

特定個人情報保護評価書(重点項目評価書)

評価書番号	評価書名
34	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 重点項目評価書

個人のプライバシー等の権利利益の保護の宣言

大東市は、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当たり、そ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、特定個人情報の漏洩その他の事態を発生させるリスクを軽減させるために十分な措置を行い、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項	なし
------	----

評価実施機関名

大東市長

公表日

令和7年8月12日

項目一覧

I 基本情報
II 特定個人情報ファイルの概要
(別添1) 特定個人情報ファイル記録項目
III リスク対策
IV 開示請求、問合せ
V 評価実施手続
(別添2) 変更箇所

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	<p>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とは、新型インフルエンザ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(以下「番号利用法」という。)の規定に従い、新型インフルエンザ等が発生した場合に、特定接種や住民接種を行う。また、接種歴に関する情報を副本として中間サーバーに登録し、情報提供ネットワークシステムに接続することで、各情報保有機関が保有する特定個人情報について照会・回答などの情報連携を行う。</p> <p>具体的には、特定個人情報ファイルを次の事務に使用している。</p> <p>①住民基本台帳をもとに、対象者の選定 ②予防接種実施状況の登録(接種日、接種場所、Lot.No等) ③情報提供ネットワークシステムでの予防接種履歴の照会・提供 ④健康被害が生じた場合の給付金の支給</p>
③対象人数	<p>[10万人以上30万人未満]</p> <p style="text-align: right;"><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</p>
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	<p>予防接種システム</p> <p>①入力機能 医療機関から送付された予診票の情報を入力し、管理する。</p> <p>②統計分析 保有するデータベースから条件を指定したものを集計する。</p> <p>③帳票印刷 保有するデータベースから条件を指定したものを出力する。</p> <p>④個別総合照会 条件を指定した対象者の保有する情報を照会する。</p>
③他のシステムとの接続	<p>[] 情報提供ネットワークシステム [<input type="radio"/>] 庁内連携システム</p> <p>[] 住民基本台帳ネットワークシステム [<input type="radio"/>] 既存住民基本台帳システム</p> <p>[<input checked="" type="radio"/>] 宛名システム等 [] 税務システム</p> <p>[] その他 ()</p>
システム2～5	
システム2	
①システムの名称	団体内総合宛名システム
②システムの機能	<p>1. 宛名番号付番機能 団体内統合宛名番号が未登録の個人について、新規に団体内統合宛名番号を付番する機能。既存業務システムからの団体内統合宛名番号要求に対し、団体内統合宛名番号を付番し、既存業務システム及び中間サーバーに対し返却する</p> <p>2. 宛名情報等管理機能 団体内統合宛名システムにおいて、宛名情報を団体内統合宛名番号、個人番号と紐づけて保存し管理する機能</p> <p>3. 中間サーバ連携機能 中間サーバまたは中間サーバ端末からの要求にも続き、団体内統合宛名番号に紐づく宛名情報等を通知する機能</p> <p>4. 既存システム連携機能 既存業務システムからの要求に基づき、個人番号又は団体内統合宛名番号に紐づく宛名情報を通知する機能</p>

③他のシステムとの接続	<input type="checkbox"/> 情報提供ネットワークシステム <input type="radio"/> 庁内連携システム <input type="checkbox"/> 住民基本台帳ネットワークシステム <input type="radio"/> 既存住民基本台帳システム <input type="radio"/> 宛名システム等 <input type="radio"/> 税務システム <input type="radio"/> その他 (中間サーバ、健康管理システム)
システム3	
①システムの名称	中間サーバシステム
②システムの機能	<p>①符号管理機能 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」とをひもづけ、当該情報を保管及び管理する機能</p> <p>②情報照会機能 情報提供ネットワークシステムを介して、特定個人情報(連携対象)の情報照会及び情報提供受領(照会した情報の受領)を行う機能</p> <p>③情報提供機能 情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報(連携対象)の提供を行う機能</p> <p>④既存システム接続機能 番号連携サーバとの間で情報照会内容、情報提供内容、特定個人情報(連携対象)、符号取得のための情報等について連携するための機能</p> <p>⑤情報提供等記録管理機能 特定個人情報(連携対象)の照会又は提供があった旨の情報提供等記録を生成し、管理する機能</p> <p>⑥情報提供データベース管理機能 特定個人情報(連携対象)を副本として、保持・管理する機能</p> <p>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</p> <p>⑧セキュリティ管理機能 セキュリティを管理するための機能</p> <p>⑨職員認証・権限管理機能 利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報(連携対象)へのアクセス制御を行う機能</p> <p>⑩システム管理機能 バッチの状況管理、業務統計情報の集計、稼動状態の通知、保管期限切れ情報の削除を行う機能</p>
③他のシステムとの接続	<input type="radio"/> 情報提供ネットワークシステム <input type="radio"/> 庁内連携システム <input type="checkbox"/> 住民基本台帳ネットワークシステム <input type="checkbox"/> 既存住民基本台帳システム <input type="checkbox"/> 宛名システム等 <input type="checkbox"/> 税務システム <input type="checkbox"/> 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	
4. 個人番号の利用 ※	
法令上の根拠	<p>1. 行政手続き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(番号利用法)(平成25年5月31日法律第27号)</p> <p>・番号利用法第9条第1項 別表14項、126項</p> <p>2. 行政手続きにおける特定の個人を識別するための番号の利用等に関する法律別表の主務省令で定める事務を定める命令(平成26年内閣府・総務省令第5号)</p> <p>・第10条 第67条の2</p>
5. 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	<p>[実施する]</p> <p style="text-align: right;"><選択肢> 1) 実施する 2) 実施しない 3) 未定</p>
②法令上の根拠	<p>(情報提供の根拠):</p> <p>・番号利用法第19条第8号</p> <p>・番号利用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2条の表の25及び26の項及び、第27、28条</p> <p>(情報照会の根拠):</p> <p>・番号利用法第19条第8号</p> <p>・番号利用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2条の表の25及び26の項及び、第27、28条</p> <p>(委託への提供)</p> <p>・番号利用法第19条第6号</p>
6. 評価実施機関における担当部署	
①部署	保健医療部 地域保健課
②所属長の役職名	地域保健課長
7. 他の評価実施機関	

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	
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 ※	大東市内に居住する予防接種の対象となる者
その必要性	住民接種は市民全員を対象に予防接種を実施するため
④記録される項目	[10項目以上50項目未満] <選択肢> 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
主な記録項目 ※	<ul style="list-style-type: none"> ・識別情報 [<input type="checkbox"/>] 個人番号 [<input type="checkbox"/>] 個人番号対応符号 [<input type="checkbox"/>] その他識別情報(内部番号) ・連絡先等情報 [<input type="checkbox"/>] 5情報(氏名、氏名の振り仮名、性別、生年月日、住所) [<input type="checkbox"/>] 連絡先(電話番号等) [<input type="checkbox"/>] その他住民票関係情報 ・業務関係情報 [<input type="checkbox"/>] 国税関係情報 [<input type="checkbox"/>] 地方税関係情報 [<input type="checkbox"/>] 健康・医療関係情報 [<input type="checkbox"/>] 医療保険関係情報 [<input type="checkbox"/>] 児童福祉・子育て関係情報 [<input type="checkbox"/>] 障害者福祉関係情報 [<input type="checkbox"/>] 生活保護・社会福祉関係情報 [<input type="checkbox"/>] 介護・高齢者福祉関係情報 [<input type="checkbox"/>] 雇用・労働関係情報 [<input type="checkbox"/>] 年金関係情報 [<input type="checkbox"/>] 学校・教育関係情報 [<input type="checkbox"/>] 災害関係情報 [<input type="checkbox"/>] その他 ()
その妥当性	<ul style="list-style-type: none"> ①識別情報 対象者を正確に特定するため ②連絡先等情報 予防接種対象者の居住地等を把握するため ③業務関係情報 予防接種の接種歴を把握するため
全ての記録項目	別添1を参照。
⑤保有開始日	令和3年6月13日
⑥事務担当部署	保健医療部 地域保健課

3. 特定個人情報の入手・使用								
①入手元 ※	<input type="checkbox"/> 本人又は本人の代理人 <input type="checkbox"/> 評価実施機関内の他部署 (市民課) <input type="checkbox"/> 行政機関・独立行政法人等 () <input type="checkbox"/> 地方公共団体・地方独立行政法人 (他自治体) <input type="checkbox"/> 民間事業者 (医療機関) <input type="checkbox"/> その他 ()							
②入手方法	<input type="checkbox"/> 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 <input type="checkbox"/> 電子メール [] 専用線 [<input type="checkbox"/>] 庁内連携システム <input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> その他 ()							
③使用目的 ※	予防接種対象者を特定し、実施記録の作成、管理を行い、情報提供する。また、予防接種等による健康被害の救済に関する給付に係る請求書等の確認を行う。							
④使用の主体	使用部署 保健医療部 地域保健課							
	使用者数 [10人以上50人未満] <table border="0" style="margin-left: 20px;"> <tr> <td colspan="2" style="text-align: center;"><選択肢></td> </tr> <tr> <td>1) 10人未満</td> <td>2) 10人以上50人未満</td> </tr> <tr> <td>3) 50人以上100人未満</td> <td>4) 100人以上500人未満</td> </tr> <tr> <td>5) 500人以上1,000人未満</td> <td>6) 1,000人以上</td> </tr> </table>	<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
<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							
⑤使用方法	<ul style="list-style-type: none"> ・予防接種対象者の抽出 ・予防接種に関する記録の作成 ・予防接種等による健康被害の救済に関する給付に係る事務 							
情報の突合	予診票に記載されている情報と住民基本台帳システムから連携された4情報を突合し、被接種者を特定し、記録を作成する。また、給付金の請求書と連携された4情報を突合して整合性を確認し、給付事務を進める。							
⑥使用開始日	令和3年6月13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	健康管理システムの保守・改修業務	
①委託内容	健康管理システムの保守・改修業務を開発業者へ委託している。	
②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	
③委託先名	アトラス情報サービス株式会社	
再委託	④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
	⑤再委託の許諾方法	
	⑥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 () 件 [] 移転を行っている () 件 [○] 行っていない
提供先1	
①法令上の根拠	
②提供先における用途	
③提供する情報	
④提供する情報の対象となる本人の数	[] [] <small><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</small>
⑤提供する情報の対象となる本人の範囲	
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	
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	[] [] <small><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</small>
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

保管場所 ※

【市における保管場所の措置】

データセンターにおいて特定個人情報を保管。
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。

＜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。

②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。

＜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。

7. 備考

(別添1) 特定個人情報ファイル記録項目

予防接種台帳

■識別情報及び連絡先等情報

1. 個人番号
2. 統合宛名番号
3. 宛名番号
4. 世帯番号
5. 氏名
6. 生年月日
7. 性別
8. 続柄
9. 現住所
10. 住所コード
11. 地区担当保健師
12. 学区
13. 電話番号
15. 住民になった日
16. 住民になった異動日
17. 住民になった届出年月日
18. 住民でなくなった事由
19. 住民でなくなった異動日
20. 住民でなくなった届出日
21. 住定事由
22. 住定年月日
23. 住定届出年月日
24. 住民区分
25. 外国人判定
26. 国籍
27. 通称名情報
28. 個人特記情報
29. DVフラグ

■業務関係情報

1. 西暦年度
2. 宛名番号
3. 性別
4. 接種日
5. 回数
6. 接種日年齢
7. 年度末年齢
8. 基準日年齢
9. 更新者
10. 更新日
11. 更新時間
12. 実施医療機関
13. 接種医
14. LotNo
15. 接種量
16. 予診フラグ
17. 対象外判定
18. 特記事項

Ⅲ リスク対策 ※(7. ②を除く。)

1. 特定個人情報ファイル名	
予防接種台帳	
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： 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	住民からの申告等による情報は、本人確認書類の提示や個人番号カード又は通知カードによる確認を行う。
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、事務に必要なない情報との紐付けが行われるリスク	
リスクに対する措置の内容	①特定個人情報を閲覧できる者はセキュリティ設定により制限されている。 ②アクセスログを取得しており、必要に応じて解析等できるようにしている。
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	健康管理システムを利用可能な職員を特定し、IDとパスワードによる認証を行っている。パスワードは定期的に変更している。
その他の措置の内容	ログインおよび操作ログの記録を行う。
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

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： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転に関するルール	[定めている]	<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	番号法及び住基法並びに個人情報保護条例の規定に基づき認められる特定個人情報の移転について、本業務では具体的マニュアルを整備し、提供を実施する	
その他の措置の内容	サーバー室への入退室及びシステムへのアクセス権を厳格に管理し、原則情報の持ち出しを制限する。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の提供・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	<p><中間サーバー・ソフトウェアにおける措置></p> <p>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照会リスト(*2)との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。</p> <p>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。</p> <p>(*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</p>		
リスクへの対策は十分か	[十分である]	<p><選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>	
リスク2: 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	<p><中間サーバー・ソフトウェアにおける措置></p> <p>①情報照会機能(*)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照会リストを情報提供ネットワークシステムから入手し、中間サーバーに格納して、情報提供機能により、照会許可照会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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>(*) 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</p>		
リスクへの対策は十分か	[十分である]	<p><選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>	
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			
<p><中間サーバー・ソフトウェアにおける措置></p> <p>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。</p> <p>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。</p> <p><中間サーバー・プラットフォームにおける措置></p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。</p>			

7. 特定個人情報の保管・消去		
リスク： 特定個人情報の漏えい・滅失・毀損リスク		
①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
②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		

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		
<p>●物理的対策 <本市における措置> ①特定個人情報を保管するサーバ設置場所には、入退室管理を行う。 ②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する。 ③特定個人情報を保管したPCはセキュリティワイヤにより盗難防止を行い、特定個人情報を扱う職員が離席する際には、パスワード付きスクリーンセーバーを利用する。 ④特定個人情報を保管した媒体の運用ルールを定め、遵守する。 ⑤特定個人情報を保管するサーバに係る脅威に対して、無停電電源装置の設置、室温管理、ケーブルの安全管理、耐震対策、防火措置、防水措置等を講じる。 ⑥特定個人情報を保管するサーバは定期保守を実施することで情報の毀損等への対策を図り、定期保守を実施する際には、事業者による漏えい等を防ぐため、秘密保持契約や情報を消去した状態にする等の対策を実施する。</p> <p><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、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。</p> <p><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。 ②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。</p> <p>●技術的対策 <本市における措置> ①ウイルス対策ソフトを導入し、定期的にパターンファイルの更新を行っている。 ②OSやアプリケーション等に対するセキュリティ対策用修正ソフト(いわゆるセキュリティパッチ)を適用している。 ③ウイルスメール/スパムメール対策システムを導入している。 ④ファイアウォールにより、特定個人情報へのアクセスを制御している。 ⑤外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止している。 ⑥使用されていないポートを閉鎖している。</p> <p><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。 ④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。 ⑤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。 ⑥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。 ⑦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。</p> <p><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契約等となっている。 ②地方公共団体が委託したアプリケーション開発事業者等は、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アプリケーション開発事業者等は、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。 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地方公共団体やアプリケーション開発事業者等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。</p>		

8. 監査	
実施の有無	[<input checked="" type="checkbox"/>] 自己点検 [] 内部監査 [] 外部監査
9. 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	<p>初任時及び一定期間ごとに、必要な知識の習得に資するための研修を実施する。</p> <p><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。</p>
10. その他のリスク対策	
<p><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、環境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。</p> <p><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。</p>	

IV 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	〒574-0028 大東市幸町8番1号 大東市保健医療部地域保健課 電話 072-874-9500
②請求方法	指定様式による書面の申し出により開示、訂正、利用停止請求を受け付ける。
③法令による特別の手続	
④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	〒574-0028 大東市幸町8番1号 大東市保健医療部地域保健課 電話 072-874-9500
②対応方法	問い合わせを受け付けた場合、問い合わせ内容及びこれに係る対応について、記録を残す。 情報漏えい等の重大な問い合わせについて、関係先等に事実確認を行うため、処理期間を設ける。

V 評価実施手続

1. 基礎項目評価	
①実施日	令和3年3月1日
②しきい値判断結果	[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] <選択肢> 1) 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 2) 基礎項目評価の実施が義務付けられる(任意に重点項目評価を実施) 3) 特定個人情報保護評価の実施が義務付けられない(任意に重点項目評価を実施)
2. 国民・住民等からの意見の聴取【任意】	
①方法	
②実施日・期間	
③主な意見の内容	
3. 第三者点検【任意】	
①実施日	
②方法	
③結果	

(別添2)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9月1日	1. 基本情報 5. 情報提供 ネットワークシステムによる 情報提供 ②法令上の根拠	番号利用法上第19条第7号	番号利用法上第19条第8号	事後	
令和7年8月12日	1. 基本情報 4. 個人番号の利用 法令上の根拠	1. 行政手続き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(番号利用法)(平成25年5月31日法律第27号) ・番号利用法第9条第1項 別表第一項番93の2 2. 行政手続き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(別表第一省令)(平成26年内閣府・総務省令第5号) ・別表第一省令第67条の2	1. 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(番号利用法)(平成25年5月31日法律第27号) ・番号利用法第9条第1項 別表14項、126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の主務省令で定める事務を定める命令(平成26年内閣府・総務省令第5号) ・第10条 第67条の2	事後	法的根拠、条項の整理
令和7年8月12日	1. 基本情報 5. 情報提供 ネットワークシステムによる 情報提供 ②法令上の根拠	1. 番号利用法上第19条第8号(特定個人情報の提供の制限)及び別表第二(別表第二における情報提供の根拠) :第三欄(情報提供者)が「市町村長」の項のうち、第四欄(特定個人情報)に「新型インフルエンザ等対策特別措置法(平成二十四年法律第三十一号)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」が含まれる項(項番115の2)(別表第二における情報照会の根拠) :第一欄(情報照会者)が「市町村長」の項のうち、第二欄(事務)に「新型インフルエンザ等対策特別措置法(平成二十四年法律第三十一号)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」が含まれる項(項番115の2) 2. 行政手続き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等を定める命令(別表第二省令)(平成26年内閣府・総務省令第7号)(別表第二主務省令における情報提供の根拠)・別表第二省令(第59条の2)(※別表第二項番115の2)(別表第二の主務省令における情報照会の根拠) ・別表第二省令(第59条の2)(※別表第二項番115の2)	(情報提供の根拠): ・番号利用法第19条第8号 ・番号利用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2条の表の25及び26の項及び、第27、28条 (情報照会の根拠): ・番号利用法第19条第8号 ・番号利用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2条の表の25及び26の項及び、第27、28条 (委託への提供) ・番号利用法第19条第6号	事後	法的根拠、条項の整理

(別添2) 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7年8月12日	Ⅲリスク対策 6. 情報提供ネットワークシステムとの接続 情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	<p><中間サーバー・ソフトウェアにおける措置></p> <p>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制する仕組みになっている。</p> <p>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は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。</p> <p><中間サーバー・プラットフォームにおける措置></p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p><中間サーバー・ソフトウェアにおける措置></p> <p>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制する仕組みになっている。</p> <p>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。</p> <p><中間サーバー・プラットフォームにおける措置></p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。</p>	事前	ガバメントクラウド利用開始に伴い変更
令和7年8月12日	Ⅲリスク対策 7. 特定個人情報の保管・消去 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	<p>●物理的対策</p> <p><本市における措置></p> <p>①特定個人情報を保管するサーバ設置場所には、入退室管理を行う。</p> <p>②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の上に設置せず、キーボードに施設保管する。</p> <p>③特定個人情報を保管したPCはセキュリティワイヤにより盗難防止を行い、特定個人情報を扱う職員が離席する際には、パスワード付きスクリーンセーバーを利用する。</p> <p>④特定個人情報を保管した媒体の運用ルールを定め、遵守する。</p> <p>⑤特定個人情報を保管するサーバに係る脅威に対して、無停電電源装置の設置、室温管理、ケーブルの安全管理、耐震対策、防火措置、防水措置等を実施する。</p> <p>⑥特定個人情報を保管するサーバは定期保守を実施することで情報の毀損等への対策を図り、定期保守を実施する際には、事業者による漏えい等を防ぐため、秘密保持契約や情報を消去した状態にする等の対策を実施する。</p> <p><中間サーバー・プラットフォームにおける措置></p> <p>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、有人監視及び施設管理をする。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。</p> <p>●技術的対策</p> <p><本市における措置></p> <p>①ウイルス対策ソフトを導入し、定期的にパターンファイルの更新を行っている。</p> <p>②OSやアプリケーション等に対するセキュリティ対策用修正ソフト(いわゆるセキュリティパッチ)を適用している。</p> <p>③ウイルスメール/スパムメール対策システムを導入している。</p> <p>④ファイアウォールにより、特定個人情報へのアクセスを制御している。</p> <p>⑤外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止している。</p> <p>⑥使用されていないポートを閉鎖している。</p> <p><中間サーバー・プラットフォームにおける措置></p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>●物理的対策</p> <p><本市における措置></p> <p>①特定個人情報を保管するサーバ設置場所には、入退室管理を行う。</p> <p>②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の上に設置せず、キーボードに施設保管する。</p> <p>③特定個人情報を保管したPCはセキュリティワイヤにより盗難防止を行い、特定個人情報を扱う職員が離席する際には、パスワード付きスクリーンセーバーを利用する。</p> <p>④特定個人情報を保管した媒体の運用ルールを定め、遵守する。</p> <p>⑤特定個人情報を保管するサーバに係る脅威に対して、無停電電源装置の設置、室温管理、ケーブルの安全管理、耐震対策、防火措置、防水措置等を実施する。</p> <p>⑥特定個人情報を保管するサーバは定期保守を実施することで情報の毀損等への対策を図り、定期保守を実施する際には、事業者による漏えい等を防ぐため、秘密保持契約や情報を消去した状態にする等の対策を実施する。</p> <p><中間サーバー・プラットフォームにおける措置></p> <p>中間サーバー・プラットフォームは、運用環境システムのためのクラウド環境構築(CMaaS)に選定されたクラウドサービス事業者が保有・管理する専用環境に、秘密保持契約を締結してクラウドサービス事業者を利用する。また、クラウドサービス事業者は、セキュリティ対策等、セキュリティ対策等の実施に努めている。ISO 27001、ISO 27002等の認証を取得している。日本国内でデータセンターを有している。</p> <p>●技術的対策</p> <p><本市における措置></p> <p>①ウイルス対策ソフトを導入し、定期的にパターンファイルの更新を行っている。</p> <p>②OSやアプリケーション等に対するセキュリティ対策用修正ソフト(いわゆるセキュリティパッチ)を適用している。</p> <p>③ウイルスメール/スパムメール対策システムを導入している。</p> <p>④ファイアウォールにより、特定個人情報へのアクセスを制御している。</p> <p>⑤外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止している。</p> <p><中間サーバー・プラットフォームにおける措置></p> <p>①中間サーバー・プラットフォームでは、運用環境システムのためのクラウド環境構築(CMaaS)に選定されたクラウドサービス事業者が保有・管理する専用環境に、秘密保持契約を締結してクラウドサービス事業者を利用する。また、クラウドサービス事業者は、セキュリティ対策等、セキュリティ対策等の実施に努めている。ISO 27001、ISO 27002等の認証を取得している。日本国内でデータセンターを有している。</p> <p>②中間サーバー・プラットフォームは、運用環境システムのためのクラウド環境構築(CMaaS)に選定されたクラウドサービス事業者が保有・管理する専用環境に、秘密保持契約を締結してクラウドサービス事業者を利用する。また、クラウドサービス事業者は、セキュリティ対策等、セキュリティ対策等の実施に努めている。ISO 27001、ISO 27002等の認証を取得している。日本国内でデータセンターを有している。</p> <p>③中間サーバー・プラットフォームは、運用環境システムのためのクラウド環境構築(CMaaS)に選定されたクラウドサービス事業者が保有・管理する専用環境に、秘密保持契約を締結してクラウドサービス事業者を利用する。また、クラウドサービス事業者は、セキュリティ対策等、セキュリティ対策等の実施に努めている。ISO 27001、ISO 27002等の認証を取得している。日本国内でデータセンターを有している。</p> <p>④中間サーバー・プラットフォームは、運用環境システムのためのクラウド環境構築(CMaaS)に選定されたクラウドサービス事業者が保有・管理する専用環境に、秘密保持契約を締結してクラウドサービス事業者を利用する。また、クラウドサービス事業者は、セキュリティ対策等、セキュリティ対策等の実施に努めている。ISO 27001、ISO 27002等の認証を取得している。日本国内でデータセンターを有している。</p> <p>⑤中間サーバー・プラットフォームは、運用環境システムのためのクラウド環境構築(CMaaS)に選定されたクラウドサービス事業者が保有・管理する専用環境に、秘密保持契約を締結してクラウドサービス事業者を利用する。また、クラウドサービス事業者は、セキュリティ対策等、セキュリティ対策等の実施に努めている。ISO 27001、ISO 27002等の認証を取得している。日本国内でデータセンターを有している。</p> <p>⑥中間サーバー・プラットフォームは、運用環境システムのためのクラウド環境構築(CMaaS)に選定されたクラウドサービス事業者が保有・管理する専用環境に、秘密保持契約を締結してクラウドサービス事業者を利用する。また、クラウドサービス事業者は、セキュリティ対策等、セキュリティ対策等の実施に努めている。ISO 27001、ISO 27002等の認証を取得している。日本国内でデータセンターを有している。</p>	事前	ガバメントクラウド利用開始に伴い変更

