

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	町田市 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

町田市は住民基本台帳事務における特定個人情報ファイルの取扱いにあたり、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減させるために適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項

町田市情報セキュリティポリシー

1 目的

町田市情報セキュリティポリシーは、様々な脅威に対する抑止、防止、検知及び回復について、組織的かつ体系的に取り組むための統一的な方針であり、情報セキュリティを実践するに当たっての基本的な考え方及び方策を定めることによって、市が保有する情報資産の機密性、完全性及び可用性を維持し、市民からの継続的な信頼を獲得することを目的とする。

評価実施機関名

町田市長

個人情報保護委員会 承認日【行政機関等のみ】

公表日

令和7年4月1日

項目一覧

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

I 基本情報

1. 特定個人情報ファイルを取り扱う事務

①事務の名称	住民基本台帳事務
②事務の内容 ※	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、市町村（特別区を含む。）（以下「市町村」という。）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。 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（住民基本台帳ネットワークシステム）を都道府県と共同して構築している。 市町村は、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 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）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 3) 1万人以上10万人未満 5) 30万人以上 2) 1,000人以上1万人未満 4) 10万人以上30万人未満

2. 特定個人情報ファイルを取り扱う事務において使用するシステム

システム1

①システムの名称	住民記録システム（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	本システムの主な機能は次のとおり。 1. 住民基本台帳の記載機能 2. 住民基本台帳の修正機能 3. 住民基本台帳の消除機能 4. 住民基本台帳の照会機能 5. 住民基本台帳に基く住民票の写し等の発行機能 6. コンビニエンスストアにおける証明書等の自動交付（住民票の写し、印鑑登録証明書）のための連携機能 7. 公的個人認証システムとの連携機能 8. 出入国在留管理庁との連携機能 9. 印鑑登録システムとの連携機能 10. 戸籍システムとの連携機能 11. 宛名システム兼連携システムとの連携機能
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 [○] 住民基本台帳ネットワークシステム [○] 宛名システム等 [○] その他 （申請管理システム [] 庁内連携システム [] 既存住民基本台帳システム [] 税務システム)

システム2～5	
システム2	
①システムの名称	住民基本台帳ネットワークシステム（以下「住基ネット」という。）
②システムの機能	本システムの主な機能は次のとおり。 1. 本人確認情報の更新機能 既存住基システムにおいて住民票の記載事項の変更又は新規作成が発生した場合に、当該情報を元に市町村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. 本人確認機能 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）処理機能 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. 本人確認情報検索機能 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。 5. 機構への情報照会機能 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. 本人確認情報整合機能 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. 送付先情報通知機能 機構において、住民に対して番号通知書類（個人番号通知書、個人番号カード交付申請書（以下「交付申請書」という。）等）を送付するため、既存住基システムから当該市町村の住民基本台帳に記載されている者の送付先情報を抽出し、当該情報を機構が設置・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能 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 ☐ 住民基本台帳ネットワークシステム ☐ 宛名システム等 ☐ その他（ ☐ 庁内連携システム ☒ 既存住民基本台帳システム ☐ 税務システム

システム3	
①システムの名称	中間サーバー
②システムの機能	本システムの主な機能は次のとおり。 1. 符号管理機能 符号管理機能は情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」とを紐付け、その情報を保管・管理する機能。 2. 情報照会機能 情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 3. 情報提供機能 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。 4. 既存システム接続機能 中間サーバーと既存システム、宛名システム及び住民記録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、又は提供があった旨の情報提供等記録を生成し、管理する機能。 6. 情報提供データベース管理機能 特定個人情報を副本として保存・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機能。 8. セキュリティ管理機能 暗号化・復号機能と、鍵情報及び照会許可用照合リストを管理する機能。 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 バッチ処理の状況管理、業務統計情報の集計、稼働状態の通知、保管切れ情報の削除を行う機能。
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4	
①システムの名称	宛名システム兼連携システム
②システムの機能	本システムの主な機能は次のとおり。 1. 団体内統合宛名番号付番機能 団体内統合宛名番号が未登録の個人について、新規に団体内統合宛名番号を付番し、各業務システムの宛名番号と紐づけて管理する。 2. 中間サーバー情報連携機能 各業務システムと中間サーバーとの情報連携を行う。 3. 統合DB機能 一般財団法人全国地域情報化推進協会（APPLIC）が定める「地域情報プラットフォーム標準仕様」に準拠した業務情報を管理し、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（ 中間サーバー、福祉、介護保険、国民健康保険、後期高齢医療等 ）

システム5	
①システムの名称	証明書等のコンビニ交付システム
②システムの機能	1 既存システム連携機能 ・既存住基、印鑑、税、戸籍システムから証明書情報を連携する機能。 2 コンビニ交付機能 ・証明書交付センターからの要求に応答し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 [] 住民基本台帳ネットワークシステム [○] 既存住民基本台帳システム [○] 宛名システム等 [○] 税務システム [○] その他 (戸籍システム、証明書交付センター)
システム6～10	
システム6	
①システムの名称	申請管理システム
②システムの機能	本システムの主な機能は次のとおり。 1 オンライン申請情報の取得機能 ・サービス検索・電子申請機能からのオンライン申請情報を取得する機能 2 オンライン申請情報の管理機能 ・オンライン申請情報を一元管理する機能 3 業務システムとの連携機能 ・オンライン申請情報を業務システムへ連携する機能
③他のシステムとの接続	[] 情報提供ネットワークシステム [] 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 (サービス検索・電子申請機能)
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	本システムの主な機能は次のとおり。 1 住民向け機能 ・市民が、自身の受けられるサービスを検索し、申請できる機能 2 地方公共団体向け機能 ・地方自治体が、市民の申請データを、画面で確認または受信できる機能
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 (申請管理システム)
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個人番号通知書の事務に必要なため。 ・個人番号カードの事務に必要なため。 (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及び機構保存本人確認情報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個人番号通知書の形式にて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項及び個人番号カード省令第7条)。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申請書の送付については、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)に基づいて機構が行うこととされていることから、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。
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) ・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(本人等の請求によ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15条の2(除票簿) ・第15条の3(除票の記載事項) ・第15条の4(除票の写し等の交付) ・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)

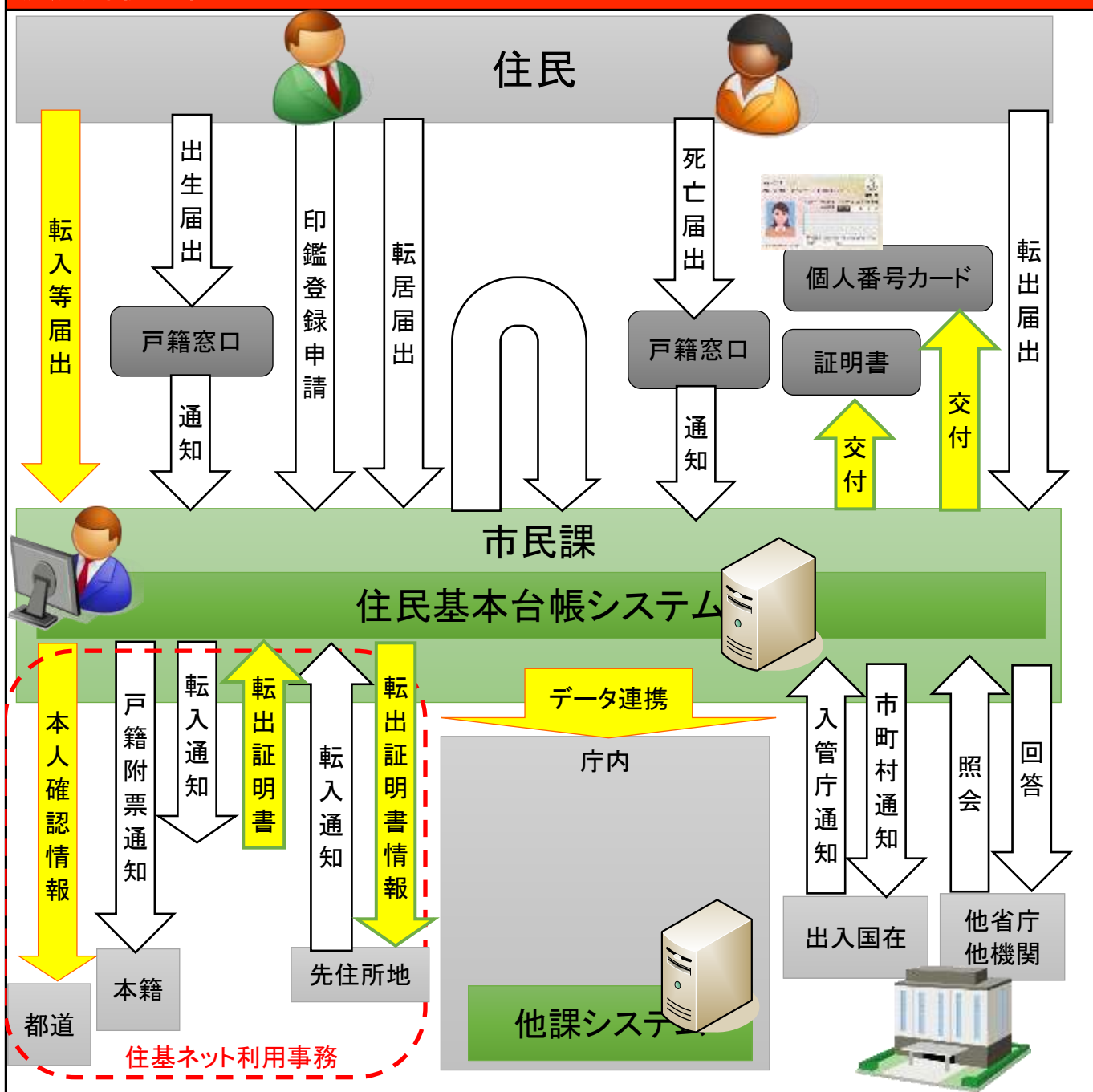
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[実施する] <選択肢> 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	<提供ができる根拠規定> 番号法第19条第8号に基づく主務省令第2条の表のうち、第三欄(情報提供者)が「市町村長」の項で第四欄(利用特定個人情報)に「住民票関係情報」が含まれる項(第1, 2, 3, 5, 7, 11, 13, 15, 20, 28, 37, 39, 48, 53, 57, 58, 59, 63, 65, 66, 69, 73, 75, 76, 81, 83, 84, 86, 87, 91, 92, 96, 106, 108, 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項) <照会ができる根拠規定> 該当なし
7. 評価実施機関における担当部署	
①部署	市民部市民課
②所属長の役職名	市民部市民課長
8. 他の評価実施機関	

(別添1) 事務の内容

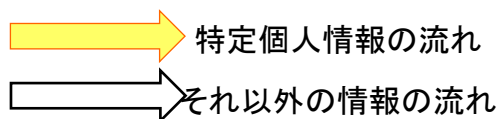
添付資料のとおり

(備考)

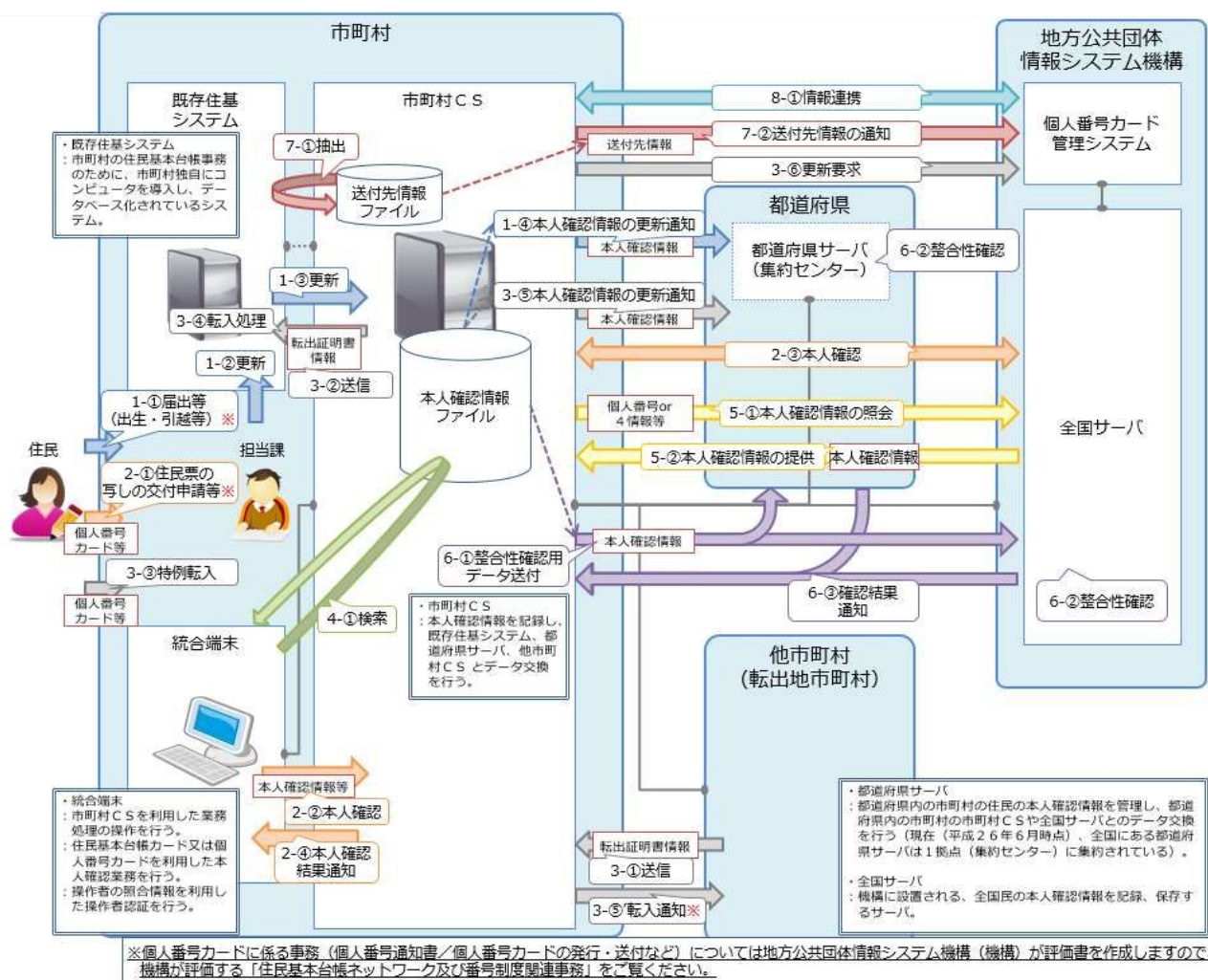
(別添1) 事務の内容



(備考)



(別添1) 事務の内容



(注) 図中に※が付されている箇所は、特定個人情報を含まない事務の流れを指す。

(備考)

上記図は、市町村CSと機構を中心とした事務の流れである。上図の「市区町村」は「町田市」、「市区町村CS」(以下、市町村CSという。)は「町田市CS」を表している。

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)。
- 2-②③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市町村CSから既存住基システムに転出証明書情報を送信する。
- 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、個人番号又は基本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、個人番号又は基本4情報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。

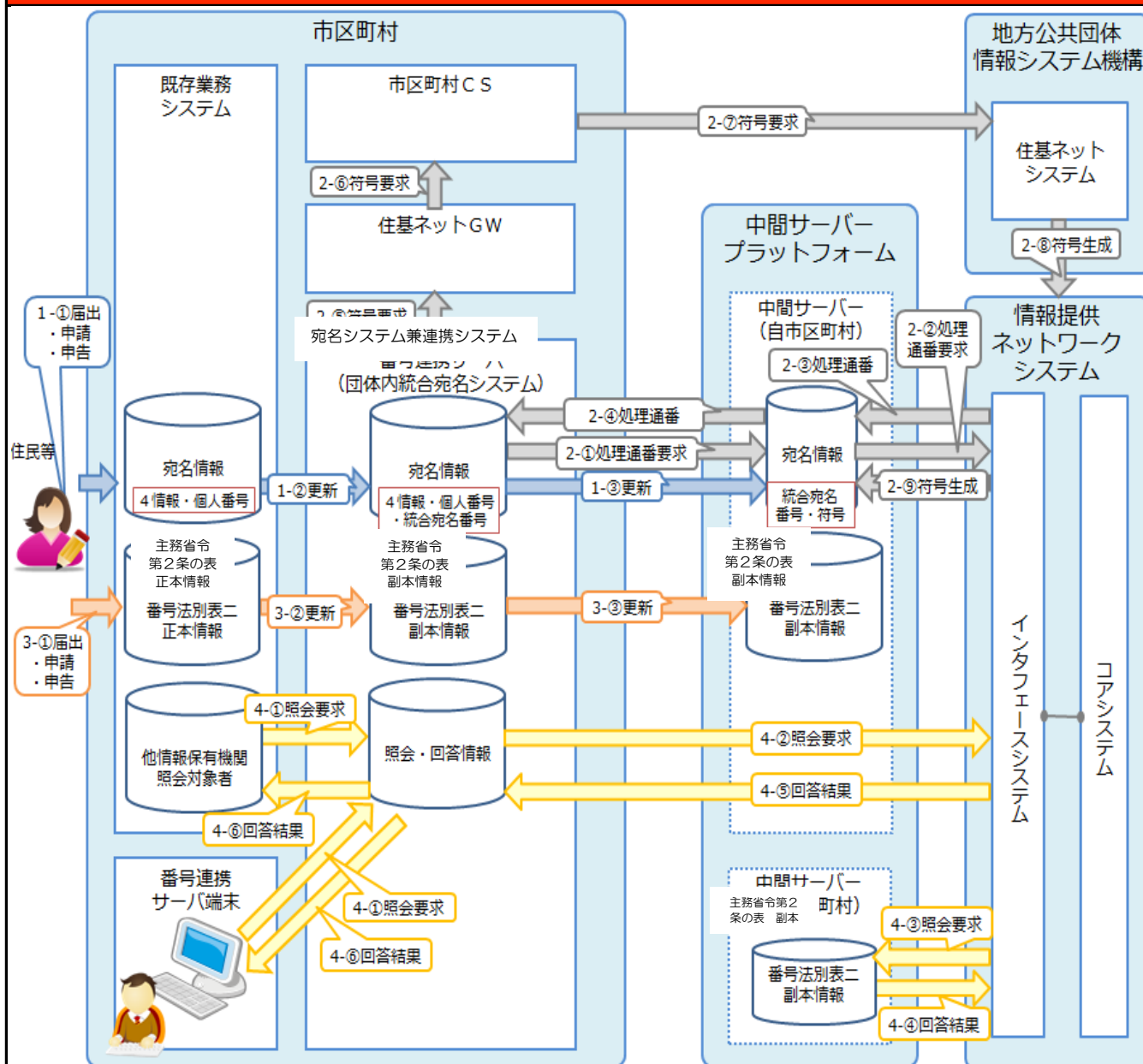
7. 送付先情報通知に関する事務

- 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。

(別添1) 事務の内容



(備考)

上記図は、特定の個人に関する市町村が保有する情報を中間サーバーに格納し符号を付番する仕組みと、中間サーバーを通じて情報提供ネットワークシステムと連携する仕組みを記述したものである。

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 ※	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	住基法第7条の住民基本台帳の記載事項であるため。 番号法第7条、第17条による個人番号の指定及び通知、個人番号カードの交付を行う上で必要となるため。
④記録される項目	[100項目以上] <選択肢> 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
主な記録項目 ※	・識別情報 [☐] 個人番号 [☐] 個人番号対応符号 [☐] その他識別情報(内部番号) ・連絡先等情報 [☐] 4情報(氏名、性別、生年月日、住所) [☐] 連絡先(電話番号等) [☐] その他住民票関係情報 ・業務関係情報 [☐] 国税関係情報 [☐] 地方税関係情報 [☐] 健康・医療関係情報 [☐] 医療保険関係情報 [☐] 児童福祉・子育て関係情報 [☐] 障害者福祉関係情報 [☐] 生活保護・社会福祉関係情報 [☐] 介護・高齢者福祉関係情報 [☐] 雇用・労働関係情報 [☐] 年金関係情報 [☐] 学校・教育関係情報 [☐] 災害関係情報 [☐] その他 (戸籍に関する情報、外国人住民に関する情報)
その妥当性	住基法第7条において住民票の記載事項と規定されているため。
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21日
⑥事務担当部署	市民部市民課・忠生市民センター・鶴川市民センター・南市民センター・なるせ駅前市民センター・堺市民センター・小山市民センター

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 ☐ 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 (行政機関・独立行政法人等)	
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システム、LGWAN等、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、町田市の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 ※		住民基本台帳法に基づき住民基本台帳に記載するため。	
変更の妥当性		届出により変更する場合がある。	
⑦使用の主体	使用部署 ※	市民部市民課・忠生市民センター・鶴川市民センター・南市民センター・なるせ駅前市民センター・堺市民センター・小山市民センター	
	使用者数	[100人以上500人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
⑧使用方法 ※		・住民基本台帳の記載 ・住民基本台帳の修正 ・住民基本台帳の消除 ・住民基本台帳に基づく住民票の写しの発行 ・個人番号の指定と個人番号通知書の発行 ・個人番号カードの発行 ・住民基本台帳ネットワークシステムによる本人確認情報の送信、個人番号の取得、符号の取得要求及び通知カード送付先情報	
情報の突合 ※		・通知カード、個人番号カード等により、正確な本人確認を行う。 ・住民票コードにより、正確な記録を行う。	
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 ※		—	
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 (5) 件
委託事項1		既存住基システムの保守業務
①委託内容		当該システムを安定的に使用するため、障害対応や法改正対応等によるシステムの構成変更対応等を実施する。
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 ※	特定個人情報ファイルの範囲と同様
	その妥当性	システムの安定した稼働のため、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人以上50人未満 <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法		専用線 電子メール 電子記録媒体(フラッシュメモリを除く。) フラッシュメモリ 紙 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) ○ その他 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		町田市情報公開条例に基づき情報提供している。
⑥委託先名		富士通Japan株式会社 多摩支店
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	原則、業務の全部または一部を第三者に再委託してはならない。ただし、必要不可欠な場合は、情報セキュリティ確保・個人情報保護のための特記仕様書に基づき、委託先が再委託承認申請書にて申請し、市が再委託を認めた上で、再委託承認書を送付する。
	⑨再委託事項	上記、再委託承認書の内容による。

委託事項2～5		
委託事項2	既存住基システムの運用業務	
①委託内容	当該システムを効率的に使用するため、稼働監視を実施する。	
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] 対象となる本人の数 対象となる本人の範囲 ※ その妥当性 <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 <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 特定個人情報ファイルの範囲と同様である。 システムの安定した稼働のため、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 原則、特定個人情報ファイルの提供は行わず、障害等の緊急時のみ、担当 [○] その他 (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)	
⑤委託先名の確認方法	町田市情報公開条例に基づき情報提供している。	
⑥委託先名	株式会社 エヌ・ティ・ティ・データ	
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	原則、業務の全部または一部を第三者に再委託してはならない。ただし、必要不可欠な場合は、情報セキュリティ確保・個人情報保護のための特記仕様書に基づき、委託先が再委託承認申請書にて申請し、市が再委託を認めた上で、再委託承認書を送付する。
	⑨再委託事項	上記、再委託承認書の内容による。

委託事項3		外部記録媒体保管業務
①委託内容		当該システムのバックアップデータを保存した外部記録媒体を遠隔地に保管する。
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] 対象となる本人の数 対象となる本人の範囲 ※ その妥当性 <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 <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 ()
⑤委託先名の確認方法		町田市情報公開条例に基づき情報提供している。
⑥委託先名		株式会社 ワンビシアーカイズ
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	原則、業務の全部または一部を第三者に再委託してはならない。ただし、必要不可欠な場合は、情報セキュリティ確保・個人情報保護のための特記仕様書に基づき、委託先が再委託承認申請書にて申請し、市が再委託を認めた上で、再委託承認書を送付する。
	⑨再委託事項	上記、再委託承認書の内容による。

委託事項4		証明書等のコンビニ交付システムの保守業務
①委託内容		当該システムを安定的に使用するため、障害対応や法改正対応等によるシステムの構成変更対応等を実施する。
②取扱いを委託する特定個人情報ファイルの範囲		<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 [特定個人情報ファイルの全体]
	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 [10万人以上100万人未満]
	対象となる本人の範囲 ※	特定個人情報ファイルの範囲と同様である。
	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		<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 [10人未満]
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 原則、特定個人情報ファイルの提供は行わず、障害等の緊急時のみ、担当 [○] その他 (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		町田市情報公開条例に基づき情報提供している。
⑥委託先名		富士フイルムシステムサービス株式会社
再委託	⑦再委託の有無 ※	<選択肢> 1) 再委託する 2) 再委託しない [再委託する]
	⑧再委託の許諾方法	原則、業務の全部または一部を第三者に再委託してはならない。ただし、必要不可欠な場合は、情報セキュリティ確保・個人情報保護のための特記仕様書に基づき、委託先が再委託承認申請書にて申請し、市が再委託を認めた上で、再委託承認書を送付する。
	⑨再委託事項	上記、再委託承認書の内容による。
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 (62) 件 ☒ 移転を行っている (18) 件 ☐ 行っていない
提供先1	番号法第19条第8号に基づく主務省令第2条の表に定める情報照会者(別表1を参照)
①法令上の根拠	番号法第19条第8号に基づく主務省令第2条の表
②提供先における用途	番号法第19条第8号に基づく主務省令第2条の表で規定された事務
③提供する情報	番号法第19条第8号に基づく主務省令第2条の表で規定された情報の範囲
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	特定個人情報ファイルの範囲と同様
⑥提供方法	☒ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	情報提供ネットワークシステムを通じて特定個人情報の提供照会があった都度、提供する。
提供先2～5	
提供先2	学校教育部保健給食課
①法令上の根拠	番号法第9条第1項別表に定める事務
②提供先における用途	災害共済給付事務
③提供する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
④提供する情報の対象となる本人の数	☐ 10万人以上100万人未満 <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	特定個人情報ファイルの範囲と同様
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 (宛名システム兼連携システム ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	住民基本台帳ファイルの更新の都度、提供する。

提供先3	学校教育部学務課	
①法令上の根拠	番号法第9条第1項別表に定める事務	
②提供先における用途	就学援助費支給事務	
③提供する情報	住所、氏名、生年月日、性別等の住民基本台帳情報	
④提供する情報の対象となる本人の数	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上	
⑤提供する情報の対象となる本人の範囲	特定個人情報ファイルの範囲と同様	
⑥提供方法	[] 情報提供ネットワークシステム [] 電子メール [] フラッシュメモリ [○] その他 （ 宛名システム兼連携システム ） [] 専用線 [] 電子記録媒体（フラッシュメモリを除く。） [] 紙	
⑦時期・頻度	住民基本台帳ファイルの更新の都度、提供する。	
提供先6～10		
提供先11～15		
提供先16～20		
移転先1	いきいき生活部介護保険課	
①法令上の根拠	番号法第9条第1項別表に定める事務	
②移転先における用途	介護保険事務	
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報	
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	特定個人情報ファイルの範囲と同様	
⑥移転方法	[] 庁内連携システム [] 電子メール [] フラッシュメモリ [○] その他 （ 宛名システム兼連携システム ） [] 専用線 [] 電子記録媒体（フラッシュメモリを除く。） [] 紙	
⑦時期・頻度	住民基本台帳ファイルの更新の都度、移転する。	

移転先2～5	
移転先2	保健所保健予防課
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	予防接種事務
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
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	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 （宛名システム兼連携システム） ☐ 専用線 ☐ 電子記録媒体（フラッシュメモリを除く。） ☐ 紙
⑦時期・頻度	住民基本台帳ファイルの更新の都度、移転する。
移転先3	
保健所保健予防課	
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	母子保健事務
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
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	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 （宛名システム兼連携システム） ☐ 専用線 ☐ 電子記録媒体（フラッシュメモリを除く。） ☐ 紙
⑦時期・頻度	住民基本台帳ファイルの更新の都度、移転する。

移転先4	保健所保健総務課、保健所健康推進課、保健所保健予防課
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	健康増進事務
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
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	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙 (宛名システム兼連携システム)
⑦時期・頻度	住民基本台帳ファイルの更新の都度、移転する。
移転先5	保健所保健予防課
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	保健所事務(養育医療)
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
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	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙 (宛名システム兼連携システム)
⑦時期・頻度	事務処理の必要に応じて随時、移転する。

移転先6～10	
移転先6	いきいき生活部保険年金課
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	国民健康保険事務
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
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	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙 (宛名システム兼連携システム)
⑦時期・頻度	住民基本台帳ファイルの更新の都度、移転する。
移転先7	
いきいき生活部保険年金課	
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	後期高齢医療事務
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
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	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙 (宛名システム兼連携システム)
⑦時期・頻度	住民基本台帳ファイルの更新の都度、移転する。

移転先8	いきいき生活部保険年金課
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	国民年金事務
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
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	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙 (宛名システム兼連携システム)
⑦時期・頻度	住民基本台帳ファイルの更新の都度、移転する。
移転先9	子ども生活部子育て推進課
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	災害共済給付事務
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
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	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙 (宛名システム兼連携システム)
⑦時期・頻度	住民基本台帳ファイルの更新の都度、移転する。

移転先10	子ども生活部子ども家庭支援課
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	母子福祉基金貸付事務
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
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	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙 (宛名システム兼連携システム)
⑦時期・頻度	住民基本台帳ファイルの更新の都度、移転する。
移転先11～15	
移転先11	子ども生活部子ども総務課
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	児童福祉事務
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
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	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙 (宛名システム兼連携システム)
⑦時期・頻度	住民基本台帳ファイルの更新の都度、移転する。

移転先12	子ども生活部保育・幼稚園課、子ども生活部児童青少年課
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	子ども・子育て支援事務
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
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	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙 (宛名システム兼連携システム)
⑦時期・頻度	住民基本台帳ファイルの更新の都度、移転する。
移転先13	財務部市民税課、財務部資産税課、財務部納税課
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	地方税務事務
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
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	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙 (宛名システム兼連携システム)
⑦時期・頻度	住民基本台帳ファイルの更新の都度、移転する。

移転先14	地域福祉部障がい福祉課
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	障害福祉事務
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
④移転する情報の対象となる本人の数	☐ 100万人以上1,000万人未満 <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	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 （宛名システム兼連携システム） ☐ 専用線 ☐ 電子記録媒体（フラッシュメモリを除く。） ☐ 紙
⑦時期・頻度	住民基本台帳ファイルの更新の都度、移転する。
移転先15	地域福祉部生活援護課
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	生活保護事務
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
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	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 （宛名システム兼連携システム） ☐ 専用線 ☐ 電子記録媒体（フラッシュメモリを除く。） ☐ 紙
⑦時期・頻度	住民基本台帳ファイルの更新の都度、移転する。

移転先16～20	
移転先16	都市づくり部住宅課
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	公営住宅入居者管理事務
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
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 [10万人以上100万人未満]
⑤移転する情報の対象となる本人の範囲	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 ☐ 専用線 ☐ 電子記録媒体（フラッシュメモリを除く。） ☐ 紙 （ 端末で既存住基システムを参照 ）
⑦時期・頻度	事務処理の必要に応じて随時、移転する。
移転先17	子ども生活部子ども家庭支援課
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	児童相談関係事務
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
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 [10万人以上100万人未満]
⑤移転する情報の対象となる本人の範囲	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 ☐ 専用線 ☐ 電子記録媒体（フラッシュメモリを除く。） ☐ 紙 （ 宛名システム兼連携システム ）
⑦時期・頻度	住民基本台帳ファイルの更新の都度、移転する。

移転先18	学校教育部学務課
①法令上の根拠	番号法第9条第1項別表に定める事務
②移転先における用途	学校保健法による医療に要する費用についての援助に関する事務
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
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	特定個人情報ファイルの範囲と同様
⑥移転方法	☐ 庁内連携システム ☐ 専用線 ☐ 電子メール ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ フラッシュメモリ ☐ 紙 ☒ その他 (宛名システム兼連携システム)
⑦時期・頻度	住民基本台帳ファイルの更新の都度、移転する。

6. 特定個人情報の保管・消去		
①保管場所 ※		<事務室における措置> 町田市情報セキュリティポリシーにより規定 ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・立ち入りを承認する場合は入退管理をしている。 ・入退室管理簿を記載している。 ・来客者用名札を着用させている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)の使用または鍵付キャビネットへの保管を行っている。 <中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームはデータセンターに設置している。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ②特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。 <ガバメントクラウドにおける措置> ①サーバー等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAP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。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本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	<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 [定められていない]
	その妥当性	現存者については消去しない。住民基本台帳法に基づき、消除者については、消除後150年経過後に消去する。
③消去方法		・データベースに記録されたデータのうち、法定保存年限を経過したデータをシステムにて判別し消去する。 町田市情報セキュリティポリシーにより規定 ・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。 ・紙媒体は、シュレッダーによる破碎、溶解、焼却等の情報の復元不能化処理を行っている。 <中間サーバー・プラットフォームにおける措置> ①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、物理的破壊または専用ソフト等を利用して完全に消去する。 <ガバメントクラウドにおける措置> 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。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。 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等に当たって確実にデータを消去する。 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。この移行に際しては、システム基盤運用事業者がデータ抽出及び利用しなくなった環境の消去等を実施し、開発事業者がクラウド環境へのデータ投入等を実施する。
7. 備考		

(別表1) 番号法第19条第8号に基づく主務省令第2条の表に定める情報照会者

別表のうち、情報提供者が市町村長、かつ、特定個人情報に住民票関係情報が含まれるもの、を抜粋しています。

項番	項番 (別表2)	情報照会者	事務	情報提供者	特定個人情報
1	1	一 厚生労働大臣	健康保険法第五条第二項の規定により厚生労働大臣が行うこととされた健康保険に関する事務であって主務省令で定めるもの	市町村長	地方税法その他の地方税に関する法律に基づく条例の規定により算定した税額若しくはその算定の基礎となる事項に関する情報（以下「地方税関係情報」という。）、住民基本台帳法第七条第四号に規定する事項（以下「住民票関係情報」という。）、又は介護保険法による保険給付の支給若しくは保険料の徴収に関する情報（以下「介護保険給付関係情報」という。）であって主務省令で定めるもの
2	2	二 全国健康保険協会	健康保険法による保険給付の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報、住民票関係情報又は介護保険給付関係情報であって主務省令で定めるもの
3	3	三 健康保険組合	健康保険法による保険給付の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報、住民票関係情報又は介護保険給付関係情報であって主務省令で定めるもの
4	5	五 厚生労働大臣	船員保険法第四条第二項の規定により厚生労働大臣が行うこととされた船員保険に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報、住民票関係情報又は介護保険給付関係情報であって主務省令で定めるもの
5	7	七 全国健康保険協会	船員保険法による保険給付又は平成十九年法律第三十号附則第三十九条の規定によりなお従前の例によるものとされた平成十九年法律第三十号第四条の規定による改正前の船員保険法による保険給付の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報、住民票関係情報又は介護保険給付関係情報であって主務省令で定めるもの
6	11	十一 都道府県知事	児童福祉法による里親の認定、養育里親の登録又は障害児入所給付費、高額障害児入所給付費若しくは特定入所障害児食費等給付費の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
7	13	十三 都道府県知事	児童福祉法による小児慢性特定疾病医療費の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
8	15	十五 市町村長	児童福祉法による障害児通所給付費、特例障害児通所給付費、高額障害児通所給付費、障害児相談支援給付費若しくは特例障害児相談支援給付費の支給又は障害福祉サービスの提供に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
9	20	二十 都道府県知事又は市町村長	児童福祉法による負担能力の認定又は費用の徴収に関する事務であって主務省令で定めるもの	市町村長	児童福祉法による障害児通所支援に関する情報、地方税関係情報、住民票関係情報又は障害者の日常生活及び社会生活を総合的に支援するための法律による自立支援給付の支給に関する情報であって主務省令で定めるもの
10	28	二十八 市町村長	予防接種法による給付の支給又は実費の徴収に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
11	37	三十七 市町村長	身体障害者福祉法による障害福祉サービス、障害者支援施設等への入所等の措置又は費用の徴収に関する事務であって主務省令で定めるもの	市町村長	住民票関係情報であって主務省令で定めるもの
12	39	三十九 都道府県知事	精神保健及び精神障害者福祉に関する法律による入院措置又は費用の徴収に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
13	48	四十八 市町村長	地方税法その他の地方税に関する法律及びこれらの法律に基づく条例による地方税の賦課徴収に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
14	53	五十三 公営住宅法第二条第十六号に規定する事業主体である都道府県知事又は市町村長	公営住宅法による公営住宅の管理に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
15	57	五十七 日本私立学校振興・共済事業団	私立学校教職員共済法による短期給付又は年金である給付の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの

項番	項番 (別表2)	情報照会者	事務	情報提供者	特定個人情報
16	58	五十八 厚生労働大臣 又は共済組合等	厚生年金保険法による年金である保険給付又は一時金の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
17	59	五十九 文部科学大臣 又は都道府県教育委員会	特別支援学校への就学奨励に関する法律による特別支援学校への就学のために必要な経費の支弁に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
18	63	六十三 都道府県教育委員会又は市町村教育委員会	学校保健安全法による医療に要する費用についての援助に関する事務であって主務省令で定めるもの	市町村長	住民票関係情報であって主務省令で定めるもの
19	65	六十五 国家公務員共済組合	国家公務員共済組合法による短期給付の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報、住民票関係情報又は介護保険給付関係情報であって主務省令で定めるもの
20	66	六十六 国家公務員共済組合連合会	国家公務員共済組合法又は国家公務員共済組合法の長期給付に関する施行法による年金である給付の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
21	69	六十九 市町村長又は国民健康保険組合	国民健康保険法による保険給付の支給又は保険料の徴収に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報、住民票関係情報又は介護保険給付関係情報であって主務省令で定めるもの
22	73	七十三 厚生労働大臣	国民年金法による年金である給付若しくは一時金の支給、保険料の納付に関する処分又は保険料その他徴収金の徴収に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
23	75	七十五 市町村長	知的障害者福祉法による障害福祉サービス、障害者支援施設等への入所等の措置又は費用の徴収に関する事務であって主務省令で定めるもの	市町村長	住民票関係情報であって主務省令で定めるもの
24	76	七十六 住宅地区改良法第二条第二項に規定する施行者である都道府県知事又は市町村長	住宅地区改良法による改良住宅の管理若しくは家賃若しくは敷金の決定若しくは変更又は収入超過者に対する措置に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
25	81	八十一 都道府県知事等	児童扶養手当法による児童扶養手当の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報、住民票関係情報又は障害者の日常生活及び社会生活を総合的に支援するための法律による療養介護若しくは施設入所支援に関する情報であって主務省令で定めるもの
26	83	八十三 地方公務員共済組合	地方公務員等共済組合法による短期給付の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報、住民票関係情報又は介護保険給付関係情報であって主務省令で定めるもの
27	84	八十四 地方公務員共済組合又は全国市町村職員共済組合連合会	地方公務員等共済組合法又は地方公務員等共済組合法の長期給付等に関する施行法による年金である給付の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
28	86	八十六 市町村長	老人福祉法による福祉の措置に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報、住民票関係情報又は介護保険給付関係情報であって主務省令で定めるもの
29	87	八十七 市町村長	老人福祉法による費用の徴収に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報、住民票関係情報又は介護保険給付関係情報であって主務省令で定めるもの
30	91	九十一 厚生労働大臣又は都道府県知事	特別児童扶養手当等の支給に関する法律による特別児童扶養手当の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
31	92	九十二 都道府県知事等	特別児童扶養手当等の支給に関する法律による障害児福祉手当若しくは特別障害者手当又は昭和六十年法律第三十四号附則第九十七条第一項の福祉手当の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
32	96	九十六 市町村長	母子保健法による費用の徴収に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの

項番	項番 (別表2)	情報照会者	事務	情報提供者	特定個人情報
33	106	百六 市町村長（児童手当法第十七条第一項の表の下欄に掲げる者を含む）	児童手当法による児童手当又は特例給付の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
34	108	百八 市町村長	災害弔慰金の支給等に関する法律（昭和四十八年法律第八十二号）による災害弔慰金若しくは災害障害見舞金の支給又は災害援護資金の貸付けに関する事務であって第百十条で定めるもの	市町村長	地方税関係情報、住民票関係情報又は介護保険給付関係情報であって主務省令で定めるもの
35	110	百十 厚生労働大臣	雇用保険法による未支給の失業等給付又は介護休業給付金の支給に関する事務であって主務省令で定めるもの	市町村長	住民票関係情報であって主務省令で定めるもの
36	112	百十二 厚生労働大臣	雇用保険法による育児休業等給付の支給に関する事務であって主務省令で定めるもの	市町村長	母子保健法による妊娠の届出に関する情報又は住民票関係情報であって主務省令で定めるもの
37	115	百十五 後期高齢者医療広域連合	高齢者の医療の確保に関する法律による後期高齢者医療給付の支給又は保険料の徴収に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報、住民票関係情報又は介護保険給付関係情報であって主務省令で定めるもの
38	118	百十八 厚生労働大臣	昭和六十年法律第三十四号附則第八十七条第二項の規定により厚生年金保険の実施者たる政府が支給するものとされた年金である保険給付の支給に関する事務であって第百二十条で定めるもの	市町村長	住民票関係情報であって主務省令で定めるもの
39	124	百二十四 特定優良賃貸住宅の供給の促進に関する法律第十八条第二項に規定する賃貸住宅の建設及び管理を行う都道府県知事又は市町村長	特定優良賃貸住宅の供給の促進に関する法律による賃貸住宅の管理に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
40	129	百二十九 厚生労働大臣	平成八年法律第八十二号附則第十六条第三項の規定により厚生年金保険の実施者たる政府が支給するものとされた年金である給付の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
41	130	百三十一 平成八年法律第八十二号附則第三十二条第二項に規定する存続組合又は平成八年法律第八十二号附則第四十八条第一項に規定する指定基金	平成八年法律第八十二号による年金である長期給付又は年金である給付の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
42	132	百三十二 市町村長	介護保険法による保険給付の支給又は保険料の徴収に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報、住民票関係情報又は介護保険給付関係情報であって主務省令で定めるもの
43	136	百三十六 都道府県知事	被災者生活再建支援法による被災者生活再建支援金の支給に関する事務であって主務省令で定めるもの	市町村長	住民票関係情報であって主務省令で定めるもの
44	137	百三十七 都道府県知事又は保健所を設置する市（特別区を含む。）の長	感染症の予防及び感染症の患者に対する医療に関する法律（平成十年法律第一百四十四号）による費用の負担又は療養費の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
45	138	百三十八 厚生労働大臣	厚生年金保険制度及び農林漁業団体職員共済組合制度の統合を図るための農林漁業団体職員共済組合法等を廃止する等の法律附則第十六条第三項の規定により厚生年金保険の実施者たる政府が支給するものとされた年金である給付の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの

項番	項番 (別表2)	情報照会者	事務	情報提供者	特定個人情報
46	141	百四十一 独立行政法人日本学生支援機構	独立行政法人日本学生支援機構法による学資の貸与に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
47	142	百四十二 厚生労働大臣	特定障害者に対する特別障害給付金の支給に関する法律による特別障害給付金の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
48	144	百四十四 都道府県知事又は市町村長	障害者の日常生活及び社会生活を総合的に支援するための法律による自立支援給付の支給又は地域生活支援事業の実施に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
49	149	百四十九 厚生労働大臣	厚生年金保険の保険給付及び国民年金の給付に係る時効の特例等に関する法律による保険給付又は給付の支給に関する事務であって主務省令で定めるもの	市町村長	住民票関係情報であって主務省令で定めるもの
50	150	百五十 厚生労働大臣	厚生年金保険の保険給付及び国民年金の給付の支払の遅延に係る加算金の支給に関する法律による保険給付遅延特別加算金又は給付遅延特別加算金の支給に関する事務であって主務省令で定めるもの	市町村長	住民票関係情報であって主務省令で定めるもの
51	151	百五十一 文部科学大臣、都道府県知事又は都道府県教育委員会	高等学校等就学支援金の支給に関する法律による就学支援金の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
52	152	百五十二 厚生労働大臣	職業訓練の実施等による特定求職者の就職の支援に関する法律による職業訓練受講給付金の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
53	155	百五十五 市町村長	子ども・子育て支援法による子どものための教育・保育給付の支給又は地域子ども・子育て支援事業の実施に関する事務であって主務省令で定めるもの	市町村長	児童福祉法による障害児通所支援に関する情報、地方税関係情報、住民票関係情報又は障害者の日常生活及び社会生活を総合的に支援するための法律による自立支援給付の支給に関する情報であって主務省令で定めるもの
54	156	百五十六 厚生労働大臣	年金生活者支援給付金の支給に関する法律による年金生活者支援給付金の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報、住民票関係情報又は介護保険給付関係情報であって主務省令で定めるもの
55	158	百五十八 都道府県知事	難病の患者に対する医療等に関する法律による特定医療費の支給に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
56	160	百六十 公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律第十条に規定する特定公的給付の支給を実施する行政機関の長等（行政機関の長、地方公共団体の機関、独立行政法人等、地方独立行政法人（地方独立行政法人法（平成十五年法律第百十八号）第二条第一項に規定する地方独立行政法人をいう。））	公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律による特定公的給付の支給を実施するための基礎とする情報の管理に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの

項番	項番 (別表2)	情報照会者	事務	情報提供者	特定個人情報
57	163	百六十三 地域優良賃貸住宅制度要綱（平成十九年三月二十八日付け国住備第百六十号国土交通省住宅局長通知）第二条第九号に規定する地域優良賃貸住宅（公共供給型）又は同条第十六号に規定する公営型地域優良賃貸住宅（公共供給型）の供給を行う都道府県知事又は市町村長	地域優良賃貸住宅制度要綱に基づく地域優良賃貸住宅の管理に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
58	164	百六十四 都道府県知事	「特定感染症検査等事業について」（平成十四年三月二十七日付け健発第〇三二七〇一〇二号厚生労働省健康局長通知）の特定感染症検査等事業実施要綱に基づくウイルス性肝炎患者等の重症化予防推進事業に係る陽性者フォローアップ事業の実施に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
59	165	百六十五 都道府県知事	「感染症対策特別促進事業について」（平成二十年三月三十一日付け健発第〇三三一〇〇一〇号厚生労働省健康局長通知）の肝炎治療特別促進事業実施要綱に基づく肝炎治療特別促進事業の実施に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
60	166	百六十六 都道府県知事	「肝がん・重度肝硬変治療研究促進事業について」（平成三十年六月二十七日付け健発第〇六二七第一号厚生労働省健康局長通知）の肝がん・重度肝硬変治療研究促進事業実施要綱に基づく肝がん・重度肝硬変治療研究促進事業の実施に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの

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 [○] 4情報(氏名、性別、生年月日、住所) [] 連絡先(電話番号等) [○] その他住民票関係情報 ・業務関係情報 [] 国税関係情報 [] 地方税関係情報 [] 健康・医療関係情報 [] 医療保険関係情報 [] 児童福祉・子育て関係情報 [] 障害者福祉関係情報 [] 生活保護・社会福祉関係情報 [] 介護・高齢者福祉関係情報 [] 雇用・労働関係情報 [] 年金関係情報 [] 学校・教育関係情報 [] 災害関係情報 [] その他 ()
その妥当性	・個人番号、4情報、その他住民票関係情報 :住基ネットを通じて本人確認を行うために必要な情報として、住民票の記載等に係る本人確認情報(個人番号、4情報、住民票コード及びこれらの変更情報)を記録する必要があるため。
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21日
⑥事務担当部署	市民部市民課・忠生市民センター・鶴川市民センター・南市民センター・なるせ駅前市民センター・堺市民センター・小山市民センター

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 ☐ 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 (市民部市民課・忠生市民センター・鶴川市民センター・南市民センター・なるせ駅前市民センター・堺市民センター・小山市民センター)	
②入手方法	☐ 紙 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ フラッシュメモリ ☐ 電子メール ☐ 専用線 ☐ 庁内連携システム ☐ 情報提供ネットワークシステム ☒ その他 (既存住基システム)	
③入手の時期・頻度	住民基本台帳の記載事項において、本人確認情報に係る変更又は新規作成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6-6(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・忠生市民センター・鶴川市民センター・南市民センター・なるせ駅前市民センター・堺市民センター・小山市民センター
	使用者数	100人以上500人未満 <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
⑧使用方法 ※	・住民票の記載事項の変更又は新規作成が生じた場合、既存住基システムから当該本人確認情報の更新情報を受領し(既存住基システム→市町村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)。 ・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)。 ・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(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。 ・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 ※	—
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 ☐ 委託しない ☐ 1) 委託する ☐ 2) 委託しない ☐ 3) 件
委託事項1	既存住基システムの保守業務
①委託内容	当該システムを安定的に使用するため、障害対応や法改正対応等によるシステムの構成変更対応等を実施する。
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 ☐ 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 ☐ 1万人未満 ☐ 1万人以上10万人未満 ☐ 10万人以上100万人未満 ☐ 100万人以上1,000万人未満 ☐ 1,000万人以上
対象となる本人の範囲 ※	特定個人情報ファイルの範囲と同様
その妥当性	システムの安定した稼働のため、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人以上50人未満 ☐ 10人未満 ☐ 10人以上50人未満 ☐ 50人以上100人未満 ☐ 100人以上500人未満 ☐ 500人以上1,000人未満 ☐ 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 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	町田市情報公開条例に基づき情報提供している。
⑥委託先名	株式会社 エヌ・ティ・ティ・データ
再委託	☐ 再委託する ☐ 再委託しない
⑦再委託の有無 ※	☐ 再委託する ☐ 再委託しない
⑧再委託の許諾方法	原則、業務の全部または一部を第三者に再委託してはならない。ただし、必要不可欠な場合は、情報セキュリティ確保・個人情報保護のための特記仕様書に基づき、委託先が再委託承認申請書にて申請し、市が再委託を認めた上で、再委託承認書を送付する。
⑨再委託事項	上記、再委託承認書の内容による。

委託事項2～5					
委託事項2		既存住基システムの運用業務			
①委託内容		当該システムを効率的に使用するため、稼働監視を実施する。			
②取扱いを委託する特定個人情報ファイルの範囲		＜選択肢＞ [特定個人情報ファイルの全体] 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		＜選択肢＞ [10万人以上100万人未満] 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 ※		特定個人情報ファイルの範囲と同様である。			
その妥当性		システムの安定した稼働のため、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		＜選択肢＞ [10人未満] 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 原則特定個人情報ファイルの提供は行わず、障害等の緊急時のみ、担当 [○] その他 (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		町田市情報公開条例に基づき情報提供している。			
⑥委託先名		株式会社 エヌ・ティ・ティ・データ			
再委託	⑦再委託の有無 ※	＜選択肢＞ [再委託する] 1) 再委託する 2) 再委託しない			
	⑧再委託の許諾方法	原則、業務の全部または一部を第三者に再委託してはならない。ただし、必要不可欠な場合は、情報セキュリティ確保・個人情報保護のための特記仕様書に基づき、委託先が再委託承認申請書にて申請し、市が再委託を認めた上で、再委託承認書を送付する。			
	⑨再委託事項	上記、再委託承認書の内容による。			

委託事項3		外部記録媒体保管業務
①委託内容		当該システムのバックアップデータを保存した外部記録媒体を遠隔地に保管する。
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 ※	特定個人情報ファイルの範囲と同様である。
	その妥当性	火災、震災等によりシステムのデータが消滅した場合、データ復旧を行うにあたって特定個人情報ファイル全体を保管の対象にする必要がある。
③委託先における取扱者数		[10人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法		[] 専用線 [] 電子メール [○] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [] その他 ()
⑤委託先名の確認方法		町田市情報公開条例に基づき情報提供している。
⑥委託先名		株式会社 ワンビシアーカイズ
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	原則、業務の全部または一部を第三者に再委託してはならない。ただし、必要不可欠な場合は、情報セキュリティ確保・個人情報保護のための特記仕様書に基づき、委託先が再委託承認申請書にて申請し、市が再委託を認めた上で、再委託承認書を送付する。
	⑨再委託事項	上記、再委託承認書の内容による。
委託事項6～10		
委託事項11～15		
委託事項16～20		

5. 特定個人情報の提供・移転(委託に伴うものを除く。)	
提供・移転の有無	☐ 提供を行っている (2) 件 ☐ 移転を行っている () 件 ☐ 行っていない
提供先1	都道府県
①法令上の根拠	住基法第30条の6(市町村長から都道府県知事への本人確認情報の通知等)
②提供先における用途	・市町村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。 ・住基法に基づいて、本人確認情報の提供及び利用等を行う。
③提供する情報	住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日
④提供する情報の対象となる本人の数	<選択肢> ☐ 10万人以上100万人未満 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	住民基本台帳へ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(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	<選択肢> ☐ 10万人以上100万人未満 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	
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	
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 ※		＜事務室における措置＞ 町田市情報セキュリティポリシーにより規定 ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・立ち入りを承認する場合は入退管理をしている。 ・入退室管理簿を記載している。 ・来客者用名札を着用させている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具（鍵付チェーン等）の使用または鍵付キャビネットへの保管を行っている。 ＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAP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。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本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	＜選択肢＞ <table><tr><td>1) 1年未満</td><td>2) 1年</td><td>3) 2年</td></tr><tr><td>4) 3年</td><td>5) 4年</td><td>6) 5年</td></tr><tr><td>7) 6年以上10年未満</td><td>8) 10年以上20年未満</td><td>9) 20年以上</td></tr><tr><td colspan="3">10) 定められていない</td></tr></table> [20年以上]	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		
	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		・本人確認情報ファイルに記録されたデータをシステムにて自動判別し消去する。 町田市情報セキュリティポリシーにより規定 ・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。 ・紙媒体は、シュレッダーによる破碎、溶解、焼却等の情報の復元不能化処理を行っている。 ＜ガバメントクラウドにおける措置＞ 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。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。 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。 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。この移行に際しては、システム基盤運用事業者がデータ抽出及び利用しなくなった環境の消去等を実施し、開発事業者がクラウド環境へのデータ投入等を実施する。												

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> 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)及び個人番号カード省令第7条(個人番号の通知)に基づき、個人番号通知書を個人番号の付番対象者全員に送付する必要がある。 また、通知カード所有者にあっては、個人番号カードは通知カードと引き換えに交付することとされている。機構は、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)に基づき、これらの事務を実施する。	
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 [☐] 4情報(氏名、性別、生年月日、住所) [☐] 連絡先(電話番号等) [☐] その他住民票関係情報 ・業務関係情報 [☐] 国税関係情報 [☐] 地方税関係情報 [☐] 健康・医療関係情報 [☐] 医療保険関係情報 [☐] 児童福祉・子育て関係情報 [☐] 障害者福祉関係情報 [☐] 生活保護・社会福祉関係情報 [☐] 介護・高齢者福祉関係情報 [☐] 雇用・労働関係情報 [☐] 年金関係情報 [☐] 学校・教育関係情報 [☐] 災害関係情報 [☐] その他 (個人番号通知書及び交付申請書の送付先情報)	
	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機構が行うために、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	市民部市民課・忠生市民センター・鶴川市民センター・南市民センター・なるせ駅前市民センター・堺市民センター・小山市民センター	

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 ☐ 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 (市民部市民課・忠生市民センター・鶴川市民センター・南市民センター・なるせ駅前市民センター・堺市民センター・小山市民センター)	
②入手方法		☐ 紙 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ フラッシュメモリ ☐ 電子メール ☐ 専用線 ☐ 庁内連携システム ☐ 情報提供ネットワークシステム ☒ その他 (既存住基システム)	
③入手の時期・頻度		個人番号通知書に係る送付先情報は、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) ※本人へ明示する場合には、明示方法について記載する。	
⑥使用目的 ※		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・忠生市民センター・鶴川市民センター・南市民センター・なるせ駅前市民センター・堺市民センター・小山市民センター	
	使用者数	[100人以上500人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
⑧使用方法 ※		・既存住基システムより個人番号の通知対象者の情報を抽出し、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)に基づいて行う機構に対し提供する(既存住基システム→市町村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 ※		—	
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 (3) 件
委託事項1		既存住基システムの保守業務
①委託内容		当該システムを安定的に使用するため、障害対応や法改正対応等によるシステムの構成変更対応等を実施する。
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 ※	特定個人情報ファイルの範囲と同様である。
	その妥当性	システムの安定した稼働のため、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人以上50人未満 <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法		専用線 電子メール 電子記録媒体(フラッシュメモリを除く。) フラッシュメモリ 紙 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) ○ その他 () 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		町田市情報公開条例に基づき情報提供している。
⑥委託先名		株式会社 エヌ・ティ・ティ・データ
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	原則、業務の全部または一部を第三者に再委託してはならない。ただし、必要不可欠な場合は、情報セキュリティ確保・個人情報保護のための特記仕様書に基づき、委託先が再委託承認申請書にて申請し、市が再委託を認めた上で、再委託承認書を送付する。
	⑨再委託事項	上記、再委託承認書の内容による。

委託事項2～5		
委託事項2	既存住基システムの運用業務	
①委託内容	当該システムを効率的に使用するため、稼動監視を実施する。	
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 ※	特定個人情報ファイルの範囲と同様である。	
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 原則、特定個人情報ファイルの提供は行わず、障害等の緊急時のみ、担当 [○] その他 (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	町田市情報公開条例に基づき情報提供している。	
⑥委託先名	株式会社 エヌ・ティ・ティ・データ	
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	原則、業務の全部または一部を第三者に再委託してはならない。ただし、必要不可欠な場合は、情報セキュリティ確保・個人情報保護のための特記仕様書に基づき、委託先が再委託承認申請書にて申請し、市が再委託を認めた上で、再委託承認書を送付する。
	⑨再委託事項	上記、再委託承認書の内容による。

委託事項3		外部記録媒体保管業務
①委託内容		当該システムのバックアップデータを保存した外部記録媒体を遠隔地に保管する。
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 ※	特定個人情報ファイルの範囲と同様である。
	その妥当性	火災、震災等によりシステムのデータが消滅した場合、データ復旧を行うにあたって特定個人情報ファイル全体を保管の対象にする必要がある。
③委託先における取扱者数		[10人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法		[] 専用線 [] 電子メール [○] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [] その他 ()
⑤委託先名の確認方法		町田市情報公開条例に基づき情報提供している。
⑥委託先名		株式会社 ワンビシアーカイズ
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	原則、業務の全部または一部を第三者に再委託してはならない。ただし、必要不可欠な場合は、情報セキュリティ確保・個人情報保護のための特記仕様書に基づき、委託先が再委託承認申請書にて申請し、市が再委託を認めた上で、再委託承認書を送付する。
	⑨再委託事項	上記、再委託承認書の内容による。
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(機構)
①法令上の根拠	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)
②提供先における用途	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)に基づき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. ④記録される項目」と同上。
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 (住民基本台帳ネットワーク) ☐ 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	個人番号通知書に係る送付先情報は、新たに個人番号の通知対象者が生じた都度提供する。
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	

[illegible]

6. 特定個人情報の保管・消去		
①保管場所 ※		<事務室における措置> 町田市情報セキュリティポリシーにより規定 ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・立ち入りを承認する場合は入退管理をしている。 ・入退室管理簿を記載している。 ・来客者用名札を着用させている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)の使用または鍵付キャビネットへの保管を行っている。 <ガバメントクラウドにおける措置> ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAP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。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本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	<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 [1年未満]
	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。 町田市情報セキュリティポリシーにより規定 ・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。 ・紙媒体は、シュレッダーによる破碎、溶解、焼却等の情報の復元不能化処理を行っている。 <ガバメントクラウドにおける措置> 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。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。 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等に当たって確実にデータを消去する。 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。この移行に際しては、システム基盤運用事業者がデータ抽出及び利用しなくなった環境の消去等を実施し、開発事業者がクラウド環境へのデータ投入等を実施する。
7. 備考		

(別添2) 特定個人情報ファイル記録項目

別紙「個人情報ファイル簿」のとおり

(別添2) 特定個人情報ファイル記録項目

個人情報ファイル簿

情報の収集元	住民基本台帳	
組織	部課名	業務の名称又は収集内容
町田市	財務部市民税課	市・都民税賦課
町田市	財務部資産税課	固定資産税・都市計画税賦課
町田市	財務部納税課	市税徴収（滞納整理） 国民健康保険税収納 国民健康保険税徴収（滞納）
町田市	市民部市民課	戸籍、住居表示戸番号付定
町田市	市民部市民課及び各市民センター	印鑑登録・証明、マイナンバー制度カード管理 在留管理 東日本大震災避難者支援（取りまとめ）
町田市	地域福祉部生活援護課	生活保護
町田市	いきいき生活部保険年金課	国民健康保険被保険者資格 国民健康保険税賦課、後期高齢者医療 国民年金資格、国民年金保険料
町田市	いきいき生活部介護保険課	介護保険被保険者管理、介護保険給付管理
町田市	子ども生活部子ども総務課	子ども手当 児童手当（2012年創設）
町田市	子ども生活部子ども家庭支援課	緊急一時保護宿泊費等助成事業
町田市	都市づくり部土地利用調整課	住居表示
町田市	都市づくり部地区街づくり課	区画整理事業（組合施行）指導 土地区画整理事業（市施行）実施
町田市	都市づくり部建築開発審査課	建築等確認審査
町田市	学校教育部学務課	就学
町田市	選挙管理委員会事務局	選挙
市区町村		住民票及び戸籍・戸籍の附票の記載通知に関する 情報、居住に関する情報
市区町村選挙管理委員会		在外選挙人名簿の登録
区画整理組合		土地の名称・地番変更に伴う新旧対照表、区画整 理区域内の土地・家屋所有者、居住者の確認
都市再生機構		土地の名称・地番変更に伴う新旧対照表、区画整 理区域内の土地・家屋所有者、居住者の確認
不動産所有者・管理者		住民実態調査対象者等の居住に関する情報
居住情報提供者		ストーカー行為又は暴力行為の被害
警察署		暴力行為の被害
配偶者暴力相談支援センター		暴力行為の被害
児童相談所		暴力行為の被害
東京都水道局		水道料金業務
出入国在留管理庁		在留管理業務、出入国記録
東京法務局町田出張所		土地・家屋の所有者の確認
東京都および地方公共団体情報シ ステム機構		本人確認情報管理

個人情報ファイル簿

2025年1月27日時点

1	個人情報ファイルの名称	住民基本台帳	備考
2	行政機関の名称	町田市	
3	個人情報ファイルが利用に供される事務をつかさどる組織の名称	市民部市民課	
3	個人情報ファイルが利用に供される事務をつかさどる組織の名称	市民部南市民センター	
3	個人情報ファイルが利用に供される事務をつかさどる組織の名称	市民部なるせ駅前市民センター	
3	個人情報ファイルが利用に供される事務をつかさどる組織の名称	市民部鶴川市民センター	
3	個人情報ファイルが利用に供される事務をつかさどる組織の名称	市民部忠生市民センター	
3	個人情報ファイルが利用に供される事務をつかさどる組織の名称	市民部小山市民センター	
3	個人情報ファイルが利用に供される事務をつかさどる組織の名称	市民部堺市民センター	
4	個人情報ファイルの利用目的	住民の居住関係の公証及び、選挙人名簿の登録の他の住民に関する事務処理の基礎とする。 その他詳細は別紙のとおり	
5	(1) 基本的項目 氏名	○	
5	(1) 基本的項目 個人番号	○	
5	(1) 基本的項目 住所	○	
5	(1) 基本的項目 性別	○	
5	(1) 基本的項目 生年月日	○	
5	(1) 基本的項目 電話番号	○	
5	(1) 基本的項目 本籍	○	
5	(1) 基本的項目 国籍	○	
5	(1) 基本的項目 世帯主との続柄	○	
5	(1) 基本的項目 親族関係	○	
5	(1) 基本的項目 家庭環境等	○	DV情報を含む
5	(1) 基本的項目 人種※		
5	(1) 基本的項目 社会的身分※		
5	(1) 基本的項目 印鑑登録・印影	○	
5	(1) 基本的項目 出生	○	
5	(1) 基本的項目 死亡	○	
5	(1) 基本的項目 帰化	○	
5	(1) 基本的項目 住民異動年月日	○	
5	(1) 基本的項目 異動事由	○	
5	(1) 基本的項目 使用の目的	○	本人以外の者の請求の場合に収集する
5	(1) 基本的項目 筆頭者	○	
5	(1) 基本的項目 住民票コード	○	電子申請者のみ
5	(1) 基本的項目 電子メールアドレス	○	電子申請者のみ
5	(1) 基本的項目 公的個人認証	○	公的個人認証とは、秘密鍵、公開鍵、証明書シリアル番号、発行年月日、有効期間満了日、失効事由をいいます。
5	(1) 基本的項目 住民基本台帳カード	○	
5	(1) 基本的項目 在留資格	○	
5	(1) 基本的項目 住民記録システム注意情報	○	
5	(1) 基本的項目 成年後見	○	

5	(1) 基本的項目 個人番号カード	○	
5	(2) 思想・信条等に関する項目 主義・主張※		
5	(2) 思想・信条等に関する項目 支持政党		
5	(2) 思想・信条等に関する項目 宗教※		
5	(2) 思想・信条等に関する項目 趣味・嗜好		
5	(3) 社会的地位等に関する項目 職業・職歴	○	
5	(3) 社会的地位等に関する項目 地位		
5	(3) 社会的地位等に関する項目 学歴		
5	(3) 社会的地位等に関する項目 各種団体加入	○	本人確認を行うためのみ
5	(3) 社会的地位等に関する項目 賞罰		
5	(3) 社会的地位等に関する項目 犯歴※		
5	(3) 社会的地位等に関する項目 加入健康保険	○	
5	(3) 社会的地位等に関する項目 加入年金	○	
5	(3) 社会的地位等に関する項目 選挙資格	○	
5	(3) 社会的地位等に関する項目 学籍	○	
5	(3) 社会的地位等に関する項目 加入介護保険	○	
5	(3) 社会的地位等に関する項目 利用施設名	○	
5	(4) 成績・資格等に関する項目 学業成績		
5	(4) 成績・資格等に関する項目 勤務成績		
5	(4) 成績・資格等に関する項目 各種試験成績		
5	(4) 成績・資格等に関する項目 各種資格	○	本人確認を行うためのみ
5	(4) 成績・資格等に関する項目 所見	○	警察署・配偶者暴力相談支援センター・児童相談所・子ども生活部子ども家庭支援センターからのストーカー行為・暴力行為の被害に関する所見
5	(5) 財産・収入に関する項目 収入状況		
5	(5) 財産・収入に関する項目 財産状況	○	
5	(5) 財産・収入に関する項目 納税額等		
5	(5) 財産・収入に関する項目 取引状況	○	クレジットカード等による本人確認及びキャッシュレス決済に使用するため
5	(5) 財産・収入に関する項目 公的扶助の受給	○	
5	(5) 財産・収入に関する項目 保険給付状況	○	
5	(5) 財産・収入に関する項目 各種貸付金	○	
5	(5) 財産・収入に関する項目 住居の間取り・図面	○	正確な住所を確定するため
5	(5) 財産・収入に関する項目 金融機関名	○	クレジットカード等によるキャッシュレス決済に使用するため
5	(5) 財産・収入に関する項目 口座番号		
5	(5) 財産・収入に関する項目 犯罪被害※		
5	(5) 財産・収入に関する項目 手当の受給	○	
5	(5) 財産・収入に関する項目 土地の状況	○	
5	(5) 財産・収入に関する項目 建物の状況	○	
5	(5) 財産・収入に関する項目 被災	○	東日本大震災の被災者のみ収集
5	(6) 心身等に関する項目 健康状況	○	病院等の入院患者の方の住所を確定するため
5	(6) 心身等に関する項目 障がい状況※	○	身体障害者手帳により本人確認及び番号連携を行うためのみ

5	(6) 心身等に関する項目 容姿	○	写真のみ。証明書等の写真により本人確認を行うためのみ
5	(6) 心身等に関する項目 健診・検査※		
5	(6) 心身等に関する項目 病名※		
5	(6) 心身等に関する項目 診療・調剤※		
5	(6) 心身等に関する項目 犯罪被害※	○	警察署・配偶者暴力相談支援センター・児童相談所・子ども生活部子ども家庭支援センターからのストーカー行為・暴力行為の被害の状況
5	(6) 心身等に関する項目 医療機関名	○	
5	(6) 心身等に関する項目 要介護認定審査	○	介護保険受給資格証明書を発行するため
6	記録範囲	①届出義務者及びその代理人 ②住民票の写し等交付請求者 ③住民実態調査対象者及びその居住に関する情報提供者のみ ④在外選挙人名簿登録者 ⑤介護保険事業所就業者 ⑥介護保険サービス利用者及びその成年後見人・補佐人・補助人	
7	記録情報の収集方法	文書（紙）・電子媒体（データ）	
8	要配慮個人情報が含まれるときは、その旨	○	
9	記録情報の経常的提供先	別紙のとおり	
10	開示請求等を受理する組織の名称及び所在地	市民部市民課（町田市森野2-2-22）	
10	開示請求等を受理する組織の名称及び所在地	市民部南市民センター（町田市金森4-5-6）	
10	開示請求等を受理する組織の名称及び所在地	市民部なるせ駅前市民センター（町田市南成瀬1-2-5）	
10	開示請求等を受理する組織の名称及び所在地	市民部鶴川市民センター（町田市大蔵町1981-4）	
10	開示請求等を受理する組織の名称及び所在地	市民部忠生市民センター（町田市忠生3-14-2）	
10	開示請求等を受理する組織の名称及び所在地	市民部小山市民センター（町田市小山町2507-1）	
10	開示請求等を受理する組織の名称及び所在地	市民部堺市民センター（町田市相原町795-1）	
11	訂正及び利用停止に関する他の法律又はこれに基づく命令の規定による特別の手続等	なし	
12	個人情報ファイルの種別：法第60条第2項第1号（電算処理ファイル）	○	
12	個人情報ファイルの種別：（電算処理ファイルの場合）令第21条第7項に該当するファイル（電算処理ファイルに付随するマニュアル処理ファイル）の有無	有	
12	個人情報ファイルの種別：法第60条第2項第2号（マニュアル処理ファイル）		
13	行政機関等匿名加工情報の提案の募集をする個人情報ファイルである旨	実施しない	
14	行政機関等匿名加工情報の提案を受ける組織の名称及び所在地	実施しない	
15	行政機関等匿名加工情報の概要	実施しない	
16	作成された行政機関等匿名加工情報に関する提案を受ける組織の名称及び所在地	実施しない	
17	作成された行政機関等匿名加工情報に関する提案をすることができる期間	実施しない	
18	記録情報に条例要配慮個人情報が含まれているときはその旨	なし	
19	備考		

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

1. 特定個人情報ファイル名	
(1)住民基本台帳ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	・届出の際、届出内容や本人確認書類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。 ・本人あるいは代理人による届出のみを受領することとし、受領の際は必ず本人あるいは代理人の本人確認及び委任状の確認を行うこととしている。 ・記載例を明示し、届出書の記載に誤りがないように誘導している。 ・届出書は、必要な情報以外を記載できない書式となっている。 ・届出書に記載された情報以外は入力できないシステム仕様になっている。 ・異動事由や日付等の項目の論理矛盾をシステムで判定している。 ・システムへの入力結果を、入力者以外が確認（ダブルチェック）している。 ・情報に誤りがあった場合に訂正を行う場合には、所属長の許可を得て行う。また、訂正した内容等については、その記録を残し、法令等により定められる期間保管する。 ・入力、削除及び訂正作業に用いた届出書・帳票等は、市で定める規程に基づいて管理し、保管している。 町田市情報セキュリティポリシーにより規定 ・業務上、必要のない情報資産を作成しない。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時においては、一般権限のアカウントを利用している。 ・情報資産は適切に保管している。
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	「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」と同じ。
その他の措置の内容	・端末のアクセス制御を実施するためICカードシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できる端末認証の仕組みを導入している。 ・端末に情報を残さない仕組みであるシンクライアントシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できるシステムを導入している。 ・権限管理が実施できるシステムを導入している。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 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	「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」と同じ。
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	届出の際、個人番号カードや運転免許証等で本人確認を行う。	
個人番号の真正性確認の措置の内容	・本人が持参する個人番号カードで確認する。 ・住民基本台帳ネットワークで確認する。 ・転入前住所等の市区町村に照会する。	
特定個人情報の正確性確保の措置の内容	「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」と同じ。	
その他の措置の内容	・端末のアクセス制御を実施するためICカードシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できる端末認証の仕組みを導入している。 ・端末に情報を残さない仕組みであるシンクライアントシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できるシステムを導入している。 ・権限管理が実施できるシステムを導入している。	
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	・届出書・帳票等の取扱いについては手順化され運用している。 ・端末は記録媒体が接続できない仕様になっている。 ・端末はインターネット接続ができない仕様になっている。 ・特定個人情報を回線を通じて入手する場合は、他のシステムからのアクセスが行えない専用回線を用いている。 町田市情報セキュリティポリシーにより規定 ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)の使用または鍵付キャビネットへの保管を行っている。 ・業務上、必要のない情報資産を作成しない。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト(ログオフ)、画面表示を起動初期状態(情報の検索結果などが表示されていない状態)にする等。 ・相談室には個室又はパーテーションを設置している。	
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		
・端末のアクセス制御を実施するためICカードシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できる端末認証の仕組みを導入している。 ・端末に情報を残さない仕組みであるシンクライアントシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できるシステムを導入している。 ・権限管理が実施できるシステムを導入している。		

3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク		
宛名システム等における措置の内容	・宛名システム等における個人番号を番号法及び条例上認められないシステムと紐付けできないように制御する。 ・個人番号利用業務以外の業務では、個人番号が含まれない画面表示とする。 ・個人番号利用業務以外の業務から住民基本台帳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し、個人番号には一切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	「3. 特定個人情報の使用 リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク 宛名システム等における措置の内容」と同じ。	
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	生体認証により操作者認証を行う。なお、生体認証が不可能な場合は、申請に基づきユーザーIDとパスワードを用いた認証を行う。 町田市情報セキュリティポリシーにより規定 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。	
アクセス権限の発効・失効の管理	[行っている]	<選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	「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 ユーザ認証の管理 具体的な管理方法」と同じ。	
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	「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 ユーザ認証の管理 具体的な管理方法」と同じ。	
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	町田市情報セキュリティポリシーにより規定 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。	
その他の措置の内容	・端末のアクセス制御を実施するためICカードシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できる端末認証の仕組みを導入している。 ・端末に情報を残さない仕組みであるシンクライアントシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できるシステムを導入している。 ・権限管理が実施できるシステムを導入している。	
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	・端末は記録媒体が接続できない仕様になっている。 ・端末はインターネット接続ができない仕様になっている。 ・特定個人情報を回線を通じて入手する場合は、他のシステムからのアクセスが行えない専用回線を用いている。 町田市情報セキュリティポリシーにより規定 ＜事務室における措置＞ ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具（鍵付チェーン等）の使用または鍵付キャビネットへの保管を行っている。 ＜アクセス制御＞ ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト（ログオフ）、画面表示を起動初期状態（情報の検索結果などが表示されていない状態）にする等。 ＜その他の措置＞ ・委託に際しては、契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付している。 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 ・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。 ・情報セキュリティ内部監査員を養成するための教育をしている。 ・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行う。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施する。	
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	「3. 特定個人情報の使用 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」と同じ。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置		
・端末のアクセス制御を実施するためICカードシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できる端末認証の仕組みを導入している。 ・端末に情報を残さない仕組みであるシンクライアントシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できるシステムを導入している。 ・権限管理が実施できるシステムを導入している。		

☐ 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	・ISO/IEC27001 (ISMS) の認証を受けていることを業者選定の際の条件としている。 ・作業者を限定するために、委託にかかる実施体制の提出を義務付けている。 ・委託先は原則的に特定個人情報ファイルを取り扱わない。 ・委託先については契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付し、町田市セキュリティポリシーを遵守させている。
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	・作業者を限定するために、委託にかかる実施体制の提出を義務付けている。 ・委託先は原則的に特定個人情報ファイルを取り扱わない。 町田市情報セキュリティポリシーにより規定 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時においては、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。
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	・委託業務の実施状況について定期的に報告を受けるとともに、その記録を残している。 ・委託先は原則的に特定個人情報ファイルを取り扱わない。 町田市情報セキュリティポリシーにより規定 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。
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	委託先から他者へ提供することはない。
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	・委託先へ原則的に提供することはない。 提供する場合は次のとおり。 磁気データの管理と取扱いに関する要領により規定 ・受渡しは、受渡確認書(別記様式)により確認し、行っている。 ・受渡しは、コンピュータセンター内の決められた場所で行っている。

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	・原則的に特定個人情報を含むデータの受け渡しは発生しないため、消去の委託はしない。 ・消去した旨の書面を提出させる。 情報セキュリティ確保・個人情報保護のための特記仕様書により規定 ・契約の終了後又は解除後、委託先は、市に返還又は納入する物もしくは特に保管を要する物を除き、受託業務の実施にあたり作成した情報の一切を抹消、焼却、切断その他の方法により復元不可能な状態にして処分するものとしている。
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	委託先については契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付し、町田市セキュリティポリシーを遵守させている。 「情報セキュリティ確保・個人情報保護のための特記仕様書」として以下の項目を定めている。 1. 秘密の保持 2. 第三者への提供の禁止 3. 指示目的以外の利用の禁止 4. 事故発生時の報告義務 5. 無許可による再委託の禁止 6. 複写又は複製の禁止 7. 情報の管理義務及び返還義務 8. 立ち入り調査 9. 監査への協力 10. 保証 11. 成果(物)に関する所有権、知的財産権の帰属 12. セキュリティ事故の対応マニュアルの作成 13. 情報の取扱いに関する教育の履行 14. 情報セキュリティ対策実施状況の報告 15. 守秘義務違反等の場合、法令及び契約条項に定める措置(告発、損害賠償等)
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	「4. 特定個人情報ファイルの取扱いの委託 委託契約中の特定個人情報ファイルの取扱いに関する規定 規定の内容」と同じ。
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	町田市情報セキュリティポリシーにより規定 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。	
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	・番号法及び条例上認められる場合のみ提供及び移転を行う。 ・番号法及び条例上認められる提供及び移転以外に、提供・移転する機能をシステム上設けない。 磁気データの管理と取扱いに関する要領により規定 第5 磁気データの利用 1 磁気データの処理を新たに行い、又は変更するに当たり、他業務の磁気データを利用しようとする課（以下「データ利用課」という。）の情報管理者は、データ保有課の情報管理者に対し、磁気データの利用を申請して承諾を得なければならない。 2 データ利用課の情報管理者は、前項の承諾を得た範囲内においてのみ、磁気データを利用できる。	
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
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	・番号法及び条例上認められる場合のみ提供及び移転を行う。 ・番号法及び条例上認められる提供及び移転以外に、提供・移転する機能をシステム上設けない。 磁気データの管理と取扱いに関する要領により規定 第5 磁気データの利用 1 磁気データの処理を新たに行い、又は変更するに当たり、他業務の磁気データを利用しようとする課（以下「データ利用課」という。）の情報管理者は、データ保有課の情報管理者に対し、磁気データの利用を申請して承諾を得なければならない。 2 データ利用課の情報管理者は、前項の承諾を得た範囲内においてのみ、磁気データを利用できる。 町田市情報セキュリティポリシーにより規定 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 ・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。 ・情報セキュリティ内部監査員を養成するための教育をしている。	
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	「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。） 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」と同じ。	
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 that 不正確であるリスク					
リスクに対する措置の内容					
リスクへの対策は十分か		[]		＜選択肢＞ 1) 特に力を入れている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 that 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		・宛名システム兼連携システムでは、情報の提供について、連携時のアクセスログと連携データ that 特定できるよう記録している。 ・宛名システム兼連携システムでは、番号法及び条例上認められる提供以外に、提供する機能をシステム上設けない。 ＜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提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報 that 不正に提供されるリスクに対応している。 ③機微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 that 不正に提供されるリスクに対応している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 (※)情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。			
リスクへの対策は十分か		[十分である]		＜選択肢＞ 1) 特に力を入れている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	・宛名システム兼連携システムでは、情報の提供について、連携時のアクセスログと連携データが特定できるよう記録している。 ・宛名システム兼連携システムでは、番号法及び条例上認められる提供以外に、提供する機能をシステム上設けない。 ＜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っている。 ②中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 (※)暗号化・復号機能と、鍵情報及び照会許可照会リストを管理する機能。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク)等を利用することにより、不適切な方法で提供されるリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォームの事業者においては、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	・宛名システム兼連携システムでは、情報の提供について、連携時のアクセスログと連携データが特定できるよう記録している。 ・宛名システム兼連携システムでは、番号法及び条例上認められる提供以外に、提供する機能をシステム上設けない。 ＜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、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事業者における情報漏えい等のリスクを極小化する。		

リスク3: 入手した特定個人情報 that 不正確であるリスク		
入手の際の本人確認の措置の内容	窓口において、対面で身分証明書等の提示を受け、本人確認を行う。 ※身分証明書とは、個人番号カード、運転免許証等の官公署から発行され又は発給された書類その他これに類する書類である。	
個人番号の真正性確認の措置の内容	・転入前住所等の市町村に照会する。 ・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(若しくは通知カードと法令により定められた身分証明書の組み合わせ)の提示がない場合には、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帳票等は、当市で定める規程に基づいて管理し、保管する。 ・本人確認情報に誤りがあった際に訂正を行う場合には、本人確認情報管理責任者の許可を得て行うこととする。また、訂正した内容等については、その記録を残し、法令等により定められる期間保管する。	
その他の措置の内容	・端末のアクセス制御を実施するためICカードシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できる端末認証の仕組みを導入している。 ・端末に情報を残さない仕組みであるシンクライアントシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できるシステムを導入している。 ・権限管理が実施できるシステムを導入している。	
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4: 入手の際に特定個人情報 that 漏えい・紛失するリスク		
リスクに対する措置の内容	・機構が作成・配付する専用のアプリケーション(※)を用いることにより、入手の際の特定個人情報の漏えい・紛失の防止に努める。 ・操作者の認証を行う。 ※市町村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		
—		

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 町田市情報セキュリティポリシーにより規定 <事務室における措置> ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)の使用または鍵付キャビネットへの保管を行っている。 <中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォーム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。 ②事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。 <ガバメントクラウドにおける措置> ①ガバメントクラウドについては政府情報システムのセキュリティ制度(ISMAP)のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された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。 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	[十分にやっている] <選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
具体的な対策の内容	・端末は記録媒体が接続できない仕様になっている。 ・端末はインターネット接続ができない仕様になっている。 ・特定個人情報を回線により入手する場合は、他のシステムからのアクセスが行えない専用回線を用いている。 町田市情報セキュリティポリシーにより規定 ・ウイルス対策ソフトを導入している。 ・ウイルス対策の対象は、サーバ、クライアント(端末)及びゲートウェイを含めた、包括的な対策を講じている。 ・常に最新のウイルス定義ファイル(パターンファイル)を使用している。 ・定期的にウイルス対策の実施状況を確認している。 ・インターネット等外部ネットワークとは分離し、不正アクセス防止をしている。 ・外部接続(インターネット接続を含む)におけるアクセス制御に関する管理策として、ファイアウォールやルータを設置している。 ・ハードウェア及びソフトウェアには、セキュリティ修正プログラムを適用している。 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト(ログオフ)、画面表示を起動初期状態(情報の検索結果などが表示されていない状態)にする等 <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。 <ガバメントクラウドにおける措置> 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。 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が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。 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。 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。 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。 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。 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。 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	[十分にやっている] <選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
⑧事故発生時手順の策定・周知	[十分にやっている] <選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない

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	生存する個人の個人番号とともに、死亡による消除後、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。	
その他の措置の内容		・端末のアクセス制御を実施するためICカードシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できる端末認証の仕組みを導入している。 ・端末に情報を残さない仕組みであるシンクライアントシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できるシステムを導入している。 ・権限管理が実施できるシステムを導入している。	
リスクへの対策は十分か		[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2: 特定個人情報が古い情報のまま保管され続けるリスク			
リスクに対する措置の内容		住民基本台帳法および同施行令に規定される届出および記載等があった都度、住民基本台帳ファイルへの入力、削除および修正を行うとともに、住民基本台帳法第14条(住民基本台帳の正確な記録を確保するための措置)および第34条(調査)の規定に基づき、実態調査等を実施することにより、既存住民システムの情報が正確であることを確保する。	
リスクへの対策は十分か		[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク3: 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	<選択肢> 1) 定めている 2) 定めていない
手順の内容	システム上、住民基本台帳法施行令第34条第2項(保存)に定める期間(150年間)を経過した住民票の記載の修正前の本人確認情報(履歴情報)及び消除者の本人確認情報を消去する仕組みとする。 町田市情報セキュリティポリシーにより規定 ・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。 ・紙媒体は、シュレッダーによる破碎、溶解、焼却等の情報の復元不能化処理を行っている。 ・情報資産の廃棄時には、必要に応じ、廃棄日時、廃棄担当者、処理内容を記録している。 <ガバメントクラウドにおける措置> 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> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		
—		

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

1. 特定個人情報ファイル名	
(2) 本人確認情報ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	本人確認情報の入手元は既存住記システムに限定されるため、既存住記システムへの情報の登録の際に、届出の窓口において届出内容や本人確認書類(写真付の公的機関発行証明書等)の確認を厳格に行い、対象者以外の情報の入手の防止に努める。
必要な情報以外を入手することを防止するための措置の内容	・総務省告示第334号(第6ー6 本人確認情報の通知及び記録)等により市町村CSにおいて既存住記システムを通じて入手することとされている情報以外を入手できないことを、システム上で担保する。 ・正当な利用目的以外の目的にデータベースが構成されることを防止するため、本人確認情報の検索を行う際の検索条件として、少なくとも性別を除く2情報以上(氏名と住所の組み合わせ、氏名と生年月日の組み合わせ)の指定を必須とする。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	本人確認情報の入手元を既存住基システムに限定する。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク		
宛名システム等における措置の内容	市町村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、IPアドレスによるフィルタリング制御等)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	生体認証により操作者認証を行う。なお、生体認証が不可能な場合は、申請に基づきユーザーIDとパスワードを用いた認証を行う。 町田市情報セキュリティポリシーにより規定 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。
アクセス権限の発効・失効の管理	[行っている]	<選択肢> 1) 行っている 2) 行っていない
	具体的な管理方法	町田市情報セキュリティポリシーにより規定 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。
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	「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 アクセス権限の発行・失効の管理 具体的な管理方法」と同じ。
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	町田市情報セキュリティポリシーにより規定 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・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	・端末は記録媒体が接続できない仕様になっている。 ・端末はインターネット接続ができない仕様になっている。 ・特定個人情報を回線を通じて入手する場合は、他のシステムからのアクセスが行えない専用回線を用いている。 町田市情報セキュリティポリシーにより規定 ＜事務室における措置＞ ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具（鍵付チェーン等）の使用または鍵付キャビネットへの保管を行っている。 ＜アクセス制御＞ ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト（ログオフ）、画面表示を起動初期状態（情報の検索結果などが表示されていない状態）にする等。 ＜その他の措置＞ ・委託先については契約時に情報セキュリティ確保・個人情報保護のための特記仕様書を添付している。 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 ・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。 ・情報セキュリティ内部監査員を養成するための教育をしている。 ・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行う。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施する。	
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	「3. 特定個人情報の使用 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」と同じ。	
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 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	・ISO/IEC27001 (ISMS) の認証を受けていることを業者選定の際の条件としている。 ・作業者を限定するために、委託にかかる実施体制の提出を義務付けている。 ・委託先は原則的に特定個人情報ファイルを取り扱わない。 ・委託先については契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を添付し、町田市セキュリティポリシーを遵守させている。	
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	・作業者を限定するために、委託にかかる実施体制の提出を義務付けている。 ・委託先は原則的に特定個人情報ファイルを取り扱わない。 町田市情報セキュリティポリシーにより規定 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時においては、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。	
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	・委託業務の実施状況について定期的に報告を受けるとともに、その記録を残している。 ・委託先は原則的に特定個人情報ファイルを取り扱わない。 町田市情報セキュリティポリシーにより規定 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。	
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	委託先から他者へ提供することはない。	
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	・委託先へ原則的に提供することはない。 提供する場合は次のとおり。 磁気データの管理と取扱いに関する要領により規定 ・受渡しは、受渡確認書(別記様式)により確認し、行っている。 ・受渡しは、コンピュータセンター内の決められた場所で行っている。	
特定個人情報の消去ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
ルール内容及びルール遵守の確認方法	・原則的に特定個人情報を含むデータの受け渡しは発生しないため、消去の委託はしない。 ・消去した旨の書面を提出させる。 情報セキュリティ確保・個人情報保護のための特記仕様書により規定 ・契約の終了後又は解除後、委託先は、市に返還又は納入する物もしくは特に保管を要する物を除き、受託業務の実施にあたり作成した情報の一切を抹消、焼却、切断その他の方法により復元不可能な状態にして処分するものとしている。	

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		<選択肢> 1) 定めている 2) 定めていない [定めている]
	規定の内容	委託先については契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付し、町田市セキュリティポリシーを遵守させている。 「情報セキュリティ確保・個人情報保護のための特記仕様書」として以下の項目を定めている。 1. 秘密の保持 2. 第三者への提供の禁止 3. 指示目的以外の利用の禁止 4. 事故発生時の報告義務 5. 無許可による再委託の禁止 6. 複写又は複製の禁止 7. 情報の管理義務及び返還義務 8. 立ち入り調査 9. 監査への協力 10. 保証 11. 成果(物)に関する所有権、知的財産権の帰属 12. セキュリティ事故の対応マニュアルの作成 13. 情報の取扱いに関する教育の履行 14. 情報セキュリティ対策実施状況の報告 15. 守秘義務違反等の場合、法令及び契約条項に定める措置(告発、損害賠償等)
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		<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 [十分に行っている]
	具体的な方法	「4. 特定個人情報ファイルの取扱いの委託 委託契約中の特定個人情報ファイルの取扱いに関する規定 規定の内容」と同じ。
その他の措置の内容		—
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 [十分である]
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
—		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	特定個人情報（個人番号、4情報等）の提供を行う際に、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> 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	・番号法及び条例上認められる場合のみ提供及び移転を行う。 ・番号法及び条例上認められる提供及び移転以外に、提供・移転する機能をシステム上設けない。 磁気データの管理と取扱いに関する要領により規定 第5 磁気データの利用 1 磁気データの処理を新たに行い、又は変更するに当たり、他業務の磁気データを利用しようとする課（以下「データ利用課」という。）の情報管理者は、データ保有課の情報管理者に対し、磁気データの利用を申請して承諾を得なければならない。 2 データ利用課の情報管理者は、前項の承諾を得た範囲内においてのみ、磁気データを利用できる。	
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
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)

[○] 接続しない(入手) [○] 接続しない(提供)

リスク1: 目的外の入手が行われるリスク

リスクに対する措置の内容	
リスクへの対策は十分か	[＜選択肢＞ 1) 特に力を入れている 3) 課題が残されている 2) 十分である]

リスク2: 安全が保たれない方法によって入手が行われるリスク

リスクに対する措置の内容	
リスクへの対策は十分か	[＜選択肢＞ 1) 特に力を入れている 3) 課題が残されている 2) 十分である]

リスク3: 入手した特定個人情報が不正確であるリスク

リスクに対する措置の内容	
リスクへの対策は十分か	[] <選択肢> 1) 特に力を入れている 3) 課題が残されている 2) 十分である

リスク4: 入手の際に特定個人情報漏えい・紛失するリスク

リスクに対する措置の内容	
リスクへの対策は十分か	[] <選択肢> 1) 特に力を入れている 3) 課題が残されている 2) 十分である

リスク5: 不正な提供が行われるリスク

リスクに対する措置の内容	
リスクへの対策は十分か	[＜選択肢＞ 1) 特に力を入れている 3) 課題が残されている 2) 十分である]

リスク6: 不適切な方法で提供されるリスク

リスクに対する措置の内容	
リスクへの対策は十分か	[] <選択肢> 1) 特に力を入れている 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 町田市情報セキュリティポリシーにより規定 <事務室における措置> ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)の使用または鍵付キャビネットへの保管を行っている。 <ガバメントクラウドにおける措置> ①ガバメントクラウドについては政府情報システムのセキュリティ制度(ISMAP)のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された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。 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	[十分にやっている] <選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
具体的な対策の内容	・端末は記録媒体が接続できない仕様になっている。 ・端末はインターネット接続ができない仕様になっている。 ・特定個人情報を回線により入手する場合は、他のシステムからのアクセスが行えない専用回線を用いている。 町田市情報セキュリティポリシーにより規定 ・ウイルス対策ソフトを導入している。 ・ウイルス対策の対象は、サーバ、クライアント(端末)及びゲートウェイを含めた、包括的な対策を講じている。 ・常に最新のウイルス定義ファイル(パターンファイル)を使用している。 ・定期的にウイルス対策の実施状況を確認している。 ・インターネット等外部ネットワークとは分離し、不正アクセス防止をしている。 ・外部接続(インターネット接続を含む)におけるアクセス制御に関する管理策として、ファイアウォールやルータを設置している。 ・ハードウェア及びソフトウェアには、セキュリティ修正プログラムを適用している。 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト(ログオフ)、画面表示を起動初期状態(情報の検索結果などが表示されていない状態)にする等 <ガバメントクラウドにおける措置> 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。 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。 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。 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。 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。 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。 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。 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	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
⑧事故発生時手順の策定・周知	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
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	生存する個人の個人番号とともに、死亡による消除後、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。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク2: 特定個人情報古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	既存住基システムとの整合処理を定期的を実施し、保存する本人確認情報が最新であるかどうかを確認することにより担保する。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	<選択肢> 1) 定めている 2) 定めていない
手順の内容	システム上、住民基本台帳法施行令第34条第2項(保存)に定める期間(150年間)を経過した住民票の記載の修正前の本人確認情報(履歴情報)及び消除者の本人確認情報を消去する仕組みとする。 町田市情報セキュリティポリシーにより規定 ・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。 ・紙媒体は、シュレッダーによる破碎、溶解、焼却等の情報の復元不能化処理を行っている。 ・情報資産の廃棄時には、必要に応じ、廃棄日時、廃棄担当者、処理内容を記録している。 <ガバメントクラウドにおける措置> 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> 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記システムに限定されるため、既存住記システムへの情報の登録の際に、届出の窓口において届出内容や本人確認書類(写真付の公的機関発行証明書等)の確認を厳格に行い、対象者以外の情報の入手の防止に努める。
必要な情報以外を入手することを防止するための措置の内容	・総務省告示第334号(第6ー6 本人確認情報の通知及び記録)等により市町村CSにおいて既存住記システムを通じて入手することとされている情報以外を入手できないことを、システム上で担保する。 ・正当な利用目的以外の目的にデータベースが構成されることを防止するため、本人確認情報の検索を行う際の検索条件として、少なくとも性別を除く2情報以上(氏名と住所の組み合わせ、氏名と生年月日の組み合わせ)の指定を必須とする。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	本人確認情報の入手元を既存住基システムに限定する。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 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 that 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。	
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、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	・端末のアクセス制御を実施するためICカードシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できる端末認証の仕組みを導入している。 ・端末に情報を残さない仕組みであるシンクライアントシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できるシステムを導入している。 ・権限管理が実施できるシステムを導入している。	
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4: 入手の際に特定個人情報 that 漏えい・紛失するリスク		
リスクに対する措置の内容	・機構が作成・配付する専用のアプリケーション(※)を用いることにより、入手の際の特定個人情報の漏えい・紛失の防止に努める。 ・操作者の認証を行う。 ※市町村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、事務に必要な情報との紐付けが行われるリスク			
宛名システム等における措置の内容	市町村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、IPアドレスによるフィルタリング制御等）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 3) 課題が残されている	2) 十分である
リスク2: 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク			
ユーザ認証の管理	[行っている]	<選択肢> 1) 行っている	2) 行っていない
	具体的な管理方法	生体認証により操作者認証を行う。なお、生体認証が不可能な場合は、申請に基づきユーザーIDとパスワードを用いた認証を行う。 町田市情報セキュリティポリシーにより規定 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。	
アクセス権限の発効・失効の管理	[行っている]	<選択肢> 1) 行っている	2) 行っていない
	具体的な管理方法	町田市情報セキュリティポリシーにより規定 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。	
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	「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 アクセス権限の発行・失効の管理 具体的な管理方法」と同じ。	
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	・送付先情報を扱うシステムの操作履歴（アクセスログ・操作ログ）を記録する。 ・不正な操作が無いことについて、操作履歴により適時確認する。 ・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 3) 課題が残されている	2) 十分である

リスク3: 従業者が事務外で使用するリスク		
リスクに対する措置の内容	町田市情報セキュリティポリシーにより規定 ＜事務室における措置＞ ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具（鍵付チェーン等）の使用または鍵付キャビネットへの保管を行っている。 ＜アクセス制御＞ ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト（ログオフ）、画面表示を起動初期状態（情報の検索結果などが表示されていない状態）にする等。 ＜その他の措置＞ ・委託先については契約時に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付している。 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 ・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。 ・情報セキュリティ内部監査員を養成するための教育をしている。 ・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行う。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施する。	
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	「3. 特定個人情報の使用 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」と同じ。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置		
—		

☐ 委託しない

情報保護管理体制の確認	・ISO/IEC27001 (ISMS) の認証を受けていることを業者選定の際の条件としている。 ・作業者を限定するために、委託にかかる実施体制の提出を義務付けている。 ・委託先は原則的に特定個人情報ファイルを取り扱わない。 ・委託先については契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付し、町田市セキュリティポリシーを遵守させている。
-------------	---

具体的な制限方法	・作業者を限定するために、委託にかかる実施体制の提出を義務付けている。 ・委託先は原則的に特定個人情報ファイルを取り扱わない。 町田市情報セキュリティポリシーにより規定 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。
-----------------	--

具体的な方法	・委託業務の実施状況について定期的に報告を受けるとともに、その記録を残している。 ・委託先は原則的に特定個人情報ファイルを取り扱わない。 町田市情報セキュリティポリシーにより規定 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。
--------	---

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	委託先から他者へ提供することはない。
-----------------------------------	--------------------

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	・委託先へ原則的に提供することはない。 - 提供する場合は次のとおり。 - 磁気データの管理と取扱いに関する要領により規定 ・受渡しは、受渡確認書(別記様式)により確認し、行っている。 ・受渡しは、コンピュータセンター内の決められた場所で行っている。
--	---

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	・原則的に特定個人情報を含むデータの受け渡しは発生しないため、消去の委託はしない。 ・消去した旨の書面を提出させる。 情報セキュリティ確保・個人情報保護のための特記仕様書により規定 ・契約の終了後又は解除後、委託先は、市に返還又は納入する物もしくは特に保管を要する物を除き、受託業務の実施にあたり作成した情報の一切を抹消、焼却、切断その他の方法により復元不可能な状態にして処分するものとしている。		
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	委託先については契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付し、町田市セキュリティポリシーを遵守させている。 「情報セキュリティ確保・個人情報保護のための特記仕様書」として以下の項目を定めている。 1. 秘密の保持 2. 第三者への提供の禁止 3. 指示目的以外の利用の禁止 4. 事故発生時の報告義務 5. 無許可による再委託の禁止 6. 複写又は複製の禁止 7. 情報の管理義務及び返還義務 8. 立ち入り調査 9. 監査への協力 10. 保証 11. 成果(物)に関する所有権、知的財産権の帰属 12. セキュリティ事故の対応マニュアルの作成 13. 情報の取扱いに関する教育の履行 14. 情報セキュリティ対策実施状況の報告 15. 守秘義務違反等の場合、法令及び契約条項に定める措置(告発、損害賠償等)		
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	「4. 特定個人情報ファイルの取扱いの委託 委託契約中の特定個人情報ファイルの取扱いに関する規定 規定の内容」と同じ。		
その他の措置の内容		－		
リスクへの対策は十分か		[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置				
－				

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	特定個人情報（個人番号、4情報等）の提供を行う際に、提供記録（提供日時、操作者等）をシステム上で管理し、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	・番号法及び条例上認められる場合のみ提供及び移転を行う。 ・番号法及び条例上認められる提供及び移転以外に、提供・移転する機能をシステム上設けない。 磁気データの管理と取扱いに関する要領により規定 第5 磁気データの利用 1 磁気データの処理を新たに行い、又は変更するに当たり、他業務の磁気データを利用しようとする課（以下「データ利用課」という。）の情報管理者は、データ保有課の情報管理者に対し、磁気データの利用を申請して承諾を得なければならない。 2 データ利用課の情報管理者は、前項の承諾を得た範囲内においてのみ、磁気データを利用できる。	
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
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		
—		

☐ 接続しない(入手) ☐ 接続しない(提供)

リスクに対する措置の内容

リスクへの対策は十分か

[

1

3) 課題が残されている

2) 十分である

リスクに対する措置の内容

リスクへの対策は十分か

[

]

1) 特に力を入れている
3) 課題が残されている

2) 十分である

リスクに対する措置の内容

リスクへの対策は十分か

[

]

1) 特に力を入れている
3) 課題が残されている

2) 十分である

リスクに対する措置の内容

リスクへの対策は十分か

[

]

1) 特に力を入れている
3) 課題が残されている

2) 十分である

リスクに対する措置の内容

リスクへの対策は十分か

[

]

1) 特に力を入れている
3) 課題が残されている

2) 十分である

リスクに対する措置の内容

リスクへの対策は十分か

[

]

1) 特に力を入れている
3) 課題が残されている

2) 十分である

リスクに対する措置の内容

リスクへの対策は十分か

[

]

3) 課題が残されている

2) 十分である

情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置

7. 特定個人情報の保管・消去		
リスク1: 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1) 特に力を入れて遵守している 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 町田市情報セキュリティポリシーにより規定 <事務室における措置> ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)の使用または鍵付キャビネットへの保管を行っている。 <ガバメントクラウドにおける措置> ①ガバメントクラウドについては政府情報システムのセキュリティ制度(ISMAP)のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された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。 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	[十分にしている] <選択肢> 1) 特に力を入れてしている 2) 十分にしている 3) 十分にしていない
具体的な対策の内容	・端末は記録媒体が接続できない仕様になっている。 ・端末はインターネット接続ができない仕様になっている。 ・特定個人情報を回線により入手する場合は、他のシステムからのアクセスが行えない専用回線を用いている。 町田市情報セキュリティポリシーにより規定 ・ウイルス対策ソフトを導入している。 ・ウイルス対策の対象は、サーバ、クライアント(端末)及びゲートウェイを含めた、包括的な対策を講じている。 ・常に最新のウイルス定義ファイル(パターンファイル)を使用している。 ・定期的にウイルス対策の実施状況を確認している。 ・インターネット等外部ネットワークとは分離し、不正アクセス防止をしている。 ・外部接続(インターネット接続を含む)におけるアクセス制御に関する管理策として、ファイアウォールやルータを設置している。 ・ハードウェア及びソフトウェアには、セキュリティ修正プログラムを適用している。 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト(ログオフ)、画面表示を起動初期状態(情報の検索結果などが表示されていない状態)にする等 <ガバメントクラウドにおける措置> 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。 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。 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。 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。 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。 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。 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。 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	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
⑧事故発生時手順の策定・周知	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	<選択肢> 1) 発生あり 2) 発生なし
その内容	—	
再発防止策の内容	—	
⑩死者の個人番号	[保管していない]	<選択肢> 1) 保管している 2) 保管していない
具体的な保管方法	—	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 特定個人情報古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	本特定個人情報ファイル(送付先情報ファイル)は、送付先情報の連携を行う必要が生じた都度作成／連携することとしており、システム上、一定期間経過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。 <ガバメントクラウドにおける措置> 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> 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、一定期間経過後、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。		

IV その他のリスク対策 ※

1. 監査		
①自己点検	[十分にやっている]	＜選択肢＞ 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
	具体的なチェック方法	情報セキュリティポリシーに基づく内部監査の一環で、チェックリストにて自己点検を全庁にわたり毎年度実施する。 ＜中間サーバー・プラットフォームにおける措置＞ ①運用規則等に基づき、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。
②監査	[十分にやっている]	＜選択肢＞ 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
	具体的な内容	町田市情報セキュリティポリシーにより規定 ・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行っている。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施している。 ＜中間サーバー・プラットフォームにおける措置＞ ①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。 ＜ガバメントクラウドにおける措置＞ 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	[十分にやっている]	＜選択肢＞ 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
	具体的な方法	町田市情報セキュリティポリシーにより規定 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 ・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。 ・情報セキュリティ内部監査員を養成するための教育をしている。 ＜中間サーバー・プラットフォームにおける措置＞ ①IPA (情報処理推進機構) が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資料を作成し、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、運用規則 (接続運用規程等) や情報セキュリティに関する教育を年次 (年2回) 及び随時 (新規要員着任時) 実施することとしている。
3. その他のリスク対策		
＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理 (入退室管理等)、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用、監視を実現する。 ＜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	郵便番号194-8520 東京都町田市森野2-2-22 担当課:総務部 法務課 電話:042-724-8407 FAX:050-3085-3142
②請求方法	指定様式による書面の提出により開示・訂正・利用停止請求を受け付ける。また、請求方法について、ホームページにおいて要領を記載し、わかりやすい説明に努めている。
特記事項	市ホームページ上に、請求先、請求方法、請求書様式等を掲載している。
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	住民基本台帳ファイル
公表場所	総務部法務課
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	郵便番号194-8520 東京都町田市森野2-2-22 担当課:市民部 市民課 電話:042-724-4225 FAX:050-3085-6262
②対応方法	窓口・電話・FAX等による。

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和5年9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] <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	意見公募の実施について、広報まちだに記事を掲載し、ホームページ及び市庁舎、市民センター、駅前連絡所等にて全文を閲覧できるようにする。意見聴取の方法は、郵便、FAX、電子メールによる。
②実施日・期間	令和6年5月15日から令和6年6月15日まで
③期間を短縮する特段の理由	—
④主な意見の内容	評価書の内容に関する意見は寄せられなかった。
⑤評価書への反映	なし
3. 第三者点検	
①実施日	令和6年6月21日
②方法	株式会社NTTデータに委託し、点検を行った。
③結果	下記2件の指摘が修正されることを前提として、適合性・妥当性の観点から問題ないとの点検結果を得た。 ・Ⅱ 特定個人情報ファイルの概要(1)～(3) 6. 特定個人情報の保管・消去 ③消去方法 「変更後の記載」が「①保管場所」に関する内容となっています(本文側では「③消去方法」に関する内容となっているため、「変更後の記載」への転記ミスとみられます)。本文側の内容にあわせ、「変更後の記載」の修正をお願いいたします。 ・Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 消去手順 手順の内容 本文側の一部(本人確認情報ファイル)の内容が変更されていません。本文側(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(本人確認情報ファイル) - 7. 特定個人情報の保管・消去 - 消去手順 - 手順の内容)の内容変更をお願いいたします。
4. 個人情報保護委員会の承認【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

(別添3)変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成27年11月30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 システム5 ICカード標準システム システム6 証明書等のコンビニ交付システムを追加 (別添1)事務概要 証明書交付センターと付随する矢印を追加	事前	
平成27年11月30日	II ファイルの概要 (1)住民基本台帳ファイル		4. 特定個人情報ファイルの取扱いの委託 委託事項4 証明書等のコンビニ交付システムの保守業務 委託事項5 ICカード標準システム保守業務を追加	事前	
平成27年11月30日	(別添2)個人情報ファイル記録項目	「住民基本台帳」業務における 個人情報業務登録票(2014.10.20) 個人情報コンピュータ処理等登録票「住民記録システム」(2014.10.20)	「住民基本台帳」業務における 個人情報業務登録票(2015.6.8) 個人情報コンピュータ処理等登録票「住民記録システム」(2015.6.8) 個人情報コンピュータ処理等登録票「コンビニエンスストアを介した証明書自動交付システム」(2015.6.8)	事前	
平成29年2月28日	I 基本情報 7. 評価実施機関における担当部署	所属長 中島 清徳	所属長 水嶋 康信	事後	
平成30年1月31日	(別添2)個人情報ファイル記録項目	「住民基本台帳」業務における 個人情報業務登録票(2015.6.8)	「住民基本台帳」業務における 個人情報業務登録票(2017.7.10)	事後	
平成31年2月28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 ・システム1 ②システムの機能 8. ICカード標準システムとの連携機能 ・システム5 ICカード標準システム	削除	事後	
平成31年2月28日	(別添2)個人情報ファイル記録項目	「住民基本台帳」業務における 個人情報業務登録票(2017.7.10)	「住民基本台帳」業務における 個人情報業務登録票(2018.3.12)	事後	
平成31年2月28日	II ファイルの概要 (1)住民基本台帳ファイル	4. 特定個人情報ファイルの取扱いの委託 委託事項5 ICカード標準システム保守業務	削除	事後	
平成31年2月28日	I 基本情報 7. 評価実施機関における担当部署	②所属長 水嶋 康信	②所属長の役職名 市民部市民課長	事後	
令和2年9月30日	II ファイルの概要 (1)住民基本台帳ファイル	「住民基本台帳」業務における 個人情報業務登録票(2018.3.12)	「住民基本台帳」業務における 個人情報業務登録票(2019.2.19)	事後	
令和2年9月30日	II 特定個人情報ファイルの概要 5 特定個人情報の提供・移転(委託に伴うものを除く。)		移転先18 学校教育部学務課	事後	
令和2年9月30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	現存者については消去しない。住民基本台帳法に基づき、消除者については消除後5年経過後に消去する。	現存者については消去しない。住民基本台帳法に基づき、消除者については、消除後150年経過後に消去する。	事後	
令和2年9月30日	III リスク対策(プロセス) 7 特定個人情報の保管・消去 ⑩死者の個人番号 具体的な保管方法	住民基本台帳においては死者も住民票の除票として管理することとなるため、現存者と同様の保管としている。	生存する個人の個人番号とともに、死亡による消除後、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。	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和2年9月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク3:従業員が事務外で使用するリスク リスクに対する措置の内容	(省略) <その他の措置の内容> ・委託先については契約時に情報セキュリティ確保・個人情報保護のための特記仕様書を添付している。 (省略)	(省略) <その他の措置の内容> ・委託に際しては、契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付している。 (省略)	事後	重要な変更に該当しない項目 の変更であるため、事前の提出・公表が義務付けられない
令和2年9月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 4. 特定個人情報ファイルの 取扱いの委託 情報保護管理体制の確認	(省略) ・委託先については契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を添付し、町田市個人情報保護条例、町田市セキュリティポリシーを遵守させている。	(省略) ・委託先には契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付し、町田市個人情報保護条例、町田市セキュリティポリシーを遵守させている。	事後	重要な変更に該当しない項目 の変更であるため、事前の提出・公表が義務付けられない
令和2年9月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 4. 特定個人情報ファイルの 取扱いの委託 委託契約書中の特定個人情報 ファイルの取扱いに関する 規定 規定の内容	委託先については契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を添付し、町田市個人情報保護条例、町田市セキュリティポリシーを遵守させている。 (省略)	委託先には契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付し、町田市個人情報保護条例、町田市セキュリティポリシーを遵守させている。 (省略)	事後	重要な変更に該当しない項目 の変更であるため、事前の提出・公表が義務付けられない
令和3年2月26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	<提供ができる根拠規定> 番号法第19条第7号別表第二(第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, 77, 80, 84, 89, 91, 92, 94, 96, 101, 102, 103, 105, 106, 108, 111, 112, 113, 114, 116, 117, 120項) 行政手続きにおける特定の個人を識別するための番号の利用等に関する法律別表第二の主務省令で定める事務及び情報を定める命令 (省略) <照会ができる根拠規定> 該当なし	<提供ができる根拠規定> 番号法第19条第7号別表第二のうち、第三欄(情報提供者)が「市町村長」の項で第四欄(特定個人情報)に「住民票関係情報」が含まれる項(第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, 92, 89, 91, 92, 94, 96, 97, 101, 102, 103, 105, 106, 108, 111, 112, 113, 114, 116, 117, 120項) <照会ができる根拠規定> 該当なし	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4年2月15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	(省略) ①個人を単位とする住民票を世帯ごとに編成し、住民基本台帳を作成 ②転入届、転居届、転出届、世帯変更届等の届出又は職権に基づく住民票の記載、消除又は記載の修正 ③住民基本台帳の正確な記録を確保するための措置 ④転入届に基づき住民票の記載をした際の転出元市町村に対する通知 ⑤本人又は同一の世帯に属する者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住民基本台帳の一部の写しの閲覧 ⑫他市町村からの通知の受理と他市町村への通知 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通知カード及び個人番号カード並びに情報提供ネットワークシステムによる特定個人情報の提供等に関する省令(平成26年11月20日総務省令第85号)第35条(通知カード、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。	(省略) ①個人を単位とする住民票を世帯ごとに編成し、住民基本台帳を作成 ②転入届、転居届、転出届、世帯変更届等の届出又は職権に基づく住民票の記載、消除又は記載の修正 ③住民基本台帳の正確な記録を確保するための措置 ④転入届に基づき住民票の記載をした際の転出元市町村に対する通知 ⑤本人又は同一の世帯に属する者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 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)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	
令和4年2月15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実務実施上の必要性	(省略) (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カード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))。通知カード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、機構に通知カード及び交付申請書の送付先情報を提供する。 (通知カード及び個人番号カード省令第35条(通知カード、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。)	(省略) (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個人番号通知書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))。個人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。)	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4年2月15日	I 基本情報 5. 個人番号の利用 法令上の根拠	(省略) 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(本人等の請求によ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)	(省略) 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(本人等の請求によ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15条の2(除票簿) ・第15条の3(除票の記載事項) ・第15条の4(除票の写し等の交付) ・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)	事後	
令和4年2月15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	<提供ができる根拠規定> 番号法第19条第7号別表第二のうち、第三欄(情報提供者)が「市町村長」の項で第四欄(特定個人情報)に「住民票関係情報」が含まれる項(第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, 106, 108, 111, 112, 113, 114, 116, 117, 120項) <照会ができる根拠規定> 該当なし	<提供ができる根拠規定> 番号法第19条第8号別表第二のうち、第三欄(情報提供者)が「市町村長」の項で第四欄(特定個人情報)に「住民票関係情報」が含まれる項(第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項) <照会ができる根拠規定> 該当なし	事後	
令和4年2月15日	II 特定個人情報ファイルの概要 ファイル名:住民基本台帳ファイル 2. 基本情報 ③その必要性	住民に関する記録を正確かつ統一に行うことにより、住民の居住関係の公証、その他の住民に関する事務の処理の基礎とするとともに、住民の住所に関する届出等の簡素化及び住民に関する記録の適正な管理を図り住民の利便を増進するため。 (住基法第1条より抜粋)	住基法第7条の住民基本台帳の記載事項であるため。 番号法第7条、第17条による個人番号の指定及び通知、個人番号カードの交付を行う上で必要となるため。	事後	
令和4年2月15日	II 特定個人情報ファイルの概要 ファイル名:住民基本台帳ファイル 3. 特定個人情報の入手・使用 ①入手元 その他	地方公共団体情報システム機構	行政機関・独立行政法人等	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4年2月15日	Ⅱ 特定個人情報ファイルの概要>ファイル名:住民基本台帳ファイル 3. 特定個人情報の入手・使用 ⑧使用方法	・住民基本台帳の記載 ・住民基本台帳の修正 ・住民基本台帳の削除 ・住民基本台帳に基づく住民票の写しの発行 ・個人番号の指定と通知カードの発行 ・個人番号カードの発行 ・住民基本台帳ネットワークシステムによる本人確認情報の送信、個人番号の取得、符号の取得要求及び通知カード送付先情報	・住民基本台帳の記載 ・住民基本台帳の修正 ・住民基本台帳の削除 ・住民基本台帳に基づく住民票の写しの発行 ・個人番号の指定と個人番号通知書の発行 ・個人番号カードの発行 ・住民基本台帳ネットワークシステムによる本人確認情報の送信、個人番号の取得、符号の取得要求及び通知カード送付先情報	事後	
令和4年2月15日	Ⅱ 特定個人情報ファイルの概要 ファイル名:住民基本台帳ファイル 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ⑥委託先名	富士通株式会社 多摩支店	富士通Japan株式会社 多摩支店	事後	
令和4年2月15日	Ⅱ 特定個人情報ファイルの概要 ファイル名:住民基本台帳ファイル 4. 特定個人情報ファイルの取扱いの委託 委託事項4 ⑥委託先名	富士ゼロックスシステムサービス株式会社	富士フイルムシステムサービス株式会社	事後	
令和4年2月15日	Ⅱ 特定個人情報ファイルの概要>ファイル名:住民基本台帳ファイル 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 ①～③	番号法第19条第7号別表第2	番号法第19条第8号別表第2	事後	
令和4年2月15日	Ⅱ 特定個人情報ファイルの概要>ファイル名:送付先情報ファイル 2. 基本情報 ③その必要性	番号法第7条第2項(指定及び通知)に基づき、通知カードを個人番号の付番対象者全員に送付する必要がある。 また、同法第17条第1項(個人番号カードの交付等)により、個人番号カードは通知カードと引き換えに交付することとされていることから、合わせて、交付申請書を通知カード送付者全員に送付する必要がある。市町村は、通知カード及び個人番号カード省令第35条(通知カード、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、通知カードを個人番号の付番対象者全員に送付する必要がある。 また、通知カード所有者にあっては、個人番号カードは通知カードと引き換えに交付することとされている。市町村は、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。	事後	
令和4年2月15日	Ⅱ 特定個人情報ファイルの概要>ファイル名:送付先情報ファイル 2. 基本情報 ④記録される項目 主な記録項目 その他	通知カード及び交付申請書の送付先情報	個人番号通知書及び交付申請書の送付先情報	事後	
令和4年2月15日	Ⅱ 特定個人情報ファイルの概要>ファイル名:送付先情報ファイル 2. 基本情報 ④記録される項目 その妥当性 その他	(省略) ・その他(通知カード及び交付申請書の送付先の情報) :機構に対し、通知カード及び個人番号カード省令第35条(通知カード、個人番号カード関連事務の委任)に基づき通知カード及び交付申請書の印刷、送付並びに個人番号カードの発行を委任するために、個人番号カードの券面記載事項のほか、通知カード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。	(省略) ・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。	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4年2月15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 ③入手の時期・頻度	使用開始日から通知カード送付までの一定の期間に、番号法施行日時点における住民の送付先情報をまとめて入手する（以降、新たに個人番号の通知対象者が生じた都度入手する）。	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入手する（以降、新たに個人番号の通知対象者が生じた都度入手する）。	事後	
令和4年2月15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 ⑤本人への明示	通知カード及び個人番号カード省令第35条（通知カード、個人番号カード関連事務の委任）	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）	事後	
令和4年2月15日	Ⅱ 特定個人情報ファイルの概要＞ファイル名：送付先情報ファイル 3. 特定個人情報の入手・使用 ⑤使用目的	通知カード及び個人番号カード省令第35条（通知カード、個人番号カード関連事務の委任）に基づく委任を受けて通知カード及び交付申請書の印刷、送付並びに個人番号カードの発行を行う機構に対し、通知カード及び交付申請書の送付先情報を提供するため。	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。	事後	
令和4年2月15日	Ⅱ 特定個人情報ファイルの概要＞ファイル名：送付先情報ファイル 3. 特定個人情報の入手・使用 ⑧使用方法	・既存住基システムより個人番号の通知対象者の情報を抽出し、通知カード及び交付申請書等の印刷及び送付に係る事務を通知カード及び個人番号カード省令第35条（通知カード、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→市町村CS又は電子記録媒体→個人番号カード管理システム（機構））。	・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、個人番号カード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。（既存住基システム→市町村CS又は電子記録媒体→個人番号カード管理システム（機構））。	事後	
令和4年2月15日	Ⅱ 特定個人情報ファイルの概要＞ファイル名：送付先情報ファイル 5. 特定個人情報の提供・移転 提供先1 ①法令上の根拠	通知カード及び個人番号カード省令第35条（通知カード、個人番号カード関連事務の委任）	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）	事後	
令和4年2月15日	Ⅱ 特定個人情報ファイルの概要＞ファイル名：送付先情報ファイル 5. 特定個人情報の提供・移転 提供先1 ②提出先における用途	市町村から通知カード及び個人番号カード省令第35条（通知カード、個人番号カード関連事務の委任）に基づく委任を受け、通知カード及び交付申請書を印刷し、送付する。	市町村から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。	事後	
令和4年2月15日	Ⅱ 特定個人情報ファイルの概要＞ファイル名：送付先情報ファイル 5. 特定個人情報の提供・移転 提供先1 ⑦時期・頻度	使用開始日から通知カード送付までの一定の期間に、番号法施行日時点における住民の送付先情報をまとめて提供する。（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）。	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）。	事後	
令和4年2月15日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7 特定個人情報の保管・消去 ⑩死者の個人番号 消去手順 手順の内容	・住民基本台帳ファイルに記録されたデータのうち、住民票の削除後5年を経過したデータをシステムにて判別し消去する。 ・消去処理の実施後、抹消されていることを確認する。 （省略）	システム上、住民基本台帳法施行令第34条第2項（保存）に定める期間（150年間）を経過した住民票の記載の修正前の本人確認情報（履歴情報）及び消除者の本人確認情報を消去する仕組みとする。 （省略）	事後	
令和4年2月15日	別表1	番号法第19条第7号	番号法第19条第8号	事後	
令和5年3月15日	1 基本情報 2. 特定個人情報ファイルを取り扱う業務において使用するシステム システム1③他のシステムとの接続	住民基本台帳ネットワークシステム 宛名システム等	住民基本台帳ネットワークシステム 宛名システム等 その他 申請管理システム	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3月15日	I 基本情報 2. 特定個人情報ファイルを取り扱う業務において使用するシステム2 ②システムの機能	3. 個人番号カードを利用した転入（特例転入）処理機能 転入の届出を受け付けた際に、あわせて個人番号カードが提示された場合、当該個人番号カードを用いて転入処理を行う。	3. 個人番号カードを利用した転入（特例転入）処理機能 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。）。	事後	
令和5年3月15日	I 基本情報 2. 特定個人情報ファイルを取り扱う業務において使用するシステム6①システムの名称		申請管理システム	事後	
令和5年3月15日	I 基本情報 2. 特定個人情報ファイルを取り扱う業務において使用するシステム6②システムの機能追加		本システムの主な機能は次のとおり。 1 オンライン申請情報の取得機能 ・サービス検索・電子申請機能からのオンライン申請情報を取得する機能 2 オンライン申請情報の管理機能 ・オンライン申請情報を一元管理する機能 3 業務システムとの連携機能 ・オンライン申請情報を業務システムへ連携する機能	事後	
令和5年3月15日	I 基本情報 2. 特定個人情報ファイルを取り扱う業務において使用するシステム6③他のシステムとの接続		既存住民基本台帳システム その他 サービス検索・電子申請機能	事後	
令和5年3月15日	I 基本情報 2. 特定個人情報ファイルを取り扱う業務において使用するシステム7①システムの名称		サービス検索・電子申請機能	事後	
令和5年3月15日	I 基本情報 2. 特定個人情報ファイルを取り扱う業務において使用するシステム7②システムの機能		本システムの主な機能は次のとおり。 1 住民向け機能 ・市民が、自身の受けられるサービスを検索し、申請できる機能 2 地方公共団体向け機能 ・地方自治体が、市民の申請データを、画面で確認または受信できる機能	事後	
令和5年3月15日	I 基本情報 2. 特定個人情報ファイルを取り扱う業務において使用するシステム7③他のシステムとの接続		その他 申請管理システム	事後	
令和5年3月15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	住民基本台帳ネットワークシステム、LGWAN等	住民基本台帳ネットワークシステム、LGWAN等、サービス検索・電子申請機能	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11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 (住民基本台帳ファイル)	<コンピュータ室における措置> 町田市情報セキュリティポリシーにより規定 ・施設案内を最小限の表示としている。 ・不正侵入者等の防止として、常時施錠し、必要の都度、開閉している。 ・入退室者の登録管理を行っている。 ・入室者は、常時、名札を着用させている。 ・機器等への未承認のアクセス(操作、触れる等)を禁止している。 ・室内の撮影等を禁止している。 ・危険物等(機器の動作に影響を与えるおそれのある通信機器を含む)の持ち込みを禁止している。 設備状況 ・施錠管理できるサーバラック、監視カメラ、冗長化電源設備、無停電電源装置、非常用電源、専用空調設備、消火設備等。 <事務室における措置> 町田市情報セキュリティポリシーにより規定 ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・立ち入りを承認する場合は入退管理をしている。 ・入退室管理簿を記載している。 ・来客者用名札を着用させている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)を使用している。	<事務室における措置> 町田市情報セキュリティポリシーにより規定 ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・立ち入りを承認する場合は入退管理をしている。 ・入退室管理簿を記載している。 ・来客者用名札を着用させている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)を使用している。 <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・プラットフォームはデータセンターに設置している。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ②特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。	事後	
		(続き) <中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームはデータセンターに設置している。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ②特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。	(続き) <クラウド環境における措置> ①サーバー等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAP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。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。		

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11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 (本人確認情報ファイル) (送付先情報ファイル)	<コンピュータ室における措置> 町田市情報セキュリティポリシーにより規定 ・施設案内を最小限の表示としている。 ・不正侵入者等の防止として、常時施錠し、必要の都度、開閉している。 ・入退室者の登録管理を行っている。 ・入室者は、常時、名札を着用させている。 ・機器等への未承認のアクセス(操作、触れる等)の禁止している。 ・室内の撮影等の禁止している。 ・危険物等(機器の動作に影響を与えるおそれのある通信機器を含む)の持ち込み禁止している。 設備状況 ・施錠管理できるサーバラック、監視カメラ、冗長化電源設備、無停電電源装置、非常用電源、専用空調設備、消火設備等。 <事務室における措置> 町田市情報セキュリティポリシーにより規定 ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・立ち入りを承認する場合は入退管理をしている。 ・入退室管理簿を記載している。 ・来客者用名札を着用させている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)を使用している。	<事務室における措置> 町田市情報セキュリティポリシーにより規定 ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・立ち入りを承認する場合は入退管理をしている。 ・入退室管理簿を記載している。 ・来客者用名札を着用させている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)を使用している。 <クラウド環境における措置> ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAP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。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップは同じデータセンター内の本番環境とは別のサーバー内に保存される。	事後	
令和5年11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消去方法 (住民基本台帳ファイル)	・データベースに登録されたデータのうち、法定保存年限を経過したデータをシステムにて判別し消去する。 町田市情報セキュリティポリシーにより規定 ・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。 ・紙媒体は、シュレッダーによる破砕、溶解、焼却等の情報の復元不能化処理を行っている。 <中間サーバー・プラットフォームにおける措置> ①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、物理的破壊または専用ソフト等を利用して完全に消去する。	・データベースに登録されたデータのうち、法定保存年限を経過したデータをシステムにて判別し消去する。 町田市情報セキュリティポリシーにより規定 ・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。 ・紙媒体は、シュレッダーによる破砕、溶解、焼却等の情報の復元不能化処理を行っている。 <中間サーバー・プラットフォームにおける措置> ①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、物理的破壊または専用ソフト等を利用して完全に消去する。	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
			(続き) ＜クラウド環境における措置＞ 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。地方公共団体の業務データは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許可なく消去することはない。 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等に準拠した事業者が定める消去プロセスにしたがって確実にデータを消去する。 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クラウド環境へ移行することになる。この移行に際しては、システム基盤運用事業者がデータ抽出及び利用しなくなった環境の消去等を実施し、開発事業者がクラウド環境へのデータ投入等を実施する。		
令和5年11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消去方法 (本人確認情報ファイル)	・本人確認情報ファイルに記録されたデータをシステムにて自動判別し消去する。 町田市情報セキュリティポリシーにより規定 ・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。 ・紙媒体は、シュレッダーによる破碎、溶解、焼却等の情報の復元不能化処理を行っている。	・本人確認情報ファイルに記録されたデータをシステムにて自動判別し消去する。 町田市情報セキュリティポリシーにより規定 ・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。 ・紙媒体は、シュレッダーによる破碎、溶解、焼却等の情報の復元不能化処理を行っている。 ＜クラウド環境における措置＞ 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。地方公共団体の業務データは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許可なく消去することはない。 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等に準拠した事業者が定める消去プロセスにしたがって確実にデータを消去する。 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クラウド環境へ移行することになる。この移行に際しては、システム基盤運用事業者がデータ抽出及び利用しなくなった環境の消去等を実施し、開発事業者がクラウド環境へのデータ投入等を実施する。	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11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消去方法 (送付先情報ファイル)	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。 町田市情報セキュリティポリシーにより規定 ・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。 ・紙媒体は、シュレッダーによる破碎、溶解、焼却等の情報の復元不能化処理を行っている。	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。 町田市情報セキュリティポリシーにより規定 ・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。 ・紙媒体は、シュレッダーによる破碎、溶解、焼却等の情報の復元不能化処理を行っている。 ＜クラウド環境における措置＞ 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。地方公共団体の業務データは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許可なく消去することはない。 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等に準拠した事業者が定める消去プロセスにしたがって確実にデータを消去する。 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クラウド環境へ移行することになる。この移行に際しては、システム基盤運用事業者がデータ抽出及び利用しなくなった環境の消去等を実施し、開発事業者がクラウド環境へのデータ投入等を実施する。	事後	
令和5年11月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用リスク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 (住民基本台帳ファイル)	・端末は記録媒体が接続できない仕様になっている。 ・端末はインターネット接続ができない仕様になっている。 ・特定個人情報を回線を通じて入手する場合は、他のシステムからのアクセスが行えない専用回線を用いている。 町田市情報セキュリティポリシーにより規定 ＜コンピュータ室における措置＞ ・施設案内を最小限の表示としている。 ・不正侵入者等の防止として、常時施錠し、必要の都度、開閉している。 ・入退室者の登録管理を行っている。 ・入室者は、常時、名札を着用させている。 ・機器等への未承認のアクセス(操作、触れる等)を禁止している。 ・室内の撮影等を禁止している。 ・危険物等(機器の動作に影響を与えるおそれのある通信機器を含む)の持ち込みを禁止している。 設備状況 ・施錠管理できるサーバラック、監視カメラ、冗長化電源設備、無停電電源装置、非常用電源、専用空調設備、消火設備等。 ＜事務室における措置＞ ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。	・端末は記録媒体が接続できない仕様になっている。 ・端末はインターネット接続ができない仕様になっている。 ・特定個人情報を回線を通じて入手する場合は、他のシステムからのアクセスが行えない専用回線を用いている。 町田市情報セキュリティポリシーにより規定 ＜事務室における措置＞ ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)を使用している。	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
		(続き) ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)を使用している。 <アクセス制御> ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。	(続き) <アクセス制御> ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト(ログオフ)、画面表示を起動初期状態(情報の検索結果などが表示されていない状態)にする等。		
		(続き) ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト(ログオフ)、画面表示を起動初期状態(情報の検索結果などが表示されていない状態)にする等。 <その他の措置> ・委託に際しては、契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付している。 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 ・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。 ・情報セキュリティ内部監査員を養成するための教育をしている。 ・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行う。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施する。	(続き) <その他の措置> ・委託に際しては、契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付している。 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 ・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。 ・情報セキュリティ内部監査員を養成するための教育をしている。 ・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行う。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施する。		

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11月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク3:従業員が事務外で使用するリスク リスクに対する措置の内容 (本人確認情報ファイル)	・端末は記録媒体が接続できない仕様になっている。 ・端末はインターネット接続ができない仕様になっている。 ・特定個人情報を回線を通じて入手する場合は、他のシステムからのアクセスが行えない専用回線を用いている。 町田市情報セキュリティポリシーにより規定 ＜コンピュータ室における措置＞ ・施設案内を最小限の表示としている。 ・不正侵入者等の防止として、常時施錠し、必要の都度、開閉している。 ・入退室者の登録管理を行っている。 ・入室者は、常時、名札を着用させている。 ・機器等への未承認のアクセス(操作、触れる等)を禁止している。 ・室内の撮影等を禁止している。 ・危険物等(機器の動作に影響を与えるおそれのある通信機器を含む)の持ち込みを禁止している。 設備状況 ・施設管理できるサーバラック、監視カメラ、冗長化電源設備、無停電電源装置、非常用電源、専用空調設備、消火設備等。 ＜事務室における措置＞ ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。	・端末は記録媒体が接続できない仕様になっている。 ・端末はインターネット接続ができない仕様になっている。 ・特定個人情報を回線を通じて入手する場合は、他のシステムからのアクセスが行えない専用回線を用いている。 町田市情報セキュリティポリシーにより規定 ＜事務室における措置＞ ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)を使用している。	事後	
		(続き) ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)を使用している。 ＜アクセス制御＞ ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時においては、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。	(続き) ＜アクセス制御＞ ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時においては、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト(ログオフ)、画面表示を起動初期状態(情報の検索結果などが表示されていない状態)にする等。		

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
		(続き) ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト(ログオフ)、画面表示を起動初期状態(情報の検索結果などが表示されていない状態)にする等。 <その他の措置> ・委託先については契約時に情報セキュリティ確保・個人情報保護のための特記仕様書を添付している。 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 ・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。 ・情報セキュリティ内部監査員を養成するための教育をしている。 ・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行う。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施する。	(続き) <その他の措置> ・委託先については契約時に情報セキュリティ確保・個人情報保護のための特記仕様書を添付している。 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 ・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。 ・情報セキュリティ内部監査員を養成するための教育をしている。 ・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行う。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施する。		
令和5年11月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク3:従業員が事務外で使用するリスク リスクに対する措置の内容 (送付先情報ファイル)	町田市情報セキュリティポリシーにより規定 <コンピュータ室における措置> ・施設案内を最小限の表示としている。 ・不正侵入者等の防止として、常時施錠し、必要の都度、開閉している。 ・入退室者の登録管理を行っている。 ・入室者は、常時、名札を着用させている。 ・機器等への未承認のアクセス(操作、触れる等)を禁止している。 ・室内の撮影等を禁止している。 ・危険物等(機器の動作に影響を与えるおそれのある通信機器を含む)の持ち込みを禁止している。 設備状況 ・施錠管理できるサーバラック、監視カメラ、冗長化電源設備、無停電電源装置、非常用電源、専用空調設備、消火設備等。 <事務室における措置> ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)を使用している。	町田市情報セキュリティポリシーにより規定 <事務室における措置> ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)を使用している。	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
		(続き) ＜アクセス制御＞ ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時においては、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト(ログオフ)、画面表示を起動初期状態(情報の検索結果などが表示されていない状態)にする等。	(続き) ＜アクセス制御＞ ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時においては、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト(ログオフ)、画面表示を起動初期状態(情報の検索結果などが表示されていない状態)にする等。		
		(続き) ＜その他の措置＞ ・委託先については契約時に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付している。 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 ・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。 ・情報セキュリティ内部監査員を養成するための教育をしている。 ・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行う。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施する。	(続き) ＜その他の措置＞ ・委託先については契約時に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付している。 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 ・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。 ・情報セキュリティ内部監査員を養成するための教育をしている。 ・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行う。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施する。		

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11月1日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク 対策 7. 特定個人情報の保管・消 去 ⑤物理的対策 具体的な対策の内容 (住民基本台帳ファイル)	町田市情報セキュリティポリシーにより規定 ＜コンピュータ室における措置＞ ・施設案内を最小限の表示としている。 ・不正侵入者等の防止として、常時施錠し、必 要の都度、開閉している。 ・入退室者の登録管理を行っている。 ・入室者は、常時、名札を着用させている。 ・機器等への未承認のアクセス(操作、触れる 等)を禁止している。 ・室内の撮影等を禁止している。 ・危険物等(機器の動作に影響を与えるおそれ のある通信機器を含む)の持ち込みを禁止して いる。 設備状況 ・施錠管理できるサーバラック、監視カメラ、冗 長化電源設備、無停電電源装置、非常用電 源、専用空調設備、消火設備等。 ＜事務室における措置＞ ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室 管理簿への記載や、来客者用名札の着用等によ り、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管 し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン 等)を使用している。	町田市情報セキュリティポリシーにより規定 ＜事務室における措置＞ ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室 管理簿への記載や、来客者用名札の着用等によ り、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管 し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン 等)を使用している。 ＜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。 ②事前に申請し承認されてない物品、記憶媒 体、通信機器などを不正に所持し、持出持込す ることがな いよう、警備員などにより確認している。	事後	
		(続き) ＜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。 ②事前に申請し承認されてない物品、記憶媒 体、通信機器などを不正に所持し、持出持込す ることがな いよう、警備員などにより確認している。	(続き) ＜クラウド環境における措置＞ ①クラウド事業者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、以下 の入退室管理策を行っている。 ・関係者以外立ち入り禁止等を表示しており、 警備員等を配置している。 ・職員および立ち入りの承認を受けた者は、生 体認証による入退室管理を行っている。 ・職員以外の立ち入りについては入退室管理 簿を記載している。 ②事前に申請し承認されてない物品、記憶媒 体、通信機器などを不正に所持し、持出持込す ることがないよう、金属探知機などにより確認し ている。		

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11月1日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 ⑤ 物理的対策 具体的な対策の内容 (本人確認情報ファイル) (送付先情報ファイル)	町田市情報セキュリティポリシーにより規定 ＜コンピュータ室における措置＞ ・施設案内を最小限の表示としている。 ・不正侵入者等の防止として、常時施錠し、必要の都度、開閉している。 ・入退室者の登録管理を行っている。 ・入室者は、常時、名札を着用させている。 ・機器等への未承認のアクセス(操作、触れる等)を禁止している。 ・室内の撮影等を禁止している。 ・危険物等(機器の動作に影響を与えるおそれのある通信機器を含む)の持ち込みを禁止している。 設備状況 ・施錠管理できるサーバラック、監視カメラ、冗長化電源設備、無停電源装置、非常用電源、専用空調設備、消火設備等。 ＜事務室における措置＞ ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)を使用している。	町田市情報セキュリティポリシーにより規定 ＜事務室における措置＞ ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)を使用している。 ①クラウド事業者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、以下の入退室管理策を行っている。 ・関係者以外立ち入り禁止等を表示しており、警備員等を配置している。 ・職員および立ち入りの承認を受けた者は、生体認証による入退室管理を行っている。 ・職員以外の立ち入りについては入退室管理簿を記載している。 ②事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、金属探知機などにより確認している。	事後	
令和5年11月1日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 ⑥ 技術的対策 具体的な対策の内容 (住民基本台帳ファイル)	・端末は記録媒体が接続できない仕様にしている。 ・端末はインターネット接続ができない仕様にしている。 ・特定個人情報を回線により入手する場合は、他のシステムからのアクセスが行えない専用回線を用いている。 町田市情報セキュリティポリシーにより規定 ・ウイルス対策ソフトを導入している。 ・ウイルス対策の対象は、サーバ、クライアント(端末)及びゲートウェイを含めた、包括的な対策を講じている。 ・常に最新のウイルス定義ファイル(パターンファイル)を使用している。 ・定期的にウイルス対策の実施状況を確認している。 ・インターネット等外部ネットワークとは分離し、不正アクセス防止をしている。 ・外部接続(インターネット接続を含む)におけるアクセス制御に関する管理策として、ファイアウォールやルータを設置している。 ・ハードウェア及びソフトウェアには、セキュリティ修正プログラムを適用している。 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。	・端末は記録媒体が接続できない仕様にしている。 ・端末はインターネット接続ができない仕様にしている。 ・特定個人情報を回線により入手する場合は、他のシステムからのアクセスが行えない専用回線を用いている。 町田市情報セキュリティポリシーにより規定 ・ウイルス対策ソフトを導入している。 ・ウイルス対策の対象は、サーバ、クライアント(端末)及びゲートウェイを含めた、包括的な対策を講じている。 ・常に最新のウイルス定義ファイル(パターンファイル)を使用している。 ・定期的にウイルス対策の実施状況を確認している。 ・インターネット等外部ネットワークとは分離し、不正アクセス防止をしている。 ・外部接続(インターネット接続を含む)におけるアクセス制御に関する管理策として、ファイアウォールやルータを設置している。 ・ハードウェア及びソフトウェアには、セキュリティ修正プログラムを適用している。 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。	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
		(続き) ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト(ログオフ)、画面表示を起動初期状態(情報の検索結果などが表示されていない状態)にする等 <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。	(続き) ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト(ログオフ)、画面表示を起動初期状態(情報の検索結果などが表示されていない状態)にする等 <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。		
			(続き) <クラウド環境における措置> ①クラウド事業者は利用者のデータに許可なくアクセスしない契約等となっている。 ②クラウド事業者は、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。 ③クラウド事業者は、クラウド環境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。 ④クラウド事業者は、クラウド環境に対し、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。 ⑤クラウド事業者は、クラウド環境に導入している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。 ⑥クラウド環境の特定個人情報保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦クラウド事業者の運用保守地点からクラウド環境への接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、クラウド事業者が許可なくアクセスできないよう対策を講じる。		

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11月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 ⑥ 技術的対策 具体的な対策の内容 (本人確認情報ファイル) (送付先情報ファイル)	・端末は記録媒体が接続できない仕様になっている。 ・端末はインターネット接続ができない仕様になっている。 ・特定個人情報回線を回線により入手する場合は、他のシステムからのアクセスが行えない専用回線を用いている。 町田市情報セキュリティポリシーにより規定 ・ウイルス対策ソフトを導入している。 ・ウイルス対策の対象は、サーバ、クライアント(端末)及びゲートウェイを含めた、包括的な対策を講じている。 ・常に最新のウイルス定義ファイル(パターンファイル)を使用している。 ・定期的にウイルス対策の実施状況を確認している。 ・インターネット等外部ネットワークとは分離し、不正アクセス防止をしている。 ・外部接続(インターネット接続を含む)におけるアクセス制御に関する管理策として、ファイアウォールやルータを設置している。 ・ハードウェア及びソフトウェアには、セキュリティ修正プログラムを適用している。 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。	・端末は記録媒体が接続できない仕様になっている。 ・端末はインターネット接続ができない仕様になっている。 ・特定個人情報回線を回線により入手する場合は、他のシステムからのアクセスが行えない専用回線を用いている。 町田市情報セキュリティポリシーにより規定 ・ウイルス対策ソフトを導入している。 ・ウイルス対策の対象は、サーバ、クライアント(端末)及びゲートウェイを含めた、包括的な対策を講じている。 ・常に最新のウイルス定義ファイル(パターンファイル)を使用している。 ・定期的にウイルス対策の実施状況を確認している。 ・インターネット等外部ネットワークとは分離し、不正アクセス防止をしている。 ・外部接続(インターネット接続を含む)におけるアクセス制御に関する管理策として、ファイアウォールやルータを設置している。 ・ハードウェア及びソフトウェアには、セキュリティ修正プログラムを適用している。 ・システムや端末利用者を識別するアカウントの管理を行う。	事後	
		(続き) ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る。パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト(ログオフ)、画面表示を起動初期状態(情報の検索結果などが表示されていない状態)にする等	(続き) ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る。パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト(ログオフ)、画面表示を起動初期状態(情報の検索結果などが表示されていない状態)にする等		

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
			(続き) ＜クラウド環境における措置＞ ①クラウド事業者は利用者のデータに許可なくアクセスしない契約等となっている。 ②クラウド事業者は、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。 ③クラウド事業者は、クラウド環境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。 ④クラウド事業者は、クラウド環境に対し、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。 ⑤クラウド事業者は、クラウド環境に導入している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。 ⑥クラウド環境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。 ⑦クラウド事業者の運用保守地点からクラウド環境への接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、クラウド事業者が許可なくアクセスできないよう対策を講じる。		
令和5年11月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 消去手順 手順の内容 (住民基本台帳ファイル) (本人確認情報ファイル)	システム上、住民基本台帳法施行令第34条第2項(保存)に定める期間(150年間)を経過した住民票の記載の修正前の本人確認情報(履歴情報)及び消除者の本人確認情報を消去する仕組みとする。 町田市情報セキュリティポリシーにより規定 ・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。 ・紙媒体は、シュレッダーによる破碎、溶解、焼却等の情報の復元不能化処理を行っている。 ・情報資産の廃棄時には、必要に応じ、廃棄日時、廃棄担当者、処理内容を記録している。	システム上、住民基本台帳法施行令第34条第2項(保存)に定める期間(150年間)を経過した住民票の記載の修正前の本人確認情報(履歴情報)及び消除者の本人確認情報を消去する仕組みとする。 町田市情報セキュリティポリシーにより規定 ・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。 ・紙媒体は、シュレッダーによる破碎、溶解、焼却等の情報の復元不能化処理を行っている。 ・情報資産の廃棄時には、必要に応じ、廃棄日時、廃棄担当者、処理内容を記録している。 ＜クラウド事業者における措置＞ 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、事業者の定めたプロセスにしたがって確実にデータを消去する。	事後	
令和5年11月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 消去手順 手順の内容 (送付先情報ファイル)	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。	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。 ＜クラウド事業者における措置＞ 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、事業者の定めたプロセスにしたがって確実にデータを消去する。	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5年11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	町田市情報セキュリティポリシーにより規定 ・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行っている。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施している。 ＜中間サーバー・プラットフォームにおける措置＞ ①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。	町田市情報セキュリティポリシーにより規定 ・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行っている。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施している。 ＜中間サーバー・プラットフォームにおける措置＞ ①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。 ＜クラウド環境における措置＞ クラウドサービス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、ISMAP監査機関リストに登録された監査機関による監査を受けることとしている。	事後	
令和5年11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、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。 ＜クラウド環境における措置＞ クラウド環境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開発事業者が責任を有する。クラウド環境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、原則としてクラウド環境に起因する事象の場合は、開発事業者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、クラウド環境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開発事業者が対応するものとする。 具体的な取扱いについて、疑義が生じる場合は、地方公共団体と開発事業者及び関係者で協議を行う。	事後	個人情報保護法施行に伴う、個人情報保護条例に係る記述の削除のため、重要な変更 に該当しない
令和5年11月1日	表紙 個人のプライバシー等の権利利益の保護の宣言 特記事項	町田市個人情報保護条例 第1条 この条例は、市民が自己に関する個人情報の主体であることにかんがみ、市民の自己に関する個人情報の開示、訂正、利用の中止等を求める権利を保障するとともに、個人情報の適正な取扱いを確保することにより個人情報の保護し、もって市民の基本的人権の擁護と、市民の信頼に裏付けられた人間尊重の市政を実現することを目的とする。	(削除)	事後	個人情報保護法施行に伴う、個人情報保護条例に係る記述の削除のため、重要な変更 に該当しない

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11月1日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 4. 特定個人情報ファイル の取扱いの委託 情報保護管理体制の確認 (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)	・委託先については契約書に「情報セキュリティ 確保・個人情報保護のための特記仕様書」を付 し、町田市個人情報保護条例、町田市セキュリ ティポリシーを遵守させている。	・委託先については契約書に「情報セキュリティ 確保・個人情報保護のための特記仕様書」を付 し、町田市セキュリティポリシーを遵守させてい る。	事後	個人情報保護法施行に伴う、 個人情報保護条例に係る記 述の削除のため、重要な変更 に該当しない
令和5年11月1日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 4. 特定個人情報ファイル の取扱いの委託 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 既定の内容 (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)	委託先には契約書に「情報セキュリティ確保・ 個人情報保護のための特記仕様書」を付し、町 田市個人情報保護条例、町田市セキュリティポ リシーを遵守させている。	委託先には契約書に「情報セキュリティ確保・ 個人情報保護のための特記仕様書」を付し、町 田市セキュリティポリシーを遵守させている。	事後	個人情報保護法施行に伴う、 個人情報保護条例に係る記 述の削除のため、重要な変更 に該当しない

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11月1日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 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。) 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 転に関するルール ルールの内容及びルー ル遵守の確認方法 (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)	磁気データの管理と取扱いに関する要領により 規定 第5 磁気データの利用 1 磁気データの処理を新たに行い、又は変更 するに当たり、他業務の磁気データを利用しよ うとする課(以下「データ利用課」という。)の情報 管理者は、データ保有課の情報管理者に対し、 磁気データの利用を申請して承諾を得なけれ ばならない。 2 データ利用課の情報管理者は、前項の承諾 を得た範囲内においてのみ、磁気データを利用 できる。 3 前項の規定により、個人情報に係る処理を 行うときは、町田市個人情報保護条例の規定 を遵守しなければならない。 町田市個人情報保護条例により規定 (目的外利用、外部提供の制限) 第13条 実施機関は、収集した保有個人情報 について、第7条第1項の規定により登録された 業務の目的の範囲を超えての利用(以下「目的 外利用」という。)及び市の機関以外のものへの 提供(以下「外部提供」という。)を行ってはな らない。 2 実施機関は、前項の規定にかかわらず、法 令に特別の定めがある場合又は正当な職務執 行に関連する場合で、審議会に諮問し、その答 申に基づき行うときは、目的外利用又は外部提 供を行うことができる。	磁気データの管理と取扱いに関する要領により 規定 第5 磁気データの利用 1 磁気データの処理を新たに行い、又は変更 するに当たり、他業務の磁気データを利用しよ うとする課(以下「データ利用課」という。)の情報 管理者は、データ保有課の情報管理者に対し、 磁気データの利用を申請して承諾を得なけれ ばならない。 2 データ利用課の情報管理者は、前項の承諾 を得た範囲内においてのみ、磁気データを利用 できる。	事後	個人情報保護法施行に伴う、 個人情報保護条例に係る記 述の削除のため、重要な変更 に該当しない
令和5年11月1日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 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。) 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 (住民基本台帳ファイル)	磁気データの管理と取扱いに関する要領により 規定 第5 磁気データの利用 1 磁気データの処理を新たに行い、又は変更 するに当たり、他業務の磁気データを利用しよ うとする課(以下「データ利用課」という。)の情報 管理者は、データ保有課の情報管理者に対し、 磁気データの利用を申請して承諾を得なけれ ばならない。 2 データ利用課の情報管理者は、前項の承諾 を得た範囲内においてのみ、磁気データを利用 できる。 3 前項の規定により、個人情報に係る処理を 行うときは、町田市個人情報保護条例の規定 を遵守しなければならない。 町田市個人情報保護条例により規定 (目的外利用、外部提供の制限) 第13条 実施機関は、収集した保有個人情報 について、第7条第1項の規定により登録された 業務の目的の範囲を超えての利用(以下「目的 外利用」という。)及び市の機関以外のものへの 提供(以下「外部提供」という。)を行ってはな らない。 2 実施機関は、前項の規定にかかわらず、法 令に特別の定めがある場合又は正当な職務執 行に関連する場合で、審議会に諮問し、その答 申に基づき行うときは、目的外利用又は外部提 供を行うことができる。	磁気データの管理と取扱いに関する要領により 規定 第5 磁気データの利用 1 磁気データの処理を新たに行い、又は変更 するに当たり、他業務の磁気データを利用しよ うとする課(以下「データ利用課」という。)の情報 管理者は、データ保有課の情報管理者に対し、 磁気データの利用を申請して承諾を得なけれ ばならない。 2 データ利用課の情報管理者は、前項の承諾 を得た範囲内においてのみ、磁気データを利用 できる。	事後	個人情報保護法施行に伴う、 個人情報保護条例に係る記 述の削除のため、重要な変更 に該当しない

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11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 (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)	・端末については、盗難防止具(鍵付チェーン等)を使用している。	・端末については、盗難防止具(鍵付チェーン等)の使用または鍵付キャビネットへの保管を行っている。	事後	事前に提出・公表済みの内容について詳細化した。
令和5年11月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 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4:入手の際に特定個人情報が漏えい・紛失するリスク リスクに対する措置の内容 (住民基本台帳ファイル)	・端末については、盗難防止具(鍵付チェーン等)を使用している。	・端末については、盗難防止具(鍵付チェーン等)の使用または鍵付キャビネットへの保管を行っている。	事後	事前に提出・公表済みの内容について詳細化した。
令和5年11月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 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 (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)	・端末については、盗難防止具(鍵付チェーン等)を使用している。	・端末については、盗難防止具(鍵付チェーン等)の使用または鍵付キャビネットへの保管を行っている。	事後	事前に提出・公表済みの内容について詳細化した。
令和5年11月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 消去手順 ⑤物理的対策 具体的な対策内容 (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)	・端末については、盗難防止具(鍵付チェーン等)を使用している。	・端末については、盗難防止対策を実施している。	事後	重要な変更該当しない項目の変更であるため、事前の提出・公表が義務付けられない
令和5年11月1日	(別添2)ファイル記録項目	別紙「個人情報業務登録票」及び「個人情報コンピュータ処理等登録票」のとおり	別紙「個人情報ファイル簿」のとおり	事後	重要な変更該当しない項目の変更であるため、事前の提出・公表が義務付けられない
令和5年11月1日	(別添2)ファイル記録項目(2)	「個人情報業務登録票」及び「個人情報コンピュータ処理等登録票」	「個人情報ファイル簿」	事後	重要な変更該当しない項目の変更であるため、事前の提出・公表が義務付けられない

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11月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4. 特定個人情報ファイルの取扱いの委託 委託契約書中の特定個人情報ファイルの取扱いに関する規定 規定の内容 (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)	13. 情報の取り扱いに関する教育の履行	13. 情報の取扱いに関する教育の履行	事後	表記揺らぎの修正
令和6年7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 (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)	<クラウド環境における措置> ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAP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。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップは同じデータセンター内の本番環境とは別のサーバー内に保存される。	<ガバメントクラウドにおける措置> ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAP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。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。	事後	
令和6年7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 (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)	<クラウド環境における措置> 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。地方公共団体の業務データは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許可なく消去することはない。 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等に準拠した事業者が定める消去プロセスにしたがって確実にデータを消去する。 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クラウド環境へ移行することになる。この移行に際しては、システム基盤運用事業者がデータ抽出及び利用しなくなった環境の消去等を実施し、開発事業者がクラウド環境へのデータ投入等を実施する。	<ガバメントクラウドにおける措置> 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。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。 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。 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。この移行に際しては、システム基盤運用事業者がデータ抽出及び利用しなくなった環境の消去等を実施し、開発事業者がクラウド環境へのデータ投入等を実施する。	事後	
令和6年7月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 ⑤物理的対策 具体的な対策の内容 (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)	<クラウド環境における措置> ①クラウド事業者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、以下の入退室管理策を行っている。 ・関係者以外立ち入り禁止等を表示しており、警備員等を配置している。 ・職員および立ち入りの承認を受けた者は、生体認証による入退室管理を行っている。 ・職員以外の立ち入りについては入退室管理簿を記載している。 ②事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、金属探知機などにより確認している。	<ガバメントクラウドにおける措置> ①ガバメントクラウドについては政府情報システムのセキュリティ制度 (ISMAP) のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された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。 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7月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 ⑥技術的対策 具体的な対策の内容 (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)	<クラウド環境における措置> ①クラウド事業者は利用者のデータに許可なくアクセスしない契約等となっている。 ②クラウド事業者は、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。 ③クラウド事業者は、クラウド環境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。 ④クラウド事業者は、クラウド環境に対し、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。 ⑤クラウド事業者は、クラウド環境に導入している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。 ⑥クラウド環境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。 ⑦クラウド事業者の運用保守地点からクラウド環境への接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、クラウド事業者が許可なくアクセスできないよう対策を講じる。	<ガバメントクラウドにおける措置> 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。 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。 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。 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。 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。 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。	事後	
令和6年7月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 消去手順 手順の内容 (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)	<クラウド事業者における措置> 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、事業者の定めたプロセスにしたがって確実にデータを消去する。	<ガバメントクラウドにおける措置> 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。	事後	
令和6年7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	<クラウド環境における措置> クラウドサービス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、ISMAP監査機関リストに登録された監査機関による監査を受けることとしている。	<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。	事後	
令和6年7月1日	Ⅳ その他のリスク対策 3. その他のリスク対策	<クラウド環境における措置> クラウド環境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開発事業者が責任を有する。 クラウド環境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、原則としてクラウド環境に起因する事象の場合は、開発事業者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、クラウド環境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開発事業者が対応するものとする。 具体的な取扱いについて、疑義が生じる場合は、地方公共団体と開発事業者及び関係者で協議を行う。	<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7年4月1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	(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)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)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	重要な変更に該当しない項目の変更であるため、事前の提出・公表が義務付けられない。
令和7年4月1日	(別添1)事務内容		別添1図のとおり 通知カードの削除 住基カードの削除 法務省通知 → 入管庁通知 法務省 → 出入国在留管理庁	事後	重要な変更に該当しない項目の変更であるため、事前の提出・公表が義務付けられない。
令和7年4月1日	(別添1)住基ネット		(注)図中に※が付されている箇所は、特定個人情報を含まない事務の流れを指す。	事後	重要な変更に該当しない項目の変更であるため、事前の提出・公表が義務付けられない。
令和7年4月1日	(別添1)住基ネット	備考 上記図は、市町村CSと機構を中心とした事務の流れである。上図の「市区町村」は「町田市」、「市区町村CS」(以下、市町村CSという。)は「町田市CS」を表している。 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。 (略) 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。 (略) 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市町村CSから既存住記システムに転出証明書情報を送信する。 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。	備考 上記図は、市町村CSと機構を中心とした事務の流れである。上図の「市区町村」は「町田市」、「市区町村CS」(以下、市町村CSという。)は「町田市CS」を表している。 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)。 (略) 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)。 (略) 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市町村CSから既存住記システムに転出証明書情報を送信する。 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。	事後	重要な変更に該当しない項目の変更であるため、事前の提出・公表が義務付けられない。

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7年4月1日		(続き) 3-④.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し、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.基本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。(略)	(続き) 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、個人番号又は基本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。(略)	事後	重要な変更に該当しない項目の変更であるため、事前の提出・公表が義務付けられない。
令和7年4月1日	(別添1) 中間サーバー	番号法別表第2	主務省令 第2条の表	事後	重要な変更に該当しない項目の変更であるため、事前の提出・公表が義務付けられない。
令和7年4月1日	I 基本情報 2. 特定個人情報ファイルを取り扱う業務において使用するシステム ①システムの機能 ②システムの機能	本システムの主な機能は次のとおり。 1. 住民基本台帳の記載機能 2. 住民基本台帳の修正機能 3. 住民基本台帳の削除機能 4. 住民基本台帳の照会機能 5. 住民基本台帳に基づく住民票の写し等の発行機能 6. コンビニエンスストアにおける証明書等の自動交付(住民票の写し、印鑑登録証明書)のための連携機能 7. 公的個人認証システムとの連携機能 8. 在留カード等発行システムとの連携機能 9. 印鑑登録システムとの連携機能 10. 戸籍システムとの連携機能 11. 宛名システム兼連携システムとの連携機能	本システムの主な機能は次のとおり。 1. 住民基本台帳の記載機能 2. 住民基本台帳の修正機能 3. 住民基本台帳の削除機能 4. 住民基本台帳の照会機能 5. 住民基本台帳に基づく住民票の写し等の発行機能 6. コンビニエンスストアにおける証明書等の自動交付(住民票の写し、印鑑登録証明書)のための連携機能 7. 公的個人認証システムとの連携機能 8. 出入国在留管理庁との連携機能 9. 印鑑登録システムとの連携機能 10. 戸籍システムとの連携機能 11. 宛名システム兼連携システムとの連携機能	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7年4月1日	I 基本情報 2. 特定個人情報ファイルを取り扱う業務において使用するシステム システム2②システムの機能	本システムの主な機能は次のとおり。 1. 本人確認情報の更新機能 既存住民基本台帳システム(以下、既存住基システム)において住民票の記載事項の変更又は新規作成が発生した場合に、当該情報を元に市町村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。 (略) 4. 本人確認情報検索機能 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。 (略) 7. 送付先情報通知機能 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(通知カード、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。 (略)	本システムの主な機能は次のとおり。 1. 本人確認情報の更新機能 既存住基システムにおいて住民票の記載事項の変更又は新規作成が発生した場合に、当該情報を元に市町村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。 (略) 4. 本人確認情報検索機能 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。 (略) 7. 送付先情報通知機能 機構において、住民に対して番号通知書類(個人番号通知書、個人番号カード交付申請書(以下「交付申請書」という。))等を送付するため、既存住基システムから当該市町村の住民基本台帳に記載されている者の送付先情報を抽出し、当該情報を機構が設置・管理する個人番号カード管理システムに通知する。 (略)	事後	
令和7年4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 ・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カード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との整合性を確認する。	(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個人番号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及び機構保存本人確認情報との整合性を確認する。	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7年4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	(続き) (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個人番号通知書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))。個人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。)	(続き) (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個人番号通知書の形式にて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項及び個人番号カード省令第7条)。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申請書の送付については、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)に基づいて機構が行うこととされていることから、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。	事後	
令和7年4月1日	I 基本情報 5. 個人番号の利用 法令上の根拠	(省略) 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) (省略)	(省略) 2. 住民基本台帳法(住基法)(昭和42年7月25日法律第81号) (省略)	事後	重要な変更に該当しない項目の変更であるため、事前の提出・公表が義務付けられない。
令和7年4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	<提供ができる根拠規定> 番号法第19条第8号別表第二のうち、第三欄(情報提供者)が「市町村長」の項で第四欄(特定個人情報)に「住民票関係情報」が含まれる項(第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項) <照会ができる根拠規定> 該当なし	<提供ができる根拠規定> 番号法第19条第8号に基づく主務省令第2条の表のうち、第三欄(情報提供者)が「市町村長」の項で第四欄(利用特定個人情報)に「住民票関係情報」が含まれる項(第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項) <照会ができる根拠規定> 該当なし	事後	重要な変更に該当しない項目の変更であるため、事前の提出・公表が義務付けられない。
令和7年4月1日	II 特定個人情報ファイルの概要 (1)住民基本台帳ファイル 5. 特定個人情報の提供・移転(委託に伴うものを除く) 提供を行っている件数	57	62	事後	
令和7年4月1日	II 特定個人情報ファイルの概要 (1)住民基本台帳ファイル 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 ①法令上の根拠 ②提供先における用途 ③提供する情報	番号法第19条第8号別表第2に定める情報照会者(別表1を参照) 番号法第19条第8号別表第2 番号法第19条第8号別表第2で規定された事務 番号法第19条第8号別表第2で規定された情報の範囲	番号法第19条第8号に基づく主務省令第2条の表に定める情報照会者(別表1を参照) 番号法第19条第8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条の表で規定された事務 番号法第19条第8号に基づく主務省令第2条の表で規定された情報の範囲	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7年4月1日	別表1	番号法第19条第8号別表第2に定める情報照会者 別表第2のうち、情報提供者が市町村長、かつ、特定個人情報に住民票関係情報が含まれるものを、抜粋しています。	番号法第19条第8号に基づく主務省令第2条の表に定める情報照会者 別表のうち、情報提供者が市町村長、かつ、特定個人情報に住民票関係情報が含まれるものを、抜粋しています。	事後	
令和7年4月1日	別表1		別表1のとおり	事後	
令和7年4月1日	Ⅱ 特定個人情報ファイルの概要 (1) 住民基本台帳ファイル 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2 ①法令上の根拠	番号法第9条第1項別表第1に定める事務	番号法第9条第1項別表に定める事務	事後	
令和7年4月1日	Ⅱ 特定個人情報ファイルの概要 (1) 住民基本台帳ファイル 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3 ①法令上の根拠	番号法第9条第1項別表第1に定める事務	番号法第9条第1項別表に定める事務	事後	
令和7年4月1日	Ⅱ 特定個人情報ファイルの概要 (1) 住民基本台帳ファイル 5. 特定個人情報の提供・移転(委託に伴うものを除く) 移転先1～18 ①法令上の根拠	番号法第9条第1項別表第1に定める事務	番号法第9条第1項別表に定める事務	事後	
令和7年4月1日	Ⅱ 特定個人情報ファイルの概要 (1) 住民基本台帳ファイル 5. 特定個人情報の提供・移転(委託に伴うものを除く) 移転先10 移転先17	子ども生活部子ども家庭支援センター	子ども生活部子ども家庭支援課	事後	
令和7年4月1日	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 3. 特定個人情報の入手・使用 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。	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6～6(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。	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7年4月1日	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 3. 特定個人情報の入手・使用 ⑧使用方法	(略) ・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。 (略)	(略) ・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ファイルの検索を行う。 (略)	事後	
令和7年4月1日	(別添2)ファイル記録項目	(2024年4月22日時点)	別紙「個人情報ファイル簿」のとおり (2025年1月27日時点)	事後	
令和7年4月1日	V 開示請求、問合せ I 特定個人情報の開示・訂正 利用停止請求 ①請求先	郵便番号194-8520 東京都町田市森野2-2-22 担当課:総務部 市政情報課 電話:042-724-8407 FAX:050-3085-3142	郵便番号194-8520 東京都町田市森野2-2-22 担当課:総務部 法務課 電話:042-724-8407 FAX:050-3085-3142	事後	
令和7年4月1日	V 開示請求、問合せ I 特定個人情報の開示・訂正 利用停止請求 ④個人情報ファイル簿の公表 公表場所	総務部市政情報課	総務部法務課	事後	
令和7年4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	システム5 ③他のシステムとの接続 〔 〕宛名システム	システム5 ③他のシステムとの接続 〔○〕宛名システム	事後	重要な変更に該当しない項目の変更であるため、事前の提出・公表が義務付けられない
令和7年4月1日	Ⅱ 特定個人情報ファイルの概要 (3)送付先情報ファイル 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、通知カードを個人番号の付番対象者全員に送付する必要がある。 また、通知カード所有者にあっては、個人番号カードは通知カードと引き換えに交付することとされている。市町村は、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。	番号法第7条第1項(指定及び通知)及び個人番号カード省令第7条(個人番号の通知)に基づき、個人番号通知書を個人番号の付番対象者全員に送付する必要がある。 また、通知カード所有者にあっては、個人番号カードは通知カードと引き換えに交付することとされている。機構は、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)に基づき、これらの事務を実施する。	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7年4月1日	Ⅱ 特定個人情報ファイルの概要 (3) 送付先情報ファイル 2. 基本情報 ④ 記録される項目 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。	・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機構が行うために、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	
令和7年4月1日	Ⅱ 特定個人情報ファイルの概要 (3) 送付先情報ファイル 3. 特定個人情報の入手・使用 ③ 入手の時期・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入手する(以降、新たに個人番号の通知対象者が生じた都度入手する)。	個人番号通知書に係る送付先情報は、新たに個人番号の通知対象者が生じた都度入手する。	事後	
令和7年4月1日	Ⅱ 特定個人情報ファイルの概要 (3) 送付先情報ファイル 3. 特定個人情報の入手・使用 ⑤ 本人への明示	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)	事後	
令和7年4月1日	Ⅱ 特定個人情報ファイルの概要 (3) 送付先情報ファイル 3. 特定個人情報の入手・使用 ⑥ 使用目的	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	
令和7年4月1日	Ⅱ 特定個人情報ファイルの概要 (3) 送付先情報ファイル 3. 特定個人情報の入手・使用 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、個人番号カード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。(既存住基システム→市町村CS又は電子記録媒体→個人番号カード管理システム(機構))。	・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、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)に基づいて行う機構に対し提供する(既存住基システム→市町村CS又は電子記録媒体→個人番号カード管理システム(機構))。	事後	
令和7年4月1日	Ⅱ 特定個人情報ファイルの概要 (3) 送付先情報ファイル 5. 特定個人情報の提供・移転 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)	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)	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7年4月1日	Ⅱ 特定個人情報ファイルの概要 (3)送付先情報ファイル 5. 特定個人情報の提供・移転 ②提供先における用途	市町村から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。	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)に基づき個人番号通知書及び交付申請書を印刷し、送付する。	事後	
令和7年4月1日	Ⅱ 特定個人情報ファイルの概要 (3)送付先情報ファイル 5. 特定個人情報の提供・移転 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)。	個人番号通知書に係る送付先情報は、新たに個人番号の通知対象者が生じた都度提供する。	事後	
令和7年4月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 (3)送付先情報ファイル 2. 特定個人情報の入手リスク3 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。	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、一定期間経過後に市町村CSから自動的に削除する。	事後	
令和7年4月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 (3)送付先情報ファイル 7. 特定個人情報の保管・消去 リスク2 リスクに対する措置の内容	本特定個人情報ファイル(送付先情報ファイル)は、送付先情報の連携を行う必要が生じた都度作成／連携することとしており、システム上、連携後速やか(1営業日後)に削除する仕組みとする。 また、媒体を用いて連携する場合、当該媒体は連携後、連携先である機構において適切に管理され、市町村では保管しない。 そのため、送付先情報ファイルにおいて特定個人情報古い情報のまま保管され続けるリスクは存在しない。	本特定個人情報ファイル(送付先情報ファイル)は、送付先情報の連携を行う必要が生じた都度作成／連携することとしており、システム上、一定期間経過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古い情報のまま保管され続けるリスクは存在しない。	事後	
令和7年4月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 (3)送付先情報ファイル 7. 特定個人情報の保管・消去 特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置	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。	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。 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。	事後	