特定個人情報保護評価書（基礎項目評価書）

評価書番号	評価書名
33	国民年金関係事務　基礎項目評価書

個人のプライバシー等の権利利益の保護の宣言

香芝市は、国民年金関係事務における特定個人情報ファイルの取扱いにあたり、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する。

特記事項	―

評価実施機関名

香芝市長

公表日

令和7年7月28日

［令和6年10月　様式2］

Ⅰ　関連情報

1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	国民年金関係事務
②事務の概要	国民年金制度は、日本国憲法第25条第2項に規定する理念に基づき、老齢、障害又は死亡によって国民生活の安定が損なわれることを国民の共同連帯によって防止し、もって健全な国民生活の維持、向上に寄与することを目的（国民年金法第1条）とし、そのための必要な給付を行う（同法第2条）制度である。 国民年金の事業は国が管掌している（同法第3条）ので、年金給付をはじめ積み立金の運用等一切については、国が責任をもって運営する責務があるが、国民年金の被保険者及び受給権者は多岐にわたっているので適用（加入・喪失）関係、給付関係等事務の一部は市町村長に委任されている。そのため、香芝市において、「国民年金法」及び「行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）」（以下「番号法」という。）の規定に従い、特定個人情報を以下の国民年金事務で取り扱う。 ①住民からの取得届、転入届に基づき、個人を単位とする国民年金加入資格得喪情報等を編成し、被保険者名簿を作成 ②転居届、転出届、出国届等の届出又は職権に基づく被保険者名簿への住民記録情報の記載、削除又は記載の修正若しくは変更 ③保険料納付困難者等からの免除等申請受付 ④老齢基礎年金ほか請求手続に関する受付 ⑤受理した届書等の日本年金機構への送付及び厚生労働大臣への報告 ⑥年金事務所が実施する未納者対策に係る適用勧奨や免除勧奨に必要な情報提供
③システムの名称	国民年金システム、社会保険オンラインシステム

2. 特定個人情報ファイル名
被保険者台帳情報ファイル

3. 個人番号の利用	
法令上の根拠	・番号法第9条、番号法第19条第1号及び第2号 ・番号法別表の46の項

4. 情報提供ネットワークシステムによる情報連携		
①実施の有無	[　　未定　　]	＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	―	

5. 評価実施機関における担当部署	
①部署	市民環境部　市民課
②所属長の役職名	市民環境部　市民課長

6. 他の評価実施機関
―

7. 特定個人情報の開示・訂正・利用停止請求	
請求先	〒639－0292　奈良県香芝市本町1397番地 香芝市役所　市民環境部　市民課 電話：0745－76－2001

8. 特定個人情報ファイルの取扱いに関する問合せ	
連絡先	〒639－0292　奈良県香芝市本町1397番地 香芝市役所　市民環境部　市民課 電話：0745－76－2001
9. 規則第9条第2項の適用	**[　　]適用した**
適用した理由	

Ⅱ　しきい値判断項目

1. 対象人数			
評価対象の事務の対象人数は何人か		[　1万人以上10万人未満　]	＜選択肢＞ 1) 1,000人未満（任意実施） 2) 1,000人以上1万人未満 3) 1万人以上10万人未満 4) 10万人以上30万人未満 5) 30万人以上
	いつ時点の計数か	令和7年4月1日 時点	
2. 取扱者数			
特定個人情報ファイル取扱者数は500人以上か		[　500人未満　]	＜選択肢＞ 1) 500人以上　2) 500人未満
	いつ時点の計数か	令和7年4月1日 時点	
3. 重大事故			
過去1年以内に、評価実施機関において特定個人情報に関する重大事故が発生したか		[　発生なし　]	＜選択肢＞ 1) 発生あり　2) 発生なし

Ⅲ　しきい値判断結果

しきい値判断結果
基礎項目評価の実施が義務付けられる

Ⅳ リスク対策

1. 提出する特定個人情報保護評価書の種類		
	[基礎項目評価書]	<選択肢> 1) 基礎項目評価書 2) 基礎項目評価書及び重点項目評価書 3) 基礎項目評価書及び全項目評価書
2)又は3)を選択した評価実施機関については、それぞれ重点項目評価書又は全項目評価書において、リスク対策の詳細が記載されている。		

2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）		
目的外の入手が行われるリスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

3. 特定個人情報の使用		
目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
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への対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

4. 特定個人情報ファイルの取扱いの委託		[○]委託しない
委託先における不正な使用等のリスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[ ]提供・移転しない
不正な提供・移転が行われるリスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

6. 情報提供ネットワークシステムとの接続		[○]接続しない（入手） [○]接続しない（提供）
目的外の入手が行われるリスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
不正な提供が行われるリスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

7. 特定個人情報の保管・消去		
特定個人情報の漏えい・滅失・毀損リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている

8. 人手を介在させる作業		[　　]人手を介在させる作業はない
人為的ミスが発生するリスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
判断の根拠	特定個人情報の取扱いに関しては、マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドラインに従い、いかなる局面においても複数人での確認を徹底しているため、人為的ミスが発生するリスクへの対策は十分であると考えられる。 〇複数人での確認を徹底している事例 ・提供された本人情報のデータベースへの入力 ・特定個人情報の記載がある書類等の鍵付きキャビネットでの保管 ・個人番号及び本人情報が記載された書類の廃棄 ■上述に加えて、移行作業時におけるリスクに対する措置としては、以下を講じる。 ①データ抽出・テストデータ生成及びデータ投入に関する作業者の権限管理 ・特定個人情報ファイルの取扱権限を持つIDを発効し、必要最小限の権限及び数に制限する。 ・作業者は範囲を超えた操作が行えないようシステム的に制御する。 ・移行以外の目的・用途でファイルを複製しないよう、作業者に対して周知徹底を行う。 ②移行データ ・移行作業に用いる電子記録媒体に格納したファイルは暗号化し、追記できない状態とする。 ・作業終了後は、不正使用がないことを確認した上で破棄し、破棄日時・破棄方法を記録する。 ・システム間でのデータ転送により移行作業を行う場合は、専用線による接続を行い、外部からの読み取りを防止する。 ③テストデータ ・特定個人情報をマスキング対象項目と定め仮名加工を施し、必要最小限のテストデータのみを生成する。 ④相互牽制 ・移行作業は二人で行う相互牽制の体制で実施する。	

9. 監査			
実施の有無	[〇] 自己点検	[　　] 内部監査	[　　] 外部監査

10. 従業者に対する教育・啓発		
従業者に対する教育・啓発	[　　十分に行っている　　]	＜選択肢＞ 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない

11. 最も優先度が高いと考えられる対策	[　　]全項目評価又は重点項目評価を実施する
最も優先度が高いと考えられる対策	[8) 特定個人情報の漏えい・滅失・毀損リスクへの対策] ＜選択肢＞ 1) 目的外の入手が行われるリスクへの対策 2) 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスクへの対策 3) 権限のない者によって不正に使用されるリスクへの対策 4) 委託先における不正な使用等のリスクへの対策 5) 不正な提供・移転が行われるリスクへの対策(委託や情報提供ネットワークシステムを通じた提供を除く。) 6) 情報提供ネットワークシステムを通じて目的外の入手が行われるリスクへの対策 7) 情報提供ネットワークシステムを通じて不正な提供が行われるリスクへの対策 8) 特定個人情報の漏えい・滅失・毀損リスクへの対策 9) 従業者に対する教育・啓発
当該対策は十分か【再掲】	[　　十分である　　]　＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
判断の根拠	■香芝市における措置 ①技術的安全管理措置 ・国民年金システムへのアクセス時における二要素認証、ウィルス対策ソフトウェアの導入、外部ネットワークと遮断された庁内ネットワーク ②移行作業時に関する措置 ・移行作業に用いる電子記録媒体に格納したファイルは暗号化し、追記できない状態とし、作業終了後は不正使用がないことを確認した上で破棄し、破棄日時、破棄方法を記録する。 ■ガバメントクラウドにおける措置 ①物理的安全管理措置 ・ガバメントクラウドについては政府情報システムのセキュリティ制度(ISMAP)のリストに登録されたクラウドサービスから調達することとしており、システムのサーバ等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行う。 ・事前に許可されていない装置等に関しては、外部に持出できないこととする。 ②技術的安全管理措置 ・国及びクラウド事業者は利用者のデータにアクセスしない契約等とする。 ・地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用について【第2.1版】」(デジタル庁。以下「利用基準」という。)に規定する「ASP」をいう。以下同じ。)又はガバメントクラウド運用管理補助者(利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。)は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ・クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ・クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ・地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ・ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ・地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ・地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。

変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成30年6月29日	Ⅱ．1．対象人数　いつ時点の計数か	平成29年3月31日　時点	平成30年3月31日　時点	事後	
平成30年6月29日	Ⅱ．2．取扱者数　いつ時点の計数か	平成29年3月31日　時点	平成30年3月31日　時点	事後	
令和1年6月10日	Ⅱ．1．対象人数　いつ時点の計数か	平成30年3月31日　時点	平成31年4月1日　時点	事後	
令和1年6月10日	Ⅱ．2．取扱者数　いつ時点の計数か	平成30年3月31日　時点	平成31年4月1日　時点	事後	
令和1年6月10日	特記事項	国民年金に関する事務では、業務の一部を外部業者に委託しているため、業者選定の際に業者の情報保護体制を確認し、併せて秘密保持に関しても契約に含めることで万全を期している。	(削除)	事後	
令和1年6月10日	Ⅳ　リスク対策	(記載なし)	(項目を追加)	事後	様式変更に伴う修正
令和2年6月12日	Ⅱ．1．対象人数　いつ時点の計数か	平成31年4月1日　時点	令和2年4月1日　時点	事後	
令和2年6月12日	Ⅱ．2．取扱者数　いつ時点の計数か	平成31年4月1日　時点	令和2年4月1日　時点	事後	
令和3年6月22日	Ⅱ．1．対象人数　いつ時点の計数か	令和2年4月1日　時点	令和3年4月1日　時点	事後	
令和3年6月22日	Ⅱ．2．取扱者数　いつ時点の計数か	令和2年4月1日　時点	令和3年4月1日　時点	事後	
令和4年6月24日	Ⅱ．1．対象人数　いつ時点の計数か	令和3年4月1日　時点	令和4年4月1日　時点	事後	
令和4年6月24日	Ⅱ．2．取扱者数　いつ時点の計数か	令和3年4月1日　時点	令和4年4月1日　時点	事後	
令和5年8月4日	Ⅱ．1．対象人数　いつ時点の計数か	令和4年4月1日　時点	令和5年4月1日　時点	事後	
令和5年8月4日	Ⅱ．2．取扱者数　いつ時点の計数か	令和4年4月1日　時点	令和5年4月1日　時点	事後	
令和6年10月29日	Ⅰ関連情報 1．特定個人情報ファイルを取り扱う事務 ②事務の概要	市町村が行っている事務は、国民年金第1号被保険者の加入・喪失の届出、任意加入の申出、保険料の免除申請、学生納付特例申請、給付申請、老齢福祉年金や特別障害給付金の諸届出等々を受理し報告する事務並びに年金相談事務などである。 ・本事務における特定個人情報ファイルは、以下の事務に使用している。 ①各種申請書受理時の申請者の本人確認及び個人番号の真正性確認に利用する。 ②上記に挙げた当市の事務において取り扱う情報に対し、日本年金機構の指定により情報の提供を行うために使用する。	そのため、香芝市において、「国民年金法」及び「行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）」（以下「番号法」という。）の規定に従い、特定個人情報を以下の国民年金事務で取り扱う。 ①住民からの取得届、転入届に基づき、個人を単位とする国民年金加入資格得喪情報等を編成し、被保険者名簿を作成 ②転居届、転出届、出国届等の届出又は職権に基づく被保険者名簿への住民記録情報の記載、削除又は記載の修正若しくは変更 ③保険料納付困難者等からの免除等申請受付 ④老齢基礎年金ほか請求手続に関する受付 ⑤受理した届書等の日本年金機構への送付及び厚生労働大臣への報告 ⑥年金事務所が実施する未納者対策に係る適用勧奨や免除勧奨に必要な情報提供	事後	内容の整理
令和6年10月29日	Ⅰ関連情報 1．特定個人情報ファイルを取り扱う事務 ③システムの名称	(追加)	社会保険オンラインシステム	事後	修正
令和6年10月29日	Ⅰ関連情報 3．個人番号の利用	別表第一の31の項	別表の46の項	事後	法改正による修正
令和6年10月29日	Ⅰ関連情報 4．情報提供ネットワークシステムによる情報連携	実施しない	未定	事後	内容の整理
令和6年10月29日	Ⅱ．1．対象人数　いつ時点の計数か	令和5年4月1日　時点	令和6年4月1日　時点	事後	
令和6年10月29日	Ⅱ．2．取扱者数　いつ時点の計数か	令和5年4月1日　時点	令和6年4月1日　時点	事後	
令和6年10月29日	Ⅳ　リスク対策 5．特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）	提供・移転しない	十分である	事後	修正
令和7年6月27日	Ⅱ．1．対象人数　いつ時点の計数か	令和6年4月1日　時点	令和7年4月1日　時点	事後	
令和7年6月27日	Ⅱ．2．取扱者数　いつ時点の計数か	令和6年4月1日　時点	令和7年4月1日　時点	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年6月27日	Ⅳ　リスク対策 8．人手を介在させる作業	（追記）	■上述に加えて、移行作業時におけるリスクに対する措置としては、以下を講じる。 ①データ抽出・テストデータ生成及びデータ投入に関する作業者の権限管理 ・特定個人情報ファイルの取扱権限を持つIDを発効し、必要最小限の権限及び数に制限する。 ・作業者は範囲を超えた操作が行えないようシステム的に制御する。 ・移行以外の目的・用途でファイルを複製しないよう、作業者に対して周知徹底を行う。 ②移行データ ・移行作業に用いる電子記録媒体に格納したファイルは暗号化し、追記できない状態とする。 ・作業終了後は、不正使用がないことを確認した上で破棄し、破棄日時・破棄方法を記録する。 ・システム間でのデータ転送により移行作業を行う場合は、専用線による接続を行い、外部からの読み取りを防止する。 ③テストデータ ・特定個人情報をマスキング対象項目と定め仮名加工を施し、必要最小限のテストデータのみを生成する。 ④相互牽制 ・移行作業は二人で行う相互牽制の体制で実施する。	事前	標準化移行およびガバメントクラウドにおける措置の追記
令和7年6月27日	Ⅳ　リスク対策 11．最も優先度が高いと考えらる作業	特定個人情報の取扱いに関しては、マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドラインに従い、いかなる局面においても複数人での確認を徹底しているため、人為的ミスが発生するリスクへの対策は十分であると考えられる。 〇複数人での確認を徹底している事例 ・提供された本人情報のデータベースへの入力 ・特定個人情報の記載がある書類等の鍵付きキャビネットでの保管 ・個人番号及び本人情報が記載された書類の廃棄	■香芝市における措置 ①技術的安全管理措置 ・国民年金システムへのアクセス時における二要素認証、ウィルス対策ソフトウェアの導入、外部ネットワークと遮断された庁内ネットワーク ②移行作業時に関する措置 ・移行作業に用いる電子記録媒体に格納したファイルは暗号化し、追記できない状態とし、作業終了後は不正使用がないことを確認した上で破棄し、破棄日時、破棄方法を記録する。 ■ガバメントクラウドにおける措置 ①物理的安全管理措置 ・ガバメントクラウドについては政府情報システムのセキュリティ制度(ISMAP)のリストに登録されたクラウドサービスから調達することとしており、システムのサーバ等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行う。 ・事前に許可されていない装置等に関しては、外部に持出できないこととする。 ②技術的安全管理措置 ・国及びクラウド事業者は利用者のデータにアクセスしない契約等とする。 ・地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用について【第2.1版】」(デジタル庁。以下「利用基準」という。)に規定する「ASP」をいう。以下同じ。)又はガバメントクラウド運用管理補助者(利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。)は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ・クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ・クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ・地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ・ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ・地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ・地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。	事前	標準化移行およびガバメントクラウドにおける措置の追記