

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
24	新型コロナウイルス感染症に係る予防接種に関する事務 重点項目評価書【令和7年2月28日終了】

個人のプライバシー等の権利利益の保護の宣言

春日部市は、新型コロナウイルス感染症に係る予防接種に関する事務における特定個人情報ファイルの取扱いに当たり、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、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て、個人のプライバシー等の権利利益の保護に取り組んでいることを、ここに宣言する。

特記事項	
------	--

評価実施機関名

春日部市長

公表日

令和5年12月8日

[平成30年5月 様式3]

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	新型コロナウイルス感染症に係る予防接種に関する事務
②事務の内容	<p>春日部市(以下「本市」という。)は、予防接種法(昭和23年法律第68号)及び行政手続における特定の個人を識別するための番号の利用等に関する法律(以下「番号法」という。)の規定に従い、特定個人情報を以下の事務で取り扱う。</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</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。 ・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。
③対象人数	<div style="text-align: right;">＜選択肢＞</div> <div style="display: flex; justify-content: space-between;"> [10万人以上30万人未満] <div> 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 </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	ワクチン接種記録システム(VRS)
②システムの機能	<ul style="list-style-type: none"> ・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
③他のシステムとの接続	<div style="display: flex; flex-wrap: wrap;"> <div style="width: 50%;">[] 情報提供ネットワークシステム</div> <div style="width: 50%;">[] 庁内連携システム</div> <div style="width: 50%;">[] 住民基本台帳ネットワークシステム</div> <div style="width: 50%;">[] 既存住民基本台帳システム</div> <div style="width: 50%;">[] 宛名システム等</div> <div style="width: 50%;">[] 税務システム</div> <div style="width: 50%;">[] その他 ()</div> </div>
システム2～5	
システム2	
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>健康管理システム</p> <p>1. 入力機能 予防接種の接種内容の入力や管理。</p> <p>2. データ照会機能 予防接種の接種内容の確認</p> <p>3. データ抽出機能 予防接種の接種内容の検索、抽出</p>
③他のシステムとの接続	<div style="display: flex; flex-wrap: wrap;"> <div style="width: 50%;">[] 情報提供ネットワークシステム</div> <div style="width: 50%;">[] 庁内連携システム</div> <div style="width: 50%;">[] 住民基本台帳ネットワークシステム</div> <div style="width: 50%;">[○] 既存住民基本台帳システム</div> <div style="width: 50%;">[] 宛名システム等</div> <div style="width: 50%;">[] 税務システム</div> <div style="width: 50%;">[○] その他 (団体内統合宛名システム)</div> </div>

システム3	
①システムの名称	団体内統合宛名システム
②システムの機能	<p>1. 団体内統合宛名番号の付番と管理 :各業務・システムで保有している宛名番号を団体内で統一し、個人を識別するための団体内統合宛名番号を付番し、各業務・システムの宛名番号と団体内宛名番号、基本情報、個人番号を紐付けて、格納・管理する。</p> <p>2. 符号取得支援・確認 :処理通番の発行依頼を中間サーバーに通知し、符号が取得できたか確認を行う。</p> <p>3. 情報提供機能 :中間サーバーへ特定個人情報を登録するために、各業務・システムのデータを変換し、中間サーバーへ提供情報を通知する。</p> <p>4. 情報照会機能 :各業務・システムに代わって、他機関の特定個人情報の照会について、宛名番号と団体内統合宛名番号の変換、データ形式等の変換を行い、中間サーバーへ照会情報を通知する。</p> <p>5. 宛名情報照会 :団体内統合宛名番号、個人番号、又は基本情報を検索キーとして、個人情報を照会する。</p> <p>6. 個人番号へのアクセス制御</p>
③他のシステムとの接続	<div> <div> <input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> 住民基本台帳ネットワークシステム <input type="checkbox"/> 宛名システム等 <input type="checkbox"/> その他 </div> <div> <input type="checkbox"/> 庁内連携システム <input type="checkbox"/> 既存住民基本台帳システム <input type="checkbox"/> 税務システム (国民健康保険(税)(資格)(給付)システム、児童手当システム等の各業務・システム、中間サーバー) </div> </div>

システム4	
①システムの名称	中間サーバー
②システムの機能	<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の受領(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、共通基盤(連携・統合宛名)及び既存住民基本台帳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> <p>8. セキュリティ管理機能 : 特定個人情報(連携対象)の暗号化及び復号や、電文への署名付与、電文及び情報提供許可証に付与されている署名の検証、それらに伴う鍵管理を行う。また、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)から受信した情報提供NWS 配信マスター情報を管理する。</p> <p>9. 職員認証・権限管理機能 : 中間サーバーを利用する職員の認証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。</p> <p>10. システム管理機能 : バッチの状況管理、業務統計情報の集計、稼動状態の通知、保管期限切れ情報の削除を行う。</p>
③他のシステムとの接続	<div style="display: flex; justify-content: space-between;"> <div> <input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> 住民基本台帳ネットワークシステム <input type="checkbox"/> 宛名システム等 <input type="checkbox"/> その他 (団体内統合宛名システム) </div> <div> <input type="checkbox"/> 庁内連携システム <input type="checkbox"/> 既存住民基本台帳システム <input type="checkbox"/> 税務システム </div> </div>
3. 特定個人情報ファイル名	
新型コロナウイルスワクチン接種記録ファイル	
4. 個人番号の利用 ※	
法令上の根拠	<ul style="list-style-type: none"> ・番号法第9条第1項 別表第一の10の項 ・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)
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	<div style="display: flex; justify-content: space-between;"> <div> <input type="checkbox"/> 実施する </div> <div> <選択肢> 1) 実施する 2) 実施しない 3) 未定 </div> </div>
②法令上の根拠	(情報提供) 番号法第19条第8号、別表第二の16の2項、16の3項 (情報照会) 番号法第19条第8号、別表第二の16の2項、17項、18項、19項
6. 評価実施機関における担当部署	
①部署	健康保険部健康課新型コロナウイルスワクチン接種担当
②所属長の役職名	参事兼新型コロナウイルスワクチン接種担当課長
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	
新型コロナウイルスワクチン接種記録ファイル	
2. 基本情報	
①ファイルの種類 ※	[システム用ファイル] <div style="text-align: 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="text-align: 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 ※	春日部市に住所を有する新型コロナウイルス感染症に係るワクチン接種の対象者
その必要性	ワクチン接種の実施、および接種記録の適正な管理のため
④記録される項目	[10項目以上50項目未満] <div style="text-align: 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 ※	・識別情報 [<input type="radio"/>] 個人番号 [<input type="checkbox"/>] 個人番号対応符号 [<input type="radio"/>] その他識別情報(内部番号) ・連絡先等情報 [<input type="radio"/>] 4情報(氏名、性別、生年月日、住所) [<input type="radio"/>] 連絡先(電話番号等) [<input type="radio"/>] その他住民票関係情報 ・業務関係情報 [<input type="checkbox"/>] 国税関係情報 [<input type="checkbox"/>] 地方税関係情報 [<input type="radio"/>] 健康・医療関係情報 [<input type="checkbox"/>] 医療保険関係情報 [<input type="checkbox"/>] 児童福祉・子育て関係情報 [<input type="checkbox"/>] 障害者福祉関係情報 [<input type="checkbox"/>] 生活保護・社会福祉関係情報 [<input type="checkbox"/>] 介護・高齢者福祉関係情報 [<input type="checkbox"/>] 雇用・労働関係情報 [<input type="checkbox"/>] 年金関係情報 [<input type="checkbox"/>] 学校・教育関係情報 [<input type="checkbox"/>] 災害関係情報 [<input type="checkbox"/>] その他 ()
その妥当性	<個人番号、その他識別情報(内部番号)> ・本人確認等、対象者を正確に特定するために保有 <4情報、その他住民票関係情報> ・接種券発行、その他本人情報を把握するために保有 <健康・医療関係情報(ワクチン接種に関する情報)> ・ワクチン接種の接種実績等を把握するために保有
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	健康保険部 健康課 新型コロナウイルスワクチン接種担当

3. 特定個人情報の入手・使用		
①入手元 ※		<input type="checkbox"/> 本人又は本人の代理人 <input type="checkbox"/> 評価実施機関内の他部署 () <input type="checkbox"/> 行政機関・独立行政法人等 (地方公共団体情報システム機構) <input type="checkbox"/> 地方公共団体・地方独立行政法人 (他自治体) <input type="checkbox"/> 民間事業者 () <input type="checkbox"/> その他 (ワクチン接種記録システム(VRS))
②入手方法		<input type="checkbox"/> 紙 <input type="checkbox"/> 電子記録媒体(フラッシュメモリを除く。) <input type="checkbox"/> フラッシュメモリ <input type="checkbox"/> 電子メール <input type="checkbox"/> 専用線 <input type="checkbox"/> 庁内連携システム <input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> その他 (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)
③使用目的 ※		新型コロナウイルス感染症に係る予防接種に関する事務の実施において、住民情報、予防接種歴情報の照会、入力等が必要なため
④使用の主体	使用部署	健康保険部 健康課 新型コロナウイルスワクチン接種担当
	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		<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。
	情報の突合	<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。
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 style="display: flex; align-items: center;"> <div style="margin-right: 10px;">[委託する]</div> <div> <選択肢> 1) 委託する 2) 委託しない (3) 件 </div> </div>
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
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)(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
②委託先における取扱者数		<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>
③委託先名		株式会社ミラボ
再委託	④再委託の有無 ※	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">[再委託しない]</div> <div> <選択肢> 1) 再委託する 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	・システムのオペレーション業務及びシステムの運用・保守業務、法制度改正に伴う改修作業業務	
①委託内容	・システムのオペレーション業務及びシステムの運用・保守業務、法制度改正に伴う改修作業	
②委託先における取扱者数	<div style="display: flex; align-items: center;"> <div style="border: 1px solid black; padding: 2px 10px; margin-right: 10px;">10人以上50人未満</div> <div style="text-align: right;"> <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>	
③委託先名	株式会社 ジーシーシー 埼玉支社	
再委託	④再委託の有無 ※ <div style="display: flex; align-items: center; margin-top: 5px;"> <div style="border: 1px solid black; padding: 2px 10px; margin-right: 10px;">再委託する</div> <div style="text-align: right;"> <選択肢> 1) 再委託する 2) 再委託しない </div> </div>	
	⑤再委託の許諾方法 以下の事項について、委託先から、下記を記載した書面の提出を受け、許諾を判断している。 ・再委託の必要性 ・再委託先の選定基準 ・再委託先の再委託管理方法 ・再委託先の名称、代表者及び所在地 ・再委託する業務の内容 ・再委託する業務に含まれる情報の種類 ・再委託先のセキュリティ管理体制 等	
	⑥再委託事項 システムの運用・保守業務の一部	
委託事項3		
①委託内容	特定個人情報データの滅失等に備えたバックアップデータの保管委託	
②委託先における取扱者数	<div style="display: flex; align-items: center;"> <div style="border: 1px solid black; padding: 2px 10px; margin-right: 10px;">10人未満</div> <div style="text-align: right;"> <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>	
③委託先名	東武デリバリー株式会社	
再委託	④再委託の有無 ※ <div style="display: flex; align-items: center; margin-top: 5px;"> <div style="border: 1px solid black; padding: 2px 10px; margin-right: 10px;">再委託しない</div> <div style="text-align: right;"> <選択肢> 1) 再委託する 2) 再委託しない </div> </div>	
	⑤再委託の許諾方法	
	⑥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	[<input type="radio"/>] 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	市区町村長
①法令上の根拠	番号法 第19条第16号
②提供先における用途	新型コロナウイルス感染症対策に係る予防接種事務
③提供する情報	市区町村コード及び転入者の個人番号(本人からの同意が得られた場合のみ)
④提供する情報の対象となる本人の数	<div style="text-align: right;">＜選択肢＞</div> <div style="text-align: right;">1) 1万人未満</div> <div style="text-align: right;">2) 1万人以上10万人未満</div> <div style="text-align: right;">3) 10万人以上100万人未満</div> <div style="text-align: right;">4) 100万人以上1,000万人未満</div> <div style="text-align: right;">5) 1,000万人以上</div> <div style="text-align: center;">[10万人以上100万人未満]</div>
⑤提供する情報の対象となる本人の範囲	「2.基本情報③対象者となる本人の範囲」と同じ
⑥提供方法	<div style="display: flex; justify-content: space-between;"> [] 情報提供ネットワークシステム [] 専用線 </div> <div style="display: flex; justify-content: space-between;"> [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) </div> <div style="display: flex; justify-content: space-between;"> [] フラッシュメモリ [] 紙 </div> <div style="text-align: right;">[<input type="radio"/>] その他 (ワクチン接種記録システム(VRS))</div>
⑦時期・頻度	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の照会を行う必要性が生じた都度

提供先2~5

6. 特定個人情報の保管・消去

<p>保管場所 ※</p>	<p>＜本市における措置＞</p> <ul style="list-style-type: none"> ・生体認証を含む二要素認証にて入退室管理をしている管理区域内に設置したサーバー内に保管する。 ・サーバーへのアクセスは、全庁的に管理しているユーザーID／パスワードによる認証が必要。 ・届出書等も保管年限内は、鍵付のキャビネット内での保管を義務付けている。 <p>＜中間サーバープラネットにおける措置＞</p> <ul style="list-style-type: none"> ・中間サーバー・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバー室への入室を厳重に管理する。 ・特定個人情報、サーバー室に設置された中間サーバー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における追加措置＞</p> <p>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。</p> <p>クラウドサービスを利用している。なお、以下のとおりの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。 <p>(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)</p> <p>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。</p> <p>(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)</p> <p>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。</p>
---------------	---

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。

(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
- ・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

Ⅲ リスク対策 ※(7. ②を除く。)

1. 特定個人情報ファイル名		
新型コロナウイルスワクチン接種記録ファイル		
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）		
リスク： 目的外の入手が行われるリスク		
リスクに対する措置の内容	<p>・システムを利用する職員はパスワード及び生体認証によりログインしている。</p> <p>・システム上、必要項目以外は取り込めないようになっている。</p> <p>・庁内からの住基情報等の入手にあたっては、既存住基システム、各業務・システムの庁内データ連携機能のシステム連携仕様に基づくため、対象者以外の情報を入手することはない。</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＞</p> <p>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手する場合は、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。</p> <p>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。</p> <p>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手するが、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。</p> <p>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手するのは、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。</p> <p>(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。</p>	
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

・不適切な方法で入手が行われるリスクに対する措置

：庁内連携機能からの住基情報等の入手については、入退室管理をしている管理区域内のサーバー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。

：庁内連携機能からの各種照会情報の入手については、接続可能なシステムをあらかじめ登録し、許可された業務・システムに限定した入手方法とすることで、対象外の業務・システムからの入手が行われないようにしている。

：健康管理システムは利用できる職員を限定している。また、パスワード/生体認証による認証を行い、アクセス権を持た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。

・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

：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。

・入手の際に特定個人情報が漏えい・紛失するリスクに対する措置

：庁内連携機能からの住基情報、各種照会情報の入手については、入退室管理をしている管理区域内に設置したサーバー間通信に限定することで漏えい・紛失を防止している。

＜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。

・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、申請者の自由入力避けることで、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、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、申請者の自由入力避けることで、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。

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	
リスクに対する措置の内容	<ul style="list-style-type: none"> ・健康管理システムには、予防接種事務に関係のない情報を保有しない。 ・担当外の業務についてはアクセスできないよう制御を行っている。 <p>＜ワクチン接種記録システムにおける追加措置＞</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。
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	<p>[行っている]</p> <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	<ul style="list-style-type: none"> ・システムを利用する職員を特定し、健康管理システムへのアクセスにおいて、パスワード及び生体認証による認証を実施している。 ・パスワード及び生体認証を複数人で共有することを禁止している。 ・パスワード及び生体認証の利用者は必要最小限とし、漏えい等が発生しないように厳重に管理している。 <p>＜ワクチン接種記録システムにおける追加措置＞</p> <p>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へのログイン用のユーザIDは、春日部市が指定する管理者が認めた者に限定して発行される。
その他の措置の内容	<ul style="list-style-type: none"> ・アクセス権限の発効・失効の管理 <ul style="list-style-type: none"> ：パスワード及び生体認証の発行・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。 ：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、適切な者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 <ul style="list-style-type: none"> ：パスワード及び生体認証の利用者は必要最小限とし、漏えい等が発生しないように厳重に管理している。 ：ユーザーIDについては、定期的にチェックを行い、不要なユーザーIDが残存しないようにしている。また、利用期間が明確になったものについては、ユーザー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。 ：上記のアクセス権限の設定は定期的に点検している。 ・特定個人情報の使用の記録 <ul style="list-style-type: none"> ：ユーザーIDとともに、健康管理システムへのアクセス、操作(登録、更新、印刷等)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における追加措置＞</p> <p>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に付与されるアクセス権限は、当市区町村が指定する管理者が必要最小限の権限で発効する。</p> <p>当市区町村が指定する管理者は、定期的又は異動/退職等のイベントが発生したタイミングで、権限を有していた職員の異動/退職等情報を確認し、当該事由が生じた際には速やかにアクセス権限を更新し、当該ユーザIDを失効させる。</p> <p>やむを得ず、複数の職員が共有するID(以下「共用ID」という。)を発行する必要がある場合は、当該IDを使用する職員・端末を特定し、管理者が把握した上で、パスワードを厳重に管理する運用を徹底し、必要最小限に発行する。なお、共用IDを使用する職員及び端末について、異動/退職等のイベントが発生したタイミングで確認し、当該事由が生じた際は速やかに把握している内容を更新する。</p> <p>当市区町村が指定する管理者は、定期的にユーザID及びアクセス権限の一覧をシステムにおいて確認し、アクセス権限及び不正利用の有無を確認する。また、不要となったユーザIDやアクセス権限を速やかに変更又は削除する。</p> <p>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。ログは定期に及び必要に応じ随時に確認する。</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
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		
<p>・従業者が事務外で使用するリスクに対する措置</p> <p>：外部媒体へのデータのコピーを制御することで、許可なく持ち出せないようにしている。</p> <p>：全職員が、年に1回、個人情報保護に関してのe-ラーニングを受講し、事務外での利用をしないよう周知している。</p> <p>：各種ログを取得しているため、業務外利用をした場合には特定可能であることを職員に周知し、事務外の利用を抑止している。</p> <p>・特定個人情報ファイルが不正に複製されるリスクに対する措置</p> <p>：特定個人情報ファイルの外部媒体への出力は、特定の端末に限定し、特定の記録媒体にのみ許可している。</p> <p>：特定個人情報を記録した紙媒体、DVD等の外部記録媒体は厳重に管理している。また、持出し・持込みのルールを定め、遵守している。</p> <p>：保管期間が経過した特定個人情報を記録した媒体は、復元不可能な状態で確実に消去・廃棄している。</p> <p>：機器を廃棄又はリース返却する場合、機器内部の記憶装置からすべての情報を消去し、復元不可能な状態にする措置を講じている。</p> <p>：業務端末の持出し、私物のPCの接続は禁止している。</p> <p>：画面コピーを取得する際には、個人番号をマスキングしている。</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></p> <p>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。</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。 <p>②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"> ・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。 <p>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。</p>		

4. 特定個人情報ファイルの取扱いの委託		[] 委託しない
リスク： 委託先における不正な使用等のリスク		
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[定めている]	<選択肢> 1) 定めている 2) 定めていない
規定の内容	<ul style="list-style-type: none"> ・目的外利用を禁止する。 ・特定個人情報の閲覧者・更新者を制限する。 ・特定個人情報の提供先を限定する。 ・情報漏洩を防ぐための保管管理に責任を負う。 ・情報が不要となったとき又は要請があったときに情報の返還又は消去などの必要な措置を講じる。 ・必要に応じて、本市が委託先の現地調査を行うことができる。 ・再委託は原則として禁止する。 ・業務上知り得た情報の守秘義務 	
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	[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	<ul style="list-style-type: none"> ・再委託が必要な場合は委託先から事前に再委託の必要性について書面で確認をし、承認を行う。 ・再委託を行う場合には、上記と同様の機密保持契約の遵守を規定しており、委託先から適宜報告を受け、改善の必要がある場合には改善の指示を行い、改善結果の報告を受ける。 	
その他の措置の内容	<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> 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。 <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 	
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		
<ul style="list-style-type: none"> ・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に対する措置 <ul style="list-style-type: none"> ：委託先から他者への特定個人情報の提供は原則として認めないことを契約書上明記する。なお、再委託を行う場合は、再委託先においても委託先と同様の安全管理措置を遵守することを書面にて確認する。また、定期的に特定個人情報の取り扱いについて書面にて報告させ、必要に応じ、本市職員が現地調査することも可能とする。 ：委託先へ特定個人情報を提供する際には、暗号化した上で提供している。 ：委託先へのデータ搬送においては、施錠可能なケースに電子媒体を格納した上で実施することを義務付けている。 ・委託先による特定個人情報の保管・消去、委託契約終了後の不正な使用等に関するリスクに対する措置 <ul style="list-style-type: none"> ：個人情報を記録した媒体（紙、外部記録媒体）の破棄は、再利用できない措置を講じている。 ：情報を記録している記録媒体が不要になった場合、記録媒体の初期化等、情報を復元できないように処置したうえで廃棄している。 ：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、確認を行っている。 ：必要に応じて本市職員が現地調査・確認を行えることとしている。 		

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>＜中間サーバー・ソフトウェアにおける措置＞</p> <p>・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照合リスト(※2)との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。</p> <p>・中間サーバーの職員認証・権限管理機能(※3)では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。</p> <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8号に基づき、事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。</p> <p>(※3) 中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。</p> <p>(「6. 情報提供ネットワークシステムとの接続」の項目全般については、新型コロナウイルス感染症対策に係る予防接種事務以外を記載)</p>				
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: 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>・中間サーバーの仕様に基づき提供するため、不正に特定個人情報が提供されないよう健康管理システムで担保している。</p> <p>＜本市の運用における措置＞</p> <p>・健康管理システムで記録している操作ログは、必要に応じてリストを出力し、確認する。</p> <p>・自動応答不可の特定個人情報の提供に当たっては、所属長の承認を得た上で、提供を実施する運用を行っている。</p> <p>＜中間サーバー・ソフトウェアにおける措置＞</p> <p>・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>・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>・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>・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>				
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に対する措置

<中間サーバー・ソフトウェアにおける措置>

・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>

・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。

・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に対する措置

<中間サーバー・ソフトウェアにおける措置>

・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・紛失するリスクに対する措置

<健康管理システムのソフトウェアにおける措置>

・中間サーバーと健康管理システム間は、管理区域内に設置したサーバー間通信に限定して、漏えい・紛失するリスクを排除している。

<中間サーバー・ソフトウェアにおける措置>

・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(※)。

・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、特定個人情報が漏えい・紛失するリスクを軽減している。

・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>

・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。

・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。

・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に対する措置

<健康管理システムのソフトウェアにおける措置>

・中間サーバーと健康管理システム間は、管理区域内に設置したサーバー間通信に限定しており、他の経路で提供できない。

・健康管理システムは、パスワード及び生体認証に認証を行い、限られた職員のみ操作可能である。

・健康管理システム以外から情報提供できないようシステム上で担保している。

<本市の運用における措置>

・情報提供内容の自動応答が出来ない場合を想定し、手動で情報提供を行う場合は、所属長への確認を行った上で、実施している。

<中間サーバー・ソフトウェアにおける措置>

・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会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>

・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。

・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。

・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に対する措置

＜健康管理システムのソフトウェアにおける措置＞

・健康管理システムの副本登録は、中間サーバーの仕様に基づき設計、テストを行っているため、誤った情報を提供してしまうリスクを排除している。

＜中間サーバー・ソフトウェアにおける措置＞

・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。

(※)特定個人情報を副本として保存・管理する機能。

◆その他の措置

＜中間サーバー・ソフトウェアにおける措置＞

・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＞

・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。

・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。

・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。

・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	[十分に行っている]	＜選択肢＞ 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
②過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	＜選択肢＞ 1) 発生あり 2) 発生なし
その内容		
再発防止策の内容		

その他の措置の内容	<p>◆物理的対策 <本市における措置> ・特定個人情報を保管するサーバー設置場所には、生体認証を含む二要素認証による入退出管理を行っている。 ・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。 ・特定個人情報を保管するサーバーに係る脅威に対して、室温管理、ケーブルの安全管理、耐震対策、防火措置等を講じている。 ・特定個人情報を保管するサーバーは定期保守を実施することで情報の毀損等への対策を図っている。 <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。</p> <p>◆技術的対策 <本市における措置> ・庁舎間の通信には専用線を使用し、外部との通信を行っていない。 ・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。 ・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。 ・定期的にバックアップファイルを取得して、外部記録媒体に記録している。 ・管理区域にある許可された端末以外の業務端末からのデータ持出を不可能にしている。 ・業務端末への外部媒体の接続は、許可された媒体に限定して可能としている。 <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。 ・導入している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> <p><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。 ・サーバー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。</p> <p>【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該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>
リスクへの対策は十分か	<div> <div>[</div> <div>十分である</div> <div>]</div> <div> <div><選択肢></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>

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	
8. 監査	
実施の有無	<input checked="" type="radio"/> 自己点検 <input checked="" type="radio"/> 内部監査 <input type="radio"/> 外部監査
9. 従業者に対する教育・啓発	
従業者に対する教育・啓発	<input type="checkbox"/> 十分に行っている <input type="checkbox"/> 十分に行っていない <div style="margin-left: 20px;"> <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>
具体的な方法	<p><本市における措置> 新規入庁者を対象に行われる研修等で、個人情報保護制度の概要について、周知徹底している。また、毎月、全職員を対象にセキュリティチェックテストを実施している。これにより、セキュリティ意識の啓発及びその理解の程度を確認し、各職員のセキュリティ意識の向上及び自己研鑽に繋がっている。</p> <ul style="list-style-type: none"> ・職員及び事業所内派遣者に対しては、個人情報保護に関する研修等を実施している。 ・年に1回、所属部署のOA担当者に対し、教育を実施している。 ・委託業者に対しては、契約内容に個人情報保護に関する規定を設けている。 <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> 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。</p>
10. その他のリスク対策	
<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> 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。</p>	

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	市政情報課市民相談・情報公開担当 所在地: 〒344-8577 春日部市中央七丁目2番地1 電話: 048-736-1111
②請求方法	指定様式による書面の提出により開示・訂正・利用停止請求を受け付ける。 自己情報開示請求書等に必要事項を記入の上、市政情報課に提出する。本人であることを証明するための書類(運転免許証、パスポート等)の提示が必要。 郵送での請求も可能。 ※春日部市ホームページ上に、請求方法、開示方法、開示請求書の様式等を掲載している。
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	市政情報課市民相談・情報公開担当 所在地: 〒344-8577 春日部市中央七丁目2番地1 電話: 048-736-1111
②対応方法	重要案件の問合せについて、対応記録を残す。 情報漏えい等の重大な事案に関する問合せについて、関係先等に事実確認を行う。

V 評価実施手続

1. 基礎項目評価	
①実施日	令和3年4月1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	—