



「特定個人情報保護評価」 ってどんな仕組みですか？

2015年1月
弁護士 水町雅子

講師略歴

◆ 水町 雅子 （みずまちまさこ）

弁護士（五番町法律事務所） ・ アプリケーションエンジニア
<http://www.miyauchi-law.com>
osg@miyauchi-law.com

- ◆ 富士総合研究所（現、みずほ情報総研）入社
 - ・ システム設計・開発・運用、事業企画、リサーチ等業務に従事
- ◆ 司法試験合格、法曹資格取得、第二東京弁護士会に弁護士登録
- ◆ 内閣官房社会保障改革担当室参事官補佐
 - ・ 社会保障・税番号制度立案（特に番号法立法作業、情報保護評価立案）に従事
- ◆ 特定個人情報保護委員会上席政策調査員
 - ・ 社会保障・税番号制度における個人情報保護業務に従事
- ◆ 五番町法律事務所設立、現在に至る


Agenda

1. 情報保護評価とは何か

2. 情報保護評価の仕組み

3. 情報保護評価書の構成

4. 質疑



1. 情報保護評価とは何か

情報保護評価とは

◆ 日本版プライバシー影響評価 (Privacy Impact Assessment, PIA)

- 個人情報を取り扱う制度・事務・ビジネス・ITシステム等を開始する前に、プライバシーに対して与える影響を検討するための仕組み
- マイナンバーのプライバシーに対する与える悪影響を防止・軽減するために、番号法に基づき義務付けられる制度
- マイナンバーに限られず、パーソナルデータ全般に通用する仕組み
- 番号法の中では「特定個人情報保護評価」という名称。元々は「プライバシー影響評価」として立案されたが、法律の中ではカタカナやプライバシーという言葉を使うのが難しいため、「情報保護評価」という名称に変更したものの、法案審査の過程で、「情報」全般を対象とする評価ではなく、「特定個人情報」を対象とする評価であることから、このような長い名称になったもの

情報保護評価の意義（市民にとって）

◆ 市民から見た意義

- ・ 今まではブラックボックスだった個人情報の取扱いを透明化

私の特定個人情報は誰にどのように取り扱われているの？

私の特定個人情報は何に使われるの？

私の特定個人情報は誰に提供されていくの？

私の特定個人情報はどのように管理されているの？

私の特定個人情報はちゃんと守られているの？

情報保護評価でわかること

実施側が宣言すること

1. マイナンバーを取り扱う**必要**があるので取り扱います
2. マイナンバーと共に取り扱う**必要**のある**個人情報**を取り扱います
3. マイナンバー＋個人情報を適切に取り扱うために、
各種リスク対策を事前に講じます

評価書からわかること

- どんなふうにマイナンバー＋個人情報を取り扱うの？
- どんなりスク対策を講じるの？
- 評価実施機関はプライバシー保護についてどのように取り組んでいるの？

情報保護評価の意義（実施側にとって）

◆ 評価実施機関側から見た意義

- 特定個人情報を取り扱う必要性を市民に理解してもらえる
 - ✓ 「危ない」VS「必要だ」の原理主義的論争に陥らず、具体的に説明できる
- 特定個人情報を取り扱うに当たって注意すべき点が見える
 - ✓ 職員の意識の向上
- 特定個人情報を適切に取り扱うことを市民にアピールできる
 - ✓ 取扱いの適正性を具体的にアピール
 - ✓ 「危ない」VS「必要だ」の原理主義的論争に陥らず、詳細な評価書を基に、問題点を具体的に市民と討論できる



2. 情報保護評価の仕組み

情報保護評価の義務付け対象者

義務付け対象者	具体例
行政機関の長	<ul style="list-style-type: none">総務大臣（情報提供ネットワークシステム運営事務）内閣総理大臣（マイ・ポータル運営事務）国税庁長官（国税事務）厚生労働大臣（ハローワーク、労災等）等
独立行政法人等	<ul style="list-style-type: none">日本年金機構（年金事務）日本学生支援機構（奨学金事務）等
地方公共団体情報システム機構	<ul style="list-style-type: none">個人番号とすべき番号の生成事務 等
地方公共団体の長その他の機関	<ul style="list-style-type: none">都道府県知事（住基事務、生活保護事務、地方税事務等）市町村長（住基事務、介護保険事務、児童福祉事務、地方税事務等）等
地方独立行政法人	<ul style="list-style-type: none">ほぼ該当なし
情報提供ネットワークを使用した情報連携を行う事業者	<ul style="list-style-type: none">健康保険組合（健康保険事務）

情報保護評価の対象

評価の対象

- マイナンバーの取扱い実態が明らかになるような粒度とする
⇒ **マイナンバーを取り扱う事務ごとに評価する**

評価の粒度

- 「マイナンバーを取り扱う事務」の大きさをどうするか？
 - ✓ 番号制度で1個とする → 評価は1個のみ
 - × 粒度が荒すぎる
 - ✓ 介護保険、健康保険、住基、生活保護、地方税、国税など、事務の単位ごとに評価する → 評価は事務の数だけ
 - マイナンバーを取り扱う必要性＝事務ごとに、取扱い実態を明らかにする

情報保護評価の仕組み（1）

- ◆ 義務付け対象者が実施する事務の数だけ評価がある
 - 評価の数が多すぎると...
 - ✓ × 市民からするとチェックしきれない
 - ✓ × 行政からすると評価が多すぎて雑なやつつけ評価になる
 - コストをかけてでも詳細に評価すべきものとそうともいえないものがある
 - ✓ 信頼関係があるか
 - ✓ 取扱者が多いか
 - ✓ 取扱情報に不正誘因性が高いか などなど
- ◆ メリハリのある仕組み
 - 網は広くかけつつ、評価の詳細さのレベルを分け、メリハリのある仕組みに
 - ⇒ **3段階の評価**

3段階の評価（1）

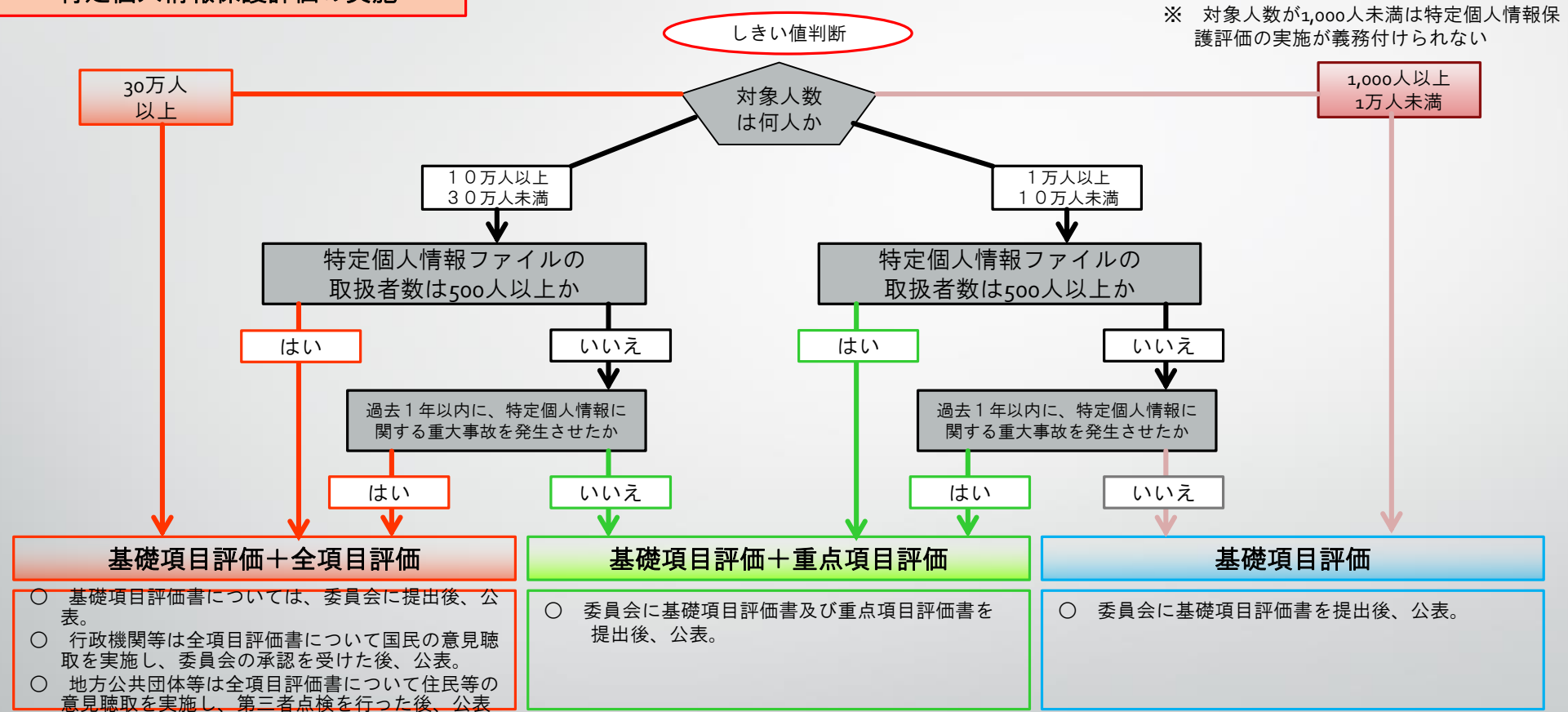
評価の振り分け

- 詳細な評価が必要かどうか、「しきい値判断」をする
- しきい値の判断基準
 - ✓ ①対象人数（∵不正誘因性）
 - ✓ ②取扱者数（∵不正誘因性）
 - ✓ ③重大事故（∵信頼関係）
- 1人のマイナンバーでもプライバシー侵害性はもちろんある
 - ✓ しかしマイナンバーを1件でも持つ以上
すべて詳細な評価をとったら、やっつけ評価になってしまう危険性。ジレンマ。
 - ✓ しかもしきい値判断は評価実施機関自身が行うので、
数や有無などの画一的判断基準にしないと、
自分に有利な評価をしているとの疑いも。

特定個人情報保護評価計画管理書

- 特定個人情報保護評価を計画的に実施し、実施状況を適切に管理するために、最初の特定個人情報保護評価を実施する前に作成する
- 特定個人情報保護評価書を委員会へ提出する際に、併せて提出する。評価書の修正等があった場合は、その都度更新し、評価書と併せて提出する。

特定個人情報保護評価の実施




















実施後に必要となる手続

- 重要な変更を加えようとするとき、特定個人情報に関する重大事故の発生等によりしきい値判断の結果が変わり新たに重点項目評価又は全項目評価を実施するものと判断されたときは、特定個人情報保護評価を再実施。
- 上記以外の変更が生じたときは、評価書を修正・公表。
- 少なくとも1年に1回は特定個人情報保護評価書の見直しを行うよう努める。
- 一定期間（5年）経過前に特定個人情報保護評価の再実施を行うよう努める。

3段階の評価（2）

評価のやり方

- しきい値判断の結果、3種類に振り分け
 - ✓ 基礎項目評価のみ
 - ✓ 基礎項目評価＋重点項目評価
 - ✓ 基礎項目評価＋全項目評価
- メリハリのある仕組み
 - ✓ 基礎項目評価：シンプルな手続＆シンプルな評価書
 - ✓ 重点項目評価：普通の手続＆普通の評価書
 - ✓ 全項目評価：丁寧な手続＆詳細な評価書

	更なる評価の 必要性	さらなる 評価 	国民の 意見 	外部第三者の 点検 	公開 
 情報保護評価 の必要性を 判断する (しきい値判断)	低い (基礎項目 評価)				 ※基礎項目評価書のみ を公開
	特に高い とはいえない (重点項目 評価)	 ※重点項目評価を 実施	 ※各機関の裁量により 意見聴取	 ※行政機関等 においては委員会	 ※基礎項目評価書、 重点項目評価書を公開
	特に高い (全項目 評価)	 ※全項目評価を実施		 ※行政機関等 においては委員会	 ※基礎項目評価書、 全項目評価書を公開

情報保護評価の継続性


◆ 情報保護評価は継続的仕組み

- ①マイナンバーを取り扱う前に評価する
- ②重要な変更があれば再評価する
- ③重要な変更がなくても1年ごとに情報が古くなっていないかチェックする（努力義務）
- ④重要な変更がなくても5年ごとに再評価する（努力義務）

◆ 既に評価済の事務でも再評価がなされる

情報保護評価の仕組み（まとめ）

- ◆ 義務付け対象者が実施する
 - ・ 行政機関の長、都道府県知事、市町村長 など
- ◆ 義務付け対象者は、マイナンバーを取り扱う事務ごとに評価する
 - ・ 年金事務、労災事務、介護保険事務、健康保険事務、住基事務 など
 - ・ 市町村長が実施する事務が多い
- ◆ メリハリのある仕組み
 - ・ 全員が同じ評価ではなく、3段階の評価制
 - ✓ 最初にしきい値判断を行い、評価のレベルを判断
 - ✓ 基礎項目評価、重点項目評価、全項目評価
 - ・ **パブコメ**の有無
 - ✓ パブコメ義務付けられるのは全項目評価
 - ✓ 基礎項目評価、重点項目評価は評価実施機関の任意の判断
 - ・ 公表の有無
 - ✓ すべて公表が義務付けられる
 - ✓ パブコメが実施されない評価についても公表された評価書をチェックできる
- ◆ 再評価義務がある



3. 情報保護評価書の構成

評価書のどこを見たらよいか


評価書の種類

- ✓ 基礎項目評価書は簡潔
- ✓ 全項目評価書がフルバージョン、重点項目評価書は全項目評価書の短縮版

どこを見たらよいか

1. 全項目評価書の“表紙”を見て何の評価かつかむ
2. 全項目評価書の“Ⅰ基本情報”を見て、概要をつかむ
3. 全項目評価書の“Ⅲリスク対策”を見て、
どのようなリスク対策を行っているか確認する

評価書には事実（取扱い実態）を踏まえてのリスク対策が記載



(1) 全項目評価書

全項目評価書

- 表紙
 - ✓ どんな評価か
- I 基本情報 … 事実
 - ✓ 評価対象の基本的情報（どんな事務？どんなシステム？）
- II 特定個人情報ファイルの概要 … 事実
 - ✓ どのように特定個人情報を取り扱うかの詳細
 - ✓ 入手・使用・委託・提供・移転・保管・消去プロセスごとの事実
- 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 … 対策
 - ✓ どのようなリスク対策を行うかの詳細
 - ✓ 入手・使用・委託・提供・移転・保管・消去ごとのリスク対策
- IV その他のリスク対策 … 対策
 - ✓ プロセスごとではない全般的な対策
- V 開示請求、問合せ
 - ✓ 開示請求等をするにはどうすればいいか
- VI 評価実施手続
 - ✓ どのように評価したか

事実（I II）を踏まえてのリスク対策（III IV）

全項目評価書

赤い詳細な評価書。パブコメ・公表が義務付け。

表紙

- 評価書名
- 個人のプライバシー等の権利利益の保護の宣言
- **特記事項 ← 力を入れている点を記載**
- 評価実施機関名
- 特定個人情報保護委員会 承認日（行政機関等のみ）
- 公表日

全項目評価書

I 基本情報

1. 特定個人情報ファイルを取り扱う事務

- どのような事務でマイナンバーを取り扱うのか。図示も。

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

- どのようなシステムでマイナンバーを取り扱うのか

3. 特定個人情報ファイル名

- どのような特定個人情報ファイルを取り扱うのか。1個か複数か。名称は。

4. 特定個人情報ファイルを取り扱う理由

- なぜ取り扱うのか。取り扱うメリットは何か。

全項目評価書

I 基本情報

5. 個人番号の利用

- 根拠条文

6. 情報提供ネットワークシステムによる情報連携

- 情報連携の有無。根拠条文。

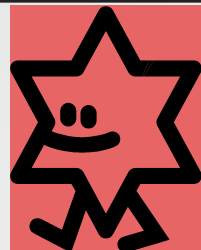
7. 評価実施機関における担当部署

- 担当部署名。所属長名。

8. 他の評価実施機関

- 表紙に出てくる以外の評価実施機関。

全項目評価書



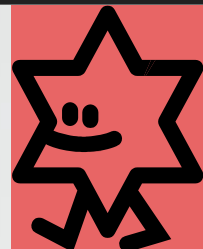
表紙のポイント

◆ 特記事項

- この事務に特有のリスクは何か。そのためにどのような対策をしているのか。
- Ex. 地方公共団体情報システム機構の評価書であれば、
 - ✓ リスク) 地方公共団体情報システム機構は、全付番対象者の個人番号とすべき番号を保有するというリスクを有している
 - ✓ 対策) そのリスク対策・不正対策として、必要最小限の情報しか保有しないこと、使用目的（利用目的）の厳格化を宣言している

リスクと対策のまとめ

全項目評価書



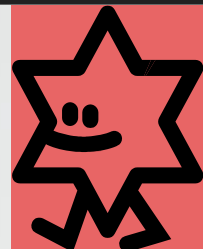
I 基本情報のポイント

1. 特定個人情報ファイルを取り扱う事務&別添1

- どのような事務でマイナンバーを取り扱うのか。今までは個人情報についてもよくわからなかったが、情報保護評価書では、文章&図示でわかりやすく説明。
- Ex. 地方公共団体情報システム機構の評価書であれば、
 - ✓ 番号制度全体に対して地方公共団体情報システム機構は何をするのか
 - ✓ 付番・住基情報の管理はどのように行われ、地方公共団体情報システム機構は何をするのか。地方公共団体情報システム機構以外に誰が関わってマイナンバーはどのように流れていくのか。

自分のマイナンバーがどのように使われるのかの見取り図

全項目評価書



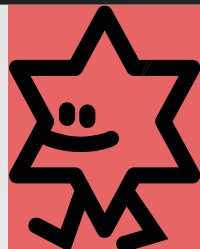
I 基本情報のポイント

4. 特定個人情報ファイルを取り扱う理由

- なぜファイルを取り扱うのか。取り扱うメリットは何か。
- 事務の流れに即して具体的に説明。
- Ex. 地方公共団体情報システム機構の評価書であれば、
 - ✓ マイナンバーを管理等するために具体的になぜファイルを取り扱うか説明。

マイナンバー&個人情報が取り扱われる理由の要約

全項目評価書



I 基本情報のポイント

4. 特定個人情報ファイルを取り扱う理由

- チェックのポイント
 - ✓ △ マイナンバーなしでもできるじゃないか
 - 合理化・システム仕様等様々な理由がある。
国会で番号法は既に成立しているので、そのような意見を言われても行政庁はいかんともしがたい場合も。
 - ✓ ○ 納得できる説明になっているか
 - なぜ取り扱われるのかが読んでわかるか。
事務の流れに即して具体的に説明されているか。

全項目評価書

Ⅱ 特定個人情報ファイルの概要

※ファイルごとに複数あり

1. 特定個人情報ファイル名

- ファイルの名前

2. 基本情報

- 手作業処理か電算処理か
- 対象人数・対象者の範囲。必要な人の情報のみ取り扱うか。
- どのような情報が取り扱われるのか。必要な情報のみ取り扱うか。
- いつから保有するか。

3. 特定個人情報の入手・使用

- 特定個人情報ファイルに記録される情報は誰からどのようにいつ入手するのか。
- 適切な入手方法といえるか。本人に入手の事実は示されるのか。
- 誰が何のためにどのように使用するのか。

全項目評価書

Ⅱ 特定個人情報ファイルの概要

※ファイルごとに複数あり

4. 特定個人情報ファイルの取扱いの委託

- 特定個人情報ファイルの取扱いを委託するか。
- どのような内容を委託するのか。どのような情報を委託するのか。適切な範囲のみ渡すのか。適切な方法で渡すのか。
- 委託先ではどれくらいの人が情報を取り扱うのか。
- 委託先はどこか。
- 再委託はするのか。

5. 特定個人情報の提供・移転（除・委託）

- 評価対象事務以外に渡すのか。提供は評価実施機関以外。移転は評価実施機関内。
- 誰に何のためにどのような範囲のどのような情報をどのような方法でいつ渡すのか。根拠条文は。

全項目評価書

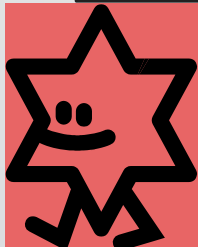
Ⅱ 特定個人情報ファイルの概要

※ファイルごとに複数あり

6. 特定個人情報の保管・消去

- どこにどれぐらいの期間保管されるのか。
- 保管期間は短すぎないか長すぎないか。
- 確実・安全な消去方法か。

全項目評価書



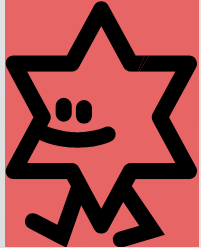
Ⅱ 特定個人情報ファイルの概要のポイント

2. 基本情報&別添2

- 誰の情報を取り扱うのか → 必要な人の情報のみ取り扱うか？
- どのような情報を取り扱うのか → 必要な情報のみ取り扱うか？
- Ex. 地方公共団体情報システム機構の評価書であれば、
 - ✓ 住民（国民＋外国人住民）の情報が取り扱われる。
 - ✓ その理由として、番号法で住民全員にマイナンバーを付番することとされているので、個人番号とすべき番号を生成・管理するために全付番対称さの情報を保有する必要があることが記載されている。

誰のどのような情報が取り扱われるか

全項目評価書



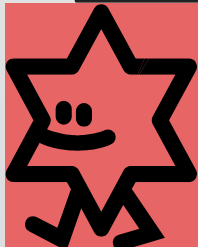
Ⅱ 特定個人情報ファイルの概要のポイント

3. 特定個人情報の入手・使用 ⑧使用方法

- 情報を誰がどのように使用するのか
- データマッチング・データマイニングをするか
→ プライバシー侵害性のある行為はないか？

情報が具体的にどのように使用されるのか

全項目評価書



Ⅱ 特定個人情報ファイルの概要のポイント

4. 特定個人情報ファイルの取扱いの委託

- チェックのポイント

- ✓ × 委託すること自体おかしい

- 合理化などの必要も考えられる。

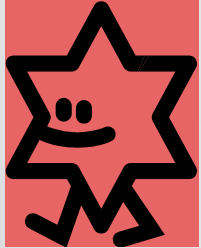
- 委託によるプライバシー権侵害のリスクをきちんと考え、

- 対策を講じているかが重要（→Ⅲのチェックへ）

- ✓ ○ 委託先がどこか確認できるか、事故があっても確認できないのか

- ✓ ○ 委託先に渡る情報は委託に必要な範囲といえるか

全項目評価書



Ⅱ 特定個人情報ファイルの概要のポイント

5. 特定個人情報の提供・移転

- チェックのポイント

- ✓ × 提供先が多すぎる

- 住基情報のように行政サービスの基礎情報は、
多くの事務に提供・移転されていく。

- 数の問題よりも、法律に基づき提供・移転しているか、

- どこに提供・移転しているかきちんと説明できているかが重要。

全項目評価書

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

※ファイルごとに複数あり

1. 特定個人情報ファイル名

- ファイルの名前

2. 特定個人情報の入手（情報提供NWSを通じた入手を除く。）

- 目的外の入手が行われるリスク
対象者以外、必要な項目以外、その他使用目的外の入手を防止するための対策
- 不適切な方法で入手が行われるリスク
入手元が使用目的を認識できるか、入手元に不必要な負担を負わせないかなど
- 入手した特定個人情報が不正確であるリスク
本人確認、マイナンバーの真正性確認、正確性確保など
- 入手の際に特定個人情報が漏えい・紛失するリスク
安全か

全項目評価書

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

※ファイルごとに複数あり

3. 特定個人情報の使用

- 目的を超えた紐付け、事務に必要なのない情報との紐付けが行われるリスク
使用目的以上に、また事務に必要なのない情報と結び付けられないための対策
- 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、アクセス権限、記録など
- 従業者が事務外で使用するリスク
内部の不正使用対策
- 特定個人情報ファイルが不正に複製されるリスク
不正複製対策

4. 特定個人情報ファイルの取扱いの委託

- 委託先（再委託先以降も含む）が適正に情報を取り扱わないリスク
体制、ルール、契約、記録など

全項目評価書

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

※ファイルごとに複数あり

5. 特定個人情報の提供・移転（委託や情報提供NWSを通じた提供を除く。）

- 不正な提供・移転が行われるリスク
記録、ルールなど
- 不適切な方法で提供・移転が行われるリスク
安全か
- 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク
誤提供・誤移転対策など

全項目評価書

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

※ファイルごとに複数あり

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
- 安全が保たれない方法によって入手が行われるリスク
- 入手した特定個人情報が不正確であるリスク
- 入手の際に特定個人情報が漏えい・紛失するリスク
- 不正な提供が行われるリスク
- 不適切な方法で提供されるリスク
- 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク

全項目評価書

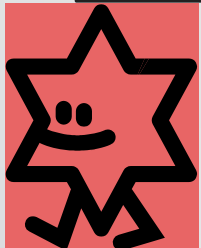
Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策

※ファイルごとに複数あり

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
NISC政府機関統一基準群、体制、規程、周知、物理的対策、技術的対策、バックアップ、事故発生時手順、過去の事故、再発防止策、死者の情報管理など
- 特定個人情報が古い情報のまま保管され続けるリスク
情報の鮮度、正確性
- 特定個人情報が消去されずいつまでも存在するリスク
消去手順など

全項目評価書

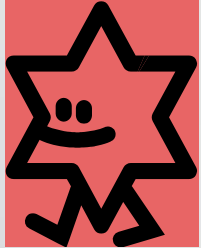


Ⅲ リスク対策のポイント

- I 基本情報 & II 概要に書かれた事実を踏まえて、Ⅲ リスク対策がある
 - ✓ Ⅲ リスク対策が重要
- 入手・使用・提供・移転・委託・情報提供NWS・保管のプロセスごとに、考えられるリスクが挙げられ、それに対する対応策が自由記述方式で記載される
- 項目に挙げられている以外のリスクはないか？
- 対策は納得できるか？

リスクを事前にきちんと想定して適切な対策を講じているか

全項目評価書



Ⅲ リスク対策のポイント

- チェックのポイント

- ✓ × 完璧なセキュリティ対策をすべき

- 完璧なセキュリティ対策がありえるのか。

リスクをきちんと考え、それに対する合理的な対策を講じているかが重要。

その機関として、リスク対策をきちんと説明できているかが重要。

全項目評価書

IV その他のリスク対策

1. 監査

- 自己点検
- 監査

2. 従業者に対する教育・啓発

3. その他

全項目評価書

V 開示請求・問い合わせ

1. 特定個人情報の開示・訂正・利用停止請求

- 請求先、請求方法、手数料等、個人情報ファイル簿など

2. 特定個人情報ファイルの取扱いに関する問合せ

- 問い合わせ窓口
- 問い合わせや苦情への対応方法

全項目評価書

VI 評価実施手続

1. 基礎項目評価

- 実施日、しきい値判断結果

2. 国民・住民等からの意見の聴取


- 方法
- 期間（短縮する場合はその理由）
- 意見の内容
- 評価書への反映結果

3. 第三者点検 ※地方公共団体のみ義務付け

- 実施日、方法、結果

4. 特定個人情報保護委員会の承認 ※行政機関等のみ

- 提出日、審査結果



(2) 基礎項目評価書

基礎項目評価書

青い簡潔な評価書。公表されるがパブコメは任意。

表紙

- 評価書名
- 個人のプライバシー等の権利利益の保護の宣言
- 特記事項
- 評価実施機関名
- 公表日

基礎項目評価書

青い簡潔な評価書。公表されるがパブコメは任意。

I 関連情報

1. 特定個人情報ファイルを取り扱う事務
2. 特定個人情報ファイル名
3. 個人番号の利用
4. 情報提供ネットワークシステムによる情報連携
5. 評価実施機関における担当部署
6. 他の評価実施機関
7. 特定個人情報の開示・訂正・利用停止請求
8. 特定個人情報ファイルの取扱いに関する問合せ

基礎項目評価書

青い簡潔な評価書。公表されるがパブコメは任意。

II しきい値判断項目

- 1 **対象人数**：評価対象の事務の対象人数は何人か
- 2 **取扱者数**：特定個人情報ファイルの取扱者数は500人以上か
- 3 **重大事故**：
過去1年以内に、評価実施機関において特定個人情報に関する重大事故が発生したか

III しきい値判断結果



4. 質疑
