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
15	健康増進事業の実施に関する事務　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、健康増進事業の実施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

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	健康増進事業の実施に関する事務
②事務の概要	健康増進事業は、健康増進法第17条第1項及び第19条の2に基づき、市民の健康増進を図るため、生活習慣相談等の実施を行うものである。 そのうち、健康増進法第19条の2に基づき実施する健康増進事業として、次の事業に係る各種検診等を実施し、対象者の抽出、検診情報の管理、各相談等の結果管理、各事業の統計業務、受診券作成や勧奨通知作成業務等を行う。 ⑴歯周疾患検診 ⑵骨粗しょう症検診 ⑶肝炎ウィルス検診 ⑷健康増進法施行規則第4条の2第4号に定める健康診査 ⑸健康増進法施行規則第4条の2第5号に定める保健指導 ⑹がん検診
③システムの名称	健康管理システム、中間サーバー、宛名システム

2. 特定個人情報ファイル名
成人検診ファイル、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　別表第111の項 番号法別表の主務省令で定める事務を定める命令第54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	[情報照会] 番号法第19条第8号 番号法第19条第8号に基づく主務省令第2条の表139の項 [情報提供] 番号法第19条第8号 番号法第19条第8号に基づく主務省令第2条の表139の項	

5. 評価実施機関における担当部署	
①部署	健康福祉部　健康推進課
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	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	健康福祉部　健康推進課 〒520-1592　滋賀県高島市新旭町北畑565番地　0740-25-8078

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」に従い、システムで照会を行う際には、4情報又は住所を含めた3情報により行うことを遵守していることから、人為的ミスが生じるリスクへの対策は「十分である」と考える。 ■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する。 ・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する。 ・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う。 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、追記できない状態にする。 ・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・破棄方法を記録する。 ・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する。 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する。 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する。	

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	［ 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 ］ ＜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	特定個人情報を取扱う基幹系システムへのアクセスが可能な職員は、パスワード及び静脈認証により管理しており、人事移動等により特定個人情報を扱わないことになった場合には、基幹系システム管理者がアクセスできないようにしているため、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は「十分である」と考える。 ■高島市における措置 ①物理的安全管理措置 ・アクセス可能な職員名簿を年度ごとに作成するとともに、アクセスログを記録するなど適切なアクセス権限の管理 ・日中は職員による監視、勤務時間外は施錠のうえ警備をセットするなど外部進入の防止 ・アクセス可能時間帯の制限 ②技術的安全管理措置 ・健康管理システムへのアクセス時におけるID、静脈認証装置による二要素認証 ・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7年4月22日	Ⅰ関連情報　1. 特定個人情報ファイルを取り扱う事務　②事務の概要	健康増進事業は、健康増進法第17条第1項及び第19条の2に基づき、市民の健康増進を図るため、生活習慣相談等の実施を行うものである。 そのうち、健康増進法第19条の2に基づき実施する健康増進事業として、次の事業に係る各種検診等を実施し、検診情報の管理、統計業務等を行う。	健康増進事業は、健康増進法第17条第1項及び第19条の2に基づき、市民の健康増進を図るため、生活習慣相談等の実施を行うものである。 そのうち、健康増進法第19条の2に基づき実施する健康増進事業として、次の事業に係る各種検診等を実施し、対象者の抽出、検診情報の管理、各相談等の結果管理、各事業の統計業務、受診券作成や勧奨通知作成業務等を行	事後	
令和7年4月22日	Ⅰ関連情報　3. 個人番号の利用　法令上の根拠	番号法第9条第1項および別表第一第76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54条	番号法第9条第1項　別表第111の項 番号法別表の主務省令で定める事務を定める命令54条	事後	
令和7年4月22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	[情報照会] 番号法第19条第8項　別表第二の102の2項 [情報提供] 番号法第19条第8項　別表第二の102の2項	[情報照会] 番号法第19条第8号 番号法第19条第8号に基づく主務省令第2条の表139の項 [情報提供] 番号法第19条第8号 番号法第19条第8号に基づく主務省令第2条の表139の項	事後	
令和7年4月22日	Ⅱしきい値判断項目　1.対象人数	令和3年4月1日時点	令和7年4月1日時点	事後	
令和7年4月22日	Ⅱしきい値判断項目　2. 取扱者数	令和3年4月1日時点	令和7年4月1日時点	事後	
令和7年4月22日	Ⅳリスク対策　8. 人手を介在させる作業	―	新様式への変更に伴い記載	事後	
令和7年4月22日	Ⅳリスク対策　11. 最も優先度が高いと考えられる対策	―	新様式への変更に伴い記載	事後	
令和7年9月12日	Ⅰ-1-③システムの名称	健康管理システム（成人検診）	健康管理システム、中間サーバー	事後	
令和7年9月12日	Ⅰ-1-③システムの名称	健康管理システム、中間サーバー	健康管理システム、中間サーバー、宛名システム	事前	
令和7年9月12日	Ⅰ-2特定個人情報ファイル名	成人検診ファイル	成人検診ファイル、住登外者宛名番号管理関係ファイル	事前	
令和7年9月12日	Ⅳ-8人手を介在させる作業	「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」に従い、システムで照会を行う際には、4情報又は住所を含めた3情報により行うことを遵守していることから、人為的ミスが生じるリスクへの対策は「十分である」と考える。	「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」に従い、システムで照会を行う際には、4情報又は住所を含めた3情報により行うことを遵守していることから、人為的ミスが生じるリスクへの対策は「十分である」と考える。 ■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する。 ・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する。 ・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う。 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、追記できない状態にする。 ・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・破棄方法を記録する。 ・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する。 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する。 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する。	事前	
令和7年9月12日	Ⅳ-11最も優先度が高いと考えられる対策　判断の根拠	特定個人情報を取扱う基幹系システムへのアクセスが可能な職員は、パスワード及び静脈認証により管理しており、人事移動等により特定個人情報を扱わないことになった場合には、基幹系システム管理者がアクセスできないようにしているため、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は「十分である」と考える。	特定個人情報を取扱う基幹系システムへのアクセスが可能な職員は、パスワード及び静脈認証により管理しており、人事移動等により特定個人情報を扱わないことになった場合には、基幹系システム管理者がアクセスできないようにしているため、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は「十分である」と考える。 ■高島市における措置 ①物理的安全管理措置 ・アクセス可能な職員名簿を年度ごとに作成するとともに、アクセスログを記録するなど適切なアクセス権限の管理 ・日中は職員による監視、勤務時間外は施錠のうえ警備をセットするなど外部進入の防止 ・アクセス可能時間帯の制限 ②技術的安全管理措置 ・健康管理システムへのアクセス時におけるID、静脈認証装置による二要素認証 ・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	事前	