

「特定個人情報保護評価指針の解説」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指針の解説を更新しました。

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指針の解説の主な更新箇所

<重大事故関係>

Q第2の6-1

新規

「特定個人情報に関する重大事故」には、具体的にどのような事態が該当するのでしょうか。

Q第2の7-1

新規

「個人情報に関する重大事故」には、どのような事態が該当するのでしょうか。

<国民・住民等への意見聴取関係>

Q第5の3(3)-2

新規

国民・住民等からの意見聴取の方法は、必ずインターネットを利用しなければならないのでしょうか。

<重要な変更関係>

Q第6の2(2)-1

修正

「重要な変更」の対象である重点項目評価書・全項目評価書の記載項目の変更であっても、重要な変更にあたり当たらないとしている「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相当程度変動させるものではないと考えられる変更」とは具体的にはどのようなものなのでしょうか。

Q第6の2(2)-3

修正

「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明らかに軽減させる変更」とは具体的にはどのようなものなのでしょうか。技術進歩に伴うシステムの

| | | |
|---|-----------|--|
| Q別表－2 | 新規 | 更新は通常リスクを軽減させることになりませんが、重要な変更にあたらないということでしょうか。 委託先の追加は「重要な変更」に該当するのでしょうか。 |
| <緊急時の事後評価関係> | | |
| Q第6の3－1 | 新規 | 指針第6の3において規則第9条第2項（緊急時の事後評価）を適用することが認められないものとして定められている「既に個人番号利用事務等として定着している事務を実施する場合」とは、具体的にどのような場合を指すのでしょうか。 |
| Q第6の3－2 | 新規 | 規則第9条第2項を適用することとした場合、特定個人情報保護評価の実施時期はどのように考えればよいのでしょうか。 |
| <基礎項目評価書関係> | | |
| 第9の2（1）－1 | 新規 | 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ファイルに記録された特定個人情報を保護するための主な措置の実施状況の評価について、どのような措置が実施されていれば、「十分である」等を選択することができますか。 |
| 第9の2（1）－2 | 新規 | 基礎項目評価書中「IV リスク対策」の「8. 人手を介在させる作業」、「11. 最も優先度が高いと考えられる対策」の「判断の根拠」の欄には、どのような内容を記載すればよいのでしょうか。【新規】 |
| 第9の2（1）－3 | 新規 | 基礎項目評価書中「IV リスク対策」の「11. 最も優先度が高いと考えられる対策」について、選択肢全てが同列で重要度が高いと考えられる場合は、どうすれば良いですか。【新規】 |
| <地方公共団体の基幹業務システムの統一・標準化関係> | | |
| Q他－2 | 新規 | 地方公共団体の基幹業務システムの統一・標準化に向けた対応として、特定個人情報保護評価を行う場合、再実施が必要になるのでしょうか。修正での対応は認められないのでしょうか。【新規】 |

<重大事故関係>

新規

第2 定義

この指針において使用する用語は、番号法及び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。以下「規則」という。）において使用する用語の例によるほか、次の定義に従うものとする。

1～5 （略）

6 特定個人情報に関する重大事故 評価実施機関が法令に基づく安全管理措置義務を負う特定個人情報に関する事態であって、次の（1）又は（2）のいずれかに該当するもの（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を除く。）をいう。

（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第二十九条の四第一項及び第二項に基づく特定個人情報の漏えい等に関する報告等に関する規則（平成27年特定個人情報保護委員会規則第5号）第2条第1号から第3号までの各号に掲げる事態（当該事態における当該特定個人情報に係る本人が当該評価実施機関の従業者であるものを除く。）のいずれかに該当するもの

（2）同条第4号に掲げる事態のうち、当該特定個人情報に係る本人（当該評価実施機関の従業者を除く。）の数が100人を超えるもの

7 個人情報に関する重大事故 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に関する事態であって、次の（1）から（3）までのいずれかに該当するもの（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を除く。）又は特定個人情報に関する重大事故に該当するものをいう。

（1）個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第3号）第7条第1号から第3号までの各号又は第43条第1号から第3号までの各号若しくは第5号に掲げる事態（当該事態における当該個人情報に係る本人が当該評価実施機関の従業者であるものを除く。）のいずれかに該当するもの

（2）同規則第7条第4号に掲げる事態のうち、当該個人情報に係る本人（当該評価実施機関の従業者を除く。下記（3）において同じ。）の数が1,000人を超えるもの

（3）同規則第43条第4号に掲げる事態のうち、当該個人情報に係る本人の数が100人を超えるもの

Q第2の6-1

「特定個人情報に関する重大事故」には、具体的にどのような事態が該当するのでしょうか。

(A)

- 基本的には、「特定個人情報に関する漏えい等報告(※1)の報告対象事態(※2)」が「特定個人情報に関する重大事故」に該当します。ただし、次の3点について、留意が必要です。

※1 番号法第29条の4の規定により、特定個人情報の安全の確保に係る事態であって「個人の権利利益を害するおそれ大きいものとして個人情報保護委員会規則で定めるもの」(具体的には※2の報告対象事態)が生じたときに、個人情報保護委員会に報告すること及び本人へ通知することが、法令上の義務になっています。

※2 「特定個人情報に関する漏えい等報告の報告対象事態」とは、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二十九条の四第一項及び第二項に基づく特定個人情報の漏えい等に関する規則(平成27年特定個人情報保護委員会規則第5号。以下「特定個人情報の漏えい等報告規則」という。)第2条各号(下記【参考】を参照。)のいずれかに該当する事態をいいます。

- ① 漏えい等報告が行われた事案のうち、規則該当性が認められた事案(特定個人情報の漏えい等報告規則第2条各号のいずれかに該当するもの)が対象であるため、単に漏えい等報告を行った事案の全てが重大事故の対象になるわけではありません。特に留意が必要であるのは、次の※3、※4の場合です。

※3 漏えい等報告を行っていなくとも、「特定個人情報に関する漏えい等報告の報告対象事態」に該当する事案が発生した場合には、「特定個人情報に関する重大事故」に該当します(漏えい等事案が発生したことを知ったにもかかわらず、漏えい等報告を行わなかった場合には、番号法に基づく権限行使の対象となり得ます。)

※4 「特定個人情報に関する漏えい等報告の報告対象事態」に該当しないものについては、任意の漏えい等報告を行ったとしても、重大事故に該当しません。

- ② 「特定個人情報に関する漏えい等報告の報告対象事態」に該当するものであっても、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については、「特定個人情報に関する重大事故」に該当しないこととしています。

- ③ 「特定個人情報の重大事故」の定義において、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者の数を含みません。

※ 令和6年4月1日に施行された特定個人情報保護評価指針の一部を改正する件（令和6年個人情報保護委員会告示第1号）による改正前に発生した「特定個人情報に関する重大事故」であって、当該改正前の定義に該当しない事案については、当該改正後の新定義に該当するとしても、「特定個人情報に関する重大事故」に該当しないこととしています（当該改正告示において、経過措置が設けられています。）。

- 実際に漏えい等事案が発生した場合は、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は設置している報告フォームからお願いします。重大事故の該当性については、報告対象事態への該当性が明らかになった時点以降に、個人情報保護委員会事務局の保護評価制度担当に問い合わせてください。

<個人情報保護委員会への漏えい等報告ページ>

<https://www.ppc.go.jp/personalinfo/legal/leakAction/>

【参考】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二十九条の四第一項及び第二項に基づく特定個人情報の漏えい等に関する報告等に関する規則（平成27年特定個人情報保護委員会規則第5号）抄

（個人の権利利益を害するおそれが大きいもの）

第二条 法第二十九条の四第一項本文の個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものは、次の各号のいずれかに該当するものとする。

一 次に掲げる特定個人情報（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下同じ。）の漏えい、滅失若しくは毀損（以下「漏えい等」という。）が発生し、又は発生したおそれがある事態

イ 情報提供ネットワークシステム及びこれに接続された電子計算機に記録された特定個人情報

ロ 個人番号利用事務実施者が個人番号利用事務を処理するために使用する情報システムにおいて管理される特定個人情報

ハ 行政機関、地方公共団体、独立行政法人等及び地方独立行政法人が個人番号関係事務を処理するために使用する情報システム並びに行政機関、地方公共団体、独立行政法人等及び地方独立行政法人から個人番号関係事務の全部又は一部の委託を受けた者が当該個人番号関係事務を処理するために使用する情報システム

ムにおいて管理される特定個人情報

二 次に掲げる事態

- イ 不正の目的をもって行われたおそれがある特定個人情報の漏えい等が発生し、又は発生したおそれがある事態
- ロ 不正の目的をもって、特定個人情報が利用され、又は利用されたおそれがある事態
- ハ 不正の目的をもって、特定個人情報が提供され、又は提供されたおそれがある事態

三 個人番号利用事務実施者又は個人番号関係事務実施者の保有する特定個人情報ファイルに記録された特定個人情報が電磁的方法により不特定多数の者に閲覧され、又は閲覧されるおそれがある事態

四 次に掲げる特定個人情報に係る本人の数が百人を超える事態

- イ 漏えい等が発生し、又は発生したおそれがある特定個人情報
- ロ 法第九条の規定に反して利用され、又は利用されたおそれがある個人番号を含む特定個人情報
- ハ 法第十九条の規定に反して提供され、又は提供されたおそれがある特定個人情報

新規

Q第2の7-1

「個人情報に関する重大事故」には、どのような事態が該当するのでしょうか。

(A)

- 基本的には、「特定個人情報に関する重大事故」に該当する事態（Q第2の6-1を参照）に加えて、「個人情報に関する漏えい等報告の報告対象事態（※1）」が「個人情報に関する重大事故」に該当します。ただし、次の3点について留意が必要です。

※1 個人情報に関する漏えい等報告の報告対象事態とは、個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第3号。）第7条各号のいずれかに該当する事態又は第43条各号（下記【参考】を参照。）のいずれかに該当する事態をいいます。

- ① 漏えい等報告が行われた事案のうち、下記の規則該当性が認められた事案が対象であるため、単に漏えい等報告を行った事案の全てが重大事故の対象になるわけではありません。

※2 漏えい等報告を行っていない場合にも、報告対象事態に該当する事案が発生した又は発生したことを知った場合には、個人情報に関する重大事故に該当します（漏えい等事案が発生したことを知ったにもかかわらず、漏えい

等報告を行わなかった場合には、個人情報保護法又は番号法に基づく権限行使の対象となり得ます。)

※3 「個人情報に関する漏えい等報告の報告対象事態」に該当しないものについては、任意の漏えい等報告を行ったとしても、重大事故に該当しません。

- ② 「個人情報に関する漏えい等報告の報告対象事態」に該当するものであっても、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については、「個人情報に関する重大事故」に該当しないこととしています。
 - ③ 「個人情報に関する重大事故」の定義において、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者の数を含みません。
- 実際に事案が発生した場合は、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は設置している報告フォームからお願いします。重大事故の該当性については、報告対象事態への該当性が明らかになった時点以降に、個人情報保護委員会事務局の保護評価制度担当に問い合わせてください。

<個人情報保護委員会への漏えい等報告ページ>

<https://www.ppc.go.jp/personalinfo/legal/leakAction/>

【参考】個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第3号）抄

（個人の権利利益を害するおそれが大きいもの）

第七条 法第二十六条第一項本文の個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものは、次の各号のいずれかに該当するものとする。

- 一 要配慮個人情報が含まれる個人データ（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下この条及び次条第一項において同じ。）の漏えい、滅失若しくは毀損（以下この条及び次条第一項において「漏えい等」という。）が発生し、又は発生したおそれがある事態
- 二 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
- 三 不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データ（当該個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予

定されているものを含む。)の漏えい等が発生し、又は発生したおそれがある事態

四 個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態

(個人の権利利益を害するおそれが大きいもの)

第四十三条 法第六十八条第一項の個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものは、次の各号のいずれかに該当するものとする。

一 要配慮個人情報に含まれる保有個人情報(高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下この条及び次条第一項において同じ。)の漏えい、滅失若しくは毀損(以下この条及び次条第一項において「漏えい等」という。)が発生し、又は発生したおそれがある事態

二 不正に利用されることにより財産的被害が生じるおそれがある保有個人情報の漏えい等が発生し、又は発生したおそれがある事態

三 不正の目的をもって行われたおそれがある当該行政機関の長等の属する行政機関等に対する行為による保有個人情報(当該行政機関の長等の属する行政機関等が取得し、又は取得しようとしている個人情報であって、保有個人情報として取り扱われることが予定されているものを含む。)の漏えい等が発生し、又は発生したおそれがある事態

四 保有個人情報に係る本人の数が百人を超える漏えい等が発生し、又は発生したおそれがある事態

五 条例要配慮個人情報に含まれる保有個人情報の漏えい等が発生し、又は発生したおそれがある事態(地方公共団体の機関又は地方独立行政法人が法第六十八条第一項の報告を行う場合であって、当該地方公共団体の機関又は地方独立行政法人に適用される条例において条例要配慮個人情報について定められているときに限る。)

<国民・住民等への意見聴取関係>

新規

(3) 全項目評価書

ア 行政機関等の場合

行政機関等は、上記2(6)、(7)又は(8)の場合は、全項目評価書(様式4参照)を作成するものとする。

また、行政機関等は、全項目評価書を作成後、番号法第28条第1項の規定に基づき、全項目評価書を公示して広く国民の意見を求め、これにより得られた意見を十分考慮した上で全項目評価書に必要な見直しを行うものとする。ただし、公表しないことができる全項目評価書又は項目(下記(4)参照)については、この限りではない(規則第10条)。

全項目評価書を公示し国民からの意見を聴取する期間は原則として30日以上とする。ただし、特段の理由がある場合には、全項目評価書においてその理由を明らかにした上でこれを短縮することができる。

また、全項目評価書の公示の方法については、規則第9条の2の規定に基づき、インターネットの利用その他の適切な方法によるものとする。

行政機関等は、番号法第28条第2項の規定に基づき、公示し国民の意見を求め、必要な見直しを行った全項目評価書を委員会へ提出し、委員会による承認を受けるものとする。

イ 地方公共団体等の場合

地方公共団体等は、上記2(6)、(7)又は(8)の場合は、全項目評価書を作成するものとする。

また、地方公共団体等は、全項目評価書を作成した後、規則第7条第1項の規定に基づき、全項目評価書を公示して広く住民等の意見を求め、これにより得られた意見を十分考慮した上で全項目評価書に必要な見直しを行うものとする。ただし、公表しないことができる全項目評価書又は項目(下記(4)参照)については、この限りではない(規則第7条第3項)。

全項目評価書を公示し住民等からの意見を聴取する期間は原則として30日以上とする。ただし、特段の理由がある場合には、全項目評価書においてその理由を明らかにした上でこれを短縮することができる。

る。

また、全項目評価書の公示の方法については、規則第9条の2の規定に基づき、インターネットの利用その他の適切な方法によるものとする。

なお、地方公共団体等が条例等に基づき住民等からの意見聴取等の仕組みを定めている場合は、これによることもできる。

地方公共団体等は、公示し住民等の意見を求め、必要な見直しを行った全項目評価書について、規則第7条第4項の規定に基づき、第三者点検を受けるものとする。第三者点検の方法は、原則として、条例等に基づき地方公共団体が設置する個人情報保護審議会又は個人情報保護審査会による点検を受けるものとするが、これらの組織に個人情報保護や情報システムに知見を有する専門家がないなど、個人情報保護審議会又は個人情報保護審査会による点検が困難な場合には、その他の方法によることができる。ただし、その他の方法による場合であっても、専門性を有する外部の第三者によるものとする。第三者点検の際は、点検者に守秘義務を課すなどした上で、公表しない部分

(下記(4)参照)を含む全項目評価書を提示し、点検を受けるものとする。第三者点検においては、下記第10の1(2)に定める審査の観点を参考にすることができる。

地方公共団体等は、規則第7条第5項の規定に基づき、第三者点検を受けた全項目評価書を委員会へ提出するものとする。

Q第5の3(3)－2

国民・住民等からの意見聴取の方法は、必ずインターネットを利用しなければならないのでしょうか。

(A)

- 令和6年の規則・指針改正により、評価実施機関が全項目評価を実施する際の意見聴取の方法は、「インターネットの利用その他の適切な方法によるものとする」ことが定められました。保護評価制度に基づく意見聴取については、規則・指針改正前からインターネットの利用による実施も認められていたところです。
- 他に効率性や周知性の高い手段がある場合には、「その他の適切な方法」に該当するものとして、インターネットを利用しない方法で意見聴取を行うことも可能です。

<重要な変更関係>

修正（赤字の記載を追記しています。）

（２）重要な変更 （略）

Q第6の2（2）－1

「重要な変更」の対象である重点項目評価書・全項目評価書の記載項目の変更であっても、重要な変更に当たらないとしている「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相当程度変動させるものではないと考えられる変更」とは具体的にはどのようなものでしょうか。

（A）

- 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相当程度変動させるものではないと考えられる変更とは、①誤字脱字の修正、組織の名称、所在地、法令の題名等の形式的な変更、②①には該当しないもののリスクを相当程度変動させるものではないと考えられる変更が考えられます。それぞれの具体例は、次のとおりです。

【①の例】

<法令の題名等の形式的な変更の場合>

- ・ 法令上の根拠における条ズレ等の反映を行うケース（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等の一部を改正する法律（令和5年法律第48号）の施行に伴い、「別表第一、別表第二」を「別表、特定個人番号利用事務を定める主務省令」と改めるケースも含まれます。）

【②の例】

<個人の権利利益に影響を及ぼし得る事務手続を終了する場合>

- ・ 「特定個人情報の突合」、「統計分析」、「個人の権利利益に影響を与え得る決定」といった個人の権利利益に影響を及ぼし得る事務手続を終了することに伴い、当該記載項目の記載内容を変更するケース。

<他の行政機関等が運営するシステムの変更を受けて、当該システムを使用する評価実施機関が当該システムに係る部分のみリスク対策の変更を行う場合>

- ・ 医療保険者向け中間サーバー、情報提供ネットワークシステム、住基システム

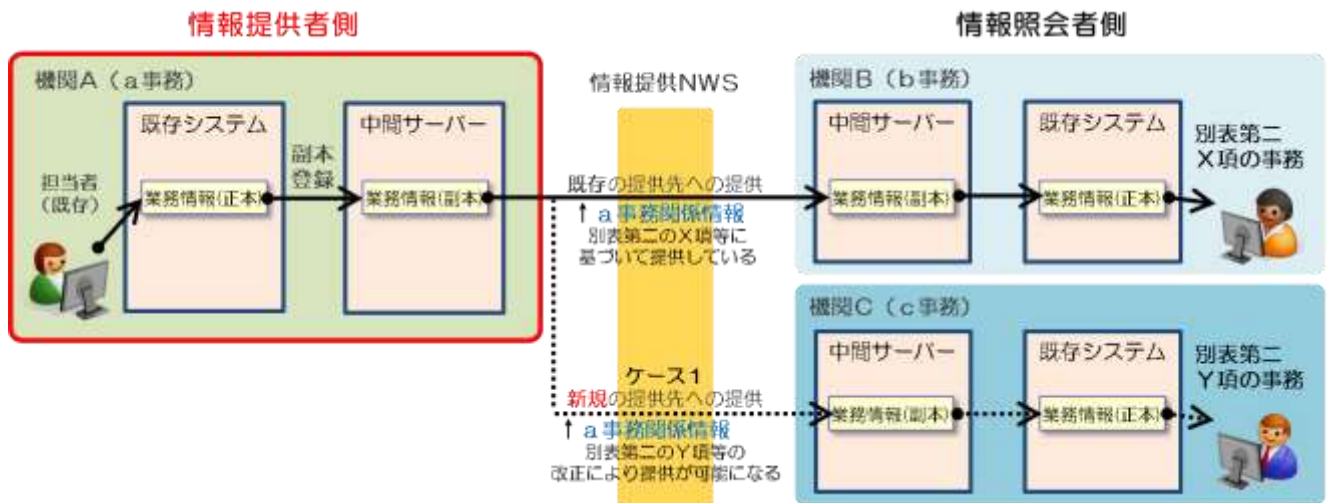
ム等について、当該システムを運営する他の行政機関等によるシステムの変更が行われた場合に、当該システムを使用している評価実施機関が、当該システムの変更後のリスク対策等について特定個人情報保護評価書に記載するものの、評価実施機関に固有の特定個人情報を取り扱うプロセス及び当該プロセスに係るリスク対策に変更がないケース。

<特定個人情報の取扱いを新規に追加するにあたり、既存の取扱いと同様のリスク対策を講ずる場合>

情報提供ネットワークシステムを使用して既に情報連携を行っている事務の特定個人情報保護評価書の記載内容に法令の改正等により変更が生じるケースであって、以下のようなケースが考えられます。

【ケース1】

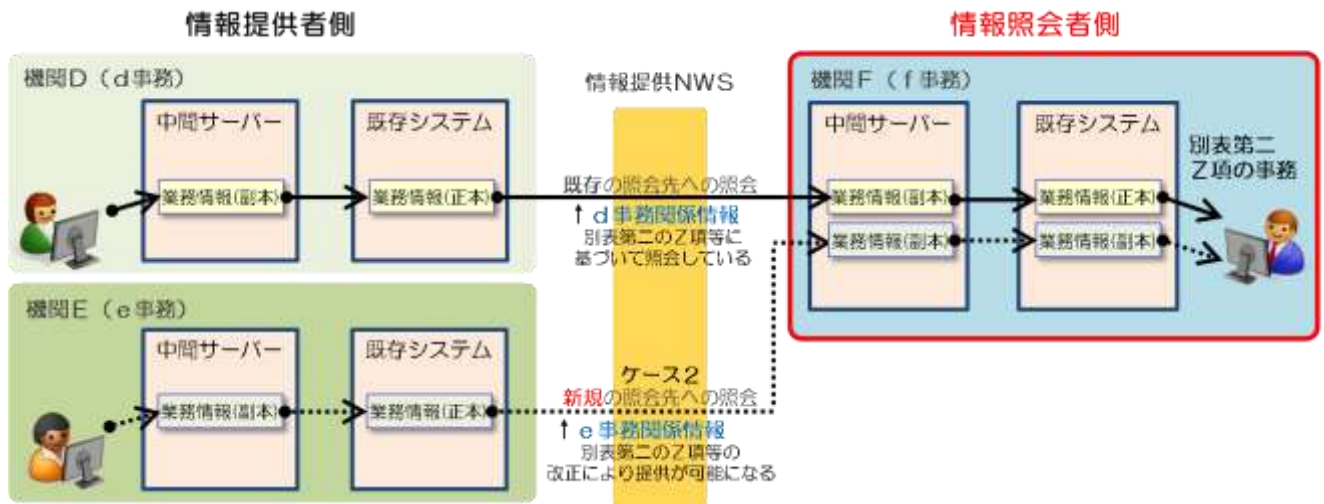
- ・ 機関A（情報提供者）が、これまでa事務で取り扱う特定個人情報ファイル（a事務関係情報）を情報提供ネットワークシステム経由で機関Bに提供していたところ、番号法別表第二等の改正により、機関Aが新たにa事務で取り扱う特定個人情報ファイル（a事務関係情報）を情報提供ネットワークシステム経由で機関Cに提供することとなるケース。



→ この場合、機関Aのa事務の特定個人情報保護評価書において、重要な変更の対象である「法令上の根拠」の記載内容に変更が生じますが、提供先の追加にあたり特定個人情報ファイルを取り扱うプロセス及び当該プロセスに係るリスク対策に変更が生じないため、リスクを相当程度変動させるものではないと考えられる変更該当し、重要な変更にあらず、機関Aは評価の再実施を行う必要はありません。

【ケース2】

- ・ 機関F（情報照会者）がこれまでf事務において、情報提供ネットワークシステム経由で機関Dに特定個人情報ファイル（d事務関係情報）を照会していたところ、番号法別表第二等の改正により、機関Fが新たに情報提供ネットワークシステム経由で機関Eに特定個人情報ファイル（e事務関係情報）を照会することとなるケース。

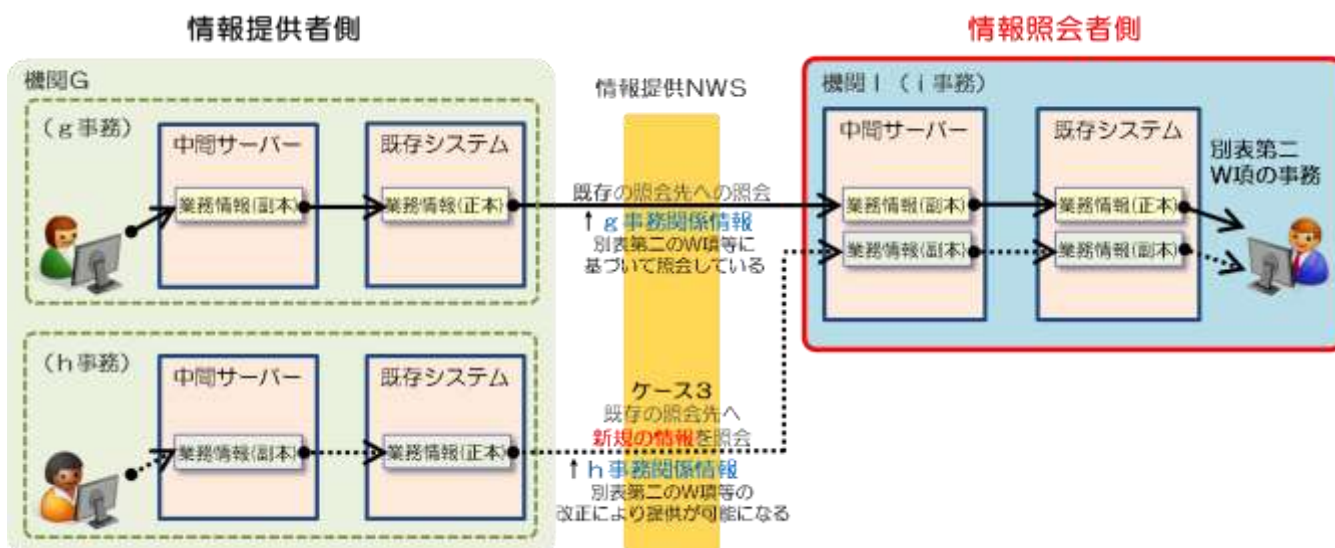


→ この場合、機関Fのf事務の特定個人情報保護評価書において、重要な変更の対象である「主な記録項目」や「入手元」の記載内容に変更が生じますが、照会先の追加にあたり特定個人情報ファイルを取り扱うプロセス及び当該プロセスに係るリスク対策に変更が生じない場合には、リスクを相当程度変動させるものではないと考えられる変更該当し、重要な変更にあらず、機関Fは評価の再実施を行う必要はありません。

※ 仮に、機関Eからの特定個人情報ファイルの入手にあたり、機関Fの特定個人情報を取り扱うプロセス及び当該プロセスに係るリスク対策に変更が生じる場合は、機関Fは評価を再実施する必要があるため注意が必要です。

【ケース3】

- ・ 機関I（情報照会者）がこれまでi事務において、情報提供ネットワークシステム経由で機関Gに特定個人情報ファイル（g事務関係情報）を照会していたところ、番号法別表第二等の改正により、機関Iが情報提供ネットワークシステム経由で機関Gに新たな特定個人情報ファイル（h事務関係情報）を照会することとなるケース。



→ この場合、機関Iのi事務の特定個人情報保護評価書において、重要な変更の対象である「主な記録項目」の記載内容に変更が生じますが、新たな情報の入手にあたり特定個人情報ファイルを取り扱うプロセス及び当該プロセスに係るリスク対策に変更が生じない場合には、リスクを相当程度変動させるものではないと考えられる変更該当し、重要な変更に当たらず、機関Iは評価の再実施を行う必要はありません。

※ 仮に、機関Gからの特定個人情報ファイルの入手にあたり、機関Iの特定個人情報を取り扱うプロセス及び当該プロセスに係るリスク対策に変更が生じる場合は、機関Iは評価を再実施する必要があるため注意が必要です。

【ケース4】

- ・事務Iで利用する特定個人情報ファイルiについて、新たな入手元より特定個人情報を入手するケース（2事例の比較）。



→ 左図の「事務I①」のケースにおいて、現行の入手と新規の入手①を比較した場合、新たに民間事業者Xからの電子記録媒体によって入手することについて、事務のプロセス（例えば、電子記録媒体をどのような方法で取得するか、取得後はどのように取り扱うかなど）に変更がなく、当該プロセスに係るリスク対策にも変更が生じない場合（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」に追記が発生しない場合だけでなく、既に記載しているリスク対策と同様の対策を追記する場合も含む。ケース5、6においても同じ。）は、「リスクを相当程度変動させるものではないと考えられる変更」に該当し、重要な変更にあらず、評価実施機関は評価の再実施を行う必要はありません。

※ 仮に、民間事業者Xからの特定個人情報ファイルの入手にあたり、評価実施機関の特定個人情報を取り扱うプロセス及び当該プロセスに係るリスク対策に変更が生じる場合は、評価実施機関は評価を再実施する必要があるため注意が必要です。

→ 一方で、右図の「事務I②」のケースにおいて現行の入手と新規の入手②を比較した場合、行政機関Yからの専用線によって入手することについて、現行の事務にないプロセスが発生しており、かつ、そのプロセスに係るリスク対策を講ずる必要があることから、事務のプロセス及び当該プロセスに係るリスク対策にも変更が生じることから、当然に「リスクを相当程度変動させるものではないと考えられる変更」に当たらないものと考えられます。

【ケース5】

- ・ 事務Ⅲで利用する特定個人情報ファイルiiiにおいて、新たな提供方法で特定個人情報を提供するケース（2事例の比較）。



→ 左図の「事務Ⅲ①」のケースにおいて、現行の提供①②と新規の提供を比較した場合、新たに行政機関Xに電子記録媒体で特定個人情報を提供することについて、事務のプロセス（例えば、電子記録媒体に含む特定個人情報をどのように選定するか、電子記録媒体をどのように受け渡すか、提供後の電子記録媒体の取扱いをどうするかなど）に変更がなく、当該プロセスに係るリスク対策にも変更が生じない場合は、「リスクを相当程度変動させるものではないと考えられる変更」に当たると考えられます。

※ ただし、行政機関Xへの電子記録媒体での提供に当たり、評価実施機関の特定個人情報を取り扱うプロセス及び当該プロセスに係るリスク対策に変更が生じる場合は、評価実施機関は評価を再実施する必要があるため注意が必要です。

→ 右図の「事務Ⅲ②」のケースにおいて、現行の提供①③と新規の提供を比較した場合、新たに行政機関Xに電子記録媒体で特定個人情報を提供することについて、現行の事務にないプロセスが発生しており、かつ、そのプロセスに係るリスク対策を講ずる必要があることから、事務のプロセス及び当該プロセスに係るリスク対策にも変更が生じることから、当然に「リスクを相当程度変動させるものではないと考えられる変更」に当たらないものと考えられます。

【ケース6】

- ・ 事務Ⅱで利用する特定個人情報ファイルiiについて、新たに特定個人情報ファイルの取扱いの委託を行うケース（2事例の比較）。



→ 左図の「事務Ⅱ①」のケースにおいて、現行の委託①と新規の委託を比較した場合、新たに届出書βのパンチ入力業務を委託先Xに委託することについて、事務のプロセス（例えば、委託先への届出書の提供方法、委託先での利用方法、委託先での保管・消去の方法など）に変更がなく、当該プロセスに係るリスク対策にも変更が生じない場合は、「リスクを相当程度変動させるものではないと考えられる変更」に当たると考えられます。

※ ただし、新たに届出書βのパンチ入力業務を委託先Xに委託するに当たり、評価実施機関の特定個人情報を取り扱うプロセス及び当該プロセスに係るリスク対策に変更が生じる場合は、評価実施機関は評価を再実施する必要があるため注意が必要です。

→ 右図の「事務Ⅱ②」のケースにおいて、現行の委託②と新規の委託を比較した場合、新たに届出書βのパンチ入力業務を委託先Yに委託することについて、現行の事務にないプロセスが発生しており、かつ、そのプロセスに係るリスク対策を講ずる必要があることから、事務のプロセス及び当該プロセスに係るリスク対策にも変更が生じることから、当然に「リスクを相当程度変動させるものではないと考えられる変更」に当たらないものと考えられます。

【ケース7】

- ・ 評価書の「I②事務の内容」の記載について、特定個人情報ファイルの取扱いが関係しない事務の変更が生じたことに伴い、記載内容の変更を行うケース。

→ 評価実施機関は、「I②事務の内容」において、評価対象事務について、事務全体の概要及び特定個人情報ファイルを使用して実施する事務の具体的な内容を記載しています。この事務について、特定個人情報ファイルの取扱いが関係しない事務の変更が発生した場合、それに伴って重要な変更の対象となる記載項目「I②事務の内容」の変更を行うことが想定されます。

この場合、特定個人情報ファイルの取扱いに関係しないものであることから、当該変更を行うことについて、現行の事務にない特定個人情報ファイルの取扱いのプロセスが新たに発生することはありません。したがって、特定個人情報ファイルを取り扱うプロセスに変更がなく、当該プロセスに係るリスク対策にも変更が生じないため、「リスクを相当程度変動させるものではない」と考えられる変更」に当たると考えられます。

※ ただし、特定個人情報ファイルの取扱いに関係しない事務の変更であっても、当該変更の結果として、特定個人情報ファイルの取扱いのプロセス及び当該プロセスに係るリスク対策に変更が生じる場合は、当然に「リスクを相当程度変動させるものではないと考えられる変更」に当たらないため、注意が必要です。

修正（赤字の記載を追記しています。）

Q第6の2（2）－3

「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明らかに軽減させる変更」とは具体的にはどのようなものでしょうか。技術進歩に伴うシステムの更新は通常リスクを軽減させることにはなりますが、重要な変更にあたらないということでしょうか。

(A)

- 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明らかに軽減させる変更とは、その変更によりリスクが軽減されることについて疑いの余地のない変更です。これらの場合は、既に公表している特定個人情報保護評価書を修正し、公表

することになります。具体的には、次のような例が考えられます。

【特定個人情報の漏えい等のリスクを明らかに軽減させる変更の事例】

- ・ ウイルス対策ソフトウェアのバージョンアップなどの単純な最新化
- ・ 監視カメラの設置台数や監視頻度の増加
- ・ 今まで行ってきた業務の一部の廃止・終了（評価書中の記載の削除）
- ・ 特定個人情報ファイルを取り扱う端末へのログインについて、現行のID・パスワードに加えて新たに生体認証を導入
- ・ ログの分析等の頻度の増加
- ・ 特定個人情報を含む機器等の廃棄について、委託先からの廃棄証明書の取得に加え、新たに職員の立会いを実施
- ・ 特定個人情報ファイルの取扱いを委託する委託先への監督の強化（取扱状況の報告及び立入検査の回数の増加等）
- ・ 再委託の終了（再委託先が行っていた業務を委託先による実施に変更）
- ・ 研修内容の充実や頻度の増加

- 一方、システムを全面的に入れ替える場合や事務手続を大幅に変更する場合などは、たとえその変更がリスク対策の強化を目的とするものであっても、評価実施機関が実施する事務又はシステム全体に複雑な影響を及ぼしかねないことから、むしろ重要な変更として、特定個人情報保護評価を再実施することが必要と考えられます。具体的には、セキュリティ対策の強化を目的の1つとするシステム更改や、オンライン環境のシステムのクラウド環境への移行等が考えられます。

新規

Q別表－2

委託先の追加は「重要な変更」に該当するのでしょうか。

(A)

- 既に特定個人情報保護評価を実施している事務について、新たに特定個人情報の取扱いに関する委託事項を追加する場合、重要な変更の対象項目である「委託件数」の欄に変更が生じ、また、新たに追加する特定個人情報の取扱いの委託の内容によっては、リスク対策に変更が生じることが考えられるため、原則としては重要な変更
- また、委託件数に変更が生じた場合や既に委託している内容に変更が生ずる場合は、単に「委託事項」の記載を追記するだけでなく、その新たな委託事項や変更後におけるプロセスやリスク対策によっては、重要な変更

「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」等への追記や変更が必要となることも想定されます。

- ただし、例えば、追加する委託事項の内容、委託の相手方が既存の委託事項と同一であり、既存の特定個人情報の取扱いの委託と事務のプロセス及びリスク対策に変更が生じない場合などは「リスクを相当程度変動させるものではないと考えられる変更」に該当し、重要な変更には該当しない可能性も考えられますので、新たに追加される委託事項に伴う特定個人情報ファイルを取り扱うプロセス及び当該プロセスに係るリスク対策の実態も踏まえ、適切に判断してください。

<緊急時の事後評価関係>

新規

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

(1) 新規保有時

規則第9条第2項の規定に基づき、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する必要がある場合は、特定個人情報ファイルを保有した後速やかに特定個人情報保護評価を実施（以下第6の3（1）において「事後評価」という。）することとされている。

ただし、特定個人情報保護評価の目的が事前対応による個人のプライバシー等の権利利益の侵害の未然防止及び国民・住民の信頼の確保であることを踏まえ、例えば、評価実施機関が新たに特定個人情報ファイルを保有する事務を行う場合において当該事務と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とき等、既に個人番号利用事務等として定着している事務を実施する場合は、当該特定個人情報ファイルの保有に一定の緊急性があるときであっても、原則どおり、特定個人情報ファイルを保有する前に特定個人情報保護評価を実施（以下第6の3（1）において「事前評価」という。）するものとする。

また、事前評価が困難である場合についても、特定個人情報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、可及的速やかに事後評価を行うものとする。

(2) 重要な変更

規則第9条第2項の規定に基づき、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に重要な変更を加える必要がある場合は、特定個人情報ファイルに重要な変更を加えた後速やかに特定個人情報保護評価を再実施（以下第6の3（2）において「事後評価」という。）することとされている。

ただし、特定個人情報保護評価の目的が事前対応による個人のプライバシー等の権利利益の侵害の未然防止及び国民・住民の信頼の確保であることを踏まえ、例えば、評価実施機関が特定個人情報ファイルに重要な変更を加える必要がある事務を行う場合において当該事務と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とき等、既に個人番号利用事務等として定着している事務を実施する場合は、当該特定個人情報ファイルに対して加える重要な変更に関し一定の緊急性があるときであっても、原則どおり、特定個人情報ファイルに重要な変更を加える前に特定個人情報保護評価を再実施（以下第6

の3（2）において「事前評価」という。）するものとする。

また、事前評価が困難である場合についても、特定個人情報保護評価を再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、可及的速やかに事後評価を行うものとする。

（解説）

特定個人情報保護評価について、特定個人情報ファイルを保有しようとする又は保有する特定個人情報ファイルに重要な変更を加えようとするときは、当該ファイルを保有する前又は重要な変更を加える前に、特定個人情報保護評価を実施又は再実施することを原則としています。

しかしながら、災害その他やむを得ない事由により、特定個人情報保護評価を実施せずに特定個人情報ファイルを保有せざるを得ない場合又は保有する特定個人情報ファイルに重要な変更を加えざるを得ない場合は、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後又は特定個人情報ファイルに重要な変更を加えた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、規則第9条第2項の規定を適用した特定個人情報ファイルに係る基礎項目評価書I9「規則第9条第2項の適用」の項目において、「適用した」にチェックを付けた上で、規則第9条第2項の規定を適用した理由を記載する必要があります（令和6年10月施行）。事前評価が困難であった理由を簡潔かつ具体的に説明してください。なお、この適用理由について、保護評価制度の趣旨に照らして疑義等がある場合には、個人情報保護委員会事務局からその記載内容について照会等を行う可能性があります。

なお、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、同様の事務を実施した実績が全くない個人番号利用事務等と比較して、「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、特定個人情報保護評価制度の趣旨又は目的を踏まえ、当該特定個人情報ファイルの保有等に一定の緊急性があるときであっても、原則どおり事前評価を実施するものとしております。

新規

Q第6の3-1

指針第6の3において規則第9条第2項（緊急時の事後評価）を適用することが認められないものとして定められている「既に個人番号利用事務等として定着している事務を実施する場合」とは、具体的にどのような場合を指すのでしょうか。

（A）

○ 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

報保護評価を実施した実績があるものであり、同様の事務を実施した実績が全くない個人番号利用事務等と比較して、「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、特定個人情報保護評価制度の趣旨又は目的を踏まえ、当該特定個人情報ファイルの保有等に一定の緊急性があるときであっても、原則どおり事前評価を実施するものとしております。

- 具体的には、例えば、第 164 回個人情報保護委員会（令和 3 年 1 月 26 日開催）において規則第 9 条第 2 項の規定の適用対象となり得ると整理された、公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律（令和 3 年法律第 38 号）第 10 条の規定に基づく特定公的給付の支給事務のうち、特定個人情報の本人の範囲が類似する事務を過去に反復して実施している（※）ものについては（例：低所得者世帯への給付事務、子育て世帯への給付事務等）、原則どおり事前評価を実施する必要があります。

※ 「過去に反復して実施している」とは、基本的には、過去 2 回以上実施している場合が考えられますが、それ以外の場合であっても、事務が実施された規模等から判断して「個人番号利用事務等として定着している」と判断される可能性があります。

- 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、特定個人情報保護評価を事前に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を保有等する前までに、委員会による審査・承認又は第三者点検及び国民又は住民等への意見聴取等の期間を確保することができないなど）には、規則第 9 条第 2 項の規定の適用対象となり得る場合も考えられます。

新規

Q 第 6 の 3 - 2

規則第 9 条第 2 項を適用することとした場合、特定個人情報保護評価の実施時期はどのように考えれば良いのでしょうか。

(A)

- 規則第 9 条第 2 項の規定を適用した場合には、当該特定個人情報ファイルを保有した後又は保有する特定個人情報ファイルに重要な変更を加えた後、速やかに（特定個人情報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）特定個人情報保護評価を実施することとされております。

具体的には、当該特定個人情報ファイルに係る事務がおおむね完了していたり、当該事務に係る臨時体制が解除され、平時の組織体制に戻ったりしているにもかかわらず

ならず、特定個人情報保護評価が実施されていない場合には、「速やかに特定個人情報保護評価を実施」していないものと考えられます。

<基礎項目評価書関係>

新規

2 評価項目

(1) 基礎項目評価書 (略)

Q第9の2(1)-1

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ファイルに記録された特定個人情報を保護するための主な措置の実施状況の評価について、どのような措置が実施されていれば、「十分である」等を選択することができますか。

(A)

- 講ずべきリスク対策は、事務やサービスの性質、システムの設計等によっても異なることから、講ずべき措置（リスク対策）を一律に示すことはできませんが、基礎項目評価において評価実施機関が自らの措置の実施状況の評価する際に参考となる一定の基準を示す観点から、次のとおり「典型的リスク対策（例）」をお示しします。ただし、「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。
- また、「特に力を入れている」を選択できる水準は、「十分である」を選択できる水準を満たした上で、さらに、評価実施機関独自の取組を実施している場合、選択することができるものと考えてください。
- なお、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ませんが、マイナンバーガイドラインに則り、必要な措置※¹、※²を講じる必要がありますので、留意してください。
 - ※1 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、取扱状況の把握及び安全管理措置の見直し
 - ※2 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
- また、次に列記する安全管理措置等を遵守することも前提となりますので、留意してください。
 - ・ 行政機関等…①番号法、②個人情報保護法等関係法令、③個人情報保護法ガイドライン、④事務対応ガイド、⑤政府機関の情報セキュリティ対策のための統

一基準等に準拠した各府省庁等における情報セキュリティポリシー、⑥情報提供ネットワークシステム等の接続規程、⑦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、等が示す安全管理措置等

- ・ 地方公共団体…上記に加え、⑧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

| リスク | 「十分である」を選択できる水準 |
|--|---|
| <p>目的外の入手が行われるリスクへの対策は十分か【情報提供 NWS 以外】</p> | <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</p> <p>＜典型的リスク対策（例）＞</p> <p>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。</p> |
| <p>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への対策は十分か</p> | <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</p> <p>＜典型的リスク対策（例）＞</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う。</p> |
| <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は十分か</p> | <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</p> <p>＜典型的リスク対策（例）＞</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。</p> <p>② アクセス権限の発効・失効の管理を行っている。</p> <p>③ アクセス権限の管理を行っている。</p> <p>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> |

| | |
|----------------------------------|--|
| <p>委託先における不正な使用等のリスクへの対策は十分か</p> | <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</p> <p><典型的リスク対策（例）></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> <p>① <u>委託先における情報保護管理体制の確認を行っている。</u></p> <p>② <u>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。</u></p> <p>③ <u>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。</u></p> <p>④ <u>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。</u></p> <p>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。</p> <p>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。</p> <p>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。</p> |
| <p>不正な提供・移転が行われるリスクへの対策は十分か</p> | <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</p> <p><典型的リスク対策（例）></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 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。</p> <p>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。</p> <p>③ 当該記録を定期的に及び随時に分析等するための体制を整備している。</p> |

| | |
|--|--|
| | <p>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。</p> |
| <p>目的外の入手が行われるリスクへの対策は十分か【情報提供NWS】</p> | <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</p> <p><典型的リスク対策（例）></p> <p>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。</p> <p>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。</p> |
| <p>不正な提供が行われるリスクへの対策は十分か【情報提供NWS】</p> | <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</p> <p><典型的リスク対策（例）></p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>（例）</p> <ul style="list-style-type: none"> ・ 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。 ・ 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。 ・ 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。 ・ 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。 |

| | |
|------------------------------------|--|
| <p>特定個人情報の漏えい・滅失・毀損リスクへの対策は十分か</p> | <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</p> <p><典型的リスク対策（例）></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 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）</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> |
| <p>人為的ミスが発生するリスクへの対策は十分か</p> | <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</p> <p><典型的リスク対策（例）></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」（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。</p> <p>（例）</p> |

| | |
|---------------------|--|
| | <ul style="list-style-type: none"> ・ 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。 ・ 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。 ・ 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。 ・ 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。 <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。</p> <p>※ 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：https://www.ppc.go.jp/legal/kensyuushiryoku/）。</p> <ul style="list-style-type: none"> ・ 「特定個人情報を取り扱う際の注意ポイント」 ・ 「特定個人情報の漏えい等の防止についてー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ー」 |
| <p>従業者に対する教育・啓発</p> | <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</p> <p><典型的リスク対策（例）></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」等を参照。</p> <ol style="list-style-type: none"> ① 研修計画を策定している。 ② 事務取扱者の適切な監督を行っている。 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"> ・ 事務取扱者への研修 ・ 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 ・ 保護責任者への研修 ・ 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）。 |

| |
|------------------------------------|
| ※ 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。 |
|------------------------------------|

新規

Q第9の2(1)-2

基礎項目評価書中「IV リスク対策」の「8. 人手を介在させる作業」、
「11. 最も優先度が高いと考えられる対策」の「判断の根拠」の欄には、
どのような内容を記載すれば良いでしょうか。

(A)

- Q第9の2(1)-1に示す「IV リスク対策」において「十分である」を選択できる水準(典型的リスク策(例))に記載の措置の内容を参考に、「課題が残されている」、「十分である」、「特に力を入れている」等の各選択肢を選択した理由を記載してください。
- なお、分量や記載内容について参考となるよう、各項目について次のとおり記載例をお示ししますので、こちらも参考としてください。

◆ 目的外の入手が行われるリスクへの対策は十分か【情報提供NWS以外】

[例1] 対象者からの申請に基づき特定個人情報入手するため、目的外の入手が行われることはない。その上で、事務に必要な情報入手することがないよう、申請書様式において、手続に必要な項目のみ記入するよう注意書きを記載している。また、●●システムへの入力に当たっては、必要な項目のみ入力できる仕様としているほか、作業者と別の者によるダブルチェックを経なければ、処理完了することができない仕組みとなっている。これらの対策を講じていることから、目的外の入手が行われるリスクへの対策は「十分である」と考えられる。

[例2] 特定個人情報の入手は、●●システムにより行うこととしているところ、あらかじめ●●システムにおいて対象者が同意した場合にのみ対象者の情報入手できるシステムとなっているため、対象者以外の情報入手することはない。また、●●については、専用線により●●より入手することとしているが、あらかじめ定められた様式に基づき、必要な情報のみを提供を受けることとしているため、不要な情報の入手が行われることはない。これらの対策を講じていることから、目的外の入手が行われるリスクへの対策は「十分である」と考えられる。

◆ **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**

[例] ●●システム(業務システム)において、担当業務に必要な範囲でのみ閲覧等が可能となるよう、アクセス制限を実施している。また、副本登録等に使用する統合宛名システムにおいても、各職員が閲覧等できる特定個人情報、担当業務に必要な範囲に制限しており、担当していない業務に関する特定個人情報を紐付けられることはない。これらの対策を講じていることから、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への対策は「十分である」と考えられる。

◆ **権限のない者(元職員、アクセス権限のない職員等)によって不正に利用されるリスク**

[例] ●●システムへのアクセスが可能な職員は、ICカードとパスワードによる認証によって限定しており、アクセス可能な職員の名簿を年度ごとに作成することで、アクセス権限の適切な管理を行っている。また、アクセスログを記録し、定期的に分析することで不正なアクセスがないことを確認している。これらの対策を講じていることから、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は「十分である」と考えられる。

◆ **委託先における不正な使用等のリスクへの対策は十分か**

[例] 委託先の選定に当たっては、委託先の設備、技術水準、経営状況、従業者に対する監督・教育の状況等を確認し、当該事業者において行政機関等と同等の安全管理措置を講じることができると判断した。また、契約書において、次の内容を義務付けている。

- ・ 組織体制の整備、漏えい等事案に対応する体制の整備及び安全管理措置の定期的見直しを行うこと。
- ・ 事務取扱担当者の監督・教育を行うこと。
- ・ 特定個人情報を取り扱う事務に従事する作業従事者を明確化するとともに、アクセス制御、アクセス者の識別と認証、外部からの不正アクセス等の防止、漏えい等の防止を行うこと。
- ・ 取扱規程(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のルール及び特定個人情報の消去のルールを含む)等を策定し、これに基づく運用を行うこと。
- ・ 事業所からの特定個人情報の持ち出しは禁止とすること。
- ・ 特定個人情報ファイルの取扱状況を記録し、定期的に分析・報告すること。
- ・ 再委託については原則として禁止し、やむを得ず再委託をする必要がある場合は、

委託元の承認を得ること。

- ・ 委託元が求めた場合、契約内容の遵守状況を報告すること。
- ・ 必要がある場合、委託元による委託先への実地の監査、調査等を行うこと。

これらの対策を講じていることから、委託先における不正な使用等のリスクへの対策は「十分である」と考えられる。

◆ 不正な提供・移転が行われるリスクへの対策は十分か【情報提供NWS以外】

[例] 特定個人情報の提供・移転に関するルールとして、●●市××規程を策定しており、当該規程に従った運用を行っている。また、システム利用者をID及びパスワードにより限定した上で、次の項目についてログの記録を行っており、この記録を定期的に分析している。

- ・ 特定個人情報ファイルの利用・出力状況の記録
- ・ 書類・媒体等の持ち運びの記録
- ・ 特定個人情報ファイルの削除・廃棄記録
- ・ 削除・廃棄を委託した場合、これを証明する記録等
- ・ 特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況（ログイン実績、アクセスログ等）の記録

これらの対策を講じていることから、不正な提供・移転が行われるリスクへの対策は「十分である」と考えられる。

◆ 目的外の入手が行われるリスクへの対策は十分か【情報提供NWS】

[例] ●●市側のシステムにおいては、情報提供ネットワークシステムで情報照会を行うことができる端末、職員、参照範囲が必要最小限となるよう、アクセス制限を設定している。また、アクセス権限の所持者には、事務取扱担当者の研修において離席時のログアウト徹底を呼びかけており、監査も実施している。これらの対策を講じていることから、目的外の入手が行われるリスクへの対策は「十分である」と考えられる。

◆ 不正な提供が行われるリスクへの対策は十分か【情報提供NWS】

[例] ●●市側のシステムにおいては、情報提供ネットワークシステムで情報提供を行うことができる端末、職員、参照範囲が必要最小限となるよう、アクセス制限を設定しており、アクセス権限の所持者には、事務取扱担当者の研修において離席時のログアウト徹底を呼びかけており、監査も実施している。副本登録は自動連携により行うこととしているところ、当該サーバーにはアクセス権限を設定している。また、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している。

また、マイナンバー登録事務は、「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」の留意事項を遵守している。

これらの対策を講じていることから、不正な提供が行われるリスクへの対策は「十分である」と考えられる。

◆ 特定個人情報の漏えい・滅失・毀損リスクへの対策は十分か

[例] ●市××情報セキュリティ規程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)に則り、漏えい・滅失・毀損を防ぐための物理的安全管理措置、技術的安全管理措置等を講じるとともに、特定個人情報ファイルの滅失・毀損が万が一発生した場合に備え、バックアップを保管している。

また、過去の滅失事案(書棚の整理の際に、職員から提出された特定個人情報が記録された申請書等を綴った文書ファイルの紛失が発覚した事案。年度末の不要文書の廃棄作業の際に、誤廃棄したと思われる。)を踏まえ、

- ・ 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。
- ・ USB メモリは、事前に許可を得た媒体のみ使用可能となるよう業務端末上制御を行っている。また、使用する場合は、暗号化、パスワードによる保護等を行うルールを周知徹底している。
- ・ 不要文書を廃棄する際は、特定個人情報が記録された書類等が混入していないか、複数人による確認を行ったことを確認すること。
- ・ 特定個人情報が記録された書類等を廃棄する場合には、廃棄した記録を保存すること。

を徹底する運用としている。

これらの対策を講じていることから、特定個人情報の漏えい・滅失・毀損リスクへの対策は「十分である」と考えられる。

◆ 人為的ミスが発生するリスクへの対策は十分か

[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。

- ・ 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
- ・ 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

- ・ 個人番号及び本人情報が記載された申請書の廃棄

等

[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。

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。

- ・ 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。
- ・ 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。
- ・ 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。
- ・ 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。
- ・ 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。

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。

[例③] (例②の内容に加え、)年に一度、業務プロセス全体について、漏えい等のリスクを軽減させるための仕組みを検討することとしており、令和●●年度は、オンライン申請受付の導入を決定した(これにより、手作業が介在する申請数が減少することが期待される)。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「特に力を入れている」と考えられる。

◆ 従業者に対する教育・啓発

[例] ●●市研修計画に従い、毎年度当初に、特定個人情報を取り扱う事務に従事する職員(会計年度職員を含む。)等に対し、教育研修を実施している。各研修においては受講確認を行い、未受講者に対しては再受講の機会を付与し、関係する全ての職員が研修を受講するための措置を講じている。また、庁内で漏えい等のヒヤリハット事案が発生した際等には、再発防止策等の周知や、必要な内部監査等を実施している。これらの対策を講じていることから、従業者に対する教育・啓発は「十分に行っている」と考えられる。

Q第9の2(1)-3

基礎項目評価書中「IV リスク対策」の「11. 最も優先度が高いと考えられる対策」について、選択肢全てが同列で重要度が高いと考えられる場合は、どうすれば良いですか。

(A)

- 評価を選択した「判断根拠」については、自由記述式で記載を求めることとしており、評価実施機関の事務負担に鑑み、「IV リスク対策」に記載の対策の中から最も優先度が高いと考えられる対策を一つ選び、記載することができることとしております。事務のプロセスや事務に使用する情報システムの仕様等に加え、これまで発生した個人情報に関する重大事故の内容等を踏まえ、該当するものを選択してください。
- なお、評価実施機関の判断で、①別添資料（様式任意）として複数の項目についての判断根拠を記載し提出・公表することや、②（しきい値判断の結果、基礎項目評価のみで足りると認められた事務についても）任意で重点項目評価又は全項目評価を実施することも可能です（第5の2、Q第5の2-4. -1を参照）。

＜地方公共団体の基幹業務システムの 統一・標準化関係＞

新規

Q他-2

地方公共団体の基幹業務システムの統一・標準化に向けた対応として、特定個人情報保護評価を行う場合、再実施が必要になるのでしょうか。修正での対応は認められないのでしょうか。

(A)

- 地方公共団体情報システムの標準化に関する法律（令和3年法律第40号。以下「標準化法」という。）では、政令で定める地方公共団体の情報システムの標準化の対象となる事務（以下「標準化対象事務」という。）について、地方公共団体が標準化基準に適合したシステム（以下「標準準拠システム」という。）を利用することを義務付けるとともに、地方公共団体にガバメントクラウドを活用して標準準拠システムを利用することを努力義務として課しています。
- 標準化対象事務のうち、特定個人情報保護評価の対象となる事務は、次の事務です（「*」の付されている事務は、個人番号の利用又は情報連携が認められていない事務であり、番号法第9条第2項に基づく条例を定めて個人番号を利用している場合を除いて、特定個人情報保護評価の実施義務はありません。）。

※ 令和6年4月1日時点の情報。

| | |
|--|---|
| <p>①児童手当</p> <ul style="list-style-type: none"> ・児童手当又は特例給付の支給に関する事務 <p>②子ども・子育て支援</p> <ul style="list-style-type: none"> ・子どものための教育・保育給付若しくは子育てのための施設等利用給付の支給、特定教育・保育施設、特定地域型保育事業者若しくは特定子ども・子育て支援施設等の確認又は地域子ども・子育て支援事業の実施に関する事務 <p>③住民基本台帳</p> <ul style="list-style-type: none"> ・住民基本台帳に関する事務 ・中長期在留者の住居地の届出又は外国人住民に係る住民票の記載等についての通知に関する事務 | <p>⑬健康管理</p> <ul style="list-style-type: none"> ・健康教育、健康相談その他の国民の健康の増進を図るための措置に関する事務 ・母性並びに乳児及び幼児に対する保健指導、健康診査、医療その他の措置に関する事務 ・予防接種の実施に関する事務 <p>⑭児童扶養手当</p> <ul style="list-style-type: none"> ・児童扶養手当の支給に関する事務 <p>⑮生活保護</p> <ul style="list-style-type: none"> ・生活保護の決定及び実施、就学自立給付金若しくは進学準備給付金の支給又は被保護者就労支援事業若しくは被保護者健康管理支援事業の実施に関する事務 |
|--|---|

| | |
|--|--|
| <ul style="list-style-type: none"> ・ 特別永住者の住居地の届出に関する事務 ・ 個人番号の指定に関する事務 ・ 住居表示に係る事項の通知に関する事務（＊） <p>④戸籍の附票（＊）</p> <ul style="list-style-type: none"> ・ 戸籍の附票に関する事務（＊） <p>⑤印鑑登録（＊）</p> <ul style="list-style-type: none"> ・ 印鑑に関する証明書の交付に関する事務（＊） <p>⑥選挙人名簿管理（＊）</p> <ul style="list-style-type: none"> ・ 選挙人名簿又は在外選挙人名簿に関する事務（＊） ・ 投票人名簿又は在外投票人名簿に関する事務（＊） <p>⑦⑧⑨⑩ 地方税</p> <ul style="list-style-type: none"> ・ 個人の道府県民税（都民税を含む。）若しくは市町村民税（特別区民税を含む。）、法人の市町村民税、固定資産税、軽自動車税、都市計画税又は森林環境税の賦課徴収に関する事務（固定資産課税台帳の登録事項等の通知に関する事務） <p>⑪戸籍（＊）</p> <ul style="list-style-type: none"> ・ 戸籍に関する事務（＊） <p>⑫就学（＊）</p> <ul style="list-style-type: none"> ・ 就学義務の猶予若しくは免除又は就学困難と認められる学齢児童又は学齢生徒の保護者に対する実用的な援助に関する事務（＊） ・ 学齢簿に関する事務（＊） ・ 就学時の健康診断に関する事務（＊） | <p>⑬障害者福祉</p> <ul style="list-style-type: none"> ・ 障害児通所給付費、特例障害児通所給付費、高額障害児通所給付費、肢体不自由児通所医療費、障害児相談支援給付費、特例障害児相談支援給付費、特別児童扶養手当、障害児福祉手当若しくは特別障害者手当の支給、障害者手帳若しくは精神障害者保険福祉手帳の交付、知的障害者の判定等に関する事務 ・ 特別児童扶養手当、障害児福祉手当又は特別障害者手当の支給に関する事務 ・ 福祉手当の支給に関する事務 ・ 自立支援給付の支給に関する事務 <p>⑭介護保険</p> <ul style="list-style-type: none"> ・ 介護保険に関する事務 （※ 介護保険法施行法第11条に基づく事務については保護評価対象外。） <p>⑮国民健康保険</p> <ul style="list-style-type: none"> ・ 被保険者の資格の取得若しくは喪失、保険給付の実施又は保険料の賦課及び徴収に関する事務 <p>⑯後期高齢者医療</p> <ul style="list-style-type: none"> ・ 被保険者の資格の取得若しくは喪失又は保険料の徴収に関する事務 <p>⑰国民年金</p> <ul style="list-style-type: none"> ・ 被保険者の資格の取得若しくは喪失、年金である給付若しくは一時金の支給、賦課保険料の納付又は保険料の免除、特別障害給付金、年金生活者支援給付金の支給に関する事務 |
|--|--|

※上記表の、①～⑳の番号は、地方公共団体情報システムの標準化に関する法律第二条第一項に規定する標準化対象事務を定める政令（令和4年政令第1号）の号番号。

<基礎項目評価書について>

- 基礎項目評価書の記載項目には、重点項目評価書や全項目評価書にあるような、特定個人情報ファイルを取り扱うシステムの詳細や、特定個人情報の種類・入手方法・提供方法の詳細等について記載する項目はないものの、標準準拠システムへの移行に当たって生じる変更（特定個人情報の保管場所等）を踏まえてリスク対策を見直した結果、当該リスク対策の実施状況の評価（「IVリスク対策」における自己評価やその根拠）を修正する必要があることが考えられます。
- * なお、上記見直しと併せて、次の2点についても、対応が必要となりますので、御留意ください（重点・全項目評価書と併せて提出する基礎項目評価書についても同様です）。
 - ・ Q第9の2（1）－1において、「IV リスク対策」における自己評価の基準を示しておりますので（令和6年4月1日最終改正版から追加）、この基準に照らして自己評価の見直しを行ってください。
 - ・ 令和6年10月1日から施行される新様式を用いた基礎項目評価書（「IV リスク対策」に「人手を介在させる作業」、「最も優先度が高いと考えられる対策」が追加されました）について、全ての評価実施機関が令和7年度末までに再提出する必要があります。

<重点・全項目評価書について>

- 標準準拠システムの移行に伴って特定個人情報に関する機能の改修等を行う場合は、特定個人情報保護評価の再実施（又は修正）が必要です。現行システムから標準準拠システムへの移行に当たっては、システムを全面的に入れ替えるケースや、事務手続を大きく変更するケースも考えられるため、重点項目評価書や全項目評価書については、原則として修正ではなく再実施が必要となるものと考えられます。
- 特に、標準準拠システムの利用において、ガバメントクラウドへの移行を行う業務システムについては、特定個人情報保護評価を再実施する必要があります。これは、ガバメントクラウドへの移行においては、委託先の事業者に変更がない場合であっても、
 - ・ サーバー等が、クラウド事業者が保有・管理する環境に設置されることとなり、特定個人情報の保管場所に変更が生じる（物理的・技術的な対策について、クラウド事業者が実施することとなる）
 - ・ 従来、職員が業務で利用していたパソコン等の操作端末からクラウドサービスに存在するシステムへ、接続する通信経路やアクセス制御等に変更が生じる
 - ・ 既存のシステム環境から特定個人情報ファイルを抽出し、新システムへデータを移し替える作業が発生する
 - ・ 既存のシステム環境に保管されていた特定個人情報の消去、機器の廃棄を実施

する

- ・ 新たに共同利用方式を選択する場合、これまで制限を行っていた委託先における特定個人情報の取扱いについて、委託先に一括の運用管理を委任することとなることから、委託先や委託内容等に変更が生じる

場合等が考えられ、漏えい、滅失等が起こらないようにそれらの変更に対応したリスクを識別・評価し、リスクを軽減させるために講ずる措置を評価書に記載する必要があり、これらの変更は、特定個人情報保護評価の再実施が義務付けられる「重要な変更」に該当するためです。

- ガバメントクラウドに関する特定個人情報保護評価書の記載については、ガバメントクラウドを調達したデジタル庁が提供する記載例を参考にした上で、ガバメントクラウド事業者が提供するクラウド上の基盤及び接続に関する部分以外の部分について（具体的には、委託に関する項目について、委託先が行うガバメントクラウドへ移行する際のデータ抽出、移行、廃棄に関するリスク対策や、運用管理に係る委託内容の変更等）、各地方公共団体において追記を行う必要があります。

※ クラウドサービスへの利用に関しては、第6の1-5、第9の1-5、Q第9の1-6も参照してください。

- 実施時期については、各地方公共団体におけるガバメントクラウドや標準準拠システムへの移行の順序・タイミングに応じて、それぞれの内容について、次のタイミングまでに特定個人情報保護評価を実施してください。

- ・ ガバメントクラウドへの移行に係る内容について：

ガバメントクラウドへ副本データを移行するまで

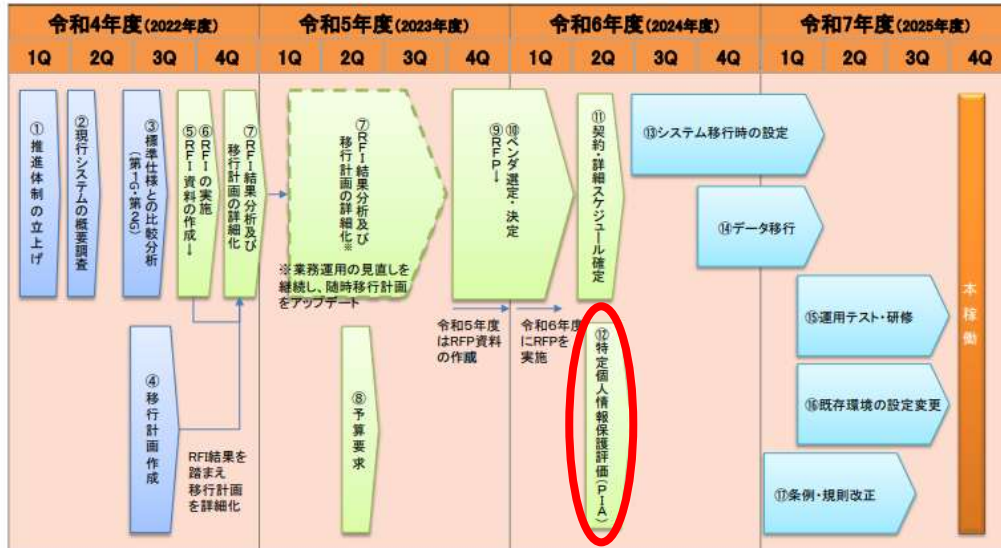
- ・ 標準準拠システムへの移行について（後述のモデルスケジュール例も参照）：システム等を稼働させるサーバー等へのパラメータ設定等の適用を実施する前まで（パラメータ設定等の適用が行われることにより、サーバー等に直接的に変更を加えることになるため、これをプログラミングに相当するものとして考えることとしています。）

<標準化モデルスケジュール例^{※1}>

※1 総務省公表資料「自治体情報システムの標準化・共通化に係る手順書【第3.0版】」より引用

図表 14 令和4年度から移行準備を行う場合のスケジュール例

PMO ツールで集計したところ、令和4年 11 月 1 日時点で、①推進体制の立上げについて概ね半数の団体で着手済み（ステップ 1-1「推進体制案の作成」について、完了済み 38.32%、作業中 13.72%となっている。）であり、未着手の自治体においては本図表を踏まえ、早急に移行作業を開始することが望ましい。



本例において、⑨RFP、⑩ベンダ選定・決定を実施する想定としているが、Bパターンを選択し、当該作業を実施しない場合は、スケジュールを前倒しすることも可能と推察。また、移行フェーズの所用期間はベンダによって異なるため、各自治体において早期に、ベンダの想定移行スケジュールを確認することが望ましい。

- なお、基礎項目評価書の説明中（*）に記載した内容について、重点・全項目評価書と併せて提出する基礎項目評価書についても、対応が必要となります。

<標準準拠システムへの移行に伴う影響（例※²）>

| 標準化等に伴い生じる取扱いの変更 | 基礎項目評価書上影響する箇所 | 全項目評価書上影響する箇所 |
|--|---|---|
| 事務で利用する情報システムの変更 | ・システムの名称 | ・システムの名称、機能、他のシステムとの接続 |
| 標準準拠システムへの移行（標準仕様に基づく業務運用見直し）に伴う事務のプロセスの変更 | ・事務の概要 | ・事務の内容（Ⅰ 1） ・本特定個人情報のファイルの本人の範囲、記録される項目（Ⅱ 2） |
| 委託先・委託内容の変更 | ・委託先における不正な使用等のリスク対策 | ・特定個人情報ファイルの取扱いの委託（Ⅱ 4、Ⅲ 4） |
| システム更改に伴う特定個人情報へのアクセス制限範囲の変更 | ・目的外の入手が行われるリスク対策、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 ・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 | ・特定個人情報の入手（Ⅲ 3） ・特定個人情報の使用（Ⅲ 3） |
| 特定個人情報の提供・移転（記録）の方法の変更 | ・不正な提供・移転が行われるリスクへの対策 | ・特定個人情報の提供・移転（Ⅲ 5） |
| 特定個人情報を取り扱う環境（データの保管場所を含む）の変更（オンプレミス環境からガバメントクラウドへの移行など） | ・特定個人情報の漏えい・滅失・毀損リスクへの対策 | ・特定個人情報の保管・消去（Ⅱ 6、Ⅲ 7） |

※2 上記の記載は、標準準拠システムの移行に当たって生じることが想定される一般的な変更の例であり、全ての変更が網羅されているものではありません。現行のシステムや標準準拠システムの仕様によって、上記以外の変更が

生じることも考えられ、その場合、当該変更に応じたリスク対策を検討する
必要があります。

以 上