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
19	健康増進事業に関する事務　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

刈谷市は、健康増進事業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	

評価実施機関名

刈谷市長

公表日

令和8年9月30日

［令和７年５月　様式3］

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	健康増進事業に関する事務
②事務の内容	健康増進法に基づき、歯周病検診、骨粗鬆症検診、肝炎ウイルス検診及びがん検診に関する事務を行い、以下の事務で特定個人情報を取り扱う。 （1）検診の対象者であるか否かの確認に関する事務 （2）検診等の実施に関する事務 （3）検診情報の記録管理等に関する事務
③対象人数	[　　10万人以上30万人未満　　] ＜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

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	番号連携システム
②システムの機能	既存システム及び中間サーバーと連携し、個人番号の管理並びに特定個人情報の照会及び提供等の業務を行う。 1　統合宛名番号管理機能 統合宛名番号・個人番号・宛名番号・5情報（住所、氏名、氏名の振り仮名、性別、生年月日）を紐付けて管理する機能 ※統合宛名番号とは、刈谷市において一意に個人を特定する団体内統合宛名番号をいう。 2　符号管理機能 符号取得要求を中間サーバーに対して行う機能 3　情報照会側機能 特定個人情報の照会業務を行うための機能 4　情報提供側機能 特定個人情報の提供業務を行うための機能 5　中間サーバー稼働状況確認機能 連携する中間サーバーの稼働状況を確認する機能 6　個人番号・統合宛名番号変換機能 個人番号を保有しない既存業務システムのために必要となる番号変換機能 7　データ連携機能 既存業務システムと中間サーバー間のデータ連携機能 8　データ変換機能 文字コード及びファイルフォーマットを変換する機能 9　操作者認証（ユーザー認証）・権限管理機能 番号連携システムの利用者を認証し、権限を管理する機能
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　　）
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	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)と番号連携システムとのデータの受け渡しを行うことで、符号の取得や各情報保有機関で保有する特定個人情報の照会及び各情報保有機関への情報提供等の業務を実現する。 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「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(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 3　情報提供機能 情報提供機能は、情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報(連携対象)の提供を行う機能 4　番号連携システム接続機能 中間サーバーと番号連携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機能 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 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 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(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 8　セキュリティ管理機能 電子証明書による接続デバイスの制御機能、情報提供NWS配信マスターによる情報の管理機能 9　操作者認証(ユーザー認証)・権限管理機能 中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報(連携対象)へのアクセス制御を行う機能 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	地域健康支援システム
②システムの機能	1　入力機能 対象者の管理、受信・実施内容の入力や管理 2　データ照会機能 受診・実施内容の確認 3　データ抽出機能 集計、統計資料作成のための受診・実施内容のデータ抽出
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
健診ファイル

4. 個人番号の利用 ※	
法令上の根拠	番号法別表の111の項
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	[　　実施する　　]　　＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	【情報提供の根拠】 番号法第19条第8号に基づく主務省令第2条の表139の項 【情報照会の根拠】 番号法第19条第8号に基づく主務省令第2条の表139の項
6. 評価実施機関における担当部署	
①部署	福祉健康部健康推進課
②所属長の役職名	健康推進課長
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		
健診ファイル		
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 ※		健康増進事業に基づく検診等の対象者
	その必要性	対象者及び受診・実施者に関する記録の適正な管理を図るため。住民の受診等に関する記録を正確かつ統一的に行い、住民の健康を増進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	識別情報：対象者を正確に特定するため必要 連絡先等情報：連絡先、住所等　健康診査等の通知書の送付先把握のため必要 医療保険関係情報：健康診査等対象者の把握のため必要。 健康・医療関係情報：健康診査等対象者の受診結果の把握・管理のため必要
	全ての記録項目	別添1を参照。
⑤保有開始日		平成28年1月1日
⑥事務担当部署		福祉健康部健康推進課　・　次世代育成部子育て支援課
3. 特定個人情報の入手・使用		
①入手元 ※		[○] 本人又は本人の代理人 [○] 評価実施機関内の他部署　（　市民課、国保年金課、税務課　） [　] 行政機関・独立行政法人等　（　） [　] 地方公共団体・地方独立行政法人　（　） [○] 民間事業者　（　刈谷市内医療機関及び歯科医療機関　） [　] 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使用目的 ※		健康増進事業に基づく健康診査等対象者を正確に把握し、管理するため
④使用の主体	使用部署	福祉健康部健康推進課 ・ 次世代育成部子育て支援課
	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
⑤使用方法		健康増進法に基づく健康診査、各種がん検診等の実施事務（対象者の抽出、通知、結果の管理）
	情報の突合	氏名、生年月日、個人コード、連絡先などにより本人を検索し、業務関連情報、受診票発行履歴を確認する。
⑥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 （　1）件
委託事項1		地域健康支援システムの開発・運用・保守
①委託内容		地域健康支援システムの開発・運用・保守に関すること
②委託先における取扱者数		[　10人以上50人未満　] ＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
③委託先名		トーテックアメニティ株式会社
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 （ 1 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	市区町村長
①法令上の根拠	番号法第19条第8号に基づく主務省令第2条の表139の項
②提供先における用途	健康増進事業に関する事務
③提供する情報	健診等情報
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	健診等受診者
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	随時
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[ ] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	[ ] 庁内連携システム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑦時期・頻度	
移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	

６．特定個人情報の保管・消去	
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、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

【個人情報】
1. 宛名番号、2. 世帯番号、3. カナ氏名、4. 漢字氏名、5. 通称カナ氏名、6. 通称氏名、7. 生年月日、8. 性別、9. 続柄、10. 異動事由、11. 異動日、12. 異動届出日、13. 住民になった事由、14. 住民になった異動日、15. 住民になった届出日、16. 住民でなくなった事由、17. 住民でなくなった異動日、18. 住民でなくなった届出日、19. 住民区分、20. 国籍、21. 転入前住所、22. 転出後住所、23. 郵便番号、24. 住所、25. 方書、26. DV情報、27. 国保資格情報、28. 個人及び世帯課税情報、29. 個人番号

【肺がん検診（一次）】
1. 受診年度、2. 受診日、3. 年齢、4. 検診方式、5. 実施医療機関、6. 喫煙指数、7. 胸部エックス線判定、8. 喀痰容器配布の有無、9. 喀痰細胞診判定、10. 総合指導区分、11. 受診番号、12. 電話番号、13. ハイリスク者かどうか、14. 取り込み連番、15. 取り込み日

【肺がん検診（精検）】
1. 受診年度、2. 受診日、3. 年齢、4. 実施医療機関、5. 検査結果、6. 組織型、7. 病期、8. 部位、9. 直接撮影実施の有無、10. CT実施の有無、11. 喀痰検査実施の有無、12. 細胞診実施の有無、13. 組織診実施の有無、14. 肺針生検法実施の有無、15. その他の検査実施の有無、16. 処置方針、17. 備考、18. 精検受診の有無の聞き取りメモ

【乳がん検診（一次）】
1. 受診年度、2. 受診日、3. 年齢、4. 検診方式、5. 実施医療機関、6. マンモグラフィ判定、7. 超音波所見、8. 超音波判定、9. 総合指導区分、10. 受診番号、11. 無料クーポン利用の有無、12. 電話番号、13. 取り込み連番、14. 取り込み日

【乳がん検診（精検）】
1. 受診年度、2. 受診日、3. 年齢、4. 実施医療機関、5. 検査結果、6. 組織型、7. 病期、8. マンモグラフィ実施の有無、9. 超音波実施の有無、10. 細胞診実施の有無、11. 組織診実施の有無、12. 処置方針、13. 備考、14. 精検受診の有無の聞き取りメモ

【胃がん検診（一次）】
1. 受診年度、2. 受診日、3. 年齢、4. 検診方式、5. 実施医療機関、6. 総合指導区分、7. X線判定結果、8. 内視鏡判定結果、9. 内視鏡生検受診の有無、10. 受診番号、11. 電話番号、12. 取り込み連番、13. 取り込み日

【胃がん検診（精検）】
1. 受診年度、2. 受診日、3. 年齢、4. 実施医療機関、5. 検査結果、6. 内視鏡検査実施の有無、7. 生検実施の有無、8. 直接X線撮影実施の有無、9. 処置方針、10. 備考、11. 精検受診の有無の聞き取りメモ

【子宮がん検診（一次）】
1. 受診年度、2. 受診日、3. 年齢、4. 検診方式、5. 実施医療機関、6. 検体の適否、7. 頚部ベセスダ判定、8. 頚部クラス判定、9. 体部判定、10. 総合指導区分、11. 無料クーポン利用の有無、12. 体部検査実施の有無、13. 電話番号、14. 取り込み連番、15. 取り込み日、16. 妊婦健診での子宮がん検診かどうか

【子宮がん検診（精検）】
1. 受診年度、2. 受診日、3. 年齢、4. 実施医療機関、5. コルポスコープ実施の有無、6. 細胞診実施の有無、7. 組織診実施の有無、8. HPV－DNAテスト実施の有無、9. その他の検査方法・内容、10. 検査結果、11. 扁平上皮病変の程度、12. 腺上皮病変の有無、13. 頸がん組織型、14. 頸がん進行期、15. 体がん組織型、16. 体がん進行期、17. 処置方針、18. 備考、19. 精検受診の有無の聞き取りメモ

【大腸がん検診（一次）】
1. 受診年度、2. 受診日、3. 年齢、4. 検診方式、5. 実施医療機関、6. 便潜血反応1日目、7. 便潜血反応2日目、8. 総合指導区分、9. 受診番号、10. 電話番号、11. 2本目提出日（別日の場合）、12. 取り込み日

【大腸がん検診（精検）】
1. 受診年度、2. 受診日、3. 年齢、4. 実施医療機関、5. 診断結果、6. 異常所見の診断名、7. 全大腸内視鏡検査実施の有無、8. 大腸CT検査実施の有無、9. S状結腸内視鏡検査実施の有無、10. 注腸X線検査実施の有無、11. 生検実施の有無、12. 異常所見の処置方針、13. 備考、14. 精検受診の有無の聞き取りメモ

（別添1）特定個人情報ファイル記録項目

【肝炎ウイルス検診（一次）】 ※精検情報はありません
1. 受診年度、2. 受診日、3. 年齢、4. 検診方式、5. 実施医療機関、6. B型判定結果（HBs抗原）、7. C型判定理由、8. C型検査理由、9. HCV抗体、10. HCV抗原、11. 取り込み日

【骨粗鬆症検診（一次）】
1. 受診年度、2. 受診日、3. 年齢、4. 検診方式、5. 実施医療機関、6. DXA検査骨量値、7. DXA検査測定部位、8. エックス線検査骨量値、9. エックス線検査判定、10. CT検査骨量値、11. CT検査判定、12. 超音波検査骨量値、13. 超音波検査判定、14. 総合指導区分、15. 同年平均、16. 最高平均、17. アキレススティフィネス、18. 電話番号、19. 骨密度

【骨粗鬆症検診（精検）】
1. 受診年度、2. 受診日、3. 年齢、4. 実施医療機関、5. 精密検査結果

【歯周疾患検診（一次）】
1. 受診年度、2. 受診日、3. 年齢、4. 検診方式、5. 実施医療機関、6. 健全歯数、7. 未処置歯数、8. 処置歯数、9. 現在歯数、10. 要補綴歯数、11. 欠損補綴歯数、12. 歯肉出血BOP、13. 歯周ポケットPD、14. 口腔清掃状態、15. 歯石の付着、16. その他の所見（歯列咬合、顎関節、粘膜）、17. 総合指導区分、18. 要指導内容、19. 要精密検査内容、20. 歯の健康づくり得点、21. 口腔粘膜などの異常の有無、22. 歯周組織などの異常の有無（X線骨吸）、23. 骨粗鬆症の疑いの有無（X線）、24. 紹介状発行状況、25. 補綴不要欠損歯数、26. パノラマ撮影の有無、27. 取り込み連番、28. 取り込み日

【歯周疾患検診（精検）】
1. 受診年度、2. 受診日、3. 年齢、4. 実施医療機関、5. 精密検査結果

Ⅲ　リスク対策　※（7. ②を除く。）

1. 特定個人情報ファイル名		
健診ファイル		
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:　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	1　対象者以外の情報の入手を防止するための措置 　氏名等を確認し、対象者以外の情報を入手しないように努めている。対象者以外の情報が含まれていた場合には、返却又は本来の提出先への回送処理等を行っている。 2　必要な情報以外を入手することを防止するための措置 　定められた仕様、帳票・データ様式に基づき入手するため、必要な情報以外は入手しないように努めている。	
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		
1　地域健康支援システムの端末は、権限を与えられたもののみが指紋による認証をした後に操作できる。 2　地域健康支援システムの端末の画面は、来庁者の目に触れないよう設置する。		
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		
リスクに対する措置の内容	健診情報を管理するデータベースと、住民情報を管理するデータベースを切り離して管理しており、データベース間の相互のアクセスができないようになっている。	
リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク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	1　対象業務システムを利用する端末は、指紋による認証を行っている。 2　対象業務システムを利用する職員を特定し、職員ごとに利用可能な機能を制御（アクセス制御）している。	
その他の措置の内容	スクリーンセーバを利用し、長時間にわたり情報を表示しない様にしている。	
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

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
1　窓口業務端末に、斜視防止フィルタ等を使用し、来庁者から見えないように設置する。 2　特定個人情報が表示された画面のハードコピーの取得は事務処理に必要となる範囲にとどめ、不要となった際はマスキング処理をし速やかに破棄する。

4. 特定個人情報ファイルの取扱いの委託	[　　]委託しない

リスク:　委託先における不正な使用等のリスク		
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	外部委託業者に発注する場合は、委託契約書に業務上知り得た秘密の公開の禁止を明記するとともに、目的外使用及び第三者への提供を禁止している。	
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担保	[　　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	再委託を原則禁止とし、やむを得ず再委託をする必要がある場合に限って、市の承諾を得て再委託ができることとしている。なお、許可した場合でも通常の委託と同様の措置を義務付ける。	
その他の措置の内容	事故が発生したときは、直ちに報告させるようにしている。	
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

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
1　特定個人情報ファイルの取扱いの記録 特定個人情報ファイルの受け渡しや廃棄の日にちや方法について、随時確認・記録を行う。

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	提供は、番号法に定められた事項にのみ行う。移転は、データ利用申請を求め、法的根拠が明らかな場合のみ行う。	
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

特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置

―

6．情報提供ネットワークシステムとの接続　　[　　]接続しない（入手）　　[　　]接続しない（提供）

リスク1：　目的外の入手が行われるリスク

リスクに対する措置の内容	＜中間サーバー・プラットフォームにおける措置＞ 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ほかに、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）番号法の規定に基づき事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。
リスクへの対策は十分か	[　　十分である　　]　＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

リスク2：不正な提供が行われるリスク

リスクに対する措置の内容	＜中間サーバー・ソフトウエアにおける措置＞ 1　情報提供機能（※）により、情報提供ネットワークシステムにおける照会許可用照合リストを情報提供ネットワークシステムから入手し、中間サーバーにも格納して情報提供機能により照会許可用照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 2　情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。 3　特に慎重な対応が求められる情報については、自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に送信内容を改めて確認し、提供を行うことでセンシティブな特定個人情報が不正に提供されるリスクに対応している。 4　中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能
リスクへの対策は十分か	[　　十分である　　]　＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

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・ソフトウエアにおける措置＞ 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　中間サーバーと番号連携システム、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・運営を行う事業者及びクラウドサービス事業者における情報漏洩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:　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
＜ガバメントクラウドにおける措置＞ ◆物理的対策 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。 ◆技術的対策 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及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。 ◆消去方法 ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。

8. 監査

実施の有無	[○] 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	1　評価書の記載内容通りの運用ができているかについて、年1回点検を行う。 2　職員に対して、情報セキュリティに関する教育を実施する。	

10. 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、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。

＜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。

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	〒448-0858　刈谷市若松町3丁目8番地2 刈谷市役所福祉健康部健康推進課（保健センター） 電話番号　0566-23-9559
②請求方法	個人情報の保護に関する法律第77条に基づき、必要事項を記載した開示請求書を提出する。
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	〒448-0858　刈谷市若松町3丁目8番地2 刈谷市役所福祉健康部健康推進課（保健センター） 電話番号　0566-23-9559
②対応方法	問合せの受付時に受付票を作成し、対応について記録を残す。

Ⅴ　評価実施手続

1. 基礎項目評価	
①実施日	令和8年9月30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6年4月1日	Ⅲ　リスク対策 8．監査	[　] 内部監査	[○] 内部監査	事後	
令和6年4月1日	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	〒448-0858　刈谷市若松町3丁目8番地2 刈谷市役所福祉健康部健康推進課（保健センター） 電話番号　0566-23-8877	〒448-0858　刈谷市若松町3丁目8番地2 刈谷市役所福祉健康部健康推進課（保健センター） 電話番号　0566-23-9559	事後	
令和6年4月1日	Ⅳ　開示請求、問合せ 1．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	〒448-0858　刈谷市若松町3丁目8番地2 刈谷市役所福祉健康部健康推進課（保健センター） 電話番号　0566-23-8877	〒448-0858　刈谷市若松町3丁目8番地2 刈谷市役所福祉健康部健康推進課（保健センター） 電話番号　0566-23-9559	事後	
令和6年12月9日	Ⅰ　基本情報 2．特定個人情報ファイルを取り扱う事務において使用するシステム	統合番号連携システム	番号連携システム	事前	
令和6年12月9日	Ⅰ　基本情報 2．特定個人情報ファイルを取り扱う事務において使用するシステム システム1 ②システムの機能	既存システム及び中間サーバーと連携し、個人番号の管理並びに特定個人情報の照会及び提供等の業務を行う。 1　統合番号管理機能 統合番号・個人番号・業務固有番号・4情報を紐付けて管理する機能 ※統合番号とは、刈谷市において一意に個人を特定する団体内統合宛名番号をいう。 2～5　略 6　個人番号・統合番号変換機能 個人番号を保有しない既存業務システムのために必要となる番号変換機能 7～9　略	既存システム及び中間サーバーと連携し、個人番号の管理並びに特定個人情報の照会及び提供等の業務を行う。 1　統合宛名番号管理機能 統合宛名番号・個人番号・宛名番号・4情報（住所、氏名、性別、生年月日）を紐付けて管理する機能 ※統合宛名番号とは、刈谷市において一意に個人を特定する団体内統合宛名番号をいう。 2～5　略 6　個人番号・統合宛名番号変換機能 個人番号を保有しない既存業務システムのために必要となる番号変換機能 7～9　略	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月9日	Ⅰ　基本情報 2．特定個人情報ファイルを取り扱う事務において使用するシステム システム2 ②システムの機能	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）と統合番号連携システムとのデータの受け渡しを行うことで、符号の取得や各情報保有機関で保有する特定個人情報の照会及び各情報保有機関への情報提供等の業務を実現する。 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「統合番号」とを紐付け、その情報を保管・管理する機能 2～3　略 4　統合番号連携システム接続機能 中間サーバーと統合番号連携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機能 5～10　略	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）と番号連携システムとのデータの受け渡しを行うことで、符号の取得や各情報保有機関で保有する特定個人情報の照会及び各情報保有機関への情報提供等の業務を実現する。 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「統合宛名番号」とを紐付け、その情報を保管・管理する機能 2～3　略 4　番号連携システム接続機能 中間サーバーと番号連携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機能 5～10　略	事前	
令和6年12月9日	Ⅰ　基本情報 4．個人番号の利用 法令上の根拠	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（以下「番号法」という。） 第9条第1項及び別表第1の76の項 2　行政手続における特定の個人を識別するための番号の利用等に関する法律別表第1の主務省令で 定める事務を定める命令第54条	行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「番号法」という。）別表の111の項	事後	
令和6年12月9日	Ⅰ　基本情報 5．情報提供ネットワークシステムによる情報連携 ②法令上の根拠	1　番号法第19条第8号及び別表第2 （1）別表第2における情報照会の根拠 102の2の項 （2）別表第2における情報提供の根拠 102の2の項 2　行政手続における特定の個人を識別するための番号の利用等に関する法律別表第2の主務省令 で定める事務及び情報を定める命令 （1）情報照会の根拠 第50条 （2）情報提供の根拠 第50条	【情報提供の根拠】 番号法第19条第8号に基づく主務省令第2条の表139の項 【情報照会の根拠】 番号法第19条第8号に基づく主務省令第2条の表139の項	事後	
令和6年12月9日	Ⅱ　特定個人情報ファイルの概要 5．特定個人情報の提供・移転（委託に伴うものを除く。） ①法令上の根拠	番号法第19条第8号	番号法第19条第8号に基づく主務省令第2条の表139の項	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月9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 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2及び第19条第14号に基づき事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。	(※2)番号法の規定に基づき事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。	事後	
令和6年12月9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	＜中間サーバー・ソフトウエアにおける措置＞ 略 ＜中間サーバー・プラットフォームにおける措置＞ 1　中間サーバーと統合番号連携システム、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。 2～4　略	＜中間サーバー・ソフトウエアにおける措置＞ 略 ＜中間サーバー・プラットフォームにおける措置＞ 1　中間サーバーと番号連携システム、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。 2～4　略	事前	
令和7年9月1日	Ⅰ　基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム1 ②システムの機能	既存システム及び中間サーバーと連携し、個人番号の管理並びに特定個人情報の照会及び提供等の業務を行う。 1　統合宛名番号管理機能 統合宛名番号・個人番号・宛名番号・4情報(住所、氏名、性別、生年月日)を紐付けて管理する機能 ※統合宛名番号とは、刈谷市において一意に個人を特定する団体内統合宛名番号をいう。 2～9　略	既存システム及び中間サーバーと連携し、個人番号の管理並びに特定個人情報の照会及び提供等の業務を行う。 1　統合宛名番号管理機能 統合宛名番号・個人番号・宛名番号・5情報(住所、氏名、氏名の振り仮名、性別、生年月日)を紐付けて管理する機能 ※統合宛名番号とは、刈谷市において一意に個人を特定する団体内統合宛名番号をいう。 2～9　略	事後	重要な変更に当たらない項目の変更であり事前の提出・公表が義務付けられない
令和7年9月1日	Ⅰ　基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム2 ②システムの機能	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)と統合番号連携システムとのデータの受け渡しを行うことで、符号の取得や各情報保有機関で保有する特定個人情報の照会及び各情報保有機関への情報提供等の業務を実現する。 1～7　略 8　セキュリティ管理機能 中間サーバーのシステム方式等の記載に沿って、対応予定 9～10　略	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)と統合番号連携システムとのデータの受け渡しを行うことで、符号の取得や各情報保有機関で保有する特定個人情報の照会及び各情報保有機関への情報提供等の業務を実現する。 1～7　略 8　セキュリティ管理機能 電子証明書による接続デバイスの制御機能、情報提供NWS配信マスターによる情報の管理機能 9～10　略	事後	重要な変更に当たらない項目の変更であり事前の提出・公表が義務付けられない
令和7年9月1日	Ⅰ　基本情報 4. 個人番号の利用 法令上の根拠	行政手続における特定の個人を識別するための番号の利用等に関する法律(以下「番号法」という。)別表の111の項	番号法別表の111の項	事後	重要な変更に当たらない項目の変更であり事前の提出・公表が義務付けられない

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年9月1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 保管場所	1　ICカード及びパスワードにて入退室管理を行っている管理区域に設置したサーバー内に保管している。 2～4　略	1　ICカード及びパスワードにて入退室管理を行っている管理区域に設置したサーバー内に保管している。 2～4　略 ＜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。	事後	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年9月1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	＜中間サーバー・ソフトウエアにおける措置＞ 略 ＜中間サーバー・プラットフォームにおける措置＞ 1～3　略 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・運営を行う事業者における情報漏洩等のリスクを極小化する。	＜中間サーバー・ソフトウエアにおける措置＞ 略 ＜中間サーバー・プラットフォームにおける措置＞ 1～3　略 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・運営を行う事業者及びクラウドサービス事業者における情報漏洩等のリスクを極小化する。	事後	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年9月1日	Ⅲ　リスク対策 10. 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、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。	事後	自治体中間サーバー・プラットフォーム更改に伴う変更

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9年3月23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 保管場所	1　ICカード及びパスワードにて入退室管理を行っている管理区域に設置したサーバー内に保管している。 2　紙媒体及び電子媒体により提出された申告情報等は、カギ付きの部屋で保管している。 3　サーバーへのアクセスはID/パスワードによる認証が必要になる。 4　バックアップはサーバー内のデータを庁外のデーターセンターに設置されたバックアップ用サーバーへデータを複写することで実現する。バックアップサーバーは施錠したサーバーラックに設置している。両拠点間の通信は第三者による不正アクセス等を排除するため、専用回線を使用している。 ＜中間サーバー・プラットフォームにおける措置＞ 略	＜中間サーバー・プラットフォームにおける措置＞ 略 ＜ガバメントクラウドにおける措置＞ 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。	事前	

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9年3月23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	―	＜ガバメントクラウドにおける措置＞ ◆物理的対策 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。 ◆技術的対策 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及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。 ◆消去方法 ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。	事前	

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9年3月23日	Ⅲ　リスク対策 10．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＞ 略	＜中間サーバー･プラットフォームにおける措置＞ 略 ＜ガバメントクラウドにおける措置＞ ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。 ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。 具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。	事前	