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
41	新型インフルエンザ等対策特別措置法に基づく予防接種及び新型コロナウイルス感染症に係る予防接種に関する事務

個人のプライバシー等の権利利益の保護の宣言

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

特記事項	なし

評価実施機関名

新宿区長

個人情報保護委員会　承認日 【行政機関等のみ】

公表日

［平成30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	新型インフルエンザ等対策特別措置法に基づく予防接種及び新型コロナウイルス感染症に係る予防接種に関する事務
②事務の内容　※	【予防接種事務の概要】 予防接種法及び新型インフルエンザ等対策特別措置法に基づき、伝染のおそれがある疾病の発生及びまん延を予防するために公衆衛生の見地から予防接種を実施するための事務 1．取り扱いの対象となる予防接種の種類 （1）　予防接種法に基づく臨時の予防接種 （2）　新型インフルエンザ等対策特別措置法に基づく予防接種 （3）　予防接種法に基づく新型コロナウイルス感染症に係る予防接種事務 2．事務の内容 （1）　予防接種法に基づく臨時の予防接種及び新型インフルエンザ等対策特別措置法に基づく予防接種 ア　予診票の発行 住民基本台帳(以下、「住基」という。)の情報を基に、予防接種法等関連法令で定められた年齢要件等に該当する者に対し、予防接種の予診票等を作成・発行する。 イ　予診票の再発行 住基の情報を基に、予診票を紛失した者等に対し予診票等の再発行を行う。 ウ　予防接種記録の管理 契約医療機関や集団接種会場等で予防接種を受けた区民の予診票について当該医療機関等からの提出を受理し、接種記録を入力・管理する。 エ　接種勧奨通知の送付 伝染の恐れがある疾病の発生及びまん延を予防するため、接種履歴から必要に応じて区民に対し、接種勧奨の通知を行う。 オ　予防接種実施依頼書等の発行 本人（保護者等を含む。）からの申請に基づき、区外の自治体で予防接種をする場合、予防接種実施依頼書等を作成し、発行する。 カ　予防接種実施報告書の送付 他自治体の長からの定期予防接種の実施依頼を受けて予防接種を実施した場合、依頼元の自治体の長に報告書を送付する。報告書には予診票の写しを添付する。 キ　国・東京都等への報告 予防接種法施行令第7条に基づき、予防接種を受けた者の数等を東京都知事に報告する。その他、国または東京都から指示された事項について報告を行う。 ク　予防接種による健康被害の救済 予防接種を受けた者が、予防接種が原因で疾病にかかり、障害の状態となり、または死亡した場合において、当該疾病、障害又は死亡が予防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場合は、予防接種法等関連法令に基づき給付を行う。 （2）　予防接種法に基づく新型コロナウイルス感染症に係る予防接種事務 ア　接種券の発行 住基の情報を基に、予防接種法等関連法令で定められた年齢要件等に該当する者に対し、予防接種の接種券等を作成・発行する。 イ　接種券票の再発行 住基の情報を基に、接種券票を紛失した者等に対し接種券等の再発行を行う。 ウ　予防接種記録の管理 契約医療機関や集団接種会場等で予防接種を受けた区民の予診票について当該医療機関等からの提出を受理し、接種記録を入力・管理する。 エ　接種勧奨通知の送付 伝染の恐れがある疾病の発生及びまん延を予防するため、接種履歴から必要に応じて区民に対し、接種勧奨の通知を行う。 オ　ワクチン接種記録システム（以下、「VRS」という。）の登録 VRSへ予防接種対象者及び発行した接種券の登録を行う。 カ　VRSを用いた接種記録の照会・提供 予防接種の実施後に接種記録等を登録、管理し、他市区町村へ接種記録の照会・提供を行う。 キ　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。 ク　国・東京都等への報告 予防接種法施行令第7条に基づき、予防接種を受けた者の数等を東京都知事に報告する。その他、国または東京都から指示された事項について報告を行う。 ケ　予防接種による健康被害の救済 予防接種を受けた者が、予防接種が原因で疾病にかかり、障害の状態となり、または死亡した場合において、当該疾病、障害又は死亡が予防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場合は、予防接種法等関連法令に基づき給付を行う。

	※行政手続における特定の個人を識別するための番号の利用等に関する法律(平成25年法律第27号)(以下、「番号法」という。)の別表第二に基づいて区は、予防接種に関する事務において、情報提供ネットワークシステムに接続し、各情報保有機関が保有する特定個人情報について情報照会を行う。また、他機関からの情報照会に対応する為に、予防接種の事務に係る特定個人情報を中間サーバーに登録する。
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	保健情報(対人)システム
②システムの機能	1.予診票及び接種券等の交付・住基情報及び過去の接種履歴を用いて予診票及び接種券等の作成・発行処理を行う機能 2.接種記録の管理・各予防接種の接種記録の登録処理を行う機能 3.接種勧奨・過去の接種履歴等から未接種者への接種勧奨を行うための宛名ラベル等を出力する機能 4.自庁内の他業務・システムと各種照会情報の連携を行い、接種対象者の情報の正確性を保つ機能
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2

①システムの名称	団体内統合宛名等システム
②システムの機能	1. 団体内統合宛名番号の付番と管理 :各業務・システムで保有している宛名番号を団体内で統一して個人を識別するための団体内統合宛名番号を付番する。各業務・システムの宛名番号と団体内統合宛名番号、基本情報、個人番号を関連付けて、格納・管理する。 2. 符号取得支援・確認 :処理通番の発行依頼を中間サーバに通知して符号が取得できたか確認を行う。 3. 情報提供機能 :中間サーバへ特定個人情報を登録するために、業務・システムのデータを変換して中間サーバへ提供情報を通知する。 4. 情報照会機能 :各業務・システムに代わって、他団体の特定個人情報の照会について、宛名番号と団体内統合宛名番号の変換、データ形式等の変換を行い、中間サーバへ照会情報を通知する。 5. 宛名情報照会 :団体内統合宛名番号、個人番号または基本情報を検索キーとして、個人情報を照会する。 6. 他業務システム連携機能 :他業務システムからの要求に基づき、個人番号または団体内統合宛名番号に紐づく宛名情報を通知する。
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 [○] 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 (各業務システム、中間サーバ、保健情報(対人)システム)

システム3	
①システムの名称	中間サーバ
②システムの機能	1. 符号管理機能 :符号管理機能は情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」を関連付けて、その情報を保管・管理する機能。 2. 情報照会機能 :情報照会機能は、情報提供ネットワークシステムを介して特定個人情報(連携対象)の情報照会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 :情報提供機能は、情報提供ネットワークシステムを介して情報照会要求の受領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 :中間サーバと既存システム、団体内統合宛名システムおよび既存住民基本台帳システムとの間で情報照会内容、情報提供内容、特定個人情報(連携対象)、符号取得のための情報等について連携するための機能。 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て管理する機能。 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 :中間サーバと情報提供ネットワークシステム(インタフェースシステム)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 :特定個人情報(連携対象)の暗号化および復号や、電文への署名付与、電文および提供許可証に付与されている署名の検証、それらに伴う鍵管理を行う。また、情報提供ネットワークシステム(インタフェースシステム)から受信した情報提供NWS 配信マスター情報を管理する機能。 9. 職員認証・権限管理機能 :中間サーバを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報(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 :バッチ処理の状況管理、業務統計情報の集計、稼動状態の通知、保管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	住民記録システム(「既存住民基本台帳システム」と同義)
②システムの機能	被保険者等の住民記録情報(個人番号・住所異動・世帯状況等)を検索・確認する機能
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　(団体内統合宛名等システム、住基GWサーバー、証明書自動交付システム、保健情報(対人)システム)

システム5	
①システムの名称	ワクチン接種記録システム（VRS）
②システムの機能	1. 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 2. 接種記録の管理 3. 転出/死亡時等のフラグ設定 4. 他市区町村への接種記録の照会・提供 5. 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 6. 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 7. 新型コロナウイルス感染症予防接種証明書のコンビニ交付の実施
③他のシステムとの接続	[　　] 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6	
①システムの名称	マイナポータルぴったりサービスのサービス検索・電子申請機能（以下「サービス検索・電子申請機能」という。）
②システムの機能	・【住民向け機能】自らが受けることができるサービスをオンラインで検索及び申請ができる機能 ・【地方公共団体向け機能】住民が電子申請を行った際の申請データ取得画面又は機能を、地方公共団体に公開する機能
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　（　　）

3. 特定個人情報ファイル名

予防接種情報ファイル

4. 特定個人情報ファイルを取り扱う理由

①事務実施上の必要性	予防接種の対象者及び接種履歴を正確に把握し、適正な管理を行うため。
②実現が期待されるメリット	・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	・番号法第9条第1項　別表第1の10、93の2の項（予防接種法に基づく臨時の予防接種、新型インフルエンザ等対策特別措置法に基づく予防接種、予防接種法に基づく新型コロナウイルス感染症に係る予防接種事務） ・番号法第19条第16号（予防接種法に基づく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(VRS)を用いた情報提供・照会のみ） ・番号法第19条第6号(委託先への提供)

6. 情報提供ネットワークシステムによる情報連携 ※

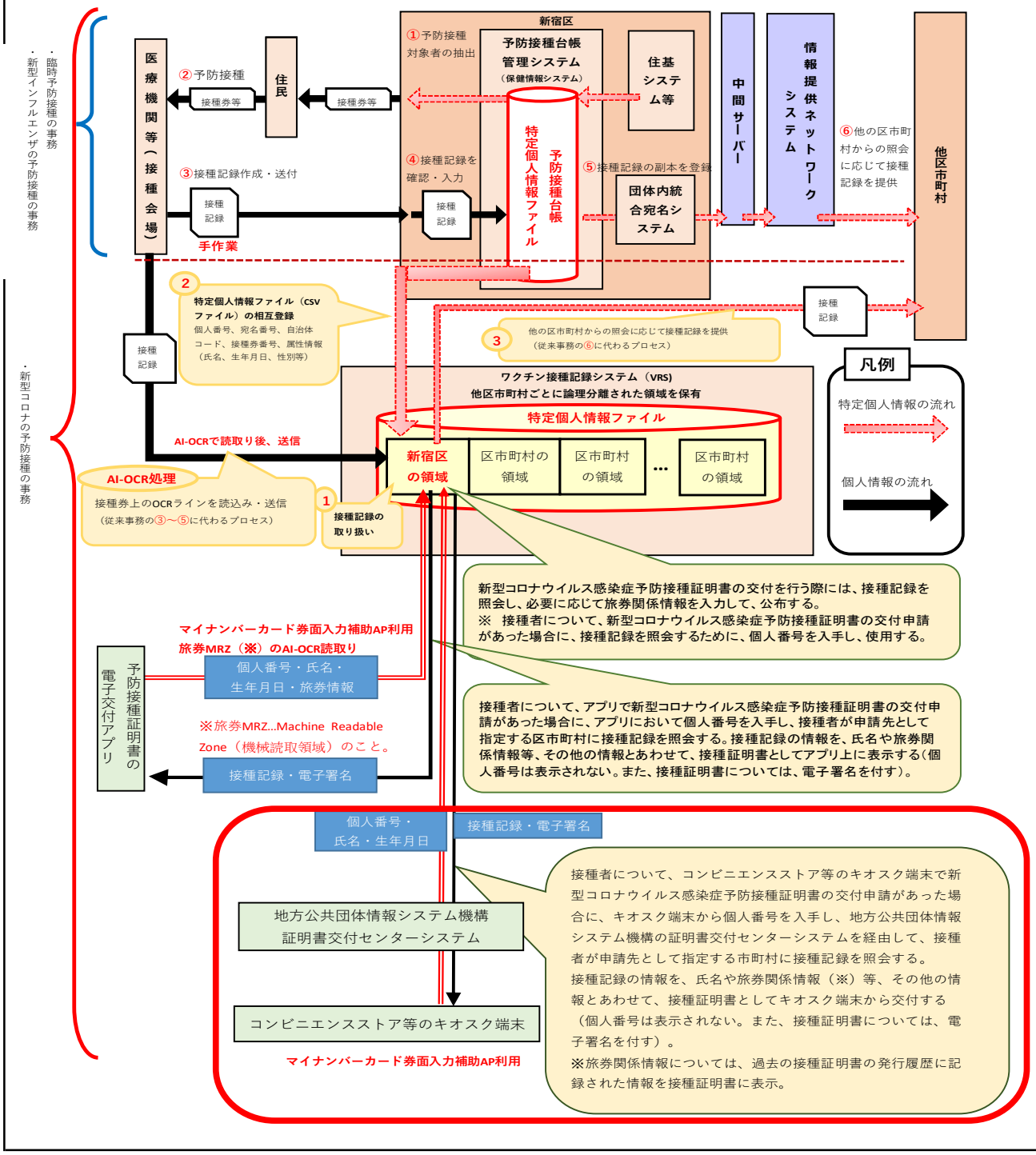
①実施の有無	[　　実施する　　]	＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	・番号法第19条第8号及び別表第2 （別表第2における情報提供の根拠）16の2、16の3、115の2の項 （別表第2における情報照会の根拠）16の2、17、18、19、115の2の項	

7. 評価実施機関における担当部署	
①部署	健康部保健予防課
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

事業のイメージ



（備考）

新型インフルエンザ等対策特別措置法に基づく予防接種事務、予防接種法に基づく臨時接種事務及び新型コロナウイルス感染症に係る予防接種事務では、予防接種台帳管理システムにより抽出された予防接種対象者に対し、区から予診票や接種券を郵送する。予診票や接種券を受け取った対象者は、医療機関等でワクチンを接種し、ワクチンの接種後、接種記録が記載された予診票等は、医療機関等から区に提出される。区は、提出された予診票等から予防接種台帳に接種記録を登録し、中間サーバー、情報提供ネットワークシステムを通じて、他区市町村に接種記録を照会又は提供できる。

なお、新型コロナウイルス感染症に係る予防接種事務では、国がワクチン接種記録システム（VRS: Vaccination Record System）を整備することで、自治体がワクチン接種の状況を可能な限り逐次把握することを支援している。また、接種者から、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、新型コロナウイルス感染症予防接種証明書を交付する。

１．新型インフルエンザ等対策特別措置法に基づく予防接種、予防接種法に基づく臨時の予防接種及び新型コロナウイルス感染症に係る予防接種事務

・予診票の発行

住民基本台帳(以下、「住基」という。)の情報を基に、予防接種法等関連法令で定められた年齢要件等に該当する者に対し、予防接種の予診票等を作成・発行する。

・予診票の再発行

住基の情報を基に、予診票を紛失した者等に対し予診票等の再発行を行う。

・予防接種記録の管理

契約医療機関や集団接種会場等で予防接種を受けた区民の予診票について当該医療機関等からの提出を受理し、接種記録を入力・管理する。

・接種勧奨通知の送付

伝染の恐れがある疾病の発生及びまん延を予防するため、接種履歴から必要に応じて区民に対し、接種勧奨の通知を行う。

・予防接種実施依頼書等の発行

本人（保護者等を含む。）からの申請に基づき、区外の自治体で予防接種をする場合、予防接種実施依頼書等を作成し、発行する。

・予防接種実施報告書の送付

他自治体の長からの定期予防接種の実施依頼を受けて予防接種を実施した場合、依頼元の自治体の長に報告書を送付する。報告書には予診票の写しを添付する。

・国、東京都等への報告

予防接種法施行令第7条に基づき、予防接種を受けた者の数等を東京都知事に報告する。その他、国または東京都から指示された事項について報告を行う。

・予防接種による健康被害の救済

予防接種を受けた者が、予防接種が原因で疾病にかかり、障害の状態となり、または死亡した場合において、当該疾病、障害又は死亡が予防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場合は、予防接種法等関連法令に基づき給付を行う。

2．予防接種法に基づく新型コロナウイルス感染症に係る予防接種事務

・接種券の発行

住基の情報を基に、予防接種法等関連法令で定められた年齢要件等に該当する者に対し、予防接種の接種券等を作成・発行する。

・接種券票の再発行

住基の情報を基に、接種券票を紛失した者等に対し接種券等の再発行を行う。

・予防接種記録の管理

契約医療機関や集団接種会場等で予防接種を受けた区民の予診票について当該医療機関等からの提出を受理し、接種記録を入力・管理する。

・接種勧奨通知の送付

伝染の恐れがある疾病の発生及びまん延を予防するため、接種履歴から必要に応じて区民に対し、接種勧奨の通知を行う。

・ワクチン接種記録システム（以下、「VRS」という。)の登録

VRSへ予防接種対象者及び発行した接種券の登録を行う。

・VRSを用いた接種記録の照会・提供

予防接種の実施後に接種記録等を登録、管理し、他市区町村へ接種記録の照会・提供を行う。

・VRS等を用いた予防接種証明書の交付

予防接種の実施後に、接種者からの申請（マイナポータルぴったりサービスのサービス検索・電子申請機能での申請を含む）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。

・国、東京都等への報告

予防接種法施行令第7条に基づき、予防接種を受けた者の数等を東京都知事に報告する。その他、国または東京都から指示された事項について報告を行う。

・予防接種による健康被害の救済

予防接種を受けた者が、予防接種が原因で疾病にかかり、障害の状態となり、または死亡した場合において、当該疾病、障害又は死亡が予防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場合は、予防接種法等関連法令に基づき給付を行う。

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名	
予防接種情報ファイル	
2. 基本情報	
①ファイルの種類 ※	[　　システム用ファイル　　] ＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※	新宿区に住民登録又は居所がある予防接種事業の対象となる者
その必要性	伝染のおそれがある疾病の発生及びまん延を予防するために公衆衛生の見地から予防接種対象者を規定するため必要。
④記録される項目	[　50項目以上100項目未満　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
主な記録項目 ※	・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 [○] 4情報（氏名、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　（　　）
その妥当性	＜識別情報＞ ・個人番号・・・手続時点において同一人の確認・特定をより的確に行うために必要である。 ・その他識別情報（内部番号）・・・庁内連携システムで利用する識別情報（世帯番号・住民番号）についても本人特定の他、庁内他事務のシステムと必要な情報を連携するために必要である。 ＜連絡先等情報＞ ・4情報、連絡先(電話番号等)については、届出(申請)者に対する届出内容の確認、問合せのために必要である。 ＜業務関係情報＞ ・健康・医療関係情報・・・予防接種情報は、予防接種の適切な実施及び接種履歴の管理をするために必要である。 ・生活保護受給情報・・・生活保護受給者については、B類疾病の予防接種費用が免除対象となるので、生活保護の受給状況に関する情報が必要である。
全ての記録項目	別添2を参照。
⑤保有開始日	令和3年2月17日
⑥事務担当部署	健康部保健予防課

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 （ 地域振興部戸籍住民課、福祉部生活福祉課 ） [ ] 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 （ 他自治体 ） [○] 民間事業者 （ 医療機関 ） [○] その他 （ 自所属 ）
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 （ ワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）、コンビニエンスストア等のキオスク端末及び証明書交付センターシステム、サービス検索・電子申請機能 ）
③入手の時期・頻度	○住民基本情報 （入手元）地域振興部戸籍住民課 （入手頻度・時期）庁内連携システムから日次連携 ○生活保護情報 （入手元）福祉部生活福祉課 （入手頻度・時期）庁内連携システムから月次連携 ○接種記録 （入手元）接種を行った医療機関又は本人等（紙） （入手頻度・時期）医療機関の場合は月１回、本人等の場合は随時 ○新型コロナウイルス感染症対策に係る予防接種事務（VRS） （入手元）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 （入手頻度・時期） ・他市区町村から接種記録の照会を受ける都度 ・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 ○予防接種による健康被害救済の申請 （入手元）接種を行った本人等（紙） （入手頻度・時期）随時
④入手に係る妥当性	○住民基本情報 法令等に基づく接種対象者であることの確認を行うため、庁内連携システムを使用して入手している。 ○生活保護情報： 生活保護情報については、接種費用の徴収の有無について確認するため、庁内連携システムを使用して入手している。 ○接種記録： 医療機関や本人等から入手する接種記録については、予防接種法施行令第6条の2及び予防接種施行規則第2条の7に示されているとおり、記録・保管することを目的に入手している。 ○新型コロナウイルス感染症対策に係る予防接種事務（VRS） ・当区への転入者について、転出元市区町村へ接種記録を照会し、提供を受ける場合のみ入手する。 （番号法第19条第16号） ・当区からの転出者について、転出先市区町村へ当市区町村での接種記録を提供するために、他市区町村から個人番号を入手する。（番号法第19条第16号） ・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。 ○予防接種による健康被害救済の申請については、予防接種法施行規則第10条及び第11条に基づいて入手している。
⑤本人への明示	・庁内連携システムの場合は、番号法第19条8号および予防接種法施行規則に基づき取得・利用している。 ・医療機関又は本人から入手する場合は、本人等が記入する予診票にも、区へ接種記録を提出されることを明記し、署名を得ている（予防接種法施行令第6条の2）。 ・VRSの場合は、接種者本人からの同意を得て入手する。また、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。 ・電子交付アプリにより予防接種証明書の電子申請を受け付ける場合及びコンビニエンスストア等のキオスク端末から予防接種証明書の申請を受け付ける場合においては、利用規約を表示し、同意を得てから入手する。 ・予防接種による健康被害救済の申請については、予防接種法施行規則第10条及び第11条に明記されている。

⑥使用目的 ※		・伝染のおそれがある疾病の発生及びまん延を予防するために公衆衛生の見地から予防接種を実施するにあたり、予防接種対象者を正確に把握するとともに、予防接種に関する記録の適正な管理を図るために使用する。
	変更の妥当性	—
⑦使用の主体	使用部署 ※	健康部保健予防課
	使用者数	[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
⑧使用方法 ※		・各届出、申請を受付するにあたって、書類の内容に不備のないことを確認するため、本特定個人情報ファイルの内容を参照する。 ・区の窓口で受付した各届出、申請内容について、予防接種に関する過去の接種履歴として、登録・管理する。 ・接種履歴は、各届出、申請を受付時に書類の記載等の不備がないことを確認するために参照する。 ・予診票等の発行等に際し、予防接種情報を使用する。 ・新型コロナウイルス感染症対策に係る予防接種事務（VRS）では、当市区町村への転入者について、転出元市区町村へ接種記録を照会するとともに、接種券の発行のために特定個人情報を使用する。また、当区からの転出者について、転出先市区町村へ当区での接種記録を提供するために特定個人情報を使用する。 ・新型コロナウイルス感染症予防接種証明書の交付の際、接種記録を照会するために特定個人情報を使用する。
	情報の突合 ※	・新型インフルエンザ等対策特別措置法に基づく予防接種、予防接種法に基づく臨時接種及び新型コロナウイルス感染症に係る予防接種事務 事務を正確かつ効率的に行うために、内部コード（住民番号）を突合キーとして、庁内連携システムから連携される4情報及び生活保護受給情報と、本特定個人情報ファイル内の予防接種対象者に関する情報とを突合する。 ・新型コロナウイルス感染症対策に係る予防接種事務（VRS） 当区からの転出者について、当区での接種記録を転出先市区町村に提供するために、他市区町村から個人番号を入手し、当市区町村の接種記録と突合する。
	情報の統計分析 ※	・厚生労働省への接種状況報告を行うが、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 ※	・予防接種健康被害発生時の給付の決定（国が行う）
⑨使用開始日		令和4年4月1日

4. 特定個人情報ファイルの取扱いの委託

委託の有無 ※		[委託する] （ 3 ）件 ＜選択肢＞ 1）委託する　2）委託しない
委託事項1		保健情報（対人）システム保守委託
①委託内容		予防接種管理システムの改修、障害対応、定期バージョンアップなどの保守業務
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] ＜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 ※	予防接種法等関連法令に定められる予防接種の対象者
	その妥当性	システムの運用保守全般を委託しているため、そのシステムが取扱う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　（運用管理、障害対応作業における、当システム端末機からの閲覧行為及び必要に応じた修正行為　）
⑤委託先名の確認方法		下記、「⑥委託者名」の項の記載により確認できる。また、当区の情報公開請求による開示請求を行うことでも確認可能。
⑥委託先名		株式会社両備システムズ
再委託	⑦再委託の有無 ※	[　再委託しない　] ＜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		団体内統合宛名等システムの保守・運用
①委託内容		システムの運用、バックアップ、改修、職員からの問い合わせ対応等の運用保守作業
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 ※	予防接種法等関連法令に定められる予防接種の対象者
	その妥当性	団体内統合宛名等システムのサーバー保守作業等は専門的な知識が要求され、職員のみで対応することは難しく、専門業者への委託が必要な業務であるため。
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」の項の記載により確認できる。また、当区の情報公開請求による開示請求を行うことでも確認可能。
⑥委託先名		日本電気株式会社
再委託	⑦再委託の有無 ※	[　再委託しない　] ＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	
委託事項3		新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）を用いた特定個人情報ファイルの管理等
①委託内容		新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）を用いた特定個人情報ファイルの管理等
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの一部] ＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部

	対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	予防接種法等関連法令に定められる予防接種の対象者
	その妥当性	ワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）を用いた特定個人情報ファイルの適切な管理等のために取り扱う必要がある。
③委託先における取扱者数		[　10人以上50人未満　] ＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[　]専用線　[　]電子メール　[　]電子記録媒体（フラッシュメモリを除く。） [　]フラッシュメモリ　[　]紙 [○]その他　（LG-WAN回線を用いた提供（VRS本体、コンビニ交付関連機能）、本人からの電子交付アプリを用いた提供（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））
⑤委託先名の確認方法		下記、「⑥委託者名」の項の記載より確認できる。
⑥委託先名		株式会社ミラボ
再委託	⑦再委託の有無 ※	[　再委託しない　] ＜選択肢＞ 1）再委託する　2）再委託しない
再委託	⑧再委託の許諾方法	
再委託	⑨再委託事項	
5. 特定個人情報の提供・移転（委託に伴うものを除く。）		
提供・移転の有無		[○]提供を行っている　（4）件　[　]移転を行っている　（　）件 [　]行っていない
提供先1		市区町村長
①法令上の根拠		番号法第19条第8号及び別表第2の16の2
②提供先における用途		予防接種法による予防接種の実施に関する事務
③提供する情報		予防接種情報
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		「2.基本情報③対象者となる本人の範囲」と同じ
⑥提供方法		[○]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		照会を受けた都度
提供先2		都道府県知事
①法令上の根拠		番号法第19条第8号及び別表第2の16の3
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、実施の指示及び実施に必要な協力に関する事務

③提供する情報	予防接種情報
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	「2.基本情報③対象者となる本人の範囲」と同じ
⑥提供方法	[○] 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	照会を受けた都度
提供先3	市区町村長
①法令上の根拠	番号法第19条第8号及び別表第2の115の2
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
③提供する情報	予防接種情報
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	「2.基本情報③対象者となる本人の範囲」と同じ
⑥提供方法	[○] 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	照会を受けた都度
提供先4	市区町村長
①法令上の根拠	番号法　第19条第16号
②提供先における用途	新型コロナウイルス感染症対策に係る予防接種事務（VRS）
③提供する情報	市区町村コード及び転入者の個人番号
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	「2.基本情報　③対象者となる本人の範囲」と同じ
⑥提供方法	[　] 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　（ VRS　）
⑦時期・頻度	当市区町村への転入者について、転出元市区町村へ接種記録の照会を行う必要性が生じた都度

6. 特定個人情報の保管・消去

①保管場所 ※		＜新宿区における措置＞ ・セキュリティゲートにて入退室を管理している部屋に設置したサーバー内に保管している。 ・入室権限を持つ者を限定し、ID及びパスワード認証による保管室への立入制限 ・ユーザーID及びパスワードによりシステムへのアクセスを制御 ・監視カメラによる入退室の監視 ・耐震対策、防火措置及び可能な限り窓を設けないことによる侵入防止対策 ・バックアップファイルは、処理に応じて日次・月次・年次でLTOへ保管 ＜申請書等の紙媒体について＞ 事務室内のキャビネット及び倉庫に施錠保管している。 ＜中間サーバー・プラットフォームについて＞ 入館及び入室が厳重に管理されたデータセンターに設置している。 ＜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。なお、以下のとおりセキュリティ対策を講じている。 ・論理的に区分された当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、都道府県からは特定個人情報にアクセスできないように制御している。 ・日本国内にデータセンターが存在するクラウドサービスを利用している。 （新型コロナウイルス感染症予防接種証明書電子交付機能） 電子交付アプリ及び同アプリの利用端末には、申請情報を記録しないこととしている。 （新型コロナウイルス感染症予防接種証明書コンビニ交付） 証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。
②保管期間	期間	［　20年以上　］ ＜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	・予防接種法施行令第6条の2において、予防接種に関する記録は少なくとも5年間保存しなければならないと規定されており、区民からの接種歴確認の問い合わせに対応するため長期間保管する必要がある。
③消去方法		＜予防接種システムにおける措置＞ ・予防接種は、ワクチンに応じ、接種回数及び接種間隔が定まっており、かつ接種対象年齢が幅広いため、区民からの問い合わせに対応する必要があることから、接種歴は消去しない。 ＜紙媒体における措置＞ ・保管期限を過ぎた紙媒体（予防接種予診票等）は、年1回庁内で行う機密文書の一斉廃棄により溶解処理をしている。 ＜団体内統合宛名システムにおける措置＞ ・団体内統合宛名システムに格納する特定個人情報は各業務システムの副本データであるため、消去のタイミング等は各業務システム（事務）の運用に準ずる。 ・ディスク交換やハードウェア更改、LTO媒体の廃棄等の際は、団体内統合宛名等システムの保守・運用を行う事業者または新宿区担当部署において、保存された情報が読み出しできないよう、物理的破壊または専用ソフト等を利用して完全に消去する。 ＜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のみ、ワクチン接種記録システム(VRS)を用いて消去することができる。 ・自機関の領域に保管されたデータは、他機関から消去できない。 ※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。 ＜サービス検索・電子申請機能における措置＞ ・LGWAN接続端末に一時的に記録した個人番号付電子申請データは、紙に打出し後、速やかに完全消去する。

7. 備考

－

（別添2）特定個人情報ファイル記録項目

●予防接種情報ファイル

（1）住民情報
住民番号、氏名、生年月日、性別、続柄、異動事由、異動年月日、異動届出年月日、区民年月日、住定年月日、
住民区分、消除フラグ、住所、世帯番号、世帯主名、特定個人番号

（2）生活保護情報
生保該当最終確認年月日、生保廃止年月日

（3）予防接種情報
＜新型インフルエンザ等対策特別措置法に基づく予防接種、予防接種法に基づく臨時接種及び新型コロナウイルス感染症対策に係る予防接種＞
接種コード、接種回数、接種・予診日、更新情報　ユーザーコード、更新年月日(西暦)、更新時間、年度、
接種日年齢、年度末年齢、基準日年齢、対象外判定、接種判定、請求日（月）、実施医療機関、接種券番号、
接種会場、問診医、接種医、所属、Lot.No（ワクチンの製品番号）、接種量、医師所見、自治体コード、
特記事項、予診フラグ、実施区分、医師の判断、

＜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(VRS)＞
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）、接種日、ワクチンメーカー、Lot.No（ワクチンの製品番号）、旅券番号、
ワクチン種類（※）
製品名（※）、旅券関係情報（旧姓・別姓・別名、ローマ字氏名、国籍、旅券番号）（※）、証明書ID（※）、
証明書発行年月日（※）
※　新型コロナウイルス感染症予防接種証明書の交付に必要な場合のみ

Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※(7. リスク1⑨を除く。)

1. 特定個人情報ファイル名	
予防接種情報ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1：　目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	＜新型インフルエンザ等対策特別措置法に基づく予防接種、予防接種法に基づく臨時接種及び新型コロナウイルス感染症対策に係る予防接種＞ ・窓口における情報の入手においては、個人番号カードの提示又は通知カードと身分証明書（官公庁発行のものに限る）の提示により本人確認を行い、対象者であることを確認している。 ・庁内連携による住民情報の入手については、各システム間で使用している共通KEY（住民番号）により対象者以外の情報が入手できない仕組みとなっている。 ・予防接種を実施する委託医療機関において本人確認を行うことにより、対象者以外の情報を入手することのないよう努める。 ＜新型コロナウイルス感染症対策に係る予防接種事務における措置(VRS)＞ ・転入者本人からの個人番号の入手 当区の転入者について、転出元市区町村へ接種記録を照会するために、本人から個人番号を入手する場合は、新接種券発行申請書兼接種記録確認同意書等により本人同意を取得し、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 ・他市区町村からの個人番号の入手 当区からの転出者について、当区での接種記録を転出先市区町へ提供するために、他市区町村から個人番号を入手するが、その際は、他市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を通じて入手する。 ・転出元市区町村からの接種記録の入手 当区への転入者について、転出元市区町村から接種記録を入手するが、その際は、当区において住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム(VRS)を通じて入手する。 ・新型コロナウイルス感染症予防接種証明書の交付申請者からの個人番号の入手 接種者について、新型コロナウイルス感染症予防接種証明書の交付のために個人番号を入手するのは、接種者から接種証明書の交付申請があった場合のみとし、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 （新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付） 交付申請には、個人番号カードのICチップ読み取り（券面事項入力補助AP）と暗証番号入力（券面事項入力補助APの暗証番号）による二要素認証を必須とすることで、対象者以外の情報の入手を防止する。 ＜サービス検索・電子申請機能における措置＞ ・マニュアルやweb上で、個人番号の提出が必要な者の要件を明示、周知し、本人以外の情報の入手を防止する。
必要な情報以外を入手することを防止するための措置の内容	・届出・申請用紙等について、あらかじめ法令等により定められた様式で提出されることから、必要以外の情報が記載できない書式となっている。 ・契約医療機関等から提出された予防接種票等の情報を保健情報システムに入力する場合、システムで定められた項目以外の登録はできない仕組みとなっている。 ・住民がサービス検索・電子申請機能の画面の誘導に従いサービスを検索し申請フォームを選択して必要情報を入力することとなるが、画面での誘導を簡潔に行うことで、異なる手続に係る申請や不要な情報を送信してしまうリスクを防止する。 ＜ワクチン接種記録システム等における追加措置＞ （新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付） 個人番号カードや旅券の読み取りにより必要な情報を入手し、申請者の自由入力を避けることで、交付申請者が不要な情報を送信してしまうリスクを防止する。
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	＜新型インフルエンザ等対策特別措置法に基づく予防接種、予防接種法に基づく臨時接種及び新型コロナウイルス感染症対策に係る予防接種＞ ・予防接種票に個人情報の使用目的を明記し、対象者に対し口頭または案内文等で利用目的・方法を説明する。 ・委託業務については委託先との契約により、委託業者が根拠法令等の規定に基づき正当な情報取扱いを実施するよう指導する。 ・「保健予防課情報セキュリティ実施手順」よる情報セキュリティ教育実施の際、根拠法令等の規定に基づく正当な資料の入手を指導徹底する。 ・保健情報システムを利用するには、個人ごとに設定されたID・パスワード・生体（顔）による認証が必要であり、操作権限を付与された職員のみ、システムの利用が可能である。 ・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、不適切な入力・更新を抑止している。 ＜新型コロナウイルス感染症対策に係る予防接種事務における措置（VRS）＞ 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。 （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） 当該機能では、専用アプリからのみ交付申請を可能とする。アプリの改ざん防止措置を講じることで、意図しない不適切な方法で特定個人情報が送信されることを避ける。 （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においてキオスク端末の操作画面を制御し、コンビニ交付に対応する市区町村に対してのみキオスク端末から交付申請を可能とすることで、意図しない不適切な方法で特定個人情報が送信されることを避ける。 ＜サービス検索・電子申請機能における措置＞ ・住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、のちに署名検証も行われるため、本人からの情報のみが送信される。 ・サービス検索・電子申請機能の画面の誘導において住民に何の手続を探し電子申請を行いたいのか理解してもらいながら操作をしていただき、たどり着いた申請フォームが何のサービスにつながるものか明示することで、住民に過剰な負担をかけることなく電子申請を実施いただけるよう措置を講じている。
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	＜全般＞ ・新宿区民の住民情報は、庁内連携システムとの連携処理（バッチ処理）にて取得するため、既に本人確認は行われている。 ・窓口での申請等で本人から個人番号を入手する場合には、個人番号カードや通知カード（※）の提示を受ける。また、本人確認を行う際は、番号法第16条及び施行令第12条に基づき、本人確認書類の提示等を受ける。 ※ 通知カードを使用してマイナンバーの確認と本人確認を同時に行うためには、別に運転免許証や旅券等の本人確認書類を必要とする。 ・医療機関や集団接種会場、他自治体から入手する予防接種情報は、予防接種票に記載された特定個人情報に基づき、保健情報システムで突合、確認を行う。 ＜サービス検索・電子申請機能における措置＞ ・住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、電子署名付与済の個人番号付電子申請データを受領した地方公共団体は署名検証（有効性確認、改ざん検知等）を実施することとなる。これにより、本人確認を実施する。 ＜ワクチン接種記録システム(VRS)における追加措置＞ （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） 個人番号カードのICチップ読み取り（券面事項入力補助AP）と暗証番号入力（券面事項入力補助APの暗証番号）による二要素認証で本人確認を行うため、本人からの情報のみが送信される。
個人番号の真正性確認の措置の内容	・新宿区民の個人番号は、統合宛名等システムで一元管理されている情報と連携しているため、真正性は確保されている。 ・窓口で住民から直接申請書等を受け付ける場合は、個人番号カードもしくは法令により定められた身分証明書の組み合わせによる確認等「特定個人情報の適正な取扱いに関するガイドライン」に例示された方法により確認を行う。

特定個人情報の正確性確保の措置の内容	＜全般＞ ・入手した特定個人情報は、システムで確認した特定個人情報と突合して正確性を確保する。 ・入手した情報の入力・削除及び訂正を行う際に、複数人による確認を行うことで正確性を確保している。 ・窓口において予診票等を発行する場合は、その場で本人等に記載内容を確認してもらうことで正確性を確保している。 ・正確性に疑義が生じた場合は、随時調査を行い、必要に応じてデータを修正することで正確性を確保する。 ＜サービス検索・電子申請機能における措置＞ 【「自動入力機能」（令和3年9月1日目途）実装前】 ・サービス検索・電子申請機能への個人番号の入力時には、チェックデジット等の機能により、不正確な個人番号が入力されないようにしている。 【「自動入力機能」（令和3年9月1日目途）実装後】 ・個人番号カード内の記憶領域に格納された個人番号を申請フォームに自動転記を行うことにより、不正確な個人番号の入力を抑止する措置を講じている。 ＜ワクチン接種記録システム(VRS)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電子交付機能、コンビニ交付） ・券面入力補助APを活用し、個人番号カード内の記憶領域に格納された個人番号を申請情報として自動的に入力することにより、不正確な個人番号の入力を抑止する措置を講じている。 ・券面事項入力補助APから取得する情報（4情報・マイナンバー）に付されている署名について、VRS又は証明書交付センターシステムにおいて真正性の検証を行い、送信情報の真正性を確認する措置を講じている。
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	＜新型インフルエンザ等対策特別措置法に基づく予防接種、予防接種法に基づく臨時接種及び新型コロナウイルス感染症対策に係る予防接種＞ ・保健情報システムは、インターネットに接続されていない閉鎖的な庁内イントラネットシステムにあり、外部システムとは接続されていないため、ネットワークを通じての情報漏えいは無い。 ・予防接種情報の提出先を事前に指定することで、送付先誤り等による情報漏えい・紛失等を防止している。 ・電子媒体を使用する場合は、保健情報システムへの入力完了後すぐに電子媒体内のデータを消去することで、情報の漏えいを防止している。 ・紙媒体による入手の場合は、保健情報システムへの入力完了後、鍵の掛かる書庫またはキャビネット等に保管している。 ・職員に対して、情報セキュリティ研修を定期的に実施して保有個人情報を不正に取り扱った場合の罰則適用等について周知している。 ＜ワクチン接種記録システム(VRS)における追加措置＞ 入手する特定個人情報については、情報漏えいを防止するために、暗号化された通信回線を使用する。 （新型コロナウイルス感染症予防接種証明書電子交付機能） 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） キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。 また、通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 さらに、キオスク端末の画面表示や音声案内により、マイナンバーカード及び証明書の取り忘れ防止対策を実施する。 ＜サービス検索・電子申請機能における措置＞ ・サービス検索・電子申請機能と地方公共団体との間は、LGWAN 回線を用いた暗号化通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしている。
リスクへの対策は十分か	[　　十分である　　]　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	
＜ワクチン接種記録システム(VRS)における措置＞ ・入手した特定個人情報については、限定された端末を利用して国から配布されたユーザIDを使用し、ログインした場合だけアクセスできるように制御している。	

3. 特定個人情報の使用		
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容		・団体内統合宛名管理機能を有する団体内統合宛名システムにおいては、システム間連携機能により、連携する庁内業務システムごとにアクセスできる情報を制限しており、目的を超えた紐付けや事務に必要のない情報との紐付けを防止している。
事務で使用するその他のシステムにおける措置の内容		・個人番号利用事務に係るシステム以外からは、特定個人情報ファイルを直接参照できないよう、アクセス制御を行っている。 ・庁内連携サーバを介した情報連携については、連携サーバ側のアクセス制御等により、業務に不必要な情報にはアクセスできないよう制御を行っている。 ・保健情報システムを使用して情報照会を行う場合、アクセス権限の設定により、許可された者以外は、当該事務情報が参照できない仕組みとしている。 ・ワクチン接種記録システム(VRS)における措置として、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。
その他の措置の内容		―
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク		
ユーザ認証の管理		[行っている] ＜選択肢＞ 1）行っている 2）行っていない
	具体的な管理方法	・庁内端末起動時にユーザID・パスワードによるユーザ認証及び生体認証（顔認証）を行っている。 ・システムを使用する職員を特定してユーザーIDとパスワードによる認証、IDに応じたアクセス制御機能により不正な使用を防止している。 ・職員ごとにユーザIDを発効して認証に使用するパスワードは、定期的に変更を行っている。 ・VRSでは、 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。 ‣ VRSにおける特定個人情報へのアクセスは、LG-WAN端末による操作に限り可能になるように制御している。 ‣ LG-WAN端末は、限定された者しかログインできる権限を保持しない。 ‣VRSにおけるログイン認証は、ユーザID・パスワードにて行う。 ‣ 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。 ・サービス検索・電子申請機能をLGWAN接続端末上で利用する必要がある職員を特定し、個人ごとのユーザIDを割り当てるとともに、IDとパスワードによる認証を行う。 ・なりすましによる不正を防止する観点から共用 ID の利用を禁止する。
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	・人事異動情報に基づいたアクセス権限の発効・失効を設定している。 ・アクセス権限の発効および失効は、管理者権限IDにより行うため、その他の者が自由に発効および失効を行うことができない。 ・年度当初に人事情報を基にアクセス権限の一括更新を行い、人事異動や退職等による権限の発効および失効を実施している。 ・年度途中にアクセス権限の追加・変更が必要な場合は、システム管理者が速やかに権限の発効および失効を行う。 ・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。 ・サービス検索・電子申請機能のアクセス権限の発効・失効については、以下の管理を行う。 ① 発効の管理 ・ アクセス権限が必要となった場合、ユーザID管理者が事務に必要となる情報にアクセスできるユーザIDを発効する。 ・ ユーザID管理者が各事務に必要となるアクセス権限の管理表を作成する。 ・ アクセス権限の付与を必要最低限とする。 ② 失効の管理 ・ 定期的又は異動/退職等のイベントが発生したタイミングで、権限を有していた職員の異動/退職等情報を確認し、当該事由が生じた際には速やかにアクセス権限を更新し、当該ユーザIDを失効させる。
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	・個人別のアクセス権限表を作成し、不要な権限を付与しないよう管理している。また、必要に応じてアクセス権限表を見直している。 ・アクセス権限の申請／失効の内容と、申請／失効の結果を突合している。 ・職員異動に伴う権限の付け替えは年度当初に一括で行い、年度途中の異動については随時行っている。これらの作業はシステム管理者により、管理者権限IDを用いて行われる。 ・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。

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	・ユーザー名、端末名、操作日時、操作画面、アクセス区分（照会、異動）、アクセス対象者のログを記録している。 ・アクセス記録は、ハードディスクまたはデータセンタ内のバックアップストレージに保管する。 ・アクセス記録について、確認が必要となった場合には即座に確認できる仕組みを準備している。また、異常アクセス（休業日や業務時間外のアクセス等）については、定期的に確認する。 ・VRSにおいても、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。 ・サービス検索・電子申請機能へのアクセスログ、システムへのアクセスログ、操作ログの記録を行い、操作者個人を特定できるようにする。 ・アクセスログ及び操作ログは、改ざんを防止するため、不正プロセス検知ソフトウェアにより、不正なログの書き込み等を防止する。 ・定期的に操作ログをチェックし、不正とみられる操作があった場合、操作内容を確認する。
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		・特定個人情報の使用は、法令等の規定がある場合以外は認められない旨を職員に周知する。 ・事務外で使用した場合には、アクセス記録等で特定可能であることを周知して事務外の使用を抑止する。（新規従業職員向けシステム操作研修時に必ず説明する。） ・職員に対しては、年1回個人情報保護に関する研修及び情報セキュリティ自己チェックを実施している。 ・委託先に対しては、個人情報保護に係る特記事項を契約書に付している。 ・システム端末は無線シンクライアント方式で、端末本体に情報を保存できず、職場以外では使用できない仕組みとなっている。 ・サービス検索・電子申請機能へアクセスできる端末を制限する。 ・外部記憶媒体にサービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータを複製する場合、使用管理簿に記載し、事前に責任者の承認を得たうえで複製する。なお、外部記憶媒体は限定されたUSBメモリ等のみを使用する。 ・外部記憶媒体内のデータは暗号化する。
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		＜新型インフルエンザ等対策特別措置法に基づく予防接種、予防接種法に基づく臨時接種及び新型コロナウイルス感染症対策に係る予防接種＞ ・特定個人情報ファイルの外部媒体への出力は、原則禁止している。 ・職員に対しては、年1回個人情報保護に関する研修を行い、業務外又は不必要な情報の複写・複製の禁止等について指導している。 ・システム上、管理権限を与えられた者以外、情報の複製は行えない仕組みとする。また、バックアップ以外に不要なファイルを複製しないよう、従業者に対し周知する。 ・バックアップファイルの作成は、入退室管理している室内のサーバー内において実施している。 ・システム保守作業の際は、必ず職員が立ち会いを実施し、委託先に対しては、個人情報保護に係る特記事項を契約に付している。 ・職員が通常使用する端末装置は、USBメモリ等外部媒体の接続をシステム上制限している。（課に1台の作業用端末のみ接続を許可。当該端末は貸出記録及び施錠管理している。） 〈新型コロナウイルス感染症対策に係る予防接種事務における措置（VRS）〉 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VRSへ登録する際には、以下のようにしている。 ・作業を行う職員及び端末を必要最小限に限定する。 ・作業に用いる電子記録媒体については、不正な複製、持ち出し等を防止するために、許可された専用の外部記録媒体を使用する。また、媒体管理簿等に使用の記録を記載する等、利用履歴を残す。 ・作業に用いる電子記録媒体の取扱いについては、承認を行い、当該承認の記録を残す。 ・電子記録媒体に格納するデータについては、暗号化やパスワード設定を行う。 ・電子記録媒体による作業を終了したら、内部のデータを確実に消去する。 ・管理簿に消去の記録を記載する等、消去履歴を残す。 ＜サービス検索・電子申請機能における措置＞ ・サービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータについて、改ざんや業務目的以外の複製を禁止するルールを定め、ルールに従って業務を行う。 ・アクセス権限を付与された最小限の職員等だけが、個人番号付電子申請等のデータについて、LGWAN 接続端末への保存や外部記憶媒体への書き出し等ができるようシステム的に制御する。 ・外部記憶媒体にサービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータを複製する場合、使用管理簿に記載し、事前に責任者の承認を得たうえで複製する。なお、外部記憶媒体は限定されたUSBメモリ等のみを使用する。 ・外部記憶媒体内のデータは暗号化する。

リスクへの対策は十分か	[　十分である　]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置

<新型コロナウイルス感染症対策に係る予防接種事務における措置（VRS）>
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。
・当区への転入者について、転出元市区町村へ接種記録を照会する場合のみ入手し、使用する。
・当区からの転出者について、当区での接種記録を転出先市区町村へ提供するために、個人番号を入手し、使用する。
・接種者について、新型コロナウイルス感染症予防接種証明書の交付申請があった場合に、接種記録を照会するために、個人番号を入手し、使用する。

②VRS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。

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	契約書の個人情報保護に関する特記事項等に基づき、個人情報の管理と情報セキュリティの遵守について、必要な措置を講ずることと記載している。また、プライバシーマーク使用許諾証等の確認をしている。 その他、当区の情報セキュリティ対策基準に基づき、委託先において個人情報が適正に管理されているかどうかを以下の観点で確認する。 ・個人情報の管理的な保護措置(個人情報取扱規定、体制の整備等) ・個人情報の物理的保護措置(人的安全管理、施設および設備の整備、データ管理、バックアップ等) ・個人情報の技術的保護措置(アクセス制御、アクセス監視やアクセス記録等) ・委託内容に応じた情報セキュリティ対策が確保されること ・情報セキュリティマネジメントシステム(ISO27001)の国際規格の認証取得情報 また、VRSにおいては、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、VRS（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとしている。 なお、次の内容については、当該確認事項に規定されている。 ・特定個人情報ファイルの閲覧者・更新者の制限 ・特定個人情報ファイルの取扱いの記録 ・特定個人情報の提供ルール/消去ルール ・委託契約書中の特定個人情報ファイルの取扱いに関する規定 ・再委託先による特定個人情報ファイルの適切な取扱いの確保 ・新型コロナウイルス感染症予防接種証明書電子交付機能において、申請者本人から特定個人情報の提供を受ける際の入手に係る保護措置
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	・特定個人情報ファイルの閲覧・更新者を限定するため、事前に情報資産を取り扱うすべての従事者名簿（所属、氏名、作業内容等）の提出を義務付けている。 ・ユーザIDによる識別とパスワードによる認証、利用可能な機能の制限等により、事前に申請許可された者以外のアクセスを制限している。 ・運用保守業務において特定個人情報ファイルにアクセスする場合は、作業者および作業内容等を事前に確認して承認を行っている。
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	・システムの操作ログを記録し、バックアップを保存している。（5年以上）

特定個人情報の提供ルール		[　　定めている　　]　＜選択肢＞ 1）定めている　2）定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	・契約書において、業務上知り得た個人情報等の第三者への提供禁止（守秘義務）を定めている。 ・原則として、事前に新宿区の承諾を得た場合を除き再委託を禁止している。 ・作業終了後、書面により作業内容等を報告させることで、その内容を確認している。 ・当区の情報セキュリティ対策基準に基づき、委託先は、特定個人情報の目的外利用及び第三者に提供してはならないこと、特定個人情報の複写、複製、またはこれらに類する行為をすることはできないことなどについて委託契約書に明記することとしている。 ・当区における個人情報保護条例第32条の4により、委託先においても個人情報の漏えい、滅失または毀損の防止等に関する安全確保の措置を義務付けしている。 ・当区の情報セキュリティ管理者が委託契約の調査事項に基づき、必要があるときは委託先に対して調査を行うまたは報告を求める。
	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	・契約において、業務上知り得た個人情報等の目的外利用・複製及び持出しの禁止を定めている。（契約終了後についても徹底するよう明記） ・作業終了後、書面により作業内容等を報告させることで、その内容を確認している。 ・当区の情報セキュリティ対策基準に基づき、委託契約書において、委託業務の定期報告及び緊急時報告を義務付けし、特定個人情報の取扱いに関して定期的に委託先から書面にて報告を受けることとしている。 ・当区の情報セキュリティ管理者が委託契約の調査事項に基づき、必要があるときは調査を行いまたは報告を求める。
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	・契約書において、契約終了後に返還又は消去するよう定めている。 ・書面により作業内容等を報告させることで、その内容を確認している。 ・特定個人情報等は、業務完了後は速やかに返還し、または漏えいを起こさない方法によって確実に消去、または処分することを、当区の情報セキュリティ対策基準に基づき、委託契約書に明記することとしている。 ・委託契約終了後は、委託先から特定個人情報等の消去・廃棄等に関する報告書を提出させ、当区の情報システム管理者が消去および廃棄状況の確認を行う。
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	・業務を行うために個人情報を収集するときは、その利用目的をできる限り特定し、その利用目的を達成するために必要な最小限の範囲で公正かつ適正な手段によって収集しなければならない。 ・業務を行うために個人情報を収集するときは、本人に対しその利用目的を明示し、かつ本人から直接これを収集しなければならない。 ・業務に関して知り得た個人情報は、この契約の目的以外に利用し、又は第三者に漏らしてはならない。この契約が終了した後においても同様とする。 ・業務で取り扱う個人情報については、施錠できる保管庫に保管する等善良な管理者の注意をもって保管及び管理にあたらなければならない。 ・収集した個人情報を複写し、又は複製してはならない。 ・個人情報を取り扱う業務を一切第三者に委託してはならない。 ・この契約の終了後は、資料等を返還し、又は消去すること。 ・事故が発生し、又は発生するおそれがあるときは、直ちに委託者に通知するとともに必要な措置を講じ、遅延なくその状況について書面をもって報告すること。 ・必要に応じて個人情報の取り扱い状況の報告を行い、又は立入調査等の監査を受けること。 ・従業者に対する個人情報の適正な管理及び情報セキュリティに関する教育を実施し、新宿区個人情報保護条例について周知すること。 ・秘密保持義務 ・事業所内からの特定個人情報の持出しの禁止 ・特定個人情報の目的外利用の禁止 ・漏えい事案等が発生した場合の再委託先の責任の明確化 ・委託契約終了後の特定個人情報の返却または廃棄 ・特定個人情報を取り扱う従業者の明確化 ・従業者に対する監督・教育 ・契約内容の遵守状況について報告を求める規定 等を定めるとともに、委託先が当区と同等の安全管理措置を講じていることを確認する。

再委託先による特定個人情報ファイルの適切な取扱いの確保		[　再委託していない　] ＜選択肢＞ 1）特に力を入れて行ってい　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	・再委託は行っていないが、再委託を行う場合は再委託契約に次の事項を盛り込むこととする。 ・秘密保持義務 ・特定個人情報等の個人情報を取り扱う業務については禁止 ・漏えい事案等が発生した場合の再委託先の責任の明確化 ・契約終了後は、資料等を返還し、又は消去すること。 ・従業者に対する監督・教育 ・契約内容の遵守状況について報告を求める規定等 ・また、再委託先が当区と同等の安全管理措置を講じていることを確認する。具体的には再委託事務の定期報告および緊急時報告義務を委託契約書に明記し、アクセス権限の管理状況を定期的に報告させる。
その他の措置の内容		―
リスクへの対策は十分か		[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
―		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）　[　] 提供・移転しない

リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録		[　記録を残している　] ＜選択肢＞ 1）記録を残している　2）記録を残していない
	具体的な方法	・特定個人情報ファイルの情報連携は、団体内統合宛名システムへの通信に限定してシステムログ（連携日時等）としてストレージ等に5年間記録している。 ＜団体内統合宛名システムにおける措置＞ ・特定個人情報ファイルの提供・移転の記録は、システムログ（情報連携先、連携日時等）としてストレージ等に5年間記録している。 ・外部媒体に記録する場合は、外部媒体を施錠管理されたデータセンタで保管する。 ＜VRSにおける措置＞ VRSでは、他市区町村への提供の記録を取得しており、委託業者から「情報提供等の記録」を入手し、記録の確認をすることができる。
特定個人情報の提供・移転に関するルール		[　定めている　] ＜選択肢＞ 1）定めている　2）定めていない
	ルールの内容及びルール遵守の確認方法	・庁内連携による情報の移転は、番号法第19条第9号に基づく条例で定められた事務・情報のみ認めている。 ・事前に移転先から利用申請を提出してもらい、その内容を審議の上承認している。 ・情報セキュリティポリシーの遵守状況及び個人情報の管理に関する問題の有無について確認を行い、問題が発生していた場合は、速やかに新宿区情報システム緊急時対応計画に従い適切な措置を講じている。 ・特定個人情報の提供・移転は、番号法等法令の規定によりその範囲を厳格に定め、その範囲についてのみ行う。 ・特定個人情報ファイルの情報連携は、団体内統合宛名システムへの通信に限定してシステムログ（連携日時等）としてストレージ等に記録している。また、必要に応じて記録の確認を行う。 ＜団体内統合宛名システムにおける措置＞ ・特定個人情報ファイルの提供・移転の記録は、システムログ（情報連携先、連携日時等）としてストレージ等に記録しており、システム管理者が必要に応じて記録の確認を行う。
その他の措置の内容		―
リスクへの対策は十分か		[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク2： 不適切な方法で提供・移転が行われるリスク	
リスクに対する措置の内容	〈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措置（VRS）〉 ・他市区町村への個人番号の提供 当区への転入者について、転出元市区町村から接種記録を入手するため、他市区町村へ個人番号を提供するが、その際は、住民基本台帳等により照会対象者の個人番号であることを確認した情報をワクチン接種記録システム(VRS)を用いて提供する。 また、転出先市区町村へ接種記録を提供するが、その際は、転出元市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム(VRS)を用いて提供する。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク	
リスクに対する措置の内容	〈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措置（VRS）〉 ・他市区町村への個人番号の提供、転出先市区町村への接種記録の提供 当区への転入者について、転出元市区町村から接種記録を入手するため他市区町村へ個人番号を提供するが、電文を受ける市区町村で、該当者がいない場合は、個人番号は保管されず、これに対して接種記録は提供されない仕組みとなっている。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置	
＜VRSにおける措置＞ ・特定個人情報の提供は、限定された端末（LG-WAN端末）だけができるように制御している。 ・特定個人情報を提供する場面を必要最小限に限定している。 具体的には、当区への転入者について、転出元市区町村での接種記録を入手するために、他市区町村へ個人番号を提供する場面に限定している。	
6. 情報提供ネットワークシステムとの接続	**[ ] 接続しない（入手） [ ] 接続しない（提供）**
リスク1： 目的外の入手が行われるリスク	
リスクに対する措置の内容	＜中間サーバ・ソフトウェアにおける措置＞ ・情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ・中間サーバの職員認証・権限管理機能（※3）では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※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リスト化し、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。 ＜中間サーバの運用における措置＞ ・中間サーバで取得した情報照会に係るシステムログを使用して目的外および不正な入手が行われていないか必要に応じて確認する。
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・ソフトウェアにおける措置＞ ・中間サーバは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 ＜中間サーバ・プラットフォームにおける措置＞ ・中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ・中間サーバと市区町村についてはVPN等の技術を利用し、市区町村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・ソフトウェアにおける措置＞ ・中間サーバは、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を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。
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・ソフトウェアにおける措置＞ ・中間サーバは、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ・既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ・情報照会が完了または中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報が漏えい・紛失するリスクを軽減している。 ・中間サーバの職員認証・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。 （※）中間サーバは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ＜中間サーバ・プラットフォームにおける措置＞ ・中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、漏えい・紛失のリスクに対応している。 ・中間サーバと市区町村についてはVPN等の技術を利用して市区町村ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ・中間サーバ・プラットフォーム事業者の業務は、中間サーバ・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。 ＜中間サーバの運用における措置＞ ・中間サーバで取得した情報照会に係るシステムログを使用して目的外および不正な入手が行われていないか必要に応じて確認する。
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	＜保健情報システムにおける措置＞ ・ユーザIDによる識別とパスワードによる認証、利用可能な権限の制限等により、不正な使用を防止している。 ・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、操作内容の記録を実施することで、不適切な端末操作を抑止する。 ・特定個人情報ファイルの情報連携は、団体内統合宛名システムへの通信に限定し、システムログ（連携日時等）として記録している。また、必要に応じて記録の確認を行う。 ＜団体内統合宛名システムにおける措置＞ ・中間サーバとの情報連携は、団体内統合宛名システムが一括して行うため、業務システムから中間サーバへ直接情報連携できない仕組みとしている。 ・団体内統合宛名システムにおいて、中間サーバへの情報提供が可能な権限と、その権限において提供可能な特定個人情報の制限を行っている。 ・特定個人情報ファイルの情報連携の記録はシステムログ（情報連携先、連携日時等）として記録しており、必要に応じて記録の確認を行う。 ・認証管理機能により、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・ソフトウェアにおける措置＞ ・情報提供機能（※）により、情報提供ネットワークシステムにおける照会許可用照合リストを情報提供ネットワークシステムから入手し、中間サーバに格納したうえで照会許可用照合リストを基に情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ・情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。 ・特に慎重な対応が求められる情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑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および情報提供を行う機能。 ＜中間サーバの運用における措置＞ ・中間サーバで取得した情報提供に係るシステムログを使用して不正な提供が行われていないか必要に応じて確認する。
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	＜保健情報システムにおける措置＞ ・特定個人情報ファイルの情報連携は、団体内統合宛名システムへの通信に限定する。 ・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、操作内容の記録を実施することで、不適切な端末操作を抑止する。 ・特定個人情報ファイルの提供・移転の記録（提供・移転先、日時等）をシステム上で管理しており、必要に応じてシステム管理者が記録の確認を行う。 ＜団体内統合宛名システムにおける措置＞ ・業務システムとの連携は、インターネット網とは分離した庁内業務専用ネットワークの通信に限定している。また、ファイアウォール等による通信制御により、権限を有しないものによる不適切な方法による情報提供を防止している。 ・中間サーバとの連携は、行政専用のネットワーク（統合行政ネットワーク等）の通信に限定している。 ・特定個人情報ファイルの情報連携の記録はシステムログ（情報連携先、連携日時等）として記録しており、必要に応じてシステム管理者が記録の確認を行う。 ・認証管理機能により、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・ソフトウェアにおける措置＞ ・セキュリティ管理機能（※）により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ・中間サーバの職員認証・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、鍵情報および照会許可用照合リストを管理する機能。 ＜中間サーバ・プラットフォームにおける措置＞ ・中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、不適切な方法で提供されるリスクに対応している。 ・中間サーバと市区町村についてはVPN等の技術を利用し、市区町村ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ・中間サーバ・プラットフォームの保守・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。 ＜中間サーバの運用における措置＞ ・中間サーバで取得した情報提供に係るシステムログを使用して不適切な方法で提供が行われていないか必要に応じて確認する。
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	＜保健情報システムにおける措置＞ ・情報登録の際には、誤った情報の登録を行わないように、複数人による二重チェックを実施する。 ・システムの機能により、項目ごとの入力制限（ありえない入力パターンの制限等）や登録前の論理チェックを実施する。 ・特定個人情報ファイルの情報連携は、団体内統合宛名システムへの通信に限定する。 ＜団体内統合宛名システムにおける措置＞ ・中間サーバとの情報連携は、団体内統合宛名システムが一括して行うため、業務システムから中間サーバへ直接情報連携できない仕組みとしている。 ・団体内統合宛名システムにおいて、中間サーバへの情報提供が可能な権限と、その権限において提供可能な特定個人情報の制限を行っている。 ・団体内連携テスト、情報提供ネットワークシステムとの連携テスト・総合運用テスト等の検証工程で、特定個人情報の正確性を十分に検証したうえで中間サーバに誤った情報を提供した場合のリカバリ手順等を明確にする。 ＜中間サーバ・ソフトウェアにおける措置＞ ・情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領したうえで情報照会内容に対応した情報提供をすることで、 誤った相手に特定個人情報が提供されるリスクに対応している。 ・情報提供データベース管理機能（※）により「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ・情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 （※）特定個人情報を副本として保存・管理する機能。 ＜中間サーバの運用における措置＞ ・中間サーバに誤った情報を提供した場合のリカバリ手順等を明確にする。
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

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・ソフトウェアにおける措置＞ ・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ・情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバ・プラットフォームにおける措置＞ ・中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ・中間サーバと市区町村についてはVPN等の技術を利用し、市区町村ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ・中間サーバ・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバ・プラットフォームを利用する市区町村であっても他市区町村が管理する情報には一切アクセスできない。 ・特定個人情報の管理を地方公共団体のみが行うことで、中間サーバ・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。

7. 特定個人情報の保管・消去

リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	＜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	＜新宿区における措置＞ ・通常業務使用する端末自体には、特定個人情報を保管していない。 ・サーバー及びネットワーク機器の設置室（以下「セキュリティ区域」という。）に入室する者をあらかじめ指定し、指定した者以外は入室させない。 ・セキュリティ区域は通常時は施錠し、入室の度に鍵又は指紋認証等で鍵を開けている。 ・セキュリティ区域のうち、特に重要な機器等を設置する場所においては、入退室の記録を行うほか、監視カメラによる入退室の監視を行っている。 ・サーバー等の機器等を取り付ける場合は、火災・水害・ほこり・振動・温度・湿度等の影響を可能な限り排除した場所に設置し、万が一、火災・水害等の災害が発生した場合に備え異常を知らせる自動監視装置を設置している。 ・紙媒体・電子記録媒体については、事務室内のキャビネット及び倉庫に施錠保管している。 ＜中間サーバ・プラットフォームにおける措置＞ ・中間サーバ・プラットフォームをデータセンタに構築して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。 ＜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。	

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	＜新宿区における措置＞ ・新宿区情報セキュリティ規定に基づき、コンピュータウイルス対策のためのソフトウェアを導入し、最新のウイルスパターンファイルのリリース後、速やかに更新作業を実施している。 ・振る舞い検知型のコンピュータウイルス検出ソフトウェアにより標的型攻撃対策を講じている。 ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォールを設置している。 ・導入しているOS及びミドルウェアには、最新のセキュリティパッチのリリース後、速やかに適用作業を実施している。 ・個々の職員のITモラルと情報セキュリティ意識の底上げを図り、当区におけるウイルス感染・不正侵入・情報漏えい等のリスクを低減することを目的に、研修の実施や不審メール受信時対応訓練等を行っている。 ＜VRSにおける措置＞ 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。 ・LG-WAN端末と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電子交付機能） ・電子交付アプリには、申請情報を記録しないこととしている。 ・電子交付アプリとVRSとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 （新型コロナウイルス感染症予防接種証明書コンビニ交付） ・証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。 ・キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。 また、通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 ＜サービス検索・電子申請機能＞ ・LGWAN 接続端末へのウィルス検出ソフトウェア等の導入により、ウィルス定義ファイルの定期的な更新及びウィルスチェックを行い、マルウェア検出を行う。 ・サービス検索・電子申請機能と地方公共団体との間は、LGWAN回線を用いた暗号化通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしている。
⑦バックアップ		[　十分に行っている　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知		[　十分に行っている　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか		[　発生なし　] ＜選択肢＞ 1）発生あり　2）発生なし
	その内容	―
	再発防止策の内容	―
⑩死者の個人番号		[　保管している　] ＜選択肢＞ 1）保管している　2）保管していない
	具体的な保管方法	生存する個人の個人番号と同様の方法にて保管している。
その他の措置の内容		―
リスクへの対策は十分か		[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク2： 特定個人情報が古い情報のまま保管され続けるリスク		
リスクに対する措置の内容		・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	・LGWAN 接続端末については、業務終了後の不要な個人番号付電子申請データ等の消去について徹底し、必要に応じて管理者が確認する。 ・文書管理基準表により保存期間を確認し、保存期間を経過した紙媒体の特定個人情報については、溶解・焼却・細断等により廃棄している。 ＜保健情報システムの手順＞ ・保管期間を経過したのちに不要となった特定個人情報をシステム保有課職員の指示のもと、委託業者が一括して削除する仕組みとする。 ・データ間の整合性を損なうことなく削除する必要があるため、業務担当職員の指示のもと、削除作業は委託しているシステム業者が行うものとする。
その他の措置の内容		－
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		
－		

Ⅳ　その他のリスク対策 ※

1. 監査		
①自己点検		[　　十分に行っている　　]　＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
	具体的なチェック方法	【当区における措置】 ・特定個人情報保護評価に関する規則（平成26年4月18日特定個人情報保護委員会規則第1号）第14条（評価書の修正）に基づき、少なくとも年1回評価書に記載した事項の見直しを担当部署において行う。また、同規則第15条及び特定個人情報保護評価指針に基づき、直近の評価書を公表してから5年を経過する前に、保護評価を再実施するよう努める。 ・「新宿区情報セキュリティ規則」に定める情報セキュリティポリシーの遵守に取り組んでいることを自己チェックにより確認する。自己チェックの結果を受けて、情報資産へのリスクを洗い出し、改善策を策定・実施する。 【中間サーバー・プラットフォームにおける措置】 ・運用規則等に基づき、中間サーバー・プラットフォーム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。 【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措置（VRS）>>>

３．その他のリスク対策

＜中間サーバ･プラットフォームにおける措置＞
・中間サーバ・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減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。

＜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措置（VRS）＞
・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。

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		新宿区健康部保健予防課予防係 〒160-0022　新宿区新宿五丁目18番21号　　電話:03-5273-3859(直通)
②請求方法		指定様式による書面の提出により開示・訂正・利用停止請求を受け付けます。 自己情報開示請求書等に必要事項を記入の上、提出していただきます。 本人であることを証明するための書類(運転免許証、パスポート等)の提出または提示が必要です。 郵送による請求は、認めておりません。
	特記事項	代理人による請求があった場合は、代理関係を確認するため、戸籍謄本、登記事項証明書、委任状等の書類を窓口にて提示してもらう。
③手数料等		[　　無料　　] (手数料額、納付方法: ＜選択肢＞ 1) 有料　　2) 無料)
④個人情報ファイル簿の公表		[　　行っている　　] ＜選択肢＞ 1) 行っている　　2) 行っていない
	個人情報ファイル名	予防接種情報ファイル
	公表場所	新宿区役所第二分庁舎分館　健康部保健予防課
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		新宿区健康部保健予防課予防係 〒160-0022　新宿区新宿五丁目18番21号　　電話:03-5273-3859(直通)
②対応方法		問い合わせの受付時に受付票等を記載することにより、対応について記録を残す。 情報漏えい等の重大な事案に関する問い合わせについて、関係先等に事実確認を行うための標準的な処理期間を設ける。

Ⅵ 評価実施手続

1. 基礎項目評価	
①実施日	令和4年2月10日
②しきい値判断結果	[基礎項目評価及び全項目評価の実施が義務付けられる] ＜選択肢＞ 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 基礎項目評価及び重点項目評価の実施が義務付けられる（任意に全項目評価を実施） 3) 基礎項目評価の実施が義務付けられる（任意に全項目評価を実施） 4) 特定個人情報保護評価の実施が義務付けられない（任意に全項目評価を実施）
2. 国民・住民等からの意見の聴取	
①方法	「新宿区パブリック・コメント制度に関する規則」に定めるところにより、郵送・ファックス・窓口持参又は区のホームページから区民意見聴取を行った。 区民意見聴取の実施に際しては、区の広報紙「広報しんじゅく」に、特定個人情報保護評価の概要と合わせ意見募集を行う旨の掲載をするとともに、本評価書の内容等を区のホームページに掲載し、かつ、保健予防課課・広聴担当課及び特別出張所に備え付け、閲覧可能な状況においた。
②実施日・期間	令和3年11月15日から令和3年12月14日までの30日間
③期間を短縮する特段の理由	－
④主な意見の内容	－ （意見の聴取の結果、意見なし）
⑤評価書への反映	－
3. 第三者点検	
①実施日	令和3年12月6日から令和3年12月27日まで
②方法	個人情報保護、情報システム等に知見を有する外部の第三者に委託して第三者点検を実施する。
③結果	特定個人情報保護評価指針第10（2）に定める審査の観点における主な考慮事項で示された考察事項に基づき点検が行われ、以下の点について指摘があった。 ●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・電子交付の実施について、追記。 ●番号法の改正に伴う、項番修正。 ●誤字・脱字・文言の統一及び補記 ●特定個人情報の保管消去の期間について、保管期間の定めはないが、区民からの照会に対応するため、20年以上に変更。 ●特定個人情報の提供・移転に関するルールを追記。
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
	P6 システム5　②システムの機能	（右記の内容を新たに追加）	7. 新型コロナウイルス感染症予防接種証明書のコンビニ交付の実施	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時の事後評価）の適用対象となるため
	P8 （別添1）事務の内容	（右記の内容を新たに追加）	下に図及び説明の追記	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時の事後評価）の適用対象となるため
	P12 特定個人情報の入手・使用 ②入手方法	〔〇〕その他　（ワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）、サービス検索・電子申請機能）	〔〇〕その他　（ワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）、コンビニエンスストア等のキオスク端末及び証明書交付センターシステム、サービス検索・電子申請機能）	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時の事後評価）の適用対象となるため
	P12 特定個人情報の入手・使用 ③入手の時期・頻度	転出先市区町村から接種記録の照会を受ける都度	他市区町村から接種記録の照会を受ける都度	事後	VRSにおける一括照会機能の追加による修正であり、指針で定める重要な変更に当たらないため
	P12 特定個人情報の入手・使用 ④入手に係る妥当性	当区からの転出者について、転出先市区町村へ当市区町村での接種記録を提供するために、転出先市区長村から個人番号を入手する。	当区からの転出者について、転出先市区町村へ当市区町村での接種記録を提供するために、他市区長村から個人番号を入手する。	事後	VRSにおける一括照会機能の追加による修正であり、指針で定める重要な変更に当たらないため
	P12 特定個人情報の入手・使用 ⑤本人への明示	電子交付アプリにより電子申請を受付ける場合においては、利用規約を表示し、同意を得てから入手する。	電子交付アプリにより予防接種証明書の電子申請を受付ける場合及びコンビニエンスストア等のキオスク端末から予防接種証明書の申請を受け付ける場合においては、利用規約を表示し、同意を得てから入手する。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時の事後評価）の適用対象となるため
	P13 特定個人情報の入手・使用 ⑧使用方法　情報の突合	当区からの転出者について、当区での接種記録を転出先市区町村に提供するために、転出先市区町村から個人番号を入手し、当市区町村の接種記録と突合する。	当区からの転出者について、当区での接種記録を転出先市区町村に提供するために、他市区町村から個人番号を入手し、当市区町村の接種記録と突合する。	事後	VRSにおける一括照会機能の追加による修正であり、指針で定める重要な変更に当たらないため

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
	P14 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事務に関するワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能を含む。)を用いた特定個人情報ファイルの管理等	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。)を用いた特定個人情報ファイルの管理等	事後	特定個人情報保護評価に関する規則第9条第2項の規定(緊急時の事後評価)の適用対象となるため
	P14 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事務に関するワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能を含む。)を用いた特定個人情報ファイルの管理等	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。)を用いた特定個人情報ファイルの管理等	事後	特定個人情報保護評価に関する規則第9条第2項の規定(緊急時の事後評価)の適用対象となるため
	P15 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)(新型コロナウイルス感染症予防接種証明書電子交付機能を含む。)を用いた特定個人情報ファイルの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)(新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。)を用いた特定個人情報ファイルの適切な管理等のために取り扱う必要がある。	事後	特定個人情報保護評価に関する規則第9条第2項の規定(緊急時の事後評価)の適用対象となるため
	P15 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	〔○〕その他　LG-WAN回線を用いた提供(VRS本体)、本人からの電子交付アプリを用いた提供(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)	〔○〕その他　LG-WAN回線を用いた提供(VRS本体、コンビニ交付関連機能)、本人からの電子交付アプリを用いた提供(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)	事後	特定個人情報保護評価に関する規則第9条第2項の規定(緊急時の事後評価)の適用対象となるため
	P17 特定個人情報の保管・消去 ①保管場所	(右記の内容を新たに追加)	(新型コロナウイルス感染症予防接種証明書コンビニ交付) 証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。	事後	特定個人情報保護評価に関する規則第9条第2項の規定(緊急時の事後評価)の適用対象となるため
	P18 (別添2)特定個人情報ファイル記録項目	接種回(1回目/2回目)	接種回(1回目/2回目/3回目/4回目)	事後	VRSにおける一括照会機能の追加による修正であり、指針で定める重要な変更に当たらないため

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
	P19 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　対象者以外の情報の入手を防止するための措置の内容	・転出先市区町村からの個人番号の入手 　当区からの転出者について、当区での接種記録を転出先市区町へ提供するために、転出先市区町村から個人番号を入手するが、その際は、転出先市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を通じて入手する。	・他市区町村からの個人番号の入手 　当区からの転出者について、当区での接種記録を転出先市区町へ提供するために、他市区町村から個人番号を入手するが、その際は、他市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を通じて入手する。	事後	VRSにおける一括照会機能の追加による修正であり、指針で定める重要な変更に当たらないため
	P19 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　対象者以外の情報の入手を防止するための措置の内容	（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）	（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）	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時の事後評価）の適用対象となるため
	P19 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　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	（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）	（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）	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時の事後評価）の適用対象となるため
	P20 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　リスクに対する措置の内容	（右記の内容を新たに追加）	（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においてキオスク端末の操作画面を制御し、コンビニ交付に対応する市区町村に対してのみキオスク端末から交付申請を可能とすることで、意図しない不適切な方法で特定個人情報が送信されることを避ける。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時の事後評価）の適用対象となるため
	P20 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　入手の際の本人確認の措置の内容	（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）	（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）	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時の事後評価）の適用対象となるため

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
	P21 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 特定個人情報の正確性確保の措置の内容	（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）	（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）	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時の事後評価）の適用対象となるため
	P21 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 特定個人情報の正確性確保の措置の内容	券面事項入力補助APから取得する情報（4情報・マイナンバー）に付されている署名について、VRSにおいて真正性の検証を行い、送信情報の真正性を確認する措置を講じている。	券面事項入力補助APから取得する情報（4情報・マイナンバー）に付されている署名について、VRS又は証明書交付センターシステムにおいて真正性の検証を行い、送信情報の真正性を確認する措置を講じている。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時の事後評価）の適用対象となるため
	P21 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 リスクに対する措置の内容	（右記の内容を新たに追加）	（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） キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。また、通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。さらに、キオスク端末の画面表示や音声案内により、マイナンバーカード及び証明書の取り忘れ防止対策を実施する。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時の事後評価）の適用対象となるため
	P24 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	VRS（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）	VRS（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時の事後評価）の適用対象となるため
	P27 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	<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（VRS）> ・転出元市区町村への個人番号の提供 当市区町村への転入者について、転出元市区町村から接種記録を入手するため、転出元市区町村へ個人番号を提供するが、その際は、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を用いて提供する。	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置（VRS）> ・他市区町村への個人番号の提供 当市区町村への転入者について、転出元市区町村から接種記録を入手するため、他市区町村へ個人番号を提供するが、その際は、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を用いて提供する。	事後	VRSにおける一括照会機能の追加による修正であり、指針で定める重要な変更に当たらないため

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
	P27 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	＜ワクチン接種記録システム(VRS)における措置＞ ・転出元市区町村への個人番号の提供、転出先市区町村への接種記録の提供 　当区への転入者について、転出元市区町村から接種記録を入手するため、転出元市区町村へ個人番号を提供するが、その際は、個人番号と共に転出元の市区町村コードを送信する。そのため、仮に誤った市区町村コードを個人番号と共に送信したとしても、電文を受ける市区町村では、該当者がいないため、誤った市区町村に対して個人番号が提供されず、これに対して接種記録も提供されない仕組みとなっている。	＜ワクチン接種記録システム(VRS)における措置（VRS）＞ ・他市区町村への個人番号の提供、転出先市区町村への接種記録の提供 　当区への転入者について、転出元市区町村から接種記録を入手するため、他市区町村へ個人番号を提供するが、電文を受ける市区町村で、該当者がいない場合は、個人番号は保管されず、これに対して接種記録は提供されない仕組みとなっている。	事後	VRSにおける一括照会機能の追加による修正であり、指針で定める重要な変更に当たらないため
	P27 特定個人情報の提供・移転 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置	・特定個人情報を提供する場面を必要最小限に限定している。 　具体的には、当区への転入者について、転出元市区町村での接種記録を入手するために、転出元市町区村へ個人番号と共に転出元の市区町村コードを提供する場面に限定している。	・特定個人情報を提供する場面を必要最小限に限定している。 　具体的には、当区への転入者について、転出元市区町村での接種記録を入手するために、他市町区村へ個人番号を提供する場面に限定している。	事後	VRSにおける一括照会機能の追加による修正であり、指針で定める重要な変更に当たらないため
	P32 特定個人情報の保管・消去 リスク1　具体的な対策の内容	（右記の内容を新たに追加）	（新型コロナウイルス感染症予防接種証明書コンビニ交付） ・証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。 ・キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。また、通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時の事後評価）の適用対象となるため