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
6	法定予防接種実施事務　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

広島市は、予防接種法に基づく法定予防接種実施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

広島市長

個人情報保護委員会　承認日 【行政機関等のみ】

公表日

令和8年3月24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	法定予防接種実施事務
②事務の内容　※	予防接種法に基づく予防接種（以下「法定予防接種」という。）については、予防接種法第5条第1項の規定により、市町村長が住民に対して行わなければならない。 また、市町村長は、予防接種法第5条第1項の規定による予防接種であってA類疾病に係るもの又は第6条第1項若しくは第3項の規定による予防接種の対象者に対して、接種を勧奨しなければならない。 広島市は、「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「番号利用法」という。）の規定に従い、以下の予防接種の実施等に係る事務において特定個人情報を取り扱う。 ①法定予防接種（インフルエンザ・新型コロナウイルス感染症の定期の予防接種を除く）の接種履歴の登録 ②法定予防接種（A類疾病）対象者への接種勧奨通知 ③法定予防接種（A類疾病）対象者のうち、未接種者への再勧奨通知 ④本市に在住歴のある者に係る接種履歴の他自治体への提供 ⑤本市への転入者に係る他自治体における接種履歴の入手 ⑥被接種者本人から申請があった場合における接種履歴の提供 ⑦新型コロナウイルス感染症に係る特例臨時接種の接種履歴の登録
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

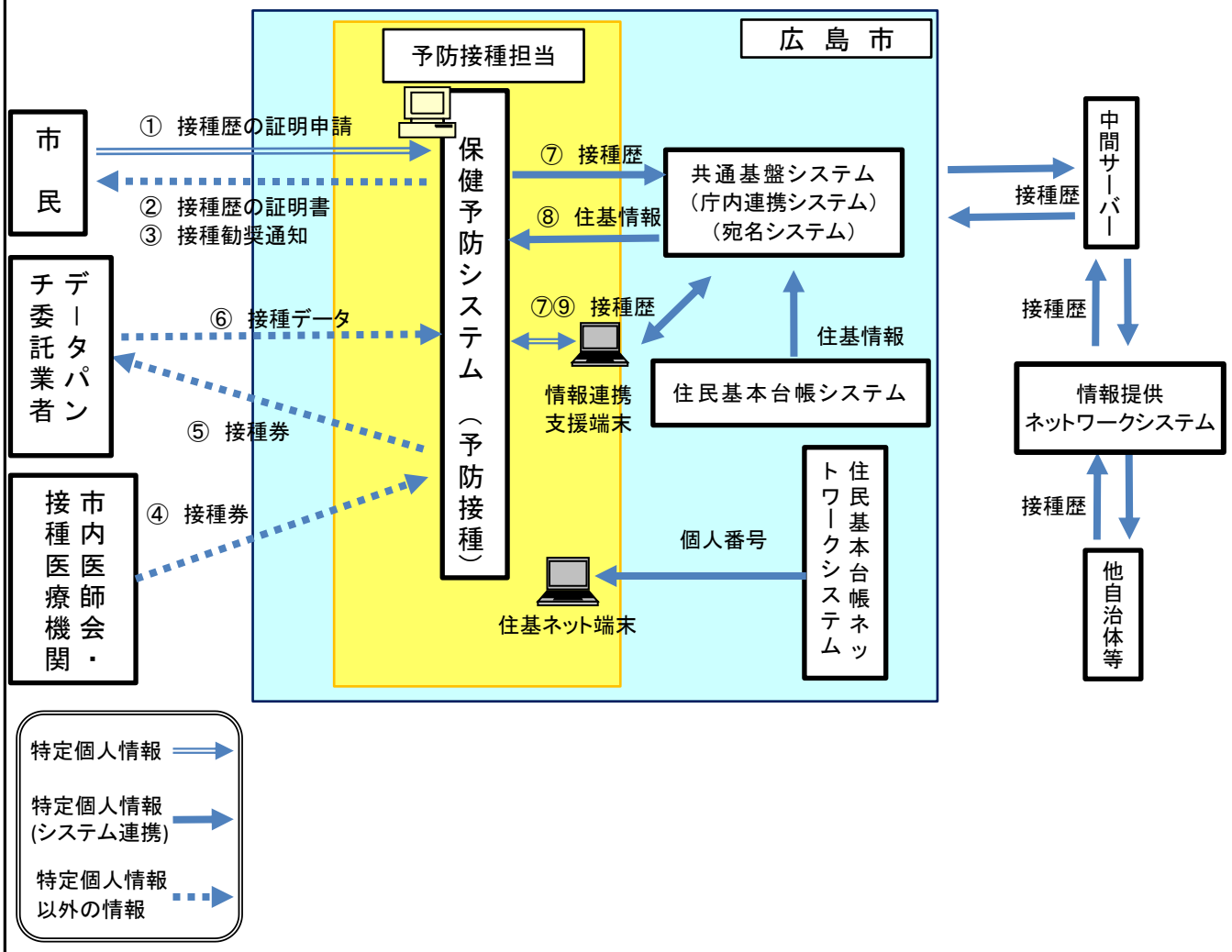
2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	共通基盤（庁内連携システム及び宛名システムに相当）
②システムの機能	1. ポータル機能 ICカードによる利用者認証、権限管理及び業務システムの起動を行う機能。 2. システム間連携制御機能 共通基盤と業務システム間及び異なる業務システム間のデータ連携を行う機能。 3. 運用管理機能 システム監視、稼働記録（ログ）管理、ウイルス対策及びデータのバックアップを行う機能。 4. 団体内統合宛名機能 個人番号と団体内統合宛名番号とを紐付けて管理する機能。団体内統合宛名番号が未登録の個人番号については、新規に団体内統合宛名番号を割り当てる。 5. 中間サーバー連携機能 中間サーバーと共通基盤間のデータ連携を行い、中間サーバーへの情報照会要求の送信及び照会結果の受信並びに特定個人情報の副本の登録を行う機能。 6. 特定個人情報登録・参照機能 情報連携支援端末を操作して、中間サーバーに登録する特定個人情報の副本を共通基盤に送信する機能。また、共通基盤に送信した中間サーバ登録前の特定個人情報の副本の内容を参照する機能。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[○] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [○] その他　（中間サーバー、国保・年金・後期高齢者医療システム、介護保険システム、福祉情報システム、市営住宅総合管理システム、選挙システム、下水道事業受益者負担金システム、財務会計システム、文書管理システム、人事・給与・庶務事務システム、水道料金オンラインシステム、小児慢性等システム、教育事務システム、放課後児童クラブ利用料金収納管理システム、庁内LAN）
システム2～5	

システム2	
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、特定個人情報の情報照会及び情報提供受領を行う機能。 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基システムとの間で情報照会内容、情報提供内容、特定個人情報、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(他市区町村への接種記録の照会・提供)。 8．セキュリティ管理機能 　特定個人情報の暗号化及び復号や、電文への署名付与、電文及び情報提供許可証に付与されている署名の検証、それらに伴う鍵管理を行う。また、情報提供ネットワークシステムから受信した情報提供NWS配信マスター情報を管理する機能。 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、機関別設定情報の管理を行う機能。 11．自己情報提供機能 　自己情報提供機能は、情報提供ネットワークシステムを介して自己情報に対する提供の求めを受領し、当該の特定個人情報及び自己情報提供用添付ファイルの提供を行う機能。 12．お知らせ機能 　お知らせ機能は、お知らせ情報提供対象者へのお知らせ情報の送信依頼に対し、情報提供ネットワークシステムを介して、お知らせ情報の提供を行う。また、お知らせ情報提供対象者へ提供したお知らせ情報に対する状況確認依頼に対し、情報提供ネットワークシステムを介して回答結果の受領を行う機能。
③他のシステムとの接続	[○] 情報提供ネットワークシステム　　[○] 庁内連携システム [　　] 住民基本台帳ネットワークシステム　　[　　] 既存住民基本台帳システム [○] 宛名システム等　　[　　] 税務システム [　　] その他　（　　）

システム3	
①システムの名称	保健予防システム
②システムの機能	≪マイナポータルぴったりサービスのサービス検索・電子申請機能及び申請管理システムを利用する場合記載≫ ・【住民向け機能】自らが受けることができるサービスをオンラインで検索及び申請ができる機能 ・【地方公共団体向け機能】住民が電子申請を行った際の申請データ取得画面又は機能を、地方公共団体に公開する機能
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　（　　）

システム4	
①システムの名称	住民基本台帳ネットワークシステム
②システムの機能	本人確認情報検索 住民登録外の者に係る申請書等に記載された個人番号の真正性の確認や個人番号の検索を行う。 なお、個人番号の真正性とは、「入手した個人番号が本人の個人番号で間違いないこと」をいう。以下同じ。
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	
予防接種台帳ファイル	
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	予防接種の履歴を登録することにより、本市の予防接種実施状況を正確かつ効率的に把握できるとともに、未接種者の把握が可能となるため未接種者に対する再度の接種勧奨を行うことができるようになる。
②実現が期待されるメリット	未接種者への通知により接種忘れによる未接種者が低減する。また、近い将来、市民が通常の端末から自分の接種履歴が確認できるようになる。
5. 個人番号の利用　※	
法令上の根拠	番号利用法第9条第1項、別表の14の項 番号利用法別表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6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	番号利用法第19条第8号、別表の14の項 番号利用法別表の主務省令で定める事務を定める命令　第10条
7. 評価実施機関における担当部署	
①部署	健康福祉局保健部健康推進課
②所属長の役職名	保健予防担当課長
8. 他の評価実施機関	
なし	

（別添1）事務の内容



（備考）

① 予防接種履歴の証明申請
② 予防接種履歴証明の手交
③ 接種勧奨通知の送付、未接種者への再勧奨通知の送付
④ 接種を受けた者の予防接種券（接種を受けた者の氏名、生年月日、宛て名番号、接種の種類が記載されたもの）を送付
⑤ 接種を受けた者の予防接種券の引き渡し
⑥ データ化された接種履歴（接種を受けた者の氏名、生年月日、宛て名番号、接種の種類）のシステムへの取り込み。
⑦ 他市区町村へ接種履歴の提供
⑧ 共通基盤システムを通じて、住民基本台帳システムからの市民の住基情報を移転
⑨ 他市区町村から接種履歴の入手

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		
予防接種台帳ファイル		
2. 基本情報		
①ファイルの種類　※		［　　システム用ファイル　　］　＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		［　100万人以上1,000万人未満　］　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲　※		・広島市に住民登録している法定予防接種事業の対象となる者 ・広島市に住民登録をしている期間に法定接種を受けた者 ・広島市に住民登録をしている者のうち、他市区町村における法定接種履歴の提供の求めがあった者
	その必要性	市が行う又は行った予防接種情報を適正に管理する必要があるため。また、市民の求めに応じて、接種履歴を提供できるようにする必要があるため。
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	1　識別情報 ・個人番号：対象者を正確に特定するために保有（参照）する。 ・その他識別情報（内部番号）：本市において、個人を一意に識別するために独自の識別番号を保有する。 2　連絡先等情報 ・4情報：接種履歴の登録、接種勧奨通知の印字等、事務で必要とする氏名、住所等を管理するために保有する。 ・その他住民票関係情報：適正な接種履歴の登録のため、被接種者の家族の情報等を保有する。 3　業務関係情報 ・医療機関で接種した接種履歴（接種日、ワクチンの種類、接種医療機関）を適正に管理するために保有する。
	全ての記録項目	別添2を参照。
⑤保有開始日		平成27年12月
⑥事務担当部署		健康福祉局健康推進課、各区地域支えあい課、出張所

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　（ 企画総務局総務課 ） [○] 行政機関・独立行政法人等　（ 地方公共団体情報システム機構 ） [○] 地方公共団体・地方独立行政法人　（ 他市区町村 ） [　] 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		・識別情報 随時 ・連絡先等情報 随時 ・業務関係情報（接種情報） 随時
④入手に係る妥当性		・識別情報 接種証明申請を行った者であることを確認するため入手する必要がある。 ・連絡先等情報 法令等に基づく接種対象者であることを相違なく抽出するため、及び住民の接種履歴を正しく登録するため入手する必要がある。 ・業務関係情報（接種情報） 法令等（予防接種法施行規則第3条、第4条等）に基づき、住民の接種履歴を記録・保管するために入手する必要がある。
⑤本人への明示		入手の根拠、使用目的 ・予防接種法施行規則第3条、第4条 ・番号利用法第9条第1項、第19条第8号
⑥使用目的 ※		予防接種の実施に当たり、対象者を適正に抽出し接種勧奨を行うとともに、未接種者に対して再勧奨を行う。また、市民の求めに応じ、本人の接種履歴を開示する。
	変更の妥当性	ー
⑦使用の主体	使用部署 ※	健康福祉局健康推進課、各区地域支えあい課、出張所
	使用者数	[　100人以上500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 ※		・本市が実施する予防接種の対象者の抽出を行い、接種勧奨を行う。 ・本市が実施する予防接種を受けた場合、本人特定を行い、その履歴を記録・保管する。 ・本人の申請により、接種履歴の証明を行う。 ・他市区町村における接種履歴を入手する。 ・本市における接種履歴情報を他市区町村へ提供する。
	情報の突合 ※	接種履歴の提供及び接種履歴の登録に当たり、証明申請書及び医療機関からの接種券に記載された住所、氏名等の情報について、住民票関係情報と突合する。
	情報の統計分析 ※	個人を特定するような情報の統計や分析は行わない。
	権利利益に影響を与え得る決定 ※	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		共通基盤の運用・保守業務
①委託内容		共通基盤に関する運用・保守業務（バックアップ取得、システムの稼働状況の監視、障害・異常発生時の確認及び復旧、自動実行ジョブスケジュールの設定・実行確認等）
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 ※	広島市に住民登録している法定予防接種事業の対象となる者、広島市に住民登録をしている期間に法定接種を受けた者及び広島市に住民登録をしている者のうち、他市区町村における法定接種履歴の提供の求めがあった者
	その妥当性	バックアップ取得、システム障害・異常発生時の対応においては、システムで保有するすべてのデータを取り扱うため、特定個人情報ファイルの全体の取扱いを委託することが妥当である。
③委託先における取扱者数		[10人未満] <選択肢> 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ]専用線 [ ]電子メール [ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ [ ]紙 [○]その他 （ システムの直接操作 ）
⑤委託先名の確認方法		広島市ホームページの調達情報公開システムにより、委託先名を公表している。
⑥委託先名		株式会社 日立製作所
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	委託契約書において、「委託業務の全部又は一部を第三者に委任し、若しくは請け負わせてはならない。ただし、あらかじめ書面により甲の承諾を得た場合は、当該業務の一部を第三者に委任し、又は請け負わせることができる。」としており、受託者から再委託承諾申請書の提出があり、内容を審査したところ適正であると認められたため、承諾している。
	⑨再委託事項	共通基盤の運用・保守業務のうち、システムの稼働状況の監視、障害・異常発生時の確認、自動実行ジョブスケジュールの実行確認等

委託事項2～5		
委託事項2		保健予防システムの運用・保守業務
①委託内容		保健予防システムに関する運用・保守業務（バックアップ取得、システムの稼働状況の監視、障害・異常発生時の確認及び復旧等）
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 ※	広島市に住民登録している法定予防接種事業の対象となる者、広島市に住民登録をしている期間に法定接種を受けた者及び広島市に住民登録をしている者のうち、他市区町村における法定接種履歴の提供の求めがあった者
	その妥当性	バックアップ取得、システム障害・異常発生時の対応においては、システムで保有する全てのデータを取り扱うため、特定個人情報ファイルの全体の取扱いを委託することが妥当である。
③委託先における取扱者数		［ 10人未満 ］ ＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		［ ］専用線　［ ］電子メール　［ ］電子記録媒体（フラッシュメモリを除く。） ［ ］フラッシュメモリ　［ ］紙 ［ ○ ］その他　（ システムの直接操作 ）
⑤委託先名の確認方法		広島市ホームページの調達情報公開システムにより、委託先名を公表している。
⑥委託先名		日本電気株式会社
再委託	⑦再委託の有無 ※	［ 再委託しない ］ ＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	

5. 特定個人情報の提供・移転（委託に伴うものを除く。）	
提供・移転の有無	[○] 提供を行っている （ 1 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	都道府県知事又は市町村長
①法令上の根拠	番号利用法第19条第8号 別表 14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	予防接種法による予防接種の実施に関する情報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	本市における予防接種履歴を有する他市区町村への転出者
⑥提供方法	[○] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑦時期・頻度	他市区町村から照会がある都度
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 ※		＜広島市における措置＞ ・特定個人情報は本市データセンター内に設置したサーバーのデータベース内に保管する。 ・データセンターでは、以下の3か所の入口において入退管理を行う。 1.データセンター入口のセキュリティゲート 2.サーバー室入口の電子錠 3.サーバー室内サーバー設置場所入口の電子錠 上記1及び2においては、ICカードでの認証を行い、3においてはICカード、パスワード及び生体認証（指紋）の三要素での認証を行っている。なお、ICカードは、事前に申請を受けて、入室を許可した者に対して個人ごとに貸与している。 また、入室を許可されない者が入室を許可された者に追従して不正に侵入すること（共連れ）を防止するため、データセンター入口のセキュリティゲートでは有人監視を実施するほか、重要な区画の入口には監視カメラを設置している。 ・データセンター内（サーバー室内を含む）には監視カメラを設置するほか、24時間365日警備員が常駐し、定期的に巡回を行う。 ・データセンターから情報記録媒体の持ち出しを行う場合、事前に本市担当職員が押印した情報記録媒体等持出承認書をデータセンターに持参し、退館する際に警備員に提出することとしている。 ・データセンターから退館する際、警備員による手荷物検査を行い、情報記録媒体等持出承認書に記載のない情報記録媒体を保持していた場合、データセンターからの持ち出しはできない。 ・特定個人情報を含むサーバー内のデータのバックアップテープはデータセンター内の耐火金庫に保管されるほか、大規模災害時の復旧に備えてデータセンターから300km以上離れた場所に分散保管される。 ・特定個人情報が記録された電子記録媒体及び紙媒体は、鍵付保管庫等で保管している。 ＜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。
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	予防接種法施行規則第3条において、記録を作成し、予防接種を行ったときから5年間保存しなければならないと規定されているため。
③消去方法		＜共通基盤における措置＞ 【共通】 ・情報セキュリティ実施手順や広島市文書取扱規程により、情報消去の責任者や手続、方法等保存期間経過後の消去時の取扱いを定めている。 ・保管期間経過後、特定個人情報が保存された記録媒体に対して一定回数以上の無作為な書き込みを行った上で、媒体そのものを物理的に破壊することで当該媒体に記録された特定個人情報を消去する。 ＜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

下表のとおり

住民情報				実施情報		結果情報	
1	個人番号	51	筆頭者氏名カナ清音	1	宛名番号	1	宛名番号
2	宛名番号	52	筆頭者氏名	2	受診日	2	受診日
3	世帯番号	53	筆頭者氏名外字Ｆ	3	業務CD	3	業務CD
4	住民種別	54	本名氏名カナ	4	種別CD	4	種別CD
5	住民状態	55	本名氏名カナ清音	5	事業CD	5	事業CD
6	大字コード	56	本名氏名	6	種別連番	6	受診日連番
7	番地	57	本名氏名外字Ｆ	7	受診日連番	7	項目CD
8	枝コード１	58	旧氏名カナ	8	受付番号	8	結果値
9	枝コード２	59	旧氏名カナ清音	9	医療機関CD	9	管轄CD
10	枝コード３	60	旧氏名	10	検索項目CD_1	10	更新年月日
11	枝コード４	61	旧氏名外字Ｆ	11	検査結果_1	11	更新時刻
12	行政区コード１	62	通称名カナ	12	検索項目CD_2	12	更新者職員番号
13	行政区コード２	63	通称名カナ清音	13	検査結果_2	13	種別連番
14	行政区コード３	64	通称名	14	検索項目CD_3		
15	民生委員地区コード	65	通称名外字Ｆ	15	検査結果_3		
16	投票区コード	66	世帯主氏名カナ	16	検索項目CD_4		
17	中学校コード	67	世帯主氏名カナ清音	17	検査結果_4		
18	小学校コード	68	世帯主氏名	18	検索項目CD_5		
19	福祉事務所コード	69	世帯主氏名外字Ｆ	19	検査結果_5		
20	住所自治省コード	70	世帯主通称名カナ	20	発行年月日		
21	住所全国大字コード	71	世帯主通称名カナ清音	21	発行時刻		
22	住所郵便番号	72	世帯主通称名	22	妊娠番号		
23	住所	73	世帯主通称名外字Ｆ	23	管轄CD		
24	住所未登録外字Ｆ	74	本名通称名区分	24	更新年月日		
25	住所方書	75	世帯主本通区分	25	更新時刻		
26	住所方書外字Ｆ	76	生年月日＿年号	26	更新者職員番号		
27	前住地自治省コード	77	生年月日				
28	前住所全国大字コード	78	性別				
29	前住地郵便番号	79	続柄				
30	前住地	80	住民異動年月日				
31	前住地外字Ｆ	81	住民届出年月日				
32	前住地方書	82	住民異動事由				
33	前住地方書外字Ｆ	83	住定異動年月日				
34	転出予定年月日	84	住定届出年月日				
35	転出区分	85	住定異動事由				
36	転先地自治省コード	86	住なく異動年月日				
37	転先地全国大字コード	87	住なく届出年月日				
38	転先地郵便番号	88	住なく異動事由				
39	転先地	89	異動年月日				
40	転先地外字Ｆ	90	届出年月日				
41	転先地方書	91	処理年月日				
42	転先地方書外字Ｆ	92	異動事由				
43	本籍地自治省コード	93	国籍コード				
44	本籍地全国大字コード	94	在留資格コード				
45	本籍地郵便番号	95	在留期間＿自				
46	本籍地	96	在留期間＿至				
47	本籍地外字Ｆ	97	外国人登録番号				
48	本籍地方書	98	更新年月日				
49	本籍地方書外字Ｆ	99	更新時刻				
50	筆頭者氏名カナ	100	更新者職員番号				

Ⅲ　特定個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	
予防接種台帳ファイル	
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	・接種証明申請受付窓口において、その内容や個人番号カード又は通知カード及び顔写真付きの身分証明書等による本人確認を厳格に行い、対象者以外の情報の入手の防止に努める。 ＜共通基盤における措置＞ ・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、当該事務の対象者以外の情報を入手することはできない。
必要な情報以外を入手することを防止するための措置の内容	・必要とする情報以外が記載できない証明申請様式としている。 ＜共通基盤における措置＞ ・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、当該事務に必要な情報以外の情報を入手することはできない。
その他の措置の内容	―
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 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	・紙媒体による入手は、あらかじめ決められた窓口に限定し、奪取が行えないようにしている。 ・システムの利用は、限られた専用の端末のみで利用でき、あらかじめ承認した利用者・権限の範囲に限っている。 ＜共通基盤における措置＞ ・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意が行われていることを必須条件としている。 ・情報を保有している事務と情報を必要としている事務双方から共通基盤の利用に係る申請書を提出させ、内容に相違がないか確認した上で設定を行っている。
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	・証明申請窓口において、本人の個人番号カード又は通知カード、身分証明書の提示等により本人確認を行っている。 ＜共通基盤における措置＞ ・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、入手した情報が他人の情報と紐付けられたり、別の情報に書き換えられたりすることはない。
個人番号の真正性確認の措置の内容	・証明申請窓口において提示された本人の個人番号カード又は通知カードに記載されている番号を、宛て名管理システム等で照合することにより、個人番号の真正性の確認を行う。 ＜共通基盤における措置＞ ・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、入手した情報が他人の個人番号と紐付けられたり、別の番号に書き換えられたりすることはない。
特定個人情報の正確性確保の措置の内容	・証明申請書に記載された事項について、提出された本人の個人番号カード又は通知カード、身分証明書の提示や聴き取りにより内容を確認することで、正確性を確保している。 ＜共通基盤における措置＞ ・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、システム間連携の過程で情報の正確性が失われることはない。
その他の措置の内容	―
リスクへの対策は十分か	[十分である]　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク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	・特定個人情報を記録した証明申請書は、鍵付き保管庫等で保管している。 ・事務処理に必要な証明申請書は、処理完了後は速やかに鍵付き保管庫等で保管するよう徹底している。 ＜共通基盤における措置＞ ・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、本市外部のネットワークからアクセスができない専用回線を用い、通信の暗号化を行った上で、あらかじめ認められた通信以外の通信を許可しない仕組みとすることで、特定個人情報の漏えいを防止している。
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	
接種情報については、医療機関から入手する時点では特定個人情報ではないが、システムに取り込んだ段階で特定個人情報となるため、次のとおり、リスクに対する措置を行う。 【本人確認の措置】 ・接種券に記載された氏名、生年月日、宛て名番号の3つの情報と、住基情報とをシステム内で照合し、合致した場合にのみシステムへ取り込むようにしている。情報が合致せず、エラーとなった場合は、接種医療機関に氏名や生年月日の記載誤りがないか確認するとともに、住所情報などを確認し、本人を特定している。 【情報の正確性確保】 ・重複接種や年齢対象外等の接種であった場合など正しい接種でない場合もエラーとなりシステムに取り込まれないようにしている。 ・取り込みエラーとなった接種については、接種した医療機関において確認してもらい、正しく修正したものを登録している。 ・システムに取り込むデータは、複数人でチェックを行い、接種券に記載されたものと同一であることを確認している。	

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		＜共通基盤における措置＞ ・共通基盤では、それぞれの番号利用事務の対象となる者の個人番号又は団体内統合宛名番号にのみアクセスできるようにアクセス制御を行っており、目的を超えた紐付けは行われない仕組みとなっている。 ・共通基盤の団体内統合宛名機能は、個人番号と団体内統合宛名番号の紐付を管理する機能であり、事務に必要のない情報との紐付けは行われない仕組みとなっている。
事務で使用するその他のシステムにおける措置の内容		・予防接種の業務で保健予防システムを利用する場合は、業務に関係のない他の情報へアクセスできないよう、内部制御されている。
その他の措置の内容		―
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク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	＜保健予防システムにおける措置＞ ・予防接種業務に従事する職員ごとに、予防接種台帳ファイルを使用できるIDを割り当て、ICカード及びパスワードによる認証を行っている。 ＜共通基盤における措置＞ ・システムを利用する必要がある職員に対し、個人ごとにユーザIDを割り当て、ICカード及びパスワードによる認証を行っている。
アクセス権限の発効・失効の管理		[行っている] ＜選択肢＞ 1）行っている　2）行っていない
	具体的な管理方法	＜保健予防システムにおける措置＞ 1．発効管理 ・所属長は毎年度、業務上、システムの操作が必要な正規職員、非正規職員に限り、利用者登録申請書をシステム管理担当課へ提出し、許可を得ている。 2．失効管理 ・業務上、システムの操作が不要になった職員については、速やかにIDカードを返却し、システムの使用が行えないようにしている。 ＜共通基盤における措置＞ 1．発効管理 ⑴人事異動等により、ユーザIDの登録が必要な場合、業務システムの管理者は、速やかに当該職員について、ユーザID申請書を共通基盤管理者に提出し、承認を得る。 ⑵共通基盤管理者はユーザID申請書に基づき、ユーザIDの割り当て及びICカードの発行を行う。 2．失効管理 ⑴人事異動等により、ユーザIDの削除が必要な場合、業務システムの管理者は、速やかに当該職員について、ユーザID申請書及びICカードを共通基盤管理者に提出し、承認を得る。 ⑵共通基盤管理者はユーザID申請書に基づき、ユーザIDの削除を行う。
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	・所属・係ごとに業務で使用する機能をあらかじめ設定し、その機能に限るよう権限設定を行っている。 ・ユーザIDの登録、変更、削除に関する記録を5年間保管することとしている。 ・アクセス権限を有する全職員について、本市職員が権限設定の登録台帳と実際の利用者の権限に差異がないか年1回確認する。 ＜共通基盤における措置＞ 1．ICカード管理台帳を作成し、ユーザIDごとのシステム利用権限を管理している。 2．ユーザIDの登録、変更、削除に関する記録を10年間保管することとしている。

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	システムのアクセスログ管理機能により、利用者、日時、利用端末、利用情報等の情報を記録し、その記録を用いて、本市職員が登録していない者のログインがないか等、不正なアクセスがないかを年1回以上分析している。 ＜共通基盤における措置＞ ・共通基盤の利用に係る稼働記録（ログ）では、利用者、日時、利用端末等を記録している。 ・稼働記録（ログ）は、10年間保存することとしている。
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		＜共通基盤における措置＞ ・操作記録（ログ）を取得・保存しており、事務外で利用した場合には、その職員を特定可能であることを職員に周知し、事務外での使用の抑止を図っている。
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		＜保健予防システム＞ ・データの複製は、管理権限を有する者のみが行える仕組みとしている。 ＜共通基盤における措置＞ ・操作記録（ログ）を取得・保存しており、事務外で利用した場合には、その職員を特定可能であることを職員に周知し、事務外での使用の抑止を図っている。
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置		
特定個人情報を記録した申請書は、鍵付き保管庫等で保管するとともに、職員に対し、情報セキュリティ研修や倫理研修を行い、職員の情報セキュリティ及び法令順守の意識の向上を図っている。		

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	＜保健予防システム及び共通基盤における措置＞ ・情報セキュリティ関連資格（プライバシーマーク、ISO27001、ISO9001）を取得している業者に運用・保守を委託している。 ・委託契約書に基づき、業務の推進体制及びセキュリティ対策等を記述した実施計画書を提出させ、確認している。	
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	＜保健予防システム及び共通基盤における措置＞ ・委託契約書により守秘義務を課しているほか、別記「個人情報取扱特記事項」に個人情報の適正な取り扱いについて、明記している。 ・あらかじめ、実施計画書により本業務の現場責任者及び従事者を報告させている。	
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	＜保健予防システム及び共通基盤における措置＞ ・委託先及び再委託先の従業員に係る操作記録（ログ）を取得し、保存している。 ・操作記録（ログ）には、操作日時、操作端末のIPアドレス、ユーザID、画面ID、個人番号等を記録している。 ・操作記録（ログ）はそれぞれ、10年間保存することとしている。	
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	＜保健予防システム及び共通基盤における措置＞ ・ルールの内容 委託契約書別記「個人情報取扱特記事項」において、本市の承諾がある場合を除き、個人情報を第三者に提供してはならないことを明記している。 ・ルール遵守の確認方法 委託契約書別記「個人情報取扱特記事項」の定めにより、履行状況を確認するため、委託先に対し、報告を求め、必要に応じて立入検査を実施する。	
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	＜保健予防システム及び共通基盤における措置＞ ・ルールの内容 委託契約書において、業務に必要な情報は本市から提供することとしている。 ・ルール遵守の確認方法 委託契約書別記「個人情報取扱特記事項」の定めにより、履行状況を確認するため、委託先に対し、報告を求め、必要に応じて立入検査を実施する。	

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	＜保健予防システム及び共通基盤における措置＞ ・ルールの内容 ・委託契約書別記「個人情報取扱特記事項」において、委託先は、個人情報が記録された資料等を契約の終了後又は解除後、直ちに本市に返還しなければならないこととされている。 ・ハードディスク等の記録装置に保存された特定個人情報については、記録装置に対する一定回数以上の上書き又は物理的な破壊等のデータ消去作業を行った上で廃棄することとしている。 ・ルール遵守の確認方法 ・委託契約書別記「個人情報取扱特記事項」の定めにより、履行状況を確認するため、委託先に対し、データ消去証明書の提出を求め、必要に応じて立入検査を実施している。
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	＜保健予防システム及び共通基盤における措置＞ 個人情報の適正な取り扱い、個人情報の取り扱いを行う場所について定めている。
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	＜共通基盤における措置＞ 情報セキュリティ実施手順に基づき、再委託先においても、委託先と同様の情報セキュリティ対策を実施させている。
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	[ ]	＜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	＜保健予防システムにおける措置＞ ・業務システムにおける権限設定により、情報提供ネットワークシステムへ情報照会の権限が与えられた者のみが利用できることにしている。 ・ログインを実施した職員、操作内容の記録が実施されるため、不適切な利用を抑止する仕組みとしている。 ＜共通基盤における措置＞ ・情報連携支援端末を操作して、中間サーバーを経由し、情報提供ネットワークシステムに情報照会を行う場合には、中間サーバー及び情報提供ネットワークシステムとの連携仕様に基づき、自動的に情報照会が行われる仕組みとなっており、目的外の情報を入手することはできない。 ・情報連携支援端末の利用にあたっては、ICカードによる利用者認証及び権限管理を行っており、あらかじめ登録された職員以外が情報照会を行うことはできない。 ＜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、番号利用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。 （「6. 情報提供ネットワークシステムとの接続」の項目全般については、新型コロナウイルス感染症対策
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	＜保健予防システムにおける措置＞ ・業務システムと共通基盤は、閉鎖した基幹業務系のネットワークで接続されており、業務システム端末機の接続に関してもMACアドレスによる認証等により、不適切な接続を防止している。 ＜共通基盤における措置＞ ・情報連携支援端末を操作して、中間サーバーを経由し、情報提供ネットワークシステムに情報照会を行う場合には、本市外部のネットワークからアクセスができない専用回線を用い、通信の暗号化を行っており、特定個人情報の漏えいを防止している。 ・情報連携支援端末の利用にあたっては、ICカードによる利用者認証及び権限管理を行っており、あらかじめ登録された職員以外が情報照会を行うことはできない。 ・磁気ディスク、USBメモリ等の電子記録媒体の利用は原則禁止とし、情報連携支援端末で利用できないよう、共通基盤で制御されている。電子記録媒体の利用は、あらかじめ、利用目的、利用頻度、利用端末等を明らかにした上で、業務主管課長から共通基盤管理責任者である情報システム課長に使用制限の解除を申請し、情報システム課長から共通基盤のシステムエンジニアに制限解除を指示する。共通基盤のシステムエンジニアが制限解除を行った後、業務主管課において、動作確認を行うという手順としている。電子記録媒体利用終了後の利用制限再設定についても、同様の手順としている。また、利用できる電子記録媒体は記録された情報を暗号化する機能を有するものに限定し、使用者も特定の職員のみとするとともに使用後は鍵付き保管庫で保管している。 ＜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、特定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。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。
リスクへの対策は十分か	[十分である]　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	＜保健予防システムにおける措置＞ ・情報照会は、個人番号をキーにして共通基盤に対して行う。共通基盤で管理する個人番号に1対1で対応する団体内統合宛名により、中間サーバーに照会し、情報を取得することから、照会対象者に係る正確な特定個人情報を入手することができる。 ＜共通基盤における措置＞ ・情報連携支援端末を操作して、中間サーバーに保存された情報照会の結果の入手を行う場合には、中間サーバーとの連携仕様に基づき、自動的に結果の入手が行われる仕組みとなっており、入手の過程で情報の正確性が失われることはない。 ＜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、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	＜保健予防システムにおける措置＞ ・業務システムと共通基盤は、閉鎖した基幹業務系のネットワークで接続されており、業務システム端末機の接続に関してもMACアドレスによる認証等により、不適切な接続を防止している。 ＜共通基盤における措置＞ ・情報連携支援端末を操作して、中間サーバーを経由し、情報提供ネットワークシステムに情報照会を行うには、本市外部のネットワークからアクセスができない専用回線を用い、通信の暗号化を行っており、特定個人情報の漏えいを防止している。 ・情報連携支援端末の利用にあたっては、ICカードによる利用者認証及び権限管理を行っており、あらかじめ登録された職員以外が情報照会を行うことはできない。 ・磁気ディスク、USBメモリ等の電子記録媒体の利用は原則禁止とし、情報連携支援端末で利用できないよう、共通基盤で制御されている。電子記録媒体の利用は、あらかじめ、利用目的、利用頻度、利用端末等を明らかにした上で、業務主管課長から共通基盤管理責任者である情報システム課長に使用制限の解除を申請し、情報システム課長から共通基盤のシステムエンジニアに制限解除を指示する。共通基盤のシステムエンジニアが制限解除を行った後、業務主管課において、動作確認を行うという手順としている。電子記録媒体利用終了後の利用制限再設定についても、同様の手順としている。また、利用できる電子記録媒体は記録された情報を暗号化する機能を有するものに限定し、使用者も特定の職員のみとするとともに使用後は鍵付き保管庫で保管している。 ＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ②既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ③情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報が漏えい・紛失するリスクを軽減している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）中間サーバーは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、漏えい・紛失のリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている

リスク5： 不正な提供が行われるリスク	
リスクに対する措置の内容	＜共通基盤における措置＞ ・共通基盤を利用し、中間サーバーに特定個人情報の副本を登録する場合には、中間サーバーとの連携仕様に基づき、自動的に特定個人情報の副本の登録が行われる仕組みとなっており、不正に特定個人情報を登録することはできない。 ①共通基盤内 ・磁気ディスク、USBメモリ等の電子記録媒体の利用は原則禁止とし、業務システム端末で利用できないよう、共通基盤で制御されている。電子記録媒体の利用は、あらかじめ、利用目的、利用頻度、利用端末等を明らかにした上で、業務主管課長から共通基盤管理責任者である情報システム課長に使用制限の解除を申請し、情報システム課長から共通基盤のシステムエンジニアに制限解除を指示する。共通基盤のシステムエンジニアが制限解除を行った後、業務主管課において、動作確認を行うという手順としている。電子記録媒体利用終了後の利用制限再設定についても、同様の手順としている。また、利用できる電子記録媒体は記録された情報を暗号化する機能を有するものに限定している。 ②情報連携支援端末 ・情報連携支援端末を操作して、中間サーバーに特定個人情報の副本を登録する場合には、中間サーバーとの連携仕様に基づき、自動的に特定個人情報の副本の登録が行われる仕組みとなっており、不正に特定個人情報を登録することはできない。 ・情報連携支援端末の利用にあたっては、ICカードによる利用者認証及び権限管理を行っており、あらかじめ登録された職員以外が中間サーバーに特定個人情報の副本を登録することはできない。 ・磁気ディスク、USBメモリ等の電子記録媒体の利用は原則禁止とし、情報連携支援端末で利用できないよう、共通基盤で制御されている。電子記録媒体の利用は、あらかじめ、利用目的、利用頻度、利用端末等を明らかにした上で、業務主管課長から共通基盤管理責任者である情報システム課長に使用制限の解除を申請し、情報システム課長から共通基盤のシステムエンジニアに制限解除を指示する。共通基盤のシステムエンジニアが制限解除を行った後、業務主管課において、動作確認を行うという手順としている。電子記録媒体利用終了後の利用制限再設定についても、同様の手順としている。また、利用できる電子記録媒体は記録された情報を暗号化する機能を有するものに限定し、使用者も特定の職員のみとするとともに使用後は鍵付き保管庫で保管している。 ＜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。
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	＜共通基盤における措置＞ ・共通基盤を利用し、中間サーバーに特定個人情報の副本を登録する場合には、中間サーバーとの連携仕様に基づき、自動的に特定個人情報の副本の登録が行われる仕組みとなっており、不適切な方法で特定個人情報を登録することはできない。 ・磁気ディスク、USBメモリ等の電子記録媒体の利用は原則禁止とし、業務システム端末で利用できないよう、共通基盤の運用管理機能で制御されている。電子記録媒体の利用は、あらかじめ、利用目的、利用頻度、利用端末等を明らかにした上で、業務主管課長から共通基盤管理責任者である情報システム課長に使用制限の解除を申請し、情報システム課長から共通基盤のシステムエンジニアに制限解除を指示する。共通基盤のシステムエンジニアが制限解除を行った後、業務主管課において、動作確認を行うという手順としている。電子記録媒体利用終了後の利用制限再設定についても、同様の手順としている。また、利用できる電子記録媒体は記録された情報を暗号化する機能を有するものに限定している。 ・情報連携支援端末を操作して、中間サーバーに特定個人情報の副本を登録する場合には、中間サーバーとの連携仕様に基づき、自動的に特定個人情報の副本の登録が行われる仕組みとなっており、不適切な方法で特定個人情報を登録することはできない。 ・情報連携支援端末の利用にあたっては、ICカードによる利用者認証及び権限管理を行っており、あらかじめ登録された職員以外が中間サーバに特定個人情報の副本を登録することはできない。 ・磁気ディスク、USBメモリ等の電子記録媒体の利用は原則禁止とし、情報連携支援端末で利用できないよう、共通基盤で制御されている。電子記録媒体の利用は、あらかじめ、利用目的、利用頻度、利用端末等を明らかにした上で、業務主管課長から共通基盤管理責任者である情報システム課長に使用制限の解除を申請し、情報システム課長から共通基盤のシステムエンジニアに制限解除を指示する。共通基盤のシステムエンジニアが制限解除を行った後、業務主管課において、動作確認を行うという手順としている。電子記録媒体利用終了後の利用制限再設定についても、同様の手順としている。また、利用できる電子記録媒体は記録された情報を暗号化する機能を有するものに限定し、使用者も特定の職員のみとするとともに使用後は鍵付き保管庫で保管している。 ＜中間サーバー・ソフトウェアにおける措置＞ ①セキュリティ管理機能（※）により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ②中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）暗号化・復号機能と、鍵情報及び照会許可用照合リストを管理する機能。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、不適切な方法で提供されるリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。
リスクへの対策は十分か	[十分である]　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	＜保健予防システムにおける措置＞ ・情報提供は、共通基盤で個人番号に1対1で対応する団体内統合宛名及び符号により行うため、提供対象者に係る正確な特定個人情報を提供することができる。 ＜共通基盤における措置＞ ・共通基盤を利用し、中間サーバーに特定個人情報の副本を登録する場合には、中間サーバーとの連携仕様に基づき、自動的に特定個人情報の副本の登録が行われる仕組みとなっており、誤った情報を中間サーバーに登録することはない。 ・情報連携支援端末を操作して、中間サーバーに特定個人情報の副本を登録する場合には、中間サーバーとの連携仕様に基づき、自動的に特定個人情報の副本の登録が行われる仕組みとなっており、誤った情報を中間サーバーに登録することはない。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。 ②情報提供データベース管理機能（※）により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ③情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 （※）特定個人情報を副本として保存・管理する機能。
リスクへの対策は十分か	[十分である]　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	
＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。	

7. 特定個人情報の保管・消去

リスク1： 特定個人情報の漏えい・滅失・毀損リスク

①NISC政府機関統一基準群	[政府機関ではない]	＜選択肢＞ 1）特に力を入れて遵守している　2）十分に遵守している 3）十分に遵守していない　4）政府機関ではない
②安全管理体制	[十分に整備している]	＜選択肢＞ 1）特に力を入れて整備している　2）十分に整備している 3）十分に整備していない
③安全管理規程	[十分に整備している]	＜選択肢＞ 1）特に力を入れて整備している　2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	＜選択肢＞ 1）特に力を入れて周知している　2）十分に周知している 3）十分に周知していない
⑤物理的対策	[十分に行っている]	＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
具体的な対策の内容	＜広島市における措置＞ ・特定個人情報は本市データセンター内に設置したサーバーのデータベース内に保管する。 ・データセンターでは、以下の3か所の入口において入退管理を行う。 1.データセンター入口のセキュリティゲート 2.サーバー室入口の電子錠 3.サーバー室内サーバー設置場所入口の電子錠 上記1及び2においては、ICカードでの認証を行い、3においてはICカード、パスワード及び生体認証（指紋）の三要素での認証を行っている。なお、ICカードは、事前に申請を受けて、入室を許可した者に対して個人ごとに貸与している。また、入室を許可されない者が入室を許可された者に追従して不正に侵入すること（共連れ）を防止するため、データセンター入口のセキュリティゲートでは有人監視を実施するほか、重要な区画の入口には監視カメラを設置している。 ・データセンター内（サーバー室内を含む）には監視カメラを設置するほか、24時間365日警備員が常駐し、定期的に巡回を行う。 ・データセンターから情報記録媒体の持ち出しを行う場合、事前に本市担当職員が押印した情報記録媒体等持出承認書をデータセンターに持参し、退館する際に警備員に提出することとしている。 ・データセンターから退館する際、警備員による手荷物検査を行い、情報記録媒体等持出承認書に記載のない情報記録媒体を保持していた場合、データセンターからの持ち出しはできない。 ・特定個人情報を含むサーバー内のデータのバックアップテープはデータセンター内の耐火金庫に保管されるほか、大規模災害時の復旧に備えてデータセンターから300km以上離れた場所に分散保管される。 ・特定個人情報の消去にあたっては、委託業者がハードディスク等の記録装置に対する一定回数以上の上書き又は物理的な破壊等のデータ消去作業を行った上で廃棄することとしている。また、データ消去証明書の提出を求め、必要に応じて立入検査を実施している。 ・特定個人情報が記録された電子記録媒体及び紙媒体は、鍵付保管庫等で保管している。 ・特定個人情報を取り扱う事務室等については、部外者の進入を禁止している。 ・窓口付近に設置する端末機は、通行人等から画面が見えない向きに設置している。 ＜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・プラットフォームを中間サーバー用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。	

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	＜広島市における措置＞ 1．不正アクセス防止 ・共通基盤の各種機能の利用にあたっては、ICカードによる利用者認証及び権限管理を行っており、あらかじめ登録された職員以外が特定個人情報にアクセスすることはできない。また、各種機能に係る操作記録（ログ）の取得・保存を行っており、不正使用が認められる場合には、職員の特定が可能であることを周知することで、特定個人情報への不正アクセスの抑止を図っている。 ・本市の庁内ネットワークは、本市外部のネットワークからアクセスができない専用回線を用い、通信の暗号化を行った上で、あらかじめ設定された通信仕様に基づく通信のみ許可する仕組みとすることで、特定個人情報の漏えいを防止している。また、本市の庁内ネットワークは、常時監視を行っており、不正アクセス等の脅威が検知された場合には、監視画面に警告が表示されると共に、脅威の種類、対象端末（又はサーバー、ネットワーク機器）、時間等を記録する操作記録（ログ）が取得・保存される。 2．ウイルス対策 ・ウイルス対策ソフトを導入し、パターンファイルを常に最新になるよう、日次レベルで更新し、各業務システム及び端末に配信している。 ・磁気ディスク、USBメモリ等の電子記録媒体の利用は原則禁止とし、業務システム端末で利用できないよう、共通基盤で制御されている。電子記録媒体の利用は、あらかじめ、利用目的、利用頻度、利用端末等を明らかにした上で、共通基盤担当へ申請する手順としている。また、利用できる電子記録媒体は記録された情報を暗号化する機能を有するものに限定している。 ・共通基盤により、業務システム端末の運用状況を監視しており、許可されていない電子記録媒体が接続された場合には、監視場面に警告が表示されるとともに、当該端末、ユーザ等を記録した操作記録（ログ）が取得・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＞ ①中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ②中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。
⑦バックアップ		[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知		[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか		[　発生なし　] ＜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	生存者の個人番号と同様の保管、管理を実施している。
その他の措置の内容		―
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク2： 特定個人情報が古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	新たに法定接種を受けた場合は、随時、最新情報に更新している。	
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： 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	＜保健予防システム及び共通基盤における措置＞ ・保管期限を経過したデータは、アクセス制御によりシステムでは使用できないようにしている。 ・特定個人情報が保存された記録媒体そのものを廃棄する場合は、記録媒体に対して一定回数以上の無作為な書き込みを行った上で、媒体そのものを物理的に破壊する。 ＜紙媒体に係る措置＞ ・申請書等の紙媒体の管理は広島市文書取扱規定に基づき管理徹底しており、保有年限を経過した文書は毎年一斉に廃棄している。廃棄に当たっては、必ず溶解処理を行っている。	
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
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		
特定個人情報を含む情報資産を廃棄する場合は、情報を復元できないように処置した上で廃棄している。また、機器リース終了等による返却の場合も同様とする。 ・紙文書は、溶解処分を行っている。 ・電子記録媒体は、物理的破壊、データ消去ソフトウェアによるデータ消去を行っている。 ・サーバー、パソコン等情報機器については、記録装置に対して、物理的破壊、データ消去ソフトウェアによるデータ消去を行っている。 ・個人情報を保管している保管庫の鍵については、一部の者しか知り得ない場所へ保管し、適切に管理している。		

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	＜共通基盤における措置＞ 【共通】 ・「広島市情報セキュリティポリシー」に、「定期的に又は必要に応じて自己点検を行い、改善の必要があるものについては、速やかに改善措置を行うこと」を定め、毎年1回、情報セキュリティの自己点検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＞ ①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、毎年1回、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	＜共通基盤における措置＞ 【共通】 ・「広島市情報セキュリティポリシー」に、「定期的に又は必要に応じて情報セキュリティ監査を行い、改善の必要があるものについては、速やかに改善措置を行うこと」を定め、4年に1回、外部監査を実施することとしている。 （監査内容） ・個人情報保護に関する規定、体制整備 ・個人情報保護に関する人的安全管理措置 ・職員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措置 など ＜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、毎年1回、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	＜共通基盤における措置＞ 【共通】 　次に掲げる情報セキュリティ研修・公務員倫理研修を毎年実施し、具体的な情報セキュリティ事故の事例紹介等により、職員の情報セキュリティ意識・法令遵守意識の向上を図っている。 　なお、情報セキュリティ研修については、eラーニングを導入し、未受講者に対して催促メールを送信することで受講率の向上を図っている。また、公務員倫理研修（情報セキュリティに関する部分）については、庁内LANの全庁資料室に研修資料を掲載しているため、未受講者がいつでも研修資料を参照できる。 ・情報セキュリティ研修 　新規採用職員研修、一般職員研修、新任課長級職員研修、新任課長補佐級職員研修 ・公務員倫理研修（情報セキュリティに関する部分） 　全職員研修、所属長研修、所属長による所属内研修 ＜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。	

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＞
①中間サーバー・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。

Ⅴ　開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	広島市公文書館 〒730－0051　広島市中区大手町四丁目1番1号　大手町平和ビル8階 電話番号　082－243－2583
②請求方法	所定の請求書に必要事項を記載し、前記「①請求先」に提出する。その際、運転免許証など本人であることを確認できる身分証明書等を提示する必要がある。
特記事項	広島市ホームページに請求方法や手数料等について掲載している。
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	保健予防システム
公表場所	広島市公文書館
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	広島市健康福祉局保健部健康推進課保健予防係 〒730－8586　広島市中区国泰寺町一丁目6番34号 電話番号　082－504－2882
②対応方法	問合せの受付時に受付票を起票し、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4年12月22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	市ホームページにおいて、意見公募する旨を掲載し、評価書（案）の所管課における閲覧及び配布、ホームページへの掲載を行う。意見の提出は、持参、郵送、FAX又は電子メールにより受け付ける。
②実施日・期間	令和4年10月15日から令和4年11月11日まで
③期間を短縮する特段の理由	－
④主な意見の内容	個人情報はどこかで広まるし本人が自分から言うこともあり、リスクは防げないので、情報が洩れても大丈夫な社会になり、みなが扶け合う精神を作ったり理解することが先決である。
⑤評価書への反映	なし
3. 第三者点検	
①実施日	令和4年11月16日から令和4年11月18日まで
②方法	専門性を有する第三者（個人情報の保護及び情報システムに知見を有している者）の意見を聞く。
③結果	第三者点検の結果、一部の記載内容の修正を行い、特段の問題はないものと認められた。
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
令和8年3月24日	I-7-②所属長の役職名	感染症対策担当課長	保健予防担当課長	事後	重要な変更に当たらないため、事前の提出、公表は義務付けられていない。
令和8年3月24日	V-2-①連絡先	広島市健康福祉局保健部健康推進課感染症対策係 〒730－8586　広島市中区国泰寺町一丁目6番34号 電話番号　082－504－2622	広島市健康福祉局保健部健康推進課保健予防係 〒730－8586　広島市中区国泰寺町一丁目6番34号 電話番号　082－504－2882	事後	重要な変更に当たらないため、事前の提出、公表は義務付けられていない。