

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
23	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

吹田市は、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あたり、そ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うることを認識し、特定個人情報の漏えいその他の事態が発生するリスクを軽減させるため、番号法及び個人情報保護に関する法令を遵守するとともに、特定個人情報ファイルの保護と安全な利用について適切な措置を実施することで、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

吹田市長

個人情報保護委員会 承認日【行政機関等のみ】

公表日

令和3年11月29日

項目一覧

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

⑧使用方法 ※		<ul style="list-style-type: none"> ・予防接種予診票を発行するため使用する ・予防接種記録をシステムに入力し、予防接種台帳を更新するため使用する ・予防接種毎の対象者や未接種者を抽出するため使用する ・本人からの問い合わせの対応に使用する <p><新型コロナウイルス感染症対策に係る予防接種事務></p> <ul style="list-style-type: none"> ・本市への転入者について、転出元市区町村へ接種記録を照会するために特定個人情報を使用する。 ・本市からの転出者について、転出先市区町村へ本市での接種記録を提供するために特定個人情報を提供する。 ・新型コロナウイルス感染症予防接種証明書の交付の際、接種記録を照会するために特定個人情報を提供する。
	情報の突合 ※	<ul style="list-style-type: none"> ・予防接種実施医療機関から提出された予診票に記載されている予防接種を受けた者の情報と、健康情報管理システムで保有する対象者の情報との突合を行うことにより、予防接種を受けた者を正確に把握する。 ・本市が実施する予防接種に起因する健康被害救済の給付について、支給を受ける者が請求する際の手続きに関して、本人から提出された予防接種健康被害救済の申請情報と、健康管理システムで保有する対象者の情報との突合を行うことにより、対象者を正確に把握する。 <p><新型コロナウイルス感染症対策に係る予防接種事務></p> <ul style="list-style-type: none"> ・本市からの転出者について、本市での接種記録を転出先市区町村に提供するため、転出先市区町村から個人番号を入手し、本市の接種記録と突合する。 (転出先市区町村にて、本人から個人番号の提供に関して同意が得られた場合のみ当処理を行う)
	情報の統計分析 ※	個人番号を用いた統計分析は行わない。(新型コロナウイルス感染症対策に係る予防接種事務を含む)
	権利利益に影響を与え得る決定 ※	該当なし
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 ※	<input type="checkbox"/> 委託する <input type="checkbox"/> 委託しない (5) 件	
委託事項1	健康情報管理システム(予防接種情報管理)の運用・保守業務、法制度改正に伴う改修業務	
①委託内容	システム運用・保守業務、法制度改正に伴うシステム改修	
②取扱いを委託する特定個人情報ファイルの範囲	<input type="checkbox"/> 特定個人情報ファイルの全体 <input type="checkbox"/> 特定個人情報ファイルの一部 <input type="checkbox"/> 10万人以上100万人未満 <input type="checkbox"/> 1万人未満 <input type="checkbox"/> 1万人以上10万人未満 <input type="checkbox"/> 10万人以上100万人未満 <input type="checkbox"/> 100万人以上1,000万人未満 <input type="checkbox"/> 1,000万人以上	
対象となる本人の数	<input type="checkbox"/> 10万人以上100万人未満 <input type="checkbox"/> 1万人未満 <input type="checkbox"/> 1万人以上10万人未満 <input type="checkbox"/> 10万人以上100万人未満 <input type="checkbox"/> 100万人以上1,000万人未満 <input type="checkbox"/> 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	正確な予防接種事務遂行のため、接種対象者の特定及び接種履歴の管理、勧奨を行う必要があるため。 また、予防接種を受けたことに起因する健康被害救済に係る給付の支給に関する事務を行うため。	
③委託先における取扱者数	<input type="checkbox"/> 10人以上50人未満 <input type="checkbox"/> 10人以上50人未満 <input type="checkbox"/> 50人以上100人未満 <input type="checkbox"/> 100人以上500人未満 <input type="checkbox"/> 500人以上1,000人未満 <input type="checkbox"/> 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 [<input checked="" type="checkbox"/>] その他 (管理区域にてシステムを直接操作)
⑤委託先名の確認方法		委託先が決定した際には、ホームページに公表
⑥委託先名		株式会社両備システムズ
再委託	⑦再委託の有無 ※	[再委託しない] <input checked="" type="checkbox"/> <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		健康情報管理システム(予防接種情報管理)のうち共通基盤部分の構築・運用業務
①委託内容		健康情報管理システム(予防接種情報管理)のうち共通基盤部分の構築・運用業務の委託
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一部] <input checked="" type="checkbox"/> <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] <input checked="" type="checkbox"/> <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	システムの構築・運用業務においては、システムに関するファイル全体を取り扱うため
③委託先における取扱者数		[10人未満] <input checked="" type="checkbox"/> <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 [<input checked="" type="checkbox"/>] その他 (管理区域にてシステムを直接操作)
⑤委託先名の確認方法		委託先が決定した際には、ホームページに公表
⑥委託先名		日本電気株式会社
再委託	⑦再委託の有無 ※	[再委託する] <input checked="" type="checkbox"/> <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	再委託の制限事項内で本市が認める場合、委託先からの書面による申請に基づき、許諾
	⑨再委託事項	健康情報管理システムのうち共通基盤部分の構築・運用業務の一部

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 [<input checked="" type="radio"/>] 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 [<input checked="" type="radio"/>] その他 (管理区域にてシステムを直接操作)
⑤委託先名の確認方法		下記、「⑥委託者名」の項の記載より確認できる。
⑥委託先名		株式会社アイ・オー・プロセス
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5		ワクチン接種記録システム(VRS)運用業務
①委託内容		新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム(VRS)を用いた特定個人情報ファイルの管理等業務
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一部] <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 ※	予防接種法等関連法令に定められる予防接種の対象者
	その妥当性	ワクチン接種記録システム(VRS)を用いた特定個人情報ファイルの適切な管理等のために取り扱う必要がある。
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 [<input checked="" type="radio"/>] その他 (LG-WAN回線を用いた提供)
⑤委託先名の確認方法		下記、「⑥委託者名」の項の記載より確認できる。
⑥委託先名		株式会社ミラボ
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	

6. 特定個人情報の保管・消去

<p>①保管場所 ※</p>	<p><吹田市における措置></p> <ul style="list-style-type: none"> ・入退室管理区域内に設置するサーバ内に保管する。管理区域については、入室権限を持つ者を限定し、入退室管理カードにより権限の有無の確認し、入室者名と時刻を記録するなど入退室管理を行っている。 ・届出書等について、保管年限内は鍵付の文書保管倉庫内での保管を義務付けている。 ・文書保管倉庫の最終退出者は、退出時に施錠を行っており、外部の者が入室できないようにしている。 <p><中間サーバ・プラットフォームにおける措置></p> <ul style="list-style-type: none"> ・中間サーバ・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバ室への入室を厳重に管理する。 ・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。 <p><ワクチン接種記録システム(VRS)における追加措置></p> <p>ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用している。</p> <p>なお、以下のとおりセキュリティ対策を講じている。</p> <ul style="list-style-type: none"> ・論理的に区分された本市の領域のデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。 ・日本国内にデータセンターが存在するクラウドサービスを利用している。 				
<p>②保管期間</p>	<table border="1"> <tr> <td data-bbox="328 871 467 1034"> <p>期間</p> </td> <td data-bbox="467 871 1520 1034"> <p><選択肢></p> <p>1) 1年未満 2) 1年 3) 2年</p> <p>4) 3年 5) 4年 6) 5年</p> <p>7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上</p> <p>10) 定められていない</p> </td> </tr> <tr> <td data-bbox="328 1034 467 1106"> <p>その妥当性</p> </td> <td data-bbox="467 1034 1520 1106"> <p>予防接種法施行令第6条の2の規定により、5年間の保存が必要とされている。</p> </td> </tr> </table>	<p>期間</p>	<p><選択肢></p> <p>1) 1年未満 2) 1年 3) 2年</p> <p>4) 3年 5) 4年 6) 5年</p> <p>7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上</p> <p>10) 定められていない</p>	<p>その妥当性</p>	<p>予防接種法施行令第6条の2の規定により、5年間の保存が必要とされている。</p>
<p>期間</p>	<p><選択肢></p> <p>1) 1年未満 2) 1年 3) 2年</p> <p>4) 3年 5) 4年 6) 5年</p> <p>7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上</p> <p>10) 定められていない</p>				
<p>その妥当性</p>	<p>予防接種法施行令第6条の2の規定により、5年間の保存が必要とされている。</p>				
<p>③消去方法</p>	<p><吹田市における措置></p> <ul style="list-style-type: none"> ・国が指定する保存期間の経過後は、必要に応じて委託先事業者のSE作業にて削除を行う。 ・ディスク交換やハード更改等の際は、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。 <p><中間サーバ・プラットフォームにおける措置></p> <ul style="list-style-type: none"> ・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。 ・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。 <p><ワクチン接種記録システム(VRS)における追加措置></p> <ul style="list-style-type: none"> ・自機関の領域に保管されたデータのみ、ワクチン接種記録システム(VRS)を用いて消去することができる。 ・自機関の領域に保管されたデータは、他機関から消去できない。 <p>※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、消去することができない。</p>				

7. 備考

(別添2) 特定個人情報ファイル記録項目

基本情報	乳幼児接種	高齢者インフルエンザ	高齢者肺炎球菌	風しん第5期
宛名番号	接種日	西暦年度	西暦年度	西暦年度
世帯番号	接種コード	接種日	接種日	接種日
カナ氏名 a	接種回数	接種日年齢	接種日年齢	接種日年齢
漢字氏名	接種日年齢	年度末年齢	年度末年齢	年度末年齢
通称カナ氏名	年度末年齢	基準日年齢	基準日年齢	基準日年齢
通称氏名	基準日年齢	請求月	請求月	クーポン
生年月日	対象外判定	実施医療機関	実施医療機関	請求月
性別	接種判定	接種判定	接種判定	実施医療機関
続柄	混合接種何種	LotNo	LotNo	接種（実施）判定
電話番号	請求月	接種量	接種量	LotNo
郵便番号	実施医療機関	65歳未満接種理由	65歳未満接種理由	接種量
住所	LotNo	未接種理由	未接種理由	65歳未満接種理由
方書	接種量	予診フラグ	予診フラグ	未接種理由
転入前住所	実施区分	特記事項	特記事項	予診フラグ
転出後住所	予診フラグ	他市依頼区分	他市依頼区分	特記事項
送付用郵便番号	他市依頼区分	接種日住民区分	接種日住民区分	他市依頼区分
送付用住所	接種日住民区分	特記事項	特記事項	接種日住民区分
送付用方書	特記事項			抗体検査方法
	B型肝炎ワクチン区分			抗体価
				抗体価単位
				抗体検査判定結果
				抗体検査番号
				抗体価範囲
				特記事項

新型コロナウイルス感染症対策に係る予防接種に関する記録項目

個人番号	接種会場	ワクチン種類（※）	証明書発行年月日（※）
宛名番号	接種状況（実施/未実施）	製品名（※）	
自治体コード	接種回（1回目/2回目）	旅券関係情報（旧姓・別姓・別名・ローマ字氏名・国籍・旅券番号）（※）	
接種券番号	接種日		
属性情報（氏名、生年月日、性別）	ワクチンメーカー		
	ロット番号	証明書ID（※）	

（※） 新型コロナウイルス感染症予防接種証明書の交付に必要な場合のみ

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	
予防接種情報管理ファイル	
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	<p>【窓口等での入手における措置】</p> <ul style="list-style-type: none"> 情報の入手の際には、届出窓口において、本人確認書類（身分証明書）の提示を求めるなどにより、厳格に本人確認を行う。 届出内容等については、複数の職員が確認し、対象者以外の情報の入手を防止する。 <p>【システムにおける措置】</p> <ul style="list-style-type: none"> 職員に配置される端末はユーザIDによる識別とパスワードによる認証を用いて起動するものとしている。 健康情報管理システムを利用する必要がある職員を特定し、ユーザIDによる識別及び生体認証を用いての利用とすることで端末が不正に利用されることを防いでいる。 システム上での庁内連携により特定個人情報を入手する場合、いつ、誰が、何のために（どの業務のために）入手したかの操作履歴（ログ）をシステム上で保存している。 <p>【予防接種業務委託医療機関における措置】</p> <ul style="list-style-type: none"> 予防接種を実施する委託医療機関において、母子手帳等により本人確認を行い対象者以外の情報を入手することがないように努めている。 委託医療機関から提出された予診票を健康情報管理システムに取込む際に予診票に記載の内容とシステムで保有する住民情報を突合し、正確なマッチングを行ったうえで取込を実施する。 <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置></p> <ul style="list-style-type: none"> 転入者本人からの個人番号の入手 本市の転入者について、転出元市区町村へ接種記録を照会するために個人番号を入手する際は、新接種券発行申請書兼接種記録確認同意書等により本人同意を取得し、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 転出先市区町村からの個人番号の入手 本市からの転出者について、本市での接種記録を転出先市区町村へ提供するために、転出先市区町村から個人番号を入手するが、その際は、転出先市区町村において、本人同意及び本人確認が行われた情報だけをワクチン接種記録システム（VRS）を通じて入手する。 新型コロナウイルス感染症予防接種証明書の交付申請者からの個人番号の入手 接種者について、新型コロナウイルス感染症予防接種証明書の交付のために個人番号を入手するのは、接種者からの接種証明書の交付申請があった場合のみとし、さらに、番号法第16条に基づき、本人確認書類を確認することで、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	<ul style="list-style-type: none"> 対象者から情報を入手する際は所定の様式を用いることで予防接種事務に必要な情報以外を入手することを防止する。 庁内連携による住民情報等の入手にあたっては、データ連携項目を必要最小限に留め、不要な項目の取得を行わない設計にすることで不要項目取得のリスクを回避している。
その他の措置の内容	—
リスクへの対策は十分か	<p>[十分である]</p> <p><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</p>
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	<ul style="list-style-type: none"> 健康情報管理システムを利用する必要がある職員については、個人ごとにユーザID・パスワード・生体情報認証を設定し、厳密に管理している。そのうえでさらに、予防接種情報については担当職員のみアクセス権限を付与しており、不適切な方法での情報入力・更新ができないよう対策を行っている。 <p><ワクチン接種記録システム（VRS）における追加措置></p> <ul style="list-style-type: none"> ワクチン接種記録システム（VRS）のデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようにアクセス制御している。
リスクへの対策は十分か	<p>[十分である]</p> <p><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</p>
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	本人確認書類（運転免許証、個人番号カード、健康保険証、母子手帳等）の提示を受け、確認を行う。
個人番号の真正性確認の措置の内容	通知カード（番号法第7条）、個人番号カード（同法第17条）の提示や、住民基本台帳ネットワークシステム内の情報の確認などにより、個人番号の真正性を確認する。
特定個人情報の正確性確保の措置の内容	情報の入力を行う際は、正確性を確保するため、入力者とは別の職員が必ず点検する。
その他の措置の内容	—
リスクへの対策は十分か	<p>[十分である]</p> <p><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</p>

リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	<p>【窓口等での入手における措置】</p> <ul style="list-style-type: none"> ・受付窓口は、衝立により間仕切りを行い、のぞき見防止のための措置を行っている。 ・届出書等については、入力及び照合した後は、鍵付の書庫に保管する。 <p>【健康情報管理システムにおける措置】</p> <ul style="list-style-type: none"> ・健康情報管理システムを利用する必要がある職員を特定し、ユーザIDによる識別と生体認証による認証を実施している。 ・アクセス権限の発効・失効の管理 識別情報(ユーザID/パスワード)の発行・更新・廃棄は、人事異動や退職時など、あらかじめ定められたルールに基づいて随時行っている。 健康情報管理システムにアクセスする職員へのアクセス権限は定期的に見直しを行い、指定した職員のみがアクセスできるようにしている。 ・アクセス権限の管理 アクセス可能なユーザIDは必要最小限とし、漏えい等が発生しないように厳重に管理している。 ユーザIDについては、定期的にチェックを行い不要なIDが使用不可になっているかを確認している。 また、利用期間が明確になったものについては、ユーザIDに有効期限を設定し、期限到来により自動的に失効するようにしている。 ・特定個人情報の使用の記録 ユーザIDとともに、健康情報管理システムへのアクセス、操作(登録、更新、印刷、外部媒体への出力等)のアクセス記録をログとして保管している。 上記アクセス記録について、確認が必要となった場合には即座に確認できる仕組みを準備している。 <p><ワクチン接種記録システム(VRS)における追加措置></p> <ul style="list-style-type: none"> ・入手する特定個人情報については、情報漏えいを防止するために、暗号化された通信回線を使用する。
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	
<ワクチン接種記録システム(VRS)における追加措置> ・入手した特定個人情報については、限定された端末を利用して国から配布されたユーザIDを使用し、ログインした場合だけアクセスできるように制御している。	
3. 特定個人情報の使用	
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク	
宛名システム等における措置の内容	<p>【健康情報管理システムにおける措置】</p> <ul style="list-style-type: none"> ・健康情報管理システムには、当該事務に関係のない情報を保有しない。 ・健康情報管理システムの機能以外からは、個人番号にアクセスできないようアクセス制御を行っている。 ・特定個人情報ファイルには、適切な権限がある担当者のみがアクセスできるよう設計されている。 また、適切な権限がある担当者からのアクセスであっても個人番号を表示する必要がない業務(機能)からのアクセスについては、個人番号を画面表示しない設計としている。 ・特定個人情報を使用できる事務については、業務マニュアルに記載し、定期的に職員研修を実施している。 <p>【団体内統合宛名システムにおける措置】</p> <ul style="list-style-type: none"> ・団体内統合宛名システムでは、個人番号関連業務以外は個人番号にアクセスできないよう、個人番号利用事務以外で個人番号の検索を行うことはできない。 ・団体内統合宛名システムの稼働するLANでは、外部からの侵入ができないようファイアウォールによる適切なアクセス制御を実施している。
事務で使用するその他のシステムにおける措置の内容	<p>特定個人情報を保有しない事務に関するシステムでは、特定個人情報との紐付けができないようアクセス制御する。</p> <p><ワクチン接種記録システム(VRS)における追加措置></p> <ul style="list-style-type: none"> ・接種会場等では、接種券番号の読取端末(タブレット端末)からインターネット経由でワクチン接種記録システム(VRS)に接続するが、個人番号にはアクセスできないよう制御している。
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	<ul style="list-style-type: none"> 健康情報管理システムを利用する必要がある職員を特定し、ユーザIDによる識別と生体認証による認証を実施している。 アクセス権限の発効・失効の管理 識別情報(ユーザID/パスワード)の発行・更新・廃棄は、人事異動や退職時など、あらかじめ定められたルールに基づいて随時行っている。 健康情報管理システムにアクセスする職員へのアクセス権限は定期的に見直しを行い、指定した職員のみがアクセスできるようにしている。 アクセス権限の管理 アクセス可能なユーザIDは必要最小限とし、漏えい等が発生しないように厳重に管理している。 ユーザIDについては、定期的にチェックを行い、不要なIDが使用不可になっているかを確認している。 また、利用期間が明確になったものについては、ユーザIDに有効期限を設定し、期限到来により自動的に失効するようにしている。 特定個人情報の使用の記録 ユーザIDとともに、健康情報管理システムへのアクセス、操作(登録、更新、印刷、外部媒体への出力等)のアクセス記録をログとして保管している。 上記アクセス記録について、確認が必要となった場合には即座に確認できる仕組みを準備している。 <p><ワクチン接種記録システム(VRS)における追加措置> 権限のない者によって不正に使用されないよう、以下の対策を講じている。</p> <ul style="list-style-type: none"> ワクチン接種記録システム(VRS)における特定個人情報へのアクセスは、LG-WAN端末による操作に限り可能になるように制御している。 LG-WAN端末は、限定された者しかログインできる権限を保持しない。 ワクチン接種記録システム(VRS)におけるログイン認証は、ユーザID・パスワードにて行う。 ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国に対してユーザ登録を事前申請した者に限定して発行される。
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	<ul style="list-style-type: none"> 職員には、所属長の申請に基づき、ユーザIDを発行し、一元管理する。 職員には、担当業務に必要な範囲で、アクセス権限を付与する。 退職職員のユーザIDは、速やかに失効させる。 アクセス権限の定期的な確認を行い、人事異動に合わせて権限の見直しを行う。 <p><ワクチン接種記録システム(VRS)における追加措置> ・ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国に対してユーザ登録を事前申請した者に限定して発行される。</p>
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	<ul style="list-style-type: none"> 操作者の担当業務に応じて、必要な範囲のアクセス権限を付与する。 共有IDは禁止し、個人に対してIDを発行する。 <p><ワクチン接種記録システム(VRS)における追加措置> ・ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国に対してユーザ登録を事前申請した者に限定して発行される。</p>
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	<ul style="list-style-type: none"> システムの操作ログとして、処理日時、職員情報、処理内容などを記録している。 システムの操作ログは、一定期間保存し、必要に応じて解析する。 <p><ワクチン接種記録システム(VRS)における追加措置> ・システム上の操作のログを取得しており、操作ログを確認できる。</p>
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	<ul style="list-style-type: none"> 職員の業務外でのシステムへのアクセスを禁止するとともに、システムの操作ログを記録する。 事務外利用の禁止について、職員への研修において徹底する。
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	<ul style="list-style-type: none"> 健康情報管理システムの端末では、許可なく外部記憶媒体の利用及び他のネットワークへのデータ移転はできないように制御する。 システムの運用管理について権限を有する操作者によるバックアップデータ以外に、特定個人情報保護ファイルの複製はできないように権限を管理する。 <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置> 住民基本台帳システムや健康情報管理システムから特定個人情報を抽出したCSVファイルをワクチン接種記録システム(VRS)へ登録する際には、以下のようにしている。</p> <ul style="list-style-type: none"> 作業を行う職員及び端末を必要最小限に限定する。 作業に用いる電子記録媒体については、不正な複製、持ち出し等を防止するために、許可された専用の外部記録媒体を使用する。また、媒体管理簿等に仕様の記録を記載する等、利用履歴を残す。 作業に用いる電子記録媒体の取扱いについては、承認を行い、当該承認の記録を残す。 電子記録媒体に格納するデータについては、暗号化やパスワード設定を行う。 電子記録媒体による作業を終了したら、内部のデータを確実に消去する。管理簿に消去の記録を記載する等、消去履歴を残す。
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	
<ul style="list-style-type: none"> 担当職員には離席時のログオフを義務づける。 一定時間操作が行われない場合は、スクリーンセーバーの自動起動設定により、端末画面上の個人情報を保護する。 <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ①特定個人情報を使用する場面を必要最小限に限定している。具体的には以下の3つの場面に限定している。</p> <ul style="list-style-type: none"> 本市への転入者について、転出元市区町村へ接種記録を照会するために、転入者本人から個人番号の提供の同意が得られた場合のみ入手し、使用する。 本市からの転出者について、本市での接種記録を転出先市区町村へ提供するために、個人番号を入手し、使用する。 接種者について、新型コロナウイルス感染症予防接種証明書の交付申請があった場合に、接種記録を照会するために、個人番号を入手し、使用する。 <p>②ワクチン接種記録システム(VRS)からCSVファイルにてダウンロードする接種記録データには、個人番号が含まれない。</p>	
4. 特定個人情報ファイルの取扱いの委託 [] 委託しない	
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク	
情報保護管理体制の確認	<ul style="list-style-type: none"> 健康情報管理システムの構築業務委託先事業者選定の際は情報セキュリティマネジメントシステム(ISO27001)認証またはプライバシーマーク認証を取得していること及び過去の類似業務履行実績等の確認を行い、適切な情報保護管理体制を確保できる事業者であるか確認したうえで選定している。 健康情報管理システムの運用、保守等の委託にあたっては、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結している。 <ul style="list-style-type: none"> 情報セキュリティポリシー及び情報セキュリティ実施手順の遵守 委託先の責任者、委託内容、作業、作業場所の特定 提供されるサービスレベルの保証 従業員に対する教育の実施 提供された情報の目的外利用及び受託者以外の者への提供の禁止 業務上知り得た情報の守秘義務 再委託に関する制限事項の遵守 委託業務終了時の情報資産の返還、廃棄等 委託業務の定期報告及び緊急時報告義務 情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等) 市による監査、検査 システムの運用を開始する前に、吹田市情報セキュリティ部会にて、特定個人情報の管理やシステムの運用体制、技術的なセキュリティ対策等について審査を行う。 <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置> 本市、国、当該システムの運用保守事業者の三者の関係で規定した「ワクチン接種記録システムの利用にあたっての確認事項(規約)」に同意することにより、当該確認事項に基づきワクチン接種記録システム(VRS)に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。</p> <p>なお、次の内容については、当該確認事項に規定されている。</p> <ul style="list-style-type: none"> 特定個人情報ファイルの閲覧者・更新者の制限 特定個人情報ファイルの取扱いの記録 特定個人情報の提供ルール/消去ルール 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 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

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	<ul style="list-style-type: none"> ・委託先の業務担当者名簿の提出を求め、その中から必要最小限の範囲の担当者にアクセス権限を付与することにより、特定個人情報ファイルの閲覧者・更新者を制限する。 ・各担当職員には、業務のため必要な範囲のアクセス権限を付与する。
特定個人情報ファイルの取扱いの記録	[記録を残している] <選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	<ul style="list-style-type: none"> ・システムの操作ログとして、処理日時、職員情報、処理内容などを記録している。 ・システムの操作ログは、一定期間保存し、必要に応じて解析する。
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	<ul style="list-style-type: none"> ・委託先から他者への提供は原則として認めていない。 ・情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明している。 ・必要に応じて本市は現地調査・確認を行えることとしている。
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	<ul style="list-style-type: none"> ・健康情報管理システムの運用・保守等の委託にあたり、個人情報を含む作業の実施場所は原則として本市の管理区域内のみとし、データの外部への持ち出しは認めていない。したがって、通常、本市サーバ内の特定個人情報の操作がその範囲であるため、操作ログによりルール遵守状況を確認できる。 ・特別な事情により、情報(複製を含む。)の保管場所からの移動又は管理区域外への持出しが業務上必要となったときは、移動については管理責任者、持出しについては統括管理者の許可を得なければならない。 ・バックアップデータの遠隔地保管の場合、施錠した手提金庫の中へデータを記録した電子記録媒体を保管して提供する。 その際、日付及び件数を記録し、委託元と委託先の双方が確認し押印する。
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	<ul style="list-style-type: none"> ・契約終了等に伴い、特定個人情報データを廃棄する場合は、記録媒体を初期化するとともに、復元不可能な状態になるよう適切な措置を施し、処理日時、処理内容等を記録する。 ・委託先から任意の様式により消去結果に係る報告書を提出させる。 ・必要に応じて本市は現地調査・確認を行えることとしている。
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	<p>委託契約書に、以下の措置をとる旨を規定する。</p> <ul style="list-style-type: none"> ・秘密保持義務 ・事業所内からの特定個人情報の持ち出しの禁止 ・特定個人情報の目的外利用の禁止 ・再委託における条件 ・漏えい事案等が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の返却又は廃棄 ・特定個人情報を取り扱う従業員の明確化 ・従業者に対する監督・教育 ・必要があると認めるときは実地の調査を行うことができる規定等
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	委託者の承諾を得た場合に例外的に再委託を可能としている。その場合は、再委託先は特定個人情報ファイルの取扱い等について、委託先と同様の措置を行うことを義務付けている。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置	
—	

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[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	<ワクチン接種記録システム(VRS)における追加措置> ・ワクチン接種記録システム(VRS)では、他市区町村への提供の記録を取得しており、委託業者から「情報提供等の記録」を入手し、記録の確認をすることができる。	
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	ワクチン接種記録システム(VRS)への提供について、国からの通達や手順に基づき提供を行う。	
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
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	<ワクチン接種記録システム(VRS)における追加措置> 転出元市区町村への個人番号の提出 ・本市への転入者について、転出元市区町村から接種記録を入手するため、転出元市区町村へ個人番号を提供するが、その際は本人同意及び本人確認が行われた情報だけをワクチン接種記録システム(VRS)を用いて提供する。	
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	<ワクチン接種記録システム(VRS)における追加措置> 転出元市区町村への個人番号の提供 ・本市への転入者について、転出元市区町村から接種記録を入手するため、転出元市区町村へ個人番号を提供するが、その際は個人番号とともに転出元の市区町村コードを送信する。そのため、仮に誤った市区町村コードを個人番号とともに送信したとしても、電文を受ける市区町村では該当者がいないため、誤った市区町村に対して、個人番号が提供されない仕組みになっている。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
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		
<ワクチン接種記録システム(VRS)における追加措置> ・特定個人情報の提供は、限定された端末(LG-WAN端末)だけができるように制御している。 ・特定個人情報を提供する場面を必要最小限に限定している。 具体的には、本市への転入者について、転出元市区町村での接種記録を入手するために、転出元市区町村へ個人番号とともに転出元の市区町村コードを提供する場面に限定している。		

6. 情報提供ネットワークシステムとの接続		[] 接続しない(入手)	[] 接続しない(提供)
リスク1: 目的外の入手が行われるリスク			
リスクに対する措置の内容	<p>【健康情報管理システムのソフトウェアにおける措置】</p> <ul style="list-style-type: none"> ・中間サーバへの情報照会処理については、業務システム側で操作ログを記録しており、処理実施者、操作内容を把握可能である。中間サーバコネクタと業務システム間のデータ連携処理についても、業務システム側で処理結果ログを記録しており、データ送受信日時、内容等を把握可能である。 <p>【健康情報管理システムの運用における措置】</p> <ul style="list-style-type: none"> ・権限を持った職員が所属長の承認を得たうえで情報照会・入手を行う。 ・健康情報管理システムで記録している操作ログは、適宜、健康情報管理システムからリストの出力を行い、目的外の入手が行われていないことの確認を行う。 ・定められたルールに基づく入手を職員に周知、徹底を行う。 <p>【中間サーバ・ソフトウェアにおける措置】</p> <ul style="list-style-type: none"> ・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会リスト(※2)との照会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。 ・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。 <p>(※1) 情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。</p> <p>(※2) 番号法別表第2及び第19条第14号に基づき、事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。</p> <p>(※3) 中間サーバを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。</p>		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 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	<p>【健康情報管理システムにおける措置】</p> <ul style="list-style-type: none"> ・中間サーバと健康情報管理システム間は、直接連携をせず中間サーバコネクタを介して連携しており、またサーバ間連携に限定して安全性を確保している。 <p>【中間サーバ・ソフトウェアにおける措置】</p> <ul style="list-style-type: none"> ・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。 <p>【中間サーバ・プラットフォームにおける措置】</p> <ul style="list-style-type: none"> ・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。 ・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	<p>【健康情報管理システムにおける措置】</p> <ul style="list-style-type: none"> ・中間サーバから健康情報管理システムあての情報照会結果の中継では、照会結果内容の改変は行わない。 <p>【中間サーバ・ソフトウェアにおける措置】</p> <ul style="list-style-type: none"> ・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づけられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。 <p>【中間サーバの運用における措置】</p> <ul style="list-style-type: none"> ・中間サーバ接続端末から情報提供を入手し、健康情報管理システムへ登録する場合、複数の職員によるチェックを行い登録する。 		
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4: 入手の際に特定個人情報漏えい・紛失するリスク	
リスクに対する措置の内容	<p>【健康情報管理システムのソフトウェアにおける措置】</p> <ul style="list-style-type: none"> ・中間サーバと健康情報管理システム間は、サーバ間連携に限定して、漏えい・紛失するリスクを排除している。 <p>【健康情報管理システムの運用における措置】</p> <ul style="list-style-type: none"> ・権限を持った職員が所属長の承認を得た上で情報照会・入手を行うこととしている。 ・外部から不正なアクセスがないか、アクセスログ等を確認している。 <p>【中間サーバ・ソフトウェアにおける措置】</p> <ul style="list-style-type: none"> ・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(※)。 ・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。 ・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、特定個人情報漏えい・紛失するリスクを軽減している。 ・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑制する仕組みになっている。 <p>(※)中間サーバは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。</p> <p>【中間サーバ・プラットフォームにおける措置】</p> <ul style="list-style-type: none"> ・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。 ・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。 ・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	<p>[十分である]</p> <p><選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>
リスク5: 不正な提供が行われるリスク	
リスクに対する措置の内容	<p>【健康情報管理システムのソフトウェアにおける措置】</p> <ul style="list-style-type: none"> ・中間サーバへの情報提供処理については、業務システム側で自動送信を行い、かつ、手動送信においても操作ログを記録しており、処理実施者、操作内容を把握可能である。 ・中間サーバコネクタと業務システム間のデータ連携処理についても、業務システム側で処理結果ログを記録しており、データ送受信日時、内容等を把握可能である。 <p>【健康情報管理システムの運用における措置】</p> <ul style="list-style-type: none"> ・健康情報管理システムで記録している操作ログは、適宜、健康情報管理システムからリストの出力を行い、目的外の提供が行われていないことの確認を行う。 <p>【中間サーバ・ソフトウェアにおける措置】</p> <ul style="list-style-type: none"> ・情報提供機能(※)により、情報提供ネットワークシステムにおける照会許可照会リストを情報提供ネットワークシステムから入手し、中間サーバにも格納して、情報提供機能により、照会許可照会リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ・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、特定個人情報不正に提供されるリスクに対応している。 ・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不正に提供されるリスクに対応している。 ・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑制する仕組みになっている。 <p>(※)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</p>
リスクへの対策は十分か	<p>[十分である]</p> <p><選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>

リスク6: 不適切な方法で提供されるリスク	
リスクに対する措置の内容	<p>【健康情報管理システムにおける措置】</p> <ul style="list-style-type: none"> ・情報提供の履歴をすべて保存することで不適切な方法で特定個人情報が提供されることを防止する。 <p>【中間サーバ・ソフトウェアにおける措置】</p> <ul style="list-style-type: none"> ・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。 ・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 <p>(※) 暗号化・復号機能と、鍵情報及び照会許可照会リストを管理する機能</p> <p>【中間サーバ・プラットフォームにおける措置】</p> <ul style="list-style-type: none"> ・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。 ・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。 ・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	<p>[十分である]</p> <p><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</p>
リスク7: 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	<p>【健康情報管理システムにおける措置】</p> <ul style="list-style-type: none"> ・提供する情報に誤りがないかの確認をデータ入力前後に複数人で複数回言い、正確性の担保が取れた時期以降に情報提供を行っている。 <p>【中間サーバ・ソフトウェアにおける措置】</p> <ul style="list-style-type: none"> ・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。 ・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。 ・情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 <p>(※) 特定個人情報を副本として保存・管理する機能</p>
リスクへの対策は十分か	<p>[十分である]</p> <p><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</p>
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	
<p>【中間サーバ・ソフトウェアにおける措置】</p> <ul style="list-style-type: none"> ・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。 <p>【中間サーバ・プラットフォームにおける措置】</p> <ul style="list-style-type: none"> ・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。 ・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。 ・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。 ・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	<p>[政府機関ではない]</p> <p><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</p>
②安全管理体制	<p>[十分に整備している]</p> <p><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</p>
③安全管理規程	<p>[十分に整備している]</p> <p><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</p>

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	<p>[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</p> <p>【吹田市における措置】</p> <ul style="list-style-type: none"> ・サーバ室と、データ、プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する保管室は、他の部屋とは区別して専用の部屋とする。 ・サーバ室と保管室の出入口には機械による入退室を管理する設備を設置し、認証に必要なカードについては貸出簿を作成して管理する。 ・サーバ室と保管室の入退室管理を徹底するため出入口の場所を限定する。 ・事務室内の端末は、ワイヤロックで施錠する。 ・特定個人情報を扱う窓口職員は、特定個人情報を記した書類は机上に放置せず、紛失漏えい不能な保管を行う。 ・特定個人情報を取り扱う職員が離席する際には、ログオフを義務づけ、一定時間操作が行われない場合はスクリーンセーバーの自動起動設定により、端末画面の個人情報を保護する。 ・特定個人情報を保管した媒体の運用ルールを定め、遵守している。 <p>【中間サーバ・プラットフォームにおける措置】</p> <ul style="list-style-type: none"> ・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。 <p><ワクチン接種記録システム(VRS)における措置></p> <p>ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める物理的対策を満たしている。</p> <p>主に以下の対策を講じている。</p> <ul style="list-style-type: none"> ・サーバ設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスを利用している。
⑥技術的対策	<p>[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</p> <p>【吹田市における措置】</p> <ul style="list-style-type: none"> ・不正プログラム対策:コンピュータウイルス監視ソフトを使用し、サーバ・端末双方でウイルスチェックを実施する。 また、新種不正プログラムに対応するために、ウイルスパターンファイルは定期的に更新し、可能な限り最新のものを使用する。 ・不正アクセス対策:本人確認情報の管理について定めた規定に基づき、ネットワーク管理に係る手順等を整備し、ファイアウォール等によりアクセス制御を行う。 <p><中間サーバ・プラットフォームにおける措置></p> <ul style="list-style-type: none"> ・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。 ・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。 <p><ワクチン接種記録システム(VRS)における措置></p> <p>ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める技術的対策を満たしている。</p> <p>主に以下の技術的対策を講じている。</p> <ul style="list-style-type: none"> ・論理的に区分された本市の領域にデータを保管する。 ・当該領域のデータは暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセス防止のため、外部からの侵入検知・通知機能を備えている。 ・LG-WAN端末とワクチン接種記録システムとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。
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	生存者の個人番号の場合と同様の安全管理を実施する中で、特定個人情報を保管している。	
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	住民基本台帳システムとの連携処理を日次で行い、随時最新の情報に更新する。 なお、住民基本台帳システムにおいては、住基法第14条第1項(住民基本台帳の正確な記録を確保するための措置)の規定に基づき調査等を実施することにより、住民基本台帳の正確な記録を担保している。	
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: 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	<選択肢> 1) 定めている 2) 定めていない
手順の内容	<ul style="list-style-type: none"> ・国が指定する保存期間の経過後は、必要に応じて委託先事業者のSE作業にて削除を行う。 ・ディスク交換やハード更改等の際は、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。 	
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	<p>[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</p>
具体的なチェック方法	<p><吹田市における措置> ・年に1回、担当部署において自己点検を実施し、評価書記載事項と運用実態のチェックを行う。</p> <p><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。</p> <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ・内閣官房情報通信技術(IT)総合戦略室から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な監督をする。</p>
②監査	<p>[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</p>
具体的な内容	<p><吹田市における措置> 吹田市情報セキュリティ内部監査実施要領に基づき、以下の観点による内部監査を定期的実施し、監査結果を踏まえて体制や規定を改善する。 ・評価書記載事項と運用実態のチェック ・個人情報保護に関する規定、体制整備 ・個人情報保護に関する人的安全管理措置 ・職員の役割責任の明確化、安全管理措置の周知・教育 ・個人情報保護に関する技術的安全管理措置</p> <p><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。</p> <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ・内閣官房情報通信技術(IT)総合戦略室から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な監督をする。</p>
2. 従業者に対する教育・啓発	
従業者に対する教育・啓発	<p>[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</p>
具体的な方法	<p><吹田市における措置> ・毎年、職員に対し、個人情報保護に関する研修を実施している。(eラーニングを含む) ・毎年、所属内のシステム担当者に対し、教育を実施している。 ・集合教育は必要に応じて実施している。 ・委託事業者に対しては、秘密保持契約を締結し、その中で個人情報保護に関する周知徹底を義務付けている。 ・評価書記載事項と運用実態のチェックを行っている。 ・個人情報保護に関する規定、体制整備 ・個人情報保護に関する人的安全管理措置 ・個人情報保護に関する技術的安全管理措置</p> <p><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。</p> <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ・内閣官房情報通信技術(IT)総合戦略室から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な指導をする。</p>

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。

<新型コロナウイルス感染症対策に係る予防接種事務における追加措置>

- ・内閣官房情報通信技術(IT)総合戦略室から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第7条(情報到達の責任分界点)、第8条(通信経路の責任分界点)、第9条(市区町村の責任)に則し、適切に当該システムを利用し、万が一、障害や情報漏えいが生じた場合、適切な対応をとることができる体制を構築する。

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	〒564-8550 大阪府吹田市泉町1丁目3番40号 吹田市役所 市民部 市民総務室 06-6384-1456
②請求方法	吹田市個人情報保護条例第14条に基づき、必要事項を記載した開示請求書を提出する。
特記事項	市ホームページ上に、請求先、請求方法、請求書様式等を掲載している。
③手数料等	[無料] <選択肢> 1) 有料 2) 無料 (手数料額、納付方法: コピーが必要な場合は10円/1枚)
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	・予防接種情報管理ファイル ・新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム(VRS)ファイル
公表場所	吹田市役所 市民部 市民総務室
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	〒564-0072 大阪府吹田市出口町19番2号(吹田市立総合福祉会館3階) 吹田市役所 健康医療部 保健センター 06-6339-1212
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。

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和3年11月15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	吹田市民の意見の提出に関する条例に準じて意見募集を行う。意見募集の実施に際しては、市ホームページ及び市役所本庁にて全文を閲覧できるものとし、意見の提出は郵便、メール、FAXにより受け付けることとする。
②実施日・期間	令和3年8月16日～令和3年9月15日
③期間を短縮する特段の理由	—
④主な意見の内容	提出意見なし。
⑤評価書への反映	—
3. 第三者点検	
①実施日	令和3年11月1日
②方法	吹田市個人情報保護審議会による第三者点検を受けた。
③結果	個人情報の取扱いについて、以下の内容の答申があった。 当審議会は、予防接種に関する事務に係る特定個人情報保護評価書(全項目評価書)の記載につき同意する。
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	

