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	児童扶養手当の支給に関する事務　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、児童扶養手当の支給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	児童扶養手当の支給に関する事務
②事務の概要	児童扶養手当法（以下「法」という。）の規定に基づき、母子家庭・父子家庭等で養育されている児童の心身の健やかな成長に寄与することを目的として支給される手当であり、児童を養育している者（父母または養育者）からの申請によって支給している。 特定個人情報を使用する事務 ①法第6条に基づく受給資格および手当額の認定の請求に関する事務 ②児童扶養手当証書に関する事務 ③法第8条に基づく手当額の改定に関する事務 ④法第16条に基づく未支払の手当に関する事務 ⑤法第28条に基づく届出に関する事務 ⑥施行規則第3条に基づく届出に関する事務
③システムの名称	児童扶養手当システム

2. 特定個人情報ファイル名
児童扶養手当受給者資格台帳

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56項 ・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別表の主務省令で定める事務を定める命令第29条

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	（情報提供の根拠） 番号法第19条第8号に基づく主務省令第2条の表第17，20，42，89，90，125，141，155，161の項 （情報照会の根拠） 番号法第19条第8号に基づく主務省令第2条の表第81の項	

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
なし

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　0740-25-8538

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	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
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	[　　]	＜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		

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：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 ・児童扶養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。 ・中間サーバー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　子ども家庭相談課	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　子ども家庭相談課 0740-25-8517	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	1万人以上10万人未満	1000人未満	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6年4月1日	Ⅱしきい値判断項目 2.取扱人数	令和5年4月1日	令和6年4月1日	事後	
令和6年4月1日	I-7.特定個人情報の開示・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しきい値判断項目 2.取扱人数	令和6年4月1日	令和7年4月1日	事後	
令和7年4月1日	4.情報ネットワークシステムによる情報連携	番号法第19条第8号および別表第二 （別表における情報提供の根拠） 第三欄（情報提供者）が「都道府県知事等」の項のうち、第四欄（特定個人情報）に「児童扶養手当関係情報」が含まれる項（13,16,26,30,47,64,65,87,116）	・番号法第9条第1項および別表第56項 ・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別表の主務省令で定める事務を定める命令第29条	事後	
令和7年4月1日	4.情報ネットワークシステムによる情報連携	（情報照会の根拠） 番号法第19条第8号別表第二57の項	（情報提供の根拠） 番号法第19条第8号に基づく主務省令第2条の表第17, 20, 42, 89, 90, 125, 141, 155, 161の項 （情報照会の根拠） 番号法第19条第8号に基づく主務省令第2条の表第81の項	事後	
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：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 ・児童扶養手当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。 ・中間サーバー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及びミドルウエアについて、必要に応じてセキュリ	事前	