特定個人情報保護評価指針の解説

平成 26 年 4 月 20 日

（令和４年４月１日最終改正）

個人情報保護委員会

この解説は、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（平成 25 年法律第 27 号。以下「番号法」という。）第 27 条第１項に基づく特定個人情報保護評価指針に関して問合せの多い事項について、個人情報保護委員会事務局で回答した事例等のうち特定個人情報保護評価を実施するに当たり参考となるものの要旨を掲載したものです。

この解説は、必要に応じて更新することを予定しています。

目次

○　ＱＡの目次

この指針は、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（平成 25 年法律第 27 号。以下「番号法」という。）第 27 条第１項の規定に基づく指針であって、行政機関の長等が、番号法第 28 条の規定に基づき特定個人情報の漏えいその他の事態の発生の危険性及び影響に関する評価（以下「特定個人情報保護評価」という。）を自ら実施し、これらの事態の発生を抑止することその他特定個人情報を適切に管理するために講ずべき措置を定めるものである。

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

番号法によって導入される社会保障・税番号制度（以下「番号制度」という。）は、社会保障制度、税制、災害対策その他の分野における行政運営の効率化を図り、国民にとって利便性の高い、公平・公正な社会を実現するための社会基盤として導入されるものである。一方で、番号制度の導入に伴い、個人のプライバシー等の権利利益の保護の観点からは、国家による個人情報の一元管理、特定個人情報の不正追跡・突合、財産その他の被害等への懸念が示されてきた。個人情報の適正な取扱いという観点からは、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）等の個人情報保護法令が整備されているが、これに加え、番号制度においては、このような懸念に対して、個人情報保護委員会（以下「委員会」という。）による監視・監督その他の制度上の保護措置を定めるとともに、特定個人情報の提供には原則として情報提供ネットワークシステムを使用するなどシステム上の安全措置を講ずることとしている。

特定個人情報保護評価は、このような番号制度の枠組みの下での制度上の保護措置の１つであり、特定個人情報ファイルの適正な取扱いを確保することにより特定個人情報の漏えいその他の事態の発生を未然に防ぎ、個人のプライバシー等の権利利益を保護することを基本理念とするものである。特定個人情報保護評価の実施により、評価実施機関が個人情報保護法令の趣旨を踏まえ、より主体的な措置を講ずることで、個人のプライバシー等の権利利益の保護につながることが期待される。

２　特定個人情報保護評価の目的

特定個人情報保護評価は、次に掲げることを目的として実施するものである。

（１）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

情報の漏えい、滅失、毀損や不正利用等により個人のプライバシー等の権利利益が一度侵害されると、拡散した情報を全て消去・修正することが困難であるなど、その回復は容易でない。したがって、個人のプライバシー等の権利利益の保護のためには、事後的な対応ではなく、事前に特定個人情報ファイルの取扱いに伴う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分析し、このようなリスクを軽減するための措置を講ずることが必要である。特定個人情報保護評価は、このような事前対応の要請に応える手段であり、これにより個人のプライバシー等の権利利益の侵害を未然に防止することを目的とするものである。

事前対応を行うことで、事後の大規模なシステムの仕様変更を防ぎ、不必要な支出を防ぐことも期待される。

（２）国民・住民の信頼の確保

番号制度の導入に対して示されてきた個人のプライバシー等の権利利益が侵害されることへの懸念を払拭する観点からは、特定個人情報ファイルを取り扱う者が、入手する特定個人情報の種類、使用目的・方法、安全管理措置等について国民・住民に分かりやすい説明を行い、その透明性を高めることが求められる。特定個人情報保護評価は、評価実施機関が、特定個人情報ファイルの取扱いにおい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自ら宣言し、どのような措置を講じているかを具体的に説明することにより、国民・住民の信頼を確保することを目的とするものである。

３　特定個人情報保護評価の内容

特定個人情報保護評価は、評価実施機関が、特定個人情報ファイルを取り扱う事務における当該特定個人情報ファイルの取扱いについて自ら評価するものである。評価実施機関は、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場合は、当該特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に与え得る影響を予測した上で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分析し、このようなリスクを軽減するための適切な措置を講じていることを確認の上、基礎項目評価書、重点項目評価書又は全項目評価書（以下「特定個人情報保護評価書」と総称する。）において自ら宣言するものである。

特定個人情報保護評価は、諸外国で採用されているプライバシー影響評価（Privacy Impact Assessment: PIA）に相当するものであり、個人のプライバシー等の権利利益の保護のために必要最小限の措置を講じているか否かについてのチェックにとどまらず、評価実施機関が自らの取組につい

て積極的、体系的に検討し、評価することが期待される。
　また、評価実施機関には、個人情報又はプライバシーの保護に関する技術の進歩、社会情勢の変化等に対応し、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軽減するための取組を継続的に実施することが期待される。

４　特定個人情報保護評価の実施体制
　評価実施機関は、特定個人情報保護評価を適切に実施するための体制整備を行うことが望ましい。例えば、①複数の特定個人情報保護評価書を作成する評価実施機関において、部署横断的な特定個人情報保護評価書の内容の確認等を行う総括的な部署を設置すること、②個人情報の取扱いに関して、部署横断的・専門的な立場から各部署・従業員の指導等を行う個人情報の取扱いに関する責任者を設置すること等が考えられる。

Q第１の１－１
　特定個人情報保護評価は個人のプライバシー等の権利利益を保護することを基本理念としていますが、これはどのような考え方なのでしょうか。

（Ａ）

○　番号制度は、行政運営の効率化を図り、国民にとって利便性の高い、公平・公正な社会を実現するための社会基盤として導入されるものですが、その導入に対しては、国家による個人情報の一元管理、特定個人情報の不正追跡・突合、財産その他の被害等への懸念が示されてきたところです。

○　番号法は、これらの懸念に対し、個人情報の保護に関する法律（以下「個人情報保護法」という。）の特別法として、制度上の保護措置等を規定しており、特定個人情報保護評価も制度上の保護措置の１つです。

○　個人情報保護法第１章から第３章までは、個人情報保護法制の基本法制として、民間事業者、行政機関、独立行政法人等のみならず、地方公共団体等にも適用されますが、同法は、個人情報は個人の人格尊重の理念の下に慎重に取り扱われるべきものであるとの基本理念に基づき、プライバシーの保護を含めた個人の権利利益を保護することを目的としています（同法第１条及び第３条並びに個人情報の保護に関する基本方針１（２）①参照）。

○　このようなことから、特定個人情報保護評価は、個人情報保護法を基本法制とする、個人情報の保護に関する一般法に定められた、プライバシーの保護を含めた個人の権利利益の保護（「個人のプライバシー等の権利利益の保護」）を基本理念としています。

○　特定個人情報保護評価の実施により、評価実施機関が個人情報保護法等の法令の

趣旨を踏まえ、より主体的な措置を講ずることで、個人のプライバシー等の権利利益の保護につながることが期待されます。

Ｑ第１の４－１

「評価実施機関は、特定個人情報保護評価を適切に実施するための体制整備を行うことが望ましい」としているのは、どのような理由なのでしょうか。また、体制整備の具体例が挙げられていますが、その他にどのような体制整備を行うことが考えられるのでしょうか。

（Ａ）

○　特定個人情報保護評価の適切な実施を確保するためには、評価実施機関全体として、特定個人情報保護評価書が評価実施機関のリスク対策の実態を正確に反映しているか、誰がどのタイミングで特定個人情報保護評価を実施する必要があるか、重大事故等の評価実施機関全体の特定個人情報保護評価に影響を与え得る事態が発生していないか等を把握し、管理すること、さらには各評価実施者・評価実施部署が適切に評価を実施するためのノウハウを共有することが重要です。このため、評価実施者・評価実施部署以外の者又は部署が特定個人情報保護評価に携わる体制を整備することが望ましいと考えられます。

○　指針に挙げられている具体例の他に、総括部署を設置することが難しい場合は、事務の担当部署以外の個人情報や情報セキュリティを担当する部署が特定個人情報保護評価書の内容の確認を行うことが考えられます。

○　また、専門的知識を有する者を新たに個人情報の取扱いに関する責任者として設置することが難しい場合は、評価実施機関全体の個人情報の管理を行う既存の責任者が、特定個人情報保護評価に関する取りまとめや助言を行う役割も担うことが考えられます。

○　これらの部署や責任者の設置について、責任者のみを設置するケースや責任者の下に総括部署を設置するケースなど、評価実施機関内での位置づけには様々なパターンがあり得ると考えられます。どのような体制を整備することが適切であるかは、評価実施機関の規模や組織体制、特定個人情報を取り扱う事務の数や内容等様々な要素によって変わるものです。これらの要素を踏まえて、特定個人情報保護評価の適切な運用を確保するために望ましい体制の在り方を各評価実施機関において適切に判断してください。

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　評価実施機関　番号法第 28 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８号に規定する情報照会者及び情報提供者並びに同条第９号に規定する条例事務関係情報照会者及び条例事務関係情報提供者）をいう。

２　行政機関等　評価実施機関のうち、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（規則第２条第３号に規定する地方公共団体等（以下単に「地方公共団体等」という。）を除く。）をいう。

３　特定個人情報保護評価計画管理書　規則第３条に規定する、評価実施機関が保有する特定個人情報ファイルについての特定個人情報保護評価の計画、実施状況等を記載し、又は記録した書面又は電磁的記録をいう。

４　全項目評価書　番号法第 28 条第１項各号に掲げる事項を評価した結果を記載し、又は記録した書面又は電磁的記録（行政機関等においては番号法第 28 条第４項及び規則第８条の規定、地方公共団体等においては規則第７条第６項の規定に基づく公表の対象となるもの）をいう。

５　情報連携　行政機関の長等の間の情報提供ネットワークシステムを使用する特定個人情報の提供の求め又は提供をいう。

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を漏えい、滅失又は毀損した場合であって、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って、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（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。

７　特定個人情報の入手　特定個人情報ファイルに記録されることとなる特定個人情報を、特定個人情報保護評価の対象となる事務において用いるために取得することをいう。

８　特定個人情報の使用　特定個人情報ファイルに記録された特定個人情報を特定個人情報保護評価の対象となる事務において用いることをいう。

９　特定個人情報の移転　評価実施機関内において、特定個人情報ファイルに記録された特定個人情報を特定個人情報保護評価の対象となる事務以外

の事務を処理する者の使用に供することをいう。

10　システム用ファイル　電子計算機で取り扱われる特定個人情報ファイルであって、要件定義、基本設計、詳細設計、プログラミング及びテストの段階を経て運用に供される電子情報処理組織で保有される特定個人情報ファイルをいう。

11　その他の電子ファイル　電子計算機で取り扱われる特定個人情報ファイルであって、システム用ファイル以外のものをいう。

（解説）

番号法、規則及びこの指針において規定されている主な定義・用語は、次のとおりです。

用　　語	定　　義
評価実施機関 （指針第２の１）	番号法第 28 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８号に規定する情報照会者及び情報提供者並びに番号法第 19 条第９号に規定する条例事務関係情報照会者及び条例事務関係情報提供者）
行政機関の長等 （番号法第２条第 14 項）	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８号に規定する情報照会者及び情報提供者並びに番号法第 19 条第９号に規定する条例事務関係情報照会者及び条例事務関係情報提供者
地方公共団体等 （規則第２条第３号）	行政機関の長等（評価実施機関）のうち、地方公共団体の機関及び地方独立行政法人
行政機関等 （指針第２の２）	評価実施機関のうち、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（規則第２条第３号に規定する地方公共団体等を除く。）
独立行政法人等 （番号法第２条第２項）	個人情報保護法第２条第９項に規定する独立行政法人等
特定個人情報保護評価計画管理書 （指針第２の３）	規則第３条に規定する、評価実施機関が保有する特定個人情報ファイルについての特定個人情報保護評価の計画、実施状況等を記載し、又は記録した書面又は電磁的記録

用　　語	定　　義
基礎項目評価書 （規則第２条第１号）	行政機関の長等（評価実施機関）が、指針で定めるところにより、番号法第28条第１項第１号から第４号までに掲げる事項及び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を評価した結果を記載し、又は記録した書面又は電磁的記録
重点項目評価書 （規則第２条第２号）	行政機関の長等（評価実施機関）が、指針で定めるところにより、番号法第 28 条第１項第１号から第６号までに掲げる事項及び特定個人情報ファイルの取扱いにより個人の権利利益を害する可能性のある要因の概要を評価した結果を記載し、又は記録した書面又は電磁的記録
全項目評価書 （指針第２の４）	番号法第 28 条第１項各号に掲げる事項を評価した結果を記載し、又は記録した書面又は電磁的記録（行政機関等においては番号法第 28 条第４項及び規則第８条の規定、地方公共団体等においては規則第７条第６項の規定に基づく公表の対象となるもの）
情報連携 （指針第２の５）	行政機関の長等の間の情報提供ネットワークシステムを使用する特定個人情報の提供の求め又は提供
重大事故 （指針第２の６）	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を漏えい、滅失又は毀損した場合であって、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って、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（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。）（※）
個人情報 （番号法第２条第３項）	個人情報保護法第２条第１項に規定する個人情報
特定個人情報 （番号法第２条第８項）	個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報
特定個人情報の入手 （指針第２の７）	特定個人情報ファイルに記録されることとなる特定個人情報を、特定個人情報保護評価の対象となる事務において用いるために取得すること
特定個人情報の使用 （指針第２の８）	特定個人情報ファイルに記録された特定個人情報を特定個人情報保護評価の対象となる事務において用いること
特定個人情報の移転 （指針第２の９）	評価実施機関内において、特定個人情報ファイルに記録された特定個人情報を特定個人情報保護評価の対象となる事務以外

用　　語	定　　義
	の事務を処理する者の使用に供すること
特定個人情報の提供	特定個人情報を評価実施機関以外の者に供与すること
個人情報ファイル （番号法第２条第４項）	個人情報保護法第 60 条第２項に規定する個人情報ファイルであって行政機関等（個人情報保護法第２条第 11 項に規定する行政機関等をいう。）が保有するもの又は個人情報保護法第 16 条第１項に規定する個人情報データベース等であって行政機関等以外の者が保有するもの
特定個人情報ファイル （番号法第２条第９項）	個人番号をその内容に含む個人情報ファイル
システム用ファイル （指針第２の 10）	電子計算機で取り扱われる特定個人情報ファイルであって、要件定義、基本設計、詳細設計、プログラミング及びテストの段階を経て運用に供される電子情報処理組織で保有される特定個人情報ファイル
その他の電子ファイル （指針第２の 11）	電子計算機で取り扱われる特定個人情報ファイルであって、システム用ファイル以外のもの
クラウドサービス	事業者等によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるもの

（※）「重大事故」と「従業者」が記載されている箇所は、次のとおりです。

〇「重大事故」

・指針

第２の６、第５の２、第６の２（２）及び（３）、別表

・指針の解説

第２の解説、第５の２の解説、第５の３（１）の解説、第５の４の解説、第６の２（１）～（４）の解説

・ＱＡ

Ｑ第１の４－１、Ｑ第２の６－１、Ｑ第２の６－２、Ｑ第２の６－３、Ｑ第２の６－４、Ｑ第２の６－５、Ｑ第５の２－３.－１、Ｑ第５の２－３.－２、Ｑ第６の２（２）－５、Ｑ第６の２（３）－３、Ｑ第６の２（３）－４、Ｑ第６の２（３）－５、Ｑ第６の２（４）－１、Ｑ別表－１

〇「従業者」

・指針

第２の６、第５の２、第９の２（１）～（３）

・指針の解説

第２の解説

・ＱＡ

Ｑ第２の６－２、Ｑ第５の２－２．－１、Ｑ第５の２－２．４

Ｑ第２の２－１

規則及び指針における「行政機関の長等」「行政機関等」「地方公共団体等」の違いはどのようなものでしょうか。

（Ａ）

〇　「行政機関の長等」は番号法第２条第 14 項の規定に基づくものであり、特定個人情報保護評価の実施が義務付けられる全ての者を指します。

〇　「行政機関等」は、指針に定義が置かれており、「行政機関の長等」のうち「地方公共団体等」（地方公共団体の機関及び地方独立行政法人）を除いたものをいいます。

特に記載のない場合、本解説における「行政機関等」は、指針の定義によります。個人情報保護法における「行政機関等」の定義については、本解説第４の３を参照してください。

〇　「地方公共団体等」は規則に定義が置かれており、「行政機関の長等」のうち地方公共団体の機関及び地方独立行政法人のみをいいます。

Ｑ第２の６－１

重大事故の定義中に「個人情報」とありますが、「特定個人情報」ではないのでしょうか。

（Ａ）

〇　特定個人情報保護評価において、「重大事故」が登場するのは、次の３点です。

①　しきい値判断項目「評価実施機関における特定個人情報に関する重大事故の発生の有無」

②　重点項目評価書　様式　Ⅲ７リスク「②個人情報に関する重大事故の発生」

③　全項目評価書　様式　Ⅲ７リスク１「⑨個人情報に関する重大事故の発生」

〇　①しきい値判断項目については、重大事故の対象を、個人番号を含まない個人情報ではなく、特定個人情報に限定しています。

これは、特定個人情報保護評価は、特定個人情報の適正な取扱いを確保することを目的とするものであり、しきい値判断項目としては、特定個人情報に関する重大事故の発生の有無とすることが適当であるとしたものです。また、対象を個人情報とした場合、特定個人情報保護評価の導入当初に実施するしきい値判断において、制度が導入される以前に発生した事故の影響を受けることとなりますが、これについては各評価実施機関において当該事故について対応が既に講じられていることが想定され、改めて当該事故を判断項目とすることは適当でないとしたものです。指針では、しきい値判断項目に関しては「特定個人情報に関する」重大事故と明記しています。

○　②重点項目評価書及び③全項目評価書の記載事項としての重大事故については対象を個人情報としています。

これは、番号法第 28 条第 1 項第 3 号において、「過去の個人情報ファイルの取扱いの状況」を評価書の記載事項としていることを反映したものです。なお、重大事故の発生自体が、②重点項目評価又は③全項目評価の再実施が必要となる重要な変更に直ちに該当するものではありませんが、重大事故の発生に伴い特定個人情報ファイルを取り扱う際のリスク対策を見直す場合は、重要な変更に該当し、②重点項目評価又は③全項目評価の再実施が必要となります。また、特定個人情報に関する重大事故の発生によりしきい値判断の結果が変わり、新たに②重点項目評価又は③全項目評価を実施するものと判断される場合は、②重点項目評価又は③全項目評価の実施が必要となります。

Ｑ第２の６－２

重大事故の定義中に「評価実施機関の従業者」とありますが、「従業者」とは具体的にどのような者を指すのでしょうか。正規職員だけでなく、非正規職員やアルバイトも含むのでしょうか。

（Ａ）

○　従業者には、契約形態にかかわらず、役員、使用人その他の者で、特定個人情報保護評価の対象となる事務に現に従事する者の全てが含まれます。したがって、行政機関、独立行政法人等、地方公共団体等においては、正規職員のみならず非正規職員、アルバイト等も含まれ、民間事業者においては、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれます。

Q第２の６－３

重大事故の定義中に「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」とありますが、具体的にどのようなものでしょうか。

（Ａ）

○　特定個人情報に関する重大事故を発生させると、当該重大事故が発生した事務のみならず評価実施機関のほかの事務のしきい値判断にも影響を与え、しきい値判断の結果が変わって新たに重点項目評価又は全項目評価の実施が義務付けられる場合には、評価を再実施することとなります。これは、重大事故を発生させた評価実施機関が、当該事務のみならず、全体として特定個人情報の取扱いについて見直す必要があると考えられるためです。

○　しかし、配送事故等には専ら配送業者の責任による事故など、評価実施機関の責めに帰さない事由によるものも想定され、これについては、評価実施機関において再発防止策を策定することは困難であると考えられます。そのため、評価実施機関の責めに帰さない事由によるものについては、重大事故の定義から除外することとしています。

○　ただし、配送業者による事故の場合であっても、（特定）個人情報や事務の性質等を踏まえ、より慎重な配送方法を選択することが求められるにもかかわらず、簡易な配送方法を選択したことにより事故が発生した場合など、評価実施機関が（特定）個人情報の取扱いに関してより慎重な措置を講じていれば事故の未然防止が図られたと考えられるものは重大事故に当たると考えられます。

○　評価実施機関の責めに帰さない事故のその他の例としては、通常想定し難い規模の自然災害（大地震等）による（特定）個人情報の滅失、毀損等が考えられます。

○　なお、ネットワークによる（特定）個人情報の流出は、特定個人情報保護評価の対象となるシステムそのものに起因するものであり、大量の情報が瞬時に流出する場合や、一度拡散した情報を消去・修正することが困難な場合もあることから、評価実施機関においてそのリスクを把握して対策を講ずべきであり、一般的に、重大事故に該当すると考えられます。

○　また、パソコンやUSBメモリ等の盗難等については、一般的に、評価実施機関の責めに帰す場合が多く、重大事故に該当する場合が多いと考えられます。ただし、例えば、評価実施機関が特定個人情報を外部のデータセンターに委託して保管し、評価実施機関が契約により当該データセンターを監督するとともに、当該データセンターが十分なセキュリティ対策を講じているにもかかわらず、何者かが当該データセンターに侵入し、当該データセンターの情報を保管しているサーバ等を持ち去るといったような盗難である場合は、評価実施機関の責めに帰さない事由によるものと考えられ、重大事故には該当しないと考えられます。

Q第２の６－４

（特定）個人情報を取り扱う事務を委託している場合、重大事故には委託先での事故は含まれるのでしょうか。

（Ａ）

○　委託先での事故も含まれます。

個人情報保護法第 66 条に基づき、行政機関及び独立行政法人等は、保有個人情報について安全管理措置義務を負っていることから、個人情報を取り扱う事務を委託する場合においても、当然ながら、受託者に対し必要かつ適切な監督を行う義務を負うこととなります。また、個人情報保護法に規定された個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合、個人情報保護法第 25 条に基づき、その委託した個人データの安全管理が図られるよう、受託者に対し必要かつ適切な監督を行う義務を負っています。

さらに、番号法では第 11 条において、特定個人情報に関する委託先の監督義務が規定されており、これらに基づき、重大事故には、委託先における（特定）個人情報の事故も含まれることとなります。

Q第２の６－５

（特定）個人情報を取り扱う事務を委託している場合、「委託先の重大事故」には、委託している事務以外における事故も含まれるのでしょうか。

（Ａ）

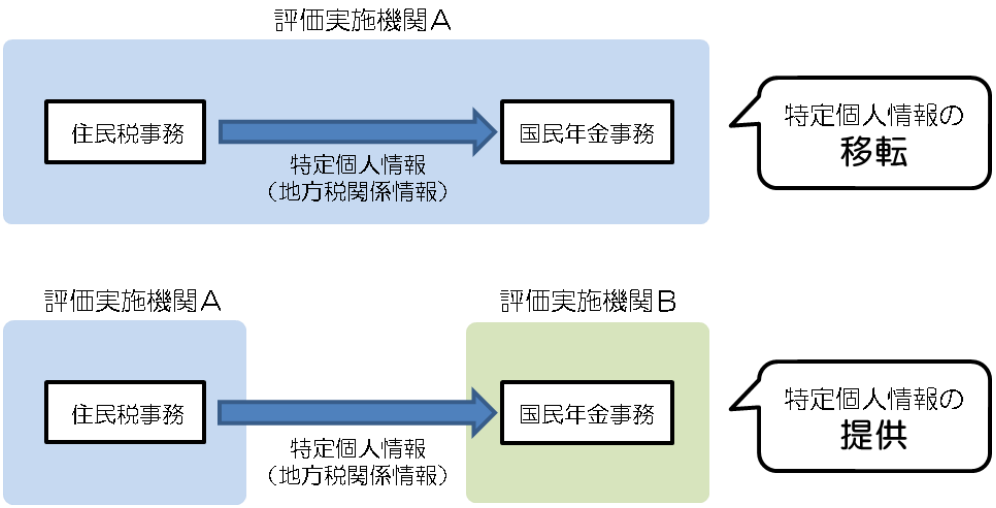
○　評価実施機関が安全管理措置義務を負うものに限定されるため、評価実施機関が委託した事務やその事務において取り扱う（特定）個人情報と無関係に発生した委託先の事故については、原則として、重大事故に含まれません。

Q第２の９－１

特定個人情報の移転の考え方はどのようなものでしょうか。

（Ａ）

○　特定個人情報の移転とは、「第２　定義」で示されているとおり、評価実施機関内において、特定個人情報ファイルに記録された特定個人情報を特定個人情報保護評価の対象となる事務以外の事務を処理する者の使用に供することを言います。一方、特定個人情報の提供とは、特定個人情報を評価実施機関以外の者に供与することを言います。具体例は、次のとおりです。



○　番号法は機関単位での規制を想定しています。特定個人情報の提供とは、機関をまたいだ行為であるため、個人番号を含まない個人情報の提供は、特定個人情報の提供に該当しません。一方で、特定個人情報の移転は、機関の内部での行為です。個人番号を含まない個人情報を渡した場合においても、渡した先において当該個人情報が個人番号と紐付くときには、機関として考えれば、渡した情報が移転先で個人番号と紐付けて利用されることを把握できるため、特定個人情報の移転と解します。例えば、次の場合が特定個人情報の移転に当たります。

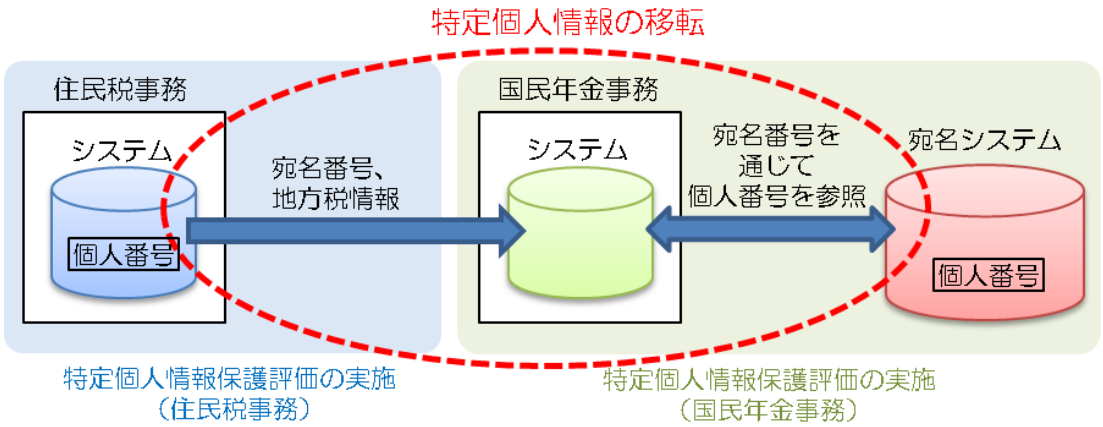
＜ケース①＞

○　下図のケース①は、次のようなケースを表しています。

・　住民税事務で保有する地方税情報については、宛名番号と紐付けて、国民年金事務に渡すことになっています。

・　国民年金事務においては、宛名番号を通じて宛名システムにアクセスし、個人番号を参照することになっています。このため、渡された地方税情報は、個人番号と紐付くことになります。

○　このケースの場合、地方税情報は、宛名番号を通じて個人番号と紐付くことになります。このため、住民税事務において地方税情報を国民年金事務に渡す行為は、特定個人情報の移転に当たります。



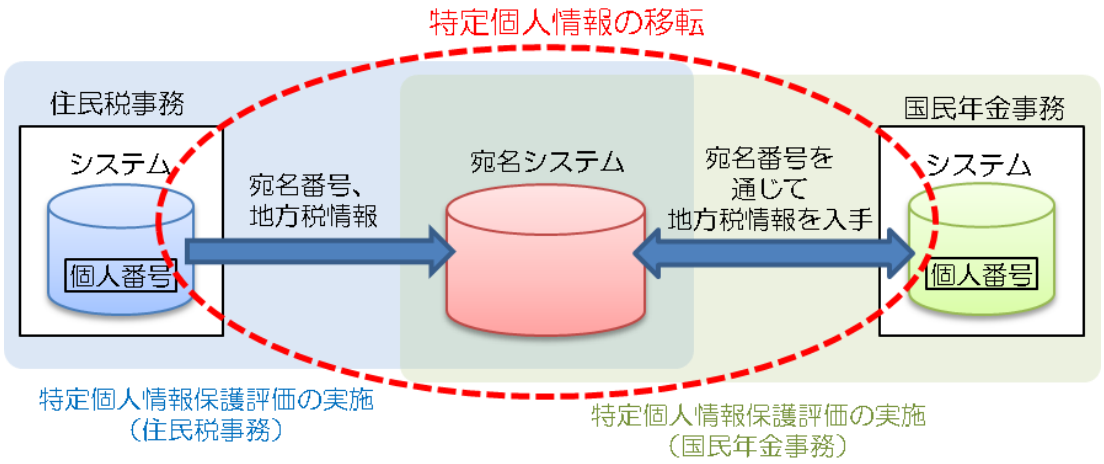
＜ケース②＞

○　下図のケース②は、次のようなケースを表しています。

・　住民税事務で保有する地方税情報については、宛名番号と紐付けて、宛名システムに渡すことになっています。宛名システムにおいては、地方税情報が個人番号と紐付くことになります。

・　国民年金事務においては、宛名番号を通じて宛名システムにアクセスし、地方税情報を入手します。

○　このケースの場合、地方税情報は宛名システムにおいて個人番号と紐付くことになります。このため、住民税事務において地方税情報を宛名システムに渡す行為は、特定個人情報の移転に当たります。



Ｑ第２の９－２

手作業処理用ファイルのみを取り扱う事務で、住民基本台帳システム端末を使用し、個人番号を検索キーとして４情報等の検索・確認を行っていますが、住民基本台帳に関する事務から見た場合、この事務に対して特定個人情報の移転をしていることになるのでしょうか。また、この場合、特定個人情報保護評価は、どのように行えばよいのでしょうか。

（Ａ）

○　この場合、住民基本台帳に関する事務から当該事務への特定個人情報の移転に当たると考えられます。以下、詳細に説明します。

○　特定個人情報の移転とは、「第２　定義」で示されているとおり、評価実施機関内において、特定個人情報ファイルに記録された特定個人情報を特定個人情報保護評価の対象となる事務以外の事務を処理する者の使用に供することをいいます。また、特定個人情報の使用とは、特定個人情報ファイルに記録された特定個人情報を特定個人情報保護評価の対象となる事務において用いることをいいます。

○　手作業処理用ファイルのみを取り扱う事務を含め、どのような事務であっても住基システム端末を使用し、個人番号を検索キーとして住民票情報を閲覧することは、当該事務において、個人番号を利用して、住基システム内の特定個人情報を使用することになりますので、住民基本台帳に関する事務から当該事務への特定個人情報の移転に当たると考えられます。また、個人番号を検索キーとして使用しなくても、閲覧した情報が当該事務において個人番号と紐付けて使用されるのであれば、これも特定個人情報の移転に当たると考えられます。

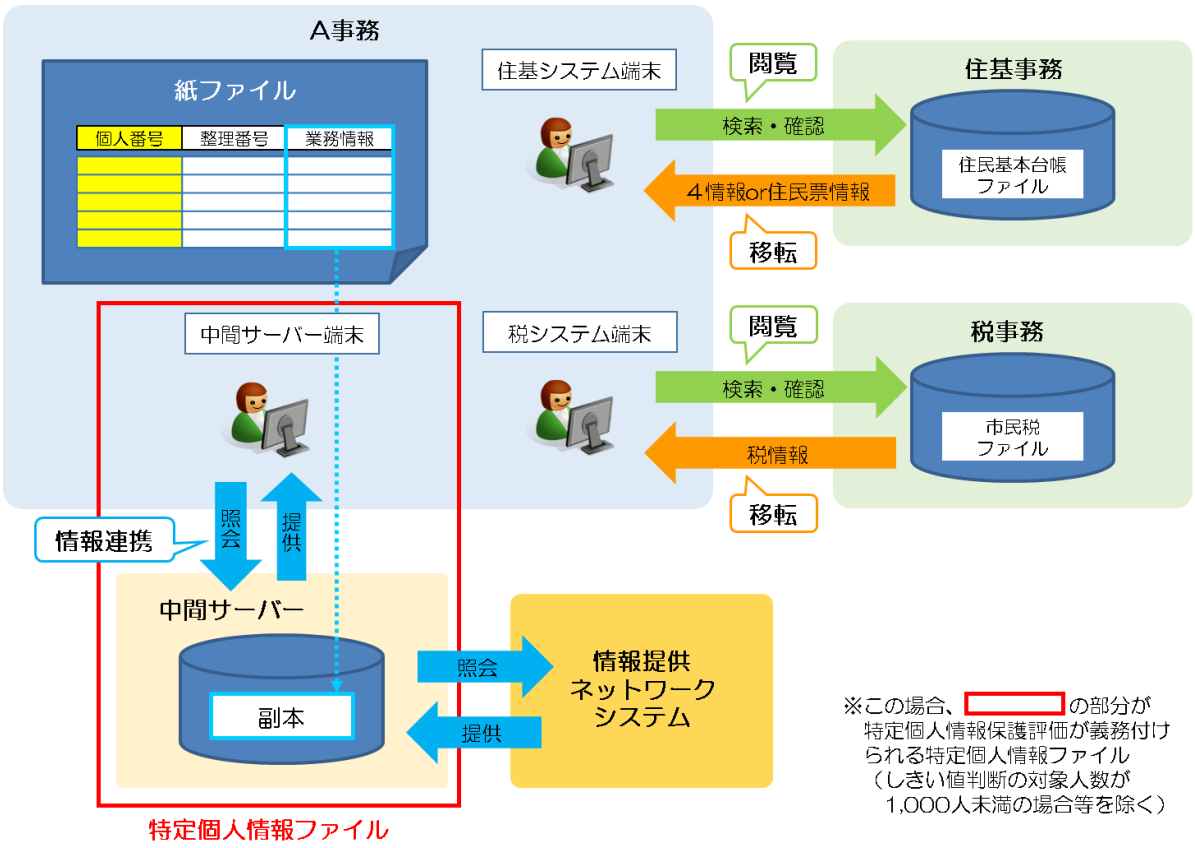
このため、このような事務を実施する部署は、住民基本台帳に関する事務における特定個人情報保護評価書の「移転先」として記載していただく必要があります。

また、この場合、住基システム端末を使用する者は、住民基本台帳に関する事務において保有する特定個人情報ファイルにアクセスできることから、住民基本台帳に関する事務のしきい値判断における取扱者数にも含まれることになります。

○　一方、当該事務で保有するファイルは、手作業処理用ファイルのみとなりますので、当該事務における特定個人情報保護評価は、義務付けられないこととなります。

ただし、番号法別表第一に掲げられる個人番号利用事務のうち、同法別表第二に掲げる情報提供ネットワークシステムを用いて特定個人情報の照会・提供を行う事務については、情報連携を行うために中間サーバーにその事務で取り扱う情報の副本を格納し、中間サーバー内において当該情報と符号（個人番号）が紐付くことから、指針第２の 10 に示すシステム用ファイルを保有することになります。このため、手作業処理用ファイルのみを取り扱う事務とはいえず、対象人数が 1,000 人未満の場合等を除き特定個人情報保護評価が義務付けられると考えます。

（※）Ｑ第４の４（１）－２②も併せて参照してください。



（参考）

個人番号の「利用」とは、行政機関における個人番号が記載された申請手続などの書類の受理、個人番号を用いた当該個人番号に係る者の情報の呼出し、情報の内部管理・保存、他の書類への個人番号の転記やデータの入力、各種行政相談等、個人番号を用いる行為を指すものである（内閣府大臣官房番号制度担当室「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【逐条解説】」から抜粋。）。

Q第２の 11－１
「システム用ファイル」と「その他の電子ファイル」との違いはどのようなものでしょうか。

（Ａ）

○　指針では、特定個人情報保護評価の実施時期を明確にするため、システム用ファイルとその他の電子ファイルとで定義を別にし、それぞれについて実施時期を定めることとしています。具体的には、システムにおいて取り扱われる特定個人情報ファイルについては、プログラミング開始前に実施することが求められるのに対し、システムにおいて取り扱われない特定個人情報ファイルについては、プログラミングが行われないことから、プログラミング開始前ではなく、それに相当する事務処理の検討段階で特定個人情報保護評価を実施するものとされています。

システム用ファイルとその他の電子ファイルとの違いは、要件定義、基本設計、詳細設計、プログラミング及びテストの段階を経て運用に供されるシステムにおいて取り扱われる特定個人情報ファイルか否かという点にあります。

○　その他の電子ファイルとは、表計算ソフトウェア、データベースソフトウェアその他の事務処理に用いられる一般的なソフトウェアを用いて作成され、パソコン等で取り扱われる特定個人情報ファイルであって、システム用ファイル以外のものをいいます。例えば、事務を処理するに当たり、システムを用いることなく、パソコンにおいて一般的な表計算ソフトウェアなどで対象者管理を行っている場合における特定個人情報ファイルなどをいいます。

第３　特定個人情報保護評価の実施主体

１　特定個人情報保護評価の実施が義務付けられる者

次に掲げる者のうち、特定個人情報ファイルを保有しようとする者又は保有する者は、この指針に基づき、特定個人情報保護評価の実施が義務付けられる。

（１）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）情報連携を行う事業者（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のうち、上記（１）から（５）までに掲げる者以外のものをいう。下記第４の４（１）カにおいて同じ。

（解説）

行政機関の長、地方公共団体の長その他の機関、独立行政法人等及び地方独立行政法人については、その公的性格から、特定個人情報ファイルをどのように取り扱い、個人のプライバシー等の権利利益の保護にどのように取り組んでいるかについて、自ら公表し、国民・住民の信頼を確保することが求められます。

そのため、情報提供ネットワークシステムを使用するか否かにかかわらず、その公的性格に鑑み、特定個人情報保護評価の実施が義務付けられることになります。

地方公共団体情報システム機構（J-LIS）については、市町村長によって指定される個人番号を生成するという、その番号制度における職務の重大性から、事後的対応ではない積極的な事前対応が求められ、また国民・住民の信頼を確保することが求められます。

そのため、情報提供ネットワークシステムを使用するか否かにかかわらず、その職責に鑑み、特定個人情報保護評価の実施が義務付けられることになります。

上記以外の者、すなわち事業者は、主に、源泉徴収義務等のために個人番号を取り扱うことが予定され、事業目的で個人番号を利用するものではないと考えられるため、このような事業者に特定個人情報保護評価の実施が義務付けられることは適当ではありません。

一方、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は、源泉徴収義務等にとどまらず、事業のために個人番号を取り扱うものであり、番号制度への関与の程度が深く、その特定個人情報ファイルの保有が個人に対して与える影

響も大きいものと考えられます。
　また、情報提供ネットワークシステムを使用して情報連携を行う場合は、源泉徴収義務等のために個人番号を利用する場合と比べ、個人番号を保有する目的や個人番号の取扱い方法が本人から見て分かりづらいものとも考えられます。
　以上の理由から、事業者については、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者に対してのみ、特定個人情報保護評価の実施が義務付けられることになります。

　なお、特定個人情報保護評価の実施が義務付けられない事業者が、任意の判断で特定個人情報保護評価を実施することは妨げられるものではなく、むしろ望ましいことといえます。

　また、情報提供ネットワークシステムは、内閣総理大臣が設置及び管理する（番号法第 21 条第１項）ため、情報提供ネットワークシステム運営機関は行政機関の長に該当します。

Ｑ第３の１－１
　　「行政機関の長」とはどのようなものを指すのでしょうか。

（Ａ）
○　「行政機関」とは、個人情報保護法第２条第８項に規定する行政機関をいい（番号法第２条第１項）、具体的には個人情報保護法第２条第８項各号において次の機関を指します。
　行政機関の長とは、当該機関の長を指します（令和４年４月現在）。
①　第１号に規定される機関
　「内閣に置かれる機関（内閣府を除く。）」とは、内閣官房、内閣法制局、復興庁、デジタル庁、国家安全保障会議等の各種会議、サイバーセキュリティ戦略本部等の各種本部を指します。「内閣の所轄の下に置かれる機関」とは人事院を指します。
②　第２号に規定される機関
　内閣府、宮内庁、公正取引委員会、国家公安委員会、個人情報保護委員会、カジノ管理委員会、金融庁及び消費者庁を指します。
③　第３号に規定される機関
　総務省、公害等調整委員会、消防庁、法務省、公安審査委員会、出入国在留管理庁、公安調査庁、外務省、財務省、国税庁、文部科学省、スポーツ庁、文化庁、厚生労働省、中央労働委員会、農林水産省、林野庁、水産庁、経済産業省、資源

エネルギー庁、特許庁、中小企業庁、国土交通省、運輸安全委員会、観光庁、気象庁、海上保安庁、環境省、原子力規制委員会、防衛省及び防衛装備庁を指します。

④　第４号に規定される機関
　　警察庁を指します。

⑤　第５号に規定される機関
　　検察庁を指します。

⑥　第６号に規定される機関
　　会計検査院を指します。

Ｑ第３の１－２
　「地方公共団体の機関」とはどのようなものを指すのでしょうか。１つの地方公共団体の中に複数の「地方公共団体の機関」がある場合、「地方公共団体の機関」ごとに特定個人情報保護評価を実施する必要があるのでしょうか。

（Ａ）

○　特定個人情報保護評価の実施が義務付けられる「地方公共団体の機関」とは、執行機関（都道府県知事、市町村長、教育委員会、公安委員会等）、執行機関の附属機関（審査会、審議会等）及び議会をいいます。

○　したがって、これらの機関が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ときは、特定個人情報保護評価の実施が義務付けられますが、指針第３の２にあるとおり、特定個人情報ファイルを取り扱う事務が、１つの地方公共団体内における複数の機関において行われている場合は、特定個人情報ファイルの取扱いの実態やリスク対策を把握し、記載事項に責任を負う立場にある機関が特定個人情報保護評価の実施を取りまとめることも可能です。

Ｑ第３の１－３
「独立行政法人等」とはどのようなものを指すのでしょうか。

（Ａ）

○　「独立行政法人等」とは、個人情報保護法第２条第９項に規定する独立行政法人をいいます（番号法第２条第２項）。

具体的には、独立行政法人のほか、個人情報保護法別表一に掲げる法人（日本私立学校振興・共済事業団、日本年金機構、国立大学法人、日本銀行等の法人）をいいます。

Ｑ第３の１－４
「情報連携を行う事業者（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のうち、上記（１）から（５）までに掲げる者以外のものをいう。）」とはどのようなものを指すのでしょうか。

（Ａ）

○　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のうち、上記（１）から（５）までに掲げる者（行政機関の長、地方公共団体の長その他の機関、独立行政法人等、地方独立行政法人、地方公共団体情報システム機構）以外のものとは、全国健康保険協会、健康保険組合、国民健康保険組合、共済組合、社会福祉協議会等、番号法別表第二に掲げる者を指します。

２　実施が義務付けられる者が複数いる場合等の特定個人情報保護評価

上記１に掲げる者が特定個人情報保護評価を実施する際に、特定個人情報ファイルを保有しようとする者又は保有する者が複数存在する場合は、特定個人情報ファイルの取扱いの実態やリスク対策を把握し、記載事項に責任を負う立場にある者が特定個人情報保護評価の実施を取りまとめる。

また、特定個人情報ファイルを保有しようとする者又は保有する者以外に特定個人情報ファイルに関わる者が存在する場合は、その者は、特定個人情報保護評価が適切に実施されるよう協力するものとする。

（解説）

番号法第 28 条では、行政機関の長等は、特定個人情報ファイルを保有しようとするときは特定個人情報保護評価を実施するものとされており、すなわち、特定個人情報ファイルの保有者が特定個人情報保護評価を実施することとなります。

個人情報保護法にいう「保有」とは、当該個人情報を事実上支配している（当該個人情報の利用、提供、廃棄等の取扱いについて判断する権限を有している）状態をいうとされています。また、「保有個人データ」は、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことができる権限を有するものをいいます（個人情報保護法 16 条第４項）。

したがって、通常の場合であれば、特定個人情報ファイルを取り扱う事務を所管する機関が、特定個人情報ファイルの保有者であり、評価実施機関として特定個人情報保護評価を実施することになります。

一方で、他の機関に権限の委任が行われている場合など、１つの事務において特定個人情報ファイルの保有者すなわち評価実施機関が複数存在する場合があります。

このような場合については、個々のケースに応じて検討する必要がありますが、基本的な考え方としては、特定個人情報ファイルの取扱いの実態やリスク対策を把握し、当該特定個人情報ファイルの取扱いに関する記載事項に責任を負う立場にある評価実施機関が特定個人情報保護評価書の作成を取りまとめます。その際、特定個人情報保護評価を主体的に実施する評価実施機関では責任を負えない評価項目については、他の評価実施機関から情報の提供を受けて記載することとなります。

また、意見聴取・第三者点検も、特定個人情報ファイルの取扱いの実態やリスク対策を把握し、記載事項に責任を負う立場にある評価実施機関が実施しますが、その際、特定個人情報保護評価書を主体的に作成する評価実施機関では責任を負えない事項について質問や意見があった場合には、他の評価実施機関からその回答に当たって必要となる情報の提供を受けて対応することが考えられます。

この場合、特定個人情報保護評価書の表紙に記載する「評価実施機関名」には、取りまとめを行う評価実施機関の名称のみ記載し、他の評価実施機関の名称は「他の評価実施機関」の欄に記載することとなります。

また、特定個人情報ファイルを保有しようとする者又は保有する者以外に、システムやアプリケーションの設計・開発等の調達を実施する者が存在するなど、特定個人情報ファイルに関わる者が存在する場合があります。

このような場合についても、個々のケースに応じて検討する必要がありますが、基本的には、特定個人情報ファイルの保有者が特定個人情報保護評価を実施し、特定個人情報ファイルの保有者では変更することのできないシステムやアプリケーションの仕様などに関わる部分については、システムやアプリケーションの設計・開発等を行った者が、特定個人情報保護評価が適切に実施されるよう協力します。

協力の具体的な内容としては、システムやアプリケーションの仕様などについて、特定個人情報保護評価書を作成する際に必要となる情報を特定個人情報ファイルの保有者に提供することが考えられます。さらに、意見聴取や第三者点検においてシステムやアプリケーションの仕様などについて質問や意見があった場合には、その回答についての情報を特定個人情報ファイルの保有者に提供することが考えられます。

この場合、基本的には、特定個人情報保護評価書の表紙に記載する「評価実施機関名」には、特定個人情報ファイルの保有者である評価実施機関の名称のみを記載し、協力する機関の名称は記載しないこととなります。

Q第３の２－１

特定個人情報ファイルを保有しようとする者又は保有する者が複数存在する場合とは、どのような場合が考えられるのでしょうか。

（Ａ）

○　例えば、行政機関が特定個人情報を取り扱う個人番号利用事務に係る権限を法令に基づき他の行政機関に委任している場合や、都道府県が権限を法令に基づき市町村に委任している場合に、特定個人情報ファイルを保有しようとする者又は保有する者が複数存在することがあると考えられます。

○　なお、請負契約や準委任契約などの委託によって他の機関に事務の一部を実施させている場合には、一般的に委託元において特定個人情報ファイルを保有していると考えられますので、委託元が特定個人情報保護評価を実施し、特定個人情報保護評価書の委託に関する項目の中に、当該委託について記載をすることとなります。

Q第３の２－２
　　特別地方公共団体については、特定個人情報保護評価の実施主体はどのようになるのでしょうか。

（Ａ）

○　一部事務組合や広域連合等の特別地方公共団体は、普通地方公共団体の事務を共同処理するために組織されます。特別地方公共団体と普通地方公共団体のどちらが、特定個人情報保護評価を実施すべきかについては、原則として、事務の実施権限を有する特定個人情報ファイルの保有者がどちらであるかによることとなります。

○　例えば、後期高齢者医療広域連合が、番号法第９条第１項・別表第一の 59 の項の事務（高齢者の医療の確保に関する法律による後期高齢者医療給付の支給、保険料の徴収又は保険事業の実施に関する事務であって主務省令で定めるもの）を実施するために、特定個人情報ファイルを保有する場合のように、特別地方公共団体が事務の実施権限を有する特定個人情報ファイルの保有者である場合は、原則として、特別地方公共団体が、特定個人情報保護評価を実施することとなります。

Q第３の２－３
　　地方公共団体は中間サーバーを用いて情報連携を行う予定ですが、これについてはどのように特定個人情報保護評価を行うのでしょうか。

（Ａ）

○　地方公共団体は、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ため、中間サーバー内に、特定個人情報ファイルを取り扱う事務で使用する個人情報の副本等を保有することになります。このため、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務について特定個人情報保護評価を実施するときは、個人情報の副本等も当該事務において保有する特定個人情報ファイルの範囲に含まれることになります。

○　また、特定個人情報保護評価の対象は、システムやサーバそのものではなく、それらを用いて特定個人情報ファイルを取り扱う事務です。このため、システムやサーバ単独で評価するのではなく、事務ごとに作成する特定個人情報保護評価書の中において、主に特定個人情報の提供等の方法として、地方公共団体における中間サーバーについての評価を記載することになります。

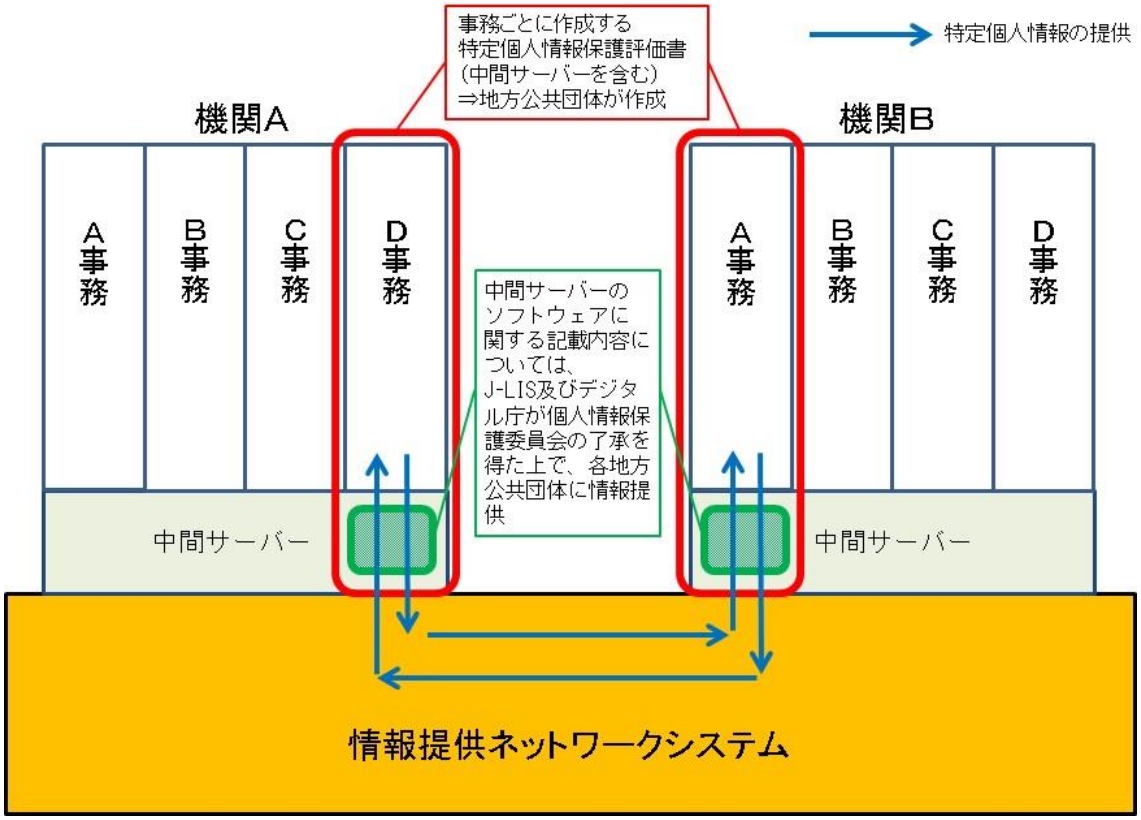
○　地方公共団体における中間サーバーのソフトウェアは、総務省が一括開発しますので、特定個人情報保護評価書の当該ソフトウェアに関する記載については、総務省が、特定個人情報保護委員会の了承を得た上で地方公共団体に対し提供した「特定個人情報保護評価書の作成の際に必要となる中間サーバーに関する情報の提供について（平成 26 年８月８日）」により、特定個人情報保護評価書の作成に必要と

なる情報を提供し、その後も必要に応じて情報を提供していました。

○　また、ハードウェアについて「中間サーバー・プラットフォーム」を地方公共団体が活用する場合においては、特定個人情報保護評価書の当該プラットフォームに関する記載については、総務省が、特定個人情報保護委員会の了承を得た上で各地方公共団体に対し提供した「特定個人情報保護評価書の作成の際に必要となる中間サーバーに関する情報の提供について（平成 26 年８月８日）」により、特定個人情報保護評価書の作成に必要となる情報を提供し、その後も必要に応じて情報を提供していました。

○　地方公共団体における中間サーバーについては、現在、地方公共団体情報システム機構（J-LIS）が運営を行っており、また、令和３年９月１日にデジタル庁が設置されたことに伴い、J-LIS 及びデジタル庁が情報提供、住民等の意見聴取及び第三者点検について、必要に応じて地方公共団体に協力することとしています。

＜地方公共団体における中間サーバーについての特定個人情報保護評価のイメージ＞



Ｑ第３の２－４

番号制度関連システム、住民基本台帳システム、市町村ＣＳ、都道府県サーバについては、地方公共団体はどのように特定個人情報保護評価を行うのでしょうか。

（Ａ）

○　特定個人情報保護評価の対象は、システムやサーバそのものではなく、それらを用いて特定個人情報ファイルを取り扱う事務です。このため、システムやサーバ単独で評価するのではなく、

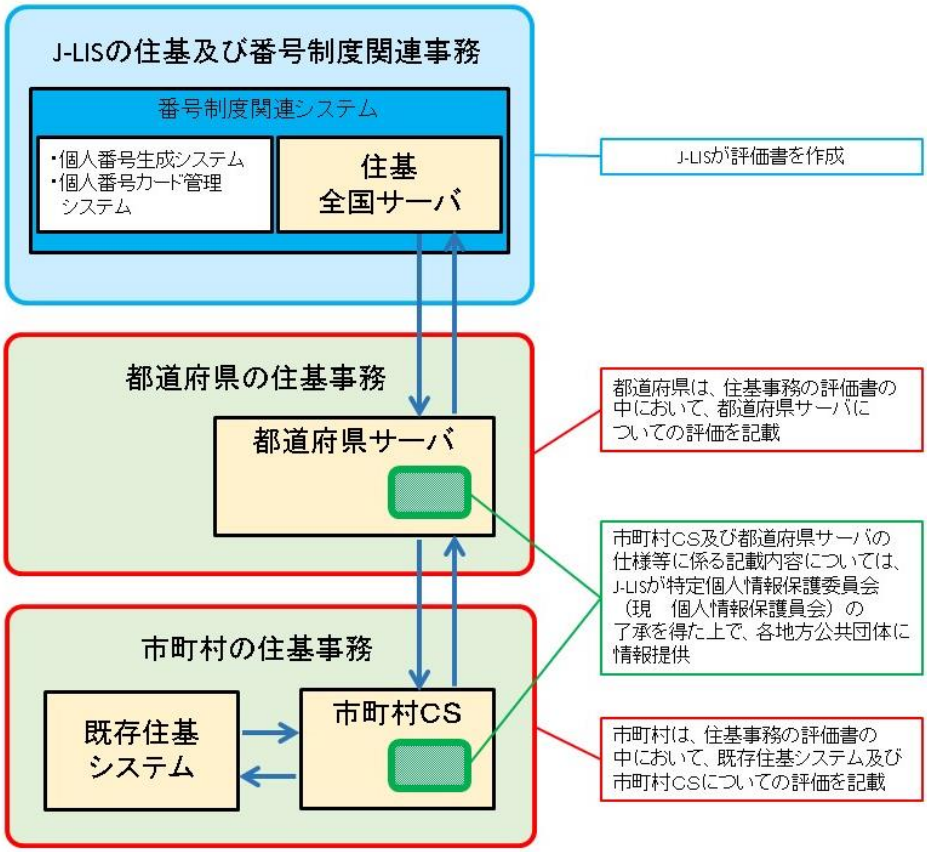
①　市町村は、住民基本台帳に関する事務について作成する特定個人情報保護評価書の中で、既存住民基本台帳システム（以下「既存住基システム」という。）及び市町村ＣＳについての評価を記載し、

②　都道府県は、住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務について作成する特定個人情報保護評価書の中で、都道府県サーバについての評価を記載することになります。

○　ただし、市町村ＣＳ及び都道府県サーバについては、地方公共団体情報システム機構（J-LIS）が開発しています。評価書における市町村ＣＳの仕様等や都道府県サーバの仕様等に関する記載については、J-LIS が特定個人情報保護委員会の了承を得た上で、平成 26 年６月 30 日に各地方公共団体に対して必要な情報を提供し、その後も必要に応じて情報を提供していますので、住民基本台帳に関する事務等についての評価の実施に当たっては、それを参考にしてください。さらに、J-LIS は、住民等の意見聴取及び第三者点検においても、必要に応じて地方公共団体に協力することとしています。

○　なお、個人番号生成システム、住基全国サーバ及び個人番号カード管理システムについては、J-LIS が実施した「住民基本台帳ネットワーク及び番号制度関連事務全項目評価書」の中で、記載されています。

＜市町村、都道府県、J-LIS の事務についての特定個人情報保護評価のイメージ＞



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。

（解説）

特定個人情報ファイルを取り扱う事務には、番号法第９条第１項及び別表第一に掲げる事務、同条第２項の規定に基づき地方公共団体が条例で定める事務、同条第３項から第６項までの規定に基づき特定個人情報ファイルを取り扱う事務、住民基本台帳法に基づく住民票に関する事務等があります。

なお、特定個人情報ファイルを取り扱う事務であっても、指針第３の１に定める特定個人情報保護評価の実施が義務付けられる者以外の者（例えば、源泉徴収義務のみのために特定個人情報ファイルを取り扱う事業者）が行う事務や、指針第４の４（１）に定める事務については、特定個人情報保護評価の実施が義務付けられません。

Ｑ第４の１－１

地方公共団体が個人に対する講演料等の支払いに際し、支払調書を作成する場合にも個人番号を利用することになりますが、このように個人番号関係事務実施者の立場で事務を行う場合には、特定個人情報保護評価を実施する必要はありますか。

（Ａ）

○　評価実施機関が特定個人情報ファイルを保有しようとするときは、特定個人情報保護評価の実施が義務付けられます。地方公共団体が特定個人情報ファイルを保有する場合には、それが個人番号関係事務に該当する場合であっても、原則として評価対象事務となります。

○　ただし、職員又は職員であった者等の人事・給与・福利厚生に係るファイルのみを取り扱う事務、対象人数が 1,000 人未満の事務等の場合には特定個人情報保護評価の実施が義務付けられません（後述第４の４参照）。

○　一方、職員以外の第三者への報酬や謝金等に係る支払調書、不動産使用料に係る支払調書等を作成する場合には、当該事務における対象人数が 1,000 人未満の場合を除き、特定個人情報保護評価の実施が必要であると考えられます。

２　特定個人情報保護評価の単位

特定個人情報保護評価は、原則として、法令上の事務ごとに実施するものとする。番号法の別表第一に掲げる事務については、原則として、別表第一の各項の事務ごとに実施するものとするが、各項の事務ごとに実施することが困難な場合は、１つの項に掲げる事務を複数の事務に分割して又は複数の項に掲げる事務を１つの事務として、特定個人情報保護評価の対象とすることができる。別表第一以外の番号法の規定、番号法以外の国の法令又は地方公共団体が定める条例に掲げる事務についても、評価実施機関の判断で、特定個人情報保護評価の対象となる事務の単位を定めることができる。

（解説）

特定個人情報保護評価は、原則として、番号法の別表第一に掲げる事務ごとに実施するものとしますが、行政機関等のシステムや事務の執行状況等によっては、別表第一の項ごとでは特定個人情報保護評価書の記載が困難な場合や、別表第一の複数の項をまとめて記載した方が分かりやすい場合などが考えられます。

そのため、別表第一の事務を分割又は統合した事務で１つの特定個人情報保護評価書を作成することを可能にしています。

Ｑ第４の２－１

１つのシステムで多くの事務を実施している場合、事務を統合して特定個人情報保護評価を実施することは可能でしょうか。

（Ａ）

○　１つのシステムで多くの事務を実施している場合においても、事務をまとめて作成した方が分かりやすい場合などは、評価実施機関の判断で、事務を統合して特定個人情報保護評価を実施することができます。

また、別表第一以外にも、番号法第９条第２項に基づき地方公共団体が条例で定める事務などで特定個人情報ファイルを保有する場合も同様です。

Ｑ第４の２－２
　　別表第二に掲げる事務や特定個人情報については特定個人情報保護評価を実施しなくてもよいのでしょうか。

（Ａ）

○　特定個人情報保護評価は、特定個人情報ファイルを取り扱う事務を対象とします。

○　別表第二に掲げる情報提供ネットワークシステムを用いて行う特定個人情報の照会・提供は、原則として別表第一を根拠として実施する事務において実施することとなります。つまり、別表第二に掲げる情報の照会・提供をする事務は別表第一に掲げられており、提供する特定個人情報は、原則として別表第一を根拠として保有することとなります。

○　したがって、特定個人情報保護評価は別表第二を評価単位として評価する必要はなく、別表第一を基本とした単位で評価を実施し、その中で別表第二の情報の入手・提供について評価することとなります。

Ｑ第４の２－３
　　同一機関内における共通システムの評価の単位は、どのようになるのでしょうか。

（Ａ）

○　特定個人情報保護評価は、事務ごとに実施することとされており、同一機関内における共通システムについても、それぞれの事務の一部として特定個人情報保護評価を実施することとなります。

○　共通システムについては、地方公共団体における宛名システムのような既存番号と個人番号の対照管理システムその他複数の事務で個人番号を共通に参照するシステムが該当すると考えられます。

３　特定個人情報ファイル

特定個人情報保護評価の対象となる事務において取り扱う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（番号法第２条第９項）、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に体系的に構成したものである。

特定個人情報ファイルの単位は、特定個人情報ファイルの使用目的に基づき、評価実施機関が定めることができる。特定個人情報保護評価の対象となる１つの事務において複数の特定個人情報ファイルを保有することもできる。

（解説）

【特定個人情報ファイルとは】

番号法第２条第８項において、「特定個人情報」とは、個人番号をその内容に含む個人情報をいうと定められ、同条第９項において、「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うと定められています。

すなわち、

（１）　行政機関等（番号法第２条第４項に規定する行政機関等をいう。以下第４の３の解説において同じ。）（※）における「特定個人情報ファイル」とは、個人情報保護法第60条第２項に規定する個人情報ファイルであって個人番号をその内容に含むもの

（２）　行政機関等以外の者（地方公共団体や民間事業者など）が保有する「特定個人情報ファイル」とは、個人情報保護法第16条第１項に規定する個人情報データベース等であって個人番号をその内容に含むもの

をいいます。

このように、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又は個人情報データベース等をいいますが、個人情報ファイル又は個人情報データベース等の定義は、番号法独自の定義ではなく、一般法の定義と同じです。

（※）行政機関及び独立行政法人等（個人情報保護法別表第二に掲げる法人を除く。）を指します（個人情報保護法第２条第11項）。

【個人情報ファイル・個人情報データベース等について】

上述したとおり、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又は個人情報データベース等をいいますが、個人情報ファイル又は個人情報データベース等には、①電子計算機用ファイルと②手作業処理用ファイルの２種類があります。

行政機関等、行政機関等以外の機関（地方公共団体や民間事業者など）について、

それぞれ次の①が電子計算機用ファイルに当たり、②が手作業処理用ファイルに当たります。

（１）　行政機関等における「個人情報ファイル」とは、個人情報保護法第60条第２項において、保有個人情報を含む情報の集合物であって、

①　一定の事務の目的を達成するために特定の保有個人情報を電子計算機を用いて検索することができるように体系的に構成したもの

②　①のほか、一定の事務の目的を達成するために氏名、生年月日、その他の記述等により特定の保有個人情報を容易に検索することができるように体系的に構成したもの

をいうとされています。

（２）　行政機関等以外の機関（地方公共団体や民間事業者など）における「個人情報データベース等」とは、個人情報保護法第16条第１項において、個人情報を含む情報の集合物であって、

①　特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの

②　①のほか、特定の個人情報を容易に検索することができるように体系的に構成したもの

をいうとされています。

①電子計算機用ファイルは、ITシステムで保有されるファイル（例えば、データベースなどをいい、指針上「システム用ファイル」と定義されています。）のほか、パソコン等で使用されるデータベースソフト用ファイル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（指針上「その他の電子ファイル」と定義されています。）などを指します。

ただし、電子ファイルであれば全てこれに該当するものではなく、表計算ソフトやワープロソフトで決裁書を起案し、このような決裁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、これに該当しないと解されます。

また、①電子計算機用ファイルであっても、指針第４の４（１）ウのとおり、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（対象人数）が1,000人未満の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こととなります。

②手作業処理用ファイルは、「索引・目次などが付された紙ファイル」などが該当すると解されます。

ただし、指針第４の４（１）イのとおり、②手作業処理用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こととなります。

【特定個人情報ファイルの単位について】

特定個人情報ファイルの単位は、評価実施機関の合理的裁量に委ねられており、複数のシステムをまとめて１つの特定個人情報ファイルとすることも可能ですし、１つのシステムの中に複数の特定個人情報ファイルを保有することも可能です。この考え方は、個人情報ファイルの考え方と同じものです。

ただし、特定個人情報ファイルの単位を検討するに当たっては、使用目的を明確にできる単位であるとともに、システムの体系がわかる適切な大きさの単位とすることが必要です。

なお、特定個人情報ファイルの単位は、データベースの設計どおりにする必要はありません。つまり、必ずしもテーブルごとに特定個人情報ファイルを分ける必要はなく、複数のテーブルを合わせて１つの特定個人情報ファイルとしたり、複数のテーブルを組み合わせたうちの一部の情報のみを１つの特定個人情報ファイルとしたりすることができます。もちろん、１つのテーブルを１つの特定個人情報ファイルとすることも可能です。

【個人番号を「その内容に含む」とは①】

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に体系的に構成したものを指します。番号法は、個人番号を悪用して不正な名寄せが行われることがないよう厳格な保護措置を規定する法律であり、特定個人情報ファイルについて検討するに当たっても、この点を十分考慮しなくてはなりません。

具体的には、電子ファイルの場合、【図１】のように異なるテーブル（表）の一方に個人番号が記録されていたとしても、個人番号にアクセスできる者が、テーブル結合によって個人番号から別のテーブルの情報にたどり着くことが可能となります。

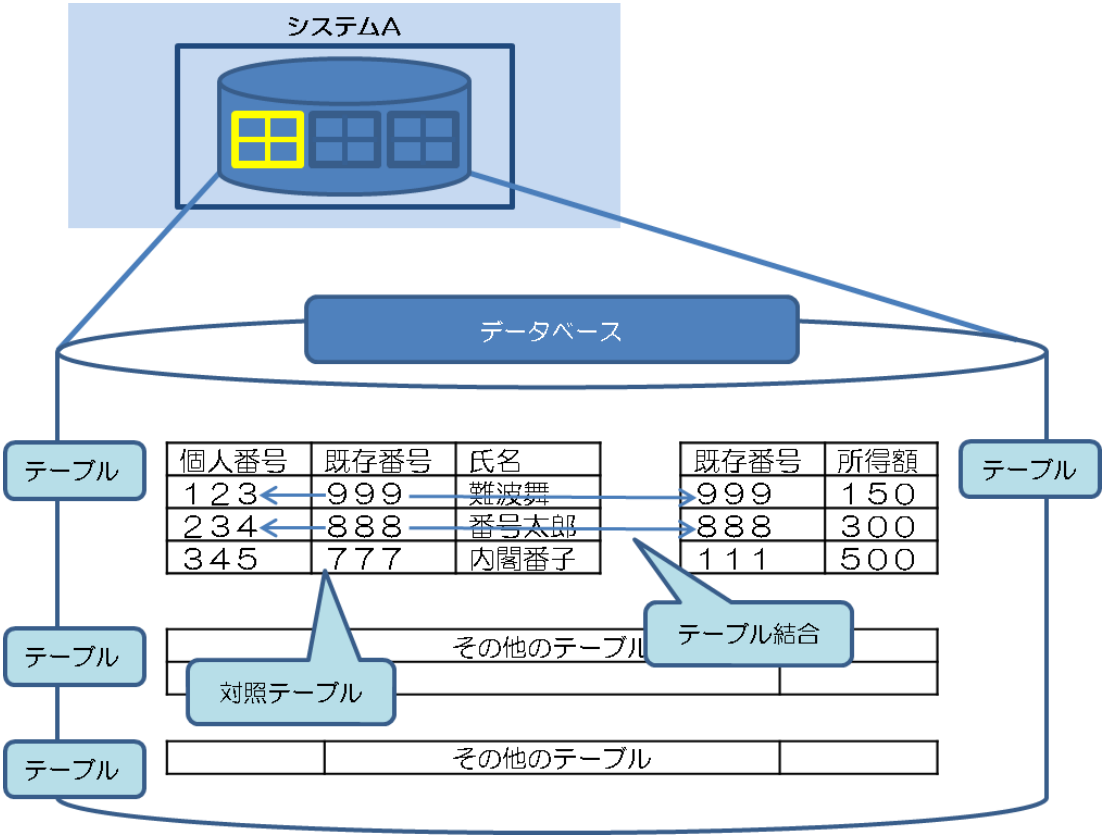
テーブル　データベース

注：黄色のテーブルのみに個人番号が存在する場合

【図１】

個人番号にアクセスできる者が個人番号と紐付けてアクセスできる範囲が紺色の範囲

⇒紺色の範囲が特定個人情報ファイル



※テーブル（表）とは、データベースを構成する要素であり、データベースは複数のテーブル（表）から構成されるのが一般的です。

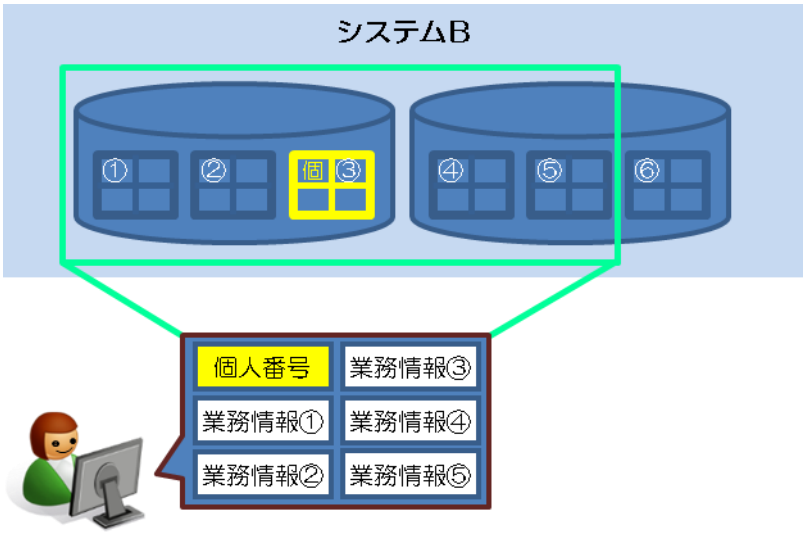
※テーブル結合によって、異なるテーブルに格納されているデータを組み合わせることができます。

また、【図２】のように異なるデータベースの一方に個人番号が記録されていたとしても、システムの内部処理で連携していれば個人番号にアクセスできる者が個人番号から別のデータベースの情報にたどり着くことができます。この場合、別のデータベースの情報を含め、個人番号と紐付けてアクセスできる範囲が特定個人情報ファイルとなります。

つまり、個人番号をその内容に含む個人情報ファイルとは、単に個人番号が含まれているテーブルのみを意味するのではなく、個人番号にアクセスできる者が、個人番号と紐付けてアクセスできる情報を意味し、これが特定個人情報ファイルということとなります。

【図２】

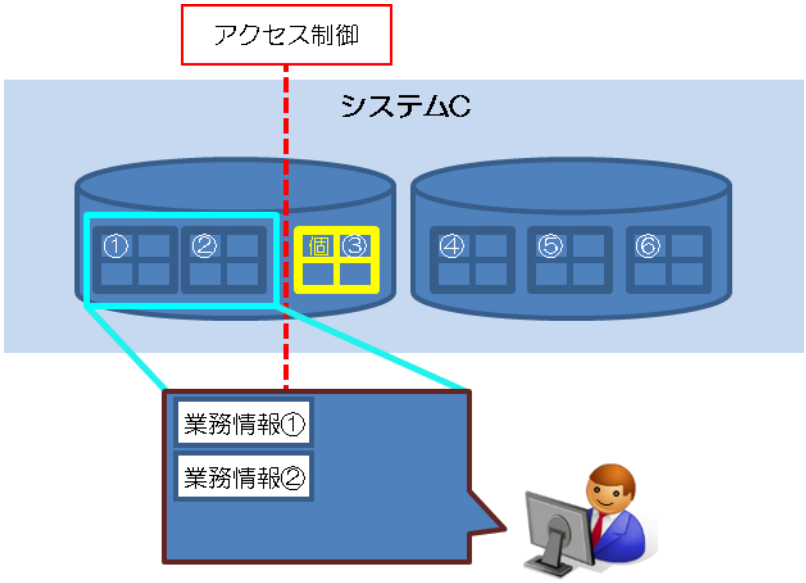
個人番号にアクセスできる者が個人番号と紐付けてアクセスできる範囲がグリーンの範囲
⇒グリーンの範囲が特定個人情報ファイル



ただし、【図３】のように、アクセス制御等により、不正アクセス等を行わない限り、個人番号を含むテーブルにアクセスできない場合は、原則、特定個人情報ファイルには該当しません。

【図３】

水色のテーブルにアクセスできる者は、アクセス制御により個人番号にアクセスできない
⇒水色の範囲は特定個人情報ファイルではない

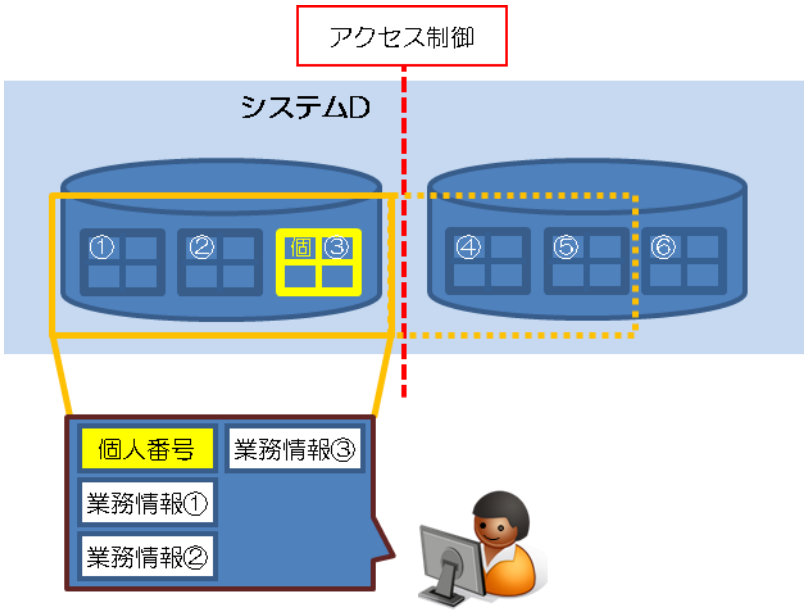


また、【図４】のように、複数のデータベースがシステムの内部処理で連携しており、個人番号と紐付けてアクセスできる範囲がオレンジの実線及び破線の範囲であった場合でも、アクセス制御等により、個人番号にアクセスできる者が個人番号と紐付けてアクセスできる範囲を実線の範囲に縮減した場合には、実線の範囲が特定個人情報ファイルとなります。

ただし、破線部分については、特定個人情報ファイルの保有者は各部署ではなく機関であるため、ある事務では、アクセス制御等により、破線部分を個人番号と紐付けてアクセスできないようにしていても、機関内のほかの事務においては、破線部分を個人番号と紐付けていた場合は、当該他の事務については、破線部分も特定個人情報ファイルに該当することとなります。

【図４】

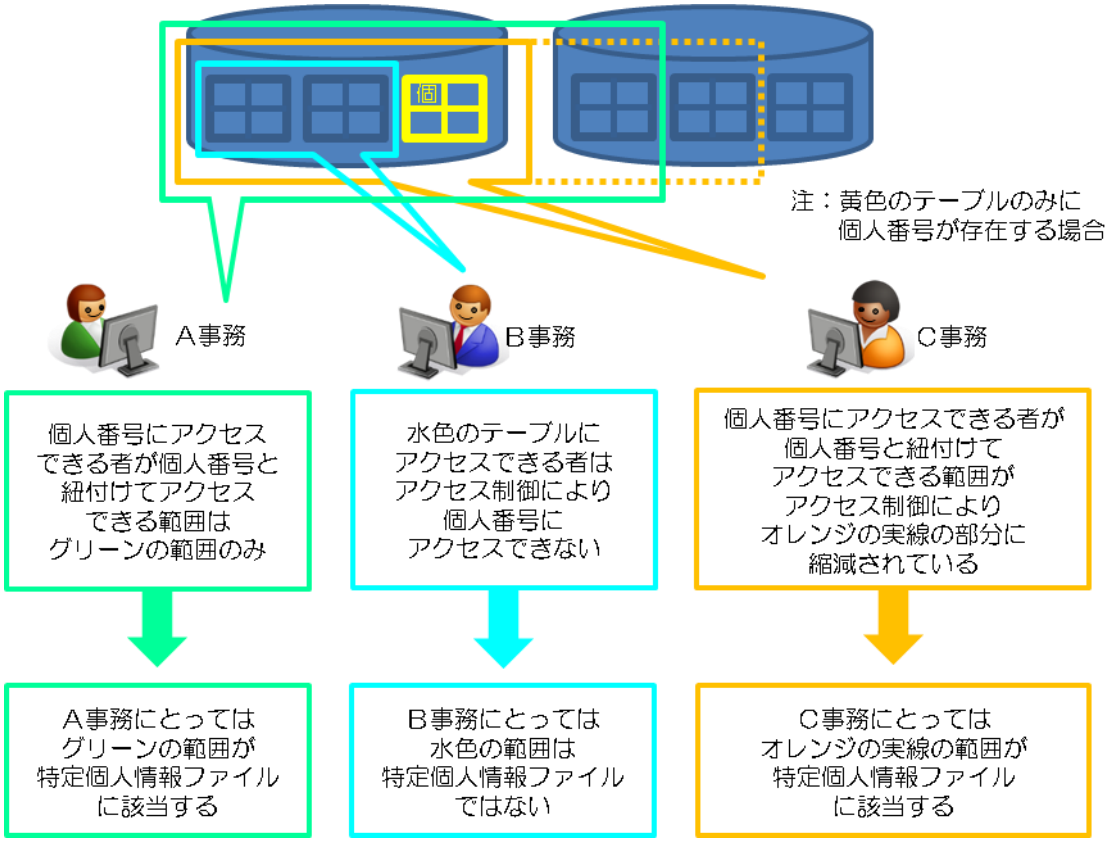
個人番号にアクセスできる者が個人番号と紐付けてアクセスできる範囲が、アクセス制御によりオレンジ実線の範囲に縮減されている。
⇒オレンジ実線の範囲が特定個人情報ファイル



上記を踏まえると、地方公共団体のように複数の事務が存在し、それぞれの事務について評価を実施する場合、特定個人情報ファイルのイメージは【図５】のとおりとなり、事務ごとに特定個人情報ファイルの範囲が異なる可能性があります。

【図５】

- Ａ事務については、特定個人情報ファイルはグリーンの範囲になり、これについて特定個人情報保護評価を実施する必要があります。
- Ｂ事務については、特定個人情報ファイルが存在しないので、特定個人情報保護評価を実施する必要はありません。
- Ｃ事務については、特定個人情報ファイルはオレンジの実線の範囲になり、これについて特定個人情報保護評価を実施する必要があります。



【個人番号を「その内容に含む」とは②】

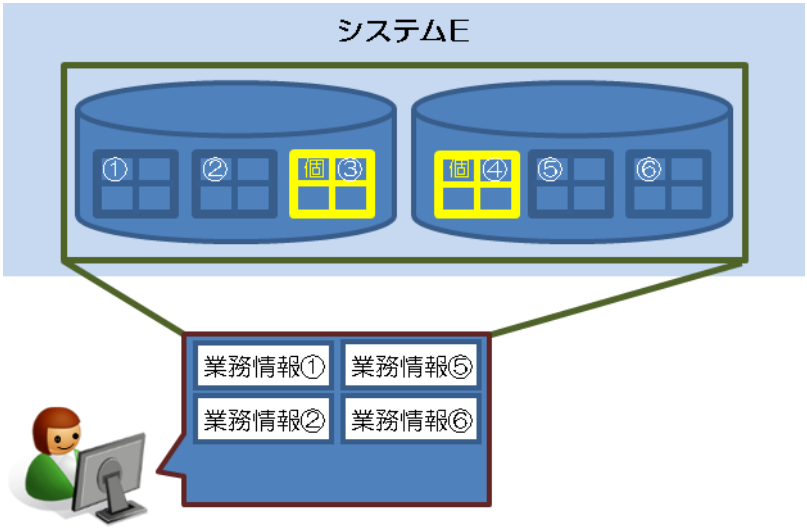
一方、【図６】のように個人番号が画面上表示されず、事務を行う権限を有するいずれの者も個人番号を画面や帳票などで見ることができない場合であっても、システム上で個人番号にアクセスし、システムの内部処理で連携する場合（例えば、システム上では画面や帳票などに既存番号を入出力するものの、当該システム内部では既存番号から個人番号を検索し、個人番号を利用している場合など）が存在します。

これについても、個人番号と紐付けてアクセスできることに変わりはないということになりますので、そのアクセスできる範囲は、特定個人情報ファイルに該当することとなります。

ただし、この場合もアクセス制御等により、個人番号と紐付かないようにしているものは、特定個人情報ファイルには該当しません。

【図６】

事務を行う者は個人番号にアクセスできないが、システムの内部で個人番号が検索キーとして利用され、個人番号により紐付けてアクセスできる範囲が濃い緑の範囲



※個人番号と、個人番号を含むテーブルに存在する業務情報③及び④は画面上表示されない。

【既存番号と個人番号の対照テーブルを保有する場合の特定個人情報ファイル】

さらに、評価実施機関では、番号法に対応するために、既存システムで検索キーとして用いられている既存番号と個人番号の対照テーブルを保有することで、番号法対応を行うことも考えられます。

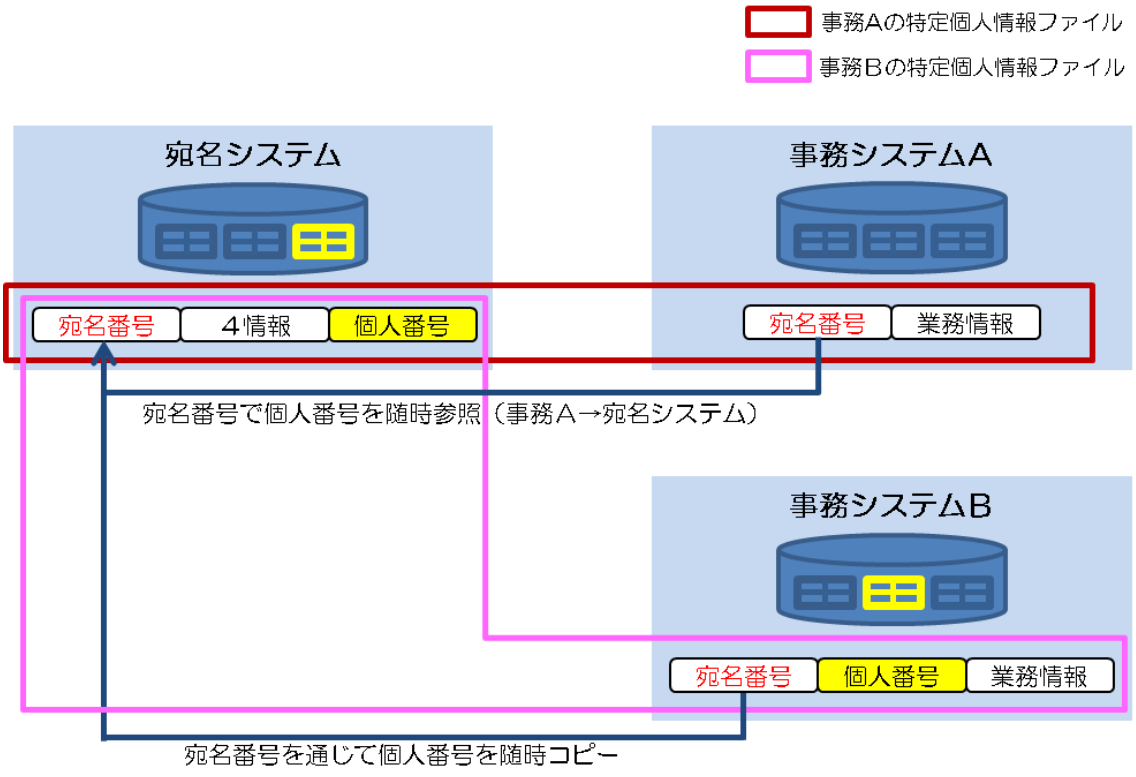
個人番号にアクセスできる者が、個人番号と紐付けてアクセスできる情報は、特定個人情報ファイルに該当することとなります。したがって、対照テーブル以外のテーブルであっても、職員等が個人番号と紐付けてアクセスできる範囲は、特定個人情報ファイルに該当することとなります。

例えば、【図７】に示されるとおり、地方公共団体における宛名システムのように、既存番号（ここでは宛名番号）と個人番号の対照テーブルを保有する場合、事務Ａのように個人番号を参照できる場合は、事務システムＡで直接個人番号を保有していなくても、特定個人情報ファイルに該当することとなります。

なお、当然、事務Ｂのように宛名システムから個人番号を随時コピーする場合についても、宛名システムで紐付く情報を含めた範囲が、事務Ｂの特定個人情報ファイルとなります。

【図７】

既存番号と個人番号の対照テーブルの例



Q第４の３－１

個人番号を含むデータベースやテーブルと既存番号で連携している場合も、全て特定個人情報ファイルに該当するのでしょうか。

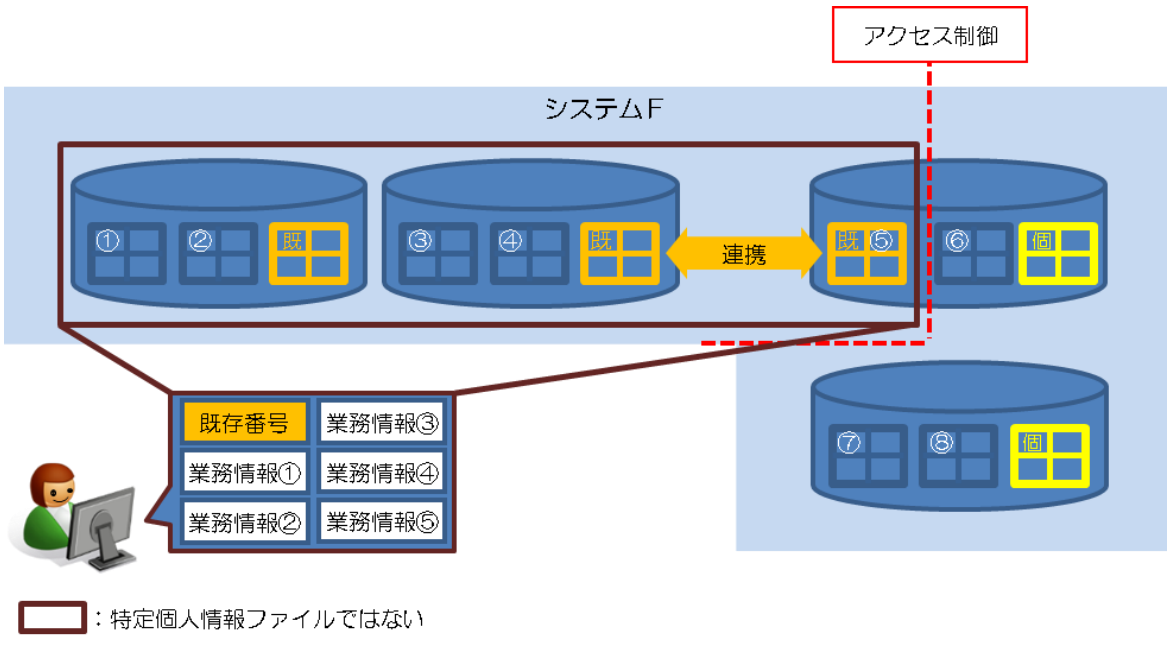
（Ａ）

○　特定個人情報ファイルに該当するか否かは、個人番号と紐付けてアクセスできるかどうかで判断します。したがって、既存番号で連携している場合であって、アクセス制御により、個人番号そのものにはアクセスできず、個人番号以外の情報にのみアクセスできるように制御されている場合は、特定個人情報ファイルには該当しません【図１参照】。これは、データベース間にアクセス制御を設ける場合もテーブル間にアクセス制御を設ける場合も同じです。

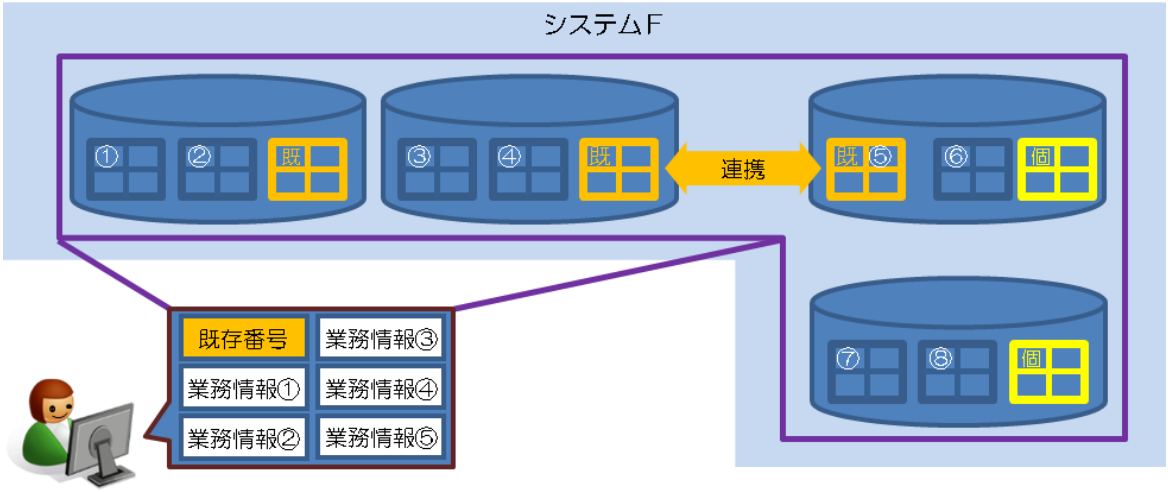
一方、既存番号で連携している場合であっても、アクセス制御がされておらず、個人番号そのものにアクセスできる場合は、特定個人情報ファイルに該当することになります【図２参照】。

○　なお、個人番号そのものにアクセスできる場合とは、事務を行う権限を有する者が個人番号とともに見ることができる場合のみでなく、システムの内部処理で個人番号と連携する場合もこれに該当します。

【図１】



【図２】



：特定個人情報ファイル

※画面には業務情報①～⑤と既存番号しか表示されない場合であっても、システムの内部で業務情報⑥～⑧と個人番号にアクセスできる場合には、紫の実線が特定個人情報ファイルに該当することとなる。

Q第４の３－２

アクセス制御により、個人番号そのものにはアクセスできず、個人番号以外の情報にのみアクセスできるように制御されている場合は、特定個人情報ファイルには該当しないとのことですが、アクセス制御とはどのようなものでしょうか。

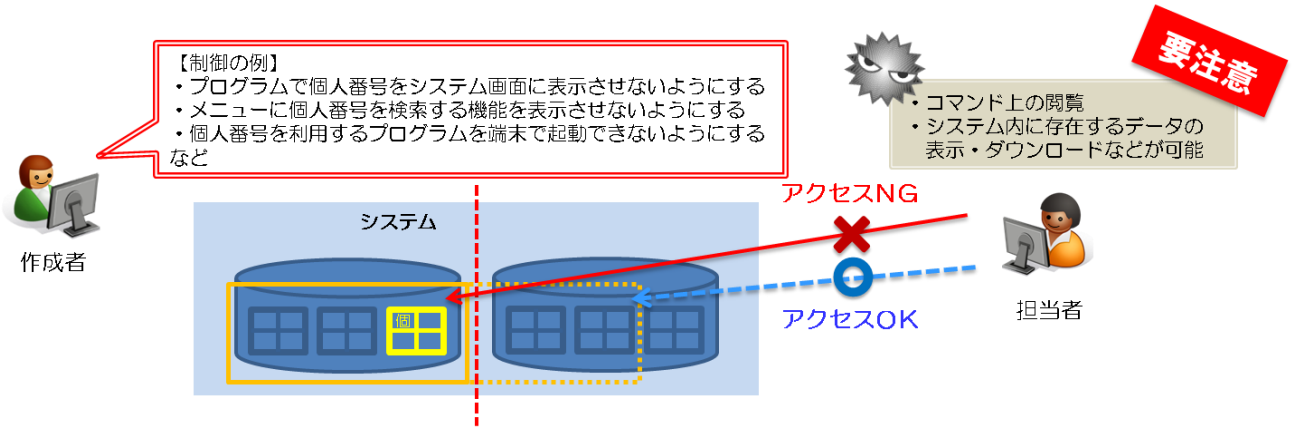
（Ａ）

○　事務を行う権限を有する者が個人番号を画面や帳票などで見ることができる場合や、システムの内部処理において個人番号を用いる場合は、特定個人情報ファイルに該当することになりますが、アクセス制御がされており、個人番号を画面や帳票で見ることができず、システムの内部処理においても用いていない場合には、特定個人情報ファイルに該当しません。アクセス制御の手法としては、次のような手法が考えられます。

①　画面・帳票における制御

事務を行う権限を有する者が個人番号を画面や帳票などで見ることができないようアクセス制御する手法としては、プログラムにより個人番号をシステム画面に表示させないようにすること、メニューに個人番号を検索する機能を表示させないようにすること、個人番号を利用するプログラムを端末で起動できないようにすることなどが考えられます。

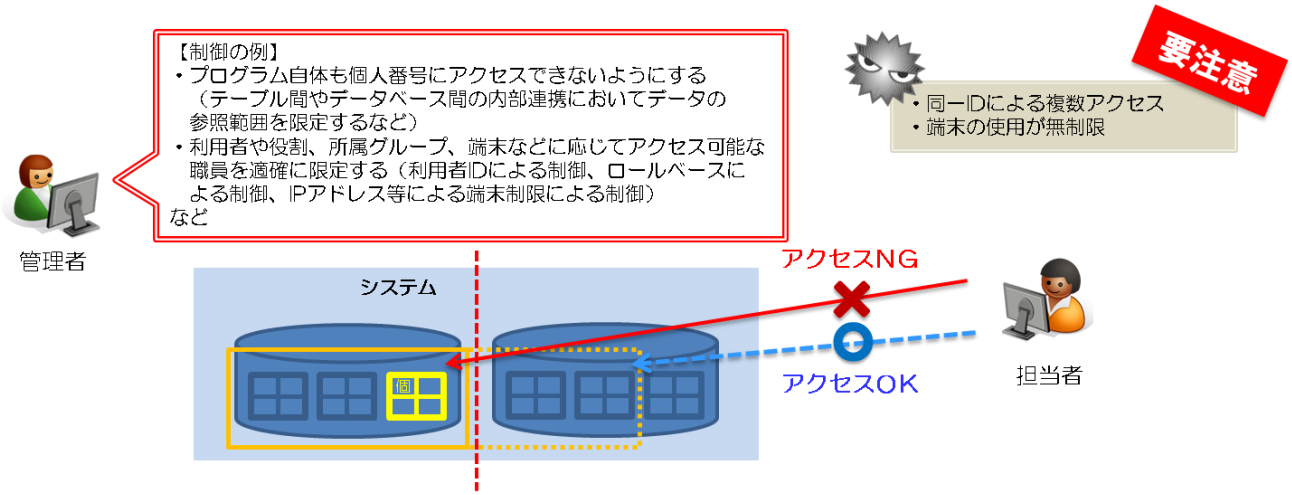
ただし、通常使用するシステム画面に個人番号が表示されなくても、コマンド上では個人番号が閲覧できるようになっている場合なども考えられますので、このような場合には、コマンド実行権限の制限などの措置も必要となります。また、通常使用するシステム画面には個人番号が表示されなくても、システムの機能により、システム内に存在するデータの表示・ダウンロードなどが可能であり、その中に個人番号が含まれる場合が考えられます。このような場合には、システム画面以外についても個人番号を表示・ダウンロードさせないよう制限するなどの措置が必要となります。



② 内部連携における制御

システムの内部処理において個人番号を用いないようアクセス制御するには、データベース・テーブル・ファイルの参照を制限したり、プログラムやコマンドの実行権限を制限したりすることなどが考えられます。具体的には、システムのプログラム自体も個人番号にアクセスできないようにすること、データベース等の設定により利用者や役割、所属グループ、端末などに応じてアクセス可能な職員を適確に限定すること（利用者 ID による制御、ロールベースによる制御、IP アドレス等による端末制限による制御）などが考えられます。

ただし、同一 ID による複数アクセスなど本来 ID を使ってはいけない者が ID を使って個人番号にアクセスする場合や、IP アドレス等による端末制限をしてもその端末が誰でも使用可能な状態になっている場合は、アクセス可能な職員を適確に限定しているとは言えません。



Q第４の３－３
　　特定個人情報と特定個人情報ファイルの差異とはどのようなものでしょうか。

（Ａ）

○　「個人番号をその内容に含む」の考え方は、上記に示す第４の３の解説のとおりとなります。

　特定個人情報と特定個人情報ファイルの違いについては、番号法第２条第８項において、特定個人情報とは個人番号をその内容に含む個人情報をいうと定められ、同条第９項において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うと定められています。したがって、特定個人情報と特定個人情報ファイルの差異は、個人情報と個人情報ファイル・個人情報データベース等の差異となります。

　個人情報と個人情報ファイル・個人情報データベース等の差異は、一般法の定義と同じとなりますが、個人情報ファイル又は個人情報データベース等とは、前記のとおり、特定の（保有）個人情報を（容易に）検索できるように体系的に構成した情報の集合物をいい、検索性を有すること、体系的構成物であること、情報の集合物であることが個人情報ファイル又は個人情報データベース等と個人情報との差異であるといえます。

Q第４の３－４
　　個人番号を含まないものは、特定個人情報に該当しないのでしょうか。

（Ａ）

○　個人番号を含まないものの、個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものをその内容に含む個人情報も、特定個人情報に該当することとなります（番号法第２条第８項）。例えば、情報提供ネットワークシステムを使用した情報提供の求め又は情報提供の際に用いられる符号や個人番号を部分的に修正したもので、個人番号と１対１で対応するものなどは、特定個人情報に該当することとなります。

Q第４の３－５

地方公共団体の個人情報保護条例等において特定個人情報ファイルについての定義が設けられていない場合は、特定個人情報保護評価の実施が義務付けられないのでしょうか。

（Ａ）

○　番号法第２条第９項において、「「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う」とされており、番号法第２条第４項においては、「「個人情報ファイル」とは、個人情報保護法第 60 条第２項に規定する個人情報ファイルであって行政機関等（個人情報保護法第２条第 11 項に規定する行政機関等をいう。）が保有するもの、又は個人情報保護法第 16 条第１項に規定する個人情報データベース等であって行政機関等以外の者が保有するものをいう」とされています。

したがって、各地方公共団体の個人情報保護条例において「特定個人情報ファイル」についての定義が設けられていない場合であっても、地方公共団体及び地方独立行政法人に対し、番号法及び個人情報保護法により定義された「特定個人情報ファイル」について特定個人情報保護評価の実施が義務付けられることとなります。

Q第４の３－６

ワープロソフトウェア等を用いて作成されたファイルは、特定個人情報ファイルに含まれるのでしょうか。

（Ａ）

○　ワープロソフトウェア等を用いて作成されたものであっても、特定個人情報が表形式に整理されたものなどは、特定個人情報ファイルに該当する可能性があります。ただし、特定の個人情報を容易に検索できるように索引や目次などを付していない場合や、文字列検索を行わなければ特定個人情報を検索できるようになっていないものについては、原則として特定個人情報ファイルに該当しません。

Q第４の３－７

　個人番号の記載された申請書を添付した決裁文書が格納された文書管理システムのようなものも特定個人情報保護評価の対象となるのでしょうか。

（Ａ）

○　決裁や文書保管を行うために文書管理システムのようなもので個人番号を保有する場合は、通常の場合であれば、特定個人情報ファイルに該当せず、特定個人情報保護評価の対象とはならないと考えられます。

○　それは、PDF ファイルなどで個人番号を含む申請書などを保管している場合は、文字列検索などで個人番号を偶然に検索することはできても、特定個人情報を検索できるような性質を有していないと考えられるためです。

○　一方で、表計算ソフトなどで個人番号を含む申請書などを保管している場合に、個人番号が表形式に整理されていたり、フィルタ機能で個人番号をソートできたりすれば、特定個人情報を検索できるような性質を有していると考えられ、特定個人情報ファイルに該当することになり、特定個人情報保護評価の対象となります。

Q第４の３－８

　特定個人情報ファイルと個人情報ファイルは、それぞれ独立したデータベースでなければならないのでしょうか。特定個人情報ファイルと個人情報ファイルを１つのデータベースの別テーブルとして管理し、アクセス制御を行うという方法は認められるのでしょうか。

（Ａ）

○　特定個人情報ファイルの単位は、データベースやテーブルの単位と合致する必要はありません。使用目的に基づき各評価実施機関の合理的裁量でファイルを分けることができます。

Q第４の３－９

　特定個人情報保護評価の対象としての特定個人情報ファイルを住所別に分ける、あるいは年齢別に分ける、といった取扱いをすることはできるのでしょうか。

（Ａ）

○　特定個人情報ファイルの単位は、使用目的に基づき評価実施機関が定めることができますが、使用目的以外の要素に基づいてファイルを分けることは、単なる属性による分類であり、適当ではありません。

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。

ア　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又はこれらに準ず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１号）

イ　手作業処理用ファイルのみを取り扱う事務（規則第４条第２号）

ウ　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（以下「対象人数」という。）が 1,000 人未満の事務（規則第４条第３号）

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）

オ　公務員若しくは公務員であった者又はその被扶養者の共済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５号）

カ　情報連携を行う事業者が情報連携の対象とならない特定個人情報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６号）

キ　会計検査院が検査上の必要により保有する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７号）

また、特定個人情報保護評価の対象となる事務において複数の特定個人情報ファイルを取り扱う場合で、その一部が上記（ウを除く。）に定める特定個人情報ファイルである場合は、その特定個人情報ファイルに関する事項を特定個人情報保護評価書に記載しないことができる。

（２）特定個人情報保護評価以外の番号法の規定の適用

上記（１）に定める特定個人情報保護評価の実施が義務付けられない事務であっても、特定個人情報保護評価以外の番号法の規定が適用され、当該事務を実施する者は、番号法に基づき必要な措置を講ずることが求められる。

（解説）

特定個人情報保護評価は、①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、②国民・住民の信頼の確保を目的とするものであり、特定個人情報ファイルを取り扱う事務については、任意での実施も含めて、特定個人情報保護評価を全て実施することも可能です。

ただし、上記の目的を踏まえ、特定個人情報保護評価の実施が義務付けられる必要があるとまでは考えられない事務（指針第４の４（１）ア～カに掲げる事務）については、特定個人情報保護評価の実施が義務付けられないとしています。また、会計検査院は、内閣から独立した立場で会計検査を実施する機関であることから、委員会の承認を得なければならないとするのは適当でないため、特定個人情報保護評価の実施が義務付けられないとしています。

なお、特定個人情報保護評価が積極的な事前対応を行うものであることに照らせば、特定個人情報ファイルが電子計算機用ファイルか手作業処理用ファイルか定まっていない段階や、特定個人情報ファイルの内容が具体的に定まっていない制度・施策の段階においても、個人のプライバシー等の権利利益に対して与える影響を事前に予測・評価し、このような影響を軽減する措置を講ずることが有益な場合もあると考えられます。

Ｑ第４の４（１）－１

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又はこれらに準ず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について特定個人情報保護評価の実施が義務付けられないのは、どのような理由なのでしょうか。

（Ａ）

○　これらの事項は、使用者としての各機関と、被用者としての職員との関係に基づく内部的な情報であり、また、その存在や利用方法も当事者たる職員にはよく知られており、国民・住民の信頼を確保するという特定個人情報保護評価の目的が直接は当てはまらないと考えられます。

○　また、これらのファイルには、職員の被扶養者又は遺族の福利厚生等に関する情報も含まれることとなりますが、各機関がこれらの者に関する事務を行うことも使用者と被用者との内部的関係に基づくものであり、また、その存在等も当事者である被扶養者又は遺族にも知られていると考えられます。

○　これらの特定個人情報ファイルにも番号法のその他の規制は及ぶことに加え、仮にこれらの特定個人情報ファイルの取扱いについて問題があれば、各機関と職員との交渉で改善を促す方が効果的かつ妥当であり、国民（地方公共団体等にあっては

住民等）からの意見聴取や特定個人情報保護評価書の公表を行う特定個人情報保護評価の対象とする必要性が乏しいと考えられるため、特定個人情報保護評価の実施が義務付けられないとしています。

○　なお、個人情報保護法でも、職員若しくは職員であった者又はそれらの者の被扶養者若しくは遺族等に係る個人情報ファイルであって、人事、給与若しくは福利厚生に関する事項又はこれらに準ずる事項を記録するものについては、個人情報ファイルの事前通知及び個人情報ファイル簿の作成・公表義務の例外とされています（同法第 74 条第２項第３号及び第 10 号、第 75 条第２項第１号、個人情報の保護に関する法律施行令第 19 条第３項）。

Ｑ第４の４（１）－２①
手作業処理用ファイルのみを取り扱う事務について特定個人情報保護評価の実施が義務付けられないのは、どのような理由なのでしょうか。

（Ａ）

○　手作業処理用ファイルとは、個人情報保護法第 60 条第２項第２号等に規定する個人情報ファイル・個人情報データベース等をいい、電子計算機を用いて特定個人情報を検索できるものではないものの、索引・目次等により容易に特定の特定個人情報を検索することができるものをいいます。具体的には、申請者の氏名を五十音順にして保管されている申請書台帳などをいいます。手作業処理用ファイルは、電子計算機用ファイルに比して大量処理・高速処理・結合の容易性・検索の容易性等の特性を有しておらず、個人のプライバシー等の権利利益に与える影響も小さいと考えられますので、特定個人情報保護評価の実施が義務付けられないとしています。

○　なお、個人情報保護法でも、手作業処理に係る個人情報ファイルについては、委員会への事前通知の義務が適用されていません（同法第 74 条第２項第 11 号）。

Ｑ第４の４（１）－２②

手作業処理用ファイルのみを取り扱う事務で情報連携を行う際は、中間サーバー端末を直接使用し、情報の入力や照会を行っていますが、特定個人情報保護評価はどのように実施すればよいのでしょうか。

（Ａ）

○　この場合、手作業処理用ファイルのみを取り扱う事務とはいえず、特定個人情報保護評価を実施する必要があります。以下、詳細に説明します。

○　番号法別表第一に掲げられる個人番号利用事務のうち別表第二に掲げる情報提供ネットワークシステムを用いて情報連携を行う事務については、特定個人情報の照会・提供を行う際に使用する中間サーバー内に「符号」を保有することになります。番号法第２条第８項では「特定個人情報」とは、「個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報」と定義されており、中間サーバー内に保有する「符号」をその内容に含む個人情報ファイルは、指針第２の10に示すシステム用ファイルに該当します。

したがって、この場合、システム用ファイルを取り扱っていますので、手作業処理用ファイルのみを取り扱う事務とはいえず、情報提供ネットワークシステムを利用して照会や提供を行うために使用する特定個人情報ファイルの取扱いについて、特定個人情報保護評価を実施する必要があります。

Ｑ第４の４（１）－３

対象人数が 1,000 人未満の事務について特定個人情報保護評価の実施が義務付けられないのは、どのような理由なのでしょうか。

（Ａ）

○　特定個人情報ファイルを取り扱う事務の対象人数が 1,000 人未満の場合、大量処理・高速処理・結合の容易性・検索の容易性等の点で、特定個人情報保護評価の実施が義務付けられる事務と比べ、個人のプライバシー等への権利利益に与える影響が小さいと考えられますので、特定個人情報保護評価の実施が義務付けられないとしています。

○　なお、個人情報保護法においても、本人の数が 1,000 人未満の個人情報ファイルは、委員会への事前通知の義務が適用されていません（個人情報保護法第 74 条第２項第９号、個人情報の保護に関する法律施行令第 19 条第２項）。

Ｑ第４の４（１）－４

複数の特定個人情報ファイルを取り扱う事務において、個々の特定個人情報ファイルに記録される本人の数が 1,000 人未満である場合も、特定個人情報保護評価の実施が義務付けられるのでしょうか。また、その中に、手作業処理用の特定個人情報ファイルや職員の福利厚生に関する事項を記録した特定個人情報ファイルが含まれる場合、対象人数はどのように考えればよいのでしょうか。

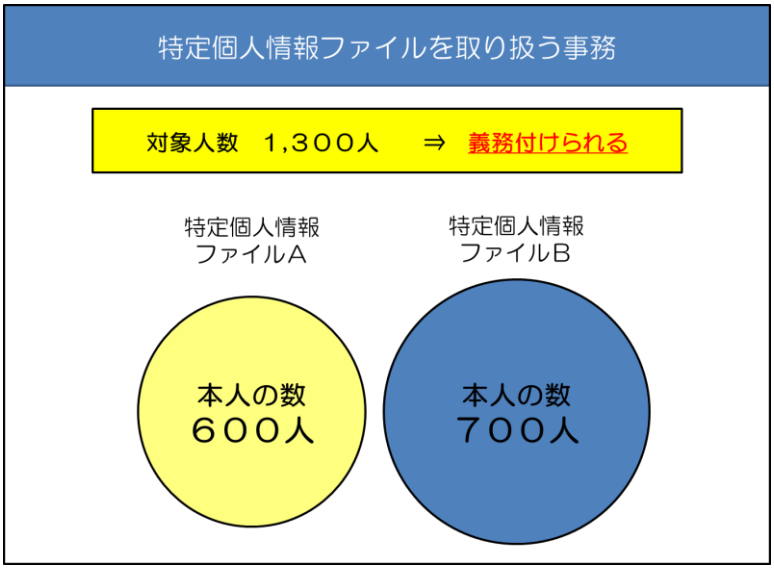
（Ａ）

○　特定個人情報ファイルＡ（本人の数 600 人）と特定個人情報ファイルＢ（本人の数 700 人）を取り扱う事務を例にとります。

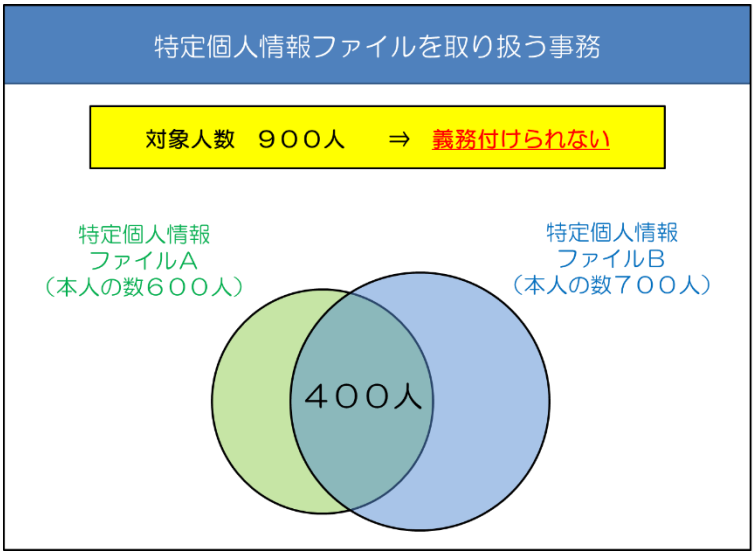
【当該事務において取り扱うファイルに、第４の４（１）ア、イ、エ、オ、カ又はキに規定する特定個人情報ファイルが含まれない場合】

○　個々の特定個人情報ファイルに記録される本人の数が 1,000 人未満であっても、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（対象人数）が 1,000 人以上である場合は、特定個人情報保護評価の実施が義務付けられます。

○　Ａの本人とＢの本人が重複しない場合、Ａ及びＢを取り扱う事務の対象人数は 1,300 人となり、特定個人情報保護評価の実施が義務付けられます。

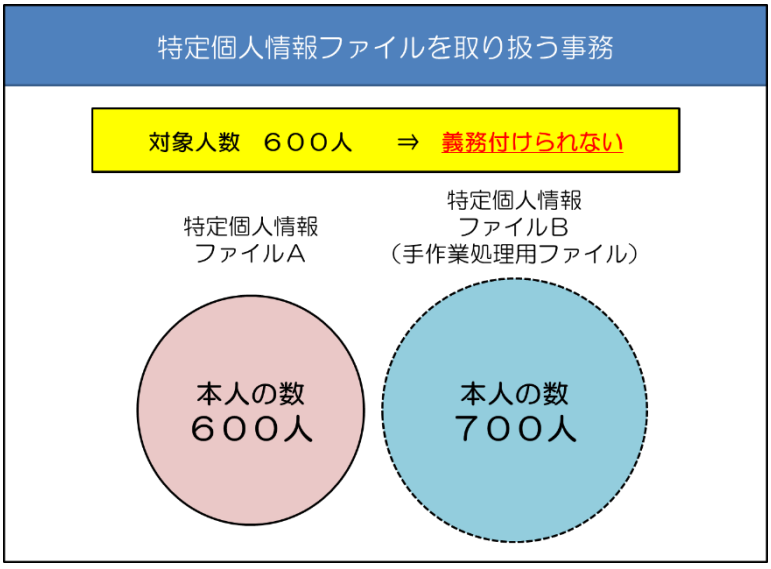


○　Ａの本人とＢの本人が全部又は一部重複しており、Ａ及びＢを取り扱う事務の対象人数が 1,000 人未満となる場合は、特定個人情報保護評価の実施が義務付けられないこととなります。



【当該事務において取り扱うファイルに、第４の４（１）ア、イ、エ、オ、カ又はキに規定する特定個人情報ファイルが含まれる場合】

○　Ａ又はＢのいずれかが第４の４（１）ア、イ、エ、オ、カ又はキに規定する特定個人情報ファイルである場合、それらの特定個人情報ファイルに記録される本人の数はカウントしません。したがって、Ａ及びＢを取り扱う事務の対象人数は 1,000 人未満となり、特定個人情報保護評価の実施が義務付けられないこととなります。



Q第４の４（１）－５

「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」とはどのようなものが該当するのでしょうか。また特定個人情報保護評価の実施が義務付けられないのは、どのような理由なのでしょうか。

（Ａ）

○　具体的には、単一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がこれに該当します。

○　単一組合には、１事業所の事業主が単独で設立した健康保険組合のほか、密接な関係を有する２以上の事業所の事業主が共同又は連合して設立した健康保険組合（※）が含まれます。

○　総合組合（※）や、全国健康保険協会（協会けんぽ）、国民健康保険組合、国民健康保険を行う市町村、後期高齢者医療広域連合、日本私立学校振興・共済事業団が保有する医療保険事務に関する特定個人情報ファイルは、これに該当せず、特定個人情報保護評価の実施が義務付けられることとなります。

（※）「健康保険組合設立認可基準について」（昭和 60 年４月 30 日保発第 44 号、最終改正平成 20 年３月６日保発第 0306004 号）参照。

○　健康保険組合と被保険者は、使用者と被用者の関係に立つものではありませんが、単一組合の場合、健康保険組合自体は使用者である企業自体とは別法人ではあるものの、使用者（事業主）が設立する法人であり、かつ健康保険組合と使用者は１対１で対応しているため、実態として健康保険組合と使用者である企業自体を同視することができます。

○　仮に、これらの特定個人情報ファイルの取扱いについて問題があっても、企業本体や健康保険組合と職員との交渉で改善を促す方が効果的であり妥当であるため、アの「職員又は職員であった者の人事、給与、福利厚生に関する事項」に準じた内部関係として考えられますので、特定個人情報保護評価の実施が義務付けられないとしています。

Q第４の４（１）－６

公務員若しくは公務員であった者又はその被扶養者の共済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について特定個人情報保護評価の実施が義務付けられないのは、どのような理由なのでしょうか。

（Ａ）

○　具体的には、国家公務員共済組合連合会、国家公務員共済組合（※１）、地方公務員共済組合連合会、地方公務員共済組合（※２）、全国市町村職員共済組合連合会、存続共済会（※３）、存続組合及び指定基金（※４）、地方公務員災害補償基金が保有する共済に関する特定個人情報ファイルがこれに該当します。

○　特定個人情報保護評価は、番号制度の導入により、国家による個人情報の一元的な管理が行われるのではないかとの懸念などに対応する観点から導入される制度であることから、公務員若しくは公務員であった者又はその被扶養者（※５）を対象とするこれらのファイルを取り扱う事務については、特定個人情報保護評価の実施が義務付けられないとしています。

（※１）国家公務員共済組合とは、衆議院共済組合、参議院共済組合、内閣共済組合、総務省共済組合、法務省共済組合、外務省共済組合、財務省共済組合、文部科学省共済組合、厚生労働省共済組合、農林水産省共済組合、経済産業省共済組合、国土交通省共済組合、防衛省共済組合、裁判所共済組合、会計検査院共済組合、刑務共済組合、厚生労働省第二共済組合、林野庁共済組合、日本郵政共済組合、国家公務員共済組合連合会職員共済組合をいいます。

（※２）地方公務員共済組合とは、市町村職員共済組合、都市職員共済組合、指定都市職員共済組合、東京都職員共済組合、地方職員共済組合、警察共済組合、公立学校共済組合をいいます。

（※３）存続共済会とは、都道府県議会議員共済会、市議会議員共済会、町村議会議員共済会をいいます。

（※４）存続組合及び指定基金とは、日本鉄道共済組合、日本たばこ産業共済組合、NTT企業年金基金をいいます。

（※５）国家公務員共済組合連合会等上記に記載した共済組合等は、公務員若しくは公務員であった者又はその被扶養者の特定個人情報ファイルのみでなく、当該共済組合等の職員若しくは職員であった者又はその被扶養者の特定個人情報ファイルも保有しますが、共済組合等の職員又は職員であった者の特定個人情報ファイルを取り扱う事務も、指針第４の４（１）エの場合と同様であることから、特定個人情報保護評価の実施が義務付けられないとしています。したがって、これらの共済組合等が保有する、当該共済組合等の組合員若しくは組合員であった者又はその被扶養者の共済に関する事項を記録する特定個人情報ファイルは、全体として特定個人情報保護評価の実施が義務付けられないこととなります。

Q第４の４（１）－７

情報連携を行う事業者が情報連携の対象とならない特定個人情報を記録した特定個人情報ファイルのみを取り扱う事務について特定個人情報保護評価の実施が義務付けられないのは、どのような理由なのでしょうか。

（Ａ）

○　情報連携を行う事業者は、事業のために個人番号を取り扱う者であり、番号制度への関与の程度が深く、その特定個人情報ファイルの保有が個人に対して与える影響も大きいと考えられることから、特定個人情報保護評価の実施が義務付けられています。

○　しかしながら、情報連携を行う事業者が実施する事務のうち、情報連携を行わない事務については、主に源泉徴収義務等のために個人番号を取り扱うことが予定され、事業目的で個人番号を利用するものではないと考えられるため、このような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としています。

Q第４の４（１）－８

会計検査院が検査上の必要により保有する特定個人情報ファイルのみを取り扱う事務について特定個人情報保護評価の実施が義務付けられないのは、どのような理由なのでしょうか。

（Ａ）

○　会計検査院は、内閣から独立した立場で会計検査を実施する機関であることから、委員会の承認を得なければならないとするのは適当でないため、特定個人情報保護評価の実施が義務付けられないとしています。

○　なお、個人情報保護法においても、会計検査院の保有する個人情報ファイルは、委員会への事前通知の義務が適用されていません（個人情報保護法第 74 条）。

Q第４の４（１）－９

特定個人情報保護評価の対象となる事務において、システムで取り扱われる特定個人情報ファイルについて特定個人情報保護評価を実施している場合に、一時的な作業のために指針第２の 11 で定義されている「その他の電子ファイル」を保有し、当該ファイルに記録される主な項目がシステムで取り扱われる特定個人情報ファイルに記録される項目の一部となっているときは、当該ファイルについて特定個人情報保護評価を実施しなければならないのでしょうか。

（Ａ）

○　特定個人情報保護評価の対象となる事務において保有する一時的な作業のためのファイルであって、当該ファイルに記録される主な項目がシステムで取り扱われる特定個人情報ファイルに記録される項目の一部となっているような場合については、当該ファイルが経常的に取り扱われるものではなく、かつ、当該ファイルに記録される本人の数が 1,000 人未満である場合には、特定個人情報保護評価の実施は求められていないと考えられます。このようなファイルは、その事務におけるシステムで取り扱われる特定個人情報ファイルについて特定個人情報保護評価が実施されており、かつ、大量処理・結合の容易性等の点で個人のプライバシー等への権利利益に与える影響が小さいと考えられるためです。

○　なお、このような特定個人情報ファイルについても、当然、番号法のその他の規制（提供制限、安全管理措置、ファイルの作成制限、開示等、収集・保管の制限等）が及ぶものであり、適切な管理のために必要な措置を講じなければなりません。

Q第４の４（１）－10

特定個人情報保護評価の実施が義務付けられる事務以外であれば、特定個人情報ファイルに対する特段の措置は不要となるのでしょうか。

（Ａ）

○　特定個人情報保護評価の実施が義務付けられる事務以外であっても、当然、番号法のその他の規制（提供制限、安全管理措置、ファイルの作成制限、開示等、収集・保管の制限等）が及ぶものであり、適切な管理のために必要な措置を講じなければなりません。

第５　特定個人情報保護評価の実施手続

１　特定個人情報保護評価計画管理書

（１）特定個人情報保護評価計画管理書の作成

評価実施機関は、最初の特定個人情報保護評価を実施する前に、特定個人情報保護評価計画管理書（様式１参照）を作成するものとする。

特定個人情報保護評価計画管理書は、特定個人情報保護評価を計画的に実施し、また、特定個人情報保護評価の実施状況を適切に管理するために作成するものである。評価実施機関で実施する特定個人情報保護評価に関する全ての事務及びシステムについて記載するものとし、評価実施機関単位で作成するものとする。

特定個人情報保護評価計画管理書の記載事項に変更が生じたときは、特定個人情報保護評価計画管理書を速やかに更新するものとする。

（２）特定個人情報保護評価計画管理書の提出

評価実施機関は、規則第３条の規定に基づき、最初の特定個人情報保護評価書の委員会への提出の際に、特定個人情報保護評価計画管理書を併せて提出するものとする。その後、評価実施機関が特定個人情報保護評価書を委員会へ提出する際は、その都度、特定個人情報保護評価計画管理書を更新し、併せて提出するものとする。

特定個人情報保護評価計画管理書の公表は、不要とする。

（解説）

評価実施機関は、機関として最初に実施する特定個人情報保護評価に先立ち、特定個人情報保護評価計画管理書を作成します。機関として初めて特定個人情報保護評価書（基礎項目評価書、重点項目評価書又は全項目評価書）を委員会に提出する際又はその前に、特定個人情報保護評価計画管理書も併せて提出することとなります。

特定個人情報保護評価計画管理書は、評価実施機関が実施する特定個人情報保護評価の全体像を記載する資料ですので、評価実施機関が実施する特定個人保護評価の対象となる事務及びそれらの事務で使用するシステム全てについて概要を記載します。特定個人情報保護評価計画管理書は機関で一通作成することになります。評価実施機関は、特定個人情報保護評価計画管理書の記載事項に変更があればその都度更新し、特定個人情報保護評価書を委員会に提出する際は、最新の状況を反映させて更新した特定個人情報保護評価計画管理書を併せて提出することとなります。

Ｑ第５の１－１
　　特定個人情報保護評価計画管理書を作成する目的はどのようなものでしょうか。

（Ａ）

○　特定個人情報保護評価計画管理書を作成する目的は、評価実施機関が実施する特定個人情報保護評価の対象となる事務とそれらの事務で使用するシステムを中心に、評価実施機関における特定個人情報ファイルの取扱いの全体像を把握し、特定個人情報保護評価の実施について、計画と管理を適切に行うことです。

○　まず、特定個人情報保護評価を実施する「事務の単位」を検討するために、特定個人情報保護評価計画管理書を活用することが考えられます。多くの評価実施機関は、数多くの事務で特定個人情報ファイルを取り扱っていると想定されます。また、それらの事務に用いるために評価実施機関で運用しているシステムも複数存在し、しかも事務とシステムとが１対１で対応してないことも想定されます。特定個人情報保護評価は、法令上の事務ごとに実施することが原則ですが、使用しているシステムとの関係等から、法令上の１つの事務を分割してあるいは複数の事務を統合して実施することが適当な場合もあります。特定個人情報保護評価計画管理書を作成・更新する中で、特定個人情報ファイルを取り扱う事務とシステムの全体像を把握し、特定個人情報保護評価を実施する事務の単位について適切に判断することが期待されます。

○　また、特定個人情報保護評価計画管理書は、特定個人情報保護評価を実施すべき時期を把握するためにも活用できます。特定個人情報保護評価は特定個人情報ファイルを保有する前、重要な変更を加える前に実施しなければなりません。また、公表した特定個人情報保護評価書を少なくとも１年に１回は見直し、公表してから５年を経過する前に再実施するよう努めることが求められています。特定個人情報保護評価の対象となる事務の一覧を、特定個人情報保護評価を直近に実施した日と併せて管理していくことで、特定個人情報保護評価の進行管理を行うことが期待されます。

Ｑ第５の１－２
　　特定個人情報保護評価の対象となる事務がなくても、特定個人情報保護評価計画管理書を作成する必要があるのでしょうか。

（Ａ）

○　作成しなければならないものではありません。

　しかしながら、特定個人情報ファイルを保有するものの対象人数が 1,000 人未満であるために特定個人情報保護評価の実施が義務付けられない場合などに、特定個

人情報保護評価計画管理書を任意で作成し、個人番号の利用あるいは特定個人情報ファイルの作成が適切な範囲で行われていることを確認するために活用することが考えられます。

Q第５の１－３
　特定個人情報保護評価の対象となる事務が１つしかなくても、特定個人情報保護評価計画管理書を作成する必要があるのでしょうか。

（Ａ）

○　特定個人情報保護評価の対象となる事務が１つでもある場合は、その特定個人情報保護評価の実施に先立って、特定個人情報保護評価計画管理書を作成することが必要となります。

Q第５の１－４
　全体を非公表とすることができる特定個人情報保護評価書（犯罪の捜査、犯則事件の調査、公訴の提起又は維持のために保有する特定個人情報ファイルに関するもの）についても、特定個人情報保護評価計画管理書に記載する必要があるのでしょうか。

（Ａ）

○　記載することが必要です。

　全体を非公表とすることができる特定個人情報保護評価書であっても、委員会による審査・承認（行政機関等が提出する全項目評価書）又は精査・確認（その他の特定個人情報保護評価書）の対象であり、特定個人情報保護評価計画管理書を作成する目的に照らし、記載することが必要となります。

　なお、特定個人情報保護評価計画管理書はその全体が非公表です。

Q第５の１－５
　特定個人情報保護評価計画管理書等に記載することになっている「法令上の根拠」について、法令の数が数百あり全て記載することが困難な場合はどのようにすればよいのでしょうか。

（Ａ）

○　代表的な法令上の根拠を幾つか選び、「●●法３条、■■法４条１項等」などと記載してください。

２　しきい値判断

特定個人情報ファイルを取り扱う事務について特定個人情報保護評価を実施するに際しては、①対象人数、②評価実施機関の従業者及び評価実施機関が特定個人情報ファイルの取扱いを委託している場合の委託先の従業者のうち、当該特定個人情報ファイルを取り扱う者の数（以下「取扱者数」という。）、③評価実施機関における規則第４条第８号ロに規定する特定個人情報に関する重大事故の発生（評価実施機関が重大事故の発生を知ることを含む。以下同じ。）の有無に基づき、次のとおり、実施が義務付けられる特定個人情報保護評価の種類を判断する（以下「しきい値判断」という。）。

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もの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ができ、重点項目評価の実施が義務付けられると判断されたものについても任意で全項目評価を実施することができる。なお、重点項目評価の実施が義務付けられると判断されたものについて、任意で全項目評価を実施した場合は、重点項目評価を併せて行ったものとして取り扱う。

（１）対象人数が 1,000 人以上１万人未満の場合は、基礎項目評価（番号法第 28 条第１項並びに規則第４条第８号イ及び第５条）

（２）対象人数が１万人以上 10 万人未満であり、かつ、取扱者数が 500 人未満であって、過去１年以内に評価実施機関における特定個人情報に関する重大事故の発生がない場合は、基礎項目評価（番号法第 28 条第１項並びに規則第４条第８号ロ及び第５条）

（３）対象人数が１万人以上 10 万人未満であり、過去１年以内に評価実施機関における特定個人情報に関する重大事故の発生があった場合は、基礎項目評価及び重点項目評価（番号法第 28 条第１項並びに規則第４条第９号、第５条並びに第６条第１項第１号及び第３項）

（４）対象人数が１万人以上 10 万人未満であり、かつ、取扱者数が 500 人以上の場合は、基礎項目評価及び重点項目評価（番号法第 28 条第１項並びに規則第４条第９号、第５条並びに第６条第１項第１号及び第３項）

（５）対象人数が 10 万人以上 30 万人未満であり、かつ、取扱者数が 500 人未満であって、過去１年以内に評価実施機関における特定個人情報に関する重大事故の発生がない場合は、基礎項目評価及び重点項目評価（番号法第 28 条第１項並びに規則第４条第９号、第５条並びに第６条第１項第２号及び第３項）

（６）対象人数が 10 万人以上 30 万人未満であり、過去１年以内に評価実施機関における特定個人情報に関する重大事故の発生があった場合は、基礎項目評価及び全項目評価（行政機関等については番号法第 28 条及び規

則第５条、地方公共団体等については番号法第 28 条第１項並びに規則第４条第 10 号並びに第７条第１項及び第３項から第６項まで）
（７）対象人数が 10 万人以上 30 万人未満であり、かつ、取扱者数が 500 人以上の場合は、基礎項目評価及び全項目評価（行政機関等については番号法第 28 条及び規則第５条、地方公共団体等については番号法第 28 条第１項並びに規則第４条第 10 号並びに第７条第１項及び第３項から第６項まで）
（８）対象人数が 30 万人以上の場合は、基礎項目評価及び全項目評価（行政機関等については番号法第 28 条及び規則第５条、地方公共団体等については番号法第 28 条第１項並びに規則第４条第 10 号並びに第７条第１項及び第３項から第６項まで）

（解説）

特定個人情報保護評価に要するコスト・作業量に鑑みれば、特定個人情報ファイルを取り扱う事務の全てについて特定個人情報保護評価を実施しようとすると、かえって特定個人情報保護評価が形式化・形骸化するおそれがあると考えられます。

そこで、特定個人情報保護評価の目的を達成し、実効性のある仕組みとするために、必要性に応じたメリハリのある仕組みをとることとし、個人のプライバシー等の権利利益に対して影響を与える可能性が高いと認められるものについて手厚い特定個人情報保護評価を実施することとしています。

具体的には個人のプライバシー等の権利利益に対し影響を与える可能性の観点から、次の３つのしきい値判断項目に基づき、実施が義務付けられる特定個人情報保護評価のレベルを判断することになります。しきい値判断項目を客観的に判定される項目とすることで、特定個人情報保護評価の実施レベルの振り分けが判断者の恣意に流れないことを担保しています。

《しきい値判断項目》

１　事務の対象人数
２　特定個人情報ファイルの取扱者数
３　特定個人情報に関する重大事故の有無

「対象人数」は、より多くの特定個人情報を取り扱う場合は、不正な使用・提供の誘因となり得る等、特定個人情報の漏えいその他の事態が発生するリスクが高いと考えられるため、しきい値判断項目としています。「取扱者数」は、少数の限定された者にのみ情報を取り扱わせる場合に比べ、多数の者が取り扱う場合は、情報の流出や不正な使用・提供のリスクが高まると考えられるため、しきい値判断項目と

しています。「特定個人情報に関する重大事故の有無」は、国民の懸念が大きいと考えられ、特定個人情報に関する重大事故が発生した場合は全項目評価又は重点項目評価を実施する必要性が高まると考えられるため、しきい値判断項目としています。

なお、諸外国で採用されているプライバシー影響評価（Privacy Impact Assessment: PIA）においても、しきい値評価を実施してプライバシー影響評価が必要か否かを判断しているものがあります。

※ しきい値評価として、例えば、アメリカの連邦法である 2002 年電子政府法（E-Government Act of 2002）や 2002 年国土安全保障法（Homeland Security Act of 2002）で義務付けられるプライバシー影響評価（PIA）では、プライバシーしきい値分析（Privacy Threshold Analysis）が行われています。また、オーストラリアの連邦のプライバシー・コミッショナーが作成したプライバシー・インパクト・アセスメント・ガイドでもしきい値評価（Threshold Assessment）が採用されています（平成 29 年 3 月現在）。

しきい値判断の結果、実施が義務付けられる特定個人情報保護評価のレベルが判断され、

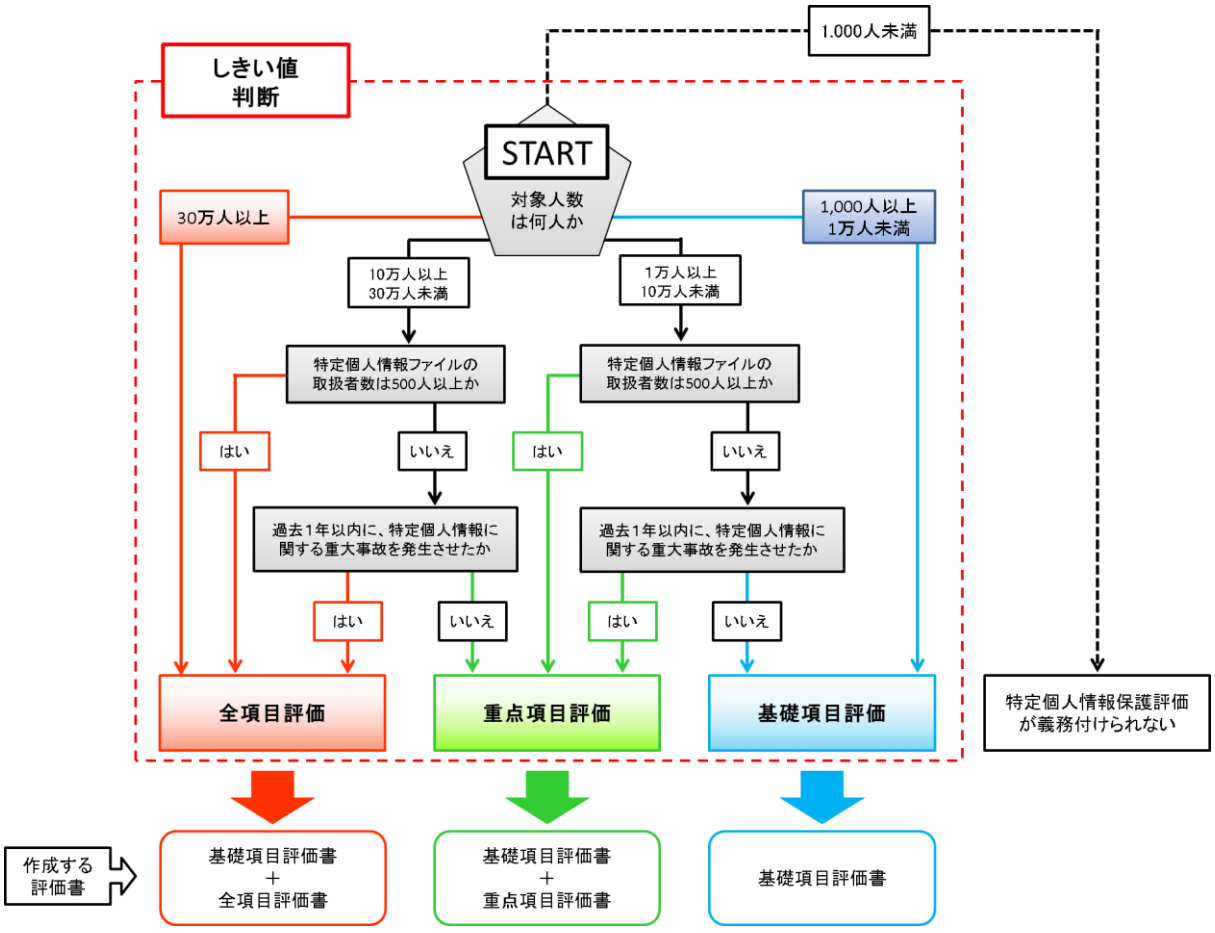
① 基礎項目評価
② 基礎項目評価及び重点項目評価
③ 基礎項目評価及び全項目評価

のいずれかの実施が求められることになります。

しきい値判断の結果、個人のプライバシー等の権利利益に影響を与えると考えられるものは、より詳細な検討・評価が行われ、これにより個人のプライバシー等の権利利益の保護のための措置の実施が促進されるものと考えられます。

また、番号法第 28 条においては、本来実施されるべき全項目評価について規定していますが、同条に基づき法律の適用を除外するものを規則で定めるとされていることから、基礎項目評価、重点項目評価及び地方公共団体等の実施する全項目評価については、規則で定めているものです。

＜しきい値判断フロー図＞


1,000人未満
しきい値
判断
START
対象人数
は何人か
30万人以上
1,000人以上
1万人未満
10万人以上
30万人未満
1万人以上
10万人未満
特定個人情報ファイルの
取扱者数は500人以上か
特定個人情報ファイルの
取扱者数は500人以上か
はい
いいえ
はい
いいえ
過去1年以内に、特定個人情報に
関する重大事故を発生させたか
過去1年以内に、特定個人情報に
関する重大事故を発生させたか
はい
いいえ
はい
いいえ
全項目評価
重点項目評価
基礎項目評価
特定個人情報保護評価
が義務付けられない
作成する
評価書
基礎項目評価書
＋
全項目評価書
基礎項目評価書
＋
重点項目評価書
基礎項目評価書

１．対象人数について

Ｑ第５の２－１．－１
　　対象人数は、どのように考えればよいのでしょうか。

（Ａ）

○　規則において、対象人数は「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」をいうとされています。一般に、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いうと考えられます。

○　なお、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、被保険者等に限定されません。例えば、医療保険の場合であれば、その被保険者だけではなく、被扶養者等についても個人番号を保有するのであれば、被保険者の数だけでなく、被扶養者等の数も対象人数に含まれます。

Ｑ第５の２－１．－２
　　対象人数の最新値を常に正確に把握することは困難です。どのようにしたらよいのでしょうか。

（Ａ）

○　対象人数は１人単位や 10 人単位などの粒度で記載するものではなく、概数で記載することができます。

Ｑ第５の２－１．－３
　　特定個人情報保護評価を実施する事務において、最初に保有している個人情報には個人番号が紐付かないものの、個人番号に紐付く個人情報が徐々に増え、対象人数が徐々に増えていくような場合、対象人数をどのように考えればよいのでしょうか。

（Ａ）

○　個人番号の利用開始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を対象人数とするのではなく、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、対象人数を記載してください。これまでその事務において経常的に取り扱ってきた個人情報の本人の数のうち個人番号と紐付くと考えられる数、その事務において今後経常的に取り扱うことが予測される個人情報の本人の数のうち個人番号と紐付くと考えられる数、特定個人情報の保存期間の予測等により推測することが考えられます。システム設計上又は予算上想定し

ている人数があれば、それを記載することも考えられます。給付申請やデータの削除時期が集中することなどにより、対象人数が期間によってばらつきがある場合は、これまでその事務において経常的に取り扱ってきた特定個人情報の本人の数のピークの水準等により、対象人数を合理的に推測することとなります。

Ｑ第５の２－１．－４
　　１つの事務において、複数の特定個人情報ファイルを取り扱う場合は、対象人数をどのように数えたらよいのでしょうか。

（Ａ）

○　それぞれの特定個人情報ファイルに記録される本人に重複がある場合、二重に算定する必要はなく、延べ人数ではなく固有数でカウントすれば足ります。

Ｑ第５の２－１．－５
　　地方公共団体の宛名システムのような個人番号と既存番号の対照テーブルを参照できる場合は、対象人数をどのようにカウントすればよいのでしょうか。

（Ａ）

○　対象人数は、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カウントする必要があり、特定個人情報ファイルの範囲と直接結びつくとは限りません。次の具体例を用いて説明すると、ケース①からケース③までのいずれの場合も、A給付事務において、経常的に取り扱う特定個人情報の本人の数は 11 万人ですので、対象人数は 11 万人ということになります。

○　ただし、番号法においては、個人番号を利用することができる事務が限定されており、個人番号を利用できるのは当該事務の処理に当たって必要な限度であるとされています。したがって、A給付事務に携わる職員が当該事務の処理以外の目的で特定個人情報の検索等を行うことは法令上禁止されていることから、システム上の対策を講ずるなど厳格に管理する必要があります。

＜ケース①　事務システムと、個人番号と既存番号（ここでは宛名番号という。）の対照テーブルを有するシステム（ここでは宛名システムという。）が別々のシステムであるケース＞

○　ケース①の図は、次のようなケースを表しています。

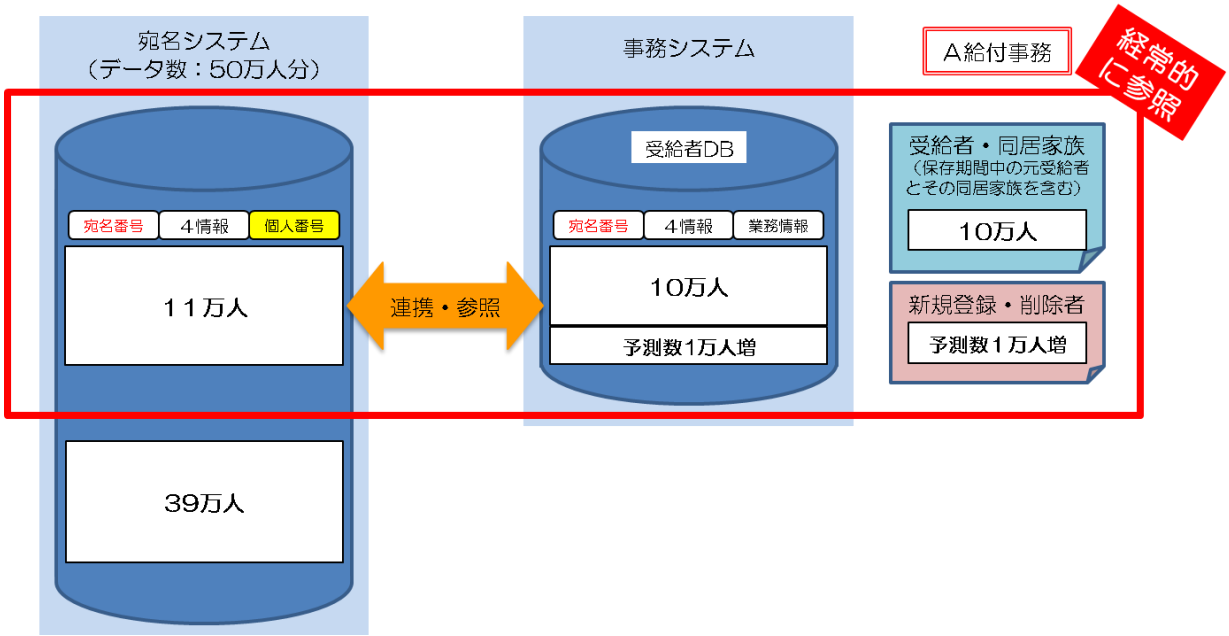
・　A給付事務を処理するために必要な情報として、評価実施機関では、受給者・同居家族（保存期間中の元受給者とその同居家族を含む。以下同じ。）の特定個人情報ファイルを取り扱っています。

・　A給付事務では、その時点における受給者・同居家族のデータとして、既に 10 万人分のデータを事務システムの受給者DBに格納しています。

・　A給付事務における今後の増減分を、新規登録によって増加する数と保存期間の満了等により削除される者の数（以下「新規登録・削除者数」という。）を基に合理的に予測すると、約１万人分のデータが増加することが予測され、この増加分についても受給者DBに格納される見込みとなっています。

・　事務システムと宛名システムは別々のシステムですが、A給付事務を処理するに当たっては、事務システム（11 万人分）の情報だけでなく、宛名番号をキーとして宛名システム（50 万人分）の個人番号にアクセスし、個人番号に紐付く情報を参照します。

【ケース①の図】



＜ケース②　事務システムの中に受給者DBと住民情報DBが存在するケース＞

○　ケース②の図は、次のようなケースを表しています。

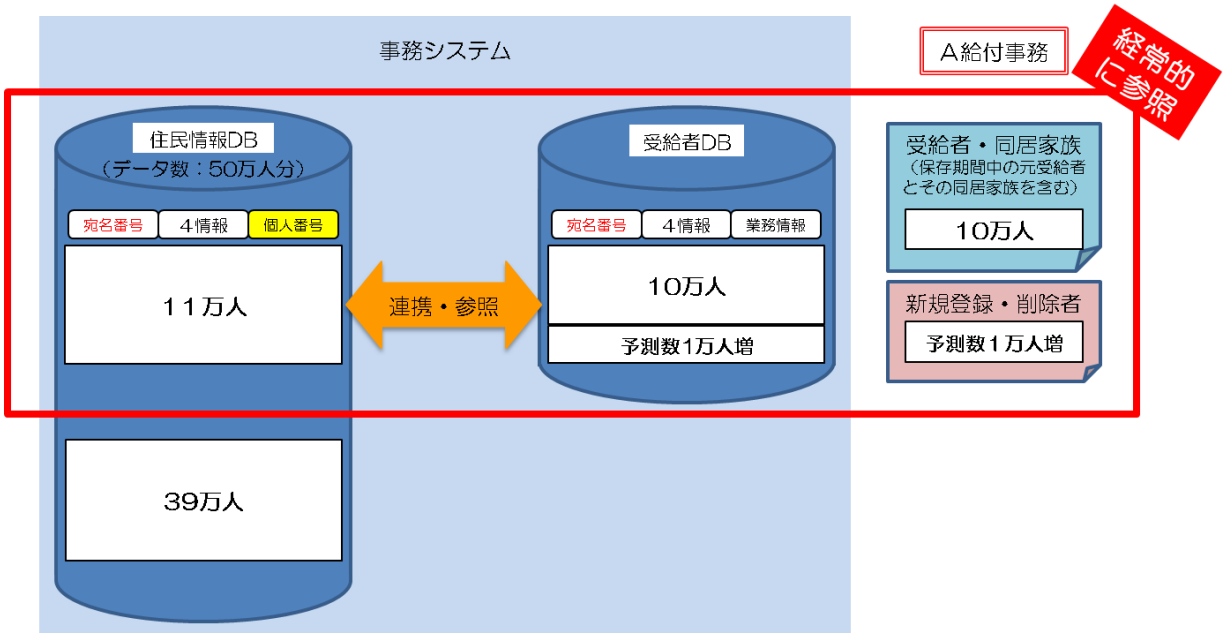
・　A給付事務を処理するために必要な情報として、評価実施機関では、受給者・同居家族の特定個人情報ファイルを取り扱っています（ケース①と同様）。

・　A給付事務においては、その時点における受給者・同居家族のデータとして、既に 10 万人分のデータを事務システムの受給者DBに格納しています（ケース①と同様）。

・　A給付事務における今後の増減分を、新規登録・削除者数を基に合理的に予測すると、約１万人分のデータが増加することが予測され、この増加分についても受給者DBに格納される見込みとなっています（ケース①と同様）。

・　事務システムの中に受給者DBと住民情報DBが存在しますが、A給付事務を処理するに当たっては、受給者DB（11 万人分）の情報だけでなく、宛名番号をキーとして住民情報DB（50 万人分）の個人番号にアクセスし、個人番号に紐付く情報を参照します。

【ケース②の図】



＜ケース③　事務システムの中の住民情報 DB において、受給者の情報を一括管理するケース＞

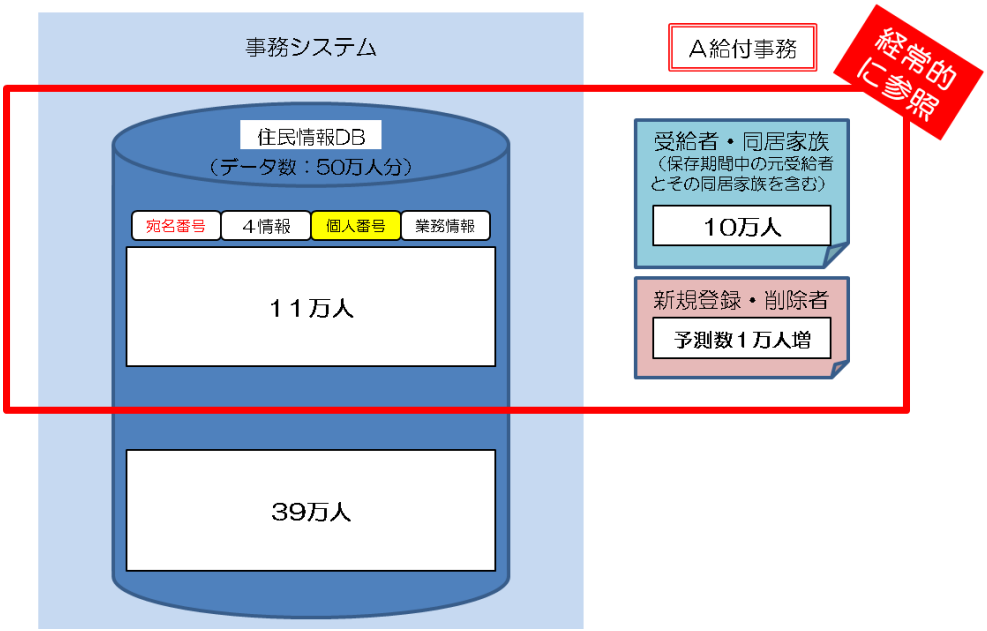
○　ケース③の図は、次のようなケースを表しています。

・　A給付事務を処理するために必要な情報として、評価実施機関では、受給者・同居家族の特定個人情報ファイルを取り扱っています（ケース①と同様）。

・　住民情報DBには、全住民のデータ（50 万人分）が格納されており、A給付事務においては、住民情報DBにおけるその時点の受給者・同居家族のデータ（10 万人分）及び増加分のデータ（１万人分）のみ参照しています。また、業務情報も直接住民情報DBに格納しています。

・　A給付事務においては、今後の増減分を、新規登録・削除者数を基に合理的に予測すると、約１万人分のデータが増加することが予測され、この増加分についても直接住民情報DBを参照することになります。

【ケース③の図】



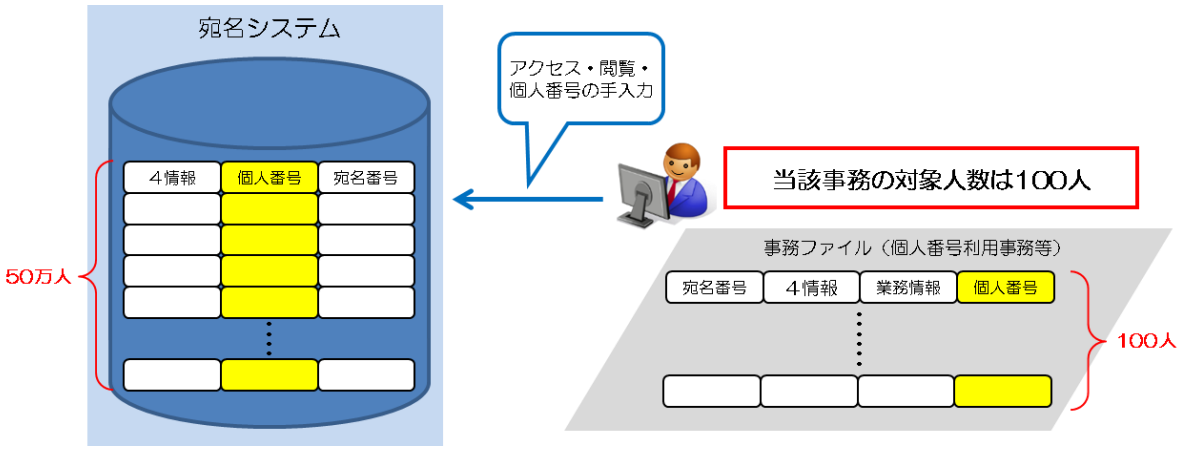
Q第５の２－１．－６

特定個人情報保護評価を実施する事務において、システムではなく、表計算ソフトで特定個人情報ファイルを管理し、既存番号を入手する等のために、宛名システムのような個人番号と既存番号の対象テーブルにアクセスする場合、対象人数はどのようになるのでしょうか。

（Ａ）

○　事務の対象人数は、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となります。したがって、次の図で例示されるとおり、当該事務における対象人数は宛名システムに格納された全ての人の数とはなりません。

【図】



Q第５の２－１．－７

特定個人情報保護評価を実施する事務において、その事務で取り扱う特定個人情報ファイルの一部が、紙ファイルのように、特定個人情報保護評価書に記載する必要のない特定個人情報ファイルの場合、そのファイルに記録される本人の数は対象人数に含まれるのでしょうか。

（Ａ）

○　特定個人情報保護評価書に記載する必要のない紙ファイル等の場合、そのファイルに記録される本人の数は対象人数から除くことができます。

Ｑ第５の２－１．－８
　　死者は対象人数に含まれるのでしょうか。

（Ａ）

○　番号法では、特定個人情報とは個人番号を含む個人情報と定義されており、個人情報は個人情報保護法の定義によります。

　個人情報保護法における個人情報とは、「生存する」個人に関する情報であり、死者に関する情報については、その対象とはなりません。したがって、番号法においても同様の取扱いとなり、死者の情報は、特定個人情報には該当しません。対象人数は特定個人情報ファイルに記録される特定個人情報の本人の数をいいますので、死者の数を対象人数に含める必要はありません。

Ｑ第５の２－１．－９
　　住民基本台帳事務において、いわゆる住民登録外の特定個人情報は対象人数に含まれるのでしょうか。

（Ａ）

○　いわゆる住民登録外の特定個人情報であっても、事務の中で経常的に取り扱うものであれば対象人数に含まれます。

Ｑ第５の２－１．－１０
　　住民基本台帳事務において、転出により除票された人についても特定個人情報を持ち続けることになりますが、それらの人についても対象人数に含まれるのでしょうか。

（Ａ）

○　除票された人についても、事務の中で経常的に取り扱うものであれば対象人数に含まれます。

２．取扱者数について

Ｑ第５の２－２．－１
　しきい値判断の取扱者数とは実際に取り扱っている人の数をいうのでしょうか。

（Ａ）

○　取扱者数とは、実際に取り扱っている人だけでなく、当該事務における特定個人情報ファイルを取り扱うことができる人の数となります。

　また、当該事務を委託している場合、委託先の従業者のうち、当該特定個人情報ファイルを取り扱う者も取扱者数に含みます。

Ｑ第５の２－２．－２
　住民記録システムのように、住民記録の担当部署だけでなく、他の事務を担当する部署の職員も当該システムにアクセスできるような場合、そのような他の部署の職員も取扱者数に含めるのでしょうか。

（Ａ）

○　「特定個人情報を取り扱う職員・委託先の人数」とは、当該事務において特定個人情報ファイルを取り扱うシステム等にアクセスできる人の数となりますので、他の事務を担当する部署の職員であっても、当該特定個人情報ファイルにアクセスできるのであれば、住民記録に関する事務における取扱者数に含まれます。ただし、他の事務の担当する部署の職員が住民記録システムにアクセスできないようにアクセス制御している場合であって、住民記録システムのデータを他のシステムにコピーするなどにより、他の事務において使用する場合は、住民記録システム上で保有される特定個人情報ファイルと当該コピーとは別々の特定個人情報ファイルになりますので、当該コピーにアクセスできる人の数は、住民記録に関する事務における取扱者数には含まれません。

（※）いずれの場合も、「住民記録に関する事務」から「他の事務」への特定個人情報の移転になります。Ｑ第２の９－１及びＱ第２の９－２も併せて参照してください。

Q第５の２－２．－３

特定個人情報保護評価を実施する事務において、その一部が紙ファイルのみを用いて実施するなどの理由により特定個人情報保護評価の実施が義務付けられない事務であり、その義務付けられない事務にのみ従事する者は、取扱者に該当するのでしょうか。

（Ａ）

○　特定個人情報保護評価の実施が義務付けられない事務にのみ従事する者は、取扱者数から除くことができます。

例えば、地方公共団体における児童手当事務において、地方公共団体の職員に対する児童手当事務にのみ従事する職員や、紙ファイルのみを取り扱う職員等は取扱者から除くことができます。

Q第５の２－２．－４

特定個人情報ファイルの取扱いを外部に委託している場合、特定個人情報ファイルの取扱者数はどのように計上すればよいのでしょうか。

（Ａ）

○　委託先で特定個人情報ファイルを取り扱う従業者の数を確認して、計上することとなります。なお、再委託、再々委託などを行っている場合は、再委託以降の従業者の数も含めて、計上してください。

Q第５の２－２．－５

特定個人情報ファイルの取扱者数には、システム保守のために特定個人情報にアクセスする者も含まれるのでしょうか。

（Ａ）

○　システム保守のためにアクセスする者でも、特定個人情報にアクセスできる者については、取扱者数に含めます。

３．重大事故の発生について

Ｑ第５の２－３．－１

しきい値判断における重大事故の発生の対象は、「特定個人情報に関する」事故に限られていますが、そのような限定がかかっていない全項目評価書や重点項目評価書とは対象が異なるということでしょうか。

（Ａ）

○　しきい値判断における重大事故の対象は特定個人情報である一方、全項目評価や重点項目評価における重大事故の対象は個人情報であり、重大事故の対象が異なります。

Ｑ第５の２－３．－２

重大事故の発生について、「評価実施機関における」とありますが、特定個人情報保護評価の対象の事務と全く関わりのない他部署が重大事故を発生させた場合も該当するのでしょうか。

（Ａ）

○　該当します。

重大事故が発生した場合、その事故を起こした事務や部署だけではなく、評価実施機関全体に対する国民・住民の信頼に関わると考えられることに加え、事故が発生した要因の分析及び再発防止策については、評価実施機関全体で取り組む必要があるとの考え方によるものです。

４．その他

Ｑ第５の２－４．－１

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ものについても、任意で重点項目評価又は全項目評価を実施することができるとありますが、どのような場合に実施したらよいのでしょうか。

（Ａ）

○　個人のプライバシー等の権利利益に対して影響を与え得る特定個人情報の漏えい等のリスクに対して対策を講じているということを、国民・住民に対して、より詳細に宣言したい場合など、各評価実施機関がより詳細な特定個人情報保護評価が必要であると判断した場合には、基礎項目評価の対象であっても重点項目評価書様式や全項目評価書様式を用いて評価を実施することが考えられます。

この場合に番号法令に基づき義務付けられるのは基礎項目評価の実施であり、それ以上の措置は任意の取組ですので、必ずしも重点項目評価又は全項目評価で求められている全ての手続等を実施する必要はなく、例えば全項目評価書様式を用いて特定個人情報保護評価書を作成するものの、国民（地方公共団体等にあっては住民等）からの意見聴取は行わないなどの対応も可能です。

３　特定個人情報保護評価書

しきい値判断の結果に従い、評価実施機関は特定個人情報保護評価を実施し、次のとおり、特定個人情報保護評価書を作成し、委員会に提出するものとする。その際、特定個人情報保護評価書の記載事項を補足的に説明する資料を作成している場合は、必要に応じて、当該特定個人情報保護評価書に添付する。

Q第５の３－１

番号法に「基礎項目評価」「重点項目評価」「全項目評価」についての規定がないにもかかわらず、なぜこれらの評価の実施が義務付けられるのでしょうか。

（Ａ）

○　番号法第 28 条において、行政機関の長等は、特定個人情報ファイルを保有しようとするとき及び特定個人情報ファイルについて重要な変更を加えようとするときは、評価書を公示し広く国民の意見を求めること（第１項）、委員会の承認を受けること（第２項）、承認を受けた評価書を公表すること（第４項）とされています。

○　他方、番号法第 28 条第１項においては、規則で定める特定個人情報ファイルを保有しようとする場合には、同条の上記に規定する手続（行政機関等の実施する全項目評価書に係る手続）の対象から除外しています。これを受けて、規則第４条各号においては番号法第 28 条の手続の対象から除外するものを規定しています。

○　規則第４条第１号～第７号には、特定個人情報保護評価の実施が義務付けられない事務（指針第４の４（１）ア～キ）が規定されています。

○　規則第４条第８号及び第９号は、しきい値判断の結果、指針に定めるとおり基礎項目評価、重点項目評価を実施した場合を対象から除外しています。また、規則第４条第 10 号は、地方公共団体等が、指針に定めるとおり全項目評価を実施した場合を対象から除外しています。

・　指針第５の２（１）又は（２）の場合であって基礎項目評価を実施した特定個人情報ファイルを取り扱う事務（第８号）。

・　指針第５の２（３）、（４）又は（５）の場合であって基礎項目評価及び重点項目評価を実施した特定個人情報ファイルを取り扱う事務（第９号）。

・　地方公共団体等が指針第５の２（６）、（７）又は（８）に該当する場合であって基礎項目評価及び全項目評価を実施した特定個人情報ファイルを取り扱う事務（第 10 号）。

（なお、規則においては、第５条に基礎項目評価、第６条に重点項目評価、第７条に地方公共団体等が実施する全項目評価に係る手続が規定されています。）

○　したがって、規則及び指針に基づき基礎項目評価を実施した場合、基礎項目評価及び重点項目評価を実施した場合又は地方公共団体が基礎項目評価及び全項目評価を実施した場合は、番号法第 28 条の手続（行政機関等の全項目評価に係る手続）の対象から除外されることとなります。

（１）基礎項目評価書

評価実施機関は、規則第５条第１項の規定に基づき、特定個人情報保護評価の実施が義務付けられる全ての事務について基礎項目評価書（様式２参照）を作成し、委員会へ提出するものとする。上記２に定めるしきい値判断の結果は、基礎項目評価書に記載するものとする。

（解説）

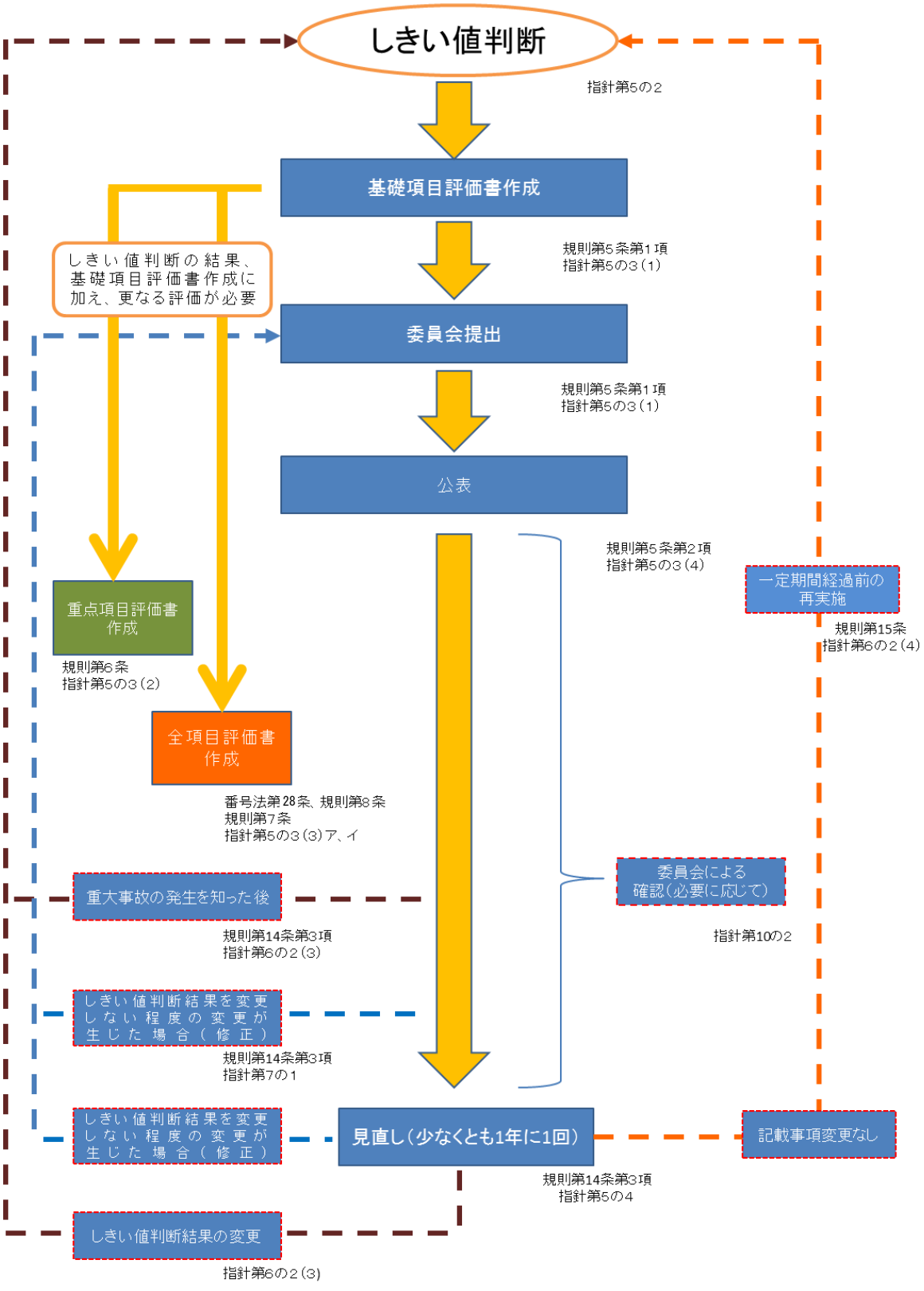
基礎項目評価書は、しきい値判断の結果にかかわらず、特定個人情報保護評価の実施対象となる全ての事務について作成することになります。しきい値判断の結果、基礎項目評価のみと判断された場合はもとより、基礎項目評価及び重点項目評価と判断された場合、基礎項目評価及び全項目評価と判断された場合にも、作成することになります。

特定個人情報ファイルを取り扱う事務の概要、保有しようとする特定個人情報ファイルの名称等の関連情報を記載するとともに、評価実施機関が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認識し、このうち主なリスクを軽減するための措置の実施状況について確認の上、宣言することで、基本的な特定個人情報保護評価を行うものです。

また、しきい値判断項目（事務の対象人数、取扱者数、評価実施機関における特定個人情報に関する重大事故発生の有無）、しきい値判断結果も基礎項目評価書に記載することになります。

基礎項目評価の実施の流れについては、次のフロー図を参照してください。

基礎項目評価実施フロー



（２）重点項目評価書

評価実施機関は、規則第６条第１項の規定に基づき、上記２（３）、（４）又は（５）の場合は、重点項目評価書（様式３参照）を作成し、委員会へ提出するものとする。

（解説）

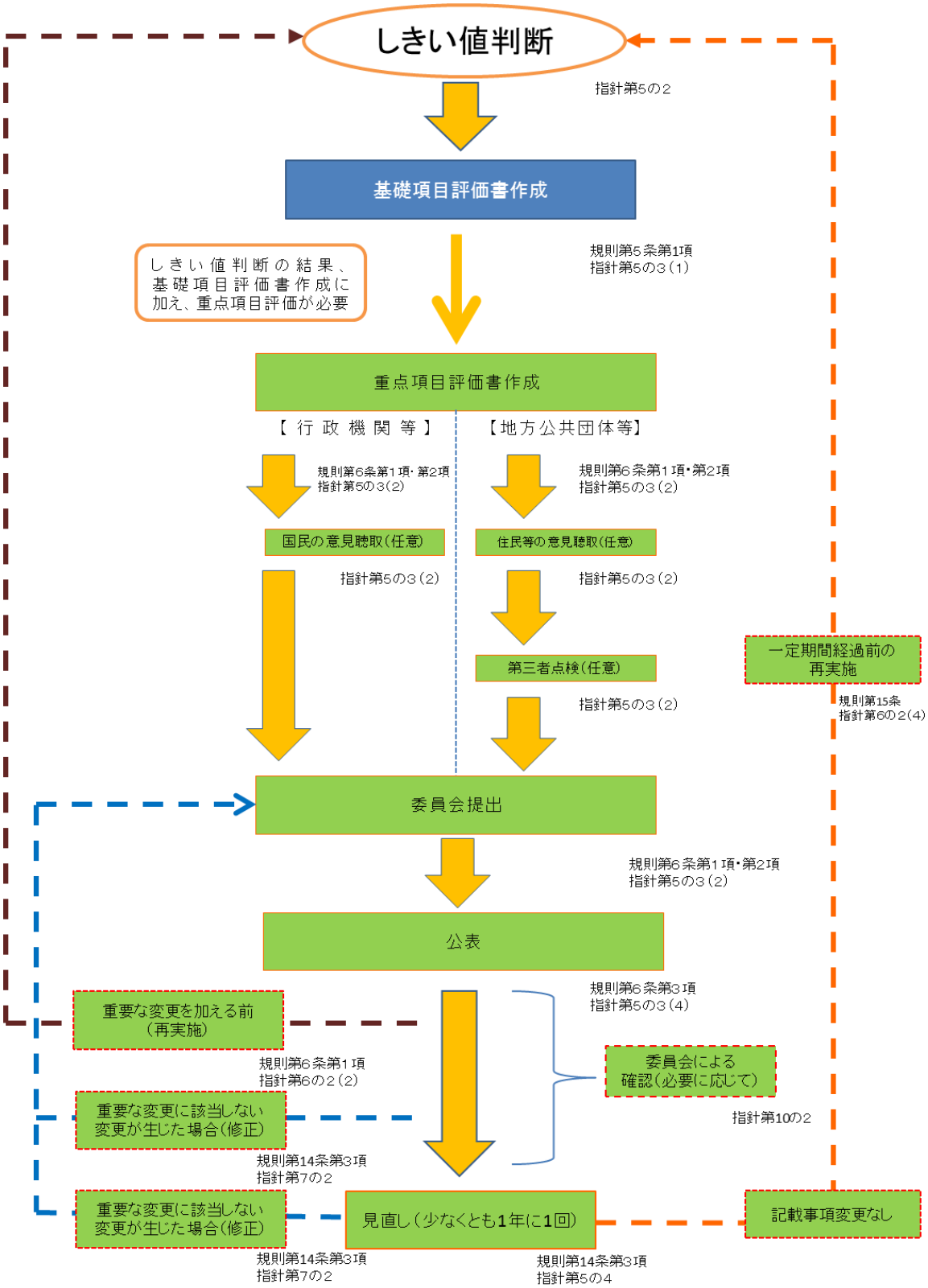
重点項目評価書は、しきい値判断の結果、基礎項目評価及び重点項目評価を実施すべきものと判断された場合に作成することになります。

重点項目評価を実施することで、特定個人情報ファイルを取り扱う事務の特性を明らかにした上で、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を与え得る特定個人情報の漏えいその他の事態を発生させる主なリスクについて分析し、このようなリスクを軽減するためにどのような措置を講ずるのかを決定していくこととなります。

また、公表された重点項目評価書を通じて、国民・住民は、各評価実施機関が、どのような事務においてどのような法令上の根拠により、具体的にどのように特定個人情報ファイルを取り扱っているかを確認することができます。

重点項目評価実施の流れについては、次のフロー図を参照してください。

重点項目評価実施フロー



Ｑ第５の３（２）－１
　　基礎項目評価書と重点項目評価書を委員会にまとめて提出することもできるのでしょうか。

（Ａ）
○　まとめて提出することも可能です。

Ｑ第５の３（２）－２
　　重点項目評価については、国民（地方公共団体等にあっては住民等）からの意見聴取、（地方公共団体等の場合）第三者点検を受ける必要はないということでしょうか。

（Ａ）
○　重点項目評価については、意見聴取、第三者点検が義務付けられるものではありませんが、評価実施機関が任意で意見聴取、第三者点検を行うことを妨げるものではありません。

（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。

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。また、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、これによることができる。

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いないなど、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。

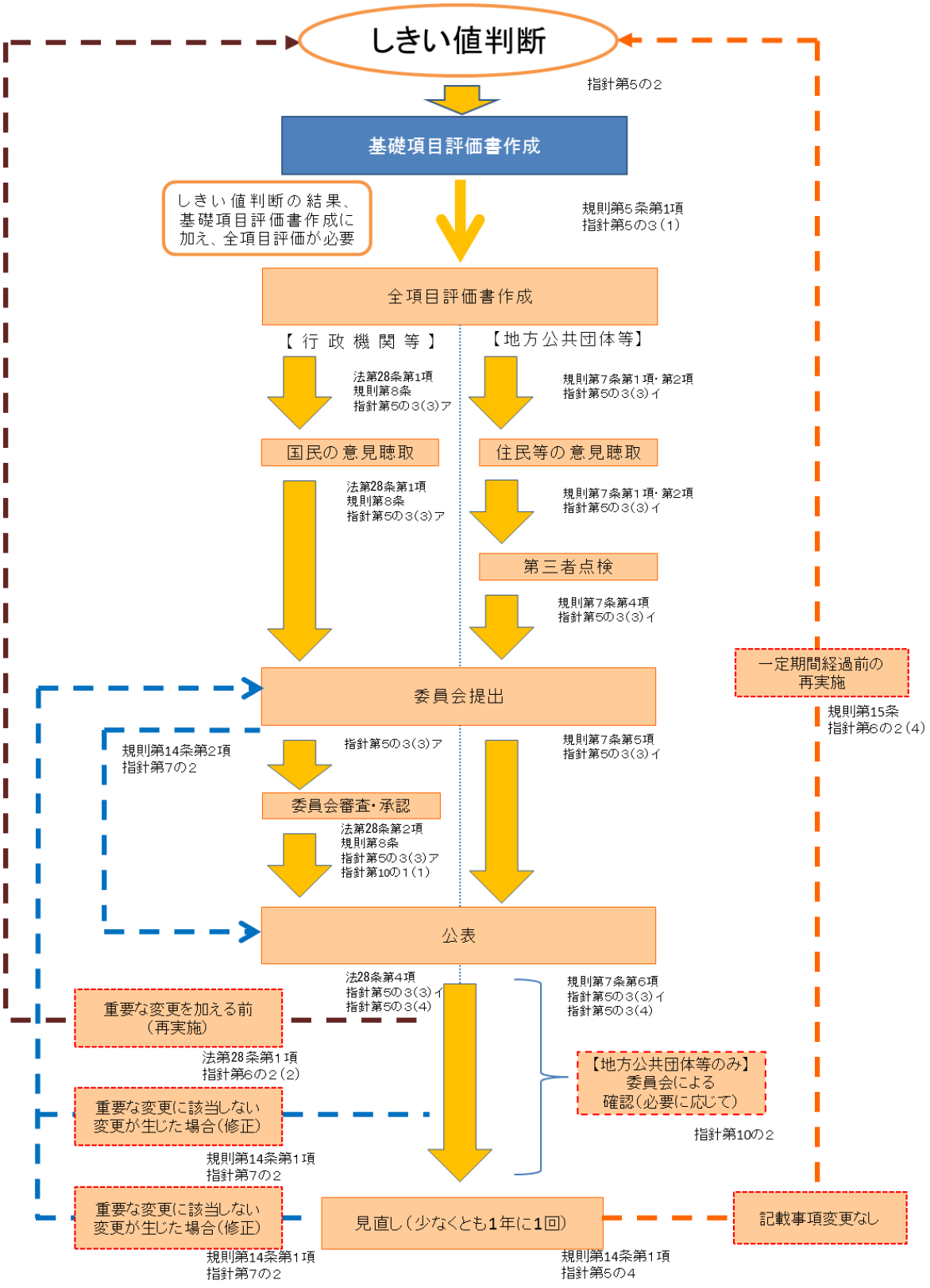
（解説）

全項目評価書は、しきい値判断の結果、基礎項目評価及び全項目評価を実施すべきものと判断された場合に作成することになります。

全項目評価を実施することの意義は基本的に重点項目評価と同じですが、加えて、全項目評価では、個人のプライバシー等の権利利益の保護のための措置に関する詳細な分析・評価を行うとともに、国民（地方公共団体等にあっては住民等）からの意見聴取、委員会の承認（地方公共団体等においては第三者点検）により、評価の適合性・妥当性を客観的に担保する仕組みとなっています。

全項目評価実施の流れについては、次のフロー図を参照してください。

全項目評価実施フロー


しきい値判断
指針第5の2
基礎項目評価書作成
しきい値判断の結果、基礎項目評価書作成に加え、全項目評価が必要
規則第5条第1項
指針第5の3（1）
全項目評価書作成
【行政機関等】
【地方公共団体等】
法第28条第1項
規則第8条
指針第5の3(3)ア
規則第7条第1項・第2項
指針第5の3(3)イ
国民の意見聴取
住民等の意見聴取
法第28条第1項
規則第8条
指針第5の3(3)ア
規則第7条第1項・第2項
指針第5の3(3)イ
第三者点検
規則第7条第4項
指針第5の3(3)イ
一定期間経過前の再実施
規則第15条
指針第6の2（4）
委員会提出
規則第14条第2項
指針第7の2
指針第5の3(3)ア
規則第7条第5項
指針第5の3(3)イ
委員会審査・承認
法第28条第2項
規則第8条
指針第5の3(3)ア
指針第10の1（1）
公表
法28条第4項
指針第5の3(3)イ
指針第5の3(4)
規則第7条第6項
指針第5の3(3)イ
指針第5の3(4)
重要な変更を加える前（再実施）
法第28条第1項
指針第6の2（2）
【地方公共団体等のみ】
委員会による
確認（必要に応じて）
指針第10の2
重要な変更に該当しない変更が生じた場合（修正）
規則第14条第1項
指針第7の2
重要な変更に該当しない変更が生じた場合（修正）
規則第14条第1項
指針第7の2
見直し（少なくとも1年に1回）
規則第14条第1項
指針第5の4
記載事項変更なし

Ｑ第５の３（３）－１

意見聴取の期間を 30 日より短縮することが認められる特段の理由とは、具体的にどのようなものがあるのでしょうか。

（Ａ）

○　例えば、評価実施機関が特定個人情報保護評価を計画的に実施するための合理的努力を行ったにもかかわらず、事務の根拠法の施行日が差し迫っているため、30 日以上の意見聴取期間を設定すると法施行が困難となるなど国民・住民の権利利益に重大な影響を与える場合などが考えられます。

Ｑ第５の３（３）－２

基礎項目評価書と全項目評価書を委員会にまとめて提出することもできるのでしょうか。

（Ａ）

○　まとめて提出することも可能です。

Ｑ第５の３（３）－３

第三者点検ではどのような議論を行うのでしょうか。

（Ａ）

○　特定個人情報保護評価の実施主体は評価実施機関であり、特定個人情報保護評価の内容を決定するのは評価実施機関です。第三者点検は、評価実施機関が特定個人情報保護評価の内容を決定するに当たって外部の有識者の意見を伺うことで、特定個人情報保護評価の適合性・妥当性を客観的に担保することを目的としており、具体的な議論の内容は各評価実施機関の判断に委ねられています。

○　一般的には、規則及び指針で定める第三者点検は、指針第 10 の１（２）に定める審査の観点や「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」（別添５）を参考に、特定個人情報保護評価の適合性・妥当性について点検を行うことを想定しています。評価実施機関はその意見を聞いて、必要に応じて特定個人情報保護評価の内容を見直すことが求められます。

Q第５の３（３）－４

地方公共団体等の実施する全項目評価書については、第三者点検を受けることとなっていますが、どのような方法があるのでしょうか。

（Ａ）

○　第三者点検は、原則として、条例に基づき地方公共団体が設置する個人情報保護審議会や個人情報保護審査会の点検を受ける方法が考えられます。

○　専門性確保の観点から、既存の個人情報保護審議会や個人情報保護審査会のメンバー（の一部）に新たに個人情報の保護に関する学識経験のある者、情報システムの知見を有している者等を追加して点検を受ける方法も考えられます。

○　また、個人情報保護審議会や個人情報保護審査会に専門的知識を有している者がいない場合、専門的知識を有している者の追加が困難な場合、適時に答申を受けることが困難な場合など、個人情報保護審議会や個人情報保護審査会による点検を受けることが困難な場合には、上記知識を有する外部の第三者に点検を受ける方法も考えられます。

○　さらに、他の地方公共団体と連携して行う方法なども考えられます。

Q第５の３（３）－５

第三者点検を行う者のスキルや資格は、どの程度のレベルまで考慮すべきでしょうか。

（Ａ）

○　第三者点検を行う者について何らかの資格を問うものではありませんが、個人情報の保護に関する学識経験を持っている者や、情報システムに知見を有している者等を含むことを想定しています。

Q第５の３（３）－６

第三者点検を諮問機関以外で行う場合、セキュリティの問題があるため、一部を省略した全項目評価書で行うことはできるのでしょうか。

（Ａ）

○　第三者点検について、原則として、非公表部分を含めて第三者点検を行うことを想定しています。

第三者点検を行う者に対して守秘義務を課すなど、情報管理の可能な態勢を構築することが必要です。

Q第５の３（３）－７

広域連合や一部事務組合など特別地方公共団体は、普通地方公共団体と同様、自ら第三者点検を行うこととなるのでしょうか。

（Ａ）

○　特別地方公共団体も普通地方公共団体と同様の扱いとなります。

ただし、構成団体の地方公共団体の個人情報保護審議会や個人情報保護審査会を活用することや、他の地方公共団体と連携して行う方法も考えられます。

Q第５の３（３）－８

第三者点検における点検の基準のようなものはないのでしょうか。

（Ａ）

○　指針第 10 の１（２）で、委員会による全項目評価書の承認に際しての審査の観点として、適合性及び妥当性の２つを示しています。また、「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」（別添５）を参考とすることができます。

Q第５の３（３）－９

第三者点検を諮問機関以外で行う場合、個人情報保護法第 140 条、第 172 条の趣旨に鑑み、罰則は設けないのでしょうか。

（Ａ）

○　個人情報保護法に基づき条例に罰則を設けることが義務付けられるわけではありません。地方公共団体の任意の判断に委ねられます。

（４）特定個人情報保護評価書の公表

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した後速やかに、全項目評価書については委員会の承認を受けた後速やかに、公表するものとする（番号法第 28 条第４項並びに規則第５条第２項、第６条第３項及び第８条）。

地方公共団体等は、特定個人情報保護評価書を委員会に提出した後速やかに、公表するものとする（規則第５条第２項、第６条第３項及び第７条第６項）。

特定個人情報保護評価書及びその添付資料は、原則として、全て公表するものとする。ただし、規則第 13 条の規定に基づき、公表することにセキュリティ上のリスクがあると認められる場合は、評価実施機関は、公表しない予定の部分を含む特定個人情報保護評価書及びその添付資料の全てを委員会に提出した上で、セキュリティ上のリスクがあると認められる部分を公表しないことができる。この場合であっても、期間、回数等の具体的な数値や技術的細目に及ぶ具体的な方法など真にセキュリティ上のリスクのある部分に、公表しない部分を限定するものとする。

犯罪の捜査、租税に関する法律の規定に基づく犯則事件の調査及び公訴の提起又は維持のために保有する特定個人情報ファイルを取り扱う事務に関する特定個人情報保護評価については、評価実施機関は、規則第 13 条の規定に基づき、公表しない予定の部分を含む特定個人情報保護評価書及びその添付資料の全てを委員会に提出した上で、その全部又は一部を公表しないことができる。

（解説）

国民・住民の信頼の確保という特定個人情報保護評価の目的に照らし、特定個人情報保護評価書及びその添付資料は、原則として全て公表することが求められます。

しかし、公表することにより、違法行為を助長する可能性やセキュリティ上のリスクを高める可能性が生じるおそれもあることから、特定個人情報保護評価書の全体又は記載内容の一部を非公表とすることができる場合を設けています。

例えば、次の表に示す特定個人情報保護評価書の各項目の記載は、内容によっては公表することによってセキュリティ上のリスクを高める場合があると考えられます。ただし、特定個人情報ファイルの取扱いへの国民・住民の信頼の確保という特定個人情報保護評価の目的に照らし、非公表とする場合でも、システム操作ログの保存期間、システム管理者による分析・検査の頻度等の具体的な数値、特定個人情報の保管場所の物理的位置、不正アクセス対策等に関する技術的細目に及ぶ具体的な方法など、真にセキュリティ上のリスクのある部分に限定する必要があります。

【非公表とできる項目の例】

特定個人情報保護評価書	項　　目
重点項目評価書	・Ⅰ２③　他のシステムとの接続 ・Ⅱ６　　保管場所 ・Ⅲ３　　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
全項目評価書	・Ⅰ２③　他のシステムとの接続 ・Ⅱ６①　保管場所 ・Ⅲ２　　リスク２：不適切な方法で入手が行われるリスク ・Ⅲ２　　リスク４：入手の際に特定個人情報が漏えい・紛失するリスク ・Ⅲ３　　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 ・Ⅲ３　　リスク４：特定個人情報ファイルが不正に複製されるリスク ・Ⅲ５　　リスク３：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 ・Ⅲ７　　リスク１⑤　物理的対策 ・Ⅲ７　　リスク１⑥　技術的対策

特定個人情報保護評価書の全体又は記載内容の一部を非公表とする場合であっても、委員会へは記載内容の全てを明らかにした特定個人情報保護評価書及びその添付資料の全体を提出しなければなりません。これは、これらの特定個人情報保護評価書も委員会による審査・承認（行政機関等が提出する全項目評価書）又は精査・確認（その他の特定個人情報保護評価書）の対象であり、委員会が特定個人情報保護評価書の内容について適合性・妥当性を判断するために、一般には非公表とする記載内容についても把握する必要があるからです。

また、評価実施機関は委員会に対して、全体を非公表とする旨又は非公表とする部分を明示しなければなりません。指針において「審査の観点」として示すとおり、非公表とする部分が適切な範囲かどうかを委員会が審査又は精査を行うためです。

Ｑ第５の３（４）－１

セキュリティ上のリスクを高めるおそれから非公表とすることができる特定個人情報保護評価書の項目は、「解説」の表に掲げるものに限られるのでしょうか。

（Ａ）

○　「解説」の表は、記載内容によってはセキュリティ上のリスクを高める場合がある特定個人情報保護評価書の項目を例示したものであり、これらに限られるものではありません。他の項目でもセキュリティ上のリスクを高めるおそれがある記載内容であれば、非公表とすることができます。

ただし、特定個人情報ファイルの取扱いへの国民・住民の信頼の確保という特定個人情報保護評価の目的に鑑みると、むやみに非公表とすることは望ましくなく、真にセキュリティ上のリスクのある部分に限定しなければなりません。

また、指針において「審査の観点」として示すように、非公表部分が適切な範囲であるかどうかは委員会による審査又は精査の対象となります。

４　特定個人情報保護評価書の見直し

評価実施機関は、少なくとも１年に１回、公表した特定個人情報保護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よう努めるものとする（規則第 14 条）。

（解説）

①特定個人情報ファイルの取扱いについて重要な変更を加えようとする場合、②対象人数若しくは取扱者数の増加又は特定個人情報に関する重大事故の発生によりしきい値判断の結果が変わる場合には、特定個人情報保護評価の再実施が義務付けられています。

しかし、担当する部署の名称変更、しきい値判断に変更をもたらさない対象人数の増減など、特定個人情報保護評価の再実施が義務付けられない程度の比較的軽微な変更・変化であっても、国民・住民からの信頼を確保するという観点から、公表している特定個人情報保護評価書の記載内容が実態と齟齬がないよう見直しておく必要があります。

評価実施機関には、公表している特定個人情報保護評価書の記載内容が実態に合致しているかを常に意識し、必要であれば修正し、公表することが期待されますが、少なくとも１年に１度は見直しを行い、記載内容の変更が必要か否かを検討するよう努めることが求められています。

Ｑ第５の４－１

特定個人情報保護評価書の見直しでは、どのようなことをすればよいのでしょうか。

（Ａ）

○　既に公表している特定個人情報保護評価書の記載内容が実態と異なっていないかを確認することになります。

Ｑ第５の４－２

特定個人情報保護評価書を見直した結果、記載内容の変更が必要となった場合は、どのように処理すればよいのでしょうか。

（Ａ）

○　変更が必要となる記載内容によってその後の処理は異なります。

○　しきい値判断項目である対象人数又は取扱者数の増加に伴いしきい値判断結果が変わる場合は、特定個人情報保護評価の再実施が必要になります。

したがって、特定個人情報保護評価計画管理書の更新から始まる特定個人情報保護評価の実施手続の全てのプロセスを実施することとなります。

○　それ以外の変更の場合は、特定個人情報保護評価書の修正が必要になります。

したがって、特定個人情報保護評価書の変更箇所を修正し、委員会に提出した上で公表することとなります。

○　なお、「重要な変更」については、そのような変更を加えようとする前に特定個人情報保護評価を実施することが必要であり、事後的な処理を行うことになる特定個人情報保護評価書の見直しにおいて、「重要な変更」が見つかることは想定されていません。

Q第５の４－３

１年ごとの見直しの際に、特定個人情報保護評価の実施手続の全てのプロセスを実施している場合でも、５年経過前の再実施を行う必要があるのでしょうか。

（Ａ）

○　本来、１年ごとの見直しは、既に公表している特定個人情報保護評価書の記載内容が実態と異なっていないかを確認する事後的な処理を行うことを想定したものですが、１年ごとの見直しにおいて、特定個人情報保護評価の実施手続の全てのプロセスを実施している場合（全項目評価の場合は、国民・住民等からの意見聴取や委員会の審査・承認（地方公共団体等においては第三者点検）も全て含む。）には、特定個人情報保護評価を再実施したものとして、委員会に提出した上で、公表することができます。この場合の公表日は、第６の２（４）の解説に記載された一定期間経過前の再実施における「５年を経過する前」の起点となる直近の再実施の際の公表日とすることができます。

５　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

評価実施機関は、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は、規則第 16 条の規定に基づき、遅滞なく委員会に通知するものとする。評価実施機関は、事務の実施をやめるなどした日から少なくとも３年間、その事務の実施をやめたこと等を記載するなど所要の修正を行った上で、特定個人情報保護評価書を公表しておくものとする。

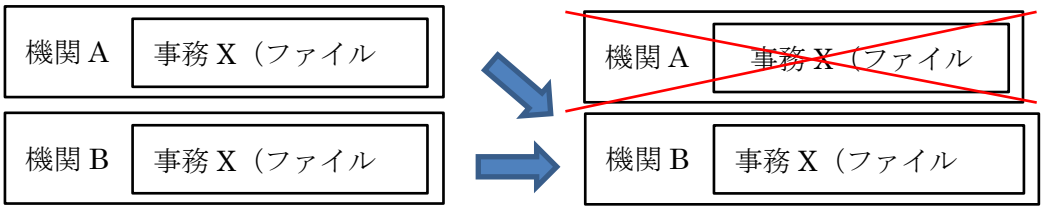
（解説）

特定個人情報ファイルを保有しようとするときは、保有しようとする事務において特定個人情報保護評価を実施する必要がありますが、その特定個人情報ファイルを取り扱う事務をやめたとき等、次の場合に該当するときは、委員会への通知及び修正した特定個人情報保護評価書の公表が必要になります。なお、事務の実施自体は継続するが、特定個人情報ファイルを取り扱うことをやめた場合（個人番号の利用をやめた場合）も、本通知が必要となります。

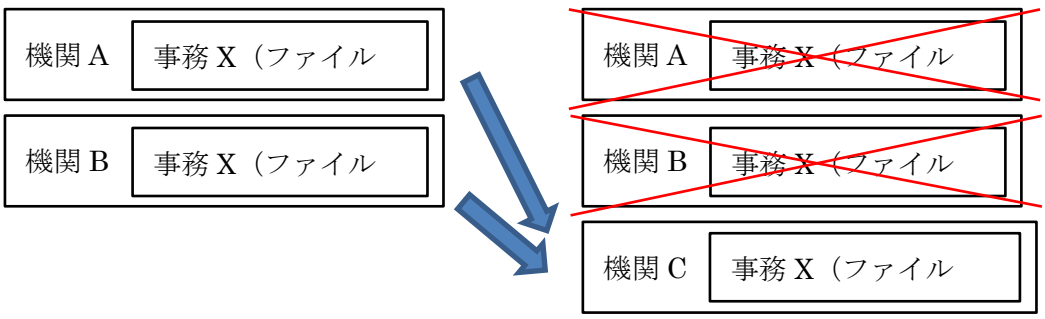
１．事務の実施をやめたとき等の通知が必要な場合

（１）　事務の実施をやめたとき

（２）　評価実施機関が廃止になり、別の評価実施機関が当該事務を引き継ぐとき



（３）　評価実施機関が廃止になり、別の機関と統合した新しい機関が当該事務を引き継ぐとき



２．通知方法・時期

（１）事務の実施をやめたとき

評価実施機関は、事務の終了後に、特定個人情報保護評価書の記載要領に従い、特定個人情報保護評価書に事務の終了と明記し、委員会に提出し公表する必要があります。公表した特定個人情報保護評価書は、事務の終了後３年間公表することとします。

（２）評価実施機関が廃止になり、別の評価実施機関が当該事務を引き継ぐとき

地方公共団体における編入合併のように、評価実施機関が廃止になり、別の評価実施機関が当該事務を引き継ぎ、特定個人情報ファイルも合わせて保有するような場合は、引き継いだ評価実施機関が評価の再実施又は特定個人情報保護評価書の修正を行います。評価の再実施か特定個人情報保護評価書の修正かは、指針の第６の２（２）の重要な変更に該当するか、第７の重要な変更に当たらない変更に該当するかで判断することになります。

評価の再実施を行う場合は、評価実施機関が廃止になり、別の評価実施機関が当該事務を引き継ぐ前までに、特定個人情報保護評価書の修正を行う場合は、引き継いだ後速やかに、それぞれ行う必要があります。

なお、廃止になった評価実施機関の特定個人情報保護評価書は、事務を引き継いだ評価実施機関（機関Ｂ）が、廃止になってから３年間は継続して公表することとなります。

（３）評価実施機関が廃止になり、別の機関と統合した新しい機関が当該事務を引き継ぐとき

地方公共団体における新設合併のように、評価実施機関が廃止になり、新しい機関が当該事務を引き継ぐ場合は、新しい機関が新たに特定個人情報保護評価を実施する必要があります。

新しい機関は、新たに特定個人情報ファイルを保有することになるので、指針に定めるところにより、システムのプログラミングの開始前の適切な時期に実施することが望まれますが、新たな機関として特定個人情報保護評価を実施することが困難な場合は、事前に委員会と協議してください。

なお、廃止になった評価実施機関の特定個人情報保護評価書は、上記（２）と同様、事務を引き継いだ評価実施機関（機関Ｃ）が、廃止になってから３年間は継続して公表することとなります。

第６　特定個人情報保護評価の実施時期

１　新規保有時

行政機関の長等は、特定個人情報ファイルを新規に保有しようとする場合、原則として、当該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するものとする。ただし、規則第９条第２項の規定に基づき、災害が発生したときの対応等、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は、特定個人情報ファイルの保有後可及的速やかに特定個人情報保護評価を実施するものとする。

（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

規則第９条第１項の規定に基づき、プログラミング開始前の適切な時期に特定個人情報保護評価を実施するものとする。

（２）その他の電子ファイルを保有しようとする場合の実施時期

事務処理の検討段階で特定個人情報保護評価を実施するものとする。

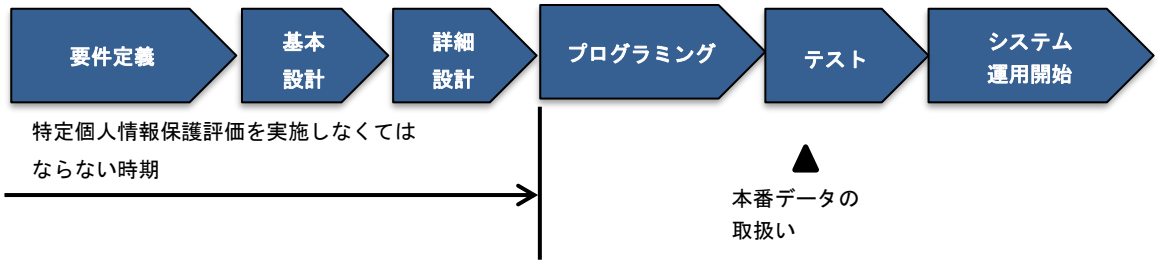
（解説）

特定個人情報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十分想定されることから、対応に要する時間を考慮して、特定個人情報保護評価は、特定個人情報ファイルを保有する直前ではなく、十分な時間的余裕をもって実施する必要があります。

特定個人情報保護評価の実施時期は、次の図表を参照してください。

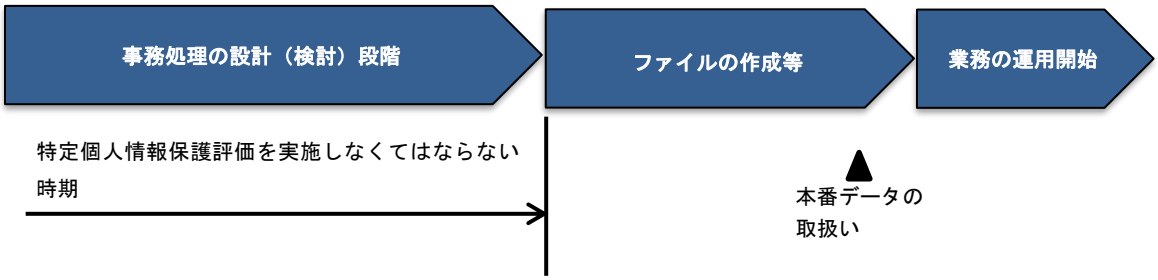
１．システム用ファイルに係る実施時期

・　遅くともプログラミング開始前の適切な時期に特定個人情報保護評価を実施する必要があります。



２．その他の電子ファイルを保有しようとする場合の実施時期

・　事務処理の検討段階で特定個人情報保護評価を実施する必要があります。



Ｑ第６の１－１

番号法第 28 条第１項では「特定個人情報ファイルを保有する前に…（評価書）を公示し」とあり、規則第９条第１項では、法第 28 条第１項の規定による評価書の公示・基礎項目評価書の提出・重点項目評価書の提出・規則第７条第１項の規定による公示を行う時期が規定されていますが、これらの規定により定められる時期までに、「公示」や「提出」のみを行えばよいということでしょうか。

（Ａ）

○　番号法第 28 条においては、特定個人情報保護評価の手続として、評価書の公示、委員会による評価書の承認、評価書の公表という一連の手続が定められています。同条第１項では「特定個人情報ファイルを保有する前に…（評価書）を公示し」と規定されていますが、これは、特定個人情報ファイルを保有する前に評価書の公示さえ行えばよいという意味ではなく、特定個人情報ファイルを保有する前に評価書の公示、委員会による評価書の承認、評価書の公表という一連の手続を行わなければならないということを意味しています。

○　規則第９条第１項においては公示の時期が規定されていますが、番号法と同様に解し、①評価書に係る特定個人情報ファイルが電子情報処理組織により取り扱われるものであるときは、特定個人情報ファイルを取り扱うために使用する電子情報処理組織を構築する前に、評価書の公示、委員会による評価書の承認、評価書の公表という一連の手続を行わなければならない、②評価書に係る特定個人情報ファイルが電子情報処理組織により取り扱われるものでないときは、特定個人情報ファイルを取り扱う事務を実施する体制その他事務の実施に当たり必要な事項の検討と併せて、評価書の公示、委員会による評価書の承認、評価書の公表という一連の手続を行わなければならない、ということを意味しています。基礎項目評価書の提出・重点項目評価書の提出・規則第７条第１項の規定による公示についても、同様に解します。

Q第６の１－２

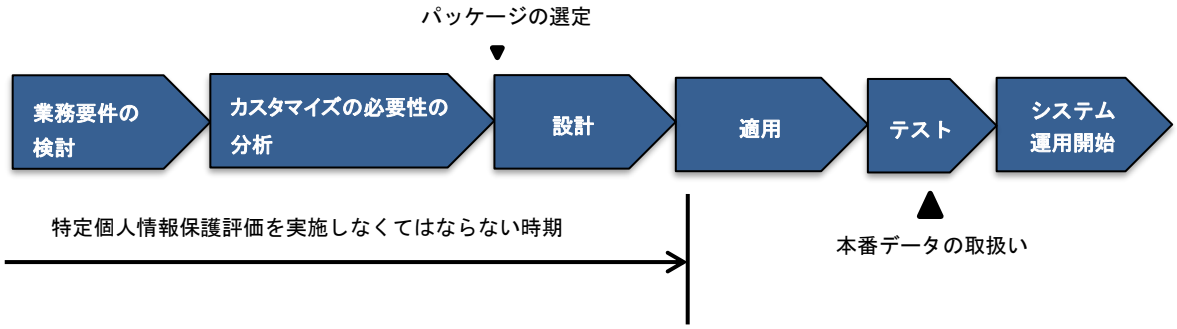
特定個人情報ファイルを取り扱う事務において、パッケージシステムをノンカスタマイズで適用する場合、特定個人情報保護評価はいつまでに実施すればよいのでしょうか。

（Ａ）

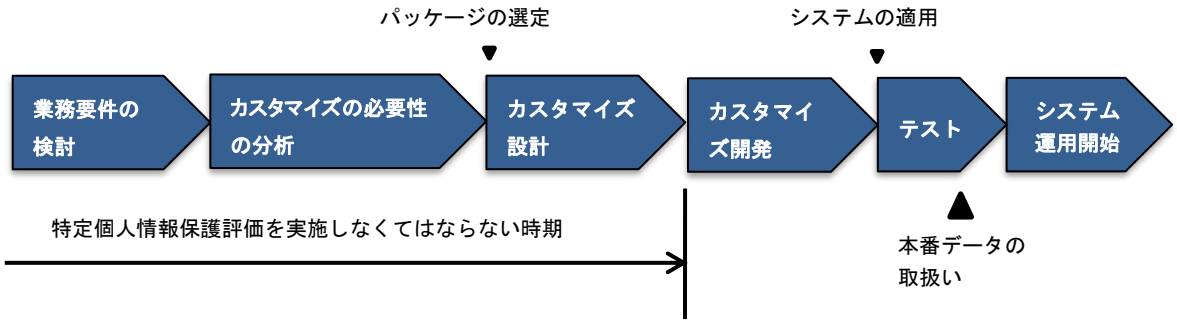
○　特定個人情報ファイルを取り扱う事務において、パッケージシステムを適用する場合、業務要件の検討やカスタマイズの必要性の分析を行う時期がいわゆる要件定義の時期に当たります。

検討の結果、カスタマイズは行わず、そのままパッケージシステムを適用することにした場合、その後、パラメータ設計や環境設計、移行設計等の「設計」を行い、システムを稼働させるサーバ等へパラメータ設定等の「適用」が行われます。

この「適用」によりサーバ等に直接的に変更を加えることとなりますので、プログラミングに相当するものとして、システムへの適用を実施する前までに特定個人情報保護評価を実施することになります。次の図表を参照してください。



○　なお、パッケージシステムをカスタマイズする場合は、次の図表のとおり、カスタマイズ開発を実施するまでに特定個人情報保護評価を実施する必要があります。



Q第６の１－３

特定個人情報保護評価については、「プログラミング開始前の適切な時期」に行うこととなっていますが、評価実施機関はどのような点に留意すればよいのでしょうか。

（Ａ）

○　従来、特定個人情報保護評価をシステムの要件定義の終了までに実施することを原則としていましたが、その趣旨は、特定個人情報保護評価の結果によっては、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十分想定されることから、対応に要する時間も考慮し、コスト増・スケジュール遅延等を防ぐために、十分な時間的余裕をもって実施するというものです。

○　しかしながら、特定個人情報保護評価は、システムの具体的な運用面も含んだリスク対策の評価を求めており、当該運用面については、システムの設計中においても関係機関等との調整を要し、要件定義終了までに評価を実施することが困難となることもあるため、特定個人情報保護評価の実施時期を、プログラミング開始前の適切な時期に変更することとしたものです。

○　この場合であっても、要件定義の重要性は変わらないことから、各評価実施機関は、特定個人情報保護評価を見据え、大規模な仕様変更等が生じないような明確な要件定義を行う必要がありますので、十分留意してください。

Q第６の１－４

個人番号を利用するためのシステム改修の後に情報連携のためのシステム改修を行い、それぞれシステム改修の時期が異なる場合、特定個人情報保護評価の実施はどのようにすればよいのでしょうか。

（Ａ）

○　特定個人情報保護評価は特定個人情報ファイルを保有しようとする事務に対して実施します。当該事務で個人番号を利用するためのシステム改修と情報連携のためのシステム改修を行う場合、当該事務に対する特定個人情報保護評価は双方のシステム改修を踏まえる必要があります。

○　特定個人情報保護評価の実施時期は、当該事務で最初に特定個人情報ファイルを保有しようとする時期である、個人番号を利用するためのシステム改修におけるプログラミング開始前となります。

その際に、情報連携のためのシステム改修の内容を踏まえた特定個人情報保護評価を実施できれば、まとめて行うことが可能ですが、その時点において、情報連携のためのシステム改修の概要が決定していない場合や、その後変更になった

場合には、情報連携のためのシステム改修の内容が判明した時点で、個人番号を利用するためのシステム改修の前に実施した特定個人情報保護評価書について、修正箇所がある場合は修正、重要な変更に該当する場合には評価を再実施する必要があります。

Ｑ第６の１－５
　被災者台帳の作成等災害対応等に係る事務について、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。

（Ａ）

○　災害が発生したときの対応等、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は、指針において、特定個人情報ファイルの保有後可及的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。例えば、災害が発生したため、特定個人情報ファイルである被災者台帳を作成したとき（手作業処理用ファイルのみを取り扱う場合を除く。）は、作成後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なりますが、具体的な実施時期については、個別に委員会事務局に御相談ください。

○　一方、例えば、被災者台帳について、特定個人情報ファイルを保有することとなるのは災害発生後であるものの、特定個人情報ファイルを保有することを想定した被災者台帳を作成するためのシステムを、災害発生前に開発する場合には、原則どおり、当該システムのプログラミング開始前の適切な時期に特定個人情報保護評価を実施する必要があると考えられます。

○　なお、この場合の対象人数については、システム設計上の想定人数を基に判断しても構いません。実際に特定個人情報ファイルを保有したときに、想定人数との間に相違があった場合には、評価書の修正又は評価の再実施を行ってください。

Ｑ第６の１－６

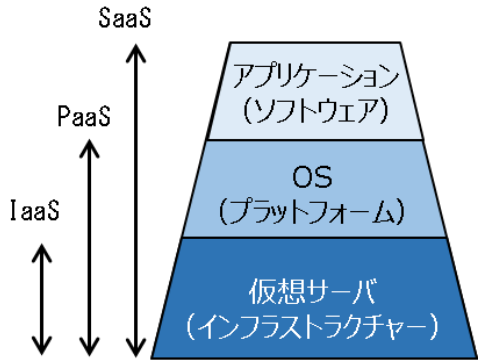
特定個人情報ファイルを取り扱うシステムを改修し、クラウドサービスを利用します。特定個人情報保護評価の実施時期はどのように考えればよいのでしょうか。

（Ａ）

○　クラウドサービスには、クラウドサービス事業者（※１）とクラウドサービス利用者の役割分担により、IaaS（※２）、PaaS（※３）、SaaS（※４）の３種に分類されます。

システムの階層を３層で捉えた場合、１段目までクラウドサービス事業者に任せるのが IaaS、２段目まで任せるのが PaaS、３段目まで任せるのが SaaS です。クラウドサービスの種類によって、クラウドサービス事業者の構築・管理の範囲が異なります。

［システムの階層とクラウドサービス事業者に任せる範囲］



○　クラウドサービス利用者側でアプリケーション等を構築・管理できる IaaS のクラウドサービスへの移行する場合には、例えば、クラウド環境への移行にあたり、クラウドサービス利用者が既存システムのアプリケーション等について、特定個人情報の取扱いに関する機能の改修を行い移行する場合と改修を行わず移行する場合が考えられます。

○　特定個人情報の取扱いに関する機能の改修を行い移行する場合は、システム開発を行いますので、「指針第６の２（２）ア　システム開発を伴う場合の実施時期」に従い、プログラミング開始前の適切な時期に特定個人情報保護評価を行う必要があります。

○　特定個人情報の取扱いに関する機能の改修を行わず移行する場合は、「指針第６の２（２）イ　システム開発を伴わない又はその他の電子ファイルを保有する場合の実施時期」に従って適切な時期に特定個人情報保護評価を行う必要があります。

（※１）クラウドサービス事業者とは、クラウドサービスを提供する事業者又はクラウドサービスを用いて情報システムを開発・運用する事業者をいいます。

（※２）IaaS（Infrastructure as a Service）とは、利用者に、CPU 機能、ストレージ、ネットワークその他の基礎的な情報システムの構築に係るリソースが提供されるものをいいます。利用者は、そのリソース上に OS や任意機能（情報セキュリティ機能を含む。）を構築することが可能です。

（※３）PaaS（Platform as a Service）とは、IaaS のサービスに加えて、OS、基本的機能、開発環境や運用管理環境等もサービスとして提供されるものをいいます。利用者は、基本機能等を組み合わせることにより情報システムを構築することが可能です。

（※４）SaaS（Software as a Service）とは、利用者に特定の業務系のアプリケーション、コミュニケーション等の機能がサービスとして提供されるものをいいます。具体的には、政府外においては、安否確認、ストレスチェック等の業務系のサービス、メールサービスやファイル保管等のコミュニケーション系のサービス等があります。政府内においては、府省共通システムによって提供される諸機能や、政府共通プラットフォーム上で提供されるコミュニケーション系のサービス・業務系のサービスが該当します。

Q第６の１－７

個人番号を利用するための既存システムを改修します。改修時の開発手法として、アジャイル型開発を採用します。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。

（Ａ）

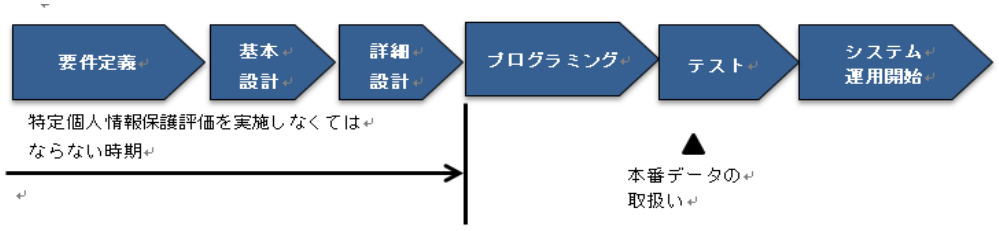
○　特定個人情報保護評価は事前対応による個人のプライバシー等の権利利益の侵害の未然防止及び国民・住民の信頼の確保を目的とすることから、特定個人情報ファイルを新規に保有しようとする場合は、規則第９条第１項の規定に基づき、プログラミング開始前の適切な時期に特定個人情報保護評価を実施するものとしています。

○　また、特定個人情報ファイルの新規保有後においても、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、当該変更を加える前に特定個人情報保護評価を再実施するものとしており、システム開発を伴う際は、新規保有時と同様の時期に特定個人情報保護評価を実施するものとしています。（指針第６の２（２）ア　システム開発を伴う場合の実施時期）

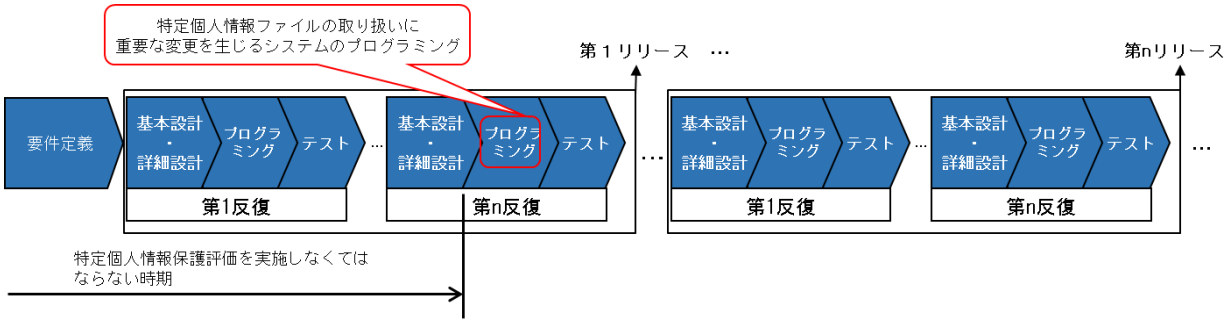
○　アジャイル型開発とは、設計、プログラミング（開発）、テストをイテレーション（反復）と呼ばれる短い期間に分けて進め情報システムを完成させていく開発手法です。

○　アジャイル型開発では、システムが完成する前に、複数回のプログラミング（開発）の工程が発生することになりますが、この場合は、特定個人情報ファイルの取扱いに関して重要な変更が生じるシステムの開発前に特定個人情報保護評価を行うことが必要と考えられます。

［ウォーターフォール型開発（※）の例（再掲（第６の１の解説　１．の図表））］



［アジャイル型開発の例］



（※）ウォーターフォール型開発とは、工程を時系列に進め、原則として前工程の完了後に次工程を開始する情報システム構築作業の進め方をいいます。設計・開発に着手する時点で、要件がしっかり定まっており、設計・開発の途中で要件の変更が少ないと見込まれる場合に用いられます。

２　新規保有時以外

（１）基本的な考え方

評価実施機関は、過去に特定個人情報保護評価を実施した特定個人情報ファイルを取り扱う事務について、下記（２）又は（３）の場合には、特定個人情報保護評価を再実施するものとし、下記（４）の場合には、再実施するよう努めるものとする。

再実施に当たっては、委員会が定める特定個人情報保護評価書様式中の変更箇所欄に変更項目等を記載するものとする。下記（２）から（４）まで以外の場合に特定個人情報保護評価を任意に再実施することを妨げるものではない。

（解説）

特定個人情報保護評価は、特定個人情報ファイルを新規に保有しようとするときに一度実施して終了するものではありません。

特定個人情報保護評価を実施（又は再実施）した後、当該特定個人情報ファイルの取扱い、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又はリスクを軽減するための措置について変更・変化が生じることがあります。評価実施機関が当該特定個人情報ファイルの取扱いを能動的に変更することもあれば、人口構成の変化など当該特定個人情報ファイルの取扱いを取り巻く状況が変化することも考えられます。

このような変更・変化が生じると、公表している特定個人情報保護評価書の記載内容が実態と合わなくなってきます。そのような記載内容と実態の齟齬を放置することは、特定個人情報ファイルの取扱いについての透明性を高め、国民・住民の信頼を確保するという特定個人情報保護評価の目的に反する結果となります。

そこで、特定個人情報保護評価を実施（又は再実施）した事務について、一定の場合には、特定個人情報保護評価の再実施を求めることとされています。具体的には、特定個人情報ファイルの取扱いについて①「重要な変更」を加えようとする場合、②対象人数若しくは取扱者数の増加又は特定個人情報に関する重大事故の発生により「しきい値判断の結果の変更」が生じた場合には、特定個人情報保護評価を再実施することになっています。また、こうした状況に至らずとも、社会情勢の変化や技術進歩を勘案し、直近の特定個人情報保護評価書を公表（ただし、修正に伴う公表を除く。）してから５年を経過する前に、再実施するよう努めることが求められています。

なお、特定個人情報保護評価を再実施することが求められない程度の比較的軽微な変更・変化の場合には、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。

Q第６の２（１）－１

特定個人情報保護評価の再実施とは、具体的には何を再実施するのでしょうか。

（Ａ）

○　特定個人情報保護評価の再実施においては、特定個人情報保護評価計画管理書の更新から始まる特定個人情報保護評価の実施手続の全てのプロセスを実施することになります。

改めて行うしきい値判断の結果により、特定個人情報保護評価書の作成、委員会への提出、公表が必要となります。全項目評価を再実施する場合には、国民・住民等からの意見聴取や委員会の審査・承認（地方公共団体等においては第三者点検）も必要です。

（２）重要な変更

特定個人情報ファイルに対する重要な変更（規則第 11 条に規定する特定個人情報の漏えいその他の事態の発生の危険性及び影響が大きい変更として指針で定めるもの）とは、重点項目評価書又は全項目評価書の記載項目のうちこの指針の別表に定めるものについての変更とする。ただし、個人のプライバシー等の権利利益に影響を与え得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又は当該リスクを明らかに軽減させる変更は、重要な変更には当たらないものとする。

この指針の別表に定めるとおり、重大事故の発生それ自体が直ちに重要な変更に当たるものではないが、特定個人情報に関する重大事故の発生に伴い評価実施機関がリスク対策等を見直すことが想定され、この場合は、重要な変更に該当する。

評価実施機関は、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、当該変更を加える前に、特定個人情報保護評価を再実施するものとする。ただし、災害が発生したときの対応等、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の取扱いを変更せざるを得ない場合は、特定個人情報ファイルの取扱いの変更後可及的速やかに特定個人情報保護評価を再実施するものとする。

ア　システムの開発を伴う場合の実施時期

上記１（１）に準ずるものとする。

イ　システムの開発を伴わない又はその他の電子ファイルを保有する場合の実施時期

事務処理の変更の検討段階で特定個人情報保護評価を実施するものとする。

（解説）

特定個人情報保護評価を実施（又は再実施）した後、当該特定個人情報ファイルの取扱い等について変更が生じることがあります。

例えば、特定個人情報保護評価の対象となった制度・事務の見直し、使用するシステムの更新等により、評価実施機関が当該特定個人情報ファイルの取扱いを変更することが想定されます。また、社会情勢の変化や技術進歩により、直近の特定個人情報保護評価を実施した時点で採用していたリスク対策が陳腐化し、再検討が必要となることも考えられます。

事前に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」とは、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と考

えられるものです。具体的には、特定個人情報ファイルの対象となる本人の範囲、特定個人情報の使用目的、特定個人情報の突合、リスク対策（重大事故の発生を除く。）など、指針の別表に掲げられている、重点項目評価書と全項目評価書の中の幾つかの項目の記載内容に限られます。

これら以外の特定個人情報保護評価書の記載項目への変更の場合は、既に公表している特定個人情報保護評価書を修正し、公表することとなります。

また、重要な変更の対象である項目の記載内容であっても、個人のプライバシー等の権利利益に影響を与え得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又は当該リスクを明らかに軽減させる変更については、特定個人情報保護評価を再実施する必要性が高くないことから、重要な変更には当たらないと整理しています。この場合も、既に公表している特定個人情報保護評価書を修正し、公表することとなります。

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。

○　②に該当する具体例は以下のとおりです。

＜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＞

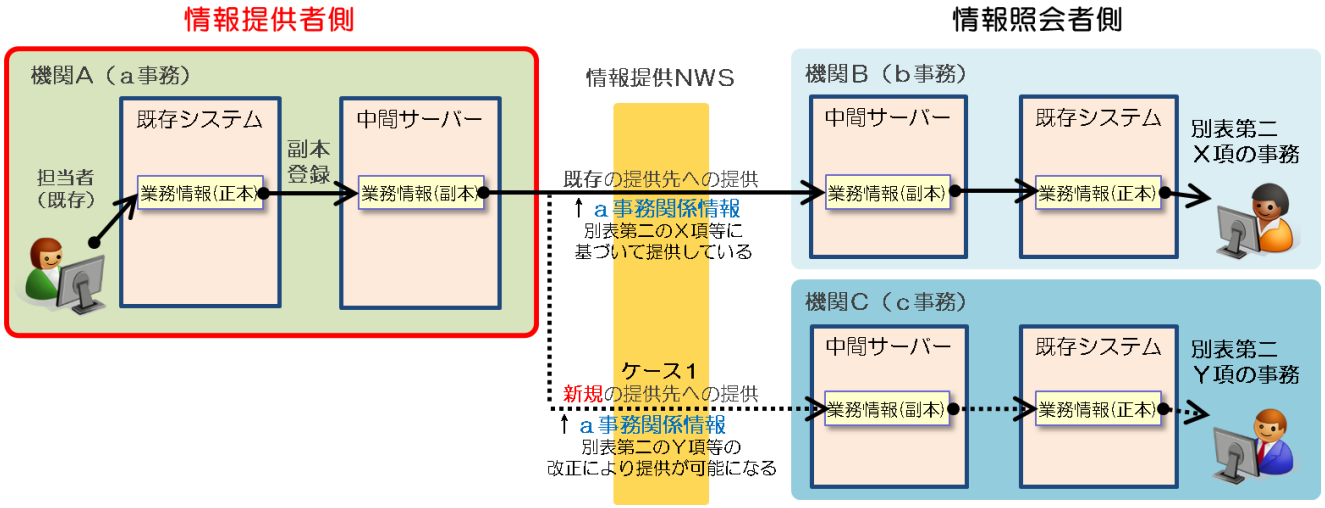
・　医療保険者向け中間サーバー、情報提供ネットワークシステム、住民基本台帳システム等について、当該システムを運営する他の行政機関等によるシステムの変更が行われた場合に、当該システムを使用している評価実施機関が、当該システムの変更後のリスク対策等について特定個人情報保護評価書に記載するものの、評価実施機関に固有の特定個人情報を取り扱うプロセス及び当該プロセスに係るリスク対策に変更がないケース

＜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】

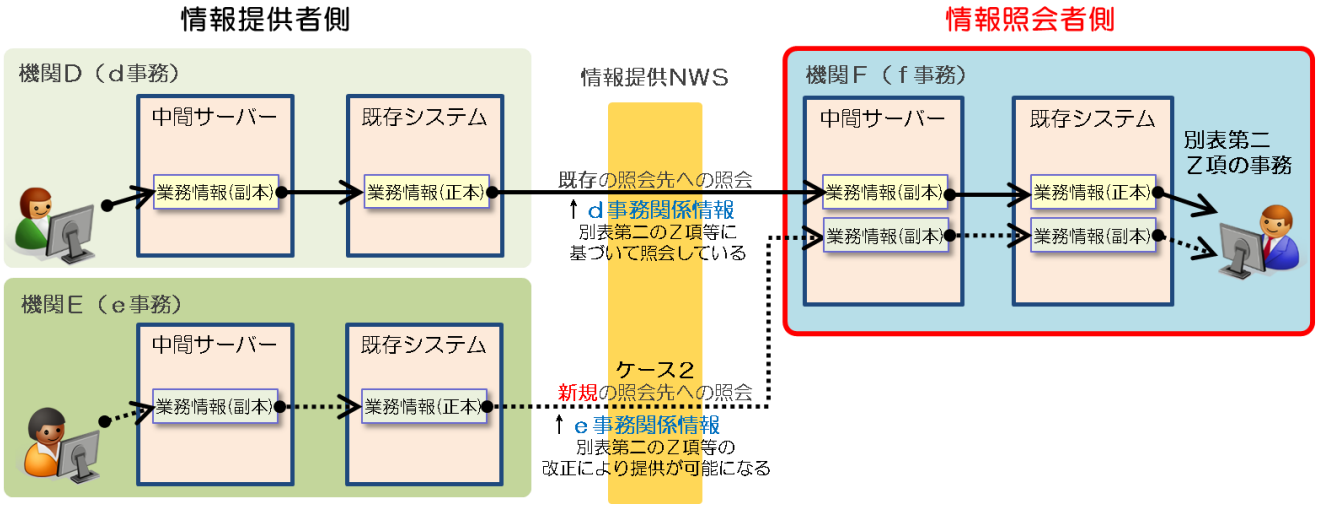
・ 機関Ａ（情報提供者）が、これまでａ事務で取り扱う特定個人情報ファイル（ａ事務関係情報）を情報提供ネットワークシステム経由で機関Ｂに提供していたところ、番号法別表第二等の改正により、機関Ａが新たにａ事務で取り扱う特定個人情報ファイル（ａ事務関係情報）を情報提供ネットワークシステム経由で機関Ｃに提供することとなるケース



→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に該当し、重要な変更に当たらず、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

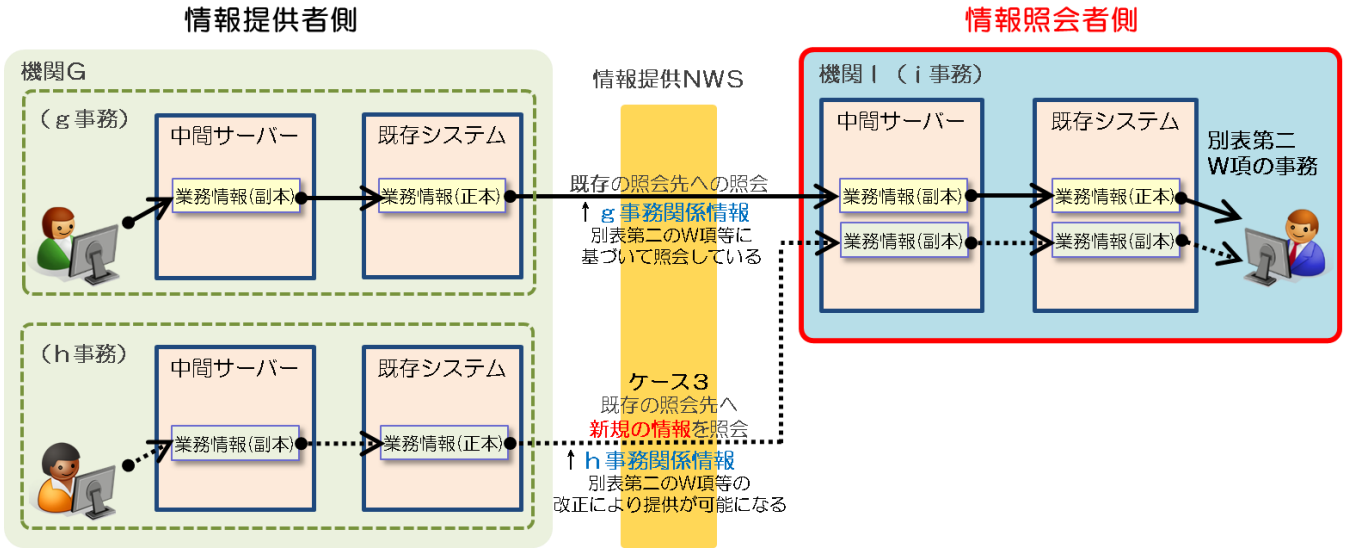


→この場合、機関Ｆのｆ事務の特定個人情報保護評価書において、重要な変更の対象である「主な記録項目」や「入手元」の記載内容に変更が生じますが、照会先の追加にあたり特定個人情報ファイルを取り扱うプロセス及び当該プロセスに係るリスク対策に変更が生じない場合には、リスクを相当程度変動させるものではないと考えられる変更に該当し、重要な変更に当たらず、機関Ｆは評価の再実施を行う必要はありません。

※　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に該当し、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。

Ｑ第６の２（２）－２

「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変更であっても、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は重要な変更に当たらないとしているのはどのような理由なのでしょうか。

（Ａ）

○　特定個人情報保護評価の基本理念は個人のプライバシー等の権利利益の保護であり、そもそも番号法が、保有する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実施することを求めているのも、事前対応により個人のプライバシー等の権利利益の侵害の未然防止を図るためです。

○　このような特定個人情報保護の基本理念・目的に照らすと、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する特定個人情報ファイルの取扱いの変更について、改めて特定個人情報保護評価を実施する理由はないと考えられます。

○　また、特定個人情報保護評価の再実施に伴う負担を課さないことにより、評価実施機関の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軽減する措置を推奨するという趣旨もあります。

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なりますが、重要な変更に当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。具体的には、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などが考えられます。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。

○　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。

Q　第６の２（２）－４

「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ものがありますが、重要な変更に該当するかどうかの判断はどのような手順で行うのでしょうか。

（Ａ）

【委員会の承認対象である全項目評価書のうち「重要な変更」の対象である記載項目を変更する場合】

○　評価実施機関において、指針第６の２（２）及びQ第６の２（２）－１、３に記載された具体例を参考に、重要な変更に当たるかどうかを検討し、事前に委員会事務局へ相談してください。委員会事務局は、評価実施機関と調整の上、重要な変更に当たるか否かを確認します。

　委員会事務局での確認は、評価実施機関に変更内容の詳細を伺いつつ行う必要があるため、余裕を持って相談してください。

【重点項目評価書又は委員会の承認対象でない全項目評価書のうち「重要な変更」の対象である記載項目を変更する場合】

○　評価実施機関において、指針第６の２（２）及びQ第６の２（２）－１、３に記載された具体例を参考に、重要な変更に当たるかどうかを判断してください。

Ｑ第６の２（２）－５

重大事故の発生は重要な変更に当たらないとしながら、「特定個人情報に関する重大事故の発生に伴い評価実施機関がリスク対策等を見直すことが想定され、この場合は、重要な変更に該当する。」としているが、どのような場合でしょうか。

（Ａ）

○　重大事故の発生を事前に知ることは不可能であり、特定個人情報保護評価を事前に再実施することが求められる「重要な変更」の対象とはなりません。したがって、別表においてリスク対策に変更を加えようとする場合であっても、重大事故の発生の場合を除くものと定めています。

○　一方、重大事故の発生を受けて、評価実施機関は原因究明を実施し、再発防止策を策定することが想定されます。

再発防止策の内容は重大事故の原因にもよりますが、システムの全面的な入替えや事務手続の大幅な変更が計画されることも想定されます。このような大規模なリスク対策の変更は、重大事故が再発するリスクを軽減させることを目的とした変更であることは確かですが、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、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になると考えられます。

Ｑ第６の２（２）－６

基礎項目評価書の変更は、重要な変更に当たらないのでしょうか。

（Ａ）

○　基礎項目評価書の記載内容の変更は、直ちに「重要な変更」の対象とはならず、特定個人情報保護評価書の修正の対象となります。

ただし、その変更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の実施が義務付けられる場合は特定個人情報保護評価の再実施が必要となります。

（３）しきい値判断の結果の変更

上記第５の４に定める特定個人情報保護評価書の見直しにおいて、対象人数又は取扱者数が増加したこと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る場合、評価実施機関は、速やかに特定個人情報保護評価を再実施するものとする（規則第６条第２項及び第３項、第７条第２項から第６項まで、第８条及び第 14 条）。

また、評価実施機関における特定個人情報に関する重大事故の発生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る場合、評価実施機関は、当該特定個人情報に関する重大事故の発生後速やかに特定個人情報保護評価を再実施するものとする（規則第６条第２項及び第３項、第７条第２項から第６項まで、第８条及び第 14 条）。

なお、対象人数又は取扱者数が減少したことによりしきい値判断の結果が変わり、全項目評価から重点項目評価若しくは基礎項目評価に、又は重点項目評価から基礎項目評価に変更になった場合については、特定個人情報保護評価書の修正として、委員会に提出した上で公表するものとする。

（解説）

特定個人情報保護評価を実施（又は再実施）した後、特定個人情報ファイルの取扱いに伴う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変動させる変更であっても、その性質上、「重要な変更」に該当しないものがあります。

基礎項目評価書中のしきい値判断項目、すなわち、①評価対象の事務の対象人数、②特定個人情報ファイルの取扱者数及び③特定個人情報に関する重大事故です。

①対象人数は人口動態や経済社会情勢の変化に影響されて変わることが多く、必ずしも評価実施機関が能動的に変更するものではなく、また日々変化します。②取扱者数も職員の異動やアルバイトの採用などに伴い日々変化するものです。③重大事故の発生を事前に知ることは不可能です。したがって、これらの変化に対応し事前に特定個人情報保護評価を再実施することは現実的ではありません。

したがって、これらのしきい値判断項目に、しきい値判断の結果が変わる程度の大幅な変更が生じた場合は、事後に特定個人情報保護評価を再実施することが求められています。

すなわち、これらのしきい値判断項目の変更に伴ってしきい値判断の結果が変わり、重点項目評価又は全項目評価の実施が新たに義務付けられる場合は、速やかに特定個

人情報保護評価を再実施することが求められます。

しきい値判断項目の中でも、①対象人数及び②取扱者数と、③重大事故の発生では、特定個人情報保護評価の再実施の契機が異なります。①及び②については、少なくとも１年に１度は実施することが努力義務とされている特定個人情報保護評価書の見直しにおいて、①又は②の人数が増加したことによりしきい値判断の結果が変わった後、速やかに特定個人情報保護評価を再実施することが求められます。

③については、特定個人情報に関する重大事故の発生を知った後速やかに特定個人情報保護評価を再実施しなければなりません。なお、対象人数が１万人未満の事務の場合は、個人のプライバシー等の権利利益に与え得る影響と評価実施機関の負担を比較衡量し、重大事故が発生した場合も、引き続き基礎項目評価の実施のみが義務付けられることとなります。

Ｑ第６の２（３）－１

特定個人情報ファイルを取り扱う事務の対象人数が 1,000 人を超えた場合や、手作業処理用ファイルを電子ファイルに変えた場合は、特定個人情報保護評価の実施が義務付けられるのでしょうか。

（Ａ）

○　特定個人情報ファイルを取り扱う事務が、指針第４の４（１）のアからキまでに該当していたものの、その後、特定個人情報ファイルに記録される本人の数の増加や手作業処理用ファイルを電子ファイルに変えようとすること等により、指針第４の４（１）のアからキまでに該当しないこととなる場合は、「特定個人情報ファイルを保有しようとするとき」に該当しますので、当該事務について、特定個人情報保護評価を実施することが求められます。

Ｑ第６の２（３）－２

しきい値判断の結果が変わり、新たに重点項目評価を実施することが必要となりましたが、国民（地方公共団体等にあっては住民等）からの意見聴取を実施する必要があるのでしょうか。

（Ａ）

○　重点項目評価を実施する場合には、国民（地方公共団体等にあっては住民等）からの意見聴取は義務付けられませんが、任意に実施することを妨げるものではありません。

Ｑ第６の２（３）－３

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しなければならないとなった場合、いつ評価を実施すればよいのでしょうか。

（Ａ）

○　重点項目評価又は全項目評価の実施は、しきい値判断の結果が明らかになった後、速やかに行うことが求められます。

○　しきい値判断の結果が変わるために新たに重点項目評価又は全項目評価を実施することとなり、システム開発等を伴わない場合には、システム開発等のフローに即した実施時期の設定は不適当です。したがって、しきい値判断の結果が明らかになった後、速やかに特定個人情報保護評価を再実施することとなります。

○　特定個人情報に関する重大事故の発生に起因する場合は、当該重大事故の発生を知った後速やかに特定個人情報保護評価を再実施しなければなりません。

Ｑ第６の２（３）－４

しきい値判断における重大事故は「評価実施機関における」とあります。評価実施機関内の全く関係のない部署において重大事故が発生した場合でも、しきい値判断の結果の変更として、特定個人情報保護評価を再実施しなければならないのでしょうか。

（Ａ）

○　その場合でも、重点項目評価又は全項目評価の実施が新たに義務付けられる場合は、速やかに特定個人情報保護評価を再実施しなければなりません。

○　ある事務について既に特定個人情報保護評価書を公表していた場合、当該事務に関わりのない評価実施機関内の部署が特定個人情報に関する重大事故を発生させたとしても、それにより当該事務に関するしきい値判断の結果が変われば、特定個人情報保護評価の再実施が必要となります。

○　重大事故が発生した場合、その事故を起こした事務や部署だけではなく、評価実施機関全体に対する国民・住民の信頼に関わると考えられることに加え、事故が発生した要因の分析及び再発防止策については、評価実施機関全体で取り組む必要があるとの考え方によるものです。

Ｑ第６の２（３）－５

評価実施機関内の他部署で重大事故が発生しましたが、元々全項目評価を実施していたため、しきい値判断の結果は変わりません。この場合は、特定個人情報保護評価を再実施することは必要でしょうか。

（Ａ）

○　重大事故の発生それ自体が直ちに重要な変更に当たるものではありません。

しかし、重大事故の発生を契機として、評価実施機関がリスク対策等を見直すことが想定され、システムの全面的な入替えや事務手続の大幅な変更が計画されることが考えられます。そのような場合は、元々全項目評価を実施していた事務についても、「重大な変更」として特定個人情報保護評価の再実施が必要となる場合があります。

Ｑ第６の２（３）－６

対象人数又は取扱者数が減少したことにより、しきい値判断の結果が変わり、全項目評価から重点項目評価に変更になった場合は、すぐに新たな重点項目評価書を提出・公表しなければならないのでしょうか。

（Ａ）

○　しきい値判断の結果の変更により、全項目評価から重点項目評価に変更になった場合は、必ず重点項目評価書を新規に作成し、提出・公表しなければならないわけでなく、任意で全項目評価書を提出・公表することが可能です。

○　その際は、全項目評価書のしきい値判断等に関する項目を修正し、委員会に提出した上で公表してください。

（４）一定期間経過

評価実施機関は、規則第 15 条の規定に基づき、直近の特定個人情報保護評価書を公表してから５年を経過する前に、特定個人情報保護評価を再実施するよう努めるものとする。

（解説）

番号法では、特定個人情報保護評価を実施（又は再実施）した後、特定個人情報ファイルの取扱いについて重要な変更を加えようとする場合、対象人数若しくは取扱者数の増加又は特定個人情報に関する重大事故の発生によりしきい値判断の結果が変更される場合には、特定個人情報保護評価の再実施が義務付けられますが、それ以外の場合は義務付けられません。

しかし、特定個人情報保護評価を実施してからある程度の期間が経過すると、個人情報の保護に関する情報技術の進歩や社会情勢の変化が生じ、特定個人情報保護評価を再実施することが望ましい状況となることが考えられます。

昨今の情報通信技術の進歩の早さを踏まえると、５年を経過すればリスク対策などを見直す必要性が高くなっていることが想定されます。そこで、直近の特定個人情報保護評価書を公表してから５年を経過する前に特定個人情報保護評価を再実施することを努力義務としています。

なお、直近の特定個人情報保護評価書の公表とは、特定個人情報保護評価の（新規保有時の）実施又は再実施に伴う公表のみであり、特定個人情報保護評価書の修正に伴う公表は含みません。したがって、「５年を経過する前」の起点は直近の実施又は再実施の際の公表日となります。

Ｑ第６の２（４）－１

特定個人情報保護評価は、５年ごとに実施すれば十分ということでしょうか。

（Ａ）

○　５年を経過する前であっても、特定個人情報ファイルの取扱いについて重要な変更を加えようとする場合、対象人数若しくは取扱者数の増加又は特定個人情報に関する重大事故の発生によりしきい値判断の結果が変更される場合は、特定個人情報保護評価の再実施が義務付けられます。また、これらに当たらない場合でも、任意に再実施することを妨げるものではありません。

第７　特定個人情報保護評価書の修正

１　基礎項目評価書

基礎項目評価書の記載事項に、上記第６の２（３）のしきい値判断の結果の変更に該当しない変更が生じた場合、評価実施機関は、規則第 14 条の規定に基づき、基礎項目評価書を速やかに修正し、委員会に提出した上で公表するものとする。修正に当たっては、委員会が定める特定個人情報保護評価書様式中の変更箇所欄に変更項目等を記載するものとする。

２　重点項目評価書・全項目評価書

重点項目評価書又は全項目評価書の記載事項に、上記第６の２（２）の重要な変更に当たらない変更が生じた場合、評価実施機関は、規則第 14 条の規定に基づき、重点項目評価書又は全項目評価書を速やかに修正し、委員会に提出した上で公表するものとする。修正に当たっては、委員会が定める特定個人情報保護評価書様式中の変更箇所欄に変更項目等を記載するものとする。

この場合は、特定個人情報保護評価の実施に該当せず、全項目評価の場合であっても、国民（地方公共団体等にあっては住民等）からの意見の聴取及び委員会による承認又は第三者点検は必要ない。評価実施機関の任意の判断で、国民（地方公共団体等にあっては住民等）からの意見の聴取又は第三者点検を行うことを妨げるものではない。

（解説）

特定個人情報保護評価を実施（又は再実施）した後、当該特定個人情報ファイルの取扱い等に変更・変化が生じることがあります。このうち、「重要な変更」と「しきい値判断の結果の変更」に当たる場合は、特定個人情報保護評価の再実施が義務付けられますが、それ以外の場合は義務付けられません（このほか、直近の特定個人情報保護評価書を公表してから５年を経過する前に特定個人情報保護評価を再実施することが努力義務とされています。）。

しかし、特定個人情報保護評価の再実施が義務付けられない程度の比較的軽微な変更・変化であっても、公表している特定個人情報保護評価書の記載内容と実態の齟齬を放置することは、特定個人情報ファイルの取扱いについての透明性を高め、国民・住民の信頼を確保するという特定個人情報保護評価の目的に反する結果となります。

そこで、こうした場合は、既に公表している特定個人情報保護評価書を修正し、委員会に提出した上で公表するものとしています。

なお、この修正に伴う公表は５年を経過する前の再実施の起点にはなりません。

第８　個人情報保護法及び番号法に基づく事前通知

個人情報保護法第 74 条第１項の規定に基づき、会計検査院を除く行政機関が個人情報ファイルを保有しようとするときは、当該行政機関の長は、同項各号に規定する事項（以下「事前通知事項」という。）をあらかじめ委員会に通知しなければならず、また、事前通知事項を変更しようとするときも同様に通知しなければならない（以下「事前通知」と総称する。）。行政機関が、特定個人情報保護評価を実施し、全項目評価書を公表した場合、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ようとするときに特定個人情報保護評価を再実施し、事前通知事項を変更した全項目評価書を公表した場合は、番号法第 28 条第５項の規定により、それぞれ事前通知を行ったものとみなす。

また、行政機関が、特定個人情報保護評価を実施し、重点項目評価書を提出・公表した場合、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に特定個人情報保護評価を再実施し、事前通知事項を変更した重点項目評価書を提出・公表した場合、保有する特定個人情報ファイルに重要な変更に当たらない変更を加えようとするときに事前通知事項を変更した全項目評価書又は重点項目評価書を変更前に提出・公表した場合等は、それぞれ事前通知等を併せて行ったものとして取り扱う。

（解説）

指針における上記の規定については、行政機関における規定となりますので、行政機関以外の評価実施機関は認識いただく必要はありません。

１．事前通知とは

個人情報保護法第 74 条第１項には、「行政機関（会計検査院を除く）が個人情報ファイルを保有しようとするときは、当該行政機関の長は、あらかじめ、委員会に対し、次に掲げる事項を通知しなければならない。」と規定されています。

２．特定個人情報保護評価の実施により事前通知を行ったものとみなす規定

事前通知事項におけるファイルの名称や利用目的等の事項は、特定個人情報保護評価における評価項目と重複していることから、番号法第 28 条第５項の規定によって、特定個人情報保護評価を実施（特定個人情報保護評価書を委員会に提出し公表）した場合、事前通知も行ったものとみなしています。

３．みなす規定が適用される場合

番号法第 28 条第５項において、事前通知を行ったものとみなす場合は「前項の規定により評価書が公表されたとき」とされており、ここでいう、前項の規定により評価書が公表されたとき、つまり行政機関が全項目評価を実施又は再実施した場合に、本規定が適用されることになります。

４．その他の通知等

上記３以外の次の場合には、指針の規定に基づいて、変更した特定個人情報保護評価書を委員会に提出し、公表することによって、個人情報保護法第 74 条第１項及び第３項に定める通知を併せて行ったものとして取り扱うこととなります。なお、次の（１）から（４）までの場合はその事象が生じる前に、（５）及び（６）の場合はその事象が生じた後に遅滞なく行うこととなります。

（１） 全項目評価書に記載する特定個人情報ファイルにおいて、事前通知事項に重要な変更に当たらない変更が生じるとき
（２） 重点項目評価書に記載する特定個人情報ファイルを保有しようとするとき
（３） 重点項目評価書に記載する特定個人情報ファイルにおいて、事前通知事項に重要な変更が生じるとき
（４） 重点項目評価書に記載する特定個人情報ファイルにおいて、事前通知事項に重要な変更に当たらない変更が生じるとき
（５） 特定個人情報ファイルの保有をやめたとき
（６） 特定個人情報ファイルの対象人数が 1,000 人未満となったとき

５．まとめ

上記１～４を整理すると次のとおりとなります。

<table>
<tr><th></th><th>全項目評価書
の提出・公表</th><th>重点項目評価書
の提出・公表</th><th>提出・公表
をすべき時期</th></tr>
<tr><td>特定個人情報ファイルを新たに保有しようとするとき</td><td>通知を行ったものとみなす</td><td rowspan="5">通知を併せて行ったものとして取り扱う</td><td rowspan="3">ファイルの保有又は変更の前</td></tr>
<tr><td>事前通知事項に重要な変更が生じるとき</td><td>通知を行ったものとみなす</td></tr>
<tr><td>事前通知事項に重要な変更に当たらない変更が生じるとき</td><td>通知を併せて行ったものとして取り扱う</td></tr>
<tr><td>特定個人情報ファイルの保有をやめたとき</td><td>通知を併せて行ったものとして取り扱う</td><td rowspan="2">ファイルの保有をやめた又は変更の後遅滞なく</td></tr>
<tr><td>特定個人情報ファイルの対象人数が1,000人未満となったとき</td><td>通知を併せて行ったものとして取り扱う</td></tr>
</table>

※　なお、全項目評価書又は重点項目評価書の事前通知事項に重要な変更に当たらない変更が生じるときに、全項目評価書又は重点項目評価書の提出・公表がファイルの変更後になる場合は、ファイルの変更の前に、委員会に別途事前通知を行う必要があります。

Ｑ第８－１

基礎項目評価のみの実施の場合は、事前通知を行ったものとみなされないのでしょうか。

（Ａ）

○　基礎項目評価のみの実施の場合は、事前通知を行ったとはみなされません。別途、委員会が定める事前通知の方法に基づいて委員会に通知していただく必要があります。

これは、基礎項目評価書においては、個人情報保護法に定める事前通知すべき事項が記載されていないことによります。

第９　特定個人情報保護評価の評価項目

１　基本的な考え方

特定個人情報保護評価を実施するに当たって、評価実施機関は、特定個人情報ファイルを取り扱う事務の特性を明らかにした上で、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を与え得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について認識又は分析し、このようなリスクを軽減するための適切な措置を講じていることを確認の上、特定個人情報保護評価書において宣言するものとする。

評価実施機関は、リスクを軽減するための措置を検討する際には、特定個人情報の安全管理に関する基本方針、特定個人情報の取扱規程等を策定することが望ましい。また、リスクを軽減するための措置には、物理的安全管理措置、技術的安全管理措置、組織的安全管理措置及び人的安全管理措置があり、評価実施機関は、基本方針、取扱規程等を踏まえ、評価実施機関の規模及び事務の特性に応じた適切な措置を講ずるものとする。

なお、技術の進歩に伴うクラウドサービス等の新たなサービス、開発手法等を導入する場合には、当該サービス、開発手法等の特性を考慮した上で、適切な安全管理措置を講ずるものとする。

２　評価項目

（１）基礎項目評価書

規則第２条第１号に規定する基礎項目評価書の記載事項は、次のとおりとする。

ア　基本情報

特定個人情報保護評価の対象となる事務の概要、当該事務において使用するシステムの名称、特定個人情報ファイルの名称、当該事務を対象とする特定個人情報保護評価の実施を担当する部署及び所属長の役職名、当該事務において個人番号を利用することができる法令上の根拠等を記載するものとする。また、当該事務において情報連携を行う場合にはその法令上の根拠を記載するものとする。

イ　リスク対策

特定個人情報ファイルを取り扱うプロセスにおいて個人のプライバシー等の権利利益に影響を与え得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認識し、このうち主なリスクを軽減するための措置の実施状況について記載するものとする。

また、自己点検・監査、従業者に対する教育・啓発等のリスク対策の実施状況についても記載するものとする。

これらのリスク対策を踏まえ、評価実施期間は、リスクを軽減するための適切な措置を講じていることを確認の上、宣言するものとする。

（２）重点項目評価書

規則第２条第２号に規定する重点項目評価書の記載事項は、次のとおりとする。

ア　基本情報

特定個人情報保護評価の対象となる事務の内容、当該事務において使用するシステムの機能、当該事務において取り扱う特定個人情報ファイルの名称、当該事務を対象とする特定個人情報保護評価の実施を担当する部署及び所属長の役職名、当該事務において個人番号を利用することができる法令上の根拠等を記載するものとする。また、当該事務において情報連携を行う場合にはその法令上の根拠を記載するものとする。

イ　特定個人情報ファイルの概要

特定個人情報ファイルの種類、対象となる本人の数・範囲、記録される項目その他の特定個人情報保護評価の対象となる事務において取り扱う特定個人情報ファイルの概要を記載するものとする。また、特定個人情報の入手及び使用の方法、特定個人情報ファイルの取扱いの委託の有無及び委託する場合にはその方法、特定個人情報の提供又は移転の有無及び提供又は移転する場合にはその方法、特定個人情報の保管場所その他の特定個人情報ファイルを取り扱うプロセスの概要を記載するものとする。

ウ　リスク対策

特定個人情報ファイルを取り扱うプロセスにおいて個人のプライバシー等の権利利益に影響を与え得る特定個人情報の漏えいその他の事態を発生させる主なリスクについて分析し、このようなリスクを軽減するための措置について記載するものとする。重点項目評価書様式は主なリスクのみを示しているが、その他のリスクについても分析し、そのようなリスクを軽減するための措置についても記載することが推奨される。

また、自己点検・監査、従業者に対する教育・啓発等のリスク対策についても記載するものとする。

これらのリスク対策を踏まえ、評価実施機関は、リスクを軽減するための適切な措置を講じていることを確認の上、宣言するものとする。

エ　その他

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合せ等について記載するものとする。

（３）全項目評価書

法第 28 条第１項各号及び規則第 12 条に規定する全項目評価書の記載事項は、次のとおりとする。

ア　基本情報

特定個人情報保護評価の対象となる事務の詳細な内容、当該事務において使用するシステムの機能、当該事務において取り扱う特定個人情報ファイルの名称、当該事務を対象とする特定個人情報保護評価の実施を担当する部署及び所属長の役職名、当該事務において個人番号を利用することができる法令上の根拠等を記載するものとする。また、当該事務において情報連携を行う場合にはその法令上の根拠を記載するものとする。

イ　特定個人情報ファイルの概要

特定個人情報ファイルの種類、対象となる本人の数・範囲、記録される項目その他の特定個人情報保護評価の対象となる事務において取り扱う特定個人情報ファイルの概要を記載するものとする。また、特定個人情報の入手及び使用の方法、特定個人情報ファイルの取扱いの委託の有無及び委託する場合にはその方法、特定個人情報の提供又は移転の有無及び提供又は移転する場合にはその方法、特定個人情報の保管及び消去の方法その他の特定個人情報ファイルを取り扱うプロセスの概要を記載するものとする。

ウ　リスク対策

特定個人情報ファイルを取り扱うプロセスにおいて個人のプライバシー等の権利利益に影響を与え得る特定個人情報の漏えいその他の事態を発生させる多様なリスクについて詳細に分析し、このようなリスクを軽減するための措置について記載するものとする。全項目評価書様式に示すもの以外のリスクについても分析し、そのようなリスクを軽減するための措置についても記載することが推奨される。

また、自己点検・監査、従業者に対する教育・啓発等のリスク対策についても記載するものとする。

これらのリスク対策を踏まえ、評価実施機関は、リスクを軽減するための適切な措置を講じていることを確認の上、宣言するものとする。

エ　評価実施手続

行政機関等は、上記第５の３（３）アにより実施した国民からの意見の聴取の方法、主な意見の内容等、下記第 10 の１に定める委員会による承認のために全項目評価書を委員会に提出した日、委員会による審査等について記載するものとする。

地方公共団体等は、上記第５の３（３）イにより実施した住民等からの意見の聴取及び第三者点検の方法等について記載するものとする。

オ　その他

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合せ等について記載するものとする。

（解説）

特定個人情報保護評価の実施に当たって評価実施機関が行うべきことは、特定個人情報保護評価の対象となる特定個人情報ファイルを取り扱う事務の特性を明らかにした上で、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を与え得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について認識・分析し、このようなリスクを軽減するために適切な措置を講じていることを確認の上、宣言することです。

特定個人情報保護評価に当たって評価実施機関が評価すべき項目（評価項目）の数又は深度は、全項目評価が最も大きく、重点項目評価、基礎項目評価の順で小さくなっています。実務上は、しきい値判断の結果に基づいて求められる特定個人情報保護評価の種類に応じ、該当する特定個人情報保護評価書に記載していくことになります。

Ｑ第９の１－１

「リスクを軽減するための適切な措置を講じていることを確認の上、宣言するものとする。」とありますが、具体的にどのように宣言すればよいのでしょうか。

（Ａ）

○　特定個人情報保護評価書の表紙にある「個人のプライバシー等の権利利益の保護の宣言」欄に記載することで宣言することができます。その際、評価実施機関が講じている措置のうち評価実施機関として特に積極的に一般に情報提供したい措置があれば、「特記事項」欄に記載することができます。

Ｑ第９の１－２

「特定個人情報の安全管理に関する基本方針、特定個人情報の取扱規程等を策定することが望ましい」としているのは、どのような理由なのでしょうか。また、どのように取り組めばよいのでしょうか。

（Ａ）

○　特定個人情報の安全管理に関する基本方針については、特定個人情報の適正な取扱いの確保について組織として取り組むために、特定個人情報の取扱規程等については、特定個人情報の適正な取扱いを確保するための具体的な取扱いを定めるために、それぞれ策定することが望ましいと考えられます。

○　基本方針、取扱規程等の策定にあたっては、「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・地方公共団体等編／事業者編）」の「（別添１）特定個人情報に関する安全管理措置（行政機関等・地方公共団体等編／事業者編）」を参照してください。

Ｑ第９の１－３

物理的安全管理措置、技術的安全管理措置、組織的安全管理措置、人的安全管理措置の４つの安全管理措置を踏まえ、「リスクを軽減するための適切な措置」を講ずるにあたりどのように考えたらよいのでしょうか。

（Ａ）

○　これまで委員会が特定個人情報の漏えい等の報告を受けている事案は、人為的ミスに起因するものが多く見られます。

○　したがって、特定個人情報保護評価の実施にあたっては、特定個人情報保護評価書に記載しているリスク対策が物理的及び技術的安全管理措置に係る内容に偏っていないかという観点も含め、各評価実施機関において組織体制や事務運営の特性にあった組織的及び人的安全管理措置に係るリスク対策も確認・見直しを行って、記載の追加や変更が必要になるかを検討することが重要です。

○　また、安全管理措置の適切な実行を確保していくために、組織の管理者、責任者等の関与の下、事前評価（特定個人情報保護評価）、事務運営、監査、教育・啓発、継続的な改善といったPDCAサイクルを回していくことが重要です。

継続的な改善を行う際には、リスク対策だけを改善するのではなく、事務運営自体にも改善の余地がないかを検討することが重要です。例えば、リスクが高い業務プロセスが多く存在する事務では、リスクを生じさせる業務プロセスを削減できないか、リスクを軽減させるための新しい業務プロセスや新しい仕組みを導入できないか等の観点から事務運営自体の見直しを検討することが考えられます。

Q第９の１－４

「リスクを軽減するための措置には、物理的安全管理措置、技術的安全管理措置、組織的安全管理措置及び人的安全管理措置があり」とありますが、具体的にどのような措置が考えられるのでしょうか。

（Ａ）

○　具体的には、物理的安全管理措置として、特定個人情報ファイルを取り扱う区域の管理を行うこと、特定個人情報ファイルを取り扱う機器及び電子媒体等の盗難等の防止のための措置を講ずること、電子媒体等の取扱いにおける漏えい等の防止のため使用や接続の制限等必要な措置を講ずること、保存期間経過後に個人番号の削除並びに機器及び電子媒体等の廃棄を復元不可能な手段で行うこと等が考えられます。

○　技術的安全管理措置として、適切なアクセス制御を行うこと、正当なアクセス権を有する者であるかを識別し認証すること、不正アクセス等による被害の防止のための仕組み等を導入し、適切な運用を行うこと、通信経路における情報漏えい等を防止する措置を講ずること等が考えられます。

○　組織的安全管理措置として、安全管理措置を講ずるための組織体制を整備すること、取扱規程等に基づいた運用を行うこと、特定個人情報ファイルの取扱状況を確認する手段を整備すること、情報漏えい等の事案の発生又は兆候を把握した場合に適切かつ迅速に対応する体制及び手順等を整備すること、取扱状況の把握及び安全管理措置の見直しを行うこと等が考えられます。

○　人的安全管理措置としては、特定個人情報が適切に取り扱われるよう、事務取扱担当者等に対する監督・教育を行うこと、法令・内部規程等に違反した職員に対して厳正な対処を行うこと等が考えられます。

○　これらの措置の詳細については、「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・地方公共団体等編／事業者編）」の「（別添１）特定個人情報に関する安全管理措置（行政機関等・地方公共団体等編／事業者編）」を参照してください。

Q第９の１－５

オンプレミス（※）環境にある特定個人情報ファイルを取り扱う既存システムを改修し、外部のクラウドサービスを利用します。どのような点を考慮して特定個人情報保護評価を行うのでしょうか。

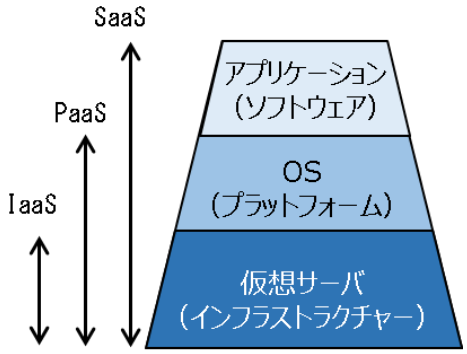
（Ａ）

【クラウドサービスの種類に対応したリスク識別、リスク評価、リスク対策の検討】

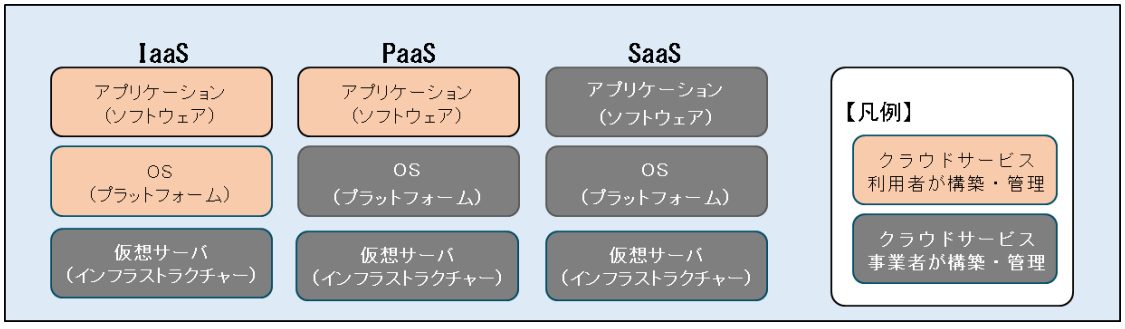
○　クラウドサービスには、クラウドサービス事業者とクラウドサービス利用者の役割分担により、IaaS、PaaS、SaaS の３種に分類されます。

システムの階層を３層で捉えた場合、１段目までクラウドサービス事業者に任せるのが IaaS、２段目まで任せるのが PaaS、３段目まで任せるのが SaaS です。クラウドサービスの種類によって、クラウドサービス事業者の構築・管理の範囲が異なります。

［システムの階層とクラウドサービス事業者に任せる範囲］



［3 種類のクラウドサービス（IaaS、PaaS、SaaS）の構築・管理範囲］



○　したがって、特定個人情報保護評価の対象となる事務において、クラウドサービスを利用する場合、クラウドサービスの種類により、生じうるリスクが異なることから、リスク識別・評価、リスクを軽減させるために講ずる措置が異なる場合があります。

○　一般的に、クラウドサービス事業者への委託については、番号法の委託に該当するか否かという点で特定個人情報保護評価書に記載が必要なリスク対策が異なり

ます。また、番号法の委託に該当するか否かは、クラウドサービス事業者が当該契約内容を履行するに当たって個人番号をその内容に含む電子データを取り扱うかどうかが基準となります。

例えば、クラウドサービス事業者が提供する IaaS を利用し、当該事業者が委託業務の範囲内で個人番号をその内容に含む電子データを取り扱わない場合は、そもそも、個人番号関係事務又は個人番号利用事務の全部又は一部の委託を受けたとみることはできないため、番号法上の委託には該当しません。

ただし、契約によって当該事業者が個人番号をその内容に含む電子データを取り扱わない旨が定められており、適切にアクセス制御を行う等の措置が講じられていることを確認し、必要に応じて、その内容を特定個人情報保護評価書に記載することが考えられます。

また、クラウドサービス事業者が提供する PaaS、SaaS を利用する場合には、当該事業者がアプリケーションや OS 等の保守サービスもクラウドサービスの一環として行うことが考えられます。この場合、サービス内容の全部又は一部として個人番号をその内容に含む電子データを取り扱う場合には、個人番号利用事務又は個人番号関係事務の一部の委託に該当します。そのため、委託内容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特定個人情報保護評価書に記載する必要があると考えられます。

〔クラウドサービス事業者が保守サービスの中で個人番号を取り扱う典型的な例〕

・ 個人番号を用いて情報システムの不具合を再現させ検証する場合
・ 個人番号をキーワードとして情報を抽出する場合

【その他】

○ クラウドサービスの種類が IaaS、PaaS、SaaS のどの分類であっても、オンプレミス環境にある既存システムからクラウド環境に移行し、特定個人情報ファイルを取り扱うシステム等の場所が変わる場合、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可能性があります。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特定個人情報保護評価書に記載する必要があります。

○ また、クラウド環境への移行の際に、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、クラウド環境へデータを移し替える作業や、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、機器の廃棄に係るリスクについても、漏えい、滅失等が起こらないように特定個人情報保護評価を実施しているか注意が必要です。

（※）オンプレミスとは、従来型の構築手法で、アプリケーションごとに個別の動作環境（データセンター、ハードウェア、サーバ等）を準備し、自らコントロールするものをいいます。

Ｑ第９の１－６

クラウドサービスを利用する場合、利用者側では、クラウドサービス事業者の情報セキュリティの管理体制を個別に把握することは困難ですが、特定個人情報保護評価において、どのように考えればよいのでしょうか。

（Ａ）

【クラウドサービスの選定における留意事項】

○　行政機関においては、「政府情報システムにおけるクラウドサービス利用に係る基本方針（デジタル社会推進会議幹事会決定）」の要件を満たすクラウドサービスの選定、「政府情報システムのためのセキュリティ評価制度（ISMAP）」の ISMAP クラウドサービスリストからのクラウドサービスの選定を行う等、サービスの選定時において、適切に情報セキュリティが確保されているサービスを利用することが重要です。

○　行政機関以外の評価実施機関においても、「政府情報システムにおけるクラウドサービス利用に係る基本方針」、「政府情報システムのためのセキュリティ評価制度（ISMAP）」の ISMAP クラウドサービスリスト、「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（総務省）」等を参考に、行政機関同様に情報セキュリティが確保されているサービスを適切な選定プロセスを経て、利用する必要があります。

【クラウドサービス事業者の情報セキュリティの管理体制の把握】

○　クラウドサービス事業者の特定個人情報ファイルを保管するサーバ設置場所への入退室管理等の物理的対策、特定個人情報ファイルの廃棄・消去の実態等について、直接、委託元が詳細に把握することは困難だと思われます。そのため、第三者による認証や各クラウドサービスが提供する監査報告書を利用し把握することが考えられます。

○　特定個人情報保護評価書のリスク対策等の記載においては、クラウドサービスを選定する際の基準を記載し、基準に合致したものを利用すること、また、特定個人情報の取扱いの実態については、各クラウドサービスが提供する監査報告書等のレポートを利用し、実態の把握に努める等、リスク対策を担保するために実施する内容を記載することが望まれます。

なお、クラウドサービスを利用する場合及びアジャイル型開発を採用する場合の特定個人情報保護評価の実施時期については、Ｑ第６の１－６及びＱ第６の１－７を参照してください。

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

委員会は、上記第５の３（３）アに基づき行政機関等から委員会に提出された全項目評価書を審査し、承認するものとする。

委員会は、基礎項目評価書、重点項目評価書、地方公共団体等から提出された全項目評価書及び任意で提出された全項目評価書の承認は行わないものとする。

（2）審査の観点

委員会は、全項目評価書の承認に際し、適合性及び妥当性の２つの観点から審査を行う。

ア　適合性

この指針に定める実施手続等に適合した特定個人情報保護評価を実施しているか。

・しきい値判断に誤りはないか。
・適切な実施主体が実施しているか。
・公表しない部分は適切な範囲か。
・適切な時期に実施しているか。
・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。
・特定個人情報保護評価の対象となる事務の実態に基づき、特定個人情報保護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。　等

イ　妥当性

特定個人情報保護評価の内容は、この指針に定める特定個人情報保護評価の目的等に照らし妥当と認められるか。

・記載された特定個人情報保護評価の実施を担当する部署は、特定個人情報保護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。
・特定個人情報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。
・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、特定個人情報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。
・特定されたリスクを軽減するために講ずべき措置についての記載

は具体的か。
・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特定個人情報保護評価の目的に照らし、妥当なものか。
・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特定個人情報保護評価の目的に照らし、妥当なものか。　等

委員会は、提出された全項目評価書の審査の結果、必要と認めるときは、番号法の規定に基づく指導・助言、勧告・命令等を行い、全項目評価書の再提出その他の是正を求めるものとする。

（解説）

特定個人情報ファイルを取り扱う事務について、しきい値判断の結果、全項目評価を実施するものとされた行政機関等は、当該事務についての全項目評価書を作成し、委員会に提出します。委員会は、提出された全項目評価書を審査し、承認することになります。この審査・承認の対象は、行政機関等がしきい値判断の結果に基づき作成した全項目評価書のみです。基礎項目評価書（行政機関等が全項目評価書と併せて提出する場合を含む。）、重点項目評価書、地方公共団体等から提出された全項目評価書、主体を問わず任意で提出された全項目評価書は審査・承認の対象ではありません。

委員会は、適合性及び妥当性の２つの観点から審査を行います。

適合性とは、指針に定める実施手続等に適合した特定個人情報保護評価を実施しているかについて審査するものです。具体例として、しきい値判断に誤りはないか、適切な実施主体が実施しているか、非公表部分は適切な範囲か等を指針に示していますが、これらに限りません。

妥当性は、特定個人情報保護評価の内容が指針に定める特定個人情報保護評価の目的等に照らし妥当と認められるかについて審査するもので、内容をより実質的に審査するものです。具体例として、特定個人情報保護評価の実施を担当する部署は特定個人情報保護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、特定個人情報保護評価の対象となる事務の内容の記載は具体的か等を指針に示していますが、これらに限りません。

委員会は、必要に応じて評価実施機関の協力を得ながら審査を進めていきます。

Q第10の１－１

委員会は、全項目評価書が提出されてからどの程度の期間で承認することを予定しているのでしょうか。

（Ａ）

○　委員会は、システムの運用開始を延期せざるを得なくなるなどの評価実施機関の実務に不必要な負担を与える事態とならないよう十分配慮し、全項目評価書が提出されてから合理的な期間内に承認することができるよう、評価実施機関の協力を得ながら、審査を進めていきます。

２　承認の対象としない特定個人情報保護評価書の確認

委員会は、評価実施機関から委員会に提出された特定個人情報保護評価書であって上記１による委員会の承認の対象としないものについては、必要に応じて、その内容を精査し、適合性及び妥当性について確認するものとする。

委員会は、提出された特定個人情報保護評価書の精査の結果、必要と認めるときは、番号法の規定に基づく指導・助言、勧告・命令等を行い、特定個人情報保護評価の再実施その他の是正を求めるものとする。

（解説）

承認の対象となる行政機関等が提出した全項目評価書以外の特定個人情報保護評価書について、委員会は、必要に応じて、その内容を精査し、適合性及び妥当性について確認することとしています。

精査・確認の対象となる可能性がある特定個人情報保護評価書は、基礎項目評価書（行政機関等が全項目評価書と併せて提出する場合を含む。）、重点項目評価書、地方公共団体等から提出された全項目評価書及び主体を問わず任意で提出された全項目評価書です。

委員会は、必要に応じて評価実施機関の協力を得ながら精査・確認を進めていきます。

第 11　特定個人情報保護評価書に記載した措置の実施

評価実施機関は、個人のプライバシー等の権利利益に影響を与え得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軽減するための措置として特定個人情報保護評価書に記載した全ての措置を講ずるものとする。

（解説）

特定個人情報保護評価は、評価実施機関が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分析し、そのようなリスクを軽減するための適切な措置を講ずることにより、特定個人情報の漏えい等を未然に防止するとともに、国民・住民の信頼を確保することを目的としていることから、記載した措置を確実に実施することで実効性が確保されるものです。

第 12　特定個人情報保護評価に係る違反に対する措置

１　特定個人情報保護評価の未実施に対する措置

　特定個人情報保護評価を実施するものとされているにもかかわらず実施していない事務については、情報連携を行うことが禁止される（番号法第 21 条第２項第２号、第 28 条第６項）。特定個人情報保護評価を実施するものとされているにもかかわらず実施していない評価実施機関に対して、委員会は、必要に応じて、番号法の規定に基づく指導・助言、勧告・命令等を行い、特定個人情報保護評価の速やかな実施その他の是正を求めるものとする。

２　特定個人情報保護評価書の記載に反する特定個人情報ファイルの取扱いに対する措置

　特定個人情報ファイルの取扱いが特定個人情報保護評価書の記載に反している場合、委員会は、必要に応じて、番号法の規定に基づく指導・助言、勧告・命令等を行い、是正を求めるものとする。

（解説）

特定個人情報保護評価を実施していない場合、特定個人情報ファイルの適正な取扱いの確保のための措置が適切に講じられていないおそれがあります。

したがって、このような場合に、情報連携を行わせると、不適切な形で特定個人情報ファイルがネットワークを通じてやりとりされることとなり、適正な取扱いがなされている他の事務やシステム（他の情報提供者又は情報照会者のシステムや情報提供ネットワークシステム等）にまで悪影響を及ぼすおそれがあることから、情報連携を行うことが禁止されています（番号法第 21 条第 2 項第 2 号、第 28 条第 6 項）。

情報連携を行わないこととされている機関については、番号法の規定に基づき委員会が指導・助言、勧告・命令等を行い、是正を求めることになります。

また、特定個人情報ファイルの取扱いの実態が特定個人情報保護評価の記載に反していたときは、上記の観点から、番号法の規定に基づき委員会が指導・助言、勧告・命令等を行い、是正を求めることになります。

別表

（第６の２（２）関係）

特定個人情報保護評価書の名称	重要な変更の対象である記載項目
１　重点項目評価書	１　個人番号の利用 ２　情報提供ネットワークシステムによる情報連携 ３　特定個人情報ファイルの種類 ４　特定個人情報ファイルの対象となる本人の範囲 ５　特定個人情報ファイルに記録される主な項目 ６　特定個人情報の入手元 ７　特定個人情報の使用目的 ８　特定個人情報ファイルの取扱いの委託の有無 ９　特定個人情報ファイルの取扱いの再委託の有無 10　特定個人情報の保管場所 11　リスク対策（重大事故の発生を除く。）
２　全項目評価書	１　特定個人情報ファイルを取り扱う事務の内容 ２　個人番号の利用 ３　情報提供ネットワークシステムによる情報連携 ４　特定個人情報ファイルの種類 ５　特定個人情報ファイルの対象となる本人の範囲 ６　特定個人情報ファイルに記録される主な項目 ７　特定個人情報の入手元 ８　特定個人情報の使用目的 ９　特定個人情報の使用部署 10　特定個人情報の使用方法 11　特定個人情報の突合 12　特定個人情報の統計分析 13　特定個人情報の使用による個人の権利利益に影響を与え得る決定 14　特定個人情報ファイルの取扱いの委託の有無 15　取扱いを委託する特定個人情報ファイルの対象となる本人の範囲 16　特定個人情報ファイルの取扱いの再委託の有無 17　特定個人情報の保管場所 18　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（重大事故の発生を除く。） 19　その他のリスク対策

（解説）

この別表は、重点項目評価書及び全項目評価書の記載項目のうち、原則として変更する前に特定個人情報保護評価を再実施することが求められる「重要な変更」の対象であるものを列記しています。様式３及び４を併せて確認してください。

Ｑ別表－１

「重要な変更」の対象である評価項目のリスク対策から、重大事故の発生を除いているのはどのような理由なのでしょうか。

（Ａ）

○　重大事故の発生を事前に知ることは不可能であり、原則として特定個人情報保護評価を事前に再実施することが求められる「重要な変更」には該当しません。

○　ただし、重大事故の発生を受けて、評価実施機関がシステムの全面的な入替えや大幅な組織改組といった大規模なリスク対策の変更を実施する場合は、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になることもあると考えられます。

その他　指針に記載されていない事項

Ｑ他－１

政府統一基準群、ISMS 適合評価制度、IT セキュリティ評価及び認証制度（JISEC）などの認定を受けている評価実施機関は、特定個人情報保護評価を実施する必要があるのでしょうか。

（Ａ）

○　情報セキュリティ対策は、情報資産の CIA(Confidentiality　機密性、Integrity 完全性、Availability　可用性)の維持を図ることを目的としています。これに対し、特定個人情報保護評価の目的は個人のプライバシー等の権利利益の保護であり、セキュリティ対策は１つの手段にすぎないと考えられます。したがって、これらの認定等を受けている評価実施機関についても、特定個人情報保護評価を実施する必要があります。

○　ただし、これらの制度の認定を受けていることは、特定個人情報に係るリスクを軽減するための適切な措置の１つであると考えられることから、既にこれらの制度の認定を受けている評価実施機関については、その旨を特定個人情報保護評価書に記載することが考えられます。