資料１－２

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
関東ITソフトウェア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
関東ITソフトウェア健康保険組合

提出日
令和６年１月29日

概要説明日
令和６年１月31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、関東ITソフトウェア健康保険組合（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	特定個人情報の入手方法の追加（ファイル交換サービスの利用開始）を3月上旬に予定しており、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、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。 なお、再実施の理由となる事務については、新たにファイル交換サービスを利用して特定個人情報を入手するものであるが、当該事務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	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、企画部が行っており、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.3 ～ P.4	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こと、マイナポータル経由で提出される電子申請データをレセオン端末等で受け取り、基幹システムへ登録すること、さらに、ファイル交換サービス経由で提出される届出書をシンクライアントPCでダウンロードし、ダウンロードした届出書をフラッシュメモリに一時記録して、フラッシュメモリから基幹システム専用端末で基幹システムへ登録すること等、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、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、書類の添付を省略することができる等、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.5 ～ P.6	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.5 ～ 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
(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.24 ～ P.50	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.49	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個人情報保護管理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、情報セキュリティ基本方針に基づき、定期的に監査責任者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。 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、個人情報保護管理規程及び取扱要領等の教育を行うこと、最低毎年2回、役職員全員に特定個人情報取扱いの教育を行うこと、ファイル交換サービス運用事業者においては研修やOJTで、機密情報の取扱いやセキュリティに関する教育を行う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.49	Ⅳ1. 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.49 ～ P.50	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.52	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。

特定個人情報ファイル
（健康保険基幹情報ファイル）

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.12	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、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、個人番号を既存システムの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。 また、特定個人情報の保管・消去について、特定個人情報ファイルは外部のデータセンター内のサーバに保管し、個人番号が記載された届出書等の帳票類、電子記録媒体及びフラッシュメモリ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、電子申請された届出書について、レセオン端末で受け取った後、レセオン端末内から速やかに削除すること、さらに、ファイル交換サービス上に保存されるファイルはフラッシュメモリにダウンロード後、速やか（ダウンロード当日）に消去すること、消去漏れ防止のため自動削除機能を設定し、設定期間経過後に自動消去すること、フラッシュメモリに一時的に記録した特定個人情報は、使用の都度速やかに完全消去すること等、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）について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.12	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.14	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.14	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.14	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.15	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.15	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.15	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.16 ～ P.18	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.16 ～ P.18	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.16 ～ P.19	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.20 P.65 ～ P.66	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.21	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.21	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.22	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.22	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.24	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、本人から郵送又は対面により個人番号を入手する場合は、番号法第16条（本人確認の措置）に則り本人確認書類を提出させて本人確認を行い、併せて資格情報を参照して個人番号の入手が必要な加入者であることを確認すること、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。 不適切な方法で入手が行われるリスク対策として、事業所がファイル交換サービスで届出書を届け出る場合、ファイル交換サービス上に事業所がアップロードした届出書のみ受け付けること等が具体的に記載されている。 個人番号の真正性の確認方法として、提出された届出書から個人番号を入力して、チェックデジットや既に登録されている別人の個人番号と同番号でないことを基幹システムでチェック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、ファイル交換サービスを利用する場合、事前に組合と共有したパスワードを使用し、ファイル交換サービス上にファイルをアップロードすること、組合は共有したパスワードにて届出書をダウンロードして入手すること、ファイル交換サービスの通信経路は、HTTPS通信（TLS1.2）により暗号化を施しており、送受信の際、最新のパターンファイルで自動的にウイルスチェックを実施すること、電子記録媒体及びフラッシュメモリによる入手は、暗号規約や標準フォーマット等が定められた仕様に基づきパスワード設定、暗号化を行い、書留等を用いて搬送すること、事業所から入手した電子記録媒体及びフラッシュメモリは媒体管理簿に記載し、速やかに保管庫に施錠保管すること、保管する必要がない使用済の電子記録媒体はメディアシュレッダー、フラッシュメモリは溶解廃棄にて物理的に破壊して廃棄し、廃棄記録を管理簿に記載すること、電子申請された届出書の入手についてはIP-VPNによる閉鎖された通信回線を利用し、通信内容の秘匿や盗聴防止の対応がされていること、シンクライアントPCにはファイアウォール、ウイルス対策ソフトを導入してパターンファイルを随時更新しておく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.24	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.25	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.25	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.25	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.26	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.27	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.28	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.29	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、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、事務の目的を超えて公金受取口座情報等が利用できないように、公金受取口座情報等に不必要な情報が紐付かないようにシステムで制御されていること、操作ログは一定期間保管し、不正アクセスや事故が疑われるときに点検し追跡できるようにすること等が具体的に記載されている。また、ファイル交換サービスサーバーについては、ファイル交換サービスの運用担当者がサーバーへアクセスする際は、事前レビュー・承認を必要とするほか、専用のGWサーバー上で認証し、接続制限とログの取得を実施すること、IPアドレス制限機能を利用して、許可された環境外からのログインを禁止すること、シンクライアントPCについては、ファイル交換サービスにおいて自動ロック機能を利用して、使わなくなったアカウントを失効すること、操作ログを確認し、不正操作の痕跡を1ヶ月ごとに確認すること、ファイルのバックアップ、電子記録媒体及びフラッシュメモリによる届出書等データの読出しについては、アクセス権限を付与された最小限の職員だけが当該端末を操作できるようアクセス制御すること等が具体的に記載されている。 特定個人情報ファイルが不正に複製されるリスク対策として、ファイルのバックアップ、基幹システム専用端末と統合専用端末との情報授受及び電子申請された届出書の入手については、操作を行う端末を限定し、アクセス権限を付与された最小限の職員だけが当該端末を操作できるようアクセス制御すること、電子記録媒体又はフラッシュメモリに複製を行う場合は、不必要な複製を制限するため事前に管理者の承認を得て、利用記録等を媒体管理簿に記載し、処理に使用後フラッシュメモリからは速やかにデータを完全消去し、返却された電子記録媒体又はフラッシュメモリを管理者が確認して、保管庫に施錠保管すること、シンクライアントPCにおいて定期的に操作ログをチェックし、必要のないアクセスが行われていないか、データ抽出等の不正な持出しが行われていないかを監視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.29	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.29	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.30	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.30 ～ P.31	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.32	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.32 ～ P.33	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.34 ～ P.35	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.35	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.36	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、担当する従業者を必要最小限に限定し、取扱い範囲やアクセス権限等を明確にすること、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又は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.36	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.36	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.36 ～ P.37	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.37	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.37	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.37	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.38	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.39	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.39	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.39	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.39	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.39	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.40	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、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止する仕組みになっていること、本人が給付金の請求をする申請書の受取口座情報を記載する欄に、登録されている公金受取口座情報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、公金受取口座情報を照会する仕組みとすることにより、目的外の公金受取口座情報の入手を防止すること、チェック欄にて利用希望が確認された場合に限り、公金受取口座情報を照会する仕組みについては、書類の記載内容を健保業務システムに登録した際の職員のチェック及び事務所管課の上長の決裁時のチェックを行うと共に、健保業務四システムに、口座の利用希望があった加入者のみの情報照会を行う仕組みを構築すること、加入者が誤った認識で申請し、本意ではない情報連携を行うことを防ぐため、公金受取口座制度の趣旨や事務での利用方法をホームページ及び申請書様式へ記載すること等が具体的に記載されている。 情報提供ネットワークシステム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との間は、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、IPSecによる暗号化された通信経路を使用することで、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、さらに、サーバー間接続について、組合と情報連携サーバー間及び情報連携サーバーと中間サーバー間の通信は、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、情報連携サーバーの運用・保守事業者は個人番号を内容に含む電子申請データを取り扱わない契約とし、情報連携サーバーの運用・保守事業者が個人番号等にアクセスできないようにアクセス制御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.40	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.40	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.41	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.41	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.41	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.42	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.42	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.43	Ⅲ 7. リスク1: ⑤	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（特定個人情報を取り扱う事務を実施する区域）においては、基幹システムの専用端末をインターネット等外部ネットワークと隔離すること等、データセンターのサーバ室や組合事務所の保管庫においては、IDカードによる立入の制限、入退室記録管理等を行うこと、ファイル交換サービスサーバーにおいては、敷地内に赤外線監視カメラを設置し、24時間有人監視を実施し、不正入館を防ぐこと、入館時には顔写真付身分証明書による本人確認に加え、マントラップゲートを設置し、共連れを防ぐこと等が具体的に記載されている。 技術的対策として、基幹システム等及び電子申請された届出書を受け付けるレセオン端末においては、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、基幹システム等及びレセオン端末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こと、基幹システムで保管している「個人番号管理ファイル」は、暗号化処理を行い、情報漏えい等の防止の措置を講ずること、ファイル交換サービスサーバーにおいては、サーバー上の特定個人情報はAESで暗号化されて保存されること、クラウドサービスプロバイダとしてのクラウドサービスの情報セキュリティ管理に関する国際規格「ISO/IEC 27017」及びクラウドサービスの個人情報管理に関する国際規格「ISO/IEC 27018」の認証を取得していること、ファイル交換サービスにおいては、多段にファイアウォールを設置し、必要な通信以外を遮断すること、不正アクセスの検知時は、必要に応じた被害の拡大防止、調査、対策を実施すること、WAF（Web Application Firewall）を設置し、不正な攻撃パターンを検知すること、検知後は必要に応じた対策を実施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への対策として、ファイル交換サービスに係るファイルは、フラッシュメモリへダウンロードするため、シンクライアントPC上にデータが保存されず、特定個人情報が消去されずいつまでも存在することはないこと、ファイル交換サービス上に保存されるファイルは、速やかに消去すること、消去漏れ防止のため自動削除機能を設定すること、フラッシュメモリに一時的に記録した特定個人情報は、使用の都度速やかに完全消去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、ファイル交換サービスサーバー上のファイルは暗号化されて保存されるため、ファイル交換サービスを提供する事業者は、ファイル交換サービスサーバー上の情報を取り扱わず、閲覧することができない仕様になっ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.43 ～ P.45	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.46	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.46	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.46	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.46	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.46 ～ P.47	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.47 ～ P.48	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。	75. 事業主からの届出書等の入手にあたり、ファイル交換サービスを利用するが、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.27 ～ P.28 等	Ⅲ2. リスク4 等	問題は認められない	・ファイル交換サービスの通信経路は、HTTPS通信（TLS1.2）により暗号化を施しており、送受信の際、最新のパターンファイルで自動的にウイルスチェックを実施すること ・シンクライアントPCにはファイアウォール、ウイルス対策ソフトを導入してパターンファイルを随時更新しておくこと ・ファイル交換サービスにおいて、自動ロック機能を利用して、使わなくなったアカウントを失効すること ・ファイルのバックアップ、電子記録媒体及びフラッシュメモリによる届出書等データの読出しについては、アクセス権限を付与された最小限の職員だけが当該端末を操作できるようアクセス制御すること ・導入するファイル交換サービスは、クラウドサービスの情報セキュリティ管理に関する国際規格「ISO/IEC 27017」、政府情報システムのためのセキュリティ評価制度（ISMAP）等の認証を取得し、特定個人情報の暗号化や不正アクセスの検知等の機能を有していること ・操作ログを確認し、不正操作の痕跡を1ヶ月ごとに確認すること ・ファイル交換サービスに係るファイルは、フラッシュメモリへダウンロードするため、シンクライアントPC上にデータが保存されず、特定個人情報が消去されずいつまでも存在することはないこと ・ファイル交換サービス上に保存されるファイルはフラッシュメモリにダウンロード後、速やか（ダウンロード当日）に消去すること ・消去漏れ防止のため自動削除機能を設定すること 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)　適用、給付及び徴収関係事務においては、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)　ファイル交換サービスを利用した事業主からの届出書等の入手等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、基幹システム等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)　特定個人情報の入手時に活用するファイル交換サービスにおいては、十分にセキュリティが確保されている必要があり、情報漏えい等に対するリスク対策については、新規のリスク対策が確実に実行されるように研修や説明会を通じた組合、事業所の職員への意識づけを行うとともに、評価書に記載されたリスク対策が既存、新規問わず適切に実行されているかの確認を実施していくことが重要である。

(5)　上記について、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。