

特定個人情報保護評価書(重点項目評価書)

評価書番号	評価書名
9	予防接種に関する事務 重点項目評価書

個人のプライバシー等の権利利益の保護の宣言

松江市は、予防接種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	
------	--

評価実施機関名

松江市長

公表日

令和7年1月30日

項目一覧

I 基本情報
II 特定個人情報ファイルの概要
(別添1) 特定個人情報ファイル記録項目
III リスク対策
IV 開示請求、問合せ
V 評価実施手続
(別添2) 変更箇所

I 基本情報

1. 特定個人情報ファイルを取り扱う事務

①事務の名称	予防接種に関する事務
②事務の内容	本事務は予防接種法(昭和23年法律第68号)に基づき、A類疾病及びB類疾病(※1)のうち政令で定めるものについて、市内に住所を有する者に対し、期日または期間を指定して予防接種を行うとともに、給付、実費徴収等の事務を行うものである。 また、新型インフルエンザ等対策特別措置法(平成24年法律第31号。以下「特措法」という。)による予防接種の実施に関する事務を行うものである。 上記の特定個人情報ファイルを次の事務に利用する。 (1) 予防接種の実施 (2) 予防接種の記録(※2) (3) 予防接種済証の発行 (4) 健康被害の救済措置 (5) 予防接種の勧奨 (6) 実費の徴収 (※1) A類疾病とは、人から人に感染することによる発生及びまん延を予防するため、又はかかった場合の症状の程度が重篤になる恐れがあることから、その発生及びまん延を予防するため特に予防接種を行う必要があると認められる疾病。 B類疾病とは、個人の発病またはその重症化を防止し、併せてそのまん延の予防に資するため特に予防接種を行う必要があると認められる疾病。 (※2) 新型コロナウイルス感染症に係る特例臨時接種の記録を含む。
③対象人数	<選択肢> [10万人以上30万人未満] 1) 1,000人未満 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

2. 特定個人情報ファイルを取り扱う事務において使用するシステム

システム1

①システムの名称	健康管理システム
②システムの機能	1 予防接種履歴管理機能(予防接種台帳) 個人ごとに予防接種の接種記録を管理し、照会ができる。 2 対象者抽出機能 予防接種手帳や予防接種の勧奨通知の発送のため、条件を指定し対象者を抽出する。 3 帳票作成機能 各種帳票(予診票や接種記録)を作成する。 4 各種統計機能 予防接種委託料支払に関する積算や年齢ごとの接種者数などの統計を作成する。 5 マスタ登録機能 予防接種受託医療機関(予防接種実施場所)や接種医師を管理する。
③他のシステムとの接続	[] 情報提供ネットワークシステム [] 庁内連携システム [] 住民基本台帳ネットワークシステム [] 既存住民基本台帳システム [○] 宛名システム等 [] 税務システム [○] その他 (番号連携サーバー(団体内統合宛名システム))

システム4	
①システムの名称	中間サーバー
②システムの機能	1 符号管理機能 情報照会・情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」とを紐づけ、その情報を保管・管理する機能 2 情報照会機能 情報提供ネットワークシステムを介して、特定個人情報(連携対象)の情報照会及び情報提供受領(照会した情報の受領)を行う機能 3 情報提供機能 情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報(連携対象)の提供を行う機能 4 既存システム接続機能 中間サーバーと既存システム、団体内統合宛名システム及び住民基本台帳システムとの間で情報照会内容、情報提供内容、特定個人情報(連携対象)、符号取得のための情報等について連携するための機能 5 情報提供等記録管理機能 特定個人情報(連携対象)の照会又は提供があった旨の情報提供等記録を生成し、管理する機能 6 情報提供データベース管理機能 特定個人情報(連携対象)を副本として、保持・管理する機能 7 データ送受信機能 中間サーバーと情報提供ネットワークシステム(インターフェイスシステム)との間で情報照会、情報提供、符号取得のための情報等について連携するための機能 8 セキュリティ管理機能 セキュリティを管理するための機能 9 職員認証・権限管理機能 中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報(連携対象)へのアクセス制御を行う機能 10 システム管理機能 処理状況の管理、業務統計情報の集計、稼働状態の通知、保管期限切れ情報の削除を行う機能
③他のシステムとの接続	[☐] 情報提供ネットワークシステム [☐] 庁内連携システム [☐] 住民基本台帳ネットワークシステム [☐] 既存住民基本台帳システム [☐] 宛名システム等 [☐] 税務システム [☐] その他 (番号連携サーバー(団体内統合宛名システム))

システム5	
①システムの名称	既存住民基本台帳システム
②システムの機能	1 住民基本台帳の照会、検索機能 2 住民基本台帳記載事項に係る修正・他システム連携機能 3 本人確認情報の更新機能 4 転入届の特例による転出届、転入届の際の通信機能 5 他市区町村への通知等の作成・送信機能 6 住民基本台帳ネットワークシステムからの通知取り込み機能 7 住民票コードの通知機能 8 住民票の写し、住民票記載事項証明書などの帳票の作成・出力機能 9 法務大臣への通知機能 10 個人番号カード送付先情報の作成・通知機能
③他のシステムとの接続	☐ 情報提供ネットワークシステム ☐ 庁内連携システム ☐ 住民基本台帳ネットワークシステム ☐ 既存住民基本台帳システム ☒ 宛名システム等 ☐ 税務システム ☒ その他（住基GWサーバー・GW証明書発行システム・GW証明書発行システム（戸籍）・中間サーバー・番号連携サーバー・コンビニ交付システム）
システム6	
①システムの名称	ワクチン接種記録システム（VRS）
②システムの機能	新型コロナウイルス感染症に係る特例臨時接種の接種対象者・接種記録の保管（令和6年10月1日からその他の機能停止）
③他のシステムとの接続	☐ 情報提供ネットワークシステム ☐ 庁内連携システム ☐ 住民基本台帳ネットワークシステム ☐ 既存住民基本台帳システム ☐ 宛名システム等 ☐ 税務システム ☐ その他（ ）
システム7	
①システムの名称	住民基本台帳ネットワークシステム
②システムの機能	1 本人確認情報の更新 2 本人確認 3 個人番号カードを利用した転入（特例転入） 4 本人確認情報検索 5 地方公共団体情報システム機構への情報照会 6 本人確認情報整合 7 送付先情報通知 8 個人番号カード管理システムとの情報連携
③他のシステムとの接続	☐ 情報提供ネットワークシステム ☐ 庁内連携システム ☐ 住民基本台帳ネットワークシステム ☐ 既存住民基本台帳システム ☐ 宛名システム等 ☐ 税務システム ☒ その他（住基GWサーバー・個人番号カード管理システム）

3. 特定個人情報ファイル名	
予防接種ファイル	
4. 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（平成25年法律第27号）（以下「番号法」という。）第9条第1号（別表14項、126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（平成26年内閣府・総務省令第5号）第10条、第67条の2
5. 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（特定個人情報の提供の制限）（別表14項、126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（情報連携主務省令）（令和6年デジタル庁・総務省令第9号） ・第2条の表 25項、26項、153項、154項 ・第27条、第28条、第155条、第156条
6. 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
7. 他の評価実施機関	
-	

Ⅱ 特定個人情報ファイルの概要

1. 特定個人情報ファイル名	
予防接種ファイル	
2. 基本情報	
①ファイルの種類 ※	システム用ファイル ☐ システム用ファイル ☐ その他の電子ファイル(表計算ファイル等)
②対象となる本人の数	10万人以上100万人未満 ☐ 1万人未満 ☐ 1万人以上10万人未満 ☐ 10万人以上100万人未満 ☐ 100万人以上1,000万人未満 ☐ 1,000万人以上
③対象となる本人の範囲 ※	接種日時点において住民基本台帳に記録された本市住民で予防接種の対象者
その必要性	予防接種に関する業務の実現のために、必要な特定個人情報を保有する必要がある。
④記録される項目	10項目以上50項目未満 ☐ 10項目未満 ☐ 10項目以上50項目未満 ☐ 50項目以上100項目未満 ☐ 100項目以上
主な記録項目 ※	・識別情報 ☐ 個人番号 ☐ 個人番号対応符号 ☐ その他識別情報(内部番号) ・連絡先等情報 ☐ 4情報(氏名、性別、生年月日、住所) ☐ 連絡先(電話番号等) ☐ その他住民票関係情報 ・業務関係情報 ☐ 国税関係情報 ☐ 地方税関係情報 ☐ 健康・医療関係情報 ☐ 医療保険関係情報 ☐ 児童福祉・子育て関係情報 ☐ 障害者福祉関係情報 ☐ 生活保護・社会福祉関係情報 ☐ 介護・高齢者福祉関係情報 ☐ 雇用・労働関係情報 ☐ 年金関係情報 ☐ 学校・教育関係情報 ☐ 災害関係情報 ☐ その他 ()
その妥当性	<個人番号、その他識別情報(内部番号)> 本人確認等、対象者を正確に特定するために保有 <4情報、その他住民票関係情報> 予防接種対象者の居住地を把握するために保有 <健康・医療関係情報(予防接種に関する情報)> 予防接種の接種記録を把握するために保有
全ての記録項目	別添1を参照。
⑤保有開始日	令和7年2月
⑥事務担当部署	健康福祉部 健康推進課

3. 特定個人情報の入手・使用		
①入手元 ※		☐ 本人又は本人の代理人 ☐ 評価実施機関内の他部署 （ 市民課 ） ☐ 行政機関・独立行政法人等 （ ） ☐ 地方公共団体・地方独立行政法人 （ 他市区町村 ） ☐ 民間事業者 （ ） ☐ その他 （ ）
②入手方法		☐ 紙 [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ ☐ 電子メール [] 専用線 ☐ 庁内連携システム ☐ 情報提供ネットワークシステム ☐ その他 （ 住民基本台帳ネットワークシステム ）
③使用目的 ※		予防接種の実施、予防接種に関する記録の作成
④使用の主体	使用部署	健康福祉部 健康推進課、鹿島支所市民生活課、島根支所市民生活課、美保関支所市民生活課、八雲支所市民生活課、玉湯支所市民生活課、宍道支所市民生活課、八束支所市民生活課、東出雲支所市民生活課
	使用者数	[50人以上100人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
⑤使用方法		予防接種の実施、予防接種に関する記録の作成等に使用
	情報の突合	4情報(氏名、性別、生年月日、住所)又は宛名番号で突合
⑥使用開始日		令和7年2月1日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		委託する <選択肢> 1) 委託する 2) 委託しない (2) 件
委託事項1		システムの運用・保守業務、法制度改正に伴う改修作業業務
①委託内容		システムの運用・保守業務、法制度改正に伴う改修作業
②委託先における取扱者数		10人以上50人未満 <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
③委託先名		松江市行政情報システムサービス共同企業体 代表企業 株式会社テクノプロジェクト
再委託	④再委託の有無 ※	再委託する <選択肢> 1) 再委託する 2) 再委託しない
	⑤再委託の許諾方法	再委託申請(事業者名、作業者、作業内容、作業期間、作業場所等記載)に対する承認
	⑥再委託事項	ハードウェア保守、遠隔地媒体保管
委託事項2		ワクチン接種記録システム(VRS)を用いた特定個人情報ファイルの管理
①委託内容		新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)事務に関するワクチン接種記録システム(VRS)を用いた特定個人情報ファイルの管理
②委託先における取扱者数		10人以上50人未満 <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
③委託先名		株式会社ミラボ
再委託	④再委託の有無 ※	再委託しない <選択肢> 1) 再委託する 2) 再委託しない
	⑤再委託の許諾方法	
	⑥再委託事項	

5. 特定個人情報の提供・移転(委託に伴うものを除く。)	
提供・移転の有無	[☐] 提供を行っている (5) 件 [] 移転を行っている () 件 [] 行っていない
提供先1	都道府県知事又は市町村長
①法令上の根拠	番号法第19条第8号 別表14項
②提供先における用途	予防接種法による予防接種の実施に関する事務で主務省令に定めるもの
③提供する情報	予防接種法による予防接種の実施に関する事務で主務省令に定めるもの
④提供する情報の対象となる本人の数	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. 基本情報③対象者となる本人の範囲」と同じ
⑥提供方法	[☐] 情報提供ネットワークシステム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [] その他 ()
⑦時期・頻度	情報提供を行う必要性が生じた都度
提供先2	厚生労働大臣、都道府県知事又は市町村長
①法令上の根拠	番号法第19条第8号 別表126項
②提供先における用途	特措法による予防接種の実施に関する事務で主務省令に定めるもの
③提供する情報	特措法による予防接種の実施に関する事務で主務省令に定めるもの
④提供する情報の対象となる本人の数	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. 基本情報③対象者となる本人の範囲」と同じ
⑥提供方法	[☐] 情報提供ネットワークシステム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [] その他 ()
⑦時期・頻度	情報提供を行う必要性が生じた都度

6. 特定個人情報の保管・消去

保管場所 ※

＜本市における措置＞

1 下記の措置を講じるデータセンター内のサーバー室に設置したサーバー内に保管され、バックアップ媒体は同データセンター内の保管室に保管される。

- (1) データセンターは、有人受付とセキュリティゲートによる入館管理を行っている。
- (2) サーバー室は、ICカードとパスワードによる個人認証及び生体認証による入室管理を行っている。
- (3) サーバーへのアクセスは、ID及びパスワードによる認証を必要とする。
- (4) 保管室は、生体認証による入室管理を行っている。

2 バックアップ媒体については、上記データセンター以外にも、下記の措置を講じる別のデータセンター内の保管室に保管される。

- (5) データセンターは、事前申請方式の有人受付による入館管理を行っている。
- (6) 保管室は、生体認証による入室管理を行っている。
- (7) バックアップ媒体の移動及び保管に当たっては、GPSによる所在確認が可能なケースに格納する。

＜中間サーバー・プラットフォームにおける措置＞

1 中間サーバー・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ー室への入室を行う際は、警備印などにより顔写真入りの身分証明書と事前申請との照合を行う。

2 特定個人情報は、サーバー室に設置された中間サーバー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。

＜ワクチン接種記録システム(VRS)における措置＞

1 ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得している。

2 クラウドサービスを利用している。なお、以下のとおりのセキュリティ対策を講じている。

- (1) 論理的に区分された本市の領域にデータを保管する。
- (2) 当該領域のデータは、暗号化処理をする。
- (3) 個人番号が含まれる領域はインターネットからアクセスできないように制御している。
- (4) 国、都道府県、市区町村からは特定個人情報にアクセスできないように制御している。
- (5) 日本国内にデータセンターが存在するクラウドサービスを利用している。

3 本市の領域に保管されたデータは、本市及び他機関から消去できない。

※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、消去することができない。

＜ガバメントクラウドにおける措置＞

1 サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。

- (1) ISO/IEC27017、ISO/IEC27018 の認証を受けていること。
- (2) 日本国内でのデータ保管を条件としていること。

2 特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。

7. 備考

＜ガバメントクラウドにおける措置＞

1 特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。

2 クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。

3 既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。

(別添1) 特定個人情報ファイル記録項目

予防接種ファイル

【識別情報】

1. 個人番号 2. 宛名番号

【連絡先情報】

1. 氏名 2. 生年月日 3. 性別 4. 住所

【業務関係情報】

1. 西暦年度 2. 宛名番号 3. 接種・予診日 4. 接種種別 5. 肺炎球菌種類(A類) 6. 接種回数 7. 接種判定 8. 接種日年齢 9. 年度末年齢

10. 請求日(月) 11. 実施医療機関 12. 実施場所 13. 実施区分 14. 問診医 15. 接種医 16. 接種番号 17. メーカー 18. Lot.No.
19. 接種量 20. 未接種理由 21. 特記事項 22. 接種自治体コード 23. VRS取込日 24. VRS移出日 25. ワクチン種類(※)

26. 製品名(※) 27. 旅券関係情報(旧姓・別姓・別名、ローマ字氏名、国籍、旅券番号)(※) 28. 証明書ID(※) 29. 証明書発行年月日(※)

※ 新型コロナウイルス感染症予防接種証明書(特例臨時接種分)の交付に必要な場合のみ

Ⅲ リスク対策 ※(7. ②を除く。)

1. 特定個人情報ファイル名	
予防接種ファイル	
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。）	
リスク： 目的外の入手が行われるリスク	
リスクに対する措置の内容	・住基情報の入手については、既存住民基本台帳システムに登録した情報を庁内連携機能で取得するため、対象候補となりうる住民以外の情報を入手することはない。 ・住民からの申請情報の入手については、申請者の本人確認（代理権限および代理者の本人確認を含む）を実施している。
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
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。)におけるその他のリスク及びそのリスクに対する措置	
<不適切な方法で入手が行われるリスクに対する措置> システムを使用できる職員を限定し、ID、パスワード、生体認証による認証を実施している。また、認証後もユーザーごとにシステム上での利用可能な機能を制限することで、不適切な方法で入手が行えない対策を実施している。 <入手した特定個人情報が不正確であるリスクに対する措置> ・入手した情報については、窓口での聞き取りや本人確認書類との照合等を通じて確認することで正確性を確保している。 ・職員にて収集した情報に基づいて、間違いがあれば職権で適宜修正することで正確性を確保している。 <入手の際に特定個人情報が漏えい・紛失するリスクに対する措置> 庁内連携機能からの住基情報、各種照会情報の入手については、庁内専用回線を使用している。	
3. 特定個人情報の使用	
リスク1： 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	
リスクに対する措置の内容	・宛名システムのアクセス制御機能により、個人番号利用事務、事務取扱部署及び事務取扱担当者以外が、特定個人情報を参照できない仕組みを講じている。 ・健康管理システムでは、特定個人情報を参照できる機能と情報を限定しており、設定された利用権限の範囲を超えてアクセスができないように制御を行っている。
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
リスク2： 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	
ユーザ認証の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	健康管理システムへのアクセスにおいて、識別情報(ユーザID/パスワードと生体)による認証を実施している。また認証後は認可機能により、そのユーザが利用できる機能を制限することで、不正利用が行えないよう対策している。
その他の措置の内容	健康管理システムは、なりすまし防止策への対応として、一定時間経過で自動ログアウトする仕組みを実装している。
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

特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	
アクセスログを取得するとともに、定期的にログを解析できる仕組み、不正利用された場合にログを追跡できる仕組みを用意する。	
4. 特定個人情報ファイルの取扱いの委託 [] 委託しない	
リスク： 委託先における不正な使用等のリスク	
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[定めている] <選択肢> 1) 定めている 2) 定めていない
規定の内容	・目的外利用の禁止 ・特定個人情報の閲覧者・更新者の制限 ・特定個人情報の提供の禁止 ・情報漏えいを防ぐために保管管理に責任を負うこと。 ・必要に応じて委託先の視察・監査を行うこと。
再委託先による特定個人情報ファイルの適切な取扱いの担保	[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 4) 再委託していない
具体的な方法	再委託については、事前申請書を提出させ、審査のうえ適当と判断したものについて承諾している。委託先が責任を持って再委託先を管理・監督し、委託先と同等のセキュリティの確保を行わせる。
その他の措置の内容	－
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
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置	
1 情報保護管理体制の確認 委託先の社会的信用と能力を確認する。具体的には、「「松江市新行政情報システム構築・運用業務」企画提案実施要領」に基づき、委託業者を選定するとともに、その記録を残す。また、委託業者が選定基準を引き続き満たしていることを適時確認するとともに、その記録を残す。 2 特定個人情報ファイルの閲覧者・更新者の制限 (1) 作業者を限定するために、委託作業者の名簿を提出させる。 (2) 閲覧、更新権限を持つ者を必要最小限にする。 (3) 閲覧、更新権限を持つ者のアカウント管理を行い、システム上で操作を制限する。 (4) 閲覧、更新の履歴(ログ)を取得し、不正な使用がないことを確認する。 3 特定個人情報ファイルの取扱いの記録 (1) 契約書等に基づき、委託業務が実施されていることを適時確認するとともに、その記録を残す。 (2) 委託業者から適時セキュリティ対策の実施状況の報告を求めるとともに、その記録を残す。	

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
リスク：不正な提供・移転が行われるリスク		
特定個人情報の提供・移転に関するルール	[]	<選択肢> 1) 定めている 2) 定めていない
ルールの内容及び ルール遵守の確認方法		
その他の措置の内容		
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
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。）におけるその他のリスク及びそのリスクに対する措置		
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)
リスク1：目的外の入手が行われるリスク		
リスクに対する措置の内容	<中間サーバー・ソフトウェアにおける措置> 1 情報照会機能(※1)により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト(※2)との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。 つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 2 中間サーバーの職員認証・権限管理機能(※3)では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 (※1) 情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能 (※2) 番号法別表第2及び第19条第14号に基づき、事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。 (※3) 中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能	
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

リスク2: 不正な提供が行われるリスク	
リスクに対する措置の内容	＜番号連携サーバのソフトウェアにおける措置＞ 番号連携サーバの職員認証・権限管理機能により、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容等の記録が実施されるため、不適切な端末操作や情報照会などを抑止する。 ＜番号連携サーバの運用における措置＞ 番号連携サーバの職員認証・権限管理において、人事異動や権限変更等が生じた場合は、人事情報を適宜反映することで、その正確性を担保している。 ＜中間サーバー・ソフトウェアにおける措置＞ 1 情報提供機能(※)により、情報提供ネットワークシステムにおける照会許可照合リストを情報提供ネットワークシステムから入手し、中間サーバーにも格納して、情報提供機能により、照会許可照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 2 情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。 3 特に慎重な対応が求められる情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 4 中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 (※) 情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能
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
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	
＜中間サーバー・ソフトウェアにおける措置＞ 1 中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 2 情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバー・プラットフォームにおける措置＞ 1 中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、安全性を確保している。 2 中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 3 中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理(アクセス制御)しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 4 特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。	

7. 特定個人情報の保管・消去		
リスク： 特定個人情報の漏えい・滅失・毀損リスク		
①事故発生時手順の策定・周知	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
②過去3年以内に、評価実施機関において、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
その内容	-	
再発防止策の内容	-	
その他の措置の内容	<ガバメントクラウドにおける措置> 【物理的対策】 1 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、システムのサーバー等は、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 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。 【技術的対策】 1 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。 2 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関する基準【第1.0版】」(令和4年10月 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。 3 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。 4 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。 5 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。 6 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。 7 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。 8 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。	
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
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		
<中間サーバー・プラットフォームにおける措置> 【物理的対策】 中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 【技術的対策】 1 中間サーバー・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。 2 中間サーバー・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。 3 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> データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。		

8. 監査	
実施の有無	☐ 自己点検 ☐ 内部監査 ☐ 外部監査
9. 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 ☐ 十分に行っていない ☐ 十分に行っていない
具体的な方法	事務担当職員及び事業者に対して、定期的に必要な知識の習得に資するための研修や指導を行う。
10. その他のリスク対策	
＜中間サーバー・プラットフォームにおける措置＞ 中間サーバー・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。 ＜ガバメントクラウドにおける措置＞ ・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、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。 ・ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。 ・ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。 ・具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。	

Ⅳ 開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	郵便番号690-8540 島根県松江市末次町86番地 松江市役所 総務部総務課 法制・情報公関係 電話番号 0852-55-5555(代表)
②請求方法	指定様式による書面の提出により開示・訂正・利用停止請求を受け付ける。
③法令による特別の手続	－
④個人情報ファイル簿への不記載等	－
2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	郵便番号690-8540 島根県松江市末次町86番地 松江市役所 政策部デジタル戦略課 情報システム係 電話番号 0852-55-5555(代表)
②対応方法	・問い合わせの受付時に受付票を起票し、対応について記録を残す。 ・情報漏えい等の重大な事案に関する問い合わせについて、関係先等に事実確認を行うための標準的な処理期間を設ける。

Ⅴ 評価実施手続

1. 基礎項目評価	
①実施日	令和7年1月30日
②しきい値判断結果	[基礎項目評価及び重点項目評価の実施が義務付けられる] <選択肢> 1) 基礎項目評価及び重点項目評価の実施が義務付けられる 2) 基礎項目評価の実施が義務付けられる(任意に重点項目評価を実施) 3) 特定個人情報保護評価の実施が義務付けられない(任意に重点項目評価を実施)
2. 国民・住民等からの意見の聴取【任意】	
①方法	－
②実施日・期間	－
③主な意見の内容	－
3. 第三者点検【任意】	
①実施日	－
②方法	－
③結果	－

(別添2) 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1月30日	重点項目評価書	—	(重点項目評価の実施) ※「新型インフルエンザ等対策特別措置法による予防接種の実施に係る事務」及び「新型コロナウイルス感染症対策に係る予防接種事務」の特定個人情報保護評価を本「予防接種に関する事務」と併せて行うよう変更したことにより、しきい値が変更(増加)し、新たに重点項目評価を実施するもの。	事後	特定個人情報保護評価の統合により、重点項目評価を実施するもの(他の既評価は廃止)
令和7年1月30日	重点項目評価書	—	標準準拠システム稼働に伴い記載内容を変更	事前	