

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
日本私立学校振興・共済事業団における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
日本私立学校振興・共済事業団
提出日
平成27年11月6日
概要説明日
平成27年11月10日

(目次)

○ 全体的な事項	1
○ 年金ファイル	7
○ 評価実施機関に特有の問題に対するリスク対策	15
○ 総評	16
○ 特定個人情報保護委員会による審査記載事項	16

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、日本私立学校振興・共済事業団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、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公的年金業務システムの開発は、平成27年6月までにシステムの要件定義、平成27年11月下旬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の上、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、日本私立学校振興・共済事業団のホームページにて、30日間実施した。 なお、寄せられた意見はなかった。

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	日本私立学校振興・共済事業団における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	日本私立学校振興・共済事業団における公的年金業務等に関する事務に係る番号制度への対応は日本私立学校振興・共済事業団企画室が行っており、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。

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	<p>日本私立学校振興・共済事業団における公的年金業務等に関する事務の内容について、平成28年1月からの社会保障・税番号制度の導入に伴い、学校法人等及び加入者の適用事務、年金裁定・給付事務、記録照会・年金相談事務において、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。</p> <p>また、別添1の事務の内容において、学校法人等から提出される加入者の資格取得報告書により個人番号を入手し、生涯共済番号と紐付けた上で年金ファイルに登録する等、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、行政機関が発行する添付書類の省略が図られるメリット等が具体的に記載されている。</p>
		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.4 ～ 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.4 ～ 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.11	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
<p>(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>	—	—	P.21 ～ P.35	Ⅲ、Ⅳ	問題は 認めら れない	<p>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。</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
<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>⑨特定個人情報ファイルの取扱いについて自己点検・監査や従業員に対する教育・啓発を行っているか。</p>	<p>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>	P.35	IV 1. ①	問題は認められない	<p>自己点検及び監査については、個人情報管理規程に基づき、情報セキュリティに関する自己点検計画を策定し、年に1回以上、全職員及び派遣職員に対し自己点検シートを配布の上、自己点検を行わせ、点検結果を提出させていること、毎年監査対象部署を決めて、2年間に全部署を、又は必要に応じて、内部監査時にセキュリティ監査を実施していること等が具体的に記載されている。</p> <p>従業員に対する教育については、個人情報管理規程に基づき、全職員及び派遣職員を対象にした年1回以上のセキュリティ研修とセキュリティ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。</p>
		<p>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>	P.35	IV1. ②	問題は認められない	
		<p>72. 特定個人情報を取り扱う従業員等に対する教育・啓発や違反行為をした従業員等に対する措置について具体的に記載しているか。</p>	P.35	IV 2.	問題は認められない	
		<p>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>	P.37	VI 2. ⑤	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>(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>	—	—	P.1	表紙	問題は認められない	<p>日本私立学校振興・共済事業団における公的年金業務等に関する事務については、日本私立学校振興・共済事業団が、年金事務における特定個人情報ファイルを取り扱うに当たり、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しかねないことを理解し、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
<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>	<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>	P.12	II 2. ③	問題は認められない	<p>特定個人情報を保有する理由、個人番号は生涯共済番号と紐付けて管理を行うこと、個人番号は年金相談・照会事務、源泉徴収票出力情報、情報提供ネットワークシステムを介した情報提供・照会において使用すること、システムデータはマシン室で一括管理をしていること等、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、保管、消去)について具体的に記載されている。</p>
		<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>	P.12	II 2. ④	問題は認められない	
		<p>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>	P.13	II 3. ④	問題は認められない	
		<p>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>	P.13	II 3. ⑤	問題は認められない	
		<p>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>	P.13	II 3. ⑥	問題は認められない	
		<p>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>	P.14	II 3. ⑧	問題は認められない	
		<p>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>	P.14	II 3. ⑧	該当なし	
		<p>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>	P.14	II 3. ⑧	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
		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.15 ～ P.17	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.15 ～ P.17	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.15 ～ P.17	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。	別紙 P.1 ～ P.16	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.18	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.19	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.19	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.19	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.21	Ⅲ 2. リスク1:	問題は認められない	<p>対象者以外の情報の入手を防止するための措置として、個人番号カード(写し)等の添付書類を求めること、手続に必要な事項のみを規定した様式により情報を入手すること等から、必要な情報以外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。</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、システム入力後の申請書等は所定の保管場所に保管するとともに、他の文書と混同することを防止する措置を講ずること、地方公共団体情報システム機構との連携においては、専用回線である住民基本台帳ネットワークシステムを用いるほか、情報の暗号化を実施する等の措置を講ずる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.21	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.21	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.22	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が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.22	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.22	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.22	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.22	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.23	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について、全ての端末において、ログイン時には、物理認証装置を挿入し(キーを挿入しないと利用不可)、ID・パスワードによる認証を実施していること、業務システムのログイン時に、端末ログインとは別のユーザ認証を実施しており、職務の利用権限によって、業務システムの利用できる機能を系統的に制限し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について、特定個人情報は、ホストコンピュータで管理しているため、一般職員の端末から特定個人情報をダウンロードできないこと、源泉徴収票データ、支払報告書データ及びバックアップを作成するために特定個人情報を媒体に書き出す操作は、システムの運用スケジュールにより、マシン室内の端末で操作され、アクセスログが残され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.23	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.23	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.23	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.23	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.24	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.24	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.25	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.25	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.26	Ⅲ 4. 情報管理 体制	問題は認められない	<p>申請書等の記載内容のパンチ業務等を委託することとしており、調達時の確認として、委託先は、ISMS等の認証資格を取得するなど情報セキュリティの管理体制が確保された業者とすること、契約書に基づき、秘密情報の取扱い、安全管理体制の整備等の実施を遵守する旨の秘密保持約定書の提出を求めること等が具体的に記載されている。</p> <p>委託先は、委託業務の実施に当たり、特定個人情報ファイルにアクセスできる担当者を必要最小限に限定し、当該者のみアクセス権限を付与すること、オンラインで参照した場合は、使用者及び参照箇所のログを取得し、一定期間保管すること、契約の履行において知り得た秘密を他に漏らしてはならない旨を契約書に定めており、委託先から他者への特定個人情報の提供を認めていない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.26	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.26	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.26	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.26	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.27	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進め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.27	Ⅲ 4. 再委託	該当なし	
		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.27	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.28	Ⅲ 5. リスク1:	問題は認められない	国税庁への公的年金等の源泉徴収票の提出においては、提出する媒体の規格が定められており、暗号化した上で、提出時にチェックシートによるチェックを行い、媒体と共に提出し受領印を取得していること、市町村(地方税電子化協議会)への公的年金等支払報告書の提出においては、提出する媒体の仕様が定められており、暗号化した上で、提出時は公的年報情報電子媒体送付書に双方で確認印を押印して提出し、返還時は公的年報情報電子媒体返還書に双方で確認印を押印して返還を受け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.28	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用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.28	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.28	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:	問題は認められない	<p>情報提供ネットワークシステムを通じた特定個人情報の入手は、資格取得報告書の報告から年金決定に至るまでの事務の流れの中でシステム的に行われるようにすることで、報告と離れた形で個別に照会が行われないようにする等、目的外の入手が行われることへのリスク対策が具体的に記載されている。</p> <p>公的年金業務システムでは、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容を記録し、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制する仕組みとすること等が具体的に記載されている。</p> <p>公的年金業務システムと情報提供ネットワークシステム(コアシステム)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ネットワーク(文部科学省ネットワーク、政府共通ネットワーク)を利用し、漏えい、紛失のリスクに対応すること等が具体的に記載されている。</p>
		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:	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.30	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.30 ~ P.31	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.31	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.31	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.31	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.32	Ⅲ 6. 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
	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.33	Ⅲ 7. リスク1: ⑤	問題は認められない	物理的対策として、全ての端末において、ログイン時は専用の物理認証装置を利用している(キーを挿入しないと利用不可)こと、マシン室(サーバの設置場所を含む。)の入退室は、入退室管理システムによりチェックを行っていること、バックアップ媒体は運用サイクルに沿って利用され、利用既定回数に達した媒体は、破壊、破棄を実施しており、廃棄履歴管理もを行っ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、外部からの不正アクセスを防止するため、インターネット利用端末と業務システム利用端末とは、ネットワークが分離されていること、情報漏えい対策のために、シンクライアント端末を導入している(データはサーバ室に保持し、操作端末はローカル保存不可かつデータ持出し不可)こと、システムに関係のない端末からアクセスできないよう、ファイアウォール等でアクセス制御してい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.33	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.34	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.34	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.34	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.34	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.34	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.34	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. データエントリー業務、システム維持管理等業務、電話相談業務等、複数の業務委託先において特定個人情報ファイルが適切に取り扱われるために講じているリスク対策は具体的に記載されているか。また、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.26 ～ P.27</p>	<p>Ⅲ 4.</p>	<p>問題は認められない</p>	<p>いずれの委託先も、ISMS等の認証資格を取得するなど情報セキュリティ管理体制が確保されている業者とし、契約の履行において知り得た秘密を他に漏らしてはならない旨を契約書に定めてい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にアクセスできる担当者を必要最小限に限定すること、オンラインで参照した場合は、使用者及び参照箇所のログを取得し、一定期間保管すること、職員が特定個人情報の取扱い状況を定期的に現地調査にて確認すること等が具体的に記載されている。</p>
		<p>75. 年金裁定事務、年金相談事務等において、ヒューマンエラー防止の観点から、システム面で講じているリスク対策は具体的に記載されているか。また、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.25 P.33 ～ P.34</p>	<p>Ⅲ 3. リスク4: Ⅲ 7.</p>	<p>問題は認められない</p>	<p>全ての端末において、ログイン時には、物理認証装置を利用し(キーを挿入しないと利用不可)、業務運用中に離席する場合は、物理認証装置を抜くことでシステムから自動ログオフすること、業務システムのログイン時にユーザ認証を実施し、職務の利用権限によって、業務システムの利用できる機能を制限していること、特定個人情報へのアクセスログを記録していること等が具体的に記載されている。</p>
		<p>76. 公的年金業務システムからインターネットへの流出やデータの複製等を防止するための対策は具体的に記載されているか。また、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.33</p>	<p>Ⅲ 7. リスク1:</p>	<p>問題は認められない</p>	<p>インターネット利用端末と業務システム利用端末とはネットワークが分離されていること、システムに関係のない端末からアクセスできないようファイアウォール等でアクセス制御していること、シンクライアント端末を導入している(データはサーバ室に保持し、操作端末はローカル保存不可かつデータ持出し不可)こと等が具体的に記載されている。</p>

【総評】

- (1) 日本私立学校振興・共済事業団における公的年金業務等に関する事務においては、公的年金業務システムを使用し、特定個人情報ファイルである年金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年金ファイルについて、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) 委託先に対するリスク対策、業務システム利用端末におけるシステム上のリスク対策、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。

【特定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. 特定個人情報保護委員会の承認)

- 日本私立学校振興・共済事業団における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、インターネット利用端末と業務システム利用端末とはネットワークが分離されていること等の措置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。
- 特定個人情報ファイルの取扱いに係る規程の改正及び職員への教育については、早急かつ確実に実行する必要がある。
- 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。