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
5	予防接種に関する事務　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	
福岡市は、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り扱いにあたり、特定個人情報ファイルの取り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
福岡市長

特定個人情報保護委員会　承認日 【行政機関等のみ】
公表日

［平成26年４月　様式4］

項目一覧

Ⅰ　基本情報

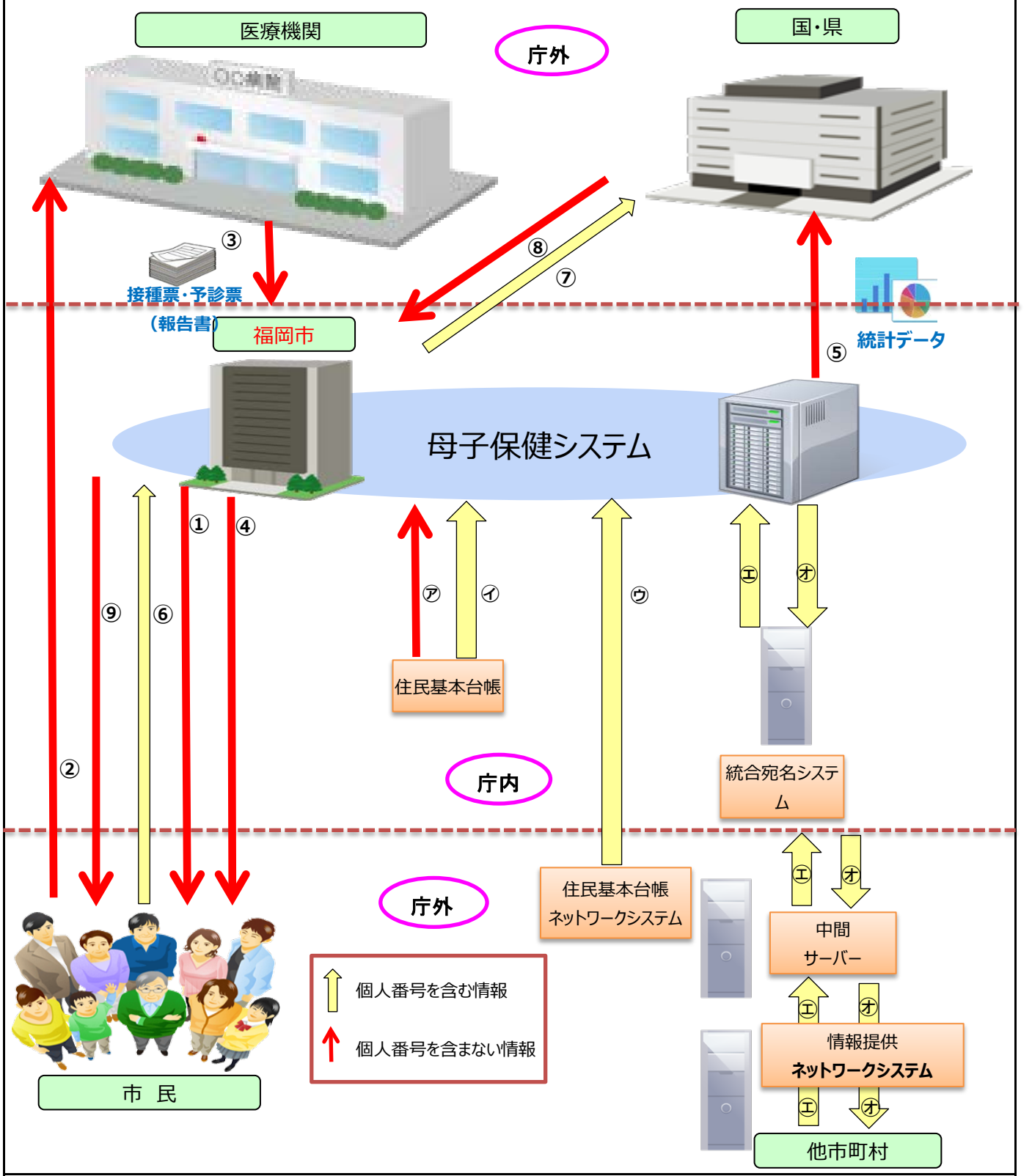
1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	予防接種に関する事務
②事務の内容　※	公衆衛生の見地から、市内に居住する者に対し、期日又は期間を指定して予防接種の実施その他必要な措置を講ずることにより、市民の健康の保持に寄与するとともに、予防接種による健康被害の迅速な救済を図る。 特定個人情報ファイルは、予防接種法及び行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「番号法」という。）の規定に従い、次の事務に利用する。 【法的根拠】 番号法第9条第1項 ①各種予防接種の案内 定期の予防接種対象者を抽出するために必要な住民基本台帳情報を入手し、予防接種の種類、実施医療機関及び期日又は期間を案内する。 ②予防接種履歴の管理 各医療機関で実施した予防接種の記録を取得し、データ化したファイルを母子保健システムに登録し、管理する。 ③予防接種による健康被害救済給付 予防接種による健康被害が発生した場合の健康被害者からの認定申請（医療費医療手当，障害児養育年金及び障害年金，死亡一時金及び遺族年金・遺族一時金，葬祭料）において被接種者の接種歴及び住基情報を確認する。
③対象人数	[　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	母子保健システム
②システムの機能	母子保健システムにおける特定個人ファイルを取り扱う事務機能は，以下の機能から構成されている。 1. 接種結果の登録 接種結果の登録及び保管 2. 未接種者リストの抽出及び作成 3. 集計及び統計機能 予防接種の種類別等の集計，国等への統計報告リストの抽出及び作成
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2	
①システムの名称	統合宛名システム
②システムの機能	1　宛名管理機能 統合宛名番号が未登録の個人について，新規に統合宛名番号を付番する。また，各既存業務システムの宛名情報を統合宛名番号，個人番号とひも付けて保存し管理する。 2　情報提供機能 各既存業務システムの業務情報を中間サーバ向けに一括で変換，連携を実施し，業務情報を中間サーバに提供する。 3　情報照会機能 他機関への情報照会をオンラインによる1件ずつの問合せ，またはバッチによる一括での問合せを行う。また，問合せ結果の受領を行う。 4　符号要求機能 符号未取得の対象者データが情報連携された場合，個人番号を特定済みの統合宛名番号を中間サーバに登録し，既存住基システム及び住基ネットを介して，機構に情報提供用個人識別符号の取得要求・取得依頼を行う。 5　権限管理機能 統合宛名システム端末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個人情報(連携対象)へのアクセス制御を行う。
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　（ 中間サーバ、各業務システム　　）
システム3	
①システムの名称	中間サーバ
②システムの機能	1　符号管理機能 符号管理機能は情報照会、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「統一識別番号」とを紐付け、その情報を保管・管理する。 2　情報照会機能 情報照会機能は、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。 3　情報提供機能 情報提供機能は、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。 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基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。 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。 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。 7　データ送受信機能 中間サーバ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。 8　セキュリティ管理機能 暗号化／復号機能と鍵情報及び照会許可用照合リスト情報を管理する。 9　職員認証・権限管理機能 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(連携対象)へのアクセス制御を行う。 10　システム管理機能 バッチの状況管理、業務統計情報の集計、稼動状態の通知、保管期限切れ情報の削除を行う。
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　（　　）

3. 特定個人情報ファイル名	
予防接種情報ファイル	
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	予防接種の対象者及び接種履歴を正確に把握し，適正な管理を行うため。
②実現が期待されるメリット	現行の予防接種の対象者であることの確認及び受けた予防接種の履歴を管理する台帳管理に加え，番号制度と結びつけることにより，転入転出等における効率的な事務が可能となる。
5. 個人番号の利用 ※	
法令上の根拠	・行政手続き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（番号法）第9条第1項 別表第一の10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第10条
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	[　　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	（別表第二における情報提供の根拠） ・番号法第19条第7号　別表第二の16の2及び18の項 （別表第二における情報照会の根拠） ・番号法第19条第7号　別表第二の16の2，17，18の項及び19の項 ・番号法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13条
7. 評価実施機関における担当部署	
①部署	保健福祉局 健康医療部 保健予防課
②所属長	保健予防課長　執行　睦実
8. 他の評価実施機関	
―	

（別添1）事務の内容



（備考）

㋐・・・定期の予防接種対象者を抽出するために必要な「住民情報」を取得（①予防接種の案内・勧奨等に使用）※個人番号は取得しない。
㋑・・・定期の予防接種者の履歴を管理する為に必要な「個人番号」を取得（③予防接種履歴を個人番号と紐づけて母子保健システムで管理）
㋒・・・住民基本台帳登録外の定期の予防接種対象者の履歴を管理する為，住民基本台帳ネットワークシステムを用いて必要な「個人番号」を取得
㋓・・・「他市町村からの転入者に関する予防接種歴情報」を取得するために中間サーバー経由で照会（平成29年7月以降）
㋔・・・「他市町村への転居者に関する予防接種歴情報」を中間サーバー経由で提供（平成29年7月以降）

①・・・予防接種の種類、予防接種場所及び期日又は期間を郵送等で案内
②・・・案内や勧奨を受けた予防接種について、医療機関で予防接種
③・・・医療機関で実施した予防接種の記録を取得し、母子保健システムに登録のうえ管理
④・・・予防接種に対し、郵送等で予防接種未接種勧奨
⑤・・・福岡県及び国へ統計等の報告
⑥・・・福岡市へ予防接種健康被害救済給付請求の提出
⑦・・・県を経由して国へ予防接種健康被害救済給付請求の進達
⑧・・・県を経由して国から認定結果通知
⑨・・・本人及び保護者への結果通知及び医療費・医療手当等の健康被害救済給付

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	
予防接種情報ファイル	
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　※	福岡市に住民登録している定期の予防接種を受けた者
その必要性	市で実施する事業の予防接種情報を適正に管理する必要があるため
④記録される項目	[　50項目以上100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　※	・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	①個人番号、その他識別情報：対象者を正確に特定するために保有 ②4情報、連絡先、その他住民票関係情報：正確な本人特定のため、接種票等に記入された情報と突合するために保有、また、予防接種の勧奨に使用するため保有 ③健康・医療関係情報：予防接種履歴管理および勧奨を適正に行うために保有
全ての記録項目	別添2を参照。
⑤保有開始日	平成27年12月予定
⑥事務担当部署	保健福祉局健康医療部保健予防課，各区保健福祉センター健康課

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 （ ・市民局総務部区政課 ） [ ] 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 （ ） [ ] 民間事業者 （ ） [○] その他 （ 地方公共団体情報システム機構 ）
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入手の時期・頻度		（1）住民基本台帳情報 ・入手先：住民基本台帳システム ・入手方法：住民基本台帳システムからのデータ連携（庁内連携により入手） ・入手時期・頻度：①個人番号の付番・通知日（平成27年10月5日）以後に準備行為として一括入手 ②番号利用開始日（平成28年1月1日）以後は日次の頻度 （2）予防接種健康被害救済請求申請の都度，紙で入手。 （3）他市町村からの転入者に対し，他市町村へ照会する都度，情報提供ネットワークシステムを介して入手。 （4）住民基本台帳登録外の対象者について，本人確認情報の調査が必要となった都度，住民基本台帳ネットワークシステムを介して入手。
④入手に係る妥当性		住民基本台帳システムから入手する住民基本情報については、本人等からの申請を受けた都度入手する必要があり、法令等に基づく予防接種対象者であることの確認。 予防接種健康被害救済請求は本人等からの申請によるものである。 住民基本台帳登録外の対象者本人確認情報の調査に必要な範囲内で，住民基本台帳ネットワークシステムにより情報収集を適宜行う必要がある。
⑤本人への明示		住民基本台帳システムから住民基本情報を入手の場合、番号法及び予防接種法施行規則により明示されている。 本人及び代理人から入手する情報は、書面にて利用目的を明示する。 住民基本台帳ネットワークシステムによる入手の場合、番号法により、地方公共団体情報システム機構に対し機構保存本人確認情報の提供を求めることができる旨明示されている。
⑥使用目的 ※		予防接種の実施にあたり、本人の資格確認（住所、年齢等）をし、接種記録の保管・管理を行い、未接種者に対する接種勧奨を実施する。 また予防接種健康被害救済給付認定については，本人の資格（住所、年齢等）及び給付対象となる接種歴を確認する。
	変更の妥当性	
⑦使用の主体	使用部署 ※	保健福祉局健康医療部保健予防課，各区保健福祉センター健康課
	使用者数	[100人以上500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 ※		①対象者の資格（住所、年齢）確認 医療機関からの接種記録について、住民基本台帳システムをもとに対象者であることを確認する。 住民基本台帳登録外の対象者について，住民基本台帳ネットワークシステムを用いて，個人番号を取得する。 ②接種記録の保管・管理 母子保健システムに医療機関からの情報を登録し、保管・管理を行う。 ③健康被害救済給付認定申請時の資格確認（住基情報及び接種歴）
	情報の突合 ※	・本人等からの申請及び医療機関からの住所・氏名等の情報について、住民基本台帳システムと突合し、対象者の資格を確認すること及び接種記録を保管・管理する。
	情報の統計分析 ※	特定の個人を判別するような情報の分析や統計は行わない。また、個人番号を使用した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		平成28年1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 （ 1 ） 件
委託事項1		母子保健システム運用保守業務
①委託内容		システムの運用管理，障害対応など
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] ＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	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
	対象となる本人の範囲 ※	福岡市に住民登録しているシステムの対象となる者
	その妥当性	システムの運用保守全般を委託しているため、そのシステムが取扱う特定個人情報ファイルについても取扱う必要がある。
③委託先における取扱者数		[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
④委託先への特定個人情報ファイルの提供方法		[ ]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 （ 運用管理、障害対応作業における母子保健システム端末機からの閲覧行為及び必要に応じた修正行為 ）
⑤委託先名の確認方法		福岡市情報公開条例に基づく情報公開請求による確認方法がある。
⑥委託先名		富士通株式会社　九州支社
再委託	⑦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
	⑧再委託の許諾方法	一部再委託承認申請において、その範囲、要件について明記させ、再委託の理由に妥当性があり、再委託の範囲が業務の全部又は主たる部分に当たらないこと及び守秘義務や個人情報保護に係る措置について審査のうえ、承諾している。
	⑨再委託事項	運用保守業務について、レベルアップ又は修正プログラムの提供、現地運用保守業務のサポート及びQ&A、定期点検等の一部業務を委託

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 （ 2 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	都道府県知事または市町村長
①法令上の根拠	番号法 別表第二 16の2
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あって主務省令で定めるもの（乳児の月齢に応じた適切な予防接種の実施勧奨等）
③提供する情報	予防接種履歴
④提供する情報の対象となる本人の数	[1万人未満] ＜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	定期予防接種の接種履歴がある他市町村への転出者
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	他市町村へ転出し，他市町村から照会を受ける都度
提供先2	福岡県知事
①法令上の根拠	番号法 別表第一 10，予防接種法第15条
②提供先における用途	健康被害救済給付認定申請書類の受付及び厚生労働省への進達
③提供する情報	健康被害救済給付認定申請書類
④提供する情報の対象となる本人の数	[1万人未満] ＜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	健康被害救済給付認定申請者
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	市民より健康被害救済給付認定申請を受け付け，福岡県知事へ進達の都度

6. 特定個人情報の保管・消去		
①保管場所 ※		＜母子保健システムにおける措置＞ ①母子保健システムのサーバはあいれふマシン室に設置しており、マシン室への入室を厳重に管理する。 ②特定個人情報は，当該サーバのデータベース内に保存されている。 ③サーバへのアクセスは，ユーザアカウントおよびパスワードによる認証が必要である。 ＜統合宛名システムにおける措置＞ ①統合宛名システムのサーバは本庁マシン室に設置しており、マシン室への入室を厳重に管理する。 ②特定個人情報は，当該サーバのデータベース内に保存されている。 ③サーバへのアクセスは，ユーザアカウントおよびパスワードによる認証が必要である。 ＜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・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厳重に管理する。 ②特定個人情報は、サーバー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。 ＜住民基本台帳ネットワークシステムにおける措置＞ ①住民基本台帳ネットワークシステム端末でデータ保管はできない。 ②住民基本台帳ネットワークシステムの利用は，福岡市の住民基本台帳登録外の者に係る本人確認情報を入手する目的に限定している。
②保管期間	期間	［　　20年以上　　］ ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	定期予防接種は，ワクチンに応じ，接種回数及び接種間隔が定まっており，かつ接種対象年齢が幅広いため，市民からの接種歴確認の問い合わせに対応する必要があることから。
③消去方法		＜母子保健システムにおける措置＞ ①定期予防接種は，ワクチンに応じ，接種回数及び接種間隔が定まっており，かつ接種対象年齢が幅広いため，市民からの接種歴確認の問い合わせに対応する必要があることから，接種歴は消去しない。 ＜統合宛名システムにおける措置＞ ①統合宛名システムに格納する特定個人情報は，各業務システムの副本データであるため，消去のタイミングは各業務システムの運用に準ずる。 ②ディスク交換やハード更改等の際は、統合宛名システムの保守・運用を行う事業者において、保存された情報が読み出しできできないよう、物理的破壊もしくは、専用ソフトを利用して完全に消去する。 ＜中間サーバ・プラットフォームにおける措置＞ 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ため、通常、中間サーバ・プラットフォームの保守・運用を行う事業者が特定個人情報を消去することはない。 ②ディスク交換やハード更改等の際は、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、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。
7. 備考		
―		

（別添2）特定個人情報ファイル記録項目

【予防接種情報】

健管番号,接種コード,接種日,接種機関コード,接種医コード,年度,性別,生年月日,受診時年齢数値(999.11),受診時年齢文字(999歳11ヶ月),集計用月齢(9999),支所コード,地区コード,小学校コード,集計用地区コード1,集計用地区コード2,集計用地区コード3,集計計上日,集計計上年度,請求日,自己負担区分(支払用),支払済フラグ,支払日,新規レコード作成者,新規レコード作成日時,新規レコード端末,新規レコードプログラム,最終レコード更新者,最終レコード更新日時,最終レコード端末,最終レコードプログラム,地域保健・受診区分,計上区分,接種区分,接種量,製造メーカー,ロット番号,徴収区分,行政措置,備考,接種日,不明区分,ハイリスク区分,三種混合区分,ツ反BCG区分,OCR登録時連番,市外フラグ,初診フラグ,同時接種フラグ,同時接種処理フラグ,支払区分,統計区分,定期接種区分,データフラグ,ナンバリングの番号,予防接種の種類,被接種者の住所,被接種者の氏名,被接種者の性別,被接種者の生年月日,予防接種の実施場所,接種年月日,予防接種名,医療機関名,個人番号,予防接種番号,カナ氏名,漢字氏名,性別,郵便番号,住所,生年月日,年齢管轄,接種年月日,医師名,摘要,保護者名,母子共通用管理部,署母子共通用部課

【マイナンバー管理情報】

健管番号,マイナンバー,統合宛名番号,マイナンバー/移動日,マイナンバー/移動事由,マイナンバー/処理日,マイナンバー/処理時間,マイナンバー/連番,新規レコード作成者,新規レコード作成日時,新規レコード端末,新規レコードプログラム,最終レコード更新者,最終更新レコード更新日時,最終レコード端末,最終レコードプログラム

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	
予防接種情報ファイル	
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母子保健システムは住基情報のみを取り込んでおり，実施医療機関から提出された接種票及び予診票をシステムへ取込む際に、それらに記載された健管番号、氏名、住所、生年月日等と住基情報のみとのマッチングを行い、適切な情報のみをシステムへ取込む。 ②予防接種健康被害救済給付申請において、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の防止に努める。 ③他市町村等から情報を入手する際は、対象者以外の情報を入手しないよう、事務マニュアル等を整備し、処理を統一化する。 ④住民基本台帳ネットワークシステムから情報を入手する際は，氏名，性別，生年月日の組合せにより本人確認情報の検索を行い，対象者以外の情報の入手を防止する。
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対象者が多数表示される一覧系の画面および帳票には個人番号は表示しない仕組みとし、不用意な閲覧が行われないようにする。 ②システムのアクセス制限により操作対象者及び権限を制限し、不必要な情報へのアクセス制限により不正なアクセスを防止する。 ③住民基本台帳システムより情報を入手する場合は、情報資産利用申請により利用する情報資産の内容、目的、用途等について、情報資産所管課の承認を得る必要がある。また，情報システム課に報告することになっており、必要な情報以外の情報の入手はできない。 ④他市町村等から情報を入手する際は、必要以外の情報を入手しないよう、事務マニュアル等を整備し、処理を統一化する。 ⑤住民基本台帳ネットワークシステムの利用は，福岡市の住民基本台帳登録外の者に係る本人確認情報を入手する目的に限定している。
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2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	①書面にて本人あるいは代理人による届出のみを受領することとし、受領の際は必ず本人あるいは代理人の本人確認及び委任状の確認を徹底する。 ②住民基本台帳システムより情報を入手する場合は、情報資産利用申請により利用する情報資産の内容、目的、用途等について、情報資産所管課の承認を得る必要がある。また，情報システム課に報告することになっている。 ③システムのアクセス制限により操作対象者及び権限を制限し、不必要な情報へのアクセスを制限により不正なアクセスを防止する。 ④住民基本台帳ネットワークシステムより入手する場合は，入手元である地方公共団体情報システム機構が使用目的を認識できるために，検索を行う際に，本人確認情報の提供に係る根拠（住民基本台帳法第30条の10第1項及び同法第30条の12第1項）に対応した「事務区分」を指定している。
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3： 入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	①本人及び代理人からの申請において，個人番号カード等本人確認書類による本人確認を行う。 ②住民基本台帳システムからの入手について，母子保健システムは外部接続できない仕組みとなっている。 ③住民基本台帳登録外の者の特定個人情報を入手する際は，住民基本台帳ネットワークシステムを用いて，氏名，性別，生年月日の組合せにより検索を行い，完全一致した場合のみ本人確認情報を取得する。
個人番号の真正性確認の措置の内容	本人及び代理人からの申請について，個人番号カード等の提示を受け、真正性確認を行う。 また，住民基本台帳ネットワークシステムにより特定個人情報を入手する際，氏名，性別，生年月日の組合せにより本人確認情報の検索を行い，対象者以外の情報の入手を防止する。
特定個人情報の正確性確保の措置の内容	①書面で提出された特定個人情報をシステムへ入力（新規入力，削除及び訂正）する際は、整合性確保のため、入力作業者以外の者による二重チェックを実施する。 ②入力、削除及び訂正作業に用いた帳票等は、厳重に保管する。 ③住民基本台帳ネットワークシステムにより入手した特定個人情報を母子保健システムへ入力する際は，整合性確保のために，入力を行った者以外の担当者による二重チェックを実施する。
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既存の母子保健システムは外部接続できない仕組みである。 ②提出された健康被害給付救済認定申請書については，鍵付きの保管庫へ保管している。 ③住民基本台帳ネットワークシステム端末では，USBメモリの使用及び照会結果確認票の印刷を制限している。また，システムは専用回線を利用して構築されており，ネットワーク上を流れるすべての通信データの暗号化が実施されている。	
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		
―		

3. 特定個人情報の使用		
リスク1： 目的を超えた紐付け、事務に必要のない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	統合宛名システムを利用するには，各ユーザに個別付与したユーザアカウントおよびパスワードによる認証が必要であり，権限を保持しない者は接続できないようになっている。 権限は，番号法に定められた利用事務の所管課の業務担当職員のみに付与され，また，情報を利用する事務と事務に必要な情報項目の対応付けをあらかじめ統合宛名システム上で設定することで、事務に必要のない情報 への接続もできないよう制限している。	
事務で使用するその他のシステムにおける措置の内容	ユーザアカウントに応じてアクセス権限を設定しており、担当業務に必要な情報へのみアクセス可としている。	
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	①システムを利用する必要がある職員を特定し、ユーザIDによる識別とパスワードによる認証を実施する。また、認証後は利用機能の認可機能により、そのユーザがシステム上で利用可能な機能を制限することで不正利用が行えない対策を実施している。 ②認証に使用するパスワードは、定期的に変更する運用を行っている。	
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	①業務に対応したアクセス権限を確認し、業務に必要なアクセス権限のみを申請しなければならないものとしている。 ②権限を有していた職員の異動退職情報を確認し、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・削除を行っている。	
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	ユーザー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・パスワードは削除している。	
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	ユーザーIDごとにシステムへのアクセスログを記録する。	
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	①システムに登録された事務分担に応じてシステム利用が制限されており、不必要な情報にはアクセスできない措置を講じている。 ②職員に対しては，情報セキュリティ研修を行っている。 ③委託先に対しては，業務外で使用しないことや，違反行為を行うと福岡市個人情報保護条例に規定する罰則が適用される場合があることを契約書等に定めている。	
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	①特定個人情報ファイルの複製は必要最低限とし，実施を特定の環境のみに制限する。また，職員に対しては，情報セキュリティ研修を行うとともに，目的外のファイル複製を行わないよう指導する。 ②委託先に対して，契約書等において許可を得ない複製を禁止し，個人情報保護及び情報セキュリティの体制整備を求め，秘密の保持について教育・訓練を義務付けている。また，必要に応じ監査等の実施や事故発生時の情報公開が可能なこと並びに罰則の適用があることを定めている。	
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		
①端末は、ディスプレイが来庁者から見えない位置に設置している。 ②端末操作時、離席する際は必ずログアウトする。 ③特定個人情報が記載された紙媒体について、離席時には引出しに入れる等の覗き見を防止している。		

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		作業者は個人情報及び情報資産の取扱いについて、「業務委託における個人情報及び情報資産の取扱いに係る措置の基準」を遵守することを契約書に明示し、かつ契約締結時に業務遂行責任者及び作業従事者一覧を提出させ確認している。
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	所属部署・職種・職位に基づき操作権限を与え、特定個人情報ファイルの閲覧者・更新者の制限を行う。
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	操作ログに操作者・操作業務・操作時間等の取り扱い記録を管理している。
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	「福岡市個人情報保護条例」並びに「福岡市情報セキュリティに関する規則」及び「情報セキュリティ共通実施手順」の規定に基づく「業務委託における個人情報及び情報資産の取扱いに係る措置の基準」において，委託業務以外の目的のための委託業務に係る個人情報及び情報資産の第三者へ提供の制限に関する事項を契約書等へ明記し，遵守させる旨定めている。 受託者における委託業務に係る個人情報及び情報資産の取扱いの状況について，契約内容の遵守を確認するため，定期的に報告を求める。また，必要に応じて監査又は検査をする。
	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	「福岡市個人情報保護条例」並びに「福岡市情報セキュリティに関する規則」及び「情報セキュリティ共通実施手順」の規定に基づく「業務委託における個人情報及び情報資産の取扱いに係る措置の基準」において，外部委託に際し，契約明記事項やこれらが遵守されているか等に係る情報セキュリティ管理者との事前協議等の手続きを定めている。 受託者における委託業務に係る個人情報及び情報資産の取扱いの状況について，契約内容の遵守を確認するため，定期的に報告を求める。また，必要に応じて監査又は検査をする。
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	「福岡市個人情報保護条例」並びに「福岡市情報セキュリティに関する規則」及び「情報セキュリティ共通実施手順」の規定に基づく「業務委託における個人情報及び情報資産の取扱いに係る措置の基準」において，委託業務終了時の個人情報及び情報資産の返還，廃棄等に関する事項を契約書等へ明記し，遵守させる旨定めている。 受託者における委託業務に係る個人情報及び情報資産の取扱いの状況について，契約内容の遵守を確認するため，定期的に報告を求める。また，必要に応じて監査又は検査をする。
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	「福岡市個人情報保護条例」並びに「福岡市情報セキュリティに関する規則」及び「情報セキュリティ共通実施手順」の規定に基づく「業務委託における個人情報及び情報資産の取扱いに係る措置の基準」において，受託者は，この契約に基づき委託された業務を実施するに当たっては，個人情報及び情報資産の取扱いについて，「個人情報・情報資産取扱特記事項」を遵守しなければならないとしている。 ＜個人情報・情報資産取扱特記事項＞ ・秘密保持に関すること ・従業者の監督等に関すること ・作業場所の制限に関する事項 ・収集に関する制限に関する事項 ・使用及び提供に関する制限に関する事項 ・安全確保の措置に関する事項 ・複写，複製又は加工の制限に関する事項 ・再委託の制限に関する事項 ・委託業務終了時の返還、廃棄等に関する事項 ・報告及び監査・検査の実施に関する事項 ・事故等発生時の報告に関する事項 ・事故等発生時の公表に関する事項 ・契約の解除に関する事項

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	「業務委託における個人情報及び情報資産の取扱いに係る措置の基準」により，委託元の承認により第三者に委託する場合は，再委託先に対して，再委託業務において取り扱う個人情報が実施機関の委託にかかるものであること，条例で受託者及び受託業務の従事者と同様の責務規定及び罰則が設けられていることを周知させる旨定めている。
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	[　　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	健康被害救済給付認定申請書類の写し	
特定個人情報の提供・移転に関するルール	[　　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	特定個人情報の提供については，番号法関係法令で定められた提供先・事項についてのみ行う。 「福岡市個人情報保護事務取扱要綱」や「情報セキュリティ共通実施手順」にて，本市の機関以外に個人情報及び情報資産を提供する場合それぞれで，それらの取扱いにかかる利用・承認，あるいは合意の手続を定めている。 ルールの遵守状況については，定期的な自己点検にて確認することとしている。	
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	「情報セキュリティ共通実施手順」に従い以下のとおり実施している。 本市の機関以外への特定個人情報の提供については，番号法関係法令で定められた提出先に定められた事項についてのみ実施する。	
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
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	「情報セキュリティ共通実施手順」に従い以下のとおり実施している。 福岡県知事へ進達する健康被害救済給付申請書類は，複数人で宛先，内容を十分に確認し提出している。	
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	＜母子保健システムにおける措置＞ ①母子保健システムは、統合宛名システムを通して情報提供ネットワークと接続しており，情報提供ネットワークとは直接接続しないこととしている。 ＜統合宛名システムにおける措置＞ ①各業務システムから中間サーバあての情報照会要求の中継においては、照会元・照会先・照会内容等の改変は行わないことで，中間サーバにおける目的外入手抑止の措置に従うことを担保している。 ②接続システムの認証及び統合宛名システム接続端末での職員認証等の機能を設けており、あらかじめ承認されたシステム・職員以外の情報入手を抑止している。 ③番号法に定められている事務以外での情報照会ができないようアクセス制限を設けている。 ＜中間サーバ・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： 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	＜母子保健システムにおける措置＞ ①母子保健システムは、統合宛名システムを通して情報提供ネットワークと接続しており，情報提供ネットワークとは直接接続しないこととしている。 ＜統合宛名システムにおける措置＞ ①中間サーバと統合宛名システム間の接続は、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）が利用され、また、VPN等の技術も利用されている。このように，福岡市の統合宛名システムと中間サーバとの間の通信回線を他団体の通信と分離するとともに、通信を暗号化することで安全性を確保している。 ②統合宛名システムは，外部インターネットと接続されている情報系ネットワークとは分離されている，業務系ネットワークに設置することで，通信の安全性を確保している。 ＜中間サーバ・ソフトウェアにおける措置＞ 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設計されるため、安全性が担保されている。 ＜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（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。
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： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	＜母子保健システムにおける措置＞ ①母子保健システムは、統合宛名システムを通して情報提供ネットワークと接続しており，情報提供ネットワークとは直接接続しないこととしている。 ＜統合宛名システムにおける措置＞ ①統合宛名システムは、照会対象者に付番された正しい個人番号に基づき、団体内統合宛名番号を付番してインタフェースシステムより処理通番等を入手した上で、情報提供用個人識別符号の取得依頼ができるよう設計される。これにより，照会対象者の個人番号に基づき正確に情報提供用個人識別符号の紐付けが行われることから、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。 ②統合宛名システム上の宛名情報・業務情報は副本であり，また，中間サーバから各業務システムあての情報照会結果の中継においては、照会結果内容の改変は行わない。これにより，各業務システムが入手する照会結果内容が中間サーバから入手した内容と同一であることを担保している。 ＜中間サーバ・ソフトウェアにおける措置＞ 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。
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母子保健システムは、統合宛名システムを通して情報提供ネットワークと接続しており，情報提供ネットワークとは直接接続しないこととしている。 ＜統合宛名システムにおける措置＞ ①接続システムの認証及び統合宛名システム接続端末での職員認証等の機能を設けており、あらかじめ承認されたシステム・職員以外の情報入手を防止している。 ②番号法に定められている事務以外での情報照会ができないようアクセス制限を設けている。 ③中間サーバと統合宛名システム間の接続は、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）が利用され、また、VPN等の技術も利用されている。このように，福岡市の中間サーバと統合宛名システム間の通信回線を他団体の通信と分離するとともに、通信を暗号化することで安全性を確保している。 ④統合宛名システムは，外部インターネットと接続されている情報系ネットワークとは分離されている、業務系ネットワークに設置することで、通信の安全性を担保している。 ⑤操作内容の追跡調査機能が設けられており、不適切な端末操作や情報照会などを抑止する仕組みになっている。 ＜中間サーバ・ソフトウェアにおける措置＞ 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（※）。 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。 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。 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。 （※）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。 ＜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（総合行政ネットワーク等）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。 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。 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。
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	＜母子保健システムにおける措置＞ ①母子保健システムは、統合宛名システムを通して情報提供ネットワークと接続しており，情報提供ネットワークとは直接接続しないこととしている。 ＜統合宛名システムにおける措置＞ ①各業務システムから中間サーバあての情報提供要求の中継においては、提供元・提供先・提供内容等の改変は行わないことで、中間サーバでの情報提供機能によるチェックに従うことを担保している。 ②接続システムの認証及び統合宛名システム接続端末での職員認証等の機能を備えてお り、あらかじめ承認されたシステム・職員以外の情報提供を防止している。 ＜中間サーバ・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用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、中間サーバにも格納して情報提供機能により、照会許可用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
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	＜母子保健システムにおける措置＞ ①母子保健システムは、統合宛名システムを通して情報提供ネットワークと接続しており，情報提供ネットワークとは直接接続しないこととしている。 ＜統合宛名システムにおける措置＞ ①統合宛名システムは自機関向けの中間サーバとだけ通信および特定個人情報の提供のみを実施するよう設計することで、不適切な方法で提供されるリスクに対応している。 ②接続システムの認証及び統合宛名システム接続端末での職員認証等の機能を備えてお り、あらかじめ承認されたシステム・職員以外による情報提供を防止している。 ③操作内容の追跡調査機能が設けられており、不適切な端末操作や情報提供などを抑止する仕組みになっている。 ＜中間サーバ・ソフトウェアにおける措置＞ 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。 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。 （※）暗号化・復号機能と、鍵情報及び照会許可用照合リストを管理する機能。 ＜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（総合行政ネットワーク等）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。 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。 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。
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	＜母子保健システムにおける措置＞ ①母子保健システムは、統合宛名システムを通して情報提供ネットワークと接続しており，情報提供ネットワークとは直接接続しないこととしている。 ＜統合宛名システムにおける措置＞ ①統合宛名システムは自機関向けの中間サーバとだけ、通信および特定個人情報の提供のみを実施するよう設計されるため、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。 ②統合宛名システムは、他機関へ提供する情報を副本として、中間サーバへ転送する機能を有するが、転送の際には情報内容の改変を行わないことで、中間サーバの副本内容が業務情報と同一であることを担保している。 ＜中間サーバ・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。 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。 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。 （※）特定個人情報を副本として保存・管理する機能。
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	
＜本市における措置＞ 情報提供ネットワークシステムとの全ての連携（接続）は、中間サーバが行う構成となっており、情報提供ネットワークシステムは，統合宛名システムや業務システムは直接接続はできない。 ＜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（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	＜本市における措置＞ ①サーバ室は入室可能な者を限定し、入室時にはパスワードで認証している。サーバ室内及びオペレート室内入口にて常時監視カメラでモニタリングしている。サーバ室の記憶装置は床に固定し、停電時も機器が正常終了できるまでの予備電源を確保している。 ＜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･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。	
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	＜母子保健システムにおける措置＞ ①サーバのネットワークは市の外部とは接続しておらず、隔離された環境である。サーバへのアクセスは限定された者のみ可能であり、アクセスログを保存している。 ＜統合宛名システムにおける措置＞ ①サーバにはウイルス対策ソフトを導入し、ウイルスチェックを実施する。ウイルスパターンファイルは定期的に更新し、最新のものを使用する。 ②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。 ③外部インターネットと接続する情報系ネットワークと分離された業務系ネットワークに設置しており，外部ネットワークからの不正アクセスを防止する。 ④内部者によるデータへの不正アクセスを防止するため、サーバ上のデータ保管フォルダに対してアクセス制限を行う。 ＜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･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。	
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	生存者の個人番号と同様の方法にてサーバで保管している。	
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	①住民登録内の者については住民基本台帳への記載、変更時にシステム間で自動的に連携する。 ②住民登録外の者については、随時本人確認を行い変更があればその都度データを更新する。	
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
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	・保存期間を経過したデータベースに格納された特定個人情報については，定められた手順に従い消去する。 ・磁気ディスクの廃棄時は，手順書等に基づき，内容の消去，破壊等を行うとともに，磁気ディスク管理簿にその記録を残す。 ・紙帳票については，手順書等に基づき，受渡し，保管及び廃棄の運用が適切になされていることを適時確認する。廃棄時には，手順書等に基づき，裁断等を行う。	
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		
①端末、サーバの更新に当たっては、データの完全消去作業を実施している。 ②媒体の廃棄に関しては、データを完全に消去する、初期化を実施する，読み取りができないように物理的に破壊する、いずれかの対応を実施したうえで廃棄している。 ③紙媒体については、鍵付の保管庫などに収納するとともに、廃棄についてはシュレッダー処理を徹底している。		

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	＜本市における措置＞ 年に1回，評価書の定期見直し時に行う自己点検チェックの中で，評価書の記載内容が運用実態と相違がないことも含めて確認している。 ＜中間サーバ･プラットフォームにおける措置＞ ①運用規則等に基づき、中間サーバ･プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。	
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	＜本市における措置＞ ･福岡市情報セキュリティ監査実施要綱に基づき，中期の監査基本方針を「福岡市情報セキュリティ監査中期計画」として策定している。 ･取り扱う情報の重要度に応じ，外部監査，内部監査を定期的に実施している。監査項目については総務省の「地方公共団体における情報セキュリティ監査に関するガイドライン」を参照し実施している。 ＜中間サーバ･プラットフォームにおける措置＞ ･運用規則等に基づき，中間サーバ･プラットフォームについて，定期的に監査を行うこととしている。	

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	＜本市における措置＞ (1)研修について ･全職員を対象とした情報セキュリティ研修を毎年度実施（eラーニング形式）し，個人情報の取扱いを含めた情報セキュリティに関する基礎的な知識の習得及び情報セキュリティに対する意識の向上を図っている。 ･情報セキュリティ及び個人情報の取扱いについて，新規採用職員を対象とした研修，情報セキュリティ責任者及び担当課個人情報保護責任者（課長）を対象とした研修等，それぞれの役割に応じた特別研修を毎年度実施（集合研修形式）している。 ･外部講師（福岡県警のサイバーテロ対策の専門家やJ-LISより派遣される講師等）を招き，情報セキュリティ講習会の開催を行っている。 (2)各種周知について ･情報セキュリティポータルや情報セキュリティニュース，注意喚起等により，情報セキュリティポリシー等各規程の内容や情報セキュリティに関する様々な情報を積極的に周知し，情報セキュリティについての職員の意識向上を図っている。 ･個人情報の適切な取り扱いや情報セキュリティポリシー等に基づき遵守すべき事項について関係課と連携して通知する等，情報セキュリティ及び個人情報の取扱いに関して継続的に周知を行っている。 ＜中間サーバ･プラットフォームにおける措置＞ ･中間サーバ･プラットフォームの運用に携わる職員及び事業者に対し，セキュリティ研修等を実施することとしている。 ･中間サーバ･プラットフォームの業務に就く場合は，運用規則等について研修を行うこととしている。	

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＞ ･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。

Ⅴ　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	〒810－8620 福岡市中央区天神一丁目8番1号 福岡市総務企画局行政部情報公開室 電話 092-711-4129　FAX 092-733-5619
②請求方法	福岡市個人情報保護条例に基づき，「開示・訂正・利用停止請求書」により請求する。
特記事項	福岡市ホームページ上に請求方法，開示請求書等を掲載している。
③手数料等	[　　無料　　]　　＜選択肢＞ 1) 有料　　2) 無料 （手数料額、納付方法：写しの交付による開示の場合は，写しの作成及び送付に係る費用を負担　）
④個人情報ファイル簿の公表	[　　行っている　　]　　＜選択肢＞ 1) 行っている　　2) 行っていない
個人情報ファイル名	予防接種情報ファイル
公表場所	・福岡市ホームページ ・総務企画局行政部情報公開室
⑤法令による特別の手続	―
⑥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	〒810－8620 福岡市中央区天神一丁目8番1号 福岡市保健福祉局健康医療部保健予防課 電話 092-711-4270　FAX 092-733-5535
②対応方法	・問い合わせについては，電話や窓口にて受付を行い，必要に応じて記録を残す。 ・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は，定められたルールに基づき，担当部署への連絡・協議の上，対応する。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	平成27年8月28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	市公報で公告のうえ市ホームページ上で意見公募する旨掲載し，市ホームページ、情報公開室・情報プラザ・各区役所・出張所等において案の閲覧及び配布を行う。意見は郵便，ファクシミリ、電子メールおよび情報公開室や情報プラザ・各区役所・出張所等への持参にて受け付ける。
②実施日・期間	平成28年11月14日（月）から平成28年12月13日（火）まで　（30日間）
③期間を短縮する特段の理由	―
④主な意見の内容	
⑤評価書への反映	
3. 第三者点検	
①実施日	
②方法	
③結果	
4. 特定個人情報保護委員会の承認 【行政機関等のみ】	
①提出日	
②特定個人情報保護委員会による審査	

（別添3）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
平成28年7月1日	Ⅰ　基本情報 7．評価実施期間における担当部署 ②所属長	保健予防課長　田中　雅人	保健予防課長　執行　睦実	事後	重要な変更に当たらない（所属長の変更）
平成28年7月1日	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。） 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 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	発生あり	発生なし	事後	重要な変更に当たらない（発生日（平成25年6月）より3年経過するために記載内容を見直しするもの）
平成28年7月1日	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。） 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 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 その内容	システムのデータ更新のため，区役所へDVDで個人情報データを運搬していた委託業者が，運搬中の交通機関車内にDVDを置き忘れた。	※記載削除	事後	同上
平成28年7月1日	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。） 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 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 再発防止策の内容	DVDで運搬していたデータを，専用線による伝送方式にシステムを改修した。	※記載削除	事後	同上

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
平成28年7月1日	Ⅳ　その他のリスク対策 1．監査 ①自己点検 具体的なチェック方法	＜本市における措置＞ 年に1回、担当部署内において実施している自己点検に用いるチェック項目に、「評価書の記載内容通りの運用がなされていること」に係る内容を追加し、運用状況を確認する。	＜本市における措置＞ 年に1回，評価書の定期見直し時に行う自己点検チェックの中で，評価書の記載内容が運用実態と相違がないことも含めて確認している。	事後	点検方法の記載内容を単に修正しただけであり，重要な変更にはあたらない。
平成28年7月1日	Ⅳ　その他のリスク対策 2．従業員に対する教育・啓発 従業員に対する教育・啓発 具体的な方法	＜本市における措置＞ (1)情報セキュリティ研修について ・全職員を対象として情報セキュリティ研修を毎年度実施（eラーニング形式）し，個人情報の取扱いを含めた情報セキュリティに関する基礎的な知識の習得及び情報セキュリティに対する意識の向上を図っている。 ・新規採用職員を対象とした研修，情報セキュリティ責任者（課長）を対象とした研修，希望者を対象とした研修等，それぞれの役割に応じた特別研修を毎年度実施（集合研修形式）している。 ・外部講師（福岡県警のサイバーテロ対策の専門家やJ-LISより派遣される講師等）を招き，情報セキュリティ講習会の開催を行っている。 (2)情報セキュリティに係る各種周知について ・情報セキュリティポータルや情報セキュリティニュース，注意喚起等により，情報セキュリティポリシー等各規程の内容や情報セキュリティに関する様々な情報を積極的に周知し，職員の意識向上を図っている。 ・個人情報の適切な取り扱いや情報セキュリティポリシー等に基づき遵守すべき事項について情報公開室等と連携して通知する等，情報セキュリティに関して継続的に周知を行っている。	＜本市における措置＞ (1)研修について ・全職員を対象とした情報セキュリティ研修を毎年度実施（eラーニング形式）し，個人情報の取扱いを含めた情報セキュリティに関する基礎的な知識の習得及び情報セキュリティに対する意識の向上を図っている。 ・情報セキュリティ及び個人情報の取扱いについて，新規採用職員を対象とした研修，情報セキュリティ責任者及び担当課個人情報保護責任者（課長）を対象とした研修等，それぞれの役割に応じた特別研修を毎年度実施（集合研修形式）している。 ・外部講師（福岡県警のサイバーテロ対策の専門家やJ-LISより派遣される講師等）を招き，情報セキュリティ講習会の開催を行っている。 (2)各種周知について ・情報セキュリティポータルや情報セキュリティニュース，注意喚起等により，情報セキュリティポリシー等各規程の内容や情報セキュリティに関する様々な情報を積極的に周知し，情報セキュリティについての職員の意識向上を図っている。 ・個人情報の適切な取り扱いや情報セキュリティポリシー等に基づき遵守すべき事項について関係課と連携して通知する等，情報セキュリティ及び個人情報の取扱いに関して継続的に周知を行っている。	事後	情報セキュリティだけでなく，個人情報の取扱いに関する内容を追記したものであり，重要な変更にはあたらない。
平成28年8月8日	Ⅰ　基本情報 5．個人番号の利用 法令上の根拠	行政手続き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（番号法）第9条第1項　別表第1の10の項	・行政手続き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（番号法）第9条第1項　別表第一の10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第10条	事後	重要な変更に当たらない（主務省令の名称及び条項の追記）

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
平成28年8月8日	Ⅰ　基本情報 6. 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2における情報提供の根拠） ・番号法第19条第7号 ・別表第2の16の2及び18の項 （別表第2における情報照会の根拠） ・番号法第19条第7号 ・別表第2の16の2，17，18の項及び19の項	（別表第二における情報提供の根拠） ・番号法第19条第7号　別表第二の16の2及び18の項 （別表第二における情報照会の根拠） ・番号法第19条第7号　別表第二の16の2，17，18の項及び19の項 ・番号法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13条	事後	重要な変更に当たらない（主務省令の名称及び条項の追記）
	（別添1）事務の内容	※記載なし	「住民基本台帳ネットワークシステム」追加	事前	特定個人情報の入手元追加に伴う重要な変更
	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ①入手元	※記載なし	「その他」を選択し，（地方公共団体情報システム機構）を追記	事前	同上
	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ②入手方法	※記載なし	「その他」を選択し，（住民基本台帳ネットワークシステム）を追記	事前	同上
	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ③入手の時期・頻度	（1）住民基本台帳情報 ・入手先：住民基本台帳システム ・入手方法：住民基本台帳システムからのデータ連携（庁内連携により入手） ・入手時期・頻度：①個人番号の付番・通知日（平成27年10月5日）以後に準備行為として一括入手 ②番号利用開始日（平成28年1月1日）以後は日次の頻度 （2）予防接種健康被害救済請求申請の都度，紙で入手。 （3）他市町村からの転入者に対し，他市町村へ照会する都度，情報提供ネットワークシステムを介して入手。	（1）住民基本台帳情報 ・入手先：住民基本台帳システム ・入手方法：住民基本台帳システムからのデータ連携（庁内連携により入手） ・入手時期・頻度：①個人番号の付番・通知日（平成27年10月5日）以後に準備行為として一括入手 ②番号利用開始日（平成28年1月1日）以後は日次の頻度 （2）予防接種健康被害救済請求申請の都度，紙で入手。 （3）他市町村からの転入者に対し，他市町村へ照会する都度，情報提供ネットワークシステムを介して入手。 （4）住民基本台帳登録外の対象者について，本人確認情報の調査が必要となった都度，住民基本台帳ネットワークシステムを介して入手。	事前	同上

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
	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ④入手に係る妥当性	住民基本台帳システムから入手する住民基本情報については、本人等からの申請を受けた都度入手する必要があり、法令等に基づく予防接種対象者であることの確認。 予防接種健康被害救済請求は本人等からの申請によるものである。	住民基本台帳システムから入手する住民基本情報については、本人等からの申請を受けた都度入手する必要があり、法令等に基づく予防接種対象者であることの確認。 予防接種健康被害救済請求は本人等からの申請によるものである。 住民基本台帳登録外の対象者本人確認情報の調査に必要な範囲内で，住民基本台帳ネットワークシステムにより情報収集を適宜行う必要がある。	事前	特定個人情報の入手元追加に伴う重要な変更
	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑤本人への明示	住民基本台帳システムから住民基本情報を入手の場合、番号法及び予防接種法施行規則により明示されている。 本人及び代理人から入手する情報は、書面にて利用目的を明示する。	住民基本台帳システムから住民基本情報を入手の場合、番号法及び予防接種法施行規則により明示されている。 本人及び代理人から入手する情報は、書面にて利用目的を明示する。 住民基本台帳ネットワークシステムによる入手の場合、番号法により、地方公共団体情報システム機構に対し機構保存本人確認情報の提供を求めることができる旨明示されている。	事前	同上
	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑧使用方法	①対象者の資格（住所、年齢）確認 　医療機関からの接種記録について、住民基本台帳システムをもとに対象者であることを確認する。	①対象者の資格（住所、年齢）確認 　医療機関からの接種記録について、住民基本台帳システムをもとに対象者であることを確認する。 　住民基本台帳登録外の対象者について，住民基本台帳ネットワークシステムを用いて，個人番号を取得する。	事前	同上
	Ⅱ　特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ①保管場所	※記載なし	＜住民基本台帳ネットワークシステムにおける措置＞ ①住民基本台帳ネットワークシステム端末でデータ保管はできない。 ②住民基本台帳ネットワークシステムの利用は，福岡市の住民基本台帳登録外の者に係る本人確認情報を入手する目的に限定している。	事前	同上

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
	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 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母子保健システムは住基情報のみを取り込んでおり，実施医療機関から提出された接種票及び予診票をシステムへ取込む際に、それらに記載された健管番号、氏名、住所、生年月日等と住基情報のみとのマッチングを行い、適切な情報のみをシステムへ取込む。 ②予防接種健康被害救済給付申請において、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の防止に努める。 ③他市町村等から情報を入手する際は、対象者以外の情報を入手しないよう、事務マニュアル等を整備し、処理を統一化する。	①母子保健システムは住基情報のみを取り込んでおり，実施医療機関から提出された接種票及び予診票をシステムへ取込む際に、それらに記載された健管番号、氏名、住所、生年月日等と住基情報のみとのマッチングを行い、適切な情報のみをシステムへ取込む。 ②予防接種健康被害救済給付申請において、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の防止に努める。 ③他市町村等から情報を入手する際は、対象者以外の情報を入手しないよう、事務マニュアル等を整備し、処理を統一化する。 ④住民基本台帳ネットワークシステムから情報を入手する際は，氏名，性別，生年月日の組合せにより本人確認情報の検索を行い，対象者以外の情報の入手を防止する。	事前	特定個人情報の入手元追加に伴う重要な変更
	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 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 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対象者が多数表示される一覧系の画面および帳票には個人番号は表示しない仕組みとし、不用意な閲覧が行われないようにする。 ②システムのアクセス制限により操作対象者及び権限を制限し、不必要な情報へのアクセス制限により不正なアクセスを防止する。 ③住民基本台帳システムより情報を入手する場合は、情報資産利用申請により利用する情報資産の内容、目的、用途等について、情報資産所管課の承認を得る必要がある。また，情報システム課に報告することになっており、必要な情報以外の情報の入手はできない。 ④他市町村等から情報を入手する際は、必要以外の情報を入手しないよう、事務マニュアル等を整備し、処理を統一化する。	①対象者が多数表示される一覧系の画面および帳票には個人番号は表示しない仕組みとし、不用意な閲覧が行われないようにする。 ②システムのアクセス制限により操作対象者及び権限を制限し、不必要な情報へのアクセス制限により不正なアクセスを防止する。 ③住民基本台帳システムより情報を入手する場合は、情報資産利用申請により利用する情報資産の内容、目的、用途等について、情報資産所管課の承認を得る必要がある。また，情報システム課に報告することになっており、必要な情報以外の情報の入手はできない。 ④他市町村等から情報を入手する際は、必要以外の情報を入手しないよう、事務マニュアル等を整備し、処理を統一化する。 ⑤住民基本台帳ネットワークシステムの利用は，福岡市の住民基本台帳登録外の者に係る本人確認情報を入手する目的に限定している。	事前	同上

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
	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 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2：不適切な方法で入手が行われるリスク リスクに対する措置の内容	①書面にて本人あるいは代理人による届出のみを受領することとし、受領の際は必ず本人あるいは代理人の本人確認及び委任状の確認を徹底する。 ②住民基本台帳システムより情報を入手する場合は、情報資産利用申請により利用する情報資産の内容、目的、用途等について、情報資産所管課の承認を得る必要がある。また，情報システム課に報告することになっている。 ③システムのアクセス制限により操作対象者及び権限を制限し、不必要な情報へのアクセスを制限により不正なアクセスを防止する。	①書面にて本人あるいは代理人による届出のみを受領することとし、受領の際は必ず本人あるいは代理人の本人確認及び委任状の確認を徹底する。 ②住民基本台帳システムより情報を入手する場合は、情報資産利用申請により利用する情報資産の内容、目的、用途等について、情報資産所管課の承認を得る必要がある。また，情報システム課に報告することになっている。 ③システムのアクセス制限により操作対象者及び権限を制限し、不必要な情報へのアクセスを制限により不正なアクセスを防止する。 ④住民基本台帳ネットワークシステムより入手する場合は，入手元である地方公共団体情報システム機構が使用目的を認識できるために，検索を行う際に，本人確認情報の提供に係る根拠（住民基本台帳法第30条の10第1項及び同法第30条の12第1項）に対応した「事務区分」を指定している。	事前	特定個人情報の入手元追加に伴う重要な変更
	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 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3：入手した特定個人情報が不正確であるリスク 入手の際の本人確認の措置の内容	①本人及び代理人からの申請において，個人番号カード等本人確認書類による本人確認を行う。 ②住民基本台帳システムからの入手について，母子保健システムは外部接続できない仕組みとなっている。	①本人及び代理人からの申請において，個人番号カード等本人確認書類による本人確認を行う。 ②住民基本台帳システムからの入手について，母子保健システムは外部接続できない仕組みとなっている。 ③住民基本台帳登録外の者の特定個人情報を入手する際は，住民基本台帳ネットワークシステムを用いて，氏名，性別，生年月日の組合せにより検索を行い，完全一致した場合のみ本人確認情報を取得する。	事前	同上
	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 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3：入手した特定個人情報が不正確であるリスク 個人番号の真正性確認の措置の内容	本人及び代理人からの申請について，個人番号カード等の提示を受け、真正性確認を行う。	本人及び代理人からの申請について，個人番号カード等の提示を受け、真正性確認を行う。 また，住民基本台帳ネットワークシステムにより特定個人情報を入手する際，氏名，性別，生年月日の組合せにより本人確認情報の検索を行い，対象者以外の情報の入手を防止する。	事前	同上

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
	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 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3：入手した特定個人情報が不正確であるリスク 特定個人情報の正確性確保の措置の内容	①書面で提出された特定個人情報をシステムへ入力（新規入力，削除及び訂正）する際は、整合性確保のため、入力作業者以外の者による二重チェックを実施する。 ②入力、削除及び訂正作業に用いた帳票等は、厳重に保管する。	①書面で提出された特定個人情報をシステムへ入力（新規入力，削除及び訂正）する際は、整合性確保のため、入力作業者以外の者による二重チェックを実施する。 ②入力、削除及び訂正作業に用いた帳票等は、厳重に保管する。 ③住民基本台帳ネットワークシステムにより入手した特定個人情報を母子保健システムへ入力する際は，整合性確保のために，入力を行った者以外の担当者による二重チェックを実施する。	事前	特定個人情報の入手元追加に伴う重要な変更
	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 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既存の母子保健システムは外部接続できない仕組みである。 ②提出された健康被害給付救済認定申請書については，鍵付きの保管庫へ保管している。	①既存の母子保健システムは外部接続できない仕組みである。 ②提出された健康被害給付救済認定申請書については，鍵付きの保管庫へ保管している。 ③住民基本台帳ネットワークシステム端末では，USBメモリの使用及び照会結果確認票の印刷を制限している。また，システムは専用回線を利用して構築されており，ネットワーク上を流れるすべての通信データの暗号化が実施されている。	事前	同上