

**「特定個人情報保護評価に関する規則(案)」  
及び「特定個人情報保護評価指針(案)」  
に関する意見**

**平成26年4月3日**

**一般社団法人 情報サービス産業協会**



**本意見書において、次の略語を使用します。**

- **特定個人情報保護評価に関する規則(案) ～ 規則**
- **特定個人情報保護評価指針(案) ～ 指針**
- **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 ～ 番号法**
- **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施行令(仮称)案  
～ 施行令**

# I 規則に対する意見（1）

## ● 規則第2条（定義）

### 【意見】

特定個人情報保護委員会規則において、全項目評価書の位置づけが文面上分かりづらくなっていることから、第2条第3号に全項目評価書の定義を示す等、分かりやすくすべき。

指針において、番号法第27条第1項に規定する評価書が全項目評価書とされているが、規則において全項目評価書の定義が置かれていないことなどから、規則が全体的に非常に分かりづらくなっているため。

## I 規則に対する意見（2）

### ● 規則第6条第1号

行政機関の長等が特定個人情報ファイルを取り扱う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数の総数が一万人以上十万人未満である場合であって、当該事務に従事する者の数が五百人以上であるとき**又は**当該行政機関の長等において過去一年以内に特定個人情報に関する重大事故が発生したとき**又は**当該行政機関の長等が過去一年以内に当該行政機関の長等における特定個人情報に関する重大事故の発生を知ったときに限る。)

### 【意見】

規則第6条第1号末尾の括弧閉じに対応する括弧開きがないなど、第1号の意が分かりづらい。

おそらく第1号は、

「行政機関の長等が特定個人情報ファイルを取り扱う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数の総数が一万人以上十万人未満である場合であって、当該事務に従事する者の数が五百人以上であるとき(当該行政機関の長等において過去一年以内に特定個人情報に関する重大事故が発生したとき**又は**当該行政機関の長等が過去一年以内に当該行政機関の長等における特定個人情報に関する重大事故の発生を知ったときに限る。)」

と思われる。

## I 規則に対する意見（3）

### ● 規則第4条(法第27第1項の特定個人情報ファイル)第8号ロ、第6条(重点項目評価)第1号、同条第2号第4条第8号

ロ 行政機関の長等が特定個人情報ファイルを取り扱う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数の総数が一万人以上十万人未満である場合であって、当該事務に従事する者の数が五百人未満であるとき(当該行政機関の長等において過去一年以内に特定個人情報の漏えいその他の事故(重大なものとして指針で定めるものに限る。以下「特定個人情報に関する**重大事故**」という。)が発生したとき又は当該行政機関の長等が過去一年以内に当該行政機関における特定個人情報に関する**重大事故の発生を知ったときを除く。)**。)

#### 第6条

一 行政機関の長等が特定個人情報ファイルを取り扱う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数の総数が一万人以上十万人未満である場合であって、当該事務に従事する者の数が五百人以上であるとき又は当該行政機関の長等において過去一年以内に特定個人情報に関する**重大事故が発生したとき又は当該行政機関の長等が過去一年以内に当該行政機関の長等における特定個人情報に関する重大事故の発生を知ったときに限る。)**

二 行政機関の長等が特定個人情報ファイルを取り扱う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数の総数が十万人以上三十万人未満である場合であって、当該事務に従事する者の数が五百人未満であるとき(当該行政機関の長等において過去一年以内に特定個人情報に関する**重大事故が発生したとき又は当該行政機関の長等が過去一年以内に当該行政機関の長等における特定個人情報に関する重大事故の発生を知ったときを除く。)**

#### 【意見】

重大事故の発生や重大事故の発生を知ったことを起算する日が不明確であり、しきい値判断に影響を与えることから、起算日を明確に規定すべき。

## II 指針に対する意見（1）

### ● 指針全体

#### 【意見】

昨今の民間事業者における情報漏洩事案を鑑み、業としてその提出する文書に個人番号を記載する必要のある関係事務実施者の内、金融機関についてはその保有する特定個人情報量を鑑み行政と同等以上の特定個人情報安全管理措置を講ずべき規定を設定すべきである。

## II 指針に対する意見（2）

### ● 指針全体

#### 【意見】

番号法第19条第14号において特定個人情報保護委員会規則に定めるとされている「特定個人情報の提供に関する制限(例外規定)」の規定に関して、今後の見通し(当該規則の公布予定の有無、例外規定の内容(見込みを含む)、規則公布の時期等)について明らかにするとともに、例外規定の内容によっては指針に反映すべき。

本規定が明確になることで、番号制度の準備行為やサービス内容を検討するにあたっての制約が具体化されるため。

## II 指針に対する意見（3）

### ● 指針第1の1

#### 第1 特定個人情報保護評価の意義

##### 1 特定個人情報保護評価の基本理念

#### 【意見】

指針における「個人のプライバシー等の権利利益」とは、諸外国で採用されているプライバシー影響評価(Privacy Impact Assessment)または ISO22307を想定すればよいか、明確にしていきたいと思います。



## II 指針に対する意見（４）

### ● 指針第2の1

#### 第2 定義

1 評価実施機関 番号法第27条及び規則の規定に基づき特定個人情報保護評価を実施する番号法第2条第14項に規定する行政機関の長等(行政機関の長、地方公共団体の機関、独立行政法人等、地方独立行政法人及び地方公共団体情報システム機構並びに番号法第19条第7号に規定する情報照会者及び情報提供者)をいう。

#### 【意見】

指針第2の1の評価実施機関は、番号法第27条及び規則に規定されている組織となっている。

一方実務では、評価対象機関の特定個人情報ファイルを取りまとめて、別の第三者組織が委託を受けて保管しているケース(例、健康保険組合連合会)が想定される。この場合、特定個人情報ファイルの管理の実態に則して特定個人情報保護評価を実施すべき組織を定めることが現実的であると考えられることから、このような第三者組織も評価対象機関と位置付けるべき。

## II 指針に対する意見（5）

### ● 指針第2の6

#### 第2 定義

6 重大事故 評価実施機関が法令に基づく安全管理措置義務を負う個人情報<sup>1</sup>を漏えい、滅失又は毀損した場合であつて、故意による又は当該個人情報の本人（個人情報によって識別される特定の個人であつて、当該評価実施機関の従業者を除く。）の数が101人以上のもの（ただし、配送事故等のうち当該評価実施機関の責めに帰さない事由によるものを除く。）をいう。

#### 【意見】

「重大事故」の定義のうち、除外規定となるもの（配送事故等のうち当該評価実施機関の責めに帰さない事由によるもの）の具体をさらに示すべき。

特定個人情報保護委員会での議論でもあったように、「配送事故等」にネットワークに関する事項が含まれるか、文面上からは読み取りづらい。またどのような措置を講じていけば「責めに帰さない」ことになるのか不明確であるため。

## II 指針に対する意見（6）

### ● 指針第4の1

#### 第4 特定個人情報保護評価の対象

##### 1 基本的な考え方

特定個人情報保護評価の対象は、番号法、番号法以外の国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の規定に基づき特定個人情報ファイルを取り扱う事務とする。

#### 【意見】

特定個人情報保護評価の対象となる事務を規定する「番号法以外の国の法令」を具体的に規則または指針で示すべき。

「指針(案)の解説」から、番号法以外の国の法令に基づく特定個人情報保護評価の対象として、番号法第9条第5号に基づく番号法第19条第12号並びに番号法施行令第24条及び番号法施行令別表の調査等の事務があると思われるが不明瞭なため、当該事務が特定個人情報保護評価の対象となる事務であるか否かを指針等で明示すべき。

## II 指針に対する意見（7）

### ● 指針第4の4(1)

#### 第4 特定個人情報保護評価の対象

#### 4 特定個人情報保護評価の実施が義務付けられない事務

#### (1) 実施が義務付けられない事務

特定個人情報ファイルを取り扱う事務のうち、次に掲げる事務(規則第4条第1号から第7号までに掲げる特定個人情報ファイルのみを取り扱う事務)は特定個人情報保護評価の実施が義務付けられない。次に掲げる事務であっても、特定個人情報保護評価の枠組みを用い、任意で評価を実施することを妨げるものではない。

### 【意見】

指針第4の4(1)の「特定個人情報ファイルのみ」の定義を、より明確に規定すべき。

本規定を明確にすることで、特定個人情報ファイルを取り扱う事務及び事務従事者を具体的に特定することができ、結果として、評価対象範囲を適切に見極められるため。

例えば規則で職員等の人事、給与、福利厚生に関する事項等とされているものに関し、義務付けられない事務の範囲をさらに具体的に指定したり、その範囲の考え方を明確化したりすることで、評価実施機関との意識相違がなくなると思われる。

## II 指針に対する意見（8）

### ● 指針第4の4(1)エ

#### 第4 特定個人情報保護評価の対象

#### 4 特定個人情報保護評価の実施が義務付けられない事務

#### (1)実施が義務付けられない事務

エ 1つの事業所の事業主が単独で設立した健康保険組合又は密接な関係を有する2以上の事業所の事業主が共同若しくは連合して設立した健康保険組合が保有する被保険者若しくは被保険者であった者又はその被扶養者の医療保険に関する事項を記録した特定個人情報ファイルのみを取り扱う事務(規則第4条第4号及び第5号)

### 【意見】

指針第4の4(1)エ」の趣旨から、「健康保険組合」だけでなく「企業年金基金」が取り扱う事務についても義務付けられない事務に該当すると考えられるため、必要に応じ企業年金組合も義務付けられない事務とすることが可能なように、規則等で規定すべき。

「指針(案)の解説」のp.40において「健康保険組合」が使用者である企業自体とを同一視できることから評価対象外とされているが、「企業年金基金」についても、同様の理由が存在すると考えられるため。

## II 指針に対する意見（9）

- 指針第4の4(2)

第4 特定個人情報保護評価の対象

4 特定個人情報保護評価の実施が義務付けられない事務

(2) 特定個人情報保護評価以外の番号法の規定の適用

**【意見】**

該当業務・システムを受託している場合、委託元・委託先を想定した評価の実施体制を明記すべきである。

## II 指針に対する意見（10）

### ● 指針第6の1(1)

#### 第6 特定個人情報保護評価の実施時期

##### 1 新規保有時

##### (1) システム用ファイルを保有しようとする場合の実施時期

#### 【意見】

指針第6の1(1)の特定個人情報保護評価の実施時期は、評価する内容に基づき、さらに柔軟性を待たせるべき。

システムの要件定義段階までに実施することを原則(例外としてシステム開発段階までに実施することも可能)としているが、評価書には、

- ・委託業者間に関する事項のリスク対策
- ・情報の保管・消去等のリスク対策

等、開発実施中に対策が決定する評価項目やシステムサービス開始後の保守期間で具体的な対策を検討する評価項目も含まれている。

このことから、評価項目の内容を踏まえ段階的(五月雨式)に評価を実施する等、提出タイミングに柔軟性を持たせる必要があるため。

## II 指針に対する意見（11）

### ● 指針第6の1(1)

#### 第6 特定個人情報保護評価の実施時期

##### 1 新規保有時

##### (1) システム用ファイルを保有しようとする場合の実施時期

#### 【意見】

指針第6の1(1)の内容(原則はシステムの要件定義段階までに特定個人情報保護評価を実施)を踏まえると、システム発注者がシステム要件定義と特定個人情報保護評価を実施し、その後、システム調達を実施する想定であると読み取れる。

仮にシステム開発着手後に特定個人情報保護評価の結果に伴うシステム要件定義内容に変更が発生した場合、開発工期等に影響が出る可能性がある。システム開発スケジュールにおいてこのようなシステム要件定義変更をどのように吸収するか指針において考え方を提示すべき。

指針第6の1(1)には、例外として「システムの開発(プログラミング)段階までに実施すること」や「困難な場合は委員会とあらかじめ協議の上実施時期を決定すること」が規定されているように、現実的にはシステムの要件定義段階までに特定個人情報保護評価を終えることが困難となる可能性がある。またシステム開発段階以降に要件定義の変更が生じた場合、システム開発スケジュールに大きな影響を与え、納期やシステム開発コストなどに変動が生じる可能性がある。これらの可能性はシステム開発に共通するため、指針において特定個人情報保護委員会との協議等の考え方を示すべき。



## II 指針に対する意見（12）

- 指針第9の2（1）、基礎項目評価書様式
- 第9 特定個人情報保護評価の評価項目
- 2 評価項目
- （1）基礎項目評価書

### 【意見】

基礎項目評価書の記載項目に、「特定個人情報の開示・訂正・利用停止請求、特定個人情報ファイルの取扱いに関する問い合わせ等」を加えるべき。

重点項目評価書及び全項目評価書には当該事項の記載があるが、基礎項目評価のみ実施する機関も特定個人情報を保有するため、請求者等の利便性から当該項目を記載すべき。

## II 指針に対する意見（13）

- 指針第10の1(1)  
第10 委員会の関与  
1 特定個人情報保護評価書の承認  
(1)承認対象

### 【意見】

指針第10の1(1)における特定個人情報保護委員会による全項目評価書の審査・承認にかかる所要期間の目安(標準処理期間)を指針等に明記すべき。

全項目評価の対象になるシステム開発のスケジュールやコスト計画に対して、場合によっては特定個人情報保護委員会による承認に係る期間や承認結果に伴う設計見直しコストを考慮する必要があるため。

第5回特定個人情報保護委員会において標準処理期間について議論があったが、特定個人情報保護委員会における作業量・質の問題もさることながら、開発スケジュールの遅延やコスト増は住民等に与える影響が大きくなり、社会的な影響が大きくなる恐れがある。

## II 指針に対する意見（14）

### ● 重点項目評価書「Ⅲ リスク対策」、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」

#### 【意見】

リスク対策に係る事項で「このリスクへの対策は十分か」との評価項目があり、チェックボックスが設定されている。選択肢は「特に力を入れている」「十分である」「課題が残されている」の三つだが、いずれか一つにチェックを入れるかどうか不明であり、選択肢(設問のワーディング等)が回答しづらいことから、設問の再考を含め記入要領を見直すべき。

論理的には「特に力を入れている」が「課題が残されている」こともあり得る(むしろ特に力を入れているからこそ課題認識が強いことがあり得)ことから、いずれか一つのみでチェックを入れることはできない(つまりマルチアンサーになる)可能性がある。

「特に力を入れている」こと、「十分に行っている」こと、「課題が残されている」ことは評価尺度がそれぞれ異なることから、三者択一にすべきではない。リスク対策における自己評価を問うのであれば、これら三つの選択肢をそれぞれ独立した設問にして「はい」「いいえ」「わからない(自己評価できない)」で回答させる(つまり明確なシングルアンサーとする)等すべき。

なお、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」の「6. 特定個人情報の保管・消去」の「⑤物理的対策」「⑥技術的対策」「⑦バックアップ」に関しては、選択肢が「特に力を入れて行っている」「十分に行っている」「十分に周知していない」とあるが、「特に力を入れて行っている」「十分に行っている」「十分に周知していない」の誤記と思われる。また「⑧事故発生時手順の策定・周知」について「特に力を入れて行っている」「十分に行っている」「十分に周知していない」についても、「特に力を入れて行っている」「十分に行っている」「十分に周知していない」の誤記と思われる。いずれも上記の問題があるため、回答方法を再考すべき。なお手順の策定と周知は別の活動であるため、設問を分けることが望ましい。

## II 指針に対する意見（15）

- 重点項目評価書「III リスク対策」、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」

### 【意見】

重点項目評価書「III リスク対策」の「6. 特定個人情報の保管・消去」の「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」及び全項目評価書の「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」の「6. 特定個人情報の保管・消去」の「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」について、過去3年の起算日を明確にすべき。

いつの時点から起算するかで記入する事項が変わる可能性があるため。