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
76	健康増進事業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	
栃木市は、健康増進事業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
栃木市長

公表日
令和8年4月1日

［令和6年10月　様式3］

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	健康増進事業の実施に関する事務
②事務の内容	健康増進法(平成十四年法律第百三号)による健康診査及びがん検診等の実施に関する事務であって主務省令で定めるものにかかる事務を行う。 ■対象となる検診(一次及び精密)の種類 ・胃がん検診 ・大腸がん検診 ・肺がん検診 ・子宮頸がん検診 ・乳がん検診 ・肝炎ウイルス検診 ・骨粗鬆症検診 ・歯周疾患検診 ■情報提供に必要な特定個人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して特定個人情報の照会と提供を行う。 ■健康診査及びがん検診等の実施に関する事務 具体的な事務内容については以下のとおり。 ①毎年、各検診の受診年齢到達者および検診対象者に対して、受診勧奨および個別通知等を送付する。 ②医療機関で実施した各検診(一次、精密)について、検診結果の情報を健康管理システムに入力し、データ管理を行う。 ③一次検診の結果、要精密検査と判定された者の内、精密検査未受診者に対し受診勧奨を行う。 ④番号法に基づいて、健康増進法による健康診査及びがん検診等の実施に関する事務において、情報提供ネットワークシステムに接続し、各情報保有機関が保有する特定個人情報について情報連携を行う。 ⑤特定保健指導の対象者把握
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	健康管理システム
②システムの機能	1. 検診対象者を抽出し、帳票等の発布を行う。 2. 検診結果をシステムに登録し、検診履歴の照会表示を行う。 3. 検診結果の通知および関連帳票の発行を行う。 4. 検診結果の集計およびデータ出力を行う。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[○] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [○] 宛名システム等　[　] 税務システム [　] その他　(　)
システム2～5	
システム2	
①システムの名称	統合宛名システム
②システムの機能	1. 宛名情報を照会する。 2. 住登外宛名情報を追加・消除・変更する。 3. 法人宛名情報を追加・消除・変更する。

③他のシステムとの接続	[○] 情報提供ネットワークシステム　[○] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[○] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [　] その他　（　）
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	＜中間サーバーの機能＞ 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」とを紐付け、その情報を保管・管理する。 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。 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。 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（連携対象）、符号取得のための情報等について連携する。 5. 情報提供等記録管理機能 特定個人情報(連携対象)の照会、又は提供があった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 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 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 特定個人情報(連携対象)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(インターフェイスシステム)から受信した情報提供NWS配信マスター情報を管理する。 9. 職員認証・権限管理機能 中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報(連携対象)へのアクセス制御を行う。 10. システム管理機能 バッチの状況管理、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。 11. 自己情報提供機能 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（連携情報）及び自己情報提供用添付ファイルの提供を行う。
③他のシステムとの接続	[○] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [○] 宛名システム等　[　] 税務システム [　] その他　（　）
システム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	
1. 健康増進事業ファイル（胃がん検診結果情報、肺がん検診結果情報、大腸がん結果情報、子宮頸がん結果情報、乳がん結果情報、肝炎ウイルス結果情報、骨粗鬆症結果情報、歯周疾患結果情報）	
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（平成二十五年法律第二十七号）（以下、番号法） ・第9条第1項　別表第111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（平成二十六年内閣府・総務省令第五号） ・第54条
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条の表第一欄（情報照会者）が「市町村長」の項のうち、第二欄（特定個人番号利用事務）に「健康増進法による健康増進事業の実施に関する事務」が含まれる項（139項） ■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条の表第三欄（情報提供者）が「市町村長」の項のうち、第四欄（利用特定個人情報）に「健康増進法による健康増進事業の実施に関する情報」が含まれる項が示す条文（第141条）
6. 評価実施機関における担当部署	
①部署	健康増進課
②所属長の役職名	健康増進課長
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	
1. 健康増進事業ファイル（胃がん検診結果情報、肺がん検診結果情報、大腸がん結果情報、子宮頸がん結果情報、乳がん結果情報、肝炎ウイルス結果情報、骨粗鬆症結果情報、歯周疾患結果情報）	
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 ※	健康増進法に基づく健康増進事業対象者
その必要性	健康増進事業の対象者管理および受診情報の管理を目的として、必要な範囲の特定個人情報を保有する
④記録される項目	[　　100項目以上　　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
主な記録項目 ※	・識別情報 [○] 個人番号　[　] 個人番号対応符号　[○] その他識別情報（内部番号） ・連絡先等情報 [○] 4情報（氏名、性別、生年月日、住所）　[○] 連絡先（電話番号等） [○] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[　] 地方税関係情報　[○] 健康・医療関係情報 [　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [　] その他　（　）
その妥当性	・個人番号及びその他識別情報：対象者を正確に特定するため ・4情報その他住民票関係情報：法廷記載項目の為 ・連絡先：本人への連絡等のため ・業務関係情報：法廷記載項目のため
全ての記録項目	別添1を参照。
⑤保有開始日	令和4年4月1日
⑥事務担当部署	健康増進課
3. 特定個人情報の入手・使用	
①入手元 ※	[○] 本人又は本人の代理人 [○] 評価実施機関内の他部署　（　） [○] 行政機関・独立行政法人等　（　） [○] 地方公共団体・地方独立行政法人　（　） [○] 民間事業者　（ 検診委託機関　） [　] 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 ※		健康増進事業の対象者を把握するため
④使用の主体	使用部署	健康増進課
	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
⑤使用方法		Ⅰ. 健康増進事業の対象者の選定、および必要な記録を作成する。 また、住民への各種通知(受診票等)や関係する機関への通知を出力する。 Ⅱ. 検診結果の登録を行う。 Ⅲ. 検診結果について情報提供ネットワークシステムを介して本人等への情報提供を行う。
	情報の突合	健康情報システムへの登録時に内部識別番号である宛名番号と住基情報を突合する。
⑥使用開始日		令和4年6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		システム保守業務
①委託内容		システム保守業務
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		(株)TKC
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	[ ] <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	
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	[ ] <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 ※	＜栃木市における措置＞ （庁内で保管） ・建物の入退館管理 ・サーバ室の入退室管理 ・サーバラックの鍵管理 （データセンターで保管） ・情報セキュリティマネジメントシステムの国際規格、ISO/IEC 27001に準拠したデータセンターにおいて保管している。 ・データセンターの扉の開閉にはICカードが必要で、特にサーバ室への入退室はバイオメトリクス認証の1つである手のひら静脈認証システムを採用している。 また、不正侵入を防止するため、窓ガラス破壊センサーや、立入に反応する赤外線センサー、監視カメラを装備している。 ＜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。 ＜ガバメントクラウドにおける措置＞ 【保管場所】 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。 【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。
7. 備考	

（別添1）特定個人情報ファイル記録項目

1.健康増進事業関係ファイル

【識別情報】
1.基本コード
【連絡先情報】
1.郵便番号、2.住所、3.方書、4.電話番号
【業務関係情報】
（共通管理項目）
1. 受診年度、2. 受診日、3. 受付番号、4. 実施区分（一次／精検）、5. 実施形態（集団／個別）、6. 受診医療機関、7. 費用区分、
8. 受診時年齢、9. 保険資格区分、10. 資格取得日、11. 保険者番号、12. 被保険者記号、13. 被保険者番号
（胃がん検診結果情報）
1. 過去の受診歴、2. 受診方法、3. 胃内視鏡検査所見、4. 胃内視鏡検査検査判定、5. 胃部エックス線検査所見、
6. 胃部エックス線検査検査判定、7. 精密検査の対象有無、8. 胃がんに係る症状の有無、9. その他所見
（肺がん検診結果情報）
1. 過去の受診歴、2. 喫煙指数、3. 受診方法、4. 喀痰検査受診日、5. 喀痰検査所見、6. 喀痰検査判定、7. 精密検査対象有無、
8. 胸部エックス線検査所見、9. 胸部エックス線検査判定、10. 肺がんに係る症状の有無、11. その他所見
（大腸がん検診結果情報）
1. 過去の受診歴、2. 受診方法、3. 便潜血検査所見、4. 便潜血検査判定、5. 精密検査の対象有無、6. 大腸がんに係る症状の有無、
7. その他所見
（子宮頸がん検診結果情報）
1. 過去の受診歴、2. 受診方法、3. 視診所見有無、4. 視診所見内容、5. 内診所見有無、6. 内診所見内容、7. 頸部細胞診検査所見、
8. 頸部細胞診検査判定、9. 精密検査の対象有無、10. 子宮頸がんに係る症状の有無、11. その他所見
（乳がん検診結果情報）
1. 過去の受診歴、2. 受診方法、3. マンモグラフィー検査所見、4. マンモグラフィー検査判定、5. 精密検査対象有無、
6. 乳がんに係る症状の有無、7. その他所見
（肝炎ウイルス検査結果情報）
1. 受診方法、2. 問診：妊娠・分娩時の多量出血の時期、3. 問診：妊娠・分娩時の多量出血歴の有無、
4. 問診：定期的な肝機能検査受診の有無、5. 問診：広範な外科的処置時期、6. 問診：広範な外科的処置歴の有無、
7. 問診：肝臓病歴、8. 問診：肝機能が悪いと言われた経験の有無、9. 問診：B型肝炎ウイルス検査の受診時期、
10. 問診：B型肝炎ウイルス検査の受診歴の有無、11. 問診：B型肝炎治療時期、12. 問診：B型肝炎治療歴の有無、
13. 問診：C型肝炎ウイルス検査の受診時期、14. 問診：C型肝炎ウイルス検査の受診歴の有無、15. 問診：C型肝炎治療時期、
16. 問診：C型肝炎治療歴の有無、17. B型肝炎ウイルス検査判定、18. C型肝炎ウイルス検査判定
（骨粗鬆症検診結果情報）
1. 受診方法、2. 問診：過去の検査判定、3. 問診：過去の精密検査の対象有無、4. 問診：飲酒量、5. 問診：喫煙習慣、
6. 問診：月経の有無、7. 問診：閉経年齢、8. 問診：閉経の理由、9. 問診：活動量（運動頻度）、10. 問診：現在の身長、
11. 問診：現在の体重、12. 問診：大腿骨近位部骨折の家族歴、13. 問診：過去の骨折の部位、14. 問診：ステロイド内服、
15. 問診：関節リウマチ罹患、16. 問診：骨折の既往歴、17. 問診：その他の既往歴、18. 問診：その他問診事項、
19. 検査測定部位、20. 検査所見、21. 検査骨量値、22. 検査判定、23. 精密検査結果、24. 判定
（歯周疾患検診結果情報）
1. 受診方法、2. 現在歯数、3. 健全歯数、4. 処置歯数、5. 未処置歯数、6. 喪失歯数、7. 要補綴歯数、8. 欠損補綴歯数、
9. 粘膜所見、10. 歯列咬合所見、11. 口腔清掃状態、12. 歯石の付着、13. 顎関節所見、14. 問診：喫煙歴、
15. 問診：1日の平均喫煙本数、16. 問診：喫煙を開始した年齢、17. 問診：喫煙を止めた年齢、18. 問診：歯をみがく頻度、
19. 問診：歯間ブラシやフロスの使用頻度、20. 問診：過去1年間の歯科検診の受診の有無、21. 問診：妊娠の有無、
22. 問診：狭心症・心筋梗塞・脳梗塞罹患の有無、23. 問診：糖尿病罹患の有無、24. 問診：関節リウマチ罹患の有無、
25. 問診：内臓脂肪型肥満の有無、26. 問診：その他全身の状態、27. 歯周ポケットPD、28. 歯肉出血BOP、
29. 精密検査所見、30. 精密検査結果、31. 判定区分、32. その他所見

2.中間サーバーで保有される特定個人情報（上記と重複する項目を除く）
情報提供用個人識別符号、団体内統合宛名番号等

Ⅲ　リスク対策　※（7. ②を除く。）

1. 特定個人情報ファイル名		
1. 健康増進事業ファイル（胃がん検診結果情報、肺がん検診結果情報、大腸がん結果情報、子宮頸がん結果情報、乳がん結果情報、肝炎ウイルス結果情報、骨粗鬆症結果情報、歯周疾患結果情報）		
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	健康管理システムは限られた端末のみ利用を可能とし、利用できる職員を限定する。さらに、ユーザーIDによる認証を行い、アクセス権を持たない職員のなりすましによる入手への対策を実施する。	
リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置		
3. 特定個人情報の使用		
リスク1:　目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク		
リスクに対する措置の内容	システムが必要とするデータベースのみアクセスできる構造になっており、その他の事務で使用するデータベースにはアクセスできないよう制御を行っている。	
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	システムを利用する必要がある職員を特定し、個人ごとにユーザーIDを割り当てるとともにIDとパスワードによる認証（又は生体認証など）認証を行っている。	
その他の措置の内容	・操作ログの記録を行う。 ・定期的に記録を確認し、不正アクセスがないか点検している。 ・サーバOSへのログインアクセス権管理 ・クライアントOSのログインID管理 ・システムへのログインID管理	
リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置

4. 特定個人情報ファイルの取扱いの委託	[　] 委託しない

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	契約書において、個人情報保護条例をはじめとする個人情報保護に関する法令並びに関連ガイドライン等の趣旨に従うことを定めている。	
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担保	[再委託していない]	＜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		
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: 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	番号法及び栃木市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、規定の範囲内において特定個人情報の移転を行う。	

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

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	＜健康管理システムのソフトウェアにおける措置＞ ①システムへのログイン時に、ログインが許可された利用者、利用端末のみが利用できるよう、認証を行っている。 ②情報照会機能は、許可された利用者、利用端末のみが利用できるよう、制御している。 ③システムが管理対象とする事務（手続き）のみを情報照会可能とするよう制御している。 ④システムへのログイン、ログアウト、情報照会を実施した際のログ（利用者、利用端末、利用日時）を記録している。 ＜健康管理システムの運用における措置＞ ①システムを利用可能な端末を制限し、ログインには2要素認証を用いている。 ②端末の操作ログを収集し、電子的記録媒体の利用制限を行っている。 ＜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）番号法第19条第14号及び、番号法第19条第8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。 ＜中間サーバーの運用における措置＞ ①中間サーバへログイン可能な端末を制限し、管理部署以外には中間サーバへ接続する端末を設置をしていない。 ②業務担当者は、業務システムを利用して情報照会等を行い、直接中間サーバへのアクセスを行っていない。
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	＜健康管理システムのソフトウェアにおける措置＞ ①システムへのログイン時に、ログインが許可された利用者、利用端末のみが利用できるよう、認証を行っている。 ②副本登録、情報提供機能は、許可された利用者、利用端末のみが利用できるよう、制御している。 ③システムが管理対象とする特定個人情報（データセットレコード）のみを副本登録、情報提供可能とするよう制御している。 ④システムへのログイン、ログアウト、副本登録、情報提供を実施した際のログ（利用者、利用端末、利用日時）を記録している。 ＜健康管理システムの運用における措置＞ ①システムを利用可能な端末を制限し、ログインには2要素認証を用いている。 ②端末の操作ログを収集し、電子的記録媒体の利用制限を行っている。 ＜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。 ＜中間サーバーの運用における措置＞ ①中間サーバへログイン可能な端末を制限し、管理部署以外には中間サーバへ接続する端末を設置をしていない。 ②業務担当者は、業務システムを利用して情報提供等を行い、直接中間サーバへのアクセスを行っていない。
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

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
■安全が保たれない方法によって入手が行われるリスク ＜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、総務大臣が設置・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。 ■入手した特定個人情報が不正確であるリスク ＜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、総務大臣が設置・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。 ■入手の際に特定個人情報が漏えい・紛失するリスク ＜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。

■不適切な方法で提供されるリスク
＜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。

■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
＜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。

■その他のリスク
＜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: 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	＜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」（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。	
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＞ 【消去手順】 データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。

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	栃木市における措置 ・職員に対し、個人情報保護に関する研修等を実施する。 ・違反行為を行ったものに対しては、その都度指導の上、違反行為の程度によっては懲戒の対象となりうる。

10. 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。

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	栃木市役所　保健福祉部　健康増進課　住所：栃木県栃木市今泉町2丁目1番40号　電話0282-25-3511
②請求方法	指定様式による書面の提出により、開示・請求・利用停止の請求を受け付ける。
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	栃木市役所　保健福祉部　健康増進課　住所：栃木県栃木市今泉町2丁目1番40号　電話0282-25-3511
②対応方法	問い合わせ受付時に、受付票を起票し、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5年3月31日	V評価実施手続き 1.基礎項目評価	2022/4/1	2023/3/1	事前	
令和6年3月31日	V評価実施手続き 1.基礎項目評価	2023/3/1	2024/3/1	事前	
令和7年4月1日	Ⅰ 基本情報 1．特定個人情報ファイルを取り扱う事務 ②事務の内容	健康増進法(平成十四年法律第百三号)による健康診査及びがん検診等の実施に関する事務であって主務省令で定めるものにかかる事務を行う。 ■対象となる検診(一次及び精密)の種類 ・胃がん検診 ・大腸がん検診 ・肺がん検診 ・子宮頸がん検診 ・乳がん検診 ・肝炎ウイルス検診 ・骨粗鬆症検診 ・歯周疾患検診 ■情報提供に必要な特定個人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して特定個人情報の照会と提供を行う。 ■健康診査及びがん検診等の実施に関する事務 具体的な事務内容については以下のとおり。 ①毎年、各検診の受診年齢到達者および検診対象者に対して、受診勧奨および個別通知等を送付する。 ②医療機関で実施した各検診(一次、精密)について、検診結果の情報を健康管理システムに入力し、データ管理を行う。 ③一次検診の結果、要精密検査と判定された者の内、精密検査未受診者に対し受診勧奨を行う。 ④番号法の別表第二に基づいて、健康増進法による健康診査及びがん検診等の実施に関する事務において、情報提供ネットワークシステムに接続し、各情報保有機関が保有する特定個人情報について情報連携を行う。 ⑤特定保健指導の対象者把握	健康増進法(平成十四年法律第百三号)による健康診査及びがん検診等の実施に関する事務であって主務省令で定めるものにかかる事務を行う。 ■対象となる検診(一次及び精密)の種類 ・胃がん検診 ・大腸がん検診 ・肺がん検診 ・子宮頸がん検診 ・乳がん検診 ・肝炎ウイルス検診 ・骨粗鬆症検診 ・歯周疾患検診 ■情報提供に必要な特定個人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して特定個人情報の照会と提供を行う。 ■健康診査及びがん検診等の実施に関する事務 具体的な事務内容については以下のとおり。 ①毎年、各検診の受診年齢到達者および検診対象者に対して、受診勧奨および個別通知等を送付する。 ②医療機関で実施した各検診(一次、精密)について、検診結果の情報を健康管理システムに入力し、データ管理を行う。 ③一次検診の結果、要精密検査と判定された者の内、精密検査未受診者に対し受診勧奨を行う。 ④番号法に基づいて、健康増進法による健康診査及びがん検診等の実施に関する事務において、情報提供ネットワークシステムに接続し、各情報保有機関が保有する特定個人情報について情報連携を行う。 ⑤特定保健指導の対象者把握	事前	
令和7年4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（平成二十五年五月三十一日法律第二十七号）第9条第1項、別表第一の第76項 並びに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一の主務省令で定める事務を定める命令(平成二十六年九月十日内閣府・総務省令第五号）　第54条	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（平成二十五年法律第二十七号）（以下、番号法） ・第9条第1項　別表第111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（平成二十六年内閣府・総務省令第五号） ・第54条	事前	
令和7年4月1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	■情報提供の根拠 ・番号法第19条第7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「健康増進法による健康増進事業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（102の2の項） （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50条）（※別表第二の102の2の項） ■情報照会の根拠 ・番号法第19条第7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「健康増進法による健康増進事業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（102の2の項） （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50条）（※別表第二の102の2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条の表第一欄（情報照会者）が「市町村長」の項のうち、第二欄（特定個人番号利用事務）に「健康増進法による健康増進事業の実施に関する事務」が含まれる項（139項） ■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条の表第三欄（情報提供者）が「市町村長」の項のうち、第四欄（利用特定個人情報）に「健康増進法による健康増進事業の実施に関する情報」が含まれる項が示す条文（第141条）	事前	

令和7年4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	＜栃木市における措置＞ （庁内で保管） ・建物の入退館管理 ・サーバ室の入退室管理 ・サーバラックの鍵管理 （データセンターで保管） ・情報セキュリティマネジメントシステムの国際規格、ISO/IEC 27001に準拠したデータセンターにおいて保管している。 ・データセンターの扉の開閉にはICカードが必要で、特にサーバ室への入退室はバイオメトリクス認証の1つである手のひら静脈認証システムを採用している。 また、不正侵入を防止するため、窓ガラス破壊センサーや、立入に反応する赤外線センサー、監視カメラを装備している。 ＜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。	＜栃木市における措置＞ （庁内で保管） ・建物の入退館管理 ・サーバ室の入退室管理 ・サーバラックの鍵管理 （データセンターで保管） ・情報セキュリティマネジメントシステムの国際規格、ISO/IEC 27001に準拠したデータセンターにおいて保管している。 ・データセンターの扉の開閉にはICカードが必要で、特にサーバ室への入退室はバイオメトリクス認証の1つである手のひら静脈認証システムを採用している。 また、不正侵入を防止するため、窓ガラス破壊センサーや、立入に反応する赤外線センサー、監視カメラを装備している。 ＜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。 ＜ガバメントクラウドにおける措置＞ 【保管場所】 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。 【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	
令和7年4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 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	＜健康管理システムのソフトウェアにおける措置＞ ①システムへのログイン時に、ログインが許可された利用者、利用端末のみが利用できるよう、認証を行っている。 ②情報照会機能は、許可された利用者、利用端末のみが利用できるよう、制御している。 ③システムが管理対象とする事務（手続き）のみを情報照会可能とするよう制御している。 ④システムへのログイン、ログアウト、情報照会を実施した際のログ（利用者、利用端末、利用日時）を記録している。 ＜健康管理システムの運用における措置＞ ①システムを利用可能な端末を制限し、ログインには2要素認証を用いている。 ②端末の操作ログを収集し、電子的記録媒体の利用制限を行っている。 ＜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）番号法別表第2及び第19条第8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。 ＜中間サーバーの運用における措置＞ ①中間サーバへログイン可能な端末を制限し、管理部署以外には中間サーバへ接続する端末を設置をしていない。 ②業務担当者は、業務システムを利用して情報照会等を行い、直接中間サーバへのアクセスを行っていない。	＜健康管理システムのソフトウェアにおける措置＞ ①システムへのログイン時に、ログインが許可された利用者、利用端末のみが利用できるよう、認証を行っている。 ②情報照会機能は、許可された利用者、利用端末のみが利用できるよう、制御している。 ③システムが管理対象とする事務（手続き）のみを情報照会可能とするよう制御している。 ④システムへのログイン、ログアウト、情報照会を実施した際のログ（利用者、利用端末、利用日時）を記録している。 ＜健康管理システムの運用における措置＞ ①システムを利用可能な端末を制限し、ログインには2要素認証を用いている。 ②端末の操作ログを収集し、電子的記録媒体の利用制限を行っている。 ＜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）番号法第19条第14号及び、番号法第19条第8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。 ＜中間サーバーの運用における措置＞ ①中間サーバへログイン可能な端末を制限し、管理部署以外には中間サーバへ接続する端末を設置をしていない。 ②業務担当者は、業務システムを利用して情報照会等を行い、直接中間サーバへのアクセスを行っていない。	事前	

令和7年4月1日	Ⅲ　リスク対策 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 その他の措置の内容	－	＜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」（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。	事前	
令和7年4月1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＞ 【消去手順】 データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。	事前	
令和7年4月1日	Ⅲ　リスク対策 10.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	
令和7年4月1日	Ⅴ評価実施手続 1．基礎項目評価 ①実施日	令和6年3月1日	令和7年3月1日	事前	
令和8年3月31日	Ⅱ　特定個人情報ファイルの概要 3.特定個人情報の入手・使用 ④使用の主体 　使用者数	50人以上100人未満	10人以上50人未満	事前	
令和8年3月31日	Ⅴ評価実施手続 1．基礎項目評価 ①実施日	R7.3.1	R8.3.1	事前	