次ページの「委託に関する記載」、「ポイント３」等を参考に、実態を踏まえたリスク対策を御記載ください。
保管・消去	特定個人情報ファイルの保管場所を変更する予定である。	Ⅱ６．特定個人情報の保管・消去 ①保管場所 Ⅲ７．特定個人情報の保管・消去 ⑤物理的対策	<サーバ設置場所> ・ 権限のない者が入室できないよう入退室管理システムによる入退室の制御がなされ、監視カメラにより監視しているサーバ室にサーバを設置する。 ・ サーバ室はICカード、生体認証により、許可された者のみが入室できることとする。 <業務端末設置場所> ・ サーバに接続する持ち運び可能な業務端末は、業務終了後に施錠できる場所へ保管している。 ・ 通常業務で使用する業務端末は、盗難防止のためにワイヤーロック等で所定の場所から移動できないようにしている。 <電子記録媒体の保管場所> ・ 権限のない者が入室できないよう入退室管理システムによる入退室の制御がなされ監視カメラにより監視している居室に保管する。 ・ 事務で用いる電子記録媒体については、利用時以外は施錠できる保管庫に保管する。 ・ 利用状況は媒体管理簿で管理し、上長の承認を得た場合のみ利用できる。

《ポイント１》リスクの識別・分析を改めて実施

特定個人情報ファイルの取扱いの委託（再委託）の記載例を御紹介します。

特定個人情報ファイルの取扱いの委託については、現状では再委託を実施していない場合でも、今後、委託業者の繁忙や人的リソースの状況によって、再委託を行う可能性がある場合は、評価書の記載に注意が必要です。また、契約書の再委託条項等において、再委託ができる旨を規定しておく必要がありますので、御注意ください。

このような場合における評価書の記載例を以下に示します。

【記載例】

４．特定個人情報ファイルの取扱いの委託		
委託の有無　※		［　　委託する　　］　＜選択肢＞ 1）委託する　2）委託しない （　　１）　件
委託事項1		○○○○のデータ入力事務
①委託内容		○○申請書のデータ入力に係る事務
⑥委託先名		○○○○のデータ入力事務
再委託	⑦再委託の有無　※	［　再委託する　］　＜選択肢＞ 1）再委託する　2）再委託しない
再委託	⑧再委託の許諾方法	原則として再委託は行わないこととするが、再委託を行う場合は、委託先より事前に書面による再委託申請を受け付け、委託先と再委託先が秘密保持に関する契約を締結していること等、再委託先において、委託元自らが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を確認し、内部における決裁及び調達責任者の承認手続を経た後に承認することとする。
再委託	⑨再委託事項	○○申請書のデータ入力に係る事務

上記のケースの場合においては、次のような観点での記載が考えられます。

【⑦再委託の有無】
→「１）再委託する」を選択してください。

【⑧再委託の許諾方法】
→ 例えば、原則として再委託しないこととしているのであれば、その旨を記載してください。
→ 再委託を行う場合は、番号法第10条等の観点から、次の内容等を記載してください。
- 再委託に際し、事前許諾を行う方法
- 再委託先において特定個人情報の適切な安全管理措置が図られることを確認する旨
- 再委託先の監督を行う旨

※「Ⅲ４．特定個人情報ファイルの取扱いの委託」の「再委託先による特定個人情報ファイルの適切な取扱いの確保」等にも、対応した記載をしてください。

※評価書の該当箇所については、全項目評価書を前提としています。重点項目評価書については、こちらを参考に対応する項目に読み替えてください。

《ポイント１》リスクの識別・分析を改めて実施

その他、リスク対策の記載の参考

国民・住民の信頼の確保という保護評価制度の目的から 各評価実施機関は、国民・住民に対して、評価書を分かりやすく記載し、周知する必要があります。例えば、評価書の「Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策」等の記載内容について、リスク識別・分析にも有用で、読み手にも分かりやすい整理方法を御紹介します。

➢ 「特定個人情報の入手」に係るリスク対策等の整理方法

入手経路や入手方法により、リスク対策を分類し整理して記載する方法があります。

【整理例】

２．特定個人情報の入手

＜住民からの入手＞
・紙面で入手する場合・・・、〇〇する。

＜他部署からの入手＞
・庁内連携システムを経由し入手する場合・・、〇〇する。
・電子記録媒体を利用して入手する場合・・・、〇〇する。

＜他の市町村からの入手＞
・紙面で入手する場合・・、〇〇する。

※「５．特定個人情報の提供・移転」等の記載についても、同じように整理できます。

➢ その他の整理方法

例えば、「特定個人情報の使用」等については、特定個人情報を取り扱うシステムが有する機能で講じるリスク対策、事務の運用管理規程等に定められた手続等で講じるリスク対策に分類し、記載する方法も有用です。

【整理例】

３．特定個人情報の使用

＜〇〇システムの機能にて講じている措置＞
・
・

＜運用管理規程等に定められた手続き等にて講じている措置＞
・

※「２．特定個人情報の入手」、「５．特定個人情報の提供・移転」等についても同じように整理できます。
※ システムが複数ある場合は、システム種別ごと、端末種別ごとに整理する記載も考えられます。

※評価書の該当箇所については、全項目評価書を前提としています。重点項目評価書については、こちらを参考に対応する項目に読み替えてください。

《ポイント２》組織的及び人的安全管理措置の確認・見直し

組織的及び人的安全管理措置の確認・見直しの重要性

個人情報保護委員会が特定個人情報の漏えい等の報告を受けているものは、行政機関等や事業者を含めて、**人為的ミスに起因するものが多く見られます**。そのため、組織的及び人的安全管理措置を適切に講じることが重要です。

類　型	漏えい等報告があった事案
紛　失 誤廃棄	・　行政機関等において、約200名分の特定個人情報が記録されたバックアップ媒体を**紛失**した事案
	・　地方公共団体において、約33,490名分の特定個人情報を保存しているUSBを**紛失**した事案
	・　事業者において、**誤って**約190名分のマイナンバーの**データを削除**した事案
	・　事業者において、約1,790名分の特定個人情報が記録されたCDを**誤廃棄**した事案
誤送付	・　事業者において、伝票の貼付ミスにより、約190名分のマイナンバーが記載された書類を**誤送付**した事案
	・　事業者において、システム開発業者に特定個人情報のダミーファイルを送付すべきところ、**誤って**実在の約4,170名分の**特定個人情報を送付**した事案
	・　事業者において、メールアドレスの宛先間違いにより、約280名分の**特定個人情報が誤送付**された事案
	・　地方公共団体において、事業者の従業員約280名分の特定個人情報を、**他の事業者に誤送付**した事案
不　正 アクセス	・　事業者において、サーバーへの**不正アクセス**により、約130名分の特定個人情報が漏えいした事案
	・　事業者において、サーバーへの**不正アクセス**により、約690名分の特定個人情報が毀損した事案

類　型	漏えい等報告があった事案
委　託 再委託 関　係	・　個人番号利用事務を受託していた事業者において、委託元である行政機関に**許諾なく再委託**が行われた事案
	・　地方公共団体において、**委託事業者より納品されたデータ**に、他の地方公共団体に納品されるべき約1,520名分の**特定個人情報が混入していたことに気付かず**に、全国の関係団体に送付した事案
	・　事業者において、**委託元の従業員の個人番号を取り違えて処理**したことにより、約160名分の特定個人情報を誤った地方公共団体に送付した事案
その他	・　地方公共団体において、**マスキング処理が不十分**なまま約10,380名分の特定個人情報が記載された書類を、**特定個人情報を取り扱わないこととなっている委託事業者に引き渡し**ていた事案
	・　地方公共団体において、**誤ったデータをシステムに取り込んだ**ことにより、約210名分の特定個人情報を特定の者がシステム上で閲覧できる状態となっていた事案

特定個人情報を取り扱うあらゆる場面で、
人為的ミスが発生するリスクに注意する必要があります。

【参考】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

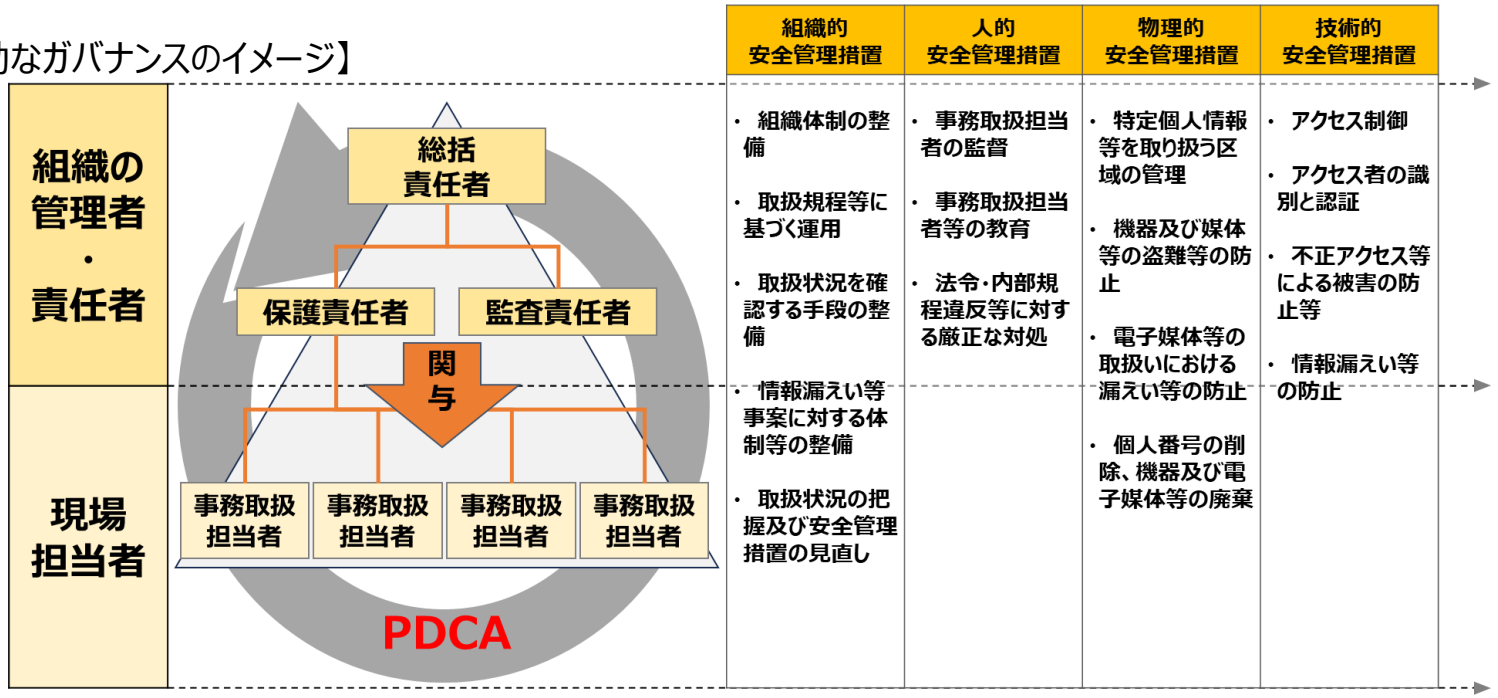
《ポイント２》組織的及び人的安全管理措置の確認・見直し

組織的及び人的安全管理措置の確認・見直しの観点を御紹介します。

マイナンバーガイドラインでは、講ずべき安全理措置として、組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置等の項目を示しています。

物理的及び技術的安全管理措置を適切に実行するために、組織的及び人的安全管理措置について、現場担当者だけでなく、組織の管理者、責任者等の関与の下、事前評価（特定個人情報保護評価）、事務運営、監査、教育・啓発、継続的な改善といったPDCAサイクルを回していくことが重要です。

【有効なガバナンスのイメージ】



継続的な改善を行う際には、リスク対策だけを改善するのではなく、事務運営自体にも改善の余地がないかを検討することが重要です。例えば、リスクが高い業務プロセスが多く存在する事務では、リスクを生じさせる業務プロセスを削減できないか、リスクを軽減させるための新しい業務プロセスや新しい仕組みを導入できないか等の観点から事務運営自体の見直しを検討することが考えられます。

《ポイント２》組織的及び人的安全管理措置の確認・見直し

組織的及び人的安全管理措置の確認・見直しによる評価書の記載内容への追加・変更例を御紹介します。

現状の評価書に記載しているリスク対策が物理的及び技術的安全管理措置に係る内容に偏っていないかという観点も含め、改めて自分の組織体制や事務運営の特性にあった組織的及び人的安全管理措置に係るリスク対策を確認・見直して、記載の追加や変更が必要になるかを検討することが重要です。

※評価書の該当箇所については、全項目評価書を前提としています。重点項目評価書については、こちらを参考に対応する項目に読み替えてください。

組織的及び人的安全管理措置の確認・見直しの観点	記載の追加や変更が必要となり得る評価書項目	追加・変更の観点（例）
組織的安全管理措置 ※　例えば、現場担当者だけでなく、組織の管理者、責任者の関与のもと、特定個人情報の適切な取扱いに関する継続的な改善の仕組みがあるか等の観点から記載内容を検討します。	Ⅳ その他のリスク対策 ３．その他のリスク対策	<事務運営に関する責任者の関与の仕組み> ・　組織の長を委員長とし、業務責任者をメンバーとする〇〇委員会を設置し、特定個人情報をはじめとする個人情報保護や情報セキュリティ等に係るリスク管理を行う。 ・　〇〇委員会では、リスク管理に係る監査・自己点検、教育・研修をはじめ、情報漏えい等のセキュリティ事案が発生した場合の対応訓練等の諸活動について、計画策定、実施状況のモニタリングを行い、　各種の課題・問題を把握し、継続的な運用改善を行う。 <特定個人情報の漏えい事案が発生した場合の対応> ※　以下の内容を踏まえて、責任をもつ部署、実施をする部署等の役割分担及び手順等の実態を確認し、記載することが考えられます。 ①　組織内における報告、被害の拡大防止 ②　事実関係の調査、原因の究明 ③　影響範囲の特定 ④　再発防止策の検討・実施 ⑤　影響を受ける可能性のある本人への連絡等 ⑥　事実関係、再発防止策の公表 ⑦　個人情報保護委員会への報告

《ポイント２》組織的及び人的安全管理措置の確認・見直し

※評価書の該当箇所については、全項目評価書を前提としています。重点項目評価書については、こちらを参考に対応する項目に読み替えてください。

組織的及び人的安全管理措置の確認・見直しの観点	記載の追加や変更が必要となり得る評価書項目	追加・変更の観点（例）
人的安全管理措置 ※例えば、 自己点検、監査、教育・啓発について、実効性を持たせるために実務に即した内容を実施しているか、継続的な改善を行うために、実施した結果を役立たせる仕組みがあるか等の観点から記載を検討します。	Ⅳ その他のリスク対策 １．監査 ①自己点検 ②監査	※　以下の内容について、実態を踏まえて、記載することが考えられます。 ➢ 規定の整備（誰が、何のために） ・ 実施者：監査責任者など ・ 目　的：規定等の整備状況の確認、規定等に基づいた運用状況の確認など ➢ 計画・頻度・対象範囲（いつ、誰に） ➢ 手法・手続（どのような観点で、どのように） ・ 自己点検項目：特定個人情報取扱規程をもとに作成したチェックシート ・ 監査基準・項目：特定個人情報取扱規程、情報セキュリティポリシーなど ➢ フォローアップ（課題・問題を発見した場合の対応、フォロー）など
	Ⅳ その他のリスク対策 ２．従業者に対する教育・啓発	※　以下の内容について、実態を踏まえて、記載することが考えられます。 ➢ 規定の整備（誰が、何のために、誰に） ・ 実施者：研修責任者、人事担当者等 ・ 目　的：注意喚起（意識改革、周知徹底、スキルの向上など） ・ 対象者：事務取扱担当者、情報システムの管理に関する事務に従事する職員、保護責任者など ➢ 研修計画を立てているか（いつ、どこで、どのように） ・ 時期：例えば「定期的に」と規定している場合は、頻度 具体的な内容など（入職時、異動時、昇格時など） ・ 方法：研修形式、実習形式、eラーニング等 ➢ 出席者、欠席者の記録をとっているか ・ 記録：名簿、報告書、アンケート、テストなど ➢ 未受講者（欠席者、異動者、新規採用者）への研修を実施しているか ➢ 未受講者に対して研修を実施した場合、記録をとっているか

《ポイント３》マイナンバーガイドライン等を踏まえたリスク対策の記載

マイナンバーガイドライン等を踏まえた対応の観点を御紹介します。

個人情報保護委員会では、立入検査の結果や、各種説明会等における問合せの内容を踏まえ、マイナンバーガイドラインの改正、「委託先に対する監督」、「ログ分析・確認手法」等に関する参考資料の公表、注意喚起等を行ってきました。
これらの参考資料やマイナンバーガイドラインの改正箇所等に対応した記載の有無を確認し、追加や変更が必要になるかを検討することが重要です。その観点を以下に例示します。

※評価書の該当箇所については、全項目評価書を前提としています。重点項目評価書については、こちらを参考に対応する項目に読み替えてください。

マイナンバーガイドラインの参照箇所		対応する 主な評価書の項目	追加・変更内容（例）
委託	➢ 委託先に対する必要かつ適切な監督 （第４－２－（１）） ～実地の監査、 調査等を行うことができる規定等を盛り込まなければならない。 委託先における特定個人情報の取扱状況の把握については、前記の契約に基づき報告を求めること、委託先に対して実地の監査、調査等を行うこと等により、委託契約で盛り込んだ内容の実施の程度を把握した上で、委託の内容等の見直しを検討することを含め、適切に評価する。	Ⅲ４．特定個人情報ファイルの委託 ・ 情報保護管理体制の確認	・ 委託契約の締結後は、必要に応じて実地の監査、調査等を行うことにより、特定個人情報の取扱状況の把握、情報保護管理体制の把握を行う。
		Ⅲ４．特定個人情報ファイルの委託 ・ 委託契約書中の特定個人情報ファイルの取扱いに関する規定	・ 委託契約書の遵守状況について、報告を求める規定を定める。 ・ 委託先に対して、実地監査、調査等が行うことができる規定を定める。

《ポイント３》マイナンバーガイドライン等を踏まえたリスク対策の記載

マイナンバーガイドラインの参照箇所		対応する 主な評価書の項目	追加・変更内容（例）
使用	➢ 取扱規程等に基づく運用（ログの記録・分析） （（別添１：安全管理措置）２－Ｃ－ｂ）） ～特定個人情報等の利用状況等を記録し、その記録を一定の期間保存し、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。 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。	Ⅲ３．特定個人情報の使用 （特定個人情報の使用の記録）	・　〇〇規程に基づき、特定個人情報のアクセスログについて、毎月、担当者が申請書とログとを突合し、当該ログの分析・確認をしている。その結果は管理責任者へ報告している。 ※　ログの分析・確認の流れは、次の１～６が一般的です。評価書の記載等の参考にしてください。 １．目的の明確化 （分析・確認する目的を明確にする） ２．実施体制の整備 （分析・確認する体制を整備する） ３．対象の選定 （分析・確認する対象を選定する） ４．ログの出力（情報システムからログを出力する） ５．ログの分析・確認 （１の目的に合う観点で分析・確認する） ６．結果報告 （確認結果を総括責任者等へ報告する）
		Ⅲ３．特定個人情報の使用 （リスク４：特定個人情報ファイルが不正に複製されるリスク）	・　特定個人情報ファイルを電子記録媒体に複製する場合やサーバから業務端末にダウンロードをする場合の操作ログを取得している。 ・　毎月、操作ログを出力し、外部媒体使用簿や申請書と突合し、当該ログの分析・確認をしている。その結果は管理責任者へ報告している。

《ポイント３》マイナンバーガイドライン等を踏まえたリスク対策の記載

マイナンバーガイドラインの参照箇所		対応する 主な評価書の項目	追加・変更内容（例）
使用	➢ 管理区域及び取扱区域 （管理区域へ持ち込む機器の制限） （（別添１：安全管理措置）２－Ｅ－ａ） 特定個人情報ファイルを取り扱う情報システム（サーバ等）を管理する区域（以下「管理区域」という。）を明確にし、物理的な安全管理措置を講ずる。 管理区域において、入退室管理及び管理区域へ持ち込む機器等の制限等の措置を講ずる。 また、特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）について、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などできないよう留意する必要がある。	Ⅱ．６特定個人情報の保管・消去 （①保管場所） Ⅲ．７特定個人情報の保管・消去 （⑤物理的対策）	・　職員等がサーバ室等へ入退室をする際は、データの漏えい防止のために、電子記録媒体、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。 ・　作業のためにサーバ室等へ入退室する際に、電子記録媒体等の機器類を持込み、持出しする場合は、事前に責任者に申請書を提出し、承認を得ることとしている。 Check! 平成30年の改正前のマイナンバーガイドラインでは、『管理区域及び取扱区域を明確にし、物理的安全管理措置を講ずる』旨が規定されていましたが、各評価実施機関の認識に差異があり、次のように、実際の事務に対応していないと思われるリスク対策を検討しているケースが見受けられました。 今回の再実施の機会に、評価対象事務の特性等を改めて考慮し、このような観点からも、リスク対策の見直しを検討することも考えられます。 ➢ 見受けられたケース ・　取扱区域の明確化について、取扱区域に該当する箇所をビニールテープ等で区切らなければならないと認識している評価実施機関が見受けられました。 ・　管理区域は、基本的にサーバ室等を想定したものですが、端末を設置している事務室等も管理区域に含まれると認識している評価実施機関が見受けられました。

《ポイント３》マイナンバーガイドライン等を踏まえたリスク対策の記載

マイナンバーガイドラインの参照箇所		対応する 主な評価書の項目	追加・変更内容（例）
使用	➢ アクセス制御（（別添１：安全管理措置）２－Ｆ－ａ） ・　特定個人情報ファイルを取り扱うことのできる情報システム端末等を限定する。 ・　各情報システムにおいて、アクセスすることのできる特定個人情報ファイルを限定する。	Ⅲ３．特定個人情報の使用 ・　リスク１：目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク	・　許可された特定の業務端末だけが、特定個人情報ファイルにアクセスすることができるように、サーバ及びネットワーク機器でアクセス制御の設定をしている。
		Ⅲ３．特定個人情報の使用 ・　リスク２：権限のない者によって不正に複製されるリスク（ユーザ認証の管理）	・　ユーザIDに付与されるアクセス権限によって、業務従事者が、業務に必要な範囲の特定個人情報ファイルだけに、アクセスすることができるよう制御している。 ・　ユーザIDのアクセス権限の設定による制御に加えて、特定個人情報ファイルにアクセスできる業務端末をサーバ及びネットワーク機器のアクセス制御により限定している。
教育	➢ 事務取扱担当者等の教育 （未受講者へ再受講の機会の付与） （（別添１：安全管理措置）２－Ｄ－ｂ） 総括責任者は、保護責任者に対し、課室等における特定個人情報等の適切な管理のために必要な教育研修を行う。 前記教育研修については、教育研修への参加の機会を付与するとともに、研修未受講者に対して再受講の機会を付与する等の必要な措置を講ずる。	Ⅳ その他のリスク対策 ２．従業者に対する教育・啓発	・　入職時に特定個人情報等の適切な取扱いに関する研修の受講を必須としている。また、入職後は年に1回以上、全職員を対象に、情報セキュリティ管理規程等に則した内容の集合研修又はeラーニング等による研修を実施している。 ・　集合研修については複数回開催することで、未受講者への受講の機会を与え、全職員が受講できるようにしている。

参考資料

- 特定個人情報保護評価に関する規則・指針・解説
  URL: https://www.ppc.go.jp/legal/assessment/

- 特定個人情報の適正な取扱いに関するガイドライン
  URL: https://www.ppc.go.jp/legal/policy/

- 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
  URL: https://www.ppc.go.jp/files/pdf/itaku_kanntoku.pdf

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

- 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～（全体版）
  URL: https://www.ppc.go.jp/files/pdf/kansa_manual.pdf

- マイナンバーを適切に取り扱うためのポイント～検査結果を踏まえて～
  URL: https://www.ppc.go.jp/files/pdf/mynumber_point.pdf