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
	大阪市　予防接種事務　全項目評価書（令和8年1月以降）

個人のプライバシー等の権利利益の保護の宣言

大阪市は、予防接種事務で特定個人情報ファイルを取り扱うに当たり、特定個人情報の不適正な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分析した上で、当該リスクを軽減させるための適切な措置を講じ、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します。

特記事項	予防接種事務では、委託先による特定個人情報の不正入手・不正使用等への対策として、委託契約書にデータ機密保持事項を明記し、委託先における情報保護管理体制の確認及びデータ保護に関する規程の確認を行うとともに、委託事業者に秘密保持に関する覚書を提出させている。 また本評価書は、令和8年1月のシステム更新後の予防接種事務について記載している。

評価実施機関名

大阪市長

個人情報保護委員会　承認日　【行政機関等のみ】

公表日

［令和6年10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　※	＜予防接種台帳管理システム・保健管理システム（標準準拠）＞ ・予防接種法（昭和二十三年六月三十日法律第六十八号）による予防接種の実施、給付の支給又は実費の徴収に関する事務であって主務省令で定めるもの。 ・新型インフルエンザ等対策特別措置法（平成二十四年法律第三十一号）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 ＜中間サーバ＞ 予防接種に関する事務では、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。）第19条第8号に基づく主務省令第2条の表に基づき、保有する個人情報のうち情報提供に必要な情報を中間サーバに格納する。中間サーバは情報提供ネットワークシステムを通じて関係する各機関と情報連携を行う。また、当事務において必要となる、他機関が保有する情報について、中間サーバを介して情報取得を行う。
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

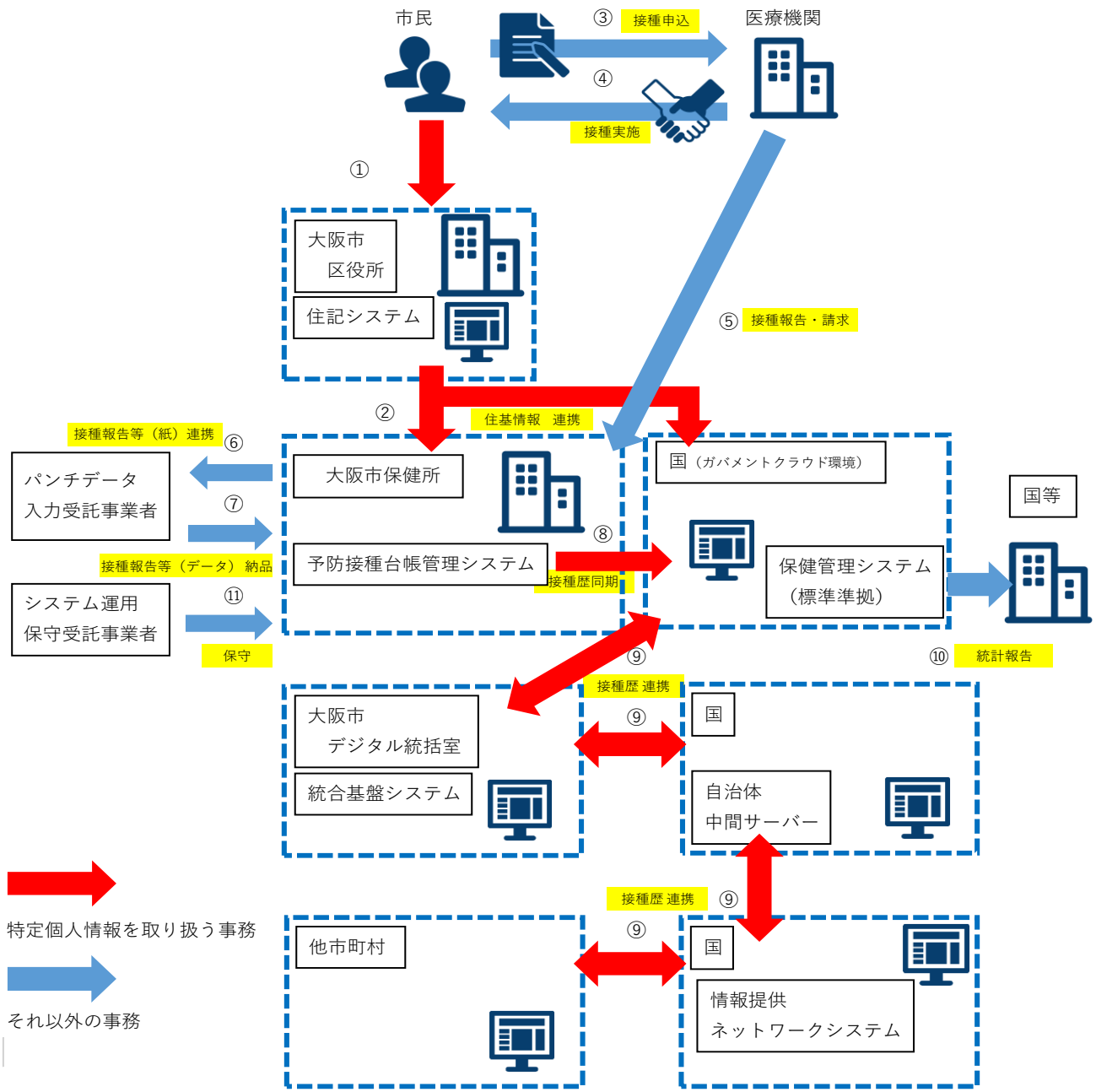
2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	予防接種台帳管理システム
②システムの機能	委託料支払関連業務 1　委託料支払 ・医療機関毎に予防接種の委託料の集計を行う。 ・医療機関宛の支払通知書の作成を行う。 2　医療機関マスタ ・医療機関情報入力（名称・住所・振込口座等） 3　金融機関マスタ ・金融機関情報入力（名称・コード等） 4　集計・統計 ・支払実績の集計 保健管理システム（標準準拠）への接種情報の同期
③他のシステムとの接続	[　]情報提供ネットワークシステム　[　]庁内連携システム [　]住民基本台帳ネットワークシステム　[○]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　（保健管理システム（標準準拠）　）

システム2～5	
システム2	
①システムの名称	統合基盤システム
②システムの機能	1　統合宛名番号付番機能 ・団体内統合宛名番号が未登録の個人について、新規に団体内統合宛名番号を付番する機能。付番した団体内統合宛名番号を業務システム、中間サーバへ連携する機能。 2　宛名情報等管理機能 ・宛名情報等を団体内統合宛名番号、個人番号と紐付けて保存し、管理する機能。 3　中間サーバ連携機能 ・中間サーバからの要求に基づき、団体内統合宛名番号に紐付く宛名情報を通知する機能。 4　業務システム連携機能 ・業務システムからの要求に基づき、団体内統合宛名番号を通知する機能。 5　セキュリティ関連機能 ・業務システムのサーバや端末に対し、ウイルスのパターンファイルの配布を行う機能。 6　認証機能 ・業務システムを利用できるユーザとその業務権限について認証を行う機能。
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　（ 中間サーバ、連携するシステム全て　）
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、本市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 ・中間サーバと既存システム、統合基盤システム及び住民記録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　セキュリティ機能 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 ・バッチ処理の状況管理、業務統計情報の集計、稼働状態の通知、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4	
①システムの名称	保健管理システム（標準準拠）
②システムの機能	台帳管理業務 1　対象者管理 ・住民基本台帳システム等情報をもとに、予防接種毎の対象者を特定する。 ・宛名シール等の印刷を行う。 2　予防接種管理 ・予防接種の種類、接種対象の変更を行う。 ・予防接種委託料の単価変更を行う。 3　接種情報等管理 ・医療機関から提出された予防接種実施報告書をパンチ委託することにより、接種実績データの一括取込を行う。 ・個人の予防接種台帳を表示する。 ・転入者等の予防接種情報を入力する。 ・個々人の予防接種の接種状況を把握し、必要に応じて、接種勧奨を行う。 4　集計・統計 ・予防接種データを基に各種統計表・グラフの作成を行う。
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　（ 予防接種台帳管理システム、住民記録システム　　）
③他のシステムとの接続	[　　] 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	
予防接種関連情報ファイル	
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	感染症のまん延防止のために、予防接種の高い接種率が必要であり、より確実な接種履歴の把握が必要である。また、健康被害救済の給付手続きにおいて、他の法令による医療の給付に関する支給状況等を把握する必要がある。
②実現が期待されるメリット	・より適切な接種勧奨につながる。 ・市民による接種歴の確認が容易となる。 ・各種証明書等の提出が不要になるなど市民負担の軽減につながる。
5. 個人番号の利用　※	
法令上の根拠	番号法第9条第1項別表第14の項、第126の項
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	＜情報照会＞ 番号法第19条第8号に基づく主務省令第2条の表　第25、27、28、153の項 ＜情報提供＞ 番号法第19条第8号に基づく主務省令第2条の表　第25、153、154の項
7. 評価実施機関における担当部署	
①部署	健康局大阪市保健所感染症対策課
②所属長の役職名	健康局長
8. 他の評価実施機関	
なし	

（別添1）事務の内容


市民
③ 接種申込
医療機関
④
接種実施
①
大阪市
区役所
住記システム
⑤ 接種報告・請求
②
住基情報　連携
接種報告等（紙）連携
⑥
パンチデータ
入力受託事業者
⑦
大阪市保健所
国（ガバメントクラウド環境）
国等
⑧
予防接種台帳管理システム
接種歴同期
保健管理システム
（標準準拠）
接種報告等（データ）納品
システム運用
保守受託事業者
⑪
保守
⑨
⑩ 統計報告
接種歴 連携
⑨
大阪市
デジタル統括室
統合基盤システム
国
自治体
中間サーバー
接種歴 連携
⑨
⑨
他市町村
国
情報提供
ネットワークシステム
特定個人情報を取り扱う事務
それ以外の事務

（備考）

＜住基情報の連携＞
①・・・出生届、住民票等の各種届出（他業務）。
②・・・予防接種台帳作成のための住基情報の連携。
＜予防接種の実施・報告＞
③・・・接種にあたって、医療機関に予約を行い、接種当日には母子手帳、予防接種手帳等を持参し、予防接種実施申込書等に必要事項を記載して接種。
④・・・医療機関で接種。
⑤・・・医療機関にて実施した予防接種の内容を取りまとめ、保健所へ請求とともに報告。
＜接種情報の予防接種台帳管理システムへの取込＞
⑥・・・医療機関から提出された報告書類の内容に基づき、パンチデータ入力委託事業者にてパンチデータを作成を依頼。
⑦・・・パンチデータを大阪市へ納品。大阪市にて予防接種台帳管理システムに取り込み、接種歴を管理。
＜予防接種台帳管理システムから保健管理システム（標準準拠）への同期＞
⑧・・・接種歴を同期。
＜個人番号での連携＞
⑨・・・予防接種履歴の情報を中間サーバへあげ、他市町村からの転入者、他市町村への転出者に係る予防接種歴の情報は情報提供ネットワークシステムを介して、取得及び提供する。
＜統計報告＞
⑩・・・予防接種に関する統計情報を国等に報告。
＜その他＞
⑪・・・予防接種台帳管理システム及び保健管理システム（標準準拠）保守に係る役務の提供

※中間サーバ接続端末・・・総務省が開発する中間サーバ・ソフトウェアの機能で、中間サーバの副本の登録・更新や、中間サーバに対する情報提供の求めを端末から直接行えるもの。

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		
予防接種関連情報ファイル		
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		[　100万人以上1,000万人未満　] ＜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 ※		定期予防接種の被接種者
	その必要性	感染症のまん延防止には、予防接種の高い接種率が必要であり、適切な接種勧奨を行う必要がある。 個人の接種歴の適正管理、未接種者に対するきめ細かな接種勧奨の実施等のために保有している。
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 [○] 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）：予防接種を受けた対象者を正確に特定するために保有 ・連絡先等情報：未接種者への接種勧奨等のために保有
	全ての記録項目	別添2を参照。
⑤保有開始日		平成28年1月4日
⑥事務担当部署		健康局大阪市保健所感染症対策課

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 （ 市町村 ） [ ] 地方公共団体・地方独立行政法人 （ ） [ ] 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入手の時期・頻度			＜予防接種台帳管理システム・保健管理システム（標準準拠）に関するもの＞ ・住民基本台帳情報について、差分データを取込 ・転入者の届出のあった接種歴情報を随時入力
④入手に係る妥当性			・感染症のまん延防止のため、適切な接種勧奨を行い、高い接種率が必要であり、接種歴の適正な管理、未接種者への接種勧奨を行うため各種情報を入手している。
⑤本人への明示			本人から入手する情報については、予防接種を受ける際に、所定様式にて利用目的を本人に明示している。
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）を行う外、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。
	変更の妥当性		
⑦使用の主体	使用部署 ※		健康局大阪市保健所感染症対策課
	使用者数		[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
⑧使用方法 ※			①台帳管理業務 ・住民基本台帳ネットワークシステム等情報をもとに、予防接種毎の対象者を特定する。 ・個々人の予防接種の接種状況を把握し、必要に応じて、接種勧奨を行う。 ・予防接種データを基に各種統計表・グラフの作成を行う。 ②委託料支払関連業務 ・医療機関毎に予防接種の委託料の集計を行う。
	情報の突合 ※		住民基本台帳情報と接種データを突合させて、接種を受けた者を特定する。
	情報の統計分析 ※		区別接種件数、種類ごとの接種件数、地域保健事業報告資料等の統計を実施。
	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4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 （ 3 ） 件
委託事項1		システム保守・運用業務
①委託内容		予防接種台帳管理システム・保健管理システム（標準準拠）の定常的な運用及びメンテナンス等の保守業務
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	[100万人以上1,000万人未満] ＜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 ※	特定個人情報ファイルの範囲と同様
	その妥当性	予防接種業務の正確かつ適正な業務の実施及び予防接種台帳管理システムの安定した稼働を図るため、専門的な知識を有する民間業者に委託する必要がある。
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 （ サーバ室内にてシステムの直接操作又は入退室を制限した部屋の端末を利用 ）
⑤委託先名の確認方法		委託先が決定した際には、本市ホームページにて公表している。
⑥委託先名		日本コンピューター株式会社
再委託	⑦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
	⑧再委託の許諾方法	
	⑨再委託事項	
委託事項2～5		
委託事項2		基盤系システム統合基盤運用保守
①委託内容		基盤系システム統合基盤の維持管理にかかる運用保守
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	[100万人以上1,000万人未満] ＜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 ※	特定個人情報ファイルの範囲と同様
	その妥当性	安定した稼働のため専門的な知識を有する民間事業者に委託している。
③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

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　（特定個人情報ファイルは提供していないが、サーバ設置場所、または中央情報処理センターにおける運用保守を行っている。）
⑤委託先名の確認方法		大阪市ホームページの入札契約情報にて確認できる。
⑥委託先名		株式会社NTTデータ関西
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	業務委託契約書の規定に基づく再委託承諾申請書の提出があった場合は、申請内容を審査した結果、再委託が適当と判断した場合は委託先に対し承諾書を交付する。
	⑨再委託事項	統合基盤システムに関する製造、試験、環境構築(本番・保守)、及び運用保守における一部業務
委託事項3		中央情報処理センター第二別館運用業務委託
①委託内容		バックアップ用媒体の管理
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	[　100万人以上1,000万人未満　]　＜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 ※	特定個人情報ファイルの対象と同様
	その妥当性	災害時においてもシステムを復元し稼働を継続させるため、復元対象となる情報を保存した媒体の管理、保管業者への受け渡しを委託している。なお、媒体作成は自動処理を行っているため、サーバ室のテープ装置でのテープ装填・取り出し作業のみで個人情報にアクセスすることはないが、基本的な個人情報の取り扱いについては契約条項に定めている。
③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
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　（サーバ室内で鍵付きのサーバラックに設置されたテープ装置に対してテープを装填・取り出し作業を実施しており、委託先に特定個人情報を提供することはない。）
⑤委託先名の確認方法		大阪市ホームページの入札契約情報にて確認できる。
⑥委託先名		株式会社オプテージ
再委託	⑦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
	⑧再委託の許諾方法	
	⑨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 （ 3 ）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	番号法第19条第8号に基づく主務省令第2条の表 第25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事務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	月次
提供先2～5	
提供先2	都道府県知事または市町村長
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 第153の項
②提供先における用途	予防接種法もしく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	予防接種履歴
④提供する情報の対象となる本人の数	[1万人以上10万人未満] ＜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	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	月次
提供先3	都道府県知事または市町村長
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 第154の項
②提供先における用途	予防接種法もしく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	予防接種履歴
④提供する情報の対象となる本人の数	[1万人以上10万人未満] ＜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	予防接種法又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	月次

6. 特定個人情報の保管・消去

①保管場所 ※		【特定個人情報の保管場所】 ・特定個人情報はシステム用ファイルとして予防接種台帳管理システムのサーバ内、及び、ガバメントクラウドの保健管理システム（標準準拠）に格納している。（また、特定個人情報のうち4情報については、統合基盤システムのサーバにも格納される。） 【保管場所の状況】 ＜サーバにおける措置＞ ①予防接種台帳管理システムのサーバは、保健医療対策課事務スペース内の、施錠可能なドアのある一室に設置。 ②記録簿を設け、日々の施錠を確認。 ＜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・プラットフォームのデータ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。 ②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。 ＜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。 ＜保健管理システム（標準準拠）における措置＞ 保健管理システム（標準準拠）はガバメントクラウドで稼働するため、保管場所は「ガバメントクラウドにおける措置」に記載するとおりとする。
②保管期間	期間	[5年] ＜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	予防接種法における定期接種実施要領等の規定に基づき保存期間を定めている。
③消去方法		＜予防接種事務における措置＞ ・データについては、保管期間満了後、システムにてデータベースより削除する。 ＜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、物理的破壊または専用ソフト等を利用して完全に消去する。 ＜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。 ＜保健管理システム（標準準拠）における措置＞ ・保健管理システム（標準準拠）はガバメントクラウドで稼働するため、保管場所は「ガバメントクラウドにおける措置」に記載するとおりとする。

7. 備考

（別添2）特定個人情報ファイル記録項目

別紙のとおり

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

予防接種関連情報ファイル

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	【申請者からの情報入手】 ・本人が書面を提出する際に、本人が本人（世帯員含む。以降、同様の定義とする）以外の情報を誤って記載することがないようチェックを行う。 ・予防接種に関する事務に係る各種申請に母子手帳、運転免許証、個人番号カード等で申請者の本人確認も行う。 【他部署からの情報入手】 ・4情報及びその他住民票関係情報（以下、住民情報）を連携しており、対象者を特定するための項目は最新の状態が維持され、対象外の情報を入手するリスクを低減する。
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	【申請者からの情報入手】 ・本人から書面提出を求める場合、本人が必要な情報以外を誤って記載することがないような書面様式とする。 【他部署からの情報入手】 ・情報入手の際、業務要件上、不要な項目は取得できないようにすることにより、対象外の項目を入手するリスクを低減する。
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

リスクに対する措置の内容	【申請者からの情報入手】 ・個人情報の収集に当たっては、本人から収集することを原則としている。 ・権利のない者からの届出を受付ないように届出人要件の確認を徹底する。 【他部署からの情報入手】 ・事務を行う上で従事者からの予防接種台帳管理システム・保健管理システム（標準準拠）へのアクセスは権限が付与された者しか利用できないよう認証機能を設けている。また、業務に必要な情報のみを入手できるようにする。 ・システムを利用する必要がある場合は、ユーザID及びパスワードによる認証、生体情報（指静脈）による認証を行い、操作者が利用可能な権限を限定している。
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	本人確認を母子手帳、運転免許証、個人番号カード等で行う。
個人番号の真正性確認の措置の内容	個人番号カード等の提示を受け、予防接種台帳管理システムにて個人番号に相違ないか確認を行う。
特定個人情報の正確性確保の措置の内容	【本人からの情報入手における措置】 ・本人の申し出に基づき特定個人情報を最新の情報に保つよう努めている。 ・住民ではない方の情報については、各事務運用において、正確性が確保された情報を取得する。 ・問題がある場合は本人への聞き取りや他部署・他団体への照会を行い、内容の正確性確保を図る。 【他部署からの情報入手】 ・住民の情報については、住民記録システムから情報を定期的に取得する。

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	【本人からの情報入手】 ・届出関係の書類は、受付後は専用の収納ケースに保管する。 【他部署からの情報入手】 ・照会情報を記載した保管不要な書類はシステムへの入力等を終えた場合は速やかに処分する。 ・事務を行う上で従事者からの統合基盤システムへのアクセスは本市専用回線によるセキュアなネットワーク利用に限定する。 【その他】 ・情報セキュリティポリシーの周知等を職員に行う。また、情報漏えい等の防止のため、責任者の許可なく端末機又は記録媒体等を執務室以外に持出すことの禁止や、アクセス権限の管理、システムへのアクセス記録、コンピュータウィルス対策などを実施。 ・定期的及び随時にウイルスソフトウエアの更新を行う。
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	・統合基盤システム（統合宛名番号付番機能、宛名情報等管理機能）に接続できるシステムは番号法で定められたものに限定しており、番号法に関係しないシステムが連携することはできない。 ・統合基盤システム（統合宛名番号付番機能、宛名情報等管理機能）から予防接種台帳管理システムには直接アクセスできない仕組みのため、統合基盤システム（統合宛名番号付番機能、宛名情報等管理機能）が情報の紐付けを行うことはできない。 ・統合基盤システム（宛名情報等管理機能）には個別業務の特定個人情報を保有しない。 ・番号法に関係する事務を行う部署において、権限を付与された者のみ統合基盤システム（統合宛名番号付番機能、宛名情報等管理機能）にアクセス可能な仕組みとする。
事務で使用するその他のシステムにおける措置の内容	予防接種台帳管理システム・保健管理システム（標準準拠）において使用する端末は、他のシステム（保健衛生システム、結核登録者情報システム）との共用端末であるが、予防接種事務を担当する職員が使用できるのは、予防接種台帳管理システム・保健管理システム（標準準拠）のみに限られている。したがって、予防接種関連情報ファイルにのみアクセスでき、その他の事務に用いるファイルにはアクセスできない。
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	【認証方法】 ＜予防接種台帳管理システム・保健管理システム（標準準拠）における措置＞ ・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、生体情報（指静脈）による認証を行っている。ログイン時において、正しくない操作が繰り返しなされた場合、ロックアウトする仕組みをとっている。 ・ユーザIDのログ情報を保管して、管理している。権限を有しない者の使用や閲覧防止のため、端末から離れる場合にはログオフし、ソーシャルエンジニアリングを防止している。 ・ユーザIDは、管理者が管理し、人事異動等でシステム操作者に変更があれば無効の設定を行う。 ＜統合基盤システムに関わる措置＞ 統合基盤システムへの利用権限を持つ従事者にのみユーザIDを付与し、ユーザIDとパスワードによる認証、生体情報（指静脈）による認証を行っている。パスワードは定期的及び随時に変更するよう周知するとともにシステム的に変更を求める設定としている。 【なりすまし防止策】 従事者は以下を遵守し、利用ユーザIDを適切に管理する。 ・パスワードは第三者に知られないように管理する ・パスワードを秘密にし、パスワードの照会等には一切応じない ・パスワードは十分な長さとし、文字列は想像しにくいものとする ・パスワードは定期的に変更する ・端末機等のパスワードの記憶機能を利用しない ・パスワードが流出した可能性がある場合は、速やかに端末機管理者に報告し、パスワードを変更する ・使用する機器や記録媒体について、権限を有しない者の使用や閲覧を防止するため、端末から離れる場合にはログオフにする等適切な措置を講じる
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	＜予防接種台帳管理システム・保健管理システム（標準準拠）における措置＞ 【アクセス権限の発効管理】 ・従事者が所属する部署、業務システムを所管する部署の管理者が業務上必要なユーザIDを確認し、アクセス権限管理を行う管理者へ発効の申請を行う。 【アクセス権限の失効管理】 ・従事者が所属する部署、業務システムを所管する部署の管理者が業務上不要となったユーザIDを確認し、アクセス権限管理を行う管理者へ失効の申請を行う。 ＜統合基盤システムに関わる措置＞ 【アクセス権限の発効管理】 ・統合基盤システムを操作する従事者の権限に応じたユーザID、アクセス権限の割付を行う。 【アクセス権限の失効管理】 ・担当替え等により操作権限を無くした者のユーザIDやアクセス権限について利用無効や権限削除を行う。
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	＜予防接種台帳管理システム・保健管理システム（標準準拠）における措置＞ ・共用IDは発行せず、必ず個人に対しユーザIDを発行する。 ・ユーザIDやアクセス権を管理者が定期的に確認し、不要となったIDやアクセス権を変更または削除する。 ・生体認証を導入し、IDとの二要素認証としている。 ＜統合基盤システムに関わる措置＞ ・操作部署や業務システムの管理者からの申請に基づき、従事者へユーザID及び権限を付与する。担当替え等の際は、システム及び管理者により利用を無効とする。 ・生体認証を導入し、IDとの二要素認証としている。

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	＜予防接種台帳システム・保健管理システム（標準準拠）における措置＞ ・システムへのログイン記録、個人を特定した検索及び特定後の操作ログの記録を行う。操作者は個人まで特定でき、記録は5年間保存する。また、記録は定期的に確認し、不正アクセスがないかどうかを確認する。 ＜統合基盤システムに関わる措置＞ ・統合基盤システムのアクセスログ、操作ログを記録し、事務運用で必要となる期間と同一の期間保存する。
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		【職員の情報管理】 ・特定個人情報の利用を事務の目的の達成に必要な範囲内に限定し、事務目的外の利用、提供を原則として禁止している。 ・職員には、業務外でのシステムへのアクセスを禁止しているとともに、システムの操作ログを記録している。 ・業務管理者が、システムの運用に関わる職員を対象に、システム及び当該システムにより処理されるデータに関わる情報セキュリティの実施手順並びに実施に必要な知識及び技術について研修を行っている。 【委託事業者の情報管理】 ・委託事業者に対しては、業務外で使用しないように委託契約書に定め、さらに委託事業者において、当該職員に対して情報セキュリティ研修を実施させている。 【職員の違反措置】 違反行為を行った場合は法の罰則規定により措置を講ずる。なお、本市では懲戒処分に関する指針により、次の事項の違反時は懲戒処分の対象としている。 ・個人情報の流出 ・個人情報の目的外使用 ・情報セキュリティポリシー違反
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		【職員の情報管理】 ・管理者が、システムの運用に関わる職員を対象に、システム及び当該システムにより処理されるデータに関わる情報セキュリティの実施手順並びに実施に必要な知識及び技術について研修を行っている。 【委託事業者の情報管理】 ・委託先に対しては、委託契約書にてデータの無断使用及び第三者への提供の禁止や、複写及び複製の禁止をしている。さらに、委託事業者において、当該職員に対して情報セキュリティ研修を実施していることを確認している。 ＜予防接種台帳管理システム・保健管理システム（標準準拠）における措置＞ ・予防接種台帳管理システム利用時の職員認証の外に、操作内容が記録されるため、不適切な利用を防止する。 ＜統合基盤システムにおける措置＞ ・統合基盤システム利用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、操作内容が記録されるため、不適切な利用を抑止する。
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
【リスク】 悪意を持った担当者が事務外で特定個人情報を使用する。 【リスクに対する措置】 特定個人情報の取扱に係る研修を実施するとともに、職務違反措置の他、正当な理由のない提供、不正な利益目的による提供・窃盗、職務上知り得た秘密を漏洩又は盗用したとき等の番号法における罰則の強化について、周知徹底し、けん制機能を働かせる。

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	【業者選定時】 ・プライバシーマークの取得を資格要件としている。 【契約時】 ・契約書において次の事項を定めている。 ア 個人情報保護に関する規程、体制の整備 イ 個人情報保護に関する安全管理措置 ウ 情報セキュリティ対策の実施責任者の配置 ・適切な社内における情報保護管理体制が構築されているか、管理体制の説明を求め確認している。 ・必要に応じ、事業者の管理記録簿の確認又は作業場所の立入検査等を実施する。
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	委託契約書に以下の規定を設ける。 ①データの機密保持に関する事項を明記し、委託処理の際にデータ保護に関する委託先の規程の確認を行っている。 ②委託事業者に対しては業務外で使用しないように委託契約書に定めている。 ③委託事業者において、当該職員に対して情報セキュリティ研修を実施していることを確認している
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	・特定個人情報が記録されたサーバ等での作業については、事前に作業報告の提出を求める。 ・システム作業のためにサーバ等のメンテナンス用のID、パスワードを利用させており、当日の作業報告と照合することで作業者の特定ができる。 ・上記の作業実績等については、サーバに記録し毎日蓄積・保存する。 ・システムの改修や設定変更に係る作業については、作業対象となるOSやミドルウェアが保有する機能により保守作業の操作内容が記録される。

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	・予防接種関連情報ファイルを扱う際には、庁舎内での作業を必須としている。また、他者への提供は一切認めない。
	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	・委託先へ特定個人情報ファイルを提供することはなく、特定個人情報を取扱う作業を行う場合は感染症対策課内設置端末又は入退室を制限した部屋の端末を利用するなど、特定の作業場所で行うこととしている。 ・委託元は、必要があると認めるときは、委託先の個人情報等の保護状況について立入検査を実施する。
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	・委託事業者には特定個人情報の持ち出しは許可していないため、消去対象の情報はない。
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	・漏えい、滅失、き損等の防止その他個人情報等の保護に必要な体制の整備及び措置を講じなければならない ・個人情報等の授受・搬送・保管・廃棄等について、管理責任者を定める ・個人情報等の管理が適切でないと認められる場合、委託業者に対し改善を求めるとともに、個人情報等の管理状況を適切であると認めるまで委託業務を中止させることができる ・目的外利用の禁止及び第三者への提供禁止 ・個人情報等の外部への持ち出し禁止 ・個人情報等を複写又は複製禁止(本市の同意を得た場合を除く) ・個人情報等の保護状況について立入検査を実施することが可能
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		[　　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		
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		
委託先事業所内に試験データ等の持ち出しを行う場合、個人情報は全てマスキングを行い、大阪市事業所以外での特定個人情報ファイルの取扱いは一切発生させない。		

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	[ ]	＜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	[ ]	＜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
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	[ ]	＜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	[ ]	＜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	＜予防接種台帳管理システム・保健管理システム（標準準拠）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。また特定個人情報保護の理解度を高めるために、教育・指導を行う。 ＜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より求め、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）番号法第19条第8号に基づく主務省令第2条の表に基づき、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	＜中間サーバ・ソフトウェアにおける措置＞ 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（バーチャルプライベートネットワーク）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	＜中間サーバ・ソフトウェアにおける措置＞ 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	＜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ができない。
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	＜予防接種台帳管理システム・保健管理システム（標準準拠）の運用における措置＞ ①情報提供ネットワークシステムにおける情報連携においては、中間サーバに保有されている情報のみが連携されることになっており、中間サーバに保有される特定個人情報は、番号法の規定に基づき定められた情報のみとなっていることから、不正に提供されるリスクに対応している。 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。 ※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。 ＜中間サーバ・ソフトウェアにおける措置＞ ①②③＜予防接種台帳管理システム・保健管理システム（標準準拠）の運用における措置＞と同様 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	＜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うえ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。 ＜中間サーバの運用における措置＞ セキュリティ実施手順等について定期的に職員へ研修を行う。また、情報漏えい等の防止のため、管理者の許可なく端末機又は記録媒体等を執務室以外に持出すことの禁止、アクセス権限の管理、システムへのアクセス記録を実施する。
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	＜予防接種台帳管理システム・保健管理システム（標準準拠）の運用における措置＞ ①情報提供ネットワークシステムにおける情報連携においては、中間サーバに保有されている情報のみが連携されることになっており、中間サーバに保有される特定個人情報は、番号法の規定に基づき定められた情報のみとなっていることから、誤った情報の提供が行われるリスクに対応している。 ＜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うえで、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
＜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	【情報システム室における対策】 特定個人情報を格納するサーバを設置する情報システム室は次の対策を行っている。 ・情報システム室、サーバ機器には複数段階における施錠をしており、容易な入退出、操作ができないようになっている。 ・情報システム室内に設置したサーバは、転倒・落下防止等の耐震対策を行っている。 ・サーバ機器には無停電電源装置を設置し、電気的障害に対する措置を講じている。 ・個人所有のパソコン等の機器や記録媒体を持ち込んではならない。また、原則として、定められた端末機以外の機器や記録媒体を業務に使用してはならないとしている。 ・業務上、やむを得ず、定められた端末機以外の機器や記録媒体を持ち込んで業務に使用する場合には、事前に目的等を明確にして責任者に申請し、承認を得ることとしている。 【端末設置場所における対策】 特定個人情報の入出力や閲覧を行う端末の設置場所については、次の対策を行っている。 ・端末機を設置する事務室は、職員不在時は施錠し、外部から立ち入りできないようにしている。 ＜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。 ＜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。 ＜保健管理システム（標準準拠）における措置＞ ・保健管理システム（標準準拠）はガバメントクラウド上で稼働するため、「ガバメントクラウドにおける措置」に記載のとおり。		

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	【ウイルス対策】 ・ウイルス対策ソフトウェアを導入し、サーバ及び端末機に常駐させることで、コンピュータウイルス等の不正プログラム検出を行っている。 ・ウイルス対策ソフトウェアについて、定期的に当該ソフトウェア及びパターンファイルの更新を実施している。 【不正アクセス対策】 ・予防接種台帳管理システムは住民情報等を取り扱う重要システムが利用する専用ネットワークに接続しており、インターネットとは物理的に接続されていない。 ＜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。 ・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。 ・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」（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。 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。 ＜保健管理システム（標準準拠）における措置＞ ・保健管理システム（標準準拠）はガバメントクラウド上で稼働するため、「ガバメントクラウドにおける措置」に記載するとおり
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保管方法としている。
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： 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	＜予防接種台帳管理システム・保健管理システム（標準準拠）における措置＞ ・住民の情報については、住民記録システムから情報を定期的に取得する。また、住民ではない方の情報については、事務運用において、正確性が確保された情報を取得する。 ＜統合基盤システムにおける措置＞ ・統合宛名に係る住民情報については、住民記録システムと連携し、最新の状態を維持する。また、住民以外の情報については、各事務運用において、正確性が確保された情報に更新される。	
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	・データについては、保管期間満了後、システムにてデータベースより削除する。 ・ガバメントクラウドにおいては、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、NIST800-88、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。	
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	・評価書の記載内容通りの運用ができているか年1回担当部署で確認する。 ・ミスを発生しにくくするための業務管理上の確認事項を定め、その遵守状況について年1回点検する。 ・個人情報保護委員会が実施する「特定個人情報の取扱いの状況に係る地方公共団体等による定期的な報告について」及び評価書の見直し時期を契機に、評価書のリスク対策に記載されている項目の措置状況を点検する。 ＜中間サーバ･プラットフォームにおける措置＞ セキュリティ実施手順等に基づき、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	・大阪市情報セキュリティ検査実施要綱に基づき、毎年1回、最高情報セキュリティ責任者が実施する内部検査において、すべてのシステムの情報セキュリティ対策の実施状況について確認を行い、対応できていない項目の改善案を作成し、順次対応を行う。 ・監査委員による監査の一環として、自己点検や情報セキュリティ検査の結果等を参考に監査対象を選定し、情報セキュリティ監査を実施している。 ＜中間サーバ･プラットフォームにおける措置＞ セキュリティ実施手順等に基づき、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。 ＜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。
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	＜予防接種台帳管理システム･保健管理システム（標準準拠）における措置＞ ・システム利用者に対し、情報セキュリティ実施手順の周知及び情報セキュリティの啓発のための研修を実施する。 ・システムの情報セキュリティ実施手順を改訂した場合は改訂ポイントとその理由について周知徹底を図る。 ・違反行為を行ったものに対しては、懲戒処分に関する指針に基づき懲戒処分の対象となる。 ・特定個人情報等の適切な取扱いに関する研修が開催される場合は、新たに従事する職員については必ず出席することとしている。また、研修後は、担当内でフィードバックを行い、全従事職員に対する研修内容の共有化を図っている。 ・情報セキュリティ管理規程等に則した内容のeラーニング等による研修を実施している。 ＜中間サーバ･プラットフォームにおける措置＞ ①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、セキュリティ研修を実施することとしている。 ②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。

＜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。

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	〒530－8201 大阪市北区中之島1丁目3番20号 大阪市総務局行政部行政課（情報公開グループ）
②請求方法	・窓口（大阪市役所本庁舎1階市民相談室）で直接、開示・訂正・利用停止請求 ・郵便にて開示・訂正・利用停止請求
特記事項	大阪市ホームページ上に請求先及び請求方法を掲載
③手数料等	[　　無料　　]　　＜選択肢＞ 1）有料　　2）無料 （手数料額、納付方法：　　）
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	1、予防接種台帳管理システム（風しん抗体検査・第5期定期接種の登録ファイル） 2、予防接種台帳管理システム
公表場所	大阪市ホームページ　https://www.city.osaka.lg.jp/kenko/page/0000605359.html
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	〒545－0051 大阪市阿倍野区旭町1丁目2番7-1000号（あべのメディックス10階） 大阪市健康局大阪市保健所感染症対策課 電話：06-6647-0813　ファックス：06-6647-1029
②対応方法	・問合せ内容を十分聴き取り、申出者に説明行い、その対応について記録を残す。 ・漏えい等に係る問合せについては、必要に応じて調査等を実施し、申出者に説明する。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	
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	
②実施日・期間	
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	大阪市個人情報保護審議会へ諮問
③結果	
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	

（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
	Ⅰ　1②事務の内容	＜予防接種台帳管理システム＞ ＜中間サーバ＞ 予防接種に関する事務では、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。）別表第二に基づき、保有する個人情報のうち情報提供に必要な情報を中間サーバに格納する。中間サーバは情報提供ネットワークシステムを通じて関係する各機関と情報連携を行う。また、当事務において必要となる、他機関が保有する情報について、中間サーバを介して情報取得を行う。	＜予防接種台帳管理システム・保健管理システム（標準準拠）＞ ＜中間サーバ＞ 予防接種に関する事務では、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。）第19条第8号に基づく主務省令第2条の表に基づき、保有する個人情報のうち情報提供に必要な情報を中間サーバに格納する。中間サーバは情報提供ネットワークシステムを通じて関係する各機関と情報連携を行う。また、当事務において必要となる、他機関が保有する情報について、中間サーバを介して情報取得を行う。	事前	標準準拠システム移行に伴う変更、保健管理システム（標準準拠）導入 ※令和7年〇月〇日公表の評価書番号32からの変更箇所を記載。以降、変更日が令和7年〇月〇日のものは同様
	Ⅰ　2　システム1 ②システムの機能	①台帳管理業務 ア　対象者管理 　・住基等システム情報をもとに、予防接種毎の対象者を特定する。 　・宛名シール等の印刷を行う。 イ　予防接種管理 　・予防接種の種類、接種対象の変更を行う。 　・予防接種委託料の単価変更を行う。 ウ　接種情報等管理 　・医療機関から提出された予防接種実施報告書をパンチ委託することにより、接種実績データの一括取込を行う。 　・個人の予防接種台帳を表示する。 　・転入者等の予防接種情報を入力する。 　・個々人の予防接種の接種状況を把握し、必要に応じて、接種勧奨を行う。 エ　集計・統計 　・予防接種データを基に各種統計表・グラフの作成を行う。	－	事前	システム追加に伴う修正
	Ⅰ　2　システム1 ②システムの機能	②委託料支払関連業務 ア　委託料支払 　・医療機関毎に予防接種の委託料の集計を行う。 　・医療機関宛の支払通知書の作成を行う。 イ　医療機関マスタ 　・医療機関情報入力（名称・住所・振込口座等） ウ　金融機関マスタ 　・金融機関情報入力（名称・コード等） エ　集計・統計 　・支払実績の集計	○委託料支払関連業務 1　委託料支払 　・医療機関毎に予防接種の委託料の集計を行う。 　・医療機関宛の支払通知書の作成を行う。 2　医療機関マスタ 　・医療機関情報入力（名称・住所・振込口座等） 3　金融機関マスタ 　・金融機関情報入力（名称・コード等） 4　集計・統計 　・支払実績の集計 ○保健管理システム（標準準拠）への接種情報の同期	事前	システム追加に伴う修正
	Ⅰ　2　システム1 ③他のシステムとの接続	－	〔○〕その他　保健管理システム（標準準拠）	事前	システム追加に伴う追加
	Ⅰ　2　システム4 ①システム名称	－	保健管理システム（標準準拠）	事前	システム追加に伴う追加
	Ⅰ　2　システム4 ②システムの機能	－	台帳管理業務 1　対象者管理 ・住民記録システム情報をもとに、予防接種毎の対象者を特定する。 ・宛名シール等の印刷を行う。 2　予防接種管理 ・予防接種の種類、接種対象の変更を行う。 ・予防接種委託料の単価変更を行う。 3　接種情報等管理 ・医療機関から提出された予防接種実施報告書をパンチ委託することにより、接種実績データの一括取込を行う。 ・個人の予防接種台帳を表示する。 ・転入者等の予防接種情報を入力する。 ・個々人の予防接種の接種状況を把握し、必要に応じて、接種勧奨を行う。 4　集計・統計 ・予防接種データを基に各種統計表・グラフの作成を行う。	事前	システム追加に伴う追加
	Ⅰ　2　システム4 ③他のシステムとの接続	－	〔○〕既存住民情報台帳システム 〔○〕宛名システム等 〔○〕その他　予防接種台帳管理システム、住民記録システム	事前	システム追加に伴う追加
	Ⅰ（別添1）事務の内容	－	別添のとおり	事前	システム追加に伴う修正

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　3③入手の時期・頻度	＜予防接種台帳管理システム＞ ・住民基本台帳情報について、日次で差分データを取込 ・転入者の届出のあった接種歴情報を随時入力	＜予防接種台帳管理システム・保健管理システム（標準準拠）に関するもの＞ ・住民基本台帳情報について、差分データを取込 ・転入者の届出のあった接種歴情報を随時入力	事前	システム追加に伴う修正
	Ⅱ　4委託の有無	4	3	事前	システム追加に伴う修正
	Ⅱ　4　委託事項1	予防接種台帳管理システムの定常的な運用及びメンテナンス等の保守業務	予防接種台帳管理システム・保健管理システム（標準準拠）の定常的な運用及びメンテナンス等の保守業務	事前	システム追加に伴う修正
	Ⅱ　4　委託事項1 ④委託先への特定個人情報ファイルの提供方法	サーバー室内にてシステムの直接操作	サーバ室内にてシステムの直接操作又は入退室を制限した部屋の端末を利用	事前	システム追加に伴う修正
	Ⅱ　4　委託事項2 ④委託先への特定個人情報ファイルの提供方法	サーバ設置場所、または中央情報処理センター内の情報システム内における運用保守のため提供しない。	特定個人情報ファイルは提供していないが、サーバ設置場所、または中央情報処理センターにおける運用保守を行っている。	事前	システム追加に伴う修正
	Ⅱ　6①保管場所	【特定個人情報の保管場所】 ・特定個人情報はシステム用ファイルとして予防接種台帳管理システムのサーバ内に格納している。（また、特定個人情報のうち4情報については、統合基盤システムのサーバにも格納される。） 【保管場所の状況】 ①サーバ ・予防接種台帳管理システムのサーバは、保健医療対策課事務スペース内の、施錠可能なドアのある一室に設置。 ・記録簿を設け、日々の施錠を確認。 ②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データ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。 ・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。	【特定個人情報の保管場所】 ・特定個人情報はシステム用ファイルとして予防接種台帳管理システムのサーバ内、及び、ガバメントクラウドの保健管理システム（標準準拠）に格納している。（また、特定個人情報のうち4情報については、統合基盤システムのサーバにも格納される。） 【保管場所の状況】 ＜サーバにおける措置＞ ①予防接種台帳管理システムのサーバは、保健医療対策課事務スペース内の、施錠可能なドアのある一室に設置。 ②記録簿を設け、日々の施錠を確認。 ＜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・プラットフォームのデータ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。 ②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。	事前	システム追加に伴う修正
	Ⅱ　6①保管場所	同上	＜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。 ＜保健管理システム（標準準拠）における措置＞ 保健管理システム（標準準拠）はガバメントクラウドで稼働するため、保管場所は「ガバメントクラウドにおける措置」に記載するとおりとする。	事前	システム追加に伴う修正
	Ⅱ　6③消去方法	―	＜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。 ＜保健管理システム（標準準拠）における措置＞ ・保健管理システム（標準準拠）はガバメントクラウドで稼働するため、保管場所は「ガバメントクラウドにおける措置」に記載するとおりとする。	事前	システム追加に伴う追加

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　2リスク1 対象者以外の情報の入手を防止するための措置の内容	【申請者からの情報入手】 ・予防接種に関する事務に係る各種申請に保険証、母子手帳、運転免許証、個人番号カード等で申請者の本人確認も行う。	【申請者からの情報入手】 ・予防接種に関する事務に係る各種申請に母子手帳、運転免許証、個人番号カード等で申請者の本人確認も行う。	事前	保険証廃止のため
	Ⅲ　2リスク2 特定個人情報の正確性確保の措置の内容	【他部署からの情報入手】 ・住民の情報については、住民基本台帳システムから	【他部署からの情報入手】 ・住民の情報については、住民記録システムから		
	Ⅲ　2リスク3 リスクに対する措置の内容	【他部署からの情報入手】 ・事務を行う上で従事者からの予防接種台帳管理システムへのアクセスは	【他部署からの情報入手】 ・事務を行う上で従事者からの予防接種台帳管理システム・保健管理システム（標準準拠）へのアクセスは	事前	システム追加に伴う修正
	Ⅲ　2リスク3 入手の際の本人確認の措置の内容	本人確認を保険証、母子手帳、運転免許証、個人番号カード等で行う。	本人確認を母子手帳、運転免許証、個人番号カード等で行う。	事前	保険証廃止のため
	Ⅲ　3リスク1 事務で使用するその他のシステムにおける措置の内容	予防接種台帳管理システムにおいて使用する端末は、他のシステム（保健衛生システム、結核登録者情報システム）との共用端末であるが、予防接種事務を担当する職員が使用できるのは、予防接種台帳管理システムのみに限られている。	予防接種台帳管理システム・保健管理システム（標準準拠）において使用する端末は、他のシステム（保健衛生システム、結核登録者情報システム）との共用端末であるが、予防接種事務を担当する職員が使用できるのは、予防接種台帳管理システム・保健管理システム（標準準拠）のみに限られている。	事前	システム追加に伴う修正
	Ⅲ　3リスク2 具体的な管理方法	＜予防接種台帳管理システムにおける措置＞	＜予防接種台帳管理システム・保健管理システム（標準準拠）における措置＞	事前	システム追加に伴う修正
	Ⅲ　4 特定個人情報の提供ルール：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	・委託先へ特定個人情報ファイルを提供することはなく、特定個人情報を取扱う作業を行う場合は感染症対策課内設置端末を利用するなど、特定の作業場所で行うこととしている。	・委託先へ特定個人情報ファイルを提供することはなく、特定個人情報を取扱う作業を行う場合は感染症対策課内設置端末又は入退室を制限した部屋の端末を利用するなど、特定の作業場所で行うこととしている。	事前	システム追加に伴う修正
	Ⅲ　6リスク1 リスクに対する措置の内容	＜予防接種台帳管理システムにおける措置＞	＜予防接種台帳管理システム・保健管理システム（標準準拠）における措置＞	事前	システム追加に伴う修正
	Ⅲ　6リスク1 リスクに対する措置の内容	＜中間サーバ・ソフトウェアにおける措置＞ ・・・ （※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。	＜中間サーバ・ソフトウェアにおける措置＞ ・・・ （※2）番号法第19条第8号に基づく主務省令第2条の表に基づき、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。	事前	システム追加に伴う修正
	Ⅲ　6リスク5 リスクに対する措置の内容	＜予防接種台帳管理システムにおける措置＞ ①情報提供ネットワークシステムにおける情報連携においては、中間サーバーに保有されている情報のみが連携されることになっており、予防接種台帳管理システムが保有する情報が全て連携されるわけではない。 ②中間サーバーに保有される特定個人情報は、番号法の規定に基づき定められた情報のみとなっており、不正な提供が行われるリスクに対応している。 ③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。 ※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。	＜予防接種台帳管理システム・保健管理システム（標準準拠）の運用における措置＞ ①情報提供ネットワークシステムにおける情報連携においては、中間サーバに保有されている情報のみが連携されることになっており、中間サーバに保有される特定個人情報は、番号法の規定に基づき定められた情報のみとなっていることから、不正に提供されるリスクに対応している。 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。 ※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。	事前	システム追加に伴う修正

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　6リスク5 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、中間サーバーにも格納して、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。	＜中間サーバ・ソフトウェアにおける措置＞ ①②③＜予防接種台帳管理システム・保健管理システム（標準準拠）の運用における措置＞と同様 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。	事前	システム追加に伴う修正
	Ⅲ　6リスク7 リスクに対する措置の内容	－	＜予防接種台帳管理システム・保健管理システム（標準準拠）の運用における措置＞ ①情報提供ネットワークシステムにおける情報連携においては、中間サーバに保有されている情報のみが連携されることになっており、中間サーバに保有される特定個人情報は、番号法の規定に基づき定められた情報のみとなっていることから、誤った情報の提供が行われるリスクに対応している。	事前	システム追加に伴う修正
	Ⅲ　7リスク1 ⑤物理的対策	－	＜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。 ＜保健管理システム（標準準拠）における措置＞ ・保健管理システム（標準準拠）はガバメントクラウド上で稼働するため、「ガバメントクラウドにおける措置」に記載のとおり。	事前	システム追加に伴う修正
	Ⅲ　7リスク1 ⑥技術的対策	－	＜ガバメントクラウドにおける措置＞ 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」（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。	事前	システム追加に伴う修正

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　7リスク1 ⑥技術的対策	―	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。 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。 ＜保健管理システム（標準準拠）における措置＞ ・保健管理システム（標準準拠）はガバメントクラウド上で稼働するため、「ガバメントクラウドにおける措置」に記載するとおり	事前	システム追加に伴う修正
	Ⅲ　7リスク2 リスクに対する措置の内容	・＜予防接種台帳管理システム＞ ・住民基本台帳システムと連携し	＜予防接種台帳管理システム・保健管理システム（標準準拠）における措置＞ ・住民記録システムと連携し	事前	システム追加に伴う修正
	Ⅲ　7リスク3 消去手順	―	・データについては、保管期間満了後、システムにてデータベースより削除する。 ・ガバメントクラウドにおいては、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、NIST800-88、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。	事前	システム追加に伴う修正
	Ⅳ　1②監査	―	＜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。	事前	システム追加に伴う修正
	Ⅳ　3その他のリスク対策	―	＜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。	事前	システム追加に伴う修正
	Ⅵ　1基礎項目評価	―	①（公表日を記載予定） ②基礎項目評価及び全項目評価の実施が義務付けられる	事後	
	Ⅵ　2国民・住民等からの意見の聴取	―	（意見公募実施後に記載予定） ① ② ③ ④ ⑤	事後	
	Ⅵ　3第三者点検	―	（第三者点検実施後に記載予定） ① ②大阪市個人情報保護審議会へ諮問 ③	事後	

（別添２） 特定個人情報ファイル記録項目

住民基本台帳	市区町村番号	行政区番号	外国人フラグ
	整理番号	番地	外国人国籍
	履歴番号	枝番	住民となった日
	カナ氏名	小枝	住民でなくなった日
	漢字氏名	郵便番号	最新異動区分
	本名カナ氏名	集配局	最新異動日
	本名漢字氏名	住所	最新異動届出日
	通称カナ氏名	方書	住民異動区分
	通称漢字氏名	続柄１	住民異動日
	アルファベット氏名	続柄２	取消区分
	漢字併記カナ氏名	続柄３	転入前住所
	漢字併記氏名	続柄４	転入前方書
	氏名利用区分	世帯番号	転出後住所
	生年月日	世帯主カナ氏名	転出後方書
	性別	世帯主漢字氏名	補記論理和
	町番号	住登外区分	連携処理日
住民基本台帳付帯情報	電話番号	世帯課税区分	障害手帳区分
	個人課税区分	被災者区分	送付除外論理和
予防接種結果（小児）	整理番号	接種量	抽出時方書
	接種名称区分	印刷区分	抽出時行政区番号
	期回数区分	印刷日	抽出時漢字氏名
	履歴番号	発注日	抽出時カナ氏名
	年度	予診理由区分	抽出時補記論理和
	事業予定連番	接種補足区分	抽出時生保区分
	接種日	ワクチンメーカー区分	抽出キー
	接種種別区分	支払対象外フラグ	抽出フラグ
	登録日	警告内容	印刷連番
	接種医療機関番号	登録支所区分	請求年月
	接種医療機関番号その他	抽出日	経過措置
	接種区分	抽出時郵便番号	調整理由
	Lot番号	抽出時住所	
予防接種結果（インフルエンザ）	履歴番号	接種区分	自己負担免除理由
	カナ氏名	年度	医療機関施設区分
	性別	接種日	支払対象外フラグ
	生年月日	登録日	請求年月
	接種名称区分	区区分	調整理由
	期回数区分	Lot番号	

（別添２） 特定個人情報ファイル記録項目

予防接種結果 （高齢者肺炎球菌）	整理番号	印刷区分	抽出時郵便番号
	履歴番号	印刷日	抽出時住所
	接種名称区分	発注日	抽出時方書
	期回数区分	予診理由区分	抽出時行政区番号
	年度	ワクチンメーカー区分	抽出時漢字氏名
	接種日	支払対象外フラグ	抽出時カナ氏名
	登録日	請求年月	抽出時補記論理和
	負担金区分	登録支所区分	抽出時生保区分
	接種医療機関番号	抽出キー	抽出フラグ
	接種医療機関番号その他	印刷連番	自己負担免除理由
	接種区分	警告内容	調整理由
	Lot番号	免除区分	
	接種量	抽出日	
予防接種結果 （コロナウイルス） 臨時接種分	接種名称	印刷区分	抽出時住所
	期・回数	印刷日	抽出時方書
	履歴番号	発送日	抽出時行政区番号
	年度	予診理由	抽出時漢字氏名
	接種日	接種補足	抽出時カナ氏名
	登録日	ワクチンメーカー	抽出時補記論理和
	医療機関番号	ワクチン名	抽出時生保区分
	医療機関	支払対象外フラグ	抽出キー
	接種種別	警告内容	抽出フラグ
	接種区分	登録支所	印刷連番
	Lot番号	抽出日	備考
	接種量	抽出時郵便番号	
予防接種結果 （コロナウイルス） 定期接種分	接種名称区分	期回数区分	接種区分
	支払対象外フラグ	登録日	請求年月
	年度	接種日	接種医療機関番号
	医療機関	登録支所	免除区分
	Lot番号	接種量	ワクチンメーカー
	予診理由区分	接種補足	警告内容
	備考	自己負担免除理由	

（別添２） 特定個人情報ファイル記録項目

統合基盤システム （団体内宛名）	個人番号	統合宛名番号	氏名（漢字）
	氏名（カナ）	住所	生年月日
	性別	業務システム固有宛名番号	異動事由
	識別項目１	識別項目２	識別項目３
	識別項目４	登録日時	更新日時
中間サーバー （中間サーバー）	情報提供用個人識別符号	情報提供記録	