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
5	枚方市　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

枚方市は、予防接種に関する事務において特定個人情報ファイルを取り扱うに当たり、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理解し、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、ここに宣言する。

特記事項	

評価実施機関名

枚方市長

公表日

令和8年3月30日

［令和7年5月　様式3］

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	感染のおそれがある疾病の発生及びまん延を予防するために、公衆衛生の見地から、市内に在住する者に対し、予防接種の実施その他必要な措置を講じることにより、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。 【事務の概要】 ①予防接種の対象者への各種通知 ②予防接種法及び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の実施 ③接種費用の徴収 ④予防接種歴の登録、管理 ⑤医療機関に対する予防接種の実施委託料の支払 ⑥健康被害救済対象者への給付 【個人番号利用事務】 個人番号は、予防接種法、新型インフルエンザ等対策特別措置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。）の規定に基づき、次に掲げる事務において利用する。 ①予防接種の実施の周知：住民基本台帳情報から抽出した予防接種の対象者に通知し、予防接種の種類、実施場所、実施期間等を周知する。 ②予防接種歴の管理：健康管理システムに予防接種の実施記録を登録し、予防接種歴を管理する。 ③未接種者に対する接種勧奨：健康管理システムを使用して抽出した未接種者に通知し、予防接種を受けるよう勧奨する。 ④接種費用の免除：接種費用の免除申請者等の個人住民税の課税状況、生活保護等の受給状況を確認し、免除対象者には無料接種券を発行する。
③対象人数	[　10万人以上30万人未満　] ＜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

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. 接種歴管理：予防接種の実施記録を登録し、接種歴を管理する。 2. 個別通知対象者抽出：予防接種の対象者や未接種者を抽出する。 3. 統計：接種歴情報を統計処理し、厚生労働省へ報告する。
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　（　）
システム2～5	
システム2	
①システムの名称	庁内連携システム
②システムの機能	統合データベース管理、連携機能 住民基本台帳情報や、住民税情報等、各業務システムを利用する上で必要な情報を、業務連携用データベース（またはファイル）として保持し、庁内業務システム間の情報連携を行う機能。
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　（ 既存各業務システム　）
システム3	
①システムの名称	団体内統合宛名システム（番号連携サーバ）

②システムの機能	1. 宛名情報管理機能 　統一識別番号が未登録の個人に対して統一識別番号を付番する。宛名情報を統一識別番号、個人番号と紐付けて保存し、管理する。中間サーバー、既存業務システム等の要求に基づき、個人番号や統一識別番号に紐付く宛名情報を通知する。 2. 情報照会機能 　中間サーバーを通して他機関への情報照会要求を行い、照会結果を通知する。 3. 情報提供機能 　他機関へ提供する特定個人情報（連携対象）を中間サーバーへ連携する。 4. 符号要求機能 　情報連携の際に個人の識別子として用いる符号の取得要求を、既存住基システムや住基ゲートウェイに送信する。 5. 権限管理機能 　団体内統合宛名システムを利用する職員の認証、職員に付与された権限に基づいた各種機能の制御、特定個人情報（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、既存業務システム　）
システム4	
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 　情報照会や情報提供の際に個人の識別子として用いる「符号」と、自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 　情報提供ネットワークシステムを介して、他機関に対して情報提供の求めを発出するとともに、他機関から提供された情報を受領する。 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、他機関からの情報提供の求めを受領するとともに、他機関に対して提供する情報を発出する。 4. 既存システム接続機能 　既存業務システム、団体内統合宛名システム、住基システムとの間で、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。 5. 情報提供等記録管理機能 　情報照会や情報提供があった旨の記録（＝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 　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 　情報を暗号化（あるいは復号）する。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 　中間サーバーを利用する職員の認証、職員に付与された権限に基づいた各種機能の制御、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　（　）
システム6～10	
システム11～15	
システム16～20	

3. 特定個人情報ファイル名	
予防接種情報ファイル	
4. 個人番号の利用 ※	
法令上の根拠	・番号法第9条第1項　別表　14の項、126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10条、第67条の2 ・番号法第19条第6号（委託先への提供）
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	【照会】 ・番号法第19条第8号に基づく主務省令第2条の表25の項、27から29の項、153の項 【提供】 ・番号法第19条第8号に基づく主務省令第2条の表25の項、26の項、153の項、154の項
6. 評価実施機関における担当部署	
①部署	枚方市　健康福祉部　保健所　保健予防課
②所属長の役職名	保健予防課長
7. 他の評価実施機関	
無し	

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 ※		枚方市に住民登録している予防接種事業の対象となる者
	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		[　　100項目以上　　] ＜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 [○] 5情報（氏名、氏名の振り仮名、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、4情報、その他住民票関係情報：対象者を正確に特定するため保有 2. 健康・医療関係情報：予防接種歴管理及び接種勧奨のため保有 3. 地方税関係情報、生活保護・社会福祉関係情報：接種費用の免除対象者を適正に認定するため保有
	全ての記録項目	別添1を参照。
⑤保有開始日		平成27年10月5日
⑥事務担当部署		枚方市　健康福祉部　保健所　保健予防課

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　（　　） [　] 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　（　　）
③使用目的 ※		接種歴を登録し、未接種者への接種勧奨を実施。接種歴管理により重複接種を防ぐ。
④使用の主体	使用部署	枚方市　健康福祉部　保健所　保健予防課
	使用者数	[　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
⑤使用方法		1. 予防接種の対象者の確認：医療機関での接種記録について、住民基本台帳システムを基に対象者であることを確認する。 2. 予防接種歴の管理：健康管理システムに医療機関から提出された予診票のデータを登録し、予防接種歴を管理する。 3. 未接種者への接種勧奨：健康管理システムを使用して未接種者を抽出し、個別通知により接種勧奨を行う。 4. 接種費用の免除要件の確認：本人等の申請に基づき、個人住民税の課税情報と生活保護の受給情報により免除要件の有無を確認する。
	情報の突合	1. 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、対象者の確認をする。 2. 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、接種歴を入力、管理する。 3. 住民基本台帳システムと突合し、入力した履歴を基に、未接種者を把握、抽出する。 4. 本人等からの申請の申請に基づき、住民基本台帳システムと市民税情報を突合し、実費徴収の有無を決定する。
⑥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] (1) 件	<選択肢> 1）委託する 2）委託しない
委託事項1		システムの運用・保守	
①委託内容		システムの運用・保守	
②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
③委託先名		アトラス情報サービス(株)	
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		
委託事項2～5			
委託事項6～10			
委託事項11～15			
委託事項16～20			

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	他市町村長
①法令上の根拠	・番号法第19条第8号に基づく主務省令第2条の表25の項、26の項、153の項
②提供先における用途	予防接種法及び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情報であって主務省令で定めるもの
③提供する情報	予防接種事業関係情報であって主務省令で定めるもの
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	枚方市に住民登録している法定接種対象者
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼の都度
提供先2～5	
提供先2	都道府県知事
①法令上の根拠	・番号法第19条第8号に基づく主務省令第2条の表26の項、153の項
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情報であって主務省令で定めるもの
③提供する情報	予防接種事業関係情報であって主務省令で定めるもの
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	枚方市に住民登録している法定接種対象者
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼の都度
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
	＜選択肢＞

④移転する情報の対象となる本人の数	[　　] 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移転する情報の対象となる本人の範囲	
⑥移転方法	[　　] 庁内連携システム　　[　　] 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	
移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	

6. 特定個人情報の保管・消去	
保管場所 ※	庁内の入退室管理（※）が行われている部屋に設置した施錠できる格納庫の内に設置したサーバ内に保管。 （※）管理室内への入室権限を持つ者を限定し、ICカードにより入退室する者を管理する。 ＜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。・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。・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	
なし	

（別添1）特定個人情報ファイル記録項目

予防接種情報：ロタ、B型肝炎、ヒブ、小児用肺炎球菌、4種混合、3種混合、ポリオ、BCG、麻しん風しん混合（MR）、麻しん、風しん、水痘、日本脳炎、2種混合、子宮頸がん予防、高齢者肺炎球菌、新型インフルエンザ
個人特定情報：個人番号、カナ氏名、生年月日、接種日、接種の可否、医療機関名、ロット番号、接種回数、接種量、性別、ワクチンの種類、請求日、費用徴収の有無、生活保護受給状況、市民税非課税状況

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：　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	・窓口においては、本人確認書類の提示を求める等、省令に定める本人確認措置を厳格に実施することにより、対象者等以外の者から特定個人情報を入手することを防止する。 ・取り決めた書式をもって申請等を受理することにより、予防接種費用の免除申請等の審査事務を処理する上で、必要のない情報の入手を防止する。 ・健康管理システムに情報を入力したときは、当該入力を行った職員以外の職員が入力内容と入力原票の照合を行うことにより、対象者以外の者の情報や、事務を処理する上で必要のない情報が入力されることを防止する。
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	
・窓口に衝立を設置することにより、応対に係る書類等の内容が、他の職員や来庁者の目に触れることを防止する。 ・健康管理システムに情報を入力したときは、当該入力を行った職員以外の職員が入力内容と入力原票の照合を行うことにより、不正確な情報が入力されることを防止する。 ・提出を受けた後、システム入力等の処理を終えた申請書等の書類については、施錠可能な所定の保管場所にただちに保管することにより、情報の漏えい、紛失を防止する。 ・システムにパスワード等による認証機能を設定することにより、権限のない職員による情報の取扱いを防止する。 ・システムログを取得する等して情報の取扱状況を記録していることを職員に周知することにより、権限のない職員による情報の取扱いを抑止する。	
3. 特定個人情報の使用	
リスク1：　目的を超えた紐付け、事務に必要のない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	庁内連携システムや健康管理システムにアクセス制御機能を付加することにより、これらの間で、予防接種費用の免除申請等の審査事務を処理するために必要な情報であって、番号法や番号法条例に定めるもの以外の情報について連携を行うことを防止する。
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	端末にアクセスするためのカード認証とシステムにアクセスするためのID･パスワードによる認証を行っており、業務上必要最低限に限定した特定の職員のみが照会できるようにしている。
その他の措置の内容	・システムを操作したログ（日時・利用者・操作内容等）を取得し、必要に応じて操作履歴を解析する。 ・サーバが設置されている管理区域に委託業者によるスマートフォンなどの持ち込みは禁止しており、また、外部記憶媒体についても許可制としている。 ・人事異動や退職、担当替えに伴うアクセス権限の発行、更新、失効を確実かつ適正に行う。
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
端末のディスプレイを、来庁者から見えない位置に置く。 ・業務運用中にやむを得ず離席する場合はシステムよりログオフする。 ・本人確認情報が表示された画面のハードコピーの取得は事務処理に必要となる範囲にとどめ、使用後のシュレッダーを徹底する。 ・職員を対象に個人情報保護及び情報セキュリティに関する注意喚起を行い、業務外利用の禁止等に徹底する。

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	委託先に対して、以下の事項を義務付ける特記仕様書を提示する。 ・番号法等の関係法令の遵守・秘密の保持・取扱区域外への情報持ち出しの禁止・目的外利用の禁止・複製の禁止・情報の返却、消去、廃棄・従業員の特定・従業員への監督及び教育・市の検査、報告の求めへの応諾・漏えい等事案に係る損害の賠償・再委託の条件・再委託先に対する監督とその履行状況の報告・その他枚方市保有個人情報安全管理規程に基づき職員が実施する措置に準じた措置の実施・特記仕様書に違反する行為の契約解除事由への該当	
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	[　　再委託していない　　]	＜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		
その他の措置の内容	再委託の契約の内容を書面により提出させ、当該再委託の契約の内容が、委託契約により委託先に課された全ての義務を再委託先に課すものである場合に限り、再委託の許諾を行う。	
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		
・サーバー室で受託業者が作業する場合は、職員が立ち会う。 ・委託先従業員が職員の許可を得ずに外部記憶媒体をサーバー室に持ち込む事を禁止するとともに、スマートフォン等については一切の持込を禁止する。 ・リモート保守を行う事業者の事業所については、情報セキュリティマネジメントシステム等の情報セキュリティの第三者認証を取得していることを条件とし、セキュリティ対策の実効性を確保する。第三者認証を取得していない場合等で必要と判断する場合、職員が実地確認を行い、セキュリティ対策の実効性を確保する。 ＜リモート保守環境におけるその他のリスクと措置＞ ・リモート保守を行う事業所の執務エリアは入退室管理された区画とし、作業者の入退室記録を取得する。また保守作業に利用する端末の利用記録の取得や、監視カメラでの監視体制を敷き、作業者へも周知することで、不適切な方法での情報入手を抑止する。 ・リモート保守環境とガバメントクラウドへの接続については、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し、通信経路上での第三者からの情報窃取を行えないよう対策する。 ・リモート保守で利用する端末等については、コンピュータウィルス対策ソフトウェアを導入しており、パターンファイルも最新版が適用されるよう管理する。また、OSには必要に応じてパッチ適用を実施する。端末内へのデータ保存を行わないシンクライアント端末を利用し、コンピュータウィルス対策ソフトウェアを導入できない場合については、シンクライアント端末からの接続先となる作業環境に対して同様の対策を実施する。 ・システムのリモート保守で委託事業者が利用する端末等へは、原則として、特定個人情報の保存を行えないように措置する。端末等への特定個人情報の保存を必要とする場合、使用後は速やかに消去するとともに、端末等のディスク廃棄時には物理的破壊または専用ソフトでのデータ消去を行わせ、データ消去証明書の提出により確認する。		

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
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	<健康管理システムにおける措置> ・番号法の規定に基づき、認められる範囲内において特定個人情報の照会を行う。また、理解度を高めるため、規定内容の周知を行い、業務以外に利用することを禁止する。 <中間サーバー・ソフトウエアにおける措置> 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）番号法第19条第7号及び第8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限を行う機能。	
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	<中間サーバー・ソフトウエアにおける措置> ・中間サーバーは、個人情報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ているため、安全性が担保されている。 <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を利用することにより、安全性を確保している。 <中間サーバー運用における措置> ・情報提供ネットワークシステムを利用する場合は、どの職員がどの特定個人情報をいつ何のために利用したかがすべて記録される。番号法上認められる提供意外は受けつけないようにしており、システム上提供外認められなかった場合においても記録を残し、提供記録は7年分保管する。	
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
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・ソフトウエアにおける措置> ・中間サーバーは、個人情報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ているため、安全性が担保されている。 <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を利用することにより、安全性を確保している。 <中間サーバー運用における措置> ・情報提供ネットワークシステムを利用する場合は、どの職員がどの特定個人情報をいつ何のために利用したかがすべて記録される。番号法上認められる提供意外は受けつけないようにしており、システム上提供外認められなかった場合においても記録を残し、提供記録は7年分保管する。		
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
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	<枚方市における措置> ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォール、不正侵入防止装置（IPS）を設置している。 ・インターネットとつながらないように、ネットワークをファイアウォールで切断している。 ・コンピューターウイルス対策ソフトウエアを導入しており、パターンファイルも最新版が適用されるよう管理している。 ・DSには必要に応じてパッチ運用を実施している。 〈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・プラットフォームでは、UTM（コンピューター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）等を購入し、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購入し、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＞ 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。 ③国及びクラウド事業者は、市の保有データにアクセスしない契約等となっている。 ④市が委託した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。 ⑤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。 ⑥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。 ⑦市が委託した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。 ⑧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。 ⑨市や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。 ⑩市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	
＜保管場所＞ ・サーバの盗難を防ぐために、施錠ができる場所等に保管し、施錠をしている。また、設置場所への入退室はICカードにより記録している。 ・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。 ・火災によるデータ消失を防ぐために、施設内に消火設備を完備している。 ＜消去について＞ ・システムに保存されている個人番号については、保存年限到達後にバッチ処理で消去する。 ・申請書等の書類は、保存年限の経過後、溶解して廃棄する。 ＜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　　] ＜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	＜枚方市における措置＞ ・職員に対しては、情報セキュリティと個人情報保護に関する研修を行う。 ・委託業者に対しては、特記仕様書を提示し、個人情報保護に関する教育を適宜実施することを義務づける。 ＜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。 ②中間サーバー・プラットフォームの業務につく場合は、運用規則等について研修を行うこととしている。

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、国及びクラウド事業者が対応する。また、ガバメントクラウドに起因しない事象の場合は、市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。

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573-8666 大阪府枚方市大垣内町二丁目１番20号 枚方市役所　総務部　コンプライアンス推進課
②請求方法	個人情報の保護に関する法律に基づき、保有個人情報の開示等請求を受け付ける。
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573-1197 大阪府枚方市禁野本町二丁目１３番１３号 枚方市役所　健康福祉部　保健所　保健予防課
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。

Ⅴ　評価実施手続

1. 基礎項目評価	
①実施日	平成29年7月13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8年3月30日	Ⅰ　基本情報 4.個人番号の利用※　法令上の根拠	・番号法別表第1の10、93の2の項 ・同法第9条第2項及び同項の規定による枚方市個人番号の利用及び特定個人情報の提供に関する条例第3条第1項に規定する法別表第2の16の2、17、18、19、115の2の項	・番号法第9条第1項　別表　14の項、126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10条、第67条の2 ・番号法第19条第6号（委託先への提供）	事後	重要な変更に当たらないため。
令和8年3月30日	Ⅰ　基本情報 5.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	【照会】 ・番号法別表第2の16の2、17、18、19、115の2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12条の2、12条の3、13条、13条の2、59条の2） 【提供】 ・同表の16の2、16の3、115の2の項（同命令第12条の2、第12条の2の2、59条の2）	【照会】 ・番号法第19条第8号に基づく主務省令第2条の表25の項、27から29の項、153の項 【提供】 ・番号法第19条第8号に基づく主務省令第2条の表25の項、26の項、153の項、154の項	事後	重要な変更に当たらないため。
令和8年3月30日	Ⅰ　基本情報 6.評価実施機関における担当部署	枚方市　健康福祉部　地域健康福祉室（母子保健担当） 地域健康福祉室（母子保健担当）課長	枚方市　健康福祉部　保健所　保健予防課 保健予防課長	事後	重要な変更に当たらないため。
令和8年3月30日	Ⅱ　特定個人情報ファイルの概要 2. 基本情報 ⑥事務担当部署	枚方市　健康福祉部　地域健康福祉室（母子保健担当）	枚方市　健康福祉部　保健所　保健予防課	事後	重要な変更に当たらないため。
令和8年3月30日	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 ⑥事務担当部署	枚方市　健康福祉部　地域健康福祉室（母子保健担当）	枚方市　健康福祉部　保健所　保健予防課	事後	重要な変更に当たらないため。
令和8年3月30日	Ⅱ　特定個人情報ファイルの概要5.特定個人情報の提供・移転（委託に伴うものを除く。）　提供先1　①法令上の根拠	番号法別表第2の16の2、115の2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12条の2、59条の2）	・番号法第19条第8号に基づく主務省令第2条の表25の項、26の項、153の項	事後	重要な変更に当たらないため。

令和8年3月30日	Ⅱ　特定個人情報ファイルの概要5.特定個人情報の提供・移転（委託に伴うものを除く。） 提供先2　①法令上の根拠	番号法別表第2の16の3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12条の2の2）	・番号法第19条第8号に基づく主務省令第2条の表26の項、153の項	事後	重要な変更に当たらないため。
令和8年3月30日	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 保管場所	庁内の入退室管理（※）が行われている部屋に設置した施錠できる格納庫の内に設置したサーバ内に保管。 （※）管理室内への入室権限を持つ者を限定し、ICカードにより入退室する者を管理する。	庁内の入退室管理（※）が行われている部屋に設置した施錠できる格納庫の内に設置したサーバ内に保管。 （※）管理室内への入室権限を持つ者を限定し、ICカードにより入退室する者を管理する。 ＜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。・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。・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。	事後	重要な変更に当たらないため。

令和8年3月30日	Ⅲリスク対策 4．特定個人情報ファイルの取扱いの委託 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	・サーバー室で受託業者が作業する場合は、職員が立ち会う。 ・委託先従業員が職員の許可を得ずに外部記憶媒体をサーバー室に持ち込む事を禁止するとともに、スマートフォン等についてはー切の持込を禁止する。	・サーバー室で受託業者が作業する場合は、職員が立ち会う。 ・委託先従業員が職員の許可を得ずに外部記憶媒体をサーバー室に持ち込む事を禁止するとともに、スマートフォン等についてはー切の持込を禁止する。 ・リモート保守を行う事業者の事業所については、情報セキュリティマネジメントシステム等の情報セキュリティの第三者認証を取得している ことを条件とし、セキュリティ対策の実効性を確保する。第三者認証を取得していない場合等で必要と判断する場合、職員が実地確認を行 い、セキュリティ対策の実効性を確保する。 ＜リモート保守環境におけるその他のリスクと措置＞ ・リモート保守を行う事業所の執務エリアは入退室管理された区画とし、作業者の入退室記録を取得する。また保守作業に利用する端末の 利用記録の取得や、監視カメラでの監視体制を敷き、作業者へも周知することで、不適切な方法での情報入手を抑止する。 ・リモート保守環境とガバメントクラウドへの接続については、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し、通信経路上での第 三者からの情報窃取を行えないよう対策する。 ・リモート保守で利用する端末等については、コンピュータウィルス対策ソフトウェアを導入しており、パターンファイルも最新版が適用される よう管理する。また、OSには必要に応じてパッチ適用を実施する。端末内へのデータ保存を行わないシンクライアント端末を利用し、コン ピュータウィルス対策ソフトウェアを導入できない場合については、シンクライアント端末からの接続先となる作業環境に対して同様の対策を 実施する。 ・システムのリモート保守で委託事業者が利用する端末等へは、原則として、特定個人情報の保存を行えないように措置する。端末等への 特定個人情報の保存を必要とする場合、使用後は速やかに消去するとともに、端末等のディスク廃棄時には物理的破壊または専用ソフトで のデータ消去を行わせ、データ消去証明書の提出により確認する。	事後	重要な変更に当たらないため。

令和8年3月30日	Ⅲリスク対策 7．特定個人情報の保管・消去 その他の措置の内容	<枚方市における措置> ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォール、不正侵入防止装置（IPS）を設置している。 ・インターネットとつながらないように、ネットワークをファイアウォールで切断している。 ・コンピューターウイルス対策ソフトウエアを導入しており、パターンファイルも最新版が適用されるよう管理している。 ・DSには必要に応じてパッチ運用を実施している。 <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・プラットフォームでは、UTM（コンピューター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）等を購入し、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購入し、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。	<枚方市における措置> ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォール、不正侵入防止装置（IPS）を設置している。 ・インターネットとつながらないように、ネットワークをファイアウォールで切断している。 ・コンピューターウイルス対策ソフトウエアを導入しており、パターンファイルも最新版が適用されるよう管理している。 ・DSには必要に応じてパッチ運用を実施している。 <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・プラットフォームでは、UTM（コンピューター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）等を購入し、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購入し、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> 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。 ③国及びクラウド事業者は、市の保有データにアクセスしない契約等となっている。 ④市が委託した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。 ⑤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。 ⑥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。 ⑦市が委託した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。 ⑧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。 ⑨市や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。 ⑩市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	事後	重要な変更に当たらないため。

令和8年3月30日	Ⅲリスク対策 7. 特定個人情報の保管・消去 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	＜保管場所＞ ・サーバの盗難を防ぐために、施錠ができる場所等に保管し、施錠をしている。また、設置場所への入退室はICカードにより記録している。 ・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。 ・火災によるデータ消失を防ぐために、施設内に消火設備を完備している。 ＜消去について＞ ・システムに保存されている個人番号については、保存年限到達後にバッチ処理で消去する。 ・申請書等の書類は、保存年限の経過後、溶解して廃棄する。	＜保管場所＞ ・サーバの盗難を防ぐために、施錠ができる場所等に保管し、施錠をしている。また、設置場所への入退室はICカードにより記録している。 ・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。 ・火災によるデータ消失を防ぐために、施設内に消火設備を完備している。 ＜消去について＞ ・システムに保存されている個人番号については、保存年限到達後にバッチ処理で消去する。 ・申請書等の書類は、保存年限の経過後、溶解して廃棄する。 ＜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。	事後	重要な変更に当たらないため。
令和8年3月30日	Ⅲリスク対策 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。	<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、国及びクラウド事業者が対応する。また、ガバメントクラウドに起因しない事象の場合は、市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。	事後	重要な変更に当たらないため。
令和8年3月30日	Ⅳ開示請求、問合せ 1. 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	枚方市個人情報保護条例に基づき、保有個人情報の開示等請求を受け付ける。	個人情報の保護に関する法律に基づき、保有個人情報の開示等請求を受け付ける。	事後	重要な変更に当たらないため。

令和8年3月30日	Ⅳ開示請求、問合せ 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573-1197 大阪府枚方市禁野本町二丁目13番13号 枚方市役所　健康福祉部　地域健康福祉室（母子保健担当）	郵便番号573-1197 大阪府枚方市禁野本町二丁目13番13号 枚方市役所　健康福祉部　保健所　保健予防課	事後	重要な変更に当たらないため。