

「特定個人情報保護評価の実施手順」の更新

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）第27条第2項の規定に基づく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）の3年ごとの再検討による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）及び特定個人情報保護評価指針の改正に伴い、特定個人情報保護評価の実施手順を更新しました。

主な更新箇所は、下記のとおりです。

記

特定個人情報保護評価の実施手順の主な更新箇所	
p. 8	<b>新規</b> 1. 事前の準備 特定個人情報保護評価の対象となる事務 (特定個人情報保護評価の義務がない事務)
p. 13	<b>新規</b> 3. スケジュールの作成 実施時期の特例（緊急時の事後評価）
p. 16	<b>修正</b> 4. (1) ①基礎項目評価書 ①基礎項目評価書
—	<b>削除</b> 4. (1) ①基礎項目評価書 マイナンバーガイドラインの参照箇所
pp. 17-20	<b>新規</b> 4. (1) ①基礎項目評価書 「IV リスク対策」において「2) 十分である」を選択できる水準
p. 21	<b>新規</b> 4. (1) ①基礎項目評価書 「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
p. 22	<b>修正</b> 4. (1) ②重点項目評価書 ②重点項目評価書
—	<b>削除</b> 4. (1) ②重点項目評価書 マイナンバーガイドラインの参照箇所

p. 23	修正	4. (1) ③全項目評価書 ③全項目評価書
—	削除	4. (1) ③全項目評価書 マイナンバーガイドラインの参照箇所
p. 24	修正	4. (1) ③全項目評価書 マイナンバーガイドラインを踏まえたリスク対策の記載例

特定個人情報保護評価の対象となる事務  
(特定個人情報保護評価の義務がない事務)

1. 事前の準備 ※地方公共団体の長その他の機関に関係する規定を抜粋

**特定個人情報保護評価の対象となる事務**

- 番号法等<※1>の規定に基づき、**特定個人情報ファイル**<※2>を**取り扱う事務**が対象。
- ・ 個人番号をシステムやサーバに保存するかどうかではなく、**事務において特定個人情報ファイルを取り扱うかどうか(事務を行う権限を有する者が個人番号に紐付けてアクセスできるかどうか)**が判断基準<※3>。
- ・ 個人番号を画面や帳票などで見ることができる場合<※1>や、システムの内部処理において個人番号を用いる場合<※4>【※2】は、保護評価の対象。
- ・ 情報提供NWSを使用した情報連携を行う事務は、(必ず特定個人情報ファイルを取り扱うこととなるため)保護評価の対象。

<※1> 番号法のほか、番号法以外の法令又は番号法第9条第2項の規定に基づき地方公共団体が定める条例に基づく事務も対象。

<※2> 「特定個人情報ファイル」とは、個人番号を含む個人情報ファイルをいい、個人情報を含む情報の集合物であって、特定個人情報を検索することができるように体系的に構成したもので、システムで保管されるファイル(データベースなど)や特定個人情報が表形式で整理された表計算ソフト用ファイル(Excelファイル)等について、評価の実施義務がある。表計算ソフトで個人番号が含まれている場合などについては、文字列検索を行わねば特定個人情報を検索できないものについては、これに該当しない。

<※3> 本人確認書類としてマイナンバーカードを確認すること自体は、「特定個人情報ファイルの取扱い」に該当しない。

<※4> 例えば、システムの画面や帳票などでは個人番号を出力することとしている(いずれの番号も個人番号を画面や帳票などで見ることができない)場合であっても、当該システム内部では個人番号から個人番号を検索し、個人番号を利用している場合などは、特定個人情報ファイルに該当する(例えば、事務システムにおいて個人番号を保有していないとしても、短名番号を保有しており、また個人番号と短名番号の対応テーブルを保有する統合短名システムを随時参照する場合等は、特定個人情報ファイルに該当する)。

**特定個人情報保護評価の義務がない事務**

- **特定個人情報ファイルを取り扱わない事務**(アクセス制御がされており、左記【※1】と【※2】のいずれも不可能な場合を含む。)
- 紙媒体の台帳等、**手作業処理用ファイルのみを取り扱う事務**。
- 下記のいずれかに該当する場合、左記対象事務も含め、保護評価の対象外。
  - ・ **対象人数<※5>が1,000人未満の事務**。
  - ・ 職員又は職員であった者等の人事、給与、福利厚生に関する事項等を記録した特定個人情報ファイルのみを取り扱う事務。

<※5> 該当事務において保有する全ての特定個人情報ファイルに記録される“本人”の総数。本人とは、個人番号によって識別される特定の個人をいい、当該事務における受給者等に限定されない(例えば、医療保険の場合、被保険者だけでなく、個人番号を保有する被扶養者等の数についても対象人数に含まれる)。また、ある時点において保有する特定個人情報ファイルに記録される本人の数はなく、その事務において総数に取扱う特定個人情報の本人の数を当該事務に横断して、対象人数を計上する必要がある。

注：黄色のテーブルのみに個人番号が存在する場合

⇒ A事務(グリーン)及びC事務(オレンジ)について評価実施義務あり、B事務(水色)については義務なし。

◆参照：指針「第4 特定個人情報保護評価の対象」、「第4の3 特定個人情報ファイル」

実施時期の特例(緊急時の事後評価)

3. スケジュールの作成

実施時期の特例(緊急時の事後評価)

- ・ 特定個人情報ファイルを保有等しようとする場合、特定個人情報ファイルを保有する前(又は特定個人情報ファイルに重要な変更を加える前)に実施すること(事前評価)が原則です。
- ・ ただし、災害その他やむを得ない事由(※)により、緊急に特定個人情報ファイルを保有等する必要がある場合には、規則第9条第2項の規定(緊急時の事後評価)に基づき、**特定個人情報ファイルの保有等の後速やかに特定個人情報保護評価を実施するものとされています。**この場合、保護評価を実施することが困難であった状態が解消された時点などの適切な時期において、**可及的速やかに保護評価を実施する必要があります。** ※「業務が多忙なため」、「人手不足のため」等の理由は、「災害その他やむを得ない事由」には該当しません。

※ 緊急時の事後評価の適用対象とならない事務

- ・ 既に個人番号利用事務等として定着している事務については、過去に特定個人情報保護評価を実施した実績があるものであり、「特定個人情報保護評価を事前に実施することが困難である」とはいえないことから、一定の緊急性がある場合であっても、**原則どおり事前評価を行うこととされています。**
- ・ 具体的には、例えば、特定公約給付の支給事務のうち、本人の範囲及び特定個人情報ファイルを取り扱うプロセスが類似する事務を過去に反復して実施している場合(例：子育て世帯への給付金、低所得世帯への給付金、出産・子育て応援給付金など。)は、事前評価を実施する必要があります。
- ・ ただし、既に個人番号利用事務等として定着している事務であっても、著しい緊急性が認められる場合や、事前評価を実施することが著しく困難である場合(例：全項目評価の再実施が義務付けられており、特定個人情報ファイルの保有等の前に、国民・住民等への意見聴取や委員会による審査・第三者点検などの期間を確保することができない等)には、緊急時の事後評価の適用対象となります。

**9. 規則第9条第2項の適用** [ ] 適用した

適用した理由

災害その他やむを得ない事由により、保護評価規則第9条第2項の規定(緊急時の事後評価)を適用し、特定個人情報ファイルを保有した後又は特定個人情報ファイルに重要な変更を加えた後に保護評価を実施した場合には、**その旨及び適用した理由を基礎項目評価書に記載する必要があります(令和6年10月1日施行)。**

◆参照：指針の解説「第6の3 規則第9条第2項の規定(緊急時の事後評価)の適用について」

修正

【p.16】 4. (1) ①基礎項目評価書

①基礎項目評価書

4. (1) ①基礎項目評価書

1. 事前準備 2. しきい値判断 3. 評価項目の作成 4. 評価書の作成 5. 評価書の提出

① 基礎項目評価書

しきい値判断の結果、重点又は全項目評価の対象となる場合も、基礎項目評価書を作成する必要があります。

【I 関連情報】、「II しきい値判断項目」、「III しきい値判断結果」

- 指針の解説「別添2 特定個人情報保護評価書（基礎項目評価書）【記載要領】」を参照しつつ、各項目について必要な内容を記載します。

【IV リスク対策】

- IVは、評価対象の事務における特定個人情報ファイルの取扱いプロセスにおいて想定されるリスクへの対策について各評価実施機関の自己評価を記載するものです。例示されている各リスクにどのように対応しているかを確認することで、十分なリスク対策が実施されているかを検討します。
- 検討に当たっては、指針の解説「別添2 特定個人情報保護評価書（基礎項目評価書）【記載要領】」及び、マイナンバーガイドラインを参考にしてください。
- 記載要領においては、「IV リスク対策」において「十分である」を選択することができる水準（本資料の次ページ以降にも掲載）や、マイナンバーガイドラインの参照箇所についても掲載しています。
- 「IV リスク対策」の「人為的ミスが発生するリスクへの対策」、「最も優先度が高いと考えられる対策」の「判断根拠」の欄について、指針の解説において記載例を掲載しています。
- マイナンバーガイドラインの参照箇所は、本資料のP.15～P.16を参考にしてください。

◆参照：指針「第9 2 (1) 基礎項目評価書」  
指針の解説「別添2 特定個人情報保護評価書（基礎項目評価書）【記載要領】」、「第9の2 (1)」  
マイナンバーガイドライン「（別添1）特定個人情報に関する安全管理措置（行政機関等編／事業者編）」

16

削除

【一】 4. (1) ①基礎項目評価書

マイナンバーガイドラインの参照箇所

4. (1) ①基礎項目評価書

マイナンバーガイドラインの参照箇所

評価項目	マイナンバーガイドラインの参照箇所
1. 特定個人情報の取扱いに係る組織体制	第4-1-1(1) 組織体制
2. 特定個人情報の取扱いに係る業務体制	第4-1-1(2) 業務体制
3. 特定個人情報の取扱いに係る安全管理措置	第4-1-2(1) 安全管理措置
4. 特定個人情報の取扱いに係る関係機関との連携	第4-1-3(1) 関係機関との連携

15

4. (1) ①基礎項目評価書

評価項目	マイナンバーガイドラインの参照箇所
1. 特定個人情報の取扱いに係る組織体制	第4-1-1(1) 組織体制
2. 特定個人情報の取扱いに係る業務体制	第4-1-1(2) 業務体制
3. 特定個人情報の取扱いに係る安全管理措置	第4-1-2(1) 安全管理措置
4. 特定個人情報の取扱いに係る関係機関との連携	第4-1-3(1) 関係機関との連携

16

「IV リスク対策」において「2) 十分である」を選択できる水準

4. (1) ①基礎項目評価書

「IV リスク対策」において「2) 十分である」を選択できる水準

基礎項目評価書中「IV リスク対策」において記載する特定個人情報保護の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。

「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、**1つでも変更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ありません。**
- 組織的安全管理措置、人的安全管理措置**については記載していないが、**マイナンバー-GLに照り、必要な措置を講ずる必要があります。**
  - ・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、漏れ等事案に対応する体制等の整備、取扱状況等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応
- 「**特に力を入れている**」を選択できる基準は、「十分である」を選択できる基準を満たした上で、さらに、**評価実施機関独自の取組を実施している場合**に選択することができます。

基礎項目評価書の項目		「2) 十分である」を選択できる水準
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	目的外の入手が行われるリスクへの対策	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 対象者、必要な情報の種類、入手方法を踏まえ、「対象者以外の情報」や「必要な情報」以外の入手を防止するための措置を、システム面、人手による作業の面から講じている。
3. 特定個人情報の使用	目的を超えた細付け、事務に必要な情報との紐付けが行われるリスクへの対策	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 宛名システムやその他の業務システムにおいて、記録されている特定個人情報のうち業務上必要のない特定個人情報に、各業務担当者がアクセスできないようにアクセス制御を行っている。
	権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスクへの対策	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）＞ ※ リスク対策の詳細については、「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／事業者編）（平成26年特定個人情報保護委員会告示第6号／平成26年特定個人情報保護委員会告示第5号）」の「E 物理的安全管理措置」「F 技術的安全管理措置」等参照。 ① ユーザ認証の管理を行っている。 ② アクセス権限の発効・失効の管理を行っている。 ③ アクセス権限の管理を行っている。 ④ 特定個人情報の使用の記録、分析（改ざん等の防止に係る対策を含む。）を行っている。

4. (1) ①基礎項目評価書

基礎項目評価書の項目

「2) 十分である」を選択できる水準

4. 特定個人情報ファイルの取扱いの委託	委託先における不正な使用等のリスクへの対策	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）＞ ※ リスク対策の詳細については、「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／事業者編）（平成26年特定個人情報保護委員会告示第6号／平成26年特定個人情報保護委員会告示第5号）」の「第4-2-（1）委託の取扱い」等を参照。 ① 委託先における情報保護管理体制の確認を行っている。 ② 委託先における特定個人情報ファイルの閲覧者・更新者を制限している。 ③ 委託先における特定個人情報ファイルの取扱いの記録を行っている。 ④ 委託先から他者への又は委託元から委託先への特定個人情報の提供に関するルールを定めている。 ⑤ 委託先における特定個人情報の消去に関するルールを定めている。 ⑥ 委託契約において、特定個人情報ファイルの取扱いに関する規定を盛り込んでいる。 ⑦ 再委託が行われる場合、再委託先による特定個人情報ファイルの適切な取扱いを確保するための措置を講じている。
5. 特定個人情報の提供・移動（委託や情報提供ネットワークシステムを通じた提供を除く。）	不正な提供・移動が行われるリスクへの対策	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）＞ ※ リスク対策の詳細については、「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／事業者編）（平成26年特定個人情報保護委員会告示第6号／平成26年特定個人情報保護委員会告示第5号）」の「E 物理的安全管理措置」「F 技術的安全管理措置」を参照。 ① 特定個人情報の提供・移動に関するルールが定められている。 ② 特定個人情報の提供・移動の記録し、その記録を一定期間保存している。 ③ 当該記録を定期的に及び随時分析等するための体制を整備している。 ④ 当該記録について、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。
6. 情報提供ネットワークシステムとの接続	目的外の入手が行われるリスクへの対策	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 自行システム側において、必要最低限の人数、参照範囲となるよう、職員のアクセス権限を設定している。 ② アクセス権限の所有者は、ID、パスワード等を適切に管理するとともに、離席時のログアウトを徹底する。

◆参照：指針の解説「第9の2（1）基礎項目評価書」

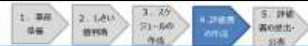
#### 4. (1) ①基礎項目評価書



基礎項目評価書の項目		「2」 十分である」を選択できる水準
6. 情報提供ネットワークシステムとの接続	不正な提供が行われるリスクへの対策	<p>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&lt;典型的リスク対策（例）&gt;</p> <ol style="list-style-type: none"> <li>① 自分システムの副本登録画面について、必要最低限の人数、情報の範囲となるよう、職員のアクセス権限を設定する。</li> <li>② アクセス権限の所有者は、ID、パスワード等を適切に管理するとともに、離席時のログアウトを徹底する。</li> <li>③ 副本登録を自動連携により行う場合は、サーバーにアクセス権限等を付与する。</li> <li>④ 住民基本台帳事務における支援措置対象者等については自動応答不可フラグを設定する等、必要な対応を行う。</li> <li>⑤ 「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。</li> </ol> <p>（例）</p> <ul style="list-style-type: none"> <li>・ 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。</li> <li>・ 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。</li> <li>・ 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。</li> <li>・ 更新時には、本人から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。</li> </ul>
7. 特定個人情報の保管・消去	特定個人情報の漏えい・滅失・毀損リスクへの対策	<p>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&lt;典型的リスク対策（例）&gt;</p> <p>※ リスク対策の詳細については、「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/事業者編）（平成26年特定個人情報保護委員会告示第6号/平成26年特定個人情報保護委員会告示第5号）」の（別添1）2「C 組織的安全管理措置」、「E 物理的安全管理措置」、「F 技術的安全管理措置」を参照。</p> <ol style="list-style-type: none"> <li>① 内閣サイバーセキュリティセンター（NISC）による政府機関等のサイバーセキュリティ対策のための統一基準群（「政府機関等のサイバーセキュリティ対策のための統一基準」中「第3部 情報の取扱い」、「第5部 情報システムのライフサイクル」、「第6部 情報システムの構成要素」、「第7部 情報システムのセキュリティ要件」、「第8部 情報システムの利用」等）及びそれに基づく各府省庁ポリシーを遵守している。（評価実施機関が政府機関の場合のみ）</li> <li>② 地方公共団体においては、地方公共団体における情報セキュリティポリシーに関するガイドライン等を参考に地方公共団体において策定した情報セキュリティポリシー等（第3編第2章中「2. 情報資産の分類と管理」、「3. 情報システム全体の強靱性の向上」、「4. 物理的セキュリティ」、「6. 技術的セキュリティ」等）を遵守している。</li> <li>③ 漏えい・滅失・毀損を防ぐために、物理的安全管理措置や技術的安全管理措置を実施している。</li> <li>④ 特定個人情報ファイルの漏失・毀損が発生した場合に復旧できるよう、バックアップを保管している。</li> <li>⑤ 過去の漏えい等事案を踏まえた、再発防止策を実施している。</li> </ol>

◆参照：指針の解説「第9の2（1）基礎項目評価書」 19

#### 4. (1) ①基礎項目評価書



基礎項目評価書の項目		「2」 十分である」を選択できる水準
8. 人手を介在させる作業	人為的ミスが発生するリスクへの対策は十分か	<p>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&lt;典型的リスク対策（例）&gt;</p> <ol style="list-style-type: none"> <li>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。</li> </ol> <p>（例）</p> <ul style="list-style-type: none"> <li>・ 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。</li> <li>・ 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。</li> <li>・ 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。</li> <li>・ 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。</li> </ul> <ol style="list-style-type: none"> <li>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。</li> </ol> <p>※ 人為的ミス発生防止の観点等として、次の資料が参考となる（いずれも個人情報保護委員会ウェブページ公表資料：<a href="https://www.ppc.go.jp/legal/kensyuushiryou/">https://www.ppc.go.jp/legal/kensyuushiryou/</a>）。</p> <ul style="list-style-type: none"> <li>・ 「特定個人情報を取り扱ふ際の注意ポイント」</li> <li>・ 「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ぐための着眼点—」</li> </ul>
10. 従業者に対する教育・啓発	従業者に対する教育・啓発	<p>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&lt;典型的リスク対策（例）&gt;</p> <p>※ リスク対策の詳細については、「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/事業者編）（平成26年特定個人情報保護委員会告示第6号/平成26年特定個人情報保護委員会告示第5号）」の「D 人的安全管理措置」を参照。</p> <ol style="list-style-type: none"> <li>① 研修計画を策定している。</li> <li>② 事務取扱者の適切な監督を行っている。</li> <li>③ 次の事務取扱者等への教育研修を行っている。</li> </ol> <ul style="list-style-type: none"> <li>・ 事務取扱者への研修</li> <li>・ 特定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への研修</li> <li>・ 保護責任者への研修</li> <li>・ 事務取扱者へのサイバーセキュリティ研修（おおむね1年ごと）。</li> </ul> <p>※ 未受講者には、再受講の機会を付与する等の必要な措置を講ずること。</p>

◆参照：指針の解説「第9の2（1）基礎項目評価書」 22

「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

4. (1) ①基礎項目評価書

1. 基礎情報 2. しい 3. スの 4. 評価 5. 評価

1. 最も優先度が低いと考えられる対策

2. 最も優先度が高いと考えられる対策

3. 基礎項目評価書又は重点項目評価書に該当する

「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

基礎項目評価書の「IV リスク対策」には、措置状況の評価の根拠（自由記述）を記載する欄が2箇所あります。指針の解説において、各項目の記載例を掲載していますので、参考にしてください。

人手的ミスが発生するリスクへの対策は十分か	十分である	人手的ミスが発生するリスクへの対策は十分か	十分である
対策の根拠	自由記述	対策の根拠	自由記述

リスク対策	記載例
人手的ミスが発生するリスクへの対策は十分か	<p>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、人手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。</p> <ul style="list-style-type: none"> <li>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</li> <li>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</li> <li>個人番号及び本人情報が記載された申請書の廃棄</li> </ul> <p>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。</p> <p>また、人手が介在する局面ごとに、人手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。</p> <ul style="list-style-type: none"> <li>人手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。</li> <li>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。</li> <li>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。</li> <li>特定個人情報を含む書類やUSBメモリは、施錠できる書類等に保管することを徹底する。</li> <li>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。</li> </ul> <p>これらの対策を講じていることから、人手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。</p>

指針の解説には、これ以外の項目の記載例も掲載しています。

◆参照：指針の解説「第9の2（1）基礎項目評価書」

②重点項目評価書

4. (1) ②重点項目評価書

1. 基礎情報 2. しい 3. スの 4. 評価 5. 評価

② 重点項目評価書

「I 基本情報」、「II 特定個人情報ファイルの概要」、「IV 開示請求、問合せ」、「V 評価実施手続」

- 指針の解説「別添3 特定個人情報保護評価書（重点項目評価書）〔記載要領〕」を参照しつつ、各項目について必要な内容を記載します。

「III リスク対策」

- 指針の解説「別添3 特定個人情報保護評価書（重点項目評価書）〔記載要領〕」を参照しつつ、**マイナンバーガイドライン**を踏まえて、項目について必要な内容を記載します。
- ◆**マイナンバーガイドラインの参照箇所は、本資料のP.18～P.19を参考にしてください。**
- 記載要領においては、マイナンバーガイドラインの主な参照箇所も掲載しています。

◆参照：指針「第9の2（2）重点項目評価書」  
指針の解説「別添3 特定個人情報保護評価書（重点項目評価書）〔記載要領〕」  
マイナンバーガイドライン「（別添1）特定個人情報に関する安全管理措置（行政機関等編／事業者編）」

削除

【一】 4. (1) ②重点項目評価書  
マイナンバーガイドラインの参照箇所

修正

【p.23】 4. (1) ③全項目評価書  
③全項目評価書

4. (1) ③全項目評価書

③ 全項目評価書

「Ⅰ基本情報」、「Ⅱ特定個人情報ファイルの概要」、「Ⅴ開示請求、問合せ」、「Ⅵ評価実施手続」

- 指針の解説「別添4 特定個人情報保護評価書（全項目評価書）〔記載要領〕」を参照しつつ、各項目について必要な内容を記載します。

「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」、「Ⅳその他のリスク対策」

- 指針の解説「別添4 特定個人情報保護評価書（全項目評価書）〔記載要領〕」を参照し、**マイナンバーガイドラインを踏まえて**、各項目について必要な内容を記載します。
- 記載要領においては、**マイナンバーガイドラインの主な参照箇所も掲載**しています。
- マイナンバーガイドラインの参照箇所は、本資料のP.21～P.22を参考にしてください。**
- また、マイナンバーガイドラインを踏まえた評価書の記載例を、本資料のP.23に示しています。**

◆参照：指針「第9 2 (3) 全項目評価書」  
指針の解説「別添4 特定個人情報保護評価書（全項目評価書）〔記載要領〕」  
マイナンバーガイドライン「（別添1）特定個人情報に関する安全管理措置（行政機関等編／事業者編）」

27

削除

【一】 4. (1) ③全項目評価書  
マイナンバーガイドラインの参照箇所



マイナンバーガイドラインを踏まえたリスク対策の記載例  
 ⇒ マイナンバーガイドラインの参照箇所を記載要領に掲載すること  
 となったことに伴い、記載要領に合わせる修正を行いました。

4. (1) ③全項目評価書

マイナンバーガイドラインを踏まえたリスク対策の記載例

3. 特定個人情報の使用

リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク

ユーザー認証の管理

具体的管理方法

【 行っている 】 <選択肢>

1) 行っている 2) 行っていない

- 特定個人情報を取り扱う端末がある区域には、事務取扱担当者以外の者が入室できないようにした上で、事務取扱担当者には、ログインしたまま端末を放置せず、離席時にはログアウトすることやログインID、パスワードの使いまわしをしないことを徹底させている。
- ユーザー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。
- 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。

■ マイナンバーガイドラインの主な参照箇所及び概要 ■

(別添1) 特定個人情報に関する安全管理措置

C 組織的安全管理措置

b 取扱規程等に基づく運用

D 人的安全管理措置

a 事務取扱担当者の監督

b 事務取扱担当者等の教育

F 技術的安全管理措置

a アクセス制御

b アクセス権の識別と認証

30

以上