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
33	愛の手帳の交付に係る全項目評価書

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

特記事項	

評価実施機関名

東京都知事

個人情報保護委員会　承認日 【行政機関等のみ】

公表日

［令和7年5月　様式4］

項目一覧

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

Ⅰ　基本情報

1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	愛の手帳の交付に関する事務
②事務の内容　※	・東京都愛の手帳交付要綱に基づき、都内に居住地を有する知的障害者の愛の手帳（東京都療育手帳）の交付、再交付、返還、居住地変更、氏名変更等の事務を行っている。 ・特定個人情報ファイルは、上記規定に従い、次の事務に使用する。 ①台帳管理（転入、氏名変更、住所変更） ②愛の手帳の交付、再交付（更新、再交付）事務 ③愛の手帳の返還 ④身体障害者手帳交付等事務システム抽出データの点検
③対象人数	[　10万人以上30万人未満　] ＜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	身体障害者手帳交付等事務システム（以下「手帳システム」という。） ※今回の評価対象は、令和11年1月稼働予定の次期システムになります。
②システムの機能	1台帳管理機能 ：台帳には氏名、生年月日、性別、住所のほか、障害内容、過去の手帳発行履歴などについて記録され、愛の手帳の交付、再交付、転入、住所変更、氏名変更、返還の各申請・届出について台帳に記録する。 2手帳発行機能 ：交付、再交付（（障害追加の更新、障害程度変更の更新、再交付）の手帳の発行を行う。 3統計機能 ：統計のデータについてシステムより出力する。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [○] その他　（ 連携サーバ　）
システム2～5	
システム2	
①システムの名称	住民基本台帳ネットワークシステム
②システムの機能	・本人確認情報の更新・管理・全国サーバに対する更新通知 ・本人確認の情報抽出・出力 ・全国サーバへの情報照会
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[○] 庁内連携システム [○] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [　] その他　（　）
システム3	
①システムの名称	団体内統合利用番号連携サーバ（以下「連携サーバ」という。）
②システムの機能	・中間サーバへの符号取得要求の仲介 ・団体内統合利用番号の取得、管理 ・団体内統合利用番号、個別業務システム利用番号の紐付管理 ・副本登録における、個別業務システムから中間サーバへの登録要求の仲介 ・情報照会における、個別業務システムからの照会要求の受付及び中間サーバと個別業務システムとの情報授受の仲介

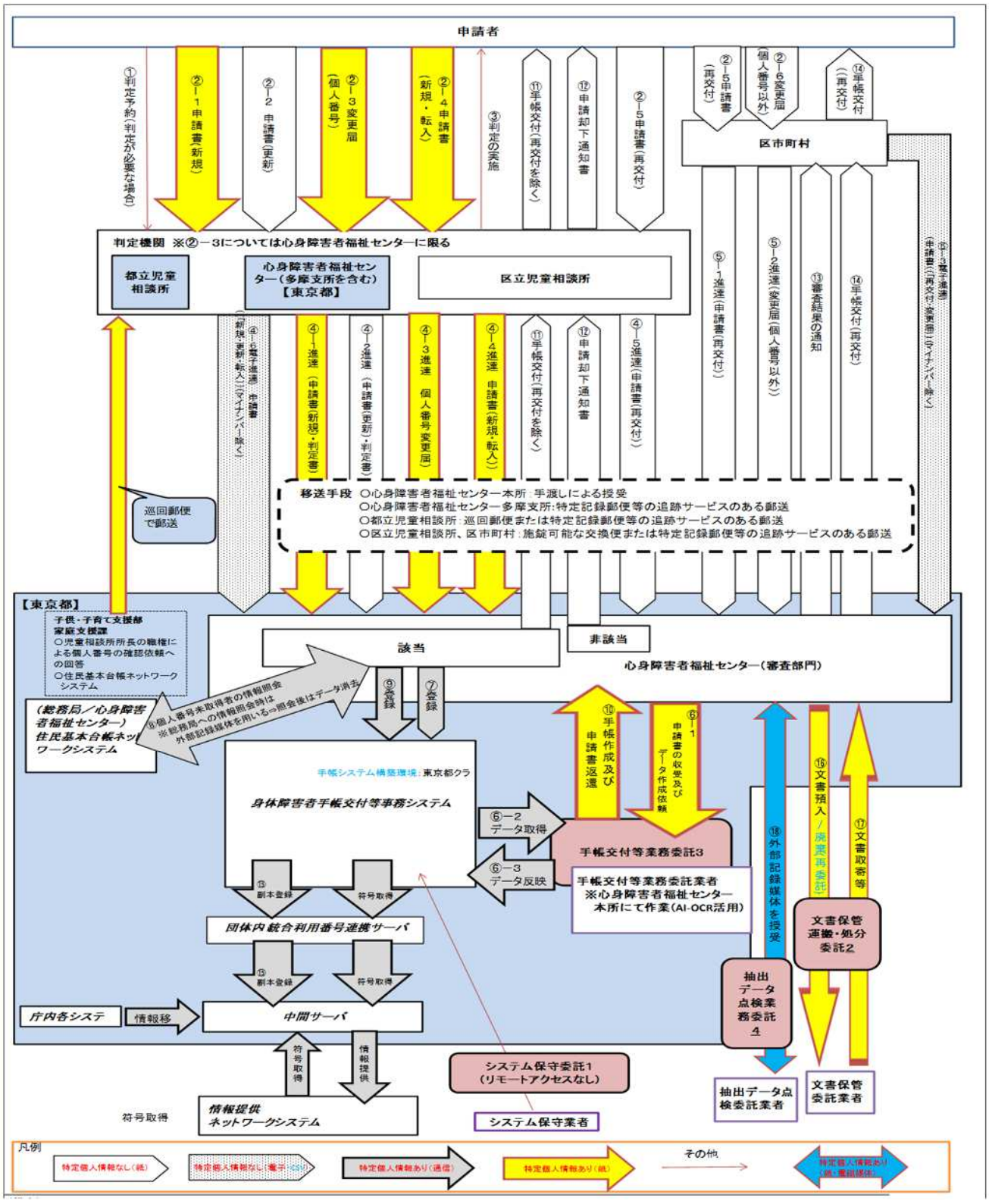
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [○] その他　（ 中間サーバ、手帳システム　）
システム4	
①システムの名称	中間サーバ
②システムの機能	・符号及び団体内統合利用番号の取得、管理 ・符号、団体内統合利用番号の紐付管理 ・副本管理 ・情報照会の受付及び管理 ・情報提供管理
③他のシステムとの接続	[○] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [○] その他　（ 連携サーバ　）
3. 特定個人情報ファイル名	
愛の手帳交付台帳ファイル	
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	・愛の手帳の台帳管理（整理統合等）をするため。 ・愛の手帳の交付に関する情報の提供が必要となるため。
②実現が期待されるメリット	・正確な台帳管理に資する。 ・愛の手帳所持者が対象となる各種手続きの利便化及び簡略化が期待される。
5. 個人番号の利用　※	
法令上の根拠	・行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「マイナンバー法」という）第9条第1項、別表8の項、50の項
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[　　実施する　　] ＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	・番号法　別表　第7項、第8項、第9項、第14項、第21項、第24項、第25項、第27項、第52項、第53項、第55項、第56項、第83項、第93項、第115項、第117項、第127項、 ・番号法第19条第8号に基づく主務省令第2条の表　14項、18項、20項、25項、37項、49項、53項、76項、77項、80項、83項、113項、124項、141項、144項、155項
7. 評価実施機関における担当部署	
①部署	福祉局心身障害者福祉センター障害認定課
②所属長の役職名	障害認定課長
8. 他の評価実施機関	
都内区市町村長	

（別添1）事務の内容

実施マニュアル_様式1
[都様式]

事務・システムフロー図

事務の名称	愛の手帳の交付に関する事務
システムの名称	身体障害者手帳交付等事務システム
担当部署	福祉局心身障害者福祉センター障害認定課



（備考）

① 判定を受ける必要がある新規・更新の場合、申請者は申請に先立って判定機関に対して判定の予約を行う。
（18歳以上は心身障害者福祉センター、18歳未満は都立児童相談所または区立児童相談所）

②－1・2　判定機関は申請者から申請書（新規、更新）を受け付ける。（新規は個人番号記載必須）
新規の場合、判定機関は番号利用法で規定された手続きに則り、申請者から個人番号を取得する。
※住民基本台帳ネットワーク・住民基本台帳を参照可能な判定機関においては上の方法のほか、職権により個人番号の確認、取得を行うことができる。
（都立児童相談所は、子供・子育て支援部家庭支援課に「個人番号の確認依頼書」を送付して、個人番号を取得する。）

②－3　判定機関（多摩支所を含む心身障害者福祉センターに限る。）は個人番号が変更になった愛の手帳所持者から個人番号変更届を受け付ける。
判定機関は番号利用法で規定された手続きに則り、届出者から個人番号を取得する。
※住民基本台帳ネットワークを参照可能な判定機関においては上の方法のほか、職権により個人番号の確認、取得を行うことができる。

②－4　判定機関は申請者から申請書（転入）を受け付ける。※転入は新規の扱いとなる。
受付を行った判定機関は番号利用法で規定された手続きに則り、申請者から個人番号を取得する。
※住民基本台帳ネットワークを参照可能な判定機関においては上の方法のほか、職権により個人番号の確認、取得を行うことができる。
（都立児童相談所は、子供・子育て支援部家庭支援課に「個人番号の確認依頼書」を送付して、個人番号を取得する。）

②－5　判定機関または区市町村は申請者から申請書（再交付）を受け付ける。

②－6　区市町村は申請者から個人番号変更以外の変更届（居住地変更、氏名変更、返還等）を受け付ける。

③　判定機関は判定の予約を受け付けた者に対して、愛の手帳の判定基準に基づく判定を行う。

④－1・2・4・5・6　判定機関は判定の実施後、判定書を作成し、申請書とともに心身障害者福祉センター（以下、「センター」と言う。なお、ここでは審査部門を指す。）に進達する。
※6は電子進達（マイナンバーは除く）。判定機関との調整が必要。

④－3　判定機関は受付をした個人番号変更届、申請書（再交付）をセンターに進達する。

⑤－1・2・3　区市町村は申請書（再交付）、個人番号以外の変更届をセンターに進達する。
※3は電子進達（マイナンバーは除く）。区市町村との調整が必要。

⑥－1・2・3　新規申請（転入含む）の対象者については、手帳交付等業務委託業者が申請書を用いて、身体障害者手帳交付等事務システムに手帳の作成に必要な情報を登録する。なお、カード様式の場合は、システムからデータを取得し手帳を作成する。

⑦ 更新・再交付申請の対象者及び変更届の対象者については、職員が身体障害者手帳交付等事務システムに変更情報を登録する。（職員が行う。）

⑧ （判定機関が個人番号を取得できない場合）職員が総務局に照会し、個人番号を取得する。（一括照会、外部媒体を用いる）
※外部記録媒体は専用の棚に施錠保管し、利用する際はその都度、利用簿に記録を残す。また、記録されたデータは使用完了後に速やかに消去し、廃棄する場合は物理的な破砕処理にて廃棄を行う。
住基端末から住民基本台帳ネットワークに接続し、個別照会で個人番号を取得する。
※令和5年2月以前に愛の手帳を取得した者については判定機関において個人番号の取得ができないため、審査機関において職員が職権により取得を行う。

⑨ センターが照会して入手した個人番号を、職員が身体障害者手帳交付等事務システムに登録する。

⑩ 身体障害者手帳交付等事務システムを用いて手帳交付等業務委託業者が手帳を作成し、発送先（判定機関または区市町村）ごとに振り分け、施錠可能な専用の交換便袋等に手帳を封入する。また、作業終了後は申請書を返還する。

⑪ 審査の結果、愛の手帳の判定基準に該当する対象者に対して、センターは判定機関を経由して手帳を交付する（再交付を除く）。
また、センターは審査結果を判定機関に通知する。

⑫ 審査の結果、愛の手帳の判定基準に該当しない対象者に対して、センターは判定機関を経由して申請却下通知書を交付する。

⑬ センターは審査結果を障害者の援護実施機関である区市町村に通知し、情報共有する。

⑭ 再交付の申請者に対して、センターは区市町村を経由して手帳を交付する。

⑮ 職員は愛の手帳の副本情報を中間サーバに登録する。
※DV・虐待等の被害者など、特別な配慮を必要とする場合は不開示コード等を設定する。

⑯ 職員は愛の手帳交付決定原議を文書保管委託業者に預け入れ、文書管理規則に則った保存を行う。

⑰ 更新・再交付申請時に過去の障害判定内容を確認する場合、職員が開示請求・行政間照会時に保管委託業者から預け入れた文書を取り寄せる。

⑱ マイナンバー総点検に係る、身体障害者手帳等交付システムから抽出したデータと、手帳システム及び住基システムから抽出したデータの照合を行う。
照合の結果に基づき、誤りの原因を個々に究明の上、手帳システムのデータを修正し、再度、符号取得及び副本登録を行う。（データの照合委託事項は、今後必要に応じて実施する）

<No.⑱の事務詳細フロー>
①データの抽出：職員が例年使用するツールにより情報抽出します。（手帳番号＋マイナンバー＋4情報等）Ⓐ
②データの搬送：抽出したデータの一部（手帳番号＋個人番号）をCD-Rに保存し、搬送します。（住基所管部署）
③データの受領：個人番号をキーに住基システムからの情報（個人番号＋４情報）を受領します。Ⓑ
④データの搬送：データⒶⒷをCD-Rに保存し、特定封筒にてゆうパックにて送付します。（マイナンバー紐づけ誤り点検委託業者）
⑤データの受領：紐づけ誤りチェック結果のデータをCD-Rで受領します。
⑥データの反映：誤りの個人番号をただし正しい番号に修正します

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		
愛の手帳交付台帳ファイル		
2. 基本情報		
①ファイルの種類 ※		[　　システム用ファイル　　] ＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※		東京都に居住地を有する知的障害者及び申請者本人が18歳未満の場合はその保護者
	その必要性	愛の手帳交付台帳の管理を行うため。
④記録される項目		[　10項目以上50項目未満　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目 ※	・識別情報 [○] 個人番号　[　] 個人番号対応符号　[○] その他識別情報（内部番号） ・連絡先等情報 [○] 5情報（氏名、氏名の振り仮名、性別、生年月日、住所）　[○] 連絡先（電話番号等） [○] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[　] 地方税関係情報　[　] 健康・医療関係情報 [　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[○] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [　] その他　（　　）
	その妥当性	【個人番号】 他の機関等から情報照会があった場合に利用するため、記録する必要がある。 【その他識別番号（手帳番号）、4情報、障害者福祉関係情報】 愛の手帳に記載される事項であるため。 【連絡先、その他の住民票関係情報】 本人へ連絡をする場合に利用するため。 在住要件を確認し、対象者を正確に確認するため。
	全ての記録項目	別添2を参照。
⑤保有開始日		令和5年2月
⑥事務担当部署		福祉局心身障害者福祉センター障害認定課

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 （ 総務局（住民基本台帳ネットワーク） ） [ ] 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 （ 各判定機関長 ） [ ] 民間事業者 （ ） [ ] その他 （ ）
②入手方法		[○] 紙 [○] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 電子メール [ ] 専用線 [ ] 庁内連携システム [ ] 情報提供ネットワークシステム [○] その他 （ 住民基本台帳ネットワークシステム ）
③入手の時期・頻度		・愛の手帳の新規、更新及び再交付申請並びに他県転入届出の都度入手する。 ・都においては、各判定機関長が個人番号の確認ができず進達した場合等必要に応じて、入手する。 ・各判定機関長においては、本人又は本人の代理人が申請した場合に、その都度入手する。
④入手に係る妥当性		〔申請・届出〕 愛の手帳の申請・記載事項の変更の届出は、愛の手帳交付等申請書（以下「申請書」という。）の提出によることが、東京都愛の手帳交付要綱第3条に定められている。 〔本人確認情報〕 ・マイナンバー法第19条第8号別表の第50項規定される情報提供に対応するため、身体障害者福祉法第15条第1項、同施行令第9条第2項、東京都身体障害者手帳に関する規則第2条で規定する申請書の提出により、本人確認情報を取得する。 ・マイナンバー法第19条第8号別表の第50項に規定される情報提供に対応するため、住民基本台帳ネットワークシステムより、本人確認情報を取得する。
⑤本人への明示		〔申請・届出〕 ・チェックシートを配布し申請者に明示している。 ・本人又は保護者の意思により申請書を記入、提出している。 ・申請書は東京都愛の手帳交付要綱第3条に基づき入手している。 〔本人確認情報〕 住民基本台帳法第30条の15により利用可能な事務として規定されているため。
⑥使用目的 ※		・東京都に居住地を有する愛の手帳保有者の交付台帳の状況を記録、更新、管理するため。 ・愛の手帳が各種のマイナポータル連携サービスを利用し、利便性の向上を図るため。
	変更の妥当性	―
⑦使用の主体	使用部署 ※	福祉局心身障害者福祉センター障害認定課
	使用者数	[10人以上50人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
⑧使用方法 ※		1台帳管理 ：台帳には氏名、生年月日、性別、住所のほか、判定度数、過去の手帳発行履歴などについて記録され、愛の手帳の交付、再交付、転入、住所変更、氏名変更、返還の各申請・届出について台帳に記録する。 2手帳発行 ：交付、再交付（更新、再交付）の手帳の発行を行う。 3統計 ：統計のデータについてシステムより出力する。
	情報の突合 ※	住基ネットと突合して本人確認を行う。
	情報の統計分析 ※	特定個人情報を用いた統計分析を行わない。

	権利利益に影響を与え得る決定 ※	判定度数の審査を行う。
⑨使用開始日		令和5年2月1日
4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] ＜選択肢＞ 1）委託する 2）委託しない （ 4 ） 件
委託事項1		身体障害者手帳交付等事務システムの保守委託
①委託内容		身体障害者手帳交付等事務システムの保守業務（システム運用に関するヘルプデスク、障害発生時の対応支援、定期点検、軽微なシステム改修）
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] ＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[10万人以上100万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	東京都に居住地を有する愛の手帳保有者（他県転出者が東京都に居住していた際の情報を含む）
	その妥当性	身体障害者手帳交付等事務システムの安定的な稼働のため、システム障害等に対応する場合に限り、特定個人情報ファイルの取扱いが必要となる。
③委託先における取扱者数		[10人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ]専用線 [ ]電子メール [ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ [ ]紙 [○]その他 （ 委託先への特定個人情報ファイルの提供はないが保守業務上閲覧する可能性がある。 ）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		SDCソリューションズ株式会社
再委託	⑦再委託の有無 ※	[再委託しない] ＜選択肢＞ 1）再委託する 2）再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	
委託事項2～5		
委託事項2		文書保管運搬・処分委託
①委託内容		愛の手帳に係る各申請・各届出を行った者の申請書及び診断書を東京都文書管理規則及び「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）」等の関係法令に則り保管する。 また、保存期間を経過した書類が発生した場合は溶解処理等により廃棄する。
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一部] ＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[10万人以上100万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上

	対象となる本人の範囲 ※	愛の手帳に係る各申請・各届出を行った者
	その妥当性	愛の手帳に係る各申請・各届出を行った者の申請書及び判定書の保管及び廃棄を適切に行うため、専用の業者に特定個人情報を提供する必要がある。
③委託先における取扱者数		[10人以上50人未満] ＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ]専用線　[ ]電子メール　[ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ　[○]紙 [ ]その他　（　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		株式会社　NXワンビシアーカイブズ
再委託	⑦再委託の有無 ※	[再委託する] ＜選択肢＞ 1）再委託する　2）再委託しない
再委託	⑧再委託の許諾方法	文書による許諾
再委託	⑨再委託事項	依頼に基づく溶解処理の実施
委託事項3		東京都心身障害者福祉センター身体障害者手帳及び愛の手帳の交付業務等委託
①委託内容		AI-OCRを用いた愛の手帳の新規・更新・再交付の申請をする者の基本情報（氏名カナ、氏名漢字、住所、電話番号、生年月日、性別、個人番号及び本人が18歳以下の場合は保護者氏名、続柄、住所、個人番号）の入力及び障害者手帳作成・交換便等への封入作業の委託
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの一部] ＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[1万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	愛の手帳に係る申請を行った者
	その妥当性	愛の手帳に係る申請を行った者の情報を効率的に台帳登録し、円滑に障害者手帳を交付するため。
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		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		マンパワーグループ株式会社

再委託	⑦再委託の有無 ※	[　　再委託しない　　] ＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	
委託事項4		身体障害者手帳交付等事務システム抽出データの点検業務委託
①委託内容		マイナンバー情報総点検に係る身体障害者手帳交付等事務システムから抽出したデータと、団体内統合宛名システム及び中間サーバから抽出したデータの照合
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの一部] ＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	身体障害者手帳保有者及び愛の手帳保有者
	その妥当性	他県において制度側で管理する制度固有の番号とマイナンバーの間に紐付け誤りが発生したことを受け、個人情報保護の観点からも、紐付けが正確に行われているか、総点検を実施したため。
③委託先における取扱者数		[　　10人以上50人未満　　] ＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[　]専用線　[　]電子メール　[○]電子記録媒体（フラッシュメモリを除く。） [　]フラッシュメモリ　[　]紙 [　]その他　（　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		SDCソリューションズ株式会社
再委託	⑦再委託の有無 ※	[　　再委託しない　　] ＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	
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　（　17　）件　[○]移転を行っている　（　3　）件 [　]行っていない
提供先1		道府県知事又は区市町村長
①法令上の根拠		マイナンバー法第9条別表第21項
②提供先における用途		児童福祉法による負担能力の認定又は費用の徴収に関する事務であって主務省令で定めるもの

③提供する情報	・被措置児童又は当該措置児童と同一の世帯に属する者に係る東京都愛の手帳交付要綱（昭和42年3月20日付42民児精発第58号）第五条の愛の手帳の交付に関する情報 ・保護児童又は当該保護児童と同一の世帯に属する者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付に関する情報 ・措置児童又は当該措置児童の扶養義務者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付に関する情報
④提供する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先2～5	
提供先2	区市町村長
①法令上の根拠	マイナンバー法第9条別表第24項
②提供先における用途	地方税法その他の地方税に関する法律及びこれらの法律に基づく条例による地方税の賦課徴収に関する事務であって主務省令で定めるもの
③提供する情報	納税義務者又は当該納税義務者の配偶者若しくは扶養親族に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報
④提供する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先3	道府県知事
①法令上の根拠	マイナンバー法第9条別表第25項
②提供先における用途	地方税法その他の地方税に関する法律及びこれらの法律に基づく条例による地方税の賦課徴収に関する事務であって主務省令で定めるもの
③提供する情報	納税義務者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報
④提供する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上

⑤提供する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先4	公営住宅法第二条第十六号に規定する事業主体である道府県知事又は区市町村長
①法令上の根拠	マイナンバー法第9条別表第27項
②提供先における用途	公営住宅法による公営住宅の管理に関する事務であって主務省令で定めるもの
③提供する情報	公営住宅の入居者又はその同居者に係る東京都愛の手帳交付要綱第二条の愛の手帳の交付及びその障害の程度に関する情報
④提供する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先5	住宅地区改良法第二条第二項に規定する施行者である道府県知事又は区市町村長
①法令上の根拠	マイナンバー法第9条別表第52項
②提供先における用途	住宅地区改良法による改良住宅の管理若しくは家賃若しくは敷金の決定若しくは変更又は収入超過者に対する措置に関する事務であって主務省令で定めるもの
③提供する情報	改良住宅の入居者又はその同居者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報
④提供する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	改良住宅の入居者又はその同居者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度

提供先6～10	
提供先6	厚生労働大臣
①法令上の根拠	マイナンバー法第9条別表第7項、第53項
②提供先における用途	障害者の雇用の促進等に関する法律による職業紹介等、障害者職業センターの設置及び運営、納付金関係業務若しくは納付金関係業務に相当する業務の実施、在宅就業障害者特例調整金若しくは報奨金等の支給又は登録に関する事務であって主務省令で定めるもの
③提供する情報	求職者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報
④提供する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先7	区市町村長
①法令上の根拠	マイナンバー法第9条別表第55項
②提供先における用途	災害対策基本法による被災者台帳の作成に関する事務
③提供する情報	被災者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報
④提供する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先8	道府県知事等
①法令上の根拠	マイナンバー法第9条別表第56項
②提供先における用途	児童扶養手当法による児童扶養手当の支給に関する事務であって主務省令で定めるもの

③提供する情報	・手当支給児童に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報 ・手当改定児童に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報 ・一部支給停止の適用除外に関する届出を行う者又は当該届出に係る児童に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報 ・現況届出児童に係る身東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報 ・障害の状態の届出に係る児童に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報
④提供する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先9	厚生労働大臣
①法令上の根拠	マイナンバー法第9条別表第83項
②提供先における用途	雇用保険法による雇用安定事業又は能力開発事業の実施に関する事務であって主務省令で定めるもの
③提供する情報	助成金の支給に係る労働者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報
④提供する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先10	特定優良賃貸住宅の供給の促進に関する法律第十八条第二項に規定する賃貸住宅の建設及び管理を行う道府県知事又は区市町村長
①法令上の根拠	マイナンバー法第9条別表第93項
②提供先における用途	特定優良賃貸住宅の供給の促進に関する法律による賃貸住宅の管理に関する事務であって主務省令で定めるもの
③提供する情報	入居の申込みをした者又はその者と同居をしようとする者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報

④提供する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先11～15	
提供先11	独立行政法人日本学生支援機構
①法令上の根拠	マイナンバー法第9条別表第115項
②提供先における用途	独立行政法人日本学生支援機構法による学資の貸与及び支給に関する事務であって主務省令で定めるもの
③提供する情報	・学資金申請者又は当該学資金貸与申請者と生計を共にする者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報 ・猶予申請者又は当該猶予申請者と住居及び生計を共にする者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報 ・学資貸与金の貸与を受けたもの若しくは学資支給金を返還すべき者若しくは学資支給金を納入すべき者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報
④提供する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先12	道府県知事又は区市町村長
①法令上の根拠	マイナンバー法第9条別表第117項
②提供先における用途	障害者の日常生活及び社会生活を総合的に支援するための法律による自立支援給付の支給又は地域生活支援事業の実施に関する事務であって主務省令で定めるもの

③提供する情報	・自立支援給付の支給の申請を行う障害者又は当該申請に係る障害児に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報 ・地域相談支援給付決定の変更に係る障害者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報 ・支給認定の申請を行う障害者又は当該申請に係る障害児に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報 ・申請内容の変更の届出を行う障害者又は当該届出に係る障害児に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報
④提供する情報の対象となる本人の数	[　10万人以上100万人未満　]　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先13	区市町村長
①法令上の根拠	マイナンバー法第9条別表第127項
②提供先における用途	子ども・子育て支援法による子どものための教育・保育給付の支給又は地域こども・子育て支援事業の実施に関する事務であって主務省令で定めるもの
③提供する情報	子どものための教育・保育給付に係る支給決定に係る小学校就学前子ども又は当該小学校就学前子どもと同一の世帯に属する者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付に関する情報
④提供する情報の対象となる本人の数	[　10万人以上100万人未満　]　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先14	区市町村長
①法令上の根拠	マイナンバー法第9条別表第9項
②提供先における用途	児童福祉法による障害児通所給付費、特例障害児通所給付費若しくは高額障害児費の支給又は障害福祉サービスの提供に関する事務であって主務省令で定めるもの

③提供する情報	・障害児通所給付費又は特例障害児通所給付費決定に係る障害児に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付に関する情報 ・障害福祉サービスが提供される障害児又は当該障害児と同一の世帯に属する者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付に関する情報
④提供する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先15	区市町村長
①法令上の根拠	マイナンバー法第9条別表第21項
②提供先における用途	身体障害者福祉法による障害福祉サービス、障害者支援施設等への入所等の措置に関する事務
③提供する情報	・障害福祉サービスが提供される知的障害者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付に関する情報 ・障害者支援施設等への入所等の措置に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付に関する情報
④提供する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先16～20	
提供先16	道府県知事又は区市町村長
①法令上の根拠	マイナンバー法第9条別表第14項
②提供先における用途	予防接種法による予防接種の実施に関する事務であって主務省令で定めるもの
③提供する情報	予防接種の対象者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付に関する情報

④提供する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先17	道府県知事
①法令上の根拠	マイナンバー法第9条別表第8項
②提供先における用途	児童福祉法による障害児入所給付費、高額障害児入所給付費又は特定入所障害児食費等給付費の支給に関する事務であって主務省令で定めるもの
③提供する情報	児童福祉法による障害児入所給付費、高額障害児入所給付費又は特定入所障害児食費等給付費の支給に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付に関する情報
④提供する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ情報
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
移転先1	福祉局子供・子育て支援部
①法令上の根拠	マイナンバー法第9条別表第8項、 行政手続における特定の個人を識別するための番号の利用等に関する法律に基づく個人番号の利用並びに特定の個人情報の利用及び提供に関する条例（以下「利用条例」という。）第4条第2項
②移転先における用途	児童福祉法による負担能力の認定又は費用の徴収に関する事務
③移転する情報	・被措置児童又は当該措置児童と同一の世帯に属する者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付に関する情報 ・保護児童又は当該保護児童と同一の世帯に属する者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付に関する情報 ・措置児童又は当該措置児童の扶養義務者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付に関する情報
④移転する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上

⑤移転する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同上
⑥移転方法	[○] 庁内連携システム　　[　] 専用線 [　] 電子メール　　[　] 電子記録媒体（フラッシュメモリを除く。） [　] フラッシュメモリ　　[　] 紙 [　] その他　（　　）
⑦時期・頻度	庁内連携システムを通じて特定個人情報の提供依頼のあった都度
移転先2～5	
移転先2	主税局課税部、資産税部、徴収部
①法令上の根拠	マイナンバー法第9条別表第24項、第25項、利用条例第4条第2項
②移転先における用途	地方税法その他の地方税に関する法律及びこれらの法律に基づく条例による地方税の賦課徴収に関する事務
③移転する情報	納税義務者に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報
④移転する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同上
⑥移転方法	[○] 庁内連携システム　　[　] 専用線 [　] 電子メール　　[　] 電子記録媒体（フラッシュメモリを除く。） [　] フラッシュメモリ　　[　] 紙 [　] その他　（　　）
⑦時期・頻度	庁内連携システムを通じて特定個人情報の提供依頼のあった都度
移転先3	福祉局子供・子育て支援部
①法令上の根拠	マイナンバー法第9条別表第43項、利用条例第4条第2項
②移転先における用途	児童扶養手当法による児童扶養手当の支給に関する事務
③移転する情報	手当支給児童に係る東京都愛の手帳交付要綱第五条の愛の手帳の交付及びその障害の程度に関する情報
④移転する情報の対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同上
⑥移転方法	[○] 庁内連携システム　　[　] 専用線 [　] 電子メール　　[　] 電子記録媒体（フラッシュメモリを除く。） [　] フラッシュメモリ　　[　] 紙 [　] その他　（　　）
⑦時期・頻度	庁内連携システムを通じて特定個人情報の提供依頼のあった都度

6. 特定個人情報の保管・消去

①保管場所 ※		【個人番号を付した申請書及び外部記録媒体】 執務室内及び専用の管理棚において施錠保管している。 また、申請書については適宜、文書保管運搬・処分業者に引き渡し保管する。委託先については「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）」及び関係法令に合致した安全管理体制の構築を義務付ける。 【手帳システム】 CSPが提供するクラウドサービスに東京都クラウドインフラとして必要と考えられる統制機能やセキュリティ設定を適用した「クラウドインフラサービス」基盤上に構築される。 採用するCSPは、AWSとなり、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスとなる。 このため、特定個人情報の適正な取扱いに関するガイドラインで求める物理的対策を満たしており、主に以下の物理的対策を講じている。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・許可されたアカウント以外は特定個人情報にアクセスできないように制御している。 ・日本国内にデータセンターが存在するクラウドサービスを利用している。 ・特定個人情報は、CSPが管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターに保存される。 ・サーバのウイルスパターンファイル、セキュリティパッチ等の適用タイミングについて、原則最新のものが公表された都度とするが、詳細についてはシステム保守業者との調整によることとする。 ・手帳システムバックアップの保存領域は、AWS Backupを利用して別リージョンに保管する想定。 【中間サーバ・プラットフォーム】 ①中間サーバ・プラットフォームは政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。 ②特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する中間サーバのデータベース内に保存され、バックアップもデータベース上に保存される。 【連携サーバ】 ① 連携サーバは、サーバ等を設置するための専用施設内に他のシステムとは分離した区画を設け、当該サーバ専用のラックに施錠して収容する。当該施設では、入退室者管理、区画ごとの施錠管理、監視カメラによる録画、有人監視等を実施する。 ② 当該施設の煙感知装置、ガス系消火設備、耐震対応等により、火災や地震に起因する滅失等のリスクを低減する。
②保管期間	期間	[20年以上] ＜選択肢＞ 1）1年未満 2）1年 3）2年 4）3年 5）4年 6）5年 7）6年以上10年未満 8）10年以上20年未満 9）20年以上 10）定められていない
	その妥当性	・愛の手帳の効力は、愛の手帳所持者が生存している間は有効であるため、知的障害程度等級及び交付決定の根拠となる書類の長期間の保存が必要となる。 ・行政処分庁として、文書管理規則上、最長の30年保存としている。 ・台帳データ（サーバ内データ）については常に使用し続けるため、常用の取り扱いとしている。

③消去方法	【中間サーバ・プラットフォーム】 ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度（ISMAP）に準拠したデータの暗号化消去及び物理的破壊を行う。さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ③中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。 【連携サーバ】 連携サーバで使用する機器のうち、特定個人情報等のデータが記録されうるものの廃棄等に当たっては、磁気的消去又は物理的破壊等により、当該データを復元不可能な状態とする。 【文書保管運搬・処分】 ・文書保管運搬・処分業者に引き渡し文書のうち、廃棄文書が発生した場合は、仕様書により安全管理措置の講じた区域内で破砕・溶解の処理を行う。 【手帳システム】 ・保存用以外の業務委託用の申請書は、身体障害者手帳発行後、担当職員がシュレッダーにて裁断している。 ・文書保管運搬・処分業者に引き渡し文書のうち、廃棄文書が発生した場合は、仕様書により安全管理措置の講じた区域内で破砕・溶解の処理を行う。 ・本システム端末のデータ消去を委託する際には、職員等が立ち会い削除するか、委託先からの書面による確証を得たうえでデータが消去されていることを確認する。 ・東京都クラウドに保存されているデータの削除については、構築するシステム上でデータ消去機能を付加する、又は別途委託の上、削除を検討する。 【外部記録媒体】 ・専用の棚に施錠保管し、利用する際はその都度、利用簿に記録を残す。外部記録媒体を廃棄する場合は物理的な破砕処理にて廃棄を行う。 ・外部記録媒体に記録されたデータは使用完了後に速やかに消去している。

7. 備考

－

（別添2）特定個人情報ファイル記録項目

愛の手帳交付台帳ファイル

1. 手帳発行者
2. 手帳番号
3. 氏名カナ
4. 氏名漢字
5. 性別
6. 住所
7. 自治体名
8. 保護者氏名
9. 保護者住所
10. 続柄
11. 生年月日
12. 障害内容（※）
13. 種別（※）
14. 級（※）
15. 再認定日
16. 再発行事由
17. 転出先都道府県
18. 転入日
19. 転出日
20. 返還事由
21. 返還日
22. 氏名履歴
23. 住所履歴
24. 手帳発行履歴
25. 特記事項
26. 個人番号
27. 団体内統合利用番号
28. 宛名連携状況
29. 不開示コード
30. 自動応答不可設定

（※）は要配慮個人情報となっている。

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	
愛の手帳交付台帳ファイル	
2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1：　目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	・特定個人情報の入手手段は本人からの申請書に限定される。 ・対象者以外の情報を記載することが出来ない書面様式としている。 ・申請の受付窓口である心身センター及び各児童相談所において、マイナンバー法の規定に基づき、本人確認を実施。 ・住民基本台帳ネットワークシステムから入手する本人確認情報の対象者については、使用簿を作成し責任者の承認手続を経た上で入手する。 ・住民基本台帳ネットワークシステムに提供依頼する対象者データは、身体障害者手帳交付等事務システムから抽出する。 ・住民基本台帳ネットワークシステムから取得できる情報は住民基本台帳法を根拠とする。
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	・特定個人情報の入手手段は本人からの申請書に限定される。 ・必要でない情報等を記載することが出来ない書面様式としている。 ・申請の受付窓口である心身センター及び各児童相談所において情報の精査を行っている。 ・住民基本台帳ネットワークシステムは、本人確認情報のみを保有している。 ・住民基本台帳ネットワークシステムから入手する本人確認情報の対象者については、使用簿を作成し責任者の承認手続を経た上で入手する。
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	・特定個人情報の入手手段は本人からの申請書に限定される。 ・東京都愛の手帳交付要綱に基づき、各児童相談所長を経由して入手している。 ・申請者に対し、パンフレットを配布し入手方法を明示している。 ・住民基本台帳ネットワークシステムを所管する総務局が定める利用届により、住民基本台帳法により本人確認情報の利用が認められている旨を申請し、総務局の許可を事前に受けた上で入手を行う。 ・住民基本台帳ネットワークシステムを所管する総務局が定める様式及び方法により、入手を行う。 ・住民基本台帳ネットワークシステムから入手する本人確認情報の対象者については、使用簿を作成し責任者の承認手続を経た上で入手する。 ・電子メールでの進達に記載の情報（最低基本4情報）と同一の情報をマイナンバー紙書面にも記載の上、進達し、入力した画面上で地区担当がダブルチェックを行うことで紐づけ誤りの防止を図る。
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	・申請の受付窓口である心身センター及び各児童相談所において、マイナンバー法第16条、マイナンバー法政令第12条第1項、マイナンバー法施行規則第1条等の規定に基づき、本人確認を実施。都は、本人確認の措置を実務手引書に追加して区市町村に周知する。 ・個人番号が進達されない場合は、都において、職権により住民基本台帳ネットワークにより取得する。 ・住民基本台帳を所管する各自治体において正確性は確保されている。
個人番号の真正性確認の措置の内容	・申請の受付窓口である心身センター及び各児童相談所において、マイナンバー法第16条、マイナンバー法政令第12条第1項、マイナンバー法施行規則第1条等の規定に基づき、真正性の確認を実施。都は、真正性確認の措置を実務手引書に追加して区市町村に周知する。 ・個人番号が進達されない場合は、都において、職権により住民基本台帳ネットワークにより取得する。 ・住民基本台帳を所管する各自治体において正確性は確保されている。
特定個人情報の正確性確保の措置の内容	・申請の受付窓口である心身センター及び各児童相談所において記載内容の確認を行う。 ・都におけるシステム入力内容については、入力者とは別な職員による相互チェックを行っている。 ・住民基本台帳を所管する各自治体において正確性は確保されている。
その他の措置の内容	―

リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク4：　入手の際に特定個人情報が漏えい・紛失するリスク		
リスクに対する措置の内容	【移送手段】 ・心身障害者福祉センター本所：手渡しによる授受 ・心身障害者福祉センター多摩支所:特定記録郵便等の追跡サービスのある郵送 ・都立児童相談所：巡回郵便または特定記録郵便等の追跡サービスのある郵送 ・区立児童相談所、区市町村：施錠可能な交換便または特定記録郵便等の追跡サービスのある郵送 ・特定個人情報等が記録された電子媒体又は書類等を持ち運ぶ必要が生じた場合には、容易に個人番号が判明しないよう安全な方策を講ずる。 【保管方法】 ・各児童相談所長から入手した申請書、判定書は収受簿に記録し、専用の棚で施錠保管を行っている。 【住民基本台帳ネットワークシステム】 （判定機関が個人番号を取得できない場合） ・職員が総務局に照会し、個人番号を取得する。（一括照会、外部媒体を用いる） ・住基端末から住民基本台帳ネットワークに接続し、個別照会で個人番号を取得する。	
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、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容	【連携サーバ】 連携サーバは、各事務所管部署で本人確認及び真正性確認を行った個人番号に基づき、個人番号、団体内統合利用番号及び個別業務システム利用番号を紐付けて管理する。これらの情報は、ユーザIDにより利用者・個別業務システム（事務）等の単位でアクセス可能な範囲が限定され、正当な権限のない利用者・個別業務システム（事務）等からは利用できないようアクセス制御を行っている。	
事務で使用するその他のシステムにおける措置の内容	手帳システムでは利用者の範囲を制限している。	
その他の措置の内容	－	
リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク2：　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク		
ユーザ認証の管理	[　行っている　]	＜選択肢＞ 1）行っている　　2）行っていない
具体的な管理方法	・情報システム管理者が指定した特定の端末でのみの使用である。 ・システムを使用する職員を特定し、個人ごとにユーザIDを割り当てるとともに、IDとパスワードによるユーザ認証を行う。また、パスワードは有効期間を1年としている。。さらに、ログイン情報は操作ログとして保管されており、どのタイミングで誰がログインしたのかが把握できるようにする。 ・外部記録媒体は、専用のID・パスワードが割り振られている。 ・手帳システムで使用する端末はID・パスワード以外に静脈認証の二要素認証を導入している。	
アクセス権限の発効・失効の管理	[　行っている　]	＜選択肢＞ 1）行っている　　2）行っていない
具体的な管理方法	・情報システム管理者がシステム利用者一覧表を作成し、一元的にID権限の管理を行っている。 ・利用者の異動に際し、管理者の権限でID、パスワード発行、失効の管理を行っている。	
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	・ID及び権限を利用者ごとに設定した一覧表について、情報システム管理者による承認手続きを経ることにより管理の適正性についてチェックする。 ・職員の担当業務に合わせて、システムアカウント毎に使用権限を制限しており、システムを使用することができる職員を限定する。 ・人事異動の都度、権限一覧表の見直しを行う。
特定個人情報の使用の記録		[　　記録を残している　　] ＜選択肢＞ 1）記録を残している　　2）記録を残していない
	具体的な方法	手帳の交付にあたっては、内部承認手続きを経ている。 システムについては、以下を行っている。 ・システムの操作履歴（アクセスログ）を記録し、誰が、いつ、どのような内容の操作を行ったかについて確認できる。 ・記録された操作履歴について、一定期間保存する。 ・情報システム担当者が定期的に手帳システムの専用メニューを利用し、操作履歴（アクセスログ）の点検・分析を行い、目的外閲覧等不要なアクセスがあった場合はその結果を情報システム管理者に報告する。 ・操作履歴は改ざん・消去が出来ないようシステム管理者のみ利用できるようにアクセス制限をかける。
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（アクセスログ）を記録し、誰が、いつ、どのような内容の操作を行ったかについて確認できるようにする。 ・システムを利用する職員へは、着任時の業務説明の際に、システムの適正利用について教育している。 ・情報セキュリティ・個人情報保護の研修で教育している。 ・システムを使用する各端末では庁内ネットワークを経由して、自動的にUSB出力ポートが無効となるように制御設定されている。 ・サーバについては、情報システム担当者に付与されたサーバ管理者IDでのみアクセスが可能とする。 ・サーバは夜間バッチにより深夜12時から翌朝5時まで利用できない。 ・個人情報の保護に関する法律第69条により、事務外での利用又は提供を制限されている。
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク4：　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		・システムのID、パスワードを所持している者以外はシステムにはアクセスできない。 ・情報システム担当者が使用する管理者のID、パスワード以外では、サーバにアクセスできない。 ・システムを使用する各端末では庁内ネットワークを経由して、自動的にUSB出力ポートが無効となるように制御設定されている。 ・台帳情報のファイル出力は、情報システム管理者が許可した情報システム担当者のIDのみの利用としている。 ・情報システム担当者は、業務上の必要から台帳情報のファイル出力を行うときは、使用目的、出力範囲等を明記した書面により情報システム管理者の許可を得ることとシステムセキュリティ管理要綱にて規定している。なお、ファイル出力時には、パスワードを設定する。なお、使用可能な外部記録媒体は限定されている。 ・システムの操作履歴（アクセスログ）を記録し、誰が、いつ、どのような内容の操作を行ったかについて確認できるようにしている。
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置		
・スクリーンセーバ等を利用して、長時間にわたりシステム画面を表示することを防止する。 ・台帳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最小限の範囲にとどめ、職員に対しては使用終了後に即時廃棄するように業務説明の際に教育して、徹底している。		
4. 特定個人情報ファイルの取扱いの委託		**[　]委託しない**
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		

情報保護管理体制の確認		契約時に委託先と取り交わす契約で、 ・責任者、作業体制（従事者全員の職氏名）、連絡体制及び作業場所を書面にして提出 ・業務従事者への遵守事項の周知及び実施報告の提出等を委託先に求めている。 また、委託先がプライバシーマーク等を保持していることを確認している。 加えて、委託元が委託先に対して必要と認める場合には実地調査を行い、適切な管理体制をとっていることを確認するとしている。
特定個人情報ファイルの閲覧者・更新者の制限		[　　制限している　　] ＜選択肢＞ 1）制限している　　2）制限していない
	具体的な制限方法	【委託事項1】 ・委託先への特定個人情報の提供はない。 ・サーバの定期点検等の作業時にID及びパスワードの入力が必要な際は、センター内で情報システム担当者がID、パスワードの入力を行うことで、委託業者の特定個人情報ファイルの閲覧を制限している。 ・特定個人情報へのアクセスについては、想定しておらず、無断で閲覧してしまう可能性があるため、職員立会いの下で保守点検作業を行う。 責任範囲については、以下のとおり。 ＜クラウドインフラサービスの責任範囲＞ 東京都クラウドインフラの責任分界点は、東京都クラウドインフラ利用者、東京都クラウドインフラ及び CSP に分けられる。東京都クラウドインフラの責任範囲は、利用ポリシー、テンプレートなどの管理機能に限定され、業務システムのアプリケーションを中心としたプロダクト管理は、東京都クラウドインフラ利用者の責任となる。 ＜責任分界点の全体像＞ ●東京都クラウドインフラ利用者の責任範囲（開発運用体制） ・データ ・アプリケーション ・マネージドサービス構成 ・ミドルウェア/OS ・ネットワーク構成 ※東京都クラウドインフラ利用者によるセキュリティ設定による。 ●東京都クラウドインフラの責任範囲（東京都クラウドインフラ管理者） ・ネットワーク接続 ・利用ポリシー ・テンプレート ・環境払出し ※東京都クラウドインフラによるセキュリティ設定による。 ●CSPの責任範囲（CSPサポート） ・マネージドサービス ・クラウド基盤 ※クラウド基盤のセキュリティによる。 【委託事項2】 ・作業者を限定するために、委託業務従事者名簿を事前に提出させる。 ・文書の引渡しの際、文書を格納した箱にコードを付与した上で、開封防止のシールを貼付し、封印したうえで運搬する。 【委託事項3】 ・基本情報入力等の作業時にID及びパスワードの入力が必要な際は、センター内で情報システム担当者がID、パスワードの入力を行い、委託業者の特定個人情報ファイルの閲覧を制限する。 ・仕様書に基づく作業体制（従事者全員の職氏名）の提出により、取扱者を明確化している。 【委託事項4】 ・仕様書に基づく作業体制（従事者全員の職氏名）の提出により、取扱者を明確化している。
特定個人情報ファイルの取扱いの記録		[　　記録を残している　　] ＜選択肢＞ 1）記録を残している　　2）記録を残していない
	具体的な方法	【委託事項1】 ・委託先への特定個人情報の提供はない。 ・システムの操作履歴（アクセスログ）を記録し、一定期間保存する。 【委託事項2】 ・委託先との契約に際して、保管庫等での施錠・管理、管理状況の記録等を規定した仕様書により、取扱いに係る必要事項を定める。 ・仕様書により、委託先に、文書の引渡しの都度、引き渡した文書を格納した箱に付与されたコード及び引渡日が記載された確認書を提出させる。 【委託事項3】 ・入力帳票の授受の際に授受票による記録を行う。 ・毎日の作業については業務日誌を提出させる。月ごとに業務報告書を提出させる。 【委託事項4】 ・照合用データの授受、抽出データの納品について、仕様書により取扱いに係る必要事項を定める。 ・データの授受を行う都度、内容が記載された授受簿により確認する。
特定個人情報の提供ルール		[　　定めている　　] ＜選択肢＞ 1）定めている　　2）定めていない

	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	【委託事項1】【委託事項2】【委託事項3】【委託事項4】 ・業務上、委託先から他社への提供はない。 ・再委託の取扱いについては、仕様書上、原則第三者に再委託を禁止することとしている。 ・委託先と取り交わしている「電子情報処理委託に係る標準特記仕様書」において、目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理に対する義務違反時の損害賠償の請求等について規定している。
	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	【委託事項1】 特定個人情報へのアクセスについては、想定しておらず、無断で閲覧してしまう可能性があるため、職員立会いの下で保守点検作業を行うこととしている。 【委託事項2】 ・文書の引渡しの際、文書を格納した箱にコードを付与した上で、開封防止のシールを貼付し、封印して運搬する。また、その際、コード及び引渡日が記載された確認書を提出させる。 ・仕様書により、搬送車の施錠など盗難、紛失等の防止措置を義務付ける。 ・システムにより、入出庫依頼を管理するとともに、保管状況を確認する。 【委託事項3】 ・入力帳票の授受の際に授受票による記録を行う。 ・執務室内での作業となるため、特定個人情報の外部への持ち出しはない。 【委託事項4】 ・データの授受を行う都度、内容が記載された授受簿により確認する。 【委託事項1～4】 ・実地調査等で現地の履行状況を確認する。
特定個人情報の消去ルール		[定めている]　＜選択肢＞ 1）定めている　2）定めていない
	ルールの内容及びルール遵守の確認方法	【委託事項3】 ・仕様書により、保存期限を過ぎた文書について、溶解処理等により、復元不可能な状態とすることを規定し、処理日、処理対象とした文書箱のコード、処理方法、処理結果等を明記した廃棄証明書を取得する。 ・文書の処分については再委託により実施し、リスク対策として仕様書に以下の項目を規定している。 溶解処理は無開梱のまま行うこととし、完了後は溶解証明書（溶解処理を実施したことを示す報告書等）を提出すること。 【委託事項1】【委託事項2】【委託事項3】【委託事項4】 ・実地調査等で現地の履行状況を確認する。 【委託事項4】 ・仕様書により、消去方法などを規定されており、納品物の検査完了後、すべて消去するとともに、データ消去完了証明書の提出を求めている。
委託契約書中の特定個人情報ファイルの取扱いに関する規定		[定めている]　＜選択肢＞ 1）定めている　2）定めていない
	規定の内容	【委託事項1】【委託事項2】【委託事項3】【委託事項4】 以下の事項の遵守を委託契約書において義務付けている。 ・業務の推進体制（業務従事者名簿を含む）に係る報告 ・業務従事者への遵守事項の周知を図ること及び実施報告 ・秘密の保持 ・目的外使用の禁止 ・複写及び複製の禁止 ・作業場所以外への持出禁止 ・情報の保管及び管理に係る遵守事項（契約履行完了時、入退室管理、個人情報等の取扱い） ・再委託の取扱い ・実地調査及び指示等について ・情報の保管及び管理等に対する義務違反について
再委託先による特定個人情報ファイルの適切な取扱いの確保		[再委託していない]　＜選択肢＞ 1）特に力を入れて行ってい　2）十分に行っている 3）十分に行っていない　4）再委託していない
	具体的な方法	―
その他の措置の内容		―
リスクへの対策は十分か		[十分である]　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		

【委託事項1】
保守業務にて特定個人情報を無断で閲覧してしまう可能性があるため、職員立会いの下で保守点検作業を行うこととしている。

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）	[　　]提供・移転しない
リスク1： 不正な提供・移転が行われるリスク	
特定個人情報の提供・移転の記録	[　　記録を残している　　] ＜選択肢＞ 1）記録を残している　2）記録を残していない
具体的な方法	庁内連携【連携サーバ】 全ての照会及び回答について、特定個人情報の照会者、移転者、日時等をシステム上でアクセスログとして記録し、7年間保存する。 【手帳システム】 アクセスログを一定期間保管し、誰がいつどの情報を操作したか記録する。
特定個人情報の提供・移転に関するルール	[　　定めている　　] ＜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	庁内連携【連携サーバ】 ・照会側と提供（回答）側の間で行われる特定個人情報の授受に当たっては、その中継のみを行い、システム内に特定個人情報（副本相当）は保有しない。 ・事務所管部署で決定された申請書を、連携サーバ管理者が承認した上で、システムへの利用者登録、変更を行う。 ・ログイン時に利用者の認証を実施する。 ・照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、法令上正当であると認められ、かつ移転者が明示的に回答を承認した場合に限り、連携を行う。照会に対しては、照会条件として指定された対象者に関する情報だけを回答する。なお、チェック項目は、マイナンバー法等の改正に応じて、更新する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・全ての照会及び回答について、特定個人情報の照会者、移転者、日時等をシステム上でアクセスログとして記録し、7年間保存する。 ・不正アクセス等を検出できるようログを監査する。 【手帳システム】 ①アクセスログを一定期間保管し、誰がいつどの情報を操作したか記録する。 ②副本登録は、内部承認のうえで手帳システムの台帳情報に異動があった都度行う。
その他の措置の内容	―
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である　3）課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク	
リスクに対する措置の内容	庁内連携【連携サーバ】 ・照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められ、かつ移転者が明示的に回答を承認した場合に限り、連携を行う。照会に対しては、照会条件として指定された対象者に関する情報だけを回答する。なお、チェック項目は、マイナンバー法等の改正に応じて、更新する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・全ての照会及び回答について、特定個人情報の照会者、移転者、日時等をシステム上でアクセスログとして記録し、7年間保存する。 【手帳システム】 ・手帳情報は連携サーバを経由してのみ中間サーバに副本登録する。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である　3）課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク	

リスクに対する措置の内容	庁内連携【連携サーバ】 ・照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められ、かつ移転者が明示的に回答を承認した場合に限り、連携を行う。照会に対しては、照会条件として指定された対象者に関する情報だけを回答する。なお、チェック項目は、番号法等の改正に応じて、更新する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・情報照会に対する回答は、当該照会を行った事務に対してのみ返却するよう制御されている。 ・各事務所管部署が個々の照会データを一意に識別できるよう付与した識別子を、連携サーバからの回答データに付記して返却することで、どの照会に対する回答かを各事務所管部署で正確に突合できるようにしている。 【手帳システム】 ・副本登録は、内部承認のうえで手帳システムの台帳情報に異動があった都度行う。 ・副本の正確性確保のため、正本は手帳交付前に職員による相互チェックを行い正確性を確保している。 ・中間サーバでのエラー発生時は、職員により手帳システムと連携サーバの情報を確認し、正確な情報をチェックするエラーフォローを行う。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている

特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置
―

6. 情報提供ネットワークシステムとの接続	**[○] 接続しない（入手） [ ] 接続しない（提供）**
リスク1： 目的外の入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 安全が保たれない方法によって入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク5： 不正な提供が行われるリスク	

リスクに対する措置の内容	【中間サーバ・ソフトウェア】 ①情報提供機能（※）により、情報提供ネットワークシステムにおける照会許可用照合リストを情報提供ネットワークシステムから入手し、中間サーバにも格納して、情報提供機能により、照会許可用照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ②情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。 ③機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ④中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。 【連携サーバ】 ・ログイン時に利用者の認証を実施する。 ・各事務所管部署からの申請に基づき、利用者とその所掌事務の紐付けが連携サーバ上であらかじめ定義され、その範囲においてのみ情報提供が可能となるようアクセス制御されている。 ・システムの利用者、日時等をシステム上でログとして記録し、7年間保存する。 ・個別業務システム（事務）と中間サーバとの間における特定個人情報の授受に当たっては、その中継のみを行い、システム内に特定個人情報（副本相当）は保有しない。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・中間サーバとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。 ・サーバ認証により真正性が担保された中間サーバに接続する。 【手帳システム】 ・手帳システムで使用する端末はID・パスワード以外に静脈認証等の二要素認証を導入している。 ・IDにより、アクセス可能な業務範囲を限定し、正当な権限のない利用者からは個人番号を利用できないようアクセス制御する ・アクセスログを一定期間保管し、情報システム管理者が定期的にアクセスログの点検・分析を行う。 ・手帳情報は、連携サーバを経由してのみ中間サーバに副本登録する。 ・副本登録するファイルは暗号化する。
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	【中間サーバ・ソフトウエア】 ①セキュリティ管理機能（※）により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ②中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。（※）暗号化・復号機能と、鍵情報及び照会許可用照合リストを管理する機能。 【中間サーバ・プラットフォーム】 ①中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、不適切な方法で提供されるリスクに対応している。 ②中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバ・プラットフォームの保守・運用を行う事業者及びクラウドサービス事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。 【連携サーバ】 ・ログイン時に利用者の認証を実施する。 ・各事務所管部署からの申請に基づき、利用者とその所掌事務の紐付けが連携サーバ上であらかじめ定義され、その範囲においてのみ情報提供が可能となるようアクセス制御されている。 ・システムの利用者、日時等をシステム上でログとして記録し、7年間保存する。 ・個別業務システム（事務）と中間サーバとの間における特定個人情報の授受に当たっては、その中継のみを行い、システム内に特定個人情報（副本相当）は保有しない。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・中間サーバとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。 ・サーバ認証により真正性が担保された中間サーバに接続する。 【手帳システム】 ・手帳システムで使用する端末はID・パスワード以外に静脈認証等の二要素認証を導入している。 ・IDにより、アクセス可能な業務範囲を限定し、正当な権限のない利用者からは個人番号を利用できないようアクセス制御する。 ・アクセスログを一定期間保管し、必要に応じてアクセスログを点検・分析する。 ・手帳情報は、連携サーバを経由してのみ中間サーバに副本登録する。 ・副本登録するファイルは暗号化する。

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	＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。 ②情報提供データベース管理機能（※）により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ③情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 （※）特定個人情報を副本として保存・管理する機能。 庁内連携【連携サーバ】 ・照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められ、かつ移転者が明示的に回答を承認した場合に限り、連携を行う。照会に対しては、照会条件として指定された対象者に関する情報だけを回答する。なお、チェック項目は、番号法等の改正に応じて、更新する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・情報照会に対する回答は、当該照会を行った事務に対してのみ返却するよう制御されている。 ・各事務所管部署が個々の照会データを一意に識別できるよう付与した識別子を、連携サーバからの回答データに付記して返却することで、どの照会に対する回答かを各事務所管部署で正確に突合できるようにしている。 【手帳システム】 ・副本登録は、内部承認のうえで手帳システムの台帳情報に異動があった都度行う。 ・副本の正確性確保のため、正本は手帳交付前に職員による相互チェックを行い正確性を確保している。 ・中間サーバでのエラー発生時は、職員により手帳システムと連携サーバの情報を確認し、正確な情報をチェックするエラーフォローを行う。	
リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置		
【中間サーバ・ソフトウエア】 ①中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 【中間サーバ・プラットフォーム】 ①中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバ・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバ・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバ・プラットフォームの保守・運用を行う事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。		
7．特定個人情報の保管・消去		
リスク1：　特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[　　政府機関ではない　　]	＜選択肢＞ 1）特に力を入れて遵守している　2）十分に遵守している 3）十分に遵守していない　4）政府機関ではない
②安全管理体制	[　　十分に整備している　　]	＜選択肢＞ 1）特に力を入れて整備している　2）十分に整備している 3）十分に整備していない
③安全管理規程	[　　十分に整備している　　]	＜選択肢＞ 1）特に力を入れて整備している　2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[　　十分に周知している　　]	＜選択肢＞ 1）特に力を入れて周知している　2）十分に周知している 3）十分に周知していない
⑤物理的対策	[　　十分に行っている　　]	＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない

	具体的な対策の内容	【中間サーバ･プラットフォーム】 ①中間サーバ･プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。 【連携サーバ】 ・サーバ等を設置するための専用施設内に他のシステムとは分離した区画を設け、当該サーバ専用のラックに施錠して収容する。当該施設では、入退室者管理、区画ごとの施錠管理、監視カメラによる録画、有人監視等を実施する。 ・当該施設の煙感知装置、ガス系消火設備、耐震対応等により、火災や地震に起因する滅失等のリスクを低減する。 ・機器のうち、特定個人情報等のデータが記録されうるものの廃棄等に当たっては、磁気的消去又は物理的破壊等により、当該データを復元不可能な状態とする。 【書類】 ・台帳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最小限の範囲にとどめ、職員に対しては使用終了後に即時廃棄するように業務説明の際に教育して、徹底している。 ・各区市福祉事務所長（町村長）から入手した申請書、診断書は専用の棚で施錠保管を行っている。 ・一定期間を経過した申請書及び診断書は東京都文書管理規則に則り、適宜、保管運搬・処分業者へ引き渡し保管する。 ・保存期間を経過した書類が発生した場合は溶解処理等により廃棄する。 ・委託先においては仕様書及び「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）」等の関係法令よる取扱いを義務付ける。 【手帳システム】 ・サーバは東京都クラウドにてデータセンターで管理している。（バックアップサーバも含む） ・データのバックアップは、世代管理する。 ・①契約の終了等に伴い、東京都が借り受けている端末、サーバ、その他電磁的記録媒体などの情報処理機器類を返却する際には、情報を復元できないように処理しなければならない。機器の撤去後にデータ消去を行う場合は、データ消去までの期間におけるサイバーセキュリティ対策を明確に定めること。 ・②　上記①の消去作業を事業者に委託する場合、あらかじめ、契約仕様書にその旨を明記するとともに、データ消去完了証明書を徴取すること。また、必要に応じて、消去作業に職員等を立ち合わせること。 【外部記録媒体】 ・専用の棚に施錠保管し、利用する際はその都度、利用簿に記録を残す。外部記録媒体を廃棄する場合は物理的な破砕処理にて廃棄を行う。 ・外部記録媒体に記録されたデータは使用完了後に速やかに消去している。
⑥技術的対策		[　　十分に行っている　　]　＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない

	具体的な対策の内容	【中間サーバ･プラットフォーム】 ①中間サーバ・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ②中間サーバ・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ④中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤中間サーバーのデータベースに保存される特定個人情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ⑥中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ⑦中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。 【連携サーバ】 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で稼働する。 ・サーバが接続されたセグメントとそれ以外のセグメントの境界にファイアウォールを導入するとともに、ログを取得する。 ・ウイルス対策ソフトを導入し、パターンファイルを更新する。 ・基本ソフトウェア(OS)及びミドルウェアは、必要に応じてセキュリティパッチを適用する。 ・データベースにデータを暗号化して保存する。 ・データベースに対する操作権限を細分化し、連携サーバ管理者であっても真に必要な場合を除いてはデータにアクセスできないよう制御する。 ・データベースに対するアクセスログを取得する。 ・データベースのバックアップを取得する。 ・あらかじめ登録された機器だけがネットワークに接続できるよう制御する。 ・サーバ及びその管理に用いる機器は、書き出し可能な外部記録媒体を内蔵せず、かつUSB機器等に対する制御を行い、外部記録媒体の利用を制限する。 【手帳システム】 ・システムの操作履歴（アクセスログ）を記録する。 ・ウイルス対策ソフトの定期的パターン更新を行うことにより、ウイルス感染を防止している。 ・システムを使用する各端末では庁内ネットワークを経由して、自動的にUSB出力ポートが無効となるように制御設定されている。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で稼働する。 ・サーバが接続されたセグメントと他のセグメント間の通信は制限されている。 ・番号系端末でウイルスを検知した場合、番号系端末が配備されたすべての局の情報化推進担当宛てに、システム管理者から自動でメール通知する。 ・システムで利用する端末、外部記録媒体はドライブ暗号化を使用する。 ・外部記録媒体に記録するデータ及びパスワードファイルは暗号化し、使用完了後は速やかに削除する。 ・廃棄時には内部のデータを復元できないように消去した上で廃棄する。 ・取得している操作ログについて、月単位で定期的に不正なアクセスがなかったか、解析する。 不正なアクセスと思われるものがあった場合、適宜個人情報管理責任者（所管課長）に報告の上、対応を仰ぐ。
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	令和5年（2023年） ①2023年8月1日 受託者における個人情報の漏えいについて（メールアドレスの流出）。総務局の備蓄品有効活用業務の受託者が、案内メールをBCCではなくCCで送信し、43団体分の代表メールアドレス等（41件）と業務用個人メールアドレス（2件）が漏えいしました。発生日は2023年7月28日で、東京都は削除依頼と謝罪を実施し、二次被害は報告されていないとしています。 ②2023年8月17日 受託者における個人情報の漏えいについて。総務局の多摩東京移管130周年記念イベント「デジタルクラフトカップ」のワークショップ申込者向けメールで、受託者が他の申込者の個人情報を閲覧できるURLを誤って送付し、56組62名分の氏名、メールアドレス、電話番号、年代、居住地（都道府県名）が対象となりました。事故発生は2023年8月10日、都への正式判明は8月17日で、全対象者への謝罪と再発防止の徹底が行われています。 令和6年（2024年） ③2024年6月14日 受託者における個人情報の漏えいについて。デジタルサービス局の高齢者向けスマホ体験会等の再委託先で、勤務調整フォームの権限設定ミスにより、75名分の氏名と60名分の最寄り駅が閲覧可能な状態になっていました。発生期間は2024年5月24日～6月12日で、都は対象者への説明・謝罪を行い、二次被害は報告されていないとしています。 ④2024年8月2日 個人情報の漏えいについて。都市整備局が区市町向けに配付した屋外広告物管理システム説明会資料に、許可申請者等の個人情報が含まれていました。対象は690名分の名字又は氏名を中心に、所属組織名・部署名・役職等（668名）、住所・電話番号の可能性がある情報（18名）、性別（3名）、社用メールアドレス（1名）です。判明は2024年7月9日、全区市町でデータ破棄と外部提供なしを7月12日までに確認し、二次被害は確認されていません。 令和7年（2025年） ⑤2025年6月2日 都立高等学校における個人情報の紛失について。都立高校のALTが、生徒課題プリントを無断で自宅に持ち帰った後、通勤途中で紛失し、77人分の氏名、学年、クラス、番号、英作文が記載された書類が所在不明になりました。都教育委員会は対象生徒・保護者へ説明と謝罪を行っています。 ⑥2025年6月13日 都立高等学校における個人情報の漏えいについて。都立高校で、就学支援金申請時に提出されたマイナンバーカードの写し1枚と健康保険証の写し1枚を、誤って別の生徒に配付しました。提出は2024年11月、誤配付は2025年4月8日、発覚は2025年6月10日です。教育庁は保護者への謝罪と、全校への再周知・研修実施を公表しています。 ⑦2025年6月27日 都立高等学校における個人情報の紛失について。都立高校教諭が生徒94人分の氏名、出欠状況、定期考査素点などが記載された教務手帳1冊を紛失しました。発見できず、学校と教育委員会が生徒・保護者へ説明と謝罪を実施しています。[metro.tokyo.lg.jp] ⑧2025年7月22日 都立高等学校における個人情報の紛失について。屋外プールでの補講中、突風で記録用紙が飛ばされ、生徒110人分の氏名、出席番号、性別、水泳に関する記録が記載された1枚が敷地外に飛散し、回収不能となりました。学校は生徒・保護者に説明と謝罪を行っています。[metro.tokyo.lg.jp] ⑨2025年8月7日 個人情報の漏えいについて。デジタルサービス局とGovTech東京の協働事業「東京デジタルアカデミー若手エンジニアコース」で、委託事業者の権限設定ミスにより、受講者561名分の氏名とメールアドレスが閲覧可能な状態になっていました。発生期間は2025年7月7日～8月6日19時45分頃で、現時点で二次被害は報告されていません。 ⑩2025年8月29日 個人情報の漏えいについて。デジタルサービス局が委託事業者A社に送る書類ひな形メールに、誤って別事業者B社の会社名、社員氏名、役職（1名分）を入力したファイルを添付しました。発生は2025年8月25日19時27分、印刷して判明したのが8月28日で、B社への謝罪とA社への削除依頼が実施されています。 ⑪2025年9月2日 個人情報の漏えいについて。同じく東京デジタルアカデミー若手エンジニアコースで、委託事業者が受講状況管理ツールの登録を誤り、受講者Aの氏名を別の受講者Bが閲覧できる状態になっていました。発生期間は2025年8月13日～9月1日8時45分頃で、GovTech東京から関係者へ謝罪が行われています。 2025年9月18日 都立高等学校における個人情報の紛失について。都立高校教諭が、36人分の氏名、出席番号、保護者氏名、選択科目希望、進路希望、大学名等が記載された生徒資料72枚入りクリアファイルを校内で紛失しました。生徒・保護者への説明と謝罪、再発防止策が公表されています。 ⑫2025年9月19日 東京都の委託事業における不正アクセス被害について。産業労働局の「TOKYO特定技能Jobマッチング支援事業」の委託事業者である株式会社パソナで、サポート詐欺起点の不正アクセスが発生し、800名分の氏名、生年月日、住所、電話番号、メールアドレス、出身国、在留資格、日本語能力レベル、合格試験分野、紹介先企業が漏えいした可能性があると公表されました。外部送信は確認できなかったが、画面閲覧等による漏えい可能性は否定できないとされ、個人情報保護委員会へ速報報告済みです。 ⑬2025年10月23日 個人情報の漏えいについて。デジタルサービス局が、A社に対し本来送るべきでないB社社員2名分の役職・氏名／苗字が含まれた契約書等を誤って郵送しました。発生は2025年10月20日、判明は10月23日で、誤送付書類の回収と謝罪が行われています。 ⑭令和8年（2026年）※6月8日現在 2026年3月6日 委託事業における不正アクセス被害について。水道局の調査研究委託先の協力会社がランサムウェア被害を受け、約13万件のお客さまの使用水量、お客さま番号、住所、使用者名等について、個人情報漏えいの可能性があると公表されました。現時点で情報流出は確認されていないとされています。 ⑮2026年3月9日 委託業務受託者へのサイバー攻撃について。デジタルサービス局が、同じ受託者によるサイバー攻撃被害について、5つの都委託事業への影響を追加公表しました。内容は、政策連携団体等204名の担当者情報、有識者2名の氏名等（うち1名は住所・電話番号・口座番号）、住民基本台帳から抽出した都内住民18,000件の住所・氏名・年齢・性別、参加企業156件の担当者情報等、有識者会議出席者8件・都道府県担当者メールアドレス47件などで、現時点で第三者への漏えいは確認されていないとされています。 ⑯2026年4月8日 個人情報等を含む関係書類の紛失について。住宅政策本部で、宅地建物取引業者から提出された一部書類が所在不明となり、55事業者分の文書の中に、法人代表者氏名、宅地建物取引士氏名・登録番号、従業者の氏名・生年月日・顔写真、733件の契約当事者の氏名・住所・電話番号・金額等が含まれていました。都は誤廃棄の可能性が高いが、外部持出しや外部漏えいは確認されていないと説明しています。 ⑰2026年5月25日 個人情報の漏えいについて。デジタルサービス局が管理する東京デジタルアカデミー（TDA）ポータルサイトで、アクセス制限の設定不備により、最大2,438人分の氏名、業務用メールアドレス、暗号化（ハッシュ化）されたパスワード（うち一般市民2人分を含む）が漏えいしました。発見後にアクセス不能化し、ログ確認の結果、過去に不正アクセスを受けCSVファイルがダウンロードされていたことを確認したと公表しています。

	再発防止策の内容	①点検・確認（総点検・再点検） 個人情報の取扱いについて再点検を実施 関連するデータやシステムについて全体的な点検・確認を行う（総点検 ②チェック体制の強化 作業時のダブルチェックの徹底 複数人による確認体制の構築 チェックリストや突合確認の導入 ③職員・委託先への教育・研修 個人情報保護に関する教育・指導の徹底 再発防止に関する研修の実施 注意喚起の継続実施 ④制度・手順の見直し 作業手順・運用ルールの見直し チェック項目や様式の見直し メール送信ルール（BCC利用等）の徹底 ⑤技術的対策・システム対策 アクセス制御・権限設定の強化 システム上の誤操作防止対策 セキュリティ対策の強化（設定・構造の見直し） ⑥ヒューマンエラー低減（仕組み化） 手作業を減らしデジタル化・自動化を推進 複数情報による照合（本人確認強化） 誤りの早期検知仕組みの導入 ⑦委託先管理の強化 委託事業者への指導・監督の強化 委託業務における個人情報管理の再徹底 委託先を含めた体制の見直し ⑧組織的安全管理措置の強化 管理体制・責任体制の整備 報告体制・内部連絡体制の整備 第三者評価・品質保証プロセスの見直し ⑨本人確認・照合の厳格化 氏名・住所・生年月日等の複数情報による照合の徹底 誤登録防止のための確認方法の見直し ⑩作業のデジタル化・自動化 手入力・手作業を減らすためのデジタル化推進 マイナンバー読み取り等の機械処理への転換 ⑪誤りの早期発見・検知体制の強化 異常検知機能の導入 ログ確認・監視体制の強化 誤りがあった場合の早期検出 ⑫報告・連絡体制の整備 漏えい発生時の庁内報告体制の整備 対応手順の明確化 人員体制の強化 ⑬ルール違反の防止（禁止事項の明確化） 私用メール利用の禁止 個人端末利用の制限 不適切運用の明確な禁止 ⑭ルール違反の防止（禁止事項の明確化） 私用メール利用の禁止 個人端末利用の制限 不適切運用の明確な禁止 ⑮継続的改善（PDCA） 定期的な見直し・改善の実施 事案を踏まえた継続的改善 ⑯透明性確保・対外説明の強化 事案の公表（速やかな情報開示） 対象者への丁寧な説明・謝罪 二次被害防止の注意喚起 国民・住民の不安払拭に向けた対応 ⑰全庁的・全体最適での管理強化（ガバナンス強化） 全庁横断での体制整備（本部設置等） 関係部署・関係機関との連携強化 ガイドライン策定・統一ルール化 データ管理・運用の標準化

⑩死者の個人番号		[保管している] ＜選択肢＞ 1）保管している 2）保管していない
	具体的な保管方法	生存者の返還データと同様に保管している。
その他の措置の内容		-
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク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		申請者に対し、愛の手帳に変更があった際には届け出ることを手帳の注意事項欄に記載し、交付の際にも説明をしている。
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 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	・一定期間を経過した申請書及び診断書は適宜、保管運搬・処分業者へ引き渡し保管する。なお、保存期間を経過した書類が発生した場合は仕様書及び「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）」等の関係法令に則った安全管理措置を講じ溶解処理等により廃棄する。 ・保存用以外の業務委託用の申請書は、身体障害者手帳発行後、担当職員がシュレッダーにて裁断している。 ・文書保管運搬・処分業者に引き渡し文書のうち、廃棄文書が発生した場合は、仕様書により安全管理措置の講じた区域内で破砕・溶解の処理を行う。 ・東京都クラウドに保存されているデータの削除については、構築するシステム上でデータ消去機能を付加する、又は別途委託の上、削除を検討する。
その他の措置の内容		―
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		
―		

Ⅳ　その他のリスク対策 ※

1. 監査

①自己点検	[　　十分に行っている　　]	＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
具体的なチェック方法	・個人情報保護については、全職員が職員向けの自己点検表を用いてチェックを実施。 ・情報セキュリティについては、システム管理者が点検表を用いてチェックを実施。 ・評価書の記載内容どおりの運用ができているか、年1回担当部署内でチェックを実施。 【中間サーバ・プラットフォーム】 ・運用規則等に基づき、中間サーバ・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。	
②監査	[　　十分に行っている　　]	＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
具体的な内容	・5年に一度のサイクルで情報セキュリティ、個人情報保護の体制に関して、外部監査人による監査を実施している。監査の結果を踏まえ、体制や規定を改善している。 ・「福祉局特定個人情報安全管理基準」、「東京都特定個人情報保護監査ガイドライン」の規定に則り、4年に一度のサイクルで実施している内部監査人による助言型監査について、令和2年度に実施した。監査の結果を踏まえ、体制や規定を改善している。 【中間サーバ・プラットフォーム】 ①運用規則等に基づき、中間サーバ・プラットフォームについて、定期的に監査を行うこととしている。 ②政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者は、定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。	

2. 従業者に対する教育・啓発

従業者に対する教育・啓発	[　　十分に行っている　　]	＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
具体的な方法	【職員（非常勤含む。）】 全職員を対象に情報セキュリティ・個人情報保護の研修を実施している。研修の目的は、個人情報保護の重要性及び適正管理等に関する理解を深め、個人情報保護の遵守を徹底することである。具体的には、以下の研修を実施している。 ・個人端末からアクセスするeラーニング研修（理解度が基準に達しないと修了できない） ・新規採用職員や他局転入職員等を対象とした研修 ・未受講者が出ないように端末のない職員に紙でeラーニング研修の実施を行い、結果の報告を受けることとしている。 【委託先】 ・業務開始に当たり、個人情報の取扱いルールを順守することを確認させている。 【中間サーバ・プラットフォーム】 IPA（情報処理推進機構）が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資材を作成し、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、運用規則（接続運用規程等）や情報セキュリティに関する教育を年次（年2回）及び随時（新規要員着任時）実施することとしている。	

3. その他のリスク対策

【中間サーバ・プラットフォーム】
中間サーバ・都クラウド・プラットフォームを活用することにより、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用、監視を実現する。

Ⅴ　開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	福祉局心身障害者福祉センター障害認定課 〒162－0823　東京都新宿区神楽河岸1－1セントラルプラザ14階 03－3235－2963
②請求方法	指定様式による書面の提出により開示・訂正・利用停止請求を受け付ける。
特記事項	請求方法、指定様式等について東京都公式ホームページ上で分かりやすく表示
③手数料等	[　　有料　　]　　＜選択肢＞ 1) 有料　　2) 無料 （手数料額、納付方法：納付書又は現金書留、現金持参により、実費相当分（10円/1枚）の手数料を支払う。）
④個人情報ファイル簿の公表	[　　行っている　　]　　＜選択肢＞ 1) 行っている　　2) 行っていない
個人情報ファイル名	愛の手帳交付ファイル
公表場所	福祉局心身障害者福祉センター障害認定課
⑤法令による特別の手続	―
⑥個人情報ファイル簿への不記載等	―

2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	福祉局心身障害者福祉センター障害認定課 〒162－0823　東京都新宿区神楽河岸1－1セントラルプラザ14階 03－3235－2963
②対応方法	問合せの受付時に受付表を起票し、対応について記録を残す。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	
②しきい値判断結果	[　　基礎項目評価及び全項目評価の実施が義務付けられる　　] ＜選択肢＞ 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 基礎項目評価及び重点項目評価の実施が義務付けられる（任意に全項目評価を実施） 3) 基礎項目評価の実施が義務付けられる（任意に全項目評価を実施） 4) 特定個人情報保護評価の実施が義務付けられない（任意に全項目評価を実施）
2. 国民・住民等からの意見の聴取	
①方法	
②実施日・期間	
③期間を短縮する特段の理由	
④主な意見の内容	
⑤評価書への反映	
3. 第三者点検	
①実施日	
②方法	
③結果	
4. 個人情報保護委員会の承認 【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

（別添3）変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和8年6月24日	Ⅱ・3・⑥使用目的	東京都に居住地を有する愛の手帳保有者の交付台帳の状況を記録、更新、管理するため。	・東京都に居住地を有する愛の手帳保有者の交付台帳の状況を記録、更新、管理するため。 ・愛の手帳が各種のマイナポータル連携サービスを利用し、利便性の向上を図るため。	事前	
令和8年6月24日	Ⅱ・4・委託事項1・⑥委託先名	株式会社　佐賀電産センター	SDCソリューションズ株式会社	事前	
令和8年6月24日	Ⅱ・4・委託事項3・①委託内容	愛の手帳の新規・更新・再交付の申請をする者の基本情報（氏名カナ、氏名漢字、住所、電話番号、生年月日、性別、個人番号及び本人が18歳以下の場合は保護者氏名、続柄、住所、個人番号）の入力及び障害者手帳作成・交換便等への封入作業の委託	AI-OCRを用いた愛の手帳の新規・更新・再交付の申請をする者の基本情報（氏名カナ、氏名漢字、住所、電話番号、生年月日、性別、個人番号及び本人が18歳以下の場合は保護者氏名、続柄、住所、個人番号）の入力及び障害者手帳作成・交換便等への封入作業の委託	事前	
令和8年6月24日	Ⅱ・4・委託事項3・⑥委託先名	シミックソリューションズ株式会社	マンパワーグループ株式会社	事前	
令和8年6月24日	Ⅱ・4・委託事項4・⑥委託先名	株式会社　佐賀電産センター	SDCソリューションズ株式会社	事前	
令和8年6月24日	Ⅱ・6・①保管場所	【手帳システム】 メインサーバは執務室内において、バックアップサーバは異なる場所のサーバ室において、ラックにて施錠保管している。メインサーバでは、ラックの解施錠は管理簿に記入し、情報システム管理者の許可を得ることが必要になっている。バックアップサーバでは、原則として情報システム管理者及び情報システム担当者のみサーバ室への入室が可能となっており、入室の際は入退室管理簿に記入をし、内部承認を得ることが必要となっている。UPSがあることにより、停電時等にシャットダウンまでの時間の対応が可能である。	【手帳システム】 CSPが提供するクラウドサービスに東京都クラウドインフラとして必要と考えられる統制機能やセキュリティ設定を適用した「クラウドインフラサービス」基盤上に構築される。 採用するCSPは、AWSとなり、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスとなる。 このため、特定個人情報の適正な取扱いに関するガイドラインで求める物理的対策を満たしており、主に以下の物理的対策を講じている。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・許可されたアカウント以外は特定個人情報にアクセスできないように制御している。 ・日本国内にデータセンターが存在するクラウドサービスを利用している。 ・特定個人情報は、CSPが管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターに保存される。 ・サーバのウイルスパターンファイル、セキュリティパッチ等の適用タイミングについて、原則最新のものが公表された都度とするが、詳細についてはシステム保守業者との調整によることとする。 ・手帳システムバックアップの保存領域は、AWS Backupを利用して別リージョンに保管する想定。	事前	

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8年6月24日	Ⅱ・6・③消去方法	【手帳システム】 ・本システム端末のデータ消去を委託する際には、職員等が立ち会い削除するか、委託先からの書面による確証を得たうえでデータが消去されていることを確認する。 ・手帳システムサーバで使用する機器の借入期間終了時においては、物理的破壊又はデータ消去の場合は米国国防総省規定に準拠した方式による3回上書き相当以上の方法で処理し、作業完了後、書面にて報告を受ける。	【手帳システム】 ・保存用以外の業務委託用の申請書は、身体障害者手帳発行後、担当職員がシュレッダーにて裁断している。 ・文書保管運搬・処分業者に引き渡し文書のうち、廃棄文書が発生した場合は、仕様書により安全管理措置の講じた区域内で破砕・溶解の処理を行う。 ・本システム端末のデータ消去を委託する際には、職員等が立ち会い削除するか、委託先からの書面による確証を得たうえでデータが消去されていることを確認する。 ・東京都クラウドに保存されているデータの削除については、構築するシステム上でデータ消去機能を付加する、又は別途委託の上、削除を検討する。	事前	
令和8年6月24日	Ⅲ・3・リスク3・リスクに対する措置の内容	・サーバは夜間バッチにより深夜12時から翌朝7時まで利用できない。	・サーバは夜間バッチにより深夜12時から翌朝5時まで利用できない。	事前	
令和8年6月24日	Ⅲ・4・特定個人情報の提供ルール・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尊寿確認方法	【委託事項1】【委託事項2】【委託事項3】【委託事項4】 ・業務上、委託先から他社への提供はない。 ・委託先と取り交わしている「電子情報処理委託に係る標準特記仕様書」において、目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理に対する義務違反時の損害賠償の請求等について規定している。	【委託事項1】【委託事項2】【委託事項3】【委託事項4】 ・業務上、委託先から他社への提供はない。 ・再委託の取扱いについては、仕様書上、原則第三者に再委託を禁止することとしている。 ・委託先と取り交わしている「電子情報処理委託に係る標準特記仕様書」において、目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理に対する義務違反時の損害賠償の請求等について規定している。	事前	
令和8年6月24日	Ⅲ・6・リスク5・リスクに対する措置の内容	【手帳システム】 ・副本登録するファイルは都の指定があった方法にて暗号化する。	【手帳システム】 ・副本登録するファイルは暗号化する。	事前	
令和8年6月24日	Ⅲ・6・リスク6・リスクに対する措置の内容	【手帳システム】 ・副本登録するファイルは都の指定があった方法にて暗号化する。	【手帳システム】 ・副本登録するファイルは暗号化する。	事前	

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8年6月24日	Ⅲ・6・リスク7・リスクに対する措置の内容	【中間サーバ・ソフトウェア】 ①情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。②情報提供データベース管理機能（※）により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。③情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。（※）特定個人情報を副本として保存・管理する機能。 【連携サーバ】 ・各事務所管部署で本人確認及び真正性確認を行った個人番号に基づき、団体内統合利用番号及び個別業務システム利用番号が紐付けられていることを前提として、当該人に対する情報提供が可能となるよう制御されている。 ・個別業務システム（事務）と中間サーバとの間における特定個人情報の授受に当たっては、その中継のみを行い、システム内に特定個人情報（副本相当）は保有しない。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・中間サーバとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。 ・サーバ認証により真正性が担保された中間サーバに接続する。 【手帳システム】 ・副本登録は、内部承認のうえで手帳システムの台帳情報に異動があった都度行う。 ・副本の正確性確保のため、正本は手帳交付前に職員による相互チェックを行い正確性を確保している。 ・中間サーバでのエラー発生時は、職員により手帳システムと連携サーバの情報を確認し、正確な情報をチェックするエラーフォローを行う。	＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。 ②情報提供データベース管理機能（※）により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ③情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 （※）特定個人情報を副本として保存・管理する機能。 庁内連携【連携サーバ】 ・照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められ、かつ移転者が明示的に回答を承認した場合に限り、連携を行う。照会に対しては、照会条件として指定された対象者に関する情報だけを回答する。なお、チェック項目は、番号法等の改正に応じて、更新する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・情報照会に対する回答は、当該照会を行った事務に対してのみ返却するよう制御されている。 ・各事務所管部署が個々の照会データを一意に識別できるよう付与した識別子を、連携サーバからの回答データに付記して返却することで、どの照会に対する回答かを各事務所管部署で正確に突合できるようにしている。 【手帳システム】 ・副本登録は、内部承認のうえで手帳システムの台帳情報に異動があった都度行う。 ・副本の正確性確保のため、正本は手帳交付前に職員による相互チェックを行い正確性を確保している。 ・中間サーバでのエラー発生時は、職員により手帳システムと連携サーバの情報を確認し、正確な情報をチェックするエラーフォローを行う。	事前	
令和8年6月24日	Ⅲ・7・リスク1・⑤・具体的な対策の内容	【手帳システム】 ・サーバ設置場所、端末設置場所を施錠管理している。（バックアップサーバも含む） ・データのバックアップは、世代管理している。 ・本システム端末のデータ消去を委託する際には、職員等が立ち会い削除するか、委託先からの書面による確証を得たうえでデータが消去されていることを確認する。 ・手帳システムサーバで使用する機器の借入期間終了時においては、物理的破壊又はデータ消去の場合は米国国防総省規定に準拠した方式による3回上書き相当以上の方法で処理し、作業完了後、書面にて報告を受ける	【手帳システム】 ・サーバは東京都クラウドにてデータセンターで管理している。（バックアップサーバも含む） ※データセンターの場所等は通信回線事業者との回線契約以後の秘密保持契約以後による。 ・データのバックアップは、世代管理する。 ・①契約の終了等に伴い、東京都が借り受けている端末、サーバ、その他電磁的記録媒体などの情報処理機器類を返却する際には、情報を復元できないように処理しなければならない。機器の撤去後にデータ消去を行う場合は、データ消去までの期間におけるサイバーセキュリティ対策を明確に定めること。 ・②　上記①の消去作業を事業者に委託する場合、あらかじめ、契約仕様書にその旨を明記するとともに、データ消去完了証明書を徴取すること。また、必要に応じて、消去作業に職員等を立ち合わせること。	事前	

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8年6月24日	Ⅲ・7・リスク1・⑥・具体的な対策の内容	【手帳システム】 ・外部記録媒体に記録するデータ及びパスワードファイルは都の指定があった方法にて暗号化し、使用完了後は速やかに削除する。	【手帳システム】 ・外部記録媒体に記録するデータ及びパスワードファイルは暗号化し、使用完了後は速やかに削除する。	事前	
令和8年6月23日	Ⅲ・7・リスク1・⑨・その内容		時点更新	事前	
令和8年6月24日	Ⅲ・7・リスク1・⑩・具体的な保管方法	生存者のデータと同様に保管している。	生存者の返還データと同様に保管している。	事前	
令和8年6月24日	Ⅲ・7・リスク3・手順の内容	・一定期間を経過した申請書及び判定書は適宜、保管運搬・処分業者へ引き渡し保管する。なお、保存期間を経過した書類が発生した場合は仕様書及び「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）」等の関係法令に則った安全管理措置を講じ溶解処理等により廃棄する。 ・外部記録媒体に記録されたデータは使用完了後に速やかに消去している。	・一定期間を経過した申請書及び診断書は適宜、保管運搬・処分業者へ引き渡し保管する。なお、保存期間を経過した書類が発生した場合は仕様書及び「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）」等の関係法令に則った安全管理措置を講じ溶解処理等により廃棄する。 ・保存用以外の業務委託用の申請書は、身体障害者手帳発行後、担当職員がシュレッダーにて裁断している。 ・文書保管運搬・処分業者に引き渡し文書のうち、廃棄文書が発生した場合は、仕様書により安全管理措置の講じた区域内で破砕・溶解の処理を行う。 ・東京都クラウドに保存されているデータの削除については、構築するシステム上でデータ消去機能を付加する、又は別途委託の上、削除を検討する。	事前	

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8年6月24日	Ⅳ・③・その他のリスク対策	【中間サーバー・プラットフォームにおける措置】 ①中間サーバー・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用、監視を実現する。 【連携サーバ】 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で稼働する。 ・サーバが接続されたセグメントとそれ以外のセグメントの境界にファイアウォールを導入するとともに、ログを取得する。 ・ウイルス対策ソフトを導入し、パターンファイルを更新する。 ・基本ソフトウェア(OS)及びミドルウェアは、必要に応じてセキュリティパッチを適用する。 ・データベースにデータを暗号化して保存する。 ・データベースに対する操作権限を細分化し、連携サーバ管理者であっても真に必要な場合を除いてはデータにアクセスできないよう制御する。 ・データベースに対するアクセスログを取得する。 ・データベースのバックアップを取得する。 ・あらかじめ登録された機器だけがネットワークに接続できるよう制御する。 ・サーバ及びその管理に用いる機器は、書き出し可能な外部記録媒体を内蔵せず、かつUSB機器等に対する制御を行い、外部記録媒体の利用を制限する。 【手帳システム】 ・システムの操作履歴（アクセスログ）を記録する。 ・ウイルス対策ソフトの定期的パターン更新を行うことにより、ウイルス感染を防止している。 ・システムを使用する各端末では庁内ネットワークを経由して、自動的にUSB出力ポートが無効となるように制御設定されている。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で稼働する。 ・サーバが接続されたセグメントと他のセグメント間の通信は制限されている。 ・番号系端末でウイルスを検知した場合、番号系端末が配備されたすべての局の情報化推進担当宛てに、システム管理者から自動でメール通知する。 ・システムで利用する端末、外部記録媒体はドライブ暗号化を使用する。 ・外部記録媒体に記録するデータ及びパスワードファイルは暗号化し、使用完了後は速やかに削除する。 ・廃棄時には内部のデータを復元できないように消去した上で廃棄する。 ・特定個人情報の適切な取扱いについて継続的な改善を実施するための仕組みとして、既に入力されているマイナンバーを入力すると、エラーメッセージが表示されるように常にアップデートするようにしている。 【組織体制】 ・評価対象の事務における事務責任者等の関与の仕組みとして、定期的に管理者が評価対象の事務をチェックしている。 ・特定個人情報保護評価を適切に実施するために整備している体制として、身体担当と協力体制を整え、関係部署と情報交換を実施している。 ・特定個人情報の漏えい事案等が発生した場合の対応として、速やかに上司に報告し、担当だけでなく関係部署からの聞き取りを行う、当人への連絡・謝罪等、定められた業務を遂行する。	【中間サーバ・プラットフォーム】 中間サーバ・都クラウド・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）やシステム業者による安定運用を目的とした保守委託によるサポートを取り入れる。	事前	
令和8年7月23日	Ⅱ・4・委託事項2・④委託先への特定個人情報ファイルの提供方法	【〇】電子記録媒体（フラッシュメモリ除く）	【　】電子記録媒体（フラッシュメモリ除く）	事前	
令和8年7月23日	Ⅱ・4・委託事項4・②「対象となる本人の範囲※」	愛の手帳に係る申請を行った者	身体障害者手帳保有者及び愛の手帳保有者	事前	
令和8年7月23日	Ⅱ・4・委託事項4・②「その妥当性」	愛の手帳に係る申請を行った者の情報を効率的に台帳登録し、円滑に障害者手帳を交付するため。	他県において制度側で管理する制度固有の番号とマイナンバーの間に紐付け誤りが発生したことを受け、個人情報保護の観点からも、紐付けが正確に行われているか、総点検を実施したため。	事前	

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8年7月23日	（別添2）ファイル記録項目	身体障害者手帳交付台帳ファイル	愛の手帳交付台帳ファイル	事前	
令和8年7月23日	Ⅴ・1・③手数料等	（手数料額、納付方法：　　）	（手数料額、納付方法：納付書又は現金書留、現金持参により、実費相当分（10円/1枚）の手数料を支払う。　　）	事前	
令和8年7月23日	Ⅲ・3・リスク2・ユーザ認証の管理・具体的な管理方法	パスワードは有効期間を指定できる。	パスワードは有効期間を1年としている。	事前	
令和8年9月17日	Ⅱ・6・①保管場所	【中間サーバ・プラットフォーム】 ①中間サーバ・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバ室への入室を行う際には、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。②特定個人情報は、サーバ室に設置された中間サーバのデータベース内に保存され、バックアップもデータベース上に保存される。	【中間サーバ・プラットフォーム】 ①中間サーバ・プラットフォームは政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。・ISO/IEC27017、ISO/IEC27018 の認証を受けている。・日本国内でデータを保管している。②特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する中間サーバのデータベース内に保存され、バックアップもデータベース上に保存される。	事前	
令和8年9月17日	Ⅱ・6・③消去方法	【中間サーバ・プラットフォーム】 ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの事業者が特定個人情報を消去することはない。 ②ディスク交換やハード更改等の際は、中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、物理的破壊により完全に消去する。	【中間サーバ・プラットフォーム】 ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度（ISMAP）に準拠したデータの暗号化消去及び物理的破壊を行う。さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ③中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。	事前	
令和8年9月17日	Ⅲ・6・リスク6・リスクに対する措置の内容	【中間サーバ・プラットフォーム】 ③中間サーバ・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。	【中間サーバ・プラットフォーム】 ③中間サーバ・プラットフォームの保守・運用を行う事業者及びクラウドサービス事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。	事前	

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8年9月17日	Ⅲ・6・リスク7・情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	【中間サーバ・プラットフォーム】 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する	【中間サーバ・プラットフォーム】 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバ・プラットフォームの保守・運用を行う事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。	事前	
令和8年9月17日	Ⅲ・7・リスク1・⑤・具体的な対策の内容	【中間サーバ・プラットフォーム】 ①中間サーバ・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 ②事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	【中間サーバ・プラットフォーム】 ①中間サーバ・プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。・ISO/IEC27017、ISO/IEC27018 の認証を受けている。・日本国内でデータを保管している。	事前	
令和8年9月17日	Ⅲ・7・リスク1・⑥・具体的な対策の内容	【中間サーバ・プラットフォーム】 ①中間サーバ・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。②中間サーバ・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。	【中間サーバ・プラットフォーム】 ④中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤中間サーバーのデータベースに保存される特定個人情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ⑥中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ⑦中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。	事前	
令和8年9月17日	Ⅳ1・②具体的な内容	【中間サーバ・プラットフォーム】 ・運用規則等に基づき、中間サーバ・プラットフォームについて、定期的に監査を行うこととしている。 【東京都クラウドインフラ】 東京都クラウドインフラについては、デジタルサービス局の定める監査要綱（2年に1回の内部監査、5年に1回の外部監査）に従って計画しております	【中間サーバ・プラットフォーム】 ①運用規則等に基づき、中間サーバ・プラットフォームについて、定期的に監査を行うこととしている。 ②政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者は、定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。	事前	
令和8年9月17日	Ⅳ3．その他のリスク対策	【中間サーバ・プラットフォーム】 中間サーバ・都クラウド・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）やシステム業者による安定運用を目的とした保守委託によるサポートを取り入れる。	【中間サーバ・プラットフォーム】 中間サーバ・都クラウド・プラットフォームを活用することにより、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者による高レベルのセキュリティ管理（入退室管理等）やシステム業者による安定運用を目的とした保守委託によるサポートを取り入れる。	事前	