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
41	都営住宅等の管理に関する事務　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

東京都知事は、都営住宅等の管理に関する事務において、個人番号を利用するに当たり、特定個人情報の不適正な取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減させるために適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組むことを宣言する。

特記事項	－

評価実施機関名

東京都知事

個人情報保護委員会　承認日　【行政機関等のみ】

公表日

［令和6年10月　様式4］

項目一覧

Ⅰ　基本情報

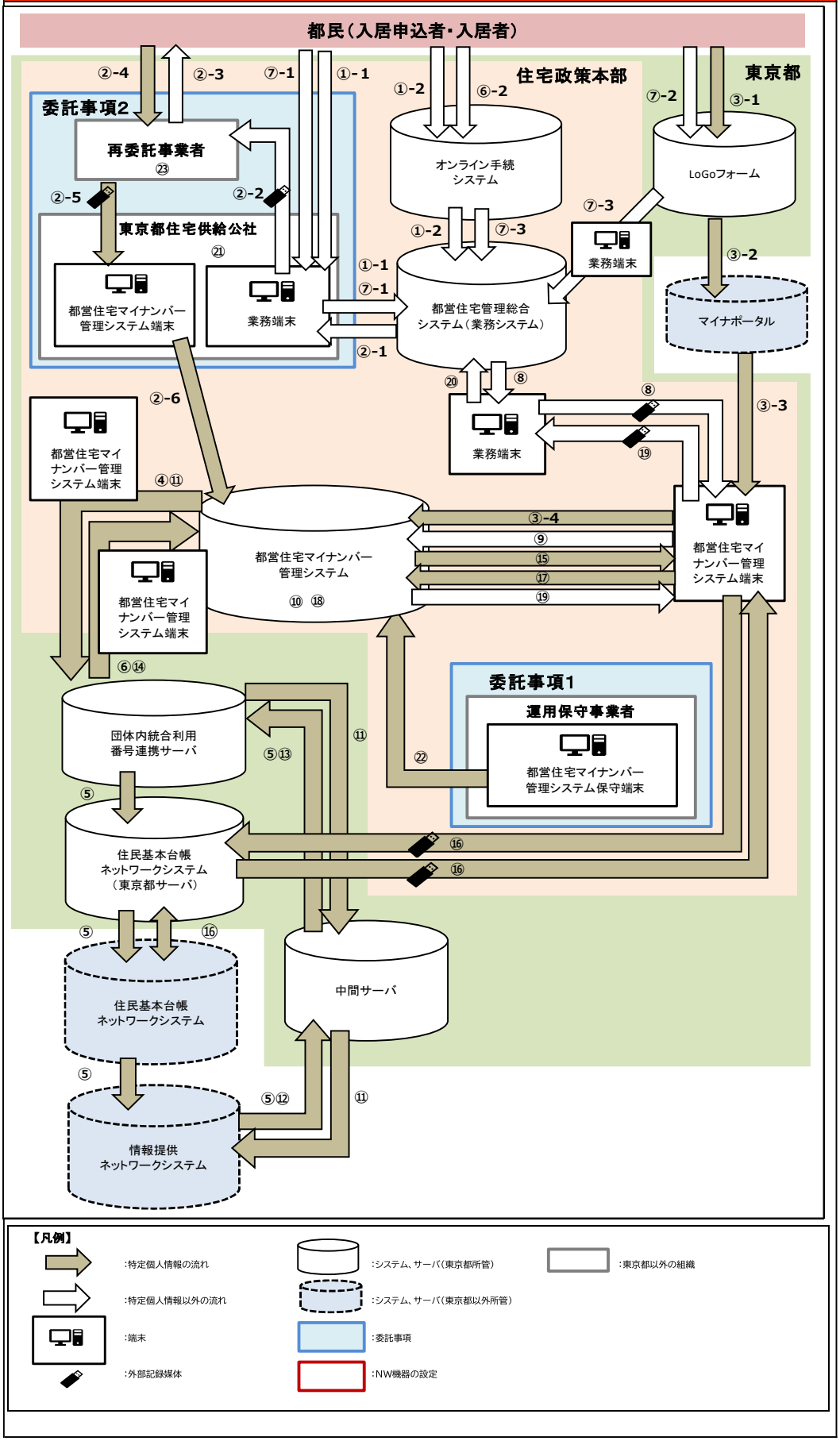
1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	都営住宅等の管理に関する事務
②事務の内容　※	○東京都営住宅条例に定める都営住宅、東京都福祉住宅条例に定める福祉住宅、東京都引揚者住宅条例に定める引揚者住宅、東京都地域特別賃貸住宅条例に定める地域特別賃貸住宅及び東京都特定公共賃貸住宅条例に定める特定公共賃貸住宅（以下「都営住宅等」という。）の管理に関する事務を行っている。 ○特定個人情報ファイルは、以下の事務で使用する。 (1) 収入の申告の受理、その申告に係る事実についての審査又はその申告に対する応答に関する事務 (2)収入の把握に関する事務 (3) 家賃若しくは金銭若しくは敷金の減免の申請の受理、その申請に係る事実についての審査又はその申請に対する応答に関する事務 (4) 入居の申込みの受理、その申込みに係る事実についての審査又はその申込みに対する応答に関する事務 (5) 同居の承認又は入居の承認の申請の受理、その申請に係る事実についての審査又はその申請に対する応答に関する事務 (6) その他東京都営住宅条例等で定める都営住宅等の管理に関する事務
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	都営住宅マイナンバー管理システム（以下「マイナンバー管理システム」という。）
②システムの機能	・個人番号一括登録 ・情報照会用ファイル作成 ・住基ネット照会用ファイル作成 ・情報照会結果の取込 ・住基ネット照会結果の取込 ・業務システム（都営住宅管理総合システム）連携用ファイル作成 ・個人番号一括削除
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [　] その他　（　）
システム2～5	
システム2	
①システムの名称	団体内統合利用番号連携サーバ（以下「連携サーバ」という。）
②システムの機能	・中間サーバへの符号取得要求の仲介 ・団体内統合利用番号の取得、管理 ・符号、団体内統合利用番号、個別業務システム利用番号の紐付管理 ・副本登録における、個別業務システムからの中間サーバへの登録要求の仲介 ・情報照会における、個別業務システムからの照会要求の受付及び中間サーバと個別業務システムとの情報授受の仲介
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　）

システム3	
①システムの名称	中間サーバ
②システムの機能	・符号及び団体内統合利用番号の取得、管理 ・符号、団体内統合利用番号の紐付管理 ・副本管理 ・情報照会の受付及び管理 ・情報提供管理
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　（ 連携サーバ　）
システム4	
①システムの名称	LoGoフォーム
②システムの機能	・電子申請機能 ・マイナポータル（ぴったりサービス）への連携 ・マイナンバーカードからの個人番号情報取得
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　（ ぴったりサービス　）
システム5	
①システムの名称	マイナポータル
②システムの機能	ぴったりサービス： ・Logoフォームからの申請情報の取得 マイナポータル申請管理： ・申請データのダウンロード ・申請データの削除
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　（ マイナンバー管理システム端末　）
システム6～10	
システム6	
①システムの名称	住民基本台帳ネットワークシステム（東京都サーバ）
②システムの機能	・本人確認情報の更新・管理 ・全国サーバに対する更新通知 ・本人確認の情報抽出・出力 ・全国サーバへの情報照会
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　（ 連携サーバ　）

3. 特定個人情報ファイル名	
都営住宅マイナンバー管理システムファイル	
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	・都営住宅等の管理に関する事務手続において、適切な審査を行うため、入居者等の特定個人情報を正確に把握する必要がある。
②実現が期待されるメリット	・情報連携により特定個人情報を入手できるため、手続の際に入居者・入居申込者から求めている公的書類の省略が可能となり、入居者・入居申込者の利便性向上が期待できる。
5. 個人番号の利用　※	
法令上の根拠	・番号法第9条第1項　別表27、52、93の項 ・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基づく個人番号の利用並びに特定個人情報の利用及び提供に関する条例第4条及び別表第一の11から15の項（予定）
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号に基づく主務省令　第2条の表53、76、124の項 ・番号法第19条第9号
7. 評価実施機関における担当部署	
①部署	東京都住宅政策本部都営住宅経営部経営企画課
②所属長の役職名	管理企画担当課長
8. 他の評価実施機関	
－	

（別添1）事務の内容


都民（入居申込者・入居者）
住宅政策本部
東京都
委託事項2
再委託事業者
㉓
東京都住宅供給公社
㉑
都営住宅マイナンバー管理システム端末
業務端末
オンライン手続システム
LoGoフォーム
業務端末
都営住宅管理総合システム（業務システム）
マイナポータル
業務端末
都営住宅マイナンバー管理システム端末
都営住宅マイナンバー管理システム
都営住宅マイナンバー管理システム端末
都営住宅マイナンバー管理システム端末
委託事項1
運用保守事業者
都営住宅マイナンバー管理システム保守端末
団体内統合利用番号連携サーバ
住民基本台帳ネットワークシステム（東京都サーバ）
住民基本台帳ネットワークシステム
中間サーバ
情報提供ネットワークシステム
②-4
②-3
⑦-1
①-1
①-2
⑥-2
⑦-2
③-1
②-5
②-2
⑦-3
①-2
⑦-3
①-1
⑦-1
②-1
③-2
②-6
⑧
⑳
⑧
⑲
③-3
④⑪
③-4
⑨
⑮
⑰
⑲
⑩ ⑱
⑥⑭
⑪
⑤⑬
⑤
⑯
⑯
⑤
⑯
⑤
⑤⑫
⑪
㉒
【凡例】
:特定個人情報の流れ
:特定個人情報以外の流れ
:端末
:外部記録媒体
:システム、サーバ（東京都所管）
:システム、サーバ（東京都以外所管）
:委託事項
:NW機器の設定
:東京都以外の組織

（備考）

1. 入居申込
①-1【窓口・郵送の場合】都民（入居申込者）が、委託業者の窓口等にて入居申込手続を行う。委託業者は受け付けた申込内容を都営住宅管理総合システム（以下「都住システム」という。）に入力する。
①-2【オンラインの場合】都民（入居申込者）が、オンライン手続システムにて入居申込手続を行う。オンライン手続システムに登録された入居申込情報は、データ連携により都住システムに登録される。
※「入居申込者」は、抽選・資格審査等を経て、都営住宅等への入居が決定すると「入居者」となる。

2. 個人番号届出・符号取得
【マイナポータル以外での届出の場合】
②-1 委託業者にて、都住システムにて管理されている、個人番号収集対象者（入居申込者・入居者）の情報を抽出し、リストを作成する。
②-2 委託業者が、個人番号収集対象者（入居申込者・入居者）リストを再委託業者に外部記録媒体で連携する。再委託業者は、データの連携完了後直ちに、外部記録媒体に保存されたデータの削除を行う。
②-3 再委託業者が、個人番号収集対象者（入居申込者・入居者）に個人番号届出用の専用キットを送付する。
②-4 個人番号収集対象者（入居申込者・入居者）は、個人番号届出用の専用キット内の様式に必要事項を記入し、本人確認書類を添付して、追跡ができる郵送方法で再委託業者に返送する。または、再委託業者の専用フォームにて届出をする。
②-5 再委託業者にて、個人番号収集対象者（入居申込者・入居者）から提出された内容の確認(個人番号の真正性確認等)を行う。不備がある場合は、追跡ができる郵送方法で本人に差戻を行う。再委託業者は、収集した個人番号情報をデータ化し、専用線または外部記録媒体で、委託業者に納品する。個人番号収集対象者（入居申込者・入居者）から提出された書類等は、再委託業者にて安全管理措置が施された環境で保管する。また、委託業者は、②-6の作業完了後直ちに、外部記録媒体に保存された個人番号情報データの削除を行う。
②-6 委託業者は、②-5で納品された個人番号情報を都営住宅マイナンバー管理システム（以下「マイナンバー管理システム」という。）に、マイナンバー管理システム端末を利用して取り込む。

【マイナポータルでの届出の場合】
③-1 個人番号を届出る都民（入居申込者・入居者）は、LoGoフォームに接続する。
③-2 LoGoフォームの個人番号届出フォームにて、マイナンバーカードを読み取り、自動的に個人番号等を入力する。必要事項を入力後、提出する。LoGoフォームで提出されたデータは、電子申請等 APIにより、マイナポータルに連携される。
③-3 特定通信により、マイナポータルと接続可能になっているマイナンバー管理システム端末にて、職員がマイナポータル申請管理に接続し、③-2で提出されたデータをダウンロードする（特定通信とは、異なるNW間において、経路を限定することで通信可能にする通信のことを指す。接続先が信頼される特定先との通信でのみ許容される。）。
③-4 職員が、③-3でダウンロードしたデータをマイナンバー管理システムに、マイナンバー管理システム端末を利用して取り込む。

④ 職員が、マイナンバー管理システム端末にて、団体内統合利用番号連携サーバ（以下「連携サーバ」という。）・住民基本台帳ネットワークシステム（以下「住基ネット」という。）を経由し、情報提供ネットワークシステムへ符号取得依頼を行う。
⑤ 情報提供ネットワークシステムから、中間サーバに符号が通知され、中間サーバから連携サーバに符号取得結果が連携される。
⑥ 職員が、マイナンバー管理システム端末にて、連携サーバから団体内統合利用番号を取得し、マイナンバー管理システムに反映する。

3. 届出・申請
⑦-1【窓口の場合】都民（入居申込者・入居者）が、マイナンバー連携対象の手続（届出・申請等）を委託業者の窓口にて紙書類で行う。委託業者は受け付けた手続内容を都住システムに入力する。
⑦-2【オンラインの場合】都民（入居申込者・入居者）が、マイナンバー連携対象の手続（届出・申請等）をオンライン手続システム又はLoGoフォームにて行う。
⑦-3 オンライン手続システム又はLoGoフォームに登録された届出・申請情報は、データ連携（オンライン手続システムの場合はシステム処理による自動連携、LoGoフォームの場合は業務端末上での職員による作業）により都住システムに登録される。
⑧ 職員が、情報照会に必要なデータを都住システムから抽出し、外部記録媒体を介して、業務端末からマイナンバー管理システム端末に連携する。職員は、データの連携完了後直ちに、外部記録媒体に保存されたデータの削除を行う。
⑨ 職員が、マイナンバー管理システムに、マイナンバー管理システム端末を利用して⑧で連携されたデータを取り込む。
⑩ マイナンバー管理システムの情報照会用ファイル作成機能により、マイナンバー情報照会用ファイル・住基ネット照会用ファイルを作成する。
⑪ 職員が、連携サーバへ情報照会要求を行う。連携サーバから、中間サーバを介して情報提供ネットワークシステムへ連携される。
⑫ 情報提供ネットワークシステムから中間サーバへ情報照会結果が連携される。
⑬ 中間サーバから、連携サーバへ情報照会結果が連携される。
⑭ 職員が、連携サーバから情報照会結果を取得する。取得した情報照会結果をマイナンバー管理システムに反映する。
⑮ 職員が、マイナンバー管理システムから住基ネット照会用ファイルを出力する。
⑯ 職員が、外部記録媒体を介して、⑮のデータにより、住基ネットで個人番号による本人確認情報照会を行う。職員は、データの連携完了後直ちに、外部記録媒体に保存されたデータの削除を行う。
⑰ 職員が、住基ネットから取得した本人確認情報照会結果をマイナンバー管理システムに反映する。
⑱ マイナンバー管理システムの都住システム連携用ファイル作成機能により、都住システム連携用ファイルを作成する。
⑲ 職員が、⑱で作成されたデータを外部記録媒体を介して、マイナンバー管理システム端末から、業務端末に連携する。職員は、データの連携完了後直ちに、外部記録媒体に保存されたデータの削除を行う。
⑳ 職員が、⑲で連携されたデータを都住システムに取り込む。
㉑ 都住システムに連携された情報照会結果を参照して、委託業者にて審査を行う。

4. 運用・保守
㉒ 運用保守事業者にてマイナンバー管理システムの運用・保守を行う。

5. 保管・消去
㉓ 個人番号収集対象者（入居申込者・入居者）から提出された書類等は、再委託業者にて一定期間経過後廃棄される。

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	
都営住宅マイナンバー管理システムファイル	
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 ※	都営住宅等の入居者・入居申込者
その必要性	・都営住宅等の管理に関する事務手続において、適切な審査を行うため、入居者等の特定個人情報を正確に把握する必要がある。
④記録される項目	[　　100項目以上　　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
主な記録項目 ※	・識別情報 [○] 個人番号　[　] 個人番号対応符号　[○] その他識別情報（内部番号） ・連絡先等情報 [○] 4情報（氏名、性別、生年月日、住所）　[　] 連絡先（電話番号等） [○] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[○] 地方税関係情報　[　] 健康・医療関係情報 [　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[○] 障害者福祉関係情報 [○] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [○] その他　（　都独自情報（愛の手帳）、戸籍関係情報　）
その妥当性	・識別情報は、特定個人情報と本人を紐づけるために保有する。 ・連絡先等情報は、特定個人情報を利用する入居者・入居申込者を正確に特定するために保有する。 ・業務関係情報は、入居者・入居申込者の事務手続における審査の際に必要となるために保有する。 ①地方税関係情報：課税情報や所得金額を把握し、使用料算定等手続の審査をするために保有 ②生活保護情報：生活保護情報や給付金支給情報を把握し、使用料算定等手続の審査をするために保有 ③障害者情報：身体障害者手帳情報や精神障害者保健福祉手帳情報を把握し、使用料算定等手続の審査をするために保有 ④その他（都独自情報（愛の手帳）、戸籍関係情報）：愛の手帳情報や戸籍関係情報（氏名変更、婚姻状況等）を把握し、使用料算定等手続の審査をするために保有
全ての記録項目	別添2を参照。
⑤保有開始日	令和9年1月
⑥事務担当部署	東京都住宅政策本部都営住宅経営部経営企画課

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 （ 東京都福祉局、総務局<住民基本台帳ネットワークシステム> ） [○] 行政機関・独立行政法人等 （ 法務省<戸籍情報連携> ） [○] 地方公共団体・地方独立行政法人 （ 区市町村 ） [ ] 民間事業者 （ ） [○] その他 （ 情報照会対象者情報<都住システムから抽出し、マイナンバー管理システムに取込> ）
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 （ マイナポータル申請管理、再委託業者による専用フォーム、住民基本台帳ネットワークシステム ）
③入手の時期・頻度		【個人番号の入手】 ・個人番号、連絡先等情報は、原則都度本人から入手する。 ・審査時に、必要に応じて申請者本人と同一住所の者の個人番号を入手する。 【情報連携による入手】 ・例年行う事務（収入の申告等）は、毎年度1回事務に必要な特定個人情報を入手する。 ・その他の事務は、申請を受けた都度特定個人情報を入手する。
④入手に係る妥当性		別紙1「入手に係る根拠規定」を参照。
⑤本人への明示		・本人から入手する際に、個人番号の利用目的を明示する。 ・ホームページに個人番号の利用目的を記載する。
⑥使用目的 ※		・都営住宅等の管理に関する事務手続において、適切な審査を行うために、入居者等の特定個人情報を情報照会し、都住システムに反映させる。
	変更の妥当性	-
⑦使用の主体	使用部署 ※	東京都住宅政策本部都営住宅経営部指導管理課
	使用者数	[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

⑧使用方法　※		・都営住宅等の管理に関する事務手続において、入手した特定個人情報をもとに、使用料の算定や各種許認可等の審査を行う。 【連絡先等情報】 ・個人番号の届出がされている入居者・入居申込者を対象に情報照会を行い、特定個人情報を入手する。 ・個人番号の届出がされている入居者・入居申込者と同一住所の者の情報照会を行い、特定個人情報を入手する。 【業務関係情報】 ・個人番号の届出があり、かつ情報照会の同意が得られた入居者・入居申込者を対象に情報照会を行い、特定個人情報を入手する。
	情報の突合　※	【個人番号の入手】 ・個人番号入手時に、委託業者にて個人番号収集対象者であることを本人確認書類との突合により行う。 ・LoGoフォームでの届出時に、マイナンバーカードを活用した本人確認を行う。 ・加えて、マイナンバー管理システムのデータベースへの登録時にも都営住宅入居者・入居申込者か否か機械的にチェックを行う。 【情報連携による入手】 ・システムにおいて申請者の申請内容と入手した特定個人情報との突合を行い、真正性を担保した上で審査を行う。
	情報の統計分析　※	個人を特定することなく、統計分析を行う。
	権利利益に影響を与え得る決定　※	入居者の決定及び収入状況の報告の請求
⑨使用開始日		2027/1/4

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] ＜選択肢＞ 1）委託する 2）委託しない （ 2 ）件
委託事項1		マイナンバー管理システムの運用委託
①委託内容		マイナンバー管理システムの運用・保守業務（サーバ管理の計画・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 ※	都営住宅等の入居者、都営住宅等の入居申込者
	その妥当性	情報照会に必要な特定個人情報をマイナンバー管理システムにおいて管理するため、委託先で特定個人情報を取り扱う必要がある。
③委託先における取扱者数		[10人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑤委託先名の確認方法		東京都公式ホームページの入札情報サービスにおいて公表する。
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	事前に書面にて都の承認を得る。 承認する際には、再委託を行う業務の内容や執行場所、再委託が必要な理由、再委託先の相手方、責任体制、特定個人情報保護措置の内容等を確認する。
	⑨再委託事項	マイナンバー管理システムのサーバ管理作業の一部
委託事項2～5		
委託事項2		都営住宅等の管理業務委託
①委託内容		都営住宅等の管理業務
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 ※	都営住宅等の入居者、都営住宅等の入居申込者
	その妥当性	情報照会に必要な個人番号を収集する際に、その個人番号が本人のものであるかどうかを確認する必要がある。

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
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		東京都住宅政策本部のホームページ及び東京都公式ホームページの入札情報サービスにおいて公表する。	
⑥委託先名		東京都住宅供給公社	
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	事前に書面にて都の承認を得る。 承認する際には、再委託を行う業務の内容や執行場所、再委託が必要な理由、再委託先の相手方、責任体制、特定個人情報保護措置の内容等を確認する。	
	⑨再委託事項	個人番号の収集業務、収集書類の廃棄等	

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　※		【個人番号提出専用キット】 ・収集した書類等・申請データは、委託先にて安全管理措置に則した管理を行っている。 ・収集した書類等は施錠保管し、業務に携わる者以外の者が触れることが無いよう委託先に求めている。 ・収集した申請データは業務に携わる者以外の者が閲覧できないように委託先に求めている。 【外部記録媒体】 ・収集した特定個人情報をマイナンバー管理システムに移動する場合には、外部記録媒体を活用する。外部記録媒体は施錠保管すると共に、保存するデータは暗号化する。また、使用する際には台帳に使用年月日・使用者等を記録することを委託先に求めている。 ・住民基本台帳ネットワークシステムに提供依頼する対象者データは、外部記録媒体を活用し、移動する。外部記録媒体は施錠保管し、総務局が定める住民基本台帳ネットワークシステムに係る運用規程に基づき暗号化する。 【マイナポータル申請管理】 ・マイナポータル上で管理される。 【マイナンバー管理システム】 ・マイナンバー管理システムは東京都が構築するクラウドインフラ上に、インターネットや庁内の番号系以外のネットワークと分離して構築する。 【中間サーバ・プラットフォーム】 ①中間サーバ・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバ室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行い、厳重に管理する。 ②特定個人情報は、サーバ室に設置された中間サーバのデータベース内に保存され、バックアップもデータベース上に保存される。 【連携サーバ】 ①連携サーバは、サーバ等を設置するための専用施設内に他のシステムとは分離した区画を設け、当該サーバ専用のラックに施錠して収容する。当該施設では、入退室者管理、区画ごとの施錠管理、監視カメラによる録画、有人監視等を実施する。 ②当該施設の煙感知装置、ガス系消火設備、耐震対応等により、火災や地震に起因する滅失等のリスクを低減する。
②保管期間	期間	[　　定められていない　　]　＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	都営住宅等の入居者の場合、入居している限り、保管が必要である。ただし、退去後、特定個人情報が不要となり、保有する必要がないと判断したものについては消去を行う。 都営住宅等の入居申込者の場合、資格審査不合格・入居辞退等の理由により特定個人情報が不要となり、保有する必要がないと判断したものについては消去を行う。

③消去方法	【個人番号提出専用キット】 ・指定した期間を経過した書類については、委託業者において、個人情報の取扱いに留意し、情報漏えい防止対策を講じて、最終的に破砕又は溶解処分し、廃棄完了後は都に証明書を提出するよう求めている。 ・委託業者において保存期間を経過した申請データは、復元不可能な状態とする。 【外部記録媒体】 ・外部記録媒体を用いて特定個人情報を移動した場合、移動完了後直ちに、外部記録媒体に保存された特定個人情報等のデータは、論理削除を行う。外部記録媒体の廃棄に当たっては、物理的破壊等により当該データを復元不可能な状態とする。 【マイナポータル申請管理】 ・申請データは一定期間経過後に削除される。 【マイナンバー管理システム】 ・職員の指示した削除対象データをバッチ処理により削除する。 ・特定個人情報等のデータが記録されうる機器の廃棄の際には、物理的破壊等により、当該データを復元不可能な状態とする。 【中間サーバ・プラットフォーム】 ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバ・プラットフォームの保守・運用を行う事業者が特定個人情報を消去することはない。 ②ディスク交換やハード更改等の際は、中間サーバ・プラットフォームの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊により完全に消去する。 【連携サーバ】 ・個別業務システム（事務）及び中間サーバとの間で授受されるデータは、所要の処理完了後又は一定時間経過後に削除される。 ・機器のうち、特定個人情報等のデータが記録されうるものの廃棄等に当たっては、磁気的消去又は物理的破壊等により、当該データを復元不可能な状態とする。

7. 備考

－

（別添2）特定個人情報ファイル記録項目

別紙2「ファイル記録項目」を参照。

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

都営住宅マイナンバー管理システムファイル

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	【個人番号提出専用キット】 ・都営住宅管理総合システム（以下「都住システム」という。）から、氏名・住所等の必要な項目を抽出し、個人番号収集対象者リストを作成する。対象者にのみ専用キットを送付する。 ・専用キット・個人番号提出用の専用フォームは、対象者の情報のみを記載する様式となっている。 ・個人番号収集対象者から提出された内容について、①収集対象者であること②添付された本人確認書類と相違が無いことを確認する。 ・個人番号収集対象者から提出された内容に不備がある場合は書類の返送等差戻を行う。 【LoGoフォーム】 ・申請の際には、公的個人認証による本人確認を行う。 ・対象者の情報のみ記載するフォームとなっている。 【マイナンバー管理システム】 ・マイナンバー管理システムに、収集した個人番号情報を反映する際に都営住宅入居者・入居申込者か否か機械的にチェックを行う。 ・チェックでエラーとなった場合は、データ反映は行わず、書類の返送等差戻を行う。 【住民基本台帳ネットワークシステム】 ・住民基本台帳法及び条例に規定された事務に関する情報以外は入手できないよう、住民基本台帳ネットワークシステムで制御されている。 ・住民基本台帳ネットワークシステムに提供依頼する対象者データは、マイナンバー管理システムから出力する。マイナンバー管理システムでは、都営住宅等の入居者・入居申込者から届出申請があった手続の情報のみ管理する。そのため、届出申請がされていない手続・対象者について照会をすることはできない。 【庁内連携】 （連携サーバ） ・照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められ、かつ移転者が明示的に回答を承認した場合に限り、連携を行う。照会に対しては、照会条件として指定された対象者に関する情報だけを回答する。なお、チェック項目は、番号法等の改正に応じて、更新する。 （マイナンバー管理システム） ・マイナンバー管理システムでは、情報連携を許可された手続かつ入居者・入居申込者から届出申請があった手続の情報（情報照会内容と、その照会結果）のみ管理する。そのため、許可されていない手続や届出申請がされていない手続について情報照会をすることはできない。 ・マイナンバー管理システムの操作履歴（ユーザID、操作時間、操作内容等）は自動的に記録される。

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	【個人番号提出専用キット】 ・専用キット・個人番号提出用の専用フォームは、必要な情報のみを記載する様式となっている。 【LoGoフォーム】 ・必要な情報のみを記載するフォームとなっている。 【マイナンバー管理システム】 ・マイナンバー管理システムに、収集した個人番号情報を反映する際に都営住宅入居者・入居申込者か否か機械的にチェックを行う。 ・チェックでエラーとなった場合は、データ反映は行わず、書類の返送等差戻を行う。 【住民基本台帳ネットワークシステム】 ・住民基本台帳ネットワークシステムが保有している情報は、住民基本台帳法によって定められており、氏名、生年月日、性別、住所、個人番号、住民票コード及びそれらの変更情報に限られている。 ・住民基本台帳法及び条例に規定された事務に関する情報以外は入手できないよう、住民基本台帳ネットワークシステムで制御されている。 ・住民基本台帳ネットワークシステムに提供依頼する対象者データは、マイナンバー管理システムから出力する。マイナンバー管理システムでは、都営住宅等の入居者・入居申込者から届出申請があった手続の情報のみ管理する。そのため、届出申請がされていない手続・対象者について照会をすることはできない。 【庁内連携】 （連携サーバ） ・照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められ、かつ移転者が明示的に回答を承認した場合に限り、連携を行う。照会に対しては、照会条件として指定された対象者に関する情報だけを回答する。なお、チェック項目は、番号法等の改正に応じて、更新する。 （マイナンバー管理システム） ・マイナンバー管理システムでは、情報連携を許可された手続かつ入居者・入居申込者から届出申請があった手続の情報（情報照会内容と、その照会結果）のみ管理する。そのため、許可されていない手続や届出申請がされていない手続について情報照会をすることはできない。 ・マイナンバー管理システムの操作履歴（ユーザID、操作時間、操作内容等）は自動的に記録される。
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	【個人番号提出専用キット・LoGoフォーム・マイナンバー管理システム】 ・本人から入手する際に、個人番号の利用目的を明示する。 ・ホームページに個人番号の利用目的を記載する。 ・個人番号等の提出にあたっては、必要最小限の書類や手順により、提出を可能とする。 ・個人番号利用事務にあたる職員を事前に指定すると共に、各システムの操作が可能な職員をログイン時の認証や権限制御により限定する。 【住民基本台帳ネットワークシステム】 ・住民基本台帳ネットワークシステムを所管する総務局が定める利用届により、住民基本台帳法により本人確認情報の利用が認められている旨を申請し、総務局の許可を事前に受けた上で入手を行う。 ・住民基本台帳ネットワークシステムを所管する総務局が定める様式及び方法により、入手を行う。 【庁内連携】 （連携サーバ） ・照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められ、かつ移転者が明示的に回答を承認した場合に限り、連携を行う。照会に対しては、照会条件として指定された対象者に関する情報だけを回答する。なお、チェック項目は、番号法等の改正に応じて、更新する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・全ての照会及び回答について、特定個人情報の照会者、移転者、日時等をシステム上でアクセスログとして記録し、7年間保存する。
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	【個人番号提出専用キット】 ・都住システムから氏名・住所等の必要な項目を抽出し、個人番号収集対象者リストを作成する。 ・収集時に、特定個人情報が確認できる本人確認書類を提出させる。 ・個人番号収集対象者から提出された内容について、①収集対象者であること②添付された本人確認書類と相違が無いことを確認する。 【LoGoフォーム】 ・申請の際には、公的個人認証による本人確認を行う。 ・マイナンバーカードの読み取りにより、自動的に申請フォームに特定個人情報が入力される。 【住民基本台帳ネットワークシステム】 ・住民基本台帳を所管する各自治体で本人確認済み。 【庁内連携】 （連携サーバ） ・各事務所管部署で本人確認及び真正性確認を行った個人番号に基づき、統合利用番号及び個別業務システム利用番号が紐付けられていることを前提として、当該人に対する情報照会が可能となるよう制御されている。 （マイナンバー管理システム） ・【個人番号提出専用キット】または【LoGoフォーム】で本人確認が完了した特定個人情報のみ、マイナンバー管理システムにて管理する。

個人番号の真正性確認の措置の内容	【個人番号提出専用キット】 ・都住システムから氏名・住所等の必要な項目を抽出し、個人番号収集対象者リストを作成する。 ・個人番号収集対象者から提出された内容について、添付された本人確認書類（個人番号が確認できる資料）との突合を行い、個人番号の真正性確認を行う。 ・個人番号のチェックデジットの検証により、真正性確認を行う。 【LoGoフォーム】 ・申請の際には、公的個人認証による本人確認を行う。 ・マイナンバーカードの読み取りにより、自動的に申請フォームに特定個人情報が入力される。 【マイナンバー管理システム】 ・個人番号のチェックデジットの検証により、真正性確認を行う。 【住民基本台帳ネットワークシステム】 ・住民基本台帳を所管する各自治体で真正性確認済み。 【庁内連携】 （連携サーバ） ・各事務所管部署で本人確認及び真正性確認を行った個人番号に基づき、統合利用番号及び個別業務システム利用番号が紐付けられていることを前提として、当該人に対する情報照会が可能となるよう制御されている。 （マイナンバー管理システム） ・【個人番号提出専用キット】または【LoGoフォーム】で本人確認が完了した特定個人情報のみ、マイナンバー管理システムにて管理する。
特定個人情報の正確性確保の措置の内容	【マイナンバー管理システム】 ・特定個人情報に変更があった場合、都営住宅入居者又は入居申込者が東京都に対して届出申請を行う。 ・届出申請内容から、職員にてマイナンバー管理システムの情報を更新する。 ・マイナンバー管理システムに、入手した特定個人情報を反映する際に、システムで管理している情報と相違がある場合は、エラーとして検知する。 【住民基本台帳ネットワークシステム】 ・住民基本台帳を所管する各自治体において正確性は確保されている。 【庁内連携】 （連携サーバ） ・各事務所管部署からの申請に基づき、利用者とその所掌事務の紐付けが連携サーバ上であらかじめ定義され、その範囲においてのみ情報照会が可能となるようアクセス制御されている。 ・情報照会に対する回答は、当該照会を行った事務に対してのみ返却するよう制御されている。 ・各事務所管部署が個々の照会データを一意に識別できるよう付与した識別子を、連携サーバからの回答データに付記して返却することで、どの照会に対する回答かを各事務所管部署で正確に突合できるようにしている。 （マイナンバー管理システム） ・連携サーバを使用して、団体内統合利用番号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。
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	・個人番号利用事務にあたる職員を事前に指定する。 【個人番号提出専用キット】 ・専用キットは発送から受け取りまでの証跡管理、状況管理が可能となるよう委託先に求めている。 ・収集した書類は施錠保管するよう求めている。 ・専用フォームで収集した個人番号情報は委託業務に携わる者以外の者が閲覧できないように委託先に求めている。 【LoGoフォーム】 ・LoGoフォームで収集した個人番号情報は、ぴったりサービス（電子申請等API）を通じてマイナポータル申請管理に連携され、庁内の専用端末（マイナンバー管理システム用端末）でのみ閲覧・取得が可能である。 ・専用端末は利用する職員ごとにユーザIDを割り当て、ログイン時に認証（多要素認証等）を行っている。 ・マイナポータル申請管理の申請データのダウンロード履歴は自動的に記録される。 【マイナンバー管理システム】 ・マイナンバー管理システムは専用端末でのみ利用が可能である。 ・専用端末は利用する職員ごとにユーザIDを割り当て、ログイン時に認証（多要素認証等）を行っている。 ・マイナンバー管理システムを使用する職員ごとにユーザID・操作権限を割り当て、ログイン時の認証と権限による機能制御を行っている。 ・マイナンバー管理システムの操作履歴（ユーザID、操作時間、操作内容等）は自動的に記録される。 【住民基本台帳ネットワークシステム】 ・入手に係る外部記録媒体は、住民基本台帳ネットワークシステムを所管する総務局に許可された物を使用する。 ・対象者に係る照会データを格納した外部記録媒体については、総務局が定める住民基本台帳ネットワークシステムに係る運用規程に基づき暗号化し、総務局に職員が持ち込む。 ・総務局から入手する本人確認情報を格納した外部記録媒体については、暗号化されている。 【庁内連携】 （連携サーバ） ・ログイン時に利用者の認証を実施する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・全ての照会及び回答について、特定個人情報の照会者、移転者、日時等をシステム上でアクセスログとして記録し、7年間保存する。 ・照会側と提供（回答）側の間で行われる特定個人情報の授受に当たっては、その中継のみを行い、システム内に特定個人情報（副本相当）は保有しない。 ・連携サーバ端末は執務室内に設置し、操作画面が部外者の目に触れないように配置する。 （マイナンバー管理システム） ・情報照会に係る操作とマイナンバー管理システムに係る操作は同一の専用端末上で行うため、特定個人情報を外部記録媒体等に書き出すことが無く、漏えい・紛失のリスクに対応している。 ・専用端末は利用する職員ごとにユーザIDを割り当て、ログイン時に認証（多要素認証等）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
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	【連携サーバ】 ・個人番号に係る共通基盤である連携サーバは、ユーザIDにより利用者・個別業務システム（事務）等の単位でアクセス可能な範囲を限定し、正当な権限のない利用者・個別業務システム（事務）等からは個人番号を利用できないよう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	【マイナポータル申請管理】 ・LoGoフォームで収集した個人番号情報は、ぴったりサービス（電子申請等API）を通じてマイナポータル申請管理に連携され、庁内の専用端末（マイナンバー管理システム用端末）でのみ閲覧・取得が可能である。 ・専用端末は利用する職員ごとにユーザIDを割り当て、ログイン時に認証（多要素認証等）を行っている。 ・マイナンバー管理システムに、収集した個人番号情報を反映する際に都営住宅入居者・入居申込者か否か機械的にチェックを行う。 【マイナンバー管理システム】 ・マイナンバー管理システムは専用端末でのみ利用が可能である。 ・専用端末は利用する職員ごとにユーザIDを割り当て、ログイン時に認証（多要素認証等）を行っている。 ・マイナンバー管理システムを使用する職員ごとにユーザID・操作権限を割り当て、ログイン時の認証と権限による機能制御を行っている。 ・マイナンバー管理システムでは、情報連携を許可された手続かつ入居者・入居申込者から届出申請があった手続の情報（情報照会内容と、その照会結果）のみ管理する。そのため、許可されていない手続や届出申請がされていない手続について情報照会をすることはできない。	
その他の措置の内容	－	
リスクへの対策は十分か	［　　十分である　　］	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク		
ユーザ認証の管理	［　行っている　］	＜選択肢＞ 1）行っている　　2）行っていない
具体的な管理方法	【マイナポータル申請管理】 ・LoGoフォームで収集した個人番号情報は、ぴったりサービス（電子申請等API）を通じてマイナポータル申請管理に連携され、庁内の専用端末（マイナンバー管理システム用端末）でのみ閲覧・取得が可能である。 ・専用端末は利用する職員ごとにユーザIDを割り当て、ログイン時に認証（多要素認証等）を行っている。 ・マイナポータル申請管理を利用する（データをダウンロードする）職員ごとにユーザIDを割り当てている。 ・職員等の採用、異動、出向、退職時等には、速やかにIDの設定や更新を行う。 【マイナンバー管理システム】 ・マイナンバー管理システムは専用端末でのみ利用が可能である。 ・専用端末は利用する職員ごとにユーザIDを割り当て、ログイン時に認証（多要素認証等）を行っている。 ・マイナンバー管理システムを使用する職員ごとにユーザIDを割り当てている。 ・マイナンバー管理システムの操作履歴（ユーザID、操作時間、操作内容等）は自動的に記録される。 ・職員等の採用、異動、出向、退職時等には、速やかにIDの設定や更新を行う。また、年1回以上定期的にIDの確認を行う。	

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	【マイナポータル申請管理】 ・マイナポータル申請管理を利用する（データをダウンロードする）職員ごとにユーザIDを割り当てている。 ・職員等の採用、異動、出向、退職時等には、速やかにID・権限の設定や更新を行う。 ・付与するアクセス権限に過不足が生じないよう設定済の内容を年1回以上定期的に確認する。 【マイナンバー管理システム】 ・マイナンバー管理システムを使用する職員ごとにユーザID・操作権限を割り当て、ログイン時の認証と権限による機能制御を行っている。 ・職員等の採用、異動、出向、退職時等には、速やかにID・権限の設定や更新を行う。 ・付与するアクセス権限に過不足が生じないよう設定済の内容を年1回以上定期的に確認する。
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	【マイナポータル申請管理】 ・個人番号利用事務にあたる職員を事前に指定すると共に、指定した職員にのみ、必要最低限のアクセス権限を付与する。 ・職員等の採用、異動、出向、退職時等には、速やかにID・権限の設定や更新を行う。 【マイナンバー管理システム】 ・個人番号利用事務にあたる職員を事前に指定すると共に、指定した職員にのみ、必要最低限のアクセス権限を付与する。 ・職員等の採用、異動、出向、退職時等には、速やかにID・権限の設定や更新を行う。
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	【マイナポータル申請管理】 ・マイナポータル申請管理の申請データのダウンロード履歴は自動的に記録される。 【マイナンバー管理システム】 ・マイナンバー管理システムの操作履歴（ユーザID、操作時間、操作内容等）は自動的に記録される。
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	【マイナポータル申請管理】 ・マイナポータル申請管理の申請データのダウンロード履歴は自動的に記録される。 ・LoGoフォームで収集した個人番号情報は、ぴったりサービス（電子申請等API）を通じてマイナポータル申請管理に連携され、庁内の専用端末（マイナンバー管理システム用端末）でのみ閲覧・取得が可能である。 ・専用端末は個人番号利用事務以外の操作が禁止となっており、利用可能なソフトウェア等が制限されている。 【マイナンバー管理システム】 ・マイナンバー管理システムの操作履歴（ユーザID、操作時間、操作内容等）は自動的に記録される。 ・マイナンバー管理システムは専用端末でのみ利用が可能である。 専用端末は個人番号利用事務以外の操作が禁止となっており、利用可能なソフトウェア等が制限されている。 ・マイナンバー管理システムでは、情報連携を許可された手続かつ入居者・入居申込者から届出申請があった手続の情報（情報照会内容と、その照会結果）のみ管理する。そのため、許可されていない手続等で使用することはできない。
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	【マイナポータル申請管理】 ・マイナポータル申請管理の申請データのダウンロード履歴は自動的に記録される。 ・LoGoフォームで収集した個人番号情報は、ぴったりサービス（電子申請等API）を通じてマイナポータル申請管理に連携され、庁内の専用端末（マイナンバー管理システム用端末）でのみ閲覧・取得が可能である。 ・専用端末は個人番号利用事務以外の操作が禁止となっており、利用可能なソフトウェア等が制限されている。 ・業務において、必要な範囲を超えての作成を禁止しており、研修や自己点検表等により注意喚起している。 【マイナンバー管理システム】 ・マイナンバー管理システムの操作履歴（ユーザID、操作時間、操作内容等）は自動的に記録される。 ・マイナンバー管理システムは専用端末でのみ利用が可能である。 専用端末は個人番号利用事務以外の操作が禁止となっており、利用可能なソフトウェア等が制限されている。 ・業務において、必要な範囲を超えての作成を禁止しており、研修や自己点検表等により注意喚起している。
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
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	
－	

4. 特定個人情報ファイルの取扱いの委託		[　　]委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認		仕様書において、下記事項を規定している。 ①責任者、作業体制及び連絡体制の承認 ②業務従事者への遵守事項の周知及び実施報告書の提出 ③(再委託の場合)再委託の事前承認
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	・個人番号利用事務にあたる職員を事前に指定する。 【個人番号提出専用キット】 ・収集した書類は施錠保管するよう求めている。委託業務に携わる者以外の者は閲覧できないように委託先に求めている。 ・専用フォームで収集した個人番号情報は委託業務に携わる者以外の者が閲覧できないように委託先に求めている。 【マイナンバー管理システム】 ・マイナンバー管理システムは専用端末でのみ利用が可能である。 ・専用端末は利用する委託先の職員ごとにユーザIDを割り当て、ログイン時に認証(多要素認証等)を行っている。 ・マイナンバー管理システムを使用する委託先の職員ごとにユーザID・操作権限を割り当て、ログイン時の認証と権限による機能制御を行っている。
特定個人情報ファイルの取扱いの記録		[　　記録を残している　　]　＜選択肢＞ 1) 記録を残している　2) 記録を残していない
	具体的な方法	【個人番号提出専用キット】 ・専用キットは発送から受け取りまでの証跡管理、状況管理が可能となるよう委託先に求めている。 ・専用フォームで収集した個人番号情報に対する操作は操作履歴を残すように委託先に求めている。 【マイナンバー管理システム】 ・マイナンバー管理システムの操作履歴(ユーザID、操作時間、操作内容等)は自動的に記録される。
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	・業務上、他者への提供は発生しない。
	委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	【委託事項1・委託事項2】 ・委託先に提供する専用端末を通じて、委託先は特定個人情報を閲覧することができる。 ・特定個人情報の提供に関するルールの遵守状況は、委託先において実施する監査や自己点検により確認するとともに、委託元が委託先に実施する監査により確認する。 【委託事項2】 ・委託先に提供する専用端末を通じて、委託先から委託元へ特定個人情報を提供する。

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	【個人番号提出専用キット】 ・仕様書において、委託業者が保管する特定個人情報を保有する必要がなくなったとき、または委託履行完了時には、確実かつ速やかに特定個人情報を廃棄または消去しなければならないとしている。 ・指定した期間を経過した書類については、委託業者において、個人情報の取扱いに留意し、情報漏えい防止対策を講じて、最終的に破砕又は溶解処分し、廃棄完了後は都に証明書を提出するよう求めている。 ・保存期間を経過した申請データは、復元不可能な状態とするよう求めている。 【マイナンバー管理システム】 ・委託履行完了時に、当該委託業務に係る情報を全て消去することを、仕様書で規定している。 ・消去方法・消去日等を記録した報告書の提出を求めている。
委託契約書中の特定個人情報ファイルの取扱いに関する規定		[　　定めている　　] ＜選択肢＞ 1）定めている　2）定めていない
	規定の内容	【個人番号提出専用キット】 ・仕様書において、安全管理措置を講じるための管理体制を構築することを規定している。 ・仕様書において、特定個人情報の管理に係る安全管理措置を講じることを求めている。 ・委託元による点検・監査への協力義務等を定めている。 【マイナンバー管理システム】 ・仕様書において、安全管理措置を講じるための管理体制を構築することを規定している。 ・仕様書において、特定個人情報の管理に係る安全管理措置を講じることを求めている。 ・委託元による点検・監査への協力義務等を定めている。
再委託先による特定個人情報ファイルの適切な取扱いの確保		[　　十分に行っている　　] ＜選択肢＞ 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	・仕様書において、再委託を開始する場合は、再委託を行う業務の内容や執行場所、再委託が必要な理由、再委託先の相手方、責任体制、特定個人情報保護措置の内容等を記載した書面で、委託元の承諾を得ることとしている。 ・委託元と委託先の間で取り交わされている契約内容と同等の条件を再委託先においても求めている。 ・委託先と同様の監査を委託元から再委託先に対して行うこととしている。
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
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	[ ] ＜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	
特定個人情報の提供・移転に関するルール	[ ] ＜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	
その他の措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
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	[ ] ＜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	
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
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	【中間サーバ・ソフトウェア】 ①情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ②中間サーバの職員認証・権限管理機能（※3）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。 （※1）情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 （※2）番号法の規定によ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に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。 【連携サーバ】 ・各事務所管部署からの申請に基づき、利用者とその所掌事務の紐付けが連携サーバ上であらかじめ定義され、その範囲においてのみ情報照会が可能となるようアクセス制御されている。 ・符号取得においては、あらかじめ各事務のシステムにて登録され、個別業務システム利用番号が割り当てられた状態の対象者のみを受付けるよう制御されている。 ・符号取得に対する回答及び情報照会に対する回答は、当該照会を行った事務に対してのみ返却するよう制御されている。 ・各事務所管部署が個々の照会データを一意に識別できるよう付与した識別子を、連携サーバからの回答データに付記して返却することで、どの照会に対する回答かを各事務所管部署で正確に突合できるようにしている。 【マイナンバー管理システム】 ・マイナンバー管理システムは専用端末でのみ利用が可能である。 ・専用端末は利用する職員ごとにユーザIDを割り当て、ログイン時に認証（多要素認証等）を行っている。 ・マイナンバー管理システムを使用する職員ごとにユーザID・操作権限を割り当て、ログイン時の認証と権限による機能制御を行っている。 ・マイナンバー管理システムでは、情報連携を許可された手続かつ入居者・入居申込者から届出申請があった手続の情報（情報照会内容と、その照会結果）のみ管理する。そのため、許可されていない手続や届出申請がされていない手続について情報照会をすることはできない。 ・マイナンバー管理システムの操作履歴（ユーザID、操作時間、操作内容等）は自動的に記録される。
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	【中間サーバ・ソフトウェア】 ①中間サーバは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理す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入手のみ実施できるよう設計されるため、安全性が担保されている。 【中間サーバ・プラットフォーム】 ①中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 【連携サーバ】 ・システムを利用可能な時間を制限している。 ・情報連携に用いる端末に対し、端末認証を行う。 ・ログイン時にID・PWと生体認証の二要素認証を実施する。 ・個別業務システム（事務）との間は、庁内のネットワークを介するとともに、暗号化を行う。 ・連携サーバから個別業務システム（事務）に提供する照会結果ファイルは、暗号化を行う。 ・中間サーバとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。 ・サーバ認証により真正性が担保された中間サーバに接続する。 【マイナンバー管理システム】 ・マイナンバー管理システムは専用端末でのみ利用が可能である。 ・専用端末は利用する職員ごとにユーザIDを割り当て、ログイン時に認証（多要素認証等）を行っている。 ・マイナンバー管理システムを使用する職員ごとにユーザID・操作権限を割り当て、ログイン時の認証と権限による機能制御を行っている。 ・マイナンバー管理システムは東京都が構築するクラウドインフラ上に、インターネットや庁内の番号系以外のネットワークと分離して構築する。 ・専用端末からの接続のみとするため、IPアドレスによる制限等により許可していない端末からの通信遮断を行う。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 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	【中間サーバ・ソフトウェア】 ①中間サーバは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。 【連携サーバ】 ・各事務所管部署で本人確認及び真正性確認を行った個人番号に基づき、個別業務システム利用番号が割り当てられていることを前提として、当該人に対する符号取得が可能となるよう制御されている。 ・各事務所管部署で本人確認及び真正性確認を行った個人番号に基づき、統合利用番号及び個別業務システム利用番号が紐付けられていることを前提として、当該人に対する情報照会が可能となるよう制御されている。 ・サーバ認証により真正性が担保された中間サーバに接続する。 【マイナンバー管理システム】 ・情報提供ネットワークシステム・中間サーバ・連携サーバを使用して、統合宛名番号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。
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

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	【中間サーバ・ソフトウェア】 ①中間サーバは、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入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ②既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ③情報照会が完了又は中断した情報照会結果については、一定期間経過後に結果情報を情報照会機能において自動で削除することにより、特定個人情報が漏えい・紛失するリスクを軽減している。 ④中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）中間サーバは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 【中間サーバ・プラットフォーム】 ①中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、漏えい・紛失のリスクに対応している。 ②中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバ・プラットフォーム事業者の業務は、中間サーバ・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはない。 【連携サーバ】 ・システムを利用可能な時間を制限している。 ・情報連携に用いる端末に対し、端末認証を行う。 ・ログイン時にID・PWと生体認証の二要素認証を実施する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・中間サーバとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。 ・サーバ認証により真正性が担保された中間サーバに接続する。 ・システムの利用者、日時等をシステム上でログとして記録し、7年間保存する。 ・個別業務システム（事務）と中間サーバとの間における特定個人情報の授受に当たっては、その中継のみを行い、システム内に特定個人情報（副本相当）は保有しない。 ・連携サーバから個別業務システム（事務）に提供する照会結果ファイルは、暗号化を行う。 【マイナンバー管理システム】 ・個人番号利用事務にあたる職員を事前に指定する。 ・情報照会に係る操作とマイナンバー管理システムに係る操作は同一の専用端末上で行うため、特定個人情報を外部記録媒体等に書き出すことが無く、漏えい・紛失のリスクに対応している。 ・専用端末は利用する職員ごとにユーザIDを割り当て、ログイン時に認証（多要素認証等）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
【中間サーバ・ソフトウェア】 ①中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 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・プラットフォーム】 ①中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバ・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバ・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバ・プラットフォームの事業者における情報漏えい等のリスクを極小化する。

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	【中間サーバ･プラットフォーム】 ・中間サーバ･プラットフォームをデータセンタに構築し、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。 ・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。 【連携サーバ】 ・サーバ等を設置するための専用施設内に他のシステムとは分離した区画を設け、当該サーバ専用のラックに施錠して収容する。当該施設では、入退室者管理、区画ごとの施錠管理、監視カメラによる録画、有人監視等を実施する。 ・当該施設の煙感知装置、ガス系消火設備、耐震対応等により、火災や地震に起因する滅失等のリスクを低減する。 ・機器のうち、特定個人情報等のデータが記録されうるものの廃棄等に当たっては、磁気的消去又は物理的破壊等により、当該データを復元不可能な状態とする。 【個人番号提出専用キット】 ・収集した書類は施錠保管するよう求めている。委託業務に携わる者以外の者は閲覧できないように委託先に求めている。 ・専用フォームで収集した個人番号情報は委託業務に携わる者以外の者が閲覧できないように委託先に求めている。 【外部記録媒体】 ・収集した特定個人情報をマイナンバー管理システムに移動する場合には、外部記録媒体を活用する。外部記録媒体は施錠保管すると共に、保存するデータは暗号化する。また、使用する際には台帳に使用年月日・使用者等を記録することを委託先に求めている。 ・住民基本台帳ネットワークシステムに提供依頼する対象者データは、外部記録媒体を活用し、移動する。外部記録媒体は施錠保管し、総務局が定める住民基本台帳ネットワークシステムに係る運用規程に基づき暗号化する。 【マイナポータル申請管理】 ・LoGoフォームで収集した個人番号情報は、ぴったりサービス（電子申請等API）を通じてマイナポータル申請管理に連携され、庁内の専用端末（マイナンバー管理システム用端末）でのみ閲覧・取得が可能である。 ・専用端末は庁内の専用の区画に設置する。 【マイナンバー管理システム】 ・マイナンバー管理システムは東京都が構築するクラウドインフラ上に、インターネットや庁内の番号系以外のネットワークと分離して構築する。 ・委託先での廃棄に当たっては、廃棄・消去方法・日時等を記録した報告書の提出を求めている。	

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	【中間サーバ･プラットフォーム】 ・中間サーバ・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ・中間サーバ・プラットフォームでは、ウィ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。 【連携サーバ】 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で稼働する。 ・サーバが接続されたセグメントとそれ以外のセグメントの境界にファイアーウォールを導入するとともに、ログを取得する。 ・ウィルス対策ソフトを導入し、パターンファイルを更新する。 ・基本ソフトウェア（OS）及びミドルウェアは、必要に応じてセキュリティパッチを適用する。 ・データベースにデータを暗号化して保存する。 ・データベースに対する操作権限を細分化し、連携サーバ管理者であっても真に必要な場合を除いてはデータにアクセスできないよう制御する。 ・データベースに対するアクセスログを取得する。 ・データベースのバックアップを取得する。 ・あらかじめ登録された機器だけがネットワークに接続できるよう制御する。 ・サーバ及びその管理に用いる機器は、書き出し可能な外部記録媒体を内蔵せず、かつUSB機器等に対する制御を行い、外部記録媒体の利用を制限する。 【マイナンバー管理システム】 ・マイナンバー管理システムは東京都が構築するクラウドインフラ上に、インターネットや庁内の番号系以外のネットワークと分離して構築する。 ・専用端末からの接続のみとするため、IPアドレスによる制限等により許可していない端末からの通信遮断を行う。	
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	[　　発生あり　　]	＜選択肢＞ 1）発生あり　　2）発生なし

	その内容	①令和3年7月、都のインターンシップ関連イベントに係る告知メールを送信する際、対象者のメールアドレスを、BCC欄ではなく宛先欄に入力して一斉に送信した。 ②令和3年9月、東日本大震災都内避難者向けに作成する「都内避難者の皆様への定期便」の一部について、送付業務の受託者が誤って本人以外の避難者の宛名を記載して発送した。 ③令和3年12月、都営住宅の毎月募集の申込者に対して抽せん番号をお知らせする郵便はがきを発送する際、料金別納で郵便局に持ち込みを完了したつもりであったが、後日、郵便局に確認したところ、持ち込まれたことを示す書類がないことが判明した。申込者に電話で確認したところ、郵便はがきが届いていることを確認できなかったため、申込者の氏名、住所等が記載されたはがきを紛失する事故が発生した。 ④令和4年5月、東京都現代美術館において、ミュージアムショップ運営の受託事業者スタッフが、展覧会図録を予約した顧客へ一斉に案内メールを送信する際、メールアドレスをBCC欄ではなく、宛先欄に入力して発信した。 ⑤令和4年5月、技能検定試験に関する通知を外国人技能実習の複数の監理団体に対してメールで送付する際、誤ってメールアドレスをBCC欄ではなく、CC欄に入力し、一斉送信した。 ⑥令和4年5月、就学支援金事務において、就学支援金の基礎データをCD-Rに情報を保存し、対象高等学校等宛て一斉に送付したところ、そのうち1校に、他校の受給者に関する情報が含まれていることが判明した。 ⑦令和4年5月、受託者が、事業に関するイベントを案内するメールマガジンを送付する際、配信プログラム改修ミスにより、宛先欄に複数のメールアドレスが入力され、送信されてしまった。 ⑧令和4年10月、東京都陽性者登録センターの運営受託者が、医療機関で新型コロナウイルス陽性の診断を受け、センターに登録申請を行った複数の患者への登録完了メールを、送付先アドレスが全て入れ替わったまま送信してしまった。 ⑨令和4年12月、労働力調査の統計調査員に対して連絡事項をメールした際、BCC欄に入力して送るべきところを宛先欄に入力し、一斉送信した。 ⑩令和5年4月、再委託先の派遣会社職員が、業務で使用するシステムを不適切に使用し、個人情報を閲覧、メモにとり自宅に持ち出した。 ⑪令和5年5月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑫令和5年6月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑬令和5年7月、施設を退所する患者に関して、退所先候補の施設と受入調整を行うため、診療関係書類をFAX送信した際、誤って別のFAX番号宛てに送信した。 ⑭令和5年8月、申請により受け付けた申請書が紛失していることが発覚した。 ⑮令和5年9月、関係施設宛に都民情報をFAX送信した際、誤って別の事業者宛てに送信した。 ⑯令和5年9月、事業の対象者に案内チラシを郵送した際、送付対象者の抽出ツールのプログラム仕様の不備により、誤って事業対象外の方に送付したことで、旧住所宛てに送付し返戻されなかったものが誤送付となった。 ⑰令和5年9月、決定通知書に公印を押印する目的で本庁に出張し、押印後持ち帰ったが、発送の準備をしていた際に、通知書1枚が紛失していることが発覚した。 ⑱令和6年1月、患者A宛てに送付すべき利用者情報を、誤ってB宛てに送付した。 ⑲令和6年1月、入所者の診療関係ファイルが紛失していることが発覚し、その後、退所者の荷物の中に当該ファイルが紛れ込んでいたことが発覚した。 ⑳令和6年2月、児童相談所の職員が、出張中に個人情報が記載されている手帳を紛失し、あわせて手帳に収納されていた、当該職員の証票及び所内職員の緊急連絡網を紛失した。 ㉑令和6年2月、施設を退所した患者Aに関する薬剤情報等を記載した書類を、誤って別の患者の退院時荷物に混入させ交付した。 ㉒令和6年2月、オンライン研修で使用した映像において、患者の情報をマスキング処理していたところ、当該映像をスマートフォンで視聴した場合に、マスキングが外れ、個人が特定できる状態になっていたことが判明した。

	再発防止策の内容	①（1）局内全職員に対して情報セキュリティ研修を実施し、二度と同様の事故を起こさないよう、情報セキュリティ対策の確認を徹底する。 （2）外部の複数の宛先に対してメールを送信する場合、「BCC」欄に入力するとともに、送信前に複数の職員によるチェックを徹底する。 ②これまで実施してきた委託事業者への発送完了時の確認のほか、委託事業者職員による宛名、住所の複数チェック等、発送作業での確認作業を確実に実施させるとともに、都においても個人情報を含む情報の適切な取扱いについて、さらなる徹底を図り、再発防止に努める。 ③（1）スケジュールの情報共有と進行管理の徹底 発送に関わる者を含め、課全員が発送スケジュールや作業進捗状況を把握・共有する。また、管理監督職が発送作業の進捗管理を密に行うことで発送遅延や発送漏れを直ちに把握できるようにする。 （2）発送前後の確認体制の見直し 当日発送すべき郵便物が揃っているか、発送を担当している係全体でチェックする。発送担当者は、郵便局からの領収証を運搬業者から受け取った後に、発送物作成担当者に引き渡す。発送物作成担当者は、領収証等に担当課長代理・課長の確認押印を受ける。 （3）紛失リスクの解消 発送予定日前にはがきが納品された場合であっても、その日のうちに郵便局へ持ち込み、はがきを長期間執務室に滞留させないようにする。 ④（1）ミュージアムショップにおいて、本社セキュリティインシデント統括部と連携して、個人情報取り扱い、情報管理体制の改善を行う。 （2）特に複数人へのメール送信に際してはダブルチェックを徹底する。 （3）現代美術館全委託業者に、適切な個人情報等の取扱い及び情報管理を徹底するよう指示する。 （4）財団が管理運営する各施設にも本事案を共有し、個人情報を含む情報の適切な管理を徹底する。 ⑤（1）個人情報の取扱い及び情報管理の徹底等について周知するとともに、職員全員に臨時研修を速やかに実施 （2）誤送信防止に向けたシステムの導入（ダイアログの自動表示など） （3）複数人チェックなど基本的対策の徹底 ⑥チェック機能を再検証し、全日制等と同様の仕組みを通信制にも直ちに導入するほか、事務フローの再構築を行い、再発防止に努める。そのうえで、本件を財団内で広く共有させ、個人情報の取扱い全般についてハード・ソフトの両面から厳しく見直すとともに、職員の意識向上を図っていく。また、都の実施機関においても個人情報の適正管理とサイバーセキュリティー対策について改めて確認を行う。 ⑦（1）システムの改善 メールマガジンの配信は、これまで「TO」により自動で1件ずつ送信がされる仕組みであったが、一括メール送信においては送信者アドレスを全て「BCC」に入れるようシステム改修を行う。 （2）システム会社における確認体制の強化 開発前にシステム会社が実施する、影響調査・テスト内容等について、これまでの2名体制によるダブルチェックから、システム会社のプロジェクトマネージャーも加えることとし、確認した内容を報告させて承認する運用へ見直す。 （3）受託者における確認体制の強化 システム会社のテスト結果の確認にあたっては、テストの証跡情報の提出を求め、内容の確認を行うとともに、受託者での運用テストでは要件定義とも照らした確認を担当だけでなく管理職も実施することにより徹底する。 ⑧受託事業者に対して厳正に指導し、登録完了メール送信作業のチェック体制を強化させる。 ⑨（1）部コンプライアンス推進委員会の臨時開催 ・メール送信時のダブルチェックを徹底させるため、個人情報等の取扱いに係るチェックリストの全職員での点検により注意を喚起、情報管理を再徹底する。 ・あわせて、最近の事故事案の事例を周知するなど、事故の再発予防を進める。 （2）定期的な事故防止意識の醸成 統計調査員を含む全職員を対象に、各所属長や指導員から情報セキュリティや感染拡大防止等に関する指導を定期・継続的に行い、危機意識の醸成等を図る。 ⑩委託先における個人情報の閲覧・使用に当たっての権限の設定や、不適切な閲覧・使用・持ち出しを防止するための体制についてあらためて確認し、適切な運用を徹底させる。 ⑪（1）情報共有をしているホワイトボードの位置、記入欄が分かりにくいとの意見が出たため、位置、記入方法について変更した。 （2）書類封入時のチェック手順中に、患者氏名の確認を明示した。 （3）2者確認を徹底するため、事務員のみでなく看護職員もチェックを行うこととし、2者チェックが終わった段階で封書のチェックボックスに記載する。 （4）責任の所在を明確にするため「転院時退所セット確認書」を新たに作成し、チェックを行った職員が記名する。 ⑫（1）チェックリストを活用し、複数人、複数回のチェックを行うとともに、最終チェック者を統括責任者とすることで、誤封入等を防ぐ体制を整える。 （2）都職員が施設へ直接出向き、個人情報管理の実態確認を実施するとともに、対応が不十分な場合は是正指導を行う。 （3）個人情報保護の研修を実施し、施設全体で個人情報保護の取り組み状況を共有した上で、改善を徹底する。 ⑬（1）委託先に対し、個人情報に関する業務手順を見直し及び徹底を図ることや、全従事者に対する個人情報保護研修を行うことを指導した。また、改善策の確認のため、都が施設へ出向き、個人情報管理の実態を確認した。 （2）再委託先において、送付の際は、まずFAX以外の手段を調整し、止むを得ずFAXを使用する際には、FAX番号の聞き取りの際の復唱や、FAX送信前の送信先への番号の再確認、複数人で複数回のチェックを必ず行うこととした。また、全従業者に対する個人情報保護研修を行った。 ⑭（1）作業環境等を見直し、書類の混入等が起きにくい環境を整備 ①執務室内の作業スペースの確保及び活用 ②引き出し付きの棚をキャビネット内に新設し、書類の分類をよりしやすくした。 （2）委託業者との書類の受け渡し方法の変更（送付する判定機関ごとに数を確認しながら受け渡す）。 ⑮個人情報をFAX送信することを禁止するよう各施設に通知した。 ⑯抽出ツールのプログラム確認は、委託先事業者の運用チームのみが行っていたが、抽出ツールを作成・利用する際には、運用チームに加えて、開発チームと委託元である都の3者で抽出ツールのプログラムの仕様・設定を確認することとした。 ⑰個人情報の持出、返却確認及び受け渡しの際の確認の徹底を行う。また、作業工程等を点検し、作業方法やチェック方法等ミスが起きにくい方法を検討、実施する。 ⑱郵便の発送作業は複数職員でチェックすることを再徹底。また、特に慎重を要する個人情報を取り扱う施設における個人情報の事故の重大性について改めて周知するとともに、書類の発送、保管、業務の進行管理等について、注意喚起や指導を行った。

		⑲(1)ファイルが他の物に紛れてしまわないよう、目立つ色に変更する。 (2)作業スペースに仕切りを立てて、使用スペースを物理的に限定する。 (3)ファイルに記載する名前をイニシャルに表記変更する等、使用する情報から個人情報を削除する。 (4)決まった時間に決まった人員が所在を確認する。 (5)チェックの時間を定刻とし、声をかけ合う。 (6)出したらしまうといった基本的事項を、改めて徹底するよう、注意喚起する。 (7)急いでいたり、忙しい時間帯でも、ダブルチェックをするよう、改めて徹底する。また、退所時にも荷物を確認してから渡すようにする ⑳(個人情報の管理について) (1) 相談援助業務上の記録をノート等に記載する場合は、イニシャルを使用するなど個人情報を特定されないようにすること。また、私物のノートや手帳に個人情報を記載しないこと。 (2) 庁舎外での会議等に出席した際には、個人端末を活用して記録の作成を行うとともに、作成した文書は暗号化し保存すること。 (3) 業務上やむを得ず個人情報が記録された書類を庁舎外に持ち出す場合は、局の保有個人情報安全管理基準に基づき管理職の許可を得ること。 (4) 個人情報を含む書類を持ち出すにあたっては、盗難や紛失を防止できる形状・機能を持つ鞄に収納し、肌身離さず持ち運ぶなど十分に注意すること。 (5) その他個人情報の取り扱いについては、局の保有個人情報安全管理基準等を遵守し、適正に行うこと。 (職員の証票の管理について) (1) 月1回、各職員の保有状況を点検すること (2) 携行する際には、ストラップ付きのケースに収納するなど、常に身体から離さずに携行することを徹底すること (職員の緊急連絡網の管理について) (1) 必要な連絡先は公用携帯に保存し、連絡網を記載した紙は庁舎外に持ち出さないこと。 ㉑ (1)入所時や退所時の手順確認のチェックリスト様式を変更し、入所時の写真撮影やリストへの正確な情報記載、退所時の荷物確認の手順など守るべきルールを追記するとともに、実施者を記載する欄を追加。 (2)個人情報紛失判明時の、本部への速やかな報告や具体的な捜索の手順などを、チェックリストに追記。 (3)毎朝のミーティングにてリーダー看護師等に個人情報保護の重要性やルールの順守を徹底。勤務者には、業務実施前に最新のマニュアルを確認するよう指導。 ㉒(1)発表資料の事前確認の徹底について幹部会で決定し、各部署に注意喚起 (2)録画や写真撮影をして保管していない旨を書面で確認 (3)画像等の個人情報の収集・利用に関する同意手続きの見直し
⑩死者の個人番号		[保管している] ＜選択肢＞ 1) 保管している 2) 保管していない
	具体的な保管方法	生存者の個人番号と同様の方法にて安全管理措置を実施している。
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	【マイナンバー管理システム】 ・特定個人情報に変更があった場合、都営住宅入居者又は入居申込者が東京都に対して届出申請を行う。 ・届出申請内容から、職員にて都営住宅マイナンバー管理システムの情報を更新する。 ・マイナンバー管理システムに、入手した特定個人情報を反映する際に、システムで管理している情報と相違がある場合は、エラーとして検知する。エラーとなった場合当該対象者に届出申請を促す。 ・特定個人情報に変更があった場合、届出申請が必要であることを都営住宅入居者又は入居申込者に対して周知する。	
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	【連携サーバ】 ・個別業務システム（事務）及び中間サーバとの間で授受されるデータは、所要の処理完了後又は一定時間経過後に削除される。 ・機器のうち、特定個人情報等のデータが記録されうるものの廃棄等に当たっては、磁気的消去又は物理的破壊等により、当該データを復元不可能な状態とする。 【個人番号提出専用キット】 ・指定した期間を経過した書類については、委託業者において、個人情報の取扱いに留意し、情報漏えい防止対策を講じて、最終的に破砕又は溶解処分し、廃棄完了後は都に証明書を提出するよう求めている。 ・保存期間を経過した申請データは、復元不可能な状態とするよう求めている。 【外部記録媒体】 ・外部記録媒体を用いて特定個人情報を移動した場合、移動完了後直ちに、外部記録媒体に保存された特定個人情報等のデータは、論理削除を行う。外部記録媒体の廃棄に当たっては、物理的破壊等により当該データを復元不可能な状態とする。 【マイナポータル申請管理】 ・申請データは一定期間経過後に削除される。 【マイナンバー管理システム】 ・特定個人情報が不要となり、保有する必要がないと判断したものについては消去を行う。 ・バッチ処理により削除する。	
その他の措置の内容	－	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 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	【東京都における取組】 ・個人情報保護については、全職員が職員向けの自己点検表を用いてチェックを実施する。情報セキュリティについては、情報システム管理者の指示により、情報システム担当者及び利用者は、1年に一度以上、本システムに係る自己点検を実施する。 【中間サーバ・プラットフォーム】 ・運用規則等に基づき、中間サーバ・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。	
②監査	[　　十分に行っている　　]	＜選択肢＞ 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	【東京都における取組】 ・内部監査人により、特定個人情報等の管理状況について定期的に監査を行っている。 ・外部監査人により、システムのセキュリティの脆弱性の有無等について定期的に監査を行っている。 【中間サーバ・プラットフォーム】 ・運用規則等に基づき、中間サーバ・プラットフォームについて、定期的に監査を行うこととしている。	

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（非常勤含む。）】 ・職員を対象に、個人情報保護の重要性及び適正管理等に関する理解を深め、個人情報保護の遵守を徹底することを目的に、サイバーセキュリティ・個人情報保護の以下の研修を実施している。 ・個人端末からアクセスするeラーニング研修（理解度が基準に達しないと修了できない） ・新規採用職員を対象とした研修 ・一般職員、管理職を対象とした研修（3年に1回受講） ・未受講者については、翌年度同様の研修を受講させている。また、eラーニングについては、システムにより受講管理を実施し、未受講者に受講を促すことで、未受講者が出ないようにしている。 【委託先】 ・業務受託に当たり、従業者に対して、個人情報の取扱いルールを遵守すべきことを確認させている。 【中間サーバ・プラットフォーム】 ・IPA（情報処理推進機構）が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資材を作成し、中間サーバ・プラットフォームの運用に携わる職員及び事業者に対し、運用規則（接続運用規程等）や情報セキュリティに関する教育を年次（年2回）及び随時（新規要員着任時）実施することとしている。	

3. その他のリスク対策

【東京都における取組】
・特定個人情報の収集や審査への活用時には、当該事務の責任者がその適切な運用について管理監督することとしている。
・万が一、特定個人情報の漏えい等が発生した際には、個人情報の保護に関する法律に基づき適切な報告等を行うこととしている。

【中間サーバー・プラットフォーム】
・中間サーバー・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用、監視を実現する。

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	東京都住宅政策本部都営住宅経営部指導管理課指導調整担当 〒163-8001　東京都新宿区西新宿2-8-1　都庁第二本庁舎13階北側 電話：03-5320-4981
②請求方法	規則で定める様式による書面の提出により開示・訂正・利用停止請求を受け付ける。
特記事項	請求方法、様式等について東京都公式ホームページ上で分かりやすく表示。
③手数料等	[　　有料　　]　＜選択肢＞ 1) 有料　2) 無料 （手数料額、納付方法：　現金等により、実費相当分の手数料を納付する。　）
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	都営住宅等への申込者及び入居予定者情報ファイル、都営住宅等の入居許可を受けた方の情報ファイル
公表場所	東京都総務局総務部情報公開課
⑤法令による特別の手続	－
⑥個人情報ファイル簿への不記載等	－
2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	東京都住宅政策本部都営住宅経営部指導管理課指導調整担当 〒163-8001　東京都新宿区西新宿2-8-1　都庁第二本庁舎13階北側 電話：03-5320-4981
②対応方法	問合せを受け付けた際は、対応について記録を残す。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	
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	
②実施日・期間	
③期間を短縮する特段の理由	
④主な意見の内容	
⑤評価書への反映	
3. 第三者点検	
①実施日	
②方法	
③結果	
4. 個人情報保護委員会の承認 【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

（別添3）変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明