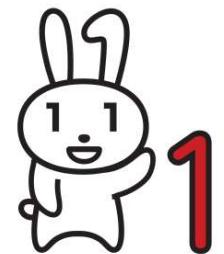




# 特定個人情報保護評価の実施手順



令和4年7月  
(令和7年7月最終改訂)  
個人情報保護委員会事務局

# 目次

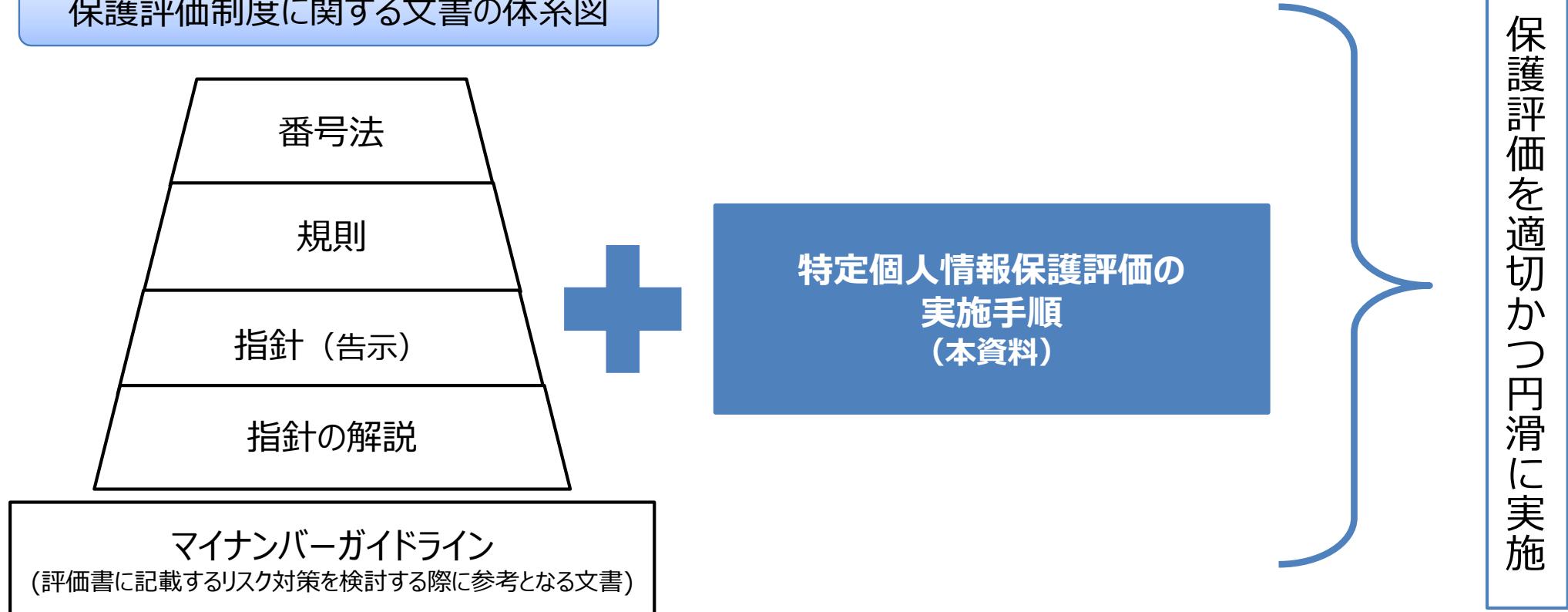
|                  |       |    |
|------------------|-------|----|
| ◆はじめに            | ..... | 2  |
| 保護評価の実施主体と実施時期   | ..... | 3  |
| ◆ I . 保護評価の実施手順  | ..... | 4  |
| 1 . 事前の準備        | ..... | 6  |
| 2 . しきい値判断       | ..... | 9  |
| 3 . スケジュールの作成    | ..... | 10 |
| 4 . 評価書の作成       | ..... | 14 |
| ( 1 ) 評価書の作成     | ..... | 15 |
| ① 基礎項目評価書        | ..... | 16 |
| ② 重点項目評価書        | ..... | 22 |
| ③ 全項目評価書         | ..... | 23 |
| ( 2 ) 評価書の確認     | ..... | 25 |
| 5 . 評価書の提出・公表    | ..... | 27 |
| ◆ II . 評価書公表後の対応 | ..... | 28 |

# はじめに

- ・本資料は、特定個人情報保護評価（以下「保護評価」という。）の実施手順と特定個人情報保護評価書（以下「評価書」という。）の作成方法について、図表を多用するなどして分かりやすく示したものです。
- ・評価実施機関において、法令等（※）をよく理解するとともに、本資料も併せて参考することにより、保護評価を適切かつ円滑に実施していただくことを期待しています。

※ 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（以下「番号法」という。）、特定個人情報保護評価に関する規則（以下「規則」という。）、特定個人情報保護評価指針（以下「指針」という。）、特定個人情報保護評価指針の解説（以下「指針の解説」という。）及び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）（以下「マイナンバーガイドライン」という。）

## 保護評価制度に関する文書の体系図



# 保護評価の実施主体と実施時期



以下に該当する者が特定個人情報ファイルを保有しようとする場合、保有前（当該事務でシステムを使用する場合は、プログラミング開始前）に評価書を作成し、個人情報保護委員会（以下「委員会」という。）へ提出の上、公表することが、番号法等により原則として義務付けられています！

## 保護評価の実施主体

- ① 国の行政機関の長
- ② 地方公共団体の長その他の機関
- ③ 独立行政法人等
- ④ 地方独立行政法人
- ⑤ 地方公共団体情報システム機構
- ⑥ 情報提供ネットワークシステムを使用した情報連携を行う事業者（健康保険組合等）



各ページに、指針等の関連箇所をお示します。  
指針や指針の解説等も併せて参考しながら保護評価を実施してください。

◆参照：指針「第1 特定個人情報保護評価の意義」、「第2 定義」、「第3 特定個人情報保護評価の実施主体」、「第6 特定個人情報保護評価の実施時期」

# I .保護評価の実施手順

---

実施手順の全体像

1. 事前の準備
2. しきい値判断
3. スケジュールの作成
4. 評価書の作成
5. 評価書の提出・公表



# 実施手順の全体像



実施手順は、下図のとおりです。実施体制及び役割は、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りますが、以下では推奨される例をお示します。

1.事前準備

2.しきい値判断

3.スケジュール  
の作成

4.評価書の作成

5.評価書の  
提出・公表

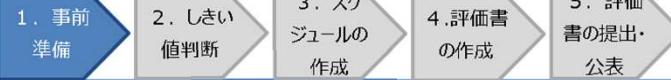
| 何をする<br>誰が | 事前の準備<br>(P. 6)     | しきい値判断<br>(P.9)       | スケジュールの作成<br>(P.10) | 評価書の作成<br>(P.14)  | 評価書の確認<br>(P.25) | 委員会への<br>提出・公表<br>(P.27) |
|------------|---------------------|-----------------------|---------------------|-------------------|------------------|--------------------------|
| 総括部署       | 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（法令面等）       | 評価書の確認           | 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 | スケジュールの作成           | 評価書の作成            | 必要に応じて根拠資料の提出等   | 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          | —                     | システム面のスケジュール管理・共有   | システム面の情報提供（作成を補助） | 必要に応じて根拠資料の提出等   | 評価書の提出・公表作業の補助           |

※ 特定個人情報保護評価計画管理書を「計画管理書」という（以下同じ。）。



◆参照：指針「第1～4 特定個人情報保護評価の実施体制」、「第5 特定個人情報保護評価の実施手続」

# 1. 事前の準備



まずは、計画管理書を用いて、保護評価の対象となる事務及びシステムを適切に把握します。



## 計画管理書の作成・更新

- ① 番号法別表等（※）を基に、保護評価の対象となる事務を特定します。

※ 地方公共団体については同法第9条第2項に基づく条例を含む。

なお、保護評価は、原則として番号法別表に掲げる事務ごとに実施するものとしていますが、評価実施機関の判断で法令上の事務を分割又は統合することも可能です。事務の実施状況等を踏まえて、保護評価の単位は合理的に判断してください。

- ② 担当部署及び使用するシステムの情報を整理します。

| 評価書番号 | 法令上の根拠       | 事務の名称      | システムの名称  | 情報連携 | 基礎項目評価    |         |        |       | 重点項目／全項目評価 |       |     |  | 備考 | 担当部署  |
|-------|--------------|------------|----------|------|-----------|---------|--------|-------|------------|-------|-----|--|----|-------|
|       |              |            |          |      | 前回実施日     | 次回実施予定日 | しきい値判断 | 前回実施日 | 次回実施予定日    |       |     |  |    |       |
| 1     | 番号法第9条別表56の項 | 児童手当に関する事務 | 児童手当システム | ○    | 令和5年5月27日 | 2025年   | 5月頃    | 重点    | 令和5年5月27日  | 2025年 | 5月頃 |  |    | 児童福祉課 |
|       | ①            | ①          | ②        | ①    |           |         |        |       |            |       |     |  |    | ②     |
|       |              |            |          |      |           |         |        |       |            |       |     |  |    |       |



◆参照：指針「第4 特定個人情報保護評価の対象」、「第5-1 特定個人情報保護評価計画管理書」  
指針の解説「別添1 特定個人情報保護評価計画管理書〔記載要領〕」

# 1. 事前の準備

1. 事前  
準備

2. しきい  
値判断

3. スケ  
ジュールの  
作成

4. 評価  
書の作成

5. 評価  
書の提出・  
公表

さらに、主務省令等から事務の内容を明確化し、保護評価の対象となる事務の範囲を整理することで、次のページ以降の「しきい値判断」や「評価書の作成」をスムーズに行うことができます。



## 事務の内容を明確化

- ③ 主務省令（※1）等を基に、計画管理書に記載した事務について、保護評価の対象となる事務の内容を明確化します。

※1 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別表の主務省令で定める事務を定める命令、  
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第十九条第八号に基づく利用特定個人情報の提供に関する命令

### 【（例）児童手当の事務の場合】

| 具体的な事務手續          | 事務でマイナンバーを使用しているか | 情報連携の有無 | 評価書への記載要否（※2） |
|-------------------|-------------------|---------|---------------|
| 受給資格等についての認定請求の受理 | ○                 | ×       | 必要            |
| 額改定請求の受理          | ○                 | ×       | 必要            |
| 届出の受理に係る事実の審査     | ○                 | ○       | 必要            |
| 通知書の送付            | ×                 | —       | 不要            |
| ...               | ...               | ...     | ...           |

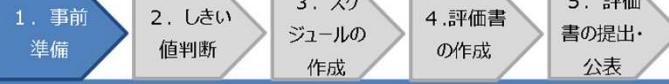
※2 保護評価の対象は、特定個人情報ファイルを取り扱う事務です。ただし、手作業処理用ファイル（紙ファイルなど）のみを取り扱う事務など、指針第4の4（1）に定める事務については、保護評価の実施が義務付けられません（任意で実施することを妨げるものではありません。）。



◆参照：指針「第4 特定個人情報保護評価の対象」

# 1. 事前の準備

※地方公共団体の長その他の機関に関する規定を抜粋



## 特定個人情報保護評価の対象となる事務

- 番号法等<sup><注1></sup>の規定に基づき、**特定個人情報ファイル**<sup><注2></sup>を取り扱う事が対象。

- 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<sup><注3></sup>。
- 個人番号を画面や帳票などで見ることができる場合<sup><※1></sup>や、システムの内部処理において個人番号を用いる場合<sup><注4></sup><sup><※2></sup>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。

<注1> 番号法（別表に掲げる事務、第9条第3項から第6項までに規定する事務）のほか、番号法以外の国の法令（住民基本台帳法に基づく住民票に関する事務等）や同条第2項の規定に基づき地方公共団体が定める条例を指す。

<注2> 「特定個人情報ファイル」とは、個人番号をその内容に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体系的に構成したもの。ITシステムで保有されるファイル（データベースなど）や特定個人情報が表形式等に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。決裁文書中に個人番号が含まれている場合などのように、文字列検索を行わなけれ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。

<注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。

<注4> 例えば、システムの画面や帳票などでは既存番号を入出力することをしている（いずれの者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既存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Aにおいて個人番号を保有していないても、宛名番号を保有しており、さらに個人番号と宛名番号の対照テーブルを保有する統合宛名システムを隨時参照する場合等は、特定個人情報ファイルに該当する。）。

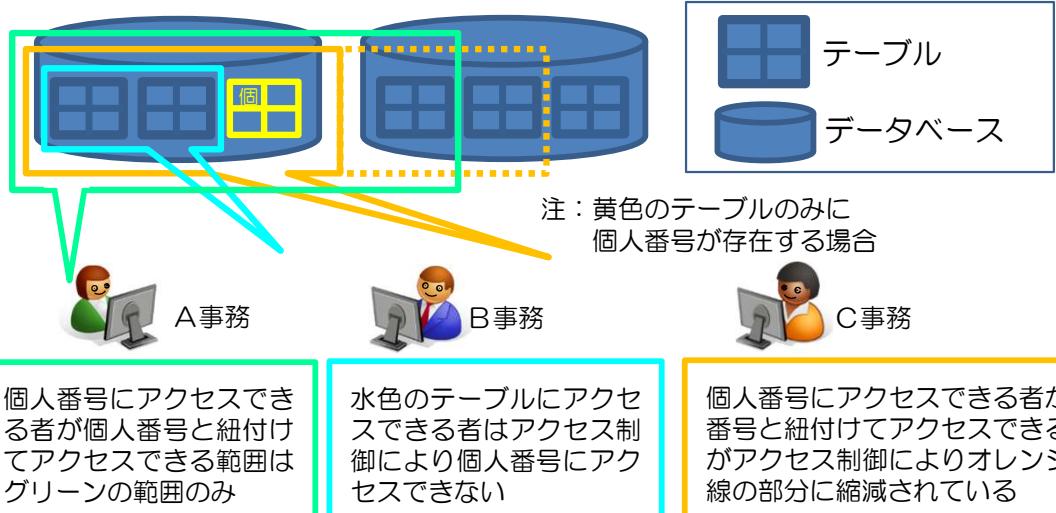


◆参考：指針「第4 特定個人情報保護評価の対象」、「第4 3 特定個人情報ファイル」

## 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<sup><注5></sup>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。

<注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”的の数の総数。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、被保険者だけではなく、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ではなく、その事務において経常的に取り扱う特定個人情報の本人の数を合理的に推測して、対象人数を計上する必要がある。



⇒ 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。

## 2. しきい値判断

1. 事前準備

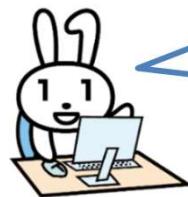
2. しきい値判断

3. スケジュールの作成

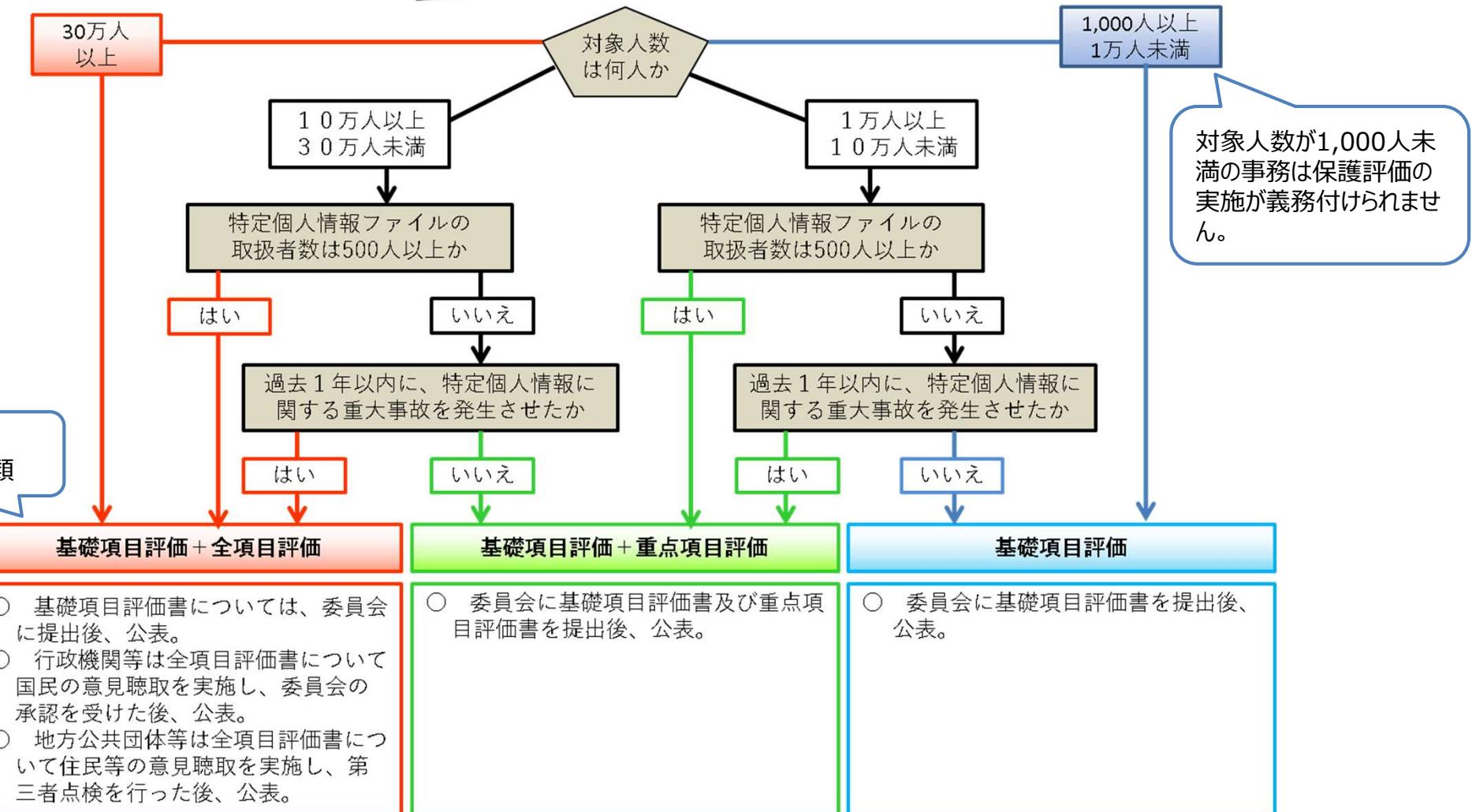
4. 評価書の提出・公表

5. 評価書の提出・公表

### しきい値判断フロー図

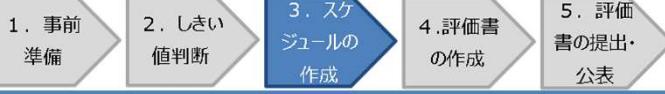


しきい値判断を行い、実施すべき保護評価の種類を判断します。



◆参照：指針「第5 2 しきい値判断」

### 3. スケジュールの作成

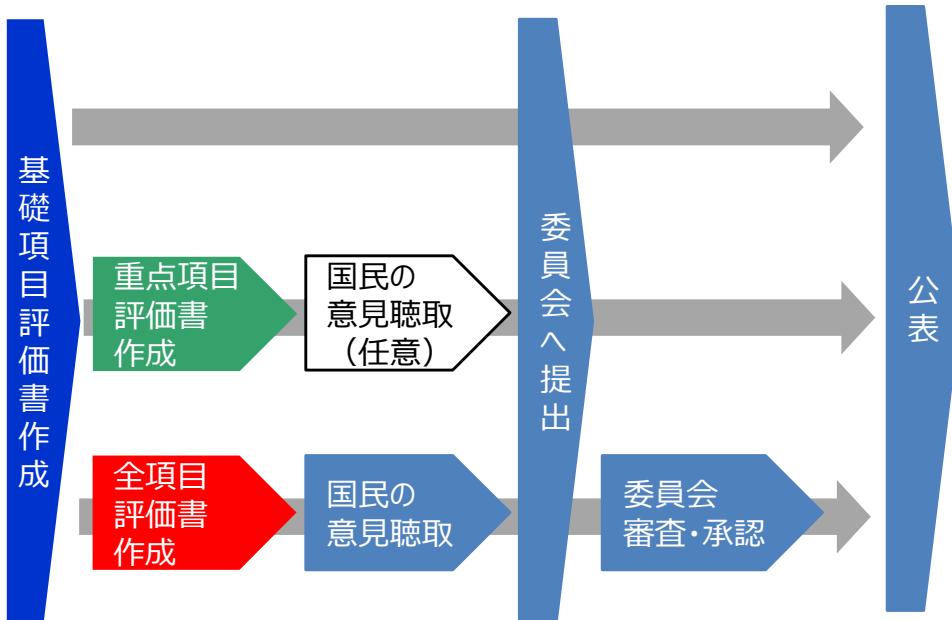


#### 保護評価の実施スケジュール

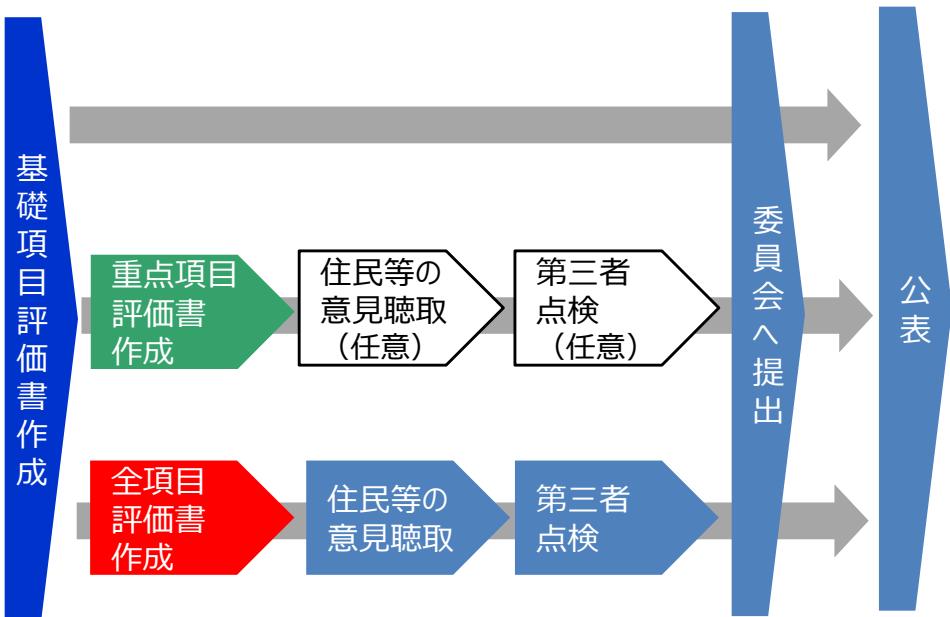


保護評価の実施主体や、どの評価書を作成するかによって、評価書の作成から公表までの手順が異なります。

#### 行政機関等



#### 地方公共団体等



- 行政機関等：地方公共団体等以外の評価実施機関（行政機関の長、独立行政法人等、地方公共団体情報システム機構並びに番号法第19条第8号に規定する情報照会者及び情報提供者）



◆参照：指針「第5 3 特定個人情報保護評価書」

### 3. スケジュールの作成

1. 事前準備

2. しきい値判断

3. スケジュールの作成

4. 評価書の提出・公表

5. 評価書の提出・公表



保護評価は原則として、特定個人情報ファイルを保有等する前に実施する必要があります。  
特定個人情報ファイルの保有等に当たりシステム開発を行う場合は、遅くともプログラミング開始前に保護評価を実施する必要があります。

#### 重点項目評価の場合

プログラミング開始前までに保護評価を実施

| 評価書名                 | 区分            | N年 |      |      |           |      |         | N+1年 |     |   |      |
|----------------------|---------------|----|------|------|-----------|------|---------|------|-----|---|------|
|                      |               | 7月 | 8    | 9    | 10        | 11   | 12      | 1    | 2   | 3 | 4    |
| ○○に関する事務<br>(重点項目評価) | システムの開発スケジュール |    | 要件定義 | 基本設計 | 詳細設計      |      | プログラミング |      | テスト |   | 運用開始 |
|                      | 保護評価の実施スケジュール |    |      | 事前準備 | 評価書の作成、確認 | 提出公表 |         |      |     |   |      |

※ 基礎項目評価のみの場合も、重点項目評価と同様の実施手順です。具体的な手順は、指針の解説にフロー図を記載しているので、参考にしてください。



◆参照：指針「第5 3 特定個人情報保護評価書」、「第6 特定個人情報保護評価の実施時期」

### 3. スケジュールの作成

1. 事前準備

2. しきい値判断

3. スケジュールの作成

4. 評価書の提出・公表

5. 評価書の提出・公表

#### 全項目評価の場合

プログラミング開始前までに保護評価を実施

| 評価書名                   | 区分            | N年 |      |           |             |       |      | N+1年    |     |   |      |
|------------------------|---------------|----|------|-----------|-------------|-------|------|---------|-----|---|------|
|                        |               | 7月 | 8    | 9         | 10          | 11    | 12   | 1       | 2   | 3 | 4    |
| ○○に関する事務※地方公共団体(全項目評価) | システムの開発スケジュール |    |      | 要件定義      | 基本設計        | 詳細設計  |      | プログラミング | テスト |   | 運用開始 |
|                        | 保護評価の実施スケジュール |    | 事前準備 | 評価書の作成、確認 | パブリックコメント実施 | 第三者点検 | 提出公表 |         |     |   |      |



保護評価の結果を受けて、当初予定していた特定個人情報ファイルの取扱いやシステム設計を変更しなければならない場合も想定されるため、特に全項目評価の場合は、住民等の意見聴取（パブリックコメント）の期間等を考慮し、十分な時間的余裕を持って実施することを推奨します。



◆参照：指針「第5 3 特定個人情報保護評価書」、「第6 特定個人情報保護評価の実施時期」

### 3. スケジュールの作成

1. 事前準備

2. しきい値判断

3. スケジュールの作成

4. 評価書の提出・公表

5. 評価書の提出・公表

#### 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、特定公的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、事前評価を行う必要があります。
- 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、事前評価を行う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得ます。

#### 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 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」

# 4. 評価書の作成

1. 事前準備

2. しきい値判断

3. スケジュールの作成

4. 評価書の提出・公表

5. 評価書の提出・公表



評価書の作成手順は、まずは評価書の前半（I、II）を用いて、事務の内容や特定個人情報ファイルの取扱いプロセス等を整理します。それらを踏まえて後半（III、IV）のリスク対策を検討・記載してください。

| 全項目評価書                          |   | 重点                    | 基礎                    |
|---------------------------------|---|-----------------------|-----------------------|
| I 基本情報                          | 1. 特定個人情報ファイルを取り扱う事務<br>2. 特定個人情報ファイルを取り扱う事務において使用するシステム<br>3. 特定個人情報ファイル名<br>4. 特定個人情報ファイルを取り扱う理由<br>5. 個人番号の利用<br>6. 情報提供ネットワークシステムによる情報連携<br>7. 評価実施機関における担当部署<br>8. 他の評価実施機関<br>(別添1) 事務の内容 | <input type="radio"/> | <input type="radio"/> |
| II 特定個人情報ファイルの概要                | 1. 特定個人情報ファイル名<br>2. 基本情報<br>3. 特定個人情報の入手・使用<br>4. 特定個人情報ファイルの取扱いの委託<br>5. 特定個人情報の提供・移転（委託に伴うものを除く。）<br>6. 特定個人情報の保管・消去<br>7. 備考<br>(別添2) 特定個人情報ファイル記録項目  | <input type="radio"/> |                       |
| 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 | 1. 特定個人情報ファイル名<br>2. 特定個人情報の入手（情報提供ネットワークを通じた入手を除く。）<br>3. 特定個人情報の使用<br>4. 特定個人情報ファイルの取扱いの委託<br>5. 特定個人情報の提供・移転（情報提供ネットワークを通じた提供を除く。）<br>6. 情報提供ネットワークシステムとの接続<br>7. 特定個人情報の保管・消去               | <input type="radio"/> | <input type="radio"/> |
| IV その他のリスク対策                    | 1. 監査<br>2. 従業者に対する教育・啓発<br>3. その他のリスク対策  | <input type="radio"/> | <input type="radio"/> |



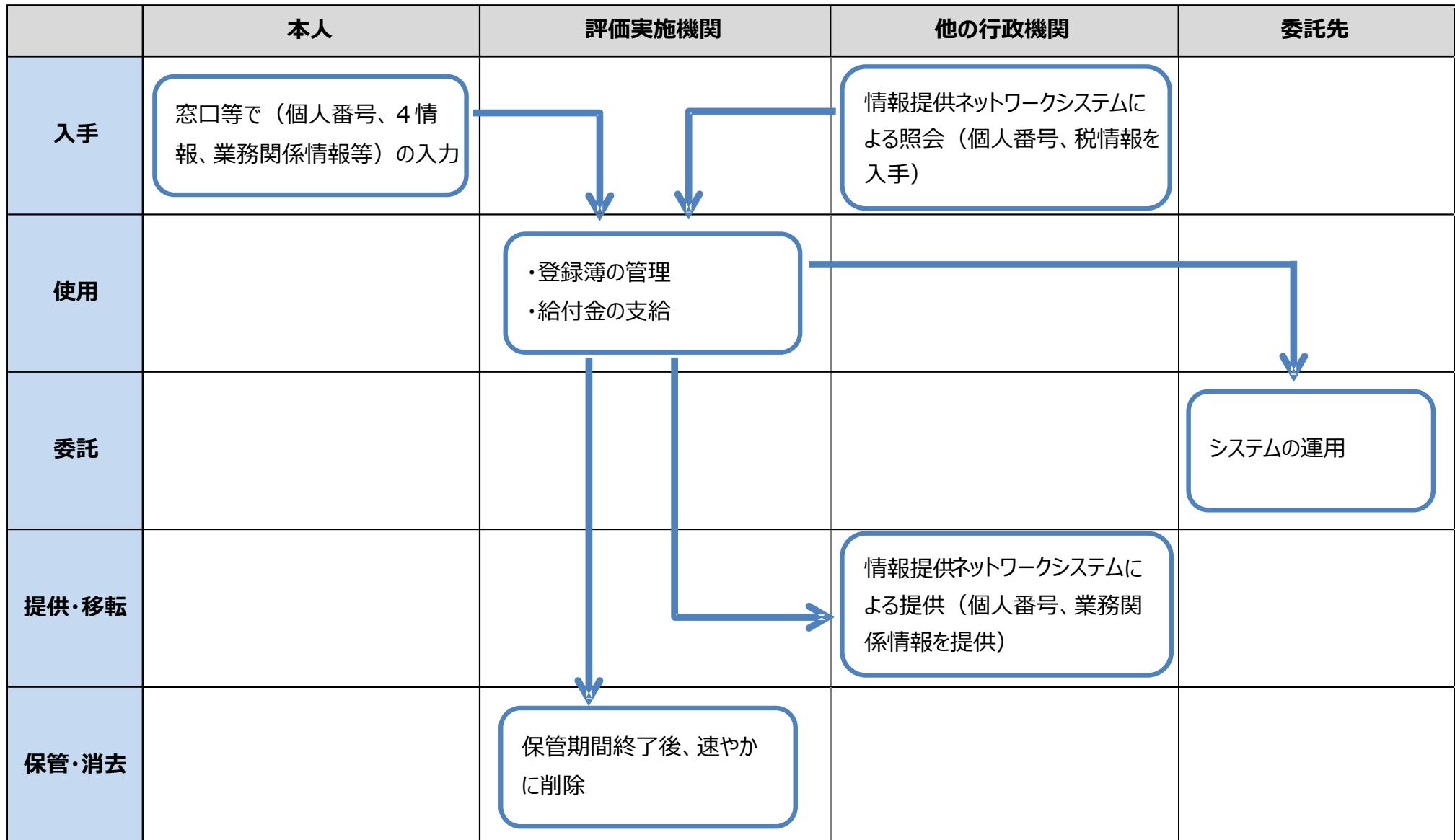
◆参照：指針「第9 特定個人情報保護評価の評価項目」

## 4. (1) 評価書の作成

1. 事前準備
2. しきい値判断
3. スケジュールの作成
4. 評価書の提出・公表
5. 評価書の提出・公表

### 事務の内容等の整理

評価書を作成する前提として、特定個人情報の取扱いを、入手、使用、委託、提供・移転、保管・消去といったプロセスごとに整理し、事務フローを可視化・詳細化しておくことが有効です。※以下の図はイメージです。



# 4. (1) ①基礎項目評価書

1. 事前  
準備

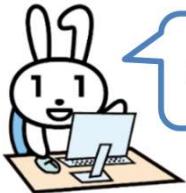
2. しきい  
値判断

3. スケ  
ジュールの  
作成

4. 評価  
書の提出・  
公表

5. 評価  
書の提出・  
公表

## 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。
- 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〕」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考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。



◆参考：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\_2\_(1) 基礎項目評価書」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）」

# 4. (1) ①基礎項目評価書

1. 事前準備

2. しきい値判断

3. スケジュールの作成

4. 評価書の提出・公表

5. 評価書の提出・公表

「IV リスク対策」において  
「2) 十分である」を選択できる水準



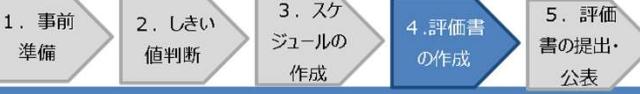
基礎項目評価書中「IV リスク対策」において記載する特定個人情報を保護するための主要な措置の実施状況の評価について、「2) 十分である」等を選択できる具体的な水準を、特定個人情報保護評価指針の解説等（記載要領及び評価書様式）に掲載しています。

## 「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ありません。
- **組織的・人的安全管理措置**については記載していませんが、**マイナンバーGLに則り、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、漏えい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処
- 「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ると考えられます。

| 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                          | <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<br/> <b>&lt;典型的なリスク対策（例）&gt;</b></p> <p>① 対象者、必要な情報の種類、入手方法等を踏まえ、“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。</p>   |
| 3. 特定個人情報の使用                           | 目的を超えた紐付け、事務に必要なない情報との紐付け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<br/> <b>&lt;典型的なリスク対策（例）&gt;</b></p> <p>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。</p>   |
|  | 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 | <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<br/> <b>&lt;典型的なリスク対策（例）&gt;</b></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「E 物理的安全管理措置」、「F 技術的安全管理措置」等を参照。</p> <p>① ユーザ認証の管理を行っている。<br/>     ② アクセス権限の発効・失効の管理を行っている。<br/>     ③ アクセス権限の管理を行っている。<br/>     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。</p> |

# 4. (1) ①基礎項目評価書

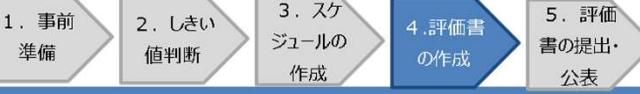


| 基礎項目評価書の項目                                   |                       | 「2）十分である」を選択できる水準  |
|--|-----------------------|--|
| 4. 特定個人情報ファイルの取扱いの委託                         | 委託先における不正な使用等のリスクへの対策 | <p>次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合<br/> <b>&lt;典型的リスク対策（例）&gt;</b></p> <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「第4－2－（1）委託の取扱い」等を参照。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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設けている。</li> <li>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。</li> </ul> |
| 5. 特定個人情報の提供・移転（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・移転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<br/> <b>&lt;典型的リスク対策（例）&gt;</b></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「E 物理的安全管理措置」、「F 技術的安全管理措置」等を参照。</p> <ul style="list-style-type: none"> <li>① 特定個人情報の提供・移転に関するルールが定められている。</li> <li>② 特定個人情報の提供・移転の記録し、その記録を一定期間保存している。</li> <li>③ 当該記録を定期に及び隨時に分析等するための体制を整備している。</li> <li>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。</li> </ul>  |
| 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    | <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<br/> <b>&lt;典型的リスク対策（例）&gt;</b></p> <ul style="list-style-type: none"> <li>① 自庁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。</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> </ul>  |



◆参考：指針の解説「第9 2 (1) 基礎項目評価書」

# 4. (1) ①基礎項目評価書

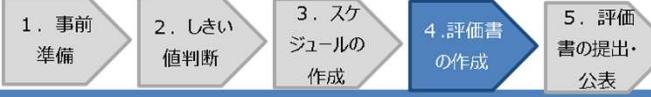


| 基礎項目評価書の項目            |                         | 「2）十分である」を選択できる水準  |
|-----------------------|-------------------------|--|
| 6. 情報提供ネットワークシステムとの接続 | 不正な提供が行われるリスクへの対策       | <p>次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合<br/> <b>&lt;典型的リスク対策（例）&gt;</b></p> <ul style="list-style-type: none"> <li>① 自庁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横断的なガイドライン」の次の留意事項等を遵守している。<br/> <b>（例）</b> <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> </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<br/> <b>&lt;典型的リスク対策（例）&gt;</b></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「E 物理的安全管理措置」、「F 技術的安全管理措置」等を参照。</p> <ul 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靭性の向上」、「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滅失・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> </ul> |



◆参照：指針の解説「第9 2 (1) 基礎項目評価書」

# 4. (1) ①基礎項目評価書

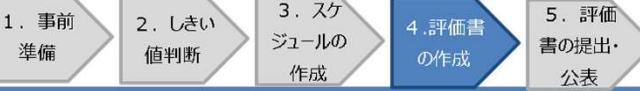


| 基礎項目評価書の項目       |                       | 「2）十分である」を選択できる水準   |
|------------------|-----------------------|---|
| 8. 人手を介在させる作業    | 人為的ミスが発生するリスクへの対策は十分か | <p>次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合<br/> <b>&lt;典型的なリスク対策（例）&gt;</b></p> <p>① 「マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドライン」の次の留意事項等を遵守している。<br/>         （例）             <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> </p> <p>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。<br/>         ※ 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>）。             <ul style="list-style-type: none"> <li>「特定個人情報を取り扱う際の注意ポイント」</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止するための着眼点—」</li> </ul> </p> |
| 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<br/> <b>&lt;典型的なリスク対策（例）&gt;</b></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> <p>① 研修計画を策定している。<br/>         ② 事務取扱者の適切な監督を行っている。<br/>         ③ 次の事務取扱者等への教育研修を行っている。             <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> <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じること。</p>  |

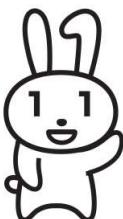


◆参照：指針の解説「第9 2 (1) 基礎項目評価書」

# 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



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。

| 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><br>1) 特に力を入れている<br>2) 十分である<br>3) 調整が残されている |  |
| 判断の根拠                 |          | (自由記述)  |  |

| 11. 最も優先度が高いと考えられる対策 |   | [ ]全項目評価又は重点項目評価を実施する |   |
|----------------------|---|-----------------------|---|
| 最も優先度が高いと考えられる対策     |   | [ ]                   |   |
|                      | <選択肢>   |                       |   |
|                      | 1) 目的外の入手が行われるリスクへの対策<br>2) 目的を超えた紐付け、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<br>3) 権限のない者によって不正に使用されるリスクへの対策<br>4) 委託先における不正な使用等のリスクへの対策<br>5) 不正な提供・移転が行われるリスクへの対策(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。)<br>6) 情報提供ネットワークシステムを通じて目的外の入手が行われるリスクへの対策<br>7) 情報提供ネットワークシステムを通じて不正な提供が行われるリスクへの対策<br>8) 特定個人情報の漏えい・滅失・毀損リスクへの対策<br>9) 従業者に対する教育・啓発 |                       |   |
| 当該対策は十分か【再掲】         |   | [ ]十分である              | <選択肢><br>1) 特に力を入れている<br>2) 十分である<br>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 | <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。</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 等</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。</p> <ul style="list-style-type: none"> <li>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。</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、施錠できる書棚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。</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 2 (1) 基礎項目評価書」

# 4. (1) ②重点項目評価書



## 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、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考箇所も掲載しています。



◆参考：指針「第9 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）」

## 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〕」を参照しつつ、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。

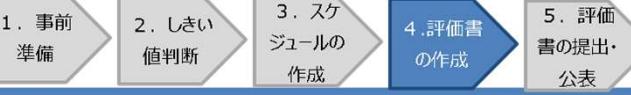


◆参考：指針「第9 2 (3) 全項目評価書」

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）」

# 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

| ユーザ認証の管理 | [ 行っている ] <選択肢> |   |           |
|----------|-----------------|---|-----------|
|          |                 | 1) 行っている  | 2) 行っていない |
| 具体的な管理方法 |                 | <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> </ul> |           |

### ■マイナンバーガイドラインの主な参考箇所及び概要 ■

#### 第4-1-(1) 個人番号の利用制限(抄)

- 個人番号は、番号法があらかじめ限定的に定めた事務以外で利用することはできない。
- 行政機関等が個人番号を利用する場合は、個人番号利用事務(番号法別表に掲げられている事務及び番号法第9条第2項に基づいて条例で規定した事務)、個人番号関係事務(職員等の社会保障及び税等に関する手続書類の作成事務)、番号法第19条第13号から第17号までに基づき特定個人情報の提供を受けた目的を達成するために必要な限度で利用する事務に限られる。

#### 第4-1-(2) 特定個人情報ファイルの作成の制限

- 個人番号利用事務等を処理するために必要な場合、又は番号法第19条第13号から第17号までのいずれかに該当して特定個人情報を提供し、又はその提供を受けることができる場合を除き、特定個人情報ファイルを作成してはならない。

#### 第4-3-(4) 収集・保管制限

- 番号法で限定的に明記された場合を除き、特定個人情報を収集又は保管してはならない。
- 番号法で限定的に明記された事務を処理する必要がなくなった場合で、文書管理に関する規程等によって定められている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廃棄又は削除しなければならない。

#### (別添1) 特定個人情報に関する安全管理措置

##### 2 講すべき安全管理措置の内容

###### C 組織的安全管理措置

###### b 取扱規程等に基づく運用

- 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时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。

###### D 人的安全管理措置

###### a 事務取扱担当者の監督

- 総括責任者及び保護責任者は、特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う。

###### b 事務取扱担当者等の教育

- 保護責任者は、部署内の事務取扱担当者等に特定個人情報の保護に関する必要な教育研修を行う。

### ■マイナンバーガイドラインの主な参考箇所及び概要 ■

(別添1) 特定個人情報に関する安全管理措置

#### 2 講すべき安全管理措置の内容

##### E 物理的安全管理措置

###### a 特定個人情報等を取り扱う区域の管理

- 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。

- 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等できないよう留意する必要がある。

- 基幹的なサーバ等の機器を設置する室等(以下「情報システム室等」という。)を区分して管理する場合は、情報システム室等について、次の①及び②に掲げる措置を講ずる。

###### ① 入退室管理

- 情報システム室等に入室する権限を有する者を定めるとともに、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の職員の立会い等の措置を講ずる。

###### ② 情報システム室等の管理

- 外部からの不正な侵入に備え、施錠装置、警報装置、監視設備の設置等の措置を講ずる。

##### F 技術的安全管理措置

###### a アクセス制御

- 情報システムを使用して個人番号利用事務等を行う場合、事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う。

###### b アクセス者の識別と認証

- 特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する。

## 4. (2) 評価書の確認

1. 事前準備

2. しきい値判断

3. スケジュールの作成

4. 評価書の提出・公表

5. 評価書の提出・公表

### 評価書の確認においてポイントとなる点（審査の観点より）



提出前に総括部署等が、評価書に記載されたリスク対策の実効性が確保されていること等を確認することを推奨します。

|                   |  |
|-------------------|--|
| ア 適合性<br>(事務的な観点) | <ul style="list-style-type: none"><li>しきい値判断に誤りはないか。</li><li>適切な実施主体が実施しているか。</li><li>公表しない部分は適切な範囲か。</li><li>適切な時期に実施しているか。</li><li>適切な方法で広く国民の意見を求め、得られた意見を十分考慮した上で必要な見直しを行っているか。</li><li>保護評価の対象となる事務の実態に基づき、評価書様式で求められる全ての項目について検討し、記載しているか。</li></ul> |
|                   | <ul style="list-style-type: none"><li>記載された保護評価の実施を担当する部署は、評価の対象となる事務を担当し、リスクを軽減させるための措置の実施に責任を負うことができるか。</li></ul>  |
|                   | <ul style="list-style-type: none"><li>保護評価の対象となる事務の内容の記載は具体的か。当該事務における特定個人情報の流れを併せて記載しているか。</li></ul>  |
|                   | <ul style="list-style-type: none"><li>特定個人情報ファイルを取り扱うプロセスにおいて特定個人情報の漏えいその他の事態を発生させるリスクを、保護評価の対象となる事務の実態に基づき、特定しているか。</li></ul>   |
|                   | <ul style="list-style-type: none"><li>特定されたリスクを軽減するために講すべき措置についての記載は具体的か。</li></ul>  |
|                   | <ul style="list-style-type: none"><li>記載されたリスクを軽減させるための措置は、個人のプライバシー等の権利利益の侵害の未然防止、国民・住民の信頼の確保という保護評価の目的に照らし、妥当なものか。</li></ul>   |
| イ 妥当性<br>(実質的な観点) | <ul style="list-style-type: none"><li>個人のプライバシー等の権利利益の保護の宣言は、国民・住民の信頼の確保という保護評価の目的に照らし、妥当なものか。</li></ul>   |

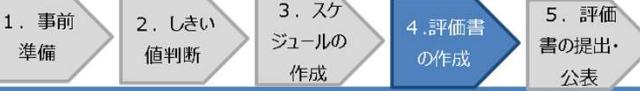
※地方公共団体等が作成する全項目評価書については、制度上の第三者点検が必須とされています。



◆参照：指針「第10 1 (2) 審査の観点」

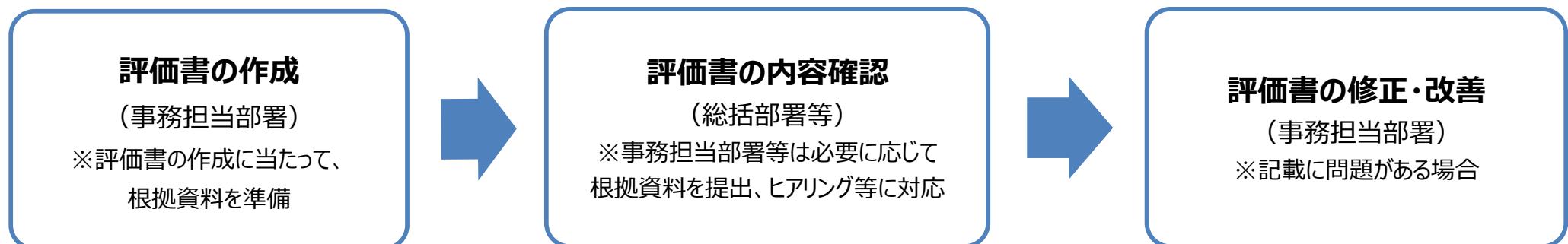
指針の解説「別添5 特定個人情報保護評価指針第10の1 (2) に定める審査の観点における主な考慮事項」

## 4. (2) 評価書の確認



- 評価書の作成に当たっては、評価書に記載したリスク対策の実効性を担保するために、記載内容を裏付ける根拠資料を準備しておくことが望ましいです。
- また、確認の際にも、保護評価の対象事務の実態を把握するために、根拠資料を収集・整理することを推奨します。

### 根拠資料の活用方法（イメージ）



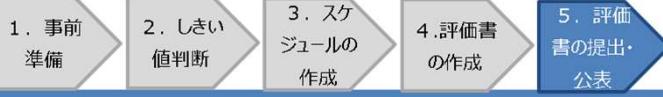
根拠となる資料としては、事務やシステムの運用ルール等に関する文書（特定個人情報取扱規程・手順書、要件定義書等）が挙げられます。

※保護評価の再実施等（P.28）の際には、運用ルールを遵守して事務を行っているか、評価書に記載したリスク対策が効果的に実施できているかを確認する手段として、各種記録（申請書、管理台帳、記録、ログ等）を活用することが考えられます。



◆参照：指針「第9 1 基本的な考え方」

# 5. 評価書の提出・公表



## 提出・公表の時期

- 行政機関等（※）は、基礎項目評価書及び重点項目評価書については、委員会に提出後速やかに、全項目評価書については、委員会の承認後速やかに公表することとなっています。
- 地方公共団体等は、評価書を委員会に提出後速やかに公表することとなっています。

※ このスライドにおける「行政機関等」とは、地方公共団体等以外の評価実施機関をいいます。

## 提出・公表の方法

- 評価書の委員会への提出及び公表作業は、マイナンバー保護評価システムから行います。
- 評価実施機関として、当該システムを初めて利用する際には、ユーザの事前登録が必要となるため、委員会事務局へ御連絡ください。
- マイナンバー保護評価システムの具体的な手続方法は、当該システム上に掲載しているシステム操作説明書を御確認ください。



公表された評価書は、マイナンバー保護評価書検索  
(<https://www.ppc.go.jp/mynumber/evaluationSearch/>) から検索・閲覧  
できます。

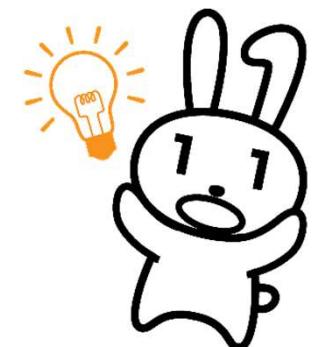


◆参照：指針「第5 3 特定個人情報保護評価書」

## II .評価書公表後の対応

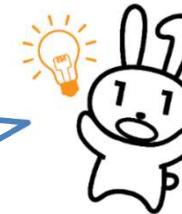
---

公表後の対応  
保護評価を実施した事務をやめたとき



# 公表後の対応

評価書の公表後、「重要な変更」、しきい値判断結果の変更又は一定期間経過に伴い、保護評価の再実施又は評価書の修正が必要となります。



## 再実施（指針第6\_2（2）・（3））

- 特定個人情報ファイルの取扱いに「重要な変更」を加えようとする場合や、しきい値判断の結果が変わる（ランクアップする）場合は、保護評価の全ての実施手続を再実施する必要があります。

## 修正（指針第7）

- 比較的軽微な変更・変化等が生じた場合は、既に公表している評価書を修正し、委員会へ提出した上で公表してください。  
※全項目評価の場合も、国民（地方公共団体等にあっては住民等）からの意見聴取及び委員会による承認又は第三者点検は必要ありません。

## プロセスの変更時（指針第5\_5）

- 事務フローの変更などにより特定個人情報ファイルを取り扱うプロセスを変更しようとするときは、リスク対策の変更の必要性を検討してください。その上で、必要に応じて保護評価の再実施又は評価書の修正、委員会への提出及び公表を行ってください。

## 1年ごとの見直し（指針第5\_4）※努力義務

- 少なくとも1年に1回、公表した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ことを努力義務としています。

## 5年経過前の再実施（指針第6\_2（4））※努力義務

- 評価書を公表してから5年を経過する前に、保護評価を再実施することを努力義務としています。



◆参照：指針「第5\_4 特定個人情報保護評価書の見直し」、  
「第5\_5 特定個人情報ファイルを取り扱うプロセスの変更時の検討」、  
「第6\_2 新規保有時以外」、「第7 特定個人情報保護評価書の修正」  
ホームページ掲載資料「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」

# 保護評価を実施した事務をやめたとき



規則第16条等に基づき、委員会に通知する必要があります。

## 委員会への通知方法

### ① 事務の実施をやめたとき※

- 右図のように、評価書に事務の終了と明記し（詳しくは評価書の記載要領を参照）、委員会へ提出することもって、委員会への通知としています。
- 当該評価書は、事務の終了後3年間は公表することとしています。

※「事務の実施をやめたとき」とは、特定個人情報ファイルの取扱いを終了した時点（文書保存期間が終了し、当該事務に係る特定個人情報ファイルを廃棄した時点等）を指します。

### ② 事務の終了から3年が経過し、マイナンバー保護評価WEBにおける公表を終了したい場合

- マイナンバー保護評価システム上では、評価書を削除する機能がないため、当該評価書を非公表とする手続を行ってください。

#### 特定個人情報保護評価書(全項目評価書)

| 評価書番号                                    | 評価書名                  |
|--|-----------------------|
| 1  | 〇〇に関する事務【令和3年1月1日 終了】 |
| 個人のプライバシー等の権利利益の保護の宣言                    |                       |
| ～をもって、個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。 |                       |
| 特記事項                                     |                       |
| 評価実施機関名                                  |                       |
| 〇〇大臣                                     |                       |
| 個人情報保護委員会 承認日【行政機関等のみ】                   |                       |
| 〇年〇月〇日                                   |                       |
| 公表日                                      |                       |
| 〇年〇月〇日                                   |                       |



◆参照：指針「第5 6 特定個人情報保護評価を実施した事務の実施をやめたとき等の通知」

# 漏えい等事案（重大事故）が発生したとき



まずは速やかに個人情報保護委員会事務局への漏えい等報告（おおむね3～5日以内）及び本人通知を行ってください。個人情報保護委員会への報告については、個人情報保護委員会ウェブサイトに設置している報告フォーム（<https://www.ppc.go.jp/personalinfo/legal/leakAction/>）からお願いします。

## 特定個人情報に関する重大事故

- 次の定義に該当する場合は、評価の再実施（及び評価の種類の変更）が必要になる可能性があります（p.9も参照。）。

| <b>&lt;特定個人情報に関する漏えい等報告の報告対象事態&gt;</b> |   |   |                                    |   |
|--|---|---|------------------------------------|---|
|  | ※ 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第29条の4第1項及び第2項に基づく<br>特定個人情報の漏えい等に関する報告等に関する規則第2条各号のいずれかに該当する事態。 |   |                                    |   |
|  | 第1号<br>情報提供NWS等   | 第2号<br>不正の目的                                | 第3号<br>不特定多数の者に閲覧                  | 第4号<br>百人超  |
| 人数 <sup>※1</sup>                       | 1人以上  |   |                                    | 101人以上  |
| 対象事態 <sup>※2</sup>                     | 漏えい・滅失・毀損<br><br>発生したおそれがある事態を含む  | 漏えい・滅失・毀損<br>不正利用・提供<br><br>発生したおそれがある事態を含む | 不特定多数の者に閲覧<br><br>閲覧されるおそれがある事態を含む | 漏えい・滅失・毀損<br>番号法の規定に反する利用・提供<br><br>発生したおそれがある事態を含む |
| 情報                                     | 特定個人情報（高度な暗号化等の措置を講じたものを除く。）  |   |                                    |   |



## ＜特定個人情報に関する重大事故＞

特定個人情報に関する漏えい等報告の報告対象事態のうち、次の2点については、「特定個人情報に関する重大事故」に適用しないこととしている。

※1. 漏えい等が発生した特定個人情報に係る本人の数について、「重大事故」が「特に国民の懸念が強いものを捕捉するべく規定されている」ことに鑑み、「当該評価実施機関の従業者数」を除いている。

※2. 「配送事故等のうち評価実施機関等の責めに帰さない事由によるもの」については、

（ワンランク上の評価書種別で再実施を行うとしても、）リスク対策等を見直すことは難しいことから、定義から除いている。



◆ 参照：指針「第2 定義 6」

# 特定個人情報保護評価制度における重大事故との関係



特定個人情報保護評価は、個人番号利用事務等に限らず、広く特定個人情報の取扱いにおける漏えいその他の事態を発生させるリスクを分析するためのものなので、報告対象事態と重大事故該当判断は完全に一致するものではありません。

## 報告対象事態

- 対象機関【番号法第29条の4】

### 個人番号利用事務等実施者

- 対象の事務

個人番号利用事務  
個人番号関係事務

- どのような場合か

規則第2条各号に掲げる事態（個人の権利利益を害するおそれが大きいもの）

※ 行政機関等は、報告対象事態非該当であっても「漏えい等事案」に該当する場合には、ガイドラインに基づく報告を行う

## 重大事故

- 対象機関【番号法第28条、番号法第27条（保護評価指針第2の6）】

### 評価実施機関

- 対象の事務

評価実施機関が特定個人情報に関して法令に基づく安全管理措置義務を負う事務

※ 個人番号利用事務等に限らない

- どのような場合か

**規則第2条各号に掲げる事態**（個人の権利利益を害するおそれが大きいもの）に該当するもの

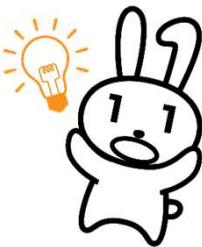
※ 漏えい等が発生した本人の数には、当該評価実施機関の従業員の数を含まない。

※ 配送事故等のうち評価実施機関の責めに帰さない事由による事態は重大事故に該当しない。



◆ 参照：指針「第2 定義 6」

# 個人情報に関する重大事故に係る対応について



個人情報に関する重大事故は、重点項目評価書と全項目評価書の記載事項であるため、該当の事案が発生した場合、評価書に追記してください。

| 7. 特定個人情報の保管・消去                        |     |  |
|--|-----|--|
| リスク： 特定個人情報の漏えい・滅失・毀損リスク               |     |  |
| ①NISC政府機関統一基準群                         | [ ] | ①事故発生時手順の策定・周知<br>[ ] <選択肢><br>1) 特に力を入れて行っている 2) 十分に行っている<br>3) 十分に行っていない |
| ②安全管理体制                                | [ ] | ②過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか<br>[ ] <選択肢><br>1) 発生あり 2) 発生なし     |
| ③安全管理規程                                | [ ] | その内容   |
| ④安全管理体制・規程の職員への周知                      | [ ] | 再発防止策の内容   |
| ⑤物理的対策                                 | [ ] | その他の措置の内容  |
| 具体的な対策の内容                              | [ ] | リスクへの対策は十分か<br>[ ] <選択肢><br>1) 特に力を入れている 2) 十分である<br>3) 課題が残されている          |
| 特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置   |     |  |
| ⑥技術的対策                                 | [ ] | 3) 十分に行っていない   |
| 具体的な対策の内容                              |     |  |
| ⑦バックアップ                                | [ ] | <選択肢><br>1) 特に力を入れて行っている 2) 十分に行っている<br>3) 十分に行っていない                       |
| ⑧事故発生時手順の策定・周知                         | [ ] | <選択肢><br>1) 特に力を入れて行っている 2) 十分に行っている<br>3) 十分に行っていない                       |
| ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか | [ ] | <選択肢><br>1) 発生あり 2) 発生なし   |
| その内容                                   |     |  |
| 再発防止策の内容                               |     |  |



◆ 参照：指針「第2 定義 6」

# 参考資料

- 特定個人情報保護評価に関する規則・指針・解説等  
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  
URL: [https://www.ppc.go.jp/files/pdf/5years\\_saijisshi\\_point.pdf](https://www.ppc.go.jp/files/pdf/5years_saijisshi_point.pdf)
- 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](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](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](https://www.ppc.go.jp/files/pdf/kansa_manual.pdf)
- 行政機関等及び地方公共団体等による特定個人情報の適正な取扱いのためのポイント～立入検査における指摘事例と着眼点～  
URL: [https://www.ppc.go.jp/files/pdf/mynumber\\_point.pdf](https://www.ppc.go.jp/files/pdf/mynumber_point.pdf)
- PIAの取組の促進について—PIAの意義と実施手順に沿った留意点—  
URL: [https://www.ppc.go.jp/files/pdf/pia\\_promotion.pdf](https://www.ppc.go.jp/files/pdf/pia_promotion.pdf)
- 特定個人情報の適正な取扱いのための各種研修資料  
URL: [https://www.ppc.go.jp/files/pdf/mynumber\\_kensyuu.pdf](https://www.ppc.go.jp/files/pdf/mynumber_kensyuu.pdf)

