

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	簡易生命保険契約に係る保険金等の支払に関する 支払調書データ(税務署提出用)作成事務
評価実施機関名	独立行政法人郵便貯金簡易生命保険管理・郵便局ネットワーク支援機構
提出日	令和7年11月5日
概要説明日	令和7年11月19日

(目次)

○ 全体的な事項	1
○ 特定個人情報ファイル(支払調書)	4
○ 評価実施機関に特有の問題に対するリスク対策	12
○ 総評	13
○ 個人情報保護委員会による審査記載事項	13

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10-1(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、独立行政法人郵便貯金簡易生命保険管理・郵便局ネットワーク支援機構(以下「機構」という。)が簡易生命保険契約に係る保険金等の支払に関する支払調書データ(税務署提出用)作成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	e-私書箱(以下「認定クラウド」という。)利用に係るパラメータ設定等の適用は令和7年12月に予定されており、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、機構のホームページにて、30日間以上実施した。 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	簡易生命保険契約に係る保険金等の支払に関する支払調書データ(税務署提出用)作成事務について、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	簡易生命保険契約に係る管理業務については、機構が監督、指導等の責任を負いつつ、郵政民営化法等の定めにより株式会社かんぽ生命保険(以下「かんぽ生命」という。)が機構の委託を受けて行うこととされている。 簡易生命保険契約に係る保険金等の支払に関する支払調書データ(税務署提出用)作成事務における番号制度への対応は機構保険部業務課が行っており、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。

審査の観点 (指針第10-1(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.2	I 1. ②	問題は認められない	簡易生命保険契約に係る保険金等の支払に関する支払調書データ(税務署提出用)作成事務の内容について、平成28年1月以降支払事由が発生する生命保険契約の一時金の支払調書及び生命保険契約の年金の支払調書において、保険契約者及び保険金等受取人の個人番号を記載するために、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て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、かんぽ生命支店及び本社法人営業開発部(以下「支店等」という。)並びに郵便局窓口で顧客が保険金等の支払請求のために来局した際に、個人番号の提示を受け、端末機に入力し、かんぽ生命情報管理センターにおいて支払調書データを作成すること等が記載されており、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。
		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.3	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.3	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.5 ～ P.9	I (別添1)	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.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。

審査の観点 (指針第10-1(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。	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。	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.36	IV 1. ①	問題は認められない	自己点検について、支店等において、四半期ごとに、個人情報保護に係る項目について、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。 監査について、機構では監督方針に基づき、委託先であるかんぽ生命本社及び支店並びに再委託先である日本郵便株式会社(以下「日本郵便」という。)本社、支社及び郵便局を対象として、特定個人情報の取扱いを含めた委託業務の実施状況の監査を実施していることや、不適正事例が発生した場合には、発生原因等を分析し、必要に応じて一層の再発防止策を講じるよう指導するなど、改善に向けた取組強化及び改善状況の検証を行っていること、その結果は担当の理事を議長、担当の部長を構成員とする管理業務推進会議において各種の課題・問題を分析、把握し、理事長に報告す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.36	IV 1. ②	問題は認められない	従業員に対する教育について、委託先であるかんぽ生命では、個人情報保護・情報セキュリティマニュアル等を策定し、同マニュアル等に基づく年度計画により定期的に研修・点検等を実施していることや、全社員を対象に実施している個人情報保護等を含むコンプライアンスに関するeラーニング研修で、実施期間中に数回実施状況を管理者に連絡し、管理者等から受講を促すよう指導・周知を行い、受講率が100%になる取組を行っていること、再委託先である日本郵便では、採用時の教育及び定期的な教育・訓練等、社員に対し安全管理措置の周知徹底、教育及び訓練を行い、個人情報保護等を含むコンプライアンスに関する研修の欠席者に対して、別途、同様の研修を実施することとし、欠席者へのフォローアップを行ってい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.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	寄せられた意見は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。	—	—	—	表紙	問題は認められない	機構は、簡易生命保険契約に係る保険金等の支払に関する支払調書データ(税務署提出用)作成事務における特定個人情報ファイルの取扱いに当たり、同ファイルの取扱いがお客様の財産、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ることをもって、お客様の財産、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
(支払調書)

審査の観点 (指針第10-1(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.10	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、簡易生命保険契約に係る保険金等の支払に関する支払調書データ(税務署提出用)を作成するために使用すること、郵政民営化法等の定めにより、かんぽ生命は機構の委託を受けて簡易生命保険管理業務を行い、その一部を日本郵便に再委託することが義務付けられていること等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.10	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.11	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.12	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.12	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.12	Ⅱ 3. ⑧	該当なし	
		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.12	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.12	Ⅱ 3. ⑧	該当なし	
		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.13	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.13	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.13	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.14	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.14	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.16	Ⅱ 6. ①	問題は認められない	特定個人情報の保管・消去について、特定個人情報は、セキュリティゲートを設けて入退室を行っている建物にあって、入退室管理を行っている部屋に設置したメインフレームに個別のマスタファイルとして保管し、暗号化とアクセス制限を施していること、保存期間経過後システムの的に削除することを記載する等、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。
		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10-1(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.19	Ⅲ 2. リスク1:	問題は認められない	対象者以外の情報の入手を防止するための措置として、保険金等支払請求の際、請求人が正当な権利を有している者であることの確認を行うことが前提であることから、対象者以外の情報を入手しないよう措置していることや、スマートフォン又はポスタルタブレットPCによる個人番号のオンライン申告が行われる際には、認証アプリの処理において、二次元バーコード内に格納されている対象者の生年月日及び性別とスマートフォン又はポスタルタブレットPCにかざされたマイナンバーカードの生年月日及び性別を照合し、両者が一致しなければ個人番号の入手ができないよう措置している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.19	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.20	Ⅲ 2. リスク2:	問題は認められない	必要な情報以外を入手することを防止するための措置として、保険証書記号番号を入力し、保険契約の契約者又は保険金等受取人であることを確認の上で個人番号を入力することから、必要最小限の情報のみ入力するよう措置していること等が具体的に記載されている。
		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.21	Ⅲ 2. リスク3:	問題は認められない	特定個人情報の正確性確保の措置として、スマートフォン又はポスタルタブレットPCによる個人番号のオンライン申告が行われる際には、公的個人認証サービスを利用した実存(本人)確認を行うことから、特定個人情報の正確性について確保されていること、特定個人情報の取得はマイナンバーカードのICチップを読み取る方法で行うため、誤入力が発生しないこと等が具体的に記載されている。
		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.21	Ⅲ 2. リスク3:	問題は認められない	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、特定個人情報について控え及び写しを作成しないこととしているほか、携帯端末機(PT5)は紙媒体を出力する機能を有していないこと、端末機(ポスタルタブレットPC、かんぽPC(事務)、CTM、JP-PC(3001)は紙媒体への出力機能を有しているが、個人番号が記録されたデータについては紙媒体で出力できないようシステムで制御していること、かんぽ総合情報システム(個人番号等管理マスタ)からのデータのダウンロードや電子記録媒体への出力もできないよう措置していること等が具体的に記載されている。
		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.21	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.22	Ⅲ 2. リスク4:	問題は認められない	その他のリスク対策として、公的個人認証サービスを提供するプラットフォーム事業者を委託PF事業者として選定しているほか、委託PF事業者とかんぽ生命間においては、特定個人情報に暗号化を施すとともに、通信については専用線を敷設し、セキュアな環境でデータを入手していること等が具体的に記載されている。
		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.22	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10-1(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.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対策について、ユーザIDに必要最低限の権限を付与し、事務処理上必要のないデータへのアクセスを制限していること、認定クラウド事業者及び認定クラウドの運用管理業者において、Firewallによるアクセス制限、WEBアプリケーションのぜい弱性攻撃遮断、侵入検知システムによる運用監視・アクセス記録といった仕組みにより、情報漏えい、なりすまし等の不正行為を防止する措置を講じ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について、個人番号等管理マスタに関するアクセス権については、ユーザIDが払い出され、辞令簿により指定を受けた者のみ有しており、特定個人情報等の取扱いに関する留意事項等について、定期的な研修等を行うこと、かんぽ総合情報システムはインターネットと分離されており、不正アクセスやウイルスによって情報を抜き取られることはないこと、さらに、携帯端末機(PT5)については、複数の要素(IDとPW、IDと生体認証)によるログイン承認を行っており、ログインできなければ、かんぽ総合情報システムへ接続できないこと、携帯端末機の通信不可とすることも可能で、通信を不可とすればかんぽ総合情報システムへ接続できないこと、かんぽPC(事務)では、光学式ドライブからのデータ書き込みは申請により許可された社員のみに制限されており、USBドライブからのデータ書き込みも申請により許可された社員、端末及びUSB機器のみに制限されていること、マイナンバーカード登録業務を行う拠点に設置するかんぽPC(事務)では、光学式ドライブを配備しないこと、JP-PC(3001)又はポスタルタブレットPCでは、光学式ドライブからのデータ書き込み及びUSBドライブからのデータ書き込みは行えないように制限されていること、専用端末(スタンドアロン)では、管理者の許可を得た者のみしか入退室できないようICカードによる入退室チェック機能による施錠管理(入退室時にICカードをかざし、暗証番号を入力しないと入退室できない仕組み)が措置されたセキュリティルームに設置されていること、複製を行う際には必ず立会者を設けて実施すること、専用端末の使用履歴のログは管理者により定期的(3か月毎)に監査を行う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.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.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.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.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10-1(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	機構とかんぼ生命における委託契約書の中で、守秘義務及び顧客情報の管理等に関する事項を約定し、機構はかんぼ生命に対して、個人情報保護管理体制を確認できるよう関連規程類等の提出を求め、必要な措置が講じられていることを確認していること、また、これらの状況について、委託先であるかんぼ生命及び再委託先である日本郵便を対象として、特定個人情報の取扱いを含めた委託業務の実施状況を監査するとともに、必要な場合にはかんぼ生命の外部委託先に対しても機構が直接実地での監査を行うことができるように措置していること、さらに、かんぼ生命は、個人データの安全管理を図るための内部管理体制として、会社全体の個人情報の保護に関する事務を統括する個人情報保護統括責任者のほか、各部署に個人情報の保護に関する事務を管理する者を配置し、個人情報の適切な保護と取扱いを行っていること等が具体的に記載されている。 かんぼ生命契約サービス部の一部の社員のみ閲覧権限を与えること、特定個人情報の取扱いの記録について、プログラム処理にて毎日自動で抽出し、確認する運用としていることのほか、業務委託契約書等において、特定個人情報の持ち出しの禁止等を規定していること等が具体的に記載されている。 特定個人情報の提供ルールについて、クラウド提出を行う際は、ネットワークに一切接続されていない専用端末(スタンドアロン)にて管理されている支払調書データからクラウド提出する支払調書データを抽出し、その内容を複数人で点検・確認するとともに、認定クラウドへのデータ連携においても、データ送信先に誤りがないか等について、操作ログを複数人で点検・確認すること等が具体的に記載されている。 再委託先においても、特定個人情報の適正な取扱いに関するガイドライン等で求められている必要かつ適切な安全管理措置を講ずることを義務付けていること等が記載されている。
		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.25	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.25	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.26	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.26	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.26	Ⅲ 4. その他のリスク	該当なし	

審査の観点 (指針第10-1(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.27	Ⅲ 5. リスク1:	問題は認められない	特定個人情報の提供又は移転の記録については、特定個人情報が含まれている支払調書データの電子媒体においては、媒体管理簿へデータ内容、利用目的、作成年月日、移送日、移送先、担当者名等を記載していることや、媒体管理簿は、管理者が月に1回以上点検・確認を行っていること等が具体的に記載されている。 提供・移転に関するルールの内容やルール遵守の確認方法については、電子媒体での搬送に当たって、セキュリティ確保のため、データの暗号化及び搬送容器の施錠を行い、郵便物の追跡が行える方法により郵送すること、暗号化した専用回線(閉塞網)を用いて、認定クラウドへデータ連携すること等が記載されている。
		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.27	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.27	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.28	Ⅲ 5. その他のリスク	該当なし	

審査の観点 (指針第10-1(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:	該当なし	—
		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:	該当なし	
		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:	該当なし	
		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.29	Ⅲ 6. リスク4:	該当なし	
		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.29	Ⅲ 6. リスク5:	該当なし	
		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.29	Ⅲ 6. リスク6:	該当なし	
		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.29	Ⅲ 6. リスク7:	該当なし	
		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.29	Ⅲ 6. その他の リスク	該当なし	

審査の観点 (指針第10-1(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.30 ～ P.31	Ⅲ 7. リスク1: ⑤	問題は認められない	物理的対策として、個人番号等管理マスターはセキュリティゲートを設けて入退室を行っている建物で管理しており、入退室管理を行っている部屋に設置したメインフレームに個別のマスターファイルとして保管していること、インターネットと分離されていることや、支払調書データを作成しCD等の電子記録媒体に出力する際には暗号化を施していること、あらかじめ設置されている端末機又は持込みを許可された電子記録媒体を除き、機器等の持込みを禁止していること、専用端末(スタンドアロン)と専用端末(閉域網通信用)をICカードによる入退室管理を行っているセキュリティルームに設置し、ワイヤーチェーンによる施錠を施して、防犯カメラによる監視を行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.32 ～ P.33	Ⅲ 7. リスク1: ⑥	問題は認められない	また、個人番号は紙媒体で取得・保管を行わないこと等が具体的に記載されている。 技術的対策として、端末機(ポスタルタブレットPC、CTM又はJP-PC(3001))へのログイン時には正当なIDとPWが必要であり、かんぽPC(事務)又は携帯端末機(PT5)へのログイン時には正当なIDとPW又は正当なIDと生体認証が必要なこと、端末機(ポスタルタブレットPC、かんぽPC(事務)、CTM、JP-PC(3001))又は携帯端末機(PT5)に特定個人情報を入力した場合は即時に暗号化を行っていること、端末機とシステム間の通信については暗号化及びセキュアな通信を行った上でかんぽ生命情報管理センター側に送信し端末内部には情報を残さないようにしていること等が具体的に記載されている。
		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	また、端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務))又は携帯端末機(PT5)とかんぽ総合情報システム間においては特定個人情報に暗号化を施している。 ポスタルタブレットPC及びかんぽPC(事務)については、ログオン時またはシャットダウン時に端末機内のローカルデータが自動削除されること等が具体的に記載されている。
		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	ポスタルタブレットPC、かんぽPC(事務)は社外からインターネットに接続される場合についても考慮し、セキュリティ基盤を構築の上、既存の回線設備と併用し、セキュリティの強化を図っている。 専用端末(閉域網通信用)は個人情報保持せず、専用線(閉域網)を使用して暗号化通信を行い、送信作業のログは送信の都度、管理者がチェックすること等が具体的に記載されている。

審査の観点 (指針第10-1(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
		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	インターネット機能やメール機能を有するポスタルタブレットPC、かんぽPC(事務)、JP-PC(3001)については、上記の技術的対策に加え、インターネット分離の仕組みや許可されたWEBサイト以外からのファイルのダウンロード・アップロードの制限を行うことでマルウェア感染による情報漏えいリスクを低減していること、社外あてメールのパスワード付与や宛先に上長を含めない場合にメールの送信を不可とすること、即時の検知や防御、ネットワーク遮断等の対応を行うEDR(エンドポイントディテクション&レスポンス)の導入と、EDRで検知したインシデント発生時の初動対応、影響調査、結果報告までをサポートするMDR(マネージド・ディテクション&レスポンス)サービスの運用により、標的型攻撃やランサムウェアの脅威に対応していること等が具体的に記載されている。 業務用携帯電話(スマートフォン)を使用する場合に備え、業務用携帯電話にはキャッシュの自動削除、スクリーンショット不可の制限をかけていること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、電子記録媒体の廃棄に当たっては事前に情報セキュリティ統括室に廃棄申請を行い、許可を受けた上で実施すること、廃棄後は電子記録媒体管理簿に廃棄の旨を記録していること、かんぽ総合情報システムへの登録が完了した個人番号データは、かんぽ生命から送信する「削除対象番号を示すキー情報と削除指示」のファイルに基づき、一時保管された日付の翌営業日中に消去すること等が具体的に記載されている。
		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.35	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10-1(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. 支払調書データを複製する専用端末(スタンドアロン)、クラウド提出を実行する専用端末(閉域網通信用)及び認定クラウドから特定個人情報が漏えい等するリスクを軽減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.23 P.24 P.32 P.33 等	Ⅲ3. リスク2 Ⅲ3. リスク4 Ⅲ7. リスク1⑥ 等	問題は認められない	専用端末から不正に複製される等により特定個人情報ファイルが漏えい等するリスクへの対策として、 ・専用端末(スタンドアロン及び閉域網通信用)は、管理者の許可を得た者のみしか入退室できないよう施錠管理(入退室時にICカードをかざし、暗証番号を入力しないと入退室できない仕組み)が措置されたセキュリティルームに設置されること ・専用端末(閉域網通信用)は、端末に個人情報を保持せず、専用線(閉域網)を使用し暗号化通信を行うこと 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。 権限のない者によって不正に認定クラウドに保存した特定個人情報にアクセスされるリスクへの対策として、 ・Firewallによるアクセス制限、WEBアプリケーションのぜい弱性攻撃遮断、侵入検知システムによる運用監視・アクセス記録を行うこと ・認定クラウドの運用管理業者が本番環境にアクセスした場合には、アクセス履歴が記録されること 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) 簡易生命保険契約に係る保険金等の支払に関する支払調書データ(税務署提出用)作成事務においては、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) 個人番号の収集・登録におけるリスク対策、機構が委託先及び再委託先に講じるリスク対策等、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) 簡易生命保険契約に係る保険金等の支払に関する支払調書データ(税務署提出用)作成事務の内容、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、かんぽ総合情報システムはインターネットと分離されていること、専用端末(閉域網通信用)は個人情報を保持せず、専用線(閉域網)を使用して暗号化通信を行う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。
- (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、機構が委託先及び再委託先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に変更が生じ、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) 委託先事業者による特定個人情報ファイルの適正な取扱いに関して、クラウドサービスに係る安全管理措置も含め、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。