

個人情報保護管理運営会議 付議事項

件名	予防接種事務のデジタル化に伴う外部結合等について（特定個人情報保護評価の報告）
----	---

内容は別紙のとおり

要綱の根拠

◇第3条第1項第3号（電算処理、外部結合、業務委託）

（担当部課：健康部保健予防課）

事業の概要

事業名	予防接種事務のデジタル化
担当課	健康部保健予防課
目 的	予防接種事務において、手続きをデジタル化することで、区民及び医療機関の事務負担を軽減し、効率的かつ正確な運用を実現するため。
対象者	区が予防接種記録を管理する区民
事業内容	1 概要 現在国では、医療費助成、予防接種、母子保健等の領域におけるマイナンバーカードを活用したデジタル化の取組を推進している。予防接種に関する事務については、感染症法改正法（令和 4 年法律第 96 号）による改正予防接種法（令和 8 年 6 月 1 日施行）に基づき事務のデジタル化が進められており、これを受け、区でも令和 10 年 4 月 1 日の運用開始に向けた準備を進める。 本事業は、予診情報・予防接種記録管理／請求支払システム（以下、「予予・請求システム」という）を活用し、マイナポータル及び医療機関用アプリ等と連携することで、予防接種事務に係る一連の手続きのデジタル化を推進するものである。 区は、対象者の個人番号を含む情報、予診票情報及び接種記録を予予・請求システムに登録・管理し、デジタル庁及び医療機関等との間で安全かつ効率的な情報の連携・授受を行う。デジタル庁と厚生労働省は、デジタル庁が運用する、医療や健康に関する自治体サービスの情報連携基盤である PMH（Public Medical Hub）を介して、効率的に情報を連携する。 区民は、マイナポータルを利用して予診票の事前入力や接種記録・通知の閲覧が可能となる。また、接種時にはマイナンバーカードによる本人確認を行い、医療機関はタブレット端末等を用いて予診票情報の確認及び接種記録の入力を行う。 これにより、従来の紙による運用を見直し、手続きのオンライン化による利便性向上及び行政事務の効率化を図る。 その他、新たに作成する特定個人情報保護評価書については、しきい値判断の結果、特定個人情報保護評価（全項目評価）を実施する。 【スケジュール（予定）】 令和 8 年度 4 月：調整会議（4/28） 6 月：電子計算組織案件の提出 9 月：個人情報保護管理運営会議（9/1）、調整会議（9/30） 10 月：政策経営会議（書面）（10/5～10/6）、 常任委員会報告（10/7） 10 月～11 月：PIA に関する区民への意見聴取（10/15～11/12） PIA に関する第三者点検（10/15～11/19） 12 月：個人情報保護管理運営会議（12/21） 1 月：調整会議（1/20） 2 月：政策経営会議（2/5）、国個人情報保護委員会への評価書提出、 評価書公表 3 月：常任委員会報告（3/16） 令和 9 年度

	4 月以降：健康管理システム改修（標準仕様書 3.1 版） 3 月：予予・請求システム接続（対象者情報・接種記録データ移行） 令和 10 年度 4 月：デジタル化運用開始予定 2 個人情報保護管理運営会議への付議内容 (1) 電算処理 予予・請求システムにおいて、対象者の個人番号、基本情報（氏名・住所等）、予診票情報及び予防接種記録情報を紐付けて登録・管理し、電算処理を行う。 (2) 外部結合 マイナポータル、医療機関用アプリ等、Public Medical Hub、オンライン資格確認等システム等と連携するため、LGWAN 回線又は閉域網回線を用いた外部結合を行う。 (3) 業務委託 ①予予・請求システムの運用保守及び情報連携業務について、東京都国民健康保険団体連合会に委託する。 ②「医療機関アプリ」の提供及び運用保守について、専門事業者に委託する。 3 対象者数 約 356 千人 ※個人情報の流れについては資料 3 8－1、2 のとおり ※予防接種事務のデジタル化の概要については資料（3 8－4）のとおり ※特定個人情報保護評価書（全項目評価書）については別添資料（3 8－5）のとおり
--	--

件名 予防接種に関する事務に係る予診情報・予防接種記録管理／請求支払システムの導入について

保有課（担当課）	保健予防課
登録業務の名称	予防接種に関する事務
記録される情報項目（だれの、どのような項目が、どのコンピュータに記録されるのか）	1 個人の範囲 予防接種法等関連法令に定められる予防接種の対象者 2 記録項目 資料38-3のとおり 3 記録するコンピュータ 予予・請求システム 健康管理システム
新規開発・追加・変更の理由	予防接種事務において、紙の予診票及び手作業による接種記録管理から、マイナポータル及び医療機関用アプリ等と連携したデジタル処理へ移行することで、区民及び医療機関の負担軽減と利便性の向上を図るとともに、行政事務の効率化及び正確性の向上を図るため。
新規開発・追加・変更の内容	予予・請求システムを導入し、対象者の個人番号を含む情報、予診票情報及び接種記録を紐付けて一元管理する。 あわせて、マイナポータルからの予診票入力及び接種記録閲覧、並びに医療機関用アプリ等による予診票確認及び接種記録入力等の情報連携を可能とする。
開発等を委託する場合における個人情報保護対策	別紙チェックリストのとおり
新規開発・追加・変更の時期	令和9年4月～ 開発 令和10年4月～ 本稼働

件名 予防接種に関する事務に係る外部結合について

保有課(担当課)	保健予防課
登録業務の名称	予防接種に関する事務
結合される情報項目(だれの、どのような項目か)	1 個人の範囲 予防接種法等関連法令に定められる予防接種の対象者 2 記録項目 資料38-3のとおり
結合の相手方	①デジタル庁(マイナポータル及びPublic Medical Hub) ②東京都国保連合会(予予・請求システム) ③医療機関(医療機関用アプリ) ④厚生労働省(オンライン資格確認等システム)
結合する理由	マイナポータルを通じた予診票の事前入力、接種記録の閲覧及び通知の提供並びに医療機関における予診票確認及び接種記録入力等を可能とするため、関係システムと情報連携を行い、予防接種事務の効率化及び区民の利便性向上を図る必要があるため。
結合の形態	LGWAN 回線又は閉域網回線を介し、①マイナポータル及びPublic Medical Hub、②予予・請求システム、③医療機関用アプリ、④オンライン資格確認等システムと区イントラネットパソコンを結合する。
結合の開始時期と期間	令和9年9月1日から令和10年3月31日(次年度以降も、同様の外部結合を行う。なお、ここで定める結合開始日はネットワークの疎通調整開始時期であり、区民へのサービス開始は令和10年4月1日以降を予定している。)
情報保護対策	別紙チェックリストのとおり

件名 予防接種に関する事務に係るシステム運用等業務の委託について

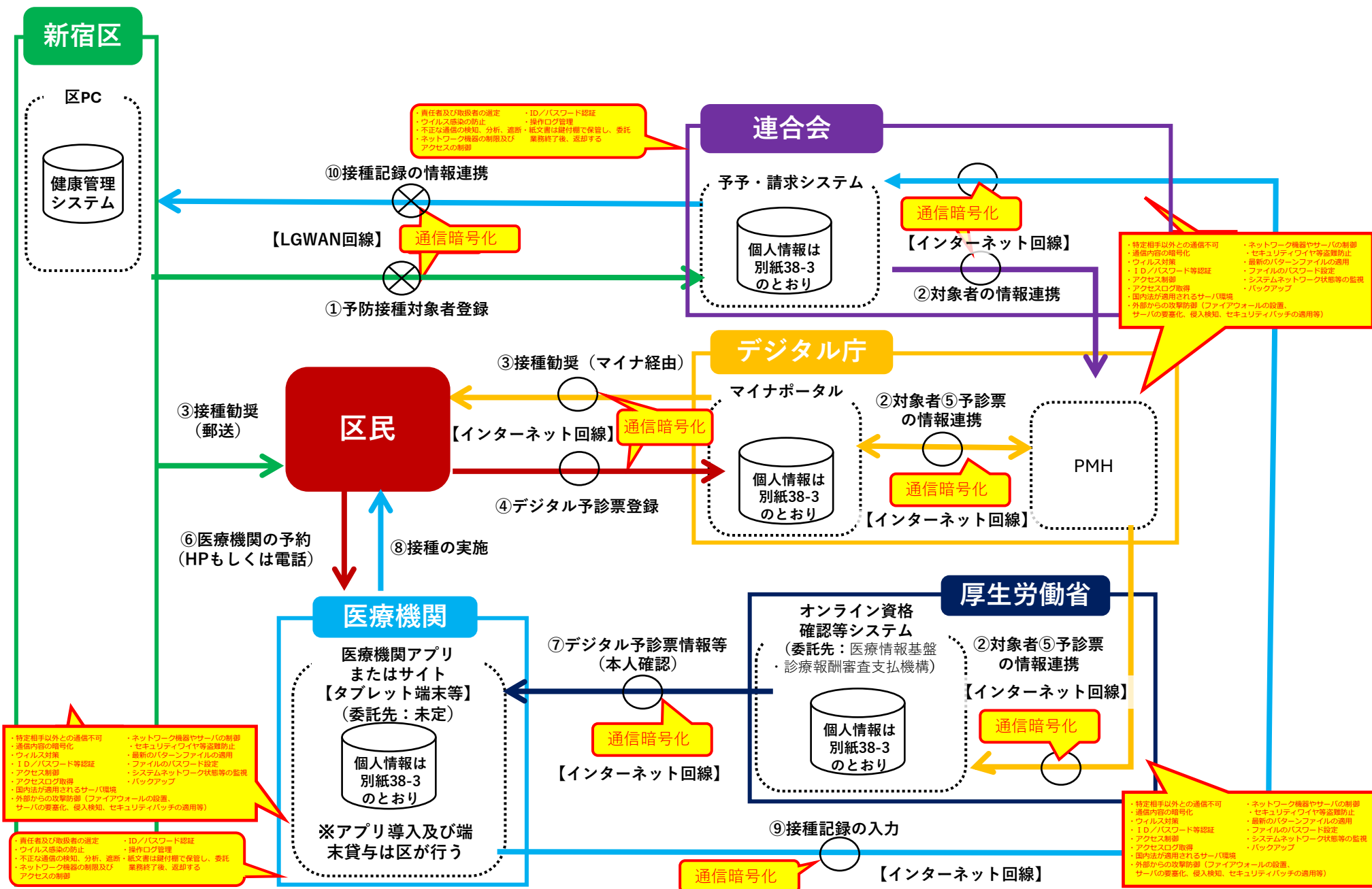
保有課(担当課)	保健予防課
登録業務の名称	予防接種に関する事務
委託先	東京都国民健康保険団体連合会
委託に伴い事業者処理させる情報項目(だれの、どのような項目か)	《委託先に提供する項目、委託先に収集させる項目》 1 個人の範囲 予防接種法等関連法令に定められる予防接種の対象者 2 情報項目 資料38-3のとおり
処理させる情報項目の記録媒体	予予・請求システム(サーバ上のデータ) LGWAN回線又は閉域網回線を用いた電子データ
委託理由	予防接種デジタル化にあたり、全国の自治体が予防接種事務を連合会に委託し、連合会は予予・請求システムの保守管理等を中央会に再委託する。これは広域的な情報連携及び安定的な運用保守が必要であり、専門的知識及び技術を有する事業者へ委託することで、安全かつ効率的なシステム運用を確保する必要があると国が判断したことから、区も同様の判断とするため。
再委託の内容	・予予・請求システムの運用保守業務 ・Public Medical Hubを介した情報連携業務 ・PMHキーの採番処理に関する業務 ・システムの障害対応、保守及び改修対応等
委託の開始時期及び期限	令和10年4月1日から令和11年3月31日まで(次年度以降も、同様の業務委託を行う。)
委託にあたり区が行う情報保護対策	別紙チェックリストのとおり
受託事業者に行わせる情報保護対策	別紙チェックリストのとおり

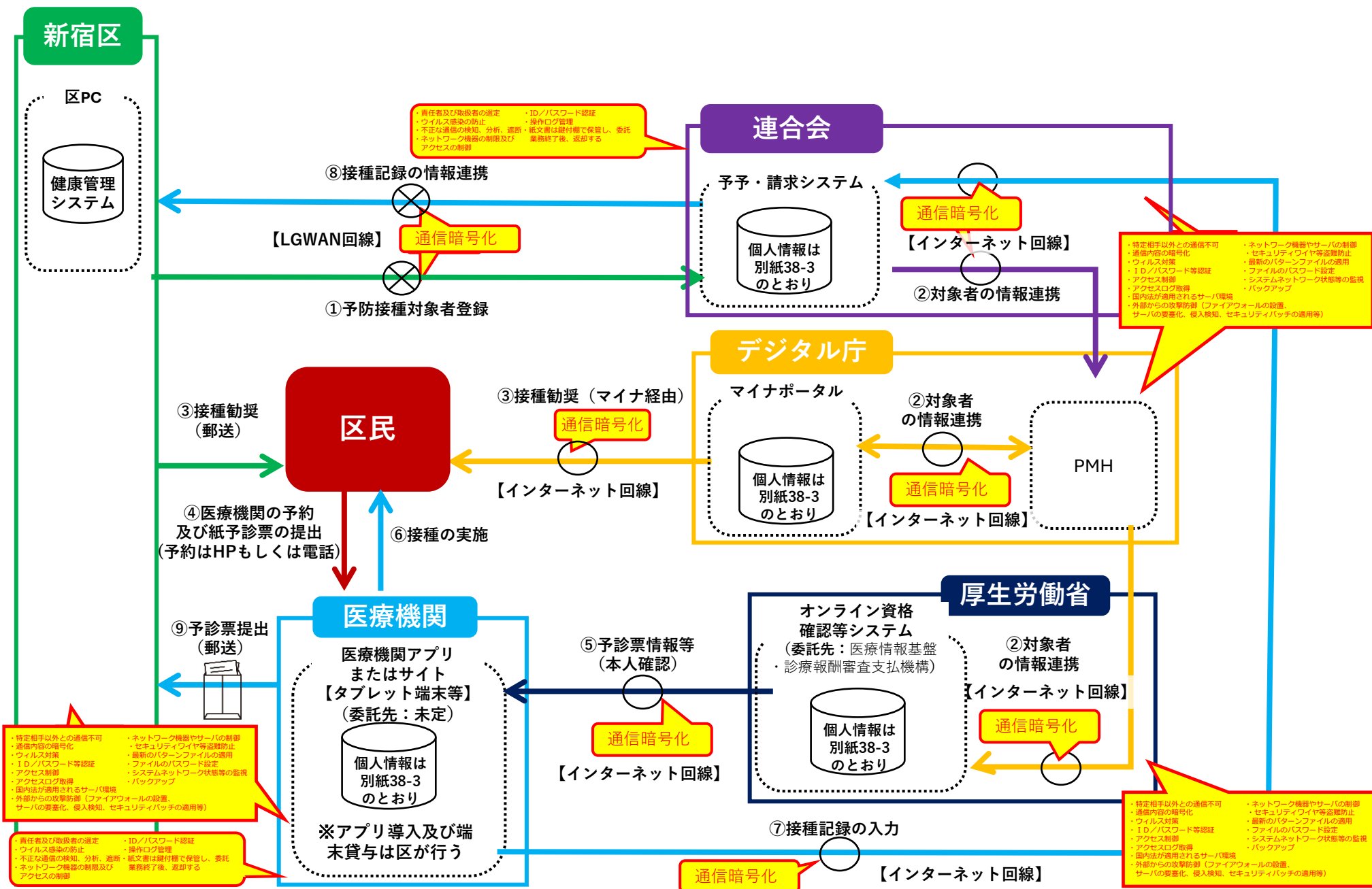
件名 予防接種に関する事務に係るシステム運用等業務の再委託について

保有課(担当課)	保健予防課
登録業務の名称	予防接種に関する事務
再委託先	国民健康保険中央会
委託に伴い事業者処理させる情報項目(だれの、どのような項目か)	《委託先に提供する項目、委託先に収集させる項目》 1 個人の範囲 予防接種法等関連法令に定められる予防接種の対象者 2 情報項目 資料38-3のとおり
処理させる情報項目の記録媒体	予予・請求システム LGWAN回線又は閉域網回線を用いた電子データ
再委託理由	予防接種デジタル化にあたり、全国の自治体が予防接種事務を連合会に委託し、連合会は予予・請求システムの保守管理等を中央会に再委託する。これは広域的な情報連携及び安定的な運用保守が必要であり、専門的知識及び技術を有する事業者へ委託することで、安全かつ効率的なシステム運用を確保する必要があると国が判断したことから、区も同様の判断とするため。
再委託の内容	・予予・請求システムの運用保守業務 ・Public Medical Hubを介した情報連携業務 ・PMHキーの採番処理に関する業務 ・システムの障害対応、保守及び改修対応等
再委託の開始時期及び期限	令和10年4月1日から令和11年3月31日まで(次年度以降も、同様の業務委託を行う。)
委託にあたり区が行う情報保護対策	別紙チェックリストのとおり
受託事業者に行わせる情報保護対策	別紙チェックリストのとおり

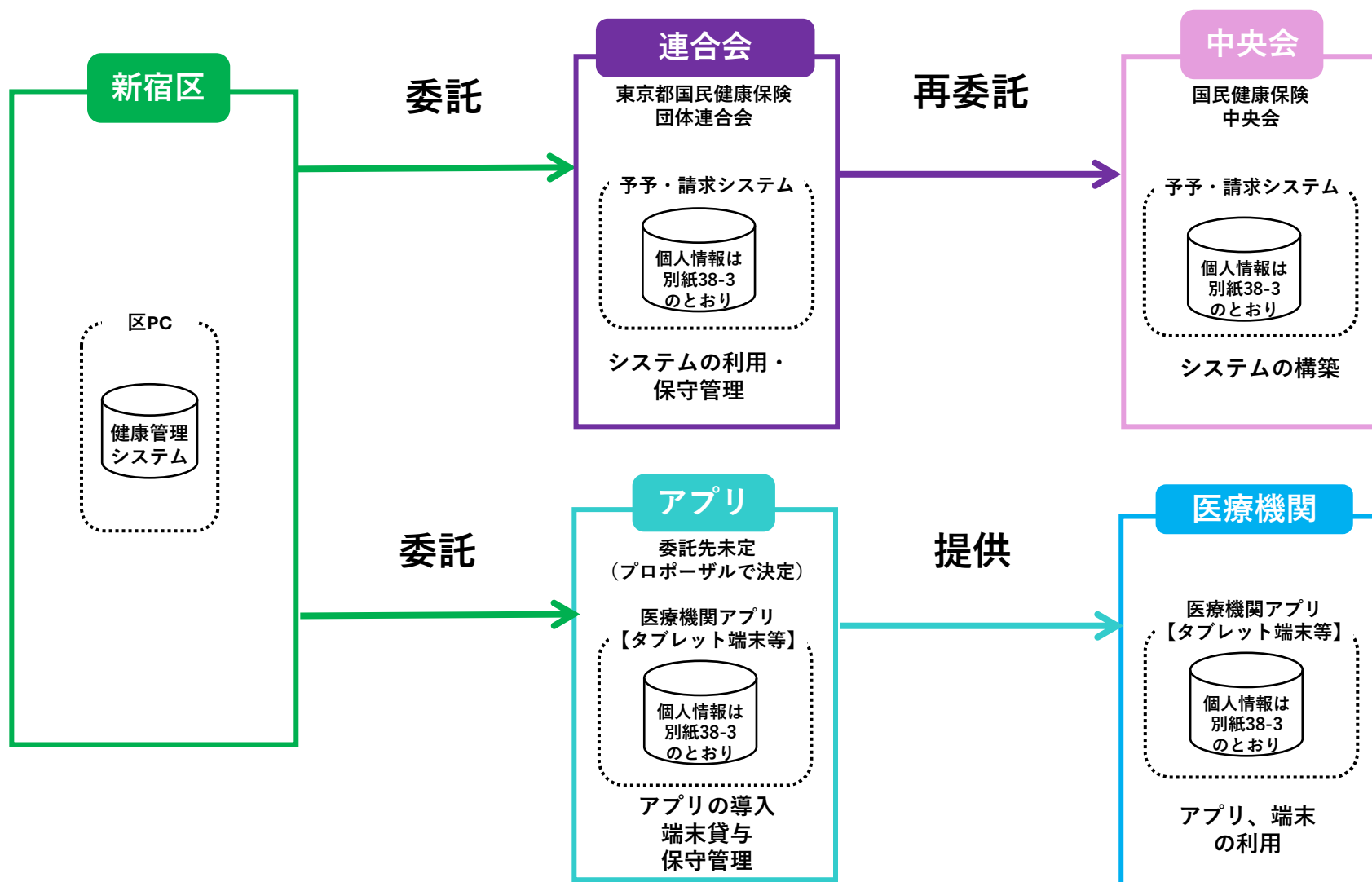
件名 予防接種に関する事務に係る医療機関アプリの業務委託について

保有課(担当課)	保健予防課
登録業務の名称	予防接種に関する事務
委託先	公募型プロポーザルにより委託事業者を決定する(プライバシーマーク等取得事業者を予定)
委託に伴い事業者処理させる情報項目(だれの、どのような項目か)	1 個人の範囲 予防接種法等関連法令に定められる予防接種の対象者 2 情報項目 資料38-3のとおり ※個人番号は取り扱わない。
処理させる情報項目の記録媒体	サーバ及び通信回線上の電磁的記録
委託理由	予防接種事務のデジタル化に伴い、医療機関においてマイナンバーカードによる本人確認を経て予診票情報の確認及び接種記録の入力を行うため、医療機関用アプリ等の提供及び運用保守を専門事業者に委託する必要があるため。
委託の内容	・医療機関用アプリ及び端末等の提供・運用保守 ・医療機関と予診情報・予防接種記録管理/請求支払システムとの間の情報連携機能の提供 ・利用者認証機能及び通信機能の運用管理 ・障害対応 ・情報セキュリティ対策の実施 なお、受託事業者は個人情報を閲覧、取得又は蓄積しない。
委託の開始時期及び期限	令和9年4月1日から令和10年3月31日まで(次年度以降も、同様の業務委託を行う。)
委託にあたり区が行う情報保護対策	別紙チェックリストのとおり
受託事業者に行わせる情報保護対策	別紙チェックリストのとおり





(参考) 業務委託の流れ



本スキームは国が指定したものであり、他自治体も同様の流れとなる

記録項目

【予診情報・予防接種記録管理／請求支払システム】

1 対象者情報の管理

個人番号、PMH キー、PMH 仮名識別子、基本 5 情報（氏名、カナ、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、予防接種対象者番号、接種対象者区分、減免区分。

2 ユーザー情報の管理

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 予診票情報の管理

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 予防接種記録情報の管理

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、接種対象者区分、減免区分。

【マイナポータル】

PMH 仮名識別子、電子証明書シリアル番号、予診票回答情報（項目 ID、回答内容、回答日時）、通知情報（通知 ID、通知種別、通知内容、通知日時）、接種記録閲覧情報、利用者同意情報（同意日時、同意状況）。

【オンライン資格確認等システム】

PMH キー、紐付番号、本人確認情報（氏名、生年月日、性別）、被保険者番号等情報、資格確認結果、認証日時、認証結果。

【医療機関アプリまたはサイト】

本人確認情報、予防接種対象者番号、医療機関コード、操作者 ID、予診票表示・入力情報（項目 ID、回答内容、入力日時）、接種記録入力情報（接種日、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、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）、処理結果、操作日時。

**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事務
特定個人情報保護評価書（全項目評価書）（素案）の概要**

I 基本情報

予防接種事務のデジタル化に伴う事務の内容、使用するシステム、特定個人情報ファイルを取り扱う理由等を記載しています。

1 事務の内容

予防接種事務のデジタル化に伴い、予診情報・予防接種記録管理／請求支払システムを活用し、区民によるマイナポータルからの予診票入力、医療機関による接種記録入力及び区による予防接種記録管理を行います。

2 使用システム

「予診情報・予防接種記録管理／請求支払システム」を中心に、予防接種事務に関する情報の管理及び情報連携を行います。

「健康管理システム」と連携し、予防接種対象者情報及び予防接種記録情報を管理します。

「マイナポータル」、「医療機関用アプリ」、「Public Medical Hub (PMH)」、「オンライン資格確認等システム」等と連携し、予診票情報及び接種記録等の情報連携を行います。

II 特定個人情報ファイルの概要

予防接種情報ファイルについて、次の事項を記載しています。

1 特定個人情報ファイル名

2 基本情報

対象となる人数・本人の範囲、記録される項目の内容等を記載しています。

※ 新宿区に住民登録又は居所がある予防接種対象者を対象とし、個人番号、基本情報、予診票情報、予防接種記録情報等を管理します。

3 入手・使用

特定個人情報の入手方法、使用目的等の情報を記載しています。

※ マイナポータル、医療機関用アプリ、PMH等を介して情報を入手し、予防接種対象者の把握及び予防接種記録の適正な管理に使用します。

4 委託

取扱いの委託内容、委託先、再委託の有無等の情報を記載しています。

※ 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ついて東京都国民健康保険団体連合会に委託し、一部業務を国保中央会へ再委託します。

5 提供・移転

6 保管・消去

特定個人情報の保管場所、保管期間及び消去方法等を記載しています。

III 取扱いプロセスにおけるリスク対策

予防接種情報ファイルを取り扱う際のリスク分析及びリスク軽減措置について、「入手」「使用」「取扱いの委託」「情報提供ネットワークシステムとの接続」「保管・消去」ごとに記載しています。

※ 利用者認証、アクセス制御、通信暗号化、ログ管理、委託先に対する監督等の措置により、特定個人情報の漏えい、不正利用等の防止を図ります。

Ⅳ その他のリスク対策

自己点検、監査、従事者に対する教育・啓発等について記載しています。

Ⅴ 開示請求、問合せ

特定個人情報の開示請求及び特定個人情報ファイルの取扱いに関する問合せ先について記載しています。

Ⅵ 評価実施手続

特定個人情報保護評価の実施に当たり行う住民意見聴取及び第三者点検等の手続について記載しています。

(素案)
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
	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事務 全項目評価書

個人のプライバシー等の権利利益の保護の宣言

新宿区は、予防接種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

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

項目一覧

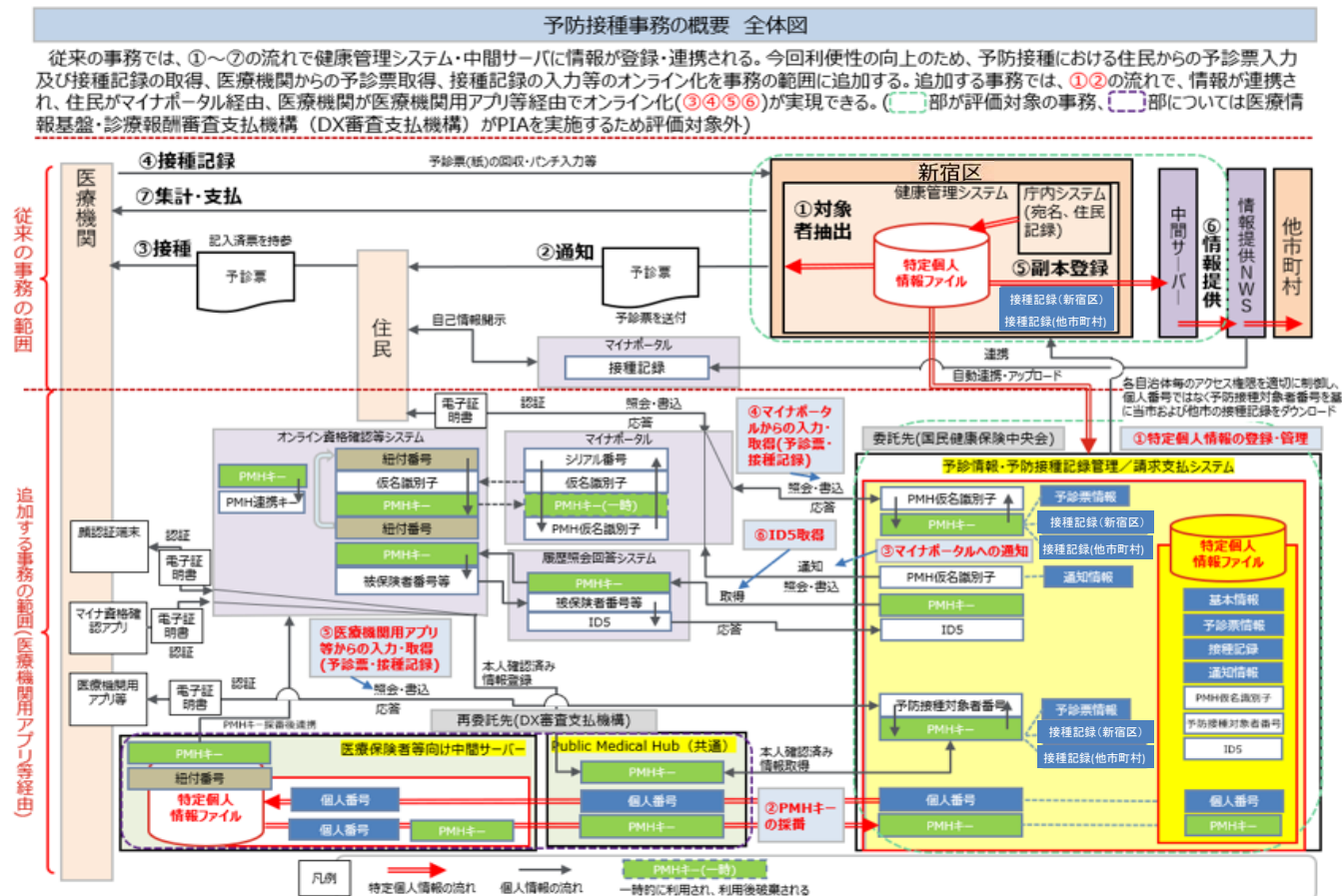
I 基本情報
(別添1) 事務の内容
II 特定個人情報ファイルの概要
(別添2) 特定個人情報ファイル記録項目
III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策
IV その他のリスク対策
V 開示請求、問合せ
VI 評価実施手続
(別添3) 変更箇所

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	予防接種事務のデジタル化
②事務の内容 ※	・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。 ・区民は、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。 ・区民が予防接種時に、マイナンバーカードを用いることにより、医療機関は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、区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区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	①予防接種関連データの登録機能 本区は、健康管理システムからの情報連携又は予診情報・予防接種記録管理／請求支払システム画面への直接入力により、予診票項目、接種勧奨における通知文言等の予防接種関連データを予診情報・予防接種記録管理／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を経由して医療情報基盤・診療報酬審査支払機構（以下、「DX審査支払機構」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（医療機関用アプリ等） ・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キーと紐づけて予診情報・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 ☐ 庁内連携システム	
	☐ 住民基本台帳ネットワークシステム ☐ 既存住民基本台帳システム	
	☐ 宛名システム等 ☐ 税務システム	
	☒ その他 (健康管理システム、マイナポータル、医療機関用アプリ、電子カルテ等、Public Medical Hub、履歴照会回答システム、オンライン資格確認等システム)	
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	行政手続における特定の個人を識別するための番号の利用等に関する法律第9条・第19条6号及び新宿区における個人番号の利用及び特定個人情報の提供に関する条例	
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 ☐ 実施しない	<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



(備考)

①特定個人情報登録・管理

- ・本区は、健康管理システムからの情報連携又は予診情報・予防接種記録管理／請求支払システム画面への直接入力により、予診情報・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の登録を行う。(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、健康管理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キ一採番

- ・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区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)

- ・区民は、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、接種時に区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 ＜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＞ ☐ その他 ・予防接種記録情報
その妥当性	・識別情報(その他識別情報) PMHキー、PMH仮名識別子、PMH連携キー、予防接種対象者番号、ID5…予診情報・予防接種記録管理／請求支払システムが、外部と情報連携するために必要となる。 ・業務関係情報(その他) 予防接種記録情報…予防接種事務の適切な実施にあたり必要となる情報を管理し、予診情報・予防接種記録管理／請求支払システムが、外部と情報連携するために必要となる。
全ての記録項目	(別添2)ファイル記録項目 を参照
⑤保有開始日	令和9年9月1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 () ☐ 行政機関・独立行政法人等 () ☐ 地方公共団体・地方独立行政法人 () ☐ 民間事業者 (医療機関) ☐ その他 (DX審査支払機構)	
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	・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。 ・国が予診情報・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、区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、区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	(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	・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	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 3) 50人以上100人未満 5) 500人以上1,000人未満 2) 10人以上50人未満 4) 100人以上500人未満 6) 1,000人以上

⑧使用方法	・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。
	情報の突合
	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 ※
⑨使用開始日	令和10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 ＜選択肢＞ 1) 委託する 2) 委託しない (2) 件
委託事項1	予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る各事務における特定個人情報ファイルの一部の取扱
①委託内容	予診情報・予防接種記録管理／請求支払システムの利用・情報連携業務及び運用保守業務
②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	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。

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 (LGWAN又は閉域網回線を用いた提供)
⑤委託先名の確認方法		下記、「⑥委託先名」の項の記載より確認できる。
⑥委託先名		東京都国保連合会
再委託	⑦再委託の有無	☐ 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	書面又は電磁的方法による承諾
	⑨再委託事項	・予診情報・予防接種記録管理／請求支払システムの運用保守 ・PMHキーの採番及びPMHキーを介した医療機関用アプリ等・マイナポータルへの情報連携 ※情報連携はPMHキーを介して行うため、特定個人情報を取り扱わない。
委託事項2～5		
委託事項2		保健情報(対人)システム(ガバメントクラウド上の標準準拠システムを含む)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、令和7年1月以降は専用回線での保守を予定)
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

⑥ 移転方法		☐ 庁内連携システム ☐ 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		
移転先2～5		
移転先6～10		
移転先11～15		
移転先16～20		
6. 特定個人情報の保管・消去		
① 保管場所		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。
② 保管期間	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		・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

(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)

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

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	・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	・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。 ・「生年月日等をチェックすることで紐付け誤りを防止する機能（以下、「紐付け誤り防止機能」という。）により、誤った情報が紐付けられるリスクを低減する。	
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	—	
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	・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。 ・紐付け誤り防止機能により、誤った情報が紐付けられるリスクを低減する。	
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： 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	・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は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。 ・紐付け誤り防止機能により、誤った情報が紐付けられるリスクを低減する。	
個人番号の真正性確認の措置の内容	・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。 ・紐付け誤り防止機能により、誤った情報が紐付けられるリスクを低減する。	
特定個人情報の正確性確保の措置の内容	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漏えい・紛失するリスク		
リスクに対する措置の内容	・予診情報・予防接種記録管理／請求支払システムとDX審査支払機構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。 ・健康管理システムは、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		
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な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	・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区民から予診情報・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		
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	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	・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	・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	・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		・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。
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		・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		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	・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	・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(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(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。				

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 3) 課題が残されている	2) 十分である
リスク2: 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容	＜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 3) 課題が残されている	2) 十分である
リスク3: 入手した特定個人情報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 3) 課題が残されている	2) 十分である

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	＜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(対人)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、中間サーバに格納したうえで照会許可照会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(対人)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(対人)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	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	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LGWAN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	・データセンタ内のサーバで管理しており、生存者の個人番号と同様の方法にて安全管理措置を実施している。	
その他の措置の内容			
リスクへの対策は十分か		[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2: 特定個人情報が古い情報のまま保管され続けるリスク			
リスクに対する措置の内容		・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		[]	<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	・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		[]	<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	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	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	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		
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	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。 保有個人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)の提示または提出が必要です。
特記事項	代理人による請求については、代理関係を確認するため、戸籍謄本、登記事項証明書、委任状等の書類を提示又は提出が必要です。
③手数料等	[無料] <選択肢> (手数料額、納付方法: 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	
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う。
②実施日・期間	
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	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	
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	

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。 保有個人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)の提示または提出が必要です。
特記事項	代理人による請求については、代理関係を確認するため、戸籍謄本、登記事項証明書、委任状等の書類を提示又は提出が必要。
③手数料等	[無料] <選択肢> 1) 有料 2) 無料 (手数料額、納付方法:)
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	「1. ①請求先」と同じ
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	
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う。
②実施日・期間	
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	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	
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

[illegible]

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

3 電算処理にかかる個人情報保護対策チェックリスト

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
開発等を委託する場合 における区が行う 情報保護対策 【運用上の対策】	○	個人情報保護法及び新宿区情報セキュリティポリシーを遵守するよう指導する。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠するよう指導する。
	○	必要に応じて、事業者への立入り調査等を実施するとともに、結合先に対し速やかに状況報告をするよう指導する。
	○	システム上で不要となった電子データを削除し、電子データの消去を行ったことの報告書を提出するよう指導する。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備し、結合先と緊急時の連絡体制や対応手順を確認する。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに結合先と今後の対応を協議する。
	○	区のシステム機器設置場所へ委託先が入退室する場合は、管理（申請、承認、記録）を行う。また、委託先がシステム機器を操作する場合には、事前に作業内容の報告を求め、区が承認した後に実施するよう指導するとともに、個人情報データの持出しを禁止する。
	○	プログラムの移行等を行う場合は、外部記録媒体の管理を行い、利用時は第三者漏えいがないようパスワードを施す等、利用制限を設ける。
	○	入力及び取込みテストにおいては、ダミーデータを使うよう指導する。
	○	実データを使用した検証作業は、区職員が実施する（委託先には、必要な支援のみ行わせる）。
	○	モバイルパソコン等の電子計算組織を持込む場合は、事前に区の許可をとらせ、用途は、社内事務連絡、設計書等の閲覧に限定させる。また、委託先のモバイルパソコン等と区のネットワーク、システム機器及びUSB等の記録媒体と接続をさせないように、区の職員が立ち会う。
開発等を委託する場合 における区が行う 情報保護対策 【システム上の対策】	○	データ項目定義の修正漏れによるシステム不具合等が無いよう、双方で事前に綿密なスケジュール計画やチェックシートを作成して実施する。なお、稼働にあたっては必ず仮移行を行うこととし、本稼働はシステムを使用していない時間帯（時間外・休日）に実施し、十分な検証を行う。
	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定する。
	○	通信内容は暗号化し、通信途上の個人情報の盗用、改ざん、成りすましを防止する。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御する。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用する。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止する。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定するとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底する。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得する。取得したログは、定期的に分析する。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備する。
	○	入退室管理等により情報資産の危殆化を防止する。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にする。

3 電算処理にかかる個人情報保護対策チェックリスト

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
開発等を委託する場合における委託先に行わせる情報保護対策 【運用上の対策】	○	個人情報保護法及び新宿区情報セキュリティポリシーを遵守させる。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠させる。
	○	必要に応じて、事業者への立入り調査等を受けさせるとともに、結合先に対し速やかに状況報告をさせる。
	○	システム上で不要となった電子データを削除させ、電子データの消去を行ったことの報告書を提出させる。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備させ、区と緊急時の連絡体制や対応手順を確認させる。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに区と今後の対応を協議させる。
	○	区のシステム機器設置場所へ委託先が入退室する場合は、区の管理（申請、承認、記録）に従わせる。また、委託先がシステム機器を操作する場合には、事前に作業内容の報告をさせ、区が承認した後に実施させるとともに、個人情報データの持出しを禁止させる。
	○	プログラムの移行等を行う場合は、外部記録媒体の管理を行い、利用時は第三者漏えいがないようパスワードを施す等、利用制限を設ける。
	○	入力及び取込みテストにおいては、ダミーデータを使わせる。
	○	実データを使用した検証作業は、区職員が実施する（委託先には、必要な支援のみ行わせる）。
	○	モバイルパソコン等の電子計算組織を持込む場合は、事前に区の許可をとらせ、用途は、社内事務連絡、設計書等の閲覧に限定させる。また、委託先のモバイルパソコン等と区のネットワーク、システム機器及びUSB等の記録媒体と接続をさせないように、区の職員の立会いに応じさせる。
開発等を委託する場合における委託先に行わせる情報保護対策 【システム上の対策】	○	データ項目定義の修正漏れによるシステム不具合等が無いよう、双方で事前に綿密なスケジュール計画やチェックシートを作成して実施する。なお、稼働にあたっては必ず仮移行を行うこととし、本稼働はシステムを使用していない時間帯（時間外・休日）に実施させ、十分な検証を行わせる。
	○	接続するネットワークについては、特定相手以外との通信を不可とさせる。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定させる。
	○	通信内容は暗号化させ、通信途上の個人情報の盗用、改ざん、成りすましを防止させる。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じさせ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御させる。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用させる。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止させる。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定させるとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底させる。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得させる。取得したログは、定期的に分析させる。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備させる。
	○	入退室管理等により情報資産の危殆化を防止させる。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にさせる。

4 外部結合にかかる個人情報保護対策チェックリスト

	・対策が可能であれば「○」 ・対策の必要がない場合は「－」	情報保護対策
区が行う情報保護対策 【運用上の対策】	○	個人情報保護法及び新宿区情報セキュリティポリシーを遵守するよう指導する。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠するよう指導する。
	○	必要に応じて、事業者への立入り調査等を実施するとともに、結合先に対し速やかに状況報告をするよう指導する。
	○	システム上で不要となった電子データを削除し、電子データの消去を行ったことの報告書を提出するよう指導する。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備し、結合先と緊急時の連絡体制や対応手順を確認する。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに結合先と今後の対応を協議する。
区が行う情報保護対策 【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定する。
	○	通信内容は暗号化し、通信途上の個人情報の盗用、改ざん、成りすましを防止する。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御する。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用する。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止する。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定するとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底する。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得する。取得したログは、定期的に分析する。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備する。
	○	入退室管理等により情報資産の危殆化を防止する。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にする。

4 外部結合にかかる個人情報保護対策チェックリスト

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
結合先に行わせる 情報保護対策 【運用上の対策】	○	個人情報保護法及び新宿区情報セキュリティポリシーを遵守させる。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠させる。
	○	必要に応じて、事業者への立入り調査等を受けさせるとともに、結合先に対し速やかに状況報告をさせる。
	○	システム上で不要となった電子データを削除させ、電子データの消去を行ったことの報告書を提出させる。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備させ、区と緊急時の連絡体制や対応手順を確認させる。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに区と今後の対応を協議させる。
結合先に行わせる 情報保護対策 【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とさせる。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定させる。
	○	通信内容は暗号化させ、通信途上の個人情報の盗用、改ざん、成りすましを防止させる。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じさせ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御させる。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用させる。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止させる。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定させるとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底させる。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得させる。取得したログは、定期的に分析させる。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備させる。
	○	入退室管理等により情報資産の危殆化を防止させる。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にさせる。

5 業務委託にかかる個人情報保護対策チェックリスト

(電磁的媒体・紙媒体の取扱い)

	・対策が可能であれば「○」 ・対策の必要がない場合は「－」	情報保護対策
委託にあたり区が行う 情報保護対策 【運用上の対策】	○	契約にあたり、「特記事項」を付すとともに、個人情報保護法及び新宿区情報セキュリティポリシーを遵守するよう指導する。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠するよう指導する。
	○	契約履行の間、特記事項に基づき立入り調査等を実施するとともに、委託先に対し速やかに状況報告をするよう指導する。
	○	再委託先がある場合には、委託先との間に立入り調査等ができる契約内容を付すとともに、必要に応じて又は定期的に立入り調査等を実施するよう指導する。
	○	取扱責任者及び取扱者をあらかじめ指定し、区に報告するよう指導する。
	○	全体の業務フローを作成し、委託先と共有する。
	○	取扱う個人情報の管理について、必要に応じて又は定期的に確認する体制を構築するよう指導する。
	○	個人情報を含むデータを作成する必要がある場合は、パスワードを付してデータを暗号化する。また、電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用して、手渡しで行うよう指導する。
	－ (電子データのみ の取扱いのため)	個人情報を手交する場合は、鍵付きカバン等を使用して運搬する。
	－ (電子データのみ の取扱いのため)	個人情報の受渡しにあたっては、管理簿に記載する。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにする。
	－ (電子データのみ の取扱いのため)	個人情報は、施錠できる金庫又はキャビネット等に保管する。
	○	業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却し、電子データは消去するよう指導する。また、区に電子データの消去を行ったことの報告書を提出するよう指導する。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備し、委託先と緊急時の連絡体制や対応手順を確認する。
委託にあたり区が行う 情報保護対策 【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定する。
	○	通信内容は暗号化し、通信途上の個人情報の盗用、改ざん、成りすましを防止する。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御する。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用する。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止する。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定するとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底する。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得する。取得したログは、定期的に分析する。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備する。
	○	入退室管理等により情報資産の危殆化を防止する。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にする。

5 業務委託にかかる個人情報保護対策チェックリスト

(電磁的媒体・紙媒体の取扱い)

	・対策が可能であれば「○」 ・対策の必要がない場合は「－」	情報保護対策
委託事業者に行わせる 情報保護対策 【運用上の対策】	○	契約にあたり、「特記事項」を付すとともに、個人情報保護法及び新宿区情報セキュリティポリシーを遵守させる。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠させる。
	○	契約履行の間、特記事項に基づき立入り調査等を受けさせるとともに、委託先に対し速やかに状況報告をさせる。
	○	再委託先がある場合には、委託先との間に立入り調査等ができる契約内容を付すとともに、必要に応じて又は定期的に立入り調査等を実施させる。
	○	取扱責任者及び取扱者をあらかじめ指定させ、区に報告させる。
	○	区が作成した業務フローに基づき、業務を行わせる。
	○	取扱う個人情報の管理について、必要に応じて又は定期的に確認する体制を構築させる。
	○	個人情報を含むデータを作成する必要がある場合は、パスワードを付してデータを暗号化させる。電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用させ、手渡しで行わせる。
	－ (電子データのみ の取扱いのため)	個人情報を手交する場合は、鍵付きカバン等を使用して運搬させる。
	－ (電子データのみ の取扱いのため)	個人情報の受け渡しにあたっては、管理簿に記載させる。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにさせる。
	－ (電子データのみ の取扱いのため)	個人情報は、施錠できる金庫又はキャビネット等に保管させる。
	○	業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却させ、電子データは消去させる。また、区に電子データの消去を行ったことの報告書を提出させる。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備させ、区と緊急時の連絡体制や対応手順を確認させる。
委託事業者に行わせる 情報保護対策 【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定させる。
	○	通信内容は暗号化させ、通信途上の個人情報の盗用、改ざん、成りすましを防止させる。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じさせ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御させる。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用させる。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止させる。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定させるとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底させる。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得させる。取得したログは、定期的に分析させる。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備させる。
	○	入退室管理等により情報資産の危殆化を防止させる。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にさせる。