特定個人情報保護評価書（全項目評価書）

評価書番号	評価書名
55	新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務　全項目評価書

個人のプライバシー等の権利利益の保護の宣言

藤沢市は、新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務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取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減させるために適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項	

評価実施機関名

藤沢市長

個人情報保護委員会　承認日　【行政機関等のみ】

公表日

令和7年2月27日

［令和6年10月　様式4］

項目一覧

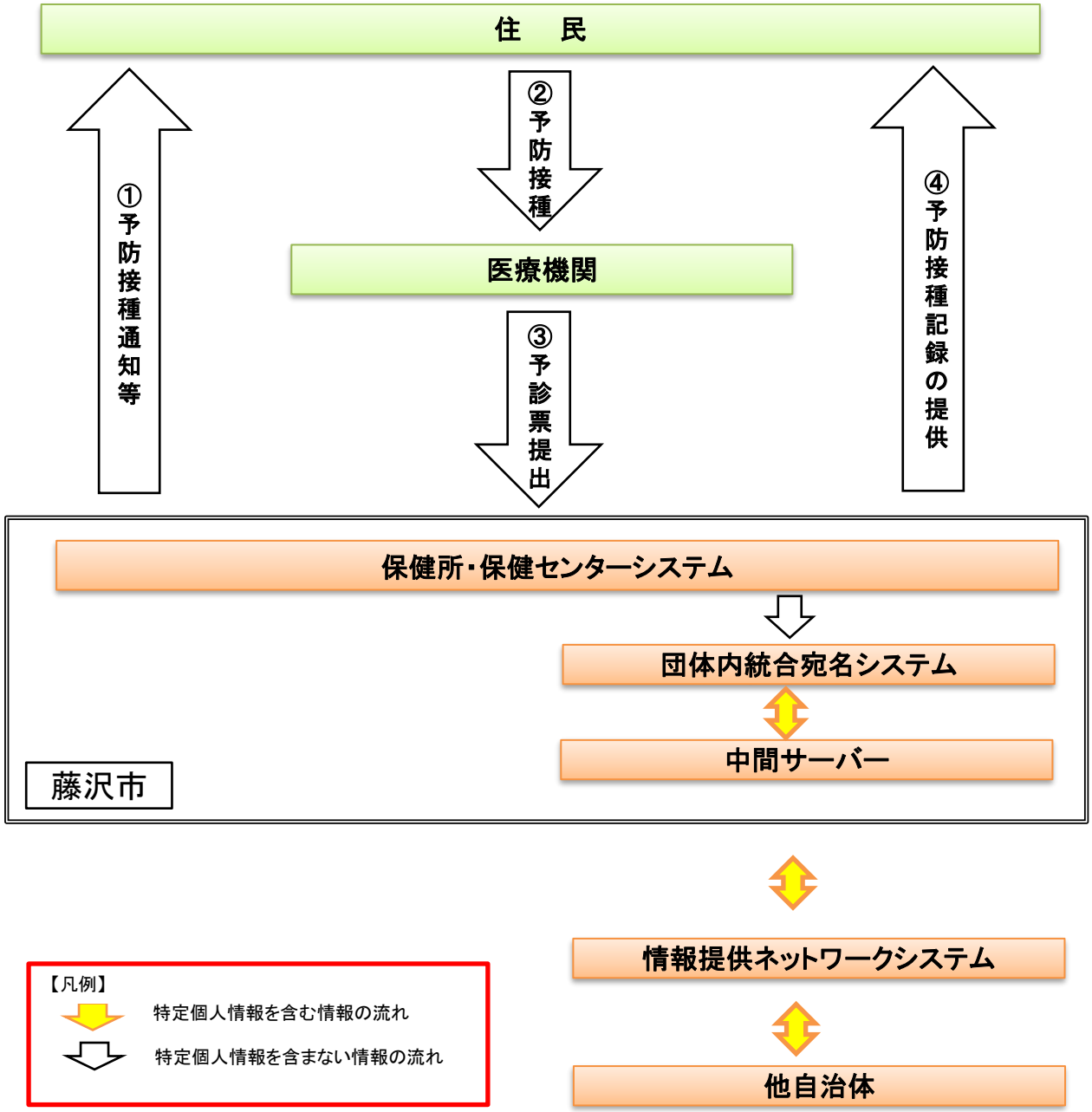
Ⅰ　基本情報

1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務
②事務の内容　※	新型インフルエンザ等が発生した場合に、特定接種や住民に対する予防接種、予診票の発行等を行う。行政手続における特定の個人を識別するための番号の利用等に関する法律（以下、「番号法」という。）第19条第8号に基づく主務省令第2条の表に基づき、新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務において、情報提供ネットワークシステムを接続し、各情報保有機関が保有する特定個人情報について情報連携を行う。
③対象人数	[　30万人以上　] ＜選択肢＞ 1) 1,000人未満　2) 1,000人以上1万人未満 3) 1万人以上10万人未満　4) 10万人以上30万人未満 5) 30万人以上

2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	保健所・保健センター業務情報システム（業務共通システム、予防接種サブシステム）
②システムの機能	1. 対象者抽出機能：予防接種対象者を抽出する。 2. 予防接種入力機能：個人の予防接種の情報を入力する。 3. 予防接種情報取込：予防接種のパンチデータを取込する。 4. 予防接種照会：予防接種の履歴を照会する。 5. 予防接種受検票(クーポン券)を印刷する。 6. 接種履歴票出力：個人の予防接種の接種履歴を印刷する。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[○] 既存住民基本台帳システム [○] 宛名システム等　[　] 税務システム [　] その他　（　）
システム2～5	
システム2	
①システムの名称	団体内統合宛名システム
②システムの機能	1. 団体内統合宛名管理 ・団体内統合宛名番号管理機能 団体内統合宛名番号の付番を行う。 団体内統合宛名番号と保健所・保健センター業務情報システムの宛名番号とをひも付けて管理する。 ・宛名情報管理機能 氏名・住所などの4情報を団体内統合宛名番号にひも付けて管理する。 ・中間サーバ連携機能 中間サーバとのオンラインデータ連携、オフラインデータ連携用の媒体作成を行う。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [○] 住民基本台帳ネットワークシステム　[○] 既存住民基本台帳システム [○] 宛名システム等　[○] 税務システム [○] その他　（ 保健所・保健センター業務情報システム、中間サーバー　）

システム3	
①システムの名称	中間サーバー
②システムの機能	1. 各種設定機能 利用する職員のアカウント登録、権限管理等の設定等。 2. 符号取得機能 団体内統合宛名システムにて保持している団体内統合宛名番号を利用し、符号を取得する。 3. 情報提供用のデータ登録機能 特定個人情報（連携対象）の登録を行う。 4. 情報照会機能 情報提供の求めを行い、特定個人情報（連携対象）を取得する。 5. 情報提供機能 情報提供の求めに対して、特定個人情報（連携対象）の提供を行う。
③他のシステムとの接続	[○] 情報提供ネットワークシステム　　[　　] 庁内連携システム [　　] 住民基本台帳ネットワークシステム　　[　　] 既存住民基本台帳システム [○] 宛名システム等　　[　　] 税務システム [　　] その他　（　　）
システム6～10	
システム11～15	
システム16～20	
3. 特定個人情報ファイル名	
予防接種対象者台帳	
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	新型インフルエンザ等対策特別措置法による予防接種においては、制度上、対象者の確認及び接種履歴や未接種者の把握のため、特定個人情報ファイルを取り扱う必要がある。
②実現が期待されるメリット	予防接種の対象者であることの確認、接種記録の管理等により、未接触者を迅速に把握でき、感染症の発生及びまん延防止につながる。
5. 個人番号の利用　※	
法令上の根拠	・番号法第9条第1項及び別表126の項 ・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第67条の2
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[　　実施する　　]　　＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	・情報照会の根拠 番号法第19条第8号に基づく主務省令第2条の表153の項 ・情報提供の根拠 番号法第19条第8号に基づく主務省令第2条の表25、26、153、154の項
7. 評価実施機関における担当部署	
①部署	藤沢市保健所　保健予防課
②所属長の役職名	保健予防課長
8. 他の評価実施機関	

（別添1）事務の内容


住　民
①予防接種通知等
②予防接種
医療機関
③予診票提出
④予防接種記録の提供
保健所・保健センターシステム
団体内統合宛名システム
中間サーバー
藤沢市
情報提供ネットワークシステム
他自治体
【凡例】
特定個人情報を含む情報の流れ
特定個人情報を含まない情報の流れ

（備考）

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名		
予防接種対象者台帳		
2. 基本情報		
①ファイルの種類 ※		[　　システム用ファイル　　] ＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※		新型インフルエンザ等対策特別措置法に基づく予防接種対象者
	その必要性	適切な予防接種事業を行うため、予防接種対象者の接種履歴を管理する必要がある。
④記録される項目		[　50項目以上100項目未満　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目 ※	・識別情報 [○] 個人番号　[　] 個人番号対応符号　[○] その他識別情報（内部番号） ・連絡先等情報 [○] 4情報（氏名、性別、生年月日、住所）　[○] 連絡先（電話番号等） [○] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[　] 地方税関係情報　[○] 健康・医療関係情報 [　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [　] その他　（　　）
	その妥当性	1. 識別情報：対象者を正確に特定するために保有 2. 連絡先情報：対象者の期日時点の居住地、連絡先を把握するために保有 3. 健康・医療関係情報：予防接種履歴管理を適正に行うために保有
	全ての記録項目	別添2を参照。
⑤保有開始日		令和3年6月11日
⑥事務担当部署		藤沢市保健所　保健予防課

3. 特定個人情報の入手・使用		
①入手元 ※		[○] 本人又は本人の代理人 [○] 評価実施機関内の他部署 （ 市民自治部市民窓口センター ） [ ] 行政機関・独立行政法人等 （ ） [○] 地方公共団体・地方独立行政法人 （ 他自治体 ） [ ] 民間事業者 （ ） [ ] その他 （ ）
②入手方法		[○] 紙 [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 電子メール [ ] 専用線 [○] 庁内連携システム [○] 情報提供ネットワークシステム [ ] その他 （ ）
③入手の時期・頻度		接種対象者の接種要件等を確認する都度
④入手に係る妥当性		適切な予防接種事業を行うため、必要な特定個人情報を保有する必要がある。
⑤本人への明示		本人から入手する情報については、使用目的を本人に明示したうえで入手する。 庁内連携・情報提供ネットワークシステムからの入手については、番号法第9条第1項別表126の項にて明示されている。（新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務であって主務省令で定めるもの）
⑥使用目的 ※		予防接種事務に関する対象者の特定及び予防接種履歴の管理
	変更の妥当性	
⑦使用の主体	使用部署 ※	藤沢市保健所 保健予防課
	使用者数	[10人以上50人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
⑧使用方法 ※		1. 予防接種対象者確定事務 国から示された予防接種対象者を抽出し必要書類を送付する。 2. 予防接種者管理事務 予防接種済者の管理をする。
	情報の突合 ※	予防接種券・予診票に記入された予防接種番号、住所、氏名、生年月日等と突合し、予防接種対象者であるかの確認。
	情報の統計分析 ※	接種状況調査などの統計分析の実施。
	権利利益に影響を与え得る決定 ※	-
⑨使用開始日		令和3年6月11日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] <選択肢> 1）委託する 2）委託しない （ 1 ） 件
委託事項1		保健所・保健センター業務情報システム保守委託
①委託内容		保健所・保健センター業務情報システム保守業務（システムの運用管理、障害復旧対応等）
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[10万人以上100万人未満] <選択肢> 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	「2、③対象となる本人の範囲」と同上。
	その妥当性	保守業務は、システム上保有する全てのファイルを取扱うため。
③委託先における取扱者数		[10人未満] <選択肢> 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ]専用線 [ ]電子メール [ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ [ ]紙 [○]その他 （ 保健所・保健センター業務情報システム端末の直接操作 ）
⑤委託先名の確認方法		藤沢市情報公開条例に基づき、委託先名の公開を請求できる。
⑥委託先名		委託契約の調達前のため未定
再委託	⑦再委託の有無 ※	[再委託しない] <選択肢> 1）再委託する 2）再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	
委託事項2～5		
委託事項6～10		
委託事項11～15		
委託事項16～20		

5. 特定個人情報の提供・移転（委託に伴うものを除く。）	
提供・移転の有無	[○] 提供を行っている （ 1 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	厚生労働大臣、都道府県知事又は市町村長
①法令上の根拠	番号法第19条第8号に基づく主務省令第2条の表25、26、153、154の項
②提供先における用途	予防接種の実施に関する事務に使用する
③提供する情報	新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務であって主務省令で定めるもの
④提供する情報の対象となる本人の数	[10万人以上100万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2、③対象となる本人の範囲」と同上
⑥提供方法	[○] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑦時期・頻度	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[ ] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	[ ] 庁内連携システム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑦時期・頻度	
移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	

6. 特定個人情報の保管・消去

①保管場所 ※		＜藤沢市における措置＞ 1. 特定個人情報が記録されるデータベースは、厳重な入退室管理を行っている区画の施錠可能なラックに設置されたサーバー内のディスクに保管され、物理的なアクセスを制限している。 2. サーバーやデータベースには、許可された者以外がアクセスできないよう、管理者による認証と認可を必要としている。 3. 届出書等の紙媒体については、施錠ができる保管庫に保管している。 ＜中間サーバー・プラットフォームにおける措置＞ 1. 中間サーバー・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバー室への入室を厳重に管理する。 2. 特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。 ＜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/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ・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。
②保管期間	期間	[20年以上] ＜選択肢＞ 1）1年未満 2）1年 3）2年 4）3年 5）4年 6）5年 7）6年以上10年未満 8）10年以上20年未満 9）20年以上 10）定められていない
	その妥当性	予防接種法等による定めのほか、接種記録確認等の事務のため長期間保管する必要がある。
③消去方法		＜藤沢市における措置＞ ディスク交換やハード更改等の際は、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とともに、必要に応じて職員が当該措置の完了まで立ち合いを行うなど確実な履行を担保する。 ＜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、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、物理的破損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＞ ・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。 ・クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ・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。

7. 備考

（別添2）特定個人情報ファイル記録項目

住民情報
1宛名番号、2カナ氏名、3漢字氏名、4郵便番号、5住所、6方書、7電話番号、8生年月日、9性別、10番地、11枝番1、12枝番2、13枝番3、14世帯番号、15続柄1、16続柄2、17続柄3、18取消コード、19住登フラグ、20外国人フラグ、21外国人本名、22住民となった日、23住民でなくなった日、24住民でなくなったCD、25前漢字住所、26前漢字方書、27転出先漢字住所、28転出先漢字方書
予防接種
1状態、2月齢、3接種種別、4回数、5接種区分、6接種年齢、7会場コード、8会場（医療機関）、9医療機関コード、10実施日、11Lot番号、12接種量、13ツ反結果、14ツ反反応状態、15長径、16ワクチンメーカー、17登録日、18予診医ID、19予診医、20接種医ID，21接種医、22予診医医療機関、23接種医医療機関、24負担金区分、25印刷区分、26印刷日、27予診理由、28地区番号、29地区名称、30備考、31予防枝番、32予備コード、33登録区

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

1．特定個人情報ファイル名	
予防接種対象者台帳	
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	・届出等特定個人情報の入手時には、本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報の入手を防止する。 ・届出書の入力作業後、入力者と別の者が、届出内容と入力内容について再度照合し、確認を行う。 ・番号法及び個人情報の保護に関する法律における不必要な情報の入手を行った際の罰則規定により、目的外の入手を抑制する。
必要な情報以外を入手することを防止するための措置の内容	庁内連携システムを介した情報の入手について、対象事務で必要な情報以外を参照できないようにする。 利用職員によって利用可能な機能を制限し、不必要な情報の入手を防止する。
その他の措置の内容	－
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2：　不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	保健所・保健センター業務情報システムを利用する職員を特定し、ユーザIDと生体認証による二要素認証を実施する。認証後はシステムの権限設定機能により、その利用職員がシステム上で利用可能な機能を制限することで、不適切な方法での入手が行えない対策を実施している。
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3：　入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	予防接種実施時及び申請時の窓口等において、身分証明書（個人番号カード等）の提示を受け、本人確認を行う。
個人番号の真正性確認の措置の内容	個人番号カードの提示または、通知カードと本人確認書類（免許証等）の提示を求め確認を行う。
特定個人情報の正確性確保の措置の内容	・上記の通り、入手の各段階で、本人確認とともに、特定個人情報の正確性を確保する。 ・職員にて収集した情報に基づいて、適宜、職権で修正することで、正確性を確保する。
その他の措置の内容	－
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク4：　入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	・システム内で特定個人情報を扱う画面のアクセスログを取得し、保管している。 ・入力端末が接続するネットワークは、インターネット等外部接続と切り離されている。 ・入力端末におけるUSBメモリー等を用いたデータの持ち出しについては、物理的またはソフトウェア等により制限している。 ・入力端末はのぞき見防止のため、部外者に見えない場所に設置している。 ・入力端末は盗難によるデータ流出を防ぐため、データを保存できない仕組みとなっている。 ・個人情報保護の重要性や情報の取り扱いについて全職員を対象としたeラーニングによる研修を実施している。
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	
－	

3. 特定個人情報の使用		
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容	団体内統合宛名システムでは、番号利用事務以外で個人番号が取得されることのないように、番号利用事務（システム）以外で個人番号での検索を行うことはできない。また、番号利用事務（システム）以外では個人番号は画面表示されない。	
事務で使用するその他のシステムにおける措置の内容	＜団体内統合宛名システムにおける措置＞ 団体内統合宛名システムでは、個人番号関連業務以外は個人番号にアクセスできないよう、個人番号利用事務以外で個人番号の検索を行うことはできない。また、個人番号利用事務以外では個人番号表示時にマスキング処理が実施される。 ＜システム共通における措置＞ システムの稼働するLANでは、外部からの侵入ができないようファイアウォールによる適切なアクセス制御を実施している。	
その他の措置の内容	－	
リスクへの対策は十分か	［　　十分である　　］	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク		
ユーザ認証の管理	［　行っている　］	＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	端末のログイン時は生体認証、業務システムへのログイン時は生体認証による識別とユーザIDによる認証を実施しており、認証後は利用の認可機能により、そのユーザがシステム上で利用可能な権限を制限することで、不正利用が行えない対策を実施している。	
アクセス権限の発効・失効の管理	［　行っている　］	＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	＜システム共通における運用にかかる措置＞ ・ユーザIDごとのアクセス権限の登録及び変更の際は、保健予防課長及び情報システム部門の長の許可を得た上で、情報システム部門担当課が設定の変更を行っている。情報システム部門担当課以外の者は、アクセス権限の登録／変更を行うためのアクセス権限が与えられていない。 ＜団体内統合宛名システムにおける措置＞ ・ユーザあるいはグループ単位で権限付与を実施できる機能を有している。	
アクセス権限の管理	［　行っている　］	＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	＜システム共通における運用にかかる措置＞ ・システムへのユーザIDごとのアクセス権限については、情報セキュリティの担当者が管理を行っている。 ・操作者ごとに更新権限の必要があるか、照会権限のみでよいのかを確認し、業務に必要なアクセス権限のみ付与されるよう管理する。 ・権限を有している職員の異動・退職情報を日々確認を実施し、不要となったIDや権限を変更または削除する。 ＜団体内統合宛名システムにおける措置＞ ・ユーザあるいはグループ単位でアクセス権限を管理している。	
特定個人情報の使用の記録	［　　記録を残している　　］	＜選択肢＞ 1）記録を残している　2）記録を残していない
具体的な方法	＜保健所・保健センター業務情報システムにおける措置＞ ・操作者による認証から認証解除を行うまでの間、監査証跡の記録を行っている。 （操作者がどの個人に対して照会を行ったかを記録している。） ・自動実行等による処理についても、同様に監査証跡の記録を行っている。 ＜団体内統合宛名システムにおける措置＞ ・操作者による認証から認証解除を行うまでの間、監査証跡の記録を行っている。 （操作者がどの個人に対して照会を行ったかを記録している。） ・自動実行等による処理については、処理の実行記録を保管しており、正常／異常の監視を翌日確認している。	
その他の措置の内容	－	
リスクへの対策は十分か	［　　十分である　　］	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク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	＜システム共通における運用にかかる措置＞ ・ユーザIDごとのアクセス権限の登録及び変更の際は、保健予防課長及び情報システム部門の長の許可を得た上で、情報システム部門担当課が設定の変更を行っている。情報システム部門担当課以外の者は、アクセス権限の登録／変更を行うためのアクセス権限が与えられていない。 ・システムの操作履歴(操作ログ)を記録する。 ・権限を有している職員の異動・退職情報を日々確認を実施し、不要となったIDや権限を変更または削除する。 ・システム利用職員への研修会等を定期的（1年に1度）に実施し、事務外使用の禁止について指導を行っている。 ・番号法及び個人情報の保護に関する法律において、事務外使用を行った際の罰則規定により抑制する。 ＜団体内統合宛名システムにおける措置＞ ・ユーザIDによる認証と認可機能により、そのユーザがシステム上で利用可能な機能を制限することで、個人番号関連業務関係者以外はアクセスできないよう対策を実施している。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク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	・端末におけるUSBメモリー等を用いたデータの持ち出しについては、物理的またはソフトウェア等により制限している。 ・番号法及び個人情報の保護に関する法律において、不正な複製を行った際の罰則規定により抑制する。 ・業務上必要に応じ作成した複製物については、使用後すみやかに廃棄削除を行う。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
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	
その他、特定個人情報の使用にあたり、以下の措置を講じる。 ・スクリーンセーバ等を利用して、長時間にわたり本人確認情報を表示させない ・端末のディスプレイを、来庁者から見えない位置に置く ・本人確認情報が表示された画面のハードコピーの取得は事務処理に必要となる範囲にとどめる	
4. 特定個人情報ファイルの取扱いの委託	**[ ] 委託しない**
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク	
情報保護管理体制の確認	外部委託業者の選定に際しては、藤沢市情報システム管理運営規程に則り、主管課の長が業者に対して、個人情報保護管理の体制が適切かどうかを確認することとしている。 主な確認項目は以下の通り。 ・ISMS、Pマーク等の認証取得情報 ・個人情報保護に関する規程、体制の整備 ・個人情報保護に関する人的安全管理措置－従業者の役割責任の明確化、安全管理措置の周知／教育 ・個人情報保護に関する技術的安全管理措置－利用者の認証、許可、監査及び監査証跡の記録 なお、確認の結果、水準に満たない業者とは委託契約を行わないこととしている。
特定個人情報ファイルの閲覧者・更新者の制限	[制限している] ＜選択肢＞ 1）制限している 2）制限していない
具体的な制限方法	・作業者を限定するために、委託作業者の名簿を提出させる。 ・閲覧／更新権限を持つものを必要最小限にする。 ・閲覧／更新権限を持つ者のアカウント管理を行い、システム上で操作を制限する。 ・閲覧／更新の履歴（ログ）を取得し、不正な使用がないことを確認する。
特定個人情報ファイルの取扱いの記録	[記録を残している] ＜選択肢＞ 1）記録を残している 2）記録を残していない
具体的な方法	委託先において利用するユーザIDについては、職員と同等のログ監視を行っており、利用履歴の参照も職員と同等の確認を行うことができる。

特定個人情報の提供ルール		[　　定めている　　] ＜選択肢＞ 1）定めている　　2）定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	委託先から他者への特定個人情報の提供は認めないことを契約書上明記する。 また、ユーザIDの再利用も認めないことを規定している。
	委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	委託している業務については、主管課に設置された専用のPCを使用して作業を実施しているため、特定個人情報を委託先には提供していない。
特定個人情報の消去ルール		[　　定めている　　] ＜選択肢＞ 1）定めている　　2）定めていない
	ルールの内容及びルール遵守の確認方法	委託先において利用するユーザIDについては、職員と同等のログ監視を行っており、利用履歴の参照も職員と同等の確認を行うことができる。
委託契約書中の特定個人情報ファイルの取扱いに関する規定		[　　定めている　　] ＜選択肢＞ 1）定めている　　2）定めていない
	規定の内容	データの保護及び秘密の保持等の関する仕様書にて、以下の内容を明記 ・個人情報の保護に関する法律の遵守 ・秘密の保持 ・指示目的以外使用及び第三者への提供の禁止 ・データの受領 ・データの持出し ・データの複製及び複製の禁止 ・安全管理義務 ・データの返却・消去 ・記録媒体の廃棄 ・監督及び監査 ・従業員に対する教育の実施 ・事故発生の報告義務
再委託先による特定個人情報ファイルの適切な取扱いの確保		[　再委託していない　] ＜選択肢＞ 1）特に力を入れて行ってい　2）十分に行っている 3）十分に行っていない　4）再委託していない
	具体的な方法	
その他の措置の内容		－
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
－		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[○] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[ ]	＜選択肢＞ 1）記録を残している　2）記録を残していない
具体的な方法		
特定個人情報の提供・移転に関するルール	[ ]	＜選択肢＞ 1）定めている　2）定めていない
ルールの内容及びルール遵守の確認方法		
その他の措置の内容		
リスクへの対策は十分か	[ ]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		

6. 情報提供ネットワークシステムとの接続	[　] 接続しない（入手）　[　] 接続しない（提供）
リスク1： 目的外の入手が行われるリスク	
リスクに対する措置の内容	＜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。つまり中間サーバーは、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。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 安全が保たれない方法によって入手が行われるリスク	
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるように設計されるため、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ネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク3： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	＜中間サーバー・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ネットワーク（総合行政ネットワーク等）を利用することにより、漏えい・紛失のリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視、障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク5： 不正な提供が行われるリスク	
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能（※）により、情報提供ネットワークシステムにおける照会許可用照合リストを情報提供ネットワークシステムから入手し、中間サーバーにも格納して、情報提供機能により、照会許可用照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ②情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。 ③特に慎重な対応が求められる情報については、自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことでセンシティブな特定個人情報が不正に提供されるリスクに対応している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている

リスク6： 不適切な方法で提供されるリスク	
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ①セキュリティ管理機能（※）により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ②中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）暗号化・復号機能と、鍵情報及び照会許可用照合リストを管理する機能。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、不適切な方法で提供されるリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	＜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は、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。 ②情報提供データベース管理機能（※）により「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ③情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 （※）特定個人情報を副本として保存・管理する機能。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	
＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。	
7. 特定個人情報の保管・消去	
リスク1： 特定個人情報の漏えい・滅失・毀損リスク	
①NISC政府機関統一基準群	[政府機関ではない] ＜選択肢＞ 1）特に力を入れて遵守している 2）十分に遵守している 3）十分に遵守していない 4）政府機関ではない
②安全管理体制	[十分に整備している] ＜選択肢＞ 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
③安全管理規程	[十分に整備している] ＜選択肢＞ 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している] ＜選択肢＞ 1）特に力を入れて周知している 2）十分に周知している 3）十分に周知していない

⑤物理的対策		[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
	具体的な対策の内容	＜藤沢市における措置＞ ・特定個人情報を保管するサーバーの設置場所では、入退室管理を行っている。 ・サーバー室内に設置したサーバーは、全て鍵付のサーバーラックに設置している。 ・特定個人情報を扱う職員が離席する際には、特定個人情報を記した書類は机上に放置せず、キャビネットに施錠保管している。 ＜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・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。 ＜ガバメントクラウドにおける措置＞ ・ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ・事前に許可されていない装置等に関しては、外部に持出できないこととしている。
⑥技術的対策		[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
	具体的な対策の内容	＜藤沢市における措置＞ ・特定個人情報ファイルを管理しているサーバーは、インターネット等の外部ネットワークから隔離されたネットワーク上に設置している。 ・特定個人情報ファイルを管理しているサーバーは、ウイルス対策ソフトを導入しており、パターンファイルも最新版が適用されるよう管理している。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームでは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。 ＜ガバメントクラウドにおける措置＞ ・国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ・地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和4年10月　デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ・クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ・クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ・地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ・ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ・地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ・地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。
⑦バックアップ		[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知		[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか		[　発生なし　] ＜選択肢＞ 1）発生あり　2）発生なし
	その内容	－
	再発防止策の内容	－

⑩死者の個人番号	[保管している]	＜選択肢＞ 1）保管している 2）保管していない
具体的な保管方法	生存する個人の個人番号と同様の管理を行う。	
その他の措置の内容	-	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
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	個人番号を含め宛名情報については、住民記録システムと随時異動データを連携することにより最新化する。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	＜選択肢＞ 1）定めている 2）定めていない
手順の内容	個人情報及び個人番号を記録した電磁的記録媒体等を廃棄する際は、必ずデータの消去又は物理的破壊処理をして廃棄をする。 ＜ガバメントクラウドにおける措置＞ データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。	
その他の措置の内容	-	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		
-		

Ⅳ　その他のリスク対策 ※

1. 監査		
①自己点検	[　　十分に行っている　　]	＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
具体的なチェック方法	＜藤沢市における措置＞ 年に1回、担当者が評価書の記載内容通りの運用がされているか確認を行い、必要に応じて運用の見直しを図る。 ＜中間サーバー・プラットフォームにおける措置＞ 運用規則等に基づき、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている	
②監査	[　　十分に行っている　　]	＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
具体的な内容	＜藤沢市における措置＞ 内部監査を定期的に実施し、監査結果を踏まえて体制や規定を改善する。 ＜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。 ＜ガバメントクラウドにおける措置＞ ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。	

2. 従業者に対する教育・啓発		
従業者に対する教育・啓発	[　　十分に行っている　　]	＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
具体的な方法	＜藤沢市における措置＞ ・「マイナンバー制度に係る職員等の教育研修計画」に基づき、個人番号利用事務実施課を対象にした集合研修を実施するとともに、受講者が課内へ研修内容の周知を行っている。また、職員全員を対象に、毎年電子上での机上研修（eラーニング）による個人情報保護及び情報セキュリティに関する研修を実施している。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、セキュリティ研修等を実施することとしている。 ②中間サーバー・プラットフォームの業務に就く場合は、運用規則等について研修を行うこととしている。	

3. その他のリスク対策
＜中間サーバー・プラットフォームにおける措置＞ 　中間サーバー・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減及び、技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。 ＜ガバメントクラウドにおける措置＞ ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。 ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。 具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。

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	藤沢市　市民自治部　市民相談情報課　情報公開センター 〒251－8601 神奈川県藤沢市朝日町1－1 0466－50－3567
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。
特記事項	市のホームページ上に、請求方法、請求様式等について掲載する。
③手数料等	[　　無料　　]　＜選択肢＞ 1) 有料　2) 無料 （手数料額、納付方法：　　）
④個人情報ファイル簿の公表	[　行っていない　]　＜選択肢＞ 1) 行っている　2) 行っていない
個人情報ファイル名	－
公表場所	－
⑤法令による特別の手続	－
⑥個人情報ファイル簿への不記載等	－

2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	藤沢市保健所　保健予防課 〒251－0022 神奈川県藤沢市鵠沼2131－1 0466－50－3593
②対応方法	・問い合わせの対応について、内容により記録を残す。 ・情報漏えい等に関する問い合わせであれば、その事実確認を行うために、処理期間を設ける。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	令和6年12月17日
②しきい値判断結果	[　　基礎項目評価及び全項目評価の実施が義務付けられる　　] ＜選択肢＞ 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 基礎項目評価及び重点項目評価の実施が義務付けられる（任意に全項目評価を実施） 3) 基礎項目評価の実施が義務付けられる（任意に全項目評価を実施） 4) 特定個人情報保護評価の実施が義務付けられない（任意に全項目評価を実施）
2. 国民・住民等からの意見の聴取	
①方法	市HP及び『広報ふじさわ』誌上にて意見の募集の掲載を行い、電子メール又は書面にて意見を受け付ける。
②実施日・期間	令和6年12月25日から令和7年1月23日までの30日間
③期間を短縮する特段の理由	_
④主な意見の内容	ワクチン接種事業に対する反対意見
⑤評価書への反映	なし
3. 第三者点検	
①実施日	令和7年2月13日（木）
②方法	藤沢市個人情報保護制度運営審議会に対する諮問
③結果	藤沢市個人情報保護制度運営審議会から「本評価書については、適当であると認められる。」旨の答申を受けた。
4. 個人情報保護委員会の承認 【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

（別添3）変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和3年12月17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	新型インフルエンザ等が発生した場合に、特定接種や住民に対する予防接種、予診票の発行等を行う。行政手続における特定の個人を識別するための番号の利用等に関する法律（以下、「番号法」という。）第19条第7号別表第二に基づき、新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務において、情報提供ネットワークシステムを接続し、各情報保有機関が保有する特定個人情報について情報連携を行う。	新型インフルエンザ等が発生した場合に、特定接種や住民に対する予防接種、予診票の発行等を行う。行政手続における特定の個人を識別するための番号の利用等に関する法律（以下、「番号法」という。）第19条第8号別表第二に基づき、新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務において、情報提供ネットワークシステムを接続し、各情報保有機関が保有する特定個人情報について情報連携を行う。	事後	番号法第19条の改正に伴う変更であり、重要な事項に該当しない
令和3年12月17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	・番号法　第19条第7号別表第二の115の2の項 ・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二の主務省令で定める事務及び情報を定める命令（以下、「別表第二省令」という。）第59条の2	1　番号法第19条第8号及び別表第二 （別表第二における情報提供の根拠） ・別表第二の115の2の項 （別表第二における情報照会の根拠） ・別表第二の115の2の項 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二の主務省令で定める事務及び情報を定める命令（以下、「別表第二省令」という。） （別表第二省令における情報提供の根拠） ・別表第二省令第59条の2　※別表第二の115の2の項 （別表第二省令における情報照会の根拠） ・別表第二省令第59条の2　※別表第二の115の2の項	事後	番号法第19条の改正に伴う変更であり、重要な事項に該当しない
令和3年12月17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	番号法第19条第7号別表第二	番号法第19条第8号別表第二	事後	番号法第19条の改正に伴う変更であり、事前の提出・公表が義務付けられない
令和3年12月17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	番号法第19条第7号別表第二	番号法第19条第8号別表第二	事後	番号法第19条の改正に伴う変更であり、事前の提出・公表が義務付けられない
令和3年12月17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	番号法第19条第7号別表第二	番号法第19条第8号別表第二	事後	番号法第19条の改正に伴う変更であり、事前の提出・公表が義務付けられない
令和3年12月17日	Ⅲ特定個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 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号に基づき事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。	（※2）番号法別表第2及び第19条第9号に基づき事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。	事後	番号法第19条の改正に伴う変更であり、重要な事項に該当しない
令和5年8月23日	Ⅰ　基本情報　7．評価実施機関における担当部署 ①部署 ②所属長の役職名	①藤沢市保健所　地域保健課 ②地域保健課長	①藤沢市保健所　保健予防課 ②保健予防課長	事後	担当部署名の変更
令和5年8月23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	藤沢市保健所　地域保健課	藤沢市保健所　保健予防課	事後	担当部署名の変更
令和5年8月23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	藤沢市保健所　地域保健課、保健予防課	藤沢市保健所　保健予防課	事後	担当部署名の変更
令和5年8月23日	Ⅲ特定個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 アクセス権限の発効・失効の管理、具体的な管理方法	＜システム共通における運用にかかる措置＞ ・ユーザIDごとのアクセス権限の登録及び変更の際は、地域保健課長及び情報システム部門の長の許可を得た上で、情報システム部門担当課が設定の変更を行っている。情報システム部門担当課以外の者は、アクセス権限の登録／変更を行うためのアクセス権限が与えられていない。 ＜団体内統合宛名システムにおける措置＞ ・ユーザあるいはグループ単位で権限付与を実施できる機能を有している。	＜システム共通における運用にかかる措置＞ ・ユーザIDごとのアクセス権限の登録及び変更の際は、保健予防課長及び情報システム部門の長の許可を得た上で、情報システム部門担当課が設定の変更を行っている。情報システム部門担当課以外の者は、アクセス権限の登録／変更を行うためのアクセス権限が与えられていない。 ＜団体内統合宛名システムにおける措置＞ ・ユーザあるいはグループ単位で権限付与を実施できる機能を有している。	事後	担当部署名の変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年8月23日	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策 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	＜システム共通における運用にかかる措置＞ ・ユーザIDごとのアクセス権限の登録及び変更の際は、地域保健課長及び情報システム部門の長の許可を得た上で、情報システム部門担当課が設定の変更を行っている。情報システム部門担当課以外の者は、アクセス権限の登録／変更を行うためのアクセス権限が与えられていない。 ・システムの操作履歴(操作ログ)を記録する。 ・権限を有している職員の異動・退職情報を日々確認を実施し、不要となったIDや権限を変更または削除する。 ・システム利用職員への研修会等を定期的（1年に1度）に実施し、事務外使用の禁止について指導を行っている。 ・番号法及び藤沢市個人情報の保護に関する条例において、事務外使用を行った際の罰則規定により抑制する。 ＜団体内統合宛名システムにおける措置＞ ・ユーザIDによる認証と認可機能により、そのユーザがシステム上で利用可能な機能を制限することで、個人番号関連業務関係者以外はアクセスできないよう対策を実施している。	＜システム共通における運用にかかる措置＞ ・ユーザIDごとのアクセス権限の登録及び変更の際は、保健予防課長及び情報システム部門の長の許可を得た上で、情報システム部門担当課が設定の変更を行っている。情報システム部門担当課以外の者は、アクセス権限の登録／変更を行うためのアクセス権限が与えられていない。 ・システムの操作履歴(操作ログ)を記録する。 ・権限を有している職員の異動・退職情報を日々確認を実施し、不要となったIDや権限を変更または削除する。 ・システム利用職員への研修会等を定期的（1年に1度）に実施し、事務外使用の禁止について指導を行っている。 ・番号法及び藤沢市個人情報の保護に関する条例において、事務外使用を行った際の罰則規定により抑制する。 ＜団体内統合宛名システムにおける措置＞ ・ユーザIDによる認証と認可機能により、そのユーザがシステム上で利用可能な機能を制限することで、個人番号関連業務関係者以外はアクセスできないよう対策を実施している。	事後	担当部署名の変更
令和5年8月23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わせ ①連絡先	藤沢市保健所　地域保健課 〒251－0022 神奈川県藤沢市鵠沼2131－1 0466－50－3592	藤沢市保健所　保健予防課 〒251－0022 神奈川県藤沢市鵠沼2131－1 0466－50－3593	事後	担当部署名の変更
令和6年12月16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	新型インフルエンザ等が発生した場合に、特定接種や住民に対する予防接種、予診票の発行等を行う。行政手続における特定の個人を識別するための番号の利用等に関する法律（以下、「番号法」という。）第19条第8号別表に基づき、新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務において、情報提供ネットワークシステムを接続し、各情報保有機関が保有する特定個人情報について情報連携を行う。	新型インフルエンザ等が発生した場合に、特定接種や住民に対する予防接種、予診票の発行等を行う。行政手続における特定の個人を識別するための番号の利用等に関する法律（以下、「番号法」という。）第19条第8号に基づく主務省令第2条の表に基づき、新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務において、情報提供ネットワークシステムを接続し、各情報保有機関が保有する特定個人情報について情報連携を行う。	事後	法令の題名等の形式的な変更のため、重要な変更に該当しない
令和6年12月16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		接続先情報の修正	事後	その他の項目であり、事前の提出・公表が義務付けられていない。
令和6年12月16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		接続先情報の修正	事後	その他の項目であり、事前の提出・公表が義務付けられていない。
令和6年12月16日	Ⅰ基本情報　6．個人番号の利用　②法令上の根拠	・番号法　第9条第1項別表第一の93の2の項 ・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一の主務省令で定める事務を定める命令（以下、「別表第一省令」という。）　第67条の2	・番号法第9条第1項及び別表126の項 ・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第67条の2	事後	法令の題名等の形式的な変更のため、重要な変更に該当しない
令和6年12月16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	1　番号法第19条第8号及び別表第二 （別表第二における情報提供の根拠） ・別表第二の115の2の項 （別表第二における情報照会の根拠） ・別表第二の115の2の項 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二の主務省令で定める事務及び情報を定める命令（以下、「別表第二省令」という。） （別表第二省令における情報提供の根拠） ・別表第二省令第59条の2　※別表第二の115の2の項 （別表第二省令における情報照会の根拠） ・別表第二省令第59条の2　※別表第二の115の2の項	・情報照会の根拠 番号法第19条第8号に基づく主務省令第2条の表153の項 ・情報提供の根拠 番号法第19条第8号に基づく主務省令第2条の表25、26、153、154の項	事後	法令の題名等の形式的な変更のため、重要な変更に該当しない
令和6年12月16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本人への明示	本人から入手する情報については、使用目的を本人に明示したうえで入手する。 庁内連携・情報提供ネットワークシステムからの入手については、番号法別表第二の115の2の項にて明示されている。（新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務）	本人から入手する情報については、使用目的を本人に明示したうえで入手する。 庁内連携・情報提供ネットワークシステムからの入手については、番号法第9条第1項別表126の項にて明示されている。（新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務であって主務省令で定めるもの）	事後	法令の題名等の形式的な変更のため、重要な変更に該当しない
令和6年12月16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取り扱いの委託　⑥委託先名	富士通株式会社神奈川支社	富士通Japan株式会社神奈川支社	事後	その他の項目であり、事前の提出・公表が義務付けられていない。
令和6年12月16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	番号法第19条第8号別表第二	厚生労働大臣、都道府県知事又は市町村長	事後	その他の項目であり、事前の提出・公表が義務付けられていない。
令和6年12月16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	番号法第19条第8号別表第二	番号法第19条第8号に基づく主務省令第2条の表25、26、153、154の項	事後	法令の題名等の形式的な変更のため、重要な変更に該当しない

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月16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	番号法第19条第8号別表第二	予防接種の実施に関する事務に使用する	事後	その他の項目であり、事前の提出・公表が義務付けられていない。
令和6年12月16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	予防接種法施行令第6条の2において、5年間保管すると定められているが、接種記録確認等の事務のため長期間保管する必要がある。	予防接種法等による定めのほか、接種記録確認等の事務のため長期間保管する必要がある。	事後	その他の項目であり、事前の提出・公表が義務付けられていない。
令和6年12月16日	Ⅲ特定個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	・届出等特定個人情報の入手時には、本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報の入手を防止する。 ・届出書の入力作業後、入力者と別の者が、届出内容と入力内容について再度照合し、確認を行う。 ・番号利用法及び藤沢市個人情報の保護に関する条例における不必要な情報の入手を行った際の罰則規定により、目的外の入手を抑制する。	・届出等特定個人情報の入手時には、本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報の入手を防止する。 ・届出書の入力作業後、入力者と別の者が、届出内容と入力内容について再度照合し、確認を行う。 ・番号法及び個人情報の保護に関する法律における不必要な情報の入手を行った際の罰則規定により、目的外の入手を抑制する。	事後	法令の題名等の形式的な変更のため、重要な変更に該当しない
令和6年12月16日	Ⅲ特定個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　入手の際の本人確認の措置の内容	窓口において、身分証明書（個人番号カード等）の提示を受け、本人確認を行う。	予防接種実施時及び申請時の窓口等において、身分証明書（個人番号カード等）の提示を受け、本人確認を行う。	事後	その他の項目であり、事前の提出・公表が義務付けられていない。
令和6年12月16日	Ⅲ特定個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：従業員が事務外で使用するリスク　リスクに対する措置の内容	＜システム共通における運用にかかる措置＞ ・ユーザIDごとのアクセス権限の登録及び変更の際は、保健予防課長及び情報システム部門の長の許可を得た上で、情報システム部門担当課が設定の変更を行っている。情報システム部門担当課以外の者は、アクセス権限の登録／変更を行うためのアクセス権限が与えられていない。 ・システムの操作履歴(操作ログ)を記録する。 ・権限を有している職員の異動・退職情報を日々確認を実施し、不要となったIDや権限を変更または削除する。 ・システム利用職員への研修会等を定期的（1年に1度）に実施し、事務外使用の禁止について指導を行っている。 ・番号法及び藤沢市個人情報の保護に関する条例において、事務外使用を行った際の罰則規定により抑制する。 ＜団体内統合宛名システムにおける措置＞ ・ユーザIDによる認証と認可機能により、そのユーザがシステム上で利用可能な機能を制限することで、個人番号関連業務関係者以外はアクセスできないよう対策を実施している。	＜システム共通における運用にかかる措置＞ ・ユーザIDごとのアクセス権限の登録及び変更の際は、保健予防課長及び情報システム部門の長の許可を得た上で、情報システム部門担当課が設定の変更を行っている。情報システム部門担当課以外の者は、アクセス権限の登録／変更を行うためのアクセス権限が与えられていない。 ・システムの操作履歴(操作ログ)を記録する。 ・権限を有している職員の異動・退職情報を日々確認を実施し、不要となったIDや権限を変更または削除する。 ・システム利用職員への研修会等を定期的（1年に1度）に実施し、事務外使用の禁止について指導を行っている。 ・番号法及び個人情報の保護に関する法律において、事務外使用を行った際の罰則規定により抑制する。 ＜団体内統合宛名システムにおける措置＞ ・ユーザIDによる認証と認可機能により、そのユーザがシステム上で利用可能な機能を制限することで、個人番号関連業務関係者以外はアクセスできないよう対策を実施している。	事後	法令の題名等の形式的な変更のため、重要な変更に該当しない
令和6年12月16日	Ⅲ特定個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	・端末におけるUSBメモリー等を用いたデータの持ち出しについては、物理的またはソフトウェア等により制限している。 ・番号法及び藤沢市個人情報の保護に関する条例において、不正な複製を行った際の罰則規定により抑制する。 ・業務上必要に応じ作成した複製物については、使用後すみやかに廃棄削除を行う。	・端末におけるUSBメモリー等を用いたデータの持ち出しについては、物理的またはソフトウェア等により制限している。 ・番号法及び個人情報の保護に関する法律において、不正な複製を行った際の罰則規定により抑制する。 ・業務上必要に応じ作成した複製物については、使用後すみやかに廃棄削除を行う。	事後	法令の題名等の形式的な変更のため、重要な変更に該当しない
令和6年12月16日	Ⅲ特定個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　規定の内容	データの保護及び秘密の保持等の関する仕様書にて、以下の内容を明記 ・藤沢市個人情報の保護に関する条例の遵守 ・秘密の保持 ・指示目的以外使用及び第三者への提供の禁止 ・データの受領 ・データの持出し ・データの複製及び複製の禁止 ・安全管理義務 ・データの返却・消去 ・記録媒体の廃棄 ・監督及び監査 ・従業員に対する教育の実施 ・事故発生の報告義務	データの保護及び秘密の保持等の関する仕様書にて、以下の内容を明記 ・個人情報の保護に関する法律の遵守 ・秘密の保持 ・指示目的以外使用及び第三者への提供の禁止 ・データの受領 ・データの持出し ・データの複製及び複製の禁止 ・安全管理義務 ・データの返却・消去 ・記録媒体の廃棄 ・監督及び監査 ・従業員に対する教育の実施 ・事故発生の報告義務	事後	法令の題名等の形式的な変更のため、重要な変更に該当しない

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月16日	Ⅲ特定個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	＜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。つまり中間サーバーは、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）番号法別表第2及び第19条第9号に基づき事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。	＜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。つまり中間サーバーは、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。	事後	法令の題名等の形式的な変更のため、重要な変更に該当しない
令和7年2月27日	（別添１）事務の内容		図表の微修正	事後	その他の項目であり、事前の提出・公表が義務付けられていない。
令和7年2月27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取扱いの委託　⑥委託先名	富士通Japan株式会社神奈川支社	委託契約の調達前のため未定	事前	その他の項目の変更であり、事後で足りるものの任意に事前に提出
令和7年2月27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取扱いの委託　⑦再委託の有無	再委託あり	再委託なし	事前	令和7年度中に予防接種対象者台帳ファイルをガバメントクラウドでの保管に移行することに伴う重要な変更であり、事前にリスク対策の評価の再実施をするもの
令和7年2月27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		（追記） ＜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/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ・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	令和7年度中に予防接種対象者台帳ファイルをガバメントクラウドでの保管に移行することに伴う重要な追加変更であり、事前にリスク対策の評価の再実施をするもの
令和7年2月27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		（追記） ＜ガバメントクラウドにおける措置＞ ・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。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。 ・クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ・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	令和7年度中に予防接種対象者台帳ファイルをガバメントクラウドでの保管に移行することに伴う重要な追加変更であり、事前にリスク対策の評価の再実施をするもの
令和7年2月27日	Ⅲ特定個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	十分に行っている	再委託していない 具体的な方法を削除	事前	令和7年度中に予防接種対象者台帳ファイルをガバメントクラウドでの保管に移行することに伴う重要な変更であり、事前にリスク対策の評価の再実施をするもの

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7年2月27日	Ⅲ特定個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		（追記） ＜ガバメントクラウドにおける措置＞ ・ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ・事前に許可されていない装置等に関しては、外部に持出できないこととしている。	事前	令和7年度中に予防接種対象者台帳ファイルをガバメントクラウドでの保管に移行することに伴う重要な追加変更であり、事前にリスク対策の評価の再実施をするもの
令和7年2月27日	Ⅲ特定個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		（追記） ＜ガバメントクラウドにおける措置＞ ・国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ・地方公共団体が委託したASP（「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和４年１０月　デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ・クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ・クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ・地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ・ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ・地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ・地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。	事前	令和7年度中に予防接種対象者台帳ファイルをガバメントクラウドでの保管に移行することに伴う重要な追加変更であり、事前にリスク対策の評価の再実施をするもの
令和7年2月27日	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策7.特定個人情報の保管・消去　リスク3：特定個人情報が消去されずいつまでも存在するリスク　消去手順　手順の内容		（追記） ＜ガバメントクラウドにおける措置＞ データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。	事前	令和7年度中に予防接種対象者台帳ファイルをガバメントクラウドでの保管に移行することに伴う重要な追加変更であり、事前にリスク対策の評価の再実施をするもの
令和7年2月27日	Ⅳ　その他のリスク対策　1.監査　②監査　具体的な内容		（追記） ＜ガバメントクラウドにおける措置＞ ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。	事前	令和7年度中に予防接種対象者台帳ファイルをガバメントクラウドでの保管に移行することに伴う重要な追加変更であり、事前にリスク対策の評価の再実施をするもの
令和7年2月27日	Ⅳ　その他のリスク対策　3.その他のリスク対策		（追記） ＜ガバメントクラウドにおける措置＞ ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。 ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。 具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。	事前	令和7年度中に予防接種対象者台帳ファイルをガバメントクラウドでの保管に移行することに伴う重要な追加変更であり、事前にリスク対策の評価の再実施をするもの