資料１－２

特定個人情報保護評価書の特定個人情報保護評価指針への適合性・妥当性の審査

評価書名
公的給付支給等口座登録簿への登録等に関する事務　全項目評価書

評価実施機関名
内閣総理大臣

提出日
令和3年10月19日

概要説明日
令和3年10月20日

（目次）

全体的な事項

※ 評価実施手続に関する事項及び特定個人情報ファイルに共通する事項

審査の観点（指針第10(2)）	主な考慮事項	主な考慮事項(細目)	該当箇所		審査結果	所見
(1)しきい値判断に誤りはないか。	—	—	—	—	問題は認められない	対象人数が30万人以上に該当するため、全項目評価を実施することは、指針に適合している。
(2)適切な実施主体が実施しているか。	—	1. 評価実施機関が複数存在し、取りまとめの評価実施機関が評価書を作成・提出する場合に、取りまとめ以外の全ての評価実施機関について記載しているか。	—	—	問題は認められない	特定個人情報ファイルは、内閣総理大臣が公的給付支給等口座登録簿への登録等に関する事務において保有するものであることから、実施主体は適切である。
(3)公表しない部分は適切な範囲か。	—	—	—	—	問題は認められない	評価書の内容は全て公表することとしている。
(4)適切な時期に実施しているか。	—	—	—	—	問題は認められない	特定個人情報ファイルを取り扱う口座情報登録システムの開発前の適切な時期に評価を実施している。
(5)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。	—	—	—	—	問題は認められない	国民への意見募集については、e-Gov（電子政府の総合窓口）において、32日間実施したほか、意見への対応状況をe-Govで公表することとしており、事後の措置も適切である。
(6)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。	—	—	—	—	問題は認められない	公的給付支給等口座登録簿への登録等に関する事務について、求められる事項が具体的に記載されている。

審査の観点（指針第10(2)）	主な考慮事項	主な考慮事項(細目)	該当箇所		審査結果	所見
(7)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。	―	―	―	―	問題は認められない	公的給付支給等口座登録簿への登録等に関する事務における番号制度への対応は、デジタル庁　デジタル社会共通機能グループが行っており、特定個人情報保護評価の対象となる事務の実施に当たって、リスクを軽減させるための措置の実施等については、責任を負うことができる部署である。
(8)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。	①特定個人情報ファイルを取り扱う事務やその事務において使用するシステムについて、基本情報を具体的に分かりやすく記載しているか。	2. 評価対象の事務全体の概要及びその中で特定個人情報ファイルを使用して実施する事務の内容を具体的に記載しているか。	P.3 ～ P.4	Ⅰ 1. ②	問題は認められない	公的給付支給等口座登録簿への登録等に関する事務において、それぞれ特定個人情報ファイルを使用することが事務の流れに即し具体的に記載されている。 また、別添1の事務の内容において、事務に関わる者、事務において使用するシステム、事務において取り扱う情報の流れが具体的に記載されているほか、国民にとって給付金に係る申請手続の簡素化・給付の迅速化等、実現が期待されるメリット等についても具体的に記載されている。
		3. 当該システムが実現する機能の名称とその概要を具体的に記載しているか。	P.5 ～ P.7	Ⅰ 2. ②	問題は認められない	
		4. 当該システムと情報をやり取りするシステムを全て記載しているか。	P.5 ～ P.7	Ⅰ 2. ③	問題は認められない	
		5. 特定個人情報ファイルを取り扱うことが評価対象の事務を実施する上で必要であることを、事務の流れに即して具体的に説明しているか。	P.8	Ⅰ 4. ①	問題は認められない	
		6. 評価対象の事務において特定個人情報ファイルを取り扱うことにより、期待されるメリットについて幅広く具体的に記載しているか。	P.8	Ⅰ 4. ②	問題は認められない	
		7. 事務に関わる者、事務において使用するシステム、事務において取り扱う情報の流れを具体的に記載しているか。	P.9 ～ P.10	Ⅰ (別添1)	問題は認められない	

審査の観点（指針第10(2)）	主な考慮事項	主な考慮事項（細目）	該当箇所		審査結果	所見
(9)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。	―	―	P.22 ～ P.33	Ⅲ、Ⅳ	問題は認められない	全項目評価書に例示されている各リスクにどのように対応しているかが具体的に記載されている。
(10)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。 (11)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。	⑨特定個人情報ファイルの取扱いについて自己点検・監査や従業者に対する教育・啓発を行っているか。	70. 評価書に記載したとおりに運用がなされていること等について、評価の実施を担当する部署自らが、どのように自己点検するか具体的に記載しているか。	P.33	Ⅳ 1. ①	問題は認められない	自己点検・監査について、情報セキュリティポリシー及び運用規則等に基づき、公的給付支給等口座登録簿の運用に携わる職員及び委託先事業者に対し、情報セキュリティ対策を実施しているかどうかについて、定期的に自己点検を実施すること、監査は委託先事業者による口座情報登録システムの運用の履行状況に関するデジタル庁の情報システム責任者等への報告の内容などから、デジタル庁の情報システム責任者等が監査の実施が必要であると判断した際に実施すること等が具体的に記載されている。 従業者に対する教育・啓発について、デジタル庁の情報セキュリティ責任者は、全職員を受講対象とした個人情報保護及び情報セキュリティに関する研修を定期的に職員に受講させ、特定個人情報の事務外での使用の禁止を徹底すること等が具体的に記載されている。
		71. 評価書に記載したとおりに運用がなされていること等について、どのように監査するか具体的に記載しているか。	P.33	Ⅳ1. ②	問題は認められない	
		72. 特定個人情報を取り扱う従業者等に対しての教育・啓発や違反行為をした従業者等に対する措置について具体的に記載しているか。	P.33	Ⅳ 2.	問題は認められない	
		73. 国民・住民等からの意見聴取により得られた意見を踏まえて評価書のどの箇所をどのように修正したかを具体的に記載しているか。	P.35	Ⅵ 2. ⑤	問題は認められない	寄せられた意見への回答として、寄せられた意見全てに対し、デジタル庁としての考え方を一覧形式で取りまとめ、e-Govにおいて公表することとしている。
(12)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。	―	―	P.1	表紙	問題は認められない	口座情報登録システムにおける公的給付支給等口座登録簿への登録等に関する事務における特定個人情報ファイルの取扱いに当たり、同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及ぼすものであることを認識し、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させるために適切な措置を講じることをもって、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宣言している。

特定個人情報ファイル
（公的給付支給等口座登録簿）

審査の観点（指針第10(2)）	主な考慮事項	主な考慮事項（細目）	該当箇所		審査結果	所見
(8)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。	②特定個人情報ファイルの取扱いプロセスの概要(特定個人情報の入手・使用、特定個人情報ファイルの取扱いの委託、特定個人情報の提供・移転、特定個人情報の保管・消去)について、具体的に分かりやすく記載しているか。	8. 対象となる国民・住民の特定個人情報を特定個人情報ファイルにおいて保有することが事務を実施する上で必要な理由を具体的に記載しているか。	P.11	Ⅱ 2. ③	問題は認められない	特定個人情報を保有する理由について、公的給付の支給等に係る金銭の授受に利用することができる一の預貯金口座を登録することにより、公的給付の支給等の迅速かつ確実な実施を行うためであることが具体的に記載されている。 委託先に特定個人情報ファイルを取り扱わせることが必要な理由として、システム全体に係る保守・運用等を適切に実施するためには、専門的かつ高度な知識・技術を要すること等、全体の取扱いを委託することが必要であることが具体的に記載されている。 また、特定個人情報の保管・消去について、特定個人情報は、クラウド上のデータベース内に保存され、バックアップもデータベース上に保存されること、オンプレミス環境と運用保守拠点には特定個人情報は保管されないこと、口座情報等は、口座情報等の抹消申請、口座凍結又は登録者の死亡を契機とし、口座情報登録システムから削除されること等が具体的に記載されている。
		9. 主な記録項目について、保有する理由をそれぞれ具体的に記載しているか。	P.11	Ⅱ 2. ④	問題は認められない	
		10. 特定個人情報の入手に係る妥当性を具体的に記載しているか。	P.12	Ⅱ 3. ④	問題は認められない	
		11. 特定個人情報の入手の事実及び使用目的が本人に示されていることを具体的に記載しているか。	P.12	Ⅱ 3. ⑤	問題は認められない	
		12. 特定個人情報を使用する理由を具体的に記載しているか。	P.12	Ⅱ 3. ⑥	問題は認められない	
		13. 特定個人情報ファイルに記録される情報を他から入手する際の突合の内容、特定個人情報ファイルに記録された情報と他の情報との突合の方法や突合の理由を具体的に記載しているか。	P.12	Ⅱ 3. ⑧	問題は認められない	
		14. 特定個人情報を用いた統計分析を行う場合は、その内容を具体的に記載しているか。	P.12	Ⅱ 3. ⑧	該当なし	
		15. 特定個人情報を使用することにより国民の権利利益に影響を与え得る決定を行う場合は、その内容を具体的に記載しているか。	P.12	Ⅱ 3. ⑧	該当なし	
		16. 委託先に当該特定個人情報ファイルを取り扱わせることが必要な理由を具体的に記載しているか。	P.13	Ⅱ 4. ②	問題は認められない	
		17. 委託先を国民・住民等が確認できるか否か、確認できる場合はどのように確認できるか、確認できない場合はそのような取扱いが評価対象の事務を実施する上で必要な理由を具体的に記載しているか。	P.13	Ⅱ 4. ⑤	問題は認められない	
		18. 特定個人情報ファイルの取扱いを再委託するに当たって、どのような手続・方法によるかを具体的に記載しているか。	P.13	Ⅱ 4. ⑧	問題は認められない	
		19. 提供した特定個人情報が、提供先において、いかなる目的で、どのように使用されることになるかを具体的に記載しているか。	P.14 P.16 ～ P.19	Ⅱ 5. ②	問題は認められない	
		20. 移転した特定個人情報が、移転先において、いかなる目的で、どのように使用されることになるかを具体的に記載しているか。	P.14	Ⅱ 5. ②	該当なし	
		21. 特定個人情報の保管場所の態様及び保管場所への立入り制限・アクセス制限について具体的に記載しているか。	P.15	Ⅱ 6. ①	問題は認められない	
		22. 特定個人情報の保管期間は妥当であるか。また、その理由を具体的に記載しているか。	P.15	Ⅱ 6. ②	問題は認められない	
		23. 保管期間を経過した特定個人情報を消去する方法を具体的に記載しているか。	P.15	Ⅱ 6. ③	問題は認められない	

審査の観点 （指針第10(2)）	主な考慮事項	主な考慮事項（細目）	該当箇所		審査結果	所見
(10)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。 (11)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。	③特定個人情報の入手について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	24. 評価対象の事務を遂行する上で必要な者以外の者の特定個人情報を入手しないよう講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.22	Ⅲ 2. リスク1:	問題は認められない	対象者以外の情報の入手を防止するリスク対策として、国民からの入手の場合、口座登録申請機能による入手は、あらかじめ開示システムにおいて、マイナンバーカード及びパスワード入力による本人確認を了した後に行うため、対象者以外の情報を入手することはないこと、行政機関等からの入手の場合、行政機関等は、入手時に本人確認措置を実施し、本人による同意を得た口座情報等が連携されるため、対象者以外の情報を入手することはないこと等が具体的に記載されている。 入手の際の特定個人情報の漏えい・紛失を防止するリスク対策として、国民からの入手の場合、本人からマイナポータル経由で口座情報登録システムへ口座情報等を登録するが、当該通信は、TSL/SSLによる暗号化された通信経路を使用することで漏えい・紛失を防止すること、行政機関等からの入手の場合、専用線を使用し、ファイル内のデータを暗号化して省庁連携機能を通じて口座情報管理システムへ登録されることで、漏えい・紛失することを防止していること等が具体的に記載されている。
		25. 事務を遂行する上で必要な情報以外の特定個人情報を入手しないよう講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.22	Ⅲ 2. リスク1:	問題は認められない	
		26. 特定個人情報の入手に際して、適切な方法で入手するために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.22	Ⅲ 2. リスク2:	問題は認められない	
		27. 特定個人情報を入手する際に、その特定個人情報が本人の情報であることを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.22	Ⅲ 2. リスク3:	問題は認められない	
		28. 入手した個人番号が本人の個人番号で間違いないことを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.23	Ⅲ 2. リスク3:	問題は認められない	
		29. 特定個人情報を入手した後、その情報の正確性を保つために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.23	Ⅲ 2. リスク3:	問題は認められない	
		30. 特定個人情報を入手する際に、情報の安全確保の観点から講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.23	Ⅲ 2. リスク4:	問題は認められない	
		31. 特定個人情報の入手において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.23	Ⅲ 2. その他のリスク	該当なし	

審査の観点 （指針第10（2））	主な考慮事項	主な考慮事項（細目）	該当箇所		審査結果	所見
	④特定個人情報の使用について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	32. 宛名システム等において、特定個人情報が、使用目的を超えて取り扱われないよう、また、評価対象の事務に必要のない情報と併せて取り扱われないよう、講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.24	Ⅲ 3. リスク1：	問題は認められない	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対策として、デジタル庁が他の事務で使用する開示システム等と口座情報登録システムにおいては、デジタル庁が定めたインターフェース仕様に沿って、決められたデータ項目のみ提供し、開示システム内の情報と個人番号が紐付かないようにシステム的に制御していること等が具体的に記載されている。 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク対策として、デジタル庁の情報システム責任者等の委任を受けた委託先事業者の運用統括責任者が従事者にID及びハードウエアトークンを払い出し、その者の役割に応じたアクセス権限を持つユーザアカウントと紐づけること、従事者のユーザアカウントの認証方式については、ID・パスワード及びハードウエアトークン等を使用した二要素認証を用いること、デジタル庁の情報システム責任者等は、運用統括責任者からユーザアカウントの割当て状況、委託先事業者による口座情報登録システムへのログイン状況などに係る報告書の内容を随時確認すること、必要に応じて口座情報登録システムの運用拠点への立入り検査を実施すること、運用統括責任者は、口座情報登録システムへのアクセスログ、口座情報登録システムでの操作ログの記録を行うとともに、定期的にログの分析を実施すること、また、これらのログの改ざんや滅失を防止するため、不正プロセス検知ソフトウェアにより不正なログの書き込み等を検知すること等が具体的に記載されている。
		33. 事務で使用するその他のシステムにおいて、特定個人情報が、使用目的を超えて取り扱われないよう、また、評価対象の事務に必要のない情報と併せて取り扱われないよう、講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.24	Ⅲ 3. リスク1：	問題は認められない	
		34. 特定個人情報にアクセスする際の認証を行う場合は、特定個人情報にアクセスするユーザの認証方法、なりすましが行われないために講じている対策について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.24	Ⅲ 3. リスク2：	問題は認められない	
		35. 特定個人情報ファイルを取り扱う者が正当なユーザであることを確認するための情報の発効・失効の管理について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.25	Ⅲ 3. リスク2：	問題は認められない	
		36. アクセス権限の発効・失効の管理を行う者による当該管理の適正性についてチェックをしている内容を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.25	Ⅲ 3. リスク2：	問題は認められない	
		37. 特定個人情報の入手から消去までの各過程において、特定個人情報ファイルの取扱い記録やアクセスの失敗の記録等を残していることを具体的に記載しているか。記録を残していない場合は、残していなくても権限のない者による不正な使用を防止できる理由を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.25	Ⅲ 3. リスク2：	問題は認められない	
		38. 従業者が特定個人情報ファイルを事務外で使用しないよう講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.26	Ⅲ 3. リスク3：	問題は認められない	
		39. 特定個人情報ファイルを取り扱う者が特定個人情報ファイルを不正に複製しないよう講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.26	Ⅲ 3. リスク4：	問題は認められない	
		40. 特定個人情報の使用において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.26	Ⅲ 3. その他のリスク	該当なし	

審査の観点 （指針第10(2)）	主な考慮事項	主な考慮事項（細目）	該当箇所		審査結果	所見
	⑤特定個人情報の委託について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	41. 委託先を決定する際に特定個人情報ファイルを適切に取り扱う委託先であることを確認する手続等について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.27	Ⅲ 4. 情報管理体制	問題は認められない	特定個人情報ファイルの取扱いの委託における特定個人情報ファイルの取扱いについて、委託契約書にて具体的にルールを定めているほか、情報セキュリティインシデントの発生時など、委託先事業者が公的給付支給等口座登録簿内の特定個人情報を確認する必要が生じた場合を除き、運用端末から公的給付支給等口座登録簿にアクセスすることを禁止すること、デジタル庁の情報システム責任者等が委託先事業者におけるユーザ認証、アクセス権限の管理や特定個人情報の使用の記録に関する報告書の内容を確認するとともに、報告書等に基づいて運用統括責任者から聴取を行い、必要に応じて立入検査を実施することで、不正な提供がなされていないことを確認すること等が具体的に記載されている。
		42. 委託先において特定個人情報ファイルの閲覧者・更新者を必要最小限に制限していることを具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.27	Ⅲ 4. 閲覧者の制限	問題は認められない	
		43. 委託先における特定個人情報ファイルの取扱いについて記録を残している場合は、その方法や保存期間等を具体的に記載しているか。また、記録を残していない場合は権限のない者による不正な使用を防止できる理由を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.27	Ⅲ 4. 記録	問題は認められない	
		44. 委託に伴う特定個人情報の提供に関するルールを定めている場合、ルールの内容やルール遵守の確認方法を具体的に記載しているか。また、委託先から他者への提供を認めていない場合、提供されていないことを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.27	Ⅲ 4. 提供ルール	問題は認められない	
		45. 委託先における特定個人情報の消去のルールを定めている場合は、ルールの内容やルール遵守の確認方法を具体的に記載しているか。また、委託契約終了後に消去されていることを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.27	Ⅲ 4. 消去ルール	問題は認められない	
		46. 委託先と締結する委託契約における特定個人情報ファイルの取扱いに関する規定について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.28	Ⅲ 4. 委託契約書中の規定	問題は認められない	
		47. 特定個人情報ファイルの取扱いを再委託している場合、再委託先での適正な取扱いの確保のために行っている措置について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.28	Ⅲ 4. 再委託	問題は認められない	
		48. 特定個人情報ファイルの取扱いの委託において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.28	Ⅲ 4. その他のリスク	該当なし	

審査の観点 （指針第10(2)）	主な考慮事項	主な考慮事項（細目）	該当箇所		審査結果	所見
	⑥特定個人情報の提供・移転について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	49. 特定個人情報の提供又は移転の記録を残している場合は、その記録の内容や記録方法、保存期間等を具体的に記載しているか。また、記録を残していない場合は特定個人情報が不正に提供又は移転されることを防止できる理由を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.29	Ⅲ 5. リスク1：	問題は認められない	不正な提供・移転が行われるリスク対策として、特定公的給付の支給を実施する行政機関の長等へ電子記録媒体および省庁連携機能を利用したファイル連携による提供を行う場合は、提供の記録を管理簿等で残すこと、電子記録媒体内及び省庁連携機能を利用して連携するファイル内のデータは暗号化やパスワード設定を行うこと等が具体的に記載されている。 不適切な方法で提供・移転が行われるリスク対策として、省庁連携機能を利用した連携には専用線を使用すること、電子記録媒体は鍵付きの衝撃防止ケースに入れて搬送する等、安全な方法で提供を行うこと等が具体的に記載されている。
		50. 特定個人情報の提供・移転に関するルールを定めている場合は、ルールの内容やルール遵守の確認方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.29	Ⅲ 5. リスク1：	問題は認められない	
		51. 特定個人情報を提供・移転する際に、情報漏えいや紛失のリスクを軽減するための措置や提供先・移転先における特定個人情報の使途が法令に基づく適切なものであることを確認するための措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.29	Ⅲ 5. リスク2：	問題は認められない	
		52. 誤った特定個人情報を提供・移転することや誤った相手に提供・移転することを防止する措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.29	Ⅲ 5. リスク3：	問題は認められない	
		53. 特定個人情報の提供・移転において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.29	Ⅲ 5. その他のリスク	該当なし	

審査の観点（指針第10(2)）	主な考慮事項	主な考慮事項（細目）	該当箇所		審査結果	所見
	⑦情報提供ネットワークシステムとの接続について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	54. 情報提供ネットワークシステムを通じて特定個人情報を入手する際に、目的外の入手が行われないために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.30	Ⅲ 6. リスク1：	該当なし	不適切な方法で提供されるリスクとして、口座情報登録システムに係る中間サーバーの職員認証及び権限管理機能では、ログイン時の職員認証のほかに、ログイン及びログアウトを実施した職員、時刻並びに操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止すること、口座情報登録システムと情報提供ネットワークシステムとの間は、通信の暗号化等の高度なセキュリティを維持した専用線を利用し、不適切な方法で提供されるリスクに対応すること等が具体的に記載されている。
		55. 情報提供ネットワークシステムを通じて特定個人情報を入手する際に、特定個人情報の安全が保たれない不適切な方法で特定個人情報を入手しないために講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.30	Ⅲ 6. リスク2：	該当なし	
		56. 情報提供ネットワークシステムを通じて特定個人情報を入手した後、その情報の正確性を保つために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.30	Ⅲ 6. リスク3：	該当なし	
		57. 情報提供ネットワークシステムを通じて特定個人情報を入手する際に、情報漏えいや紛失のリスクを軽減するために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.30	Ⅲ 6. リスク4：	該当なし	
		58. 情報提供ネットワークシステムを通じて提供する際に、特定個人情報の不正な提供が行われるリスクを軽減するために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.30	Ⅲ 6. リスク5：	問題は認められない	
		59. 情報提供ネットワークシステムを通じて提供する際に、特定個人情報の提供方法が不適切とならないよう講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.30	Ⅲ 6. リスク6：	問題は認められない	
		60. 情報提供ネットワークシステムを通じて提供する際に、誤った特定個人情報を提供することや、誤った相手に提供することを防止するために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.30	Ⅲ 6. リスク7：	問題は認められない	
		61. 情報提供ネットワークシステムとの接続に伴うリスクについて、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.30	Ⅲ 6. その他のリスク	該当なし	

審査の観点（指針第10(2)）	主な考慮事項	主な考慮事項（細目）	該当箇所		審査結果	所見
	⑧特定個人情報の保管・消去について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	62. 特定個人情報の漏えい・滅失・毀損を防ぐために行っている物理的な対策について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.31	Ⅲ 7. リスク1: ⑤	問題は認められない	物理的対策として、クラウド事業者選定時の要件として、「政府情報システムのためのセキュリティ評価制度（ISMAP）」において登録されたサービス等による各種条件を満たす事業者であること等を求めていること等が具体的に記載されている。 技術的対策としてクラウド事業者は個人番号を内容に含む電子データを取り扱わない契約とし、個人番号等にクラウド事業者がアクセスできないように、アクセス制御を行うこと等が具体的に記載されている。 特定個人情報が消去されずいつまでも存在するリスク対策として、オンプレミス環境では、特定個人情報等が記録された機器や電子記録媒体等廃棄する場合、専用のデータ削除ソフトウェアの利用により、データを復元できないよう電子的に完全に消去するとともに、消去証明書を提出させること、クラウド環境では、データの復元がなされないよう、クラウド事業者においてISO/IEC27001に準拠した廃棄プロセスを確保すること等が具体的に記載されている。
		63. 特定個人情報の漏えい・滅失・毀損を防ぐために行っている技術的な対策について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.31	Ⅲ 7. リスク1: ⑥	問題は認められない	
		64. 過去3年以内に発生した全ての重大事故の内容、原因、影響、重大事故発生時への対応等について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.32	Ⅲ 7. リスク1: ⑨	該当なし	
		65. 重大事故を受けて策定・実施した再発防止策の内容について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.32	Ⅲ 7. リスク1: ⑨	該当なし	
		66. 死者の個人番号を保管している場合は保管方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.32	Ⅲ 7. リスク1: ⑩	問題は認められない	
		67. 特定個人情報を最新の状態で保管するために行っている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.32	Ⅲ 7. リスク2:	問題は認められない	
		68. 保管期間を経過した特定個人情報を適切な時に安全かつ確実に消去できる手続・体制・手法になっているか等について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.32	Ⅲ 7. リスク3:	問題は認められない	
		69. 特定個人情報の保管・消去において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.32	Ⅲ 7. その他のリスク	該当なし	

評価実施機関に特有の問題に対するリスク対策

審査の観点（指針第10(2)）	主な考慮事項	主な考慮事項（細目）	該当箇所		審査結果	所見
(10)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。 (11)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。	⑩その他、評価実施機関に特有な問題や懸念に対し、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	74.デジタル庁は国民又は行政機関等から口座情報等を入手し、口座情報登録システムを用いて管理するが、口座情報等が不正に使用されるリスク対策について、具体的に記載しているか。 記載された対策は特定個人情報保護評価の目的に照らし、妥当なものか。	P.24等	Ⅲ 3.リスク2等	問題は認められない	・デジタル庁の情報システム責任者の委任を受けた委託先事業者の運用統括責任者が従事者にID及びハードウエアトークン等を払い出し、その者の役割に応じたアクセス権限を持つユーザアカウントと紐づけること ・ID・パスワード及びハードウエアトークン等を使用した二要素認証を用いること ・デジタル庁の情報システム責任者は、運用統括責任者から口座情報登録システムへのログイン状況などに係る報告書の内容を随時確認し、必要に応じて口座情報登録システムの運用拠点への立入り検査を実施すること ・口座情報登録システムへのアクセスログ等の記録を行うとともに、定期的にログの分析を実施すること 等が具体的に記載されており、特定個人情報保護評価の目的に照らし、妥当である。
		75.デジタル庁が評価対象の事務において使用する口座情報等について、個人番号を用いて他の事務で使用するシステムの情報と紐づく等、目的を超えた紐づけが行われて使用されるリスク対策について、具体的に記載しているか。 記載された対策は特定個人情報保護評価の目的に照らし、妥当なものか。	P24	Ⅲ 3.リスク1	問題は認められない	デジタル庁が他の事務で使用する開示システムと口座情報登録システムにおいては、デジタル庁が定めたインターフェース仕様に沿って、決められたデータ項目のみ提供し、開示システム内の情報と個人番号が紐付かないようにシステム的に制御していること等が具体的に記載されており、特定個人情報保護評価の目的に照らし、妥当である。
		76.口座情報登録システムはクラウド環境を利用するが、クラウド環境の利用に係るリスク対策を具体的に記載しているか。記載された対策は特定個人情報保護評価の目的に照らし、妥当なものか。	P.31等	Ⅲ 7.リスク1等	問題は認められない	・クラウド事業者選定時の要件として、「政府情報システムのためのセキュリティ評価制度（ISMAP）」において登録されたサービス等による各種条件を満たす事業者であること等を求めていること ・クラウド事業者は個人番号を内容に含む電子データを取り扱わない契約とし、個人番号等にクラウド事業者がアクセスできないように、アクセス制御を行うこと 等が具体的に記載されており、特定個人情報保護評価の目的に照らし、妥当である。

【総評】

(1)　公的給付支給等口座登録簿への登録等に関する事務においては、特定個人情報ファイルを取り扱うことについて、一連の事務の内容や流れが具体的に記載されており、特段の問題は認められないものと考えられる。

(2)　事務で取り扱われる特定個人情報ファイルの取扱いについてのリスク及びリスク対策が具体的に記載されており、特段の問題は認められないものと考えられる。

(3)　登録された口座情報等が不正に使用されるリスク対策、口座情報等がマイナンバーを用いて目的を超えた紐づけが行われ使用されるリスク対策等、本評価対象事務において懸念されるリスク及びリスク対策についても、具体的に記載されており、特段の問題は認められないものと考えられる。

【個人情報保護委員会による審査記載事項】

（Ⅵ　評価実施手続　4. 個人情報保護委員会の承認）

(1)　公的給付支給等口座登録簿への登録等に関する事務の内容、特定個人情報ファイルの内容、特定個人情報の流れ並びに リスク及びリスク対策が具体的に記載されており、特段の問題は認められないと考えられるが、特定個人情報保護評価書に記載されているとおり確実に実行する必要がある。

(2)　特定個人情報のインターネットへの流出を防止する対策については、インターネットを通じて外部に特定個人情報が漏えいしないよう、口座情報登録システムにおいてアクセス制御、侵入検知及び侵入防止、ログの解析を行うこと、口座情報登録システムと登録者本人との間において暗号化通信を実施すること等が記載されているが、特定個人情報保護評価書に記載されているとおり確実に実行する必要がある。

(3)　組織的及び人的安全管理措置については、適切な組織体制の整備、職員への必要な教育・研修、実効性のある自己点検・監査等を実施し、実務に即して適切に運用・見直しを行うことが重要である。

(4)　情報漏えい等に対するリスク対策全般について、特定個人情報保護評価書に記載されているとおり確実に実行することに加え、不断の見直し・検討を行うことが重要である。