

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	住民基本台帳ネットワークに関する事務 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、住民基本台帳ネットワークに関する事務において個人番号を利用するにあたり、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んでいることを宣言する。

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12月13日

項目一覧

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

I 基本情報

1. 特定個人情報ファイルを取り扱う事務

①事務の名称	住民基本台帳ネットワークに関する事務		
②事務の内容 ※	住民基本台帳ネットワークに関する事務は、「1. 本人確認情報の管理及び提供等に関する事務」及び「2. 附票本人確認情報の管理及び提供等に関する事務」に分かれる。 1. 本人確認情報の管理及び提供等に関する事務 都道府県は、住民基本台帳法(以下「住基法」という。)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(住基ネット)を市町村と共同して構築している。 なお、住民基本台帳は、住基法に基づき作成されるものであり、市町村における住民の届出に関する制度及びその住民たる地位を記録する各種の台帳に関する制度を一元化し、もって、住民の利便を増進するとともに行政の近代化に対処するため、住民に関する記録を正確かつ統一に行うものであり、市町村において、住民の居住関係の公証、選挙人名簿の登録、その他住民に関する事務の処理の基礎となるものである。 具体的に東京都では、住基法及び「住民サービスの向上と行政事務の効率化を図るために住民基本台帳ネットワークシステムの本人確認情報を利用する事務等を定める条例」(以下「都条例」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磁気ディスクによる特定個人情報ファイルの管理 ②区市町村からの本人確認情報に係る変更の通知に基づく特定個人情報ファイルの更新及び機構への通知 ③都知事から本人確認情報に係る東京都の他の執行機関への提供又は他部署への移転 ④住民による請求に基づく当該個人の本人確認情報の開示並びに開示結果に基づく住民からの本人確認情報の訂正、追加又は削除の申出に対する調査 ⑤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 2. 附票本人確認情報の管理及び提供等に関する事務 都道府県は、市町村における市町村コミュニケーションサーバ(以下「CS」という。)、都道府県における附票都道府県サーバ及び機構における附票全国サーバ等により構成される「附票連携システム」において、国外転出者に係る本人確認を行うための社会的基盤としての役割を担うため、4情報(氏名、住所、生年月日、性別)、住民票コード及びこれらの変更情報で構成される「都道府県知事保存附票本人確認情報ファイル」を作成し、戸籍の附票に関する記録を正確に行う責務がある。そのため、附票本人確認情報の管理及び提供等に係る以下の事務を実施する。なお、都道府県知事保存附票本人確認情報(以下条文に併せて記載する場合は、「都道府県知事保存附票本人確認情報」とし、それ以外の記載は、「附票本人確認情報」とする。)には、個人番号は含まれない。 ①磁気ディスクによる特定個人情報ファイルの管理 ②区市町村からの附票本人確認情報に係る変更の通知に基づく特定個人情報ファイルの更新及び機構への通知 ③都知事から附票本人確認情報に係る東京都の他の執行機関への提供又は他部署への移転 ④住民による請求に基づく当該個人の附票本人確認情報の開示並びに開示結果に基づく住民からの附票本人確認情報の訂正、追加又は削除の申出に対する調査 ⑤機構への附票本人確認情報の照会		
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	住民基本台帳ネットワークシステム ※「3. 特定個人情報ファイル名」に示す「都道府県知事保存本人確認情報ファイル」は、住民基本台帳ネットワークシステムの構成要素のうち、都道府県サーバにおいて管理がなされているため、以降は、住民基本台帳ネットワークシステムの内の東京都サーバ部分について記載する。
②システムの機能	1. 本人確認情報の更新 ：都道府県知事保存本人確認情報ファイルを最新の状態に保つため、区市町村CSを経由して通知された本人確認情報の更新情報を元に当該ファイルを更新し、全国サーバに対して当該本人確認情報の更新情報を通知する。 2. 東京都の他の執行機関への情報提供又は他部署への移転 ：東京都の他の執行機関又は他部署による住基法に基づく情報照会に対応するため、照会のあった当該個人の個人番号又は4情報（氏名、住所、性別、生年月日）等に対応する本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、照会元を提供・移転する。 3. 本人確認情報の開示 ：法律に基づく住民による自己の本人確認情報の開示請求に対応するため、当該個人の本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、帳票に出力する。 4. 機構への情報照会 ：全国サーバに対して住民票コード、個人番号又は4情報の組合せをキーとした本人確認情報照会要求を行い、該当する個人の本人確認情報を受領する。 5. 本人確認情報検索 ：東京都サーバの代表端末又は業務端末において入力された4情報の組合せをキーに都道府県知事保存本人確認情報ファイルを探索し、探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。 6. 本人確認情報整合 ：都道府県知事保存本人確認情報ファイルの正確性を担保するため、区市町村から本人確認情報を受領し、当該本人確認情報を用いて当該ファイルに記録された本人確認情報の整合性確認を行う。
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 （)
システム2～5	

システム2～5

システム2									
①システムの名称	附票連携システム ※「3. 特定個人情報ファイル名」に示す「都道府県知事保存附票本人確認情報ファイル」は、住民基本台帳ネットワークシステムの構成要素のうち、附票都道府県サーバにおいて管理がなされているため、以降は、附票連携システムの内の附票東京都サーバ部分について記載する。								
②システムの機能	1. 附票本人確認情報の更新 : 都道府県知事保存附票本人確認情報ファイルを最新の状態に保つため、区市町村CSを経由して通知された附票本人確認情報の更新情報を元に当該ファイルを更新し、附票全国サーバに対して当該附票本人確認情報の更新情報を通知する。 2. 東京都の他の執行機関への情報提供又は他部署への移転 : 東京都の他の執行機関又は他部署による住基法に基づく情報照会に対応するため、照会のあった当該個人の4情報(氏名、住所、性別、生年月日)等に対応する附票本人確認情報を都道府県知事保存附票本人確認情報ファイルから抽出し、照会元に提供・移転する。 その際、番号法で認められた場合に限り、東京都の他の執行機関又は他部署からの求めに応じ、附票本人確認情報の提供・移転に併せて当該個人の住民票コードを用いて、都道府県知事保存本人確認情報ファイルから個人番号を抽出し、照会元に提供・移転する場合がある。 3. 附票本人確認情報の開示 : 法律に基づく住民による自己の附票本人確認情報の開示請求に対応するため、当該個人の附票本人確認情報を都道府県知事保存附票本人確認情報ファイルから抽出し、帳票に出力する。 4. 機構への情報照会 : 附票全国サーバに対して住民票コード又は4情報の組合せをキーとした附票本人確認情報照会要求を行い、該当する個人の附票本人確認情報を受領する。 5. 附票本人確認情報検索 : 附票東京都サーバの代表端末又は業務端末(都道府県サーバと共用する。)において入力された4情報の組合せをキーに都道府県知事保存附票本人確認情報ファイルを検索し、検索条件に該当する附票本人確認情報の一覧を画面上に表示する。 6. 附票本人確認情報整合 : 都道府県知事保存附票本人確認情報ファイルの正確性を担保するため、区市町村から附票本人確認情報を受領し、当該附票本人確認情報を用いて当該ファイルに記録された附票本人確認情報の整合性確認を行う。								
③他のシステムとの接続	<table border="0"> <tr> <td>☐ 情報提供ネットワークシステム</td><td>☐ 庁内連携システム</td></tr> <tr> <td>☐ 住民基本台帳ネットワークシステム</td><td>☐ 既存住民基本台帳システム</td></tr> <tr> <td>☐ 宛名システム等</td><td>☐ 税務システム</td></tr> <tr> <td>☐ その他 (</td><td>)</td></tr> </table>	☐ 情報提供ネットワークシステム	☐ 庁内連携システム	☐ 住民基本台帳ネットワークシステム	☐ 既存住民基本台帳システム	☐ 宛名システム等	☐ 税務システム	☐ その他 (	)
☐ 情報提供ネットワークシステム	☐ 庁内連携システム								
☐ 住民基本台帳ネットワークシステム	☐ 既存住民基本台帳システム								
☐ 宛名システム等	☐ 税務システム								
☐ その他 (	)								
システム6～10									
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)都道府県知事保存本人確認情報ファイル (2)都道府県知事保存附票本人確認情報ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	(1)都道府県知事保存本人確認情報ファイル 東京都では、都道府県知事保存本人確認情報ファイルを、下記に記載の通りの必要性から取り扱う。 ・都道府県知事保存本人確認情報ファイルは、転出入があった場合等にスムーズな住民情報の処理を行うため、また全国的な本人確認手段として、1つの市町村内にとどまらず、全地方公共団体で、本人確認情報を正確かつ統一的に記録・管理することを目的として、以下の用途に用いられる。 ①住基ネットを用いて区市町村の区域を越えた住民基本台帳に関する事務（住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務）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区市町村からの本人確認情報の更新情報の通知を受けて都道府県知事保存本人確認情報ファイルを更新し、当該更新情報を機構に対して通知する。 ③東京都の他の執行機関又は他部署からの照会に基づき、本人確認情報を提供・移転する。 ④住民からの請求に基づき、当該個人の本人確認情報を開示する。 ⑤住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務において、本人確認情報を検索する。 ⑥区市町村において保存する本人確認情報との整合性を確認する。 (2)都道府県知事保存附票本人確認情報ファイル 東京都では、都道府県知事保存附票本人確認情報ファイルを、下記に記載の通りの必要性から取り扱う。 ・都道府県知事保存附票本人確認情報ファイルは、国外転出者に係る本人確認手段として、1つの市町村内にとどまらず、全地方公共団体で、附票本人確認情報を正確かつ統一的に記録・管理することを目的として、以下の用途に用いられる。 ①附票連携システムに係る附票本人確認情報の管理及び提供等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附票本人確認情報を管理する。 ②区市町村からの附票本人確認情報の更新情報の通知を受けて都道府県知事保存附票本人確認情報ファイルを更新し、当該更新情報を機構に対して通知する。 ③東京都の他の執行機関又は他部署からの照会に基づき、附票本人確認情報を提供・移転する。その際、番号法で認められた場合に限り、東京都の他の執行機関又は他部署からの求めに応じ、附票本人確認情報の提供・移転に併せて当該個人の住民票コードを用いて、都道府県知事保存本人確認情報ファイルから個人番号を抽出し、照会元に提供・移転する場合がある。 ④住民からの請求に基づき、当該個人の附票本人確認情報を開示する。 ⑤附票本人確認情報の管理及び提供等に関する事務において、附票本人確認情報を検索する。 ⑥区市町村において保存する附票本人確認情報との整合性を確認する。
②実現が期待されるメリット	住民票の写し等にかえて本人確認情報を利用することにより、これまでに窓口で提出が求められていた行政機関が発行する添付書類(住民票の写し等)の省略が図られ、もって国民／住民の負担軽減(各機関を訪問し、証明書等を入手する金銭的、時間的コストの節約)につながることが見込まれる。また、国外転出者を含め個人番号カードによる本人確認、個人番号の真正性確認が可能となり、行政事務の効率化に資することが期待される。

5. 個人番号の利用 ※		
法令上の根拠	住民基本台帳法(昭和42年7月25日法律第81号) ・第7条(住民票の記載事項) ・第12条の5(住民基本台帳の脱漏等に関する都道府県知事の通報) ・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7(都道府県知事から機構への本人確認情報の通知等) ・第30条の8(本人確認情報の誤りに関する機構の通報) ・第30条の11(通知都道府県以外の都道府県の執行機関への本人確認情報の提供) ・第30条の13(都道府県の条例による本人確認情報の提供) ・第30条の15(本人確認情報の利用) ・第30条の22(市町村間の連絡調整等) ・第30条の32(自己の本人確認情報の開示) ・第30条の35(自己の本人確認情報の訂正) ・第30条の44の6第3項(都道府県知事保存附票本人確認情報(住民票コードに限る。)の利用)	
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	[実施しない]	<選択肢> 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	—	
7. 評価実施機関における担当部署		
①部署	総務局行政部振興企画課	
②所属長の役職名	振興調整担当課長	
8. 他の評価実施機関		
—		

(別添1) 事務の内容

別紙のとおり

(備考)

別紙のとおり

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) 都道府県知事保存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	[1,000万人以上]	＜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 ※	東京都民 (東京都内のいずれかの区市町村において、住基法第5条(住民基本台帳の備付け)に基づき住民基本台帳に記録された住民を指す。) ※住民基本台帳に記録されていた者で、転出等の事由により住民票が消除(死亡による消除を除く。)された者(以下「消除者」という。)を含む。	
	その必要性	住基ネット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(都道府県知事保存本人確認情報ファイル)において東京都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。
④記録される項目	[10項目以上50項目未満]	＜選択肢＞ 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
	主な記録項目 ※	・識別情報 [○] 個人番号 [] 個人番号対応符号 [] その他識別情報(内部番号) ・連絡先等情報 [○] 4情報(氏名、性別、生年月日、住所) [] 連絡先(電話番号等) [○] その他住民票関係情報 ・業務関係情報 [] 国税関係情報 [] 地方税関係情報 [] 健康・医療関係情報 [] 医療保険関係情報 [] 児童福祉・子育て関係情報 [] 障害者福祉関係情報 [] 生活保護・社会福祉関係情報 [] 介護・高齢者福祉関係情報 [] 雇用・労働関係情報 [] 年金関係情報 [] 学校・教育関係情報 [] 災害関係情報 [] その他 ()
	その妥当性	・個人番号、4情報、その他住民票関係情報 :住基ネットを通じて本人確認を行うために必要な情報として、住民票の記載等に係る本人確認情報(個人番号、4情報、住民票コード及びこれらの変更情報)を記録する必要がある。
	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	総務局行政部振興企画課	

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 () ☐ 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 (東京都内の区市町村) ☐ 民間事業者 () ☐ その他 ()	
②入手方法		☐ 紙 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ フラッシュメモリ ☐ 電子メール ☐ 専用線 ☐ 庁内連携システム ☐ 情報提供ネットワークシステム ☒ その他 (区市町村CSを通じて入手する。)	
③入手の時期・頻度		住民基本台帳の記載事項において、本人確認情報に係る変更又は新規作成が発生した都度入手する。	
④入手に係る妥当性		住民に関する情報に変更があった又は新規作成された際は、区市町村がそれをまず探知した上で、全国的なシステムである住基ネットで管理する必要があるため、区市町村から東京都へ、東京都から機構へと通知がなされることとされているため。	
⑤本人への明示		都道府県知事が当該区市町村の区域内の住民の本人確認情報を入手することについて、住基法第30条の6(市町村長から都道府県知事への本人確認情報の通知等)に明示されている。	
⑥使用目的 ※		住基ネットを通じて全国共通の本人確認を行うため、本特定個人情報ファイル(都道府県知事保存本人確認情報ファイル)において東京都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 ※	総務局行政部振興企画課・庁内利用部署	
	使用者数	[1,000人以上] <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 ※		・市町村長からの住民票の記載事項の変更又は新規作成の通知を受け(既存住基システム→区市町村CS→東京都県サーバ)、都道府県知事保存本人確認情報ファイルを更新し、機構に対して当該本人確認情報の更新情報を通知する(東京都サーバ→全国サーバ)。 ・東京都の他の執行機関又は他部署からの本人確認情報の照会要求を受け(東京都の他の執行機関又は他部署→東京都サーバ)、照会のあった住民票コード、個人番号又は4情報の組合せを元に都道府県知事保存本人確認情報ファイルを検索し、該当する本人確認情報を照会元へ提供・移転する(東京都サーバ→東京都の他の執行機関又は他部署)。 ・住民からの開示請求に基づき(住民→東京都窓口→東京都サーバ)、当該住民の本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、書面により提供する(東京都サーバ→帳票出力→住民)。 ・4情報(氏名、住所、性別、生年月日)の組合せをキーに都道府県知事保存本人確認情報ファイルの検索を行う。 ・都道府県知事保存本人確認情報ファイルの正確性を担保するため、区市町村から本人確認情報を受領し(区市町村CS→東京都サーバ)、当該本人確認情報を用いて都道府県知事保存本人確認情報ファイルに記録された本人確認情報について、整合性確認を行う。	
情報の突合 ※		・都道府県知事保存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都道府県知事保存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。 ・東京都の他の執行機関又は他部署からの照会に基づいて本人確認情報を提供・移転する際に、照会元から受信した対象者の4情報等との突合を行う。 ・請求に基づいて本人確認情報を開示する際に、開示請求者から受領した本人確認情報との突合を行う。 ・区市町村CSとの整合処理を実施するため、4情報等との突合を行う。	

	情報の統計分析 ※	住基法第30条の15第1項第4号(本人確認情報の利用)の規定に基づいて統計資料の作成を行う場合、情報の統計分析を行うことがある。 また、本人確認情報の更新件数や提供件数等の集計を行う。
	権利利益に影響を 与え得る決定 ※	なし
⑨使用開始日		平成27年6月1日

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 (3) 件 ☐ 移転を行っている (1) 件 ☐ 行っていない
提供先1	地方公共団体情報システム機構(機構)
①法令上の根拠	住基法第30条の7(都道府県知事から機構への本人確認情報の通知等)
②提供先における用途	都道府県知事より受領した本人確認情報を元に機構保存本人確認情報ファイルを更新する。
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	[1,000万人以上] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 (住民基本台帳ネットワークシステム) ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	区市町村長からの通知に基づいて都道府県知事保存本人確認情報ファイルの更新を行った都度、随時。
提供先2～5	
提供先2	東京都の他の執行機関(下水道局、水道局、警視庁、東京消防庁、東京都教育委員会)
①法令上の根拠	住基法第30条の15第2項(本人確認情報の利用) 住民サービスの向上と行政事務の効率化を図るために住民基本台帳ネットワークシステムの本人確認情報を利用する事務等を定める条例 但し、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第九条第一項又は第二項の規定により提供先が個人番号を利用することができる場合に限る。
②提供先における用途	住基法別表第6に掲げる、東京都の他の執行機関への情報提供が認められる事務(例:教育委員会における特別支援学校への就学のため必要な経費の支弁に関する事務等)の処理及び都条例に定める事務(例:東京都恩給条例による年金である給付の支給に関する事務)の処理に用いる。
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 ※住民票コードについては、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施行に伴う関係法律の整備等に関する法律(平成25年5月31日法律第28号)第22条第7項に基づく経過措置である。
④提供する情報の対象となる本人の数	[1,000万人以上] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 (住民基本台帳ネットワークシステム) ☐ 専用線 ☒ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	東京都の他の執行機関からの情報照会の要求があった都度、随時。

提供先3	住基法上の住民
①法令上の根拠	住基法第30条の32(自己の本人確認情報の開示)
②提供先における用途	開示された情報を確認し、必要に応じてその内容の全部又は一部の訂正、追加又は削除の申出を行う。
③提供する情報	住民票コード、氏名、住所、生年月日、性別、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	[1,000万人以上] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上
⑥提供方法	[] 情報提供ネットワークシステム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [○] 紙 [] その他 ()
⑦時期・頻度	開示請求があった都度、随時。
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	東京都の他部署(総務局(総務部、人事部)、主税局(税制部、課税部、資産税部、徴収部、都税事務所、都税総合事務センター)、生活文化スポーツ局(都民生活部、私学部)、保健医療局(医療政策部、保健政策部)、福祉局(生活福祉部、子供・子育て支援部、障害者施策推進部)、産業労働局(商工部、観光部)等)
①法令上の根拠	住基法第30条の15第1項(本人確認情報の利用) 住民サービスの向上と行政事務の効率化を図るために住民基本台帳ネットワークシステムの本人確認情報を利用する事務等を定める条例 但し、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第9条第1項又は第2項の規定により移転先が個人番号を利用することができる場合に限る。
②移転先における用途	住基法別表第5に掲げる、都道府県知事において都道府県知事保存本人確認情報の利用が認められた事務の処理に用いる。
③移転する情報	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 ※住民票コードについては、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施行に伴う関係法律の整備等に関する法律(平成25年5月31日法律第28号)第22条第7項に基づく経過措置である。
④移転する情報の対象となる本人の数	[1,000万人以上] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上
⑥移転方法	[] 庁内連携システム [] 専用線 [] 電子メール [○] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [○] その他 (住民基本台帳ネットワークシステム)
⑦時期・頻度	東京都の他部署からの検索要求があった都度、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 ※		【東京都サーバ】 セキュリティゲートにて入退館管理をしている都道府県サーバの集約センターにおいて、施錠管理及び入退室管理（監視カメラを設置してサーバ設置場所への入退室者を特定・管理）を行っている部屋に設置したサーバ内に保管する。サーバへのアクセスはIDと生体認証（又はパスワード）による認証が必要となる。 【電子記録媒体】 総務局行政部から貸与する指定のDVD－RWに暗号化の上格納し、施錠が出来る金庫等に保管する。 【紙】 各所属において、施錠が出来る金庫等に保管する。
②保管期間	期間	＜選択肢＞ 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない
	その妥当性	【東京都サーバ】 9) 20年以上 ・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）及び削除者の本人確認情報は、住基法施行令第30条の6（都道府県における本人確認情報の保存期間）に定める期間（150年間）保管する。 【電子記録媒体】 1) 1年未満 データの受け渡し又は利用が終了した場合、速やかにデータを消去する。 【紙】 10) 定められていない 利用事務での文書保存期間終了後又は各所属で利用が終了した場合、速やかに廃棄する。
③消去方法		【東京都サーバ】 都道府県知事保存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、復元できないように消去する仕組みになっている。 東京都サーバのハードディスク等は地方公共団体情報システム機構により、物理的に利用できなくなつた上、廃棄される。 【電子記録媒体】 総務局行政部から貸与する指定のDVD－RWのみ使用を認めており、書き込みができなくなったり、不要となった媒体については、総務局行政部にて回収の上、物理的に破壊し、廃棄記録をつけている。 【紙】 シュレッダー又は溶解処分により確実に廃棄を行っている。
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) 都道府県知事保存附票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	[1,000万人以上] <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 ※	東京都内のいずれかの区市町村において、住基法第16条(戸籍の附票の作成)に基づき戸籍の附票に記録された住民を指す。 ※消除者を含む。
その必要性	本特定個人情報ファイル(都道府県知事保存附票本人確認情報ファイル)において東京都内の戸籍の附票に記録された全ての住民の情報を保有し、その記録を常に正確に更新・管理・提供・移転する必要がある。
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 (その他戸籍の附票関係情報(戸籍の表示に係る情報は含まない。))
その妥当性	・4情報、その他戸籍の附票関係情報(戸籍の表示に係る情報は含まない。) :法令に基づき戸籍の附票に記録された者に関する記録を正確に行う上で、戸籍の附票の記載等に係る附票本人確認情報(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。なお、別添2に記載のとおり、記録項目には戸籍の表示に係る情報(本籍及び筆頭者の氏名)は含まない。 ・個人番号 :国外転出者に係る事務処理に関し、番号法で認められた場合に限り、東京都他の執行機関等からの求めに応じ、当該個人の住民票コードを用いて、都道府県知事保存本人確認情報ファイルから個人番号を抽出し、附票東京都サーバに連携する場合がある。提供又は移転後、個人番号は、都道府県知事保存附票本人確認情報ファイルに保有することはない。
全ての記録項目	別添2を参照。
⑤保有開始日	令和6年5月27日
⑥事務担当部署	総務局行政部振興企画課

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 () ☐ 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 (東京都内の区市町村) ☐ 民間事業者 () ☒ その他 (東京都サーバ(※入手には該当しないが、東京都サーバから個人番号を抽出する場合がある))
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 ()
③入手の時期・頻度		戸籍の附票において、附票本人確認情報の変更又は新規作成(出生等)が発生した都度入手する。 ※番号法別表に掲げる事務につき、東京都の他の執行機関等から国外転出者に係るものに関し求めがあった場合、個人番号をその都度抽出する場合がある。
④入手に係る妥当性		法令に基づき、住民の利便の増進と国及び地方公共団体の行政の合理化に資するため、国外転出者に係る本人確認を行う上で、区市町村の戸籍の附票の記載事項に変更が生じた都度、当該区市町村を通じて入手し、機構に通知する必要がある。 また、入手の手段として、法令に基づき構築された専用回線である、住基ネット(※※)を用いることで、入手に係るリスクを軽減している。 ※なお、住基法第30条の44の6第3項に基づき、都道府県知事保存附票本人確認情報(住民票コードに限る。)を利用し、第30条の15第1項又は第2項の規定による事務について個人番号を提供することができるとされている。 ※※附票連携システムは、住基ネットを利用して構築されている。住基ネットは、保有情報・利用の制限、内部の不正利用の防止、外部からの侵入防止など、セキュリティ確保のための様々な措置が講じられており、平成14年8月5日の稼働後、住基ネットへのハッキングや情報漏えいなどの事件や障害は一度も発生していない。
⑤本人への明示		都道府県知事が当該区市町村の区域内における附票本人確認情報を入手することについて、住基法第30条の41(市町村長から都道府県知事への附票本人確認情報の通知等)に明示されている。 ※都道府県知事が国外転出者に係る個人番号を抽出する場合があることについて、住基法第30条の44の6第3項に明示されている。
⑥使用目的 ※		本特定個人情報ファイル(都道府県知事保存附票本人確認情報ファイル)において区域内の戸籍の附票に記載された全ての者の情報を保有し、その記録を常に正確に更新・管理・提供・移転する。 ※番号法別表に掲げる事務につき、東京都の他の執行機関等から国外転出者に係るものに関し求めがあった場合、個人番号をその都度抽出し、第30条の15第1項又は第2項の規定による事務について提供する場合がある。
変更の妥当性		—
⑦使用の主体	使用部署 ※	総務局行政部振興企画課
	使用者数	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

⑧使用方法 ※		・東京都の他の執行機関又は他部署からの附票本人確認情報の照会要求を受け(東京都の他の執行機関又は他部署→附票東京都サーバ)、照会のあった住民票コード又は4情報の組合せを元に都道府県知事保存附票本人確認情報ファイルを検索し、該当する個人の附票本人確認情報を照会元へ提供・移転する(附票東京都サーバ→東京都の他の執行機関又は他部署)。 ※その際、番号法で認められた場合に限り、附票本人確認情報の提供に併せて、当該個人の住民票コードを用いて都道府県知事保存本人確認情報ファイルから個人番号を抽出し、照会元に提供・移転する場合がある。
	情報の突合 ※	・都道府県知事保存附票本人確認情報ファイルの住民票コードと道府県知事保存本人確認情報ファイルの個人番号を突合する。
	情報の統計分析 ※	なし
	権利利益に影響を与え得る決定 ※	なし
⑨使用開始日		令和6年5月27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	附票東京都サーバの運用及び監視に関する業務	
①委託内容	全国の都道府県サーバを1拠点(集約センター)に集約化することとしたことに伴い、東京都サーバと同様に附票東京都サーバの運用及び監視に関する業務を、集約センター運用者に委託する。 委託する業務は、直接附票本人確認情報に係わらない(直接附票本人確認情報にアクセスできず、閲覧・更新・削除等を行わない)業務を対象とする。	
②取扱いを委託する特定個人情報ファイルの範囲	特定個人情報ファイルの全体 <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
対象となる本人の数	1,000万人以上	<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
対象となる本人の範囲 ※	「2. ③対象となる本人の範囲」と同上	
その妥当性	本特定個人情報ファイル(都道府県知事保存附票本人確認情報ファイル)が保存される附票都東京都サーバの運用及び監視業務を委託することによる。 なお、「①委託内容」の通り、委託事項は、直接附票本人確認情報に係わらない事務を対象としているため、委託先においては、特定個人情報ファイルに記録された情報そのものを扱う事務は実施しない。	
③委託先における取扱者数	10人未満	<選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法	○] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [] その他 ()	
⑤委託先名の確認方法	東京都総務局行政部のホームページにて確認できる。	
⑥委託先名	地方公共団体情報システム機構(機構)	
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	書面による承諾
	⑨再委託事項	附票東京都サーバの運用及び監視に関する業務。再委託する業務は、直接附票本人確認情報に係わらない(直接附票本人確認情報にアクセスできず、閲覧・更新・削除等を行わない。)業務を対象とする。
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 (1) 件 ☐ 行っていない
提供先1	東京都の他の執行機関(下水道局、水道局、警視庁、東京消防庁、東京都教育委員会)
①法令上の根拠	住基法第30条の15第2項(本人確認情報の利用) 住基法第30条の44の6第3項(都道府県知事保存附票本人確認情報(住民票コードに限る。))の利用) 住民サービスの向上と行政事務の効率化を図るために住民基本台帳ネットワークシステムの本人確認情報を利用する事務等を定める条例
②提供先における用途	住基法別表第6に掲げる、東京都の他の執行機関への情報提供が認められる事務(例:教育委員会における特別支援学校への就学のため必要な経費の支弁に関する事務等)の処理及び都条例に定める事務(例:東京都恩給条例による年金である給付の支給に関する事務)の処理に用いる。
③提供する情報	住民票コード、氏名、住所、生年月日、性別、個人番号(番号法に基づく東京都の他の執行機関からの求めがあった場合に限る。) ※住民票コードについては、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施行に伴う関係法律の整備等に関する法律(平成25年5月31日法律第28号)第22条第7項に基づく経過措置である。
④提供する情報の対象となる本人の数	[1,000万人以上] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (住民基本台帳ネットワークシステム) ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	東京都の他の執行機関からの情報照会の要求があった都度、随時。
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	

移転先1	東京都の他部署(総務局(総務部、人事部)、主税局(税制部、課税部、資産税部、徴収部、都税事務所、都税総合事務センター)、生活文化スポーツ局(都民生活部、私学部)、保健医療局(医療政策部、保健政策部)、福祉局(生活福祉部、子供・子育て支援部、障害者施策推進部)、産業労働局(商工部、観光部)等)
①法令上の根拠	住基法第30条の15第1項(本人確認情報の利用) 住基法第30条の44の6第3項(都道府県知事保存附票本人確認情報(住民票コードに限る。))の利用 住民サービスの向上と行政事務の効率化を図るために住民基本台帳ネットワークシステムの本人確認情報を利用する事務等を定める条例
②移転先における用途	住基法別表第5に掲げる、都道府県知事において都道府県知事保存附票本人確認情報の利用が認められた事務の処理に用いる。
③移転する情報	住民票コード、氏名、住所、生年月日、性別、個人番号(番号法に基づく自都道府県の他部署からの求めがあった場合に限る。) ※住民票コードについては、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施行に伴う関係法律の整備等に関する法律(平成25年5月31日法律第28号)第22条第7項に基づく経過措置である。
④移転する情報の対象となる本人の数	[1,000万人以上] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上
⑥移転方法	[] 庁内連携システム [] 電子メール [] フラッシュメモリ [○] その他 (住民基本台帳ネットワークシステム) [] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙
⑦時期・頻度	東京都の他部署からの検索要求があった都度、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 ※		【東京都サーバ】 セキュリティゲートにて入退館管理をしている都道府県サーバの集約センターにおいて、施錠管理及び入退室管理（監視カメラを設置してサーバ設置場所への入退室者を特定・管理）を行っている部屋に設置したサーバ内に保管する。サーバへのアクセスはIDと生体認証（又はパスワード）による認証が必要となる。 【電子記録媒体】 総務局行政部から貸与する指定のDVD－RWに暗号化の上格納し、施錠が出来る金庫等に保管する。 【紙】 各所属において、施錠が出来る金庫等に保管する。
②保管期間	期間	＜選択肢＞ 1) 1年未満 4) 3年 7) 6年以上10年未満 10) 定められていない 2) 1年 5) 4年 8) 10年以上20年未満 3) 2年 6) 5年 9) 20年以上 [1年未満]
	その妥当性	附票本人確認情報の提供に併せて提供される個人番号は、東京都の他の執行機関又は他部署からの求めにより提供・移転された後は、障害発生等により提供・移転先で情報を受領できなかった場合に備えて、一時的に保存されるのみである。
③消去方法		【東京都サーバ】 一時的な保存後にシステムにて自動判別し消去する。 【電子記録媒体】 総務局行政部から貸与する指定のDVD－RWのみ使用を認めており、書き込みができなくなったり、不要となった媒体については、総務局行政部にて回収の上、物理的に破壊し、廃棄記録をつけている。 【紙】 シュレッダー又は溶解処分により確実に廃棄を行っている。
7. 備考		
—		

(別添2) 特定個人情報ファイル記録項目

(1) 都道府県知事保存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. 生年月日、6. 性別、7. 住所、8. 外字数(住所)、9. 個人番号、10. 異動事由、11. 異動年月日、12. 保存期間フラグ、13. 清音化かな氏名、14. 市町村コード、15. 大字・字コード、16. 操作者ID、17. 操作端末ID、18. タイムスタンプ、19. 通知を受けた年月日、20. 外字フラグ、21. 削除フラグ、22. 更新順番号、23. 氏名外字変更連番、24. 住所外字変更連番、25. 旧氏 漢字、26. 旧氏 外字数、27. 旧氏 ふりがな、28. 旧氏 外字変更連番

(2) 都道府県知事保存附票本人確認情報ファイル

ア 附票本人確認情報

1. 住民票コード、2. 氏名 漢字、3. 氏名 外字数、4. 氏名 ふりがな、5. 生年月日、6. 性別、7. 住所 市町村コード、8. 住所 漢字、9. 住所、外字数、10. 最終住所 漢字、11. 最終住所 外字数、12. 異動年月日、13. 旧住民票コード、14. 附票管理市町村コード、15. 附票本人確認情報状態区分、16. 外字フラグ、17. 外字パターン、18. 通知区分

イ その他

1. 個人番号(※国外転出者に係る事務処理に関し、番号法で認められた場合に限り、自都道府県の他の執行機関又は他部署からの求めに応じ、当該個人の住民票コードを用いて、都道府県知事保存本人確認情報ファイルから個人番号を抽出し、提供・移転する場合がある。)

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

1. 特定個人情報ファイル名		
(1)都道府県知事保存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	都道府県知事保存本人確認情報ファイルにおける特定個人情報の入手手段は、区市町村CSからの本人確認情報更新要求の際に通知される本人確認情報に限定される。この場合、区市町村CSから対象者以外の情報が通知されてしまうことがリスクとして想定されるが、制度上、対象者の真正性の担保は区市町村側の確認に委ねられるため、区市町村において厳格な審査が行われることが前提となる。	
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	法令により区市町村から通知を受けることとされている情報のみを入手できることを、システム上で担保する。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 不適切な方法で入手が行われるリスク		
リスクに対する措置の内容	本人確認情報の入手元を区市町村CS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	住民の異動情報の届出等を受け付ける区市町村の窓口において、対面で身分証明書（個人番号カード等）の提示を受け、本人確認を行う。	
個人番号の真正性確認の措置の内容	区市町村において真正性が確認された情報を区市町村CSを通じて入手できることを、システムで担保する。	
特定個人情報の正確性確保の措置の内容	システム上、本人確認情報更新の際に、論理チェックを行う（例えば、現存する住民に対して転入を異動事由とする更新が行われようとした場合や、転居を異動事由とする更新の際に住所以外の更新が行われようとした場合に当該処理をエラーとする）仕組みとする。 また、入手元である区市町村CSにおいて、項目（フォーマット、コード）のチェックを実施する。	
その他の措置の内容	システムでは対応できない事象が発生した際に、本人確認情報の正確性を維持するため、要領・手順書等に基づいて本人確認情報の入力、削除及び訂正が行われていることを定期的に確認する。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク		
リスクに対する措置の内容	・機構が作成・配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。 ・区市町村CSと接続するネットワーク回線に専用回線を用いる、情報の暗号化を実施する等の措置を講じる。 ・特定個人情報の入手は、システム上自動処理にて行われるため、操作者は存在せず人為的なアクセスが行われることはない。 ※東京都サーバのサーバ上で稼動するアプリケーション。 都道府県内の市町村の住民の本人確認情報を管理し、都道府県内の市町村の市町村CSや全国サーバとのデータ交換を行う。 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。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置		
—		

3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク		
宛名システム等における措置の内容	東京都サーバは、宛名システム等とは接続しない。	
事務で使用するその他のシステムにおける措置の内容	庁内システムと東京都サーバとの接続は行わない。 東京都サーバは、集約センター内において、附票東京都サーバと接続する。 なお、東京都サーバと附票東京都サーバのシステム間のアクセスは、以下の場合の処理に限られるよう、システムにより制限する。 (1) 東京都サーバ⇒附票東京都サーバへのアクセス 番号法で認められた場合に限り、東京都の他の執行機関又は他部署等からの求めに応じ、国外転出者に係る個人番号を連携する場合。 (2) 附票東京都サーバ⇒東京都サーバへのアクセス 国外転出者に係る事務処理に関し、番号法で認められた場合に限り、東京都の他の執行機関又は他部署等からの求めに応じ、個人番号を入手する場合(目的を超えた紐付けが行われないよう、個人番号は附票本人確認情報DBとは別の一時保存領域で処理する。))。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2: 権限のない者(元職員、アクセス権限のない職員等)によって不正に使用されるリスク		
ユーザ認証の管理	[行っている]	<選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	操作者に固有のIDを付与するとともに、生体認証によるユーザ認証を行っている。	
アクセス権限の発効・失効の管理	[行っている]	<選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	職員の異動や退職等が発生した際に、発行及び失効について照合情報等管理簿により管理を行っている。失効管理が適切に行われていることについての確認は、年度当初に照合情報等管理簿を作成する際に行っている。	
アクセス権限の管理	[行っている]	<選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	・操作者の権限等に応じたアクセス権限が付与されるよう管理する。 ・不正アクセスを分析するために、業務端末におけるアプリケーションの操作ログ、アクセスログを取得し、保管する。	
特定個人情報の使用の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	・本人確認情報を扱うシステムの操作履歴(アクセスログ・操作ログ)を記録する。 ・ログを総務局行政部にて分析し、確認を実施する。 ・不正な操作が無いことについて、操作履歴により適時確認する。 ・操作履歴の確認により本人確認情報の検索に関して不正な操作の疑いがある場合は、申請文書等との整合性を確認する。 ・バックアップされた操作履歴について、一定期間、安全な場所に施錠保管する。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 従業者が事務外で使用するリスク		
リスクに対する措置の内容	・システムの操作履歴(操作ログ)を記録する。 ・担当者へのヒアリングを実施し、業務上必要のない検索又は抽出が行われていないことを確認する。 ・システムを利用する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。 ・外部記録媒体の持ち出しは、「住民基本台帳ネットワークシステム 情報セキュリティ実施手順 利用者用」により禁止されている。 ・職員以外の従業者(委託先)には、当該事項についての誓約書の提出を求める。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク4: 特定個人情報ファイルが不正に複製されるリスク	
リスクに対する措置の内容	システム上、管理権限を与えられた者以外、情報の複製は行えない仕組みとする。 システムを利用する職員への研修会において、複製の禁止等について指導する。 また、定期運用に基づくバックアップ以外にファイルを複製しないよう、委託先等の従業者に対し指導する。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	
その他、特定個人情報の使用にあたり、以下の措置を講じている。 【端末利用】 ①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することを防止する ②代表端末及び業務端末のディスプレイを、来庁者から見えない位置に設置する ③ディスプレイに覗き見防止シートを取り付ける ④本人確認情報が表示された画面のハードコピーの取得ができないよう設定している ⑤大量のデータ出力に際しては、事前に管理責任者の承認を得るよう指導している 【住民対応】 ①本人確認情報の開示・訂正の請求により、住民が特定個人情報の正確性等を確認できる ②本人確認情報の提供状況の開示請求により、住民が特定個人情報の提供先等を確認できる	

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	契約後、秘密保持に関する誓約書とあわせて、委託先の管理体制図、連絡先一覧等を提出させている。 また、Pマークを取得していることを確認している。	
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	①委託先には、特定個人情報の更新／閲覧権限を付与していない。 ②障害対応、機器更新等で委託先が都道府県知事保存本人確認情報ファイルをデータ移管する場合は、作業報告を受けることになっている。	
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	秘密保持のため、下記について指導している。 ①契約書等に基づき、委託業務が実施されていることを適時確認するとともに、その記録を残す。 ②委託業者から適時セキュリティ対策の実施状況の報告を受けるとともに、その記録を残す。 ③その他、システムによる取扱い記録(アクセスログ)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	契約上、特定個人情報の提供は一切認めていない。 操作ログ、検索件数の取得により確認している。	
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	下記を定めた仕様書を用いて契約を行っている。 ・秘密の保持 ・目的外利用の禁止 ・複写・複製の禁止 ・持ち出しの禁止 ・情報の管理及び保管のための安全管理措置を講じる義務(入退室管理、施錠管理、契約解除時等の消去、事故報告等) ・機密情報取扱いに関する教育及び研修の実施 ・再委託に関する取扱い(再委託の許諾、委託先と同等の遵守義務、誓約書の提出等) ・実地調査及び改善の指示	
特定個人情報の消去ルール	[定めている]	＜選択肢＞ 1) 定めている 2) 定めていない
ルールの内容及びルール遵守の確認方法	委託先には、特定個人情報の更新／閲覧権限を付与していないため、消去は障害対応、機器更新等での機器交換(ディスク故障含む)時のみとなる。 破損や耐用年数を過ぎた媒体(ハードディスク等)は、委託先が管理簿に理由を明記し物理的に廃棄している。 保管状況を週次で管理簿と現物の点検を実施し、月次報告を行っている。	
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	下記を定めた仕様書を用いて契約を行っている。 ・秘密の保持 ・目的外利用の禁止 ・複写・複製の禁止 ・持ち出しの禁止 ・情報の管理及び保管のための安全管理措置を講じる義務(入退室管理、施錠管理、契約解除時等の消去、事故報告等) ・機密情報取扱いに関する教育及び研修の実施 ・再委託に関する取扱い(再委託の許諾、委託先と同等の遵守義務、誓約書の提出等) ・実地調査及び改善の指示	
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	契約上、特定個人情報の取扱いについて委託先が順守すべき事項を再委託先・再々委託先においても遵守すべき旨定めるとともに、再委託・再々委託承諾の際、再委託先等から同事項を遵守する旨の誓約書を徴している。また、必要に応じ、再委託先に対しても必要な実地調査や指示を行うことができることとしている。 また、再委託先等に対しては、東京都サーバ内の特定個人情報の更新／閲覧権限を付与していない。	
その他の措置の内容	—	
リスクへの対策は十分な	[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

「東京都サーバの運用及び監視に関する業務」

再委託先については、毎年度の契約において、再委託先業者の業務内容や委託先との業務分担を審査した上で承認を行っている。

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	住民基本台帳ネットワークシステムを通じて特定個人情報（個人番号、4情報等）の提供・移転を行っており、特定個人情報（個人番号、4情報等）の提供・移転に係る処理を行った際、記録（日時、操作者等）をシステム上で管理し保存する。 なお、システム上、提出・移転に係る処理を行ったものの提出・移転が認められなかった場合についても記録を残す。	
特定個人情報の提供・移転に関するルール	[定めている]	＜選択肢＞ 1) 定めている 2) 定めていない
ルールの内容及びルール遵守の確認方法	以下の法令等に従い特定個人情報の提供・移転を行っている。 ・住基法第30条の7（都道府県から機構へ本人確認情報の通知等） ・住基法第30条の15第1項（本人確認情報の利用） ・電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準 ・東京都住民基本台帳ネットワークシステム運用管理規程 操作ログを分析し、不正な操作がなされていないか確認を行っている。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2：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	連携手段として通信の記録が逐一保存され、また、連携するデータが暗号化される仕組みが確立した住民基本台帳ネットワークシステムを用いることにより、不適切な方法による特定個人情報の提供を防止する。 なお、全国サーバと東京都サーバの間の通信では専用線を用い相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。 また、東京都の他の執行機関への提供及び他の部署への移転のため、外部記録媒体へ出力する必要がある場合には、情報を暗号化し逐一出力の記録が残される仕組みを構築している。	
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	・誤った情報を提供・移転してしまうリスクへの措置 :システム上、照会元から指定された検索条件に基づき得た結果を適切に提供・移転することを担保する。 ・誤った相手に提供・移転してしまうリスクへの措置 :全国サーバと東京都サーバの間の通信では専用線を用い相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。 また、情報を暗号化し格納した媒体による情報の提供・移転が必要な場合には文書による確認を実施し、法令上の根拠のない相手先へ情報の提供・移転を防止している。	
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
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		
—		

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

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1) 特に力を入れて遵守している 2) 十分に遵守している 3) 十分に遵守していない 4) 政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1) 特に力を入れて周知している 2) 十分に周知している 3) 十分に周知していない
⑤物理的対策	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
	具体的な対策の内容	セキュリティゲートにて入退館管理をしている都道府県サーバの集約センターにおいて、施錠管理及び入退室管理(監視カメラを設置してサーバ設置場所への入退室者を特定・管理)を行っている部屋に設置したサーバ内に保管する。サーバへのアクセスはID／パスワードによる認証が必要となる。
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	・ウイルス対策ソフトの定期的なパターン更新を実施している。 ・庁内のネットワークにおいて、ファイアウォールを導入しログの解析を行っている。 ・専用回線を利用し、データを暗号化してやり取りしている。 ・サーバ間の相互認証を行っている。 ・集約センターにおいて、ファイアウォールを導入し、ログの解析を行っている。
⑦バックアップ	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
⑧事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない

⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生あり] <選択肢> 1) 発生あり 2) 発生なし
その内容	①令和2年8月21日に東京都人権プラザにおいて開催した「心と体を傷つけられて亡くなった天国の子供たちのメッセージ」展のメディア向けカンファレンスの動画配信案内を（公財）東京都人権啓発センターの行事案内希望者に対して送付する際、事務担当者が誤ってメールアドレスをBCC欄ではなく、CC欄に入力して発信したため、個人情報が流出する事故が発生した。 ②令和3年1月に東京都電子調達システムにより印刷物の契約案件を公表した際、印刷物の配布先となる町会名のみを公表するところ、誤って中野区内の町会の代表者の氏名、住所及び電話番号を1月28日から2月3日までの間、公表してしまった。 ③令和3年3月、助成金返還事務のためにワンピシより取り寄せていた平成29年度教育助成金調査票（B表）の返却手続きを行った際、段ボール二箱分がないことが発覚した。当該段ボール箱は執務室内の空きスペースにて保管していた。 ④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、都が過去に出展した民間企業主催の就職イベント参加者及び当該企業に対して都関連の採用情報の提供を希望した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ため、個人情報が流出する事故が発生した。 ⑤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てしまい、氏名が流出する事故が発生した。 ⑥令和3年12月、都営住宅の毎月募集の申込者に対して、東京都住宅供給公社において、抽せん番号をお知らせする郵便はがきを発送する準備を行い、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。 ⑦令和4年5月、指定管理者が運営する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。 ⑧令和4年5月、都の技能検定試験に関する業務を行う東京都職業能力開発協会において、技能検定試験に関する通知を外国人技能実習の監理団体に対してメールで送付する際、事務担当者が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。 ⑨令和4年5月、就学支援金事務の受託者である東京都私学財団が、就学支援金の基礎データをCD-Rに情報を保存し、対象高等学校等宛で一斉に送付したところ、そのうち1校において、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。 ⑩令和4年5月、都の医療機器産業への参入支援事業の受託者が、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、宛先欄に複数のメールアドレスを入力し、送信してしまった。同社の配信システムは、1名分のメールを送信した後、宛先欄のメールアドレスが自動で次の1名のアドレスに上書き処理されるプログラムが組まれていたが、プログラムの改修ミスにより、メールアドレスが上書きではなく追記されて送信されていた。 ⑪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。 ⑫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。

再発防止策の内容

- ① 団体に対し、外部へ一斉送信する際は、メールアドレスをBCC欄に入力すべきことと、メール送信前に、複数の職員で宛先の確認作業を必ず行うことを、職員全員に改めて周知徹底するとともに、組織としての検証を行い、再発防止策を検討するよう指導した。
- ② (1) 事務フローの見直し
 - ・起工部署の事務フローを、別紙1のとおり見直し、周知徹底を図る。
 - ・契約部署は、着手起案作成時及び発注図書登録時、電子調達システムに、起工部署から提出されたPDFデータを公表前の登録を行ってから印刷した上で、契約依頼文書に添付された仕様書と照合し、一致していることを確認する。また、この確認方法について、令和元年12月19日付経理部契約課長事務連絡「契約事務に係る情報漏えい等の防止策について」により配布されたチェックリストに追記した。
- (2) 臨時支所コンプライアンス推進委員会の開催
臨時支所コンプライアンス推進委員会を開催し、再発防止に向け、上記事務フローの見直しの周知徹底を図った。
- ③ (1) 個人情報の重要性を再確認し、高い危機意識をもって個人情報の適正な管理・運用を図るよう、改めて基本的な取扱いルール of 徹底を図る。
- (2) 書類の所在及び処理状況が明確に分かるような管理方法の整備や、文書廃棄の際の事務処理手順の整備など、書類管理の徹底に向けた仕組みの構築を図る。
- ④ (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徹底を図る。
- (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。
- ⑤ 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。
- ⑥ (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。
- ⑦ (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業を共有し、個人情報を含む情報の適切な管理を徹底する。
- ⑧ (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
- ⑨ 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対策について改めて確認を行う。
- ⑩ (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。
- ⑪ 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。
- ⑫ (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、最近の事故事例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

⑩死者の個人番号	[保管している]	<選択肢> 1) 保管している 2) 保管していない
具体的な保管方法	生存する個人の個人番号とともに、死亡による消除後、住基法施行令第30条の6(都道府県における本人確認情報の保存期間)に定める期間(150年間)保管する。	
その他の措置の内容	—	
リスクへの対策は十分か	[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	区市町村の住民基本台帳で本人確認情報の変更があった場合には住民基本台帳ネットワークシステムを通して本人確認情報の更新が行われる仕組みとなっているため、古い情報のまま保管されることはない。 また、区市町村CSとの整合処理を定期的 to 実施し、保存する本人確認情報が最新であるかどうかを確認する。	
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	【ファイル上の個人ごとの消去】 ・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法令(住民基本台帳法施行令第30条の6)に定める保存期間(150年)を経過した後にシステムにて自動的に消去する。 【物理的なファイル全体の消去】 ・磁気ディスクの廃棄時は、要領・手順書等に基づき、内容の消去、破壊等を行うとともに、磁気ディスク管理簿にその記録を残す。 また、専用ソフトによるフォーマット、物理的粉砕等を行うことにより、内容を読み出すことができないようにする。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		
—		

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

1. 特定個人情報ファイル名			
(2)都道府県知事保存附票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	都道府県知事保存附票本人確認情報ファイルにおける特定個人情報の入手手段は、区市町村CSからの附票本人確認情報更新要求の際に通知される附票本人確認情報に限定される。この場合、区市町村CSから対象者以外の情報が通知されてしまうことがリスクとして想定されるが、制度上、対象者の真正性の担保は区市町村側の確認に委ねられるため、区市町村において厳格な審査が行われることが前提となる。また、対象者以外の個人番号は入手できないことを、システムにより担保する。		
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	法令により区市町村から通知を受けることとされている情報のみを入手できることを、システム上で担保する。また、対象者の個人番号以外の個人情報入手できないことを、システムにより担保する。		
その他の措置の内容	—		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
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	附票本人確認情報の入手元を区市町村CSIに限定する。 また、国外転出者に係る事務処理に関し、番号法で認められた場合に限り、東京都の他の執行機関又は他部署等からの求めに応じ、個人番号を入手することを、システムにより担保する。		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク3： 入手した特定個人情報が不正確であるリスク			
入手の際の本人確認の措置の内容	住民の異動情報の届出等を受け付ける区市町村の窓口において、対面で身分証明書（個人番号カード等）の提示を受け、本人確認を行う。 個人番号については、都道府県知事保存本人確認情報ファイルから入手するため、該当なし。		
個人番号の真正性確認の措置の内容	区市町村において真正性が確認された情報を区市町村CSを通じて入手できることを、システムで担保する。 また、都道府県知事保存附票本人確認情報ファイルに保存される段階で真正性が担保されている。		
特定個人情報の正確性確保の措置の内容	システム上、附票本人確認情報更新の際に、論理チェックを行う（例えば、既に削除されている者に対して、削除を要求する通知があった場合に当該処理をエラーとする）仕組みとする。 また、入手元である区市町村CSにおいて、項目（フォーマット、コード）のチェックを実施する。 個人番号については、都道府県知事保存附票本人確認情報ファイルに保存される段階で正確性が確保されている。		
その他の措置の内容	システムでは対応できない事象が発生した際に、附票本人確認情報の正確性を維持するため、要領・手順書等に基づいて附票本人確認情報の入力、削除及び訂正が行われていることを定期的に確認する。		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である

リスク4： 入手の際に特定個人情報漏えい・紛失するリスク	
リスクに対する措置の内容	・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。 ・区市町村CSと接続するネットワーク回線に専用回線を用いる、情報の暗号化を実施する等の措置を講じる。 ・特定個人情報の入手は、システム上自動処理にて行われるため、操作者は存在せず人為的なアクセスが行われることはない。 ※附票東京都サーバのサーバ上で稼動するアプリケーション。 都道府県内の市町村の住民の附票本人確認情報を管理し、都道府県内の市町村の市町村CSや附票全国サーバとのデータ交換を行う。 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。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。)におけるその他のリスク及びそのリスクに対する措置	
—	

3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク		
宛名システム等における措置の内容	附票東京都サーバは、宛名システム等とは接続しない。	
事務で使用するその他のシステムにおける措置の内容	庁内システムと附票東京都サーバとの接続は行わない。 附票東京都サーバは、集約センター内において、東京都サーバと接続する。 なお、附票東京都サーバと東京都サーバのシステム間のアクセスは、以下の場合の処理に限られるよう、システムにより制限する。 (1)附票東京都サーバ⇒東京都サーバへのアクセス 国外転出者に係る事務処理に関し、番号法で認められた場合に限り、東京都の他の執行機関又は他部署等からの求めに応じ、個人番号を入手する場合(目的を越えた紐づけが行われないよう、個人番号は附票本人確認情報DBとは別の一時保存領域で処理する。))。 (2)東京都サーバ⇒附票東京都サーバへのアクセス 番号法で認められた場合に限り、東京都の他の執行機関又は他部署等からの求めに応じ、国外転出者に係る個人番号を連携する場合。	
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	操作者に固有のIDを付与するとともに、生体認証によるユーザ認証を行っている。	
アクセス権限の発効・失効の管理	[行っている]	<選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	職員の異動や退職等が発生した際に、発行及び失効について照合情報等管理簿により管理を行っている。失効管理が適切に行われていることについての確認は、年度当初に照合情報等管理簿を作成する際に行っている。	
アクセス権限の管理	[行っている]	<選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	・操作者の権限等に応じたアクセス権限が付与されるよう管理する。 ・不正アクセスを分析するために、業務端末におけるアプリケーションの操作ログ、アクセスログを取得し、保管する。	
特定個人情報の使用の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	・附票本人確認情報を扱うシステムの操作履歴(アクセスログ・操作ログ)を記録する。 ・ログを総務局行政部にて分析し、確認を実施する。 ・不正な操作が無いことについて、操作履歴により適時確認する。 ・操作履歴の確認により附票本人確認情報の検索に関して不正な操作の疑いがある場合は、申請文書等との整合性を確認する。 ・バックアップされた操作履歴について、一定期間、安全な場所に施錠保管する。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 従業者が事務外で使用するリスク		
リスクに対する措置の内容	・システムの操作履歴(操作ログ)を記録する。 ・担当者へのヒアリングを実施し、業務上必要のない検索又は抽出が行われていないことを確認する。 ・システムを利用する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。 ・外部記録媒体の持ち出しは、「住民基本台帳ネットワークシステム 情報セキュリティ実施手順 利用者用」により禁止されている。 ・職員以外の従業者(委託先)には、当該事項についての誓約書の提出を求める。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク4： 特定個人情報ファイルが不正に複製されるリスク		
リスクに対する措置の内容	システム上、管理権限を与えられた者以外、情報の複製は行えない仕組みとする。 システムを利用する職員への研修会において、複製の禁止等について指導する。 また、定期運用に基づくバックアップ以外にファイルを複製しないよう、委託先等の従業者に対し指導する。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置		
その他、特定個人情報の使用にあたり、以下の措置を講じている。 【端末利用】 ①スクリーンセーバ等を利用して、長時間にわたり附票本人確認情報を表示することを防止する ②代表端末及び業務端末のディスプレイを、来庁者から見えない位置に設置する ③ディスプレイに覗き見防止シートを取り付ける ④附票本人確認情報が表示された画面のハードコピーの取得ができないよう設定している ⑤大量のデータ出力に際しては、事前に管理責任者の承認を得よう指導している 【住民対応】 ①附票本人確認情報の開示・訂正の請求により、住民が特定個人情報の正確性等を確認できる ②附票本人確認情報の提供状況の開示請求により、住民が特定個人情報の提供先等を確認できる		

☐ 委託しない

情報保護管理体制の確認	契約後、秘密保持に関する誓約書とあわせて、委託先の管理体制図、連絡先一覧等を提出させている。 また、Pマークを取得していることを確認している。
-------------	--

具体的な制限方法	①委託先には、特定個人情報の更新／閲覧権限を付与していない。 ②障害対応、機器更新等で委託先が都道府県知事保存附票本人確認情報ファイルをデータ移管する場合は、作業報告を受けることになっている。
----------	---

具体的な方法	秘密保持のため、下記について指導している。 ①契約書等に基づき、委託業務が実施されていることを適時確認するとともに、その記録を残す。 ②委託業者から適時セキュリティ対策の実施状況の報告を受けるとともに、その記録を残す。 ③その他、システムによる取扱い記録(アクセスログ)を残す。
--------	--

委託先から他者への提供に関するルール内容及びルール導	契約上、特定個人情報の提供は一切認めていない。 操作ログ、検索件数の取得により確認している。
----------------------------	---

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	下記を定めた仕様書を用いて契約を行っている。 ・秘密の保持 ・目的外利用の禁止 ・複写・複製の禁止 ・持ち出しの禁止 ・情報の管理及び保管のための安全管理措置を講じる義務（入退室管理、施錠管理、契約解除時等の消去、事故報告等） ・機密情報取扱いに関する教育及び研修の実施 ・再委託に関する取扱い（再委託の許諾、委託先と同等の遵守義務、誓約書の提出等） ・実地調査及び改善の指示
---	--

ルール内容及び ルール遵守の確認方法	委託先には、特定個人情報の更新／閲覧権限を付与していないため、消去は障害対応、機器更新等での機器交換（ディスク故障含む）時のみとなる。 破損や耐用年数を過ぎた媒体（ハードディスク等）は、委託先が管理簿に理由を明記し物理的に廃棄している。 保管状況を週次で管理簿と現物の点検を実施し、月次報告を行っている。
-------------------------------	---

規定の内容	下記を定めた仕様書を用いて契約を行っている。 ・秘密の保持 ・目的外利用の禁止 ・複写・複製の禁止 ・持ち出しの禁止 ・情報の管理及び保管のための安全管理措置を講じる義務（入退室管理、施錠管理、契約解除時等の消去、事故報告等） ・機密情報取扱いに関する教育及び研修の実施 ・再委託に関する取扱い（再委託の許諾、委託先と同等の遵守義務、誓約書の提出等） ・実地調査及び改善の指示
-------	--

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	十分にやっている <選択肢> 1) 特に力を入れて行っている 2) 十分にやっている 3) 十分にやっていない 4) 再委託していない
具体的な方法	契約上、特定個人情報の取扱いについて委託先が順守すべき事項を再委託先・再々委託先においても遵守すべき旨定めるとともに、再委託・再々委託承諾の際、再委託先等から同事項を遵守する旨の誓約書を徴している。また、必要に応じ、再委託先に対しても必要な実地調査や指示を行うことができることとしている。 また、再委託先等に対しては、附票東京都サーバ内の特定個人情報の更新／閲覧権限を付与していない。
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
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	
「附票東京都サーバの運用及び監視に関する業務」 再委託先については、毎年度の契約において、再委託先業者の業務内容や委託先との業務分担を審査した上で承認を行っている。	

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	住民基本台帳ネットワークシステムを通じて特定個人情報（個人番号、4情報等）の提供・移転を行っており、特定個人情報（個人番号、4情報等）の提供・移転に係る処理を行った際、記録（日時、操作者等）をシステム上で管理し保存する。なお、システム上、提供・移転に係る処理を行ったものの提供・移転が認められなかった場合についても記録を残す。		
特定個人情報の提供・移転に関するルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない	
ルールの内容及びルール遵守の確認方法	以下の法令等に従い特定個人情報の提供・移転を行っている。 ・住基法第30条の7（都道府県から機構へ本人確認情報の通知等） ・住基法第30条の15第1項（本人確認情報の利用） ・電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準 ・東京都住民基本台帳ネットワークシステム運用管理規程 操作ログを分析し、不正な操作がなされていないか確認を行っている。		
その他の措置の内容	—		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク2： 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	連携手段として通信の記録が逐一保存され、また、連携するデータが暗号化される仕組みが確立した附票連携システムを用いることにより、不適切な方法による特定個人情報の提供を防止する。 なお、附票全国サーバと附票東京都サーバの間の通信では専用線を用い相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。 また、東京都の他の執行機関への提供及び他の部署への移転のため、外部記録媒体へ出力する必要がある場合には、情報を暗号化し逐一出力の記録が残される仕組みを構築している。		
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	・誤った情報を提供・移転してしまうリスクへの措置 :システム上、照会元から指定された検索条件に基づき得た結果を適切に提供・移転することを担保する。 ・誤った相手に提供・移転してしまうリスクへの措置 :附票全国サーバと附票東京都サーバの間の通信では専用線を用い相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置			
—			

6. 情報提供ネットワークシステムとの接続

☐ 接続しない(入手) ☐ 接続しない(提供)

リスク1: 目的外の入手が行われるリスク

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

リスク2: 安全が保たれない方法によって入手が行われるリスク

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

リスク3: 入手した特定個人情報が不正確であるリスク

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

リスク4: 入手の際に特定個人情報情報が漏えい・紛失するリスク

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

リスク5: 不正な提供が行われるリスク

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

リスク6: 不適切な方法で提供されるリスク

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

リスク7: 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク

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

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

100

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	セキュリティゲートにて入退館管理をしている附票都道府県サーバの集約センターにおいて、施錠管理及び入退室管理(監視カメラを設置してサーバ設置場所への入退室者を特定・管理)を行っている部屋に設置したサーバ内に保管する。サーバへのアクセスはID／パスワードによる認証が必要となる。
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	・ウイルス対策ソフトの定期的なパターン更新を実施している。 ・庁内のネットワークにおいて、ファイアウォールを導入しログの解析を行っている。 ・専用回線を利用し、データを暗号化してやり取りしている。 ・サーバ間の相互認証を行っている。 ・集約センターにおいて、ファイアウォールを導入し、ログの解析を行っている。
⑦バックアップ	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
⑧事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない

⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生あり] <選択肢> 1) 発生あり 2) 発生なし
その内容	①令和2年8月21日に東京都人権プラザにおいて開催した「心と体を傷つけられて亡くなった天国の子供たちのメッセージ」展のメディア向けカンファレンスの動画配信案内を（公財）東京都人権啓発センターの行事案内希望者に対して送付する際、事務担当者が誤ってメールアドレスをBCC欄ではなく、CC欄に入力して発信したため、個人情報が流出する事故が発生した。 ②令和3年1月に東京都電子調達システムにより印刷物の契約案件を公表した際、印刷物の配布先となる町会名のみを公表するところ、誤って中野区内の町会の代表者の氏名、住所及び電話番号を1月28日から2月3日までの間、公表してしまった。 ③令和3年3月、助成金返還事務のためにワンビシより取り寄せていた平成29年度教育助成金調査票（B表）の返却手続きを行った際、段ボール二箱分がないことが発覚した。当該段ボール箱は執務室内の空きスペースにて保管していた。 ④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、都が過去に出展した民間企業主催の就職イベント参加者及び当該企業に対して都関連の採用情報の提供を希望した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ため、個人情報が流出する事故が発生した。 ⑤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てしまい、氏名が流出する事故が発生した。 ⑥令和3年12月、都営住宅の毎月募集の申込者に対して、東京都住宅供給公社において、抽せん番号をお知らせする郵便はがきを発送する準備を行い、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。 ⑦令和4年5月、指定管理者が運営する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。 ⑧令和4年5月、都の技能検定試験に関する業務を行う東京都職業能力開発協会において、技能検定試験に関する通知を外国人技能実習の監理団体に対してメールで送付する際、事務担当者が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。 ⑨令和4年5月、就学支援金事務の受託者である東京都私学財団が、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校において、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。 ⑩令和4年5月、都の医療機器産業への参入支援事業の受託者が、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、宛先欄に複数のメールアドレスを入力し、送信してしまった。同社の配信システムは、1名分のメールを送信した後、宛先欄のメールアドレスが自動で次の1名のアドレスに上書き処理されるプログラムが組まれていたが、プログラムの改修ミスにより、メールアドレスが上書きではなく追記されて送信されていた。 ⑪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。 ⑫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。

再発防止策の内容

- ①団体に対し、外部へ一斉送信する際は、メールアドレスをBCC欄に入力すべきことと、メール送信前に、複数の職員で宛先の確認作業を必ず行うことを、職員全員に改めて周知徹底するとともに、組織としての検証を行い、再発防止策を検討するよう指導した。
- ②(1)事務フローの見直し
 ・起工部署の事務フローを、別紙1のとおり見直し、周知徹底を図る。
 ・契約部署は、着手起案作成時及び発注図書登録時、電子調達システムに、起工部署から提出されたPDFデータを公表前の登録を行ってから印刷した上で、契約依頼文書に添付された仕様書と照合し、一致していることを確認する。また、この確認方法について、令和元年12月19日付経理部契約課長事務連絡「契約事務に係る情報漏えい等の防止策について」により配布されたチェックリストに追記した。
- (2)臨時支所コンプライアンス推進委員会の開催
 臨時支所コンプライアンス推進委員会を開催し、再発防止に向け、上記事務フローの見直しの周知徹底を図った。
- ③(1)個人情報の重要性を再確認し、高い危機意識をもって個人情報の適正な管理・運用を図るよう、改めて基本的な取扱いルールの徹底を図る。
 (2)書類の所在及び処理状況が明確に分かるような管理方法の整備や、文書廃棄の際の事務処理手順の整備など、書類管理の徹底に向けた仕組みの構築を図る。
- ④(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。
- ⑤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。
- ⑥(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。
- ⑦(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。
- ⑧(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
- ⑨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対策について改めて確認を行う。
- ⑩(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を実施する、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。
- ⑪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。
- ⑫(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、最近の事故事例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

⑩死者の個人番号	[保管していない]	<選択肢> 1) 保管している 2) 保管していない
具体的な保管方法	—	
その他の措置の内容	—	
リスクへの対策は十分か	[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	附票本人確認情報の提供・移転に併せて提供される個人番号は、東京都の他の執行機関又は他部署等からの求めにより提供・移転された後は、障害発生等により提供・移転先で情報を受領できなかった場合に備えて一時的に保存がされるのみであり、情報が更新される必要はない。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	<選択肢> 1) 定めている 2) 定めていない
手順の内容	・障害発生等により提供・移転先で情報を受領できなかった場合に備えた一時的な保存の終了後、特定個人情報を、システムにて自動判別し消去する(消去されたデータは、復元できない)。 ・磁気ディスクの廃棄時は、要領・手順書等に基づき、内容の消去、破壊等を行うとともに、磁気ディスク管理簿にその記録を残す。また、専用ソフトによるフォーマット、物理的粉碎等を行うことにより、内容を読み出すことができないようにする。 ・帳票については、要領・手順書等に基づき、帳票管理簿等を作成し、受渡し、保管および廃棄の運用が適切になされていることを適時確認するとともに、その記録を残す。廃棄時には、要領・手順書等に基づき、裁断、溶解等を行うとともに、帳票管理簿等にその記録を残す。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		
—		

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1回、チェックシートを活用して、自己点検を実施している。点検結果を踏まえて、手順や運用方法を改善する。	
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	年1回、第三者機関による監査を実施している。監査結果を踏まえて体制や規定を改善する。	
2. 従業員に対する教育・啓発		
従業員に対する教育・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	住民基本台帳ネットワークシステム関係職員に対して、必要な知識の習得に資するための研修を実施するとともに、その記録を残す。	
3. その他のリスク対策		
—		

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	東京都総務局行政部振興企画課 163-8001 東京都新宿区西新宿2-8-1 03-5388-2469
②請求方法	法令等で定める様式による書面の提出により開示・停止・利用停止請求を受け付ける。
特記事項	個人情報保護対策として下記のホームページに開示方法や様式のリンク先を掲示している。 https://www.soumu.metro.tokyo.lg.jp/05gyousei/07juuki04.html
③手数料等	[有料] <選択肢> 1) 有料 2) 無料 (手数料額、納付方法: 納付書により、実費相当分(10円/1枚)の手数料を納付する。)
④個人情報ファイル簿の公表	[行っていない] <選択肢> 1) 行っている 2) 行っていない
個人情報ファイル名	—
公表場所	—
⑤法令による特別の手続	—
⑥個人情報ファイル簿への不記載等	—
2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	東京都総務局行政部振興企画課 163-8001 東京都新宿区西新宿2-8-1 03-5388-2469
②対応方法	開示請求と同様の手順となる。

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和5年11月21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	東京都公式ホームページ及び行政部公式ホームページにおいて全項目評価書を公開し、郵送及び電子メールにて意見を受け付ける。
②実施日・期間	令和5年8月4日から令和5年9月3日まで
③期間を短縮する特段の理由	—
④主な意見の内容	なし
⑤評価書への反映	なし
3. 第三者点検	
①実施日	令和5年9月27日から令和5年10月26日まで
②方法	東京都情報公開・個人情報保護審議会 特定個人情報保護評価部会において点検を受けた。
③結果	以下の答申を受けた。 本評価書案を点検したところ、住民基本台帳ネットワークに関する事務における特定個人情報ファイルの取扱いについては、個人のプライバシー等の権利利益に与える影響を予測した上で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分析し、そのようなリスクを軽減するための適切な措置をおおむね講じていると認められる。
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31年3月13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	振興調整担当課長 中島敬子	振興調整担当課長	事後	人事異動
平成31年3月13日	I 基本情報/(別添)事務の内容	図(略) ※備考 1. 本人確認情報の更新に関する事務 1-①.市区町村において受け付けた住民の異動に関する情報を、市区町村CSを通じて東京都サーバに通知する。 1-②.東京都サーバにおいて、市区町村より受領した本人確認情報を元に都道府県知事保存本人確認情報ファイルを更新する。 1-③.機構に対し、住民基本台帳ネットワークシステムを介して、本人確認情報の更新を通知する。	図(略) ※備考 1. 本人確認情報の更新に関する事務 1-①.市区町村は、住民から受け付けた住民の異動に関する情報を、市区町村コミュニケーションサーバ(市区町村CS)を通じて東京都サーバに通知する。 1-②.東京都知事は、東京都サーバにおいて、市区町村より受領した本人確認情報を元に都道府県知事保存本人確認情報ファイル(以下「本人確認情報ファイル」という。)を更新する。 1-③.東京都知事は、地方公共団体情報システム機構(以下「機構」という。)に対し、住民基本台帳ネットワークシステムを介して、本人確認情報の更新を通知する(これを受けて、機構が保管する全国サーバ内の本人確認情報が更新される。)	事後	概要図、記載内容の明確化

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31年3月13日	I 基本情報/(別添)事務の内容	2. 東京都の執行機関への情報提供 2-①.東京都の執行機関において、個人番号又は4情報をキーワードとした本人確認情報の照会を行う。 2-②.東京都知事において、提示されたキーワードを元に都道府県知事保存本人確認情報ファイルを検索し、 照会元に対し、当該個人の本人確認情報を提供する。 ※検索対象者が他都道府県の場合は全国サーバに対して検索の要求を行う。 ※一括提供の方式により本人確認情報を提供する場合には、都道府県知事において代表端末を操作し、電子記録媒体を用いて提供する。 3. 本人確認情報の開示に関する事務 3-①.住民より本人確認情報の開示請求を受け付ける。 3-②.開示請求者(住民)に対し、都道府県知事保存本人確認情報ファイルに記録された当該個人の本人確認情報を開示する。	2. 東京都の他の執行機関(東京消防庁など)への情報提供又は東京都の他部署への移転 2-①.東京都の他の執行機関又は東京都の他部署において、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。 2-②.東京都知事において、提示されたキーワードを元に本人確認情報ファイルを検索し、照会元に対し、当該個人の本人確認情報を提供する。 ※検索対象者が他都道府県の場合は全国サーバに対して検索の要求を行う(後記4)。 ※一括提供の方式により本人確認情報を提供する場合には、東京都知事(所管部署:総務局)において代表端末を操作し、外部記録媒体(DVD-RW)を用いて提供する。 3. 本人確認情報の開示に関する事務 3-①.総務局において、住民より自己に係る本人確認情報の開示請求を受け付ける。 3-②.開示請求者(住民)に対し、本人確認情報ファイルに記録された当該個人の本人確認情報を開示する。	事後	概要図、記載内容の明確化

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31年3月13日	I 基本情報/(別添)事務の内容	4. 機構への情報照会に係る事務 4-①.機構に対し、個人番号又は4情報をキーワードとした本人確認情報の照会を行う。 4-②.機構より、当該個人の本人確認情報を受領する。 5. 本人確認情報検索に関する事務 5-①.4情報の組み合わせを検索キーに、都道府県知事保存本人確認情報ファイルを検索する。 6. 本人確認情報整合 6-①.市区町村CSより、東京都サーバに対し、整合性確認用の本人確認情報を送付する。 6-②.東京都サーバにおいて、市区町村CSより受領した整合性確認用の本人確認情報を用いて都道府県知事保存本人確認情報ファイルの整合性確認を行う。 6-③.東京都サーバより、市区町村CSに対して整合性確認結果を通知する。	4. 機構への情報照会に係る事務(対象検索者が他道府県の場合) 4-①.東京都知事は、機構に対し、他道府県住民の個人番号又は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。 4-②. 東京都知事は、機構より、当該個人の本人確認情報を受領する。 5. 本人確認情報検索に関する事務 5-①. 東京都知事は、4情報の組み合わせを検索キーに、本人確認情報ファイルを検索する。 6. 本人確認情報整合 6-①. 東京都知事は、市区町村CSより、東京都サーバに対し、整合性確認用の本人確認情報を送付する。 6-②. 東京都知事は、東京都サーバにおいて、市区町村CSより受領した整合性確認用の本人確認情報を用いて本人確認情報ファイルの整合性確認を行う。 6-③. 東京都知事は、東京都サーバより、市区町村CSに対して整合性確認結果を通知する。	事後	概要図、記載内容の明確化
平成31年3月13日	II 特定個人情報ファイルの概要/2. 基本情報/⑤保有開始日	平成27年6月予定	平成27年6月	事後	時点修正

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
平成31年3月13日	Ⅱ 特定個人情報ファイルの概要/3. 特定個人情報の入手・使用/⑧使用方法	【Ⅰ 本人確認情報の更新(最新化)での使用】 市区町村長からの住民票の記載事項の変更又は新規作成の通知を受け(既存住基システム→市区町村CS→東京都サーバ)、都道府県知事保存本人確認情報ファイルを更新し、機構に対して当該本人確認情報の更新情報を通知する(東京都サーバ→全国サーバ)。 【Ⅱ 東京都の執行機関へ本人確認情報の提供(法令又は条例に基づく事務)で使用】 東京都の執行機関からの本人確認情報の照会要求を受け(東京都の執行機関→東京都サーバ)、照会のあった住民票コード、個人番号又は4情報の組合せを元に都道府県知事保存本人確認情報ファイルを検索し、該当する個人の本人確認情報を照会元へ提供する(東京都サーバ→東京都の執行機関)。 【Ⅲ 東京都内の市区町村の市区町村長その他の執行機関へ本人確認情報の提供(条例に基づく事務)で使用】 東京都内の市区町村の市区町村長その他の執行機関からの本人確認情報の照会要求を受け(東京都内の市区町村の市区町村長その他の執行機関→東京都サーバ)、照会のあった住民票コード、個人番号又は4情報の組合せを元に都道府県知事保存本人確認情報ファイルを検索し、該当する個人の本人確認情報を照会元へ提供する(東京都サーバ→東京都内の市区町村の市区町村長その他の執行機関)。	【Ⅰ 本人確認情報の更新(最新化)】 市区町村長からの住民票の記載事項の変更又は新規作成の通知を受け(既存住基システム→市区町村CS→東京都サーバ)、都道府県知事保存本人確認情報ファイルを更新し、機構に対して当該本人確認情報の更新情報を通知する(東京都サーバ→全国サーバ)。 【Ⅱ 東京都の他の執行機関(又は他部署への提供・移転)】 法令に定められた個人番号取扱事務を実施する必要上、東京都の他の執行機関又は他部署からの本人確認情報の照会要求を受け(東京都の他の執行機関又は他部署→東京都サーバ)、照会のあった住民票コード、個人番号又は4情報の組合せを元に都道府県知事保存本人確認情報ファイルを検索し、該当する本人確認情報を照会元へ提供する(東京都サーバ→東京都の他の執行機関又は他部署)。 【Ⅲ 住民からの開示請求に係る対応】 住民からの開示請求に基づき(住民→東京都の窓口→東京都サーバ)、当該住民の本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、書面により提供する(東京都サーバ→帳票出力→住民)。	事後	住基法・都条例改正に伴う修正

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
平成31年3月13日	Ⅱ 特定個人情報ファイルの概要 要/3. 特定個人情報の入手・使用/⑧使用方法	【Ⅳ 住民からの開示請求での使用】 住民からの開示請求に基づき(住民→東京都の窓口→東京都サーバ)、当該住民の本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、書面により提供する(東京都サーバ→帳票出力→住民)。 【Ⅴ 住民基本台帳法に定められた事務での照会業務での使用】 4情報(氏名、住所、性別、生年月日)の組合せをキーに都道府県知事保存本人確認情報ファイルの検索を行う。 【Ⅵ 住民基本台帳ネットワークシステム情報の整合性確認での使用】 都道府県知事保存本人確認情報ファイルの正確性を担保するため、市区町村から本人確認情報を受領し(市区町村CS→東京都サーバ)、当該本人確認情報を用いて都道府県知事保存本人確認情報ファイルに記録された本人確認情報の整合性確認を行う。	【Ⅳ 住民基本台帳法に定められた事務での照会業務における使用】 4情報(氏名、住所、性別、生年月日)の組合せをキーに都道府県知事保存本人確認情報ファイルの検索を行う。 【Ⅴ 住民基本台帳ネットワークシステム情報の整合性確認】 都道府県知事保存本人確認情報ファイルの正確性を担保するため、市区町村から本人確認情報を受領し(市区町村CS→東京都サーバ)、当該本人確認情報を用いて都道府県知事保存本人確認情報ファイルに記録された本人確認情報について、整合性確認を行う。	事後	住基法・都条例改正に伴う修正
平成31年3月13日	Ⅱ 特定個人情報ファイルの概要 要/3. 特定個人情報の入手・使用/⑧使用方法/情報の突合	【上記 Ⅰ】 ・都道府県知事保存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都道府県知事保存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。 【上記 Ⅱ、Ⅲ、Ⅴ】 ・東京都の執行機関等からの照会に基づいて本人確認情報を提供する際に、照会元から受信した対象者の4情報等との突合を行う。	【上記 Ⅰ】 ・都道府県知事保存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都道府県知事保存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。 【上記 Ⅱ、Ⅳ】 ・東京都の他の執行機関又は他部署からの照会に基づいて本人確認情報を提供する際に、照会元から受信した対象者の4情報等との突合を行う。	事後	住基法・都条例改正に伴う修正
平成31年3月13日	Ⅱ 特定個人情報ファイルの概要 要/3. 特定個人情報の入手・使用/⑧使用方法/情報の突合	【上記 Ⅳ】 ・請求に基づいて本人確認情報を開示する際に、開示請求者から受領した本人確認情報との突合を行う。 【上記 Ⅵ】 ・市区町村CSとの整合処理を実施するため、4情報等との突合を行う。	【上記 Ⅲ】 ・住民からの請求に基づいて本人確認情報を開示する際に、請求者から受領した本人確認情報との突合を行う。 【上記 Ⅴ】 ・市区町村CSとの整合処理を実施するため、4情報等との突合を行う。	事後	住基法・都条例改正に伴う修正

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
平成31年3月13日	Ⅱ 特定個人情報ファイルの概 要/4. 特定個人情報ファイルの取扱いの委託/委託事項1/②取扱いを委託する特定個人情報ファイル/その妥当性	委託業務の内容は、「①委託内容」とおり特定個人情報ファイル(都道府県知事保存本人確認情報ファイル)が保存される東京都サーバの運用及び監視業務とするため、本人確認情報を扱う事務は実施しない。	都道府県職員のサーバ管理に係る運用負担の軽減、都道府県サーバ導入費及び維持管理費の削減、セキュリティ水準の向上の観点から、集約センターにおいて一元的に運用している。 運用については、住基ネットについてのシステム設計やセキュリティに関する専門的な知識と、運用するサーバやネットワーク機器に関する高度な技術力を有する地方公共団体情報システム機構に委託している。	事後	集約管理の経緯について記載
平成31年3月13日	Ⅱ 特定個人情報ファイルの概 要/5. 特定個人情報の提供・移転(委託に伴うものを除く。)/提供先2	東京都の他の執行機関	東京都の他の執行機関(下水道局、東京消防庁、東京都教育委員会)	事後	提供先を明示
平成31年3月13日	Ⅱ 特定個人情報ファイルの概 要/5. 特定個人情報の提供・移転(委託に伴うものを除く。)/提供先3	東京都内の市区町村の市区町村長その他の執行機関		事後	住基法・都条例改正に伴う削除
平成31年3月13日	Ⅱ 特定個人情報ファイルの概 要/5. 特定個人情報の提供・移転(委託に伴うものを除く。)/提供先1	東京都の他の部署	東京都の他の部署(総務局人事部、主税局(課税部、徴収部、都税事務所、都税事務総合センター)、生活文化局都民生活部、環境局環境改善部、福祉保健局(医療政策部、保健政策部、生活福祉部、少子社会対策部、障害者施策推進部)、産業労働局(商工部、観光部))※計53か所	事後	移転先を明示
平成31年3月13日	Ⅱ 特定個人情報ファイルの概 要/6. 特定個人情報の保管・消去/①保管場所	セキュリティゲートにて入退館管理をしている都道府県サーバの集約センターにおいて、施錠管理及び入退室管理(監視カメラを設置してサーバ設置場所への入退室者を特定・管理)を行っている部屋に設置したサーバ内に保管する。サーバへのアクセスはID/パスワードによる認証が必要となる。	【東京都サーバ】 セキュリティゲートにて入退館管理をしている都道府県サーバの集約センターにおいて、施錠管理及び入退室管理(監視カメラを設置してサーバ設置場所への入退室者を特定・管理)を行っている部屋に設置したサーバ内に保管する。サーバへのアクセスはID/パスワードによる認証が必要となる。 【電子記録媒体】 総務局行政部から貸与する指定のDVD-RWに暗号化の上格納し、施錠が出来る金庫等に保管する。 【紙】 各所属において、施錠が出来る金庫等に保管する。	事後	記載の明確化

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31年3月13日	II 特定個人情報ファイルの概要 要/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後の本人確認情報は、本人確認情報の提供のため、市区町村CSを通じて新たに記載の修正の通知を受けるまで保管する必要がある。 ・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30条の6（都道府県における本人確認情報の保存期間）に定める期間（履歴の情報：5年間、消除者の情報：原則5年間（最長80年間））保管する必要がある。	【東京都サーバ】 9)20年以上 ・住民票の記載の修正後の本人確認情報は、本人確認情報の提供のため、市区町村CSを通じて新たに記載の修正の通知を受けるまで保管する必要がある。 ・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、住基法施行令第30条の6（都道府県における本人確認情報の保存期間）に定める期間（150年間）保管する。 【電子記録媒体】 1)1年未満 データの受け渡し又は利用が終了した場合、速やかにデータを消去する。 【紙】 10)定められていない 利用事務での文書保存期間終了後又は各所属で利用が終了した場合、速やかに廃棄する。	事後	記載の明確化
平成31年3月13日	II 特定個人情報ファイルの概要 要/6. 特定個人情報の保管・消去/②保管期間/消去方法	都道府県知事保存本人確認情報ファイルに記載されたデータをシステムにて自動判別し、復元できないように消去する仕組みになっている。	【東京都サーバ】 都道府県知事保存本人確認情報ファイルに記載されたデータをシステムにて自動判別し、復元できないように消去する仕組みになっている。 東京都サーバのハードディスク等は地方公共団体情報システム機構により、物理的に利用できなくした上、廃棄される。 【電子記録媒体】 総務局行政部から貸与する指定のDVD-RWのみ使用を認めており、書き込みができなくなったり、不要となった媒体については、総務局行政部にて回収の上、物理的に破壊し、廃棄記録をつけている。 【紙】 シュレッダー又は溶解処分により確実に廃棄を行っている。	事後	記載の明確化

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31年3月13日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策/2. 特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。)/リスク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	法令により、市区町村から通知を受けることとされている情報のみを入手できることを、住民基本台帳ネットワークシステムのシステム上で担保する。	住民基本台帳法第30条の6により、市区町村から通知を受けることとされている情報のみを入手できることを、住民基本台帳ネットワークシステムのシステム上で担保する。	事後	記載の明確化
平成31年3月13日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策/2. 特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。)/リスク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市町村CSIに限定することを、住民基本台帳ネットワークシステムのシステム上で担保する。	本人確認情報の入手元を市区町村CSIに限定することを、専用線の都内ネットワークにより実現し、住民基本台帳ネットワークシステムのシステム上で担保する。	事後	記載の明確化
平成31年3月13日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策/2. 特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。)/リスク4:入手の際に特定個人情報が漏えい・紛失するリスク/リスクに対する措置の内容	・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。 ・市区町村CSと接続するネットワーク回線に専用回線を用いる、情報の暗号化を実施する、操作者の認証を行う等の措置を講じる。 ・特定個人情報の入手は、システム上自動処理にて行われるため、操作者は存在せず人為的なアクセスが行われることはない。 ※都道府県サーバ上で稼動するアプリケーション。 これにより、都内の市区町村の住民の本人確認情報を管理し、市区町村CSや全国サーバとのデータ交換を行う。 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。	・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。 ・市区町村CSと接続するネットワーク回線に専用回線を用いる、情報の暗号化を実施する、操作者の認証を行う等の措置を講じる。 ※都道府県サーバ上で稼動するアプリケーション。 これにより、都内の市区町村の住民の本人確認情報を管理し、市区町村CSや全国サーバとのデータ交換を行う。 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。	事後	記載の明確化

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31年3月13日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク 対策/3. 特定個人情報の使用/リスク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/ユーザー認証の管理/具体的な管理方法	生体認証(左右の手の静脈)によるユーザー認証を行っている。	生体認証によるユーザー認証を行っている。	事後	記載の簡素化
平成31年3月13日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク 対策/3. 特定個人情報の使用/リスク2: 権限のない者(元職員、アクセス権限のない職員等)によって不正に使用されるリスク/アクセス権限の管理/具体的な管理方法	・操作者の権限等に応じたアクセス権限が付与されるよう管理する。 ・不正アクセスを分析するために、検索サブシステム及び業務端末においてアプリケーションの操作履歴の記録を取得し、保管する。	・操作者の権限等に応じたアクセス権が付与されるよう管理する。 ・不正アクセスを分析するために、業務端末におけるアプリケーションの操作ログ、アクセスログを取得し、保管する。	事後	記載の明確化
平成31年3月13日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク 対策/3. 特定個人情報の使用/リスク2: 権限のない者(元職員、アクセス権限のない職員等)によって不正に使用されるリスク/特定個人情報の使用の記録/具体的な方法	・本人確認情報を扱うシステムの操作履歴(アクセスログ・操作ログ)を記録する。 ・不正な操作が無いことについて、操作履歴により適時確認する。 ・操作履歴の確認により本人確認情報の検索に関して不正な操作の疑いがある場合は、申請文書等との整合性を確認する。 ・バックアップされた操作履歴について、定められた期間、安全な場所に施錠保管する。	・本人確認情報を扱うシステムの操作履歴(アクセスログ・操作ログ)を記録する。 ・ログを総務局行政部にて分析し、確認を実施する。 ・不正な操作が無いことについて、操作履歴により適時確認する。 ・操作履歴の確認により本人確認情報の検索に関して不正な操作の疑いがある場合は、申請文書等との整合性を確認する。 ・バックアップされた操作履歴について、一定期間、安全な場所に施錠保管する。	事後	ログの分析を記載
平成31年3月13日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク 対策/3. 特定個人情報の使用/リスク4: 特定個人情報ファイルが不正に複製されるリスク/リスクに対する措置の内容	システム上、管理権限を与えられた者以外、情報の複製は行えない仕組みとする。 また、定期運用に基づくバックアップ以外にファイルを複製しないよう、従業員に対し指導する。	システム上、管理権限を与えられた者以外、情報の複製は行えない仕組みとする。 システムを利用する職員への研修会において、複製の禁止等について指導する。 また、定期運用に基づくバックアップ以外にファイルを複製しないよう、委託先等の従業員に対し指導する。	事後	複製禁止の指導を記載

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31年3月13日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策/3. 特定個人情報の使用/特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	その他、特定個人情報の使用にあたり、以下の措置を講じている。 【端末利用】 ①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することを防止する ②代表端末及び業務端末のディスプレイを、来庁者から見えない位置に設置する ③本人確認情報が表示された画面のハードコピーの取得は事務処理に必要となる範囲にとどめるよう指導している ④大量のデータ出力に際しては、事前に管理責任者の承認を得よう指導している 【住民対応】 ①本人確認情報の開示・訂正の請求により、住民が特定個人情報の正確性等を確認できる ②本人確認情報の提供状況の開示請求により、住民が特定個人情報の提供先等を確認できる	その他、特定個人情報の使用にあたり、以下の措置を講じている。 【端末利用】 ①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することを防止する ②代表端末及び業務端末のディスプレイを、来庁者から見えない位置に設置する ③ディスプレイに覗き見防止シートを取り付ける ③本人確認情報が表示された画面のハードコピーの取得ができないよう設定している ④大量のデータ出力に際しては、事前に管理責任者の承認を得よう指導している 【住民対応】 ①本人確認情報の開示・訂正の請求により、住民が特定個人情報の正確性等を確認できる ②本人確認情報の提供状況の開示請求により、住民が特定個人情報の提供先等を確認できる	事後	覗き見防止シートの設置、スクリーンショットの制限設定を記載
平成31年3月13日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策/4. 特定個人情報ファイルの取扱いの委託/情報管理体制の確認	契約後、秘密保持に関する誓約書とあわせて、委託先の管理体制図、連絡先一覧等を提出させている。	契約後、秘密保持に関する誓約書とあわせて、委託先の管理体制図、連絡先一覧等を提出させている。 また、Pマークを取得していることを確認している。	事後	Pマーク確認を記載
平成31年3月13日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策/4. 特定個人情報ファイルの取扱いの委託/特定個人情報の提供ルール/委託から他者の提供に関するルールの内容及びルール順守の確認方法	特定個人情報の提供は一切認めていない。	契約上、特定個人情報の提供は一切認めていない。 操作ログ、検案件数の取得により確認している。	事後	記載の明確化

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31年3月13日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策/4. 特定個人情報ファイルの取扱いの委託/特定個人情報の提供ルール/委託元と委託先間の提供に関するルール内容及びルール順守の確認方法	ー(特定個人情報の提供は一切認めていない。)	下記を定めた仕様書を用いて契約を行っている。 ・秘密の保持 ・目的外利用の禁止 ・複写・複製の禁止 ・持ち出しの禁止 ・情報の管理及び保管のための安全管理措置を講じる義務(入退室管理、施錠管理、契約解除時等の消去、事故報告等) ・機密情報取扱いに関する教育及び研修の実施 ・再委託に関する取扱い(再委託の許諾、委託先と同等の遵守義務、誓約書の提出等) ・実地調査及び改善の指示	事後	契約内容を記載
平成31年3月13日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策/4. 特定個人情報ファイルの取扱いの委託/特定個人情報の消去ルール/ルール内容及びルール順守の確認方法	委託先には、特定個人情報の更新／閲覧権限を付与していないため、消去は障害対応、機器更新等での機器交換(ディスク故障含む)時のみとなる。 破損や耐用年数を過ぎた媒体は、管理簿に理由を明記し保管庫に格納している。 保管状況を週次で管理簿と現物の点検を実施し、月次報告を行っている。	委託先には、特定個人情報の更新／閲覧権限を付与していないため、消去は障害対応、機器更新等での機器交換(ディスク故障含む)時のみとなる。 破損や耐用年数を過ぎた媒体(ハードディスク等)は、委託先が管理簿に理由を明記し物理的に廃棄している。 保管状況を週次で管理簿と現物の点検を実施し、月次報告を行っている。	事後	記載の明確化
平成31年3月13日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策/4. 特定個人情報ファイルの取扱いの委託/再委託先による特定個人情報ファイルの適切な取扱いの確保/具体的な方法	ー(再委託先が、特定個人情報ファイルを取り扱えないように特定個人情報の更新／閲覧権限を付与していない。)	契約上、特定個人情報の取扱いについて委託先が順守すべき事項を再委託先・再々委託先においても遵守すべき旨定めるとともに、再委託・再々委託承諾の際、再委託先等から同事項を遵守する旨の誓約書を徴している。また、必要に応じ、再委託先に対しても必要な実地調査や指示を行うことができることとしている。 また、再委託先等に対しては、東京都サーバ内の特定個人情報の更新／閲覧権限を付与していない。	事後	記載の明確化
平成31年3月13日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策/5. 特定個人情報の提供・移転(委託や情報提供ネットワークシステムを通じた提供を除く。)/リスク1:不正な提供・移転が行われるリスク/特定個人情報の提供・移転の記録/具体的な方法	住民基本台帳ネットワークシステムを通じて特定個人情報(個人番号、4情報等)の提供・移転を行っており、特定個人情報(個人番号、4情報等)の提供・移転に係る処理を行った際、記録(日時、操作者等)をシステム上で管理し保存する。(ログの削除は行わない。)	住民基本台帳ネットワークシステムを通じて特定個人情報(個人番号、4情報等)の提供・移転を行っており、特定個人情報(個人番号、4情報等)の提供・移転に係る処理を行った際、記録(日時、操作者等)をシステム上で管理し保存する。	事後	記載の明確化

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31年3月13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 策/5. 特定個人情報の提供・移転(委託や情報提供ネットワークシステムを通じた提供を除く。)/リスク1:不正な提供・移転が行われるリスク/特定個人情報の提供・移転に関するルール/ルール内容及びルール順守の確認方法	住民基本台帳法第30条の7(都道府県から機構へ本人確認情報の通知等) 住民基本台帳法第30条の15第1項(本人確認情報の利用) 電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準 東京都住民基本台帳ネットワークシステム運用管理規程	以下の法令等に従い特定個人情報の提供・移転を行っている。 ・住民基本台帳法第30条の7(都道府県から機構へ本人確認情報の通知等) ・住民基本台帳法第30条の15第1項(本人確認情報の利用) ・電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準 ・東京都住民基本台帳ネットワークシステム運用管理規程 操作ログを分析し、不正な操作がなされていないか確認を行っている。	事後	記載の明確化
平成31年3月13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 策/5. 特定個人情報の提供・移転(委託や情報提供ネットワークシステムを通じた提供を除く。)/リスク2:不適切な方法で提供・移転が行われるリスク/リスクに対する措置の内容	相手方(全国サーバ)と東京都サーバの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。 また、東京都の他の執行機関への提供及び他の部署への移転のため、媒体へ出力する必要がある場合には、情報を暗号化し逐一出力の記録が残される仕組みを構築している。	全国サーバと東京都サーバの間の通信では専用線を用い相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。 また、東京都の他の執行機関への提供及び他の部署への移転のため、外部記録媒体へ出力する必要がある場合には、情報を暗号化し逐一出力の記録が残される仕組みを構築している。	事前	記載の明確化
平成31年3月13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 策/5. 特定個人情報の提供・移転(委託や情報提供ネットワークシステムを通じた提供を除く。)/リスク3:誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク/リスクに対する措置の内容	・誤った情報を提供・移転してしまうリスクへの措置 :システム上、照会元から指定された検索条件に基づき得た結果を適切に提供することを担保する。 ・誤った相手に提供・移転してしまうリスクへの措置 :相手方(全国サーバ)と東京都サーバの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。 また、情報を暗号化し格納した媒体による情報の提供・移転が必要な場合には文書による確認を実施し、法令上の根拠のない相手先へ情報の提供・移転を防止している。	・誤った情報を提供・移転してしまうリスクへの措置 :システム上、照会元から指定された検索条件に基づき得た結果を適切に提供・移転することを担保する。 ・誤った相手に提供・移転してしまうリスクへの措置 :全国サーバと東京都サーバの間の通信では専用線を用い相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。 また、情報を暗号化し格納した媒体による情報の提供・移転が必要な場合には文書による確認を実施し、法令上の根拠のない相手先へ情報の提供・移転を防止している。		記載の明確化

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31年3月13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/具体的な対策の内容	主に下記の対策を講じている。 ・ファイアウォールの導入、ログの解析 ・専用回線の利用 ・データの暗号化 ・サーバ間の相互認証 ・ウイルス対策ソフト(定期的なパターンファイルの更新)	・ウイルス対策ソフトの定期的なパターン更新を実施している。 ・庁内のネットワークにおいて、ファイアウォールを導入しログの解析を行っている。 ・専用回線を利用し、データを暗号化してやり取りしている。 ・サーバ間の相互認証を行っている。 ・集約センターにおいて、ファイアウォールを導入し、ログの解析を行っている。		記載の明確化
平成31年3月13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1/⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか/その内容	東京都防災(語学)ボランティアに関する事務において、平成26年10月15日(水曜日)、業務委託業者が研修の案内に関する通知をメール送信する際、データ設定の誤りに気付かず、769名分のメールについて、本人以外の1名分の氏名が宛先に表示されてしまった。 ※ 住民基本台帳ネットワークシステムに係る本人確認情報の管理及び提供等に関する事務においては、個人情報に関する重大事故の発生はない。	① 平成28年4月21日、事務担当者が「海の森友の会通信」をメールで送信する際、全員のメールアドレス443件をbcc欄ではなく、誤って宛先欄に入力し、送信してしまった。 ② 平成28年9月16日、都が委託している私立高等学校等就学支援金の審査に係る事務において、再委託先が、審査に係る生徒保護者への書類を、誤った住所に送付した。送付書類は、書類に不備がある生徒保護者に対し、不足書類の提出期限等を連絡するものであり、生徒の氏名及び就学支援金認定番号が含まれていた。 ③ 平成29年1月17日、都民の健康と安全を確保する環境に関する条例に基づき、排出量取引に利用する指定管理口座の名義人情報を環境局ホームページで公表している。個人情報については希望する場合に公表するものとしているが、公表を希望しない個人の名義人情報(8指定口座396名分)がホームページで閲覧可能な状況になっており、個人情報が流出した。 ④ 平成29年3月10日、都税のクレジットカード納付を行うために受託事業者が運営している「都税クレジットカードお支払サイト」について、ソフトウェアの脆弱性に起因する第三者による不正アクセスが確認され、サーバ上に保持していたクレジットカード番号及び有効期限(36万4,181件)メールアドレス(36万2,049件)の情報を不正に取得されていたことが判明した。		時点修正

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
平成31年3月13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1/⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか/その内容	東京都防災(語学)ボランティアに関する事務において、平成26年10月15日(水曜日)、業務委託業者が研修の案内に関する通知をメール送信する際、データ設定の誤りに気付かず、769名分のメールについて、本人以外の1名分の氏名が宛先に表示されてしまった。 ※ 住民基本台帳ネットワークシステムに係る本人確認情報の管理及び提供等に関する事務においては、個人情報に関する重大事故の発生はない。	⑤平成29年9月1日、一般財団法人東京マラソン財団から海外メディア記者126名に対し、東京マラソンの申込者数についてプレスリリースのメール配信を実施した際、記者126名のメールアドレスを誤ってbccではなくccに入力し、メールアドレスが表示された状態で一斉送信してしまった。 ⑥平成29年11月29日、建設局職員が出張先において、所属職員324名分の個人情報を記載した緊急連絡網等が入った鞆を置いたまま移動し、紛失した。 ⑦平成30年4月24日、上野動物園で行った動物の観覧抽選に関し、指定管理者の委託先事業者が当選ハガキ上を発送したところ、内209件について、「代表者氏名」「同行者氏名」の全部または一部に他の当選者(代行者・同行者)の氏名が記載されていた。 ⑧平成30年9月21日、公益財団法人東京都公園協会が、委託事業者(131社)に電子メールを送信する際に、誤って委託事業者のメールアドレスを「宛先」欄へ入力し送信した結果、委託事業者(131社)の会社名、担当者名及びメールアドレスが送信先に漏えいした。		時点修正
平成31年3月13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1/⑨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/再発防止策の内容	東京都防災(語学)ボランティアに関する事務において、委託業務を見直し、今回のミスの元となった作業を不要としたほか、委託業者に対し、複数名での最終確認の徹底、個人情報の取扱いに関する指示系統の確認を指示した。また、庁内全部局に対し、委託事業者における保有個人情報の安全管理の徹底を注意喚起する。	① 事故発生の翌日(4月22日)緊急に港湾局情報セキュリティ委員会を開催し、各委員に対し事故の概要報告及び情報セキュリティ対策の更なる徹底について、部署内職員に対し周知徹底するよう指示した。また、当局監理団体及び報告団体に対して、総務課長より電話で、事故の概要報告及び情報セキュリティ対策の更なる徹底について指示した。 今後も、情報セキュリティ委員会などあらゆる機会をとらえて、都民の方等へメールによる連絡等を行う場合は、複数の担当者により送信先について確認するよう、定期的な注意喚起を徹底する。 ② 個人情報等の適正管理について事例等を通じて知識を習得し、適正な職務の執行を図るため、職員及び委託先職員を対象に個人情報保護研修を行った。生活文化局情報セキュリティ委員会において、各部署の庶務担当課長に対し、今回の事故について報告し、再発防止に努めるよう注意喚起を行う。また、業務全般について個人情報の管理方法を総点検し、事務改善を行う。		時点修正

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
平成31年3月13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1/⑨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/再発防止策の内容	東京都防災(語学)ボランティアに関する事務において、委託業務を見直し、今回のミスの元となった作業を不要としたほか、委託業者に対し、複数名での最終確認の徹底、個人情報の取扱いに関する指示系統の確認を指示した。また、庁内全部局に対し、委託事業者における保有個人情報の安全管理の徹底を注意喚起する。	③ システム改修により、出力した口座一覧を所属内で回付・確認する体制を構築する。環境局内で本件について周知し、職員に対し改めて個人情報の適切な取扱いについて徹底するよう注意喚起をした。環境局所管のホームページにおいて公表している情報について、公表理由や公表の適否等を確認する点検を実施した。 情報セキュリティ委員会事故対策部会を開催し、事故の原因の確認及び再発防止策について検討を行った。 ④ ソフトウェアの脆弱性について修正を行うとともに、サイト全体の安全性を総点検し、システム変更やサーバ監視体制の強化を実施した。カード情報やメールアドレスは、サーバ内に保持しない等の措置を講じた。サイトの運用面においては、運用基準を見直し、危機管理体制を強化した。 今後も安全なサイト運営のために、セキュリティ対策の強化を継続して実施する。		時点修正
平成31年3月13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1/⑨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/再発防止策の内容	東京都防災(語学)ボランティアに関する事務において、委託業務を見直し、今回のミスの元となった作業を不要としたほか、委託業者に対し、複数名での最終確認の徹底、個人情報の取扱いに関する指示系統の確認を指示した。また、庁内全部局に対し、委託事業者における保有個人情報の安全管理の徹底を注意喚起する。	⑤財団事務局長による職員への事案周知、情報管理に関する注意喚起を行うとともに、複数人への同時メール送信におけるccの使用原則禁止とした。また、情報管理に関する財団全職員悉皆の研修を緊急に実施した。 ⑥「建設局個人情報漏えい事故等対策本部」を設置し、本件周知と再発防止についての検討を行った上で、同日、局内に対し通知を发出し、建設局個人情報安全管理基準の趣旨を踏まえ、事故防止に向けて万全を期すよう局内に周知した。 ⑦「建設局個人情報漏えい事故等対策本部」を設置し、本件周知と再発防止についての検討を行った上で、同日、局内に通知を发出し、建設局個人情報安全管理基準の趣旨を踏まえ、事故防止に向けて万全を期すよう局内に周知した。また、他の監理団体及び指定管理者に対しても、同様の事故が起きないように指導した。 ⑧東京都公園協会において、個人情報の取扱いの徹底など周知するとともに、職員に対しても本件周知と情報管理の徹底を指示した。建設局においても、「建設局個人情報漏えい事故等対策本部」を設置し、本件周知と再発防止を徹底した。		時点修正

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
平成31年3月13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	【ファイル上の個人ごとの消去】 ・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法令（住民基本台帳法施行令第30条の6）に定める保存期間を経過した後に系統的に消去する。 【物理的なファイル全体の消去】 ・磁気ディスクの廃棄時は、要領・手順書等に基づき、内容の消去、破壊等を行うとともに、磁気ディスク管理簿にその記録を残す。また、専用ソフトによるフォーマット、物理的粉碎等を行うことにより、内容を読み出すことができないようにする。	【ファイル上の個人ごとの消去】 ・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法令（住民基本台帳法施行令第30条の6）に定める保存期間（150年）を経過した後にシステムにて自動的に消去する。 【物理的なファイル全体の消去】 ・磁気ディスクの廃棄時は、要領・手順書等に基づき、内容の消去、破壊等を行うとともに、磁気ディスク管理簿にその記録を残す。また、専用ソフトによるフォーマット、物理的粉碎等を行うことにより、内容を読み出すことができないようにする。		記載の明確化
平成31年3月13日	V 開示請求、問合せ/特定個人情報の開示・訂正・利用停止要求/③手数料等/手数料額・納付方法	納付書により、実費相当分（20円/1枚）の手数料を納付する。	納付書により、実費相当分（10円/1枚）の手数料を納付する。		条例改正
令和5年11月30日	表紙 評価書名	住民基本台帳ネットワークシステムに係る本人確認情報の管理及び提供等に関する事務 全項目評価書	住民基本台帳ネットワークに関する事務 全項目評価書		
令和5年11月30日	表紙 個人のプライバシー等の権利利益保護の宣言	東京都知事は、住民基本台帳ネットワークシステムに係る本人確認情報の管理及び提供等に関する事務において個人番号を利用するにあたり、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んでいることを宣言する。	東京都知事は、住民基本台帳ネットワークに関する事務において個人番号を利用するにあたり、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んでいることを宣言する。		
令和5年11月30日	I 基本情報 1. ①事務の名称	住民基本台帳ネットワークシステムに係る本人確認情報の管理及び提供等に関する事務	住民基本台帳ネットワークに関する事務		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	I 基本情報 1. ②事務の内容	都道府県は、住民基本台帳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ができるシステムとして住民基本台帳ネットワークシステムを市区町村と共同して構築している。 なお、住民基本台帳は、住民基本台帳法に基づき作成されるものであり、市区町村における住民の届出に関する制度及びその住民たる地位を記録する各種の台帳に関する制度を一元化し、もって、住民の利便を増進するとともに行政の近代化に対処するため、住民に関する記録を正確かつ統一的行うものであり、市区町村において、住民の居住関係の公証、選挙人名簿の登録、その他住民に関する事務の処理の基礎となるものである。	住民基本台帳ネットワークに関する事務は、「1. 本人確認情報の管理及び提供等に関する事務」及び「2. 附票本人確認情報の管理及び提供等に関する事務」に分かれる。 1. 本人確認情報の管理及び提供等に関する事務 都道府県は、住民基本台帳法（以下「住基法」という。）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（住基ネット）を市町村と共同して構築している。 なお、住民基本台帳は、住基法に基づき作成されるものであり、市町村における住民の届出に関する制度及びその住民たる地位を記録する各種の台帳に関する制度を一元化し、もって、住民の利便を増進するとともに行政の近代化に対処するため、住民に関する記録を正確かつ統一的行うものであり、市町村において、住民の居住関係の公証、選挙人名簿の登録、その他住民に関する事務の処理の基礎となるものである。		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	I 基本情報 1. ②事務の内容	具体的に東京都では、「住民基本台帳法及び住民サービスの向上と行政事務の効率化を図るために住民基本台帳ネットワークシステムの本人確認情報を利用する事務等を定める条例」(以下「都条例」という。)の規定に従い、特定個人情報(行政手続きにおける特定の個人を識別するための番号の利用等に関する法律第2条第8項)を以下の事務で取り扱う。 ①磁気ディスクによる特定個人情報ファイルの管理 ②市区町村からの本人確認情報(住民基本台帳法第3条の6)に係る変更の通知に基づく特定個人情報ファイルの更新及び地方公共団体情報システム機構(以下「機構」という。)への通知 ③都知事から都のその他の執行機関への本人確認情報の提供 ④住民による請求に基づく当該個人の本人確認情報の開示並びに開示結果に基づく住民からの本人確認情報の訂正、追加又は削除の申出に対する調査 ⑤機構への本人確認情報の照会	具体的に東京都では、住基法及び「住民サービスの向上と行政事務の効率化を図るために住民基本台帳ネットワークシステムの本人確認情報を利用する事務等を定める条例」(以下「都条例」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磁気ディスクによる特定個人情報ファイルの管理 ②区市町村からの本人確認情報に係る変更の通知に基づく特定個人情報ファイルの更新及び機構への通知 ③都知事から本人確認情報に係る東京都の他の執行機関への提供又は他部署への移転 ④住民による請求に基づく当該個人の本人確認情報の開示並びに開示結果に基づく住民からの本人確認情報の訂正、追加又は削除の申出に対する調査 ⑤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		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	I 基本情報 1. ②事務の内容	—	2. 附票本人確認情報の管理及び提供等に関する事務 都道府県は、市町村における市町村コミュニケーションサーバ(以下「CS」という。)、都道府県における附票都道府県サーバ及び機構における附票全国サーバ等により構成される「附票連携システム」において、国外転出者に係る本人確認を行うための社会的基盤としての役割を担うため、4情報(氏名、住所、生年月日、性別)、住民票コード及びこれらの変更情報で構成される「都道府県知事保存附票本人確認情報ファイル」を作成し、戸籍の附票に関する記録を正確に行う責務がある。そのため、附票本人確認情報の管理及び提供等に係る以下の事務を実施する。なお、都道府県知事保存附票本人確認情報(以下条文に併せて記載する場合は、「都道府県知事保存附票本人確認情報」とし、それ以外の記載は、「附票本人確認情報」とする。)には、個人番号は含まれない。 ①磁気ディスクによる特定個人情報ファイルの管理 ②区市町村からの附票本人確認情報に係る変更の通知に基づく特定個人情報ファイルの更新及び機構への通知 ③都知事から附票本人確認情報に係る東京都の他の執行機関への提供又は他部署への移転 ④住民による請求に基づく当該個人の附票本人確認情報の開示並びに開示結果に基づく住民からの附票本人確認情報の訂正、追加又は削除の申出に対する調査 ⑤機構への附票本人確認情報の照会		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	I 基本情報 2. システム1 ②システムの機能	1. 本人確認情報の更新に関する事務 :都道府県知事保存本人確認情報ファイル(住民基本台帳法第30条の8)を最新の状態に保つため、市区町村CSを経由して通知された本人確認情報の更新情報を元に当該ファイルを更新し、全国サーバに対して当該本人確認情報の更新情報を通知する。 2. 東京都の他の執行機関(東京消防庁など)への情報提供又は他部署への移転 :東京都の他の執行機関又は他部署における住民基本台帳法に基づく情報照会に対応するため、照会のあった当該個人の個人番号又は4情報(氏名、住所、性別、生年月日)等に対応する本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、照会元に提供・移転する。 3. 本人確認情報の開示に関する事務 :法律に基づく住民による自己の本人確認情報の開示請求に対応するため、当該個人の本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、帳票に出力する。	1. 本人確認情報の更新 :都道府県知事保存本人確認情報ファイルを最新の状態に保つため、区市町村CSを経由して通知された本人確認情報の更新情報を元に当該ファイルを更新し、全国サーバに対して当該本人確認情報の更新情報を通知する。 2. 東京都の他の執行機関への情報提供又は他部署への移転 :東京都の他の執行機関又は他部署による住民基本台帳法に基づく情報照会に対応するため、照会のあった当該個人の個人番号又は4情報(氏名、住所、性別、生年月日)等に対応する本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、照会元に提供・移転する。 3. 本人確認情報の開示 :法律に基づく住民による自己の本人確認情報の開示請求に対応するため、当該個人の本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、帳票に出力する。		
令和5年11月30日	I 基本情報 2. システム1 ②システムの機能	4. 機構への情報照会に係る事務 :全国サーバに対して住民票コード、個人番号又は4情報の組合せをキーとした本人確認情報照会要求を行い、該当する個人の本人確認情報を受領する。 5. 本人確認情報検索に関する事務 :東京都サーバの代表端末又は業務端末において入力された4情報の組合せをキーに都道府県知事保存本人確認情報ファイルを検索し、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。 6. 本人確認情報整合 :都道府県知事保存本人確認情報ファイルの正確性を担保するため、市区町村から本人確認情報を受領し、当該本人確認情報を用いて当該ファイルに記録された本人確認情報の整合性確認を行う。	4. 機構への情報照会 :全国サーバに対して住民票コード、個人番号又は4情報の組合せをキーとした本人確認情報照会要求を行い、該当する個人の本人確認情報を受領する。 5. 本人確認情報検索 :東京都サーバの代表端末又は業務端末において入力された4情報の組合せをキーに都道府県知事保存本人確認情報ファイルを検索し、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。 6. 本人確認情報整合 :都道府県知事保存本人確認情報ファイルの正確性を担保するため、区市町村から本人確認情報を受領し、当該本人確認情報を用いて当該ファイルに記録された本人確認情報の整合性確認を行う。		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	I 基本情報 2. システム2	—	(新規追加)		
令和5年11月30日	I 基本情報 3. 特定個人情報ファイル名	都道府県知事保存本人確認情報ファイル(東京都分)	(1)都道府県知事保存本人確認情報ファイル (2)都道府県知事保存附票本人確認情報ファイル		
令和5年11月30日	I 基本情報 4. ①事務実施上の必要性	東京都では、都道府県知事保存本人確認情報ファイルを、下記の必要性から取り扱う。 ・都道府県知事保存本人確認情報ファイルは、転出入があった場合等にスムーズな住民情報の処理を行うため、また全国的な本人確認手段として、1つの市区町村内にとどまらず、全地方公共団体で、本人確認情報を正確かつ統一的に記録・管理することを目的として、以下の用途に用いられる。 ①住民基本台帳ネットワークシステムを用いて市区町村の区域を越えた住民基本台帳に関する事務 (住民基本台帳ネットワークシステムに係る本人確認情報の管理及び提供等に関する事務)の処理を行うため、東京都内の住民に係る最新の本人確認情報を管理する。 ②市区町村からの本人確認情報の更新情報の通知を受けて都道府県知事保存本人確認情報ファイルを更新し、当該更新情報を機構に対して通知する。 ③東京都の執行機関からの照会に基づき、本人確認情報を提供する。 ④住民からの請求に基づき、当該個人の本人確認情報を開示する。 ⑤住民基本台帳ネットワークシステムに係る本人確認情報の管理及び提供等に関する事務において、本人確認情報を検索する。 ⑥市区町村において保存する本人確認情報との整合性を確認する。	(1)都道府県知事保存本人確認情報ファイル 東京都では、都道府県知事保存本人確認情報ファイルを、下記に記載の通りの必要性から取り扱う。 ・都道府県知事保存本人確認情報ファイルは、転出入があった場合等にスムーズな住民情報の処理を行うため、また全国的な本人確認手段として、1つの市町村内にとどまらず、全地方公共団体で、本人確認情報を正確かつ統一的に記録・管理することを目的として、以下の用途に用いられる。 ①住基ネットを用いて区市町村の区域を越えた住民基本台帳に関する事務 (住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務)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区市町村からの本人確認情報の更新情報の通知を受けて都道府県知事保存本人確認情報ファイルを更新し、当該更新情報を機構に対して通知する。 ③東京都の他の執行機関又は他部署からの照会に基づき、本人確認情報を提供・移転する。 ④住民からの請求に基づき、当該個人の本人確認情報を開示する。 ⑤住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務において、本人確認情報を検索する。 ⑥区市町村において保存する本人確認情報との整合性を確認する。		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	I 基本情報 4. ①事務実施上の必要性	—	(2)都道府県知事保存附票本人確認情報ファイル 東京都では、都道府県知事保存附票本人確認情報ファイルを、下記に記載の通りの必要性から取り扱う。 ・都道府県知事保存附票本人確認情報ファイルは、国外転出者に係る本人確認手段として、1つの市町村内にとどまらず、全地方公共団体で、附票本人確認情報を正確かつ統一的に記録・管理することを目的として、以下の用途に用いられる。 ①附票連携システムに係る附票本人確認情報の管理及び提供等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附票本人確認情報を管理する。 ②区市町村からの附票本人確認情報の更新情報の通知を受けて都道府県知事保存附票本人確認情報ファイルを更新し、当該更新情報を機構に対して通知する。 ③東京都の他の執行機関又は他部署からの照会に基づき、附票本人確認情報を提供・移転する。 その際、番号法で認められた場合に限り、東京都の他の執行機関又は他部署からの求めに応じ、附票本人確認情報の提供・移転に併せて当該個人の住民票コードを用いて、都道府県知事保存本人確認情報ファイルから個人番号を抽出し、照会元に提供・移転する場合がある。 ④住民からの請求に基づき、当該個人の附票本人確認情報を開示する。 ⑤附票本人確認情報の管理及び提供等に関する事務において、附票本人確認情報を検索する。 ⑥区市町村において保存する附票本人確認情報との整合性を確認する。		
令和5年11月30日	I 基本情報 4. ②実現が期待されるメリット	住民票の写し等にかえて本人確認情報を利用することにより、これまでに窓口で提出が求められていた行政機関が発行する添付書類(住民票の写し等)の省略が図られ、もって国民／住民の負担軽減(各機関を訪問し、証明書等入手する金銭的、時間的コストの節約)につながるが見込まれる。	住民票の写し等にかえて本人確認情報を利用することにより、これまでに窓口で提出が求められていた行政機関が発行する添付書類(住民票の写し等)の省略が図られ、もって国民／住民の負担軽減(各機関を訪問し、証明書等入手する金銭的、時間的コストの節約)につながるが見込まれる。 また、国外転出者を含め個人番号カードによる本人確認、個人番号の真正性確認が可能となり、行政事務の効率化に資することが期待される。		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	I 基本情報 5. 個人番号の利用	住民基本台帳法(昭和42年7月25日法律第81号) (平成30年7月6日公布(平成30年法律第71号)時点) ・第7条(住民票の記載事項) ・第12条の5(住民基本台帳の脱漏等に関する都道府県知事の通報) ・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7(都道府県知事から機構への本人確認情報の通知等) ・第30条の8(本人確認情報の誤りに関する機構の通報) ・第30条の11(通知都道府県以外の都道府県の執行機関への本人確認情報の提供) ・第30条の13(都道府県の条例による本人確認情報の提供) ・第30条の15(本人確認情報の利用) ・第30条の32(自己の本人確認情報の開示) ・第30条の35(自己の本人確認情報の訂正)	住民基本台帳法(昭和42年7月25日法律第81号) ・第7条(住民票の記載事項) ・第12条の5(住民基本台帳の脱漏等に関する都道府県知事の通報) ・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7(都道府県知事から機構への本人確認情報の通知等) ・第30条の8(本人確認情報の誤りに関する機構の通報) ・第30条の11(通知都道府県以外の都道府県の執行機関への本人確認情報の提供) ・第30条の13(都道府県の条例による本人確認情報の提供) ・第30条の15(本人確認情報の利用) ・第30条の22(市町村間の連絡調整等) ・第30条の32(自己の本人確認情報の開示) ・第30条の35(自己の本人確認情報の訂正) ・第30条の44の6第3項(都道府県知事保存附票本人確認情報(住民票コードに限る。)の利用)		
令和5年11月30日	(別添1)事務の内容 (1)本人確認情報の管理及び提供等に関する事務	本人確認情報の管理及び提供等に関する事務	(1)本人確認情報の管理及び提供等に関する事務		
令和5年11月30日	(別添1)事務の内容 (1)本人確認情報の管理及び提供等に関する事務 図		(図差替え)		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	(別添1)事務の内容 (1)本人確認情報の管理及び提供等に関する事務 (備考)	1. 本人確認情報の更新に関する事務 1-①.市区町村は、住民から受け付けた住民の異動に関する情報を、市区町村コミュニケーションサーバ(市区町村CS)を通じて東京都サーバに通知する。 1-②.東京都知事は、東京都サーバにおいて、市区町村より受領した本人確認情報を元に都道府県知事保存本人確認情報ファイル(以下「本人確認情報ファイル」という。)を更新する。 1-③.東京都知事は、地方公共団体情報システム機構(以下「機構」という。)に対し、住民基本台帳ネットワークシステムを介して、本人確認情報の更新を通知する(これを受けて、機構が保管する全国サーバ内の本人確認情報が更新される。))。	1. 本人確認情報の更新に関する事務 1-①.区市町村において受け付けた住民の異動に関する情報を、区市町村CSを通じて東京都サーバに通知する。 1-②.東京都サーバにおいて、区市町村より受領した本人確認情報を元に都道府県知事保存本人確認情報ファイルを更新する。 1-③.機構に対し、住民基本台帳ネットワークを介して、本人確認情報の更新を通知する。		
令和5年11月30日	(別添1)事務の内容 (1)本人確認情報の管理及び提供等に関する事務 (備考)	2. 東京都の他の執行機関(東京消防庁など)への情報提供又は東京都の他部署への移転 2-①.東京都の他の執行機関又は東京都の他部署において、個人番号又は4情報をキーワードとした本人確認情報の照会を行う。 2-②.東京都知事において、提示されたキーワードを元に本人確認情報ファイルを検索し、照会元に対し、当該個人の本人確認情報を提供する。 ※検索対象者が他都道府県の場合は全国サーバに対して検索の要求を行う(後記4)。 ※一括提供の方式により本人確認情報を提供する場合には、東京都知事(所管部署:総務局)において代表端末を操作し、外部記録媒体(DVD-RW)を用いて提供する。	2. 東京都の他の執行機関への情報提供又は他部署への移転 2-①.東京都の他の執行機関又は他部署において、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。 2-②.都道府県知事において、提示されたキーワードを元に都道府県知事保存本人確認情報ファイルを検索し、照会元に対し、当該個人の本人確認情報を提供・移転する。 ※検索対象者が他都道府県の場合は全国サーバに対して検索の要求を行う。 ※東京都の他の執行機関又は他部署に対し、住民基本台帳ネットワークシステムに係る本人確認情報を一括して提供する場合(一括提供の方式(注1)により行う場合)には、東京都知事(所管部署:総務局)において、東京都サーバの代表端末を操作し、媒体連携(注2)により行う。 (注1)東京都の他の執行機関又は他部署においてファイル化された本人確認情報照会対象者の情報(検索条件のリスト)を元に東京都サーバに照会し、照会結果ファイルを提供する方式を指す。 (注2)媒体連携とは、一括提供の方式により本人確認情報の提供を行う場合に、情報連携に電子記録媒体を用いる方法を指す。		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	(別添1)事務の内容 (1)本人確認情報の管理及び提供等に関する事務 (備考)	3. 本人確認情報の開示に関する事務 3-①.総務局において、住民より自己に係る本人確認情報の開示請求を受け付ける。 3-②.開示請求者(住民)に対し、本人確認情報ファイルに記録された当該個人の本人確認情報を開示する。 4. 機構への情報照会に係る事務(対象検索者が他道府県の場合) 4-①.東京都知事は、機構に対し、他道府県住民の個人番号又は4情報をキーワードとした本人確認情報の照会を行う。 4-②. 東京都知事は、機構より、当該個人の本人確認情報を受領する。 5. 本人確認情報検索に関する事務 5-①. 東京都知事は、4情報の組み合わせを検索キーに、本人確認情報ファイルを検索する。	3. 本人確認情報の開示に関する事務 3-①.住民より本人確認情報の開示請求を受け付ける(※特定個人情報を含まない)。 3-②.開示請求者(住民)に対し、都道府県知事保存本人確認情報ファイルに記録された当該個人の本人確認情報を開示する。 3-③.施設のできる金庫等に保管し、保存期間の終了後、シュレッダーにて廃棄する。 4. 機構への情報照会に係る事務 4-①.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。 4-②.機構より、当該個人の本人確認情報を受領する。 5. 本人確認情報検索に関する事務 5-①. 4情報の組み合わせを検索キーに、都道府県知事保存本人確認情報ファイルを検索する。		
令和5年11月30日	(別添1)事務の内容 (1)本人確認情報の管理及び提供等に関する事務 (備考)	6. 本人確認情報整合 6-①. 東京都知事は、市区町村CSより、東京都サーバに対し、整合性確認用の本人確認情報を送付する。 6-②. 東京都知事は、東京都サーバにおいて、市区町村CSより受領した整合性確認用の本人確認情報を用いて本人確認情報ファイルの整合性確認を行う。 6-③. 東京都知事は、東京都サーバより、市区町村CSに対して整合性確認結果を通知する。	6. 本人確認情報整合 6-①. 区市町村CSより、東京都サーバに対し、整合性確認用の本人確認情報を送付する。 6-②. 東京都サーバにおいて、区市町村CSより受領した整合性確認用の本人確認情報を用いて都道府県知事保存本人確認情報ファイルの整合性確認を行う。 6-③. 東京都サーバより、区市町村CSに対して整合性確認結果を通知する。 ※東京都サーバのデータは、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、住民票の記載の修正前の本人確認情報(履歴情報)及び削除者の本人確認情報は住基法施行令第30条の6に定める期間(150年間)保管後、システムにて自動判別し、復元できないように消去される。 ※電子記録媒体のデータは受け渡し又は利用が終了した場合、速やかに消去される。		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	(別添1)事務の内容 (2)附票本人確認情報の管理及び提供等に関する事務	—	(新規追加)		
令和5年11月30日	Ⅱ 特定個人情報ファイルの概要 1. 特定個人情報ファイル名	都道府県知事保存本人確認情報ファイル	(1)都道府県知事保存本人確認情報ファイル		
令和5年11月30日	Ⅱ 特定個人情報ファイルの概要 2. ③その必要性	住民基本台帳ネットワークシステムを通じて全国共通の本人確認を行うため、特定個人情報ファイル(都道府県知事保存本人確認情報ファイル)において東京都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。	住基ネットを通じて全国共通の本人確認を行うため、本特定個人情報ファイル(都道府県知事保存本人確認情報ファイル)において東京都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。		
令和5年11月30日	Ⅱ 特定個人情報ファイルの概要 3. ⑤本人への明示	住民基本台帳法第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)にて、都道府県知事が当該市区町村の区域内の住民の本人確認情報を入手することについて規定している。	都道府県知事が当該区市町村の区域内の住民の本人確認情報を入手することについて、住基法第30条の6(市町村長から都道府県知事への本人確認情報の通知等)に明示されている。		
令和5年11月30日	Ⅱ 特定個人情報ファイルの概要 3. ⑦使用部署	総務局行政部振興企画課	総務局行政部振興企画課・庁内利用部署		
令和5年11月30日	Ⅱ 特定個人情報ファイルの概要 3. ⑦利用者数	10人未満	1,000人以上		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	II 特定個人情報ファイルの概要 3. ⑧使用方法	【Ⅰ 本人確認情報の更新(最新化)】 市区町村長からの住民票の記載事項の変更又は新規作成の通知を受け(既存住基システム→市区町村CS→東京都サーバ)、都道府県知事保存本人確認情報ファイルを更新し、機構に対して当該本人確認情報の更新情報を通知する(東京都サーバ→全国サーバ)。 【Ⅱ 東京都の他の執行機関(又は他部署)への提供・移転】 法令に定められた個人番号取扱事務を実施する必要上、東京都の他の執行機関又は他部署からの本人確認情報の照会要求を受け(東京都の他の執行機関又は他部署→東京都サーバ)、照会のあった住民票コード、個人番号又は4情報の組合せを元に都道府県知事保存本人確認情報ファイルを検索し、該当する本人確認情報を照会元へ提供する(東京都サーバ→東京都の他の執行機関又は他部署)。	・市区町村長からの住民票の記載事項の変更又は新規作成の通知を受け(既存住基システム→市区町村CS→東京都県サーバ)、都道府県知事保存本人確認情報ファイルを更新し、機構に対して当該本人確認情報の更新情報を通知する(東京都サーバ→全国サーバ)。 ・東京都の他の執行機関又は他部署からの本人確認情報の照会要求を受け(東京都の他の執行機関又は他部署→東京都サーバ)、照会のあった住民票コード、個人番号又は4情報の組合せを元に都道府県知事保存本人確認情報ファイルを検索し、該当する本人確認情報を照会元へ提供・移転する(東京都サーバ→東京都の他の執行機関又は他部署)。		
令和5年11月30日	II 特定個人情報ファイルの概要 3. ⑧使用方法	【Ⅲ 住民からの開示請求に係る対応】 住民からの開示請求に基づき(住民→東京都の窓口→東京都サーバ)、当該住民の本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、書面により提供する(東京都サーバ→帳票出力→住民)。 【Ⅳ 住民基本台帳法に定められた事務での照会業務における使用】 4情報(氏名、住所、性別、生年月日)の組合せをキーに都道府県知事保存本人確認情報ファイルの検索を行う。 【Ⅴ 住民基本台帳ネットワークシステム情報の整合性確認】 都道府県知事保存本人確認情報ファイルの正確性を担保するため、市区町村から本人確認情報を受領し(市区町村CS→東京都サーバ)、当該本人確認情報を用いて都道府県知事保存本人確認情報ファイルに記録された本人確認情報について、整合性確認を行う。	・住民からの開示請求に基づき(住民→東京都窓口→東京都サーバ)、当該住民の本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、書面により提供する(東京都サーバ→帳票出力→住民)。 ・4情報(氏名、住所、性別、生年月日)の組合せをキーに都道府県知事保存本人確認情報ファイルの検索を行う。 ・都道府県知事保存本人確認情報ファイルの正確性を担保するため、区市町村から本人確認情報を受領し(区市町村CS→東京都サーバ)、当該本人確認情報を用いて都道府県知事保存本人確認情報ファイルに記録された本人確認情報について、整合性確認を行う。		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	Ⅱ 特定個人情報ファイルの概要 3. ⑧情報の突合	【上記 Ⅰ】 ・都道府県知事保存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都道府県知事保存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。 【上記 Ⅱ、Ⅳ】 ・東京都の他の執行機関又は他部署からの照会に基づいて本人確認情報を提供する際に、照会元から受信した対象者の4情報等との突合を行う。 【上記 Ⅲ】 ・住民からの請求に基づいて本人確認情報を開示する際に、請求者から受領した本人確認情報との突合を行う。 【上記 Ⅴ】 ・市区町村CSとの整合処理を実施するため、4情報等との突合を行う。	・都道府県知事保存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都道府県知事保存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。 ・東京都の他の執行機関又は他部署からの照会に基づいて本人確認情報を提供・移転する際に、照会元から受信した対象者の4情報等との突合を行う。 ・請求に基づいて本人確認情報を開示する際に、開示請求者から受領した本人確認情報との突合を行う。 ・区市町村CSとの整合処理を実施するため、4情報等との突合を行う。		
令和5年11月30日	Ⅱ 特定個人情報ファイルの概要 4. ②その妥当性	都道府県職員のサーバ管理に係る運用負担の軽減、都道府県サーバ導入費及び維持管理費の削減、セキュリティ水準の向上の観点から、集約センターにおいて一元的に運用している。 運用については、住基ネットについてのシステム設計やセキュリティに関する専門的な知識と、運用するサーバやネットワーク機器に関する高度な技術力を有する地方公共団体情報システム機構に委託している。	本特定個人情報ファイル(都道府県知事保存本人確認情報ファイル)が保存される東京都サーバの運用及び監視業務を委託することによる。 なお、「①委託内容」の通り、委託事項は、直接本人確認情報に係わらない事務を対象としているため、委託先においては、特定個人情報ファイルに記載された情報そのものを扱う事務は実施しない。		
令和5年11月30日	Ⅱ 特定個人情報ファイルの概要 4. ⑨再委託事項	集約センター内における東京都サーバの運用及び監視に関する業務を再委託する。	東京都サーバの運用及び監視に関する業務。再委託する業務は、直接本人確認情報に係わらない(直接本人確認情報にアクセスできず、閲覧・更新・削除等を行わない。)業務を対象とする。		
令和5年11月30日	Ⅱ 特定個人情報ファイルの概要 5. 提出先2	東京都の他の執行機関(下水道局、東京消防庁、東京都教育委員会)	東京都の他の執行機関(下水道局、水道局、警視庁、東京消防庁、東京都教育委員会)		
令和5年11月30日	Ⅱ 特定個人情報ファイルの概要 5. 移転先1	東京都の他の部署(総務局人事部、主税局(課税部、徴収部、都税事務所、都税事務総合センター)、生活文化局都民生活部、環境局環境改善部、福祉保健局(医療政策部、保健政策部、生活福祉部、少子社会対策部、障害者施策推進部)、産業労働局(商工部、観光部))※計53か所	東京都の他部署(総務局(総務部、人事部)、主税局(税制部、課税部、資産税部、徴収部、都税事務所、都税総合事務センター)、生活文化スポーツ局(都民生活部、私学部)、保健医療局(医療政策部、保健政策部)、福祉局(生活福祉部、子供・子育て支援部、障害者施策推進部)、産業労働局(商工部、観光部)等)		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	Ⅱ 特定個人情報ファイルの概要 6. ①保管場所	【東京都サーバ】 セキュリティゲートにて入退館管理をしている都道府県サーバの集約センターにおいて、施錠管理及び入退室管理(監視カメラを設置してサーバ設置場所への入退室者を特定・管理)を行っている部屋に設置したサーバ内に保管する。サーバへのアクセスはID／パスワードによる認証が必要となる。 【電子記録媒体】 総務局行政部から貸与する指定のDVD－RWに暗号化の上格納し、施錠が出来る金庫等に保管する。 【紙】 各所属において、施錠が出来る金庫等に保管する。	【東京都サーバ】 セキュリティゲートにて入退館管理をしている都道府県サーバの集約センターにおいて、施錠管理及び入退室管理(監視カメラを設置してサーバ設置場所への入退室者を特定・管理)を行っている部屋に設置したサーバ内に保管する。サーバへのアクセスはIDと生体認証(又はパスワード)による認証が必要となる。 【電子記録媒体】 総務局行政部から貸与する指定のDVD－RWに暗号化の上格納し、施錠が出来る金庫等に保管する。 【紙】 各所属において、施錠が出来る金庫等に保管する。		
令和5年11月30日	Ⅱ 特定個人情報ファイルの概要 6. ②その妥当性	【東京都サーバ】 9)20年以上 ・住民票の記載の修正後の本人確認情報は、本人確認情報の提供のため、市区町村CSを通じて新たに記載の修正の通知を受けるまで保管する必要がある。 ・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、住基法施行令第30条の6(都道府県における本人確認情報の保存期間)に定める期間(150年間)保管する。 【電子記録媒体】 1)1年未満 データの受け渡し又は利用が終了した場合、速やかにデータを消去する。 【紙】 10)定められていない 利用事務での文書保存期間終了後又は各所属で利用が終了した場合、速やかに廃棄する。	【東京都サーバ】 9)20年以上 ・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、住基法施行令第30条の6(都道府県における本人確認情報の保存期間)に定める期間(150年間)保管する。 【電子記録媒体】 1)1年未満 データの受け渡し又は利用が終了した場合、速やかにデータを消去する。 【紙】 10)定められていない 利用事務での文書保存期間終了後又は各所属で利用が終了した場合、速やかに廃棄する。		
令和5年11月30日	Ⅱ 特定個人情報ファイルの概要 (2)都道府県知事保存附票 本人確認情報ファイル	—	(新規追加)		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	(別添2)ファイル記録項目	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. 生年月日、6. 性別、7. 住所、8. 外字数(住所)、9. 個人番号、10. 異動事由、11. 異動年月日、12. 保存期間フラグ、13. 清音化かな氏名、14. 市町村コード、15. 大字・字コード、16. 操作者ID、17. 操作端末ID、18. タイムスタンプ、19. 通知を受けた年月日、20. 外字フラグ、21. 削除フラグ、22. 更新順番号、23. 氏名外字変更連番、24. 住所外字変更連番	(1)都道府県知事保存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. 生年月日、6. 性別、7. 住所、8. 外字数(住所)、9. 個人番号、10. 異動事由、11. 異動年月日、12. 保存期間フラグ、13. 清音化かな氏名、14. 市町村コード、15. 大字・字コード、16. 操作者ID、17. 操作端末ID、18. タイムスタンプ、19. 通知を受けた年月日、20. 外字フラグ、21. 削除フラグ、22. 更新順番号、23. 氏名外字変更連番、24. 住所外字変更連番、25. 旧氏 漢字、26. 旧氏 外字数、27. 旧氏 ふりがな、28. 旧氏 外字変更連番		
令和5年11月30日	(別添2)ファイル記録項目	—	(2)都道府県知事保存附票本人確認情報ファイル ア 附票本人確認情報 1. 住民票コード、2. 氏名 漢字、3. 氏名外字数、4. 氏名 ふりがな、5. 生年月日、6. 性別、7. 住所 市町村コード、8. 住所漢字、9. 住所、外字数、10. 最終住所 漢字、11. 最終住所 外字数、12. 異動年月日、13. 旧住民票コード、14. 附票管理市町村コード、15. 附票本人確認情報状態区分、16. 外字フラグ、17. 外字パターン、18. 通知区分 イ その他 1. 個人番号(※国外転出者に係る事務処理に関し、番号法で認められた場合に限り、自都道府県の他の執行機関又は他部署からの求めに応じ、当該個人の住民票コードを用いて、都道府県知事保存本人確認情報ファイルから個人番号を抽出し、提供・移転する場合がある。)		
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 1. 特定個人情報保護ファイル名	都道府県知事保存本人確認情報ファイル	(1)都道府県知事保存本人確認情報ファイル		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 2. リスク1 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	住民基本台帳法第30条の6により、市区町村 から通知を受けることとされている情報のみを 入手できることを、住民基本台帳ネットワース テムのシステム上で担保する。	法令により区市町村から通知を受けることとさ れている情報のみを入手できることを、システ ム上で担保する。		
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 2. リスク2 リスクに対する措置の内容	本人確認情報の入手元を市区町村CSに限定 することを、専用線の都内ネットワークにより実 現し、住民基本台帳ネットワークシステムのシ ステム上で担保する。	本人確認情報の入手元を区市町村CSに限定 する。		
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 2. リスク3 その他の措置の内容	—	システムでは対応できない事象が発生した際 に、本人確認情報の正確性を維持するため、 要領・手順書等に基づいて本人確認情報の入 力、削除及び訂正が行われていることを定期 的に確認する。		
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 2. リスク4 リスクに対する措置の内容	・機構が作成・配付する専用のアプリケーション (※)を用いることにより、入手の際の特定個人 情報の漏えい・紛失の防止に努める。 ・市区町村CSと接続するネットワーク回線に専 用回線を用いる、情報の暗号化を実施する、操 作者の認証を行う等の措置を講じる。 ※都道府県サーバ上で稼動するアプリケーショ ン。 これにより、都内の市区町村の住民の本人確 認情報を管理し、市区町村CSや全国サーバと のデータ交換を行う。 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。	・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。 ・区市町村CSと接続するネットワーク回線に専 用回線を用いる、情報の暗号化を実施する等 の措置を講じる。 ・特定個人情報の入手は、システム上自動処 理にて行われるため、操作者は存在せず人為 的なアクセスが行われることはない。 ※東京都サーバのサーバ上で稼動するアプリ ケーション。 都道府県内の市町村の住民の本人確認情報 を管理し、都道府県内の市町村の市町村CS や全国サーバとのデータ交換を行う。 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。		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 3. リスク1 事務で使用するその他のシス テムにおける措置の内容	東京都サーバは、事務で使用するその他の庁 内システムとは接続しない。	庁内システムと東京都サーバとの接続は行わ ない。 東京都サーバは、集約センター内において、附 票東京都サーバと接続する。 なお、東京都サーバと附票東京都サーバのシ ステム間のアクセスは、以下の場合の処理に 限られるよう、システムにより制限する。 (1)東京都サーバ⇒附票東京都サーバへのア クセス 番号法で認められた場合に限り、東京都の 他の執行機関又は他部署等からの求めに応 じ、国外転出者に係る個人番号を連携する場 合。 (2)附票東京都サーバ⇒東京都サーバへのア クセス 国外転出者に係る事務処理に関し、番号法で 認められた場合に限り、東京都の他の執行機 関又は他部署等からの求めに応じ、個人番号 を入手する場合(目的を越えた紐づけが行われ ないよう、個人番号は附票本人確認情報DBと は別の一時保存領域で処理する。)		
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 3. リスク3 リスクに対する措置の内容	・システムの操作履歴(操作ログ)を記録する。 ・担当者へのヒアリングを実施し、業務上必要 のない検索又は抽出が行われていないことを 確認する。 ・システムを利用する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。 ・外部記録媒体の持ち出しは、「住民基本台帳 ネットワークシステム 情報セキュリティ実施手 順 利用者用」により禁止されている。	・システムの操作履歴(操作ログ)を記録する。 ・担当者へのヒアリングを実施し、業務上必要 のない検索又は抽出が行われていないことを 確認する。 ・システムを利用する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。 ・外部記録媒体の持ち出しは、「住民基本台帳 ネットワークシステム 情報セキュリティ実施手 順 利用者用」により禁止されている。 ・職員以外の従業者(委託先)には、当該事項 についての誓約書の提出を求める。		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク 対策 3. 特定個人情報の仕様に おけるその他のリスク及びその リスクに対する措置	その他、特定個人情報の使用にあたり、以下の措置を講じている。 【端末利用】 ①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することを防止する ②代表端末及び業務端末のディスプレイを、来庁者から見えない位置に設置する ③ディスプレイに覗き見防止シートを取り付ける ③本人確認情報が表示された画面のハードコピーの取得ができないよう設定している ④大量のデータ出力に際しては、事前に管理責任者の承認を得よう指導している 【住民対応】 ①本人確認情報の開示・訂正の請求により、住民が特定個人情報の正確性等を確認できる ②本人確認情報の提供状況の開示請求により、住民が特定個人情報の提供先等を確認できる	その他、特定個人情報の使用にあたり、以下の措置を講じている。 【端末利用】 ①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することを防止する ②代表端末及び業務端末のディスプレイを、来庁者から見えない位置に設置する ③ディスプレイに覗き見防止シートを取り付ける ④本人確認情報が表示された画面のハードコピーの取得ができないよう設定している ⑤大量のデータ出力に際しては、事前に管理責任者の承認を得よう指導している 【住民対応】 ①本人確認情報の開示・訂正の請求により、住民が特定個人情報の正確性等を確認できる ②本人確認情報の提供状況の開示請求により、住民が特定個人情報の提供先等を確認できる		
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク 対策 4. 特定個人情報ファイルの 取扱いの委託におけるその他 のリスク及びそのリスクに対 する措置	—	「東京都サーバの運用及び監視に関する業務」再委託先については、毎年度の契約において、再委託先業者の業務内容や委託先との業務分担を審査した上で承認を行っている。		
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク 対策 5. リスク1 特定個人情報の提出・移転の 記録—具体的な方法	住民基本台帳ネットワークシステムを通じて特定個人情報(個人番号、4情報等)の提供・移転を行っており、特定個人情報(個人番号、4情報等)の提供・移転に係る処理を行った際、記録(日時、操作者等)をシステム上で管理し保存する。	住民基本台帳ネットワークシステムを通じて特定個人情報(個人番号、4情報等)の提供・移転を行っており、特定個人情報(個人番号、4情報等)の提供・移転に係る処理を行った際、記録(日時、操作者等)をシステム上で管理し保存する。 なお、システム上、提出・移転に係る処理を行ったものの提出・移転が認められなかった場合についても記録を残す。		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 5. リスク2 リスクに対する措置の内容	全国サーバと東京都サーバの間の通信では専用線を用い相互認証を実施しているため、認証できない相手先への情報の提供はなされることがシステム上担保される。 また、東京都の他の執行機関への提供及び他の部署への移転のため、外部記録媒体へ出力する必要がある場合には、情報を暗号化し逐一出力の記録が残される仕組みを構築している。	連携手段として通信の記録が逐一保存され、また、連携するデータが暗号化される仕組みが確立した住民基本台帳ネットワークシステムを用いることにより、不適切な方法による特定個人情報の提供を防止する。 なお、全国サーバと東京都サーバの間の通信では専用線を用い相互認証を実施しているため、認証できない相手先への情報の提供はなされることがシステム上担保される。 また、東京都の他の執行機関への提供及び他の部署への移転のため、外部記録媒体へ出力する必要がある場合には、情報を暗号化し逐一出力の記録が残される仕組みを構築している。		
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 5. リスク3 リスクに対する措置の内容	・誤った情報を提供・移転してしまうリスクへの措置 :システム上、照会元から指定された検索条件に基づき得た結果を適切に提供することを担保する。 ・誤った相手に提供・移転してしまうリスクへの措置 :全国サーバと東京都サーバの間の通信では専用線を用い相互認証を実施しているため、認証できない相手先への情報の提供はなされることがシステム上担保される。 また、情報を暗号化し格納した媒体による情報の提供・移転が必要な場合には文書による確認を実施し、法令上の根拠のない相手先へ情報の提供・移転を防止している。	・誤った情報を提供・移転してしまうリスクへの措置 :システム上、照会元から指定された検索条件に基づき得た結果を適切に提供・移転することを担保する。 ・誤った相手に提供・移転してしまうリスクへの措置 :全国サーバと東京都サーバの間の通信では専用線を用い相互認証を実施しているため、認証できない相手先への情報の提供はなされることがシステム上担保される。 また、情報を暗号化し格納した媒体による情報の提供・移転が必要な場合には文書による確認を実施し、法令上の根拠のない相手先へ情報の提供・移転を防止している。		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 7. リスク1 ⑨その内容	① 平成28年4月21日、事務担当者が「海の森友の会通信」をメールで送信する際、全員のメールアドレス443件をbcc欄ではなく、誤って宛先欄に入力し、送信してしまった。 ② 平成28年9月16日、都が委託している私立高等学校等就学支援金の審査に係る事務において、再委託先が、審査に係る生徒保護者への書類を、誤った住所に送付した。送付書類は、書類に不備がある生徒保護者に対し、不足書類の提出期限等を連絡するものであり、生徒の氏名及び就学支援金認定番号が含まれていた。 ③ 平成29年1月17日、都民の健康と安全を確保する環境に関する条例に基づき、排出量取引に利用する指定管理口座の名義人情報を環境局ホームページで公表している。個人情報については希望する場合に公表するものとしているが、公表を希望しない個人の名義人情報（8指定口座396名分）がホームページで閲覧可能な状況になっており、個人情報が出た。 ④ 平成29年3月10日、都税のクレジットカード納付を行うために受託事業者が運営している「都税クレジットカードお支払サイト」について、ソフトウェアの脆弱性に起因する第三者による不正アクセスが確認され、サーバ上に保持していたクレジットカード番号及び有効期限（36万4,181件）メールアドレス（36万2,049件）の情報を不正に取得されていたことが判明した。	①令和2年8月21日に東京都人権プラザにおいて開催した「心と体を傷つけられて亡くなった天国の子供たちのメッセージ」展のメディア向けカンファレンスの動画配信案内を（公財）東京都人権啓発センターの行事案内希望者に対して送付する際、事務担当者が誤ってメールアドレスをBCC欄ではなく、CC欄に入力して発信したため、個人情報が流出する事故が発生した。 ②令和3年1月に東京都電子調達システムにより印刷物の契約案件を公表した際、印刷物の配布先となる町会名のみを公表するところ、誤って中野区内の町会の代表者の氏名、住所及び電話番号を1月28日から2月3日までの間、公表してしまった。 ③令和3年3月、助成金返還事務のためにワンピンより取り寄せていた平成29年度教育助成金調査票（B表）の返却手続きを行った際、段ボール二箱分がないことが発覚した。当該段ボール箱は執務室内の空きスペースにて保管していた。 ④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、都が過去に出展した民間企業主催の就職イベント参加者及び当該企業に対して都関連の採用情報の提供を希望した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ため、個人情報が流出する事故が発生した。		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 7. リスク1 ⑨その内容	⑤平成29年9月1日、一般財団法人東京マラソン財団から海外メディア記者126名に対し、東京マラソンの申込者数についてプレスリリースのメール配信を実施した際、記者126名のメールアドレスを誤ってbccではなくccに入力し、メールアドレスが表示された状態で一斉送信してしまった。 ⑥平成29年11月29日、建設局職員が出張先において、所属職員324名分の個人情報を記載した緊急連絡網等が入った鞆を置いたまま移動し、紛失した。 ⑦平成30年4月24日、上野動物園で行った動物の観覧抽選に関し、指定管理者の委託先事業者が当選ハガキ上を発送したところ、内209件について、「代表者氏名」「同行者氏名」の全部または一部に他の当選者（代行者・同行者）の氏名が記載されていた。 ⑧平成30年9月21日、公益財団法人東京都公園協会が、委託事業者（131社）に電子メールを送信する際に、誤って委託事業者のメールアドレスを「宛先」欄へ入力し送信した結果、委託事業者（131社）の会社名、担当者名及びメールアドレスが送信先に漏えいした。	⑤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てしまい、氏名が流出する事故が発生した。 ⑥令和3年12月、都営住宅の毎月募集の申込者に対して、東京都住宅供給公社において、抽せん番号をお知らせする郵便はがきを発送する準備を行い、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。 ⑦令和4年5月、指定管理者が運営する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。 ⑧令和4年5月、都の技能検定試験に関する業務を行う東京都職業能力開発協会において、技能検定試験に関する通知を外国人技能実習の監理団体に対してメールで送付する際、事務担当者が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。		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 7. リスク1 ⑨その内容	—	⑨令和4年5月、就学支援金事務の受託者である東京都私学財団が、就学支援金の基礎データをCD-Rに情報を保存し、対象高等学校等宛で一斉に送付したところ、そのうち1校において、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。 ⑩令和4年5月、都の医療機器産業への参入支援事業の受託者が、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、宛先欄に複数のメールアドレスを入力し、送信してしまった。同社の配信システムは、1名分のメールを送信した後、宛先欄のメールアドレスが自動で次の1名のアドレスに上書き処理されるプログラムが組まれていたが、プログラムの改修ミスにより、メールアドレスが上書きではなく追記されて送信されていた。 ⑪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。 ⑫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。		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 7. リスク1 ⑨再発防止策の内容	① 事故発生の翌日(4月22日)緊急に港湾局情報セキュリティ委員会を開催し、各委員に対し事故の概要報告及び情報セキュリティ対策の更なる徹底について、部署内職員に対し周知徹底するよう指示した。また、当局監理団体及び報告団体に対して、総務課長より電話で、事故の概要報告及び情報セキュリティ対策の更なる徹底について指示した。 今後も、情報セキュリティ委員会などあらゆる機会をとらえて、都民の方等へメールによる連絡等を行う場合は、複数の担当者により送信先について確認するよう、定期的な注意喚起を徹底する。 ② 個人情報等の適正管理について事例等を通じて知識を習得し、適正な職務の執行を図るため、職員及び委託先職員を対象に個人情報保護研修を行った。生活文化局情報セキュリティ委員会において、各部署の庶務担当課長に対し、今回の事故について報告し、再発防止に努めるよう注意喚起を行う。また、業務全般について個人情報の管理方法を総点検し、事務改善を行う。	① 団体に対し、外部へ一斉送信する際は、メールアドレスをBCC欄に入力すべきことと、メール送信前に、複数の職員で宛先の確認作業を必ず行うことを、職員全員に改めて周知徹底するとともに、組織としての検証を行い、再発防止策を検討するよう指導した。 ② (1) 事務フローの見直し ・ 起工部署の事務フローを、別紙1のとおり見直し、周知徹底を図る。 ・ 契約部署は、着手起案作成時及び発注図書登録時、電子調達システムに、起工部署から提出されたPDFデータを公表前の登録を行ってから印刷した上で、契約依頼文書に添付された仕様書と照合し、一致していることを確認する。また、この確認方法について、令和元年12月19日付経理部契約課長事務連絡「契約事務に係る情報漏えい等の防止策について」により配布されたチェックリストに追記した。 (2) 臨時支所コンプライアンス推進委員会の開催 臨時支所コンプライアンス推進委員会を開催し、再発防止に向け、上記事務フローの見直しの周知徹底を図った。		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 7. リスク1 ⑨再発防止策の内容	③ システム改修により、出力した口座一覧を所属内で回付・確認する体制を構築する。環境局内で本件について周知し、職員に対し改めて個人情報の適切な取扱いについて徹底するよう注意喚起をした。環境局所管のホームページにおいて公表している情報について、公表理由や公表の適否等を確認する点検を実施した。 情報セキュリティ委員会事故対策部会を開催し、事故の原因の確認及び再発防止策について検討を行った。 ④ ソフトウェアの脆弱性について修正を行うとともに、サイト全体の安全性を総点検し、システム変更やサーバ監視体制の強化を実施した。カード情報やメールアドレスは、サーバ内に保持しない等の措置を講じた。サイトの運用面においては、運用基準を見直し、危機管理体制を強化した。 今後も安全なサイト運営のために、セキュリティ対策の強化を継続して実施する。 ⑤ 財団事務局長による職員への事案周知、情報管理に関する注意喚起を行うとともに、複数人への同時メール送信におけるccの使用原則禁止とした。また、情報管理に関する財団全職員悉皆の研修を緊急に実施した。	③(1)個人情報の重要性を再確認し、高い危機意識をもって個人情報の適正な管理・運用を図るよう、改めて基本的な取扱いルールの徹底を図る。 (2)書類の所在及び処理状況が明確に分かるような管理方法の整備や、文書廃棄の際の事務処理手順の整備など、書類管理の徹底に向けた仕組みの構築を図る。 ④(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。 ⑤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。		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 7. リスク1 ⑨再発防止策の内容	⑥「建設局個人情報漏えい事故等対策本部」を設置し、本件周知と再発防止についての検討を行った上で、同日、局内に対し通知を発出し、建設局個人情報安全管理基準の趣旨を踏まえ、事故防止に向けて万全を期すよう局内に周知した。	⑥(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。		
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 7. リスク1 ⑨再発防止策の内容	⑦「建設局個人情報漏えい事故等対策本部」を設置し、本件周知と再発防止についての検討を行った上で、同日、局内に通知を発出し、建設局個人情報安全管理基準の趣旨を踏まえ、事故防止に向けて万全を期すよう局内に周知した。また、他の監理団体及び指定管理者に対しても、同様の事故が起きないように指導した。 ⑧東京都公園協会において、個人情報の取扱いの徹底など周知するとともに、職員に対しても本件周知と情報管理の徹底を指示した。建設局においても、「建設局個人情報漏えい事故等対策本部」を設置し、本件周知と再発防止を徹底した。	⑦(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。 ⑧(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		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 7. リスク1 ⑨再発防止策の内容	—	⑨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対策について改めて確認を行う。 ⑩(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を実施する、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。		
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 7. リスク1 ⑨再発防止策の内容	—	⑪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。 ⑫(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		

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年11月30日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 (2)都道府県知事保存附票 本人確認情報ファイル	—	(新規追加)		
令和5年11月30日	全般	「住民基本台帳法」「住基法」	「住基法」に統一		
令和5年11月30日	全般	「市区町村」	「区市町村」に統一		
令和5年11月30日	全般	「都道府県サーバ」「附票都道府県サーバ」	「東京都サーバ」「附票東京都サーバ」に統一		
令和5年11月30日	全般	「住民基本台帳ネットワークシステム」「住基 ネット」	「住基ネット」に統一		
令和6年12月13日	Ⅱ. 特定個人情報ファイルの 概要 2. 基本情報 ⑤保有開始日	「情報通信技術の活用による行政手続等に係 る関係者の利便性の向上並びに行政運営の 簡素化及び効率化を図るための行政手続き等 における情報通信の技術の利用に関する法律 等の一部を改正する法律(令和元年法律第16 号)」附則第1条第10号にて規定される公布か ら起算して5年を超えない範囲内の政令で定め る日	令和6年5月27日		
令和6年12月13日	Ⅱ. 特定個人情報ファイルの 概要 3. 特定個人情報の入手・使 用 ⑨使用開始日	「情報通信技術の活用による行政手続等に係 る関係者の利便性の向上並びに行政運営の 簡素化及び効率化を図るための行政手続き等 における情報通信の技術の利用に関する法律 等の一部を改正する法律(令和元年法律第16 号)」附則第1条第10号にて規定される公布か ら起算して5年を超えない範囲内の政令で定め る日	令和6年5月27日		