

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	産業機械健康保険組合における 適用、給付及び徴収関係事務 全項目評価書
評価実施機関名	産業機械健康保険組合
提出日	令和2年2月19日
概要説明日	令和2年2月26日

(目次)

○ 全体的な事項	1
○ 健康保険基幹情報ファイル.....	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、産業機械健康保険組合(以下「組合」という。)が適用、給付及び徴収関係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	特定個人情報保護評価書の見直しに伴うしきい値判断の結果の変更後、速やかに評価が再実施されている。
(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、組合のホームページにて、31日間実施した。 なお、寄せられた意見はなかった。
(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	適用、給付及び徴収関係事務について、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	適用、給付及び徴収関係事務における番号制度への対応は、総務部総務課が行っており、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、責任を負うことができる部署である。
(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.2 ~ P.3	I 1. ②	問題は認められない	適用、給付及び徴収関係事務において、それぞれ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、被保険者及び事業主から提出される各種届出により個人番号を入手し、識別番号と紐付けた上で基幹システムに登録する等、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、加入者が申請届出をする際に添付することが定められている他の情報保有機関発行の書類について、中間サーバー等を通じて情報提供ネットワークシステムで情報照会することにより、添付書類の省略が図ら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.3	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.3	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.4	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.4	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.8	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.19 ～ P.36	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) 特定されたり 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。	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.35	Ⅳ 1. ①	問題は 認めら れない	自己点検については、定期的に評価書記 載事項や規程に基づいて特定個人情報の 取扱い及び業務運用が行われているか、 チェックリストを作って各担当部署内で点検 し報告すること、また、監査については、定 期的に内部監査責任者及び内部監査人が 特定個人情報の取扱いや運用実態を監査 すること等が具体的に記載されている。
(11) 記載されたり 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。		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.35	Ⅳ 1. ②	問題は 認めら れない	従業者に対する教育・啓発については、 職員等の採用・就任時に、特定個人情報 管理規定及び取扱要領等の教育を行うこ と、最低年1回、特定個人情報取扱いの教 育研修を全職員を対象に行うこと、教育研 修未受講者に対して再受講の機会を付与 す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.36	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.38	Ⅵ 2. ⑤	問題は 認めら れない	寄せられた意見がなかったことが記載さ 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	組合は、適用、保険給付及び保険料等徴 収関係事務において、特定個人情報ファ イルを取り扱うに当たり、その取扱いが個人 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認識し、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適切な措置を講じ、 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。

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.9	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、加入者資格情報の更新管理、給付申請帳票の資格情報確認・審査、保険料徴収等の事務処理で、個人番号を識別番号と紐付けて必要な情報の検索・参照を行うこと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管理区域内に設置したサーバ及び外部のデータセンターに設置したサーバに保管すること、個人番号が記載された届出書等の帳票類及び電子記録媒体もセキュリティ管理区域内に設置した保管庫に保管すること、基幹システム専用端末や基幹システムに接続していない事務用PC、個人ロッカー・事務デスク内には一切保管・留置しないよう規制していること等、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、提供、保管・消去)について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.9	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.10	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.11	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.11	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.11	II 3. ⑧	問題は認められない	
		14. 特定個人情報を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.11	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.11	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.12 ～ P.15	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.12 ～ P.15	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.12 ～ P.15	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.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.16	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.17	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.17	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.17	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.19	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リスク対策として、①個人番号の記載が必要な届出書の種類、様式、記載説明を明示して周知すること、②事業所が被保険者から個人番号の提出を受ける際、番号法第16条(本人確認の措置)に則り本人確認を実施するよう通知し、これを求めること、③地方公共団体情報システム機構から社会保険診療報酬支払基金(以下「支払基金」という。)経由で機構保存本人確認情報を入手する場合には、組合の照会要求に該当した機構保存本人確認情報のみ入手するため、対象者以外の情報入手が行われることはないこと等が具体的に記載されている。</p> <p>入手の際の特定個人情報の漏えい・紛失を防止するリスク対策として、本人から入手した特定個人情報が記載された届出書は特定個人情報受付システムに登録して保管庫に施錠保管し、届出書を使用後は文章保存管理規程に従って保管及び廃棄措置すること、事業所から入手した電子記録媒体は特定個人情報受付システムに登録して保管庫に施錠保管し、保管する必要がない使用済の電子記録媒体は廃棄の記録を管理簿を用いて行い、シュレッダーで粉碎し破棄すること、中間サーバー等と組合の通信は、IP-VPNによる閉域サービスを使用することで、データ転送時の通信内容秘匿、盗聴防止の対応をしてい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.19	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.20	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.20	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.20	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.20	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.21	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.21	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.21	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、基幹システムについては、全てのシステム利用者にユーザID、パスワードを発行してログイン認証を行うこと、共有のユーザIDは使用しないこととすること、アクセス権限が付与されたシステム利用者以外は個人番号を取り扱えないようシステム管理・制御機能に設定して、システム的に制御すること、アクセス権限を付与するシステム利用者は最小限に限定すること、パスワードに有効期間を設けて、定期的に変更するようシステム的に制御す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.21	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.22	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.22	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.23	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.23	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.24	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.24	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.25	Ⅲ 4. 情報管理体制	問題は認められない	基幹システムの導入、保守・点検、障害調査等を委託することとしているが、委託先は認証資格を取得する等、情報保護管理について十分な体制である者を選定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、担当する従業員を必要最低限に限定し、特定個人情報ファイルへのアクセス権限を系統的に制限すること、操作ログ等を記録し一定期間保管して、不正な取扱いがされてないことを定期及び不定期に調査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.25	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.25	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.27	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.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:	該当なし	
		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:	該当なし	
		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:	該当なし	—
		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:	該当なし	
		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.28	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。		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力する際に、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.29	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情報照会・提供は、支払基金を經由して行うこととしており、目的外の特定個人情報の入手を防止するリスク対策として、支払基金の職員が統合専用端末を利用して情報照会依頼及び情報照会結果の確認等を行う際、ログイン時の職員認証の他に、統合専用端末の操作履歴(操作ログ)を中間サーバー等で記録しているため、不適切な統合専用端末の操作や、不適切なオンライン連携を抑制する仕組みになっていること等が具体的に記載されている。</p> <p>情報提供ネットワークとの接続に伴うその他のリスク対策として、中間サーバー等と情報提供ネットワークシステムの間は、高度なセキュリティを維持した厚生労働省統合ネットワークを利用することにより、安全性を確保していること、中間サーバー等と医療保険者等の通信は、IP-VPNによる閉域サービスを使用することで、データ転送時の通信内容秘匿、盗聴防止の対応をしてい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力する際に、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力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.29	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力した後、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.29	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力する際に、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	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.30	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.30	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.31	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.32	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.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.33	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.33	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.33	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	

物理的対策として、セキュリティ管理区域において、IDカード、パスワード認証による立入りの制限や入退室記録管理を行うこと、監視カメラの設置やサーバーラックの施錠を行うこと等が具体的に記載されている。

技術的対策として、基幹システム等においては、不正アクセス防止のため、ファイアウォールを設置すること、基幹システムをインターネット等に接続する情報システムから分離すること等が具体的に記載されている。

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. 中間サーバー等を利用して他の機関に情報連携する際、基幹システム専用端末と統合専用端末との間でフラッシュメモリを用いた特定個人情報の授受が行われるが、権限の無い者による不正な操作及びフラッシュメモリの紛失等による漏えいを防止するリスク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>P.31</p>	<p>Ⅲ 6. その他のリスク対策</p>	<p>問題は認められない</p> <p>基幹システム専用端末と統合専用端末との間の情報授受は、業務を行う職員を必要最小限に限定し、アクセス権限が付与された者以外が情報授受に係る業務ができないようシステムの的に制御すること、フラッシュメモリは、パスワード認証付きのものを使用し、システム管理責任者が設定した媒体以外は使用できないようシステムの的に制御すること、さらに、フラッシュメモリの利用記録等は管理簿に記載し、利用後は保管庫に施錠保管すること等が具体的に記載されている。</p>

【総評】

- (1) 適用、給付及び徴収関係事務においては、基幹システム及び中間サーバー等を使用し、特定個人情報ファイルである健康保険基幹情報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健康保険基幹情報ファイルについて、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) 中間サーバー等を利用し、情報連携を行う際に使用するフラッシュメモリに係るリスク対策、特定個人情報ファイルの消去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) 適用、給付及び徴収関係事務の内容、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、基幹システムをインターネット等に接続する情報系システムから分離する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。
- (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。