

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
26	予防接種に関する事務

個人のプライバシー等の権利利益の保護の宣言

品川区は、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あたり、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最大限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

評価実施機関名

東京都品川区長

公表日

[令和7年5月 様式4]

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	予防接種に関する事務
②事務の内容 ※	予防接種法(昭和23年法律第68号)に基づき、A類疾病及びB類疾病のうち政令で定めるものについて、区内に居住する者に対し、期日又は期間を指定して予防接種を行うとともに、国・都への事業報告、実費の徴収等に関する事務を行う。また、新型インフルエンザ等対策特別措置法(平成24年法律第31号)に基づき、新型インフルエンザ等が発生した場合において、同法第28条に基づく「特定接種」の実施に関する事務を行う。 具体的には、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「番号利用法」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。 ①住民情報システムと連携し、予防接種システムより予防接種の対象者データの抽出 ②抽出した対象者データに基づき、予防接種を受ける際に必要な定期予防接種予診票(以下「予診票」という。)を予防接種の種類ごとに作成 ③予診票、予防接種の案内、契約医療機関一覧を封筒に同封し、対象者への個別発送 ④予防接種を実施した者の予診票が医師会および契約医療機関より送付された後、予防接種の種類ごとに、予防接種システムへ実施記録を登録 ⑤定期予防接種は種類ごとに接種期間が決められており、対象者で未接種の者を予防接種システムより抽出し、接種勧奨を個別に通知 ⑥転入及び紛失等にて、予診票がない住民より予診票の交付申請があった場合には、予防接種の履歴を確認し、予診票を作成する。 ⑦定期予防接種依頼書の発行 ⑧定期予防接種実施状況の報告 ⑨予防接種証明書の発行 ⑩健康被害救済の給付 【新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)事務】 ①予防接種システムへ予防接種対象者及び発行した接種券番号の登録を行う。 ②予防接種の実施後に接種記録等を登録、管理を行う。 ③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。 【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】 ・本区は、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。 ・本区は、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。
③対象人数	[30万人以上] <選択肢> 1) 1,000人未満 2) 1,000人以上1万人未満 3) 1万人以上10万人未満 4) 10万人以上30万人未満 5) 30万人以上

2. 特定個人情報ファイルを取り扱う事務において使用するシステム

システム1

①システムの名称	予防接種システム
②システムの機能	①対象者抽出機能 : 予診票を発送する定期予防接種対象者のデータを抽出する機能 ②登録照会機能 : 予防接種を実施した者の記録を登録、照会する機能 ③帳票の発行機能 : 予診票の発行や、予防接種証明書の発行機能 ④統計機能 : 予防接種の種類ごとの実施人数、未接種者数を検索する機能 ⑤庁内連携機能 : 住民情報システムと連携し、転入、転出等の情報がシステムに反映される機能
③他のシステムとの接続	[] 情報提供ネットワークシステム [○] 庁内連携システム [] 住民基本台帳ネットワークシステム [] 既存住民基本台帳システム [] 宛名システム等 [] 税務システム [○] その他 (予診情報・予防接種記録管理/請求支払システム)

システム2	
①システムの名称	番号連携サーバ(団体内統合宛名システム)
②システムの機能	①宛名管理機能:住民記録システムから住登者データ、住登外データを受領し、番号連携サーバ内の統合宛名DBに反映を行う。 ②統合宛名番号の付番機能:個人番号が新規入力されたタイミングで、統合宛名番号の付番を行う。 ③符号要求機能:統合宛名番号を中間サーバーに登録し、中間サーバーに情報提供用個人識別符号の取得要求・取得依頼を行う。 ④情報提供機能:各業務で管理している提供業務情報を受領し、中間サーバーへの情報提供を行う。 ⑤情報照会機能:中間サーバーへ他団体への情報照会を要求し、返却された照会結果を画面表示または、各業務にファイル転送を行う。
③他のシステムとの接続	☐ 情報提供ネットワークシステム ☐ 庁内連携システム ☐ 住民基本台帳ネットワークシステム ☒ 既存住民基本台帳システム ☐ 宛名システム等 ☒ 税務システム ☒ その他 (中間サーバー、予防接種システム)
システム3	
①システムの名称	中間サーバー
②システムの機能	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」とをひもづけ、その情報を保管・管理する機能。 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)の情報照会および情報提供受領(照会した情報の受領)を行う機能。 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および当該特定個人情報(連携対象)の提供を行う機能。 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およ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ための機能。 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、または提供があった旨の情報提供等記録を生成し、管理する機能。 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・管理する機能。 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ための機能。 ⑧セキュリティ管理機能:セキュリティを管理するための機能。 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機能。 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機能。
③他のシステムとの接続	☒ 情報提供ネットワークシステム ☐ 庁内連携システム ☐ 住民基本台帳ネットワークシステム ☐ 既存住民基本台帳システム ☒ 宛名システム等 ☐ 税務システム ☐ その他 ()

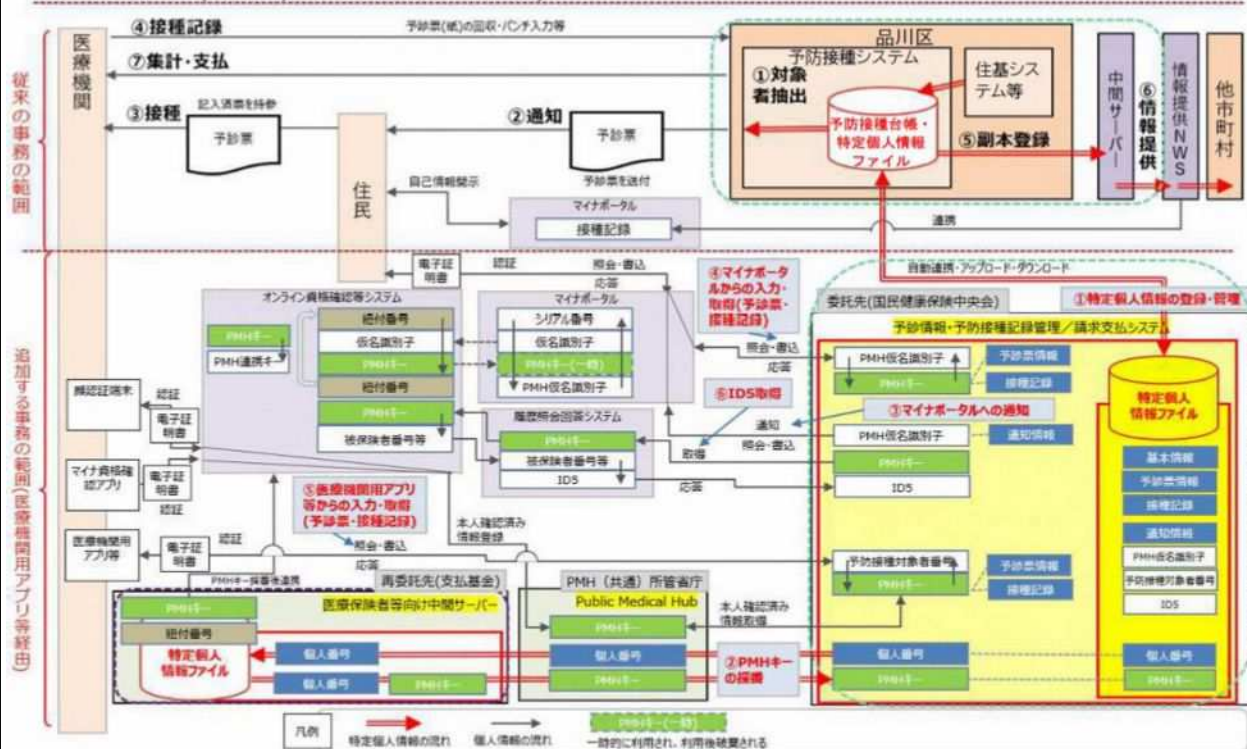
システム4	
①システムの名称	予診情報・予防接種記録管理／請求支払システム
②システムの機能	<予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務> ①予防接種関連データの登録機能 本区は、予防接種システムからの情報連携又は予診情報・予防接種記録管理／請求支払システム画面への直接入力により、予診票項目、接種勧奨における通知文言等の予防接種関連データを予診情報・予防接種記録管理／請求支払システムへ登録する。 ②情報登録機能及びPMHキー採番依頼機能等 予診情報・予防接種記録管理／請求支払システムは、本区で管理している個人番号、対象者情報、予診票情報及び接種記録を予診情報・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。 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。 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取得し、本人確認情報に紐づく予防接種対象者番号をキーに予診票情報を医療機関用アプリ等に提供する。また、医療機関が接種記録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予防接種対象者番号からPMHキーを特定し、PMHキーに紐づく接種記録を登録する。 ⑤情報連携機能（履歴照会回答システム） ・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接種記録等の情報を予防接種DBに連携し、予防接種DBにおいて予防接種の有効性・安全性等の調査・研究を行う。予診情報・予防接種記録管理／請求支払システムから履歴照会回答システムにPMHキーを連携し、履歴照会回答システムはオンライン資格確認等システムから被保険者番号等を取得し、履歴照会回答システム上で生成したID5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連携する。
③他のシステムとの接続	☐ 情報提供ネットワークシステム ☐ 市内連携システム ☐ 住民基本台帳ネットワークシステム ☐ 既存住民基本台帳システム ☐ 宛名システム等 ☐ 税務システム ☐ その他（ 予防接種システム、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 ）
3. 特定個人情報ファイル名	
予防接種台帳ファイル	

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	予防接種法及び新型インフルエンザ等特別対策措置法等関連法令に基づき、予防接種時期に応じた既接種者及び未接種者の数を確認し、区内における予防接種の実施状況についての的確に把握する必要がある。また、健康被害が発生した際に迅速な救済を図るため。
②実現が期待されるメリット	・接種履歴を管理することにより、接種時期や年齢、回数や接種間隔等の誤りを防止し、健康被害を防ぐとともに、健康被害発生時の対応を迅速に行うことができる。 ・個人番号を利用して他自治体等と情報連携することにより、転入転出時等における接種実施状況を把握し、未接種のものについて接種勧奨を行い、当該疾病の発生及び蔓延を防止できる。
5. 個人番号の利用 ※	
法令上の根拠	1. 番号利用法 ・第9条第1項、別表14の項、126の項 2. 番号利用法別表の主務省令で定める事務を定める命令 ・第10条、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（特例臨時接種）事務関係】 【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関係】 3. 番号利用法 ・第19条第6号（委託先への提供）
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[実施する] <選択肢> 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	情報提供：番号利用法第19条第8号に基づく利用特定個人情報の提供に関する命令第2条の表25、26、153、154 情報照会：番号利用法第19条第8号に基づく利用特定個人情報の提供に関する命令第2条の表25、27、28、29、153
7. 評価実施機関における担当部署	
①部署	品川区 保健予防課
②所属長の役職名	保健予防課長
8. 他の評価実施機関	
—	

(別添1) 事務の内容

予防接種事務の概要 全体図

従来の事務では、①～⑦の流れで予防接種システム・中間サーバに情報が登録・連携される。今回利便性の向上のため、予防接種における住民からの予診票入力及び接種記録の取得、医療機関からの予診票取得、接種記録の入力等のオンライン化を事務の範囲に追加する。追加する事務では、①②の流れで、情報が連携され、住民がマイナポータル経由、医療機関が医療機関用アプリ等経由でオンライン化(③④⑤⑥)が実現できる。()部が評価対象の事務、[]部については社会保険診療報酬支払基金(支払基金)がPIAを実施するため評価対象外)



(備考)

①特定個人情報の登録・管理

- ・本区は、予防接種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、予診情報・予防接種記録管理／請求支払システムにおいて対象者の個人番号を含む対象者情報と予防接種管理情報の紐付け及び登録を行う。(LGWAN回線等経由)
- ・本区は予診情報・予防接種記録管理／請求支払システムから接種記録等、必要な情報を自動連携またはダウンロードし、予防接種システム等への取込を行う。
- ・予診情報・予防接種記録管理／請求支払システムへ登録された個人情報へのアクセスは適切に制御される。

②PMHキー採番

- ・予診情報・予防接種記録管理／請求支払システムは、Public Medical Hubに対して個人番号を連携することで、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する。
- ・Public Medical Hubは、医療保険者等向け中間サーバーを経由しPMHキーを採番して予診情報・予防接種記録管理／請求支払システムに回答する。
- ・医療保険者等向け中間サーバーは、PMHキーと個人番号を紐付けて、PMHキーと紐付番号をオンライン資格確認等システムへ連携する。
- ・オンライン資格確認等システムは、紐付番号をキーに仮名識別子とPMHキーを紐付けて、マイナポータルに連携する。
- ・マイナポータルは、新たにPMH用の仮名識別子(PMH仮名識別子)を生成し、シリアル番号、仮名識別子、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連携する。(連携後、マイナポータル上からPMHキーは削除される。)以降、③④⑤⑥が可能となる。

③マイナポータルへの通知

- ・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経由で住民向けの通知を行うため、本区は予診情報・予防接種記録管理／請求支払システムを利用してマイナポータルに識別子(PMH仮名識別子)と通知情報を登録する。

④マイナポータルからの入力・取得(予診票・接種記録)

- ・住民は、マイナポータル経由で予診情報・予防接種記録管理／請求支払システムへの予診票の事前入力や、予診情報・予防接種記録管理／請求支払システムから接種記録や通知情報を閲覧/取得する。

⑤医療機関用アプリ等からの入力・取得(予診票・接種記録)

- ・医療機関が医療機関用アプリ等を利用し、接種時に住民からマイナンバーカードによる本人確認を経て、事前入力された予診票及び接種記録の閲覧/取得/入力を行う。

⑥ID5取得

- ・予防接種DBへの接種記録等の連携時に個人を特定する識別子情報として、予診情報・予防接種記録管理／請求支払システムが履歴照会回答システム経由でID5を取得する。

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

予防接種台帳ファイル

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 ※	予防接種法及び新型インフルエンザ等対策特別措置法その他関連法令で規定されている対象者のうち、個人番号を有する者	
その必要性	各種予防接種の対象者を把握し、予防接種に関する事務を行う上での基礎として利用するため。	
④記録される項目	[10項目以上50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 ※	・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 (予防接種履歴情報)	
その妥当性	【その他識別情報(内部番号)】 個人番号や住民基本情報との紐付けに使用するため。 【5情報】 送付先等の把握、予防接種履歴の登録に使用するため。 【連絡先(電話番号)】 届出内容に不明点があった際の問い合わせのため。 【健康・医療関係情報】【障害者福祉関係情報】【生活保護・社会福祉関係情報】 定期予防接種の対象者の確認、自己負担額免除者の確認に使用するため。 【その他(予防接種履歴情報)】 定期予防接種対象者の予防接種履歴を管理するため <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> 【個人番号】【その他識別情報(内部番号)】【その他住民票関係情報】 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。 【その他(予防接種履歴情報)】 (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2を参照。	
⑤保有開始日	平成28年1月	
⑥事務担当部署	保健予防課	

3. 特定個人情報の入手・使用

①入手元 ※	[○] 本人又は本人の代理人 [○] 評価実施機関内の他部署 (戸籍住民課、生活福祉課、障害者支援課) [] 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 (都道府県知事又は市町村長) [○] 民間事業者 (医療機関) [○] その他 (支払基金)
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 (Public Medical Hub、医療機関用アプリ等、マイナポータル)
③入手の時期・頻度	・現住者の住民票関係情報は、住民基本台帳システムから日次連携により取得する。 ・転入時に転出元市区町村への接種記録の照会が必要になる都度取得する。 ・予防接種健康被害による給付に関する申請情報は、障害年金は年1回、医療費・医療手当は年2回を基本として、本人または法定代理人等からの申請により取得する。 ・戸籍および住民票に記載のない児童の特定個人情報については、予診票発行の申請時に取得する。 <新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)事務> ・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、接種者から交付申請があった場合であって接種記録の照会が必要になる都度取得する。 <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> ・予診情報・予防接種記録管理／請求支払システムがPMHキーの採番処理依頼時に都度、Public Medical Hubから特定個人情報を入手する。 ・本区が予診情報・予防接種記録管理／請求支払システムに登録した予診票のひな形に対して、住民が接種前にマイナポータル等を介して予診票情報を入力することにより、本区が個人情報を入手し、予診情報・予防接種記録管理／請求支払システムにおいて個人番号と結びついて特定個人情報となる。 ・接種時に、医療機関のタブレットに搭載された医療機関用アプリ等又は医療機関での顔認証端末を用いて、住民がマイナンバーカードで認証することにより、医療機関が入力した予診票情報、接種記録を個人情報として入手し、予診情報・予防接種記録管理／請求支払システムにおいて個人番号と結びついて特定個人情報となる。
④入手に係る妥当性	・住民票関係情報については、住民基本台帳法本人情報確認事務であるため、本人情報入力に係る事務処理負担軽減のため、住民記録台帳システムから随時取得する。 ・予防接種健康被害の給付に関する申請情報は、予防接種法施行規則第10条、第11条および第11条の2から29までに基づき取得する。 ・戸籍及び住民票に記載のない児童の特定個人情報については、「平成19年6月20日厚生労働省健康局結核感染症課発事務連絡」の記載に基づき、定期予防接種を実施する目的で取得する。 <新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)事務> ・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、接種者から交付申請があった場合のみ入手する。 <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> (PMHキー採番処理依頼時に入手される特定個人情報) ・特定個人情報は、外部との情報連携のため、PMHキーの採番処理依頼時にPublic Medical Hubを経由して医療保険者等向け中間サーバーから自動的に入手される。 (その他:個人情報として入手し、予診情報・予防接種記録管理／請求支払システムにおいて個人番号と結び付き特定個人情報となる情報) 本区が入手する特定個人情報のうち、既存事務と同様に予診票に事前入力される事項は、本人又は本人の代理人から情報を入手し、予診票の医師記入欄及び接種記録は、予防接種を実施する医療機関から入手する。 ・予診票の事前入力のオンライン化により、住民の利便性の向上が図られる。マイナポータルではマイナンバーカードによる認証(本人確認)の後、本人又は本人の代理人の同意に基づいて情報が入力される。接種を受託する医療機関は、当該情報確認し、接種の可否を判断する。 ・医療機関において、タブレットに搭載された医療機関用アプリ等を用いた予診票の確認・接種記録がオンライン化されることにより住民及び医療機関の利便性の向上が図られる。また、情報の入手期間が短縮されることにより行政事務の効率化が図られる。医療機関での本人確認後、医療機関用アプリ等又は顔認証端末を用いて本人又は本人の代理人がマイナンバーカードで認証することにより、医療機関が予診票情報を確認して予診・問診を行い、接種後に接種記録の入力を行う。

⑤本人への明示		・住民票関係情報、身体障害者手帳情報および生活保護情報については、個人情報保護に関する法令に基づき取得・利用している。 ・予防接種健康被害の給付に関する申請関係情報の取得については、予防接種法施行規則第10条、第11条および第11条の2から29までに明記されている。 ＜新型コロナウイルス感染症対策に係る予防接種（特例臨時接種）事務＞ ・接種者からの接種証明書の交付申請に合わせて本人から入手する。 ＜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＞ ・本人又は本人の代理人から入手する情報については、利用目的を明示した上で入手している。マイナポータル等では、本人又は本人の代理人が画面に表示された利用目的を確認して、本人確認することにより入手する。
⑥使用目的 ※		各種予防接種対象者の管理、各種申請書への記載、予防接種に関する事務の基礎情報とするため
変更の妥当性		—
⑦使用の主体	使用部署 ※	保健予防課、品川保健センター、大井保健センター、荏原保健センター
	使用者数	〔 50人以上100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 ※		予防接種法に基づく、予防接種の実施 1. 定期予防接種対象者の接種履歴等の管理 2. 定期予防接種対象者への通知 3. 予診票の発行 4. 定期予防接種依頼書の発行 5. 予防接種証明書の発行 ＜新型コロナウイルス感染症対策に係る予防接種（特例臨時接種）事務＞ ・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。 ＜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、本区は、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答する。 ・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。
情報の突合 ※		予防接種システムに登録されている宛名番号、4情報を基に対象者を特定し、システム側で突合する。
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 ※		予防接種健康被害の給付の決定
⑨使用開始日		平成28年1月1日

4. 特定個人情報ファイルの取扱いの委託			
委託の有無 ※	☐ 委託する ☒ 委託しない (3) 件		
委託事項1	予防接種システムの保守		
①委託内容	予防接種システムのパッケージアプリケーション保守作業、職員からの問い合わせに対する調査、システムの定期診断等		
②取扱いを委託する特定個人情報ファイルの範囲	☐ 特定個人情報ファイルの全体 <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部		
対象となる本人の数	☐ 10万人以上100万人未満 <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上		
対象となる本人の範囲 ※	予防接種法及び新型インフルエンザ等対策特別措置法その他関連法令で規定されている対象者のうち、個人番号を有する者		
その妥当性	システムの運用保守全般を委託しており、システムにて管理する特定個人情報ファイルについても取扱う必要がある。		
③委託先における取扱者数	☐ 10人未満 <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上		
④委託先への特定個人情報ファイルの提供方法	☐ 専用線 ☐ 電子メール ☒ 電子記録媒体(フラッシュメモリを除く。) ☐ フラッシュメモリ ☐ 紙 ☐ その他 ()		
⑤委託先名の確認方法	下記、「⑥委託者名」の項の記載より確認できる。		
⑥委託先名	日本コンピューター株式会社		
再委託	⑦再委託の有無 ※	☐ 再委託しない ☒ 再委託する <選択肢> 1) 再委託する 2) 再委託しない	
	⑧再委託の許諾方法		
	⑨再委託事項		
委託事項2	番号連携サーバー(団体内統合宛名システム)の保守		
①委託内容	システムのアプリケーション開発・保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業、職員からの問い合わせに対する調査、作業指示に基づくデータ抽出等		
②取扱いを委託する特定個人情報ファイルの範囲	☐ 特定個人情報ファイルの全体 <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部		
対象となる本人の数	☐ 10万人以上100万人未満 <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上		
対象となる本人の範囲 ※	予防接種法及び新型インフルエンザ等対策特別措置法その他関連法令で規定されている対象者のうち、個人番号を有する者		
その妥当性	団体内統合宛名システムの運用保守全般を委託しており、システムにて管理する特定個人情報ファイルについても取扱う必要がある。		
③委託先における取扱者数	☐ 10人以上50人未満 <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上		

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 (5) 件 [☐] 移転を行っている () 件 [☐] 行っていない
提供先1	市町村長
①法令上の根拠	番号利用法第19条第8号に基づく主務省令第2条の表第25項
②提供先における用途	予防接種法(昭和二十三年法律第六十八号)による予防接種の実施に関する事務であって第二十七条で定めるもの
③提供する情報	予防接種法による予防接種の実施に関する情報であって第二十七条で定めるもの
④提供する情報の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
⑤提供する情報の対象となる本人の範囲	予防接種法等関連法令に定められる予防接種の対象者
⑥提供方法	[☐] 情報提供ネットワークシステム [☐] 専用線 [☐] 電子メール [☐] 電子記録媒体(フラッシュメモリを除く。) [☐] フラッシュメモリ [☐] 紙 [☐] その他 ()
⑦時期・頻度	照会を受けたら都度
提供先2	都道府県知事
①法令上の根拠	番号利用法第19条第8号に基づく主務省令第2条の表第26項
②提供先における用途	予防接種法による予防接種の実施に関する事務であって第二十八条で定めるもの
③提供する情報	予防接種法による予防接種の実施に関する情報であって第二十八条で定めるもの
④提供する情報の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
⑤提供する情報の対象となる本人の範囲	予防接種法等関連法令に定められる予防接種の対象者
⑥提供方法	[☐] 情報提供ネットワークシステム [☐] 専用線 [☐] 電子メール [☐] 電子記録媒体(フラッシュメモリを除く。) [☐] フラッシュメモリ [☐] 紙 [☐] その他 ()
⑦時期・頻度	照会を受けたら都度
提供先3	都道府県知事又は市町村長
①法令上の根拠	番号利用法第19条第8号に基づく主務省令第2条の表第153項
②提供先における用途	新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務であって第百五十五条で定めるもの
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第百五十五条で定めるもの

6. 特定個人情報の保管・消去

①保管場所 ※	＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 ＜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・プラットフォームは政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。 なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO・IEC27018の認証を受けている。 ・日本国内でデータを保管している。 ②特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する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。 ＜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。 ・サーバ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当区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。 ・国保中央会や医療機関及び住民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。				
②保管期間	<table border="1"> <tr> <td data-bbox="347 1093 478 1227">期間</td><td data-bbox="478 1093 1485 1227"> ＜選択肢＞ 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない </td></tr> <tr> <td data-bbox="347 1227 478 1294">その妥当性</td><td data-bbox="478 1227 1485 1294"> 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いる。 </td></tr> </table>	期間	＜選択肢＞ 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない	その妥当性	予防接種に関する記録は、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いる。
期間	＜選択肢＞ 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない				
その妥当性	予防接種に関する記録は、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いる。				
③消去方法	＜ガバメントクラウドにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 ＜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＞ ・本区の領域に保管されたデータのみ、予診情報・予防接種記録管理／請求支払システムを用いて消去することができる。 ・本区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。 ・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。				
7. 備考					
—					

(別添2) 特定個人情報ファイル記録項目

<予防接種システム>

1. 宛名番号
2. 漢字氏名
3. かな氏名
4. 生年月日
5. 年齢
6. 性別
7. 住登外者情報
8. 郵便番号
9. 住所
10. 電話番号
11. 接種名称
12. 接種数(期・回数)
13. 接種区分
14. 接種種別
15. Lot番号
16. 接種量
17. 登録日
18. 接種日
19. 接種医療機関
20. 予診票発行情報
21. 依頼書発行情報
22. 証明書発行情報
23. 自己負担区分
24. 生活保護等受給者情報
25. 障害者情報

<番号連携サーバー>

27. 個人番号
28. 団体内統合宛名番号

<中間サーバー>

29. 情報提供用個人識別符号

<新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)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/4回目/5回目/6回目/7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(※)
- ・接種名称
- ・接種種別
- ・接種量
- ・登録日
- ・接種医療機関
- ・予診票発行情報

※ 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

<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 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	
予防接種台帳ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	・申請書の内容や本人確認書類を照合し、対象者以外の情報の入手防止に努める ・予防接種システムにて対象者を検索する際、生年月日、氏名、住所等で照合し、対象者以外の情報の入手防止に努める ・庁内連携システムとの連携は、インタフェース仕様に基づき、対象者以外の情報や必要外の情報は入手しない。 ＜新型コロナウイルス感染症対策に係る予防接種（特例臨時接種）事務における追加措置＞ ・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、番号利用法第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。 ＜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＞ ・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。
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	必要な情報以外を誤って記載することがないよう、記入例等の案内書類を工夫する。また、他自治体から情報を入手する際は必要な情報以外の情報を入手してしまうことがないよう、事務マニュアルを整備し処理の標準化を図る。 ＜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＞ ・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。
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	・窓口において申請等があった場合、記載された申請書等は、窓口から離席する際は携行する等、職員の管理下に置くことを徹底する。 ・予防接種システムにアクセスした際には処理事由によってアクセスログに残された内容から処理目的を認識できる。 ＜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＞ ・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、システム自動処理により、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的に制御している。 ・予診情報・予防接種記録管理／請求支払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。
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	・申請書等と照合情報との相違がある場合は、申請者等に聞き取りを行い、申請書の内容を補正し、正確性を確保する。 ＜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＞ ・予診情報・予防接種記録管理／請求支払システムが提供した個人番号をPublic Medical Hubから加工することなく返却されるため、本人のものではない誤った個人番号を入手することはない。
個人番号の真正性確認の措置の内容	①既存住民基本台帳システム及び団体内統合宛名システムから入手した住民票関係情報並びに他システムから入手した資格情報等（課税区分、生保区分等のフラグ情報）については、入手元において本人確認を行っている。 ②窓口において入手する場合には、対面で個人番号カード又は身分証明書等の提示を受け、本人確認及び個人番号の真正性の確認を行う。 ＜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＞ ・予診情報・予防接種記録管理／請求支払システムが提供した個人番号をPublic Medical Hubから加工することなく返却されるため、本人のものではない誤った個人番号を入手することはない。
特定個人情報の正確性確保の措置の内容	・入手の段階において本人確認及び特定個人情報の正確性を確保している。 ・予診票送付により、万が一誤りを指摘された場合には、すぐに調査を行い修正を行っている。 ＜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＞ ・個人番号及び基本情報の正確性は、既存事務において住基システムとの連携等により担保されている。
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	・個人情報の記載のある文書は、鍵付の書庫に保管する。 ＜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＞ ・予診情報・予防接種記録管理／請求支払システムと支払基金の医療保険者等向け中間サーバーは、Public Medical Hubを経由した閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。 ・予防接種システムは、予診情報・予防接種記録管理／請求支払システムへの連携時にLGWAN回線による閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
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	
・予防接種システムにログインする際、IDとパスワードの入力が必要となり、特定の職員や作業従事者のみ照会できる	
3. 特定個人情報の使用	
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク	
宛名システム等における措置の内容	・宛名システム等は、必要な情報以外の紐付けが行われないよう、システム上で制限している。 ・他機関連携においては、事務に必要な情報の定められたインタフェースに基づいて連携しており、番号利用法に定められた情報のみを提供するように制限している。
事務で使用するその他のシステムにおける措置の内容	予防接種事務を行う上で必要な情報のみ連携している。 ＜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＞ ・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区の職員について、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。
その他の措置の内容	予防接種システムでは、管理者が職員ごとにアクセスできる項目を定めており、許可された者が許可された項目にだけアクセスできるようにシステムで制御している。
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	システムの利用可能な職員を特定し、職員ごとにIDとパスワードを設定し、承認を行っている。 ＜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＞ 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。 ・本区は、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。

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	人事異動があった場合には、適宜、システムに反映させている。 <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> ・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。 ・管理者は、アクセス権限の管理表を作成し、申請者に対して管理表に基づき適切なアクセス権限を付与する。 ・本区において、人事異動や退職等があった際は、異動情報に基づき、不要となったアクセス権限を管理し、失効させる。	
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	権限変更があった場合には、適宜、システムに反映させている。 <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> ・共用IDは発行せず、必ず個人に対し、ユーザーIDを発行する。 ・管理者が定期的に管理表を確認し、必要に応じて見直しを行う。	
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	システム上の操作のログを取得しており、操作ログを確認できる。 <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> ・本区は、システム上の操作のログを取得し、操作ログを定期的に確認する。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3： 従業者が事務外で使用するリスク		
リスクに対する措置の内容	・アクセスログを取得するとともに、不正に利用された場合にログを追跡できる仕組みを用意することで抑止を図る。 ・従業者に対するセキュリティ教育を年に1度行っている。 ・職員以外の従業者(委託先等)には、情報管理者の監督のもと、「情報セキュリティ基本方針」、「情報セキュリティ対策基準」を遵守するよう指導し、契約時にその内容を含める。 <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> ・本区は、特定個人情報を取り扱う職員に対して、セキュリティに関する研修を行い、個人情報保護の重要性について教育するとともに、業務外での特定個人情報の取扱いの禁止等の指導を徹底することで、事務外の使用を防止している。 ・委託業務については、委託先との契約により、委託業者が従業者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。本区は、当該教育の実施について履行確認を行う。再委託先においても同様の取扱いとする。 ・本区は、操作ログの追跡により不正アクセス者の特定が可能であることを周知徹底することで、コンプライアンスの意識を高め、事務外での使用を防止する。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

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	・予防接種システムの利用に際して、IDとパスワードが必要であり、外部の者に操作権限を与えていない。 ・スクリーンセ이버等を利用して、長時間にわたり本人確認情報を画面に表示させない。 ・予診票を印刷する際に、データの抽出を行う際は、利用可能な操作者を限定している。 ・端末のディスプレイを、来庁者から見えない位置に置く。 ＜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＞ ・既存システム(各業務システム)から特定個人情報を抽出したCSVファイルを予診情報・予防接種記録管理／請求支払システムへ登録する際は、作業を行う職員及び端末を必要最小限に限定する。 ・本区の既存システム(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特定個人情報の連携は、情報漏えいを防止するために暗号化された通信回線(LGWAN又はその他の閉域網回線)を利用した接続のみが認められる。 ・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。 ・システムにアクセスする職員について、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。	
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	①委託先の社会的信用と能力を確認する。 ②委託契約書及び「個人情報の保護に関する特記事項」により、個人情報の秘密保持、安全管理についての責任体制の整備等必要条件を付す。 ＜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＞ 本区は、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における特定個人情報の取扱いを東京都国保連合会に委託し、東京都国保連合会は国保中央会に再委託することとする。 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)に基づき、国保中央会の設備、技術水準、従業者に対する監督・教育の状況等を事前に確認する。	
特定個人情報ファイルの閲覧者・更新者の制限	[制限している]	＜選択肢＞ 1) 制限している 2) 制限していない
具体的な制限方法	①委託先には作業責任者及び作業従事者の届出を義務付けている。 ②閲覧又は更新権限を持つ者は必要最小限とする。 ③閲覧又は更新権限を持つ者のアカウント管理を行い、システム上で操作を制限する。 ④閲覧又は更新の履歴を記録し、必要に応じて不正な使用の有無を確認できるようにする。 ＜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＞ ・本区がアクセス権限の管理状況を確認できる。 ・本区は、アクセス権限を付与する者を必要最小限に限定する。 ・本区は、アクセス権限を付与する範囲を必要最小限に限定する。 ・本区は、アクセス権限を付与した者と権限の範囲を適切に管理する。 ※特定個人情報に係るアクセス権限は、再々委託先(PMHキー採番や運用保守)のみに付与される。	

特定個人情報ファイルの取扱いの記録		[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
	具体的な方法	・作業端末へのログイン記録やシステム保守における作業記録を残している。 <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> ・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取り扱いのログを保存し、本区は特定個人情報に係る操作のログを閲覧・出力できる。 ※再々委託先(PMHキー採番や運用保守)に係る特定個人情報の取扱いログに限られる。	
特定個人情報の提供ルール		[定めている]	<選択肢> 1) 定めている 2) 定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	・委託先から他者への特定個人情報の提供、ならびに当該情報の外部持ち出しを認めないことを契約書上明記する。 <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> ・委託先(再委託先及び再々委託先を含む。)から他者への提供は行わない。 ・本区は委託契約に基づき、委託先(再委託先及び再々委託先を含む。)から他者への提供が行われていないことを確認できる。	
	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	・委託先等への定期的な視察を行っている。 ・個人情報の管理状況について、日常運用においてチェックし、必要に応じて調査も行う。 <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> ・委託先(再委託先及び再々委託先を含む。)には、業務上、最低限必要な範囲の特定個人情報のみを提供できる。それ以外の提供は一切認められず、その旨を委託契約書にも明記する。 ・本区は委託契約に基づき、委託先(再委託先及び再々委託先を含む。)から契約書で定められた範囲の特定個人情報しか提供されていないことを確認できる。	
特定個人情報の消去ルール		[定めている]	<選択肢> 1) 定めている 2) 定めていない
	ルールの内容及びルール遵守の確認方法	・委託業者は、この契約による事務を終了したとき、または委託元が請求したときは、この契約に係る個人情報を直ちに委託元に返還しなければならない。また、機器の廃棄時は、磁気記録等装置に記録されている個人情報等を削除し復元ソフト等による復元が不可能な状態にし、または磁気記録等装置を物理的に破壊した上で撤去し、データ消去証明書を提出することを契約に含めている。 <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> ・委託契約終了後は予診情報・予防接種記録管理／請求支払システムに保管していた全ての特定個人情報を国保中央会が消去する。 ・特定個人情報を紙媒体で保管しない。 ・委託契約書に基づき、本区は消去について国保中央会から報告を受けることができ、それにより消去状況について確認が可能となる。	

委託契約書中の特定個人情報ファイルの取扱いに関する規定		[定めている] <選択肢> 1) 定めている 2) 定めていない
	規定の内容	委託先に対して、個人情報保護に関する法令に基づき、以下の規定を記載している。 ・直接または間接に知り得た個人情報を第三者に漏らしてはならない。また契約期間満了後も同様とする。 ・個人情報を業務の目的以外に使用してはならない。また第三者に提供してはならない。 ・個人情報の全部または一部を許可なく複写し、または複製してはならない。許可を受けて複写または複製したときは、当該複写物または複製物を焼却裁断等により利用できないように処分しなければならない。 ・個人情報の授受、保管および管理について、善良な管理者の注意をもってあたり、個人情報の消滅、き損等の事故を防止しなければならない。 ・契約を終了したとき、または委託者が請求したときは、その保有する個人情報を直ちに返還しなければならない。 ・委託者は、個人情報の管理状況について随時に立入検査または調査をし、必要な報告を求め、または委託事務の処理に関して指示を与えることができる。 ・事故が生じたときには、直ちに委託者に対して通知するとともに、遅滞なくその状況を書面をもって報告し、委託者の指示に従わなければならない。 <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> 東京都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。 ・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確保		[十分に行っている] <選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない 4) 再委託していない
	具体的な方法	委託先と同等のリスク対策を実施する。 <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> ・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、点検結果について東京都国保連合会及び本市市区町村に年1回報告を行う。
その他の措置の内容		<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> ・委託契約書に以下の規定を設ける。 委託先及び再委託先は、従業員に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。
リスクへの対策は十分か		[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
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		
—		

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	＜区における措置＞ ①番号利用法の規定に基づき、認められている範囲内において特定個人情報の照会を行う。 ②システムの利用可能な職員を特定し、職員ごとにIDとパスワードを設定し、承認を行っており、承認された職員以外が情報を入手できないように制御を行う。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報照会機能(※1)により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可照会リスト(※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、番号利用法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ②中間サーバーの職員認証・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。 (※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および照会した情報の受領を行う機能。 (※2) 番号利用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。 (※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。		
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク2: 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、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。		
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク3: 入手した特定個人情報が不正確であるリスク			
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ・中間サーバーは、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入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。		
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている	

リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク		
リスクに対する措置の内容	＜中間サーバー・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、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはできない。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク5: 不正な提供が行われるリスク		
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能(※)により、情報提供ネットワークシステムにおける照会許可照会リストを情報提供ネットワークシステムから入手し、中間サーバーにも格納して、情報提供機能により、照会許可照会リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 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、特定個人情報に不正に提供されるリスクに対応している。 ③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。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 (※)情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク6: 不適切な方法で提供されるリスク		
リスクに対する措置の内容	＜中間サーバー・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＞ 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・運用を行う事業者及びクラウドサービス事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク7: 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク		
リスクに対する措置の内容	＜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。	
リスクへの対策は十分か	[十分にである]	＜選択肢＞ 1) 特に力を入れている 2) 十分にである 3) 課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置		
＜中間サーバー・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・運用を行う事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。		
7. 特定個人情報の保管・消去		
リスク1: 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[十分に遵守している]	＜選択肢＞ 1) 特に力を入れて遵守している 2) 十分に遵守している 3) 十分に遵守していない 4) 政府機関ではない
②安全管理体制	[十分に整備している]	＜選択肢＞ 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
③安全管理規程	[十分に整備している]	＜選択肢＞ 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	＜選択肢＞ 1) 特に力を入れて周知している 2) 十分に周知している 3) 十分に周知していない

⑤物理的対策	[十分にしている] <選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分に行っていない
具体的な対策の内容	・記録媒体、紙媒体は鍵付の書庫に保管する。 ・データ消去処理は、情報を復元できないように処置した上で廃棄する。 <ガバメントクラウドにおける措置> ①ガバメントクラウドについては政府情報システムのセキュリティ制度 (ISMAP) のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、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。 <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・プラットフォームは、政府情報システムのためのセキュリティ評価制度 (ISMAP) に登録されたクラウドサービス事業者が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サービス事業者が実施する。 なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018の認証を受けている。 ・日本国内でデータ保管している。 <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> 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ため、特定個人情報の適正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の利用

⑥技術的対策	[十分に行っている] <選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的な対策の内容	・ウイルス対策ソフトを導入し、定期チェックを行うとともに、ウイルスパターン更新も随時行っている。 ・不正アクセス防止策として、ファイアウォールを導入している。 <ガバメントクラウドにおける措置> ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【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。 <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、侵入検知およ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。 ④中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤中間サーバーのデータベースに保存される特定個人情報、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ⑥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。 ⑦中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。 <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> 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ため、特定個人情報の適正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。 ・予診情報・予防接種記録管理／請求支払システムは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。 ・国保中央会や医療機関及び住民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、予診情報・予防接種記録管理／請求支払システムは外部からの侵入検知・通知機能を備えている。 ・本区の端末と予診情報・予防接種記録管理／請求支払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。 ・本区の端末と予診情報・予防接種記録管理／請求支払システムとの通信はL2WAN回線又は閉域網VPN等に限定されている。 ・クラウドマネージドサービスを利用する場合においても、パブリッククラウド事業者は特定個人情報にはアクセスできない。 ・バックアップは地理的に十分に離れた拠点に保管することで、大規模なシステム障害や震災などの発生によりデータが破損・消失しても、バックアップからデータを復元できるようにする。

⑦バックアップ	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
⑧事故発生時手順の策定・周知	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
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	・死者も現存者と同様の管理となっている	
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	・指定の保持年数を経過した場合に物理削除。 ・磁気ディスクの廃棄時は、記録されている個人情報等を削除し復元ソフト等による復元が不可能な状態にし、または物理的に破壊する仕組みとしている。 <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> ・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。	
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	・指定の保持年数を経過した場合は、パッケージ機能にて対象者情報を物理削除する。 ・磁気ディスクの廃棄時は、記録されている個人情報等を削除し復元ソフト等による復元が不可能な状態にし、または物理的に破壊する仕組みとしている。 ・申請書類等については、『品川区文書取扱規程第21条』に基づき適切な処理を行う。 <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。 <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> ・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。	
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	・特定個人情報の保護を担保するために、毎年評価書の記載通りの運用がなされているか「特定個人情報保護評価書運用報告書」で見直しを行う。 <中間サーバー・プラットフォームにおける措置> ①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。 <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> 本区は、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職員等の当該システムの利用を管理し、必要な自己点検を行う。	
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	評価実施機関内の内部監査を「情報セキュリティ監査実施ガイドライン」に基づき、以下の観点により定期的に実施し、監査結果を踏まえて体制や規定を改善する。なお、情報セキュリティ監査統括責任者は、副統括情報セキュリティ責任者(システム所管課長)をもって充て、情報セキュリティ監査統括責任者が指名する監査人によって、当監査を行う。 ・評価書記載事項と運用実態について確認する。 ・特定個人情報を取扱うシステムについて、適切なセキュリティ対策が実施され、かつ有効に機能していることを確認する。 <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> ①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政府情報システムのセキュリティ評価制度(ISMAP)に登録された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。 <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> 本区は、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職員等の当該システムの利用を管理し、必要な監査を行う。	
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	・職員に対しては、個人情報保護に関する研修の受講を義務付けている。 ・委託業者に対しては、個人情報保護に関する法令に基づき個人情報の保護を図るよう秘密保持契約を締結している。 ・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。 ・セキュリティ事故の情報を課内で共有するため、全員に回覧している。 ・全庁的な研修として、eラーニングによる情報セキュリティおよび個人情報保護研修を行っている。 <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。 <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> 本区は、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職員等の当該システムの利用を管理し、適切な指導を行う。	

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、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者による高い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、およ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。

＜事務運営に関する責任者の関与の仕組み＞

・副区長を議長とし、業務責任者をメンバーとする情報管理安全対策会議を設置し、特定個人情報をはじめとする個人情報保護や情報セキュリティ等に係るリスク管理を行う。

・情報管理安全対策会議では、リスク管理に係る監査・自己点検、教育・研修をはじめ、情報漏えい等のセキュリティ事案が発生した場合の対応訓練等の諸活動について、計画策定、実施状況のモニタリングを行い、各種の課題・問題を把握し、継続的な運用改善を行う。

＜特定個人情報の漏えい事案が発生した場合の対応＞

以下①～⑦について「マイナンバー事務に係る緊急事案等の報告手順」に則り対応する。

- ①組織内における報告、被害の拡大防止
- ②事実関係の調査、原因の究明
- ③影響範囲の特定
- ④再発防止策の検討・実施
- ⑤影響を受ける可能性のある本人の連絡等
- ⑥事実関係、再発防止策の公表
- ⑦個人情報保護委員会への報告

＜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＞

本区は、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。

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	〒140-8715 東京都品川区広町2丁目1番36号 品川区 保健予防課 予防接種担当	
②請求方法	本人が窓口または郵送で所定の様式により開示請求を申請する。	
	特記事項	
③手数料等	[有料] <選択肢> 1) 有料 2) 無料 手数料額: 写しの交付1枚につき10円 (手数料額、納付方法: 納付方法: 窓口の場合は現金、郵送の場合は納付書により金融機関に) て納付	
④個人情報ファイル簿の公表	[行っている] <選択肢> 1) 行っている 2) 行っていない	
	個人情報ファイル名	予防接種台帳ファイル
	公表場所	第三庁舎3階 区政資料コーナー
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	「1. ①請求先」と同じ	
②対応方法	問い合わせの受付時に受付票を起票し、対応について記録を残す。	

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和8年6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(任意に全項目評価を実施)] <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	「品川区区民意見公募手続の実施に関する要綱」に基づき、区民意見聴取を行う。区民意見聴取の実施に際しては、「広報しながわ」に、番号制度の概要と合わせ意見募集を行うことの記事を掲載し、品川区役所HP、区の広報紙への掲載(7月15日号)、保健予防課窓口、区政資料コーナーにおいて全文を閲覧できるようにする。
②実施日・期間	令和8年7月15日から令和8年8月14日
③期間を短縮する特段の理由	—
④主な意見の内容	
⑤評価書への反映	
3. 第三者点検	
①実施日	
②方法	
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6月1日	I-1 特定個人情報を取り扱う事務 ①事務の名称	—	本文中の「番号法」の表記について「番号利用法」に変更	事後	
令和6年6月1日	I-1 特定個人情報を取り扱う事務 ②事務の内容	【新型コロナウイルス感染症対策に係る予防接種（特例臨時接種）事務】 ①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番号の登録を行う。	【新型コロナウイルス感染症対策に係る予防接種（特例臨時接種）事務】 ①予防接種システムへ予防接種対象者及び発行した接種券番号の登録を行う。	事後	
令和6年6月1日	I-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 ③他のシステムとの接続	その他：ワクチン接種記録システム（VRS）	（削除）	事後	
令和6年6月1日	I-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2 ②システムの機能	④情報提供機能：各業務で管理している別表2の提供業務情報を受領し、中間サーバーへの情報提供を行う。	④情報提供機能：各業務で管理している提供業務情報を受領し、中間サーバーへの情報提供を行う。	事後	
令和6年6月1日	I-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	・ワクチン接種記録システム（VRS）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	・令和6年9月30日時点における接種記録等の特定個人情報の保管	事後	
令和6年6月1日	I-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 ③他のシステムとの接続	その他：予防接種システム	（削除）	事後	
令和6年6月1日	I-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5	—	（削除）	事後	
令和6年6月1日	I-5 個人番号の利用 法令上の根拠	・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）	（削除）	事後	
令和6年6月1日	I-5 個人番号の利用 法令上の根拠	1. 番号法 ・第9条第1項、別表第一10の項、別表第一93の2の項 2. 番号法第9条第1項別表第1の主務省令で定める事務を定める命令 ・第10条、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関係】 3. 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） ・第19条第6号（委託先への提供）	1. 番号利用法 ・第9条第1項、別表10の項、別表93の2の項 2. 番号利用法第9条第1項別表の主務省令で定める事務を定める命令 ・第10条、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関係】 3. 番号利用法 ・第19条第6号（委託先への提供）	事後	
令和6年6月1日	I-6 情報提供ネットワークシステム における情報連携 ②法令上の根拠	情報照会：番号法第19条第8号 別表第二項番16の2、16の3、17、18、19、115の2 情報提供：番号法第19条第8号 別表第二項番16の2、16の3、115の2	情報照会：番号利用法第19条第8号に基づく利用特定個人情報の提供に関する命令 第2条 表25、26、27、28、29 情報提供：番号利用法第19条第8号に基づく利用特定個人情報の提供に関する命令 第2条 表25、26	事後	
令和6年6月1日	II-3 特定個人情報の入手・使用 ①入手元、②入手方法	その他：ワクチン接種記録システム（VRS）	（削除）	事前	

令和6年6月1日	Ⅱ－3 特定個人情報の入手・使用 ③、④、⑤、⑧の新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)事務委託事項4	3. 特定個人情報の入手・使用 ③、④、⑤、⑧の新型コロナウイルス感染症対策に係る予防接種事務 ・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 委託事項4(新型コロナウイルスワクチン住民接種事務運営業務委託)	3.③、④、⑤、⑧の記載から削除 委託事項4を削除	事前	
令和6年6月1日	Ⅱ－3 特定個人情報の入手・使用 ⑤本人への明示	－	本文中の「品川区情報公開・個人情報保護条例」の表記について「個人情報保護に関する法令」に変更	事後	
令和6年6月1日	Ⅱ－4 特定個人情報の取り扱いの委託	－	本文中の「番号法」の表記について「番号利用法」に変更	事後	
令和6年6月1日	Ⅱ－4 特定個人情報の取り扱いの委託 委託事項3 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(特例臨時接種)事務に関するワクチン接種記録システム(VRS)を用いた特定個人情報ファイルの管理等	新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)事務に関するワクチン接種記録システム(VRS)内に記録されている令和6年9月30日時点の特定個人情報ファイルの保管	事後	
令和6年6月1日	Ⅱ－4 特定個人情報の取り扱いの委託 委託事項3 ②取り扱いを委託する特定個人情報ファイルの範囲 その妥当性	ワクチン接種記録システム(VRS)を用いた特定個人情報ファイルの適切な管理等のために取り扱う必要がある。	ワクチン接種記録システム(VRS)を用いた特定個人情報ファイルの適切な保管のために取り扱う必要がある。	事後	
令和6年6月1日	Ⅱ－4 特定個人情報の取り扱いの委託 委託事項3 ④委託先への特定個人情報ファイルの提供方法	その他:LGWAN回線を用いた提供(VRS)	(削除)	事後	
令和6年6月1日	Ⅱ－5 提供先1 ①法令上の根拠	番号利用法 第19条第8号 別表二の16の2の項	番号利用法第19条第8号に基づく利用特定個人情報の提供に関する命令 第2条 表25	事後	
令和6年6月1日	Ⅱ－5 提供先2	－	(削除)	事後	
令和6年6月1日	Ⅱ－5 提供先3 ①法令上の根拠	－	(削除)	事後	
令和6年6月1日	Ⅱ－5 提供先4	－	(削除)	事後	
令和6年6月1日	Ⅱ－6 特定個人情報の保管・消去 ①保管場所	＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)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、以下のとおりの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。	＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)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、以下のとおりの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、市区町村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。	事後	

令和6年6月1日	Ⅱ－6 特定個人情報の保管・消去 ①保管場所	(追加)	<ガバメントクラウドにおける措置> ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。	事後	
令和6年6月1日	Ⅱ－6 特定個人情報の保管・消去 ③消去方法	<ワクチン接種記録システム(VRS)における追加措置> ワクチン接種記録システム(VRS)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、以下のとおりの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。	<ワクチン接種記録システム(VRS)における追加措置> ・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	
令和6年6月1日	Ⅱ－6 特定個人情報の保管・消去 ③消去方法	(追加)	<ガバメントクラウドにおける措置> ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。	事後	
令和6年6月1日	Ⅲ－2 特定個人情報の入手 リスク1 対象者以外の情報の入手を防止するための措置の内容	－	本文中の「番号法」の表記について「番号利用法」に変更	事後	
令和6年6月1日	Ⅲ－2 特定個人情報の入手 新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)事務における追加措置	2. 特定個人情報の入手 <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> ・転入者本人からの個人番号の入手 ・他市区町村からの個人番号の入手 ・転出元市区町村からの接種記録の入手 ・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 ・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)	2. から「申請書からの個人情報の入手」以外の記載を削除。	事後	
令和6年6月1日	Ⅲ－2 リスク4 リスクに対する措置の内容		<ワクチン接種記録システム(VRS)における追加措置> 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。 (削除)	事後	

令和6年6月1日	Ⅲ－2 リスク4 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	＜ワクチン接種記録システム(VRS)における追加措置＞ ・入手した特定個人情報については、限定された端末を利用して国から配布されたユーザIDを使用し、ログインした場合だけアクセスできるように制御している。	(削除)	事後	
令和6年6月1日	Ⅲ－3 特定個人情報の使用 リスク1 宛名システム等における措置の内容	・他機関連携においては、事務に必要な情報の定められたインタフェースに基づいて連携しており、番号利用法別表第2に定められた情報のみを提供するように制限している。	・他機関連携においては、事務に必要な情報の定められたインタフェースに基づいて連携しており、番号利用法に定められた情報のみを提供するように制限している。	事後	
令和6年6月1日	Ⅲ－3 特定個人情報の使用 リスク1 事務で使用するその他のシステムにおける措置の内容	＜ワクチン接種記録システム(VRS)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(VRS)に接続するが、個人番号にはアクセスできないように制御している。	(削除)	事後	
令和6年6月1日	Ⅲ－3 特定個人情報の使用 リスク2 ユーザ認証の管理 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、LGWAN端末による操作に限り可能になるように制御している。 ・LGWAN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、国に対してユーザ登録を事前申請した者に限定して発行される。	(削除)	事後	
令和6年6月1日	Ⅲ－3 特定個人情報の使用 リスク2 アクセス権限の発行・失効の管理 具体的な管理方法	＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国に対してユーザ登録を事前申請した者に限定して発行される。	(削除)	事後	
令和6年6月1日	Ⅲ－3 特定個人情報の使用 リスク2 アクセスの管理 具体的な管理方法	＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国に対してユーザ登録を事前申請した者に限定して発行される。	(削除)	事後	
令和6年6月1日	Ⅲ－3 特定個人情報の使用 リスク4 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（特例臨時接種）事務における追加措置＞ 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(VRS)へ登録する際には、以下のようになっている。 ・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。	(削除)	事後	

令和6年6月1日	Ⅲ－３ 特定個人情報の使用 リスク４ 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 (特例臨時接種)事務における追加措置＞ ①特定個人情報を使用する場面を必要最小限に 限定している。具体的には以下の３つの場面に限 定している。 ・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。 ②ワクチン接種記録システム(VRS)からCSVファイ ルにてダウンロードする接種記録データには、個 人番号が含まれない。	(削除)	事後	
令和6年6月1日	Ⅲ－４ 特定個人情報の取り扱いの委 託 情報保護管理体制の確認	＜新型コロナウイルス感染症対策に係る予防接種 (特例臨時接種)事務における追加措置＞ 品川区、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)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対策に係る予防接種 (特例臨時接種)事務における追加措置＞ 品川区、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)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。	事後	
令和6年6月1日	Ⅲ－４ 特定個人情報の取り扱いの委 託 情報保護管理体制の確認	(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。)	(削除)	事後	
令和6年6月1日	Ⅲ－４ 特定個人情報の取り扱いの委 託 委託契約書中の特定個人情報 ファイルの取り扱いに関する規 定	－	本文中の「品川区情報公開・個人情報保護条例」 の表記について「個人情報保護に関する法令」に 変更	事後	
令和6年6月1日	Ⅲ－４ 特定個人情報の取り扱いの委 託 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 (特例臨時接種)事務における追加措置＞ 当区、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)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対策に係る予防接種 (特例臨時接種)事務における追加措置＞ 当区、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)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。	事後	
令和6年6月1日	Ⅲ－５ 特定個人情報の提供・移転 リスク１ 特定個人情報の提供・移転に 関するルール ルール内容及びルール順守 の確認方法	－	本文中の「番号法」の表記について「番号利用法」 に変更 本文中の「品川区情報公開・個人情報保護条例」 の表記について「個人情報保護に関する法令」に 変更	事後	
令和6年6月1日	Ⅲ－５ 特定個人情報の提供・移転 リスク３ 特定個人情報の提供・移転に おけるその他のリスクおよびそ のリスクに対する措置	＜ワクチン接種記録システム(VRS)における追加 措置＞ ・特定個人情報の提供は、限定された端末 (LGWAN端末)だけができるように制御している。	(削除)	事後	

令和6年6月1日	Ⅲー6 情報提供ネットワークシステムとの接続 リスク1 リスクに対する措置の内容	ー	本文中の「番号法」の表記について「番号利用法」に変更	事後	
令和6年6月1日	Ⅲー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（具体的な対策の内容）	（追加）	<ガバメントクラウドにおける措置> ①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、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。	事後	
令和6年6月1日	Ⅲー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（具体的な対策の内容）	（追加）	<ガバメントクラウドにおける措置> ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP（「地方公共団体情報システムのガバメントクラウドの利用に関する基準【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。	事前	
令和6年6月1日	（上段の続き）	（上段の続き）	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。	事前	
令和6年6月1日	（上段の続き）	（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ていない。 ・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。	（削除）	事前	
令和6年6月1日	Ⅲー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 消去手順・手順の内容	（追加）	<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/IEC 27001等に準拠したプロセスにしたがって確実にデータを消去する。	事前	

令和6年6月1日	Ⅲ－７ 特定個人情報の保管・消去 リスク1 ⑥技術的対策 具体的な対策の内容	<ワクチン接種記録システム(VRS)における措置> ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める技術的対策を満たしている。 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。 ・LGWAN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。	<ワクチン接種記録システム(VRS)における措置> ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める技術的対策を満たしている。 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、市区町村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。	事前	
令和6年6月1日	Ⅳ－１ 監査 ①自己点検 具体的なチェック方法	<新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)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、必要な監督をする。	<新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)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、必要な監督をする。	事前	
令和6年6月1日	Ⅳ－１ 監査 ②監査 具体的な内容	(追加)	<ガバメントクラウドにおける措置> ガバメントクラウドについては政府情報システムのセキュリティ制度(ISMAP)のリストに登録されたクラウドサービスから調達することとしており、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。	事前	
令和6年6月1日	Ⅳ－１ 監査 ②監査 具体的な内容	<新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)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、必要な監督をする。	<新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)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、必要な監督をする。	事前	
令和6年6月1日	Ⅳ－２ 従業員に対する教育・啓発 具体的な方法	－	本文中の「品川区情報公開・個人情報保護条例」の表記について「個人情報保護に関する法令」に変更	事前	
令和6年6月1日	Ⅳ－２ 従業員に対する教育・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。	(削除)	事前	

令和6年6月1日	Ⅳ－3 その他のリスク対策	(追加)	<ガバメントクラウドにおける措置> ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。 ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。 具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。	事前	
令和6年6月1日	Ⅳ－3 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(特例臨時接種)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。	(削除)	事前	
令和6年6月1日	(別添1)事務内容	・ワクチン接種記録システム(VRS)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	・ワクチン接種記録システム(VRS)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 ・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	事後	
令和6年6月1日	(別添2)ファイル記録項目	<予防接種システム> 24. 生活保護等受給者情報 25. 公害被害対象者情報 26. 障害者情報 <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> ・接種回(1回目/2回目/3回目)	<予防接種システム> 24. 生活保護等受給者情報 25. 障害者情報 <新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)に関する記録項目> ・接種回(1回目/2回目/3回目/4回目/5回目/6回目/7回目)	事前	
令和6年6月1日	V－1 特定個人情報の開示・訂正・利用停止請求 ②手数料等	手数料額:1件につき300円、写しの交付1枚につき10円	手数料額:写しの交付1枚につき10円	事後	
令和6年9月30日	I－1 特定個人情報を取り扱う事務 ②事務の内容	また、新型インフルエンザ等対策特別措置法(平成24年法律第31号)に基づき、新型インフルエンザ等が発生した場合において、同法第28条に基づく「特定接種」及び同法第46条に基づく「住民接種」の実施に関する事務を行う。	法改正による修正 また、新型インフルエンザ等対策特別措置法(平成24年法律第31号)に基づき、新型インフルエンザ等が発生した場合において、同法第28条に基づく「特定接種」の実施に関する事務を行う。	事後	
令和6年9月30日	(別添1)事務の内容	予防接種台帳管理システム	予防接種システム	事後	
令和6年9月30日	Ⅱ－3 特定個人情報の入手・使用 ①入手元、②入手方法	(追加)	[○] 本人又は本人の代理人 [○] 紙	事後	
令和6年9月30日	Ⅱ－3 特定個人情報の入手・使用 ①入手元	[○] 電子メール	(削除)	事後	

令和6年9月30日	Ⅱ－3 特定個人情報の入手・使用 ③入手の時期・頻度	・医療機関で実施した予防接種に関する記録を回収した医師会および医療機関より月1回取得する。 ・23区間の協定に基づき他区で接種した区民の予防接種に関する記録は、他区より年2回取得する。 ・品川区が発行した予防接種実施依頼書に基づき他自治体で実施した予防接種に関する記録は、他自治体および接種医療機関からの実施報告書により随時取得する。 ・生活保護、身体障害者手帳情報については、所管する部署から予防接種の予診票発行時に取得する。	(削除)	事後	
令和6年9月30日	Ⅱ－3 特定個人情報の入手・使用 ④入手に係る妥当性	・予防接種に関する記録については、予防接種法施行令第6条の2及び予防接種法施行規則第2条の7に示されてるとおり記録・保管する目的で取得する。	(削除)	事後	
令和6年9月30日	Ⅱ－3 特定個人情報の入手・使用 ⑤本人への明示	・予防接種に関する記録については、予防接種法等関連法令(予防接種法施行令第6条の2及び予防接種法施行規則第2条の7)に、区市町村が予防接種に関する記録の作成・保管する義務が明記されており、予防接種票においても、接種済の予防接種票が区に提出されることを明記し、本人(親権者)から署名を得た上で取得。 ・他自治体で予防接種を実施する際の予防接種に関する記録の入手については、区発行の依頼文に、実施した予防接種に関する記録について依頼先自治体より報告を受けることを明記している。	(削除)	事後	
令和6年9月30日	Ⅱ－3 特定個人情報の入手・使用 ⑧使用方法	予防接種健康被害は政治の給付の決定	予防接種健康被害の給付の決定	事後	
令和6年9月30日	Ⅱ－6 特定個人情報の保管・消去 ②保管期間	予防接種に関する記録は、予防接種法施行令第6条の2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いる。	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いる。	事後	
令和6年9月30日	Ⅲ－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	[○] 提供・移転しない	事後	

令和6年9月30日	Ⅲ－５ 特定個人情報の提供・移転 リスク１ 特定個人情報の提供・移転の 記録 具体的な方法	・移転は、庁内ネットワーク内や庁内システム間連 携のみであり、連携時のログにより確認できる。	未解決！	事後	
令和6年9月30日	Ⅲ－５ 特定個人情報の提供・移転 リスク１ 特定個人情報の提供・移転の 記録	記録を残している	(削除)	事後	
令和6年9月30日	Ⅲ－５ 特定個人情報の提供・移転 リスク１ 特定個人情報の提供・移転の 記録 具体的な方法	・移転は、庁内ネットワーク内や庁内システム間連 携のみであり、連携時のログにより確認できる。	(削除)	事後	
令和6年9月30日	Ⅲ－５ 特定個人情報の提供・移転 リスク１ 特定個人情報の提供・移転に 関するルール	定めている	(削除)	事後	
令和6年9月30日	Ⅲ－５ 特定個人情報の提供・移転 リスク１ 特定個人情報の提供・移転に 関するルール ルール内容及び遵守の確認 方法	・番号利用法で定められた事項及び『個人情報保 護に関する法令』の定めに従いルールを遵守す る。	(削除)	事後	
令和6年9月30日	Ⅲ－５ 特定個人情報の提供・移転 リスク１ リスクへの対策は十分か	十分である	(削除)	事後	
令和6年9月30日	Ⅲ－５ 特定個人情報の提供・移転 リスク２ リスクに対する措置の内容	・システムで制御した上で、庁内ネットワーク以外 での移転を禁止している。	(削除)	事後	
令和6年9月30日	Ⅲ－５ 特定個人情報の提供・移転 リスク２ リスクへの対策は十分か	十分である	(削除)	事後	
令和6年9月30日	Ⅲ－５ 特定個人情報の提供・移転 リスク３ リスクに対する措置の内容	・品質やセキュリティが保証されている連携システ ムでのみの移転に限定している。 ・移転に関する連携システムで十分な検証を行う。	(削除)	事後	
令和6年9月30日	Ⅲ－５ 特定個人情報の提供・移転 リスク３ リスクへの対策は十分か	十分である	(削除)	事後	
令和6年9月30日	Ⅵ－２ 国民・住民等からの意見の聴取 ④主な意見の内容	－	予防接種に関する事務概要全体図において、縦 円筒形の図はデータベースであれば、ファイルと するのではなくデータベースと明記すべきではな いか。	事後	
令和6年9月30日	Ⅵ－２ 国民・住民等からの意見の聴取 ⑤評価書への反映	－	なし	事後	
令和6年9月30日	Ⅵ－３ 第三者点検 ①実施日	－	令和7年9月17日	事後	

令和6年9月30日	Ⅵー3 第三者点検 ②方法	—	品川区個人情報保護審議会による第三者点検を実施	事後	
令和6年9月30日	Ⅵー3 第三者点検 ③結果	—	個人情報保護委員会が定める特定個人情報保護評価指針に基づき、評価が適切に行われているものと認められた。	事後	
令和7年7月1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 (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	提供を行っている 2件	事後	
令和7年7月1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 (委託に伴うものを除く。) 提供先1	都道府県知事又は市町村長	市町村長	事後	
令和7年7月1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 (委託に伴うものを除く。) 提供先1 ①法令上の根拠	番号利用法第19条第8号に基づく利用特定個人情報の提供に関する命令 第2条 表25	番号利用法第19条第8号に基づく主務省令第2条の表第25項	事後	
令和7年7月1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 (委託に伴うものを除く。) 提供先1 ②提供先における用途	予防接種法による予防接種の実施に関する事務であって主務省令で定めるもの	予防接種法(昭和二十三年法律第六十八号)による予防接種の実施に関する事務であって第二十七条で定めるもの	事後	
令和7年7月1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 (委託に伴うものを除く。) 提供先1 ③提供する情報	予防接種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	予防接種法による予防接種の実施に関する情報であって第二十七条で定めるもの	事後	
令和7年7月1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 (委託に伴うものを除く。) 提供先2	(追加)	都道府県知事	事後	
令和7年7月1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 (委託に伴うものを除く。) 提供先2 ①法令上の根拠	(追加)	番号利用法第19条第8号に基づく主務省令第2条の表第26項	事後	
令和7年7月1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 (委託に伴うものを除く。) 提供先2 ②提供先における用途	(追加)	予防接種法による予防接種の実施に関する事務であって第二十八条で定めるもの	事後	
令和7年7月1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 (委託に伴うものを除く。) 提供先2 ③提供する情報	(追加)	予防接種法による予防接種の実施に関する情報であって第二十八条で定めるもの	事後	

令和7年7月1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 (委託に伴うものを除く。) 提供先2 ④提供する情報の対象となる本人の数	(追加)	10万人以上100万人未満	事後	
令和7年7月1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 (委託に伴うものを除く。) 提供先2 ⑤提供する情報の対象となる本人の範囲	(追加)	予防接種法等関連法令に定められる予防接種の対象者	事後	
令和7年7月1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 (委託に伴うものを除く。) 提供先2 ⑥提供方法	(追加)	情報提供ネットワークシステム	事後	
令和7年7月1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 (委託に伴うものを除く。) 提供先2 ⑦時期・頻度	(追加)	照会を受けたら都度	事後	
令和7年7月1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	<ガバメントクラウドにおける措置> ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 <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。 ②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。 <ワクチン接種記録システム(VRS)における追加措置> ワクチン接種記録システム(VRS)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、以下のとおりの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、市区町村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。	<ガバメントクラウドにおける措置> ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 <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・プラットフォームは政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。 なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018の認証を受けている。 ・日本国内でデータを保管している。 ②特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する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。 <ワクチン接種記録システム(VRS)における追加措置> ワクチン接種記録システム(VRS)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、以下のとおりの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、市区町村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。	事後	

令和7年7月1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・紛失するリスクに対する措置の内容	<中間サーバー・ソフトウェアにおける措置> ①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。	<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、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはできない。	事後	
令和7年7月1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 リスクに対する措置の内容	<中間サーバー・ソフトウェアにおける措置> ①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用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。	<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用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・運用を行う事業者及びクラウドサービス事業者においては、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。	事後	

令和7年7月1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 情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	<中間サーバー・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。	<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・運用を行う事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。	事後
令和7年7月1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 ⑤物理的対策 具体的な対策の内容	・記録媒体、紙媒体は鍵付の書庫に保管する。 ・データ消去処理は、情報を復元できないように配置した上で廃棄する。 <ガバメントクラウドにおける措置> ①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、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。 <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、有人監視およ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。 ②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。 <ワクチン接種記録システム(VRS)における措置> ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める物理的対策を満たしている。 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。	・記録媒体、紙媒体は鍵付の書庫に保管する。 ・データ消去処理は、情報を復元できないように配置した上で廃棄する。 <ガバメントクラウドにおける措置> ①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、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。 <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・プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が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サービス事業者が実施する。 なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018の認証を受けている。 ・日本国内でデータ保管している。 <ワクチン接種記録システム(VRS)における措置> ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める物理的対策を満たしている。 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。	事後

令和7年7月1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 ⑥技術的対策 具体的な対策の内容	・ウイルス対策ソフトを導入し、定期チェックを行うとともに、ウイルスパターン更新も随時行っている。 ・不正アクセス防止策として、ファイアウォールを導入している。 ＜ガバメントクラウドにおける措置＞ ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【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。 ＜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、侵入検知およ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。 ＜ワクチン接種記録システム(VRS)における措置＞ ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める技術的対策を満たしている。 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、市区町村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。	(上位省略) 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。 ④中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤中間サーバーのデータベースに保存される特定個人情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ⑥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。 ⑦中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。 ＜ワクチン接種記録システム(VRS)における措置＞ ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める技術的対策を満たしている。 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、市区町村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。	事後
----------	---	--	--	----

令和7年7月1日	IVその他のリスク対策 1. 監査 ②監査 具体的な内容	評価実施機関内の内部監査を「情報セキュリティ監査実施ガイドライン」に基づき、以下の観点により定期的実施し、監査結果を踏まえて体制や規定を改善する。なお、情報セキュリティ監査統括責任者は、副統括情報セキュリティ責任者(システム所管課長)をもって充て、情報セキュリティ監査統括責任者が指名する監査人によって、当監査を行う。 ・評価書記載事項と運用実態について確認する。 ・特定個人情報を取扱うシステムについて、適切なセキュリティ対策が実施され、かつ有効に機能していることを確認する。 ＜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＞ ①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。 ＜新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)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、必要な監督をする。	評価実施機関内の内部監査を「情報セキュリティ監査実施ガイドライン」に基づき、以下の観点により定期的実施し、監査結果を踏まえて体制や規定を改善する。なお、情報セキュリティ監査統括責任者は、副統括情報セキュリティ責任者(システム所管課長)をもって充て、情報セキュリティ監査統括責任者が指名する監査人によって、当監査を行う。 ・評価書記載事項と運用実態について確認する。 ・特定個人情報を取扱うシステムについて、適切なセキュリティ対策が実施され、かつ有効に機能していることを確認する。 ＜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＞ ①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政府情報システムのセキュリティ評価制度(ISMAP)に登録された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。 ＜新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)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、必要な監督をする。	事前	
-----------------	---	---	---	-----------	--

令和7年7月1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> 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い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、およ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。 <事務運営に関する責任者の関与の仕組み> ・副区長を議長とし、業務責任者をメンバーとする情報管理安全対策会議を設置し、特定個人情報をはじめとする個人情報保護や情報セキュリティ等に係るリスク管理を行う。 ・情報管理安全対策会議では、リスク管理に係る監査・自己点検、教育・研修をはじめ、情報漏えい等のセキュリティ事象が発生した場合の対応訓練等の諸活動について、計画策定、実施状況のモニタリングを行い、各種の課題・問題を把握し、継続的な運用改善を行う。 <特定個人情報の漏えい事象が発生した場合の対応> 以下①～⑦について「マイナンバー事務に係る緊急事案等の報告手順」に則り対応する。 ①組織内における報告、被害の拡大防止 ②事実関係の調査、原因の究明 ③影響範囲の特定 ④再発防止策の検討・実施 ⑤影響を受ける可能性のある本人の連絡等 ⑥事実関係、再発防止策の公表 ⑦個人情報保護委員会への報告	<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、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者による高い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、およ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。 <事務運営に関する責任者の関与の仕組み> ・副区長を議長とし、業務責任者をメンバーとする情報管理安全対策会議を設置し、特定個人情報をはじめとする個人情報保護や情報セキュリティ等に係るリスク管理を行う。 ・情報管理安全対策会議では、リスク管理に係る監査・自己点検、教育・研修をはじめ、情報漏えい等のセキュリティ事象が発生した場合の対応訓練等の諸活動について、計画策定、実施状況のモニタリングを行い、各種の課題・問題を把握し、継続的な運用改善を行う。 <特定個人情報の漏えい事象が発生した場合の対応> 以下①～⑦について「マイナンバー事務に係る緊急事案等の報告手順」に則り対応する。 ①組織内における報告、被害の拡大防止 ②事実関係の調査、原因の究明 ③影響範囲の特定 ④再発防止策の検討・実施 ⑤影響を受ける可能性のある本人の連絡等 ⑥事実関係、再発防止策の公表 ⑦個人情報保護委員会への報告	事後	
----------	-----------------------------	--	--	----	--

令和8年6月1日	I-1 特定個人情報ファイルを取り扱う事務 ②事務の内容	予防接種法(昭和23年法律第68号)に基づき、A類疾病及びB類疾病のうち政令で定めるものについて、区内に居住する者に対し、期日又は期間を指定して予防接種を行うとともに、国・都への事業報告、実費の徴収等に関する事務を行う。また、新型コロナウイルス等対策特別措置法(平成24年法律第31号)に基づき、新型コロナウイルス等が発生した場合において、同法第28条に基づく「特定接種」の実施に関する事務を行う。 具体的には、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「番号利用法」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。 ①住民情報システムと連携し、予防接種システムより予防接種の対象者データの抽出 ②抽出した対象者データに基づき、予防接種を受ける際に必要な定期予防接種予診票(以下「予診票」という。)を予防接種の種類ごとに作成 ③予診票、予防接種の案内、契約医療機関一覧を封筒に同封し、対象者への個別発送 ④予防接種を実施した者の予診票が医師会および契約医療機関より送付された後、予防接種の種類ごとに、予防接種システムへ実施記録を登録 ⑤定期予防接種は種類ごとに接種期間が決められており、対象者で未接種の者を予防接種システムより抽出し、接種勧奨を個別に通知 ⑥転入及び紛失等にて、予診票がない住民より予診票の交付申請があった場合には、予防接種の履歴を確認し、予診票を作成する。 ⑦定期予防接種依頼書の発行 ⑧定期予防接種実施状況の報告 ⑨予防接種証明書の発行 ⑩健康被害救済の給付 【新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)事務】 ①予防接種システムへ予防接種対象者及び発行した接種券番号の登録を行う。 ②予防接種の実施後に接種記録等を登録、管理を行う。 ③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。	予防接種法(昭和23年法律第68号)に基づき、A類疾病及びB類疾病のうち政令で定めるものについて、区内に居住する者に対し、期日又は期間を指定して予防接種を行うとともに、国・都への事業報告、実費の徴収等に関する事務を行う。また、新型コロナウイルス等対策特別措置法(平成24年法律第31号)に基づき、新型コロナウイルス等が発生した場合において、同法第28条に基づく「特定接種」の実施に関する事務を行う。 具体的には、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「番号利用法」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。 ①住民情報システムと連携し、予防接種システムより予防接種の対象者データの抽出 ②抽出した対象者データに基づき、予防接種を受ける際に必要な定期予防接種予診票(以下「予診票」という。)を予防接種の種類ごとに作成 ③予診票、予防接種の案内、契約医療機関一覧を封筒に同封し、対象者への個別発送 ④予防接種を実施した者の予診票が医師会および契約医療機関より送付された後、予防接種の種類ごとに、予防接種システムへ実施記録を登録 ⑤定期予防接種は種類ごとに接種期間が決められており、対象者で未接種の者を予防接種システムより抽出し、接種勧奨を個別に通知 ⑥転入及び紛失等にて、予診票がない住民より予診票の交付申請があった場合には、予防接種の履歴を確認し、予診票を作成する。 ⑦定期予防接種依頼書の発行 ⑧定期予防接種実施状況の報告 ⑨予防接種証明書の発行 ⑩健康被害救済の給付 【新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)事務】 ①予防接種システムへ予防接種対象者及び発行した接種券番号の登録を行う。 ②予防接種の実施後に接種記録等を登録、管理を行う。 ③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。 【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】 ・本区は、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。 ・本区は、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。	事前	
令和8年6月1日	I-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 ③他のシステムとの接続	(追加)	[O]その他(予診情報・予防接種記録管理/請求支払システム)	事前	

令和8年6月1日	I-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 ②システムの機能 ③他のシステムとの接続	①ワクチン接種記録システム（VRS） ②・令和6年9月30日時点における接種記録等の特定個人情報の保管 ③（追加）	①予診情報・予防接種記録管理／請求支払システム 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予防接種事務＞ ①予防接種関連データの登録機能 本区は、予防接種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、接種勸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・予防接種記録管理／請求支払システムへ登録する。 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、本区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。 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。 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取得し、本人確認情報に紐づく予防接種対象者番号をキーに予診票情報を医療機関用アプリ等に提供する。また、医療機関が接種記録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予防接種対象者番号からPMHキーを特定し、PMHキーに紐づく接種記録を登録する。 ⑤情報連携機能（履歴照会回答システム） ・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接種記録等の情報を予防接種DBに連携し、予防接種DBにおいて予防接種の有効性・安全性等の調査・研究を行う。予診情報・予防接種記録管理／請求支払システムから履歴照会回答システムにPMHキーを連携し、履歴照会回答システムはオンライン資格確認等システムから被保険者番号等を取得し、履歴照会回答システム上で生成したID5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連携する。 ③〔〇〕 その他（予防接種システム、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）	事前	
-----------------	--	--	---	-----------	--

令和8年6月1日	I-5 個人番号の利用 法令上の根拠	1. 番号利用法 ・第9条第1項、別表10の項、別表93の2の項 2. 番号利用法第9条第1項別表の主務省令で定める事務を定める命令 ・第10条、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（特例臨時接種）事務関係】 3. 番号利用法 ・第19条第6号（委託先への提供）	1. 番号利用法 ・第9条第1項、別表14の項、126の項 2. 番号利用法別表の主務省令で定める事務を定める命令 ・第10条、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（特例臨時接種）事務関係】 【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関係】 3. 番号利用法 ・第19条第6号（委託先への提供）	事前	
令和8年6月1日	I-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	情報提供：番号利用法第19条第8号に基づく主務省令第2条の表25、26 情報照会：番号利用法第19条第8号に基づく主務省令第2条の表25、26、27、28、29	情報提供：番号利用法第19条第8号に基づく利用特定個人情報の提供に関する命令第2条の表25、26、153、154 情報照会：番号利用法第19条第8号に基づく利用特定個人情報の提供に関する命令第2条の表25、27、28、29、153	事後	

令和8年6月1日	(別添1) 事務内容	(追加)	全体図追加 (備考) ①特定個人情報の登録・管理 ・本区は、予防接種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、予診情報・予防接種記録管理／請求支払システムにおいて対象者の個人番号を含む対象者情報と予防接種管理情報の紐付け及び登録を行う。(LGWAN回線等経由) ・本区は予診情報・予防接種記録管理／請求支払システムから接種記録等、必要な情報を自動連携またはダウンロードし、予防接種システム等への取込を行う。 ・予診情報・予防接種記録管理／請求支払システムへ登録された個人情報へのアクセスは適切に制御される。 ②PMHキー採番 ・予診情報・予防接種記録管理／請求支払システムは、Public Medical Hubに対して個人番号を連携することで、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する。 ・Public Medical Hubは、医療保険者等向け中間サーバーを経由しPMHキーを採番して予診情報・予防接種記録管理／請求支払システムに回答する。 ・医療保険者等向け中間サーバーは、PMHキーと個人番号を紐付けて、PMHキーと紐付番号をオンライン資格確認等システムへ連携する。 ・オンライン資格確認等システムは、紐付番号をキーに仮名識別子とPMHキーを紐付けて、マイナポータルに連携する。 ・マイナポータルは、新たにPMH用の仮名識別子(PMH仮名識別子)を生成し、シリアル番号、仮名識別子、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連携する。(連携後、マイナポータル上からPMHキーは削除される。)以降、③④⑤⑥が可能となる。 ③マイナポータルへの通知 ・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経由で住民向けの通知を行うため、本区は予診情報・予防接種記録管理／請求支払システムを利用してマイナポータルに識別子(PMH仮名識別子)と通知情報を登録する。 ④マイナポータルからの入力・取得(予診票・接種記録) ・住民は、マイナポータル経由で予診情報・予防接種記録管理／請求支払システムへの予診票の事前入力や、予診情報・予防接種記録管理／請求支払システムから接種記録や通知情報を閲覧/取得する。 ⑤医療機関用アプリ等からの入力・取得(予診票・接種記録) ・医療機関が医療機関用アプリ等を利用し、接種時に住民からマイナバーカードによる本人確認を経て、事前入力された予診票及び接種記録の閲覧/取得/入力を行う。 ⑥ID5取得 ・予防接種DBへの接種記録等の連携時に個人を特定する識別子情報として、予診情報・予防接種記録管理／請求支払システムが履歴照会回答システム経由でID5を取得する。	事前	
----------	------------	------	---	----	--

令和8年6月1日	Ⅱ 特定個人情報ファイルの概要 2. 基本情報 ④記録される項目 主な記録項目	(追加)	☐ 個人番号 ☐ その他住民票関係情報	事前	
令和8年6月1日	Ⅱ 特定個人情報ファイルの概要 2. 基本情報 ④記録される項目 その妥当性	【その他識別情報(内部番号)】 個人番号や住民基本情報との紐付けに使用するため。 【5情報】 送付先等の把握、予防接種履歴の登録に使用するため。 【連絡先(電話番号)】 届出内容に不明点があった際の問い合わせのため。 【健康・医療関係情報】【障害者福祉関係情報】 【生活保護・社会福祉関係情報】 定期予防接種の対象者の確認、自己負担額免除者の確認に使用するため。 【その他(予防接種履歴情報)】 定期予防接種対象者の予防接種履歴を管理するため	【その他識別情報(内部番号)】 個人番号や住民基本情報との紐付けに使用するため。 【5情報】 送付先等の把握、予防接種履歴の登録に使用するため。 【連絡先(電話番号)】 届出内容に不明点があった際の問い合わせのため。 【健康・医療関係情報】【障害者福祉関係情報】 【生活保護・社会福祉関係情報】 定期予防接種の対象者の確認、自己負担額免除者の確認に使用するため。 【その他(予防接種履歴情報)】 定期予防接種対象者の予防接種履歴を管理するため 〈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〉 【個人番号】【その他識別情報(内部番号)】【その他住民票関係情報】 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。 【その他(予防接種履歴情報)】 (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。	事前	
令和8年6月1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 ①入手元	(追加)	☐ 民間事業者(医療機関) ☐ その他(支払基金)	事前	
令和8年6月1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	(追加)	☐ その他(Public Medical Hub、医療機関用アプリ等、マイナポータル)	事前	
令和8年6月1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 ③入手の時期・頻度	・現住者の住民票関係情報は、住民基本台帳システムから日次連携により取得する。 ・転入時に転出元市区町村への接種記録の照会が必要になる都度取得する。 ・予防接種健康被害による給付に関する申請情報は、障害年金は年1回、医療費・医療手当は年2回を基本として、本人または法定代理人等からの申請により取得する。 ・戸籍および住民票に記載のない児童の特定個人情報については、予診票発行の申請時に取得する。 〈新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)事務〉 ・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、接種者から交付申請があった場合であって接種記録の照会が必要になる都度取得する。	・現住者の住民票関係情報は、住民基本台帳システムから日次連携により取得する。 ・転入時に転出元市区町村への接種記録の照会が必要になる都度取得する。 ・予防接種健康被害による給付に関する申請情報は、障害年金は年1回、医療費・医療手当は年2回を基本として、本人または法定代理人等からの申請により取得する。 ・戸籍および住民票に記載のない児童の特定個人情報については、予診票発行の申請時に取得する。 (中間省略) 〈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／請求支払システムがPMHキーの採番処理依頼時に都度、Public Medical Hubから特定個人情報を入手する。 ・本区が予診情報・予防接種記録管理／請求支払システムに登録した予診票のひな形に対して、住民が接種前にマイナポータル等を介して予診票情報を入力することにより、本区が個人情報を入力し、予診情報・予防接種記録管理／請求支払システムにおいて個人番号と結びついて特定個人情報となる。 ・接種時に、医療機関のタブレットに搭載された医療機関用アプリ等又は医療機関での顔認証端末を用いて、住民がマイナンバーカードで認証することにより、医療機関が入力した予診票情報、接種記録を個人情報として入手し、予診情報・予防接種記録管理／請求支払システムにおいて個人番号と結びついて特定個人情報となる。	事前	

令和8年6月1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 ④入手に係る妥当性	・住民票関係情報については、住民基本台帳法本人情報確認事務であるため、本人情報入力に係る事務処理負荷軽減のため、住民記録台帳システムから随時取得する。 ・予防接種健康被害の給付に関する申請情報は、予防接種法施行規則第10条、第11条および第11条の4に基づき取得する。 ・戸籍及び住民票に記載のない児童の特定個人情報については、「平成19年6月20日厚生労働省健康局結核感染症課発事務連絡」の記載に基づき、定期予防接種を実施する目的で取得する。 〈新型コロナウイルス感染症対策に係る予防接種（特例臨時接種）事務〉 ・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、接種者から交付申請があった場合のみ入手する。	・住民票関係情報については、住民基本台帳法本人情報確認事務であるため、本人情報入力に係る事務処理負荷軽減のため、住民記録台帳システムから随時取得する。 ・予防接種健康被害の給付に関する申請情報は、予防接種法施行規則第10条、第11条および第11条の2から29までにに基づき取得する。 ・戸籍及び住民票に記載のない児童の特定個人情報については、「平成19年6月20日厚生労働省健康局結核感染症課発事務連絡」の記載に基づき、定期予防接種を実施する目的で取得する。 （中間省略） 〈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〉（PMHキー採番処理依頼時に入手される特定個人情報） ・特定個人情報は、外部との情報連携のため、PMHキーの採番処理依頼時にPublic Medical Hubを経由して医療保険者等向け中間サーバーから自動的に入手される。 （その他：個人情報として入手し、予診情報・予防接種記録管理／請求支払システムにおいて個人番号と結び付き特定個人情報となる情報） 本区が入手する特定個人情報のうち、既存事務と同様に予診票に事前入力される事項は、本人又は本人の代理人から情報を入力し、予診票の医師記入欄及び接種記録は、予防接種を実施する医療機関から入手する。 ・予診票の事前入力のオンライン化により、住民の利便性の向上が図られる。マイナポータルではマイナンバーカードによる認証（本人確認）の後、本人又は本人の代理人の同意に基づいて情報が入力される。接種を受託する医療機関は、当該情報確認し、接種の可否を判断する。 ・医療機関において、タブレットに搭載された医療機関用アプリ等を用いた予診票の確認・接種記録がオンライン化されることにより住民及び医療機関の利便性の向上が図られる。また、情報の入手期間が短縮されることにより行政事務の効率化が図られる。医療機関での本人確認後、医療機関用アプリ等又は顔認証端末を用いて本人又は本人の代理人がマイナンバーカードで認証することにより、医療機関が予診票情報を確認して予診・問診を行い、接種後に接種記録の入力を行う。	事前	
令和8年6月1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本人への明示	・住民票関係情報、身体障害者手帳情報および生活保護情報については、個人情報保護に関する法令に基づき取得・利用している。 ・予防接種健康被害の給付に関する申請関係情報の取得については、予防接種法施行規則第10条、第11条および第11条の4に明記されている。 〈新型コロナウイルス感染症対策に係る予防接種（特例臨時接種）事務〉 ・接種者からの接種証明書の交付申請に合わせて本人から入手する。	・住民票関係情報、身体障害者手帳情報および生活保護情報については、個人情報保護に関する法令に基づき取得・利用している。 ・予防接種健康被害の給付に関する申請関係情報の取得については、予防接種法施行規則第10条、第11条および第11条の2から29までに明記されている。 〈新型コロナウイルス感染症対策に係る予防接種（特例臨時接種）事務〉 ・接種者からの接種証明書の交付申請に合わせて本人から入手する。 〈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〉 ・本人又は本人の代理人から入手する情報については、利用目的を明示した上で入手している。マイナポータル等では、本人又は本人の代理人が画面に表示された利用目的を確認して、本人確認することにより入手する。	事前	

令和8年6月1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	予防接種法に基づく、予防接種の実施 1. 定期予防接種対象者の接種履歴等の管理 2. 定期予防接種対象者への通知 3. 予診票の発行 4. 定期予防接種依頼書の発行 5. 予防接種証明書の発行 〈新型コロナウイルス感染症対策に係る予防接種（特例臨時接種）事務〉 ・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。 〈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、本区は、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。	事前	
令和8年6月1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3	新型コロナウイルス感染症対策に係る予防接種（特例臨時接種）事務に関するワクチン接種記録システム（VRS）内に記録されている令和6年9月30日時点の特定個人情報ファイルの保管	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	事前
令和8年6月1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3 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（特例臨時接種）事務に関するワクチン接種記録システム（VRS）内に記録されている令和6年9月30日時点の特定個人情報ファイルの保管	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	事前
令和8年6月1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3 ②取扱いを委託する特定個人情報ファイルの範囲 その妥当性	ワクチン接種記録システム（VRS）を用いた特定個人情報ファイルの適切な保管のために取り扱う必要がある。	予診情報・予防接種記録管理／請求支払システムは公益社団法人国民健康保険中央会（以下、国保中央会という。）が構築し、希望する市区町村が利用するが、その適切な管理のため運用保守、PMHキーの採番において特定個人情報ファイルを取り扱う必要がある。 ただし、予診情報・予防接種記録管理／請求支払システムに格納された特定個人情報は、自動処理により再々委託先（これ以降の全ての委託を含む。以下、同じ。）に情報連携されるため、東京都国民健康保険団体連合会（以下、東京都国保連合会という。）及び国保中央会は特定個人情報にアクセスすることはない。	事前
令和8年6月1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3 ④委託先への特定個人情報ファイルの提供方法	(追加)	[○] その他(LGWAN又は閉域網回線を用いた提供)	事前

令和8年6月1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3 ⑥委託先名	株式会社ミラボ	東京都国保連合会	事前	
令和8年6月1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3 ⑦再委託の有無	再委託しない	再委託する	事前	
令和8年6月1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3 ⑧再委託の許諾方法	(追加)	書面又は電磁的方法による承諾	事前	
令和8年6月1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3 ⑨再委託事項	(追加)	〈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。	事前	
令和8年6月1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 (委提供・移転の有無)	提供を行っている 2件	提供を行っている 5件	事後	
令和8年6月1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 (委託に伴うものを除く。) 提供先3	(追加)	(以下追加) 番号利用法第19条第8号に基づく主務省令第2条の表第28項	事後	
令和8年6月1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 (委託に伴うものを除く。) 提供先3	(追加)	(以下追加) 番号利用法第19条第8号に基づく主務省令第2条の表第153項	事後	
令和8年6月1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 (委託に伴うものを除く。) 提供先4	(追加)	(以下追加) 番号利用法第19条第8号に基づく主務省令第2条の表第154項	事後	

令和8年6月1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	＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 ＜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・プラットフォームは政府情報システムのためのセキュリティ評価制度 (ISMAP) に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。 なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO・IEC27018の認証を受けている。 ・日本国内でデータを保管している。 ②特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する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。 ＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)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、以下のとおりの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、市区町村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。	＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 ＜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・プラットフォームは政府情報システムのためのセキュリティ評価制度 (ISMAP) に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。 なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO・IEC27018の認証を受けている。 ・日本国内でデータを保管している。 ②特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する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。 ＜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。 ・サーバ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。 ・国保中央会や医療機関及び住民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。	事前	
----------	---	--	--	----	--

令和8年6月1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	＜ガバメントクラウドにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 ＜ワクチン接種記録システム(VRS)における追加措置＞ ・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。	＜ガバメントクラウドにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 ＜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＞ ・本区の領域に保管されたデータのみ、予診情報・予防接種記録管理／請求支払システムを用いて消去することができる。 ・本区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。 ・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。	事前	
----------	---	---	---	----	--

令和8年6月1日	(別添2) 特定個人情報ファイル記録項目	(省略)	(上記省略) <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 ・勧奨情報(ルールID、勧奨日) (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)	事前
----------	----------------------	------	--	----

令和8年6月1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. リスク1⑨を除く。) 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク1： 目的外の入手が行われるリスク 対象者以外の情報の入手を防止するための措置の内容	・申請書の内容や本人確認書類を照合し、対象者以外の情報の入手防止に努める ・予防接種システムにて対象者を検索する際、生年月日、氏名、住所等で照合し、対象者以外の情報の入手防止に努める ・市内連携システムとの連携は、インタフェース仕様に基づき、対象者以外の情報や必要外の情報は入手しない。 ・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、番号利用法第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、番号利用法第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。	・申請書の内容や本人確認書類を照合し、対象者以外の情報の入手防止に努める ・予防接種システムにて対象者を検索する際、生年月日、氏名、住所等で照合し、対象者以外の情報の入手防止に努める ・市内連携システムとの連携は、インタフェース仕様に基づき、対象者以外の情報や必要外の情報は入手しない。 ・新型コロナウイルス感染症対策に係る予防接種（特例臨時接種）事務における追加措置 ・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、番号利用法第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。 ・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 ・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。	事前	
令和8年6月1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. リスク1⑨を除く。) 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 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	必要な情報以外を誤って記載することがないよう、記入例等の案内書類を工夫する。また、他自治体から情報を入手する際は必要な情報以外の情報を入手してしまうことがないよう、事務マニュアルを整備し処理の標準化を図る。	必要な情報以外を誤って記載することがないよう、記入例等の案内書類を工夫する。また、他自治体から情報を入手する際は必要な情報以外の情報を入手してしまうことがないよう、事務マニュアルを整備し処理の標準化を図る。 ・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 ・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的に制御している。 ・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的に制御している。 ・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的に制御している。	事前	

令和8年6月1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. リスク1⑨を除く。) 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	・窓口において申請等があった場合、記載された申請書等は、窓口から離席する際は携行する等、職員の管理下に置くことを徹底する。 ・予防接種システムにアクセスした際には処理事由によってアクセスログに残された内容から処理目的を認識できる。 ＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)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。	・窓口において申請等があった場合、記載された申請書等は、窓口から離席する際は携行する等、職員の管理下に置くことを徹底する。 ・予防接種システムにアクセスした際には処理事由によってアクセスログに残された内容から処理目的を認識できる。 ＜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＞ ・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、システム自動処理により、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的に制御している。 ・予診情報・予防接種記録管理／請求支払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。	事前	
令和8年6月1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. リスク1⑨を除く。) 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3: 入手した特定個人情報が入手の際の本人確認の措置の内容	・申請書等と照合情報との相違がある場合は、申請者等に聞き取りを行い、申請書の内容を補正し、正確性を確保する。	・申請書等と照合情報との相違がある場合は、申請者等に聞き取りを行い、申請書の内容を補正し、正確性を確保する。 ＜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＞ ・予診情報・予防接種記録管理／請求支払システムが提供した個人番号をPublic Medical Hubから加工することなく返却されるため、本人のものではない誤った個人番号を入手することはない。	事前	
令和8年6月1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. リスク1⑨を除く。) 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3: 入手した特定個人情報が入手の際の本人確認の措置の内容	①既存住民基本台帳システム及び団体内統合宛名システムから入手した住民票関係情報並びに他システムから入手した資格情報等(課税区分、生保区分等のフラグ情報)については、入手元において本人確認を行っている。 ②窓口において入手する場合には、対面で個人番号カード又は身分証明書等の提示を受け、本人確認及び個人番号の真正性の確認を行う。	①既存住民基本台帳システム及び団体内統合宛名システムから入手した住民票関係情報並びに他システムから入手した資格情報等(課税区分、生保区分等のフラグ情報)については、入手元において本人確認を行っている。 ②窓口において入手する場合には、対面で個人番号カード又は身分証明書等の提示を受け、本人確認及び個人番号の真正性の確認を行う。 ＜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＞ ・予診情報・予防接種記録管理／請求支払システムが提供した個人番号をPublic Medical Hubから加工することなく返却されるため、本人のものではない誤った個人番号を入手することはない。	事前	
令和8年6月1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. リスク1⑨を除く。) 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3: 入手した特定個人情報が入手の際の本人確認の措置の内容	・入手の段階において本人確認及び特定個人情報の正確性を確保している。 ・予診票送付により、万が一誤りを指摘された場合には、すぐに調査を行い修正を行っている。	・入手の段階において本人確認及び特定個人情報の正確性を確保している。 ・予診票送付により、万が一誤りを指摘された場合には、すぐに調査を行い修正を行っている。 ＜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＞ ・個人番号及び基本情報の正確性は、既存事務において住基システムとの連携等により担保されている。	事前	

令和8年6月1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. リスク1⑨を除く。) 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 リスクに対する措置の内容	・個人情報の記載のある文書は、鍵付の書庫に保管する。	・個人情報の記載のある文書は、鍵付の書庫に保管する。 ＜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＞ ・予診情報・予防接種記録管理／請求支払システムと支払基金の医療保険者等向け中間サーバーは、Public Medical Hubを経由した閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。 ・予防接種システムは、予診情報・予防接種記録管理／請求支払システムへの連携時にLGWAN回線による閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。	事前	
令和8年6月1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. リスク1⑨を除く。) 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	予防接種事務を行う上で必要な情報のみ連携している。	予防接種事務を行う上で必要な情報のみ連携している。 ＜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＞ ・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区の職員について、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。	事前	
令和8年6月1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. リスク1⑨を除く。) 3. 特定個人情報の使用 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 具体的な管理方法	システムの利用可能な職員を特定し、職員ごとにIDとパスワードを設定し、承認を行っている。	システムの利用可能な職員を特定し、職員ごとにIDとパスワードを設定し、承認を行っている。 ＜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＞ 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。 ・本区は、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。	事前	
令和8年6月1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. リスク1⑨を除く。) 3. 特定個人情報の使用 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 アクセス権限の発効・失効の管理 具体的な管理方法	人事異動があった場合には、適宜、システムに反映させている。	人事異動があった場合には、適宜、システムに反映させている。 ＜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＞ ・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。 ・管理者は、アクセス権限の管理表を作成し、申請者に対して管理表に基づき適切なアクセス権限を付与する。 ・本区において、人事異動や退職等があった際は、異動情報に基づき、不要となったアクセス権限を管理し、失効させる。	事前	

令和8年6月1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. リスク1⑨を除く。) 3. 特定個人情報の使用 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 アクセス権限の管理 具体的な管理方法	権限変更があった場合には、適宜、システムに反映させている。	権限変更があった場合には、適宜、システムに反映させている。 ＜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＞ ・共用IDは発行せず、必ず個人に対し、ユーザーIDを発行する。 ・管理者が定期的に管理表を確認し、必要に応じで見直しを行う。	事前	
令和8年6月1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. リスク1⑨を除く。) 3. 特定個人情報の使用 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 特定個人情報の使用の記録 具体的な方法	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。	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。 ＜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＞ ・本区は、システム上の操作のログを取得し、操作ログを定期的に確認する。	事前	
令和8年6月1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. リスク1⑨を除く。) 3. 特定個人情報の使用 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	・アクセスログを取得するとともに、不正に利用された場合にログを追跡できる仕組みを用意することで抑止を図る。 ・従業者に対するセキュリティ教育を年に1度行っている。 ・職員以外の従業者(委託先等)には、情報管理者の監督のもと、「情報セキュリティ基本方針」、「情報セキュリティ対策基準」を遵守するよう指導し、契約時にその内容を含める。	・アクセスログを取得するとともに、不正に利用された場合にログを追跡できる仕組みを用意することで抑止を図る。 ・従業者に対するセキュリティ教育を年に1度行っている。 ・職員以外の従業者(委託先等)には、情報管理者の監督のもと、「情報セキュリティ基本方針」、「情報セキュリティ対策基準」を遵守するよう指導し、契約時にその内容を含める。 ＜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＞ ・本区は、特定個人情報を取り扱う職員に対して、セキュリティに関する研修を行い、個人情報保護の重要性について教育するとともに、業務外での特定個人情報の取扱いの禁止等の指導を徹底することで、事務外の使用を防止している。 ・委託業務については、委託先との契約により、委託業者が従業者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。本区は、当該教育の実施について履行確認を行う。再委託先においても同様の取扱とする。 ・本区は、操作ログの追跡により不正アクセス者の特定が可能であることを周知徹底することで、コンプライアンスの意識を高め、事務外での使用を防止する。	事前	
令和8年6月1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. リスク1⑨を除く。) 3. 特定個人情報の使用 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	・予防接種システムの利用に際して、IDとパスワードが必要であり、外部の者に操作権限を与えていない。 ・スクリーンセ이버等を利用して、長時間にわたり本人確認情報を画面に表示させない。 ・予診票を印刷する際に、データの抽出を行う際は、利用可能な操作者を限定している。 ・端末のディスプレイを、来庁者から見えない位置に置く。	・予防接種システムの利用に際して、IDとパスワードが必要であり、外部の者に操作権限を与えていない。 ・スクリーンセ이버等を利用して、長時間にわたり本人確認情報を画面に表示させない。 ・予診票を印刷する際に、データの抽出を行う際は、利用可能な操作者を限定している。 ・端末のディスプレイを、来庁者から見えない位置に置く。 ＜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＞ ・既存システム(各業務システム)から特定個人情報を抽出したCSVファイルを予診情報・予防接種記録管理／請求支払システムへ登録する際は、作業を行う職員及び端末を必要最小限に限定する。 ・本区の既存システム(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特定個人情報の連携は、情報漏えいを防止するために暗号化された通信回線(LGWAN又はその他の閉域網回線)を利用した接続のみが認められる。 ・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。 ・システムにアクセスする職員について、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。	事前	

令和8年6月1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. リスク1⑨を除く。) 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	①委託先の社会的信用と能力を確認する。 ②委託契約書及び「個人情報の保護に関する特記事項」により、個人情報の秘密保持、安全管理についての責任体制の整備等必要条件を付す。 〈新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)事務における追加措置〉 品川区、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)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。	①委託先の社会的信用と能力を確認する。 ②委託契約書及び「個人情報の保護に関する特記事項」により、個人情報の秘密保持、安全管理についての責任体制の整備等必要条件を付す。 〈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〉 本区は、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における特定個人情報の取扱いを東京都国保連合会に委託し、東京都国保連合会は国保中央会に再委託することとする。 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)に基づき、国保中央会の設備、技術水準、従業者に対する監督・教育の状況等を事前に確認する。	事前	
令和8年6月1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. リスク1⑨を除く。) 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限 具体的な制限方法	①委託先には作業責任者及び作業従事者の届出を義務付けている。 ②閲覧又は更新権限を持つ者は必要最小限とする。 ③閲覧又は更新権限を持つ者のアカウント管理を行い、システム上で操作を制限する。 ④閲覧又は更新の履歴を記録し、必要に応じて不正な使用の有無を確認できるようにする。	①委託先には作業責任者及び作業従事者の届出を義務付けている。 ②閲覧又は更新権限を持つ者は必要最小限とする。 ③閲覧又は更新権限を持つ者のアカウント管理を行い、システム上で操作を制限する。 ④閲覧又は更新の履歴を記録し、必要に応じて不正な使用の有無を確認できるようにする。 〈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〉 ・本区がアクセス権限の管理状況を確認できる。 ・本区は、アクセス権限を付与する者を必要最小限に限定する。 ・本区は、アクセス権限を付与する範囲を必要最小限に限定する。 ・本区は、アクセス権限を付与した者と権限の範囲を適切に管理する。 ※特定個人情報に係るアクセス権限は、再々委託先(PMHキー採番や運用保守)のみに付与される。	事前	
令和8年6月1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. リスク1⑨を除く。) 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの取扱いの記録 具体的方法	・作業端末へのログイン記録やシステム保守における作業記録を残している。	・作業端末へのログイン記録やシステム保守における作業記録を残している。 〈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〉 ・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取り扱いのログを保存し、本区は特定個人情報に係る操作のログを閲覧・出力できる。 ※再々委託先(PMHキー採番や運用保守)に係る特定個人情報の取扱いログに限られる。	事前	
令和8年6月1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. リスク1⑨を除く。) 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	・委託先から他者への特定個人情報の提供、ならびに当該情報の外部持ち出しを認めないことを契約書上明記する。	・委託先から他者への特定個人情報の提供、ならびに当該情報の外部持ち出しを認めないことを契約書上明記する。 〈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〉 ・委託先(再委託先及び再々委託先を含む。)から他者への提供は行わない。 ・本区は委託契約に基づき、委託先(再委託先及び再々委託先を含む。)から他者への提供が行われていないことを確認できる。	事前	
令和8年6月1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. リスク1⑨を除く。) 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 委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・委託先等への定期的な視察を行っている。 ・個人情報の管理状況について、日常運用においてチェックし、必要に応じて調査も行う。	・委託先等への定期的な視察を行っている。 ・個人情報の管理状況について、日常運用においてチェックし、必要に応じて調査も行う。 〈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〉 ・委託先(再委託先及び再々委託先を含む。)には、業務上、最低限必要な範囲の特定個人情報のみを提供できる。それ以外の提供は一切認められず、その旨を委託契約書にも明記する。 ・本区は委託契約に基づき、委託先(再委託先及び再々委託先を含む。)から契約書で定められた範囲の特定個人情報しか提供されていないことを確認できる。	事前	

令和8年6月1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. リスク1⑨を除く。) 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 ルールの内容及びルール遵守の確認方法	・委託業者は、この契約による事務を終了したとき、または委託元が請求したときは、この契約に係る個人情報を直ちに委託元に返還しなければならない。また、機器の廃棄時は、磁気記録等装置に記録されている個人情報等を削除し復元ソフト等による復元が不可能な状態にし、または磁気記録等装置を物理的に破壊した上で撤去し、データ消去証明書を提出することを契約に含めている。	・委託業者は、この契約による事務を終了したとき、または委託元が請求したときは、この契約に係る個人情報を直ちに委託元に返還しなければならない。また、機器の廃棄時は、磁気記録等装置に記録されている個人情報等を削除し復元ソフト等による復元が不可能な状態にし、または磁気記録等装置を物理的に破壊した上で撤去し、データ消去証明書を提出することを契約に含めている。 ＜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＞ ・委託契約終了後は予診情報・予防接種記録管理／請求支払システムに保管していた全ての特定個人情報を国保中央会が消去する。 ・特定個人情報を紙媒体で保管しない。 ・委託契約書に基づき、本区は消去について国保中央会から報告を受けることができ、それにより消去状況について確認が可能となる。	事前	
令和8年6月1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. リスク1⑨を除く。) 4. 特定個人情報ファイルの取扱いの委託 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の内容	委託先に対して、個人情報保護に関する法令に基づき、以下の規定を記載している。 ・直接または間接に知り得た個人情報を第三者に漏らしてはならない。また契約期間満了後も同様とする。 ・個人情報を業務の目的以外に使用してはならない。また第三者に提供してはならない。 ・個人情報の全部または一部を許可なく複写し、または複製してはならない。許可を受けて複写または複製したときは、当該複写物または複製物を焼却裁断等により利用できないように処分しなければならない。 ・個人情報の授受、保管および管理について、善良な管理者の注意をもってあたり、個人情報の消滅、き損等の事故を防止しなければならない。 ・契約を終了したとき、または委託者が請求したときは、その保有する個人情報を直ちに返還しなければならない。 ・委託者は、個人情報の管理状況について随時に立入検査または調査をし、必要な報告を求め、または委託事務の処理に関して指示を与えることができる。 ・事故が生じたときには、直ちに委託者に対して通知するとともに、遅滞なくその状況を書面をもって報告し、委託者の指示に従わなければならない。	委託先に対して、個人情報保護に関する法令に基づき、以下の規定を記載している。 ・直接または間接に知り得た個人情報を第三者に漏らしてはならない。また契約期間満了後も同様とする。 ・個人情報を業務の目的以外に使用してはならない。また第三者に提供してはならない。 ・個人情報の全部または一部を許可なく複写し、または複製してはならない。許可を受けて複写または複製したときは、当該複写物または複製物を焼却裁断等により利用できないように処分しなければならない。 ・個人情報の授受、保管および管理について、善良な管理者の注意をもってあたり、個人情報の消滅、き損等の事故を防止しなければならない。 ・契約を終了したとき、または委託者が請求したときは、その保有する個人情報を直ちに返還しなければならない。 ・委託者は、個人情報の管理状況について随時に立入検査または調査をし、必要な報告を求め、または委託事務の処理に関して指示を与えることができる。 ・事故が生じたときには、直ちに委託者に対して通知するとともに、遅滞なくその状況を書面をもって報告し、委託者の指示に従わなければならない。 ＜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＞ 東京都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。 ・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	事前	

令和8年6月1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. リスク1⑨を除く。) 4. 特定個人情報ファイルの取扱いの委託 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 具体的な方法	委託先と同等のリスク対策を実施する	委託先と同等のリスク対策を実施する。 ＜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＞ ・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、点検結果について東京都国保連合会及び本区に年1回報告を行う。	事前	
令和8年6月1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. リスク1⑨を除く。) 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	＜新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)事務における追加措置＞ 当区、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)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。	＜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＞ ・委託契約書に以下の規定を設ける。 委託先及び再委託先は、従業者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。	事前	

令和8年6月1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. リスク1⑨を除く。) 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 具体的な対策の内容	・記録媒体、紙媒体は鍵付の書庫に保管する。 ・データ消去処理は、情報を復元できないように処置した上で廃棄する。 ＜ガバメントクラウドにおける措置＞ ①ガバメントクラウドについては政府情報システムのセキュリティ制度 (ISMAP) のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、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。 ＜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・プラットフォームは、政府情報システムのためのセキュリティ評価制度 (ISMAP) に登録されたクラウドサービス事業者が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サービス事業者が実施する。 なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018の認証を受けている。 ・日本国内でデータ保管している。 ＜ワクチン接種記録システム(VRS)における措置＞ ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウド サービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める物理的対策を満たしている。 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。	・記録媒体、紙媒体は鍵付の書庫に保管する。 ・データ消去処理は、情報を復元できないように処置した上で廃棄する。 ＜ガバメントクラウドにおける措置＞ ①ガバメントクラウドについては政府情報システムのセキュリティ制度 (ISMAP) のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、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。 ＜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・プラットフォームは、政府情報システムのためのセキュリティ評価制度 (ISMAP) に登録されたクラウドサービス事業者が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サービス事業者が実施する。 なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018の認証を受けている。 ・日本国内でデータ保管している。 ＜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＞ 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ため、特定個人情報の適正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 サービスの利用	事前	
令和8年6月1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. リスク1⑨を除く。) 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 具体的な対策の内容	(上記省略) ＜ワクチン接種記録システム(VRS)における措置＞ ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める技術的対策を満たしている。 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、市区町村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。	(左記内容削除)	事前	

令和8年6月1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. リスク1⑨を除く。) 7. 特定個人情報の保管・消去 リスク2: 特定個人情報が高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	・指定の保持年数を経過した場合に物理削除。 ・磁気ディスクの廃棄時は、記録されている個人情報等を削除し復元ソフト等による復元が不可能な状態にし、または物理的に破壊する仕組みとしている。	・指定の保持年数を経過した場合に物理削除。 ・磁気ディスクの廃棄時は、記録されている個人情報等を削除し復元ソフト等による復元が不可能な状態にし、または物理的に破壊する仕組みとしている。 〈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〉 ・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。	事前	
令和8年6月1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. リスク1⑨を除く。) 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 消去手順 手順の内容	・指定の保持年数を経過した場合は、パッケージ機能にて対象者情報を物理削除する。 ・磁気ディスクの廃棄時は、記録されている個人情報等を削除し復元ソフト等による復元が不可能な状態にし、または物理的に破壊する仕組みとしている。 ・申請書類等については、『品川区文書取扱規程第21条』に基づき適切な処理を行う。 〈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。 〈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。	・指定の保持年数を経過した場合は、パッケージ機能にて対象者情報を物理削除する。 ・磁気ディスクの廃棄時は、記録されている個人情報等を削除し復元ソフト等による復元が不可能な状態にし、または物理的に破壊する仕組みとしている。 ・申請書類等については、『品川区文書取扱規程第21条』に基づき適切な処理を行う。 〈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。 〈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〉 ・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。	事前	
令和8年6月1日	Ⅳ その他のリスク対策 1. 監査 ①自己点検 具体的なチェック方法	・特定個人情報の保護を担保するために、毎年評価書の記載通りの運用がなされているか「特定個人情報保護評価書運用報告書」で見直しを行う。 〈中間サーバー・プラットフォームにおける措置〉 ①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。 〈新型コロナウイルス感染症対策に係る予防接種（特例臨時接種）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、必要な監督をする。	・特定個人情報の保護を担保するために、毎年評価書の記載通りの運用がなされているか「特定個人情報保護評価書運用報告書」で見直しを行う。 〈中間サーバー・プラットフォームにおける措置〉 ①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。 〈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〉 本区は、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職員等の当該システムの利用を管理し、必要な自己点検を行う。	事前	

令和8年6月1日	IV その他のリスク対策 1. 監査 ②監査 具体的な内容	評価実施機関内の内部監査を「情報セキュリティ監査実施ガイドライン」に基づき、以下の観点により定期的に実施し、監査結果を踏まえて体制や規定を改善する。なお、情報セキュリティ監査統括責任者は、副統括情報セキュリティ責任者(システム所管課長)をもって充て、情報セキュリティ監査統括責任者が指名する監査人によって、当監査を行う。 ・評価書記載事項と運用実態について確認する。 ・特定個人情報を取扱うシステムについて、適切なセキュリティ対策が実施され、かつ有効に機能していることを確認する。 ＜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＞ ①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政府情報システムのセキュリティ評価制度(ISMAP)に登録された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。 ＜新型コロナウイルス感染症対策に係る予防接種(特例臨時接種)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、必要な監督をする。	評価実施機関内の内部監査を「情報セキュリティ監査実施ガイドライン」に基づき、以下の観点により定期的に実施し、監査結果を踏まえて体制や規定を改善する。なお、情報セキュリティ監査統括責任者は、副統括情報セキュリティ責任者(システム所管課長)をもって充て、情報セキュリティ監査統括責任者が指名する監査人によって、当監査を行う。 ・評価書記載事項と運用実態について確認する。 ・特定個人情報を取扱うシステムについて、適切なセキュリティ対策が実施され、かつ有効に機能していることを確認する。 ＜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＞ ①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政府情報システムのセキュリティ評価制度(ISMAP)に登録された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。 ＜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＞ 本区は、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職員等の当該システムの利用を管理し、必要な監査を行う。	事前	
令和8年6月1日	IV その他のリスク対策 2. 従業員に対する教育・啓発 従業員に対する教育・啓発 具体的な方法	・職員に対しては、個人情報保護に関する研修の受講を義務付けている。 ・委託業者に対しては、個人情報保護に関する法令に基づき個人情報の保護を図るよう秘密保持契約を締結している。 ・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る。 ・セキュリティ事故の情報を課内で共有するため、全員に回覧している。 ・全庁的な研修として、eラーニングによる情報セキュリティおよび個人情報保護研修を行っている。 ＜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。	・職員に対しては、個人情報保護に関する研修の受講を義務付けている。 ・委託業者に対しては、個人情報保護に関する法令に基づき個人情報の保護を図るよう秘密保持契約を締結している。 ・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る。 ・セキュリティ事故の情報を課内で共有するため、全員に回覧している。 ・全庁的な研修として、eラーニングによる情報セキュリティおよび個人情報保護研修を行っている。 ＜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。 ＜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＞ 本区は、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職員等の当該システムの利用を管理し、適切な指導を行う。	事前	

令和8年6月1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＞ 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、政府情報システムのためのセキュリティ評価制度 (ISMAP) に登録されたクラウドサービス事業者による高い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、およ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。 ＜事務運営に関する責任者の関与の仕組み＞ ・副区長を議長とし、業務責任者をメンバーとする情報管理安全対策会議を設置し、特定個人情報をはじめとする個人情報保護や情報セキュリティ等に係るリスク管理を行う。 ・情報管理安全対策会議では、リスク管理に係る監査・自己点検、教育・研修をはじめ、情報漏えい等のセキュリティ事象が発生した場合の対応訓練等の諸活動について、計画策定、実施状況のモニタリングを行い、各種の課題・問題を把握し、継続的な運用改善を行う。 ＜特定個人情報の漏えい事象が発生した場合の対応＞ 以下①～⑦について「マイナンバー事務に係る緊急事案等の報告手順」に則り対応する。 ①組織内における報告、被害の拡大防止 ②事実関係の調査、原因の究明 ③影響範囲の特定 ④再発防止策の検討・実施 ⑤影響を受ける可能性のある本人の連絡等 ⑥事実関係、再発防止策の公表 ⑦個人情報保護委員会への報告	＜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、政府情報システムのためのセキュリティ評価制度 (ISMAP) に登録されたクラウドサービス事業者による高い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、およ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。 ＜事務運営に関する責任者の関与の仕組み＞ ・副区長を議長とし、業務責任者をメンバーとする情報管理安全対策会議を設置し、特定個人情報をはじめとする個人情報保護や情報セキュリティ等に係るリスク管理を行う。 ・情報管理安全対策会議では、リスク管理に係る監査・自己点検、教育・研修をはじめ、情報漏えい等のセキュリティ事象が発生した場合の対応訓練等の諸活動について、計画策定、実施状況のモニタリングを行い、各種の課題・問題を把握し、継続的な運用改善を行う。 ＜特定個人情報の漏えい事象が発生した場合の対応＞ 以下①～⑦について「マイナンバー事務に係る緊急事案等の報告手順」に則り対応する。 ①組織内における報告、被害の拡大防止 ②事実関係の調査、原因の究明 ③影響範囲の特定 ④再発防止策の検討・実施 ⑤影響を受ける可能性のある本人の連絡等 ⑥事実関係、再発防止策の公表 ⑦個人情報保護委員会への報告 ＜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＞ 本区は、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。	事前	
令和8年6月1日	IV VI 評価実施手続 2. 国民・住民等からの意見の聴取	「品川区区民意見公募手続の実施に関する要綱」に基づき、区民意見聴取を行う。区民意見聴取の実施に際しては、「広報しながわ」に、番号制度の概要と合わせ意見募集を行うことの記事を掲載し、品川区役所HP、区の広報紙への掲載(7月11日号)、保健予防課窓口、区政資料コーナーにおいて全文を閲覧できるようにする。	「品川区区民意見公募手続の実施に関する要綱」に基づき、区民意見聴取を行う。区民意見聴取の実施に際しては、「広報しながわ」に、番号制度の概要と合わせ意見募集を行うことの記事を掲載し、品川区役所HP、区の広報紙への掲載(7月15日号)、保健予防課窓口、区政資料コーナーにおいて全文を閲覧できるようにする。	事前	

【案】特定個人情報保護評価書(全項目評価書)「住民基本台帳に関する事務」用語解説

項番	記載ページ	記載箇所	用語	意味
1	P1	表紙 個人のプライバシー等の権利利益の保護の宣言	特定個人情報ファイル	個人番号をその内容に含む個人情報ファイルをいい、個人情報を含む情報の集合物であって、その情報を検索することができるように体系的に構成したもの。
2	P3	I-1. ②事務の内容	健康被害救済	予防接種を受け健康被害が生じた場合、その健康被害が接種を受けたことによるものであると厚生労働大臣が認定したときに、市町村により給付が行われる。
3	P3	I-1. ②事務の内容	情報連携	情報提供ネットワークシステムを使用して他の行政機関、地方公共団体等が保有する利用特定個人情報を照会・提供すること。
4	P3	I-2. ③他のシステムとの接続	情報提供ネットワークシステム	番号利用法により、国や他機関との連携が可能な情報をやり取りする際に、必要となるシステム。
5	P3	I-2. ③他のシステムとの接続	住民基本台帳ネットワークシステム	住民基本台帳を基礎にした全国的なコンピューターネットワークのこと。記録される項目は、個人番号の他に法律で定められている氏名・住所・性別・生年月日・住民票コード・これらの変更情報に限られる。
6	P4	I-2. システム2 ①システムの名称	番号連携サーバ(団体内統合宛名システム)	「地方公共団体における番号制度の導入ガイドライン 第2章第4節 団体内統合宛名システム等の整備に係るガイドライン」における地方公共団体で業務横断的に宛名、住所、所在地等の情報の保持・管理を行うシステム。
7	P4	I-2. システム2 ②システムの機能	中間サーバー	情報提供ネットワークシステム・団体内統合宛名システム間のデータ受け渡しをすることで、符号の取得や他情報保有機関間の特定個人情報照会・提供の機能を提供するサーバー。
8	P4	I-2. システム3 ②システムの機能	団体内統合宛名番号	情報提供用個人識別符号と一意に個人を特定する番号。中間サーバでは個人番号(マイナンバー)を保有しないため、この番号を使用し、区の保有情報と中間サーバに記録されている情報を紐付ける際に必要となる。
9	P5	I-2. システム4 ②システムの機能	Public Medical Hub	介護保険、予防接種、母子保健(乳幼児健診、妊婦健診)、公費負担医療や地方単独の医療費助成、自治体検診などに係る情報を、自治体や医療機関、対象者間で連携するシステム。 PMHIは略称。
10	P5	I-2. システム4 ②システムの機能	社会保険診療報酬支払基金	健康保険制度における診療報酬の「審査」及び「支払」について、保険者等の委託を受けて実施する審査支払の専門機関。
11	P5	I-2. システム4 ②システムの機能	医療保険者等向け中間サーバー	番号利用法の規定に基づき、医療保険者等において保持する特定個人情報の副本を保存・管理し、情報提供ネットワークシステム等を経由した情報連携、機関別符号及び情報提供等記録の管理等の役割を担うシステム。
12	P5	I-2. システム4 ②システムの機能	電子証明書	電子申請における、本人確認手段やデータ改ざん防止のために利用する電子的な身分証明書。電子証明書は、公的個人認証制度におけるICカード(マイナンバーカードなど)に搭載されたり、ファイル形式で提供される。
13	P5	I-2. システム4 ②システムの機能	履歴回答照会システム	オンライン資格確認等システムに保持されている資格情報の履歴を活用し、オンライン資格確認等システムに保存されている一番古い被保険者番号等からIDとなる情報を生成することで、被保険者番号等や氏名が変わっても、レセプト情報等を連結するシステム。
14	P8	(別添1)事務内容 (備考)	LGWAN	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のこと。Local Government Wide Area Networkの略。

【案】特定個人情報保護評価書(全項目評価書)「住民基本台帳に関する事務」用語解説

項番	記載ページ	記載箇所	用語	意味
15	P10	Ⅱ-3 ②入手方法	フラッシュメモリ	データの消去・書き込みを自由に行うことができ、電源を切っても内容が消えない外部記憶媒体。
16	P11	Ⅱ-3 ⑧使用方法	オンライン資格確認等システム	医療機関等の窓口でマイナンバーカードのICチップまたは資格確認書の記号番号等により、オンラインにて資格情報を確認するためのシステム。
17	P13	Ⅱ-4 委託事項3 ②取扱いを委託する 特定個人情報ファイル の範囲 その妥当性	公益社団法人国民健康保険中央会	一般社団法人及び一般財団法人に関する法律に基づき各都道府県の国保連合会を会員として組織され、公益社団法人及び公益財団法人の認定等に関する法律に基づき、内閣府から公益認定を受けた公益社団法人。 国民健康保険事業、高齢者医療事業、健康保険事業、介護保険事業及び障害者総合支援事業の普及、健全な運営及び発展を図り、社会保障及び国民保健の向上に寄与することを目的としている。
18	P13	Ⅱ-4 委託事項3 ②取扱いを委託する 特定個人情報ファイル の範囲 その妥当性	東京都国民健康保険団体連合会	国民健康保険法第83条に基づき、東京都の保険者(区市町村・国民健康保険組合)が共同して目的を達成するため、東京都知事の認可を受け設立された公法人。
19	P13	Ⅱ-4 委託事項3 ④委託先への特定個人情報ファイルの提供 方法	閉域網回線	インターネットから切り離された独自のネットワークのこと。
20	P16	Ⅱ-6 ①保管場所	ガバメントクラウド	政府共通のクラウドサービスの利用環境。クラウドサービスの利点を最大限に活用することで、迅速、柔軟、かつセキュアでコスト効率の高いシステムを構築可能とし、利用者にとって利便性の高いサービスをいち早く提供し改善していくことを目的とする。
21	P16	Ⅱ-6 ①保管場所	ISMAP	政府情報システムのためのセキュリティ評価制度(Information system Security Management and Assessment Program)。政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的としている。
22	P16	Ⅱ-6 ①保管場所	ISO/IEC27017	クラウドサービスに関する情報セキュリティ管理策のガイドライン規格。情報セキュリティ全般に関するマネジメントシステム規格であるISO/IEC 27001の取り組みをISO/IEC 27017で強化することで、クラウドサービスにも対応した情報セキュリティ管理体制を構築することが可能。
23	P16	Ⅱ-6 ①保管場所	ISO/IEC27018	クラウドサービス事業者がパブリッククラウド上で管理する個人情報の保護に焦点を当てた国際規格。ISO/IEC 27001(ISMS)を前提としたアドオン認証となり、クラウド情報における個人情報の保護に対応したISMSにアップグレードすることが可能。
24	P16	Ⅱ-6 ①保管場所	中間サーバー・プラットフォーム	情報提供ネットワークシステムを使用した情報提供を行うために設置する中間サーバーの拠点のこと。地方公共団体情報システム機構が整備を進めている。
25	P16	Ⅱ-6 ③消去方法	NIST 800-88	2006年にNIST(National Institute of Standards and Technology:米国国立標準技術研究所)が発行した記録媒体のデータ消去(サニタイゼーション)に関するガイドライン。総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」でも準拠が求められている。
26	P16	Ⅱ-6 ③消去方法	IaaS	クラウドコンピューティングのうちの1つで、仮想化技術を利用してハードウェアリソース(CPU/メモリ/ストレージ)などのデジタルインフラをインターネット経由でオンデマンドで提供するサービス。

【案】特定個人情報保護評価書(全項目評価書)「住民基本台帳に関する事務」用語解説

項番	記載ページ	記載箇所	用語	意味
27	P28	Ⅲ-6 リスク4 リスクに対する措置の内容	VPN	VPNはVirtual Private Networkの略。 公衆回線を使用してネットワークを利用する際、様々な利用者の情報が流れるため、VPNの技術により仮想的に専用回線を作り、自社ネットワーク内部の通信のように遠隔地との通信が行える技術。
28	P31	Ⅲ-7 リスク1 ⑥技術的対策 具体的な対策の内容	ASP	インターネットを介して遠隔からソフトウェアが利用できるサービス、またはサービスの提供事業者のこと。
29	P31	Ⅲ-7 リスク1 ⑥技術的対策 具体的な対策の内容	DDos	ネットワークを通じてコンピューターおよび通信機器に行われるサイバー攻撃のひとつ。大量のデータや不正データを目標に送り付け、通信状態を飽和させたり、コンピューターが正常に稼働できないような状態に陥らせたりする。