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
15	浜松市　予防接種の実施等に関する事務　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

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

特記事項	

評価実施機関名

浜松市長

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5月　様式4］

項目一覧

Ⅰ　基本情報

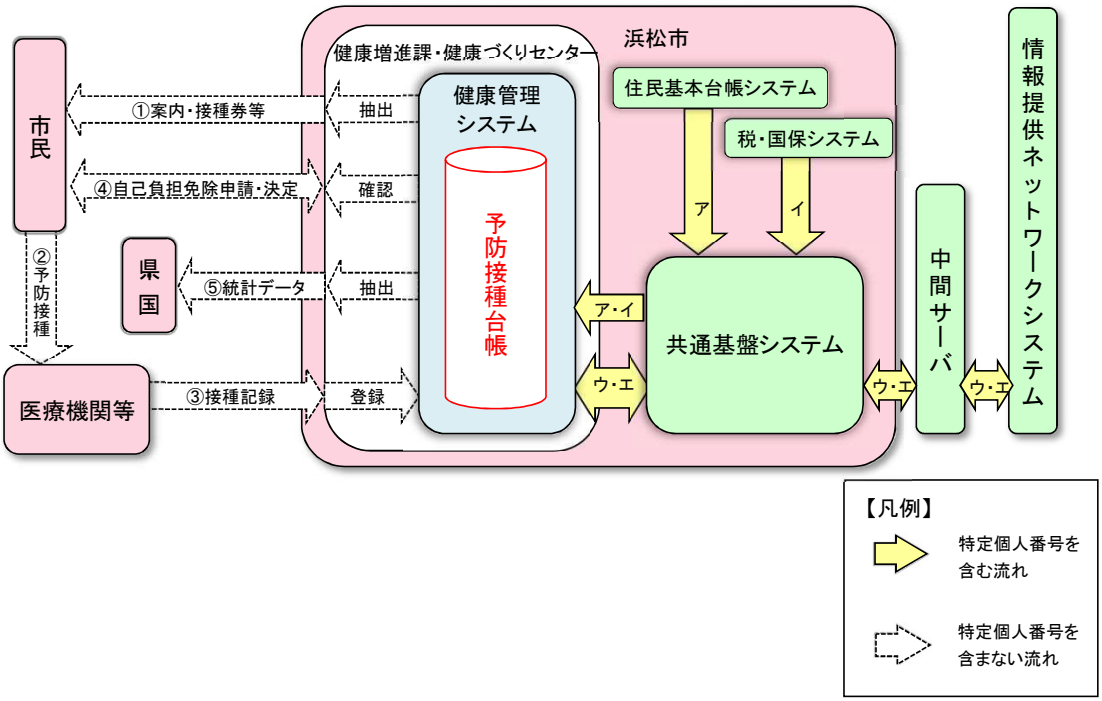
1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	予防接種の実施等に関する事務
②事務の内容　※	市町村は「予防接種法」、「新型インフルエンザ等対策特別措置法」及び「行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年5月31日法律第27号）」（以下「番号法」という。）の規定に従い、特定個人情報を予防接種等の以下の事務において取り扱う。 ①予防接種等の実施に関する事務 ②予防接種等健康被害救済の給付の支給に関する事務 ③予防接種等の自己負担の実費徴収に関する事務 ④予防接種等の記録の管理に関する事務 番号法において、情報保有機関は情報提供ネットワークシステムに接続し、各情報保有機関が保有する個人情報について情報連携を行うことが必要とされている。 健康管理システム（予防接種システム）と共通基盤システムの間でデータ（副本）の受け渡しを行い、共通基盤システムが中間サーバーを介して（※1）、情報提供ネットワークシステムと接続することで、符号の取得（※2）や各情報保有期間で保有する特定個人情報の照会と提供等を実現する。 ※1浜松市では、共通基盤システムが庁内連携・団体内統合宛名システムとしての機能を有し、一括して中間サーバーとの情報連携を行う。 ※2セキュリティの観点により、特定個人情報の照会と提供の際は「個人番号」を直接利用せず「符号」を取得して利用する。
③対象人数	[　30万人以上　] ＜選択肢＞ 1) 1,000人未満　2) 1,000人以上1万人未満 3) 1万人以上10万人未満　4) 10万人以上30万人未満 5) 30万人以上

2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	健康管理システム
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 予防接種照会：接種別や全接種の履歴を照会する。 4 予診票出力：転入者等の予診票を印刷する。 5 クラウド型バックアップセンターとの連携 地方公共団体情報システム機構（以下、「機構」という）のクラウド型バックアップセンターに対して、基本データリストを送付する。
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　（ クラウド型バックアップセンター　）
システム2～5	
システム2	
①システムの名称	共通基盤システム
②システムの機能	1　システム間連携機能 庁内業務システム間のデータ連携を統一して制御する機能。 2外字管理機能 外字を作成し、作成した外字データを各業務システムのサーバー・クライアントに提供する機能。 3　大量帳票印刷管理機能 庁内で印刷する大量帳票の印刷制御を行う機能。 4　共有データ管理機能 業務システム間で受け渡すデータ等を管理する機能。 5　認証管理機能 共通基盤システムへのログイン認証、各業務システムへのシングルサインオン、職員情報等のアカウントを管理する機能 6　団体内統合宛名管理機能 団体内統合宛名番号を管理する機能。 7　情報連携機能 他団体に提供する情報を、中間サーバーに連携する機能。 8　情報照会機能 業務システムからの要求に応じ、中間サーバーを介して、他団体への情報照会を行う機能。

③他のシステムとの接続	[　] 情報提供ネットワークシステム　[○] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[○] 既存住民基本台帳システム [　] 宛名システム等　[○] 税務システム [○] その他　（ 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　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、情報保有機関内での個人特定に利用する「統一識別番号」とを紐付け、その情報を保管・管理する。 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)の情報照会及び提供情報受領(照会した情報の受領)を行う。 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。 4　既存システム接続機能 　各業務システム・共通基盤システム(団体内統合宛名システム含む)と情報照会内容、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。 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際の情報提供等記録を生成・管理する。 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)の副本を保持・管理する。 7　データ送受信機能 　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。 8　セキュリティ管理機能 　暗号化／復号機能と、鍵情報及び照会許可用照合リスト情報を管理する。 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。 10　システム管理機能 　バッチ処理の状況管理、業務統計情報の集計、稼動状態の通知、保管期限切れ情報の削除を行う。
③他のシステムとの接続	[○] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [○] 宛名システム等　[　] 税務システム [　] その他　（　）
システム4	
①システムの名称	クラウド型バックアップセンター
②システムの機能	地方公共団体情報システム機構が提供するクラウドサービス(LGWAN-ASP)。 主な機能は次のとおり。 バックアップ機能 ・地方公共団体が保有する情報を特定のデータレイアウト(基本データリスト)でバックアップする機能
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [○] その他　（ 健康管理システム　）

システム5	
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	
予防接種関係情報ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	・予防接種の対象者及び接種履歴を正確に把握し、適正な管理を行うため。 ・対象者の所得状況を判断し、公平・公正な実費徴収を行うため。
②実現が期待されるメリット	・現行の予防接種の対象者であることの確認及び受けた予防接種の履歴を管理するシステム台帳管理に加え、番号制度と結びつけることにより、転入転出時等における効率的な事務が可能となる。・番号制度の導入により、情報提供ネットワークを通じて他市町村の地方税情報等を照会することが可能となり、実費徴収に関する面で、低所得者対策として講じている自己負担金免除の手続きが簡素化され、市民の負担軽減につながる。
5. 個人番号の利用　※	
法令上の根拠	①番号法第九条　番号表別表第十四の項　及び　番号法別表第百二十六の項 ②番号法別表の主務省令で定める事務を定める命令　第十条　及び　第六十七条の二 ③番号法第十九条　第六号（委託先への提供）
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[　　実施する　　]　　＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	（情報提供） 番号法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 第二条表　第二十五、二十六、百五十三の項 第二十七条、第二十八条、第百五十五条 （情報照会） 番号法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 第二条表　第二十五、二十六、二十七、二十八、二十九、百五十三の項 第二十七条、第二十八条、第二十九条、第三十条、第三十一条、第百五十五条
7. 評価実施機関における担当部署	
①部署	健康福祉部　健康増進課
②所属長の役職名	健康増進課長
8. 他の評価実施機関	
―	

（別添1）事務の内容



（備考）

ア・・・予防接種対象者を抽出するために必要な「住民情報」を取得
イ・・・実費徴収の有無を決定するために必要な「税情報」を取得
ウ・・・「他市町村からの転入者に関する予防接種歴情報」及び「税情報」を情報提供ネットワークシステム経由で取得
エ・・・「他市町村への転出者に関する予防接種歴情報」を情報提供ネットワークシステム経由で提供

①・・・予防接種の案内等を郵送等で通知。また、未接種者に対し、郵送等で接種勧奨
②・・・案内や勧奨を受けた予防接種について、医療機関等で接種
③・・・医療機関等で実施した予防接種の記録を取得し、健康管理システムに登録
④・・・自己負担金の免除申請を受け付け、実費徴収の有無を決定
⑤・・・静岡県及び国へ統計等の報告

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		
予防接種関係情報ファイル		
2. 基本情報		
①ファイルの種類 ※		[　　システム用ファイル　　] ＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　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 ※		・住民基本台帳法第5条に基づき本市住民基本台帳に記録された住民（以下、住民登録内の者） ・住民基本台帳に記録されていた者で転出等の事由により住民票が消除（死亡による消除を除く。）された者または本市住民基本台帳に未記録の者のうち本市の業務上必要な者（以下、住民登録外の者）のうち、本市で個人番号を把握した者。
	その必要性	予防接種事務を行うにあたり、予防接種を接種した本人を管理する必要がある。
④記録される項目		[　　100項目以上　　] ＜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 [○] 5情報（氏名、氏名の振り仮名、性別、生年月日、住所）　[○] 連絡先（電話番号等） [○] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[○] 地方税関係情報　[○] 健康・医療関係情報 [　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [○] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [　] その他　（　　）
	その妥当性	・個人番号及びその他識別情報：対象者を正確に特定するために保有 ・4情報、連絡先及びその他住民票関係情報：①予診票を発送する際、正確な住所、連絡先が必要なため。②年齢要件によって異なる予防接種の接種有無の判断のため。③本人への連絡等のため。④死亡転出等を把握し、発送物の送付有無を判断するため。 ・地方税関係情報及び生活保護・社会福祉関係情報：予防接種の実費に係る負担の有無を決定するために保有 ・健康・医療関係情報：予防接種履歴管理及び勧奨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		平成28年1月1日
⑥事務担当部署		健康福祉部　健康増進課

3. 特定個人情報の入手・使用		
①入手元 ※		[○] 本人又は本人の代理人 [○] 評価実施機関内の他部署 （ ） [ ] 行政機関・独立行政法人等 （ ） [○] 地方公共団体・地方独立行政法人 （ ） [ ] 民間事業者 （ ） [ ] 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		住民基本情報： （入手元）評価実施機関内の他部署 （入手頻度・時期）随時 （入手方法）庁内連携システム 税情報： （入手元）評価実施機関内の他部署 （入手頻度・時期）随時 （入手方法）庁内連携システム
④入手に係る妥当性		個人を特定し、適正に接種を管理する必要がある。
⑤本人への明示		・他機関、情報提供ネットワークシステム等を通じた入手・提供を行うことは番号法に明示されている。（番号法第九条・番号法第十九条） ・当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。
⑥使用目的 ※		予防接種記録の保管管理を行う。未接種者に対する接種勧奨を実施する。予防接種の実費徴収を適正に決定する。
	変更の妥当性	―
⑦使用の主体	使用部署 ※	健康増進課及び各区健康づくりセンター
	使用者数	[50人以上100人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
⑧使用方法 ※		・予防接種記録の保管管理：予防接種台帳システムに接種記録を登録し、接種記録の保管及び管理を行う。 ・接種勧奨：対象年齢・生年月日・性別の対象者情報を把握し、接種勧奨を行う。 ・生活保護受給者及び市民税非課税世帯の接種者に接種券を発行する。
	情報の突合 ※	医療機関等から提出された予防接種予診票内の予防接種情報をパンチデータから取り込み、システム内の情報と突合する。
	情報の統計分析 ※	特定の個人を特定するような統計や分析は行わない。
	権利利益に影響を与え得る決定 ※	該当なし。
⑨使用開始日		平成28年1月1日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] ＜選択肢＞ 1）委託する 2）委託しない （ 2 ） 件
委託事項1		健康管理システムの保守・運用
①委託内容		システム等のパッケージアプリケーション保守作業、ジョブスケジューリング等のシステム運用作業、職員からの問い合わせに対する調査、作業指示に基づくデータ抽出等、遠隔地保管情報の媒体作成、システム監視・通報等。
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」と同じ。
	その妥当性	健康管理システムを安全かつ安定して稼動させるために専門知識を有する民間事業者へ委託する。
③委託先における取扱者数		[10人以上50人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ]専用線 [ ]電子メール [ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ [ ]紙 [○]その他 （ システム保守作業において、特定個人情報ファイルの提供は行わない。 ）
⑤委託先名の確認方法		浜松市情報公開条例により公文書の公開請求を行うことにより確認することができる。
⑥委託先名		日本コンピューター株式会社
再委託	⑦再委託の有無 ※	[再委託する] ＜選択肢＞ 1）再委託する 2）再委託しない
	⑧再委託の許諾方法	契約書に基づき、業務委託一部再委託届を提出し、委託者の許可を受ける。
	⑨再委託事項	システムの保守作業、それに付随する付帯作業及び運用支援作業
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 （ 2 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	都道府県知事又は市町村長
①法令上の根拠	番号法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 第二条表 第二十五の項
②提供先における用途	予防接種法による予防接種の実施に関する事務であって主務省令で定めるもの
③提供する情報	予防接種履歴
④提供する情報の対象となる本人の数	[1万人未満] <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	他市町村への転出者のうち定期予防接種の接種履歴があるもの
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	随時
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 ※		＜浜松市における措置＞ ・入室許可権限を設定したICカードにより入室管理を行っているフロアの、更にICカードで入室管理を行っているサーバ室内のサーバ内に保管している。 ・サーバへのアクセス制御機能としては、ユーザIDによる識別とパスワードによる認証（ログイン）、さらに認証したユーザに対する認可機能（処理権限の付与）があるため、そのユーザがシステム上で利用できる範囲を制限している。また、ログインしたユーザのログ監査（操作記録の監査）を行っている。 ＜ガバメントクラウドにおける措置＞ ①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。 ②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。 ＜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政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。 なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018の認証を受けている。 ・日本国内でデータを保管している。 ・特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する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。 ＜クラウド型バックアップセンターにおける措置＞ ・クラウド型バックアップセンターは、地方公共団体情報システム機構が選定したクラウドサービス上に構築する。クラウドサービスは、ISO/IEC 27017:2015によるクラウドサービス分野におけるISMS（（情報セキュリティ管理システム））認証の国際規格の外部認証を取得したサービスを選定している。クラウドサービスと接続するネットワークにIP-VPN網（通信事業者の閉域網内のVPNサービス）の利用に加え、通信の暗号化及びクラウドサービス上に保存する際に暗号化を実施。
②保管期間	期間	［　　5年　　］ ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	予防接種法施行令第6条の2において、5年間保存しなければならないと規定されている。
③消去方法		＜浜松市における措置＞ ・予防接種法施行令第6条の2には、保管期間を過ぎた場合に削除する規定は記載されていない。宛名連携をしている他課で必要なためにデータは消去していない。 ・庁内に設置するサーバ等のディスク交換やハードウェア更改等の際は、特定個人情報を保存するシステムのハードウェア事業者が、ディスク等に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、消去証明書を提出させる。 ・庁外のデータセンターに設置するサーバ等のディスク交換やハードウェア更改等の際はISO/IEC27001に準拠した手順（ データを復元できないよう電子的完全消去または廃棄する。）でデータ消去、破棄が適切に実施されていることを、第三者の監査機関による監査結果等必要な資料を提出させ確認する。 ＜ガバメントクラウドにおける措置＞ 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。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。 ②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。 ③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壊等を実施する。

	＜中間サーバー・プラットフォームにおける措置＞ ・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。 ・クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度(ISMAP)に準拠したデータの暗号化消去及び物理的破壊を行う。 さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ・中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。
7. 備考	

（別添2）特定個人情報ファイル記録項目

整理番号,カナ氏名,カナ氏名略,漢字氏名,生年月日,性別,町番号,行政区番号,番地,枝番,小枝,郵便番号,集配局,住所,方書,小学校区,中学校区,続柄1,続柄2,続柄3,続柄4,世帯番号,世帯主カナ氏名,世帯主漢字氏名,取消区分,住登外区分,宛名種別,外国人フラグ,外国人国籍,住民となった日,住民でなくなった日,最新異動区分,最新異動日,最新異動届出日,住民異動区分,住民異動日,転入前住所,転入前方書,転出後住所,転出後方書,電話番号,FAX番号,携帯番号,メールアドレス,補記論理和,送付除外論理和,個人課税区分,世帯課税区分,被災者区分,DV区分,国保区分,徴収区分,課税区分,年金区分,生保区分,介護区分,後期高齢区分,接種名称区分,期回数区分,履歴番号,年度,事業予定連番,接種日,実施時間,会場区分,会場区分その他,接種種別区分,登録日,負担金区分,接種医療機関番号,接種医療機関番号その他,接種区分,Lot番号,接種量,印刷区分,印刷日,発送日,予診理由区分,接種補足区分,予診票再発行フラグ,予診票再発行枚数,予診票再発行日,依頼書印刷区分,依頼書印刷日,証明書印刷区分,証明書印刷日,予診医医療機関番号,予診医医療機関番号その他,予診医番号,予診医職員番号,予診医職員枝番,接種医番号,接種医職員番号,接種医職員枝番,ワクチンメーカー区分,ワクチン名区分,備考,支払対象外フラグ,予診番号,警告内容,登録支所区分,抽出日,抽出時郵便番号,抽出時住所,抽出時方書,抽出時行政区番号,抽出時漢字氏名,抽出時カナ氏名,抽出時補記論理和,抽出時生保区分,抽出キー,抽出フラグ,印刷連番,抽出時居住区,予診票番号,予診票無効フラグ,依頼書発行元,依頼書受付日,依頼番号,実施報告書印刷日,請求年月,経過措置,予診票発行部署,送付先名,起案番号,発行日,保護者カナ氏名,保護者氏名,保護者電話番号,続柄,滞在先郵便番号,滞在先住所,滞在先方書,依頼書発行理由,依頼書発行理由その他,担当者名

Ⅲ　特定個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	＜運用における措置＞ 予防接種を受付する委託医療機関において、本人確認書類（身分証明証等）の確認を実施し、対象者以外の情報を入手することはない。 ・委託医療機関から提出された予診票をシステムへ取込む際に、予診票に記載された個人コード、氏名、住所、生年月日等とマッチングを行い、適切な情報のみをシステムへ取込む。 ＜システムにおける措置＞ ・ユーザIDによる識別とパスワードによる認証、利用可能機能の権限設定及び制限により、権限が無い者による目的外の入手を防止している。 ・庁内連携による入手の場合は、共通基盤システムの連携機能により、許可外のシステムには連携されない仕組みとなっている。
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	＜運用における措置＞ ・予防接種業務に必要な情報以外は入力できないよう、システム上担保されている。 ・申請書類については、必要な情報以外を誤って記載することがないよう、様式を定める。
その他の措置の内容	－
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク2：　不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	＜システムにおける措置＞ ・ユーザIDによる識別とパスワードによる認証、利用可能機能の権限設定及び制限により、権限が無い者による目的外の入手を防止している。 ・庁内連携による入手の場合は、共通基盤システムの連携機能により、許可外のシステムには連携されない仕組みとなっている。
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
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	・個人番号カード（番号法17条）の提示を受け、本人確認を行う。 ・通知カード（同第7条）と官公庁発行の写真入身分証明書の提示を受け、本人確認を行う。 ・通知カードと官公庁発行の写真なし資格証(保険証など)の提示を求め、住基情報等の聞き取りを行い、本人確認を行う。
個人番号の真正性確認の措置の内容	・窓口で個人番号カード又は通知カードと他の証明書類の提示を求め、照合する。 ・システム内の番号検索機能を使用して本人確認情報を検索し、個人番号の真正性確認を行う。
特定個人情報の正確性確保の措置の内容	・入手した情報については、窓口での聞き取りや添付書類との照合等を通じて確認することで正確性を確保している。 ・職員にて収集した情報に基づいて、間違いがあれば職権で適宜修正することで正確性を確保している。 ・庁内連携による入手の場合は、共通基盤システムの連携機能で、情報移転元の業務システムと、共通基盤システム、情報移転先の業務システムで同期を取り、情報の順序性・正当性・正確性を確保している。
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	・予防接種システムは基幹系システム用の専用ネットワーク回線を利用することにより情報リスクを低減させている。 ・提出された予診票については、提出後、全件確認し、保管については、施錠された部屋へ保管している。

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	・団体内統合宛名管理機能を有する共通基盤システムでは、業務システムごとに連携する情報を制限し、必要のない情報との紐付けを防止している。 ・特定個人情報の利用・提供は、「浜松市電子計算機組織の運営及びデータの保護に関する規定」に基づき、必要事項のみ利用・提供を行なっている。	
事務で使用するその他のシステムにおける措置の内容	・番号法で定められた業務システム以外には、連携しないこととしている。 ・各業務を行うにあたり、利用者の担当業務ごとにアクセス権限区分を設け、権限に応じて不必要な情報にはアクセスできないよう制御を行っている。	
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	・業務システムへのアクセスを、共通基盤システムの認証管理機能によりシングルサインオンで実施し、ユーザごとのシステム利用権限をシステム管理部署が一元管理している。 ＜共通基盤システムにおける措置＞ ・職員個人単位でユーザIDを発効している。 ・ユーザIDによる識別とパスワードによる認証により、不正な業務システム使用を防止している。 ・認証に使用するパスワードは、定期的に変更を行っている。 ＜業務システムにおける措置＞ ・特定個人情報の表示の有無を、権限にて限定している。	
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	＜運用における措置＞ ・業務システムへのアクセスを、共通基盤システムの認証管理機能によりシングルサインオンで実施し、ユーザごとのシステム利用権限を発効・失効管理をシステム管理部署が一元管理している。 ＜共通基盤システムにおける措置＞ ・人事異動等により権限変更が必要な場合は、システム管理部署にて、異動当日の業務開始直前に権限の発効及び失効を行う。	
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	・業務システムへのアクセスを、共通基盤システムの認証管理機能によりシングルサインオンで実施し、ユーザごとのシステム利用権限はシステム管理部署が一元管理している。 ・システム管理部署は、定期的に部署及び個人ごとの利用権限設定の見直しを行う。
特定個人情報の使用の記録		[　　記録を残している　　] ＜選択肢＞ 1）記録を残している　　2）記録を残していない
	具体的な方法	・特定個人情報へのアクセスログ（使用日時、使用者、使用情報等）を記録している。
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		・ユーザIDによる識別とパスワードによる認証、利用可能な機能の権限設定及び制限により、不必要な情報へのアクセスを防止している。 また、全職員を対象に情報セキュリティに関する研修を年１回実施している。
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		予防接種システムの利用に際して、IDとパスワードが必要であり、外部の者に操作権限を与えていない。 データ抽出においてはいかなる処理であってもマイナンバーを出力しない。
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置		
－		

4. 特定個人情報ファイルの取扱いの委託		[　　] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認	・業務委託契約書において、個人情報を取扱う従業者の明確化を義務付けている。 ・プロジェクト計画書において、情報保護管理体制の確認を実施している。	
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	・業務委託契約書にて、特定個人情報を取扱う従業者を必要最低限にするよう義務付けている。 ・ユーザIDによる識別とパスワードによる認証、利用可能な機能の制限等により、許可された従業者以外の利用を制限している。	
特定個人情報ファイルの取扱いの記録	[　記録を残している　]	＜選択肢＞ 1）記録を残している　2）記録を残していない
具体的な方法	・特定個人情報へのアクセスログ（使用日時、使用者、使用情報等）を記録している。	
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	・業務委託契約書にて、特定個人情報の第三者への提供を禁止している。 ・特定個人情報の管理状況検査を、必要に応じて実施する。	
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	・業務委託契約書にて、委託者の承諾がない特定個人情報の複製・複写又は持出しを禁止している。 ・特定個人情報の管理状況検査を、必要に応じて実施する。	
特定個人情報の消去ルール	[　定めている　]	＜選択肢＞ 1）定めている　2）定めていない
ルールの内容及びルール遵守の確認方法	・業務委託契約書にて、業務完了後に業務処理上で保有した特定個人情報を全て処分させ、その処分内容の書面報告を義務付けている。 ・ハードウェア調達契約書にて、特定個人情報を記録したハードウェア等をリース返却又は処分する際、情報の読み出しができないよう、物理的破壊又は専用ソフト等による完全消去を実施させた上で、データ消去証明書の提出を義務付けている。 ・庁外のデータセンターに設置するサーバ等のディスク交換やハードウェア更改等の際はISO/IEC27001に準拠した手順（ データを復元できないよう電子的完全消去または廃棄する。）でデータ消去、破棄が適切に実施されていることを、第三者の監査機関による監査結果等必要な資料を提出させ確認する。	
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	業務委託契約書に下記事項を記載して締結することを義務付けている。 ・一括再委託の禁止、一部再委託する場合の申請・許諾の手続きに関する事項 ・業務処理状況の調査権、報告義務に関する事項 ・秘密保持義務に関する事項 ・番号法関係法令、浜松市個人情報保護条例等の法律遵守に関する事項 ・特定個人情報を取り扱う従業員の明確化及び従業員に対する指導に関する事項 ・特定個人情報の目的外利用・複製・複写又は持出しの禁止に関する事項 ・特定個人情報の適正な管理に関する事項 ・特定個人情報の処分に関する事項 ・契約解除時の遵守事項に関する事項	
再委託先による特定個人情報ファイルの適切な取扱いの確保	[　十分に行っている　]	＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない

	具体的な方法	・業務委託契約書にて、一括再委託を禁止している。 ・一部再委託する場合は、再委託先名称・再委託理由・再委託者の処理内容・再委託先が取り扱う情報、再委託先での情報取り扱い上の安全性及び信頼性確保対策・再委託先に対する管理及び監督方法を、受託者に申請させ、内容を確認し許諾している。
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
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
―		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[　　] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[　　記録を残している　　]	＜選択肢＞ 1）記録を残している　　2）記録を残していない
具体的な方法	・特定個人情報ファイルの提供・移転のシステムログ（提供及び移転先・日時等）を記録している。	
特定個人情報の提供・移転に関するルール	[　　定めている　　]	＜選択肢＞ 1）定めている　　2）定めていない
ルールの内容及びルール遵守の確認方法	・他の業務所管課より、保有情報の移転・提供を求められた場合は、書面による事前申請を受け、提供・移転の必要性及び内容等の審査を行い、承認したもののみ情報の移転・提供を行う。 ・特定個人情報ファイルの提供・移転は、システムログ（提供及び移転先・日時等）を記録し、必要に応じて確認を行う。	
その他の措置の内容	－	
リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容	＜システムにおける措置＞ ・庁内連携による他業務システムとの連携は、共通基盤システムの連携機能による連携先の限定に加え、ファイアウォール等の通信制御により、不適切な提供・移転が発生しない仕組みとなっている。	
リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
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	・提供・移転情報のチェックにより、誤った情報の作成を防止している。 ・庁内連携による他業務システムとの連携は、共通基盤システムの連携機能による連携先の限定に加え、ファイアウォール等の通信制御により、誤った相手への提供・移転がされない仕組みとなっている。 ・共通基盤システムの連携機能で、情報移転元の業務システムと、共通基盤システム、情報移転先の業務システムで同期を取り、情報の順序性・正当性・正確性を確保している。	
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
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	＜業務システムにおける措置＞ ・特定個人情報ファイルの送受信は、共通基盤システムのみに限定している。 ・ユーザIDによる識別と、共通基盤システムを経由した情報提供ネットワークシステムへの情報照会の権限設定及び制限により、権限が無い者の目的外入手を防止する。 ＜共通基盤システムにおける措置＞ ・共通基盤システムの連携機能による連携先の限定に加え、ファイアウォール等の通信制御により、不適切な方法による入手が不可能な仕組みとなっている。 ・中間サーバーへの情報照会は、共通基盤システムにて照会できる業務システムを限定している。 ・ログイン時の職員認証に加え、ログイン・ログアウトした職員・時刻・操作内容を記録し、不適切な端末操作や照会等を抑止する仕組みとなっている。 ＜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。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、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加え、ログイン・ログアウトした職員・時刻・操作内容を記録し、不適切な端末操作や照会等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情報の受領を行う機能。 （※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。 （※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	＜業務システムにおける措置＞ ・ユーザIDによる識別と、情報提供ネットワークシステムへの情報照会の権限設定及び制限により、権限の無い者の不適切な方法による入手を防止している。 ・特定個人情報ファイルの送受信は、共通基盤システムのみに限定している。 ＜共通基盤システムにおける措置＞ ・共通基盤システムの連携機能による連携先の限定に加え、ファイアウォール等の通信制御により、不適切な方法による入手ができない仕組みとしている。 ・中間サーバへの情報照会は、共通基盤システムにて照会できる業務システムを限定している。 ＜中間サーバ・ソフトウェアにおける措置＞ ・中間サーバは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 ＜中間サーバ・プラットフォームにおける措置＞ ・中間サーバと共通基盤システム、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）を利用することで、安全性を確保している。 ・中間サーバと市町村以外の団体は、VPN等の技術を利用し、団体ごとの通信回線分離と通信の暗号化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	＜業務システムにおける措置＞ ・共通基盤システムと情報照会元業務システム間で同期を取り、情報の順序性・正当性・正確性等を担保する仕組みとなっている。 ＜共通基盤システムにおける措置＞ ・情報照会機能で中間サーバに情報照会を行う際には、共通基盤システムは照会結果情報の改変を行わない仕組みとし、中間サーバの情報と同一であることを担保している。 ＜中間サーバ・ソフトウェアにおける措置＞ ・中間サーバは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	＜業務システムにおける措置＞ ・ユーザIDによる識別と、情報提供ネットワークシステムへの情報照会の権限設定及び制限により、権限の無い者の照会及び入手を防止している。 ・特定個人情報ファイルの送受信は、共通基盤システムのみに限定している。 ＜共通基盤システムにおける措置＞ ・共通基盤システムの連携機能による連携先の限定に加え、ファイアウォール等による通信制御により、不正なアクセスによる情報漏えいを防止している。 ・中間サーバへの情報照会は、共通基盤システムにて照会できる業務システムを限定している。 ・ログイン時の職員認証に加え、ログイン及び業務システムを起動した職員・時刻・操作内容を記録し、不適切な端末操作や照会等を抑止する仕組みになっている。 ＜中間サーバ・ソフトウェアにおける措置＞ ・中間サーバは、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ・中間サーバへ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は、一定期間経過後に当該結果を情報照会機能にて自動で削除することで、特定個人情報が漏えい・紛失するリスクを軽減している。 ・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトした職員・時刻・操作内容を記録し、不適切な端末操作や照会等を抑止する仕組みになっている。 （※）中間サーバは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバ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＞ ・中間サーバーと共通基盤システム及び情報提供ネットワークシステム間は、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）を利用することで、漏えい・紛失のリスクに対応している。 ・中間サーバーと市町村以外の団体は、VPN等の技術を利用し、団体ごとの通信回線分離と、通信の暗号化で漏えい・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、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはない。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク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	＜業務システムにおける措置＞ ・特定個人情報ファイルの送受信は、共通基盤システムのみに限定している。 ・ユーザIDによる識別と、共通基盤システムを経由した情報提供ネットワークシステムへの情報提供の権限設定及び制限により、不正な提供を防止している。 ・特定個人情報ファイルの登録は、システムログ（登録者・登録日時・登録内容）を記録し、必要に応じ確認を行う。 ＜共通基盤システムにおける措置＞ ・中間サーバーとの連携通信は、行政専用のネットワーク（統合行政ネットワーク等）のみに限定している。 ・特定個人情報ファイルの登録は、システムログ（登録者・登録日時・登録内容）を記録し、必要に応じて確認を行う。 ・ログイン時の職員認証に加え、ログイン及び業務システムの起動を実施した職員・時刻・操作内容を記録し、不適切な端末操作や照会等を抑止する仕組みになっている。 ＜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から照会許可用照合リストを中間サーバーに入手・格納し、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。 ・特に慎重な対応が求められる情報は、自動応答不可フラグを設定し、特定個人情報提供の際に、送信内容を改めて確認して提供することで、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・操作内容を記録し、不適切な端末操作や照会等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	＜業務システムにおける措置＞ ・ユーザIDによる識別と、情報提供ネットワークシステムへの情報照会の権限設定及び制限により、不正な使用を防止している。 ・特定個人情報ファイルの登録は、システムログ（登録者・登録日時・登録内容）を記録し、必要に応じて確認を行う。 ・特定個人情報ファイルの送受信は、共通基盤システムのみに限定している。 ＜共通基盤システムにおける措置＞ ・中間サーバとの連携通信は、行政専用のネットワーク（統合行政ネットワーク等）のみに限定している。 ・特定個人情報ファイルの登録は、システムログ（登録者・登録日時・登録内容）を記録し、必要に応じて確認を行う。 ・ログイン時の職員認証に加え、ログイン及び業務システムの起動を実施した職員・時刻・操作内容を記録し、不適切な端末操作や照会等を抑止する仕組みになっている。 ＜中間サーバ・ソフトウェアにおける措置＞ ・セキュリティ管理機能（※）により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証に加え、ログイン・ログアウトした職員・時刻・操作内容を記録し、不適切な端末操作や照会等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＞ ・中間サーバーと共通基盤システム及び情報提供ネットワークシステム間は、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）を利用することで、不適切な方法で提供されるリスクに対応している。 ・中間サーバーと市町村以外の団体は、VPN等の技術を利用し、団体ごとの通信回線分離と、通信の暗号化で漏えい･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・運用を行う事業者及びクラウドサービス事業者においては、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	＜業務システムにおける措置＞ ・特定個人情報ファイルの送受信は、共通基盤システムのみに限定する。 ＜共通基盤システムにおける措置＞ ・中間サーバへの情報提供は、共通基盤システムにて提供できる業務システムを限定している。 ・団体内連携テスト・情報提供ネットワークシステムとの連携テスト・総合運用テスト等の検証工程で、特定個人情報の正確性を十分に検証し、中間サーバに誤情報を提供した場合のリカバリ手順等を明確にする。 ＜中間サーバ・ソフトウェアにおける措置＞ ・情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領し、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データを共通基盤システムのデータベース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	
＜浜松市における措置＞ 本市では、情報提供ネットワークシステムとの連携接続は、全て中間サーバーが行う構成とし、情報提供ネットワークシステムから、直接、本市の業務システムへのアクセスはできない。 ＜中間サーバー・ソフトウェアにおける措置＞ ・中間サーバーの職員認証・権限管理機能は、ログイン時の職員認証に加え、ログイン・ログアウトした職員・時刻・操作内容を記録し、不適切な端末操作や照会等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＞ ・中間サーバーと共通基盤システム及び情報提供ネットワークシステム間は、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）を利用することで、安全性を確保している。 ・中間サーバーと市町村以外の団体は、VPN等の技術を利用し、団体ごとの通信回線分離と、通信の暗号化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）され、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よ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	＜浜松市における措置＞ ・情報を保管するサーバ室及びサーバ室が設けられたフロアの出入口にて、ICカードにより入室管理を行なっている。また、その入退室履歴を保存して入室者を特定している。 ・建物内の機械警備システム及び警備員の巡回により、安全管理を行っている。 ＜ガバメントクラウドにおける措置＞ ①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、システムのンサーバー等は、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。 ＜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、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。 なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018の認証を受けている。 ・日本国内でデータを保管している。	
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	＜浜松市における措置＞ ・ウィルス対策ソフトの定期的パターン更新を行っている。 ・特定個人情報を管理しているサーバは、インターネットに接続していない隔離されたネットワーク上に設置している。 ＜ガバメントクラウドにおける措置＞ ①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等となっている。 ②地方公共団体が委託したASP(「地方公共団体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】(案)」(令和４年８月　デジタル庁。以下「利用基準」という。)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。 ③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。 ④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。 ⑤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。 ⑥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。 ⑦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。 ⑧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。 ＜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・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。 ・中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。	

		・中間サーバーのデータベースに保存される特定個人情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ・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・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。
⑦バックアップ		[　十分に行っている　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知		[　十分に行っている　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか		[　発生あり　] ＜選択肢＞ 1）発生あり　2）発生なし
	その内容	・令和6年度 パソコンで特定の操作を加えると個人情報が表示されてしまう状態のまま、エクセルファイルを市ホームページに掲載したため、個人情報が閲覧可能な状態となっていた。(1,015人分) ・令和7年度 イベントのWEB申し込みについて、イベント受託者が民間サービスの申し込みフォームをりようしたところ、申し込み完了者が申し込みフォーム内において既に申し込みした者の個人情報が閲覧可能な設定となっていた(103人分)。
	再発防止策の内容	・令和6年度 (1)市ホームページへ掲載するファイルをエクセルファイルからPDFファイルに変更 (2)市ホームページで公開中のファイルを全件点検 (3) 市ホームページの添付ファイルに関する全庁への注意喚起 ・令和7年度 (1)申し込みフォームを準備した受託者に厳重注意と再発防止について指示を実施 (2)当該申し込みフォーム作成ツールを利用する際に同じミスが起こらないように、当該設定を全庁に周知し、注意喚起
⑩死者の個人番号		[　保管している　] ＜選択肢＞ 1）保管している　2）保管していない
	具体的な保管方法	死者の特定個人情報は、生存する特定個人情報と分けて管理しないため、生存する個人の特定個人情報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		住民基本台帳システムより随時異動データを連携することにより、最新化する、また住民記録システムとの整合処理を定期的に実施する。
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	保管期間の経過した特定個人情報を一括して削除する仕組みとなっている住民基本台帳システムと随時データを連携することにより、最新化する、また住民記録システムとの整合処理を定期的に実施する。 ＜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	＜浜松市における措置＞ ・年に1回担当部署内で、運用状況が評価書の記載内容通りかどうかを自己点検する。 ＜中間サーバー・プラットフォームにおける措置＞ ・運用規則等に基づき、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。	
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	＜浜松市における措置＞ ・情報セキュリティに関する内部監査を定期的に行う。 ＜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。 ＜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。 ・政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者は、定期的にISMAP監査期間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	＜浜松市における措置＞ 特定個人情報の適正な取扱いに関するガイドラインに基づき、人的セキュリティ研修を定期的に実施することに加え、意識教育や情報漏えいに伴う罰則規定を含む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。	
3. その他のリスク対策		
＜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。 ＜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、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。		

Ⅴ　開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	〒430-8652　浜松市中区元城町103番地の2 浜松市総務部文書行政課 053-457-2093
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	―
③手数料等	[　　無料　　]　＜選択肢＞ 1) 有料　2) 無料 （手数料額、納付方法：　　）
④個人情報ファイル簿の公表	[　　行っている　　]　＜選択肢＞ 1) 行っている　2) 行っていない
個人情報ファイル名	予防接種台帳
公表場所	浜松市市政情報室
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	〒430-8652　浜松市中央区鴨江二丁目11番2号 浜松市　健康福祉部　健康増進課 053-453-6119
②対応方法	問い合わせの受付時及びその対応について、記録を残す。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	令和2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	浜松市特定個人情報保護評価実施要綱に従って意見募集を実施。浜松市ホームページで評価書を公表するとともに、健康福祉部健康増進課、各区役所(区振興課)、協働センター、市政情報室、中央図書館にて閲覧を行う。
②実施日・期間	令和4年7月15日(金)～令和4年8月15日(月)　32日間
③期間を短縮する特段の理由	―
④主な意見の内容	提出された意見はなかった。
⑤評価書への反映	―
3. 第三者点検	
①実施日	令和4年8月23日（火）
②方法	浜松市情報公開・個人情報保護委員会による点検
③結果	評価書の内容について、問題なしとして了承された。
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
	Ⅰ-1 ①事務の内容	（略） 保健総合管理システム（予防接種システム）と共通基盤システムの間でデータ（副本）の受け渡しを行い、共通基盤システムが中間サーバーを介して（※1）、情報提供ネットワークシステムと接続することで、符号の取得（※2）や各情報保有期間で保有する特定個人情報の照会と提供等を実現する。 （略）	（略） 健康管理システム（予防接種システム）と共通基盤システムの間でデータ（副本）の受け渡しを行い、共通基盤システムが中間サーバーを介して（※1）、情報提供ネットワークシステムと接続することで、符号の取得（※2）や各情報保有期間で保有する特定個人情報の照会と提供等を実現する。 （略）		名称の変更
	Ⅰ-2 システム1 ②システムの名称	保健総合管理システム	健康管理システム		名称の変更
	Ⅰ-2 システム1 ②システムの機能	（略） 4 予診票出力：転入者等の予診票を印刷する。	（略） 4 予診票出力：転入者等の予診票を印刷する。 5 クラウド型バックアップセンターとの連携 　地方公共団体情報システム機構（以下、「機構」という）のクラウド型バックアップセンターに対して、基本データリストを送付する。		重要な変更（庁内データ分析基盤に予防接種関係情報ファイルを格納することによる変更）
	Ⅰ-2 システム1 ③他のシステムとの接続	（略） [　]その他（　）	（略） [○]その他（クラウド型バックアップセンター）		重要な変更（庁内データ分析基盤に予防接種関係情報ファイルを格納することによる変更）
	Ⅰ-2 システム4	無	①システムの名称 クラウド型バックアップセンター ②システムの機能 地方公共団体情報システム機構が提供するクラウドサービス（LGWAN-ASP）。 主な機能は次のとおり。 バックアップ機能 ・地方公共団体が保有する情報を特定のデータレイアウト（基本データリスト）でバックアップする機能 ③他のシステムとの接続 [○]その他（健康管理システム）		重要な変更（庁内データ分析基盤に予防接種関係情報ファイルを格納することによる変更）
	（別添1）事務内容	保健総合管理システム	健康管理システム		名称の変更
	Ⅱ-4 ①保管場所 委託事項1	保健総合管理システム	健康管理システム		名称の変更
	Ⅱ-4 ①保管場所 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 その他妥当性	保健総合管理システムを安全かつ安定して稼動させるために専門知識を有する民間事業者へ委託する。	健康管理システムを安全かつ安定して稼動させるために専門知識を有する民間事業者へ委託する。		名称の変更
	Ⅱ-6 ①保管場所	＜浜松市における措置＞ 略 ＜中間サーバー・プラットフォームにおける措置＞ 略	＜浜松市における措置＞ 略 ＜ガバメントクラウドにおける措置＞ ①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。 ②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。 ＜中間サーバー・プラットフォームにおける措置＞ 略 ＜クラウド型バックアップセンターにおける措置＞ ・クラウド型バックアップセンターは、地方公共団体情報システム機構が選定したクラウドサービス上に構築する。クラウドサービスは、ISO/IEC 27017:2015によるクラウドサービス分野におけるISMS（（情報セキュリティ管理システム））認証の国際規格の外部認証を取得したサービスを選定している。クラウドサービスと接続するネットワークにIP-VPN網（通信事業者の閉域網内のVPNサービス）の利用に加え、通信の暗号化及びクラウドサービス上に保存する際に暗号化を実施。	事前	重要な変更（ガバメントクラウド移行・庁内データ分析基盤に予防接種関係情報ファイルを格納することによる変更）

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅱ-6 ③消去方法	＜浜松市における措置＞ 略 ＜中間サーバー・プラットフォームにおける措置＞ 略	＜浜松市における措置＞ 略 ＜ガバメントクラウドにおける措置＞ 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。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。 ②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。 ③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壊等を実施する。 ＜中間サーバー・プラットフォームにおける措置＞ 略	事前	重要な変更(ガバメントクラウド移行による変更)
	Ⅲ-7 リスク1 ⑤物理的対策 具体的な対策の内容	＜浜松市における措置＞ 略 ＜中間サーバー･プラットフォームにおける措置＞ 略	＜浜松市における措置＞ 略 ＜ガバメントクラウドにおける措置＞ ①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、システムのンサーバー等は、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	重要な変更(ガバメントクラウド移行による変更)
	Ⅲ-7 リスク1 ⑥技術的対策 具体的な対策の内容	＜浜松市における措置＞ 略 ＜中間サーバー･プラットフォームにおける措置＞ 略	＜浜松市における措置＞ 略 ＜ガバメントクラウドにおける措置＞ ①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等となっている。 ②地方公共団体が委託したASP(「地方公共団体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】(案)」(令和4年8月　デジタル庁。以下「利用基準」という。)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。 ③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。 ④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。 ⑤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。 ⑥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。 ⑦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。 ⑧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。 ＜中間サーバー･プラットフォームにおける措置＞ 略	事前	重要な変更(ガバメントクラウド移行による変更)
	Ⅲ-7 リスク3 消去手順 手順の内容	保管期間の経過した特定個人情報を一括して削除する仕組みとなっている住民基本台帳システムと随時データを連携することにより、最新化する、また住民記録システムとの整合処理を定期的に実施する。	保管期間の経過した特定個人情報を一括して削除する仕組みとなっている住民基本台帳システムと随時データを連携することにより、最新化する、また住民記録システムとの整合処理を定期的に実施する。 ＜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。	事前	重要な変更(ガバメントクラウド移行による変更)
	Ⅳ-1 ②監査 具体的な内容	＜浜松市における措置＞ 略 ＜中間サーバー･プラットフォームにおける措置＞ 略	＜浜松市における措置＞ 略 ＜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。 ＜中間サーバー･プラットフォームにおける措置＞ 略	事前	重要な変更(ガバメントクラウド移行による変更)

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅳ-3	＜中間サーバー・プラットフォームにおける措置＞ 略	＜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。 ＜中間サーバー・プラットフォームにおける措置＞ 略	事前	重要な変更(ガバメントクラウド移行による変更)