

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
2	地方税に関する事務

個人のプライバシー等の権利利益の保護の宣言	
台東区は、地方税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あたり、特定個人情報ファイルの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	なし

評価実施機関名
東京都台東区長

個人情報保護委員会 承認日【行政機関等のみ】
公表日
令和7年10月8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	地方税に関する事務
②事務の内容 ※	台東区における地方税に関する賦課、徴収等の事務の内容は、以下のとおり。 1. 特別区民税、都民税賦課関連事務 地方税法に基づき、その年の1月1日において区内に住所のある者、または区内に住所はないが区内に事務所・事業所・家屋敷がある者について、前年の所得に対して賦課を行う地方税（以下「特別区民税・都民税」という。）に関する以下の事務である。 ○課税資料の入手 確定申告書、給与支払報告書、公的年金支払報告書、特別区民税・都民税申告書等の課税資料を区役所窓口申告、郵送、電子申告等で入手する。 ○課税資料の入力 入手した課税資料を基に収入、所得情報、控除情報等を税務システムに登録する。 ○課税資料の名寄せ 課税資料に記載された個人番号を基に、住民基本台帳と照合、または住民基本台帳ネットワークに照会し本人特定を実施、複数資料の名寄せを行う。 ○課税資料の回送及び調査、他機関への提供 本区に課税する根拠がないと判断された場合は課税すべき自治体へ課税資料の回送を行う。 本区にて住民登録外課税を行う場合は地方税法第294条第3項の規定により住民登録自治体へ通知する。 また、本区外に住所を有する被扶養者等についても所得情報等の照会及び回答を行う。 ○税額の通知 課税資料の入力を行った内容に基づく税額等の情報を納税義務者へ通知する。 ○減免の審査・処理 生活保護受給や災害による減免申請の受付、審査、審査結果反映、反映後の税額等情報の通知を行う。 ○特別区民税・都民税情報の提供・移転 行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「番号法」という。）並びに番号法第9条第2項及び第19条第11号に基づき制定した東京都台東区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施行条例（以下「台東区番号条例」という。）に基づき、特別区民税・都民税等情報の提供・移転を行う。 ○各種証明書（課税・非課税・納税）等の発行 本人もしくは代理人（要委任状）の申請に基づき証明書の発行を行う。 2. 軽自動車税賦課関連事務 地方税法に基づき4月1日現在、軽自動車等の所有者に課税を行う。 ○登録、名義変更 ・台東区ナンバー：住民等から軽自動車税申告（報告）書兼標識交付申請書の提出を受け、税務システムに入力し、標識（ナンバープレート）、標識交付証明書を交付する。他自治体からの転入、譲受の場合は旧の自治体に課税物件異動通知書を送付する。 ・足立ナンバー：住民等から全国軽自動車協会連合会を通じて、軽自動車税申告書（報告書）の提出を受け、税務システムに入力する。 ○廃車 ・台東区ナンバー：住民等から軽自動車税廃車申告書兼標識返納書、標識（ナンバープレート）の提出を受け、税務システムに入力し、廃車申告受付書を交付する。 ・足立ナンバー：住民等から全国軽自動車協会連合会を通じて、軽自動車税申告書（報告書）、転出車両情報リストの提出を受け、税務システムに入力する。 ○軽自動車税の賦課決定、通知 賦課決定した課税データを印刷・印字業者へ提供し、通知書の作成を委託する。納税義務者に対し納税通知書を送付する。 ○軽自動車税の減免 住民等から減免申請書の提出を受け、税務システムに入力し、減免可否決定通知書を送付する。 3. 収納関連事務 ○収納管理 地方税法に基づき賦課・更正された特別区民税・都民税及び軽自動車税の収納情報を管理する。 ・賦課情報の入手 特別区民税・都民税及び軽自動車税の賦課・更正情報を各システムから入手する。 ・収納（納付（納入）済通知書）情報の登録 指定金融機関が取りまとめた住民等が納付、納入した情報を、指定金融機関へデータ化を委託し、データ化したファイルを収納管理システムに一括登録する。 コンビニエンスストアにおいて、バーコードを利用した納付、納付した情報を、通信事業者へデータ化を委託し、データ化したファイルを収納管理システムに一括登録する。 eLTAX地方税共通納税システムを利用した納付、納入した情報を、地方税共同機構よりデータ化したファイルを取得し、収納管理システムに一括登録する。

	○口座振替情報登録 住民から申請された口座振替に関する情報の登録・変更・取消情報を管理する。 ○過誤納金 過納付もしくは誤納付が生じた場合、還付・充当通知書を印刷し、住民等に通知する。 住民等から取得した還付請求書の情報を税務システムに登録し、指定された口座に振り込みを行う。 マイナポータル(デジタル庁)に登録されている公金受取用口座を、個人番号を用いて参照し税務システムに登録、その後該当口座に振り込みを行う。 ○督促 地方税法に基づき、納期限までに完納しなかった対象者を抽出し、督促状を印刷する。 印刷した督促状を封入封緘委託事業者に提供し、封入封緘等を行い、住民等に督促状を送付する。 4. 滞納整理関連事務 地方税法、国税徴収法に基づき、特別区民税・都民税、軽自動車税を滞納している個人及び法人(以下「滞納者」という。)に対し、納税交渉、催告、調査、滞納処分等の滞納整理を行う。 ○宛名・賦課・収納管理情報の入手 庁内連携システムから連携した特別区民税・都民税及び軽自動車税の賦課・収納・還付情報等を滞納管理システムから入手する。 ○催告 滞納者の未納額等の情報を抽出し、催告書を印字、発送する。また、電話による催告を行う。 ○納税相談 滞納者と納税相談を行い、分割納付や納税猶予を行う。 ○各種調査 地方税法、国税徴収法に基づき、滞納者について官公署や金融機関等へ財産調査を行う。 ○滞納処分 地方税法、国税徴収法に基づき、滞納者について差押・交付要求等を行い、換価・充当する。 また、滞納処分の執行停止処理と、不納欠損処理を行う。 滞納処分情報は滞納管理システムに登録し管理する。		
③対象人数	[30万人以上]	<選択肢> 1) 1,000人未満 2) 1,000人以上1万人未満 3) 1万人以上10万人未満 4) 10万人以上30万人未満 5) 30万人以上	

2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	特別区民税・都民税課税支援システム
②システムの機能	① eLTAXデータ対応機能 国税連携データ(e-Taxデータ、KSKデータ)の取込処理に対応している。 また、KSKデータのOCR処理や給与支払報告データ、年金支払報告データ等の取込処理に対応している。 ② 疑似イメージ自動生成機能 課税資料データ取込時、システムが疑似イメージを一括生成する。 ③ 各種システム内バッチ処理機能 課税資料の名寄せ処理、データの検算処理、課税資料の合算処理、扶養親族の特定処理等の機能が備わっている。
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（申請管理システム）
システム2	
①システムの名称	団体内統合宛名システム
②システムの機能	①団体内統合宛名番号採番機能:業務システムからの要求に応じて団体内統合宛名番号を採番し、業務システム及び中間サーバーに返却する。 ②番号管理情報更新機能:住民情報、住登外情報が更新された際に、団体内統合宛名番号、個人番号、宛名番号(各業務システム)にひも付く情報を更新する。 ③中間サーバー連携機能:中間サーバー、または中間サーバー接続端末からの要求に応じて、団体内統合宛名番号にひも付く宛名情報を返却する。 ④団体内統合宛名番号の変更機能(名寄せ機能):個人番号が同一で複数の団体内統合宛名番号が付番されていた場合の団体内統合宛名番号の変更を行う。 ⑤住民情報参照、住登外情報登録・参照機能:住民情報、住登外情報の参照及び住登外情報の登録を行う。
③他のシステムとの接続	☐ 情報提供ネットワークシステム ☒ 庁内連携システム ☐ 住民基本台帳ネットワークシステム ☒ 既存住民基本台帳システム ☐ 宛名システム等 ☐ 税務システム ☒ その他（中間サーバー）
システム3	
①システムの名称	庁内連携システム
②システムの機能	【情報連携機能】 ①庁内連携機能:住民情報、住登外情報、特定個人情報について業務システムとの連携を行う。 ②中間サーバー連携機能(副本登録):各システムで抽出した特定個人情報を、中間サーバーに連携する。 【情報照会機能】 ①情報照会機能:業務システムから「他団体への情報照会依頼」を受信する。また、中間サーバーから受信した「他団体からの情報提供内容」を、業務システムに連携する。 ②中間サーバー連携機能(情報照会):業務システムから受信した「他団体への情報照会依頼」を、中間サーバーに連携する。また、中間サーバーから「他団体からの情報提供内容」を取得する。 【特定個人情報登録機能】
③他のシステムとの接続	☐ 情報提供ネットワークシステム ☐ 庁内連携システム ☐ 住民基本台帳ネットワークシステム ☒ 既存住民基本台帳システム ☒ 宛名システム等 ☒ 税務システム ☒ その他（中間サーバー、国民健康保険、国民年金、介護保険、後期高齢、学務、保健、住宅、高齢、障害、滞納管理、児童保育、児童手当、児童扶養手当、生活保護、児童相談支援、災害時避難行動要支援者の各システム）

システム4	
①システムの名称	中間サーバー
②システムの機能	①符号管理機能 情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」とを紐付け、その情報を保管・管理する。 ②情報照会機能 情報提供ネットワークシステムを介して、特定個人情報(連携対象)の情報照会及び情報提供受領(照会した情報の受領)を行う。 ③情報提供機能 情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報(連携対象)の提供を行う。 ④既存システム接続機能 中間サーバーと既存システム、団体内統合宛名システム及び住基システムとの間で情報照会内容、情報提供内容、特定個人情報(連携対象)、符号取得のための情報等について連携する。 ⑤情報提供等記録管理機能 特定個人情報(連携対象)の照会、又は提供があった旨の情報提供等記録を生成し、管理する。必要に応じて保管されたアクセス記録を検索、抽出、出力、不開示設定や過誤事由の更新を行い、保管期間の過ぎたアクセス記録を削除する。 ⑥情報提供データベース管理機能 特定個人情報(連携対象)を副本として、保持・管理する。 ⑦データ送受信機能 中間サーバーと情報提供ネットワークシステム(インターフェイスシステム)との間で情報照会内容、情報提供内容、符号取得のための情報等について連携する。 ⑧セキュリティ管理機能 特定個人情報(連携対象)の暗号化及び復号や、電文への署名付与、電文及び提供許可証に付与されている署名の検証、それらに伴う鍵管理を行う。また、情報提供ネットワークシステム(インターフェイスシステム)から受信した情報提供NWS 配信マスター情報を管理する。 ⑨職員認証・権限管理機能 中間サーバーを利用する職員を認証し、操作者を一意に特定する。職員に付与された権限に基づき、システム機能や特定個人情報へのアクセス制御を行う。 ⑩システム管理機能 中間サーバー・ソフトウェアで提供するバッチの状況管理、業務統計情報の集計、中間サーバー・ソフトウェアの移動状態の通知、保管期限切れ情報の削除を行う。
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 ☐ 住民基本台帳ネットワークシステム ☐ 宛名システム等 ☐ その他 (☐ 庁内連携システム ☐ 既存住民基本台帳システム ☐ 税務システム)

システム5

①システムの名称	eLTAX審査システム
②システムの機能	地方税における電子申告、電子申請・届出に係るデータの管理、検索、帳票表示、印刷、ダウンロード等を行うシステム。 ○データダウンロード機能 特別徴収義務者や公的年金等支払者等がeLTAXを使用して提出した給与支払報告書や公的年金等支払報告書等のデータをダウンロードする。 ○特別徴収税額通知データ送信機能 eLTAXを使用して給与支払報告書を提出した特別徴収義務者に対して、特別徴収に係る税額通知データを送信する。 ○申告データ審査・照会機能 特別徴収義務者や公的年金等支払者等がeLTAXを使用して提出した給与支払報告データや公的年金等支払報告データ等の審査、照会を行う。 ○申請・届出データ審査・照会機能 eLTAXを使用して提出された申請・届出データ等の審査、照会を行う。
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 [] 住民基本台帳ネットワークシステム [] 宛名システム等 [] その他 （ [] 庁内連携システム [] 既存住民基本台帳システム [] 税務システム)

システム6

①システムの名称	国税連携システム(eLTAX)
②システムの機能	所得税確定申告書等に係るデータ(国税連携データ)の管理、検索、帳票表示、印刷、ダウンロード、団体間回送等を行うシステム。 ○確定申告データ(e-TAXデータ、KSKデータ)のダウンロード機能 インターネットを使用して電子送信した確定申告データ(e-TAXデータ)や書面で提出した確定申告書のデータ(KSKデータ)をダウンロードする。 ○確定申告書イメージデータのダウンロード機能 書面で提出された確定申告書のイメージデータ(TIFFファイル)をダウンロードする。 ○確定申告データの検索、印刷、XMLファイルのCSV変換機能 確定申告データを検索、印刷等する。 ○団体間回送機能 課税資料のイメージデータを他の地方公共団体に送信する。また、扶養是正情報データを国税庁連絡サーバへ送信する。
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 ☐ 住民基本台帳ネットワークシステム ☐ 宛名システム等 ☐ その他 () ☐ 庁内連携システム ☐ 既存住民基本台帳システム ☐ 税務システム

システム7

①システムの名称	特徴税通システム
②システムの機能	個人住民税の給与所得に係る特別徴収税額通知(納税義務者)について、電子データを作成しeLTAXに連携させ、当該通知の内容を電磁的方法により提供を行うシステム。 ○通知書作成システム 特別徴収税額通知(納税義務者用)の電子データを地方団体が本システムを利用して作成する。 ○eLTAX特徴税通パスワード確認機能 特別徴収税額通知(納税義務者用)の暗号化を納税義務者が解除するためのパスワードを提供する。 ○eLTAX特徴税通記載事項確認機能 特別徴収税額通知(納税義務者用)の記載内容の真正性を納税義務者が確認する。
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 [] 住民基本台帳ネットワークシステム [] 宛名システム等 [] その他 () [] 庁内連携システム [] 既存住民基本台帳システム [] 税務システム

システム8

①システムの名称	税務システム
②システムの機能	地方税法に基づく特別区民税・都民税及び軽自動車税の賦課徴収等を管理するシステム。 ・特別区民税・都民税賦課機能：当初賦課の課税準備処理から当初賦課、納付書や納税通知書の帳票発行、異動更正、証明書発行を行う。 ・軽自動車税賦課機能：車両の登録、納税義務者に対する賦課、登録情報の管理、各種証明書の発行を行う。 ・収納機能：上記で賦課した税額に基づく地方税の収納管理、納付書の発行、証明書発行、還付・充当を行う。
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 （ 特別区民税・都民税課税支援システム、滞納管理システム ）

システム9

①システムの名称	軽自動車検査情報市区町村提供システム
②システムの機能	軽自動車税の経年車重課及びグリーン化特例(軽課)の税率判定に必要となる、初度検査年月、燃費性能や燃料の種類等の軽自動車検査情報を市区町村が入手するためのシステム。 地方公共団体情報システム機構は、一般社団法人全国軽自動車協会連合会から軽自動車検査情報を取得後、重課及び軽課の判定情報を付加し、市区町村に提供を行う。市区町村はJ-LISポータルサイトにアクセスして検査情報を取得する。
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 [] 市内連携システム [] 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13	
①システムの名称	申請管理システム
②システムの機能	○申請データ格納 マイナポータル申請管理でダウンロードしたデータを復号する機能 ○申請内容照会と審査状況管理 申請内容の確認や審査を行うため、申請データの参照や添付書類等の確認、申請データごとに審査状況のステータス管理を行う機能
③他のシステムとの接続	[] 情報提供ネットワークシステム [] 庁内連携システム [] 住民基本台帳ネットワークシステム [] 既存住民基本台帳システム [] 宛名システム等 [] 税務システム [○] その他 （ 特別区民税・都民税課税支援システム、サービス検索・電子申請機能 ）

3. 特定個人情報ファイル名	
(1) 特別区民税・都民税賦課情報ファイル (2) 軽自動車税賦課情報ファイル (3) 収納情報ファイル (4) 滞納整理情報ファイル	
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	台東区では、下記の4ファイルについて記載の目的、理由から取り扱う。 1. 特別区民税・都民税賦課情報ファイル ・申告者(課税対象者)の本人確認及び申告書等の課税資料の名寄せ ・賦課決定に係る情報の正確な把握 2. 軽自動車税賦課情報ファイル ・申告者(課税対象者)の本人確認 ・賦課決定に係る情報の正確な把握 3. 収納情報ファイル ・地方税の徴収、還付充当処理を正確に行う。 4. 滞納整理情報ファイル ・滞納処分、猶予、執行停止を行うため、正確な情報を把握する。
②実現が期待されるメリット	・正確な賦課徴収による公正、公平化が図られる。 ・二重課税の防止など正確性の向上が図られる。
5. 個人番号の利用 ※	
法令上の根拠	番号法第9条第1項(別表24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	【情報提供の根拠】 ・番号法第19条第8号及び行政手続における特定の個人を識別するための番号の利用等に関する法律第十九条第八号に基づく利用特定個人情報の提供に関する命令(以下「命令」という。)第2条の表 項番 1,2,3,4,5,7,11,13,15,20,28,37,39,42,48,49,53,57,58,59,63,65,66,69,73,75,76,81,83,84,86,87,88,89,90,91,92,96,98,106,108,115,124,125,129,130,132,137,138,140,141,142,144,147,151,152,155,156,158,160,161,163,164,165,166,167,168,169,170,171,172,173 【情報照会の根拠】 ・番号法第19条第8号及び命令第2条の表48の項 ・命令第50条
7. 評価実施機関における担当部署	
①部署	税務課、収納課
②所属長の役職名	税務課長、収納課長
8. 他の評価実施機関	
—	

(別添1) 事務の内容

別添1のとおり

(備考)

Ⅱ 特定個人情報ファイルの概要

1. 特定個人情報ファイル名

(1) 特別区民税・都民税賦課情報ファイル

2. 基本情報

①ファイルの種類 ※	[システム用ファイル]	<選択肢> 1) システム用ファイル 2) その他の電子ファイル(表計算ファイル等)
②対象となる本人の数	[10万人以上100万人未満]	<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
③対象となる本人の範囲 ※	地方税法その他地方税に関する法律及び東京都台東区特別区税条例の規定により、税務関係書類に個人番号を記載することとされる者(納税義務者及び被扶養者、その他調査対象者)	
	その必要性	住民税の適正な賦課徴収を行うため。
④記録される項目	[100項目以上]	<選択肢> 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
主な記録項目 ※	・識別情報 [○] 個人番号 [] 個人番号対応符号 [○] その他識別情報(内部番号) ・連絡先等情報 [○] 5情報(氏名、氏名の振仮名、性別、生年月日、住所) [○] 連絡先(電話番号等) [○] その他住民票関係情報 ・業務関係情報 [○] 国税関係情報 [○] 地方税関係情報 [] 健康・医療関係情報 [○] 医療保険関係情報 [] 児童福祉・子育て関係情報 [○] 障害者福祉関係情報 [○] 生活保護・社会福祉関係情報 [○] 介護・高齢者福祉関係情報 [○] 雇用・労働関係情報 [○] 年金関係情報 [] 学校・教育関係情報 [] 災害関係情報 [] その他 ()	
	・個人番号、その他識別情報:対象者を正確に特定するため。 ・5情報、連絡先、その他住民票関係情報:対象者の賦課期日時点の居住地、世帯情報及び通知書等の送付先を把握するため。 ・国税関係情報:対象の確定申告書に係る情報に基づき、住民税の算出、減免等を行うため。 ・地方税関係情報:公平かつ適正な課税を行い、対象者に対し税額通知、各種証明書を発行するため。 ・医療保険関係情報、障害者福祉関係情報、介護・高齢者福祉関係情報、雇用・労働関係情報:住民税の非課税判定や所得控除の判定等に使用するため。 ・生活保護・社会福祉関係情報:住民税の非課税判定及び減免判定を行うため。 ・年金関係情報:対象者の公的年金等支払報告書に係る情報に基づき、住民税の算出(年金特別徴収税額の算出)を行うため。	
	全ての記録項目	
⑤保有開始日	平成27年10月5日	
⑥事務担当部署	税務課	

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（ 戸籍住民サービス課・保護課 ） ☐ 行政機関・独立行政法人等（ 情報共有ネットワークシステムを利用する機関、国税庁、日本年金機構 ） ☐ 地方公共団体・地方独立行政法人（ 情報共有ネットワークシステムを利用する機関、他自治体 ） ☐ 民間事業者（ 給与支払者、年金支払者 ） ☐ その他（ 地方公共団体情報システム機構 ）
②入手方法		☐ 紙 ☐ 電子記録媒体（フラッシュメモリを除く。） ☐ フラッシュメモリ ☐ 電子メール ☐ 専用線 ☐ 庁内連携システム ☐ 情報提供ネットワークシステム ☐ その他（ — ）
③入手の時期・頻度		・住民票関係情報 業務システム更新時、即時連携され入手可能となる。通年を通して複数回入手。 ・給与支払報告書 入手方法は、eLTAX（電子提出）、窓口・郵送提出。毎年1月～3月に複数回入手。その後、都度入手。 ・確定申告書 入手方法は、eLTAX、窓口・郵送提出。毎年2月～4月に複数回入手。その後、都度入手。 ・特別区民税・都民税申告書 入手方法は、窓口・郵送提出。毎年2月～3月に複数回入手。その後、都度入手。 ・年金支払報告書 入手方法は、eLTAX、窓口・郵送提出。毎年1月末～2月上旬に複数回入手。その後、都度入手。 ・寄附金税額控除申告特例通知書 入手方法は、eLTAX、郵送提出。毎年1月末～2月中旬に複数回入手。その後、都度入手。
④入手に係る妥当性		各種申告書等（特別区民税・都民税申告書、確定申告書、給与支払報告書、公的年金等支払報告書等）については、地方税法、区税条例等で提出、情報提供等が定められている。
⑤本人への明示		住民税の賦課に必要な各種情報については、地方税法第317条の2、命令第2条の表48の項に基づき収集していることを周知している。
⑥使用目的 ※		各種申告書の受付、本人確認、正確な住民税の課税及び通知等
変更の妥当性		
⑦使用の主体	使用部署 ※	税務課、収納課、戸籍住民サービス課、各区民事務所（分室）
	使用者数	[100人以上500人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
⑧使用方法 ※		①各種申告書等の受付に関する事務 ・特別区民税・都民税申告書、確定申告書、給与支払報告書、公的年金等支払報告書等の国税関係情報、地方税関係情報から住民等の所得情報、控除額情報を把握する。 ・住民票関係情報から、申告者の個人番号、賦課期日時点での住所、世帯情報を把握する。 ・障害者関係情報、生活保護関係情報から非課税者を把握する。 ②各種申告情報等に基づく特別区民税・都民税の賦課、通知に関する事務 ・上記で収集した各種情報に基づき、住民等に対する特別区民税・都民税賦課額を決定する。 ・決定した特別区民税・都民税賦課額情報を元に書面または電子データで税額を通知する。

	情報の突合 ※	・住民票関係情報と国税関係情報、地方税関係情報、障害者関係情報、生活保護関係情報を突合して、非課税者を確認する。【上記①】 ・住民票関係情報と国税関係情報、地方税関係情報を突合して、所得額、控除額を確認する。【上記①】 ・本人から申告された扶養控除情報等と他市町村又は情報提供ネットワークシステムから入手した地方税関係情報を突合して、控除額等を確認する。【上記①、②】 ・住民票関係情報と地方税関係情報を突合して、税額通知に係るデータを作成する。【上記②】
	情報の統計分析 ※	地方自治法第252条の17の5第1項に基づく「市町村税課税状況等の調」に関する集計等の統計処理を行っているが、特定の個人を判別するような情報の統計や分析は行っていない。
	権利利益に影響を与え得る決定 ※	所得額、各種控除額に基づき住民税額の賦課決定を行う。
⑨使用開始日		平成28年1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	システム保守委託	
①委託内容	システムの保守作業	
②取扱いを委託する特定個人情報ファイルの範囲	特定個人情報ファイルの全体 <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
対象となる本人の数	10万人以上100万人未満 <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上	
対象となる本人の範囲 ※	地方税法その他地方税に関する法律及び東京都台東区特別区税条例の規定により、税務関係書類に個人番号を記載することとされる者（納税義務者及び被扶養者、その他調査対象者）	
その妥当性	システム開発元であり、かつ申請管理システムの安定的な稼働のための専門的な知識及び技術を有するため。 なお、税務システムの運用、保守、改修の際に正常に動作することを確認する必要があるため、特定個人情報ファイルの全体を委託対象とする。	
③委託先における取扱者数	10人以上50人未満 <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
④委託先への特定個人情報ファイルの提供方法	専用線 電子メール 電子記録媒体（フラッシュメモリを除く。） フラッシュメモリ 紙 ○ その他 （サーバ室内にてシステムの直接操作を行うため、特定個人情報ファイルの提供は発生しない。）	
⑤委託先名の確認方法	東京都台東区情報公開条例に基づく開示請求を行うことで確認ができる。	
⑥委託先名	株式会社日立システムズ	
再委託	⑦再委託の有無 ※	再委託する <選択肢> 1) 再委託する 2) 再委託しない
	⑧再委託の許諾方法	やむを得ず再委託する必要があるときは、委託先はあらかじめ以下の内容を記載した書面を台東区に提出することにより、再委託を許諾する。 ・再委託の理由 ・再委託先の選定理由 ・再委託先に対する業務の管理方法 ・再委託先の名称、代表者及び所在地 ・再委託する業務の内容 ・再委託する業務に含まれる情報の種類 ・再委託先のセキュリティ管理体制 ・その他、委託者が指定する事項
	⑨再委託事項	委託内容の一部とし、協議により定める。

委託事項2		当初課税資料データファイルの作成委託	
①委託内容		課税資料をデータ入力し、データファイルを作成する。	
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 ☐ 1万人以上10万人未満 ☐ 10万人以上100万人未満 ☐ 100万人以上1,000万人未満 ☐ 1,000万人以上	
対象となる本人の数		☐ 1万人未満 ☐ 1万人以上10万人未満 ☐ 10万人以上100万人未満 ☐ 100万人以上1,000万人未満 ☐ 1,000万人以上	
対象となる本人の範囲 ※		地方税法その他地方税に関する法律及び東京都台東区特別区税条例の規定により、税務関係書類に個人番号を記載することとされる者（納税義務者及び被扶養者、その他調査対象者）	
その妥当性		電算処理を行うために申告書等の情報をデータ化する必要があるが、処理件数など時間的制約のある中で専門業者への委託が必要である。	
③委託先における取扱者数		☐ 10人以上50人未満 ☐ 10人未満 ☐ 10人以上50人未満 ☐ 50人以上100人未満 ☐ 100人以上500人未満 ☐ 500人以上1,000人未満 ☐ 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		東京都台東区情報公開条例に基づく開示請求を行うことで確認ができる。	
⑥委託先名		株式会社プログレス	
再委託	⑦再委託の有無 ※	☐ 再委託しない ☐ 再委託する ☐ 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3		地方税ポータルシステム(eLTAX) ASPサービス提供委託
①委託内容		審査システム、国税連携システム、特徴税通システムをASPサービスとして利用するための業務
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの一部] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	対象となる本人の数	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	地方税法その他地方税に関する法律及び東京都台東区特別区税条例の規定により、税務関係書類に個人番号を記載することとされる者(納税義務者及び被扶養者)
	その妥当性	システムの保守やバージョンアップ作業等、専門性が必要であるため。
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		東京都台東区情報公開条例に基づく開示請求を行うことで確認ができる。
⑥委託先名		株式会社TKC
再委託	⑦再委託の有無 ※	[再委託する] <選択肢> 1) 再委託する 2) 再委託しない
	⑧再委託の許諾方法	委託先からの申し出を受け、下記の事項をもとに許諾を判断する。 ・再委託の必要性 ・再委託先の選定基準 ・再委託先の委託管理方法 ・再委託先の事業者名 ・再委託する業務の内容 ・再委託する業務に含まれる情報の種類 ・再委託先のセキュリティ管理体制
	⑨再委託事項	委託内容の一部とし、協議により定める。

委託事項4		課税資料作成補助及び賦課事務補助業務に係る人材派遣委託
①委託内容		課税資料作成補助
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 ※	地方税法その他地方税に関する法律及び東京都台東区特別区税条例の規定により、税務関係書類に個人番号を記載することとされる者(納税義務者及び被扶養者、その他調査対象者)
	その妥当性	処理件数など時間的制約のある中で業者への委託が必要である。
③委託先における取扱者数		☐ 10人以上50人未満 <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法		☐ 専用線 ☐ 電子メール ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ フラッシュメモリ ☒ 紙 ☐ その他 ()
⑤委託先名の確認方法		東京都台東区情報公開条例に基づく開示請求を行うことで確認ができる。
⑥委託先名		キャリアリンク株式会社
再委託	⑦再委託の有無 ※	☐ 再委託しない <選択肢> 1) 再委託する 2) 再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	

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 (77) 件 ☐ 移転を行っている (38) 件 ☐ 行っていない
提供先1	命令第2条の表に定める情報照会者
①法令上の根拠	(別紙1) 命令第2条の表に定める事務に記載
②提供先における用途	(別紙1) 命令第2条の表に定める事務に記載
③提供する情報	住民税関係情報
④提供する情報の対象となる本人の数	☐ 10万人以上100万人未満 <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	住民税の課税権を台東区が有する者と被扶養者
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 () ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	照会を受けた都度。
提供先2	国税庁長官
①法令上の根拠	番号法第19条第10号 地方税法第317条
②提供先における用途	所得税に関する事務
③提供する情報	住民税関係情報
④提供する情報の対象となる本人の数	☐ 10万人以上100万人未満 <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	住民税の課税権を台東区が有する者と被扶養者
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 (国税連携システム→LGWAN→地方税ポータルセンター→専用回線) ☒ 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	対象があった場合に随時。

提供先3	市町村長
①法令上の根拠	番号法第19条第10号 地方税法第294条第3項 同法附則第7条第5及び第12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
③提供する情報	住民税関係情報
④提供する情報の対象となる本人の数	☐ 1万人以上10万人未満 <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	他の自治体に課税権のある者、地方税法第294条第3項の規定により課税した者、申告特例を選択した寄附者等
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☒ 紙 (国税連携システム→LGWAN→地方税ポータルセンター→LGWAN)
⑦時期・頻度	対象があった場合に随時。
提供先4	特別徴収義務者(給与支払者)
①法令上の根拠	番号法第19条第1号、地方税法第321条の4第2項
②提供先における用途	給与所得等に係る個人住民税について、給与の支払いをする際に特別徴収し、市区町村に納入するため。
③提供する情報	住民税関係情報
④提供する情報の対象となる本人の数	☐ 1万人以上10万人未満 <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	納税義務者のうち給与からの特別徴収となる者
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☒ その他 ☐ 専用線 ☒ 電子記録媒体(フラッシュメモリを除く。) ☒ 紙 (審査システム→LGWAN→地方税ポータルセンター→インターネット回線)
⑦時期・頻度	当初課税(毎年5月)1回、当初課税後随時

提供先5	特別徴収義務者(公的年金等支払者)
①法令上の根拠	番号法第19条第1号、地方税法第321条の7の5、同法第321条の7の7
②提供先における用途	公的年金等所得に係る個人住民税について、年金支給をする際に特別徴収し、市区町村に納入するため。
③提供する情報	住民税関係情報
④提供する情報の対象となる本人の数	[1万人以上10万人未満] <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	納税義務者のうち公的年金等からの特別徴収となる者
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 (LGWAN) ☐ 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	特別徴収税額通知 年1回(7月) 特別徴収停止通知・特別徴収税額等変更通知 月1回
提供先6	東京都台東区教育委員会
①法令上の根拠	番号法第19条第11号、台東区番号条例
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子ども・子育て支援事業の実施に関する事務
③提供する情報	住民税関係情報
④提供する情報の対象となる本人の数	[1万人以上10万人未満] <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	主務省令又は規則で定める者
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 (庁内連携システム) ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	照会を受けた都度。

移転先1	番号法において個人番号の利用可能な事務を行う実施機関内の主管課
①法令上の根拠	番号法第9条第1項別表 台東区番号条例第3条
②移転先における用途	番号法第9条第1項別表で定める事務(別紙2のとおり)
③移転する情報	住民税関係情報
④移転する情報の対象となる本人の数	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	主務省令又は規則で定める者
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 () ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	照会を受けた都度。
移転先2～5	
移転先2	以下の条例において、個人番号の利用可能な事務を行う実施機関内の主管課 ・台東区番号条例 ・行政手続における特定の個人を識別するための番号の利用等に関する法律に基づく個人番号の利用並びに特定個人情報の利用及び提供に関する条例(以下「東京都番号条例」という。)
①法令上の根拠	番号法第9条第2項 台東区番号条例第3条 東京都番号条例第4条
②移転先における用途	台東区番号条例及び東京都番号条例で定める事務(別紙3のとおり)
③移転する情報	住民税関係情報
④移転する情報の対象となる本人の数	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	以下の規則で定める者 ・東京都台東区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施行条例施行規則 ・行政手続における特定の個人を識別するための番号の利用等に関する法律に基づく個人番号の利用並びに特定個人情報の利用及び提供に関する条例施行規則
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 () ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	照会を受けた都度。

6. 特定個人情報の保管・消去

①保管場所 ※		＜台東区における措置＞ ①データセンターに設置するサーバに保管している。 ※データセンターでは事前に申請のうえ入館を許可しており、入館時は本人確認を行っている。サーバ室への入退室では、ICカードと生体による認証が行われている。また、監視カメラ等セキュリティ装置による不正侵入対策や不正入退室対策や不正持込・持出防止対策を行っている。 ②課税資料等の紙媒体については、施錠可能な書庫により保管する。 ＜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、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ー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。 ＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 ＜サービス検索・電子申請機能における措置＞ ・サービス検索・電子申請機能から取得したデータは、セキュリティゲートにて入退館管理をしている建物のうち、さらに厳格な入退室管理を行っている区画に設置したサーバ内に保管している。 ・LGWAN接続端末から紙帳票の打ち出しや、ダウンロードはせず、外部記録媒体等への保存も行わない。 ＜申請管理システムにおける措置＞ ①データセンターに設置するサーバに保管している。 ※データセンターでは事前に申請のうえ入館を許可しており、入館時は本人確認を行っている。サーバ室への入退室では、ICカードと生体による認証が行われている。また、監視カメラ等セキュリティ装置による不正侵入対策や不正入退室対策や不正持込・持出防止対策を行っている。												
②保管期間	期間	＜選択肢＞ <table><tr><td>1) 1年未満</td><td>2) 1年</td><td>3) 2年</td></tr><tr><td>4) 3年</td><td>5) 4年</td><td>6) 5年</td></tr><tr><td>7) 6年以上10年未満</td><td>8) 10年以上20年未満</td><td>9) 20年以上</td></tr><tr><td colspan="3">10) 定められていない</td></tr></table> [6年以上10年未満]	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		
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	地方税法の規定により、賦課決定ができる最長の期間が法定納期限翌日から7年間であるため。												

③消去方法	＜台東区における措置＞ ・ディスク交換やハード更改等の際は、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。 ・課税資料等の紙媒体については、外部業者による溶解処理を実施している。 ・eLTAXについては、削除権限を有する区職員において、クライアントから操作手順書により消去する。 ＜中間サーバー・プラットフォームにおける措置＞ ・特定個人情報の消去は地方公共団体からの操作によって実施されるため、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。 ・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。 ・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。 ＜ガバメントクラウドにおける措置＞ ・特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ・クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に当たって確実にデータを消去する。 ・既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 ＜サービス検索・電子申請機能における措置＞ ・LGWAN接続端末から紙帳票の打ち出しや、ダウンロードはせず、外部記録媒体等への保存も行わない。 ＜申請管理システムにおける措置＞ ・事務手続きごとに定められた保管期間を超過した申請管理システムデータを、バッチ処理によりデータベースから消去する。 ・ディスク交換やハード更改等の際は、物理的破壊又は専用ソフト等を利用して完全に消去する。
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) 軽自動車税賦課情報ファイル

2. 基本情報

①ファイルの種類 ※		[システム用ファイル]	＜選択肢＞ 1) システム用ファイル 2) その他の電子ファイル(表計算ファイル等)
②対象となる本人の数		[10万人以上100万人未満]	＜選択肢＞ 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
③対象となる本人の範囲 ※		台東区内に主たる定置場を有する軽自動車等の納税義務者(所有者)	
	その必要性	軽自動車税の適正な賦課徴収を行うため。	
④記録される項目		[100項目以上]	＜選択肢＞ 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
	主な記録項目 ※	・識別情報 [○] 個人番号 [] 個人番号対応符号 [○] その他識別情報(内部番号) ・連絡先等情報 [○] 5情報(氏名、氏名の振り仮名、性別、生年月日、住所) [○] 連絡先(電話番号等) [○] その他住民票関係情報 ・業務関係情報 [] 国税関係情報 [○] 地方税関係情報 [] 健康・医療関係情報 [] 医療保険関係情報 [] 児童福祉・子育て関係情報 [○] 障害者福祉関係情報 [○] 生活保護・社会福祉関係情報 [] 介護・高齢者福祉関係情報 [] 雇用・労働関係情報 [] 年金関係情報 [] 学校・教育関係情報 [] 災害関係情報 [] その他 ()	
	その妥当性	・個人番号、その他識別情報:対象者を正確に特定するため。 ・5情報、連絡先、その他住民票関係情報:納税者に対する通知書等の送付先情報として使用するため。 ・地方税関係情報:公平かつ適正な課税を行うため。また対象者に対し税額通知、各種証明書を発行するため。 ・障害者福祉関係情報、生活保護・社会福祉関係情報:軽自動車税の減免を行うため。	
	全ての記録項目	別添2を参照。	
⑤保有開始日		平成27年10月5日	
⑥事務担当部署		税務課	

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（ 戸籍住民サービス課・保護課 ） ☐ 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（ 都道府県等 ） ☐ 民間事業者（ ） ☐ その他（ 地方公共団体情報システム機構 ）	
②入手方法		☐ 紙 ☐ 電子記録媒体（フラッシュメモリを除く。） ☐ フラッシュメモリ ☐ 電子メール ☐ 専用線 ☐ 庁内連携システム ☐ 情報提供ネットワークシステム ☐ その他（ 住民基本台帳ネットワークシステム、軽自動車検査情報市区町村提供システム ）	
③入手の時期・頻度		・住民票関係情報 業務システム更新時、即時連携され入手可能となる。通年を通して複数回入手する。 ・軽自動車税申告（報告）書 原動機付自転車及び小型特殊自動車の登録、廃車等の申告時に随時入手する。 ・障害者関係情報、生活保護関係情報 原則年1回、減免の可否を決定する際に入手する。	
④入手に係る妥当性		軽自動車税申告（報告）書については、地方税法、区税条例等で提出、報告等が定められている。	
⑤本人への明示		住民税の賦課に必要な各種情報については、地方税法第463条の19、命令第2条の表48の項に基づき収集していることを周知している。	
⑥使用目的 ※		各種申告書の受付け、本人確認、正確な軽自動車税の課税及び通知等	
変更の妥当性		—	
⑦使用の主体	使用部署 ※	税務課、収納課、戸籍住民サービス課、各区民事務所（分室）	
	使用者数	[100人以上500人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
⑧使用方法 ※		①申告書の受付に関する事務 ・軽自動車税申告（報告）書から車両情報や所有者等の情報を登録する。 ・住民票関係情報から、申告者の個人番号、住所を把握する。 ・障害者関係情報、生活保護関係情報から減免者を把握する。 ②各種申告情報等に基づく特別区民税・都民税の賦課、通知に関する事務 ・上記で収集した各所情報に基づき、賦課額を決定する。 ・決定した軽自動車税賦課情報を元に税額決定通知書を送付する。	
情報の突合 ※		・住民票関係情報と障害者関係情報、生活保護関係情報を突合して、減免者を確認する。【上記①】 ・住民票関係情報と地方税関係情報を突合して、税額通知に係るデータを作成する。【上記②】	
情報の統計分析 ※		地方自治法第252条の17の5第1項に基づく「市町村税課税状況等の調」に関する集計等の統計処理を行っているが、特定の個人を判別するような情報の統計や分析は行っていない。	
権利利益に影響を与え得る決定 ※		車両の所有状況と障害者関係情報、生活保護関係情報に基づき賦課決定を行う。	
⑨使用開始日		平成28年1月1日	

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※	委託する <選択肢> 1) 委託する 2) 委託しない (1) 件	
委託事項1	システム保守委託	
①委託内容	システムの保守作業	
②取扱いを委託する特定個人情報ファイルの範囲	特定個人情報ファイルの全体 <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
	対象となる本人の数	10万人以上100万人未満 <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	台東区内に主たる定置場を有する軽自動車等の納税義務者(所有者)
	その妥当性	税務システムの運用、保守、改修の際に正常に動作することを確認する必要があるため、特定個人情報ファイルの全体を委託対象とする。
③委託先における取扱者数	10人以上50人未満 <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
④委託先への特定個人情報ファイルの提供方法	専用線 電子メール 電子記録媒体(フラッシュメモリを除く。) フラッシュメモリ 紙 ○ その他 (サーバ室内にてシステムの直接操作を行うため、特定個人情報ファイルの提供は発生しない。)	
⑤委託先名の確認方法	東京都台東区情報公開条例に基づく開示請求を行うことで確認ができる。	
⑥委託先名	株式会社日立システムズ	
再委託	⑦再委託の有無 ※	再委託する <選択肢> 1) 再委託する 2) 再委託しない
	⑧再委託の許諾方法	やむを得ず再委託する必要があるときは、委託先はあらかじめ以下の内容を記載した書面を台東区に提出することにより、再委託を許諾する。 ・再委託の理由 ・再委託先の選定理由 ・再委託先に対する業務の管理方法 ・再委託先の名称、代表者及び所在地 ・再委託する業務の内容 ・再委託する業務に含まれる情報の種類 ・再委託先のセキュリティ管理体制 ・その他、委託者が指定する事項
	⑨再委託事項	委託内容の一部とし、協議により定める。

5. 特定個人情報の提供・移転(委託に伴うものを除く。)	
提供・移転の有無	☐ 提供を行っている () 件 ☐ 移転を行っている () 件 ☐ 行っていない
提供先1	
①法令上の根拠	
②提供先における用途	
③提供する情報	
④提供する情報の対象となる本人の数	☐ 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	
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 () ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	☐ ① 1万人未満 ② 1万人以上10万人未満 ③ 10万人以上100万人未満 ④ 100万人以上1,000万人未満 ⑤ 1,000万人以上
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 () ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	

6. 特定個人情報の保管・消去																	
①保管場所 ※	＜台東区における措置＞ ①データセンターに設置するサーバに保管している。 ※データセンターでは事前に申請のうえ入館を許可しており、入館時は本人確認を行っている。サーバ室への入退室では、ICカードと生体による認証が行われている。また、監視カメラ等セキュリティ装置による不正侵入対策や不正入退室対策や不正持込・持出防止対策を行っている。 ②課税資料等の紙媒体については、施錠可能な書庫により保管する。 ＜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ー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。 ＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。																
	②保管期間	<table><tr><td>期間</td><td> ＜選択肢＞ <table><tr><td>1) 1年未満</td><td>2) 1年</td><td>3) 2年</td></tr><tr><td>4) 3年</td><td>5) 4年</td><td>6) 5年</td></tr><tr><td>7) 6年以上10年未満</td><td>8) 10年以上20年未満</td><td>9) 20年以上</td></tr><tr><td colspan="3">10) 定められていない</td></tr></table></td></tr><tr><td>その妥当性</td><td>地方税法の規定により、賦課決定ができる最長の期間が法定納期限翌日から7年間であるため</td></tr></table>	期間	＜選択肢＞ <table><tr><td>1) 1年未満</td><td>2) 1年</td><td>3) 2年</td></tr><tr><td>4) 3年</td><td>5) 4年</td><td>6) 5年</td></tr><tr><td>7) 6年以上10年未満</td><td>8) 10年以上20年未満</td><td>9) 20年以上</td></tr><tr><td colspan="3">10) 定められていない</td></tr></table>	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
期間	＜選択肢＞ <table><tr><td>1) 1年未満</td><td>2) 1年</td><td>3) 2年</td></tr><tr><td>4) 3年</td><td>5) 4年</td><td>6) 5年</td></tr><tr><td>7) 6年以上10年未満</td><td>8) 10年以上20年未満</td><td>9) 20年以上</td></tr><tr><td colspan="3">10) 定められていない</td></tr></table>	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						
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	地方税法の規定により、賦課決定ができる最長の期間が法定納期限翌日から7年間であるため																
③消去方法	＜台東区における措置＞ ・ディスク交換やハード更改等の際は、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。 ・課税資料等の紙媒体については、外部業者による溶解処理を実施する。 ＜中間サーバー・プラットフォームにおける措置＞ ・特定個人情報の消去は地方公共団体からの操作によって実施されるため、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。 ・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。 ・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。 ＜ガバメントクラウドにおける措置＞ ・特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ・クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ・既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。																
7. 備考																	
—																	

II 特定個人情報ファイルの概要

1. 特定個人情報ファイル名

(3) 収納情報ファイル

2. 基本情報

①ファイルの種類 ※		[システム用ファイル]	<選択肢> 1) システム用ファイル 2) その他の電子ファイル(表計算ファイル等)
②対象となる本人の数		[10万人以上100万人未満]	<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
③対象となる本人の範囲 ※		納税者、納税管理人、納税承継者	
	その必要性	住民税、軽自動車税の適正な収納管理業務及び過誤納還付金の振り込みを行うため。	
④記録される項目		[100項目以上]	<選択肢> 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
	主な記録項目 ※	・識別情報 [☐] 個人番号 [☐] 個人番号対応符号 [☐] その他識別情報(内部番号) ・連絡先等情報 [☐] 5情報(氏名、氏名の振り仮名、性別、生年月日、住所) [☐] 連絡先(電話番号等) [☐] その他住民票関係情報 ・業務関係情報 [☐] 国税関係情報 [☐] 地方税関係情報 [☐] 健康・医療関係情報 [☐] 医療保険関係情報 [☐] 児童福祉・子育て関係情報 [☐] 障害者福祉関係情報 [☐] 生活保護・社会福祉関係情報 [☐] 介護・高齢者福祉関係情報 [☐] 雇用・労働関係情報 [☐] 年金関係情報 [☐] 学校・教育関係情報 [☐] 災害関係情報 [☐] その他 (口座関連情報、標識番号)	
	その妥当性	・個人番号、その他識別情報:対象者を正確に特定するため。 ・5情報、連絡先、その他住民票関係情報:納税者に対する通知書等の送付先情報として使用するため。 ・地方税関係情報:公平かつ適正な課税を行い、対象者に対し税額通知、各種証明書を発行するため。 ・その他:口座振替情報及び標識番号を管理するため。また、公金受取口座として登録されている口座に、還付金の振り込みを行うため。	
	全ての記録項目	別添2を参照。	
⑤保有開始日		平成27年10月5日	
⑥事務担当部署		税務課	

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 （ 収納課 ） ☐ 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 （ 各市町村 ） ☐ 民間事業者 （ ） ☐ その他 （ 地方公共団体情報システム機構 ）	
②入手方法		☐ 紙 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ フラッシュメモリ ☐ 電子メール ☐ 専用線 ☐ 庁内連携システム ☐ 情報提供ネットワークシステム ☐ その他 （ 住民基本台帳ネットワークシステム ）	
③入手の時期・頻度		・住民票関係情報 業務システム更新時、即時連携され入手可能となる。通年を通して複数回入手する。 ・収納関係情報 収納があった都度入手する。	
④入手に係る妥当性		住民票関係情報については、本人情報確認、本人情報入力に係る事務処理負荷軽減のため、庁内連携システムを利用して取得している。	
⑤本人への明示		住民票関係情報については、税務情報システム内でも利用していることを、広く区民に周知している。	
⑥使用目的 ※		住民税、軽自動車税の適正な収納管理	
変更の妥当性			
⑦使用の主体	使用部署 ※	税務課、収納課、戸籍住民サービス課、各区民事務所(分室)	
	使用者数	100人以上500人未満 <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
⑧使用方法 ※	○収納管理事務 ・収納状況を管理する。 ・納期限を過ぎても完納しない納税者に対して督促状を発送する。 ・申請に基づき、口座振替の登録処理を行う。 ○還付充当処理 ・過誤納金が生じたものについて、還付及び充当の処理を行い、通知書を作成し発送する。また、公金受取口座として登録されている口座に、還付金の振り込みを行う。 ○納税証明書 ・交付申請があったものについて、収納状況を確認の上、交付する。		
	情報の突合 ※	・本人特定のため、内部番号を使用し、特別区民税・都民税賦課情報ファイル及び軽自動車税賦課情報ファイルの氏名、住所等と突合する。 ・本人または代理人の申請内容と台東区で登録されている氏名、住所、生年月日で検索し突合する。	
	情報の統計分析 ※	調定額や収入額、滞納額等の統計処理を行っているが、特定の個人を判別するような情報の統計や分析は行っていない。	
	権利利益に影響を与え得る決定 ※	収納情報に基づき、過誤納金が発生した場合、還付充当処理を行う。	
⑨使用開始日		平成28年1月1日	

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※	委託する <選択肢> 1) 委託する 2) 委託しない (1) 件	
委託事項1	システム保守委託	
①委託内容	システムの保守作業	
②取扱いを委託する特定個人情報ファイルの範囲	特定個人情報ファイルの全体 <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
対象となる本人の数	10万人以上100万人未満 <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上	
対象となる本人の範囲 ※	納税義務者のうち、個人番号を有する者	
その妥当性	税務システムの運用、保守、改修の際に正常に動作することを確認する必要があるため、特定個人情報ファイルの全体を委託対象とする	
③委託先における取扱者数	10人以上50人未満 <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
④委託先への特定個人情報ファイルの提供方法	専用線 電子メール 電子記録媒体(フラッシュメモリを除く。) フラッシュメモリ 紙 ○ その他 (サーバ室内にてシステムの直接操作を行うため、特定個人情報ファイルの提供は発生しない。)	
⑤委託先名の確認方法	東京都台東区情報公開条例に基づく開示請求を行うことで確認ができる。	
⑥委託先名	株式会社日立システムズ	
再委託	⑦再委託の有無 ※	再委託する <選択肢> 1) 再委託する 2) 再委託しない
	⑧再委託の許諾方法	やむを得ず再委託する必要があるときは、委託先はあらかじめ以下の内容を記載した書面を台東区に提出することにより、再委託を許諾する。 ・再委託の理由 ・再委託先の選定理由 ・再委託先に対する業務の管理方法 ・再委託先の名称、代表者及び所在地 ・再委託する業務の内容 ・再委託する業務に含まれる情報の種類 ・再委託先のセキュリティ管理体制 ・その他、委託者が指定する事項
	⑨再委託事項	委託内容の一部とし、協議により定める

5. 特定個人情報の提供・移転(委託に伴うものを除く。)

提供・移転の有無	[] 提供を行っている（ ）件 [] 移転を行っている（ ）件 [○] 行っていない
提供先1	
①法令上の根拠	
②提供先における用途	
③提供する情報	
④提供する情報の対象となる本人の数	[] ＜選択肢＞ 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	
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	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[] ＜選択肢＞ 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	[] 庁内連携システム [] 専用線 [] 電子メール [] 電子記録媒体（フラッシュメモリを除く。） [] フラッシュメモリ [] 紙 [] その他（ ）
⑦時期・頻度	

6. 特定個人情報の保管・消去													
①保管場所 ※		＜台東区における措置＞ ①データセンターに設置するサーバに保管している。 ※データセンターでは事前に申請のうえ入館を許可しており、入館時は本人確認を行っている。サーバ室への入退室では、ICカードと生体による認証が行われている。また、監視カメラ等セキュリティ装置による不正侵入対策や不正入退室対策や不正持込・持出防止対策を行っている。 ②課税資料等の紙媒体については、施錠可能な書庫により保管する。 ＜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ー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。 ＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。											
	②保管期間	＜選択肢＞ <table border="0"> <tr> <td>1) 1年未満</td> <td>2) 1年</td> <td>3) 2年</td> </tr> <tr> <td>4) 3年</td> <td>5) 4年</td> <td>6) 5年</td> </tr> <tr> <td>7) 6年以上10年未満</td> <td>8) 10年以上20年未満</td> <td>9) 20年以上</td> </tr> <tr> <td>10) 定められていない</td> <td></td> <td></td> </tr> </table> [定められていない]	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	
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	還付、充当など収納管理のため、過去の記録を保存する必要がある。											
③消去方法		＜台東区における措置＞ ・ディスク交換やハード更改等の際は、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。 ・課税資料等の紙媒体については、外部業者による溶解処理を実施する。 ＜中間サーバー・プラットフォームにおける措置＞ ・特定個人情報の消去は地方公共団体からの操作によって実施されるため、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。 ・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。 ・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。 ＜ガバメントクラウドにおける措置＞ ・特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ・クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に当たって確実にデータを消去する。 ・既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。											
7. 備考													
—													

Ⅱ 特定個人情報ファイルの概要

1. 特定個人情報ファイル名	
(4)滞納整理情報ファイル	
2. 基本情報	
①ファイルの種類 ※	システム用ファイル ☐ システム用ファイル ☐ 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 ☐ 1万人未満 ☐ 1万人以上10万人未満 ☐ 10万人以上100万人未満 ☐ 100万人以上1,000万人未満 ☐ 1,000万人以上
③対象となる本人の範囲 ※	納税者、納税管理人、納税承継者
その必要性	特別区民税・都民税及び軽自動車税の適正な滞納整理実現のため。
④記録される項目	100項目以上 ☐ 10項目未満 ☐ 10項目以上50項目未満 ☐ 50項目以上100項目未満 ☐ 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、その他識別情報:対象者を正確に特定するため。 ・5情報、連絡先、その他住民票関係情報:納税者に対する通知書等の送付先情報として使用するため。 ・地方税関係情報:対象者の実態を把握するため。 ・生活保護・社会福祉関係情報:執行停止の判断に使用するため。
全ての記録項目	別添2を参照。
⑤保有開始日	平成27年10月5日
⑥事務担当部署	収納課

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 （ 戸籍住民サービス課 ） ☐ 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 （ 都道府県、各区市町村 ） ☐ 民間事業者 （ ） ☒ その他 （ 地方公共団体情報システム機構 ）	
②入手方法		☒ 紙 ☐ 電子記録媒体（フラッシュメモリを除く。） ☐ フラッシュメモリ ☐ 電子メール ☐ 専用線 ☒ 庁内連携システム ☐ 情報提供ネットワークシステム ☒ その他 （ 住民基本台帳ネットワークシステム ）	
③入手の時期・頻度		・住民票関係情報 業務システム更新時、即時連携され入手可能となる。通年を通して複数回入手する。 ・他自治体からの滞納状況・再転出先等調査回答情報 事務調査が必要となった都度入手する。	
④入手に係る妥当性		・住民票関係情報については、本人情報確認、本人情報入力に係る事務処理負荷軽減のため、庁内連携システムを利用して取得している。 ・地方税法第20条の11により、地方税に関する調査について必要がある場合に当該調査に関し参考となる資料を取得している。	
⑤本人への明示		・住民票関係情報については、税務情報システム内でも利用していることを広く区民に周知している。 ・滞納整理状況等調査回答情報については、地方税法第20条の11に基づき、利用していることを住民に周知している。	
⑥使用目的 ※		住民税、軽自動車税の適正な収納管理	
変更の妥当性			
⑦使用の主体	使用部署 ※	収納課	
	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 ※		☐ 個人情報の管理 対象者個人の特定に必要な情報管理を行う。 ☐ 家族情報の管理 世帯単位での滞納把握に必要な情報管理を行う。 ☐ 課税収納情報の管理 調定額、収納額および滞納額と延滞金等の管理に必要な情報管理を行う。 ☐ 交渉経過情報の管理 対象者との交渉内容情報管理を行う。 ☐ 処分情報の管理 財産、行政処分情報の管理を行う。 ☐ 分納情報の管理 分納誓約情報の管理を行う。	
情報の突合 ※		賦課・収納情報と突合して滞納有無の確認を行う。	
情報の統計分析 ※		税の滞納整理に関する統計や分析は行っているが、特定の個人を判別するような情報の統計や分析は行っていない。	
権利利益に影響を与え得る決定 ※		滞納情報に基づき、財産調査等の結果に応じて、滞納処分を行う。	
⑨使用開始日		平成28年1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	システム保守委託	
①委託内容	システムの保守作業	
②取扱いを委託する特定個人情報ファイルの範囲	特定個人情報ファイルの一部 <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 ※	納税者、納税管理人、納税承継者	
その妥当性	滞納管理システムでは、特別区民税・都民税、軽自動車税、国民健康保険料、後期高齢者医療保険料、介護保険料が賦課された者全員が管理対象となっており、システムを安定的に稼働させるためには、専門知識を有している必要がある。	
③委託先における取扱者数	10人未満 <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
④委託先への特定個人情報ファイルの提供方法	専用線 電子メール 電子記録媒体(フラッシュメモリを除く。) フラッシュメモリ 紙 ○ その他 (サーバ室内にてシステムの直接操作を行うため、特定個人情報ファイルの提供は発生しない。)	
⑤委託先名の確認方法	東京都台東区情報公開条例に基づく開示請求を行うことで確認ができる。	
⑥委託先名	北日本コンピューターサービス株式会社	
再委託	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		滞納管理システム入力等業務委託	
①委託内容		滞納者の実態調査及び財産調査等の回答に係る事務補助	
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 ※	納税者、納税管理人、納税承継者	
	その妥当性	職員が滞納処分および納税交渉に専心するため、滞納管理システムへの入力等の業務を委託することにより、効率的かつ効果的な滞納整理事務が推進される。	
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 (サーバ室内にてシステムの直接操作を行うため、特定個人情報ファイルの提供は発生しない。)	
⑤委託先名の確認方法		東京都台東区情報公開条例に基づく開示請求を行うことで確認ができる。	
⑥委託先名		株式会社ケー・デー・シー	
再委託	⑦再委託の有無 ※	[再委託しない] <選択肢> 1) 再委託する 2) 再委託しない	
	⑧再委託の許諾方法		
	⑨再委託事項		

委託事項3		電話催告業務委託
①委託内容		滞納者等に対する電話による自主的納付の勧奨に関する業務
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの一部] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	対象となる本人の数	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	納税者、納税管理人、納税承継者
	その妥当性	特別区民税・都民税および軽自動車税等の未納者へ対して早期対応を図り、新規滞納者の増加を抑制するため、電話催告をしている。職員では対応しきれない部分を補うため、委託が必要である。
③委託先における取扱者数		[10人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法		[] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [○] その他 (サーバ室内にてシステムの直接操作を行うため、特定個人情報ファイル の提供は発生しない。)
⑤委託先名の確認方法		東京都台東区情報公開条例に基づく開示請求を行うことで確認ができる。
⑥委託先名		株式会社ケー・デー・シー
再委託	⑦再委託の有無 ※	[再委託しない] <選択肢> 1) 再委託する 2) 再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	

委託事項4		滞納整理指導員派遣委託	
①委託内容		職員への助言、指導事務、滞納整理事務補助等	
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの一部] <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 ※	納税者、納税管理人、納税承継者	
	その妥当性	困難案件の滞納整理において適切な助言・指導が必要となる。	
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 (サーバ室内にてシステムの直接操作を行うため、特定個人情報ファイル の提供は発生しない。)	
⑤委託先名の確認方法		東京都台東区情報公開条例に基づく開示請求を行うことで確認ができる。	
⑥委託先名		公益財団法人 東京税務協会	
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 () 件 ☐ 移転を行っている () 件 ☐ 行っていない
提供先1	
①法令上の根拠	
②提供先における用途	
③提供する情報	
④提供する情報の対象となる本人の数	<input style="margin-right: 10px;" type="checkbox"/> <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	
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 () ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	<input style="margin-right: 10px;" type="checkbox"/> <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 () ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	

6. 特定個人情報の保管・消去		
①保管場所 ※		・データセンターに設置するサーバに保管している。 ※データセンターでは事前に申請のうえ入館を許可しており、入館時は本人確認を行っている。サーバ室への入退室では、ICカードと生体による認証が行われている。また、監視カメラ等セキュリティ装置による不正侵入対策や不正入退室対策や不正持込・持出防止対策を行っている。 ・課税資料等の紙媒体については、施錠可能な書庫により保管する。
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 [定められていない]
	その妥当性	還付、充当など収納管理のため、過去の記録を保存する必要がある。
③消去方法		申請書、届出書等の紙媒体については、外部業者による溶解処理を実施している。
7. 備考		
—		

(別添2) 特定個人情報ファイル記録項目

別添2のとおり

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)特別区民税・都民税賦課情報ファイル	
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	・区民の個人番号、基本5情報、その他の住民票関係情報の入手方法は、住民基本台帳システムにて入力した情報を、庁内連携システム経由で取得する方法に限定されるため、対象者以外の情報を入手することはない。区民、企業、国税庁、日本年金機構等から予め定められた方法に基づき入手する課税対象者情報は、1件ごとに基本5情報等を確認の上、対象者以外の情報を入手しないように精査する。 ・地方税ポータルセンター(eLTAX)では、申告等の手続きを行おうとしている者からしか情報を受け付けられないようにシステムで制御している。申告データ等を送信する際は電子証明書に電子署名を行うことにより、なりすましの確認を行うことができる。 ・申告データ等に設定された提出先情報により、提出先の自治体の審査サーバーへ送信されるようシステムで制御されており、対象者以外の情報を入手することはない。 ・国税連携システムにおいても台東区を送信先と設定した対象者以外の情報を入手することができないようにシステムで制御されている。 ＜サービス検索・電子申請機能における措置＞ マニュアルやweb上で、個人番号の提出が必要な者の要件を明示・周知し、本人以外の情報の入手を防止する。 ＜申請管理システムにおける措置＞ 申請データは、マイナポータル申請管理以外の方法では入手はできず、申請者以外の情報を格納することはできない。
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	・区民の個人番号、基本5情報、その他の住民票関係情報の入手方法は、住民基本台帳システムにて入力した情報を、庁内連携システム経由で予め定められたインターフェース仕様に基づき、取得する方法に限定されるため、必要な情報以外の情報を入手することはない。 ・区民、企業、国税庁、日本年金機構等から入手する課税対象者情報は、予め定められたインターフェース仕様、帳票様式に基づき入手するため、必要な情報以外を入手することはない。 ＜サービス検索・電子申請機能における措置＞ 住民がマイナポータル申請管理の画面の誘導に従いサービスを検索し申請フォームを選択して必要情報を入力することとなるが、画面での誘導を簡潔に行うことで、異なる手続に係る申請や不要な情報を送信してしまうリスクを防止する。 ＜申請管理システムにおける措置＞ 権限によって参照できる申請データが制限しており、他業務の申請情報が混在しない仕組みになっている。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 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	各届出受領の際に必ず個人番号カード等の身分証明書による本人確認が実施されており、不適切な方法での入手は行わない。申告等を行う者は、法令等で規定されている様式において、必要事項を記載することによって申告等を行うことを認識した上で手続きを行うこととなる。 ＜サービス検索・電子申請機能における措置＞ ・住民が個人住民税申請ポータルから個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、のちに署名検証も行われる。 ・個人住民税申請ポータルの画面の誘導において、住民に理解してもらいながら操作をしていただくことで、住民に過剰な負担をかけることなく電子申請を実施いただけるよう措置を講じている。 ＜申請管理システムにおける措置＞ ・申請データは、サービス検索・電子申請機能以外の方法では入手はできない。 ・システムを利用する職員を限定し、利用者権限を設定することによって入手可能な情報に制限をかける。
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 that 不正確であるリスク		
入手の際の本人確認の措置の内容	番号法第16条に基づく本人確認を行う。ただし、給与支払者、公的年金等支払者、国税庁から入手する特定個人情報については、入手元が番号法第16条等の規定に基づき、本人確認を行った上で情報を入手していることが前提となっており、台東区が当該入手元から入手する際は番号法第16条等は適用されない。電子処理組織を使用して個人番号の提供を受ける場合には、署名用電子証明書及び電子署名が行われた当該提供に係る情報の送信を受けることなどにより、本人確認を行う。 ＜個人住民税申告ポータルにおける措置＞ 住民が個人住民税申告ポータルからサービス検索・電子申請機能へ個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、電子署名付与済の個人番号付電子申請データを受領した地方公共団体は署名検証(有効性確認、改ざん検知等)を実施することとなる。これにより、本人確認を実施する。	
個人番号の真正性確認の措置の内容	番号法第16条に基づく本人確認を行う。ただし、給与支払者、公的年金等支払者、国税庁から入手する特定個人情報については、入手元が番号法第16条等の規定に基づき、本人確認を行った上で情報を入手していることが前提となっており、台東区が当該入手元から入手する際は番号法第16条等は適用されない。電子処理組織を使用して個人番号の提供を受ける場合、個人番号の入手元が番号法第16条の規定に基づき真正性確認を行った上で情報を入手していることが前提となっているため、台東区は既に真正性が確認された情報を入手している。	
特定個人情報の正確性確保の措置の内容	・特定個人情報の入力、削除及び訂正を行う際は、正確性を確保するために、入力、削除及び訂正を行った者以外の者が確認する等、複数の者による確認を行う。また、入力、削除及び訂正した内容を確認した者に申告書等の様式の行政側使用欄にサインさせる。 ・職員が収集した情報に基づいて、間違いがあれば職権で適宜修正することで正確性を確保している。 ・地方税法に基づいて台東区に提出する申告書、法定調書等については、提出されたものをそのまま原本として保管する必要がある。 ・納税者の申告内容を帳簿等で確認し、申告内容に誤りがあれば是正を求めるなどの対応を行っている。 ・国税連携システムで入手する所得税申告書等については、国税庁が申告内容に誤りがあれば是正を求めるなどの対応をし、修正された情報が国税庁から送信される。 ＜個人住民税申告ポータルにおける措置＞ 個人番号カード内の記憶領域に格納された個人番号を申請フォームに自動転記を行うことにより、不正確な個人番号の入力を抑止する措置を講じている。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク4: 入手の際に特定個人情報 that 漏えい・紛失するリスク		
リスクに対する措置の内容	・窓口で本人又は本人の代理人が来庁する場合は、職員が直接申告書等を収受する。また窓口仕切り板を設置し、他者の目に触れないようにしている。 ・郵送の場合は事前に提出先を広く周知し、誤送付などによる漏えい等を防止している。 ・地方税ポータルセンターと審査システム及び国税連携システムについては、閉域網であるLGWANを利用している。 ＜サービス検索・電子申請機能における措置＞ マイナポータル申請管理と地方公共団体との間は、LGWAN回線を用いた暗号化通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。 ＜申請管理システムにおける措置＞ サービス検索・電子申請機能と申請管理システム間は、LGWAN回線を含めた閉域網となっている。また、通信は暗号化されており、外部からの盗聴、漏洩等が起こらない仕組みになっている。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。)におけるその他のリスク及びそのリスクに対する措置		
—		

3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク		
宛名システム等における措置の内容	個人番号を必要としない事務に関して住民情報の要求があった場合は、個人番号が含まれない情報のみを提供するようにアクセス制御を行っている。	
事務で使用するその他のシステムにおける措置の内容	税務システムでは、対象者の初期画面に特定個人情報が表示されない仕組みとなっている。事務遂行にあたっては、対象者の初期画面にて、評価対象の事務を遂行する上で必要な者であることを確認したうえで、特定個人情報を表示させている。	
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	システムを使用する際には、二要素認証を用いて使用する職員を特定している。また、その認証により使用者がシステム上、使用できる機能を制限することで不適切な方法で入手が行えない対策を行っている。 <サービス検索・電子申請機能における措置> ・サービス検索・電子申請機能をLGWAN接続端末上で利用する必要がある職員を特定し、個人ごとのユーザIDを割り当てるとともに、IDとパスワードによる認証を行う。 ・なりすましによる不正を防止する観点から共用IDの利用を禁止する。 <申請管理システムにおける措置> システムを使用する際には、二要素認証を用いて使用する職員を特定している。また、その認証により使用者がシステム上、使用できる機能を制限することで不適切な方法で入手が行えない対策を行っている。	
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	発効及び失効については、人事異動があった場合は業務に対応したアクセス権限を確認し、情報システム課に書面にて権限付与及び喪失の依頼を行っている。 <サービス検索・電子申請機能における措置> サービス検索・電子申請機能のアクセス権限の発効・失効については、以下の管理を行う。 ① 発効の管理 ・アクセス権限が必要となった場合、ユーザID管理者が事務に必要な情報にアクセスできるユーザIDを発効する。 ・ユーザID管理者が各事務に必要なアクセス権限の管理表を作成する。 ・アクセス権限の付与を必要最低限とする。 ② 失効の管理 ・定期的又は異動、退職等のイベントが発生したタイミングで、権限を有していた職員の異動、退職等情報を確認し、当該事由が生じた際には速やかにアクセス権限を更新し、当該ユーザIDを失効させる。 <申請管理システムにおける措置> 発効及び失効については、人事異動があった場合は業務に対応したアクセス権限を確認し、情報システム課に書面にて権限付与及び喪失の依頼を行っている。	
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	操作者の取り扱う事務に応じたアクセス権限が付与されるように管理している。 <サービス検索・電子申請機能における措置> サービス検索・電子申請機能のアクセス権限については、以下の管理を行う。 ・定期的にユーザーID一覧をシステムより出力し、アクセス権限の管理表と突合を行い、アクセス権限の確認及び不正利用の有無をユーザーID管理者が確認を行う。また、不要となったユーザーIDやアクセス権限を速やかに変更又は削除する。 <申請管理システムにおける措置> 操作者の取り扱う事務に応じたアクセス権限が付与されるように管理している。	

特定個人情報の使用の記録		[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
	具体的な方法	誰が、いつ、どの情報にアクセスしたかについて、アクセスログを残して管理している。 <サービス検索・電子申請機能における措置> ・サービス検索・電子申請機能を管理する端末の操作ログの記録を行い、操作者個人を特定できるようにする。 <申請管理システムにおける措置> 誰が、いつ、どの情報にアクセスしたかについて、アクセスログを残して管理している。	
その他の措置の内容			
リスクへの対策は十分か		[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク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		・業務目的以外にファイルを利用してはならないことを研修により指導する。 ・情報参照履歴を管理し、業務外利用をした場合には特定可能であることを職員に周知し、業務外の利用を防止する。 ・特定個人情報などのシステム上管理している情報はサーバー一括管理とし、各クライアント端末には情報を保管しない仕組みとする。 <サービス検索・電子申請機能における措置> ・サービス検索・電子申請機能へアクセスできる端末を制限する。 ・LGWAN接続端末から紙帳票の打ち出しや、ダウンロードはせず、外部記録媒体等への保存も行わない。 <申請管理システムにおける措置> ・業務目的以外にファイルを利用してはならないことを研修により指導する。	
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
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		・ファイルの不必要な複製、送付及び送信を行ってはならないことを研修により指導する。 ・作業上、止むを得ず特定個人情報を持ち出さなければならない事態が生じたときは、情報セキュリティ責任者及び情報セキュリティ運用管理者の承認を得るものとする。 <サービス検索・電子申請機能における措置> ・サービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータについて、改ざんや業務目的以外の複製を禁止するルールを定め、ルールに従って業務を行う。 ・LGWAN接続端末から紙帳票の打ち出しや、ダウンロードはせず、外部記録媒体等への保存も行わない。 <申請管理システムにおける措置> 申請データは、外部記憶媒体に書き出せない仕組みとなっており、不正に複製することはできない。	
リスクへの対策は十分か		[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
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			
・税務システムの照会画面等には個人番号をデフォルト表示せず、照会ボタンを押下することにより表示させ、そのアクセスログを管理している。 ・税務システム端末が設置してある場所から離席する場合、ログアウトするよう指導・教育をしている。ログアウトをせずに離席した場合、時間が経過すると強制ログアウトとなる。 ・特定個人情報が表示された画面のハードコピーの取得については、事務処理に必要となる範囲にとどめ、終了後にシュレッダーを用いて裁断処理を行う。			

☐ 委託しない

情報保護管理体制の確認

- ・財団法人日本情報処理開発協会（JIPDEC）が認定している「プライバシーマーク」を取得している。
- ・個人情報保護に関する規定、体制の整備、安全管理措置を取っている。

具体的な制限方法	業務使用権限の付与が制限されているため、作業従事者への特定個人情報の閲覧権限及び更新権限は付与されない。
----------	--

具体的な方法

- ・作業を実施した場合、作業従事者と作業内容を作業実績票に記載をしている。
- ・作業実績票については、台東区に提出することを義務付けている。

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遵守の確認方法	他者への提供は実施していない。
----------------------------------	-----------------

委託元と委託先間の提供に関するルール の内容及びルール遵守の確認方法	【データファイルの作成委託】 ・電子媒体での提供の際は暗号化を行い、運搬の際は施錠可能なケースに格納することとしている。 ・情報の受渡しの際に、媒体の受渡し、及び内容・件数について確認のうえ署名等を行わせている。 【システム運用保守の委託】 ・基本的に情報提供は行わない。 ・作業上、情報提供がある場合は、庁舎外への持ち出しを禁止している。
---	--

ルール内容及び ルール遵守の確認方法	【データファイルの作成委託】 ・特定個人情報が記載された媒体(各種帳票・外部記録媒体)を提供した場合は、必ず返却させる。 ・機器に記録されたデータについては消去させ、処理日や処理件数を報告させている。 【システム運用保守の委託】 ・情報が記載された媒体(紙、外部記録媒体)を提供した場合は、必ず返却させる。 ・情報を記録している機器が不要となった場合、機器を復元不可の状態としたうえで廃棄する。
-------------------------------	---

委託契約書中の特定個人情報ファイルの取扱いに関する規定		[定めている] <選択肢> 1) 定めている 2) 定めていない
	規定の内容	① 契約の履行により直接又は間接に知り得た特定個人情報を第三者に漏らしてはならない。また、契約期間満了後も同様とする。 ② 特定個人情報保護管理に関する社内規定を委託者に提出しなければならない。当該規定を変更する場合も同様とする。 ③ 従業者に対して特定個人情報保護に関する監督・教育を行わなければならない。 ④ 電算処理施設、処理日程及び特定個人情報の取扱者を通知しなければならない。 ⑤ 第三者に再委託してはならない。ただし、当該業務の一部についてやむを得ず第三者に委託する必要があるときは、あらかじめ再委託する業者名、再委託の内容、事業執行の場所を委託者に通知し、委託者の承諾を得なければならない。また、再受託者に対してもこの契約を遵守させなければならない。 ⑥ 特定個人情報を委託者の指示する目的以外に使用してはならない。また、第三者に提供してはならない。 ⑦ 特定個人情報の全部又は一部を委託者の許可なく複写し、又は複製してはならない。委託者の許可を受け複写したときは、電算処理業務の終了後直ちに複写した当該特定個人情報を消去し、再生又は再利用ができない状態にしなければならない。 ⑧ 特定個人情報の授受に従事する者をあらかじめ定め、その引渡しは、委託者が指定した日時、場所において行わなければならない。また、受託者は、引渡しの際に預かり証を委託者に提出しなければならない。 ⑨ 特定個人情報の保管及び管理について、善良な管理者の注意をもって当たり、個人情報の消滅、毀損等の事故を防止しなければならない。 ⑩ 特定個人情報へのアクセス制限等、データ保護に関する措置を講じなければならない。 ⑪ 契約による業務を終了したとき又は委託者が請求したときは、その保有する特定個人情報を直ちに委託者に返還しなければならない。 ⑫ 特定個人情報を搬送する必要がある場合は、記録された電磁的記録、帳票等を専用ケースに収納し、事故防止措置を講じたうえ搬送しなければならない。 ⑬ 特定個人情報をこの契約によって定める場所以外の場所に持ち出してはならない。 ⑭ 特定個人情報の管理状況について随時に立入検査又は調査をし、受託者に対して契約内容の遵守状況等の必要な報告を求め、又は委託業務の処理に関して指示を与えることができる。 ⑮ 事故が生じたときには、直ちに委託者に対して通知するとともに、遅滞なくその状況を書面をもって委託者に報告し、委託者の指示に従わなければならない。 ⑯ 業務処理中に不良又は不用品が発生したときは、受託者は、その発生数量、発生原因を委託者に報告し、その処分について委託者と協議するものとする。 ⑰ ⑯に違反し委託者に損害を与えたときは、受託者はその損害を賠償しなければならない。
再委託先による特定個人情報ファイルの適切な取扱いの確保		[十分に行っている] <選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない 4) 再委託していない
	具体的な方法	・委託先は、再委託先名、再委託内容及び再委託する業務に含まれる情報の種類、再委託先のセキュリティ管理体制等を記載した書面を台東区に提出し、台東区の承認を受けなければならない。 ・情報の保管及び管理等に関する特記事項については、委託先と同様に、再委託先においても遵守するものとし、委託先は、再委託先がこれを遵守することに關して一切の責任を負う。
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
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
—		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	・庁内のデータ連携については、全て連携処理のログを取得している。 ・参照した画面のアクセスログを残している。 ・審査システムを利用して提供する特定個人情報については、送信処理の際に、提供した情報のファイル名、送信処理の日時及び結果等が審査システムに記録される。 ・国税連携システムを利用して提供する特定個人情報については、送信処理の際に、データ登録を行った職員名や送信処理の日時、送信先団体名等が国税連携システムに記録される。	
特定個人情報の提供・移転に関するルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
ルールの内容及びルール遵守の確認方法	・番号法及び台東区番号条例の規定により、認められる範囲の特定個人情報の提供・移転を行う。 ・審査システム及び国税連携システムを利用した特定個人情報の提供は、地方税共同機構が指定する方法で行っており、番号法施行規則第20条第2号の規定に基づき、安全性及び信頼性を確保するために必要な基準として、内閣総理大臣が定める基準に従って処理している。	
その他の措置の内容		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 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	・情報の移転については、庁内連携システムを通して行うことで、不適切な移転を防止する。 ・審査システム及び国税連携システムを使用した情報提供は、担当者ID及び暗証番号を設定した一部の職員のみ実施することができる。また、提供方法は各システムの機能で決められている。なお、地方税ポータルセンターへの送信には閉域網であるLGWANが用いられている。また番号法施行規則第20条第2号の規定に基づき、安全性及び信頼性を確保するために必要な基準として、内閣総理大臣が定める基準に従って処理している。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容	・庁内連携については、事務単位で使用する連携インターフェイスを取り決めている。また、画面の参照については、個人単位で参照権限を付与している。 ・審査システム及び国税連携システムを使用して情報提供を行う場合、データ内容や提供先の確認を複数名で複層的に行っている。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の提供・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	＜台東区における措置＞ ・庁内連携システムを介した情報照会による特定個人情報の入手は、各業務システム一庁内連携システム間の自動連携に限定しているため、職員が目的外で入手を行うことはない。 ・各業務システム一庁内連携システム間の自動連携では接続システムの認証やシステム毎に異なる通信規則の定義を行い、接続を承認されているシステムのみが接続可能となっている。 ＜中間サーバー・ソフトウェアにおける措置＞ ・情報照会機能(※1)により、情報提供ネットワークシステムに情報照会を行う際には、提供許可証の発行と照会内容の照会許可照会リスト(※2)との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから提供許可証を受領してから情報照会を実施することになる。そのため、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ・中間サーバーの職員認証・権限管理機能(※3)では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 (※1) 情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 (※2) 番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 (※3) 中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。		
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク2: 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ 中間サーバーは個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークを使用した特定個人情報の入手のみを実施できるように設計されるため、安全性が担保されている。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバーと既存システム、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対策を維持した行政専用ネットワーク(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。 ・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。		
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク3: 入手した特定個人情報が不正確であるリスク			
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ 中間サーバーは個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークを使用して、情報提供用個人識別符号にうより紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。		
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている	

リスク4： 入手の際に特定個人情報漏えい・紛失するリスク		
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ・中間サーバーは情報提供ネットワークを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している。中間サーバーは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みとなっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ・既存システムからの接続に対し認証を行い、許可されないシステムからのアクセスを防止する仕組みを設けている。 ・情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報漏えい・紛失するリスクを軽減している。 ・中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバーと既存システム、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対策を維持した行政専用ネットワーク（総合行政ネットワーク等）を利用することにより、漏えい・紛失のリスクに対応している。 ・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漏えい・紛失のリスクに対応している。 ・中間サーバー・プラットフォームの事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはできない。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク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	＜中間サーバー・ソフトウェアにおける措置＞ ・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照会リストを情報提供ネットワークシステムから入手し、中間サーバーにも格納して、情報提供機能により、照会許可照会リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ・情報提供機能により、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、特定個人情報不正に提供されるリスクに対応している。 ・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不正に提供されるリスクに対応している。 ・中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク6： 不適切な方法で提供されるリスク		
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ・セキュリティ管理機能（暗号化・複合機能と、鍵情報及び照会許可照合リストを管理する機能）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っている。 ・中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバーと既存システム、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対策を維持した行政専用ネットワーク（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。 ・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漏えい・紛失のリスクに対応している。 ・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。	
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＞ ・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提供されるリスクに対応している。 ・情報提供データベース管理機能（特定個人情報を副本として保存・管理する機能。）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。 ・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。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置		
＜中間サーバー・ソフトウェアにおける措置＞ ・中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ・情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ・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。 ・中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ・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。		

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	<台東区における措置> ・各端末機から、外部媒体に個人情報を移動できない仕組みになっている。また、同端末機のローカルに個人情報を保存できない仕組みになっている。 ・新耐震基準に基づいたデータセンター内にサーバ室を設置している。 ・データセンターは、事前に申請のうえ入館を許可する形式となっており、入館時も本人確認を行っている。サーバ室への入退室では、ICカードと生体による認証が行われている。また、監視カメラ等セキュリティ装置による不正侵入対策や不正入退室対策や不正持込・持出防止対策を行っている。 ・災害等の急な停電によるデータの消失を防ぐために、非常発電装置を導入している。 ・特定個人情報が記載された申告書等の紙媒体や外部記録媒体については、施錠管理を行っている書庫やキャビネットに保管している。 <中間サーバー・プラットフォームにおける措置> 中間サーバー・プラットフォームは、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。 <ガバメントクラウドにおける措置> ・ガバメントクラウドについては政府情報システムのセキュリティ制度 (ISMAP) のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ・事前に許可されていない装置等に関しては、外部に持出できないこととしている。 <サービス検索・電子申請機能における措置> ・LGWAN接続端末については、業務時間内のセキュリティワイヤー等による固定、操作場所への入退室管理、業務時間外の施錠できるキャビネット等への保管、などの物理的対策を講じている。 ・LGWAN接続端末から紙帳票の打ち出しや、ダウンロードはせず、外部記録媒体等への保存も行わない。 <申請管理システムにおける措置> <台東区における措置>と同様

⑥技術的対策	[十分にやっている]	<選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
具体的な対策の内容		<台東区における措置> ・情報提供にあたっては、システムで作成した特定個人情報、庁内連携システムに誤った状態で作成されることがないことを、検証工程で十分に確認している。 ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォールを設置している。 ・アンチウイルスソフトを導入している。 ・日次でバックアップファイルを取得している。 <中間サーバー・プラットフォームにおける措置> ・中間サーバー・プラットフォームでは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、アクセス制御、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ・中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ・導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ・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。 ・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。 ・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。 ・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。 <ガバメントクラウドにおける措置> ・国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ・地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」(令和4年10月 デジタル庁。以下「利用基準」という。)に規定する「ASP」をいう。以下同じ。)又はガバメントクラウド運用管理補助者(利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。)は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ・クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ・クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ・地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ・ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ・地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ・地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。 <サービス検索・電子申請機能における措置> ・LGWAN接続端末へのウイルス検出ソフトウェア等の導入により、ウイルス定義ファイルの定期的な更新及びウイルスチェックを行い、マルウェア検出を行う。 ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。 <申請管理システムにおける措置> <台東区における措置>と同様
⑦バックアップ	[十分にやっている]	<選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
⑧事故発生時手順の策定・周知	[十分にやっている]	<選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	<選択肢> 1) 発生あり 2) 発生なし
その内容	—	
再発防止策の内容	—	

⑩死者の個人番号	[保管している]	<選択肢> 1) 保管している 2) 保管していない
具体的な保管方法	生存者の個人番号と同様の方法にて安全管理措置を実施している。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2: 特定個人情報が古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	住基事務所において、住基法第14条及び第34条の規定に基づく実態調査等を行っており、最新の住民基本台帳情報を利用して特別区民税・都民税の賦課事務を行っている。 <サービス検索・電子申請機能における措置> LGWAN接続端末は、個人番号付電子申請データの一時保管として使用していない。 <申請管理システムにおける措置> 申請管理システムはサービス検索・電子申請機能から取得したデータの一時保管として使用し、審査等は行わない。	
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	<台東区における措置> ・システム上で保管している情報は期間経過後、必要に応じて削除を行う。 ・紙媒体で保管している申告書等は保管期間の経過後、外部業者による溶解処理を実施している。 <ガバメントクラウドにおける措置> データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。 <サービス検索・電子申請機能における措置> LGWAN接続端末から紙帳票の打ち出しや、ダウンロードはせず、外部記録媒体等への保存も行わない。 <申請管理システムにおける措置> システム上で保管している情報は期間経過後、必要に応じて削除を行う。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
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)軽自動車税賦課情報ファイル	
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	・区民の個人番号、基本5情報、その他の住民票関係情報の入手方法は、住民基本台帳システムにて入力した情報を、庁内連携システム経由で取得する方法に限定されるため、対象者以外の情報を入手することはない。 ・区民等から入手する課税対象者情報は、1件ごとに基本5情報等を確認の上、対象者以外の情報を入手しないように精査している。対象者以外の情報が含まれている場合には、本来の提出先へ回送を行っている。
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	・区民の個人番号、基本5情報、その他の住民票関係情報の入手方法は、住民基本台帳システムにて入力した情報を、庁内連携システム経由で予め定められたインタフェース仕様に基づき、取得する方法に限定されるため、必要な情報以外の情報を入手することはない。 ・区民等から入手する課税対象者情報は、予め定められた帳票様式に基づき入手するため、必要な情報以外を入手することはない。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 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	・各届出受領の際に必ず個人番号カード等の身分証明書による本人確認が実施されており、不適切な方法での入手は行わない。 ・申告等を行う者は、法令等で規定されている様式において、必要事項を記載することによって申告等を行うことを認識した上で手続きを行う。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	・個人番号カードの提示、若しくは運転免許証等の官公署が発行した写真付きの身分証明書の提示など、その者が本人であることを確認するに至る書類を提示を受けて本人確認を行う。 ・代理人については、代理人の個人番号カード又は身分証明書、代理権確認書類の提示による確認を行う。
個人番号の真正性確認の措置の内容	・上記、入手の際の本人確認とともに個人番号の真正性確認を行っている。
特定個人情報の正確性確保の措置の内容	・特定個人情報の入力、削除及び訂正を行う際は、正確性を確保するために、入力、削除及び訂正を行った者以外の者が確認する等、複数の者による確認を行う。また、入力、削除及び訂正した内容を確認した者に申告書等の様式の行政側使用欄にサインさせる。 ・職員が収集した情報に基づいて、間違いがあれば職権で適宜修正することで正確性を確保している。
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	・窓口で本人又は本人の代理人が来庁する場合は、職員が直接申告書等を収受する。また窓口仕切り板を設置し、他者の目に触れないようにしている。 ・郵送の場合は事前に提出先を広く周知し、誤送付などによる漏えい等を防止している。 ・入手から使用、保管までの保管方法などルール化している。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。)におけるその他のリスク及びそのリスクに対する措置	
—	

3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク		
宛名システム等における措置の内容	個人番号を必要としない事務に関して住民情報の要求があった場合は、個人番号が含まれない情報のみを提供するようにアクセス制御を行っている。	
事務で使用するその他のシステムにおける措置の内容	税務システムでは、対象者の初期画面に特定個人情報が表示されない仕組みとなっている。事務遂行にあたっては、対象者の初期画面にて、評価対象の事務を遂行する上で必要な者であることを確認したうえで、特定個人情報を表示させている。	
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	システムを使用する際には、二要素認証を用いて使用する職員を特定している。また、その認証により使用者がシステム上、使用できる機能を制限することで不適切な方法で入手が行えない対策を行っている。	
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	発効及び失効については、人事異動があった場合は業務に対応したアクセス権限を確認し、情報システム課に書面にて権限付与及び喪失の依頼を行っている。	
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	操作者の取り扱う事務に応じたアクセス権限が付与されるように管理している。	
特定個人情報の使用の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	誰が、いつ、どの情報にアクセスしたかについて、アクセスログを残して管理している。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク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	各種研修等を通して、業務外利用の禁止について指導するとともに、システムの操作ログの記録から業務外利用の特定が可能な旨を職員に周知している。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク4: 特定個人情報ファイルが不正に複製されるリスク		
リスクに対する措置の内容	・バックアップファイルの作成はバックアップサーバ内に取得し、外部記憶媒体による持出は行っていない。 ・バックアップを実行する都度、ログを保存している。 ・特定個人情報ファイルの外部媒体への出力は、特定のアクセス権限を持ったユーザのみが、特定の端末で実施することに限定している。	
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		
・税務システムの照会画面等には個人番号をデフォルト表示せず、照会ボタンを押下することにより表示させ、そのアクセスログを管理している。 ・税務システム端末が設置してある場所から離席する場合、ログアウトするよう指導・教育をしている。ログアウトをせずに離席した場合、時間が経過すると強制ログアウトとなる。 ・特定個人情報が表示された画面のハードコピーの取得については、事務処理に必要な範囲にとどめ、終了後にシュレッダーを用いて裁断処理をする。		

☐ 委託しない

情報保護管理体制の確認

特定個人情報ファイルの閲覧者・更新者の制限

具体的な制限方法

特定個人情報ファイルの取
扱いの記録

具体的な方法

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
の内容及びルール遵
守の確認方法

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

特定個人情報の消去ルール

ルール内容及び ルール遵守の確認方 法

委託契約書中の特定個人情報
 報ファイルの取扱いに関する
 規定

＜選択肢＞

1) 定めている

2) 定めていない

	規定の内容	① 契約の履行により直接又は間接に知り得た特定個人情報を第三者に漏らしてはならない。また、契約期間満了後も同様とする。 ② 特定個人情報保護管理に関する社内規定を委託者に提出しなければならない。当該規定を変更する場合も同様とする。 ③ 従業者に対して特定個人情報保護に関する監督・教育を行わなければならない。 ④ 電算処理施設、処理日程及び特定個人情報の取扱者を通知しなければならない。 ⑤ 第三者に再委託してはならない。ただし、当該業務の一部についてやむを得ず第三者に委託する必要があるときは、あらかじめ再委託する業者名、再委託の内容、事業執行の場所を委託者に通知し、委託者の承諾を得なければならない。また、再受託者に対してもこの契約を遵守させなければならない。 ⑥ 特定個人情報を委託者の指示する目的以外に使用してはならない。また、第三者に提供してはならない。 ⑦ 特定個人情報の全部又は一部を委託者の許可なく複写し、又は複製してはならない。委託者の許可を受け複写したときは、電算処理業務の終了後直ちに複写した当該特定個人情報を消去し、再生又は再利用ができない状態にしなければならない。 ⑧ 特定個人情報の授受に従事する者をあらかじめ定め、その引渡しは、委託者が指定した日時、場所において行わなければならない。また、受託者は、引渡しの際に預かり証を委託者に提出しなければならない。 ⑨ 特定個人情報の保管及び管理について、善良な管理者の注意をもって当たり、個人情報の消滅、毀損等の事故を防止しなければならない。 ⑩ 特定個人情報へのアクセス制限等、データ保護に関する措置を講じなければならない。 ⑪ 契約による業務を終了したとき又は委託者が請求したときは、その保有する特定個人情報を直ちに委託者に返還しなければならない。 ⑫ 特定個人情報を搬送する必要がある場合は、記録された電磁的記録、帳票等を専用ケースに収納し、事故防止措置を講じたうえ搬送しなければならない。 ⑬ 特定個人情報をこの契約によって定める場所以外の場所に持ち出してはならない。 ⑭ 特定個人情報の管理状況について随時に立入検査又は調査をし、受託者に対して契約内容の遵守状況等の必要な報告を求め、又は委託業務の処理に関して指示を与えることができる。 ⑮ 事故が生じたときには、直ちに委託者に対して通知するとともに、遅滞なくその状況を書面をもって委託者に報告し、委託者の指示に従わなければならない。 ⑯ 業務処理中に不良又は不用品が発生したときは、受託者は、その発生数量、発生原因を委託者に報告し、その処分について委託者と協議するものとする。 ⑰ ⑯に違反し委託者に損害を与えたときは、受託者はその損害を賠償しなければならない。
再委託先による特定個人情報ファイルの適切な取扱いの確保		＜選択肢＞ [十分に行っている] 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	・委託先は、再委託先名、再委託内容及び再委託する業務に含まれる情報の種類、再委託先のセキュリティ管理体制等を記載した書面を台東区に提出し、台東区の承認を受けなければならない。 ・情報の保管及び管理等に関する特記事項については、委託先と同様に、再委託先においても遵守するものとし、委託先は、再委託先がこれを遵守することに関して一切の責任を負う。
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
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
—		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[○] 提供・移転しない
リスク1：不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法		
特定個人情報の提供・移転に関するルール	[]	<選択肢> 1) 定めている 2) 定めていない
ルールの内容及び ルール遵守の確認方法		
その他の措置の内容		
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2：不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3：誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		

6. 情報提供ネットワークシステムとの接続		[] 接続しない(入手) [○] 接続しない(提供)	
リスク1: 目的外の入手が行われるリスク			
リスクに対する措置の内容	＜台東区における措置＞ ・庁内連携システムを介した情報照会による特定個人情報の入手は、各業務システムー庁内連携システム間の自動連携に限定しているため、職員が目的外で入手を行うことはない。 ・各業務システムー庁内連携システム間の自動連携では接続システムの認証やシステム毎に異なる通信規則の定義を行い、接続を承認されているシステムのみが接続可能となっている。 ＜中間サーバー・ソフトウェアにおける措置＞ ・情報照会機能により、情報提供ネットワークシステムに情報照会を行う際には、提供許可証の発行と照会内容の照会許可照合リストとの照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ・中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。		
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 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	＜中間サーバー・ソフトウェアにおける措置＞ 中間サーバーは個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークを使用した特定個人情報の入手のみを実施できるように設計されるため、安全性が担保されている。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバーと既存システム、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対策を維持した行政専用ネットワーク(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。 ・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。		
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			
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＞ 中間サーバーは個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。		
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	<中間サーバー・ソフトウェアにおける措置> ・中間サーバーは情報提供ネットワークを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している。中間サーバーは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みとなっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ・既存システムからの接続に対し認証を行い、許可されないシステムからのアクセスを防止する仕組みを設けている。 ・情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報漏えい・紛失するリスクを軽減している。 中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 <中間サーバー・プラットフォームにおける措置> ・中間サーバーと既存システム、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対策を維持した行政専用ネットワーク(総合行政ネットワーク等)を利用することにより、漏えい・紛失のリスクに対応している。 ・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漏えい・紛失のリスクに対応している。 ・中間サーバー・プラットフォームの事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはできない。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク5: 不正な提供が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク6: 不適切な方法で提供されるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク7: 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	
<中間サーバー・ソフトウェアにおける措置> ・中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ・情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 <中間サーバー・プラットフォームにおける措置> ・中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、安全性を確保している。 ・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。 ・中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理(アクセス制御)しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ・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。	

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	<台東区における措置> ・各端末機から、外部媒体に個人情報を移動できない仕組みになっている。また、同端末機のローカルに個人情報を保存できない仕組みになっている。 ・新耐震基準に基づいたデータセンター内にサーバ室を設置している。 ・データセンターは、事前に申請のうえ入館を許可する形式となっており、入館時も本人確認を行っている。サーバ室への入退室では、ICカードと生体による認証が行われている。また、監視カメラ等セキュリティ装置による不正侵入対策や不正入退室対策や不正持込・持出防止対策を行っている。 ・災害等の急な停電によるデータの消失を防ぐために、非常発電装置を導入している。 ・特定個人情報が記載された申告書等の紙媒体や外部記録媒体については、施錠管理を行っている書庫やキャビネットに保管している。 <中間サーバー・プラットフォームにおける措置> 中間サーバー・プラットフォームは、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。 <ガバメントクラウドにおける措置> ・ガバメントクラウドについては政府情報システムのセキュリティ制度(ISMAP)のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ・事前に許可されていない装置等に関しては、外部に持出できないこととしている。

⑥技術的対策	十分にやっている <選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
具体的な対策の内容	<台東区における措置> ・情報提供にあたっては、システムで作成した特定個人情報、庁内連携システムに誤った状態で作成されることがないことを、検証工程で十分に確認している。 ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォールを設置している。 ・アンチウイルスソフトを導入している。 ・日次でバックアップファイルを取得している。 <中間サーバー・プラットフォームにおける措置> ・中間サーバー・プラットフォームでは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、アクセス制御、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ・中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ・導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ・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。 ・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。 ・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。 ・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。 <ガバメントクラウドにおける措置> ・国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ・地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」(令和4年10月 デジタル庁。以下「利用基準」という。)に規定する「ASP」をいう。以下同じ。)又はガバメントクラウド運用管理補助者(利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。)は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ・クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ・クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ・地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ・ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ・地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ・地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。
⑦バックアップ	十分にやっている <選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
⑧事故発生時手順の策定・周知	十分にやっている <選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	発生なし <選択肢> 1) 発生あり 2) 発生なし
その内容	—
再発防止策の内容	—
⑩死者の個人番号	保管している <選択肢> 1) 保管している 2) 保管していない
具体的な保管方法	生存者の個人番号と同様の方法にて安全管理措置を実施している。
その他の措置の内容	—

リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2: 特定個人情報古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	住基事務所において、住基法第14条及び第34条の規定に基づく実態調査等を行っており、最新の住民基本台帳情報を利用して軽自動車税の賦課事務を行っている。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 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	<台東区における措置> ・システム上で保管している情報は期間経過後、必要に応じて削除を行う。 ・紙媒体で保管している申告書等は保管期間の経過後、外部業者による溶解処理を実施している。 <ガバメントクラウドにおける措置> データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		
—		

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

1. 特定個人情報ファイル名	
(3)収納情報ファイル	
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	・区民の個人番号、基本5情報、その他の住民票関係情報の入手方法は、住民基本台帳システムにて入力した情報を、庁内連携システム経由で取得する方法に限定されるため、対象者以外の情報を入手することはない。 ・また、区民等から入手する課税対象者情報は、1件ごとに基本5情報等を確認の上、対象者以外の情報を入手しないように精査している。対象者以外の情報が含まれている場合には、本来の提出先へ回送を行っている。
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	・区民の個人番号、基本5情報、その他の住民票関係情報の入手方法は、住民基本台帳システムにて入力した情報を、庁内連携システム経由で予め定められたインターフェース仕様に基づき、取得する方法に限定されるため、必要な情報以外の情報を入手することはない。 ・区民等から入手する課税対象者情報は、予め定められた帳票様式に基づき入手するため、必要な情報以外を入手することはない。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 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	・各届出受領の際に必ず個人番号カード等の身分証明書による本人確認が実施されており、不適切な方法での入手は行わない。 ・申告等を行う者は、法令等で規定されている様式において、必要事項を記載することによって申告等を行うことを認識した上で手続きを行うこととなる。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	・個人番号カードの提示、若しくは運転免許証等の官公署が発行した写真付きの身分証明書の提示など、その者が本人であることを確認するに至る書類を提示を受けて本人確認を行う。 ・代理人については、代理人の個人番号カード又は身分証明書、代理権確認書類の提示による確認を行う。
個人番号の真正性確認の措置の内容	・上記、入手の際の本人確認とともに個人番号の真正性確認を行っている。
特定個人情報の正確性確保の措置の内容	・特定個人情報の入力、削除及び訂正を行う際は、正確性を確保するために、入力、削除及び訂正を行った者以外の者が確認する等、複数の者による確認を行う。また、入力、削除及び訂正した内容を確認した者に申告書等の様式の行政側使用欄にサインさせる。 ・職員が収集した情報に基づいて、間違いがあれば職権で適宜修正することで正確性を確保している。
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	・窓口で本人又は本人の代理人が来庁する場合は、職員が直接申告書等を収受する。また窓口仕切り板を設置し、他者の目に触れないようにしている。 ・郵送の場合は事前に提出先を広く周知し、誤送付などによる漏えい等を防止している。 ・入手から使用、保管までの保管方法などルール化している。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	
—	

3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク		
宛名システム等における措置の内容	個人番号を必要としない事務に関して住民情報の要求があった場合は、個人番号が含まれない情報のみを提供するようにアクセス制御を行っている。	
事務で使用するその他のシステムにおける措置の内容	税務システムでは、対象者の初期画面に特定個人情報が表示されない仕組みとなっている。事務遂行にあたっては、対象者の初期画面にて、評価対象の事務を遂行する上で必要な者であることを確認したうえで、特定個人情報を表示させている。	
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	システムを使用する際には、二要素認証を用いて使用する職員を特定している。また、その認証により使用者がシステム上、使用できる機能を制限することで不適切な方法で入手が行えない対策を行っている。	
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	発効及び失効については、人事異動があった場合は業務に対応したアクセス権限を確認し、情報システム課に書面にて権限付与及び喪失の依頼を行っている。	
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	操作者の取り扱う事務に応じたアクセス権限が付与されるように管理している。	
特定個人情報の使用の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	誰が、いつ、どの情報にアクセスしたかについて、アクセスログを残して管理している。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク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	各種研修等を通して、業務外利用の禁止について指導するとともに、システムの操作ログの記録から業務外利用の特定が可能な旨を職員に周知している。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク4: 特定個人情報ファイルが不正に複製されるリスク		
リスクに対する措置の内容	・バックアップファイルの作成はバックアップサーバ内に取得し、外部記憶媒体による持出は行っていない。 ・バックアップを実行する都度、ログを保存している。 ・特定個人情報ファイルの外部媒体への出力は、特定のアクセス権限を持ったユーザのみが、特定の端末で実施することに限定している。	
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		
・税務システムの照会画面等には個人番号をデフォルト表示せず、照会ボタンを押下することにより表示させ、そのアクセスログを管理している。 ・税務システム端末が設置してある場所から離席する場合、ログアウトするよう指導・教育をしている。ログアウトをせずに離席した場合、時間が経過すると強制ログアウトとなる。 ・特定個人情報が表示された画面のハードコピーの取得については、事務処理に必要となる範囲にとどめ、終了後にシュレッダーを用いて裁断処理をする。		

☐ 委託しない

情報保護管理体制の確認

特定個人情報ファイルの閲覧者・更新者の制限

具体的な制限方法

特定個人情報ファイルの取
扱いの記録

具体的な方法

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
の内容及びルール遵
守の確認方法

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

特定個人情報の消去ルール

ルール内容及び ルール遵守の確認方 法

【システム運用保守の委託】

- ・情報が記載された媒体(紙、外部記録媒体)を提供した場合は、必ず返却をさせている。
- ・情報を記録している機器が不要となった場合、機器を復元不可の状態としたうえで廃棄をしている。

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	① 契約の履行により直接又は間接に知り得た特定個人情報を第三者に漏らしてはならない。また、契約期間満了後も同様とする。 ② 特定個人情報保護管理に関する社内規定を委託者に提出しなければならない。当該規定を変更する場合も同様とする。 ③ 従業者に対して特定個人情報保護に関する監督・教育を行わなければならない。 ④ 電算処理施設、処理日程及び特定個人情報の取扱者を通知しなければならない。 ⑤ 第三者に再委託してはならない。ただし、当該業務の一部についてやむを得ず第三者に委託する必要があるときは、あらかじめ再委託する業者名、再委託の内容、事業執行の場所を委託者に通知し、委託者の承諾を得なければならない。また、再受託者に対してもこの契約を遵守させなければならない。 ⑥ 特定個人情報を委託者の指示する目的以外に使用してはならない。また、第三者に提供してはならない。 ⑦ 特定個人情報の全部又は一部を委託者の許可なく複写し、又は複製してはならない。委託者の許可を受け複写したときは、電算処理業務の終了後直ちに複写した当該特定個人情報を消去し、再生又は再利用ができない状態にしなければならない。 ⑧ 特定個人情報の授受に従事する者をあらかじめ定め、その引渡しは、委託者が指定した日時、場所において行わなければならない。また、受託者は、引渡しの際に預かり証を委託者に提出しなければならない。 ⑨ 特定個人情報の保管及び管理について、善良な管理者の注意をもって当たり、個人情報の消滅、毀損等の事故を防止しなければならない。 ⑩ 特定個人情報へのアクセス制限等、データ保護に関する措置を講じなければならない。 ⑪ 契約による業務を終了したとき又は委託者が請求したときは、その保有する特定個人情報を直ちに委託者に返還しなければならない。 ⑫ 特定個人情報を搬送する必要がある場合は、記録された電磁的記録、帳票等を専用ケースに収納し、事故防止措置を講じたうえ搬送しなければならない。 ⑬ 特定個人情報をこの契約によって定める場所以外の場所に持ち出してはならない。 ⑭ 特定個人情報の管理状況について随時に立入検査又は調査をし、受託者に対して契約内容の遵守状況等の必要な報告を求め、又は委託業務の処理に関して指示を与えることができる。 ⑮ 事故が生じたときには、直ちに委託者に対して通知するとともに、遅滞なくその状況を書面をもって委託者に報告し、委託者の指示に従わなければならない。 ⑯ 業務処理中に不良又は不用品が発生したときは、受託者は、その発生数量、発生原因を委託者に報告し、その処分について委託者と協議するものとする。 ⑰ ⑯に違反し委託者に損害を与えたときは、受託者はその損害を賠償しなければならない。
再委託先による特定個人情報ファイルの適切な取扱いの確保		[十分に行っている] ＜選択肢＞ 1) 特に力を入れて行っていない 2) 十分に行っている 3) 十分に行っていない 4) 再委託していない
	具体的な方法	・委託先は、再委託先名、再委託内容及び再委託する業務に含まれる情報の種類、再委託先のセキュリティ管理体制等を記載した書面を台東区に提出し、台東区の承認を受けなければならない。 ・情報の保管及び管理等に関する特記事項については、委託先と同様に、再委託先においても遵守するものとし、委託先は、再委託先がこれを遵守することに關して一切の責任を負う。
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
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
—		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[○] 提供・移転しない
リスク1：不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法		
特定個人情報の提供・移転に関するルール	[]	<選択肢> 1) 定めている 2) 定めていない
ルールの内容及び ルール遵守の確認方法		
その他の措置の内容		
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2：不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3：誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		

6. 情報提供ネットワークシステムとの接続		[] 接続しない(入手) [○] 接続しない(提供)	
リスク1: 目的外の入手が行われるリスク			
リスクに対する措置の内容	＜台東区における措置＞ ・庁内連携システムを介した情報照会による特定個人情報の入手は、各業務システム-庁内連携システム間の自動連携に限定しているため、職員が目的外の入手を行うことはない。 ・各業務システム-庁内連携システム間の自動連携では接続システムの認証やシステム毎に異なる通信規則の定義を行い、接続を承認されているシステムのみが接続可能となっている。 ＜中間サーバー・ソフトウェアにおける措置＞ ・情報照会機能により、情報提供ネットワークシステムに情報照会を行う際には、提供許可証の発行と照会内容の照会許可照合リストとの照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ・中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。		
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク2: 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ 中間サーバーは個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークを使用した特定個人情報の入手のみを実施できるように設計されているため、安全性が担保されている。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバーと既存システム、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対策を維持した行政専用ネットワーク(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。 ・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。		
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 that 不正確であるリスク			
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ 中間サーバーは個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。		
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている	

リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク			
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ・中間サーバーは情報提供ネットワークを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している。中間サーバーは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みとなっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ・既存システムからの接続に対し認証を行い、許可されないシステムからのアクセスを防止する仕組みを設けている。情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報が漏えい・紛失するリスクを軽減している。 ・中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバーと既存システム、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対策を維持した行政専用ネットワーク(総合行政ネットワーク等)を利用することにより、漏えい・紛失のリスクに対応している。 ・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漏えい・紛失のリスクに対応している。 ・中間サーバー・プラットフォームの事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはできない。		
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 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	<台東区における措置> ・各端末機から、外部媒体に個人情報を移動できない仕組みになっている。また、同端末機のローカルに個人情報を保存できない仕組みになっている。 ・新耐震基準に基づいたデータセンター内にサーバ室を設置している。 ・データセンターは、事前に申請のうえ入館を許可する形式となっており、入館時も本人確認を行っている。サーバ室への入退室では、ICカードと生体による認証が行われている。また、監視カメラ等セキュリティ装置による不正侵入対策や不正入退室対策や不正持込・持出防止対策を行っている。 ・災害等の急な停電によるデータの消失を防ぐために、非常発電装置を導入している。 ・特定個人情報が記載された申告書等の紙媒体や外部記録媒体については、施錠管理を行っている書庫やキャビネットに保管している。 <中間サーバー・プラットフォームにおける措置> 中間サーバー・プラットフォームは、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。 <ガバメントクラウドにおける措置> ・ガバメントクラウドについては政府情報システムのセキュリティ制度(ISMAP)のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ・事前に許可されていない装置等に関しては、外部に持出できないこととしている。
⑥技術的対策	[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	＜台東区における措置＞ ・情報提供にあたっては、システムで作成した特定個人情報、庁内連携システムに誤った状態で作成されることがないことを、検証工程で十分に確認している。 ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォールを設置している。 ・アンチウイルスソフトを導入している。 ・日次でバックアップファイルを取得している。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバー・プラットフォームでは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、アクセス制御、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ・中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ・導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ・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。 ・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。 ・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。 ・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。 ＜ガバメントクラウドにおける措置＞ ・国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ・地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」(令和4年10月 デジタル庁。以下「利用基準」という。)に規定する「ASP」をいう。以下同じ。)又はガバメントクラウド運用管理補助者(利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。)は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ・クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ・クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ・地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ・ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ・地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ・地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。
⑦バックアップ		[十分にしている] ＜選択肢＞ 1) 特に力を入れて行っている 2) 十分にしている 3) 十分に行っていない
⑧事故発生時手順の策定・周知		[十分にしている] ＜選択肢＞ 1) 特に力を入れて行っている 2) 十分にしている 3) 十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか		[発生なし] ＜選択肢＞ 1) 発生あり 2) 発生なし
	その内容	—
	再発防止策の内容	—
⑩死者の個人番号		[保管している] ＜選択肢＞ 1) 保管している 2) 保管していない
	具体的な保管方法	生存者の個人番号と同様の方法にて安全管理措置を実施している。
その他の措置の内容		—
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク2: 特定個人情報が古い情報のまま保管され続けるリスク	
リスクに対する措置の内容	—
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	<台東区における措置> ・システム上で保管している情報は期間経過後、必要に応じて削除を行う。 ・紙媒体で保管している申告書等は保管期間の経過後、外部業者による溶解処理を実施している。 <ガバメントクラウドにおける措置> データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置	
—	

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

1. 特定個人情報ファイル名	
(4)滞納整理情報ファイル	
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	区民の個人番号、基本5情報、その他の住民票関係情報の入手方法は、住民基本台帳システムにて入力した情報を、庁内連携システム経由で取得する方法に限定されるため、対象者以外の情報を入手することはない。
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	・区民の個人番号、基本5情報、その他の住民票関係情報の入手方法は、住民基本台帳システムにて入力した情報を、庁内連携システム経由で予め定められたインターフェース仕様に基づき、取得する方法に限定されるため、必要な情報以外の情報を入手することはない。 ・区民等から入手する課税対象者情報は、予め定められた帳票様式に基づき入手するため、必要な情報以外を入手することはない。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 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	・各届出受領の際に必ず個人番号カード等の身分証明書による本人確認が実施されており、不適切な方法での入手は行わない。 ・申告等を行う者は、法令等で規定されている様式において、必要事項を記載することによって申告等を行うことを認識した上で手続きを行うこととなる。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	・個人番号カードの提示、若しくは運転免許証等の官公署が発行した写真付きの身分証明書の提示など、その者が本人であることを確認するに至る書類を提示を受けて本人確認を行う。 ・代理人については、代理人の個人番号カード又は身分証明書、代理権確認書類の提示による確認を行う。
個人番号の真正性確認の措置の内容	上記、入手の際の本人確認とともに個人番号の真正性確認を行っている。
特定個人情報の正確性確保の措置の内容	・特定個人情報の入力、削除及び訂正を行う際は、正確性を確保するために、入力、削除及び訂正を行った者以外の者が確認する等、複数の者による確認を行う。 ・職員が収集した情報に基づいて、間違いがあれば職権で適宜修正することで正確性を確保している。
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	・窓口で本人又は本人の代理人が来庁する場合は、職員が直接申請書等を収受する。また窓口仕切り板を設置し、他者の目に触れないようにしている。 ・郵送の場合は事前に提出先を広く周知し、誤送付などによる漏えい等を防止している。 ・入手から使用、保管までの保管方法などルール化している。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	
—	

3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク		
宛名システム等における措置の内容	個人番号を必要としない事務に関して住民情報の要求があった場合は、個人番号が含まれない情報のみを提供するようにアクセス制御を行っている。	
事務で使用するその他のシステムにおける措置の内容	税務システムでは、対象者の初期画面に特定個人情報が表示されない仕組みとなっている。事務遂行にあたっては、対象者の初期画面にて、評価対象の事務を遂行する上で必要な者であることを確認したうえで、特定個人情報を表示させている。	
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	システムを使用する際には、二要素認証を用いて使用する職員を特定している。また、その認証により使用者がシステム上、使用できる機能を制限することで不適切な方法で入手が行えない対策を行っている。	
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	発効及び失効については、人事異動があった場合は業務に対応したアクセス権限を確認し、情報システム課に書面にて権限付与及び喪失の依頼を行っている。	
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	操作者の取り扱う事務に応じたアクセス権限が付与されるように管理している。	
特定個人情報の使用の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	誰が、いつ、どの情報にアクセスしたかについて、アクセスログを残して管理している。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク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	各種研修等を通して、業務外利用の禁止について指導するとともに、システムの操作ログの記録から業務外利用の特定が可能な旨を職員に周知している。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク4: 特定個人情報ファイルが不正に複製されるリスク		
リスクに対する措置の内容	・バックアップファイルの作成はバックアップサーバ内に取得し、外部記憶媒体による持出は行っていない。 ・バックアップを実行する都度、ログを保存している。 ・特定個人情報ファイルの外部媒体への出力は、特定のアクセス権限を持ったユーザのみが、特定の端末で実施することに限定している。	
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		
・税務システムの照会画面等には個人番号をデフォルト表示せず、照会ボタンを押下することにより表示させ、そのアクセスログを管理している。 ・税務システム端末が設置してある場所から離席する場合、ログアウトするよう指導・教育をしている。ログアウトをせずに離席した場合、時間が経過すると強制ログアウトとなる。 ・特定個人情報が表示された画面のハードコピーの取得については、事務処理に必要となる範囲にとどめ、終了後にシュレッダーを用いて裁断処理をする。		

☐ 委託しない

情報保護管理体制の確認

特定個人情報ファイルの閲覧者・更新者の制限

具体的な制限方法

特定個人情報ファイルの取
扱いの記録

具体的な方法

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
の内容及びルール遵
守の確認方法

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

特定個人情報の消去ルール

ルール内容及び ルール遵守の確認方 法

委託者の許可を受けて複写・複製したときは、業務終了後、直ちに利用できないよう処分することとしている。

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

		＜選択肢＞	
「	定めている	1) 定めている	2) 定めていない

	規定の内容 ① 契約の履行により直接又は間接に知り得た特定個人情報を第三者に漏らしてはならない。また、契約期間満了後も同様とする。 ② 特定個人情報保護管理に関する社内規定を委託者に提出しなければならない。当該規定を変更する場合も同様とする。 ③ 従業者に対して特定個人情報保護に関する監督・教育を行わなければならない。 ④ 電算処理施設、処理日程及び特定個人情報の取扱者を通知しなければならない。 ⑤ 第三者に再委託してはならない。ただし、当該業務の一部についてやむを得ず第三者に委託する必要があるときは、あらかじめ再委託する業者名、再委託の内容、事業執行の場所を委託者に通知し、委託者の承諾を得なければならない。また、再受託者に対してもこの契約を遵守させなければならない。 ⑥ 特定個人情報を委託者の指示する目的以外に使用してはならない。また、第三者に提供してはならない。 ⑦ 特定個人情報の全部又は一部を委託者の許可なく複写し、又は複製してはならない。委託者の許可を受け複写したときは、電算処理業務の終了後直ちに複写した当該特定個人情報を消去し、再生又は再利用ができない状態にしなければならない。 ⑧ 特定個人情報の授受に従事する者をあらかじめ定め、その引渡しは、委託者が指定した日時、場所において行わなければならない。また、受託者は、引渡しの際に預かり証を委託者に提出しなければならない。 ⑨ 特定個人情報の保管及び管理について、善良な管理者の注意をもって当たり、個人情報の消滅、毀損等の事故を防止しなければならない。 ⑩ 特定個人情報へのアクセス制限等、データ保護に関する措置を講じなければならない。 ⑪ 契約による業務を終了したとき又は委託者が請求したときは、その保有する特定個人情報を直ちに委託者に返還しなければならない。 ⑫ 特定個人情報を搬送する必要がある場合は、記録された電磁的記録、帳票等を専用ケースに収納し、事故防止措置を講じたうえ搬送しなければならない。 ⑬ 特定個人情報をこの契約によって定める場所以外の場所に持ち出してはならない。 ⑭ 特定個人情報の管理状況について随時に立入検査又は調査をし、受託者に対して契約内容の遵守状況等の必要な報告を求め、又は委託業務の処理に関して指示を与えることができる。 ⑮ 事故が生じたときには、直ちに委託者に対して通知するとともに、遅滞なくその状況を書面をもって委託者に報告し、委託者の指示に従わなければならない。 ⑯ 業務処理中に不良又は不用品が発生したときは、受託者は、その発生数量、発生原因を委託者に報告し、その処分について委託者と協議するものとする。 ⑰ ⑯に違反し委託者に損害を与えたときは、受託者はその損害を賠償しなければならない。
再委託先による特定個人情報ファイルの適切な取扱いの確保	＜選択肢＞ [十分にしている] 1) 特に力を入れて行っていない 2) 十分にしている 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	・委託先は、再委託先名、再委託内容及び再委託する業務に含まれる情報の種類、再委託先のセキュリティ管理体制等を記載した書面を台東区に提出し、台東区の承認を受けなければならない。 ・情報の保管及び管理等に関する特記事項については、委託先と同様に、再委託先においても遵守するものとし、委託先は、再委託先がこれを遵守することに関して一切の責任を負う。
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] 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置	
—	

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[○] 提供・移転しない
リスク1：不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法		
特定個人情報の提供・移転に関するルール	[]	<選択肢> 1) 定めている 2) 定めていない
ルールの内容及び ルール遵守の確認方法		
その他の措置の内容		
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2：不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3：誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		

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	<台東区における措置> ・各端末機から、外部媒体に個人情報を移動できない仕組みになっている。また、同端末機のローカルに個人情報を保存できない仕組みになっている。 ・新耐震基準に基づいたデータセンター内にサーバ室を設置している。 ・データセンターは、事前に申請のうえ入館を許可する形式となっており、入館時も本人確認を行っている。サーバ室への入退室では、ICカードと生体による認証が行われている。また、監視カメラ等セキュリティ装置による不正侵入対策や不正入退室対策や不正持込・持出防止対策を行っている。 ・災害等の急な停電によるデータの消失を防ぐために、非常発電装置を導入している。 ・特定個人情報が記載された申告書等の紙媒体や外部記録媒体については、施錠管理を行っている書庫やキャビネットに保管している。
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	<台東区における措置> ・情報提供にあたっては、システムで作成した特定個人情報が、庁内連携システムに誤った状態で作成されることがないことを、検証工程で十分に確認している。 ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォールを設置している。 ・アンチウイルスソフトを導入している。 ・日次でバックアップファイルを取得している。
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	[発生なし]	<選択肢> 1) 発生あり 2) 発生なし
	その内容	—
	再発防止策の内容	—
⑩死者の個人番号	[保管している]	<選択肢> 1) 保管している 2) 保管していない
	具体的な保管方法	生存者の個人番号と同様の方法にて安全管理措置を実施している。
その他の措置の内容		—
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク2： 特定個人情報古い情報のまま保管され続けるリスク	
リスクに対する措置の内容	住基事務所において、住基法第14条及び第34条の規定に基づく実態調査等を行っており、最新の住民基本台帳情報を利用して滞納整理事務を行っている。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3： 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	<台東区における措置> ・システム上で保管している情報は期間経過後、必要に応じて削除を行う。 ・紙媒体で保管している申告書等は保管期間の経過後、外部業者による溶解処理を実施している。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
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	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
具体的なチェック方法		<台東区における措置> ・年に1回自己点検を実施し、チェック、確認を行った自己点検シートを所属内で共有している。 ・内部統制制度により情報資産に対するリスクを洗い出し、改善策の策定、実施、評価を行い、特定個人情報保護評価に関する規則第14条に規定される評価書の再評価に反映させる。 ・国税連携システムにあつては、「電気通信回線その他の電気通信設備に関する技術基準及び情報通信の技術の利用における安全性及び信頼性を確保するために必要な事項に関する基準」の達成状況について自己評価を実施している。 <中間サーバー・プラットフォームにおける措置> 運用規則等に基づき、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、定期的な自己点検を実施することとしている。
②監査	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にっていない
具体的な内容		<台東区における措置> ・以下の観点により自己監査を年に1回実施する。 評価書記載事項と運用実態のチェック 個人情報保護に関する規程、体制整備 個人情報保護に関する人的安全管理措置 職員の役割責任の明確化、安全管理措置の周知、教育 個人情報保護に関する技術的安全管理措置 ・審査システム及び国税連携システムについては、運営する認定委託先事業者が、情報セキュリティ監査(外部監査)を受けている。 <中間サーバー・プラットフォームにおける措置> ・運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。 ・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。 <ガバメントクラウドにおける措置> ガバメントクラウドについては政府情報システムのセキュリティ制度(ISMAP)のリストに登録されたクラウドサービスから調達することとしており、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。
2. 従業者に対する教育・啓発		
従業者に対する教育・啓発	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にっていない
具体的な方法		<台東区における措置> ・従事する職員(非常勤職員等を含む。)に対して、初任時及び一定期間毎に、必要な知識の習得に資するための研修を実施するとともに、その記録を残している。 ・違反行為を行った者に対しては、都度指導の上、違反行為の程度によっては懲戒の対象となりうる。 ・委託業者に対しては、「個人情報を取り扱う業務委託契約に関する特約条項」及び「特定個人情報を取り扱う業務委託契約の特記事項」を遵守することを義務付けている。 <中間サーバー・プラットフォームにおける措置> 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料を作成し、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

＜中間サーバー・プラットフォームにおける措置＞

中間サーバー・プラットフォームを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。

＜ガバメントクラウドにおける措置＞

ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。

ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。

具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。

V 開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	台東区 総務部 総務課 文書係 〒110-8615 東京都台東区東上野4丁目5番6号 電話 03-5246-1055
②請求方法	台東区役所区政情報コーナーにおいて、本人又は代理人が請求書を提出する。
特記事項	区公式ホームページ上において請求の手続きや請求書の様式を公表している。
③手数料等	[無 料] <選択肢> 1) 有料 2) 無料 (手数料額、納付方法:)
④個人情報ファイル簿の公表	[行っている] <選択肢> 1) 行っている 2) 行っていない
個人情報ファイル名	保有個人情報業務登録票(業務の名称:特別区民税、都民税に関する業務及び軽自動車税に関する業務)
公表場所	台東区役所 区政情報コーナー
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	台東区 区民部 税務課・収納課 〒110-8615東京都台東区東上野4丁目5番6号 電話03-5246-1102
②対応方法	電話・手紙での受付を行う。情報漏えい等の重要な事項については受付票に記録し、関係部署に報告を行う。また、速やかに事実確認を行い対応する。

Ⅵ 評価実施手続

1. 基礎項目評価	
①実施日	令和7年8月31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	台東区パブリックコメント実施要綱に基づき、パブリックコメントによる意見募集を行う。 ・広報たいとう及び区公式ホームページ上で周知を行う。 ・区政情報コーナー、区民事務所、生涯学習センター及び区公式ホームページにおいて本評価書を閲覧できるようにする。
②実施日・期間	令和6年8月16日から令和6年9月17日
③期間を短縮する特段の理由	—
④主な意見の内容	意見なし
⑤評価書への反映	—
3. 第三者点検	
①実施日	令和6年12月18日
②方法	東京都台東区情報公開及び個人情報保護制度運営審議会において意見を聴く。
③結果	審議の結果、了承された。
4. 個人情報保護委員会の承認【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

(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7年10月8日	I 基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム1 ③他のシステムとの接続	[]その他()	[○]その他(申請管理システム)	事前	個人住民税申告の電子化に伴う変更
令和7年10月8日	I 基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム11	(追加)	※該当箇所を参照	事前	個人住民税申告の電子化に伴う変更
令和7年10月8日	I 基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム12	(追加)	※該当箇所を参照	事前	個人住民税申告の電子化に伴う変更
令和7年10月8日	I 基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム13	(追加)	※該当箇所を参照	事前	個人住民税申告の電子化に伴う変更
令和7年10月8日	I 基本情報 (別添1)事務内容(住民税)	(追加)	※該当箇所を参照 (追加部分) ①特別区民税・都民税申告(電子) ②個人住民税申告ポータル ③マイナポータル申請管理(サービス検索・電子申請機能) ④申請管理システム	事前	個人住民税申告の電子化に伴う変更
令和7年10月8日	II 特定個人情報ファイルの概要 (1)特別区民税・都民税賦課情報ファイル 2. 基本情報 ④記録される項目 主な記録項目	4情報(氏名、性別、生年月日、住所)	5情報(氏名、氏名の振り仮名、性別、生年月日、住所)	事後	法令改正に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8日	Ⅱ 特定個人情報ファイルの概要 (1)特別区民税・都民税 賦課情報ファイル 2. 基本情報 ④記録される項目 その妥当性	4情報	5情報	事後	法令改正に伴う変更
令和7年10月8日	Ⅱ 特定個人情報ファイルの概要 (1)特別区民税・都民税 賦課情報ファイル 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ⑥委託先名	株式会社イマージュ	株式会社プログレス	事後	その他の項目の変更であり 事前の提出・公表が義務付けられない
令和7年10月8日	Ⅱ 特定個人情報ファイルの概要 (1)特別区民税・都民税 賦課情報ファイル 6. 特定個人情報の保管・消去 ①保管場所	<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・プラットフォームはデータセンターに設置している。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ②特定個人情報は、サーバー室に設置された中間サーバー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。	※該当箇所参照	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年10月8日	Ⅱ 特定個人情報ファイルの概要 (1)特別区民税・都民税 賦課情報ファイル 6. 特定個人情報の保管・消去 ①保管場所	(追加)	<サービス検索・電子申請機能における措置> ・サービス検索・電子申請機能から取得したデータは、セキュリティゲートにて入退館管理をしている建物のうち、さらに厳格な入退室管理を行っている区画に設置したサーバ内に保管している。 ・LGWAN接続端末から紙帳票の打ち出しや、ダウンロードはせず、外部記録媒体等への保存も行わない。 <申請管理システムにおける措置> ①データセンターに設置するサーバに保管している。 ※データセンターでは事前に申請のうえ入館を許可しており、入館時は本人確認を行っている。サーバ室への入退室では、ICカードと生体による認証が行われている。また、監視カメラ等セキュリティ装置による不正侵入対策や不正入退室対策や不正持込・持出防止対策を行っている。	事前	個人住民税申告の電子化に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8日	Ⅱ 特定個人情報ファイルの概要 (1) 特別区民税・都民税 賦課情報ファイル 6. 特定個人情報の保管・消去 ③ 消去方法	<中間サーバー・プラットフォームにおける措置> ・特定個人情報の消去は地方公共団体からの操作によって実施されるため、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。 ・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。	※該当箇所参照	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年10月8日	Ⅱ 特定個人情報ファイルの概要 (1) 特別区民税・都民税 賦課情報ファイル 6. 特定個人情報の保管・消去 ③ 消去方法	(追加)	<サービス検索・電子申請機能における措置> ・LGWAN接続端末から紙帳票の打ち出しや、ダウンロードはせず、外部記録媒体等への保存も行わない。 <申請管理システムにおける措置> ・事務手続きごとに定められた保管期間を超過した申請管理システムデータを、バッチ処理によりデータベースから消去する。 ・ディスク交換やハード更改等の際は、物理的破壊又は専用ソフト等を利用して完全に消去する。	事前	個人住民税申告の電子化に伴う変更
令和7年10月8日	Ⅱ 特定個人情報ファイルの概要 (2) 軽自動車税賦課情報ファイル 2. 基本情報 ④ 記録される項目 主な記録項目	4情報(氏名、性別、生年月日、住所)	5情報(氏名、氏名の振り仮名、性別、生年月日、住所)	事後	法令改正に伴う変更
令和7年10月8日	Ⅱ 特定個人情報ファイルの概要 (2) 軽自動車税賦課情報ファイル 2. 基本情報 ④ 記録される項目 その妥当性	4情報	5情報	事後	法令改正に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8日	Ⅱ 特定個人情報ファイルの概要 (2) 軽自動車税賦課情報ファイル 6. 特定個人情報の保管・消去 ① 保管場所	< 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・プラットフォームはデータセンターに設置している。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ② 特定個人情報は、サーバー室に設置された中間サーバー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。	※該当箇所参照	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年10月8日	Ⅱ 特定個人情報ファイルの概要 (2) 軽自動車税賦課情報ファイル 6. 特定個人情報の保管・消去 ③ 消去方法	< 中間サーバー・プラットフォームにおける措置 > ・特定個人情報の消去は地方公共団体からの操作によって実施されるため、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。 ・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。	※該当箇所参照	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年10月8日	Ⅱ 特定個人情報ファイルの概要 (3) 収納情報ファイル 2. 基本情報 ④ 記録される項目 主な記録項目	4情報 (氏名、性別、生年月日、住所)	5情報 (氏名、氏名の振り仮名、性別、生年月日、住所)	事後	法令改正に伴う変更
令和7年10月8日	Ⅱ 特定個人情報ファイルの概要 (3) 収納情報ファイル 2. 基本情報 ④ 記録される項目 その妥当性	4情報	5情報	事後	法令改正に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8日	Ⅱ 特定個人情報ファイルの概要 (3) 収納情報ファイル 6. 特定個人情報の保管・消去 ① 保管場所	(追加)	< 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ー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	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年10月8日	Ⅱ 特定個人情報ファイルの概要 (3) 収納情報ファイル 6. 特定個人情報の保管・消去 ③ 消去方法	(追加)	< 中間サーバー・プラットフォームにおける措置 > ・特定個人情報の消去は地方公共団体からの操作によって実施されるため、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。 ・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。 ・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	自治体中間サーバー・プラットフォーム更改に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8日	Ⅱ 特定個人情報ファイルの概要 (4)滞納整理情報ファイル 2. 基本情報 ④記録される項目 主な記録項目	4情報(氏名、性別、生年月日、住所)	5情報(氏名、氏名の振り仮名、性別、生年月日、住所)	事後	法令改正に伴う変更
令和7年10月8日	Ⅱ 特定個人情報ファイルの概要 (4)滞納整理情報ファイル 2. 基本情報 ④記録される項目 主な記録項目	4情報	5情報	事後	法令改正に伴う変更
令和7年10月8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)特別区民税・都民税賦課情報ファイル 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	基本4情報	基本5情報	事後	法令改正に伴う変更
令和7年10月8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)特別区民税・都民税賦課情報ファイル 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	(追加)	<サービス検索・電子申請機能における措置> マニュアルやweb上で、個人番号の提出が必要な者の要件を明示・周知し、本人以外の情報の入手を防止する。 <申請管理システムにおける措置> 申請データは、マイナポータル申請管理以外の方法では入手はできず、申請者以外の情報を格納することはできない。	事前	個人住民税申告の電子化に伴う変更
令和7年10月8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)特別区民税・都民税賦課情報ファイル 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 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	基本4情報	基本5情報	事後	法令改正に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8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) 特別区民税・都民税賦課情報ファイル 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 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	(追加)	<サービス検索・電子申請機能における措置> 住民がマイナポータル申請管理の画面の誘導に従いサービスを検索し申請フォームを選択して必要情報を入力することとなるが、画面での誘導を簡潔に行うことで、異なる手続に係る申請や不要な情報を送信してしまうリスクを防止する。 <申請管理システムにおける措置> 権限によって参照できる申請データが制限しており、他業務の申請情報が混在しない仕組みになっている。	事前	個人住民税申告の電子化に伴う変更
令和7年10月8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) 特別区民税・都民税賦課情報ファイル 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	(追加)	<サービス検索・電子申請機能における措置> ・住民が個人住民税申請ポータルから個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、のちに署名検証も行われる。 ・個人住民税申請ポータルの画面の誘導において、住民に理解してもらいながら操作をしていただくことで、住民に過剰な負担をかけることなく電子申請を実施いただけるよう措置を講じている。 <申請管理システムにおける措置> ・申請データは、サービス検索・電子申請機能以外の方法では入手はできない。 ・システムを利用する職員を限定し、利用者権限を設定することによって入手可能な情報に制限をかける。	事前	個人住民税申告の電子化に伴う変更
令和7年10月8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) 特別区民税・都民税賦課情報ファイル 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	(追加)	<個人住民税申告ポータルにおける措置> 住民が個人住民税申告ポータルからサービス検索・電子申請機能へ個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、電子署名付と済の個人番号付電子申請データを受領した地方公共団体は署名検証(有効性確認、改ざん検知等)を実施することとなる。これにより、本人確認を実施する。	事前	個人住民税申告の電子化に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8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)特別区民税・都民税賦課情報ファイル 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3:入手した特定個人情報が不正確であるリスク 特定個人情報の正確性確保の措置の内容	(追加)	<個人住民税申告ポータルにおける措置> 個人番号カード内の記憶領域に格納された個人番号を申請フォームに自動転記を行うことにより、不正確な個人番号の入力を抑止する措置を講じている。	事前	個人住民税申告の電子化に伴う変更
令和7年10月8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)特別区民税・都民税賦課情報ファイル 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	(追加)	<サービス検索・電子申請機能における措置> マイナポータル申請管理と地方公共団体との間は、LGWAN回線を用いた暗号化通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。 <申請管理システムにおける措置> サービス検索・電子申請機能と申請管理システム間は、LGWAN回線を含めた閉域網となっている。また、通信は暗号化されており、外部からの盗聴、漏洩等が起こらない仕組みになっている。	事前	個人住民税申告の電子化に伴う変更
令和7年10月8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)特別区民税・都民税賦課情報ファイル 3. 特定個人情報の使用 リスク2:権限のない者(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 具体的な管理方法	(追加)	<サービス検索・電子申請機能における措置> ・サービス検索・電子申請機能をLGWAN接続端末上で利用する必要がある職員を特定し、個人ごとのユーザIDを割り当てるとともに、IDとパスワードによる認証を行う。 ・なりすましによる不正を防止する観点から共用IDの利用を禁止する。 <申請管理システムにおける措置> システムを使用する際には、二要素認証を用いて使用する職員を特定している。また、その認証により使用者がシステム上、使用できる機能を制限することで不適切な方法で入手が行えない対策を行っている。	事前	個人住民税申告の電子化に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8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) 特別区民税・都民税賦課情報ファイル 3. 特定個人情報の使用 リスク2: 権限のない者(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 アクセス権限の発効・失効の管理 具体的な管理方法	(追加)	<サービス検索・電子申請機能における措置> サービス検索・電子申請機能のアクセス権限の発効・失効については、以下の管理を行う。 ① 発効の管理 ・アクセス権限が必要となった場合、ユーザID管理者が事務に必要な情報にアクセスできるユーザIDを発効する。 ・ユーザID管理者が各事務に必要なアクセス権限の管理表を作成する。 ・アクセス権限の付与を必要最低限とする。 ② 失効の管理 ・定期的又は異動、退職等のイベントが発生したタイミングで、権限を有していた職員の異動、退職等情報を確認し、当該事由が生じた際には速やかにアクセス権限を更新し、当該ユーザIDを失効させる。 <申請管理システムにおける措置> 発効及び失効については、人事異動があった場合は業務に対応したアクセス権限を確認し、情報システム課に書面にて権限付与及び喪失の依頼を行っている。	事前	個人住民税申告の電子化に伴う変更
令和7年10月8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) 特別区民税・都民税賦課情報ファイル 3. 特定個人情報の使用 リスク2: 権限のない者(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	(追加)	<サービス検索・電子申請機能における措置> サービス検索・電子申請機能のアクセス権限については、以下の管理を行う。 ・定期的にユーザーID一覧をシステムより出力し、アクセス権限の管理表と突合を行い、アクセス権限の確認及び不正利用の有無をユーザーID管理者が確認を行う。また、不要となったユーザーIDやアクセス権限を速やかに変更又は削除する。 <申請管理システムにおける措置> 操作者の取り扱う事務に応じたアクセス権限が付与されるように管理している。	事前	個人住民税申告の電子化に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8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)特別区民税・都民税賦課情報ファイル 3. 特定個人情報の使用 リスク2:権限のない者(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	(追加)	<サービス検索・電子申請機能における措置> ・サービス検索・電子申請機能を管理する端末の操作ログの記録を行い、操作者個人を特定できるようにする。 <申請管理システムにおける措置> 誰が、いつ、どの情報にアクセスしたかについて、アクセスログを残して管理している。	事前	個人住民税申告の電子化に伴う変更
令和7年10月8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)特別区民税・都民税賦課情報ファイル 3. 特定個人情報の使用 リスク3:従事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	(追加)	<サービス検索・電子申請機能における措置> ・サービス検索・電子申請機能へアクセスできる端末を制限する。 ・LGWAN接続端末から紙帳票の打ち出しや、ダウンロードはせず、外部記録媒体等への保存も行わない。 <申請管理システムにおける措置> ・業務目的以外にファイルを利用してはならないことを研修により指導する。	事前	個人住民税申告の電子化に伴う変更
令和7年10月8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)特別区民税・都民税賦課情報ファイル 3. 特定個人情報の使用 リスク4:特定個人情報が不正に複製されるリスク リスクに対する措置の内容	(追加)	<サービス検索・電子申請機能における措置> ・サービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータについて、改ざんや業務目的以外の複製を禁止するルールを定め、ルールに従って業務を行う。 ・LGWAN接続端末から紙帳票の打ち出しや、ダウンロードはせず、外部記録媒体等への保存も行わない。 <申請管理システムにおける措置> 申請データは、外部記憶媒体に書き出せない仕組みとなっており、不正に複製することはできない。	事前	個人住民税申告の電子化に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8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)特別区民税・都民税賦課情報ファイル 6. 情報提供ネットワークシステムとの接続 リスク1: 目的外の手が行われるリスク リスクに対する措置の内容	情報提供許可証	提供許可証	事後	その他の項目の変更であり事前の提出・公表が義務付けられない
令和7年10月8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)特別区民税・都民税賦課情報ファイル 6. 情報提供ネットワークシステムとの接続 リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク リスクに対する措置の内容	<中間サーバー・プラットフォームにおける措置> (中略) ・中間サーバー・プラットフォームの事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。	<中間サーバー・プラットフォームにおける措置> (中略) ・中間サーバー・プラットフォームの事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはできない。	事前	自治体中間サーバー・プラットフォーム更改に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8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)特別区民税・都民税賦課情報ファイル 6. 情報提供ネットワークシステムとの接続 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	<中間サーバー・ソフトウェアにおける措置> ・情報照会機能により、情報提供ネットワークシステムにおける照会許可照会リストを情報提供ネットワークシステムから入手し、中間サーバーにも格納して、情報提供機能により照会許可照会リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ・情報提供機能により、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、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。 ・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。 ・中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。	※該当箇所を参照	事後	その他の項目の変更であり事前の提出・公表が義務付けられない
令和7年10月8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)特別区民税・都民税賦課情報ファイル 6. 情報提供ネットワークシステムとの接続 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	<中間サーバー・プラットフォームにおける措置> ・中間サーバーと既存システム、情報提供ネットワークシステムとの間は高度なセキュリティ対策を維持した行政専用ネットワーク(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。 - 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漏えい・紛失のリスクに対応している。 ・中間サーバー・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセス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。	※該当箇所を参照	事前	自治体中間サーバー・プラットフォーム更改に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8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)特別区民税・都民税賦課情報ファイル 6. 情報提供ネットワークシステムとの接続 情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	<中間サーバー・プラットフォームにおける措置> (中略) ・特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。	<中間サーバー・プラットフォームにおける措置> (中略) ・特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者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	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年10月8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)特別区民税・都民税賦課情報ファイル 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	<中間サーバー・プラットフォームにおける措置> 中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室管理、有人監視及び施錠管理をすることとしている。また設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 事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。	※該当箇所を参照	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年10月8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)特別区民税・都民税賦課情報ファイル 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	(追加)	<サービス検索・電子申請機能における措置> ・LGWAN接続端末については、業務時間内のセキュリティワイヤー等による固定、操作場所への入退室管理、業務時間外の施錠できるキャビネット等への保管、などの物理的対策を講じている。 ・LGWAN接続端末から紙帳票の打ち出しや、ダウンロードはせず、外部記録媒体等への保存も行わない。 <申請管理システムにおける措置> <台東区における措置>と同様	事前	個人住民税申告の電子化に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8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)特別区民税・都民税賦課情報ファイル 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	<中間サーバー・プラットフォームにおける措置> 中間サーバー・プラットフォームではUTM(コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置)等を導入し、アクセス制御、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。	※該当箇所を参照	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年10月8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)特別区民税・都民税賦課情報ファイル 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	(追加)	<サービス検索・電子申請機能における措置> ・LGWAN接続端末へのウイルス検出ソフトウェア等の導入により、ウイルス定義ファイルの定期的な更新及びウイルスチェックを行い、マルウェア検出を行う。 ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。 <申請管理システムにおける措置> <台東区における措置>と同様	事前	個人住民税申告の電子化に伴う変更
令和7年10月8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)特別区民税・都民税賦課情報ファイル 7. 特定個人情報の保管・消去 リスク2: 特定個人情報が古い情報のまま保管され続けるリスク リスクに対する措置の内容	(追加)	<サービス検索・電子申請機能における措置> LGWAN接続端末は、個人番号付電子申請データの一時保管として使用していない。 <申請管理システムにおける措置> 申請管理システムはサービス検索・電子申請機能から取得したデータの一時保管として使用し、審査等は行わない。	事前	個人住民税申告の電子化に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8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) 特別区民税・都民税賦課情報ファイル 7. 特定個人情報の保管・消去 リスク3: 特定個人情報が消去されずいつまでも存在するリスク 消去手順 手順の内容	(追加)	<サービス検索・電子申請機能における措置> LGWAN接続端末から紙帳票の打ち出しや、ダウンロードはせず、外部記録媒体等への保存も行わない。 <申請管理システムにおける措置> システム上で保管している情報は期間経過後、必要に応じて削除を行う。	事前	個人住民税申告の電子化に伴う変更
令和7年10月8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) 軽自動車税賦課情報ファイル 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	基本4情報	基本5情報	事後	法令改正に伴う変更
令和7年10月8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) 軽自動車税賦課情報ファイル 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 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	基本4情報	基本5情報	事後	法令改正に伴う変更
令和7年10月8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) 軽自動車税賦課情報ファイル 6. 情報提供ネットワークシステムとの接続 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	情報提供許可証	提供許可証	事後	その他の項目の変更であり事前の提出・公表が義務付けられない

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8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）軽自動車税賦課情報ファイル 6. 情報提供ネットワークシステムとの接続 リスク4: 入手の際に特定個人情報に漏えい・紛失するリスクに対する措置の内容	＜中間サーバー・プラットフォームにおける措置＞ （中略） ・中間サーバー・プラットフォームの事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。	＜中間サーバー・プラットフォームにおける措置＞ （中略） ・中間サーバー・プラットフォームの事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはできない。	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年10月8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）軽自動車税賦課情報ファイル 6. 情報提供ネットワークシステムとの接続 情報提供ネットワークシステムとの接続に伴うそのほかのリスク及びそのリスクに対する措置	＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバーと既存システム、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である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。 ・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。 ・中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ・特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。	※該当箇所を参照	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年10月8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）軽自動車税賦課情報ファイル 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損 リスク ⑤物理的対策 具体的な対策の内容	＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室管理、有人監視及び施錠管理をすることとしている。また設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 ・事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。	※該当箇所を参照	事前	自治体中間サーバー・プラットフォーム更改に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8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）軽自動車税賦課情報ファイル 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	<中間サーバー・プラットフォームにおける措置> 中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制御、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。	※該当箇所を参照	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年10月8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）収納情報ファイル 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	基本4情報	基本5情報	事後	法令改正に伴う変更
令和7年10月8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）収納情報ファイル 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 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	基本4情報	基本5情報	事後	法令改正に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8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) 収納情報ファイル 6. 情報提供ネットワークシステムとの接続 リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク リスクに対する措置の内容	<中間サーバー・プラットフォームにおける措置> (中略) ・中間サーバー・プラットフォームの事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。	<中間サーバー・プラットフォームにおける措置> (中略) ・中間サーバー・プラットフォームの事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはできない。	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年10月8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) 収納情報ファイル 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損リスク ⑤ 物理的対策 具体的な対策の内容	<中間サーバー・プラットフォームにおける措置> 中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室管理、有人監視及び施錠管理をすることとしている。また設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 事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。	※該当箇所を参照	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年10月8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) 収納情報ファイル 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損リスク ⑥ 技術的対策 具体的な対策の内容	<中間サーバー・プラットフォームにおける措置> 中間サーバー・プラットフォームではUTM(コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置)等を導入し、アクセス制御、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。	※該当箇所を参照	事前	自治体中間サーバー・プラットフォーム更改に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年10月8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)滞納整理情報ファイル 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	基本4情報	基本5情報	事後	法令改正に伴う変更
令和7年10月8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)滞納整理ファイル 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 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	基本4情報	基本5情報	事後	法令改正に伴う変更
令和7年10月8日	Ⅳその他のリスク対策 1. 監査 ②監査 具体的な内容	＜中間サーバー・プラットフォームにおける措置＞ 運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。	※該当箇所を参照	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年10月8日	Ⅳその他のリスク対策 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＞ 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。	※該当箇所を参照	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年10月8日	Ⅵ評価実施手続 1. 基礎項目評価 ①実施日	令和7年1月10日	令和7年8月31日	事後	特定個人情報保護評価に関する規則第14条に基づく定期的な見直しによる変更