

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
21	健康増進法による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

ひたちなか市は、健康増進法による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

ひたちなか市長

公表日

令和7年4月15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	健康増進法による健康増進事業に関する事務
②事務の内容	ひたちなか市は、健康増進法(平成14年法律第103号。以下「法」という。)に基づき、健康増進事業の実施に関する事務を行っている。 これらの事務のうち、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25年法律第27号。以下「番号法」という。)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)に基づき、特定個人情報ファイルを取り扱い、かつ、基礎項目評価書の作成を行う必要のある事務は、次に掲げるものとする。 1 法第17条第1項に規定する栄養指導及び保健指導の実施に関する事務 2 法第19条の2の規定による健康増進事業の実施に関する事務
③対象人数	＜選択肢＞ [10万人以上30万人未満] 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. 住基等情報確認機能 健(検)診対象者の4情報(氏名、性別、生年月日、住所)・健(検)診履歴を確認する。 2. 健(検)診管理 受診希望者は、各自集団又は個別健診を選択し、市指定の健診実施機関で受診する。受診後ひたちなか市は、健診機関から報告された健診結果を入力する。また過去の受診者の受診状況や健(検)診結果を管理し保健業務に利用する。 3. 登録及び予約 登録の必要な健(検)診(骨粗しょう症検診・国保以外の健(検)診)の登録管理や予約管理を行う。 4. 発行 受診時に必要な「健(検)診受診券」の発行を行う。 5. 宛名管理 受診券宛名欄の作成 6. 抽出 各健(検)診受診者や申込者等の対象者の抽出を行う。	
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 ☐ 住民基本台帳ネットワークシステム ☒ 宛名システム等 ☐ その他（	☐ 庁内連携システム ☐ 既存住民基本台帳システム ☐ 税務システム ）

システム2～5

システム2

①システムの名称	宛名管理システム
②システムの機能	1. 宛名管理機能 住民記録システムより情報移転を行い4情報(氏名、性別、生年月日、住所)、その他住民票関係情報を記録する。住登外者の宛名項目(氏名及び名称、性別、生年月日、住所など)の作成・管理をする。 2. 個人番号の保護機能 個人番号の保護を行うため認証の制御や暗号化をする。 3. 宛名連携機能 同一人の宛名番号を紐付する機能を有し、宛名番号の関連付けしたデータを作成・管理する。中間サーバーとの連携時には、紐付した宛名番号から団体内宛名番号を取得する。 4. 団体内宛名統合機能 提供を行うため税務システム等から提供するデータを受け、中間サーバーへ送信する。情報の照会を行うため税務システム等からの要求情報を受け、中間サーバーへ送信し結果を受信する。符号付番の際に符号と紐付ける団体内統合宛名番号を中間サーバーへ送信する。団体内宛名番号と4情報(氏名、性別、生年月日、住所)を管理し、中間サーバーからの要求に対応する。 5. 中間サーバー連携機能 中間サーバーと連携し、必要に応じてデータの連携を行う。データの連携を行うことで、結果の情報を取得し、住民記録システムに反映させる。

	中間サーバーとの連携によりデータの送信・受信を行う。データの送信・受信を行うに結果の情報を取得・管理する。
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	1. 符号管理機能 符号管理機能は情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」とを紐付け、その情報を保管・管理する 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 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 4. 既存システム接続機能 中間サーバーと既存システム、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 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 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 バッチ処理の状況管理、業務統計情報の集計、稼働状態の通知、保管切れ情報の削除を行う
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4	
①システムの名称	EUCシステム
②システムの機能	1. データ抽出・出力機能 基本データリストを利用し、任意の抽出条件に該当する情報をCSV形式で出力する機能。 2. 認証権限管理機能 職員の認証及び付与された権限に基づき、機能や基本データリストへのアクセス制限を行う機能 3. ログ管理機能 抽出を行った日時・条件及び操作ログを保管する機能
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 (同一パッケージシステム)
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	
住民健診ファイル	
4. 個人番号の利用 ※	
法令上の根拠	・番号法第9条第1項 別表の111の項 ・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	(特定個人情報の照会) ・番号法第19条第8号 ・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(令和6年デジタル庁・総務省令第9号)第2条の表の139の項及び第141条 (特定個人情報の提供) ・番号法第19条第8号 ・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139の項及び第141条
6. 評価実施機関における担当部署	
①部署	保健福祉部健康推進課
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	
住民健診ファイル	
2. 基本情報	
①ファイルの種類 ※	システム用ファイル ☐ システム用ファイル ☐ 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 ☐ 1万人未満 ☐ 1万人以上10万人未満 ☐ 10万人以上100万人未満 ☐ 100万人以上1,000万人未満 ☐ 1,000万人以上
③対象となる本人の範囲 ※	本市の区域内に居住する18歳以上の者
その必要性	適正な国民健康保険事務を行うために、対象となる特定個人情報が必要
④記録される項目	50項目以上100項目未満 ☐ 10項目未満 ☐ 10項目以上50項目未満 ☐ 50項目以上100項目未満 ☐ 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	○識別情報:対象者を特定するために記録 ○連絡先情報:対象者を正確に把握するために保有 ○健康・医療関係情報:健(検)診の受診勧奨及び受診結果の管理を行うため保有する。
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
⑥事務担当部署	保健福祉部健康推進課

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 (他の市区町村) ☐ 民間事業者 () ☐ その他 ()
②入手方法		☒ 紙 [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ ☐ 電子メール [] 専用線 [] 庁内連携システム ☒ 情報提供ネットワークシステム ☐ その他 ()
③使用目的 ※		健康増進事業の実施
④使用の主体	使用部署	保健福祉部健康推進課
	使用者数	[50人以上100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		1. 届出・申請の受付に関する事務 各種健診の届出・申請の受付後、基幹システムより対象者の受診券を発行する。 2. 審査・認定に関する事務 健康相談や健康教育対象者を健康・医療関係情報により審査し、必要に応じた事後対応を行う。 3. 台帳管理に関する事務 健康増進事業の受診者台帳を作成し、受診情報等を管理する。
	情報の突合	入手した情報と本市所管の特定個人情報を突合する
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 (3) 件
委託事項1		システムの運用・保守
①委託内容		システムの運用・保守業務, 法制度改正に伴う改修作業
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		株式会社茨城計算センター
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2		バックアップシステムの構築
①委託内容		システム障害に備えた代替システムの構築
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		株式会社茨城計算センター
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3		遠隔地保管
①委託内容		特定個人情報データの滅失等に備えたバックアップデータの保管委託
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		株式会社茨城計算センター
再委託	④再委託の有無 ※	再委託する <選択肢> 1) 再委託する 2) 再委託しない
	⑤再委託の許諾方法	委託先から, 再委託の必要性, 再委託先の委託管理方法, 再委託先の名称, 代表者及び所在地, 再委託する業務内容, 再委託する業務に含まれる情報の種類, 再委託先のセキュリティ管理体制の申請を受け, 許諾を判断している。
	⑥再委託事項	バックアップデータの管理
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	
保管場所 ※	＜ひたちなか市における措置＞ ①特定個人情報が保管されているサーバは電子錠がかけられたサーバ室に設置しており、サーバ室への入退室を厳重に管理する。 ②サーバへアクセスするためには、IDとパスワードによる認証が必要となる。 ＜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】 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
7. 備考	

(別添1) 特定個人情報ファイル記録項目

【住民健診情報】

1. 宛名番号, 2. 年度, 3. 申込日時, 4. 申請方法, 5. 希望受診機関, 6. 開始時間, 7. 終了時間, 8. 検査区分, 9. クーポン, 10. 検診方法, 11. 検診料金, 12. 受診日, 13. 受診番号, 14. 受診機関, 15. 受診歴, 16. 検査方法, 17. 所見, 18. 所見別判定, 19. 結果, 20. 総合判定, 21. 精検受診日, 22. 精検番号, 23. 精検受診機関, 24. 精検事後指導, 25. 精検検査方法1, 26. 精検検査方法2, 27. 精検検査方法3, 28. 精検所見1, 29. 精検所見2, 30. 精検所見3, 31. 精検所見4, 32. 精検所見5, 33. 精検判定, 34. 精検がん病期, 35. 精検部位1(がん組織), 36. 精検部位2(がん組織), 37. 精検部位3(がん組織), 38. 原発性, 39. 偶発症

【宛名情報】

1. 個人番号 2. 宛名番号 3. 宛先区分 4. 宛先名カナ 5. 宛先名漢字 6. 性別 7. 生年月日 8. 続柄コード 9. 郵便番号 10. 住所コード 11. 住所カナ 12. 番地カナ 13. 方書カナ 14. 様方カナ 15. 住所漢字 16. 番地漢字 17. 方書漢字 18. 様方漢字 19. 世帯処理番号 20. 行政区 21. 住定日 22. 住定事由 23. 住民となった日 24. 住民となった事由 25. 消除日 26. 消除事由 27. 転出予定日 28. 転出確定日 29. 異動日 30. 送付先宛先名 31. 送付先住所 32. 電話番号

Ⅲ リスク対策 ※(7. ②を除く。)

1. 特定個人情報ファイル名	
住民健診ファイル	
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	・市民等からの個人情報の入手については、本人の個人番号カード又は通知カード、身分証明書の提示や窓口での聞き取りにより本人確認を行い、対象者であることを確認する。 ・申請書類等は、必要な情報のみを記載する様式としており、また、記載要領を提示し、必要な情報以外は記載しないようにしている。 ・他団体からの個人情報の入手については、1件ごとに住所・氏名等の情報により当該事務の対象者と合致するかを確認している。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	
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	
リスクに対する措置の内容	健康管理システムからは、事務に必要なファイルのみにアクセスし、必要のない情報にアクセスしないように制御を行っている。
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	システムを使用可能な職員を特定し、アクセス権限の制御を行っている。 認証カードにより、操作者の認証を行う。
その他の措置の内容	・システムの操作履歴（操作ログ）を記録している。 ・個人ごとにシステムの操作範囲権限の設定を行っている。 ・端末を利用していない際は、システムからログオフする。
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	・機密の保持 ・目的外利用及び提供の禁止 ・複写等の禁止 ・許可のない再委託の禁止	
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	契約書には、原則として、再委託の禁止を定めている。但し、書面により本市が承諾した場合には、委託先と同等の守秘義務及び監督義務を負わせることとしている。	
その他の措置の内容		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
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 ・執務室の外へ特定個人情報ファイルを持ち出す場合は、所属長の許可を得るとともに持ち出し状況を記録することを定めている。 ・特定個人情報ファイルの管理状況について、定期及びその他必要があると認められる場合には随時に監査を行っている。			
その他の措置の内容	サーバ室等への入室及び本特定個人情報ファイルを扱うシステムへのアクセス権限を有する者を厳格に管理し、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			
<不適切な方法で提供・移転が行われるリスクへの措置> 不正なアクセスに対してアクセスを許可していない。 指定した端末、アクセスルートでのみ提供・移転できる制御を行っている。 予め定められた方法でのみ情報の提供・移転を行う。 <誤った情報を提供・移転してしまうリスクへの措置> システムにより、指定された条件に基づき得られた情報を提供できる制御を行っている。 <誤った相手に提供・移転してしまうリスクへの措置> 情報の移転を行う相手先について、システムでの接続制御を行っている。			

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・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。 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)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。		
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、中間サーバーにも格納して、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。 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	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 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	【中間サーバー・プラットフォームにおける物理的措置】 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、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 【中間サーバー・プラットフォームにおける技術的措置】 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。 ＜ガバメントクラウドにおける措置＞ 【保管：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。 【保管：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ガバメントクラウドASP、ガバメントクラウド運用管理補助者は、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ガバメントクラウドASP、ガバメントクラウド運用管理補助者は、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、ガバメントクラウドASP、ガバメントクラウド運用管理補助者の各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業務データには、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】
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	

8. 監査	
実施の有無	☐ 〇 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 ☐ 十分に行っていない ☐ 十分に行っていない
具体的な方法	・職員及び事業所内派遣者に対しては、個人情報保護に関する研修の受講を義務付けている。 ・委託事業者に対しては、秘密保持契約を締結し、その中で個人情報保護に関する研修を義務付けている。 ・違反行為を行った者に対しては、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。 ＜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こととしている。 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。
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、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リテラシー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。 ・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及びガバメントクラウド運用管理責任者が責任を有する。 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及びガバメントクラウド運用管理責任者が対応するものとする。	

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	総務部総務課 茨城県ひたちなか市東石川2丁目10番1号 029-273-0111
②請求方法	指定様式による書面の提出により、開示・訂正・削除・目的外利用の中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	保健福祉部健康推進課 茨城県ひたちなか市松戸町1丁目14番1号 029-276-5222
②対応方法	問合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6年4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6年4月2日	I 基本情報 6. 評価実施機関における担当部署 ①部署	福祉部健康推進課	保健福祉部健康推進課	事後	
令和6年4月2日	II 特定個人情報ファイルの概要 2. 基本情報 ⑥事務担当部署	福祉部健康推進課	保健福祉部健康推進課	事後	
令和6年4月2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・利用部署	福祉部健康推進課	保健福祉部健康推進課	事後	
令和6年4月2日	IV 開示請求・問合せ 2. 特定個人情報ファイルの取り扱いに関する問合せ ①連絡先	福祉部健康推進課 茨城県ひたちなか市ひたちなか市松戸町1丁目14番1号 029-276-5222	保健福祉部健康推進課 茨城県ひたちなか市ひたちなか市松戸町1丁目14番1号 029-276-5222	事後	
令和6年4月2日	V 評価実施手続き 1. 基礎項目評価 ①実施日	2021/4/1	2023/4/1	事後	
令和7年3月31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	ひたちなか市は、健康増進法(平成14年法律第103号。以下「法」という。)に基づき、健康増進事業の実施に関する事務を行っている。これらの事務のうち、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25年法律第27号。以下「番号法」という。)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別表第一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)に基づき、特定個人情報ファイルを取り扱い、かつ、基礎項目評価書の作成を行う必要のある事務は、次に掲げるものとする。 1 法第17条第1項に規定する栄養指導及び保健指導の実施に関する事務 2 法第19条の2の規定による健康増進事業の実施に関する事務	ひたちなか市は、健康増進法(平成14年法律第103号。以下「法」という。)に基づき、健康増進事業の実施に関する事務を行っている。これらの事務のうち、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25年法律第27号。以下「番号法」という。)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別表第一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)に基づき、特定個人情報ファイルを取り扱い、かつ、基礎項目評価書の作成を行う必要のある事務は、次に掲げるものとする。 1 法第17条第1項に規定する栄養指導及び保健指導の実施に関する事務 2 法第19条の2の規定による健康増進事業の実施に関する事務	事後	
令和7年3月31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4 ①システムの名称		EUCシステム	事後	
令和7年3月31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4 ②システムの機能		1. テータ抽出・出力機能 基本データリストを利用し、任意の抽出条件に該当する情報をCSV形式で出力する機能。 2. 認証権限管理機能 職員の認証及び付与された権限に基づき、機能や基本データリストへのアクセス制限を行う機能 3. ログ管理機能 抽出を行った日時・条件及び操作ログを保管する機能	事後	
令和7年3月31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4 ③他のシステムとの接続		その他(同一パッケージシステム)	事後	
令和7年3月31日	I 基本情報 4. 個人情報の利用 法令上の根拠	・番号法第9条第1項 別表第1の76の項 ・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第54条	・番号法第9条第1項 別表の111の項 ・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第54条	事後	
令和7年3月31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	(特定個人情報の照会) ・番号法第19条第8号 別表第2の102の2の項 ・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二の主務省令で定める事務及び情報を定める命令(平成26年内閣府・総務省令第7号)第50条 (特定個人情報の提供) ・番号法第19条第8号 別表第2の102の2の項 ・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二の主務省令で定める事務及び情報を定める命令第50条	(特定個人情報の照会) ・番号法第19条第8号 ・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(令和6年デジタル庁・総務省令第9号)第2条の表の139の項及び第141条 (特定個人情報の提供) ・番号法第19条第8号 ・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139の項及び第141条	事後	
令和7年3月31日	II 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託	システムの管理運用	システムの運用・保守	事後	
令和7年3月31日	II 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ①委託内容	磁気ディスクによる事務運用を安全確実に行なうために必要な範囲で、特定個人情報ファイルの管理を委託	システムの運用・保守業務、法制度改正に伴う改修作業	事後	
令和7年3月31日	II 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ②委託先における取扱者数	10人未満	10人以上50人未満	事後	

令和7年3月31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・移転提供先1 (1) 法令上の根拠	・番号法第19条第8号 別表第2の102の2の項 ・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二の主務省令で定める事務及び情報を定める命令第50条	・番号法第19条第8号 ・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139の項及び第141条	事後	
令和7年3月31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	＜ひたちなか市における措置＞ ①特定個人情報が保管されているサーバは電子錠がかけられたサーバ室に設置しており、サーバ室への入退室を厳重に管理する。 ②サーバへアクセスをするためには、IDとパスワードによる認証が必要となる。 ＜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。	＜ひたちなか市における措置＞ ①特定個人情報が保管されているサーバは電子錠がかけられたサーバ室に設置しており、サーバ室への入退室を厳重に管理する。 ②サーバへアクセスをするためには、IDとパスワードによる認証が必要となる。 ＜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】 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】 ①国及びガバメントクラウドのクラウド事業者はアクセスが制御されているため消去をすることはない。	事後	
令和7年3月31日	Ⅲ リスク対策 6. 情報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	＜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利用照会リスト(※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制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。	＜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利用照会リスト(※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制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) 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	事後	

令和7年3月31日	Ⅲリスク対策 7. 特定個人情報の保管・消去	【中間サーバー・プラットフォームにおける物理的措置】 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技術的措置】 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物理的措置】 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技術的措置】 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。 ＜ガバメントクラウドにおける措置＞ 【保管：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。 【保管：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ガバメントクラウドASP、ガバメントクラウド運用管理補助者は、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、 ＜中間サーバー・プラットフォームにおける措置＞	事後	
令和7年3月31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、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リテラシー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、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リテラシー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。 ・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及びガバメントクラウド運用管理責任者が責任を有する。 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及びガバメントクラウド運用管理責任者が対応するものとする。 具体的な取り扱いについて、疑義が生じた場合は、地方公共団体とデジタル庁及び関係者で協議を行う。	事後	
令和7年3月31日	V 評価実施手続き 1. 基礎項目評価 ①実施日	2023/4/1	2024/4/1	事後	