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	調布市　住民基本台帳事務　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

調布市は住民基本台帳の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

調布市長

個人情報保護委員会　承認日 【行政機関等のみ】

公表日

令和8年3月13日

［令和7年5月　様式4］

項目一覧

Ⅰ　基本情報
（別添1）事務の内容
Ⅱ　特定個人情報ファイルの概要
（別添2）特定個人情報ファイル記録項目
Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策
Ⅳ　その他のリスク対策
Ⅴ　開示請求、問合せ
Ⅵ　評価実施手続
（別添3）　変更箇所

Ⅰ　基本情報

1. 特定個人情報ファイルを取り扱う事務

①事務の名称	住民基本台帳に関する事務
②事務の内容　※	市区町村が住民を対象とする行政を適切に行い，また，住民の正しい権利を保障するためには，市区町村の住民に関する正確な記録が整備されていなければならない。 住民基本台帳は，住民基本台帳法（以下「住基法」という。）に基づき，作成されるものであり，市区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，市区町村において，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。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である住民基本台帳ネットワークシステム（以下「住基ネット」という。）を都道府県と共同して構築している。 市区町村は，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（以下「番号法」という。）の規定に従い，特定個人情報を以下の事務で取り扱う。（別添1を参照） ①個人を単位とする住民票を世帯ごとに編成し，住民基本台帳を作成 ②転入届，転居届，転出届，世帯変更届等の届出又は職権に基づく住民票の記載，消除又は記載の修正 ③住民基本台帳の正確な記録を確保するための措置 ④転入届に基づき住民票の記載をした際の転出元市区町村に対する通知 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 ⑥住民票の記載事項に変更があった際の都道府県知事に対する通知 ⑦地方公共団体情報システム機構（以下「機構」という。）への本人確認情報の照会 ⑧住民からの請求に基づく住民票コードの変更 ⑨個人番号の通知及び個人番号カードの交付 ⑩個人番号カード等を用いた本人確認 ⑪窓口や郵送での書類の受入，サービス検索・電子申請機能での受領 なお，⑨の「個人番号の通知及び個人番号カードの交付」に係る事務については，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の規定による個人番号カード並びに情報提供ネットワークシステムによる特定個人情報の提供等に関する命令（平成26年11月20日総務省令第85号）（以下「個人番号カード省令」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。 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＞ 1) 1,000人未満　2) 1,000人以上1万人未満 3) 1万人以上10万人未満　4) 10万人以上30万人未満 5) 30万人以上

2. 特定個人情報ファイルを取り扱う事務において使用するシステム

システム1

①システムの名称	既存住民基本台帳システム（以下「既存住基システム」という。）
②システムの機能	①住民基本台帳管理機能　：　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機能 ②通知機能：　住民票コード通知書の発行機能 ③証明書発行機能　：　住民票の写し，記載事項証明書などの各種証明書の発行機能 ④住基ネット連携機能　：　住基ネットへの本人確認情報の連携機能，転出証明書情報などの市町村間の通知機能，個人番号の要求機能，個人番号通知書の送付先連携機能 ⑤庁内連携機能　：　庁内の各システムで，住登者を基礎データとして利用するための，共通宛名システムや他システムへの連携機能 ⑥庁外連携機能：　住基ネットや法務省との庁外とのデータ連携を行い，各種通知情報の収受を行う機能
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 [○]住民基本台帳ネットワークシステム　[　]既存住民基本台帳システム [○]宛名システム等　[　]税務システム [　]その他　（　）

システム2～5

システム2

①システムの名称	住基GWシステム
②システムの機能	①住基ネット連携機能　：　住基ネットへの本人確認情報の連携機能，転入通知・戸籍附票通知・転出証明書情報等の市区町村間の通知機能 ②在留カード等発行システム連携機能　：　在留カード等発行システムと連携し，法務省通知情報の取込，市町村通知情報の作成を行う機能 ③文字同定機能　：　住基ネットと既存住基システムとの文字同定や在留カード等発行システムとのデータ連携時の文字コード変換機能 ④送付先情報連携機能　：　送付先情報を地方公共団体情報システム機構へ連携させる機能

③他のシステムとの接続	[　] 情報提供ネットワークシステム　[○] 庁内連携システム [○] 住民基本台帳ネットワークシステム　[○] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [　] その他　（　）
システム3	
①システムの名称	証明書発行システム
②システムの機能	①証明書発行機能住民票の写し，印鑑登録証明書，税証明書などの各種証明書の発行をダウンリカバリ・コンビニ交付機（ダウンリカバリ・コンビニ交付機については住民票の写し，印鑑登録証明書のみ対応）から行う。 ②業務間データ連携機能（住民記録，税）データ連携機能を利用し，業務間のデータ連携を証明書発行システムを経由して行う。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[○] 既存住民基本台帳システム [○] 宛名システム等　[○] 税務システム [　] その他　（　）
システム4	
①システムの名称	住民基本台帳ネットワークシステム（以下｛住基ネットCS｝）
②システムの機能	①本人確認情報の更新　：　既存住基システムにおいて住民票の記載事項の変更又は新規作成が発生した場合に，当該情報を元に住基ネットCSの本人確認情報を更新し，都道府県サーバへ更新情報を送信する。 ②本人確認　：　特例転入処理や住民票の写しの広域交付などを行う際，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。 ③個人番号カードを利用した転入（特例転入）　：　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。）。 ④本人確認情報検索　：　統合端末において入力された4情報（氏名，住所，性別，生年月日）の組合せをキーに本人確認情報の検索を行い，検索条件に該当する本人確認情報の一覧を画面上に表示する。 ⑤機構への情報照会　：　全国サーバに対して住民票コード，個人番号又は4情報の組合せをキーとした本人確認情報照会要求を行い，該当する個人の本人確認情報を受領する。 ⑥本人確認情報整合　：　本人確認情報ファイルの内容が都道府県知事が都道府県サーバにおいて保有している都道府県知事保存本人確認情報ファイル及び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。 ⑦送付先情報通知　：　個人番号の通知に係る事務の委任先である機構において，住民に対して番号通知書類(通知書，個人番号カード交付申請書（以下「交付申請書」という。）等)を送付するため，既存住基システムから当該市町村の住民基本台帳に記載されている者の送付先情報を抽出し，当該情報を，機構が設置・管理する個人番号カード管理システムに通知する。 ⑧個人番号カード管理システムとの情報連携　：　機構が設置・管理する個人番号カード管理システムに対し，個人番号カードの交付，廃止，回収又は一時停止解除に係る情報や個人番号カードの返還情報等を連携する。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[○] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [　] その他　（　）
システム5	
①システムの名称	番号連携サーバー（団体内統合宛名システム）
②システムの機能	①宛名管理機能　：　既存業務システムから住登者データ，住登外データを受領し，番号連携サーバ内の統合宛名DBに反映を行う。 ②統合宛名番号の付番機能　：　個人番号が新規入力されたタイミングで，統合宛名番号の付番を行う。 ③符号要求機能　：　個人番号を特定済みの統合宛名番号を中間サーバーに登録し，中間サーバーに情報提供用個人識別符号の取得要求・取得依頼を行う。中間サーバーから返却された処理通番は住基GWシステムへ送信する。 ④情報提供機能　：　各業務で管理している番号法第19条別表の提供業務情報を受領し，中間サーバーへの情報提供を行う。 ⑤情報照会機能　：　中間サーバーへ他団体への情報照会を要求し，返却された照会結果を画面表示または，各業務システムにファイル転送を行う。

③他のシステムとの接続	[　] 情報提供ネットワークシステム　[○] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[○] 既存住民基本台帳システム [○] 宛名システム等　[○] 税務システム [○] その他　（ 中間サーバー　）
システム6～10	
システム6	
①システムの名称	中間サーバー
②システムの機能	①符号管理機能 ： 情報照会，情報提供に用いる個人の識別子である「符号」と，情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」とをひもづけ，その情報を保管・管理する機能。 ②情報照会機能 ： 情報提供ネットワークシステムを介して，特定個人情報（連携対象）の情報照会および情報提供受領（照会した情報の受領）を行う機能。 ③情報提供機能 ： 情報提供ネットワークシステムを介して，情報照会要求の受領および当該特定個人情報（連携対象）の提供を行う機能。 ④既存システム接続機能 ： 中間サーバーと既存システム，番号連携サーバー（団体内統合宛名システム）及び既存住基システムとの間で情報照会内容，情報提供内容，特定個人情報（連携対象），符号取得のための情報等について連携するための機能。 ⑤情報提供等記録管理機能 ： 特定個人情報（連携対象）の照会，または提供があった旨の情報提供等記録を生成し，管理する機能。 ⑥情報提供データベース管理機能 ： 特定個人情報（連携対象）を副本として，保持・管理する機能。 ⑦データ送受信機能 ： 中間サーバーと情報提供ネットワークシステム（インターフェイスシステム）との間で情報照会，情報提供，符号取得のための情報等について連携するための機能。 ⑧セキュリティ管理機能 ： セキュリティを管理するための機能。 ⑨職員認証・権限管理機能 ： 中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報（連携対象）へのアクセス制御を行う機能。 ⑩システム管理機能 ： バッチの状況管理，業務統計情報の集計，稼動状態の通知，保管期限切れ情報の削除を行う機能。
③他のシステムとの接続	[○] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [○] その他　（ 番号連携サーバー（団体内統合宛名システム）　）
システム7	
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	【住民向け機能】自らが受けることができるサービスをオンラインで検索及び申請ができる機能 【地方公共団体向け機能】住民が電子申請を行った際の申請データ取得画面又は機能を，地方公共団体に公開する機能
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [○] その他　（ 番号連携サーバー（団体内統合宛名システム　）
システム11～15	
システム16～20	
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	

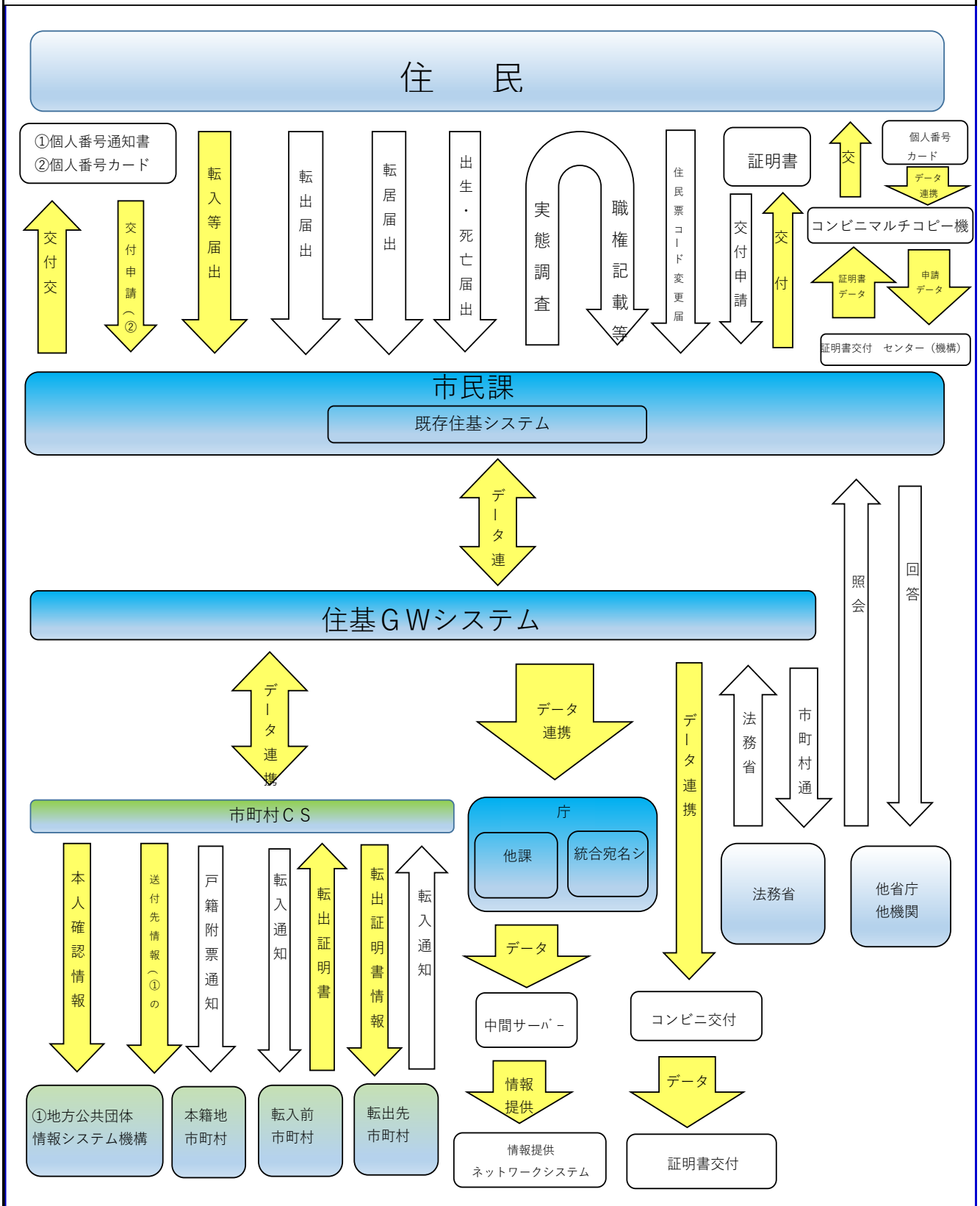
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	(1)住民基本台帳ファイル ・住民基本台帳への記載項目であるため。 ・個人番号の指定及び通知書の事務に必要であるため。 ・個人番号カードの事務に必要であるため。 (2)本人確認情報ファイル 本人確認情報ファイルは、転出入があった場合等にスムーズな住民情報の処理を行うため、また全国的な本人確認手段として、1つの市町村内にとどまらず、全地方公共団体で、本人確認情報を正確かつ統 一的に記録・管理することを目的として、以下の用途に用いられる。 ①住基ネットを用いて市町村の区域を越えた住民基本台帳に関する事務の処理を行うため、区域内の住民に係る最新の本人確認情報を管理する。 ②都道府県に対し、本人確認情報の更新情報を通知する。 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。 ④個人番号カードを利用した転入手続きを行う。 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。 ⑥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との整合性を確認する。 (3)送付先情報ファイル 市町村長が個人番号を指定した際は通知書の形式にて全付番対象者に個人番号を通知するものとされている(行政手続における特定の個人を識別するための番号の利用等に関する法律(平成25年法律第27号。以下「番号法」。(番号法第7条第1項))。通知書による番号の通知及び個人番号カード交付申請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)により機構に対する事務の一部の委任が認められている。)
②実現が期待されるメリット	住民票の写し等にかえて，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出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。 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。
5. 個人番号の利用 ※	
法令上の根拠	1. 行政手続における特定の個人を識別するための番号の利用等に関する法律(番号法)(平成25年5月31日法律第27号) ・第7条(指定及び通知) ・第16条(本人確認の措置) ・第17条(個人番号カードの交付等) 2. 住民基本台帳法(住基法)(昭和42年7月25日法律第81号)(平成25年5月31日法律第28号施行時点) ・第5条(住民基本台帳の備付け) ・第6条(住民基本台帳の作成) ・第7条(住民票の記載事項) ・第8条(住民票の記載等) ・第12条(本人等の請求に係る住民票の写し等の交付) ・第12条の4(本人等の請求に係る住民票の写しの交付の特例) ・第14条(住民基本台帳の正確な記録を確保するための措置) ・第22条(転入届) ・第24条の2(個人番号カードの交付を受けている者等に関する転入届の特例) ・第30条の6(市町村長から都道府県知事への本人確認情報の通知等) ・第30条の10(通知都道府県の区域内の市町村の執行機関への本人確認情報の提供) ・第30条の12(通知都道府県以外の都道府県の区域内の市町村の執行機関への本人確認情報の提供)
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[　　実施する　　] ＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	・番号法第19条第8号(特定個人情報の提供の制限)及び同号に基づく主務省令第2条の表 (番号法第19条第8号に基づく主務省令第2条の表における情報提供の根拠) ： 第三欄(情報提供者)が「市町村長」の項のうち，第四欄(利用特定個人情報)に「住民票関係情報」が含まれる項 (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) (番号法第19条第8号に基づく主務省令第2条の表における情報照会の根拠) ： なし (住民基本台帳に関する事務において情報提供ネットワークシステムによる情報照会は行わない)
7. 評価実施機関における担当部署	
①部署	市民部市民課 市民部神代出張所

②所属長の役職名	市民課長 神代出張所長

8. 他の評価実施機関

（別添1）事務の内容

「（2）本人確認情報ファイル」及び「（3）送付先情報ファイル」を取り扱う事務の内容（市町村CSを中心とした事務の流れ）



特定個人情報の流れ

それ以外の情報の流れ

（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.市町村の住民基本台帳（既存住基システム）を更新する。
1-③.市町村の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当該都道府県の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。
3-⑤.市町村CSより，既存住基システムから転入処理完了後に受け渡される転入通知情報(※特定個人情報を含まない)を転出地市町村へ送信すると同時に，都道府県サーバへ本人確認情報の更新情報を送信する。
3-⑥.転入処理完了後，個人番号カードの継続利用処理を行い，個人番号カード管理システムに対し，個人番号カード管理情報の更新要求を行う。

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。
※検索対象者が自都道府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.既存住基システムより，当該市町村における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＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※		住民基本台帳に登録されている者のうち，個人番号を有する者（平成27年10月の番号法施行日時点で住民である者，それ以後の届出・通知により住民となった者）
	その必要性	住民に関する市町村事務の処理の基礎として利用する ・住基法第7条において，住民基本台帳の記載項目と規定されるため ・番号法第19条別表の事務において，符号の取得に利用するため
④記録される項目		[　50項目以上100項目未満　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目 ※	・識別情報 [○] 個人番号　[　] 個人番号対応符号　[○] その他識別情報（内部番号） ・連絡先等情報 [○] 5情報（氏名、氏名の振り仮名、性別、生年月日、住所）　[　] 連絡先（電話番号等） [○] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[　] 地方税関係情報　[　] 健康・医療関係情報 [○] 医療保険関係情報　[○] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[○] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[○] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [　] その他　（　）
	その妥当性	住民基本台帳を整備するため，住民基本台帳法の記載事項を保有
	全ての記録項目	別添2を参照。
⑤保有開始日		平成27年6月
⑥事務担当部署		市民部市民課 市民部神代出張所

3. 特定個人情報の入手・使用

①入手元 ※	[○] 本人又は本人の代理人 [　] 評価実施機関内の他部署　（　） [　] 行政機関・独立行政法人等　（　） [○] 地方公共団体・地方独立行政法人　（ 他市町村　） [　] 民間事業者　（　） [○] その他　（ 地方公共団体情報システム機構　）

②入手方法		[○] 紙　[　] 電子記録媒体(フラッシュメモリを除く。)　[　] フラッシュメモリ [　] 電子メール　[　] 専用線　[○] 庁内連携システム [　] 情報提供ネットワークシステム [○] その他　(住民基本台帳ネットワーク，サービス検索・電子申請機能　)
③入手の時期・頻度		転入，出生等，住民基本台帳に初めて記載する際に入手する。
④入手に係る妥当性		住民基本台帳の記載事項であり，届出等に必要であるため。
⑤本人への明示		住民基本台帳法第7条(住民票の記載事項)において明示されている。
⑥使用目的 ※		住民基本台帳の整備
	変更の妥当性	—
⑦使用の主体	使用部署 ※	市民部市民課 市民部神代出張所
	使用者数	[　50人以上100人未満　] ＜選択肢＞ 1) 10人未満　2) 10人以上50人未満 3) 50人以上100人未満　4) 100人以上500人未満 5) 500人以上1,000人未満　6) 1,000人以上
⑧使用方法 ※		1. 住民基本台帳への個人番号の記載及び住民票の写しなどの証明書への個人番号の記載 2. 本人への個人番号の通知(個人番号通知書を発行する機構への情報連携) 3. 再転入時などの同一人であることの識別キーとしての利用 4. 番号法第9条に基づく個人番号の利用のため
	情報の突合 ※	窓口業務において本人確認書類に個人番号カードが使われた際に個人番号で単件検索を行う
	情報の統計分析 ※	個人に着目した分析・統計は行わず，住民基本台帳の更新件数の集計等，事務処理実績の確認のための統計のみ行う。
	権利利益に影響を与え得る決定 ※	該当なし
⑨使用開始日		平成27年6月1日
4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[　委託する　] ＜選択肢＞ 1) 委託する　2) 委託しない (　2　) 件
委託事項1		既存住基システム，住基GWシステム，住基ネットCS，GW証明発行システム(以下「住民基本台帳システム等」という。)の保守・運用
①委託内容		既存住基システム等のパッケージアプリケーション保守作業，ジョブスケジューリングや帳票印刷等のシステム運用作業，職員からの問い合わせに対する調査，作業指示に基づくデータ抽出等
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] ＜選択肢＞ 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	「2. ③対象となる本人の範囲」と同上。

	その妥当性	システムの安定した稼動のため，システムに専門的な知識を有する民間事業者に委託している。ただし，通常業務では特定個人情報ファイルを取り扱わない。
③委託先における取扱者数		[10人未満] <選択肢> 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ]専用線 [ ]電子メール [ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ [ ]紙 [○]その他 （ 原則，特定個人情報ファイルの提供は行わず，障害等の緊急時及びシステムの運用・保守を行ううえで必要不可欠な場合で，担当課が許可した場合にのみ，管理端末にてシステムの直接操作を認めている。 ）
⑤委託先名の確認方法		委託先を決定した際に調布市ホームページに公表している（公表期限には上限あり）
⑥委託先名		富士通株式会社
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
再委託	⑧再委託の許諾方法	再委託の必要がある場合には，事前に委託先から，再委託承諾願（会社名，担当者名，委託の範囲等を記載した書面）を提出させ，再委託の必要性や業務内容等を確認したうえで承認する。
再委託	⑨再委託事項	住民基本台帳システム等のパッケージアプリケーション保守作業，ジョブスケジューリング等のシステム運用作業，職員からの問い合わせに対する調査，作業指示に基づくデータ抽出等。
委託事項2～5		
委託事項2		住民基本台帳システム等への入力事務
①委託内容		届出や通知に基づく住民基本台帳システム等への住民情報の入力，証明書の発行
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[10万人以上100万人未満] <選択肢> 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	「2．③対象となる本人の範囲」と同上。
	その妥当性	住民票の写し等の受付・作成業務を行うためには，保有する住民基本台帳ファイルを取扱う必要がある。
③委託先における取扱者数		[50人以上100人未満] <選択肢> 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ]専用線 [ ]電子メール [ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ [ ]紙 [○]その他 （ 市民部市民課内端末の直接操作 ）
⑤委託先名の確認方法		委託先を決定した際に調布市ホームページに公表している（公表期限には上限あり）
⑥委託先名		株式会社エイジェック
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
再委託	⑧再委託の許諾方法	

⑨再委託事項	
委託事項6～10	
委託事項11～15	
委託事項16～20	
5. 特定個人情報の提供・移転（委託に伴うものを除く。）	
提供・移転の有無	[○] 提供を行っている （ 55 ）件 [○] 移転を行っている （ 32 ）件 [ ] 行っていない
提供先1	（別紙1）提供先一覧に記載
①法令上の根拠	（別紙1）提供先一覧に記載
②提供先における用途	（別紙1）提供先一覧に記載
③提供する情報	住民基本台帳法第7条第4号に規定する事項（世帯主についてはその旨，世帯主でない者については世帯主の氏名及び世帯主との続柄）
④提供する情報の対象となる本人の数	[10万人以上100万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	情報提供ネットワークシステムを通じて特定個人情報の提供照会を受けた都度
⑥提供方法	[○] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑦時期・頻度	情報提供ネットワークシステムを通じて特定個人情報の提供照会を受けた都度
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	（別紙2）移転先一覧に記載
①法令上の根拠	（別紙2）移転先一覧に記載
②移転先における用途	（別紙2）移転先一覧に記載
③移転する情報	住民票関係情報
④移転する情報の対象となる本人の数	[10万人以上100万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲	住民基本台帳への記載者
⑥移転方法	[○] 庁内連携システム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [○] 紙 [ ] その他 （ ）

⑦時期・頻度		随時
移転先2～5		
移転先6～10		
移転先11～15		
移転先16～20		
6. 特定個人情報の保管・消去		
①保管場所 ※		・入退館管理をしている建物内のうち，個人に貸与された入室カードによる入退室管理を行っている部屋に設置したサーバ内に保管。サーバへのアクセスはID及びパスワードによる認証が必要。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームは政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し，設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお，クラウドサービス事業者は，セキュリティ管理策が適切に実施されているほか，次を満たしている。 ・ISO/IEC27017，ISO/IEC27018の認証を受けている。 ・日本国内でデータを保管している。 ②特定個人情報は，クラウドサービス事業者が保有・管理する環境に構築する中間サーバーのデータベース内に保存され，バックアップもデータベース上に保存される。
②保管期間	期間	［　定められていない　］ ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	・住民基本台帳に記載されている限り保管する必要がある。
③消去方法		特定個人情報が記載された届書，申請書等は，規定の保存期間が経過した後，溶解処理している。 ＜中間サーバー・プラットフォームにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施されるため，通常，中間サーバー・プラットフォームの保守・運用を行う事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②クラウドサービス事業者が保有・管理する環境において，障害やメンテナンス等によりディスクやハード等を交換する際は，クラウドサービス事業者において，政府情報システムのためのセキュリティ評価制度（ISMAP）に準拠したデータの暗号化消去及び物理的破壊を行う。さらに，第三者の監査機関が定期的に発行するレポートにより，クラウドサービス事業者において，確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ③中間サーバー・プラットフォームの移行に際は，地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において，保存された情報が読み出しできないよう，データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。
7. 備考		

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名		
(2)本人確認情報ファイル		
2. 基本情報		
①ファイルの種類 ※		[　　システム用ファイル　　] ＜選択肢＞ 1) システム用ファイル 2) その他の電子ファイル(表計算ファイル等)
②対象となる本人の数		[　10万人以上100万人未満　] ＜選択肢＞ 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
③対象となる本人の範囲 ※		区域内の住民(住基法第5条(住民基本台帳の備付け)に基づき住民基本台帳に記録された住民を指す) ※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	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		[　10項目以上50項目未満　] ＜選択肢＞ 1) 10項目未満　2) 10項目以上50項目未満 3) 50項目以上100項目未満　4) 100項目以上
	主な記録項目 ※	・識別情報 [○] 個人番号　[　] 個人番号対応符号　[○] その他識別情報(内部番号) ・連絡先等情報 [○] 5情報(氏名、氏名の振り仮名、性別、生年月日、住所)　[　] 連絡先(電話番号等) [○] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[　] 地方税関係情報　[　] 健康・医療関係情報 [　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [　] その他　(　　)
	その妥当性	・個人番号，4情報，その他住民票関係情報　：　住基ネットを通じて本人確認を行うために必要な情報として，住民票の記載等に係る本人確認情報(個人番号，4情報，住民票コード及びこれらの変更情報)を記録する必要があるため。
	全ての記録項目	別添2を参照。
⑤保有開始日		平成27年10月
⑥事務担当部署		市民部市民課 市民部神代出張所

3. 特定個人情報の入手・使用		
①入手元 ※		[　] 本人又は本人の代理人 [　] 評価実施機関内の他部署　（　） [　] 行政機関・独立行政法人等　（　） [　] 地方公共団体・地方独立行政法人　（　） [　] 民間事業者　（　） [○] その他　（ 自部署　）
②入手方法		[　] 紙　[　] 電子記録媒体（フラッシュメモリを除く。）　[　] フラッシュメモリ [　] 電子メール　[　] 専用線　[○] 庁内連携システム [　] 情報提供ネットワークシステム [○] その他　（ 既存住基システム，サービス検索・電子申請機能　）
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，まず既存住基システムで情報を管理した上で，全国的なシステムである住基ネットに格納する必要があるため。
⑤本人への明示		市町村CSが既存住基システムより本人確認情報を入手することについて，住基法第30条の6（市町村長から都道府県知事への本人確認情報の通知等）及び平成14年6月10日総務省告示第334号（第6－7（市町村長から都道府県知事への通知及び記録）に記載されている。
⑥使用目的 ※		住基ネットを通じて全国共通の本人確認を行うため，本特定個人情報ファイル（本人確認情報ファイル）において区域内の全ての住民の情報を保有し，住民票に記載されている住民全員の記録を常に正確に更新・管理・提供する。
	変更の妥当性	—
⑦使用の主体	使用部署 ※	市民部市民課 市民部神代出張所
	使用者数	[　50人以上100人未満　] ＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
⑧使用方法 ※		・住民票の記載事項の変更又は新規作成が生じた場合，既存住基システムから当該本人確認情報の更新情報を受領し(既存住基システム→住基ネット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（住基ネットCS→都道府県サーバ)。 ・住民から提示された個人番号カードに登録された住民票コードをキーとして本人確認情報ファイルを検索し，画面に表示された本人確認情報と申請・届出書等の記載内容を照合し確認することで本人確認を行う（個人番号カード→住基ネットCS）。 ・4情報（氏名，住所，性別，生年月日）の組合せをキーに本人確認情報ファイルの検索を行う。 ・本人確認情報ファイルの内容が都道府県知事保存本人確認情報ファイル（都道府県サーバ）及び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（住基ネット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。 ・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を行う。

	権利利益に影響を与え得る決定 ※	該当なし。
⑨使用開始日		平成27年10月1日
4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] ＜選択肢＞ 1）委託する 2）委託しない （ 2 ） 件
委託事項1		住基ネットCSの保守・運用
①委託内容		住基ネットCSのアプリケーション保守作業，ジョブスケジューリングや帳票印刷等のシステム運用作業，職員からの問い合わせに対する調査等
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] ＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[10万人以上100万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	「2. ③対象となる本人の範囲」と同上。
	その妥当性	運用支援業務は，システム上保有する全てのファイルを取扱うため。
③委託先における取扱者数		[10人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ]専用線 [ ]電子メール [ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ [ ]紙 [○]その他 （ 原則，特定個人情報ファイルの提供は行わず，障害等の緊急時及びシステムの運用・保守を行ううえで必要不可欠な場合で，担当課が許可した場合にのみ，管理端末にてシステムの直接操作を認めている。 ）
⑤委託先名の確認方法		委託先を決定した際に調布市ホームページに公表している（公表期限には上限あり）
⑥委託先名		富士通株式会社
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	再委託の必要がある場合には，事前に委託先から，再委託承諾願（会社名，担当者名，委託の範囲等を記載した書面）を提出させ，再委託の必要性や業務内容等を確認したうえで承認する。
	⑨再委託事項	住基ネットCSのアプリケーション保守作業，ジョブスケジューリング等のシステム運用作業，職員からの問い合わせに対する調査等。
委託事項2～5		
委託事項6～10		
委託事項11～15		
委託事項16～20		

5. 特定個人情報の提供・移転（委託に伴うものを除く。）	
提供・移転の有無	[○] 提供を行っている （ 2 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	都道府県
①法令上の根拠	住基法第30条の6（市町村長から都道府県知事への本人確認情報の通知等）
②提供先における用途	・市区町村より受領した住民の本人確認情報の変更情報（当該提供情報）を元に都道府県知事保存本人確認情報ファイルの当該住民に係る情報を更新し，機構に通知する。 ・都道府県の執行機関に対し本人確認情報を提供する。
③提供する情報	住民票コード，氏名，生年月日，性別，住所，個人番号，異動事由，異動年月日
④提供する情報の対象となる本人の数	[10万人以上100万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上。
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [○] その他 （ 住民基本台帳ネットワークシステム ）
⑦時期・頻度	住民基本台帳の記載事項において，本人確認情報に係る変更又は新規作成が発生した都度，随時。
提供先2～5	
提供先2	都道府県及び地方公共団体情報システム機構（以下「機構」という。）
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] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上。
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [○] その他 （ 住民基本台帳ネットワークシステム ）
⑦時期・頻度	必要に応じて随時（1年に1回程度）。
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	
①法令上の根拠	

②移転先における用途		
③移転する情報		
④移転する情報の対象となる本人の数	[ ]	＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲		
⑥移転方法	[ ] 庁内連携システム [ ] 電子メール [ ] フラッシュメモリ [ ] その他 （ ）	[ ] 専用線 [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] 紙
⑦時期・頻度		
移転先2～5		
移転先6～10		
移転先11～15		
移転先16～20		
6．特定個人情報の保管・消去		
①保管場所 ※		・施錠管理・入退室管理を行っている部屋内に設置した，さらに施錠管理されたラックに設置したサーバ内に保管。
②保管期間	期間	[20年以上] ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	住基ネットCSのアプリケーション保守作業，ジョブスケジューリング等のシステム運用作業，職員からの問い合わせに対する調査等・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。 ・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第34条第2項（保存）に定める期間（150年間）保管する。
③消去方法		所属長の決裁手続を経たうえで，システム操作により消去する。
7．備考		

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名	
（3）送付先情報ファイル	
2. 基本情報	
①ファイルの種類 ※	［　　システム用ファイル　　］　＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数	［　10万人以上100万人未満　］　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※	区域内の住民（住基法第5条（住民基本台帳の備付け）に基づき住民基本台帳に記録された住民を指す）
その必要性	番号法第7条第1項（指定及び通知）に基づき，個人番号通知書を個人番号の付番対象者全員に送付する必要がある。 市区町村は，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
④記録される項目	［　50項目以上100項目未満　］　＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
主な記録項目 ※	・識別情報 ［ ○ ］個人番号　［　］個人番号対応符号　［　］その他識別情報（内部番号） ・連絡先等情報 ［ ○ ］5情報（氏名、氏名の振り仮名、性別、生年月日、住所）　［　］連絡先（電話番号等） ［ ○ ］その他住民票関係情報 ・業務関係情報 ［　］国税関係情報　［　］地方税関係情報　［　］健康・医療関係情報 ［　］医療保険関係情報　［　］児童福祉・子育て関係情報　［　］障害者福祉関係情報 ［　］生活保護・社会福祉関係情報　［　］介護・高齢者福祉関係情報 ［　］雇用・労働関係情報　［　］年金関係情報　［　］学校・教育関係情報 ［　］災害関係情報 ［ ○ ］その他　（　通知書及び交付申請書の送付先の情報　）
その妥当性	・個人番号，4情報，その他住民票関係情報：個人番号カードの券面記載事項として，法令に規定された項目を記録する必要がある。 ・その他（個人番号通知書及び交付申請書の送付先の情報）：機構に対し，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。
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
⑥事務担当部署	市民部市民課 市民部神代出張所

3. 特定個人情報の入手・使用		
①入手元 ※		[　] 本人又は本人の代理人 [　] 評価実施機関内の他部署　（　） [　] 行政機関・独立行政法人等　（　） [　] 地方公共団体・地方独立行政法人　（　） [　] 民間事業者　（　） [○] その他　（ 自部署　）
②入手方法		[　] 紙　[　] 電子記録媒体（フラッシュメモリを除く。）　[　] フラッシュメモリ [　] 電子メール　[　] 専用線　[　] 庁内連携システム [　] 情報提供ネットワークシステム [○] その他　（ 既存住基システム，サービス検索・電子申請機能　）
③入手の時期・頻度		個人番号通知書にかかる送付先情報は，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		個人番号通知書及び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）
⑥使用目的 ※		法令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	—
⑦使用の主体	使用部署 ※	市民部市民課 市民部神代出張所
	使用者数	[　50人以上100人未満　] ＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
⑧使用方法 ※		・既存住基システムより個人番号の通知対象者の情報を抽出し，通知書及び交付申請書等の印刷及び送付に係る事務を通知書及び個人番号カード省令第35条（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（既存住基システム→住基ネットCS又は電子記録媒体→個人番号カード管理システム（機構））。
	情報の突合 ※	入手した送付先情報に含まれる4情報等の変更の有無を確認する（最新の4情報等であることを確認する）ため，機構（全国サーバ）が保有する「機構保存本人確認情報」との情報の突合を行う。
	情報の統計分析 ※	送付先情報ファイルに記録される個人情報を用いた統計分析は行わない。
	権利利益に影響を与え得る決定 ※	該当なし。
⑨使用開始日		平成27年10月1日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] <選択肢> 1）委託する 2）委託しない （ 1 ） 件
委託事項1		住基ネットCSの保守・運用
①委託内容		住基ネットCSのアプリケーション保守作業，ジョブスケジューリングや帳票印刷等のシステム運用作業，職員からの問い合わせに対する調査等
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[10万人以上100万人未満] <選択肢> 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	「2. ③対象となる本人の範囲」と同上。
	その妥当性	運用支援業務は，システム上保有する全てのファイルを取扱うため。
③委託先における取扱者数		[10人未満] <選択肢> 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [○] その他 （ 原則，特定個人情報ファイルの提供は行わず，障害等の緊急時及びシステムの運用・保守を行ううえで必要不可欠な場合で，担当課が許可した場合にのみ，管理端末にてシステムの直接操作を認めている。 ）
⑤委託先名の確認方法		委託先を決定した際に調布市ホームページに公表している（公表期限には上限あり）
⑥委託先名		富士通株式会社
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	再委託の必要がある場合には，事前に委託先から，再委託承諾願（会社名，担当者名，委託の範囲等を記載した書面）を提出させ，再委託の必要性や業務内容等を確認したうえで承認する。
	⑨再委託事項	上記委託内容と同様。
委託事項2～5		
委託事項6～10		
委託事項11～15		
委託事項16～20		

5. 特定個人情報の提供・移転（委託に伴うものを除く。）	
提供・移転の有無	[○] 提供を行っている （ 1 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	地方公共団体情報システム機構
①法令上の根拠	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）
②提供先における用途	市区町村からの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。
③提供する情報	「2. ④記録される項目」と同上。
④提供する情報の対象となる本人の数	[10万人以上100万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上。
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [○] その他 （ 住民基本台帳ネットワークシステム ）
⑦時期・頻度	使用開始日から個人番号通知書送付までの一定の期間に，番号法施行日時点における住民の送付先情報をまとめて提供する（以降，新たに個人番号の通知対象者が生じた都度提供する）。
提供先2～5	
提供先2	
①法令上の根拠	
②提供先における用途	
③提供する情報	
④提供する情報の対象となる本人の数	[ ] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上。
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑦時期・頻度	
提供先6～10	
提供先11～15	
提供先16～20	

移転先1		
①法令上の根拠		
②移転先における用途		
③移転する情報		
④移転する情報の対象となる本人の数	[ ]	＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲		
⑥移転方法	[ ] 庁内連携システム [ ] 電子メール [ ] フラッシュメモリ [ ] その他 （ ）	[ ] 専用線 [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] 紙
⑦時期・頻度		
移転先2～5		
移転先6～10		
移転先11～15		
移転先16～20		
6．特定個人情報の保管・消去		
①保管場所 ※		・個人に貸与された入室カードによる入退室管理を行っている部屋に設置したサーバ内に保管。サーバへのアクセスはID及びパスワードによる認証が必要。
②保管期間	期間	[1年未満] ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	送付先情報は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送付先情報は，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。
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
1. 宛名番号，2. 住民票コード，3. 個人番号，4. 世帯番号，5. 氏名情報，6. 生年月日，7. 性別，8. 続柄，9. 住民となった年月日住民となった届出年月日，10. 住民となった事由，11. 住民区分（日本人，外国人），12. 世帯主情報，13. 現住所情報，14. 住所を定めた年月日　住所を定めた届出年月日，15. 前住所情報　転入元住所情報　転出先住所情報，16. 本籍・筆頭者情報，17. 備考欄履歴情報，18. 事実上の世帯主情報，19. 消除情報，20. 外国人住民となった年月日（外国人住民のみ），21. 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），22. 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），23. 個別記載情報，24. 転出予定者情報　除票住民票情報，25. 証明書発行履歴情報　異動履歴情報，26. 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，27. 処理停止情報，28. 印鑑登録情報　印影情報　印鑑登録異動履歴　印鑑証明書発行履歴、29. 旧氏情報

（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

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	＜既存住基システムのソフトウェアにおける措置＞ ・対象者が多数表示される一覧系の画面および帳票には個人番号は表示しない仕組みとし，不用意な閲覧が行われないようにする。 ・他の業務から住民基本台帳ファイルを利用する場合は，個人番号が含まれないファイルのみを提供する。 ＜既存住基システムの運用における措置＞ ・個人番号が含まれるファイルに対し，目的を超えた入手が行われている恐れがないかなどを確認するため，アクセスログを取得し，定期的に点検することを可能とする。 ＜サービス検索・電子申請機能における措置＞ ・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	・転入届の申請書を住民基本台帳法上必要とされる事項のみ記入できる書面様式とし，申請者が必要な情報以外の情報を記載することを防止する。 ・転入届によって住民票を新規に作成する際は，法定添付書類である転出証明書に記載された情報を入力する。 ・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＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	・転入届の受付・入力をマニュアル化し，住民基本台帳法上の各規定に反する取扱いがされないよう対策している。 ・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，後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。 ・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＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報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	・個人番号カードの提示等，番号法，住民基本台帳法等に定められた本人確認を実施する。 ・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	・個人番号カード等の提示を受け，本人確認を行う。 ・出生等により新たに個人番号が指定される場合や，転入の際に個人番号カード（法令により定められた身分証明書の組み合わせ）の提示がない場合には，市町村CSにおいて本人確認情報と個人番号の対応付けの確認を行う。
特定個人情報の正確性確保の措置の内容	・本人確認情報の入力，削除及び訂正を行う際には，整合性を確保するために，入力，削除及び訂正を行った者以外の者が確認する等，必ず入力，削除及び訂正した内容を確認する。 ・入力，削除及び訂正作業に用いた届出書，申請書等は，当市で定める規程に基づいて管理し，保管する。 ・個人番号カード内の記憶領域に格納された個人番号を申請フォームに自動転記を行うことにより，不正確な個人番号の入力を抑止する措置を講じている。
その他の措置の内容	―

リスクへの対策は十分か	[　　十分である　　]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク4：　入手の際に特定個人情報が漏えい・紛失するリスク		
リスクに対する措置の内容	・提出された届出書，申請書等は，処理後速やかに鍵付きの書庫に保管する。 ・住民基本台帳端末のディスプレイは来庁者から見えない位置に置き，のぞき見防止フィルターを使用している。 ・サービス検索・電子申請機能と地方公共団体との間は，専用線であるLGWAN回線を用いた通信を行うことで，外部からの盗聴，漏えい等が起こらないようにしており，さらに通信自体も暗号化している。	
リスクへの対策は十分か	[　　十分である　　]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置		
—		
3．特定個人情報の使用		
リスク1：　目的を超えた紐付け、事務に必要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	・個人番号利用業務以外または個人番号を必要としない業務では，画面表示に個人番号を表示しない。 ・個人番号利用業務以外または個人番号を必要としない業務から情報の要求があった場合は，個人番号が含まれない情報のみを提供するようにアクセス制御を行っている。 ・権限のない者が統合宛名システムに接続することを認めない。	
事務で使用するその他のシステムにおける措置の内容	・他業務からアクセスされる住民情報の基本情報を保持するテーブルと特定個人情報を含むデータベースを切り離して管理する。	
その他の措置の内容	—	
リスクへの対策は十分か	[　　十分である　　]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2：　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	・住民記録システムを使用する必要のある職員を特定し，個人ごとにユーザーIDを割り当てるとともに，IDとパスワードによる認証及び生体認証を行っている。ログインは特定の端末でのみ可能となっている。	
アクセス権限の発効・失効の管理	[　行っている　]	<選択肢> 1）行っている　2）行っていない
具体的な管理方法	①発行管理・職員ごとに業務上必要な権限のみ付与している。 ②失効管理・異動，退職等が生じた都度，権限を更新，削除している。	
アクセス権限の管理	[　行っている　]	<選択肢> 1）行っている　2）行っていない
具体的な管理方法	・権限表を作成し，権限の更新・削除について記録している。	
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	・操作履歴（アクセスログ・操作ログ）を記録する。 ・バックアップされた操作履歴については定められた期間，安全な場所に施錠管理している。 ・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。 ・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> 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	・操作履歴（アクセスログ・操作ログ）を記録する。 ・情報セキュリティについて研修する。 ・サービス検索・電子申請機能へアクセスできる端末を制限する。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
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	・既存住基システム端末から住民基本台帳ファイルの複製はシステム上できない仕組みになっている。 ・委託先における無許可のデータ複製を禁止している。 ・情報セキュリティについて研修を行う。 ・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。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	
その他，特定個人情報の使用にあたり，以下の措置を講じる。 ・スクリーンセーバ等を利用して，長時間にわたり情報を表示させない。 ・一定時間端末が操作されない場合，自動的にログオフする設定とする。	

4. 特定個人情報ファイルの取扱いの委託 [ ] 委託しない

委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認	・委託先の社会的信用（プライバシーマーク，ISMSの取得）と能力を確認する。また，委託業者が選定基準を引き続き満たしていることを適時確認するとともに，その記録を残す。 ・委託先に対し，従業者の教育・啓発の実施を契約において義務付けている。	
特定個人情報ファイルの閲覧者・更新者の制限	[制限している] ＜選択肢＞ 1）制限している 2）制限していない	
具体的な制限方法	・委託先の業務体制を書面にて提出させている。 ・アカウント管理を行い，操作を制限している。	
特定個人情報ファイルの取扱いの記録	[記録を残している] ＜選択肢＞ 1）記録を残している 2）記録を残していない	
具体的な方法	・アクセスログを保存している	
特定個人情報の提供ルール	[定めている] ＜選択肢＞ 1）定めている 2）定めていない	
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	・委託先から他者への個人情報の提供を禁止している。 ・委託元は，事前に通知することなく個人情報の取扱状況について報告を求めることができる。	
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・データの授受に際して記録を残すこととしている。 ・委託先が特定個人情報を目的外に使用することは契約上禁止している。 ・委託元は，事前に通知することなく個人情報の取扱状況について報告を求めることができる。	
特定個人情報の消去ルール	[定めている] ＜選択肢＞ 1）定めている 2）定めていない	
ルールの内容及びルール遵守の確認方法	・個人情報を保管する必要がなくなったときには，速やかに委託元に返却又は復元が不可能な方法により消去しなければならない。 ・委託元は，事前に通知することなく個人情報の取扱状況について報告を求めることができる。	
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＞ 1）定めている 2）定めていない	
規定の内容	・個人情報の複写，複製の禁止 ・秘密保持 ・目的外使用，第三者提供の禁止 ・再委託の禁止（再委託をする場合は，委託元の書面による事前の同意が必要） ・事故等の報告・検査監督権	

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> 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない
具体的な方法	・再委託先に対し，委託先と同様の機密保持に関する規定を契約において義務付けている。 ・委託元は，事前に通知することなく個人情報の取扱状況について報告を求めることができる。	
その他の措置の内容	—	
リスクへの対策は十分か	[　十分である　]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
—		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）　[　]提供・移転しない

リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[　記録を残している　]	<選択肢> 1）記録を残している　2）記録を残していない
具体的な方法	・提供・移転についてログを保存する。	
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> 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	・提供先・移転先からのデータ利用申請を求め，利用に関して法的根拠等を判断し，提供・移転を行う。	
その他の措置の内容	—	
リスクへの対策は十分か	[　十分である　]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容	・適切に制御された庁内ネットワークにより提供・移転を行う。	
リスクへの対策は十分か	[　十分である　]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容	・誤った情報を提供・移転してしまうリスクに対する措置　：　住民基本台帳ファイルの入力，削除及び訂正を行う際には，整合性を確保するために，入力，削除及び訂正を行った者以外の者が確認する等，必ず入力，削除及び訂正した内容を確認し，誤った情報が提供・移転されることを防止する。 ・誤った相手に提供・移転してしまうリスクに対する措置　：　誤った相手に提供・移転されないよう，庁内連携システムにおいて制御する。	
リスクへの対策は十分か	[　十分である　]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		
—		

6. 情報提供ネットワークシステムとの接続	[○]接続しない(入手)　[　]接続しない(提供)
リスク1: 目的外の入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[　]　<選択肢> 1) 特に力を入れている　2) 十分である 3) 課題が残されている
リスク2: 安全が保たれない方法によって入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[　]　<選択肢> 1) 特に力を入れている　2) 十分である 3) 課題が残されている
リスク3: 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[　]　<選択肢> 1) 特に力を入れている　2) 十分である 3) 課題が残されている
リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[　]　<選択肢> 1) 特に力を入れている　2) 十分である 3) 課題が残されている
リスク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	＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能(※)により，情報提供ネットワークシステムにおける照会許可用照合リストを情報提供ネットワークシステムから入手し，中間サーバーにも格納して，情報提供機能により，照会許可用照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ②情報提供機能により，情報提供ネットワークシステムに情報提供を行う際には，情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し，照会内容に対応した情報を自動で生成して送付することで，特定個人情報が不正に提供されるリスクに対応している。 ③特に慎重な対応が求められる情報については自動応答を行わないように自動応答不可フラグを設定し，特定個人情報の提供を行う際に，送信内容を改めて確認し，提供を行うことで，センシティブな特定個人情報が不正に提供されるリスクに対応している。④中間サーバーの職員認証・権限管理機能では，ログイン時の職員認証の他に，ログイン・ログアウトを実施した職員，時刻，操作内容の記録が実施されるため，不適切な接続端末の操作や，不適切なオンライン連携を抑止する仕組みになっている。(※)情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。
リスクへの対策は十分か	[　十分である　]　<選択肢> 1) 特に力を入れている　2) 十分である 3) 課題が残されている
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	＜中間サーバー・ソフトウェアにおける措置＞ ①セキュリティ管理機能(※)により，情報提供ネットワークシステムに送信する情報は，情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ②中間サーバーの職員認証・権限管理機能では，ログイン時の職員認証の他に，ログイン・ログアウトを実施した職員，時刻，操作内容の記録が実施されるため，不適切な接続端末の操作や，不適切なオンライン連携を抑止する仕組みになっている。 (※)暗号化・復号機能と，鍵情報及び照会許可用照合リストを管理する機能。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム，情報提供ネットワークシステムとの間は，高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより，不適切な方法で提供されるリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し，団体ごとに通信回線を分離するとともに，通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォームの保守・運用を行う事業者及びクラウドサービス事業者においては，特定個人情報に係る業務にはアクセスができないよう管理を行い，不適切な方法での情報提供を行えないよう管理している。

リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク7：　誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク		
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能により，情報提供ネットワークシステムに情報提供を行う際には，情報提供許可証と情報照会者への経路情報を受領した上で，情報照会内容に対応した情報提供をすることで，誤った相手に特定個人情報が提供されるリスクに対応している。 ②情報提供データベース管理機能（※）により，「情報提供データベースへのインポートデータ」の形式チェックと，接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで，誤った特定個人情報を提供してしまうリスクに対応している。 ③情報提供データベース管理機能では，情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 （※）特定個人情報を副本として保存・管理する機能。	
リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置		
＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーの職員認証・権限管理機能では，ログイン時の職員認証の他に，ログイン・ログアウトを実施した職員，時刻，操作内容の記録が実施されるため，不適切な接続端末の操作や，不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ，情報提供用個人識別符号を用いることがシステム上担保されており，不正な名寄せが行われるリスクに対応している。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム，情報提供ネットワークシステムとの間は，高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより，安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し，団体ごとに通信回線を分離するとともに，通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは，特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており，中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで，中間サーバー・プラットフォームの保守・運用を行う事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。		
7．特定個人情報の保管・消去		
リスク1：　特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[　　政府機関ではない　　]	＜選択肢＞ 1）特に力を入れて遵守している　　2）十分に遵守している 3）十分に遵守していない　　4）政府機関ではない
②安全管理体制	[　　十分に整備している　　]	＜選択肢＞ 1）特に力を入れて整備している　　2）十分に整備している 3）十分に整備していない
③安全管理規程	[　　十分に整備している　　]	＜選択肢＞ 1）特に力を入れて整備している　　2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[　　十分に周知している　　]	＜選択肢＞ 1）特に力を入れて周知している　　2）十分に周知している 3）十分に周知していない
⑤物理的対策	[　　十分に行っている　　]	＜選択肢＞ 1）特に力を入れて行っている　　2）十分に行っている 3）十分に行っていない
具体的な対策の内容	＜調布市における措置＞ ①カードキーによりサーバー室への入室を制限している。 ②バックアップは施錠管理された場所に保管している。 ③サーバー室出入口には監視カメラを設置している。 ④端末をワイヤーで固定している。 ⑤常時施錠の書庫に保管し，鍵の利用記録を残し，退庁時に確認している。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 ＜コンビニ交付システムデータセンターにおける措置＞ ①生体認証によりサーバー室への入室を制限している ②無停電電源装置及び自家発電装置を設置している。 ③震度7程度の地震に対応可能な耐震性を有している。 ・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。	

⑥技術的対策		[　　十分に行っている　　] <選択肢> 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
	具体的な対策の内容	＜調布市における措置＞ ・コンピュータウイルス監視ソフトを使用し，サーバー・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。 ・既存住基システムを利用できる職員を特定し，個人ごとにIDを割り当て，操作履歴（アクセスログ・操作ログ）を記録する。 ・USBなどの外部媒体の使用を制限している。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し，アクセス制限，侵入検知及び侵入防止を行うとともに，ログの解析を行う。 ②中間サーバー・プラットフォームでは，ウイルス対策ソフトを導入し，パターンファイルの更新を行う。 ③導入しているOS及びミドルウェアについて，必要に応じてセキュリティパッチの適用を行う。 ④中間サーバー・プラットフォームは，政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し，インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤中間サーバーのデータベースに保存される特定個人情報は，中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ⑥中間サーバーと団体についてはVPN等の技術を利用し，団体ごとに通信回線を分離するとともに，通信を暗号化することで安全性を確保している。 ⑦中間サーバー・プラットフォームの移行の際は，中間サーバー・プラットフォームの事業者において，移行するデータを暗号化した上で，インターネットを経由しない専用回線を使用し，VPN等の技術を利用して通信を暗号化することでデータ移行を行う。 ＜サービス検索・電子申請機能における措置＞ ・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。
⑦バックアップ		[　　十分に行っている　　] <選択肢> 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知		[　　十分に行っている　　] <選択肢> 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか		[　発生なし　] <選択肢> 1）発生あり　2）発生なし
	その内容	—
	再発防止策の内容	—
⑩死者の個人番号		[　　保管している　　] <選択肢> 1）保管している　2）保管していない
	具体的な保管方法	生存者の個人番号と同様の方法により保管している。
その他の措置の内容		—
リスクへの対策は十分か		[　　十分である　　] <選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
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		既存住基システムの整合処理を定期的に実施し，保存する本人確認情報が最新であるかどうかを確認することにより担保する。
リスクへの対策は十分か		[　　十分である　　] <選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている

リスク3： 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	＜選択肢＞ 1）定めている 2）定めていない
手順の内容	保存期間が経過した消除者に関するデータは，システム更新等の機会に一括して消去している。保存期間が経過した申請書等は，溶解処理によって廃棄している。	
その他の措置の内容	―	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の保管・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		
＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバー・プラットフォームを活用することにより，統一した設備環境による高レベルのセキュリティ管理（入退室管理等），ITリテラシーの高い運用担当者によるセキュリティリスクの低減及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。		

Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7．リスク1⑨を除く。）

1．特定個人情報ファイル名	
（2）本人確認情報ファイル	
2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1：　目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	本人確認情報の入手元は既存住基システムに限定されるため，既存住基システムへの情報の登録の際に，申請等の窓口における届出及び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。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	・平成14年6月10日総務省告示第334号（第6－7　本人確認情報の通知及び記録）等により市町村CSにおいて既存住基システムを通じて入手することととされている情報以外を入手できないことをシステム上で担保する。 ・正当な利用目的以外の目的にデータベースが構成されることを防止するため，本人確認情報の検索を行う際の検索条件として，少なくとも性別を除く2情報以上（氏名と住所の組み合わせ，氏名と生年月日の組み合わせ）の指定を必須とする。 ・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＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク2：　不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	・本人確認情報の入手元を既存住基システムに限定する。 ・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，後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。 ・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＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク3：　入手した特定個人情報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	・窓口において，対面で身分証明書（個人番号カード等）の提示を受け，本人確認を行う。 ・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	・個人番号カード等の提示を受け，本人確認を行う。 ・出生等により新たに個人番号が指定される場合や，転入の際に個人番号カード（法令により定められた身分証明書の組み合わせ）の提示がない場合には，市町村CSにおいて本人確認情報と個人番号の対応付けの確認を行う。
特定個人情報の正確性確保の措置の内容	・本人確認情報の入力，削除及び訂正を行う際には，整合性を確保するために，入力，削除及び訂正を行った者以外の者が確認する等，必ず入力，削除及び訂正した内容を確認する。 ・入力，削除及び訂正作業に用いた届出書，申請書等は、当市で定める規程に基づいて管理し，保管する。 ・個人番号カード内の記憶領域に格納された個人番号を申請フォームに自動転記を行うことにより，不正確な個人番号の入力を抑止する措置を講じている。
その他の措置の内容	―
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	・機構が作成・配付する専用のアプリケーション（※）を用いることにより，入手の際の特定個人情報の漏えい・紛失の防止に努める。 ・操作者の認証を行う。 ・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。 ※市町村CSのサーバ上で稼動するアプリケーション。市町村CSで管理されるデータの安全保護対策，不正アクセスの防止策には，最新の認証技術や暗号化技術を採用し，データの盗聴，改ざん，破壊及び盗難，端末の不正利用及びなりすまし等を防止する。また，市町村CSのサーバ自体には，外部からのこじあけ等に対して防御性に優れた耐タンパー装置（通信時の相互認証及びデータの暗号化に必要な情報を保管管理する）を内蔵している。
リスクへの対策は十分か	[十分である]　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	
—	

3. 特定個人情報の使用

リスク1： 目的を超えた紐付け、事務に必要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等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のサーバ上には住民基本台帳ネットワークシステムの管理及び運用に必要なソフトウェア以外作動させず，また，市町村CSが設置されたセグメントにあるハブには権限の無い者が機器を接続できないよう，適切な対策（物理的なアクセス制限，MACアドレスによるフィルタリング等）を講じる。
その他の措置の内容	—
リスクへの対策は十分か	[十分である]　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク	
ユーザ認証の管理	[行っている]　＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	・生体認証による操作者認証を行う。
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発行管理・職員ごとに業務上必要な権限のみ付与している。 ②失効管理・異動，退職等が生じた都度，権限を更新，削除している。
アクセス権限の管理	[行っている]　＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	・権限表を作成し，権限の更新・削除について記録している。
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	・操作履歴（アクセスログ・操作ログ）を記録する。 ・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。 ・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＞ 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	・操作履歴（アクセスログ・操作ログ）を記録する。 ・情報セキュリティについて研修する。 ・サービス検索・電子申請機能へアクセスできる端末を制限する。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク4：特定個人情報ファイルが不正に複製されるリスク	
リスクに対する措置の内容	・システム上，管理権限を与えられた者以外，情報の複製は行えない仕組みとする。 ・委託先における無許可のデータ複製を禁止している。 ・情報セキュリティについて研修を行う。 ・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。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	
その他，特定個人情報の使用にあたり，以下の措置を講じる。 ・スクリーンセーバ等を利用して，長時間にわたり本人確認情報を表示させない。 ・統合端末のディスプレイを，来庁者から見えない位置に置く。 ・本人確認情報が表示された画面のハードコピーはできない。 ・一定時間端末が操作されない場合，自動的にログオフする設定とする。	

4．特定個人情報ファイルの取扱いの委託		**[　]委託しない**
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認	・委託先の社会的信用（プライバシーマーク，ISMSの取得）と能力を確認する。また，委託業者が選定基準を引き続き満たしていることを適時確認するとともに，その記録を残す。 ・委託先に対し，従業者の教育・啓発の実施を契約において義務付けている。	
特定個人情報ファイルの閲覧者・更新者の制限	[　制限している　] ＜選択肢＞ 1）制限している　2）制限していない	
具体的な制限方法	・委託先の業務体制を書面にて提出させている。 ・アカウント管理を行い，操作を制限している。	
特定個人情報ファイルの取扱いの記録	[　記録を残している　] ＜選択肢＞ 1）記録を残している　2）記録を残していない	
具体的な方法	・アクセスログを保存している	
特定個人情報の提供ルール	[　定めている　] ＜選択肢＞ 1）定めている　2）定めていない	
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	・委託先から他者への個人情報の提供を禁止している。 ・委託元は，事前に通知することなく個人情報の取扱状況について報告を求めることができる。	
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・データの授受に際して記録を残すこととしている。 ・委託先が特定個人情報を目的外に使用することは契約上禁止している。 ・委託元は，事前に通知することなく個人情報の取扱状況について報告を求めることができる。	

特定個人情報の消去ルール	[定めている]	<選択肢> 1）定めている 2）定めていない
ルールの内容及びルール遵守の確認方法	・個人情報を保管する必要がなくなったときには，速やかに委託元に返却又は復元が不可能な方法により消去しなければならない。 ・委託元は，事前に通知することなく個人情報の取扱状況について報告を求めることができる。	
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> 1）定めている 2）定めていない
規定の内容	・個人情報の複写，複製の禁止 ・秘密保持 ・目的外使用，第三者提供の禁止 ・再委託の禁止（再委託をする場合は，委託元の書面による事前の同意が必要） ・事故等の報告 ・検査監督権	
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> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない 4）再委託していない
具体的な方法	・再委託先に対し，委託先と同様の機密保持に関する規定を契約において義務付けている。 ・委託元は，事前に通知することなく個人情報の取扱状況について報告を求めることができる。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
—		
5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）	**[ ] 提供・移転しない**	
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[記録を残している]	<選択肢> 1）記録を残している 2）記録を残していない
具体的な方法	特定個人情報（個人番号，4情報（氏名，性別，生年月日，住所）等）の提供を行う際に，提供記録等をシステム上で管理し，ログを保存する。なお，システム上，提供に係る処理を行ったものの提供が認められなかった場合についても記録を残す。	
特定個人情報の提供・移転に関するルール	[定めている]	<選択肢> 1）定めている 2）定めていない
ルールの内容及びルール遵守の確認方法	番号法，住基法等の法令により認められる提供のみ行う。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 不適切な方法で提供・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提供はなされないことがシステム上担保される。 また，媒体へ出力する必要がある場合には，逐一出力の記録が残される仕組みを構築する。	
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている

リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク	
リスクに対する措置の内容	・誤った情報を提供・移転してしまうリスクへの措置 ： システム上，照会元から指定された検索条件に基づき得た結果を適切に提供・移転することを担保する。 また，本人確認情報に変更が生じた際には，市町村CSへの登録時点で項目のフォーマットチェックや論理チェック（例えば，現存する住民に対して転入を異動事由とする更新が行われようとした場合や，転居を異動事由とする更新の際に住所以外の更新が行われようとした場合に当該処理をエラーとする）がなされた情報を通知することをシステム上で担保する。 ・誤った相手に提供・移転してしまうリスクへの措置 ： 相手方（都道府県サーバ）と市町村CSの間の通信では相互認証を実施するため，認証できない相手先への情報の提供はなされないことがシステム上担保される。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている

特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置
―

6. 情報提供ネットワークシステムとの接続	[○] 接続しない（入手） [○] 接続しない（提供）
リスク1： 目的外の入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 安全が保たれない方法によって入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク5： 不正な提供が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 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＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置		

7. 特定個人情報の保管・消去

リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	＜選択肢＞ 1）特に力を入れて遵守している　2）十分に遵守している 3）十分に遵守していない　4）政府機関ではない
②安全管理体制	[十分に整備している]	＜選択肢＞ 1）特に力を入れて整備している　2）十分に整備している 3）十分に整備していない
③安全管理規程	[十分に整備している]	＜選択肢＞ 1）特に力を入れて整備している　2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	＜選択肢＞ 1）特に力を入れて周知している　2）十分に周知している 3）十分に周知していない
⑤物理的対策	[十分に行っている]	＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
具体的な対策の内容	①カードキーによりサーバー室への入室を制限している。 ②バックアップは施錠管理された場所に保管している。 ③サーバー室出入口には監視カメラを設置している。 ④端末をワイヤーで固定している。 ・業務時間外は施錠できるキャビネット等への保管している。 ・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。	
⑥技術的対策	[十分に行っている]	＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
具体的な対策の内容	・不正プログラム対策　：　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。 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を定期的に入手し，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。 ・不正アクセス対策　：　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している。 ・USBなどの外部媒体の使用を制限している。 ・サービス検索・電子申請機能と地方公共団体との間は，専用線であるLGWAN回線を用いた通信を行うことで，外部からの盗聴，漏えい等が起こらないようにしており，さらに通信自体も暗号化している。	
⑦バックアップ	[十分に行っている]	＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない

⑧事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	<選択肢> 1）発生あり 2）発生なし
その内容	—	
再発防止策の内容	—	
⑩死者の個人番号	[保管している]	<選択肢> 1）保管している 2）保管していない
具体的な保管方法	生存者の個人番号と同様の方法により保管している。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
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	既存住基システムとの整合処理を定期的に実施し，保存する本人確認情報が最新であるかどうかを確認することにより担保する。	
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	<選択肢> 1）定めている 2）定めていない
手順の内容	・システム上，住民基本台帳法施行令第34条第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。 ・磁気ディスクの廃棄時は，要領・手順書等に基づき，内容の消去、破壊等を行うとともに，磁気ディスク管理簿にその記録を残す。また，専用ソフトによるフォーマット，物理的粉砕等を行うことにより，内容を読み出すことができないようにする。 ・帳票については，要領・手順書等に基づき，帳票管理簿等を作成し，受渡し，保管及び廃棄の運用が適切になされていることを適時確認するとともに，その記録を残す。廃棄時には，要領・手順書等に基づき，裁断，溶解等を行うとともに，帳票管理簿等にその記録を残す。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		
—		

Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7. リスク1⑨を除く。）

1. 特定個人情報ファイル名	
（3）送付先情報ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	送付先情報の入手元は既存住基システムに限定されるため，既存住基システムへの情報の登録の際に，申請等の窓口における届出及び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。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	・平成14年6月10日総務省告示第334号（第6－7　本人確認情報の通知及び記録）等により市町村CSにおいて既存住基システムを通じて入手することとされている情報以外を入手できないことをシステム上で担保する。 ・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＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	送付先情報の入手元を既存住基システムに限定する。 ・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。 ・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＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報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	・特定個人情報の入手元である既存住基システムへの情報の登録の際，窓口において，対面で身分証明書の提示を受け，本人確認を行う。 ・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	個人番号の生成元である機構が設置・管理する全国サーバから住民票コードに対応付く個人番号を適切に取得できることをシステムにより担保する。
特定個人情報の正確性確保の措置の内容	既存住基システムにおいて正確性が確保された送付先情報を適切に受信できることをシステムにより担保する。なお，送付先情報ファイルは、既存住基システムから入手後，個人番号カード管理システムに送付先情報を送付した時点で役割を終える（不要となる）ため，送付後速やかに市町村CSから削除する。そのため，入手から削除までのサイクルがごく短期間であることから，入手から削除の間の正確性を維持するための特段の対策は講じない。 ・個人番号カード内の記憶領域に格納された個人番号を申請フォームに自動転記を行うことにより，不正確な個人番号の入力を抑止する措置を講じている。
その他の措置の内容	―
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	・機構が作成・配付する専用のアプリケーション（※）を用いることにより，入手の際の特定個人情報の漏えい・紛失の防止に努める。 ・操作者の認証を行う。 ・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。 ※市町村CSのサーバ上で稼動するアプリケーション。市町村CSで管理されるデータの安全保護対策，不正アクセスの防止策には，最新の認証技術や暗号化技術を採用し，データの盗聴，改ざん，破壊及び盗難，端末の不正利用及びなりすまし等を防止する。また，市町村CSのサーバ自体には，外部からのこじあけ等に対して防御性に優れた耐タンパー装置（通信時の相互認証及びデータの暗号化に必要な情報を保管管理する）を内蔵している。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	
—	

3．特定個人情報の使用

リスク1： 目的を超えた紐付け、事務に必要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等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のサーバ上には住民基本台帳ネットワークシステムの管理及び運用に必要なソフトウェア以外作動させず，また，市町村CSが設置されたセグメントにあるハブには権限の無い者が機器を接続できないよう，適切な対策（物理的なアクセス制限，MACアドレスによるフィルタリング等）を講じる。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク	
ユーザ認証の管理	[行っている] ＜選択肢＞ 1）行っている 2）行っていない
具体的な管理方法	・生体認証による操作者認証を行う。
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発行管理・職員ごとに業務上必要な権限のみ付与している。 ②失効管理・異動，退職等が生じた都度、権限を更新、削除している。
アクセス権限の管理	[行っている] ＜選択肢＞ 1）行っている 2）行っていない
具体的な管理方法	・権限表を作成し，権限の更新・削除について記録している。
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	・操作履歴（アクセスログ・操作ログ）を記録する。 ・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。 ・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＞ 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	・操作履歴（アクセスログ・操作ログ）を記録する。 ・情報セキュリティについて研修する。 ・サービス検索・電子申請機能へアクセスできる端末を制限する。
リスクへの対策は十分か	[十分である] <選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク4： 特定個人情報ファイルが不正に複製されるリスク	
リスクに対する措置の内容	・システム上，管理権限を与えられた者以外，情報の複製は行えない仕組みとする。 ・委託先における無許可のデータ複製を禁止している。 ・情報セキュリティについて研修を行う。 ・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。
リスクへの対策は十分か	[十分である] <選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	
その他，特定個人情報の使用にあたり，以下の措置を講じる。 ・スクリーンセーバ等を利用して，長時間にわたり本人確認情報を表示させない ・統合端末のディスプレイを，来庁者から見えない位置に置く ・本人確認情報が表示された画面のハードコピーはできない ・一定時間端末が操作されない場合，自動的にログオフする設定とする。	
4．特定個人情報ファイルの取扱いの委託	**[ ] 委託しない**
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク	
情報保護管理体制の確認	・委託先の社会的信用（プライバシーマーク，ISMSの取得）と能力を確認する。また，委託業者が選定基準を引き続き満たしていることを適時確認するとともに，その記録を残す。 ・委託先に対し，従業者の教育・啓発の実施を契約において義務付けている。
特定個人情報ファイルの閲覧者・更新者の制限	[制限している] <選択肢> 1）制限している 2）制限していない
具体的な制限方法	・委託先の業務体制を書面にて提出させている。 ・アカウント管理を行い，操作を制限している。
特定個人情報ファイルの取扱いの記録	[記録を残している] <選択肢> 1）記録を残している 2）記録を残していない
具体的な方法	・アクセスログを保存している
特定個人情報の提供ルール	[定めている] <選択肢> 1）定めている 2）定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	・委託先から他者への個人情報の提供を禁止している。 ・委託元は，事前に通知することなく個人情報の取扱状況について報告を求めることができる。
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・データの授受に際して記録を残すこととしている。 ・委託先が特定個人情報を目的外に使用することは契約上禁止している。 ・委託元，事前に通知することなく個人情報の取扱状況について報告を求めることができる。
特定個人情報の消去ルール	[定めている] <選択肢> 1）定めている 2）定めていない
ルールの内容及びルール遵守の確認方法	・個人情報を保管する必要がなくなったときには，速やかに委託元に返却又は復元が不可能な方法により消去しなければならない。 ・委託元は，事前に通知することなく個人情報の取扱状況について報告を求めることができる。

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> 1）定めている 2）定めていない
	規定の内容	・個人情報の複写，複製の禁止 ・秘密保持 ・目的外使用，第三者提供の禁止 ・再委託の禁止（再委託をする場合は，委託元の書面による事前の同意が必要） ・事故等の報告 ・検査監督権
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> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない 4）再委託していない
	具体的な方法	・再委託先に対し，委託先と同様の機密保持に関する規定を契約において義務付けている。 ・委託元は，事前に通知することなく個人情報の取扱状況について報告を求めることができる。
その他の措置の内容		—
リスクへの対策は十分か		[十分である] <選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
—		
5．特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		**[ ] 提供・移転しない**
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録		[記録を残している] <選択肢> 1）記録を残している 2）記録を残していない
	具体的な方法	特定個人情報（個人番号，4情報（氏名，性別，生年月日，住所）等）の提供を行う際に，提供記録等をシステム上で管理し，ログを保存する。なお，システム上，提供に係る処理を行ったものの提供が認められなかった場合についても記録を残す。
特定個人情報の提供・移転に関するルール		[定めている] <選択肢> 1）定めている 2）定めていない
	ルールの内容及びルール遵守の確認方法	番号法，住基法等の法令により認められる提供のみ行う。
その他の措置の内容		—
リスクへの対策は十分か		[十分である] <選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 不適切な方法で提供・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提供はなされないことがシステム上担保される。 また，媒体へ出力する必要がある場合には，逐一出力の記録が残される仕組みを構築する。
リスクへの対策は十分か		[十分である] <選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容		・誤った情報を提供・移転してしまうリスクへの措置 ： システム上，既存住基システムから入手した情報の内容に編集を加えず，適切に個人番号カード管理システムに提供することを担保する。 ・誤った相手に提供・移転してしまうリスクへの措置 ： 相手方（個人番号カード管理システム）と市町村CSの間の通信では相互認証を実施するため，認証できない相手先への情報の提供はなされないことがシステム上担保される。
リスクへの対策は十分か		[十分である] <選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている

特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置
―

6. 情報提供ネットワークシステムとの接続	[○] 接続しない（入手） [○] 接続しない（提供）
リスク1： 目的外の入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] <選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 安全が保たれない方法によって入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] <選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] <選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] <選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク5： 不正な提供が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] <選択肢> 1）特に力を入れている 2）十分である 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> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] <選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1）特に力を入れて遵守している 2）十分に遵守している 3）十分に遵守していない 4）政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1）特に力を入れて周知している 2）十分に周知している 3）十分に周知していない
⑤物理的対策	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
具体的な対策の内容	①カードキーによりサーバー室への入室を制限している。 ②バックアップは施錠管理された場所に保管している。 ③サーバー室出入口には監視カメラを設置している。 ④端末をワイヤーで固定している。 ・業務時間外は施錠できるキャビネット等への保管している。 ・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。	
⑥技術的対策	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
具体的な対策の内容	・不正プログラム対策 ： 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。 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を定期的に入手し，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。 ・不正アクセス対策 ： 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している。 ・USBなどの外部媒体の使用を制限している。 ・サービス検索・電子申請機能と地方公共団体との間は，専用線であるLGWAN回線を用いた通信を行うことで，外部からの盗聴，漏えい等が起こらないようにしており，さらに通信自体も暗号化している。	
⑦バックアップ	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	<選択肢> 1）発生あり 2）発生なし
その内容	—	
再発防止策の内容	—	
⑩死者の個人番号	[保管している]	<選択肢> 1）保管している 2）保管していない
具体的な保管方法	生存者の個人番号と同様の方法により保管している。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている

リスク2： 特定個人情報が古い情報のまま保管され続けるリスク	
リスクに対する措置の内容	本特定個人情報ファイル（送付先情報ファイル）は，送付先情報の連携を行う必要が生じた都度作成し連携することとしており，システム上，連携後速やか（1営業日後）に削除する仕組みとする。また，媒体を用いて連携する場合，当該媒体は連携後，連携先である機構において適切に管理され，市町村では保管しない。 そのため，送付先情報ファイルにおいて特定個人情報が古い情報のまま保管され続けるリスクは存在しない。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 特定個人情報が消去されずいつまでも存在するリスク	
消去手順	[定めている] ＜選択肢＞ 1）定めている 2）定めていない
手順の内容	システム上，保管期間の経過した特定個人情報を一括して削除する仕組みとする。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置	
送付先情報ファイルは，機構への特定個人情報の提供後，速やかに市町村CSから削除される。その後，当該特定個人情報は機構において管理されるため，送付先情報ファイルのバックアップは取得しない予定である。	

Ⅳ　その他のリスク対策 ※

1. 監査		
①自己点検	[　　十分に行っている　　]	＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
具体的なチェック方法	＜当市における措置＞ ①年に一回，担当者が評価書の記載内容通りの運用がされているか確認を行い，必要に応じて運用の見直しを図る。 ＜中間サーバー･プラットフォームにおける措置＞ ①運用規則等に基づき，中間サーバー･プラットフォームの運用に携わる職員及び事業者に対し，定期的に自己点検を実施することとしている。	
②監査	[　　十分に行っている　　]	＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
具体的な内容	＜当市における措置＞ ①内部監査を定期的に実施し，監査結果を踏まえて体制や規定を改善する。 ＜中間サーバー･プラットフォームにおける措置＞ ①運用規則等に基づき，中間サーバー･プラットフォームについて，定期的に監査を行うこととしている。 ②政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者は，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＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
具体的な方法	＜当市における措置＞ ①情報セキュリティに関する研修を行い，情報セキュリティに対する意識の向上を図っている。 ②情報漏えい事件等に関する新聞記事を職員に回覧し，個人情報保護に対する意識の向上を図っている。 ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバー･プラットフォームの運用に携わる職員及び事業者に対し，セキュリティ研修等を実施することとしている。 ②中間サーバー･プラットフォームの業務に就く場合は，運用規則等について研修を行うこととしている。	

3. その他のリスク対策
＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバー･プラットフォームを活用することにより，政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者による高レベルのセキュリティ管理（入退室管理等），ITリテラシの高い運用担当者によるセキュリティリスクの低減及び技術力の高い運用担当者による均一的で安定したシステム運用･監視を実現する。

Ⅴ　開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	市民部市民課 〒182-8511　調布市小島町2－35－1　電話番号　042－481－7043
②請求方法	開示・訂正及び利用停止は，指定様式による書面の提出により請求する。
特記事項	―
③手数料等	[　　無料　　]　　＜選択肢＞ 1) 有料　　2) 無料 （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＞ 1) 行っている　　2) 行っていない
個人情報ファイル名	住民基本台帳事務 （住民基本台帳ファイル・本人確認情報ファイル・送付先情報ファイル）
公表場所	公文書資料室
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	市民部市民課 〒182-8511　調布市小島町2－35－1　電話番号　042－481－7043
②対応方法	対応内容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8年3月13日
②しきい値判断結果	［　　基礎項目評価及び全項目評価の実施が義務付けられる　　］ ＜選択肢＞ 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 基礎項目評価及び重点項目評価の実施が義務付けられる（任意に全項目評価を実施） 3) 基礎項目評価の実施が義務付けられる（任意に全項目評価を実施） 4) 特定個人情報保護評価の実施が義務付けられない（任意に全項目評価を実施）
2. 国民・住民等からの意見の聴取	
①方法	市ホームページ，市民課，公文書資料室，神代出張所，文化会館たづくり11階みんなの広場，市民活動支援センター，各図書館，各公民館，各地域福祉センター（深大寺を除く），教育会館（1階）において評価書を閲覧できるものとし，意見の提出は，持参，郵便，FAX，電子メール，公表場所に設置する意見提出箱により受け付けることとする。
②実施日・期間	令和7年9月1日から令和7年9月30日（30日以上実施）
③期間を短縮する特段の理由	―
④主な意見の内容	意見なし
⑤評価書への反映	
3. 第三者点検	
①実施日	令和7年12月24日
②方法	調布市個人情報保護審査会による点検
③結果	指摘事項なし
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3年9月1日	Ⅰ 基本情報 6．情報提供ネットワークシステムによる情報連携 ※ ②法令上の根拠	・番号法第19条第7号（特定個人情報の提供の制限）及び別表第二	・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	事後	
令和5年6月22日	Ⅰ基本情報 1特定個人情報ファイルを取り扱う事務 ②事務の内容 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 ①システム名称 ②システム機能 ③他のシステムとの接続		⑪窓口や郵送の書類の受入，サービス検索・電子申請機能での受領 システム7	事後	
令和5年6月22日	Ⅱ特定個人情報ファイルの概要 3特定個人情報の入手・使用 ②入手方法	（〇）その他（住民基本台帳台帳ネットワーク）	（〇）その他（住民基本台帳台帳ネットワーク，サービス検索・電子申請機能）	事後	
令和5年6月22日	Ⅲ特定個人情報の取扱いプロセスにおけるリスク対策 2特定個人情報の入手（特定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 ・必要な情報以外を入手することを防止するための措置		（対象者以外の情報の入手を防止するための措置の内容） ・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） ・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，異なる手続きに係る申請や不要な情報を送信してしまうリスクを防止する。	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年6月22日	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 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 ・特定個人情報の正確性確保の措置の内容 リスク4入手した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		＜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） ・サービス検索・電子申請機能の画面の誘導において住民に何の手続きを探し電子申請を行いたいのか理解してもらいながら操作していただき，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。 ＜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） ・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。 （特定個人情報の正確性確保の措置の内容） ・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。 ＜入手した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） ・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，漏えい等がお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。	事後	
令和5年6月22日	3特定個人情報の使用 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 （特定個人情報の使用の記録）		（特定個人情報の使用の記録） ・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。 ・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。	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年6月22日	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）		（リスクに対する措置） ・サービス検索・電子申請機能へアクセスできる端末を制限する。	事後	
令和5年6月22日	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）		（リスクに対する措置） ・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。	事後	
令和5年6月22日	7特定個人情報の保管・消去 ⑥技術的対策 （具体的な対策の内容）		＜サービス検索・電子申請機能における措置＞ ・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。	事後	
令和6年11月7日	Ⅰ－1 ②事務の内容	（略） 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省令（平成26年11月20日総務省令第85号。以下「個人番号カード省令」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。 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。	（略） 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「個人番号カード省令」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。 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。	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年11月7日	Ⅰ－6 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 （別表第二における情報提供の根拠） ：第三欄（情報提供者）が「市町村長」の項のうち、第四欄（特定個人情報）に「住民票関係情報」が含まれる項（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、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） （別表第二における情報照会の根拠） ：なし （住民基本台帳に関する事務において情報提供ネットワークシステムによる情報照会は行わない）	・番号法第19条第8号（特定個人情報の提供の制限）及び同号に基づく主務省令第2条の表 （番号法第19条第8号に基づく主務省令第2条の表における情報提供の根拠） ：第三欄（情報提供者）が「市町村長」の項のうち、第四欄（利用特定個人情報）に「住民票関係情報」が含まれる項 （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） （番号法第19条第8号に基づく主務省令第2条の表における情報照会の根拠） ：なし （住民基本台帳に関する事務において情報提供ネットワークシステムによる情報照会は行わない）	事後	
令和8年3月1日	Ⅱ特定個人情報ファイルの概要 4特定個人情報ファイルの取扱いの委託 委託事項2 ③委託先における取扱者数	10人以上50人未満	50人以上100人未満	事後	
令和8年3月1日	Ⅱ特定個人情報ファイルの概要 6特定個人情報の保管・消去 ②保管期間　その妥当性	住基ネットCSのアプリケーション保守作業，ジョブスケジューリング等のシステム運用作業，職員からの問い合わせに対する調査等・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。 ・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第34条第3項（保存）に定める期間（150年間）保管する。	住基ネットCSのアプリケーション保守作業，ジョブスケジューリング等のシステム運用作業，職員からの問い合わせに対する調査等・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。 ・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第34条第2項（保存）に定める期間（150年間）保管する。	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和8年3月1日	Ⅱ特定個人情報ファイルの概要 6特定個人情報の保管・消去 ①保管場所	・入退館管理をしている建物内のうち，個人に貸与された入室カードによる入退室管理を行っている部屋に設置したサーバ内に保管。サーバへのアクセスはID及びパスワードによる認証が必要。	（略） ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームは政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し，設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお，クラウドサービス事業者は，セキュリティ管理策が適切に実施されているほか，次を満たしている。 ・ISO/IEC27017，ISO/IEC27018の認証を受けている。 ・日本国内でデータを保管している。 ②特定個人情報は，クラウドサービス事業者が保有・管理する環境に構築する中間サーバーのデータベース内に保存され，バックアップもデータベース上に保存される。	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和8年3月1日	Ⅱ特定個人情報ファイルの概要 6特定個人情報の保管・消去 ③消去方法	特定個人情報が記載された届書，申請書等は，規定の保存期間が経過した後，溶解処理している。 ＜中間サーバー・プラットフォームにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施されるため，通常，中間サーバー・プラットフォームの保守・運用を行う事業者が特定個人情報を消去することはない。 ②ディスク交換やハード更改等の際は，中間サーバー・プラットフォームの保守・運用を行う事業者において，保存された情報が読み出しできないよう，物理的破壊又は専用ソフト等を利用して完全に消去する。	特定個人情報が記載された届書，申請書等は，規定の保存期間が経過した後，溶解処理している。 ＜中間サーバー・プラットフォームにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施されるため，通常，中間サーバー・プラットフォームの保守・運用を行う事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②クラウドサービス事業者が保有・管理する環境において，障害やメンテナンス等によりディスクやハード等を交換する際は，クラウドサービス事業者において，政府情報システムのためのセキュリティ評価制度（ISMAP）に準拠したデータの暗号化消去及び物理的破壊を行う。さらに，第三者の監査機関が定期的に発行するレポートにより，クラウドサービス事業者において，確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ③中間サーバー・プラットフォームの移行に際は，地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において，保存された情報が読み出しできないよう，データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和8年3月1日	Ⅲ特定個人情報ファイルの概取扱いプロセスにおけるリスク対策 6情報提供ネットワークシステムとの接続 リスク6　リスクに対する措置の内容	（略） ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバーと既存システム，情報提供ネットワークシステムとの間は，高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより，不適切な方法で提供されるリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し，団体ごとに通信回線を分離するとともに，通信を暗号化することで漏えい･紛失のリスクに対応している。 ③中間サーバー･プラットフォームの保守･運用を行う事業者においては，特定個人情報に係る業務にはアクセスができないよう管理を行い，不適切な方法での情報提供を行えないよう管理している。	（略） ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバーと既存システム，情報提供ネットワークシステムとの間は，高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより，不適切な方法で提供されるリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し，団体ごとに通信回線を分離するとともに，通信を暗号化することで漏えい･紛失のリスクに対応している。 ③中間サーバー･プラットフォームの保守･運用を行う事業者及びクラウドサービス事業者においては，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。	事後	
令和8年3月1日	Ⅲ特定個人情報ファイルの概取扱いプロセスにおけるリスク対策 6情報提供ネットワークシステムとの接続 リスク6　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	（略） ④特定個人情報の管理を地方公共団体のみが行うことで，中間サーバー･プラットフォームの保守･運用を行う事業者における情報漏えい等のリスクを極小化する。	（略） ④特定個人情報の管理を地方公共団体のみが行うことで，中間サーバー･プラットフォームの保守･運用を行う事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。	事後	
令和8年3月1日	Ⅲ特定個人情報ファイルの概取扱いプロセスにおけるリスク対策 7特定個人情報の保管･消去 リスク1　⑤物理的対策	（略） ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバー･プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 （略）	（略） ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバー･プラットフォームは，政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有･管理する環境に設置し，設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお，クラウドサービス事業者は，セキュリティ管理策が適切に実施されているほか，次を満たしている。 ･ISO/IEC27017，ISO/IEC27018の認証を受けている。 ･日本国内でデータを保管している。 （略）	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和8年3月1日	Ⅲ特定個人情報ファイルの概取扱いプロセスにおけるリスク対策 7特定個人情報の保管・消去リスク1　⑥技術的対策	（略） ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し，アクセス制限，侵入検知及び侵入防止を行うとともに，ログの解析を行う。 ②中間サーバー・プラットフォームでは，ウイルス対策ソフトを導入し，パターンファイルの更新を行う。 ③導入しているOS及びミドルウェアについて，必要に応じてセキュリティパッチの適用を行う。 （略）	（略） ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し，アクセス制限，侵入検知及び侵入防止を行うとともに，ログの解析を行う。 ②中間サーバー・プラットフォームでは，ウイルス対策ソフトを導入し，パターンファイルの更新を行う。 ③導入しているOS及びミドルウェアについて，必要に応じてセキュリティパッチの適用を行う。 ④中間サーバー・プラットフォームは，政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し，インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤中間サーバーのデータベースに保存される特定個人情報は，中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ⑥中間サーバーと団体についてはVPN等の技術を利用し，団体ごとに通信回線を分離するとともに，通信を暗号化することで安全性を確保している。 ⑦中間サーバー・プラットフォームの移行の際は，中間サーバー・プラットフォームの事業者において，移行するデータを暗号化した上で，インターネットを経由しない専用回線を使用し，VPN等の技術を利用して通信を暗号化することでデータ移行を行う。 （略）	事後	
令和8年3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	（略） ＜中間サーバー･プラットフォームにおける措置＞ ①運用規則等に基づき，中間サーバー・プラットフォームについて，定期的に監査を行うこととしている。	（略） ＜中間サーバー･プラットフォームにおける措置＞ ①運用規則等に基づき，中間サーバー・プラットフォームについて，定期的に監査を行うこととしている。 ②政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者は，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。	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和8年3月1日	Ⅳその他のリスク対策 3その他のリスク対策	＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバー・プラットフォームを活用することにより，統一した設備環境による高レベルのセキュリティ管理（入退室管理等），ITリテラシの高い運用担当者によるセキュリティリスクの低減及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。	＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバー・プラットフォームを活用することにより，政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者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。	事後	
令和8年3月1日	Ⅰ基本情報 2特定個人情報ファイルを取り扱う事務において使用するシステム ①システム名称	GW証明書発行システム	証明書発行システム	事後	
令和8年3月1日	Ⅱ特定個人情報ファイルの概要 4特定個人情報ファイルの取扱いの委託 委託事項1	既存住基システム，住基GWシステム，住基ネットCS，GW証明発行システム（以下「住民基本台帳システム等」という。）の保守・運用	既存住基システム，住基GWシステム，住基ネットCS，証明発行システム（以下「住民基本台帳システム等」という。）の保守・運用	事後	
令和8年3月1日	Ⅰ基本情報 2特定個人情報ファイルを取り扱う事務において使用するシステム ②システムの機能	④情報提供機能　：　各業務で管理している別表2の提供業務情報を受領し，中間サーバーへの情報提供を行う。	④情報提供機能　：　各業務で管理している番号法第19条別表の提供業務情報を受領し，中間サーバーへの情報提供を行う。	事後	
令和8年3月1日	Ⅱ特定個人情報ファイルの概要 2基本情報 ③対象となる本人の範囲 その必要性	住民に関する市町村事務の処理の基礎として利用する ・住基法第7条において，住民基本台帳の記載項目と規定されるため ・番号法第19条　別表第二の事務において，符号の取得に利用するため	住民に関する市町村事務の処理の基礎として利用する ・住基法第7条において，住民基本台帳の記載項目と規定されるため ・番号法第19条別表の事務において，符号の取得に利用するため	事後	
令和8年3月1日	Ⅲ特定個人情報ファイルの概取扱いプロセスにおけるリスク対策 7特定個人情報の保管・消去 リスクに対する措置の内容	住既存住基システムとの整合処理を定期的に実施し，保存する本人確認情報が最新であるかどうかを確認することにより担保する。	既存住基システムとの整合処理を定期的に実施し，保存する本人確認情報が最新であるかどうかを確認することにより担保する。	事後	