

特定個人情報保護評価書(全項目評価書)

評価書番号	評価書名
1	住民基本台帳に関する事務 全項目評価書

個人のプライバシー等の権利利益の保護の宣言

中野区は、住民基本台帳に関する事務において特定個人情報ファイルを取扱うにあたり、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事前に分析し、このようなリスクを軽減させるために適切な措置を講じることによって、個人のプライバシー等の権利利益の保護に取り組むことをここに宣言する。

特記事項

住民基本台帳に関する事務では、事務の一部を民間事業者に委託しているため、事業者選定の際に事業者の情報保護管理体制を確認し、秘密保持に関しても契約に含めることで万全を期している。

評価実施機関名

中野区長

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7月11日

項目一覧

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

I 基本情報

1. 特定個人情報ファイルを取り扱う事務

①事務の名称	住民基本台帳に関する事務
②事務の内容 ※	市町村(特別区を含む。)(以下「市町村」という。))が住民を対象とする行政を適切に行い、また、住民の正しい権利を保障するためには、市町村の住民に関する正確な記録が整備されていなければならない。 住民基本台帳は、住民基本台帳法(以下「住基法」という。))に基づき、作成されるものであり、市町村における住民の届出に関する制度及びその住民たる地位を記録する各種の台帳に関する制度を一元化し、もって、住民の利便を増進するとともに行政の近代化に対処するため、住民に関する記録を正確かつ統一的行うものであり、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。 当区は、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、その他住基法で定める者の請求による住民票の写し等証明書の交付 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及び個人番号の変更 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情報提供ネットワークシステムを利用した住民票情報(住基法第7条第4号に規定する項目)の提供 なお、⑨の「個人番号の通知及び個人番号カードの交付」に係る事務については、行政手続における特定の個人を識別するための番号の利用等に関する法律に規定する個人番号、個人番号カード、特定個人情報の提供等に関する命令(平成26年11月20日総務省令第85号。以下「個人番号カード省令」という。))第35条(個人番号通知書、個人番号カード関連事務の委任)により機構に対する事務の一部の委任が認められている。 そのため、当該事務においては、事務を委任する機構に対する情報の提供を含めて特定個人情報ファイルを使用する。
③対象人数	＜選択肢＞ [30万人以上] 1) 1,000人未満 2) 1,000人以上1万人未満 3) 1万人以上10万人未満 4) 10万人以上30万人未満 5) 30万人以上

2. 特定個人情報ファイルを取り扱う事務において使用するシステム

システム1

①システムの名称	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	1. 住民基本台帳の記載 転入、出生、入国、職権等により住民基本台帳に新たに住民を記載(住民票を作成)する機能 2. 住民基本台帳の記載変更 住民基本台帳に記載されている事項に変更があったときに、記載内容を修正する機能 3. 住民基本台帳の消除処理 転出、死亡、出国、職権等により住民基本台帳から住民に関する記載を消除(住民票を除票)する機能 4. 住民基本台帳の照会 住民基本台帳から該当する住民に関する記載(住民票)を照会する機能 5. 帳票の発行機能 住民票の写し、住民票記載事項証明書、転出証明書、住民票コード通知書等の各種帳票を発行する機能 6. 住民基本台帳の統計機能 異動集計表や、人口統計用の集計表を作成する機能 7. 住民基本台帳ネットワークシステムとの連携機能 機構、都、他自治体と住民基本台帳ネットワークシステム(以下「住基ネットシステム」という。)を通じ連携する機能 8. 法務省への通知事項の作成機能 外国人住民票の記載等に応じて、市町村通知の作成を行う機能 9. 戸籍システムへの連携 住民票の記載等に応じ、戸籍システムへ附票情報等を連携する機能
③他のシステムとの接続	[] 情報提供ネットワークシステム [○] 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 (法務省連携システム、証明書自動交付(コンビニ交付)システム)

システム2									
①システムの名称	住民基本台帳ネットワークシステム ※「3. 特定個人情報ファイル名」に示す「本人確認情報ファイル」及び「送付先情報ファイル」は、住基ネットシステムの構成要素のうち、市町村CSにおいて管理がなされているため、以降は、住基ネットシステムの内の市町村CS部分について記載する。								
②システムの機能	1. 本人確認情報の更新 既存住基システムにおいて住民票の記載事項の変更又は新規作成が発生した場合に、当該情報を元に市町村CSの本人確認情報を更新し、都道府県サーバへ更新情報を送信する。 2. 本人確認 特例転入処理や住民票の写しの広域交付などを行う際、窓口における本人確認のため、提示された個人番号カード等を元に住基ネットシステムが保有する本人確認情報に照会を行い、確認結果を画面上に表示する。 3. 個人番号カードを利用した転入（特例転入） 個人番号カードの交付を受けている者等の転入が予定される場合に、転出証明書情報をCSを通じて受け取り、その者に係る転入の届出を受け付けた際に、個人番号カードを用いて転入処理を行う（一定期間経過後も転入の届出が行われない場合は、受け取った転出証明書情報を消去する。）。 4. 本人確認情報検索 統合端末において入力された住民票コード、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 全国サーバに対して住民票コード、個人番号又は4情報の組合せをキーとした本人確認情報照会要求を行い、該当する個人の本人確認情報を受領する。 6. 本人確認情報整合 本人確認情報ファイルの内容が都道府県知事が都道府県サーバにおいて保有している都道府県知事保存本人確認情報ファイル及び機構が全国サーバにおいて保有している機構保存本人確認情報ファイルと整合することを確認するため、都道府県サーバ及び全国サーバに対し、整合性確認用本人確認情報を提供する。 7. 送付先情報通知 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	<table border="0"> <tr> <td>☐ 情報提供ネットワークシステム</td><td>☐ 庁内連携システム</td></tr> <tr> <td>☐ 住民基本台帳ネットワークシステム</td><td>☒ 既存住民基本台帳システム</td></tr> <tr> <td>☐ 宛名システム等</td><td>☐ 税務システム</td></tr> <tr> <td colspan="2">☒ その他 （ 戸籍附票システム ）</td></tr> </table>	☐ 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 （ 戸籍附票システム ）	
☐ 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 （ 戸籍附票システム ）									

システム3	
①システムの名称	証明書自動交付(コンビニ交付)システム(以下「コンビニシステム」という。)
②システムの機能	1. 利用者証明用電子証明等の利用 個人番号カードの利用者証明用電子証明等の情報を用いて個人を特定し、住民票の写し等証明書のPDFデータを作成する。 2. 証明書交付センターとの通信 コンビニ交付システムインターフェース及び電文応答機能を備えた証明書交付センターと通信する。 3. 住民票の写し等証明書の発行 ・コンビニエンスストア(以下「コンビニ」という。)に設置されているマルチコピー機を利用して、住民票の写し等証明書を発行する。 ・窓口のバックアップとして住民票の写し等証明書を発行する。
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 (証明書交付センター(機構))
システム4	
①システムの名称	住民情報連携基盤システム
②システムの機能	住民情報連携基盤システムは、中間サーバーと、庁内の既存住基システムや各業務システムとのデータ連携を担うシステムである。 1. 中間サーバー連携機能 中間サーバーまたは中間サーバー端末からの要求に基づき、団体内統合宛名番号に紐付く宛名情報等を通知する機能。 2. 宛名情報等管理機能 住民情報連携基盤システムにおいて宛名情報を団体内統合宛名番号、個人番号と紐付けて保存し、管理する機能。 3. 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する機能。 4. 既存システム連携機能 既存業務システムからの要求に基づき、個人番号または団体内統合宛名番号に紐付く宛名情報を通知する機能。 5. 符号取得・生成要求機能 (1) 団体内統合宛名番号および個人番号を中間サーバーに渡し、符号取得を依頼する。 (2) 中間サーバーから個人番号及び処理通番(情報提供ネットワークシステムで作成)を受領後、住民基本台帳ネットワークシステムに渡し、符号生成を要求する。
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)

システム5	
①システムの名称	中間サーバー
②システムの機能	1. 符号管理機能 情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」とを紐づけ、その情報を保管・管理する機能 2. 情報照会機能 情報提供ネットワークシステムを介して、特定個人情報(連携対象)の情報照会および情報提供受領(照会した情報の受領)を行う機能 3. 情報提供機能 情報提供ネットワークシステムを介して、情報照会要求の受領および当該特定個人情報(連携対象)の提供を行う機能 4. 既存システム接続機能 中間サーバーと住民情報連携基盤システム、既存住基システムおよび既存業務システムとの間で情報照会内容、情報提供内容、特定個人情報(連携対象)、符号取得のための情報等について連携するための機能 5. 情報提供等記録管理機能 特定個人情報(連携対象)の照会、または提供があった旨の情報提供等記録を生成し、管理する機能 6. 情報提供データベース管理機能 特定個人情報(連携対象)を副本として、保持・管理する機能 7. データ送受信機能 中間サーバーと情報提供ネットワークシステムとの間で情報照会、情報提供、符号取得のための情報等について連携するための機能 8. セキュリティ管理機能 特定個人情報の暗号化及び復号機能と、鍵情報を管理する。 9. 職員認証・権限管理機能 中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報(連携対象)へのアクセス制御を行う機能 10. システム管理機能 バッチの状況管理、業務統計情報の集計、稼動状態の通知、保管期限切れ情報の削除を行う機能
③他のシステムとの接続	☐ 情報提供ネットワークシステム ☐ 庁内連携システム ☐ 住民基本台帳ネットワークシステム ☒ 既存住民基本台帳システム ☒ 宛名システム等 ☐ 税務システム ☐ その他 ()
システム6	
①システムの名称	宛名システム
②システムの機能	1. 宛名情報管理機能 中野区民の住所、氏名その他の住民票関係情報を既存住基システムから連携し、あわせて住民登録外者及び区外居住者の住民票関係情報並びに特別徴収義務者の宛名情報を管理する。 2. 郵送先管理機能 郵便物発送時の郵送先を管理する。
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 ()

3. 特定個人情報ファイル名

- (1) 住民基本台帳ファイル
- (2) 本人確認情報ファイル
- (3) 送付先情報ファイル
- (4) コンビニ情報ファイル

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 住民を対象とする行政を適切に行い、また、住民の正しい権利を保障することを目的として、当区において、住基法第7条に規定される住民に関する記録を正確かつ統一的行うとともに、住民の居住関係の公証その他住民に関する事務の処理の基礎とするため、取り扱う。 (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 住基ネットシステム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。 (4) コンビニ情報ファイル 区役所開庁時間外も含め区の窓口に出向かなくても証明書交付サービスが提供される「24時間365日どこでも区役所」の実現のため、個人番号カードを利用しコンビニに設置されているマルチコピー機等から住民票の写し等証明書を発行するため、取り扱う。
② 実現が期待されるメリット	住民票の写し等証明書にかえて本人確認情報を利用することにより、これまで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(住民票の写し等証明書)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. 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8条第1項（個人番号とすべき番号の生成） ・第16条（本人確認の措置） ・第17条（個人番号カードの交付等） ・附則第3条第1項、第2項、第3項（個人番号の指定及び通知に関する経過措置） 2. 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）
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[実施する] <選択肢> 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	・番号法第19条第8号（特定個人情報の提供の制限）及同法に基づく主務省令第2条の表 （番号法第19条第8号に基づく主務省令第2条の表における情報提供の根拠） ：第三欄（情報提供者）が「市町村長」の項のうち、第四欄（利用特定個人情報）に「住民票関係情報」が含まれる項（1、2、3、5、7、11、13、15、20、28、37、39、48、53、57、58、59、63、65、66、69、73、75、76、81、83、84、86、87、91、92、96、106、108、110、112、115、118、124、129、130、132、136、137、138、141、142、144、149、150、151、152、155、156、158、160、163、164、165、166の項） （番号法第19条第8号に基づく主務省令第2条の表における情報照会の根拠） ：なし （住民基本台帳に関する事務において情報提供ネットワークシステムによる情報照会を行わない）
7. 評価実施機関における担当部署	
①部署	中野区 区民部戸籍住民課
②所属長の役職名	区民部戸籍住民課長
8. 他の評価実施機関	
—	

(別添1) 事務の内容

別紙1参照

(備考)

Ⅱ 特定個人情報ファイルの概要

1. 特定個人情報ファイル名

(1) 住民基本台帳ファイル

2. 基本情報

①ファイルの種類 ※	[システム用ファイル]	<選択肢> 1) システム用ファイル 2) その他の電子ファイル(表計算ファイル等)
②対象となる本人の数	[10万人以上100万人未満]	<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
③対象となる本人の範囲 ※	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を含む	
その必要性	法令に基づき住民基本台帳を作成し必要に応じて住民票に記載、消除又は修正すべきとされているため。	
④記録される項目	[100項目以上]	<選択肢> 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
主な記録項目 ※	・識別情報 [☐] 個人番号 [☐] 個人番号対応符号 [☐] その他識別情報(内部番号) ・連絡先等情報 [☐] 5情報(氏名、氏名の振り仮名、性別、生年月日、住所) [☐] 連絡先(電話番号等) [☐] その他住民票関係情報 ・業務関係情報 [☐] 国税関係情報 [☐] 地方税関係情報 [☐] 健康・医療関係情報 [☐] 医療保険関係情報 [☐] 児童福祉・子育て関係情報 [☐] 障害者福祉関係情報 [☐] 生活保護・社会福祉関係情報 [☐] 介護・高齢者福祉関係情報 [☐] 雇用・労働関係情報 [☐] 年金関係情報 [☐] 学校・教育関係情報 [☐] 災害関係情報 [☐] その他 (選挙資格に関する情報、事務手続きの連絡事項)	
その妥当性	住基法第7条(住民票の記載事項)にて住民票に記載すべきものとなっている。	
全ての記録項目	別添2を参照。	
⑤保有開始日	平成27年6月	
⑥事務担当部署	区民部 戸籍住民課	

3. 特定個人情報の入手・使用

①入手元 ※	☐ 本人又は本人の代理人 ☐ 評価実施機関内の他部署 () ☐ 行政機関・独立行政法人等 () ☐ 地方公共団体・地方独立行政法人 () ☐ 民間事業者 () ☐ その他 ()	
②入手方法	☐ 紙 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ フラッシュメモリ ☐ 電子メール ☐ 専用線 ☐ 庁内連携システム ☐ 情報提供ネットワークシステム ☐ その他 (住基ネットシステム、申請管理システム、マイナポータルぴったりサービス)	
③入手の時期・頻度	転入、入国等の住民異動届及び出生、国籍取得等の戸籍届の申請並びに通知を受けた都度	
④入手に係る妥当性	当区住民基本台帳に記載する時点での入手となることから上記方法、時期、頻度となる。	
⑤本人への明示	住基法第7条(住民票の記載事項)において明示されている	
⑥使用目的 ※	住基法に基づき住民基本台帳への記載を行う	
変更の妥当性	—	
⑦使用の主体	使用部署 ※	区民部 戸籍住民課
	使用者数	[50人以上100人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
⑧使用方法 ※	・住民基本台帳への個人番号を記載し、本人からの希望及び使用目的に応じて住民票の写しに記載する。 ・本人への個人番号の通知(個人番号通知を発行する機構への情報連携) ・窓口事務における本人確認書類からの検索キーとしての利用 ・転出証明書への記載	
	情報の突合 ※	・住民異動届の際に入手する場合は、個人番号カード等の本人確認書類で突合を行う。 ・機構で新たに個人番号が生成された場合は、個人番号の要求時に提供を行っている住民票コードと突合を行う。
	情報の統計分析 ※	個人番号を用いた統計分析は行わない。
	権利利益に影響を与え得る決定 ※	該当なし
⑨使用開始日	平成27年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 1) 委託する 2) 委託しない (4) 件)	
委託事項1		データ別置保管	
①委託内容		個別業務システムが保有する重要情報を不慮の災害から守る為、外部に適切な保管環境を有する業者に保管する。	
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 ※		「2. ③対象となる本人の範囲」と同上。	
その妥当性		システム復旧が目的のため、システムで保管されている全対象が範囲となる。	
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		中野区区政情報の公開に関する条例に基づく開示請求を行うことで確認ができる。	
⑥委託先名		東武デリバリー株式会社	
再委託	⑦再委託の有無 ※	再委託しない ＜選択肢＞ 1) 再委託する 2) 再委託しない	
	⑧再委託の許諾方法		
	⑨再委託事項		
委託事項2		既存住基システムに関する運用・保守	
①委託内容		既存住基システムの運用及び保守作業	
②取扱いを委託する特定個人情報ファイルの範囲		特定個人情報ファイルの全体 ＜選択肢＞ 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
対象となる本人の数		10万人以上100万人未満 ＜選択肢＞ 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上	
対象となる本人の範囲 ※		「2. ③対象となる本人の範囲」と同上。	
その妥当性		既存住基システムの運用・保守のためファイルにアクセスする。	

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 (運用・保守管理用の端末)	
⑤委託先名の確認方法		中野区区政情報の公開に関する条例に基づく開示請求を行うことで確認ができる。	
⑥委託先名		株式会社RKKCS	
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	契約に基づく納入等の全部又は主要な部分を一括して第三者に再委託することは禁止する。ただし、緊急その他のやむを得ない事情により第三者に委託する必要がある場合は、委託内容(範囲)、委託理由、委託先の監督方法等を明記した書面を徴取し、妥当なものであれば、再委託を認める。	
	⑨再委託事項	既存住基システムの運用及び保守作業の一部	
委託事項3		戸籍住民窓口における入出力等業務及び証明書発行等業務の業務委託	
①委託内容		戸籍住民窓口における入出力等業務及び証明書発行等業務	
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体]	<選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	対象となる本人の数	[10万人以上100万人未満]	<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	「2. ③対象となる本人の範囲」と同上。	
	その妥当性	大量定型的業務について民間事業者に委託できる範囲内で委託することで、柔軟性のある運用体制の確立と効率的で安定した業務運営の維持を図り、コストの低減と行政サービスの向上を図る。	
③委託先における取扱者数		[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
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 (業務処理用の端末)	
⑤委託先名の確認方法		中野区区政情報の公開に関する条例に基づく開示請求を行うことで確認ができる。	
⑥委託先名		パーソルビジネスプロセスデザイン株式会社 株式会社ヒューマントラスト	
再委託	⑦再委託の有無 ※	[再委託しない]	<選択肢> 1) 再委託する 2) 再委託しない
	⑧再委託の許諾方法		
	⑨再委託事項		

委託事項4		住基ネットワーク連携システム等の改修及び関連システムの運用に関するSE支援委託	
①委託内容		障害対応、外字配信作業、CSクライアントシステムアップデート作業、CSサーバーレベルアップ作業、整合性チェック作業、ウィルス対策ソフトのパターンファイルアップデート作業等	
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
	対象となる本人の数	[10万人以上100万人未満]	<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	「2. ③対象となる本人の範囲」と同上。	
	その妥当性	専門的なスキルが必要な業務について民間事業者に委託できる範囲内で委託することで、安定したシステム環境を効率的に維持することができ、コストの低減と行政サービスの向上を図る。	
③委託先における取扱者数		[10人以上50人未満]	<選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法		[] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [○] その他 (システム管理用の端末)	
⑤委託先名の確認方法		中野区区政情報の公開に関する条例に基づく開示請求を行うことで確認ができる。	
⑥委託先名		富士通Japan株式会社	
再委託	⑦再委託の有無 ※	[再委託する]	<選択肢> 1) 再委託する 2) 再委託しない
	⑧再委託の許諾方法	委託内容(範囲)、委託理由、委託先の監督方法等を明記した書面により報告し、妥当なものであれば再委託を認める。	
	⑨再委託事項	障害対応、外字配信作業、CSクライアントシステムアップデート作業、CSサーバーレベルアップ作業、整合性チェック作業、ウィルス対策ソフトのパターンファイルアップデート作業等	
委託事項5		既存住基システムの標準化・共通化への移行作業委託	
①委託内容		既存住基システムの標準化・共通化への移行作業	
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体]	<選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	対象となる本人の数	[10万人以上100万人未満]	<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	「2. ③対象となる本人の範囲」と同上。	
	その妥当性	・全てのデータを移行するために、特定個人情報ファイル全体を委託の対象にする必要がある。	
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

		[○] 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。)
④委託先への特定個人情報 ファイルの提供方法		[] フラッシュメモリ [] 紙
		[] その他 ()
⑤委託先名の確認方法		中野区政情報の公開に関する条例に基づく開示請求を行うことで確認ができる。
⑥委託先名		株式会社RKKCS
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	契約に基づく納入等の全部又は主要な部分を一括して第三者に再委託することは禁止する。ただし、緊急その他のやむを得ない事情により第三者に委託する必要がある場合は、委託内容(範囲)、委託理由、委託先の監督方法を明記した書面を徴取し、妥当なものであれば、再委託を認める。
	⑨再委託事項	必要に応じて、既存住基システムの標準化・I共通化への移行作業の一部

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 (9) 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(別紙2参照)
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条の表に定める各事務
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条の表に定める住民票関係情報
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 ☐ 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依頼のあった都度
提供先2	教育委員会事務局 学務課
①法令上の根拠	中野区個人番号の利用及び特定個人情報の提供に関する条例
②提供先における用途	就学援助等関係資料との突合に利用する。
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	＜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 ☐ 電子メール ☐ フラッシュメモリ ☒ その他 (市内連携システム) ☐ 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 移転先からの情報提供を求められた都度

移転先1	区民部 保険医療課
①法令上の根拠	番号法第9条及び別表に規定する事務の効率化に利用
②移転先における用途	国民健康保険関係資料、国民年金関係資料及び後期高齢関係資料との突合に利用する。
③移転する情報	「2. ④記録される項目」と同上。
④移転する情報の対象となる本人の数	☐ 10万人以上100万人未満 <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上。
⑥移転方法	☒ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	住民基本台帳ファイルの更新の都度 移転先からの情報提供を求められた都度
移転先2	区民部 税務課
①法令上の根拠	番号法第9条及び別表に規定する事務の効率化に利用
②移転先における用途	住民税関係資料との突合に利用する。
③移転する情報	「2. ④記録される項目」と同上。
④移転する情報の対象となる本人の数	☐ 10万人以上100万人未満 <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上。
⑥移転方法	☒ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	住民基本台帳ファイルの更新の都度 移転先からの情報提供を求められた都度
移転先3	地域支えあい推進部 介護保険課
①法令上の根拠	番号法第9条及び別表に規定する事務の効率化に利用
②移転先における用途	介護保険関係資料との突合に利用する。
③移転する情報	「2. ④記録される項目」と同上。
④移転する情報の対象となる本人の数	☐ 10万人以上100万人未満 <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上

⑤移転する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上。	
⑥移転方法	☐ 〇 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 ()	☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	住民基本台帳ファイルの更新の都度 移転先からの情報提供を求められた都度	
移転先4	子ども教育部 子育て支援課	
①法令上の根拠	番号法第9条及び別表に規定する事務の効率化に利用	
②移転先における用途	子育て支援等関係資料との突合に利用する。	
③移転する情報	「2. ④記録される項目」と同上。	
④移転する情報の対象となる本人の数	☐ 10万人以上100万人未満	<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上。	
⑥移転方法	☐ 〇 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 ()	☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	住民基本台帳ファイルの更新の都度 移転先からの情報提供を求められた都度	
移転先5	子ども教育部 保育園・幼稚園課	
①法令上の根拠	番号法第9条及び別表に規定する事務の効率化に利用	
②移転先における用途	子どものための教育・保育関係資料との突合に利用する。	
③移転する情報	「2. ④記録される項目」と同上。	
④移転する情報の対象となる本人の数	☐ 10万人以上100万人未満	<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上。	
⑥移転方法	☐ 〇 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 ()	☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	住民基本台帳ファイルの更新の都度 移転先からの情報提供を求められた都度	

移転先6	健康福祉部 福祉推進課
①法令上の根拠	番号法第9条及び別表に規定する事務の効率化に利用
②移転先における用途	福祉の措置又は費用の徴収関係資料との突合に利用する。
③移転する情報	「2. ④記録される項目」と同上。
④移転する情報の対象となる本人の数	☐ 10万人以上100万人未満 <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上。
⑥移転方法	☐ 〇 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	住民基本台帳ファイルの更新の都度 移転先からの情報提供を求められた都度
移転先7	健康福祉部 生活支援課
①法令上の根拠	番号法第9条及び別表に規定する事務の効率化に利用
②移転先における用途	生活保護関係資料との突合に利用する。
③移転する情報	「2. ④記録される項目」と同上。
④移転する情報の対象となる本人の数	☐ 10万人以上100万人未満 <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上。
⑥移転方法	☐ 〇 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	住民基本台帳ファイルの更新の都度 移転先からの情報提供を求められた都度
移転先8	地域支えあい推進部 すこやか福祉センター
①法令上の根拠	番号法第9条及び別表に規定する事務の効率化に利用
②移転先における用途	子育て支援等関係資料との突合に利用する。
③移転する情報	「2. ④記録される項目」と同上。
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	

⑥移転方法	☒ 庁内連携システム ☐ 専用線 ☐ 電子メール ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ フラッシュメモリ ☐ 紙 ☐ その他 ()
⑦時期・頻度	住民基本台帳ファイルの更新の都度 移転先からの情報提供を求められた都度
移転先9	都市基盤部 住宅課
①法令上の根拠	番号法第9条及び別表に規定する事務の効率化に利用
②移転先における用途	住宅施策事業関係資料との突合に利用する。
③移転する情報	「2. ④記録される項目」と同上。
④移転する情報の対象となる本人の数	☐ 10万人以上100万人未満 <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上。
⑥移転方法	☒ 庁内連携システム ☐ 専用線 ☐ 電子メール ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ フラッシュメモリ ☐ 紙 ☐ その他 ()
⑦時期・頻度	

6. 特定個人情報の保管・消去

①保管場所 ※		＜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 [20年以上]
	その妥当性	・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		＜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が、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。
7. 備考		
—		

Ⅱ 特定個人情報ファイルの概要

1. 特定個人情報ファイル名

(2) 本人確認情報ファイル

2. 基本情報

①ファイルの種類 ※	[システム用ファイル]	<選択肢> 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、転出等の事由により住民票が消除(死亡による消除を除く。)された者(以下「消除者」という。)を含む	
その必要性	住基ネットシステムを通じて全国共通の本人確認を行うため、本特定個人情報ファイル(本人確認情報ファイル)において区域内の全ての住民の情報を保有し、住民票に記載されている住民全員の記録を常に正確に更新・管理・提供する必要があるため。	
④記録される項目	[10項目以上50項目未満]	<選択肢> 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
主な記録項目 ※	・識別情報 [☐] 個人番号 [☐] 個人番号対応符号 [☐] その他識別情報(内部番号) ・連絡先等情報 [☐] 5情報(氏名、氏名の振り仮名、性別、生年月日、住所) [☐] 連絡先(電話番号等) [☐] その他住民票関係情報 ・業務関係情報 [☐] 国税関係情報 [☐] 地方税関係情報 [☐] 健康・医療関係情報 [☐] 医療保険関係情報 [☐] 児童福祉・子育て関係情報 [☐] 障害者福祉関係情報 [☐] 生活保護・社会福祉関係情報 [☐] 介護・高齢者福祉関係情報 [☐] 雇用・労働関係情報 [☐] 年金関係情報 [☐] 学校・教育関係情報 [☐] 災害関係情報 [☐] その他 ()	
その妥当性	・個人番号、4情報、その他住民票関係情報 住基ネットシステム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6月	
⑥事務担当部署	区民部 戸籍住民課	

3. 特定個人情報の入手・使用

①入手元 ※	☐ 本人又は本人の代理人 ☐ 評価実施機関内の他部署 () ☐ 行政機関・独立行政法人等 () ☐ 地方公共団体・地方独立行政法人 () ☐ 民間事業者 () ☒ その他 (自部署)
②入手方法	☐ 紙 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ フラッシュメモリ ☐ 電子メール ☐ 専用線 ☐ 庁内連携システム ☐ 情報提供ネットワークシステム ☒ その他 (既存住基システム)
③入手の時期・頻度	住民基本台帳の記載事項において、本人確認情報に係る変更又は新規作成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システムに格納する必要があるため。
⑤本人への明示	市町村CSが既存住基システムより本人確認情報を入手することについて、住基法第30条の6(市町村長から都道府県知事への本人確認情報の通知等)及び平成14年6月10日総務省告示第334号(第6-7(1)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 ※	住基ネットシステム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 ※
	区民部 戸籍住民課 使用者数 ☐ 50人以上100人未満 ☐ 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
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探索し、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)。 ・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探索を行う。 ・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 ※ 該当なし
⑨使用開始日	平成27年6月1日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		委託する ＜選択肢＞ 1) 委託する 2) 委託しない (1) 件
委託事項1		住基ネットワークシステム（CSサーバ）の改修及び関連システムの運用に関するSE支援委託
①委託内容		障害対応、外字配信作業、CSクライアントシステムアップデート作業、CSサーバーレベルアップ作業、整合性チェック作業、ウィルス対策ソフトのパターンファイルアップデート作業等
②取扱いを委託する特定個人情報ファイルの範囲		特定個人情報ファイルの全体 ＜選択肢＞ 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	対象となる本人の数	10万人以上100万人未満 ＜選択肢＞ 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	「2. ③対象となる本人の範囲」と同上。
	その妥当性	専門的なスキルが必要な業務について民間事業者に委託できる範囲内で委託することで、安定したシステム環境を効率的に維持することができ、コストの低減と行政サービスの向上を図る。
③委託先における取扱者数		10人以上50人未満 ＜選択肢＞ 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法		専用線 電子メール 電子記録媒体（フラッシュメモリを除く。） フラッシュメモリ 紙 ○ その他 （システム管理用の端末）
⑤委託先名の確認方法		中野区区政情報の公開に関する条例に基づく開示請求を行うことで確認ができる。
⑥委託先名		富士通Japan株式会社
再委託	⑦再委託の有無 ※	再委託する ＜選択肢＞ 1) 再委託する 2) 再委託しない
	⑧再委託の許諾方法	委託内容（範囲）、委託理由、委託先の監督方法等を明記した書面により報告し、妥当なものであれば再委託を認める。
	⑨再委託事項	障害対応、外字配信作業、CSクライアントシステムアップデート作業、CSサーバーレベルアップ作業、整合性チェック作業、ウィルス対策ソフトのパターンファイルアップデート作業等

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
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 ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (住基ネットシステム) ☐ 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	住民基本台帳の記載事項において、本人確認情報に係る変更又は新規作成が発生した都度、随時。
提供先2	都道府県及び機構
①法令上の根拠	住基法第14条(住民基本台帳の正確な記録を確保するための措置)
②提供先における用途	住民基本台帳の正確な記録を確保するために、本人確認情報ファイルの記載内容(当該提供情報)と都道府県知事保存本人確認情報ファイル及び機構保存本人確認情報ファイルの記載内容が整合することを確認する。
③提供する情報	住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日
④提供する情報の対象となる本人の数	＜選択肢＞ ☐ 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
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 ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (住基ネットシステム) ☐ 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	必要に応じて随時(1年に1回程度)

6. 特定個人情報の保管・消去		
①保管場所 ※		庁舎の中で、入退室管理を実施している部屋に設置したサーバ内に記録している。 サーバへのアクセスは、指定された端末からのID／パスワードによる認証が必要となる。
②保管期間	期間	<選択肢> 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない [20年以上]
	その妥当性	・住民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。
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に送付する必要がある。 また、通知カード所持者にあつては、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 [☐] 5情報(氏名、氏名の振り仮名、性別、生年月日、住所) [☐] 連絡先(電話番号等) [☐] その他住民票関係情報 ・業務関係情報 [☐] 国税関係情報 [☐] 地方税関係情報 [☐] 健康・医療関係情報 [☐] 医療保険関係情報 [☐] 児童福祉・子育て関係情報 [☐] 障害者福祉関係情報 [☐] 生活保護・社会福祉関係情報 [☐] 介護・高齢者福祉関係情報 [☐] 雇用・労働関係情報 [☐] 年金関係情報 [☐] 学校・教育関係情報 [☐] 災害関係情報 [☐] その他 (個人番号通知及び交付申請書の送付先の情報)
	その妥当性	・個人番号、4情報、その他住民票関係情報 個人番号カードの券面記載事項として、番号法第2条第7項(定義)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	
⑥事務担当部署	区民部 戸籍住民課	

3. 特定個人情報の入手・使用			
①入手元 ※		☐ 本人又は本人の代理人 ☐ 評価実施機関内の他部署 () ☐ 行政機関・独立行政法人等 () ☐ 地方公共団体・地方独立行政法人 () ☐ 民間事業者 () ☒ その他 (自部署)	
②入手方法		☐ 紙 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ フラッシュメモリ ☐ 電子メール ☐ 専用線 ☐ 庁内連携システム ☐ 情報提供ネットワークシステム ☒ その他 (既存住基システム)	
③入手の時期・頻度		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システムを用いるため、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)	
⑥使用目的 ※		・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))。	
		変更の妥当性 —	
⑦使用の主体	使用部署 ※	戸籍住民課	
	使用者数	[50人以上100人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
⑧使用方法 ※		・既存住基システムより個人番号の通知対象者の情報を抽出し、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ういた統計分析は行わない。
		権利利益に影響を与え得る決定 ※	該当なし
⑨使用開始日		平成27年10月5日	

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※	☐ 委託する ☐ 再委託する (1) 件 1) 件	

1

)

件

1

)

件

1

)

件

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	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. 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 (住基ネットシステム)
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。

6. 特定個人情報の保管・消去		
①保管場所 ※		庁舎の中で、入退室管理を実施している部屋に設置したサーバ内に記録している。 サーバへのアクセスは、指定された端末からのID／パスワードによる認証が必要となる。
②保管期間	期間	＜選択肢＞ 1) 1年未満 4) 3年 7) 6年以上10年未満 10) 定められていない 2) 1年 5) 4年 8) 10年以上20年未満 3) 2年 6) 5年 9) 20年以上 [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送付先情報は、機構より指定された方法により、システム上、一括して消去する仕組みとする。
7. 備考		

Ⅱ 特定個人情報ファイルの概要

1. 特定個人情報ファイル名

(4) コンビニ情報ファイル

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を含む	
その必要性	個人番号カードを利用し、コンビニに設置されているマルチコピー機等で住民票の写し等証明書を発行するため。	
④記録される項目	[50項目以上100項目未満]	<選択肢> 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
主な記録項目 ※	・識別情報 [☐] 個人番号 [☐] 個人番号対応符号 [☐] その他識別情報(内部番号) ・連絡先等情報 [☐] 5情報(氏名、氏名の振り仮名、性別、生年月日、住所) [☐] 連絡先(電話番号等) [☐] その他住民票関係情報 ・業務関係情報 [☐] 国税関係情報 [☐] 地方税関係情報 [☐] 健康・医療関係情報 [☐] 医療保険関係情報 [☐] 児童福祉・子育て関係情報 [☐] 障害者福祉関係情報 [☐] 生活保護・社会福祉関係情報 [☐] 介護・高齢者福祉関係情報 [☐] 雇用・労働関係情報 [☐] 年金関係情報 [☐] 学校・教育関係情報 [☐] 災害関係情報 [☐] その他 (発行抑止情報)	
その妥当性	住基法第7条(住民票の記載事項)にて住民票に記載すべきものとなっている。	
全ての記録項目	別添2を参照。	
⑤保有開始日	平成27年10月	
⑥事務担当部署	区民部 戸籍住民課	

3. 特定個人情報の入手・使用

①入手元 ※	☐ 本人又は本人の代理人 ☐ 評価実施機関内の他部署 () ☒ 行政機関・独立行政法人等 (地方公共団体情報システム機構) ☐ 地方公共団体・地方独立行政法人 () ☐ 民間事業者 () ☒ その他 (自部署)
②入手方法	☐ 紙 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ フラッシュメモリ ☐ 電子メール ☐ 専用線 ☐ 庁内連携システム ☐ 情報提供ネットワークシステム ☒ その他 (既存住基システム)
③入手の時期・頻度	転入、入国等の住民異動届及び出生、国籍取得等の戸籍届の申請並びに通知を受けた都度 カード発行管理情報に変更があった都度
④入手に係る妥当性	当区住民基本台帳に記載する時点での入手又はカード発行管理情報に変更があった時点での入手となることから上記方法、時期、頻度となる
⑤本人への明示	住基法第7条(住民票の記載事項)において明示されている
⑥使用目的 ※	コンビニに設置されているマルチコピー機等の住民票の写し等証明書の発行 既存住基システムに障害等が発生した場合に窓口で交付する住民票の写し等証明書の発行
変更の妥当性	—
⑦使用の主体	使用部署 ※ 区民部 戸籍住民課 使用者数 <選択肢> 50人以上100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
⑧使用方法 ※	コンビニに設置されているマルチコピー機等での申請に応じて住民票の写し等証明書を発行する。 既存住基システムに障害等が発生した場合に窓口で交付する住民票の写し等証明書を発行する。
情報の突合 ※	コンビニ情報ファイルを更新する際に、受領したコンビニ情報ファイルに関する更新データとコンビニ情報ファイルを、内部番号をもとに突合する。 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コンビニ情報ファイルを機構の定める仕様に基づき突合する。
情報の統計分析 ※	個人に着目した分析・統計は行わず、コンビニ情報の更新件数の集計等、事務処理実績の確認のための統計のみ行う。
権利利益に影響を与え得る決定 ※	該当なし
⑨使用開始日	平成27年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 1) 委託する 2) 委託しない
委託事項1		コンビニ交付システム構築・保守委託
①委託内容		問合せ対応、業務アプリケーションソフトの適用業務、ハードウェア及び業務アプリケーションの設定変更等、障害対応、定期点検、データ整合性確認、発行履歴DB削除、外字適応、システム構築等
②取扱いを委託する特定個人情報ファイルの範囲		特定個人情報ファイルの全体 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 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	「2. ③対象となる本人の範囲」と同上。
	その妥当性	専門的なスキルが必要な業務について民間事業者に委託できる範囲内で委託することで、安定したシステム環境を効率的に維持することができ、コストの低減と行政サービスの向上を図る。
	③委託先における取扱者数	
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		中野区区政情報の公開に関する条例に基づく開示請求を行うことで確認ができる。
⑥委託先名		富士フィルムシステムサービス株式会社
再委託	⑦再委託の有無 ※	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	委託内容(範囲)、委託理由、委託先の監督方法等を明記した書面により報告し、妥当なものであれば再委託を認める。
	⑨再委託事項	問合せ対応、業務アプリケーションソフトの適用業務、ハードウェア及び業務アプリケーションの設定変更等、障害対応、定期点検、データ整合性確認、発行履歴DB削除、外字適応等

5. 特定個人情報の提供・移転(委託に伴うものを除く。)

提供・移転の有無

[] 提供を行っている () 件 [] 移転を行っている () 件
[○] 行っていない

6. 特定個人情報の保管・消去

①保管場所 ※		入退室管理(生体認証装置付)を実施している部屋に設置したサーバ内に記録している。 サーバへのアクセスは、指定された端末からのID／パスワードによる認証が必要となる。
②保管期間	期間	＜選択肢＞ 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない [20年以上]
	その妥当性	・住民基本台帳に記載されている限り保管が必要
③消去方法		コンビニ情報データベースに記録された特定個人情報のうち、保存年限に従いデータを年に1回、システムにて判別し消去する。

7. 備考

—

(別添2) 特定個人情報ファイル記録項目

別紙3参照

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

1. 特定個人情報ファイル名

(1) 住民基本台帳ファイル

2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）

リスク1： 目的外の入手が行われるリスク

対象者以外の情報の入手を防止するための措置の内容	・既存住基システムへの情報の登録の際に、届出／申請等の窓口において届出／申請内容や本人確認書類（個人番号カード等）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。 ・届出／申請書を既存住基システムへ入力後、届出／申請書と既存住基システムの入力内容を照合し、確認を行う。
必要な情報以外を入手することを防止するための措置の内容	・届出／申請等の様式において届出／申請等を行う者が記載する部分は、住民基本台帳業務に必要な項目のみに限っている。 ・届出／申請書を既存住基システムへ入力後、届出／申請書と既存住基システムの入力内容を照合し、確認を行う。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク2： 不適切な方法で入手が行われるリスク

リスクに対する措置の内容	・届出／申請等の窓口において、届出／申請等を行う者が記載した届出／申請書等は、窓口から離席する際は携行するなど、職員の管理下に置くことを徹底している。 ・既存住基システムを利用する必要がある職員を特定し、ユーザーIDによる識別とパスワードによる認証を実施する。また、認証後は利用機能の認可機能により、そのユーザーが既存住基システム上で利用可能な機能を制限することで不適切な方法で入手が行えない対策を実施している。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク3： 入手した特定個人情報が不正確であるリスク

入手の際の本人確認の措置の内容	・窓口において、対面で本人確認書類（個人番号カード等）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（通知カードの所持者にあつては、通知カードと法令により定められた本人確認書類の組合せ）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	・特定個人情報の入力、削除及び訂正を行う際は、整合性を確保するため、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、当区で定める規程に基づいて管理し、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4： 入手の際に特定個人情報が漏えい・紛失するリスク

リスクに対する措置の内容	・住民からの届出／申請書については、特定個人情報の漏えい及び紛失を防止するため、入力及び照合した後は、当区の規程により定められる期間、施錠して保管する。 ・既存住基システムは認められたシステム以外とは外部接続できない仕組みである。 ・住基ネットシステムにおける通信はすべて専用回線及び専用交換装置で構成されたネットワークを介して行い、また、通信を行うごとに、意図した通信相手に接続されたことを相互に認証する仕組みを採用している。
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	個人番号利用業務以外又は個人番号を必要としない業務から住民情報の要求があった場合は、個人番号が含まれない情報のみを提供するようにアクセス制御を行っている。	
事務で使用するその他のシステムにおける措置の内容	特定個人情報の使用権限を持つ業務と不必要な業務を特定して、特定個人情報へのアクセスを管理している。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2: 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	・業務端末については、二要素認証(生体認証とパスワード)を導入し、厳格なユーザ認証を実施している。 ・システムについては、ユーザID及びパスワードによる認証を実施しており、そのユーザがシステム上で利用可能な機能を制限することで、不正利用ができない対策を実施している。	
アクセス権限の発効・失効の管理	[行っている]	<選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	【発効管理】 ユーザごとのアクセス権限の登録及び変更は、情報システム担当課の管理担当者が行っており、その他の者は、アクセス権限の登録及び変更を行うためのアクセス権限が与えられていない。 ②失効管理 人事異動等により権限が変更または不要となった場合は、情報システム担当課の管理担当者が不要となったユーザIDや権限を変更または削除する。	
アクセス権限の管理	[行っている]	<選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	ユーザID及びアクセス権限については、情報システム担当課の管理担当者が管理を行っており、職員の異動及び業務の担当内容の変更等について、定期的に確認し、不要となったユーザIDや権限を変更または削除している。	
特定個人情報の使用の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	・個人を特定した検索及び操作の記録を行っている。 ・記録したログは、システム上3年間保管しており、システム全体の運用管理を担うシステム管理者が解析・追跡できる仕組みとなっている。	
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	・アクセスログを取得するとともに、定期的にログを解析できる仕組み、不正利用された場合にログを追跡できる仕組みを用意する。 ・従業者に対するセキュリティ教育を年に1度行っている。 ・業務時間中、所属長等が定期的に職場を巡回し、情報資産の管理を徹底している。 ・執務室の扉は施錠されており、カードキーがなければ入室できない。 休日は、事前の届出がなければカードキーがあっても入室できない。 ・執務室の扉に至るまでの廊下等には監視カメラが設置されている。 ・個人情報に係るメモ用紙や執務室内における携帯端末(スマートフォン等)の管理を徹底している。	
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: 特定個人情報ファイルが不正に複製されるリスク		
リスクに対する措置の内容	・システム操作を行う端末はスクリーンショットの取得やローカルフォルダへのデータ保存を禁止しており、業務用端末から行うことができる処理は特定個人情報の照会・更新であり、特定個人情報ファイルそのものを複製することはできない。 ・違反行為に対しては、区は、法の罰則規定を踏まえ適切な対応を行う。なお、職員の場合はあわせて、地方公務員法及び中野区職員の懲戒に関する規定に基づく措置を講じる。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
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		
特定個人情報が表示された画面のハードコピーの取得は、事務処理に必要となる範囲にとどめるほか、所管課設置の既存住基システム端末からはできない仕組みとなっている。		

4. 特定個人情報ファイルの取扱いの委託		[] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認	個人情報を扱う業務を委託するときは、個人情報の保護に関する法律、中野区個人情報の保護に関する法律施行条例及び中野区個人情報の保護に関する法律等施行規則、並びに中野区情報安全対策基本方針に基づき、個人情報保護に関する遵守事項及び外部委託情報安全対策遵守事項について契約に含むことで、特定個人情報の保護についても万全を期している。 なお、委託事業者の募集要項に、「一般財団法人日本情報経済社会推進協会が承認する「プライバシーマーク」又は「ISMS適合性評価制度」の認定を受けていることを応募要件としている。	
特定個人情報ファイルの閲覧者・更新者の制限	[制限している]	＜選択肢＞ 1) 制限している 2) 制限していない
具体的な制限方法	・委託にかかる実施体制の提出を義務付けている。 ・契約書に個人情報保護に関する遵守すべき事項を明記し、従事者名簿の提出やセキュリティ研修の実施等を義務付けている。 ・従事者名簿に記載のあった従事者に対してのみシステム操作の権限を与え、閲覧／更新権限を持つ者を必要最小限にする。 ・閲覧／更新権限を持つ者のアカウント管理を行い、システム上で操作を制限する。	
特定個人情報ファイルの取扱いの記録	[記録を残している]	＜選択肢＞ 1) 記録を残している 2) 記録を残していない
具体的な方法	・個人を特定した検索及び操作の記録を行っている。 ・記録したログは、システム上3年間保管しており、システム全体の運用管理を担うシステム管理者が解析・追跡できる仕組みとなっている。	
特定個人情報の提供ルール	[定めている]	＜選択肢＞ 1) 定めている 2) 定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	委託先から他者への提供は認めていない。	
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	・個人情報の適切な取扱いに関する条項を含む契約を締結している。 ・日常運用におけるチェックを行っている。 ・委託契約の報告条項に基づき必要があると認めるときは調査を行い、または書面にて報告を求める。	
特定個人情報の消去ルール	[定めている]	＜選択肢＞ 1) 定めている 2) 定めていない
ルールの内容及びルール遵守の確認方法	委託先に特定個人情報の消去を行わせるときは、物理的な破壊・専用ソフトウェアによるフォーマット等により、内容を読み出すことができないようにさせ、消去を証する書面の提出を求めることとし、必要に応じ、実地の検査等により確認することとする。	
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[定めている]	＜選択肢＞ 1) 定めている 2) 定めていない
規定の内容	個人情報の保護に関する法律等及び中野区情報安全対策基本方針に基づき、個人情報保護に関する遵守事項及び外部委託情報安全対策遵守事項を含む契約書の中で、特定個人情報を含む全てのデータについて以下のことを明記している。 ・業務上知り得た情報について、第三者に開示・提供・漏えいしてはならない。なお、本契約終了後も同様とする。 ・契約を履行するにあたり知り得た個人情報の漏えい、紛失、改ざん及び破損を防止するため、必要かつ適切な措置を講じなければならない。 ・中野区が提供した個人情報の内容を中野区が許可した範囲を超えて複写し、又は複製してはならない。 ・契約業務に従事する者に個人情報を取り扱わせる場合は、当該個人情報の安全管理が図られるよう、当該従事者に対する必要かつ適切な教育及び監督を行わなければならない。 ・事故が生じたときは直ちに中野区に対して連絡するとともに、遅滞なくその状況について書面により中野区に報告し、中野区の指示に従わなければならない。	
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	許可のない再委託は禁止している。許可した場合でも通常の委託と同様の措置を義務付けている。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
—		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[] 提供・移転しない	
リスク1： 不正な提供・移転が行われるリスク			
特定個人情報の提供・移転の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない	
具体的な方法	・移転は庁内ネットワークや庁内システム間連携のみであるため、連携時のログ、アクセスログ及び收受両システムのタイムスタンプにより確認できる。		
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	・番号法及び条例の規定により認められた範囲内においてのみ、情報の提供・移転を行う。 ・移転を開始する前に、情報を保有する部長に対し情報の利用の協議をすることを規則で定めている。		
その他の措置の内容	「サーバ室等への入室権限」及び「住民基本台帳ファイルを扱うシステムへのアクセス制限」を有する者を、当区の規程に基づき厳格に管理し、情報の持ち出しを制限する。		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
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	・法令に基づく情報の提供については、その法令で定める情報・項目について、法令・法令に基づく基準で定める方法に則り、提供する。 ・個人情報の目的外利用・外部提供に該当する場合には、責任者の決裁を伴う所定の手続きを経た上で行うこととすることで、あらかじめ情報提供の適法性を確保する。		
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： 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	・品質やセキュリティが保証されている連携システムでのみの移転に限定している。 ・移転に関する連携システムでの十分な検証を行う。		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
特定個人情報の提供・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			
・システム管理者の許可なく端末のUSBポート・CDドライブ等を使用できない仕組みになっている。			
6. 情報提供ネットワークシステムとの接続		[○] 接続しない(入手) [] 接続しない(提供)	
リスク1： 目的外の入手が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク2： 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク3： 入手した特定個人情報が不正確であるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	

リスク5： 不正な提供が行われるリスク		
リスクに対する措置の内容	①特定個人情報の情報照会があった場合、番号法で提供が認められている事務以外に情報を提供しないように判別する仕組みがシステム上担保されている。 ②特定個人情報が不正に提供されないように、情報照会に対しては業務コードを判別し、自動的に照会内容に対応する情報を送付する仕組みがシステム上担保されている。 ③特に慎重な対応が求められる情報については、自動的に送付しないように制限をかけて送信内容を確認してから提供できるように設定できる仕組みがシステム上担保されている。 ④従業者による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制するために、住民情報連携基盤システムへの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、操作内容を記録している。	
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	①提供の安全性を確保するために、送受信するデータについて暗号化した上で情報提供を行う仕組みがシステム上担保されている。 ②従業者による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制するために、住民情報連携基盤システムへの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、操作内容を記録している。 ③法や規程等で定められた方法以外で提供が行われないように、中間サーバと住民情報連携基盤システム、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)を利用している。 ④中間サーバ・プラットフォームを利用する団体であっても、他団体が管理する情報には一切アクセスできない仕組みがシステム上担保されている。 ⑤中間サーバ・プラットフォームの保守・運用を行う事業者が不適切な方法での情報提供を行えないように、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っている。	
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	①誤った相手に特定個人情報が提供されないように、情報照会者の情報を適切に受領し、情報照会者へ自動的に提供する仕組みがシステム上担保されている。 ②誤った特定個人情報が提供されないように、情報提供内容をシステムでチェックし、接続端末の画面でも情報提供内容を確認できる仕組みがシステム上担保されている。	
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
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		
①不正な名寄せが行われないように、特定個人情報に紐付く番号(情報提供用個人識別符号)を情報連携においてのみ利用することがシステム上担保されている。 ②外部から不正に特定個人情報にアクセスされないように、中間サーバと住民情報連携基盤システム、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)を利用している。また、中間サーバ・プラットフォームを利用する団体であっても、他団体が管理する情報には一切アクセスできない仕組みがシステム上担保されている。 ③中間サーバ・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化するために、特定個人情報の管理は地方公共団体のみが行う。		
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 具体的な対策の内容	[十分にやっている] <選択肢> 1) 特に力を入れて行っている 2) 十分にやっている 3) 十分にやっていない <中間サーバー・プラットフォームにおける措置> ・中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 <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 具体的な対策の内容	[十分にやっている] <選択肢> 1) 特に力を入れて行っている 2) 十分にやっている 3) 十分にやっていない <中間サーバー・プラットフォームにおける措置> ・中間サーバー・プラットフォームではUTM(コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置)等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ・中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ・導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 <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	[十分にやっている] <選択肢> 1) 特に力を入れて行っている 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) 特に力を入れて行っている 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 その内容 再発防止策の内容	[発生なし] <選択肢> 1) 発生あり 2) 発生なし — —
⑩死者の個人番号 具体的な保管方法	[保管している] <選択肢> 1) 保管している 2) 保管していない ・住民基本台帳においては死者も除票住民票として管理しているため、現存者と同様の管理となっている。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク2： 特定個人情報古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	住基法施行令第11条(届出に基づく住民票の記載等)及び第12条(職権による住民票の記載等)の規定に基づき住民票の記載、消除又は記載の修正を行うとともに、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)の規定に基づき必要な措置を講じることで、本特定個人情報の正確性を確保する。	
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	<中野区における措置> ・法令等の定めによる保存期間が経過したデータは一定期間経過後に消去する。 ・消去の際は、物理的な破壊、消去ソフトの使用等により、判読不能な状態にする。 <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		
—		

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

1. 特定個人情報ファイル名	
(2)本人確認情報ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	本人確認情報の入手元は既存住基システムに限定されるため、既存住基システムへの情報の登録の際に、届出の窓口において届出内容や本人確認書類（個人番号カード等）の確認を厳格に行い、対象者以外の情報の入手の防止に努める。
必要な情報以外を入手することを防止するための措置の内容	・平成14年6月10日総務省告示第334号（第6－7 本人確認情報の通知及び記録）等により市町村CSにおいて既存住基システムを通じて入手することとされている情報以外を入手できないことを、システム上で担保する。 ・正当な利用目的以外の目的にデータベースが構成されることを防止するため、本人確認情報の検索を行う際の検索条件として、少なくとも性別を除く2情報以上（氏名と住所の組合せ、氏名と生年月日の組合せ）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が不正確であるリスク	
入手の際の本人確認の措置の内容	・窓口において、対面で本人確認書類（個人番号カード等）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本人確認書類の組合せ）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、当区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	本人確認情報の正確性を維持するため、中野区住民基本台帳ネットワークシステム事務処理基準に基づいて本人確認情報の入力、削除及び訂正が行われていることを定期的に確認する。
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： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	・機構が作成・配布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。 ・静脈認証による操作者認証を行う。 ※市町村CSのサーバ上で稼働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、事務に必要なない情報との紐付けが行われるリスク		
宛名システム等における措置の内容	市町村CSと宛名管理システム間の接続は行わない。	
事務で使用するその他のシステムにおける措置の内容	庁内システムにおける市町村CSへのアクセスは既存住基システムに限定しており、また、既存住基システムと市町村CS間では、法令に基づく事務で使用する以外の情報との紐付けは行わない。 なお、市町村CSのサーバ上には住基ネットシステムの管理及び運用に必要なソフトウェア以外作動させず、また、市町村CSが設置されたセグメントにあるハブには権限の無い者が機器を接続できないよう、適切な対策(物理的なアクセス制限、MACアドレスによるフィルタリング等)を講じる。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク2: 権限のない者(元職員、アクセス権限のない職員等)によって不正に使用されるリスク		
ユーザ認証の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない	
具体的な管理方法	静脈認証による操作者認証を行う。	
アクセス権限の発効・失効の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない	
具体的な管理方法	・アクセス権限と業務の対応表を作成する。 ・業務ごとに更新権限の必要があるか、照会権限のみでよいかを確認し、業務に必要なアクセス権限のみを許可している。 ・権限を有していた職員の異動退職情報を確認し、異動退職があった際はアクセス権限を速やかに更新し、当該IDを失効させている。	
アクセス権限の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない	
具体的な管理方法	・操作者の権限等に応じたアクセス権限が付与されるよう管理する。 ・不正アクセスを分析するために、市町村CS及び統合端末においてアプリケーションの操作履歴の記録を取得し、保管する。	
特定個人情報の使用の記録	[記録を残している] <選択肢> 1) 記録を残している 2) 記録を残していない	
具体的な方法	・本人確認情報を扱う住基ネットシステムの操作履歴(アクセスログ・操作ログ)を記録する。 ・不正な操作が無いことについて、操作履歴により適時確認する。 ・操作履歴の確認により本人確認情報の検索に関して不正な操作の疑いがある場合は、申請文書等との整合性を確認する。 ・バックアップされた操作履歴について、定められた期間、安全な場所に施錠保管する。	
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	・住基ネットシステムの操作履歴(操作ログ)を記録する。 ・担当者へのヒアリングを実施し、業務上必要のない検索又は抽出が行われていないことを確認する。 ・住基ネットシステム利用職員への研修会において、事務外利用の禁止等について指導する。 ・業務時間中、所属長等が定期的に職場を巡回し、情報資産の管理を徹底している ・執務室の扉は施錠されており、カードキーがなければ入室できない。 ・休日は、事前の届出がなければカードキーがあっても入室できない。 ・執務室の扉に至るまでの廊下等には監視カメラが設置されている。 ・個人情報に係るメモ用紙や執務室内における携帯端末(スマートフォン等)の管理を徹底している。 ・委託先に対しては当該事項について仕様書に定め、事務外利用の禁止を徹底させている。	
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: 特定個人情報ファイルが不正に複製されるリスク		
リスクに対する措置の内容	・所管課設置の統合端末からは物理的に複製できない仕組みとなっている。 ・システム上、管理権限を与えられた者以外、情報の複製は行えない仕組みとし、また、バックアップ以外にファイルを複製しないよう、職員・委託先等に指導する。 ・違反行為を行った場合は、法の罰則規定により措置を講じる。なお、職員の場合はあわせて、地方公務員法及び中野区職員の懲戒に関する条例の規定に基づく措置を講じる。	
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
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		
・統合端末のディスプレイを、来庁者から見えない位置に置く。 ・統合端末での画面のハードコピーの取得は、物理的にできない仕組みになっている。 ・大量のデータ出力に際しては、事前に管理責任者の承認を得る。		

4. 特定個人情報ファイルの取扱いの委託		[] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認		個人情報を扱う業務を委託するときは、個人情報の保護に関する法律、中野区個人情報の保護に関する法律施行条例及び中野区個人情報の保護に関する法律等施行規則、並びに中野区情報安全対策基本方針に基づき、個人情報保護に関する遵守事項及び外部委託情報安全対策遵守事項について契約を含むことで、特定個人情報の保護についても万全を期している。 なお、委託事業者の募集要項に、一般財団法人日本情報経済社会推進協会が承認する「プライバシーマーク」又は「ISMS適合性評価制度」の認定を受けていることを応募要件としている。
特定個人情報ファイルの閲覧者・更新者の制限	[制限している]	<選択肢> 1) 制限している 2) 制限していない
具体的な制限方法	委託にかかる実施体制の提出を義務付けている。 ・契約書に個人情報保護に関する遵守すべき事項を明記し、従事者名簿の提出やセキュリティ研修の実施等を義務付けている。 ・従事者名簿に記載のあった従事者に対してのみシステム操作の権限を与え、閲覧／更新権限を持つ者を必要最小限にする。 ・閲覧／更新権限を持つ者のアカウント管理を行い、システム上で操作を制限する。	
特定個人情報ファイルの取扱いの記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	・アクセスログによる記録を残している。	
特定個人情報の提供ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	委託事業者から他者への特定個人情報の提供は一切認めないことを契約書に明記している。また、委託契約の報告条項に基づき、必要があると認めるときは調査を行い、または書面にて報告を求める。	
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・保守運用委託やオペレーション業務委託に関しては、仕様書にて委託業務実施場所を中野区役所本庁舎内に限定し、外部への持ち出しを禁止している。 ・委託先に提供する際、日付及び件数を記録した受け渡しの確認印を押印させている。 ・委託契約の報告条項に基づき必要があると認めるときは調査を行い、または書面にて報告を求める。	
特定個人情報の消去ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
ルールの内容及びルール遵守の確認方法	委託契約書に、以下の措置をとる旨を規定する。 ・保管期間の過ぎた特定個人情報を、システムにて自動判別し消去 ・紙媒体は、保管期間ごとに分けて保管し、保管期間が過ぎているものを外部業者にて溶解処理 ・データか紙かを問わず、廃棄の際は廃棄履歴を作成し保存 ・特定個人情報と同様、保管期間の過ぎたバックアップを、システムにて自動判別し消去 また、委託契約の報告条項に基づき、定期的に特定個人情報の取扱いについて書面にて報告させ、必要があれば当区職員が現地調査することも可能とする。	
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[定めている]	<選択肢> 1) 定めている 2) 定めていない
規定の内容	個人情報の保護に関する法律等及び中野区情報安全対策基本方針に基づき、個人情報保護に関する遵守事項及び外部委託情報安全対策遵守事項を含む契約書の中で、特定個人情報を含む全てのデータについて以下のことを明記している。 ・業務上知り得た情報について、第三者に開示・提供・漏えいしてはならない。なお、本契約終了後も同様とする。 ・契約を履行するにあたり知り得た個人情報の漏えい、紛失、改ざん及び破損を防止するため、必要かつ適切な措置を講じなければならない。 ・中野区が提供した個人情報の内容を中野区が許可した範囲を超えて複写し、又は複製してはならない。 ・契約業務に従事する者に個人情報を取り扱わせる場合は、当該個人情報の安全管理が図られるよう、当該従事者に対する必要かつ適切な教育及び監督を行わなければならない。 ・事故が生じたときは直ちに中野区に対して連絡するとともに、遅滞なくその状況について書面により中野区に報告し、中野区の指示に従わなければならない。	
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ない 2) 十分に行っている 3) 十分に行っていない 4) 再委託していない
具体的な方法	許可のない再委託は禁止している。許可した場合でも通常の委託と同様の措置を義務付けている。	
その他の措置の内容		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
—		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[] 提供・移転しない	
リスク1： 不正な提供・移転が行われるリスク			
特定個人情報の提供・移転の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない	
具体的な方法	特定個人情報（個人番号、4情報等）の提供・移転を行う際に、提供・移転の記録（提供・移転日時、操作者等）をシステム上で管理し、5年分保存する。 なお、システム上、提供・移転に係る処理を行ったものの提供・移転が認められなかった場合についても記録を残す。		
特定個人情報の提供・移転に関するルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない	
ルールの内容及びルール遵守の確認方法	・相手方（都道府県サーバ）と当区CS間の通信は、専用回線であり相互認証を実施している住民基本台帳ネットワーク以外では行わない。 ・当区CSは、既存住基システムとの通信において専用回線を用いて相互認証を実施している。 ・また、外部媒体を使用する場合においても、当区の規程を整備し、法令を遵守して提供・移転を行う。		
その他の措置の内容	「サーバ室等への入室権限」及び「本特定個人情報ファイルを扱うシステムへのアクセス権限」を有する者を厳格に管理し、情報の持ち出しを制限する。		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク2： 不適切な方法で提供・移転が行われるリスク			
リスクに対する措置の内容	相手方（都道府県サーバ）と市町村CSの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。 また、媒体へ出力する必要がある場合には、逐一出力の記録が残される仕組みを構築する。		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク			
リスクに対する措置の内容	・誤った情報を提供・移転してしまうリスクへの措置 システム上、照会元から指定された検索条件に基づき得た結果を適切に提供・移転することを担保する。 また、本人確認情報に変更が生じた際には、市町村CSへの登録時点で項目のフォーマットチェックや論理チェック（例えば、現存する住民に対して転入を異動事由とする更新が行われようとした場合や、転居を異動事由とする更新の際に住所以外の更新が行われようとした場合に当該処理をエラーとする）がなされた情報を通知することをシステム上で担保する。 ・誤った相手に提供・移転してしまうリスクへの措置 相手方（都道府県サーバ）と市町村CSの間の通信では相互認証を実施するため、認証できない相手先への情報の提供はなされないことがシステム上担保される。		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置			
—			
6. 情報提供ネットワークシステムとの接続		[○] 接続しない（入手） [○] 接続しない（提供）	
リスク1： 目的外の入手が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク2： 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク3： 入手した特定個人情報 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	

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: 特定個人情報が古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	既存住基システムとの整合処理を定期的に実施し、保存する本人確認情報が最新であるかどうかを確認することにより担保する。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	<選択肢> 1) 定めている 2) 定めていない
手順の内容	・システム上、住民基本台帳法施行令第34条第2項(保存)に定める期間(150年間)を経過した住民票の記載の修正前の本人確認情報(履歴情報)及び消除者の本人確認情報を消去する仕組みとする。 ・磁気ディスクの廃棄時は、専用ソフトによるフォーマット、物理的粉碎等を行うことにより、内容を読み出すことができないようにする。 ・中野区住民基本台帳ネットワーク事務処理基準に基づき、帳票については、帳簿等を作成し、保管及び廃棄の運用が適切になされていることを適時確認するとともに、その記録を残す。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		
—		

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

1. 特定個人情報ファイル名	
(3)送付先情報ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	送付先情報の入手元は既存住基システムに限定されるため、既存住基システムへの情報の登録の際に、届出の窓口において届出内容や本人確認書類（個人番号カード等）の確認を厳格に行い、対象者以外の情報の入手の防止に努める。
必要な情報以外を入手することを防止するための措置の内容	・平成14年6月10日総務省告示第334号（第6ー7 本人確認情報の通知及び記録）等により市町村CSにおいて既存住基システムを通じて入手することとされている情報以外を入手できないことを、システム上で担保する。 ・正当な利用目的以外の目的にデータベースが構成されることを防止するため、本人確認情報の検索を行う際の検索条件として、少なくとも性別を除く2情報以上（氏名と住所の組合せ、氏名と生年月日の組合せ）の指定を必須とする。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	送付先情報の入手元を既存住基システムに限定する。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	特定個人情報の入手元である既存住基システムへの情報の登録の際、窓口において、対面で本人確認書類（個人番号カード等）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、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。
その他の措置の内容	送付先情報の正確性を維持するため、中野区住民基本台帳ネットワークシステム事務処理基準に基づいて送付先情報の入力、削除及び訂正が行われていることを定期的に確認する。
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： 入手の際に特定個人情報が増えい・紛失するリスク	
リスクに対する措置の内容	・機構が作成・配布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。 ・静脈認証による操作者認証を行う。 ※市町村CSのサーバ上で稼働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のサーバ上には住基ネットシステムの管理及び運用に必要なソフトウェア以外作動させず、また、市町村CSが設置されたセグメントにあるハブには権限の無い者が機器を接続できないよう、適切な対策(物理的なアクセス制限、MACアドレスによるフィルタリング等)を講じる。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク2： 権限のない者(元職員、アクセス権限のない職員等)によって不正に使用されるリスク		
ユーザ認証の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない	
具体的な管理方法	静脈認証による操作者認証を行う。	
アクセス権限の発効・失効の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない	
具体的な管理方法	・アクセス権限と業務の対応表を作成する。 ・業務ごとに更新権限の必要があるか、照会権限のみでよいかを確認し、業務に必要なアクセス権限のみを許可している。 ・権限を有していた職員の異動退職情報を確認し、異動退職があった際はアクセス権限を速やかに更新し、当該IDを失効させている。	
アクセス権限の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない	
具体的な管理方法	・操作者の権限等に応じたアクセス権限が付与されるよう管理する。 ・不正アクセスを分析するために、市町村CS及び統合端末においてアプリケーションの操作履歴の記録を取得し、保管する。	
特定個人情報の使用の記録	[記録を残している] <選択肢> 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	・送付先情報を扱う住基ネットシステムの操作履歴(アクセスログ・操作ログ)を記録する。 ・不正な操作が無いことについて、操作履歴により適時確認する。 ・操作履歴の確認により送付先情報の検索に関して不正な操作の疑いがある場合は、申請文書等との整合性を確認する。 ・バックアップされた操作履歴について、定められた期間、安全な場所に施錠保管する。	
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	・住基ネットシステムの操作履歴(操作ログ)を記録する。 ・担当者へのヒアリングを実施し、業務上必要のない検索又は抽出が行われていないことを確認する。 ・住基ネットシステム利用職員への研修会において、事務外利用の禁止等について指導する。 ・業務時間中、所属長等が定期的に職場を巡回し、情報資産の管理を徹底している。 ・執務室の扉は施錠されており、カードキーがなければ入室できない。 休日は、事前の届出がなければカードキーがあっても入室できない。 ・執務室の扉に至るまでの廊下等には監視カメラが設置されている。 ・個人情報に係るメモ用紙や執務室内における携帯端末(スマートフォン等)の管理を徹底している。 ・委託先に対しては当該事項について仕様書に定め、事務外利用の禁止を徹底させている。	
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： 特定個人情報ファイルが不正に複製されるリスク		
リスクに対する措置の内容	・所管課設置の統合端末からは物理的に複製できない仕組みとなっている。 ・システム上、管理権限を与えられた者以外、情報の複製は行えない仕組みとし、また、バックアップ以外にファイルを複製しないよう、職員・委託先等に指導する。 ・違反行為を行った場合は、法の罰則規定により措置を講じる。なお、職員の場合はあわせて、地方公務員法及び中野区職員の懲戒に関する条例の規定に基づく措置を講じる。	
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
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		
・統合端末のディスプレイを、来庁者から見えない位置に置く。 ・統合端末での画面のハードコピーの取得は、物理的にできない仕組みになっている。 ・大量のデータ出力に際しては、事前に管理責任者の承認を得る。		

4. 特定個人情報ファイルの取扱いの委託		[] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認	個人情報を扱う業務を委託するときは、個人情報の保護に関する法律、中野区個人情報の保護に関する法律施行条例及び中野区個人情報の保護に関する法律等施行規則、並びに中野区情報安全対策基本方針に基づき、個人情報保護に関する遵守事項及び外部委託情報安全対策遵守事項について契約に含むことで、特定個人情報の保護についても万全を期している。 なお、委託事業者の募集要項に、一般財団法人日本情報経済社会推進協会が承認する「プライバシーマーク」又は「ISMS適合性評価制度」の認定を受けていることを応募要件としている。	
特定個人情報ファイルの閲覧者・更新者の制限	[制限している]	＜選択肢＞ 1) 制限している 2) 制限していない
具体的な制限方法	委託にかかる実施体制の提出を義務付けている。 ・契約書に個人情報保護に関する遵守すべき事項を明記し、従事者名簿の提出やセキュリティ研修の実施等を義務付けている。 ・従事者名簿に記載のあった従事者に対してのみシステム操作の権限を与え、閲覧／更新権限を持つ者を必要最小限にする。 ・閲覧／更新権限を持つ者のアカウント管理を行い、システム上で操作を制限する。	
特定個人情報ファイルの取扱いの記録	[記録を残している]	＜選択肢＞ 1) 記録を残している 2) 記録を残していない
具体的な方法	・アクセスログによる記録を残している。	
特定個人情報の提供ルール	[定めている]	＜選択肢＞ 1) 定めている 2) 定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	委託事業者から他者への特定個人情報の提供は一切認めないことを契約書に明記している。 また、委託契約の報告条項に基づき、必要があると認めるときは調査を行い、または書面にて報告を求める。	
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・保守運用委託やオペレーション業務委託に関しては、仕様書にて委託業務実施場所を中野区役所本庁舎内に限定し、外部への持ち出しを禁止している。 ・委託先に提供する際、日付及び件数を記録した受け渡しの確認印を押印させている。 ・委託契約の報告条項に基づき必要があると認めるときは調査を行い、または書面にて報告を求める。	
特定個人情報の消去ルール	[定めている]	＜選択肢＞ 1) 定めている 2) 定めていない
ルールの内容及びルール遵守の確認方法	送付先情報はシステムで連携が終わり次第自動的に消去する仕組みとなっているほか、紙媒体は、保管期間ごとに分けて保管し、保管期間が過ぎているものを外部業者に溶解処理をする旨を委託契約書に規定する。 また、委託契約の報告条項に基づき、定期的に特定個人情報の取扱いについて書面にて報告させ、必要があれば当区職員が現地調査することも可能とする。	
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[定めている]	＜選択肢＞ 1) 定めている 2) 定めていない
規定の内容	個人情報の保護に関する法律等及び中野区情報安全対策基本方針に基づき、個人情報保護に関する遵守事項及び外部委託情報安全対策遵守事項を含む契約書の中で、特定個人情報を含む全てのデータについて以下のことを明記している。 ・業務上知り得た情報について、第三者に開示・提供・漏えいしてはならない。なお、本契約終了後も同様とする。 ・契約を履行するにあたり知り得た個人情報の漏えい、紛失、改ざん及び破損を防止するため、必要かつ適切な措置を講じなければならない。 ・中野区が提供した個人情報の内容を中野区が許可した範囲を超えて複写し、又は複製してはならない。 ・契約業務に従事する者に個人情報を取り扱わせる場合は、当該個人情報の安全管理が図られるよう、当該従事者に対する必要かつ適切な教育及び監督を行わなければならない。 ・事故が生じたときは直ちに中野区に対して連絡するとともに、遅滞なくその状況について書面により中野区に報告し、中野区の指示に従わなければならない。	
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	許可のない再委託は禁止している。許可した場合でも通常の委託と同様の措置を義務付けている。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
—		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[記録を残している]	☐ 記録を残している 2) 記録を残していない ☐ 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、提供の記録（提供日時、操作者等）をシステム上で管理する。	
特定個人情報の提供・移転に関するルール	[定めている]	☐ 定めている 2) 定めていない ☐ 定めていない
ルールの内容及びルール遵守の確認方法	・相手方（個人番号カード管理システム）と当区CS間の通信は、専用回線であり相互認証を実施している住民基本台帳ネットワーク以外では行わない。 ・当区CSは、既存住基システムとの通信において専用回線を用いて相互認証を実施している。 ・また、外部媒体を使用する場合においても、当区の規程を整備し、法令を遵守して提供・移転を行う。	
その他の措置の内容	「サーバ室等への入室権限」及び「本特定個人情報ファイルを扱うシステムへのアクセス権限」を有する者を厳格に管理し、情報の持ち出しを制限する。	
リスクへの対策は十分か	[十分である]	☐ 十分である 2) 十分である ☐ 十分でない
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]	☐ 十分である 2) 十分である ☐ 十分でない
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]	☐ 十分である 2) 十分である ☐ 十分でない
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	[]	☐ 十分である 2) 十分である ☐ 十分でない
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	[]	☐ 十分である 2) 十分である ☐ 十分でない
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	[]	☐ 十分である 2) 十分である ☐ 十分でない

リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク					
リスクに対する措置の内容					
リスクへの対策は十分か	[]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている			
リスク5： 不正な提供が行われるリスク					
リスクに対する措置の内容					
リスクへの対策は十分か	[]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている			
リスク6： 不適切な方法で提供されるリスク					
リスクに対する措置の内容					
リスクへの対策は十分か	[]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている			
リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク					
リスクに対する措置の内容					
リスクへの対策は十分か	[]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている			
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置					
7. 特定個人情報の保管・消去					
リスク1： 特定個人情報の漏えい・滅失・毀損リスク					
①NISC政府機関統一基準群	[政府機関ではない]	＜選択肢＞ 1) 特に力を入れて遵守している 2)十分に遵守している 3)十分に遵守していない 4) 政府機関ではない			
②安全管理体制	[十分に整備している]	＜選択肢＞ 1) 特に力を入れて整備している 2)十分に整備している 3)十分に整備していない			
③安全管理規程	[十分に整備している]	＜選択肢＞ 1) 特に力を入れて整備している 2)十分に整備している 3)十分に整備していない			
④安全管理体制・規程の職員への周知	[十分に周知している]	＜選択肢＞ 1) 特に力を入れて周知している 2)十分に周知している 3)十分に周知していない			
⑤物理的対策	[十分に行っている]	＜選択肢＞ 1) 特に力を入れて行っている 2)十分に行っている 3)十分に行っていない			
	具体的な対策の内容	・サーバ室と、データ、プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する保管室は、他の部屋とは区別して専用の部屋としている。出入口にはIDと静脈認証による入退室管理を行っている。入退室管理を徹底するため出入口の場所を限定している。 ・停電(落雷等)によるデータの消失を防ぐために、サーバ等必要な機器に無停電電源装置を付設している。			
⑥技術的対策	[十分に行っている]	＜選択肢＞ 1) 特に力を入れて行っている 2)十分に行っている 3)十分に行っていない			
	具体的な対策の内容	・不正プログラム対策 コンピュータウイルス監視ソフトを使用し、サーバ・端末双方でウイルスチェックを実施する。また、新種の不正プログラムに対応するために、ウイルスパターンファイルは定期的に更新し、可能な限り最新のものを使用する。 送付先情報の管理について定めた規程に基づき、コンピュータウイルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。 また、同規程に基づき、オペレーション管理に係る手順等を整備し、当該手順に従って、情報セキュリティホールに関連する情報(コンピュータウイルス等の有害なソフトウェアに関連する情報を含む)を定期的(コンピュータウイルス関連情報は毎日、その他の情報は少なくとも半年に1度)に入手し、機器の情報セキュリティに関する設定の内容が適切かどうかを確認する。 ・不正アクセス対策 送付先情報の管理について定めた規程に基づき、ネットワーク管理に係る手順等を整備し、ファイアウォール、侵入検知システム(IDS)、侵入防御システム(IPS)を導入する。			

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) 十分にっていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	<選択肢> 1) 発生あり 2) 発生なし
その内容	—	
再発防止策の内容	—	
⑩死者の個人番号	[保管していない]	<選択肢> 1) 保管している 2) 保管していない
具体的な保管方法	—	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2: 特定個人情報が古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	本特定個人情報ファイル(送付先情報ファイル)は、送付先情報の連携を行う必要が生じた都度作成及び連携することとしており、システム上、連携後速やか(1営業日後)に削除する仕組みとする。また、媒体を用いて連携する場合、当該媒体は連携後、連携先である機構において適切に管理され、市町村では保管しない。そのため、送付先情報ファイルにおいて特定個人情報が古い情報のまま保管され続けるリスクは存在しない。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	<選択肢> 1) 定めている 2) 定めていない
手順の内容	・システム上、保管期間の経過した特定個人情報を一括して削除する仕組みとする。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		
送付先情報ファイルは、機構への特定個人情報の提供後、速やかに市町村CSから削除される。その後、当該特定個人情報は機構において管理されるため、送付先情報ファイルのバックアップは取得しない予定である。		

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

1. 特定個人情報ファイル名	
(4)コンビニ情報ファイル	
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	コンビニ情報の入手元は既存住基システムに限定されるため、届出の窓口において届出内容や本人確認書類(個人番号カード等)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	・コンビニシステムにおいて既存住基システムを通じて入手することとされている情報以外を入手できないことを、システム上で担保する。
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	コンビニ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が不正確であるリスク	
入手の際の本人確認の措置の内容	特定個人情報の入手元である既存住基システムへの情報の登録の際、窓口において、対面で本人確認書類(個人番号カード等)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	既存住基システムに登録された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コンビニ情報を適切に受信できることをシステムにより担保する。
その他の措置の内容	コンビニ情報の正確性を維持するため、既存住基システムとの整合性を定期的に確認する。
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： 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	・コンビニ情報の入手元を既存住基システムに限定する。 ・操作者の認証を行う。
リスクへの対策は十分か	[十分である] <選択肢> 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、事務に必要なない情報との紐付けが行われるリスク	
宛名システム等における措置の内容	コンビニシステム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コンビニシステムへのアクセスは既存住基システムに限定しており、また、システム間では、住民票の写し等証明書発行事務で使用する以外の情報との紐付けは行わない。 なお、コンビニシステムのサーバ上にはコンビニ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、コンビニシステム用端末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(MACアドレスによるフィルタリング)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	IDと暗証番号による操作者認証を行う。
アクセス権限の発効・失効の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	・アクセス権限と業務の対応表を作成する。 ・権限を有していた職員の異動退職情報を確認し、異動退職があった際はアクセス権限を速やかに更新し、当該IDを失効させている。
アクセス権限の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	・操作者の権限等に応じたアクセス権限が付与されるよう管理する。 ・不正アクセスを分析するために、コンビニシステム用端末においてアプリケーションの操作履歴の記録を取得し、保管する。
特定個人情報の使用の記録	[記録を残している] <選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	・コンビニシステムの操作履歴(アクセスログ・操作ログ)を記録する。 ・不正な操作が無いことについて、操作履歴により適時確認する。 ・操作履歴の確認によりコンビニシステムにおいて不正な操作の疑いがある場合は、利用登録申請文書等との整合性を確認する。 ・バックアップされた操作履歴について、定められた期間、安全な場所に施錠保管する。
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	・コンビニシステムの操作履歴(操作ログ)を記録する。 ・担当者へのヒアリングを実施し、業務上必要のない検索又は抽出が行われていないことを確認する。 ・コンビニシステム利用職員への研修会において、事務外利用の禁止等について指導する。 ・業務時間中、所属長等が定期的に職場を巡回し、情報資産の管理を徹底している。 ・執務室の扉は施錠されており、カードキーがなければ入室できない。 休日、事前の届出がなければカードキーがあっても入室できない。 ・執務室の扉に至るまでの廊下等には監視カメラが設置されている。 ・個人情報に係るメモ用紙や執務室内における携帯端末(スマートフォン等)の管理を徹底している。 ・委託先に対しては当該事項について仕様書に定め、事務外利用の禁止を徹底させている。
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: 特定個人情報ファイルが不正に複製されるリスク		
リスクに対する措置の内容	・所管課設置のコンビニシステム用端末には、デバイスロックをかけ、物理的に複製できない仕組みとなっている。 ・システム上、管理権限を与えられた者以外、情報の複製は行えない仕組みとし、また、バックアップ以外にファイルを複製しないよう、職員・委託先等に指導する。 ・違反行為を行った場合は、法の罰則規定により措置を講じる。なお、職員の場合はあわせて、地方公務員法及び中野区職員の懲戒に関する条例の規定に基づく措置を講じる。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
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		
・コンビニシステム用端末のディスプレイを、来庁者から見えない位置に置く。 ・大量のデータ出力に際しては、事前に管理責任者の承認を得る。 ・コンビニシステムの操作画面には個人番号を表示させない。		
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	個人情報を扱う業務を委託するときは、個人情報の保護に関する法律、中野区個人情報の保護に関する法律施行条例及び中野区個人情報の保護に関する法律等施行規則、並びに中野区情報安全対策基本方針に基づき、個人情報保護に関する遵守事項及び外部委託情報安全対策遵守事項について契約に含むことで、特定個人情報の保護についても万全を期している。 なお、委託事業者の募集要項に、一般財団法人日本情報経済社会推進協会が承認する「プライバシーマーク」又は「ISMS適合性評価制度」の認定を受けていることを応募要件としている。	
特定個人情報ファイルの閲覧者・更新者の制限	[制限している]	<選択肢> 1) 制限している 2) 制限していない
具体的な制限方法	委託にかかる実施体制の提出を義務付けている。 ・契約書に個人情報保護に関する遵守すべき事項を明記し、従事者名簿の提出やセキュリティ研修の実施等を義務付けている。 ・従事者名簿に記載のあった従事者に対してのみシステム操作の権限を与え、閲覧／更新権限を持つ者を必要最小限にする。 ・閲覧／更新権限を持つ者のアカウント管理を行い、システム上で操作を制限する。	
特定個人情報ファイルの取扱いの記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	・アクセスログによる記録を残している。	
特定個人情報の提供ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	委託事業者から他者への特定個人情報の提供は一切認めないことを契約書に明記している。また、委託契約の報告条項に基づき、必要があると認めるときは調査を行い、または書面にて報告を求める。	
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・保守運用委託に関しては、契約書にて委託業務実施場所を中野区役所本庁舎内に限定し、外部への持ち出しを禁止している。 ・委託契約の報告条項に基づき必要があると認めるときは調査を行い、または書面にて報告を求める。	
特定個人情報の消去ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
ルールの内容及びルール遵守の確認方法	委託契約書に、以下の措置をとる旨を規定する。 ・保管期間の過ぎた特定個人情報を、システムにて判別し消去 ・データ廃棄の際は廃棄履歴を作成し保存 ・特定個人情報と同様、保管期間の過ぎたバックアップを、システムで消去 また、委託契約の報告条項に基づき、定期的に特定個人情報の取扱いについて書面にて報告させ、必要があれば当区職員が調査することも可能とする。	

委託契約書中の特定個人情報ファイルの取扱いに関する規定			
規定の内容		個人情報の保護に関する法律等及び中野区情報安全対策基本方針に基づき、個人情報保護に関する遵守事項及び外部委託情報安全対策遵守事項を含む契約書の中で、特定個人情報を含む全てのデータについて以下のことを明記している。 ・業務上知り得た情報について、第三者に開示・提供・漏えいしてはならない。なお、本契約終了後も同様とする。 ・契約を履行するにあたり知り得た個人情報の漏えい、紛失、改ざん及び破損を防止するため、必要かつ適切な措置を講じなければならない。 ・中野区が提供した個人情報の内容を中野区が許可した範囲を超えて複写し、又は複製してはならない。 ・契約業務に従事する者に個人情報を取り扱わせる場合は、当該個人情報の安全管理が図られるよう、当該従事者に対する必要かつ適切な教育及び監督を行わなければならない。 ・事故が生じたときは直ちに中野区に対して連絡するとともに、遅滞なくその状況について書面により	
再委託先による特定個人情報ファイルの適切な取扱いの確保			
具体的な方法		許可のない再委託は禁止している。許可した場合でも通常の委託と同様の措置を義務付けている。	
その他の措置の内容			
リスクへの対策は十分か			
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置			
—			
5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。） [○] 提供・移転しない			
リスク1： 不正な提供・移転が行われるリスク			
特定個人情報の提供・移転の記録			
具体的な方法			
特定個人情報の提供・移転に関するルール			
ルール内容及びルール遵守の確認方法			
その他の措置の内容			
リスクへの対策は十分か			
リスク2： 不適切な方法で提供・移転が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か			
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク			
リスクに対する措置の内容			
リスクへの対策は十分か			
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置			

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

7. 特定個人情報の保管・消去		
リスク1: 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1) 特に力を入れて遵守している 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	・サーバ室と、データ、プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する保管室は、他の部屋とは区別して専用の部屋としている。出入口にはIDと静脈認証による入退室管理を行っている。入退室管理を徹底するため出入口の場所を限定している。 ・停電(落雷等)によるデータの消失を防ぐために、サーバ等必要な機器に無停電電源装置を付設している。
⑥技術的対策	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
	具体的な対策の内容	・不正プログラム対策 コンピュータウィルス監視ソフトを使用し、サーバ・端末双方でウィルスチェックを実施する。また、新種の不正プログラムに対応するために、ウィルスパターンファイルは定期的に更新し、可能な限り最新のものを使用する。 コンビニ情報の管理について定めた規程に基づき、コンピュータウィルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。 また、同規程に基づき、オペレーション管理に係る手順等を整備し、当該手順に従って、情報セキュリティホールに関連する情報(コンピュータウィルス等の有害なソフトウェアに関連する情報を含む)を定期的(コンピュータウィルス関連情報は毎日、その他の情報は少なくとも半年に1度)に入手し、機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。 ・不正アクセス対策 コンビニ情報の管理について定めた規程に基づき、ネットワーク管理に係る手順等を整備し、ファイアウォールを導入する。
⑦バックアップ	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
⑧事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	<選択肢> 1) 発生あり 2) 発生なし
	その内容	—
	再発防止策の内容	—
⑩死者の個人番号	[保管している]	<選択肢> 1) 保管している 2) 保管していない
	具体的な保管方法	死亡による削除データ受信後、システムにて判別しデータを削除
その他の措置の内容		—
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2: 特定個人情報が古い情報のまま保管され続けるリスク		
リスクに対する措置の内容		本特定個人情報ファイル(コンビニ情報ファイル)は、コンビニ情報の連携を行う必要が生じた都度作成及び連携することとしている。
リスクへの対策は十分か	[十分である]	<選択肢> 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。 ・削除されたデータについて、年に1回抹消処理を実行し、物理抹消されていることを確認する。
その他の措置の内容		—
リスクへの対策は十分か		[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
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		
—		

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	特定個人情報保護評価に関する規則第14条に規定する評価書の見直しについて、評価書の内容と運用実態のチェックを1年に1回担当部署内において行う。
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	<中野区における措置> ・中野区情報安全対策方針及び同基準に基づき、情報資産全体の情報安全保護についての外部監査を定期的に行う。監査結果を踏まえ、情報安全対策の改定の際に活用することとしている。 <中間サーバー・プラットフォームにおける措置> ・運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。 <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	・関係職員に対して、初任時及び1年毎に、必要な知識の習得に資するための研修を実施するとともに、その記録を残している。 ・各責任者に対して、その管理に関する必要な知識や技術を習得させる研修を実施するとともに、その記録を残している。 ・委託事業者に対しては、個人情報保護に関する条項を含む契約を締結している。 ・違反行為を行った場合は、法の罰則規定により措置を講じる。なお、職員の場合はあわせて、地方公務員法及び中野区職員の懲戒に関する条例の規定に基づく措置を講じる。
3. その他のリスク対策		
<ガバメントクラウドにおける措置> ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。 ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。 具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。		

V 開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	郵便番号164-8501 東京都中野区中野四丁目11番19号 中野区役所 区民部 戸籍住民課
②請求方法	個人情報の保護に関する法律第77条第1項の規定により、必要事項を記載した開示請求書を提出する。
特記事項	中野区ホームページ上に、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	[有料] ＜選択肢＞ 1) 有料 2) 無料 (手数料額、納付方法: 手数料額: 写しの交付10円／1枚 納付方法: 現金)
④個人情報ファイル簿の公表	[行っていない] ＜選択肢＞ 1) 行っている 2) 行っていない
個人情報ファイル名	住民基本台帳ファイル
公表場所	—
⑤法令による特別の手続	—
⑥個人情報ファイル簿への不記載等	—
2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	郵便番号164-8501 東京都中野区中野四丁目11番19号 中野区役所 区民部 戸籍住民課
②対応方法	問合せを受け付けた際には、対応内容について記録を残す。

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和7年1月22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	中野区自治基本条例及び中野区パブリック・コメント手続に関する規則の規定に基づきパブリックコメントによる意見聴取を実施する。パブリックコメントの実施に際しては、区報に公表している旨の記事を掲載し、区ホームページへの掲載と戸籍住民課、区政資料センター及び区民活動センターの窓口にて全文を閲覧できるようにする。
②実施日・期間	令和6年8月29日～令和6年9月27日
③期間を短縮する特段の理由	—
④主な意見の内容	なし(提出意見なし)
⑤評価書への反映	—
3. 第三者点検	
①実施日	令和6年11月19日
②方法	中野区個人情報の保護に関する法律施行条例第17条に基づき設置の中野区個人情報保護審議会に諮問し、点検を実施した。
③結果	特定個人情報保護評価指針(個人情報保護委員会作成)の審査の観点に照らし、本評価書の内容は適当と判断された。
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	

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1月22日	I 基本情報 1 特定個人情報を取り扱う事務 ②事務の内容	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、平成26年11月20日総務省令第85号（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）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。	なお、⑨の「個人番号の通知及び個人番号カードの交付」に係る事務については、行政手続における特定の個人を識別するための番号の利用等に関する法律に規定する個人番号、個人番号カード、特定個人情報の提供等に関する命令（平成26年11月20日総務省令第85号。以下「個人番号カード省令」という。）第35条（個人番号通知書、個人番号カード関連事務の委任）により機構に対する事務の一部の委任が認められている。 そのため、当該事務においては、事務を委任する機構に対する情報の提供を含めて特定個人情報ファイルを使用する。	事後	法令改正によるものであり、重要な変更にあたらぬ（リスク変動なし）
令和7年1月22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	(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（番号法第7条第1項）。通知カードによる番号の通知及び交付申請書の送付については、事務効率化等の観点から、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）に基づき、市町村から機構に委任するため、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。	(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	その他の項目の変更であり、事前の提出・公表が義務付けられない
令和7年1月22日	I 基本情報 6 情報提供ネットワークシステムによる情報連携 ②法令上の根拠	番号法第19条第7号及び別表二（別表第二における情報提供の根拠） 第四欄（特定個人情報） 1, 2, 3, 4, 6, 8, 9, 11, 16, 18, 20, 23, 27, 30, 31, 34, 35, 37, 38, 39, 40, 42, 48, 53, 54, 57, 58, 59, 61, 62, 66, 67, 70, 74, 77, 80, 84, 85の2, 89, 91, 92, 94, 96, 97, 101, 102, 103, 105, 106, 107, 108, 111, 112, 113, 114, 116, 117, 120の項 （別表第二における情報照会の根拠）	番号法第19条第8号及び同号に基づく主務省令第2条の表（番号法第19条第8号に基づく主務省令第2条の表における情報提供の根拠） 第四欄（利用特定個人情報） 1, 2, 3, 5, 7, 11, 13, 15, 20, 28, 37, 39, 48, 53, 57, 58, 59, 63, 65, 66, 69, 73, 75, 76, 81, 83, 84, 86, 87, 91, 92, 96, 106, 108, 110, 112, 115, 118, 124, 129, 130, 132, 136, 137, 138, 141, 142, 144, 149, 150, 151, 152, 155, 156, 158, 160, 163, 164, 165, 166の項 （番号法第19条第8号に基づく主務省令第2条の表における情報照会の根拠）	事後	法令改正によるものであり、重要な変更にあたらぬ
令和7年1月22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 (1)住民基本台帳ファイル 3 特定個人情報の入手・使用 ②入手方法	[○]その他（住基ネットシステム）	[○]その他（住基ネットシステム、申請管理システム、マイナポータルびったりサービス）	事後	その他の項目の変更であり、事前の提出・公表が義務付けられない
令和7年1月22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 (1)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 情報の突合	・住民異動届の際に入手する場合は、個人番号カード若しくは通知カードとその他本人確認書類で突合を行う。	・住民異動届の際に入手する場合は、個人番号カード等の本人確認書類で突合を行う。	事後	法令改正によるものであり、重要な変更にあたらぬ（リスク変動なし）
令和7年1月22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 (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2 ⑥委託先名	株式会社アール・ケー・ケー・コンピューター・サービス	株式会社RKKCS	事後	その他の項目の変更であり、事前の提出・公表が義務付けられない
令和7年1月22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 (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3 ③委託先における取扱者数	10人未満	10人以上50人未満	事後	その他の項目の変更であり、事前の提出・公表が義務付けられない
令和7年1月22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 (1)住民基本台帳ファイル 5 特定個人情報の提供・移転 提供先1 ①法令上の根拠 ②提供先における用途 ③提供する情報	番号法第19条第7号及び別表第二	番号法第19条第8号に基づく主務省令第2条の表	事後	法令改正によるものであり、重要な変更にあたらぬ

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1月22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 (1)住民基本台帳ファイル 6 特定個人情報の保管・消去 ①保管場所	庁舎の中で、入退室管理を実施している部屋に設置したサーバ内に記録している。 サーバへのアクセスは、指定された端末からのID／パスワードによる認証が必要となる。	＜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。	事前	重要な変更
令和7年1月22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 (1)住民基本台帳ファイル 6 特定個人情報の保管・消去 ②保管期間 その妥当性	・住民基本台帳に記載されている限り保管が必要 ・住基法施行令第34条第1項(保存)で規定する。削除された住民票については5年間保管する。	・住民票の記載の修正前の本人確認情報(履歴情報)及び消除者の本人確認情報は、住民基本台帳法施行令第34条第2項(保存)に定める期間(150年間)保管する。	事後	法令改正等によるものであり、重要な変更にあたらな
令和7年1月22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 (1)住民基本台帳ファイル 6 特定個人情報の保管・消去 ③消去方法	住民基本台帳データベース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。	＜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が、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。	事前	事前通知事項でなく、事後で足りるものの任意に事前に提出
令和7年1月22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 (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、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。 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。	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に送付する必要がある。 また、通知カード所持者にあつては、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	法令改正によるものであり、重要な変更にあたらな (リスク変動なし)
令和7年1月22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 (3)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	〔〇〕その他(通知カード及び交付申請書の送付先の情報)	〔〇〕その他(個人番号通知及び交付申請書の送付先の情報)	事後	法令改正によるものであり、重要な変更にあたらな (リスク変動なし)
令和7年1月22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 (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	・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、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。	・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	法令改正によるものであり、重要な変更にあたらな
令和7年1月22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 (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)。	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	法令改正によるものであり、重要な変更にあたらな

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1月22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 (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	送付先情報は、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)の規定に基づいて、機構に委任された事務において使用される。	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)	事後	法令改正によるものであり、重要な変更にあたらない
令和7年1月22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 (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	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。	・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	法令改正によるものであり、重要な変更にあたらない(リスク変動なし)
令和7年1月22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 (3)送付先情報ファイル 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	富士通Japan株式会社	事後	その他の項目の変更であり事前の提出・公表が義務付けられない
令和7年1月22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 (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	平成26年11月20日総務省令第85号第36条(通知カード・個人番号カード関連事務に係る通知)	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	法令改正によるものであり、重要な変更にあたらない
令和7年1月22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 (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。	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	法令改正によるものであり、重要な変更にあたらない
令和7年1月22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 (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)。	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	法令改正によるものであり、重要な変更にあたらない
令和7年1月22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 1 特定個人情報ファイル (1)住民基本台帳ファイル 2 特定個人情報の入手 リスク3: 入手した特定個人情報 が不正確であるリスク 個人番号の真正性確認の措置の内容	・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本人確認書類の組合せ)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。	・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(通知カードの所持者にとっては、通知カードと法令により定められた本人確認書類の組合せ)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。	事後	法令改正によるものであり、重要な変更にあたらない(リスク変動なし)
令和7年1月22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 1 特定個人情報ファイル (1)住民基本台帳ファイル 3 特定個人情報の使用 リスク2: 権限のない者によって不正に使用されるリスク 特定個人情報の使用の記録 具体的な管理方法	・操作ログ解析ツールにより、職員ごとの検索内容(検索日、被検索者等)を所属長等が確認できる仕組みとなっている。	削除	事前	重要な変更
令和7年1月22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 1 特定個人情報ファイル (1)住民基本台帳ファイル 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	・執務室内に監査カメラを設置し、所属長が所管の映像の確認を行っている。	・執務室の扉は施錠されており、カードキーがなければ入室できない。 休日・事前の届出がなければカードキーがあっても入室できない。 ・執務室の扉に至るまでの廊下等には監視カメラが設置されている。	事後	庁舎移転による運用変更であり重要な変更にあたらない。(リスク変動なし)

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1月22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 1 特定個人情報ファイル (1)住民基本台帳ファイル 3 特定個人情報の使用 リスク4:特定個人情報ファイルが不正に複製されるリスク リスクに対する措置の内容	所管課設置の既存住基システム端末には、端末内保存領域を定期的に自動削除する仕組みとなっており、特定個人情報ファイルが保存されない。 既存住基システムのバックアップデータ等は厳重に管理し、権限を持った者のみがアクセスできる仕組みになっている。	・システム操作を行う端末はスクリーンショットの取得やローカルフォルダへのデータ保存を禁止しており、業務用端末から行うことができる処理は特定個人情報の照会・更新であり、特定個人情報ファイルそのものを複製することはできない。 ・違反行為に対しては、区は、法の罰則規定を踏まえ適切な対応を行う。なお、職員の場合はあわせて、地方公務員法及び中野区職員の懲戒に関する規定に基づく措置を講じる。	事後	機器更改による運用変更であり重要な変更にあたらない。(リスク変動なし)
令和7年1月22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 1 特定個人情報ファイル (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 特定個人情報ファイルの閲覧者・更新者の制限 具体的な制限方法	・委託事業者に対し、個人情報保護にかかる誓約書及び従事者名簿を提出させている。また、セキュリティ研修の実施も義務付けている。	・契約書に個人情報保護に関する遵守すべき事項を明記し、従事者名簿の提出やセキュリティ研修の実施等を義務付けている。	事後	記載内容の整理であり、重要な変更にあたらない(リスク変動なし)
令和7年1月22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 1 特定個人情報ファイル (1)住民基本台帳ファイル 5 特定個人情報の提供・移転 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 ルール内容及びルール遵守の確認方法	個人情報保護審議会による審査	・番号法及び条例の規定により認められた範囲内においてのみ、情報の提供・移転を行う。 ・移転を開始する前に、情報を保有する部長に対し情報の利用の協議をすることを規則で定めている。	事後	法令改正によるものであり、重要な変更にあたらない(リスク変動なし)
令和7年1月22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 1 特定個人情報ファイル (1)住民基本台帳ファイル 5 特定個人情報の提供・移転 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	個人情報保護審議会が認められた以外の提供・移転を禁止する。	・法令に基づく情報の提供については、その法令で定める情報・項目について、法令・法令に基づく基準で定める方法に則り、提供する。 ・個人情報の目的外利用・外部提供に該当する場合には、責任者の決裁を伴う所定の手続きを経た上で行うこととすることで、あらかじめ情報提供の適法性を確保する。	事後	法令改正によるものであり、重要な変更にあたらない(リスク変動なし)
令和7年1月22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 1 特定個人情報ファイル (1)住民基本台帳ファイル 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 ⑤物理的対策 具体的な対策の内容	・インターネットと接続されているネットワークとの完全分離を行っている。 ・コンピュータウィルス対策ソフトウェアを導入及び更新している。＜中野区における措置＞ ・サーバ・ネットワーク機器等設置室へのIDと静脈認証による入退室管理。 ・監視カメラを設置し24時間監視体制をとっている。 ・所管課の事務室への入退室を入退室管理システムで管理するとともに、業務終了後施錠する。	＜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。	事前	重要な変更
令和7年1月22日	上記に同じ	—	＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。	事後	リスクを低減させる変更のため、重要な変更にあたらない

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1月22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 1 特定個人情報ファイル (1)住民基本台帳ファイル 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 ⑥技術的対策 具体的な対策の内容	・インターネットと接続されているネットワークとの完全分離を行っている。 ・コンピュータウイルス対策ソフトウェアを導入及び更新している。	＜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。	事前	重要な変更
令和7年1月22日	上記に同じ	—	＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバー・プラットフォームではUTM(コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置)等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ・中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ・導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。	事後	リスクを低減させる変更のため、重要な変更にあたらない
令和7年1月22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 1 特定個人情報ファイル (1)住民基本台帳ファイル 7 特定個人情報の保管・消去 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 手順の内容	・法令等の定めによる保存期間が経過したデータは一定期間経過後に消去する。 ・消去の際は、物理的な破壊、消去ソフトの使用等により、判読不能な状態にする。	左記に以下を追加する。 ＜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。	事前	重要な変更
令和7年1月22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 1 特定個人情報ファイル (2)本人確認情報ファイル 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	・執務室内に監査カメラを設置し、所属長が所管の映像の確認を行っている。 ・委託先に対しては当該事項について仕様書に定め、誓約書を提出させる。	・執務室の扉は施錠されており、カードキーがなければ入室できない。 休日・事前の届出がなければカードキーがあっても入室できない。 ・執務室の扉に至るまでの廊下等には監視カメラが設置されている。 ・委託先に対しては当該事項について仕様書に定め、事務外利用の禁止を徹底させている。	事後	庁舎移転による運用変更等であり重要な変更にあたらない。(リスク変動なし)
令和7年1月22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 1 特定個人情報ファイル (2)本人確認情報ファイル 4 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限 具体的な制限方法	・委託事業者に対し、個人情報保護にかかる誓約書及び従事者名簿を提出させている。また、セキュリティ研修の実施も義務付けている。	・契約書に個人情報保護に関する遵守すべき事項を明記し、従事者名簿の提出やセキュリティ研修の実施等を義務付けている。	事後	記載内容の整理であり、重要な変更にあたらない(リスク変動なし)
令和7年1月22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 1 特定個人情報ファイル (3)送付先情報ファイル 2 特定個人情報の入手 リスク1:目的外の入手が行われるリスク 必要な情報以外を入手することを防止するための措置の内容	・今後示される予定である総務省告示等により市町村CSIにおいて既存住基システムを通じて入手することとされている情報以外を入手できないことを、システム上で担保する。	・平成14年6月10日総務省告示第334号(第6-7 本人確認情報の通知及び記録)等により市町村CSIにおいて既存住基システムを通じて入手することとされている情報以外を入手できないことを、システム上で担保する。	事後	法令改正によるものであり、重要な変更にあたらない(リスク変動なし)

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1月22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 1 特定個人情報ファイル (3)送付先情報ファイル 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	・執務室内に監査カメラを設置し、所属長が所管の映像の確認を行っている。 ・委託先に対しては当該事項について仕様書に定め、誓約書を提出させる。	・執務室の扉は施錠されており、カードキーがなければ入室できない。 休日には、事前の届出がなければカードキーがあっても入室できない。 ・執務室の扉に至るまでの廊下等には監視カメラが設置されている。 ・委託先に対しては当該事項について仕様書に定め、事務外利用の禁止を徹底させている。	事後	庁舎移転による運用変更等であり重要な変更にあたらない。(リスク変動なし)
令和7年1月22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 1 特定個人情報ファイル (3)送付先情報ファイル 4 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限 具体的な制限方法	・委託事業者に対し、個人情報保護にかかる誓約書及び従事者名簿を提出させている。また、セキュリティ研修の実施も義務付けている。	・契約書に個人情報保護に関する遵守すべき事項を明記し、従事者名簿の提出やセキュリティ研修の実施等を義務付けている。	事後	記載内容の整理であり、重要な変更にあたらない(リスク変動なし)
令和7年1月22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 1 特定個人情報ファイル (4)コンビニ情報ファイル 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	・執務室内に監査カメラを設置し、所属長が所管の映像の確認を行っている。 ・委託先に対しては当該事項について仕様書に定め、誓約書を提出させる。	・執務室の扉は施錠されており、カードキーがなければ入室できない。 休日には、事前の届出がなければカードキーがあっても入室できない。 ・執務室の扉に至るまでの廊下等には監視カメラが設置されている。 ・委託先に対しては当該事項について仕様書に定め、事務外利用の禁止を徹底させている。	事後	庁舎移転による運用変更等であり重要な変更にあたらない。(リスク変動なし)
令和7年1月22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 1 特定個人情報ファイル (4)コンビニ情報ファイル 4 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限 具体的な制限方法	・委託事業者に対し、個人情報保護にかかる誓約書及び従事者名簿を提出させている。また、セキュリティ研修の実施も義務付けている。	・契約書に個人情報保護に関する遵守すべき事項を明記し、従事者名簿の提出やセキュリティ研修の実施等を義務付けている。	事後	記載内容の整理であり、重要な変更にあたらない(リスク変動なし)
令和7年1月22日	Ⅳ その他のリスク対策 1 監査 ② 監査 具体的な内容	中野区情報安全対策方針及び同基準に基づき、情報資産全体の情報安全保護についての外部監査を定期的に行う。	＜中野区における措置＞ ・中野区情報安全対策方針及び同基準に基づき、情報資産全体の情報安全保護についての外部監査を定期的に行う。監査結果を踏まえ、情報安全対策の改定の際に活用することとしている。 ＜中間サーバー・プラットフォームにおける措置＞ ・運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。	事後	リスクを低減させる変更のため、重要な変更にあたらない
令和7年1月22日	同上	—	＜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。	事前	重要な変更
令和7年1月22日	Ⅳ その他のリスク対策 3 その他のリスク対策	—	＜ガバメントクラウドにおける措置＞ ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。 ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。 具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。	事前	重要な変更
令和7年1月22日	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	東京都中野区中野四丁目8番1号	東京都中野区中野四丁目11番19号	事後	その他の項目の変更であり事前の提出・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1月22日	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 ②請求方法	中野区個人情報の保護に関する条例第28条に基づき、必要事項を記載した開示請求書を提出する。	個人情報の保護に関する法律第77条第1項の規定により、必要事項を記載した開示請求書を提出する。	事後	法令改正によるものであり、重要な変更にあたらな
令和7年1月22日	V 開示請求、問合せ 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	東京都中野区中野四丁目8番1号	東京都中野区中野四丁目11番19号	事後	その他の項目の変更であり、事前の提出・公表が義務付けられない
令和7年7月11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 (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3 ③委託先における取扱者数	10人以上50人未満	100人以上500人未満	事後	その他の項目の変更であり、事前の提出・公表が義務付けられない
令和7年7月11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 (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3 ⑥委託先名	パーソルテンプスタッフ株式会社	パーソルビジネスプロセスデザイン株式会社 株式会社ヒューマントラスト	事後	その他の項目の変更であり、事前の提出・公表が義務付けられない