

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	公的年金業務等に関する事務 全項目評価書
評価実施機関名	厚生労働大臣
提出日	令和4年1月18日
概要説明日	令和4年1月19日

(目次)

○ 全体的な事項	1
○ 特定個人情報ファイル(公的年金業務等に関するシステム関連ファイル).....	4
○ 評価実施機関に特有の問題に対するリスク対策	11
○ 総評	12
○ 個人情報保護委員会による審査記載事項	12

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、厚生労働省が公的年金業務等に関する事務において保有するものであることから、評価実施機関を厚生労働大臣としていることは適切である。 また、一連の業務運営は法律に基づき日本年金機構が行うこととされているため、日本年金機構を他の評価実施機関としている。
(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システム改修に伴うプログラミング開始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30日間実施したほか、意見への対応状況は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	公的年金業務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	公的年金業務等に関する事務における番号制度への対応は厚生労働省年金局事業企画課が行っており、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、日本年金機構における措置を取りまとめて記載している。
(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.6	I 1. ②	問題は認められない	公的年金業務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、事象が起きる順に番号を付けている等、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.6 ～ P.9	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.7 ～ P.9	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.10	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.10	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.12 ～ P.43	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.63 ～ P.80	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.80	Ⅳ 1. ①	問題 は 認め られ ない	自己点検については毎月、日本年金機 構全職員に対して、機構LANを通じて自 己点検シートを配付の上、自己点検を行 わせ管理責任者が内容を確認すること、 また、監査については、計画的に管理 ルール・手順書等の閲覧、インタビュー及 び現場確認により監査を行い確認を行っ ていること、日本年金機構における委託 先に対する監査の見直し等により、監査 体制の強化を図った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.77 ～ P.79 P.80	Ⅲ 7. リスク1: ⑨ Ⅳ 1. ②	問題 は 認め られ ない	従業員に対する教育・啓発については、 職員に対し毎年度個人情報保護研修を 義務付けていること等が具体的に記載 されている。
		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.80	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.82	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 れた意見に対し、厚生労働省としての考 え方を取りまとめ、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	公的年金業務等に関する事務について は、厚生労働省が財政責任・管理運営 責任を負いつつ、一連の業務運営は法 律に基づき日本年金機構が行うことと されており、厚生労働省が保有する公 的年金業務等に係るシステムや特定 個人情報ファイルを取り扱う全ての 事務を行う日本年金機構も同様の 措置を講じることを特記事項として 記載した上で、特定個人情報の漏 えい、その他の事態が発生するリ スクを軽減させるために十分な措 置を講じ、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
(公的年金業務等に関する
システム関連ファイル)

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
<p>(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。</p>	<p>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。</p>	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.44	II 2. ③	問題は認められない	<p>特定個人情報の使用目的として、(ア)個人番号と基礎年金番号との紐付けを行い、個人番号により基礎年金番号を検索し、年金相談・照会事務を行うこと、(イ)協会けんぽが行う事務において必要となる特定個人情報を協会けんぽへ提供するために使用すること、(ウ)公的年金から所得税等を源泉徴収する事務、源泉徴収票及び公的年金等支払報告書への個人番号の記載や、地方税の特別徴収事務に係る情報の市区町村への回付(国家公務員共済組合及び日本私立学校振興・共済事業団への回付も含む。)を行う際に使用すること、(エ)年金受給に関する各種届け書等のワンストップサービスを行うため、他の実施機関で処理が必要な届け書を受け付けた実施機関は、届け書を画像化し、公的年金給付総合情報連携システムを使用して当該他の実施機関に電子回付すること、(オ)各年金法令等に基づく届出に個人番号を利用することにより、被保険者等の届出の利便性を向上させる他、情報提供ネットワークシステムを通じて届け書の審査に必要となる情報を取得し添付書類の省略を行うために使用すること等が具体的に記載されている。</p> <p>また、特定個人情報ファイルは、セキュリティゲートによって入退管理されている建物の中で、更に入退室管理を行っている機械室(マシン室)に設置したサーバ内に保管すること等、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)が具体的に記載されている。</p>
		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.44	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.47	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.48	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.48	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.49 ～ P.50	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.50	II 3. ⑧	問題は認められない	
		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.50	II 3. ⑧	問題は認められない	
		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.51 ～ P.55	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.51 ～ P.55	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.52 ～ P.55	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.56 ～ P.59 別紙1	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.59	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.60	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.60	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.61	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
<p>(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。</p> <p>(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。</p>	<p>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。</p>	<p>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>	P.63	Ⅲ 2. リスク1:	問題は認められない	<p>必要な情報以外の入手を防止する措置として、①地方公共団体情報システム機構からの入手については、提供される情報は個人番号及び基本情報のみにシステム制御されているため、不必要な情報の入手はできないこと、②本人及び事業主等からの入手については、様式には、審査に必要な情報のみ記載すること等が具体的に記載されている。</p> <p>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、①書類による入手の際は、内容審査、入力処理、決裁が完了するまでの間、未処理書類を保管する容器に収納し、施錠した保管庫の中に格納、管理されること、②事業主等から電子媒体を入手する際は、電子媒体内の情報ファイルにパスワードを設定し、情報の暗号化を行った上で提出することを事業主等に推奨するとともに、提出された場合は管理簿に記載し、鍵付の保管庫に保管・管理すること、③専用線による入手の際は、他のシステムからのアクセスが行えない専用線を用いて行うこと等が具体的に記載されている。</p>
		<p>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>	P.64	Ⅲ 2. リスク1:	問題は認められない	
		<p>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>	P.64	Ⅲ 2. リスク2:	問題は認められない	
		<p>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>	P.65	Ⅲ 2. リスク3:	問題は認められない	
		<p>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>	P.65	Ⅲ 2. リスク3:	問題は認められない	
		<p>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>	P.65	Ⅲ 2. リスク3:	問題は認められない	
		<p>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>	P.66	Ⅲ 2. リスク4:	問題は認められない	
		<p>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>	P.66	Ⅲ 2. 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
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な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.67	Ⅲ 3. リスク1:	問題は認められない	<p>目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク対策として、年金業務システム、記録管理システム、基礎年金番号管理システム、年金給付システムではシステム上、①個人番号や基礎年金番号等による検索と、②カナ氏名・漢字氏名・生年月日等を用いた検索以外は不可能となっており、公的給付支給等口座登録簿関係情報等(例えば、年金加入期間や振込先口座情報等)から不必要な情報に紐付かない仕様となっていること、情報連携で取得した情報は業務上必要な範囲で各システムに保管し、業務に必要な権限を付与された者のみがアクセスできるように制御していること等が具体的に記載されている。</p> <p>権限のない者によって不正に使用されるリスク対策として、①業務端末のユーザ認証は生体認証及びID、パスワードによる認証を行い、IDは共用ではなく個人ごとにユーザIDを割り当てていること、②部署ごとに設置した管理者が、所属する職員のシステムへのアクセスを許可する設定を行っていること等が具体的に記載されている。</p> <p>従業者が事務外で使用するリスク対策として、個人番号を含む特定個人情報を取り扱うことが必要な職員にのみ情報照会を許可することで、必要最小限の職員に限定するとともに、情報照会のログ等を定期及び必要に応じ随時に分析し、不適切な使用を防止すること等が具体的に記載されている。</p>
		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な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.67	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.67	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.67	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.67	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.68	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.68	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.68	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.68	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.69	Ⅲ 4. 情報管理体制	問題は認められない	<p>届け書等のデータ入力等を委託することとしており、委託先を選定する際は、認証資格の取得状況を確認する等、委託先の個人情報管理体制を確認すること等が具体的に記載されている。</p> <p>委託先においては、①特定個人情報にアクセスできる業務委託員を必要最小限に特定し、当該者のみにアクセス権限を付与すること、②アクセス権限の設定に当たっては、業務上の責務と必要性を勘案し、必要最小限の範囲に限り許可を与えること等が具体的に記載されている。</p> <p>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は、再委託の原則禁止等を定めていること、履行開始前検査等を適切に行うことを徹底するため、調達や外部委託管理に関するルールの改正を行っていること、また、標準契約書において、委託先に履行能力がないと判断した場合には契約解除できることを規定していること等が具体的に記載されている。</p>
		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.69	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.69	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.69	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.69	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.69	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.69	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.69	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.70	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、①外部機関(市区町村を除く。)に電子媒体で特定個人情報の提供を行う場合は、暗号化した電子媒体を、機構職員が提供先の職員に手渡し、提供すること、②市区町村に紙又は電子媒体で特定個人情報の提供を行う場合は、各管理簿を使用して事前に管理者の許可を得た上で郵送・持参すること等が具体的に記載されている。 また、国家公務員共済組合、地方公務員共済組合及び日本私立学校振興・共済事業団(以下「3共済」という。)へ特定個人情報の提供を行う場合は、機構と3共済との情報連携は専用線を用いて行うことによって、決められた提供先のみに必要な情報を提供できる仕組みを構築する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.70	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.71	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.71	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.71	Ⅲ 5. 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
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.72	Ⅲ 6. 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、照会実施者は業務目的に沿った範囲内で情報照会を実施するとともに、照会を行う毎にどの契機で何の目的のためにどの情報を照会したかを処理票に記録し、管理者は業務目的に沿った照会を行っているかを処理結果リストと突合し確認すること、本人が年金又は年金生活者支援給付金の請求をする際に、受取口座として登録した公金受取口座の利用希望の有無を確認するチェック欄を設け、当該チェック欄にて利用希望が確認された場合に限り、公的給付支給等口座登録簿関係情報を情報照会する運用とすることにより、目的外の公的給付支給等口座登録簿関係情報の入手を防止すること等が具体的に記載されている。 安全が保たれない方法によって入手が行われるリスク対策として、情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計された中間サーバーを利用すること、年金業務システムと情報提供ネットワークシステムとの間では通信の暗号化を行い、セキュリティを維持した専用ネットワーク(厚生労働省統合ネットワーク、政府共通ネットワーク)を利用し、安全性を確保すること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、年金業務システムでは、ネットワーク接続制御機能を持つことで、不適切な端末の接続を防止し、ファイアウォール機能により、適正な接続先とのみ通信を行う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.72	Ⅲ 6. リスク2:	問題は認められない	
		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.72	Ⅲ 6. リスク3:	問題は認められない	
		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.72	Ⅲ 6. リスク4:	問題は認められない	
		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.72	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.73	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.73	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.73	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.74	Ⅲ 7. リスク1: ⑤	問題は認められない	
		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.74	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.74	Ⅲ 7. リスク1: ⑨	問題は認められない	物理的対策として、①マシン室出入口には生体認証によるセキュリティゲートを設置すること、②入退室監視設備として監視カメラを設置すること、③本人、市区町村等から提出された届け書等の紙・電子媒体(DVD・CD)については、受付簿に受付の記録を残し施錠できる保管庫において保管していること等が具体的に記載されている。
		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.77 ～ P.79	Ⅲ 7. リスク1: ⑨	問題は認められない	技術的対策として、①事務で使用する端末は、外部媒体への書き込み、インターネットへの接続、OSのセキュリティレベルの変更等を制限するとともに、ウイルス、スパイウェア等の不正プログラムを検知し、駆除又は隔離を行うソフトウェアを導入していること、②ネットワーク上に許可のない端末が接続した場合、検知、通信の遮断、管理者へ通知する仕組みとすること等が具体的に記載されている。
		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.75	Ⅲ 7. リスク1: ⑩	問題は認められない	令和3年10月定期支払分の年金振込通知書について、振込金額等の記載内容を誤って印刷し、通知した事案を踏まえ、委託事業者による印刷物等納品物の作成において、納品物の作成プロセスの各段階で、テスト品についても作業手法・工程を確認のうえ、各工程において必要な証跡を取得し確認する等、作成プロセスの適切さを確認する立入・書類検査ルールを改善し、実効性を高めること、作成プロセスの検査を厳格に実施することを前提に、最終的なアウトプット段階においても完成品の現物等で検査することを具体化すること等が具体的に記載されている。
		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.75	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.76	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.76	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
<p>(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。</p> <p>(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。</p>	<p>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。</p>	<p>74. 公的年金等の給付にあたり、口座情報登録システムから情報提供ネットワークシステムを介して公的給付支給等口座登録簿関係情報を入手し、使用するが、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されているか。 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> <p>75. 個人情報ファイルの取扱いの委託において発生した年金振込通知書の印刷誤り事案及び当該事案の再発防止策を踏まえ、特定個人情報ファイルの取扱いの委託において、同様の事案が発生しないようにリスク対策について具体的に記載されているか。 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>	<p>P.67 P.72 等</p>	<p>Ⅲ 3. リスク1 Ⅲ 6. リスク1 等</p>	<p>問題は認められない</p>	<p>・情報連携で取得した情報は業務上必要な範囲で各システムに保管し、業務に必要な権限を付与された者のみがアクセスできるように制御していること ・本人が年金又は年金生活者給付金の給付請求をする際に、受取口座として登録した公金受取口座の利用希望の有無を確認するチェック欄を設け、当該チェック欄にて利用希望が確認された場合に限り、公的給付支給等口座登録簿関係情報を情報照会する運用とすることにより、目的外の口座関係情報の入手を防止すること ・照会実施者は業務目的に沿った範囲内で情報照会を実施するとともに、照会を行う毎にどの契機で何の目的のためにどの情報を照会したかを処理票に記録し、管理者は業務目的に沿った照会を行っているかを処理結果リストと突合し確認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。</p> <p>委託事業者の業務プロセスが適切であることを確認するための立入・書類検査ルールを改善し、実効性を高めるため、 ・納品物等の作成プロセスの各段階において、テスト品についても、作業手法・工程を確認のうえ、各工程において必要な証跡を取得し確認すること、 ・最終的なアウトプット段階においても完成品の現物で検査することを具体化すること等が記載されており、特定個人情報保護評価の目的に照らし、妥当である</p>

【総評】

- (1) 公的年金業務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) 公的給付支給等口座登録簿関係情報等の入手・使用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) 公的年金業務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、事務を行う業務端末をインターネットに接続させないとともに、特定個人情報はインターネットに接続する端末や情報系システムの共有フォルダには保管しない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・監査等を実施するとともに、厚生労働省及び機構本部が、各拠点の実態を十分に把握した上で、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。また、見直しの際には、厚生労働省及び機構本部が、各拠点の実態を十分に把握した上で、より実効性のあるリスク対策を講じることが重要である。