

特定個人情報保護評価書(全項目評価書)

評価書番号	評価書名
1	住民基本台帳に関する事務 全項目評価書

個人のプライバシー等の権利利益の保護の宣言

那覇市は、住民基本台帳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

住民基本台帳事務では、事務の一部を委託する外部業者に対し、業者選定の際に業者の情報保護管理体制を確認し、併せて秘密保持に関しても、契約書への特記事項として記載している。また職員に対しても個人情報保護のための研修を実施するなど必要な措置を行っている。

評価実施機関名

那覇市長

個人情報保護委員会 承認日【行政機関等のみ】

公表日

令和5年2月28日

項目一覧

I 基本情報
(別添1) 事務の内容
II 特定個人情報ファイルの概要
(別添2) 特定個人情報ファイル記録項目
III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策
IV その他のリスク対策
V 開示請求、問合せ
VI 評価実施手続
(別添3) 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	住民基本台帳に関する事務
②事務の内容 ※	那覇市(以下「本市」という。)が住民を対象とする行政を適切に行い、また、住民の正しい権利を保障するためには、本市の住民に関する正確な記録が整備されていなければならない。 住民基本台帳は、住民基本台帳法(昭和42年7月25日法律第81号。以下「住基法」という。)に基づき、作成されるものであり、本市において、住民の居住関係の公証、選挙人名簿の登録、その他住民に関する事務の処理の基礎とするとともに、住民の住所に関する届出等の簡素化を図り、あわせて住民に関する記録の適正な管理を図るため、住民に関する記録を正確かつ統一的行うものである。 また、住基法に基づいて住民基本台帳のネットワーク化を図り、全国共通の本人確認システム(住基ネット)を都道府県と共同で構築している。 本市は、住基法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5月31日法律第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。(別添1を参照) ①個人を単位とする住民票を世帯ごとに編成し、住民基本台帳を作成 ②転入届、転居届、転出届、世帯変更届等の届出又は職権に基づく住民票の記載、消除又は記載の修正 ③住民基本台帳の正確な記録を確保するための措置 ④転入届に基づき住民票の記載をした際の転出元市町村に対する通知 ⑤本人又は同一の世帯に属する者、その他法で定める者の請求による住民票の写し等の交付 ⑥住民票の記載事項に変更があった際の都道府県知事に対する通知 ⑦地方公共団体情報システム機構への本人確認情報の照会 ⑧住民からの請求に基づく住民票コードの変更 ⑨個人番号の通知及び個人番号カードの交付 ⑩個人番号カード等を用いた本人確認 ⑪マイナポータルのお知らせ機能での通知による申請データの受領 ※なお、⑨の「個人番号の通知及び個人番号カードの交付」に係る事務については、総務省令により機構に対する事務の委任が認められているため、機構に対する情報の提供を含めて特定個人情報ファイルを使用する。
③対象人数	<選択肢> [30万人以上] 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 5) 30万人以上

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	既存住民基本台帳システム(以下「既存住基システム」という。)
②システムの機能	1. 住民基本台帳の記載 転入、出生、入国、職権等により住民基本台帳に新たに住民を記載(住民票を作成)する機能 2. 住民基本台帳の記載変更 住民基本台帳に記載されている事項に変更があったときに、記載内容を修正する機能 3. 住民基本台帳の消除処理 転出、死亡、出国、職権等により住民基本台帳から住民に関する記載を消除(住民票を除票)する機能 4. 住民基本台帳の照会 住民基本台帳から該当する住民に関する記載(住民票)を照会する機能 5. 帳票の発行 住民票の写し、住民票記載事項証明書、転出証明書、住民票コード通知書等の各種帳票を発行する機能 6. 住民基本台帳の統計 異動集計表や、人口統計用の集計表を作成する機能 7. 住民基本台帳ネットワークシステムとの連携 地方公共団体情報システム機構、県、他自治体と住民基本台帳ネットワークシステム(以下「住基ネット」という。)を通じて連携する機能 8. 法務省への通知事項の作成 外国人住民票の記載等に応じて、市町村通知の作成を行う機能 9. 戸籍システムへの連携 住民票の記載等に応じ、戸籍システムへ附票情報等を連携する機能
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 [○] 市内連携システム [○] 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	住民基本台帳ネットワークシステム(住基ネット) ※次頁の「3. 特定個人情報ファイル名」に記載している「本人確認情報ファイル」及び「送付先情報ファイル」は、住民基本台帳ネットワークシステムの構成要素のうち、市町村コミュニケーションサーバにおいて管理がなされているため、以降は、住民基本台帳ネットワークシステムにおける市町村コミュニケーションサーバ部分について記載する。
②システムの機能	1. 本人確認情報の更新 : 既存住基システムにおいて住民票の記載事項の変更又は新規作成が発生した場合に、当該情報を元に市町村コミュニケーションサーバの本人確認情報を更新し、都道府県サーバへ更新情報を送信する。 2. 本人確認 : 特例転入処理や住民票の写しの広域交付を行う際、窓口における本人確認のため、提示された個人番号カード等を元に住基ネットが保有する本人確認情報に照会を行い、確認結果を画面上に表示する。 3. 個人番号カードを利用した転入(特例転入) : 転入の届出を受け付けた際に、あわせて個人番号カードが提示された場合、当該個人番号カードを用いて転入処理を行う。 4. 本人確認情報検索 : 統合端末において入力された4情報(氏名、住所、性別、生年月日)の組合せをキーに本人確認情報の検索を行い、検索条件に該当する本人確認情報の一覧を画面上に表示する。 5. 地方公共団体情報システム機構への情報照会 : 全国サーバに対して住民票コード、個人番号又は4情報の組合せをキーとした本人確認情報照会要求を行い、該当する個人の本人確認情報を受領する。 6. 本人確認情報整合 : 本人確認情報ファイルの内容が都道府県知事が都道府県サーバにおいて保有している都道府県知事保存本人確認情報ファイル及び地方公共団体情報システム機構が全国サーバにおいて保有している地方公共団体情報システム機構保存本人確認情報ファイルと整合することを確認するため、都道府県サーバ及び全国サーバに対し、整合性確認用本人確認情報を提供する。 7. 送付先情報通知 : 個人番号の通知に係る事務の委任先である地方公共団体情報システム機構において、住民に対して番号通知書類(個人番号通知書、個人番号カード交付申請書(以下「交付申請書」という。)等)を送付するため、既存住基システムから当該市町村の住民基本台帳に記載されている者の送付先情報を抽出し、当該情報を、地方公共団体情報システム機構が設置・管理する個人番号カード管理システムに通知する。 8. 個人番号カード管理システムとの情報連携 : 地方公共団体情報システム機構が設置・管理する個人番号カード管理システムに対し、個人番号カードの交付、廃止、回収又は一時停止解除に係る情報や個人番号カードの返還情報等を連携する。
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	庁内連携システム
②システムの機能	1. 情報連携テーブル格納機能 : 各事務システム間の連携において、各事務システムの連携用テーブルに情報を格納する。 2. 情報連携テーブル修正機能 : 各事務システムにおいて、異動等により情報に修正があった場合、その異動情報等を連携用テーブルに格納する。 3. 情報連携テーブル参照機能 : 各事務システムにおいて、他システムの情報が必要な場合に、他システムの連携用テーブルを参照する。
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 (各事務システム)

システム4	
①システムの名称	宛名システム(番号連携サーバー)
②システムの機能	1. 宛名番号付番機能 :宛名番号が未登録の個人について、新規に宛名番号を付番する。各事務システムからの宛名番号要求に対し、宛名番号を付番し、各事務システム及び中間サーバーに対し返却する。 2. 宛名情報等管理機能 :宛名システムにおいて宛名情報を宛名番号、個人番号と紐付けて保存し、管理する。 3. 中間サーバー連携機能 :中間サーバー、又は中間サーバー端末からの要求に基づき、宛名番号に紐付く宛名情報等を通知する。 4. 各事務システム連携機能 :各事務システムからの要求に基づき、個人番号、又は宛名番号に紐付く宛名情報を通知する。 5. サービス検索・電子申請機能連携機能 :住民が電子申請を行った際の申請データを取得、反映させる機能
③他のシステムとの接続	☐ 情報提供ネットワークシステム ☒ 庁内連携システム ☐ 住民基本台帳ネットワークシステム ☐ 既存住民基本台帳システム ☐ 宛名システム等 ☐ 税務システム ☒ その他 （ 中間サーバー、サービス検索・電子申請機能 ）
システム5	
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 :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「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. 各事務システム接続機能 :中間サーバーと各事務システム、宛名システム及び既存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 :セキュリティを管理する。 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 （

[illegible]

5. 個人番号の利用 ※	
法令上の根拠	1. 番号法 ・第7条(指定及び通知) ・第16条(本人確認の措置) ・第17条(個人番号カードの交付等) 2. 住基法 (平成25年5月31日法律第28号施行時点) ・第5条(住民基本台帳の備付け) ・第6条(住民基本台帳の作成) ・第7条(住民票の記載事項) ・第8条(住民票の記載等) ・第12条(本人等の請求に係る住民票の写し等の交付) ・第12条の4(本人等の請求に係る住民票の写しの交付の特例) ・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) ・第24条の2(個人番号カードの交付を受けている者等に関する転入届の特例) ・第30条の6(市町村長から都道府県知事への本人確認情報の通知等) ・第30条の10 (通知都道府県の区域内の市町村の執行機関への本人確認情報の提供) ・第30条の12 (通知都道府県以外の都道府県の区域内の市町村の執行機関への本人確認情報の提供)
6. 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7号に係る別表第二(特定個人情報を提供できる事項)の各項 (別表第2の第3欄(情報提供者)が「市町村長」であり、第4欄(特定個人情報)が「住民票関係情報」で主務省令で定めるもの) ※()は「番号法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」(内閣府・総務省令)に規定された項 1(第1条第2号ハ)、2(第2条第5号ロ、第10号ハ、第11号ハ、第17号ハ、第18号)、3(第3条第6号ロ、第11号ハ、第12号ハ)、4(第4条第2号ハ)、6(第6条第3号、第7号ロ、第8号ロ、第16号)、8(第7条第1号ロ、第2号ハ、第3号ハ、第4号ロ、第5号ロ)、9(第8条第1号ホ、第2号ホ、第4号)、11(第10条第1号ハ、第3号ハ、第4号ハ)、16(第12条第1号ハ、第2号ロ、第4号ハ、第6号ロ、第8号ハ)、18(第13条第1号ロ、第2号二)、20(第14条第1号ハ、第2号ハ、第3号二)、23(第16条第2号)、27(第20条第9号ロ)、31(第22条第1号二)、34(第22条の3第4号ロ、第5号ロ、第6号)、35(第22条の4第1項第1号、第2号二、第2項第1号、第2号ホ、第3項第1号、第2号ホ、第4項第1号、第2号ホ)、37(第23条第3号)、38(第24条第3号)、39(第24条の2第4号ロ、第8号ハ、第9号ハ、第10号)、40(第24条の3第2号)、42(第25条第8号二、第9号、第10号)、48(第26条の3第1号ロ、第3号ロ)、53(第27条第1号イ、第2号イ、第3号二)、54(第28条第1号ホ)、57(第31条第1号ホ、第2号二、第5号ホ)、58(第31条の2第5号ロ、第9号ハ、第10号ハ、第11号)、59(第31条の3第2号)、61(第32条第1号ハ、第2号ハ)、62(第33条第5号)、66(第37条第1号ロ、第2号イ)、67(第38条第1号ロ)、70(第39条第4号)、74(第40条第1号ロ第2号第3号ロ)、77(第41条第1号、第2号)、80(第43条第1号ロ、第5号ハ)、84(第43条の3第2号)、85の2(第43条の4第1号二)、91(第44条の2第2号)、92(第45条第2号)、94(第47条第1項第2号二、第3号二、第4号二、第5号二、第6号二、第7号二、第8号二、第9号二、第10号二、第11号二、第12号二、第13号二、第14号二、第15号二、第16号二、第17号ハ、第18号二、第19号二、第22号二、第23号二)、96(第48条)、97(第49条第1号ロ、第3号ロ)、101(第49条の2第2号)、102(第50条第1号、第2号ロ、第3号ロ、第4号ロ、第5号ロ)、103(第51条第2号、第3号、第4号ロ、第5号、第6号、第8号、第9号、第10号、第11号、第12号)、106(第53条第2号ハ、第3号ホ、第5号ハ)、108(第55条第1号ハ、第6号ロ、第7号ロ、第9号ロ、第10号ロ、第11号ロ)、111(第56条)、112(第57条)、113(第58条第1号ロ、第2号ロ)、114(第59条第2号)、116(第59条の2第1号ハ)、117(第59条の2の2第2号)、120(第59条の3第1号ホ、第2号ホ、第4号) 第59条の3第1号二、第2号二、第4号 (別表第二における情報照会の根拠) :なし(住民基本台帳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よる情報照会を行わない)
7. 評価実施機関における担当部署	
①部署	市民文化部 ハイサイ市民課
②所属長の役職名	参事兼課長
8. 他の評価実施機関	

(別添1) 事務の内容

(別紙のとおり)

(備考)

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) 住民基本台帳ファイル

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 ※	住基法第5条(住民基本台帳の備付け)に基づき住民基本台帳に記録された住民 ※住民基本台帳に記録されていた者で、転出・死亡等の事由により住民票が削除された者を含む。	
その必要性	法令に基づき住民基本台帳を作成し必要に応じて住民票に記載、削除又は修正すべきとされているため	
④記録される項目	[100項目以上]	<選択肢> 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
主な記録項目 ※	・識別情報 [☐] 個人番号 [☐] 個人番号対応符号 [☐] その他識別情報(内部番号) ・連絡先等情報 [☐] 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 (戸籍に関する情報、外国籍住民に関する情報)	
その妥当性	住基法第7条(住民票の記載事項)にて住民票に記載すべきものとなっている。	
全ての記録項目	別添2を参照。	
⑤保有開始日	平成27年7月1日	
⑥事務担当部署	ハイサイ市民課(首里支所、真和志支所、小禄支所含む)	

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 (地方公共団体情報システム機構) ☐ 地方公共団体・地方独立行政法人 (市町村) ☐ 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 (住基ネット、サービス検索・電子申請機能)

③入手の時期・頻度		転入、入国等の住民異動届及び出生、国籍取得等の戸籍届の申請を受けたとき	
④入手に係る妥当性		本市住民基本台帳に記載する時点での入手となることから上記方法、時期、頻度となる。	
⑤本人への明示		住基法第7条(住民票の記載事項)において明示されている。	
⑥使用目的 ※		住基法に基づき住民基本台帳への記載を行う。	
変更の妥当性		-	
⑦使用の主体	使用部署 ※	ハイサイ市民課(首里支所、真和志支所、小禄支所含む)	
	使用者数	[100人以上500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	
⑧使用方法 ※		・住民基本台帳へ記載することで、本人からの希望及び使用目的に応じて住民票の写しに記載する。 ・地方公共団体情報システム機構、県、及び他市町村間での通知に使用する。 ・個人番号の管理を行う。	
	情報の突合 ※	・住民異動届の際に入手する場合は、個人番号カード又は個人番号通知書とその他本人確認書類で突合を行う。 ・地方公共団体情報システム機構で新たに個人番号が生成された場合は、個人番号の要求時に提供を行っている住民票コードと突合を行う。	
	情報の統計分析 ※	人口統計等個人番号を用いない統計は行いが、個人番号を用いた統計分析は行わない。	
	権利利益に影響を与え得る決定 ※	該当なし	
⑨使用開始日		平成27年10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		住民基本台帳システムのデータ入出力業務委託	
①委託内容		既存住基システムにて行う各種処理の実行	
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
	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	
	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	
	その妥当性	・住民の異動に係る記載等処理や発行処理を行う場合、既存住基システムに蓄積されている住民基本台帳ファイルの全てのデータが処理の対象となるため。 ・既存住基システムの多岐にわたる入力業務を、専門的な知識を有し業務に精通した民間事業者に委託することによって効率・安定的に実施している。	
③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	
④委託先への特定個人情報ファイルの提供方法		[] 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 (既存住基システム端末の直接操作)	

⑤委託先名の確認方法		確認できる。(問合せがあれば回答する)	
⑥委託先名		グローバルデザイン株式会社	
再委託	⑦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
	⑧再委託の許諾方法		
	⑨再委託事項		
委託事項2～5			
委託事項2		住民異動届受付事務及び証明書発行等市民課窓口業務委託	
①委託内容		法市等により職員に限定される事務以外の郵送請求郵便物(申請書)の仕分け、受付簿への入力、電話照会、発送処理、届書の受付、住民からの電子申請データの受領・印刷、証明書の交付等市民課窓口業務。	
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体]	<選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	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
	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	
	その妥当性	・住民の異動届けの受付や、交付請求に基づく証明書の検索、発行処理を行う場合、既存住基システムに蓄積されている住民基本台帳ファイルの全てのデータが処理の対象となるため。 ・法令等により職員に限定される事務以外の事務を民間事業者に委託することで、柔軟性のある運用体制の確立と効率化、作業品質の確保と安定した業務運営の維持を図り、コストの低減と行政サービスの向上を図っている。	
③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
④委託先への特定個人情報ファイルの提供方法		[○] 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 (既存住基システム端末の直接操作)	
⑤委託先名の確認方法		確認できる。(問合せがあれば回答する)	
⑥委託先名		那覇市市民課窓口業務運営連合体(株式会社PBコミュニケーションズ・株式会社沖縄コングレ・グローバルデザイン株式会社)	
再委託	⑦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
	⑧再委託の許諾方法		
	⑨再委託事項		
委託事項3		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取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体]	<選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	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
	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	
	その妥当性	・既存住基システムの運用保守において、データバックアップ等を行うにあたり、住民基本台帳 ファイルの全体を取り扱う必要があるため。 ・既存住基システムの安定した稼動のため専門的な知識を有する民間事業者に委託している。	

③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
④委託先への特定個人情報ファイルの提供方法		[] 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 (サーバ室内にてシステムの直接操作)	
⑤委託先名の確認方法		確認できる。(問合せがあれば回答する)	
⑥委託先名		沖縄行政システム株式会社	
再委託	⑦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
	⑧再委託の許諾方法		
	⑨再委託事項		
委託事項4			
委託事項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 (56) 件 [☒] 移転を行っている (14) 件 [] 行っていない	
提供先1		番号法第19条第8号別表第2に定める情報照会者(55件)	
①法令上の根拠		番号法第19条第8号別表第2	
②提供先における用途		番号法別表第2に定める各事務	
③提供する情報		住民票関係情報(住基法第7条第4号に規定する事項:世帯主についてはその旨、世帯主でない者については世帯主の氏名及び世帯主との続柄)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		「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依頼があるとき	
提供先2～5			
提供先2		那覇市教育委員会 学校教育部 学務課	
①法令上の根拠		番号法第19条第11号	
②提供先における用途		学校保健安全法による医療に要する費用についての援助に関する事務に使用	
③提供する情報		住所、氏名、個人番号等住基法第7条に規定する事項	
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 (庁内連携システム)
⑦時期・頻度	特定個人情報の提供依頼のある都度
提供先3	
提供先4	
提供先5	
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	健康部 国民健康保険課
①法令上の根拠	番号法第9条第1項別表第1に定める事務
②移転先における用途	国民健康保険、後期高齢者医療事務
③移転する情報	住所、氏名、個人番号等住基法第7条に規定する事項
④移転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移転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	住民基本台帳ファイルの更新の際
移転先2～5	
移転先2	福祉部 チャーがんじゅう課
①法令上の根拠	番号法第9条第1項別表第1に定める事務
②移転先における用途	介護保険、在宅福祉サービス、施設入所管理
③移転する情報	住所、氏名、個人番号等住基法第7条に規定する事項
④移転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移転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	住民基本台帳ファイルの更新の際

移転先3	こどもみらい部 子育て応援課
①法令上の根拠	番号法第9条第1項別表第1に定める事務
②移転先における用途	児童手当、児童扶養手当、児童相談、母子寡婦貸付事務
③移転する情報	住所、氏名、個人番号等住基法第7条に規定する事項
④移転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移転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	住民基本台帳ファイルの更新の際
移転先4	福祉部 保護管理課・保護第1課・保護第2課・保護第3課
①法令上の根拠	番号法第9条第1項別表第1に定める事務
②移転先における用途	生活保護ケースワーク、支給点検、相談、医療・介護
③移転する情報	住所、氏名、個人番号等住基法第7条に規定する事項
④移転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移転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	住民基本台帳ファイルの更新の際
移転先5	福祉部 障がい福祉課
①法令上の根拠	番号法第9条第1項別表第1に定める事務
②移転先における用途	精神障害者福祉、地域生活支援、障害者福祉給付、障害者福祉サービス
③移転する情報	住所、氏名、個人番号等住基法第7条に規定する事項
④移転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移転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	住民基本台帳ファイルの更新の際

移転先6～10	
移転先6	健康部 健康増進課
①法令上の根拠	番号法第9条第1項別表第1に定める事務
②移転先における用途	母子支援、成人健診、予防接種
③移転する情報	住所、氏名、個人番号等住基法第7条に規定する事項
④移転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移転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	住民基本台帳ファイルの更新の際
移転先7	こどもみらい部 こども政策課
①法令上の根拠	番号法第9条第1項別表第1に定める事務
②移転先における用途	幼稚園保育、子育て支援事業の実施に関する事務
③移転する情報	住所、氏名、個人番号等住基法第7条に規定する事項
④移転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移転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	住民基本台帳ファイルの更新の際
移転先8	企画財務部 市民税課
①法令上の根拠	番号法第9条第1項別表第1に定める事務
②移転先における用途	市民税の賦課に関する事務
③移転する情報	住所、氏名、個人番号等住基法第7条に規定する事項
④移転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移転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	「2. ③対象となる本人の範囲」と同様。
移転先9	企画財務部 納税課

①法令上の根拠	番号法第9条第1項別表第1に定める事務
②移転先における用途	市税の徴収に関する事務
③移転する情報	住所、氏名、個人番号等住基法第7条に規定する事項
④移転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移転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移転方法	☐ 〇 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	住民基本台帳ファイルの更新の際
移転先10	
①法令上の根拠	番号法第9条第1項別表第1に定める事務
②移転先における用途	税証明発行事務
③移転する情報	住所、氏名、個人番号等住基法第7条に規定する事項
④移転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移転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移転方法	☐ 〇 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	住民基本台帳ファイルの更新の際
移転先11～15	
移転先11	
	企画財務部 資産税課
①法令上の根拠	番号法第9条第1項別表第1に定める事務
②移転先における用途	土地、家屋、償却資産の課税に関する事務
③移転する情報	住所、氏名、個人番号等住基法第7条に規定する事項
④移転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移転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移転方法	☐ 〇 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	住民基本台帳ファイルの更新の際

移転先12	まちなみ共創部 市営住宅課
①法令上の根拠	番号法第9条第1項別表第1に定める事務
②移転先における用途	市営住宅の管理に関する事務
③移転する情報	住所、氏名、個人番号等住基法第7条に規定する事項
④移転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移転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移転方法	☐ 〇 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	住民基本台帳ファイルの更新の際
移転先13	こどもみらい部 こどもみらい課
①法令上の根拠	番号法第9条第1項別表第1に定める事務となる予定
②移転先における用途	子ども子育て支援法による保育園業務
③移転する情報	住所、氏名、個人番号等住基法第7条に規定する事項
④移転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移転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移転方法	☐ 〇 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	住民基本台帳ファイルの更新の際
移転先14	健康部 地域保健課
①法令上の根拠	番号法第9条第1項別表第1に定める事務となる予定
②移転先における用途	母子保健法による保健業務
③移転する情報	住所、氏名、個人番号等住基法第7条に規定する事項
④移転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移転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移転方法	☐ 〇 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	住民基本台帳ファイルの更新の際
移転先15	
移転先16～20	

6. 特定個人情報の保管・消去		
①保管場所 ※		<本市における措置> セキュリティゲートにて入退館管理をしている建物の中で、さらに入退室管理(※)を行っている部屋(サーバ室)に設置したサーバ内に保管する。 ※サーバ室への入室権限を持つ者を限定し、入退室管理カードによりサーバ室に入退室する者が権限を有することを確認する等の管理を行う。 <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。
②保管期間	期間	<選択肢> 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない [20年以上]
	その妥当性	・住民基本台帳に記載している間は保管が必要である。 ・住民基本台帳の世帯全部が削除された住民基本台帳については、150年間保存する。(住民基本台帳法施行令第34条第1項)
③消去方法		<本市における措置> 住民基本台帳システムに記録されたデータのうち、住民基本台帳の削除後150年を経過したデータをシステムで判別して消去する。 <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		

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	
(2) 本人確認情報ファイル	
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 ※	区域内の住民(住基法第5条(住民基本台帳の備付け)に基づき住民基本台帳に記録された住民) ※住民基本台帳に記録されていた者で、転出等の事由により住民票が消除(死亡による消除を除く。)された者(以下「消除者」という。)を含む
その必要性	住基ネットを通じて全国共通の本人確認を行うため、本特定個人情報ファイル(本人確認情報ファイル)において区域内の全ての住民の情報を保有し、住民票に記載されている住民全員の記録を常に正確に更新・管理・提供するため。
④ 記録される項目	10項目以上50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	・個人番号、4情報、その他住民票関係情報 :住基ネットを通じて本人確認を行うために必要な情報として、住民票の記載等に係る本人確認情報(個人番号、4情報、住民票コード及びこれらの変更情報)を記録するため
全ての記録項目	別添2を参照。
⑤ 保有開始日	平成27年6月1日
⑥ 事務担当部署	ハイサイ市民課(首里支所、真和志支所、小禄支所含む)
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 (自部署)
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 (既存住基システム)

③入手の時期・頻度		住民基本台帳の記載事項において、本人確認情報に係る変更又は新規作成時に入手する。	
④入手に係る妥当性		法令に基づき住民に関する記録を正確に行う上で、住民に関する情報に変更があった又は新規作成された際は、住民からの申請等を受け、まず既存住基システムで情報を管理した上で、全国的なシステムである住基ネットに格納する必要があるため	
⑤本人への明示		市町村コミュニケーションサーバが既存住基システムより本人確認情報を入手することについて、住基法第30条の6(市町村長から都道府県知事への本人確認情報の通知等)及び平成14年6月10日総務省告示第334号(第6-7(市町村長から都道府県知事への通知及び記録))に記載されている。	
⑥使用目的 ※		住基ネットを通じて全国共通の本人確認を行うため、本特定個人情報ファイル(本人確認情報ファイル)において区域内の全ての住民の情報を保有し、住民票に記載されている住民全員の記録を常に正確に更新・管理・提供する。	
		変更の妥当性	
		-	
⑦使用の主体	使用部署 ※	ハイサイ市民課(首里支所、真和志支所、小禄支所含む)	
	使用者数	[100人以上500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	
⑧使用方法 ※		・住民票の記載事項の変更又は新規作成が生じた場合、既存住基システムから当該本人確認情報の更新情報を受領し(既存住基システム→市町村コミュニケーションサーバ)、受領した情報を元に本人確認情報ファイルを更新し、当該本人確認情報の更新情報を都道府県知事に通知する(市町村コミュニケーションサーバ→都道府県サーバ)。 ・住民から提示された個人番号カードに登録された住民票コードをキーとして本人確認情報ファイルを検索し、画面に表示された本人確認情報と申請・届出書等の記載内容を照合し確認することで本人確認を行う(個人番号カード→市町村コミュニケーションサーバ)。 ・4情報(氏名、住所、性別、生年月日)の組合せをキーに本人確認情報ファイルの検索を行う。 ・本人確認情報ファイルの内容が都道府県知事保存本人確認情報ファイル(都道府県サーバ)及び地方公共団体情報システム機構保存本人確認情報ファイル(全国サーバ)と整合することを確認するため、都道府県サーバ及び全国サーバに対し、整合性確認用本人確認情報を提供する(市町村コミュニケーションサーバ→都道府県サーバ/全国サーバ)。	
		情報の突合 ※	
		・本人確認情報ファイルを更新する際に、受領した本人確認情報に関する更新データと本人確認情報ファイルを、住民票コードをもとに突合する。 ・個人番号カードを用いて本人確認を行う際に、提示を受けた個人番号カードと本人確認情報ファイルを、住民票コードをもとに突合する。	
		情報の統計分析 ※	
		個人に着目した分析・統計は行わず、本人確認情報の更新件数の集計等、事務処理実績の確認のための統計のみ行う。	
		権利利益に影響を与え得る決定 ※	
		該当なし	
⑨使用開始日		平成27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		住民基本台帳ネットワーク保守業務委託	
①委託内容		住民基本台帳ネットワーク機器等の運用保守	
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
		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	
		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	
		その妥当性	
		・住基ネットの運用・保守作業を実施するため、特定個人情報ファイル全体を委託の対象にする必要がある。 ・住基ネットコミュニケーションサーバ(市町村コミュニケーションサーバ)の安定した稼働のため専門的な知識を有する民間事業者に委託している。	

③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
④委託先への特定個人情報ファイルの提供方法		[] 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 (サーバ室内にてシステムの直接操作)	
⑤委託先名の確認方法		確認できる。(問合せがあれば回答する)	
⑥委託先名		沖縄行政システム株式会社	
再委託	⑦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
	⑧再委託の許諾方法		
	⑨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 (2) 件 [] 移転を行っている () 件 [] 行っていない		
提供先1	都道府県		
①法令上の根拠	住基法第30条の6(市町村長から都道府県知事への本人確認情報の通知等)		
②提供先における用途	・市町村から受領した住民の本人確認情報の変更情報(当該提供情報)を元に都道府県知事保存本人確認情報ファイルの当該住民に係る情報を更新し、地方公共団体情報システム機構に通知する。 ・住基法に基づいて、本人確認情報の提供及び利用等を行う。		
③提供する情報	住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日		
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 (住基ネット)		
⑦時期・頻度	住民基本台帳の記載事項において、本人確認情報に係る変更又は新規作成が発生した都度、随時。		
提供先2～5			
提供先2	都道府県及び地方公共団体情報システム機構		
①法令上の根拠	住基法第14条(住民基本台帳の正確な記録を確保するための措置)		
②提供先における用途	住民基本台帳の正確な記録を確保するために、本人確認情報ファイルの記載内容(当該提供情報)と都道府県知事保存本人確認情報ファイル及び地方公共団体情報システム機構保存本人確認情報ファイルの記載内容が整合することを確認する。		
③提供する情報	住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日		
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 （住基ネット）					
⑦時期・頻度		必要に応じて随時（１年に１回程度）。					
提供先3							
提供先4							
提供先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							
①保管場所 ※		セキュリティゲートにて入退館管理をしている建物の中で、さらに入退室管理を行っている部屋(サーバ室)に設置したサーバ内に保管する。 サーバへのアクセスはID／パスワードによる認証が必要となる。					
②保管期間	期間	☐ 20年以上		<選択肢> 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない			
	その妥当性	(住民基本台帳法施行令第34条第2項) 1 住民票の記載又は記載の修正を行ったことにより通知した本人確認情報は、当該本人確認情報に係る者に係る新たな本人確認情報の通知をした日から起算して150年間保存する。 2 住民票の消除を行ったことにより通知した本人確認情報は、当該本人確認情報の通知の日から起算して150年間保存する。					
③消去方法		本人確認情報ファイルに記録されたデータをシステムにて自動判別し消去する。					
7. 備考							

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	
(3) 送付先情報ファイル	
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 ※	区域内の住民(住基法第5条(住民基本台帳の備付け)に基づき住民基本台帳に記録された住民を指す) ☐ その必要性 番号法第7条第1項(指定及び通知)に基づき、個人番号通知書を個人番号の付番対象者全員に送付する必要がある。 また、同法第17条第1項(個人番号カードの交付等)により、個人番号カードは個人番号通知書と引き換えに交付することとされていることから、併せて、交付申請書を個人番号通知書送付者全員に送付する必要がある。市町村は、法令に基づき、これらの事務の実施を地方公共団体情報システム機構に委任する。
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 (通知カード及び交付申請書の送付先の情報)
	その妥当性 ・個人番号、4情報、その他住民票関係情報 ・個人番号カードの券面記載事項として、法令に規定された項目を記録する必要がある。 ・その他(個人番号通知書及び交付申請書の送付先の情報) ・地方公共団体情報システム機構に対し、法令に基づき個人番号通知書及び交付申請書の印刷、送付並びに個人番号カードの発行を委任するために、個人番号カードの券面記載事項のほか、個人番号通知書及び交付申請書の送付先に係る情報を記録する必要がある。
	全ての記録項目
⑤保有開始日	平成27年10月5日
⑥事務担当部署	ハイサイ市民課(首里支所、真和志支所、小禄支所含む)
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 (自部署)
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 (既存住基システム)

③入手の時期・頻度		使用開始日(平成27年10月5日)から通知カード送付までの一定の期間に、番号法施行日時点における住民の送付先情報をまとめて入手した。(以降は、新たに個人番号の通知対象者が生じた際に入手している)	
④入手に係る妥当性		送付先情報の提供手段として住基ネットを用いるため、市町村コミュニケーションサーバにデータを格納する必要がある。 また、提供手段として電子記録媒体を用いる場合には、暗号化の機能を備える市町村コミュニケーションサーバにおいて電子記録媒体を暗号化した後に提供する必要がある。	
⑤本人への明示		番号法の規定による個人番号通知書及び個人番号カード並びに情報提供ネットワークシステムによる特定個人情報の提供等に関する省令第8条(住民票に基づく通知カードの記載)において明示している。	
⑥使用目的 ※		法令に基づく委任を受けて通知カード及び交付申請書の印刷、送付並びに個人番号カードの発行を行う機構に対し、通知カード及び交付申請書の送付先情報を提供するため。	
変更の妥当性		-	
⑦使用の主体	使用部署 ※	ハイサイ市民課(首里支所、真和志支所、小禄支所含む)	
	使用者数	[100人以上500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	
⑧使用方法 ※		・既存住基システムより個人番号の通知対象者の情報を抽出し、通知カード及び交付申請書等の印刷及び送付に係る事務を法令に基づいて委任する地方公共団体情報システム機構に対し提供する(既存住基システム→市町村コミュニケーションサーバ又は電子記録媒体→個人番号カード管理システム(機構))。	
情報の突合 ※		入手した送付先情報に含まれる4情報等の変更の有無を確認する(最新の4情報等であることを確認するため、機構(全国サーバ)が保有する「地方公共団体情報システム機構保存本人確認情報」との情報の突合を行う。	
情報の統計分析 ※		送付先情報ファイルに記録される個人情報を用いた統計分析は行わない。	
権利利益に影響を与え得る決定 ※		該当なし	
⑨使用開始日		平成27年10月5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		住民基本台帳ネットワーク保守業務委託	
①委託内容		住民基本台帳ネットワーク機器等の運用保守	
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
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	
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	
その妥当性		・住基ネットの運用・保守作業を実施するため、特定個人情報ファイル全体を委託の対象にする必要がある。 ・市町村コミュニケーションサーバの安定した稼働のため専門的な知識を有する民間事業者に委託している。	
③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	
④委託先への特定個人情報ファイルの提供方法		[] 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 (サーバ室内にてシステムの直接操作)	

⑤委託先名の確認方法		確認できる。(問合せがあれば回答する)
⑥委託先名		沖縄行政システム株式会社
再委託	⑦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
	⑧再委託の許諾方法	
	⑨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	地方公共団体情報システム機構	
①法令上の根拠	番号法の規定による個人番号通知書及び個人番号カード並びに情報提供ネットワークシステムによる特定個人情報の提供等に関する総務省令第35条第1項	
②提供先における用途	市町村からの法令に基づく委任を受け、個人番号通知書及び交付申請書を印刷し、送付する。	
③提供する情報	「2. ④記録される項目」と同様。	
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 (住基ネット)	
⑦時期・頻度	使用開始日(平成27年10月5日)から通知カード送付までの一定の期間に、番号法施行日時点における住民の送付先情報をまとめて提供した。(以降は、新たに個人番号の通知対象者が生じた際に提供している)	
提供先2～5		
提供先3		
提供先4		
提供先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		
①保管場所 ※		セキュリティゲートにて入退館管理をしている建物の中で、さらに入退室管理を行っている部屋(サーバ室)に設置したサーバ内に保管する。 サーバへのアクセスはID／パスワードによる認証が必要となる。
②保管期間	期間	[1年未満] ＜選択肢＞ 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない
	その妥当性	送付先情報は、地方公共団体情報システム機構へ提供するために使用され、送付後の変更は行わないことから、セキュリティ上、速やかに削除することが望ましいため。
③消去方法		保存期間が到来した本人確認情報は、地方公共団体情報システム機構から指定された方法により、システム上、一括して消去する仕組みとする。
7. 備考		

(別添2) 特定個人情報ファイル記録項目

(別紙のとおり)

Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※(7. リスク1⑨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1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	・届出の窓口において届出内容や本人確認書類として写真付きの書類(運転免許証や住民基本台帳カードなど)、または複数点の書類(保険証など)の提示を求めて確認を厳格に行い、対象者以外の情報の入手の防止に努める。 ・届出書をシステムへ入力後、異動届とシステムの入力内容を照合し、確認を行う。 ・住基ネットを通じての入手は対象者以外の情報を入手できないよう、仕組みとして担保されている。 ・サービス検索・電子申請機能を利用した申請において、マニュアルやweb上で、個人番号の提出が必要な者の要件を明示、周知し、本人以外の情報の入手を防止する。
必要な情報以外を入手することを防止するための措置の内容	・届出書に記載された情報以外は入力できない仕組みとなっている。 ・届出書をシステムへ入力後、届出書とシステムの入力内容を照合し、確認を行う。 ・住基ネットを通じての入手は対象者以外の情報を入手できないよう、仕組みとして担保されている。 ・サービス検索・電子申請機能においては、画面の誘導に従いサービスを検索し、申請フォームを選択して必要情報を入力することとなるが、画面の誘導を簡潔に行うことで、異なる手続きに係る申請や不要な情報を送信してしまうリスクを防止する。
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
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	・住民異動届出においては住基法第27条の規定に基づき、書面にて本人あるいは代理人による届出のみを受領することとし、受領の際は必ず本人あるいは代理人の本人確認(本人確認書類として写真付きの書類(運転免許証や住民基本台帳カードなど)、または複数点の書類(保険証など)の提示を求めて確認)及び委任状の確認を行うこととしている。 ・親権者や法定代理人については、戸籍謄抄本等の提示または本籍地の市町村へ照会して確認する。 ・任意代理人の持参した委任状の内容(委任の範囲、権限等)に不明瞭な点がある場合には委任者へ電話等で確認する。その場合、委任者の住民票または戸籍の記録をもとに本籍地・世帯構成・前住所等を聞き取る方法で本人確認を行う。 ・システムを利用する必要がある職員を特定し、ユーザIDによる識別とパスワードによる認証を実施する。また、認証後は利用機能の認可機能により、そのユーザがシステム上で利用可能な機能を制限することで不適切な方法で入手が行えない対策を実施している。 ・サービス検索・電子申請機能を利用した申請の場合においては、住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、のちに署名検証も行われるため、本人からの情報のみが発信される。また、サービス検索・電子申請機能の画面の誘導において住民に何の手続きを探し電子申請を行いたいのか理解してもらいながら操作をしていただき、たどり着いた申請フォームが何のサービスにつながるものか明示することで、住民に過剰な負担をかけることなく電子申請を実施いただけるよう措置を講じている。
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3： 入手した特定個人情報ที่ไม่正確であるリスク	
入手の際の本人確認の措置の内容	・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。 ・個人番号通知書(番号法第7条)、個人番号カード(同第17条)の提示を受け、本人確認を行う。 ・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。 ・サービス検索・電子申請機能を利用した申請において、住民がサービス検索・電子相談機能から個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、電子署名付与済の個人番号付電子申請データを受領した地方公共団体は署名検証(有効性確認、改ざん検知等)を実施することとなる。これにより、本人確認を実施する。
個人番号の真正性確認の措置の内容	・個人番号カード等の提示を受け、本人確認を行う。 ・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は個人番号カード(若しくは個人番号通知書と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、住基ネットにて本人確認情報と個人番号の対応付けの確認を行う。
特定個人情報の正確性確保の措置の内容	・特定個人情報の入力、削除及び訂正を行う際は、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。 ・入力、削除及び訂正作業に用いた帳票等は、当市で定める規程に基づいて管理し、保管する。 ・特定個人情報に誤りがあった際に訂正を行う場合には、特定個人情報管理責任者の許可を得て行うこととする。また、訂正した内容等については、その記録を残し、法令等により定められた期間保管する。 ・サービス検索・電子申請機能を利用した申請があった場合は、個人番号カード内の記憶領域に格納された個人番号を申請フォームに自動転記を行うことにより、不正確な個人番号の入力を抑止する措置を講じている。

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
リスク4: 入手の際に特定個人情報情報が漏えい・紛失するリスク		
リスクに対する措置の内容	・住民からの届出書については、特定個人情報の漏洩及び紛失を防止するため、入力及び照会した後は、鍵付の書庫に保管する。 ・既存住基システムは住基ネット以外とは外部接続できない仕組みである ・住基ネットワークでの通信は全て専用回線及び専用交換装置で構成されたネットワークを介して行い、また、通信を行うごとに、意図した通信相手に接続されたことを相互に認証する仕組みを採用している。 ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。	
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、事務に必要なのない情報との紐付けが行われるリスク		
宛名システム等における措置の内容	・統合宛名システムは、番号法別表第1及び関係事務省令に定められた部署以外からの特定個人情報へのアクセスが行えないような仕組みを構築する。また、統合宛名システムへは個人番号、氏名や生年月日等の基本的な情報のみ保持する仕組みとする予定であり、当該事務にて必要のない情報との紐付けは物理的に不可能である。 ・統合宛名システムへは、権限のない者の接続を認めない。	
事務で使用するその他のシステムにおける措置の内容	・既存住基システムと住基ネット市町村コミュニケーションサーバ間では、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。 ・戸籍システムで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。また、戸籍システムには特定個人情報を保有しない。	
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
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、ユーザIDによる識別とパスワードによる認証を実施する。また、認証後は利用機能の認可機能により、そのユーザがシステム上で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。	
アクセス権限の発効・失効の管理	[行っている]	<選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	① ID/パスワードの発行管理 ・アクセス権限と業務の対応表を作成する。 ・業務に対応したアクセス権限を確認し、業務に必要なアクセス権限のみを申請しなければならないものとしている。 ② 失効管理 ・権限を有していた職員の異動退職情報を確認し、異動退職があった際はアクセス権限を更新し、当該IDを失効させている。	
アクセス権限の管理	[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	ユーザIDやアクセス権限を定期的に確認し、業務上アクセスが不要となったIDやアクセス権限を変更または削除する。	
特定個人情報の使用の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	・システムを操作した履歴を磁気ディスクに記録し、必要に応じて操作履歴を解析する。 ・バックアップされた操作履歴は定められた期間、保管する。	
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

リスク3: 従業者が事務外で使用するリスク		
リスクに対する措置の内容	・システムの操作履歴(操作ログ)を記録し、その旨を職員及び受託者へ周知することで不正な使用の防止を図る。 ・職員に対しては、データ保護に関する研修を行っていく。 ・委託先に対しては業務外で使用しないよう仕様書に定め、個人情報保護にかかる誓約書を提出させている。また、セキュリティ研修の実施も義務付けている。 ・業務委託契約の特約において、「個人情報の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる」と定めており、事故発生時は公表を検討する。	
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
リスク4: 特定個人情報ファイルが不正に複製されるリスク		
リスクに対する措置の内容	・所管課設置の端末からは物理的に複製できない仕組みとなっている。 ・委託先に対しては仕様書にて許可を得ない複製を禁止し、個人情報保護にかかる誓約書を提出させている。また、セキュリティ研修の実施も義務付けている。 ・職員に対しては、データ保護に関する研修を行っていく。 ・業務委託契約の特約において、「個人情報の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる」と定めており、事故発生時は公表を検討する。	
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		
・端末機は、スクリーンセーバ等を利用して、長時間にわたり特定個人情報を表示させない。 ・スクリーンセーバの解除は再度ID/パスワードの入力を行い、ログインすることが必要となる。 ・特定個人情報が表示された画面のハードコピー(特定個人情報の入力、削除及び訂正を行う際に正確性を確保するため、異動届受付担当と審査担当で二重にチェックする目的で使用)は、事務処理に必要な範囲にとどめ、使用後はシュレッダーにて廃棄する。		
4. 特定個人情報ファイルの取扱いの委託		[] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認	委託契約を締結するときは、「那覇市情報セキュリティポリシー」に基づき作成された「外部委託時の契約に関する手順」において、委託に関する責任を有する部署を明確にするとともに、セキュリティ要件を記載した契約書の締結を定めている。また、「那覇市情報セキュリティポリシー」において、管理体制についても報告を求めている。	
特定個人情報ファイルの閲覧者・更新者の制限	[制限している]	<選択肢> 1) 制限している 2) 制限していない
具体的な制限方法	・委託にかかる実施体制の提出を義務付けている。 ・委託事業者に対し、個人情報保護にかかる誓約書を提出させている。また、セキュリティ研修の実施も義務付けている。 ・誓約書の提出があった要員に対してのみシステム操作の権限を与えている。	
特定個人情報ファイルの取扱いの記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	・アクセスログによる記録を残している。	
特定個人情報の提供ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	・提供の禁止を契約書に明記している	
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・保守運用委託やオペレーション業務委託に関しては、仕様書にて委託業務実施場所を本市庁舎内に限定し、外部への持ち出しを禁止している。 ・住民異動届関係受付事務及び郵送請求証明書発行等業務委託に関しては、仕様書にて委託業務実施場所を本市庁舎内に限定し、適切な取扱いを行うよう規定している。 ・委託契約の調査条項に基づき必要があると認めるときは調査を行い、または報告を求める。	
特定個人情報の消去ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
ルール内容及びルール遵守の確認方法	・保守運用委託やオペレーション業務委託に関しては、委託実施場所を本市庁舎内のみとしており、かつ直接のシステム操作であるため、特定個人情報を含むデータの受け渡しは発生しないため、消去の委託はしない。 ・住民異動届関係受付事務及び郵送請求証明書発行等業務委託に関しては、特定個人情報が記載された紙媒体については、シュレッダーもしくは溶解処理を行うことを契約書に記載。 ・委託契約の調査条項に基づき必要があると認めるときは調査を行い、または報告を求める。	

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		
規定の内容		加那利市個人情報保護条例第22条」、「那覇市個人情報保護条例施行規則第14条」に基づき、特定個人情報を含む、すべてのデータに対して以下のことを規定している。 ・受託者及び受託者の従業員は、本市の業務で知り得た情報を、本市の許可なく第三者に開示しない。この契約に基づく委託期間が満了し、又はこの契約が解除された後においても同様とする。 ・本市が貸与する情報、成果品（作成途中を含む。以下同じ）を当該業務以外で使用しない。 ・特に認める場合を除き、本市が貸与する情報、成果品を指定場所以外で使用しない。 ・本市が貸与する情報、成果品の破壊、滅失、改ざん、盗難、又は漏洩等がないよう十分に管理し、取り扱う。 ・本市が貸与する情報、成果品を使用する必要がなくなった時は、速やかに返却、納品、又は破棄する。 ・本市が貸与する情報、成果品の破壊、滅失、改ざん、盗難、又は漏洩等が起きたとき、又は起きる懸念があるときは、速やかに本市に報告する。 ・本市が情報セキュリティに関する検査を行うときは、外部委託事業者又は外部要員個人は、関係書類の提出等、検査への積極的な協力を行う。 ・業務委託契約の特約において、「個人情報の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる」と定めている。
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確保		
具体的な方法		・許可のない再委託は禁止している。許可した場合でも通常の委託と同様の措置を義務付けている。
その他の措置の内容		-
リスクへの対策は十分か		
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1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録		
具体的な方法		・庁内連携システムを利用した情報の移転は全て記録を残しており、どのシステムから移転の要求があったかまで記録される。
特定個人情報の提供・移転に関するルール		
ルール内容及びルール遵守の確認方法		・データ移転先からの「データ利用申請」を求め、データ移転元がその法的根拠等を判断し、承認を得たもののみ、データの移転を許可することを「那覇市情報セキュリティポリシー」に定めている。
その他の措置の内容		・庁内連携システムはデータの移転が認められた移転先からのみアクセスを許可された連携システムへデータを移転している。 ・違反行為を行った場合は、法の罰則規定により措置を講じる。 ・個人番号の盗用等が発生した場合は、番号法第7条第2項により、職権及び該当者からの申請により個人番号の変更を行う。
リスクへの対策は十分か		
リスク2： 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容		・情報照会・情報提供の記録が逐一保存される仕組みが確立した庁内連携システムを通してやりとりすることで、不適切な方法で特定個人情報やりとりされることを防止している。
リスクへの対策は十分か		
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容		・庁内連携システムでは本業務で保有する情報を全て連携することはできず、移転元から承認された情報しか移転できないよう、仕組みとして担保されている。また、決められた提供・移転先のみにはしか情報の提供・移転ができない仕組みとなっている。
リスクへの対策は十分か		

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			
・特定個人情報をフラッシュメモリ等の媒体を用いて移転する場合は、セキュリティ機能付きの媒体を用い、かつ、データの暗号化の措置を施したうえで移転を行う。			
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 3) 課題が残されている	2) 十分である
リスク2： 安全が保たれない方法によって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 3) 課題が残されている	2) 十分である
リスク3： 入手した特定個人情報that不正確であるリスク			
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 3) 課題が残されている	2) 十分である
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク			
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 3) 課題が残されている	2) 十分である
リスク5： 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	<既存住基システムにおける措置> ①番号法によって認められている機関等、番号法によって認められている理由をシステムの又は職員による検査にて判断し、提供できる仕組みを構築する予定。 <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that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、特定個人情報that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 3) 課題が残されている	2) 十分である

リスク6: 不適切な方法で提供されるリスク		
リスクに対する措置の内容	<既存住基システムにおける措置> ①提供の記録が逐一保存される仕組みが整備された情報提供ネットワークシステムを用いて連携することで、不適切な方法で特定個人情報提供が提供されることを防止する。 <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照会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。	
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7: 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		
リスクに対する措置の内容	<既存住基システムにおける措置> ①中間サーバーへの連携は適切な頻度で行い、その正確性を担保する。また、情報提供の際は相手先とその妥当性について検証し、誤った相手に提供してしまうことを防止することが担保されたシステムを国が構築する予定である。 <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。	
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		
<本市における措置> 情報提供ネットワークシステムにおいてのリスク及びそのリスクに対する措置については、今後国が作成、公表を行う情報提供ネットワークシステムの特定個人情報保護評価において明示される予定である。 <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1: 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1) 特に力を入れて遵守している 2) 十分に遵守している 3) 十分に遵守していない 4) 政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1) 特に力を入れて周知している 2) 十分に周知している 3) 十分に周知していない
⑤物理的対策	[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
	具体的な対策の内容	<本市における措置> ①電子計算機の盗難を防ぐために、施錠ができる場所等に保管し、施錠をしている。 ②停電(落雷等)によるデータの消失を防ぐために、電子計算機に無停電電源装置等を付設している。 ③火災によるデータ消失を防ぐために、施設内に消火設備を完備している。 ④新耐震基準に基づいて設計、施工された施設内にサーバ室を設置している。 <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。
⑥技術的対策	[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
	具体的な対策の内容	<本市における措置> ①ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォールを設置している。 ②コンピュータウイルス対策ソフトウェアを導入している。 ③OSには随時パッチ適用を実施している。 <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。 <サービス検索・電子申請機能> ①サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起らないようにしており、さらに通信自体も暗号化している。
⑦バックアップ	[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
⑧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
⑨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	-
⑩死者の個人番号	[保管している]	<選択肢> 1) 保管している 2) 保管していない
	具体的な保管方法	死者の個人番号は、生存者の個人番号と同様に保管している。死者の属する住民基本台帳の世帯全部が削除された場合、削除された日から150年間保管する。
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

リスク2: 特定個人情報が古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	住基法第14条第1項(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実施することにより、住民基本台帳の正確な記録を確保する。 サービス検索・電子申請機能を利用した届出については、LGWAN接続端末に個人番号付電子申請データの一時保管として使用するが、一時保管中に再申請や申請情報の訂正が発生した場合は古い情報で審査等を行わないよう、履歴管理を行う。	
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
リスク3: 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	<選択肢> 1) 定めている 2) 定めていない
手順の内容	・住民基本台帳の世帯全部が削除された日から150年間保管し、保管期間が過ぎた特定個人情報データをシステムで判別し消去する。 ・磁気ディスクの廃棄時は、規定に基づき、内容の復元及び判読が不可能になるような方法により消去する。 ・帳票については、規定に基づき、帳簿等を作成し、保管及び廃棄の運用が適切にな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。 ・廃棄時には、規定に基づき、廃棄を行うとともに、廃棄文書目録を残す。	
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		
-		

Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※(7. リスク1⑨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1： 目的外の入手が行われるリスク			
対象者以外の情報の入手を防止するための措置の内容	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、届出の窓口において届出内容や本人確認書類（写真付の公的機関発行証明書等）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の内容	・平成14年6月10日総務省告示第334号（第6ー7 本人確認情報の通知及び記録）等により市町村コミュニケーションサーバ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。		
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 3) 課題が残されている	2) 十分である
リスク2： 不適切な方法で入手が行われるリスク			
リスクに対する措置の内容	本人確認情報の入手元を既存住基システムに限定する。		
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 3) 課題が残されている	2) 十分である
リスク3： 入手した特定個人情報が不正確であるリスク			
入手の際の本人確認の措置の内容	本人確認情報の入手元は既存住基システム（(1) 住民基本台帳ファイル）に限定される。また、既存住基システムへの情報の登録の際に、届出の窓口において本人確認書類の確認を厳格に行った情報が自動的に市町村コミュニケーションサーバの本人確認情報ファイルに連携されることから、本人確認情報ファイルにおける入手の際の本人確認は行わない。		
個人番号の真正性確認の措置の内容	・本人確認情報の既存住基システムからの取得が適切に行われることをシステムにより担保する。 ・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は個人番号カード（若しくは個人番号通知書と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、住基ネットにて本人確認情報と個人番号の対応付けの確認を行う。		
特定個人情報の正確性確保の措置の内容	・既存住基システムへの登録の際に正確性確保の措置がされた住民基本台帳ファイルと本人確認情報ファイルとの整合性の確認を定期的に行うことで、特定個人情報の正確性確保を図る。 ・本人確認情報に誤りがあった際に統合端末上で直接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。また、訂正した内容等については、その記録を残し、法令等により定められる期間保管する。		
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 3) 課題が残されている	2) 十分である
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク			
リスクに対する措置の内容	・地方公共団体情報システム機構が作成・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。 ・操作者の認証を行う。 ※市町村コミュニケーションサーバのサーバ上で稼動するアプリケーション。市町村コミュニケーションサーバ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。		
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 3) 課題が残されている	2) 十分である
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			
宛名システム等における措置の内容	市町村コミュニケーションサーバ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の内容	庁内システムにおける市町村コミュニケーションサーバ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コミュニケーションサーバ間では、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、市町村コミュニケーションサーバには住基ネット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、市町村コミュニケーションサーバが設置されたセグメントにある通信機器は入退室者を制限したマシンルーム内にあり、さらに、施錠を施したラック内に設置している。なお、ラックの鍵も厳重に入退室管理を施された別の部屋に管理されている。		
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 3) 課題が残されている	2) 十分である
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。 ・システムを利用する必要がある職員を特定し、その者に対し照合IDと生体認証登録を行い、それらによるアクセス管理を実施する。 ・そのユーザがシステム上で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。		
アクセス権限の発効・失効の管理	[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	・ユーザIDやアクセス権限を操作者照合情報認証管理責任者が定期的に確認し、業務上アクセスが不要となったIDやアクセス権限を変更または削除する。 ・不正アクセスを分析するために、市町村CS及び統合端末においてアプリケーション操作履歴の記録を取得し、保管する		
アクセス権限の管理	[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	・ユーザIDやアクセス権限を操作者照合情報認証管理責任者が定期的に確認し、業務上アクセスが不要となったIDやアクセス権限を変更または削除する。 ・不正アクセスを分析するために、市町村CS及び統合端末においてアプリケーション操作履歴の記録を取得し、保管する。		
特定個人情報の使用の記録	[記録を残している]	<選択肢> 1) 記録を残している	2) 記録を残していない
具体的な方法	・システム管理者はシステムを操作した履歴を磁気ディスクに記録し、情報保護管理者から操作履歴の内容について提供の要請があれば速やかに対応する。 ・業務上やむを得ず本人確認情報が表示された画面のハードコピーを保管する場合には、本人確認情報表示画面のハードコピー管理簿に記入する。 ・バックアップされた操作履歴は定められた期間、保管する。		
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 3) 課題が残されている	2) 十分である
リスク3: 従業者が事務外で使用するリスク			
リスクに対する措置の内容	・システムの操作履歴(操作ログ)を記録する。 ・職員に対しては、データ保護に関する研修を行っていく。 ・委託先に対しては業務外で使えないよう仕様書に定め、個人情報保護にかかる誓約書を提出させている。また、セキュリティ研修の実施も義務付けている。 ・業務委託契約の特約において、「個人情報の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる」と定めており、事故発生時は公表を検討する。		
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 3) 課題が残されている	2) 十分である
リスク4: 特定個人情報ファイルが不正に複製されるリスク			
リスクに対する措置の内容	・システム上、管理権限を与えられた者以外、情報の複製はできない仕組みとなっている。 ・委託先に対しては仕様書にて許可を得ない複製を禁止し、個人情報保護にかかる誓約書を提出させている。また、セキュリティ研修の実施も義務付けている。 ・職員に対しては、データ保護に関する研修を行っていく。 ・業務委託契約の特約において、「個人情報の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる」と定めており、事故発生時は公表を検討する。		
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 3) 課題が残されている	2) 十分である

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。 ・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。 ・スクリーンセーバの解除は再度ID/パスワードの入力を行い、ログインすることが必要となる。 ・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（特定個人情報の入力、削除及び訂正を行う際に正確性を確保するため、異動届受付担当と審査担当で二重にチェックする目的で使用）は、事務処理に必要となる範囲にとどめ、使用後はシュレッダーにて廃棄する。		
4. 特定個人情報ファイルの取扱いの委託		[] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認	委託契約を締結するときは、「那覇市情報セキュリティポリシー」に基づき作成された「外部委託時の契約に関する手順」において、委託に関する責任を有する部署を明確にするとともに、セキュリティ要件を記載した契約書の締結を定めている。また、「那覇市情報セキュリティポリシー」において、管理体制についても報告を求めている。	
特定個人情報ファイルの閲覧者・更新者の制限	[制限している]	<選択肢> 1) 制限している 2) 制限していない
具体的な制限方法	・委託にかかる実施体制の提出を義務付けている。 ・委託事業者に対し、個人情報保護にかかる誓約書を提出させている。また、セキュリティ研修の実施も義務付けている。 ・誓約書の提出があった要員に対してのみシステム操作の権限を与えている。	
特定個人情報ファイルの取扱いの記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	・アクセスログによる記録を残している。	
特定個人情報の提供ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	・提供を禁止している。	
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・保守運用委託やオペレーション業務委託に関しては、仕様書にて委託業務実施場所を本市庁舎内に限定し、外部への持ち出しを禁止している。 ・委託契約の調査条項に基づき必要があると認めるときは調査を行い、または報告を求める。	
特定個人情報の消去ルール	[定めていない]	<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	・保守運用委託やオペレーション業務委託に関しては、委託実施場所を本市庁舎内のみとしており、かつ直接のシステム操作であるため、特定個人情報を含むデータの受け渡しは発生しないため、消去の委託はしない。	
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	「那覇市情報セキュリティポリシー」に基づき作成された「外部委託時の契約に関する手順」及び「那覇市個人情報保護条例第22条」、「那覇市個人情報保護条例施行規則第14条」に基づき、特定個人情報を含む、すべてのデータに対して以下のことを規定している。 ・受託者及び受託者の従業員は、本市の業務で知り得た情報を、本市の許可なく第三者に開示しない。この契約に基づく委託期間が満了し、又はこの契約が解除された後においても同様とする。 ・本市が貸与する情報、成果品（作成途中を含む。以下同じ）を当該業務以外で使用しない。 ・特に認める場合を除き、本市が貸与する情報、成果品を指定場所以外で使用しない。 ・本市が貸与する情報、成果品の破壊、滅失、改ざん、盗難、又は漏洩等がないよう十分に管理し、取り扱う。 ・本市が貸与する情報、成果品を使用する必要がなくなった時は、速やかに返却、納品、又は破棄する。 ・本市が貸与する情報、成果品の破壊、滅失、改ざん、盗難、又は漏洩等が起きたとき、又は起きる懸念があるときは、速やかに本市に報告する。 ・本市が情報セキュリティに関する検査を行うときは、外部委託事業者又は外部要員個人は、関係書類の提出等、検査への積極的な協力を行う。 ・業務委託契約の特約において、「個人情報の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる」と定めている。	
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確保	[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	・許可のない再委託は禁止している。許可した場合でも通常の委託と同様の措置を義務付けている。	
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1： 不正な提供・移転が行われるリスク			
特定個人情報の提供・移転の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない	
具体的な方法	特定個人情報（個人番号、4情報等）の提供・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し、5年分保存する。 なお、システム上、提供に係る処理を行ったものの提供が認められなかった場合についても記録を残す。		
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	・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。		
その他の措置の内容	「サーバ室等への入室権限」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」を有する者を適切に管理する。		
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	
リスク2： 不適切な方法で提供・移転が行われるリスク			
リスクに対する措置の内容	相手方（都道府県サーバ）と市町村コミュニケーションサーバ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。		
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3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク			
リスクに対する措置の内容	・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、市町村コミュニケーションサーバ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）と市町村コミュニケーションサーバ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。		
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			
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： 安全が保たれない方法によって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3： 入手した特定個人情報ที่ไม่正確であるリスク			
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4： 入手の際に特定個人情報情報が漏えい・紛失するリスク					
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 3) 課題が残されている	2) 十分である	
リスク5： 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 3) 課題が残されている	2) 十分である	
リスク6： 不適切な方法で提供されるリスク					
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 3) 課題が残されている	2) 十分である	
リスク7： 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					
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 3) 課題が残されている	2) 十分である	
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1： 特定個人情報の漏えい・滅失・毀損リスク					
①NISC政府機関統一基準群		[政府機関ではない]	<選択肢> 1) 特に力を入れて遵守している 3)十分に遵守していない	2)十分に遵守している 4) 政府機関ではない	
②安全管理体制		[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 3)十分に整備していない	2)十分に整備している	
③安全管理規程		[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 3)十分に整備していない	2)十分に整備している	
④安全管理体制・規程の職員への周知		[十分に周知している]	<選択肢> 1) 特に力を入れて周知している 3)十分に周知していない	2)十分に周知している	
⑤物理的対策		[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 3)十分に行っていない	2)十分に行っている	
	具体的な対策の内容	・電子計算機の盗難を防ぐために、施錠ができる場所等に保管し、施錠をしている。 ・停電(落雷等)によるデータの消失を防ぐために、電子計算機に無停電電源装置を付設している。 ・火災によるデータ消失を防ぐために、施設内に消火設備を完備している。 ・新耐震基準に基づいて設計、施工された施設内にサーバ室を設置している。			
⑥技術的対策		[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 3)十分に行っていない	2)十分に行っている	
	具体的な対策の内容	・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォールを設置している。 ・コンピュータウイルス対策ソフトウェアを導入している。 ・OSには随時パッチ適用を実施している。			
⑦バックアップ		[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 3)十分に行っていない	2)十分に行っている	
⑧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 3)十分に行っていない	2)十分に行っている	
⑨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	-			

⑩死者の個人番号	[保管している]	<選択肢> 1) 保管している 2) 保管していない
具体的な保管方法	・死者のデータは生存者のデータと同様に保存、管理している。 ・死者のデータは、死亡の処理日から150年間保存する。(住民基本台帳法施行令第34条)	
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
リスク2: 特定個人情報古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	既存住基システムとの整合処理を定期的に実施し、保存する本人確認情報が最新であるかどうかを確認することにより担保する。	
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
リスク3: 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	<選択肢> 1) 定めている 2) 定めていない
手順の内容	・システム上、住民基本台帳法施行令第34条第2項(保存)に定める期間(150年間)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。 ・磁気ディスクの廃棄時は、規定に基づき、内容の復元及び判読が不可能になるような方法により消去する。 ・帳票については、規定に基づき、帳簿等を作成し、保管及び廃棄の運用が適切にな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。 ・廃棄時には、規定に基づき、廃棄を行うとともに、廃棄文書目録を残す。	
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		
-		

Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※(7. リスク1⑨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1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	送付先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、届出の窓口において届出内容や本人確認書類(写真付の公的機関発行証明書等)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の内容	・平成14年6月10日総務省告示第334号(第6ー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。
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
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	送付先情報の入手元を既存住基システムに限定する。
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
リスク3： 入手した特定個人情報ที่ไม่正確であるリスク	
入手の際の本人確認の措置の内容	送付先情報の入手元は既存住基システム((1)住民基本台帳ファイル)に限定される。また、既存住基システムへの情報の登録の際に、届出の窓口において本人確認書類の確認を厳格に行った情報が自動的に市町村コミュニケーションサーバの送付先情報ファイルに連携されることから、送付先情報ファイルにおける入手の際の本人確認は行わない。
個人番号の真正性確認の措置の内容	個人番号の生成元である機構が設置・管理する全国サーバから住民票コードに対応付く個人番号を適切に取得できることを、システムにより担保する。
特定個人情報の正確性確保の措置の内容	既存住基システムにおいて正確性が確保された送付先情報を適切に受信できることをシステムにより担保する。 なお、送付先情報ファイルは、既存住基システムから入手後、個人番号カード管理システムに送付先情報を送付した時点で役割を終える(不要となる)ため、送付後速やかに市町村コミュニケーションサーバから削除する。 そのため、入手から削除までのサイクルがごく短期間であることから、入手から削除の間の正確性を維持する。
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
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	・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。 ・操作者の認証を行う。 ※市町村コミュニケーションサーバで稼動するアプリケーション。市町村コミュニケーションサーバ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、市町村コミュニケーションサーバは、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。
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		
宛名システム等における措置の内容	市町村コミュニケーションサーバ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の内容	庁内システムにおける市町村コミュニケーションサーバ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、市町村コミュニケーションサーバにおいて住基ネット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、市町村コミュニケーションサーバ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）	
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	
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。 ・システムを利用する必要がある職員を特定し、その者に対し照合IDと生体認証登録を行い、それらによるアクセス管理を実施する。 ・そのユーザがシステム上で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。	
アクセス権限の発効・失効の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない	
具体的な管理方法	① ID/生体認証登録管理 ・アクセス権限と業務の対応表を作成する。 ・業務ごとに更新権限の必要があるか、照会権限のみでよいかを確認し、業務に必要なアクセス権限のみを申請しなければならないものとしている。 ・申請に対して、操作者照合情報認証管理責任者が対応表を確認の上、アクセス権限を付与する仕組みである。 ② 失効管理 ・権限を有していた職員の異動や退職によりその都度アクセス権限の失効管理を行っている。	
アクセス権限の管理	[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	・ユーザIDやアクセス権限を操作者照合情報認証管理責任者が定期的に確認し、業務上アクセスが不要となったIDやアクセス権限を変更または削除する。 ・不正アクセスを分析するために、市町村CS及び統合端末においてアプリケーション操作履歴の記録を取得し、保管する。	
特定個人情報の使用の記録	[記録を残している] <選択肢> 1) 記録を残している 2) 記録を残していない	
具体的な方法	・システム管理者はシステムを操作した履歴を磁気ディスクに記録し、情報保護管理者から操作履歴の内容について提供の要請があれば速やかに対応する。 ・バックアップされた操作履歴は定められた期間、保管する。	
その他の措置の内容	-	
リスクへの対策は十分か	[特に力を入れている] <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3: 従業者が事務外で使用するリスク		
リスクに対する措置の内容	・システムの操作履歴（操作ログ）を記録する。 ・職員に対しては、データ保護に関する研修を行っていく。 ・委託先に対しては業務外で使えないよう仕様書に定め、個人情報保護にかかる誓約書を提出させている。また、セキュリティ研修の実施も義務付けている。 ・業務委託契約の特約において、「個人情報の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる」と定めており、事故発生時は公表を検討する。	
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	
リスク4: 特定個人情報ファイルが不正に複製されるリスク		
リスクに対する措置の内容	・システム上、管理権限を与えられた者以外、情報の複製はできない仕組みとなっている。 ・委託先に対しては仕様書にて許可を得ない複製を禁止し、個人情報保護にかかる誓約書を提出させている。また、セキュリティ研修の実施も義務付けている。 ・職員に対しては、データ保護に関する研修を行っていく。 ・業務委託契約の特約において、「個人情報の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる」と定めており、事故発生時は公表を検討する。	
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					
・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。 ・スクリーンセーバの解除は再度ID/パスワードの入力を行い、ログインすることが必要となる。 ・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。 ・特定個人情報が表示された画面のハードコピー（特定個人情報の入力、削除及び訂正を行う際に正確性を確保するため、異動届受付担当と審査担当で二重にチェックする目的で使用）は、事務処理に必要な範囲にとどめ、使用後はシュレッダーにて廃棄する。					
4. 特定個人情報ファイルの取扱いの委託				[] 委託しない	
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク					
情報保護管理体制の確認		委託契約を締結するときは、「那覇市情報セキュリティポリシー」に基づき作成された「外部委託時の契約に関する手順」において、委託に関する責任を有する部署を明確にするとともに、セキュリティ要件を記載した契約書の締結を定めている。また、「那覇市情報セキュリティポリシー」において、管理体制についても報告を求めている。			
特定個人情報ファイルの開覧者・更新者の制限		[制限している] <選択肢> 1) 制限している 2) 制限していない			
具体的な制限方法		・委託にかかる実施体制の提出を義務付けている。 ・委託事業者に対し、個人情報保護にかかる誓約書を提出させている。また、セキュリティ研修の実施も義務付けている。 ・誓約書の提出があった要員に対してのみシステム操作の権限を与えている。			
特定個人情報ファイルの取扱いの記録		[記録を残している] <選択肢> 1) 記録を残している 2) 記録を残していない			
具体的な方法		・アクセスログによる記録を残している。			
特定個人情報の提供ルール		[定めている] <選択肢> 1) 定めている 2) 定めていない			
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法		・提供を禁止している			
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法		・保守運用委託やオペレーション業務委託に関しては、仕様書にて委託業務実施場所を本市庁舎内に限定し、外部への持ち出しを禁止している。 ・委託契約の調査条項に基づき必要があると認めるときは調査を行い、または報告を求める。			
特定個人情報の消去ルール		[定めていない] <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		・保守運用委託やオペレーション業務委託に関しては、委託実施場所を本市庁舎内のみとしており、かつ直接のシステム操作であるため、特定個人情報を含むデータの受け渡しは発生しないため、消去の委託はしない。			
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		「那覇市情報セキュリティポリシー」に基づき作成された「外部委託時の契約に関する手順」及び「那覇市個人情報保護条例第22条」、「那覇市個人情報保護条例施行規則第14条」に基づき、特定個人情報を含む、すべてのデータに対して以下のことを規定している。 ・受託者及び受託者の従業員は、本市の業務で知り得た情報を、本市の許可なく第三者に開示しない。この契約に基づく委託期間が満了し、又はこの契約が解除された後においても同様とする。 ・本市が貸与する情報、成果品（作成途中を含む。以下同じ）を当該業務以外で使用しない。 ・特に認める場合を除き、本市が貸与する情報、成果品を指定場所以外で使用しない。 ・本市が貸与する情報、成果品の破壊、滅失、改ざん、盗難、又は漏洩等がないよう十分に管理し、取り扱う。 ・本市が貸与する情報、成果品を使用する必要がなくなった時は、速やかに返却、納品、又は破棄する。 ・本市が貸与する情報、成果品の破壊、滅失、改ざん、盗難、又は漏洩等が起きたとき、又は起きる懸念があるときは、速やかに本市に報告する。 ・本市が情報セキュリティに関する検査を行うときは、外部委託事業者又は外部要員個人は、関係書類の提出等、検査への積極的な協力を行う。 ・業務委託契約の特約において、「個人情報の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる」と定めている。			
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確保		[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) 課題が残されている 4) 再委託していない			
具体的な方法		・許可のない再委託は禁止している。許可した場合でも通常の委託と同様の措置を義務付けている。			
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1： 不正な提供・移転が行われるリスク	
特定個人情報の提供・移転の記録	[記録を残している] ＜選択肢＞ 1) 記録を残している 2) 記録を残していない
具体的な方法	特定個人情報（個人番号、4情報等）の提供・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し、5年分保存する。 なお、システム上、提供に係る処理を行ったものの提供が認められなかった場合についても記録を残す。
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	・相手方（都道府県サーバ）と市町村コミュニケーションサーバ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。
その他の措置の内容	「サーバ室等への入室権限」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」を有する者を適切に管理する。
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
リスク2： 不適切な方法で提供・移転が行われるリスク	
リスクに対する措置の内容	相手方（都道府県サーバ）と市町村コミュニケーションサーバ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。
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3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク	
リスクに対する措置の内容	・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。
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	
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： 安全が保たれない方法によって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3： 入手した特定個人情報情報が不正確であるリスク					
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 3) 課題が残されている		2) 十分である	
リスク4： 入手の際に特定個人情報情報が漏えい・紛失するリスク					
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 3) 課題が残されている		2) 十分である	
リスク5： 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 3) 課題が残されている		2) 十分である	
リスク6： 不適切な方法で提供されるリスク					
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 3) 課題が残されている		2) 十分である	
リスク7： 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					
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 3) 課題が残されている		2) 十分である	
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1： 特定個人情報の漏えい・滅失・毀損リスク					
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1) 特に力を入れて遵守している 3)十分に遵守していない		2)十分に遵守している 4) 政府機関ではない	
②安全管理体制	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 3)十分に整備していない		2)十分に整備している	
③安全管理規程	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 3)十分に整備していない		2)十分に整備している	
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1) 特に力を入れて周知している 3)十分に周知していない		2)十分に周知している	
⑤物理的対策	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 3)十分に行っていない		2)十分に行っている	
	具体的な対策の内容	・電子計算機の盗難を防ぐために、施錠ができる場所等に保管し、施錠をしている。 ・停電(落雷等)によるデータの消失を防ぐために、電子計算機に無停電電源装置を付設している。 ・火災によるデータ消失を防ぐために、施設内に消火設備を完備している。 ・新耐震基準に基づいて設計、施工された施設内にサーバ室を設置している。			
⑥技術的対策	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 3)十分に行っていない		2)十分に行っている	
	具体的な対策の内容	・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォールを設置している。 ・コンピュータウィルス対策ソフトウェアを導入している。 ・OSには随時パッチ適用を実施している。			

⑦バックアップ	[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
⑧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
⑨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	-	
⑩死者の個人番号	[保管していない]	<選択肢> 1) 保管している 2) 保管していない
具体的な保管方法	-	
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
リスク2： 特定個人情報が古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	本特定個人情報ファイル(送付先情報ファイル)は、送付先情報の連携を行う必要が生じた都度作成／連携することとしており、システム上、連携後速やか(1営業日後)に削除する仕組みとする。 また、媒体を用いて連携する場合、当該媒体は連携後、連携先である機構において適切に管理され、市町村では保管しない。 そのため、送付先情報ファイルにおいて特定個人情報が古い情報のまま保管され続けるリスクは存在しない。	
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3： 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	<選択肢> 1) 定めている 2) 定めていない
手順の内容	システム上、保管期間の経過した特定個人情報を一括して削除する仕組みとする。	
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		
送付先情報ファイルは、機構への特定個人情報の提供後、速やかに市町村コミュニケーションサーバから削除される。 その後、当該特定個人情報は機構において管理されるため、送付先情報ファイルのバックアップは取得しない予定である。		

IV その他のリスク対策 ※

1. 監査		
①自己点検	[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
具体的なチェック方法	<本市における措置> ①年に1回担当部署内において、評価書の記載内容通りの運用がなされていることについて、自己点検を行い、運用状況を確認する。 <中間サーバー・プラットフォームにおける措置> ①運用規則等に基づき、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、定期的に自己点検を実施することとしている。	
②監査	[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
具体的な内容	<中間サーバー・プラットフォームにおける措置> 運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。	
2. 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
具体的な方法	<本市における措置> ①職員に対しては、個人情報保護に関する研修を行っていく。 ②委託業者に対しては、契約内容に個人情報保護に関する研修の実施を義務付け、秘密保持契約を締結している。 ③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。	
3. 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。		

V 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	那覇市役所 総務部 法制契約課(市政情報センター) 〒900-8585 那覇市泉崎1丁目1番1号 電話:098-869-8191
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。
特記事項	-
③手数料等	[有料] <選択肢> 1) 有料 2) 無料 写しの交付を受ける場合には、那覇市個人情報保護条例施行規則に規 (手数料額、納付方法: 定する写しの作成に要する費用(例:A4一枚10円)、郵送により写しの交) 付を受ける場合は郵送料の負担が必要
④個人情報ファイル簿の公表	[行っていない] <選択肢> 1) 行っている 2) 行っていない
個人情報ファイル名	-
公表場所	-
⑤法令による特別の手続	-
⑥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	那覇市役所 市民文化部 ハイサイ市民課 〒900-8585 那覇市泉崎1丁目1番1号 電話:098-862-3274
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。

VI 評価実施手続

1. 基礎項目評価	
①実施日	平成26年10月29日
②しきい値判断結果	[基礎項目評価及び全項目評価の実施が義務付けられる] <選択肢> 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 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(任意に全項目評価を実施) 3) 基礎項目評価の実施が義務付けられる(任意に全項目評価を実施) 4) 特定個人情報保護評価の実施が義務付けられない(任意に全項目評価を実施)
2. 国民・住民等からの意見の聴取	
①方法	「那覇市民意見提出に関する要綱」に基づきパブリックコメントによる意見聴取を実施する。パブリックコメントの実施に際しては、市報に公表している旨の記事を掲載し、市ホームページ及び市内公共施設にて全文を閲覧できるようにする。
②実施日・期間	平成26年11月4日から12月3日
③期間を短縮する特段の理由	—
④主な意見の内容	特になし
⑤評価書への反映	—
3. 第三者点検	
①実施日	平成26年12月17日、平成27年1月22日
②方法	那覇市情報公開・個人情報保護運営審議会にて第三者点検を実施。
③結果	評価書の記載内容については概ね問題ないとして了承された。 (意見) 委託については、委託する特定個人情報ファイルの範囲についての妥当性だけでなく、「なぜ委託するのか」の理由を記載する欄も必要ではないか。
4. 個人情報保護委員会の承認【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

(別添3)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28年3月26日	I-4-①事務実施上の必要性	市町村から、機構に委任することを予定しており、	市町村から、機構に委任しており、	事後	
平成28年3月26日	I-7-②所属長	ハイサイ市民課長 仲真 均	ハイサイ市民課長 宮城 寿満子	事後	
平成28年3月26日	II-2-⑥ 事務担当部署	新都市市民サービスセンター	銘苅証明発行センター	事後	
平成28年3月26日	II-5-移転先10	企画財務部 税制課	企画財務部 市民税課	事後	
平成28年3月26日	II 本人確認情報ファイル -2-⑤保有開始日	平成27年6月予定	平成27年6月	事後	
平成28年3月26日	II 送付先情報ファイル -2-⑤保有開始日	平成27年10月予定	平成27年10月5日	事後	
平成28年4月1日	II 住民基本台帳ファイル -2-⑤保有開始日	平成27年7月1日予定	平成27年7月1日	事後	
平成28年4月1日	V-1-①請求先	那覇市役所 総務部 総務課 市政情報センター	那覇市役所 市民文化部 市民生活安全課 市政情報センター		
平成31年4月1日	I 基本情報 1. ②	・住民基本台帳は、住民基本台帳法(昭和42年7月25日法律第81号。以下「住基法」という。)に基づき、作成されるものであり、本市における住民の届出に関する制度及びその住民たる地位を記録する各種の台帳に関する制度を一元化し、もって、住民の利便を増進するとともに行政の近代化に対処するため、住民に関する記録を正確かつ統一的行うものであり、本市において、住民の居住関係の公証、選挙人(117、120の項)	・住民基本台帳は、住民基本台帳法(昭和42年7月25日法律第81号。以下「住基法」という。)に基づき、作成されるものであり、本市において、住民の居住関係の公証、選挙人名簿の登録、その他住民に関する事務の処理の基礎とするとともに、住民の住所に関する届出等の簡素化を図り、あわせて(別表第二における情報提供の根拠)(別紙1のとおり、119の項)	事後	
平成31年4月1日	I 基本情報 6. ②	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(以下「別表第二の主務省令」という。)第1条第2号ハ 第2条第3号ロ、第6号ハ、第7号ロ及び第12号ハ 第3条第3号ロ、第7号ハ及び第8号ロ 第4条第2号ハ 第6条第2号、第6号ロ及び第7号 第7条第1号ロ及び第2号ロ 第8条第1号ハ、第2号ハ、第3号、第4号及び第5号 第10条第1号ロ、第2号及び第3号 第12条第1号ヌ、第2号ハ、第3号ヌ及び第4号 第13条第1号ロ及び第2号ロ 第14条第1号及び第2号 第15条 第16条第1号、第2号及び第3号 第20条第8号ロ 第22条第1号ニ、第2号、第3号、第4号、第5号、第6号、第7号、第8号、第9号及び第10号 第23条第2号 第24条 第25条第8号ロ、第9号、第10号及び第11号 第27条第1号、第2号及び第3号 第28条第1号ホ、第2号、第3号、第4号、第5号、第6号、第7号、第8号、第9号及び第10号 第31条第1号ホ、第2号ニ及び第5号ホ 第32条第1号ロ及び第2号ロ 第33条第4号 第37条第1号ロ及び第2号 第38条第1号ロ 第39条第3号 第41条第1号及び第2号 第43条第1号ロ 第45条 第47条第2号ハ、第3号ハ、第4号ハ、第5号ハ、第6号ハ、第7号ハ、第10号ハ及び第11号ハ 第48条 第50条第1号、第2号ロ、第3号ロ、第4号ロ及び第5号ロ 第51条第2号、第3号、第4号ロ、第5号、第6号、第8号、第9号、第10号、第11号及び第12号 第53条第2号ニ、第3号ニ及び第4号イ 第55条第1号ニ、第2号ハ、第3号ニ及び第4号ニ 第56条 第57条 第58条第1号ロ及び第2号ロ 第59条第2号	第1条第2号ハ 第2条第5号ロ、第10号ハ、第11号ハ、第17号ハ、第18号 第3条第6号ロ、第11号ハ、第12号ハ 第4条第2号ハ 第6条第3号、第7号ロ、第8号ロ、第16号 第7条第1号ロ、第2号ハ、第3号ハ、第4号ロ、第5号ロ 第8条第1号ニ、第2号ニ、第4号 第10条第1号ハ、第3号ハ、第4号ロ 第12条第1号ロ、第2号イ、第4号ハ、第6号イ、第8号ハ 第13条第1号ロ、第2号ロ 第14条第1号ロ、第2号ロ、第3号ハ 第16条 第20条第8号ロ 第22条第1号ニ 第22条の3第5号ロ、第6号ロ、第7号ロ、第8号 第22条の4第1項第1号、第2号ホ、第2項第1号、第2号ホ、第3項第1号、第2号ホ、第4項第1号、第2号ホ 第23条第3号 第24条第3号 第24条の2第4号ロ、第8号ハ、第9号ハ、第10号 第24条の3第2号 第25条第8号ロ、第9号、第10号 第26条の3第1号ロ、第3号ロ 第27条第1号イ、第2号イ、第3号ハ 第28条第1号ホ 第31条第1号ホ、第2号ニ、第5号ホ 第31条の2第5号ロ、第9号ハ、第10号ハ、第11号 第31条の3第2号 第32条第1号ロ、第2号ロ 第33条第4号 第37条第1号ロ、第2号イ 第38条第1号ロ 第39条第4号 第40条第1号ロ第2号第3号ロ 第41条第1号、第2号 第43条第1号ロ、第5号ハ 第43条の3第2号 第43条の4第1号ニ 第44条の2第2号 第45条第2号 第47条第2号ハ、第3号ハ、第4号ハ、第5号ハ、第6号ハ、第7号ハ、第8号ハ、第9号ハ、第10号ハ	事後	
平成31年4月1日	I 基本情報 7. ②	所属長 ハイサイ市民課長 宮城寿満子	所属長の役職名 参事兼課長	事後	
平成31年4月1日	II 特定個人情報ファイルの概要 2. ⑥	事務担当部署 (、銘苅証明発行センター)	事務担当部署 (※削除する)	事後	
平成31年4月1日	II 特定個人情報ファイルの概要 3. ⑦	使用部署 (、銘苅証明発行センター)	使用部署 (※削除する)	事後	
平成31年4月1日	II 特定個人情報ファイルの概要 4. ⑤	確認できる。(公表されていないが、問合せがあれば回答可能)	確認できる。(問合せがあれば回答する)	事後	
平成31年4月1日	II 特定個人情報ファイルの概要 5. 移転先12	建設管理部 市営住宅課	まちなみ共創部 市営住宅課	事後	
令和2年12月28日	※複数箇所所有	機構	地方公共団体情報システム機構	事後	
令和2年12月28日	※複数箇所所有	通知カード	個人番号通知書	事後	
令和2年12月28日	II 特定個人情報ファイルの概要 (1)住民基本台帳ファイル 6.特定個人情報の保管・消去	・住基法施行令第8条(住民票の消除)、第8条の2(日本の国籍の取得又は喪失による住民票の記載及び消除)、第10条(転居又は世帯変更による住民票の記載及び消除)若しくは第12条第3項(職権による住民票の記載等)の規定により消除された住民票について、住基法施行令第34条(保存)に基づいて5年間保管する。	(住民基本台帳法施行令第34条第1項) 住民基本台帳の世帯全部が削除された住民基本台帳については、150年間保存する。	事後	
令和2年12月28日	II 特定個人情報ファイルの概要 (2)本人確認情報ファイル 6.特定個人情報の保管・消去	・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は、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)に定める期間(5年間)保管する。	(住民基本台帳法施行令第34条第2項) 1 住民票の記載又は記載の修正を行ったことにより通知した本人確認情報は、当該本人確認情報に係る者に係る新たな本人確認情報の通知をした日から起算して150年間保存する。 2 住民票の消除を行ったことにより通知した本人確認情報は、当該本人確認情報の通知の日から起算して150年間保存する。	事後	
令和2年12月28日	II 特定個人情報ファイルの概要 (3)送付先情報ファイル 3.特定個人情報の入手・使用 ⑤本人への明示	法令上に記載予定	番号法の規定による個人番号通知書及び個人番号カード並びに情報提供ネットワークシステムによる特定個人情報の提供等に関する省令第8条(住民票に基づく個人番号通知書の記載)において明示している。	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和2年12月28日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3.特定個人情報の使用(従業者が事務外で使用するリスクに対する措置の内容)	違反行為を行った場合は、契約上の損害賠償規定により措置を講じる予定。	業務委託契約の特約において、「個人情報の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる」と定めており、事故発生時は公表を検討する。	事後	
令和2年12月28日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4.特定個人情報の取扱いの委託(規定の内容)	外部委託業者又は外部要因個人が本市の情報セキュリティ保持に関する契約に違反した場合の措置について記載する。	業務委託契約の特約において、「個人情報の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる」と定めている。	事後	
令和2年12月28日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7.特定個人情報の保管・消去(死者の個人番号の保管方法)	住基法第8条(住民票の記載等)の規定により削除された住民票について、住基法施行令第34条(保存)において定める期間(5年間)、システム上にて保管する。	死者の個人番号は、生存者の個人番号と同様に保管している。死者の属する住民基本台帳の世帯全部が削除された場合、削除された日から150年間保管する。	事後	
令和2年12月28日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7.特定個人情報の保管・消去(消去手順)	住民基本台帳ファイルに記録されたデータのうち、住民票の削除後5年を経過したデータをシステムにて判別し消去することができる。	住民基本台帳の世帯全部が削除された日から150年間保管し、保管期間が過ぎた特定個人情報データをシステムで判別し消去する。	事後	
令和2年12月28日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 (2)本人確認情報ファイル 3.特定個人情報の使用の記録(具体的な内容)	操作者はシステムを業務運用、業務終了する都度、住基ネット操作者照合情報認証使用簿に記入する。	業務上やむを得ず本人確認情報が表示された画面のハードコピーを保管する場合には、本人確認情報表示画面のハードコピー管理簿に記入する。	事後	
令和2年12月28日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 (2)本人確認情報ファイル 7.特定個人情報の保管・消去リスク3:消去手順の内容	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。	システム上、住民基本台帳法施行令第34条第2項(保存)に定める期間(150年間)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。	事後	
令和3年9月10日	I-6 ②法令上の根拠	・番号法第19条第7号に係る別表第二(特定個人情報を提供できる事項)の各項目	・番号法第19条第8号に係る別表第二(特定個人情報を提供できる事項)の各項目	事後	
令和3年9月10日	Ⅱ-5(1)住民基本台帳ファイル 提供先1	番号法第19条第7号別表第2に定める情報照会者(55件)	番号法第19条第8号別表第2に定める情報照会者(55件)	事後	
令和3年9月10日	Ⅱ-5(1)住民基本台帳ファイル 提供先1 ①法令上の根拠	番号法第19条第7号別表第2	番号法第19条第8号別表第2	事後	
令和3年9月10日	Ⅱ-5(1)住民基本台帳ファイル 提供先2 ①法令上の根拠	番号法第19条第10号	番号法第19条第11号	事後	
令和5年2月1日	I-1特定個人情報を取り扱う事務②事務内容		①マイナポータルのお知らせ機能での通知による申請データの受領	事前	
令和5年2月1日	I-2特定個人情報を取り扱う事務(別添1)事務の内容「(1)住民基本台帳ファイル」を取り扱う事務の内容(既存住基システムを中心とした事務の流れ)		※上記の図中、【申請管理システム】及び【宛名システム】については、どちらも番号連携サーバを指しているが、連携の状況や事務の流れの理解がしやすいよう、分けて表記している。	事前	
令和5年2月1日	I-2特定個人情報を取り扱う事務(別添1)事務の内容「(1)住民基本台帳ファイル」		1-①' マイナポータルのお知らせ機能での通知による申請データの受領	事前	
令和5年2月1日	I-2システム4②システムの機能		5. サービス検索・電子申請機能連携機能 :住民が電子申請を行った際の申請データを取得、反映させる機能	事前	
令和5年2月1日	I-2システム4③他システムとの接続	【○】その他(中間サーバー)	【○】その他(中間サーバー、サービス検索・電子申請機能)	事前	
令和5年2月1日	I-2システム6①システムの名称		サービス検索・電子申請機能	事前	
令和5年2月1日	I-2システム6②システムの機能		【住民向け機能】 自らが受けることができるサービスをオンラインで検索及び申請できる機能 【地方公共団体向け機能】 住民が電子申請を行った際の申請データ取得画面又は機能を、地方公共団体に公開する機能	事前	
令和5年2月1日	I-2システム6③他システムとの接続		【○】宛名システム等	事前	
令和5年2月1日	Ⅱ-3特定個人情報ファイルの入手・使用 ②入手方法	【○】その他(住基ネット)	【○】その他(住基ネット、サービス検索・電子申請機能)	事前	
令和5年2月1日	Ⅱ-4特定個人情報ファイルの取り扱いの委託 委託事項1	(株)那覇データセンター	グローバルデザイン株式会社	事後	
令和5年2月1日	Ⅱ-4特定個人情報ファイルの取り扱いの委託 委託事項2 ①委託内容	法令等により職員に限定される事務以外の郵送請求郵便物(申請書)の仕分け、受付簿への入力、電話照会、発送処理、届書の受付、証明書の交付等市民課窓口業務	法令等により職員に限定される事務以外の郵送請求郵便物(申請書)の仕分け、受付簿への入力、電話照会、発送処理、届書の受付、住民からの電子申請データの受領・印刷、証明書の交付等市民課窓口業務	事前	
令和5年2月1日	Ⅱ-4特定個人情報ファイルの取り扱いの委託 委託事項2		【○】専用線	事前	
令和5年2月1日	Ⅱ-4特定個人情報ファイルの取り扱いの委託 委託事項2 ⑥委託先名	那覇市市民課窓口業務運営連合体(株式会社PBコミュニケーションズ・株式会社沖縄コングレ)	那覇市市民課窓口業務運営連合体(株式会社PBコミュニケーションズ・株式会社沖縄コングレ・グローバルデザイン株式会社)	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年2月1日	Ⅲ-2特定個人情報の入手 (情報提供音ネットワークを通じた手法を除く)リスク1:目的外の入手が行われるリスク 対象者以外の情報の入手を防止するための措置の内容	・届出の窓口において届出内容や本人確認書類として写真付きの書類(運転免許証や住民基本台帳カードなど)、または複数点の書類(保険証など)の提示を求めて確認を厳格に行い、対象者以外の情報の入手の防止に努める。 ・届出書をシステムへ入力後、異動届とシステムの入力内容を照合し、確認を行う。 ・住基ネットを通じての入手は対象者以外の情報を入手できないよう、仕組みとして担保されている。	・届出の窓口において届出内容や本人確認書類として写真付きの書類(運転免許証や住民基本台帳カードなど)、または複数点の書類(保険証など)の提示を求めて確認を厳格に行い、対象者以外の情報の入手の防止に努める。 ・届出書をシステムへ入力後、異動届とシステムの入力内容を照合し、確認を行う。 ・住基ネットを通じての入手は対象者以外の情報を入手できないよう、仕組みとして担保されている。 ・サービス検索・電子申請機能を利用した申請において、マニュアルやweb上で、個人番号の提出が必要な者の要件を明示、周知し、本人以外の情報の入手を防止する。	事前	
令和5年2月1日	Ⅲ-2特定個人情報の入手 (情報提供音ネットワークを通じた手法を除く)リスク1:目的外の入手が行われるリスク 必要な情報以外を入手することを防止するための措置の内容	・届出書に記載された情報以外は入力できない仕組みとなっている。 ・届出書をシステムへ入力後、届出書とシステムの入力内容を照合し、確認を行う。 ・住基ネットを通じての入手は対象者以外の情報を入手できないよう、仕組みとして担保されている。	・届出書に記載された情報以外は入力できない仕組みとなっている。 ・届出書をシステムへ入力後、届出書とシステムの入力内容を照合し、確認を行う。 ・住基ネットを通じての入手は対象者以外の情報を入手できないよう、仕組みとして担保されている。 ・サービス検索・電子申請機能においては、画面の誘導に従いサービスを検索し、申請フォームを選択して必要情報を入力することとなるが、画面の誘導を簡潔に行うことで、異なる手続きに係る申請や不要情報を送信してしまうリスクを防止する。	事前	
令和5年2月1日	Ⅲ-2特定個人情報の入手 (情報提供音ネットワークを通じた手法を除く) リスク2:不適切な方法で入手が行われるリスク リスクに対する措置の内容	・住民異動届出においては住基法第27条の規定に基づき、書面にて本人あるいは代理人による届出のみを受領することとし、受領の際は必ず本人あるいは代理人の本人確認(本人確認書類として写真付きの書類(運転免許証や住民基本台帳カードなど)、または複数点の書類(保険証など)の提示を求めて確認)及び委任状の確認を行うこととしている。 ・親権者や法定代理人については、戸籍謄抄本等の提示または本籍地の市町村へ照会して確認する。 ・任意代理人の持参した委任状の内容(委任の範囲、権限等)に不明瞭な点がある場合には委任者へ電話等で確認する。その場合、委任者の住民票または戸籍の記録をもとに本籍地・世帯構成・前住所等を聞き取る方法で本人確認を行う。 ・システムを利用する必要がある職員を特定し、ユーザIDによる識別とパスワードによる認証を実施する。また、認証後は利用機能の認可機能により、そのユーザがシステム上で利用可能な機能を制限することで不適切な方法で入手が行えない対策を実施している。	・住民異動届出においては住基法第27条の規定に基づき、書面にて本人あるいは代理人による届出のみを受領することとし、受領の際は必ず本人あるいは代理人の本人確認(本人確認書類として写真付きの書類(運転免許証や住民基本台帳カードなど)、または複数点の書類(保険証など)の提示を求めて確認)及び委任状の確認を行うこととしている。 ・親権者や法定代理人については、戸籍謄抄本等の提示または本籍地の市町村へ照会して確認する。 ・任意代理人の持参した委任状の内容(委任の範囲、権限等)に不明瞭な点がある場合には委任者へ電話等で確認する。その場合、委任者の住民票または戸籍の記録をもとに本籍地・世帯構成・前住所等を聞き取る方法で本人確認を行う。 ・システムを利用する必要がある職員を特定し、ユーザIDによる識別とパスワードによる認証を実施する。また、認証後は利用機能の認可機能により、そのユーザがシステム上で利用可能な機能を制限することで不適切な方法で入手が行えない対策を実施している。 ・サービス検索・電子申請機能を利用した申請の場合においては、住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、のちに署名検証も行われるため、本人からの情報のみが送信される。また、サービス検索・電子申請機能の画面の誘導において住民に何の手続きを採し電子申請を行いたいのか理解してもらいながら操作をしていただき、たどり着いた申請フォームが何のサービスにつながるものか明示することで、住民に過剰な負担をかけることなく電子申請を実施いただけるよう措置を講じている。	事前	
令和5年2月1日	Ⅲ-2特定個人情報の入手 (情報提供音ネットワークを通じた手法を除く) リスク3入手の際の本人確認の措置の内容	・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。 ・個人番号通知書(番号法第7条)、個人番号カード(同第17条)の提示を受け、本人確認を行う。 ・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。	・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。 ・個人番号通知書(番号法第7条)、個人番号カード(同第17条)の提示を受け、本人確認を行う。 ・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。 ・サービス検索・電子申請機能を利用した申請において、住民がサービス検索・電子相談機能から個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、電子署名付与済の個人番号付電子申請データを受領した地方公共団体は署名検証(有効性確認、改ざん検知等)を実施することとなる。これにより、本人確認を実施する。	事前	
令和5年2月1日	Ⅲ-2特定個人情報の入手 (情報提供音ネットワークを通じた手法を除く) リスク3入手した特定個人情報が不正確であるリスク 特定個人情報の正確性確保の措置の内容	・特定個人情報の入力、削除及び訂正を行う際は、整合性を確保するために、入力、削除及び訂正を行な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。 ・入力、削除及び訂正作業に用いた帳票等は、当市で定める規程に基づいて管理し、保管する。 ・特定個人情報に誤りがあった際に訂正を行う場合には、特定個人情報管理責任者の許可を得て行うこととする。また、訂正した内容等については、その記録を残し、法令等により定められた期間保管する。	・特定個人情報の入力、削除及び訂正を行う際は、整合性を確保するために、入力、削除及び訂正を行な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。 ・入力、削除及び訂正作業に用いた帳票等は、当市で定める規程に基づいて管理し、保管する。 ・特定個人情報に誤りがあった際に訂正を行う場合には、特定個人情報管理責任者の許可を得て行うこととする。また、訂正した内容等については、その記録を残し、法令等により定められた期間保管する。 ・サービス検索・電子申請機能を利用した申請があった場合は、個人番号カード内の記憶領域に格納された個人番号を申請フォームに自動転記を行うことにより、不正確な個人番号の入力を抑止する措置を講じている。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年2月1日	Ⅲ-2特定個人情報の入手 (情報提供音ネットワークを通じた手法を除く) リスク4入手の際に特定個人情報が漏えい・紛失するリスク リスクに対する措置の内容	・住民からの届出書については、特定個人情報の漏洩及び紛失を防止するため、入力及び照会した後は、鍵付の書庫に保管する。 ・既存住基システムは住基ネット以外とは外部接続できない仕組みである ・住基ネットワークでの通信は全て専用回線及び専用交換装置で構成されたネットワークを介して行い、また、通信を行うごとに、意図した通信相手に接続されたことを相互に認証する仕組みを採用している。	・住民からの届出書については、特定個人情報の漏洩及び紛失を防止するため、入力及び照会した後は、鍵付の書庫に保管する。 ・既存住基システムは住基ネット以外とは外部接続できない仕組みである ・住基ネットワークでの通信は全て専用回線及び専用交換装置で構成されたネットワークを介して行い、また、通信を行うごとに、意図した通信相手に接続されたことを相互に認証する仕組みを採用している。 ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。	事前	
令和5年2月1日	Ⅲ-7特定個人情報の保管・消去 リスク1特定個人情報の漏洩・滅失・棄損リスク ⑥技術的な対策＞具体的な対策の内容	＜本市における措置＞ ①ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォールを設置している。 ②コンピュータウイルス対策ソフトウェアを導入している。 ③OSには随時パッチ適用を実施している。 ＜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。	＜本市における措置＞ ①ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォールを設置している。 ②コンピュータウイルス対策ソフトウェアを導入している。 ③OSには随時パッチ適用を実施している。 ＜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。 ＜サービス検索・電子申請機能＞ ①サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。	事前	
令和5年2月1日	Ⅲ-7特定個人情報の保管・消去 リスク2特定個人情報が古い情報のまま保管され続けるリスク リスクに対する措置の内容	住基法第14条第1項(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実施することにより、住民基本台帳の正確な記録を確保する。	住基法第14条第1項(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実施することにより、住民基本台帳の正確な記録を確保する。 サービス検索・電子申請機能を利用した届出については、LGWAN接続端末に個人番号付電子申請データの一時保管として使用するが、一時保管中に再申請や申請情報の訂正が発生した場合は古い情報で審査等を行わないよう、履歴管理を行う。	事前	