

# 特定個人情報保護評価書(全項目評価書)

評価書番号	評価書名
32	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関する事務 全項目評価書

## 個人のプライバシー等の権利利益の保護の宣言

宮崎市は、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十分な措置を行い、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

宮崎市長

## 個人情報保護委員会 承認日【行政機関等のみ】

## 公表日

令和5年3月1日

## 項目一覧

I 基本情報
(別添1) 事務の内容
II 特定個人情報ファイルの概要
(別添2) 特定個人情報ファイル記録項目
III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策
IV その他のリスク対策
V 開示請求、問合せ
VI 評価実施手続
(別添3) 変更箇所

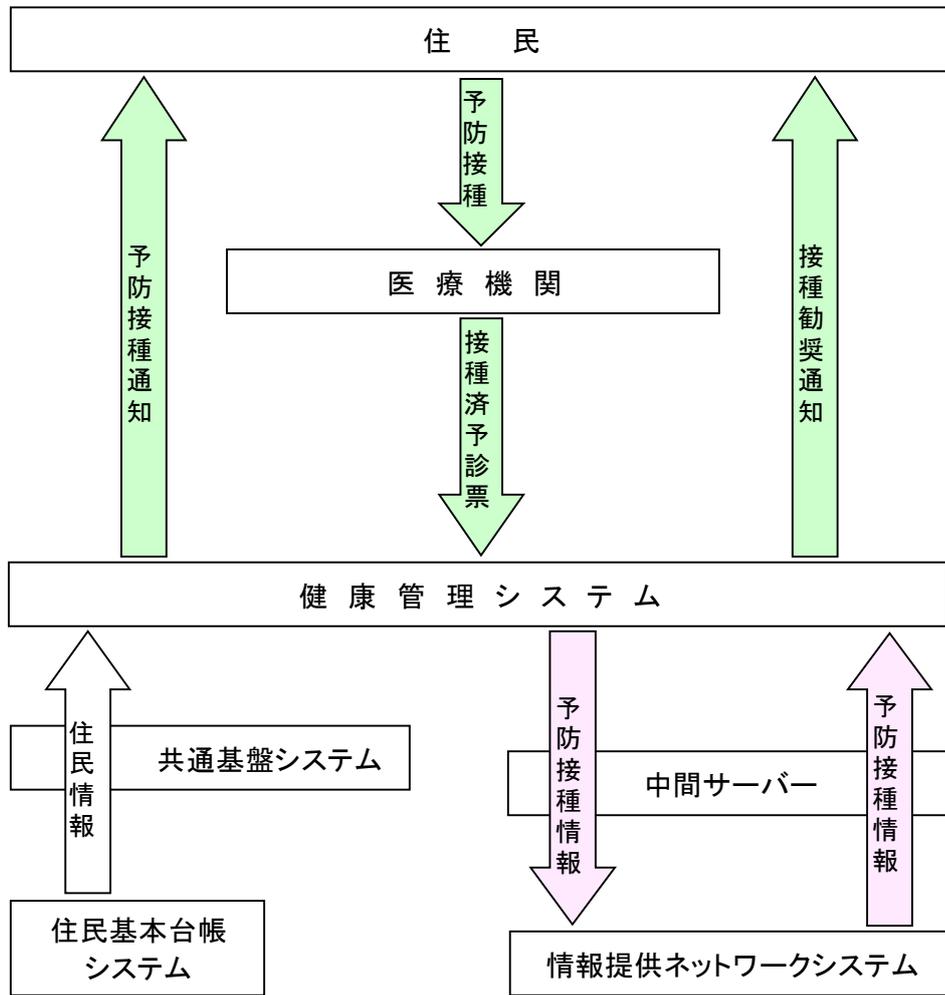
# I 基本情報

1. 特定個人情報ファイルを取り扱う事務									
①事務の名称	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関する事務								
②事務の内容 ※	新型インフルエンザ等対策特別措置法の規定に基づき、予防接種を実施する。 特定個人情報 は次の事務に利用する。 1. 予防接種対象者の確認と通知 2. 予防接種の記録とその管理 3. 未接種者への勧奨通知 4. 照会申請による予防接種履歴の照会								
③対象人数	[ 30万人以上 ] <table style="display: inline-table; vertical-align: middle; margin-left: 20px;"> <tr> <td colspan="2" style="text-align: center;">&lt;選択肢&gt;</td> </tr> <tr> <td style="width: 50%;">1) 1,000人未満</td> <td style="width: 50%;">2) 1,000人以上1万人未満</td> </tr> <tr> <td>3) 1万人以上10万人未満</td> <td>4) 10万人以上30万人未満</td> </tr> <tr> <td>5) 30万人以上</td> <td></td> </tr> </table>	<選択肢>		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	5) 30万人以上	
<選択肢>									
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								
5) 30万人以上									
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. 対象者のデータ抽出 2. 予防接種履歴の入力 3. 委託料の支払明細書の出力 4. 予防接種台帳の検索 5. その他上記に関連する機能								
③他のシステムとの接続	<table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">[ ] 情報提供ネットワークシステム</td> <td style="width: 50%;">[ ] 庁内連携システム</td> </tr> <tr> <td>[ ] 住民基本台帳ネットワークシステム</td> <td>[ <input checked="" type="checkbox"/> ] 既存住民基本台帳システム</td> </tr> <tr> <td>[ <input checked="" type="checkbox"/> ] 宛名システム等</td> <td>[ ] 税務システム</td> </tr> <tr> <td colspan="2">[ ] その他 ( )</td> </tr> </table>	[ ] 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	[ <input checked="" type="checkbox"/> ] 既存住民基本台帳システム	[ <input checked="" type="checkbox"/> ] 宛名システム等	[ ] 税務システム	[ ] その他 ( )	
[ ] 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	[ <input checked="" type="checkbox"/> ] 既存住民基本台帳システム								
[ <input checked="" type="checkbox"/> ] 宛名システム等	[ ] 税務システム								
[ ] その他 ( )									
システム2～5									
システム2									
①システムの名称	団体内統合宛名システム								
②システムの機能	1. 宛名管理機能 (1) サーバ内の宛名データベースのセットアップ (2) 宛名の異動データを取り込み、宛名データベースへ反映 (3) 個人番号にて同一人物判定を行い、団体内統合宛名番号を採番し管理 (4) 宛名データベースの検索、参照、更新 (5) オンラインで入力したデータを業務システムに連携 (6) 団体内統合宛名番号を業務システムに連携  2. 情報提供機能 (1) 中間サーバに連携する各業務情報をデータベースへセットアップ (2) 各業務の異動データを取り込み、データベースに反映 (3) 各業務情報を一括で中間サーバに連携 (4) 各業務の異動情報を中間サーバに連携  3. 情報照会機能(他機関への情報照会) (1) 各業務の宛名番号で対象者を検索し、他自治体への情報提供を依頼し、オンラインにて表示する。 (2) 情報照会の対象者情報を基に中間サーバに情報を要求し、一括ファイルを作成する。  4. 符号要求 (1) 処理通番を要求、受信し、符号要求データを住記システム(既存住民基本台帳システム)に送信す								



3. 特定個人情報ファイル名	
予防接種台帳ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	<p>新型インフルエンザ等対策特別措置法に基づく予防接種を円滑に実施するために、次の作業を迅速に行う必要がある。</p> <p>1. 対象者の抽出し、接種勧奨を行い、接種記録を保存し、万が一健康被害が生じたときに速やかに対応する。</p> <p>2. 既接種者又は未接種者を正確に把握し、再勧奨を行う。</p> <p>3. 接種情報の集計を行う。</p>
②実現が期待されるメリット	<p>1. 対象者を正確に抽出できることで、接種順位が高い者により早く勧奨することができる。</p> <p>2. 市民からの予防接種歴に関する問い合わせに正確に回答でき、接種間違いを防止できる。</p> <p>3. 未接種者を把握することにより、再勧奨を行い、接種率を向上させ、新型インフルエンザのまん延防止を図ることができる。</p> <p>4. 健康被害が生じた際に、接種情報が確認でき、速やかに対応できる。</p> <p>5. 集計作業が速やかに行うことができる。</p>
5. 個人番号の利用 ※	
法令上の根拠	<p>・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5月31日法律第27号)(以下「番号法」という。)第9条第1項 別表第一の93の2の項</p> <p>・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(平成26年9月10日内閣府・総務省令第5号)第67条の2</p>
6. 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	<p>[ 実施する ]</p> <p style="text-align: right;">&lt;選択肢&gt; 1) 実施する 2) 実施しない 3) 未定</p>
②法令上の根拠	<p>・番号法第19条第7号(特定個人情報の提供の制限)及び別表第二及び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(平成26年12月12日内閣府・総務省令第7号。以下「別表第二主務省令」という。)</p> <p>[情報提供の根拠]</p> <p>・別表第二(16の2、16の3の項、115の2の項)</p> <p>・別表第二主務省令(第12条の2、第12条の2の2)</p> <p>[情報照会の根拠]</p> <p>・別表第二(16の2、17、18、19の項、115の2の項)</p> <p>・別表第二主務省令(第12条の2、第12条の3、第13条、第13条の2)</p>
7. 評価実施機関における担当部署	
①部署	宮崎市健康管理部健康支援課
②所属長の役職名	健康支援課長
8. 他の評価実施機関	
—	

(別添1) 事務の内容



(備考)

## 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		
予防接種台帳ファイル		
2. 基本情報		
①ファイルの種類 ※	[ システム用ファイル ] <選択肢> 1) システム用ファイル 2) 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 ] <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	
③対象となる本人の範囲 ※	予防接種対象者及び予防接種済みの者	
その必要性	予防接種状況を把握するために、接種履歴を管理する必要がある。	
④記録される項目	[ 10項目以上50項目未満 ] <選択肢> 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上	
主な記録項目 ※	<ul style="list-style-type: none"> <li>・識別情報 [ <input type="checkbox"/> ] 個人番号 [ <input type="checkbox"/> ] 個人番号対応符号 [ <input type="checkbox"/> ] その他識別情報(内部番号)</li> <li>・連絡先等情報 [ <input type="checkbox"/> ] 4情報(氏名、性別、生年月日、住所) [ <input type="checkbox"/> ] 連絡先(電話番号等) [ <input type="checkbox"/> ] その他住民票関係情報</li> <li>・業務関係情報 [ <input type="checkbox"/> ] 国税関係情報 [ <input type="checkbox"/> ] 地方税関係情報 [ <input type="checkbox"/> ] 健康・医療関係情報 [ <input type="checkbox"/> ] 医療保険関係情報 [ <input type="checkbox"/> ] 児童福祉・子育て関係情報 [ <input type="checkbox"/> ] 障害者福祉関係情報 [ <input type="checkbox"/> ] 生活保護・社会福祉関係情報 [ <input type="checkbox"/> ] 介護・高齢者福祉関係情報 [ <input type="checkbox"/> ] 雇用・労働関係情報 [ <input type="checkbox"/> ] 年金関係情報 [ <input type="checkbox"/> ] 学校・教育関係情報 [ <input type="checkbox"/> ] 災害関係情報 [ <input type="checkbox"/> ] その他 ( )</li> </ul>	
	その妥当性	<ul style="list-style-type: none"> <li>・個人番号:住民であることの確認</li> <li>・その他識別番号:対象者を正確に把握するために保有</li> <li>・4情報:予防接種の事務遂行と接種歴の保管のために保有</li> <li>・連絡先:予防接種事故等に対応する際連絡先が必要</li> <li>・その他住民票関係情報:異動等の年月日確認のために保有</li> <li>・健康・医療関係情報:予防接種歴の保管のために保有</li> </ul>
	全ての記録項目	別添2を参照。
⑤保有開始日	令和3年4月1日	
⑥事務担当部署	宮崎市健康管理部健康支援課	

3. 特定個人情報の入手・使用		
①入手元 ※	<input checked="" type="checkbox"/> 本人又は本人の代理人 <input checked="" type="checkbox"/> 評価実施機関内の他部署 ( 市民課 ) <input type="checkbox"/> 行政機関・独立行政法人等 ( ) <input checked="" type="checkbox"/> 地方公共団体・地方独立行政法人 ( 都道府県、他市区町村 ) <input type="checkbox"/> 民間事業者 ( ) <input type="checkbox"/> その他 ( )	
②入手方法	<input checked="" type="checkbox"/> 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 <input type="checkbox"/> 電子メール [ ] 専用線 <input checked="" type="checkbox"/> 庁内連携システム <input checked="" type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> その他 ( )	
③入手の時期・頻度	予防接種実施後、提出される予診票による。	
④入手に係る妥当性	予防接種に関する記録については、法令に基づき記録・保管する目的で取得している。接種状況を常に把握するために、接種が確認できた時点で速やかに反映させる必要がある。	
⑤本人への明示	予防接種に関する記録については、予防接種法等関連法令に、市区町村が予防接種に関する記録を作成・保管する義務が明記されており、予防接種票においても、接種済の予防接種票が市に提出されることを明記し、本人(親権者等)から署名を得た上で取得する。	
⑥使用目的 ※	予防接種の実施、予防接種に関する記録の作成	
	変更の妥当性	—
⑦使用の主体	使用部署 ※	宮崎市健康管理部健康支援課
	使用者数	<input type="checkbox"/> 10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
⑧使用方法 ※	<ul style="list-style-type: none"> <li>・予防接種対象者の抽出</li> <li>・予防接種履歴の入力と確認</li> <li>・統計データの出力</li> </ul>	
	情報の突合 ※	本人を検索し、住民情報、接種履歴を確認する。
	情報の統計分析 ※	特定の個人を判明する情報の統計分析は行わない。
	権利利益に影響を与え得る決定 ※	—
⑨使用開始日	令和3年4月1日	









**(別添2) 特定個人情報ファイル記録項目**

**<健康管理システム>**

**(1) 識別情報**

- ① 個人番号
- ② 健康管理番号
- ③ 住民票コード

**(2) 連絡先等情報**

- ① 氏名情報
- ② 生年月日
- ③ 性別
- ④ 続柄
- ⑤ 住民となった年月日
- ⑥ 住民となった事由
- ⑦ 住民区分(日本人、外国人)
- ⑧ 世帯主情報
- ⑨ 現住所情報
- ⑩ 住所を定めた年月日
- ⑪ 前住所情報、転入元住所情報、転出先住所情報
- ⑫ 消除情報
- ⑬ 通称(外国人住民のみ)の記載
- ⑭ 転出予定者情報
- ⑮ 電話番号

**(3) 業務関係情報**

- ① 予防接種歴

### Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※(7. リスク1⑨を除く。)

1. 特定個人情報ファイル名	
予防接種台帳ファイル	
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1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	(1)届出／申請等の窓口において届出／申請内容や本人確認書類(身分証明書等)の確認を厳格に行い、対象者以外の情報の入手を防止する。 (2)予防接種歴の入手については複数項目の本人情報の確認を行っている。
必要な情報以外を入手することを防止するための措置の内容	(1)予防接種歴の記載箇所を明確化し、不要な情報は記載されない様式となっている。 (2)システムに入力する情報は予診票等に記載された内容を番号化し、入力する仕様になっている。 (3)入力内容の点検は入力を行った者以外のものが確認する。
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
リスク2： 不適切な方法で入手が行われるリスク	
特定個人情報の正確性確保の措置の内容	入手した特定個人情報は、システムで確認した特定個人情報と突合して正確性を確保する。正確性に疑義が生じた場合は、随時調査を行い、必要に応じてデータを修正することで正確性を確保する。
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
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	①システムは、インターネットに接続されていない閉鎖的なネットワークであり、外部システムとは接続されていないため、ネットワークを通じての情報漏えいは無い。 ②紙媒体による入手の場合は、システムへの入力完了後、鍵のかかる書庫またはキャビネット等に保管する。
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
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	
—	

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	
宛名システム等における措置の内容	<ul style="list-style-type: none"> <li>・健康管理システムから他のシステムへの特定個人情報の連携は必要となる情報のみに制限し、必要のない情報との紐付けは行われないう制限する。</li> <li>・市で定める個人番号利用事務実施者以外(予防接種事業の事務実施者以外)から特定個人情報の要求があった場合は、個人番号と個人情報の紐付けが行われないうシステムで アクセス制御を行っている。</li> <li>・団体内統合宛名システムにおいては個別業務において管理する特定個人情報を保持しない。</li> </ul>
事務で使用するその他のシステムにおける措置の内容	
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
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	<ul style="list-style-type: none"> <li>・ユーザIDとパスワード及び静脈による認証を行っている。</li> <li>・認証後は、ユーザ毎に利用可能な機能を制限している。</li> <li>・パスワードについては、定期的に変更している。</li> </ul>
アクセス権限の発効・失効の管理	[ 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	<ul style="list-style-type: none"> <li>・人事異動があった場合や権限変更があった場合には書面にて決裁し、システムに反映させている。</li> <li>・ユーザIDやアクセス権限を定期的に確認し、業務上アクセスが不要となったIDやアクセス権限を変更又は削除する。</li> </ul>
アクセス権限の管理	[ 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	・共用IDは発行せず、個人に対してユーザIDを発行する。
特定個人情報の使用の記録	[ 記録を残している ] <選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	端末から参照、更新した場合のアクセスログ(操作日時、操作端末、操作者情報(所属・職員名)等)を記録している。
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
リスク3: 従業者が事務外で使用するリスク	
リスクに対する措置の内容	定期的実施する情報セキュリティや守秘義務に関する研修を通して、特定個人情報の事務外利用の禁止や漏えい時の罰則、アクセスログが確実に記録されていること等について、職員に周知徹底している。
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
リスク4: 特定個人情報ファイルが不正に複製されるリスク	
リスクに対する措置の内容	特定の電子記録媒体以外は作業端末に使用できないように制限しており、電子記録媒体は厳重に管理している。
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	
—	

4. 特定個人情報ファイルの取扱いの委託		[ ] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認	<ul style="list-style-type: none"> <li>・システム運用で、外部委託業者を選定する際、委託先の情報保護管理体制としてプライバシーマーク等、個人情報保護や対策を目的として公共機関の認定・認証を取得していることを契約要件としているほか、事業実績など社会的信用と能力があることを確認している。</li> <li>・システム運用以外の委託については、委託契約書で個人情報の保護について遵守するよう義務付けている。</li> </ul>	
特定個人情報ファイルの閲覧者・更新者の制限	[ 制限している ] <選択肢> 1) 制限している 2) 制限していない	
具体的な制限方法	委託契約において、委託業務で取り扱う情報の目的外使用や複写等の禁止、委託業務の終了後の情報の消去及び消去内容の報告、委託業務で使用するパソコン等の盗難防止対策の実施、システム用IDの適切な管理等の対策の実施、情報セキュリティに関する教育の実施等、情報セキュリティの確保に必要な人的・物的・技術的対策の実施を義務付けている。	
特定個人情報ファイルの取扱いの記録	[ 記録を残している ] <選択肢> 1) 記録を残している 2) 記録を残していない	
具体的な方法	<ul style="list-style-type: none"> <li>・システムへのログイン記録やシステム保守における作業記録を残している。</li> <li>・電子記録媒体等については、管理簿を作成し、引渡し及び返却を管理する。</li> </ul>	
特定個人情報の提供ルール	[ 定めている ] <選択肢> 1) 定めている 2) 定めていない	
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	<ul style="list-style-type: none"> <li>・契約書にて委託先から他者への提供を禁止している。</li> </ul>	
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	<ul style="list-style-type: none"> <li>・委託先への提供、または委託先から受領するときは、日付、枚数を記録した受け渡しの確認記録を残す。</li> <li>・搬送時は、媒体にパスワードを付けるなど、運搬時のセキュリティーが確保できる方法で行っている。</li> <li>・遵守の確認は、提供・受領の都度行っている。</li> </ul>	
特定個人情報の消去ルール	[ 定めている ] <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	<ul style="list-style-type: none"> <li>・委託先は、業務に使用した資料等を契約完了後直ちに委託元に返却または消去する事を契約書、協定書に明記している。</li> <li>・遵守の確認は業務完了報告書で行う。</li> </ul>	
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	個人情報保護条項として以下を定めている。 <ul style="list-style-type: none"> <li>・第三者への提供・開示・漏えいの禁止</li> <li>・目的外利用の禁止</li> <li>・無断複製の禁止</li> <li>・契約終了後の返還・廃棄・消去</li> <li>・安全管理体制の整備・確保・報告</li> </ul>	
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確保	[ 十分に行っている ] <選択肢> 1) 特に力を入れている 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	契約書において、「受注者は、委託業務の処理を他に委託し、又は請け負わせてはならない。ただし、書面により発注者の承諾を得たときは、この限りでない。」としている。許可した場合は、通常の委託と同様の措置を再委託先にも義務付けている。	
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		
—		

**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1： 不正な提供・移転が行われるリスク**

特定個人情報の提供・移転の記録	[ <input type="checkbox"/> ]	<選択肢> 1) 記録を残している	2) 記録を残していない
具体的な方法			
特定個人情報の提供・移転に関するルール	[ <input type="checkbox"/> ]	<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	[ <input type="checkbox"/> ]	<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： 不適切な方法で提供・移転が行われるリスク**

リスクに対する措置の内容			
リスクへの対策は十分か	[ <input type="checkbox"/> ]	<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3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク**

リスクに対する措置の内容			
リスクへの対策は十分か	[ <input type="checkbox"/> ]	<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	<p>&lt;中間サーバ・プラットフォームにおける措置&gt;</p> <p>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。</p> <p>②中間サーバの職員認証・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制する仕組みになっている。</p> <p>(※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</p> <p>(※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</p> <p>(※3)中間サーバ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</p>		
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 3) 課題が残されている	2) 十分である
リスク2: 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容	<p>&lt;中間サーバ・ソフトウェアにおける措置&gt;</p> <p>①中間サーバは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理す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入手のみ実施できるように設計されるため、安全性が担保されている。</p> <p>&lt;中間サーバ・プラットフォームにおける措置&gt;</p> <p>①中間サーバと既存システム、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(LGWAN等)を利用することにより、安全性を確保している。</p> <p>②中間サーバと団体については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。</p>		
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 3) 課題が残されている	2) 十分である
リスク3: 入手した特定個人情報ที่ไม่正確であるリスク			
リスクに対する措置の内容	<p>&lt;中間サーバ・ソフトウェアにおける措置&gt;</p> <p>①中間サーバは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。</p>		
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 3) 課題が残されている	2) 十分である
リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク			
リスクに対する措置の内容	<p>&lt;中間サーバ・ソフトウェアにおける措置&gt;</p> <p>①中間サーバは、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入手のみを実施するため、漏えい・紛失のリスクに対応している(※)。</p> <p>②既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。</p> <p>③情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報が漏えい・紛失するリスクを軽減している。</p> <p>④中間サーバの職員認証・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制する仕組みになっている。</p> <p>(※)中間サーバは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。</p> <p>&lt;中間サーバ・プラットフォームにおける措置&gt;</p> <p>①中間サーバと既存システム、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(LGWAN等)を利用することにより、漏えい・紛失のリスクに対応している。</p> <p>②中間サーバと団体については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漏えい・紛失のリスクに対応している。</p> <p>③中間サーバ・プラットフォーム事業者の業務は、中間サーバ・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。</p>		

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5: 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	<p>&lt;中間サーバ・ソフトウェアの措置&gt;</p> <p>①情報提供機能(※)により、情報提供ネットワークシステムの照会許可照会リストを情報提供ネットワークシステムから入手し、中間サーバにも格納して、情報提供機能により、照会許可照会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。</p> <p>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。</p> <p>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。</p> <p>④中間サーバの職員認証・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。</p> <p>(※)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</p>	
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6: 不適切な方法で提供されるリスク		
リスクに対する措置の内容	<p>&lt;中間サーバ・ソフトウェアにおける措置&gt;</p> <p>①セキュリティ管理機能(※)により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。</p> <p>②中間サーバの職員認証・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。</p> <p>(※)暗号化・復号機能と、鍵情報及び照会許可照会リストを管理する機能</p> <p>&lt;中間サーバ・プラットフォームにおける措置&gt;</p> <p>①中間サーバと既存システム、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(LGWAN等)を利用することにより、不適切な方法で提供されるリスクに対応している。</p> <p>②中間サーバと団体については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漏えい・紛失のリスクに対応している。</p> <p>③中間サーバ・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。</p>	
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7: 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク		
リスクに対する措置の内容	<p>&lt;中間サーバ・ソフトウェアにおける措置&gt;</p> <p>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情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。</p> <p>②情報提供データベース管理機能(※)により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。</p> <p>③情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。</p> <p>(※)特定個人情報を副本として保存・管理する機能。</p>	
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・ソフトウェアにおける措置＞

- ①中間サーバの職員認証・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・プラットフォームにおける措置＞

- ①中間サーバと既存システム、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(LGWAN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・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・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・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1: 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[ 政府機関ではない ]	<選択肢> 1) 特に力を入れて遵守している 2) 十分に遵守している 3) 十分に遵守していない 4) 政府機関ではない
②安全管理体制	[ 十分に整備している ]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
③安全管理規程	[ 十分に整備している ]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
④安全管理体制・規程の職員への周知	[ 十分に周知している ]	<選択肢> 1) 特に力を入れて周知している 2) 十分に周知している 3) 十分に周知していない
⑤物理的対策	[ 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
	具体的な対策の内容	<p>&lt;本市における措置&gt;</p> <ul style="list-style-type: none"> <li>・サーバ室の入口でチェックを行い、サーバの操作を許可された人だけが入場できる場所に施錠されたサーバラック内にサーバを設置している。</li> <li>・入退室は鍵の使用簿により管理している。</li> <li>・停電(落雷等)によるデータの消失を防ぐために、サーバに無停電電源装置等を付設している。</li> <li>・火災によるデータ消失を防ぐために、施設内に消火設備の完備や消化器具の設置を行っている。</li> <li>・紙媒体については、カルテ庫など施錠可能な場所に保管している。</li> </ul> <p>&lt;中間サーバ・プラットフォームにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul>
⑥技術的対策	[ 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
	具体的な対策の内容	<p>&lt;本市における措置&gt;</p> <ul style="list-style-type: none"> <li>・ウイルス対策ソフトの定期的パターンファイルの更新を行っている。</li> <li>・外部ネットワークから遮断された独自のネットワークで運用することで、不正アクセス対策を行っている。</li> </ul> <p>&lt;中間サーバ・プラットフォームにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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驚異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。</li> <li>・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。</li> <li>・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。</li> </ul>
⑦バックアップ	[ 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
⑧事故発生時手順の策定・周知	[ 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
⑨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	
⑩死者の個人番号	[ 保管している ]	<選択肢> 1) 保管している 2) 保管していない
	具体的な保管方法	現存者と同様の管理を行っている。
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

リスク2: 特定個人情報が古い情報のまま保管され続けるリスク	
リスクに対する措置の内容	住民記録情報については、住民基本台帳上の記録が更新される都度、最新の情報が連携される。
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
リスク3: 特定個人情報が消去されずいつまでも存在するリスク	
消去手順	[ 定めている ] <選択肢> 1) 定めている 2) 定めていない
手順の内容	<ul style="list-style-type: none"> <li>・サーバ、端末(パソコン)、記録媒体、予診票等の情報資産を廃棄する場合は、情報を復元できないように処置した上で廃棄する。機器リース終了による返却の場合も同様とする。</li> <li>・紙文書は、溶解又はシュレッダー処分を行う。</li> <li>・電磁的な記録媒体は、破碎処理、電磁気破壊、データ消去ソフトウェアによるデータ消去を行った上で廃棄する。</li> <li>・サーバ、パソコン等情報機器については、記録装置に対し、物理破壊、磁気破壊、データ消去ソフトウェアによるデータ消去を行う。</li> <li>・データ消去を業者に委託した場合は、消去作業証明書を提出させる。</li> </ul>
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	
—	

## IV その他のリスク対策 ※

1. 監査	
①自己点検	[ 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
具体的なチェック方法	・特定個人情報保護に関する自己点検項目を整備し、年に1回、特定個人情報保護に関する研修を実施するとともに自己点検を実施する。
②監査	[ 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
具体的な内容	内部監査 2年に1回、組織内に置かれた監査担当により、以下の観点による自己監査を実施し、監査結果を踏まえて体制や規定を改善する。 ・評価書記載事項と運用実態のチェック ・個人情報保護に関する規定、体制整備 ・個人情報保護に関する人的安全管理措置 ・職員の役割責任の明確化、安全管理措置の周知・教育 ・個人情報保護に関する技術的安全管理措置 外部監査 民間機関等の外部監査事業者による監査を実施し、監査結果を踏まえて体制や規定を改善する。
2. 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
具体的な方法	・関係職員(会計年度任用職員等を含む。)に対して、初任時及び一定期間毎に、守秘義務を含む必要な知識の習得に資するための研修を実施している。併せて不正な取扱いが重大な罪であることを十分に周知する。
3. その他のリスク対策	
<中間サーバ・プラットフォームにおける措置> ①中間サーバ・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リテラシー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。	



## VI 評価実施手続

1. 基礎項目評価	
①実施日	令和4年12月21日
②しきい値判断結果	[ 基礎項目評価及び全項目評価の実施が義務付けられる ] <選択肢> 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 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(任意に全項目評価を実施) 3) 基礎項目評価の実施が義務付けられる(任意に全項目評価を実施) 4) 特定個人情報保護評価の実施が義務付けられない(任意に全項目評価を実施)
2. 国民・住民等からの意見の聴取	
①方法	宮崎市パブリックコメント制度実施要綱に基づくパブリックコメント手続により意見聴取を実施する。実施に際しては、宮崎市ホームページ及び市民課、市民情報センター等において全文を閲覧できるようにした。
②実施日・期間	令和3年7月1日から8月2日(33日間)
③期間を短縮する特段の理由	-
④主な意見の内容	・意見なし
⑤評価書への反映	なし
3. 第三者点検	
①実施日	令和3年10月22日
②方法	宮崎市個人情報保護審査会による第三者点検を実施した。
③結果	・意見なし
4. 個人情報保護委員会の承認【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

