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）

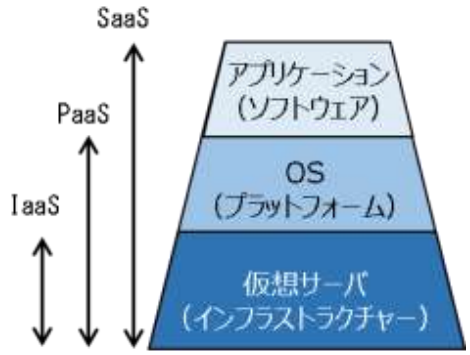
【クラウドサービスの種類に対応したリスク識別、リスク評価、リスク対策の検討】

○　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。

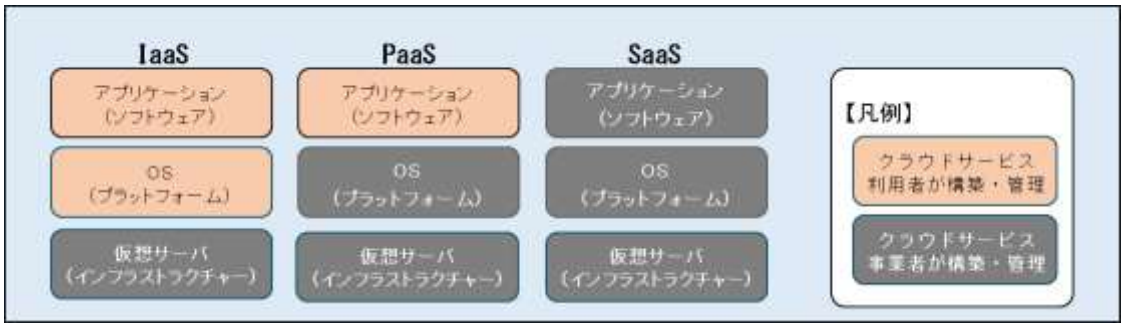
システムの階層を３層で捉えた場合、１段目までクラウドサービス事業者に任せ

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、サーバー等）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ー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。

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。

（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２（１）－１

基礎項目評価書中「Ⅳ　リスク対策」において記載する特定個人情報ファイルに記録された特定個人情報を保護するための主な措置の実施状況の評価について、どのような措置が実施されていれば、「十分である」等を選択することができますか。

（Ａ）

○　講ずべきリスク対策は、事務やサービスの性質、システムの設計等によっても異

なることから、講ずべき措置（リスク対策）を一律に示すことはできませんが、基礎項目評価において評価実施機関が自らの措置の実施状況を評価する際に参考となる一定の基準を示す観点から、次のとおり「典型的リスク対策（例）」をお示しします。ただし、「典型的なリスク対策（例）」は、あくまでも例示であり、１つでも実施していない対策があれば、「十分である」を選択できないというものではありません。

○　また、「特に力を入れている」を選択できる水準は、「十分である」を選択できる水準を満たした上で、さらに、評価実施機関独自の取組を実施している場合、選択することができるものと考えてください。

○　なお、組織的安全管理措置、人的安全管理措置については記載していませんが、マイナンバーガイドラインに則り、必要な措置※1、※2を講じる必要がありますので、留意してください。

※１　組織的安全管理措置：組織体制の整備、取扱規程等に基づく運用、取扱状況を確認する手段の整備、漏えい等事案に対応する体制等の整備、取扱状況の把握及び安全管理措置の見直し

※２　人的安全管理措置：事務取扱担当者の監督、事務取扱担当者等の教育、法令・内部規程違反等に対する厳正な対処

○　また、次に列記する安全管理措置等を遵守することも前提となりますので、留意してください。

・　行政機関等･･･①番号法、②個人情報保護法等関係法令、③個人情報保護法ガイドライン、④事務対応ガイド、⑤政府機関の情報セキュリティ対策のための統一基準等に準拠した各府省庁等における情報セキュリティポリシー、⑥情報提供ネットワークシステム等の接続規程、⑦マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドライン、等が示す安全管理措置等

・　地方公共団体･･･上記に加え、⑧地方公共団体における情報セキュリティポリシーに関するガイドライン等を参考に地方公共団体において策定した情報セキュリティポリシー等

リスク	「十分である」を選択できる水準
目的外の入手が行われるリスクへの対策は十分か【情報提供 NWS 以外】	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 ＜典型的リスク対策（例）＞ ①　対象者、必要な情報の種類、入手方法等を踏まえ、“対象者以外の情報”や“必要な情報”以外の入手を防止するための措置を、システム面、人手による作業の面から講じている。

目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスクへの対策は十分か	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 ＜典型的リスク対策（例）＞ ① 宛名システムやその他の業務システムにおいて、記録されている特定個人情報のうち業務上必要のない特定個人情報に、各業務担当者がアクセスできないようにアクセス制御を行う。
権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスクへの対策は十分か	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 ＜典型的リスク対策（例）＞ ※ リスク対策の詳細については、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編／事業者編）（平成 26 年特定個人情報保護委員会告示第６号／平成 26 年特定個人情報保護委員会告示第５号）」の「Ｅ　物理的安全管理措置」、「Ｆ　技術的安全管理措置」等を参照。 ① ユーザ認証の管理を行っている。 ② アクセス権限の発効・失効の管理を行っている。 ③ アクセス権限の管理を行っている。 ④ 特定個人情報の使用の記録、分析（改ざん等の防止に係る対策を含む。）を行っている。
委託先における不正な使用等のリスクへの対策は十分か	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 ＜典型的リスク対策（例）＞ ※ リスク対策の詳細については、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編／事業者編）（平成 26 年特定個人情報保護委員会告示第６号／平成 26 年特定個人情報保護委員会告示第５号）」の「第４－２－（１）委託の取扱い」等を参照。 ① 委託先における情報保護管理体制の確認を行っている。 ② 委託先における特定個人情報ファイルの閲覧者・更新者を制限している。 ③ 委託先における特定個人情報ファイルの取扱いの記録を行っている。

	④　委託先から他者への又は委託元から委託先への特定個人情報の提供に関するルールを定めている。 ⑤　委託先における特定個人情報の消去に関するルールを定めている。 ⑥　委託契約において、特定個人情報ファイルの取扱いに関する規定を設けている。 ⑦　再委託が行われる場合、再委託先による特定個人情報ファイルの適切な取扱いを確保するための措置を講じている。
不正な提供・移転が行われるリスクへの対策は十分か	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 ＜典型的リスク対策（例）＞ ※　リスク対策の詳細については、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編／事業者編）（平成 26 年特定個人情報保護委員会告示第６号／平成 26 年特定個人情報保護委員会告示第５号）」の「Ｅ　物理的安全管理措置」、「Ｆ　技術的安全管理措置」等を参照。 ①　特定個人情報の提供・移転に関するルールが定められている。 ②　特定個人情報の提供・移転の記録し、その記録を一定期間保存している。 ③　当該記録を定期に及び随時に分析等するための体制を整備している。 ④　当該記録について、改ざん、窃取又は不正な削除の防止のために必要な措置を講じている。
目的外の入手が行われるリスクへの対策は十分か【情報提供 NWS】	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 ＜典型的リスク対策（例）＞ ①　自庁システム側において、必要最低限の人数、参照範囲となるよう、職員のアクセス権限を設定している。 ②　アクセス権限の所有者は、ＩＤ、パスワード等を適切に管理するとともに、離席時のログアウトを徹底する。
不正な提供が行われるリスクへの対策は十分か【情報提供 NWS】	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 ＜典型的リスク対策（例）＞

	① 自庁システムの副本登録画面について、必要最低限の人数、情報の範囲となるよう、職員のアクセス権限を設定する。 ② アクセス権限の所有者は、ＩＤ、パスワード等を適切に管理するとともに、離席時のログアウトを徹底する。 ③ 副本登録を自動連携により行う場合は、サーバーにアクセス権限等を付与する。 ④ 住民基本台帳事務における支援措置対象者等については自動応答不可フラグを設定する等、必要な対応を行う。 ⑤「マイナンバー利用事務におけるマイナンバー登録事務に係るガイドライン」（令和５年 12 月 18 日デジタル庁）の次の留意事項等を遵守している。 （例） ・ 住基ネット照会によりマイナンバーを取得するのではなく、申請者からマイナンバーの提供を受け、その上で記載されたマイナンバーの真正性確認を行うこと。 ・ 申請者からマイナンバーが得られない場合にのみ行う住基ネット照会は、４情報又は住所を含む３情報による照会を原則とすること。 ・ 複数人での確認や上長による最終確認を行った上でマイナンバーの紐付けを行い、その記録を残すこと。 ・ 更新時には、本人からマイナンバーを取得し、登録されているマイナンバーに誤りがないか、確認すること。
特定個人情報の漏えい・滅失・毀損リスクへの対策は十分か	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 ＜典型的リスク対策（例）＞ ※ リスク対策の詳細については、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編／事業者編）（平成 26 年特定個人情報保護委員会告示第６号／平成 26 年特定個人情報保護委員会告示第５号）」の「Ｅ 物理的安全管理措置」、「Ｆ 技術的安全管理措置」等を参照。 ① 内閣サイバーセキュリティセンター（NISC)による政府機関等のサイバーセキュリティ対策のための統一基準群（「政府機関等のサイバーセキュリティ対策のための統一基準」中「第３部 情報の取扱い」、「第５部 情報システムのライフサイクル」、「第６部 情報システムの構成要素」、「第７部 情報システムのセ

	キュリティ要件」、「第８部　情報システムの利用」等）及びそれに基づく各府省庁ポリシーを遵守している。（評価実施機関が政府機関の場合のみ） ②　地方公共団体においては、地方公共団体における情報セキュリティポリシーに関するガイドライン等を参考に地方公共団体において策定した情報セキュリティポリシー等（第３編第２章中「２．情報資産の分類と管理」、「３．情報システム全体の強靭性の向上」、「４．物理的セキュリティ」、「６．技術的セキュリティ」等）を遵守している。 ③　漏えい・滅失・毀損を防ぐために、物理的安全管理措置や技術的安全管理措置を実施している。 ④　特定個人情報ファイルの滅失・毀損が発生した場合に復旧できるよう、バックアップを保管している。 ⑤　過去の漏えい等事案を踏まえた、再発防止策を実施している。
人為的ミスが発生するリスクへの対策は十分か	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 ＜典型的リスク対策（例）＞ ①　「マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドライン」（令和５年 12 月 18 日デジタル庁）の次の留意事項等を遵守している。 （例） ・　住基ネット照会によりマイナンバーを取得するのではなく、申請者からマイナンバーの提供を受け、その上で記載されたマイナンバーの真正性確認を行うこと。 ・　申請者からマイナンバーが得られない場合にのみ行う住基ネット照会は、４情報又は住所を含む３情報による照会を原則とすること。 ・　複数人での確認や上長による最終確認を行った上でマイナンバーの紐付けを行い、その記録を残すこと。 ・　更新時には、本人からマイナンバーを取得し、登録されているマイナンバーに誤りがないか、確認すること。 ②　特定個人情報の入手から保管・廃棄までのプロセスで、人手が介在する局面ごとに人為的ミスが発生するリスクへの対策を講じている。

	※　人為的ミス発生防止の着眼点等として、次の資料が参考となる（いずれも個人情報保護委員会ウェブページ公表資料：https://www.ppc.go.jp/legal/kensyuushiryou/）。 ・「特定個人情報を取り扱う際の注意ポイント」 ・「特定個人情報の漏えい等の防止について－地方公共団体における単純な事務ミスを防止するための着眼点－」
従業者に対する教育・啓発	**次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合** **＜典型的リスク対策（例）＞** ※　リスク対策の詳細については、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編／事業者編）（平成 26 年特定個人情報保護委員会告示第６号／平成 26 年特定個人情報保護委員会告示第５号）」の「Ｄ　人的安全管理措置」等を参照。 **①　研修計画を策定している。** **②　事務取扱者の適切な監督を行っている。** **③　次の事務取扱者等への教育研修を行っている。** **・　事務取扱者への研修** **・　特定個人情報を取り扱う情報システムの管理に関する事務に従事する職員への研修** **・　保護責任者への研修** **・　事務取扱者へのサイバーセキュリティ研修（おおむね１年ごと）。** **※　未受講者には、再受講の機会を付与する等の必要な措置を講じること。**

Ｑ第９の２（１）－２

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

（Ａ）

○　Ｑ第９の２（１）－１に示す「Ⅳ　リスク対策」において「十分である」を選択できる水準（典型的リスク策（例））に記載の措置の内容を参考に、「課題が残されている」、「十分である」、「特に力を入れている」等の各選択肢を選択した理由を記

載してください。

○　なお、分量や記載内容について参考となるよう、各項目について次のとおり記載例をお示ししますので、こちらも参考としてください。

◆　目的外の入手が行われるリスクへの対策は十分か【情報提供ＮＷＳ以外】

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

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

◆　目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスクへの対策は十分か

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

◆　権限のない者（元職員、アクセス権限のない職員等）によって不正に利用されるリスクへの対策は十分か

［例］●●システムへのアクセスが可能な職員は、ICカードとパスワードによる認証によって限

定しており、アクセス可能な職員の名簿を年度ごとに作成することで、アクセス権限の適切な管理を行っている。また、アクセスログを記録し、定期的に分析することで不正なアクセスがないことを確認している。これらの対策を講じていることから、権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスクへの対策は「十分である」と考えられる。

◆　委託先における不正な使用等のリスクへの対策は十分か

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

- 組織体制の整備、漏えい等事案に対応する体制の整備及び安全管理措置の定期的見直しを行うこと。
- 事務取扱担当者の監督・教育を行うこと。
- 特定個人情報を取り扱う事務に従事する作業従事者を明確化するとともに、アクセス制御、アクセス者の識別と認証、外部からの不正アクセス等の防止、漏えい等の防止を行うこと。
- 取扱規程（委託先から他者への又は委託元から委託先への特定個人情報の提供のルール及び特定個人情報の消去のルールを含む）等を策定し、これに基づく運用を行うこと。
- 委託する業務の遂行に必要な範囲を超える事業所からの特定個人情報の持ち出しは禁止とすること。
- 特定個人情報ファイルの取扱状況を記録し、定期的に分析・報告すること。
- 再委託については原則として禁止し、やむを得ず再委託をする必要がある場合は、委託元の承認を得ること。
- 委託元が求めた場合、契約内容の遵守状況を報告すること。
- 必要がある場合、委託元による委託先への実地の監査、調査等を行うこと。

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

◆　不正な提供・移転が行われるリスクへの対策は十分か【情報提供ＮＷＳ以外】

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

- 特定個人情報ファイルの利用・出力状況の記録

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

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

◆　目的外の入手が行われるリスクへの対策は十分か【情報提供ＮＷＳ】

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

◆　不正な提供が行われるリスクへの対策は十分か【情報提供ＮＷＳ】

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

また、マイナンバー登録事務は、「マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドライン」の留意事項を遵守している。

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

◆　特定個人情報の漏えい・滅失・毀損リスクへの対策は十分か

［例］●市××情報セキュリティ規程及び特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）に則り、漏えい・滅失・毀損を防ぐための物理的安全管理措置、技術的安全管理措置等を講じるとともに、特定個人情報ファイルの滅失・毀損が万が一発生した場合に備え、バックアップを保管している。

また、過去の滅失事案（書棚の整理の際に、職員から提出された特定個人情報が記

録された申請書等を綴った文書ファイルの紛失が発覚した事案。年度末の不要文書の廃棄作業の際に、誤廃棄したと思われる。）を踏まえ、

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

を徹底する運用としている。

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

◆ 人為的ミスが発生するリスクへの対策は十分か

[例①]マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドラインに従い、マイナンバー登録や副本登録の際には、本人からのマイナンバー取得の徹底や、住基ネット照会を行う際には４情報又は住所を含む３情報による照会を行うことを厳守している。また、●●事務では、上記のほか、下記の局面で特定個人情報の取扱いに関して手作業が介在するが、いずれの局面においても複数人での確認を行うようにしており、人為的ミスが発生するリスクへの対策は十分であると考えられる。

- 申請書に記載された個人番号及び本人情報のデータベースへの入力
- 特定個人情報の記載がある申請書等（USB メモリを含む。）の保管
- 個人番号及び本人情報が記載された申請書の廃棄

等

[例②]マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドラインに従い、マイナンバー登録や副本登録の際には、本人からのマイナンバー取得の徹底や、住基ネット照会を行う際には４情報又は住所を含む３情報による照会を行うことを厳守している。また、必ず複数人での確認を行った上で●●（上長）の最終確認を経ることとしている。

また、人手が介在する局面ごとに、人為的ミスが発生するリスクに対し、例えば次のような対策を講じている。

- 人為的ミスを防止する対策を盛り込んだ事務処理手順をマニュアル化し、事務取扱担当者間で共有する。

・　特定個人情報を受け渡す際（USB メモリを使用する場合を含む。）は、事前に、暗号化、パスワードによる保護、確実なマスキング処理等を行うとともに、これらの対策を確実に実施したことの確認を複数人で行う。
・　マイナンバー入りの書類を郵送等する際は、宛先に間違いがないか、関係のない者の特定個人情報が含まれていないかなど、ダブルチェックを行う。
・　特定個人情報を含む書類や USB メモリは、施錠できる書棚等に保管することを徹底する。
・　廃棄書類に特定個人情報が含まれていないか、ダブルチェックを行う。

これらの対策を講じていることから、人為的ミスが発生するリスクへの対策は「十分である」と考えられる。

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

◆　従業者に対する教育・啓発

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

Q第９の２（１）－３
基礎項目評価書中「Ⅳ　リスク対策」の「11. 最も優先度が高いと考えられる対策」について、選択肢全てが同列で重要度が高いと考えられる場合は、どうすれば良いですか。

（A）

○　評価を選択した「判断根拠」については、自由記述式で記載を求めることとしており、評価実施機関の事務負担に鑑み、「Ⅳ　リスク対策」に記載の対策の中から最も優先度が高いと考えられる対策を一つ選び、記載することができることとしております。事務のプロセスや事務に使用する情報システムの仕様等に加え、これま

で発生した個人情報に関する重大事故の内容等を踏まえ、該当するものを選択してください。

○　なお、評価実施機関の判断で、①別添資料（様式任意）として複数の項目についての判断根拠を記載し提出・公表することや、②（しきい値判断の結果、基礎項目評価のみで足りると認められた事務についても）任意で重点項目評価又は全項目評価を実施することも可能です（第５の２、Ｑ第５の２－４．－１を参照）。

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 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 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など、重要な変更の対象となる記載項目の内容に変更が生じる場合には、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。

Ｑ別表－２

委託先の追加は「重要な変更」に該当するのでしょうか。

（Ａ）

○　既に特定個人情報保護評価を実施している事務について、新たに特定個人情報の取扱いに関する委託事項を追加する場合、重要な変更の対象項目である「委託件数」の欄に変更が生じ、また、新たに追加する特定個人情報の取扱いの委託の内容によっては、リスク対策に変更が生じることが考えられるため、原則としては重要な変更に該当するものと考えられます。

○　また、委託件数に変更が生じた場合や既に委託している内容に変更が生ずる場合は、単に「委託事項」の記載を追記するだけでなく、その新たな委託事項や変更後におけるプロセスやリスク対策によっては、重要な変更に該当する記載項目である「Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策」等への追記や変更が必要となることも想定されます。

○　ただし、例えば、追加する委託事項の内容、委託の相手方が既存の委託事項と同一であり、既存の特定個人情報の取扱いの委託と事務のプロセス及びリスク対策に変更が生じない場合などは「リスクを相当程度変動させるものではないと考えられる変更」に該当し、重要な変更に該当しない可能性も考えられますので、新たに追

加される委託事項に伴う特定個人情報ファイルを取り扱うプロセス及び当該プロセスに係るリスク対策の実態も踏まえ、適切に判断してください。

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。

Ｑ他－２

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

（Ａ）

○　地方公共団体情報システムの標準化に関する法律（令和３年法律第 40 号。以下「標準化法」という。）では、政令で定める地方公共団体の情報システムの標準化の対象となる事務（以下「標準化対象事務」という。）について、地方公共団体が標準化基準に適合したシステム（以下「標準準拠システム」という。）を利用することを義務付けるとともに、地方公共団体にガバメントクラウドを活用して標準準拠システムを利用することを努力義務として課しています。

○　標準化対象事務のうち、特定個人情報保護評価の対象となる事務は、次の事務です（「＊」の付されている事務は、個人番号の利用又は情報連携が認められていない事務であり、番号法第９条第２項に基づく条例を定めて個人番号を利用している場合を除いて、特定個人情報保護評価の実施義務はありません。）。

※　令和６年５月 27 日時点の情報。

①児童手当	**⑬健康管理**

・児童手当又は特例給付の支給に関する事務

②子ども・子育て支援

・子どものための教育・保育給付若しくは子育てのための施設等利用給付の支給、特定教育・保育施設、特定地域型保育事業者若しくは特定子ども・子育て支援施設等の確認又は地域子ども・子育て支援事業の実施に関する事務

③住民基本台帳

・住民基本台帳に関する事務

・中長期在留者の住居地の届出又は外国人住民に係る住民票の記載等についての通知に関する事務

・特別永住者の住居地の届出に関する事務

・個人番号の指定に関する事務

・住居表示に係る事項の通知に関する事務（＊）

④戸籍の附票（＊）

・戸籍の附票に関する事務（＊）

⑤印鑑登録（＊）

・印鑑に関する証明書の交付に関する事務（＊）

⑥選挙人名簿管理（＊）

・選挙人名簿又は在外選挙人名簿に関する事務（＊）

・投票人名簿又は在外投票人名簿に関する事務（＊）

⑦⑧⑨⑩　地方税

・個人の道府県民税（都民税を含む。）若しくは市町村民税（特別区民税を含む。）、法人の市町村民税、固定資産税、軽自動車税、都市計画税又は森林環境税の賦課徴収に関する事務（固

・健康教育、健康相談その他の国民の健康の増進を図るための措置に関する事務

・母性並びに乳児及び幼児に対する保健指導、健康診査、医療その他の措置に関する事務

・予防接種の実施に関する事務

⑭児童扶養手当

・児童扶養手当の支給に関する事務

⑮生活保護

・生活保護の決定及び実施、就学自立給付金若しくは進学・就学準備給付金の支給又は被保護者就労支援事業若しくは被保護者健康管理支援事業の実施に関する事務

⑯障害者福祉

・障害児通所給付費、特例障害児通所給付費、高額障害児通所給付費、肢体不自由児通所医療費、障害児相談支援給付費、特例障害児相談支援給付費、特別児童扶養手当、障害児福祉手当若しくは特別障害者手当の支給、障害者手帳若しくは精神障害者保険福祉手帳の交付、知的障害者の判定等に関する事務

・特別児童扶養手当、障害児福祉手当又は特別障害者手当の支給に関する事務

・福祉手当の支給に関する事務

・自立支援給付の支給に関する事務

⑰介護保険

・介護保険に関する事務

（※　介護保険法施行法第11条に基づく事務については保護評価対象外。）

⑱国民健康保険

・被保険者の資格の取得若しくは喪失、

定資産課税台帳の登録事項等の通知に関する事務） **⑪戸籍**（＊） ・戸籍に関する事務（＊） **⑫就学**（＊） ・就学義務の猶予若しくは免除又は就学困難と認められる学齢児童又は学齢生徒の保護者に対する実用的な援助に関する事務（＊） ・学齢簿に関する事務（＊） ・就学時の健康診断に関する事務（＊）	保険給付の実施又は保険料の賦課及び徴収に関する事務 **⑲後期高齢者医療** ・被保険者の資格の取得若しくは喪失又は保険料の徴収に関する事務 **⑳国民年金** ・被保険者の資格の取得若しくは喪失、年金である給付若しくは一時金の支給、賦課保険料の納付又は保険料の免除、特別障害給付金、年金生活者支援給付金の支給に関する事務

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

＜基礎項目評価書について＞

○　基礎項目評価書の記載項目には、重点項目評価書や全項目評価書にあるような、特定個人情報ファイルを取り扱うシステムの詳細や、特定個人情報の種類・入手方法・提供方法の詳細等について記載する項目はないものの、標準準拠システムへの移行に当たって生じる変更（特定個人情報の保管場所等）を踏まえてリスク対策を見直した結果、当該リスク対策の実施状況の評価（「Ⅳリスク対策」における自己評価やその根拠）を修正する必要が生じることが考えられます。

＊　なお、上記見直しと併せて、次の２点についても、対応が必要となりますので、御留意ください（重点・全項目評価書と併せて提出する基礎項目評価書についても同様です）。

・　Q第９の２（１）－１において、「Ⅳ　リスク対策」における自己評価の基準を示しておりますので（令和６年４月１日最終改正版から追加）、この基準に照らして自己評価の見直しを行ってください。

・　令和６年 10 月１日から施行される新様式を用いた基礎項目評価書（「Ⅳ　リスク対策」に「人手を介在させる作業」、「最も優先度が高いと考えられる対策」が追加されました）について、全ての評価実施機関が令和７年度末までに再提出する必要があります。

＜重点・全項目評価書について＞

○　標準準拠システムの移行に伴って特定個人情報に関する機能の改修等を行う場合は、特定個人情報保護評価の再実施（又は修正）が必要です。現行システムから

標準準拠システムへの移行に当たっては、システムを全面的に入れ替えるケースや、事務手続を大きく変更するケースも考えられるため、重点項目評価書や全項目評価書については、原則として修正ではなく再実施が必要となるものと考えられます。

○　特に、標準準拠システムの利用において、ガバメントクラウドへの移行を行う業務システムについては、特定個人情報保護評価を再実施する必要があります。これは、ガバメントクラウドへの移行においては、委託先の事業者に変更がない場合であっても、

・　サーバー等が、クラウド事業者が保有・管理する環境に設置されることとなり、特定個人情報の保管場所に変更が生じる（物理的・技術的な対策について、クラウド事業者が実施することとなる）

・　従来、職員が業務で利用していたパソコン等の操作端末からクラウドサービスに存在するシステムへ、接続する通信経路やアクセス制御等に変更が生じる

・　既存のシステム環境から特定個人情報ファイルを抽出し、新システムへデータを移し替える作業が発生する

・　既存のシステム環境に保管されていた特定個人情報の消去、機器の廃棄を実施する

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

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

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

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

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

・　ガバメントクラウドへの移行に係る内容について：
ガバメントクラウドへ副本データを移行するまで

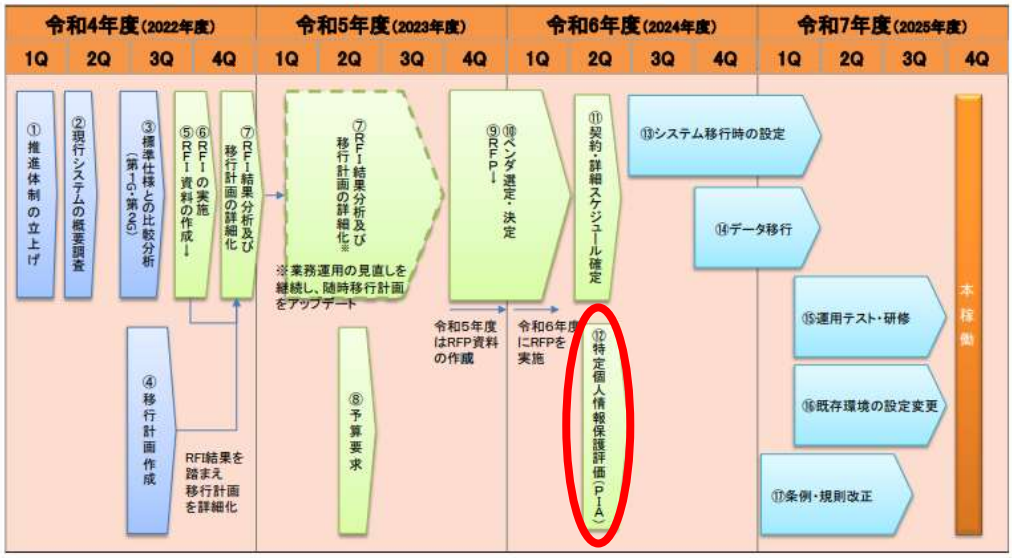
・　標準準拠システムへの移行について（後述のモデルスケジュール例も参照）：システム等を稼働させるサーバー等へのパラメータ設定等の適用を実施する前まで（パラメータ設定等の適用が行われることにより、サーバー等に直接的に変更を加えることになるため、これをプログラミングに相当するものとして考えることとしています。）

＜標準化モデルスケジュール例※1＞

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

図表 14　令和４年度から移行準備を行う場合のスケジュール例

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



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

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

＜標準準拠システムへの移行に伴う影響（例※2）＞

標準化等に伴い生じる取扱いの変更	基礎項目評価書上影響する箇所	全項目評価書上影響する箇所
事務で利用する情報システムの変更	・システムの名称	・システムの名称、機能、他のシステムとの接続

標準準拠システムへの移行（標準仕様に基づく業務運用見直し）に伴う事務のプロセスの変更	・事務の概要	・事務の内容（Ⅰ１） ・本特定個人情報のファイルの本人の範囲、記録される項目（Ⅱ２）
委託先・委託内容の変更	・委託先における不正な使用等のリスク対策	・特定個人情報ファイルの取扱いの委託（Ⅱ４、Ⅲ４）
システム更改に伴う特定個人情報へのアクセス制限範囲の変更	・目的外の入手が行われるリスク対策、目的を超えた紐付け ・事務に必要のない情報との紐付けが行われるリスクへの対策 ・権限のない者によって不正に使用されるリスクへの対策	・特定個人情報の入手（Ⅲ３） ・特定個人情報の使用（Ⅲ３）
特定個人情報の提供・移転（記録）の方法の変更	・不正な提供・移転が行われるリスクへの対策	・特定個人情報の提供・移転（Ⅲ５）
特定個人情報を取り扱う環境（データの保管場所を含む）の変更（オンプレミス環境からガバメントクラウドへの移行など）	・特定個人情報の漏えい・滅失・毀損リスクへの対策	・特定個人情報の保管・消去（Ⅱ６、Ⅲ７）

※２　上記の記載は、標準準拠システムの移行に当たって生じることが想定される一般的な変更の例であり、全ての変更が網羅されているものではありません。現行のシステムや標準準拠システムの仕様によって、上記以外の変更が生じることも考えられ、その場合、当該変更に応じたリスク対策を検討する必要があります。