

# 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
36	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 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

足立区は、新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務の特定個人情報ファイルの取り扱いにあたり、特定個人情報ファイルの取り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

保健衛生システムに係る運用管理業務を外部業者に委託しているが、不正入手・不正使用対策として、業者の情報保護管理体制を確認し、秘密保持に関しても契約に含めることで万全を期している。

## 評価実施機関名

東京都足立区長

## 個人情報保護委員会 承認日【行政機関等のみ】

## 公表日

## 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

# 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
②事務の内容 ※	<p>足立区は、新型インフルエンザ等対策特別措置法及び行政手続き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>新型インフルエンザ等が発生した場合に、特定接種や、住民に対する予防接種、予診票の発行等を行う。番号法第19条第8号に基づき、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において、情報提供ネットワークシステムに接続し、各情報保有機関が保有する特定個人情報について情報連携を行う。情報提供に必要な情報を「副本」として中間サーバーへ登録する。</p> <p>具体的には、特定個人情報ファイルを次の事務に使用する。</p> <p>①住民基本台帳をもとに、予防接種対象者の選定                  ②予防接種実施の登録(予防接種の種類、実施日、実施場所等)                  ③照会申請による予防接種履歴の照会                  ④交付申請による転入者・予診票紛失者への予診票発行等                  ⑤予防接種により健康被害が生じた場合の給付金の支給</p>
③対象人数	<p>[ 30万人以上 ]</p> <p>&lt;選択肢&gt;                  1) 1,000人未満                  2) 1,000人以上1万人未満                  3) 1万人以上10万人未満                  4) 10万人以上30万人未満                  5) 30万人以上</p>

## 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	保健衛生システム
②システムの機能	<ul style="list-style-type: none"> <li>・対象者抽出機能: 予防接種対象者を抽出する。</li> <li>・予防接種入力機能: 個人の予防接種の情報を入力する。</li> <li>・予防接種情報取込: 予防接種のパンチデータを取込する。</li> <li>・予防接種照会: 予防接種の履歴を照会する。</li> <li>・予診票出力: 転入者等の予診票を印刷する。</li> <li>・接種履歴票出力: 個人の予防接種の接種履歴を印刷する。</li> </ul>
③他のシステムとの接続	<p>[ ] 情報提供ネットワークシステム      [ <input checked="" type="checkbox"/> ] 庁内連携システム</p> <p>[ ] 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</p> <p>[ <input checked="" type="checkbox"/> ] 宛名システム等      [ ] 税務システム</p> <p>[ ] その他 ( )</p>

### システム2～5

#### システム2

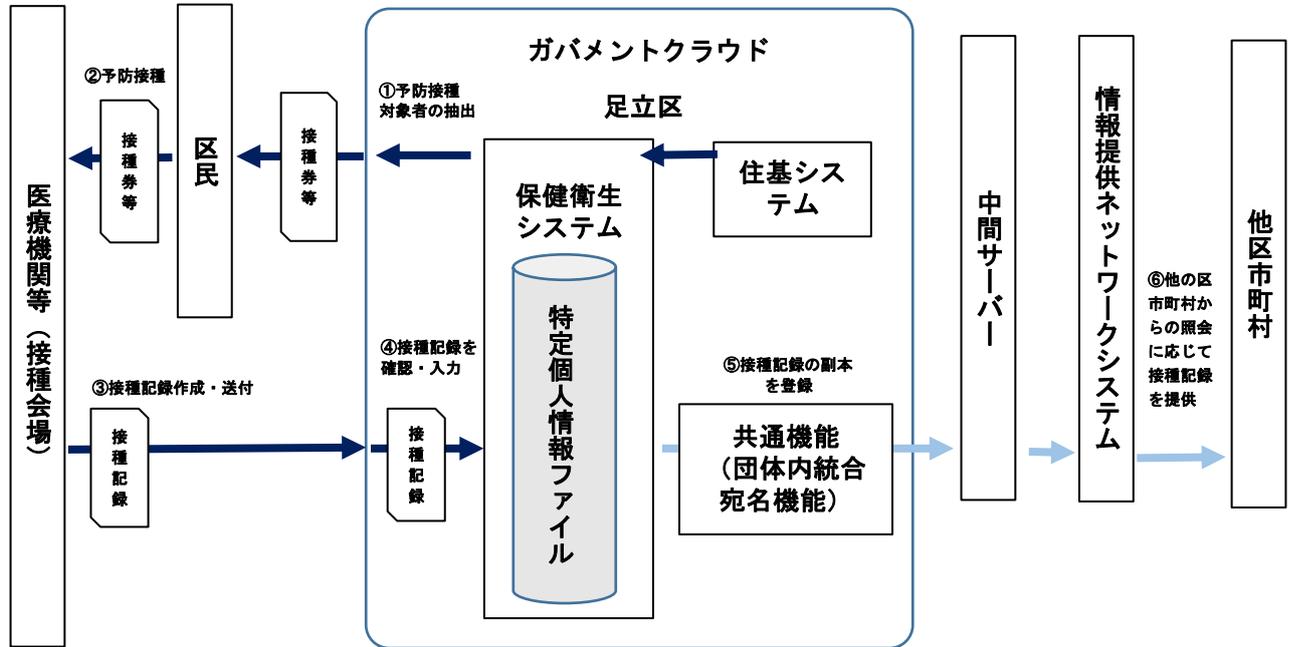
①システムの名称	中間サーバー・プラットフォーム
	<p>※中間サーバー・プラットフォームは、地方公共団体情報システム機構(JLIS)が整備するハードウェアと、国(総務省)が整備する中間サーバー・ソフトウェアから成る。以降の説明において、とくに明記していない場合は、「中間サーバー・プラットフォーム」は中間サーバー・ソフトウェアを含んで機能するシステムを表す。</p>

<p>②システムの機能</p>	<ul style="list-style-type: none"> <li>・符号管理機能 符号管理機能は情報照会、情報提供に用いる個人の識別子である「符号」と、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。</li> <li>・情報照会機能 情報照会機能は、情報提供ネットワークシステムを介して、特定個人情報(連携対象)の情報照会及び情報提供受領(照会した情報の受領)を行う。</li> <li>・情報提供機能 情報提供機能は、情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報(連携対象)の提供を行う。</li> <li>・既存システム接続機能 中間サーバーと既存システム、情報連携プラットフォーム及び住民記録システムとの間で情報照会内容、情報提供内容、特定個人情報(連携対象)、符号取得のための情報等について連携する。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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機能。</li> <li>・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。</li> <li>・システム管理機能 バッチ処理の状況管理、業務統計情報の集計、稼動状態の通知、保管切れ情報の削除を行う。</li> </ul>		
<p>③他のシステムとの接続</p>	<table border="0" style="width: 100%;"> <tr> <td style="width: 50%; vertical-align: top;"> <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 ( ) </td> <td style="width: 50%; vertical-align: top;"> <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 </td> </tr> </table>	<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 ( )	<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
<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 ( )	<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		
<p><b>システム3</b></p>			
<p>①システムの名称</p>	<p>共通機能(団体内統合宛名機能) ※旧「情報連携プラットフォーム」</p>		
<p>②システムの機能</p>	<ol style="list-style-type: none"> <li>1 団体内統合宛名(利用)管理機能 足立区において個人を識別するための団体内統合宛名(利用)番号の管理を行う。 ・団体内統合宛名(利用)番号の符番管理</li> <li>2 情報連携機能 各業務システムと中間サーバー・プラットフォームとの間で発生する各種の要求処理を中継し、情報連携を行うために共通で必要となる情報連携インターフェースを提供する。 ・情報照会要求と照会結果の中継 ・特定個人情報ファイルの登録の中継 ・符号の取得要求 ・中間サーバー・プラットフォームからの氏名、性別、生年月日、住所(以下「4情報」という。)照会への応答 ・自動応答不可・不開示フラグの中継(団体内統合宛名番号単位)</li> </ol>		
<p>③他のシステムとの接続</p>	<table border="0" style="width: 100%;"> <tr> <td style="width: 50%; vertical-align: top;"> <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 ( 保健衛生システム、福祉総合システム等 ) </td> <td style="width: 50%; vertical-align: top;"> <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 </td> </tr> </table>	<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 ( 保健衛生システム、福祉総合システム等 )	<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
<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 ( 保健衛生システム、福祉総合システム等 )	<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		

システム4	
3. 特定個人情報ファイル名	
予防接種情報ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	特定個人情報ファイルを活用することにより、対象者を迅速に把握し、予防接種を実施することが可能となる。
②実現が期待されるメリット	新型インフルエンザ等蔓延防止
5. 個人番号の利用 ※	
法令上の根拠	1 番号法第9条第1項 別表の126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の主務省令で定める事務を定める命令 (平成26年内閣府、総務省令第5号) ・第67条の2 3 番号法第19条第6号
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[ 実施する ] <div style="float: right; text-align: right;">             &lt;選択肢&gt;              1) 実施する              2) 実施しない              3) 未定           </div>
②法令上の根拠	1 番号法第19条第8号 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第十九条第八号に基づく利用特定個人情報の提供に関する命令(令和6年デジタル庁、総務省令第9号) ・省令第2条の表 25,26,27,28,29,153,154の項
7. 評価実施機関における担当部署	
①部署	衛生部 足立保健所感染症対策課
②所属長の役職名	衛生部 足立保健所感染症対策課長
8. 他の評価実施機関	

**(別添1) 事務の内容**

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の全体システム



(備考)

## II 特定個人情報ファイルの概要

1. 特定個人情報ファイル名	
予防接種情報ファイル	
2. 基本情報	
①ファイルの種類 ※	[ システム用ファイル ] <選択肢> 1) システム用ファイル 2) その他の電子ファイル(表計算ファイル等)
②対象となる本人の数	[ 10万人以上100万人未満 ] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
③対象となる本人の範囲 ※	新型インフルエンザ等対策特別措置法に基づく接種対象者
その必要性	予防接種に関する業務実現のために、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	[ 50項目以上100項目未満 ] <選択肢> 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
主な記録項目 ※	<ul style="list-style-type: none"> <li>・識別情報 [ <input type="checkbox"/> ] 個人番号 [ <input type="checkbox"/> ] 個人番号対応符号 [ <input type="checkbox"/> ] その他識別情報(内部番号)</li> <li>・連絡先等情報 [ <input type="checkbox"/> ] 4情報(氏名、性別、生年月日、住所) [ <input type="checkbox"/> ] 連絡先(電話番号等) [ <input type="checkbox"/> ] その他住民票関係情報</li> <li>・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="checkbox"/> ] 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 ( )</li> </ul>
その妥当性	<ul style="list-style-type: none"> <li>・個人番号、その他識別情報: 対象者を正確に特定するために保有</li> <li>・4情報、その他住民票関係情報: 対象者の接種日時時点の年齢、居住地等を把握するために保有</li> <li>・健康・医療関係情報: 接種した予防接種の種類、ワクチン名、LotNo.等を把握するために保有</li> <li>・障害者福祉関係情報、及び生活保護・社会福祉関係情報: 接種の自己負担区分を正確に把握するために保有</li> </ul>
全ての記録項目	別添2を参照。
⑤保有開始日	令和3年4月1日
⑥事務担当部署	衛生部 足立保健所感染症対策課

3. 特定個人情報の入手・使用		
①入手元 ※	<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 ( 障害者福祉関係情報、及び生活保護・社会福祉関係情報を担当課から情報システム課経由で入手 ) <input type="checkbox"/> 行政機関・独立行政法人等 ( ) <input type="checkbox"/> 地方公共団体・地方独立行政法人 ( ) <input type="checkbox"/> 民間事業者 ( ) <input type="checkbox"/> その他 ( )	
②入手方法	<input type="checkbox"/> 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 <input type="checkbox"/> 電子メール [ ] 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 ( )	
③入手の時期・頻度	接種対象者の接種要件等を確認する都度	
④入手に係る妥当性	予防接種に関する業務実現のために、必要な特定個人情報を保有する必要がある。	
⑤本人への明示	本人又は本人の代理人からの入手がないため、該当なし	
⑥使用目的 ※	接種対象者の接種要件等を把握するため	
	変更の妥当性	—
⑦使用の主体	使用部署 ※	衛生部 足立保健所感染症対策課
	使用者数	<input type="checkbox"/> 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
⑧使用方法 ※	I 対象者抽出事務: 対象者を抽出する。 II 予防接種管理事務: 個人の予防接種の接種情報を入力する。 III 予防接種情報取込: 予防接種の接種情報(パンチデータ)を取込する。 IV 予防接種照会事務: 住民からの問い合わせなど、接種別や接種履歴を照会し、回答する。 V 転入者処理: 転入者があった場合、過去の接種歴などから予防接種の予診票を印刷する。	
	情報の突合 ※	・4情報を確認して、対象者を決める。【上記Ⅰ】 ・4情報を確認して、接種済み対象者の情報とシステム上のその他内部番号と突合し、予防接種の接種有無を管理する。【上記Ⅱ、Ⅲ】 ・区民からの問い合わせ時、4情報や住民票関係情報と突合し、接種別や全接種の履歴を照会し、回答する。【上記Ⅳ】 ・住民票関係情報と突合して、転入者の把握、過去の接種歴などから予防接種の予診票を印刷する。【上記Ⅴ】
	情報の統計分析 ※	特定の個人を判別するような情報の統計や分析は行わない
	権利利益に影響を与え得る決定 ※	該当なし
⑨使用開始日	令和3年3月12日	





6. 特定個人情報の保管・消去

①保管場所 ※		<p>&lt;足立区における措置&gt; ・届出書等の紙媒体については、施錠ができるキャビネットに保管している。</p> <p>&lt;ガバメントクラウドにおける措置&gt; ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が設置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>&lt;中間サーバー・プラットフォームにおける措置&gt; ・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いる。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ・特定個人情報は、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>
		<p>&lt;選択肢&gt; 1) 1年未満                      2) 1年                      3) 2年 4) 3年                              5) 4年                      6) 5年 7) 6年以上10年未満      8) 10年以上20年未満      9) 20年以上 10) 定められていない</p>
②保管期間	期間	[            20年以上            ]
	その妥当性	予防接種に関する記録は、予防接種法施行規則第3条で5年間保存とされ、少なくとも5年間は適正に管理・保管することとされており、接種記録の確認や証明書の発行事務において長期間保管する必要がある。
③消去方法		<p>&lt;足立区における措置&gt; ・届出書等の紙媒体については、外部業者による裁断溶解処理を実施している。</p> <p>&lt;ガバメントクラウドにおける措置&gt; ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。</p> <p>&lt;中間サーバー・プラットフォームにおける措置&gt; ・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為、通常、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、中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、物理的破壊または専用ソフト等を利用して完全に消去する。</p>
7. 備考		

## (別添2) 特定個人情報ファイル記録項目

### 【住民情報】

整理番号、個人番号、履歴番号、カナ氏名、漢字氏名、本名カナ氏名、本名漢字氏名、通称カナ氏名、通称漢字氏名、漢字併記カナ氏名、生年月日、性別、町番号、番地、枝番、小枝、郵便番号、住所、方書、続柄、世帯番号、世帯主カナ氏名、世帯主漢字氏名、住登外区分、住民でなくなった日、最新異動区分、最新異動日、最新異動届出日、住民異動区分、住民異動日、取消区分、転入前住所、転入前方書、転出後住所、転出後方書、電話番号、FAX番号、携帯番号、

### 【予防接種結果】

接種名称区分、期回数区分、履歴番号、年度、事業予定連番、接種日、実施時間、会場区分、会場区分その他、接種種別区分、登録日、接種医療機関番号、接種医療機関番号その他、接種区分、Lot番号、接種量、印刷区分、印刷日、発送日、予診理由区分、接種補足区分、予診票再発行フラグ、予診票再発行枚数、予診票再発行日、依頼書印刷区分、依頼書印刷日、証明書印刷区分、証明書印刷日、予診医医療機関番号、備考、予診番号、登録支所区分、抽出日、印刷連番、予診票番号、依頼書発行元、依頼書受付日、依頼番号、実施報告書印刷日、請求年月、経過措置、予診票発行部署、備考

### 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	基本4情報、その他の住民票関係情報の入手は、区住記システムに入力された情報を、庁内連携システムで取得する方法に限定されるため、対象者以外の情報を入手することはない。
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	庁内連携システムを介した情報の入手について、対象事務で必要な情報以外を参照できないようにする。
その他の措置の内容	—
リスクへの対策は十分か	[ 十分である ] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	足立区民の個人番号、4情報、その他の住民関係情報の入手については、入退室管理をしているガバメントクラウド上のサーバ間通信に限定することで、安全を担保している。
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： 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	—
個人番号の真正性確認の措置の内容	個人番号は庁内連携システムから連携され、基本4情報や予防接種情報と自動的に関連付けて登録される仕組みを取ることで真正性を確保している。
特定個人情報の正確性確保の措置の内容	・基本4情報、その他の住民票関係関係情報の入手は、区住記システムに入力した情報を、庁内連携システムで取得する方法により正確性を確保している。 ・予防接種情報については予診票をパンチ入力によりデータ化してシステムに登録する。入力はペリファイ入力を採用することで正確性を確保している。
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	・足立区民の個人番号、4情報、その他の住民関係情報の入手は、入退室管理をしているガバメントクラウド上のサーバ間通信に限定することで、情報漏えい、紛失等を防止している。 ・保健衛生システムでの情報の入手については決められた仕様に基づく連携での入手に限定することで情報漏えい・紛失等を防止している。
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
特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。)におけるその他のリスク及びそのリスクに対する措置	
—	

### 3. 特定個人情報の使用

リスク1: 目的を超えた紐付け、事務に必要なでない情報との紐付けが行われるリスク

宛名システム等における措置の内容	<ul style="list-style-type: none"> <li>・共通機能(団体内統合宛名機能)は、番号利用法別表および関係主務省令に定められた事務を担当する部署以外からの特定個人情報へのアクセスが行えない仕組みである。また、個人番号、氏名や生年月日等の基本的な情報のみ保持する仕組みとなっており、当該事務にて必要のない情報との紐付けは物理的に不可能である。</li> <li>・共通機能(団体内統合宛名機能)へは、権限のない者の接続は認めない。</li> </ul>
事務で使用するその他のシステムにおける措置の内容	区民情報系基盤システムより入手する情報項目は、足立区情報公開・個人情報審議会の承認を得た情報項目(事務に必要なもの)のみに限定しており、事務に必要なでない情報との紐付けはできないよう設計している。
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	・保健衛生システムの利用の際には、二要素認証を必要としているため、ログイン権限のない者は保健衛生システムを使用できない。また、保健衛生システム内の各機能の利用権限は、ログインIDに対して付与しているため、権限のない者は当該業務を行うことができない。
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	・年度当初に、システムの各機能を利用する職員のIDや二要素認証カードの新規発行、更新、削除を行う。 ・年度当初以外の時期に異動が生じた場合は、都度、追加・削除を行う。
アクセス権限の管理	[ 行っている ] <選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	・ID及び権限設定については、システム管理者のみが操作できる仕組みとしている。
特定個人情報の使用の記録	[ 記録を残している ] <選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	・システム内で特定個人情報を扱う画面のアクセスログを取得し、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"> <li>・アクセスログを残しておくことで、事務外で特定個人情報を使用するリスクの抑止を図っている。</li> <li>・職員に対して、情報セキュリティ研修を行っている。</li> <li>・委託業者(再委託業者を含む。)に従業者に対するセキュリティ教育を義務付ける。</li> </ul>
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"> <li>・個人(ID)単位の操作ログ(いつ、誰が、誰の情報にアクセスし、どのような操作をしたかの記録)を取得し、追跡可能な形式で管理しており、特定個人情報ファイルが不正に複製されるリスクの抑止を図っている。</li> <li>・端末は、原則、外部媒体を使用することができない仕組みとなっている。ただし、許可された端末のみ外部媒体を使用することができる。</li> </ul>
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

—

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"> <li>委託仕様書に「個人情報に係る契約約款別紙」、「個人情報に関する情報セキュリティ対策の実施について」及び「特定個人情報の安全管理措置に関する特記事項」について遵守することと記載しており、その実施状況を検査し報告することを受託者に課している。</li> <li>作業者を限定するために、委託作業者の名簿を提出させる。</li> <li>閲覧／更新権限等の設定をIDごとに行い、システム上で操作を制限する。</li> </ul>	
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"> <li>閲覧／更新権限の設定をIDごとに行い、システム上で操作を制限する。</li> <li>システム内で特定個人情報を扱う画面のアクセスログを取得し、保管している。</li> </ul>	
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	システム内で特定個人情報を扱う画面のアクセスログを取得し、保管している。	
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	契約書にて委託事業者から第三者へ個人情報を提供することを禁止している。	
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	委託契約書内にてルールを明確化している。	
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"> <li>契約書にて委託事業者から第三者へ個人情報を提供することを禁止している。</li> <li>契約期間終了後、委託先は速やかに廃棄し、廃棄証明書を提出するルールを定めている。</li> </ul>	
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	機密保持契約として以下を定める。 <ul style="list-style-type: none"> <li>第三者への提供、開示、漏えいの禁止</li> <li>目的外利用の禁止</li> <li>無断複製の禁止</li> <li>契約終了後の返還、廃棄、消去</li> <li>セキュリティ事故発生時の報告</li> <li>安全管理体制の報告、資料提出</li> <li>厳重な保管</li> <li>再委託に係る規定</li> <li>公表措置及び損害賠償義務に係る規定</li> </ul>	
再委託先による特定個人情報ファイルの適切な取扱いの確保	[ 再委託していない ]	<選択肢> 1) 特に力を入れて行っている    2) 十分に行っている 3) 十分に行っていない            4) 再委託していない
具体的な方法	—	
その他の措置の内容	—	
リスクへの対策は十分か	[ 十分である ]	<選択肢> 1) 特に力を入れている            2) 十分である 3) 課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
—		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[○] 提供・移転しない	
リスク1： 不正な提供・移転が行われるリスク			
特定個人情報の提供・移転の記録	[ ]	<選択肢> 1) 記録を残している	2) 記録を残していない
具体的な方法			
特定個人情報の提供・移転に関するルール	[ ]	<選択肢> 1) 定めている	2) 定めていない
ルールの内容及びルール遵守の確認方法			
その他の措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク2： 不適切な方法で提供・移転が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置			

6. 情報提供ネットワークシステムとの接続		[ ] 接続しない(入手)	[ ] 接続しない(提供)
リスク1: 目的外の入手が行われるリスク			
リスクに対する措置の内容	<p>&lt;足立区における措置&gt;</p> <ul style="list-style-type: none"> <li>・特定個人情報の照会が可能な事務および当該事務の権限を有する職員のみが実施できるよう認証および権限の管理を厳格に行う。</li> <li>・中間サーバーへの処理要求のログを記録し、処理実施者および操作内容を把握する。</li> <li>・中間サーバーへの処理要求のログや認証ログなどから、目的外の入手が行われていないことを適宜確認する。</li> <li>・操作ログにより操作者、操作内容が把握可能である旨、職員および関係者に周知を行う。</li> <li>・特定個人情報の照会が認められている事務であることを確認した上で、情報提供ネットワークシステムとの接続を許可する。</li> <li>・番号法に定められている事務以外での情報照会は禁止されている旨、職員および関係者への周知を実施する。</li> <li>・個人番号を取り扱う業務を委託する場合には、区は委託先を適切に管理するとともに、委託先に対し特定個人情報の取り扱いの徹底と厳格な安全保護措置の実施を義務付けることとする。</li> </ul> <p>&lt;中間サーバー・ソフトウェア(中間サーバー・プラットフォームの機能を実現するソフトウェア)における措置&gt;</p> <ul style="list-style-type: none"> <li>・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。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。</li> <li>・中間サーバー・ソフトウェアの職員認証・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。</li> </ul> <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) 番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。</p> <p>(※3) 中間サーバー・ソフトウェア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 3) 課題が残されている	2) 十分である
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>&lt;保健衛生システム、庁内連携システムのソフトウェアにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・中間サーバー・プラットフォームと庁内連携システム、保健衛生システム間の連携は、LGWAN、庁内ネットワーク、サーバー間通信及びガバメントクラウドとの専用線接続に限定されるため、安全が確保されている。</li> </ul> <p>&lt;中間サーバー・ソフトウェアにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・中間サーバー・ソフトウェアは、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</li> </ul> <p>&lt;中間サーバー・プラットフォームにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・中間サーバー・プラットフォームと既存システム、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。</li> <li>・中間サーバー・プラットフォームと団体については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。</li> </ul>		
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 3) 課題が残されている	2) 十分である

リスク3： 入手した特定個人情報 that 不正確であるリスク	
リスクに対する措置の内容	<p>&lt;保健衛生システム、庁内連携システムのソフトウェアにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・情報照会にあたっては、中間サーバー・プラットフォームから入手した特定個人情報が庁内連携システム、保健衛生システムへの登録の際に誤った状態で登録されないことを、検証工程で十分に確認しているため、入手にあたって特定個人情報が不正確となることはない。</li> </ul> <p>&lt;中間サーバー・ソフトウェアにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・中間サーバー・ソフトウェアは、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。</li> </ul>
リスクへの対策は十分か	<p>[ 十分である ]</p> <p>&lt;選択肢&gt;</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>&lt;足立区における措置&gt;</p> <ul style="list-style-type: none"> <li>・保健衛生システムが接続する基幹系ネットワークのセグメントは、インターネットとの接続を禁止している。区の基幹系ネットワークとガバメントクラウドの間はインターネット接続回線を介さない専用線接続となっている。</li> <li>・権限を有する職員のみが情報照会を行えるよう、使用者の認証および権限の認可の管理を厳格に行う。</li> <li>・中間サーバー・プラットフォームへの処理要求ログを記録し、処理実施者および操作内容を把握する。</li> <li>・操作ログや認証ログなどのアクセスログを基に、権限外の職員による操作の有無や、不正な照会が無いことを適宜確認する。</li> <li>・情報照会処理が行える端末を制限するとともに、画面コピー操作やフォルダー共有、外部記憶媒体の接続を制限する。</li> <li>・操作端末から離れる際には、画面のロックもしくはログアウトを徹底する。</li> <li>・職員に対して特定個人情報の適切な取り扱いについて周知するとともに安全保護対策の遵守を徹底させる。</li> <li>・個人番号を取り扱う業務を委託する場合には、区は委託先を適切に管理するとともに、委託先に対し特定個人情報の取り扱いの徹底と厳格な安全保護措置の実施を義務付けることとする。</li> </ul> <p>&lt;中間サーバー・ソフトウェアにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・中間サーバー・ソフトウェアは、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(※)。</li> <li>・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。</li> <li>・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。</li> <li>・中間サーバー・ソフトウェアの職員認証・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。</li> <li>(※)中間サーバー・プラットフォームは、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。</li> <li>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。</li> </ul> <p>&lt;中間サーバー・プラットフォームにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・中間サーバー・プラットフォームと既存システム、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。</li> <li>・中間サーバー・プラットフォームと団体については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。</li> <li>・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。</li> </ul>
リスクへの対策は十分か	<p>[ 十分である ]</p> <p>&lt;選択肢&gt;</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>&lt;足立区における措置&gt;</p> <ul style="list-style-type: none"> <li>・特定個人情報の提供が可能な事務および当該事務の権限を有する職員のみが実施できるよう認証および権限の管理を厳格に行う。</li> <li>・中間サーバー・プラットフォームへの処理要求のログを記録し、処理実施者および操作内容を把握する。</li> <li>・中間サーバー・プラットフォームへの処理要求のログや認証ログなどから、不正な提供が行われていないことを適宜確認する。</li> <li>・操作ログにより操作者、操作内容が把握可能である旨、職員および関係者に周知を行う。</li> <li>・特定個人情報の提供が認められている事務であることを確認した上で、情報提供ネットワークシステムとの接続を許可する。</li> <li>・職員に対して特定個人情報の適切な取り扱いについて周知するとともに安全保護対策の遵守を徹底させる。</li> <li>・個人番号を取り扱う業務を委託する場合には、区は委託先を適切に管理するとともに、委託先に対し特定個人情報の取り扱いの徹底と厳格な安全保護措置の実施を義務付けることとする。</li> </ul> <p>&lt;中間サーバー・ソフトウェア(中間サーバー・プラットフォームの機能を実現するソフトウェア)における措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・機微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。</li> <li>・中間サーバー・プラットフォームの職員認証・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。</li> </ul> <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	<p>[ 十分である ]</p> <p>&lt;選択肢&gt;</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>&lt;足立区における措置&gt;</p> <ul style="list-style-type: none"> <li>・保健衛生システムが接続する基幹系ネットワークのセグメントは、インターネットとの接続を禁止している。区の基幹系ネットワークとガバメントクラウドの間はインターネット接続回線を介さない専用線接続となっている。</li> <li>・権限を有する職員のみが情報提供を行えるよう、使用者の認証および権限の認可の管理を厳格に行う。</li> <li>・中間サーバーへの処理要求ログを記録し、処理実施者および操作内容を把握する。</li> <li>・操作ログや認証ログなどのアクセスログを基に、権限外の職員による操作の有無や、不正な提供が無いことを適宜確認する。</li> <li>・情報照会処理が行える端末を制限するとともに、画面コピー操作やフォルダー共有、外部記憶媒体の接続を制限する。</li> <li>・操作端末から離れる際には、画面のロックもしくはログアウトを徹底する。</li> <li>・職員に対して特定個人情報の適切な取り扱いについて周知するとともに安全保護対策の遵守を徹底させる。</li> <li>・個人番号を取り扱う業務を委託する場合には、区は委託先を適切に管理するとともに、委託先に対し特定個人情報の取り扱いの徹底と厳格な安全保護措置の実施を義務付けることとする。</li> </ul> <p>&lt;中間サーバー・ソフトウェアにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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っている。</li> <li>・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。</li> </ul> <p>(※)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。</p>

	<p>&lt;中間サーバー・プラットフォームにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・中間サーバー・プラットフォームの事業者においては、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。</li> </ul>	
リスクへの対策は十分か	[ 十分である ]	<p>&lt;選択肢&gt;</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>&lt;足立区における措置&gt;</p> <p>提供方式を情報提供ネットワークシステムによる提供に限定することで、誤った相手に提供してしまうリスクを軽減する。</p> <p>&lt;中間サーバー・ソフトウェアにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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、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。</li> <li>・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。</li> <li>・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。</li> </ul> <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	[ 十分である ]	<p>&lt;選択肢&gt;</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		
<p>&lt;中間サーバー・ソフトウェアにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul> <p>&lt;中間サーバー・プラットフォームにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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事業者における情報漏えい等のリスクを極小化する。</li> </ul>		
<b>7. 特定個人情報の保管・消去</b>		
リスク1: 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[ 政府機関ではない ]	<p>&lt;選択肢&gt;</p> <p>1) 特に力を入れて遵守している      2) 十分に遵守している</p> <p>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	[ 十分に整備している ]	<p>&lt;選択肢&gt;</p> <p>1) 特に力を入れて整備している      2) 十分に整備している</p> <p>3) 十分に整備していない</p>
③安全管理規程	[ 十分に整備している ]	<p>&lt;選択肢&gt;</p> <p>1) 特に力を入れて整備している      2) 十分に整備している</p> <p>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	[ 十分に行っている ]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
	具体的な対策の内容	<p>&lt;足立区における措置&gt;</p> <ul style="list-style-type: none"> <li>・特定個人情報を扱う職員が離席する際には、特定個人情報を記した書類は机上に放置せず、キャビネットに施錠保管している。</li> <li>・特定個人情報を媒体に保管する場合は、運用ルールを定め、遵守している。</li> </ul> <p>&lt;ガバメントクラウドにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul> <p>&lt;中間サーバー・プラットフォームにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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、設置場所はマシン室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。</li> <li>・事前に申請し承認されていない物品、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。</li> </ul>
⑥技術的対策	[ 十分に行っている ]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
	具体的な対策の内容	<p>&lt;足立区における措置&gt;</p> <ul style="list-style-type: none"> <li>・足立区とガバメントクラウド間は専用回線を敷き、サーバーへのアクセスを制限している。</li> </ul> <p>&lt;ガバメントクラウドにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul> <p>&lt;中間サーバー・プラットフォームにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul>
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	サーバーで管理しており、生存者の個人番号と同様の方法にて安全管理措置を実施している。	
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	氏名、住所等の情報については、既存住記システムを介して、常に最新情報に更新している。	
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	<足立区における措置> 届出書等の紙媒体については、外部業者による裁断溶解処理を実施している。  <ガバメントクラウドにおける措置> データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。	
その他の措置の内容	-	
リスクへの対策は十分か	[ 十分である ]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		
-		

## IV その他のリスク対策 ※

1. 監査		
①自己点検	[ 十分に行っている ]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的なチェック方法		<足立区における措置> ・実際の運用が評価書記載の内容と合致しているかについて、定期的にチェックを行う。  <中間サーバー・プラットフォームにおける措置> ・運用規則等に基づき、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。
②監査	[ 十分に行っている ]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的な内容		<足立区における措置> ・全項目評価書の記載内容について、個人情報保護委員会が発行するガイドラインに基づき、定期的に外部監査を実施する。  <ガバメントクラウドにおける措置> ・ガバメントクラウド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。  <中間サーバー・プラットフォームにおける措置> ・運用規則等に基づき、中間サーバー・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。
2. 従業者に対する教育・啓発		
従業者に対する教育・啓発	[ 十分に行っている ]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的な方法		<足立区における措置> ・職員に対し、個人情報保護や情報セキュリティに関する研修等を実施する。 ・事業者には、事業の従事者に対し、委託契約の仕様に個人情報保護や情報セキュリティに関する教育又は研修の実施を義務付けている。 ・違反行為を行った者に対しては、都度指導の上、違反行為の程度によっては懲戒の対象となりうる。  <中間サーバー・プラットフォームにおける措置> ・IPA(情報処理推進機構)が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資料を作成し、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、運用規則(接続運用規程等)や情報セキュリティに関する教育を年次(年2回)及び随時(新規要員着任時)実施することとしている。
3. その他のリスク対策		
<ガバメントクラウドにおける措置> ・ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。 ・ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。 ・具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。  <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リテラシー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。		

## 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	足立区政策経営部区政情報課情報公開担当 〒120-8510 東京都足立区中央本町一丁目17番1号 03-3880-5225
②請求方法	法令等で定める様式による書面の提出により開示・停止・利用停止請求を受け付ける。
特記事項	開示請求の手続きについては、以下のホームページに掲載している。 <a href="http://www.city.adachi.tokyo.jp/kuse/ku/mado/joho-kaijisekyu.html">http://www.city.adachi.tokyo.jp/kuse/ku/mado/joho-kaijisekyu.html</a>
③手数料等	[ 無料 ] <選択肢> 1) 有料 2) 無料 (手数料額、納付方法: 手数料はかからないが、写しを交付する場合は実費の負担が生じる。)
④個人情報ファイル簿の公表	[ 行っていない ] <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	—
公表場所	—
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	足立保健所感染症対策課 郵便番号120-0011 足立区中央本町一丁目5番3号 電話: 足立保健所感染症対策課 03-3880-5372
②対応方法	・問合せがあった場合、問合せの内容と対応の経過について記録を残す。 ・情報漏えい等に関する問合せがあった場合は、実施機関において必要な対応を行い、政策経営部区政情報課情報公開担当に報告する。

## VI 評価実施手続

1. 基礎項目評価	
①実施日	令和6年11月26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	足立区パブリックコメント実施要綱に基づき、意見公募手続きを実施し、広く住民等の意見を聴取する。
②実施日・期間	令和6年11月26日から令和6年12月25日まで
③期間を短縮する特段の理由	なし
④主な意見の内容	
⑤評価書への反映	
3. 第三者点検	
①実施日	令和7年2月(予定)
②方法	足立区情報公開・個人情報保護審議会の小委員会において点検を受ける。
③結果	—
4. 個人情報保護委員会の承認【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

(別添3)変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年11月26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	新型インフルエンザ等が発生した場合に、特定接種や、住民に対する予防接種、予診票の発行等を行う。番号利用別表第二に基づき、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において、情報提供ネットワークシステムに接続し、各情報保有機関が保有する特定個人情報について情報連携を行う。情報提供に必要な情報を「副本」として中間サーバーへ登録する。	新型インフルエンザ等が発生した場合に、特定接種や、住民に対する予防接種、予診票の発行等を行う。番号法第19条第8号に基づき、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において、情報提供ネットワークシステムに接続し、各情報保有機関が保有する特定個人情報について情報連携を行う。情報提供に必要な情報を「副本」として中間サーバーへ登録する。	事後	番号法改正に伴う修正
令和6年11月26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3 ①システムの名称	情報連携プラットフォーム	共通機能(団体内統合宛名機能)	事前	
令和6年11月26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3 ②システムの機能	1. 団体内統合宛名(利用)管理機能 足立区において個人を識別するための団体内統合宛名(利用)番号と事務および保有する特定個人情報を紐付け、その情報の管理を行う。 ・団体内統合宛名(利用)番号の符番管理 ・個人番号利用事務と特定個人情報ファイルの紐付け ・個人特定のためのデータ照合機能(名寄せ管理機能) 2. 情報連携機能 各業務システムと中間サーバー・プラットフォームとの間で発生する各種の要求処理を中継し、情報連携を行うために共通で必要となる情報連携インターフェースを提供する。 ・文字コード変換機能 ・情報照会要求と照会結果の中継 ・特定個人情報ファイルの登録 ・符号の取得要求 ・中間サーバー・プラットフォームからの氏名、性別、生年月日、住所(以下「4情報」という。)照会への応答	1 団体内統合宛名(利用)管理機能 足立区において個人を識別するための団体内統合宛名(利用)番号の管理を行う。 ・団体内統合宛名(利用)番号の符番管理 2 情報連携機能 各業務システムと中間サーバー・プラットフォームとの間で発生する各種の要求処理を中継し、情報連携を行うために共通で必要となる情報連携インターフェースを提供する。 ・情報照会要求と照会結果の中継 ・特定個人情報ファイルの登録の中継 ・符号の取得要求 ・中間サーバー・プラットフォームからの氏名、性別、生年月日、住所(以下「4情報」という。)照会への応答 ・自動応答不可・不開示フラグの中継(団体内統合宛名番号単位)	事前	
令和6年11月26日	I 基本情報 5. 個人番号の利用 法令上の根拠	1. 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(番号利用法) (平成25年5月31日法律第27号) ・番号利用法第9条第1項 別表第一の93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一の主務省令で定める事務を定める命令(別表第一省令) (平成26年内閣府・総務省令第5号) ・別表第一省令第67条の2	1 番号法第9条第1項 別表の126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の主務省令で定める事務を定める命令(平成26年内閣府、総務省令第5号) ・第67条の2 3 番号法第19条第6号	事後	番号法改正に伴う修正
令和6年11月26日	I 基本情報 6. 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	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、及び照会の根拠) 別表第二の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、及び照会の根拠) ・別表第二省令(第59条の2) (※別表第二の115の2の項)	1 番号法第19条第8号 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第十九条第八号に基づく利用特定個人情報の提供に関する命令(令和6年デジタル庁、総務省令第9号) ・省令第2条の表 25,26,27,28,29,153,154の項	事後	番号法改正に伴う修正
令和6年11月26日	I 基本情報 7. 評価実施期間における担当部署 ①部署	衛生部 感染症対策課	衛生部 足立保健所感染症対策課	事後	
令和6年11月26日	I 基本情報 7. 評価実施期間における担当部署 ②所属長の役職名	課長	衛生部 足立保健所感染症対策課	事後	

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6年11月26日	別添1 事務の内容	(略)	システム構成図において、ガバメントクラウドの範囲を明示	事前	
令和6年11月26日	II 特定個人情報ファイルの概要 2.基本情報 ⑥事務担当部署	衛生部 感染症対策課	衛生部 足立保健所感染症対策課	事後	
令和6年11月26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 ⑦使用の主体 使用部署	衛生部 感染症対策課	衛生部 足立保健所感染症対策課	事後	
令和6年11月26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 ⑦使用の主体 使用者数	50人以上100人未満	10人以上50人未満	事後	
令和6年11月26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 ⑧使用方法 情報の統計分析	接種者数、接種率等個人番号を用いず統計は実施。	特定の個人を判別するような情報の統計や分析は行わない	事後	
令和6年11月26日	II 特定個人情報ファイルの概要 4.特定個人情報の取扱いの委託 ④委託先への特定個人情報ファイルの提供方法	保健衛生システム端末の直接操作	受託者の社内アクセスルーム端末よりガバメントクラウド上の特定個人情報ファイルにアクセスする	事前	
令和6年11月26日	II 特定個人情報ファイルの概要 5.特定個人情報の提供・移転 提供先1	番号法第19条第7号別表第二に定める情報照会者	特定個人番号利用事務を処理するものとして主務省令で定めるもの	事後	番号法改正に伴う修正
令和6年11月26日	II 特定個人情報ファイルの概要 5.特定個人情報の提供・移転 提供先1 ①法令上の根拠	番号法第19条第7号別表第二	1 番号法第19条第8号 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第十九条第八号に基づく利用特定個人情報の提供に関する命令(令和6年デジタル庁、総務省令第9号) ・省令第2条の表	事後	番号法改正に伴う修正
令和6年11月26日	II 特定個人情報ファイルの概要 5.特定個人情報の提供・移転 提供先1 ②提供先における用途	番号法第19条第7号別表第二に掲げる事務を処理するため	主務省令で定める用途	事後	番号法改正に伴う修正
令和6年11月26日	II 特定個人情報ファイルの概要 5.特定個人情報の提供・移転 提供先1 ③提供する情報	新型インフルエンザ等対策特別措置法による予防接種の実施に関する情報であって主務省令で定めるもの	主務省令で定める利用特定個人情報	事後	番号法改正に伴う修正
令和6年11月26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 ①保管場所	<足立区における措置> ・特定個人情報が記録されるデータベースは、厳重な入退室管理を行っている区画の施設可能なラックに設置されたサーバー内のディスクに保管され、物理的なアクセスを制限している。 ・サーバーやデータベースには、許可された者以外がアクセスできないよう、管理者による認証と認可を必要としている。	自庁内にデータを保管しなくなることから、左記の2点は削除	事前	

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6年11月26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 ②保管期間 その妥当性	予防接種に関する正確な履歴を記録しておく必要がある。	予防接種に関する記録は、予防接種法施行規則第3条で5年間保存とされ、少なくとも5年間は適正に管理・保管することとされており、接種記録の確認や証明書の発行事務において長期間保管する必要がある。	事後	文言の修正
令和6年11月26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 ③消去方法	<足立区における措置> ・足立区情報セキュリティ対策に関する要綱第24条の規定に基づき、ディスク交換やハード更改等の際は、保存された特定個人情報が不正に読み出されないよう、物理的破壊または専用ソフトで完全に消去を行う。	<足立区における措置> ・届出書等の紙媒体については、外部業者による裁断溶解処理を実施している。	事前	
令和6年11月26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 ①保管場所、③消去方法	—	「ガバメントクラウドにおける措置」を追記	事前	
令和6年11月26日	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 2.特定個人情報の入手 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	保健衛生システムを利用する職員を特定し、ICカードとパスワードによる二要素認証を実施する。認証後はシステムの権限設定機能により、そのユーザーがシステム上で利用可能な機能を制限することで、不適切な方法での入手が行えない対策を実施している。	足立区民の個人番号、4情報、その他の住民関係情報の入手については、ガバメントクラウド上のサーバー間通信に限定することで、安全を担保している。	事前	
令和6年11月26日	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 2.特定個人情報の入手 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	特定個人情報の入手については、外部と隔離された庁内ネットワークを介して行われる。	・足立区民の個人番号、4情報、その他の住民関係情報の入手は、入退室管理をしているガバメントクラウド上のサーバー間通信に限定することで、情報漏えい、紛失等を防止している。 ・保健衛生システムでの情報の入手については決められた仕様に基づく連携での入手に限定することで情報漏えい・紛失等を防止している。	事前	
令和6年11月26日	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 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	・情報連携プラットフォームは、番号法別表第1および関係主務省令に定められた事務を担当する部署以外からの特定個人情報へのアクセスが行えない仕組みである。また、個人番号、氏名や生年月日等の基本的な情報のみ保持する仕組みとなっており、当該事務にて必要のない情報との紐付けは物理的に不可能である。 ・情報連携プラットフォームへは、権限のない者の接続は認めない。	・共通機能(団体内統合宛名機能)は、個人番号、氏名や生年月日等の基本的な情報のみ保持する仕組みとしており、当該事務にて必要のない情報との紐付けは物理的に不可能である。 ・共通機能(団体内統合宛名機能)へは、権限のない者の接続を認めない。	事前	
令和6年11月26日	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 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 事務で使用するその他のシステムにおける措置の内容	・保健衛生システムと住民基本台帳ネットワークシステム足立区CS間では、法令に基づく事務で使用する以外の情報との紐付けは行わない。	区民情報系基盤システムより入手する情報項目は、足立区情報公開・個人情報審議会の承認を得た情報項目(事務に必要なもの)のみに限定しており、事務に必要な情報との紐付けはできないよう設計している。	事後	
令和6年11月26日	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 3.特定個人情報の使用 リスク3:従業員が事務外で使用するリスク リスクに対する措置の内容	・システム内で特定個人情報を扱う画面のアクセスログを取得し、保管している。 ・職員に対してセキュリティに関する研修を行っている。 ・職員以外の従業者(委託先等)には、個人情報保護についての誓約書の提出を求めている。またセキュリティ研修の実施も義務付けている。 ・違反行為を行った場合は、条例の罰則規定により措置を講じる。	・アクセスログを残しておくことで、事務外で特定個人情報を使用するリスクの抑止を図っている。 ・職員に対して、情報セキュリティ研修を行っている。 ・委託業者(再委託業者を含む。)に従業者に対するセキュリティ教育を義務付ける。	事後	
令和6年11月26日	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 3.特定個人情報の使用 リスク4:特定個人情報保護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	・システム内で特定個人情報を扱う画面のアクセスログを取得し、保管している。 ・管理権限を与えられた者以外、情報のファイル書き出しが行えない仕組みである。 ・職員に対しては、セキュリティに関する研修を行っている。 ・職員以外の従業者(委託先等)には、個人情報保護についての誓約書の提出を求めている。またセキュリティ研修の実施も義務付けている。 ・違反行為を行った場合は、条例の罰則規定により措置を講じる。	・個人(ID)単位の操作ログ(いつ、誰が、誰の情報にアクセスし、どのような操作をしたかの記録)を取得し、追跡可能な形式で管理しており、特定個人情報ファイルが不正に複製されるリスクの抑止を図っている。 ・端末は、原則、外部媒体を使用することができない仕組みとなっている。ただし、許可された端末のみ外部媒体を使用することができる。	事後	

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6年11月26日	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 4.特定個人情報ファイルの取扱いの委託 情報保護管理体制の確認	システムの運用等を委託するときは、足立区情報セキュリティ対策に関する要綱第41条の規定に基づき、外部委託事業者が守るべき内容等について説明を行い、特定個人情報の保護を適切に行える委託先であることを確認する。	・委託仕様書に「個人情報に係る契約約款別紙」、「個人情報に関する情報セキュリティ対策の実施について」及び「特定個人情報の安全管理措置に関する特記事項」について遵守することと記載しており、その実施状況を検査し報告することを受託者に課している。 ・作業者を限定するために、委託作業者の名簿を提出させる。 ・閲覧／更新権限等の設定をIDごとに行い、システム上で操作を制限する。	事後	
令和6年11月26日	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 4.特定個人情報ファイルの取扱いの委託 具体的な制限方法	・作業者を限定するために、委託作業者の名簿を提出させる。 ・委託事業者に対し、個人情報保護に関する誓約書を提出させる。また、セキュリティ研修の実施も義務付ける。 ・閲覧／更新権限の設定をIDごとに行い、システム上で操作を制限する。 ・システム内で特定個人情報を扱う画面のアクセスログを取得し、保管している。	・閲覧／更新権限の設定をIDごとに行い、システム上で操作を制限する。 ・システム内で特定個人情報を扱う画面のアクセスログを取得し、保管している。	事後	
令和6年11月26日	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 4.特定個人情報ファイルの取扱いの委託 特定個人情報の提供ルール 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	・提供の禁止を契約書に明記する。	契約書にて委託事業者から第三者へ個人情報を提供することを禁止している。	事後	表現の修正
令和6年11月26日	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 4.特定個人情報ファイルの取扱いの委託 特定個人情報の提供ルール 委託先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	・依頼書の作成は保健衛生システムを通じて作成するように運用上限定し、出力時に送付先・発行日時等を自動的に保健衛生システム内に記録する。 ・予診票の送付は処理を行う職員をあらかじめ限定し、情報提供を実施する。	委託契約書内にルールを明確化している。	事後	表現の修正
令和6年11月26日	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 4.特定個人情報ファイルの取扱いの委託 特定個人情報の消去ルールの内容及びルール遵守の確認方法	・足立区情報セキュリティ対策に関する要綱第24条に基づき、ディスク交換やハード更改等の際は、保存された特定個人情報不正に読み出されないよう、物理的破壊または専用ソフトで完全に消去を行う。	・契約書にて委託事業者から第三者へ個人情報を提供することを禁止している。 ・契約期間終了後、委託先は速やかに廃棄し、廃棄証明書を提出するルールを定めている。	事後	実際の運用に合わせて修正
令和6年11月26日	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 6.情報提供ネットワークシステムとの接続 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	<衛生システム、庁内連携システムのソフトウェアにおける措置> ・中間サーバー・プラットフォームと庁内連携システム、衛生システム間の連携は、LGWAN、庁内ネットワーク及びサーバー間通信に限定されるため、安全が確保されている。	<保健衛生システム、庁内連携システムのソフトウェアにおける措置> 中間サーバー・プラットフォームと庁内連携システム、保健衛生システム間の連携は、LGWAN、庁内ネットワーク、サーバー間通信及びガバメントクラウドとの専用線接続に限定されるため、安全が確保されている。	事前	
令和6年11月26日	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 6.情報提供ネットワークシステムとの接続 リスク3:入手した特定個人情報が不正確であるリスク	<衛生システム、庁内連携システムのソフトウェアにおける措置> ・情報照会にあたっては、中間サーバー・プラットフォームから入手した特定個人情報が庁内連携システム、衛生システムへの登録の際に誤った状態で登録されることがないことを、検証工程で十分に確認しているため、入手にあたって特定個人情報が不正確となることはない。	<保健衛生システム、庁内連携システムのソフトウェアにおける措置> ・情報照会にあたっては、中間サーバー・プラットフォームから入手した特定個人情報が庁内連携システム、保健衛生システムへの登録の際に誤った状態で登録されることがないことを、検証工程で十分に確認しているため、入手にあたって特定個人情報が不正確となることはない。	事後	

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6年11月26日	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 6.情報提供ネットワークシステムとの接続 リスク4: 入手の際に特定個人情報情報が漏えい・紛失するリスク	<足立区における措置> ・衛生システムが接続する基幹系ネットワークのセグメントは、インターネットと接続されている庁内ネットワークとは分離されており、その境界はルーターおよびファイアウォールにより相互の通信が行えないよう制御を行っている。なお、基幹系ネットワークは、インターネットとの接続を禁止している。	<足立区における措置> ・保健衛生システムが接続する基幹系ネットワークのセグメントは、インターネットとの接続を禁止している。区の基幹系ネットワークとガバメントクラウドの間はインターネット接続回線を介さない専用線接続となっている。	事前	
令和6年11月26日	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 6.情報提供ネットワークシステムとの接続 リスク6: 不適切な方法で提供されるリスク	<足立区における措置> ・既存住記システムが接続する基幹系ネットワークのセグメントは、インターネットと接続可能な庁内ネットワークとは物理的に分離されており、相互の通信が行えないようになっている。	・保健衛生システムが接続する基幹系ネットワークのセグメントは、インターネットとの接続を禁止している。区の基幹系ネットワークとガバメントクラウドの間はインターネット接続回線を介さない専用線接続となっている。	事前	
令和6年11月26日	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.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 ⑤物理的対策	<足立区における措置> ・特定個人情報を保管するサーバーの設置場所では、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ー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。	自庁内にデータを保管しなくなることから、左記の2点は削除	事前	
令和6年11月26日	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.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 ⑥技術的対策	<足立区における措置> ・ネットワークシステムの設定により、サーバーへのアクセスを制御している。 ・日次でバックアップファイルを取得して、遠隔地に電送して保管している。	<足立区における措置> ・足立区とガバメントクラウド間は専用回線を敷き、サーバーへのアクセスを制限している。	事前	
令和6年11月26日	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.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 ⑤物理的対策、⑥技術的対策	—	「ガバメントクラウドにおける措置」を追記	事前	
令和6年11月26日	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.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 ⑩死者の個人番号	住基法第8条(住民票の記載等)の規定により削除された住民票について、住基法施行令第34条(保存)において定める期間(150年間)、システム上にて保管する。	サーバーで管理しており、生存者の個人番号と同様の方法にて安全管理措置を実施している。	事後	
令和6年11月26日	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.特定個人情報の保管・消去 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	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確保している。	氏名、住所等の情報については、既存住記システムを介して、常に最新情報に更新している。	事後	
令和6年11月26日	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.特定個人情報の保管・消去 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	・磁気ディスクの廃棄時は、足立区情報セキュリティ対策に関する要綱第24条に基づき、内容の復元及び判読が不可能になるような方法により消去している。	<足立区における措置> 届出書等の紙媒体については、外部業者による裁断溶解処理を実施している。  <ガバメントクラウドにおける措置> データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。	事後	
令和6年11月26日	Ⅳ その他のリスク対策 1. 監査 ②監査	—	「ガバメントクラウドにおける措置」を追記	事前	
令和6年11月26日	Ⅳ その他のリスク対策 3. その他のリスク対策	—	「ガバメントクラウドにおける措置」を追記	事前	