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
28	新型インフルエンザ等対策特別措置法による予防接種に関する事務

個人のプライバシー等の権利利益の保護の宣言

うるま市は、新型インフルエンザ等対策特別措置法による予防接種事務における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、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

沖縄県うるま市長

公表日

令和6年12月25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	新型インフルエンザ等特別措置法による予防接種の実施にかかる事務
②事務の内容	新型インフルエンザ等対策特別措置法（平成24年法律第31号）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（平成25年法律第27号、以下「番号法」という）の規定に従い、特定個人情報を以下の事務で取り扱う。 新型インフルエンザ等が発生した場合に、新型インフルエンザの予防接種（特定接種、住民に対する予防接種）の実施に関する事務を行う。番号法別表に基づき、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。情報提供に必要な情報を副本として中間サーバーへ登録する。 具体的には、特定個人情報ファイルを次の事務に使用する。 ①住民基本台帳をもとに、新型インフルエンザ等の予防接種対象者の選定 ②個人番号を用い、新型インフルエンザ等の予防接種実施の登録 ③照会申請による新型インフルエンザ等の予防接種履歴の照会 ④新型インフルエンザ等の予防接種委託料の支払い ⑤交付申請による転入者・予診票紛失者への新型インフルエンザ等の予防接種予診票配付等 ⑥新型インフルエンザ等の予防接種により健康被害が生じた場合の給付金の支給
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	健康かるて標準仕様対応版
②システムの機能	・予防接種履歴の入力 ・予防接種台帳の検索 ・対象者のデータ抽出 ・委託料の支払い明細書の出力 ・その他上記に関連する機能
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　（ 戸籍システム　）
システム2～5	
システム2	
①システムの名称	MICJET番号連携サーバ（統合宛名管理）
②システムの機能	1. 宛名管理機能 既存住基システムにより宛名の移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移動データを取り込み、中間サーバーに連携する。
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。
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
予防接種台帳ファイル

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25年5月31日法律第27号) 第9条第1項　別表126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（平成26年内閣府・総務省令第5号） 第67条の2

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	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25年5月31日法律第27号) 第19条第8号（特定個人情報の提供の制限）及び別表126項 [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「新型インフルエンザ等対策特別措置法（平成24年法律第31号）による予防接種の実施に関する情報であって主務省令で定めるもの」が含まれる項（別表126項） [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「新型インフルエンザ等対策特別措置法（平成24年法律第31号）による予防接種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（別表126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26年内閣府・総務省令第5号） [情報提供の根拠]　第67条の2	

6. 評価実施機関における担当部署	
①部署	市民生活部　健康支援課
②所属長の役職名	健康支援課長
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

予防接種台帳ファイル

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、特定接種及び住民に対する接種の対象者
	その必要性	新型インフルエンザ等対策特別措置法、予防接種法及び関係法令に基づき、接種記録等の管理を適正に行う必要がある。
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 ※	・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	1　識別情報　対象者を正確に特定するため保有 2　連絡先情報　正確な本人特定のため、予診票等に記入された情報と突合するために保有 3　業務関係情報　予防接種履歴管理を適正に行うために保有
	全ての記録項目	別添1を参照。
⑤保有開始日		令和3年6月14日
⑥事務担当部署		市民生活部　健康支援課

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　（　） [○] 行政機関・独立行政法人等　（住民基本台帳ネットワークシステムを通じて地方公共団体情報システム機構から入手） [○] 地方公共団体・地方独立行政法人　（住民基本台帳ネットワークシステムを通じて他市町村から入手） [　] 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 ※		新型インフルエンザ等対策特別措置法に基づく、特定接種及び住民に対する接種の対象者の個人番号を利用して効率的な事務運用を図るため。
④使用の主体	使用部署	市民生活部　健康支援課
	使用者数	[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
⑤使用方法		・予防接種対象者の抽出 ・予防接種履歴の入力と確認 ・統計データ出力
	情報の突合	氏名、性別、生年月日、住所で突合する。
⑥使用開始日		令和3年6月14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 (2) 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		株式会社熊本計算センター
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		住民基本台帳システムの運用保守委託
①委託内容		住民基本台帳システムの運用保守
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		沖縄行政システム株式会社
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		市町村長
①法令上の根拠		番号法第19条第8号別表126項
②提供先における用途		番号法第19条第8号別表126項に掲げる事務を処理するため
③提供する情報		予防接種の対象者に係る予防接種法施行令第6条の2第1項各号に掲げる事項を記載した当該予防接種に関する情報
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		「2．③対象となる本人の範囲」と同様。
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		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照会があった都度
提供先2～5		
提供先2		
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　（ 庁内連携システム　　）
⑦時期・頻度	
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　※	・申告書及び届出書等の紙やデータ授受に利用する電磁的記録媒体については、許可された者以外入室することのできない室内で取り扱う。また使用後は定められた場所で施錠管理を行って格納している。 ・データの保管は、予め登録された者のICカード認証により、入退室管理を行っている室内（サーバー室）で保管している。 ＜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。 ②ディスク交換やハード更改等の際は、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。
7．備考	

（別添1）特定個人情報ファイル記録項目

年度
宛名番号
体質的理由1
体質的理由2
新型コロナ接種券　券番号
接種コード
接種回数
接種・予診日
接種判定
予診フラグ
性別
接種日年齢
年度末年齢
基準日年齢
実施区分
実施医療機関
Lot.No
接種量
接種番号
接種医
請求日（月）
対象外判定
未接種理由
医師の判断
特記事項
通知時予定日
実施市町村
実施市町村（合併前）
ワクチンメーカー
接種方式
受付番号
ワクチンタイプ
通知済フラグ
通知回数
接種完了フラグ
罹患FLG
受付日（委託料）
自己負担有無（委託料）
集団個別区分（委託料）
特定高齢者候補者区分（委託料）
コースコード（委託料）
支払先コード（委託料）
削除FLG（委託料）
ロックFLG（委託料）
決済済みFLG（委託料）
決済コースFLG（委託料）
更新者
更新日
更新時間

Ⅲ　リスク対策　※(7. ②を除く。)

1. 特定個人情報ファイル名		
(1)住民基本台帳ファイル		
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	照会を行う際は、番号法に定められている事務であることを確認する。 外部に照会文書等を送付する場合は、対象者に関する必要な項目のみを記載するようにチェックを行う。	
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		
入手した情報についてはシステムで氏名・生年月日等の情報で照合を行い、誤った情報については事務に利用しないことを徹底する。		
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	・番号法第9条第1項別表に記載されない事務については、個人番号を用いた連携を行えないよう、仕組みとして担保する。 ・個人番号は、利用権限を有する職員に限り参照することができる措置を講じている。	
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	・個人番号を利用する必要がある職員を特定し、ICカード認証によるユーザ認証管理を実施する。 ・利用毎に利用可能な機能を制限することで不正利用が行えない対策を実施している。 ・なりすましによる不正を防止する観点から、共用IDの利用を禁止する。 ・アクセス権限と業務の対応表を作成する。 ・職員と、その職員が利用する端末機の対応表を作成する。 ・職員は、業務の遂行に必要な権限レベル(照会のみで良いか、更新まで必要か)を管理者に申請し、申請にもとづき、権限を付与する。 ・権限を有していた職員の異動や退職情報を確認し、異動や退職があった際にはアクセス権限を更新し、当該IDを失効させる。	
その他の措置の内容	・特定の管理者がシステム使用に関する権限を与え、システム利用対象者は管理者に対し申請を行う運用としている。 ・システム利用者管理表を作成し、必要毎に随時更新している。 ・システムを使用した場合にはログとして記録される仕組みである。 ・画面の盗み見や不正利用を防止するため、一定時間操作が行われなかった場合にスクリーンセーバーを起動し、元の画面に復帰する際には再度認証を行う必要がある。 ・外部媒体の接続は、端末の各種ポートを制限し、予め決められた利用者及び媒体のみ可能であり、セキュリティ機能付きの媒体として利用記録の管理を行っている。 ・個人情報の保護に関する研修を受講し、業務担当職員の啓発に努める。	
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		
・委託先に対しては、契約書に「情報セキュリティ対策のうち受託者が講ずべき内容」、「守秘義務」、「受託者が本市に損害を与えたときの損害賠償責任」について明記している。 ・委託先に対しては、契約書において、個人情報が記録された資料等を複写し、又は複製してはならない旨明記している。・特定個人情報を記録した紙媒体、外部記録媒体は施錠保管する。		

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	・守秘義務 ・複写及び複製の禁止 ・提供資料の返還 ・個人情報の目的外使用及び第三者への提供の禁止 ・漏えい，減失等の防止 ・従事者への周知 ・事故発生時の報告義務 ・個人情報の持出しの禁止 ・再委託の条件 ・実地調査及び報告 ・取扱者の明確化 ・漏えい事案等が発生した場合の委託先の責任 ・・ISO9001，JIS Q 15001，ISO(JIS Q)27001の取得義務・業務終了後の情報の消去	
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	・市の承諾を得たときを除き再委託を禁止とし，再委託先においても特定個人情報ファイルの適切な取扱いの担保をする。	
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		
・契約書等に基づき，委託業務が実施されていることを適時確認するとともに，その記録を残す。		

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	・番号法の規定により、その範囲を厳格に遵守し提供を行うものとしている。 ・うるま市個人情報保護条例及び情報セキュリティポリシー等の規則に基づき運用を実施している。 ・委託先等への情報の提供に当たっては、契約書で提供情報や再委託の許諾の方法について規定している。	
その他の措置の内容	・情報の移転について、庁内ネットワークにおいて送信記録の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
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		
・番号法第9条第1項別表に記載されていない事務については、個人番号を用いた連携を行えないよう、仕組みとして担保している。 ・提供先への情報の正確性を保つため、入力項目において整合性のチェックを行った情報を提供している。 ・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。 ・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。 ・システムを使用している職員を限定し、システムは業務上必要な職員のみ利用できる。 ・番号法第9条第1項別表及び関係主務省令に定められた事業担当者以外からの特定個人情報へのアクセスが行えない仕組みを構築している。また、当該事業に必要のない情報との紐付けは行えない。		

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	
リスクへの対策は十分か	[ ] ＜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	
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
うるま市における措置 ・サーバ室への入室については、ICカード認証による入退室管理を行い、許可を得た者に限る。 ・特定の職員にのみICカード認証により、PCを利用させる措置をとっている。 ・ウイルス対策ソフトを導入し、定義ファイルを常に最新化するとともに、外部媒体の接続制限、他のネットワークとの接続については、ファイアウォールを設置し外部からのアクセスを常時監視している。 ・特定個人情報が記憶・記録された媒体の保管場所は、施錠管理している。 特定個人情報が古い情報のまま保管され続けるリスクへの措置 ・住人基本台帳法第14条（住民基本台帳の正確な記録を確保するための措置）の規定に基づき、調査等を行い、住民基本台帳の正確な記録を確保する。情報に誤りがある場合は、職権により修正を行っている。 特定個人情報が消去されずいつまでも存在するリスクに対する措置 ・保存期間満了後の申請書や届出書等は溶解処分する。 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。 ・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。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。

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	・情報セキュリティや情報漏えいに関する記事について、職員へ周知している。 ・それぞれの役割や情報セキュリティについての理解度を高めるため、正規職員を対象に情報セキュリティ研修を実施するとともに、非正規職員に対しては、職場内研修により教育を行うことで、個人情報の事務外での利用をしないように周知している。	

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。

Ⅲ　リスク対策　※（7．②を除く。）

1．特定個人情報ファイル名	
（2）本人確認情報ファイル	
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：　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	＜対象者以外の情報の入手を防止するための措置＞ ・本人確認情報の入手元は既存住基システムに限定されるため、既存住基システムへの情報の登録の際に、届出／申請等の窓口において届出／申請内容や本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報の入手の防止に努める。 ＜必要な情報以外を入手することを防止するための措置＞ ・平成14年6月10日総務省告示第334号（第6－7　本人確認情報の通知及び記録）等により市町村CSにおいて既存住基システムを通じて入手することととされている情報以外を入手できないことを、システム上で担保する。 ・正当な利用目的以外の目的にデータベースが構成されることを防止するため、本人確認情報の検索を行う際の検索条件として、少なくとも性別を除く2情報以上（氏名と住所の組み合わせ、氏名と生年月日の組み合わせ）の指定を必須とする。
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	

・不適切な方法で入手が行われるリスクに対する措置
　本人確認情報の入手元を既存住基システムに限定する。

・入手した特定個人情報が不正確であるリスクに対する措置
窓口において、身分証明書（個人番号カード等）の提示により本人確認を行う。特定個人情報の入手元である既存住民基本台帳システムへの情報の登録の際、窓口において、対面で本人確認書類の提示を受け、本人確認を行う。
・通知カード（番号法第7条）と主務省令で定める書類の提示、個人番号カード（同第17条）の提示を求める。
・写真入りの官公庁発行の身分証明書となるものの提示を求める。
・写真なしの官公庁発行の資格証（保険証、国民年金手帳など）2点の提示を求める。
・本人確認情報の入力、削除及び訂正を行う際には、整合性を確保するために、入力、削除及び訂正を行った者以外の者が確認する等、必ず入力、削除及び訂正した内容を確認する。

出生等により新たに個人番号が指定される場合や、転入の際に個人番号カードや法令により定められた身分証明書の組み合わせの提示がない場合には、市町村CSにおいて本人確認情報と個人番号の確認を行う。本人確認情報の入力、削除及び訂正を行う際には、整合性を確保するために入力、削除及び訂正した内容を確認する。本人確認情報に誤りがあった際に訂正を行う場合には、本人確認情報管理責任者の許可を得て行うこととする。

入手の際に特定個人情報が漏えい・紛失するリスクに対する措置
　・機構が作成・配付する専用のアプリケーションを用いることにより、入手の際の特定個人情報の漏えい・紛失の防止に努める。
　・生体認証により操作者の認証を行う。
　・端末のディスプレイは可能な限り来庁者から見えないように配置している。

（注）　専用のアプリケーション：市町村CSのサーバ上で稼動するアプリケーション。市町村CSで管理されるデータの安全保護対策、不正アクセスの防止策には、最新の認証技術や暗号化技術を採用し、データの盗聴、改ざん、破壊及び盗難、端末の不正利用及びなりすまし等を防止する。また、市町村CSのサーバ自体には、外部からのこじあけ等に対して防御性に優れた耐タンパー装置（通信時の相互認証及びデータの暗号化に必要な情報を保管管理する）を内蔵している。

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	・事務で使用するその他のシステムにおける措置： 庁内システムにおける市町村CSへのアクセスは既存住基システムに限定しており、また、既存住基システムと市町村CS間では、法令に基づく事務で使用する以外の情報との紐付けは行わない。なお、市町村CSのサーバ上には住民基本台帳ネットワークシステムの管理及び運用に必要なソフトウェア以外作動させず、また、市町村CSが設置されたセグメントにあるハブには権限の無い者が機器を接続できないよう、適切な対策（物理的なアクセス制限、MACアドレスによるフィルタリング等）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
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	生体認証による操作者認証を行う。	
その他の措置の内容	・操作管理者は操作者に対し、事務に必要な権限のみを与え、生体認証等を行う。 ・退職した元職員や異動した職員等のアクセス権限の失効管理を適切に行う。 ・アクセス権限の登録・失効させたことについて、管理簿に記録を残す。 ・操作者の権限等に応じたアクセス権限が付与されるよう管理する。 ・本人確認情報を扱うシステムの操作履歴（アクセスログ・操作ログ）を記録する。 ・不正な操作が無いことについて、操作履歴により適時確認する。 ・操作履歴の確認により本人確認情報の検索に関して不正な操作の疑いがある場合は、申請文書等との整合性を確認する。・バックアップされた操作履歴について、定められた期間、安全な場所に施錠保管する。	
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		
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。 ・システム利用職員へ事務外利用の禁止等について指導する。 ・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。		
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	・守秘義務 ・複写及び複製の禁止 ・提供資料の返還 ・個人情報の目的外使用及び第三者への提供の禁止 ・漏えい，滅失等の防止 ・従事者への周知 ・事故発生時の報告義務 ・個人情報の持出しの禁止 ・再委託の条件 ・実地調査及び報告 ・取扱者の明確化 ・・ISO9001，JIS Q 15001，ISO(JIS Q)27001の取得義務 ・漏えい事案等が発生した場合の委託先の責任	

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	・移転を行う際に、提供・移転の記録（提供・移転日時、操作者等）をシステム上で管理する。 ・「提供」については，番号法等関係法令で定められた事項についてのみ行う。 ・番号法及び住民基本台帳法並びに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利用について，具体的に誰に対し何の目的で提供できるかを整理し，特定個人情報の提供を行う。	
その他の措置の内容	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 ・相手方（都道府県サーバ）と市町村CSの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。また、媒体へ出力する必要がある場合には、逐一出力の記録が残される仕組みを構築する。 誤った情報を提供・移転してしまうリスクへの措置： システム上、照会元から指定された検索条件に基づき得た結果を適切に提供・移転することを担保する。また、本人確認情報に変更が生じた際には、市町村CSへの登録時点で項目のフォーマットチェックや論理チェック（例えば、現存する住民に対して転入を異動事由とする更新が行われようとした場合や、転居を異動事由とする更新の際に住所以外の更新が行われようとした場合に当該処理をエラーとする）がなされた情報を通知することをシステム上で担保する。 誤った相手に提供・移転してしまうリスクへの措置 ・相手方（都道府県サーバ）と市町村CSの間の通信では相互認証を実施するため、認証できない相手先への情報の提供はなされないことがシステム上担保される。

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		

リスクへの対策は十分か	[ ]	＜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		
リスクへの対策は十分か	[ ]	＜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		

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	・サーバ室への入室については、ICカード認証による入退室管理を行い、許可を得た者に限る。 ・適宜バックアップを行っている。 ・サーバ及び端末にコンピュータウイルス対策ソフトを導入し、ウイルスチェックを実施している。また、新種の不正プログラムに対応するために、パターンファイルを更新している。 ・ネットワーク管理に係る体制等を整備し、ファイアウォールを導入することにより、不正アクセスを防いでいる。	
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		
・契約期間満了後の機器等の撤去時において、記憶媒体がある場合は、そのデータを全て消去し、その証明書を提出させて確認している。 ・システム上、平成14年6月10日総務省告示第334号（第6－8（1）市町村長における本人確認情報の消去）に定める保存期間を経過した住民票の記載の修正前の本人確認情報（履歴情報）及び消除者の本人確認情報を消去する仕組みとする。		

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	・それぞれの役割や情報セキュリティについての理解度を高めるため、正規職員を対象に情報セキュリティ研修を実施するとともに、非正規職員に対しては、職場内研修により教育を行うことで、個人情報について、事務外での利用をしないように周知している。・委託業者については、個人情報の取扱いを含んだ契約を締結している。	

10. その他のリスク対策

Ⅲ　リスク対策　※（7. ②を除く。）

1. 特定個人情報ファイル名	
（3）送付先情報ファイル	
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:　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	＜対象者以外の情報の入手を防止するための措置＞ ・本人確認情報の入手元は既存住基システムに限定されるため、既存住基システムへの情報の登録の際に、届出／申請等の窓口において届出／申請内容や本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報の入手の防止に努める。 ＜必要な情報以外を入手することを防止するための措置＞ ・平成14年6月10日総務省告示第334号（第6－7　本人確認情報の通知及び記録）等により市町村CSにおいて既存住基システムを通じて入手することとされている情報以外を入手できないことを、システム上で担保する。 ・正当な利用目的以外の目的にデータベースが構成されることを防止するため、本人確認情報の検索を行う際の検索条件として、少なくとも性別を除く2情報以上（氏名と住所の組み合わせ、氏名と生年月日の組み合わせ）の指定を必須とする。
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	
・不適切な方法で入手が行われるリスクに対する措置 本人確認情報の入手元を既存住基システムに限定する。 ・入手した特定個人情報が不正確であるリスクに対する措置 窓口において、身分証明書（個人番号カード等）の提示により本人確認を行う。特定個人情報の入手元である既存住民基本台帳システムへの情報の登録の際、窓口において、対面で本人確認書類の提示を受け、本人確認を行う。 ・主務省令で定める書類の提示、個人番号カード（同第17条）の提示を求める。 ・写真入りの官公庁発行の身分証明書となるものの提示を求める。 ・写真なしの官公庁発行の資格証（保険証、国民年金手帳など）2点の提示を求める。 ・本人確認情報の入力、削除及び訂正を行う際には、整合性を確保するために、入力、削除及び訂正を行った者以外の者が確認する等、必ず入力、削除及び訂正した内容を確認する。 出生等により新たに個人番号が指定される場合や、転入の際に個人番号カードや法令により定められた身分証明書の組み合わせの提示がない場合には、市町村CSにおいて本人確認情報と個人番号の確認を行う。本人確認情報の入力、削除及び訂正を行う際には、整合性を確保するために入力、削除及び訂正した内容を確認する。本人確認情報に誤りがあった際に訂正を行う場合には、本人確認情報管理責任者の許可を得て行うこととする。 入手の際に特定個人情報が漏えい・紛失するリスクに対する措置 ・機構が作成・配付する専用のアプリケーションを用いることにより、入手の際の特定個人情報の漏えい・紛失の防止に努める。 ・生体認証により操作者の認証を行う。 ・端末のディスプレイは可能な限り来庁者から見えないように配置している。 （注）　専用のアプリケーション：市町村CSのサーバ上で稼動するアプリケーション。市町村CSで管理されるデータの安全保護対策、不正アクセスの防止策には、最新の認証技術や暗号化技術を採用し、データの盗聴、改ざん、破壊及び盗難、端末の不正利用及びなりすまし等を防止する。また、市町村CSのサーバ自体には、外部からのこじあけ等に対して防御性に優れた耐タンパー装置（通信時の相互認証及びデータの暗号化に必要な情報を保管管理する）を内蔵している。	
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	・宛名システム等における措置： 市町村CSと宛名管理システム間の接続は行わない。 ・事務で使用するその他のシステムにおける措置： 庁内システムにおける市町村CSへのアクセスは既存住基システムに限定しており、また、既存住基システムと市町村CS間では、法令に基づく事務で使用する以外の情報との紐付けは行わない。なお、市町村CSのサーバ上には住民基本台帳ネットワークシステムの管理及び運用に必要なソフトウェア以外作動させず、また、市町村CSが設置されたセグメントにあるハブには権限の無い者が機器を接続できないよう、適切な対策（物理的なアクセス制限、MACアドレスによるフィルタリング等）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

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	生体認証による操作者認証を行う。	
その他の措置の内容	・操作管理者は操作者に対し、事務に必要な権限のみを与え、生体認証等を行う。 ・退職した元職員や異動した職員等のアクセス権限の失効管理を適切に行う。 ・アクセス権限の登録・失効させたことについて、管理簿に記録を残す。 ・操作者の権限等に応じたアクセス権限が付与されるよう管理する。 ・本人確認情報を扱うシステムの操作履歴（アクセスログ・操作ログ）を記録する。 ・不正な操作が無いことについて、操作履歴により適時確認する。 ・操作履歴の確認により本人確認情報の検索に関して不正な操作の疑いがある場合は、申請文書等との整合性を確認する。 ・バックアップされた操作履歴について、定められた期間、安全な場所に施錠保管する。	
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		
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。 ・システム利用職員へ事務外利用の禁止等について指導する。 ・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。		
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	・守秘義務 ・複写及び複製の禁止 ・提供資料の返還・個人情報の目的外使用及び第三者への提供の禁止 ・漏えい，滅失等の防止 ・従事者への周知 ・事故発生時の報告義務 ・個人情報の持出しの禁止 ・再委託の条件 ・実地調査及び報告 ・取扱者の明確化 ・ISO9001，JIS Q 15001，ISO(JIS Q)27001の取得義務 ・漏えい事案等が発生した場合の委託先の責任	
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	・移転を行う際に、提供・移転の記録（提供・移転日時、操作者等）をシステム上で管理する。 ・「提供」については，番号法等関係法令で定められた事項についてのみ行う。 ・番号法及び住民基本台帳法並びに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利用について，具体的に誰に対し何の目的で提供できるかを整理し，特定個人情報の提供を行う。
その他の措置の内容	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：相手方（個人番号カード管理システム）と市町村CSの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。また、媒体へ出力する必要がある場合には、逐一出力の記録が残される仕組みを構築する。・誤った情報を提供・移転してしまうリスクへの措置：システム上、既存住基システムから入手した情報の内容に編集を加えず、適切に個人番号カード管理システムに提供することを担保する。・誤った相手に提供・移転してしまうリスクへの措置：相手方（個人番号カード管理システム）と市町村CSの間の通信では相互認証を実施するため、認証できない相手先への情報の提供はなされないことがシステム上担保される。	

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	
リスクへの対策は十分か	[　　] ＜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	
リスクへの対策は十分か	[　　] ＜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	

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		・サーバ室への入室については、ICカード認証による入退室管理を行い、許可を得た者に限る。 ・適宜バックアップを行っている。 ・サーバ及び端末にコンピュータウイルス対策ソフトを導入し、ウイルスチェックを実施している。また、新種の不正プログラムに対応するために、パターンファイルを更新している。 ・ネットワーク管理に係る体制等を整備し、ファイアウォールを導入することにより、不正アクセスを防いでいる。
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
・契約期間満了後の機器等の撤去時において、記憶媒体がある場合は、そのデータを全て消去し、その証明書を提出させて確認している。 ・システム上、平成14年6月10日総務省告示第334号（第6－8（1）市町村長における本人確認情報の消去）に定める保存期間を経過した住民票の記載の修正前の本人確認情報（履歴情報）及び消除者の本人確認情報を消去する仕組みとする。

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	・課内に情報セキュリティ管理者を配置し、個人情報を取り扱う職員等に対して、適切な管理、指導等を行っている。 ・それぞれの役割や情報セキュリティについての理解度を高めるため、正規職員を対象に情報セキュリティ研修を実施するとともに、非正規職員に対しては、職場内研修により教育を行うことで、個人情報について、事務外での利用をしないように周知している。 ・委託業者については、個人情報の取扱いを含んだ契約を締結している。

10. その他のリスク対策

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	うるま市役所総務部総務政策課 沖縄県うるま市みどり町1丁目1番1号 TEL098-973-0606
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	うるま市役所市民生活部健康支援課 沖縄県うるま市安慶名一丁目8番1号 TEL098-979-0950
②対応方法	問い合わせの受付時に対応記録を残す。 必要に応じ関連部署と連携を取り対応する。

Ⅴ　評価実施手続

1. 基礎項目評価	
①実施日	令和3年6月17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3年4月1日	Ⅰ6. ②所属長	こども部 こども健康課長 濱比嘉 由美子	こども部 こども健康課長 美里 直樹	事後	人事異動
令和3年6月14日	Ⅱ2. ⑤保有開始日	2021/6/13	2021/6/14	事後	運用の開始
令和3年4月1日	Ⅴ1. ①実施日	2021/3/12	2021/6/17	事後	評価の再実施
令和4年6月24日	Ⅰ 6. ①部署 ②所属長	①こども部 こども健康課 ②こども部 こども健康課長 美里 直樹	①こども未来部 子育て世代包括支援センター ②所長 松本 隆宏	事後	機構改革、人事異動
令和4年6月24日	Ⅱ ⑥事務担当部署	こども部 こども健康課	こども未来部 子育て世代包括支援センター	事後	機構改革
令和4年6月24日	Ⅳ 2. ①連絡先	うるま市役所 こども部 こども健康課	うるま市役所 こども未来部 子育て世代包括支援センター	事後	機構改革
令和5年6月16日	Ⅰ 6. ①部署 ②所属長の役職名	①こども未来部 子育て世代包括支援センター ②所長 松本 隆宏	①市民生活部 健康支援課 ②健康支援課長	事後	機構改革
令和5年6月16日	Ⅱ 2. ⑥事務担当部署	こども未来部 子育て世代包括支援センター	市民生活部 健康支援課	事後	機構改革
令和5年6月16日	Ⅱ 3. ④使用の主体 使用部署	こども未来部 子育て世代包括支援センター	市民生活部 健康支援課	事後	機構改革
令和5年6月16日	Ⅳ 1. ①請求先	うるま市役所総務部総務課 沖縄県うるま市みどり町1丁目1番1号 TEL098-973-0606	うるま市役所総務部総務政策課 沖縄県うるま市みどり町1丁目1番1号 TEL098-973-0606	事後	機構改革
令和5年6月16日	Ⅳ 2. ①連絡先	うるま市役所 こども未来部 子育て世代包括支援センター	うるま市役所市民生活部健康支援課 沖縄県うるま市安慶名一丁目8番1号 TEL098-979-0950	事後	機構改革
令和6年12月25日	Ⅰ4.個人番号の利用	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5月31日法律第27号) 第9条第1項 別表第1 93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) 第67条の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(平成25年5月31日法律第27号) 第9条第1項 別表126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(平成26年内閣府・総務省令第5号) 第67条の2	事後	評価の再実施
令和6年12月25日	Ⅰ5.情報提供のネットワークシステムによる情報連携	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25年5月31日法律第27号) 第19条第7号(特定個人情報の提供の制限)及び別表第二 [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「新型インフルエンザ等対策特別措置法(平成24年法律第31号)による予防接種の実施に関する情報であって主務省令で定めるもの」が含まれる項(別表第二 115の2の項) [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「新型インフルエンザ等対策特別措置法(平成24年法律第31号)による予防接種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(別表第二 115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二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) [情報提供の根拠] 第59条の2 [情報照会の根拠] 第59条の2	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25年5月31日法律第27号) 第19条第8号(特定個人情報の提供の制限)及び別表126項 [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「新型インフルエンザ等対策特別措置法(平成24年法律第31号)による予防接種の実施に関する情報であって主務省令で定めるもの」が含まれる項(別表126項) [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「新型インフルエンザ等対策特別措置法(平成24年法律第31号)による予防接種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(別表126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26年内閣府・総務省令第5号) [情報提供の根拠] 第67条の2	事後	評価の再実施
令和6年12月25日	Ⅱ5.特定個人情報の提供・移転(委託に伴うものを除く)①	番号法第19条第7号別表第2第115の2	番号法第19条第8号別表126項	事後	評価の再実施
令和6年12月25日	Ⅱ5.特定個人情報の提供・移転(委託に伴うものを除く)②	番号法第19条第7号別表第2第115の2に掲げる事務を処理するため	番号法第19条第8号別表126項に掲げる事務を処理するため	事後	評価の再実施
令和6年12月25日	Ⅲ3.特定個人情報の使用	【措置内容】 ・番号法第9条第1項別表第1に記載されない事務については、個人番号を用いた連携を行えないよう、仕組みとして担保する。 ・個人番号は、利用権限を有する職員に限り参照することができる措置を講じている。	【措置内容】 ・番号法第9条第1項別表に記載されない事務については、個人番号を用いた連携を行えないよう、仕組みとして担保する。 ・個人番号は、利用権限を有する職員に限り参照することができる措置を講じている。	事後	評価の再実施