

特定個人情報保護評価（PIA）

～目的・第三者点検ポイント・評価書作成ポイント～

2015/10 弁護士水町雅子

略歴

◆ 水町 雅子 （みずまちなまさこ）

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、第二東京弁護士会に弁護士登録、西村あさひ法律事務所入所
- ◆ 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、特定個人情報保護評価立案）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

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。「情報保護評価」「保護評価」「情報保護評価」「マイナンバー評価」「PIA」などと、略称が統一されていない現状。

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わかる
 - ✓ 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

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	- 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	- 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	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	- 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	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	健康保険組合（健康保険事務）

情報保護評価でわかること

実施側が宣言すること

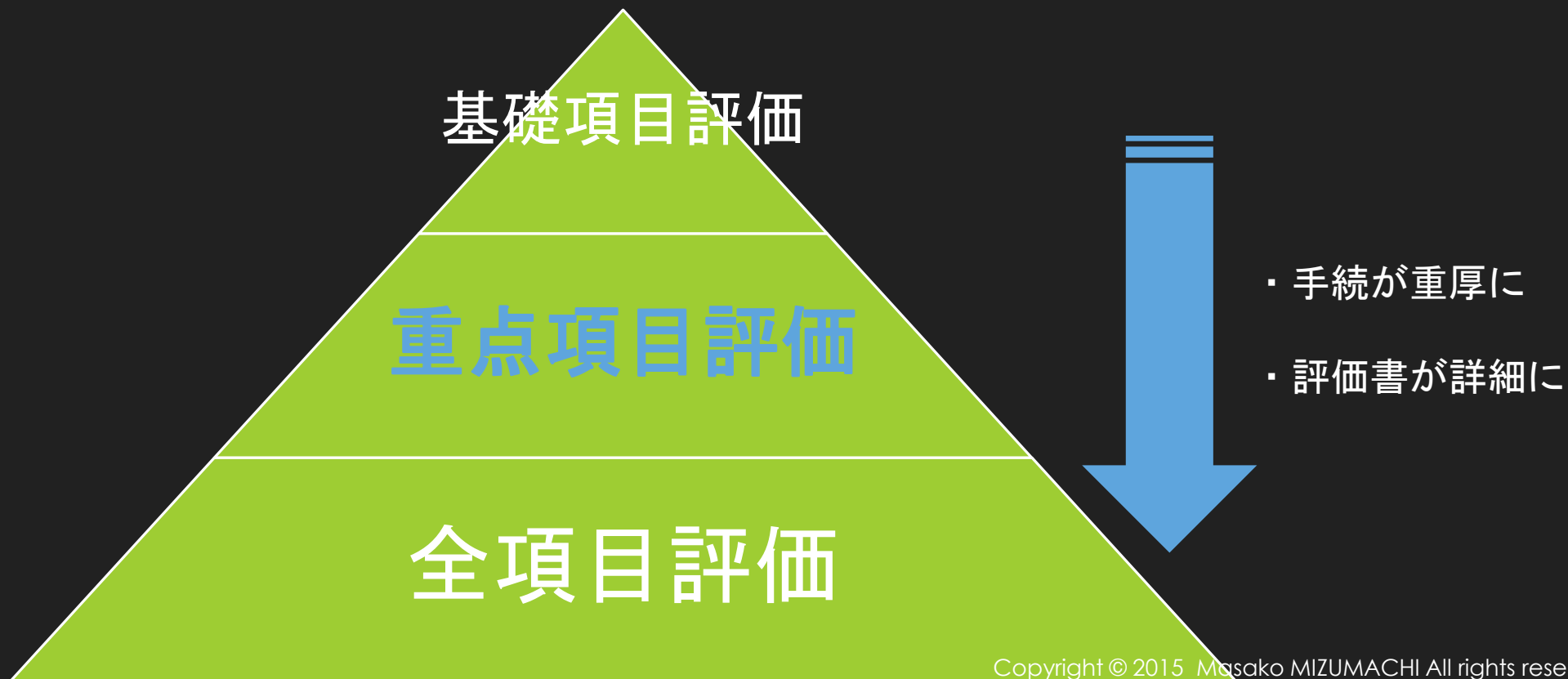
- マイナンバーを取り扱う**必要**があるので取り扱います
- マイナンバーと共に取り扱う**必要**のある**個人情報**を取り扱います
- マイナンバー＋個人情報を適切に取り扱うために、
各種リスク対策を事前に講じます

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？
- どんなリ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？

3 段階の仕組み

- しきい値判断で、評価のレベルが自動的に振り分けられる



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**

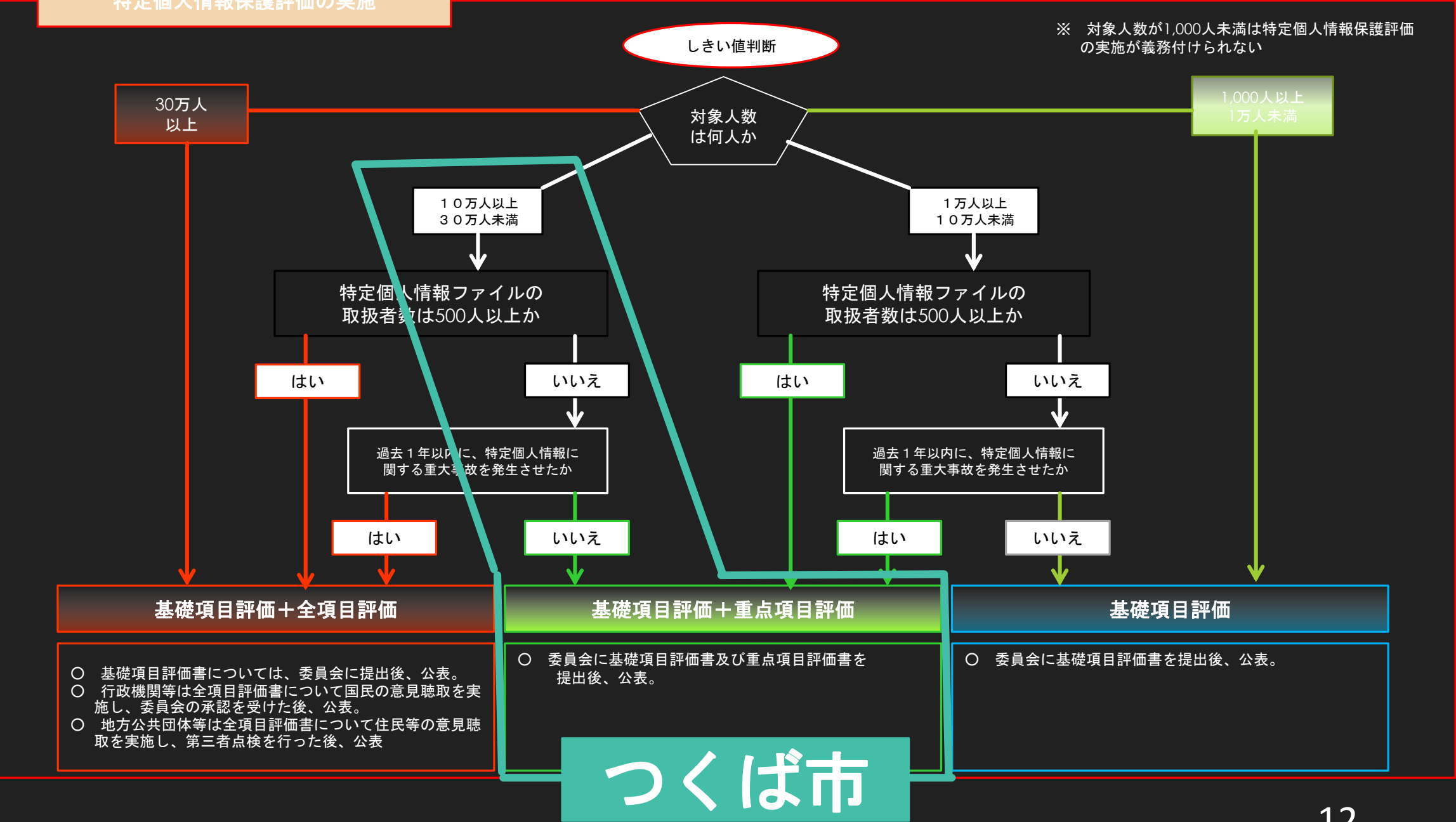
情報保護評価の仕組み（２）

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の実施

※ 対象人数が1,000人未満は特定個人情報保護評価の実施が義務付けられない



 情報保護評価 の必要性を 判断する (しきい値判断)	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 
	低い (基礎項目 評価)	✕ ※基礎項目評価のみ	✕	✕	○ ※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	△	○ ※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

つくば市は重点項目評価だが、自発的に保護充実のため、第三者点検を任意実施

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して、評価書を修正する（努力義務）
 - もっとも評価書記載事項は、首長名で市民等に向けて宣言したものであるから、情報が実態を表さなくなれば、修正がマスト。
 - 努力義務は見直し時期にかかるもの。
- 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・修正がなされる

- 再評価→すべての手順を踏む（全項目であればパブコメ・第三者点検）
- 修正→評価書を修正して公表するのみでよい

情報保護評価の仕組み（まとめ）

- ◆ 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
 - ・ 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
 - ・ **第三者点検**の有無
 - ✓ 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・修正**がある

情報保護評価でやるべきこと

- 中心は、評価書
- 評価書をブラッシュアップしていく仕組み
 - パブコメ、第三者点検によって得られた意見をもとにブラッシュアップ
 - パブコメや第三者点検で提出されなかった意見、又はパブコメや第三者点検を実施しない場合でも、評価書を公表することで、市民等からの反応が考えられる。その反応・意見によって、評価書をブラッシュアップ。
 - 再評価・修正によって、継続的にブラッシュアップ

2. 第三者点検のポイント

第三者点検の趣旨

外部者のチェック

- 情報保護評価は自己評価ではあるが、自己評価だからといっておざなりな評価であったり、評価実施機関にとって都合の良い評価であったりしては決してならない
- 自己評価であるのは、自らプライバシー・リスクを想定し、対策を講じることを目的としたものであって、安易な評価を量産するためではない
- そこで、外部者が点検することで、情報保護評価が適切に実施されることを担保する

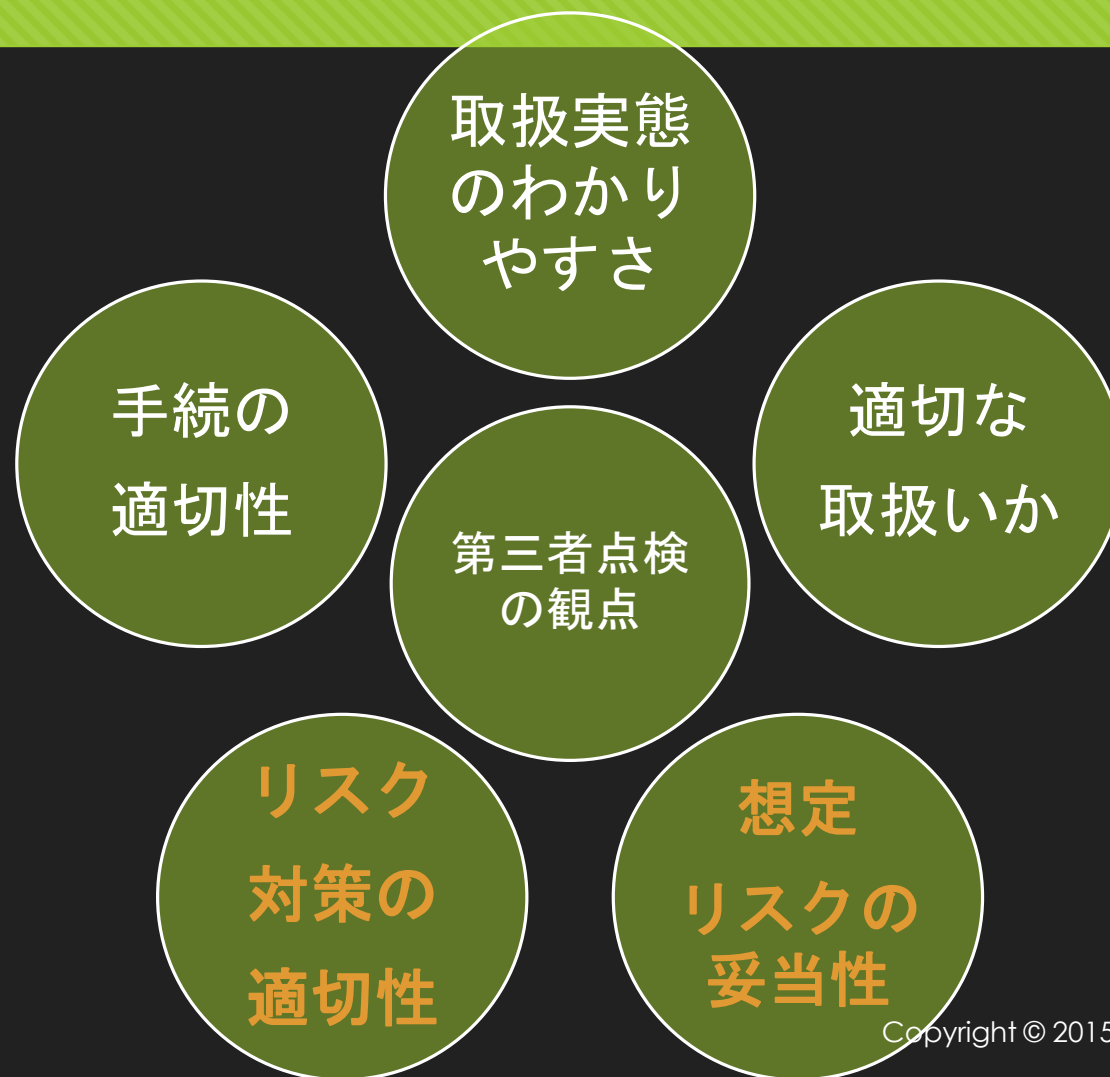
専門的知見の獲得

- 情報保護評価ではプライバシー・リスクを想定しその対策を検討するが、プライバシーの考え方、対策の考え方等において、専門家の観点を入れることで、より適切なプライバシー保護を目指す

方法

- 原則として、個人情報保護審査会・審議会。それ以外には、個人情報保護・セキュリティの専門家の意見聴取でもよい。

第三者点検の5つの観点



- 情報保護評価に関し
広く意見を述べる
ことができるものの、
主な意見の観点は
5点に大別される

1. 取扱実態のわかりやすさ

ポイント

- 一般人の視点で、「私の個人情報がどのようになぜ取り扱われるのか」がわかりやすく示されているか、情報保護評価書のⅠⅡを見て確認
- 第三者点検は実地監査ではない。実際の事務状況を逐一確認し、情報保護評価書に記載された通りの実態となるかどうかを監査することは、求められていない。情報保護評価書を読んで、論理的矛盾がないか確認するなどする。

点検の観点

- 個人情報の流れ（全体的な流れのほか、どこからどのように入手して、どのように誰が使用し、誰に委託され、誰に提供・移転され、どのように保管・消去されるか）が理解できるよう説明されているか
 - この点は、国民・一般の意見聴取プロセスで重点的に点検される。しかし重点項目評価では国民・一般の意見聴取は義務付けられず、また任意に実施しても、現実の実務を踏まえると、あまり意見が提出されないこともあるため、第三者点検においても点検する。
- 個人情報の取扱いの説明に誤りがないか、確認してもよい。例えば、事務を遂行するのに、評価書に記載されている対象者の範囲では狭すぎる場合等は、誤りでないか評価実施機関に確認する。

2. 適切な取扱いか

ポイント

- 「個人情報をおのように取り扱う理由などを合理的に説明できているか」、情報保護評価書のⅠⅡを見て確認

点検の観点

- まず、情報保護評価書に記載したような取扱いをする必要性が、合理的に説明できているか
 - 例えば、その範囲の個人情報を取り扱う必要があるか（評価書Ⅱ 2③）、その個人情報の項目を取り扱う必要があるか（評価書Ⅱ 2④）
 - 説明を読んで、一般人の視点に立って納得できる程度に合理的か
- 個人情報の取扱いがプライバシー等へ与える影響度合いはどの程度か
 - 必要性が低かったり影響が大きい場合は、代替策があれば代替策を立て、代替策がない場合は取扱いをやめるか、リスク対策を厚く講じるべき
- 但し、プライバシーへの影響が大きい場合でも、取扱いをやめたり、代替策を立てることが困難なときも
 - 取扱い中止・変更が必須とされるわけではない←プライバシー以外の権利保護のために必要な場合も
 - そのような場合は、リスク対策を厚くする等、個人情報を取り扱う必要性とプライバシーに与える影響とを比較考量し、適切な取扱いを図っていく。

3. 想定リスクの妥当性

○ 第三者点検の中心部分の一つ

ポイント

- 当該事務で自分の個人情報を取り扱われることで、何を**脅威**に感じるか
- 情報保護評価書のⅢを見て、既に挙げられているもの（**典型リスク**）以外にリスクはないのか検討

点検の観点

- 脅威の例
 - 住民税：正確な情報か（→税額が誤ったりしないか）、みだりに他人に自分の収入を知られないか、みだりに他人の自分の勤務先を知られないか
- 典型リスクも含め、リスク高低を検討するとさらに良い
 - プライバシーへの影響・リスクが大きいものは、リスク対策の適切性の観点から十分なチェックを行う
- 評価実施機関は日々遂行している事務のことなので、プライバシー・リスクを見落とすことも
 - 専門家でない一般人の視点で、自分の個人情報が取り扱われることで何が不安なのか、脅威なのか
 - さらに専門家の視点から、想定されるリスクが他にないのか、リスクの高低はどの程度か

4. リスク対策の適切性

- 第三者点検の中心部分の一つ
- 合理的説明ができていますか
 - 情報保護評価書のⅢⅣ（重点項目評価書はⅢのみ）を見て、リスクへの対策として合理的な説明となっているかを確認
 - 最低限、日本語としてリスクと対策がかみ合い、かつその対策によってリスクを防止できることを、一般人が納得できること
 - × 個人情報情報を過剰に入手してしまうリスクに対し、「個人情報情報を暗号化する」等といった対策
 - ← リスクと対策がかみ合っていない。個人情報情報を暗号化しても、不必要な個人情報情報を入手しないようにはならない
 - × 漏えい・紛失リスクに対し、「安全性が担保されているシステムを使用する」といった記載
 - ← なぜそのシステムが安全性を担保されているといえるのかが明らかではない。またトートロジーに陥ったリスク対策も見られる。
- リスクレベルに応じた対策か
 - 情報保護評価書のⅢⅣ（重点項目評価書はⅢのみ）を見て、リスクレベルに応じた対策となっているかを確認
 - プライバシーへの影響・リスクが大きいものについては、十分な対策がとられているか
 - リスク対策が現在の水準と合致しているか確認することも考えられる
 - 特に、専門的知見を要する観点！
- リスク対策として良い点があれば、その旨を意見するのもよい
 - 行政を批判することは当然重要だが、良い点があれば認めることも、行政側のモチベーションにつながったり、他の評価実施機関の手本になる等、良い効果が期待

5. 手続の適切性

- しきい値判断
 - 判断結果に謝りがないか
 - しきい値判断項目の事実認定に誤りがないか
 - 数値のカウント方法を確認する
 - 重大事故の有無。評価実施対象事務と無関係でも評価実施機関が発生させた重大事故であれば、「有」。帰責性のない事故は除外可だが、身びいきになっていないか
- 情報保護評価書の非公表箇所は妥当か
 - 情報保護評価書に求められる透明性を重視し、真に公表することでリスクがある場合のみ、また公表することでリスクがある部分に限って、非公表とすべき。記載のレベルを抽象化しても、情報保護評価の趣旨を体現でき、かつ記載のレベルを抽象化すれば公表できるのであれば、そのように評価書を改めることも検討すべき。記載のうちの一部のみを非公表とすれば足りるのであれば、当該一部のみを墨塗りするなどの措置をとるべき。
- 国民・一般の意見聴取手続の適切性
 - 聴取期間が適切か、形式的に手続を経ただけではないか、得られた意見のうち評価書に反映すべき点を反映しているか、得られた意見のうち評価実施機関の考え方を回答すべきものに回答しているか等
- しきい値判断結果以外は、国民・一般は確認できない点なので、第三者点検での確認が重要

3. 情報保護評価書のポイント

重点項目評価書・全項目評価書の構成

- 表紙
 - ✓ どんな評価か
- I 基本情報
 - ✓ 評価対象の基本的情報（どんな事務？どんなシステム？） **事実**
- II 特定個人情報ファイルの概要
 - ✓ 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 **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
 - ✓ 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 **対策**
- IV その他のリスク対策 …重点項目評価ではなし
 - ✓ プロセスごとではない全般的な対策 **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 **手続等**
- VI 評価実施手続
 - ✓ どのように評価したか **手続等**

事実（I II）を踏まえてのリスク対策（III IV）

該当箇所		内容	わかること
表紙		・評価書名、評価実施機関名 ・特記事項	・誰の何に対する評価か ・力を入れている対策
I	別添 1	・事務の内容	・自分のマイナンバーがどのように取り扱われるかの見取り図
II	2 ③	・対象となる本人の範囲、その必要性	・誰のマイナンバーがなぜ取り扱われるか
	2 ④、別添 2	・記録される項目、主な記録項目、その妥当性、すべての記録項目	・マイナンバーと共にどのような情報が取り扱われるか
	3 ⑧	・使用方法、情報の突合、情報の統計分析、権利利益に影響を与え得る決定	・マイナンバーが具体的にどのように使用されるか
	4	・委託事項、委託先名、再委託の有無等	・マイナンバーの取扱いがどこに委託されるか
III	2 リスク 1	・目的外の入手が行われるリスク	・マイナンバー情報を過剰に入手しないための対策としてどのような措置がとられるか
	2 リスク 3	・入手した特定個人情報が不正確であるリスク	・本人確認がどのように行われるか等
	3 リスク 1	・目的を超えた紐づけ、事務に必要なない情報との紐づけが行われるリスク	・マイナンバーが必要のない情報と過剰に紐づかないための対策としてはどのような措置がとられるか
	3 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	・業務に必要なくマイナンバーが利用されないための対策としてどのような措置がとられるか
	4	・特定個人情報ファイルの取扱いの委託	・委託先においてマイナンバーが適切に取り扱われるための対策としてどのような措置がとられるか
	5 リスク 1	・不正な提供・移転が行われるリスク	・マイナンバー情報が不正に提供・移転されないための対策としてどのような措置がとられるか
	6	・情報提供ネットワークシステムとの接続	・情報提供ネットワークシステムを通して不正な提供が行われないための対策としてどのような措置がとられるか
	7 リスク 3	・特定個人情報が消去されずいつまでも存在するリスク	・マイナンバー情報が適切に廃棄されるための対策としてどのような措置がとられるか
VI	2 ④⑤	・国民・住民等からの意見の聴取の主な意見の内容、評価書への反映	・評価書案に対し国民からどのような意見が提出され、それをどのように評価書に反映したのか
	3 ③	・第三者点検の結果＜自治体のみ＞	・自治体から独立した第三者専門家がこの評価書についてどのような点検を行い、どのような意見が出されたか
	4 ②	・特定個人情報保護委員会による審査＜自治体以外＞	・特定個人情報保護委員会でこの評価書についてどのような審査が行われ、どのような意見が出されたか

1. どういう業務か説明しよう

- 業務の全体像をわかりやすく平易に説明しよう
 - ✓ 市民・消費者に向けての説明をイメージ
 - ✓ 市民・消費者は、行政内部・企業内部の者とは違い、どのような業務なのかが全く分からない場合も多い。行政内部・企業内部にとっては当然のことであっても、外部から見たらわからない。
 - ✓ たとえるなら、この業務に新しく加わった従業員（新人・異動者）に説明するように、全体像をわかりやすく説明する。
- さらに、業務の全体像の中での個人情報の流れを追記しよう
- できれば図にするとよい。難しいようであれば平易な文章で。

→ 重点項目評価書Ⅰ 1②・全項目評価書Ⅰ 1②別添1に記載する

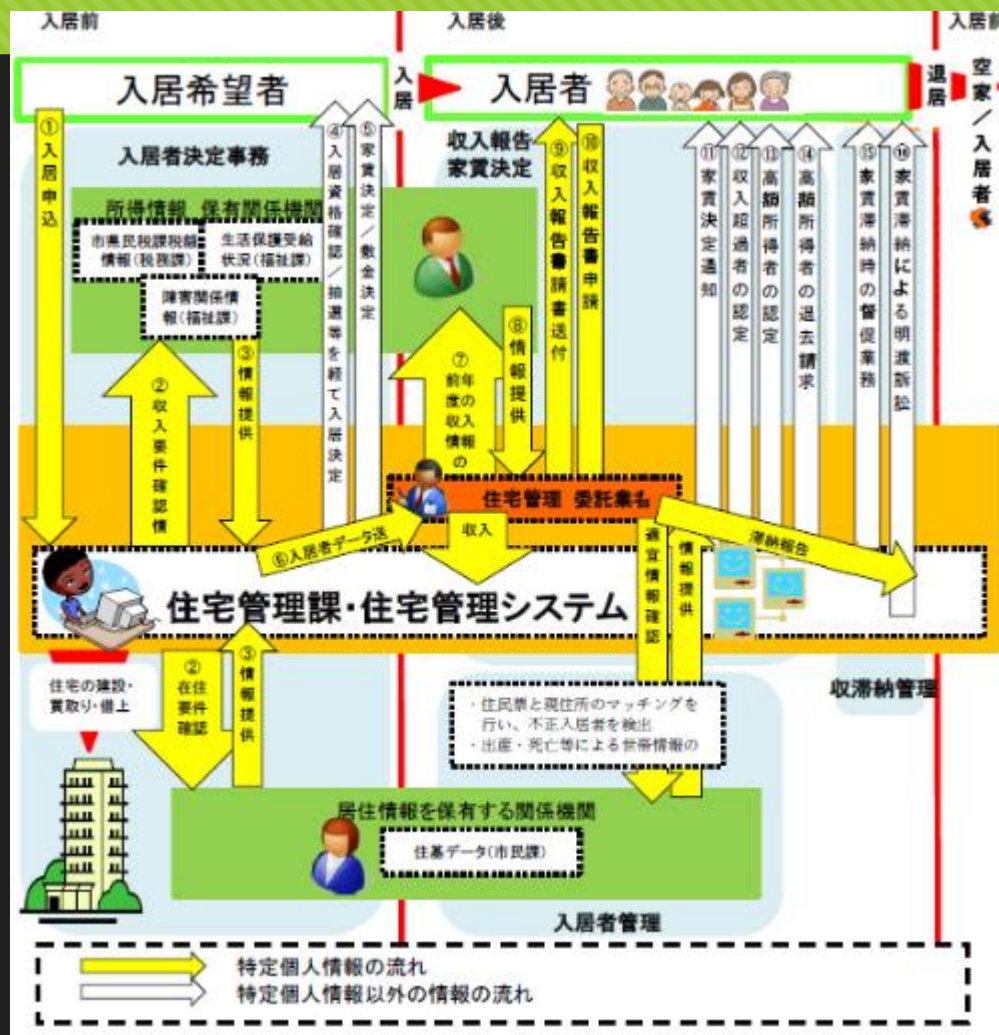
1. どういう業務か説明しよう（例）

○ 文章の例（イメージ）

- 目的：乳幼児医療費助成：経済的負担を心配しなくてもお子さんが病気などを治療できるよう、〇才未満のお子さん*1の医療費等*2のうち保護者等が負担しなければならない分を、市で助成します。
- 概要：当市では、出生届を受け取ったら、保護者等に申請を促します。保護者等の申請を受け付けたら、助成対象外*1に当たらないか当市で確認し、医療証を発行します。保護者等は病院の窓口等で医療証・健康保険証を提示の上、診療等を受けます。そうすると保険外等の、対象外となる医療費等*2を除き、保護者等は自己負担がなくなります。当市では、病院等から請求を受け、病院等へ対象額を支払います*3。
- *1～3：例外や、審査・支払機関等の点は、注記するとわかりやすくなる可能性。注記とせず、本文に書いてもよいが、正確に記載しようとして例外の解説が多すぎると、わかりにくくなるので、留意する。

1. どういう業務が説明しよう（例）

○ 絵の例（イメージ）



2. 個人情報はどう取り扱うか説明しよう

- 業務の中で個人情報をどう取り扱うか、平易に説明しよう
 - ✓ 市民・消費者に向けての説明をイメージ
 - ✓ 市民・消費者からすれば、誰の個人情報が何のためにどのように使われるかわからない。行政内部・企業内部にとっては当然のことであっても、外部から見たらわからない。

→ 重点項目評価書Ⅱ 2③④ 3⑤ ・ 全項目評価書Ⅱ 2③④ 3⑧に記載

2. 個人情報はどう取り扱うか説明しよう（例）

○ 例（イメージ）

○ 誰の個人情報：当市在住の○才未満のお子さん、保護者、過去の対象者*1

- *1 ○才以上になったお子さんと保護者の個人情報についても、過去△年分の情報を保存しています。

○ どんな個人情報：

- 主な記録項目：個人番号、4 情報（氏名・住所・性別・生年月日）、連絡先、その他住民票関係情報、医療保険関係情報、児童福祉・子育て関係情報・生活保護・社会福祉関係情報、障害者福祉関係情報

- 全ての記録項目：○○関係情報とある点を、もっと具体的に記載する

○ どう使用するのか：

○ 医療証関係

- 出生届を受け取ったら、保護者等の住所宛に乳幼児医療費助成について申請を促す連絡をする
- 申請を受け付けたら、助成対象外*1に当たらないか○、△、□情報を元に当市で確認し、医療証を発行する
- ○○の時に、医療証を再発行する
- ○○の時に、医療証を更新する
- 転出届を受け取ったら、・・・

3. 委託について説明しよう

- 委託先に個人情報を取り扱わせるか、平易に説明しよう
 - ✓ 評価実施機関以外に、誰が個人情報を取り扱うのかを説明する。

→ 重点項目評価書Ⅱ 4 ・ 全項目評価書Ⅱ 4 に記載

- 例（イメージ）
 - 何を委託するのか：システム運用・保守
 - 乳幼児医療費助成システムの運用・保守を委託
 - どこに委託するのか：
 - Aシステム会社
 - 再委託するのか
 - 再委託は禁止 OR 再委託先の条件はこれこれ

4. 目的外入手リスク対策について説明しよう

どんなリスク？

- 利用目的の達成に不必要・不相当な個人情報を入手しないよう、どのような対策を講じるかを説明する
 - 過剰入手とも表現できる
 - 利用目的の範囲外の個人情報を入手してしまうと、そもそも何のためにそのような個人情報を保有するのか疑問であるし、悪用されるリスクも高まる。
 - 例えば、デモのための道路使用申請の際に、生活保護を受給しているか聞くことは、利用目的（道路使用許可）の範囲外であるし、プライバシー侵害に当たりうる。
 - 網羅的・探索的に個人情報を入手する場合や、利用目的や入手経路、対象者の範囲が十分に特定されていない場合に特に問題になる。
 - まずは前提として、使用目的（Ⅱ 4 ⑥）、使用方法（Ⅱ 4 ⑧）、入手元（Ⅱ 3 ①）、入手方法（Ⅱ 3 ②）、入手の時期・頻度（Ⅱ 3 ③）が明らかになっているか。次に人と情報の両面から対策。

→ 重点項目評価書Ⅲ 2 ・全項目評価書Ⅲ 2 リスク 1 に記載

4. 目的外入手リスク対策について説明しよう

対策

(1) 必要な人以外から入手しないように

- 後期高齢者医療事務で仮に「65才以上の住民」を対象者とするのであれば*1、評価書の記載を読めば、なぜ「65歳以上の住民」の個人情報を必要とするのかがわかるようになっているか。
- 次に、誰がどのようにして「65才以上の住民」に該当する者を洗い出すのか、どうやって特定個人情報を入手するのか、その際、それ以外の者の個人情報を入手するリスクを防止するためにどのような対策がとられているか。
- 例えば住民基本台帳で生年月日を調査し、65歳以上の住民の特定個人情報を、システム上抽出して入手するのであれば、間違いは少ないものと考えられる。
- *1 後期高齢者医療事務では、実際には、「65才以上の住民」以外も対象者とするが、ここでは説明のために単純化して記載している。

4. 目的外入手リスク対策について説明しよう

対策

(2) 必要な個人情報以外を入手しないように

- 保有する項目は記録項目（Ⅱ 2 ④・別添 2）に示す。まずは、その項目をなぜ必要とするかが説明（Ⅱ 2 ④「その妥当性」）する。
- 入手項目をシステムで限定したりダブルチェックする等、必要な個人情報以外を入手してしまうリスクに対し、どのような対策を講じるか。

(3) その他の観点からの対策があれば記載

- 人、情報以外にも、目的外入手を防止するための対策があれば記載する。

5. 過剰紐づけ対策について説明しよう

どんなリスク？

- 目的を超えた紐づけ、事務に必要なのない情報との紐づけが行われないう、どのような対策を講じるかを説明する
- 個人情報 が過剰に集約・使用されてしまうと、対象者について、業務に必要な範囲を超えて情報を得ることができ、人のプライバシーを不正に暴いてしまう恐れがある。個人情報 が、使用目的を超えて取り扱われないう、また、業務に必要なのない情報と併せて取り扱われないう、合理的な対策が講じられるか、システムと人の操作の両面から評価する。
- 例えば、乳幼児医療費助成の担当者が、乳幼児医療費助成の対象者以外の住民の個人情報を見られるようになっていないか。道路の使用許可をする担当者が、申請者がどのような家族関係で、どのような持病があつて、所得額がいくらかみられるようになっていないか、など。

→ 重点項目評価書Ⅲ 3 リスク 1 ・全項目評価書Ⅲ 3 リスク 1 に記載

5. 過剰紐づけ対策について説明しよう

対策

(1) システムで適切な制御がなされているか

- システム間ではさまざまな接続／連携がなされており、適切な制御をしなければ、別々のシステムで保有されている個人情報全てを紐づけ・参照等することもできてしまう。
- 特に、さまざまな事務で共通基盤として用いられているようなシステムでは、一つの事務に必要な情報以外のさまざまな範囲の情報を保有することが考えられる。共通システムではない個別システムであっても、過剰紐づけ・参照等のリスクがある。
- 共通システム、個別システムともに、当該事務に必要な情報のみアクセスできるよう、どのような制御がなされているか、説明する。
- 特定個人情報については、特に、業務上不要な個人番号にアクセスできないようになっているかも、十分説目する。

(2) 人が過剰紐づけしないよう対策がされているか

- システム上で適切な制御がなされていても、職員がさまざまな権限を悪用して、業務と無関係な個人情報を手動で集めてしまうリスクもある。そのようなリスクを防止するためにどのような対策がとられるか。

6. 無権限者使用対策について説明しよう

どんなリスク？

- 個人情報を取り扱うことが必要な者以外には、原則として個人情報を使用させてはならない。また、退職者・異動者のように、かつては特定個人情報を取り扱う必要があったが今はない者についても、個人情報を使用できないようにする必要がある。さらに、内部者だけではなく、外部者（市役所窓口を訪れた一般人、無関係のクラッカー）についても同様に、他人の個人情報を使用できないようにする必要がある。そこで、個人情報を使用できる者を特定した上で、特定された者のみ個人情報を使用できるようになっていることを具体的に説明する。
- 例えば、個人の所得額を、地方税担当職員・生活保護担当職員が見るのは業務上必要であると思われるが、個人の所得額を業務上知る必要のない者が所得額にアクセスできないよう、どのような対策を講じているのか。

→ 重点項目評価書Ⅲ 3 リスク 2・全項目評価書Ⅲ 3 リスク 2に記載

6. 無権限者使用対策について説明しよう

対策

(1) システム面での対策

- システムの場合は、ユーザ認証を行い、アクセス権限の発効・失効を適切に実施し、アクセス権限を管理すること、使用記録を取得・監査すること等が考えられる。
- 全項目評価書には、「ユーザ認証の管理」「アクセス権限の発効・失効の管理」「アクセス権限の管理」「特定個人情報の使用の記録」欄が設けられているので、これらを具体的に説明し、無権限者が個人情報を使用できないようにしていることを説明する。

○

(2) システム外での対策

- 書面の場合も、施錠管理等で、個人情報を使用できる者を特定した上で、特定された者のみ個人情報を使用できることなどを、具体的に説明する。

7. 委託先の不正対策について説明しよう

どんなリスク？

- 委託先に特定個人情報を取り扱わせると、委託元で取り扱う場合と比べ、特定個人情報を取り扱われる本人からは予期できなかったり、委託元の監督が及びにくいことが考えられる。そこで、委託先が特定個人情報を適切に取り扱うことを、委託元がどのようにして確認・担保しているかが、具体的かつ合理的に説明されているか説明する。
- どんなに自治体内では厳格な取扱いをしても、委託先（指定管理者）でずさんな扱いをされてしまったり、不適切である。例えば、指定管理者に特定個人情報を取り扱わせている場合、指定管理者にどのようなことを守らせ、指定管理者を自治体として監督しているか。
- 全項目評価書では、対策として、①情報保護管理体制の確認、②閲覧者・更新者の制限、③取扱記録、④ルール策定、⑤ルール遵守確認、⑥契約、⑦再委託の7点が、すでに欄として設けられている。重点項目では、⑥契約、⑦再委託が、欄として設けられている。
 - いずれも重要な対策であるが、特に⑥契約、⑦再委託がポイントとなる。
 - 重点項目評価書では、全項目評価書の①から⑦を参考に、さらに対策を記載してもよい。

→ 重点項目評価書Ⅲ 4・全項目評価書Ⅲ 4に記載

7. 委託先の不正対策について説明しよう

対策

○ ⑥契約

- 委託先と締結する委託契約において、特定個人情報の取扱いに関してどのような定めを置いているか
- 例えば、目的外利用の禁止、特定個人情報の閲覧者・更新者の制限、特定個人情報の提供先の限定、情報漏洩等を防ぐための保管責任、情報の返還・消去措置、特定個人情報の取扱いに関する定期的な点検・報告、委託先に対する視察・監査、委託契約終了後の特定個人情報の取扱い、再委託の取決め等。
- 委託先に法律やガイドラインを遵守させることは当然であるが、法律やガイドラインの内容をさらに具体化して、どのような取り決めをしているか。例えば、委託先で特定個人情報の目的外利用、利用範囲を超えた利用が行われないよう、どうするのか。特定個人情報自体にアクセスできる人を限定したり、管理者が従業員をチェックしたり、取扱いのログを取るなど。

○ ⑦再委託

- 再委託先で特定個人情報が適正に取り扱われるために行っている措置について記載する。
- ①情報保護管理体制の確認、②閲覧者・更新者の制限、③取扱記録、④ルール策定、⑤ルール遵守確認、⑥契約を参考に、具体的に記載する。
- 例えば、再委託先における特定個人情報の管理状況を定期的に監査・点検している場合は、実施頻度、点検方法（訪問確認、セルフチェック）、点検後の改善指示の実施有無、改善状況のモニタリングの実施有無等を記載する。

8. 不正提供・不正移転対策について説明しよう

どんなリスク？

- 番号法では、特定個人情報の必要な範囲外の提供・移転を防止するため、厳格な規制が講じられている。評価実施機関においても特定個人情報が違法・不正に提供・移転され、転々流通しないよう、流用されないようにしなければならない。
- 例えば、乳幼児医療費助成事務で、乳幼児の保護者からマイナンバーが記載された申請書を受け取り、処理を行い、マイナンバーを記載した医療証を交付することは、適法・妥当（医療証にマイナンバーを記載しない選択もありうる）。
一方で、乳幼児医療費助成事務で、乳幼児の病名・医療費と乳幼児・保護者のマイナンバーを、名簿業者に売却しては当然いけないし、保険会社に提供してもいけない。自治体内で情報移転することも、例えば保育課に渡すことも、条例で規定しなければ原則だめ。
∴ プライバシー侵害のおそれ、マイナンバーによる紐づけのおそれ
- 「Ⅱ 5. 提供・移転」に法律上認められた提供・移転だけが記載されているか、法令上の根拠欄（Ⅱ 5 ①）などを確認した上で、それら以外の提供・移転を防止できることが、具体的かつ合理的に説明する

8. 不正提供・不正移転対策について説明しよう

対策

- 提供・移転時に記録を作成し、不正行為を抑止する。
 - 具体的にどのような記録が作成されるか。
 - 記録を作成しない場合でも、不正提供・移転を防止できる理由が合理的に記載されていればよい。
- 提供・移転に関して、ルールを定める
 - どのようにしてルール遵守を確認するか。
 - ルールを定めなくても、不正提供・移転を防止できる理由が合理的に記載されていればよい。

→ 重点項目評価書Ⅲ 5・全項目評価書Ⅲ 5 リスク 1 に記載

9. 情報提供ネットワークによる不正提供対策について説明しよう

どんなリスク？

- 情報提供ネットワークシステムを使用して、他の自治体・行政機関・日本年金機構などと特定個人情報授受がなされうる。マイナンバーによって情報連携がしやすくなることで効果が見込まれると同時に、本人の知らないところで勝手に情報がやりとりされないかとの不安も。
- 例えば、業務上必要性があって、法令に明記された範囲内で、適正に情報授受がなされているのならばよいが、情報提供ネットワークシステムを利用できることを奇貨として、自治体職員が興味本位で住民の情報を入手することは当然認められない。
- また、情報提供ネットワークシステムが安全でなければ、そこで大量の特定個人情報が授受されるので、さまざまな情報が抜き取られたりするのではという不安も。
 - →中間サーバー部分の安全面については、総務省からの情報提供を参照
 - →情報提供ネットワークシステム部分の安全面については、総務省・内閣官房より情報提供がなされていないように見受けられ、非常に問題

→ 重点項目評価書Ⅲ 6・全項目評価書Ⅲ 6に記載

9. 情報提供ネットワークによる不正提供対策について説明しよう

対策

- 目的外人手防止対策
 - まず目的と入手経路が特定されていることが前提となる。
 - 情報提供ネットワークシステムを通じた入手の場合、使用目的と入手経路は法律上限定されていて、明確に特定されている（番号法19条7号・別表第二）
 - 対象者以外の情報を入手しない
 - どのように対象者を洗い出すのか、マイナンバーを入手する担当者等に対象者のリストを示し、入手の際は複数人でチェックする等
 - この点、事務処理の流れをすべてシステム化することで、対象者情報以外は職員が入手できないようにする対策も考えられる。厚生労働大臣が平成27年4月21日に公表した「労働者災害補償保険法による保険給付等（年金給付）に関する事務全項目評価書」では「情報提供ネットワークシステムを通じた特定個人情報の入手は、労災年金の請求等から決定に至るまでの事務の流れの中でシステム的に行われるようにすることで（請求内容のOCR（文字認識）入力を契機として、日本年金機構への情報照会を自動的に行う等）、請求等と離れた形で個別に照会が行われないようにしている」と記載されており、参考になる。
 - 必要な情報以外を入手しない
 - 情報提供ネットワークシステム又は中間サーバーの仕様上、番号法で認められた特定個人情報のみ入手できるよう、一定の制御がなされていると考えられるので、その点をわかりやすく記載。
 - その他

9. 情報提供ネットワークによる不正提供対策について説明しよう

対策

○ 不正提供防止対策

○ 提供記録

- 情報提供ネットワークシステム又は中間サーバーの仕様上、情報提供等記録の作成が行われると考えられるので、その点をわかりやすく記載。

○ ルール

- 自治体内で、情報提供ネットワークシステムを使用した情報提供について、どのようなルールが設けられており、それに従えば、不正提供が防止できる理由を説明する。

○ その他

10. 開示請求・問合せについて説明しよう

何を説明する？

- 特定個人情報の取扱いについて不安に思った市民等がとりうるアクションは、主に①情報保護評価書を読む、②特定個人情報の開示・訂正・利用停止を請求、③評価実施機関に問い合わせる
- アクションを取りたいと思ったときにとれるように、方法をわかりやすく説明する

→重点項目評価書Ⅳ・全項目評価書Ⅴに記載

参考

- 作った人が明かすマイナンバー プライバシー保護の勘所 (Itpro)
 - 実はカンタン、「プライバシー影響評価」
 - <http://itpro.nikkeibp.co.jp/atcl/column/15/052100128/052100005/?ST=security&P=1>
 - 脱・行政文書、間違いのコピペ丸投げ
 - <http://itpro.nikkeibp.co.jp/atcl/column/15/052100128/080600008/>
 - どうなっている？あなたの街のマイナンバー
 - <http://itpro.nikkeibp.co.jp/atcl/column/15/052100128/080600006/?ST=management&P=1>
- 『特定個人情報保護評価のための番号法解説～プライバシー影響評価 (PIA)のすべて』
 - 第一法規、2015年11月～12月ごろ刊行予定