

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
19	国民健康保険関係事務 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

高島市は、国民健康保険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	なし
------	----

評価実施機関名

滋賀県高島市長

公表日

令和7年9月12日

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	国民健康保険関係事務
②事務の概要	国民健康保険法(昭和33年法律第192号)およ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(以下「番号法」という。)の規定に従い、特定個人情報を以下の事務で取り扱う。 1. 国民健康保険被保険者資格に関する事務 2. 国民健康保険被保険者証等に関する事務 3. 保険給付に関する事務 4. 国民健康保険被保険者を対象として実施する保健事業に関する事務 5. オンライン資格確認等システム稼働に向けた準備としての資格履歴管理事務、機関別符号の取得等事務(以下「オンライン資格確認の準備業務」という。)
③システムの名称	・国民健康保険システム ・国保総合システム ・高額療養費支給システム ・国保データベースシステム ・番号連携サーバー ・中間サーバー ・特定健診管理システム ・宛名システム ・個人住民税システム ・滞納管理システム ・国保情報集約システム

2. 特定個人情報ファイル名

・被保険者台帳情報ファイル ・給付情報ファイル ・滞納管理情報ファイル ・住登外者宛名番号管理関係ファイル

3. 個人番号の利用

法令上の根拠	・番号法 第9条第1項、別表の44の項 ・番号法別表第一の主務省令で定める事務を定める命令 第24条 (オンライン資格確認の準備業務) ・番号法 第9条第1項 別表の44の項 ・番号法別表第一の主務省令で定める事務を定める命令 第24条 ・国民健康保険法 第113条の3 第1項及び第2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	<選択肢> 1) 実施する 2) 実施しない 3) 未定 [実施する]
②法令上の根拠	・番号法第19条第8号に基づく主務省令第2条の表 (情報提供の根拠) 2、3、6、13、42、48、56、65、69、70、83、87、115、120、131、158、161の項 (情報照会の根拠) 69、70、71の項 (オンライン資格確認の準備業務) 番号利用法 附則第6条第4項(利用目的:情報連携のためではなくオンライン資格確認の準備として機関別符号を取得する等) 国民健康保険法第113条の3 第1項及び第2項

5. 評価実施機関における担当部署

①部署	市民生活部 保険年金課
②所属長の役職名	課長

6. 他の評価実施機関

なし	
7. 特定個人情報の開示・訂正・利用停止請求	
請求先	総務部 総務課 滋賀県高島市新旭町北畑565番地 電話:0740-25-8538
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	市民生活部 保険年金課 滋賀県高島市新旭町北畑565番地 電話:0740-25-8137
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、事務に必要な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	[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
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	[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
不正な提供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

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		
	[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
人為的ミスが発生するリスクへの対策は十分か		■ 経常作業時におけるリスクに対する措置としては、以下を講じている。 ① 特定個人情報の入手に関する対策 ・ 国民健康保険システムにおける措置：個人番号カードや本人確認書類の厳格な確認を行い、対象者以外の情報の入手を防止している。 ・ 4情報や保険証番号を用いて突合を行い、対象者以外の情報の入手を防止している。 ・ 複数職員によるチェックを行い誤入力を防止している。 ② 不正な使用を防止する対策 ・ 国民健康保険システムにおける措置：二要素認証やユーザIDによる識別とパスワードによる認証、利用可能な機能の制限を行っている。 ・ アクセス権限がなくなる場合は速やかにユーザIDの失効処理を行っている。 ・ 国保総合PCにおける措置：市ごとにユーザIDを割り当て、パスワードによるユーザ認証を実施している。 ③ 特定個人情報の使用に関する対策 ・ 国民健康保険システムにおける措置：個人番号利用以外の業務では、個人番号がマスキングされた画面表示としている。 ■ 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、以下を講じている。 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している。 ・ 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している。 ・ 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っている。 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している。 ・ 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・破棄方法を記録している。 ・ 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している。 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している。 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している
	判断の根拠	

9. 監査		
実施の有無	☐ 自己点検 ☐ 内部監査 ☐ 外部監査	
10. 従業員に対する教育・啓発		
従業員に対する教育・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	☐ 1) 目的外の入手が行われるリスクへの対策	
	<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、事務に必要な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) 従業員に対する教育・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	■高島市における措置 ①物理的安全管理措置 ・外部進入防止:警備キーによる施錠、日中は職員による監視、勤務時間外は施錠の上警備をセット ・入退館管理:事前申請の上台帳にて入退室の管理 ・持込・持出防止:持込・持出物は申請の上、サーバ室管理課職員の確認が必要 ②技術的安全管理措置 ・国民健康保険システムへのアクセス時における二要素認証 ・ウイ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 ③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。 ■中間サーバ・プラットフォームにおける措置 ①物理的安全管理措置 ・中間サーバ・プラットフォームはサーバ室に設置しており、サーバ室への入室を厳重に管理する。 ・特定個人情報は、サーバ室に設置された中間サーバのデータベース内に保存され、バックアップもデータベース上に保存される。 ②技術的安全管理措置 ・中間サーバ・プラットフォームでは庁内に設置のあるマイナンバー利用系端末とは物理的にネットワークを分離し運用するほか、使用可能な職員を限定することでアクセス制御を行っている。 ・中間サーバ・プラットフォームに副本登録データを移動する際は移動することが可能な記録媒体を情報システム部門保管のウイルス対策機能付きの媒体に限定している。 ■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アカウントによる制限を行っている。 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なっている。 ・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及びミドルウェアについて、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
令和3年4月1日	Ⅱ-1 じきい鑑判断項目 1. 対象人数	平成27年9月30日	令和3年4月1日	事後	
令和3年4月1日	Ⅱ-1 じきい鑑判断項目 2. 取扱者数	平成27年9月30日	令和3年4月1日	事後	
令和3年6月29日	Ⅱ-4②法令上の根拠	番号法第19条7号	番号法第19条8号	事前	令和3年9月1日付で施行される番号法の改正に向けた
令和8年4月1日	Ⅱ-7特定個人情報開示・訂正・利用停止請求	総務部 総務課 〒520-1592 滋賀県高島市新旭町北畑565番	総務部 総務課 〒520-1592 滋賀県高島市新旭町北畑565番	事後	
令和7年4月1日	Ⅱ-3法令上の根拠	・番号法 第9条第1項 別表第一(16.30の項) ・番号法別表第一の主務省令で定める事務を定める命令 第24条 ・国民健康保険法 第113条の3 第1項及び第2項	(オンライン資格確認の準備業務) ・番号法 第9条第1項 別表の44の項 ・番号法別表第一の主務省令で定める事務を定める命令 第24条 ・国民健康保険法 第113条の3 第1項及び第2項	事後	
令和7年4月1日	Ⅱ-4法令上の根拠	・番号法第19条第8号 別表第二 (別表第二における情報提供の根拠) 1.2,3,4,5,9,12,15,17,22,26,27,30,33,39,42,43,46,58,62,78,80,87,88,93,97,106,109,120の項 番号法別表第二の主務省令で定める事務及び情報を定める命令 第1条, 第2条, 第3条, 第4条, 第5条, 第6条, 第10条の2, 第11条の2, 第12条の3, 第15条, 第19条, 第20条, 第25条, 第33条, 第41条の2, 第43条, 第44条, 第46条, 第49条, 第53条, 第55条の2, 第59条3 (別表第二における情報照会)の根拠) 42,43,44,45の項 番号法別表第二の主務省令で定める事務及び情報を定める命令 第25条, 第25条の2, 第28条 (オンライン資格確認の準備業務) 番号利用法 附則第6条第4項(利用目的・情報連携のためではなくオンライン資格確認の準備として機関別符号を取得する等) 国民健康保険法第113条の3 第1項及び第2項	・番号法第19条第8号に基づく主務省令第2条の表 (情報提供の根拠) 2, 3, 6, 13, 42, 48, 56, 65, 69, 70, 83, 87, 115, 120, 131, 158, 161の項 (情報照会)の根拠) 69, 70, 71の項 (オンライン資格確認の準備業務) 番号利用法 附則第6条第4項(利用目的・情報連携のためではなくオンライン資格確認の準備として機関別符号を取得する等) 国民健康保険法第113条の3 第1項及び第2項	事後	
令和7年4月1日	Ⅱ-1 じきい鑑判断項目 1. 対象人数	令和3年4月1日	令和7年4月1日	事後	
令和7年4月1日	Ⅱ-1 じきい鑑判断項目 2. 取扱者数	令和3年4月1日	令和7年4月1日	事後	
令和7年4月1日	ⅡV-4特定個人情報ファイルの取扱いの委託	【○】委託しない	【 】 委託しない	事後	
令和7年4月1日	ⅡV-4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	—	十分である	事後	
令和7年9月12日	Ⅱ-1-③システムの名称	・国民健康保険システム・国保総合システム ・高額療養費支給システム・国保データベースシステム ・番号連携サーバー・中間サーバー ・特定健診管理システム・宛名システム ・個人住民税システム・滞納管理システム ・国保情報集約システム	・国民健康保険システム・国保総合システム ・高額療養費支給システム・国保データベースシステム ・番号連携サーバー・中間サーバー ・特定健診管理システム・宛名システム ・個人住民税システム・滞納管理システム ・国保情報集約システム	事前	
令和7年9月12日	Ⅱ-2 特定個人情報ファイル名	・被保険者台帳情報ファイル・給付情報ファイル・滞納管理情報ファイル	・被保険者台帳情報ファイル・給付情報ファイル・滞納管理情報ファイル・住登外者宛番号管理関係ファイル	事前	
令和7年9月12日	ⅡV-8 人手を介在させる作業判断の根拠	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機密的なガイドラインの留意事項等を遵守し、マイナンバーを取得する際には、原則、申請者から提供を受け、記載されたマイナンバーに誤りがないか確認を行っている。	■経常作業場におけるリスクに対する措置としては、以下を講じている ①特定個人情報の入手に関する対策 ・国民健康保険システムにおける措置：個人番号カードや本人確認書類の照会等を行い、対象者は外の情報の入手を防止している。 ・4機関・4機関等を用いて実地を行い、対象者は外の情報の入手を防止している。 ・2機関によるチェックを行い、個人番号カードを防止している。 ・2機関によるチェックを行い、個人番号カードを防止している。 ②国民健康保険システムにおける措置：二重登録やエラーによる重複などについて、利用可能な情報の照会を行っている。 ・アクセス権限がなくなる場合は速やかにユーザIDの失効処理を行っている。 ・国民健康保険システムにおける措置：市町村にユーザIDを割り当て、パスワードによる二重登録は発生している。 ③特定個人情報の提供に関する対策 ・国民健康保険システムにおける措置：個人番号利用以外の業務では、個人番号がマスキングされた画面表示としている。 ■上述に加えて、移行作業場におけるリスクに対する措置としては、以下を講じている。 ①データベース・システム生成及びデータ移行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い権限を持つ者を発注し、必要最小限の権限及び制限に制限している。 ・作業者は権限を越えたり操作を行えないようシステム的に制限している。 ②移行作業場 ・移行作業場における電子記録媒体に格納したファイルは暗号化し、遠隔で取り扱っている。 ・作業終了後、作業場を閉鎖し、作業場を閉鎖した上で確認し、確認日時・確認方法を記録している。 ③システム側でのデータ移行により移行作業を行う場合は、専用機による確認を行い、外部からの読み取りを防止している。 ④パスワード ・特定個人情報とマスキング対象項目とを別々に加工し、必要最小限のパスワードのみを生成している。 ・移行作業は二人で行う相互牽制の体制で実施している。		
令和7年9月12日	ⅡV-11 最も優先度が高いと考えられる対策判断の根拠	移行システムにおいて、必要最低限の人数、参照範囲となるよう、職員のアクセス権限を設定している。アクセス権限の所有者は、ID、パスワード等を適切に管理している。	■高島市における措置 ①物理的セキュリティ管理 ・物理的セキュリティ管理—による施設、日中は職員による監視、勤務時間外は施設の上層をセクト ・入退室管理、非常時の上層にて入退室の管理 ・待機・待出禁止・待機・待出物は申請の上、セクト管理職員の検閲 ②技術的セキュリティ管理 ・国民健康保険システムへのアクセス時における二重認証 ・ウイルス対策ソフトウェアの導入 ・外部ネットワークと接続された社内ネットワーク ③移行作業場に関する措置 ・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、遠隔で取り扱っている。 ・作業終了後、作業場を閉鎖し、作業場を閉鎖した上で確認し、確認日時・確認方法を記録している。 ④データベース ・特定個人情報とマスキング対象項目とを別々に加工し、必要最小限のパスワードのみを生成している。 ・移行作業は二人で行う相互牽制の体制で実施している。 ■バリエーションに関する措置 ①物理的セキュリティ管理 ・物理的セキュリティ管理—による施設、日中は職員による監視、勤務時間外は施設の上層をセクト ・入退室管理、非常時の上層にて入退室の管理 ・待機・待出禁止・待機・待出物は申請の上、セクト管理職員の検閲 ②技術的セキュリティ管理 ・国民健康保険システムへのアクセス時における二重認証 ・ウイルス対策ソフトウェアの導入 ・外部ネットワークと接続された社内ネットワーク ③移行作業場に関する措置 ・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、遠隔で取り扱っている。 ・作業終了後、作業場を閉鎖し、作業場を閉鎖した上で確認し、確認日時・確認方法を記録している。 ④データベース ・特定個人情報とマスキング対象項目とを別々に加工し、必要最小限のパスワードのみを生成している。 ・移行作業は二人で行う相互牽制の体制で実施している。		