

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
15	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等に関する事務 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

ふじみ野市は、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等に関する事務の特定個人情報ファイルの取扱いが、個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減させるために適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項

予防接種関係事務においては、事務の一部を外部業者に委託しているが、委託先による情報の不正入手、不正使用、情報漏えい等の対策として、契約において、個人情報保護条例及び情報セキュリティポリシーに基づき、「個人情報の取扱いに関する特記仕様書」を遵守させ、かつ、受託者から「個人情報の取扱いに関する特記仕様書の項目遵守確認表」を提出させ、個人情報の保護を積極的に進めている。

評価実施機関名

埼玉県 ふじみ野市長

公表日

令和8年8月20日

項目一覧

I 基本情報
II 特定個人情報ファイルの概要
(別添1) 特定個人情報ファイル記録項目
III リスク対策
IV 開示請求、問合せ
V 評価実施手続
(別添2) 変更箇所

I 基本情報

1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	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等に関する事務
②事務の内容	<p>予防接種法及び新型インフルエンザ等対策特別措置法の規定に基づき、 予防接種情報の管理、統計報告資料作成、データ分析の処理を行う。 特定個人情報ファイルは、以下の場合に使用する。 ①予防接種法による予防接種の実施対象者把握 ②情報提供ネットワークシステムへの予防接種データ提供 ③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</p> <p>情報提供に必要な特定個人情報を副本として中間サーバーに登録し、情報提供ネットワークシステムに接続して特定個人情報の照会と提供を行う。</p> <p>＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務＞ ・情報連携のため、予診情報・予防接種記録管理／請求支払システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び接種記録の紐付け及び登録を行う。 ・住民は、マイナポータルを介して予診票情報の入力並びに接種記録及び通知の取得／閲覧が可能となる。 ・住民が予防接種時に、従来の紙の予診票に代えて、タブレットに搭載された医療機関用アプリ等においてマイナンバーカードを用いることにより、医療機関は住民が事前に入力した予診票情報、接種記録の取得／閲覧／入力が可能となる。 ・医療機関から入力された予診票情報、接種記録の取得及び住民への通知が可能となる。</p>
③対象人数	<div style="display: flex; align-items: center;"> <div style="margin-right: 20px;"> ☐ 10万人以上30万人未満 </div> <div style="text-align: center;"> ＜選択肢＞ 1) 1,000人未満 3) 1万人以上10万人未満 </div> <div style="margin-left: 20px;"> 2) 1,000人以上1万人未満 4) 10万人以上30万人未満 </div> </div>
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	<p>予防接種 ・接種の対象者の選定を行い、条件に該当した住民情報の表示と帳票発布等を行う。 ・医療機関または、実施取りまとめ機関より返送された予診票等の内容を接種実績として登録する。 ・個人ごとの接種実績および、費用徴収に関する事務に必要な情報の参照を行う。</p>
③他のシステムとの接続	<div style="display: flex; justify-content: space-between;"> <div> ☐ 情報提供ネットワークシステム ☐ 住民基本台帳ネットワークシステム ☒ 宛名システム等 ☐ その他（ </div> <div> ☐ 庁内連携システム ☐ 既存住民基本台帳システム ☐ 税務システム </div> </div>
システム2～5	
システム2	
①システムの名称	統合宛名システム
②システムの機能	<p>1. 宛名情報を照会する。 2. 住登外宛名情報を追加・削除・変更する。 3. 法人宛名情報を追加・削除・変更する。</p>
③他のシステムとの接続	<div style="display: flex; justify-content: space-between;"> <div> ☐ 情報提供ネットワークシステム ☐ 住民基本台帳ネットワークシステム ☐ 宛名システム等 ☒ その他（中間サーバー </div> <div> ☐ 庁内連携システム ☒ 既存住民基本台帳システム ☐ 税務システム </div> </div>

システム3	
①システムの名称	中間サーバー・ソフトウェア
②システムの機能	<p><中間サーバーの機能></p> <p>1. 符号管理機能 情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「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。</p> <p>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、特定個人情報(連携対象)の情報照会及び情報提供受領(照会した情報の受領)を行う。</p> <p>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、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。</p> <p>4. 既存システム接続機能 中間サーバーと既存システム、団体内統合宛名システム及び住基システムとの間で情報照会内容、情報提供内容、特定個人情報(連携対象)、符号取得のための情報等について連携する。</p> <p>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。</p> <p>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。</p> <p>7. データ送受信機能 中間サーバー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。</p>
③他のシステムとの接続	<div> <div> ☐ 情報提供ネットワークシステム ☐ 市内連携システム </div> <div> ☐ 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 </div> <div> ☒ 宛名システム等 ☐ 税務システム </div> <div> ☐ その他 () </div> </div>
システム4	
①システムの名称	予診情報・予防接種記録管理／請求支払システム
	<p>【予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務】</p> <p>①予防接種関連データの登録機能 健康管理システムからの情報連携又は予診情報・予防接種記録管理／請求支払システム画面への直接入力により、予診票項目、接種勧奨における通知文言等の予防接種関連データを予診情報・予防接種記録</p>

<p>②システムの機能</p>	<p>管理／請求支払システムへ登録する。</p> <p>②情報登録機能及びPMHキー採番依頼機能等 予診情報・予防接種記録管理／請求支払システムは、本市で管理している個人番号、対象者情報、予診票情報及び接種記録を予診情報・予防接種記録管理／請求支払システムに登録する。また、Public Medical Hubを経由して社会保険診療報酬支払基金（以下、「支払基金」という。）の医療保険者等向け中間サーバーと連動し、PMHキーを自動採番する。すでにPMHキーが採番済みの個人番号であれば、採番は行わずに既存のPMHキーを利用する。</p> <p>③情報連携機能（マイナポータル） ・識別子の格納機能 予診情報・予防接種記録管理／請求支払システムは、マイナポータルからの予診情報・予防接種記録管理／請求支払システム初回利用時に、マイナポータル上で生成されたPMH仮名識別子をPMHキーと紐付けて予診情報・予防接種記録管理／請求支払システムに格納して保管する。 ・仮名識別子を利用した情報入力/提供機能 予防接種の対象者は、マイナポータルへログインしてマイナンバーカードの電子証明書のシリアル番号に紐づくPMH仮名識別子を利用した照会を行う。予診情報・予防接種記録管理／請求支払システムは、PMH仮名識別子からPMHキーを特定し、PMHキーに紐づく接種記録・通知をマイナポータルへ提供する。また、マイナポータルへログインして予診票の入力画面から情報を入力することにより、予診情報・予防接種記録管理／請求支払システムはPMH仮名識別子からPMHキーを特定し、PMHキーに紐づく予診票情報を登録する。</p> <p>④情報連携機能（医療機関用アプリ） ・本人確認情報の格納機能 予防接種対象者が、顔認証端末又はマイナ資格確認アプリを利用してマイナンバーカードで認証及び同意することにより、オンライン資格確認等システムを経由してPublic Medical Hubに本人確認情報が格納される。 ・本人確認情報を利用した情報入力/提供機能 医療機関用アプリ等は、予診情報・予防接種記録管理／請求支払システムへ本人確認情報を利用した照会を行う。予診情報・予防接種記録管理／請求支払システムは、Public Medical Hubから本人確認情報を</p>								
<p>③他のシステムとの接続</p>	<table border="0"> <tr> <td>[] 情報提供ネットワークシステム</td> <td>[] 庁内連携システム</td> </tr> <tr> <td>[] 住民基本台帳ネットワークシステム</td> <td>[] 既存住民基本台帳システム</td> </tr> <tr> <td>[] 宛名システム等</td> <td>[] 税務システム</td> </tr> <tr> <td colspan="2"> [○] その他 （健康管理システム、マイナポータル、医療機関用アプリ、電子カルテ等、Public Medical Hub、履歴照会回答システム、オンライン資格確認等システム） </td> </tr> </table>	[] 情報提供ネットワークシステム	[] 庁内連携システム	[] 住民基本台帳ネットワークシステム	[] 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 （健康管理システム、マイナポータル、医療機関用アプリ、電子カルテ等、Public Medical Hub、履歴照会回答システム、オンライン資格確認等システム）	
[] 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 （健康管理システム、マイナポータル、医療機関用アプリ、電子カルテ等、Public Medical Hub、履歴照会回答システム、オンライン資格確認等システム）									
<p>システム6～10</p>									
<p>システム11～15</p>									
<p>システム16～20</p>									

3. 特定個人情報ファイル名		
予防接種対象者ファイル、宛名情報ファイル		
4. 個人番号の利用 ※		
法令上の根拠	【予防接種法による予防接種の実施等に関する事務】 【予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務】 番号法第9条第1項 別表14の項 【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】 番号法第9条第1項 別表126の項	
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	【予防接種法による予防接種の実施等に関する事務】 (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25の項、27の項、28の項、29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25の項 【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】 (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25の項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25の項153の項、154の項 【予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務】 番号利用法第19条第8号(特定個人情報の提供の制限)及び別表の14の項	
6. 評価実施機関における担当部署		
①部署	こども・元気健康部 保健センター	
②所属長の役職名	保健センター所長	
7. 他の評価実施機関		

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	
予防接種対象者ファイル	
2. 基本情報	
①ファイルの種類 ※	[システム用ファイル] <div style="float: right;"> <small>＜選択肢＞</small> 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) </div>
②対象となる本人の数	[10万人以上100万人未満] <div style="float: right;"> <small>＜選択肢＞</small> 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 </div>
③対象となる本人の範囲 ※	当該市町村の区域内に居住する予防接種の対象となる者
その必要性	予防接種に関する業務の実現のために、必要な特定個人情報を保有する必要がある。
④記録される項目	[10項目以上50項目未満] <div style="float: right;"> <small>＜選択肢＞</small> 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 </div>
主な記録項目 ※	<ul style="list-style-type: none"> ・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 (<small>＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係</small>)
その妥当性	<small>＜個人番号、その他識別情報(内部番号)＞</small> ・本人確認等、対象者を正確に特定するために保有 <small>＜4情報、その他住民票関係情報＞</small> ・予防接種対象者の居住地を把握するために保有 <small>＜健康・医療関係情報(予防接種に関する情報)＞</small> ・予防接種の接種実績、接種料金等を把握するために保有 <small>＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務＞</small> ・識別情報(その他識別情報) PMHキー、PMH仮名識別子、PMH連携キー、予防接種対象者番号、ID5…予診情報・予防接種記録管理／請求支払システムが、外部と情報連携するために必要となる。 ・業務関係情報(その他) 予防接種記録情報…予防接種事務の適切な実施にあたり必要となる情報を管理し、予診情報・予防接種記録管理／請求支払システムが、外部と情報連携するために必要となる。
全ての記録項目	別添1を参照。
⑤保有開始日	令和3年4月1日
⑥事務担当部署	こども・元気健康部 保健センター

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 () ☐ 民間事業者 (医療機関) ☐ その他 (住民基本台帳ネットワークシステム、ワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能を含む。))
②入手方法		☐ 紙 [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ ☐ 電子メール [] 専用線 ☐ 庁内連携システム ☐ 情報提供ネットワークシステム ☐ その他 (住民基本台帳ネットワークシステム、ワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能を含む。)、コンビニエンスストア等のキオスク端末及び証明書交付センターシステム、Public Medical Hub、医療機関用アプリ等、マイナポータル)
③使用目的 ※		予防接種の実施、予防接種に関する記録の作成
④使用の主体	使用部署	こども・元気健康部 保健センター
	使用者数	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">[10人以上50人未満]</div> <div> <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 </div> </div>
⑤使用方法		<p>予防接種の実施、予防接種に関する記録の作成等に使用する。</p> <p><予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務> ・情報連携のため、予診情報・予防接種記録管理／請求支払システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び予防接種管理情報の紐付け及び登録を行う。 ・登録後、予診情報・予防接種記録管理／請求支払システムは、Public Medical Hubに対してオンライン資格確認等システムと予診情報・予防接種記録管理／請求支払システムが連動するためのPMHキーの採番処理を依頼し、医療保険者等向け中間サーバーは、情報連携用の識別子としてPMHキーを採番して個人番号と共にPublic Medical Hubを経由して予診情報・予防接種記録管理／請求支払システムに伝送する。 ・PMHキーが、個人情報として医療保険者等向け中間サーバーから既存の紐付番号とともにオンライン資格確認等システムに連携され、更にマイナポータルで生成されたPMH仮名識別子がマイナポータルと予診情報・予防接種記録管理／請求支払システムで共有されることで予診情報・予防接種記録管理／請求支払システムからマイナポータルへの通知、マイナポータルや医療機関用アプリ等から予診情報・予防接種記録管理／請求支払システムの予診票情報及び接種記録の取得/閲覧/入力等といった情報連携が可能となる。</p>
情報の突合		住民からの費用助成申請書等の内容と地方税関係情報を突合する。
⑥使用開始日		令和3年4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 ※		<div> <div>委託する</div> <div><選択肢></div> <div>1) 委託する</div> <div>2) 委託しない</div> </div> <div>(1) 件</div>
委託事項1		システム保守業務
①委託内容		システム保守業務
②委託先における取扱者数		<div> <div>10人以上50人未満</div> <div><選択肢></div> <div>1) 10人未満</div> <div>2) 10人以上50人未満</div> <div>3) 50人以上100人未満</div> <div>4) 100人以上500人未満</div> <div>5) 500人以上1,000人未満</div> <div>6) 1,000人以上</div> </div>
③委託先名		株式会社TKC
再委託	④再委託の有無 ※	<div> <div>再委託しない</div> <div><選択肢></div> <div>1) 再委託する</div> <div>2) 再委託しない</div> </div>
	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2		予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る各事務における特定個人情報ファイルの一部の取扱
①委託内容		予診情報・予防接種記録管理／請求支払システムの利用・情報連携業務及び運用保守業務
②委託先における取扱者数		<div> <div>10人以上50人未満</div> <div><選択肢></div> <div>1) 10人未満</div> <div>2) 10人以上50人未満</div> <div>3) 50人以上100人未満</div> <div>4) 100人以上500人未満</div> <div>5) 500人以上1,000人未満</div> <div>6) 1,000人以上</div> </div>
③委託先名		埼玉県国保連合会
再委託	④再委託の有無 ※	<div> <div>再委託する</div> <div><選択肢></div> <div>1) 再委託する</div> <div>2) 再委託しない</div> </div>
	⑤再委託の許諾方法	書面又は電磁的方法による承諾
	⑥再委託事項	<予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務> ・予診情報・予防接種記録管理／請求支払システムの運用保守 ・PMHキーの採番及びPMHキーを介した医療機関用アプリ等・マイナポータルへの情報連携 ※情報連携はPMHキーを介して行うため、特定個人情報を取り扱わない。
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（ 1 ）件 ☐ 移転を行っている（ ）件 ☐ 行っていない	
提供先1	都道府県または市町村	
①法令上の根拠	番号利用法第19条第8号及び別表14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	
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	<div style="display: flex; justify-content: space-between;"> [10万人以上100万人未満] <div style="text-align: right;"> <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 </div> </div>	
⑤提供する情報の対象となる本人の範囲	本市の区域内に居住する予防接種の対象となる者	
⑥提供方法	<div style="display: flex; justify-content: space-between;"> <div> ☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他（ ） </div> <div> ☐ 専用線 ☐ 電子記録媒体（フラッシュメモリを除く。） ☐ 紙 </div> </div>	
⑦時期・頻度	照会を受けたら、その都度	
提供先2～5		
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		
④移転する情報の対象となる本人の数	<div style="display: flex; justify-content: space-between;"> [] <div style="text-align: right;"> <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 </div> </div>	
⑤移転する情報の対象となる本人の範囲		
⑥移転方法	<div style="display: flex; justify-content: space-between;"> <div> ☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☐ その他（ ） </div> <div> ☐ 専用線 ☐ 電子記録媒体（フラッシュメモリを除く。） ☐ 紙 </div> </div>	
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 ※	<p>情報・統計課サーバー室及び株式会社TKCのデータセンター</p> <p>＜ガバメントクラウドにおける措置＞</p> <p>①サーバー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。</p> <ul style="list-style-type: none"> ・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。 <p>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。</p>
	<p>＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務＞</p> <p>予診情報・予防接種記録管理／請求支払システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバー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、政府</p> <p>情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスか、ISO/IEC27017:2015</p> <p>又はCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用している。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"> ・サーバー設置場所等への入退室記録管理、施錠管理 ・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。
7. 備考	

【別添1）特定個人情報ファイル記録項目

1. 予防接種ファイル

【識別情報】

1.基本コード

【連絡先情報】

1.電話番号

【業務関係情報】

1.基本コード、2.接種種類、3.接種回数、4.接種年度、5.接種年月日、6.予診医コード、7.接種医コード、8.接種会場コード、9.医療機関コード、10.接種区分、11.接種不适当区分、12.接種済証発行区分、13.接種量、14.接種部位、15.接種方法、16.メーカー、17.ワクチン名、18.ロットN
O、
19.有効期限、20.罹患区分、21.罹患年月日、22.助成区分、23.助成年月日、24.助成金額、25.請求年月、27.他市町村接種区分、26.備考

2. 中間サーバーで保有される特定個人情報(上記と重複する項目を除く) 情報提供用個人識別符号、団体内統合宛名番号等

< 予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加の記録項目 >

(1)対象者情報

- ・個人番号
- ・PMHキー
- ・PMH仮名識別子
- ・基本5情報(カナ・氏名・住所・生年月日・性別)
- ・保護者氏名
- ・自治体コード
- ・自治体業務ID
- ・連携ファイル名
- ・連携日時
- ・連携処理ステータス/エラー内容
- ・制御フラグ(リカバリー/不開示/閲覧停止)
- ・変更区分
- ・消除の異動日
- ・その他管理番号・ID等(予防接種対象者番号)
- ・その他区分等(接種対象者区分/減免区分)

(2)ユーザー情報

- ・機関マスタID
- ・機関ユーザーID
- ・メールアドレス
- ・ユーザー氏名
- ・ユーザー区分
- ・ユーザー権限ID
- ・個人番号閲覧可能フラグ
- ・ユーザー削除フラグ

(3)予診票情報

- ・項目ID
- ・管理ID
- ・更新日時
- ・回答ID
- ・回答内容
- ・回答処理ステータス
- ・回答日時
- ・接種不可フラグ
- ・予防接種設定ID
- ・予防接種管理ID
- ・組み合わせ番号
- ・強制失効日

・勸奨情報(ルールID、勸奨日)

(4)予防接種記録情報

・予防接種記録ID

・予防接種管理ID

・接種日

・接種同意フラグ

・医療機関コード

・医師名

・実施場所

・実施区分

・接種区分

・GTINコード

・ワクチンメーカー名

・ワクチン名(ワクチン一般名/ワクチン通称/ワクチン販売名)

・ロット番号

・接種量

・接種部位

・接種方法

・ワクチン有効期限

・要注意接種フラグ

・特別の事情

・海外接種フラグ

・更新日時

・最新/削除フラグ

・その他区分等(接種対象者区分/減免区分)

Ⅲ リスク対策 ※(7. ②を除く。)

1. 特定個人情報ファイル名	
1. 予防接種ファイル(健康管理システム)	
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	<ul style="list-style-type: none"> ・住民からの申告・申請情報の入手については、本人確認や個人番号の真正性確認を実施している。 ・市町村OSからの住登外情報については、職員2名以上でダブルチェックを行って対象者を確定した上で情報を入手している。 ・庁内連携機能からの各種照会情報の入手については、個人単位の操作ログを取得し追跡可能な形式で管理しており、対象者以外の情報の入手の抑止を図っている。
リスクへの対策は十分か	<div> <div>[十分である]</div> <div> <div><選択肢></div> <div> <div>1) 特に力を入れている</div> <div>2) 十分である</div> <div>3) 課題が残されている</div> </div> </div> </div>
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	
<p><不適切な方法で入手が行われるリスクに対する措置></p> <ul style="list-style-type: none"> ・住基情報の入手については、入退室管理をしているデータセンタ内のサーバ間通信に限定することで、詐取・奪取が行われないようにしている。 ・各種照会情報の入手については、アクセス権を有しない職員のなりすましによる入手への対策を施している。 <p>また、当該情報に接続可能なシステム及び端末を予め登録し、許可された機器に限定した入手方法とすることで、対象外の機器からの入手が行われないようにしている。</p> <p><入手した特定個人情報が不正確であるリスクに対する措置></p> <ul style="list-style-type: none"> ・入手した情報については、窓口での聞き取りや本人確認書類との照合等を通じて確認することで正確性を確保している。 ・職員にて収集した情報に基づいて、間違いがあれば職権で適宜修正することで正確性を確保している。 <p><予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置></p> <p>■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> <ul style="list-style-type: none"> ・医療機関の受付窓口で本人確認の後、医療機関用アプリ等又は顔認証端末でマイナンバーカードを利用した認証により本人の情報のみが対象者として連携される。 ・本人が、マイナポータルへログインし、予診票情報を入力する際には、マイナンバーカードを利用した認証により、本人以外からの情報の入力を防止する。 ・既存事務において本人確認を行った個人番号を既存システム(各業務システム)から予診情報・予防接種記録管理／請求支払システムに連携し、その本人確認済みの個人番号を医療保険者等向け中間サーバーに連携するが、提供した個人番号は加工することなく返却されるため、対象者以外の情報を入手することはない。 <p>■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</p> <ul style="list-style-type: none"> ・医療保険者等向け中間サーバーからPublic Medical Hubを経由した予診情報・予防接種記録管理／請求支払システムへは、定められたインターフェース仕様に沿って決められたデータ項目(PMHキーと個人番号)のみが返却されるようシステムの制御している。 ・医療機関から医療機関用アプリ等を介して入力される際は、定められたインターフェース仕様に沿って決められたデータ項目のみが連携されるようシステムの制御している。 ・本人が、マイナポータルへログインし、予診票情報を入力する際には、定められたデータ項目のみが入力されるようシステムの制御している。 	

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	<p>システムが必要とするデータベースのみアクセスできる構造になっており、その他の事務で使用するデータベースにはアクセスできないよう制御を行っている。</p> <p>＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞</p> <p>■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> <ul style="list-style-type: none"> ・予診情報・予防接種記録管理／請求支払システムにアクセスする本市の職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。 ・予診情報・予防接種記録管理／請求支払システムでは、権限のある者しか個人番号にはアクセスできないように制御している。 ・医療機関用アプリ等や住民から予診情報・予防接種記録管理／請求支払システムに接続するが、必要な情報のみアクセスでき、個人番号にはアクセスできないように制御している。 	
リスクへの対策は十分か	[十分である]	<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]	<p>＜選択肢＞</p> <p>1) 行っている 2) 行っていない</p>
具体的な管理方法	<p>システムを利用する必要がある職員を特定し、個人ごとにユーザIDを割り当てるとともにIDとパスワードによる認証(又は生体認証など)認証を行っている。</p> <p>＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞</p> <p>権限のない者に不正使用されないよう、以下の対策を講じている。</p> <ul style="list-style-type: none"> ・予診情報・予防接種記録管理／請求支払システムのアクセス権限を管理する管理者を定める。 ・予診情報・予防接種記録管理／請求支払システムのログインはユーザID・パスワードで行う。 ・予診情報・予防接種記録管理／請求支払システムへのログイン用のユーザIDは、管理者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。 ・端末は、限定された者しかログインできない。 ・予診情報・予防接種記録管理／請求支払システムにおける特定個人情報へのアクセスは、LGWAN回線又はその他の閉域網回線経由の接続のみ認められるよう制御している。 ・既存システム(各業務システム)から予診情報・予防接種記録管理／請求支払システムへの連携は、アクセス権限を持つ者のみ実施が可能となっている。 ・予診情報・予防接種記録管理／請求支払システムへのアップロード・ダウンロードに用いる外部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、媒体管理簿等に使用の記録を記載する等、利用履歴を残す。 ・作業に用いる外部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。 	
その他の措置の内容	<ul style="list-style-type: none"> ・操作ログの記録を行う。 ・定期的に記録を確認し、不正アクセスがないか点検している。 ・サーバOSへのログインアクセス権管理 ・クライアントOSのログインID管理 ・システムへのログインID管理 	
リスクへの対策は十分か	[十分である]	<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>

特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	
4. 特定個人情報ファイルの取扱いの委託 [] 委託しない	
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	<div style="display: flex; justify-content: space-between;"> [定めている] <div> <div><選択肢></div> <div> 1) 定めている 2) 定めていない </div> </div> </div>
規定の内容	<p>契約書において、個人情報保護条例をはじめとする個人情報保護に関する法令並びに関連ガイドライン等の趣旨に従うことを定めている。</p> <p><予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置></p> <p>埼玉県国保連合会及び国保中央会は特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）を遵守し、委託契約書に以下の規定を設ける。</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 ・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 ・再委託における条件 ・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 ・漏えい等事案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消去 ・特定個人情報を取り扱う従業員の明確化 ・従業員に対する監督・教育 ・契約内容の遵守状況についての報告 ・実地の監査、調査等に関する事項
再委託先による特定個人情報ファイルの適切な取扱いの担保	<div style="display: flex; justify-content: space-between;"> [十分に行っている] <div> <div><選択肢></div> <div> 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 </div> </div> </div>
具体的な方法	<p>再委託先においても委託先と同様の対策を実施している。</p> <p><予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置></p> <ul style="list-style-type: none"> ・再々委託の相手方は、委託先が負っている本契約上の義務と同等の義務を負うことを委託契約書に定める。 ・国保中央会が、再々委託先における特定個人情報ファイルの管理状況の定期的な点検（年1回程度又は随時）を実施する。 ・点検は、再々委託の相手方によるセルフチェックを基本とし、必要に応じて国保中央会が訪問確認を行う。 ・点検後に改善事項がある場合は、国保中央会が改善指示及び改善状況のモニタリングを行う。 ・国保中央会は、点検結果について埼玉県国保連合会及び本市に年1回報告を行う。
その他の措置の内容	
リスクへの対策は十分か	<div style="display: flex; justify-content: space-between;"> [十分である] <div> <div><選択肢></div> <div> 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 </div> </div> </div>

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： 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	<div style="display: flex; align-items: center;"> [<div style="flex-grow: 1; border: 1px solid black; height: 20px;"></div>] <div style="margin-left: 10px;"> <選択肢> 1) 定めている 2) 定めていない </div> </div>
<div style="border: 1px solid black; padding: 5px; width: 100px; float: left;"> ルールの内容及び ルール遵守の確認方法 </div>	
その他の措置の内容	
リスクへの対策は十分か	<div style="display: flex; align-items: center;"> [<div style="flex-grow: 1; border: 1px solid black; height: 20px;"></div>] <div style="margin-left: 10px;"> <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 </div> </div>
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	
リスクへの対策は十分か	<div style="display: flex; align-items: center;"> [<div style="flex-grow: 1; border: 1px solid black; height: 20px;"></div>] <div style="margin-left: 10px;"> <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 </div> </div>

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	<p>＜健康管理システムのソフトウェアにおける措置＞</p> <p>①システムへのログイン時に、ログインが許可された利用者、利用端末のみが利用できるよう、認証を行っている。</p> <p>②副本登録、情報提供機能は、許可された利用者、利用端末のみが利用できるよう、制御している。</p> <p>③システムが管理対象とする特定個人情報（データセットレコード）のみを副本登録、情報提供可能とするよう制御している。</p> <p>④システムへのログイン、ログアウト、副本登録、情報提供を実施した際のログ（利用者、利用端末、利用日時）を記録している。</p> <p>＜健康管理システムの運用における措置＞</p> <ul style="list-style-type: none"> ・健康管理システムで記録している操作ログは、適宜リストの出力を行い、不正な提供が行われていないことを定期的に確認している。 ・提供に制限のある特定個人情報は、適切に不開示設定を行う実施手順を運用ルールに定め、当該ルールに従い実施している。 ・自動応答不可の特定個人情報の提供に当たっては、上長の承認を得た上で、提供を実施する運用を義務付けている。 <p>＜中間サーバー・ソフトウェアにおける措置＞</p> <p>①情報提供機能（※）により、情報提供ネットワークシステムにおける照会許可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、照会許可照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。</p> <p>②情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。</p> <p>③特に慎重な対応が求められる情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。</p> <p>④中間サーバーの職員認証・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。</p> <p>（※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。</p> <p>＜中間サーバーの運用における措置＞</p> <ul style="list-style-type: none"> ・不正検知の目的で、ログを定期的に確認する。 ・中間サーバー接続端末の情報提供機能の利用にあたっては、事前に情報提供の内容について、上長の承認を得た上で、提供を実施する運用を義務付けている。 	
リスクへの対策は十分か	[十分である]	<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>

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

■安全が保たれない方法によって入手が行われるリスク

＜中間サーバー・ソフトウェアにおける措置＞

①中間サーバーは、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。

＜中間サーバー・プラットフォームにおける措置＞

①中間サーバーと既存システム、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中間サーバーと団体については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。

■入手した特定個人情報が不正確であるリスク

＜中間サーバー・ソフトウェアにおける措置＞

①中間サーバーは、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。

■入手の際に特定個人情報が漏えい・紛失するリスク

＜中間サーバー・ソフトウェアにおける措置＞

①中間サーバーは、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。

(※)中間サーバーは、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ー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。

＜中間サーバー・プラットフォームにおける措置＞

①中間サーバーと既存システム、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中間サーバーと団体については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中間サーバー・プラットフォーム事業者の業務は、中間サーバー・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。

■不適切な方法で提供されるリスク

＜中間サーバー・ソフトウェアにおける措置＞

①セキュリティ管理機能(※)により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。

②中間サーバーの職員認証・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。

(※)暗号化・復号機能と、鍵情報及び照会許可照合リストを管理する機能。

＜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中間サーバーと団体については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中間サーバー・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。

■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

＜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情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。

②情報提供データベース管理機能(※)により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。

③情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。

(※)特定個人情報を副本として保存・管理する機能。

■その他のリスク

＜中間サーバー・ソフトウェアにおける措置＞

①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。

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。

＜中間サーバー・プラットフォームにおける措置＞

①中間サーバーと既存システム、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中間サーバーと団体については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中間サーバー・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、中間サーバー・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、中間サーバー・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： 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	[十分にしている]	<選択肢> 1) 特に力を入れている 2) 十分にしている 3) 十分にしていない
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
<div>その内容</div>		
<div>再発防止策の内容</div>		
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

◆物理的対策

＜市における措置＞

- ・特定個人情報を保管するサーバ設置場所には、入退室管理を行っている。
- ・特定個人情報を保管するサーバに係る脅威に対して、無停電電源装置の設置、室温管理、ケーブルの安全管理、耐震対策、防火措置、防水措置等を講じている。
- ・特定個人情報を保有するサーバが設置された専用部屋への入室はICカードと生体による2因子認証で管理されている。
- ・特定個人情報を保有するサーバが設置された部屋には監視カメラ等が設置されている。
- ・特定個人情報を保有するサーバが設置されたラックは施錠管理されている。
- ・特定個人情報を保有するサーバは定期的に保守点検を実施することで情報の毀損等への対策を図っている。
- ・特定個人情報を含む電子データを定期的に電子媒体に保存し、入退室管理された専用の保管場所に保管している。

＜中間サーバー・プラットフォームにおける措置＞

- ・中間サーバー・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。
- ・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。

◆技術的対策

＜市における措置＞

- ・ウイルス対策ソフトを導入し、定期的にパターンファイルの更新を行っている。
- ・OSやアプリケーション等に対するセキュリティ対策用修正ソフトウェア(いわゆるセキュリティパッチ)を適用している。
- ・ファイアウォールにより、特定個人情報へのアクセスを制御している。
- ・使用されていないポートを閉鎖している。
- ・情報漏えい等の防止のため、特定個人情報を保有するサーバをインターネット等の外部ネットワークから隔離されたネットワーク上に設置している。
- ・盗聴による情報漏えい等の防止のため特定個人情報を保有するサーバとの通信を暗号化している。
- ・内部の部品が2重化された高可用性の外部記憶装置(ストレージ)に特定個人情報を保存することで情報の毀損等への対策を図っている。
- ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォールを設置している。

＜中間サーバー・プラットフォームにおける措置＞

- ①中間サーバー・プラットフォームではUTM(コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置)等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。
- ②中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。
- ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。

＜ガバメントクラウドにおける措置＞

●消去方法

- 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等に示した方法で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。

●消去手順

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。

●物理的対策

- 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。

●技術的対策

- 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【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。
- 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。
- 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。

＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞

◆特定個人情報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

- ・本特定個人情報ファイルの個人情報は、住基及び住民登録外者の異動情報を取得し、内部番号を基に最新の情報に反映されるため、古い情報のまま保管され続けるリスクは存在しない。

◆特定個人情報が消去されずいつまでも存在するリスク

以下の通り消去手順を定めている。

- ・消去が必要となった情報は内部手続を経て消去し、その記録を残す。
- ・不要となった特定個人情報は、削除用データの連携又は運用保守事業者に依頼して消去する。
- ・不要となったバックアップファイルは、ストレージに適用されたライフサイクルルールに基づき、保管されたログ情報については、各オブジェクトの保管日(作成日)を起点として3年が経過した時点で、自動的に削除される。

8. 監査		
実施の有無	☐ 自己点検 ☐ 内部監査 ☐ 外部監査	
9. 従業員に対する教育・啓発		
従業員に対する教育・啓発	☐ 十分に行っている ☐ 十分に行っていない <div> <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 </div>	
	<div> 具体的な方法 </div>	<div> <市における措置> ・毎年、職員全員に情報セキュリティ研修を実施している。 ・サーバ室への入退室については、生体情報による認証を実施している。 ・年に1回、所属部署のICT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。 </div>
10. その他のリスク対策		
<div> <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。 </div> <div> <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。 ・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。 </div> <div> <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> 情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき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。 </div>		

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	総務部 契約・法務課 〒356-8501 埼玉県ふじみ野市福岡一丁目1番1号 049-261-2611
②請求方法	市個人情報保護条例に基づき、請求書に住所、氏名、請求内容等の必要事項を記入し、請求する。 個人情報の本人であることを証明する書類等を持参の上、個人情報保護窓口に提出する。
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	こども・元気健康部 保健センター 〒356-0011 埼玉県ふじみ野市福岡一丁目2番5号 049-264-8292
②対応方法	問い合わせの受付時に受付票等を記載することにより、対応について記録を残す。 情報漏えい等の重大な事案に関する問い合わせについて、関係先等に事実確認を行うための標準的な 処理期間を設ける

V 評価実施手続

1. 基礎項目評価	
①実施日	令和4年12月15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4年1月14日	I 基本情報 1. 特定個人情報ファイルを取り扱う事務 ②事務の内容	<p>予防接種法及び新型コロナウイルス等対策特別措置法の規定に基づき、 予防接種情報の管理、統計報告資料作成、データ分析の処理を行う。 特定個人情報ファイルは、以下の場合に使用する。 ①予防接種法による予防接種の実施対象者把握 ②情報提供ネットワークシステムへの予防接種データ提供 ③新型コロナウイルス等対策特別措置法による予防接種の実施に関する事務</p> <p>情報提供に必要な特定個人情報等を副本として中間サーバーに登録し、 情報提供ネットワークシステムに接続して特定個人情報の照会と提供を行う。</p>	<p>予防接種法及び新型コロナウイルス等対策特別措置法の規定に基づき、 予防接種情報の管理、統計報告資料作成、データ分析の処理を行う。 特定個人情報ファイルは、以下の場合に使用する。 ①予防接種法による予防接種の実施対象者把握 ②情報提供ネットワークシステムへの予防接種データ提供 ③新型コロナウイルス等対策特別措置法による予防接種の実施に関する事務</p> <p>情報提供に必要な特定個人情報等を副本として中間サーバーに登録し、 情報提供ネットワークシステムに接続して特定個人情報の照会と提供を行う。</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 ・ワクチン接種記録システム(VRS)へ予防接種対象者及び発行した接種券の登録を行う。 ・予防接種の実施後に接種記録等を登録、管理し、他市区町村へ接種記録の照会・提供を行う。 ・予防接種の実施後に、接種者からの申請に基づき、新型コロナウイルス感染症予防接種証明書の交付を行う。</p>	事後	特定個人情報保護評価に関する規則第9条第2項の規定(緊急時の事後評価)
令和4年1月14日	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4 ①システムの名称		ワクチン接種記録システム(VRS)	事後	特定個人情報保護評価に関する規則第9条第2項の規定(緊急時の事後評価)
令和4年1月14日	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4 ②システムの機能		<p>・ワクチン接種記録システムへの接種対象者・接種券発行登録 ・接種記録の管理 ・転出/死亡時等のフラグ設定 ・他市区町村への接種記録の照会・提供 ・新型コロナウイルス感染症予防接種証明書の交付に係る接種記録の照会 ・新型コロナウイルス感染症予防接種証明書の電子申請受付・電子交付の実施</p>	事後	特定個人情報保護評価に関する規則第9条第2項の規定(緊急時の事後評価)
令和4年1月14日	4. 個人番号の利用 法令上の根拠	<p>【予防接種法による予防接種の実施等に関する事務】 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9条第1項、別表第一の10の項番号法別表第一の主務省令で定める事務を定める命令(内閣府令第5号、総務省令第5号)第10条 【新型コロナウイルス等対策特別措置法による予防接種の実施に関する事務】 行政手続における特定の個人を識別するための番号の利用等に関する法律(平成25年法律第27号)第9条第1項(利用範囲)、別表第一の93の2の項 ・番号法別表第一の主務省令で定める事務を定める命令(内閣府令第5号、総務省令第5号)第67条の2</p>	<p>【予防接種法による予防接種の実施等に関する事務】 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9条第1項、別表第一の10の項番号法別表第一の主務省令で定める事務を定める命令(内閣府令第5号、総務省令第5号)第10条 【新型コロナウイルス等対策特別措置法による予防接種の実施に関する事務】 行政手続における特定の個人を識別するための番号の利用等に関する法律(平成25年法律第27号)第9条第1項(利用範囲)、別表第一の93の2の項 ・番号法別表第一の主務省令で定める事務を定める命令(内閣府令第5号、総務省令第5号)第67条の2 【新型コロナウイルス感染症対策に係る予防接種事務】 ・番号法第19条第16号(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ワクチン接種記録システムを用いた情報提供・照会のみ) ・番号法第19条第6号(委託先への提供)</p>	事後	特定個人情報保護評価に関する規則第9条第2項の規定(緊急時の事後評価)
令和4年1月14日	5. 情報ネットワークシステムによる情報連携 法令上の根拠	<p>1. 番号利用法第19条第7号(特定個人情報の提供の制限)及び別表第二(別表第二における情報提供の根拠) 第三欄(情報提供者)が「市町村長」の項のうち、第四欄(特定個人情報)に「新型コロナウイルス等対策特別措置法(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情報であって主務省令で定めるものが含まれる項(115の2の項) (別表第二における情報照会の根拠) 第一欄(情報照会者)が「市町村長」の項のうち、第二欄(事務)に「新型コロナウイルス等対策特別措置法(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が含まれる項(115の2の項) 2. 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(別表第二省令) (平成26年内閣府・総務省令第7号) (別表第二主務省令における情報提供の根拠) ・別表第二省令(第59条の2) (※別表第二の115の2の項) (別表第二主務省令における情報照会の根拠) ・別表第二省令(第59条の2) (※別表第二の115の2の項)</p>	<p>1. 番号利用法第19条第6号(特定個人情報の提供の制限)及び別表第二(別表第二における情報提供の根拠) 第三欄(情報提供者)が「市町村長」の項のうち、第四欄(特定個人情報)に「新型コロナウイルス等対策特別措置法(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情報であって主務省令で定めるものが含まれる項(115の2の項) (別表第二における情報照会の根拠) 第一欄(情報照会者)が「市町村長」の項のうち、第二欄(事務)に「新型コロナウイルス等対策特別措置法(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が含まれる項(115の2の項) 2. 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(別表第二省令) (平成26年内閣府・総務省令第7号) (別表第二主務省令における情報提供の根拠) ・別表第二省令(第59条の2) (※別表第二の115の2の項) (別表第二主務省令における情報照会の根拠) ・別表第二省令(第59条の2) (※別表第二の115の2の項)</p>	事後	特定個人情報保護評価書の見直しを実施
令和4年5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 ⑤使用方法 情報の突合	<p>住民からの費用助成申請書等の内容と地方税関係情報を突合する。</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＞ 当市区町村からの転出者について、当市区町村での接種記録を転出先市区町村に提供するために、転出先市区町村から個人番号を入手し、当市区町村の接種記録と突合する。</p>	<p>住民からの費用助成申請書等の内容と地方税関係情報を突合する。</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＞ 当市区町村からの転出者について、当市区町村での接種記録を転出先市区町村に提供するために、他市区町村から個人番号を入手し、当市区町村の接種記録と突合する。</p>	事後	法改正に基づく変更
令和4年5月30日	II 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ②委託先における取扱者数	10人未満	10人以上50人未満	事後	法改正に基づく変更
令和4年5月30日	(別添1) ファイル記録項目 ＜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＞	<p>＜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 ・宛名番号 ・自治体コード ・接種券番号 ・属性情報(氏名、生年月日、性別) ・接種状況(実施/未実施) ・接種回(1回目/2回目) ・接種日 ・ワクチンメーカー ・ロット番号 ・ワクチン種類(※) ・製品名(※) ・旅券関係情報(旧姓・別姓・別名、ローマ字氏名、国籍、旅券番号)(※) ・証明書ID(※) ・証明書発行年月日(※) ※ 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</p>	<p>＜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 ・宛名番号 ・自治体コード ・接種券番号 ・属性情報(氏名、生年月日、性別) ・接種状況(実施/未実施) ・接種回(1回目/2回目/3回目) ・接種日 ・ワクチンメーカー ・ロット番号 ・ワクチン種類(※) ・製品名(※) ・旅券関係情報(旧姓・別姓・別名、ローマ字氏名、国籍、旅券番号)(※) ・証明書ID(※) ・証明書発行年月日(※) ※ 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</p>	事後	法改正に基づく変更

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4年5月30日	Ⅲ リスク対策 2.特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。) リスクに対する措置の内容 〈新型コロナウイルス感染症対策に係る予防接種事務における追加措置〉 ②転出先市区町村からの個人番号の入手	〈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〉 ②転出先市区町村からの個人番号の入手 当市区町村からの転出者について、当市区町村での接種記録を転出先市区町へ提供するため、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、住民基本台帳等により照会対象者の個人番号であることを確認した上で、ワクチン接種記録システムを通じて入手する。	〈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〉 ②他市区町村からの個人番号の入手 当市区町村からの転出者について、当市区町村での接種記録を転出先市区町へ提供するため、他市区町村から個人番号を入手するが、その際は、他市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認した上で、ワクチン接種記録システムを通じて入手する。	事後	法改正に基づく変更
令和4年7月22日	Ⅰ 基本情報 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 ②システムの機能	・ワクチン接種記録システムへの接種対象者・接種券発行登録 ・接種記録の管理 ・転出/死亡時等のフラグ設定 ・他市区町村への接種記録の照会・提供 ・新型コロナウイルス感染症予防接種証明書の交付に係る接種記録の照会 ・新型コロナウイルス感染症予防接種証明書の電子申請受付・電子交付の実施	・ワクチン接種記録システムへの接種対象者・接種券発行登録 ・接種記録の管理 ・転出/死亡時等のフラグ設定 ・他市区町村への接種記録の照会・提供 ・新型コロナウイルス感染症予防接種証明書の交付に係る接種記録の照会 ・新型コロナウイルス感染症予防接種証明書の電子申請受付・電子交付の実施 ・新型コロナウイルス感染症予防接種証明書のコンビニ交付の実施	事前	接種証明書のコンビニ交付制度開始前に伴う変更
令和4年7月22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 ②入手方法	[○] その他 住民基本台帳ネットワークシステム、ワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能を含む。)	[○] その他 住民基本台帳ネットワークシステム、ワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能を含む。)、コンビニエンスストア等のキオスク端末及び証明書交付センターシステム	事前	接種証明書のコンビニ交付制度開始前に伴う変更
令和4年7月22日	Ⅱ 特定個人情報ファイルの概要 4.特定個人情報ファイルの取扱いの委託 委託事項1	システム保守業務 〈新型コロナウイルス感染症対策に係る予防接種事務〉 〈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)(新型コロナウイルス感染症予防接種証明書電子交付機能を含む。))を用いた特定個人情報ファイルの管理等	システム保守業務 〈新型コロナウイルス感染症対策に係る予防接種事務〉 〈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)(新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。))を用いた特定個人情報ファイルの管理等	事前	接種証明書のコンビニ交付制度開始前に伴う変更
令和4年7月22日	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ①委託内容	システム保守業務 〈新型コロナウイルス感染症対策に係る予防接種事務〉 〈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)(新型コロナウイルス感染症予防接種証明書電子交付機能を含む。))を用いた特定個人情報ファイルの管理等	システム保守業務 〈新型コロナウイルス感染症対策に係る予防接種事務〉 〈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)(新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。))を用いた特定個人情報ファイルの管理等	事前	接種証明書のコンビニ交付制度開始前に伴う変更
令和4年7月22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	情報・統計課サーバー室及び株式会社TKCのデータセンター 〈ワクチン接種記録システムにおける追加措置〉 ワクチン接種記録システムは、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。なお、以下のとおりセキュリティ対策を講じている。 ・論理的に区分された当市区町村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。 ・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。 (新型コロナウイルス感染症予防接種証明書電子交付機能) 電子交付アプリ及び同アプリの利用端末には、申請情報を記録しないこととしている。	情報・統計課サーバー室及び株式会社TKCのデータセンター 〈ワクチン接種記録システムにおける追加措置〉 ワクチン接種記録システムは、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。なお、以下のとおりセキュリティ対策を講じている。 ・論理的に区分された当市区町村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。 ・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。 (新型コロナウイルス感染症予防接種証明書電子交付機能) 電子交付アプリ及び同アプリの利用端末には、申請情報を記録しないこととしている。 (新型コロナウイルス感染症予防接種証明書コンビニ交付) 証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。	事前	接種証明書のコンビニ交付制度開始前に伴う変更
令和4年7月22日	Ⅲ リスク対策 2.特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く) リスク: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	・住民からの申告・申請情報の入手については、本人確認や個人番号の真正性確認を実施している。 ・市町村CSからの住登外情報については、職員2名以上でダブルチェックを行って対象者を確定した上で情報を入手している。 ・庁内連携機能からの各種照会情報の入手については、個人単位の操作ログを取得し追跡可能な形式で管理しており、対象者以外の情報の入手の抑止を図っている。	・住民からの申告・申請情報の入手については、本人確認や個人番号の真正性確認を実施している。 ・市町村CSからの住登外情報については、職員2名以上でダブルチェックを行って対象者を確定した上で情報を入手している。 ・庁内連携機能からの各種照会情報の入手については、個人単位の操作ログを取得し追跡可能な形式で管理しており、対象者以外の情報の入手の抑止を図っている。	事前	接種証明書のコンビニ交付制度開始前に伴う変更
令和4年7月22日	Ⅲ リスク対策 2.特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く) 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。) 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における追加措置〉 (略) 〈新型コロナウイルス感染症予防接種証明書電子交付機能〉 (略)	〈ワクチン接種記録システムにおける追加措置〉 (略) (新型コロナウイルス感染症予防接種証明書電子交付機能) (略) (新型コロナウイルス感染症予防接種証明書コンビニ交付) ・個人番号カードの読み取りにより必要な情報を入手し、申請者の自由入力を受けることで、交付申請者が不要な情報を送信してしまうリスクを防止する。 ・証明書交付センターにおいてキオスク端末の操作画面を制御し、コンビニ交付に対応する市町村に対してのみキオスク端末から交付申請を可能とすることで、意図しない不適切な方法で特定個人情報が発送されることを避ける。 ・個人番号カードのICチップ読み取り(券面事項入力補助AP)と暗証番号入力(券面事項入力補助APの暗証番号)による二要素認証で本人確認を行うため、本人からの情報のみが発信される。 ・券面入力補助APを活用し、個人番号カード内の記憶領域に格納された個人番号を申請情報として自動的に入力することにより、不正確な個人番号の入力を抑制する措置を講じている。 ・券面事項入力補助APから取得する情報(4情報・マイナンバー)に付されている署名について、証明書交付センターシステムにおいて真正性の検証を行い、送信情報の真正性を確認する措置を講じている。	事前	接種証明書のコンビニ交付制度開始前に伴う変更
令和4年7月22日			・キオスク端末と証明書交付センターシステム間の通信については、専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。また、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。さらに、キオスク端末の画面表示や音声案内により、マイナンバーカード及び証明書の取り忘れ防止対策を実施する。		

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4年7月22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 その他の措置の内容	<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> <p>当市区町村、国、当該システムの運用保守事業者の三者の関係を規定した「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）（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）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。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 ・新型コロナウイルス感染症予防接種証明書電子交付機能において、申請者本人から特定個人情報の提供を受ける際の入手に係る保護措置 	<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> <p>当市区町村、国、当該システムの運用保守事業者の三者の関係を規定した「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）（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）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。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 ・新型コロナウイルス感染症予防接種証明書電子交付機能において、申請者本人から特定個人情報の提供を受ける際の入手に係る保護措置 	事前	接種証明書のコンビニ交付制度開始前に伴う変更
令和4年7月22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	<p>＜ワクチン接種記録システムにおける措置＞</p> <p>【物理的対策】 （略）</p> <p>【技術的対策】 （略） （新型コロナウイルス感染症予防接種証明書電子交付機能） （略）</p>	<p>＜ワクチン接種記録システムにおける措置＞</p> <p>【物理的対策】 （略）</p> <p>【技術的対策】 （略） （新型コロナウイルス感染症予防接種証明書電子交付機能） （略） （新型コロナウイルス感染症予防接種証明書コンビニ交付） ・証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。 ・キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。また、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。</p>	事前	接種証明書のコンビニ交付制度開始前に伴う変更
令和6年3月22日	表紙公表日	2023/2/10	2024/3/22	事後	特定個人情報保護評価書の見直しを実施
令和7年2月28日	I 基本情報 4. 個人番号の利用		・番号法第9条第1項及び別表の126の項	事後	データ標準レイアウト改版に伴う申請をしたため
令和7年2月28日	表紙公表日	2024/3/22	2025/2/28	事後	特定個人情報保護評価書の見直しを実施
令和7年3月25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		<p>＜ガバメントクラウドにおける措置＞</p> <p>●消去方法 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壊等を実施する。</p> <p>●消去手順 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。</p> <p>●物理的対策 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な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。</p> <p>●技術的対策 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【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。 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。 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</p>	事後	ガバメントクラウド利用開始に伴う変更
令和7年3月25日	Ⅲ リスク対策 10. その他のリスク対策		<p>＜ガバメントクラウドにおける措置＞</p> <p>・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。</p> <p>・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。</p> <p>・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。</p> <p>・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。</p>	事後	ガバメントクラウド利用開始に伴う変更
令和7年3月25日	I 基本情報 1. 特定個人情報ファイルを取り扱う事務 ②事務の内容	<p>新型コロナウイルス感染症予防接種証明書交付事務</p> <ul style="list-style-type: none"> ・ワクチン接種記録システム（VRS）へ予防接種対象者及び発行した接種券の登録を行う。 ・予防接種の実施後に接種記録等を登録、管理し、他市区町村へ接種記録の照会・提供を行う。 ・接種者からの申請に基づき、臨時接種時の新型コロナウイルス感染症予防接種証明書の交付を行う。 		事後	特定個人情報保護評価書の見直しを実施

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7年3月25日	I 基本情報 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4 ①システムの名称	ワクチン接種記録システム（VRS）		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25日	I 基本情報 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4 ①システムの機能	・ワクチン接種記録システムへの接種対象者・接種券発行登録 ・接種記録の管理 ・転出/死亡時等のフラグ設定 ・他市区町村への接種記録の照会・提供 ・新型コロナウイルス感染症予防接種証明書の交付に係る接種記録の照会 ・新型コロナウイルス感染症予防接種証明書の電子申請受付・電子交付の実施 ・新型コロナウイルス感染症予防接種証明書のコンビニ交付の実施		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25日	I 基本情報 4. 個人番号の利用 法令上の根拠	【新型コロナウイルス感染症対策に係る予防接種事務】 ・番号法第19条第16号（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ワクチン接種記録システムを用いた情報提供・照会のみ） ・番号法第19条第6号（委託先への提供）		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25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	【新型コロナウイルス感染症対策に係る予防接種事務】 （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25の項、27の項、28の項、29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25の項、26の項		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25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 ⑤使用方法	＜新型コロナウイルス感染症対策に係る予防接種事務＞ ・当市区町村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とともに、接種券の発行のために特定個人情報を使用する。 ・当市区町村からの転出者について、転出先市区町村へ当市区町村での接種記録を提供するために特定個人情報を使用する。 ・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使用する。		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25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 ⑤使用方法	住民からの費用助成申請書等の内容と地方税関係情報を突合する。 ＜新型コロナウイルス感染症対策に係る予防接種事務＞ 当市区町村からの転出者について、当市区町村での接種記録を転出先市区町村に提供するために、他市区町村から個人番号を入手し、当市区町村の接種記録と突合する。		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25日	II 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1	＜新型コロナウイルス感染症対策に係る予防接種事務＞ 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）（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）を用いた特定個人情報ファイルの管理等		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25日	II 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 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＞ 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）（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）を用いた特定個人情報ファイルの管理等		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25日	II 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ①委託先名	＜新型コロナウイルス感染症対策に係る予防接種事務＞ 株式会社ミラボ		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25日	II 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ①委託先名	＜新型コロナウイルス感染症対策に係る予防接種事務＞ 株式会社ミラボ		事後	特定個人情報保護評価書の見直しを実施

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7年3月25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	<ワクチン接種記録システムにおける追加措置> ワクチン接種記録システムは、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。なお、以下のとおりセキュリティ対策を講じている。 ・論理的に区分された当市区町村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。 ・県、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。 (新型コロナウイルス感染症予防接種証明書電子交付機能) 電子交付アプリ及び同アプリの利用端末には、申請情報を記録しないこととしている。 (新型コロナウイルス感染症予防接種証明書コンビニ交付) 証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25日	Ⅱ 特定個人情報ファイルの概要 7. 備考	<ワクチン接種記録システムにおける追加措置> ・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。 ※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。		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25日	(別添1) 特定個人情報ファイル記録項目	<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 ・宛名番号 ・自治体コード ・接種券番号 ・属性情報(氏名、生年月日、性別) ・接種状況(実施/未実施) ・接種回(1回目/2回目/3回目) ・接種日 ・ワクチンメーカー ・ロット番号 ・ワクチン種類(※) ・製品名(※) ・旅券関係情報(旧姓・別姓・別名、ローマ字氏名、国籍、旅券番号)(※) ・証明書ID(※) ・証明書発行年月日(※)		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25日	Ⅲ リスク対策 2. 特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。) リスクに対する措置の内容	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ① 転入者本人からの個人番号の入手 当市区町村の転入者について、転出元市区町村へ接種記録を照会するために、本人から個人番号を入力する場合又は、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。 ② 他市区町村からの個人番号の入手 当市区町村からの転出者について、当市区町村での接種記録を転出先市区町へ提供するため、他市区町村から個人番号を入力するが、その際は、他市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認した上で、ワクチン接種記録システムを通じて入手する。 ③ 転出元市区町村からの接種記録の入手 当市区町村への転入者について、転出元市区町村から接種記録を入力するが、その際は、当市区町村において住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム(VRS)を通じて入手する。 ④ 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力するのは、接種者から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。 (新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付) 交付申請には、個人番号カードのICチップ読み取り(券面事項入力補助AP)と暗証番号入力(券面事項入力補助APの暗証番号)による二要素認証を必須とすることで、対象者以外の情報の入手を防止する。		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25日	Ⅲ リスク対策 2. 特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。) 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固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。 ・ワクチン接種記録システムのデータベースは、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。 ・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。 (新型コロナウイルス感染症予防接種証明書電子交付機能) ・個人番号カードや旅券の読み取りにより必要な情報を入手し、申請者の自由入力を受けることで、交付申請者が不要な情報を送信してしまうリスクを防止する。 ・当該機能では、専用アプリからのみ交付申請を可能とする。アプリの改ざん防止措置を講じることで、意図しない不適切な方法で特定個人情報送信されることを避ける。 ・個人番号カードのICチップ読み取り(券面事項入力補助AP)と暗証番号入力(券面事項入力補助APの暗証番号)による二要素認証で本人確認を行うため、本人からの情報のみが送信される。 ・券面入力補助APを活用し、個人番号カード内の記憶領域に格納された個人番号を申請情報として自動的に入力することにより、不正確な個人番号の入力を抑止する措置を講じている。 ・券面事項入力補助APから取得する情報(4情報・マイナンバー)に付されている署名について、VRSにおいて真正性の検証を行い、送信情報の真正性を確認する措置を講じている。 ・電子交付アプリとVRS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。 (新型コロナウイルス感染症予防接種証明書コンビニ交付) ・個人番号カードの読み取りにより必要な情報を入手し、申請者の自由入力を受けることで、交付申請者が不要な情報を送信してしまうリスクを防止する。 ・証明書交付センターにおいてキオスク端末の操作画面を制御し、コンビニ交付に対応する市町村に対してのみキオスク端末から交付申請を可能とすることで、意図しない不適切な方法で特定個人情報が送信されることを避ける。 ・個人番号カードのICチップ読み取り(券面事項入力補助AP)と暗証番号入力(券面事項入力補助APの暗証番号)による二要素認証で本人確認を行うため、本人からの情報のみが送信される。 ・券面入力補助APを活用し、個人番号カード内の記憶領域に格納された個人番号を申請情報として自動的に入力することにより、不正確な個人番号の入力を抑止する措置を講じている。 ・券面事項入力補助APから取得する情報(4情報・マイナンバー)に付されている署名について、証明書交付センターシステムにおいて真正性の検証を行い、送信情報の真正性を確認する措置を講じている。 ・キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはI-GWAN		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25日	Ⅲ リスク対策 3. 特定個人情報の使用 リスクに対する措置の内容	<ワクチン接種記録システムにおける追加措置> ・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に接続できるが、個人番号にはアクセスできないように制御している。		事後	特定個人情報保護評価書の見直しを実施

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7年3月25日	Ⅲ リスク対策 3.特定個人情報の使用 具体的な管理方法	＜ワクチン接種記録システムにおける追加措置＞ 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。 ・ワクチン接種記録システム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		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25日	Ⅲ リスク対策 3.特定個人情報の使用 その他の措置の内容	＜ワクチン接種記録システムにおける追加措置＞ 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。		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25日	Ⅲ リスク対策 3.特定個人情報の使用 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	＜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住民基本台帳システムや予防接種台帳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へ登録する際には、以下のようにしている。 ・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、媒体管理簿等に使用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。 ②特定個人情報を使用する場を、必要最小限に限定している。具体的に以下の3つの場面に限定している。 ・当市区町村の転入者について、転出元市区町村へ接種記録を照会する場合のみ入手し、使用する。 ・当市区町村からの転出者について、当市区町村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。 ③ワクチン接種記録システムから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。		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25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	＜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＞ 当市区町村、国、当該システムの運用保守事業者の三者の間を規定した「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）（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）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。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。 ・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 ・新型コロナウイルス感染症予防接種証明書電子交付機能において、申請者本人から特定個人情報の提供を受ける際の入手に係る保護措置		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25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	＜ワクチン接種記録システムにおける措置＞ 【物理的対策】 ワクチン接種記録システムは、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。主に以下の物理的対策を講じている。 ・サーバ設置場所等への入退室記録管理、施設管理 ・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。 【技術的対策】 ワクチン接種記録システムは、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。主に以下の技術的対策を講じている。 ・論理的に区分された当市区町村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の防止のため、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。 （新型コロナウイルス感染症予防接種証明書電子交付機能） ・電子交付アプリには、申請情報を記録しないこととしている。 ・電子交付アプリとVRS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。 （新型コロナウイルス感染症予防接種証明書コンビニ交付） ・証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。 ・キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLG WAN回線を使用し、情報漏えいを防止する。また、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。		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25日	Ⅲ リスク対策 9.従業者に対する教育・啓発 具体的な方法	＜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＞ デジタル庁（旧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。		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25日	Ⅲ リスク対策 10. その他のリスク対策	＜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＞ デジタル庁（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。		事後	特定個人情報保護評価書の見直しを実施
令和7年3月25日	表紙公表日	2025/2/28	2025/3/25	事後	特定個人情報保護評価書の見直しを実施

[illegible]