

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
25	釧路市 健康増進法に関する事務 重点項目評価書 個

個人のプライバシー等の権利利益の保護の宣言

釧路市は、健康増進法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低減させるために十分な措置を講じ、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	なし
------	----

評価実施機関名

北海道釧路市長

公表日

令和8年7月6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	健康増進法に関する事務
②事務の内容	健康増進法に基づき、市民の健康の増進を図るため、検診(健診)、健康教育、健康相談その他市民の健康の増進のために必要な事業を実施している。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。)別表に基づき、健康増進法による健康増進事業の実施に関する事務に個人番号を活用する。
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	名称:検診結果の入力、管理概要:検診結果を、住所・氏名・生年月日・性別などの個人情報と結び付けて管理することができる。また、管理しているデータから指定した条件の情報を抽出できる。
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2～5	
システム2	
①システムの名称	番号連携サーバ
②システムの機能	①宛名管理機能 既存住記システムより宛名の異動データを取り込み、個人番号にて同一人判定を行い、団体内統合宛名番号を採番し管理する。 ②情報提供機能 各業務システムより異動データを取り込み、中間サーバーに連携する。 ③情報照会機能 各業務の宛名番号で対象者を検索し、他機関への情報提供を依頼し、結果をオンライン画面にて表示する。 ④符号要求機能 処理通番を要求及び受信し、符号要求データを住基ネットへ送信する。
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	
②システムの機能	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 中間サーバと既存システム、番号連携サーバ及び既存住記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 暗号化／復号機能と、鍵情報及び照会許可照合リスト情報を管理する。 ⑨職員認証・権限管理機能 中間サーバ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		
健康増進法に関わる事務関連ファイル		
4. 個人番号の利用 ※		
法令上の根拠	番号法第9条第1項 別表第111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	・番号法第19条第8号に基づく主務省令第2条の表 (主務省令第2条の表における情報提供の根拠)第3欄(情報提供者)に「市町村長」が含まれる項のうち、第4欄(特定個人情報)に「健康増進法による健康増進事業」が含まれる項(139の項) (主務省令第2条の表における情報照会の根拠)第1欄(情報照会者)に「市町村長」が含まれる項のうち、第2欄(事務)に「健康増進法による健康増進事業」が含まれる項(139の項)	
6. 評価実施機関における担当部署		
①部署	釧路市こども保健部健康推進課	
②所属長の役職名	課長	
7. 他の評価実施機関		
なし		

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

健康増進事業関連ファイル

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 ※	健診対象者	
	その必要性	健診対象者及び受診者を把握するために管理している。
④記録される項目	[50項目以上100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 ※	・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 ・個人番号 対象者を特定するため ・その他識別情報 対象者を特定するため○連絡先等情報 ・4情報 4情報の組み合わせをキーにし、対象者を特定するため○業務関係情報 ・健康・医療関係情報 検診対象者の受診結果等の管理を行うため
	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	こども保健部健康推進課	

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 () ☐ 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 ※		健康増進事業対象者等の個人番号を利用して効率的な事務を図る。
④使用の主体	使用部署	こども保健部健康推進課
	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
⑤使用方法		健康増進法に基づく健康診査、各種がん検診を実施する上で、まず対象者に受診券を作成し送付を行う。一斉送付の場合は、対象者の抽出特定、検診項目の確定、特別徴収の有無を確認し、受診券送付者を確定し送付する。また、特定した対象者の受診の履歴等を把握し、検診項目を確定させ、受診券を作成し送付をする。その後、受診結果を取り込むときは、個人番号または、内部付番した番号、氏名、性別、生年月日を基に本人を特定し結果の登録を行う。
情報の突合		個人を正確に特定するために個人番号を利用して正確性を担保する。
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		健康管理システムの保守に関する委託
①委託内容		問合せ対応、システムの軽微な法改正対応、システムのソフトウェア・パッケージ等のバージョンアップ対応、システム障害対応、システム管理にかかる設定支援
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 ポータス
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 ・行政手続きにおける特定の個人を識別するための番号の利用等に関する法律第19条第8号に基づく利用 特定個人情報の提供に関する命令第2条別表第139項および第141条	
②提供先における用途	健康増進法に係る健康増進事業	
③提供する情報	健康増進事業関係書類であって主務省令で定めるもの	
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	釧路市に住民登録している健康増進法に基づく健康増進事業対象者	
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他（ ☐ 専用線 ☐ 電子記録媒体（フラッシュメモリを除く。） ☐ 紙 ☐	
⑦時期・頻度	情報提供ネットワークシステムを通じて特定個人情報の提供の求めがある都度	
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 ☐ 電子メール ☐ フラッシュメモリ ☐ その他（ ☐ 専用線 ☐ 電子記録媒体（フラッシュメモリを除く。） ☐ 紙 ☐	
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 ※	＜本市における措置＞ ●保管 ①庁内の入退室管理(ICカードにより入退室者を特定及び限定)が行われている部屋に設置したサーバ内に保管する。 ②申請書・帳票等は施錠可能な部屋又は棚に保管する。 ③BCP対策として、外部の建物で施錠可能な部屋に設置したサーバ内に保管する。 ※これらの鍵の管理は、ログ又は台帳によって行う。 ●消去 ①サーバ内の情報資産については、物理的破壊又はデータ消去ソフトにより復元できないように行っている。 ②紙媒体については、個人情報廃棄場所に廃棄し、溶解処理を行っている。 ＜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・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。
7. 備考	

(別添1) 特定個人情報ファイル記録項目

1:宛名番号 2:世帯番号 3:住居区分 4:カナ氏名 5:漢字氏名 6:性別 7:生年月日 8:大字コード 9:行政区コード 10:郵便番号 11:住所 12:方書 13:続柄 14:続柄 15:続柄 16:続柄 17:住民となった日 18:住民となった区分 19:住民となった届出日 20:住民でなくなった日 21:住民でなくなった区分 22:住民でなくなった届出日 23:異動日 24:世帯主カナ 25:世帯主漢字 26:死亡転出区分 27:転出先住所 28:税区分 29:被保険者番号 30:要介護度認定区分 31:認定日 32:有効期間開始日 33:有効期間終了日 34:国保資格区分 35:国保番号 36:被保番号 37:保健の適用年月日 38:資格喪失年月日 39:資格喪失コード 40:消防 41:若年 42:臨職 43:教委 44:共被 45:他被 46:肝炎 47:生活保護区分 48:世帯TEL 49:住民TEL1 50:住民TELコメント1 51:住民TEL2 52:住民TELコメント2 53:年度 54:受診区分 55:検診日 56:検診区分 57:会場コード 58:医療機関コード 59:領収金額 60:実施本庁支所区分 61:入力順 62:未収フラグ 63:国保フラグ 64:70歳以上フラグ 65:非課税フラグ 66:生活保護フラグ 67:年度 68:検診日 69:項目コード 70:検査値 71:判定 72:所見

Ⅲ リスク対策 ※(7. ②を除く。)

1. 特定個人情報ファイル名	
関連ファイル	
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	<システムにおける措置> ・対象者以外の情報の入手を防止するための措置として、対象者が多数表示される一覧系の画面および帳票には個人番号は表示しない仕組みとし、不正な閲覧が行われないようにする。 ・必要な情報以外を入手することを防止するための措置として、職員単位に権限管理を行い、権限がない者は個人番号が参照できない仕組みとし、不正な閲覧が行われないようにする。 <運用における措置> ・個人番号が含まれるファイルに対し、目的を超えた入手が行われている恐れがないかなどを確認するため、アクセスログを取得し、定期的に点検することを可能とする。
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	・個人番号利用業務以外または、個人番号を必要としない業務から宛名情報の要求があった場合は、個人番号が含まれない情報のみを提供するようにアクセス制御を行っている。 ・宛名情報の基本情報を保持する各マスタと、特定個人情報を含むデータベースを切り離して管理しており、特定個人情報を含むデータベースへアクセスする際は専用のAPIを使用し、アクセスログを取得している。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク	
ユーザ認証の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	・健康管理システムを利用する必要がある職員、派遣者、委託先の特定、また、個人番号の照会を可能とする対象者、不可とする対象者を特定し、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を行っている。 ・ユーザーIDについては、正確性を維持する仕組みを構築し、適宜更新している。
その他の措置の内容	なりすまし防止策への対応として、一定時間経過で自動ログアウトする仕組みを実装している。
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	
アクセスログを取得するとともに、定期的にログを解析できる仕組み、不正利用された場合にログを追跡できる仕組みを用意する。その他、特定個人情報の使用にあたり、以下の措置を講じる。 ・スクリーンセーバ等を利用して、長時間にわたり本人確認情報を表示させない ・統合端末のディスプレイを、来庁者から見えない位置に置く ・本人確認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・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、ログイン・ログアウトを実施した職員、時刻、操作内容が記録されるため、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。 (※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	<番号連携サーバーのソフトウェアにおける措置> ①番号連携サーバーの職員認証・権限管理機能により、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容等の記録が実施されるため、不適切な端末操作や情報照会などを抑止する。 <番号連携サーバーの運用における措置> ①番号連携サーバーの職員認証・権限管理において、人事異動や権限変更等が生じた場合は、人事情報を適宜反映することで、その正確性を担保している。 <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		
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・ログアウトを実施した職員、時刻、操作内容が記録されるため、不適切な接続端末の操作やオンライン連携を抑止する仕組みになっている ②情報連携に限り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、不正な名寄せが行な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ネットワーク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、団体ごとの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) 十分にしていない
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	データバックアップを毎日実施し、外部サーバ及び外部媒体に二重保管している。	
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＞

- 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ものだけがアクセスできるような適切なアクセス管理を行っている。
- ②事前に許可されていない装置などに関しては、外部に持ち出しできないこととしている。
- ③国およ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となっている。
- ④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、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、根と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。
- ⑤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。
- ⑥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。
- ⑦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およ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。
- ⑧ガバメントクラウドの特定個人情報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。
- ⑨地方公共団体の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。
- ⑩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。

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	[十分にやっている] <選択肢> 1) 特に力を入れて行っている 2) 十分にやっている 3) 十分に行っていない
具体的な方法	・職員に対しては、個人情報保護に関する研修を行う。・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。

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＞

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提言、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引用・監視を実施する。

＜ガバメントクラウドにおける措置＞

①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。

②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。

③ガバメントクラウド上で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

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	釧路市総合政策部市民協働推進課 釧路市黒金町7丁目5番地 0154-31-4503
②請求方法	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。
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	釧路市こども保健部健康推進課 釧路市黒金町8丁目2番地 0154-31-4524
②対応方法	・問い合わせの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7年12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
平成29年6月20日	I 基本情報 6. 評価実施機関における担当部署 ②所属長	こども保健部次長 中山 朗生	健康推進課長 西山 潤	事後	重要な変更にあたらないため (人事異動)
平成31年3月25日	I 基本情報 6. 評価実施機関における担当部署 ②所属長の役職名	健康推進課長 西山 潤	課長	事前	重要な変更にあたらないため (様式変更)
平成31年3月25日	Ⅲ リスク対策 8. 監査	自己点検	自己点検、内部監査	事前	重要な変更にあたらないため (内部監査の開始)
令和4年2月10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※ ①実施の有無	2)実施しない	1)実施する	事前	
令和4年2月10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		＜情報照会の根拠法令＞・番号法第19条第8号及び別表第二の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提供の根拠法令＞・第50条(健康増進法関係)＜情報提供の根拠法令＞・番号法第19条第8号及び別表第二の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提供を定める命令 第50条(健康増進法関係)	事前	
令和4年2月10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 ②入手方法	・紙・庁内システム	・紙・庁内システム・情報提供ネットワークシステム	事前	
令和4年2月10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		＜中間サーバ・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、操作内容が記録されるため、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。(※3)中間サーバ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。	事前	
令和4年2月10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 リスクへの対策は十分か		2)十分である	事前	
令和4年2月10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 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		＜番号連携サーバのソフトウェアにおける措置＞①番号連携サーバの職員認証・権限管理機能により、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容等の記録が実施されるため、不適切な端末操作や情報照会などを抑制する。＜番号連携サーバの運用における措置＞①番号連携サーバの職員認証・権限管理において、人事異動や権限変更等が生じた場合は、人事情報を適宜反映することで、その正確性を担保している。	事前	
令和4年2月10日	《続き》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		②中間サーバの職員認証・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リスト化したものの。(※3)中間サーバ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。	事前	
令和4年2月10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 2. 目的外の入手が行われるリスク リスクへの対策は十分か		2)十分である	事前	
令和7年2月25日	I 基本情報 4.個人番号の利用※	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。)(平成25年5月31日法律第27号)・番号法第9条第1項 別表第一の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一の主務省令で定める事務を定める命令(別表第一省令)(平成26年内閣府・総務省令第5号)・別表第一省令第54条	番号法第9条第1項 別表第111項	事後	
令和7年2月25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		・番号法第19条第8号に基づく主務省令第2条の表(主務省令第2条の表における情報提供の根拠)第3欄(情報提供者)に「市町村長」が含まれる項のうち、第4欄(特定個人情報)に「健康増進法による健康増進事業」が含まれる項(139の項)(主務省令第2条の表における情報照会の根拠)第1欄(情報照会者)に「市町村長」が含まれる項のうち、第2欄(事務)に「健康増進法による健康増進事業」が含まれる項(139の項)	事後	

令和7年2月25日	V 評価実施手続 1.基礎項目 評価①実施日	平成27年10月15日	令和6年12月1日	事後	
令和8年2月25日	V 評価実施手続 1.基礎項目 評価①実施日	令和6年12月1日 時点	令和7年12月1日 時点	事後	重要な変更に当たらないため (計数の見直し)
	I 基本情報 2. 特定個人情報 ファイルを取り扱う事務 ②事務 の内容	健康増進法に基づき、市民の健康の増進を図るため、検診(健診)、健康教育、健康相談その他市民の健康の増進のために必要な事業を実施している。番号法においては、別表第一項番76に基づき、健康増進法による健康増進事業の実施に関する事務に個人番号を活用する。	健康増進法に基づき、市民の健康の増進を図るため、検診(健診)、健康教育、健康相談その他市民の健康の増進のために必要な事業を実施している。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。)別表に基づき、健康増進法による健康増進事業の実施に関する事務に個人番号を活用する。	事後	記載事項の整理
	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		①システム名称 番号連携サーバ ②システムの機能 ①宛名管理機能 既存住記システムより宛名の異動データを取り込み、個人番号にて同一人判定を行い、団体内統合宛名番号を採番し管理する。②情報提供機能 各業務システムより異動データを取り込み、中間サーバーに連携する。③情報照会機能 各業務の宛名番号で対象者を検索し、他機関への情報提供を依頼し、結果をオンライン画面にて表示する。④符号要求機能 処理通番を要求及び受信し、符号要求データを住基ネットへ送信する。③他システムとの連携 【○】情報提供ネットワークシステム 【○】宛名システム等	事後	記載事項の整理
	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3		①システム名称 中間サーバ ②システムの機能 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、番号連携サーバー及び既存住記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 暗号化/復号機能と、鍵情報及び照会許可用照会リスト情報を管理する。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、移動状態の通知、保管期限切れ情報の削除を行う。③他システムとの連携 【○】情報提供ネットワークシステム	事後	記載事項の整理
	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。)	移転・提供の有無 【○】行っていない。	移転・提供の有無 【○】提供を行っている。移転先1 市区町村 ①法令上の根拠 ・番号法第19条第8号 ・行政手続きにおける特定の個人を識別するための番号の利用等に関する法律第19条第8号に基づく利用特定個人情報の提供に関する命令第2条別表第139項および第141条 ②提供先における用途 健康増進法に係る健康増進事業 ③提供される情報 健康増進事業関係書類であって主務省令で定めるもの 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 ⑤提供する情報の対象となる本人の範囲 釧路市に住民登録している健康増進法に基づく健康増進事業対象者 ⑥提供方法 【○】情報提供ネットワークシステム ⑦時期・頻度 情報提供ネットワークシステムを通じて特定個人情報の提供の求めがある都度	事後	記載事項の整理

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 ①庁内の入退室管理(ICカードにより入退室者を特定及び限定)が行われている部屋に設置したサーバ内に保管する。②申請書・帳票等は施設可能な部屋又は棚に保管する。③BCP対策として、外部の建物で施設可能な部屋に設置したサーバ内に保管する。※これらの鍵の管理は、ログ又は台帳によって行う。●消去 ①サーバ内の情報資産については、物理的破壊又はデータ消去ソフトにより復元できないように行っている。②紙媒体については、個人情報廃棄場所に廃棄し、溶解処理を行っている。	＜本市における措置＞ ●保管 ①庁内の入退室管理(ICカードにより入退室者を特定及び限定)が行われている部屋に設置したサーバ内に保管する。②申請書・帳票等は施設可能な部屋又は棚に保管する。③BCP対策として、外部の建物で施設可能な部屋に設置したサーバ内に保管する。※これらの鍵の管理は、ログ又は台帳によって行う。●消去 ①サーバ内の情報資産については、物理的破壊又はデータ消去ソフトにより復元できないように行っている。②紙媒体については、個人情報廃棄場所に廃棄し、溶解処理を行っている。 ＜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・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サーバー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署環境とは別のデータセンター内に保存され、＜中間サーバー・プラットフォームにおける措置＞	事前	ガバメントクラウド移行に伴い追記
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			中間サーバーの職員認証・権限管理機能では、ログイン・ログアウトを実施した職員、時刻、操作内容が記録されるため、不適切な接続端末の操作やオンライン連携を抑制する仕組みになっている ②情報連携に限り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、不正な名寄せが行な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ネットワーク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、団体ごとの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。	事後	記載事項の整理
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＞ 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ものだけがアクセスできるような適切なアクセス管理を行っている。②事前に許可されていない装置などに関しては、外部に持ち出せないこととしている。③国およ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となっている。④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、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、根と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。⑤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。⑥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。⑦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およ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。⑧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。⑨地方公共団体の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。⑩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	ガバメントクラウド移行に伴い追記

	Ⅲ リスク対策 10. その他のリスク対策	で中間サーバー・プラットフォームにおける指直 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リテランの高い運用担当者によるセキュリティリスクの提言、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引用・監視を実施する。＜ガバメントクラウドにおける措置＞ ①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 800-68、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。②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。③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	ガバメントクラウド移行に伴い追記
--	-----------------------	--	----	------------------