（別紙）全項目評価書の変更箇所 【Ⅰ基本情報】

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
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
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

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
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
令和3年6月15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 ①法令上の根拠 【提供】	番号法別表第二　16の2 行政手続における特定の個人を識別するための番号の利用等に関する法律別表第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	番号法別表第二　16の2、16の3 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	事後	必要な記載の追加

令和4年6月28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】 ・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。 (追加)	【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、特定個人情報を含むデータのファイルでの保存はしない。 【新型コロナウイルス感染症対策に係る予防接種事務について】 ・ワクチン接種記録システム(VRS)へ予防接種対象者及び発行した接種券の登録を行う。 ・予防接種の実施後に接種記録等を登録、管理し、他市区町村へ接種記録の照会・提供を行う。 ・予防接種の実施後に、接種者からの申請に基づき、新型コロナウイルス感染症予防接種証明書の交付を行う。	事後	特定個人情報保護評価に関する規則第9条第2項の規定(緊急時事後評価)の適用
令和4年6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使用するシステム システム7 ①システムの名称	(追加)	ワクチン接種記録システム(VRS)	事後	特定個人情報保護評価に関する規則第9条第2項の規定(緊急時事後評価)の適用
令和4年6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使用するシステム システム7 ②システムの機能	(追加)	・ワクチン接種記録システム(VRS)への接種対象者・接種券発行登録 ・接種記録の管理 ・転出/死亡時等のフラグ設定 ・他市区町村への接種記録の照会・提供 ・新型コロナウイルス感染症予防接種証明書の交付に係る接種記録の照会 ・新型コロナウイルス感染症予防接種証明書の電子申請受付・電子交付の実施	事後	特定個人情報保護評価に関する規則第9条第2項の規定(緊急時事後評価)の適用
令和4年6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使用するシステム システム7 ③他のシステムとの接続	[　　]住民基本台帳ネットワークシステム	[　○　]住民基本台帳ネットワークシステム	事後	特定個人情報保護評価に関する規則第9条第2項の規定(緊急時事後評価)の適用
令和4年6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	(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) 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8号及び第9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	号ずれによる軽微な修正
令和4年6月28日	Ⅰ　基本情報 5. 個人番号の利用 法令上の根拠	(追加)	・番号法第19条第16号(新型コロナウイルス感染症対策に係る予防接種事務におけるワクチン接種記録システム(VRS)を用いた情報提供・照会のみ) ・番号法第19条第6号(委託先への提供)	事後	特定個人情報保護評価に関する規則第9条第2項の規定(緊急時事後評価)の適用

令和4年6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 ①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、3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	【情報提供】 番号法第19条第8号　別表第2　16の2項、3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8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	号ずれによる軽微な修正
令和5年8月4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	（追加）	・新型コロナウイルス感染症予防接種証明書のコンビニ交付を行う。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和5年8月4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使用するシステム システム7 ②システムの機能	・新型コロナウイルス感染症予防接種証明書の電子申請受付・電子交付の実施	・新型コロナウイルス感染症予防接種証明書の電子申請受付・電子交付・コンビニ交付の実施	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅰ基本情報 7. 評価実施期間における担当部署 ①部署	健康福祉局健康安全部健康安全課	医療局健康安全部健康安全課	事後	組織再編による修正
令和5年8月4日	Ⅰ基本情報 7. 評価実施期間における担当部署 ②所属長の役職名	健康福祉局健康安全部健康安全課長	医療局健康安全部健康安全課長	事後	組織再編による修正
令和6年4月30日	Ⅰ　基本情報 1. 特定個人情報ファイルを取り扱う事務 ②事務の内容	【新型コロナウイルス感染症対策に係る予防接種事務について】 ・ワクチン接種記録システム（VRS)へ予防接種対象者及び発行した接種券の登録を行う。 ・予防接種の実施後に接種記録等を登録、管理し、他市区町村へ接種記録の照会・提供を行う。 ・予防接種の実施後に、接種者からの申請に基づき、新型コロナウイルス感染症予防接種証明書の交付を行う。 ・新型コロナウイルス感染症予防接種証明書のコンビニ交付を行う。	【新型コロナウイルス感染症対策に係る予防接種事務について】 ・令和6年3月31日以前の接種記録等を登録、管理する。 ・接種者からの申請に基づき、令和6年3月31日以前の新型コロナウイルス感染症予防接種証明書の交付を行う。	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅰ　基本情報 1. 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7 ②システムの機能	・ワクチン接種記録システム(VRS)への接種対象者・接種券発行登録 ・接種記録の管理 ・転出/死亡時等のフラグ設定 ・他市区町村への接種記録の照会・提供 ・新型コロナウイルス感染症予防接種証明書の交付に係る接種記録の照会 ・新型コロナウイルス感染症予防接種証明書の電子申請受付・電子交付・コンビニ交付の実施	・令和6年3月31日以前の接種記録の管理 ・令和6年3月31日以前の新型コロナウイルス感染症予防接種証明書の交付に係る接種記録の照会	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正

令和6年4月30日	Ⅰ　基本情報 1．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7 ③他のシステムとの接続	[○] 住民基本台帳ネットワークシステム	[　] 住民基本台帳ネットワークシステム	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅰ　基本情報 5．個人番号の利用 法令上の根拠	・番号法第19条第16号（新型コロナウイルス感染症対策に係る予防接種事務におけるワクチン接種記録システム(VRS)を用いた情報提供・照会のみ）	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和8年1月13日	表紙 評価書名	予防接種法による予防接種の実施に関する事務	予防接種の実施に関する事務	事後	評価書統合による修正
令和8年1月13日	表紙 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。	横浜市は、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。	事後	評価書統合による修正
令和8年1月13日	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	予防接種の実施に関する事務	事後	評価書統合による修正

令和8年1月13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	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。 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。	(1)予防接種法(昭和23年法律第68号)による予防接種の実施について 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。 ・横浜市ではA類(こども)及びB類(高齢者)の成人用肺炎球菌及び帯状疱疹、新型コロナウイルスワクチン(臨時接種分)の接種記録をシステムにて管理している。 ・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。 ・A類(こども)の対象者及びB類(高齢者)の成人用肺炎球菌及び帯状疱疹の対象者に対しては個別に通知を送付している。 ・健康被害救済給付に係る事務は紙の書類やデータで行う。 ・接種者からの申請に基づき、新型コロナウイルスワクチン(臨時接種分)の予防接種証明証の交付を行う。 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(平成25年法律第27号。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。 (2)新型インフルエンザ等対策特別措置法(平成24年法律第31号。以下、「特措法」という。)による予防接種の実施について 特措法及び番号法の規定に従い、特定個人情報は(1)と同様の事務に利用する。	事後	評価書統合による修正

令和8年1月13日	Ⅰ　基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム3 ②システムの機能	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民記録システムとの間で情報照会内容、情報提供内容、特定個人情報（連携対象）、符号取得のための情報等について連携するための機能。 (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、対応する。 (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。	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民基本台帳ネットワーク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、対応する。 (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。	事後	誤字、脱字等の修正、表現の軽微な修正
令和8年1月13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8 ①システムの名称	ワクチン接種記録システム（VRS）	（削除）	事後	重複による削除
令和8年1月13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8 ②システムの機能	・令和6年3月31日以前の接種記録の管理 ・令和6年3月31日以前の新型コロナウイルス感染症予防接種証明書の交付に係る接種記録の照会	（削除）	事後	重複による削除

令和8年1月13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8 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（　　）	（削除）	事後	重複による削除
令和8年1月13日	Ⅰ　基本情報 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	(1) 予防接種関係情報ファイル (2) 統合番号連携ファイル	事後	表現の軽微な修正
令和8年1月13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	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8号及び第9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。	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8号及び第9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	表現の軽微な修正
令和8年1月13日	Ⅰ　基本情報 4. 特定個人情報ファイルを取り扱う理由 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。	(1)予防接種関係情報ファイル ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅰ　基本情報 5. 個人番号の利用	・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 ・番号法第19条第16号（新型コロナウイルス感染症対策に係る予防接種事務におけるワクチン接種記録システム(VRS)を用いた情報提供・照会のみ） ・番号法第19条第6号(委託先への提供)	・番号法第9条第1項　別表の14項、126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の主務省令で定める事務を定める命令（平成26年内閣府・総務省令第5号。以下、「主務省令」という。）第10条、第67条の2 ・番号法第19条第6号(委託先への提供)	事後	番号法改正及び評価書統合に伴う修正
令和8年1月13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	【情報提供】 番号法第19条第8号　別表第2　16の2項、3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8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	【情報提供】 ・行政手続における特定の個人を識別するための番号の利用等に関する法律第十九条第八号に基づく利用特定個人情報の提供に関する命令（令和6年デジタル庁・総務省令第9号）第2条の表25、26、153、154の項 【情報照会】 ・行政手続における特定の個人を識別するための番号の利用等に関する法律第十九条第八号に基づく利用特定個人情報の提供に関する命令（令和6年デジタル庁・総務省令第9号）第2条の表25、27、28、29、153の項	事後	番号法改正及び評価書統合に伴う修正

令和8年1月13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	（1）予防接種法（昭和23年法律第68号）による予防接種の実施について 　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。 ・横浜市ではA類(こども)及びB類（高齢者）の成人用肺炎球菌及び帯状疱疹、新型コロナウイルスワクチン（臨時接種分）の接種記録をシステムにて管理している。 ・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。 ・A類（こども）の対象者及びB類（高齢者）の成人用肺炎球菌及び帯状疱疹の対象者に対しては個別に通知を送付している。 ・健康被害救済給付に係る事務は紙の書類やデータで行う。 ・接種者からの申請に基づき、新型コロナウイルスワクチン（臨時接種分）の予防接種証明証の交付を行う。 　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(平成25年法律第27号。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。 （2）新型インフルエンザ等対策特別措置法（平成24年法律第31号。以下、「特措法」という。）による予防接種の実施について 　特措法及び番号法の規定に従い、特定個人情報は（1）と同様の事務に利用する。	（1）予防接種法（昭和23年法律第68号）による予防接種の実施について 　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。 ・横浜市ではA類（こども）及びB類（高齢者）の成人用肺炎球菌及び帯状疱疹、新型コロナウイルスワクチン（臨時接種分）の接種記録をシステムにて管理している。 ・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。 ・A類（こども）の対象者及びB類（高齢者）の成人用肺炎球菌及び帯状疱疹の対象者に対しては個別に通知を送付している。 ・健康被害救済給付に係る事務は紙の書類やデータで行う。 ・接種者からの申請に基づき、新型コロナウイルスワクチン（臨時接種分）の予防接種証明証の交付を行う。 　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(平成25年法律第27号。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、団体内統合宛名システムを使用し、中間サーバーにアップロードを行う。 〇予防接種歴を宛名番号を利用して管理する。 （2）新型インフルエンザ等対策特別措置法（平成24年法律第31号。以下、「特措法」という。）による予防接種の実施について 　特措法及び番号法の規定に従い、特定個人情報は（1）と同様の事務に利用する。	事前	システム標準化による修正
令和8年1月13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 ①システムの名称	予防接種台帳システム	団体内統合宛名システム	事前	システム標準化による修正

令和8年1月13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	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。	団体内統合宛名システムは、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。 団体内統合宛名番号とは、本市において一意に個人を特定する番号のことをいう。 (1) 団体内統合宛名番号管理機能 　団体内統合宛名番号・個人番号・宛名番号・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) 宛名番号・団体内統合宛名番号変換機能 　団体内統合宛名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 　団体内統合宛名システムの利用者を認証し、権限を管理する機能。	事前	システム標準化による修正
令和8年1月13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	[　　] 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（　　）	[　　] 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）	事前	システム標準化による修正
令和8年1月13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2 ①システムの名称	統合番号連携システム	中間サーバー	事前	システム標準化による修正

令和8年1月13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2 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統合宛名番号のことをいう。 ⑴ 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。 ⑵ 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。 ⑶ 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。 ⑷ 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。 ⑸ 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。 ⑹ 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。 ⑺ 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。 ⑻ 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。 ⑼ 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。	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、団体内統合宛名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「団体内統合宛名番号」とを紐付け、その情報を保管・管理する機能。 (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、団体内統合宛名システム及び住民基本台帳ネットワーク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、対応する。 (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。	事前	システム標準化による修正
令和8年1月13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2 ③他のシステムとの接続	[　　] 情報提供ネットワークシステム [○] 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）	[○] 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（　　）	事前	システム標準化による修正
令和8年1月13日	Ⅰ　基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム3 ①システムの名称	中間サーバー	住民基本台帳ネットワークシステム	事前	システム標準化による修正

令和8年1月13日	Ⅰ　基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム3 ②システムの機能	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民基本台帳ネットワーク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、対応する。 (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。	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、次の機能のみ使用する。 (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。	事前	システム標準化による修正
令和8年1月13日	Ⅰ　基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム3 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（　　）	[　　] 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（　　）	事前	システム標準化による修正
令和8年1月13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	健康管理システム（予防接種分野）	事前	システム標準化による修正

令和8年1月13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4 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。	1　対象者管理機能 　宛名番号を含む、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。	事前	システム標準化による修正
令和8年1月13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4 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（　　）	[　　] 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（　　）	事前	システム標準化による修正
令和8年1月13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	情報共有基盤システム	ワクチン接種記録システム（VRS）	事前	システム標準化による修正
令和8年1月13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 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。	・令和6年3月31日以前の新型コロナウイルスワクチン接種記録の管理	事前	システム標準化による修正

令和8年1月13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 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 ）	[　　] 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（　　）	事前	システム標準化による修正
令和8年1月13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7 ①システムの名称	ワクチン接種記録システム（VRS）	（削除）	事前	システム標準化による修正
令和8年1月13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7 ②システムの機能	・令和6年3月31日以前の接種記録の管理 ・令和6年3月31日以前の新型コロナウイルス感染症予防接種証明書の交付に係る接種記録の照会	（削除）	事前	システム標準化による修正
令和8年1月13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7 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（　　）	（削除）	事前	システム標準化による修正
令和8年1月13日	Ⅰ　基本情報 3. 特定個人情報ファイル名	(1) 予防接種関係情報ファイル (2) 統合番号連携ファイル	(1) 予防接種関係情報ファイル (2) 団体内統合宛名ファイル	事前	システム標準化による修正
令和8年1月13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	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8号及び第9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。	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) 団体内統合宛名ファイル ・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。	事前	システム標準化による修正

令和8年1月13日	Ⅰ　基本情報 4. 特定個人情報ファイルを取り扱う理由 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。	(1)予防接種関係情報ファイル 　・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) 団体内統合宛名ファイル 　・団体内統合宛名番号・個人番号・宛名番号・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。	事前	システム標準化による修正

（別紙）全項目評価書の変更箇所 【別添1（事務内容）】

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
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
令和4年6月28日	（別添1）事務内容 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	（追加）	【新型コロナの予防接種事務】 ①特定個人情報ファイル（CSVファイル）の登録（従来の予防接種事務①に代わるプロセス） ②住民記録システムより接種対象者へ接種券（予診票）を通知 ③医療機関（接種会場）にて接種券上のOCRラインの読み込み、又は手入力にて接種記録をVRSへ登録 ④他市町村からの照会に応じて接種記録を提供 ⑤他市町村が保有する予防接種歴情報を照会 ⑥VRSから出力した接種記録を予防接種台帳システムに登録 ⑦新型コロナウイルス感染症予防接種証明書の交付の申請（接種記録を照会するために、個人番号を入手し使用） ⑧接種記録を照会し、旅券情報を入力後交付 【電子証明書（アプリ）の事務】 ①市民が予防接種証明書の電子交付アプリにて電子証明書を申請 ②接種者から個人番号を入手し、接種記録をVRSに照会 ③接種記録を氏名や旅券関係情報等、その他の情報とあわせて接種証明書を作成 ④作成した接種証明書をアプリ上に表示	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和5年8月4日	（別添1）事務内容 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	（追加）	【証明書のコンビニ交付の事務】 ⑤市民がコンビニエンスストア等のキオスク端末からマイナンバーカード券面入力補助APを利用して、証明書交付センターシステムを経由し接種記録を照会 ⑥接種記録の情報を、氏名や旅券関係情報等とあわせ接種証明書をキオスク端末から発行（個人番号は表示されない。接種証明書には電子署名を付す）※旅券関係情報は、過去の接種証明書の発行履歴に記録された情報を表示	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和6年4月30日	（別添1）事務内容 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	【新型コロナの予防接種事務】 ①特定個人情報ファイル（CSVファイル）の登録（従来の予防接種事務①に代わるプロセス） ②住民記録システムより接種対象者へ接種券（予診票）を通知 ③医療機関（接種会場）にて接種券上のOCRラインの読み込み、又は手入力にて接種記録をVRSへ登録 ④他市町村からの照会に応じて接種記録を提供 ⑤他市町村が保有する予防接種歴情報を照会 ⑥VRSから出力した接種記録を予防接種台帳システムに登録 ⑦新型コロナウイルス感染症予防接種証明書の交付の申請（接種記録を照会するために、個人番号を入手し使用） ⑧接種記録を照会し、旅券情報を入力後交付 【電子証明書（アプリ）の事務】 ①市民が予防接種証明書の電子交付アプリにて電子証明書を申請 ②接種者から個人番号を入手し、接種記録をVRSに照会 ③接種記録を氏名や旅券関係情報等、その他の情報とあわせて接種証明書を作成 ④作成した接種証明書をアプリ上に表示 【証明書のコンビニ交付の事務】 ⑤市民がコンビニエンスストア等のキオスク端末からマイナンバーカード券面入力補助APを利用して、証明書交付センターシステムを経由し接種記録を照会 ⑥接種記録の情報を、氏名や旅券関係情報等とあわせ接種証明書をキオスク端末から発行（個人番号は表示されない。接種証明書には電子署名を付す） ※旅券関係情報は、過去の接種証明書の発行履歴に記録された情報を表示	【新型コロナの予防接種事務】 ①VRSから出力した接種記録を予防接種台帳システムに登録 ②新型コロナウイルス感染症予防接種証明書の発行	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和8年1月13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	従来の予防接種の事務	（削除）	事後	実態に基づく削除
令和8年1月13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	新型コロナの予防接種事務	（削除）	事後	実態に基づく削除

令和8年1月13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	住基ネット総合端末	住基ネット統合端末	事後	誤字、脱字等の修正、表現の軽微な修正
令和8年1月13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	住基システム	住記システム	事後	誤字、脱字等の修正、表現の軽微な修正
令和8年1月13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	各区福祉保健課	各区福祉保健課 医療局健康安全課	事後	誤字、脱字等の修正、表現の軽微な修正
令和8年1月13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接種記録の反映	（削除）	事後	実態に基づく削除
令和8年1月13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	②予防接種証明書の発行	⑩予防接種証明書の発行	事後	実態に基づく修正
令和8年1月13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住基情報 ②接種券通知 ③費用免除に係る確認書類 （接種費用免除対象者のみ） ④費用免除に係る確認回答 （接種費用免除対象者のみ） ⑤接種 ⑥接種費用免除 （接種費用免除対象者のみ）	住基情報 接種券通知 ①費用免除に係る確認書類 （接種費用免除対象者のみ） ②費用免除に係る確認回答 （接種費用免除対象者のみ） ③接種 ④接種費用免除 （接種費用免除対象者のみ）	事後	表現の軽微な修正

令和8年1月13日	（別添1）事務の内容 （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	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 【従来の予防接種事務】 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総合端末を利用して検索 ⑦ 予防接種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 ⑧ 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 ⑨ 接種記録統計を厚生労働省へ報告 【新型コロナの予防接種事務】 ① VRSから出力した接種記録を健康管理システムに登録 ② 新型コロナウイルス感染症予防接種証明書の発行	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 【予防接種事務】 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統合端末を利用して検索 ⑦ 予防接種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 ⑧ 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 ⑨ 接種記録統計を厚生労働省へ報告 ⑩ 令和6年3月31日以前の新型コロナウイルス感染症予防接種証明書の発行 ※ ワクチン記録システム（VRS）は、特定個人情報ファイルを保有しているのみです。	事後	実態に基づく修正
令和8年1月13日	（別添1）事務の内容 （備考） 〇予防接種の実費徴収の有無の確認に関する事務	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 税務システムが保有する税情報を、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、団体内統合宛名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	〇予防接種の実費徴収の有無の確認に関する事務 ① 免除確認資料が無い上で、接種費用免除を希望する場合、各区福祉保健課・健康安全課の予防接種窓口にて免除の可否確認を申請 ② 税務システムが保有する税情報を、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 ③ 接種対象者が予防接種協力医療機関を受診 ④ 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	事後	表現の軽微な修正

令和8年1月13日	（別添1）事務の内容 （備考） 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	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、厚生労働省に進達する 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	事後	実態に基づく修正
令和8年1月13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	予防接種台帳システム	健康管理システム（予防接種分野）	事前	システム標準化による修正
令和8年1月13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	統合番号連携システム	団体内統合宛名システム	事前	システム標準化による修正
令和8年1月13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	統合番号連携システム	団体内統合宛名システム	事前	システム標準化による修正
令和8年1月13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	基幹系システム	（削除）	事前	表現の軽微な修正
令和8年1月13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	情報共有基盤システム	（削除）	事前	表現の軽微な修正
令和8年1月13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	統合番号連携システム	団体内統合宛名システム	事前	システム標準化による修正

令和8年1月13日	（別添1）事務の内容 （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	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 【予防接種事務】 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統合端末を利用して検索 ⑦ 予防接種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 ⑧ 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 ⑨ 接種記録統計を厚生労働省へ報告 ⑩ 令和6年3月31日以前の新型コロナウイルス感染症予防接種証明書の発行 ※ ワクチン記録システム（VRS）は、特定個人情報ファイルを保有しているのみです。	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 【予防接種事務】 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、接種歴を健康管理システム（予防接種分野）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統合端末を利用して検索 ⑦ 予防接種歴を団体内統合宛名システム経由で中間サーバーへ副本提供 ⑧ 他市町村が保有する予防接種歴情報を、団体内統合宛名システム経由で中間サーバーへ照会 ⑨ 接種記録統計を厚生労働省へ報告 ⑩ 令和6年3月31日以前の新型コロナウイルス感染症予防接種証明書の発行 ※ ワクチン記録システム（VRS）は、特定個人情報ファイルを保有しているのみです。	事前	システム標準化による修正
令和8年1月13日	（別添1）事務の内容 （備考） 〇予防接種の実費徴収の有無の確認に関する事務	〇予防接種の実費徴収の有無の確認に関する事務 ① 免除確認資料が無い上で、接種費用免除を希望する場合、各区福祉保健課・健康安全課の予防接種窓口にて免除の可否確認を申請 ② 税務システムが保有する税情報を、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ーへ照会し、免除の可否を回答 ③ 接種対象者が予防接種協力医療機関を受診 ④ 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	〇予防接種の実費徴収の有無の確認に関する事務 ① 免除確認資料が無い上で、接種費用免除を希望する場合、各区福祉保健課・健康安全課の予防接種窓口にて免除の可否確認を申請 ② 税務システムが保有する税情報を、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、団体内統合宛名システム経由で中間サーバーへ照会し、免除の可否を回答 ③ 接種対象者が予防接種協力医療機関を受診 ④ 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	事前	システム標準化による修正
令和8年1月13日	（別添1）事務の内容 （備考） 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、厚生労働省に進達する 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	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、厚生労働省に進達する 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団体内統合宛名システム経由で中間サーバーへ照会する	事前	システム標準化による修正

（別紙）全項目評価書の変更箇所 【Ⅱファイルの概要（予防接種関係情報ファイル）】

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 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
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
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
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	（追加）	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

令和3年6月15日	Ⅱ　ファイルの概要 （予防接種対象者関係情報ファイル） 5. 特定個人情報の提供・移転（委託に伴うものは除く。） 提供先1 ①法令上の根拠	番号法別表第二　16の2	番号法別表第二　16の2、16の3	事後	必要な記載の追加
令和4年6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	[　]その他（　　）	[○]その他（ワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。））	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6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。 （追加） ◎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。 （追加）	◎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。 　・転入時に転出元市区町村への接種記録の照会が必要になる都度入手する。 　（転入者本人から個人番号の提供の同意が得られた場合のみ） 　・転出先市区町村から接種記録の照会を受ける都度入手する。 ◎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。 <新型コロナウイルス感染症対策に係る予防接種事務における追加措置> 　・転入時に転出元市区町村への接種記録の照会が必要になる都度 　・転出先市区町村から接種記録の照会を受ける都度 　・新型コロナウイルス感染症予防接種証明書の交付のため、接種者から交付申請があった場合であって接種記録の照会が必要になる都度	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　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	・転出先市区町村から接種記録の照会を受ける都度	・他市区町村から接種記録の照会を受ける都度	事後	誤字、脱字等の修正、表現の軽微な修正

令和4年6月28日	Ⅱ　ファイルの概要（予防接種対象者） 3. 特定個人情報の入手・使用 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。 （追加）	・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。 〈新型コロナウイルス感染症対策に係る予防接種事務における追加措置〉 ・本市への転入者について、転出元市区町村へ接種記録を照会し、提供を受ける場合のみ入手する。（番号法第19条第16号） ・本市からの転出者について、転出先市区町村へ本市での接種記録を提供するために、転出先市区町村から個人番号を入手する。（番号法第19条第16号） ・新型コロナウイルス感染症予防接種証明書の交付のため、接種者から交付申請があった場合のみ入手する。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　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 ④入手に係る妥当性	・本市からの転出者について、転出先市区町村へ当市区町村での接種記録を提供するために、転出先市区町村から個人番号を入手する。（番号法第19条第15号）	本市からの転出者について、転出先市区町村へ当市区町村での接種記録を提供するために、他市区町村から個人番号を入手する。（番号法第19条第16号）	事後	誤字、脱字等の修正、表現の軽微な修正
令和4年6月28日	Ⅱ　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	（追加）	・本市への転入者について接種者からの同意を得て入手する。 ・接種者からの接種証明書の交付申請に合わせて本人から入手する。 ・電子交付アプリにより電子申請を受付ける場合においては、利用規約を表示し、同意を得てから入手する。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　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 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。 （追加）	・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。 ・本市への転入者について、転出元市区町村へ接種記録を照会するために特定個人情報を使用する。 ・本市からの転出者について、転出先市区町村へ本市での接種記録を提供するために特定個人情報を使用する。 〈新型コロナウイルス感染症対策に係る予防接種事務における追加措置〉 　・本市への転入者について、転出元市区町村へ接種記録を照会するとともに、接種券の発行のために特定個人情報を使用する。 　・本市からの転出者について、転出先市区町村へ本市での接種記録を提供するために特定個人情報を使用する。 　・新型コロナウイルス感染症予防接種証明書の交付の際、接種記録を照会するために特定個人情報を使用する。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　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 ⑧使用方法 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。 （追加）	・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。 ・本市からの転出者について、本市での接種記録を転出先市区町村に提供するために、転出先市区町村から個人番号を入手し、本市の接種記録と突合する。 （転出先市区町村にて、本人から個人番号の提供に関して同意が得られた場合のみ当処理を行う。）	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和4年6月28日	Ⅱ　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 ⑧使用方法　情報の突合	当市区町村からの転出者について、当市区町村での接種記録を転出先市区町村に提供するために、転出先市区町村から個人番号を入手し、当市区町村の接種記録と突合する。	本市からの転出者について、本市での接種記録を転出先市区町村に提供するために、他市区町村から個人番号を入手し、本市の接種記録と突合する。	事後	誤字、脱字等の修正、表現の軽微な修正
令和4年6月28日	Ⅱ　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 ⑧使用方法 情報の統計分析	（追加）	＜新型コロナウイルス感染症対策に係る予防接種事務＞ 特定の個人を判別するような情報の統計や分析は行わない。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　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 委託の有無	（　３　）件	（　４　）件	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　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 ②取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の数	[　10万人以上100万人未満　]	[　100万人以上1,000万人未満　]	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　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	日本通信紙株式会社	日本通信紙株式会社、トッパン・フォームズ株式会社	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　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 ⑥委託先名	株式会社アシスト	株式会社横浜電算、株式会社システム情報センター	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　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4	（追加）	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）を用いた特定個人情報ファイルの管理等	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用

令和4年6月28日	Ⅱ　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4 ①委託内容	（追加）	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）を用いた特定個人情報ファイルの管理等	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　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4 ②取扱いを委託する特定個人情報ファイルの範囲	（追加）	[　特定個人情報ファイルの一部　]	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　ファイルの概要（予防接種対象者） 4．特定個人情報ファイルの取扱いの委託 委託事項4 ②取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の数	（追加）	[　100万人以上1,000万人未満　]	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　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4 ②取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の範囲	（追加）	予防接種法等関連法令に定められる予防接種の対象者	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　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4 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	（追加）	ワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）を用いた特定個人情報ファイルの適切な管理等のために取り扱う必要がある。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　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4 ③委託先における取扱者数	（追加）	[　10人以上50人未満　]	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用

令和4年6月28日	Ⅱ　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4 ④委託先への特定個人情報ファイルの提供方法	（追加）	[　〇　]その他　（LG-WAN回線を用いた提供（VRS本体）、本人からの電子交付アプリを用いた提供（新型コロナウイルス感染症予防接種証明書電子交付機能））	事後	特定個人情報保護評価に関する規則第９条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　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4 ⑤委託先名の確認方法	（追加）	下記、「⑥委託者名」の項の記載より確認できる。	事後	特定個人情報保護評価に関する規則第９条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　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4 ⑥委託先名	（追加）	株式会社ミラボ	事後	特定個人情報保護評価に関する規則第９条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　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4 ⑦再委託の有無	（追加）	[　再委託しない　]	事後	特定個人情報保護評価に関する規則第９条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　ファイルの概要（予防接種対象者関係情報ファイル） 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	[　〇　]提供を行っている （　１　）件	[　〇　]提供を行っている （　２　）件	事後	特定個人情報保護評価に関する規則第９条第2項の規定（緊急時事後評価）の適用

令和4年6月28日	Ⅱ　ファイルの概要（予防接種対象者関係情報ファイル） 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 提供先2	（追加）	市区町村長	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　ファイルの概要（予防接種対象者関係情報ファイル） 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 提供先2 ①法令上の根拠	（追加）	番号法　第19条第16号	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　ファイルの概要（予防接種対象者関係情報ファイル） 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 提供先2 ②提供先における用途	（追加）	新型コロナウイルス感染症対策に係る予防接種事務	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　ファイルの概要（予防接種対象者関係情報ファイル） 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 提供先2 ③提供する情報	（追加）	市区町村コード及び転入者の個人番号（本人からの同意が得られた場合のみ）	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　ファイルの概要（予防接種対象者関係情報ファイル） 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 提供先2 ④提供する情報の対象となる本人の数	（追加）	[　100万人以上1,000万人未満　]	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和4年6月28日	Ⅱ　ファイルの概要（予防接種対象者関係情報ファイル） 5．特定個人情報の提供・移転（委託に伴うものを除く。） 提供先2 ⑤提供する情報の対象となる本人の範囲	（追加）	「2.基本情報　③対象者となる本人の範囲」と同じ	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　ファイルの概要（予防接種対象者） 5．特定個人情報の提供・移転（委託に伴うものを除く。） 提供先2 ⑥提供方法	（追加）	[　〇　]その他（ワクチン接種記録システム（VRS））	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　ファイルの概要（予防接種対象者関係情報ファイル） 5．特定個人情報の提供・移転（委託に伴うものを除く。） 提供先2 ⑦時期・頻度	（追加）	本市への転入者について、転出元市区町村へ接種記録の照会を行う必要性が生じた都度	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅱ　ファイルの概要（予防接種対象者） 6．特定個人情報の保管・消去 ①保管場所	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用している。なお、以下のとおりのセキュリティ対策を講じている。 ・論理的に区分された本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。 ・日本国内にデータセンターが存在するクラウドサービスを利用している。 （新型コロナウイルス感染症予防接種証明書電子交付機能） 電子交付アプリ及び同アプリの利用端末には、申請情報を記録しないこととしている。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和4年6月28日	Ⅱ　ファイルの概要（予防接種対象者） 6. 特定個人情報の保管・消去 ③消去方法	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ ・自機関の領域に保管されたデータのみ、ワクチン接種記録システム(VRS)を用いて消去することができる。 ・自機関の領域に保管されたデータは、他機関から消去できない。 ※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、消去することができない。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和5年8月4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） 2. 基本情報 ⑥事務担当部署	健康福祉局健康安全課	医療局健康安全部健康安全課	事後	組織再編による修正
令和5年8月4日	Ⅱ　特定個人情報ファイルの概要（予防接種対象者） 3. 特定個人情報の入手・使用 ②入手方法	ワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）	ワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）、コンビニエンスストア等のキオスク端末及び証明書交付センターシステム	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅱ　特定個人情報ファイルの概要（予防接種対象者） 3. 特定個人情報の入手・使用 ⑤本人への明示	・電子交付アプリにより電子申請を受付ける場合においては、利用規約を表示し、同意を得てから入手する。	・電子交付アプリにより予防接種証明書の電子申請を受付ける場合及びコンビニエンスストア等のキオスク端末から予防接種証明書の申請を受け付ける場合においては、利用規約を表示し、同意を得てから入手する。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅱ　特定個人情報ファイルの概要（予防接種対象者） 3. 特定個人情報の入手・使用 ⑦使用の主体　使用部署	健康福祉局健康安全課	医療局健康安全部健康安全課	事後	組織再編による修正
令和5年8月4日	Ⅱ　特定個人情報ファイルの概要（予防接種対象者） 4. 特定個人情報ファイルの取扱いの委託 委託事項4	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）を用いた特定個人情報ファイルの管理等	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）を用いた特定個人情報ファイルの管理等	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅱ　特定個人情報ファイルの概要（予防接種対象者） 4. 特定個人情報ファイルの取扱いの委託 委託事項4 ①委託内容	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）を用いた特定個人情報ファイルの管理等	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）を用いた特定個人情報ファイルの管理等	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用

令和5年8月4日	Ⅱ　特定個人情報ファイルの概要（予防接種対象者） 4．特定個人情報ファイルの取扱いの委託 委託事項4 ②取扱いを委託する特定個人情報ファイルの範囲 その妥当性	ワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）を用いた特定個人情報ファイルの適切な管理等のために取り扱う必要がある。	ワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）を用いた特定個人情報ファイルの適切な管理等のために取り扱う必要がある。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅱ　特定個人情報ファイルの概要（予防接種対象者） 4．特定個人情報ファイルの取扱いの委託 委託事項4 ④委託先への特定個人情報ファイルの提供方法	LG-WAN回線を用いた提供（VRS本体）、本人からの電子交付アプリを用いた提供（新型コロナウイルス感染症予防接種証明書電子交付機能）	LG-WAN回線を用いた提供（VRS本体、コンビニ交付関連機能）、本人からの電子交付アプリを用いた提供（新型コロナウイルス感染症予防接種証明書電子交付機能）	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅱ　特定個人情報ファイルの概要（予防接種対象者） 6．特定個人情報の保管・消去 ①保管場所	（追加）	（新型コロナウイルス感染症予防接種証明書コンビニ交付） ・証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和6年4月30日	Ⅱ　特定個人情報ファイルの概要 3．特定個人情報の入手・使用 ②入手方法	[○] その他 ワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）、コンビニエンスストア等のキオスク端末及び証明書交付センターシステム	[　] その他	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅱ　特定個人情報ファイルの概要 3．特定個人情報の入手・使用 ③入手の時期・頻度	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ・転入時に転出元市区町村への接種記録の照会が必要になる都度 ・他市区町村から接種記録の照会を受ける都度 ・新型コロナウイルス感染症予防接種証明書の交付のため、接種者から交付申請があった場合で あって接種記録の照会が必要になる都度	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅱ　特定個人情報ファイルの概要 3．特定個人情報の入手・使用 ④入手に係る妥当性	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ・本市への転入者について、転出元市区町村へ接種記録を照会し、提供を受ける場合のみ入手する。 （番号法第19条第16号） ・本市からの転出者について、転出先市区町村へ本市での接種記録を提供するために、他市区町村から個人番号を入手する。 （番号法第19条第16号） ・新型コロナウイルス感染症予防接種証明書の交付のため、接種者から交付申請があった場合のみ入手する。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正

令和6年4月30日	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑤本人への開示	・接種者からの接種証明書の交付申請に合わせて本人から入手する。 ・電子交付アプリにより予防接種証明書の電子申請を受付ける場合及びコンビニエンスストア等のキオスク端末から予防接種証明書の申請を受け付ける場合においては、利用規約を表示し、同意を得てから入手する。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑧使用方法	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ・本市への転入者について、転出元市区町村へ接種記録を照会するとともに、接種券の発行のために特定個人情報を使用する。 ・本市からの転出者について、転出先市区町村へ本市での接種記録を提供するために特定個人情報を使用する。 ・新型コロナウイルス感染症予防接種証明書の交付の際、接種記録を照会するために特定個人情報を使用する。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑧使用方法 情報の突合	＜新型コロナウイルス感染症対策に係る予防接種事務＞ ・本市からの転出者について、本市での接種記録を転出先市区町村に提供するために、他市区町村から個人番号を入手し、本市の接種記録と突合する。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項4	（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項4　①委託内容	（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項4　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	（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項4　④委託先への特定個人情報ファイルの提供方法	LG-WAN回線を用いた提供（VRS本体、コンビニ交付関連機能）、本人からの電子交付アプリを用いた提供（新型コロナウイルス感染症予防接種証明書電子交付機能）	LG-WAN回線を用いた提供（VRS本体）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正

令和6年4月30日	Ⅱ　特定個人情報ファイルの概要 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 提供・移転の有無	2件	1件	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅱ　特定個人情報ファイルの概要 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 提供先2	①～⑦	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅱ　特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ①保管場所	（新型コロナウイルス感染症予防接種証明書電子交付機能） ・電子交付アプリ及び同アプリの利用端末には、申請情報を記録しないこととしている。 （新型コロナウイルス感染症予防接種証明書コンビニ交付） ・証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和8年1月13日	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	予防接種関係情報ファイル	事後	表現の軽微な修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 2. 基本情報 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	予防接種法又は特措法に基づく予防接種の対象者及び被接種者	事後	評価書統合による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 2. 基本情報 ③ 対象となる本人の範囲 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、接種対象者の接種記録を適正に管理・保管するために必要。	接種対象者であることの管理、被接種者の接種記録を適正に管理・保管するために必要。	事後	評価書統合による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 2. 基本情報 ④ 記録される項目	10項目以上50項目未満	50項目以上100項目以上	事後	評価書統合による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 2. 基本情報 ④ 記録される項目 その他妥当性	○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	○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 ○4情報（氏名、性別、生年月日、住所） ・予防接種法又は特措法に基づく接種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	事後	表現の軽微な修正

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ①　入手元	[○] 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)	[○] 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、デジタル統括本部住民情報基盤課) [　　] 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(市町村(特別区含む)) [　　] 民間事業者(　　) [○] その他(医療機関)	事後	表現の軽微な修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ③　入手の時期・頻度	◎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。 ・転入時に転出元市区町村への接種記録の照会が必要になる都度入手する。 ・転出先市区町村から接種記録の照会を受ける都度入手する。 ◎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。 ・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。 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。	◎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。 ・転入時に転出元市区町村への接種記録の照会が必要になる都度入手する。 ・転出先市区町村から接種記録の照会を受ける都度入手する。 ◎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。 ・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。 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。	事後	表現の軽微な修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ④　入手に係る妥当性	・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。	・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。 (予防接種法第9条の3、予防接種法施行規則第3条)	事後	表現の軽微な修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑤　本人への明示	・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。 ・本市への転入者について接種者からの同意を得て入手する。 ・接種者からの接種証明書の交付申請に合わせて本人から入手する。	・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条別表第14項又は126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8の項、及び別表第五の6の5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。 ・本市への転入者について接種者からの同意を得て入手する。 ・接種者からの接種証明書の交付申請に合わせて本人から入手する。	事後	評価書統合による修正

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 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	対象者の資格管理、被接種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	事後	表現の軽微な修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑦ 使用の主体 使用者数	10人未満	10人以上50人未満	事後	評価書統合による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑧ 使用方法 情報の統計分析	＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ 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。	人数等の集計分析は行うが、特定の個人を判別するような情報の統計や分析は行わない。	事後	表現の軽微な修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託の有無	[　委託する　] （　4　）件	[　委託する　] （　3　）件	事後	実態に基づく修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ② 取扱いを委託する特定個人情報ファイルの範囲 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	予防接種法又は特措法に基づく予防接種の対象者及び被接種者	事後	評価書統合による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ⑦ 再委託の有無	[　再委託する　]	[　再委託しない　]	事後	実態に基づく修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 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）	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 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	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ② 取扱いを委託する特定個人情報ファイルの範囲 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	・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 ・特措法に基づく接種対象者	事後	評価書統合による修正

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 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。 ）	[　　] 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等を利用し、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。 ）	事後	実態に基づく修正・表現の軽微な修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ⑥ 委託先名	日本通信紙株式会社、トッパン・フォームズ株式会社	日本通信紙株式会社（ただし、特措法に基づく予防接種は今後入札等により業者を選択する）	事後	評価書統合による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 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）	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、個人情報の保護に関する法律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6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7条（再委託の禁止等）	事後	委託契約約款等の改正による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 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	印刷工場から郵便局までの運搬	事後	実態に基づく修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項3 ② 取扱いを委託する特定個人情報ファイルの範囲 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	・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 ・特措法に基づく接種対象者	事後	評価書統合による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項3 ⑥ 委託先名	株式会社横浜電算、株式会社システム情報センター	株式会社横浜電算（ただし、特措法に基づく予防接種は、今後入札等により業者を選定する）	事後	評価書統合による修正

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項4	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム（VRS)を用いた特定個人情報ファイルの管理等	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項4 ①　委託内容	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム（VRS)を用いた特定個人情報ファイルの管理等	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項4 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　] [　100万人以上1,000万人未満　] 予防接種法等関連法令に定められる予防接種の対象者 ワクチン接種記録システム（VRS）を用いた特定個人情報ファイルの適切な管理等のために取り扱う必要がある。	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項4 ③　委託先における取扱者数	[　10人以上50人未満　]	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項4 ④　委託先への特定個人情報ファイルの提供方法	[　　]専用線 [　　]電子メール [　　]電子記録媒体（フラッシュメモリを除く。） [　　]フラッシュメモリ [　　]紙 [○]その他（　LG-WAN回線を用いた提供（VRS本体）　）	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項4 ⑤　委託先名の確認方法	下記、「⑥委託者名」の項の記載より確認できる。	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項4 ⑥　委託先名	株式会社ミラボ	（削除）	事後	実態に基づく削除

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項4 ⑦ 再委託の有無	[再委託しない]	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 提供先1 ① 法令上の根拠	都道府県知事又は市町村長	厚生労働大臣、都道府県知事又は市町村長	事後	評価書統合による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 提供先1 ① 法令上の根拠	番号法別表第二　16の2、16の3	番号法第19条　別表第14項、第126項	事後	番号法改正及び評価書統合に伴う変更
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 提供先1 ② 提供先における用途	予防接種法による予防接種の実施に関する事務であって、主務省令で定めるもの	予防接種法又は特措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	事後	評価書統合による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 提供先1 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]	[100万人以上1,000万人未満]	事後	評価書統合による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 提供先1 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	予防接種法又は特措法に基づく予防接種の接種履歴がある他市町村への転出者	事後	評価書統合による修正

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ①　保管場所	＜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いる。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ②特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。 ＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用している。なお、以下のとおりのセキュリティ対策を講じている。 ・論理的に区分された本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。 ・日本国内にデータセンターが存在するクラウドサービスを利用している。	＜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＞ ・中間サーバー･プラットフォームはデータセンターに設置している。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ・特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。	事後	実態に基づく修正

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ③ 消去方法	＜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。 ＜ワクチン接種記録システム(VRS)における追加措置＞ ・自機関の領域に保管されたデータのみ、ワクチン接種記録システム(VRS)を用いて消去することができる。 ・自機関の領域に保管されたデータは、他機関から消去できない。 ※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、 消去することができない。	＜横浜市における措置＞ ・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＞ ・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。 ・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。	事後	実態に基づく修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑧ 使用方法	・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。 ・本市への転入者について、転出元市区町村へ接種記録を照会するとともに、接種券の発行のために特定個人情報を使用する。 ・本市からの転出者について、転出先市区町村へ本市での接種記録を提供するために特定個人情報を使用する。	・接種記録の管理・保管 　健康管理システム（予防接種分野）に接種記録を登録し、接種記録の管理及び保管を行う。 ・本市への転入者について、転出元市区町村へ接種記録を照会するとともに、接種券の発行のために特定個人情報を使用する。 ・本市からの転出者について、転出先市区町村へ本市での接種記録を提供するために特定個人情報を使用する。	事前	システム標準化による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1	予防接種台帳システムの運用・保守	健康管理システム（予防接種分野）の運用・保守	事前	システム標準化による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 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。	健康管理システム（予防接種分野）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。	事前	システム標準化による修正

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ②　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（　サーバー室内おけるシステムの直接操作　）	[　　]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（　保守センター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り扱いを行う。　）	事前	システム標準化による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項3 ②　取扱いを委託する特定個人情報ファイルの範囲 その妥当性	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。	データ化した接種対象者の接種記録を健康管理システム（予防接種分野）に取り込むため。	事前	システム標準化による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ①　保管場所	＜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いる。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 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。	＜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いる。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 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。 ＜ガバメントクラウドにおける措置＞ ○サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27018の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ○特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。	事前	システム標準化による修正

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ③ 消去方法	＜横浜市における措置＞ ・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。	＜横浜市における措置＞ ・電子データ：国が定めた保存年限が経過した後、健康管理システム（予防接種分野）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。 ＜ガバメントクラウドにおける措置＞ 〇特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 〇クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 〇既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。	事前	システム標準化による修正

（別紙）全項目評価書の変更箇所 【Ⅱファイルの概要（団体内統合宛名ファイル）】

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
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
令和4年6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 ③対象となる本人の範囲 その必要性	・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。	・番号法第19条第8号及び第9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。	事後	号ずれによる軽微な修正
令和5年8月4日	Ⅱ　特定個人情報ファイルの概要（統合番号連携） 2．基本情報 ⑥事務担当部署	健康福祉局健康安全課	医療局健康安全部健康安全課	事後	組織再編による修正
令和5年8月4日	Ⅱ　特定個人情報ファイルの概要（統合番号連携） 3．特定個人情報の入手・使用 ⑦使用の主体　使用部署	健康福祉局健康安全課	医療局健康安全部健康安全課	事後	組織再編による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 2．基本情報 ⑥　事務担当部署	医療局健康安全課 各区福祉保健センター福祉保健課健康づくり係	医療局健康安全部健康安全課 各区福祉保健センター福祉保健課健康づくり係	事後	表現の軽微な修正

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑤ 本人への明示	・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。	・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条別表第14項又は126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8の項、及び別表第五の6の5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。 ・本市への転入者について接種者からの同意を得て入手する。 ・接種者からの接種証明書の交付申請に合わせて本人から入手する。	事後	評価書統合による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 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	被接種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	事後	表現の軽微な修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑦ 使用の主体 使用部署	医療局健康安全課、各区役所福祉保健センター福祉保健課	医療局健康安全部健康安全課、各区役所福祉保健センター福祉保健課、デジタル統括本部住民情報基盤課	事後	表現の軽微な修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑦ 使用の主体 使用者数	50人以上100人未満	100人以上500人未満	事後	実態に基づく修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託の有無	[委託する] (3)件	[委託する] (1)件	事後	実態に基づく修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ⑦ 再委託の有無	[再委託する]	[再委託しない]	事後	実態に基づく修正

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 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）	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ⑨ 再委託事項	システム運用保守支援業務	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2	オペレーション業務委託	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 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。	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ② 取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の数 対象となる本人の範囲 その妥当性	特定個人情報ファイルの全体 100万人以上1,000万人未満 特定個人情報ファイルの対象者の範囲と同様 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。	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ③ 委託先における取扱者数	10人以上50人未満	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 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。 ）	（削除）	事後	実態に基づく削除

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 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。	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ⑥ 委託先名	株式会社SH-Net	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ⑦ 再委託の有無	[再委託する]	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 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）	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ⑨ 再委託事項	オペレーション支援業務	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項3	データ保管業務委託	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項3 ① 委託内容	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。	（削除）	事後	実態に基づく削除

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項3 ②　取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の数 対象となる本人の範囲 その妥当性	特定個人情報ファイルの全体 100万人以上1,000万人未満 特定個人情報ファイルの対象者の範囲と同様 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。	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項3 ③　委託先における取扱者数	10人以上50人未満	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項3 ④　委託先への特定個人情報ファイルの提供方法	[　　]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（　　）	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項3 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。	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項3 ⑥　委託先名	未定	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項3 ⑦　再委託の有無	[再委託する]	（削除）	事後	実態に基づく削除

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項3 ⑧ 再委託の許諾方法	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）	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項3 ⑨ 再委託事項	データ保管支援業務	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ① 保管場所	＜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いる。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 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。	＜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。 ・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＞ ・中間サーバー・プラットフォームはデータセンターに設置している。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ・特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。	事後	表現の軽微な修正

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ③ 消去方法	＜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、保守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で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、裁断また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。	＜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、保守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で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、裁断また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＞ ・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。 ・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。	事後	表現の軽微な修正
令和8年1月13日	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	団体内統合宛名ファイル	事前	システム標準化による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 2. 基本情報 ④ 記録される項目 主な記録項目 ・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（　　）	[　　] 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（ 自動応答不可フラグ　　）	事前	システム標準化による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 2. 基本情報 ④ 記録される項目 その妥当性	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。	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：団体内統合宛名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。	事前	システム標準化による修正

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 3．特定個人情報の入手・使用 ③　入手の時期・頻度	◎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 　〇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。 　〇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。 　〇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。	横浜市住民記録システムが管理する特定個人情報に変更が生じた都度、入手します。 市民から直接特定個人情報の入手は行わず、横浜市住民記録システムで管理する特定個人情報に変更が生じた都度、情報連携を行っています。	事前	システム標準化による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 3．特定個人情報の入手・使用 ④　入手に係る妥当性	◎住民登録内の者の分：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の最新の情報を取得する。	個人番号の管理、特定個人情報の照会及び提供等の業務を行うために必要です。 横浜市住民記録システム、中間サーバーと連携し、個人番号の管理、特定個人情報の照会及び提供等の業務を行うシステムです。 横浜市住民記録システムが取得、管理した特定個人情報ファイルから、個人番号の管理、特定個人情報の照会及び提供等の業務で使用する内容に限定して連携することで、必要最小限の情報を保存しています。 なお、住民基本台帳事務では市民から直接特定個人情報を入手しません。	事前	システム標準化による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 3．特定個人情報の入手・使用 ⑧　使用方法	・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。	・団体内統合宛名番号を生成する。 　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、団体内統合宛名番号を生成する。 　住民登録外の者の分：当該事務で必要となった者を団体内統合宛名システムへ登録した際に、団体内統合宛名番号を生成する。 ・生成した団体内統合宛名番号を登録元及び中間サーバーへ送信する。	事前	システム標準化による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 3．特定個人情報の入手・使用 ⑧　使用方法 情報の突合	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。	個人番号、4情報、団体内統合宛名番号及び宛名番号を相互に突合し、個人を特定する。	事前	システム標準化による修正

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ①　保管場所	＜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＞ ・中間サーバー・プラットフォームはデータセンターに設置している。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ・特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。	＜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。 ・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＞ ・中間サーバー・プラットフォームはデータセンターに設置している。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ・特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。 ＜ガバメントクラウドにおける措置＞ 〇サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27018の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 〇特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。	事前	システム標準化による修正
令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ②　保管期間 その妥当性	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。	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。 ・宛名番号は、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。	事前	システム標準化による修正

令和8年1月13日	Ⅱ　特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ③ 消去方法	＜横浜市における措置＞ ・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＞ ・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。 ・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。	＜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、団体内統合宛名システムの保守・運用を行う事業者において、保守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で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、裁断また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＞ ・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。 ・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。 ＜ガバメントクラウドにおける措置＞ 〇特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 〇クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 〇既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。	事前	システム標準化による修正

（別紙）全項目評価書の変更箇所 【（別添2）ファイル記録項目】

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4年6月28日	（別添2）ファイル記録項目 【予防接種対象者関係情報ファイル】	（追加）	以下の項目を追加。 46 個人番号 47 個別宛名番号 48 接種券番号 49 自治体コード 50 接種状況（実施／未実施） 51 接種回（1回目／2回目／3回目） 52 接種医師名 53 接種履歴登録日時 54 ワクチンメーカー 55 ワクチン接種量 56 ワクチン種類（※） 57 製品名（※） 58 旅券関係情報（旧姓・別姓・別名、ローマ字氏名、国籍、旅券番号）（※） 59 証明書ID（※） 60 証明書発行年月日（※） ※ 新型コロナウイルス感染症予防接種証明書の交付に必要な場合のみ	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和8年1月13日	（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】	【予防接種関係情報ファイル】	事後	表現の軽微な修正
令和8年1月13日	（別添2）特定個人情報ファイル記録項目	【統合番号連携ファイル】	【団体内統合宛名ファイル】	事前	システム標準化による修正
令和8年1月13日	（別添2）特定個人情報ファイル記録項目 【団体内統合宛名番号連携ファイル】	2 統合番号	2 団体内統合宛名番号	事前	システム標準化による修正
令和8年1月13日	（別添2）特定個人情報ファイル記録項目 【団体内統合宛名番号連携ファイル】	4 業務固有番号	4 宛名番号	事前	システム標準化による修正

（別紙）全項目評価書の変更箇所 【Ⅲリスク対策(予防接種関係情報ファイル)】

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
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

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
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
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
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 （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

令和3年6月15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：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	（※2）番号法第19条第7号、第8号及び第16号に基づき、事務手続ごとに情報照会者、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。	（※2）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。	事後	中間サーバー・プラットフォームの更改に伴う修正
令和3年6月15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	・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。	・機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。	事後	中間サーバー・プラットフォームの更改に伴う修正
令和3年6月15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：特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	＜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。	＜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。 ・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	事後	中間サーバー・プラットフォームの更改に伴う修正
令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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	（追加）	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> （以下、長文のため評価書本体を参照）	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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	②転出先市区町村からの個人番号の入手 　本市からの転出者について、本市での接種記録を転出先市区町へ提供するために、転出先市区町村から個人番号を入手するが、その際は、転出先市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を通じて入手する。	②他市区町村からの個人番号の入手 　本市からの転出者について、本市での接種記録を転出先市区町へ提供するために、他先市区町村から個人番号を入手するが、その際は、他市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を通じて入手する。	事後	誤字、脱字等の修正、表現の軽微な修正
令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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（情報ネットワークシステムを通じた入手を除く。） リスク1：目的外の入手が行われるリスク 必要な情報以外を入手することを防止するための措置の内容	（追加）	＜ワクチン接種記録システム等における追加措置＞ （新型コロナウイルス感染症予防接種証明書電子交付機能） 　個人番号カードや旅券の読み取りにより必要な情報を入手し、申請者の自由入力を避けることで、交付申請者が不要な情報を送信してしまうリスクを防止する。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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（情報ネットワークシステムを通じた入手を除く。） リスク2：不適切な方法で入手が行われるリスク リスクに対する措置の内容	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)のデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようにアクセス制御している。 （新型コロナウイルス感染症予防接種証明書電子交付機能） 　当該機能では、専用アプリからのみ交付申請を可能とする。アプリの改ざん防止措置を講じることで、意図しない不適切な方法で特定個人情報が送信されることを避ける。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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（情報ネットワークシステムを通じた入手を除く。） リスク3：　入手した特定個人情報が不正確であるリスク 入手の際の本人確認の措置の内容	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ （新型コロナウイルス感染症予防接種証明書電子交付機能）個人番号カードのICチップ読み取り（券面事項入力補助AP）と暗証番号入力（券面事項入力補助APの暗証番号）による二要素認証で本人確認を行うため、本人からの情報のみが送信される。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用

令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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（情報ネットワークシステムを通じた入手を除く。） リスク3：入手した特定個人情報が不正確であるリスク 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。	・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：住基ネット総合端末を利用して照合を行う。	事後	端末名変更のため修正
令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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（情報ネットワークシステムを通じた入手を除く。） リスク3：　入手した特定個人情報が不正確であるリスク 特定個人情報の正確性確保の措置の内容	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ （新型コロナウイルス感染症予防接種証明書電子交付機能） ・券面入力補助APを活用し、個人番号カード内の記憶領域に格納された個人番号を申請情報として自動的に入力することにより、不正確な個人番号の入力を抑止する措置を講じている。 ・券面事項入力補助APから取得する情報（4情報・マイナンバー）に付されている署名について、VRSにおいて真正性の検証を行い、送信情報の真正性を確認する措置を講じている。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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（情報ネットワークシステムを通じた入手を除く。） リスク4：入手の際に特定個人情報が漏えい・紛失するリスク リスクに対する措置の内容	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ 入手する特定個人情報については、情報漏えいを防止するために、暗号化された通信回線を使用する。 （新型コロナウイルス感染症予防接種証明書電子交付機能） 電子交付アプリとVRSとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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（情報ネットワークシステムを通じた入手を除く。） 特定個人情報の入手（情報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	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ ・入手した特定個人情報については、限定された端末を利用して国から配布されたユーザIDを使用し、ログインした場合だけアクセスできるように制御している。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和4年6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 ※（7．リスク1⑨を除く。） （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：　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 事務で使用するその他のシステムにおける措置の内容	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ ・接種会場等では、接種券番号の読取端末（タブレット端末）からインターネット経由でワクチン接種記録システム(VRS)に接続するが、個人番号にはアクセスできないように制御している。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （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：　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク ユーザ認証の管理 具体的な管理方法	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ 権限のない者によって不正に使用されないよう、以下の対策を講じている。 ・ワクチン接種記録システム(VRS)における特定個人情報へのアクセスは、LG-WAN端末による 操作に限り可能になるように制御している。 ・LG-WAN端末は、限定された者しかログインできる権限を保持しない。 ・ワクチン接種記録システム(VRS)におけるのログイン認証は、ユーザID・パスワードにて行う。 ・ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国に対してユーザ登録を事前申請した者に限定して発行される。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （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：　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の発効・失効の管理 具体的な管理方法	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国に対してユーザ登録を事前申請した者に限定して発行される。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （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：　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク 特定個人情報の使用の記録 具体的な方法	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ システム上の操作のログを取得しており、操作ログを確認できる。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用

令和4年6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 ※（7．リスク1⑨を除く。） （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。 （追加）	・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。 （削除） ・作業を行う職員及び端末を必要最小限に限定する。 ・作業に用いる電子記録媒体については、不正な複製、持ち出し等を防止するために、許可された 専用の外部 記録媒体を使用する。また、媒体管理簿等に使用の記録を記載する等、利用履歴を残す。 ・作業に用いる電子記録媒体の取扱いについては、承認を行い、当該承認の記録を残す。 ・電子記録媒体に格納するデータについては、暗号化やパスワード設定を行う。 ・電子記録媒体による作業を終了したら、内部のデータを確実に消去する。 管理簿に消去の記録を記載する等、消去履歴を残す。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （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 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	（追加）	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ①特定個人情報を使用する場面を必要最小限に限定している。具体的には以下の3つの場面に限定している。 ・本市への転入者について、転出元市区町村へ接種記録を照会する場合のみ入手し、使用する。 ・本市からの転出者について、本市での接種記録を転出先市区町村へ提供するために、個人番号を入手し、使用する。 ・接種者について、新型コロナウイルス感染症予防接種証明書の交付申請があった場合に、接種記録を照会するために、個人番号を入手し、使用する。 ②ワクチン接種記録システム(VRS)からCSVファイルにてダウンロードする接種記録データには、個人番号が含まれない。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （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	（追加）	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> 本市、国、当該システムの運用保守事業者の三者の関係を規定した「ワクチン接種記録システムの利用にあたっての確認事項（規約）」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム(VRS)（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。 ・ 特定個人情報ファイルの閲覧者・更新者の制限 ・ 特定個人情報ファイルの取扱いの記録 ・ 特定個人情報の提供ルール/消去ルール ・ 委託契約書中の特定個人情報ファイルの取扱いに関する規定 ・ 再委託先による特定個人情報ファイルの適切な取扱いの確保 ・ 新型コロナウイルス感染症予防接種証明書電子交付機能において、申請者本人から特定個人情報の提供を受ける際の入手に係る保護措置	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用

令和4年6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 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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	（追加）	[　記録を残している　]	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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 具体的な方法	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)では、他市区町村への提供の記録を取得しており、委託業者から「情報提供等の記録」を入手し、記録の確認をすることができる。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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	（追加）	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ・転出元市区町村への個人番号の提供 本市への転入者について、転出元市区町村から接種記録を入手するため、転出元市区町村へ個人番号を提供するが、その際は、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を用いて提供する。 転出先市区町村へ接種記録を提供するが、その際は、本市において、住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム(VRS)を用いて提供する。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） リスク2：　不適切な方法で提供・移転が行われるリスク	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ・転出元市区町村への個人番号の提供 本市への転入者について、転出元市区町村から接種記録を入手するため、転出元市区町村へ個人番号を提供するが、その際は、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を用いて提供する。 転出先市区町村へ接種記録を提供するが、その際は、本市において、住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム(VRS)を用いて提供する。	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ・他市区町村への個人番号の提供 本市への転入者について、転出元市区町村から接種記録を入手するため、他市区町村へ個人番号を提供するが、その際は、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を用いて提供する。 転出先市区町村へ接種記録を提供するが、その際は、本市において、住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム(VRS)を用いて提供する。	事後	誤字、脱字等の修正、表現の軽微な修正
令和4年6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 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） リスク2：　不適切な方法で提供・移転が行われるリスク リスクへの対策は十分か	（追加）	[　十分である　]	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ ・転出元市区町村への個人番号の提供、転出先市区町村からの接種記録の提供 本市への転入者について、転出元市区町村から接種記録を入手するため、転出元市区町村へ個人番号を提供するが、その際は、個人番号と共に転出元の市区町村コードを送信する。そのため、仮に誤った市区町村コードを個人番号と共に送信したとしても、電文を受ける市区町村では、該当者がいないため、誤った市区町村に対して個人番号が提供されず、これに対して接種記録も提供されない仕組みとなっている。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和4年6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 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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	＜ワクチン接種記録システム(VRS)における追加措置＞ ・転出元市区町村への個人番号の提供、転出先市区町村からの接種記録の提供 本市への転入者について、転出元市区町村から接種記録を入手するため、転出元市区町村へ個人番号を提供するが、その際は、個人番号と共に転出元の市区町村コードを送信する。そのため、仮に誤った市区町村コードを個人番号と共に送信したとしても、電文を受ける市区町村では、該当者がいないため、誤った市区町村に対して個人番号が提供されず、これに対して接種記録も提供されない仕組みとなっている。	＜ワクチン接種記録システム(VRS)における追加措置＞ ・他市区町村への個人番号の提供、転出先市区町村への接種記録の提供 本市への転入者について、転出元市区町村から接種記録を入手するため、他市区町村へ個人番号を提供するが、電文を受ける市区町村で、該当者がいない場合は、個人番号は保管されず、これに対して接種記録も提供されない仕組みとなっている。	事後	誤字、脱字等の修正、表現の軽微な修正
令和4年6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 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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 リスクへの対策は十分か	（追加）	[　十分である　]	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ ・特定個人情報の提供は、限定された端末（LG-WAN端末）だけができるように制御している。　・特定個人情報を提供する場面を必要最小限に限定している。　具体的には、本市への転入者について、転出元市区町村での接種記録を　入手するために、転出元市町区村へ個人番号と共に転出元の市区町村コードを提供する場面に限定している。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和4年6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 ※（7．リスク1⑨を除く。） （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：　特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	（追加）	＜ワクチン接種記録システム(VRS)における措置＞ ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための 統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウド サービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める物理的対策を満たしている。 主に以下の物理的対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスを利用している。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （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：　特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策	（追加）	十分に行っている	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （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：　特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	（追加）	＜ワクチン接種記録システム(VRS)における措置＞ ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める技術的対策を満たしている。 主に以下の技術的対策を講じている。 ・論理的に区分された本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、外部からの侵入検知・通知機能を備えている。 ・LG-WAN端末とワクチン接種記録システムとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 （新型コロナウイルス感染症予防接種証明書電子交付機能） ・電子交付アプリには、申請情報を記録しないこととしている。 ・電子交付アプリとVRSとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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	（新型コロナウイルス感染症予防接種証明書電子交付機能）	（新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付）	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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	（追加）	（新型コロナウイルス感染症予防接種証明書コンビニ交付） 証明書交付センターにおいてキオスク端末の操作画面を制御し、コンビニ交付に対応する市町村に対してのみキオスク端末から交付申請を可能とすることで、意図しない不適切な方法で特定個人情報が送信されることを避ける。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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3：入手した特定個人情報が不正確であるリスク 特定個人情報の正確性確保の措置の内容	・券面事項入力補助APから取得する情報（4情報・マイナンバー）に付されている署名について、VRSにおいて真正性の検証を行い、送信情報の真正性を確認する措置を講じている。	・券面事項入力補助APから取得する情報（4情報・マイナンバー）に付されている署名について、VRS又は証明書交付センターシステムにおいて真正性の検証を行い、送信情報の真正性を確認する措置を講じている。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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	（追加）	（新型コロナウイルス感染症予防接種証明書コンビニ交付） キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。 また、通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。さらに、キオスク端末の画面表示や音声案内により、マイナンバーカード及び証明書の取り忘れ防止対策を実施する	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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4：　入手の際に特定個人情報が漏えい・紛失するリスク 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	入手した特定個人情報については、限定された端末を利用して国から配布されたユーザIDを使用し、ログインした場合だけアクセスできるように制御している。	入手した特定個人情報については、限定された端末を利用して横浜市が指定する管理者から配布されたユーザIDを使用し、ログインした場合だけアクセスできるように制御している。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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：　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク ユーザ認証の管理 具体的な管理方法	・ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国に対してユーザ登録を事前申請した者に限定して発行される。	・ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、横浜市が指定する管理者が認めた者に限定して発行される。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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：　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の発効・失効の管理 具体的な管理方法	＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国に対してユーザ登録を事前申請した者に限定して発行される。	＜ワクチン接種記録システム(VRS)における追加措置＞ 　ワクチン接種記録システム(VRS)へのログイン用のユーザIDに付与されるアクセス権限は、横浜市が指定する管理者が必要最小限の権限で発効する。 　横浜市が指定する管理者は、定期的又は異動/退職等のイベントが発生したタイミングで、権限を有していた職員の異動/退職等情報を確認し、当該事由が生じた際には速やかにアクセス権限を更新し、当該ユーザ ID を失効させる。 　やむを得ず、複数の職員が共有するID（以下「共用ID」という。）を発行する必要がある場合は、当該IDを使用する職員・端末を特定し、管理者が把握した上で、パスワードを厳重に管理する運用を徹底し、必要最小限に発行する。なお、共用IDを使用する職員及び端末について、異動／退職等のイベントが発生したタイミングで確認し、当該事由が生じた際は速やかに把握している内容を更新する。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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：　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の管理 具体的な管理方法	ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国に対してユーザ登録を事前申請した者に限定して発行される。	ワクチン接種記録システム(VRS)へのログイン用のユーザIDに付与されるアクセス権限は、横浜市が指定する管理者が必要最小限の権限で発効する。 　横浜市が指定する管理者は、定期的にユーザID及びアクセス権限の一覧をシステムにおいて確認し、アクセス権限及び不正利用の有無を確認する。また、不要となったユーザ ID やアクセス権限を速やかに変更又は削除する。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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：　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク 特定個人情報の使用の記録 具体的な方法	（追加）	ログは定期に及び必要に応じ随時に確認する。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> 本市、国、当該システムの運用保守事業者の三者の関係を規定した「ワクチン接種記録システムの利用にあたっての確認事項（規約）」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム(VRS)（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> 本市、国、当該システムの運用保守事業者の三者の関係を規定した「ワクチン接種記録システムの利用にあたっての確認事項（規約）」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム(VRS)（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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：　特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	（追加）	（新型コロナウイルス感染症予防接種証明書コンビニ交付） ・証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。 ・キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。また、通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。		特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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1：　目的外の入手が行われるリスク 対象者以外の情報の入手を 防止するための措置の内容	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ①転入者本人からの個人番号の入手 本市の転入者について、転出元市区町村へ接種記録を照会するために、本人から個人番号を入手する場合は、新接種券発行申請書兼接種記録確認同意書等により本人同意を取得し、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 ②他市区町村からの個人番号の入手 本市からの転出者について、本市での接種記録を転出先市区町へ提供するために、他先市区町村から個人番号を入手するが、その際は、他市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を通じて入手する。 ③転出元市区町村からの接種記録の入手 本市への転入者について、転出元市区町村から接種記録を入手するが、その際は、本市において住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム(VRS)を通じて入手する。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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	④新型コロナウイルス感染症予防接種証明書の交付申請者からの個人番号の入手 接種者について、新型コロナウイルス感染症予防接種証明書の交付のために個人番号を入手するのは、接種者から接種証明書の交付申請があった場合のみとし、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 （新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付） 交付申請には、個人番号カードのICチップ読み取り（券面事項入力補助AP）と暗証番号入力（券面事項入力補助APの暗証番号）による二要素認証を必須とすることで、対象者以外の情報の入手を防止する。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正

令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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1：　目的外の入手が行われるリスク 必要な情報以外を入手すること とを防止するための措置の内容	＜ワクチン接種記録システム等における追加措置＞ （新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付） 個人番号カードや旅券の読み取りにより必要な情報を入手し、申請者の自由入力を避けることで、交付申請者が不要な情報を送信してしまうリスクを防止する。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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：　不適切な方法で入手が行われるリスク リスクに対する措置の内容	（新型コロナウイルス感染症予防接種証明書電子交付機能） 当該機能では、専用アプリからのみ交付申請を可能とする。アプリの改ざん防止措置を講じることで、意図しない不適切な方法で特定個人情報が送信されることを避ける。 （新型コロナウイルス感染症予防接種証明書コンビニ交付） 証明書交付センターにおいてキオスク端末の操作画面を制御し、コンビニ交付に対応する市町村に対してのみキオスク端末から交付申請を可能とすることで、意図しない不適切な方法で特定個人情報が送信されることを避ける。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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	＜ワクチン接種記録システム(VRS)における追加措置＞ （新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付） 個人番号カードのICチップ読み取り（券面事項入力補助AP）と暗証番号入力（券面事項入力補助APの暗証番号）による二要素認証で本人確認を行うため、本人からの情報のみが送信される。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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3：　入手した特定個人情報が不正確であるリスク 特定個人情報の正確性確保の措置の内容	種記録システム(VRS)における追加措置＞ （新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付） ・券面入力補助APを活用し、個人番号カード内の記憶領域に格納された個人番号を申請情報として自動的に入力することにより、不正確な個人番号の入力を抑止する措置を講じている。 ・券面事項入力補助APから取得する情報（4情報・マイナンバー）に付されている署名について、VRS又は証明書交付センターシステムにおいて真正性の検証を行い送信情報の真正性を確認する措置を講じている。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正

令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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4：　入手の際に特定個人情報が漏えい・紛失するリスク リスクに対する措置の内容	（新型コロナウイルス感染症予防接種証明書電子交付機能） 電子交付アプリとVRSとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 （新型コロナウイルス感染症予防接種証明書コンビニ交付） キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。 また、通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。さらに、キオスク端末の画面表示や音声案内により、マイナンバーカード及び証明書の取り忘れ防止対策を実施する。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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：　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 事務で使用するその他のシステムにおける措置の内容	＜ワクチン接種記録システム(VRS)における追加措置＞ ・接種会場等では、接種券番号の読取端末（タブレット端末）からインターネット経由でワクチン接種記録システム(VRS)に接続するが、個人番号にはアクセスできないように制御している。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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4：　特定個人情報ファイルが不正に複製されるリスク 特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ①特定個人情報を使用する場面を必要最小限に限定している。具体的には以下の3つの場面に限定している。 ・本市への転入者について、転出元市区町村へ接種記録を照会する場合のみ入手し、使用する。 ・本市からの転出者について、本市での接種記録を転出先市区町村へ提供するために、個人番号を入手し、使用する。 ・接種者について、新型コロナウイルス感染症予防接種証明書の交付申請があった場合に、接種記録を照会するために、個人番号を入手し、使用する。 ②ワクチン接種記録システム(VRS)からCSVファイルにてダウンロードする接種記録データには、個人番号が含まれない。	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ワクチン接種記録システム(VRS)からCSVファイルにてダウンロードする接種記録データには、個人番号が含まれない。	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正

令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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 情報保護管理体制の確認	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> 本市、国、当該システムの運用保守事業者の三者の関係を規定した「ワクチン接種記録システムの利用にあたっての確認事項（規約）」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム(VRS)（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。 ・特定個人情報ファイルの閲覧者・更新者の制限 ・特定個人情報ファイルの取扱いの記録 ・特定個人情報の提供ルール/消去ルール ・委託契約書中の特定個人情報ファイルの取扱いに関する規定 ・再委託先による特定個人情報ファイルの適切な取扱いの確保 ・新型コロナウイルス感染症予防接種証明書電子交付機能において、申請者本人から特定個人情報の 提供を受ける際の入手に係る保護措置	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 5．特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）	[　]提供・移転しない	[○]提供・移転しない	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） リスク1：　不正な提供・移転が行われるリスク 特定個人情報の提供・移転の記録	[記録を残している]	[（削除）]	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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 具体的な方法	＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)では、他市区町村への提供の記録を取得しており、委託業者から「情報提供等の記録」を入手し、記録の確認をすることができる。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正

令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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・移転に関するルール	[定めている]	[（削除）]	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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・移転に関するルール ルールの内容及びルール遵守の確認方法	・市で管理する個人情報を移転・提供する際には、番号法及び横浜市個人情報保護条例の規定により、その範囲を厳格に規定し、当該規定内容のみ提供・移転する制御をシステムで行う。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） リスク1：　不正な提供・移転が行われるリスク その他の措置の内容	＜ワクチン接種記録システムにおける追加措置＞ ・接種者の旧住所地があった市町村に存在する接種履歴に限定した照会しか行えないこと ・接種者が転入した新住所地がある市町村からの照会に応じた提供しか行えないこと ・本人同意が得られた照会要求に応じた情報提供しか行わない仕組みとしている。 ※その他記載事項について追ってさらに確認	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） リスク1：　不正な提供・移転が行われるリスク その他の措置の内容	[十分である]	[（削除）]	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正

令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） リスク2：　不適切な方法で提供・移転が行われるリスク リスクに対する措置の内容	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ・他市区町村への個人番号の提供 本市への転入者について、転出元市区町村から接種記録を入手するため、他市区町村へ個人番号を提供するが、その際は、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を用いて提供する。 転出先市区町村へ接種記録を提供するが、その際は、転出元市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム(VRS)を用いて提供する。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） リスク2：　不適切な方法で提供・移転が行われるリスク リスクへの対策は十分か	[　十分である　]	[　（削除）　]	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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	＜ワクチン接種記録システム(VRS)における追加措置＞ ・他市区町村への個人番号の提供、転出先市区町村への接種記録の提供 本市への転入者について、転出元市区町村から接種記録を入手するため、他市区町村へ個人番号を提供するが、電文を受ける市区町村で、該当者がいない場合は、個人番号は保管されず、これに対して接種記録も提供されない仕組みとなっている。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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 リスクへの対策は十分	[　十分である　]	[　（削除）　]	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正

令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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	＜ワクチン接種記録システム(VRS)における追加措置＞ ・特定個人情報の提供は、限定された端末（LG-WAN端末）だけができるように制御している。 ・特定個人情報を提供する場面を必要最小限に限定している。具体的には、本市への転入者について、転出元市区町村での接種記録を入手するために、他市町区村へ個人番号を提供する場面に限定している。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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 ⑥技術的対策 具体的な対策の内容	（新型コロナウイルス感染症予防接種証明書電子交付機能） ・電子交付アプリには、申請情報を記録しないこととしている。 ・電子交付アプリとVRSとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 （新型コロナウイルス感染症予防接種証明書コンビニ交付） ・証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。 ・キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。また、通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和8年1月13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 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	予防接種関係情報ファイル	事後	表現の軽微な修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2．特定個人情報の入手（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。	・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。 〇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。	事後	実態に基づく修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク1：目的外の入手が行われるリスク 必要な情報以外を入手することを防止するための措置の内容	・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。	・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。 〇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。 ・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。	事後	実態に基づく修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク2：不適切な方法で入手が行われるリスク リスクに対する措置の内容	・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。 ＜ワクチン接種記録システム（VRS）における追加措置＞ ワクチン接種記録システム（VRS）のデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようアクセス制御している。	・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。	事後	実態に基づく削除
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク3：入手した特定個人情報が不正確であるリスク 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：住基ネット総合端末を利用して照合を行う。	・住登内者の場合：統合番号連携システムを利用して照合を行う。 ・住登外者の場合：住基ネット統合端末を利用して照合を行う。	事後	誤字、脱字等の修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク4：入手の際に特定個人情報が漏えい・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。 ＜ワクチン接種記録システム(VRS)における追加措置＞ 入手する特定個人情報については、情報漏えいを防止するために、暗号化された通信回線を使用する。	・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。	事後	実態に基づく削除
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク4：入手の際に特定個人情報が漏えい・紛失するリスク 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	＜ワクチン接種記録システム(VRS)における追加措置＞ ・入手した特定個人情報については、限定された端末を利用して横浜市が指定する管理者から配布されたユーザIDを使用し、ログインした場合だけアクセスできるように制御している。	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3．特定個人情報の使用 リスク1：目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク 事務で使用するその他のシステムにおける措置の内容	・予防接種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。	・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よう記録を残す。	事後	誤字、脱字等の修正、表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3．特定個人情報の使用 リスク2：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク ユーザ認証の管理 具体的な管理方法	・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。 ＜ワクチン接種記録システム(VRS)における追加措置＞ 　権限のない者によって不正に使用されないよう、以下の対策を講じている。 　・ワクチン接種記録システム(VRS)における特定個人情報へのアクセスは、LG-WAN端末による操作に限り可能になるように制御している。 　・LG-WAN端末は、限定された者しかログインできる権限を保持しない。 　・ワクチン接種記録システム(VRS)におけるのログイン認証は、ユーザID・パスワードにて行う。 　・ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、横浜市が指定する管理者が認めた者に限定して発行される。	・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。 ＜統合番号連携システムにおける対策＞ ・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。	事後	実態に基づく修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3．特定個人情報の使用 リスク2：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の発行・失効の管理 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。 ＜ワクチン接種記録システム(VRS)における追加措置＞ 　ワクチン接種記録システム(VRS)へのログイン用のユーザIDに付与されるアクセス権限は、横浜市が指定する管理者が必要最小限の権限で発効する。 　横浜市が指定する管理者は、定期的又は異動/退職等のイベントが発生したタイミングで、権限を有していた職員の異動/退職等情報を確認し、当該事由が生じた際には速やかにアクセス権限を更新し、当該ユーザ ID を失効させる。 　やむを得ず、複数の職員が共有するID（以下「共用ID」という。）を発行する必要がある場合は、当該IDを使用する職員・端末を特定し、管理者が把握した上で、パスワードを厳重に管理する運用を徹底し、必要最小限に発行する。なお、共用IDを使用する職員及び端末について、異動／退職等のイベントが発生したタイミングで確認し、当該事由が生じた際は速やかに把握している内容を更新する。	＜予防接種台帳システムにおける対策＞ ・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。 ・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。 ＜統合番号連携システムにおける対策＞ ・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。 ・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	実態に基づく修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3．特定個人情報の使用 リスク2：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の管理 具体的な管理方法	・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。 ＜ワクチン接種記録システム(VRS)における追加措置＞ 　ワクチン接種記録システム(VRS)へのログイン用のユーザIDに付与されるアクセス権限は、横浜市が指定する管理者が必要最小限の権限で発効する。 　横浜市が指定する管理者は、定期的にユーザID及びアクセス権限の一覧をシステムにおいて確認し、アクセス権限及び不正利用の有無を確認する。また、不要となったユーザ ID やアクセス権限を速やかに変更又は削除する。	＜予防接種台帳システムにおける対策＞ ・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。 ＜統合番号連携システムにおける対策＞ ・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。	事後	実態に基づく修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3．特定個人情報の使用 リスク2：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク 特定個人情報の使用の記録 具体的な管理方法	・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。 ＜ワクチン接種記録システム(VRS)における追加措置＞ システム上の操作のログを取得しており、操作ログを確認できる。ログは定期に及び必要に応じ随時に確認する。	・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。 ＜統合番号連携システムにおける対策＞ ・「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。	事後	実態に基づく修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3．特定個人情報の使用 リスク4：特定個人情報ファイルが不正に複製されるリスク 特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ワクチン接種記録システム(VRS)からCSVファイルにてダウンロードする接種記録データには、個人番号が含まれない。	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4．特定個人情報ファイルの取扱いの委託 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	個人情報の保護に関する法律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	軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク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）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。	＜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＞ ・情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ・中間サーバーの職員認証・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）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク2：安全が保たれない方法によって入手が行われるリスク 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。 ・団体内統合宛名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。	＜横浜市における措置＞ ・統合番号連携システムのサーバ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＞ ・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。 ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク4：入手の際に特定個人情報が漏えい・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。 ・団体内統合宛名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＞ 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。	＜横浜市における措置＞ ・統合番号連携システムのサーバ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、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ・既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ・情報照会が完了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。 ・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＞ ・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。 ・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。 ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク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機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。	＜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の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＞ ・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。 ・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。 ・機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク6：不適切な方法で提供されるリスク リスクに対する措置の内容	＜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。	＜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の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＞ ・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＞ ・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。 ・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。 ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク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。	＜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の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＞ ・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。 ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。	＜中間サーバー・ソフトウェアにおける措置＞ ・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＞ ・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。 ・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。 ・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。 ・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。	事後	表現の軽微な修正

令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	＜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。 ②事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。 ＜ワクチン接種記録システム(VRS)における措置＞ ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための 統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウド サービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める物 理的対策を満たしている。 主に以下の物理的対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスを利用している。	＜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＞ ・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。 ・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	事後	実態に基づく修正

令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	・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。 ＜ワクチン接種記録システム(VRS)における措置＞ ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める技術的対策を満たしている。 主に以下の技術的対策を講じている。 ・論理的に区分された本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、外部からの侵入検知・通知機能を備えている。 ・LG-WAN端末とワクチン接種記録システムとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。	＜横浜市における措置＞ ・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＞ ・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。 ・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。 ・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。	事後	実態に基づく修正
令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク 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 その内容	別紙のとおり	別紙2のとおり	事後	表現の軽微な修正

令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク 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 再発防止策の内容	別紙のとおり	別紙2のとおり	事後	表現の軽微な修正
令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑩死者の個人番号	[　保管していない　]	[　保管している　]	事後	実態に基づく修正
令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑩死者の個人番号 具体的な保管方法	（追加）	・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、団体内統合宛名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：団体内統合宛名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。	事後	実態に基づく修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2．特定個人情報の入手（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。 〇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。	・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。 〇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、個人番号と団体内統合宛名番号及び宛名番号の正確な紐付けを担保する。 ・住民登録外の者の分：統合端末を用いて本人確認を行うか、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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク1：目的外の入手が行われるリスク 必要な情報以外を入手することを防止するための措置の内容	・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。 〇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。 ・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。	・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。 〇団体内統合宛名システムの検索画面を使用する際の措置 ・個人番号、団体内統合宛名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。 ・団体内統合宛名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。 ・団体内統合宛名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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク2：不適切な方法で入手が行われるリスク リスクに対する措置の内容	・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。	・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。 ・健康管理システム（予防接種分野）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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク3：入手した特定個人情報が不正確であるリスク 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を利用して照合を行う。 ・住登外者の場合：住基ネット統合端末を利用して照合を行う。	・住登内者の場合：団体内統合宛名システム端末を利用して照合を行う。 ・住登外者の場合：住基ネット統合端末を利用して照合を行う。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク1：目的を超えた紐付け、事務に必要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。	・団体内統合宛名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。 ・団体内統合宛名システムでは個人番号、団体内統合宛名番号及び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。 ・団体内統合宛名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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク1：目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク 事務で使用するその他のシステムにおける措置の内容	・予防接種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よう記録を残す。	・健康管理システム（予防接種分野）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よう記録を残す。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク ユーザ認証の管理 具体的な管理方法	・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。 ＜統合番号連携システムにおける対策＞ ・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。	・健康管理システム（予防接種分野）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。 ＜団体内統合宛名システムにおける対策＞ ・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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の発行・失効の管理 具体的な管理方法	＜予防接種台帳システムにおける対策＞ ・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。 ・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。 ＜統合番号連携システムにおける対策＞ ・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。 ・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。	＜健康管理システム（予防接種分野）における対策＞ ・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。 ・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。 ＜団体内統合宛名システムにおける対策＞ ・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。 ・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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の管理 具体的な管理方法	＜予防接種台帳システムにおける対策＞ ・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。 ＜統合番号連携システムにおける対策＞ ・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。	＜健康管理システム（予防接種分野）における対策＞ ・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。 ＜団体内統合宛名システムにおける対策＞ ・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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク 特定個人情報の使用の記録 具体的な管理方法	・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。 ＜統合番号連携システムにおける対策＞ ・「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。	・健康管理システム（予防接種分野）へのログイン記録、健康管理システム（予防接種分野）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。 ＜団体内統合宛名システムにおける対策＞ ・「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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク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＞ ・情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ・中間サーバーの職員認証・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）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。	＜横浜市における措置＞ 〇団体内統合宛名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団体内統合宛名システムを使用できる仕組みを構築する。 ・団体内統合宛名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、団体内統合宛名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。 ・団体内統合宛名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＞ ・情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ・中間サーバーの職員認証・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）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク2：安全が保たれない方法によって入手が行われるリスク 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＞ ・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。 ・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。	＜横浜市における措置＞ ・団体内統合宛名システムのサーバ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。 ・団体内統合宛名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＞ ・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。 ・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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク3：入手した特定個人情報が不正確であるリスク 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。	＜横浜市における措置＞ 団体内統合宛名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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク4：入手の際に特定個人情報が漏えい・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、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ・既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ・情報照会が完了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。 ・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＞ ・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。 ・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。 ・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。	＜横浜市における措置＞ ・団体内統合宛名システムのサーバ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。 ・団体内統合宛名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、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ・既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ・情報照会が完了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。 ・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＞ ・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。 ・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。 ・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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク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の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＞ ・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。 ・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。 ・機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ・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。	＜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、サーバ等へのアクセス権限を設定する。 ・団体内統合宛名システムの画面からの副本への登録においては、団体内統合宛名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＞ ・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。 ・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。 ・機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ・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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク6：不適切な方法で提供されるリスク リスクに対する措置の内容	＜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の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＞ ・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＞ ・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。 ・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。 ・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。	＜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、サーバ等へのアクセス権限を設定する。 ・団体内統合宛名システムの画面からの副本への登録においては、団体内統合宛名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＞ ・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＞ ・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。 ・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。 ・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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク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の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＞ ・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。 ・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。	＜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、サーバ等へのアクセス権限を設定する。 ・団体内統合宛名システムの画面からの副本への登録においては、団体内統合宛名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＞ ・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。 ・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。	事前	システム標準化による修正

令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	＜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＞ ・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。 ・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	＜横浜市における措置＞ ・団体内統合宛名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。 ・団体内統合宛名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。 ・団体内統合宛名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＞ ・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。 ・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	事前	システム標準化による修正
令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	＜横浜市における措置＞ ・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＞ ・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。 ・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。 ・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。	＜横浜市における措置＞ ・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。 ・団体内統合宛名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＞ ・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。 ・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。 ・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。	事前	システム標準化による修正

（別紙）全項目評価書の変更箇所 【Ⅲリスク対策(予防接種関係情報ファイル)】

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
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

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
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
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
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 （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

令和3年6月15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：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	（※2）番号法第19条第7号、第8号及び第16号に基づき、事務手続ごとに情報照会者、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。	（※2）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。	事後	中間サーバー・プラットフォームの更改に伴う修正
令和3年6月15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	・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。	・機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。	事後	中間サーバー・プラットフォームの更改に伴う修正
令和3年6月15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：特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	＜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。	＜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。 ・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	事後	中間サーバー・プラットフォームの更改に伴う修正
令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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	（追加）	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> （以下、長文のため評価書本体を参照）	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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	②転出先市区町村からの個人番号の入手 　本市からの転出者について、本市での接種記録を転出先市区町へ提供するために、転出先市区町村から個人番号を入手するが、その際は、転出先市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を通じて入手する。	②他市区町村からの個人番号の入手 　本市からの転出者について、本市での接種記録を転出先市区町へ提供するために、他先市区町村から個人番号を入手するが、その際は、他市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を通じて入手する。	事後	誤字、脱字等の修正、表現の軽微な修正
令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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（情報ネットワークシステムを通じた入手を除く。） リスク1：目的外の入手が行われるリスク 必要な情報以外を入手することを防止するための措置の内容	（追加）	＜ワクチン接種記録システム等における追加措置＞ （新型コロナウイルス感染症予防接種証明書電子交付機能） 　個人番号カードや旅券の読み取りにより必要な情報を入手し、申請者の自由入力を避けることで、交付申請者が不要な情報を送信してしまうリスクを防止する。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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（情報ネットワークシステムを通じた入手を除く。） リスク2：不適切な方法で入手が行われるリスク リスクに対する措置の内容	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)のデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようにアクセス制御している。 （新型コロナウイルス感染症予防接種証明書電子交付機能） 　当該機能では、専用アプリからのみ交付申請を可能とする。アプリの改ざん防止措置を講じることで、意図しない不適切な方法で特定個人情報が送信されることを避ける。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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（情報ネットワークシステムを通じた入手を除く。） リスク3：　入手した特定個人情報が不正確であるリスク 入手の際の本人確認の措置の内容	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ （新型コロナウイルス感染症予防接種証明書電子交付機能）個人番号カードのICチップ読み取り（券面事項入力補助AP）と暗証番号入力（券面事項入力補助APの暗証番号）による二要素認証で本人確認を行うため、本人からの情報のみが送信される。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用

令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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（情報ネットワークシステムを通じた入手を除く。） リスク3：入手した特定個人情報が不正確であるリスク 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。	・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：住基ネット総合端末を利用して照合を行う。	事後	端末名変更のため修正
令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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（情報ネットワークシステムを通じた入手を除く。） リスク3：　入手した特定個人情報が不正確であるリスク 特定個人情報の正確性確保の措置の内容	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ （新型コロナウイルス感染症予防接種証明書電子交付機能） ・券面入力補助APを活用し、個人番号カード内の記憶領域に格納された個人番号を申請情報として自動的に入力することにより、不正確な個人番号の入力を抑止する措置を講じている。 ・券面事項入力補助APから取得する情報（4情報・マイナンバー）に付されている署名について、VRSにおいて真正性の検証を行い、送信情報の真正性を確認する措置を講じている。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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（情報ネットワークシステムを通じた入手を除く。） リスク4：入手の際に特定個人情報が漏えい・紛失するリスク リスクに対する措置の内容	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ 入手する特定個人情報については、情報漏えいを防止するために、暗号化された通信回線を使用する。 （新型コロナウイルス感染症予防接種証明書電子交付機能） 電子交付アプリとVRSとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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（情報ネットワークシステムを通じた入手を除く。） 特定個人情報の入手（情報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	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ ・入手した特定個人情報については、限定された端末を利用して国から配布されたユーザIDを使用し、ログインした場合だけアクセスできるように制御している。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和4年6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 ※（7．リスク1⑨を除く。） （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：　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 事務で使用するその他のシステムにおける措置の内容	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ ・接種会場等では、接種券番号の読取端末（タブレット端末）からインターネット経由でワクチン接種記録システム(VRS)に接続するが、個人番号にはアクセスできないように制御している。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （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：　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク ユーザ認証の管理 具体的な管理方法	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ 権限のない者によって不正に使用されないよう、以下の対策を講じている。 ・ワクチン接種記録システム(VRS)における特定個人情報へのアクセスは、LG-WAN端末による 操作に限り可能になるように制御している。 ・LG-WAN端末は、限定された者しかログインできる権限を保持しない。 ・ワクチン接種記録システム(VRS)におけるのログイン認証は、ユーザID・パスワードにて行う。 ・ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国に対してユーザ登録を事前申請した者に限定して発行される。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （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：　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の発効・失効の管理 具体的な管理方法	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国に対してユーザ登録を事前申請した者に限定して発行される。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （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：　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク 特定個人情報の使用の記録 具体的な方法	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ システム上の操作のログを取得しており、操作ログを確認できる。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用

令和4年6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 ※（7．リスク1⑨を除く。） （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。 （追加）	・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。 （削除） ・作業を行う職員及び端末を必要最小限に限定する。 ・作業に用いる電子記録媒体については、不正な複製、持ち出し等を防止するために、許可された 専用の外部 記録媒体を使用する。また、媒体管理簿等に使用の記録を記載する等、利用履歴を残す。 ・作業に用いる電子記録媒体の取扱いについては、承認を行い、当該承認の記録を残す。 ・電子記録媒体に格納するデータについては、暗号化やパスワード設定を行う。 ・電子記録媒体による作業を終了したら、内部のデータを確実に消去する。 管理簿に消去の記録を記載する等、消去履歴を残す。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （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 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	（追加）	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ①特定個人情報を使用する場面を必要最小限に限定している。具体的には以下の3つの場面に限定している。 ・本市への転入者について、転出元市区町村へ接種記録を照会する場合のみ入手し、使用する。 ・本市からの転出者について、本市での接種記録を転出先市区町村へ提供するために、個人番号を入手し、使用する。 ・接種者について、新型コロナウイルス感染症予防接種証明書の交付申請があった場合に、接種記録を照会するために、個人番号を入手し、使用する。 ②ワクチン接種記録システム(VRS)からCSVファイルにてダウンロードする接種記録データには、個人番号が含まれない。	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （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	（追加）	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> 本市、国、当該システムの運用保守事業者の三者の関係を規定した「ワクチン接種記録システムの利用にあたっての確認事項（規約）」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム(VRS)（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。 ・ 特定個人情報ファイルの閲覧者・更新者の制限 ・ 特定個人情報ファイルの取扱いの記録 ・ 特定個人情報の提供ルール/消去ルール ・ 委託契約書中の特定個人情報ファイルの取扱いに関する規定 ・ 再委託先による特定個人情報ファイルの適切な取扱いの確保 ・ 新型コロナウイルス感染症予防接種証明書電子交付機能において、申請者本人から特定個人情報の提供を受ける際の入手に係る保護措置	事後	特定個人情報保護評価に関する規則第９条第２項の規定（緊急時事後評価）の適用

令和4年6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 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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	（追加）	[　記録を残している　]	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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 具体的な方法	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)では、他市区町村への提供の記録を取得しており、委託業者から「情報提供等の記録」を入手し、記録の確認をすることができる。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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	（追加）	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ・転出元市区町村への個人番号の提供 本市への転入者について、転出元市区町村から接種記録を入手するため、転出元市区町村へ個人番号を提供するが、その際は、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を用いて提供する。 転出先市区町村へ接種記録を提供するが、その際は、本市において、住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム(VRS)を用いて提供する。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和4年6月28日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） リスク2：　不適切な方法で提供・移転が行われるリスク	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ・転出元市区町村への個人番号の提供 本市への転入者について、転出元市区町村から接種記録を入手するため、転出元市区町村へ個人番号を提供するが、その際は、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を用いて提供する。 転出先市区町村へ接種記録を提供するが、その際は、本市において、住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム(VRS)を用いて提供する。	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ・他市区町村への個人番号の提供 本市への転入者について、転出元市区町村から接種記録を入手するため、他市区町村へ個人番号を提供するが、その際は、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を用いて提供する。 転出先市区町村へ接種記録を提供するが、その際は、本市において、住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム(VRS)を用いて提供する。	事後	誤字、脱字等の修正、表現の軽微な修正
令和4年6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 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） リスク2：　不適切な方法で提供・移転が行われるリスク リスクへの対策は十分か	（追加）	[　十分である　]	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ ・転出元市区町村への個人番号の提供、転出先市区町村からの接種記録の提供 本市への転入者について、転出元市区町村から接種記録を入手するため、転出元市区町村へ個人番号を提供するが、その際は、個人番号と共に転出元の市区町村コードを送信する。そのため、仮に誤った市区町村コードを個人番号と共に送信したとしても、電文を受ける市区町村では、該当者がいないため、誤った市区町村に対して個人番号が提供されず、これに対して接種記録も提供されない仕組みとなっている。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和4年6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 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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	＜ワクチン接種記録システム(VRS)における追加措置＞ ・転出元市区町村への個人番号の提供、転出先市区町村からの接種記録の提供 本市への転入者について、転出元市区町村から接種記録を入手するため、転出元市区町村へ個人番号を提供するが、その際は、個人番号と共に転出元の市区町村コードを送信する。そのため、仮に誤った市区町村コードを個人番号と共に送信したとしても、電文を受ける市区町村では、該当者がいないため、誤った市区町村に対して個人番号が提供されず、これに対して接種記録も提供されない仕組みとなっている。	＜ワクチン接種記録システム(VRS)における追加措置＞ ・他市区町村への個人番号の提供、転出先市区町村への接種記録の提供 本市への転入者について、転出元市区町村から接種記録を入手するため、他市区町村へ個人番号を提供するが、電文を受ける市区町村で、該当者がいない場合は、個人番号は保管されず、これに対して接種記録も提供されない仕組みとなっている。	事後	誤字、脱字等の修正、表現の軽微な修正
令和4年6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 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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 リスクへの対策は十分か	（追加）	[　十分である　]	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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	（追加）	＜ワクチン接種記録システム(VRS)における追加措置＞ ・特定個人情報の提供は、限定された端末（LG-WAN端末）だけができるように制御している。　・特定個人情報を提供する場面を必要最小限に限定している。　具体的には、本市への転入者について、転出元市区町村での接種記録を　入手するために、転出元市町区村へ個人番号と共に転出元の市区町村コードを提供する場面に限定している。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和4年6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 ※（7．リスク1⑨を除く。） （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：　特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	（追加）	＜ワクチン接種記録システム(VRS)における措置＞ ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための 統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウド サービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める物理的対策を満たしている。 主に以下の物理的対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスを利用している。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （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：　特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策	（追加）	十分に行っている	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6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 ※（7．リスク1⑨を除く。） （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：　特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	（追加）	＜ワクチン接種記録システム(VRS)における措置＞ ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める技術的対策を満たしている。 主に以下の技術的対策を講じている。 ・論理的に区分された本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、外部からの侵入検知・通知機能を備えている。 ・LG-WAN端末とワクチン接種記録システムとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 （新型コロナウイルス感染症予防接種証明書電子交付機能） ・電子交付アプリには、申請情報を記録しないこととしている。 ・電子交付アプリとVRSとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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	（新型コロナウイルス感染症予防接種証明書電子交付機能）	（新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付）	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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	（追加）	（新型コロナウイルス感染症予防接種証明書コンビニ交付） 証明書交付センターにおいてキオスク端末の操作画面を制御し、コンビニ交付に対応する市町村に対してのみキオスク端末から交付申請を可能とすることで、意図しない不適切な方法で特定個人情報が送信されることを避ける。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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3：入手した特定個人情報が不正確であるリスク 特定個人情報の正確性確保の措置の内容	・券面事項入力補助APから取得する情報（4情報・マイナンバー）に付されている署名について、VRSにおいて真正性の検証を行い、送信情報の真正性を確認する措置を講じている。	・券面事項入力補助APから取得する情報（4情報・マイナンバー）に付されている署名について、VRS又は証明書交付センターシステムにおいて真正性の検証を行い、送信情報の真正性を確認する措置を講じている。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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	（追加）	（新型コロナウイルス感染症予防接種証明書コンビニ交付） キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。 また、通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。さらに、キオスク端末の画面表示や音声案内により、マイナンバーカード及び証明書の取り忘れ防止対策を実施する	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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4：　入手の際に特定個人情報が漏えい・紛失するリスク 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	入手した特定個人情報については、限定された端末を利用して国から配布されたユーザIDを使用し、ログインした場合だけアクセスできるように制御している。	入手した特定個人情報については、限定された端末を利用して横浜市が指定する管理者から配布されたユーザIDを使用し、ログインした場合だけアクセスできるように制御している。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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：　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク ユーザ認証の管理 具体的な管理方法	・ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国に対してユーザ登録を事前申請した者に限定して発行される。	・ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、横浜市が指定する管理者が認めた者に限定して発行される。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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：　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の発効・失効の管理 具体的な管理方法	＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国に対してユーザ登録を事前申請した者に限定して発行される。	＜ワクチン接種記録システム(VRS)における追加措置＞ 　ワクチン接種記録システム(VRS)へのログイン用のユーザIDに付与されるアクセス権限は、横浜市が指定する管理者が必要最小限の権限で発効する。 　横浜市が指定する管理者は、定期的又は異動/退職等のイベントが発生したタイミングで、権限を有していた職員の異動/退職等情報を確認し、当該事由が生じた際には速やかにアクセス権限を更新し、当該ユーザ ID を失効させる。 　やむを得ず、複数の職員が共有するID（以下「共用ID」という。）を発行する必要がある場合は、当該IDを使用する職員・端末を特定し、管理者が把握した上で、パスワードを厳重に管理する運用を徹底し、必要最小限に発行する。なお、共用IDを使用する職員及び端末について、異動／退職等のイベントが発生したタイミングで確認し、当該事由が生じた際は速やかに把握している内容を更新する。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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：　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の管理 具体的な管理方法	ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国に対してユーザ登録を事前申請した者に限定して発行される。	ワクチン接種記録システム(VRS)へのログイン用のユーザIDに付与されるアクセス権限は、横浜市が指定する管理者が必要最小限の権限で発効する。 　横浜市が指定する管理者は、定期的にユーザID及びアクセス権限の一覧をシステムにおいて確認し、アクセス権限及び不正利用の有無を確認する。また、不要となったユーザ ID やアクセス権限を速やかに変更又は削除する。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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：　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク 特定個人情報の使用の記録 具体的な方法	（追加）	ログは定期に及び必要に応じ随時に確認する。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> 本市、国、当該システムの運用保守事業者の三者の関係を規定した「ワクチン接種記録システムの利用にあたっての確認事項（規約）」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム(VRS)（新型コロナウイルス感染症予防接種証明書電子交付機能を含む。）に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> 本市、国、当該システムの運用保守事業者の三者の関係を規定した「ワクチン接種記録システムの利用にあたっての確認事項（規約）」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム(VRS)（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用

令和5年8月4日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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：　特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	（追加）	（新型コロナウイルス感染症予防接種証明書コンビニ交付） ・証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。 ・キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。また、通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。		特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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1：　目的外の入手が行われるリスク 対象者以外の情報の入手を 防止するための措置の内容	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ①転入者本人からの個人番号の入手 本市の転入者について、転出元市区町村へ接種記録を照会するために、本人から個人番号を入手する場合は、新接種券発行申請書兼接種記録確認同意書等により本人同意を取得し、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 ②他市区町村からの個人番号の入手 本市からの転出者について、本市での接種記録を転出先市区町へ提供するために、他先市区町村から個人番号を入手するが、その際は、他市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を通じて入手する。 ③転出元市区町村からの接種記録の入手 本市への転入者について、転出元市区町村から接種記録を入手するが、その際は、本市において住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム(VRS)を通じて入手する。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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	④新型コロナウイルス感染症予防接種証明書の交付申請者からの個人番号の入手 接種者について、新型コロナウイルス感染症予防接種証明書の交付のために個人番号を入手するのは、接種者から接種証明書の交付申請があった場合のみとし、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 （新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付） 交付申請には、個人番号カードのICチップ読み取り（券面事項入力補助AP）と暗証番号入力（券面事項入力補助APの暗証番号）による二要素認証を必須とすることで、対象者以外の情報の入手を防止する。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正

令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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1：　目的外の入手が行われるリスク 必要な情報以外を入手すること とを防止するための措置の内容	＜ワクチン接種記録システム等における追加措置＞ （新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付） 個人番号カードや旅券の読み取りにより必要な情報を入手し、申請者の自由入力を避けることで、交付申請者が不要な情報を送信してしまうリスクを防止する。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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：　不適切な方法で入手が行われるリスク リスクに対する措置の内容	（新型コロナウイルス感染症予防接種証明書電子交付機能） 当該機能では、専用アプリからのみ交付申請を可能とする。アプリの改ざん防止措置を講じることで、意図しない不適切な方法で特定個人情報が送信されることを避ける。 （新型コロナウイルス感染症予防接種証明書コンビニ交付） 証明書交付センターにおいてキオスク端末の操作画面を制御し、コンビニ交付に対応する市町村に対してのみキオスク端末から交付申請を可能とすることで、意図しない不適切な方法で特定個人情報が送信されることを避ける。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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	＜ワクチン接種記録システム(VRS)における追加措置＞ （新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付） 個人番号カードのICチップ読み取り（券面事項入力補助AP）と暗証番号入力（券面事項入力補助APの暗証番号）による二要素認証で本人確認を行うため、本人からの情報のみが送信される。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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3：　入手した特定個人情報が不正確であるリスク 特定個人情報の正確性確保の措置の内容	種記録システム(VRS)における追加措置＞ （新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付） ・券面入力補助APを活用し、個人番号カード内の記憶領域に格納された個人番号を申請情報として自動的に入力することにより、不正確な個人番号の入力を抑止する措置を講じている。 ・券面事項入力補助APから取得する情報（4情報・マイナンバー）に付されている署名について、VRS又は証明書交付センターシステムにおいて真正性の検証を行い送信情報の真正性を確認する措置を講じている。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正

令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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4：　入手の際に特定個人情報が漏えい・紛失するリスク リスクに対する措置の内容	（新型コロナウイルス感染症予防接種証明書電子交付機能） 電子交付アプリとVRSとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 （新型コロナウイルス感染症予防接種証明書コンビニ交付） キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。 また、通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。さらに、キオスク端末の画面表示や音声案内により、マイナンバーカード及び証明書の取り忘れ防止対策を実施する。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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：　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 事務で使用するその他のシステムにおける措置の内容	＜ワクチン接種記録システム(VRS)における追加措置＞ ・接種会場等では、接種券番号の読取端末（タブレット端末）からインターネット経由でワクチン接種記録システム(VRS)に接続するが、個人番号にはアクセスできないように制御している。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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4：　特定個人情報ファイルが不正に複製されるリスク 特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ①特定個人情報を使用する場面を必要最小限に限定している。具体的には以下の3つの場面に限定している。 ・本市への転入者について、転出元市区町村へ接種記録を照会する場合のみ入手し、使用する。 ・本市からの転出者について、本市での接種記録を転出先市区町村へ提供するために、個人番号を入手し、使用する。 ・接種者について、新型コロナウイルス感染症予防接種証明書の交付申請があった場合に、接種記録を照会するために、個人番号を入手し、使用する。 ②ワクチン接種記録システム(VRS)からCSVファイルにてダウンロードする接種記録データには、個人番号が含まれない。	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ワクチン接種記録システム(VRS)からCSVファイルにてダウンロードする接種記録データには、個人番号が含まれない。	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正

令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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 情報保護管理体制の確認	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> 本市、国、当該システムの運用保守事業者の三者の関係を規定した「ワクチン接種記録システムの利用にあたっての確認事項（規約）」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム(VRS)（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。 ・特定個人情報ファイルの閲覧者・更新者の制限 ・特定個人情報ファイルの取扱いの記録 ・特定個人情報の提供ルール/消去ルール ・委託契約書中の特定個人情報ファイルの取扱いに関する規定 ・再委託先による特定個人情報ファイルの適切な取扱いの確保 ・新型コロナウイルス感染症予防接種証明書電子交付機能において、申請者本人から特定個人情報の 提供を受ける際の入手に係る保護措置	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 5．特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）	[　]提供・移転しない	[○]提供・移転しない	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） リスク1：　不正な提供・移転が行われるリスク 特定個人情報の提供・移転の記録	[記録を残している]	[（削除）]	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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 具体的な方法	＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)では、他市区町村への提供の記録を取得しており、委託業者から「情報提供等の記録」を入手し、記録の確認をすることができる。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正

令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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・移転に関するルール	[定めている]	[（削除）]	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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・移転に関するルール ルールの内容及びルール遵守の確認方法	・市で管理する個人情報を移転・提供する際には、番号法及び横浜市個人情報保護条例の規定により、その範囲を厳格に規定し、当該規定内容のみ提供・移転する制御をシステムで行う。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） リスク1：　不正な提供・移転が行われるリスク その他の措置の内容	＜ワクチン接種記録システムにおける追加措置＞ ・接種者の旧住所地があった市町村に存在する接種履歴に限定した照会しか行えないこと ・接種者が転入した新住所地がある市町村からの照会に応じた提供しか行えないこと ・本人同意が得られた照会要求に応じた情報提供しか行わない仕組みとしている。 ※その他記載事項について追ってさらに確認	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） リスク1：　不正な提供・移転が行われるリスク その他の措置の内容	[十分である]	[（削除）]	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正

令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） リスク2：　不適切な方法で提供・移転が行われるリスク リスクに対する措置の内容	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ・他市区町村への個人番号の提供 本市への転入者について、転出元市区町村から接種記録を入手するため、他市区町村へ個人番号を提供するが、その際は、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を用いて提供する。 転出先市区町村へ接種記録を提供するが、その際は、転出元市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム(VRS)を用いて提供する。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） リスク2：　不適切な方法で提供・移転が行われるリスク リスクへの対策は十分か	[　十分である　]	[　（削除）　]	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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	＜ワクチン接種記録システム(VRS)における追加措置＞ ・他市区町村への個人番号の提供、転出先市区町村への接種記録の提供 本市への転入者について、転出元市区町村から接種記録を入手するため、他市区町村へ個人番号を提供するが、電文を受ける市区町村で、該当者がいない場合は、個人番号は保管されず、これに対して接種記録も提供されない仕組みとなっている。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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 リスクへの対策は十分	[　十分である　]	[　（削除）　]	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正

令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （予防接種対象者関係情報ファイル） 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。） 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	＜ワクチン接種記録システム(VRS)における追加措置＞ ・特定個人情報の提供は、限定された端末（LG-WAN端末）だけができるように制御している。 ・特定個人情報を提供する場面を必要最小限に限定している。具体的には、本市への転入者について、転出元市区町村での接種記録を入手するために、他市町区村へ個人番号を提供する場面に限定している。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和6年4月30日	Ⅲ　特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。） （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 ⑥技術的対策 具体的な対策の内容	（新型コロナウイルス感染症予防接種証明書電子交付機能） ・電子交付アプリには、申請情報を記録しないこととしている。 ・電子交付アプリとVRSとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 （新型コロナウイルス感染症予防接種証明書コンビニ交付） ・証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。 ・キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。また、通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和8年1月13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 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	予防接種関係情報ファイル	事後	表現の軽微な修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2．特定個人情報の入手（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。	・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。 〇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。	事後	実態に基づく修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク1：目的外の入手が行われるリスク 必要な情報以外を入手することを防止するための措置の内容	・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。	・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。 〇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。 ・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。	事後	実態に基づく修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク2：不適切な方法で入手が行われるリスク リスクに対する措置の内容	・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。 ＜ワクチン接種記録システム（VRS）における追加措置＞ ワクチン接種記録システム（VRS）のデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようアクセス制御している。	・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。	事後	実態に基づく削除
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク3：入手した特定個人情報が不正確であるリスク 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：住基ネット総合端末を利用して照合を行う。	・住登内者の場合：統合番号連携システムを利用して照合を行う。 ・住登外者の場合：住基ネット統合端末を利用して照合を行う。	事後	誤字、脱字等の修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク4：入手の際に特定個人情報が漏えい・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。 ＜ワクチン接種記録システム(VRS)における追加措置＞ 入手する特定個人情報については、情報漏えいを防止するために、暗号化された通信回線を使用する。	・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。	事後	実態に基づく削除
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク4：入手の際に特定個人情報が漏えい・紛失するリスク 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	＜ワクチン接種記録システム(VRS)における追加措置＞ ・入手した特定個人情報については、限定された端末を利用して横浜市が指定する管理者から配布されたユーザIDを使用し、ログインした場合だけアクセスできるように制御している。	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3．特定個人情報の使用 リスク1：目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク 事務で使用するその他のシステムにおける措置の内容	・予防接種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。	・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よう記録を残す。	事後	誤字、脱字等の修正、表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3．特定個人情報の使用 リスク2：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク ユーザ認証の管理 具体的な管理方法	・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。 ＜ワクチン接種記録システム(VRS)における追加措置＞ 　権限のない者によって不正に使用されないよう、以下の対策を講じている。 　・ワクチン接種記録システム(VRS)における特定個人情報へのアクセスは、LG-WAN端末による操作に限り可能になるように制御している。 　・LG-WAN端末は、限定された者しかログインできる権限を保持しない。 　・ワクチン接種記録システム(VRS)におけるのログイン認証は、ユーザID・パスワードにて行う。 　・ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、横浜市が指定する管理者が認めた者に限定して発行される。	・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。 ＜統合番号連携システムにおける対策＞ ・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。	事後	実態に基づく修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3．特定個人情報の使用 リスク2：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の発行・失効の管理 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。 ＜ワクチン接種記録システム(VRS)における追加措置＞ 　ワクチン接種記録システム(VRS)へのログイン用のユーザIDに付与されるアクセス権限は、横浜市が指定する管理者が必要最小限の権限で発効する。 　横浜市が指定する管理者は、定期的又は異動/退職等のイベントが発生したタイミングで、権限を有していた職員の異動/退職等情報を確認し、当該事由が生じた際には速やかにアクセス権限を更新し、当該ユーザ ID を失効させる。 　やむを得ず、複数の職員が共有するID（以下「共用ID」という。）を発行する必要がある場合は、当該IDを使用する職員・端末を特定し、管理者が把握した上で、パスワードを厳重に管理する運用を徹底し、必要最小限に発行する。なお、共用IDを使用する職員及び端末について、異動／退職等のイベントが発生したタイミングで確認し、当該事由が生じた際は速やかに把握している内容を更新する。	＜予防接種台帳システムにおける対策＞ ・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。 ・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。 ＜統合番号連携システムにおける対策＞ ・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。 ・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	実態に基づく修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3．特定個人情報の使用 リスク2：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の管理 具体的な管理方法	・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。 ＜ワクチン接種記録システム(VRS)における追加措置＞ 　ワクチン接種記録システム(VRS)へのログイン用のユーザIDに付与されるアクセス権限は、横浜市が指定する管理者が必要最小限の権限で発効する。 　横浜市が指定する管理者は、定期的にユーザID及びアクセス権限の一覧をシステムにおいて確認し、アクセス権限及び不正利用の有無を確認する。また、不要となったユーザ ID やアクセス権限を速やかに変更又は削除する。	＜予防接種台帳システムにおける対策＞ ・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。 ＜統合番号連携システムにおける対策＞ ・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。	事後	実態に基づく修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3．特定個人情報の使用 リスク2：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク 特定個人情報の使用の記録 具体的な管理方法	・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。 ＜ワクチン接種記録システム(VRS)における追加措置＞ システム上の操作のログを取得しており、操作ログを確認できる。ログは定期に及び必要に応じ随時に確認する。	・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。 ＜統合番号連携システムにおける対策＞ ・「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。	事後	実態に基づく修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3．特定個人情報の使用 リスク4：特定個人情報ファイルが不正に複製されるリスク 特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ワクチン接種記録システム(VRS)からCSVファイルにてダウンロードする接種記録データには、個人番号が含まれない。	（削除）	事後	実態に基づく削除
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4．特定個人情報ファイルの取扱いの委託 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	個人情報の保護に関する法律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	軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク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）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。	＜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＞ ・情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ・中間サーバーの職員認証・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）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク2：安全が保たれない方法によって入手が行われるリスク 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。 ・団体内統合宛名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。	＜横浜市における措置＞ ・統合番号連携システムのサーバ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＞ ・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。 ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク4：入手の際に特定個人情報が漏えい・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。 ・団体内統合宛名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＞ 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。	＜横浜市における措置＞ ・統合番号連携システムのサーバ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、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ・既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ・情報照会が完了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。 ・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＞ ・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。 ・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。 ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク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機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。	＜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の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＞ ・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。 ・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。 ・機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク6：不適切な方法で提供されるリスク リスクに対する措置の内容	＜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。	＜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の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＞ ・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＞ ・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。 ・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。 ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク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。	＜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の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＞ ・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。 ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。	＜中間サーバー・ソフトウェアにおける措置＞ ・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＞ ・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。 ・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。 ・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。 ・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。	事後	表現の軽微な修正

令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	＜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。 ②事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。 ＜ワクチン接種記録システム(VRS)における措置＞ ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための 統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウド サービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める物 理的対策を満たしている。 主に以下の物理的対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスを利用している。	＜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＞ ・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。 ・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	事後	実態に基づく修正

令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	・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。 ＜ワクチン接種記録システム(VRS)における措置＞ ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める技術的対策を満たしている。 主に以下の技術的対策を講じている。 ・論理的に区分された本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、外部からの侵入検知・通知機能を備えている。 ・LG-WAN端末とワクチン接種記録システムとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。	＜横浜市における措置＞ ・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＞ ・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。 ・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。 ・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。	事後	実態に基づく修正
令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク 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 その内容	別紙のとおり	別紙2のとおり	事後	表現の軽微な修正

令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク 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 再発防止策の内容	別紙のとおり	別紙2のとおり	事後	表現の軽微な修正
令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑩死者の個人番号	[　保管していない　]	[　保管している　]	事後	実態に基づく修正
令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑩死者の個人番号 具体的な保管方法	（追加）	・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、団体内統合宛名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：団体内統合宛名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。	事後	実態に基づく修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2．特定個人情報の入手（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。 〇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。	・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。 〇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、個人番号と団体内統合宛名番号及び宛名番号の正確な紐付けを担保する。 ・住民登録外の者の分：統合端末を用いて本人確認を行うか、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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク1：目的外の入手が行われるリスク 必要な情報以外を入手することを防止するための措置の内容	・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。 〇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。 ・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。	・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。 〇団体内統合宛名システムの検索画面を使用する際の措置 ・個人番号、団体内統合宛名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。 ・団体内統合宛名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。 ・団体内統合宛名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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク2：不適切な方法で入手が行われるリスク リスクに対する措置の内容	・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。	・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。 ・健康管理システム（予防接種分野）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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク3：入手した特定個人情報が不正確であるリスク 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を利用して照合を行う。 ・住登外者の場合：住基ネット統合端末を利用して照合を行う。	・住登内者の場合：団体内統合宛名システム端末を利用して照合を行う。 ・住登外者の場合：住基ネット統合端末を利用して照合を行う。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク1：目的を超えた紐付け、事務に必要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。	・団体内統合宛名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。 ・団体内統合宛名システムでは個人番号、団体内統合宛名番号及び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。 ・団体内統合宛名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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク1：目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク 事務で使用するその他のシステムにおける措置の内容	・予防接種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よう記録を残す。	・健康管理システム（予防接種分野）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よう記録を残す。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク ユーザ認証の管理 具体的な管理方法	・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。 ＜統合番号連携システムにおける対策＞ ・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。	・健康管理システム（予防接種分野）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。 ＜団体内統合宛名システムにおける対策＞ ・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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の発行・失効の管理 具体的な管理方法	＜予防接種台帳システムにおける対策＞ ・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。 ・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。 ＜統合番号連携システムにおける対策＞ ・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。 ・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。	＜健康管理システム（予防接種分野）における対策＞ ・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。 ・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。 ＜団体内統合宛名システムにおける対策＞ ・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。 ・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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の管理 具体的な管理方法	＜予防接種台帳システムにおける対策＞ ・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。 ＜統合番号連携システムにおける対策＞ ・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。	＜健康管理システム（予防接種分野）における対策＞ ・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。 ＜団体内統合宛名システムにおける対策＞ ・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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2：権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク 特定個人情報の使用の記録 具体的な管理方法	・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。 ＜統合番号連携システムにおける対策＞ ・「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。	・健康管理システム（予防接種分野）へのログイン記録、健康管理システム（予防接種分野）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。 ＜団体内統合宛名システムにおける対策＞ ・「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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク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＞ ・情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ・中間サーバーの職員認証・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）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。	＜横浜市における措置＞ 〇団体内統合宛名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団体内統合宛名システムを使用できる仕組みを構築する。 ・団体内統合宛名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、団体内統合宛名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。 ・団体内統合宛名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＞ ・情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ・中間サーバーの職員認証・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）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク2：安全が保たれない方法によって入手が行われるリスク 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＞ ・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。 ・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。	＜横浜市における措置＞ ・団体内統合宛名システムのサーバ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。 ・団体内統合宛名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＞ ・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。 ・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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク3：入手した特定個人情報が不正確であるリスク 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。	＜横浜市における措置＞ 団体内統合宛名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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク4：入手の際に特定個人情報が漏えい・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、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ・既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ・情報照会が完了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。 ・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＞ ・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。 ・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。 ・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。	＜横浜市における措置＞ ・団体内統合宛名システムのサーバ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。 ・団体内統合宛名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、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ・既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ・情報照会が完了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。 ・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＞ ・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。 ・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。 ・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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク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の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＞ ・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。 ・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。 ・機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ・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。	＜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、サーバ等へのアクセス権限を設定する。 ・団体内統合宛名システムの画面からの副本への登録においては、団体内統合宛名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＞ ・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。 ・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。 ・機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ・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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク6：不適切な方法で提供されるリスク リスクに対する措置の内容	＜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の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＞ ・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＞ ・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。 ・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。 ・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。	＜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、サーバ等へのアクセス権限を設定する。 ・団体内統合宛名システムの画面からの副本への登録においては、団体内統合宛名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＞ ・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＞ ・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。 ・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。 ・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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク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の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＞ ・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。 ・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。	＜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、サーバ等へのアクセス権限を設定する。 ・団体内統合宛名システムの画面からの副本への登録においては、団体内統合宛名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＞ ・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。 ・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。	事前	システム標準化による修正

令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	＜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＞ ・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。 ・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	＜横浜市における措置＞ ・団体内統合宛名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。 ・団体内統合宛名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。 ・団体内統合宛名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＞ ・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。 ・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	事前	システム標準化による修正
令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	＜横浜市における措置＞ ・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＞ ・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。 ・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。 ・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。	＜横浜市における措置＞ ・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。 ・団体内統合宛名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＞ ・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。 ・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。 ・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。	事前	システム標準化による修正

（別紙）全項目評価書の変更箇所 【Ⅲリスク対策(団体内統合宛名ファイル)】

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） 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
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
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
令和3年6月15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：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	（※2）番号法第19条第7号、第8号及び第16号に基づき、事務手続ごとに情報照会者、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。	（※2）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。	事後	中間サーバー・プラットフォームの更改に伴う修正

令和3年6月15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	・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。	・機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。	事後	中間サーバー・プラットフォームの更改に伴う修正
令和3年6月15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） 7. 特定個人情報の保管・消去 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	＜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。	＜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。 ・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	事後	中間サーバー・プラットフォームの更改に伴う修正
令和6年4月30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） 7. 特定個人情報の保管・消去 ⑤物理的対策 具体的な対策の内容	（新型コロナウイルス感染症予防接種証明書コンビニ交付） ・証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。 ・キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。また、通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。	（削除）	事後	ワクチン接種記録システム（VRS）の機能縮小等に伴う軽微な修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク1：目的外の入手が行われるリスク 必要な情報以外を入手することを防止するための措置の内容	○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。	○統合番号連携システムの検索画面を使用する際の措置 ・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。 ・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。 ○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。	事後	実態に基づく修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク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 ユーザー認証の管理 具体的な方法	・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。	＜統合番号連携システムにおける対策＞ ・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。	事後	表現の軽微な修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4. 特定個人情報ファイルの取扱いの委託 特定個人情報の消去ルール 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。	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。消去したときは、消去報告書を提出させる。 遵守の確認については、毎月業務完了報告書にて行う。	事後	実態に基づく修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4. 特定個人情報ファイルの取扱いの委託 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	個人情報の保護に関する法律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	軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク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団体内統合宛名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団体内統合宛名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）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。	＜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＞ ・情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ・中間サーバーの職員認証・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）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク2：安全が保たれない方法によって入手が行われるリスク 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。	＜横浜市における措置＞ ・統合番号連携システムのサーバ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＞ ・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。 ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク4：入手の際に特定個人情報が漏えい・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。	＜横浜市における措置＞ ・統合番号連携システムのサーバ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、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ・既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ・情報照会が完了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。 ・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＞ ・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。 ・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。 ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク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機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。	＜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の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＞ ・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。 ・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。 ・機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク6：不適切な方法で提供されるリスク リスクに対する措置の内容	＜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。	＜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の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＞ ・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＞ ・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。 ・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。 ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク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。	＜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の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＞ ・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。 ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。	＜中間サーバー・ソフトウェアにおける措置＞ ・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＞ ・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。 ・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。 ・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。 ・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。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 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。 ・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、仏用に応じてセキュリティパッチの適用を行う。	＜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＞ ・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。 ・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	事後	表現の軽微な修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7．特定個人情報の保管・消去 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	＜横浜市における措置＞ ・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。 ＜ワクチン接種記録システム(VRS)における措置＞ ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める技術的対策を満たしている。 主に以下の技術的対策を講じている。 ・論理的に区分された本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、外部からの侵入検知・通知機能を備えている。 ・LG-WAN端末とワクチン接種記録システムとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。	＜横浜市における措置＞ ・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＞ ・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。 ・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。 ・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。	事後	表現の軽微な修正
令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク 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 その内容	別紙のとおり	別紙2のとおり	事後	表現の軽微な修正

令和8年1月13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 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 リスク1：特定個人情報の漏えい・滅失・毀損リスク 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 再発防止策の内容	別紙のとおり	別紙2のとおり	事後	表現の軽微な修正
令和8年1月13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 1．特定個人情報ファイル名	統合番号連携ファイル	団体内統合宛名ファイル	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2．特定個人情報の入手（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。	○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、個人番号と団体内統合宛名番号及び宛名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、健康管理システム（予防接種分野）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。 ○団体内統合宛名システムの検索画面を使用する際の措置 ・個人番号、団体内統合宛名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。 ・団体内統合宛名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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク1：目的外の入手が行われるリスク 必要な情報以外を入手することを防止するための措置の内容	○統合番号連携システムの検索画面を使用する際の措置 ・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。 ・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。 ○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。	○団体内統合宛名システムの検索画面を使用する際の措置 ・団体内統合宛名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、団体内統合宛名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。 ・団体内統合宛名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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク2：不適切な方法で入手が行われるリスク リスクに対する措置の内容	○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。	○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、団体内統合宛名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団体内統合宛名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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク3：入手した特定個人情報が不正確であるリスク 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。	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、その結果をもとに団体内統合宛名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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク3：入手した特定個人情報が不正確であるリスク 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。	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、随時に団体内統合宛名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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク4：入手の際に特定個人情報が漏えい・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。	○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。 両システムとも団体内統合宛名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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク1：目的を超えた紐付け、事務に必要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。	・団体内統合宛名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。 ・団体内統合宛名システムでは個人番号、団体内統合宛名番号及び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。 ・団体内統合宛名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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク1：目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク 事務で使用するその他のシステムにおける措置の内容	○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。	○福祉保健システム端末を使用する際の措置 ・団体内統合宛名システム、健康管理システム（予防接種分野）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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク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 ユーザー認証の管理 具体的な方法	＜統合番号連携システムにおける対策＞ ・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。	＜団体内統合宛名システムにおける対策＞ ・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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク3：従業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。	・団体内統合宛名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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク4：特定個人情報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。	・管理者権限を持たない者に対する措置：団体内統合宛名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。団体内統合宛名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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク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＞ ・情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ・中間サーバーの職員認証・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）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。	＜横浜市における措置＞ 〇団体内統合宛名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団体内統合宛名システムを使用できる仕組みを構築する。 ・団体内統合宛名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、団体内統合宛名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。 ・団体内統合宛名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＞ ・情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ・中間サーバーの職員認証・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）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク2：安全が保たれない方法によって入手が行われるリスク 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＞ ・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。 ・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。	＜横浜市における措置＞ ・団体内統合宛名システムのサーバ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。 ・団体内統合宛名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＞ ・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。 ・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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク3：入手した特定個人情報が不正確であるリスク 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。	＜横浜市における措置＞ 団体内統合宛名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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク4：入手の際に特定個人情報が漏えい・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、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ・既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ・情報照会が完了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。 ・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＞ ・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。 ・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。 ・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。	＜横浜市における措置＞ ・団体内統合宛名システムのサーバ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。 ・団体内統合宛名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、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ・既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ・情報照会が完了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。 ・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＞ ・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。 ・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。 ・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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク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の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＞ ・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。 ・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。 ・機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ・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。	＜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、サーバ等へのアクセス権限を設定する。 ・団体内統合宛名システムの画面からの副本への登録においては、団体内統合宛名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＞ ・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。 ・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。 ・機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ・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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク6：不適切な方法で提供されるリスク リスクに対する措置の内容	＜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の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＞ ・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＞ ・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。 ・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。 ・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。	＜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、サーバ等へのアクセス権限を設定する。 ・団体内統合宛名システムの画面からの副本への登録においては、団体内統合宛名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＞ ・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＞ ・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。 ・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。 ・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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク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の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＞ ・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。 ・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。	＜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、サーバ等へのアクセス権限を設定する。 ・団体内統合宛名システムの画面からの副本への登録においては、団体内統合宛名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＞ ・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。 ・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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 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＞ ・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。 ・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	＜横浜市における措置＞ ・団体内統合宛名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。 ・団体内統合宛名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。 ・団体内統合宛名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＞ ・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。 ・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	＜横浜市における措置＞ ・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＞ ・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。 ・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。 ・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。	＜横浜市における措置＞ ・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。 ・団体内統合宛名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＞ ・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。 ・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。 ・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。	事前	システム標準化による修正

令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑩死者の個人番号 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。	・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、団体内統合宛名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：団体内統合宛名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。	事前	システム標準化による修正
令和8年1月13日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 リスク2：特定個人情報が古い情報のまま保管され続けるリスク 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。	○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、必要に応じて団体内統合宛名システムの画面から更新する。 ○4情報以外 ・宛名番号は、当該事務にて変更した後、団体内統合宛名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団体内統合宛名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。	事前	システム標準化による修正

（別紙）全項目評価書の変更箇所 【Ⅳリスク対策（その他）】

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3年6月15日	Ⅳ　その他のリスク対策 2. 従業者に対する教育・啓発 従業者に対する教育・啓発 具体的な方法	＜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。 ・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。	＜中間サーバー・プラットフォームにおける措置＞ ・IPA（情報処理推進機構）が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資材を作成し、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、運用規則（接続運用規程等）や情報セキュリティに関する教育を年次（年2回）及び随時（新規要員着任時）実施することとしている。	事後	中間サーバー・プラットフォームの更改に伴う修正
令和4年6月28日	Ⅳ　その他のリスク対策 1. 監査 ①自己点検 具体的なチェック方法	（追加）	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> デジタル庁（旧内閣官房情報通信技術（IT）総合戦略室）から発出された「新型コロナウイルスワクチン接種記録　システムの利用にあたっての確認事項」に同意のうえ、第9条（市区町村の責任）に則し、適切に　職員等の当該システムの利用を管理し、必要な監督をする。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅳ　その他のリスク対策 1. 監査 ②監査 具体的な内容	（追加）	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> デジタル庁（旧内閣官房情報通信技術（IT）総合戦略室）から発出された「新型コロナウイルスワクチン接種記録　システムの利用にあたっての確認事項」に同意のうえ、第9条（市区町村の責任）に則し、適切に　職員等の当該システムの利用を管理し、必要な監督をする。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅳ　その他のリスク対策 2. 従業者に対する教育・啓発 従業者に対する教育・啓発 具体的な方法	（追加）	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> デジタル庁（旧内閣官房情報通信技術（IT）総合戦略室）から発出された「新型コロナウイルスワクチン接種記録　システムの利用にあたっての確認事項」に同意のうえ、第9条（市区町村の責任）に則し、適切に　職員等の当該システムの利用を管理し、必要な指導をする。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和4年6月28日	Ⅳ　その他のリスク対策 3. その他のリスク対策	（追加）	<新型コロナウイルス感染症対策に係る予防接種事務における追加措置> デジタル庁（旧内閣官房情報通信技術（IT）総合戦略室）から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての　確認事項」に同意のうえ、第7条（情報到達の責任分界点）、第8条（通信経路の責任分界点）、　第9条（市区町村の責任）に　則し、適切に当該システムを利用し、万が一、障害や情報漏えいが生じた場合、適切な対応をとることができる体制を構築する。	事後	特定個人情報保護評価に関する規則第9条第2項の規定（緊急時事後評価）の適用
令和6年4月30日	Ⅳ　その他のリスク対策 1. 監査 ①自己点検 具体的なチェック方法	デジタル庁（旧内閣官房情報通信技術（IT）総合戦略室）	厚生労働省	事後	ワクチン接種記録システム（VRS）の業務移管に伴う軽微な修正

令和6年4月30日	Ⅳ その他のリスク対策 1. 監査 ②監査 具体的なチェック方法	デジタル庁（旧内閣官房情報通信技術（IT）総合戦略室）	厚生労働省	事後	ワクチン接種記録システム（VRS）の業務移管に伴う軽微な修正
令和6年4月30日	Ⅳ その他のリスク対策 2. 従業者に対する教育・啓発 従業者に対する教育・啓発 具体的な方法	デジタル庁（旧内閣官房情報通信技術（IT）総合戦略室）	厚生労働省	事後	ワクチン接種記録システム（VRS）の業務移管に伴う軽微な修正
令和6年4月30日	Ⅳ その他のリスク対策 3. その他のリスク対策	デジタル庁（旧内閣官房情報通信技術（IT）総合戦略室）	厚生労働省	事後	ワクチン接種記録システム（VRS）の業務移管に伴う軽微な修正
令和8年1月13日	Ⅳ その他のリスク対策 1. 監査 ① 自己点検 具体的なチェック方法	＜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。 ＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ 厚生労働省から発出された「新型コロナウイルスワクチンに接種切ろうシステムの利用にあたっての確認事項」に同意のうえ、第9上（市区町村の責任）に則し、適切に職員等の当該システムの利用を管理し、必要な監督をする。	＜横浜市における措置＞ 特定個人情報に関する監査において、定期的に自己点検を行う。 ＜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。	事後	実態に基づく修正
令和8年1月13日	Ⅳ その他のリスク対策 1. 監査 ② 監査 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。 ＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ 厚生労働省から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条（市区町村の責任）に則し、適切に職員等の当該システムの利用を管理し、必要な監督をする。	＜横浜市における措置＞ 特定個人情報に関する監査において、定期的に監査を行う。 ＜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・プラットフォームについて、定期的に監査を行うこととしている。	事後	実態に基づく修正

令和8年1月13日	Ⅳ　その他のリスク対策 2.　従業者に対する教育・啓発 従業者に対する教育・啓発 具体的な方法	＜横浜市における措置＞ 年に1回、特定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＞ ・IPA（情報処理推進機構）が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資材を作成し、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、運用規則（接続運用規程等）や情報セキュリティに関する教育を年次（年2回）及び随時（新規要員着任時）実施することとしている。 ＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ 厚生労働省から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条（市区町村の責任）に則し、適切に職員等の当該システムの利用を管理し、必要な指導をする。	＜横浜市における措置＞ 年に1回、特定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＞ ・IPA（情報処理推進機構）が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資材を作成し、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、運用規則（接続運用規程等）や情報セキュリティに関する教育を年次（年2回）及び随時（新規要員着任時）実施することとしている。	事後	実態に基づく修正
令和8年1月13日	Ⅳ　その他のリスク対策 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。 ＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ 厚生労働省から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第7条（情報到達の責任分界点）、第8条（通信経路の責任分界点）、第9条（市区町村の責任）に則し、適切に当該システムの利用し、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。	＜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。	事後	実態に基づく修正

（別紙）全項目評価書の変更箇所 【Ⅴ開示請求、問合せ】

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3年6月15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	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	横浜市役所 　市民局市民情報センター 231-0005　横浜市中区本町6-50-10 045-671-3882	事後	市庁舎移転に伴う修正
令和3年6月15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 ④個人情報ファイル簿の公表 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	横浜市役所　市民局市民情報センター 231-0005 横浜市中区本町6-50-10 045-671-3900	事後	市庁舎移転に伴う修正
令和3年6月15日	Ⅴ 開示請求、問合せ 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	健康福祉局健康安全部健康安全課　予防接種担当 住　　所：〒231-0005　横浜市中区本町6-50-10 電話番号：045-671-4190	事後	市庁舎移転に伴う修正
令和5年8月4日	Ⅴ　開示請求、問合せ 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	医療局健康安全部健康安全課　予防接種担当	事後	組織再編による修正
令和8年1月13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 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。	持参又は郵送による指定様式での書面の提出により開示・訂正・利用停止請求を受け付ける。	事後	軽微な修正
令和8年1月13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 ④　個人情報ファイル簿の公表 個人情報ファイル名	予防接種対象者関係情報ファイル	予防接種関係情報ファイル、統合番号連携ファイル	事後	表現の軽微な修正

令和8年1月13日	Ⅴ　開示請求、問合せ 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	医療局健康安全部健康安全課　予防接種担当 住　　所:〒231-0005　横浜市中区本町6-50-10 電話番号:045-671-4190	医療局健康安全部健康安全課　予防接種係 住　　所:〒231-0005　横浜市中区本町6-50-10 電話番号:045-671-4190	事後	組織再編による修正
令和8年1月13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 ④　個人情報ファイル簿の公表 個人情報ファイル名	予防接種関係情報ファイル、統合番号連携ファイル	予防接種関係情報ファイル、団体内統合宛名ファイル	事前	表現の軽微な修正

（別紙）全項目評価書の変更箇所 【Ⅵ評価実施手続】

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	（追加）	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8年1月13日	Ⅵ　評価実施手続 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）、番号制度事務取りまとめ課への持参いよる意見聴取を行う。	市ウェブサイトでの公開、市民情報センター及び各区役所での閲覧により市民意見募集を行う。意見は、郵便、ファクシミリ又は所管課への持参により受け付ける。	事後	軽微な修正
令和8年1月13日	Ⅵ　評価実施手続 2．国民・住民等からの意見の聴取 ②　実施日・期間	令和5年4月10日から令和5年5月10日まで	令和7年9月18日～10月17日	事前	実施日・期間の更新
令和8年1月13日	Ⅵ　評価実施手続 3．第三者点検 ①　実施日	令和5年5月31日	令和7年11月26日	事前	実施日の更新