

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
11	生活保護関係事務 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

葛城市は、生活保護に関する事務における特定個人情報ファイルの取扱いにあたり、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

奈良県葛城市長

公表日

令和7年8月1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	生活保護に関する事務
②事務の概要	<p>生活保護法による保護の決定及び実施並びに就労自立給付金の支給並びに保護に要する費用の返還又は徴収金の徴収に関する次の事務を行う。</p> <p>1 生活保護の決定及び実施等に関する事務</p> <p>①要保護者の申請に対し、生活保護法に基づき、保護を決定し、実施する。</p> <p>②職権により、要保護者に対する保護の開始又は変更を決定し、実施する。</p> <p>③保護の停止又は廃止に関する事務を行う。</p> <p>④就労自立給付金の支給の申請の受理、決定及び支給に関する事務を行う。</p> <p>⑤生活保護法63条の保護に要する費用の返還に関する事務を行う。</p> <p>⑥生活保護法77条1項又は第78条1項から第3項までの徴収金の徴収に関する事務を行う。</p> <p>2 医療扶助のオンライン資格確認導入に関する事務</p> <p>①生活保護システムから医療保険者等向け中間サーバー等への特定個人情報の連携に関する事務</p> <p>②医療保険者等向け中間サーバー等における資格履歴の管理に関する事務</p> <p>③医療保険者等向け中間サーバー等における本人確認事務に関する事務</p> <p>④医療保険者等向け中間サーバー等における機関別符号の取得等に関する事務</p> <p>(②～④は委託元:葛城市福祉事務所、委託先:社会保険診療報酬支払基金)</p> <p>特定個人情報ファイルは、上記の事務実施において、申請の受理、申請に係る事実についての審査、申請に対する応答を行うために使用する。</p>
③システムの名称	生活保護システム、番号連携サーバ(団体内統合宛名システム)、中間サーバー、統合専用端末、医療保険者等向け中間サーバー
2. 特定個人情報ファイル名	
生活保護システム	
3. 個人番号の利用	
法令上の根拠	<p>・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、「番号利用法」という。)第9条第1項、第2項及び別表第一の第15項</p> <p>・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別表第一の主務命令で定める事務を定める命令</p> <p>・葛城市行政手続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に基づく個人番号の利用に関する条例第4条</p>
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	<div> <div><選択肢></div> <div> <div>1) 実施する</div> <div>2) 実施しない</div> <div>3) 未定</div> </div> </div> <div>[実施する]</div>
②法令上の根拠	<p>1.情報提供の根拠</p> <p>・番号利用法19条第8号,第9号及び別表第二(別表第二における情報提供)</p> <p>9,10,14,16,18,20,24,26,27,28,30,31,37,38,42,50,53,54,61,62,64,70,87,90,94,104,106,108,113,116,120の項</p> <p>・番号利用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</p> <p>第8条,第9条,第11条,第12条,第13条,第14条,第17条,第19条,第20条,第21条,第22条,第23条,第24条,第25条,第26条の4,第27条,第28条,第32条,第33条,第35条,第39条,第44条,第47条,第52条,第53条,第55条,第58条,第59条の2の2,第59の3条,</p> <p>2.情報照会を行う根拠</p> <p>・番号利用法19条第8号,9号及び別表第二 26の項</p> <p>・番号利用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19条各号</p> <p>・葛城市行政手続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に基づく個人番号の利用に関する条例第4条別表第2(第4条関係)</p>
5. 評価実施機関における担当部署	
①部署	保健福祉部 社会福祉課
②所属長の役職名	社会福祉課長

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	葛城市役所 総務部 総務課 住所: 奈良県葛城市柿本166番地 電話: 0745-69-3001
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	葛城市役所 保健福祉部 社会福祉課 住所: 奈良県葛城市柿本166番地 電話: 0745-69-3001
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	[1,000人未満(任意実施)]	<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5月30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5月30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
特定個人情報保護評価の実施が義務付けられない

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 [<input type="radio"/>]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。)		
[<input type="checkbox"/>]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 [<input type="checkbox"/>]接続しない(入手) [<input type="checkbox"/>]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		
[] 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	■ 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 ・生活保護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。 ・複数職員によるチェックや入力結果確認用リストを用いた事後チェックで誤入力を防止している。 ・伝送通信ソフトでは個人番号を表示せず、誤った対象者に関する情報の入手を防止している。 ② 必要な情報以外を入手することを防止する対策 ・生活保護システムにおける措置：データベース項目の設計や入力項目の制御を行い、必要な情報以外の登録を防止します。 複数人による二重チェックを実施している。 ③ 不正な使用を防止する対策 ・生活保護システムにおける措置：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。 ・住民から入手する場合も届出等の書面を用いて取得し、使用用途を明確にしている。 ④ 特定個人情報の使用に関する対策 ・生活保護システムにおける措置：個人番号利用事務に係るシステム以外からは特定個人情報ファイルを直接参照できないようアクセス制御を行っている。 ⑤ ユーザ認証の管理 ・生活保護システムにおける措置：二要素認証を行い、ユーザIDに付与されるアクセス権限によって利用可能な機能を制限している。 ・不正な端末から利用できないよう制御し、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。 ・伝送通信ソフトにおける措置：個人ごとにユーザ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 ・共用IDの発行を禁止し、個人番号を表示しないことで不正使用のリスクを軽減している。	
	■ 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の的に制御している。 ・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。	

9. 監査		
実施の有無	<input type="checkbox"/> 自己点検 <input type="radio"/> 内部監査 <input type="checkbox"/> 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	<input type="checkbox"/> 十分に行っている <input type="checkbox"/>	<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 <input type="checkbox"/> 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	<input type="checkbox"/> 8) 特定個人情報の漏えい・滅失・毀損リスクへの対策 <input type="checkbox"/>	
	<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) 従業者に対する教育・啓発	
当該対策は十分か【再掲】	<input type="checkbox"/> 十分である <input type="checkbox"/>	<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

- 葛城市における措置
 - ①物理的安全管理措置
 - ・持込・持出台帳管理
 - ②技術的安全管理措置
 - ・生活保護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データセンターに設置、データセンターへの入館及びサーバ室への入室を厳重に管理する。
 - ・特定個人情報等は、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UTM(コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置)等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。
 - ・中間サーバ・プラットフォームでは、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。
 - ・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。
- 伝送通信ソフトに関する措置
 - ・伝送通信ソフトへのアクセス権限を必要最小限に制限し、アクセス権限を持つ従業員の数を最小限に抑えることで、不正アクセスや誤操作のリスクを低減している。
 - ・伝送通信ソフトを使用する従業員に対して、適切な操作方法やセキュリティ対策に関する教育と訓練を実施し、人為的ミスの発生を防止している。

変更日	
-----	--

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10日	IVリスク対策 8.人手を介在させる作業	10である。	<p>■経営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。</p> <p>①特定個人情報への入手に関する対策</p> <p>・生活保護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。</p> <p>・複数職員によるチェックや入力結果確認（用）リストを用いた事後チェックで誤入力を防止している。</p> <p>・伝送通信ソフトでは個人番号を表示せず、誤った対象者に関する情報の入手を防止している。</p> <p>②必要な情報以外を入手することを防止する対策</p> <p>・生活保護システムにおける措置：データベース項目の設計や入力項目の制御を行い、必要な情報以外の登録を防止し、必要最小限の機能及び数に制限する。</p> <p>③不正な使用を防止する対策</p> <p>・生活保護システムにおける措置：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。</p> <p>・住民から入手する場合も届出等の書面を用いて取得し、使用用途を明確にしている。</p> <p>④特定個人情報への入手に関する対策</p> <p>・生活保護システムにおける措置：個人番号利用事務に係るシステム以外からは特定個人情報ファイルの取得を参照できないアクセス制御を行っている。</p> <p>⑤ユーザ認証の管理</p> <p>・生活保護システムにおける措置：二要素認証を行い、ユーザIDに付与されるアクセス権限によって利用可能な機能を制限している。</p> <p>・不正な結果から利用できないよう制限し、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。</p> <p>・伝送通信ソフトにおける措置：個人ごとにユーザ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。</p> <p>・共用IDの発行を禁止し、個人番号を表示しないことで不正使用のリスクを軽減している。</p> <p>■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。</p> <p>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</p> <p>・特定個人情報ファイルの取扱権限を持つIDを授け、必要最小限の権限及び数に制限している。</p> <p>・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約している。</p> <p>・移行以外の目的・用途でファイルを利用しないよう、作業者に対して周知徹底を行っている。</p> <p>②移行データ</p> <p>・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。</p> <p>・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。</p> <p>・システム間でデータの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。</p> <p>③テストデータ</p> <p>・特定個人情報とセキュリティ対策項目と定める加工を行い、必要最小限のテストデータのみを生成している。</p> <p>④相互牽制</p> <p>・移行作業は二人で行う相互牽制の体制で実施している。</p>	事後	
令和7年6月10日	IVリスク対策 9.監査		内部監査	事後	
令和7年6月10日	IVリスク対策 10.従業員に関する教育・啓発		十分に行っている	事後	
令和7年6月10日	IVリスク対策 11最も優先度が高いと考えられる対策		<p>①特定個人情報の漏えい・滅失・毀損リスクへの対策</p> <p>■漏えいに関する措置</p> <p>①物理的セキュリティ管理</p> <p>・持ち出し・持ち出し台管理</p> <p>②技術的セキュリティ管理</p> <p>・生活保護システムへのアクセス時に二要素認証</p> <p>・ウイルス対策ソフトウェアの導入</p> <p>・ファイアウォールと接続された内外部ネットワーク</p> <p>③移行作業時に関する措置</p> <p>・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。</p> <p>■中間サーバ・クラウド環境における措置</p> <p>①物理的セキュリティ管理</p> <p>・中間サーバ・クラウド環境はデータセンターに設置、データセンターへの入館及びサーバ室への入室を厳重に管理する。</p> <p>②技術的セキュリティ管理</p> <p>・中間サーバ・クラウド環境ではUTM（ファイアウォールやパケットフィルタリングなどの機能）やネットワークを効率的かつ包括的に保護する装置を導入し、アクセス制限、侵入検知及び侵入防止を行うこととし、ログの解析を行う。</p> <p>③中間サーバ・クラウド環境でのセキュリティ対策</p> <p>・ファイアウォールを導入し、パケットフィルタリングの機能を行う。</p> <p>・導入しているOS及びソフトウェアについて、必要に応じてセキュリティパッチの適用を行う。</p> <p>■ガバナンスクラウドにおける措置</p> <p>①物理的セキュリティ管理</p> <p>・ガバナンスクラウドについては設備・機器・システムのセキュリティ・制度（ISAP）のリストに準拠されたクラウドサービスを利用することにより、システムサーバ（物理）クラウド事業者の保護・管理する環境に構築し、その環境には認可された者がアクセスできるような適切な入居管理を行っている。</p> <p>②技術的セキュリティ管理</p> <p>・クラウド事業者は、ガバナンスクラウドに対するセキュリティの脅威に対し、脅威検出・対応・軽減・回復のサイクルを構築し、その環境には認可された者がアクセスできるような適切な入居管理を行っている。</p> <p>③ガバナンスクラウドのセキュリティ対策</p> <p>・クラウド事業者は、ガバナンスクラウドに対するセキュリティの脅威に対し、脅威検出・対応・軽減・回復のサイクルを構築し、その環境には認可された者がアクセスできるような適切な入居管理を行っている。</p> <p>④ガバナンスクラウドのセキュリティ対策</p> <p>・クラウド事業者は、ガバナンスクラウドに対するセキュリティの脅威に対し、脅威検出・対応・軽減・回復のサイクルを構築し、その環境には認可された者がアクセスできるような適切な入居管理を行っている。</p> <p>⑤ガバナンスクラウドのセキュリティ対策</p> <p>・クラウド事業者は、ガバナンスクラウドに対するセキュリティの脅威に対し、脅威検出・対応・軽減・回復のサイクルを構築し、その環境には認可された者がアクセスできるような適切な入居管理を行っている。</p> <p>⑥ガバナンスクラウドのセキュリティ対策</p> <p>・クラウド事業者は、ガバナンスクラウドに対するセキュリティの脅威に対し、脅威検出・対応・軽減・回復のサイクルを構築し、その環境には認可された者がアクセスできるような適切な入居管理を行っている。</p> <p>⑦ガバナンスクラウドのセキュリティ対策</p> <p>・クラウド事業者は、ガバナンスクラウドに対するセキュリティの脅威に対し、脅威検出・対応・軽減・回復のサイクルを構築し、その環境には認可された者がアクセスできるような適切な入居管理を行っている。</p> <p>⑧ガバナンスクラウドのセキュリティ対策</p> <p>・クラウド事業者は、ガバナンスクラウドに対するセキュリティの脅威に対し、脅威検出・対応・軽減・回復のサイクルを構築し、その環境には認可された者がアクセスできるような適切な入居管理を行っている。</p> <p>⑨ガバナンスクラウドのセキュリティ対策</p> <p>・クラウド事業者は、ガバナンスクラウドに対するセキュリティの脅威に対し、脅威検出・対応・軽減・回復のサイクルを構築し、その環境には認可された者がアクセスできるような適切な入居管理を行っている。</p> <p>⑩ガバナンスクラウドのセキュリティ対策</p> <p>・クラウド事業者は、ガバナンスクラウドに対するセキュリティの脅威に対し、脅威検出・対応・軽減・回復のサイクルを構築し、その環境には認可された者がアクセスできるような適切な入居管理を行っている。</p>	事後	