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
10	児童手当に関する事務　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、児童手当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、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

［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	児童手当に関する事務
②事務の概要	児童手当法に基づき、次代の社会を担う子どもの健やかな育ちを支援するため、18歳到達後の最初の3月31日までの間にある児童を養育している者に対し、児童手当または特例給付を支給する。 特定個人情報ファイルは以下の事務で利用する。 ①児童手当受給資格の確認を行う。 ②児童を養育する者からの認定請求の受理、審査を行い結果を通知する。 ③認定した受給者に対し、手当を年3回の定期支払いおよび、状況に応じて随時支払いを行う。 ④年に一度、現況届の受理、審査を行い、継続支給の確認を行う。 　所得に応じて「児童手当」・「特例給付」を認定する。現況届の提出がない場合は支払差止めを行う。 ⑤受給者にかかる世帯、所得等の変更による各種届出の受理、審査、認定を行い通知を行う。 ⑥児童手当支給に関する確認を行う。
③システムの名称	児童手当システム、宛名システム

2. 特定個人情報ファイル名
児童手当受給者資格台帳、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項および別表第81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	[　　実施する　　]	＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	番号法第19条第8号に基づく利用特定個人情報の提供に関する命令（令和6年デジタル庁・総務省第9号）第2条別表 【情報提供の根拠】第42、125、141、161項 【情報照会の根拠】第106、107項	

5. 評価実施機関における担当部署	
①部署	高島市　子ども未来部　子育て政策課
②所属長の役職名	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	高島市　総務部　総務課 〒520-1592　滋賀県高島市新旭町北畑565番地　0740-25-8000

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	高島市　子ども未来部　子育て政策課 〒520-1592　滋賀県高島市新旭町北畑565番地　0740-25-8136
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人以上1万人未満　] ＜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	[ ]	<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		[　　]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	マイナンバーの紐づけを行う際は2名以上で作業および確認を行う体制をとっている。 ■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 ・児童手当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。 ・宛名番号や用いて突合を行い、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。 ②必要な情報以外を入手することを防止する対策 ・児童手当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ている。 ・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 ・児童手当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。 ・庁内連携により、移転元から提供されるデータファイルを取り込む方式で、予め決められた情報以外のデータを入手しない仕組みにしている。 ④特定個人情報の使用に関する対策 ・児童手当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。 ・庁内連携機能側のアクセス制御により業務に不必要な情報にはアクセスできないようにしている。 ・アクセス権限の設定により、許可された者以外は個人番号がマスクされた状態で表示している。 ⑤ユーザ認証の管理 ・児童手当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。 ・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	［ ○ ］ 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	■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：外周警備(赤外線センサー)、24時間有人監視、監視カメラ ・入退館管理：ICカード認証 ・持込・持出防止：金属探知機、DRタグ媒体管理、持込・持出台帳管理 ②技術的安全管理措置 ・児童手当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 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データセンターに設置しており、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。 ・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している。 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
令和5年4月1日	Ⅰ－5 ① 部署	高島市　子ども未来部　子育て支援課	高島市　子ども未来部　子育て政策課	事後	
令和5年4月1日	Ⅰ－8 連絡先	高島市　子ども未来部　子育て支援課 0740-25-8136	高島市　子ども未来部　子育て政策課 0740-25-8136	事後	
令和5年4月1日	Ⅱしきい値判断項目 1.対象人数	令和3年4月1日	令和5年4月1日	事後	
令和5年4月1日	Ⅱしきい値判断項目 2.取扱人数	令和3年4月1日	令和5年4月1日	事後	
令和6年4月1日	Ⅱしきい値判断項目 1.対象人数	令和5年4月1日	令和6年4月1日	事後	
令和7年4月1日	Ⅱしきい値判断項目 2.取扱人数	対象人数：1,000人未満（任意実施） 令和6年4月1日	対象人数：1,000人以上1万人未満 令和7年4月1日	事後	
令和7年4月1日	Ⅰ関連情報 3.個人番号の利用	・番号法第9条第1項および別表第一の第56項 ・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省令で定める事務を定める命令（平成26年内閣府・総務省令第5号）第44条	・番号法第9条第1項および別表第81項	事後	
令和7年4月1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提供	番号法第19条第8号および別表第二 【情報提供の根拠】26,30,87項 【情報照会の根拠】74,75項 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二の主務省令で定める事務及び情報を定める命令（平成26年内閣府・総務省令第7号） 【情報提供の根拠】第19,44条 【情報照会の根拠】第40条	番号法第19条第8号に基づく利用特定個人情報の提供に関する命令（令和6年デジタル庁・総務省第9号）第2条別表 【情報提供の根拠】第42、125、141、161項 【情報照会の根拠】第106、107項	事後	
令和7年9月12日	Ⅳリスク対策 8．人手を介在させる作業判断の根拠		■経常作業時における 以下を講じている。 ①特定個人情報の入手に関する対策 ・児童手当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。 ・宛名番号や用いて突合を行い、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。 ②必要な情報以外を入手することを防止する対策 ・児童手当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ている。 ・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 ・児童手当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。 ・庁内連携により、移転元から提供されるデータファイルを取り込む方式で、予め決められた情報以外のデータを入手しない仕組みにしている。 ④特定個人情報の使用に関する対策 ・児童手当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。 ・庁内連携機能側のアクセス制御により業務に不必要な情報にはアクセスできないようにしている。 ・アクセス権限の設定により、許可された者以外は個人番号がマスクされた状態で表示している。 ⑤ユーザ認証の管理 ・児童手当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。 ・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。	事前	
令和7年9月12日	Ⅳリスク対策 11．最も優先度が高いと考えられる対策	事務取扱者を限定し、漏えい等のリスクがないよう書類は鍵付きの保管庫に格納するなど管理を徹底している。	■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：外周警備(赤外線センサー)、24時間有人監視、監視カメラ ・入退館管理：ICカード認証 ・持込・持出防止：金属探知機、DRタグ媒体管理、持込・持出台帳管理 ②技術的安全管理措置 ・児童手当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 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データセンターに設置しており、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。 ・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している。 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	事前	