

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

個人のプライバシー等の権利利益の保護の宣言

越谷市は、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、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

新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務では、事務の一部を外部業者に委託しているため、業者選定の際に業者の情報保護管理体制を確認し、併せて秘密保持に関しても契約に含めることで万全を期している。

評価実施機関名

越谷市長

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16日

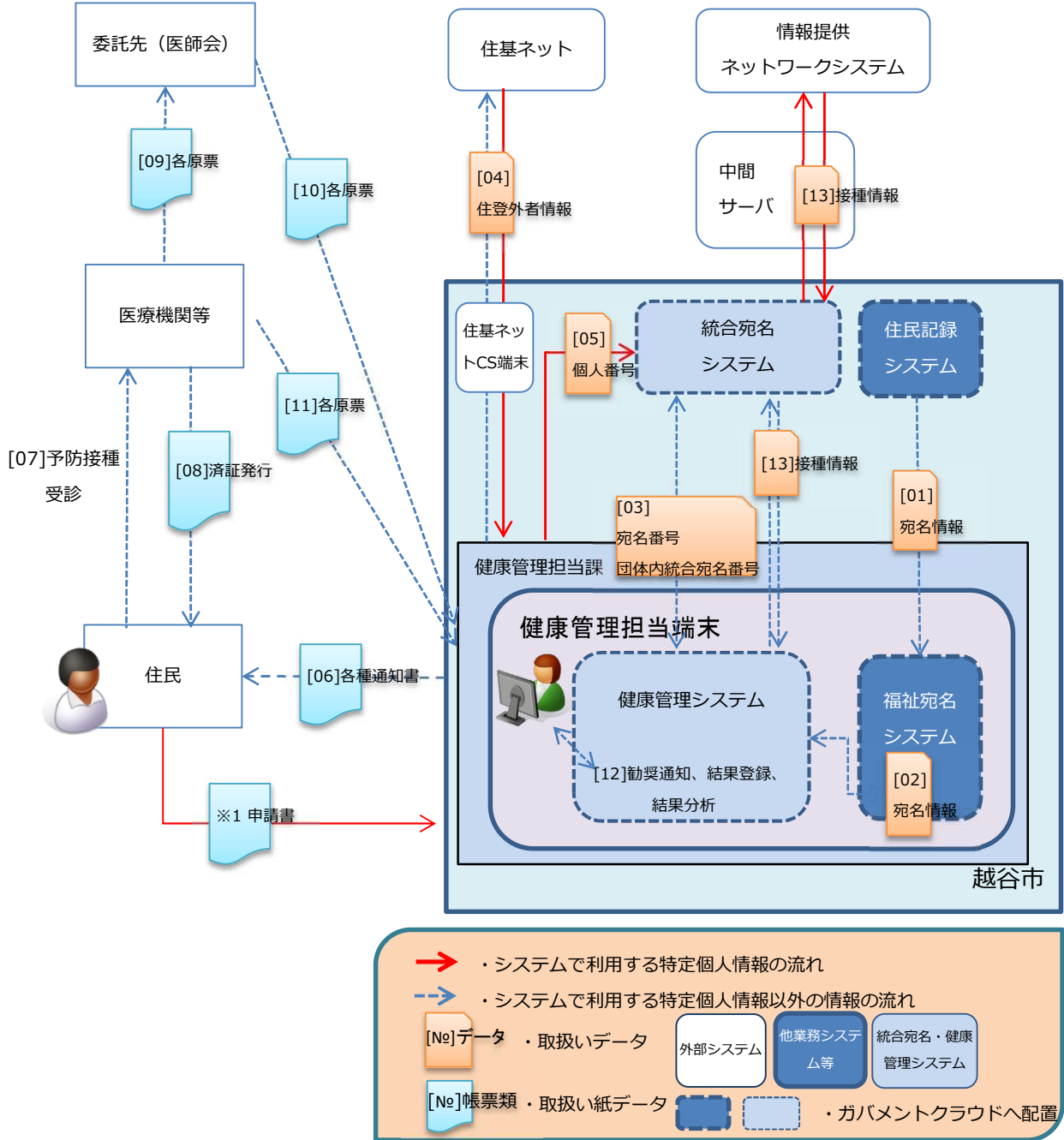
項目一覧

I 基本情報
(別添1) 事務の内容
II 特定個人情報ファイルの概要
(別添2) 特定個人情報ファイル記録項目
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
IV その他のリスク対策
V 開示請求、問合せ
VI 評価実施手続
(別添3) 変更箇所

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	<p>中間サーバーは、情報提供ネットワークシステム・団体内統合宛名システム間のデータ受け渡しをすることで、符号の取得や他情報保有機関間の特定個人情報照会・提供の機能を提供する。</p> <ol style="list-style-type: none"> 1. 符号管理機能 <ul style="list-style-type: none"> ・符号管理機能は情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「統一識別番号」とを紐付け、その情報を保管・管理する。 2. 情報照会機能 <ul style="list-style-type: none"> ・情報照会機能は、情報提供ネットワークシステムを介して、特定個人情報(連携対象)の情報照会及び情報提供受領(照会した情報の受領)を行う。 3. 情報提供機能 <ul style="list-style-type: none"> ・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. 各業務システム接続機能 <ul style="list-style-type: none"> ・中間サーバーと各業務システム、団体内統合宛名システム及び住民記録システムとの間で情報照会内容、情報提供内容、特定個人情報(連携対象)、符号取得のための情報等について連携する。 5. 情報提供等記録管理機能 <ul style="list-style-type: none"> ・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。 6. 情報提供データベース管理機能 <ul style="list-style-type: none"> ・特定個人情報(連携対象)を副本として、保持・管理する。 7. データ送受信機能 <ul style="list-style-type: none"> ・中間サーバーと情報提供ネットワークシステム(インターフェイスシステム)との間で情報照会、情報提供、符号取得のための情報等について連携する。 8. セキュリティ管理機能 <ul style="list-style-type: none"> ・暗号化/復号機能と、鍵情報及び照会許可照会リスト情報を管理する。 9. 職員認証・権限管理機能 <ul style="list-style-type: none"> ・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 <ul style="list-style-type: none"> ・バッチの状況管理、業務統計情報の集計、稼働状態の通知、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	<table border="0"> <tr> <td><input type="checkbox"/> 情報提供ネットワークシステム</td> <td><input type="checkbox"/> 庁内連携システム</td> </tr> <tr> <td><input type="checkbox"/> 住民基本台帳ネットワークシステム</td> <td><input type="checkbox"/> 既存住民基本台帳システム</td> </tr> <tr> <td><input type="checkbox"/> 宛名システム等</td> <td><input type="checkbox"/> 税務システム</td> </tr> <tr> <td colspan="2"><input type="checkbox"/> その他 ()</td> </tr> </table>	<input type="checkbox"/> 情報提供ネットワークシステム	<input type="checkbox"/> 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 ()	
<input type="checkbox"/> 情報提供ネットワークシステム	<input type="checkbox"/> 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4									
①システムの名称	団体内統合宛名システム(以下「統合宛名システム」という。)								
②システムの機能	<ol style="list-style-type: none"> 1. 宛名番号付番機能 <ul style="list-style-type: none"> ・団体内統合宛名番号(以下「統合宛名番号」という。)が未登録の個人について、新規に統合宛名番号を付番する。各事務システムからの統合宛名番号要求に対し、統合宛名番号を付番し、各事務システム及び中間サーバーに対し返却する。 2. 宛名情報等管理機能 <ul style="list-style-type: none"> ・統合宛名システムにおいて宛名情報を統合宛名番号、個人番号と紐付けて保存し、管理する。 3. 中間サーバー連携機能 <ul style="list-style-type: none"> ・中間サーバー、又は中間サーバー端末からの要求に基づき、統合宛名番号に紐づく宛名情報等を通知する。 4. 各事務システム連携機能 <ul style="list-style-type: none"> ・各事務システムからの要求に基づき、個人番号、又は統合宛名番号に紐づく宛名情報を通知する。 								
③他のシステムとの接続	<table border="0"> <tr> <td><input type="checkbox"/> 情報提供ネットワークシステム</td> <td><input checked="" type="checkbox"/> 庁内連携システム</td> </tr> <tr> <td><input type="checkbox"/> 住民基本台帳ネットワークシステム</td> <td><input checked="" type="checkbox"/> 既存住民基本台帳システム</td> </tr> <tr> <td><input checked="" type="checkbox"/> 宛名システム等</td> <td><input type="checkbox"/> 税務システム</td> </tr> <tr> <td colspan="2"><input checked="" type="checkbox"/> その他 (中間サーバー)</td> </tr> </table>	<input type="checkbox"/> 情報提供ネットワークシステム	<input checked="" type="checkbox"/> 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 checked="" type="checkbox"/> 既存住民基本台帳システム	<input checked="" type="checkbox"/> 宛名システム等	<input type="checkbox"/> 税務システム	<input checked="" type="checkbox"/> その他 (中間サーバー)	
<input type="checkbox"/> 情報提供ネットワークシステム	<input checked="" type="checkbox"/> 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 checked="" type="checkbox"/> 既存住民基本台帳システム								
<input checked="" type="checkbox"/> 宛名システム等	<input type="checkbox"/> 税務システム								
<input checked="" type="checkbox"/> その他 (中間サーバー)									

6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[実施する] <選択肢> 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	情報照会: 番号法第19条第8号及び番号法第19条第8号に基づく主務省令第2条の表153の項 情報提供: 番号法第19条第8号及び番号法第19条第8号に基づく主務省令第2条の表153の項、154の項
7. 評価実施機関における担当部署	
①部署	保健医療部健康づくり推進課
②所属長の役職名	課長
8. 他の評価実施機関	
-	

(別添1) 事務の内容



(備考)

- [01] 住民記録システムより宛名情報を入手する。
 - [02] 福祉宛名システムより宛名情報を入手する。
 - [03] 統合宛名システムより宛名番号情報を入手する。
 - [04] 住基ネットCS端末より住登外者情報を照会する。
 - [05] 健康管理担当課にて番号情報を入手、更正する。
 - [06] 個人に各種通知書(勸奨通知、受診券、結果表等)を発行する。
 - [07] 個人が医療機関に受診を行う。
 - [08] 医療機関より個人宛に済証を発行する。
 - [09] 医療機関より委託先へ各種原票が送付される。
 - [10] 委託先より健康管理担当課へ各種原票が送付される。
 - [11] 医療機関より健康管理担当課へ各種原票が送付される。
 - [12] 健康管理担当課にて健康管理システムより各種通知書、結果登録等を行う。
 - [13] 情報提供ネットワークシステムより情報入手する。(接種履歴)
- ※1 住民から申請書を受け付ける。

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	
新型インフルエンザ等対策特別措置法に基づく予防接種関係情報ファイル	
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 ※	新型インフルエンザ等対策特別措置法に基づく予防接種の対象者
その必要性	新型インフルエンザ等対策特別措置法に基づく予防接種に基づく予防接種対象者であることの管理、対象者の接種記録を適正に管理・保管するために必要
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"> ・個人番号、その他識別情報: 対象者の特定、接種記録の管理を行うために保有 ・5情報、連絡先: 正確に本人を特定するために保有 ・健康・医療関係情報: 予防接種記録の管理を行うために保有
全ての記録項目	別添2を参照。
⑤保有開始日	令和3年6月13日
⑥事務担当部署	保健医療部健康づくり推進課

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 () <input type="checkbox"/> 行政機関・独立行政法人等 () <input checked="" type="checkbox"/> 地方公共団体・地方独立行政法人 () <input type="checkbox"/> 民間事業者 () <input type="checkbox"/> その他 ()	
②入手方法	<input checked="" 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 checked="" type="checkbox"/> 庁内連携システム <input checked="" type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> その他 ()	
③入手の時期・頻度	・連絡先情報については本人から申請を受けた都度入手する。 ・接種記録については、接種を行った医療機関から月次単位で入手する。	
④入手に係る妥当性	・連絡先情報を本人等から入手する場合、本人又は本人の代理人等が必要となった時に申請書により申請を行うため、情報は申請を受けた都度入手する。 ・連絡先情報を情報提供ネットワークを使用して入手する場合、本人又は本人の代理人等が必要となった時に申請書により申請を行うため、情報は申請を受けた都度入手する。 ・接種記録は実施した医療機関から月ごとに入手する。	
⑤本人への明示	本人等から入手する場合は本人等に対し、使用目的等を文書に明示又は口頭で説明する	
⑥使用目的 ※	対象者の資格管理、接種記録の管理・保管に係る事務を適正に行うため	
	変更の妥当性 ー	
⑦使用の主体	使用部署 ※	保健医療部健康づくり推進課
	使用者数	[10人以上50人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
⑧使用方法 ※		①対象者の資格管理 住民票関係情報、本人等の申請内容等をシステムに登録し、登録された情報を基に新型インフルエンザ等対策特別措置法に基づく予防接種の対象者を確認する。 ②接種記録の管理・保管 システムに接種記録を登録し、接種記録の管理・保管を行う。
	情報の突合 ※	申請者情報を住民票関係情報と突合し、対象者の資格を確認する。
	情報の統計分析 ※	個人を判別しうるような情報の統計は行わない。
	権利利益に影響を与え得る決定 ※	接種対象者であるかの決定を行う。
⑨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運用
①委託内容	健康管理システムの保守運用
②取扱いを委託する特定個人情報ファイルの範囲	[特定個人情報ファイルの全体] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
対象となる本人の数	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
対象となる本人の範囲 ※	「2. ③対象となる本人の範囲」と同上
その妥当性	保守運用業務の範囲は、ハードウェア、ソフトウェア、運用業務としての電算処理にわたり、システム上保有する全てのファイルを取り扱うため
③委託先における取扱者数	[10人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法	[<input checked="" type="checkbox"/>] 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 ()
⑤委託先名の確認方法	総務部契約課窓口にて公表している
⑥委託先名	株式会社アイネス
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
再委託	⑧再委託の許諾方法
再委託	⑨再委託事項
委託事項2～5	
委託事項6～10	
委託事項11～15	
委託事項16～20	

6. 特定個人情報の保管・消去

①保管場所 ※

<越谷市における措置>
 ①入退室管理を行っている部屋に設置したサーバー内に保管する。
 ②サーバーへのアクセスはIDと生体認証(又はパスワード)による認証が必要となる。
 ③紙媒体については越谷市文書管理規程により施錠できるファイリングキャビネットに保管する。
 ④電子記録媒体については、施錠できる場所に保管する。

<中間サーバー・プラットフォームにおける措置>
 ①中間サーバー・プラットフォームは、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。

②保管期間	期間	[20年以上]	<選択肢> 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない
	その妥当性	予防接種法施行令第6条の2において、5年間保管すると定められているが、接種記録確認等の事務のため長期間保管する必要がある。	

③消去方法

<越谷市における措置>
 ①サーバーやパソコン等の処理時には、データ消去ソフトによりデータ復元不可能な状態にし、物理的な破棄を行う。
 ②申請書等紙媒体については、内部にて定められた期間保存後溶解処理を行う。
 ③電子記録媒体については、内部にて定められた期間保存後、読み取りが不可能な状態にして破棄している。

<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事業者及びクラウドサービス事業者が特定個人情報を消去することはない。
 ②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。
 ③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。

<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、NIST800-88、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棄等を実施する。

7. 備考

(別添2) 特定個人情報ファイル記録項目

〈新型インフルエンザ〉

1.接種日,2.接種場所,3.接種時年齢,4.請求年月, 5.診察区分, 6.LOT-NO, 7.ワクチン, 8.転入前接種, 9.予診医師名, 10.接種医師名, 11.公費自費区分, 12.委託料, 13.接種量, 14.備考1, 15.備考2, 16.備考3,

団体内統合宛名

1.個人番号、2.情報提供用個人番号識別符号、3.団体内宛名番号

中間サーバー

1.情報提供等の記録等

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	
新型インフルエンザ等対策特別措置法に基づく予防接種関係情報ファイル	
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	個人番号カード、または通知カードと本人確認書類の提示による本人確認を厳守する。 申請内容等と健康管理システムの登録情報との確認を行うことにより、申請内容の確認を行う。
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	・本人からの申請等による入手については、必要項目のみ記載できる用紙を使用し、必要な情報以外の入手を防止する。 ・システムにおいては、情報の取得を必要情報のみに限定しており、それ以外の情報の取得はできない構成となっている。
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： 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	<事務における措置> ①個人番号カード、または通知カードと本人確認書類の提示による本人確認を厳守することで、対象者以外の情報入手を防止する。 ②申請書等への記載を求める場合、若しくは調査又は照会等を行う際は、利用目的等を示した上で実施している。 ③システムを利用する職員を限定している。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	個人番号カード、または通知カードと本人確認書類の提示を受け、必ず本人確認を行う。
個人番号の真正性確認の措置の内容	データ化してシステムに取り込む際に論理的エラーチェックを行い正確性を確保し、個人番号に加え基本5情報の合致により対象者の確認を行う。
特定個人情報の正確性確保の措置の内容	・申請による入手においては、対面での聞き取り及び添付書類との照合により正確性を確保し、併せて庁内連携や情報提供ネットワークによる照会により入手情報の正確性を担保する。 ・正確性に疑義が生じた場合は、随時調査を行い補正を行う。
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	申請書等の紙媒体については、定められた保管場所で施錠管理を行う。
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	<ul style="list-style-type: none"> ・ユーザ単位の権限により、不要なアクセスを行えないよう制御している。 ・個人番号を利用しない各システムから要求に応じないよう制御している。 ・中間サーバーからの要求に応じるだけであるため、必要な情報の切分けは中間サーバーで行われている。 ・特定個人情報の中間サーバーへの連携システムであり、その他のシステムに連携する機能は有していない。
事務で使用するその他のシステムにおける措置の内容	・他の業務システムについても、アクセス権限が設定されており、権限のない業務システムについてはアクセスできない仕組みとなっている。
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	・システムを利用できる職員を限定しており、生体認証とすることでなりすましを防止している。
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	<ul style="list-style-type: none"> ・権限の妥当性を確認した上で各事務を所管する事業課からの依頼に応じて必要な権限を付与している。 ・職員が退職した等により、システムを利用しなくなった場合については、各事務を所管する事業課からの依頼に応じて、速やかにシステムの利用権限を消去することとしている。
アクセス権限の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	<ul style="list-style-type: none"> ・権限の妥当性を確認した上で各事務を所管する事業課からの依頼に応じて必要な権限を付与している。 ・アクセス権限は定期的に更新を行っている。
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	・アクセスログやシステム操作の履歴(利用者ID、日時、システムへのアクセス状況、データへのアクセス状況)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	<ul style="list-style-type: none"> ・生体認証や権限設定により対象外の情報にはアクセスできない仕組みとなっている。 ・職員に対して情報セキュリティ研修を実施し、事務外利用の禁止について指導している。
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	<ul style="list-style-type: none"> ・システムの権限設定により、管理者以外は複製ができない仕組みとなっている。 ・情報セキュリティ研修において、複製禁止について指導している。
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	
—	

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、提供許可証の発行と照会内容の照会許可用照会リスト(※2)との照会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。</p> <p>(※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。</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</p> <p>2) 十分である</p> <p>3) 課題が残されている</p>	
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	<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に設計されるため、安全性が担保されている。</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>		
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</p> <p>2) 十分である</p> <p>3) 課題が残されている</p>	
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	<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。</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</p> <p>2) 十分である</p> <p>3) 課題が残されている</p>	
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	<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(※)。</p> <p>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。</p> <p>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、一定期間経過後に結果情報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。</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>(※)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。</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、漏えい・紛失のリスクに対応している。</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漏えい・紛失のリスクに対応している。</p> <p>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、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。</p>		

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 3) 課題が残されている	2) 十分である
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	<p><中間サーバー・ソフトウェアにおける措置></p> <p>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。</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提供許可証と情報照会者へと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。</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]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
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	<p><中間サーバー・ソフトウェアにおける措置></p> <p>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っている。</p> <p>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。</p> <p>(※)暗号化・復号機能と、鍵情報及び照会許可照合リストを管理する機能。</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、不適切な方法で提供されるリスクに対応している。</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漏えい・紛失のリスクに対応している。</p> <p>③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。</p>		
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 3) 課題が残されている	2) 十分である
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	<p><中間サーバー・ソフトウェアにおける措置></p> <p>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、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。</p> <p>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。</p> <p>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。</p> <p>(※)特定個人情報を副本として保存・管理する機能。</p>		
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 3) 課題が残されている	2) 十分である

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。

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	＜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出来るよう適切な入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。 ＜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。	

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	<p><越谷市における処置></p> <ul style="list-style-type: none"> ・コンピュータウイルス監視ソフトを導入している。また新種の不正プログラムに対応するために、ウイルスパターンファイルを定期的に更新している。 ・システムを利用できる職員を限定している。 ・ログインには生体認証を用いており、簡単になりすましができないよう制御している。 ・アクセスログや操作ログといった履歴を記録している。 <p><中間サーバー・プラットフォームにおける措置></p> <ol style="list-style-type: none"> 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、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><ガバメントクラウドにおける措置></p> <ol style="list-style-type: none"> 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ASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」(令和4年10月 デジタル庁。以下「利用基準」という。)に規定する「ASP」をいう。以下同じ。)又はガバメントクラウド運用管理補助者(利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。)はガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 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。 	
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	・死者の個人番号と生存する個人の個人番号とを分けて管理しないため、生存する個人の個人番号と同様の管理を行う。	
その他の措置の内容	-	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク2: 特定個人情報が古い情報のまま保管され続けるリスク	
リスクに対する措置の内容	・個人番号を含め宛名情報については、住民記録システムより、随時、異動データを連携することにより最新化する。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 特定個人情報が消去されずいつまでも存在するリスク	
消去手順	[定めている] <選択肢> 1) 定めている 2) 定めていない
手順の内容	<ul style="list-style-type: none"> ・各庁内連携システムの特定個人情報の保存期間等を考慮して、定期的に削除を実施することとしている。 ・紙や電子媒体は、特定個人情報の保存期間等を考慮して、定期的に削除を実施することとしている。 <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、NIST800-88、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	<p>[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</p>
具体的なチェック方法	<p><越谷市における措置> ・毎年、情報セキュリティに関連する意識調査を実施し、特定個人情報の保護に努めている。 ・毎年、維持管理点検により、特定個人情報の保存、アクセス記録、持ち出し履歴等について適切に取り扱っているかのチェックをしている。</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。</p>
②監査	<p>[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</p>
具体的な内容	<p><越谷市における措置> ・毎年、マイナンバーを含む個人情報の扱いについて、情報セキュリティを専門に扱う事業者と契約し、外部監査を実施している。</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。 ②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。</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。</p>
2. 従業者に対する教育・啓発	
従業者に対する教育・啓発	<p>[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</p>
具体的な方法	<p><越谷市における措置> ・毎年、情報セキュリティや個人情報(マイナンバーも含む)についての研修を受講している。また、受講できない職員については研修資料を回覧するなどの情報共有を図り、勉強の機会を与えている。</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実施している。</p>
3. 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、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>	

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	越谷市総務部総務課 住所：〒343-8501 埼玉県越谷市越ヶ谷四丁目2番1号 電話：048-963-9136
②請求方法	本人確認書類の提示および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。 ※電話及びFAXでの請求は、開示請求者が本人であることが十分に確認できないことから認めていない。
特記事項	任意の書式においても記載事項を網羅していれば、開示・訂正・利用停止請求を受け付ける。
③手数料等	<div style="text-align: right;"><選択肢></div> <div style="text-align: center;">[無料]</div> <div style="text-align: right;">1) 有料 2) 無料</div> <p>(手数料額、納付方法: 手数料は無料である。ただし、写しの交付を希望する場合は、写しの作成に要する費用を現金にて納付する。)</p>
④個人情報ファイル簿の公表	<div style="text-align: right;"><選択肢></div> <div style="text-align: center;">[行っている]</div> <div style="text-align: right;">1) 行っている 2) 行っていない</div>
個人情報ファイル名	新型インフルエンザ等対策特別措置法に基づく予防接種関係事務
公表場所	越谷市役所エントランス棟2階 行政資料コーナー
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	越谷市保健医療部健康づくり推進課 住所：〒343-0023 埼玉県越谷市東越谷十丁目31番地 電話：048-960-1100
②対応方法	受付票を作成し、問合せ内容・対応等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8年3月16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	「越谷市意見公募手続に関する要綱」に基づき、パブリックコメントによる意見公募を実施した。 【周知・公表】広報紙、越谷市ホームページ、所管課窓口・行政資料コーナー等にて周知・公表を行った。 【意見の提出】行政資料コーナー、各地区センターに設置するご意見箱。または電子申請、郵送、ファクス、メールにて意見書を提出。
②実施日・期間	令和6年10月12日から11月10日までの30日間
③期間を短縮する特段の理由	—
④主な意見の内容	意見の提出はなかった。
⑤評価書への反映	—
3. 第三者点検	
①実施日	令和7年1月10日
②方法	越谷市情報公開・個人情報保護審議会に諮問し、点検を実施した。
③結果	特定個人情報保護評価指針の審査の観点に照らし、適合性・妥当性ともに基準を満たしていると判断された。 なお、特定個人情報の漏えいその他の事態を発生させる多様なリスクについて、最小限にするための付加的な努力が求められるため、個人情報保護対策について更なる調査研究を重ね、適切な措置を講じて万全を期すとともに、特定個人情報の取扱いに当たっては、運用ルールに則って適切に対応するよう意見が付された。
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	

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16日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4. 特定個人情報ファイルの取扱いの委託 特定個人情報の提供ルール委託先から他者への提供に関するルール内容及びルール遵守の確認方法	越谷市個人情報取扱事務の委託に関する指針に基づき、越谷市の指示又は承諾があったときを除き、委託契約事務に係る個人情報を第三者に提供することを禁止している。また、必要に応じて委託先に対し報告を求める又は検査等を行う。	越谷市保有個人情報の適切な管理に関する指針に基づき、越谷市の指示又は承諾があったときを除き、委託契約事務に係る個人情報を第三者に提供することを禁止している。また、必要に応じて委託先に対し報告を求める又は検査等を行う。	事後	法改正に基づく軽微な修正
令和8年3月16日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4. 特定個人情報ファイルの取扱いの委託 特定個人情報の提供ルール委託元と委託先間の提供に関するルール内容及びルール遵守の確認方法	越谷市個人情報取扱事務の委託に関する指針に基づき、委託先に提供する際は、受託する事務を処理するために必要最小限のものとする。委託先の事業所内からの搬送は、越谷市の承諾があったときを除き、行ってはならない。なお、搬送の際は、従事者名簿に記載されている者が行う。	越谷市保有個人情報の適切な管理に関する指針に基づき、委託先に提供する際は、受託する事務を処理するために必要最小限のものとする。委託先の事業所内からの搬送は、越谷市の承諾があったときを除き、行ってはならない。なお、搬送の際は、従事者名簿に記載されている者が行う。	事後	法改正に基づく軽微な修正
令和8年3月16日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4. 特定個人情報ファイルの取扱いの委託 特定個人情報の消去ルールルールの内容及びルール遵守の確認方法	越谷市個人情報取扱事務の委託に関する指針に基づき、委託先は、委託契約が終了し、又は解除された場合は、契約事務に係る特定個人情報等を速やかに越谷市に返還し、又は越谷市の指示若しくは承諾があるときは、漏えいをきさない方法で確実に処分することを義務付けている。越谷市は、確実に処分したことについて、証明書等により確認するものとする。	越谷市保有個人情報の適切な管理に関する指針に基づき、委託先は、委託契約が終了し、又は解除された場合は、契約事務に係る特定個人情報等を速やかに越谷市に返還し、又は越谷市の指示若しくは承諾があるときは、漏えいをきさない方法で確実に処分することを義務付けている。越谷市は、確実に処分したことについて、証明書等により確認するものとする。	事後	法改正に基づく軽微な修正
令和8年3月16日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4. 特定個人情報ファイルの取扱いの委託 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程の内容	越谷市個人情報取扱事務の委託に関する指針に基づき、委託先における安全管理措置、秘密保持、厳重な保管及び搬送、再委託の制限、委託目的以外の利用等の禁止、複写及び複製の禁止、事故発生時の報告義務、委託契約終了時の個人情報の返還又は処分などを規定している。	越谷市保有個人情報の適切な管理に関する指針に、委託先における安全管理措置、秘密保持、厳重な保管及び搬送、再委託の制限、委託目的以外の利用等の禁止、複写及び複製の禁止、事故発生時の報告義務、委託契約終了時の個人情報の返還又は処分などを規定している。	事後	法改正に基づく軽微な修正
令和8年3月16日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク1: 目的外の入手が行われるリスク リスクに対する措置の内容	(※2)番号法別表第二及び第19号第14号に基づき、事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。	(※2)番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。	事後	法改正に基づく軽微な修正
令和8年3月16日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	<越谷市における処置> ・大部分のシステムについては、停電への備えや耐震性能を備えた強固なデータセンターへサーバを移設している。 ・庁内サーバ室、データセンターの出入口には生体認証による入退室管理設備を設置している。 ・庁内サーバ室へ入室可能な職員等を限定し、更には入退室管理簿の記入を徹底している。	<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出来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。	事前	標準化に伴う変更
令和8年3月16日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	-	<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ASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」(令和4年10月 デジタル庁。以下「利用基準」という。))に規定する「ASP」をいう。以下同じ。)又はガバメントクラウド運用管理補助者(利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。)はガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 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。	事前	標準化に伴う変更
令和8年3月16日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 リスク3: 特定個人情報は消去されずいつまでも存在するリスク 消去手順	-	・紙や電子媒体は、特定個人情報の保存期間等を考慮して、定期的に削除を実施することとしている。 <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、NIST800-88、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	標準化に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和8年3月16日	IV その他のリスク対策 1. 監査 ②監査 具体的な内容	—	<ガバメントクラウドにおける措置> ・ガバメントクラウドについては政府情報システムのセキュリティ制度 (ISMAP) のリストに登録されたクラウドサービスから調達することとしており、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。	事前	標準化に伴う変更
令和8年3月16日	IV その他のリスク対策 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。	事前	標準化に伴う変更
令和8年3月16日	V 開示請求、問合せ 1. 特定個人情報の開示・訂正・利用停止請求 ②請求方法	本人確認書類の提示および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。 ※電話、FAX及び郵送での請求は、開示請求者が本人であることが十分に確認できないことから認めていない。	本人確認書類の提示および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。 ※電話及びFAXでの請求は、開示請求者が本人であることが十分に確認できないことから認めていない。	事後	法改正に基づく軽微な修正
令和8年3月16日	V 開示請求、問合せ 1. 特定個人情報の開示・訂正・利用停止請求 ④個人情報ファイル簿の公表 公表場所	第二庁舎2階 情報公開センター	越谷市役所エントランス棟2階 行政資料コーナー	事後	軽微な修正
令和8年3月16日	VI 評価実施手続 1. 基礎項目評価 ①実施日	令和2年12月15日	令和8年3月16日	事前	評価の再実施に伴う変更
令和8年3月16日	VI 評価実施手続 2. 国民・住民等からの意見の聴取 ①方法	「越谷市意見公募手続に関する要綱」に基づき、パブリックコメントによる意見公募を実施した。 【周知・公表】広報紙、越谷市ホームページ、所管課窓口・情報公開センター等にて周知・公表を行った。 【意見の提出】郵便、FAX、電子メール又は所管課窓口・情報公開センター等にて意見(書)を提出する。	「越谷市意見公募手続に関する要綱」に基づき、パブリックコメントによる意見公募を実施した。 【周知・公表】広報紙、越谷市ホームページ、所管課窓口・行政資料コーナー等にて周知・公表を行った。 【意見の提出】行政資料コーナー、各地区センターに設置するご意見箱。または電子申請、郵送、ファクス、メールにて意見書を提出。	事前	評価の再実施に伴う変更
令和8年3月16日	VI 評価実施手続 2. 国民・住民等からの意見の聴取 ②実施日・期間	令和3年1月4日から2月3日までの30日間	令和6年10月12日から11月10日までの30日間	事前	評価の再実施に伴う変更
令和8年3月16日	VI 評価実施手続 3. 第三者点検 ①実施日 ③結果	令和3年5月11日 特定個人情報保護評価指針の審査の観点に照らし、適合性・妥当性ともに基準を満たしている」と判断された。 なお、特定個人情報の漏えいその他の事態を発生させる多様なリスクについて、最小限にするための付加的な努力が求められるため、個人情報保護対策について更なる調査研究を重ね、適切な措置を講じて万全を期すよう意見が付された。	令和7年1月10日 特定個人情報保護評価指針の審査の観点に照らし、適合性・妥当性ともに基準を満たしている」と判断された。 なお、特定個人情報の漏えいその他の事態を発生させる多様なリスクについて、最小限にするための付加的な努力が求められるため、個人情報保護対策について更なる調査研究を重ね、適切な措置を講じて万全を期すとともに、特定個人情報の取扱いに当たっては、運用ルールに則って適切に対応するよう意見が付された。	事後	再実施に伴う第三者点検結果の反映
令和8年3月16日	II 特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ①保管場所	<中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバー室への入室を厳重に管理する。 ②特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。	<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。	事前	中間サーバー更改に伴う修正

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16日	II 特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ③消去方法	<p><中間サーバー・プラットフォームにおける措置></p> <p>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。</p> <p>②ディスク交換やハード更改の際は、中間サーバー・プラットフォームの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。</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事業者及びクラウドサービス事業者が特定個人情報を消去することはない。</p> <p>②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。</p> <p>③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。</p>	事前	中間サーバー更改に伴う修正
令和8年3月16日	III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク4: 入手の際に特定個人情報情報が漏えい・紛失するリスク リスクに対する措置の内容	<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、漏えい・紛失のリスクに対応している。</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漏えい・紛失のリスクに対応している。</p> <p>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ない。</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、漏えい・紛失のリスクに対応している。</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漏えい・紛失のリスクに対応している。</p> <p>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、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。</p>	事前	中間サーバー更改に伴う修正
令和8年3月16日	III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク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	<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中間サーバーと統合宛名システム、情報提供ネットワークとの間は、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、安全性を担保している。</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担保している。</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っている。</p> <p>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制する仕組みになっている。</p> <p>(※)暗号化・復号機能と、鍵情報及び照会許可照会リストを管理する機能。</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、不適切な方法で提供されるリスクに対応している。</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漏えい・紛失のリスクに対応している。</p> <p>③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。</p>	事前	中間サーバー更改に伴う修正
令和8年3月16日	III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 情報提供ネットワークシステム及びそのリスクに対する措置	<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・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	中間サーバー更改に伴う修正

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16日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	<中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施設管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。	<中間サーバー・プラットフォームにおける措置> 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。	事前	中間サーバー更改に伴う修正
令和8年3月16日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損リスク ⑤技術的対策 具体的な対策の内容	<中間サーバー・プラットフォームにおける措置> 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。	<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。	事前	中間サーバー更改に伴う修正
令和8年3月16日	Ⅳ その他のリスク対策 1. 監査 ②監査 具体的な内容	<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、定期的に監査を実施している。	<中間サーバー・プラットフォームにおける措置> ①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。 ②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監査機関リストに登録された監査機関による監査を行うこととしている。	事前	中間サーバー更改に伴う修正
令和8年3月16日	Ⅳ その他のリスク対策 3. その他のリスク対策	<中間サーバー・プラットフォームにおける措置> ・中間サーバー・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理 (入退室管理等)、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。	<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、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。	事前	中間サーバー更改に伴う修正