資料１－１

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５年12月19日

概要説明日
令和５年12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、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。 得られた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。 なお、再実施の理由となる重要な変更については、記録管理システム及び基礎年金番号管理システムを刷新し、年金業務システム(フェーズ2)を開発するものであるが、当該重要な変更についても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.7	Ⅰ1.②	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の事務の内容において、被保険者、年金受給権者等から提出される各種届出により個人番号を入手し、基礎年金番号と紐付けた上で年金業務システムに登録すること等、事務において取り扱う特定個人情報の流れが事務の内容に即して具体的に記載されているほか、情報提供ネットワークシステムを通じた関係機関との情報連携を行うことにより、被保険者、年金受給権者等の各届出の省略、各届出の際に必要となる所得証明書等の添付書類の省略を実施し、被保険者、年金受給権者等の届出負担の軽減や日本年金機構の事務処理の効率化等、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.8 ～ P.16	Ⅰ2.②	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.9 ～ P.16	Ⅰ2.③	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.19	Ⅰ4.①	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.19	Ⅰ4.②	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.21 ～ P.81	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.103 ～ P.129	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.128	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、個人情報保護管理責任者が点検結果の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。 従業者に対する教育・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。
		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.128	Ⅳ 1. 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.128	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.131	Ⅵ 2. ⑤	問題は認められない	「等」や助詞の使い方についての意見への回答として、日本年金機構で取り扱う業務・届書の数は膨大であり、その全てを個別に記載すると可読性を損なう恐れがあることから、評価書への反映は行わないこととしたことが記載されている。
(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を発生させ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
(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.82	Ⅱ 2. ③	問題は認められない	特定個人情報の使用目的として、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、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、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、国税庁への公的年金等の源泉徴収票の提出、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、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、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が具体的に記載されている。 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、さら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。
		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.82	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.84 ～ P.85	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.85	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.85	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.86 ～ P.87	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.87	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.87	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.88 ～ P.93	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.88 ～ P.94	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.88 ～ P.94	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.95 ～ P.98 P.142 ～ P.143	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.99	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.100	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.100	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.101	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.103 ～ P.104	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、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、本人又は本人の代理人からの入手については、電子申請により届け書（年金請求書、資格届出書等）を受け付ける場合は、電子証明書による電子署名又は法人共通認証基盤によるID・パスワード方式によって、なりすましを防止し、提出者等からの情報のみ受け付けるようにシステムで制御されていること、届け書の様式には、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。 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、書類による入手について、本人又は本人の代理人、事業主等からの入手の際は、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、電子媒体による入手について、届け書のデータ入力を行う委託業者からの入手の際は、委託契約書において個人情報保護に関する体制の整備を求めている他、実際の届け書や電子媒体の受渡しの際は、委託票（受託表）や納品書（収録一覧表）を取り交わしており、納品された電子媒体については、業務端末から専用線を通じて年金業務システム、源泉徴収サブシステムに登録を行うこと、事業主等からの入手の際は、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こと、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、電子申請による入手について、本人、事業主等からの入手の際は、厚生労働省統合ネットワーク（専用線）を経由して、社会保険オンラインシステム・年金業務システムに情報が回付されることとなっており、個人情報が漏えい、紛失するおそれはない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.104	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.104 ～ P.105	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.105 ～ P.106	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.106	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.106	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.107 ～ P.108	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.108	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.108	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、個人番号を利用する際は、年金業務システムにおいて個人番号を基礎年金番号に変換した上で、処理を行うこととしているため、社会保険オンラインシステムの中の年金給付システムには個人番号を保有しないこと、電子申請システム、年金給付システムの中の源泉徴収サブシステム、公的年金給付総合情報連携システム及び障害年金業務支援システムにて個人番号を保有するが、アクセス権限の管理、外部回付データの暗号化により、源泉徴収事務、電子申請による届け書の届出処理事務、被用者年金の一元化に伴う届け書の回付事務及び障害年金の事務以外の事務では個人番号にアクセスできないよう措置を行っていること、年金業務システム、年金給付システムではシステム上、個人番号や基礎年金番号等による検索と、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。 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。 特定個人情報の使用におけるその他のリスク対策として、業務におけるDBアクセスについては、端末から管理するデータまでは多層的な防御を行うとの考え方のもと、セキュリティレベルに応じて領域を分割することで、隣接する領域でのみ通信を可能とする対策を行っていること、マイナンバーと基礎年金番号の紐付け作業をシステム的に行う事を基本としていること、データ移行の作業については、機構が別途指示する作業場所において、基本的には人の手を介さないようアプリケーション機能により実施し、人を介した作業が必要な場合には、最低限必要な情報取扱者により、機構職員の立ち会いの下で行うこと、作業を実施するに当たっては、事前に作業計画を策定し、受注者において関係する一連の責任者及び統括責任者の承認を得た上で、刷新システム開発部長の承認を得ること、情報取扱者は作業終了後、計画通りに作業が行われたことを示すアクセスログ等を提出し、同様に統括責任者等及び刷新システム開発部長の承認を得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.108 ～ P.109	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.110	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.111	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.111	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.111	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.112	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.112	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.113	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.114	Ⅲ 4. 情報管理体制	問題は認められない	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。 委託先においては、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、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って許可を与えること等が具体的に記載されている。 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、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。
		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.114	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.114	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.114	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.114	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.115	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.115	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.115	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.116	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、協会けんぽ、市区町村、国税庁、2共済、3共済、内閣総理大臣への提供について、年金業務システムや年金給付システムで特定個人情報を提供した事跡を保管する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、内閣総理大臣（デジタル庁）への提供は、特定個人情報の提供を行う場合は、厚生労働省情報セキュリティポリシー及び日本年金機構情報セキュリティポリシーに従った情報セキュリティ対策を取り、適切に権限設定された特定者及び特定機能が、許可された特定個人情報にのみにしかアクセスできない仕組みを構築す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、協会けんぽへの電子媒体による提供については、暗号化した電子媒体を職員が確認し、直接提供先の職員へ手渡す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.116 ～ P.117	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.117 ～ P.118	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.118	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.118	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.119	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、照会を行うごと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、年金業務システムは、情報照会機能により、情報提供ネットワークシステムを利用して情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リストとの照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施する機能（番号法上認められた情報連携以外の照会を拒否する機能）を通して、目的外提供等のセキュリティリスクに対応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、中間サーバーは、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は、通信の暗号化を行い、高度な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及び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.119	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.119	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.119	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.120	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.120	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.120	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.120	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.121	Ⅲ 7. リスク1: ⑤	問題は認められない	物理的対策として、機械室（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及び守衛を設置すること、入退室監視設備として監視カメラを設置すること、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。 技術的対策として、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、ウィルス、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、不正アクセス対策については、侵入防止及び侵入検知機能を有した装置を導入し、ネットワークへの不正侵入を検知し、管理者に通知する仕組みとし、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。 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、記録管理システム、基礎年金番号管理システム等から年金業務システムへのデータ移行に使用する電子媒体については、年金業務システム内に情報を登録移行した後は、機構本部の担当部署において、廃棄（消去）伺を作成し、責任者の許可を受けた後、速やかに物理的破壊を実施し廃棄証明書を作成し保管すること等が具体的に記載されている。 特定個人情報の保管・消去におけるその他のリスク対策として、移行データをフェーズ2で使用する統合データベースに格納するまでの間及び統合データベースに格納後電子記録媒体のデータを消去するまでの間は、データセンター内の施錠可能な保管庫で管理すること、電子記録媒体の保管庫への媒体搬入及び搬出の際は、機構の担当部門職員が立ち会い、複数人で電子記録媒体の移送を行うことにより、紛失のリスクを軽減すること、既存システムの機器の撤去に際しては、既存システム保守業者が物理的破壊、データを消去するソフトウェア、データ消去装置等を用いて、全ての情報を復元不可能な状態とした後、機構に「撤去完了報告書」を提出し、承認を得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.121	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.122	Ⅲ 7. リスク1: ⑨	問題は認められない	
		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.125 ～ P.127	Ⅲ 7. リスク1: ⑨	問題は認められない	
		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.122	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.122	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.123 ～ P.124	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.124	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. 記録管理システム及び基礎年金番号管理システムを刷新し、年金業務システム（フェーズ2）を開発するものであるが、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.113等	Ⅲ 3. その他のリスク等	問題は認められない	・業務におけるDBアクセスについては、端末から管理するデータまでは多層的な防御を行うとの考え方のもと、セキュリティレベルに応じて領域を分割することで、隣接する領域でのみ通信を可能とする対策を行っていること ・年金業務システム、年金給付システムではシステム上、個人番号や基礎年金番号等による検索と、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から不必要な情報に紐付かない仕様となっていること ・データ移行の作業については、機構が別途指示する作業場所において、基本的には人の手を介さないようアプリケーション機能により実施し、人を介した作業が必要な場合には、最低限必要な情報取扱者により、機構職員の立ち会いの下で行うものとすること ・作業を実施するに当たっては、事前に作業計画を策定し、受注者において関係する一連の責任者及び統括責任者の承認を得た上で、刷新システム開発部長の承認を得ること ・情報取扱者は作業終了後、計画通りに作業が行われたことを示すアクセスログ等を提出し、同様に統括責任者等及び刷新システム開発部長の承認を得ること ・記録管理システム、基礎年金番号管理システム等から年金業務システムへの移行データを収録した電子媒体を使用して年金業務システム内に情報を登録移行した後は、機構本部の担当部署において、廃棄（消去）伺を作成し、責任者の許可を受けた後、速やかに物理的破壊を実施し廃棄証明書を作成し保管すること ・移行データをフェーズ2で使用する統合データベースに格納するまでの間及び統合データベースに格納後電子記録媒体のデータを消去するまでの間は、データセンター内の施錠可能な保管庫で管理し、電子記録媒体の保管庫への媒体搬入及び搬出の際は、機構の担当部門職員が立ち会い、複数人で電子記録媒体の移送を行うことにより、紛失のリスクを軽減すること ・既存システムの機器の撤去に際しては、既存システム保守業者が物理的破壊、データを消去するソフトウェア、データ消去装置等を用いて、全ての情報を復元不可能な状態とした後、機構に「撤去完了報告書」を提出し、承認を得ること ・統合DBへのデータ移行については、移行前の既存システムで管理されているデータを個人ごとに識別して抽出、そのまま移行することとしており、他の個人として識別されたデータと統合するなどのデータの補正は一切行わないことで既存システム内で別人として管理されている情報同士が紐づくことを防止すること ・移行プログラムの設計、開発の際、他人のデータと統合されないよう設計、開発、テストで品質を高めるとともに、記録照会機能を利用した現新一致検証を行うことで、データ移行の正確性を確認すること 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。

【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) 年金業務システム(フェーズ2)を開発し、特定個人情報を移行する際のリスク対策等、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・見直しを行い、今後リスクを相当程度変動させ得る事実関係の変更が生じ、当該変更に応じたリスク対策を講ずる際などには、必要な特定個人情報保護評価を適切に実施する体制を、有効に機能させることが重要である。

(4) 情報漏えい等に対するリスク対策については、特に統合データベースへのアクセスに係るリスク対策や、フェーズ2への移行の際の委託や電子記録媒体等の取扱いのリスク対策等については、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。また、リスク対策の見直しにあたっては、知見を有する外部機関などから意見を聴取することなども有用であるため、必要に応じて検討すること。

(5) 年金業務システム(フェーズ2)は大規模かつ長期の開発となるため、上記について、開発中の要件変更や技術の進歩等により不断の見直し・検討を行うことに加え、事務フローの変更や新たなリスク対策が生ずることとなった場合は、必要に応じて評価の再実施を行うことが重要である。