

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 | 平成29年4月5日 |
| 概要説明日 | 平成29年4月10日 |

(目次)

| | |
|-------------------------------|----|
| ○ 全体的な事項 | 1 |
| ○ 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 | 10 |
| ○ 総評 | 11 |
| ○ 個人情報保護委員会による審査記載事項..... | 11 |

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。 | — | — | — | — | 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の開発は、平成29年2月までにシステムの要件定義が終了し、平成29年4月下旬以降からプログラミングの開始を予定しており、実施時期については委員会と協議を行ったところである(平成29年3月6日付けで個人情報保護委員会了承済み)。 |
| (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。 |
| (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。 |

| 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 ～ P.5 | 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.8 | 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.6 ～ P.8 | 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.9 | 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 | |
| (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.55 ～ P.70 | 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.70 | 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.70 | Ⅳ 1. ② | 問題は 認めら れない | |
| | | 72. 特定個人情報を取り扱 う従業者等に対する教育・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.70 | 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.72 | 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。 |

| 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 |
|--|--------|------------|------|----|-----------|--|
| (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 | <p>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。</p> |

| 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.35 | 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、(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) 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(以下「2共済」という。) への回付も含む。)を行う際に使用するこ と、(ウ) 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、 (エ) 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 審査に必要な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。 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。 |
| | | 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.35 | 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.38 | 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.39 | 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.39 | 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.40 P.41 | 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.41 | 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.41 | 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.42~P.47 | 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.42~P.47 | 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.42~P.47 | II 4. ⑧ | 該当なし | |
| | | 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.48~P.51 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.51 | 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.52 | 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.52 | 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.53 | 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.55 | 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.56 | 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.56 | 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.57 | 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.57 | 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.57 | 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.58 | 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.58 | 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、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.59 | Ⅲ 3. リスク1: | 問題は認められない | 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、所属する職員のリモートワーク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。 不正に複製されるリスク対策として、①個人情報を扱う業務端末から電子媒体へ情報の書き出しができないよう原則的にシステム上制限すること、②電子媒体への情報の書き出しの際は、台帳記載・承認・暗号化・ログ検証等を行ってい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、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.59 | 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.59 | 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.59 | 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.59 | 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.60 | 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.60 | 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.60 | 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.60 | 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.61 | 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、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与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.61 | 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.61 | 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.61 | 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.61 | 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.61 | 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.61 | 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.61 | 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.62 | 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。 |
| | | 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.64 | 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.64 | 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.64 | 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.64 | 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.65 | 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.65 | 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.65 | 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.66 | Ⅲ 7. リスク1: ⑤ | 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。 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、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、管理者へ通知する機能を構築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.66 | 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.66 | 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.67 P.68 | 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.68 | 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.68 | 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.69 | 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.69 | 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. 事業主等や市区町村から電子媒体で特定個人情報を入手する際に、情報漏えいが発生しないように講じ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> | P.58 | Ⅲ 2. リスク4: | 問題は認められない | <p>①事業主等が提出する電子媒体は、情報の暗号化を行った上で提出することを推奨していること、②市区町村が提出する電子媒体は、情報の暗号化を行った上で提出されること、③電子媒体が提出された際は、管理簿に記載し、鍵付の保管庫で保管・管理すること等が具体的に記載されている。</p> |
| | | <p>75. 権限のない者が、特定個人情報を保有するシステムを不正に使用しないように講じ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> | P.59 | Ⅲ 3. リスク2: | 問題は認められない | <p>①アクセス権限が必要となった利用者に対して、事務に必要な業務権限を確認し、必要なアクセス権限のみを付与すること、②職員の退職により不要となったユーザID及び生体認証は速やかに失効すること等が具体的に記載されている。</p> |
| | | <p>76. 委託先に対して、特定個人情報を適切に取り扱わせるために講じ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> | P.58 P.61 P.70 | Ⅲ 2. リスク4: Ⅲ 4. Ⅳ 2. | 問題は認められない | <p>①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ること、②特定個人情報にアクセスできる者を必要最小限に特定すること、③特定個人情報ファイルへのアクセス記録を取得し、委託業務以外の作業を実施していないか確認すること等が具体的に記載されている。</p> |
| | | <p>77. 特定個人情報の利用記録の確認及び自己点検・監査、従業員に対する教育・啓発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> | P.60 P.70 | Ⅲ 3. リスク2: Ⅳ 1. Ⅳ 2. | 問題は認められない | <p>①部署ごとに所属する職員の利用記録を処理結果として作成し、管理者が確認すること、②毎月、機構全職員に対して自己点検を行わせ、点検結果を個人情報保護管理責任者に提出させること、③計画的に監査を行い確認を行っていること、④職員に対し、毎年度個人情報保護研修の受講を義務付けていること等が具体的に記載されている。</p> |

【総評】

- (1) 公的年金業務等に関する事務においては、年金業務システム及び社会保険オンラインシステムを使用し、特定個人情報ファイルである公的年金業務等に関するシステム関連ファイルを適切に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、公的年金業務等に関するシステム関連ファイルについて、特定個人情報ファイルの内容、特定個人情報の流れ、使用するシステムの機能並びに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) 特定個人情報を入手する際に用いる電子媒体のリスク対策、アクセス権限の管理、特定個人情報の取扱いの委託及び利用記録の確認方法等、本評価対象事務において特に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)

- 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。特に電子媒体やアクセス権限の管理については、各拠点においても適切な管理を確実に実行することが重要である。
- 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。
- 特定個人情報の取扱いについては厳格な対応が求められるため、職員への教育・研修を実務に即して実施するとともに、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、実効性のある自己点検・監査を実施することが重要である。
- 情報漏えい等に対するリスク対策については、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とともに、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構築することが重要である。