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
64	令和5年度低所得の子育て世帯に対する子育て世帯生活支援特別給付金（ひとり親世帯以外の低所得の子育て世帯分）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

藤沢市は、令和5年度低所得の子育て世帯に対する子育て世帯生活支援特別給付金（ひとり親世帯以外の低所得の子育て世帯分）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

藤沢市長

公表日

令和7年7月18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	令和5年度低所得の子育て世帯に対する子育て世帯生活支援特別給付金（ひとり親世帯以外の低所得の子育て世帯分）の支給に関する事務　基礎項目評価書
②事務の概要	公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律第10条の特定公的給付として指定された「低所得の子育て世帯に対する子育て世帯生活支援特別給付金（ひとり親世帯以外の低所得の子育て世帯分）の支給について」（令和5年4月10日こ支家第14号こども家庭庁支援局長通知）に基づき、給付金の支給を実施するための基礎とする情報の管理に関する事務において取り扱う。
③システムの名称	保健福祉総合システム（福祉共通管理システム）、団体内統合宛名システム、中間サーバー

2. 特定個人情報ファイル名
子育て世帯生活支援特別給付金情報ファイル

3. 個人番号の利用	
法令上の根拠	「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」第9条第1項及び別表の135の項、「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74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	＜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おける情報提供の根拠＞ 情報提供なし ＜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おける情報照会の根拠＞ 「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」第19条第8号別表の135の項 「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及び情報を定める命令」第74条	

5. 評価実施機関における担当部署	
①部署	子ども青少年部　子育て給付課
②所属長の役職名	子育て給付課長

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	〒251-8601 藤沢市朝日町1番地の1 藤沢市役所　市民自治部　市民相談情報課　情報公開センター 0466-50-3567

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	〒251-8601 藤沢市朝日町1番地の1 藤沢市役所　子ども青少年部　子育て給付課 0466-50-3581
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6月5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6月5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	[　　]	＜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の留意事項を遵守している。 特定個人情報の入手から保管・廃棄までのプロセスで、人手が介在する局面ごとに人為的ミスが発生するリスクへの対策を講じている。

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	[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	藤沢市側のシステムにおいては、情報提供ネットワークシステムで情報照会を行うことができる端末、職員、参照範囲が必要最小限となるよう、アクセス制限を設定している。また、アクセス権限の所持者には、事務取扱担当者の研修において離席時のログアウト徹底を呼びかけており、監査も実施している。これらの対策を講じていることから、目的外の入手が行われるリスクへの対策は「十分である」と考えられる。 ＜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 」(最新版に準拠。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6年12月19日	Ⅰ 関連情報 3．個人番号の利用	「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」第9条第1項及び別表第一の101の項、「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第一の主務省令で定める事務を定める命令」第74条	「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」第9条第1項及び別表の135の項、「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74条	事後	
令和6年12月19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 ②法令上の根拠	＜別表第二における情報提供の根拠＞ 情報提供なし ＜別表第二における情報照会の根拠＞ 「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」第19条第8号別表第二の121の項 「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第二の主務省令で定める事務及び情報を定める命令」第59条の4	＜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おける情報提供の根拠＞ 情報提供なし ＜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おける情報照会の根拠＞ 「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」第19条第8号別表の135の項 「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及び情報を定める命令」第74条	事後	
令和6年12月19日	Ⅳ リスク対策	－	項目追加	事後	評価書の様式変更に伴う記載の変更のため、重要な事項に該当しない。
令和7年7月18日	Ⅱ しきい値判断項目 1．対象者人数（いつの時点の計数か）	2023/5/1	2025/6/5	事前	基幹系システム標準化・共通化に伴い、データ保管場所がガバメントクラウドへ移行するため再実施を行った。
令和7年7月18日	Ⅱ しきい値判断項目 2．取扱者数（いつの時点の計数か）	2023/5/1	2025/6/5	事前	基幹系システム標準化・共通化に伴い、データ保管場所がガバメントクラウドへ移行するため再実施を行った。
令和7年7月18日	Ⅳ リスク対策 11.最も優先度が高いと考えられる対策 当該対策は十分か【再掲】 判断の根拠	藤沢市側のシステムにおいては、情報提供ネットワークシステムで情報照会を行うことができる端末、職員、参照範囲が必要最小限となるよう、アクセス制限を設定している。また、アクセス権限の所持者には、事務取扱担当者の研修において離席時のログアウト徹底を呼びかけており、監査も実施している。これらの対策を講じていることから、目的外の入手が行われるリスクへの対策は「十分である」と考えられる。	現行にガバメントクラウドにおける措置の内容を追記する。 ＜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」（最新版に準拠。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	基幹系システム標準化・共通化に伴い、ガバメントクラウドにおける措置を追記するもの。