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
38	予防接種法による予防接種の実施に関する事務　全項目評価書

個人のプライバシー等の権利利益の保護の宣言	
横浜市は、予防接種法による予防接種の実施に関する事務における特定個人情報ファイルの取扱いにあたり、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを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
横浜市長

個人情報保護委員会　承認日　【行政機関等のみ】
公表日
令和1年11月26日

［平成30年５月　様式4］

項目一覧

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	予防接種法による予防接種の実施に関する事務
②事務の内容　※	対象者への接種勧奨、予防接種の実費徴収、医療機関での予防接種の実施、医療機関への接種委託料の支払い、接種記録の管理・保管、及び予防接種による健康被害救済給付に関する事務を行う。 【予防接種事務について】 ・予防接種対象者はA類(こども)とB類(高齢者)に区別され、それぞれ予防接種法に定める接種年齢がある。 ・A類(こども)の接種費用は全額公費である。接種費用の実費徴収及び減免は、B類(高齢者)のみである。 ・健康被害救済給付に係る事務は紙の書類で行い、データのファイルでの保存はしない。 なお、特定個人情報は次の事務に利用している。 〇情報提供ネットワークシステム(中間サーバー)を使用した情報照会事務 当該事務を行うにあたって必要となる情報を入手するため、行政手続における特定の個人を識別するための番号の利用等に関する法律(以下、「番号法」という。)第9条及び第19条で定める範囲において、他情報保有機関に対して照会を行う。 〇情報提供ネットワークシステム(中間サーバー)を使用した情報提供事務 番号法第22条による特定個人情報の提供に備え、内閣官房の定めたデータ標準項目について、統合番号連携システムを使用し、中間サーバーにアップロードを行う。 〇予防接種歴を業務固有番号を利用して管理する。
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	予防接種台帳システム
②システムの機能	1　対象者管理機能 業務固有番号を含む、住所、氏名等の情報を管理する機能。接種勧奨を行うための対象者を抽出する機能。 2　接種履歴管理機能 対象者の接種した予防接種情報を管理・保管する機能。 3　接種歴照会機能 過去の接種歴照会や、予診票の再発行を行う機能。 4　集計・統計機能 予防接種情報を集計し、国や県への事業報告書を作成する機能。 5　副本作成機能 中間サーバーに登録する副本を作成する機能。
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　[〇] 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2～5	
システム2	
①システムの名称	統合番号連携システム
②システムの機能	統合番号連携システムは、中間サーバー、既存業務システム等と連携し、特定個人情報の照会及び提供等の業務を実現する。 統合番号とは、本市において一意に個人を特定する団体内統合宛名番号のことをいう。 (1) 統合番号管理機能 統合番号・個人番号・業務固有番号・4情報（住所、氏名、性別、生年月日）を紐づけて管理する機能。 (2) 符号管理機能 符号取得要求を中間サーバーに対して行う機能。 (3) 情報照会側機能 特定個人情報の照会業務を行うための機能。 (4) 情報提供側機能 特定個人情報の提供業務を行うための機能。 (5) 中間サーバー稼働状況確認機能 連携する中間サーバーの稼働状況を確認する機能。 (6) 個人番号・統合番号変換機能 個人番号を保有しない既存業務システムのために必要となる番号変換機能。 (7) データ連携機能 既存業務システムと中間サーバー間のデータ連携機能。 (8) データ変換機能 文字コード及びファイルフォーマットを変換する機能。 (9) 職員認証・権限管理機能 統合番号連携システムの利用者を認証し、権限を管理する機能。
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　（ 中間サーバー、既存業務システム　）

システム3	
①システムの名称	中間サーバー
②システムの機能	中間サーバーは、情報提供ネットワークシステム（インターフェイスシステム）、既存システム、統合番号連携システム等の各システムとデータの受け渡しを行うことで、符号の取得や各情報保有機関で保有する特定個人情報の照会、及び各情報保有機関への情報提供等の業務を実現する。 (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「統合番号」とを紐付け、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)の情報照会及び情報提供受領（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及び当該特定個人情報(連携対象)の提供を行う機能。 (4) 既存システム接続機能 　中間サーバーと既存システム、統合番号連携システム及び住基システムとの間で情報照会内容、情報提供内容、特定個人情報（連携対象）、符号取得のための情報等について連携するための機能。 (5) 情報提供等記録管理機能 　特定個人情報(連携対象)の照会、又は提供があった旨の情報提供等記録を生成し、管理する機能。 (6) 情報提供データベース管理機能 　特定個人情報（連携対象）を副本として、保持・管理する機能。 (7) データ送受信機能 　中間サーバーと情報提供ネットワークシステム（インターフェイスシステム）との間で情報照会、情報提供、符号取得のための情報等について連携するための機能。 (8) セキュリティ管理機能 　中間サーバーの「システム方式設計書」の記載に沿って、対応予定。 (9) 職員認証・権限管理機能 　中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報(連携対象)へのアクセス制御を行う機能。 (10) システム管理機能 　バッチの状況管理、業務統計情報の集計、稼動状態の通知、保管期限切れ情報の削除を行う機能。
③他のシステムとの接続	[○] 情報提供ネットワークシステム　　[　　] 庁内連携システム [　　] 住民基本台帳ネットワークシステム　　[○] 既存住民基本台帳システム [○] 宛名システム等　　[　　] 税務システム [　　] その他　（　　）

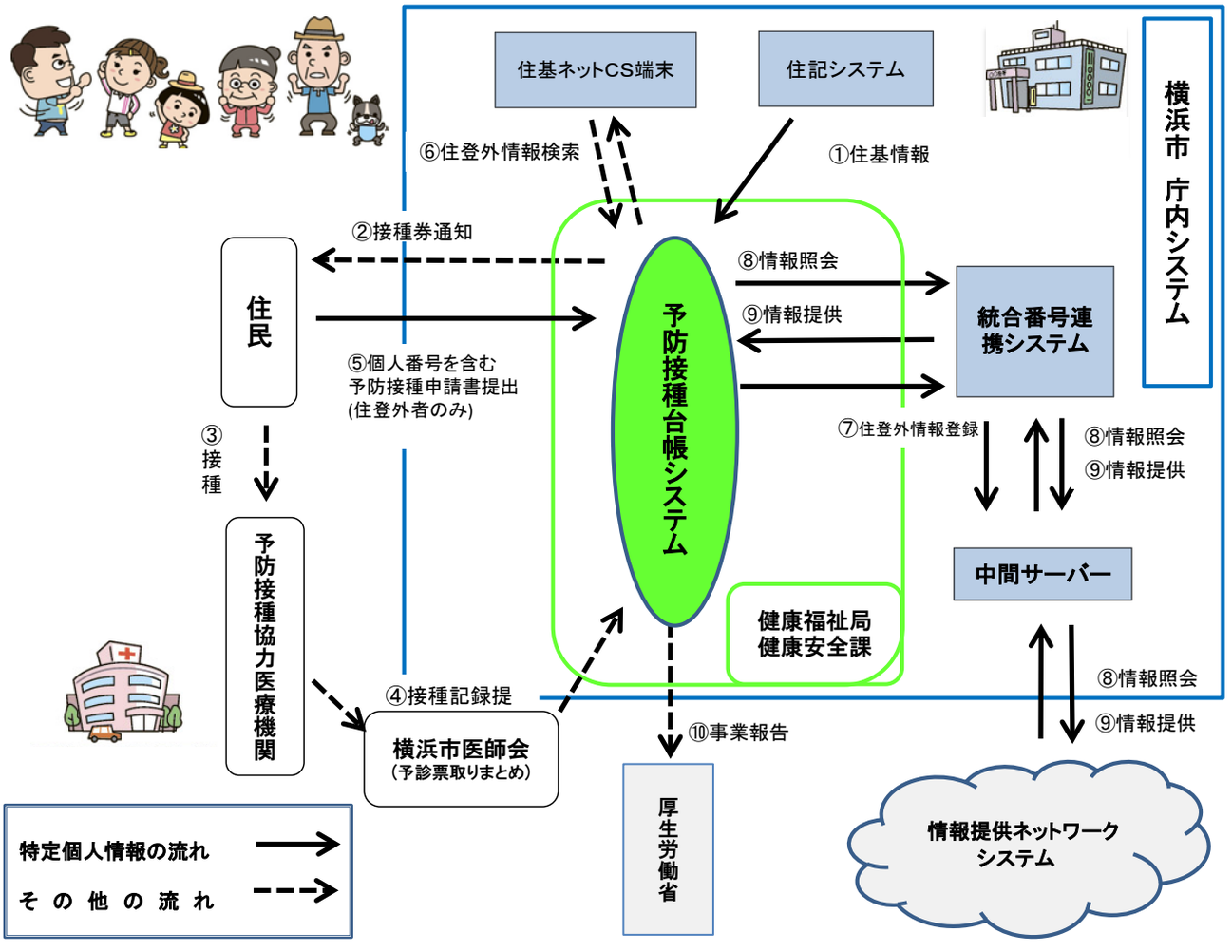
システム4	
①システムの名称	住民基本台帳ネットワークシステム
②システムの機能	(1) 本人確認情報検索 　統合端末において入力された4情報（氏名、住所、性別、生年月日）の組合せをキーに本人確認情報の検索を行い、検索条件に該当する本人確認情報の一覧を画面上に表示する。 (2) 機構への情報照会 　全国サーバーに対して個人番号又は4情報の組合せをキーとした本人確認情報照会要求を行い、該当する個人の本人確認情報を受領する。 当該事務においては、住民基本台帳ネットワークシステムの機能のうち、上記機能のみ使用する。
③他のシステムとの接続	[　　] 情報提供ネットワークシステム　　[　　] 庁内連携システム [　　] 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　（　　）

システム5	
①システムの名称	福祉保健システム
②システムの機能	福祉保健システムは、住民記録情報等を活用し、総合的な福祉データベースを構築し、申請・決定・費用徴収等の事務の簡素化・迅速化を図り、福祉サービス利用にかかる総合的な情報を管理する。 福祉保健システムにおいては、個人番号、統合番号の保有はせず、統合番号連携システムと連携し、情報の提供・照会を行う。なお、アクセス制限により統合番号の閲覧・利用は不可能となる。 予防接種法による予防接種の実施に関する事務においては、接種対象者の接種費用の減免確認事務を行うため、福祉保健システム内の下記機能のみを使用する。 (1) 接種対象者を含む世帯員情報検索 福祉保健システム端末において入力された4情報(氏名、住所、性別、生年月日)の組み合わせをキーに、接種対象者を含む世帯員情報の検索を行い、検索条件に該当する情報の一覧を画面上に表示する。 (2) 接種対象者を含む世帯員の課税・非課税情報検索 （1）で特定した対象者につき、課税・非課税情報の検索を行い、検索条件に該当する情報の一覧を画面上に表示する。
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　（　）
システム6～10	
システム6	
①システムの名称	情報共有基盤システム
②システムの機能	情報共有基盤システムは、既存住民基本台帳システム、税務システム等と連携し、情報共有基盤システム上に構築された業務システム（以下「基盤関連システム」という。）が利用する住民情報の一元管理を実現する。 (1)統合データベース機能 基盤関連システムが利用する住民情報を保管及び提供する機能。 (2)データ連携機能 住民記録システム、新税務システム等と連携する機能。 (3)データ変換機能 文字コード及びファイルフォーマットを変換する機能。 (4)個人認証機能 基盤関連システムの利用者を認証し、権限を管理する機能。 (5)システム管理機能 情報共有基盤システム及び基盤関連システムにおけるバッチの状況管理、サーバーの死活監視等を行う機能。
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　（ 基盤関連システム　）
システム11～15	
システム16～20	

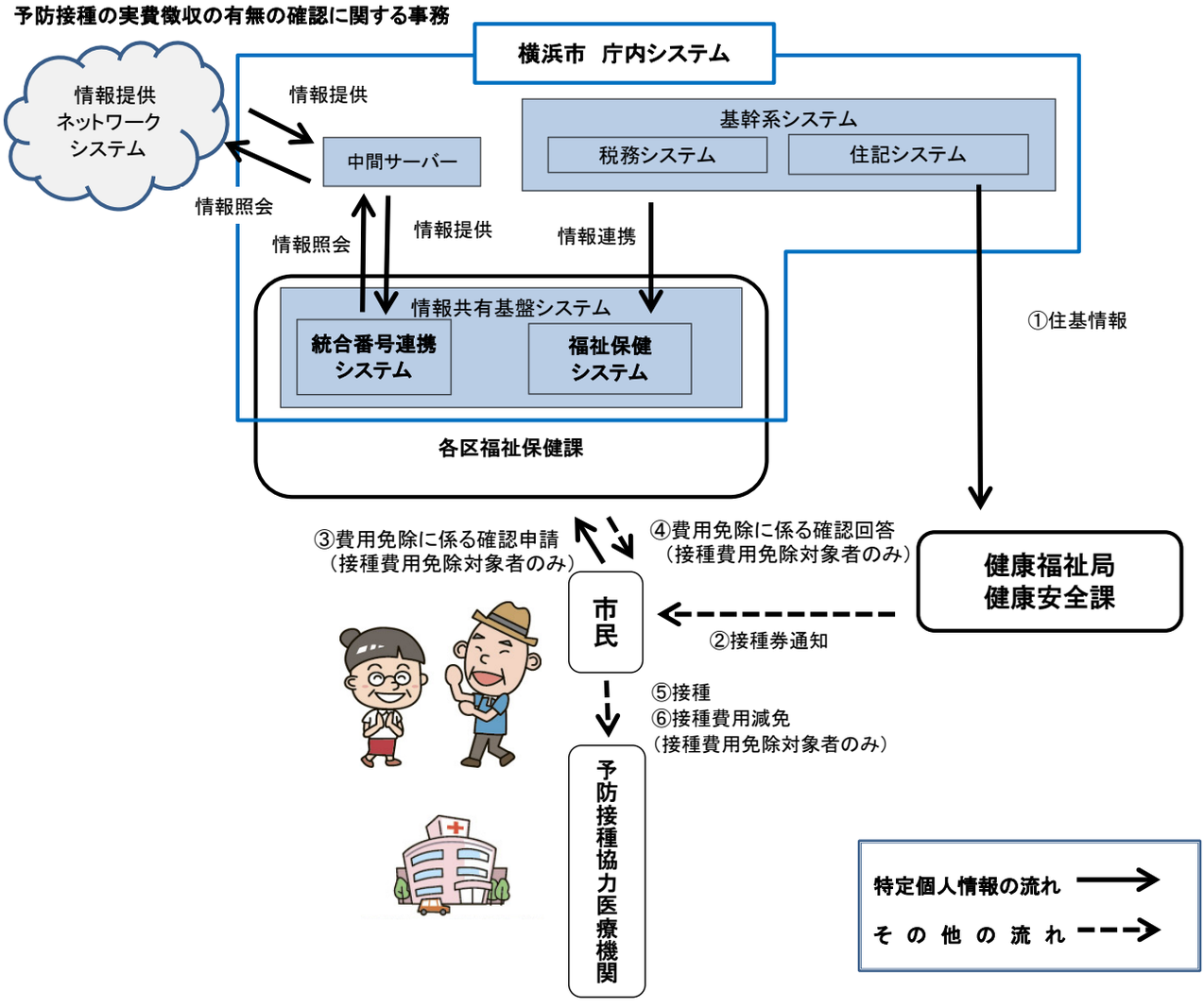
3. 特定個人情報ファイル名	
(1) 予防接種対象者関係情報ファイル (2) 統合番号連携ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	当該事務において、以下のファイルを下記の目的遂行のため取り扱う。 (1) 予防接種対象者関係情報ファイル ・予防接種の対象者・予防接種の実施記録等の情報の正確な把握かつ適正な管理を行う。 (2) 統合番号連携ファイル ・個人の特定を正確かつ効率的に行う。 ・番号法第19条第7号及び第8号に基づき、情報提供ネットワークシステムを通じた情報照会、情報提供業務を行う。
②実現が期待されるメリット	(1)予防接種対象者関係情報ファイル ・予防接種の対象者であることを確認し、対象者と受けた接種記録を紐づけることで、接種記録の管理・保管等について効率的な事務が可能となる。 ・対象者の接種歴を管理することで、未接種者を迅速に把握でき、感染症の発生及びまん延防止のために確保すべき一定の予防接種率となるよう接種率向上の取り組みを強化できる。 (2) 統合番号連携ファイル ・統合番号・個人番号・業務固有番号・4情報を紐づけて管理することにより、個人を特定する際の正確性が向上すること、また、事務の効率化に資することが期待できる。 ・住民票の写し等に代えて本人確認情報を利用することにより、これまでに窓口で提出が求められていた行政機関が発行する添付書類(住民票の写し等)の省略が図られ、もって国民・住民の負担軽減(各機関を訪問し、証明書等を入手する金銭的、時間的コストの節約)につながることが見込まれる。 ・個人番号を保有するファイルを局所化し、漏洩リスクを低減できる。
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 10項 ・行政手続における特定の個人を識別するための番号の利用等に関する法律別表第1の主務省令で定める事務を定める命令第10条
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[実施する] <選択肢> 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	【情報提供】 番号法第19条第7号 別表第2 16の2項 行政手続における特定の個人を識別するための番号の利用等に関する法律別表第2の主務省令で定める事務及び情報を定める命令 第12条の2 【情報照会】 番号法第19条第7号 別表第2 16の2項、17項、18項、19項 行政手続における特定の個人を識別するための番号の利用等に関する法律別表第2の主務省令で定める事務及び情報を定める命令 第12条の2、第12条の3、第13条、第13条の2
7. 評価実施機関における担当部署	
①部署	健康福祉局健康安全部健康安全課
②所属長の役職名	健康福祉局健康安全部健康安全課長
8. 他の評価実施機関	
―	

（別添1）事務の内容

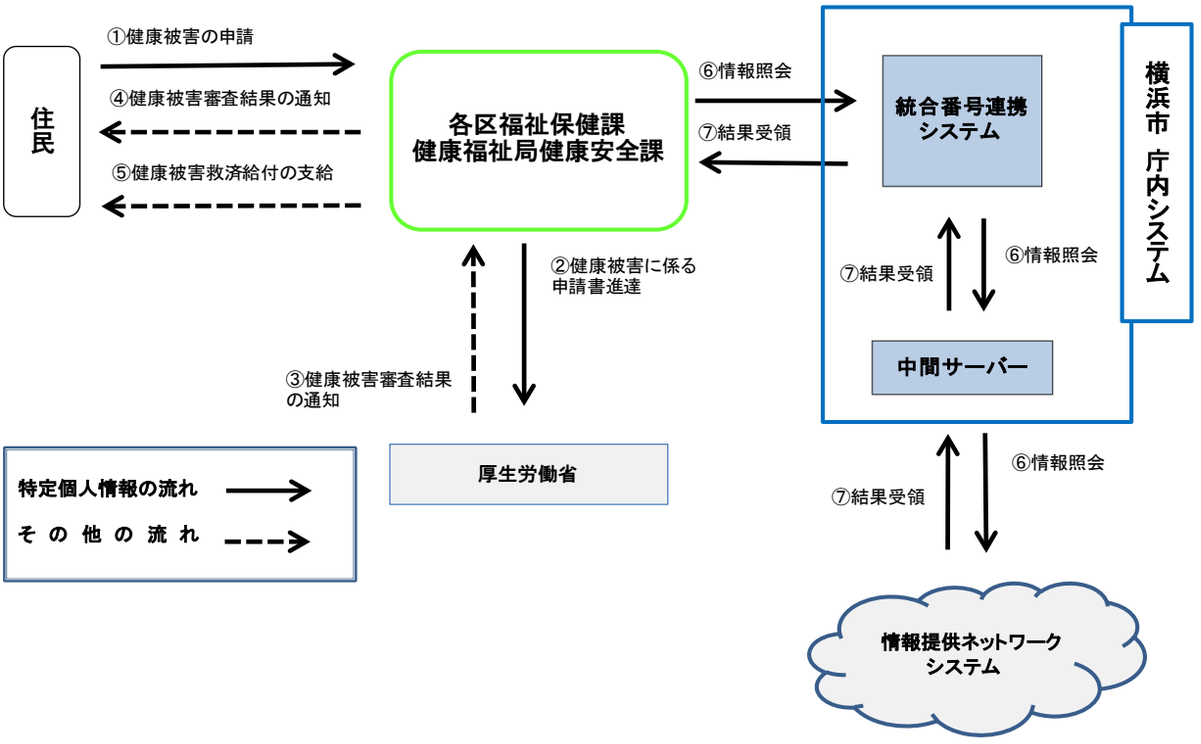
予防接種対象者への接種勧奨、接種記録の管理・保管に関する事務



予防接種の実費徴収の有無の確認に関する事務



予防接種健康被害救済給付に関する事務



（備考）

〇予防接種対象者への接種勧奨、接種記録の管理・保管に関する事務
① 予防接種対象者と判断するために必要な情報を住民記録システムから取得
② 住民記録システムより取得した情報から、接種対応年齢等を抽出し、接種対象者へ接種券(予診票)を通知
③ 接種対象者が予防接種協力医療機関へ受診
④ 予診票に記載されている接種記録を医師会経由で医療機関から取得し、接種歴を予防接種台帳システムに登録
⑤ 特別な事情等で、横浜市内に住民票がない対象者(住登外者)から、マイナンバーを含む予防接種申請書を受領
⑥ 住登外者の情報を住基ネットCS端末を利用して検索
⑦ 登録がない住登外者のデータを、統合番号連携システムに番号を登録し、中間サーバーへ副本登録
⑧ 予防接種履歴を統合番号連携システム経由で中間サーバーへ副本提供
⑨ 他市町村が保有する予防接種歴情報を、統合番号連携システム経由で中間サーバーへ照会
⑩ 接種記録統計を厚生労働省へ報告

〇予防接種の実費徴収の有無の確認に関する事務
① 予防接種対象者と判断するために必要な情報を住民基本台帳システムから取得
② 接種対象者へ接種券(予診票)を通知
③ 免除確認資料が無い上で、接種費用免除を希望する場合、各区・健康安全課の予防接種窓口にて免除の可否確認を申請
④ 情報共有基盤システム・税務システムが保有する世帯員情報と税情報を、福祉保健システム経由で確認し、免除の可否を回答
当年1月1日時点で本市に課税台帳が存在しない場合、他市町村が保有する本人及び世帯員の税情報を、統合番号連携システム経由で中間サーバへ照会し、免除の可否を回答
⑤ 接種対象者が予防接種協力医療機関を受診
⑥ 免除確認資料を医療機関が確認し、対象の場合は接種費用減免

〇予防接種健康被害救済給付に関する事務
① 予防接種健康被害救済給付に係る申請を受理する
② 横浜市予防接種事故対策調査会にて申請書類の内容を協議後、紙の申請用紙で厚生労働省あて送付する
③ 厚生労働省所管の審査会において審議が行われ、厚生労働省からの審査結果を紙で受理する
④ 申請者へ厚生労働省の審査結果を通知する
⑤ 厚生労働省から健康被害が認定された場合は健康被害救済給付の支給を行う
⑥・⑦ 1度で給付が終了せず、健康被害が長期化した対象者への毎年の給付額を決定するため、他の行政機関が保有する情報を統合番号連携システム経由で中間サーバーへ照会する

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		
予防接種対象者関係情報ファイル		
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		[　100万人以上1,000万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※		予防接種法に基づく予防接種の対象者
	その必要性	予防接種法に基づく定期予防接種対象者であることの管理、対象者の接種記録を適正に管理・保管するために必要。
④記録される項目		[　　10項目以上50項目未満　　] ＜選択肢＞ 1）10項目未満　　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目 ※	・識別情報 [　] 個人番号　　[　] 個人番号対応符号　　[○] その他識別情報（内部番号） ・連絡先等情報 [○] 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	○健康・医療関係情報 ・予防接種履歴の管理、及び勧奨を適正に行うために必要 ○その他識別情報 ・対象者を特定するため、本人確認措置を適正に行うために必要 ○連絡先等情報 ・4情報：予防接種法に基づく対象者であることを確認するために必要 ・その他住民票関係情報：予防接種対象者であることを確認し、接種履歴を入力・管理するために必要
	全ての記録項目	別添2を参照。
⑤保有開始日		平成28年４月１日
⑥事務担当部署		健康福祉局健康安全課

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 （ 市民局窓口サービス課 ） [ ] 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 （ ） [ ] 民間事業者 （ ） [○] その他 （ 医療機関 ）
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 （ ）
③入手の時期・頻度		◎住民登録内の者の分 住民基本台帳システムから、1日1回、システム間の連携により自動的に入手する。予診票の接種記録については、接種を行った医療機関から月次単位で入手する。 ◎住民登録外の者の分 ○本人または本人の代理人からの紙書類による入手。 ・横浜市内に住民票がない対象者(住登外者)から、個人番号を含む予防接種申請書を受領。 ○医療機関からの入手 ・予診票の接種記録については、接種を行った医療機関から月次単位で入手する。
④入手に係る妥当性		・個人を特定し、適正に予防接種情報を管理する必要がある。
⑤本人への明示		・本人または本人の代理人から特定個人情報の提供を受ける場合は、当該事務が番号法第9条別表1第10項で定める個人番号利用事務であること及び個人番号の利用目的を説明する。 ・個人番号及び4情報は住民基本台帳法で定義する本人確認情報であり、整備法第19条の定めにより改正される住民基本台帳法の別表第三の5の5の項、及び別表第五の6の3の項において、当該事務で本人確認情報を使用して良い旨が明示されている。 ・書面提出などによる入手のため本人または本人の代理人に直接説明できない場合にあっても、本人確認情報の使用については上記のとおり明示されている。
⑥使用目的 ※		対象者の資格管理、接種記録の管理・保管に係る事務を適正かつ公正に行うため
	変更の妥当性	
⑦使用の主体	使用部署 ※	健康福祉局健康安全課
	使用者数	[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
⑧使用方法 ※		・接種記録の管理・保管 予防接種台帳システムに接種記録を登録し、接種記録の管理及び保管を行う。
	情報の突合 ※	予診票に記入された住所、氏名、生年月日等と突合し、接種対象者かどうか確認する。
	情報の統計分析 ※	―
	権利利益に影響を与え得る決定 ※	―
⑨使用開始日		平成28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 （ 3 ） 件
委託事項1		予防接種台帳システムの運用・保守
①委託内容		予防接種台帳システムの管理及び保守点検、並びに改修作業等 ファイルのバックアップ作業、データの更新作業、及び保守点検作業などの運用業務を行うにあたり、民間事業者に委託することにより専門的な知識を有する人員を確保し、当該事業を安定的に運用することが可能となる。
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	[100万人以上1,000万人未満] ＜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 ※	予防接種法に基づく予防接種の対象者
	その妥当性	全ての接種対象者の情報を管理しているため、上記の範囲を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 （ サーバー室内におけるシステムの直接操作 ）
⑤委託先名の確認方法		市報での公告又は本市webページでの公表による。 ただし、公表を要しない契約の場合は、横浜市の保有する情報の公開に関する条例に基づく開示請求により提示する。
⑥委託先名		日本コンピューター株式会社
再委託	⑦再委託の有無 ※	[再委託する] ＜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	番号法第10条第１項において、再委託については委託元の許諾を得た場合に認めている。横浜市では、委託契約を行う際に再委託を原則禁止しているが、再委託を行う場合は、横浜市個人情報の保護に関する条例並びに以下の約款及び特記事項による。 ・委託契約約款　第6条（一括委任又は一括下請負の禁止） ・個人情報取扱特記事項　第8条（再委託の禁止等） ・電子計算機処理等の契約に関する情報取扱特記事項　第8条（再委託の禁止等）
	⑨再委託事項	サーバー、及びPC端末本体のハードウェア面の保守委託業務

委託事項2～5		
委託事項2		予診票の印刷、封入及び搬送業務委託
①委託内容		予防接種対象者への予診票の印刷、封入、及び搬送作業。 接種対象の年齢を迎えた対象者へ向けて、必要な予診票を印刷、封入し、発送するまでの一連の作業を委託します。
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　※	特定個人情報ファイルの対象者のうち、接種対象年齢を迎えた対象者の範囲と同様
	その妥当性	抽出した対象者全員に、予診票を印刷、封入、発送するため。
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　（本市が管理する大容量ファイル転送サービスを利用し、サーバー上に対象者情報をアップロードし、委託先はデータをダウンロードし、宛名情報を印刷する。）
⑤委託先名の確認方法		市報での公告又は本市webページでの公表による。 ただし、公表を要しない契約の場合は、横浜市の保有する情報の公開に関する条例に基づく開示請求により提示する。
⑥委託先名		日本通信紙株式会社
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	番号法第10条第１項において、再委託については委託元の許諾を得た場合に認めている。横浜市では、委託契約を行う際に再委託を原則禁止しているが、再委託を行う場合は、横浜市個人情報の保護に関する条例並びに以下の約款及び特記事項による。 ・委託契約約款　第6条（一括委任又は一括下請負の禁止） ・個人情報取扱特記事項　第8条（再委託の禁止等） ・電子計算機処理等の契約に関する情報取扱特記事項　第8条（再委託の禁止等）
	⑨再委託事項	対象者データファイルを用いた宛名情報の印刷を除く、軽微な書類の印刷

委託事項3		予防接種予診票におけるパンチ委託
①委託内容		予防接種予診票からデータを入力し、CSVデータ及び予診票の画像データを作成する。
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 ※	特定個人情報ファイルの対象者のうち、接種対象年齢を迎えた対象者の範囲と同様
	その妥当性	データ化した接種対象者の接種記録を予防接種台帳システムに取り込むため。
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　（　　）
⑤委託先名の確認方法		市報での公告又は本市webページでの公表による。 ただし、公表を要しない契約の場合は、横浜市の保有する情報の公開に関する条例に基づく開示請求により提示する。
⑥委託先名		株式会社アシスト
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	

5. 特定個人情報の提供・移転（委託に伴うものを除く。）		
提供・移転の有無		［ ○ ］提供を行っている　（　　1 ）件　［　　］移転を行っている　（　　）件 ［　　］行っていない
提供先1		都道府県知事又は市町村長
①法令上の根拠		番号法別表第二　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であって主務省令で定めるもの
③提供する情報		予防接種履歴
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		定期予防接種の接種履歴がある他市町村への転出者
⑥提供方法		［ ○ ］情報提供ネットワークシステム　［　　］専用線 ［　　］電子メール　［　　］電子記録媒体（フラッシュメモリを除く。） ［　　］フラッシュメモリ　［　　］紙 ［　　］その他　（　　）
⑦時期・頻度		情報提供ネットワークシステムを通じて依頼のあった都度
6. 特定個人情報の保管・消去		
①保管場所　※		＜横浜市における措置＞ ・システムのサーバー機器はデータセンターに設置する。 ・データセンターへの入退館及びサーバー室への入退室は生体認証を用いて厳重に管理する。 ・ラックは施錠し、関係者以外はアクセスできない。 ・サーバー内のデータへのアクセスはID・パスワードによる認証が必要。 ・バックアップデータは暗号化機能のあるソフトウェアで保存用媒体に書き出した後、入退館管理を行っている遠隔地にて保管している。 ・保存用媒体は専門の搬送車を使用して安全に搬送している。 ・医療機関等から入手した紙書類は、職員立会いの上で搬送し、入退出管理している倉庫に施錠して保管する。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバー室への入室を厳重に管理する。 ②特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。
②保管期間	期間	［　5年　］　＜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	予防接種関係法令に基づき少なくとも5年間は適正に管理・保存を行うことが規定されているため。
③消去方法		＜予防接種台帳システムにおける措置＞ ・電子データ：国が定めた保存年限が経過した後、予防接種台帳システムの保守・運用を行う事業者において、特定個人情報を消去する。ディスク交換やハード更改等の際は、機器の保守を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。 ・紙書類：入手した紙書類は入退出記録を管理された倉庫で5年保存の後、職員立会いのもと外部業者による溶解処理を行う。 ＜中間サーバー・プラットフォームにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの保守・運用を行う事業者が特定個人情報を消去することはない。 ②ディスク交換やハード更改等の際は、中間サーバー・プラットフォームの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。
7. 備考		
－		

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名		
統合番号連携ファイル		
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		[　100万人以上1,000万人未満　] ＜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 ※		・住民基本台帳法第5条に基づき本市住民基本台帳に記録された住民（以下、住民登録内の者） ・住民基本台帳に記録されていた者で転出等の事由により住民票が消除（死亡による消除を除く。）された者または本市住民基本台帳に未記録の者のうち本市の業務上必要な者（以下、住民登録外の者）のうち、本市で個人番号を把握した者。
	その必要性	・個人の特定を正確かつ効率的に行う必要がある。 ・番号法第19条第7号及び第8号に基づき、情報提供ネットワークシステムを通じた情報照会、情報提供業務を行う必要がある。
④記録される項目		[　　10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	個人番号、4情報、その他識別情報（内部番号）：対象者を正確に特定するために保有する。 その他住民票関係情報：統合番号連携システムの画面上で、DV被害者等の理由による自動応答不可の状況及びその理由等を表示するために保有する。
	全ての記録項目	別添2を参照。
⑤保有開始日		平成27年10月5日
⑥事務担当部署		健康福祉局健康安全課 各区福祉保健センター福祉保健課健康づくり係

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 （ 市民局窓口サービス課 ） [ ] 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 （ ） [ ] 民間事業者 （ ） [○] その他 （ 地方公共団体情報システム機構が管理する住民基本台帳ネットワークシステム ）
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 （ 住民基本台帳ネットワークシステム ）
③入手の時期・頻度		◎住民登録内の者の分 住民基本台帳への記載またはその変更時に、都度、システム間の連携により自動的に入手する。 ◎住民登録外の者の分 ○本人または本人の代理人からの紙書類による入手。 ・特別な事情により本市外に住民票が存在する場合、対象者から紙書類で入手する。 ○住民基本台帳ネットワークシステムから即時提供方式による入手。 ・本人または本人の代理人が上記紙書類に記載した情報と、統合番号連携システムで管理する情報で相違する際に、最新情報を確認するために都度入手する。 ○住民基本台帳ネットワークシステムから一括提供方式による入手。 ・定期更新。1日1回。統合番号連携システムに登録のある住民登録外の者全て。
④入手に係る妥当性		◎住民登録内の者の分：住民基本台帳への記載またはその変更時に、都度、システム間の連携により自動的に入手するため、別途提供を受ける必要はない。 ◎住民登録外の者の分：住民登録外の者の分は、紙書類による申請が必要である。紙書類に記載された情報を確認するため、必要に応じて、住民基本台帳ネットワークシステムから最新の情報を取得する。
⑤本人への明示		・本人または本人の代理人から特定個人情報の提供を受ける場合は、当該事務が番号法第9条別表1第10項で定める個人番号利用事務であること及び個人番号の利用目的を説明する。 ・個人番号及び4情報は住民基本台帳法で定義する本人確認情報であり、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の施行に伴う関係法律の整備等に関する法律（以下、「整備法」という。）第19条の定めにより改正される住民基本台帳法の別表第三の5の5の項、及び別表第五の6の3の項において、当該事務で本人確認情報を使用して良い旨が明示されている。 ・書面提出などによる入手のため本人または本人の代理人に直接説明できない場合にあっても、本人確認情報の使用については上記のとおり明示されている。
⑥使用目的 ※		対象者の接種記録の管理・保管に係る事務を適正かつ公正に行うため
	変更の妥当性	
⑦使用の主体	使用部署 ※	健康福祉局健康安全課、各区役所福祉保健センター福祉保健課
	使用者数	[50人以上100人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上

⑧使用方法 ※		・統合番号を生成する。 住民登録内の者の分：住民基本台帳への記載時にシステム間の連携によりデータを受信・登録し、統合番号を生成する。 住民登録外の者の分：当該事務で必要となった者を統合番号連携システムへ登録した際に、統合番号を生成する。 ・生成した統合番号を登録元及び中間サーバーへ送信する。 ・統合番号並びに個人番号及び業務固有番号を紐付けて管理することにより、効率的に個人を特定する。 ・統合番号を用いて、情報照会、情報提供業務を行う。
	情報の突合 ※	個人番号、4情報、統合番号及び業務固有番号を相互に突合し、個人を特定する。
	情報の統計分析 ※	―
	権利利益に影響を与え得る決定 ※	―
⑨使用開始日		平成28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 （ 3 ） 件
委託事項1		運用保守業務委託
①委託内容		システムの管理作業及び処理作業並びに改修作業等 ファイルのバックアップ作業、データの一括更新作業などの運用業務を行うにあたり、民間事業者に委託することにより専門的な知識を有する人員を確保し、当該事業を安定的に運用することが可能となる。
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	[100万人以上1,000万人未満] ＜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 ※	特定個人情報ファイルの対象者の範囲と同様
	その妥当性	作業対象がファイル全体に及ぶため、上記の範囲を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 （ 保守センタからの遠隔操作及びデータセンター内での直接操作にて取扱いを行う。 ）
⑤委託先名の確認方法		市報での公告又は本市webページでの公表による。 ただし、公表を要しない契約の場合は、横浜市の保有する情報の公開に関する条例に基づく開示請求により提示する。
⑥委託先名		日本ソフトウェアマネジメント株式会社
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	番号法第10条第1項において、再委託については委託元の許諾を得た場合に認めている。横浜市では、委託契約を行う際に再委託を原則禁止しているが、再委託を行う場合は、横浜市個人情報の保護に関する条例並びに以下の約款及び特記事項による。 ・委託契約約款 第6条（一括委任又は一括下請負の禁止） ・個人情報取扱特記事項 第8条（再委託の禁止等） ・電子計算機処理等の契約に関する情報取扱特記事項 第8条（再委託の禁止等）
	⑨再委託事項	システム運用保守支援業務

委託事項2～5		
委託事項2		オペレーション業務委託
①委託内容		システムの処理実行作業及び監視作業等。 処理の実行、監視などのオペレーション業務を行うにあたり、民間事業者に委託することにより専門的な知識を有する人員を確保し、当該事業を安定的に運用することが可能となる。
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	［ 100万人以上1,000万人未満 ］ ＜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 ※	特定個人情報ファイルの対象者の範囲と同様
	その妥当性	作業対象がファイル全体に及ぶため、上記の範囲を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　（ 保守センタからの遠隔操作及びデータセンター内での直接操作にて取扱いを行う。 ）
⑤委託先名の確認方法		市報での公告又は本市webページでの公表による。 ただし、公表を要しない契約の場合は、横浜市の保有する情報の公開に関する条例に基づく開示請求により提示する。
⑥委託先名		株式会社SH-Net
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	番号法第10条第１項において、再委託については委託元の許諾を得た場合に認めている。横浜市では、委託契約を行う際に再委託を原則禁止しているが、再委託を行う場合は、横浜市個人情報の保護に関する条例並びに以下の約款及び特記事項による。 ・委託契約約款　第６条（一括委任又は一括下請負の禁止） ・個人情報取扱特記事項　第８条（再委託の禁止等） ・電子計算機処理等の契約に関する情報取扱特記事項　第８条（再委託の禁止等）
	⑨再委託事項	オペレーション支援業務

委託事項3		データ保管業務委託
①委託内容		データの滅失等に備えたバックアップデータの保管及び保管施設までの運搬。 本市データセンターと同時に被災する可能性が低い遠隔地にバックアップ用データを保管するにあたり、媒体保管のための専用施設及び人員を確保することが可能となる。
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	[100万人以上1,000万人未満]　＜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 ※	特定個人情報ファイルの対象者の範囲と同様
	その妥当性	作業対象がファイル全体に及ぶため、上記の範囲を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　（　　）
⑤委託先名の確認方法		市報での公告又は本市webページでの公表による。 ただし、公表を要しない契約の場合は、横浜市の保有する情報の公開に関する条例に基づく開示請求により提示する。
⑥委託先名		未定
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	番号法第10条第１項において、再委託については委託元の許諾を得た場合に認めている。横浜市では、委託契約を行う際に再委託を原則禁止しているが、再委託を行う場合は、横浜市個人情報の保護に関する条例並びに以下の約款及び特記事項による。 ・委託契約約款　第６条（一括委任又は一括下請負の禁止） ・個人情報取扱特記事項　第８条（再委託の禁止等） ・電子計算機処理等の契約に関する情報取扱特記事項　第８条（再委託の禁止等）
	⑨再委託事項	データ保管支援業務

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　（　　）件　[　　] 移転を行っている　（　　）件 [○] 行っていない

6. 特定個人情報の保管・消去		
①保管場所　※		＜横浜市における措置＞ ・統合番号連携システムのサーバー機器はデータセンターに設置する。 ・データセンターへの入退館及びサーバー室への入退室は生体認証を用いて厳重に管理する。 ・統合番号連携システムのサーバーのラックは施錠し、関係者以外はアクセスできない。 ・サーバー内のデータへのアクセスはID・パスワードによる認証が必要。 ・バックアップデータは暗号化機能のあるソフトウェアで保存用媒体に書き出した後、入退館管理を行っている遠隔地にて保管している。 ・保存用媒体は専門の搬送車を使用して安全に搬送している。 ・紙書類：入手した書類は鍵のかかる棚に施錠して保管する。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバー室への入室を厳重に管理する。 ②特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。
②保管期間	期間	[　定められていない　]　＜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	情報提供ネットワークシステムを通じた情報の照会及び提供を行うため、当該事務で使用する期間において、情報を保管する必要がある。本市住民基本台帳に記載されている期間または本市の番号利用事務で利用する期間を保管期間とする。消去は以下の時点で行う。 ・業務固有番号は、当該事務で情報の照会及び提供を行う必要がなくなった時点。 ・個人番号、4情報、その他の項目は、本市の番号利用事務で情報の照会及び提供を行う必要がなくなった時点。
③消去方法		＜横浜市における措置＞ ・電子データ：上記必要な期間を経過後、削除処理によりシステムにて削除する。年間1回程度。削除対象はシステムで判定する。ディスク交換やハード更改等の際は、統合番号連携システムの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。媒体に保存したバックアップ用データは、次回バックアップ時に次回バックアップデータを上書きすることにより削除する。 ・紙書類：特定個人情報を含む起案文書等の紙資料については、保存期間経過後、裁断又は溶解処理を行って消去する。 ＜中間サーバー・プラットフォームにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの保守・運用を行う事業者が特定個人情報を消去することはない。 ②ディスク交換やハード更改等の際は、中間サーバー・プラットフォームの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。

7. 備考

（別添2）特定個人情報ファイル記録項目

【予防接種対象者関係情報ファイル】

1	個人基本番号
2	個人基本履歴番号
3	個人コード
4	個人種別
5	住民状態
6	氏名（漢字）
7	氏名（カナ）
8	通称名（漢字）
9	通称名（カナ）
10	併記名（漢字）
11	併記名（カナ）
12	国籍コード
13	生年月日
14	性別
15	郵便番号
16	現住所_区コード
17	現住所_町コード
18	現住所_字コード
19	現住所_番地コード（1）
20	現住所_番地コード（2）
21	現住所_番地コード（3）
22	現住所_番地コード（4）
23	現住所_番地編集コード（1）
24	現住所_番地編集コード（2）
25	現住所_番地編集コード（3）
26	現住所_番地編集コード（4）
27	現住所_住所
28	現住所_方書
29	世帯コード
30	続柄コード
31	市民年月日
32	異動事由コード
33	異動年月日
34	転入前住所_住所
35	転入前住所_方書
36	転出先住所_住所
37	転出先住所_方書
38	届出年月日
39	個人基本_付せんコード
40	情報源コード
41	DV区分
42	接種年月日
43	予防接種種類
44	接種場所
45	ワクチンロット番号

【統合番号連携ファイル】

1	個人番号
2	統合番号
3	4情報
4	業務固有番号
5	自動応答不可フラグ用サイン

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	
予防接種対象者関係情報ファイル	
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	・予防接種対象者のみに予診票を送付し、実際に接種した者に限り接種履歴管理を行う。 ・窓口や郵送での申請書を受理した際には、本人確認及び申請内容のチェックを複数の職員により行う。
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	・予防接種業務に必要な情報以外は入力できないよう、システム上担保されている。 ・申請書類については、必要な情報以外を誤って記載することがないよう、様式を定める。
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	・紙の申請書類等、本人等を通じて入手する場合は、説明書等を用いて利用目的を本人に明示する。 ・予防接種台帳システムを利用する職員を限定し、個人ごとにユーザーID及びパスワードを発行し、端末利用時は画像認証を行っている。また、利用者権限を設定することによって、認証後に入手可能な情報に制限をかける。
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	番号法第16条に基づいた本人確認の措置を行う。
個人番号の真正性確認の措置の内容	・住登内者の場合：統合番号連携システム端末を利用して照合を行う。 ・住登外者の場合：住基ネットCS端末を利用して照合を行う。
特定個人情報の正確性確保の措置の内容	・個人番号のみではなく、氏名・住所・生年月日等の複数の情報により本人確認を行う。 ・特定個人情報の入力、削除及び訂正を行う際には、入力した原本(申請書類等)とデータファイルの内容について、複数人による確認を行う(ダブルチェック)。
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	・予防接種を実施した後の予診票は、実施医療機関から医師会を通じて、健康安全課へ提出される。 ・申請書類等は、対象者又は当該者と同一の世帯に属する者から受理することを原則とし、それ以外の代理人については、書面により予防接種対象者から委任を受けたことを確認できる者とし、かつ代理人の本人確認を行う。 ・特定個人情報が記載された申請書類等は、漏えい及び紛失を防止するため、入力及び照合した後は、施錠可能な場所に保管する。
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	・統合番号連携システムへのログイン時の職員認証により担当事務を特定する。担当事務に限定した権限の割り当てを行い、権限のある事務のみ情報を検索及び登録できるようにし、目的を超えた紐付けを抑止する。 ・統合番号連携システムでは個人番号、統合番号及び4情報など基本的な情報のみ保持する仕組みとするため、当該事務にて必要のない情報との紐付けは不可能である。 ・誤操作による検索及び登録を行わないよう、業務マニュアルを整備した上、操作方法、手順等を周知する。 ・統合番号連携システムへのログイン時の職員認証に加えて、「誰が」「いつ」「どのような操作をしたのか」を記録することを周知し、不要な操作を抑止する。	
事務で使用するその他のシステムにおける措置の内容	・予防接種台帳システムは予防接種事業を行う上で必要な情報のみを保持しており、必要のない情報は記録できないため、紐付けを行うことはない。情報管理責任者により、利用する職員ごとに業務単位で利用者権限を設定することで、アクセスできる情報を制限している。個人ごとにユーザーID及びパスワードを発行し、端末利用時は画像認証を行っている。 ・福祉保健システムのデータの管理、運用について、システムを使用する職員を限定し、個人ごとにユーザーID及びパスワードを発行し、端末利用時は画像認証を行っている。なお、ログインIDにより、誰が、いつ、どの端末で、誰の情報を取り扱ったか分かる様記録を残す。	
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	・予防接種台帳システムを利用する職員を限定し、個人ごとにユーザーID及びパスワードを発行し、端末利用時は画像認証を行っている。	
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	○ID・パスワードの発効管理 ・利用する職員のユーザIDとパスワードの発効とともに、事務従事者の画像との紐づけを行う。 ○失効管理 ・権限を有していた職員の異動または退職情報を確認し、異動または退職があった際はアクセス権限を更新し、当該IDでの利用権限を失効させる。	
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	・適切なアクセス権限が付与されるよう、利用する職員ごとに業務単位で利用者権限を設定する。 ・操作ログを取得・保管し、不正な利用を分析するため、定期的に確認を行う。	
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	・予防接種台帳システムへのログイン記録、予防接種台帳システムの操作記録、特定個人情報を取り扱った記録（操作日、操作時間、取扱者）等のログ情報を残し、不正な操作がないことについて定期的に確認を行う。	
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	・操作ログを取得し、定期的に確認を行う。 ・利用する職員への研修等において、事務外利用の禁止等について指導する。	
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	・利用権限を業務単位ごとに設定することで、アクセスできる情報を制限する。 ・操作端末へのファイルのダウンロードはでき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		〇委託業務の開始前に体制図等の資料を提出させる。 〇横浜市個人情報の保護に関する条例並びに以下の約款及び特記事項に基づき、個人情報の適正な取扱い並びに条例に基づく罰則の内容及び民事上の責任についての研修を受けさせ、個人情報保護に関する誓約書を提出させる。 ・委託契約約款 ・個人情報取扱特記事項 ・電子計算機処理等の契約に関する情報取扱特記事項
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	・作業者を限定するため、委託作業者の名簿を事前に提出させる。 ・操作ログを取得、定期的に確認することで、不正な使用がないことを確認する。
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	・アクセスログを取得し、ログイン記録を残す。 ・契約書等に基づき、委託業務が実施されていることを適時確認するとともに、その記録を残す。
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	個人情報取扱特記事項において、再委託は原則禁止であり、再委託する場合は個人情報取扱特記事項に定める内容と同等の内容を再委託先に対して約定する旨を定めている。 遵守の確認については、業務完了報告書等にて行う。
	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	個人情報取扱特記事項に基づいて取り扱いを行う。遵守の確認については、業務完了報告書等にて行う。
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	契約が終了したとき、当該特定個人情報ファイルの使用が終了したとき若しくは委託元が指示したとき又はその他契約で定めたときに消去を行う。 遵守の確認については、毎月業務完了報告書にて行う。
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	契約書に添付する個人情報取扱特記事項において、次のとおり規定 ・目的外利用の原則禁止 ・複写、複製の原則禁止 ・再委託の原則禁止 ・資料等の返還 ・事故発生時等における報告 ・研修の実施及び誓約書の提出 ・作業場所の外への持出禁止
再委託先による特定個人情報ファイルの適切な取扱いの確保	[　十分に行っている　]	＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない
	具体的な方法	横浜市個人情報の保護に関する条例並びに以下の約款及び特記事項による。 ・委託契約約款 ・個人情報取扱特記事項 ・電子計算機処理等の契約に関する情報取扱特記事項
その他の措置の内容	―	
リスクへの対策は十分か	[　十分である　]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

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

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	＜横浜市における措置＞ 〇統合番号連携システムの画面において、 ・番号法第9条に定められた事務担当者のみ統合番号連携システムを使用できる仕組みを構築する。 ・統合番号連携システムへのログイン時の職員認証により担当事務を特定する。担当事務に限定した権限の割り当てを行い、権限のない事務の情報を入手できないように制御する。 ・個人番号、統合番号等の番号入力時は、チェックディジットによる入力チェックを行い、誤入力により誤って他人の情報を表示することを抑止する。 ・誤操作による検索及び登録を行わないよう、業務マニュアルを整備した上、操作方法、手順等を周知する。 ・統合番号連携システムへのログイン時の職員認証に加えて、「誰が」「いつ」「どのような操作をしたのか」を記録することを周知し、不要な操作を抑止する。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※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。 ②中間サーバーの職員認証・権限管理機能（※3）では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※1）情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 （※2）番号法第19条第1項第7号、第8号及び第16号に基づき、事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 安全が保たれない方法によって入手が行われるリスク	
リスクに対する措置の内容	＜横浜市における措置＞ ・統合番号連携システムのサーバーをデータセンター内に設置し、物理的にアクセスできる者を限定する。 ・統合番号連携システムと中間サーバ間の通信は下記＜中間サーバー・ソフトウェアにおける措置＞及び＜中間サーバー･プラットフォームにおける措置＞と同一である。 ＜中間サーバー・ソフトウェアにおける措置＞ 中間サーバーは、個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	＜横浜市における措置＞ 統合番号連携システムでは情報提供ネットワークシステムからの情報照会結果を保管しない。このためデータが不正確となるリスクは存在しない。 ＜中間サーバー・ソフトウェアにおける措置＞ 中間サーバーは、個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、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	＜横浜市における措置＞ ・統合番号連携システムのサーバーをデータセンター内に設置し、物理的にアクセスできる者を限定する。 ・統合番号連携システムと中間サーバー間の通信は下記＜中間サーバー・ソフトウェアにおける措置＞及び＜中間サーバー・プラットフォームにおける措置＞と同一である。 ＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ②既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ③情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報が漏えい・紛失するリスクを軽減している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）中間サーバーは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、漏えい・紛失のリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク5： 不正な提供が行われるリスク	
リスクに対する措置の内容	＜横浜市における措置＞ ・当該事務で保有する正本から副本への登録は、原則システム間の自動連携により行う。これにより手作業による入力誤り等を防止する。一時的に作成される登録用ファイルが不正に更新されないよう、サーバー等へのアクセス権限を設定する。 ・統合番号連携システムの画面からの副本への登録においては、統合番号連携システムの職員認証機能により担当事務の特定、担当事務に限定した権限の割り当てを行い、権限のある事務のみ情報を検索及び登録できる仕組みとする。 ・住民基本台帳事務における支援措置対象者等については自動応答不可フラグを設定する。自動応答不可フラグを設定したデータへ情報照会の要求があった場合は、 　番号法第19条に基づき提供が認められている機関及び事務であること 　その照会の必要性 　提供する情報の取扱に十分な注意が必要であること を照会元の機関に連絡、確認したうえで、情報提供の許可権限を持つ業務担当者が情報送信を許可したデータのみ提供する。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能（※）により、情報提供ネットワークシステムにおける照会許可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、中間サーバーにも格納して、情報提供機能により、照会許可用照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ②情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。 ③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。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク6： 不適切な方法で提供されるリスク	
リスクに対する措置の内容	＜横浜市における措置＞ ・当該事務で保有する正本から副本への登録は、原則システム間の自動連携により行う。これにより手作業による入力誤り等を防止する。一時的に作成される登録用ファイルが不正に更新されないよう、サーバー等へのアクセス権限を設定する。 ・統合番号連携システムの画面からの副本への登録においては、統合番号連携システムの職員認証機能により担当事務の特定、担当事務に限定した権限の割り当てを行い、権限のある事務のみ情報を検索及び登録できる仕組みとする。 ＜中間サーバー・ソフトウェアにおける措置＞ ①セキュリティ管理機能（※）により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ②中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）暗号化・復号機能と、鍵情報及び照会許可用照合リストを管理する機能。 ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、不適切な方法で提供されるリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい･紛失のリスクに対応している。 ③中間サーバー・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	＜横浜市における措置＞ ・当該事務で保有する正本から副本への登録は、原則システム間の自動連携により行う。これにより手作業による入力誤り等を防止する。一時的に作成される登録用ファイルが不正に更新されないよう、サーバー等へのアクセス権限を設定する。 ・統合番号連携システムの画面からの副本への登録においては、統合番号連携システムの職員認証機能により担当事務の特定、担当事務に限定した権限の割り当てを行い、権限のある事務のみ情報を検索及び登録できる仕組みとする。 ・正本に誤りを発見した際は、速やかに自動応答不可フラグを設定する。業務マニュアルを整備した上、操作方法、手順等を周知する。 ・誤操作による検索及び登録を行わないよう、業務マニュアルを整備した上、操作方法、手順等を周知する。 ・誤った相手への提供に対する措置は、＜中間サーバー・ソフトウェアにおける措置＞により行う。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。 ②情報提供データベース管理機能（※）により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ③情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 （※）特定個人情報を副本として保存・管理する機能。
リスクへの対策は十分か	［　　十分である　　］　＜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
＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者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	＜横浜市における措置＞ ・統合番号連携システムのサーバー機器はデータセンターに設置する。 ・データセンターへの入退館及びサーバー室への入退室は生体認証を用いて厳重に管理する。 ・統合番号連携システムのサーバーのラックは施錠し、関係者以外はアクセスできない。 ・バックアップデータは暗号化機能のあるソフトウェアで保存用媒体に書き出した後、入退館管理を行っている遠隔地にて保管している。 ・保存用媒体は専門の搬送車を使用して安全に搬送している。 ・統合番号連携システムでは端末に特定個人情報を保存しないため、端末盗難時の漏洩はない。 ・入手した紙書類は入退出記録を管理された倉庫で5年保存する。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。	
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	・特定個人情報にアクセスするサーバ及び端末にウイルス対策ソフトを導入し、定期的にパターン更新を行う。管理者がウイルス対策ソフトの適用及び状況の監視、管理を一括して管理できる仕組みとする。 ・サーバ、端末とも、OSのパッチ適用を随時実施する。 ・ネットワークへの不正侵入を防止するため、ファイアウォール、IDS、IPSを設置し、監視する。 ・統合番号連携システムの画面ではファイルを取り出す機能を持たない仕組みとする。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ②中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。	
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	[発生あり]	<選択肢> 1）発生あり 2）発生なし
その内容	別紙のとおり	
再発防止策の内容	別紙のとおり	
⑩死者の個人番号	[保管していない]	<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	―	
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	◎住民登録内の者の分 住民基本台帳システムから、1日1回、システム間の連携により自動的に入手する。予診票の接種記録については、接種を行った医療機関から月次単位で入手する。 ◎住民登録外の者の分 〇本人または本人の代理人からの紙書類による入手。 ・本人の申請により変更等が生じた場合、その都度データを更新している。 〇医療機関からの入手 ・予診票の接種記録については、接種を行った医療機関から月次単位で入手する。
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： 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	・媒体に保存したバックアップ用データは、次回バックアップ時に次回バックアップデータを上書きすることにより削除する。 ・システムプログラムを作成し、期間を経過した情報の削除処理を行う。 ・入手した紙書類は入退出記録を管理された倉庫で5年保存の後、職員立会いのもと外部業者による溶解処理を行う。
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
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	
―	

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	
統合番号連携ファイル	
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	○データを登録する際の防止措置 ・住民登録内の者の分：住民基本台帳への記載時にシステム間で自動的に連携することにより、個人番号と統合番号及び業務固有番号の正確な紐付けを担保する。 ・住民登録外の者の分：申請された内容と、予防接種台帳システムの登録情報との確認を行う。 また、住民登録外の者については、住民基本台帳ネットワークシステムからの一括提供方式による連携データを受信し、定期的にシステムで整合性の確認を行う。 ○統合番号連携システムの検索画面を使用する際の措置 ・個人番号、統合番号等の番号入力時は、チェックディジットによる入力チェックを行い、誤入力により誤って他人の情報を表示することを抑止する。 ・誤操作による検索及び登録を行わないよう、業務マニュアルを整備した上、操作方法、手順等を周知する。 ・統合番号連携システムへのログイン時の職員認証に加えて、「誰が」「いつ」「どのような操作をしたのか」を記録することを周知し、不要な操作を抑止する。
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	○統合番号連携システムに登録してあるデータを利用する際の措置 ・統合番号連携システムへのログイン時の職員認証により担当事務を特定する。担当事務に限定した権限の割り当てを行い、権限のない事務の情報を入手できないように制御する。 ・誤操作による検索及び登録を行わないよう、業務マニュアルを整備した上、操作方法、手順等を周知する。 ・統合番号連携システムへのログイン時の職員認証に加えて、「誰が」「いつ」「どのような操作をしたのか」を記録することを周知し、不要な操作を抑止する。 ○本人から情報を入手する際の措置 ・申請書類については、必要な情報以外を誤って記載することがないよう、記入しやすい書類を作成する。
その他の措置の内容	ー
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	○システムから入手する際の措置 ・住民登録内の者の分：データセンター内の専用線を用いて、住民基本台帳への記載時にシステム間で自動的に連携することにより安全を担保する。入手元である市民局窓口サービス課に対して、統合番号連携システムでの使用目的を事前に明示する。 ・住民登録外の者の分：住民基本台帳ネットワークシステムの即時提供方式による入手及び住民基本台帳ネットワークシステムの一括提供方式による連携データをデータセンター内の専用線を用いて入手することにより安全を担保する。入手元である市民局窓口サービス課に対して、統合番号連携システムでの使用目的を事前に明示する。 ○本人または本人の代理人から直接情報を入手する際の措置 ・当該事務において初めて個人番号を入手する際は、当該事務が番号法第9条で定める個人番号利用事務であること及び個人番号の利用目的を説明する。 ・個人番号の提供を受けるときは番号法第16条に基づいた本人確認の措置を行う。
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	番号法第16条に基づいた本人確認の措置を行う。
個人番号の真正性確認の措置の内容	個人番号カードの提示を受け、確認する。 個人番号カードの提示を受けられないときは、上記「入手の際の本人確認の措置の内容」により本人確認を行い、その結果をもとに統合番号連携システムまたは住民基本台帳ネットワークシステムで個人番号を照合する。
特定個人情報の正確性確保の措置の内容	住民登録内の者の分：住民基本台帳への記載時にシステム間で自動的に連携する。 住民登録外の者の分：業務で変更を把握した際に、随時に統合番号連携システムに入力する。また、住民基本台帳ネットワークシステムから一括提供方式による連携データを入手する。
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	○システム間の連携により入手する際の措置 ・住民登録内の者の分：住民基本台帳への記載時にシステム間で自動的に連携する。 ・住民登録外の者の分：住民基本台帳ネットワークシステムから一括提供方式により入手する場合は、システム間で自動的に連携する。 両システムとも統合番号連携システムへの連携はデータセンター内の専用線を使用する。FW、IDS等を設置し、他システム、外部ネットワークからの侵入防止措置を講じる。 ○申請書等の紙書類の管理は業務で入手した特定個人情報を記載した書類の扱いに準ずる。
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	・統合番号連携システムへのログイン時の職員認証により担当事務を特定する。担当事務に限定した権限の割り当てを行い、権限のある事務のみ情報を検索及び登録できるようにし、目的を超えた紐付けを抑止する。 ・統合番号連携システムでは個人番号、統合番号及び4情報など基本的な情報のみ保持する仕組みとするため、当該事務にて必要のない情報との紐付けは不可能である。 ・誤操作による検索及び登録を行わないよう、業務マニュアルを整備した上、操作方法、手順等を周知する。 ・統合番号連携システムへのログイン時の職員認証に加えて、「誰が」「いつ」「どのような操作をしたのか」を記録することを周知し、不要な操作を抑止する。	
事務で使用するその他のシステムにおける措置の内容	○福祉保健システム端末を使用する際の措置 ・統合番号連携システム、予防接種台帳システムとは別に構築、稼働しており、目的を超えた紐付け、必要のない情報との紐付けはできない。 ・ユーザID及びパスワードによる認証を行っているため、世帯情報、及び税情報の閲覧以外のシステムは使用できない。また、他業務の担当者が当該業務のシステムを使用することもできない。	
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	・統合番号連携システムへのログイン時の職員認証により担当事務を特定する。担当事務に限定した権限の割り当てを行い、権限のある事務のみ情報の検索及び登録ができる仕組みとする。 ・職員ごとにユーザIDとパスワードを発効し、端末利用時は画像認証により、当該職員が操作していることを認証する。 ・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。 ・同一ユーザIDの同時ログインを制限する。	
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	○ID・パスワードの発効管理 ・システム管理者は、事務所管課と調整の上、アクセス権限と事務の対応表を作成する。 ・事務所管課は、事務担当者を特定し、システム管理者にユーザIDとパスワードの発効とともに、事務従事者の画像との紐づけを依頼する。 ・システム管理者は、依頼に基づきユーザIDとパスワードを発効し、事務従事者の画像との紐づけを行う。 ○失効管理 ・権限を有していた職員の異動または退職情報を確認し、異動または退職があった際はアクセス権限を更新し、当該IDでの利用権限を失効させる。	
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	・アクセス権限の設定作業は、システム管理者が行う。 ・アクセス権限の設定内容は、事務所管課からの依頼により決定する。 ・設定変更の結果は、事務所管課の確認を受ける。 ・定期の人事異動においては人事給与の所管部署から職員異動、機構改革等の情報を入手する。当該情報はシステム間の連携により入手し、手入力による設定ミス等を削減する。	
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	・「誰が」「いつ」「どのような操作をしたのか」を記録する。 ・操作履歴は一定期間、保管する。	
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	・統合番号連携システムへのログイン時の職員認証に加えて、「誰が」「いつ」「どのような操作をしたのか」を記録することを周知し、不要な操作を抑止する。 ・職員に対しては、個人情報保護に関する研修を行う。 ・委託先に対しては業務外で使用しないよう仕様書に定め、個人情報保護にかかる誓約書を提出させる。また、セキュリティ研修の実施も義務付ける。 ・違反行為を行った場合は、法の罰則規定により措置を講じる。
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	・管理者権限を持たない者に対する措置：統合番号連携システムの画面からのみファイルにアクセスできる仕組みを構築する。統合番号連携システムの画面においては、ファイル作成、出力機能を持たない仕組みとする。 ・管理者権限を持つ者に対する措置：原則外部記憶媒体等の使用を制限し物理的に複製できない仕組みとする。バックアップ作業や外部記憶媒体を用いたデータ連携のため、一部端末のみ外部媒体の使用を許可する。 ・職員に対しては、データ保護に関する研修を行う。 ・委託先に対しては仕様書にて許可を得ない複製を禁止し、個人情報保護にかかる誓約書を提出させる。また、セキュリティ研修の実施も義務付ける。 ・違反行為を行った場合は、法の罰則規定により措置を講じる。
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		〇委託業務の開始前に体制図等の資料を提出させる。 〇横浜市個人情報の保護に関する条例並びに以下の約款及び特記事項に基づき、個人情報の適正な取扱い並びに条例に基づく罰則の内容及び民事上の責任についての研修を受けさせ、個人情報保護に関する誓約書を提出させる。 ・委託契約約款 ・個人情報取扱特記事項 ・電子計算機処理等の契約に関する情報取扱特記事項
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	・委託業務に従事する者については、受託者からの書面による事前の申請を受け、管理者が承認する。 ・従事する者の担当業務を特定する。担当業務に限定した権限の割り当てを行い、権限のある業務ファイルのみアクセスできる仕組みとする。 ・従事する者ごとにユーザIDとパスワードを発効し、当該従事者の画像と紐づけることで、従事者以外の操作を防止する。 ・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。
特定個人情報ファイルの取扱いの記録		[　　記録を残している　　] ＜選択肢＞ 1）記録を残している　2）記録を残していない
	具体的な方法	作業内容について事前に申請を受け、管理者が承認したうえで実施し、その記録を残す。
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	個人情報取扱特記事項において、再委託は原則禁止であり、再委託する場合は個人情報取扱特記事項に定める内容と同等の内容を再委託先に対して約定する旨を定めている。 遵守の確認については、業務完了報告書等にて行う。
	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	個人情報取扱特記事項に基づいて取り扱いを行う。遵守の確認については、業務完了報告書等にて行う。
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	契約が終了したとき、当該特定個人情報ファイルの使用が終了したとき若しくは委託元が指示したとき又はその他契約で定めたときに消去を行う。 遵守の確認については、業務完了報告書等にて行う。
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	契約書に添付する個人情報取扱特記事項において、次のとおり規定 ・目的外利用の原則禁止 ・複写、複製の原則禁止 ・再委託の原則禁止 ・資料等の返還 ・事故発生時等における報告 ・研修の実施及び誓約書の提出 ・作業場所の外への持出禁止
再委託先による特定個人情報ファイルの適切な取扱いの確保		[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない
	具体的な方法	横浜市個人情報の保護に関する条例並びに以下の約款及び特記事項による。 ・委託契約約款 ・個人情報取扱特記事項 ・電子計算機処理等の契約に関する情報取扱特記事項
その他の措置の内容		ー
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

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

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	＜横浜市における措置＞ 〇統合番号連携システムの画面において、 ・番号法第9条に定められた事務担当者のみ統合番号連携システムを使用できる仕組みを構築する。 ・統合番号連携システムへのログイン時の職員認証により担当事務を特定する。担当事務に限定した権限の割り当てを行い、権限のない事務の情報を入手できないように制御する。 ・個人番号、統合番号等の番号入力時は、チェックディジットによる入力チェックを行い、誤入力により誤って他人の情報を表示することを抑止する。 ・誤操作による検索及び登録を行わないよう、業務マニュアルを整備した上、操作方法、手順等を周知する。 ・統合番号連携システムへのログイン時の職員認証に加えて、「誰が」「いつ」「どのような操作をしたのか」を記録することを周知し、不要な操作を抑止する。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※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。 ②中間サーバーの職員認証・権限管理機能（※3）では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※1）情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 （※2）番号法第19条第1項第7号、第8号及び第16号に基づき、事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 安全が保たれない方法によって入手が行われるリスク	
リスクに対する措置の内容	＜横浜市における措置＞ ・統合番号連携システムのサーバーをデータセンタ内に設置し、物理的にアクセスできる者を限定する。 ・統合番号連携システムと中間サーバ間の通信は下記＜中間サーバー・ソフトウェアにおける措置＞及び＜中間サーバー･プラットフォームにおける措置＞と同一である。 ＜中間サーバー・ソフトウェアにおける措置＞ 中間サーバーは、個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	＜横浜市における措置＞ 統合番号連携システムでは情報提供ネットワークシステムからの情報照会結果を保管しない。このためデータが不正確となるリスクは存在しない。 ＜中間サーバー・ソフトウェアにおける措置＞ 中間サーバーは、個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、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	＜横浜市における措置＞ ・統合番号連携システムのサーバーをデータセンター内に設置し、物理的にアクセスできる者を限定する。 ・統合番号連携システムと中間サーバー間の通信は下記＜中間サーバー・ソフトウェアにおける措置＞及び＜中間サーバー・プラットフォームにおける措置＞と同一である。 ＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ②既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ③情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報が漏えい・紛失するリスクを軽減している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）中間サーバーは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、漏えい・紛失のリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク5： 不正な提供が行われるリスク	
リスクに対する措置の内容	＜横浜市における措置＞ ・当該事務で保有する正本から副本への登録は、原則システム間の自動連携により行う。これにより手作業による入力誤り等を防止する。一時的に作成される登録用ファイルが不正に更新されないよう、サーバー等へのアクセス権限を設定する。 ・統合番号連携システムの画面からの副本への登録においては、統合番号連携システムの職員認証機能により担当事務の特定、担当事務に限定した権限の割り当てを行い、権限のある事務のみ情報を検索及び登録できる仕組みとする。 ・住民基本台帳事務における支援措置対象者等については自動応答不可フラグを設定する。自動応答不可フラグを設定したデータへ情報照会の要求があった場合は、 　番号法第19条に基づき提供が認められている機関及び事務であること 　その照会の必要性 　提供する情報の取扱に十分な注意が必要であること を照会元の機関に連絡、確認したうえで、情報提供の許可権限を持つ業務担当者が情報送信を許可したデータのみ提供する。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能（※）により、情報提供ネットワークシステムにおける照会許可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、中間サーバーにも格納して、情報提供機能により、照会許可用照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ②情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。 ③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。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク6： 不適切な方法で提供されるリスク	
リスクに対する措置の内容	＜横浜市における措置＞ ・当該事務で保有する正本から副本への登録は、原則システム間の自動連携により行う。これにより手作業による入力誤り等を防止する。一時的に作成される登録用ファイルが不正に更新されないよう、サーバー等へのアクセス権限を設定する。 ・統合番号連携システムの画面からの副本への登録においては、統合番号連携システムの職員認証機能により担当事務の特定、担当事務に限定した権限の割り当てを行い、権限のある事務のみ情報を検索及び登録できる仕組みとする。 ＜中間サーバー・ソフトウェアにおける措置＞ ①セキュリティ管理機能（※）により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ②中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）暗号化・復号機能と、鍵情報及び照会許可用照合リストを管理する機能。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、不適切な方法で提供されるリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。
リスクへの対策は十分か	[十分である]　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	＜横浜市における措置＞ ・当該事務で保有する正本から副本への登録は、原則システム間の自動連携により行う。これにより手作業による入力誤り等を防止する。一時的に作成される登録用ファイルが不正に更新されないよう、サーバー等へのアクセス権限を設定する。 ・統合番号連携システムの画面からの副本への登録においては、統合番号連携システムの職員認証機能により担当事務の特定、担当事務に限定した権限の割り当てを行い、権限のある事務のみ情報を検索及び登録できる仕組みとする。 ・正本に誤りを発見した際は、速やかに自動応答不可フラグを設定する。業務マニュアルを整備した上、操作方法、手順等を周知する。 ・誤操作による検索及び登録を行わないよう、業務マニュアルを整備した上、操作方法、手順等を周知する。 ・誤った相手への提供に対する措置は、＜中間サーバー・ソフトウェアにおける措置＞により行う。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。 ②情報提供データベース管理機能（※）により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ③情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 （※）特定個人情報を副本として保存・管理する機能。
リスクへの対策は十分か	[十分である]　＜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
＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者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	＜横浜市における措置＞ ・統合番号連携システムのサーバー機器はデータセンターに設置する。 ・データセンターへの入退館及びサーバー室への入退室は生体認証を用いて厳重に管理する。 ・統合番号連携システムのサーバーのラックは施錠し、関係者以外はアクセスできない。 ・バックアップデータは暗号化機能のあるソフトウェアで保存用媒体に書き出した後、入退館管理を行っている遠隔地にて保管している。 ・保存用媒体は専門の搬送車を使用して安全に搬送している。 ・統合番号連携システムでは端末に特定個人情報を保存しないため、端末盗難時の漏洩はない。 ・入手した紙書類は入退出記録を管理された倉庫で5年保存する。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。	
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	・特定個人情報にアクセスするサーバ及び端末にウイルス対策ソフトを導入し、定期的にパターン更新を行う。管理者がウイルス対策ソフトの適用及び状況の監視、管理を一括して管理できる仕組みとする。 ・サーバー、端末とも、OSのパッチ適用を随時実施する。 ・ネットワークへの不正侵入を防止するため、ファイアウォール、IDS、IPSを設置し、監視する。 ・統合番号連携システムの画面ではファイルを取り出す機能を持たない仕組みとする。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ②中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。	
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		[　　発生あり　　] ＜選択肢＞ 1）発生あり　2）発生なし
	その内容	別紙のとおり
	再発防止策の内容	別紙のとおり
⑩死者の個人番号		[　　保管している　　] ＜選択肢＞ 1）保管している　2）保管していない
	具体的な保管方法	・死者のデータは生存者のデータと一体となって保管している。 住民登録内だった者の分：消除後、住民基本台帳法施行令第34条第1項に定める期間が経過し、かつ、統合番号連携システムを使用する全業務で不要となるまでの間保管する。 住民登録外だった者の分：統合番号連携システムを使用する全業務で不要となるまでの間保管する。
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：　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		○個人番号、4情報 ・住民登録内の者の分：住民基本台帳への記載及びその変更時にシステム間で自動的に連携する。 ・住民登録外の者の分：定期的に住民基本台帳ネットワークシステムから一括提供方式によりデータを受信し、更新する。 ・事務上入手したデータのほうが新しい場合は、必要に応じて統合番号連携システムの画面から更新する。 ○4情報以外 ・業務固有番号は、当該事務にて変更した後、統合番号連携システムへ再登録する。 ・情報提供ネットワークシステムへの照会結果は統合番号連携システムには保存しないため、古い情報のまま保管することはない。
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	・保存期間の過ぎた情報は、削除処理によりシステムで判別して自動削除する。 ・媒体に保存したバックアップ用データは、次回バックアップ時に次回バックアップデータを上書きすることにより削除する。 ・入手した紙書類は入退出記録を管理された倉庫で5年保存の後、職員立会いのもと外部業者による溶解処理を行う。
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
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	＜横浜市における措置＞ 定期的に自己点検を実施し、実際の運用が評価書記載の内容と合致しているかについて確認を行う。 ＜中間サーバー･プラットフォームにおける措置＞ 運用規則等に基づき、中間サーバー･プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。	
②監査	［　　十分に行っている　　］	＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
具体的な内容	＜横浜市における措置＞ 定期的に個人番号利用事務所管部署間での相互監査を実施する。 ＜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･プラットフォームについて、定期的に監査を行うこととしている。	
2. 従業者に対する教育･啓発		
従業者に対する教育･啓発	［　　十分に行っている　　］	＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
具体的な方法	＜横浜市における措置＞ 年に1回、個人情報保護に関する所属研修を実施する。 ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバー･プラットフォームの運用に携わる職員及び事業者に対し、セキュリティ研修等を実施することとしている。 ②中間サーバー･プラットフォームの業務に就く場合は、運用規則等について研修を行うこととしている。	
3. その他のリスク対策		
＜中間サーバー･プラットフォームにおける措置＞ 中間サーバー･プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用･監視を実現する。		

Ⅴ　開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求

①請求先		横浜市役所 　市民局市民情報センター 231-0017 横浜市中区港町1-1 045-671-3884 鶴見区役所 　区政推進課広報相談係 230-0051 横浜市鶴見区鶴見中央3-20-1 045-510-1680 神奈川区役所 　区政推進課広報相談係 221-0824 横浜市神奈川区広台太田町3-8 045-411-7021 西区役所 　区政推進課広報相談係 220-0051 横浜市西区中央1-5-10 045-320-8321 中区役所 　区政推進課広報相談係 231-0021 横浜市中区日本大通35 045-224-8121 南区役所 　区政推進課広報相談係 232-0024 横浜市南区浦舟町2-33 045-341-1112 港南区役所 　区政推進課広報相談係 233-0003 横浜市港南区港南4-2-10 045-847-8321 保土ケ谷区役所 　区政推進課広報相談係 240-0001 横浜市保土ケ谷区川辺町2-9 045-334-6221 旭区役所 　区政推進課広報相談係 241-0022 横浜市旭区鶴ケ峰1-4-12 045-954-6023 磯子区役所 　区政推進課広報相談係 235-0016 横浜市磯子区磯子3-5-1 045-750-2335 金沢区役所 　区政推進課広報相談係 236-0021 横浜市金沢区泥亀2-9-1 045-788-7721 港北区役所 　区政推進課広報相談係 222-0032 横浜市港北区大豆戸町26-1 045-540-2221 緑区役所 　区政推進課広報相談係 226-0013 横浜市緑区寺山町118 045-930-2220 青葉区役所 　区政推進課広報相談係 225-0024 横浜市青葉区市ケ尾町31-4 045-978-2221 都筑区役所 　区政推進課広報相談係 224-0032 横浜市都筑区茅ケ崎中央32-1 045-948-2222 戸塚区役所 　区政推進課広報相談係 244-0003 横浜市戸塚区戸塚町16-17 045-866-8321 栄区役所 　区政推進課広報相談係 247-0005 横浜市栄区桂町303-19 045-894-8335 泉区役所 　区政推進課広報相談係 245-0024 横浜市泉区和泉中央北5-1-1 045-800-2335 瀬谷区役所 　区政推進課広報相談係 246-0021 横浜市瀬谷区二ッ橋町190 045-367-5635
②請求方法		指定様式による書面の提出により開示・訂正・利用停止請求を受け付ける。 （指定様式はこちら　http://www.city.yokohama.lg.jp/shimin/shiminjoho/） 請求先に持参又は郵送。
	特記事項	受付時に本人確認を行う。
③手数料等		［　　無料　　］　　＜選択肢＞ 1) 有料　　2) 無料 閲覧等の手数料は無料。 （手数料額、納付方法：ただし、写しの交付には実費負担が必要。郵送交付の場合は送料負担が必要。　）
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	予防接種対象者関係情報ファイル
	公表場所	横浜市役所　市民情報センター 231-0017 横浜市中区港町1-1 045-671-3884
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	健康福祉局健康安全部健康安全課　予防接種担当 住　　所：〒231-0017横浜市中区港町１－１ 電話番号：045-671-4190
②対応方法	窓口、電話等の問合せは随時対応し、必要に応じて対応記録を残す。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	平成31年1月4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	評価書を本市Webページにて掲載及び市民情報センターに配架し、閲覧できるようにする。郵便、ファクシミリ、本市Webページ（電子申請・届出システム）、番号制度事務とりまとめ課への持参による意見聴取を行う。
②実施日・期間	平成31年２月１日～３月３日
③期間を短縮する特段の理由	－
④主な意見の内容	評価書の修正に係る意見の提出はありませんでした。
⑤評価書への反映	
3. 第三者点検	
①実施日	平成31年3月20日
②方法	横浜市個人情報保護審議会で審議
③結果	評価書の内容について修正を求める意見はありませんでした。
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
平成31年1月28日	Ⅰ　基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム1 ②システムの機能	（追加）	5　副本作成機能 　中間サーバーに登録する副本を作成する機能	事後	事前の提出、公表が義務付けられない
平成31年1月28日	Ⅰ　基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム1 ③他のシステムとの接続	（追加）	【○】庁内連携システム	事前	事後で足りるものの任意に事前提出
平成31年1月28日	Ⅰ　基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム5 ②システムの機能	なお、アクセス制限により個人番号の閲覧・利用は不可能となる。 (2) 接種対象者を含む世帯員の課税・非課税情報検索 　福祉保健システム端末において入力された4情報(氏名、住所、性別、生年月日)の組み合わせをキーに、接種対象者を含む世帯員情報の課税;非課税情報の検索を行い、検索条件に該当する情報の一覧を画面上に表示する。	なお、アクセス制限により統合番号の閲覧・利用は不可能となる。 予防接種法による予防接種の実施に関する事務においては、接種対象者の接種費用の減免確認事務を行うため、福祉保健システム内の下記機能のみを使用する。 (2) 接種対象者を含む世帯員の課税・非課税情報検索 （1）で特定した対象者につき、課税・非課税情報の検索を行い、検索条件に該当する情報の一覧を画面上に表示する。	事後	誤字、脱字等の修正、表現の軽微な修正
平成31年1月28日	Ⅰ　基本情報 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	・番号法第19条第7号に基づき、情報提供ネットワークシステムを通じた情報照会、情報提供業務を行う。	・番号法第19条第7号及び第8号に基づき、情報提供ネットワークシステムを通じた情報照会、情報提供業務を行う。	事後	事前の提出、公表が義務付けられない

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
平成31年1月28日	Ⅰ　基本情報 6. 情報提供ネットワークシステムによる情報連携 ②法令上の根拠 【提供】	（追加）	行政手続における特定の個人を識別するための番号の利用等に関する法律別表第2の主務省令で定める事務及び情報を定める命令　第12条の2各号	事後	必要な記載の追加
平成31年1月28日	Ⅰ　基本情報 7. 評価実施機関における担当部署 ②所属長の役職名	木村　博和	（削除）	事後	事前の提出、公表が義務付けられない
平成31年1月28日	（別添1）事務の内容 （予防接種対象者への接種勧奨、接種記録の管理・保管に関する事務） 図	①住記情報 情報提供ネットワーク	①住基情報 情報提供ネットワークシステム	事後	誤字、脱字等の修正、表現の軽微な修正
平成31年1月28日	（別添1）事務の内容 （予防接種の実費徴収の有無の確認に関する事務） 図	①住記情報 （追加）	①住基情報、住基情報連携 （追加） 情報提供ネットワークシステム・中間サーバー・統合番号連携システムの情報照会・情報提供基幹系システム	事後	誤字、脱字等の修正、表現の軽微な修正

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
平成31年1月28日	（別添1）事務の内容 （予防接種の実費徴収の有無の確認に関する事務） （備考）④	（追加）	当年1月1日時点で本市に課税台帳が存在しない場合、他市町村が保有する本人及び世帯員の税情報を、統合番号連携システム経由で中間サーバへ照会し、免除の可否を回答	事後	事前の提出、公表が義務付けられない
平成31年1月28日	（別添1）事務の内容 （予防接種健康被害救済給付に関する事務） 図	情報提供ネットワーク	情報提供ネットワークシステム	事後	誤字、脱字等の修正、表現の軽微な修正
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要（予防接種対象者関係情報ファイル） 3．特定個人情報の入手・使用 ②入手方法	フラッシュメモリ【〇】	フラッシュメモリ【　】	事前	事後で足りるものの任意に事前提出
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要（予防接種対象者関係情報ファイル） 3．特定個人情報の入手・使用 ③入手の時期・頻度	◎住民登録内の者の分 住民記録システムから一括提供方式による入手。 ・1日1回の定期更新。住民記録システムからフラッシュメモリで予防接種台帳サーバーへデータ登録。	◎住民登録内の者の分 　住民基本台帳システムから、1日1回、システム間の連携により自動的に入手する。予診票の接種記録については、接種を行った医療機関から月次単位で入手する。	事前	事後で足りるものの任意に事前提出

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
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要（予防接種対象者関係情報ファイル） 3．特定個人情報の入手・使用 ⑤本人への明示	・個人番号及び4情報は住民基本台帳法で定義する本人確認情報であり、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の施行に伴う関係法律の整備等に関する法律（以下、「整備法」という。）第19条の定めにより改正される住民基本台帳法の別表第三の5の5の項、及び別表第五の6の3の項において、当該事務で本人確認情報を使用して良い旨が明示されている。	・個人番号及び4情報は住民基本台帳法で定義する本人確認情報であり、整備法第19条の定めにより改正される住民基本台帳法の別表第三の5の5の項、及び別表第五の6の3の項において、当該事務で本人確認情報を使用して良い旨が明示されている。	事後	誤字、脱字等の修正、表現の軽微な修正
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要（予防接種対象者関係情報ファイル） 4．特定個人情報ファイルの取扱いの委託 委託事項1 ①委託内容	システムを安定的に運用することが可能となる。	当該事業を安定的に運用することが可能となる。	事後	誤字、脱字等の修正、表現の軽微な修正
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要（予防接種対象者関係情報ファイル） 4．特定個人情報ファイルの取扱いの委託 委託事項1 ⑧再委託の許諾方法	横浜市個人情報保護に関する条例並びに以下の契約約款及び特記事項による。	横浜市個人情報の保護に関する条例並びに以下の契約約款及び特記事項による。	事後	誤字、脱字等の修正、表現の軽微な修正
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要（予防接種対象者関係情報ファイル） 4．特定個人情報ファイルの取扱いの委託 委託事項2 ⑥委託先名	未定	日本通信紙株式会社	事後	事前の提出、公表が義務付けられない

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
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要（予防接種対象者関係情報ファイル） 4．特定個人情報ファイルの取扱いの委託 委託事項2 ⑧再委託の許諾方法	（追加）	・個人情報取扱特記事項　第8条（再委託の禁止等）	事後	事前の提出、公表が義務付けられない
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要（予防接種対象者関係情報ファイル） 6．特定個人情報の保管・消去 ①保管場所	＜予防接種台帳システムにおける措置＞ ①予防接種台帳システムは、入退室管理をしている庁舎エリア内の施錠された部屋にサーバーを設置し、保管している。 ②サーバーへのアクセスはIDとパスワードによる認証が必要となる。サーバー内のデータへのアクセスはID・パスワードによる認証が必要。	＜横浜市における措置＞ ・システムのサーバー機器はデータセンターに設置する。 ・データセンターへの入退館及びサーバー室への入退室は生体認証を用いて厳重に管理する。 ・ラックは施錠し、関係者以外はアクセスできない。 ・サーバー内のデータへのアクセスはID・パスワードによる認証が必要。 ・バックアップデータは暗号化機能のあるソフトウェアで保存用媒体に書き出した後、入退館管理を行っている遠隔地にて保管している。 ・保存用媒体は専門の搬送車を使用して安全に搬送している。 ・医療機関等から入手した紙書類は、職員立会いの上で搬送し、入退出管理している倉庫に施錠して保管する。	事前	重要な変更に該当する
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要 （予防接種対象者関係情報ファイル） 6．特定個人情報の保管・消去 ②保管期間	期間　定められていない その妥当性　・胎児に重篤な障害を引き起こす感染症を防ぐために、妊娠可能な時期になってから予防接種履歴の確認が必要となるなど、予防接種履歴の長期保存が重要となる。 ・予防接種履歴データの保管期間については、国で方針が示されていないため、現時点では保存年限を定めることができない。	期間　5年 その妥当性　予防接種関係法令に基づき少なくとも5年間は適正に管理・保存を行うことが規定されているため。	事後	事前の提出、公表が義務付けられない

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
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要（統合番号連携ファイル） 2．基本情報 ⑥事務担当部署	健康福祉局健康安全課	健康福祉局健康安全課 各区福祉保健センター福祉保健課健康づくり係	事後	事前の提出、公表が義務付けられない
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要（統合番号連携ファイル） 3．特定個人情報の入手・使用 ①入手元	評価実施機関内の他部署（市民局窓口サービス課が保管する住民基本台帳）	評価実施機関内の他部署（市民局窓口サービス課）	事後	誤字、脱字等の修正、表現の軽微な修正
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要（統合番号連携ファイル） 4．特定個人情報ファイルの取扱の委託 委託事項1，2 ①委託内容	システムを安定的に運用することが可能となる。	当該作業を安定的に運用することが可能となる。	事後	誤字、脱字等の修正、表現の軽微な修正
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要 （統合番号連携ファイル） 4．特定個人情報ファイルの取扱いの委託 委託事項1 ⑥委託先名	未定	日本ソフトウェアマネジメント株式会社	事後	事前の提出、公表が義務付けられない
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要（統合番号連携ファイル） 4．特定個人情報ファイルの取扱いの委託 委託事項2 ⑥委託先名	未定	株式会社SH－Net	事後	事前の提出、公表が義務付けられない

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
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要（統合番号連携ファイル） 4．特定個人情報ファイルの取扱いの委託 委託事項2 ⑧再委託の許諾方法	横浜市個人情報保護に関する条例並びに以下の契約約款及び特記事項による。	横浜市個人情報の保護に関する条例並びに以下の契約約款及び特記事項による。	事後	誤字、脱字等の修正、表現の軽微な修正
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要 （統合番号連携ファイル） 6．特定個人情報の保管・消去 ①保管場所	＜予防接種台帳システムにおける措置＞ ①予防接種台帳システムは、入退室管理をしている庁舎エリア内の施錠された部屋にサーバーを設置し、保管している。 ②サーバーへのアクセスはIDとパスワードによる認証が必要となる。	（削除）	事前	重要な変更に該当する
平成31年1月28日	Ⅱ　特定個人情報ファイルの概要（統合番号連携ファイル） 6．特定個人情報の保管・消去 ③消去方法	＜横浜市における措置＞ （追記） ＜予防接種台帳システムにおける措置＞ ①予防接種台帳システムの保守・運用を行う事業者において、特定個人情報を順次消去する。 ②ディスク交換やハード更改等の際は、予防接種台帳システムに係る保守を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。 ・紙書類：入手した書類は5年保存の後、職員立会いのもと外部業者による溶解処理を行う。	＜横浜市における措置＞ ・紙書類：特定個人情報を含む起案文書等の紙資料については、保存期間経過後、裁断又は溶解処理を行って消去する。 ＜予防接種台帳システムにおける措置＞（削除）	事前	事後で足りるものの任意に事前提出

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
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 （予防接種対象者関係情報ファイル） 3．特定個人情報の使用 リスク1 事務で使用するその他のシステムにおける措置の内容	・予防接種台帳システムは予防接種事業を行う上で必要な情報のみを保持しており、必要のない情報は記録できないため、紐付けを行うことはない。 ・情報管理責任者により、利用する職員ごとに業務単位で利用者権限を設定することで、アクセスできる情報を制限している。	・予防接種台帳システムは予防接種事業を行う上で必要な情報のみを保持しており、必要のない情報は記録できないため、紐付けを行うことはない。情報管理責任者により、利用する職員ごとに業務単位で利用者権限を設定することで、アクセスできる情報を制限している。 ・福祉保健システムのデータの管理、運用について、システムを使用する際にはIDカード、ログインID、パスワードが必要となり、権限を制限している。なお、ログインIDにより、誰が、いつ、どの端末で、誰の情報を取り扱ったか分かる様記録を残す。	事後	セキュリティリスクを明らかに低減させる変更
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 （予防接種対象者関係情報ファイル） 4．特定個人情報の取扱いの委託 情報保護管理体制の確認	○横浜市個人情報保護に関する条例並びに以下の約款及び特記事項に基づき、個人情報の適正な取扱い並びに条例に基づく罰則の内容及び民事上の責任についての研修を受けさせ、個人情報保護に関する誓約書を提出する。	○横浜市個人情報の保護に関する条例並びに以下の約款及び特記事項に基づき、個人情報の適正な取扱い並びに条例に基づく罰則の内容及び民事上の責任についての研修を受けさせ、個人情報保護に関する誓約書を提出する。	事後	誤字、脱字等の修正、表現の軽微な修正
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 （予防接種対象者関係情報ファイル） 4．特定個人情報の取扱いの委託 委託契約中の特定個人情報ファイルの取扱いに関する規定 規定の内容	（追記）	・作業場所の外への持出禁止	事後	セキュリティリスクを明らかに低減させる変更

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
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 （予防接種対象者関係情報ファイル） 4. 特定個人情報の取扱いの委託 再委託先による特定個人情報ファイルの適切な取扱いの確保 具体的な方法	横浜市個人情報保護に関する条例並びに以下の約款及び特記事項による。 ・委託契約約款 ・個人情報取扱特記事項 ・電子計算機処理等の契約に関する情報取扱特記事項	横浜市個人情報の保護に関する条例並びに以下の約款及び特記事項による。 ・委託契約約款 ・個人情報取扱特記事項 ・電子計算機処理等の契約に関する情報取扱特記事項	事後	誤字、脱字等の修正、表現の軽微な修正
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策（予防接種対象者関係情報ファイル） 6. 情報提供ネットワークシステムとの接続 リスク1 リスクに対する措置の内容	（※2）番号法別表第2及び第19条第14号に基づき、	（※2）番号法第19条第1項第7号、第8号及び第16号に基づき、	事後	誤字、脱字等の修正、表現の軽微な変更
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策（予防接種対象者関係情報ファイル） 6. 情報提供ネットワークシステムとの接続 リスク2 リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。	＜中間サーバー・ソフトウェアにおける措置＞ 中間サーバーは、個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用し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。	事後	誤字、脱字等の修正、表現の軽微な変更

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
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策（予防接種対象者関係情報ファイル） 6．情報提供ネットワークシステムとの接続 リスク3 リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。	＜中間サーバー・ソフトウェアにおける措置＞ 中間サーバーは、個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、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。	事後	誤字、脱字等の修正、表現の軽微な変更
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 （予防接種対象者関係情報ファイル） 7．特定個人情報の保管・消去 リスク1 ⑤物理的対策 具体的な対策の内容	＜予防接種台帳システムにおける措置＞ ①予防接種台帳システムは、入退室管理をしている庁舎エリア内の部屋にサーバーを設置・保管している。 ②サーバーへのアクセスはIDとパスワードによる認証が必要となる。・サーバー内のデータへのアクセスはID・パスワードによる認証が必要。 ③停電等に備え、災害時の非常用電源装置等を付設している。	＜横浜市における措置＞ ・統合番号連携システムのサーバー機器はデータセンターに設置する。 ・データセンターへの入退館及びサーバー室への入退室は生体認証を用いて厳重に管理する。 ・統合番号連携システムのサーバーのラックは施錠し、関係者以外はアクセスできない。 ・バックアップデータは暗号化機能のあるソフトウェアで保存用媒体に書き出した後、入退館管理を行っている遠隔地にて保管している。 ・保存用媒体は専門の搬送車を使用して安全に搬送している。 ・統合番号連携システムでは端末に特定個人情報を保存しないため、端末盗難時の漏洩はない。 ・入手した紙書類は入退出記録を管理された倉庫で5年保存する。 ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバー･プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。	事前	重要な変更に該当する

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
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 （予防接種対象者関係情報ファイル） 7．特定個人情報の保管・消去 リスク2 リスクに対する措置の内容	◎住民登録内の者の分 　住民記録システムから一括提供方式による入手。 　・1日1回、住民記録システムからフラッシュメモリ経由で予防接種台帳サーバーへデータ更新を行っている。	◎住民登録内の者の分 　住民基本台帳システムから、1日1回、システム間の連携により自動的に入手する。予診票の接種記録については、接種を行った医療機関から月次単位で入手する。	事前	重要な変更に該当する
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策（統合番号連携ファイル） 2．特定個人情報の入手 リスク2 不適切な方法で入手が行われるリスク リスクに対する措置の内容	・住民登録外の者の分：住民基本台帳ネットワークシステム及びデータセンター内の専用線を用いて、住民基本台帳ネットワークシステテから一括提供方式による連携データを受信することにより安全を担保する。	・住民登録外の者の分：住民基本台帳ネットワークシステムの即時提供方式による入手及び住民基本台帳ネットワークシステムの一括提供方式による連携データをデータセンター内の専用線を用いて入手することにより安全を担保する。	事後	誤字、脱字等の修正、表現の軽微な修正
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策（統合番号連携ファイル） 3．特定個人情報ファイルの入手 リスク2 ユーザ認証の管理 具体的な管理方法	職員ごとにユーザIDとパスワードを発効する。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。	・職員ごとにユーザIDとパスワードを発効し、端末利用時は画像認証により、当該職員が操作していることを認証する。 ・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。	事後	セキュリティリスクを明らかに低減させる変更
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策（統合番号連携ファイル） 3．特定個人情報ファイルの入手 リスク2 アクセス権限の発効、失効の管理 具体的な管理方法	事務所管課は、事務担当者を特定し、システム管理者にユーザIDとパスワードの発効を依頼する。 システム管理者は、依頼に基づきユーザIDとパスワードの発効を行う。	事務所管課は、事務担当者を特定し、システム管理者にユーザIDとパスワードの発効とともに、事務従事者の画像との紐づけを依頼する。 システム管理者は、依頼に基づきユーザIDとパスワードを発効し、事務従事者の画像との紐づけを行う。	事後	セキュリティリスクを明らかに低減させる変更

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
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 （統合番号連携ファイル） 4. 特定個人情報の取扱いの委託 情報保護管理体制の確認	○横浜市個人情報保護に関する条例並びに以下の約款及び特記事項に基づき、個人情報の適正な取扱い並びに条例に基づく罰則の内容及び民事上の責任についての研修を受けさせ、個人情報保護に関する誓約書を提出する。	○横浜市個人情報の保護に関する条例並びに以下の約款及び特記事項に基づき、個人情報の適正な取扱い並びに条例に基づく罰則の内容及び民事上の責任についての研修を受けさせ、個人情報保護に関する誓約書を提出する。	事後	誤字、脱字等の修正、表現の軽微な修正
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策（統合番号連携ファイル） 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限 具体的な制限方法	従事する者ごとにユーザIDとパスワードを発効し、従事者以外の操作を防止する。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。	・従事する者ごとにユーザIDとパスワードを発効し、当該従事者の画像と紐づけることで、従事者以外の操作を防止する。 ・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。	事後	セキュリティリスクを明らかに低減させる変更
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策（統合番号連携ファイル） 4. 特定個人情報ファイルの取扱いの委託 委託契約書中の特定個人情報ファイルの取扱いに関する規定 規定の内容	（追加）	・作業場所の外への持出禁止	事後	セキュリティリスクを明らかに低減させる変更

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
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策（統合番号連携ファイル） 6．情報提供ネットワークシステムとの接続 リスク1 リスクに対する措置の内容	（※2）番号法別表第2及び第19条第14号に基づき、	（※2）番号法第19条第1項第7号、第8号及び第16号に基づき、	事後	誤字、脱字等の修正、表現の軽微な修正
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策（統合番号連携ファイル） 6．情報提供ネットワークシステムとの接続 リスク2 リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。	＜中間サーバー・ソフトウェアにおける措置＞ 中間サーバーは、個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用し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。	事後	誤字、脱字等の修正、表現の軽微な変更
平成31年1月28日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策（統合番号連携ファイル） 6．情報提供ネットワークシステムとの接続 リスク3 リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。	＜中間サーバー・ソフトウェアにおける措置＞ 中間サーバーは、個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、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。	事後	誤字、脱字等の修正、表現の軽微な変更

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
平成31年1月28日	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	港南区役所 　区政推進課広報相談係 233-0004 横浜市港南区港南中央通10-1　045-847-8321 泉区役所 　区政推進課広報相談係 245-0016 横浜市泉区和泉町4636-2　045-800-2335	港南区役所 　区政推進課広報相談係 233-0003 横浜市港南区港南4-2-10　045-847-8321 泉区役所 　区政推進課広報相談係 245-0024 横浜市泉区和泉中央北5-1-1　045-800-2335	事後	事前の提出、公表が義務付けられない
令和1年5月24日	Ⅰ　基本情報 1．特定個人情報ファイルを取り扱う事務 ②事務の内容	【予防接種事務について】 ・横浜市ではA類(こども)のみ、接種記録を管理している。 ・接種勧奨は両方に行っている。	【予防接種事務について】 （削除）	事前	重要な変更に該当する

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和1年5月24日	Ⅰ　基本情報 2．特定個人情報ファイルを取り扱う事務において使用するシステム システム6 ①システムの名称 ②システムの機能 ③他のシステムとの接続	（追記）	①情報共有基盤システム ②情報共有基盤システムは、既存住民基本台帳システム、税務システム等と連携し、情報共有基盤システム上に構築された業務システム（以下「基盤関連システム」という。）が利用する住民情報の一元管理を実現する。 (1)統合データベース機能 　基盤関連システムが利用する住民情報を保管及び提供する機能。 (2)データ連携機能 　住民記録システム、新税務システム等と連携する機能。 (3)データ変換機能 　文字コード及びファイルフォーマットを変換する機能。 (4)個人認証機能 　基盤関連システムの利用者を認証し、権限を管理する機能。 (5)システム管理機能 　情報共有基盤システム及び基盤関連システムにおけるバッチの状況管理、サーバーの死活監視等を行う機能。 ③〔〇〕既存住民基本台帳システム　〔〇〕宛名システム　〔〇〕税務システム　〔〇〕その他（基盤関連システム）	事後	事前の提出、公表が義務付けられない
令和1年5月24日	Ⅱ　特定個人情報ファイルの概要 （予防接種対象者関係情報ファイル） 4．特定個人情報ファイルの取扱いの委託 委託事項1 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	接種対象年齢はこどもから高齢者まで作業ファイル全体に及ぶため、上記の範囲を取り扱う必要がある。	全ての接種対象者の情報を管理しているため、上記の範囲を取り扱う必要がある。	事後	事前の提出、公表が義務付けられない

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和1年5月24日	Ⅱ　特定個人情報ファイルの概要 （予防接種対象者関係情報ファイル） 4. 特定個人情報ファイルの取扱いの委託 委託事項3	（追記）	予防接種予診票におけるパンチ委託 ①委託内容 予防接種予診票からデータを入力し、CCSVデータ及び予診票の画像データを作成する。 ②取り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、10万人以上100万人未満、特定個人情報ファイルの対象者のうち、接種対象年齢を迎えた対象者の範囲と同様、データ化した接種対象者の接種記録を予防接種台帳システムに取り込むため。 ③委託先における取扱者数　10人以上50人未満 ④委託先への特定個人情報ファイルの提供方法【〇】紙 ⑤委託先名の確認方法 市報での公告又は本市webページでの公表による。 ただし、公表を要しない契約の場合は、横浜市の保有する情報の公開に関する条例に基づく開示請求により提示する。 ⑥委託先名　株式会社アシスト ⑦再委託の有無　再委託しない	事後	事前の提出、公表が義務付けられない
令和1年5月24日	Ⅱ　特定個人情報ファイルの概要 （予防接種対象者関係情報ファイル） 6. 特定個人情報の保管・消去 ③消去方法	＜予防接種台帳システムにおける措置＞ ①国が定めた保存年限が経過した後、予防接種台帳システムの保守・運用を行う事業者において、特定個人情報を消去する。 ②ディスク交換やハード更改等の際は、予防接種台帳システムに係る保守を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。	＜予防接種台帳システムにおける措置＞ ・電子データ：国が定めた保存年限が経過した後、予防接種台帳システムの保守・運用を行う事業者において、特定個人情報を消去する。 ディスク交換やハード更改等の際は、機器の保守を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。	事後	事前の提出、公表が義務付けられない

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和1年5月24日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 （予防接種対象者関係情報ファイル） 2. 特定個人情報の入手 リスク2 リスクに対する措置の内容	・予防接種台帳システムを利用する職員を限定し、個人ごとにユーザーID及びパスワードによる認証を行っている。	・予防接種台帳システムを利用する職員を限定し、個人ごとにユーザーID及びパスワードを発行し、端末利用時は画像認証を行っている。	事後	事前の提出、公表が義務付けられない
令和1年5月24日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 （予防接種対象者関係情報ファイル） 3. 特定個人情報の使用 リスク1 事務で使用するその他のシステムにおける措置の内容	・予防接種台帳システムは予防接種事業を行う上で必要な情報のみを保持しており、必要のない情報は記録できないため、紐付けを行うことはない。情報管理責任者により、利用する職員ごとに業務単位で利用者権限を設定することで、アクセスできる情報を制限している。 ・福祉保健システムのデータの管理、運用について、システムを使用する際にはIDカード、ログインID、パスワードが必要となり、権限を制限している。なお、ログインIDにより、誰が、いつ、どの端末で、誰の情報を取り扱ったか分かる様記録を残す。	・予防接種台帳システムは予防接種事業を行う上で必要な情報のみを保持しており、必要のない情報は記録できないため、紐付けを行うことはない。情報管理責任者により、利用する職員ごとに業務単位で利用者権限を設定することで、アクセスできる情報を制限している。個人ごとにユーザーID及びパスワードを発行し、端末利用時は画像認証を行っている。 ・福祉保健システムのデータの管理、運用について、システムを使用する職員を限定し、個人ごとにユーザーID及びパスワードを発行し、端末利用時は画像認証を行っている。なお、ログインIDにより、誰が、いつ、どの端末で、誰の情報を取り扱ったか分かる様記録を残す。	事後	セキュリティリスクを明らかに低減させる変更
令和1年5月24日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 （予防接種対象者関係情報ファイル） 3. 特定個人情報の使用 リスク2 ユーザー認証の管理 具体的な管理方法	・予防接種台帳システムを利用する職員を限定し、個人ごとにユーザーID及びパスワードによる認証を行っている。	・予防接種台帳システムを利用する職員を限定し、個人ごとにユーザーID及びパスワードを発行し、端末利用時は画像認証を行っている。	事後	セキュリティリスクを明らかに低減させる変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和1年5月24日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 （予防接種対象者関係情報ファイル） 3．特定個人情報の使用 リスク2 アクセス権限の発行・失効の管理 具体的な管理方法	・アクセス権限の発効・失効の管理は、利用する職員が変わるごとに実施し、記録を残す。	○ID・パスワードの発効管理 ・利用する職員のユーザIDとパスワードの発効とともに、事務従事者の画像との紐づけを行う。 ○失効管理 ・権限を有していた職員の異動または退職情報を確認し、異動または退職があった際はアクセス権限を更新し、当該IDでの利用権限を失効させる。	事後	セキュリティリスクを明らかに低減させる変更
令和1年5月24日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 （予防接種対象者関係情報ファイル） 7．特定個人情報の保管・消去 リスク1 ⑥技術的対策 具体的な管理方法	＜予防接種台帳システムにおける措置＞ ①予防接種台帳システムでは、ファイアウォールや通信の暗号化により、アクセス制限、侵入防止対策を行っている。 ②予防接種台帳システムのサーバーには、新種の不正プログラムに対応するためにウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③予防接種台帳システムで利用する端末には、新種の不正プログラムに対応するためにウイルス対策ソフトを導入し、パターンファイルの更新を行う。	・特定個人情報にアクセスするサーバ及び端末にウイルス対策ソフトを導入し、定期的にパターン更新を行う。管理者がウイルス対策ソフトの適用及び状況の監視、管理を一括して管理できる仕組みとする。 ・サーバ、端末とも、OSのパッチ適用を随時実施する。 ・ネットワークへの不正侵入を防止するため、ファイアウォール、IDS、IPSを設置し、監視する。 ・統合番号連携システムの画面ではファイルを取り出す機能を持たない仕組みとする。	事後	セキュリティリスクを明らかに低減させる変更
令和1年5月24日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7．特定個人情報の保管・消去 リスク3 消去手順	・媒体に保存したバックアップ用データは、次回バックアップ時に次回バックアップデータを上書きすることにより削除する。 ・ディスク交換やハード更改等の際は、予防接種台帳管理システムに係る保守を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。 ・入手した紙書類は入退出記録を管理された倉庫で5年保存の後、職員立会いのもと外部業者による溶解処理を行う。	・媒体に保存したバックアップ用データは、次回バックアップ時に次回バックアップデータを上書きすることにより削除する。 ・システムプログラムを作成し、期間を経過した情報の削除処理を行う。 ・入手した紙書類は入退出記録を管理された倉庫で5年保存の後、職員立会いのもと外部業者による溶解処理を行う。	事後	セキュリティリスクを明らかに低減させる変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和1年5月24日	Ⅵ　評価実施手続 1．基礎項目評価 ①実施日		平成31年 4月1日	事後	事前の提出、公表が義務付けられない
令和1年11月26日	Ⅰ　基本情報 6．情報提供ネットワークシステムによる情報連携 ②法令上の根拠【提供】	【提供】 番号法第19条第7号　別表第2　16の2項 行政手続における特定の個人を識別するための番号の利用等に関する法律別表第2の主務省令で定める事務及び情報を定める命令　第12条の2各号 【照会】 番号法第19条第7号　別表第2　17項、18項、19項 行政手続における特定の個人を識別するための番号の利用等に関する法律別表第2の主務省令で定める事務及び情報を定める命令　第13条各号	【情報提供】 番号法第19条第7号　別表第2　16の2項 行政手続における特定の個人を識別するための番号の利用等に関する法律別表第2の主務省令で定める事務及び情報を定める命令　第12条の2 【情報照会】 番号法第19条第7号　別表第2　16の2項、17項、18項、19項 行政手続における特定の個人を識別するための番号の利用等に関する法律別表第2の主務省令で定める事務及び情報を定める命令　第12条の2、第12条の3、第13条、第13条の2	事後	必要な記載の追加

別紙

過去3年以内に評価実施機関において発生した個人情報に関する重大事故の内容及び再発防止策の内容

	発生年月日	内容	件数	再発防止策
1	平成29年4月12日	水道局の職員が、協議会の会員企業に、「ビジネスセミナーのご案内」を電子メールで送信する際、会員企業164社の175件のメールアドレスを、他の受信者のメールアドレスが判別できない方式（BCC）に設定して送信すべきところ、全員のメールアドレスが表示された状態（TO[宛先]）で一斉送信した。	104件	(1)メールを送信する際、他の受信者のメールアドレスが判別できない方式（BCC）になっているかどうかなど、複数人によるダブルチェックを再度徹底する。 (2)間違いを犯しやすい項目を抽出したチェックリストを活用することで、再発防止に努める。
2	平成29年8月8日	水道局の水道事務所で、水道料金・下水道使用料の請求漏れを防ぐため、毎月作成して処理を行っている「未請求者一覧」という帳票7枚が所在不明となった。	最大112件	当該水道事務所では職員個人が未請求者一覧を保管していたが、今後は、組織として管理ルールを徹底し紛失を防止。また、未請求者一覧に処理内容の記載欄を設けるとともに、ダブルチェックを徹底する。
3	平成29年10月27日	経済局が運営する「横浜ライフイノベーションプラットフォーム」の会員や関係者向けに「セミナーのご案内」を電子メールで送信する際、他の受信者のメールアドレスが判別できない方式（BCC）に設定して送信すべきところ、送信した139か所のメールアドレスが表示された状態（TO[宛先]）で一斉送信した。	131件	当課職員のメール設定を、誤操作があってもすぐにメールが送信されないよう変更。 また、個人情報を扱っていることを再認識し、特に、お互いにアドレスを知らないと思われる相手先にメールを送信する際には、チェックリストを活用して注意するとともに、ダブルチェックの方法を、送信時だけではなく、作業開始時にも行うなど再徹底する。
4	平成29年12月25日	地域ケアプラザ（指定管理者が運営）において、通所介護送迎時に使用する送迎車用ファイル1冊（139人分）を紛失した。ファイルは直後に隣接する消防署の職員により地域ケアプラザ裏の路上で拾得され、警察に届けられていたため、回収した。	139件	＜地域ケアプラザ＞ 「個人情報保護マニュアル」の改定を検討する。また、送迎を担当する職員は、ファイルの持ち出しはせずに、必要な情報を地域ケアプラザ内で確認する。 それに加えて、全職員に事例を共有し、個人情報の取り扱いに対する指導を行い、再発防止を徹底する。 ＜区役所＞ 地域ケアプラザに対し、個人情報の管理の徹底を指示し、再発防止に向けた研修を行うよう指導した。また、区内のケアプラザと今回の事例を共有し、全職員への注意喚起を要請した。
5	平成30年8月9日	水道局の責任職が、職務上携帯している公用の携帯電話を帰宅途中に紛失した。携帯電話は、セキュリティロックをしていたが、水道局責任職が保有する公用携帯電話の電話番号、メールアドレス、水道局の職場電話番号及び水道局責任職の自宅又は個人携帯電話番号（158人分）が登録されていた。	158件	勤務時間内外における公用携帯電話の管理を徹底するとともに、職務上取り扱う情報についても管理を徹底し、あらためて公用携帯電話を携帯する全職員へセキュリティロックを設定すること等の注意喚起をする。
6	平成30年10月26日	地域ケアプラザ（指定管理者が運営）において、子育て情報の電子メールを送信する際、配信登録している方（123人分）のメールアドレスを、他の受信者のメールアドレスが判別できない方式（BCC）に設定して送信すべきところ、全員のメールアドレスが表示された状態（TO）で一斉送信した。	123件	外部の複数のメールアドレス宛にメールを送信する際は、BCC にメールアドレスを入れることを確実に実施する。また、ダブルチェックの実施について再度周知し、徹底する。
7	平成31年2月25日	「広報よこはま」の配送を受託しているドライバー（再委託者）が当日の配送終了後、配送先（自治会等）の担当者氏名、住所、電話番号等が記載された配送伝票を車に残したまま、事業所に戻らずに自宅近くの駐車場に車を一晩駐車していたところ、車上荒らし被害にあい当該配送伝票を盗まれた。	189件	車から長時間離れる際には、車内に配送伝票を残さないよう徹底するとともに、個人情報の取扱いについて、個人情報取扱特記事項に基づき、適正に運用するよう事業者に対して再度指導した。
8	令和元年9月27日	横浜市プレミアム付商品券事業における子育て世帯分の購入引換券について、世帯主の前住所地へ誤送付してしまったものがあった。	410件	住所情報を、抽出処理時点の最新のものにする「更新」の作業が抜けていたことにより、前住所地が抽出されてしまった。再発防止策として、委託業者と抽出要件を再協議し、今後は更新作業をした上で送付先住所の抽出処理を行うことを確認した。さらに発送前に最新住所情報と照合し、より発送日に近い情報に更新することとした。