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

港区は、住民基本台帳に関する事務において、特定個人情報の漏えいその他の事態が発生するリスクを軽減させるために適切な措置を講じることで、区民等のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項	住民基本台帳に関する事務では、事務の一部を外部業者に委託している。情報の不正使用対策として、業者選定の際に業者の情報保護管理体制を確認し、秘密保持に関し契約に含めることで万全を期している。

評価実施機関名

港区長

個人情報保護委員会　承認日 【行政機関等のみ】

公表日

令和8年10月26日

［令和6年10月　様式4］

項目一覧

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

Ⅰ　基本情報

1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	住民基本台帳に関する事務
②事務の内容　※	区市町村が住民を対象とする行政を適切に行い、また、住民の正しい権利を保障するためには、区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、区市町村における住民の届出に関する制度及びその住民たる地位を記録する各種の台帳に関する制度を一元化し、もって、住民の利便を増進するとともに行政の近代化に対処するため、住民に関する記録を正確かつ統一的に行うものであり、区市町村において、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。 区市町村は、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。 1　個人を単位とする住民票を世帯ごとに編成し、住民基本台帳を作成 2　転入届、転居届、転出届、世帯変更届等の届出又は職権に基づく住民票の記載、消除又は記載の修正 3　住民基本台帳の正確な記録を確保するための措置 4　転入届に基づき住民票の記載をした際の転出元市区町村に対する通知 5　本人又は同一の世帯に属する者の請求による住民票の写し等の交付 6　住民票の記載事項に変更があった際の都道府県知事に対する通知 7　地方公共団体情報システム機構（以下「機構」という。）への本人確認情報の照会 8　住民からの請求に基づく個人番号の変更 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 ※申請・届出等は、窓口、郵送及びサービス検索・電子申請機能で受領する。 なお、9「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命令（平成26年11月20日総務省令第85号）により、地方公共団体情報システム機構に事務の一部を委任する。そのため、当該事務においては、事務を委任する機構に対する情報の提供を含めて特定個人情報ファイルを使用する。
③対象人数	[　30万人以上　] ＜選択肢＞ 1) 1,000人未満　2) 1,000人以上1万人未満 3) 1万人以上10万人未満　4) 10万人以上30万人未満 5) 30万人以上

2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	住民記録システム
②システムの機能	1　異動入力機能 届出や通知に基づく異動時における、入力機能および入力された住民基本台帳を管理する機能 2　照会機能 住民基本台帳を検索、照会する機能 3　帳票発行機能 住民票の写し・記載事項証明書等の各種証明書の発行、付帯帳票の発行機能 4　一括処理機能 転入通知・法務省通知等に基づく異動を一括で住民基本台帳に記載する機能 5　庁内連携機能 庁内の各システムへの基礎データとして利用するため、宛名システムや他システムへの連携機能 6　印鑑登録機能 印鑑登録情報の管理機能や印鑑登録証明書の交付機能 7　住基ネットへの連携機能 住基ネットへの本人確認情報の連携機能、転入通知・戸籍附票通知・転出証明書情報等の区市町村間の通知機能 8　在留カード等発行システム連携機能 在留カード等発行システムと連携し、法務省通知情報の取込、市町村通知情報の作成を行う機能 9　文字同定機能 住基ネットと既存住基との文字同定や、在留カード等発行システムとのデータ連携時の文字コード変換機能

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　（証明書自動交付システム、法務省在留カード等発行システム、戸籍システム）
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
②システムの機能	1　本人確認情報の更新 住民記録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、当該情報を基に市町村統合端末の本人確認情報を更新し、都道府県サーバー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等を行う際、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基に住基ネットが保有する本人確認情報に照会を行い、確認結果を画面上に表示する。 3　個人番号カードを利用した転入（特例転入） 転入の届出を受け付けた際に、あわせて個人番号カードが提示された場合、当該個人番号カードを用いて転入処理を行う。 4　本人確認情報検索 統合端末において入力された4情報（氏名、住所、性別、生年月日）の組合せをキーに本人確認情報の検索を行い、検索条件に該当する本人確認情報の一覧を画面上に表示する。 5　機構への情報照会 全国サーバー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ー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ー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、都道府県サーバー及び全国サーバーに対し、整合性確認用本人確認情報を提供する。 7　送付先情報通知 個人番号の通知に係る事務の委任先である機構において、住民に対して番号通知書類（通知カード、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、住民記録システムから当該市町村の住民基本台帳に記載されている者の送付先情報を抽出し、当該情報を機構が設置・管理する個人番号カード管理システムに通知する。 8　個人番号カード管理システムとの情報連携 機構が設置・管理する個人番号カード管理システムに対し、個人番号カードの交付、廃止、回収又は一時停止解除に係る情報や個人番号カードの返還情報等を連携する。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[○] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [　] その他　（　）
システム3	
①システムの名称	システム共通基盤
②システムの機能	【団体内統合宛名管理システム（共通宛名）】 1　宛名管理機能 住民記録システムから取得した住記データを、統合宛名データベースに反映を行う。 2　団体内宛名番号の付番機能 個人番号が新規入力されたタイミングで、団体内統合宛名番号の付番を行う。 3　団体内宛名番号の変更機能 個人番号が同一で複数の団体内統合宛名番号が付番されていた場合の、団体内統合宛名番号の変更を行う。 4　符号管理機能 符号取得要求、符号取得依頼受信等を行う。 【住民情報・年金特徴情報照会システム】 1　住民情報照会機能：住民登録者の住民記録情報を照会する。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[○] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[○] 既存住民基本台帳システム [　] 宛名システム等　[○] 税務システム

	[　]その他　（　　）

システム4	
①システムの名称	中間サーバ連携システム
②システムの機能	情報提供機能 各業務で管理している別表2の提供業務情報を受領し、中間サーバーへの情報提供を行う。
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　（ 中間サーバー連携システム　　）
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、情報照会、情報提供に用いる個人の識別子である「符号」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介して、特定個人情報（連携対象）の情報照会及び情報提供受領（照会した情報の受領）を行う機能。 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及び当該特定個人情報（連携対象）の提供を行う機能。 4　既存システム接続機能 　中間サーバーと既存システム、番号連携サーバーとの間で情報照会内容、情報提供内容、特定個人情報（連携対象）、符号取得のための情報等について連携するための機能。 5　情報提供等記録管理機能 　特定個人情報（連携対象）の照会、または提供があった旨の情報提供等記録を生成し、管理する機能。 6　情報提供データベース管理機能 　特定個人情報（連携対象）を副本として、保持・管理する機能。 7　データ送受信機能 　中間サーバーと情報提供ネットワークシステム（インターフェイスシステム）との間で情報照会、情報提供、符号取得のための情報等について連携するための機能。 8　セキュリティ管理機能 　セキュリティを管理する機能。 9　職員認証・権限管理機能 　中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報（連携対象）へのアクセス制御を行う機能。 10　システム管理機能 　バッチの状況管理、業務統計情報の集計、稼動状況の通知、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　（ 中間サーバー連携システム　　）
システム6～10	
システム6	
①システムの名称	証明書自動交付システム
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：コンビニ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　　）

	［○］その他　（戸籍システム　　）

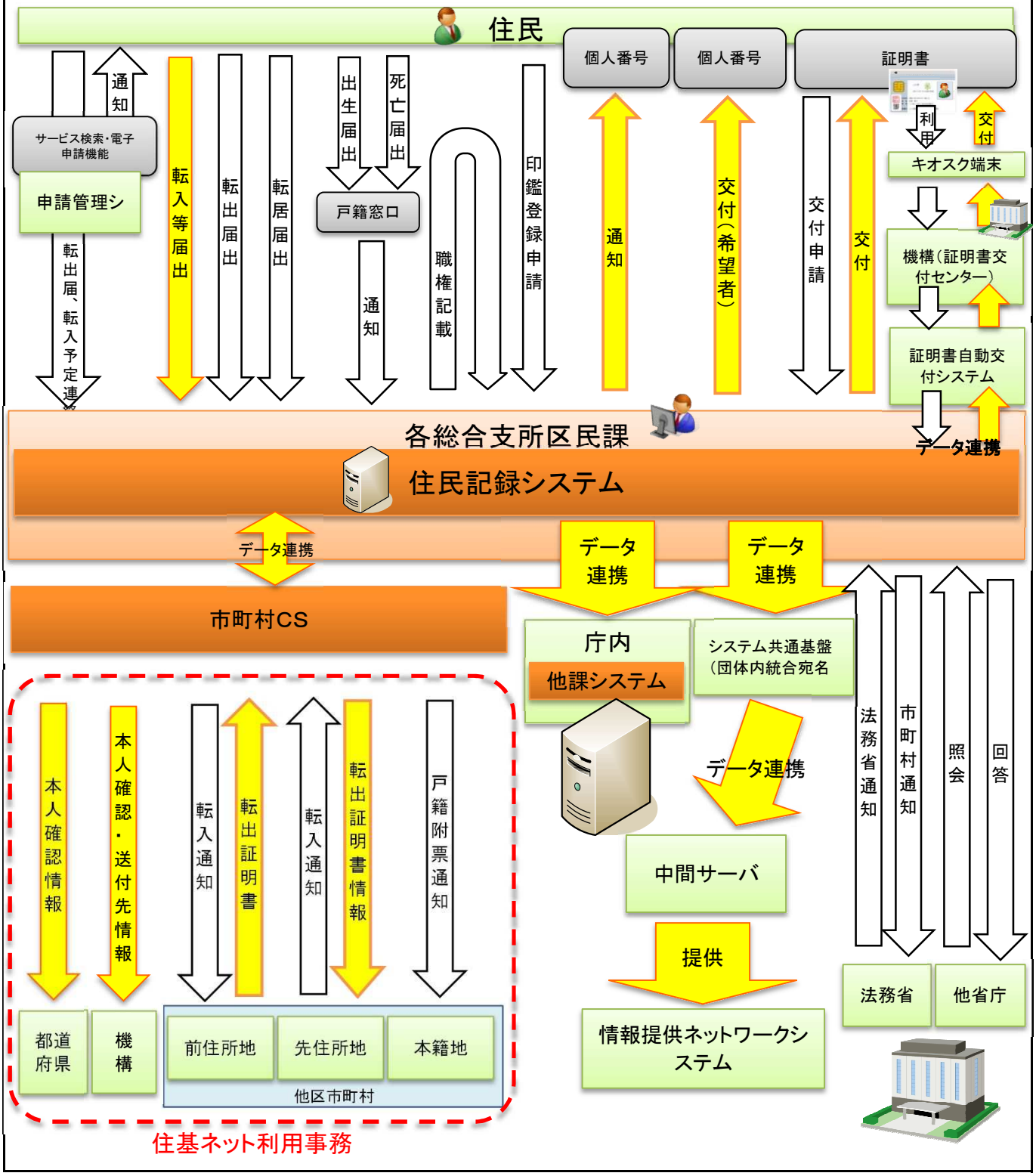
システム7	
①システムの名称	窓口総合支援システム
②システムの機能	1　区民利用側 　区民によるインターネットを利用した手続検索、電子申請サイトへのリンク、一括申請用データ作成機能 2　職員利用側 　窓口における区民申請用データの読取、申請データに係る住記データ参照及び突合、申請データ補正、署名、申請書一括作成、住記システムへのデータ連携機能
③他のシステムとの接続	[　] 情報提供ネットワークシステム　　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　　[○] 既存住民基本台帳システム [○] 宛名システム等　　[　] 税務システム [　] その他　（　）
システム8	
①システムの名称	サービス検索・電子申請機能
②システムの機能	1　住民向け機能 　自らが受けることができるサービスをオンラインで検索及び申請ができる機能 2　地方公共団体向け機能 　住民が電子申請を行った際の申請データ取得画面又は機能を、地方公共団体に公開する機能
③他のシステムとの接続	[　] 情報提供ネットワークシステム　　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　　[　] 既存住民基本台帳システム [　] 宛名システム等　　[　] 税務システム [○] その他　（ 申請管理システム（MINATO申請ネット）　）
システム9	
①システムの名称	申請管理システム（MINATO申請ネット）
②システムの機能	＜申請管理システム＞ 1．データの参照機能 連携サーバから連携された電子申請データを参照する機能。 2．格納機能 サービス検索・電子申請機能からの電子申請データを取込み共通DBへ格納する機能を有する。また、格納された申請データを対象の申請手続き業務システムに連携する。 3．通知機能 住民からオンライン申請があった手続の件数をメールで通知する（1回／日）。 4．ステータスの更新機能 5．宛名番号設定機能 申請データに含まれる申請者の利用者用証明書シリアル番号と宛名番号を紐づける処理を実施するが、紐づけできなかった場合に、宛名番号を設定する機能（MINATO申請ネット内のみ）。 ＜連携サーバ＞ サービス検索・電子申請機能で受け付けた電子申請データを申請管理システムに連携する（受け渡す）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	港区では以下の3ファイルを取り扱う。 （1）住民基本台帳ファイル 住民基本台帳法に規定する住民基本台帳への記載項目の整備を行い、住民に関する記録を正確かつ統一的に管理することを目的として、住民基本台帳ファイルにおいて個人番号を含む個人情報の管理を行う。 ①住民票に関する届出による異動や、戸籍関係の届出や通知による異動、又は職権により、住民基本台帳の作成・更新を行う。 ②住民からの交付請求に応じて、住民票の写しの交付を行う。 ③機構から住民票コードに対応する個人番号を取得し、住民基本台帳へ記録する。又、機構へ通知カードの送付先情報を通知する。 ④庁内の他業務システムへ住民異動情報や国民健康保険等の資格情報のデータ連携を行う。 ⑤他機関へ情報提供を行う住民票関係情報を中間サーバーへ登録する。 ⑥最新・過去時点の世帯構成の照会や、世帯構成と個人履歴の検索・照会を行う。 （2）本人確認情報ファイル ①住基ネットを用いて区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。 （3）送付先情報ファイル 区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により区から機構に委任し、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。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。
②実現が期待されるメリット	住民票の写し等に代えて本人確認情報を利用することにより、これまで窓口で提出が求められていた行政機関が発行する住民票の写し等の添付書類を省略し、区民の負担軽減につながることが見込まれる。また、個人番号カードによる本人確認、個人番号の真正性確認が可能となり、行政事務効率化の進展が期待される。
5. 個人番号の利用　※	
法令上の根拠	1. 行政手続における特定の個人を識別するための番号の利用等に関する法律（番号法）（平成25年5月31日法律第27号） ・第7条（指定及び通知） ・第16条（本人確認の措置） ・第17条（個人番号カードの交付等） 2. 住民基本台帳法（住基法）（昭和42年7月25日法律第81号） （平成25年5月31日法律第28号施行時点） ・第5条（住民基本台帳の備付け） ・第6条（住民基本台帳の作成） ・第7条（住民票の記載事項） ・第8条（住民票の記載等） ・第12条（本人等の請求に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）

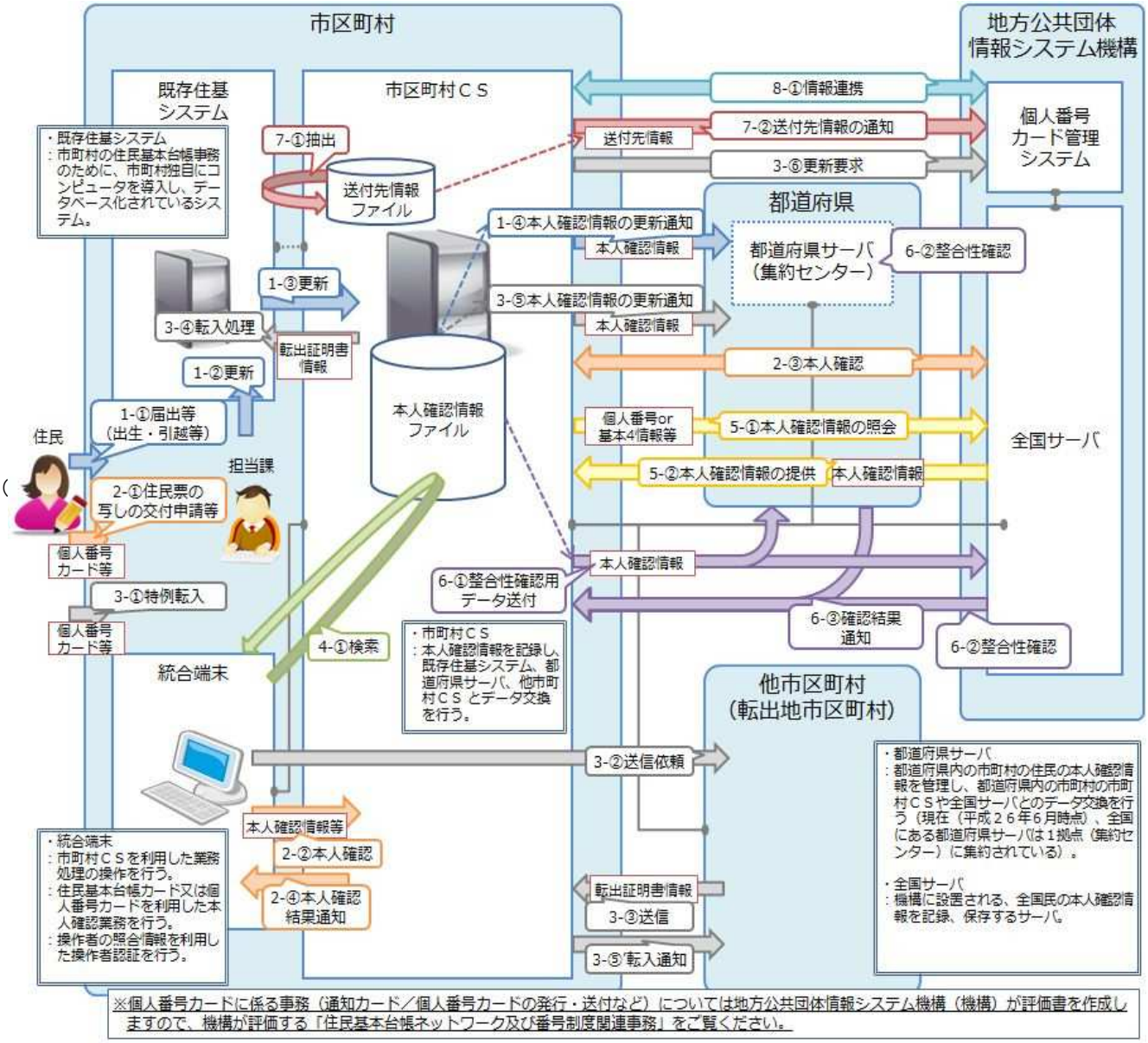
6. 情報提供ネットワークシステムによる情報連携 ※		
①実施の有無	[　　実施する　　]	<選択肢> 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	・番号法第19条8号（特定個人情報の提供の制限）及び同号に基づく主務省令第2条の表 （番号法第19条第8号に基づく主務省令第2条の表における情報提供の根拠） ：第三欄（情報提供者）が「市町村長」の項のうち、第四欄（利用特定個人情報）に「住民票関係情報」が含まれる項 （1、2、3、5、7、11、13、15、20、28、37、39、48、53、57、58、59、63、65、66、69、73、75、76、81、83、84、86、87、91、92、96、106、108、110、112、115、118、124、129、130、132、136、137、138、141、142、144、149、150、151、152、155、156、158、160、163、164、165、166の項） （番号法第19条第8号に基づく主務省令第2条の表における情報照会の根拠） ：なし （住民基本台帳に関する事務において情報提供ネットワークシステムによる情報照会は行わない）	
7. 評価実施機関における担当部署		
①部署	芝地区総合支所　区民課 ※事務を担当する各総合支所区民課（芝・麻布・赤坂・高輪・芝浦港南）のうち芝地区総合支所区民課が取りまとめを担う。	
②所属長の役職名	区民課長	
8. 他の評価実施機関		
―		

（別添1）事務の内容

（1）「住民基本台帳ファイル」を取り扱う事務の内容（住民記録システムを中心とした事務の流れ）



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



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

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

3．個人番号カードを利用した転入（特例転入）
3-①.市町村CSにおいて転出地市町村より転出証明書情報を受信する。
3-②.既存住基システムにおいて、市町村CSから転出証明書情報を受信する。
3-③.転入手続を行う住民から提示された個人番号カードを利用して本人確認(「2．本人確認」を参照)を行う。
※転出証明書情報に記載の転出の予定年月日から30日後までに転入手続が行われない場合には、当該転出証明書情報を消去する。
※3-③の転入手続時に転出証明書情報を受信していない場合又は消去している場合には、統合端末から、市町村CSを経由して転出地市町村に対し転出証明書情報の送信依頼を行い(※特定個人情報を含まない)、その後、3-①・②を行う。
3-④.既存住基システムにおいて、転入処理を行う。
3-⑤.市町村CSより、既存住基システムから転入処理完了後に受け渡される転入通知情報(※特定個人情報を含まない)を転出地市町村へ送信すると同時に、都道府県サーバへ本人確認情報の更新情報を送信する。
3-⑥.転入処理完了後、個人番号カードの継続利用処理を行い、個人番号カード管理システムに対し、個人番号カード管理情報の更新要求を行う。

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

5．機構への情報照会に係る事務
5-①.機構に対し、個人番号又は4情報等をキーワードとした本人確認情報の照会を行う。
5-②.機構より、当該個人の本人確認情報を受領する。
6．本人確認情報整合に係る事務
6-①.市町村CSより、都道府県サーバ及び全国サーバに対し、整合性確認用の本人確認情報を送付する。
6-②.都道府県サーバ及び住基全国サーバにおいて、市町村CSより受領した整合性確認用の本人確認情報を用いて保有する本人確認情報の整合性確認を行う。
6-③.都道府県サーバ及び全国サーバより、市町村CSに対して整合性確認結果を通知する。

7．送付先情報通知に関する事務
7-①.既存住基システムより、当該市町村における個人番号カードの交付対象者の送付先情報を抽出する。
7-②.個人番号カード管理システムに対し、送付先情報を通知する。

8．個人番号カード管理システムとの情報連携
8-①.個人番号カード管理システムに対し、個人番号カードの交付、廃止、回収又は一時停止解除に係る情報や個人番号カードの返還情報等を連携する。

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名		
（1）住民基本台帳ファイル		
2. 基本情報		
①ファイルの種類 ※		［　　システム用ファイル　　］　＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		［　10万人以上100万人未満　］　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※		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）　※平成27年10月5日以前に、転出・死亡等の事由により住民票が消除された者は含まない。
	その必要性	住民に関する市町村事務の処理の基礎として利用する ・住基法第7条において、住民基本台帳の記載項目と規定されるため ・番号法第19条別表第二の事務において、符号の取得に利用するため
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　（　印鑑登録情報　）
	その妥当性	住民基本台帳事務に関する事務を行うため、住民基本台帳法に規定される事項を保有
	全ての記録項目	別添2を参照。
⑤保有開始日		平成27年6月
⑥事務担当部署		芝地区総合支所区民課、麻布地区総合支所区民課、赤坂地区総合支所区民課、高輪地区総合支所区民課、芝浦港南地区総合支所区民課

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 （ 他区市町村 ） [ ] 民間事業者 （ ） [○] その他 （ 地方公共団体情報システム機構 ）
②入手方法		[○] 紙 [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 電子メール [ ] 専用線 [○] 庁内連携システム [ ] 情報提供ネットワークシステム [○] その他 （ サービス検索・電子申請機能、申請管理システム ）
③入手の時期・頻度		住民基本台帳に係る届出または通知の都度入手。
④入手に係る妥当性		住基法及び住基法施行令に規定される届出及び記載等による。
⑤本人への明示		番号法第7条（個人番号の指定及び通知）に規定される個人番号は、住基法第7条(住民票の記載事項)において「八の二」として規定される。
⑥使用目的 ※		住民基本台帳の整備、証明書等への記載、住民サービスの基礎情報とするため
	変更の妥当性	-
⑦使用の主体	使用部署 ※	芝地区総合支所　区民課 麻布地区総合支所　区民課 赤坂地区総合支所　区民課 高輪地区総合支所　区民課 芝浦港南地区総合支所　区民課（台場分室含む）
	使用者数	[100人以上500人未満] ＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
⑧使用方法 ※		・届出や職権等に基づき、住民票の記載及び記載事項の修正を行う。 ・本人等の請求に基づき、住民票の写し等の交付を行う。 ・住所地市町村以外の市町村長への住民票の写し請求に基づき、住民票の写しに関する情報を請求先の市町村長に通知する。 ・住民票の記載及び記載事項の修正を行った場合、本人確認情報を都道府県知事へ通知する。 ・転入届の特例による転入地市町村長からの通知に基づき、転出証明書情報の通知を行う。 ・住民に関する事務処理において使用する宛名情報を提供する。 ・番号法別表第二に基づき、情報提供ネットワークシステムへ住民票関係情報を提供する。 ・窓口総合支援システムへ住民票関係情報を提供する。 ・「サービス検索・電子申請機能」を通じて申請された電子申請データの受理、審査等。
	情報の突合 ※	・窓口業務において本人確認書類に通知カード、個人番号カードが使われた際に個人番号で単件検索を行う。 ・申請者を確認するために既存住基システムを通じて取り込んだ番号紐付情報と突合する（サービス検索・電子申請機能）。
	情報の統計分析 ※	区政の基礎資料や都への報告資料とするための人口統計、事務処理実績確認のための帳票発行枚数統計等のみに利用する。
	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29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 （ 8 ） 件
委託事項1		住民記録システムの保守、運用
①委託内容		住民記録システム等のパッケージアプリケーション保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業、職員からの問合せに対する調査、作業指示に基づくデータ抽出等
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] ＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[10万人以上100万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	「2. ③対象となる本人の範囲」と同。
	その妥当性	住民記録システム等で管理される全対象が範囲となる。
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 （ ）
⑤委託先名の確認方法		委託先については、入札結果として港区ホームページ上で公開している。
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	やむを得ず再委託する必要があるときは、区と委託先で再委託の内容について協議のうえ、再受託者に当該委託契約書に記載された個人情報保護に関する特記事項を遵守させるとともに、再受託事業者名、従事者名簿、内容を区に事前に通知し、その承認を得ることを契約の条件としている。
	⑨再委託事項	住民記録システム等のパッケージアプリケーション保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業。職員からの問合せに対する調査、作業指示に基づくデータ抽出等

委託事項2～5		
委託事項2		システム共通基盤の保守委託
①委託内容		システム共通基盤の保守作業
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。
	その妥当性	システム共通基盤の保守作業を委託するため、システムで管理される全対象が範囲となる。
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　（　）
⑤委託先名の確認方法		委託先については、入札結果として港区ホームページ上で公開している。
⑥委託先名		株式会社日立システムズ
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	やむを得ず再委託する必要があるときは、区と委託先で再委託の内容について協議のうえ、再受託者に当該委託契約書に記載された個人情報保護に関する特記事項を遵守させるとともに、再受託事業者名、従事者名簿、内容を区に事前に通知し、その承認を得ることを契約の条件としている。
	⑨再委託事項	システム共通基盤の保守作業の一部を再委託する。

委託事項3		システム運用にかかるオペレーション業務委託
①委託内容		ジョブスケジューリングやバッチ処理監視、帳票印刷等のシステム運用作業等
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。
	その妥当性	システム運用にかかるオペレーション業務を委託するため、システム運用に係る全範囲が対象となる。
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　（　　）
⑤委託先名の確認方法		委託先については、入札結果として港区ホームページ上で公開している。
⑥委託先名		株式会社日立システムズ
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	やむを得ず再委託する必要があるときは、区と委託先で再委託の内容について協議のうえ、再受託者に当該委託契約書に記載された個人情報保護に関する特記事項を遵守させるとともに、再受託事業者名、従事者名簿、内容を区に事前に通知し、その承認を得ることを契約の条件としている。
	⑨再委託事項	ジョブスケジューリングや帳票印刷、アクセスログ開示請求運用等のシステム運用作業等

委託事項4		住民記録窓口事務における証明書発行業務の委託
①委託内容		住民記録窓口事務における証明書発行
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの一部]　＜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。
	その妥当性	窓口における証明書の発行にあたり、特定個人情報を取り扱う必要があるため。
③委託先における取扱者数		[50人以上100人未満]　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○] 専用線　[ ] 電子メール　[ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ　[ ] 紙 [ ] その他　（　）
⑤委託先名の確認方法		委託先については、入札結果として港区ホームページ上で公開している。
⑥委託先名		パーソルテンプスタッフ株式会社
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5		中間サーバー連携システムの保守・運用
①委託内容		中間サーバー連携システムの保守作業、ジョブスケジューリング等のシステム運用作業等
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。
	その妥当性	中間サーバー連携システムの保守作業を委託するため、システム運用に係る全範囲が対象となる。
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　（　）
⑤委託先名の確認方法		委託先については、入札結果として港区ホームページ上で公開している。
⑥委託先名		株式会社日立システムズ
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	やむを得ず再委託する必要があるときは、区と委託先で再委託の内容について協議のうえ、再受託者に当該委託契約書に記載された個人情報保護に関する特記事項を遵守させるとともに、再受託事業者名、従事者名簿、内容を区に事前に通知し、その承認を得ることを契約の条件としている。
	⑨再委託事項	中間サーバー連携システムの保守作業、ジョブスケジューリング等のシステム運用作業等

委託事項6～10		
委託事項6		住基ネット統合端末の保守
①委託内容		住基ネット統合端末の業務アプリケーション等の適用作業、職員からの問合せに対する調査等
②取扱いを委託する特定個人情報ファイルの範囲		［ 特定個人情報ファイルの全体 ］　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	［　10万人以上100万人未満　］　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲　※	「2．③対象となる本人の範囲」と同。
	その妥当性	システム運用に係る全範囲が対象となる。
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		委託先については、入札結果として港区ホームページ上で公開している。
⑥委託先名		株式会社オーイーシー
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7		通知カード及び個人番号カード交付等に係る人材派遣委託
①委託内容		各地区総合支所区民課窓口サービス係における通知カード及び個人番号カード交付等に関する業務
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの一部] ＜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。
	その妥当性	窓口における個人番号カード関係の事務を委託することにより、迅速かつ正確な処理を可能とする。
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　（　）
⑤委託先名の確認方法		委託先については、入札結果として港区ホームページ上で公開している。
⑥委託先名		キャリアリンク株式会社
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8		窓口総合支援システム構築及び保守・運用
①委託内容		窓口総合支援システム（区民利用側及び職員利用側）のシステム構築及び保守・運用
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一部]　＜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。
	その妥当性	窓口総合システム設計・構築・保守及び運用等に係る全範囲が対象となる。
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		委託先については、入札結果として港区ホームページ上で公開している。
⑥委託先名		日本電気株式会社
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	区と委託先で再委託の内容について協議のうえ、再受託者に当該委託契約書に記載された個人情報保護に関する特記事項を遵守させるとともに、再受託事業者名、従事者名簿、内容を区に事前に通知し、その承認を得ることを契約の条件としている。
	⑨再委託事項	区民利用側及び職員利用側のシステム構築に係る要件定義・基本設計・開発作業の一部
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 （ 60 ）件 [○] 移転を行っている （ 11 ）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1参照）
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関係情報
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	住民基本台帳に登録されている者のうち、個人番号を有する者
⑥提供方法	[○] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑦時期・頻度	
提供先2～5	
提供先2	教育委員会事務局
①法令上の根拠	番号法第19条第11号、港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第5条　別表第3項、第4項
②提供先における用途	児童及び生徒の就学等に関する事務
③提供する情報	住民票関係情報であって主務省令で定めるもの
④提供する情報の対象となる本人の数	[10万人以上100万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	住民基本台帳に登録されている者のうち、個人番号を有する者
⑥提供方法	[ ] 情報提供ネットワークシステム [○] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑦時期・頻度	随時
提供先6～10	
提供先11～15	
提供先16～20	

移転先1	芝地区総合支所、麻布地区総合支所、赤坂地区総合支所、高輪地区総合支所、芝浦港南地区総合支所 産業・地域振興支援部、保健福祉支援部、みなと保健所、子ども家庭支援部、街づくり支援部、防災危機管理室
①法令上の根拠	番号法第9条及び別表第一に規定する事務の効率化に利用
②移転先における用途	区の運用する各業務システムにて、基本情報として利用する。
③移転する情報	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関係情報
④移転する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲	住民基本台帳に登録されている者のうち、個人番号を有する者
⑥移転方法	[○] 庁内連携システム　　[　] 専用線 [　] 電子メール　　[　] 電子記録媒体（フラッシュメモリを除く。） [　] フラッシュメモリ　　[　] 紙 [　] その他　（　　）
⑦時期・頻度	随時
移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	

6. 特定個人情報の保管・消去

①保管場所 ※		＜区における措置＞ 特定個人情報はデータセンターに設置した専用サーバーに保管し、次の対策を実施している。 ・外部侵入防止として、外周赤外線センサー監視、24時間有人監視、監視カメラ設置。 ・入退館（室）管理として、管理用 ICカードと手の甲静脈認証による要員（事務従事者）特定や、共連れ（権限のある者が開錠した扉から権限のない者が入室すること）防止及び要員の位置情報把握などの機能を有する要員所在管理システムにより、複数の対策を講じている。 ・不正持込・持出防止のため、金属探知機及びセンター職員による所持品検査、生体認証とセンター職員によるラック開閉管理、防犯用セキュリティタグによる媒体管理を行っている。 ＜中間サーバー・プラットフォームにおける措置＞ 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。・サーバー室と、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。 ・出入口には機械による入退室を管理する設備を設置している。 ・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。 ・サーバー室内に設置したサーバーは、全て鍵付のサーバーラックに設置している。 ・監視設備として監視カメラ等を設置している。 ＜ガバメントクラウドにおける措置＞ ・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。 ・特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。
②保管期間	期間	[　　20年以上　　] ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	住民票が消除されない限り、情報は保存される。ただし、住民票が消除された場合は、住民基本台帳施行令第34条に定めるとおり、消除された日から150年間となる。
③消去方法		・保存期間を過ぎた申請書・帳票等紙媒体の特定個人情報については，外部業者による溶解処理を行い廃棄する。 ・特定個人情報等の重要な情報資産については物理的破壊またはデータ消去ソフトの使用により、情報資産を復元できないように消去を行うことをルール化している。 ＜中間サーバーにおける措置＞ ・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、中間サーバーの保守・運用事業者が特定個人情報を消去することはない。 ・ディスク交換やハード更改等の際は、中間サーバーの保守・運用事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。 ＜サービス検索・電子申請機能＞ サービス検索・電子申請機能から送信された電子申請データは、LGWAN環境サーバに一時的に格納され、サインアウト時に消去される。 ＜申請管理システム＞ 連携サーバに一時的に保管した個人番号付電子申請データは、申請管理システムへ連携後、速やかに完全消去する。 ＜ガバメントクラウドにおける措置＞ ・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。 ・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。 ・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・死亡等の事由により住民票が消除された者は含まない。
	その必要性	住民基本台帳ネットワーク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	住民基本台帳ネットワーク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		芝地区総合支所区民課、麻布地区総合支所区民課、赤坂地区総合支所区民課、高輪地区総合支所区民課、芝浦港南地区総合支所区民課

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 （ 住民記録システム ）
③入手の時期・頻度		住民基本台帳に係る届出または通知の都度入手。
④入手に係る妥当性		住基法及び住基法施行令に規定される届出及び記載等による。
⑤本人への明示		番号法第7条（個人番号の指定及び通知）に規定される個人番号は、住基法第7条(住民票の記載事項)において「八の二」として規定される。
⑥使用目的 ※		住民基本台帳ネットワーク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 ※	芝地区総合支所　区民課 麻布地区総合支所　区民課 赤坂地区総合支所　区民課 高輪地区総合支所　区民課 芝浦港南地区総合支所　区民課（台場分室含む）
	使用者数	[100人以上500人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
⑧使用方法 ※		・住民票の記載事項の変更又は新規作成が生じた場合、住民記録システムから当該本人確認情報の更新情報を受領し(住民記録システム→市区町村統合端末)、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（市区町村統合端末→都道府県サーバー）。 ・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→市区町村統合端末）。 ・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（都道府県サーバー）及び機構保存本人確認情報ファイル（全国サーバー）と整合することを確認するため、都道府県サーバー及び全国サーバーに対し、整合性確認用本人確認情報を提供する（市区町村統合端末→都道府県サーバー／全国サーバー）。
	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 ※	区政の基礎資料や都への報告資料とするための人口統計、事務処理実績確認のための帳票発行枚数統計等のみに利用する。
	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29日

⑨使用開始日	平成27年6月29日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] <選択肢> 1）委託する 2）委託しない （ 1 ） 件
委託事項1		住民基本台帳ネットワーク統合端末の保守・運用
①委託内容		住民基本台帳ネットワーク統合端末のアプリケーション保守作業、ジョブスケジューリング等のシステム運用作業、職員からの問い合わせに対する調査等
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。
	その妥当性	住民基本台帳ネットワーク統合端末で管理され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		委託先については、入札結果として港区ホームページ上で公開している。
⑥委託先名		株式会社オーイーシー
再委託	⑦再委託の有無 ※	[再委託しない] <選択肢> 1）再委託する 2）再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	
委託事項2～5		
委託事項6～10		
委託事項11～15		
委託事項16～20		

５．特定個人情報の提供・移転（委託に伴うものを除く。）	
提供・移転の有無	[○] 提供を行っている （ 2 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	都道府県
①法令上の根拠	住基法第30条の6（市町村長から都道府県知事への本人確認情報の通知等）
②提供先における用途	区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。 都道府県の執行機関に対し本人確認情報を提供する。
③提供する情報	住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日
④提供する情報の対象となる本人の数	[10万人以上100万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	住民基本台帳に登録されている者のうち、個人番号を有する者
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [○] その他 （ 住民基本台帳ネットワークシステム ）
⑦時期・頻度	住民基本台帳の記載事項において、本人確認情報に係る変更又は新規作成が発生した都度、随時

提供先2～5	
提供先2	都道府県及び地方公共団体情報システム機構
①法令上の根拠	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）
②提供先における用途	住民基本台帳の正確な記録を確保するために、本人確認情報ファイルの記載内容（当該提供情報）と都道府県知事保存本人確認情報ファイル及び機構保存本人確認情報ファイルの記載内容が整合することを確認する。
③提供する情報	住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日
④提供する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	住民基本台帳に登録されている者のうち、個人番号を有する者
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	随時
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	[　]庁内連携システム　[　]専用線 [　]電子メール　[　]電子記録媒体（フラッシュメモリを除く。） [　]フラッシュメモリ　[　]紙 [　]その他　（　）
⑦時期・頻度	
移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	

6. 特定個人情報の保管・消去		
①保管場所 ※		生体認証による入退室管理室内のサーバーに記録。 （管理室へのアクセスは個人ID及び手のひら静脈による認証が必要）
②保管期間	期間	[20年以上] ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	・住民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） ※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は含まない。
	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。 区市町村は、法令に基づき、これらの事務の実施を機構に委任する。
④記録される項目		［　50項目以上100項目未満　］　＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目　※	・識別情報 ［ ○ ］個人番号　［　］個人番号対応符号　［　］その他識別情報（内部番号） ・連絡先等情報 ［ ○ ］4情報（氏名、性別、生年月日、住所）　［ ○ ］連絡先（電話番号等） ［ ○ ］その他住民票関係情報 ・業務関係情報 ［　］国税関係情報　［　］地方税関係情報　［　］健康・医療関係情報 ［　］医療保険関係情報　［　］児童福祉・子育て関係情報　［　］障害者福祉関係情報 ［　］生活保護・社会福祉関係情報　［　］介護・高齢者福祉関係情報 ［　］雇用・労働関係情報　［　］年金関係情報　［　］学校・教育関係情報 ［　］災害関係情報 ［ ○ ］その他　（　通知カード及び交付申請書の送付先の情報　）
	その妥当性	・個人番号、4情報、その他住民票関係情報 　個人番号カードの券面記載事項として、法令に規定された項目を記録する必要がある。 ・その他（通知カード及び交付申請書の送付先の情報） 　機構に対し、法令に基づき通知カード及び個人番号カード交付申請書の印刷、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。
	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		芝地区総合支所区民課、麻布地区総合支所区民課、赤坂地区総合支所区民課、高輪地区総合支所区民課、芝浦港南地区総合支所区民課

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　（ 住民記録システム　　）
③入手の時期・頻度		住民基本台帳に係る届出または通知の都度入手。
④入手に係る妥当性		住基法及び住基法施行令に規定される届出及び記載等による。
⑤本人への明示		番号法第7条（個人番号の指定及び通知）に規定される個人番号は、住基法第7条(住民票の記載事項)において「八の二」として規定される。
⑥使用目的 ※		法令に基づく委任を受けて通知カード及び交付申請書の印刷、送付並びに個人番号カードの発行を行う機構に対し、通知カード及び交付申請書の送付先情報を提供するため。
	変更の妥当性	-
⑦使用の主体	使用部署 ※	芝地区総合支所　区民課 麻布地区総合支所　区民課 赤坂地区総合支所　区民課 高輪地区総合支所　区民課 芝浦港南地区総合支所　区民課（台場分室含む）
	使用者数	[　100人以上500人未満　]　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
⑧使用方法 ※		・住民記録システムより個人番号の通知対象者の情報を抽出し、通知カード及び交付申請書等の印刷及び送付に係る事務を法令に基づいて委任する機構に対し提供する（市区町村統合端末→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（全国サーバー）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 ※	区政の基礎資料や都への報告資料とするための人口統計、事務処理実績確認のための帳票発行枚数統計等のみに利用する。
	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29日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] ＜選択肢＞ 1）委託する 2）委託しない （ 1 ） 件
委託事項1		住民基本台帳ネットワーク統合端末の保守・運用
①委託内容		住民基本台帳ネットワーク統合端末のアプリケーション保守作業、ジョブスケジューリング等のシステム運用作業、職員からの問い合わせに対する調査等
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。
	その妥当性	住民基本台帳ネットワーク統合端末で管理され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		委託先については、入札結果として港区ホームページ上で公開している。
⑥委託先名		株式会社オーイーシー
再委託	⑦再委託の有無 ※	[再委託しない] ＜選択肢＞ 1）再委託する 2）再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	
委託事項2～5		
委託事項6～10		
委託事項11～15		
委託事項16～20		

5. 特定個人情報の提供・移転（委託に伴うものを除く。）	
提供・移転の有無	[○] 提供を行っている （ 1 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	地方公共団体情報システム機構
①法令上の根拠	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条第1項第1号から第8号までに関する事務による。
②提供先における用途	区市町村からの法令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。
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、通知カード及び交付申請書の送付先の情報
④提供する情報の対象となる本人の数	[10万人以上100万人未満] ＜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	住民基本台帳に登録されている者のうち、個人番号を有する者
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [○] その他 （ 住民基本台帳ネットワークシステム ）
⑦時期・頻度	使用開始日から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）。
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	

移転先1		
①法令上の根拠		
②移転先における用途		
③移転する情報		
④移転する情報の対象となる本人の数	[ ]	＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲		
⑥移転方法	[ ] 庁内連携システム [ ] 電子メール [ ] フラッシュメモリ [ ] その他 （ ）	[ ] 専用線 [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] 紙
⑦時期・頻度		
移転先2～5		
移転先6～10		
移転先11～15		
移転先16～20		
6．特定個人情報の保管・消去		
①保管場所 ※		生体認証による入退室管理室内のサーバーに記録 （管理室へのアクセスは個人ID及び手のひら静脈による認証が必要）
②保管期間	期間	[1年未満] ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	送付先情報は機構への提供のみに用いられ、また、送付後の変更は行わないことから、セキュリティ上、速やかに削除することが望ましいため。
③消去方法		保存期間が到来した本人確認情報は、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。
7．備考		

（別添2）特定個人情報ファイル記録項目

（1）住民基本台帳ファイル
＜住民基本台帳情報＞
1. 宛名番号
2. 住民票コード
3. 個人番号
4. 世帯番号
5. 氏名情報
6. 生年月日
7. 性別
8. 続柄
9. 住民となった年月日
10. 住民となった届出年月日
11. 住民となった事由
12. 住民区分（日本人、外国人）
13. 世帯主情報
14. 現住所情報
15. 住所を定めた年月日
16. 住所を定めた届出年月日
17. 前住所情報
18. 転入元住所情報
19. 転出先住所情報
20. 本籍・筆頭者情報
21. 備考欄履歴情報
22. 事実上の世帯主情報
23. 消除情報
24. 外国人住民となった年月日（外国人住民のみ）
25. 国籍（外国人住民のみ）
26. 法30条45規定区分（外国人住民のみ）
27. 在留カード等の番号（外国人住民のみ）
28. 在留資格情報（外国人住民のみ）
29. 通称（外国人住民のみ）
30. 通称の記載と削除に関する事項（外国人住民のみ）
31. 個別記載情報
32. 転出予定者情報
33. 除票住民票情報
34. 証明書発行履歴情報
35. 異動履歴情報
36. 住基カード発行状況
37. 個人番号カード等情報
38. 在留カード等情報
39. 法務省通知履歴
40. 市町村通知履歴
41. 戸籍附票通知履歴
42. 処理停止情報
43. 印鑑登録情報
44. 印影情報
45. 印鑑登録異動履歴
46. 印鑑証明書発行履歴
＜住基ネットゲートウェイシステム＞
47. 住民記録システムの一部情報
＜システム共通基盤＞
48. 住民記録システムの一部情報
＜中間サーバー＞
49. 情報提供用個人識別符号

（別添2）特定個人情報ファイル記録項目

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

（別添2）特定個人情報ファイル記録項目

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

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・申請等の窓口において届出・申請内容や本人確認書類の確認を厳格に行い、対象者以外の情報入手の防止に努める。 ・サービス検索・電子申請機能については、マニュアルやWEB上で、個人番号の提出が必要な者の要件を明示、周知し、本人以外の情報の入手を防止する。
必要な情報以外を入手することを防止するための措置の内容	・届出・申請等の様式において記載する部分は、住民基本台帳業務に必要項目のみに限る。 ・届出・申請等内容を住民記録システムへ入力後、入力内容の確認を複数人で行う。 ・サービス検索・電子申請機能においては、画面での誘導を簡潔に行うことで、異なる手続きに係る申請や不要な情報を送信してしまうリスクを防止する。
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・申請の際には住基法第27条の規定に基づき、書面にて本人又は代理人による届出のみを受領することとし、受領の際には本人又は代理人の本人確認書類及び委任状の確認を徹底している。 ・住民記録システムを利用する必要がある職員を特定し、ICカードによる識別とパスワードによる認証を実施する。 ・サービス検索・電子申請機能からの電子申請の際には、署名用電子証明書による電子署名を付して送信することとなり、のちに署名検証も行われるため、本人からの情報のみが送信される。
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	・区の要領・手順書等に基づき窓口において、対面で本人確認証明書（個人番号カード等）の提示を受け、本人確認を行う。 ・サービス検索・電子申請機能からの電子申請の際には、署名用電子証明書による電子署名を付すこととなり、電子署名付与済の電子申請データを受領した自治体は署名検証を実施する。これにより本人確認を実施する。
個人番号の真正性確認の措置の内容	・個人番号カード（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）の提示を受けて本人確認を行う。 ・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み合わせ）の提示がない場合には、統合端末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	・住民基本台帳ファイルへの情報の入力、削除及び訂正を行う際は、必ず入力、削除及び訂正した内容を複数職員が確認し、届出／申請等の様式に確認結果を記載する。 ・当日に行った入力、削除及び訂正作業の内容を翌日にリストとして出力し、入力、削除及び訂正した内容と当該リストの内容が合致していることを再確認する。 ・訂正した内容等については、その記録を残し、法令等により定められた期間保管する。 ・サービス検索・電子申請機能においては、個人番号カード内の記憶領域に格納された個人番号を申請フォームに自動転記を行うことにより、不正確な個人番号の入力を抑止する措置を講じている。
その他の措置の内容	－
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	・届出・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、区の規程により定められる期間、施錠して保管する。 ・住民記録システムを利用するには、ICカードとパスワードによるログインが必要で、対象業務の職員以外に権限を与えていない。 ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。 ・LGWAN系ネットワークとマイナンバー利用事務系ネットワークの間にDMZ（両ネットワークの中間に置かれ、連携サーバ経由でのみ利用できるようにする機能）を設け、申請管理システムから外部への直接通信を遮断することにより、安全を確保している。また境界FWや連携サーバで外部接続先との通信を制限している。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	

3. 特定個人情報の使用

リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク	
宛名システム等における措置の内容	個人番号利用業務以外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	住民基本台帳業務と他業務間においては、事務に必要な情報について定められたインターフェースに基づいて連携しており、その他の情報が紐付けされることはないよう設定している。
その他の措置の内容	帳票印刷等のためにデータ化したものについては、行政情報システム専用のセキュリティ対策が施された指定の一時保管場所にのみ保管し、他への利用が出来ないようにアクセスや複写の制限をかけている。また、利用後はすみやかに削除している。
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： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク	
ユーザ認証の管理	[行っている] ＜選択肢＞ 1）行っている 2）行っていない
具体的な管理方法	・システムの利用が可能な職員を特定し、ICカードとパスワードによる認証を行っている。 ・認証後は各システムの利用機能ごとに利用認可を設定し、職員ひとりひとりにシステム上で利用可能な機能を設定して、不正利用が行えない権限設定を実施する。 ・不正なアクセスが行われないように、端末の操作記録であるアクセスログを各区民課職員が毎月1回確認して、記録を残している。
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	・発行管理：人事異動があった場合や権限変更があった場合は、所属長の承認を受けてシステムに反映させている。また、承認期間は最長1年とし、毎年任用期間や委託期間を明示する書面を添えて再申請が必要な運用としている。 ・失効管理：人事異動等により失効者が出た場合には、所属長の承認を受けてシステムに反映させるとともに、処理の遅れが出ないように人事システムからも職員情報を連携して随時更新を行っている。特に任期の定めがある臨時職員・非常勤職員や委託事業者の従事者については、発行申請時に提示された任用期間または、委託期間を超えて利用できないよう自動失効させており、期間の延長は再度発行申請によることとして、失効の手続き漏れを防いでいる。
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	・ICカードについて、利用者を年度ごとに名簿管理し、業務外には施錠できる書庫で保管している。 ・人事情報を入手し、それをもとに権限表を作成する。システム担当者が権限表により発効管理・失効管理を行っており、毎年の年度当初までに内容を確認している。

		・大規模な組織変更、人事異動があるときはイベント処理として、事前検証（リハーサル）を行っている。

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	記録項目：処理日時、職員情報、部署情報、端末情報、処理事由、宛名番号、4情報 ・端末から参照、更新した場合の操作記録であるアクセスログを記録している。記録は7年間保存しており、記録を検査・分析し、不正なアクセスがないことを確認している。 ・業務所管課設置の端末には、特定個人情報ファイルを保存できないようシステムで制限をかけている。 ・特定個人情報のバックアップデータ及び操作記録は厳重に管理し、権限を持った者のみがアクセスできるよう制限をかけている。
その他の措置の内容		データベース内では個人番号を保有するテーブル（表）と個人情報を保有するテーブル（表）は別になっており、個人番号を利用しない事務の担当職員は、個人番号を保有する場所にはアクセスできない仕組みとしている。
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：　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		・個人情報保護や取扱いについて職員のセキュリティ意識を高めるため、区のセキュリティポリシー、事故事例や対応方法の解説等を行う情報セキュリティ研修の受講とeラーニングの実施を全員に義務付けている。また、年度途中で新規に業務に携わる者についても、業務に携わる前に研修を実施する。 ・情報セキュリティ研修等を通して、特定個人情報の業務外利用の禁止や漏洩時の罰則、アクセスログが確実に記録されていること等についても、従業者に周知徹底している。 ・申請管理システムへアクセスできる端末を制限する。
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク4：　特定個人情報ファイルが不正に複製されるリスク		
リスクに対する措置の内容		・業務主管課設置の住記端末には特定個人情報ファイルが保存されない仕組みとなっている。 ・住民記録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。 ・個人番号等を保持するテーブル（表）と住民情報等を保持するテーブル（表）は別となっており、個人番号を使用しない事務では個人番号を保持するテーブルにアクセスしない仕組みとなっている。 ・申請管理システムから取得した個人番号付電子申請データ等のデータについて、改ざんや業務目的以外の複製を禁止するルールを定め、ルールに従って業務を行う。
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		
・区の情報セキュリティ研修については、派遣事業者及び指定管理事業者の責任者にも毎年参加を義務付けており、事業者の事務従事者全員に対しても職員と同じeラーニング受講と区の研修を受講した責任者による内部研修実施を義務付けている。 ・情報セキュリティ研修においては、標的型メールや委託事業者による情報漏えい等、最新セキュリティ事故の実例をあげるとともに、特定個人情報の業務外利用禁止や漏えい時の罰則（4年以下の懲役又は200万円以下の罰金など）、アクセスログが確実に記録されていること等、従業者に周知徹底している。 ・スクリーンセーバ等を利用して長時間にわたり本人確認情報を表示させない。 ・統合端末のディスプレイを、来庁者から見えない位置に置く。 ・統合端末での画面のハードコピーの取得ができない仕組みになっている。		

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	・業者選定時に選定基準を設定し、委託先の社会的信用と能力を確認する。 ・仕様書には、プライバシーマークを取得している会社に委託先を限定するなど、委託先の安全管理体制と安全管理措置の内容等、特定個人情報の取扱いが適正であることを条件にしている。	
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	・作業者を限定するために、委託業者の従事者名簿を提出させる。 ・閲覧／更新権限を持つもの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。 ・閲覧／更新の履歴（ログ）を取得し、不正な使用がないことを確認する。	
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	・作業端末へのログイン記録やシステム保守における作業記録をアクセスログとともに、港区情報安全対策実施手順の規定により7年間保存している。 ・委託業務の実施状況について月１回定期的に報告を受け、記録を残す。	
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	・番号法で定められた事項、及び港区情報公開条例、港区個人情報保護条例、港区個人番号の利用並びに特定個人情報の保護及び提供に関する条例、港区情報安全対策指針、港区情報安全対策実施手順等に従いルールを遵守する。	
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	・委託先のデータセンター等への定期的な視察、監査を行う。 ・日常運用においては、港区情報安全対策手順に規定された申請や承認ルールを遵守して事務が執行されていることを定期的にチェックする。 ・再委託先以外の他者に提供してはならないよう契約している。	
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	・業務委託が終了した場合、委託元の指示に従い、委託元の責任と負担において個人情報を委託元に返還、破棄若しくは消去しなければならない旨を規定している。また、書面にて、破棄、消去の方法、完了日等を報告させ、必要に応じて職員が実地調査を行う。	
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	・データの秘密保持に関する事項 ・再委託の禁止又は制限に関する事項 ・情報資産の指示された目的外への使用及び第三者への提示の禁止に関する事項 ・データの複写及び複製の禁止に関する事項 ・事故発生時における報告義務に関する事項 ・情報資産の保護状況の検査の実施に関する事項 ・データの授受及び搬送に関する事項 ・委託を受けた事業者等におけるデータの保管及び廃棄に関する事項 ・その他データの保護に関し必要な事項 ・前記各事項の定めに違反した場合における契約解除等の措置及び損害賠償に関する事項	
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、事前の再委託協議を義務付けている。 ・委託先と同等のリスク対策を実施するよう、再委託の協議書と契約特記事項において、受注者が負うべき義務を再委託先も同様に負うことを明記している。	
その他の措置の内容	新たに個人情報を取り扱う事務を委託する場合は、「委託・指定管理チェックリスト」を所管課が作成し、総務課に提出しています。	

リスクへの対策は十分か	[　　特に力を入れている　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
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		
・区の情報セキュリティ研修については、委託事業者の責任者にも毎年参加を義務付けており、事業者の事務従事者全員に対しても職員と同じeラーニング受講と区の研修を受講した責任者による内部研修実施を義務付けている。 ・情報セキュリティ研修においては、標的型メールや委託事業者による情報漏えい等、最新セキュリティ事故の実例をあげるとともに、特定個人情報の業務外利用禁止や漏えい時の罰則（4年以下の懲役又は200万円以下の罰金など）、アクセスログが確実に記録されていること等、従業者に周知徹底している。		
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、連携時のログ、アクセスログ、収受両システムの連携データ内に記載された連携日時記録であるタイムスタンプにより確認できる。これらの記録は、港区情報安全対策実施手順の規定により7年間保存している。	
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	港区個人番号の利用並びに特定個人情報の保護及び提供に関する条例に基づき、特定個人情報を取り扱う事務の登録簿を整備して公開し、適正な利用を定期的に登録簿から確認できるようにする。	
その他の措置の内容	・情報の移転については、移転の記録が残る庁内連携システムを通して行うことで、不適切な移転を防止する。 ・他市区町村への情報提供については、情報提供ネットワーク接続用の端末でしか操作できず、また権限を持った職員しか操作できない仕組みとしている。	
リスクへの対策は十分か	[　　特に力を入れている　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク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	・庁内連携では、本業務で保有する情報をすべて連携することは行わず、番号法及び番号条例にて規定された部署のみ照会可能となっている。 ・情報の移転については、移転の記録が残る庁内連携システムを通して行うことで、不適切な移転を防止する。 ・他市区町村への情報提供については、情報提供ネットワーク接続用の端末でしか操作できず、また権限を持った職員しか操作できない仕組みとしている。	
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：　誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容	・庁内連携では、番号法及び番号条例にて規定された部署のみ照会可能となっている。 ・庁内連携では、本業務で保有する情報をすべて連携することは行わず、限定された情報のみ照会対象としている。 ・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		
・情報セキュリティ研修に重ねて、番号制度施行前研修において、特定個人情報の法定利用及び条例独自利用にかかる規定、業務外利用や情報漏えい時の罰則（4年以下の懲役又は200万円以下の罰金など）等、従業者に周知徹底する。		

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	情報提供機能（※）により、情報提供ネットワークシステムにおける照会許可用照合リストを情報提供ネットワークシステムから入手し、中間サーバーにも格納して、情報提供機能により、照会許可用照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 （※）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	情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。
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	特に慎重な対応が求められる情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、きわめて慎重に取り扱うべき特定個人情報が不正に提供されるリスクに対応している。 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。
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＞ 3　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。 4　中間サーバーと団体については専用線を設け、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。 5　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。 6　特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。

7. 特定個人情報の保管・消去

リスク1：　特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[　　政府機関ではない　　]	＜選択肢＞ 1）特に力を入れて遵守している　2）十分に遵守している 3）十分に遵守していない　4）政府機関ではない
②安全管理体制	[　特に力を入れて整備している　]	＜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	[　特に力を入れて整備している　]	＜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	[　特に力を入れて周知している　]	＜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	[　特に力を入れて行っている　]	＜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	＜区における措置＞ ・特定個人情報はデータセンターに設置した専用サーバーに保管し、次の対策を実施している。 −外部侵入防止として、外周赤外線センサー監視、24時間有人監視、監視カメラ設置。 −入退館（室）管理として、管理用 ICカードと手の甲静脈認証による要員（事務従事者）特定や、共連れ（権限のある者が開錠した扉から権限のない者が入室すること）防止及び要員の位置情報把握などの機能を有する要員所在管理システムにより、複数の対策を講じている。 ・不正持込・持出防止のため、金属探知機及びセンター職員による所持品検査、生体認証とセンター職員によるラック開閉管理、防犯用セキュリティタグによる媒体管理を行っている。 ・LGWAN接続端末については、業務時間内のセキュリティワイヤーによる固定、業務時間外の施錠できるキャビネットへの保管等の安全管理措置を講じている。 ＜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。・サーバー室と、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。 ・出入口には機械による入退室を管理する設備を設置している。 ・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。 ・サーバー室内に設置したサーバーは、全て鍵付のサーバーラックに設置している。 ・監視設備として監視カメラ等を設置している。 ＜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、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。 ・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		[　特に力を入れて行っている　] <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	＜区における措置＞ ・ネットワークは不正アクセス防止のため、業務系専用ネットワークで結ぶと共にファイアウォールを設置している。 ・サーバーにウイルス対策ソフトを導入し、パターンファイルを随時更新すると共に、サーバー及び端末のウイルススキャンを日次で行っている。 ・導入しているオペレーティングシステム及びミドルウェアについては、必要に応じてセキュリティパッチの適用を行っている。 ・業務系端末には個人情報等を保管できないよう、システムで制限をかけている。 ・区では情報処理システム導入当初より業務用端末の外部接続を禁止しており、業務用端末はインターネットに接続していない。 ＜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。 ・導入しているオペレーティングシステム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。 ＜LGWAN接続端末における措置＞ ・サービス検索・電子申請機能から電子申請データを受領するLGWAN接続端末について、ウイルス検出ソフトウェア等の導入により、ウイルス定義ファイルの定期的な更新及びウイルスチェックを実施する。 ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。 ＜申請管理システムにおける措置＞ ・申請管理システム及び連携サーバ、申請管理システム接続端末へのウイルス検出ソフトウェア等の導入により、ウイルス定義ファイルの定期的な更新及びウイルスチェックを行い、マルウェア検出を行う。 ・LGWAN系ネットワークとマイナンバー利用事務系ネットワークの間にDMZを設け、申請管理システムから外部への直接通信を遮断することにより、安全を確保している。また、境界FWや連携サーバで外部接続先との通信を制限している。 ＜ガバメントクラウドにおける措置＞ ・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。 ・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ついて」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（「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ついて」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。 ・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。 ・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。 ・地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ・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。 ・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。 ・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		[　特に力を入れて行っている　] <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	住民基本台帳においては死者も除票住民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。
その他の措置の内容		-
リスクへの対策は十分か		[特に力を入れている] <選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク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		・個人番号を含む住民情報については、住民記録システムにより、随時異動情報を連携することで最新の情報であることを担保している。また、定期的に住民基本台帳ネットワークシステムと住民記録システムの整合性点検を行っており、それによる修正情報も随時連携されている。 ・電子申請データの一時保管中に再申請や申請情報の訂正が発生した場合には古い情報で審査等を行わないよう、履歴管理を行う。 ・申請管理システムでは、申請データの再申請や申請情報の訂正が発生した場合には古い情報で審査等を行わないよう履歴管理を行う。 ・連携サーバに一時的に保管した個人番号付電子申請データは、申請管理システムへ連携後、速やかに完全消去する。
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	・サーバ、端末（パソコン）、記録媒体、紙文書等の情報資産を廃棄する場合は、情報を復元できないように処置した上で廃棄する。 ・紙文書は、溶解またはシュレッダー処分を行う。 ・電磁的な記録媒体は、破砕処理、電磁気破壊、データ消去ソフトウエアによるデータ消去を行った上で廃棄する。 ・サーバ、パソコン等情報機器については、記録装置に対し、物理破壊、磁気破壊、データ消去ソフトウエアによるデータ消去を行う。 ・サービス検索・電子申請機能におけるLGWAN接続端末については、業務終了後の不要な電子申請データ等の消去を実施する。必要に応じて管理者が確認する。 ・申請管理システム及び連携サーバ内の不要な個人番号付電子申請データの消去について徹底し、必要に応じて管理者が確認する。 <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		データ消去を業者に委託した場合は、消去作業証明書を提出させる。
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
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		

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

1．特定個人情報ファイル名	
（2）本人確認情報ファイル	
2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1：　目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	本人確認情報の入手元は既存住民基本台帳ネットワークシステムに限定されるため、既存住民基本台帳ネットワークシステムへの情報の登録の際に、届出／申請等の窓口において届出／申請内容や本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報の入手の防止に努める。
必要な情報以外を入手することを防止するための措置の内容	・平成14年6月10日総務省告示第334号（第6－6　本人確認情報の通知及び記録）等により住民基本台帳ネットワークシステムを利用する端末（統合端末）において既存住民基本台帳ネットワークシステムを通じて入手することととされている情報以外を入手できないことを、システム上で担保する。 ・正当な利用目的以外の目的にデータベースが構成されることを防止するため、本人確認情報の検索を行う際の検索条件として、少なくとも性別を除く2情報以上（氏名と住所の組み合わせ、氏名と生年月日の組み合わせ）の指定を必須とする。
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民基本台帳ネットワーク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	区の要領・手順書等に基づき窓口において、対面で本人確認証明書（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（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）の提示を受けて本人確認を行う。 ・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み合わせ）の提示がない場合には、統合端末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	・「2．特定個人情報の入手」におけるリスク1、リスク2、リスク3に記載した各措置の通り、入手の各段階で、本人確認とともに、特定個人情報の正確性を確保している。 ・特定個人情報の入力、修正、削除を行う際は、異動対象者又は入力内容に誤りのないよう、入力した職員以外による照合を実施する。
その他の措置の内容	－
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 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	・操作者の認証を行う。 ・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。 ※統合端末のサーバー上で稼動するアプリケーション。市区町村システムで管理されるデータの安全保護対策、不正アクセスの防止策には、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、統合端末のサーバー自体には、外部からのこじあけ等に対して防御性に優れた耐タンパー装置（通信時の相互認証及びデータの暗号化に必要な情報を保管管理する）を内蔵している。
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	

3. 特定個人情報の使用	
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク	
宛名システム等における措置の内容	・団体内統合宛名・連携宛名システムにおいては、番号法及び関係主務省令で定められた事務の担当部署の担当職員以外からは、特定個人情報へのアクセスができないよう制限している。 ・個人番号利用業務以外または、個人番号を必要としない業務から課税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	庁内システムにおける統合端末へのアクセスは既存住民基本台帳ネットワークシステムに限定しており、また、既存住民基本台帳ネットワークシステムと統合端末間では、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。 統合端末のサーバー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、統合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（物理的なアクセス制限、個々の機器を識別する番号（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	帳票印刷等のためにデータ化したものについては、行政情報システム専用のセキュリティ対策が施された指定の一時保管場所にのみ保管し、他への利用が出来ないようにアクセスや複写の制限をかけている。また、利用後はすみやかに削除している。
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： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク	
ユーザ認証の管理	[行っている] ＜選択肢＞ 1）行っている 2）行っていない
具体的な管理方法	・システムの利用が可能な職員を特定し、ICカードと生体情報による認証を行っている。 ・認証後は各システムの利用機能ごとに利用認可を設定し、職員ひとりひとりにシステム上で利用可能な機能を設定して、不正利用が行えない権限設定を実施する。 ・不正なアクセスが行われないように、端末の操作記録であるアクセスログを各区民課職員が毎月1回確認して、記録を残している。
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	・発行管理：人事異動があった場合や権限変更があった場合は、所属長の承認を受けてシステムに反映させている。また、承認期間は最長1年とし、毎年任用期間や委託期間を明示する書面を添えて再申請が必要な運用としている。 ・失効管理：人事異動等により失効者が出た場合には、所属長の承認を受けてシステムに反映させるとともに、処理の遅れが出ないように人事システムからも職員情報を連携して随時更新を行っている。特に任期の定めがある臨時職員・非常勤職員や委託事業者の従事者については、発行申請時に提示された任用期間または、委託期間を超えて利用できないよう自動失効させており、期間の延長は再度発行申請によることとして、失効の手続き漏れを防いでいる。
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	・ICカードについて、利用者を年度ごとに名簿管理し、業務外には施錠できる書庫で保管している。 ・人事情報を入手し、それをもとに権限表を作成する。システム担当者が権限表により発効管理・失効管理を行っており、毎年年度当初までに内容を確認している。 ・大規模な組織変更、人事異動があるときはイベント処理として、事前検証（リハーサル）を行っている。
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	記録項目：処理日時、職員情報、部署情報、端末情報、処理事由、宛名番号、4情報 ・端末から参照、更新した場合の操作記録であるアクセスログを記録している。記録は7年間保存しており、記録を検査・分析し、不正なアクセスがないことを確認している。 ・業務所管課設置の端末には、特定個人情報ファイルを保存できないようシステムで制限をかけている。 ・特定個人情報のバックアップデータ及び操作記録は厳重に管理し、権限を持った者のみがアクセスできるよう制限をかけている。
その他の措置の内容	データベース内では個人番号を保有するテーブル（表）と個人情報を保有するテーブル（表）は別になっており、個人番号を利用しない事務の担当職員は、個人番号を保有する場所にはアクセスできない仕組みとしている。
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： 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	・住民基本台帳ネットワークシステムの操作履歴（操作ログ）を記録する。 ・ログ確認結果を踏まえ、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。 ・住民基本台帳ネットワーク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。 個人情報保護や取扱いについて職員のセキュリティ意識を高めるため、区のセキュリティポリシー、事故事例や対応方法の解説等を行う情報セキュリティ研修の受講とeラーニングの実施を全員に義務付けている。また、年度途中で新規に業務に携わる者についても、業務に携わる前に研修を実施する。 情報セキュリティ研修等を通して、特定個人情報の業務外利用の禁止や漏洩時の罰則、アクセスログが確実に記録されていること等についても、従業者に周知徹底している。
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	業務主管課設置の住記端末には特定個人情報ファイルが保存されない仕組みとなっている。 住民記録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。 個人番号等を保持するテーブル（表）と住民情報等を保持するテーブル（表）は別となっており、個人番号を使用しない事務では個人番号を保持するテーブルにアクセスしない仕組みとなっている。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 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	
・区の情報セキュリティ研修については、派遣事業者及び指定管理事業者の責任者にも毎年参加を義務付けており、事業者の事務従事者全員に対しても職員と同じeラーニング受講と区の研修を受講した責任者による内部研修実施を義務付けている。 ・情報セキュリティ研修においては、標的型メールや委託事業者による情報漏えい等、最新セキュリティ事故の実例をあげるとともに、特定個人情報の業務外利用禁止や漏えい時の罰則（4年以下の懲役又は200万円以下の罰金など）、アクセスログが確実に記録されていること等、従業者に周知徹底している。 ・スクリーンセーバ等を利用して長時間にわたり本人確認情報を表示させない。 ・統合端末のディスプレイを、来庁者から見えない位置に置く。 ・統合端末での画面のハードコピーの取得ができない仕組みになっている。	

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	・業者選定時に選定基準を設定し、委託先の社会的信用と能力を確認する。 ・仕様書には、プライバシーマークを取得している会社に限るなど、委託先の安全管理体制と安全管理措置の内容等、特定個人情報の取扱いが適正であることを条件にしている。	
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	・作業者を限定するために、委託業者の従事者名簿を提出させる。 ・閲覧／更新権限を持つもの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。 ・閲覧／更新の履歴（ログ）を取得し、不正な使用がないことを確認する。	
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	・作業端末へのログイン記録やシステム保守における作業記録をアクセスログとともに、港区情報安全対策実施手順の規定により7年間保存している。 ・委託業務の実施状況について月１回定期的に報告を受け、記録を残す。	
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	・番号法で定められた事項、及び港区情報公開条例、港区個人情報保護条例、港区個人番号の利用並びに特定個人情報の保護及び提供に関する条例、港区情報安全対策指針、港区情報安全対策実施手順等に従いルールを遵守する。	
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	・日常運用においては、港区情報安全対策手順に規定された申請や承認ルールを遵守して事務が執行されていることを定期的にチェックする。	
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	・業務委託が終了した場合、委託元の指示に従い、委託元の責任と負担において個人情報を委託元に返還、破棄若しくは消去しなければならない旨を規定している。 また、書面にて、破棄、消去の方法、完了日等報告させ、必要に応じて職員が実地調査を行う。	
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	・データの秘密保持に関する事項 ・再委託の禁止又は制限に関する事項 ・情報資産の指示された目的外への使用及び第三者への提示の禁止に関する事項 ・データの複写及び複製の禁止に関する事項 ・事故発生時における報告義務に関する事項 ・情報資産の保護状況の検査の実施に関する事項 ・データの授受及び搬送に関する事項 ・委託を受けた事業者等におけるデータの保管及び廃棄に関する事項 ・その他データの保護に関し必要な事項 ・前記各事項の定めに違反した場合における契約解除等の措置及び損害賠償に関する事項	
再委託先による特定個人情報ファイルの適切な取扱いの確保	[　再委託していない　]	＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない
具体的な方法	―	
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		
・区の情報セキュリティ研修については、委託事業者の責任者にも毎年参加を義務付けており、事業者の事務従事者全員に対しても職員と同じeラーニング受講と区の研修を受講した責任者による内部研修実施を義務付けている。 ・情報セキュリティ研修においては、標的型メールや委託事業者による情報漏えい等、最新セキュリティ事故の実例をあげるとともに、特定個人情報の業務外利用禁止や漏えい時の罰則（4年以下の懲役又は200万円以下の罰金など）、アクセスログが確実に記録されていること等、従業者に周知徹底している。		

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、連携時のログ、アクセスログ、収受両システムの連携データ内に記載された連携日時記録であるタイムスタンプにより確認できる。これらの記録は、安全対策実施手順の規定により7年間保存している。
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	・相手方（都道府県サーバー）と区統合端末間の通信は、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システム以外では行わない。 ・区の統合端末は、住民記録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。 ・外部媒体を使用する場合においても、法令及び港区の規程を遵守して提供・移転を行う。
その他の措置の内容	「サーバー室等への入室権限」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（都道府県サーバー）と区統合端末の間の通信では相互認証を実施しているため、認証できない相手先への情報の移転はなされないことがシステム上担保される。
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	・システム上、照会元から指定された検索条件に基づき得た結果を適切に提供することを担保する。 ・相手方（都道府県サーバー）と市区町村統合端末の間の通信では相互認証を実施するため、認証できない相手先への情報の移転はなされないことがシステム上担保される。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 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	
・情報セキュリティ研修に重ねて、番号制度施行前研修において、特定個人情報の法定利用及び条例独自利用にかかる規定、業務外利用や情報漏えい時の罰則（4年以下の懲役又は200万円以下の罰金など）等、従業者に周知徹底する。	

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	
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	[特に力を入れて整備している]	<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	[特に力を入れて整備している]	<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	[特に力を入れて周知している]	<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	[特に力を入れて行っている]	<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	・サーバー室と、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。 ・出入口には機械による入退室を管理する設備を設置している。 ・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。 ・サーバー室内に設置したサーバーは、全て鍵付のサーバーラックに設置している。 ・監視設備として監視カメラ等を設置している。	
⑥技術的対策	[特に力を入れて行っている]	<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	＜区における措置＞ ①ネットワークは不正アクセス防止のため、業務系専用ネットワークで結ぶと共にファイアウォールを設置している。 ②サーバーにウイルス対策ソフトを導入し、パターンファイルを随時更新すると共に、サーバー及び端末のウイルススキャンを日次で行っている。 ③導入しているオペレーティングシステム及びミドルウェアについては、必要に応じてセキュリティパッチの適用を行っている。 ④業務系端末には個人情報等を保管できないよう、システムで制限をかけている。 ⑤区では情報処理システム導入当初より業務用端末の外部接続を禁止しており、業務用端末はインターネットに接続していない。 ＜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導入しているオペレーティングシステム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。	
⑦バックアップ	[特に力を入れて行っている]	<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	[特に力を入れて行っている]	<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	住民基本台帳においては死者も除票住民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。	
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	・個人番号を含む住民情報については、住民記録システムにより、随時異動情報を連携することで最新の情報であることを担保している。また、定期的に住民基本台帳ネットワークシステムと住民記録システムの整合性点検を行っており、それによる修正情報も随時連携されている。
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
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	・サーバー、端末（パソコン）、記録媒体、紙文書等の情報資産を廃棄する場合は、情報を復元できないように処置した上で廃棄する。 ・紙文書は、溶解またはシュレッダー処分を行う。 ・電磁的な記録媒体は、破砕処理、電磁気破壊、データ消去ソフトウエアによるデータ消去を行った上で廃棄する。 ・サーバー、パソコン等情報機器については、記録装置に対し、物理破壊、磁気破壊、データ消去ソフトウエアによるデータ消去を行う。
その他の措置の内容	・データ消去を業者に委託した場合は、消去作業証明書を提出させる。
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	本人確認情報の入手元は既存住民基本台帳ネットワークシステムに限定されるため、既存住民基本台帳ネットワークシステムへの情報の登録の際に、届出／申請等の窓口において届出／申請内容や本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報の入手の防止に努める。
必要な情報以外を入手することを防止するための措置の内容	・平成14年6月10日総務省告示第334号（第6－6　本人確認情報の通知及び記録）等により住民基本台帳ネットワークシステムを利用する端末（統合端末）において既存住民基本台帳ネットワークシステムを通じて入手することととされている情報以外を入手できないことを、住民基本台帳ネットワークシステム上で担保する。 ・正当な利用目的以外の目的にデータベースが構成されることを防止するため、本人確認情報の検索を行う際の検索条件として、少なくとも性別を除く2情報以上（氏名と住所の組み合わせ、氏名と生年月日の組み合わせ）の指定を必須とする。
その他の措置の内容	―
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2：　不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	・送付先情報の入手元を住民記録システムに限定する。 ・届出、申請の記載項目は必要最小限とし、不必要な書類は受理しない。 ・住民基本台帳ネットワークシステムを利用する必要がある職員を特定し、ICカードによる識別とパスワードによる認証を実施しており、不適切な特定個人情報入手が出来ないよう、権限設定を行っている。
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	・窓口にて直接申告書を受け取る場合には、区の要領・手順書等に基づき対面で次の本人確認の書類の提示を受け、本人確認を行う。①個人番号カード、②通知カードと主務省令で定める書類（顔写真入りの官公署発行の身分証明書または顔写真無しの官公署発行の資格証2点） ・各種申告書に記載された個人番号については、住民基本台帳ネットワークシステム及びその運用において照合し、本人確認を行う。
個人番号の真正性確認の措置の内容	・窓口にて直接申告書を受け取る場合には、通知カードと身分証明書、個人番号カードや本人への聞き取りに基づき、宛名システムで管理する真正性の確認が取れた個人番号及び基本4情報等と照合することにより個人番号の真正性確認を行う。 ・他関係機関を経由して、入手した各種申告書の個人番号については、個人番号と基本4情報に基づいて住民記録システム及び住民基本台帳ネットワークシステムに照会を行うことで真正性確認を行う。
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」におけるリスク1、リスク2、リスク3に記載した各措置の通り、入手の各段階で、本人確認とともに、特定個人情報の正確性を確保している。 ・特定個人情報の入力、修正、削除を行う際は、異動対象者又は入力内容に誤りのないよう、入力した職員以外による照合を実施する。
その他の措置の内容	―
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 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	・操作者の認証を行う。 ・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。 ※統合端末のサーバー上で稼動するアプリケーション。市区町村システムで管理されるデータの安全保護対策、不正アクセスの防止策には、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、統合端末のサーバー自体には、外部からのこじあけ等に対して防御性に優れた耐タンパー装置（通信時の相互認証及びデータの暗号化に必要な情報を保管管理する）を内蔵している。
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	

3. 特定個人情報の使用	
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク	
宛名システム等における措置の内容	・団体内統合宛名・連携宛名システムにおいては、番号法及び関係主務省令で定められた事務の担当部署の担当職員以外からは、特定個人情報へのアクセスができないよう制限している。 ・個人番号利用業務以外または、個人番号を必要としない業務から課税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	庁内システムにおける統合端末へのアクセスは既存住民基本台帳ネットワークシステムに限定しており、また、既存住民基本台帳ネットワークシステムと統合端末間では、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。 統合端末のサーバー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、統合端末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、個々の機器を識別する番号（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	帳票印刷等のためにデータ化したものについては、行政情報システム専用のセキュリティ対策が施された指定の一時保管場所にのみ保管し、他への利用が出来ないようにアクセスや複写の制限をかけている。また、利用後はすみやかに削除している。
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： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク	
ユーザ認証の管理	[行っている] ＜選択肢＞ 1）行っている 2）行っていない
具体的な管理方法	・システムの利用が可能な職員を特定し、ICカードと生体情報による認証を行っている。 ・認証後は各システムの利用機能ごとに利用認可を設定し、職員ひとりひとりにシステム上で利用可能な機能を設定して、不正利用が行えない権限設定を実施する。 ・不正なアクセスが行われないように、端末の操作記録であるアクセスログを各区民課職員が毎月1回確認して、記録を残している。
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	・発行管理：人事異動があった場合や権限変更があった場合は、所属長の承認を受けてシステムに反映させている。また、承認期間は最長1年とし、毎年任用期間や委託期間を明示する書面を添えて再申請が必要な運用としている。 ・失効管理：人事異動等により失効者が出た場合には、所属長の承認を受けてシステムに反映させるとともに、処理の遅れが出ないように人事システムからも職員情報を連携して随時更新を行っている。特に任期の定めがある臨時職員・非常勤職員や委託事業者の従事者については、発行申請時に提示された任用期間または、委託期間を超えて利用できないよう自動失効させており、期間の延長は再度発行申請によることとして、失効の手続き漏れを防いでいる。
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	・ICカードについて、利用者を年度ごとに名簿管理し、業務外には施錠できる書庫で保管している。 ・人事情報を入手し、それをもとに権限表を作成する。システム担当者が権限表により発効管理・失効管理を行っており、毎年の年度当初までに内容を確認している。 ・大規模な組織変更、人事異動があるときはイベント処理として、事前検証（リハーサル）を行っている。
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	記録項目：処理日時、職員情報、部署情報、端末情報、処理事由、宛名番号、4情報 ・端末から参照、更新した場合の操作記録であるアクセスログを記録している。記録は7年間保存しており、記録を検査・分析し、不正なアクセスがないことを確認している。 ・業務所管課設置の端末には、特定個人情報ファイルを保存できないようシステムで制限をかけている。 ・特定個人情報のバックアップデータ及び操作記録は厳重に管理し、権限を持った者のみがアクセスできるよう制限をかけている。
その他の措置の内容	データベース内では個人番号を保有するテーブル（表）と個人情報を保有するテーブル（表）は別になっており、個人番号を利用しない事務の担当職員は、個人番号を保有する場所にはアクセスできない仕組みとしている。
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： 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	・住民基本台帳ネットワークシステムの操作履歴（操作ログ）を記録する。 ・ログ確認結果を踏まえ、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。 ・住民基本台帳ネットワーク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。 個人情報保護や取扱いについて職員のセキュリティ意識を高めるため、区のセキュリティポリシー、事故事例や対応方法の解説等を行う情報セキュリティ研修の受講とeラーニングの実施を全員に義務付けている。また、年度途中で新規に業務に携わる者についても、業務に携わる前に研修を実施する。 情報セキュリティ研修等を通して、特定個人情報の業務外利用の禁止や漏洩時の罰則、アクセスログが確実に記録されていること等についても、従業者に周知徹底している。
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	業務主管課設置の住記端末には特定個人情報ファイルが保存されない仕組みとなっている。 住民記録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。 個人番号等を保持するテーブル（表）と住民情報等を保持するテーブル（表）は別となっており、個人番号を使用しない事務では個人番号を保持するテーブルにアクセスしない仕組みとなっている。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 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	
・区の情報セキュリティ研修については、派遣事業者及び指定管理事業者の責任者にも毎年参加を義務付けており、事業者の事務従事者全員に対しても職員と同じeラーニング受講と区の研修を受講した責任者による内部研修実施を義務付けている。 ・情報セキュリティ研修においては、標的型メールや委託事業者による情報漏えい等、最新セキュリティ事故の実例をあげるとともに、特定個人情報の業務外利用禁止や漏えい時の罰則（4年以下の懲役又は200万円以下の罰金など）、アクセスログが確実に記録されていること等、従業者に周知徹底している。 ・スクリーンセーバ等を利用して長時間にわたり本人確認情報を表示させない。 ・統合端末のディスプレイを、来庁者から見えない位置に置く。 ・統合端末での画面のハードコピーの取得ができない仕組みになっている。	

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	・業者選定時に選定基準を設定し、委託先の社会的信用と能力を確認する。 ・仕様書には、プライバシーマークを取得している会社に限るなど、委託先の安全管理体制と安全管理措置の内容等、特定個人情報の取扱いが適正であることを条件にしている。	
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	・作業者を限定するために、委託業者の従事者名簿を提出させる。 ・閲覧／更新権限を持つもの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。 ・閲覧／更新の履歴（ログ）を取得し、不正な使用がないことを確認する。	
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	・作業端末へのログイン記録やシステム保守における作業記録をアクセスログとともに、港区情報安全対策実施手順の規定により7年間保存している。 ・委託業務の実施状況について月１回定期的に報告を受け、記録を残す。	
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	・番号法で定められた事項、及び港区情報公開条例、港区個人情報保護条例、港区個人番号の利用並びに特定個人情報の保護及び提供に関する条例、港区情報安全対策指針、港区情報安全対策実施手順等に従いルールを遵守する。	
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	・日常運用においては、港区情報安全対策手順に規定された申請や承認ルールを遵守して事務が執行されていることを定期的にチェックする。	
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	・業務委託が終了した場合、委託元の指示に従い、委託元の責任と負担において個人情報を委託元に返還、破棄若しくは消去しなければならない旨を規定している。 また、書面にて、破棄、消去の方法、完了日等を報告させ、必要に応じて職員が実地調査を行う。	
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	・データの秘密保持に関する事項 ・再委託の禁止又は制限に関する事項 ・情報資産の指示された目的外への使用及び第三者への提示の禁止に関する事項 ・データの複写及び複製の禁止に関する事項 ・事故発生時における報告義務に関する事項 ・情報資産の保護状況の検査の実施に関する事項 ・データの授受及び搬送に関する事項 ・委託を受けた事業者等におけるデータの保管及び廃棄に関する事項 ・その他データの保護に関し必要な事項 ・前記各事項の定めに違反した場合における契約解除等の措置及び損害賠償に関する事項	
再委託先による特定個人情報ファイルの適切な取扱いの確保	[　再委託していない　]	＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない
具体的な方法	—	
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		
・区の情報セキュリティ研修については、委託事業者の責任者にも毎年参加を義務付けており、事業者の事務従事者全員に対しても職員と同じeラーニング受講と区の研修を受講した責任者による内部研修実施を義務付けている。 ・情報セキュリティ研修においては、標的型メールや委託事業者による情報漏えい等、最新セキュリティ事故の実例をあげるとともに、特定個人情報の業務外利用禁止や漏えい時の罰則（4年以下の懲役又は200万円以下の罰金など）、アクセスログが確実に記録されていること等、従業者に周知徹底している。		

ること等、従来台に周知徹底している。

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、連携時のログ、アクセスログ、収受両システムの連携データ内に記載された連携日時記録であるタイムスタンプにより確認できる。これらの記録は、安全対策実施手順の規定により7年間保存している。
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	・相手方（個人番号カード管理システム）と区の統合端末間の通信は、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。 ・区の統合端末は、住民記録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。 ・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	「サーバー室等への入室権限」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（個人番号カード管理システム）と市区町村統合端末の間の通信では相互認証を実施しているため、認証できない相手先への情報の移転はなされないことがシステム上担保される。
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	・システム上、照会元から指定された検索条件に基づき得た結果を適切に提供することを担保する。 ・相手方（個人番号カード管理システム）と市区町村統合端末の間の通信では相互認証を実施するため、認証できない相手先への情報の移転はなされないことがシステム上担保される。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 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	
・情報セキュリティ研修に重ねて、番号制度施行前研修において、特定個人情報の法定利用及び条例独自利用にかかる規定、業務外利用や情報漏えい時の罰則（4年以下の懲役又は200万円以下の罰金など）等、従業者に周知徹底する。	

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	
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	[特に力を入れて整備している]	<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	[特に力を入れて整備している]	<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	[特に力を入れて周知している]	<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	[特に力を入れて行っている]	<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	・サーバー室と、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。 ・出入口には機械による入退室を管理する設備を設置している。 ・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。 ・サーバー室内に設置したサーバーは、全て鍵付のサーバーラックに設置している。 ・監視設備として監視カメラ等を設置している。	
⑥技術的対策	[特に力を入れて行っている]	<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	＜区における措置＞ ①ネットワークは不正アクセス防止のため、業務系専用ネットワークで結ぶと共にファイアウォールを設置している。 ②サーバーにウイルス対策ソフトを導入し、パターンファイルを随時更新すると共に、サーバー及び端末のウイルススキャンを日次で行っている。 ③導入しているオペレーティングシステム及びミドルウェアについては、必要に応じてセキュリティパッチの適用を行っている。 ④業務系端末には個人情報等を保管できないよう、システムで制限をかけている。 ⑤区では情報処理システム導入当初より業務用端末の外部接続を禁止しており、業務用端末はインターネットに接続していない。 ＜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導入しているオペレーティングシステム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。	
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	住民基本台帳においては死者も除票住民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。	
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

リスクへの対策は十分か	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	・個人番号を含む住民情報については、住民記録システムにより、随時異動情報を連携することで最新の情報であることを担保している。また、定期的に住民基本台帳ネットワークシステムと住民記録システムの整合性点検を行っており、それによる修正情報も随時連携されている。
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
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	・サーバー、端末（パソコン）、記録媒体、紙文書等の情報資産を廃棄する場合は、情報を復元できないように処置した上で廃棄する。 ・紙文書は、溶解またはシュレッダー処分を行う。 ・電磁的な記録媒体は、破砕処理、電磁気破壊、データ消去ソフトウエアによるデータ消去を行った上で廃棄する。 ・サーバー、パソコン等情報機器については、記録装置に対し、物理破壊、磁気破壊、データ消去ソフトウエアによるデータ消去を行う。
その他の措置の内容	データ消去を業者に委託した場合は、消去作業証明書を提出させる。
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	[　　十分に行っている　　]	＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
具体的なチェック方法	年に1回、担当部署内において実施している自己点検に用いるチェック項目に、「評価書の記載内容通りの運用がなされていること」に係る内容を追加し、運用状況を自己点検する。 内部監査チェックリスト及びセキュリティ自己点検チェックリストを用いて、特定個人情報を取扱う従事者全員が定期的に点検作業を行う。	
②監査	[　　十分に行っている　　]	＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
具体的な内容	・内部監査 年に1回、組織内に置かれた監査担当により、以下の観点による自己監査を実施し、監査結果を踏まえて体制や規定を改善する。 ・評価書記載事項と運用実態のチェック ・個人情報保護に関する規定、体制整備 ・個人情報保護に関する人的安全管理措置 ・職員の役割責任の明確化、安全管理措置の周知・教育 ・個人情報保護に関する技術的安全管理措置 ・外部監査 民間機関等より調達する外部監査事業者による情報セキュリティ監査を実施し、監査結果を踏まえて体制や規定を改善する。 ＜ガバメントクラウドにおける措置＞ ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。	

2. 従業者に対する教育・啓発

従業者に対する教育・啓発	[　　十分に行っている　　]	＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
具体的な方法	・職員及び事業所派遣者に対しては、初任時及び1年ごとに、必要な知識の習得に資するため個人情報保護に関する研修の受講を義務付けるとともに、実施記録を残している。 ・委託業者に対しては、個人情報に関する条項を含む契約を締結し区と同等の安全管理措置を求めており、従事者に対する個人情報保護に関する研修の実施や秘密保持契約の締結を義務付けている。 ・自己点検として、住民基本台帳ネットワークや公的個人認証など先行している全国規模のシステムの例にならい、内部監査チェックリスト及びセキュリティ自己点検チェックリストを用いて、特定個人情報を取扱う従事者全員が定期的に点検作業を行うことを義務付ける。 ・違反行為を行った者に対しては、都度指導の上、違反行為の程度によっては懲戒の対象となることを周知している。	

3. その他のリスク対策

区では、情報漏えいなどの万一の事態に備え、次の対策に取り組む。
・情報漏えい等の事案の発生又は兆候を把握した場合に、適切かつ迅速に対応するための安全管理措置を定め、組織体制を整備する。
・特定個人情報等を取り扱う各部署の任務分担や責任を明確化し、特定個人情報等の漏えい、滅失及び毀損等の発生又は兆候を把握した場合や、事務担当者が取扱規程に違反している事実又は兆候を把握した場合に、職員が直ちに責任者へ報告することを義務付ける。
・報告を受けた責任者は、事実関係の調査を行い、漏えい等事案が発覚した場合は、原因の究明に必要な措置を講じ、再発防止策を検討・実施する。
・委託事業者についても区の安全管理措置と同等の措置を講ずることを契約で義務付け、事故発生時における報告や調査への協力、公表措置及び損害賠償、並びに従業者への教育訓練や監督等を義務付ける。

＜ガバメントクラウドにおける措置＞

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

Ⅴ　開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	〒105-8511 東京都港区芝公園1丁目5番25号 芝地区総合支所　区民課 〒106-8515 東京都港区六本木5丁目16番45号 麻布地区総合支所　区民課 〒107-8516 東京都港区赤坂4丁目18番13号 赤坂地区総合支所　区民課 〒108-8581 東京都港区高輪1丁目16番25号 高輪地区総合支所　区民課 〒105-8516 東京都港区芝浦1丁目16番1号 芝浦港南地区総合支所　区民課
②請求方法	開示、訂正等を請求する自己の個人情報を保有している所管課の窓口で相談し、必要事項を記入した指定様式による書面を提出する。
特記事項	区ホームページ上に、請求先、請求方法、諸費用等について掲載する。
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	住民記録システム
公表場所	港区ホームページ
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	芝地区総合支所　区民課　個人番号カード交付推進担当 電話番号　03-3578-3151
②対応方法	問合せを受けた際には、対応内容を記録に残す。 情報漏えい等に関する問い合わせがあった場合は、関係機関と連携して対処する。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	2024/6/28
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	パブリックコメントによる区民意見募集を実施
②実施日・期間	令和7年2月3日～3月4日
③期間を短縮する特段の理由	_
④主な意見の内容	意見なし
⑤評価書への反映	―
3. 第三者点検	
①実施日	令和7年1月15日（諮問）
②方法	港区情報公開・個人情報保護運営審議会諮問
③結果	問題は認められない
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29年8月1日	新規記載	なし	全項目を新規記載	事後	しきい値の再確認により重点項目評価書からの変更
平成31年4月1日	平成30年5月版様式4に変更			事後	様式変更のため
平成31年4月1日	Ⅰ基本情報　7評価実施機関における担当部署②所属長の役職名	区民課長　安藤　俊彰	区民課長	事後	項目内容変更のため
令和2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	（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、101、102、103、105、106、108、111、112、113、114、116、119の項）	（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の項）	事後	法別表第二の根拠修正
令和2年4月1日	Ⅱ ファイルの概要（住民基本台帳）　6．特定個人情報の保管・消去　②保管期間　その妥当性	住民票が消除されない限り、情報は保存される。ただし、住民票が消除された場合は、住民基本台帳施行令第34条に定めるとおり、消除された日から5年間となる。	住民票が消除されない限り、情報は保存される。ただし、住民票が消除された場合は、住民基本台帳施行令第34条に定めるとおり、消除された日から150年間となる。	事後	法改正による項目内容変更のため
令和2年4月1日	Ⅱ ファイルの概要（本人確認情報ファイル）　6．特定個人情報の保管・消去　②保管期間　その妥当性	住民票の記載の修正前の本人確認情報（履歴情報）及び消除者の本人確認情報は、住民基本台帳法施行令第34条第3項（保存）に定める期間（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	法改正による項目内容変更のため
令和2年4月1日	（別添2）ファイル記録項目（本人確認情報ファイル）	－	37．旧氏情報	事後	法改正による項目内容追加のため
令和3年6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	なし	システム8を新規記載	事前	システム追加による重要な変更
令和3年6月30日	Ⅱ　特定個人情報ファイルの概要（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	略	前略 ・窓口総合支援システムへ住民票関係情報を提供する。	事前	システム追加による重要な変更に併せて事前提出
令和3年6月30日	Ⅱ　特定個人情報ファイルの概要（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	なし	委託事項8を新規記載	事前	委託先追加による重要な変更
令和3年6月30日	Ⅱ　特定個人情報ファイルの概要（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、2、3及び5　⑤委託先名の確認方法	委託先については、入札結果として港区ホームページ上で公開している。 再委託先がある場合は、港区個人情報公開条例に基づき情報公開請求を行う。	委託先については、入札結果として港区ホームページ上で公開している。	事後	項目内容（委託先名の確認方法）に合わせ、委託先名の確認方法のみに修正
令和3年6月30日	Ⅱ　特定個人情報ファイルの概要（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	富士通Japan株式会社	事後	名称が変更となったため
令和3年6月30日	Ⅱ　特定個人情報ファイルの概要（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7　⑥委託先名	アデコ株式会社	キャリアリンク株式会社	事後	委託先が変更となったため
令和3年6月30日	Ⅵ　評価実施手続　1．基礎項目評価　①実施日	2017/9/1	2021/3/18	事後	評価書を再点検したため
令和3年6月30日	Ⅵ　評価実施手続　2．国民・住民等からの意見の聴取　②実施日・期間	平成29年9月1日～10月2日（32日間）	令和3年4月1日～4月30日	事後	評価書の再点検に伴い、パブリックコメントを実施したため
令和3年6月30日	Ⅵ　評価実施手続　2．国民・住民等からの意見の聴取　④主な意見の内容	Ⅱファイルの概要　4．特定個人情報ファイルの取扱いの委託について、委託先名の確認方法を情報公開請求を行う、としているが、表現としては他の自治体のように、情報公開条例に基づく公開請求により確認することができるとしたほうが適切ではないか。	システムの追加により委託先が追加されている。今後もシステムの追加のたびに委託先が追加されることが予想される。委託先の追加は個人情報の取扱先が増え、リスクも増える。安易に委託先を増やすのではなく、総合的な観点で委託先を考えるべき。また、LINEによる個人情報問題を鑑み、セキュリティ対策について、体制をしっかりしていただきたい。	事後	評価書の再点検に伴い、パブリックコメントを実施したため
令和3年6月30日	Ⅵ　評価実施手続　2．国民・住民等からの意見の聴取　⑤評価書への反映	「委託先については、入札結果として港区ホームページ上で公開している。再委託先がある場合は、港区情報公開条例に基づき情報公開請求を行う。」	評価書の修正はしませんが、新たな委託事業者に対しても、日ごろからセキュリティ対策を徹底するよう、管理、監督します。	事後	評価書の再点検に伴い、パブリックコメントを実施したため
令和3年6月30日	Ⅵ　評価実施手続　3．第三者点検　①実施日	2017/11/10	2021/6/4	事後	評価書の再点検に伴い、第三者評価を実施したため
令和3年6月30日	Ⅰ基本情報　5情報提供ネットワークシステムによる情報連携　②法令上の根拠	番号法第19条第7号（特定個人情報の提供の制限）	番号法第19条第8号（特定個人情報の提供の制限）	事前	番号法改正のため
令和3年6月30日	Ⅱファイルの概要（住民基本台帳）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7号	番号法第19条第8号	事前	番号法改正のため
令和3年6月30日	別紙1	番号法第19条第7号別表第2に定める事務	番号法第19条第8号別表第2に定める事務	事前	番号法改正のため

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和3年6月30日	Ⅱファイルの概要（住民基本台帳）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19条第10号	番号法第19条第11号	事前	番号法改正のため
令和3年6月30日	Ⅱファイルの概要（住民基本台帳）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1③移転する情報	番号法第19条第7号	番号法第19条第8号	事前	番号法改正のため
令和4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	（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の項）	（1、2、3、4、6、8、9、11、16、18、20、23、27、30、31、34、35、37、38、39、40、42、48、53、54、57、58、59、61、62、66、67、70、74、77、80、84、85の2、89、91、92、94、96、97、101、102、103、105、106、107、108、111、112、113、114、116、117、120の項）	事後	法別表第二の根拠修正
令和5年2月3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	1から10 略	1から10 略 ※申請・届出等は、窓口、郵送及びサービス検索・電子申請機能で受領する。	事前	サービス検索・電子申請機能の利用に伴う見直し
令和5年2月3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（別添1）	新規	（図） サービス検索・電子申請機能による申請の流れを追記	事前	サービス検索・電子申請機能の利用に伴う見直し
令和5年2月3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9	新規	システム9 ①システムの名称 サービス検索・電子申請機能 ②システムの機能 1 住民向け機能 自らが受けることができるサービスをオンラインで検索及び申請ができる機能 2 地方公共団体向け機能 住民が電子申請を行った際の申請データ取得画面又は機能を、地方公共団体に公開する機能 ③他システムとの接続 [○]その他（申請管理システム（MINATO申請ネット））	事前	サービス検索・電子申請機能の利用に伴う見直し
令和5年2月3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10	新規	システム10 ①システムの名称 申請管理システム（MINATO申請ネット） ②システムの機能 サービス検索・電子申請機能からの電子申請データを取込む機能を有する。また、格納された申請データを対象の申請手続き業務システムに連携する。 ③他システムとの接続 [○]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）	事前	サービス検索・電子申請機能の利用に伴う見直し
令和5年2月3日	Ⅱ 特定個人情報ファイルの概要（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	略	前略 [○]その他（サービス検索・電子申請機能）	事前	サービス検索・電子申請機能の利用に伴う見直し
令和5年2月3日	Ⅱ 特定個人情報ファイルの概要（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	略	前略 ＜サービス検索・電子申請機能＞ サービス検索・電子申請機能から送信された電子申請データは、LGWAN環境サーバに一時的に格納され、サインアウト時に消去される。	事前	サービス検索・電子申請機能の利用に伴う見直し
令和5年2月3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（住民基本台帳ファイル）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 対象者以外の情報の入手を防止するための措置の内容	略	前略 ・サービス検索・電子申請機能については、マニュアルやWEB上で、個人番号の提出が必要な者の要件を明示、周知し、本人以外の情報の入手を防止する。	事前	サービス検索・電子申請機能の利用に伴う見直し
令和5年2月3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（住民基本台帳ファイル）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	略	前略 ・サービス検索・電子申請機能においては、画面での誘導を簡潔に行うことで、異なる手続きに係る申請や不要な情報を送信してしまうリスクを防止する。	事前	サービス検索・電子申請機能の利用に伴う見直し
令和5年2月3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（住民基本台帳ファイル）2. 特定個人情報の入手 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	略	前略 ・サービス検索・電子申請機能からの電子申請の際には、署名用電子証明書による電子署名を付して送信することとなり、のちに署名検証も行われるため、本人からの情報のみが送信される。	事前	サービス検索・電子申請機能の利用に伴う見直し
令和5年2月3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（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 入手の際の本人確認の措置の内容	略	前略 ・サービス検索・電子申請機能からの電子申請の際には、署名用電子証明書による電子署名を付すこととなり、電子署名付与済の電子申請データを受領した自治体は署名検証を実施する。これにより本人確認を実施する。	事前	サービス検索・電子申請機能の利用に伴う見直し

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5年2月3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（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　特定個人情報の正確性確保の措置の内容	略	前略 ・サービス検索・電子申請機能においては、個人番号カード内の記憶領域に格納された個人番号を申請フォームに自動転記を行うことにより、不正確な個人番号の入力を抑止する措置を講じている。	事前	サービス検索・電子申請機能の利用に伴う見直し
令和5年2月3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（住民基本台帳ファイル） 2. 特定個人情報の入手　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	略	前略 ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。	事前	サービス検索・電子申請機能の利用に伴う見直し
令和5年2月3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（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　具体的な措置の内容	略	前略 ・LGWAN接続端末については、業務時間内のセキュリティワイヤーによる固定、業務時間外の施錠できるキャビネットへの保管等の安全管理措置を講じている。	事前	サービス検索・電子申請機能の利用に伴う見直し
令和5年2月3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　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　具体的な措置の内容	略	前略 ＜LGWAN接続端末における措置＞ ・サービス検索・電子申請機能から電子申請データを受領するLGWAN接続端末について、ウイルス検出ソフトウェア等の導入により、ウイルス定義ファイルの定期的な更新及びウイルスチェックを実施する。 ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。	事前	サービス検索・電子申請機能の利用に伴う見直し
令和5年2月3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（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	略	前略 ・電子申請データの一時保管中に再申請や申請情報の訂正が発生した場合には古い情報で審査等を行わないよう、履歴管理を行う。	事前	サービス検索・電子申請機能の利用に伴う見直し
令和5年2月3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（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	略	前略 ・サービス検索・電子申請機能におけるLGWAN接続端末については、業務終了後の不要な電子申請データ等の消去を実施する。必要に応じて管理者が確認する。	事前	サービス検索・電子申請機能の利用に伴う見直し
令和5年6月21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10	略	＜申請管理システム＞ 1. データの参照機能 連携サーバから連携された電子申請データを参照する機能。 後略 ＜連携サーバ＞ サービス検索・電子申請機能で受け付けた電子申請データを申請管理システムに連携する（受け渡す）機能。	事後	申請管理システムの導入に伴う見直し
令和5年6月21日	Ⅱ　特定個人情報ファイルの概要（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	略	前略 ［〇］その他（サービス検索・電子申請機能、申請管理システム）	事後	申請管理システムの導入に伴う見直し
令和5年6月21日	Ⅱ　特定個人情報ファイルの概要（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2　①法令上の根拠	番号法第19条第11号、港区個人番号の利用並びに特定個人情報の保護及び提供に関する条例第15条の2別表第3第4項	番号法第19条第11号、港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第5条　別表第3項、第4項	事後	条例改正のため
令和5年6月21日	Ⅱ　特定個人情報ファイルの概要（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	略	前略 ＜申請管理システム＞ 連携サーバに一時的に保管した個人番号付電子申請データは、申請管理システムへ連携後、速やかに完全消去する。	事後	申請管理システムの導入に伴う見直し
令和5年6月21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（住民基本台帳ファイル） 2. 特定個人情報の入手　リスク4　入手した個人情報が漏えい・紛失するリスク　リスクに対する措置の内容	略	前略 ・LGWAN系ネットワークとマイナンバー利用事務系ネットワークの間にDMZ（両ネットワークの中間に置かれ、連携サーバ経由でのみ利用できるようにする機能）を設け、申請管理システムから外部への直接通信を遮断することにより、安全を確保している。また境界FWや連携サーバで外部接続先との通信を制限している。	事後	申請管理システムの導入に伴う見直し

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5年6月21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（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	略	前略 ・申請管理システムへアクセスできる端末を制限する。	事後	申請管理システムの導入に伴う見直し
令和5年6月21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（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	略	前略 ・申請管理システムから取得した個人番号付電子申請データ等のデータについて、改ざんや業務目的以外の複製を禁止するルールを定め、ルールに従って業務を行う。	事後	申請管理システムの導入に伴う見直し
令和5年6月21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（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	略	前略 ＜申請管理システムにおける措置＞ ・申請管理システム及び連携サーバ、申請管理システム接続端末へのウイルス検出ソフトウェア等の導入により、ウイルス定義ファイルの定期的な更新及びウイルスチェックを行い、マルウェア検出を行う。 ・LGWAN系ネットワークとマイナンバー利用事務系ネットワークの間にDMZを設け、申請管理システムから外部への直接通信を遮断することにより、安全を確保している。また境界FWや連携サーバで外部接続先との通信を制限している。	事後	申請管理システムの導入に伴う見直し
令和5年6月21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（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	略	前略 ・申請管理システムでは、申請データの再申請や申請情報の訂正が発生した場合には古い情報で審査等を行わないよう、履歴管理を行う。 ・連携サーバに一時的に保管した個人番号付電子申請データは、申請管理システムへ連携後、速やかに完全消去する。	事後	申請管理システムの導入に伴う見直し
令和5年6月21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（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	略	前略 ・申請管理システム及び連携サーバ内の不要な個人番号付電子申請データの消去について徹底し、必要に応じて管理者が確認する。	事後	申請管理システムの導入に伴う見直し
令和5年6月21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　④個人情報ファイル簿の公表　個人情報ファイル名　公表場所	個人情報取扱業務登録簿　港区役所区政資料室	住民記録システム　港区ホームページ	事後	港区ホームページで個人情報ファイル簿を公表したため
令和6年6月21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	略	前略 7　住基ネットへの連携機能 　住基ネットへの本人確認情報の連携機能、転入通知・戸籍附票通知・転出証明書情報等の区市町村間の通知機能 8　在留カード等発行システム連携機能 　在留カード等発行システムと連携し、法務省通知情報の取込、市町村通知情報の作成を行う機能 9　文字同定機能 　住基ネットと既存住基との文字同定や、在留カード等発行システムとのデータ連携時の文字コード変換機能	事後	利用システムの機能変更に係る修正
令和6年6月21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2	①システムの名称 住基ネットゲートウェイシステム ②システムの機能 略 ③他システムとの接続 略	削除 ※以降のシステムの項番繰り上げ	事後	利用システムの機能変更に係る修正
令和7年3月31日	表紙　欄外	［平成30年5月　様式4］	［令和6年10月　様式4］	事後	様式の変更
令和7年3月31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	（略） なお、9「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）により、地方公共団体情報システム機構に事務の一部を委任する。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「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命令（平成26年11月20日総務省令第85号）により、地方公共団体情報システム機構に事務の一部を委任する。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	誤記修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月31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8号（特定個人情報の提供の制限）　別表第二（別表第二における情報提供の根拠） 第三欄（情報提供者）が「市町村長」の項のうち、第四欄（特定個人情報）に「住民票関係情報」が含まれる項 （1、2、3、4、6、8、9、11、16、18、20、23、27、30、31、34、35、37、38、39、40、42、48、53、54、57、58、59、61、62、66、67、70、74、77、80、84、85の2、89、91、92、94、96、97、101、102、103、105、106、107、108、111、112、113、114、116、117、120の項） （別表第二における情報照会の根拠） なし （住民基本台帳に関する事務において情報提供ネットワークシステムによる情報照会は行わない）	・番号法第19条8号（特定個人情報の提供の制限）及び同号に基づく主務省令第2条の表 （番号法第19条第8号に基づく主務省令第2条の表における情報提供の根拠） ：第三欄（情報提供者）が「市町村長」の項のうち、第四欄（利用特定個人情報）に「住民票関係情報」が含まれる項 （1、2、3、5、7、11、13、15、20、28、37、39、48、53、57、58、59、63、65、66、69、73、75、76、81、83、84、86、87、91、92、96、106、108、110、112、115、118、124、129、130、132、136、137、138、141、142、144、149、150、151、152、155、156、158、160、163、164、165、166の項） （番号法第19条第8号に基づく主務省令第2条の表における情報照会の根拠） ：なし （住民基本台帳に関する事務において情報提供ネットワークシステムによる情報照会は行わない）	事後	番号法別表第二主務省令の改正
令和7年3月31日	Ⅰ　基本情報　7. 評価実施機関における担当部署　①部署	芝地区総合支所区民課	芝地区総合支所区民課 ※事務を担当する各総合支所区民課（芝・麻布・赤坂・高輪・芝浦港南）のうち芝地区総合支所区民課が取りまとめを担う。	事後	第三者点検による修正
令和7年3月31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（別添1）	略	（図） 住民記録システムを中心とした事務の流れの関連システム等を追記	事後	第三者点検による修正
令和7年3月31日	Ⅱ　特定個人情報ファイルの概要（住民基本台帳ファイル） 2. 基本情報　③対象となる本人の範囲　その必要性	（略） 番号法19条第8号表第二の事務において、符号の取得に利用するため	（略） 番号法19条第8号にもとづく主務省令第2条の表に定める事務において、符号の取得に利用するため	事後	番号法別表第二主務省令の改正
令和7年3月31日	Ⅱ　特定個人情報ファイルの概要（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	[○]地方公共団体・地方独立行政法人（他区市町村、地方公共団体情報システム機構）	[○]その他（地方公共団体情報システム機構）	事後	第三者点検による修正
令和7年3月31日	Ⅱ　特定個人情報ファイルの概要（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	（略） 番号法別表第二に基づき、情報提供ネットワークシステムへ住民票関係情報を提供する。	（略） 番号法主務省令第2条の表に基づき、情報提供ネットワークシステムへ住民票関係情報を提供する。	事後	番号法別表第二主務省令の改正
令和7年3月31日	Ⅱ　特定個人情報ファイルの概要（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	番号法第19条第8号別表第二に定める情報照会者（別紙1参照）	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1参照） ※別紙1の修正内容は省略します。	事後	番号法別表第二主務省令の改正
令和7年3月31日	Ⅱ　特定個人情報ファイルの概要（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	番号法第19条第8号別表第二	番号法第19条第8号に基づく主務省令第2条の表	事後	番号法別表第二主務省令の改正
令和7年3月31日	Ⅱ　特定個人情報ファイルの概要（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　②提供先における用途	番号法第19条第8号別表第二に定める各事務	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	事後	番号法別表第二主務省令の改正
令和7年3月31日	Ⅱ　特定個人情報ファイルの概要（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　③提供する情報	番号法第19条第8号別表第二で規定された住民票関係情報	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関係情報	事後	番号法別表第二主務省令の改正
令和7年3月31日	Ⅱ　特定個人情報ファイルの概要（住民基本台帳ファイル） 5. 特定個人情報の提供・移転　移転先1　③移転する情報	番号法第19条第8号別表第二で規定された住民票関係情報	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関係情報	事後	番号法別表第二主務省令の改正
令和7年3月31日	Ⅱ　特定個人情報ファイルの概要（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	略	（略） ＜ガバメントクラウドにおける措置＞ ・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。 ・特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。	事前	ガバメントクラウド移行に伴う修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月31日	Ⅱ　特定個人情報ファイルの概要（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	略	＜ガバメントクラウドにおける措置＞ ・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。 ・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。 ・既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。	事前	ガバメントクラウド移行に伴う修正
令和7年3月31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（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）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　具体的な管理方法	（略） 不正なアクセスが行われないように、端末の操作記録であるアクセスログを取得して、保管している。	（略） 不正なアクセスが行われないように、端末の操作記録であるアクセスログを各区民課職員が毎月1回確認して、記録を残している。	事後	第三者点検による修正
令和7年3月31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（本人確認情報ファイル・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	（略） 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。	（略） ログ確認結果を踏まえ、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。	事後	第三者点検による修正
令和7年3月31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（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）4．特定個人情報ファイルの取扱い　特定個人情報ファイルの取扱いの記録　具体的な方法	（略） 委託業務の実施状況について定期的に報告を受け、記録を残す。	（略） 委託業務の実施状況について月1回定期的に報告を受け、記録を残す。	事後	第三者点検による修正
令和7年3月31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（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　その他の措置の内容	特定個人情報及び個人情報を取り扱う事務の委託について、初回の契約締結前に港区個人情報保護運営審議会に諮問し、承認を受けている。	新たに個人情報を取り扱う事務を委託する場合は、「委託・指定管理チェックリスト」を所管課が作成し、総務課に提出しています。	事後	第三者点検による修正
令和7年3月31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（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	略	（略） ＜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、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。 ・事前に許可されていない装置等に関しては、外部に持出できないこととしている。	事前	ガバメントクラウド移行に伴う修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月31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（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	略	（略） ＜ガバメントクラウドにおける措置＞ ・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。 ・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ついて」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（「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ついて」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。 ・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。 ・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。 ・地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ・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。 ・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。 ・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	ガバメントクラウド移行に伴う修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月31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（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	略	（略） ＜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	ガバメントクラウド移行に伴う修正
令和7年3月31日	Ⅳ　その他のリスク対策 1. 監査　②監査　具体的な内容	略	（略） ＜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	ガバメントクラウド移行に伴う修正
令和7年3月31日	Ⅳ　その他のリスク対策 3　その他のリスク対策	略	（略） 報告を受けた責任者は、事実関係の調査を行い、漏えい等事案が発覚した場合は、原因の究明に必要な措置を講じ、再発防止策を検討・実施する。	事後	第三者点検による修正
令和7年3月31日	Ⅳ　その他のリスク対策 3. その他のリスク対策	略	（略） ＜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	ガバメントクラウド移行に伴う修正
令和7年3月31日	Ⅵ　評価実施手続き 1　基礎項目評価 ①実施日	略	令和7年3月31日	事前	ガバメントクラウド移行に伴う修正
令和7年3月31日	Ⅵ　評価実施手続き 2　国民・住民等からの意見の聴取 ②実施日 ④主な意見の内容	略	②令和7年2月3日～3月4日 ④意見なし	事前	ガバメントクラウド移行に伴う修正
令和7年3月31日	Ⅵ　評価実施手続き 3　第三者点検 ①実施日 ②方法 ③結果	略	①令和7年1月15日（諮問）、令和7年3月17日（答申） ②港区情報公開・個人情報保護運営審議会答申 ③	事前	ガバメントクラウド移行に伴う修正