# 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 | 高知市　住民票に関する事務　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

高知市は，住民票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，そ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十分な措置を行い，もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

| 特記事項 | |
| --- | --- |

## 評価実施機関名

高知市長

## 個人情報保護委員会　承認日　【行政機関等のみ】

## 公表日

［令和6年10月　様式4］

# 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 | 住民基本台帳事務 |
| ②事務の内容　※ | 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，市町村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に行うものであり，市町村において，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なるものである。<br>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）を都道府県と共同して構築している。<br>高知市は，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）<br>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<br>②転入届，転居届，転出届，世帯変更届等の届出（電子申請機能による申請管理システムからの電子申請データを基幹システムに取り込むことを含む）又は職権に基づく住民票の記載，消除又は記載の修正<br>③住民基本台帳の正確な記録を確保するための措置<br>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<br>⑤本人又は同一の世帯に属する者の請求による住民票の写し等の交付<br>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<br>⑦地方公共団体情報システム機構（以下「機構」という。）への本人確認情報の照会<br>⑧住民からの請求に基づく住民票コードの変更<br>⑨個人番号の通知及び個人番号カードの交付<br>⑩個人番号等を用いた本人確認<br>⑪住民票の記載事項を庁内連携システム等を介して庁内連携し，住民に関する市町村事務の処理の基礎として利用<br>⑫他団体からの要求に基づき，情報提供ネットワークシステムを介して住民票関係情報を提供<br><br>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，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に規定する個人番号、個人番号カード、特定個人情報の提供等に関する命令（平成26年11月20日総務省令第85号）（以下「個人番号カード命令」という。）第35条（個人番号通知書，個人番号カード関連事務の委任）により機構に対する事務の一部の委任が認められている。<br>そのため，当該事務においては，事務を委任する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 | [　30万人以上　] ＜選択肢＞<br>1) 1,000人未満　2) 1,000人以上1万人未満<br>3) 1万人以上10万人未満　4) 10万人以上30万人未満<br>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 | 住民基本台帳システム（既存住民基本台帳システム） |
| ②システムの機能 | 1. 住民基本台帳の管理<br>・異動処理機能および，異動入力された個人データを住民基本台帳として記録する。<br>2. 住民票コードの通知<br>・住民票コード通知書を発行する。<br>3. 各種証明書の発行<br>・住民票の写し，記載事項証明書などの各種証明書を発行する。<br>4. 住基ネットとの連携<br>・住基ネットへの本人確認情報の連携，転出証明書情報などの市町村間の通知，個人番号の要求，通知カード情報の送付を実施する。<br>5. 庁内連携データの作成<br>・住民票の記載事項を他のシステムに庁内連携する為のデータを作成する。 |
| 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<br>[ ○ ] 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<br>[ ○ ] 宛名システム等　[　] 税務システム<br>[ ○ ] その他　（ 中継サーバ，申請管理システム　） |

| 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） |
| ②システムの機能 | 1．本人確認情報の更新<br>・既存住民基本台帳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CSの本人確認情報を更新し，都道府県知事が管理する都道府県サーバへ更新情報を送信する。<br>2．本人確認<br>・特例転入処理や住民票の写しの広域交付などを行う際，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。<br>3．個人番号カードを利用した転入（特例転入）<br>・個人番号カードの交付を受けている者等の転入が予定される場合に、転出証明書情報をCSを通じて受け取り、その者に係る転入の届出を受け付けた際に、個人番号カードを用いて転入処理を行う（一定期間経過後も転入の届出が行われない場合は、受け取った転出証明書情報を消去する。）。<br>4．本人確認情報検索<br>・統合端末において入力された住民票コード，個人番号又は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。<br>5．機構への情報照会<br>・機構の管理する住基ネットの全国サーバ（以下「全国サーバ」という。）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。<br>6．本人確認情報整合<br>・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機構が全国サーバにおいて保有している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。<br>7．送付先情報通知<br>・個人番号の通知に係る事務の委任先である機構において，住民に対して番号通知書類(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，既存住民基本台帳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，機構が設置・管理する個人番号カード管理システム（以下「個人番号カード管理システム」という。）に通知する。<br>8．個人番号カード管理システムとの情報連携<br>・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<br>[　] 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<br>[　] 宛名システム等　　[　] 税務システム<br>[　] その他　（　） |

| システム3 | |
|---|---|
| ①システムの名称 | 中間サーバ |
| ②システムの機能 | 1．符号管理<br>・符号の取得を行う。<br>・取得した符号と団体内統合宛名番号の紐付け管理を行う。<br><br>2．情報照会<br>・情報保有機関が保有する特定個人情報（連携対象）の情報照会を行う。<br>・情報提供ネットワークシステムを通じた他情報保有機関が保有する特定個人情報（連携対象）の提供を求める。<br><br>3．情報提供<br>・情報提供対象となる特定個人情報（連携対象）の保有・管理を行う。<br>・他情報保有機関から特定個人情報（連携対象）の提供の求めに対して，情報提供ネットワークシステムを通じて保有する情報を提供する。<br><br>4．情報提供等記録管理<br>・情報照会者と情報提供者との間で行った特定個人情報（連携対象）の情報照会及び情報提供に係る記録の管理を行う。<br>・各情報保有機関の個人情報保護条例に基づき，情報提供等記録の開示請求に対応する。<br><br>5．副本管理<br>・情報提供データベースへ特定個人情報（連携対象）を副本として登録する。<br>・情報提供データベースに蓄積された副本の検索及び削除を行う。 |
| 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<br>[　 ] 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<br>[　 ] 宛名システム等　　[　 ] 税務システム<br>[　 ] その他　（　　） |

| システム4 | |
|---|---|
| ①システムの名称 | 団体内統合利用番号兼連携サーバ（連携サーバ） |
| ②システムの機能 | 1．団体内統合宛名番号の管理<br>・各システムの宛名情報を取り込み，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。<br><br>2．情報提供（中間サーバに提供情報を連携する）<br>・中間サーバに連携する各業務システムの情報を集約して管理する。<br>・蓄積した情報を中間サーバに連携する。<br><br>3．情報照会（中間サーバに情報照会を依頼する）<br>・各業務の宛名番号で対象者を検索し，中間サーバに対して他情報保有機関が保有する特定個人情報（連携対象）の照会を依頼し，結果を表示する。 |
| 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<br>[　 ] 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<br>[　 ] 宛名システム等　　[　 ] 税務システム<br>[　 ] その他　（　　） |

| システム5 | |
|---|---|
| ①システムの名称 | 中継サーバ |
| ②システムの機能 | 1. 既存システム連携機能<br>・既存住民基本台帳システムから証明書情報を連携する機能<br><br>2. コンビニ交付機能<br>・証明書交付センター（J-LISが運営管理）からの要求に応じて証明書自動交付を行う機能 |
| 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<br>[　] 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<br>[　] 宛名システム等　[　] 税務システム<br>[○] その他　（ J-LIS証明書交付センター　） |

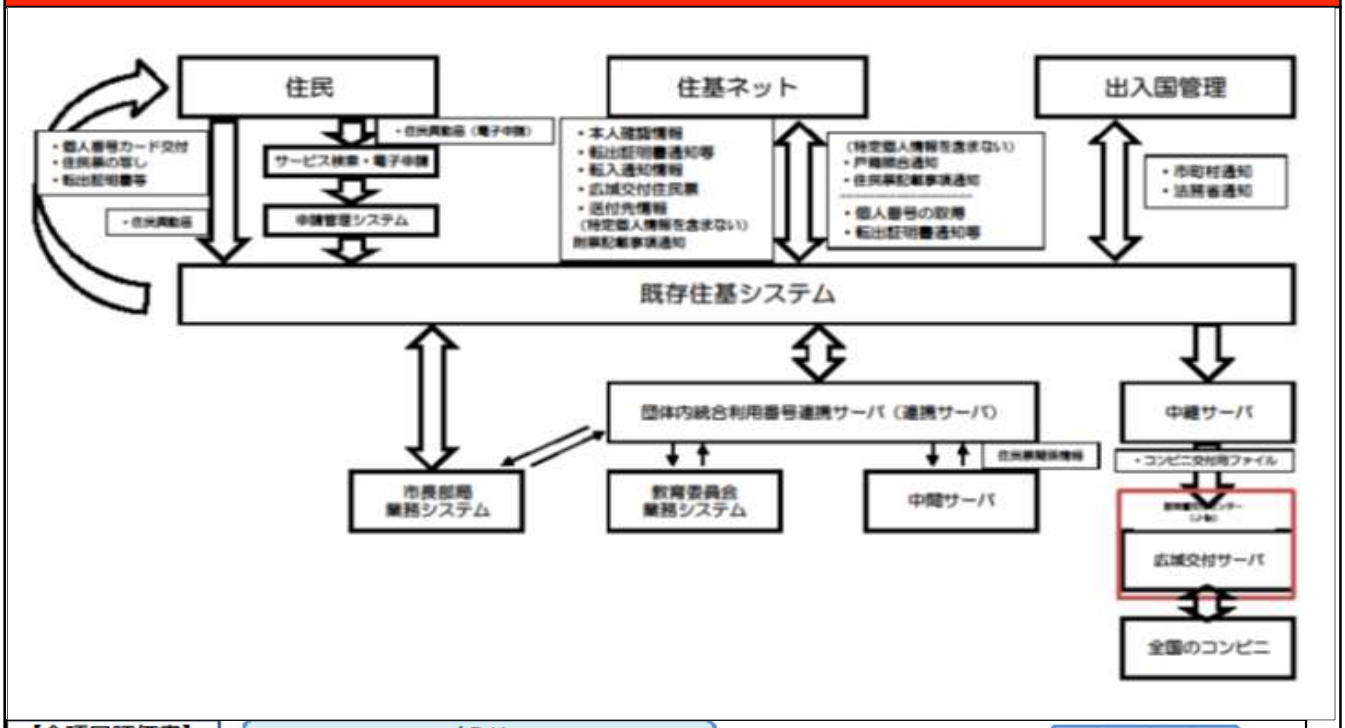
| システム6 | |
|---|---|
| ①システムの名称 | サービス検索・電子申請機能 |
| ②システムの機能 | 1. 住民向け機能<br>・自らが受けることができるサービスをオンラインで検索及び申請ができる機能<br><br>2. 地方公共団体向け機能<br>・住民が電子申請を行った際の申請データ取得画面又は機能を、地方公共団体に公開する機能 |
| ③他のシステムとの接続 | [　] 情報提供ネットワークシステム　[　] 庁内連携システム<br>[　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム<br>[　] 宛名システム等　[　] 税務システム<br>[○] その他　（ 申請管理システム　） |

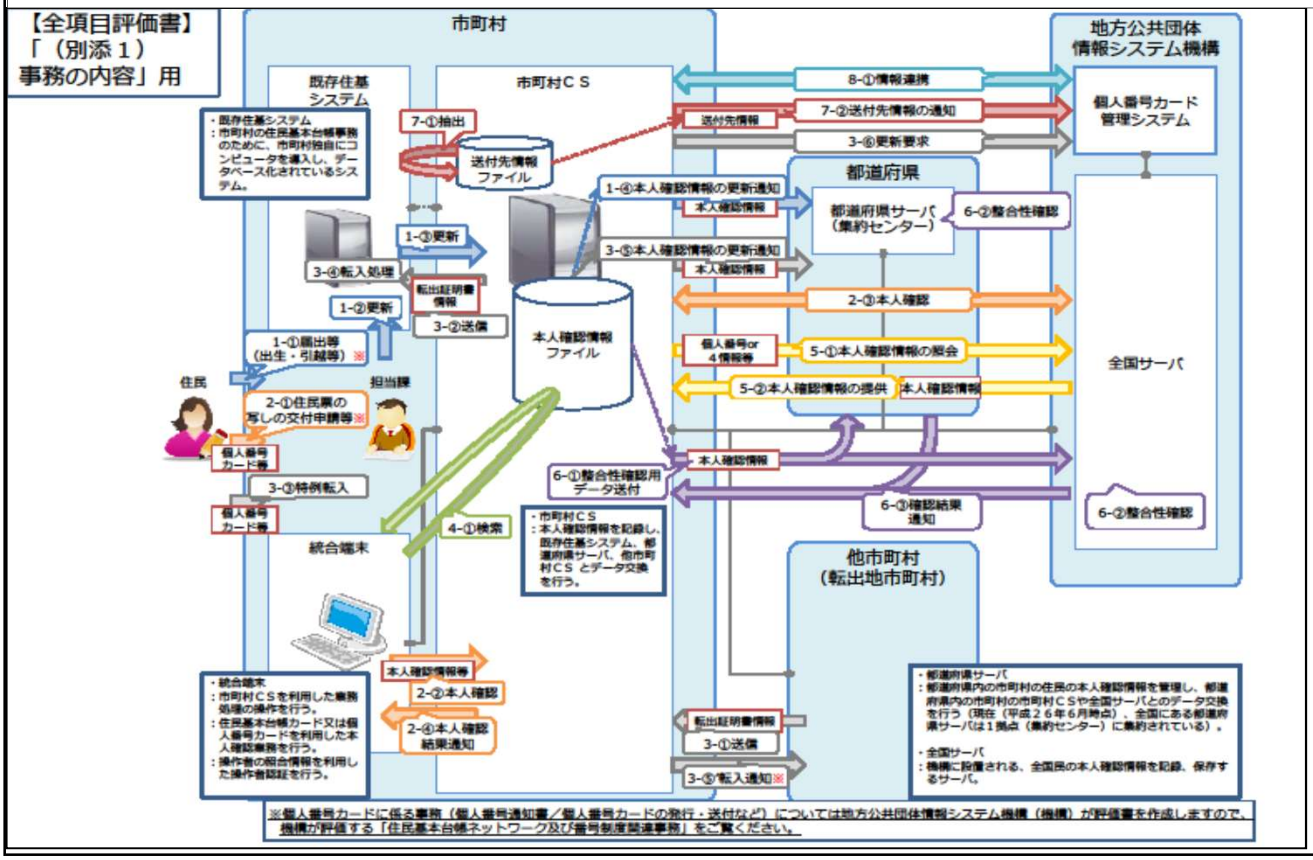
| システム7 | |
|---|---|
| ①システムの名称 | 申請管理システム |
| ②システムの機能 | 1. サービス検索・電子申請機能で受け付けた電子申請を申請管理システムに連携する機能<br><br>2. 連携サーバから連携された電子申請データを参照・保存する機能 |
| ③他のシステムとの接続 | [　] 情報提供ネットワークシステム　[　] 庁内連携システム<br>[　] 住民基本台帳ネットワークシステム　[○] 既存住民基本台帳システム<br>[　] 宛名システム等　[　] 税務システム<br>[○] その他　（ サービス検索・電子申請機能　） |

| 3. 特定個人情報ファイル名 | |
|---|---|
| （1）住民基本台帳ファイル　（2）本人確認情報ファイル　（3）送付先情報ファイル　（4）コンビニ交付用ファイル | |
| **4. 特定個人情報ファイルを取り扱う理由** | |
| ①事務実施上の必要性 | （1）住民基本台帳ファイル<br>本市では，住民基本台帳事務がシステム化されており，当該特定個人情報ファイルは，住民基本台帳の原本として取り扱われるものである。<br><br>（2）本人確認情報ファイル<br>本人確認情報ファイルは，転出入があった場合等にスムーズな住民情報の処理を行うため，また全国的な本人確認手段として，1つの市町村内にとどまらず全地方公共団体で本人確認情報を正確かつ統一的に記録・管理することを目的として，以下の用途に用いられる。<br>①住基ネットを用いて市町村の区域を越えた住民基本台帳に関する事務の処理を行うため，区域内の住民に係る最新の本人確認情報を管理する。<br>②都道府県に対し，本人確認情報の更新情報を通知する。<br>③申請・届出の際に提示された個人番号カード等を用いた本人確認を行う。<br>④個人番号カードを利用した転入手続きを行う。<br>⑤住民基本台帳に関する事務において，本人確認情報を検索する。<br>⑥都道府県知事保存本人確認情報及び機構保存本人確認情報との整合性を確認する。<br><br>（3）送付先情報ファイル<br>市町村長が個人番号を指定した際は全付番対象者に個人番号を通知するものとされている（番号法第7条第1項）。個人番号通知書による番号の通知及び個人番号カード交付通知書の送付については，事務効率化等の観点から，市町村から機構に委任しており，機構に個人番号通知書及び交付申請書の送付先情報を提供する。（個人番号，個人番号カード命令第35条（個人番号通知書・個人番号カード関連事務の委任）により機構に対する事務の一部の委任が認められている。）<br><br>（4）コンビニ交付用ファイル<br>市役所開庁時間外も含め，窓口に出向かなくても証明書交付サービスの提供を実施するため，個人番号カードを利用してコンビニに設置されているマルチコピー機から住民票の写し等証明書を発行するため，取り扱う。 |
| ②実現が期待されるメリット | （1）住民基本台帳ファイル<br>住民基本台帳ファイルについては，住民基本台帳の正確かつ効率的な管理が可能となる。<br>（2）本人確認情報ファイル<br>住民票の写し等に代えて本人確認情報を利用することにより，これまでに窓口で提供が求められていた行政機関が発行する添付書類（住民票の写し等）の省略が図られ，もって国民・住民の負担軽減（各機関を訪問し，証明書等を入手する金銭的，時間的コストの節約）につながることが見込まれる。<br>また，個人番号カードによる本人確認，個人番号の真正性確認が可能となり，行政事務の効率化に資することが期待される。<br>（3）送付先情報ファイル<br>市町村長が個人番号を指定した際は全付番対象者に個人番号を通知する。<br>（4）コンビニ交付用ファイル<br>市役所開庁時間外も含め，窓口に出向かなくても証明書交付サービスの提供を実施するため，個人番号カードを利用してコンビニに設置されているマルチコピー機から住民票の写し等証明書の発行が可能となる。 |

| 5. 個人番号の利用 ※ | |
|---|---|
| 法令上の根拠 | 1. 番号法（平成25年5月31日法律第27号）<br>・第7条（指定及び通知）<br>・第16条（本人確認の措置）<br>・第17条（個人番号カードの交付等）<br><br>2. 住基法（昭和42年7月25日法律第81号）<br>・第5条（住民基本台帳の備付け）<br>・第6条（住民基本台帳の作成）<br>・第7条（住民票の記載事項）<br>・第8条（住民票の記載等）<br>・第12条（本人等の請求に係る住民票の写し等の交付）<br>・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）<br>・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）<br>・第22条（転入届）<br>・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）<br>・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）<br>・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）<br>・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＞<br>1) 実施する<br>2) 実施しない<br>3) 未定 |
| ②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第十九条第八号に基づく利用特定個人情報の提供に関する命令（令和6年5月27 日デジタル庁・総務省令第9号。以下「番号法第19 条第8号に基づく主務省令」という。）<br>（情報提供の根拠）<br>・番号法第19 条第8号に基づく主務省令第2条の別表（1，2，3，5，7，11，13，15，20，28，37，39，48，53，57，58，59，63，65，66，69，73，75，76，81，83，84，86，87，91，92，96，106，108，110，112，115，118，124，129，130，132，136，137，138，141，142，144，149，150，151，152，155，156，158，160，163，164，165，166）の項<br><br>（情報照会の根拠）<br>・なし |
| **7. 評価実施機関における担当部署** | |
| ①部署 | 市民協働部　中央窓口センター |
| ②所属長の役職名 | 中央窓口センター所長 |
| **8. 他の評価実施機関** | |
| ― | |

## （別添1）事務の内容


住民
住基ネット
出入国管理
既存住基システム
団体内統合利用番号連携サーバ（連携サーバ）
中継サーバ
市長部局
業務システム
教育委員会
業務システム
中間サーバ
広域交付サーバ
全国のコンビニ


【全項目評価書】
「（別添１）
事務の内容」用
市町村
既存住基
システム
市町村ＣＳ
地方公共団体
情報システム機構
個人番号カード
管理システム
都道府県
都道府県サーバ
（集約センター）
全国サーバ
他市町村
（転出地市町村）
住民
担当課
統合端末
本人確認情報
ファイル
送付先情報
ファイル
7-①抽出
1-③更新
1-②更新
3-④転入処理
3-②送信
1-①届出等
（出生・引越等）
2-①住民票の
写しの交付申請等
個人番号
カード等
3-③特例転入
4-①検索
8-①情報連携
7-②送付先情報の通知
3-⑥更新要求
1-④本人確認情報の更新通知
3-⑤本人確認情報の更新通知
6-②整合性確認
2-③本人確認
5-①本人確認情報の照会
5-②本人確認情報の提供
6-①整合性確認用
データ送付
6-①確認結果
通知
本人確認情報等
2-②本人確認
2-④本人確認
結果通知
転出証明書情報
3-①送信
3-⑤転入通知
※個人番号カードに係る事務（個人番号通知書／個人番号カードの発行・送付など）については地方公共団体情報システム機構（機構）が評価書を作成し次第ので、機構が評価する「住民基本台帳ネットワーク及び番号制度関連事務」をご覧ください。

（備考）

1．本人確認情報の更新に関する事務
1-①.住民より転入，転出，転居，出生，死亡等の届出等を受け付ける（※特定個人情報を含まない）。
1-②.住民基本台帳（既存住民基本台帳システム）を更新する。
1-③.住民基本台帳にて更新された住民情報を基に，市町村CSの本人確認情報を更新する。
1-④.市町村CSにて更新された本人確認情報を都道府県サーバに通知する。

2．本人確認に関する事務
2-①.住民より，住民票の写しの交付申請等，本人確認が必要となる申請を受け付ける（※特定個人情報を含まない）。
2-②,③.統合端末において，住民から提示された個人番号カードに記録された住民票コード（又は法令で定めた書類に記載された4情報）を送信し，市町村CSを通じて，全国サーバに対して本人確認を行う。
2-④.全国サーバより，市町村CSを通じて，本人確認結果を受領する。

3．個人番号カードを利用した転入（特例転入）
3-①.市町村CSにおいて転出地市町村より転出証明書情報を受信する。
3-②.既存住基システムにおいて、市町村CSから転出証明書情報を受信する。
3-③.転入手続を行う住民から提示された個人番号カードを利用して本人確認(「2．本人確認」を参照)を行う。
※転出証明書情報に記載の転出の予定年月日から30日後までに転入手続が行われない場合には、当該転出証明書情報を消去する。
※3-③の転入手続時に転出証明書情報を受信していない場合又は消去している場合には、統合端末から、市町村CSを経由して転出地市町村に対し転出証明書情報の送信依頼を行い(※特定個人情報を含まない)、その後、3-①・②を行う。
3-④.既存住基システムにおいて、転入処理を行う。

4．本人確認情報検索に関する事務
4-①.住民票コード，個人番号又は4情報の組み合わせをキーワードとして，市町村CSの本人確認情報を検索する。
（検索対象者が高知県の住所地市町村以外の場合は都道府県サーバ，他都道府県の場合は全国サーバに対してそれぞれ検索の要求を行う。）

5．機構への情報照会に係る事務
5-①.機構に対し，個人番号又は4情報等をキーワードとした本人確認情報の照会を行う。
5-②.機構より，当該個人の本人確認情報を受領する。

6．本人確認情報整合に係る事務
6-①.市町村CSより，都道府県サーバ及び全国サーバに対し，整合性確認用の本人確認情報を送付する。
6-②.都道府県サーバ及び住基全国サーバにおいて，市町村CSより受領した整合性確認用の本人確認情報を用いて保有する本人確認情報の整合性確認を行う。
6-③.都道府県サーバ及び全国サーバより，市町村CSに対して整合性確認結果を通知する。

7．送付先情報通知に関する事務
7-①.既存住民基本台帳システムより，個人番号カードの交付対象者の送付先情報を抽出する。
7-②.個人番号カード管理システムに対し，送付先情報を通知する。

8．個人番号カード管理システムとの情報連携
8-①.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。

# 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＞<br>1) システム用ファイル<br>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＞<br>1) 1万人未満<br>2) 1万人以上10万人未満<br>3) 10万人以上100万人未満<br>4) 100万人以上1,000万人未満<br>5) 1,000万人以上 |
| ③対象となる本人の範囲 ※ | | 高知市の住民(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)。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消除された者(以下「消除者」という。)を含む。 |
| | その必要性 | 当該特定個人情報ファイルは，住民基本台帳の原本であり，住基法に基づき，上記範囲の住民に関する正確な記録及び住民に関する記録の適正な管理を行う責務があるため。 |
| ④記録される項目 | | [　　100項目以上　　] ＜選択肢＞<br>1) 10項目未満　2) 10項目以上50項目未満<br>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<br>[ ○ ] 個人番号　[　] 個人番号対応符号　[ ○ ] その他識別情報(内部番号)<br>・連絡先等情報<br>[ ○ ] 4情報(氏名、性別、生年月日、住所)　[　] 連絡先(電話番号等)<br>[ ○ ] その他住民票関係情報<br>・業務関係情報<br>[　] 国税関係情報　[　] 地方税関係情報　[　] 健康・医療関係情報<br>[ ○ ] 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<br>[　] 生活保護・社会福祉関係情報　[ ○ ] 介護・高齢者福祉関係情報<br>[　] 雇用・労働関係情報　[ ○ ] 年金関係情報　[ ○ ] 学校・教育関係情報<br>[　] 災害関係情報<br>[ ○ ] その他　(　住民基本台帳カード及び個人番号カード等情報　) |
| | その妥当性 | 住基法第7条に規定する住民票の記載事項であるため。 |
| | 全ての記録項目 | 別添2を参照。 |
| ⑤保有開始日 | | 平成27年7月17日 |
| ⑥事務担当部署 | | 市民協働部　中央窓口センター |

| 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<br>[ ○ ] 評価実施機関内の他部署 （ 保険医療課，子育て給付課，介護保険課，中央窓口センター(年金担当) ）<br>[ ○ ] 行政機関・独立行政法人等 （ 法務省 ）<br>[ ○ ] 地方公共団体・地方独立行政法人 （ 地方公共団体情報システム機構 ）<br>[ ○ ] 民間事業者 （ ）<br>[ ○ ] その他 （ 高知市教育委員会，高知市選挙管理委員会 ） |
| 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<br>[ ] 電子メール [ ○ ] 専用線 [ ] 庁内連携システム<br>[ ] 情報提供ネットワークシステム<br>[ ○ ] その他 （ 住基ネット，サービス検索・電子申請機能，申請管理システム ） |
| ③入手の時期・頻度 | | (1)個別的に本人から入手する事務<br>・転入，出生等の異動に伴う申請・届出時<br>（機構からの個人番号の入手も含む）<br><br>(2)他の事務の所管部署から入手する事務<br>・個別記載事項(国民年金被保険者資格)<br>所管部署における本人からの申請時<br>・個別記載事項(国保被保険者資格) 月1回<br>・個別記載事項(児童手当受給資格) 月1回<br>・個別記載事項(介護被保険者資格) 日1回<br>・個別記載事項(後期高齢者医療被保険者資格) 日1回<br>・個別記載事項(選挙人名簿登録の旨)年4回 (選挙人名簿の定時登録時(年4回))<br>・外国人記載事項 日1回 (法務省連携) |
| ④入手に係る妥当性 | | 個別的に本人から入手する情報は，住基法に規定される届出によるものである。他の事務の担当部署から入手する情報は，住基法第7条に規定される住民票の記載事項のうち，他部署で管理する情報であり，情報の更新タイミングやシステム間で情報連携の仕組みに応じて本市において適切と思われる時期・頻度で入手しているものである。 |
| ⑤本人への明示 | | 住民票の記載事項として住基法第7条に規定されているものである。 |
| ⑥使用目的 ※ | | 住基法に基づく住民に関する正確な記録及び住民に関する記録の適正な管理のため。 |
| | 変更の妥当性 | 非該当 |
| ⑦使用の主体 | 使用部署 ※ | 市民協働部 中央窓口センター |
| | 使用者数 | [ 100人以上500人未満 ]<br>＜選択肢＞<br>1) 10人未満 2) 10人以上50人未満<br>3) 50人以上100人未満 4) 100人以上500人未満<br>5) 500人以上1,000人未満 6) 1,000人以上 |
| ⑧使用方法 ※ | | ・異動処理機能及び異動入力された個人データを住民基本台帳として記録する。<br>・住民票コード通知書を発行する。<br>・住民票の写し，記載事項証明書などの各種証明書を発行する。<br>・住基ネットへの本人確認情報の連携，転出証明書情報などの市町村間の通知，個人番号の要求，個人番号通知書の送付を行う。<br>・住民票の記載事項を庁内連携する為の連携データを作成する。 |
| | 情報の突合 ※ | 異動処理(転入)時に，転出証明書に記載された個人番号と除票者の個人番号を突合して，再転入者であるかを確認する。 |
| | 情報の統計分析 ※ | 特定個人情報を用いた統計や情報の分析は行わない。 |
| | 権利利益に影響を与え得る決定 ※ | 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<br>（ 2 ） 件 |
| **委託事項1** | | 住民票の写し等の交付受付及び発行業務 |
| ①委託内容 | | 住民票の写し等の交付受付及び発行業務 |
| 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 ※ | 「Ⅱ．2．③対象となる本人の範囲」に同じ |
| | その妥当性 | 当該委託事務は，住民基本台帳に記録された全員を対象とした事務を行う必要があるため。 |
| 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。）<br>[ ]フラッシュメモリ [ ]紙<br>[ ○ ]その他 （ 特定個人情報ファイルの直接の提供は行わず，既存住民基本台帳システムの端末を利用して，特定個人情報を取り扱う。 ） |
| ⑤委託先名の確認方法 | | 高知市行政情報公開条例（平成12年条例第68号）に基づき，契約関係書類の公開請求が可能。 |
| ⑥委託先名 | | テンプスタッフフォーラム株式会社 |
| 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** | | 情報システムの運用支援及び改修業務 |
| ①委託内容 | | 既存住民基本台帳システムの運用支援及び改修業務 |
| 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＞<br>1）特定個人情報ファイルの全体<br>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＞<br>1）1万人未満<br>2）1万人以上10万人未満<br>3）10万人以上100万人未満<br>4）100万人以上1,000万人未満<br>5）1,000万人以上 |
| | 対象となる本人の範囲　※ | 「Ⅱ．2．③対象となる本人の範囲」に同じ |
| | その妥当性 | 住民基本台帳ファイルを含む既存住民基本台帳システムの運用保守を委託しているため。<br>（システムの運用保守は，高度で専門的な知識・技能を要するため，職員による実施が困難） |
| ③委託先における取扱者数 | | ［　　10人以上50人未満　　］　＜選択肢＞<br>1）10人未満　2）10人以上50人未満<br>3）50人以上100人未満　4）100人以上500人未満<br>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。）<br>［　］フラッシュメモリ　［　］紙<br>［ ○ ］その他　（ システムを構成するサーバ及び端末機を使用して特定個人情報を取り扱う。　） |
| ⑤委託先名の確認方法 | | ・高知市行政情報公開条例に基づき，契約関係書類の公開請求が可能。<br>・契約の都度，高知市ホームページで業務名，契約相手方，契約期間，契約金額等を公表。 |
| ⑥委託先名 | | 富士通Japan株式会社　四国公共ビジネス部 |
| 再委託 | ⑦再委託の有無　※ | ［　　再委託する　　］　＜選択肢＞<br>1）再委託する　2）再委託しない |
| | ⑧再委託の許諾方法 | 業務委託契約書に規定する手続に基づき，委託先からの再委託承認申請書を審査のうえ，再委託承諾通知を行う。 |
| | ⑨再委託事項 | 既存住民基本台帳システムの運用支援及び改修業務 |

| 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 （ 2 ）件<br>[ ] 行っていない |
| **提供先1** | 番号第十九条第八号に基づく利用特定個人情報の提供に関する命令第二条の表に規定する住民票関係情報の照会者 （詳細は別紙1参照） |
| ①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第十九条第八号に基づく利用特定個人情報の提供に関する命令（令和6年5月27 日デジタル庁・総務省令第9号。以下「番号法第19 条第8号に基づく主務省令」という。）<br><br>（情報提供の根拠）<br>・番号法第19 条第8号に基づく主務省令第2条の別表（1，2，3，5，7，11，13，15，20，28，37，39，48，53，57，58，59，63，65，66，69，73，75，76，81，83，84，86，87，91，92，96，106，108，110，112，115，118，124，129，130，132，136，137，138，141，142，144，149，150，151，152，155，156，158，160，163，164，165，166）の項 |
| ②提供先における用途 | 別紙1参照 |
| 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） |
| 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 ]<br>＜選択肢＞<br>1）1万人未満<br>2）1万人以上10万人未満<br>3）10万人以上100万人未満<br>4）100万人以上1,000万人未満<br>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 | 「Ⅱ．2．③対象となる本人の範囲」に同じ |
| ⑥提供方法 | [ ○ ] 情報提供ネットワークシステム [ ] 専用線<br>[ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。）<br>[ ] フラッシュメモリ [ ] 紙<br>[ ○ ] その他 （ 住基ネット ） |
| ⑦時期・頻度 | 情報提供ネットワーク・システム及び住基ネットにより特定個人情報の提供依頼がある都度。 |
| **提供先2** | 高知市教育委員会 |
| ①法令上の根拠 | 高知市個人番号の利用及び特定個人情報の提供に関する条例（平成27年条例第105号。以下「独自利用条例」という。） |
| ②提供先における用途 | 就学援助に関する事務 |
| 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）<br>宛名基本情報（個人番号，既存宛名番号，氏名，性別，生年月日，住所等） |
| ④提供する情報の対象となる本人の数 | [ 1万人以上10万人未満 ]<br>＜選択肢＞<br>1）1万人未満<br>2）1万人以上10万人未満<br>3）10万人以上100万人未満<br>4）100万人以上1,000万人未満<br>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 | 高知市に居住し，高知市立学校等に在学する児童・生徒及びその保護者 |
| ⑥提供方法 | [ ] 情報提供ネットワークシステム [ ] 専用線<br>[ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。）<br>[ ] フラッシュメモリ [ ] 紙<br>[ ○ ] その他 （ 庁内連携システム ） |
| ⑦時期・頻度 | 住民票関係情報については，就学援助の申請に合わせて随時<br>宛名基本情報については，異動情報を日1回 |

| | |
|---|---|
| **移転先1** | 防災政策課，市民税課，資産税課，税務管理課，介護保険課，保険医療課，障がい福祉課，福祉管理課，第一福祉課，第二福祉課，高齢者支援課，地域保健課，健康増進課，保育幼稚園課，子育て給付課，子ども家庭支援センター，母子保健課，住宅政策課，市街地整備課 |
| ①法令上の根拠 | 住民基本台帳は，住基法第1条に基づき住民に関する事務の処理の基礎とされており，台帳を備える市町村の執行機関が，当該市町村の住民の住民票に係る情報（個人番号を含む本人確認情報もその一部）をその事務処理に利用できる。 |
| ②移転先における用途 | 個人番号利用事務に係る各業務システムをおいて，個人番号，氏名，性別，生年月日，住所等を宛名基本情報として利用する。 |
| ③移転する情報 | 宛名基本情報（個人番号，既存宛名番号，氏名，性別，生年月日，住所等） |
| 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　] <br> ＜選択肢＞<br>1）1万人未満<br>2）1万人以上10万人未満<br>3）10万人以上100万人未満<br>4）100万人以上1,000万人未満<br>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 | 「Ⅱ．2．③対象となる本人の範囲」に同じ |
| ⑥移転方法 | [ ○ ] 庁内連携システム　　[　] 専用線<br>[　] 電子メール　　[　] 電子記録媒体（フラッシュメモリを除く。）<br>[　] フラッシュメモリ　　[　] 紙<br>[　] その他　（　　） |
| ⑦時期・頻度 | 宛名基本情報については，異動情報を日1回 |
| **移転先2** | 介護保険課，保険医療課，健康福祉総務課，障がい福祉課，福祉管理課，第一福祉課，第二福祉課，高齢者支援課，地域保健課，健康増進課，保育幼稚園課，子育て給付課，子ども家庭支援センター，母子保健課，住宅政策課 |
| ①法令上の根拠 | 独自利用条例第4条（個人番号の利用に係る事務） |
| ②移転先における用途 | 住民基本台帳登録情報の確認 |
| ③移転する情報 | 住民票関係情報（住基法第7条第4号に規定する事項） |
| 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　] <br> ＜選択肢＞<br>1）1万人未満<br>2）1万人以上10万人未満<br>3）10万人以上100万人未満<br>4）100万人以上1,000万人未満<br>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 | 「Ⅱ．2．③対象となる本人の範囲」に同じ |
| ⑥移転方法 | [　] 庁内連携システム　　[　] 専用線<br>[　] 電子メール　　[　] 電子記録媒体（フラッシュメモリを除く。）<br>[　] フラッシュメモリ　　[　] 紙<br>[ ○ ] その他　（ 住民基本台帳閲覧端末　　） |
| ⑦時期・頻度 | 各事務で住民基本台帳情報の確認が必要な際に随時。 |

## 6. 特定個人情報の保管・消去

| | | |
|---|---|---|
| ①保管場所　※ | | ＜高知市における措置＞<br>・カメラ監視付きの入退室管理を行っているサーバ室内で，鍵付き専用ラックに搭載されたサーバ内に保管。<br>・サーバへのアクセスは，ID／パスワードによる認証が必要。<br>・システム内のデータは，セキュリティゲートにて入退館管理をしている建物のうち，さらに厳格な入退室管理を行っている区画に設置したサーバ内に保管している。<br>・外部記憶媒体は，施錠できるキャビネットに保管している。<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・中間サーバ・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。<br>・特定個人情報は，サーバ室に設置された中間サーバ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。<br><br>＜ガバメントクラウドにおける措置＞<br>①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAP のリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。<br>・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。<br>・日本国内でのデータ保管を条件としていること。<br>②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 |
| ②保管期間 | 期間 | ［　　20年以上　　］<br>＜選択肢＞<br>1）1年未満　2）1年　3）2年<br>4）3年　5）4年　6）5年<br>7）6年以上10年未満　8）10年以上20年未満　9）20年以上<br>10）定められていない |
| | その妥当性 | 住民基本台帳は，消除者についても記録を保持しておく必要があるため，実質永年保管となる。 |
| ③消去方法 | | ＜高知市における措置＞<br>・サーバ内の特定個人情報については，サーバの機器更新時等に完全に消去する。<br>・バックアップ媒体については，破砕処理を実施。<br>・申請書等の紙媒体については，焼却処理を行う。<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・特定個人情報の消去は高知市からの操作によって実施されるため，通常，中間サーバ・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。<br>・ディスク交換やハード更改等の際は，中間サーバ・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完全に消去を行う。<br><br>＜申請管理システムにおける措置＞<br>・申請管理システムに記録した個人番号付電子申請データは，データ連携後に速やかに完全消去する。<br>・外部記憶媒体に一時的に記録した場合は、個人番号付電子申請データを使用の都度速やかに完全消去する。<br><br>＜ガバメントクラウドにおける措置＞<br>①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。<br>②クラウド事業者がHDD やSSD などの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001 等にしたがって確実にデータを消去する。<br>③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 |

## 7. 備考

―

# 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　　] ＜選択肢＞<br>1) システム用ファイル<br>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＞<br>1) 1万人未満<br>2) 1万人以上10万人未満<br>3) 10万人以上100万人未満<br>4) 100万人以上1,000万人未満<br>5) 1,000万人以上 |
| ③対象となる本人の範囲 ※ | | 高知市の住民(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)消除者を含む(死亡による消除を除く。)。 |
| | 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・提供する必要があるため。 |
| ④記録される項目 | | [　　100項目以上　　] ＜選択肢＞<br>1) 10項目未満　2) 10項目以上50項目未満<br>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<br>[ ○ ] 個人番号　[　] 個人番号対応符号　[　] その他識別情報(内部番号)<br>・連絡先等情報<br>[ ○ ] 4情報(氏名、性別、生年月日、住所)　[　] 連絡先(電話番号等)<br>[ ○ ] その他住民票関係情報<br>・業務関係情報<br>[　] 国税関係情報　[　] 地方税関係情報　[　] 健康・医療関係情報<br>[　] 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<br>[　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報<br>[　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報<br>[　] 災害関係情報<br>[　] 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<br>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)を記録する必要があるため。 |
| | 全ての記録項目 | 別添2を参照。 |
| ⑤保有開始日 | | 平成27年7月17日 |
| ⑥事務担当部署 | | 市民協働部　中央窓口センター |

| 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<br>[　] 評価実施機関内の他部署　（　）<br>[　] 行政機関・独立行政法人等　（　）<br>[　] 地方公共団体・地方独立行政法人　（　）<br>[　] 民間事業者　（　）<br>[ ○ ] 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<br>[　] 電子メール　[　] 専用線　[　] 庁内連携システム<br>[　] 情報提供ネットワークシステム<br>[ ○ ] その他　（ 住基ネット　） |
| 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が発生した都度入手する。 |
| 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，まず既存住民基本台帳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CSが既存住民基本台帳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 | 非該当 |
| ⑦使用の主体 | 使用部署 ※ | 市民協働部　中央窓口センター |
| | 使用者数 | [　100人以上500人未満　]　＜選択肢＞<br>1）10人未満　2）10人以上50人未満<br>3）50人以上100人未満　4）100人以上500人未満<br>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，既存住民基本台帳システムから当該本人確認情報の更新情報を受領し（既存住民基本台帳システム→市町村CS），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CS→都道府県サーバ）。<br>・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CS）。<br>・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。<br>・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CS→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。<br>・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 ※ | 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<br>（ 1 ） 件 |
| **委託事項1** | | 住民基本台帳ネットワークシステムの運用支援及び改修に関する業務 |
| ①委託内容 | | 住民基本台帳ネットワークシステムの運用支援及び改修に関する業務 |
| 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 ※ | 「Ⅱ．2．③対象となる本人の範囲」に同じ |
| | その妥当性 | 本人確認情報ファイルを含む住基ネットの運用保守を委託しているため。<br>（システムの運用保守は，高度で専門的な知識・技能を要するため，職員による実施が困難） |
| 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。）<br>[ ] フラッシュメモリ [ ] 紙<br>[ ○ ] その他 （ システムを構成するサーバ及び端末機を使用して特定個人情報を取り扱う。 ） |
| ⑤委託先名の確認方法 | | ・高知市行政情報公開条例に基づき，契約関係書類の公開請求が可能。<br>・契約の都度，高知市ホームページで業務名，契約相手方，契約期間，契約金額等を公表。 |
| ⑥委託先名 | | 富士通Japan株式会社 四国公共ビジネス部 |
| 再委託 | ⑦再委託の有無 ※ | [ 再委託する ] ＜選択肢＞ 1）再委託する 2）再委託しない |
| | ⑧再委託の許諾方法 | 業務委託契約書に規定する手続に基づき，委託先からの再委託承認申請書を審査のうえ，再委託承諾通知を行う。 |
| | ⑨再委託事項 | 住民基本台帳ネットワークシステムの運用支援及び改修に関する業務 |

| 5. 特定個人情報の提供・移転（委託に伴うものを除く。） | |
|---|---|
| 提供・移転の有無 | [ ○ ] 提供を行っている （ ）件 [ ] 移転を行っている （ ）件<br>[ ] 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 | 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 |
| 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） |
| 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 ]<br>＜選択肢＞<br>1）1万人未満<br>2）1万人以上10万人未満<br>3）10万人以上100万人未満<br>4）100万人以上1,000万人未満<br>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 | 「Ⅱ．2．③対象となる本人の範囲」に同じ |
| ⑥提供方法 | [ ] 情報提供ネットワークシステム [ ] 専用線<br>[ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。）<br>[ ] フラッシュメモリ [ ] 紙<br>[ ○ ] 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** | 都道府県及び機構 |
| 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 ]<br>＜選択肢＞<br>1）1万人未満<br>2）1万人以上10万人未満<br>3）10万人以上100万人未満<br>4）100万人以上1,000万人未満<br>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 | 「Ⅱ．2．③対象となる本人の範囲」に同じ |
| ⑥提供方法 | [ ] 情報提供ネットワークシステム [ ] 専用線<br>[ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。）<br>[ ] フラッシュメモリ [ ] 紙<br>[ ○ ] 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）。 |

| 6. 特定個人情報の保管・消去 | | |
|---|---|---|
| ①保管場所　※ | | ・カメラ監視付きの入退室管理を行っているサーバ室内で，鍵付き専用ラックに搭載されたサーバ内に保管。<br>・サーバへのアクセスは，ID／パスワードによる認証が必要。<br><br>＜ガバメントクラウドにおける措置＞<br>①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAP のリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。<br>・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。<br>・日本国内でのデータ保管を条件としていること。<br>②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 |
| ②保管期間 | 期間 | ［　　20年以上　　］<br>＜選択肢＞<br>1）1年未満　2）1年　3）2年<br>4）3年　5）4年　6）5年<br>7）6年以上10年未満　8）10年以上20年未満　9）20年以上<br>10）定められていない |
| | その妥当性 | ・住民票の記載の修正後の本人確認情報は，新たに記載の修正の通知を受けるまで保管する。<br>・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，住民基本台帳法施行令（昭和42年９月11日政令第292号）第34条第３項（保存）に定める期間（150年間）保管する。 |
| ③消去方法 | | ・サーバ内の特定個人情報については，サーバの機器更新時等に完全に消去する。<br>・バックアップ媒体については，破砕処理を実施。<br>・申請書等の紙媒体については，焼却処理を行う。<br><br>＜ガバメントクラウドにおける措置＞<br>①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。<br>②クラウド事業者がHDD やSSD などの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001 等にしたがって確実にデータを消去する。<br>③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 |
| 7. 備考 | | |
| ― | | |

# 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　　] ＜選択肢＞<br>1) システム用ファイル<br>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＞<br>1) 1万人未満<br>2) 1万人以上10万人未満<br>3) 10万人以上100万人未満<br>4) 100万人以上1,000万人未満<br>5) 1,000万人以上 |
| ③対象となる本人の範囲 ※ | 高知市の住民(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，当該個人番号を通知する必要がある。また，同法第17条第1項(個人番号カードの交付等)により，本人の申請により，個人番号カードを交付することとされていることから，必要に応じて交付申請書を該当者に送付する必要がある。市町村は，個人番号，個人番号カード命令第35条(個人番号通知書・個人番号カード関連事務の委任)に基づき，これらの事務の実施を機構に委任する。 |
| ④記録される項目 | [　50項目以上100項目未満　] ＜選択肢＞<br>1) 10項目未満　2) 10項目以上50項目未満<br>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<br>[ ○ ] 個人番号　[　] 個人番号対応符号　[　] その他識別情報(内部番号)<br>・連絡先等情報<br>[ ○ ] 4情報(氏名、性別、生年月日、住所)　[　] 連絡先(電話番号等)<br>[ ○ ] その他住民票関係情報<br>・業務関係情報<br>[　] 国税関係情報　[　] 地方税関係情報　[　] 健康・医療関係情報<br>[　] 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<br>[　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報<br>[　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報<br>[　] 災害関係情報<br>[ ○ ] その他　(　個人番号通知書及び交付申請書の送付先の情報　) |
| その妥当性 | (1)個人番号，4情報，その他住民票関係情報<br>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。<br><br>(2)その他(個人番号通知書及び交付申請書の送付先の情報)<br>機構に対し，個人番号，個人番号カード命令第35条(個人番号通知書・個人番号カード関連事務の委任)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 | 別添2を参照。 |
| ⑤保有開始日 | 平成27年10月5日 |
| ⑥事務担当部署 | 市民協働部　中央窓口センター |

| 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<br>[　] 評価実施機関内の他部署　（　）<br>[　] 行政機関・独立行政法人等　（　）<br>[　] 地方公共団体・地方独立行政法人　（　）<br>[　] 民間事業者　（　）<br>[ ○ ] 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<br>[　] 電子メール　[　] 専用線　[　] 庁内連携システム<br>[　] 情報提供ネットワークシステム<br>[ ○ ] その他　（ 既存住民基本台帳システム　） |
| ③入手の時期・頻度 | | 新たに個人番号の通知対象者が生じた都度入手する。 |
| 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CS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CS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 | | 個人番号カード命令第23条の2（個人番号通知書及び個人番号カードに関し機構が処理する事務）により広く国民に示されている。 |
| ⑥使用目的 ※ | | 個人番号，個人番号カード命令第35条（個人番号通知書・個人番号カード関連事務の委任）に基づく委任を受けて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行う機構に対し，個人番号通知書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 | 非該当 |
| ⑦使用の主体 | 使用部署 ※ | 市民協働部　中央窓口センター |
| | 使用者数 | [　10人未満　] ＜選択肢＞<br>1）10人未満　2）10人以上50人未満<br>3）50人以上100人未満　4）100人以上500人未満<br>5）500人以上1,000人未満　6）1,000人以上 |
| ⑧使用方法 ※ | | 既存住民基本台帳システムより個人番号の通知対象者の情報を抽出し，個人番号通知書及び交付申請書等の印刷及び送付に係る事務を個人番号，個人番号カード命令第35条（個人番号通知書・個人番号カード関連事務の委任）に基づいて委任する機構に対し提供する（既存住民基本台帳システム→市町村CS→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「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 ※ | 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<br>（ 1 ） 件 |
| **委託事項1** | | 住民基本台帳ネットワークシステムの運用支援及び改修に関する業務 |
| ①委託内容 | | 住民基本台帳ネットワークシステムの運用支援及び改修に関する業務 |
| 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 ※ | 「Ⅱ．2．③対象となる本人の範囲」に同じ |
| | その妥当性 | 送付先情報ファイルを含む住基ネットの運用保守を委託しているため。<br>（システムの運用保守は，高度で専門的な知識・技能を要するため，職員による実施が困難） |
| 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。）<br>[ ]フラッシュメモリ [ ]紙<br>[ ○ ]その他 （ システムを構成するサーバ及び端末機を使用して特定個人情報を取り扱う。 ） |
| ⑤委託先名の確認方法 | | ・高知市行政情報公開条例（平成12年条例第68号）に基づき，契約関係書類の公開請求が可能。<br>・契約の都度，高知市ホームページで業務名，契約相手方，契約期間，契約金額等を公表。 |
| ⑥委託先名 | | 富士通Japan株式会社 四国公共ビジネス部 |
| 再委託 | ⑦再委託の有無 ※ | [ 再委託する ] <選択肢> 1）再委託する 2）再委託しない |
| | ⑧再委託の許諾方法 | 業務委託契約書に規定する手続に基づき，委託先からの再委託承認申請書を審査のうえ，再委託承諾通知を行う。 |
| | ⑨再委託事項 | 住民基本台帳ネットワークシステムの運用支援及び改修に関する業務 |

| 5. 特定個人情報の提供・移転（委託に伴うものを除く。） | |
|---|---|
| 提供・移転の有無 | [ ○ ] 提供を行っている （ ）件 [ ] 移転を行っている （ ）件<br>[ ] 行っていない |
| **提供先1** | 機構 |
| ①法令上の根拠 | 個人番号，個人番号カード命令第35条（個人番号通知書・個人番号カード関連事務の委任） |
| ②提供先における用途 | 市町村からの個人番号通知書，個人番号カード命令第35条（個人番号通知書・個人番号カード関連事務の委任）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 | 個人番号，4情報（氏名，住所，性別，生年月日），その他住民票関係情報，通知カード及び交付申請書の送付先の情報 |
| 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 ]<br>＜選択肢＞<br>1）1万人未満<br>2）1万人以上10万人未満<br>3）10万人以上100万人未満<br>4）100万人以上1,000万人未満<br>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 | 「Ⅱ．2．③対象となる本人の範囲」に同じ |
| ⑥提供方法 | [ ] 情報提供ネットワークシステム [ ] 専用線<br>[ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。）<br>[ ] フラッシュメモリ [ ] 紙<br>[ ○ ] その他 （ 住基ネット ） |
| ⑦時期・頻度 | 新たに個人番号の通知対象者が生じた都度提供する。 |

| 6. 特定個人情報の保管・消去 | | |
|---|---|---|
| ①保管場所　※ | | ・カメラ監視付きの入退室管理を行っているサーバ室内で，鍵付き専用ラックに搭載されたサーバ内に保管。<br>・サーバへのアクセスは，ID／パスワードによる認証が必要。<br><br>＜ガバメントクラウドにおける措置＞<br>①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAP のリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。<br>・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。<br>・日本国内でのデータ保管を条件としていること。<br>②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 |
| ②保管期間 | 期間 | ［　　1年未満　　］<br>＜選択肢＞<br>1）1年未満　2）1年　3）2年<br>4）3年　5）4年　6）5年<br>7）6年以上10年未満　8）10年以上20年未満　9）20年以上<br>10）定められていない |
| | その妥当性 | 送付先情報は機構への提供のみに用いられ，また，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，機構より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。<br><br>＜ガバメントクラウドにおける措置＞<br>①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。<br>②クラウド事業者がHDD やSSD などの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001 等にしたがって確実にデータを消去する。<br>③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 |
| 7. 備考 | | |
| ― | | |

# 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 | | |
|---|---|---|
| (4)コンビニ交付用ファイル | | |
| **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＞<br>1）システム用ファイル<br>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＞<br>1）1万人未満<br>2）1万人以上10万人未満<br>3）10万人以上100万人未満<br>4）100万人以上1,000万人未満<br>5）1,000万人以上 |
| ③対象となる本人の範囲 ※ | | 高知市の住民（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 | 住民票の写しをコンビニで交付するため。 |
| ④記録される項目 | | [　50項目以上100項目未満　] ＜選択肢＞<br>1）10項目未満　2）10項目以上50項目未満<br>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<br>[　]個人番号　[　]個人番号対応符号　[　]その他識別情報（内部番号）<br>・連絡先等情報<br>[ ○ ]4情報（氏名、性別、生年月日、住所）　[　]連絡先（電話番号等）<br>[ ○ ]その他住民票関係情報<br>・業務関係情報<br>[　]国税関係情報　[　]地方税関係情報　[　]健康・医療関係情報<br>[　]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<br>[　]生活保護・社会福祉関係情報　[　]介護・高齢者福祉関係情報<br>[　]雇用・労働関係情報　[　]年金関係情報　[　]学校・教育関係情報<br>[　]災害関係情報<br>[　]その他　（　　） |
| | その妥当性 | 住基法第7条に規定する住民票の記載事項であるため。 |
| | 全ての記録項目 | 別添2を参照。 |
| ⑤保有開始日 | | 令和4年3月1日 |
| ⑥事務担当部署 | | 市民協働部　中央窓口センター |

| 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<br>[　] 評価実施機関内の他部署　（　） <br>[　] 行政機関・独立行政法人等　（　） <br>[　] 地方公共団体・地方独立行政法人　（　） <br>[　] 民間事業者　（　） <br>[ ○ ] 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<br>[　] 電子メール　[　] 専用線　[　] 庁内連携システム<br>[　] 情報提供ネットワークシステム<br>[ ○ ] その他　（ 既存住民基本台帳システム　） |
| ③入手の時期・頻度 | | ・転入，出生等の異動に伴う申請・届出時<br>（機構からの個人番号の入手も含む） |
| ④入手に係る妥当性 | | 個別的に本人から入手する情報は，住基法に規定される届出によるものである。 |
| ⑤本人への明示 | | 住民票の記載事項として住基法第7条に規定されているものである。 |
| ⑥使用目的 ※ | | 住民票の写しを交付するため。 |
| | 変更の妥当性 | 非該当 |
| ⑦使用の主体 | 使用部署 ※ | 市民協働部　中央窓口センター |
| | 使用者数 | [　10人未満　] ＜選択肢＞<br>1）10人未満　2）10人以上50人未満<br>3）50人以上100人未満　4）100人以上500人未満<br>5）500人以上1,000人未満　6）1,000人以上 |
| ⑧使用方法 ※ | | 既存住民基本台帳システムより住民票の写しの情報を抽出し，コンビニ交付を委任する機構に対し提供する。 |
| | 情報の突合 ※ | 住民基本台帳ファイルとの突合を行う。 |
| | 情報の統計分析 ※ | コンビニ交付用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 ※ | なし |
| ⑨使用開始日 | | 令和4年3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<br>（ 1 ） 件 |
| **委託事項1** | | 証明発行サーバ運用支援及び改修業務 |
| ①委託内容 | | 証明発行サーバ運用支援及び改修業務 |
| 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><br>1）特定個人情報ファイルの全体<br>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><br>1）1万人未満<br>2）1万人以上10万人未満<br>3）10万人以上100万人未満<br>4）100万人以上1,000万人未満<br>5）1,000万人以上 |
| | 対象となる本人の範囲 ※ | 高知市の住民（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）。 |
| | その妥当性 | 住民票写し等コンビニ交付システム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人未満 ] <選択肢><br>1）10人未満 2）10人以上50人未満<br>3）50人以上100人未満 4）100人以上500人未満<br>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。）<br>[ ] フラッシュメモリ [ ] 紙<br>[ ○ ] その他 （ システムを構成するサーバ及び端末機を使用して特定個人情報を取り扱う。 ） |
| ⑤委託先名の確認方法 | | ・高知市行政情報公開条例（平成12年条例第68号）に基づき，契約関係書類の公開請求が可能。<br>・契約の都度，高知市ホームページで業務名，契約相手方，契約期間，契約金額等を公表。 |
| ⑥委託先名 | | 富士通Japan株式会社 四国公共ビジネス部 |
| 再委託 | ⑦再委託の有無 ※ | [ 再委託する ] <選択肢><br>1）再委託する 2）再委託しない |
| | ⑧再委託の許諾方法 | 業務委託契約書に規定する手続に基づき，委託先からの再委託承認申請書を審査のうえ，再委託承諾通知を行う。 |
| | ⑨再委託事項 | 証明発行サーバ運用支援及び改修業務 |

| 5. 特定個人情報の提供・移転（委託に伴うものを除く。） | |
|---|---|
| 提供・移転の有無 | [ ○ ] 提供を行っている （ ）件 [ ] 移転を行っている （ ）件<br>[ ] 行っていない |
| **提供先1** | 機構 |
| ①法令上の根拠 | 平成26年11月20日総務省令第85号第36条（通知カード・個人番号カード関連事務に係る通知） |
| ②提供先における用途 | コンビニでの住民票の写しの交付に使用する。 |
| 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） |
| 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 ]<br>＜選択肢＞<br>1）1万人未満<br>2）1万人以上10万人未満<br>3）10万人以上100万人未満<br>4）100万人以上1,000万人未満<br>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 | 「Ⅱ．2．③対象となる本人の範囲」に同じ |
| ⑥提供方法 | [ ] 情報提供ネットワークシステム [ ] 専用線<br>[ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。）<br>[ ] フラッシュメモリ [ ] 紙<br>[ ○ ] その他 （ LGWAN ） |
| ⑦時期・頻度 | 住民基本台帳の記載事項において，コンビニ交付情報に係る変更又は新規作成が発生した都度，随時。 |

| 6. 特定個人情報の保管・消去 | | |
|---|---|---|
| ①保管場所　※ | | ・カメラ監視付きの入退室管理を行っているサーバ室内で，鍵付き専用ラックに搭載されたサーバ内に保管。<br>・サーバへのアクセスは，ID／パスワードによる認証が必要。<br><br>＜ガバメントクラウドにおける措置＞<br>①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAP のリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。<br>・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。<br>・日本国内でのデータ保管を条件としていること。<br>②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 |
| ②保管期間 | 期間 | ［　　20年以上　　］<br>＜選択肢＞<br>1）1年未満　2）1年　3）2年<br>4）3年　5）4年　6）5年<br>7）6年以上10年未満　8）10年以上20年未満　9）20年以上<br>10）定められていない |
| | その妥当性 | 住民基本台帳に登録されている者が対象のなるためめ。 |
| ③消去方法 | | ・サーバ内の特定個人情報については，サーバの機器更新時等に完全に消去する。<br>・バックアップ媒体については，破砕処理を実施。<br>・申請書等の紙媒体については，焼却処理を行う。<br>・消除者の特定個人情報の消去は高知市からの操作によって実施される。<br><br>＜ガバメントクラウドにおける措置＞<br>①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。<br>②クラウド事業者がHDD やSSD などの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001 等にしたがって確実にデータを消去する。<br>③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 |

| 7. 備考 |
|---|
| ― |

## （別添2）特定個人情報ファイル記録項目

（1）住民基本台帳ファイル
宛名番号，住民票コード，個人番号，世帯番号，氏名情報，生年月日，性別，続柄，住民となった年月日，住民となった届出年月日，住民となった事由，世帯主情報，現住所情報，住所を定めた年月日，住所を定めた届出年月日，前住所情報，転入元住所情報，転出先住所情報，本籍・筆頭者情報，消除情報，外国人住民となった年月日（外国人住民のみ），国籍（外国人住民のみ），法30条45規定区分（外国人住民のみ），在留カード等の番号（外国人住民のみ），在留資格情報（外国人住民のみ），通称（外国人住民のみ），通称の記載と削除関する事項（外国人住民のみ），個別記載情報，転出予定者情報，除票住民票情報，異動履歴情報，住基カード発行状況，個人番号カード等情報，在留カード等情報，旧氏漢字，旧氏ふりがな

（2）本人確認情報ファイル
1．住民票コード，2．漢字氏名，3．外字数（氏名），4．ふりがな氏名，5．清音化かな氏名，6．生年月日，7．性別，8．市町村コード，9．大字・字コード，10．郵便番号，11．住所，12．外字数（住所），13．個人番号，14．住民となった日，15．住所を定めた日，16．届出の年月日，17．市町村コード（転入前），18．転入前住所，19．外字数（転入前住所），20．続柄，21．異動事由，22．異動年月日，23．異動事由詳細，24．旧住民票コード，25．住民票コード使用年月日，26．依頼管理番号，27．操作者ID，28．操作端末ID，29．更新順番号，30．異常時更新順番号，31．更新禁止フラグ，32．予定者フラグ，33．排他フラグ，34．外字フラグ，35．レコード状況フラグ，36．タイムスタンプ，37．旧氏　漢字，38．旧氏　外字数，39．旧氏　ふりがな，40．旧氏　外字変更連番

（3）送付先情報ファイル
1．送付先管理番号，2．送付先郵便番号，3．送付先住所　漢字項目長，4．送付先住所　漢字，5．送付先住所　漢字外字数，6．送付先氏名　漢字項目長，7．送付先氏名　漢字，8．送付先氏名　漢字　外字数，9．市町村コード，10．市町村名　項目長，11．市町村名，12．市町村郵便番号，13．市町村住所　項目長，14．市町村住所，15．市町村住所　外字数，16．市町村電話番号，17．交付場所名　項目長，18．交付場所名，19．交付場所名　外字数，20．交付場所郵便番号，21．交付場所住所　項目長，22．交付場所住所，23．交付場所住所　外字数，24．交付場所電話番号，25．カード送付場所名　項目長，26．カード送付場所名，27．カード送付場所名　外字数，28．カード送付場所郵便番号，29．カード送付場所住所　項目長，30．カード送付場所住所，31．カード送付場所住所　外字数，32．カード送付場所電話番号，33．対象となる人数，34．処理年月日，35．操作者ID，36．操作端末ID，37．印刷区分，38．住民票コード，39．氏名　漢字項目長，40．氏名　漢字，41．氏名　漢字　外字数，42．氏名　かな項目長，43．氏名　かな，44．郵便番号，45．住所　項目長，46．住所，47．住所　外字数，48．生年月日，49．性別，50．個人番号，51．第30条の45に規定する区分，52．在留期間の満了の日，53．代替文字変換結果，54．代替文字氏名　項目長，55．代替文字氏名，56．代替文字住所　項目長，57．代替文字住所，58．代替文字氏名位置情報，59．代替文字住所位置情報，60．外字フラグ，61．外字パターン，62．旧氏　漢字，63．旧氏　外字数，64．旧氏　ふりがな，65．旧氏　外字変更連番，66．ローマ字　氏名，67．ローマ字　旧氏

（4）コンビニ交付用ファイル
識別ID，世帯情報　世帯員数，世帯情報　交付可能フラグ，世帯情報　交付不可事由，個人情報　交付可能フラグ，個人情報　交付不可事由，個人情報　世帯員識別ID，個人情報　住民区分，個人情報　カナ氏名，個人情報　漢字氏名，個人情報　漢字氏名イメージ，個人情報　生年月日，証明書用途　用途コード，証明書用途　用途名称，記載有無　コード，記載有無　名称，記載有無　デフォルト，住記記載有無選択指定，個人番号有無選択指定，単価，徴収単位，問い合わせ有無フラグ

# 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 | ・申請・届出等の様式を，不必要な情報が記載されないよう分かりやすいものにするとともに，様式に記載された情報について，事務マニュアルに基づき，受付時に確認を行う。<br>・他部署又は他機関から情報を入手する場合は，庁内連携システム等の認められた方法以外での入手を禁止するとともに，入手記録を保存し，定期的に確認を行う。<br>・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 | ・上記の措置の実施に加え，庁内連携システムで情報を入手する場合については，必要な情報以外を入手できないようシステム上で制限を行う。<br>・住民がサービス検索・電子申請機能の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、画面での誘導を簡潔に行うことで、異なる手続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＞<br>1）特に力を入れている　　2）十分である<br>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 | ・特定個人情報を入手する場合の適切な方法や法令等に違反した場合の罰則等について，教育を徹底する。<br>・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。<br>・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＞<br>1）特に力を入れている　　2）十分である<br>3）課題が残されている |
| 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 | ・個人番号カード及び主務省令で定められた本人確認書類の提示を受け，本人確認を行う。<br>・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，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 | 住登住民については既存住民基本台帳システム，住登外住民については住基ネットで，個人番号及び4情報（氏名，住所，性別，生年月日）と入手した情報の照合を行う。 |
| 特定個人情報の正確性確保の措置の内容 | ・住基ネットCSと連携して，定期的に氏名，住所，性別，生年月日情報の正確性を確認する。<br>・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＞<br>1）特に力を入れている　　2）十分である<br>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 | ・窓口においては，本人から直接書面を受け取ることを原則とする。<br>・他部署又は他機関から情報を入手する場合は，安全性が確認された庁内連携システム等を介してしか情報を入手しないよう事務を徹底する。<br>・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＞<br>1）特に力を入れている　　2）十分である<br>3）課題が残されている |

| 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置 | |
|---|---|
| ― | |

## 3. 特定個人情報の使用

| リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク | | |
|---|---|---|
| 宛名システム等における措置の内容 | 宛名システム等へは，個人番号及び4情報の連携を行うが，宛名システム等を介して他の事務で使用する特定個人情報ファイルにはアクセスできないようアクセス制御を行う。 | |
| 事務で使用するその他のシステムにおける措置の内容 | ・既存住民基本台帳システムでは，住民基本台帳事務に関係のない情報を保有しない。<br>・他のシステムで保有する特定個人情報ファイルを直接参照できないようアクセス制限を行う。 | |
| その他の措置の内容 | ・原則としてシステムファイル以外の電子ファイルでの特定個人情報を保有を禁止する。<br>・保有する場合は，他の特定個人情報と紐付けを行わないよう，教育を徹底する。 | |
| リスクへの対策は十分か | [ 十分である ] | ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>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＞<br>1）行っている 2）行っていない |
| 具体的な管理方法 | ・既存住民基本台帳システムを利用する必要がある職員，派遣者，委託先を特定し，個人毎にユーザIDを割り当てるとともに，IDとパスワードによるユーザ認証を行う。<br>・既存住民基本台帳システムが設置されているサーバ室への入退出の際には，ICカード認証，生体認証を行う。<br>・申請管理システムを利用する必要がある職員を特定し、個人ごとのユーザ ID を割り当てるとともにIDとパスワードによる認証を行う。<br>・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＞<br>1）行っている 2）行っていない |
| 具体的な管理方法 | (1)発効管理<br>業務とアクセス権限（使用できる業務メニューの範囲，更新・閲覧等の区別等）の対応表を作成するとともに，アクセス権限の発効に際しては，利用者からの申請に基づき，中央窓口センター長が対応表を確認し，アクセス権限を発効する。<br>(2)失効管理<br>定期的又は異動/退職等のイベントが発生したタイミングで、権限を有していた職員の異動/退職等情報を確認し、当該事由が生じた際には速やかにアクセス権限を更新し、当該ユーザ ID を失効させる。 | |
| アクセス権限の管理 | [ 行っている ] | ＜選択肢＞<br>1）行っている 2）行っていない |
| 具体的な管理方法 | ・複数の利用者が共有する共通IDは発行せず，必ず個人に対しユーザIDを発効する。<br>・パスワードは6か月ごとに変更しなければ，システムにログインできないよう制限を行う。<br>・ユーザID及び付与された権限の棚卸しを6か月ごとにに実施し，現状と齟齬がある場合には，直ちに修正を行う。<br>・定期的にユーザ ID 一覧をシステムより出力し、アクセス権限の管理表と突合を行い、アクセス権限の確認及び不正利用の有無をユーザID管理者が確認を行う。また、不要となったユーザ ID やアクセス権限を速やかに変更又は削除する。 | |
| 特定個人情報の使用の記録 | [ 記録を残している ] | ＜選択肢＞<br>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 | ・個人を特定した検索及び個人特定後の操作について，ユーザID，端末，操作日時，アクセスした特定個人情報の項目等を記録する。<br>・記録は，5年間分保存する。<br>・申請管理システム等へのアクセスログ、操作ログの記録を行い、操作者個人を特定できるようにする。<br>・アクセスログ及び操作ログは、改ざんを防止するため、不正プロセス検知ソフトウェアにより、不正なログの書き込み等を防止する。<br>・定期的に操作ログをチェックし、不正とみられる操作があった場合、操作内容を確認する。 | |
| 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＞<br>1）特に力を入れている 2）十分である<br>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 | ・番号法及び番号法第9条第2項に基づく条例で認められた事務以外で特定個人情報の利用が禁止されていること，また，法令等に違反した場合の罰則について教育を徹底する。<br>・申請管理システムへアクセスできる端末を制限する。<br>・外部記憶媒体にサービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータを複製する場合、使用管理簿に記載し、事前に責任者の承認を得たうえで複製する。なお、外部記憶媒体は限定された USB メモリ等のみを使用する。<br>・外部記憶媒体内のデータは暗号化する。 |
| リスクへの対策は十分か | [ 十分である ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>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 | ・サーバ上の特定個人情報ファイルに直接アクセス（バックアップ処理，データ抽出等）できる者を限定するとともに，サーバでの操作ログを記録する。<br>・バックアップ処理以外に特定個人情報ファイルを複製しないことや，認められた処理以外で個人番号を含むデータ抽出を行わないことを関係者に徹底する。<br>・申請管理システムから取得した個人番号付電子申請データ等のデータについて、改ざんや業務目的以外の複製を禁止するルールを定め、ルールに従って業務を行う。<br>・アクセス権限を付与された最小限の職員等だけが、個人番号付電子申請等のデータについて、操作端末への保存や外部記憶媒体への書き出し等ができるようシステム的に制御する。<br>・外部記憶媒体にサービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータを複製する場合、使用管理簿に記載し、事前に責任者の承認を得たうえで複製する。なお、外部記憶媒体は限定された USB メモリ等のみを使用する。<br>・外部記憶媒体内のデータは暗号化する。 |
| リスクへの対策は十分か | [ 十分である ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| 特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置 | |
| ― | |

| 4. 特定個人情報ファイルの取扱いの委託 | | [　　]委託しない |
|---|---|---|
| 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<br>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<br>委託先による特定個人情報の保管・消去に関するリスク<br>委託契約終了後の不正な使用等のリスク<br>再委託に関するリスク | | |
| 情報保護管理体制の確認 | 委託業者と契約を締結する際は，事前に以下の項目について確認を行うとともに，契約締結後は，書面による報告を義務付ける。<br>・個人情報保護に関する規定，体制の整備<br>・個人情報保護に関する人的安全管理措置<br>・個人情報保護に関する技術的安全管理措置 | |
| 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＞<br>1）制限している　2）制限していない |
| 具体的な制限方法 | ・アクセス権限を付与する従業員数を必要最小限に限定する。<br>・従業員に付与するアクセス権限を必要最小限に限定する。 | |
| 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＞<br>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 | ・特定個人情報の利用履歴について，ユーザID，操作日時，処理事由等を記録する。<br>・記録は，５年間保存する。 | |
| 特定個人情報の提供ルール | [　定めている　] | ＜選択肢＞<br>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 | ・窓口証明の受付及び交付業務では，委託先は申請のあった本人に対してのみ特定個人情報が提供でき，それ以外の提供は一切認めないことを，契約書に明記する。<br>・”情報システムの運用支援及び改修業務”と”住民票の写し等の交付受付及び発行業務”では，委託先は契約書に明記された以外の提供を一切認めない。<br>・委託先から他者に特定個人情報を提供する場合は，記録を残し，月1回確認を行う。 | |
| 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 | ・委託先には電子ファイル等の形式で特定個人情報を直接提供しない。<br>・特定個人情報の取扱いは，職員と同様にシステムを利用して行うこととする。 | |
| 特定個人情報の消去ルール | [　定めている　] | ＜選択肢＞<br>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 | ・業務上一時的に作成した特定個人情報ファイルは，不要となった時点で直ちに消去する。<br>・業務遂行に伴い出力した特定個人情報を含む帳票等については，不要になった時点で，定められた方法により廃棄する。<br>・情報の消去が適切に行われていることを，定期的に職員が確認する。 | |
| 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 | [　定めている　] | ＜選択肢＞<br>1）定めている　2）定めていない |
| 規定の内容 | ・目的外利用の禁止<br>・特定個人情報の閲覧者・更新者を制限<br>・特定個人情報の提供先の限定<br>・情報漏洩を防ぐための保管管理に責任を負う<br>・消去のルール<br>・特定個人情報の取扱いについて四半期に一度チェックを行った上で結果を報告をする<br>・必要に応じて，本市が委託先の視察・監査を行うことができる | |
| 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 | [　十分に行っている　] | ＜選択肢＞<br>1）特に力を入れて行ってい　2）十分に行っている<br>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 | 委託先と同等のリスク対策を実施する。 | |
| 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＞<br>1）特に力を入れている　2）十分である<br>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＞<br>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 | ・庁内連携システム等を利用して提供・移転を行う場合は，操作者，操作日時，利用する事務，提供する情報の項目等をシステムで記録する。<br>・庁内ネットワーク等の専用線を利用して電子ファイル等により提供・移転を行う場合は，提供者，提供日時，提供先，利用する事務・システム，提供する情報の項目等を提供側で記録する。<br>・記録は，５年間保存する。 | |
| 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＞<br>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 | ・特定個人情報の提供・移転が認められるものについては，番号法で規定されているもののほか，独自利用条例で規定する。<br>・認められた提供・移転については，庁内連携システム等の認められた方法以外を禁止する。<br>・提供・移転の記録を，定期的に確認する。 | |
| 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＞<br>1）特に力を入れている　　2）十分である<br>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 | ・システム用ファイル以外の電子ファイルでの特定個人情報の保有を原則禁止する。<br>・提供・移転のルールや，法令等に違反した場合の罰則等について，教育を徹底する。 | |
| リスクへの対策は十分か | [　　十分である　　] | ＜選択肢＞<br>1）特に力を入れている　　2）十分である<br>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 | 庁内連携システム等において，番号法及び独自利用条例で規定された照会者，提供者，特定個人情報のみ情報の提供・移転を認めるようシステムで制御を行う。 | |
| リスクへの対策は十分か | [　　十分である　　] | ＜選択肢＞<br>1）特に力を入れている　　2）十分である<br>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＞<br>1) 特に力を入れている　2) 十分である<br>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＞<br>1) 特に力を入れている　2) 十分である<br>3) 課題が残されている |
| リスク3： 入手した特定個人情報が不正確であるリスク | |
| 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＞<br>1) 特に力を入れている　2) 十分である<br>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 | |
| リスクへの対策は十分か | [　] ＜選択肢＞<br>1) 特に力を入れている　2) 十分である<br>3) 課題が残されている |
| 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 | ＜中間サーバ・ソフトウェアにおける措置＞<br>・情報提供機能(注)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。<br>・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。<br>・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。<br>・中間サーバの職員認証・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。<br>(注)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＞<br>1) 特に力を入れている　2) 十分である<br>3) 課題が残されている |

| 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 | ＜中間サーバ・ソフトウェアにおける措置＞<br>・セキュリティ管理機能（注）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。<br>・中間サーバの職員認証・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。<br>（注）暗号化・復号機能と，鍵情報及び照会許可用照合リストを管理する機能。<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・中間サーバと既存システム，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。<br>・中間サーバと団体については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。<br>・中間サーバ・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＞<br>1）特に力を入れている　2）十分である<br>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 | ＜中間サーバ・ソフトウェアにおける措置＞<br>・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。<br>・情報提供データベース管理機能（注）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。<br>・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。<br>（注）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＞<br>1）特に力を入れている　2）十分である<br>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・ソフトウェアにおける措置＞<br>・中間サーバの職員認証・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。<br>・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。<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・中間サーバと既存システム，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。<br>・中間サーバと団体については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。<br>・中間サーバ・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・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。<br>・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・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><br>1）特に力を入れて遵守している 2）十分に遵守している<br>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><br>1）特に力を入れて整備している 2）十分に整備している<br>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><br>1）特に力を入れて整備している 2）十分に整備している<br>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><br>1）特に力を入れて周知している 2）十分に周知している<br>3）十分に周知していない |
| ⑤物理的対策 | [ 特に力を入れて行っている ] | <選択肢><br>1）特に力を入れて行っている 2）十分に行っている<br>3）十分に行っていない |
| 具体的な対策の内容 | ＜高知市における措置＞<br>(1)サーバ<br>・入退室管理されたサーバ室内の施錠管理された専用ラックに設置する。<br>・入退室管理装置及び監視カメラによる入退室者の記録を行う。<br>(2)記録媒体（バックアップ媒体等）<br>・原則持ち込みを禁止とし，特に必要がある場合のみ許可とする。<br>・施錠できる保管庫等で管理する。<br>・事故，自然災害等によるデータの滅失等を回避するため，遠隔地での分散保管を実施。<br>(3)紙媒体<br>・施錠できる保管庫等で管理する。<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・中間サーバ・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。<br><br>＜申請管理システムにおける措置＞<br>・操作端末については、業務時間内のセキュリティワイヤー等による固定、操作場所への入退室管理、業務時間外の施錠できるキャビネット等への保管、などの物理的対策を講じている。<br>・外部記憶媒体については、限定された USB メモリ等以外の利用不可、施錠できるキャビネット等への保管、使用管理簿による管理、などの安全管理措置を講じている。<br><br>＜ガバメントクラウドにおける措置＞<br>①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。<br>②事前に許可されていない装置等に関しては、外部に持出できないこととしている。 | |

| | | |
|---|---|---|
| ⑥技術的対策 | | [　　十分に行っている　　] ＜選択肢＞<br>1）特に力を入れて行っている　2）十分に行っている<br>3）十分に行っていない |
| | 具体的な対策の内容 | ＜高知市における措置＞<br>(1)ウィルス対策<br>・全てのサーバ及び端末にウィルス対策ソフトを導入する。<br>・定期的なパターンファイルの更新，リアルタイムでの監視，週1回の全ファイルチェックを実施する。<br>(2)OS等の修正プログラムの適用<br>・全てのサーバ及び端末に対して，OS等の修正プログラムの適用を行う。<br>(3)不正アクセス対策<br>・外部のネットワークとは，ファイアウォールを介して接続し，不正アクセスの監視を行う。<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・中間サーバ・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。<br>・中間サーバ・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。<br>・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。<br><br>＜申請管理システムにおける措置＞<br>・操作端末へのウイルス検出ソフトウェア等の導入により、ウイルス定義ファイルの定期的な更新及びウイルスチェックを行い、マルウェア検出を行う。<br>・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。<br><br>＜ガバメントクラウドにおける措置＞<br>①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。<br>②地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和4年10月 デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。)又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。<br>③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos 対策を24 時間365日講じる。<br>④クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。<br>⑤地方公共団体が委託したASP 又はガバメントクラウド運用管理補助者は、導入しているOS 及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。<br>⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。<br>⑦地方公共団体やASP 又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。<br>⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。 |
| ⑦バックアップ | | [　　十分に行っている　　] ＜選択肢＞<br>1）特に力を入れて行っている　2）十分に行っている<br>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＞<br>1）特に力を入れて行っている　2）十分に行っている<br>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＞<br>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＞<br>1）保管している　2）保管していない |
| | 具体的な保管方法 | 生存者の個人番号と同様の方法で安全管理措置を実施する。 |
| 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＞<br>1）特に力を入れている　2）十分である<br>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 | ・取得した個人番号が変更されていないか，月１回機構が管理する本人確認情報と照合する。<br>・他部署から入手する住民票記載事項に係る情報については，情報ごとに更新頻度を定め，鮮度を維持する。<br>・操作端末は、基本的には、個人番号付電子申請データの取込に使用するが、再申請や申請情報の訂正が発生した場合に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＞<br>1）特に力を入れている　2）十分である<br>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＞<br>1）定めている　2）定めていない |
| 手順の内容 | ・住民基本台帳は，消除者についても記録を保持しておく必要があり，当該特定個人情報は実質永年保管となるため，データベース上の各データについては消去手順は定めていない。<br>・サーバの機器更新時等においては，情報の復元が不可能な専用ソフトによりハードディスクの消去作業を行っている。<br>・バックアップ媒体については，保管期限が経過したものについて破砕処理を行っている。<br>・紙媒体については，保管期限が経過したものについて，焼却処理を行っている。<br>・操作端末については、業務終了後に不要な個人番号付電子申請データ等の消去について徹底し、必要に応じて管理者が確認する。<br>・外部記憶媒体については、定期的に内部のチェックを行い不要なデータの確認を行い、廃棄する場合は管理者の承認を得て行う手順を定めている。<br><br>＜ガバメントクラウドにおける措置＞<br>データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001 等に準拠したプロセスにしたがって確実にデータを消去する。 |
| 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＞<br>1）特に力を入れている　2）十分である<br>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民基本台帳システムに限定されるため，既存住民基本台帳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の内容 | 平成14年6月10日総務省告示第334号（第6－6　本人確認情報の通知及び記録）等により市町村CSにおいて既存住民基本台帳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。<br>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＞<br>1）特に力を入れている　2）十分である<br>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 | 本人確認情報の入手元を既存住民基本台帳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＞<br>1）特に力を入れている　2）十分である<br>3）課題が残されている |
| 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民基本台帳システムに限定されており，既に本人確認された情報である。 |
| 個人番号の真正性確認の措置の内容 | 本人確認情報の入手元は既存住民基本台帳システムに限定さており，既に個人番号の真正性確認がされている。 |
| 特定個人情報の正確性確保の措置の内容 | 既存住民基本台帳システムにおいて正確性が確保された本人確認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。 |
| 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＞<br>1）特に力を入れている　2）十分である<br>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（注）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。<br>・操作者の認証を行う。<br>(注)市町村CSのサーバ上で稼動するアプリケーション。市町村システム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，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＞<br>1）特に力を入れている　2）十分である<br>3）課題が残されている |
| 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置 | |
| ― | |

| 3. 特定個人情報の使用 | | |
|---|---|---|
| リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク | | |
| 宛名システム等における措置の内容 | 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の内容 | 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。 | |
| 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＞<br>1）特に力を入れている　2）十分である<br>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 | [ 行っていない ] | ＜選択肢＞<br>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。 | |
| アクセス権限の発効・失効の管理 | [ 行っている ] | ＜選択肢＞<br>1）行っている　2）行っていない |
| 具体的な管理方法 | (1)発効管理<br>・業務とアクセス権限（使用できる業務メニューの範囲，更新・閲覧等の区別等）の対応表を作成するとともに，アクセス権限の発効に際しては，利用者からの申請に基づき，中央窓口センター長が対応表を確認し，アクセス権限を発効する。<br>(2)失効管理<br>・権限を有していた職員が異動・退職した場合は，直ちに権限の失効を行う。 | |
| アクセス権限の管理 | [ 行っている ] | ＜選択肢＞<br>1）行っている　2）行っていない |
| 具体的な管理方法 | ・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。<br>・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の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＞<br>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 | ・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。<br>・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。<br>・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。<br>・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。 | |
| 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＞<br>1）特に力を入れている　2）十分である<br>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 | 番号法及び番号法第9条第2項に基づく条例で認められた事務以外で特定個人情報の利用が禁止されていること，また，法令等に違反した場合の罰則について教育を徹底する。 | |
| リスクへの対策は十分か | [ 十分である ] | ＜選択肢＞<br>1）特に力を入れている　2）十分である<br>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 | ・サーバ上の特定個人情報ファイルに直接アクセス（バックアップ処理，データ抽出等）できる者を限定するとともに，サーバでの操作ログを記録する。<br>・バックアップ処理以外に特定個人情報ファイルを複製しないことや，認められた処理以外で個人番号を含むデータ抽出を行わないことを関係者に徹底する。 | |
| リスクへの対策は十分か | [ 課題が残されている ] | ＜選択肢＞<br>1）特に力を入れている　2）十分である<br>3）課題が残されている |

| 特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置 |
|---|
| ― |

## 4. 特定個人情報ファイルの取扱いの委託　　[　]委託しない

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 | | 委託業者と契約を締結する際は，事前に以下の項目について確認を行うとともに，契約締結後は，書面による報告を義務付ける。<br>・個人情報保護に関する規定，体制の整備<br>・個人情報保護に関する人的安全管理措置<br>・個人情報保護に関する技術的安全管理措置 |
| 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＞<br>1）制限している　2）制限していない |
| | 具体的な制限方法 | ・アクセス権限を付与する従業員数を必要最小限に限定する。<br>・従業員に付与するアクセス権限を必要最小限に限定する。 |
| 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＞<br>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 | ・特定個人情報の利用履歴について，ユーザID，操作日時，処理事由等を記録しする。<br>・記録は，10年間保存する。 |
| 特定個人情報の提供ルール | | [　定めている　] ＜選択肢＞<br>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 | ・”住民基本台帳ネットワークシステムの運用支援及び改修に関する業務”では，委託先は契約書に明記された以外の提供を一切認めない。<br>・委託先から他者に特定個人情報を提供する場合は，記録を残し，月1回確認を行う。 |
| | 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 | ・委託先には電子ファイル等の形式で特定個人情報を直接提供しない。<br>・特定個人情報の取扱いは，職員と同様にシステムを利用して行うこととする。 |
| 特定個人情報の消去ルール | | [　定めている　] ＜選択肢＞<br>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 | ・業務上一時的に作成した特定個人情報ファイルは，不要となった時点で直ちに消去する。<br>・業務遂行に伴い出力した特定個人情報を含む帳票等については，不要になった時点で，定められた方法により廃棄する。<br>・情報の消去が適切に行われていることを，定期的に職員が確認する。 |
| 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 | | [　定めている　] ＜選択肢＞<br>1）定めている　2）定めていない |
| | 規定の内容 | ・目的外利用の禁止<br>・特定個人情報の閲覧者・更新者を制限<br>・特定個人情報の提供先の限定<br>・情報漏洩を防ぐための保管管理に責任を負う<br>・消去のルール<br>・特定個人情報の取扱いについて四半期に一度チェックを行った上で結果を報告をする<br>・必要に応じて，本市が委託先の視察・監査を行うことができる |
| 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 | | [　十分に行っている　] ＜選択肢＞<br>1）特に力を入れて行ってい　2）十分に行っている<br>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 | 委託先と同等のリスク対策を実施する。 |
| 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＞<br>1）特に力を入れている　2）十分である<br>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＞<br>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）の提供を行う際に，提供記録（提供日時，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＞<br>1）定めている　　2）定めていない |
| ルールの内容及びルール遵守の確認方法 | ・番号法及び住基法並びに高知市個人情報保護条例（平成18年条例第37号）の規定に基づき認められた提供・移転のみ許可をし，認められた方法以外での提供・移転を禁止する。<br>・提供・移転の記録を，定期的に確認する。 | |
| 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＞<br>1）特に力を入れている　　2）十分である<br>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移転はなされないことがシステム上担保される。<br>・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となっている。 |
| リスクへの対策は十分か | [　　十分である　　]　＜選択肢＞<br>1）特に力を入れている　　2）十分である<br>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 | (1)誤った情報を提供・移転してしまうリスクへの措置<br>・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することを担保する。<br>・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。<br><br>(2)誤った相手に提供・移転してしまうリスクへの措置<br>・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移転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＞<br>1）特に力を入れている　　2）十分である<br>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＞<br>1）特に力を入れている 2）十分である<br>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＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| リスク3： 入手した特定個人情報が不正確であるリスク | |
| 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＞<br>1）特に力を入れている 2）十分である<br>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 | |
| リスクへの対策は十分か | [ ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| 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＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| 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＞<br>1）特に力を入れている 2）十分である<br>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 | |
| リスクへの対策は十分か | [ ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>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><br>1）特に力を入れて遵守している 2）十分に遵守している<br>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><br>1）特に力を入れて整備している 2）十分に整備している<br>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><br>1）特に力を入れて整備している 2）十分に整備している<br>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><br>1）特に力を入れて周知している 2）十分に周知している<br>3）十分に周知していない |
| ⑤物理的対策 | [ 特に力を入れて行っている ] | <選択肢><br>1）特に力を入れて行っている 2）十分に行っている<br>3）十分に行っていない |
| 具体的な対策の内容 | (1)サーバ<br>・入退室管理されたサーバ室内の施錠管理された専用ラックに設置する。<br>・入退室管理装置及び監視カメラによる入退室者の記録を行う。<br>(2)記録媒体（バックアップ媒体等）<br>・施錠できる保管庫等で管理する。<br>・事故，自然災害等によるデータの滅失等を回避するため，遠隔地での分散保管を実施。<br>(3)紙媒体<br>・施錠できる保管庫等で管理する。<br><br>＜ガバメントクラウドにおける措置＞<br>①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており，システムのサーバー等は，クラウド事業者が保有・管理する環境に構築し，その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。<br>②事前に許可されていない装置等に関しては、外部に持出できないこととしている。 | |
| ⑥技術的対策 | [ 十分に行っている ] | <選択肢><br>1）特に力を入れて行っている 2）十分に行っている<br>3）十分に行っていない |
| 具体的な対策の内容 | (1)不正プログラム対策<br>・コンピュータウイルス監視ソフトを使用し，サーバ・端末双方でウイルスチェックを実施する。また，新種の不正プログラムに対応するために，ウイルスパターンファイルは定期的に更新し，可能な限り最新のものを使用する。<br>・本人確認情報の管理について定めた規程に基づき，コンピュータウイルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。また，同規程に基づき，オペレーション管理に係る手順等を整備し，当該手順に従って，情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的（コンピュータウィルス関連情報は毎日，その他の情報は少なくとも半年に一度）に入手し，機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。<br>(2)不正アクセス対策<br>・本人確認情報の管理について定めた規程に基づき，ネットワーク管理に係る手順等を整備し，ファイアウォールを導入する。<br><br>＜ガバメントクラウドにおける措置＞<br>①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。<br>②地方公共団体が委託したASP（「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和4年10月 デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は，ガバメントクラウドが提供するマネージドサービスにより，ネットワークアクティビティ，データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに，ログ管理を行う。<br>③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し，脅威検出やDDos 対策を24 時間365日講じる。<br>④クラウド事業者は，ガバメントクラウドに対し，ウイルス対策ソフトを導入し，パターンファイルの更新を行う。<br>⑤地方公共団体が委託したASP 又はガバメントクラウド運用管理補助者は，導入しているOS 及びミドルウエアについて，必要に応じてセキュリティパッチの適用を行う。<br>⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は，インターネットとは切り離された閉域ネットワークで構成する。<br>⑦地方公共団体やASP 又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については，閉域ネットワークで構成する。<br>⑧地方公共団体が管理する業務データは，国及びクラウド事業者がアクセスできないよう制御を講じる。 | |

| | | |
|---|---|---|
| ⑦バックアップ | [　十分に行っている　] | ＜選択肢＞<br>1）特に力を入れて行っている　2）十分に行っている<br>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＞<br>1）特に力を入れて行っている　2）十分に行っている<br>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＞<br>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＞<br>1）保管している　2）保管していない |
| 具体的な保管方法 | 生存者の個人番号と同様の方法で安全管理措置を実施する。 | |
| 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＞<br>1）特に力を入れている　2）十分である<br>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 | 既存住民基本台帳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＞<br>1）特に力を入れている　2）十分である<br>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＞<br>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3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。<br><br>＜ガバメントクラウドにおける措置＞<br>データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001 等に準拠したプロセスにしたがって確実にデータを消去する。 | |
| 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＞<br>1）特に力を入れている　2）十分である<br>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民基本台帳システムに限定されるため，既存住民基本台帳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の内容 | 市町村CSにおいて既存住民基本台帳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。 |
| 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＞<br>1）特に力を入れている　2）十分である<br>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 | 本人確認情報の入手元を既存住民基本台帳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＞<br>1）特に力を入れている　2）十分である<br>3）課題が残されている |
| 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民基本台帳システムに限定されており，既に本人確認された情報であるため，個別の措置は不要。 |
| 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 | 既存住民基本台帳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，既存住民基本台帳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，一定期間経過後に市町村CSから自動的に削除する。 |
| 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＞<br>1）特に力を入れている　2）十分である<br>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（注）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。<br>・操作者の認証を行う。<br>（注）市町村CSのサーバ上で稼動するアプリケーション。市町村システムで管理されるデータの安全保護対策，正アクセスの防止策に，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＞<br>1）特に力を入れている　2）十分である<br>3）課題が残されている |
| 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置 | |
| ― | |

| 3. 特定個人情報の使用 | | |
|---|---|---|
| リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク | | |
| 宛名システム等における措置の内容 | 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の内容 | 庁内システムにおける市町村CSへのアクセスは既存住民基本台帳システムに限定しており，また，既存住民基本台帳システムと市町村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。 | |
| 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＞<br>1）特に力を入れている　2）十分である<br>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＞<br>1）行っている　2）行っていない |
| 具体的な管理方法 | 法生体認証による操作者認証を行う。 | |
| アクセス権限の発効・失効の管理 | [ 行っている ] | ＜選択肢＞<br>1）行っている　2）行っていない |
| 具体的な管理方法 | (1)発効管理<br>・業務とアクセス権限（使用できる業務メニューの範囲，更新・閲覧等の区別等）の対応表を作成するとともに，アクセス権限の発効に際しては，利用者からの申請に基づき，中央窓口センター長が対応表を確認し，アクセス権限を発効する。<br>(2)失効管理<br>・権限を有していた職員が異動・退職した場合は，直ちに権限の失効を行う。 | |
| アクセス権限の管理 | [ 行っている ] | ＜選択肢＞<br>1）行っている　2）行っていない |
| 具体的な管理方法 | ・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。<br>・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の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＞<br>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 | ・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。<br>・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。<br>・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。 | |
| 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＞<br>1）特に力を入れている　2）十分である<br>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 | 番号法及び番号法第9条第2項に基づく条例で認められた事務以外で特定個人情報の利用が禁止されていること，また，法令等に違反した場合の罰則について教育を徹底する。 | |
| リスクへの対策は十分か | [ 十分である ] | ＜選択肢＞<br>1）特に力を入れている　2）十分である<br>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 | ・サーバ上の特定個人情報ファイルに直接アクセス（バックアップ処理，データ抽出等）できる者を限定するとともに，サーバでの操作ログを記録する。<br>・バックアップ処理以外に特定個人情報ファイルを複製しないことや，認められた処理以外で個人番号を含むデータ抽出を行わないことを関係者に徹底する。 | |
| リスクへの対策は十分か | [ 十分である ] | ＜選択肢＞<br>1）特に力を入れている　2）十分である<br>3）課題が残されている |

| 特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置 |
|---|
| ― |

## 4. 特定個人情報ファイルの取扱いの委託　　[　]委託しない

| | | |
|---|---|---|
| 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<br>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<br>委託先による特定個人情報の保管・消去に関するリスク<br>委託契約終了後の不正な使用等のリスク<br>再委託に関するリスク | | |
| 情報保護管理体制の確認 | 委託業者と契約を締結する際は，事前に以下の項目について確認を行うとともに，契約締結後は，書面による報告を義務付ける。<br>・個人情報保護に関する規定，体制の整備<br>・個人情報保護に関する人的安全管理措置<br>・個人情報保護に関する技術的安全管理措置 | |
| 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＞<br>1）制限している　2）制限していない |
| 具体的な制限方法 | ・アクセス権限を付与する従業員数を必要最小限に限定する。<br>・従業員に付与するアクセス権限を必要最小限に限定する。 | |
| 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＞<br>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 | ・特定個人情報の利用履歴について，ユーザID，操作日時，処理事由等を記録する。<br>・記録は，５年間保存する。 | |
| 特定個人情報の提供ルール | [　定めている　] | ＜選択肢＞<br>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 | ・”住民基本台帳ネットワークシステムの運用支援及び改修に関する業務”では，委託先には契約書に明記された以外の提供を一切認めない。<br>・委託先から他者に特定個人情報を提供する場合は，記録を残し，月1回確認を行う。 | |
| 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 | ・委託先には電子ファイル等の形式で特定個人情報を直接提供しない。<br>・特定個人情報の取扱いは，職員と同様にシステムを利用して行うこととする。 | |
| 特定個人情報の消去ルール | [　定めている　] | ＜選択肢＞<br>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 | ・業務上一時的に作成した特定個人情報ファイルは，不要となった時点で直ちに消去する。<br>・業務遂行に伴い出力した特定個人情報を含む帳票等については，不要になった時点で，定められた方法により廃棄する。<br>・情報の消去が適切に行われていることを，定期的に職員が確認する。 | |
| 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 | [　定めている　] | ＜選択肢＞<br>1）定めている　2）定めていない |
| 規定の内容 | ・目的外利用の禁止<br>・特定個人情報の閲覧者・更新者を制限<br>・特定個人情報の提供先の限定<br>・情報漏洩を防ぐための保管管理に責任を負う<br>・消去のルール<br>・特定個人情報の取扱いについて四半期に一度チェックを行った上で結果を報告をする<br>・必要に応じて，本市が委託先の視察・監査を行うことができる | |
| 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 | [　十分に行っている　] | ＜選択肢＞<br>1）特に力を入れて行ってい　2）十分に行っている<br>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 | 委託先と同等のリスク対策を実施する。 | |
| 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＞<br>1）特に力を入れている　2）十分である<br>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＞<br>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（送付先情報）の提供を行う際に，提供記録（提供日時、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＞<br>1）定めている　2）定めていない |
| ルールの内容及びルール遵守の確認方法 | ・番号法及び住基法並びに高知市個人情報保護条例（平成18年条例第37号）の規定に基づき認められた提供・移転のみ許可をし，認められた方法以外での提供・移転を禁止する。<br>・提供・移転の記録を，定期的に確認する。 | |
| 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＞<br>1）特に力を入れている　2）十分である<br>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（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移転はなされないことがシステム上担保される。<br>・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となっている。 | |
| リスクへの対策は十分か | [　十分である　] | ＜選択肢＞<br>1）特に力を入れている　2）十分である<br>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 | (1)誤った情報を提供・移転してしまうリスクへの措置<br>・システム上，既存住民基本台帳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。<br>(2)誤った相手に提供・移転してしまうリスクへの措置<br>・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移転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＞<br>1）特に力を入れている　2）十分である<br>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＞<br>1）特に力を入れている 2）十分である<br>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＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| リスク3： 入手した特定個人情報が不正確であるリスク | |
| 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＞<br>1）特に力を入れている 2）十分である<br>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 | |
| リスクへの対策は十分か | [ ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| 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＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| 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＞<br>1）特に力を入れている 2）十分である<br>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 | |
| リスクへの対策は十分か | [ ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>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><br>1）特に力を入れて遵守している 2）十分に遵守している<br>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><br>1）特に力を入れて整備している 2）十分に整備している<br>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><br>1）特に力を入れて整備している 2）十分に整備している<br>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><br>1）特に力を入れて周知している 2）十分に周知している<br>3）十分に周知していない |
| ⑤物理的対策 | [ 特に力を入れて行っている ] | <選択肢><br>1）特に力を入れて行っている 2）十分に行っている<br>3）十分に行っていない |
| 具体的な対策の内容 | (1)サーバ<br>・入退室管理されたサーバ室内の施錠管理された専用ラックに設置する。<br>・入退室管理装置及び監視カメラによる入退室者の記録を行う。<br>(2)記録媒体（バックアップ媒体等）<br>・施錠できる保管庫等で管理する。<br>・事故，自然災害等によるデータの滅失等を回避するため，遠隔地での分散保管を実施。<br>(3)紙媒体<br>・施錠できる保管庫等で管理する。<br><br>＜ガバメントクラウドにおける措置＞<br>①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており，システムのサーバー等は，クラウド事業者が保有・管理する環境に構築し，その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。<br>②事前に許可されていない装置等に関しては，外部に持出できないこととしている。 | |
| ⑥技術的対策 | [ 十分に行っている ] | <選択肢><br>1）特に力を入れて行っている 2）十分に行っている<br>3）十分に行っていない |
| 具体的な対策の内容 | (1)不正プログラム対策<br>・コンピュータウイルス監視ソフトを使用し，サーバ・端末双方でウイルスチェックを実施する。また，新種の不正プログラムに対応するために，ウイルスパターンファイルは定期的に更新し，可能な限り最新のものを使用する。<br>・送付先情報の管理について定めた規程に基づき，コンピュータウイルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。また，同規程に基づき，オペレーション管理に係る手順等を整備し，当該手順に従って，情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的（コンピュータウィルス関連情報は毎日，その他の情報は少なくとも半年一度）に入手し，機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。<br>(2)不正アクセス対策<br>・送付先情報の管理について定めた規程に基づき，ネットワーク管理に係る手順等を整備し，ファイアウォールを導入する。<br><br>＜ガバメントクラウドにおける措置＞<br>①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。<br>②地方公共団体が委託したASP（「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和4年10月 デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は，ガバメントクラウドが提供するマネージドサービスにより，ネットワークアクティビティ，データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに，ログ管理を行う。<br>③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し，脅威検出やDDos 対策を24 時間365日講じる。<br>④クラウド事業者は，ガバメントクラウドに対し，ウイルス対策ソフトを導入し，パターンファイルの更新を行う。<br>⑤地方公共団体が委託したASP 又はガバメントクラウド運用管理補助者は，導入しているOS 及びミドルウエアについて，必要に応じてセキュリティパッチの適用を行う。<br>⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は，インターネットとは切り離された閉域ネットワークで構成する。<br>⑦地方公共団体やASP 又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については，閉域ネットワークで構成する。<br>⑧地方公共団体が管理する業務データは，国及びクラウド事業者がアクセスできないよう制御を講じる。 | |

| | | |
|---|---|---|
| ⑦バックアップ | [　十分に行っている　] | ＜選択肢＞<br>1）特に力を入れて行っている　2）十分に行っている<br>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＞<br>1）特に力を入れて行っている　2）十分に行っている<br>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＞<br>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＞<br>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＞<br>1）特に力を入れている　2）十分である<br>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 | 以下のことから，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。<br>・送付先情報ファイルは，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，一定期間経過後にに削除する仕組みとする。<br>・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。 | |
| リスクへの対策は十分か | [　十分である　] | ＜選択肢＞<br>1）特に力を入れている　2）十分である<br>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＞<br>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なっている。<br><br>＜ガバメントクラウドにおける措置＞<br>データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001 等に準拠したプロセスにしたがって確実にデータを消去する。 | |
| 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＞<br>1）特に力を入れている　2）十分である<br>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，一定期間経過後，市町村CSから削除される。<br>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。 | | |

# 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 | |
|---|---|
| （4）コンビニ交付用ファイル | |
| **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 | コンビニ交付用ファイルの情報の入手元は既存住民基本台帳システムに限定されるため，既存住民基本台帳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の内容 | 中継サーバにおいて既存住民基本台帳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。 |
| 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＞<br>1）特に力を入れている　2）十分である<br>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 | 本人確認情報の入手元を既存住民基本台帳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＞<br>1）特に力を入れている　2）十分である<br>3）課題が残されている |
| 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民基本台帳システムに限定されており，既に本人確認された情報であるため，個別の措置は不要。 |
| 個人番号の真正性確認の措置の内容 | 個人番号の入手元は既存住民基本台帳システムに限定されており，既に真正性確認された情報であるため，個別の措置は不要。 |
| 特定個人情報の正確性確保の措置の内容 | 既存住民基本台帳システムにおいて正確性が確保されたコンビニ交付用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。 |
| 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＞<br>1）特に力を入れている　2）十分である<br>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。<br>・操作者の認証を行う。 |
| リスクへの対策は十分か | ［　　十分である　　］　＜選択肢＞<br>1）特に力を入れている　2）十分である<br>3）課題が残されている |
| 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置 | |
| ― | |

| 3. 特定個人情報の使用 | |
|---|---|
| リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク | |
| 宛名システム等における措置の内容 | 中継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中継サーバへのアクセスは既存住民基本台帳システムに限定しており，また，既存住民基本台帳システムと中継サーバ間では，コンビニ交付で使用する以外の情報との紐付けは行わない。 |
| 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 | 操作者認証を行う。 |
| 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)発効管理<br>・業務とアクセス権限（使用できる業務メニューの範囲，更新・閲覧等の区別等）の対応表を作成するとともに，アクセス権限の発効に際しては，利用者からの申請に基づき，中央窓口センター長が対応表を確認し，アクセス権限を発効する。<br>(2)失効管理<br>・権限を有していた職員が異動・退職した場合は，直ちに権限の失効を行う。 |
| 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 | ・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。<br>・不正アクセスを分析するために，管理端末においてアプリケーションの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 | ・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。<br>・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。<br>・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。 |
| 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 | 番号法及び番号法第9条第2項に基づく条例で認められた事務以外で特定個人情報の利用が禁止されていること，また，法令等に違反した場合の罰則について教育を徹底する。 |
| 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 | ・サーバ上の特定個人情報ファイルに直接アクセス（バックアップ処理，データ抽出等）できる者を限定するとともに，サーバでの操作ログを記録する。<br>・バックアップ処理以外に特定個人情報ファイルを複製しないことや，認められた処理以外で個人番号を含むデータ抽出を行わないことを関係者に徹底する。 |
| リスクへの対策は十分か | [ 十分である ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている |
| 特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置 | |
| ― | |

| 4. 特定個人情報ファイルの取扱いの委託 | | [　　]委託しない |
|---|---|---|
| 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<br>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<br>委託先による特定個人情報の保管・消去に関するリスク<br>委託契約終了後の不正な使用等のリスク<br>再委託に関するリスク | | |
| 情報保護管理体制の確認 | 委託業者と契約を締結する際は，事前に以下の項目について確認を行うとともに，契約締結後は，書面による報告を義務付ける。<br>・個人情報保護に関する規定，体制の整備<br>・個人情報保護に関する人的安全管理措置<br>・個人情報保護に関する技術的安全管理措置 | |
| 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＞<br>1）制限している　2）制限していない |
| 具体的な制限方法 | ・アクセス権限を付与する従業員数を必要最小限に限定する。<br>・従業員に付与するアクセス権限を必要最小限に限定する。 | |
| 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＞<br>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 | ・特定個人情報の利用履歴について，ユーザID，操作日時，処理事由等を記録する。<br>・記録は，５年間保存する。 | |
| 特定個人情報の提供ルール | [　定めている　] | ＜選択肢＞<br>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 | ・”コンビニ交付用システムの運用支援及び改修に関する業務”では，委託先には契約書に明記された以外の提供を一切認めない。<br>・委託先から他者に特定個人情報を提供する場合は，記録を残し，月1回確認を行う。 | |
| 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 | ・委託先には電子ファイル等の形式で特定個人情報を直接提供しない。<br>・特定個人情報の取扱いは，職員と同様にシステムを利用して行うこととする。 | |
| 特定個人情報の消去ルール | [　定めている　] | ＜選択肢＞<br>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 | ・業務上一時的に作成した特定個人情報ファイルは，不要となった時点で直ちに消去する。<br>・業務遂行に伴い出力した特定個人情報を含む帳票等については，不要になった時点で，定められた方法により廃棄する。<br>・情報の消去が適切に行われていることを，定期的に職員が確認する。 | |
| 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 | [　定めている　] | ＜選択肢＞<br>1）定めている　2）定めていない |
| 規定の内容 | ・目的外利用の禁止<br>・特定個人情報の閲覧者・更新者を制限<br>・特定個人情報の提供先の限定<br>・情報漏洩を防ぐための保管管理に責任を負う<br>・消去のルール<br>・特定個人情報の取扱いについて四半期に一度チェックを行った上で結果を報告をする<br>・必要に応じて，本市が委託先の視察・監査を行うことができる | |
| 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 | [　十分に行っている　] | ＜選択肢＞<br>1）特に力を入れて行ってい　2）十分に行っている<br>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 | 委託先と同等のリスク対策を実施する。 | |
| 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＞<br>1）特に力を入れている　2）十分である<br>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＞<br>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（送付先情報）の提供を行う際に，提供記録（提供日時、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＞<br>1）定めている　　2）定めていない |
| ルールの内容及びルール遵守の確認方法 | ・番号法及び住基法並びに高知市個人情報保護条例（平成18年条例第37号）の規定に基づき認められた提供・移転のみ許可をし，認められた方法以外での提供・移転を禁止する。<br>・提供・移転の記録を，定期的に確認する。 | |
| 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＞<br>1）特に力を入れている　　2）十分である<br>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（コンビニ交付用システム）と中継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移転はなされないことがシステム上担保される。<br>・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となっている。 | |
| リスクへの対策は十分か | [　　十分である　　] | ＜選択肢＞<br>1）特に力を入れている　　2）十分である<br>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 | (1)誤った情報を提供・移転してしまうリスクへの措置<br>・システム上，既存住民基本台帳システムから入手した情報の内容に編集を加えず，適切にコンビニ交付用システムに提供することを担保する。<br>(2)誤った相手に提供・移転してしまうリスクへの措置<br>・相手方（コンビニ交付用システム）と中継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移転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＞<br>1）特に力を入れている　　2）十分である<br>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＞<br>1）特に力を入れている 2）十分である<br>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＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| リスク3： 入手した特定個人情報が不正確であるリスク | |
| 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＞<br>1）特に力を入れている 2）十分である<br>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 | |
| リスクへの対策は十分か | [ ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| 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＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| 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＞<br>1）特に力を入れている 2）十分である<br>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 | |
| リスクへの対策は十分か | [ ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>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><br>1）特に力を入れて遵守している 2）十分に遵守している<br>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><br>1）特に力を入れて整備している 2）十分に整備している<br>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><br>1）特に力を入れて整備している 2）十分に整備している<br>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><br>1）特に力を入れて周知している 2）十分に周知している<br>3）十分に周知していない |
| ⑤物理的対策 | [ 特に力を入れて行っている ] | <選択肢><br>1）特に力を入れて行っている 2）十分に行っている<br>3）十分に行っていない |
| 具体的な対策の内容 | (1)サーバ<br>・入退室管理されたサーバ室内の施錠管理された専用ラックに設置する。<br>・入退室管理装置及び監視カメラによる入退室者の記録を行う。<br>(2)記録媒体（バックアップ媒体等）<br>・施錠できる保管庫等で管理する。<br>・事故，自然災害等によるデータの滅失等を回避するため，遠隔地での分散保管を実施。<br>(3)紙媒体<br>・施錠できる保管庫等で管理する。<br><br>＜ガバメントクラウドにおける措置＞<br>①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており，システムのサーバー等は，クラウド事業者が保有・管理する環境に構築し，その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。<br>②事前に許可されていない装置等に関しては，外部に持出できないこととしている。 | |
| ⑥技術的対策 | [ 十分に行っている ] | <選択肢><br>1）特に力を入れて行っている 2）十分に行っている<br>3）十分に行っていない |
| 具体的な対策の内容 | (1)不正プログラム対策<br>・コンピュータウイルス監視ソフトを使用し，サーバ・端末双方でウイルスチェックを実施する。また，新種の不正プログラムに対応するために，ウイルスパターンファイルは定期的に更新し，可能な限り最新のものを使用する。<br>・送付先情報の管理について定めた規程に基づき，コンピュータウイルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。また，同規程に基づき，オペレーション管理に係る手順等を整備し，当該手順に従って，情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的（コンピュータウィルス関連情報は毎日，その他の情報は少なくとも半年に一度）に入手し，機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。<br>(2)不正アクセス対策<br>・送付先情報の管理について定めた規程に基づき，ネットワーク管理に係る手順等を整備し，ファイアウォールを導入する。<br><br>＜ガバメントクラウドにおける措置＞<br>①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。<br>②地方公共団体が委託したASP（「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和4年10月 デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は，ガバメントクラウドが提供するマネージドサービスにより，ネットワークアクティビティ，データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに，ログ管理を行う。<br>③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し，脅威検出やDDos 対策を24 時間365日講じる。<br>④クラウド事業者は，ガバメントクラウドに対し，ウイルス対策ソフトを導入し，パターンファイルの更新を行う。<br>⑤地方公共団体が委託したASP 又はガバメントクラウド運用管理補助者は，導入しているOS 及びミドルウエアについて，必要に応じてセキュリティパッチの適用を行う。<br>⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は，インターネットとは切り離された閉域ネットワークで構成する。<br>⑦地方公共団体やASP 又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については，閉域ネットワークで構成する。<br>⑧地方公共団体が管理する業務データは，国及びクラウド事業者がアクセスできないよう制御を講じる。 | |

| | | |
|---|---|---|
| ⑦バックアップ | [　十分に行っている　] | ＜選択肢＞<br>1）特に力を入れて行っている　2）十分に行っている<br>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＞<br>1）特に力を入れて行っている　2）十分に行っている<br>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＞<br>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＞<br>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＞<br>1）特に力を入れている　2）十分である<br>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 | 以下のことから，コンビニ交付用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。<br>・コンビニ交付用ファイルは，連携を行う必要が生じた都度作成・連携することとしている。 | |
| リスクへの対策は十分か | [　十分である　] | ＜選択肢＞<br>1）特に力を入れている　2）十分である<br>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＞<br>1）定めている　2）定めていない |
| 手順の内容 | システム上，消除者の特定個人情報を削除する仕組みとなっている。<br><br>＜ガバメントクラウドにおける措置＞<br>データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001 等に準拠したプロセスにしたがって確実にデータを消去する。 | |
| 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＞<br>1）特に力を入れている　2）十分である<br>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 | | |
| コンビニ交付用ファイルは，機構への特定個人情報の提供後，消除者の情報が削除される。<br>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，コンビニ交付用ファイルのバックアップは取得しない。 | | |

# Ⅳ　その他のリスク対策 ※

## 1. 監査

| | | |
|---|---|---|
| ①自己点検 | [　　十分に行っている　　] | ＜選択肢＞<br>1) 特に力を入れて行っている　2) 十分に行っている<br>3) 十分に行っていない |
| 具体的なチェック方法 | ＜高知市における措置＞<br>・評価書の記載内容どおり運用が行われているか年に1回自己点検を行う。<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・運用規則等に基づき，中間サーバ・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 | [　　十分に行っている　　] | ＜選択肢＞<br>1) 特に力を入れて行っている　2) 十分に行っている<br>3) 十分に行っていない |
| 具体的な内容 | ＜高知市における措置＞<br>監査方式：内部監査<br>監査責任者：情報政策課長<br>監査実施体制：情報政策課特定個人情報保護評価担当者（数名）<br>監査の頻度：年１回<br>監査手法：監査事項に対する書面回答及び現地監査<br>※現地監査は，情報政策課が決定した部署のみ（毎年数部署を抽出して実施）<br>監査事項：評価書記載事項及び各部署で策定している情報セキュリティ実施手順の記載事項に対する運用状況<br>監査結果の活用：結果に基づき運用改善を実施<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・運用規則等に基づき，中間サーバ・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。<br><br>＜ガバメントクラウドにおける措置＞<br>ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、ISMAP において，クラウドサービス事業者は定期的にISMAP 監査機関リストに登録された監査機関による監査を行うこととしている。 | |

## 2. 従業者に対する教育・啓発

| | | |
|---|---|---|
| 従業者に対する教育・啓発 | [　　十分に行っている　　] | ＜選択肢＞<br>1) 特に力を入れて行っている　2) 十分に行っている<br>3) 十分に行っていない |
| 具体的な方法 | ＜高知市における措置＞<br>・職員（派遣職員を含む）に対しては，配属時（新規事務従事時）及び年１回，個人情報保護，特定個人情報の取扱い，法令等に違反した場合の罰則，情報セキュリティ等に関する研修を実施する。<br>・委託業者に対しては，契約書に個人情報（特定個人情報を含む）保護に関する条文を規定するとともに，業務に従事する従業員に対して，着任時及び年１回，職員に対する研修と同等の研修の実施及び結果報告を義務付ける。<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・中間サーバ・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。<br>・中間サーバ・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・プラットフォームにおける措置＞
・中間サーバ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。

＜ガバメントクラウドにおける措置＞
ガバメントクラウド上での業務データの取扱いについては，当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP 又はガバメントクラウド運用管理補助者が責任を有する。
ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については，原則としてガバメントクラウドに起因する事象の場合は，国はクラウド事業者と契約する立場から，その契約を履行させることで対応する。また，ガバメントクラウドに起因しない事象の場合は，地方公共団体に業務アプリケーションサービスを提供するASP 又はガバメントクラウド運用管理補助者が対応するものとする。
具体的な取り扱いについて、疑義が生じる場合は，地方公共団体とデジタル庁及び関係者で協議を行う。

# 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 | 総務部　政策推進室　広聴広報課　情報公開・市民相談センター<br>高知市本町五丁目１番45号　電話　088-823-9412<br>市民協働部　中央窓口センター<br>高知市本町五丁目１番45号　電話088-823-9432 |
| ②請求方法 | 指定の様式による書面の提出（電話等の口頭は不可）により，開示，訂正及び利用停止請求を受け付ける。 |
| 特記事項 | ― |
| ③手数料等 | [　　無料　　]　　＜選択肢＞<br>1) 有料　　2) 無料<br>（手数料額、納付方法：　　） |
| ④個人情報ファイル簿の公表 | [　　行っている　　]　　＜選択肢＞<br>1) 行っている　　2) 行っていない |
| 個人情報ファイル名 | 住民基本台帳 |
| 公表場所 | 総務部　政策推進室　広聴広報課　情報公開・市民相談センター<br>高知市本町五丁目１番45号　電話　088-823-9412 |
| 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 | 市民協働部　中央窓口センター<br>高知市本町五丁目１番45号<br>電話　088-823-9430 |
| ②対応方法 | 問合せ時に問合せ受付票を起票し，問合せに対する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 | 令和6年10月1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　　]<br>＜選択肢＞<br>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<br>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）<br>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）<br>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 | 高知市パブリックコメント制度に基づき，高知市広報及び高知市ホームページで告知し，郵送・電子メール・FAXにより意見募集を行った。 |
| ②実施日・期間 | 令和6年11月5日から令和6年12月4日 |
| ③期間を短縮する特段の理由 | |
| ④主な意見の内容 | |
| ⑤評価書への反映 | |
| **3. 第三者点検** | |
| ①実施日 | |
| ②方法 | |
| ③結果 | |
| **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 |
|---|---|---|---|---|---|
| 令和6年10月1日 | Ⅰ基本情報　1．特定個人情報ファイルの取り扱う事務②事務の内容 | 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，市町村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に行うものであり，市町村において，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なるものである。<br>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）を都道府県と共同して構築している。<br><br>高知市は，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）<br><br>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<br>②転入届，転居届，転出届，世帯変更届等の届出（電子申請機能による申請管理システムからの電子申請データを基幹システムに取り込むことを含む）又は職権に基づく住民票の記載，消除又は記載の修正<br>③住民基本台帳の正確な記録を確保するための措置<br>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<br>⑤本人又は同一の世帯に属する者の請求による住民票の写し等の交付<br>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 | 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，市町村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に行うものであり，市町村において，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なるものである。<br>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）を都道府県と共同して構築している。<br>高知市は，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）<br>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<br>②転入届，転居届，転出届，世帯変更届等の届出（電子申請機能による申請管理システムからの電子申請データを基幹システムに取り込むことを含む）又は職権に基づく住民票の記載，消除又は記載の修正<br>③住民基本台帳の正確な記録を確保するための措置<br>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<br>⑤本人又は同一の世帯に属する者の請求による住民票の写し等の交付<br>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<br>⑦地方公共団体情報システム機構（以下「機構」という。）への本人確認情報の照会 | 事後 | 改正番号法施行に伴う評価書の修正（番号法別表第二の削除関係） |
| 令和6年10月1日 | Ⅰ基本情報　4．特定個人情報ファイルを取り扱う理由①事務実施上の必要性 | （1）住民基本台帳ファイル<br>本市では，住民基本台帳事務がシステム化されており，当該特定個人情報ファイルは，住民基本台帳の原本として取り扱われるものである。<br><br>（2）本人確認情報ファイル<br>本人確認情報ファイルは，転出入があった場合等にスムーズな住民情報の処理を行うため，また全国的な本人確認手段として，1つの市町村内にとどまらず全地方公共団体で本人確認情報を正確かつ統一的に記録・管理することを目的として，以下の用途に用いられる。<br><br>①住基ネットを用いて市町村の区域を越えた住民基本台帳に関する事務の処理を行うため，<br>区域内の住民に係る最新の本人確認情報を管理する。<br>②都道府県に対し，本人確認情報の更新情報を通知する。<br>③申請・届出の際に提示された個人番号カード等を用いた本人確認を行う。<br>④個人番号カードを利用した転入手続きを行う。<br>⑤住民基本台帳に関する事務において，本人確認情報を検索する。<br>⑥都道府県知事保存本人確認情報及び機構保存本人確認情報との整合性を確認する。<br><br>（3）送付先情報ファイル<br>市町村長が個人番号を指定した際は全付番対象者に個人番号を通知するものとされている（番号法第7条第1項）。個人番号通知書による番号の通知及び個人番号カード交付通知書の送付については，事務効率化等の観点から，市町村から機構に委任しており，機構に個 | （1）住民基本台帳ファイル<br>本市では，住民基本台帳事務がシステム化されており，当該特定個人情報ファイルは，住民基本台帳の原本として取り扱われるものである。<br><br>（2）本人確認情報ファイル<br>本人確認情報ファイルは，転出入があった場合等にスムーズな住民情報の処理を行うため，また全国的な本人確認手段として，1つの市町村内にとどまらず全地方公共団体で本人確認情報を正確かつ統一的に記録・管理することを目的として，以下の用途に用いられる。<br>①住基ネットを用いて市町村の区域を越えた住民基本台帳に関する事務の処理を行うため，区域内の住民に係る最新の本人確認情報を管理する。<br>②都道府県に対し，本人確認情報の更新情報を通知する。<br>③申請・届出の際に提示された個人番号カード等を用いた本人確認を行う。<br>④個人番号カードを利用した転入手続きを行う。<br>⑤住民基本台帳に関する事務において，本人確認情報を検索する。<br>⑥都道府県知事保存本人確認情報及び機構保存本人確認情報との整合性を確認する。<br><br>（3）送付先情報ファイル<br>市町村長が個人番号を指定した際は全付番対象者に個人番号を通知するものとされている（番号法第7条第1項）。個人番号通知書による番号の通知及び個人番号カード交付通知書の送付については，事務効率化等の観点から，市町村から機構に委任しており，機構に個人番号通知書及び交付申請書の送付先情報を提供する。（個人番号，個人番号カード命令 | 事後 | 個人番号カード省令の改正に伴う評価書の修正 |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 令和6年10月1日 | Ⅰ基本情報　6．情報提供ネットワークによ情報連携②法令上の根拠 | ・番号法第19条第8号（特定個人情報の提供の制限）及び別表第二及び行政手続における特定の個人を識別するための番号の利用等に関する法律別表第二の主務省令で定める事務及び情報を定める命令（平成26年12月12日内閣府・総務省令第7号。以下「別表第二主務省令」という。）<br><br>（別表第二における情報提供の根拠）<br>・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「住民票関係情報」が含まれる項<br>（1，2，3，4，6，8，9，11，16，18，20，23，27，30，31，34，35，37，38，39，40，42，48，53，54，<br>57，58，59，61，62，66，67，70，74，77，80，84，85の2，89，91，92，94，96，97，101，102，103，105，106，107，108，111，112，113，114，116，117，120の項）<br>（別表第二主務省令で定める情報として「住民票関係情報」が含まれる条文）<br>（1，2，3，4，6，7，8，10，12，13，14，16，20，22，22条の3，22条の4，23，24，24条の2，24条の3，25，26条の3，27，28，31，31条の2の2，31条の3，32，33，37，38，39，40，41，43，43条の3，43条の4，44条の2，44条の5，45，47，48，49条の2，53，55，56，57，58，59，59条の2，59条の3の各条）<br><br>（別表第二における情報照会の根拠）<br>・なし（情報提供ネットワークシステムによる情報照会は行わない） | ○行政手続における特定の個人を識別するための番号の利用等に関する法律第十九条第八号に基づく利用特定個人情報の提供に関する命令（令和6年5月27 日デジタル庁・総務省令第9号。以下「番号法第19 条第8号に基づく主務省令」という。）<br>（情報提供の根拠）<br>・番号法第19 条第8号に基づく主務省令第2条の別表（1，2，3，5，7，11，13，15，20，28，37，39，48，53，57，58，59，63，65，66，69，73，75，76，81，83，84，86，87，91，92，96，106，108，110，112，115，118，124，129，130，132，136，137，138，141，142，144，149，150，151，152，155，156，158，160，163，164，165，166）の項<br><br>（情報照会の根拠）<br>・なし | 事後 | 改正番号法施行に伴う評価書の修正（番号法別表第二の削除関係） |
| 令和6年10月1日 | （別添1）事務内容 | | 戸籍照合通知，住民票記載事項通知が住基ネット経由の追加及び他市町村等側のネットワークの削除 | 事後 | 戸籍照合通知，住民票記載事項通知が住基ネット経由の追加及び他市町村等のネットワークの削除 |
| 令和6年10月1日 | Ⅱ ファイルの概要5．特定個人情報の提供・移転（委託に伴うものを除く。）提供先1 | 番号法別表第二に規定する住民票関係情報の照会者　（詳細は別紙1参照） | 番号第十九条第八号に基づく利用特定個人情報の提供に関する命令第二条の表に規定する住民票関係情報の照会者　（詳細は別紙1参照） | 事後 | 改正番号法施行に伴う評価書の修正（番号法別表第二の削除関係） |
| 令和6年10月1日 | Ⅱ ファイルの概要5．特定個人情報の提供・移転（委託に伴うものを除く。）提供先1①法令上の根拠 | 番号法別表第二（項番1，2，3，4，6，8，9，11，16，18，20，21，23，27，30，31，34，35，37，38，39，40，42，48，53，54，57，58，59，61，62，66，67，70，74，77，80，84，85の2，89，91，92，94，96，97，101，102，103，105，107，106，108，111，112，113，114，116，117，120） | ○行政手続における特定の個人を識別するための番号の利用等に関する法律第十九条第八号に基づく利用特定個人情報の提供に関する命令（令和6年5月27 日デジタル庁・総務省令第9号。以下「番号法第19 条第8号に基づく主務省令」という。）<br><br>（情報提供の根拠）<br>・番号法第19 条第8号に基づく主務省令第2条の別表（1，2，3，5，7，11，13，15，20，28，37，39，48，53，57，58，59，63，65，66，69，73，75，76，81，83，84，86，87，91，92，96，106，108，110，112，115，118，124，129，130，132，136，137，138，141，142，144，149，150，151，152，155，156，158，160，163，164，165，166）の項 | 事後 | 改正番号法施行に伴う評価書の修正（番号法別表第二の削除関係） |
| 令和6年10月1日 | Ⅱ ファイルの概要6．特定個人情報の保管・消去①保管場所 | ＜高知市における措置＞<br>・カメラ監視付きの入退室管理を行っているサーバ室内で，鍵付き専用ラックに搭載されたサーバ内に保管。<br>・サーバへのアクセスは，ID／パスワードによる認証が必要。<br>・システム内のデータは，セキュリティゲートにて入退館管理をしている建物のうち，さらに厳格な入退室管理を行っている区画に設置したサーバ内に保管している。<br>・外部記憶媒体は，施錠できるキャビネットに保管している。<br>＜中間サーバ・プラットフォームにおける措置＞<br>・中間サーバ・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。<br>・特定個人情報は，サーバ室に設置された中間サーバ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。 | ＜高知市における措置＞<br>・カメラ監視付きの入退室管理を行っているサーバ室内で，鍵付き専用ラックに搭載されたサーバ内に保管。<br>・サーバへのアクセスは，ID／パスワードによる認証が必要。<br>・システム内のデータは，セキュリティゲートにて入退館管理をしている建物のうち，さらに厳格な入退室管理を行っている区画に設置したサーバ内に保管している。<br>・外部記憶媒体は，施錠できるキャビネットに保管している。<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・中間サーバ・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。<br>・特定個人情報は，サーバ室に設置された中間サーバ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。<br><br>＜ガバメントクラウドにおける措置＞<br>①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAP のリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。<br>・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。<br>・日本国内でのデータ保管を条件としていること。<br>②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数 | 事前 | ガバメントクラウドへ移行のため |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 令和6年10月1日 | Ⅱ ファイルの概要6．特定個人情報の保管・消去③消去方法 | ＜高知市における措置＞<br>・サーバ内の特定個人情報については，サーバの機器更新時等に完全に消去する。<br>・バックアップ媒体については，破砕処理を実施。<br>・申請書等の紙媒体については，焼却処理を行う。<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・特定個人情報の消去は高知市からの操作によって実施されるため，通常，中間サーバ・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。<br>・ディスク交換やハード更改等の際は，中間サーバ・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完全に消去を行う。<br><br>＜申請管理システムにおける措置＞<br>・申請管理システムに記録した個人番号付電子申請データは，データ連携後に速やかに完全消去する。<br>・外部記憶媒体に一時的に記録した場合は、個人番号付電子申請データを使用の都度速やかに完全消去する。 | ＜高知市における措置＞<br>・サーバ内の特定個人情報については，サーバの機器更新時等に完全に消去する。<br>・バックアップ媒体については，破砕処理を実施。<br>・申請書等の紙媒体については，焼却処理を行う。<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・特定個人情報の消去は高知市からの操作によって実施されるため，通常，中間サーバ・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。<br>・ディスク交換やハード更改等の際は，中間サーバ・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完全に消去を行う。<br><br>＜申請管理システムにおける措置＞<br>・申請管理システムに記録した個人番号付電子申請データは，データ連携後に速やかに完全消去する。<br>・外部記憶媒体に一時的に記録した場合は、個人番号付電子申請データを使用の都度速やかに完全消去する。<br><br>＜ガバメントクラウドにおける措置＞<br>①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。<br>②クラウド事業者がHDD やSSD などの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001 | 事前 | ガバメントクラウドへ移行のため |
| 令和6年10月1日 | Ⅱ ファイルの概要（2）6．特定個人情報の保管・消去①保管場所 | ・カメラ監視付きの入退室管理を行っているサーバ室内で，鍵付き専用ラックに搭載されたサーバ内に保管。<br>・サーバへのアクセスは，ID／パスワードによる認証が必要。 | ・カメラ監視付きの入退室管理を行っているサーバ室内で，鍵付き専用ラックに搭載されたサーバ内に保管。<br>・サーバへのアクセスは，ID／パスワードによる認証が必要。<br><br>＜ガバメントクラウドにおける措置＞<br>①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAP のリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。<br>・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。<br>・日本国内でのデータ保管を条件としていること。<br>②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 | 事前 | ガバメントクラウドへ移行のため |
| 令和6年10月1日 | Ⅱ ファイルの概要（2）6．特定個人情報の保管・消去③消去方法 | ・サーバ内の特定個人情報については，サーバの機器更新時等に完全に消去する。<br>・バックアップ媒体については，破砕処理を実施。<br>・申請書等の紙媒体については，焼却処理を行う。 | ・サーバ内の特定個人情報については，サーバの機器更新時等に完全に消去する。<br>・バックアップ媒体については，破砕処理を実施。<br>・申請書等の紙媒体については，焼却処理を行う。<br><br>＜ガバメントクラウドにおける措置＞<br>①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。<br>②クラウド事業者がHDD やSSD などの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。<br>③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 | 事前 | ガバメントクラウドへ移行のため |
| 令和6年10月1日 | Ⅱ ファイルの概要（3）2．基本情報③対象となる本人の範囲−その必要性 | 番号法第7条第1項（指定及び通知）に基づき，当該個人番号を通知する必要がある。また，同法第17条第1項（個人番号カードの交付等）により，本人の申請により，個人番号カードを交付することとされていることから，必要に応じて交付申請書を該当者に送付する必要がある。市町村は，個人番号，個人番号カード省令第35条（個人番号通知書・個人番号カード関連事務の委任）に基づき，これらの事務の実施を機構に委任する。 | 番号法第7条第1項（指定及び通知）に基づき，当該個人番号を通知する必要がある。また，同法第17条第1項（個人番号カードの交付等）により，本人の申請により，個人番号カードを交付することとされていることから，必要に応じて交付申請書を該当者に送付する必要がある。市町村は，個人番号，個人番号カード命令第35条（個人番号通知書・個人番号カード関連事務の委任）に基づき，これらの事務の実施を機構に委任する。 | 事後 | 個人番号カード省令の改正に伴う評価書の修正 |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 令和6年10月1日 | Ⅱ ファイルの概要（3）2. 基本情報④記録される項目-その妥当性 | (1)個人番号，4情報，その他住民票関係情報<br>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。<br>(2)その他（個人番号通知書及び交付申請書の送付先の情報）<br>機構に対し，個人番号，個人番号カード省令第35条（個人番号通知書・個人番号カード関連事務の委任）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。 | (1)個人番号，4情報，その他住民票関係情報<br>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。<br>(2)その他（個人番号通知書及び交付申請書の送付先の情報）<br>機構に対し，個人番号，個人番号カード命令第35条（個人番号通知書・個人番号カード関連事務の委任）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。 | 事後 | 個人番号カード省令の改正に伴う評価書の修正 |
| 令和6年10月1日 | Ⅱ ファイルの概要（3）3. 特定個人の入手・使用⑤本人への明示 | 個人番号カード省令第23条の2（個人番号通知書及び個人番号カードに関し機構が処理する事務）により広く国民に示されている。 | 個人番号カード命令第23条の2（個人番号通知書及び個人番号カードに関し機構が処理する事務）により広く国民に示されている。 | 事後 | 個人番号カード省令の改正に伴う評価書の修正 |
| 令和6年10月1日 | Ⅱ ファイルの概要（3）3. 特定個人の入手・使用⑥使用目的 | 個人番号，個人番号カード省令第35条（個人番号通知書・個人番号カード関連事務の委任）に基づく委任を受けて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行う機構に対し，個人番号通知書及び交付申請書の送付先情報を提供するため。 | 個人番号，個人番号カード命令第35条（個人番号通知書・個人番号カード関連事務の委任）に基づく委任を受けて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行う機構に対し，個人番号通知書及び交付申請書の送付先情報を提供するため。 | 事後 | 個人番号カード省令の改正に伴う評価書の修正 |
| 令和6年10月1日 | Ⅱ ファイルの概要（3）3. 特定個人の入手・使用⑧使用方法 | 既存住民基本台帳システムより個人番号の通知対象者の情報を抽出し，個人番号通知書及び交付申請書等の印刷及び送付に係る事務を個人番号，個人番号カード省令第35条（個人番号通知書・個人番号カード関連事務の委任）に基づいて委任する機構に対し提供する（既存住民基本台帳システム→市町村CS→個人番号カード管理システム（機構））。 | 既存住民基本台帳システムより個人番号の通知対象者の情報を抽出し，個人番号通知書及び交付申請書等の印刷及び送付に係る事務を個人番号，個人番号カード命令第35条（個人番号通知書・個人番号カード関連事務の委任）に基づいて委任する機構に対し提供する（既存住民基本台帳システム→市町村CS→個人番号カード管理システム（機構））。 | 事後 | 個人番号カード省令の改正に伴う評価書の修正 |
| 令和6年10月1日 | Ⅱ ファイルの概要（3）5. 特定個人情報の提供・移転-提供先1①法令上の根拠 | 個人番号，個人番号カード省令第35条（個人番号通知書・個人番号カード関連事務の委任） | 個人番号，個人番号カード命令第35条（個人番号通知書・個人番号カード関連事務の委任） | 事後 | 個人番号カード省令の改正に伴う評価書の修正 |
| 令和6年10月1日 | Ⅱ ファイルの概要（3）5. 特定個人情報の提供・移転-提供先1②提供先における用途 | 市町村からの個人番号通知書，個人番号カード省令第35条（個人番号通知書・個人番号カード関連事務の委任）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。 | 市町村からの個人番号通知書，個人番号カード命令第35条（個人番号通知書・個人番号カード関連事務の委任）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。 | 事後 | 個人番号カード省令の改正に伴う評価書の修正 |
| 令和6年10月1日 | Ⅱ ファイルの概要（3）6. 特定個人情報の保管・消去①保管場所 | ・カメラ監視付きの入退室管理を行っているサーバ室内で，鍵付き専用ラックに搭載されたサーバ内に保管。<br>・サーバへのアクセスは，ID／パスワードによる認証が必要。 | ・カメラ監視付きの入退室管理を行っているサーバ室内で，鍵付き専用ラックに搭載されたサーバ内に保管。<br>・サーバへのアクセスは，ID／パスワードによる認証が必要。<br><br>＜ガバメントクラウドにおける措置＞<br>①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAP のリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。<br>・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。<br>・日本国内でのデータ保管を条件としていること。<br>②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 | 事前 | ガバメントクラウドへ移行のため |
| 令和6年10月1日 | Ⅱ ファイルの概要（3）6. 特定個人情報の保管・消去③消去方法 | ・保存期間が到来した本人確認情報は，機構より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。 | ・サーバ内の特定個人情報については，サーバの機器更新時等に完全に消去する。<br>・バックアップ媒体については，破砕処理を実施。<br>・申請書等の紙媒体については，焼却処理を行う。<br><br>＜ガバメントクラウドにおける措置＞<br>①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。<br>②クラウド事業者がHDD やSSD などの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、ST800-88、ISO/IEC27001等にしたがって確実にデータを消去する。<br>③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 | 事前 | ガバメントクラウドへ移行のため |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 令和6年10月1日 | Ⅱ ファイルの概要（4）6．特定個人情報の保管・消去①保管場所 | ・カメラ監視付きの入退室管理を行っているサーバ室内で，鍵付き専用ラックに搭載されたサーバ内に保管。<br>・サーバへのアクセスは，ID／パスワードによる認証が必要。 | ・カメラ監視付きの入退室管理を行っているサーバ室内で，鍵付き専用ラックに搭載されたサーバ内に保管。<br>・サーバへのアクセスは，ID／パスワードによる認証が必要。<br><br>＜ガバメントクラウドにおける措置＞<br>①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAP のリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。<br>・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。<br>・日本国内でのデータ保管を条件としていること。<br>②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 | 事前 | ガバメントクラウドへ移行のため |
| 令和6年10月1日 | Ⅱ ファイルの概要（4）6．特定個人情報の保管・消去③消去方法 | ・サーバ内の特定個人情報については，サーバの機器更新時等に完全に消去する。<br>・バックアップ媒体については，破砕処理を実施。<br>・申請書等の紙媒体については，焼却処理を行う。<br>・消除者の特定個人情報の消去は高知市からの操作によって実施される。 | ・サーバ内の特定個人情報については，サーバの機器更新時等に完全に消去する。<br>・バックアップ媒体については，破砕処理を実施。<br>・申請書等の紙媒体については，焼却処理を行う。<br>・消除者の特定個人情報の消去は高知市からの操作によって実施される。<br><br>＜ガバメントクラウドにおける措置＞<br>①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。<br>②クラウド事業者がHDD やSSD などの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST800-88、ISO/IEC27001等にしたがって確実にデータを消去する。<br>③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 | 事前 | ガバメントクラウドへ移行のため |
| 令和6年10月1日 | Ⅲリスク対策（プロセス）7．特定個人情報の保管・消去⑤物理的対策－具体的な対策 | ＜高知市における措置＞<br>(1)サーバ<br>・入退室管理されたサーバ室内の施錠管理された専用ラックに設置する。<br>・入退室管理装置及び監視カメラによる入退室者の記録を行う。<br>(2)記録媒体（バックアップ媒体等）<br>・原則持ち込みを禁止とし，特に必要がある場合のみ許可とする。<br>・施錠できる保管庫等で管理する。<br>・事故，自然災害等によるデータの滅失等を回避するため，遠隔地での分散保管を実施。<br>(3)紙媒体<br>・施錠できる保管庫等で管理する。<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・中間サーバ・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。<br><br>＜申請管理システムにおける措置＞<br>・操作端末については、業務時間内のセキュリティワイヤー等による固定、操作場所への入退室管理、業務時間外の施錠できるキャビネット等への保管、などの物理的対策を講じている。<br>・外部記憶媒体については、限定された USBメモリ等以外の利用不可、施錠できるキャビネット等への保管、使用管理簿による管理、などの安全管理措置を講じている。 | ＜高知市における措置＞<br>(1)サーバ<br>・入退室管理されたサーバ室内の施錠管理された専用ラックに設置する。<br>・入退室管理装置及び監視カメラによる入退室者の記録を行う。<br>(2)記録媒体（バックアップ媒体等）<br>・原則持ち込みを禁止とし，特に必要がある場合のみ許可とする。<br>・施錠できる保管庫等で管理する。<br>・事故，自然災害等によるデータの滅失等を回避するため，遠隔地での分散保管を実施。<br>(3)紙媒体<br>・施錠できる保管庫等で管理する。<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・中間サーバ・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。<br><br>＜申請管理システムにおける措置＞<br>・操作端末については、業務時間内のセキュリティワイヤー等による固定、操作場所への入退室管理、業務時間外の施錠できるキャビネット等への保管、などの物理的対策を講じている。<br>・外部記憶媒体については、限定された USBメモリ等以外の利用不可、施錠できるキャビネット等への保管、使用管理簿による管理、などの安全管理措置を講じている。<br><br>＜ガバメントクラウドにおける措置＞<br>①ガバメントクラウドについては政府情報シス | 事前 | ガバメントクラウドへ移行のため |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 令和6年10月1日 | Ⅲリスク対策（プロセス）7．特定個人情報の保管・消去⑥技術的対策－具体的な対策 | ＜高知市における措置＞<br>(1)ウィルス対策<br>・全てのサーバ及び端末にウィルス対策ソフトを導入する。<br>・定期的なパターンファイルの更新，リアルタイムでの監視，週1回の全ファイルチェックを実施する。<br>(2)OS等の修正プログラムの適用<br>・全てのサーバ及び端末に対して，OS等の修正プログラムの適用を行う。<br>(3)不正アクセス対策<br>・外部のネットワークとは，ファイアウォールを介して接続し，不正アクセスの監視を行う。<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・中間サーバ・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。<br>・中間サーバ・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。<br>・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。<br><br>＜申請管理システムにおける措置＞<br>・操作端末へのウイルス検出ソフトウェア等の導入により、ウイルス定義ファイルの定期的な更新及びウイルスチェックを行い、マルウェア検出を行う。<br>・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。 | ＜高知市における措置＞<br>(1)ウィルス対策<br>・全てのサーバ及び端末にウィルス対策ソフトを導入する。<br>・定期的なパターンファイルの更新，リアルタイムでの監視，週1回の全ファイルチェックを実施する。<br>(2)OS等の修正プログラムの適用<br>・全てのサーバ及び端末に対して，OS等の修正プログラムの適用を行う。<br>(3)不正アクセス対策<br>・外部のネットワークとは，ファイアウォールを介して接続し，不正アクセスの監視を行う。<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・中間サーバ・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。<br>・中間サーバ・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。<br>・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。<br><br>＜申請管理システムにおける措置＞<br>・操作端末へのウイルス検出ソフトウェア等の導入により、ウイルス定義ファイルの定期的な更新及びウイルスチェックを行い、マルウェア検出を行う。<br>・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 | ガバメントクラウドへ移行のため |
| 令和6年10月1日 | Ⅲリスク対策（プロセス）7．特定個人情報の保管・消去リスク3消去手順－手順の内容 | ・住民基本台帳は，消除者についても記録を保持しておく必要があり，当該特定個人情報は実質永年保管となるため，データベース上の各データについては消去手順は定めていない。<br>・サーバの機器更新時等においては，情報の復元が不可能な専用ソフトによりハードディスクの消去作業を行っている。<br>・バックアップ媒体については，保管期限が経過したものについて破砕処理を行っている。<br>・紙媒体については，保管期限が経過したものについて，焼却処理を行っている。<br>・操作端末については、業務終了後に不要な個人番号付電子申請データ等の消去について徹底し、必要に応じて管理者が確認する。<br>・外部記憶媒体については、定期的に内部のチェックを行い不要なデータの確認を行い、廃棄する場合は管理者の承認を得て行う手順を定めている。 | ・住民基本台帳は，消除者についても記録を保持しておく必要があり，当該特定個人情報は実質永年保管となるため，データベース上の各データについては消去手順は定めていない。<br>・サーバの機器更新時等においては，情報の復元が不可能な専用ソフトによりハードディスクの消去作業を行っている。<br>・バックアップ媒体については，保管期限が経過したものについて破砕処理を行っている。<br>・紙媒体については，保管期限が経過したものについて，焼却処理を行っている。<br>・操作端末については、業務終了後に不要な個人番号付電子申請データ等の消去について徹底し、必要に応じて管理者が確認する。<br>・外部記憶媒体については、定期的に内部のチェックを行い不要なデータの確認を行い、廃棄する場合は管理者の承認を得て行う手順を定めている。<br><br>＜ガバメントクラウドにおける措置＞<br>データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001 等に準拠したプロセスにしたがって確実にデータを消去する。 | 事前 | ガバメントクラウドへ移行のため |
| 令和6年10月1日 | Ⅲリスク対策（プロセス）（2）7．特定個人情報の保管・消去⑤物理的対策－具体的な対策 | (1)サーバ<br>・入退室管理されたサーバ室内の施錠管理された専用ラックに設置する。<br>・入退室管理装置及び監視カメラによる入退室者の記録を行う。<br>(2)記録媒体（バックアップ媒体等）<br>・施錠できる保管庫等で管理する。<br>・事故，自然災害等によるデータの滅失等を回避するため，遠隔地での分散保管を実施。<br>(3)紙媒体<br>・施錠できる保管庫等で管理する。 | (1)サーバ<br>・入退室管理されたサーバ室内の施錠管理された専用ラックに設置する。<br>・入退室管理装置及び監視カメラによる入退室者の記録を行う。<br>(2)記録媒体（バックアップ媒体等）<br>・施錠できる保管庫等で管理する。<br>・事故，自然災害等によるデータの滅失等を回避するため，遠隔地での分散保管を実施。<br>(3)紙媒体<br>・施錠できる保管庫等で管理する。<br><br>＜ガバメントクラウドにおける措置＞<br>①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており，システムのサーバー等は，クラウド事業者が保有・管理する環境に構築し，その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。<br>②事前に許可されていない装置等に関しては、外部に持出できないこととしている。 | 事前 | ガバメントクラウドへ移行のため |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 令和6年10月1日 | Ⅲリスク対策（プロセス）（2）<br>7．特定個人情報の保管・消去⑥技術的対策－具体的な対策 | (1)不正プログラム対策<br>・コンピュータウイルス監視ソフトを使用し，サーバ・端末双方でウイルスチェックを実施する。また，新種の不正プログラムに対応するために，ウイルスパターンファイルは定期的に更新し，可能な限り最新のものを使用する。<br>・本人確認情報の管理について定めた規程に基づき，コンピュータウイルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。また，同規程に基づき，オペレーション管理に係る手順等を整備し，当該手順に従って，情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的（コンピュータウィルス関連情報は毎日，その他の情報は少なくとも半年に一度）に入手し，機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。<br><br>(2)不正アクセス対策<br>・本人確認情報の管理について定めた規程に基づき，ネットワーク管理に係る手順等を整備し，ファイアウォールを導入する。 | (1)不正プログラム対策<br>・コンピュータウイルス監視ソフトを使用し，サーバ・端末双方でウイルスチェックを実施する。また，新種の不正プログラムに対応するために，ウイルスパターンファイルは定期的に更新し，可能な限り最新のものを使用する。<br>・本人確認情報の管理について定めた規程に基づき，コンピュータウイルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。また，同規程に基づき，オペレーション管理に係る手順等を整備し，当該手順に従って，情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的（コンピュータウィルス関連情報は毎日，その他の情報は少なくとも半年に一度）に入手し，機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。<br><br>(2)不正アクセス対策<br>・本人確認情報の管理について定めた規程に基づき，ネットワーク管理に係る手順等を整備し，ファイアウォールを導入する。<br><br>＜ガバメントクラウドにおける措置＞<br>①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。<br>②地方公共団体が委託したASP（「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和４年１０月 デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は，ガバメントクラウドが提供するマネージドサービスにより，ネットワークアクティビティ，データアクセスパターン、アカウント動作等に | 事前 | ガバメントクラウドへ移行のため |
| 令和6年10月1日 | Ⅲリスク対策（プロセス）（2）<br>7．特定個人情報の保管・消去リスク3消去手順－手順の内容 | システム上，住民基本台帳法施行令第34条第3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。 | システム上，住民基本台帳法施行令第34条第3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。<br><br>＜ガバメントクラウドにおける措置＞<br>データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001 等に準拠したプロセスにしたがって確実にデータを消去する。 | 事前 | ガバメントクラウドへ移行のため |
| 令和6年10月1日 | Ⅲリスク対策（プロセス）（3）<br>7．特定個人情報の保管・消去⑤物理的対策－具体的な対策 | (1)サーバ<br>・入退室管理されたサーバ室内の施錠管理された専用ラックに設置する。<br>・入退室管理装置及び監視カメラによる入退室者の記録を行う。<br>(2)記録媒体（バックアップ媒体等）<br>・施錠できる保管庫等で管理する。<br>・事故，自然災害等によるデータの滅失等を回避するため，遠隔地での分散保管を実施。<br>(3)紙媒体<br>・施錠できる保管庫等で管理する。 | (1)サーバ<br>・入退室管理されたサーバ室内の施錠管理された専用ラックに設置する。<br>・入退室管理装置及び監視カメラによる入退室者の記録を行う。<br>(2)記録媒体（バックアップ媒体等）<br>・施錠できる保管庫等で管理する。<br>・事故，自然災害等によるデータの滅失等を回避するため，遠隔地での分散保管を実施。<br>(3)紙媒体<br>・施錠できる保管庫等で管理する。<br><br>＜ガバメントクラウドにおける措置＞<br>①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており，システムのサーバー等は，クラウド事業者が保有・管理する環境に構築し，その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。<br>②事前に許可されていない装置等に関しては，外部に持出できないこととしている。 | 事前 | ガバメントクラウドへ移行のため |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 令和6年10月1日 | Ⅲリスク対策（プロセス）（3）<br>7．特定個人情報の保管・消去⑥技術的対策－具体的な対策 | (1)不正プログラム対策<br>・コンピュータウイルス監視ソフトを使用し，サーバ・端末双方でウイルスチェックを実施する。また，新種の不正プログラムに対応するために，ウイルスパターンファイルは定期的に更新し，可能な限り最新のものを使用する。<br>・送付先情報の管理について定めた規程に基づき，コンピュータウイルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。また，同規程に基づき，オペレーション管理に係る手順等を整備し，当該手順に従って，情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的（コンピュータウィルス関連情報は毎日，その他の情報は少なくとも半年に一度）に入手し，機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。<br>(2)不正アクセス対策<br>・送付先情報の管理について定めた規程に基づき，ネットワーク管理に係る手順等を整備し，ファイアウォールを導入する。 | (1)不正プログラム対策<br>・コンピュータウイルス監視ソフトを使用し，サーバ・端末双方でウイルスチェックを実施する。また，新種の不正プログラムに対応するために，ウイルスパターンファイルは定期的に更新し，可能な限り最新のものを使用する。<br>・送付先情報の管理について定めた規程に基づき，コンピュータウイルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。また，同規程に基づき，オペレーション管理に係る手順等を整備し，当該手順に従って，情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的（コンピュータウィルス関連情報は毎日，その他の情報は少なくとも半年に一度）に入手し，機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。<br>(2)不正アクセス対策<br>・送付先情報の管理について定めた規程に基づき，ネットワーク管理に係る手順等を整備し，ファイアウォールを導入する。<br><br>＜ガバメントクラウドにおける措置＞<br>①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。<br>②地方公共団体が委託したASP（「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和4年10月 デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は，ガバメントクラウドが提供するマネージドサービスにより，ネットワークアクティビティ，データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに，ロ | 事前 | ガバメントクラウドへ移行のため |
| 令和6年10月1日 | Ⅲリスク対策（プロセス）（3）<br>7．特定個人情報の保管・消去リスク3消去手順－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なっている。 | 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なっている。<br><br>＜ガバメントクラウドにおける措置＞<br>データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001 等に準拠したプロセスにしたがって確実にデータを消去する。 | 事前 | ガバメントクラウドへ移行のため |
| 令和6年10月1日 | Ⅲリスク対策（プロセス）（4）<br>7．特定個人情報の保管・消去⑤物理的対策－具体的な対策 | (1)サーバ<br>・入退室管理されたサーバ室内の施錠管理された専用ラックに設置する。<br>・入退室管理装置及び監視カメラによる入退室者の記録を行う。<br>(2)記録媒体（バックアップ媒体等）<br>・施錠できる保管庫等で管理する。<br>・事故，自然災害等によるデータの滅失等を回避するため，遠隔地での分散保管を実施。<br>(3)紙媒体<br>・施錠できる保管庫等で管理する。 | (1)サーバ<br>・入退室管理されたサーバ室内の施錠管理された専用ラックに設置する。<br>・入退室管理装置及び監視カメラによる入退室者の記録を行う。<br>(2)記録媒体（バックアップ媒体等）<br>・施錠できる保管庫等で管理する。<br>・事故，自然災害等によるデータの滅失等を回避するため，遠隔地での分散保管を実施。<br>(3)紙媒体<br>・施錠できる保管庫等で管理する。<br><br>＜ガバメントクラウドにおける措置＞<br>①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており，システムのサーバー等は，クラウド事業者が保有・管理する環境に構築し，その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。<br>②事前に許可されていない装置等に関しては，外部に持出できないこととしている。 | 事前 | ガバメントクラウドへ移行のため |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 令和6年10月1日 | Ⅲリスク対策（プロセス）（4）7．特定個人情報の保管・消去⑥技術的対策－具体的な対策 | (1)不正プログラム対策<br>・コンピュータウイルス監視ソフトを使用し，サーバ・端末双方でウイルスチェックを実施する。また，新種の不正プログラムに対応するために，ウイルスパターンファイルは定期的に更新し，可能な限り最新のものを使用する。<br>・送付先情報の管理について定めた規程に基づき，コンピュータウイルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。また，同規程に基づき，オペレーション管理に係る手順等を整備し，当該手順に従って，情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的（コンピュータウィルス関連情報は毎日，その他の情報は少なくとも半年に一度）に入手し，機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。<br>(2)不正アクセス対策<br>・送付先情報の管理について定めた規程に基づき，ネットワーク管理に係る手順等を整備し，ファイアウォールを導入する。 | (1)不正プログラム対策<br>・コンピュータウイルス監視ソフトを使用し，サーバ・端末双方でウイルスチェックを実施する。また，新種の不正プログラムに対応するために，ウイルスパターンファイルは定期的に更新し，可能な限り最新のものを使用する。<br>・送付先情報の管理について定めた規程に基づき，コンピュータウイルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。また，同規程に基づき，オペレーション管理に係る手順等を整備し，当該手順に従って，情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的（コンピュータウィルス関連情報は毎日，その他の情報は少なくとも半年に一度）に入手し，機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。<br>(2)不正アクセス対策<br>・送付先情報の管理について定めた規程に基づき，ネットワーク管理に係る手順等を整備し，ファイアウォールを導入する。<br><br>＜ガバメントクラウドにおける措置＞<br>①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。<br>②地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和4年10月 デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は，ガバメントクラウドが提供するマネージドサービスにより，ネットワークアクティビティ，データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに，ロ | 事前 | ガバメントクラウドへ移行のため |
| 令和6年10月1日 | Ⅲリスク対策（プロセス）（4）7．特定個人情報の保管・消去リスク3消去手順－手順の内容 | システム上，消除者の特定個人情報を削除する仕組みとなっている。 | システム上，消除者の特定個人情報を削除する仕組みとなっている。<br><br>＜ガバメントクラウドにおける措置＞<br>データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001 等に準拠したプロセスにしたがって確実にデータを消去する。 | 事前 | ガバメントクラウドへ移行のため |
| 令和6年10月1日 | Ⅳその他のリスク対策1．監査②監査-具体的な内容 | ＜高知市における措置＞<br>監査方式：内部監査<br>監査責任者：情報政策課長<br>監査実施体制：情報政策課特定個人情報保護評価担当者（数名）<br>監査の頻度：年１回<br>監査手法：監査事項に対する書面回答及び現地監査<br>※現地監査は，情報政策課が決定した部署のみ（毎年数部署を抽出して実施）<br>監査事項：評価書記載事項及び各部署で策定している情報セキュリティ実施手順の記載事項に対する運用状況<br>監査結果の活用：結果に基づき運用改善を実施<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・運用規則等に基づき，中間サーバ・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。 | ＜高知市における措置＞<br>監査方式：内部監査<br>監査責任者：情報政策課長<br>監査実施体制：情報政策課特定個人情報保護評価担当者（数名）<br>監査の頻度：年１回<br>監査手法：監査事項に対する書面回答及び現地監査<br>※現地監査は，情報政策課が決定した部署のみ（毎年数部署を抽出して実施）<br>監査事項：評価書記載事項及び各部署で策定している情報セキュリティ実施手順の記載事項に対する運用状況<br>監査結果の活用：結果に基づき運用改善を実施<br><br>＜中間サーバ・プラットフォームにおける措置＞<br>・運用規則等に基づき，中間サーバ・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。<br><br>＜ガバメントクラウドにおける措置＞<br>ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、ISMAP において，クラウドサービス事業者は定期的にISMAP 監査機関リストに登録された監査機関による監査を行うこととしている。 | 事前 | ガバメントクラウドへ移行のため |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
| --- | --- | --- | --- | --- | --- |
| 令和6年10月1日 | | ＜中間サーバ・プラットフォームにおける措置＞<br>・中間サーバ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。 | ＜中間サーバ・プラットフォームにおける措置＞<br>・中間サーバ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。<br><br>＜ガバメントクラウドにおける措置＞<br>ガバメントクラウド上での業務データの取扱いについては，当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP 又はガバメントクラウド運用管理補助者が責任を有する。<br>ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については，原則としてガバメントクラウドに起因する事象の場合は，国はクラウド事業者と契約する立場から，その契約を履行させることで対応する。また，ガバメントクラウドに起因しない事象の場合は，地方公共団体に業務アプリケーションサービスを提供するASP 又はガバメントクラウド運用管理補助者が対応するものとする。<br>具体的な取り扱いについて、疑義が生じる場合は，地方公共団体とデジタル庁及び関係者で協議を行う。 | 事前 | ガバメントクラウドへ移行のため |