資料４－２

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
預貯金者の意思に基づく個人番号の利用による 預貯金口座の管理等に関する事務　全項目評価書

評価実施機関名
預金保険機構

提出日
令和5年3月23日

概要説明日
令和5年3月29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、預金保険機構（以下「機構」という。）が預貯金者の意思に基づく個人番号の利用による預貯金口座の管理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	再実施の理由となる新たに実施する事務は、令和5年10月までに事務の開始を予定しており、事務処理の変更の検討段階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、機構のホームページにて、31日間実施したほか、意見への対応状況をHP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	預貯金者の意思に基づく個人番号の利用による預貯金口座の管理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。 なお、再実施の理由となる新たに実施する事務については、災害時における預貯金口座に関する情報の提供の申し出において、申し出た預貯金者から個人番号の提供がない場合に、受付金融機関が既に当該預貯金者の付番口座を保有していれば、機構が、受付金融機関から当該付番口座の個人番号を入手し、提供等するものであるが、当該事務についても求められる事項が具体的に記載されている。
(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	預貯金者の意思に基づく個人番号の利用による預貯金口座の管理等に関する事務においては、預金保険部及びシステム統括室が連携して番号制度への対応を行っており、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。

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。	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	Ⅰ 1. ②	問題は認められない	預貯金者の意思に基づく個人番号の利用による預貯金口座の管理等に関する事務において、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の事務の内容では、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明記されており、特定個人情報の流れとそれ以外の情報の流れを区別する等、特定個人情報の流れが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	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	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.5	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.5	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.6 ～ P.17	(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.26 ～ P.38	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.38	Ⅳ 1. ①	問題は認められない	自己点検については、預金保険機構情報セキュリティポリシー（以下「ポリシー」という。）に基づき、年1回、特定個人情報等取扱者を含む全役職員を対象として、総務部情報セキュリティ室から提示された情報セキュリティ対策の自己点検実施要領に基づき、eラーニングを用いて自己点検を実施していること等が具体的に記載されている。 監査については、ポリシーに基づき、情報セキュリティ関係規程の遵守状況、情報システムにおける情報セキュリティ対策の運用状況の確認のための監査及び情報システムの脆弱性診断について、外部専門事業者に委託して実施してい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・啓発については、ポリシーに基づき、毎年度、情報セキュリティ対策の教育に関する実施計画を立て、新規着任時の研修や情報セキュリティ関連責任者・管理者向け研修等の研修を実施していること等を具体的に記載している。 また、ポリシー及びその下位規程について、政府統一基準群に準拠しており、政府機関等の情報セキュリティ対策と同等の対策を講じていること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.38	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.38	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.40	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、機構としての考え方を一覧形式で取りまとめ、HP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	機構は、預貯金者の意思に基づく個人番号の利用による預貯金口座の管理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、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
（受付依頼情報ファイル）

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.18	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、特定個人情報を利用することで、公的給付支給時に迅速かつ効率的に口座情報の提供が可能となり、また、災害時又は相続時において迅速かつ効率的に口座情報の提供が可能となることが具体的に記載されている。 特定個人情報の使用方法について、金融機関又はマイナポータルを通じて預貯金者から提供を受けた個人番号を当該預貯金者名義の口座を管理する金融機関に通知すること等、特定個人情報ファイルの取扱いプロセスの概要（入手・使用、委託、提供、保管・消去）について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.18	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.19	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.19	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.19	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.20	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.20	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.20	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.21～P.22	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.21～P.22	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.21～P.22	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.23	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.23	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.24	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.24	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.24	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.26	Ⅲ 2. リスク1:	問題は認められない	目的外の入手が行われるリスク対策として、委託先の受付金融機関に対して、金融機関システムから個人番号を依頼ファイルに連携する場面で、受付金融機関の受付システムに手入力やUSBメモリ等の媒体を介したデータ提供が行われない対策や運用等を講ずることを業務委託契約によって求めるとともに、業務委託契約に基づき、定期的な管理態勢の報告を受け、口座登録法及び口座管理法に係るガイドライン（金融機関編）で定められる特定個人情報を適切に扱うことができる方式の遵守状況を確認すること等が具体的に記載されている。 不適切な方法で入手が行われるリスク対策として、災害時における被災者への口座情報の通知以外にも、行政機関の税務調査等において預貯金者の預貯金口座を特定するために利用され得ることを説明した上で、同意を得た預貯金者のみから入手するため、当該目的を把握していない預貯金者が付番申し出を行うことはないこと、受付金融機関において、預貯金者名義の口座へ付番済みであり、当該預貯金者の個人番号を機構に提供する場合、必要最小限の情報のみを入手できるように定められたインタフェースを介して入手することとなり、手入力やUSBメモリ等の媒体を介したデータ提供を行わず、特定個人情報を適切に扱うことができる方式（専用線、閉域ネットワーク又はLAN接続によるシステム間連携）で行うこと等が具体的に記載されている。 入手の際に特定個人情報が漏えい・紛失するリスク対策として、金融機関からの入手においては、通信を閉域ネットワークで暗号化し、アップロードファイルも暗号化すること、受付金融機関において、預貯金者名義の口座へ付番済みであり、当該預貯金者の個人番号を機構に提供する場合、手入力やUSBメモリ等の媒体を介したデータ提供を行わず、特定個人情報を適切に扱うことができる方式で行うこと、金融機関の受付システムを接続するに当たっては、セキュリティの観点から、金融機関に対してシステムの利用端末に関する要件及びシステムとの接続に関する要件を定め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.26	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.27	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.28	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.28	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.28	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.29	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.29	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.30	Ⅲ 3. リスク1:	問題は認められない	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、外部との情報の授受及び処理は全てシステムで自動的に行うため、システムにログインする利用者が特定個人情報を視認する必要はなく、視認するための機能も装備しないこと、機構においては、機構内の決裁を経て管理者IDを付与された管理者が、利用者IDの発行・配布・抹消を行い、利用者IDの一覧は、データ出力機能を用いて定期的に確認すること、金融機関等に関しては、機構の管理者が当該金融機関等管理者IDの発行・配布・抹消を行い、当該金融機関において、当該管理者IDを付与された管理者が、機構が定めた基準・ルールに従って、利用者IDの発行・配布・抹消を行うこと、金融機関等における利用者IDの一覧は、データ出力機能を用いて当該金融機関等の管理者が定期的に確認を行うこと等が具体的に記載されている。 特定個人情報ファイルが不正に複製されるリスク対策として、システムで保有する特定個人情報の電子記録媒体への書き出しができないように、システム的な措置を講ずること、取得した操作ログについては、一定期間（7年間）保存し、定期に及び必要に応じて分析を随時行うこと等が具体的に記載されている。 特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置として、仮に不正使用等が発生した場合、操作ログには特定個人情報を含めない仕様としているため、当該ログから不正操作により流出した特定個人情報を把握することはできないが、システムから特定個人情報ファイルを削除するまでの間は、当該ファイルから流出した特定個人情報を把握し、また、当該ファイルの削除後は、連携する金融機関等の協力を得て流出した特定個人情報把握のための調査を行うこと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.30	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.30	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.30	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.30	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.30	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.31	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.31	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.31	Ⅲ 3. その他のリスク	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
	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.32	Ⅲ 4. 情報管理体制	問題は認められない	災害時における預貯金者の受付事務等を委託することとしているが、金融機関等に対しては、委託契約書、口座登録法及び口座管理法に係るガイドライン等において、特定個人情報の保護を適切に行えることを求めること、業務委託契約において、機構が承認した再委託先以外の他者への特定個人情報の提供を禁ずるとともに、当該再委託先への特定個人情報の提供について、委託業務を実施するために必要な範囲に限定する旨を記載すること、再委託を承諾するに当たり、再委託先が再委託に係る業務を適切に履行する能力及び体制を備えるものであることその他機構が求める情報、再委託先が委託先に対して負うセキュリティ水準（委託先と同等以上のものに限る）具備義務の具体的内容、再委託先の情報セキュリティに関する対策方針及び管理方法についての情報を求めること等が具体的に記載されている。 特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置として、平時においては定期的に委託先の管理態勢について報告を受けるなどで確認するとともに、報道等により委託先の管理態勢に疑義が生じた場合には、必要に応じて状況報告を求めること、特定個人情報の漏えい、滅失又は毀損等の不備が発生した際は、漏えい等事案に係る対処状況、原因分析、再発防止策等の報告を求め、事案の内容によっては、実地の監査・調査等を行う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.32	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.32	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.32	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.32	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.32	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.32	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.33	Ⅲ 4. その他のリスク	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
	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.34	Ⅲ 5. リスク1:	問題は認められない	不適切な方法で提供・移転が行われるリスク対策として、閉域ネットワークを利用して通信の暗号化等の高度なセキュリティを確保するとともに、システム間連携、限定されたフォーマットによるダウンロードにより、不適切な方法で提供されるリスクに対処すること、取得した操作ログについては、一定期間（7年間）保存し、定期に及び必要に応じて分析を随時行い、不適切な方法で提供されるリスクに対処すること、金融機関の受付システムとシステムを接続するに当たっては、セキュリティの観点から金融機関に対してシステムの利用端末に関する要件及びシステムとの接続に関する要件を定めていること等が具体的に記載されている。 誤った情報を提供・移転してしまうリスク対策及び誤った相手に提供・移転してしまうリスク対策として、システムの仕様に基づき、該当者に関する必要な情報を自動的に抽出し提供するため、誤った情報を提供することはないこと、システムによる処理に基づき、専用線又は閉域ネットワークを介する適切な制御のもとで提供するため、誤った相手に提供することはないこと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.34	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.34	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.34	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.34	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.35	Ⅲ 6. リスク1:	該当なし	—
		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.35	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.35	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.35	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.35	Ⅲ 6. リスク5:	該当なし	
		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.35	Ⅲ 6. リスク6:	該当なし	
		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.35	Ⅲ 6. リスク7:	該当なし	
		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.35	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.36	Ⅲ 7. リスク1: ⑤	問題は認められない	物理的対策として、システムは、機構が契約した専用クラウド環境に構築すること、利用予定のクラウドサービスは、ISMAPに登録されたサービスか、ISO/IEC27017:2015又はCSマーク（ゴールド）の認証を取得しているサービスであること、操作端末設置場所には許可された利用者のみが入退室可能であり、入退記録をログとして保管するほか、監視カメラを設置すること等が具体的に記載されている。 技術的対策として、特定個人情報が記録されたデータは、機構が契約した専用クラウド環境に暗号化された状態で保存すること、利用者との間の通信を保護するため、SSL/TLSにより通信の暗号化を行うこと、Firewallによるアクセス制限、WAFによるWEBアプリケーションの脆弱性攻撃遮断及びIDSによる侵入検知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、データベース形式で保有する特定個人情報は、利用業務が終了後に一定期間（照会対応のための期間）経過後に復元できない形（復元不可能なマスク値等にアップデート）で消去すること、データの削除はシステム処理により自動で行われること、正常に削除されたかについて削除処理の結果（正常終了/異常終了）により確認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.36	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.37	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.37	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.37	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.37	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.37	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.37	Ⅲ 7. その他のリスク	問題は認められない	

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. 災害時における預貯金口座に関する情報の提供の申し出において、申し出た預貯金者から個人番号の提供がない場合に、受付金融機関が既に当該預貯金者の付番口座を保有していれば、機構が、受付金融機関から当該付番口座の個人番号を入手し、提供等するが、その際の取扱いに係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.26等	Ⅲ 2. リスク1等	問題は認められない	・委託先の受付金融機関に対して、金融機関システムから個人番号を依頼ファイルに連携する場面で、受付金融機関の受付システムに手入力やUSBメモリ等の媒体を介したデータ提供が行われない対策や運用等を講ずることを業務委託契約によって求めるとともに、業務委託契約に基づき、定期的な管理態勢の報告を受け、口座登録法及び口座管理法に係るガイドライン（金融機関編）で定められる特定個人情報を適切に扱うことができる方式の遵守状況を確認すること ・受付金融機関において、預貯金者名義の口座へ付番済みであり、当該預貯金者の個人番号を機構に提供する場合、必要最小限の情報のみを入手できるように定められたインタフェースを介して入手することとなり、手入力やUSBメモリ等の媒体を介したデータ提供を行わず、特定個人情報を適切に扱うことができる方式（専用線、閉域ネットワーク又はLAN接続によるシステム間連携）で行うこと ・平時においては定期的に委託先の管理態勢について報告を受けるなどで確認するとともに、報道等により委託先の管理態勢に疑義が生じた場合には、必要に応じて状況報告を求めること ・特定個人情報の漏えい、滅失又は毀損等の不備が発生した際は、漏えい等事案に係る対処状況、原因分析、再発防止策等の報告を求め、事案の内容によっては、実地の監査・調査等を行うこと 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）　預貯金者の意思に基づく個人番号の利用による預貯金口座の管理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）　金融機関への特定個人情報の入手の委託に係るリスク対策等、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）　預貯金者の意思に基づく個人番号の利用による預貯金口座の管理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、暗号化通信や、Firewallによるアクセス制御、WAFによるWEBアプリケーションの脆弱性攻撃遮断、IDSによる侵入検知を行うなどの旨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について、手入力やUSBメモリ等の媒体を介したデータ提供を行わず、特定個人情報を適切に扱うことができる方式（専用線、閉域ネットワーク又はLAN接続によるシステム間連携）で行うこと、受付金融機関に対して、対策や運用等を講じることを業務委託契約によって求めるとともに、定期的な管理態勢の報告を受け、口座登録法及び口座管理法に係るガイドラインで定められる特定個人情報を適切に扱うことができる方式の遵守状況を確認すること等が記載されている。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。