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
31	地方税の賦課徴収に関する事務　全項目評価書

個人のプライバシー等の権利利益の保護の宣言

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

特記事項	

評価実施機関名

東京都知事

個人情報保護委員会　承認日 【行政機関等のみ】

公表日

令和7年9月26日

［令和7年5月　様式4］

項目一覧

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

Ⅰ　基本情報

1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	地方税の賦課徴収に関する事務
②事務の内容　※	地方税の賦課徴収に関する事務は、地方税法等の法令に従い、以下の13業務で構成されている。 各業務の詳細については、「別紙1_事務の内容」に記載する。 1　あて名管理業務 2　個人事業税賦課業務 3　不動産取得税賦課業務 4　自動車税賦課業務 5　固定資産税・都市計画税（土地・家屋）賦課業務 6　固定資産税（償却資産）賦課業務 7　事業所税賦課業務 8　都民税三割賦課業務 9　軽油引取税賦課業務 10 諸税賦課業務 11 収入管理業務 12 滞納整理業務 13 情報連携業務
③対象人数	[　　30万人以上　　]　＜選択肢＞ 1）1,000人未満　　2）1,000人以上1万人未満 3）1万人以上10万人未満　　4）10万人以上30万人未満 5）30万人以上

2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	税務総合支援システム
②システムの機能	・職員等による税務情報のオンライン入力及び登録 ・課税データ等の一括更新処理 ・税務データ保存、帳票データ作成 ・外部からのデータ取込み（外部連携機能） ・外部へのデータ出力（外部連携機能） ・出力する書類の電子帳票化機能 ・申告書等税務業務情報の保存（電子書庫機能） ・税務業務の電子決裁（電子決裁機能） ・スキャニングデータのテキストデータ（CSV）への変換及び修正機能（AI-OCR機能） ・共通システムによる公簿等照会機能 ・モバイル端末へのデータ移行、モバイル端末上での税務情報の表示
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　（地方税ポータルシステム（eLTAX）、審査システム（eLTAX）、国税連携システム（eLTAX）、団体内統合利用番号連携サーバー、国税データ閲覧機能、地方税外部連携システム（eLTAX）、eLTAX電子納税通知システム（eLTAX））
システム2～5	
システム2	
①システムの名称	審査システム（eLTAX）
②システムの機能	・地方税法等に明文規定を有する申告・申請等データの受領（地方税ポータルシステム（eLTAX）経由） ・税務総合支援システムとの特定通信を経由した連携 ・申告データ、利用届出データを他システムへ出力 ・プレ申告書データを償却資産所有者へ送信（地方税ポータルシステム（eLTAX）経由） ・本人確認用データを地方税ポータルシステム（eLTAX）へ送信
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　（地方税ポータルシステム（eLTAX））

システム3	
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	・所得税申告書等データの受領 ・他道府県への所得税申告書等データの送付 ・所得税申告書等データの保存 ・媒体による外部へのデータ出力 ・所得税申告書等データの閲覧、印刷 ・国税及び地方税間の照会・回答
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　（ 地方税ポータルシステム（eLTAX）　）

システム4	
①システムの名称	住民基本台帳ネットワークシステム
②システムの機能	・本人確認情報の更新・管理 ・全国サーバーに対する更新通知 ・本人確認の情報抽出・出力 ・全国サーバーへの情報照会
③他のシステムとの接続	[○] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [　] その他　（　）

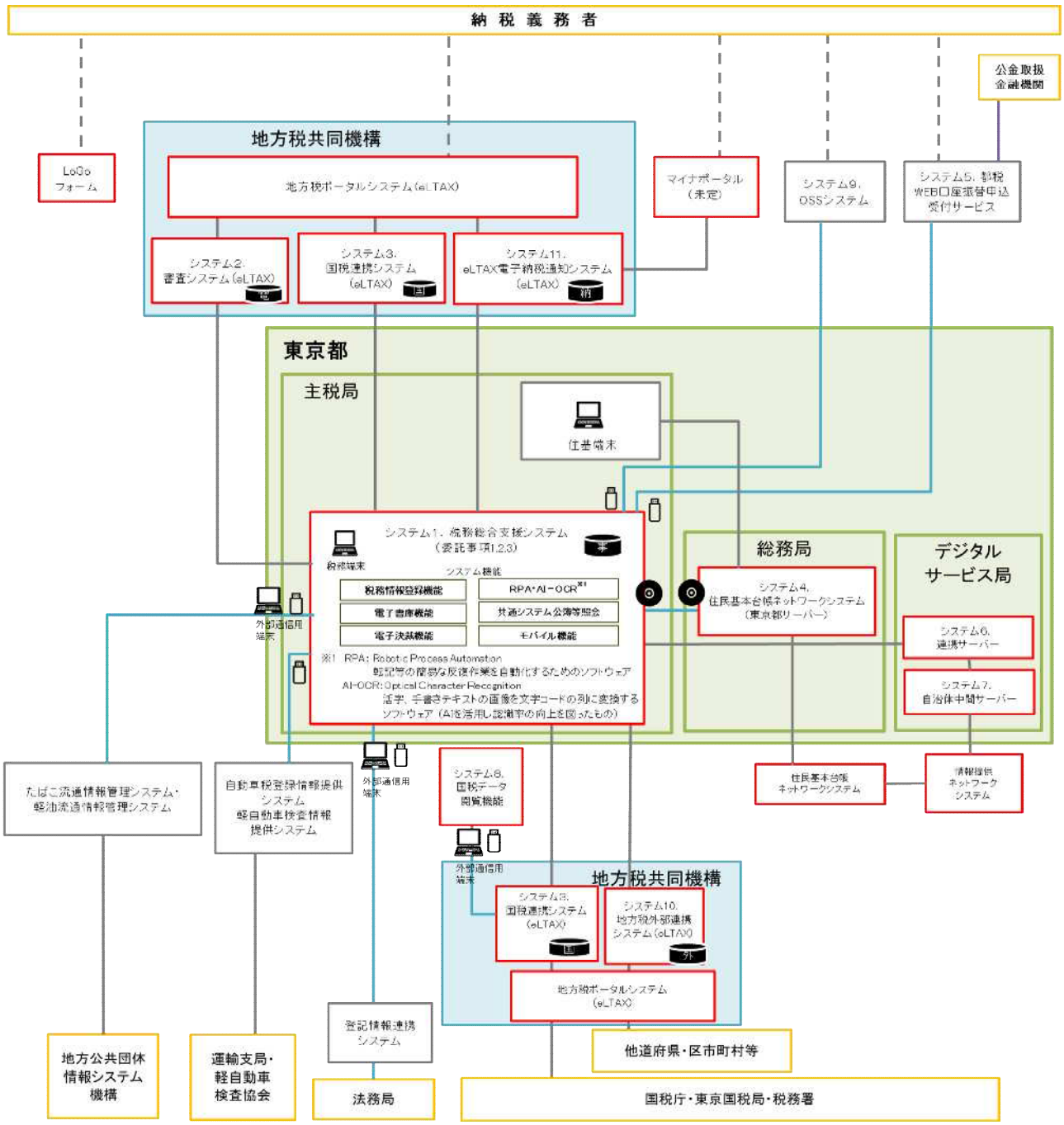
システム5	
①システムの名称	都税WEB口座振替申込受付サービス
②システムの機能	・パソコン・スマートフォンでの口座振替申込受付 ・金融機関への口座照会・登録依頼 ・上記登録結果を税務総合支援システムへ送付する
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [　] その他　（　）

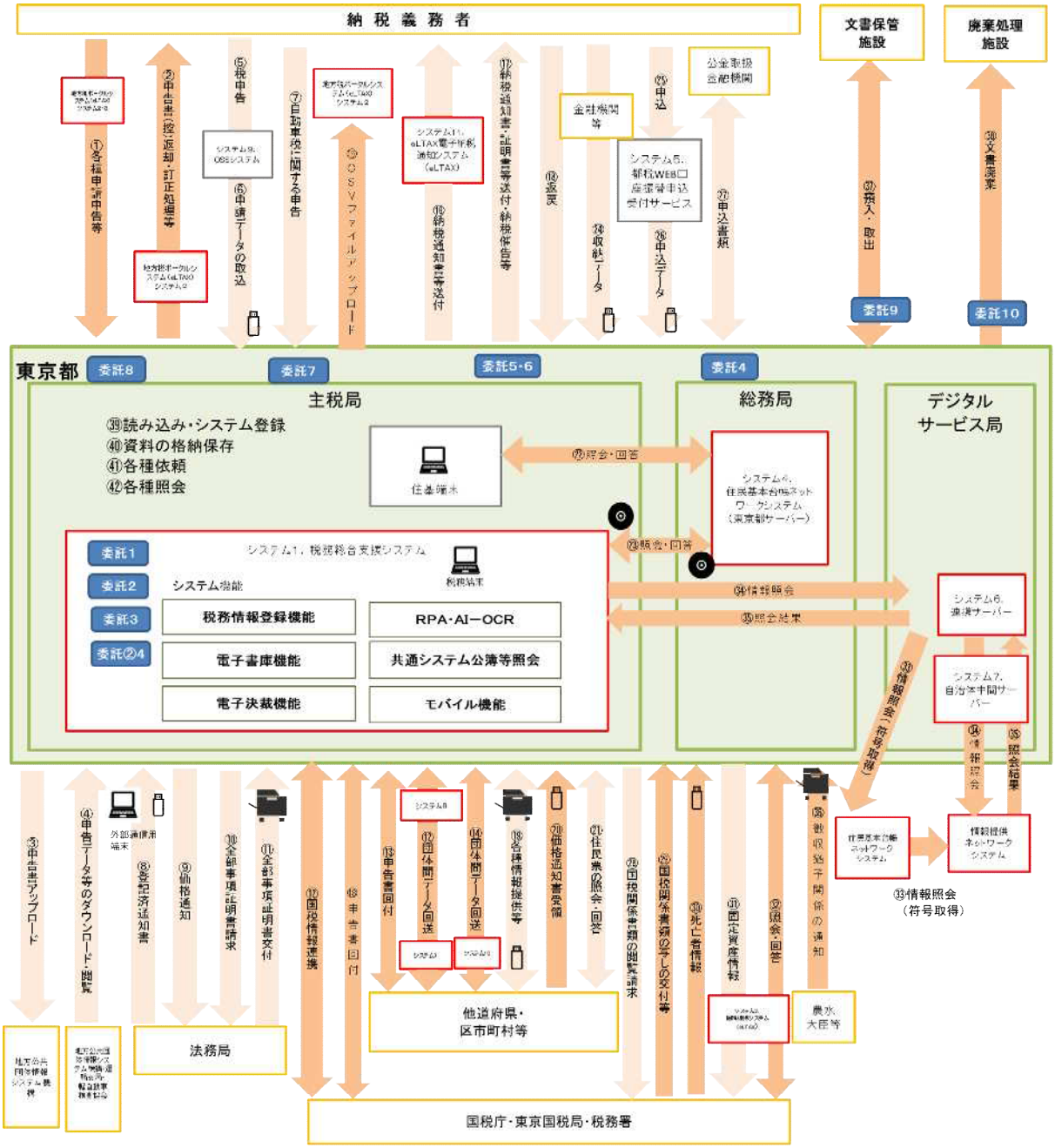
システム6～10	
システム6	
①システムの名称	団体内統合利用番号連携サーバー（以下、「連携サーバー」という。）
②システムの機能	・自治体中間サーバーへの符号取得要求の仲介 ・団体内統合利用番号の取得、管理 ・符号、団体内統合利用番号、個別業務システム利用番号の紐付管理 ・副本登録における、個別業務システムから自治体中間サーバーへの登録要求の仲介 ・情報照会における、個別業務システムからの照会要求の受付及び自治体中間サーバーと税務総合支援システムとの情報授受の仲介
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[○] 税務システム [○] その他　（ 自治体中間サーバー　）
システム7	
①システムの名称	自治体中間サーバー
②システムの機能	・符号及び団体内統合利用番号の取得、管理 ・符号、団体内統合利用番号の紐付管理 ・副本管理 ・情報照会の受付及び管理 ・情報提供管理
③他のシステムとの接続	[○] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [○] その他　（ 連携サーバー　）
システム8	
①システムの名称	国税データ閲覧機能
②システムの機能	・所得税申告書等データの取り込み ・所得税申告書等データの保存（7年分） ・所得税申告書等データの閲覧、印刷 （国税連携システムでの保存可能容量が最大1年分のため、容量を超えた年分を参照する目的として使用）
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　（ 地方税ポータルシステム（eLTAX）、国税連携システム（eLTAX）　）
システム9	
①システムの名称	OSSシステムワンストップサービスシステム（以下、「OSS システム」という。）
②システムの機能	・オンラインサービスの提供（申告書データの入力、提出） ・税務総合支援システムへのデータ送付
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [　] その他　（　）

システム10	
①システムの名称	地方税外部連携システム（eLTAX）
②システムの機能	地方税外部連携システム（eLTAX）は次の3つの機能により構成される。 ・団体間回送機能：地方団体間で提携様式にてデータ連携を行う機能。 ・法人税情報連携機能：国税庁から連携される法人税申告関連データを地方団体へ連携する機能 ・団体間照会・ファイル送信機能：地方団体間で必要となる様々な照会業務を想定し、対象手続を定めずにデータ授受可能な機能
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　（ 地方税ポータルシステム（eLTAX）　　）
システム11～15	
システム11	
①システムの名称	eLTAX電子納税通知システム
②システムの機能	予め申請があった納税義務者に対して、eLTAXを経由して電子的に納税通知書の副本を送付する。（令和10年4月1日以降、実装予定。） ・マイナポータルから提供される電子通知希望申請の電子データをeLTAX電子納税通知システムで受信する。 ・受信した電子通知希望申請の電子データについて、システム登録を行い、税務総合支援システムへ送信する。 ・税務総合支援システムから送付された副本データについて、システム登録を行い、納税義務者に対して通知する。
③他のシステムとの接続	[　　] 情報提供ネットワークシステム　　[　　] 庁内連携システム [　　] 住民基本台帳ネットワークシステム　　[　　] 既存住民基本台帳システム [　　] 宛名システム等　　[○] 税務システム [○] その他　（ 地方税ポータルシステム（eLTAX）、マイナポータル（予定）　　）
3. 特定個人情報ファイル名	
①賦課徴収事務ファイル　②国税連携ファイル　③電子申告ファイル　④eLTAX電子納税通知システムファイル　⑤地方税外部連携ファイル（仮称）	
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	地方税法に基づき、適正かつ公正に賦課徴収を行うため、必要な範囲の特定個人情報を保有する。
②実現が期待されるメリット	税目間における確実な名寄せにより、適正かつ公正な賦課徴収が実現するとともに、手続き簡素化による納税者サービスの向上を図ることができる。
5. 個人番号の利用　※	
法令上の根拠	・番号法第9条第1項　別表24及び135 ・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別表の主務省令で定める事務を定める命令第16条 ・公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律第2条第2項
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[　　実施する　　]　　＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	番号法第19条第8号に基づく主務省令第2条の表49の項

7. 評価実施機関における担当部署	
①部署	東京都主税局 総務部システム管理課、課税部計画課、課税部課税指導課、課税部法人課税指導課、資産税部固定資産税課、資産税部固定資産評価課、徴収部計画課、徴収部徴収指導課
②所属長の役職名	システム管理課長、システム改善担当課長、自動車税担当課長、課税指導課長、法人課税指導課長、固定資産税課長、固定資産評価課長、計画課長（徴収部）、滞納整理対策担当課長
8. 他の評価実施機関	
―	

（別添1）事務の内容


納税義務者
公金取扱金融機関
LoGo フォーム
地方税共同機構
地方税ポータルシステム（eLTAX）
システム2. 審査システム（eLTAX）
システム3. 国税連携システム（eLTAX）
システム11. eLTAX電子納税通知システム（eLTAX）
マイナポータル（未定）
システム9. OSSシステム
システム5. 軽油WEB口座振替申込受付サービス
東京都
主税局
住基端末
システム1. 税務総合支援システム（委託事項1,2,3）
税務端末
システム機能
税務情報登録機能
RPA・AI－OCR※1
電子書庫機能
共通システム公簿等照会
電子決裁機能
モバイル機能
※1 RPA: Robotic Process Automation 転記等の際限な反復作業を自動化するためのソフトウェア
AI-OCR: Optical Character Recognition 活字、手書きテキストの画像を文字コードの列に変換するソフトウェア（AIを活用し認識率の向上を図ったもの）
外部通信用端末
総務局
システム4. 住民基本台帳ネットワークシステム（東京都サーバー）
デジタルサービス局
システム6. 連携サーバー
システム7. 自治体中間サーバー
たばこ流通情報管理システム・軽油流通情報管理システム
自動車税登録情報提供システム 軽自動車検査情報提供システム
外部通信用端末
システム8. 国税データ閲覧機能
住民基本台帳ネットワークシステム
情報提供ネットワークシステム
外部通信用端末
地方税共同機構
システム3. 国税連携システム（eLTAX）
システム10. 地方税外部連携システム（eLTAX）
地方税ポータルシステム（eLTAX）
登記情報連携システム
他道府県・区市町村等
地方公共団体情報システム機構
運輸支局・軽自動車検査協会
法務局
国税庁・東京国税局・税務署
【凡例】
委託1：税務総合支援システムアプリケーション保守委託　委託2：税務総合支援システム運用委託　委託3：：基盤（サーバー類）賃借・保守委託
組織の名称等 ：東京都以外
システムNo システム名 ：システム等（特定個人情報を含まない）
システムNo システム名 ：システム等（特定個人情報を含む）
端末
外部記録媒体
事 ：賦課徴収事務ファイル
電 ：電子申告ファイル
国 ：国税連携ファイル
納 ：デジタル納税通知システム事務ファイル
外 ：地方税外部連携ファイル
：インターネット
：専用線・閉域ネットワーク
：外部記録媒体による接続
：MPN


納税義務者
文書保管施設
廃棄処理施設
①各種申請・申告等
②申告書(控)返却・訂正処理等
⑤税申告
⑥申請データの取込
⑦自動車税に関する申告
⑧OCSVファイルアップロード
⑨申込
⑩申込データ
⑪申込書類
⑫返戻
⑬納税通知書・証明書等送付・納税催告等
⑭納税通知書等送付
⑮収入・取出
⑯文書廃棄
委託9
委託10
東京都
委託8
委託7
委託5・6
委託4
主税局
総務局
デジタルサービス局
㊴読み込み・システム登録
㊵資料の格納保存
㊶各種依頼
㊷各種照会
㉑照会・回答
㉒照会・回答
㉓情報照会
㉔照会結果
㉕情報照会(符号取得)
㉖情報照会
㉗照会結果
㉘情報照会
(符号取得)
委託1
委託2
委託3
委託②4
システム1、税務総合支援システム
システム機能
税務情報登録機能
RPA・AI－OCR
電子書庫機能
共通システム公簿等照会
電子決裁機能
モバイル機能
③申告書アップロード
④申告データ等のダウンロード・閲覧
⑨価格通知
⑩全部事項証明書請求
⑪全部事項証明書交付
⑫国税情報連携
⑬申告書回付
⑭団体間データ回送
⑮各課情報提供等
⑰住民票の照会・回答
⑱国税関係書類の閲覧請求
⑲国税関係書類の写しの交付等
⑳死亡者情報
㉛固定資産情報
㉜照会・回答
㉝徴収猶予関係の通知
㉞価格通知書受領
他道府県・区市町村等
法務局
農水大臣等
国税庁・東京国税局・税務署
【凡例】
委託1：税務総合支援システムアプリケーション保守委託
委託2：税務総合支援システム運用委託
委託3：基盤(サーバー類)賃借・保守委託
委託4：口座振替業務委託
委託5：納税慫慂(しょうよう)業務委託
委託6：還付業務委託
委託7：都税総合事務センター業務委託
委託8：償却資産申告書等処理業務委託
委託9：文書保存箱保管等委託
委託10：都税事務所等保管文庫の溶解処理に係る文書保存箱の運搬・溶解処理委託
委託②4：国税連携データ保存・検索閲覧サービス提供業務委託
組織の名称等：東京都以外
システムNo. システム名：システム等(特定個人情報を含まない)
システムNo. システム名：システム等(特定個人情報を含む)
：特定個人情報の流れ
：特定個人情報以外の情報の流れ
端末
外部記録媒体
スキャナ
※外部記録媒体は情報を取り込む側に図示している

（備考）

※ファイル②～⑤は各事務のためにファイル①から必要な項目を抽出し、各システムで使用する。

1納税者からの申告及び課税事務

①納税義務者等から窓口や郵送によって各種申請・申告書等を受領する。また、eLTAX（地方税ポータルシステム）（システム2・3経由）やLoGoフォームを通じて電子的に送付される各種申請・申告書を受領する。これらに含まれる情報を基に、税務総合支援システムに住所・氏名・生年月日・個人番号等を登録する。LoGoフォームの申請情報は、税務総合支援システムには連携されていないため、手入力で登録している。なお、固定資産税（償却資産）賦課業務については、委託事項8により、償却資産申告書等の内容の税務総合支援システムの登録を委託している。
②必要に応じ、受付印を押した申告書の控えを納税者に返送または返却する。また、訂正等の依頼や審査結果の通知書等を送付する。これらの事務は、①で電子的に申告された場合はeLTAX（地方税ポータルシステム）（システム2経由）を通じて電子的に送付する。
③諸税賦課業務や軽油引取税賦課業務において、申告書の内容を地方公共団体情報システム機構のたばこ流通情報管理システム・軽油流通情報管理システムにアップロードする。
④自動車税賦課業務において、軽自動車検査情報提供システム（LVIS）から、東京都に定置場を有する軽自動車の軽自動車検査情報について提供を受ける。委託事項2により、税務総合支援システムへの取込を行う。運輸支局から自動車税登録情報提供サービス（※自動車税登録情報提供サービスは地方公共団体情報システム機構所管）を通じて、東京都に定置場を有する自動車の自動車税登録情報について提供を受ける。委託事項2により、税務総合支援システムへの取込を行う。また、地方公共団体情報システム機構のたばこ流通情報管理システム・軽油流通情報管理システムから、他の道府県の申告データについて提供を受け、閲覧する。
⑤自動車税賦課業務において、納税者がシステム9.OSS（ワンストップサービス）システムを利用し、自動車税の申告をする。OSSシステムにて、申告内容の審査を行う（自動審査）。
⑥自動車税賦課業務において、OSSシステムから申告データ（OSS・軽OSS分）が転送される。委託事項2により、税務総合支援システムへの取込を行う。
⑦自動車税賦課業務において、納税者から自動車税の申告書等が提出される。委託事項7により、申告内容の審査を行う。
⑧固定資産税（土地・家屋）賦課業務等において、東京法務局から、登記物件に係る表示及び権利の登記済通知書データを登記情報連携システムで受領する。
⑨固定資産税（土地・家屋）賦課業務において、東京法務局に対し、土地課税台帳又は家屋課税台帳に登録された土地及び家屋の決定した価格についての通知を行う。
⑩滞納整理業務における滞納者の財産調査や法人の所在確認のため、及び、固定資産税（土地・家屋）賦課業務における法人の所在地や物件の登記内容確認のため、法務局に対し、不動産・法人登記事項証明書の交付を請求する。
⑪滞納整理業務・固定資産税（土地・家屋）賦課業務等において、法務局から、不動産・法人登記事項証明書を受領する。紙で受領した登記事項証明書を手入力もしくはスキャンにより、税務総合支援システムに取込を行う。
⑫滞納整理業務において、国税庁・税務署との税務情報の照会・回答について、システム3．国税連携システム(eLTAX)を介して行う。
個人事業税賦課業務において、国税庁・税務署からデータ送信されない申告書等について、税務署において閲覧・複写し、各事務所に配送する。申告書の審査に当たってはシステム8．国税データ閲覧機能も併せて使用し、納税義務者の申告情報等を参照する。
また、他道府県から東京都が課税権を有する所得税確定申告の書類が回送され、東京都から他道府県が課税権を有する所得税確定申告書の書類を回送する。併せて該当の国税データもシステム3．国税連携システム(eLTAX)又はシステム10．地方税外部連携システムを介して、他道府県へ団体間回送する。
⑬諸税賦課業務において、地方団体に国たばこ税・市町村たばこ税の申告書が一括提出された際、当該地方団体にて受け付け、申告先の税務署や区市町村に回付する。
⑭不動産取得税賦課業務等において、市町村が作成する取得通知（不動産の取得の事実や不動産の評価額等の情報が記載されたもの）について、eLTAXのシステム10．地方税外部連携システムにより団体間回送を行う。また、物件に係る詳細情報について、個別に団体間照会を行う。受領した情報については、税務総合支援システムへ取込を行う。
⑮事業所税賦課業務において、特定個人情報ファイル（CSV形式）を、eLTAX（地方税ポータルシステム）へ（システム2経由）アップロードする。アップロード対象は下記ア・イをともに満たすものに限られる。
ア：電子申告の利用届出が提出されている個人事業者
イ：郵送又は来所で申告書を提出し、番号確認及び身元確認ができた個人事業者
⑯固定資産税（土地・家屋、償却資産）賦課業務等において、税務総合支援システム登録情報を基に都税を賦課する。予め申請があった納税義務者には、システム11．eLTAX電子納税通知システム（eLTAX）を経由して電子的に納税通知書（課税明細書、更正（価格）決定通知書及び更正（賦課）決定通知書を含む）及び納付書（以下、納税通知書等という）の副本を送付する。
eLTAX電子納税通知システムファイルにおいて、納税義務者からの申請書の電子データを受信し、副本データを提供する。
⑰・納税通知書等を納税義務者宛てに紙で送付する。
・申請内容を基に発行した証明書や申告書等を紙で送付する。
・電算スケジュールに基づき督促状、還付通知書、口座振替開始（変更）通知書を紙で発付する。
・文書や電話、臨戸により納税催告を行う。なお、委託事項5により、催告のうち電算スケジュールに基づく一括発付及び電話・文書の一部しょうよう業務については委託する。
・委託事項6により、電算スケジュールに基づき、還付業務の一部については委託する。
⑱固定資産税（土地・家屋、償却資産）賦課業務等において、紙で発付した納税通知書等の一部について、納税義務者のもとに送達されずに返戻になる場合がある。
⑲固定資産税（土地・家屋）賦課業務等において、
・特別区に対して、農地台帳作成のための土地台帳情報や災害時のり災証明発行事務のための家屋台帳情報を外部記録媒体に格納して提供する。また、三税協力に基づく区市町村からの照会に対して、必要に応じて土地家屋名寄帳を紙媒体で提供する。
・特別区に対して、必要に応じて、建築計画概要書等の交付を請求し、受領する。
・評価を行う家屋に係る登記申請書等を多摩地域の市町村から紙媒体で受領する。また、多摩地域の市町村に対して、東京都で評価を行った家屋に係る不動産取得税課税における価格を紙媒体で通知する。
・軽自動車税環境性能割（市町村税）については、当分の間、東京都が賦課徴収を行い、その定置場の市区町村へ払い込みを行う。
⑳不動産取得税賦課業務において、市町村が作成する取得通知（不動産の取得の事実や不動産の評価額等の情報が記載されたもの）について、外部記録媒体を用いてデータで受領する。また、物件に係る詳細情報について、個別に照会回答をデータもしくは紙で受

領する。受領した情報については、税務総合支援システムへ取込を行う。
㉑固定資産税（土地・家屋）賦課業務等における納税義務者の居住地が適用要件となる軽減制度の要件確認や納税通知書等の返戻調査等のため、又は滞納整理業務における納税義務者の所在調査等のため、区市町村に対して紙で住民票の申請を行う。
㉒住基ネット端末を用いて、住民基本台帳ネットワークシステムにアクセスし、本人確認情報を照会し、住基ネット端末に表示された本人確認情報に記載された情報を取得する。
㉓あて名管理業務等において、外務記録媒体により、東京都総務局に住民基本台帳ネットワークシステムによる一括照会を依頼し、東京都総務局より住民基本台帳ネットワークシステムによる住基ネット一括照会結果データを取得して、あて名情報との突合を行ったうえで、税務総合支援システムへ登録する。

2納税義務者からの納付
㉔納税者が納付した情報を指定金融機関等が受領する。指定金融機関等は受領したデータを収納データに変換し、東京都へ送付する。
　収納チャネル：都税窓口、金融機関、MPN、コンビニ、クレジット、スマホ、地方税共通納税システム
　収納データ送付：指定金融機関、pufure、地方税共通納税システム
㉕システム5．都税WEB口座振替申込受付サービスにより、インターネットで口座振替の申込を受け付ける。
㉖受付内容に基づき公金取扱金融機関へ照会を行い、口座が確認できた場合は申込内容を外部記録媒体を用いて、税務総合支援システムに取込む。
㉗口座振替に係る納税義務者等からの申請に基づき、公金取扱金融機関へ照会を行い、照会結果を東京都に返送する。なお、委託事項4により、口座振替手続業務の一部を委託する。

3その他賦課徴収のために必要な調査等
㉘固定資産税（償却資産）賦課業務において未捕捉資産・事業者の捕捉及び申告内容の確認調査のため、又は滞納整理業務において滞納者の財産・所得等の状況を調査するため、必要に応じて、税務署に対して国税関係書類の閲覧及び写しの交付を申請する。
㉙㉘の固定資産税（償却資産）賦課業務又は滞納整理業務において申請した内容に基づき、税務署より、国税関係書類の写しを受け取る。
㉚固定資産税（土地・家屋）賦課業務において、東京国税局から、個人番号を含む死亡者情報のCSVファイルが格納された外部記録媒体を受領し、税務総合支援システムに取込を行い、あて名情報と突合する。
㉛突合したあて名情報を基に、固定資産（土地・家屋）システムに登録された固定資産情報をCSVファイルで東京国税局へ提供する。（システム3経由）
㉜税務署より、固定資産税（土地・家屋、償却資産）、自動車税、滞納整理に係る照会について個人番号を含むCSVファイルで受領し、あて名情報との突合を行う。あて名情報から当該事績がある場合は税目等情報を付加してCSVファイルで回答する。また、都税の滞納に係る照会を個人番号を含むCSVファイルで依頼する。該当がある場合は滞納情報が付加されたCSVファイルで回答を受ける。（システム3経由）
㉝「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に関する法律」第21条の2に基づき、初回登録の特定個人情報については、連携サーバ、自治体中間サーバ、情報提供ネットワークシステムを介して住民基本台帳ネットワークシステムへ符号取得依頼を行い、中間サーバに符号を登録する。
㉞「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に関する法律」第19条第8号に基づき、減免申請者に係る特定個人情報及び減免申請並びに公金受取口座に関係する他団体保有情報の照会事項を税務総合支援システムに登録する。照会することについて電子決裁を得た上で、登録した内容を基に照会ファイルをシステムで作成し、外部連携機能を用いてシステム6．デジタルサービス局連携サーバー（以下「連携サーバー」という。）に送信する。連携サーバーは、システム7．自治体中間サーバーに情報提供ネットワーク経由の情報照会依頼を登録する。なお、照会にあたり、連携サーバーを経由して住民基本台帳ネットワークシステムへ符号取得依頼を行い、情報提供ネットワークシステムを経由し、自治体中間サーバーに符号を登録する。
※照会先が庁内の場合は、情報提供ネットワークへの照会を実施せず、自治体中間サーバーに自団体照会情報を照会する。
㉟提供ネットワークシステムは、接続する他機関中間サーバーから必要な情報を取得し、照会結果として自治体中間サーバーに提供する。照会結果は、連携サーバーを経由し、外部連携機能を用いて税務総合支援システムに提供され、各担当者が照会結果を確認する。
※自団体照会情報については、自治体中間サーバーから照会結果が提供され、上記同様の流れで税務総合支援システムに登録される。
㊱農地の生前一括贈与に係る不動産取得税の徴収猶予について、個人番号を含む農地猶予関係通知を紙で受領し、スキャナにて取り込む。

4申告書及び調査資料等の保管及び廃棄
㊲申告書及び調査資料等の文書を文書保管施設に預け入れ、必要に応じて取り出す。（委託事項9）
㊳保存年限を経過した文書を運搬し、委託業者により、溶解処理を行う。（委託事項10）

5税務総合支援システム内で行う処理
㊴紙で受領した申請書・申告書等に記載された情報をスキャナ、AI-OCR等にて取り込む。また、税務総合支援システムに住所・氏名・生年月日等を登録する。なお、一部の登録については委託する。（委託事項4・6・8）
㊵各種申請書を電子書庫に格納・保存し、保存年限経過後に廃棄する。
㊶あて名統合分離、あて名の修正・復活、名寄せ禁止情報登録等の各種依頼を電子決裁システムにより受領し、情報を税務総合支援システムに登録する。
㊷区市町村、税務署、法務局に照会文書を送付し回答文書を受領する。また、金融機関等第三債務者への財産調査を行う。一部の金融機関等への財産調査は電子にて行う。

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賦課徴収事務ファイル		
2. 基本情報		
①ファイルの種類 ※		[　　システム用ファイル　　] ＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　　1,000万人以上　　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※		都税に係る納税義務者、申告義務者及び課税調査対象者
	その必要性	適正・公平な賦課徴収を目的とし、必要な範囲の特定個人情報を保有
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　（　公的給付支給等口座登録簿関係情報　）
	その妥当性	・個人番号：納税義務者情報を正確に管理するために保有 ・個人番号対応符号：対象者を正確に特定するために保有 ・その他識別情報：対象者を正確に特定するために保有 ・5情報及び連絡先：納税義務者を特定するため、連絡するために保有 ・その他住民票関係情報：納税義務者情報を正確に把握するために保有 ・地方税関係情報：都税の賦課徴収を行うため、他道府県との情報連携のため、還付金額清算のために保有 ・国税関係情報：税額決定に際し所得額等を用いて確認するため、還付金額清算のために保有 ・障害者福祉関係情報、生活保護・社会福祉関係情報：賦課事務を適切に行うために保有 ・公的給付支給等口座登録簿関係情報：還付事務を適切行うために保有
	全ての記録項目	別添2を参照。
⑤保有開始日		令和9年1月4日
⑥事務担当部署		東京都主税局 総務部システム管理課、課税部計画課、課税部課税指導課、課税部法人課税指導課、資産税部固定資産税課、資産税部固定資産評価課、徴収部計画課、徴収部徴収指導課

3. 特定個人情報の入手・使用		
①入手元 ※		[○] 本人又は本人の代理人 [○] 評価実施機関内の他部署 （ 総務局、福祉局、デジタルサービス局 ） [○] 行政機関・独立行政法人等 （ 地方税共同機構、国税庁・東京国税局・税務署、法務局、裁判所、運輸支局、農林水産大臣、農業委員会 ） [○] 地方公共団体・地方独立行政法人 （ 区市町村等、道府県 ） [○] 民間事業者 （ 指定金融機関、全国軽自動車検査協会 ） [ ] その他 （ ）
②入手方法		[○] 紙 [○] 電子記録媒体（フラッシュメモリを除く。） [○] フラッシュメモリ [ ] 電子メール [○] 専用線 [○] 庁内連携システム [○] 情報提供ネットワークシステム [○] その他 （ 住民基本台帳ネットワークシステム、地方税ポータルシステム（eLTAX）、国税連携システム（eLTAX）、審査システム、自動車税登録情報提供システム、軽自動車検査情報登録情報提供システム、地方税共通納税システム、pufure、eLTAX電子納税通知システム（eLTAX）、国税データ閲覧機能、地方税外部連携システム（eLTAX） ）
③入手の時期・頻度		別紙2のとおり
④入手に係る妥当性		別紙3のとおり
⑤本人への明示		別紙4のとおり
⑥使用目的 ※		必要範囲の特定個人情報を保有することにより、適正かつ公平な賦課徴収を実現するため。
	変更の妥当性	ー
⑦使用の主体	使用部署 ※	主税局各部、各都税事務所（都税支所を含む）、都税総合事務センター及び各支庁
	使用者数	[1,000人以上] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上

⑧使用方法　※		別紙5のとおり
	情報の突合　※	【共通】 ＜住民票の写し、本人確認情報＞ あて名管理システムに登録されている納税義務者・申告義務者情報（氏名・住所）と、住民票の写し等に記載されている情報を突合（目視による確認）し、現住所が正しいものかを確認する。また、個人番号については、あて名管理システムに登録されている公簿情報と突合（検索）し、あて名割れ等が発生していないかを確認する。 ＜申告書・申請書・通知等＞ あて名管理システムに登録されている納税義務者情報・申告義務者（氏名・住所）と申告書等に記載されている情報を突合（検索）し、システム上のあて名の有無及び適正な申告等であることを確認する。また、必要に応じて、個人番号を利用して、あて名管理システムに登録されている公簿情報と突合（検索）し、申告された氏名・住所等が正しいものかを確認する。 ＜国税連携＞ 地方税共同機構へ電子データを提供する。 【個人事業税】 ＜個人事業税申告書等＞ ・あて名管理システムに登録されている納税義務者・申告義務者情報（氏名・住所）と、住民票の写し等に記載されている情報を突合し、現住所が正しいものかを確認する。 ・申告書等に記載された所得情報等と所得税申告書等情報を突合（目視による確認）し、適正な申告であることを確認する。 【固定資産税（土地・家屋）】 ＜死亡者情報＞ あて名管理システムに登録されている納税義務者情報（個人番号又は氏名・住所）と、死亡者情報の情報をシステム上で突合（検索）し、システム上に存在するあて名であるかどうかを確認する。 【収入管理】 ＜収納データ＞ 金融機関等から入手した収納データと課税徴収マスタを突合し、納税者の収入管理を行う。 ＜公金受取口座＞ あて名管理システムに登録されている納税義務者情報（住所、氏名等）と請求書兼口座振替依頼書を突合し、 情報提供ネットワークシステムに対して公金受取口座情報の照会を行うべきかを確認する。 【情報連携】 ＜身体・精神障害者手帳及び障害の程度に関する情報、生活保護実施関係情報＞ 入手した身体・精神障害者手帳及び障害の程度に関する情報、生活保護実施関係情報と減免申請書を突合する。
	情報の統計分析　※	個人を特定することなく、統計分析を行う。
	権利利益に影響を与え得る決定　※	賦課決定、減免決定
⑨使用開始日		令和9年1月4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 （ 10 ） 件
委託事項1		税務総合支援システムアプリケーション保守委託
①委託内容		税務総合支援システムの仕様変更、障害対応等 ※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] ＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[1,000万人以上] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	都税に係る納税義務者、申告義務者及び課税調査対象者
	その妥当性	税務総合支援システムの安定的な稼働のため、データの修正やシステムの異常終了時の対応などを行う上で特定個人情報ファイルを取り扱う必要がある。
③委託先における取扱者数		[10人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表予定。
⑥委託先名		未定
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	再委託する場合は、委託元は委託先に対してあらかじめ再委託を行う旨を書面により提出させ、委託元が承諾を与える。
	⑨再委託事項	未定

委託事項2～5		
委託事項2		税務総合支援システム運用委託
①委託内容		税務総合支援システム（情報連携サーバーを含む。）の稼働に必要な機能の提供　※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体]　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[1,000万人以上]　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲　※	都税に係る納税義務者、申告義務者及び課税調査対象者
	その妥当性	特定個人情報ファイルが含まれる税務総合支援システムの運用管理を行うために取扱う必要がある。
③委託先における取扱者数		[10人未満]　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○] 専用線　[ ] 電子メール　[ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ　[ ] 紙 [ ] その他　（　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表予定。
⑥委託先名		未定
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	再委託する場合は、委託元は委託先に対してあらかじめ再委託を行う旨を書面により提出させ、委託元が承諾を与える。
	⑨再委託事項	未定

委託事項3		基盤（サーバー類）賃借・保守委託
①委託内容		税務総合支援システムの稼働に必要なサーバー類の提供　※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体]　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[1,000万人以上]　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲　※	都税に係る納税義務者、申告義務者及び課税調査対象者
	その妥当性	税務総合支援システムの安定的な稼働のため、運用保守作業を行う上で特定個人情報ファイルを取り扱う必要がある。
③委託先における取扱者数		[10人未満]　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○] 専用線　[　] 電子メール　[　] 電子記録媒体（フラッシュメモリを除く。） [　] フラッシュメモリ　[　] 紙 [　] その他　（　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表予定。
⑥委託先名		未定
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	再委託する場合は、委託元は委託先に対してあらかじめ再委託を行う旨を書面により提出させ、委託元が承諾を与える。
	⑨再委託事項	未定

委託事項4		口座振替業務委託
①委託内容		地方税法に基づき賦課・申告された地方税における納税義務者のうち、固定資産税（土地家屋）、固定資産税（償却）、個人事業税で口座振替を希望する納税者を対象とする口座振替手続業務　※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		［ 特定個人情報ファイルの一部 ］　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	［ 100万人以上1,000万人未満 ］　＜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　※	地方税法に基づき賦課・申告された地方税における納税義務者のうち、口座振替払いの申し出があった対象者
	その妥当性	適正な口座振替手続業務を行うため、税務総合支援システムを使用する必要がある。
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　（ 税務総合支援システムによる特定個人情報ファイルの閲覧 ）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		未定
再委託	⑦再委託の有無　※	［ 再委託しない ］　＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	

委託事項5		納税慫慂(しょうよう)業務委託
①委託内容		地方税法に基づき賦課・申告された地方税における納税義務者のうち、督促状発付後一定期間が経過した者に対しての納税のしょうよう業務(申請による換価の猶予業務を含む) ※項目③「委託先における取扱者数」は未定のため、1)10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの一部]　＜選択肢＞ 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	対象となる本人の数	[10万人以上100万人未満]　＜選択肢＞ 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	地方税法に基づき賦課・申告された地方税における納税義務者のうち、督促状発付後一定期間が経過した者
	その妥当性	納税慫慂(しょうよう)業務を行うため、税務総合支援システムを使用する必要がある。
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 (税務総合支援システム端末による特定個人情報ファイルの閲覧)
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		未定
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6～10		
委託事項6		還付業務委託
①委託内容		地方税法に基づき賦課・申告された地方税において、過誤納金等が発生した納税義務者等に対する還付を行うための業務　※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		［ 特定個人情報ファイルの一部 ］　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	［ 100万人以上1,000万人未満 ］　＜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　※	地方税法に基づき賦課・申告された地方税において、過誤納金等が発生した納税義務者等
	その妥当性	還付業務を行うため、税務総合支援システムを使用する必要がある。
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　（ 税務総合支援システムによる特定個人情報ファイルの閲覧 ）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にてしている。
⑥委託先名		未定
再委託	⑦再委託の有無　※	［ 再委託しない ］　＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	

委託事項7		都税総合事務センター業務委託
①委託内容		自動車税（環境性能割・種別割）申告書の受付、記載事項の定型的な審査及びデータ入力等の窓口業務等　※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		［ 特定個人情報ファイルの一部 ］　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	［ 100万人以上1,000万人未満 ］　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲　※	東京都内に定置場のある自動車を取得し、又は保有している納税義務者及び生計を一にする障害者。
	その妥当性	本委託契約の事務内容は、東京都都税総合事務センター総務課及び自動車税課における申告書照合事務及び住所訂正入力事務等並びに同センター自動車税事務所における自動車税（環境性能割・種別割）の申告受付、納税に係る照会、確認事務等であるため、必要な範囲の特定個人情報ファイルについて取り扱う必要がある。
③委託先における取扱者数		［ 10人未満 ］　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		［　］専用線　［　］電子メール　［　］電子記録媒体（フラッシュメモリを除く。） ［　］フラッシュメモリ　［　］紙 ［ ○ ］その他　（ 税務総合支援システムによる特定個人情報ファイルの閲覧 ）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		未定
再委託	⑦再委託の有無　※	［ 再委託しない ］　＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	

委託事項8		償却資産申告書等処理業務委託
①委託内容		償却資産申告書及び種類別明細書等に記載されている償却資産の評価内容等を、各都税事務所内で税務総合支援システムにオンライン入力を行う。 ※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		［ 特定個人情報ファイルの一部 ］　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	［　10万人以上100万人未満　］　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	固定資産税の納税義務者 ⇒東京都特別区内の固定資産税（償却資産）の所有者（償却資産課税台帳に所有者として登録されている者）
	その妥当性	価格等の固定資産課税台帳への登録を、適正かつ効率的に行うため。
③委託先における取扱者数		［　10人未満　］　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		［　］専用線　［　］電子メール　［　］電子記録媒体（フラッシュメモリを除く。） ［　］フラッシュメモリ　［ ○ ］紙 ［　］その他　（　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		未定
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9		文書保存箱保管等委託
①委託内容		(1)文書の保管 (2)文書の配送、引取り及びそれに伴う入出庫作業 (3)文書の廃棄 ※項目③「委託先における取扱者数」は未定のため、1)10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの一部] ＜選択肢＞ 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	対象となる本人の数	[1,000万人以上] ＜選択肢＞ 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	都税に係る納税義務者、申告義務者及び課税調査対象者
	その妥当性	東京都文書管理規則第44条に基づき、特定個人情報ファイルを含む文書等のうち、保存期間が終了していないものについて保管するために委託する必要がある。
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 ( )
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		未定
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	再委託する場合は、委託元は委託先に対してあらかじめ再委託を行う旨を書面により提出させ、委託元が承諾を与えている。
	⑨再委託事項	・文書の配送、引取り及びそれに伴う入出庫作業 ・文書の廃棄

委託事項10		都税事務所等保管文書の溶解処理に係る文書保存箱の運搬・溶解処理委託
①委託内容		各都税事務所、都税総合事務センター及び徴収部納税推進課の文書保存箱を運搬し、溶解処理工場において溶解槽への投入作業を実施する。 ※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの一部]　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[1,000万人以上]　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲　※	都税に係る納税義務者、申告義務者及び課税調査対象者
	その妥当性	東京都文書管理規則第53条及び第56条に基づき、特定個人情報ファイルを含む文書等のうち、保存期間が終了したものについて廃棄場所へ運搬・廃棄するために委託する必要がある。
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　（　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		未定
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　（ 3 ）件　[　]移転を行っている　（　）件 [　]行っていない

提供先1	道府県
①法令上の根拠	番号法第19条第10号　番号法施行令第21条　地方税法第72条の59
②提供先における用途	個人事業税の賦課徴収
③提供する情報	都内に事務所、事業所がなく他道府県に課税権がある個人事業税の納税義務者及び調査対象者の所得税申告書等データ
④提供する情報の対象となる本人の数	[　　1万人未満　　]　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	都内に事務所、事業所がなく他道府県に課税権がある個人事業税の納税義務者及び調査対象者
⑥提供方法	[　]情報提供ネットワークシステム　　[　]専用線 [　]電子メール　　[　]電子記録媒体（フラッシュメモリを除く。） [　]フラッシュメモリ　　[○]紙 [○]その他　（ 国税連携システム（eLTAX）、地方税外部連携システム（eLTAX）　）
⑦時期・頻度	都内に事務所、事業所がなく他の道府県が賦課する者であったことが判明した場合に随時提供する。
提供先2～5	
提供先2	国税庁
①法令上の根拠	地方税法第72条の55の2第1項、第72条の59第1項
②提供先における用途	東京都に閲覧させる資料の選定
③提供する情報	所得税申告書等データ
④提供する情報の対象となる本人の数	[　　1万人未満　　]　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	東京都に課税権がある個人事業税の納税義務者及び調査対象者
⑥提供方法	[　]情報提供ネットワークシステム　　[○]専用線 [　]電子メール　　[　]電子記録媒体（フラッシュメモリを除く。） [　]フラッシュメモリ　　[　]紙 [　]その他　（　　）
⑦時期・頻度	国税連携システムにて一括でデータ送信を受けたものだけでは審査ができず、国税に追加の資料要求を行う都度発生する。

提供先3	税務署、区市町村
①法令上の根拠	所得税法等の一部を改正する法律（平成30年法律第7号）附則第51条第3項及び地方税法等の一部を改正する法律（平成30年法律第3号）附則第23条第4項等の規定により、国のたばこ税等手持品課税の申告書と区市町村のたばこ税等手持品課税の申告書を合わせて都道府県に提出した場合は、該当する税務署及び区市町村に対して申告されたものとみなされる。 また、「道府県たばこ税及び市町村たばこ税の税率の引上げに伴う手持品課税の取扱いについて」（平成30年6月25日付総税市第49号総務省自治税務局市町村税課長通知）により、都に併せて提出された国のたばこ税等手持品課税申告書と区市町村のたばこ税等手持品課税の申告書は、受理後速やかに税務署又は区市町村に回付することとなっている。
②提供先における用途	国と区市町村のたばこ税等手持品課税の賦課徴収
③提供する情報	都に提出された国と区市町村のたばこ税等手持品課税の申告書情報
④提供する情報の対象となる本人の数	[　　1万人未満　　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	国と区市町村のたばこ税等手持品課税の納税義務者
⑥提供方法	[　] 情報提供ネットワークシステム　　[　] 専用線 [　] 電子メール　　[　] 電子記録媒体（フラッシュメモリを除く。） [　] フラッシュメモリ　　[○] 紙 [　] その他　（　　）
⑦時期・頻度	毎月
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 ※		【税務総合支援システム（サーバー）】 ・特定個人情報を保管するデータセンタは、都市計画法における防火・準防火地域に指定されていること、サーバ室等へ滞りなく電力を供給できる電源設備及び非常用自家発電設備を備えていること等の防災性を重視した条件により、選定している。 ・データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際してはICカード及び静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。 【紙媒体】 ・文書等の取扱いに関する規定に基づき、施錠された書庫に保管している。 ・文書の預入れを行う場合の保管倉庫は、地盤が強固で、海抜が高く、河川、池沼、運河、ため池等に隣接せず、近隣に危険物貯蔵倉庫及び工場がなく、人口及び建築物の密集地域ではない場所に建設している。 ・上記保管倉庫は、専用保管庫として設計された耐震・耐火構造を備えた堅固な建築物であり、外部からの侵入を防ぐための人的及び施設的管理体制（警備員による警備、監視カメラ、警報装置、赤外線センサー等）を備え、入退室は権限のある者のみ可能とし、入退室の記録をとり、一定期間保管している。 【中間サーバー・プラットフォーム】 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。 【外部記録媒体】 ・外部記録媒体は、施錠された保管庫に保管している。 【連携サーバー】 ・サーバー等を設置するための専用施設内に他のシステムとは分離した区画を設け、当該サーバー専用のラックに施錠して収容する。当該施設では、入退室者管理、区画ごとの施錠管理、監視カメラによる録画、有人監視等を実施する。 ・当該施設の煙感知装置、ガス系消火設備、耐震対応等により、火災や地震に起因する滅失等のリスクを低減する。
②保管期間	期間	[　6年以上10年未満　]　＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	文書等の取扱いに関する規定の保存期間に基づき保管しておく必要がある。

③消去方法	【紙媒体】 廃棄等に関する規定に基づき、保存期間経過後、職員の立会いのもとで溶解等により廃棄を行っている。運搬・廃棄にあたっては、委託先から適切に処理する旨の誓約書を徴取している。また、廃棄後にすべての書類等を廃棄したことを示す溶解証明を徴取している。 【中間サーバー・プラットフォーム】 ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの保守・運用を行う事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度（ISMAP）に準拠したデータの暗号化消去及び物理的破壊を行う。さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ③中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。 【連携サーバー】 特定個人情報（副本相当）は、提供・移転の都度、中継されるのみであり、税務総合支援システムの取得後に消去し、且つ一定期間内に自動で消去する。 なお、機器のうち特定個人情報等のデータが記録されうるものの廃棄等に当たっては、磁気的消去又は物理的破壊等により、当該データを復元不可能な状態とする。 【税務総合支援システム（サーバー）】 一定期間経過後、バッチ処理により削除する。 また、機器リース期間満了時には特定個人情報等のデータを全て消去の上、消去結果について、記録媒体ごとに、消去した情報項目、数量、消去方法及び消去日等を明示した書面で委託事業者より報告を受けている。 【外部記録媒体】 ・データ授受後、直ちに保存データを削除することとしている。 ・保管している外部記録媒体が不要となった場合は、当該外部記録媒体内部の情報を復元できないように消去した上で廃棄する。

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国税連携ファイル		
2. 基本情報		
①ファイルの種類 ※		[　　システム用ファイル　　] ＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　　1,000万人以上　　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※		国税庁に対して申告を行った者で、都税の賦課徴収の納税義務者と想定される者
	その必要性	適正かつ公平な賦課を目的とし、必要な範囲の特定個人情報を保有するため。
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	・個人番号及びその他の識別情報：対象者を正確に特定するために保有 ・5情報及び連絡先：①課税対象者の認定に際し在住要件を確認するため、②本人への通知等送付及び連絡等のために保有 ・国税関係情報：租税の賦課徴収及び国税との情報連携のために保有 ・地方税関係情報：租税の賦課徴収及び他道府県との情報連携のために保有
	全ての記録項目	別添2を参照。
⑤保有開始日		平成28年１月
⑥事務担当部署		主税局総務部システム管理課

3. 特定個人情報の入手・使用		
①入手元 ※		[　　] 本人又は本人の代理人 [　　] 評価実施機関内の他部署　（　　） [○] 行政機関・独立行政法人等　（ 国税庁・税務署　　） [○] 地方公共団体・地方独立行政法人　（ 他の道府県　　） [　　] 民間事業者　（　　） [　　] その他　（　　）
②入手方法		[　　] 紙　[　　] 電子記録媒体（フラッシュメモリを除く。）　[　　] フラッシュメモリ [　　] 電子メール　[○] 専用線　[　　] 庁内連携システム [　　] 情報提供ネットワークシステム [　　] その他　（　　）
③入手の時期・頻度		【国税庁・税務署からの電子データでの入手】 ・国税当局に提出された個人番号が記載された所得税申告書等情報を地方税ポータルシステム（eLTAX）を通じてデータで定期的に受信している。 ・2～5月の繁忙期は休日を除くほぼ毎日受信。 ・6～1月は月1回受信。 【照会・回答情報】 国税連携システムで受信した照会・回答情報データを税務総合支援システムに取込み入手する。取込みは随時実施する。
④入手に係る妥当性		【所得税申告書等】 地方税法の規定により国税庁・税務署へ所得税の申告等をしたものは道府県知事（都知事）へ個人事業税の申告もしたものとみなされることから、国税庁・税務署より所得税申告書等をデータにて入手する。なお、他道府県も同規定に基づき国税庁・税務署からデータを入手するとともに事務所、事業所の所在地が都であることが判明した場合は都へデータを回送し入手している。 【照会・回答情報】 地方税法第20条の11及び国税徴収法146条の2の規定により、地方税及び滞納処分に関する調査について必要があるときは、事業者（特別の法律により設立された法人を含む。）又は官公署に、当該調査に関し参考となるべき簿書及び資料の閲覧又は提供その他の協力を求めることができることから、国税庁・税務署より照会・回答情報のデータを入手する。
⑤本人への明示		【所得税申告書等】 地方税法の規定により国税庁・税務署へ所得税の申告等をしたものは道府県知事（都知事）へ個人事業税の申告がされたものみなすことが規定されており、国税関係書類の入手を行っている。 【照会・回答情報】 地方税法第20条の11及び国税徴収法146条の2の規定の規定により、事業者又は官公署への簿書及び資料の閲覧又は提供その他の協力を求めることができるとされている。
⑥使用目的 ※		適正かつ公平な賦課及び徴収を実現するため。
	変更の妥当性	―
⑦使用の主体	使用部署 ※	主税局各部、各都税事務所（都税支所を含む）、都税総合事務センター及び各支庁
	使用者数	[　1,000人以上　] ＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
⑧使用方法 ※		【所得税申告書等】 国税連携システムで受信した所得税申告書等データを税務総合支援システムに取込み、申告書等関係書類の情報と併せて審査し、課税処理等のシステム登録を行う。 【照会・回答情報】 ・国税連携システムで受信した照会情報データを税務事務総合支援システムに取込み、あて名情報との突合を行う。 ・財産差押等滞納処分のためシステム登録を行う。

	情報の突合 ※	【所得税申告書等、照会・回答情報】 ・あて名管理システムに登録されている納税義務者情報（氏名・住所）と入手した所得税申告書等に記載及び記録されている情報を突合（検索）し、システム上に存在するあて名であるかどうかを確認する。
	情報の統計分析 ※	個人を特定することなく、統計分析を行う。
	権利利益に影響を与え得る決定 ※	賦課決定
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		税務総合支援システムアプリケーション保守委託
①委託内容		税務総合支援システムの仕様変更、障害対応等 ※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] ＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[1,000万人以上] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	都税に係る納税義務者、申告義務者及び課税調査対象者
	その妥当性	税務総合支援システムの安定的な稼働のため、データの修正やシステムの異常終了時の対応などを行う上で特定個人情報ファイルを取り扱う必要がある。
③委託先における取扱者数		[10人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表予定。
⑥委託先名		未定
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	再委託する場合は、委託元は、委託先に対してあらかじめ再委託を行う旨を書面により提出させ、委託元が承諾を与える。
	⑨再委託事項	未定

委託事項2～5		
委託事項2		基盤（サーバー類）賃借・保守委託
①委託内容		税務総合支援システムの稼働に必要なサーバー類の提供　※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		［ 特定個人情報ファイルの全体 ］　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	［　　1,000万人以上　　］　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲　※	都税に係る納税義務者、申告義務者及び課税調査対象者
	その妥当性	税務総合支援システムの安定的な稼働のため、運用保守作業を行う上で特定個人情報ファイルを取り扱う必要がある。
③委託先における取扱者数		［　　10人未満　　］　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		［ ○ ］専用線　［　］電子メール　［　］電子記録媒体（フラッシュメモリを除く。） ［　］フラッシュメモリ　［　］紙 ［　］その他　（　　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表予定。
⑥委託先名		未定
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	再委託する場合は、委託元は、委託先に対してあらかじめ再委託を行う旨を書面により提出させ、委託元が承諾を与える。
	⑨再委託事項	未定

委託事項3		税務総合支援システム運用委託
①委託内容		税務総合支援システム（情報連携サーバーを含む。）の稼働に必要な機能の提供　※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		［ 特定個人情報ファイルの全体 ］　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	［　1,000万人以上　］　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲　※	都税に係る納税義務者、申告義務者及び課税調査対象者
	その妥当性	特定個人情報ファイルが含まれる税務総合支援システムの運用管理を行うために取扱う必要がある。
③委託先における取扱者数		［　10人未満　］　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		［ ○ ］専用線　［　］電子メール　［　］電子記録媒体（フラッシュメモリを除く。） ［　］フラッシュメモリ　［　］紙 ［　］その他　（　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表予定。
⑥委託先名		未定
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	再委託する場合は、委託元は、委託先に対してあらかじめ再委託を行う旨を書面により提出させ、委託元が承諾を与える。
	⑨再委託事項	未定

委託事項4		国税連携データ保存・検索閲覧サービス提供業務委託
①委託内容		国税データ閲覧機能の提供（閲覧用アプリケーション及びサーバーの維持管理） ※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] ＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[100万人以上1,000万人未満] ＜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 ※	所得税申告等を税務署に行った者のうち個人事業税の課税調査の対象となる者 →国税当局に提出される所得税申告書等の税務関係書類に個人番号を記載することとされている者で、都内に事務所、事業所を有する個人が行う事業のうち、地方税法に定められている事業（法定業種）を行っている課税調査対象者
	その妥当性	国税データ閲覧機能の安定的な稼働のため、システムの仕様調整や異常終了時の対応などを行ううえで特定個人情報を取扱う必要がある。
③委託先における取扱者数		[10人未満] ＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○]専用線　[ ]電子メール　[○]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ　[ ]紙 [ ]その他　（　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		未定
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　（　2　）件　[ ]移転を行っている　（　）件 [ ]行っていない

提供先1	他の道府県知事
①法令上の根拠	番号法第19条第10号　番号法施行令第21条　地方税法第72条の59
②提供先における用途	個人事業税の賦課徴収
③提供する情報	都内に事務所、事業所がなく他道府県に課税権がある個人事業税の納税義務者及び調査対象者の所得税申告書等データ
④提供する情報の対象となる本人の数	[　　1万人未満　　]　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	都内に事務所、事業所がなく他道府県に課税権がある個人事業税の納税義務者及び調査対象者
⑥提供方法	[　]情報提供ネットワークシステム　[○]専用線 [　]電子メール　[　]電子記録媒体（フラッシュメモリを除く。） [　]フラッシュメモリ　[　]紙 [　]その他　（　　）
⑦時期・頻度	都内に事務所、事業所がなく他の道府県が賦課する者であったことが判明した場合に随時提供する。
提供先2～5	
提供先2	国税庁
①法令上の根拠	地方税法第72条の55の2第1項、第72条の59第1項、国税徴収法第146条の2、国税通則法第74条の12
②提供先における用途	東京都に閲覧させる資料の選定及び滞納処分に関する調査
③提供する情報	所得税申告書等データ、固定資産税情報及び都市計画税情報、自動車税課税情報、滞納情報（地方税）
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	納税義務者及び調査対象者
⑥提供方法	[　]情報提供ネットワークシステム　[○]専用線 [　]電子メール　[　]電子記録媒体（フラッシュメモリを除く。） [　]フラッシュメモリ　[　]紙 [　]その他　（　　）
⑦時期・頻度	国税連携システムにて一括でデータ送信を受けたものだけでは審査ができず、国税に追加の資料要求を行う都度発生する。 国税庁から照会データの送信がある度、随時提供する。

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

6. 特定個人情報の保管・消去

①保管場所　※		【国税連携システム（サーバー）】 ・特定個人情報を保管するデータセンタは、都市計画法における防火・準防火地域に指定されていること、サーバー室等へ滞りなく電力を供給できる電源設備及び非常用自家発電設備を備えていること等の防災性を重視した条件により、選定している。 ・データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とする等、厳重なセキュリティ対策を行っている。 【国税データ閲覧機能（サーバー）】 特定個人情報を保管するデータセンタは、浸水対策を施した場所に立地していること、データ保管に利用するキャビネット等を耐火仕様にすること、サーバー室等へ滞りなく電力を供給できる電源設備及び停電時にも機器の稼働を止めないための非常用自家発電設備を備えていること等の防災性を重視した条件により選定している。データセンタへの立ち入りはICカード所持者に限られている。また、サーバー室に入るためには、ICカードに加え、パスワード及び指紋認証を必要とする等、厳重なセキュリティ対策を行っている。
②保管期間	期間	[　6年以上10年未満　]　＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	文書等の取扱に関する規定の保存期間に基づき保管しておく必要がある。
③消去方法		【国税連携システム（サーバー）】 ・保存年限を経過した課税データについて、電子データの削除等に関する規定に基づき、職員によるオンライン処理により削除している。 ・機器リース期間満了時には特定個人情報等のデータを全て消去の上、消去結果について、記録媒体ごとに、消去した情報項目、数量、消去方法及び消去日等を明示した書面で委託事業者より報告を受けている。 【国税データ閲覧機能（サーバー）】 契約書により、7年保存するという契約履行完了時には、業務に係る情報を記録した一切の媒体については、記録媒体上に含まれる当該委託業務に係る情報を全て消去して、その消去結果について、記録媒体ごとに、消去した情報項目、数量、消去方法及び消去日等を明示した書面で委託者に報告することが規定されている。

7. 備考

―

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名		
③電子申告ファイル		
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 ※		eLTAXを利用して電子申告を利用する納税義務者
	その必要性	適正かつ公平な賦課を目的とし、必要な範囲の特定個人情報を保有するため。
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	・個人番号及びその他の識別情報：対象者を正確に特定するために保有 ・5情報及び連絡先等情報：①課税台帳の台帳記載事項として登録するため、②納税通知書等を送達するため、③本人への連絡等のため、保有する。 ・業務関連情報：租税の賦課を行うために保有する。
	全ての記録項目	別添2を参照。
⑤保有開始日		平成28年1月
⑥事務担当部署		主税局総務部システム管理課

3. 特定個人情報の入手・使用			
①入手元 ※			[　] 本人又は本人の代理人 [　] 評価実施機関内の他部署　（　） [　] 行政機関・独立行政法人等　（　） [　] 地方公共団体・地方独立行政法人　（　） [　] 民間事業者　（　） [○] その他　（ 本人又は本人の代理人→地方税ポータルシステム（eLTAX）　）
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			納税義務者等の申告の都度、入手する。
④入手に係る妥当性			地方税法の規定により、東京都へ提出される申告書、報告書、申請書、届出に記載された個人番号を取得している。 なお、行政機関等への申請・届出等手続きについては、「行政手続等における情報通信の技術の利用に関する法律」及び総務省令の定めるところにより可能となっている。
⑤本人への明示			地方税法の規定により、申告、申請、報告、届出が求められている。
⑥使用目的 ※			適正かつ公平な賦課を目的とし、必要な範囲の特定個人情報を保有するため。
	変更の妥当性		ー
⑦使用の主体	使用部署 ※		主税局各部、各都税事務所（都税支所を含む）、都税総合事務センター及び各支庁
	使用者数		[　1,000人以上　]　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
⑧使用方法 ※			・申告内容について、システムに登録する。 ・地方税共同機構へ電子データを提供する。
	情報の突合 ※		税務総合支援システムに登録されている納税義務者情報（氏名・住所）と、申告書等に記載されている情報を突合し、適正な申告であることを確認する。
	情報の統計分析 ※		個人を特定することなく、統計分析を行う。
	権利利益に影響を与え得る決定 ※		賦課決定
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 （ 3 ） 件
委託事項1		税務総合支援システムアプリケーション保守委託
①委託内容		税務総合支援システムの仕様変更、障害対応等 ※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] ＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[1,000万人以上] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	都税に係る納税義務者、申告義務者及び課税調査対象者
	その妥当性	税務総合支援システムの安定的な稼働のため、データの修正やシステムの異常終了時の対応などを行う上で特定個人情報ファイルを取り扱う必要がある。
③委託先における取扱者数		[10人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表予定。
⑥委託先名		未定
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	再委託する場合は、委託元は、委託先に対してあらかじめ再委託を行う旨を書面により提出させ、委託元が承諾を与える。
	⑨再委託事項	未定

委託事項2～5		
委託事項2		基盤（サーバー類）賃借・保守委託
①委託内容		税務総合支援システムの稼働に必要なサーバー類の提供　※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		［ 特定個人情報ファイルの全体 ］　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	［　　1,000万人以上　　］　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲　※	都税に係る納税義務者、申告義務者及び課税調査対象者
	その妥当性	税務総合支援システムの安定的な稼働のため、運用保守作業を行う上で特定個人情報ファイルを取り扱う必要がある。
③委託先における取扱者数		［　　10人未満　　］　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		［ ○ ］専用線　［　］電子メール　［　］電子記録媒体（フラッシュメモリを除く。） ［　］フラッシュメモリ　［　］紙 ［　］その他　（　　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表予定。
⑥委託先名		未定
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	再委託する場合は、委託元は、委託先に対してあらかじめ再委託を行う旨を書面により提出させ、委託元が承諾を与える。
	⑨再委託事項	未定

委託事項3		税務総合支援システム運用委託
①委託内容		税務総合支援システム（情報連携サーバーを含む。）の稼働に必要な機能の提供　※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		［ 特定個人情報ファイルの全体 ］　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	［　1,000万人以上　］　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲　※	都税に係る納税義務者、申告義務者及び課税調査対象者
	その妥当性	特定個人情報ファイルが含まれる税務総合支援システムの運用管理を行うために取扱う必要がある。
③委託先における取扱者数		［　10人未満　］　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		［ ○ ］専用線　［　］電子メール　［　］電子記録媒体（フラッシュメモリを除く。） ［　］フラッシュメモリ　［　］紙 ［　］その他　（　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表予定。
⑥委託先名		未定
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	再委託する場合は、委託元は、委託先に対してあらかじめ再委託を行う旨を書面により提出させ、委託元が承諾を与える。
	⑨再委託事項	未定
5．特定個人情報の提供・移転（委託に伴うものを除く。）		
提供・移転の有無		［ ○ ］提供を行っている　（　1 ）件　［　］移転を行っている　（　）件 ［　］行っていない

提供先1	地方税共同機構
①法令上の根拠	番号法第9条第3項、第19条第1号
②提供先における用途	地方税共同機構が納税者から電子申告により受領した情報について、個人番号の本人確認を行うため。
③提供する情報	電子申告により申告、申請、報告、届出を行った個人の納税者ID及び個人番号
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	eLTAXを利用して電子申告を利用する納税義務者
⑥提供方法	[　]情報提供ネットワークシステム　[○]専用線 [　]電子メール　[　]電子記録媒体（フラッシュメモリを除く。） [　]フラッシュメモリ　[　]紙 [　]その他　（　）
⑦時期・頻度	地方税共同機構からの求めに応じ、随時
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 ※		【審査システム（サーバー）】 ・特定個人情報を保管するデータセンタは、都市計画法における防火・準防火地域に指定されていること、サーバー室等へ滞りなく電力を供給できる電源設備及び非常用自家発電設備を備えていること等の防災性を重視した条件により、選定している。 ・データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とする等、厳重なセキュリティ対策を行っている。 【外部記録媒体】 ・税務総合支援システムと審査システム（eLTAX）の間のデータ授受に使用する外部記録媒体（ハードディスク・USBフラッシュメモリ）は、施錠された保管庫で管理している。
②保管期間	期間	［　6年以上10年未満　］ ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	文書等の取扱いに関する規定の保存期間に基づく。
③消去方法		【審査システム（サーバー）】 ・課税から収入までの一連のサイクルを完了し保存年限を経過した課税データについて、電子データの削除等に関する規定に基づき、委託先によるバッチ処理により削除している。 ・地方税共同機構への提供が完了したデータについて、電子データの削除等に関する規定に基づき、委託先によるバッチ処理により削除している。 ・機器リース期間満了時には特定個人情報等のデータを全て消去の上、消去結果について、記録媒体ごとに、消去した情報項目、数量、消去方法及び消去日等を明示した書面で委託事業者より報告を受けている。 【外部記録媒体】 ・税務総合支援システムと審査システム（eLTAX）の間のデータ授受に使用する外部記録媒体（ハードディスク）については、一定の保存期間の経過後、委託先が手作業でデータを消去している。 ・同目的に使用するUSBフラッシュメモリについては、データ移行後直ちに、職員が手作業でデータを消去している。 ・保管している外部記録媒体が不要となった場合は、当該外部記録媒体内部の情報を復元できないように消去した上で廃棄する。
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		
④eLTAX電子納税通知システムファイル		
2. 基本情報		
①ファイルの種類 ※		[　　システム用ファイル　　] ＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　　1,000万人以上　　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※		都税に係る納税義務者
	その必要性	納税義務者の申請に応じて、eLTAXを経由して電子的に納税通知書等の副本を送付することを可能とするため
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	・個人番号及びその他識別情報：対象者を正確に管理するために保有 ・5情報：納税通知書等を電子的に送付する納税義務者を特定するために保有 ・地方税関係情報：納税通知書等を電子的に送付する納税義務者等を特定するために保有
	全ての記録項目	別添2を参照。
⑤保有開始日		令和10年4月1日（予定）
⑥事務担当部署		東京都主税局 総務部システム管理課、課税部計画課、課税部課税指導課、課税部法人課税指導課、資産税部固定資産税課、資産税部固定資産評価課

3. 特定個人情報の入手・使用		
①入手元 ※		[　　]本人又は本人の代理人 [　　]評価実施機関内の他部署　（　　） [　　]行政機関・独立行政法人等　（　　） [　　]地方公共団体・地方独立行政法人　（　　） [　　]民間事業者　（　　） [○]その他　（ 本人又は本人の代理人→地方税通知ポータル（eLTAX）　　）
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		納税通知書等の電子化を希望する納税義務者等からの申請の都度、入手する。
④入手に係る妥当性		地方団体が、納税義務者等の求めに応じて、eLTAXを経由して電子的に納税通知書等の副本を送付することが地方税法（未定）に規定により可能となっている。
⑤本人への明示		地方税法（未定）に、地方団体が、納税義務者等の申請に応じて、eLTAXを経由して電子的に納税通知書等の副本を送付することができることが明記されている。
⑥使用目的 ※		納税義務者等の申請に応じて、eLTAXを経由して電子的に納税通知書等の副本を送付することを可能とするため。
	変更の妥当性	―
⑦使用の主体	使用部署 ※	主税局各部、各都税事務所（都税支所を含む）、都税総合事務センター及び各支庁
	使用者数	[　　1,000人以上　　]　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
⑧使用方法 ※		・地方税通知ポータル（eLTAX）から提供される申請書の電子データをeLTAX電子納税通知システムで受信する。 ・受信した申請書の電子データについて、システム登録を行う。 ・地方税通知ポータル（eLTAX）へ副本データを提供する。
	情報の突合 ※	あて名管理システムに登録されている納税義務者・申告義務者情報（氏名・住所）と、申請情報を突合し、適正な申請であることを確認する。
	情報の統計分析 ※	個人を特定することなく、統計分析を行う。
	権利利益に影響を与え得る決定 ※	賦課決定
⑨使用開始日		令和10年4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 （ 3 ） 件
委託事項1		税務総合支援システムアプリケーション保守委託
①委託内容		税務総合支援システムの仕様変更、障害対応等 ※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[1,000万人以上] <選択肢> 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	都税に係る納税義務者
	その妥当性	税務総合支援システムの安定的な稼働のため、データの修正やシステムの異常終了時の対応などを行う上で特定個人情報ファイルを取り扱う必要がある。
③委託先における取扱者数		[10人未満] <選択肢> 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表予定。
⑥委託先名		未定
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	再委託する場合は、委託元は、委託先に対してあらかじめ再委託を行う旨を書面により提出させ、委託元が承諾を与える。
	⑨再委託事項	未定

委託事項2～5		
委託事項2		基盤（サーバー類）賃借・保守委託
①委託内容		税務総合支援システムの稼働に必要なサーバー類の提供　※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		［ 特定個人情報ファイルの全体 ］　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	［　1,000万人以上　］　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲　※	都税に係る納税義務者
	その妥当性	特定個人情報ファイルが含まれる税務総合支援システムの運用管理を行うために取扱う必要がある。
③委託先における取扱者数		［　10人未満　］　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		［ ○ ］専用線　［　］電子メール　［　］電子記録媒体（フラッシュメモリを除く。） ［　］フラッシュメモリ　［　］紙 ［　］その他　（　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表予定。
⑥委託先名		未定
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	再委託する場合は、委託元は、委託先に対してあらかじめ再委託を行う旨を書面により提出させ、委託元が承諾を与える。
	⑨再委託事項	未定

委託事項3		税務総合支援システム運用委託
①委託内容		税務総合支援システム（情報連携サーバーを含む。）の稼働に必要な機能の提供　※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		［ 特定個人情報ファイルの全体 ］　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	［　1,000万人以上　］　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲　※	都税に係る納税義務者
	その妥当性	特定個人情報ファイルが含まれる税務総合支援システムの運用管理を行うために取扱う必要がある。
③委託先における取扱者数		［　10人未満　］　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		［ ○ ］専用線　［　］電子メール　［　］電子記録媒体（フラッシュメモリを除く。） ［　］フラッシュメモリ　［　］紙 ［　］その他　（　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表予定。
⑥委託先名		未定
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	再委託する場合は、委託元は、委託先に対してあらかじめ再委託を行う旨を書面により提出させ、委託元が承諾を与える。
	⑨再委託事項	未定
5．特定個人情報の提供・移転（委託に伴うものを除く。）		
提供・移転の有無		［　］提供を行っている　（　）件　［　］移転を行っている　（　）件 ［ ○ ］行っていない

6. 特定個人情報の保管・消去		
①保管場所 ※		【税務総合支援システム（サーバー）】 ・特定個人情報を保管するデータセンタは、都市計画法における防火・準防火地域に指定されていること、サーバ室等へ滞りなく電力を供給できる電源設備及び非常用自家発電設備を備えていること等の防災性を重視した条件により、選定している。 ・データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際してはICカード及び静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。
②保管期間	期間	［　6年以上10年未満　］ ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	文書等の取扱いに関する規定の保存期間に基づき保管しておく必要がある。
③消去方法		【税務総合支援システム（サーバー）】 一定期間経過後、バッチ処理により削除する。 また、機器リース期間満了時には特定個人情報等のデータを全て消去の上、消去結果について、記録媒体ごとに、消去した情報項目、数量、消去方法及び消去日等を明示した書面で委託事業者より報告を受けている。
7. 備考		
―		

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名		
⑤地方税外部連携ファイル（仮称）		
2. 基本情報		
①ファイルの種類 ※		[　　システム用ファイル　　] ＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　　1,000万人以上　　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※		都税に係る納税義務者
	その必要性	適正かつ公平な賦課を目的とし、必要な範囲の特定個人情報を保有するため。
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	・個人番号及びその他の識別情報：対象者を正確に特定するために保有 ・5情報：①課税対象者の認定に際し在住要件を確認するため、②本人への通知等送付及び連絡等のために保有 ・国税関係情報：租税の賦課徴収及び国税との情報連携のために保有 ・地方税関係情報：租税の賦課徴収及び他道府県との情報連携のために保有
	全ての記録項目	別添2を参照。
⑤保有開始日		令和9年9月（予定）
⑥事務担当部署		主税局総務部システム管理課

3. 特定個人情報の入手・使用		
①入手元 ※		[　　] 本人又は本人の代理人 [　　] 評価実施機関内の他部署　（　　） [　　] 行政機関・独立行政法人等　（　　） [○] 地方公共団体・地方独立行政法人　（ 市町村　　） [　　] 民間事業者　（　　） [　　] その他　（　　）
②入手方法		[　　] 紙　[　　] 電子記録媒体（フラッシュメモリを除く。）　[　　] フラッシュメモリ [　　] 電子メール　[○] 専用線　[　　] 庁内連携システム [　　] 情報提供ネットワークシステム [　　] その他　（　　）
③入手の時期・頻度		【不動産評価情報等の通知】 ・市町村から通知の都度、入手する。
④入手に係る妥当性		【不動産評価情報等の通知】 地方税法第73条の18第3項及び第73条の22等の規定により、市町村長は取得の事実を東京都知事に通知することとされている。また、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規則第19条の規定により、個人番号の提供を受けることができる。 また、市町村の税務システム標準仕様書上、個人番号が通知項目の一つとして定義されている。
⑤本人への明示		【不動産評価情報等の通知】 地方税法第73条の18第3項及び第73条の22等の規定により、納税義務者氏名・住所等の入手を行っている。 また、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規則第19条の規定により、個人番号の提供を受けることができる。
⑥使用目的 ※		適正かつ公平な賦課及び徴収を実現するため。
	変更の妥当性	―
⑦使用の主体	使用部署 ※	主税局各部、各都税事務所（都税支所を含む）、都税総合事務センター及び各支庁
	使用者数	[　　1,000人以上　　]　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
⑧使用方法 ※		【不動産評価情報等の通知】 市町村からの取得通知により入手する情報について、システム登録を行う。
	情報の突合 ※	あて名管理システムに登録されている納税義務者情報・申告義務者（氏名・住所等）と通知等に記載されている情報を突合（検索）し、システム上のあて名の有無及び適正な通知等であることを確認する。
	情報の統計分析 ※	個人を特定することなく、統計分析を行う。
	権利利益に影響を与え得る決定 ※	賦課決定
⑨使用開始日		令和9年9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 （ 3 ） 件
委託事項1		税務総合支援システムアプリケーション保守委託
①委託内容		税務総合支援システムの仕様変更、障害対応等 ※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] ＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[1,000万人以上] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	都税に係る納税義務者、申告義務者及び課税調査対象者
	その妥当性	税務総合支援システムの安定的な稼働のため、データの修正やシステムの異常終了時の対応などを行う上で特定個人情報ファイルを取り扱う必要がある。
③委託先における取扱者数		[10人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表予定。
⑥委託先名		未定
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	再委託する場合は、委託元は、委託先に対してあらかじめ再委託を行う旨を書面により提出させ、委託元が承諾を与える。
	⑨再委託事項	未定

委託事項2～5		
委託事項2		基盤（サーバー類）賃借・保守委託
①委託内容		税務総合支援システムの稼働に必要なサーバー類の提供　※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		［ 特定個人情報ファイルの全体 ］　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	［　1,000万人以上　］　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲　※	都税に係る納税義務者、申告義務者及び課税調査対象者
	その妥当性	税務総合支援システムの安定的な稼働のため、運用保守作業を行う上で特定個人情報ファイルを取り扱う必要がある。
③委託先における取扱者数		［　10人未満　］　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		［ ○ ］専用線　［　］電子メール　［　］電子記録媒体（フラッシュメモリを除く。） ［　］フラッシュメモリ　［　］紙 ［　］その他　（　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表予定。
⑥委託先名		未定
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	再委託する場合は、委託元は、委託先に対してあらかじめ再委託を行う旨を書面により提出させ、委託元が承諾を与える。
	⑨再委託事項	未定

委託事項3		税務総合支援システム運用委託
①委託内容		税務総合支援システム（情報連携サーバーを含む。）の稼働に必要な機能の提供　※項目③「委託先における取扱者数」は未定のため、1）10人未満を選択している。
②取扱いを委託する特定個人情報ファイルの範囲		［ 特定個人情報ファイルの全体 ］　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	［ 1,000万人以上 ］　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲　※	都税に係る納税義務者、申告義務者及び課税調査対象者
	その妥当性	特定個人情報ファイルが含まれる税務総合支援システムの運用管理を行うために取扱う必要がある。
③委託先における取扱者数		［ 10人未満 ］　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		［ ○ ］専用線　［　］電子メール　［　］電子記録媒体（フラッシュメモリを除く。） ［　］フラッシュメモリ　［　］紙 ［　］その他　（　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表予定。
⑥委託先名		未定
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	再委託する場合は、委託元は、委託先に対してあらかじめ再委託を行う旨を書面により提出させ、委託元が承諾を与える。
	⑨再委託事項	未定
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 ※		【地方税外部連携システム（サーバー）】 ・特定個人情報を保管するデータセンタは、都市計画法における防火・準防火地域に指定されていること、サーバー室等へ滞りなく電力を供給できる電源設備及び非常用自家発電設備を備えていること等の防災性を重視した条件により、選定している。 ・データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とする等、厳重なセキュリティ対策を行っている。
②保管期間	期間	[　6年以上10年未満　]　＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	文書等の取扱に関する規定の保存期間に基づき保管しておく必要がある。
③消去方法		【地方税外部連携システム（サーバー）】 一定期間経過後、バッチ処理により削除する。 また、機器リース期間満了時には特定個人情報等のデータを全て消去の上、消去結果について、記録媒体ごとに、消去した情報項目、数量、消去方法及び消去日等を明示した書面で委託事業者より報告を受けている。
7. 備考		
―		

（別添2）特定個人情報ファイル記録項目

・①賦課徴収事務ファイルに関するマスター覧は別紙10のとおり
・記録項目の詳細については別紙11参照
・④eLTAX電子納税通知システムファイルのファイルレイアウト案は令和7年9月に地方税共同機構より公開予定
・DA（個人事業税）:「個人事業税カルテ管理マスタ」、「個人事国税申告事績情報マスタ」、「減免受付管理マスタ」
FA（自動車二税）:「自二税減免申請情報マスタ」、「受付管理（減免申請書）マスタ」、「受付管理（更新申立）マスタ」
GA（固定資産税（土地・家屋））:「閲覧証明管理申請統括マスタ」
SA（情報連携）:「番号連携精神障害者手帳マスタ」、「番号連携身体障害者手帳マスタ」
には要配慮個人情報を含む。

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賦課徴収事務ファイル	
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	別紙6のとおり
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	別紙6のとおり
その他の措置の内容	ー
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	別紙7のとおり
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	別紙8のとおり
個人番号の真正性確認の措置の内容	別紙8のとおり
特定個人情報の正確性確保の措置の内容	別紙8のとおり
その他の措置の内容	ー
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	別紙9のとおり
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	
・税務総合支援システムは、誤操作のリスクに対する措置として、所定欄に所定形式でのみ特定個人情報をデータ登録できる仕組みをとっている。 ・誤操作リスクに対する措置として、特定の方法でしか特定個人情報をデータ登録できない仕組みをとっている。また、万が一登録内容に誤りがあった場合、エラーを検知し、誤った入手を未然に防止している。	

3. 特定個人情報の使用		
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容	【連携サーバー】 連携サーバーは、ユーザIDにより利用者等の単位でアクセス可能な範囲を限定し、正当な権限のない利用者等からは個人番号を利用できないアクセス制御を行っている。 【税務総合支援システム（サーバー）】 ・税務総合支援システムからデジタルサービス局所管の団体内統合利用番号連携サーバーへの接続については、都税の賦課徴収事務のうち、特定個人情報の提供・照会事務に従事する者に限定して権限を付与することにより、正当な権限のない者の利用を防止する。	
事務で使用するその他のシステムにおける措置の内容	税務総合支援システムでは、税務事務に係るデータのみを保有しているため、税務事務以外の情報と紐付けることを禁止している。	
その他の措置の内容	ー	
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	①税務総合支援システムを使用する職員に対して、静脈等による生体認証およびID・パスワードを用いた認証の二要素認証を導入する。なお、IDについては職員毎に割り当てを行うものとする。 ②操作内容は、操作ログとして保管されており、いつどのIDでログインしたのかを把握できるようにしている。	
アクセス権限の発効・失効の管理	[行っている]	＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	人事担当部署が職員の異動情報を把握又は公表次第、異動情報をシステム管理部署へ連絡される。これに基づき、システム管理部署が各ユーザIDに必要な権限を付与・削除する。	
アクセス権限の管理	[行っている]	＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	①アクセス権限については、システム管理部署が全ての権限を一元的に管理し、操作者の所属及び業務に合わせて、システムの機能ごとに「更新・参照可」、「参照のみ可」、「更新・参照不可」の権限を設定する。 ②設定に際しては、サブシステム所管部署より権限設定申請を受領し、システム管理部署での承認を経て申請内容をシステムへ反映する。 ③設定済の内容については、毎年度末に見直しを行うことにより、付与する権限に過不足が生じないようにする。 ④権限に変更を加えた際には、システム管理部署が登録した権限設定状況を示した各サブごとの一覧表を確認することにより、どの部署にどのような権限が設定されているのかを把握できるようにしている。 ⑤年に1度、各サブシステムに画面表示等の権限設定のヒアリングを行ったうえで、付与されている権限が適切かサブシステムの所管部署の職員がシステムを直接操作してテストを実施している。	
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	①システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、どのユーザIDで、どの情報にアクセスし、抽出したのかを記録し、この記録を保存している。なお、当該操作履歴はシステム利用者がアクセスすることはできず、改ざん防止を図っている。 ②また、特定個人情報等を記録した公文書が不要となった場合は、溶解等の復元不可能な手段により特定個人情報等の消去又は廃棄を行っている。	
その他の措置の内容	ー	
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	①局内の規定において、原則、情報資産の外部持ち出しを禁止している。 ②税務総合支援システム端末での外部記録媒体の使用を制限すること等により、容易に情報資産の持出しができないようにしている。 ③税務総合支援システムは、当該システムの専用端末以外では使用することができないよう対策が講じられている。 ④不正持出しの抑制手段として、全操作履歴を記録することによる監視を行っている。 ⑤外部持出しが必要な際には専用ソフトを用いてデータを暗号化しており、パスワード入力による暗号解除を行わない限り参照することができない。 ⑥所外用モバイル端末にて情報資産の持ち出しを行う場合は、持ち出し時に複数名でデータ内容を全て確認した上で上司の承認を得て持ち出しを行う。また、出張時は2名で対応する等相互監視により、事務外での不正な利用を防止している。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
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	①税務総合支援システム内の特定個人情報ファイルは、税務総合支援システム端末以外から閲覧することができない。 ②税務総合支援システム端末での外部記録媒体の使用を制限し、情報資産の持出しができないようにしている。ただし、規定等に基づき、情報資産を外部へ持ち出す必要がある場合については、当該規定及びサブシステム所管部署の申請に基づき、情報資産の持出しを可能としている。この際には、例外的に外部記録媒体の使用が許可されている端末により、システム管理部署がデータの移行を実施している。 ③ハードコピー等の紙資料については、取扱いに細心の注意を払うよう、研修や自己点検表等により注意喚起している。 ④業務において、必要な範囲を超えての作成を禁止している。 ⑤所外用モバイル端末にて情報資産の持ち出しを行う場合は、持ち出し時に複数名でデータ内容を全て確認した上で上司の承認を得て持ち出しを行う。 ⑥所外用モバイル端末に保存する情報資産について、規定により特定個人情報は保存することができないようにしている。 ⑦特定個人情報を取り扱う事務において使用するシステム及びその間のネットワークにおいても不正に複製されるリスクに対する対策が講じられている。
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
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	
①入力した情報について、職員間でのダブルチェック等を行い、正確性を確保している。 ②特定個人情報ファイルについては、インターネットと接続している端末に転記・保存することのないよう規定し、研修等で職員に周知した上、定期的な再点検や監査を実施している。 ③税務総合支援システムは、クローズドネットワーク、ネットワークへの接続を許可された専用端末以外からのアクセス不可、時間外使用不可、業務ごとに付与された権限外での使用不可、データ書き出し制限等、システムそのものに強力なセキュリティ対策を施すことで、不正使用のリスク対策を講じている。 ④ネットワークへのアクセスを許可されていない端末の不正接続について、常時監視を行っている。 ⑤不正使用を未然に防ぐため、毎年実施する研修で上記作業を行うことについて職員に周知している。 ⑥不正使用の疑いがある場合には、操作ログの確認を行っている。	

4. 特定個人情報ファイルの取扱いの委託	[　　] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク	
情報保護管理体制の確認	【委託事項1～3、7、8】 ・委託契約で下記事項を規定している。 （1）責任者、作業体制、連絡体制及び作業場所の提出 （2）業務従事者への遵守事項の周知及び実施報告の提出 （3）再委託の承諾申請の提出 （4）作業担当者の名簿の提出　等 ・委託先がプライバシーマーク等を保有していることを確認している。 【委託事項4～6】 委託契約で下記事項を規定している。 （1）責任者、作業体制、連絡体制及び作業場所の提出 （2）業務従事者への遵守事項の周知及び実施報告の提出 （3）作業担当者の名簿の提出　等 【委託事項9】 ・委託先が倉庫業法第3条による登録を受けた事業者であること、貨物自動車運送事業法第3条による一般貨物運送事業の許可を受けた事業者であること、プライバシーマークを取得していることを確認している。 ・保管をISMS(環境セキュリティマネジメントシステム)適合性評価制度の認証を受けている施設において行うことを確認している。 【委託事項10】 ・責任者及び業務従事者の名簿を提出する旨を、委託契約で規定している。 【委託事項1～10】 ・委託事項の内容、委託先等におけるリスクに応じて情報保護管理体制の確認を行っている。
特定個人情報ファイルの閲覧者・更新者の制限	[　　制限している　　] ＜選択肢＞ 1）制限している　　2）制限していない
具体的な制限方法	【委託事項1～3、8】 ・委託先が使用するユーザIDは、局内のIDに関する規定に基づき、委託元が割り当てを行っている。 ・ユーザIDの設定に際しては、用途を確認した上で必要最小限の権限のみ付与し、使用する期間のみ有効とし、有効期間が経過した場合には当該ユーザIDでは特定個人情報ファイルを閲覧できないようにしている。 【委託事項4～6】 ・委託先の業務の推進体制の作成、秘密の保持、目的外使用の禁止、複写及び複製の禁止、作業場所以外への持ち出し禁止、情報の保管および管理等を規定した契約を取り交わしている。 【委託事項7】 仕様書において、都が受託者に貸与するユーザIDは、「税務総合支援システムユーザID管理要綱」に則り受託者が管理することになっている。ユーザIDを使用しない限り特定個人情報ファイルの閲覧はできない。作業者を限定するために、委託業務従事者名簿を提出させ、その者以外の委託業務場所への立入りを禁じている。 【委託事項9】 委託契約で下記事項を規定している。 ・再委託業務を除き、作業員には正社員を充て、委託者の求めに応じて作業員の身分を証する書面等を提出する。 【委託事項10】 ・委託契約で、一連の業務を委託先が自ら行うことを規定している。 ・搬入された箱は開封することなく処理することを委託契約で規定しているため、特定個人情報ファイルの閲覧・更新のおそれはない。

特定個人情報ファイルの取扱いの記録		[　　記録を残している　　] ＜選択肢＞ 1）記録を残している　　2）記録を残していない
	具体的な方法	【委託事項1～5、7、8】 ・施錠された保管庫等での管理、管理状況の記録、管理記録の報告等を委託契約で規定している。 ・システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、いつどの情報にアクセスし、抽出したのかが記録されている。また、操作履歴データは、アクセス制御・暗号化により改竄や削除ができないようにしている。 【委託事項9】 ・新規預入れ、保管、配送、返却、解約及び廃棄処理実績について、内訳書を毎月提出する。 【委託事項10】 ・作業完了後、委託先と委託元の双方が箱数の確認印を押印した「作業数量確認書」を作成し、毎月委託元へ提出する。 ・処理完了後、溶解証明書を毎月委託元へ提出する。
特定個人情報の提供ルール		[　　定めている　　] ＜選択肢＞ 1）定めている　　2）定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	【委託事項1～10】 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について委託契約で規定している。
	委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	【委託事項1～7】 ① 委託先から他者への提供はない。なお、提供する必要性が発生する場合は、目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について契約で取り交わしている。 ② 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。 【委託事項3】 データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。 【委託事項7】 受託者は、業務委託仕様書の内容を遵守する旨記載した誓約書を都に提出することになっている。また、都による監査、点検及び検査に協力することが仕様書に規定されている。 【委託事項8】 ・ 申告書を委託先へ搬入する際及び委託先から申告書の返却を受ける際は、受払票を用いて委託元・委託先相互に部数の確認を行っている。 ・ 申告書を委託元へ返却するまでの期間は、ロッカー等で施錠保管しており、委託先の退出後、都税事務所職員が施錠確認を行っている。 【委託事項9】 委託契約で下記事項を規定している。 ・配送及び引取りは、施錠可能なコンテナ車を使用する。 ・配送及び引取りの際は、従事する作業員は写真付き証明書（社員証等）を提示するとともに、委託元職員に対して配送及び引取りの事実を証する書面を交付する。 【委託事項10】 委託契約で下記事項を規定している。 ・引渡しの際、委託元に身分証明書を提示し、確認を受ける。 ・運搬にあたっては、荷台を施錠するとともに、委託元職員が随行する。 ・委託先作業員は、一連の作業の際、運搬車から離れてはならず、作業においては文書保存箱の内容物を一片たりとも散逸、抜取り等してはならない。 ・搬入された箱はほかの場所に一時保管することなく直ちに処理を開始し、その日のうちに処理を終える。

特定個人情報の消去ルール		[　　定めている　　] ＜選択肢＞ 1）定めている　2）定めていない
	ルールの内容及びルール遵守の確認方法	【委託事項1～3】 ・ 契約履行完了後に当該委託業務に係る情報を全て消去することを、委託契約で規定している。 ・ 消去した情報項目、数量、消去方法及び消去日等については報告書類にて確認している。 【委託事項4～6】 ・委託元から委託先への提供はない。 ・消去は行わない。 【委託事項7】 特定個人情報の提供はない。 【委託事項8】 ・ 入力に使用した帳票及び出力した帳票類は委託元に返却すること、複写ミス等によりコピー用紙等の廃棄を行う必要が生じた場合も委託元に引継ぐことを、委託契約で規定している。 ・ 受払票にて、委託前後で帳票の部数が一致することを確認している。 ・ 委託先は業務の過程で特定個人情報ファイルを保有しないため、電子データを消去する必要はない。 【委託事項9】 委託契約で下記事項を規定している。 ・廃棄処理は、秘密が漏えいすることのないよう、箱ごと溶解する方法で行う。 ・廃棄処理の実施に当たっては、事前に、委託元と委託先とで協議の上、実施計画を定める。 ・都職員の要求があった場合には、廃棄処理への立会いを認める。 ・廃棄処理を終了したときは、速やかに委託元の担当者に報告し、後日廃棄処理の完了届を提出する。 【委託事項10】 委託契約で下記事項を規定している。 ・搬入された文書保保存箱を開封することなく直接溶解槽に投入し、処理する。 ・処理に際して、委託元職員の立会いを認める。 ・機械トラブル等やむを得ない理由により箱を開封する必要が生じた場合は、委託元の監視のもとで開封する。この場合、内容物を直ちに溶解槽に投入し、一片たりとも散逸、抜取り等してはならない。 ・処理完了後、溶解証明書を毎月委託元へ提出する。
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	・委託契約で下記事項を規定している。 【委託事項1、2】 （1）プログラム、データ等が格納されたサーバー及び端末機器等は、適切なアクセス権限を設定すること。 （2）外部記録媒体でやり取りするプログラム、データ等は、最新のパターンファイルを適用したウイルス対策ソフトでチェックすること。 【委託事項1～3】 （3）セキュリティ監査を実施する際は協力すること。 （4）委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく委託元に報告すること。 【委託事項4～6】 ・委託契約で下記事項を規定している。 (1）目的外使用の禁止、情報の保管及び管理、再委託の取扱い、実地調査の実施 (2）委託先の担当者名簿の提出 (3）委託の履行に関して知り得た情報を漏らしてはならない。 (4）契約書及び仕様書の内容を遵守する旨記載した誓約書を提出すること。 【委託事項7】 特定個人情報の提供はない。 【委託事項9】 ・目的外使用の禁止、情報の保管及び管理　等 【委託事項10】 (1）目的外使用の禁止、情報の保管及び管理、実地調査及び指示すること。 (2）委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく委託元に報告すること。

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	【委託事項1～3】 ①委託元と委託先の間で取り交わされている契約内容と同等の条件を再委託先においても課している。 ②委託元が再委託先に対して実地調査を1年に1回行い、適切な管理体制をとっていることを確認している。 ③委託先が再委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく報告させている。 【委託事項4、5、8、10】 再委託について禁止している。 【委託事項7】 特定個人情報の提供はない。 【委託事項9】 再委託先への特定個人情報ファイルの受渡し、廃棄作業時に委託元が立ち会っている。
その他の措置の内容		・委託に関する契約書や仕様書及び受託者から受領する誓約書等の書類については、文書等の取扱に関する規定の保存期間に基づき保管している。 ・委託先に対し、作業場所へ業務に関係がない物の持込みを禁止する。
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報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	他道府県との間で個人情報の提供等行う場合は特定個人情報の提供等対象者の名称、特定個人情報の提供の日時、提供先及び提供する特定個人情報の項目等を通報処理簿及び受報処理簿に記録して、7年間保存するなどの措置をとる。
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	国税庁及び他道府県との間で行う提供等の作業については、事務マニュアルや実施手順書において提供方法等を規定している。具体的には、通報に当たっては所属長の確認・決裁を得た上で通報処理簿に記録のうえ通報を行っており、受報する際にも受報処理簿の記載等を行いシステム上適切に管理するよう事務処理方法についても定めている。
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	国税庁及び他道府県に特定個人情報を提供するに当たっては所属長の確認・決裁を得てから提供しており、提供した内容等については通報処理簿に記録している。
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	国税庁及び他道府県に特定個人情報を提供するに当たっては所属長の確認・決裁を得てから提供しており、提供した内容等については通報処理簿に記録している。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置	
―	

6. 情報提供ネットワークシステムとの接続	[　　]接続しない（入手）　[○]接続しない（提供）
リスク1：　目的外の入手が行われるリスク	
リスクに対する措置の内容	【中間サーバー・ソフトウェアにおける措置】 ①情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ②中間サーバーの職員認証・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。 【連携サーバー】 ・各事務所管部署からの申請に基づき、利用者とその所掌事務の紐付けが連携サーバー上であらかじめ定義され、その範囲においてのみ情報照会が可能となるようアクセス制御されている。 ・情報照会に対する回答は、当該照会を行った事務に対してのみ返却するよう制御されている。 ・各事務所管部署が個々の照会データを一意に識別できるよう付与した識別子を、連携サーバーからの回答データに付記して返却することで、どの照会に対する回答かを各事務所管部署で正確に突合できるようにしている。 【税務総合支援システム】 ・個人事業税、自動車税、固定資産税の減免に関係する者のみにアクセス権限を付与する。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク2：　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】 ①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システムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 【中間サーバー・プラットフォーム】 ①中間サーバー、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバ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。 【連携サーバー】 ・システムの利用可能な時間を制限している。 ・情報連携に用いる端末に対し、端末認証を行う。 ・ログイン時に利用者の認証を実施する。 ・個別業務システム（事務）との間は、庁内のネットワークを介するとともに、暗号化を行う。 ・連携サーバーから個別業務システム（事務）に提供する照会結果ファイルは、暗号化を行う。 ・中間サーバーとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。 ・サーバー認証により真正性が担保された中間サーバーに接続する。 【税務総合支援システム】 ・連携サーバーに登録する照会ファイルを暗号化する。 ・連携サーバーに登録する照会ファイル及び取得する照会結果ファイルは、システム処理を前提にアクセス制限されたフォルダに格納するため、外部に持ち出すことはない。 ・上記の作業は、情報連携ファイルを管理する職員のみが行う。なお、情報連携ファイルを持ち出す際は事前に許可申請書による内部認証を経るとともに、作業後には報告書を提出している。
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】 ①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システムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。 【連携サーバー】 ・各事務所管部署で本人確認及び真正性確認を行った個人番号に基づき、団体内統合利用番号及び個別業務システム利用番号が紐付けられていることを前提として、当該人に対する情報照会が可能となるよう制御されている。 ・サーバー認証により真正性が担保された中間サーバーに接続する。 【税務総合支援システム】 ・税務総合支援システムは、情報提供ネットワークシステム・中間サーバー・連携サーバーを使用して、団体内統合利用番号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。
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】 ①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た特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ②既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ③情報照会が完了又は中断した情報照会結果については、一定期間経過後に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。 ④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になっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 【中間サーバー・プラットフォーム】 ①中間サーバー、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、漏えい・紛失のリスクに対応している。 ②中間サーバ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。 ③中間サーバー・プラットフォーム事業者の業務は、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。 【連携サーバー】 ・システムの利用可能な時間を制限している。 ・情報連携に用いる端末に対し、端末認証を行う。 ・ログイン時に利用者の認証を実施する。 ・個別業務システムとの間は、庁内のネットワークを介するとともに、暗号化を行う。 ・中間サーバーとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。 ・サーバー認証により真正性が担保された中間サーバーに接続する。 ・システムの利用者、日時等をシステム上でログとして記録し、7年間保存する。 ・個別業務システム（事務）と中間サーバーとの間における特定個人情報の授受に当たっては、その中継のみを行う。中継した情報は、個別業務システム（事務）の取得後に消去し、且つ一定期間内に自動で消去する。 ・連携サーバーから個別業務システム（事務）に提供する照会結果ファイルは、暗号化を行う。 【税務総合支援システム】 ・連携サーバーに登録する照会ファイルを暗号化する。 ・連携サーバーに登録する照会ファイル及び取得する照会結果ファイルは、システム処理を前提にアクセス制限されたフォルダに格納するため、外部に持ち出すことはない。 ・.情報提供ネットワークシステムにより障害者関係情報及び生活保護関係情報を取得する際は、対象者について照会ファイル作成のためのシステム登録を行う。なお、照会ファイル作成は、登録された内容に問題がないかを内部承認にて確認した上で行う。 ・連携サーバーから取得する障害者関係情報及び生活保護関係情報は、データセンタ内でシステム処理（バッチ処理）によって取り込みを行う。
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】
①中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。
②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。

【中間サーバー･プラットフォーム】
①中間サーバー、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。
②中間サーバ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。
③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。
④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・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。

【連携サーバー】
連携サーバーと接続する端末に対し端末認証を行い、権限のない職員がアクセスできないようになっている。

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	【紙媒体】 ・文書等の取扱いに関する規定に基づき、施錠された書庫に保管している。 ・文書の預入れを行う場合の保管倉庫は、地盤が強固で、海抜が高く、河川、池沼、運河、ため池等に隣接せず、近隣に危険物貯蔵倉庫及び工場がなく、人口及び建築物の密集地域ではない場所に建設している。 ・上記保管倉庫は、専用保管庫として設計された耐震・耐火構造を備えた堅固な建築物であり、外部からの侵入を防ぐための人的及び施設的管理体制（警備員による警備、監視カメラ、警報装置、赤外線センサー等）を備え、入退室は権限のある者のみ可能とし、入退室の記録をとり、一定期間保管している。 【税務総合支援システム（サーバー）】 ・特定個人情報を保管するデータセンタは、都市計画法における防火・準防火地域に指定されていること、サーバ室等へ滞りなく電力を供給できる電源設備及び非常用自家発電設備を備えていること等の防災性を重視した条件により、選定している。 ・データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際してはICカード及び静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。 【中間サーバー・プラットフォーム】 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。 【連携サーバー】 ・サーバー等を設置するための専用施設内に他のシステムとは分離した区画を設け、当該サーバー専用のラックに施錠して収容する。当該施設では、入退室者管理、区画ごとの施錠管理、監視カメラによる録画、有人監視等を実施する。 ・当該施設の煙感知装置、ガス系消火設備、耐震対応等により、火災や地震に起因する滅失等のリスクを低減する。 ・機器のうち、特定個人情報等のデータが記録されうるものの廃棄等に当たっては、磁気的消去又は物理的破壊等により、当該データを復元不可能な状態とする。 【外部記録媒体】 外部記録媒体については施錠したケースに格納し、引渡しの際にはデータ引渡し兼受領書を用いて行っている。	

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	【税務総合支援システム（サーバー）】 ①税務総合支援システム端末での外部記録媒体の使用を制限し、予期しないデータの取込み及び持出しができないようにしている。また、データベースは税務総合支援システム端末以外から閲覧できないようにしている。 ②サーバー、端末等の機器にはウイルス対策ソフトを適用するとともに、パターンファイルの更新を定期的に行うことにより、ウイルス感染を防止している。さらに、住民情報等の流出防止を目的に総務省が提示している三層分離の観点から、税務総合支援システムの外部ネットワーク接続は個人番号利用事務系のみに制限している。 ③税務総合支援システムと外部システム間のデータ連携は委託業者の運用作業場所である、システム運用拠点（以下「運用拠点」と言う。）で専用の外部記録媒体を使用して行っている。なお、運用拠点への入室はデータセンタ同様生体認証が必要である。 ④特定通信として税務総合支援システムに接続している電子申告、国税連携システムに係るネットワークについては、ファイアウォールを運用するとともに、接続状況を監視することにより、不正接続への対策を行っている。 【中間サーバー･プラットフォーム】 ①中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ②中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ④中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤中間サーバーのデータベースに保存される特定個人情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ⑥中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ⑦中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。 【連携サーバー】 ・サーバーが接続されたセグメントとそれ以外のセグメントの境界にファイアウォールを導入するとともに、ログを取得する。 ・ウイルス対策ソフトを導入し、パターンファイルを更新する。 ・基本ソフトウェア(OS)及びミドルウェアは、必要に応じてセキュリティパッチを適用する。

⑦バックアップ	[　　十分に行っている　　]	＜選択肢＞ 1）特に力を入れて行っている　　2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知	[　　十分に行っている　　]	＜選択肢＞ 1）特に力を入れて行っている　　2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[　発生あり　]	＜選択肢＞ 1）発生あり　　2）発生なし
その内容	①令和4年5月、東京都現代美術館において、ミュージアムショップ運営の受託事業者スタッフが、展覧会図録を予約した顧客へ一斉に案内メールを送信する際、メールアドレスをBCC欄ではなく、宛先欄に入力して発信した。 ②令和4年5月、技能検定試験に関する通知を外国人技能実習の複数の監理団体に対しメールで送付する際、誤ってメールアドレスをBCC欄ではなく、CC欄に入力し、一斉送信した。 ③令和4年5月、就学支援金事務において、就学支援金の基礎データをCD-Rに情報を保存し、対象高等学校等宛て一斉に送付したところ、そのうち1校に、他校の受給者に関する情報が含まれていることが判明した。 ④令和4年5月、受託事業者が、事業に関するイベントを案内するメールマガジンを送付する際、配信プログラム改修ミスにより、宛先欄に複数のメールアドレスが入力され、送信された。 ⑤令和4年10月、東京都陽性者登録センターの運営受託事業者が、医療機関で新型コロナウイルス陽性の診断を受け、センターに登録申請を行った複数の患者への登録完了メールを、送付先アドレスが全て入れ替わったまま送信した。 ⑥令和4年12月、労働力調査の統計調査員に対して連絡事項をメールした際、BCC欄に入力して送るべきところを宛先欄に入力し、一斉送信した。 ⑦令和5年4月、再委託先の派遣会社職員が、業務で使用するシステムを不適切に使用し、個人情報を閲覧、メモにとり自宅に持ち出した。 ⑧令和5年5月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑨令和5年6月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑩令和5年7月、施設を退所する患者に関して、退所先候補の施設と受入調整を行うため、診療関係書類をFAX送信した際、誤って別のFAX番号宛てに送信した。 ⑪令和5年8月、申請により受け付けた申請書が紛失していることが発覚した。 ⑫令和5年9月、関係施設宛に都民情報をFAX送信した際、誤って別の事業者宛てに送信した。 ⑬令和5年9月、事業の対象者に案内チラシを郵送した際、送付対象者の抽出ツールのプログラム仕様の不備により、誤って事業対象外の方に送付したことで、旧住所宛てに送付し返戻されなかったものが誤送付となった。 ⑭令和5年9月、決定通知書に公印を押印する目的で本庁に出張し、押印後持ち帰ったが、発送の準備をしていた際に、通知書1枚が紛失していることが発覚した。 ⑮令和6年1月、患者A宛てに送付すべき利用者情報を、誤ってB宛てに送付した。 ⑯令和6年1月、入所者の診療関係ファイルが紛失していることが発覚し、その後、退所者の荷物の中に当該ファイルが混入していたことが発覚した。 ⑰令和6年2月、児童相談所の職員が、出張中に個人情報が記載されている手帳を紛失し、あわせて手帳に収納されていた、当該職員の証票及び所内職員の緊急連絡網を紛失した。 ⑱令和6年2月、施設を退所した患者Aに関する薬剤情報等を記載した書類を、誤って別の患者の退院時の荷物に混入させ交付した。 ⑲令和6年2月、オンライン研修で使用した映像において、患者の情報をマスキング処理していたところ、当該映像をスマートフォンで視聴した場合に、マスキングが外れ、個人が特定できる状態になっていたことが判明した。 ⑳令和6年4月、受け付けた申請書を紛失していることが発覚した。 ㉑令和6年4月、施設職員が、利用者の通院付添の際、処方箋を紛失した。 ㉒令和6年4月、指定管理者が、事業者に対してExcel資料をメールで送信した際、本来削除すべきだった個人情報の入力されたシートを削除しなかった。 ㉓令和6年7月、受託事業者が、都へ交付すべき納入済通知書を、誤って他の事業者宛てに交付したことが発覚した。 ㉔令和6年7月、受託事業者がイベントを行った際の申込時の個人情報が掲載されたウェブページが、一時外部からアクセス可能な状態となっていたことが発覚した。 ㉕令和6年7月、職員が、説明会の資料の中に個人情報が含まれていることに気が付かずに、各自治体にデータを配布した。 ㉖令和6年7月、職員が、A宛てに送付すべき個人情報を、誤ってB宛てに送付していたことが発覚した。 ㉗令和6年7月、受託事業者から送付した個人情報を含む資料が、紛失していることが発覚した。 ㉘令和6年7月、受け付けた申請書を紛失していることが発覚した。 ㉙令和6年8月、受託事業者が配付した資料の中に、個人情報等が含まれる資料が混入していたことが発覚した。 ㉚令和6年10月、職員が、受託者に資料をメールで送信した際、誤って個人情報が記載された別のファイルを添付した。 ㉛令和6年10月、受託事業者が、A宛てに送付すべき電話記録を、誤ってB宛てにFAXで送信した。 ㉜令和6年11月、受け付けた申請書を紛失していることが発覚した（後日発見）。 ㉝令和6年11月、令和3年頃に個人情報が記載された資料を紛失していたことが発覚した。 ㉞令和6年12月、受託事業者が、個人情報が記載された資料を、誤って外部へ送信した。 ㉟令和7年1月、受託事業者が、個人情報が記載された資料を、誤って期限前に廃棄した。 ㊱令和7年1月、受け付けた届出書が、誤って机ごと廃棄されていることが発覚した。	

	再発防止策の内容	①（1）ミュージアムショップにおいて、本社セキュリティインシデント統括部と連携して、個人情報取り扱い、情報管理体制の改善を行う。 （2）特に複数人へのメール送信に際してはダブルチェックを徹底する。 （3）現代美術館全委託業者に、適切な個人情報等の取扱い及び情報管理を徹底するよう指示する。 （4）財団が管理運営する各施設にも本事案を共有し、個人情報を含む情報の適切な管理を徹底する。 ②（1）個人情報の取扱い及び情報管理の徹底等について周知するとともに、職員全員に臨時研修を速やかに実施 （2）誤送信防止に向けたシステムの導入（ダイアログの自動表示など） （3）複数人チェックなど基本的対策の徹底 ③チェック機能を再検証し、全日制等と同様の仕組みを通信制にも直ちに導入するほか、事務フローの再構築を行い、再発防止に努める。そのうえで、本件を財団内で広く共有させ、個人情報の取扱い全般についてハード・ソフトの両面から厳しく見直すとともに、職員の意識向上を図っていく。また、都の実施機関においても個人情報の適正管理とサイバーセキュリティー対策について改めて確認を行う。 ④（1）システムの改善 メールマガジンの配信は、これまで「TO」により自動で1件ずつ送信がされる仕組みであったが、一括メール送信においては送信者アドレスを全て「BCC」に入れるようシステム改修を行う。 （2）システム会社における確認体制の強化 開発前にシステム会社が実施する、影響調査・テスト内容等について、これまでの2名体制によるダブルチェックから、システム会社のプロジェクトマネージャーも加えることとし、確認した内容を報告させて承認する運用へ見直す。 （3）受託事業者における確認体制の強化 システム会社のテスト結果の確認にあたっては、テストの証跡情報の提出を求め、内容の確認を行うとともに、受託事業者での運用テストでは要件定義とも照らした確認を担当だけでなく管理職も実施することにより徹底する。 ⑤受託事業者に対して厳正に指導し、登録完了メール送信作業のチェック体制を強化させる。 ⑥（1）部コンプライアンス推進委員会の臨時開催 ・メール送信時のダブルチェックを徹底させるため、個人情報等の取扱いに係るチェックリストの全職員での点検により注意を喚起、情報管理を再徹底する。 ・あわせて、最近の事故事案の事例を周知するなど、事故の再発予防を進める。 （2）定期的な事故防止意識の醸成 統計調査員を含む全職員を対象に、各所属長や指導員から情報セキュリティや感染拡大防止等に関する指導を定期・継続的に行い、危機意識の醸成等を図る。 ⑦委託先における個人情報の閲覧・使用に当たっての権限の設定や、不適切な閲覧・使用・持ち出しを防止するための体制についてあらためて確認し、適切な運用を徹底させる。 ⑧（1）情報共有をしているホワイトボードの位置、記入欄が分かりにくいとの意見が出 ため、位置、記入方法について変更した。 （2）書類封入時のチェック手順中に、患者氏名の確認を明示した。 （3）2者確認を徹底するため、事務員のみでなく看護職員もチェックを行うこととし、 2者チェックが終わった段階で封書のチェックボックスに記載する。 （4）責任の所在を明確にするため「転院時退所セット確認書」を新たに作成し、チェックを行った職員が記名する。 ⑨（1）チェックリストを活用し、複数人、複数回のチェックを行うとともに、最終チェック者を統括責任者とすることで、誤封入等を防ぐ体制を整える。 （2）都職員が施設へ直接出向き、個人情報管理の実態確認を実施するとともに、対応 が不十分な場合は是正指導を行う。 （3）個人情報保護の研修を実施し、施設全体で個人情報保護の取り組み状況を共有した上で、改善を徹底する。 ⑩（1）委託先に対し、個人情報に関する業務手順を見直し及び徹底を図ることや、全従 事者に対する個人情報保護研修を行うことを指導した。また、改善策の確認のため、都が施設へ出向き、個人情報管理の実態を確認した。 （2）再委託先において、送付の際は、まずFAX以外の手段を調整し、止むを得ずFAXを使用する際には、FAX番号の聞き取りの際の復唱や、FAX送信前の送信先への番号の再確認、複数人で複数回のチェックを必ず行うこととした。また、全従業者に対する個人情報保護研修を行った。 ⑪（1）作業環境等を見直し、書類の混入等が起きにくい環境を整備 ①執務室内の作業スペースの確保及び活用 ②引き出し付きの棚をキャビネット内に新設し、書類の分類をよりしやすくした。 （2）委託業者との書類の受け渡し方法の変更（送付する判定機関ごとに数を確認しながら受け渡す）。 ⑫個人情報をFAX送信することを禁止するよう各施設に通知した。 ⑬抽出ツールのプログラム確認は、委託先事業者の運用チームのみが行っていたが、抽出ツールを作成・利用する際には、運用チームに加えて、開発チームと委託元である都の3者で抽出ツールのプログラムの仕様・設定を確認することとした。 ⑭個人情報の持出、返却確認及び受け渡しの際の確認の徹底を行う。また、作業工程等を点検し、作業方法やチェック方法等ミスが起きにくい方法を検討、実施する。 ⑮郵便の発送作業は複数職員でチェックすることを再徹底。また、特に慎重を要する個人情報を取り扱う施設における個人情報の事故の重大性について改めて周知するとともに、書類の発送、保管、業務の進行管理等について、注意喚起や指導を行った。 ⑯（1）ファイルが他の物に紛れてしまわないよう、目立つ色に変更する。 （2）作業スペースに仕切りを立てて、使用スペースを物理的に限定する。 （3）ファイルに記載する名前をイニシャルに表記変更する等、使用する情報から個人情報を削除する。 （4）決まった時間に決まった人員が所在を確認する。 （5）チェックの時間を定刻とし、声をかけ合う。 （6）出したらしまうといった基本的事項を、改めて徹底するよう、注意喚起する。 （7）急いでいたり、忙しい時間帯でも、ダブルチェックをするよう、改めて徹底する。また、退所時にも荷物を確認してから渡すようにする ⑰（個人情報の管理について） （1） 相談援助業務上の記録をノート等に記載する場合は、イニシャルを使用するなど個人情報を特定されないようにすること。また、私物のノートや手帳に個人情報を記載しないこと。 （2） 庁舎外での会議等に出席した際には、個人端末を活用して記録の作成を行うとともに、作成した文書は暗号化し保存すること。 （3） 業務上やむを得ず個人情報が記録された書類を庁舎外に持ち出す場合は、局の保有個人情報安全管理基準に基づき管理職の許可を得ること。 （4） 個人情報を含む書類を持ち出すにあたっては、盗難や紛失を防止できる形状・機能を持つ鞄に収納し、肌身離さず持ち運ぶなど十分に注意すること。 （5） その他個人情報の取り扱いについては、局の保有個人情報安全管理基準等を遵守し、適正に行うこと。 （職員の証票の管理について） （1） 月1回、各職員の保有状況を点検すること （2） 携行する際には、ストラップ付きのケースに収納するなど、常に身体から離さずに携行することを徹底すること （職員の緊急連絡網の管理について） （1） 必要な連絡先は公用携帯に保存し、連絡網を記載した紙は庁舎外に持ち出さないこと。 ⑱（1）入所時や退所時の手順確認のチェックリスト様式を変更し、入所時の写真撮影やリストへの正確な情報記載、退所時の荷物確認の手順など守るべきルールを追記するとともに、実施者を記載する欄を追加。 （2）個人情報紛失判明時の、本部への速やかな報告や具体的な捜索の手順などを、チェックリストに追記。 （3）毎朝のミーティングにてリーダー看護師等に個人情報保護の重要性やルールの順守を徹底。勤務者には、業務実施前に最新のマニュアルを確認するよう指導。 ⑲（1）発表資料の事前確認の徹底について幹部会で決定し、各部署に注意喚起 （2）録画や写真撮影をして保管していない旨を書面で確認 （3）画像等の個人情報の収集・利用に関する同意手続きの見直し ⑳（1）電子申請を推奨して紙文書の紛失リスクを軽減 （2）個人情報の適切な管理を職員に改めて周知徹底 ㉑（1）病院へ持ち運ぶファイルに、処方箋を収納する専用スペースを作る （2）医療機関受診時に係るマニュアルを作成 （3）帰園後は可能な限り速やかに所管部署に処方箋等を提出する （4）重要な個人情報を預かっている状況での裁断作業を避ける

		(4)重要な個人情報を預かっている状況での裁断作業を避ける (5)上記対応について、ミーティング等で周知徹底、注意喚起 ㉒(1)必要なデータファイルのみを送信用データとしてPDF化し、送信前に、PDFに不要な箇所が入っていないことを確認の上、送信することを徹底 (2)メールシステム上、外部送信時に必須である上長の承認の際、個人情報が含まれていないか等の確認を徹底 (3)「メール送信時のセルフチェックリスト」を作成、活用 (4)各管理職より各職員に対する面談時に、個別に再度、再発防止策を徹底 ㉓(1)交付前の事務手順や確認方法の見直し、交付時の最終確認方法の見直し (2)作業スペースへの注意文の掲示やチェックリストへの注意文の記載 (3)確認等を行う人数を増員し、誤交付を防ぐ体制を強化 (4)再発防止勉強会を実施 ㉔(1)委託事業者及び再委託事業者に厳重注意、再発防止策等の作成を指示し、受領 (2)WEBページの脆弱性等の確認を受けるため、デジタルサービス局との調整を開始 ㉕(1)精査が十分でないデータを外部に提供しないこと、精査及び送付の際には複数体制でチェックすることを徹底 (2)受託事業者において、作成した資料のレビューフローの再検討、個人情報データの受領・管理方法に関する社内再教育等の取組を実施 ㉖(1)ダブルチェックの徹底及びその旨の指導 (2)作業項目の文章化、わかりやすいチェックリストの作成 ㉗(1)受託事業者において、マニュアルに沿った処理を徹底し、送付書類の引継ぎ時には、郵便局ともに引継ぎ件数ーを確認 (2)3か月間、受託事業者から送付先に対し、発送日の連絡及び到着の確認を行う。 ㉘(1)原則電子申請として紙文書の紛失リスクを軽減 (2) 書類の所在及び処理状況を明確に把握できるよう管理方法を見直す ㉙(1)個人情報の取扱い及び情報管理の徹底等について、厳重に注意喚起 (2)個人情報が特定できない記載にする等の対策 ㉚(1)局内各職場にて個人情報事故防止対策等をテーマとした職場討議実施 (2)個人情報安全管理強化月間の自己点検・職場点検による一層の意識啓発 ㉛(1)張り紙の掲示、FAXボタンへの着色による物理的な注意喚起 (2)FAX送付時のダブルチェック、送信履歴の確認等をマニュアルに追加 ㉜(1)区市町村からの書類を収受する際の件数記載用の共通様式を作成し、受領時に種類ごとの件数を確認・記入 (2)本件の事務のプロセスを細分化し、各プロセス毎の書類の受渡し時に、各担当者がそれぞれ(1)の様式に記載した件数に基づき、書類、件数の確認作業を行うよう整理 (3)使用頻度ごとに文書の保管場所を整理し、常時使用しないものは施錠。作業中に開錠しているキャビネットについても、中に担当者ごとの鍵付きの引き出し等を設置して自分の担当以外の書類は持ち出せないようにし、作業の際にその都度施錠。 (4)緊急の所内幹部会を開催し、個人情報を含む書類の受け渡し時の確認等、個人情報の取り扱いのルールが適正に行われているか確認を指示し、報告を受ける。 ㉝(1)個人情報の保管ルールについて全職員に徹底 (2)現在の保管状況の再点検を実施 ㉞(1)受託事業者に対する個人情報の取扱い及び情報管理の徹底に向けた注意喚起 (2)管理番号の活用など個人情報が特定できない情報管理方法等の導入 ㉟(1)廃棄時の職員立会いの徹底、チェックリストの作成、活用 (2)廃棄対象文書とシステム登録情報の照会の実施 ㊱書類の保管場所の見直し

⑩死者の個人番号		[保管している] ＜選択肢＞ 1）保管している 2）保管していない
	具体的な保管方法	生存者の個人番号と同様の方法にて安全管理措置を実施している。
その他の措置の内容		バックアップデータについても、システムで使用している元データと同様の方法にて安全管理措置を実施している。
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 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		・東京都主税局賦課徴収主管課が入力した情報を随時取得・更新する。 ・納税義務者・申告義務者のあて名情報に異動があった場合等に最新の情報を住民基本台帳ネットワークシステムから随時取得・更新する。 ・納税義務者・申告義務者から提出を受けた申告書等に記載された住所等に更新する。 ・納税義務者・申告義務者の異動に際しては、法令等に則り、適切に届出等を行うよう周知を行っている。 ・所得税等申告情報に変更があれば、国税庁・税務署からの情報提供を受けた際に確認し、更新している。 ・国税庁・税務署に提出された所得税の訂正申告、修正申告、更正決議書等についてもデータの提供を受けており最新情報の取り込み処理を行っている。 ・納税通知書等の返戻調査時に新たな住所が判明すれば、最新の情報に更新している。 ・毎年、経済産業省関東経済産業局において、鉱業原簿に登録された鉱区税のあて名に係る情報の確認を行っており、その際に更新があれば確認できる。 ・減免決定を行う際、対象者について最新の情報を取得している。 ・還付決定を行う際、対象者について最新の情報を取得している。
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 特定個人情報が消去されずいつまでも存在するリスク		
消去手順		[定めている] ＜選択肢＞ 1）定めている 2）定めていない
	手順の内容	【連携サーバー】 ・個別業務システム（事務）及び中間サーバーとの間で授受されるデータは、所要の処理完了後又は一定時間経過後に削除される。 ・機器のうち、特定個人情報等のデータが記録されうるものの廃棄等に当たっては、磁気的消去又は物理的破壊等により、当該データを復元不可能な状態とする。 【税務総合支援システム（サーバー）】 ①課税から収入までの一連のサイクルを完了した課税データについて、電子データの削除等に関する規定に基づき、バッチ処理により削除している。 ②情報資産を破棄する場合、規定に基づきデータ消去ソフトウェア又はデータ消去装置によるデータ廃棄、あるいは、物理的な破壊又は磁気的な破壊によるデータ廃棄作業を行っている。 【紙媒体】 ①紙資料について、廃棄等に関する規定に基づき、保存期間経過後、職員の立会いのもとで溶解等により廃棄を行っている。運搬・廃棄にあたっては、委託先から適切に処理する旨の誓約書を徴取している。また、廃棄後にすべての書類等を廃棄したことを示す溶解証明を徴取している。 ②軽易な文書（資料文書）については、事務遂行上必要な期間の終了する日をもって随時に廃棄を行っている。 【外部記録媒体】 媒体内のデータは授受の都度、削除している。
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		
文書の保管契約、文書廃棄の溶解処理に係る運搬契約、文書廃棄の溶解処理契約において、「公文書等を一片たりとも散逸及び抜き取ることなく、またその内容や知り得た事項を外に漏らさず契約書の内容を厳守して処理を行う」旨の誓約書を委託業者から徴取するとともに、仕様書において、文書の安全管理や秘密の保護、作業方法、業者の資格等様々な条件を定め、リスクに対する措置を行っている。		

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

1．特定個人情報ファイル名	
②国税連携ファイル	
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	国税連携システム（eLTAX）は、地方税ポータルシステム（eLTAX）を通じて国税庁及び他地方公共団体としか繋がっていないことから、国税庁及び他道府県から送信される対象者の情報以外は入手できない。 なお、他道府県に課税権のあるデータがあることが判明した場合は、速やかに他道府県にデータを回送する。
必要な情報以外を入手することを防止するための措置の内容	国税連携システム（eLTAX）では、法令等により定められた様式を用いることで、必要な情報以外を入手することを防止している。
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：　不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	特定個人情報の入手元である国税庁及び他道府県は、使用目的が法令に基づくものであることを理解した上で提供を行っている。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク3：　入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	特定個人情報の入手元が番号法第16条の規定に基づき、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、都が国税庁及び他道府県から入手する際は番号法第16条が適用されない。
個人番号の真正性確認の措置の内容	特定個人情報の入手元が番号法第16条の規定に基づき、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、都が国税庁及び他道府県から入手する際は番号法第16条が適用されない。
特定個人情報の正確性確保の措置の内容	正確性の確保については、特定個人情報の入手元である国税庁に委ねられており、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行い、修正等行われた情報が国税庁や他道府県から送信されてくる。
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	・国税庁から地方税ポータルセンタ（eLTAX）までは、専用回線を利用するとともに、暗号化通信を行っている。 ・地方税ポータルセンタ（eLTAX）から国税連携システム（eLTAX）までは、閉域網であるLGWANを利用するとともに、暗号化通信を行っている。 ・セキュリティについては、「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」（平成25年5月1日総務省告示第206号）に定められた事項を順守するとともに、局内のセキュリティ実施手順において端末の管理に関する事項等を定め、順守することとしている。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	
―	

3. 特定個人情報の使用		
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容	国税連携システムから入手した情報と税務総合支援システムのあて名管理システムに登録されている納税義務者情報（氏名・住所）とを突合（検索）し、システム上に存在するあて名であるかどうかを確認して紐づけを行っている。目的外の情報の紐付けは行われない。	
事務で使用するその他のシステムにおける措置の内容	税務総合支援システムでは、税務事務に係るデータのみを保有しているため、税務事務以外の情報と紐付けることはできない。	
その他の措置の内容	－	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク		
ユーザ認証の管理	[行っている]	＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	・国税連携システムを使用する職員に対して、静脈等による生体認証およびID・パスワードを用いた認証の二要素認証を導入する。なお、IDについては職員毎に割り当てを行うものとする。 ・パスワードは3ヵ月に1度変更しなければならず、システム上も、同頻度でのパスワード変更を利用の必須条件としている。 ・操作内容は、操作ログとして保管されており、いつどのIDでログインしたのかを把握できるようにしている。	
アクセス権限の発効・失効の管理	[行っている]	＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	人事担当部署が職員の異動情報を把握又は公表次第、異動情報をシステム管理部署へ連絡している。これに基づき、システム管理部署が必要な権限を付与・削除している。	
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	・アクセス権限については、システム管理部署が全ての権限を一元的に管理しており、操作者の所属及び業務に合わせて、「データ管理・閲覧可」、「閲覧のみ可」の権限を設定している。 ・設定済の内容については、毎年度末に見直しを行うことにより、付与する権限に過不足が生じないようにしている。 ・権限に変更を加えた際には、システム管理部署が権限設定状況を示した一覧表を更新することにより、どの部署にどのような権限が設定されているのかを把握できるようにしている。	
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	システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、いつどの情報にアクセスし、抽出したのかが記録されている。また、操作履歴データは、暗号化により改竄や削除ができないようにしている。なお、記録は1年以上保存している。	
その他の措置の内容	・システム管理部署は、不正な操作の疑いがある場合には、参照情報と業務内容の関係性を確認している。 ・不正アクセスを未然に防ぐため、毎年実施する研修で上記作業を行うことについて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	・局内の規定において、原則、情報資産の外部持出しは禁止している。 ・これらを担保する手段として、国税連携システム端末での外部記憶媒体の使用を制限すること等により、容易に情報資産の持出しができないようにしている。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

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	・国税連携システム内の特定個人情報ファイルは、ソフトにより暗号化されているため、国税連携システム端末以外からデータを閲覧することはできない。 ・端末での外部記録媒体の使用を制限し、予期しないデータの取込み及び持出しができないようにしている。 ・ハードコピー等の紙資料については、取扱いに細心の注意を払うよう、研修や自己点検表等により注意喚起している。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	
・国税連携システム端末から印刷したハードコピー資料等の特定個人情報が記載されている紙資料について紛失や権限外の者に不正利用等されるリスクが想定されるが、紙資料については鍵の付いたロッカーに町名・氏名コード順にファイリングされて保管することで使用中のファイルがあれば分かるように並べており、退庁時には使用途中であっても必ずロッカーに全て返却し返却漏れがないか確認してから鍵を閉めて退庁している。 ・退庁後に特定個人情報等の書類のしまい忘れや鍵の閉め忘れがないかなどについて、他部署の執務室を相互点検するなどの措置を定期的に行っている。 ・特定個人情報ファイルについては、インターネットと接続している端末に転記・保存することのないよう規定し、徹底する。	

4．特定個人情報ファイルの取扱いの委託 [ ]委託しない	
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク	
情報保護管理体制の確認	【委託事項1～4】 ・委託契約で下記事項を規定し、確認している。 （1）責任者、作業体制、連絡体制及び作業場所の提出 （2）業務従事者への遵守事項の周知及び実施報告の提出 （3）再委託の承諾申請の提出 （4）作業担当者の名簿の提出 等 ・委託先がプライバシーマーク等を保有していることを確認している。 ・委託事項の内容、委託先等におけるリスクに応じて情報保護管理体制の確認を行っている。
特定個人情報ファイルの閲覧者・更新者の制限	[制限している] ＜選択肢＞ 1）制限している 2）制限していない
具体的な制限方法	【委託事項1～4】 ・委託先が使用するユーザIDは、局内のIDに関する規定に基づき、委託元が割り当てを行っている。 ・ユーザIDの設定に際しては、用途を確認した上で必要最小限の権限のみ付与し、使用する期間のみ有効とし、有効期間が経過した場合には当該ユーザIDでは特定個人情報ファイルを閲覧できないようにしている。

特定個人情報ファイルの取扱いの記録		[　　記録を残している　　] <選択肢> 1）記録を残している　2）記録を残していない
	具体的な方法	【委託事項1～4】 ・施錠された保管庫等での管理、管理状況の記録、管理記録の報告等を委託契約で規定している。 ・システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、いつどの情報にアクセスし、抽出したのかが記録されている。また、操作履歴データは、アクセス制御・暗号化により改竄や削除ができないようにしている。
特定個人情報の提供ルール		[　　定めている　　] <選択肢> 1）定めている　2）定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	【委託事項1～4】 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。
	委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	【委託事項1～4】 ① 委託先から他者への提供はない。なお、提供する必要性が発生する場合は、目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について契約で取り交わしている。 ② 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。 【委託事項2】 データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。
特定個人情報の消去ルール		[　　定めている　　] <選択肢> 1）定めている　2）定めていない
	ルールの内容及びルール遵守の確認方法	【委託事項1～4】 ・契約履行完了後に外部記憶媒体上に含まれる当該委託業務に係る情報を全て消去することを、委託契約で規定している。 ・消去した情報項目、数量、消去方法及び消去日等について報告書類等にて確認している。
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	・委託契約で下記事項を規定している。 【委託事項1、2、4】 （1）プログラム、データ等が格納されたサーバー及び端末機器等は、適切なアクセス権限を設定すること。 （2）外部記録媒体でやり取りするプログラム、データ等は、最新のパターンファイルを適用したウイルス対策ソフトでチェックすること。 【委託事項1～3】 （3）セキュリティ監査を実施する際は協力すること。 （4）委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく委託元に報告すること。
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	【委託事項1～4】 ・委託元と委託先の間で取り交わされている契約内容と同等の条件を再委託先においても課している。 ・委託元が再委託先に対して実地調査を定期的に行い、適切な管理体制をとっていることを確認している。 ・委託先が再委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく報告させている。
その他の措置の内容		・委託に関する契約書や仕様書及び受託者から受領する誓約書等の書類については、文書等の取扱に関する規定の保存期間に基づき保管している。 ・委託先に対し、作業場所へ業務に関係がない物の持込みを禁止する。
リスクへの対策は十分か		[　　十分である　　] <選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報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	国税連携システム（eLTAX）を利用して国税庁及び他都道府県へ提供する特定個人情報については、データ登録を行った職員や送信日時、送信先、送信状況等の当該提供記録をシステム上で記録をしている。（記録の保存期間は最大730日）
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	国税庁及び他道府県との間で行う提供等の作業については、局内のマニュアルやセキュリティに関する規定において国税連携システムでの提供方法等を規定している。具体的には、他道府県に提供する際には所属長の確認・決裁を得た上で通報処理簿に記録のうえ電子データでの通報を行っており、受領する際にも受報処理簿の記載等を行い適切に管理するよう事務処理方法についても定めている。
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	・国税庁及び他道府県に特定個人情報を提供するに当たっては所属長の確認・決裁を得てから提供しており、提供した内容等については通報処理簿に記録している。 ・また、国税連携システムにおいては、ユーザ認証を受けたアクセス権限のある者以外は操作できず、提供先として国税庁及び道府県以外を設定することはできない仕様となっている。 ・なお、地方税ポータルセンタ（eLTAX）と都道府県間は閉域網であるLGWAN，地方税ポータルセンタ（eLTAX）と国税庁間は専用回線を用いており、データも暗号化をしているため情報漏えいや紛失のリスクが軽減されている。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 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	・国税庁及び他道府県に特定個人情報を提供する際には、提供する対象者や提供する情報および提供先等について所属長の確認・決裁を得たもの以外は提供しておらず、提供した内容等については通報処理簿に記録している。 ・また、都と国税庁との間の情報連携については、提供先として国税庁及び市区町村以外を設定することはできない仕様になっている。都から地方税ポータルセンタ（eLTAX）までは閉域網であるLGWANが利用され、暗号化通信がされている。地方税ポータルセンタ（eLTAX）から国税庁までは、専用回線が利用され、暗号化通信がされており、決められた情報のみを提供するようにシステム的に担保している。 ・なお、他道府県との間の情報連携については、地方税ポータルセンタ（eLTAX）から他道府県までは、閉域網であるLGWANが利用されているほかは、同様である。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置	
―	

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

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1）特に力を入れて遵守している 2）十分に遵守している 3）十分に遵守していない 4）政府機関ではない
②安全管理体制	[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	【国税連携システム】 ・特定個人情報を保管するデータセンタは、都市計画法における防火・準防火地域に指定されていること、サーバー室等へ滞りなく電力を供給できる電源設備及び非常用自家発電設備を備えていること等の防災性を重視した条件により、選定している。 ・データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。 【外部記録媒体】 ・国税連携システムのデータ授受に使用する外部記録媒体（ハードディスク・USBフラッシュメモリ）は、施錠された保管庫で管理している。 【国税データ閲覧機能（サーバー）】 特定個人情報を保管するデータセンタは、浸水対策を施した場所に立地していること、データ保管に利用するキャビネット等を耐火仕様にすること、サーバー室等へ滞りなく電力を供給できる電源設備及び停電時にも機器の稼働を止めないための非常用自家発電設備を備えていること等の防災性を重視した条件により選定している。データセンタへの立ち入りはICカード所持者に限られている。また、サーバー室に入るためには、ICカードに加え、パスワード及び指紋認証を必要とする等、厳重なセキュリティ対策を行っている。	
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	【国税連携システム】 ・国税連携システム端末での外部記憶媒体の使用を制限し、予期しないデータの取り込み及び持ち出しができないようにしている。 ・サーバ、端末等の機器にはウイルス対策ソフトを適用するとともに、パターンファイルの更新を定期的に行うことにより、ウイルス感染を防止している。 ・地方税ポータルシステム（eLTAX）との接続は、LGWANを使用し、ファイアウォールを適用するとともに、接続状況を監視することにより、不正接続への対策を行っている。 【国税データ閲覧機能（サーバー）】 契約書の中にサーバー室の入退出管理を行うこと、7年保存するという契約履行完了時には、業務に係る情報を記録した一切の媒体については、記録媒体上に含まれる当該委託業務に係る情報を全て消去して、その消去結果について、記録媒体ごとに、消去した情報項目、数量、消去方法及び消去日等を明示した書面で委託者に報告すること、受託者は、アクセスを許可する情報の種類と範囲、アクセス方法について、業務着手前に委託者から承認を得ること等が規定されている。	
⑦バックアップ	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生あり]	<選択肢> 1）発生あり 2）発生なし

	その内容	①令和4年5月、東京都現代美術館において、ミュージアムショップ運営の受託事業者スタッフが、展覧会図録を予約した顧客へ一斉に案内メールを送信する際、メールアドレスをBCC欄ではなく、宛先欄に入力して発信した。 ②令和4年5月、技能検定試験に関する通知を外国人技能実習の複数の監理団体に対しメールで送付する際、誤ってメールアドレスをBCC欄ではなく、CC欄に入力し、一斉送信した。 ③令和4年5月、就学支援金事務において、就学支援金の基礎データをCD-Rに情報を保存し、対象高等学校等宛て一斉に送付したところ、そのうち1校に、他校の受給者に関する情報が含まれていることが判明した。 ④令和4年5月、受託事業者が、事業に関するイベントを案内するメールマガジンを送付する際、配信プログラム改修ミスにより、宛先欄に複数のメールアドレスが入力され、送信された。 ⑤令和4年10月、東京都陽性者登録センターの運営受託事業者が、医療機関で新型コロナウイルス陽性の診断を受け、センターに登録申請を行った複数の患者への登録完了メールを、送付先アドレスが全て入れ替わったまま送信した。 ⑥令和4年12月、労働力調査の統計調査員に対して連絡事項をメールした際、BCC欄に入力して送るべきところを宛先欄に入力し、一斉送信した。 ⑦令和5年4月、再委託先の派遣会社職員が、業務で使用するシステムを不適切に使用し、個人情報を閲覧、メモにとり自宅に持ち出した。 ⑧令和5年5月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑨令和5年6月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑩令和5年7月、施設を退所する患者に関して、退所先候補の施設と受入調整を行うため、診療関係書類をFAX送信した際、誤って別のFAX番号宛てに送信した。 ⑪令和5年8月、申請により受け付けた申請書が紛失していることが発覚した。 ⑫令和5年9月、関係施設宛に都民情報をFAX送信した際、誤って別の事業者宛てに送信した。 ⑬令和5年9月、事業の対象者に案内チラシを郵送した際、送付対象者の抽出ツールのプログラム仕様の不備により、誤って事業対象外の方に送付したことで、旧住所宛てに送付し返戻されなかったものが誤送付となった。 ⑭令和5年9月、決定通知書に公印を押印する目的で本庁に出張し、押印後持ち帰ったが、発送の準備をしていた際に、通知書1枚が紛失していることが発覚した。 ⑮令和6年1月、患者A宛てに送付すべき利用者情報を、誤ってB宛てに送付した。 ⑯令和6年1月、入所者の診療関係ファイルが紛失していることが発覚し、その後、退所者の荷物の中に当該ファイルが混入していたことが発覚した。 ⑰令和6年2月、児童相談所の職員が、出張中に個人情報が記載されている手帳を紛失し、あわせて手帳に収納されていた、当該職員の証票及び所内職員の緊急連絡網を紛失した。 ⑱令和6年2月、施設を退所した患者Aに関する薬剤情報等を記載した書類を、誤って別の患者の退院時の荷物に混入させ交付した。 ⑲令和6年2月、オンライン研修で使用した映像において、患者の情報をマスキング処理していたところ、当該映像をスマートフォンで視聴した場合に、マスキングが外れ、個人が特定できる状態になっていたことが判明した。 ⑳令和6年4月、受け付けた申請書を紛失していることが発覚した。 ㉑令和6年4月、施設職員が、利用者の通院付添の際、処方箋を紛失した。 ㉒令和6年4月、指定管理者が、事業者に対してExcel資料をメールで送信した際、本来削除すべきだった個人情報の入力されたシートを削除しなかった。 ㉓令和6年7月、受託事業者が、都へ交付すべき納入済通知書を、誤って他の事業者宛てに交付したことが発覚した。 ㉔令和6年7月、受託事業者がイベントを行った際の申込時の個人情報が掲載されたウェブページが、一時外部からアクセス可能な状態となっていたことが発覚した。 ㉕令和6年7月、職員が、説明会の資料の中に個人情報が含まれていることに気が付かずに、各自治体にデータを配布した。 ㉖令和6年7月、職員が、A宛てに送付すべき個人情報を、誤ってB宛てに送付していたことが発覚した。 ㉗令和6年7月、受託事業者から送付した個人情報を含む資料が、紛失していることが発覚した。 ㉘令和6年7月、受け付けた申請書を紛失していることが発覚した。 ㉙令和6年8月、受託事業者が配付した資料の中に、個人情報等が含まれる資料が混入していたことが発覚した。 ㉚令和6年10月、職員が、受託者に資料をメールで送信した際、誤って個人情報が記載された別のファイルを添付した。 ㉛令和6年10月、受託事業者が、A宛てに送付すべき電話記録を、誤ってB宛てにFAXで送信した。 ㉜令和6年11月、受け付けた申請書を紛失していることが発覚した（後日発見）。 ㉝令和6年11月、令和3年頃に個人情報が記載された資料を紛失していたことが発覚した。 ㉞令和6年12月、受託事業者が、個人情報が記載された資料を、誤って外部へ送信した。 ㉟令和7年1月、受託事業者が、個人情報が記載された資料を、誤って期限前に廃棄した。 ㊱令和7年1月、受け付けた届出書が、誤って机ごと廃棄されていることが発覚した。

	再発防止策の内容	①（1）ミュージアムショップにおいて、本社セキュリティインシデント統括部と連携して、個人情報取り扱い、情報管理体制の改善を行う。 （2）特に複数人へのメール送信に際してはダブルチェックを徹底する。 （3）現代美術館全委託業者に、適切な個人情報等の取扱い及び情報管理を徹底するよう指示する。 （4）財団が管理運営する各施設にも本事案を共有し、個人情報を含む情報の適切な管理を徹底する。 ②（1）個人情報の取扱い及び情報管理の徹底等について周知するとともに、職員全員に臨時研修を速やかに実施 （2）誤送信防止に向けたシステムの導入（ダイアログの自動表示など） （3）複数人チェックなど基本的対策の徹底 ③チェック機能を再検証し、全日制等と同様の仕組みを通信制にも直ちに導入するほか、事務フローの再構築を行い、再発防止に努める。そのうえで、本件を財団内で広く共有させ、個人情報の取扱い全般についてハード・ソフトの両面から厳しく見直すとともに、職員の意識向上を図っていく。また、都の実施機関においても個人情報の適正管理とサイバーセキュリティー対策について改めて確認を行う。 ④（1）システムの改善 メールマガジンの配信は、これまで「TO」により自動で1件ずつ送信がされる仕組みであったが、一括メール送信においては送信者アドレスを全て「BCC」に入れるようシステム改修を行う。 （2）システム会社における確認体制の強化 開発前にシステム会社が実施する、影響調査・テスト内容等について、これまでの2名体制によるダブルチェックから、システム会社のプロジェクトマネージャーも加えることとし、確認した内容を報告させて承認する運用へ見直す。 （3）受託事業者における確認体制の強化 システム会社のテスト結果の確認にあたっては、テストの証跡情報の提出を求め、内容の確認を行うとともに、受託事業者での運用テストでは要件定義とも照らした確認を担当だけでなく管理職も実施することにより徹底する。 ⑤受託事業者に対して厳正に指導し、登録完了メール送信作業のチェック体制を強化させる。 ⑥（1）部コンプライアンス推進委員会の臨時開催 ・メール送信時のダブルチェックを徹底させるため、個人情報等の取扱いに係るチェックリストの全職員での点検により注意を喚起、情報管理を再徹底する。 ・あわせて、最近の事故事案の事例を周知するなど、事故の再発予防を進める。 （2）定期的な事故防止意識の醸成 統計調査員を含む全職員を対象に、各所属長や指導員から情報セキュリティや感染拡大防止等に関する指導を定期・継続的に行い、危機意識の醸成等を図る。 ⑦委託先における個人情報の閲覧・使用に当たっての権限の設定や、不適切な閲覧・使用・持ち出しを防止するための体制についてあらためて確認し、適切な運用を徹底させる。 ⑧（1）情報共有をしているホワイトボードの位置、記入欄が分かりにくいとの意見が出 ため、位置、記入方法について変更した。 （2）書類封入時のチェック手順中に、患者氏名の確認を明示した。 （3）2者確認を徹底するため、事務員のみでなく看護職員もチェックを行うこととし、 2者チェックが終わった段階で封書のチェックボックスに記載する。 （4）責任の所在を明確にするため「転院時退所セット確認書」を新たに作成し、チェックを行った職員が記名する。 ⑨（1）チェックリストを活用し、複数人、複数回のチェックを行うとともに、最終チェック者を統括責任者とすることで、誤封入等を防ぐ体制を整える。 （2）都職員が施設へ直接出向き、個人情報管理の実態確認を実施するとともに、対応 が不十分な場合は是正指導を行う。 （3）個人情報保護の研修を実施し、施設全体で個人情報保護の取り組み状況を共有した上で、改善を徹底する。 ⑩（1）委託先に対し、個人情報に関する業務手順を見直し及び徹底を図ることや、全従 事者に対する個人情報保護研修を行うことを指導した。また、改善策の確認のため、都が施設へ出向き、個人情報管理の実態を確認した。 （2）再委託先において、送付の際は、まずFAX以外の手段を調整し、止むを得ずFAXを使用する際には、FAX番号の聞き取りの際の復唱や、FAX送信前の送信先への番号の再確認、複数人で複数回のチェックを必ず行うこととした。また、全従業者に対する個人情報保護研修を行った。 ⑪（1）作業環境等を見直し、書類の混入等が起きにくい環境を整備 ①執務室内の作業スペースの確保及び活用 ②引き出し付きの棚をキャビネット内に新設し、書類の分類をよりしやすくした。 （2）委託業者との書類の受け渡し方法の変更（送付する判定機関ごとに数を確認しながら受け渡す）。 ⑫個人情報をFAX送信することを禁止するよう各施設に通知した。 ⑬抽出ツールのプログラム確認は、委託先事業者の運用チームのみが行っていたが、抽出ツールを作成・利用する際には、運用チームに加えて、開発チームと委託元である都の3者で抽出ツールのプログラムの仕様・設定を確認することとした。 ⑭個人情報の持出、返却確認及び受け渡しの際の確認の徹底を行う。また、作業工程等を点検し、作業方法やチェック方法等ミスが起きにくい方法を検討、実施する。 ⑮郵便の発送作業は複数職員でチェックすることを再徹底。また、特に慎重を要する個人情報を取り扱う施設における個人情報の事故の重大性について改めて周知するとともに、書類の発送、保管、業務の進行管理等について、注意喚起や指導を行った。 ⑯（1）ファイルが他の物に紛れてしまわないよう、目立つ色に変更する。 （2）作業スペースに仕切りを立てて、使用スペースを物理的に限定する。 （3）ファイルに記載する名前をイニシャルに表記変更する等、使用する情報から個人情報を削除する。 （4）決まった時間に決まった人員が所在を確認する。 （5）チェックの時間を定刻とし、声をかけ合う。 （6）出したらしまうといった基本的事項を、改めて徹底するよう、注意喚起する。 （7）急いでいたり、忙しい時間帯でも、ダブルチェックをするよう、改めて徹底する。また、退所時にも荷物を確認してから渡すようにする ⑰（個人情報の管理について） （1） 相談援助業務上の記録をノート等に記載する場合は、イニシャルを使用するなど個人情報を特定されないようにすること。また、私物のノートや手帳に個人情報を記載しないこと。 （2） 庁舎外での会議等に出席した際には、個人端末を活用して記録の作成を行うとともに、作成した文書は暗号化し保存すること。 （3） 業務上やむを得ず個人情報が記録された書類を庁舎外に持ち出す場合は、局の保有個人情報安全管理基準に基づき管理職の許可を得ること。 （4） 個人情報を含む書類を持ち出すにあたっては、盗難や紛失を防止できる形状・機能を持つ鞄に収納し、肌身離さず持ち運ぶなど十分に注意すること。 （5） その他個人情報の取り扱いについては、局の保有個人情報安全管理基準等を遵守し、適正に行うこと。 （職員の証票の管理について） （1） 月1回、各職員の保有状況を点検すること （2） 携行する際には、ストラップ付きのケースに収納するなど、常に身体から離さずに携行することを徹底すること （職員の緊急連絡網の管理について） （1） 必要な連絡先は公用携帯に保存し、連絡網を記載した紙は庁舎外に持ち出さないこと。 ⑱（1）入所時や退所時の手順確認のチェックリスト様式を変更し、入所時の写真撮影やリストへの正確な情報記載、退所時の荷物確認の手順など守るべきルールを追記するとともに、実施者を記載する欄を追加。 （2）個人情報紛失判明時の、本部への速やかな報告や具体的な捜索の手順などを、チェックリストに追記。 （3）毎朝のミーティングにてリーダー看護師等に個人情報保護の重要性やルールの順守を徹底。勤務者には、業務実施前に最新のマニュアルを確認するよう指導。 ⑲（1）発表資料の事前確認の徹底について幹部会で決定し、各部署に注意喚起 （2）録画や写真撮影をして保管していない旨を書面で確認 （3）画像等の個人情報の収集・利用に関する同意手続きの見直し ⑳（1）電子申請を推奨して紙文書の紛失リスクを軽減 （2）個人情報の適切な管理を職員に改めて周知徹底 ㉑（1）病院へ持ち運ぶファイルに、処方箋を収納する専用スペースを作る （2）医療機関受診時に係るマニュアルを作成 （3）帰園後は可能な限り速やかに所管部署に処方箋等を提出する （4）重要な個人情報を預かっている状況での裁断作業を避ける （5）上記対応について、ミーティング等で周知徹底、注意喚起 ㉒（1）必要なデータファイルのみを送信用データとしてPDF化し、送信前に、PDFに不要な箇所が入っていないことを確認の上、送信することを徹底 （2）メールシステム上、外部送信時に必須である上長の承認の際、個人情報が含まれていないか等の確認を徹底 （3）「メール送信時のセルフチェックリスト」を作成、活用 （4）各管理職より各職員に対する面談時に、個別に再発防止策を徹底

		(4)各管理職より各職員に対する面談時に、個別に再度、再発防止策を徹底 ㉓(1)交付前の事務手順や確認方法の見直し、交付時の最終確認方法の見直し (2)作業スペースへの注意文の掲示やチェックリストへの注意文の記載 (3)確認等を行う人数を増員し、誤交付を防ぐ体制を強化 (4)再発防止勉強会を実施 ㉔(1)委託事業者及び再委託事業者に厳重注意、再発防止策等の作成を指示し、受領 (2)WEBページの脆弱性等の確認を受けるため、デジタルサービス局との調整を開始 ㉕(1)精査が十分でないデータを外部に提供しないこと、精査及び送付の際には複数体制でチェックすることを徹底 (2)受託事業者において、作成した資料のレビューフローの再検討、個人情報データの受領・管理方法に関する社内再教育等の取組を実施 ㉖(1)ダブルチェックの徹底及びその旨の指導 (2)作業項目の文章化、わかりやすいチェックリストの作成 ㉗(1)受託事業者において、マニュアルに沿った処理を徹底し、送付書類の引継ぎ時には、郵便局ともに引継ぎ件数ーを確認 (2)3か月間、受託事業者から送付先に対し、発送日の連絡及び到着の確認を行う。 ㉘(1)原則電子申請として紙文書の紛失リスクを軽減 (2) 書類の所在及び処理状況を明確に把握できるよう管理方法を見直す ㉙(1)個人情報の取扱い及び情報管理の徹底等について、厳重に注意喚起 (2)個人情報が特定できない記載にする等の対策 ㉚(1)局内各職場にて個人情報事故防止対策等をテーマとした職場討議実施 (2)個人情報安全管理強化月間の自己点検・職場点検による一層の意識啓発 ㉛(1)張り紙の掲示、FAXボタンへの着色による物理的な注意喚起 (2)FAX送付時のダブルチェック、送信履歴の確認等をマニュアルに追加 ㉜(1)区市町村からの書類を収受する際の件数記載用の共通様式を作成し、受領時に種類ごとの件数を確認・記入 (2)本件の事務のプロセスを細分化し、各プロセス毎の書類の受渡し時に、各担当者がそれぞれ(1)の様式に記載した件数に基づき、書類、件数の確認作業を行うよう整理 (3)使用頻度ごとに文書の保管場所を整理し、常時使用しないものは施錠。作業中に開錠しているキャビネットについても、中に担当者ごとの鍵付きの引き出し等を設置して自分の担当以外の書類は持ち出せないようにし、作業の際にその都度施錠。 (4)緊急の所内幹部会を開催し、個人情報を含む書類の受け渡し時の確認等、個人情報の取り扱いのルールが適正に行われているか確認を指示し、報告を受ける。 ㉝(1)個人情報の保管ルールについて全職員に徹底 (2)現在の保管状況の再点検を実施 ㉞(1)受託事業者に対する個人情報の取扱い及び情報管理の徹底に向けた注意喚起 (2)管理番号の活用など個人情報が特定できない情報管理方法等の導入 ㉟(1)廃棄時の職員立会いの徹底、チェックリストの作成、活用 (2)廃棄対象文書とシステム登録情報の照会の実施 ㊱書類の保管場所の見直し
⑩死者の個人番号		[保管している] ＜選択肢＞ 1) 保管している 2) 保管していない
	具体的な保管方法	生存者の個人番号と同様の方法にて安全管理措置を実施している。
その他の措置の内容		バックアップデータについても、システムで使用している元データと同様の方法にて安全管理措置を実施している。
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク2： 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	・国税庁・税務署に提出された所得税・法人税の訂正申告、修正申告、更正決議書等についてもデータの提供を受けており最新情報の取り込み処理も行っている。 ・納税義務者の異動に際しては、法令等に則り、適切に届出等を行うよう周知を行っている。 ・税務調査で異動の事実が判明した場合は、情報の更新を行っている。	
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	【国税連携システム（サーバー）】 一定期間を経過したデータは、電子データの削除等に関する規定に基づき、職員によるオンライン処理により削除している。 【外部記録媒体】 データ移行のため、外部記録媒体（ハードディスク）、USBフラッシュメモリに一時保存したデータについては、移行後直ちに職員が手作業で消去している。	
その他の措置の内容	ー	
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		
仕様書において、文書の安全管理や秘密の保護、作業方法、業者の資格等様々な条件を定め、リスクに対する措置を行っている。		

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

1. 特定個人情報ファイル名	
③電子申告ファイル	
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	・申告義務のある者については、地方税法に規定されている。 ・手引きやホームページにて申告義務のある者について解説し、対象者以外の情報入手を未然に防いでいる。 ・地方税ポータルセンタ（eLTAX）では、申告等を行う者以外からは情報を受け付けないようにシステムで制御している。eLTAXを利用するためには、利用届出を提出し、利用者IDと暗証番号を取得して、電子証明書を登録する必要がある。申告等の手続きの際に添付される電子証明書と登録情報との確認を行い、本人確認を実施している。 ・利用届出や申告データ等に記載された提出先により、審査システム（eLTAX）が地方税ポータルセンタ（eLTAX）から取得できる情報をシステムで制御している。
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	・申告データには様式の定めがあり、必要でない情報等を入力することはできない。 ・手引きやホームページにて申告義務のある者について解説し、対象者以外の情報入手を防止している。 ・審査システム（eLTAX）では、法令等により定められた様式を受領することから、必要な情報以外の入手を防止している。
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： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	納税義務者に提出を求める申告データ及び様式には定めがあり、当該データに入力する情報が課税及び徴税事務に使用されることを認識したうえでデータを提出する。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	番号法の規定に基づき、公的個人認証による電子署名を確認するなどの方法により、本人確認の措置をとる。
個人番号の真正性確認の措置の内容	・番号法の規定に基づき、地方公共団体情報システム機構へ確認するなどの方法により、個人番号の真正性確認の措置をとる。 ・地方税共同機構による、申告データと真正性確認済の個人番号情報との突合により、当該申告データ上の個人番号の真正性確認の措置をとる。
特定個人情報の正確性確保の措置の内容	審査システム（eLTAX）は、地方税ポータルセンタ（eLTAX）で受け付けた情報を、原本として保存するシステムであるため、受領した情報が改変されることはない。
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	・納税義務者から地方税ポータルセンタ（eLTAX）までのインターネット回線については、暗号化通信を行っている。 ・地方税ポータルセンタ（eLTAX）から審査システム（eLTAX）までは、閉域網であるLGWANを利用するとともに、暗号化通信を行っている。 ・審査システム（eLTAX）から税務総合支援システムまでは、運用拠点内において外部記録媒体によるデータの受け渡しを行っており、外部への持ち出しは行っていない。
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
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	
―	

3. 特定個人情報の使用		
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容		審査システム（eLTAX）は、都における宛名システム等との接続はない。
事務で使用するその他のシステムにおける措置の内容		審査システム（eLTAX）では、税務事務に係るデータのみを保有しているため、税務事務以外の情報と紐付けることはできない。
その他の措置の内容		―
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク		
ユーザ認証の管理		[行っている] ＜選択肢＞ 1）行っている 2）行っていない
	具体的な管理方法	・電子申告システムを使用する職員に対して、静脈等による生体認証およびID・パスワードを用いた認証の二要素認証を導入する。なお、IDについては職員毎に割り当てを行うものとする。 ・パスワードは3ヵ月に1度変更しなければならず、システム上も、同頻度でのパスワード変更を利用の必須条件としている。 ・操作内容は、システム稼働当初から現在に至るまで操作ログとして保管されており、いつどのIDでログインしたのかを把握できるようにしている。
アクセス権限の発効・失効の管理		[行っている] ＜選択肢＞ 1）行っている 2）行っていない
	具体的な管理方法	人事担当部署が職員の異動情報を把握又は公表次第、異動情報をシステム管理部署へ連絡している。これに基づき、システム管理部署が必要な権限を付与・削除している。
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	・アクセス権限については、システム管理部署が全ての権限を一元的に管理しており、操作者の所属及び業務に合わせて、システムの機能ごとに「更新・参照可」、「参照のみ可」、「更新・参照不可」の権限を設定している。 ・設定済の内容については、毎年度末に見直しを行うことにより、付与する権限に過不足が生じないようにしている。 ・権限に変更を加えた際には、システム管理部署が権限設定状況を示した一覧表を更新することにより、どの部署にどのような権限が設定されているのかを把握できるようにしている。
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	システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、いつどの情報にアクセスし、抽出したのかが記録されている。また、操作履歴データは、暗号化により改竄や削除ができないようにしている。なお、記録は1年以上保存している。
その他の措置の内容		・システム管理部署は、不正な操作の疑いがある場合には、参照情報と業務内容の関係性を確認している。 ・不正アクセスを未然に防ぐため、毎年実施する研修で上記作業を行うことについて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	・局内の規定において、原則、情報資産の外部持出しは禁止している。 ・これらを担保する手段として、審査システム端末での外部記憶媒体の使用を制限すること等により、容易に情報資産の持出しができないようにしている。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
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	・「電子申告システム内の特定個人情報ファイルは、ソフトにより暗号化されているため、審査システム端末以外からデータを閲覧することはできない。 ・端末での外部記録媒体の使用を制限し、予期しないデータの取込み及び持出しができないようにしている。 ・ハードコピー等の紙資料については、取扱いに細心の注意を払うよう、研修や自己点検表等により注意喚起している。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	
―	

4. 特定個人情報ファイルの取扱いの委託		[　　] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認		【委託事項1～3】 ・委託契約で下記事項を規定し、確認している。 （1）責任者、作業体制、連絡体制及び作業場所の提出 （2）業務従事者への遵守事項の周知及び実施報告の提出 （3）再委託の承諾申請の提出 （4）作業担当者の名簿の提出　等 ・委託先がプライバシーマーク等を保有していることを確認している。
特定個人情報ファイルの閲覧者・更新者の制限		[　　制限している　　] ＜選択肢＞ 1）制限している　　2）制限していない
	具体的な制限方法	【委託事項1～3】 ・委託先が使用するユーザIDは、局内のIDに関する規定に基づき、委託元が割り当てを行っている。 ・ユーザIDの設定に際しては、用途を確認した上で必要最小限の権限のみ付与し、使用する期間のみ有効とし、有効期間が経過した場合には当該ユーザIDでは特定個人情報ファイルを閲覧できないようにしている。
特定個人情報ファイルの取扱いの記録		[　　記録を残している　　] ＜選択肢＞ 1）記録を残している　　2）記録を残していない
	具体的な方法	【委託事項1～3】 ・施錠された保管庫等での管理、管理状況の記録、管理記録の報告等を委託契約で規定している。 ・システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、いつどの情報にアクセスし、抽出したのかが記録されている。また、操作履歴データは、アクセス制御・暗号化により改竄や削除ができないようにしている。
特定個人情報の提供ルール		[　　定めている　　] ＜選択肢＞ 1）定めている　　2）定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	【委託事項1～3】 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。
	委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	【委託事項1～3】 ① 委託先から他者への提供はない。なお、提供する必要性が発生する場合は、目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について契約で取り交わしている。 ② 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。 【委託事項2】 データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。
特定個人情報の消去ルール		[　　定めている　　] ＜選択肢＞ 1）定めている　　2）定めていない
	ルールの内容及びルール遵守の確認方法	【委託事項1～3】 ・契約履行完了後に外部記憶媒体上に含まれる当該委託業務に係る情報を全て消去することを、委託契約で規定している。 ・消去した情報項目、数量、消去方法及び消去日等について報告書類等にて確認している。
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	・委託契約で下記事項を規定している。 【委託事項1、2】 （1）プログラム、データ等が格納されたサーバー及び端末機器等は、適切なアクセス権限を設定すること。 （2）外部記録媒体でやり取りするプログラム、データ等は、最新のパターンファイルを適用したウイルス対策ソフトでチェックすること。 【委託事項1～3】 （3）セキュリティ監査を実施する際は協力すること。 （4）委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく委託元に報告すること。

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	【委託事項1～3】 ・委託元と委託先の間で取り交わされている契約内容と同等の条件を再委託先においても課している。 ・委託元が再委託先に対して実地調査を定期的に行い、適切な管理体制をとっていることを確認している。 ・委託先が再委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく報告させている。
その他の措置の内容		・委託に関する契約書や仕様書及び受託者から受領する誓約書等の書類については、文書等の取扱に関する規定の保存期間に基づき保管している。 ・委託先に対し、作業場所へ業務に関係がない物の持込みを禁止する。
リスクへの対策は十分か		[　十分である　] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報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	提供の記録（提供を受ける者の名称、提供の日時、提供する特定個人情報の項目等）を作成し、7年間保管する。
特定個人情報の提供・移転に関するルール		[　定めている　] ＜選択肢＞ 1）定めている 2）定めていない
	ルールの内容及びルール遵守の確認方法	・審査システム（eLTAX）を利用して地方税共同機構へ提供する特定個人情報については、納税者IDと個人番号のみの送信を行う。 ・データ作成及び送信方法の手順を定め、管理者の承認を得た上で送信を行う。
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
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		・税務総合支援システムから審査システム（eLTAX）までは、同一センタ内又は同一執務室内において外部記録媒体によるデータの受渡しを行っており、外部への持ち出しは行っていない。 ・審査システム（eLTAX）から地方税ポータルセンタ（eLTAX）までは、閉域網であるLGWANを利用するとともに、暗号化通信を行っている。
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： 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		・審査システム（eLTAX）から地方税ポータルセンタ（eLTAX）までは、閉域網であるLGWANを利用するとともに、暗号化通信を行っており、決められた情報のみを提供するようにシステム上担保している。 ・システム上、提供先として地方税共同機構以外を設定することはできない仕様になっている。
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
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		
―		

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

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	＜選択肢＞ 1）特に力を入れて遵守している 2）十分に遵守している 3）十分に遵守していない 4）政府機関ではない
②安全管理体制	[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	【審査システム（サーバー）】 ・特定個人情報を保管するデータセンタは、都市計画法における防火・準防火地域に指定されていること、サーバー室等へ滞りなく電力を供給できる電源設備及び非常用自家発電設備を備えていること等の防災性を重視した条件により、選定している。 ・データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。 【外部記録媒体】 ・審査システムのデータ授受に使用する外部記録媒体（ハードディスク・USBフラッシュメモリ）は、施錠された保管庫で管理している。	
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	【審査システム】 ・ 審査システム端末での外部記憶媒体の使用を制限し、予期しないデータの取り込み及び持ち出しができないようにしている。 ・ データはソフトにより暗号化されているため、審査システム端末以外からデータを閲覧することはできない。 ・ サーバー、端末等の機器にはウイルス対策ソフトを適用するとともに、パターンファイルの更新を定期的に行うことにより、ウイルス感染を防止している。 ・ 地方税ポータルシステム（eLTAX）との接続は、LGWANを使用し、ファイアウォールを適用するとともに、接続状況を監視することにより、不正接続への対策を行っている。	
⑦バックアップ	[十分に行っている]	＜選択肢＞ 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知	[十分に行っている]	＜選択肢＞ 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生あり]	＜選択肢＞ 1）発生あり 2）発生なし

	その内容	①令和４年５月、東京都現代美術館において、ミュージアムショップ運営の受託事業者スタッフが、展覧会図録を予約した顧客へ一斉に案内メールを送信する際、メールアドレスをBCC欄ではなく、宛先欄に入力して発信した。 ②令和４年５月、技能検定試験に関する通知を外国人技能実習の複数の監理団体に対しメールで送付する際、誤ってメールアドレスをBCC欄ではなく、CC欄に入力し、一斉送信した。 ③令和４年５月、就学支援金事務において、就学支援金の基礎データをCD-Rに情報を保存し、対象高等学校等宛て一斉に送付したところ、そのうち１校に、他校の受給者に関する情報が含まれていることが判明した。 ④令和４年５月、受託事業者が、事業に関するイベントを案内するメールマガジンを送付する際、配信プログラム改修ミスにより、宛先欄に複数のメールアドレスが入力され、送信された。 ⑤令和４年10月、東京都陽性者登録センターの運営受託事業者が、医療機関で新型コロナウイルス陽性の診断を受け、センターに登録申請を行った複数の患者への登録完了メールを、送付先アドレスが全て入れ替わったまま送信した。 ⑥令和４年12月、労働力調査の統計調査員に対して連絡事項をメールした際、BCC欄に入力して送るべきところを宛先欄に入力し、一斉送信した。 ⑦令和５年４月、再委託先の派遣会社職員が、業務で使用するシステムを不適切に使用し、個人情報を閲覧、メモにとり自宅に持ち出した。 ⑧令和５年５月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑨令和５年６月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑩令和５年７月、施設を退所する患者に関して、退所先候補の施設と受入調整を行うため、診療関係書類をFAX送信した際、誤って別のFAX番号宛てに送信した。 ⑪令和５年８月、申請により受け付けた申請書が紛失していることが発覚した。 ⑫令和５年９月、関係施設宛に都民情報をFAX送信した際、誤って別の事業者宛てに送信した。 ⑬令和５年９月、事業の対象者に案内チラシを郵送した際、送付対象者の抽出ツールのプログラム仕様の不備により、誤って事業対象外の方に送付したことで、旧住所宛てに送付し返戻されなかったものが誤送付となった。 ⑭令和５年９月、決定通知書に公印を押印する目的で本庁に出張し、押印後持ち帰ったが、発送の準備をしていた際に、通知書１枚が紛失していることが発覚した。 ⑮令和６年１月、患者A宛てに送付すべき利用者情報を、誤ってB宛てに送付した。 ⑯令和６年１月、入所者の診療関係ファイルが紛失していることが発覚し、その後、退所者の荷物の中に当該ファイルが混入していたことが発覚した。 ⑰令和６年２月、児童相談所の職員が、出張中に個人情報が記載されている手帳を紛失し、あわせて手帳に収納されていた、当該職員の証票及び所内職員の緊急連絡網を紛失した。 ⑱令和６年２月、施設を退所した患者Aに関する薬剤情報等を記載した書類を、誤って別の患者の退院時の荷物に混入させ交付した。 ⑲令和６年２月、オンライン研修で使用した映像において、患者の情報をマスキング処理していたところ、当該映像をスマートフォンで視聴した場合に、マスキングが外れ、個人が特定できる状態になっていたことが判明した。 ⑳令和６年４月、受け付けた申請書を紛失していることが発覚した。 ㉑令和６年４月、施設職員が、利用者の通院付添の際、処方箋を紛失した。 ㉒令和６年４月、指定管理者が、事業者に対してExcel資料をメールで送信した際、本来削除すべきだった個人情報の入力されたシートを削除しなかった。 ㉓令和６年７月、受託事業者が、都へ交付すべき納入済通知書を、誤って他の事業者宛てに交付したことが発覚した。 ㉔令和６年７月、受託事業者がイベントを行った際の申込時の個人情報が掲載されたウェブページが、一時外部からアクセス可能な状態となっていたことが発覚した。 ㉕令和６年７月、職員が、説明会の資料の中に個人情報が含まれていることに気が付かずに、各自治体にデータを配布した。 ㉖令和６年７月、職員が、A宛てに送付すべき個人情報を、誤ってB宛てに送付していたことが発覚した。 ㉗令和６年７月、受託事業者から送付した個人情報を含む資料が、紛失していることが発覚した。 ㉘令和６年７月、受け付けた申請書を紛失していることが発覚した。 ㉙令和６年８月、受託事業者が配付した資料の中に、個人情報等が含まれる資料が混入していたことが発覚した。 ㉚令和６年10月、職員が、受託者に資料をメールで送信した際、誤って個人情報が記載された別のファイルを添付した。 ㉛令和６年10月、受託事業者が、A宛てに送付すべき電話記録を、誤ってB宛てにFAXで送信した。 ㉜令和６年11月、受け付けた申請書を紛失していることが発覚した（後日発見）。 ㉝令和６年11月、令和３年頃に個人情報が記載された資料を紛失していたことが発覚した。 ㉞令和６年12月、受託事業者が、個人情報が記載された資料を、誤って外部へ送信した。 ㉟令和７年１月、受託事業者が、個人情報が記載された資料を、誤って期限前に廃棄した。 ㊱令和７年１月、受け付けた届出書が、誤って机ごと廃棄されていることが発覚した。

	再発防止策の内容	①（1）ミュージアムショップにおいて、本社セキュリティインシデント統括部と連携して、個人情報取り扱い、情報管理体制の改善を行う。 （2）特に複数人へのメール送信に際してはダブルチェックを徹底する。 （3）現代美術館全委託業者に、適切な個人情報等の取扱い及び情報管理を徹底するよう指示する。 （4）財団が管理運営する各施設にも本事案を共有し、個人情報を含む情報の適切な管理を徹底する。 ②（1）個人情報の取扱い及び情報管理の徹底等について周知するとともに、職員全員に臨時研修を速やかに実施 （2）誤送信防止に向けたシステムの導入（ダイアログの自動表示など） （3）複数人チェックなど基本的対策の徹底 ③チェック機能を再検証し、全日制等と同様の仕組みを通信制にも直ちに導入するほか、事務フローの再構築を行い、再発防止に努める。そのうえで、本件を財団内で広く共有させ、個人情報の取扱い全般についてハード・ソフトの両面から厳しく見直すとともに、職員の意識向上を図っていく。また、都の実施機関においても個人情報の適正管理とサイバーセキュリティー対策について改めて確認を行う。 ④（1）システムの改善 メールマガジンの配信は、これまで「TO」により自動で1件ずつ送信がされる仕組みであったが、一括メール送信においては送信者アドレスを全て「BCC」に入れるようシステム改修を行う。 （2）システム会社における確認体制の強化 開発前にシステム会社が実施する、影響調査・テスト内容等について、これまでの2名体制によるダブルチェックから、システム会社のプロジェクトマネージャーも加えることとし、確認した内容を報告させて承認する運用へ見直す。 （3）受託事業者における確認体制の強化 システム会社のテスト結果の確認にあたっては、テストの証跡情報の提出を求め、内容の確認を行うとともに、受託事業者での運用テストでは要件定義とも照らした確認を担当だけでなく管理職も実施することにより徹底する。 ⑤受託事業者に対して厳正に指導し、登録完了メール送信作業のチェック体制を強化させる。 ⑥（1）部コンプライアンス推進委員会の臨時開催 ・メール送信時のダブルチェックを徹底させるため、個人情報等の取扱いに係るチェックリストの全職員での点検により注意を喚起、情報管理を再徹底する。 ・あわせて、最近の事故事案の事例を周知するなど、事故の再発予防を進める。 （2）定期的な事故防止意識の醸成 統計調査員を含む全職員を対象に、各所属長や指導員から情報セキュリティや感染拡大防止等に関する指導を定期・継続的に行い、危機意識の醸成等を図る。 ⑦委託先における個人情報の閲覧・使用に当たっての権限の設定や、不適切な閲覧・使用・持ち出しを防止するための体制についてあらためて確認し、適切な運用を徹底させる。 ⑧（1）情報共有をしているホワイトボードの位置、記入欄が分かりにくいとの意見が出 ため、位置、記入方法について変更した。 （2）書類封入時のチェック手順中に、患者氏名の確認を明示した。 （3）2者確認を徹底するため、事務員のみでなく看護職員もチェックを行うこととし、 2者チェックが終わった段階で封書のチェックボックスに記載する。 （4）責任の所在を明確にするため「転院時退所セット確認書」を新たに作成し、チェックを行った職員が記名する。 ⑨（1）チェックリストを活用し、複数人、複数回のチェックを行うとともに、最終チェック者を統括責任者とすることで、誤封入等を防ぐ体制を整える。 （2）都職員が施設へ直接出向き、個人情報管理の実態確認を実施するとともに、対応 が不十分な場合は是正指導を行う。 （3）個人情報保護の研修を実施し、施設全体で個人情報保護の取り組み状況を共有した上で、改善を徹底する。 ⑩（1）委託先に対し、個人情報に関する業務手順を見直し及び徹底を図ることや、全従事者に対する個人情報保護研修を行うことを指導した。また、改善策の確認のため、都が施設へ出向き、個人情報管理の実態を確認した。 （2）再委託先において、送付の際は、まずFAX以外の手段を調整し、止むを得ずFAXを使用する際には、FAX番号の聞き取りの際の復唱や、FAX送信前の送信先への番号の再確認、複数人で複数回のチェックを必ず行うこととした。また、全従業者に対する個人情報保護研修を行った。 ⑪（1）作業環境等を見直し、書類の混入等が起きにくい環境を整備 ①執務室内の作業スペースの確保及び活用 ②引き出し付きの棚をキャビネット内に新設し、書類の分類をよりしやすくした。 （2）委託業者との書類の受け渡し方法の変更（送付する判定機関ごとに数を確認しながら受け渡す）。 ⑫個人情報をFAX送信することを禁止するよう各施設に通知した。 ⑬抽出ツールのプログラム確認は、委託先事業者の運用チームのみが行っていたが、抽出ツールを作成・利用する際には、運用チームに加えて、開発チームと委託元である都の3者で抽出ツールのプログラムの仕様・設定を確認することとした。 ⑭個人情報の持出、返却確認及び受け渡しの際の確認の徹底を行う。また、作業工程等を点検し、作業方法やチェック方法等ミスが起きにくい方法を検討、実施する。 ⑮郵便の発送作業は複数職員でチェックすることを再徹底。また、特に慎重を要する個人情報を取り扱う施設における個人情報の事故の重大性について改めて周知するとともに、書類の発送、保管、業務の進行管理等について、注意喚起や指導を行った。 ⑯（1）ファイルが他の物に紛れてしまわないよう、目立つ色に変更する。 （2）作業スペースに仕切りを立てて、使用スペースを物理的に限定する。 （3）ファイルに記載する名前をイニシャルに表記変更する等、使用する情報から個人情報を削除する。 （4）決まった時間に決まった人員が所在を確認する。 （5）チェックの時間を定刻とし、声をかけ合う。 （6）出したらしまうといった基本的事項を、改めて徹底するよう、注意喚起する。 （7）急いでいたり、忙しい時間帯でも、ダブルチェックをするよう、改めて徹底する。また、退所時にも荷物を確認してから渡すようにする ⑰（個人情報の管理について） （1）相談援助業務上の記録をノート等に記載する場合は、イニシャルを使用するなど個人情報を特定されないようにすること。また、私物のノートや手帳に個人情報を記載しないこと。 （2）庁舎外での会議等に出席した際には、個人端末を活用して記録の作成を行うとともに、作成した文書は暗号化し保存すること。 （3）業務上やむを得ず個人情報が記録された書類を庁舎外に持ち出す場合は、局の保有個人情報安全管理基準に基づき管理職の許可を得ること。 （4）個人情報を含む書類を持ち出すにあたっては、盗難や紛失を防止できる形状・機能を持つ鞄に収納し、肌身離さず持ち運ぶなど十分に注意すること。 （5）その他個人情報の取り扱いについては、局の保有個人情報安全管理基準等を遵守し、適正に行うこと。 （職員の証票の管理について） （1）月1回、各職員の保有状況を点検すること （2）携行する際には、ストラップ付きのケースに収納するなど、常に身体から離さずに携行することを徹底すること （職員の緊急連絡網の管理について） （1）必要な連絡先は公用携帯に保存し、連絡網を記載した紙は庁舎外に持ち出さないこと。 ⑱（1）入所時や退所時の手順確認のチェックリスト様式を変更し、入所時の写真撮影やリストへの正確な情報記載、退所時の荷物確認の手順など守るべきルールを追記するとともに、実施者を記載する欄を追加。 （2）個人情報紛失判明時の、本部への速やかな報告や具体的な捜索の手順などを、チェックリストに追記。 （3）毎朝のミーティングにてリーダー看護師等に個人情報保護の重要性やルールの順守を徹底。勤務者には、業務実施前に最新のマニュアルを確認するよう指導。 ⑲（1）発表資料の事前確認の徹底について幹部会で決定し、各部署に注意喚起 （2）録画や写真撮影をして保管していない旨を書面で確認 （3）画像等の個人情報の収集・利用に関する同意手続きの見直し ⑳（1）電子申請を推奨して紙文書の紛失リスクを軽減 （2）個人情報の適切な管理を職員に改めて周知徹底 ㉑（1）病院へ持ち運ぶファイルに、処方箋を収納する専用スペースを作る （2）医療機関受診時に係るマニュアルを作成 （3）帰園後は可能な限り速やかに所管部署に処方箋等を提出する

		(4)重要な個人情報を預かっている状況での裁断作業を避ける (5)上記対応について、ミーティング等で周知徹底、注意喚起 ㉒(1)必要なデータファイルのみを送信用データとしてPDF化し、送信前に、PDFに不要な箇所が入っていないことを確認の上、送信することを徹底 (2)メールシステム上、外部送信時に必須である上長の承認の際、個人情報が含まれていないか等の確認を徹底 (3)「メール送信時のセルフチェックリスト」を作成、活用 (4)各管理職より各職員に対する面談時に、個別に再度、再発防止策を徹底 ㉓(1)交付前の事務手順や確認方法の見直し、交付時の最終確認方法の見直し (2)作業スペースへの注意文の掲示やチェックリストへの注意文の記載 (3)確認等を行う人数を増員し、誤交付を防ぐ体制を強化 (4)再発防止勉強会を実施 ㉔(1)委託事業者及び再委託事業者に厳重注意、再発防止策等の作成を指示し、受領 (2)WEBページの脆弱性等の確認を受けるため、デジタルサービス局との調整を開始 ㉕(1)精査が十分でないデータを外部に提供しないこと、精査及び送付の際には複数体制でチェックすることを徹底 (2)受託事業者において、作成した資料のレビューフローの再検討、個人情報データの受領・管理方法に関する社内再教育等の取組を実施 ㉖(1)ダブルチェックの徹底及びその旨の指導 (2)作業項目の文章化、わかりやすいチェックリストの作成 ㉗(1)受託事業者において、マニュアルに沿った処理を徹底し、送付書類の引継ぎ時には、郵便局ともに引継ぎ件数ーを確認 (2)3か月間、受託事業者から送付先に対し、発送日の連絡及び到着の確認を行う。 ㉘(1)原則電子申請として紙文書の紛失リスクを軽減 (2) 書類の所在及び処理状況を明確に把握できるよう管理方法を見直す ㉙(1)個人情報の取扱い及び情報管理の徹底等について、厳重に注意喚起 (2)個人情報が特定できない記載にする等の対策 ㉚(1)局内各職場にて個人情報事故防止対策等をテーマとした職場討議実施 (2)個人情報安全管理強化月間の自己点検・職場点検による一層の意識啓発 ㉛(1)張り紙の掲示、FAXボタンへの着色による物理的な注意喚起 (2)FAX送付時のダブルチェック、送信履歴の確認等をマニュアルに追加 ㉜(1)区市町村からの書類を収受する際の件数記載用の共通様式を作成し、受領時に種類ごとの件数を確認・記入 (2)本件の事務のプロセスを細分化し、各プロセス毎の書類の受渡し時に、各担当者がそれぞれ(1)の様式に記載した件数に基づき、書類、件数の確認作業を行うよう整理 (3)使用頻度ごとに文書の保管場所を整理し、常時使用しないものは施錠。作業中に開錠しているキャビネットについても、中に担当者ごとの鍵付きの引き出し等を設置して自分の担当以外の書類は持ち出せないようにし、作業の際にその都度施錠。 (4)緊急の所内幹部会を開催し、個人情報を含む書類の受け渡し時の確認等、個人情報の取り扱いのルールが適正に行われているか確認を指示し、報告を受ける。 ㉝(1)個人情報の保管ルールについて全職員に徹底 (2)現在の保管状況の再点検を実施 ㉞(1)受託事業者に対する個人情報の取扱い及び情報管理の徹底に向けた注意喚起 (2)管理番号の活用など個人情報が特定できない情報管理方法等の導入 ㉟(1)廃業時の職員立会いの徹底、チェックリストの作成、活用 (2)廃業対象文書とシステム登録情報の照会の実施 ㊱書類の保管場
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		バックアップデータについても、システムで使用している元データと同様の方法にて安全管理措置を実施している。
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク2： 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	・納税義務者の異動に際しては、法令等に則り、適切に届出等を行うよう周知を行っている。 ・税務調査で異動の事実が判明した場合は、情報の更新を行っている。	
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	【審査システム（サーバー）】 ・課税から収入までの一連のサイクルを完了した課税データについて、電子データの削除等に関する規定に基づき、委託先によるバッチ処理により削除している。 【外部記録媒体】 ・データ移行のため、外部記録媒体（ハードディスク）、USBフラッシュメモリに一時保存したデータについては、移行後直ちに職員が手作業で消去している。	
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		
仕様書において、文書の安全管理や秘密の保護、作業方法、業者の資格等様々な条件を定め、リスクに対する措置を行っている。		

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

1. 特定個人情報ファイル名	
④eLTAX電子納税通知システムファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	・eLTAX電子納税通知システム（eLTAX）では、電子通知希望申請等を行う者以外からは情報を受け付けないようにシステムで制御し、「対象者の」情報以外は入手できない。
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	・必要な情報以外を記載することがないような様式としている。 ・納税義務者等宛に送達された納税通知書に記載されたキー情報をもとに申請を行うため、対象者以外の情報の入手を防止している。
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： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	・対象者以外の情報を記載することがないような様式としている。 ・納税義務者等宛に送達された納税通知書に記載されたキー情報をもとに申請を行うため、対象者以外の情報を入手することができない。
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	・納税義務者等宛に送達された納税通知書に記載されたキー情報をもとに申請を行うため、本人の真正性・実在性は担保されている。 ・eLTAX経由での申請においては、本人確認には申請者IDや電子署名を使用する。 ・マイナポータル経由での申請においては、マイナポータルにおいて本人確認を実施している。
個人番号の真正性確認の措置の内容	・納税義務者等宛に送達された納税通知書に記載されたキー情報をもとに申請を行うため、本人の真正性・実在性は担保されている。 ・マイナポータル経由での申請においては、マイナポータルにおいて真正性確認済み。
特定個人情報の正確性確保の措置の内容	・eLTAX経由での申請においては、eLTAXに委ねられる。 ・マイナポータル経由での申請においては、マイナポータルに委ねられる。
その他の措置の内容	―
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク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	eLTAX又はマイナポータルを経由した申請について、は政府共通ネットワーク及びLGWANが使用され、特定の権限が割り振られた官公庁にのみ届くようシステムで制御されている。
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
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	
―	

3. 特定個人情報の使用		
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容	eLTAX電子納税通知システムは、都における宛名システム等との接続はない。	
事務で使用するその他のシステムにおける措置の内容	eLTAX電子納税通知システムでは、税務事務に係るデータのみを保有しているため、税務事務以外の情報と紐付けることはできない。	
その他の措置の内容	―	
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク		
ユーザ認証の管理	[行っている]	<選択肢> 1）行っている　2）行っていない
具体的な管理方法	・eLTAX電子納税通知システムを使用する職員に対して、静脈等による生体認証およびID・パスワードを用いた認証の二要素認証を導入する。なお、IDについては職員毎に割り当てを行うものとする。 ・パスワードは3ヵ月に1度変更しなければならず、システム上も、同頻度でのパスワード変更を利用の必須条件としている。 ・操作内容は、システム稼働当初から現在に至るまで操作ログとして保管されており、いつどのIDでログインしたのかを把握できるようにしている。	
アクセス権限の発効・失効の管理	[行っている]	<選択肢> 1）行っている　2）行っていない
具体的な管理方法	人事担当部署が職員の異動情報を把握又は公表次第、異動情報をシステム管理部署へ連絡している。これに基づき、システム管理部署が必要な権限を付与・削除している。	
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	・アクセス権限については、システム管理部署が全ての権限を一元的に管理しており、操作者の所属及び業務に合わせて、システムの機能ごとに「更新・参照可」、「参照のみ可」、「更新・参照不可」の権限を設定している。 ・設定済の内容については、毎年度末に見直しを行うことにより、付与する権限に過不足が生じないようにしている。 ・権限に変更を加えた際には、システム管理部署が権限設定状況を示した一覧表を更新することにより、どの部署にどのような権限が設定されているのかを把握できるようにしている。	
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	システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、いつどの情報にアクセスし、抽出したのかが記録されている。また、操作履歴データは、暗号化により改竄や削除ができないようにしている。なお、記録は1年以上保存している。	
その他の措置の内容	・システム管理部署は、不正な操作の疑いがある場合には、参照情報と業務内容の関係性を確認している。 ・不正アクセスを未然に防ぐため、毎年実施する研修で上記作業を行うことについて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	・局内の規定において、原則、情報資産の外部持出しは禁止している。 ・これらを担保する手段として、審査システム端末での外部記憶媒体の使用を制限すること等により、容易に情報資産の持出しができないようにしている。	
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
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	・eLTAX電子納税通知システム内の特定個人情報ファイルは、ソフトにより暗号化されているため、eLTAX電子納税通知システム以外からデータを閲覧することはできない。 ・端末での外部記録媒体の使用を制限し、予期しないデータの取込み及び持出しができないようにしている。 ・ハードコピー等の紙資料については、取扱いに細心の注意を払うよう、研修や自己点検表等により注意喚起している。	
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置		
―		

4. 特定個人情報ファイルの取扱いの委託		[　　]委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認		【委託事項1～3】 ・委託契約で下記事項を規定し、確認している。 （1）責任者、作業体制、連絡体制及び作業場所の提出 （2）業務従事者への遵守事項の周知及び実施報告の提出 （3）再委託の承諾申請の提出 （4）作業担当者の名簿の提出　等 ・委託先がプライバシーマーク等を保有していることを確認している。
特定個人情報ファイルの閲覧者・更新者の制限		[　　制限している　　]　＜選択肢＞ 1）制限している　　2）制限していない
	具体的な制限方法	【委託事項1～3】 ・委託先が使用するユーザIDは、局内のIDに関する規定に基づき、委託元が割り当てを行っている。 ・ユーザIDの設定に際しては、用途を確認した上で必要最小限の権限のみ付与し、使用する期間のみ有効とし、有効期間が経過した場合には当該ユーザIDでは特定個人情報ファイルを閲覧できないようにしている。
特定個人情報ファイルの取扱いの記録		[　　記録を残している　　]　＜選択肢＞ 1）記録を残している　　2）記録を残していない
	具体的な方法	【委託事項1～3】 ・施錠された保管庫等での管理、管理状況の記録、管理記録の報告等を委託契約で規定している。 ・システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、いつどの情報にアクセスし、抽出したのかが記録されている。また、操作履歴データは、アクセス制御・暗号化により改竄や削除ができないようにしている。
特定個人情報の提供ルール		[　　定めている　　]　＜選択肢＞ 1）定めている　　2）定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	【委託事項1～3】 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。
	委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	【委託事項1～3】 ① 委託先から他者への提供はない。なお、提供する必要性が発生する場合は、目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について契約で取り交わしている。 ② 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。 【委託事項2】 データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。
特定個人情報の消去ルール		[　　定めている　　]　＜選択肢＞ 1）定めている　　2）定めていない
	ルールの内容及びルール遵守の確認方法	【委託事項1～3】 ・契約履行完了後に外部記憶媒体上に含まれる当該委託業務に係る情報を全て消去することを、委託契約で規定している。 ・消去した情報項目、数量、消去方法及び消去日等について報告書類等にて確認している。
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	・委託契約で下記事項を規定している。 【委託事項1、2】 （1）プログラム、データ等が格納されたサーバー及び端末機器等は、適切なアクセス権限を設定すること。 （2）外部記録媒体でやり取りするプログラム、データ等は、最新のパターンファイルを適用したウイルス対策ソフトでチェックすること。 【委託事項1～3】 （3）セキュリティ監査を実施する際は協力すること。 （4）委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく委託元に報告すること。

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	【委託事項1～3】 ・委託元と委託先の間で取り交わされている契約内容と同等の条件を再委託先においても課している。 ・委託元が再委託先に対して実地調査を定期的に行い、適切な管理体制をとっていることを確認している。 ・委託先が再委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく報告させている。
その他の措置の内容		・委託に関する契約書や仕様書及び受託者から受領する誓約書等の書類については、文書等の取扱に関する規定の保存期間に基づき保管している。 ・委託先に対し、作業場所へ業務に関係がない物の持込みを禁止する。
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報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	
リスクへの対策は十分か	[　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 安全が保たれない方法によって入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク5： 不正な提供が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク6： 不適切な方法で提供されるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1）特に力を入れて遵守している 2）十分に遵守している 3）十分に遵守していない 4）政府機関ではない
②安全管理体制	[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	【税務総合支援システム（サーバー）】 ・特定個人情報を保管するデータセンタは、都市計画法における防火・準防火地域に指定されていること、サーバー室等へ滞りなく電力を供給できる電源設備及び非常用自家発電設備を備えていること等の防災性を重視した条件により、選定している。 ・データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。	
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	【eLTAX電子納税通知システム】 ・ eLTAX電子納税通知システムでの外部記憶媒体の使用を制限し、予期しないデータの取り込み及び持ち出しができないようにしている。 ・ データはソフトにより暗号化されているため、eLTAX電子納税通知システム以外からデータを閲覧することはできない。 ・ サーバー、端末等の機器にはウイルス対策ソフトを適用するとともに、パターンファイルの更新を定期的に行うことにより、ウイルス感染を防止している。 ・ 地方税ポータルシステム（eLTAX）との接続は、LGWANを使用し、ファイアウォールを適用するとともに、接続状況を監視することにより、不正接続への対策を行っている。	
⑦バックアップ	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生あり]	<選択肢> 1）発生あり 2）発生なし

	その内容	①令和4年5月、東京都現代美術館において、ミュージアムショップ運営の受託事業者スタッフが、展覧会図録を予約した顧客へ一斉に案内メールを送信する際、メールアドレスをBCC欄ではなく、宛先欄に入力して発信した。 ②令和4年5月、技能検定試験に関する通知を外国人技能実習の複数の監理団体に対しメールで送付する際、誤ってメールアドレスをBCC欄ではなく、CC欄に入力し、一斉送信した。 ③令和4年5月、就学支援金事務において、就学支援金の基礎データをCD-Rに情報を保存し、対象高等学校等宛て一斉に送付したところ、そのうち1校に、他校の受給者に関する情報が含まれていることが判明した。 ④令和4年5月、受託事業者が、事業に関するイベントを案内するメールマガジンを送付する際、配信プログラム改修ミスにより、宛先欄に複数のメールアドレスが入力され、送信された。 ⑤令和4年10月、東京都陽性者登録センターの運営受託事業者が、医療機関で新型コロナウイルス陽性の診断を受け、センターに登録申請を行った複数の患者への登録完了メールを、送付先アドレスが全て入れ替わったまま送信した。 ⑥令和4年12月、労働力調査の統計調査員に対して連絡事項をメールした際、BCC欄に入力して送るべきところを宛先欄に入力し、一斉送信した。 ⑦令和5年4月、再委託先の派遣会社職員が、業務で使用するシステムを不適切に使用し、個人情報を閲覧、メモにとり自宅に持ち出した。 ⑧令和5年5月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑨令和5年6月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑩令和5年7月、施設を退所する患者に関して、退所先候補の施設と受入調整を行うため、診療関係書類をFAX送信した際、誤って別のFAX番号宛てに送信した。 ⑪令和5年8月、申請により受け付けた申請書が紛失していることが発覚した。 ⑫令和5年9月、関係施設宛に都民情報をFAX送信した際、誤って別の事業者宛てに送信した。 ⑬令和5年9月、事業の対象者に案内チラシを郵送した際、送付対象者の抽出ツールのプログラム仕様の不備により、誤って事業対象外の方に送付したことで、旧住所宛てに送付し返戻されなかったものが誤送付となった。 ⑭令和5年9月、決定通知書に公印を押印する目的で本庁に出張し、押印後持ち帰ったが、発送の準備をしていた際に、通知書1枚が紛失していることが発覚した。 ⑮令和6年1月、患者A宛てに送付すべき利用者情報を、誤ってB宛てに送付した。 ⑯令和6年1月、入所者の診療関係ファイルが紛失していることが発覚し、その後、退所者の荷物の中に当該ファイルが混入していたことが発覚した。 ⑰令和6年2月、児童相談所の職員が、出張中に個人情報が記載されている手帳を紛失し、あわせて手帳に収納されていた、当該職員の証票及び所内職員の緊急連絡網を紛失した。 ⑱令和6年2月、施設を退所した患者Aに関する薬剤情報等を記載した書類を、誤って別の患者の退院時の荷物に混入させ交付した。 ⑲令和6年2月、オンライン研修で使用した映像において、患者の情報をマスキング処理していたところ、当該映像をスマートフォンで視聴した場合に、マスキングが外れ、個人が特定できる状態になっていたことが判明した。 ⑳令和6年4月、受け付けた申請書を紛失していることが発覚した。 ㉑令和6年4月、施設職員が、利用者の通院付添の際、処方箋を紛失した。 ㉒令和6年4月、指定管理者が、事業者に対してExcel資料をメールで送信した際、本来削除すべきだった個人情報の入力されたシートを削除しなかった。 ㉓令和6年7月、受託事業者が、都へ交付すべき納入済通知書を、誤って他の事業者宛てに交付したことが発覚した。 ㉔令和6年7月、受託事業者がイベントを行った際の申込時の個人情報が掲載されたウェブページが、一時外部からアクセス可能な状態となっていたことが発覚した。 ㉕令和6年7月、職員が、説明会の資料の中に個人情報が含まれていることに気が付かずに、各自治体にデータを配布した。 ㉖令和6年7月、職員が、A宛てに送付すべき個人情報を、誤ってB宛てに送付していたことが発覚した。 ㉗令和6年7月、受託事業者から送付した個人情報を含む資料が、紛失していることが発覚した。 ㉘令和6年7月、受け付けた申請書を紛失していることが発覚した。 ㉙令和6年8月、受託事業者が配付した資料の中に、個人情報等が含まれる資料が混入していたことが発覚した。 ㉚令和6年10月、職員が、受託者に資料をメールで送信した際、誤って個人情報が記載された別のファイルを添付した。 ㉛令和6年10月、受託事業者が、A宛てに送付すべき電話記録を、誤ってB宛てにFAXで送信した。 ㉜令和6年11月、受け付けた申請書を紛失していることが発覚した（後日発見）。 ㉝令和6年11月、令和3年頃に個人情報が記載された資料を紛失していたことが発覚した。 ㉞令和6年12月、受託事業者が、個人情報が記載された資料を、誤って外部へ送信した。 ㉟令和7年1月、受託事業者が、個人情報が記載された資料を、誤って期限前に廃棄した。 ㊱令和7年1月、受け付けた届出書が、誤って机ごと廃棄されていることが発覚した。

	再発防止策の内容	①（1）ミュージアムショップにおいて、本社セキュリティインシデント統括部と連携して、個人情報取り扱い、情報管理体制の改善を行う。 （2）特に複数人へのメール送信に際してはダブルチェックを徹底する。 （3）現代美術館全委託業者に、適切な個人情報等の取扱い及び情報管理を徹底するよう指示する。 （4）財団が管理運営する各施設にも本事案を共有し、個人情報を含む情報の適切な管理を徹底する。 ②（1）個人情報の取扱い及び情報管理の徹底等について周知するとともに、職員全員に臨時研修を速やかに実施 （2）誤送信防止に向けたシステムの導入（ダイアログの自動表示など） （3）複数人チェックなど基本的対策の徹底 ③チェック機能を再検証し、全日制等と同様の仕組みを通信制にも直ちに導入するほか、事務フローの再構築を行い、再発防止に努める。そのうえで、本件を財団内で広く共有させ、個人情報の取扱い全般についてハード・ソフトの両面から厳しく見直すとともに、職員の意識向上を図っていく。また、都の実施機関においても個人情報の適正管理とサイバーセキュリティー対策について改めて確認を行う。 ④（1）システムの改善 メールマガジンの配信は、これまで「TO」により自動で1件ずつ送信がされる仕組みであったが、一括メール送信においては送信者アドレスを全て「BCC」に入れるようシステム改修を行う。 （2）システム会社における確認体制の強化 開発前にシステム会社が実施する、影響調査・テスト内容等について、これまでの2名体制によるダブルチェックから、システム会社のプロジェクトマネージャーも加えることとし、確認した内容を報告させて承認する運用へ見直す。 （3）受託事業者における確認体制の強化 システム会社のテスト結果の確認にあたっては、テストの証跡情報の提出を求め、内容の確認を行うとともに、受託事業者での運用テストでは要件定義とも照らした確認を担当だけでなく管理職も実施することにより徹底する。 ⑤受託事業者に対して厳正に指導し、登録完了メール送信作業のチェック体制を強化させる。 ⑥（1）部コンプライアンス推進委員会の臨時開催 ・メール送信時のダブルチェックを徹底させるため、個人情報等の取扱いに係るチェックリストの全職員での点検により注意を喚起、情報管理を再徹底する。 ・あわせて、最近の事故事案の事例を周知するなど、事故の再発予防を進める。 （2）定期的な事故防止意識の醸成 統計調査員を含む全職員を対象に、各所属長や指導員から情報セキュリティや感染拡大防止等に関する指導を定期・継続的に行い、危機意識の醸成等を図る。 ⑦委託先における個人情報の閲覧・使用に当たっての権限の設定や、不適切な閲覧・使用・持ち出しを防止するための体制についてあらためて確認し、適切な運用を徹底させる。 ⑧（1）情報共有をしているホワイトボードの位置、記入欄が分かりにくいとの意見が出 ため、位置、記入方法について変更した。 （2）書類封入時のチェック手順中に、患者氏名の確認を明示した。 （3）2者確認を徹底するため、事務員のみでなく看護職員もチェックを行うこととし、 2者チェックが終わった段階で封書のチェックボックスに記載する。 （4）責任の所在を明確にするため「転院時退所セット確認書」を新たに作成し、チェ ックを行った職員が記名する。 ⑨（1）チェックリストを活用し、複数人、複数回のチェックを行うとともに、最終チェ ック者を統括責任者とすることで、誤封入等を防ぐ体制を整える。 （2）都職員が施設へ直接出向き、個人情報管理の実態確認を実施するとともに、対応 が不十分な場合は是正指導を行う。 （3）個人情報保護の研修を実施し、施設全体で個人情報保護の取り組み状況を共有し た上で、改善を徹底する。 ⑩（1）委託先に対し、個人情報に関する業務手順を見直し及び徹底を図ることや、全従 事者に対する個人情報保護研修を行うことを指導した。また、改善策の確認のた め、都が施設へ出向き、個人情報管理の実態を確認した。 （2）再委託先において、送付の際は、まずFAX以外の手段を調整し、止むを得ずFAXを使用する際には、FAX番号の聞き取りの際の復唱や、FAX送信前の送信先への番号の再確認、複数人で複数回のチェックを必ず行うこととした。また、全従業者に対する個人情報保護研修を行った。 ⑪（1）作業環境等を見直し、書類の混入等が起きにくい環境を整備 ①執務室内の作業スペースの確保及び活用 ②引き出し付きの棚をキャビネット内に新設し、書類の分類をよりしやすくした。 （2）委託業者との書類の受け渡し方法の変更（送付する判定機関ごとに数を確認しながら受け渡す）。 ⑫個人情報をFAX送信することを禁止するよう各施設に通知した。 ⑬抽出ツールのプログラム確認は、委託先事業者の運用チームのみが行っていたが、抽出ツールを作成・利用する際には、運用チームに加えて、開発チームと委託元である都の3者で抽出ツールのプログラムの仕様・設定を確認することとした。 ⑭個人情報の持出、返却確認及び受け渡しの際の確認の徹底を行う。また、作業工程等を点検し、作業方法やチェック方法等ミスが起きにくい方法を検討、実施する。 ⑮郵便の発送作業は複数職員でチェックすることを再徹底。また、特に慎重を要する個人情報を取り扱う施設における個人情報の事故の重大性について改めて周知するとともに、書類の発送、保管、業務の進行管理等について、注意喚起や指導を行った。 ⑯（1）ファイルが他の物に紛れてしまわないよう、目立つ色に変更する。 （2）作業スペースに仕切りを立てて、使用スペースを物理的に限定する。 （3）ファイルに記載する名前をイニシャルに表記変更する等、使用する情報から個人情報を削除する。 （4）決まった時間に決まった人員が所在を確認する。 （5）チェックの時間を定刻とし、声をかけ合う。 （6）出したらしまうといった基本的事項を、改めて徹底するよう、注意喚起する。 （7）急いでいたり、忙しい時間帯でも、ダブルチェックをするよう、改めて徹底する。また、退所時にも荷物を確認してから渡すようにする ⑰（個人情報の管理について） （1） 相談援助業務上の記録をノート等に記載する場合は、イニシャルを使用するなど個人情報を特定されないようにすること。また、私物のノートや手帳に個人情報を記載しないこと。 （2） 庁舎外での会議等に出席した際には、個人端末を活用して記録の作成を行うとともに、作成した文書は暗号化し保存すること。 （3） 業務上やむを得ず個人情報が記録された書類を庁舎外に持ち出す場合は、局の保有個人情報安全管理基準に基づき管理職の許可を得ること。 （4） 個人情報を含む書類を持ち出すにあたっては、盗難や紛失を防止できる形状・機能を持つ鞄に収納し、肌身離さず持ち運ぶなど十分に注意すること。 （5） その他個人情報の取り扱いについては、局の保有個人情報安全管理基準等を遵守し、適正に行うこと。 （職員の証票の管理について） （1） 月1回、各職員の保有状況を点検すること （2） 携行する際には、ストラップ付きのケースに収納するなど、常に身体から離さずに携行することを徹底すること （職員の緊急連絡網の管理について） （1） 必要な連絡先は公用携帯に保存し、連絡網を記載した紙は庁舎外に持ち出さないこと。 ⑱（1）入所時や退所時の手順確認のチェックリスト様式を変更し、入所時の写真撮影やリストへの正確な情報記載、退所時の荷物確認の手順など守るべきルールを追記するとともに、実施者を記載する欄を追加。 （2）個人情報紛失判明時の、本部への速やかな報告や具体的な捜索の手順などを、チェックリストに追記。 （3）毎朝のミーティングにてリーダー看護師等に個人情報保護の重要性やルールの順守を徹底。勤務者には、業務実施前に最新のマニュアルを確認するよう指導。 ⑲（1）発表資料の事前確認の徹底について幹部会で決定し、各部署に注意喚起 （2）録画や写真撮影をして保管していない旨を書面で確認 （3）画像等の個人情報の収集・利用に関する同意手続きの見直し ⑳（1）電子申請を推奨して紙文書の紛失リスクを軽減 （2）個人情報の適切な管理を職員に改めて周知徹底 ㉑（1）病院へ持ち運ぶファイルに、処方箋を収納する専用スペースを作る （2）医療機関受診時に係るマニュアルを作成 （3）帰園後は可能な限り速やかに所管部署に処方箋等を提出する

		(4)重要な個人情報を預かっている状況での裁断作業を避ける (5)上記対応について、ミーティング等で周知徹底、注意喚起 ㉒(1)必要なデータファイルのみを送信用データとしてPDF化し、送信前に、PDFに不要な箇所が入っていないことを確認の上、送信することを徹底 (2)メールシステム上、外部送信時に必須である上長の承認の際、個人情報が含まれていないか等の確認を徹底 (3)「メール送信時のセルフチェックリスト」を作成、活用 (4)各管理職より各職員に対する面談時に、個別に再度、再発防止策を徹底 ㉓(1)交付前の事務手順や確認方法の見直し、交付時の最終確認方法の見直し (2)作業スペースへの注意文の掲示やチェックリストへの注意文の記載 (3)確認等を行う人数を増員し、誤交付を防ぐ体制を強化 (4)再発防止勉強会を実施 ㉔(1)委託事業者及び再委託事業者に厳重注意、再発防止策等の作成を指示し、受領 (2)WEBページの脆弱性等の確認を受けるため、デジタルサービス局との調整を開始 ㉕(1)精査が十分でないデータを外部に提供しないこと、精査及び送付の際には複数体制でチェックすることを徹底 (2)受託事業者において、作成した資料のレビューフローの再検討、個人情報データの受領・管理方法に関する社内再教育等の取組を実施 ㉖(1)ダブルチェックの徹底及びその旨の指導 (2)作業項目の文章化、わかりやすいチェックリストの作成 ㉗(1)受託事業者において、マニュアルに沿った処理を徹底し、送付書類の引継ぎ時には、郵便局ともに引継ぎ件数ーを確認 (2)3か月間、受託事業者から送付先に対し、発送日の連絡及び到着の確認を行う。 ㉘(1)原則電子申請として紙文書の紛失リスクを軽減 (2) 書類の所在及び処理状況を明確に把握できるよう管理方法を見直す ㉙(1)個人情報の取扱い及び情報管理の徹底等について、厳重に注意喚起 (2)個人情報が特定できない記載にする等の対策 ㉚(1)局内各職場にて個人情報事故防止対策等をテーマとした職場討議実施 (2)個人情報安全管理強化月間の自己点検・職場点検による一層の意識啓発 ㉛(1)張り紙の掲示、FAXボタンへの着色による物理的な注意喚起 (2)FAX送付時のダブルチェック、送信履歴の確認等をマニュアルに追加 ㉜(1)区市町村からの書類を収受する際の件数記載用の共通様式を作成し、受領時に種類ごとの件数を確認・記入 (2)本件の事務のプロセスを細分化し、各プロセス毎の書類の受渡し時に、各担当者がそれぞれ(1)の様式に記載した件数に基づき、書類、件数の確認作業を行うよう整理 (3)使用頻度ごとに文書の保管場所を整理し、常時使用しないものは施錠。作業中に開錠しているキャビネットについても、中に担当者ごとの鍵付きの引き出し等を設置して自分の担当以外の書類は持ち出せないようにし、作業の際にその都度施錠。 (4)緊急の所内幹部会を開催し、個人情報を含む書類の受け渡し時の確認等、個人情報の取り扱いのルールが適正に行われているか確認を指示し、報告を受ける。 ㉝(1)個人情報の保管ルールについて全職員に徹底 (2)現在の保管状況の再点検を実施 ㉞(1)受託事業者に対する個人情報の取扱い及び情報管理の徹底に向けた注意喚起 (2)管理番号の活用など個人情報が特定できない情報管理方法等の導入 ㉟(1)廃棄時の職員立会いの徹底、チェックリストの作成、活用 (2)廃棄対象文書とシステム登録情報の照会の実施 ㊱書類の保管場所の見直し
⑩死者の個人番号		[保管している] <選択肢> 1) 保管している 2) 保管していない
	具体的な保管方法	生存者の個人番号と同様の方法にて安全管理措置を実施している。
その他の措置の内容		バックアップデータについても、システムで使用している元データと同様の方法にて安全管理措置を実施している。
リスクへの対策は十分か		[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク2： 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	・納税義務者の異動に際しては、法令等に則り、適切に届出等を行うよう周知を行っている。 ・税務調査で異動の事実が判明した場合は、情報の更新を行っている。	
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	【税務総合支援システム（サーバー）】 一定期間経過後、バッチ処理により削除する。 また、機器リース期間満了時には特定個人情報等のデータを全て消去の上、消去結果について、記録媒体ごとに、消去した情報項目、数量、消去方法及び消去日時を明示した書面で委託事業者より報告を受けている。	
その他の措置の内容	ー	
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		
仕様書において、文書の安全管理や秘密の保護、作業方法、業者の資格等様々な条件を定め、リスクに対する措置を行っている。		

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

1．特定個人情報ファイル名	
⑤地方税外部連携ファイル（仮称）	
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	地方税外部連携システム（eLTAX）は、地方税ポータルシステム（eLTAX）を通じて他の方公共団体としか繋がっていないことから、他地方公共団体から送信される対象者の情報以外は入手できない。
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	地方税外部連携システム（eLTAX）では、法令等により定められた様式を用いることで、必要な情報以外を入手することを防止している。
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：　不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	特定個人情報の入手元である他地方公共団体は、使用目的が法令に基づくものであることを理解した上で提供を行っている。
リスクへの対策は十分か	［　十分である　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3：　入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	特定個人情報の入手元が番号法第16条の規定に基づき、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、都が他地方公共団体から入手する際は番号法第16条が適用されない。
個人番号の真正性確認の措置の内容	特定個人情報の入手元が番号法第16条の規定に基づき、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、都が他地方公共団体から入手する際は番号法第16条が適用されない。
特定個人情報の正確性確保の措置の内容	正確性の確保については、特定個人情報の入手元である他地方公共団体に委ねられており、他地方公共団体が申告内容に誤りがあれば是正を求めるなどの対応を行い、修正等行われた情報が他地方公共団体から送信されてくる。
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	・他地方公共団体から地方税ポータルセンタ（eLTAX）までは、専用回線を利用するとともに、暗号化通信を行っている。 ・地方税ポータルセンタ（eLTAX）から地方税外部連携システム（eLTAX）までは、閉域網であるLGWANを利用するとともに、暗号化通信を行っている。 ・セキュリティについては、「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」（平成25年5月1日総務省告示第206号）に定められた事項を順守するとともに、局内のセキュリティ実施手順において端末の管理に関する事項等を定め、順守することとしている。
リスクへの対策は十分か	［　十分である　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	
―	

3. 特定個人情報の使用		
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容	地方税外部連携システムから入手した情報と税務総合支援システムのあて名管理システムに登録されている納税義務者情報（氏名・住所）とを突合（検索）し、システム上に存在するあて名であるかどうかを確認して紐づけを行っている。目的外の情報の紐付けは行われない。	
事務で使用するその他のシステムにおける措置の内容	税務総合支援システムでは、税務事務に係るデータのみを保有しているため、税務事務以外の情報と紐付けることはできない。	
その他の措置の内容	ー	
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	・地方税外部連携システムを使用する職員に対して、静脈等による生体認証およびID・パスワードを用いた認証の二要素認証を導入する。なお、IDについては職員毎に割り当てを行うものとする。 ・パスワードは3ヵ月に1度変更しなければならず、システム上も、同頻度でのパスワード変更を利用の必須条件としている。 ・操作内容は、操作ログとして保管されており、いつどのIDでログインしたのかを把握できるようにしている。	
アクセス権限の発効・失効の管理	[行っている]	＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	人事担当部署が職員の異動情報を把握又は公表次第、異動情報をシステム管理部署へ連絡している。これに基づき、システム管理部署が必要な権限を付与・削除している。	
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	・アクセス権限については、システム管理部署が全ての権限を一元的に管理しており、操作者の所属及び業務に合わせて、「データ管理・閲覧可」、「閲覧のみ可」の権限を設定している。 ・設定済の内容については、毎年度末に見直しを行うことにより、付与する権限に過不足が生じないようにしている。 ・権限に変更を加えた際には、システム管理部署が権限設定状況を示した一覧表を更新することにより、どの部署にどのような権限が設定されているのかを把握できるようにしている。	
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	システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、いつどの情報にアクセスし、抽出したのかが記録されている。また、操作履歴データは、暗号化により改竄や削除ができないようにしている。なお、記録は1年以上保存している。	
その他の措置の内容	・システム管理部署は、不正な操作の疑いがある場合には、参照情報と業務内容の関係性を確認している。 ・不正アクセスを未然に防ぐため、毎年実施する研修で上記作業を行うことについて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	・局内の規定において、原則、情報資産の外部持出しは禁止している。 ・これらを担保する手段として、地方税外部連携システム端末での外部記憶媒体の使用を制限すること等により、容易に情報資産の持出しができないようにしている。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

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	・地方税外部連携システム内の特定個人情報ファイルは、ソフトにより暗号化されているため、地方税外部連携システム端末以外からデータを閲覧することはできない。 ・端末での外部記録媒体の使用を制限し、予期しないデータの取込み及び持出しができないようにしている。 ・ハードコピー等の紙資料については、取扱いに細心の注意を払うよう、研修や自己点検表等により注意喚起している。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	
・地方税外部連携システム端末から印刷したハードコピー資料等の特定個人情報が記載されている紙資料について紛失や権限外の者に不正利用等されるリスクが想定されるが、紙資料については鍵の付いたロッカーに町名・氏名コード順にファイリングされて保管することで使用中のファイルがあれば分かるように並べており、退庁時には使用途中であっても必ずロッカーに全て返却し返却漏れがないか確認してから鍵を閉めて退庁している。 ・退庁後に特定個人情報等の書類のしまい忘れや鍵の閉め忘れがないかなどについて、他部署の執務室を相互点検するなどの措置を定期的に行っている。 ・特定個人情報ファイルについては、インターネットと接続している端末に転記・保存することのないよう規定し、徹底する。	
4. 特定個人情報ファイルの取扱いの委託	**[ ] 委託しない**
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク	
情報保護管理体制の確認	【委託事項1～3】 ・委託契約で下記事項を規定し、確認している。 （1）責任者、作業体制、連絡体制及び作業場所の提出 （2）業務従事者への遵守事項の周知及び実施報告の提出 （3）再委託の承諾申請の提出 （4）作業担当者の名簿の提出 等 ・委託先がプライバシーマーク等を保有していることを確認している。
特定個人情報ファイルの閲覧者・更新者の制限	[制限している] ＜選択肢＞ 1）制限している 2）制限していない
具体的な制限方法	【委託事項1～3】 ・委託先が使用するユーザIDは、局内のIDに関する規定に基づき、委託元が割り当てを行っている。 ・ユーザIDの設定に際しては、用途を確認した上で必要最小限の権限のみ付与し、使用する期間のみ有効とし、有効期間が経過した場合には当該ユーザIDでは特定個人情報ファイルを閲覧できないようにしている。
特定個人情報ファイルの取扱いの記録	[記録を残している] ＜選択肢＞ 1）記録を残している 2）記録を残していない
具体的な方法	【委託事項1～3】 ・施錠された保管庫等での管理、管理状況の記録、管理記録の報告等を委託契約で規定している。 ・システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、いつどの情報にアクセスし、抽出したのかが記録されている。また、操作履歴データは、アクセス制御・暗号化により改竄や削除ができないようにしている。

特定個人情報の提供ルール		[定めている] ＜選択肢＞ 1）定めている 2）定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	【委託事項1～3】 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。
	委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	【委託事項1～3】 ① 委託先から他者への提供はない。なお、提供する必要性が発生する場合は、目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について契約で取り交わしている。 ② 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。 【委託事項2】 データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。
特定個人情報の消去ルール		[定めている] ＜選択肢＞ 1）定めている 2）定めていない
	ルールの内容及びルール遵守の確認方法	【委託事項1～3】 ・契約履行完了後に外部記憶媒体上に含まれる当該委託業務に係る情報を全て消去することを、委託契約で規定している。 ・消去した情報項目、数量、消去方法及び消去日等について報告書類等にて確認している。
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	・委託契約で下記事項を規定している。 【委託事項1、2】 （1）プログラム、データ等が格納されたサーバー及び端末機器等は、適切なアクセス権限を設定すること。 （2）外部記録媒体でやり取りするプログラム、データ等は、最新のパターンファイルを適用したウイルス対策ソフトでチェックすること。 【委託事項1～3】 （3）セキュリティ監査を実施する際は協力すること。 （4）委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく委託元に報告すること。
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	【委託事項1～3】 ・委託元と委託先の間で取り交わされている契約内容と同等の条件を再委託先においても課している。 ・委託元が再委託先に対して実地調査を定期的に行い、適切な管理体制をとっていることを確認している。 ・委託先が再委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく報告させている。
その他の措置の内容		・委託に関する契約書や仕様書及び受託者から受領する誓約書等の書類については、文書等の取扱に関する規定の保存期間に基づき保管している。 ・委託先に対し、作業場所へ業務に関係がない物の持込みを禁止する。
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報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	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 安全が保たれない方法によって入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク5： 不正な提供が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク6： 不適切な方法で提供されるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1）特に力を入れて遵守している 2）十分に遵守している 3）十分に遵守していない 4）政府機関ではない
②安全管理体制	[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	【地方税外部連携システム】 ・特定個人情報を保管するデータセンタは、都市計画法における防火・準防火地域に指定されていること、サーバー室等へ滞りなく電力を供給できる電源設備及び非常用自家発電設備を備えていること等の防災性を重視した条件により、選定している。 ・データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。	
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	【地方税外部連携システム】 ・地方税外部連携システム端末での外部記憶媒体の使用を制限し、予期しないデータの取り込み及び持ち出しができないようにしている。 ・サーバ、端末等の機器にはウイルス対策ソフトを適用するとともに、パターンファイルの更新を定期的に行うことにより、ウイルス感染を防止している。 ・地方税ポータルシステム（eLTAX）との接続は、LGWANを使用し、ファイアウォールを適用するとともに、接続状況を監視することにより、不正接続への対策を行っている。	
⑦バックアップ	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生あり]	<選択肢> 1）発生あり 2）発生なし

	その内容	①令和４年５月、東京都現代美術館において、ミュージアムショップ運営の受託事業者スタッフが、展覧会図録を予約した顧客へ一斉に案内メールを送信する際、メールアドレスをBCC欄ではなく、宛先欄に入力して発信した。 ②令和４年５月、技能検定試験に関する通知を外国人技能実習の複数の監理団体に対しメールで送付する際、誤ってメールアドレスをBCC欄ではなく、CC欄に入力し、一斉送信した。 ③令和４年５月、就学支援金事務において、就学支援金の基礎データをCD-Rに情報を保存し、対象高等学校等宛て一斉に送付したところ、そのうち１校に、他校の受給者に関する情報が含まれていることが判明した。 ④令和４年５月、受託事業者が、事業に関するイベントを案内するメールマガジンを送付する際、配信プログラム改修ミスにより、宛先欄に複数のメールアドレスが入力され、送信された。 ⑤令和４年10月、東京都陽性者登録センターの運営受託事業者が、医療機関で新型コロナウイルス陽性の診断を受け、センターに登録申請を行った複数の患者への登録完了メールを、送付先アドレスが全て入れ替わったまま送信した。 ⑥令和４年12月、労働力調査の統計調査員に対して連絡事項をメールした際、BCC欄に入力して送るべきところを宛先欄に入力し、一斉送信した。 ⑦令和５年４月、再委託先の派遣会社職員が、業務で使用するシステムを不適切に使用し、個人情報を閲覧、メモにとり自宅に持ち出した。 ⑧令和５年５月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑨令和５年６月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑩令和５年７月、施設を退所する患者に関して、退所先候補の施設と受入調整を行うため、診療関係書類をFAX送信した際、誤って別のFAX番号宛てに送信した。 ⑪令和５年８月、申請により受け付けた申請書が紛失していることが発覚した。 ⑫令和５年９月、関係施設宛に都民情報をFAX送信した際、誤って別の事業者宛てに送信した。 ⑬令和５年９月、事業の対象者に案内チラシを郵送した際、送付対象者の抽出ツールのプログラム仕様の不備により、誤って事業対象外の方に送付したことで、旧住所宛てに送付し返戻されなかったものが誤送付となった。 ⑭令和５年９月、決定通知書に公印を押印する目的で本庁に出張し、押印後持ち帰ったが、発送の準備をしていた際に、通知書１枚が紛失していることが発覚した。 ⑮令和６年１月、患者A宛てに送付すべき利用者情報を、誤ってB宛てに送付した。 ⑯令和６年１月、入所者の診療関係ファイルが紛失していることが発覚し、その後、退所者の荷物の中に当該ファイルが混入していたことが発覚した。 ⑰令和６年２月、児童相談所の職員が、出張中に個人情報が記載されている手帳を紛失し、あわせて手帳に収納されていた、当該職員の証票及び所内職員の緊急連絡網を紛失した。 ⑱令和６年２月、施設を退所した患者Aに関する薬剤情報等を記載した書類を、誤って別の患者の退院時の荷物に混入させ交付した。 ⑲令和６年２月、オンライン研修で使用した映像において、患者の情報をマスキング処理していたところ、当該映像をスマートフォンで視聴した場合に、マスキングが外れ、個人が特定できる状態になっていたことが判明した。 ⑳令和６年４月、受け付けた申請書を紛失していることが発覚した。 ㉑令和６年４月、施設職員が、利用者の通院付添の際、処方箋を紛失した。 ㉒令和６年４月、指定管理者が、事業者に対してExcel資料をメールで送信した際、本来削除すべきだった個人情報の入力されたシートを削除しなかった。 ㉓令和６年７月、受託事業者が、都へ交付すべき納入済通知書を、誤って他の事業者宛てに交付したことが発覚した。 ㉔令和６年７月、受託事業者がイベントを行った際の申込時の個人情報が掲載されたウェブページが、一時外部からアクセス可能な状態となっていたことが発覚した。 ㉕令和６年７月、職員が、説明会の資料の中に個人情報が含まれていることに気が付かずに、各自治体にデータを配布した。 ㉖令和６年７月、職員が、A宛てに送付すべき個人情報を、誤ってB宛てに送付していたことが発覚した。 ㉗令和６年７月、受託事業者から送付した個人情報を含む資料が、紛失していることが発覚した。 ㉘令和６年７月、受け付けた申請書を紛失していることが発覚した。 ㉙令和６年８月、受託事業者が配付した資料の中に、個人情報等が含まれる資料が混入していたことが発覚した。 ㉚令和６年10月、職員が、受託者に資料をメールで送信した際、誤って個人情報が記載された別のファイルを添付した。 ㉛令和６年10月、受託事業者が、A宛てに送付すべき電話記録を、誤ってB宛てにFAXで送信した。 ㉜令和６年11月、受け付けた申請書を紛失していることが発覚した（後日発見）。 ㉝令和６年11月、令和３年頃に個人情報が記載された資料を紛失していたことが発覚した。 ㉞令和６年12月、受託事業者が、個人情報が記載された資料を、誤って外部へ送信した。 ㉟令和７年１月、受託事業者が、個人情報が記載された資料を、誤って期限前に廃棄した。 ㊱令和７年１月、受け付けた届出書が、誤って机ごと廃棄されていることが発覚した。

	再発防止策の内容	①（1）ミュージアムショップにおいて、本社セキュリティインシデント統括部と連携して、個人情報取り扱い、情報管理体制の改善を行う。 （2）特に複数人へのメール送信に際してはダブルチェックを徹底する。 （3）現代美術館全委託業者に、適切な個人情報等の取扱い及び情報管理を徹底するよう指示する。 （4）財団が管理運営する各施設にも本事案を共有し、個人情報を含む情報の適切な管理を徹底する。 ②（1）個人情報の取扱い及び情報管理の徹底等について周知するとともに、職員全員に臨時研修を速やかに実施 （2）誤送信防止に向けたシステムの導入（ダイアログの自動表示など） （3）複数人チェックなど基本的対策の徹底 ③チェック機能を再検証し、全日制等と同様の仕組みを通信制にも直ちに導入するほか、事務フローの再構築を行い、再発防止に努める。そのうえで、本件を財団内で広く共有させ、個人情報の取扱い全般についてハード・ソフトの両面から厳しく見直すとともに、職員の意識向上を図っていく。また、都の実施機関においても個人情報の適正管理とサイバーセキュリティー対策について改めて確認を行う。 ④（1）システムの改善 メールマガジンの配信は、これまで「TO」により自動で1件ずつ送信がされる仕組みであったが、一括メール送信においては送信者アドレスを全て「BCC」に入れるようシステム改修を行う。 （2）システム会社における確認体制の強化 開発前にシステム会社が実施する、影響調査・テスト内容等について、これまでの2名体制によるダブルチェックから、システム会社のプロジェクトマネージャーも加えることとし、確認した内容を報告させて承認する運用へ見直す。 （3）受託事業者における確認体制の強化 システム会社のテスト結果の確認にあたっては、テストの証跡情報の提出を求め、内容の確認を行うとともに、受託事業者での運用テストでは要件定義とも照らした確認を担当だけでなく管理職も実施することにより徹底する。 ⑤受託事業者に対して厳正に指導し、登録完了メール送信作業のチェック体制を強化させる。 ⑥（1）部コンプライアンス推進委員会の臨時開催 ・メール送信時のダブルチェックを徹底させるため、個人情報等の取扱いに係るチェックリストの全職員での点検により注意を喚起、情報管理を再徹底する。 ・あわせて、最近の事故事案の事例を周知するなど、事故の再発予防を進める。 （2）定期的な事故防止意識の醸成 統計調査員を含む全職員を対象に、各所属長や指導員から情報セキュリティや感染拡大防止等に関する指導を定期・継続的に行い、危機意識の醸成等を図る。 ⑦委託先における個人情報の閲覧・使用に当たっての権限の設定や、不適切な閲覧・使用・持ち出しを防止するための体制についてあらためて確認し、適切な運用を徹底させる。 ⑧（1）情報共有をしているホワイトボードの位置、記入欄が分かりにくいとの意見が出 ため、位置、記入方法について変更した。 （2）書類封入時のチェック手順中に、患者氏名の確認を明示した。 （3）2者確認を徹底するため、事務員のみでなく看護職員もチェックを行うこととし、 2者チェックが終わった段階で封書のチェックボックスに記載する。 （4）責任の所在を明確にするため「転院時退所セット確認書」を新たに作成し、チェックを行った職員が記名する。 ⑨（1）チェックリストを活用し、複数人、複数回のチェックを行うとともに、最終チェック者を統括責任者とすることで、誤封入等を防ぐ体制を整える。 （2）都職員が施設へ直接出向き、個人情報管理の実態確認を実施するとともに、対応 が不十分な場合は是正指導を行う。 （3）個人情報保護の研修を実施し、施設全体で個人情報保護の取り組み状況を共有した上で、改善を徹底する。 ⑩（1）委託先に対し、個人情報に関する業務手順を見直し及び徹底を図ることや、全従 事者に対する個人情報保護研修を行うことを指導した。また、改善策の確認のため、都が施設へ出向き、個人情報管理の実態を確認した。 （2）再委託先において、送付の際は、まずFAX以外の手段を調整し、止むを得ずFAXを使用する際には、FAX番号の聞き取りの際の復唱や、FAX送信前の送信先への番号の再確認、複数人で複数回のチェックを必ず行うこととした。また、全従業者に対する個人情報保護研修を行った。 ⑪（1）作業環境等を見直し、書類の混入等が起きにくい環境を整備 ①執務室内の作業スペースの確保及び活用 ②引き出し付きの棚をキャビネット内に新設し、書類の分類をよりしやすくした。 （2）委託業者との書類の受け渡し方法の変更（送付する判定機関ごとに数を確認しながら受け渡す）。 ⑫個人情報をFAX送信することを禁止するよう各施設に通知した。 ⑬抽出ツールのプログラム確認は、委託先事業者の運用チームのみが行っていたが、抽出ツールを作成・利用する際には、運用チームに加えて、開発チームと委託元である都の3者で抽出ツールのプログラムの仕様・設定を確認することとした。 ⑭個人情報の持出、返却確認及び受け渡しの際の確認の徹底を行う。また、作業工程等を点検し、作業方法やチェック方法等ミスが起きにくい方法を検討、実施する。 ⑮郵便の発送作業は複数職員でチェックすることを再徹底。また、特に慎重を要する個人情報を取り扱う施設における個人情報の事故の重大性について改めて周知するとともに、書類の発送、保管、業務の進行管理等について、注意喚起や指導を行った。 ⑯（1）ファイルが他の物に紛れてしまわないよう、目立つ色に変更する。 （2）作業スペースに仕切りを立てて、使用スペースを物理的に限定する。 （3）ファイルに記載する名前をイニシャルに表記変更する等、使用する情報から個人情報を削除する。 （4）決まった時間に決まった人員が所在を確認する。 （5）チェックの時間を定刻とし、声をかけ合う。 （6）出したらしまうといった基本的事項を、改めて徹底するよう、注意喚起する。 （7）急いでいたり、忙しい時間帯でも、ダブルチェックをするよう、改めて徹底する。また、退所時にも荷物を確認してから渡すようにする ⑰（個人情報の管理について） （1） 相談援助業務上の記録をノート等に記載する場合は、イニシャルを使用するなど個人情報を特定されないようにすること。また、私物のノートや手帳に個人情報を記載しないこと。 （2） 庁舎外での会議等に出席した際には、個人端末を活用して記録の作成を行うとともに、作成した文書は暗号化し保存すること。 （3） 業務上やむを得ず個人情報が記録された書類を庁舎外に持ち出す場合は、局の保有個人情報安全管理基準に基づき管理職の許可を得ること。 （4） 個人情報を含む書類を持ち出すにあたっては、盗難や紛失を防止できる形状・機能を持つ鞄に収納し、肌身離さず持ち運ぶなど十分に注意すること。 （5） その他個人情報の取り扱いについては、局の保有個人情報安全管理基準等を遵守し、適正に行うこと。 （職員の証票の管理について） （1） 月1回、各職員の保有状況を点検すること （2） 携行する際には、ストラップ付きのケースに収納するなど、常に身体から離さずに携行することを徹底すること （職員の緊急連絡網の管理について） （1） 必要な連絡先は公用携帯に保存し、連絡網を記載した紙は庁舎外に持ち出さないこと。 ⑱（1）入所時や退所時の手順確認のチェックリスト様式を変更し、入所時の写真撮影やリストへの正確な情報記載、退所時の荷物確認の手順など守るべきルールを追記するとともに、実施者を記載する欄を追加。 （2）個人情報紛失判明時の、本部への速やかな報告や具体的な捜索の手順などを、チェックリストに追記。 （3）毎朝のミーティングにてリーダー看護師等に個人情報保護の重要性やルールの順守を徹底。勤務者には、業務実施前に最新のマニュアルを確認するよう指導。 ⑲（1）発表資料の事前確認の徹底について幹部会で決定し、各部署に注意喚起 （2）録画や写真撮影をして保管していない旨を書面で確認 （3）画像等の個人情報の収集・利用に関する同意手続きの見直し ⑳（1）電子申請を推奨して紙文書の紛失リスクを軽減 （2）個人情報の適切な管理を職員に改めて周知徹底 ㉑（1）病院へ持ち運ぶファイルに、処方箋を収納する専用スペースを作る （2）医療機関受診時に係るマニュアルを作成 （3）帰園後は可能な限り速やかに所管部署に処方箋等を提出する （4）重要な個人情報を預かっている状況での裁断作業を避ける

		(5)上記対応について、ミーティング等で周知徹底、注意喚起 ㉒(1)必要なデータファイルのみを送信用データとしてPDF化し、送信前に、PDFに不要な箇所が入っていないことを確認の上、送信することを徹底 (2)メールシステム上、外部送信時に必須である上長の承認の際、個人情報が含まれていないか等の確認を徹底 (3)「メール送信時のセルフチェックリスト」を作成、活用 (4)各管理職より各職員に対する面談時に、個別に再度、再発防止策を徹底 ㉓(1)交付前の事務手順や確認方法の見直し、交付時の最終確認方法の見直し (2)作業スペースへの注意文の掲示やチェックリストへの注意文の記載 (3)確認等を行う人数を増員し、誤交付を防ぐ体制を強化 (4)再発防止勉強会を実施 ㉔(1)委託事業者及び再委託事業者に厳重注意、再発防止策等の作成を指示し、受領 (2)WEBページの脆弱性等の確認を受けるため、デジタルサービス局との調整を開始 ㉕(1)精査が十分でないデータを外部に提供しないこと、精査及び送付の際には複数体制でチェックすることを徹底 (2)受託事業者において、作成した資料のレビューフローの再検討、個人情報データの受領・管理方法に関する社内再教育等の取組を実施 ㉖(1)ダブルチェックの徹底及びその旨の指導 (2)作業項目の文章化、わかりやすいチェックリストの作成 ㉗(1)受託事業者において、マニュアルに沿った処理を徹底し、送付書類の引継ぎ時には、郵便局ともに引継ぎ件数ーを確認 (2)3か月間、受託事業者から送付先に対し、発送日の連絡及び到着の確認を行う。 ㉘(1)原則電子申請として紙文書の紛失リスクを軽減 (2) 書類の所在及び処理状況を明確に把握できるよう管理方法を見直す ㉙(1)個人情報の取扱い及び情報管理の徹底等について、厳重に注意喚起 (2)個人情報が特定できない記載にする等の対策 ㉚(1)局内各職場にて個人情報事故防止対策等をテーマとした職場討議実施 (2)個人情報安全管理強化月間の自己点検・職場点検による一層の意識啓発 ㉛(1)張り紙の掲示、FAXボタンへの着色による物理的な注意喚起 (2)FAX送付時のダブルチェック、送信履歴の確認等をマニュアルに追加 ㉜(1)区市町村からの書類を収受する際の件数記載用の共通様式を作成し、受領時に種類ごとの件数を確認・記入 (2)本件の事務のプロセスを細分化し、各プロセス毎の書類の受渡し時に、各担当者がそれぞれ(1)の様式に記載した件数に基づき、書類、件数の確認作業を行うよう整理 (3)使用頻度ごとに文書の保管場所を整理し、常時使用しないものは施錠。作業中に開錠しているキャビネットについても、中に担当者ごとの鍵付きの引き出し等を設置して自分の担当以外の書類は持ち出せないようにし、作業の際にその都度施錠。 (4)緊急の所内幹部会を開催し、個人情報を含む書類の受け渡し時の確認等、個人情報の取り扱いのルールが適正に行われているか確認を指示し、報告を受ける。 ㉝(1)個人情報の保管ルールについて全職員に徹底 (2)現在の保管状況の再点検を実施 ㉞(1)受託事業者に対する個人情報の取扱い及び情報管理の徹底に向けた注意喚起 (2)管理番号の活用など個人情報が特定できない情報管理方法等の導入 ㉟(1)廃棄時の職員立会いの徹底、チェックリストの作成、活用 (2)廃棄対象文書とシステム登録情報の照会の実施 ㊱書類の保管場所の見直し
⑩死者の個人番号		[保管している] <選択肢> 1) 保管している 2) 保管していない
	具体的な保管方法	生存者の個人番号と同様の方法にて安全管理措置を実施している。
その他の措置の内容		バックアップデータについても、システムで使用している元データと同様の方法にて安全管理措置を実施している。
リスクへの対策は十分か		[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク2： 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	・納税義務者の異動に際しては、法令等に則り、適切に届出等を行うよう周知を行っている。 ・税務調査で異動の事実が判明した場合は、情報の更新を行っている。	
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	【地方税外部連携システム（サーバー）】 一定期間経過後、バッチ処理により削除する。 また、機器リース期間満了時には特定個人情報等のデータを全て消去の上、消去結果について、記録媒体ごとに、消去した情報項目、数量、消去方法及び消去日時を明示した書面で委託事業者より報告を受けている。	
その他の措置の内容	ー	
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		
仕様書において、文書の安全管理や秘密の保護、作業方法、業者の資格等様々な条件を定め、リスクに対する措置を行っている。		

Ⅳ　その他のリスク対策 ※

1. 監査		
①自己点検		[　　十分に行っている　　] ＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
	具体的なチェック方法	・サイバーセキュリティ責任者・個人情報管理責任者・特定個人情報管理責任者及び全職員は、毎年度1回以上、点検表に基づき、職場の文書管理、サイバーセキュリティ及び個人情報安全管理に関する点検を行っている。点検結果については、主税局サイバーセキュリティ委員会へ報告している。 ・国税連携システム（eLTAX）については、「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（平成25年総務省告示第206号）」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ついては、運用規則等に基づき、中間サーバ・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。
②監査		[　　十分に行っている　　] ＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
	具体的な内容	運用規則等に基づき、税務総合支援システム等について、定期的に監査を行うこととしている。 1．内部監査 以下の観点で内部監査人による特定個人情報保護監査を所属ごとに3年に1回実施している。 ・自己点検結果の確認 ・情報資産台帳・情報処理機器等の保有状況簿の確認 ・情報資産の保管・持ち出し等に係る帳票等の確認 ・執務室の視察 2．外部監査 以下の観点で、税務総合支援システム等を対象とした外部監査人による監査を定期的に実施している。 ・サーバー機器等に対する脆弱性診断 ・セキュリティポリシー遵守や運用管理体制に関するヒアリング 3．その他 ・国税連携システム（eLTAX）については、サイバーセキュリティ監査（外部監査）を実施している。 ・地方税法ポータルセンタ（eLTAX）については、運営する地方税共同機構が、毎年度、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ついては、運用規則等に基づき、定期的に監査を行うこととしている。また、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者は、定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。
2. 従業者に対する教育・啓発		
従業者に対する教育・啓発		[　　十分に行っている　　] ＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
	具体的な方法	【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）が提供する最新のサイバーセキュリティ教育用資料等を基にセキュリティ教育資材を作成し、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、運用規則（接続運用規程等）やサイバー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。 【税務総合支援システム】 ・全職員を対象にサイバーセキュリティ・個人情報保護の研修を実施している。研修の目的は、個人情報保護の重要性及び適正管理等に関する理解を深め、個人情報保護の遵守を徹底することである。具体的には、以下の研修を実施している。 ・毎年の悉皆研修 ・個人端末からアクセスするeラーニング研修（理解度が基準に達しないと修了できない） なお、未受講者については、翌年度同様の研修を受講させている。また、eラーニングについては、システムにより受講管理を実施し、未受講者に受講を促すことで、未受講者が出ないようにしている。 ・委託業務の従事者に対し、個人情報及び機密情報の取扱いについて必要な教育及び研修を実施させている。 【税務総合支援システム（サーバー）】 ・データセンタにおける緊急時対応を想定した訓練を毎年度実施している。

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。

Ⅴ　開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	東京都主税局総務部総務課 163-8001　東京都新宿区西新宿2-8-1 都庁第一本庁舎22階南側 03-5388-2922
②請求方法	法令等で定める様式による書面の提出により開示・訂正・利用停止請求を受け付ける。
特記事項	請求方法等について東京都公式ホームページ上で分かりやすく表示。
③手数料等	[　　有料　　]　　＜選択肢＞ 1) 有料　　2) 無料 （手数料額、納付方法：　納付書により、実費相当分（10円／1枚）の手数料を納付する。　　）
④個人情報ファイル簿の公表	[　　行っている　　]　　＜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	個人事業税の課税情報ファイル、自動車税（環境性能割・種別割）の課税情報ファイル、事業所税の課税情報ファイル、あて名管理ファイル、収入管理事務ファイル、滞納整理事務ファイル、固定資産税（土地・家屋）の課税情報ファイル、不動産取得税の課税情報ファイル、不動産登記済通知データ変換・加工システム、固定資産税（償却資産）の課税情報ファイル、情報連携ファイル
公表場所	東京都総務局総務部情報公開課
⑤法令による特別の手続	―
⑥個人情報ファイル簿への不記載等	―
2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	東京都主税局総務部総務課 163-8001　東京都新宿区西新宿2-8-1 都庁第一本庁舎22階南側 03-5388-2918
②対応方法	問合せの受付時に受付票を起票し、対応について記録を残す。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	令和7年9月18日
②しきい値判断結果	［　　基礎項目評価及び全項目評価の実施が義務付けられる　　］ ＜選択肢＞ 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 基礎項目評価及び重点項目評価の実施が義務付けられる（任意に全項目評価を実施） 3) 基礎項目評価の実施が義務付けられる（任意に全項目評価を実施） 4) 特定個人情報保護評価の実施が義務付けられない（任意に全項目評価を実施）
2. 国民・住民等からの意見の聴取	
①方法	東京都公式ホームページにおいて、全項目評価書を公開し、郵送及び電子メールにて意見を受け付けた。
②実施日・期間	令和7年6月24日（火曜日）から同年7月23日（水曜日）までの30日間
③期間を短縮する特段の理由	期間短縮なし
④主な意見の内容	意見なし
⑤評価書への反映	なし
3. 第三者点検	
①実施日	令和7年7月29日（火）から令和7年9月4日（木）まで
②方法	東京都情報公開・個人情報保護審議会特定個人情報保護評価部会において点検を受けた。
③結果	以下答申を受けた。 本評価書案を点検したところ、地方税の賦課徴収に関する事務における特定個人情報ファイルの取扱いについては、個人のプライバシー等の権利利益に与える影響を予測した上で、特定個人情報の漏えいその他の事態の発生に関して考慮すべきリスクを分析し、リスクを軽減するための適切な措置をおおむね講じていると認められる。
4. 個人情報保護委員会の承認 【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

（別添3）変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅰ 1. ②事務の内容（別紙1）	（省略）	（省略）	事前	実態に合わせ修正
令和7年2月28日	Ⅰ 2. システム1 ②システムの機能	・オンライン入力 ・課税データ等の一括更新処理 ・税務データ保存、帳票データ作成 ・外部からのデータ取込み（外部連携機能） ・外部へのデータ出力（外部連携機能） ・電子帳票機能 ・申告書等税務業務情報の保存（電子書庫機能） ・税務業務の電子決裁（電子決裁機能） ・スキャニングデータのテキストデータ（CSV）への変換及び修正機能（AI-OCR機能）	・職員等による税務情報のオンライン入力及び登録 ・課税データ等の一括更新処理 ・税務データ保存、帳票データ作成 ・外部からのデータ取込み（外部連携機能） ・外部へのデータ出力（外部連携機能） ・出力する書類の電子帳票化機能 ・申告書等税務業務情報の保存（電子書庫機能） ・税務業務の電子決裁（電子決裁機能） ・スキャニングデータのテキストデータ（CSV）への変換及び修正機能（AI-OCR機能） ・共通システムによる公簿等照会機能 ・モバイル端末へのデータ移行、モバイル端末上での税務情報の表示。	事前	実態に合わせ修正
令和7年2月28日	Ⅰ 2. システム4 ③他のシステムとの接続		[〇]情報提供ネットワークシステム	事前	実態に合わせ修正
令和7年2月28日	Ⅰ 5.	・番号法第9条第1項別表第一第16号 ・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に関する法律別表第一の主務省令で定める事務及び情報を定める命令　第16条	・番号法第9条第1項　別表24及び135 ・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別表の主務省令で定める事務を定める命令第16条 ・公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律第2条第2項	事前	実態に合わせ修正
令和7年2月28日	Ⅰ 6. ②法令上の根拠	・番号法第19条第8号、別表2 28の項 ・行政手続における特定の個人を識別するための番号の利用に関する法律別表第二の主務省令で定める事務及び情報を定める命令　第21条	番号法第19条第8号に基づく主務省令第2条の表49の項	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要① 2. ⑤保有開始日	令和9年1月1日	令和9年1月4日	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要① 3. ③入手の時期・頻度	（省略）	（省略）	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要① 3. ④入手に係る妥当性	（省略）	（省略）	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要① 3. ⑤本人への明示	（省略）	（省略）	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅱ ファイルの概要① 3. ⑥使用目的	適正・公平な賦課徴収を実現するため。	必要範囲の特定個人情報を保有することにより、適正かつ公平な賦課徴収を実現するため。	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要① 3. ⑧情報の突合	【個人事業税】 ＜個人事業税申告書等＞ ・申告書等に記載された所得情報等と所得税申告書等情報を突合（目視による確認）し、適正な申告であることを確認する。 【固定資産税（土地・家屋）】について記載なし 【収入管理】 ＜収納データ＞ 金融機関等から入手した収納データと課税徴収マスタを突合し、納税者の収入管理を行う。	【個人事業税】 ＜個人事業税申告書等＞ ・あて名管理システムに登録されている納税義務者・申告義務者情報（氏名・住所）と、住民票の写し等に記載されている情報を突合し、現住所が正しいものかを確認する。 ・申告書等に記載された所得情報等と所得税申告書等情報を突合（目視による確認）し、適正な申告であることを確認する。 【固定資産税（土地・家屋）】 ＜死亡者情報＞ あて名管理システムに登録されている納税義務者情報（個人番号又は氏名・住所）と、死亡者情報の情報をシステム上で突合（検索）し、システム上に存在するあて名であるかどうかを確認する。 【収入管理】 ＜収納データ＞ 金融機関等から入手した収納データと課税徴収マスタを突合し、納税者の収入管理を行う。 ＜公金受取口座＞ あて名管理システムに登録されている納税義務者情報（住所、氏名等）と請求書兼口座振替依頼書を突合し、 情報提供ネットワークシステムに対して公金受取口座情報の照会を行うべきかを確認する。	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要① 3. ⑨使用開始日	令和9年1月1日	令和9年1月4日	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要② 2. ②対象となる本人の数	100万人以上1,000万人未満	1,000万人以上	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要② 2. ④主な記録項目	・識別情報 [○]個人番号[　]個人場号対応符号[○]その他識別情報（内部符号）	・識別情報 [○]個人番号[○]個人場号対応符号[○]その他識別情報（内部符号）	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅱ ファイルの概要② 3. ③入手の時期・頻度	【所得税申告書等】 国税連携システムで受信した所得税申告書等データを税務総合支援システムに取込み入手する。 取込みは随時実施する。	【国税庁・税務署からの電子データでの入手】 ・国税当局に提出された個人番号が記載された所得税申告書等情報を地方税ポータルシステムeLTAX)を通じてデータで定期的に受信している。 ・2～5月の繁忙期は休日を除くほぼ毎日受信。 ・6～1月は月1回受信。 【照会・回答情報】 国税連携システムで受信した照会・回答情報データを税務総合支援システムに取込み入手する。 取込みは随時実施する。	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要② 3. ④入手に係る妥当性	【所得税申告書等】 地方税法第72条の55の2第1項により国税庁・税務署へ所得税の申告等をしたものは道府県知事（都知事）へ個人事業税の申告もしたものとみなされ、また、同法第72条の59第1項により道府県知事（都知事）が国税庁・税務署に対し、事業税の賦課徴収について所得税の申告書等の書類を閲覧又は記録することを請求した場合は、国税庁・税務署は道府県知事（都知事）又はその指定する職員に関係書類を閲覧させ、又は記録させることと規定されている。	【所得税申告書等】 地方税法の規定により国税庁・税務署へ所得税の申告等をしたものは道府県知事（都知事）へ個人事業税の申告もしたものとみなされることから、国税庁・税務署より所得税申告書等をデータにて入手する。なお、他道府県も同規定に基づき国税庁・税務署からデータを入手するとともに事務所、事業所の所在地が都であることが判明した場合は都へデータを回送し入手している。 【照会・回答情報】 地方税法第20条の11及び国税徴収法146条の2の規定により、地方税及び滞納処分に関する調査について必要があるときは、事業者（特別の法律により設立された法人を含む。）又は官公署に、当該調査に関し参考となるべき簿書及び資料の閲覧又は提供その他の協力を求めることができることから、国税庁・税務署より照会・回答情報のデータを入手する。	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要② 3. ⑤本人への明示	【所得税申告書等】 地方税法第72条の55の2第1項により国税庁・税務署へ所得税の申告等をしたものは道府県知事（都知事）へ個人事業税の申告もしたものとみなされ、また、同法第72条の59第1項により道府県知事（都知事）が国税庁・税務署に対し、事業税の賦課徴収について所得税の申告書等の書類を閲覧又は記録することを請求した場合は、国税庁・税務署は道府県知事（都知事）又はその指定する職員に関係書類を閲覧させ、又は記録させることと規定されている。	【所得税申告書等】 地方税法の規定により国税庁・税務署へ所得税の申告等をデータにてしたものは道府県知事（都知事）へ個人事業税の申告がされたものみなすことが規定されており、国税関係書類の入手を行っている。 【照会・回答情報】 地方税法第20条の11及び国税徴収法146条の2の規定の規定により、事業者又は官公署への簿書及び資料の閲覧又は提供その他の協力を求めることができるとされている。	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要② 3. ⑥使用目的	個人事業税の適正かつ公平な賦課及び徴収の実現のため。	適正かつ公平な賦課及び徴収を実現するため。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅱ ファイルの概要② 3. ⑧使用方法	【所得税申告書等】 〇国税連携システムで受信し税務総合支援システムへ取込む所得税申告書等データ 　国税連携システムで受信した所得税申告書等データを税務総合支援システムに取込み、告書等関係書類の情報と併せて審査し、課税処理等のシステム登録を行う。	【所得税申告書等】 　国税連携システムで受信した所得税申告書等データを税務総合支援システムに取込み、申告書等関係書類の情報と併せて審査し、課税処理等のシステム登録を行う。 【照会・回答情報】 ・国税連携システムで受信した照会情報データを税務事務総合支援システムに取込み、あて名情報との突合を行う。 ・財産差押等滞納処分のためシステム登録を行う。	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要② 3. ⑧情報の突合	【所得税申告書等】 ・あて名管理システムに登録されている納税義務者情報（氏名・住所）と入手した所得税申告書等に記載及び記録されている情報を突合（検索）し、システム上に存在するあて名であるかどうかを確認する。	【所得税申告書等、照会・回答情報】 ・あて名管理システムに登録されている納税義務者情報（氏名・住所）と入手した所得税申告書等に記載及び記録されている情報を突合（検索）し、システム上に存在するあて名であるかどうかを確認する。	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要② 5. 提供先2 ①法令上の根拠	地方税法第72条の55の2第1項、第72条の59第1項	地方税法第72条の55の2第1項、第72条の59第1項、国税徴収法第146条の2、国税通則法第74条の12	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要② 5. 提供先2 ②提供先における用途	東京都に閲覧させる資料の選定	東京都に閲覧させる資料の選定及び滞納処分に関する調査	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要② 5. 提供先2 ③提供する情報	所得税申告書等データ	所得税申告書等データ、固定資産税情報及び都市計画税情報、自動車税課税情報、滞納情報（地方税）	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要② 5. 提供先2 ④提供する情報の対象となる本人の数	1万人未満	10万人以上100万人未満	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要② 5. 提供先2 ④提供する情報の対象となる本人の範囲	東京都に課税権がある個人事業税の納税義務者及び調査対象者	納税義務者及び調査対象者	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要② 5. 提供先2 ⑦時期・頻度	国税連携システムにて一括でデータ送信を受けたものだけでは審査ができず、国税に追加の資料要求を行う都度発生する。	国税連携システムにて一括でデータ送信を受けたものだけでは審査ができず、国税に追加の資料要求を行う都度発生する。 国税庁から照会データの送信がある度、随時提供する。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅱ ファイルの概要② 6. ③消去方法	【国税連携システム（サーバー）】 ・保存年限を経過した課税データについて、電子データの削除等に関する規定に基づき、委託先によるバッチ処理により削除している。 ・機器リース期間満了時には特定個人情報等のデータを全て消去の上、消去結果について、記録媒体ごとに、消去した情報項目、数量、消去方法及び消去日等を明示した書面で委託事業者より報告を受けている。 【国税データ閲覧機能（サーバー）】 契約書により、7年保存するという契約履行完了時には、業務に係る情報を記録した一切の媒体については、記録媒体上に含まれる当該委託業務に係る情報を全て消去して、その消去結果について、記録媒体ごとに、消去した情報項目、数量、消去方法及び消去日等を明示した書面で委託者に報告することが規定されている。	【国税連携システム（サーバー）】 ・保存年限を経過した課税データについて、電子データの削除等に関する規定に基づき、委託先によるバッチ処理職員によるオンライン処理により削除している。 ・機器リース期間満了時には特定個人情報等のデータを全て消去の上、消去結果について、記録媒体ごとに、消去した情報項目、数量、消去方法及び消去日等を明示した書面で委託事業者より報告を受けている。 【国税データ閲覧機能（サーバー）】 契約書により、7年保存するという契約履行完了時には、業務に係る情報を記録した一切の媒体については、記録媒体上に含まれる当該委託業務に係る情報を全て消去して、その消去結果について、記録媒体ごとに、消去した情報項目、数量、消去方法及び消去日等を明示した書面で委託者に報告することが規定されている。	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要④		④デジタル納税通知システム事務ファイル（仮称）について新規で記載。	事前	実態に合わせ修正
令和7年2月28日	Ⅲ リスク対策① 2. リスク1　別紙6	（省略）	（省略）	事前	実態に合わせ修正
令和7年2月28日	Ⅲ リスク対策① 2. リスク1　別紙7	（省略）	（省略）	事前	実態に合わせ修正
令和7年2月28日	Ⅲ リスク対策① 2. リスク1　別紙8	（省略）	（省略）	事前	実態に合わせ修正
令和7年2月28日	Ⅲ リスク対策① 2. リスク1　別紙9	（省略）	（省略）	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策① 3. リスク1事務で使用するその他システムにおける措置の内容	・税務総合支援システムでは、税務事務に係るデータのみを保有しているため、税務事務以外の情報と紐付けることはできない。 【AI-OCR】 ・AI-OCRは、税務総合支援システムと同様、税務事務に係るデータのみを保有しているため、税務事務以外の情報と紐づけることはできない。 【電子書庫】 ・電子書庫は、税務総合支援システムと同様、税務事務に係るデータのみを保有しているため、税務事務以外の情報と紐づけることはできない。 【EUC】 ・EUCは、税務総合支援システムと同様、税務事務に係るデータのみを保有しているため、税務事務以外の情報と紐づけることはできない。 【電子決裁】 ・電子決裁は、税務総合支援システムと同様、税務事務に係るデータのみを保有しているため、税務事務以外の情報と紐づけることはできない。 【外部連携基盤】 ・外部連携基盤は、税務総合支援システムと同様、税務事務に係るデータのみを保有しているため、税務事務以外の情報と紐づけることはで	税務総合支援システムでは、税務事務に係るデータのみを保有しているため、税務事務以外の情報と紐付けることを禁止している。	事前	実態に合わせ修正
令和7年2月28日	Ⅲ リスク対策① 3. リスク2ユーザー認証の管理	①税務総合支援システムを使用する職員に対して、静脈等による生体認証およびID・パスワードを用いた認証の二要素認証を導入する。なお、IDについては職員毎に割り当てを行うものとする。 ②パスワードは一定期間ごとに変更しなければならず、システム上も、同頻度でのパスワード変更を利用の必須条件とする。 ③操作内容は、操作ログとして保管されており、いつどのIDでログインしたのかを把握できる。 【AI-OCR】 （認証については、税務総合支援システムと同様に実施している。 【電子書庫】 （認証については、税務総合支援システムと同様に実施している。 【EUC】 （認証については、税務総合支援システムと同様に実施している。 【電子決裁】 （認証については、税務総合支援システムと同様に実施している。 【外部連携基盤】 （認証については、税務総合支援システムと同様に実施している。	①税務総合支援システムを使用する職員に対して、静脈等による生体認証およびID・パスワードを用いた認証の二要素認証を導入する。なお、IDについては職員毎に割り当てを行うものとする。 ②操作内容は、操作ログとして保管されており、いつどのIDでログインしたのかを把握できるようにしている。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策① 3. リスク2アクセス権限の発効・失効の管理	①人事担当部署が職員の異動情報を把握又は公表次第、異動情報をシステム管理部署へ連絡される。これに基づき、システム管理部署が各ユーザIDに必要な権限を付与・削除する。 【AI-OCR】 （認証については、税務総合支援システムと同様に実施している。 【電子書庫】 （認証については、税務総合支援システムと同様に実施している。 【EUC】 （認証については、税務総合支援システムと同様に実施している。 【電子決裁】 （認証については、税務総合支援システムと同様に実施している。 【外部連携基盤】 （認証については、税務総合支援システムと同様に実施している。	人事担当部署が職員の異動情報を把握又は公表次第、異動情報をシステム管理部署へ連絡される。これに基づき、システム管理部署が各ユーザIDに必要な権限を付与・削除する。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策① 3. リスク2アクセス権限の管理	①アクセス権限については、システム管理部署が全ての権限を一元的に管理し、操作者の所属及び業務に合わせて、システムの機能ごとに「更新・参照可」、「参照のみ可」、「更新・参照不可」の権限を設定する。 ②設定に際しては、サブシステム所管部署より権限設定申請を受領し、システム管理部署での承認を経て申請内容をシステムへ反映する。 ③設定済の内容については、毎年度末に見直しを行うことにより、付与する権限に過不足が生じないようにする。 ④権限に変更を加えた際には、システム管理部署が登録した権限設定状況を示した各サブごとの一覧表を確認することにより、どの部署にどのような権限が設定されているのかを把握できるようにしている。 ⑤年に1度、全ての権限について打鍵テストを行い、権限設定が正しく行われていることを確認する。 【AI-OCR】 ・システム管理部署が職員に対して、所属や職位等をもとにアクセス権を付与・削除している。 ・システム管理部署がフォルダの新規作成・構成変更を一元的に管理している。 【電子書庫】 ・システム管理部署が職員に対して、所属や職位等をもとにアクセス権を付与・削除している。 ・システム管理部署がフォルダの新規作成・構成変更を一元的に管理している。 【EUC】 ・システム管理部署が職員に対して、所属や職位等をもとにアクセス権を付与・削除している。 【電子決裁】 ・システム管理部署が職員に対して、所属や職位等をもとにアクセス権を付与・削除している。 【外部連携基盤】 ・システム管理部署が職員に対して、所属や職位等をもとにアクセス権を付与・削除している。	①アクセス権限については、システム管理部署が全ての権限を一元的に管理し、操作者の所属及び業務に合わせて、システムの機能ごとに「更新・参照可」、「参照のみ可」、「更新・参照不可」の権限を設定する。 ②設定に際しては、サブシステム所管部署より権限設定申請を受領し、システム管理部署での承認を経て申請内容をシステムへ反映する。 ③設定済の内容については、毎年度末に見直しを行うことにより、付与する権限に過不足が生じないようにする。 ④権限に変更を加えた際には、システム管理部署が登録した権限設定状況を示した各サブごとの一覧表を確認することにより、どの部署にどのような権限が設定されているのかを把握できるようにしている。 ⑤年に1度、各サブシステムに画面表示等の権限設定のヒアリングを行ったうえで、付与されている権限が適切かサブシステムの所管部署の職員がシステムを直接操作してテストを実施している。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策① 3. リスク2特定個人情報の使用の記録	①システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、どのユーザIDで、どの情報にアクセスし、抽出したのかを記録し、この記録を保存している。なお、当該操作履歴はシステム利用者がアクセスすることはできず、改ざん防止を図っている。 ②また、特定個人情報等を記録した公文書が不要となった場合は、溶解等の復元不可能な手段により特定個人情報等の消去又は廃棄を行っている。 【AI-OCR】 ・ユーザ単位のアクセスの証跡を取得し、一定期間保存できるようにしている。 【電子書庫】 ・ユーザ単位のアクセスの証跡を取得し、一定期間保存できるようにしている。 【EUC】 ・データベースへのアクセス証跡をユーザ単位で取得、保管している。 【電子決裁】 ・ユーザ単位のアクセスの証跡を取得し、一定期間保存できるようにしている。 【外部連携基盤】 ・ユーザ単位のアクセスの証跡を取得し、一定期間保存できるようにしている	①システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、どのユーザIDで、どの情報にアクセスし、抽出したのかを記録し、この記録を保存している。なお、当該操作履歴はシステム利用者がアクセスすることはできず、改ざん防止を図っている。 ②また、特定個人情報等を記録した公文書が不要となった場合は、溶解等の復元不可能な手段により特定個人情報等の消去又は廃棄を行っている。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策① 3. 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	①入力した情報について、職員間でのダブルチェック等を行い、正確性を確保している。 ②特定個人情報ファイルについては、インターネットと接続している端末に転記・保存することのないよう規定し、研修等で職員に周知した上、所属ごとに3年に1回再点検や監査を実施している。 ③税務総合支援システムは、個人番号利用事務系のみとネットワーク接続、時間外使用不可、業務ごとに付与された権限外での使用不可、データ書き出し制限等、システムそのものに強力なセキュリティ対策を施すことで、不正使用のリスク対策を講じている。 ④ネットワークへのアクセスを許可されていない端末の不正接続について、常時監視を行っている。 ⑤不正使用を未然に防ぐため、毎年実施する研修で上記作業を行うことについて職員に周知している。 ⑥不正使用の疑いがある場合には、操作ログの確認を行っている。	①入力した情報について、職員間でのダブルチェック等を行い、正確性を確保している。 ②特定個人情報ファイルについては、インターネットと接続している端末に転記・保存することのないよう規定し、研修等で職員に周知した上、定期的な再点検や監査を実施している。 ③税務総合支援システムは、クローズドネットワーク、ネットワークへの接続を許可された専用端末以外からのアクセス不可、時間外使用不可、業務ごとに付与された権限外での使用不可、データ書き出し制限等、システムそのものに強力なセキュリティ対策を施すことで、不正使用のリスク対策を講じている。 ④ネットワークへのアクセスを許可されていない端末の不正接続について、常時監視を行っている。 ⑤不正使用を未然に防ぐため、毎年実施する研修で上記作業を行うことについて職員に周知している。 ⑥不正使用の疑いがある場合には、操作ログの確認を行っている。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策① 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか その内容	①平成31年4月7日、晴海客船ターミナル「客船友の会」※の会員に対して、4月の入港スケジュール等を送付する際、事務担当者が誤ってメールアドレスをBCC欄ではなくCC欄に入力して発信したため、個人情報が流出する事故が発生 (※) 晴海客船ターミナル「客船友の会」:晴海客船ターミナルに入出港する客船を歓迎するために平成25年に発足した会 ②平成31年4月8日、「外国人おもてなし語学ボランティア」育成講座の連携先団体(企業、大学等)の事務担当者に対して、東京都の担当者変更についてメール連絡した際、本来BCC欄に入れるべきメールアドレスを、宛先欄に入力して一斉送信したため、個人情報(メールアドレス)が流出する事故が発生 ③令和元年6月17日、「個人住宅建設資金融資あっせん制度」において、都から金融機関ごとに同制度の利用状況に関するデータをメールで送信する際に、1つの金融機関に送付したファイルに、当該金融機関以外の情報(個人住宅建設資金融資あっせん制度の利用者864人分の情報(氏名、融資額、前月及び当月利子補給対象元本額、償還内容、当月及び累計利子補給額、利率))を含んで送付した。 ④令和2年8月21日に東京都人権プラザにおいて開催した「心と体を傷つけられて亡くなった天国の子供たちのメッセージ」展のメディア向けカンファレンスの動画配信案内を(公財)東京都人権啓発センターの行事案内希望者に対して送付する際、事務担当者が誤ってメールアドレスをBCC欄ではなく、CC欄に入力して発信したため、個人情報が流出する事故が発生した。	①令和4年5月、東京都現代美術館において、ミュージアムショップ運営の受託事業者スタッフが、展覧会図録を予約した顧客へ一斉に案内メールを送信する際、メールアドレスをBCC欄ではなく、宛先欄に入力して発信した。 ②令和4年5月、技能検定試験に関する通知を外国人技能実習の複数の監理団体に対しメールで送付する際、誤ってメールアドレスをBCC欄ではなく、CC欄に入力し、一斉送信した。 ③令和4年5月、就学支援金事務において、就学支援金の基礎データをCD-Rに情報を保存し、対象高等学校等宛て一斉に送付したところ、そのうち1校に、他校の受給者に関する情報が含まれていることが判明した。 ④令和4年5月、受託事業者が、事業に関するイベントを案内するメールマガジンを送付する際、配信プログラム改修ミスにより、宛先欄に複数のメールアドレスが入力され、送信された。 ⑤令和4年10月、東京都陽性者登録センターの運営受託事業者が、医療機関で新型コロナウイルス陽性の診断を受け、センターに登録申請を行った複数の患者への登録完了メールを、送付先アドレスが全て入れ替わったまま送信した。 ⑥令和4年12月、労働力調査の統計調査員に対して連絡事項をメールした際、BCC欄に入力して送るべきところを宛先欄に入力し、一斉送信した。 ⑦令和5年4月、再委託先の派遣会社職員が、業務で使用するシステムを不適切に使用し、個人情報を閲覧、メモにとり自宅に持ち出した。 ⑧令和5年5月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑨令和5年6月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策① 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか その内容	⑤東京都電子調達システムにより印刷物の契約案件を公表した際、印刷物の配布先となる町会名のみを公表するところ、誤って中野区内の町会の代表者の氏名、住所及び電話番号を1月28日から2月3日までの間、公表してしまった。 ⑥助成金返還事務のため、ワンビシより平成29年度教育助成金調査票（B表）を預かっていた。ワンビシへの返却手続きを行った際に段ボール二箱分がないことが発覚した。当該段ボール箱は執務室内の空きスペースにて保管していた。 ⑦令和3年7月、都のインターンシップ関連イベントに係る告知メールを送信する際、都が過去に出展した民間企業主催の就職イベント参加者及び当該企業に対して都関連の採用情報の提供を希望した者のメールアドレスを、「BCC」欄ではなく「TO」欄に入力して一斉に送信したため、個人情報が流出する事故が発生した。 ⑧令和3年9月、東日本大震災都内避難者向けに作成する「都内避難者の皆様への定期便」の一部について、送付業務の受託者が誤って本人以外の避難者の宛名を記載して発送してしまい、氏名が流出する事故が発生した。 ⑨令和3年12月、都営住宅の毎月募集の申込者に対して、東京都住宅供給公社において、抽せん番号をお知らせする郵便はがきを発送する準備を行い、料金別納で郵便局に持ち込みを完了したつもりであったが、後日、郵便局に確認したところ、持ち込まれたことを示す書類がないことが判明した。申込者に電話で確認したところ、郵便はがきが届いていることを確認できなかったため、申込者の氏名、住所等が記載されたはがきを紛失する事故が発生した。	⑩令和5年7月、施設を退所する患者に関して、退所先候補の施設と受入調整を行うため、診療関係書類をFAX送信した際、誤って別のFAX番号宛てに送信した。 ⑪令和5年8月、申請により受け付けた申請書が紛失していることが発覚した。 ⑫令和5年9月、関係施設宛に都民情報をFAX送信した際、誤って別の事業者宛てに送信した。 ⑬令和5年9月、事業の対象者に案内チラシを郵送した際、送付対象者の抽出ツールのプログラム仕様の不備により、誤って事業対象外の方に送付したことで、旧住所宛てに送付し返戻されなかったものが誤送付となった。 ⑭令和5年9月、決定通知書に公印を押印する目的で本庁に出張し、押印後持ち帰ったが、発送の準備をしていた際に、通知書1枚が紛失していることが発覚した。 ⑮令和6年1月、患者A宛てに送付すべき利用者情報を、誤ってB宛てに送付した。 ⑯令和6年1月、入所者の診療関係ファイルが紛失していることが発覚し、その後、退所者の荷物の中に当該ファイルが混入していたことが発覚した。 ⑰令和6年2月、児童相談所の職員が、出張中に個人情報が記載されている手帳を紛失し、あわせて手帳に収納されていた、当該職員の証票及び所内職員の緊急連絡網を紛失した。 ⑱令和6年2月、施設を退所した患者Aに関する薬剤情報等を記載した書類を、誤って別の患者の退院時の荷物に混入させ交付した。 ⑲令和6年2月、オンライン研修で使用した映像において、患者の情報をマスキング処理していたところ、当該映像をスマートフォンで視聴した場合に、マスキングが外れ、個人が特定できる状態になっていたことが判明した。 ⑳令和6年4月、受け付けた申請書を紛失していることが発覚した。 ㉑令和6年4月、施設職員が、利用者の通院付添の際、処方箋を紛失した。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策① 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか その内容		㉒令和6年4月、指定管理者が、事業者に対してExcel資料をメールで送信した際、本来削除すべきだった個人情報の入力されたシートを削除しなかった。 ㉓令和6年7月、受託事業者が、都へ交付すべき納入済通知書を、誤って他の事業者宛てに交付したことが発覚した。 ㉔令和6年7月、受託事業者がイベントを行った際の申込時の個人情報が掲載されたウェブページが、一時外部からアクセス可能な状態となっていたことが発覚した。 ㉕令和6年7月、職員が、説明会の資料の中に個人情報が含まれていることに気が付かずに、各自治体にデータを配布した。 ㉖令和6年7月、職員が、A宛てに送付すべき個人情報を、誤ってB宛てに送付していたことが発覚した。 ㉗令和6年7月、受託事業者から送付した個人情報を含む資料が、紛失していることが発覚した。 ㉘令和6年7月、受け付けた申請書を紛失していることが発覚した。 ㉙令和6年8月、受託事業者が配付した資料の中に、個人情報等が含まれる資料が混入していたことが発覚した。 ㉚令和6年10月、職員が、受託者に資料をメールで送信した際、誤って個人情報が記載された別のファイルを添付した。 ㉛令和6年10月、受託事業者が、A宛てに送付すべき電話記録を、誤ってB宛てにFAXで送信した。 ㉜令和6年11月、受け付けた申請書を紛失していることが発覚した（後日発見）。 ㉝令和6年11月、令和3年頃に個人情報が記載された資料を紛失していたことが発覚した。 ㉞令和6年12月、受託事業者が、個人情報が記載された資料を、誤って外部へ送信した。 ㉟令和7年1月、受託事業者が、個人情報が記載された資料を、誤って期限前に廃棄した。 ㊱令和7年1月、受け付けた届出書が、誤って机ごと廃棄されていることが発覚した。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策① 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか再発防止策の内容	①社員教育を実施し、個人情報保護法等関係法令等に則った対応について点検・実施を行う。 ②・平成31年４月９日に係会を開催し、情報管理の重要性について話し合うとともに、平成30年度に職員に対して周知した、個人情報等に関する注意喚起事項を改めて全員に配布・説明し、コンプライアンス意識の徹底を図った。 ・他局での事故発生に係るプレス発表時等には、係内で情報共有するとともに、複数の宛先にメール送信する際のBCC利用・複数職員による確認の徹底していく。 ・メール送付に限らず、管理ミス・誤操作・紛失・置き忘れなど「うっかりミス」による個人情報の漏えい事故防止のため、個人情報管理徹底に関する周知を継続的に実施することで意識向上を図っていく。 ・生活文化局情報セキュリティ委員会において、各部署の庶務担当課長と共に、今回の事故について共有し、再発防止につなげていく。 ③メールによる連絡等を行う場合は、複数の担当者により、送信先及び添付ファイルの内容について確認することを徹底する。また、今後、再発防止のため、個人情報を厳正に管理するとともに、職員に対し、情報セキュリティの確保に向け指導等を徹底していく。 ④団体に対し、外部へ一斉送信する際は、メールアドレスをBCC欄に入力すべきことと、メール送信前に、複数の職員で宛先の確認作業を必ず行うことを、職員全員に改めて周知徹底するとともに、組織としての検証を行い、再発防止策を検討するよう指導した。	①(1)ミュージアムショップにおいて、本社セキュリティインシデント統括部と連携して、個人情報取り扱い、情報管理体制の改善を行う。 (2)特に複数人へのメール送信に際してはダブルチェックを徹底する。 (3)現代美術館全委託業者に、適切な個人情報等の取扱い及び情報管理を徹底するよう指示する。 (4)財団が管理運営する各施設にも本事案を共有し、個人情報を含む情報の適切な管理を徹底する。 ②(1)個人情報の取扱い及び情報管理の徹底等について周知するとともに、職員全員に臨時研修を速やかに実施 (2)誤送信防止に向けたシステムの導入(ダイアログの自動表示など) (3)複数人チェックなど基本的対策の徹底 ③チェック機能を再検証し、全日制等と同様の仕組みを通信制にも直ちに導入するほか、事務フローの再構築を行い、再発防止に努める。そのうえで、本件を財団内で広く共有させ、個人情報の取扱い全般についてハード・ソフトの両面から厳しく見直すとともに、職員の意識向上を図っていく。また、都の実施機関においても個人情報の適正管理とサイバーセキュリティー対策について改めて確認を行う。 ④(1)システムの改善 メールマガジンの配信は、これまで「TO」により自動で1件ずつ送信がされる仕組みであったが、一括メール送信においては送信者アドレスを全て「BCC」に入れるようシステム改修を行う。 (2)システム会社における確認体制の強化 開発前にシステム会社が実施する、影響調査・テスト内容等について、これまでの2名体制によるダブルチェックから、システム会社のプロジェクトマネージャーも加えることとし、確認した内容を報告させて承認する運用へ見直す。 (3)受託事業者における確認体制の強化 システム会社のテスト結果の確認にあたっては、テストの証跡情報の提出を求め、内容の確認を行うとともに、受託事業者での運用テストでは要件定義とも照らした確認を担当だけでなく管理職も実施することにより徹底する。 ⑤受託事業者に対して厳正に指導し、登録完了メール送信作業のチェック体制を強化させる。 ⑥(1)部コンプライアンス推進委員会の臨時開催 ・メール送信時のダブルチェックを徹底させるため、個人情報等の取扱いに係るチェックリストの全職員での点検により注意を喚起、情報管理を再徹底する。 ・あわせて、最近の事故事案の事例を周知するなど、事故の再発予防を進める。 (2)定期的な事故防止意識の醸成 統計調査員を含む全職員を対象に、各所属長や指導員から情報セキュリティや感染拡大防止等に関する指導を定期・継続的に行い、危機意識の醸成等を図る。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策① 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか 再発防止策の内容	⑤（1）事務フローの見直し ・起工部署の事務フローを、別紙1のとおり見直し、周知徹底を図る。 ・契約部署は、着手起案作成時及び発注図書登録時、電子調達システムに、起工部署から提出されたPDFデータを公表前の登録を行ってから印刷した上で、契約依頼文書に添付された仕様書と照合し、一致していることを確認する。また、この確認方法について、令和元年12月19日付経理部契約課長事務連絡「契約事務に係る情報漏えい等の防止策について」により配布されたチェックリストに追記した。 （2）臨時支所コンプライアンス推進委員会の開催 ・臨時支所コンプライアンス推進委員会を開催し、再発防止に向け、上記事務フローの見直しの周知徹底を図った。 ⑥（1）個人情報の重要性を再確認し、高い危機意識をもって個人情報の適正な管理・運 用を図るよう、改めて基本的な取扱いルールの徹底を図る。 （2）書類の所在及び処理状況が明確に分かるような管理方法の整備や、文書廃棄の際 の事務処理手順の整備など、書類管理の徹底に向けた仕組みの構築を図る。 ⑦（1）局内全職員に対して情報セキュリティ研修を実施し、二度と同様の事故を起こさないよう、情報セキュリティ対策の確認を徹底する。 （2）外部の複数の宛先に対してメールを送信する場合、「BCC」欄に入力するとと に、送信前に複数の職員によるチェックを徹底する。	⑦委託先における個人情報の閲覧・使用に当たっての権限の設定や、不適切な閲覧・使用・持ち出しを防止するための体制についてあらためて確認し、適切な運用を徹底させる。 ⑧（1）情報共有をしているホワイトボードの位置、記入欄が分かりにくいとの意見が出 ため、位置、記入方法について変更した。 （2）書類封入時のチェック手順中に、患者氏名の確認を明示した。 （3）2者確認を徹底するため、事務員のみでなく看護職員もチェックを行うこととし、 2者チェックが終わった段階で封書のチェックボックスに記載する。 （4）責任の所在を明確にするため「転院時退所セット確認書」を新たに作成し、チェ ックを行った職員が記名する。 ⑨（1）チェックリストを活用し、複数人、複数回のチェックを行うとともに、最終チェ ック者を統括責任者とすることで、誤封入等を防ぐ体制を整える。 （2）都職員が施設へ直接出向き、個人情報管理の実態確認を実施するとともに、対応 が不十分な場合は是正指導を行う。 （3）個人情報保護の研修を実施し、施設全体で個人情報保護の取り組み状況を共有し た上で、改善を徹底する。 ⑩（1）委託先に対し、個人情報に関する業務手順を見直し及び徹底を図ることや、全従 事者に対する個人情報保護研修を行うことを指導した。また、改善策の確認のた め、都が施設へ出向き、個人情報管理の実態を確認した。 （2）再委託先において、送付の際は、まずFAX以外の手段を調整し、止むを得ずFAXを使用する際には、FAX番号の聞き取りの際の復唱や、FAX送信前の送信先への番号の再確認、複数人で複数回のチェックを必ず行うこととした。また、全従業者に対する個人情報保護研修を行った。 ⑪（1）作業環境等を見直し、書類の混入等が起きにくい環境を整備 ①執務室内の作業スペースの確保及び活用 ②引き出し付きの棚をキャビネット内に新設し、書類の分類をよりしやすくした。 （2）委託業者との書類の受け渡し方法の変更（送付する判定機関ごとに数を確認しながら受け渡す）。 ⑫個人情報をFAX送信することを禁止するよう各施設に通知した。 ⑬抽出ツールのプログラム確認は、委託先事業者の運用チームのみが行っていたが、抽出ツールを作成・利用する際には、運用チームに加えて、開発チームと委託元である都の3者で抽出ツールのプログラムの仕様・設定を確認することとした。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策① 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか再発防止策の内容	⑧これまで実施してきた委託事業者への発送完了時の確認のほか、委託事業者職員による宛名、住所の複数チェック等、発送作業での確認作業を確実に実施させるとともに、都においても個人情報を含む情報の適切な取扱いについて、さらなる徹底を図り、再発防止に努める。 ⑨（1）スケジュールの情報共有と進行管理の徹底 発送に関わる者を含め、課全員が発送スケジュールや作業進捗状況を把握・共有する。また、管理監督職が発送作業の進捗管理を密に行うことで発送遅延や発送漏れを直ちに把握できるようにする。 （2）発送前後の確認体制の見直し 当日発送すべき郵便物が揃っているか、発送を担当している係全体でチェックする。発送担当者は、郵便局からの領収証を運搬業者から受け取った後に、発送物作成担当者に引き渡す。発送物作成担当者は、領収証等に担当係長・課長の確認押印を受ける。 （3）紛失リスクの解消 発送予定日前にはがきが納品された場合であっても、その日のうちに郵便局へ持ち込み、はがきを長期間執務室に滞留させないようにする。	⑭個人情報の持出、返却確認及び受け渡しの際の確認の徹底を行う。また、作業工程等を点検し、作業方法やチェック方法等ミスが起きにくい方法を検討、実施する。 ⑮郵便の発送作業は複数職員でチェックすることを再徹底。また、特に慎重を要する個人情報を取り扱う施設における個人情報の事故の重大性について改めて周知するとともに、書類の発送、保管、業務の進行管理等について、注意喚起や指導を行った。 ⑯（1）ファイルが他の物に紛れてしまわないよう、目立つ色に変更する。 （2）作業スペースに仕切りを立てて、使用スペースを物理的に限定する。 （3）ファイルに記載する名前をイニシャルに表記変更する等、使用する情報から個人情報を削除する。 （4）決まった時間に決まった人員が所在を確認する。 （5）チェックの時間を定刻とし、声をかけ合う。 （6）出したらしまうといった基本的事項を、改めて徹底するよう、注意喚起する。 （7）急いでいたり、忙しい時間帯でも、ダブルチェックをするよう、改めて徹底する。また、退所時にも荷物を確認してから渡すようにする ⑰（個人情報の管理について） （1） 相談援助業務上の記録をノート等に記載する場合は、イニシャルを使用するなど個人情報を特定されないようにすること。また、私物のノートや手帳に個人情報を記載しないこと。 （2） 庁舎外での会議等に出席した際には、個人端末を活用して記録の作成を行うとともに、作成した文書は暗号化し保存すること。 （3） 業務上やむを得ず個人情報が記録された書類を庁舎外に持ち出す場合は、局の保有個人情報安全管理基準に基づき管理職の許可を得ること。 （4） 個人情報を含む書類を持ち出すにあたっては、盗難や紛失を防止できる形状・機能を持つ鞄に収納し、肌身離さず持ち運ぶなど十分に注意すること。 （5） その他個人情報の取り扱いについては、局の保有個人情報安全管理基準等を遵守し、適正に行うこと。 （職員の証票の管理について） （1） 月１回、各職員の保有状況を点検すること （2） 携行する際には、ストラップ付きのケースに収納するなど、常に身体から離さずに携行することを徹底すること （職員の緊急連絡網の管理について） （1） 必要な連絡先は公用携帯に保存し、連絡網を記載した紙は庁舎外に持ち出さないこと。 ⑱（1）入所時や退所時の手順確認のチェックリスト様式を変更し、入所時の写真撮影やリストへの正確な情報記載、退所時の荷物確認の手順など守るべきルールを追記するとともに、実施者を記載する欄を追加。 （2）個人情報紛失判明時の、本部への速やかな報告や具体的な捜索の手順などを、チェックリストに追記。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策① 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか 再発防止策の内容		(3)毎朝のミーティングにてリーダー看護師等に個人情報保護の重要性やルールの順守を徹底。勤務者には、業務実施前に最新のマニュアルを確認するよう指導。 ⑲(1)発表資料の事前確認の徹底について幹部会で決定し、各部署に注意喚起 (2)録画や写真撮影をして保管していない旨を書面で確認 (3)画像等の個人情報の収集・利用に関する同意手続きの見直し ⑳(1)電子申請を推奨して紙文書の紛失リスクを軽減 (2)個人情報の適切な管理を職員に改めて周知徹底 ㉑(1)病院へ持ち運ぶファイルに、処方箋を収納する専用スペースを作る (2)医療機関受診時に係るマニュアルを作成 (3)帰園後は可能な限り速やかに所管部署に処方箋等を提出する (4)重要な個人情報を預かっている状況での裁断作業を避ける (5)上記対応について、ミーティング等で周知徹底、注意喚起 ㉒(1)必要なデータファイルのみを送信用データとしてPDF化し、送信前に、PDFに不要な箇所が入っていないことを確認の上、送信することを徹底 (2)メールシステム上、外部送信時に必須である上長の承認の際、個人情報が含まれていないか等の確認を徹底 (3)「メール送信時のセルフチェックリスト」を作成、活用 (4)各管理職より各職員に対する面談時に、個別に再度、再発防止策を徹底 ㉓(1)交付前の事務手順や確認方法の見直し、交付時の最終確認方法の見直し (2)作業スペースへの注意文の掲示やチェックリストへの注意文の記載 (3)確認等を行う人数を増員し、誤交付を防ぐ体制を強化 (4)再発防止勉強会を実施 ㉔(1)委託事業者及び再委託事業者に厳重注意、再発防止策等の作成を指示し、受領 (2)WEBページの脆弱性等の確認を受けるため、デジタルサービス局との調整を開始	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策① 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか 再発防止策の内容		㉕（1）精査が十分でないデータを外部に提供しないこと、精査及び送付の際には複数体制でチェックすることを徹底 （2）受託事業者において、作成した資料のレビューフローの再検討、個人情報データの受領・管理方法に関する社内再教育等の取組を実施 ㉖（1）ダブルチェックの徹底及びその旨の指導 （2）作業項目の文章化、わかりやすいチェックリストの作成 ㉗（1）受託事業者において、マニュアルに沿った処理を徹底し、送付書類の引継ぎ時には、郵便局ともに引継ぎ件数一を確認 （2）3か月間、受託事業者から送付先に対し、発送日の連絡及び到着の確認を行う。 ㉘（1）原則電子申請として紙文書の紛失リスクを軽減 （2） 書類の所在及び処理状況を明確に把握できるよう管理方法を見直す ㉙（1）個人情報の取扱い及び情報管理の徹底等について、厳重に注意喚起 （2）個人情報が特定できない記載にする等の対策 ㉚（1）局内各職場にて個人情報事故防止対策等をテーマとした職場討議実施 （2）個人情報安全管理強化月間の自己点検・職場点検による一層の意識啓発 ㉛（1）張り紙の掲示、FAXボタンへの着色による物理的な注意喚起 （2）FAX送付時のダブルチェック、送信履歴の確認等をマニュアルに追加 ㉜（1）区市町村からの書類を収受する際の件数記載用の共通様式を作成し、受領時に種類ごとの件数を確認・記入 （2）本件の事務のプロセスを細分化し、各プロセス毎の書類の受渡し時に、各担当者がそれぞれ（1）の様式に記載した件数に基づき、書類、件数の確認作業を行うよう整理 （3）使用頻度ごとに文書の保管場所を整理し、常時使用しないものは施錠。作業中に開錠しているキャビネットについても、中に担当者ごとの鍵付きの引き出し等を設置して自分の担当以外の書類は持ち出せないようにし、作業の際にその都度施錠。 （4）緊急の所内幹部会を開催し、個人情報を含む書類の受け渡し時の確認等、個人情報の取り扱いのルールが適正に行われているか確認を指示し、報告を受ける。 ㉝（1）個人情報の保管ルールについて全職員に徹底 （2）現在の保管状況の再点検を実施 ㉞（1）受託事業者に対する個人情報の取扱い及び情報管理の徹底に向けた注意喚起 （2）管理番号の活用など個人情報が特定できない情報管理方法等の導入 ㉟（1）廃棄時の職員立会いの徹底、チェックリストの作成、活用 （2）廃棄対象文書とシステム登録情報の照会の実施 ㊱書類の保管場所の見直し	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策① 7. リスク2	・東京都主税局賦課徴収主管課が入力した情報を随時取得・更新する。 ・納税義務者・申告義務者のあて名情報に異動があった場合等に最新の情報を住民基本台帳ネットワークシステムから随時取得・更新する。 ・納税義務者・申告義務者から提出を受けた申告書等に記載された住所等に更新する。 ・納税義務者・申告義務者の異動に際しては、法令等に則り、適切に届出等を行うよう周知を行っている。 ・所得税等申告情報に変更があれば、国税庁・税務署からの情報提供を受けた際に確認し、更新している。 ・国税庁・税務署に提出された所得税の訂正申告、修正申告、更正決議書等についてもデータの提供を受けており最新情報の取り込み処理を行っている。 ・納税通知書等の返戻調査時に新たな住所が判明すれば、最新の情報に更新している。 ・毎年、経済産業省関東経済産業局において、鉱業原簿に登録された鉱区税のあて名に係る情報の確認を行っており、その際に更新があれば確認できる。 ・減免決定を行う際、対象者について最新の情報を取得している。	・東京都主税局賦課徴収主管課が入力した情報を随時取得・更新する。 ・納税義務者・申告義務者のあて名情報に異動があった場合等に最新の情報を住民基本台帳ネットワークシステムから随時取得・更新する。 ・納税義務者・申告義務者から提出を受けた申告書等に記載された住所等に更新する。 ・納税義務者・申告義務者の異動に際しては、法令等に則り、適切に届出等を行うよう周知を行っている。 ・所得税等申告情報に変更があれば、国税庁・税務署からの情報提供を受けた際に確認し、更新している。 ・国税庁・税務署に提出された所得税の訂正申告、修正申告、更正決議書等についてもデータの提供を受けており最新情報の取り込み処理を行っている。 ・納税通知書等の返戻調査時に新たな住所が判明すれば、最新の情報に更新している。 ・毎年、経済産業省関東経済産業局において、鉱業原簿に登録された鉱区税のあて名に係る情報の確認を行っており、その際に更新があれば確認できる。 ・減免決定を行う際、対象者について最新の情報を取得している。 ・還付決定を行う際、対象者について最新の情報を取得している。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策① 7. リスク3	①課税から収入までの一連のサイクルを完了した課税データについて、電子データの削除等に関する規定に基づき、バッチ処理により削除している。 ②情報資産を破棄する場合、規定に基づきデータ消去ソフトウェア又はデータ消去装置によるデータ廃棄、あるいは、物理的な破壊又は磁気的な破壊によるデータ廃棄作業を行っている。 ③紙資料について、廃棄等に関する規定に基づき、保存期間経過後、職員の立会いのもとで溶解等により廃棄を行っている。運搬・廃棄にあたっては、委託先から適切に処理する旨の誓約書を徴取している。また、廃棄後にすべての書類等を廃棄したことを示す溶解証明を徴取している。 ④軽易な文書（資料文書）については、事務遂行上必要な期間の終了する日をもって随時に廃棄を行っている。 【AI-OCR】 ・OCR処理を施すためのスキャンデータはスキャナシャットダウン時に自動で削除される。 ・スキャナは他の電子機器同様、日々の業務終了時にはスキャナをシャットダウンしている。 ・共有フォルダ内の不使用となったデータは適宜職員及び利用管理者が削除を行っている。 【電子書庫】 ・データ登録時にデータ種類、属性等に応じて予め指定した保存期限を自動設定できること。また、データの保存期限からデータ削除を自動的に実施できるようにしている。 【EUC】 ・データ蓄積期間は各マスタと同じ期間とし、完結処理でマスタから削除されるとEUCからも削除するようにしている。 【電子決裁】 ・文書管理規則に則り、文書廃棄処理を行っている。 【外部連携基盤】 ・保管期間を超過した過去ファイルについては、定期的に自動で削除している。	【連携サーバー】 ・個別業務システム（事務）及び中間サーバーとの間で授受されるデータは、所要の処理完了後又は一定時間経過後に削除される。 ・機器のうち、特定個人情報等のデータが記録されうるものの廃棄等に当たっては、磁気的消去又は物理的破壊等により、当該データを復元不可能な状態とする。 【税務総合支援システム（サーバー）】 ①課税から収入までの一連のサイクルを完了した課税データについて、電子データの削除等に関する規定に基づき、バッチ処理により削除している。 ②情報資産を破棄する場合、規定に基づきデータ消去ソフトウェア又はデータ消去装置によるデータ廃棄、あるいは、物理的な破壊又は磁気的な破壊によるデータ廃棄作業を行っている。 【紙媒体】 ①紙資料について、廃棄等に関する規定に基づき、保存期間経過後、職員の立会いのもとで溶解等により廃棄を行っている。運搬・廃棄にあたっては、委託先から適切に処理する旨の誓約書を徴取している。また、廃棄後にすべての書類等を廃棄したことを示す溶解証明を徴取している。 ②軽易な文書（資料文書）については、事務遂行上必要な期間の終了する日をもって随時に廃棄を行っている。 【外部記録媒体】 媒体内のデータは授受の都度、削除している。	事前	実態に合わせ修正
令和7年2月28日	Ⅲ リスク対策② 3. リスク1 宛名システム等における措置の内容	国税連携システムから入手した所得税申告書等に記録されている情報と税務総合支援システムのあて名管理システムに登録されている納税義務者情報（氏名・住所）とを突合（検索）し、システム上に存在するあて名であるかどうかを確認して紐づけを行っている。目的外の情報の紐付けは行われない。	国税連携システムから入手した所得税申告書等に記録されている情報と税務総合支援システムのあて名管理システムに登録されている納税義務者情報（氏名・住所）とを突合（検索）し、システム上に存在するあて名であるかどうかを確認して紐づけを行っている。目的外の情報の紐付けは行われない。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策② 3. リスク3	・「東京都特定個人情報の保護に関する条例」で目的外利用は禁止されている。 ・局内の規定において、原則、情報資産の外部持出しは禁止している。 ・これらを担保する手段として、上記条例等を研修や自己点検表等で職員へ周知するとともに、国税連携システム端末での外部記憶媒体の使用を制限すること等により、容易に情報資産の持出しができないようにしている。	・局内の規定において、原則、情報資産の外部持出しは禁止している。 ・これらを担保する手段として、国税連携システム端末での外部記憶媒体の使用を制限すること等により、容易に情報資産の持出しができないようにしている。	事前	実態に合わせ修正
令和7年2月28日	Ⅲ リスク対策② 7. リスク1 ⑤物理的対策	【外部記録媒体】 ・審査システムのデータ授受に使用する外部記録媒体（ハードディスク・USBフラッシュメモリ）は、施錠された保管庫で管理している。	【外部記録媒体】 ・国税連携システムのデータ授受に使用する外部記録媒体（ハードディスク・USBフラッシュメモリ）は、施錠された保管庫で管理している。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策② 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか その内容	①平成31年4月7日、晴海客船ターミナル「客船友の会」※の会員に対して、4月の入港スケジュール等を送付する際、事務担当者が誤ってメールアドレスをBCC欄ではなくCC欄に入力して発信したため、個人情報が流出する事故が発生 (※) 晴海客船ターミナル「客船友の会」:晴海客船ターミナルに入出港する客船を歓迎するために平成25年に発足した会 ②平成31年4月8日、「外国人おもてなし語学ボランティア」育成講座の連携先団体(企業、大学等)の事務担当者に対して、東京都の担当者変更についてメール連絡した際、本来BCC欄に入れるべきメールアドレスを、宛先欄に入力して一斉送信したため、個人情報(メールアドレス)が流出する事故が発生 ③令和元年6月17日、「個人住宅建設資金融資あっせん制度」において、都から金融機関ごとに同制度の利用状況に関するデータをメールで送信する際に、1つの金融機関に送付したファイルに、当該金融機関以外の情報(個人住宅建設資金融資あっせん制度の利用者864人分の情報(氏名、融資額、前月及び当月利子補給対象元本額、償還内容、当月及び累計利子補給額、利率))を含んで送付した。 ④令和2年8月21日に東京都人権プラザにおいて開催した「心と体を傷つけられて亡くなった天国の子供たちのメッセージ」展のメディア向けカンファレンスの動画配信案内を(公財)東京都人権啓発センターの行事案内希望者に対して送付する際、事務担当者が誤ってメールアドレスをBCC欄ではなく、CC欄に入力して発信したため、個人情報が流出する事故が発生した。	①令和4年5月、東京都現代美術館において、ミュージアムショップ運営の受託事業者スタッフが、展覧会図録を予約した顧客へ一斉に案内メールを送信する際、メールアドレスをBCC欄ではなく、宛先欄に入力して発信した。 ②令和4年5月、技能検定試験に関する通知を外国人技能実習の複数の監理団体に対しメールで送付する際、誤ってメールアドレスをBCC欄ではなく、CC欄に入力し、一斉送信した。 ③令和4年5月、就学支援金事務において、就学支援金の基礎データをCD-Rに情報を保存し、対象高等学校等宛て一斉に送付したところ、そのうち1校に、他校の受給者に関する情報が含まれていることが判明した。 ④令和4年5月、受託事業者が、事業に関するイベントを案内するメールマガジンを送付する際、配信プログラム改修ミスにより、宛先欄に複数のメールアドレスが入力され、送信された。 ⑤令和4年10月、東京都陽性者登録センターの運営受託事業者が、医療機関で新型コロナウイルス陽性の診断を受け、センターに登録申請を行った複数の患者への登録完了メールを、送付先アドレスが全て入れ替わったまま送信した。 ⑥令和4年12月、労働力調査の統計調査員に対して連絡事項をメールした際、BCC欄に入力して送るべきところを宛先欄に入力し、一斉送信した。 ⑦令和5年4月、再委託先の派遣会社職員が、業務で使用するシステムを不適切に使用し、個人情報を閲覧、メモにとり自宅に持ち出した。 ⑧令和5年5月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑨令和5年6月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策② 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか その内容	⑨案系都電子調達システムにより印刷物の契約案件を公表した際、印刷物の配布先となる町会名のみを公表するところ、誤って中野区内の町会の代表者の氏名、住所及び電話番号を1月28日から2月3日までの間、公表してしまった。 ⑥助成金返還事務のため、ワンビシより平成29年度教育助成金調査票（B表）を預かっていた。ワンビシへの返却手続きを行った際に段ボール二箱分がないことが発覚した。当該段ボール箱は執務室内の空きスペースにて保管していた。 ⑦令和3年7月、都のインターンシップ関連イベントに係る告知メールを送信する際、都が過去に出展した民間企業主催の就職イベント参加者及び当該企業に対して都関連の採用情報の提供を希望した者のメールアドレスを、「BCC」欄ではなく「TO」欄に入力して一斉に送信したため、個人情報が流出する事故が発生した。 ⑧令和3年9月、東日本大震災都内避難者向けに作成する「都内避難者の皆様への定期便」の一部について、送付業務の受託者が誤って本人以外の避難者の宛名を記載して発送してしまい、氏名が流出する事故が発生した。 ⑨令和3年12月、都営住宅の毎月募集の申込者に対して、東京都住宅供給公社において、抽せん番号をお知らせする郵便はがきを発送する準備を行い、料金別納で郵便局に持ち込みを完了したつもりであったが、後日、郵便局に確認したところ、持ち込まれたことを示す書類がないことが判明した。申込者に電話で確認したところ、郵便はがきが届いていることを確認できなかったため、申込者の氏名、住所等が記載されたはがきを紛失する事故が発生した。	⑩令和5年7月、施設を退所する患者に関して、退所先候補の施設と受入調整を行うため、診療関係書類をFAX送信した際、誤って別のFAX番号宛てに送信した。 ⑪令和5年8月、申請により受け付けた申請書が紛失していることが発覚した。 ⑫令和5年9月、関係施設宛に都民情報をFAX送信した際、誤って別の事業者宛てに送信した。 ⑬令和5年9月、事業の対象者に案内チラシを郵送した際、送付対象者の抽出ツールのプログラム仕様の不備により、誤って事業対象外の方に送付したことで、旧住所宛てに送付し返戻されなかったものが誤送付となった。 ⑭令和5年9月、決定通知書に公印を押印する目的で本庁に出張し、押印後持ち帰ったが、発送の準備をしていた際に、通知書1枚が紛失していることが発覚した。 ⑮令和6年1月、患者A宛てに送付すべき利用者情報を、誤ってB宛てに送付した。 ⑯令和6年1月、入所者の診療関係ファイルが紛失していることが発覚し、その後、退所者の荷物の中に当該ファイルが混入していたことが発覚した。 ⑰令和6年2月、児童相談所の職員が、出張中に個人情報が記載されている手帳を紛失し、あわせて手帳に収納されていた、当該職員の証票及び所内職員の緊急連絡網を紛失した。 ⑱令和6年2月、施設を退所した患者Aに関する薬剤情報等を記載した書類を、誤って別の患者の退院時の荷物に混入させ交付した。 ⑲令和6年2月、オンライン研修で使用した映像において、患者の情報をマスキング処理していたところ、当該映像をスマートフォンで視聴した場合に、マスキングが外れ、個人が特定できる状態になっていたことが判明した。 ⑳令和6年4月、受け付けた申請書を紛失していることが発覚した。 ㉑令和6年4月、施設職員が、利用者の通院付添の際、処方箋を紛失した。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策② 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか その内容		㉒令和6年4月、指定管理者が、事業者に対してExcel資料をメールで送信した際、本来削除すべきだった個人情報の入力されたシートを削除しなかった。 ㉓令和6年7月、受託事業者が、都へ交付すべき納入済通知書を、誤って他の事業者宛てに交付したことが発覚した。 ㉔令和6年7月、受託事業者がイベントを行った際の申込時の個人情報が掲載されたウェブページが、一時外部からアクセス可能な状態となっていたことが発覚した。 ㉕令和6年7月、職員が、説明会の資料の中に個人情報が含まれていることに気が付かずに、各自治体にデータを配布した。 ㉖令和6年7月、職員が、A宛てに送付すべき個人情報を、誤ってB宛てに送付していたことが発覚した。 ㉗令和6年7月、受託事業者から送付した個人情報を含む資料が、紛失していることが発覚した。 ㉘令和6年7月、受け付けた申請書を紛失していることが発覚した。 ㉙令和6年8月、受託事業者が配付した資料の中に、個人情報等が含まれる資料が混入していたことが発覚した。 ㉚令和6年10月、職員が、受託者に資料をメールで送信した際、誤って個人情報が記載された別のファイルを添付した。 ㉛令和6年10月、受託事業者が、A宛てに送付すべき電話記録を、誤ってB宛てにFAXで送信した。 ㉜令和6年11月、受け付けた申請書を紛失していることが発覚した（後日発見）。 ㉝令和6年11月、令和3年頃に個人情報が記載された資料を紛失していたことが発覚した。 ㉞令和6年12月、受託事業者が、個人情報が記載された資料を、誤って外部へ送信した。 ㉟令和7年1月、受託事業者が、個人情報が記載された資料を、誤って期限前に廃棄した。 ㊱令和7年1月、受け付けた届出書が、誤って机ごと廃棄されていることが発覚した。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策② 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか再発防止策の内容	①社員教育を実施し、個人情報保護法等関係法令等に則った対応について点検・実施を行う。 ②・平成31年４月９日に係会を開催し、情報管理の重要性について話し合うとともに、平成30年度に職員に対して周知した、個人情報等に関する注意喚起事項を改めて全員に配布・説明し、コンプライアンス意識の徹底を図った。 ・他局での事故発生に係るプレス発表時等には、係内で情報共有するとともに、複数の宛先にメール送信する際のBCC利用・複数職員による確認の徹底していく。 ・メール送付に限らず、管理ミス・誤操作・紛失・置き忘れなど「うっかりミス」による個人情報の漏えい事故防止のため、個人情報管理徹底に関する周知を継続的に実施することで意識向上を図っていく。 ・生活文化局情報セキュリティ委員会において、各部署の庶務担当課長と共に、今回の事故について共有し、再発防止につなげていく。 ③メールによる連絡等を行う場合は、複数の担当者により、送信先及び添付ファイルの内容について確認することを徹底する。また、今後、再発防止のため、個人情報を厳正に管理するとともに、職員に対し、情報セキュリティの確保に向け指導等を徹底していく。 ④団体に対し、外部へ一斉送信する際は、メールアドレスをBCC欄に入力すべきことと、メール送信前に、複数の職員で宛先の確認作業を必ず行うことを、職員全員に改めて周知徹底するとともに、組織としての検証を行い、再発防止策を検討するよう指導した。	①(1)ミュージアムショップにおいて、本社セキュリティインシデント統括部と連携して、個人情報取り扱い、情報管理体制の改善を行う。 (2)特に複数人へのメール送信に際してはダブルチェックを徹底する。 (3)現代美術館全委託業者に、適切な個人情報等の取扱い及び情報管理を徹底するよう指示する。 (4)財団が管理運営する各施設にも本事案を共有し、個人情報を含む情報の適切な管理を徹底する。 ②(1)個人情報の取扱い及び情報管理の徹底等について周知するとともに、職員全員に臨時研修を速やかに実施 (2)誤送信防止に向けたシステムの導入(ダイアログの自動表示など) (3)複数人チェックなど基本的対策の徹底 ③チェック機能を再検証し、全日制等と同様の仕組みを通信制にも直ちに導入するほか、事務フローの再構築を行い、再発防止に努める。そのうえで、本件を財団内で広く共有させ、個人情報の取扱い全般についてハード・ソフトの両面から厳しく見直すとともに、職員の意識向上を図っていく。また、都の実施機関においても個人情報の適正管理とサイバーセキュリティー対策について改めて確認を行う。 ④(1)システムの改善 メールマガジンの配信は、これまで「TO」により自動で1件ずつ送信がされる仕組みであったが、一括メール送信においては送信者アドレスを全て「BCC」に入れるようシステム改修を行う。 (2)システム会社における確認体制の強化 開発前にシステム会社が実施する、影響調査・テスト内容等について、これまでの2名体制によるダブルチェックから、システム会社のプロジェクトマネージャーも加えることとし、確認した内容を報告させて承認する運用へ見直す。 (3)受託事業者における確認体制の強化 システム会社のテスト結果の確認にあたっては、テストの証跡情報の提出を求め、内容の確認を行うとともに、受託事業者での運用テストでは要件定義とも照らした確認を担当だけでなく管理職も実施することにより徹底する。 ⑤受託事業者に対して厳正に指導し、登録完了メール送信作業のチェック体制を強化させる。 ⑥(1)部コンプライアンス推進委員会の臨時開催 ・メール送信時のダブルチェックを徹底させるため、個人情報等の取扱いに係るチェックリストの全職員での点検により注意を喚起、情報管理を再徹底する。 ・あわせて、最近の事故事案の事例を周知するなど、事故の再発予防を進める。 (2)定期的な事故防止意識の醸成 統計調査員を含む全職員を対象に、各所属長や指導員から情報セキュリティや感染拡大防止等に関する指導を定期・継続的に行い、危機意識の醸成等を図る。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策② 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか 再発防止策の内容	⑤（1）事務フローの見直し ・起工部署の事務フローを、別紙1のとおり見直し、周知徹底を図る。 ・契約部署は、着手起案作成時及び発注図書登録時、電子調達システムに、起工部署から提出されたPDFデータを公表前の登録を行ってから印刷した上で、契約依頼文書に添付された仕様書と照合し、一致していることを確認する。また、この確認方法について、令和元年12月19日付経理部契約課長事務連絡「契約事務に係る情報漏えい等の防止策について」により配布されたチェックリストに追記した。 （2）臨時支所コンプライアンス推進委員会の開催 ・臨時支所コンプライアンス推進委員会を開催し、再発防止に向け、上記事務フローの見直しの周知徹底を図った。 ⑥（1）個人情報の重要性を再確認し、高い危機意識をもって個人情報の適正な管理・運 用を図るよう、改めて基本的な取扱いルールの徹底を図る。 （2）書類の所在及び処理状況が明確に分かるような管理方法の整備や、文書廃棄の際 の事務処理手順の整備など、書類管理の徹底に向けた仕組みの構築を図る。 ⑦（1）局内全職員に対して情報セキュリティ研修を実施し、二度と同様の事故を起こさないよう、情報セキュリティ対策の確認を徹底する。 （2）外部の複数の宛先に対してメールを送信する場合、「BCC」欄に入力するとと に、送信前に複数の職員によるチェックを徹底する。	⑦委託先における個人情報の閲覧・使用に当たっての権限の設定や、不適切な閲覧・使用・持ち出しを防止するための体制についてあらためて確認し、適切な運用を徹底させる。 ⑧（1）情報共有をしているホワイトボードの位置、記入欄が分かりにくいとの意見が出 ため、位置、記入方法について変更した。 （2）書類封入時のチェック手順中に、患者氏名の確認を明示した。 （3）2者確認を徹底するため、事務員のみでなく看護職員もチェックを行うこととし、 2者チェックが終わった段階で封書のチェックボックスに記載する。 （4）責任の所在を明確にするため「転院時退所セット確認書」を新たに作成し、チェ ックを行った職員が記名する。 ⑨（1）チェックリストを活用し、複数人、複数回のチェックを行うとともに、最終チェ ック者を統括責任者とすることで、誤封入等を防ぐ体制を整える。 （2）都職員が施設へ直接出向き、個人情報管理の実態確認を実施するとともに、対応 が不十分な場合は是正指導を行う。 （3）個人情報保護の研修を実施し、施設全体で個人情報保護の取り組み状況を共有し た上で、改善を徹底する。 ⑩（1）委託先に対し、個人情報に関する業務手順を見直し及び徹底を図ることや、全従 事者に対する個人情報保護研修を行うことを指導した。また、改善策の確認のた め、都が施設へ出向き、個人情報管理の実態を確認した。 （2）再委託先において、送付の際は、まずFAX以外の手段を調整し、止むを得ずFAXを使用する際には、FAX番号の聞き取りの際の復唱や、FAX送信前の送信先への番号の再確認、複数人で複数回のチェックを必ず行うこととした。また、全従業者に対する個人情報保護研修を行った。 ⑪（1）作業環境等を見直し、書類の混入等が起きにくい環境を整備 ①執務室内の作業スペースの確保及び活用 ②引き出し付きの棚をキャビネット内に新設し、書類の分類をよりしやすくした。 （2）委託業者との書類の受け渡し方法の変更（送付する判定機関ごとに数を確認しながら受け渡す）。 ⑫個人情報をFAX送信することを禁止するよう各施設に通知した。 ⑬抽出ツールのプログラム確認は、委託先事業者の運用チームのみが行っていたが、抽出ツールを作成・利用する際には、運用チームに加えて、開発チームと委託元である都の3者で抽出ツールのプログラムの仕様・設定を確認することとした。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策② 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか 再発防止策の内容	⑧これまで実施してきた委託事業者への発送完了時の確認のほか、委託事業者職員による宛名、住所の複数チェック等、発送作業での確認作業を確実に実施させるとともに、都においても個人情報を含む情報の適切な取扱いについて、さらなる徹底を図り、再発防止に努める。 ⑨（1）スケジュールの情報共有と進行管理の徹底 発送に関わる者を含め、課全員が発送スケジュールや作業進捗状況を把握・共有する。また、管理監督職が発送作業の進捗管理を密に行うことで発送遅延や発送漏れを直ちに把握できるようにする。 （2）発送前後の確認体制の見直し 当日発送すべき郵便物が揃っているか、発送を担当している係全体でチェックする。発送担当者は、郵便局からの領収証を運搬業者から受け取った後に、発送物作成担当者に引き渡す。発送物作成担当者は、領収証等に担当係長・課長の確認押印を受ける。 （3）紛失リスクの解消 発送予定日前にはがきが納品された場合であっても、その日のうちに郵便局へ持ち込み、はがきを長期間執務室に滞留させないようにする。	⑭個人情報の持出、返却確認及び受け渡しの際の確認の徹底を行う。また、作業工程等を点検し、作業方法やチェック方法等ミスが起きにくい方法を検討、実施する。 ⑮郵便の発送作業は複数職員でチェックすることを再徹底。また、特に慎重を要する個人情報を取り扱う施設における個人情報の事故の重大性について改めて周知するとともに、書類の発送、保管、業務の進行管理等について、注意喚起や指導を行った。 ⑯（1）ファイルが他の物に紛れてしまわないよう、目立つ色に変更する。 （2）作業スペースに仕切りを立てて、使用スペースを物理的に限定する。 （3）ファイルに記載する名前をイニシャルに表記変更する等、使用する情報から個人情報を削除する。 （4）決まった時間に決まった人員が所在を確認する。 （5）チェックの時間を定刻とし、声をかけ合う。 （6）出したらしまうといった基本的事項を、改めて徹底するよう、注意喚起する。 （7）急いでいたり、忙しい時間帯でも、ダブルチェックをするよう、改めて徹底する。また、退所時にも荷物を確認してから渡すようにする ⑰（個人情報の管理について） （1） 相談援助業務上の記録をノート等に記載する場合は、イニシャルを使用するなど個人情報を特定されないようにすること。また、私物のノートや手帳に個人情報を記載しないこと。 （2） 庁舎外での会議等に出席した際には、個人端末を活用して記録の作成を行うとともに、作成した文書は暗号化し保存すること。 （3） 業務上やむを得ず個人情報が記録された書類を庁舎外に持ち出す場合は、局の保有個人情報安全管理基準に基づき管理職の許可を得ること。 （4） 個人情報を含む書類を持ち出すにあたっては、盗難や紛失を防止できる形状・機能を持つ鞄に収納し、肌身離さず持ち運ぶなど十分に注意すること。 （5） その他個人情報の取り扱いについては、局の保有個人情報安全管理基準等を遵守し、適正に行うこと。 （職員の証票の管理について） （1） 月１回、各職員の保有状況を点検すること （2） 携行する際には、ストラップ付きのケースに収納するなど、常に身体から離さずに携行することを徹底すること （職員の緊急連絡網の管理について） （1） 必要な連絡先は公用携帯に保存し、連絡網を記載した紙は庁舎外に持ち出さないこと。 ⑱（1）入所時や退所時の手順確認のチェックリスト様式を変更し、入所時の写真撮影やリストへの正確な情報記載、退所時の荷物確認の手順など守るべきルールを追記するとともに、実施者を記載する欄を追加。 （2）個人情報紛失判明時の、本部への速やかな報告や具体的な捜索の手順などを、チェックリストに追記。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策② 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか 再発防止策の内容		(3)毎朝のミーティングにてリーダー看護師等に個人情報保護の重要性やルールの順守を徹底。勤務者には、業務実施前に最新のマニュアルを確認するよう指導。 ⑲(1)発表資料の事前確認の徹底について幹部会で決定し、各部署に注意喚起 (2)録画や写真撮影をして保管していない旨を書面で確認 (3)画像等の個人情報の収集・利用に関する同意手続きの見直し ⑳(1)電子申請を推奨して紙文書の紛失リスクを軽減 (2)個人情報の適切な管理を職員に改めて周知徹底 ㉑(1)病院へ持ち運ぶファイルに、処方箋を収納する専用スペースを作る (2)医療機関受診時に係るマニュアルを作成 (3)帰園後は可能な限り速やかに所管部署に処方箋等を提出する (4)重要な個人情報を預かっている状況での裁断作業を避ける (5)上記対応について、ミーティング等で周知徹底、注意喚起 ㉒(1)必要なデータファイルのみを送信用データとしてPDF化し、送信前に、PDFに不要な箇所が入っていないことを確認の上、送信することを徹底 (2)メールシステム上、外部送信時に必須である上長の承認の際、個人情報が含まれていないか等の確認を徹底 (3)「メール送信時のセルフチェックリスト」を作成、活用 (4)各管理職より各職員に対する面談時に、個別に再度、再発防止策を徹底 ㉓(1)交付前の事務手順や確認方法の見直し、交付時の最終確認方法の見直し (2)作業スペースへの注意文の掲示やチェックリストへの注意文の記載 (3)確認等を行う人数を増員し、誤交付を防ぐ体制を強化 (4)再発防止勉強会を実施 ㉔(1)委託事業者及び再委託事業者に厳重注意、再発防止策等の作成を指示し、受領 (2)WEBページの脆弱性等の確認を受けるため、デジタルサービス局との調整を開始	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策② 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか 再発防止策の内容		㉕（1）精査が十分でないデータを外部に提供しないこと、精査及び送付の際には複数体制でチェックすることを徹底 （2）受託事業者において、作成した資料のレビューフローの再検討、個人情報データの受領・管理方法に関する社内再教育等の取組を実施 ㉖（1）ダブルチェックの徹底及びその旨の指導 （2）作業項目の文章化、わかりやすいチェックリストの作成 ㉗（1）受託事業者において、マニュアルに沿った処理を徹底し、送付書類の引継ぎ時には、郵便局ともに引継ぎ件数一を確認 （2）3か月間、受託事業者から送付先に対し、発送日の連絡及び到着の確認を行う。 ㉘（1）原則電子申請として紙文書の紛失リスクを軽減 （2） 書類の所在及び処理状況を明確に把握できるよう管理方法を見直す ㉙（1）個人情報の取扱い及び情報管理の徹底等について、厳重に注意喚起 （2）個人情報が特定できない記載にする等の対策 ㉚（1）局内各職場にて個人情報事故防止対策等をテーマとした職場討議実施 （2）個人情報安全管理強化月間の自己点検・職場点検による一層の意識啓発 ㉛（1）張り紙の掲示、FAXボタンへの着色による物理的な注意喚起 （2）FAX送付時のダブルチェック、送信履歴の確認等をマニュアルに追加 ㉜（1）区市町村からの書類を収受する際の件数記載用の共通様式を作成し、受領時に種類ごとの件数を確認・記入 （2）本件の事務のプロセスを細分化し、各プロセス毎の書類の受渡し時に、各担当者がそれぞれ（1）の様式に記載した件数に基づき、書類、件数の確認作業を行うよう整理 （3）使用頻度ごとに文書の保管場所を整理し、常時使用しないものは施錠。作業中に開錠しているキャビネットについても、中に担当者ごとの鍵付きの引き出し等を設置して自分の担当以外の書類は持ち出せないようにし、作業の際にその都度施錠。 （4）緊急の所内幹部会を開催し、個人情報を含む書類の受け渡し時の確認等、個人情報の取り扱いのルールが適正に行われているか確認を指示し、報告を受ける。 ㉝（1）個人情報の保管ルールについて全職員に徹底 （2）現在の保管状況の再点検を実施 ㉞（1）受託事業者に対する個人情報の取扱い及び情報管理の徹底に向けた注意喚起 （2）管理番号の活用など個人情報が特定できない情報管理方法等の導入 ㉟（1）廃棄時の職員立会いの徹底、チェックリストの作成、活用 （2）廃棄対象文書とシステム登録情報の照会の実施 ㊱書類の保管場所の見直し	事前	実態に合わせ修正
令和7年2月28日	Ⅲ リスク対策② 7. リスク2	・国税庁・税務署に提出された所得税の訂正申告、修正申告、更正決議書等についてもデータの提供を受けており最新情報の取り込み処理も行っている。 ・納税義務者の異動に際しては、法令等に則り、適切に届出等を行うよう周知を行っている。 ・税務調査で異動の事実が判明した場合は、情報の更新を行っている。	・国税庁・税務署に提出された所得税・法人税の訂正申告、修正申告、更正決議書等についてもデータの提供を受けており最新情報の取り込み処理も行っている。 ・納税義務者の異動に際しては、法令等に則り、適切に届出等を行うよう周知を行っている。 ・税務調査で異動の事実が判明した場合は、情報の更新を行っている。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策② 7. リスク3 消去手順の内容	【国税連携システム（サーバー）】 一定期間を経過したデータは、電子データの削除等に関する規定に基づき、委託先によるバッチ処理により削除している。 【外部記録媒体】 データ移行のため、外部記録媒体（ハードディスク）、USBフラッシュメモリに一時保存したデータについては、移行後直ちに職員が手作業で消去している。	【国税連携システム（サーバー）】 一定期間を経過したデータは、電子データの削除等に関する規定に基づき、職員によるオンライン処理により削除している。 【外部記録媒体】 データ移行のため、外部記録媒体（ハードディスク）、USBフラッシュメモリに一時保存したデータについては、移行後直ちに職員が手作業で消去している。	事前	実態に合わせ修正
令和7年2月28日	Ⅲ リスク対策② 7. 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		仕様書において、文書の安全管理や秘密の保護、作業方法、業者の資格等様々な条件を定め、リスクに対する措置を行っている。	事前	実態に合わせ修正
令和7年2月28日	Ⅲ リスク対策③ 3. リスク3	・「東京都特定個人情報の保護に関する条例」で目的外利用は禁止されている。 ・局内の規定において、原則、情報資産の外部持出しは禁止している。 ・これらを担保する手段として、上記条例等を研修や自己点検表等で職員へ周知するとともに、審査システム端末での外部記憶媒体の使用を制限すること等により、容易に情報資産の持出しができないようにしている。	・局内の規定において、原則、情報資産の外部持出しは禁止している。 ・これらを担保する手段として、審査システム端末での外部記憶媒体の使用を制限すること等により、容易に情報資産の持出しができないようにしている。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策③ 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか その内容	①平成31年4月7日、晴海客船ターミナル「客船友の会」※の会員に対して、4月の入港スケジュール等を送付する際、事務担当者が誤ってメールアドレスをBCC欄ではなくCC欄に入力して発信したため、個人情報が流出する事故が発生 (※) 晴海客船ターミナル「客船友の会」:晴海客船ターミナルに入出港する客船を歓迎するために平成25年に発足した会 ②平成31年4月8日、「外国人おもてなし語学ボランティア」育成講座の連携先団体(企業、大学等)の事務担当者に対して、東京都の担当者変更についてメール連絡した際、本来BCC欄に入れるべきメールアドレスを、宛先欄に入力して一斉送信したため、個人情報(メールアドレス)が流出する事故が発生 ③令和元年6月17日、「個人住宅建設資金融資あっせん制度」において、都から金融機関ごとに同制度の利用状況に関するデータをメールで送信する際に、1つの金融機関に送付したファイルに、当該金融機関以外の情報(個人住宅建設資金融資あっせん制度の利用者864人分の情報(氏名、融資額、前月及び当月利子補給対象元本額、償還内容、当月及び累計利子補給額、利率))を含んで送付した。 ④令和2年8月21日に東京都人権プラザにおいて開催した「心と体を傷つけられて亡くなった天国の子供たちのメッセージ」展のメディア向けカンファレンスの動画配信案内を(公財)東京都人権啓発センターの行事案内希望者に対して送付する際、事務担当者が誤ってメールアドレスをBCC欄ではなく、CC欄に入力して発信したため、個人情報が流出する事故が発生した。	①令和4年5月、東京都現代美術館において、ミュージアムショップ運営の受託事業者スタッフが、展覧会図録を予約した顧客へ一斉に案内メールを送信する際、メールアドレスをBCC欄ではなく、宛先欄に入力して発信した。 ②令和4年5月、技能検定試験に関する通知を外国人技能実習の複数の監理団体に対しメールで送付する際、誤ってメールアドレスをBCC欄ではなく、CC欄に入力し、一斉送信した。 ③令和4年5月、就学支援金事務において、就学支援金の基礎データをCD-Rに情報を保存し、対象高等学校等宛て一斉に送付したところ、そのうち1校に、他校の受給者に関する情報が含まれていることが判明した。 ④令和4年5月、受託事業者が、事業に関するイベントを案内するメールマガジンを送付する際、配信プログラム改修ミスにより、宛先欄に複数のメールアドレスが入力され、送信された。 ⑤令和4年10月、東京都陽性者登録センターの運営受託事業者が、医療機関で新型コロナウイルス陽性の診断を受け、センターに登録申請を行った複数の患者への登録完了メールを、送付先アドレスが全て入れ替わったまま送信した。 ⑥令和4年12月、労働力調査の統計調査員に対して連絡事項をメールした際、BCC欄に入力して送るべきところを宛先欄に入力し、一斉送信した。 ⑦令和5年4月、再委託先の派遣会社職員が、業務で使用するシステムを不適切に使用し、個人情報を閲覧、メモにとり自宅に持ち出した。 ⑧令和5年5月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑨令和5年6月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策③ 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか その内容	⑤東京都電子調達システムにより印刷物の契約案件を公表した際、印刷物の配布先となる町会名のみを公表するところ、誤って中野区内の町会の代表者の氏名、住所及び電話番号を1月28日から2月3日までの間、公表してしまった。 ⑥助成金返還事務のため、ワンビシより平成29年度教育助成金調査票（B表）を預かっていた。ワンビシへの返却手続きを行った際に段ボール二箱分がないことが発覚した。当該段ボール箱は執務室内の空きスペースにて保管していた。 ⑦令和3年7月、都のインターンシップ関連イベントに係る告知メールを送信する際、都が過去に出展した民間企業主催の就職イベント参加者及び当該企業に対して都関連の採用情報の提供を希望した者のメールアドレスを、「BCC」欄ではなく「TO」欄に入力して一斉に送信したため、個人情報が流出する事故が発生した。 ⑧令和3年9月、東日本大震災都内避難者向けに作成する「都内避難者の皆様への定期便」の一部について、送付業務の受託者が誤って本人以外の避難者の宛名を記載して発送してしまい、氏名が流出する事故が発生した。 ⑨令和3年12月、都営住宅の毎月募集の申込者に対して、東京都住宅供給公社において、抽せん番号をお知らせする郵便はがきを発送する準備を行い、料金別納で郵便局に持ち込みを完了したつもりであったが、後日、郵便局に確認したところ、持ち込まれたことを示す書類がないことが判明した。申込者に電話で確認したところ、郵便はがきが届いていることを確認できなかったため、申込者の氏名、住所等が記載されたはがきを紛失する事故が発生した。	⑩令和5年7月、施設を退所する患者に関して、退所先候補の施設と受入調整を行うため、診療関係書類をFAX送信した際、誤って別のFAX番号宛てに送信した。 ⑪令和5年8月、申請により受け付けた申請書が紛失していることが発覚した。 ⑫令和5年9月、関係施設宛に都民情報をFAX送信した際、誤って別の事業者宛てに送信した。 ⑬令和5年9月、事業の対象者に案内チラシを郵送した際、送付対象者の抽出ツールのプログラム仕様の不備により、誤って事業対象外の方に送付したことで、旧住所宛てに送付し返戻されなかったものが誤送付となった。 ⑭令和5年9月、決定通知書に公印を押印する目的で本庁に出張し、押印後持ち帰ったが、発送の準備をしていた際に、通知書1枚が紛失していることが発覚した。 ⑮令和6年1月、患者A宛てに送付すべき利用者情報を、誤ってB宛てに送付した。 ⑯令和6年1月、入所者の診療関係ファイルが紛失していることが発覚し、その後、退所者の荷物の中に当該ファイルが混入していたことが発覚した。 ⑰令和6年2月、児童相談所の職員が、出張中に個人情報が記載されている手帳を紛失し、あわせて手帳に収納されていた、当該職員の証票及び所内職員の緊急連絡網を紛失した。 ⑱令和6年2月、施設を退所した患者Aに関する薬剤情報等を記載した書類を、誤って別の患者の退院時の荷物に混入させ交付した。 ⑲令和6年2月、オンライン研修で使用した映像において、患者の情報をマスキング処理していたところ、当該映像をスマートフォンで視聴した場合に、マスキングが外れ、個人が特定できる状態になっていたことが判明した。 ⑳令和6年4月、受け付けた申請書を紛失していることが発覚した。 ㉑令和6年4月、施設職員が、利用者の通院付添の際、処方箋を紛失した。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策③ 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか その内容		㉒令和6年4月、指定管理者が、事業者に対してExcel資料をメールで送信した際、本来削除すべきだった個人情報の入力されたシートを削除しなかった。 ㉓令和6年7月、受託事業者が、都へ交付すべき納入済通知書を、誤って他の事業者宛てに交付したことが発覚した。 ㉔令和6年7月、受託事業者がイベントを行った際の申込時の個人情報が掲載されたウェブページが、一時外部からアクセス可能な状態となっていたことが発覚した。 ㉕令和6年7月、職員が、説明会の資料の中に個人情報が含まれていることに気が付かずに、各自治体にデータを配布した。 ㉖令和6年7月、職員が、A宛てに送付すべき個人情報を、誤ってB宛てに送付していたことが発覚した。 ㉗令和6年7月、受託事業者から送付した個人情報を含む資料が、紛失していることが発覚した。 ㉘令和6年7月、受け付けた申請書を紛失していることが発覚した。 ㉙令和6年8月、受託事業者が配付した資料の中に、個人情報等が含まれる資料が混入していたことが発覚した。 ㉚令和6年10月、職員が、受託者に資料をメールで送信した際、誤って個人情報が記載された別のファイルを添付した。 ㉛令和6年10月、受託事業者が、A宛てに送付すべき電話記録を、誤ってB宛てにFAXで送信した。 ㉜令和6年11月、受け付けた申請書を紛失していることが発覚した（後日発見）。 ㉝令和6年11月、令和3年頃に個人情報が記載された資料を紛失していたことが発覚した。 ㉞令和6年12月、受託事業者が、個人情報が記載された資料を、誤って外部へ送信した。 ㉟令和7年1月、受託事業者が、個人情報が記載された資料を、誤って期限前に廃棄した。 ㊱令和7年1月、受け付けた届出書が、誤って机ごと廃棄されていることが発覚した。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策③ 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか再発防止策の内容	①社員教育を実施し、個人情報保護法等関係法令等に則った対応について点検・実施を行う。 ②・平成31年４月９日に係会を開催し、情報管理の重要性について話し合うとともに、平成30年度に職員に対して周知した、個人情報等に関する注意喚起事項を改めて全員に配布・説明し、コンプライアンス意識の徹底を図った。 ・他局での事故発生に係るプレス発表時等には、係内で情報共有するとともに、複数の宛先にメール送信する際のBCC利用・複数職員による確認の徹底していく。 ・メール送付に限らず、管理ミス・誤操作・紛失・置き忘れなど「うっかりミス」による個人情報の漏えい事故防止のため、個人情報管理徹底に関する周知を継続的に実施することで意識向上を図っていく。 ・生活文化局情報セキュリティ委員会において、各部署の庶務担当課長と共に、今回の事故について共有し、再発防止につなげていく。 ③メールによる連絡等を行う場合は、複数の担当者により、送信先及び添付ファイルの内容について確認することを徹底する。また、今後、再発防止のため、個人情報を厳正に管理するとともに、職員に対し、情報セキュリティの確保に向け指導等を徹底していく。 ④団体に対し、外部へ一斉送信する際は、メールアドレスをBCC欄に入力すべきことと、メール送信前に、複数の職員で宛先の確認作業を必ず行うことを、職員全員に改めて周知徹底するとともに、組織としての検証を行い、再発防止策を検討するよう指導した。	①(1)ミュージアムショップにおいて、本社セキュリティインシデント統括部と連携して、個人情報取り扱い、情報管理体制の改善を行う。 (2)特に複数人へのメール送信に際してはダブルチェックを徹底する。 (3)現代美術館全委託業者に、適切な個人情報等の取扱い及び情報管理を徹底するよう指示する。 (4)財団が管理運営する各施設にも本事案を共有し、個人情報を含む情報の適切な管理を徹底する。 ②(1)個人情報の取扱い及び情報管理の徹底等について周知するとともに、職員全員に臨時研修を速やかに実施 (2)誤送信防止に向けたシステムの導入(ダイアログの自動表示など) (3)複数人チェックなど基本的対策の徹底 ③チェック機能を再検証し、全日制等と同様の仕組みを通信制にも直ちに導入するほか、事務フローの再構築を行い、再発防止に努める。そのうえで、本件を財団内で広く共有させ、個人情報の取扱い全般についてハード・ソフトの両面から厳しく見直すとともに、職員の意識向上を図っていく。また、都の実施機関においても個人情報の適正管理とサイバーセキュリティー対策について改めて確認を行う。 ④(1)システムの改善 メールマガジンの配信は、これまで「TO」により自動で1件ずつ送信がされる仕組みであったが、一括メール送信においては送信者アドレスを全て「BCC」に入れるようシステム改修を行う。 (2)システム会社における確認体制の強化 開発前にシステム会社が実施する、影響調査・テスト内容等について、これまでの2名体制によるダブルチェックから、システム会社のプロジェクトマネージャーも加えることとし、確認した内容を報告させて承認する運用へ見直す。 (3)受託事業者における確認体制の強化 システム会社のテスト結果の確認にあたっては、テストの証跡情報の提出を求め、内容の確認を行うとともに、受託事業者での運用テストでは要件定義とも照らした確認を担当だけでなく管理職も実施することにより徹底する。 ⑤受託事業者に対して厳正に指導し、登録完了メール送信作業のチェック体制を強化させる。 ⑥(1)部コンプライアンス推進委員会の臨時開催 ・メール送信時のダブルチェックを徹底させるため、個人情報等の取扱いに係るチェックリストの全職員での点検により注意を喚起、情報管理を再徹底する。 ・あわせて、最近の事故事案の事例を周知するなど、事故の再発予防を進める。 (2)定期的な事故防止意識の醸成 統計調査員を含む全職員を対象に、各所属長や指導員から情報セキュリティや感染拡大防止等に関する指導を定期・継続的に行い、危機意識の醸成等を図る。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策③ 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか 再発防止策の内容	⑤（1）事務フローの見直し ・起工部署の事務フローを、別紙1のとおり見直し、周知徹底を図る。 ・契約部署は、着手起案作成時及び発注図書登録時、電子調達システムに、起工部署から提出されたPDFデータを公表前の登録を行ってから印刷した上で、契約依頼文書に添付された仕様書と照合し、一致していることを確認する。また、この確認方法について、令和元年12月19日付経理部契約課長事務連絡「契約事務に係る情報漏えい等の防止策について」により配布されたチェックリストに追記した。 （2）臨時支所コンプライアンス推進委員会の開催 ・臨時支所コンプライアンス推進委員会を開催し、再発防止に向け、上記事務フローの見直しの周知徹底を図った。 ⑥（1）個人情報の重要性を再確認し、高い危機意識をもって個人情報の適正な管理・運 用を図るよう、改めて基本的な取扱いルールの徹底を図る。 （2）書類の所在及び処理状況が明確に分かるような管理方法の整備や、文書廃棄の際 の事務処理手順の整備など、書類管理の徹底に向けた仕組みの構築を図る。 ⑦（1）局内全職員に対して情報セキュリティ研修を実施し、二度と同様の事故を起こさないよう、情報セキュリティ対策の確認を徹底する。 （2）外部の複数の宛先に対してメールを送信する場合、「BCC」欄に入力するとともに、送信前に複数の職員によるチェックを徹底する。	⑦委託先における個人情報の閲覧・使用に当たっての権限の設定や、不適切な閲覧・使用・持ち出しを防止するための体制についてあらためて確認し、適切な運用を徹底させる。 ⑧（1）情報共有をしているホワイトボードの位置、記入欄が分かりにくいとの意見が出 ため、位置、記入方法について変更した。 （2）書類封入時のチェック手順中に、患者氏名の確認を明示した。 （3）2者確認を徹底するため、事務員のみでなく看護職員もチェックを行うこととし、 2者チェックが終わった段階で封書のチェックボックスに記載する。 （4）責任の所在を明確にするため「転院時退所セット確認書」を新たに作成し、チェ ックを行った職員が記名する。 ⑨（1）チェックリストを活用し、複数人、複数回のチェックを行うとともに、最終チェ ック者を統括責任者とすることで、誤封入等を防ぐ体制を整える。 （2）都職員が施設へ直接出向き、個人情報管理の実態確認を実施するとともに、対応 が不十分な場合は是正指導を行う。 （3）個人情報保護の研修を実施し、施設全体で個人情報保護の取り組み状況を共有し た上で、改善を徹底する。 ⑩（1）委託先に対し、個人情報に関する業務手順を見直し及び徹底を図ることや、全従 事者に対する個人情報保護研修を行うことを指導した。また、改善策の確認のた め、都が施設へ出向き、個人情報管理の実態を確認した。 （2）再委託先において、送付の際は、まずFAX以外の手段を調整し、止むを得ずFAXを使用する際には、FAX番号の聞き取りの際の復唱や、FAX送信前の送信先への番号の再確認、複数人で複数回のチェックを必ず行うこととした。また、全従業者に対する個人情報保護研修を行った。 ⑪（1）作業環境等を見直し、書類の混入等が起きにくい環境を整備 ①執務室内の作業スペースの確保及び活用 ②引き出し付きの棚をキャビネット内に新設し、書類の分類をよりしやすくした。 （2）委託業者との書類の受け渡し方法の変更（送付する判定機関ごとに数を確認しながら受け渡す）。 ⑫個人情報をFAX送信することを禁止するよう各施設に通知した。 ⑬抽出ツールのプログラム確認は、委託先事業者の運用チームのみが行っていたが、抽出ツールを作成・利用する際には、運用チームに加えて、開発チームと委託元である都の3者で抽出ツールのプログラムの仕様・設定を確認することとした。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策③ 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか 再発防止策の内容	⑧これまで実施してきた委託事業者への発送完了時の確認のほか、委託事業者職員による宛名、住所の複数チェック等、発送作業での確認作業を確実に実施させるとともに、都においても個人情報を含む情報の適切な取扱いについて、さらなる徹底を図り、再発防止に努める。 ⑨（1）スケジュールの情報共有と進行管理の徹底 発送に関わる者を含め、課全員が発送スケジュールや作業進捗状況を把握・共有する。また、管理監督職が発送作業の進捗管理を密に行うことで発送遅延や発送漏れを直ちに把握できるようにする。 （2）発送前後の確認体制の見直し 当日発送すべき郵便物が揃っているか、発送を担当している係全体でチェックする。発送担当者は、郵便局からの領収証を運搬業者から受け取った後に、発送物作成担当者に引き渡す。発送物作成担当者は、領収証等に担当係長・課長の確認押印を受ける。 （3）紛失リスクの解消 発送予定日前にはがきが納品された場合であっても、その日のうちに郵便局へ持ち込み、はがきを長期間執務室に滞留させないようにする。	⑭個人情報の持出、返却確認及び受け渡しの際の確認の徹底を行う。また、作業工程等を点検し、作業方法やチェック方法等ミスが起きにくい方法を検討、実施する。 ⑮郵便の発送作業は複数職員でチェックすることを再徹底。また、特に慎重を要する個人情報を取り扱う施設における個人情報の事故の重大性について改めて周知するとともに、書類の発送、保管、業務の進行管理等について、注意喚起や指導を行った。 ⑯（1）ファイルが他の物に紛れてしまわないよう、目立つ色に変更する。 （2）作業スペースに仕切りを立てて、使用スペースを物理的に限定する。 （3）ファイルに記載する名前をイニシャルに表記変更する等、使用する情報から個人情報を削除する。 （4）決まった時間に決まった人員が所在を確認する。 （5）チェックの時間を定刻とし、声をかけ合う。 （6）出したらしまうといった基本的事項を、改めて徹底するよう、注意喚起する。 （7）急いでいたり、忙しい時間帯でも、ダブルチェックをするよう、改めて徹底する。また、退所時にも荷物を確認してから渡すようにする ⑰（個人情報の管理について） （1） 相談援助業務上の記録をノート等に記載する場合は、イニシャルを使用するなど個人情報を特定されないようにすること。また、私物のノートや手帳に個人情報を記載しないこと。 （2） 庁舎外での会議等に出席した際には、個人端末を活用して記録の作成を行うとともに、作成した文書は暗号化し保存すること。 （3） 業務上やむを得ず個人情報が記録された書類を庁舎外に持ち出す場合は、局の保有個人情報安全管理基準に基づき管理職の許可を得ること。 （4） 個人情報を含む書類を持ち出すにあたっては、盗難や紛失を防止できる形状・機能を持つ鞄に収納し、肌身離さず持ち運ぶなど十分に注意すること。 （5） その他個人情報の取り扱いについては、局の保有個人情報安全管理基準等を遵守し、適正に行うこと。 （職員の証票の管理について） （1） 月１回、各職員の保有状況を点検すること （2） 携行する際には、ストラップ付きのケースに収納するなど、常に身体から離さずに携行することを徹底すること （職員の緊急連絡網の管理について） （1） 必要な連絡先は公用携帯に保存し、連絡網を記載した紙は庁舎外に持ち出さないこと。 ⑱（1）入所時や退所時の手順確認のチェックリスト様式を変更し、入所時の写真撮影やリストへの正確な情報記載、退所時の荷物確認の手順など守るべきルールを追記するとともに、実施者を記載する欄を追加。 （2）個人情報紛失判明時の、本部への速やかな報告や具体的な捜索の手順などを、チェックリストに追記。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策③ 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか 再発防止策の内容		(3)毎朝のミーティングにてリーダー看護師等に個人情報保護の重要性やルールの順守を徹底。勤務者には、業務実施前に最新のマニュアルを確認するよう指導。 ⑲(1)発表資料の事前確認の徹底について幹部会で決定し、各部署に注意喚起 (2)録画や写真撮影をして保管していない旨を書面で確認 (3)画像等の個人情報の収集・利用に関する同意手続きの見直し ⑳(1)電子申請を推奨して紙文書の紛失リスクを軽減 (2)個人情報の適切な管理を職員に改めて周知徹底 ㉑(1)病院へ持ち運ぶファイルに、処方箋を収納する専用スペースを作る (2)医療機関受診時に係るマニュアルを作成 (3)帰園後は可能な限り速やかに所管部署に処方箋等を提出する (4)重要な個人情報を預かっている状況での裁断作業を避ける (5)上記対応について、ミーティング等で周知徹底、注意喚起 ㉒(1)必要なデータファイルのみを送信用データとしてPDF化し、送信前に、PDFに不要な箇所が入っていないことを確認の上、送信することを徹底 (2)メールシステム上、外部送信時に必須である上長の承認の際、個人情報が含まれていないか等の確認を徹底 (3)「メール送信時のセルフチェックリスト」を作成、活用 (4)各管理職より各職員に対する面談時に、個別に再度、再発防止策を徹底 ㉓(1)交付前の事務手順や確認方法の見直し、交付時の最終確認方法の見直し (2)作業スペースへの注意文の掲示やチェックリストへの注意文の記載 (3)確認等を行う人数を増員し、誤交付を防ぐ体制を強化 (4)再発防止勉強会を実施 ㉔(1)委託事業者及び再委託事業者に厳重注意、再発防止策等の作成を指示し、受領 (2)WEBページの脆弱性等の確認を受けるため、デジタルサービス局との調整を開始	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅲ リスク対策③ 7. リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか 再発防止策の内容		㉕(1)精査が十分でないデータを外部に提供しないこと、精査及び送付の際には複数体制でチェックすることを徹底 (2)受託事業者において、作成した資料のレビューフローの再検討、個人情報データの受領・管理方法に関する社内再教育等の取組を実施 ㉖(1)ダブルチェックの徹底及びその旨の指導 (2)作業項目の文章化、わかりやすいチェックリストの作成 ㉗(1)受託事業者において、マニュアルに沿った処理を徹底し、送付書類の引継ぎ時には、郵便局ともに引継ぎ件数一を確認 (2)3か月間、受託事業者から送付先に対し、発送日の連絡及び到着の確認を行う。 ㉘(1)原則電子申請として紙文書の紛失リスクを軽減 (2) 書類の所在及び処理状況を明確に把握できるよう管理方法を見直す ㉙(1)個人情報の取扱い及び情報管理の徹底等について、厳重に注意喚起 (2)個人情報が特定できない記載にする等の対策 ㉚(1)局内各職場にて個人情報事故防止対策等をテーマとした職場討議実施 (2)個人情報安全管理強化月間の自己点検・職場点検による一層の意識啓発 ㉛(1)張り紙の掲示、FAXボタンへの着色による物理的な注意喚起 (2)FAX送付時のダブルチェック、送信履歴の確認等をマニュアルに追加 ㉜(1)区市町村からの書類を収受する際の件数記載用の共通様式を作成し、受領時に種類ごとの件数を確認・記入 (2)本件の事務のプロセスを細分化し、各プロセス毎の書類の受渡し時に、各担当者がそれぞれ(1)の様式に記載した件数に基づき、書類、件数の確認作業を行うよう整理 (3)使用頻度ごとに文書の保管場所を整理し、常時使用しないものは施錠。作業中に開錠しているキャビネットについても、中に担当者ごとの鍵付きの引き出し等を設置して自分の担当以外の書類は持ち出せないようにし、作業の際にその都度施錠。 (4)緊急の所内幹部会を開催し、個人情報を含む書類の受け渡し時の確認等、個人情報の取り扱いのルールが適正に行われているか確認を指示し、報告を受ける。 ㉝(1)個人情報の保管ルールについて全職員に徹底 (2)現在の保管状況の再点検を実施 ㉞(1)受託事業者に対する個人情報の取扱い及び情報管理の徹底に向けた注意喚起 (2)管理番号の活用など個人情報が特定できない情報管理方法等の導入 ㉟(1)廃棄時の職員立会いの徹底、チェックリストの作成、活用 (2)廃棄対象文書とシステム登録情報の照会の実施 ㊱書類の保管場所の見直し	事前	実態に合わせ修正
令和7年2月28日	Ⅲ リスク対策④		④eLTAX電子納税通知システムファイルについて新規で記載。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅳ1. ①自己点検 具体的なチェック方法	・サイバーセキュリティ責任者・個人情報管理責任者・特定個人情報管理責任者及び全職員は、毎年度1回以上、点検表に基づき、職場の文書管理、サイバーセキュリティ及び個人情報安全管理に関する点検を行っている。点検結果については、主税局サイバーセキュリティ委員会へ報告している。 ・国税連携システム（eLTAX）については、「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（平成25年総務省告示第206号）」の達成状況について、自己評価を実施している。	・サイバーセキュリティ責任者・個人情報管理責任者・特定個人情報管理責任者及び全職員は、毎年度1回以上、点検表に基づき、職場の文書管理、サイバーセキュリティ及び個人情報安全管理に関する点検を行っている。点検結果については、主税局サイバーセキュリティ委員会へ報告している。 ・国税連携システム（eLTAX）については、「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（平成25年総務省告示第206号）」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ついては、運用規則等に基づき、中間サーバ･プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。	事前	実態に合わせ修正
令和7年2月28日	Ⅳ2. 従業者に対する教育・啓発 具体的な方法	・IPA（情報処理推進機構）が提供する最新のサイバーセキュリティ教育用資料等を基にセキュリティ教育資材を作成し、中間サーバー･プラットフォームの運用に携わる職員及び事業者に対し、運用規則（接続運用規程等）やサイバー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。 ・全職員を対象にサイバーセキュリティ・個人情報保護の研修を実施している。研修の目的は、個人情報保護の重要性及び適正管理等に関する理解を深め、個人情報保護の遵守を徹底することである。具体的には、以下の研修を実施している。 ・毎年の悉皆研修 ・個人端末からアクセスするeラーニング研修（理解度が基準に達しないと修了できない） ・新規採用職員や他局転入職員等を対象とした研修 なお、未受講者については、翌年度同様の研修を受講させている。また、eラーニングについては、システムにより受講管理を実施し、未受講者に受講を促すことで、未受講者が出ないようにしている。	【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）が提供する最新のサイバーセキュリティ教育用資料等を基にセキュリティ教育資材を作成し、中間サーバー･プラットフォームの運用に携わる職員及び事業者に対し、運用規則（接続運用規程等）やサイバー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。 【税務総合支援システム】 ・全職員を対象にサイバーセキュリティ・個人情報保護の研修を実施している。研修の目的は、個人情報保護の重要性及び適正管理等に関する理解を深め、個人情報保護の遵守を徹底することである。具体的には、以下の研修を実施している。 ・毎年の悉皆研修 ・個人端末からアクセスするeラーニング研修（理解度が基準に達しないと修了できない） なお、未受講者については、翌年度同様の研修を受講させている。また、eラーニングについては、システムにより受講管理を実施し、未受講者に受講を促すことで、未受講者が出ないようにしている。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年2月28日	Ⅴ1. ④個人情報ファイル簿の公表	行っていない	行っている	事前	実態に合わせ修正
令和7年2月28日	Ⅴ1. ④個人情報ファイル簿の公表 個人情報ファイル名		個人事業税の課税情報ファイル、自動車税（環境性能割・種別割）の課税情報ファイル、事業所税の課税情報ファイル、あて名管理ファイル、収入管理事務ファイル、滞納整理事務ファイル、固定資産税（土地・家屋）の課税情報ファイル、不動産取得税の課税情報ファイル、不動産登記済通知データ変換・加工システム、固定資産税（償却資産）の課税情報ファイル、情報連携ファイル	事前	実態に合わせ修正
令和7年2月28日	Ⅴ1. ④個人情報ファイル簿の公表 公表場所		東京都総務局総務部情報公開課	事前	実態に合わせ修正
令和7年3月28日	Ⅱ特定個人情報ファイルの概要① 4. 特定個人情報ファイルの取扱いの委託	委託事項1～15	・AI-OCR等保守委託 ・基盤（データセンタ・回線）賃借・保守委託 ・税務総合支援システムデータ出力センタ委託 ・登記済通知書等処理業務委託 ・AI－OCR業務委託 ・自動車保有関係手続ワンストップサービスに係る維持管理委託 を削除。項番を修正。	事前	実態に合わせ修正
令和7年3月28日	（別添2）特定個人情報ファイル記録項目	・記録項目の詳細については別紙11参照 ・①賦課徴収事務ファイルに関するマスター覧は次頁のとおり	・①賦課徴収事務ファイルに関するマスター覧は別紙10のとおり ・記録項目の詳細については別紙11参照 ・④eLTAX電子納税通知システムファイルのファイルレイアウト案は令和7年9月に地方税共同機構より公開予定 ・DA（個人事業税）：「個人事業税カルテ管理マスタ」、「個人事国税申告事績情報マスタ」、「減免受付管理マスタ」 FA（自動車二税）：「自二税減免申請情報マスタ」、「受付管理（減免申請書）マスタ」、「受付管理（更新申立）マスタ」 GA（固定資産税（土地・家屋））：「閲覧証明管理申請統括マスタ」 SA（情報連携）：「番号連携精神障害者手帳マスタ」、「番号連携身体障害者手帳マスタ」 には要配慮個人情報を含む。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月28日	Ⅲリスク対策① 3. 特定個人情報の使用 リスク3：従業者が事務外で使用するリスク ・リスクに対する措置の内容	①「東京都特定個人情報の保護に関する条例」で目的外利用は禁止されている。 ②局内の規定において、原則、情報資産の外部持ち出しを禁止している。 ③これらを担保する手段として、上記条例等を研修や自己点検表等で職員へ周知するとともに、税務総合支援システム端末での外部記録媒体の使用を制限すること等により、容易に情報資産の持出しができないようにしている。 ④税務総合支援システムは、当該システムの専用端末以外では使用することができないよう対策が講じられている。 ⑤不正持出しの抑制手段として、全操作履歴を記録することによる監視を行っている。 ⑥外部持出しが必要な際には専用ソフトを用いてデータを暗号化しており、パスワード入力による暗号解除を行わない限り参照することができない。 【AI-OCR】 （事務外での使用については、税務総合支援システムと同様に禁止している。①～④） ・ユーザ単位のアクセスの証跡を取得し、一定期間保存できるようにしている。 【電子書庫】 （事務外での使用については、税務総合支援システムと同様に禁止している。①～④） ・ユーザ単位のアクセスの証跡を取得し、一定期間保存できるようにしている。 【EUC】 （事務外での使用については、税務総合支援システムと同様に禁止している。①～④） ・データベースへのアクセス証跡をユーザ単位で取得、保管している 【電子決裁】 （事務外での使用については、税務総合支援システムと同様に禁止している。①～④ ） ・ユーザ単位のアクセスの証跡を取得し、一定期間保存できるようにしている。 【外部連携基盤】 （事務外での使用については、税務総合支援システムと同様に禁止している。①～④ ） ・ユーザ単位のアクセスの証跡を取得し、一定期間保存できるようにしている	①局内の規定において、原則、情報資産の外部持ち出しを禁止している。 ②税務総合支援システム端末での外部記録媒体の使用を制限すること等により、容易に情報資産の持出しができないようにしている。 ③税務総合支援システムは、当該システムの専用端末以外では使用することができないよう対策が講じられている。 ④不正持出しの抑制手段として、全操作履歴を記録することによる監視を行っている。 ⑤外部持出しが必要な際には専用ソフトを用いてデータを暗号化しており、パスワード入力による暗号解除を行わない限り参照することができない。 ⑥所外用モバイル端末にて情報資産の持ち出しを行う場合は、持ち出し時に複数名でデータ内容を全て確認した上で上司の承認を得て持ち出しを行う。また、出張時は2名で対応する等相互監視により、事務外での不正な利用を防止している。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月28日	Ⅲリスク対策① 3．特定個人情報の使用 リスク4：特定個人情報ファイルが不正に複製されるリスク ・リスクに対する措置の内容	①税務総合支援システム内の特定個人情報ファイルは、税務総合支援システム端末以外から閲覧することができない。 ②税務総合支援システム端末での外部記録媒体の使用を制限し、情報資産の持出しができないようにしている。ただし、規定等に基づき、情報資産を外部へ持ち出す必要がある場合については、当該規定及びサブシステム所管部署の申請に基づき、情報資産の持出しを可能としている。この際には、例外的に外部記録媒体の使用が許可されている端末により、システム管理部署がデータの移行を実施している。 ③ハードコピー等の紙資料については、取扱いに細心の注意を払うよう、研修や自己点検表等により注意喚起している。 ④東京都特定個人情報の保護に関する条例第25条により、必要な範囲を超えての作成を禁止している。 【AI-OCR】 ・OCR処理を施すためのスキャンデータはスキャナシャットダウン時に自動で削除される。 ・共有フォルダ内の不使用となったデータは適宜職員及び利用管理者が削除を行っている。 【電子書庫】 ・特定個人情報ファイルの保存を禁止している。 ・電子ファイルについて、データの改ざん防止策を行っている。具体的には、タイムスタンプを付与し、以下を証明できるようにしている。ある時刻にその文書が存在していた（存在）その文書は改ざんされていない（完全性） 【EUC】 ・なし（「マイナンバーを除く個人情報（氏名、郵便番号、住所、電話番号）も蓄積可能とすること。」を要件化しているため、特定個人情報を含む情報は抽出できない） ・なし（データの改ざん防止策は特に取られていない。） 【電子決裁】 ・特定個人情報ファイルの保存を禁止している。 【外部連携基盤】 ・外部機関との自動ファイル連携では、特別な管理者権限またはバッチ処理しかフォルダにアクセスできないように制限し、一般ユーザーがファイルを参照することを防止している。 ・業務ファイルについては、特定個人情報の取り扱いを禁止しており、ファイル送受信時には上位者の承認を必要としている。	①税務総合支援システム内の特定個人情報ファイルは、税務総合支援システム端末以外から閲覧することができない。 ②税務総合支援システム端末での外部記録媒体の使用を制限し、情報資産の持出しができないようにしている。ただし、規定等に基づき、情報資産を外部へ持ち出す必要がある場合については、当該規定及びサブシステム所管部署の申請に基づき、情報資産の持出しを可能としている。この際には、例外的に外部記録媒体の使用が許可されている端末により、システム管理部署がデータの移行を実施している。 ③ハードコピー等の紙資料については、取扱いに細心の注意を払うよう、研修や自己点検表等により注意喚起している。 ④業務において、必要な範囲を超えての作成を禁止している。 ⑤所外用モバイル端末にて情報資産の持ち出しを行う場合は、持ち出し時に複数名でデータ内容を全て確認した上で上司の承認を得て持ち出しを行う。 ⑥所外用モバイル端末に保存する情報資産について、規定により特定個人情報は保存することができないようにしている。 ⑦特定個人情報を取り扱う事務において使用するシステム及びその間のネットワークにおいても不正に複製されるリスクに対する対策が講じられている。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月28日	Ⅲリスク対策① 4. 特定個人情報ファイルの取扱いの委託 情報保護管理体制の確認	【委託事項1～6、9、11、12(予定)、13】 ・委託契約で下記事項を規定している。 （1）責任者、作業体制、連絡体制及び作業場所の提出 （2）業務従事者への遵守事項の周知及び実施報告の提出 （3）再委託の承諾申請の提出 （4）作業担当者の名簿の提出　等 【委託事項7、8】 委託契約で下記事項を規定している。 （1）責任者、作業体制、連絡体制及び作業場所の提出 （2）業務従事者への遵守事項の周知及び実施報告の提出 （3）作業担当者の名簿の提出　等 【委託事項10】 ・責任者及び業務従事者の名簿を提出する旨を、委託契約で規定している。 【委託事項14】 ・現場を総括する業務責任者を選任し委託元に届け出る旨を、委託契約で規定している。 【委託事項15】 ・責任者及び業務従事者の名簿を提出する旨を、委託契約で規定している。	【委託事項1～3、7、8】 ・委託契約で下記事項を規定している。 （1）責任者、作業体制、連絡体制及び作業場所の提出 （2）業務従事者への遵守事項の周知及び実施報告の提出 （3）再委託の承諾申請の提出 （4）作業担当者の名簿の提出　等 ・委託先がプライバシーマーク等を保有していることを確認している。 【委託事項4～6】 委託契約で下記事項を規定している。 （1）責任者、作業体制、連絡体制及び作業場所の提出 （2）業務従事者への遵守事項の周知及び実施報告の提出 （3）作業担当者の名簿の提出　等 【委託事項9】 ・委託先が倉庫業法第3条による登録を受けた事業者であること、貨物自動車運送事業法第3条による一般貨物運送事業の許可を受けた事業者であること、プライバシーマークを取得していることを確認している。 ・保管をISMS(環境セキュリティマネジメントシステム)適合性評価制度の認証を受けている施設において行うことを確認している。 【委託事項10】 ・責任者及び業務従事者の名簿を提出する旨を、委託契約で規定している。 【委託事項1～10】 ・委託事項の内容、委託先等におけるリスクに応じて情報保護管理体制の確認を行っている。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月28日	Ⅲリスク対策① 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限	【委託事項1～6、10、11、12(予定)】 ・委託先が使用するユーザIDは、局内のIDに関する規定に基づき、委託元が割り当てを行っている。 ・ユーザIDの設定に際しては、用途を確認した上で必要最小限の権限のみ付与し、使用する期間のみ有効とし、有効期間が経過した場合には当該ユーザIDでは特定個人情報ファイルを閲覧できないようにしている。 【AI-OCR】 (認証については、税務総合支援システムと同様に実施している。 【電子書庫】 (認証については、税務総合支援システムと同様に実施している。 【EUC】 (認証については、税務総合支援システムと同様に実施している。 【電子決裁】 (認証については、税務総合支援システムと同様に実施している。 【外部連携基盤】 (認証については、税務総合支援システムと同様に実施している。 【委託事項7、8】 ・ 委託先の業務の推進体制の作成、秘密の保持、目的外使用の禁止、複写及び複製の禁止、作業場所以外への持ち出し禁止、情報の保管および管理等を規定した契約を取り交わしている。 【委託事項9】 仕様書において、都が受託者に貸与するユーザIDは、「税務総合支援システムユーザID管理要綱」に則り受託者が管理することになっている。ユーザIDを使用しない限り特定個人情報ファイルの閲覧はできない。作業者を限定するために、委託業務従事者名簿を提出させ、その者以外の委託業務場所への立入りを禁じている。 【委託事項13】 委託先が閲覧等する際は、委託元からの依頼をもとに運用業務委託業者(委託先2)が操作端末を立ち上げ、委託先が当該端末を使用する体制となっている。 【委託事項14】 委託契約で下記事項を規定している。 ・再委託業務を除き、作業員には正社員を充て、委託者の求めに応じて作業員の身分を証する書面等を提出する。 【委託事項15】 ・委託契約で、一連の業務を委託先が自ら行うことを規定している。 ・搬入された箱は開封することなく処理することを委託契約で規定しているため、特定個人情報ファイルの閲覧・更新のおそれはない。	【委託事項1～3、8】 ・委託先が使用するユーザIDは、局内のIDに関する規定に基づき、委託元が割り当てを行っている。 ・ユーザIDの設定に際しては、用途を確認した上で必要最小限の権限のみ付与し、使用する期間のみ有効とし、有効期間が経過した場合には当該ユーザIDでは特定個人情報ファイルを閲覧できないようにしている。 【委託事項4～6】 ・委託先の業務の推進体制の作成、秘密の保持、目的外使用の禁止、複写及び複製の禁止、作業場所以外への持ち出し禁止、情報の保管および管理等を規定した契約を取り交わしている。 【委託事項7】 仕様書において、都が受託者に貸与するユーザIDは、「税務総合支援システムユーザID管理要綱」に則り受託者が管理することになっている。ユーザIDを使用しない限り特定個人情報ファイルの閲覧はできない。作業者を限定するために、委託業務従事者名簿を提出させ、その者以外の委託業務場所への立入りを禁じている。 【委託事項9】 委託契約で下記事項を規定している。 ・再委託業務を除き、作業員には正社員を充て、委託者の求めに応じて作業員の身分を証する書面等を提出する。 【委託事項10】 ・委託契約で、一連の業務を委託先が自ら行うことを規定している。 ・搬入された箱は開封することなく処理することを委託契約で規定しているため、特定個人情報ファイルの閲覧・更新のおそれはない。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月28日	Ⅲリスク対策① 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの取扱いの記録	【委託事項1～9、10、11、12（予定）、13】 ・施錠された保管庫等での管理、管理状況の記録、管理記録の報告等を委託契約で規定している。 ・システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、いつどの情報にアクセスし、抽出したのかが記録されている。また、操作履歴データは、アクセス制御・暗号化により改竄や削除ができないようにしている。 【AI-OCR】 ・ユーザ単位のアクセスの証跡を取得し、一定期間保存できるようにしている。 【電子書庫】 ・ユーザ単位のアクセスの証跡を取得し、一定期間保存できるようにしている。 【EUC】 ・データベースへのアクセス証跡をユーザ単位で取得、保管している。 【電子決裁】 ・ユーザ単位のアクセスの証跡を取得し、一定期間保存できるようにしている。 【外部連携基盤】 ・ユーザ単位のアクセスの証跡を取得し、一定期間保存できるようにしている。 【委託事項14】 ・新規預入れ、保管、配送、返却、解約及び廃棄処理実績について、内訳書を毎月提出する。 【委託事項15】 ・作業完了後、委託先と委託元の双方が箱数の確認印を押印した「作業数量確認書」を作成し、毎月委託元へ提出する。 ・処理完了後、溶解証明書を毎月委託元へ提出する。	【委託事項1～5、7、8】 ・施錠された保管庫等での管理、管理状況の記録、管理記録の報告等を委託契約で規定している。 ・システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、いつどの情報にアクセスし、抽出したのかが記録されている。また、操作履歴データは、アクセス制御・暗号化により改竄や削除ができないようにしている。 【委託事項9】 ・新規預入れ、保管、配送、返却、解約及び廃棄処理実績について、内訳書を毎月提出する。 【委託事項10】 ・作業完了後、委託先と委託元の双方が箱数の確認印を押印した「作業数量確認書」を作成し、毎月委託元へ提出する。 ・処理完了後、溶解証明書を毎月委託元へ提出する。	事前	実態に合わせ修正
令和7年3月28日	Ⅲリスク対策① 4. 特定個人情報ファイルの取扱いの委託 特定個人情報の提供ルール 委託先から他社への提供に関するルールの内容及びルール遵守の方法	【委託事項1～11、12（予定）、13～15】 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について委託契約で規定している。	【委託事項1～10】 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について委託契約で規定している。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月28日	Ⅲリスク対策① 4. 特定個人情報ファイルの取扱いの委託 特定個人情報の提供ルール 委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	【委託事項1～9】 ① 委託先から他者への提供はない。なお、提供する必要性が発生する場合は、目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について契約で取り交わしている。 ② 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。 【委託事項4】 データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。 【委託事項9】 受託者は、業務委託仕様書の内容を遵守する旨記載した誓約書を都に提出することになっている。また、都による監査、点検及び検査に協力することが仕様書に規定されている。 【委託事項10】 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。 【委託事項11、12(予定)】 ・ 申告書を委託先へ搬入する際及び委託先から申告書の返却を受ける際は、受払票を用いて委託元・委託先相互に部数の確認を行っている。 ・ 申告書を委託元へ返却するまでの期間は、ロッカー等で施錠保管しており、委託先の退出後、都税事務所職員が施錠確認を行っている。 【委託事項13】 テスト用データを含め委託元から委託先への提供はない。また、委託先が行う本番データの参照は、委託元からの作業依頼を基にデータセンタに設置されている専用の端末により、実施している。 【委託事項14】 委託契約で下記事項を規定している。 ・配送及び引取りは、施錠可能なコンテナ車を使用する。 ・配送及び引取りの際は、従事する作業員は写真付き証明書(社員証等)を提示するとともに、委託元職員に対して配送及び引取りの事実を証する書面を交付する。 【委託事項15】 委託契約で下記事項を規定している。 ・引渡しの際、委託元に身分証明書を提示し、確認を受ける。 ・運搬にあたっては、荷台を施錠するとともに、委託元職員が随行する。 ・委託先作業員は、一連の作業の際、運搬車から離れてはならず、作業においては文書保存箱の内容物を一片たりとも散逸、抜取り等してはならない。 ・搬入された箱はほかの場所に一時保管することなく直ちに処理を開始し、その日のうちに処理を終える。	【委託事項1～7】 ① 委託先から他者への提供はない。なお、提供する必要性が発生する場合は、目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について契約で取り交わしている。 ② 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。 【委託事項7】 受託者は、業務委託仕様書の内容を遵守する旨記載した誓約書を都に提出することになっている。また、都による監査、点検及び検査に協力することが仕様書に規定されている。 【委託事8】 ・ 申告書を委託先へ搬入する際及び委託先から申告書の返却を受ける際は、受払票を用いて委託元・委託先相互に部数の確認を行っている。 ・ 申告書を委託元へ返却するまでの期間は、ロッカー等で施錠保管しており、委託先の退出後、都税事務所職員が施錠確認を行っている。 【委託事項9】 委託契約で下記事項を規定している。 ・配送及び引取りは、施錠可能なコンテナ車を使用する。 ・配送及び引取りの際は、従事する作業員は写真付き証明書(社員証等)を提示するとともに、委託元職員に対して配送及び引取りの事実を証する書面を交付する。 【委託事項10】 委託契約で下記事項を規定している。 ・引渡しの際、委託元に身分証明書を提示し、確認を受ける。 ・運搬にあたっては、荷台を施錠するとともに、委託元職員が随行する。 ・委託先作業員は、一連の作業の際、運搬車から離れてはならず、作業においては文書保存箱の内容物を一片たりとも散逸、抜取り等してはならない。 ・搬入された箱はほかの場所に一時保管することなく直ちに処理を開始し、その日のうちに処理を終える。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月28日	Ⅲリスク対策① 4. 特定個人情報ファイルの取扱いの委託 特定個人情報消去ルール、ルールの内容及びルール遵守の確認方法	【委託事項1～6】 ・ 契約履行完了後に当該委託業務に係る情報を全て消去することを、委託契約で規定している。 ・ 消去した情報項目、数量、消去方法及び消去日等については報告書類にて確認している。 【委託事項7、8、10】 ・委託元から委託先への提供はない。 ・消去は行わない。 【委託事項9、13】 特定個人情報の提供はない。 【委託事項11、12(予定)】 ・ 入力に使用した帳票及び出力した帳票類は委託元に返却すること、複写ミス等によりコピー用紙等の廃棄を行う必要が生じた場合も委託元に引継ぐことを、委託契約で規定している。 ・ 受払票にて、委託前後で帳票の部数が一致することを確認している。 ・ 委託先は業務の過程で特定個人情報ファイルを保有しないため、電子データを消去する必要はない。	【委託事項1～3】 ・ 契約履行完了後に当該委託業務に係る情報を全て消去することを、委託契約で規定している。 ・ 消去した情報項目、数量、消去方法及び消去日等については報告書類にて確認している。 【委託事項4～6】 ・委託元から委託先への提供はない。 ・消去は行わない。 【委託事項7】 特定個人情報の提供はない。 【委託事項8】 ・ 入力に使用した帳票及び出力した帳票類は委託元に返却すること、複写ミス等によりコピー用紙等の廃棄を行う必要が生じた場合も委託元に引継ぐことを、委託契約で規定している。 ・ 受払票にて、委託前後で帳票の部数が一致することを確認している。 ・ 委託先は業務の過程で特定個人情報ファイルを保有しないため、電子データを消去する必要はない。 【委託事項9】 委託契約で下記事項を規定している。 ・廃棄処理は、秘密が漏えいすることのないよう、箱ごと溶解する方法で行う。 ・廃棄処理の実施に当たっては、事前に、委託元と委託先とで協議の上、実施計画を定める。 ・都職員の要求があった場合には、廃棄処理への立会いを認める。 ・廃棄処理を終了したときは、速やかに委託元の担当者に報告し、後日廃棄処理の完了届を提出する。 【委託事項10】 委託契約で下記事項を規定している。 ・搬入された文書保保存箱を開封することなく直接溶解槽に投入し、処理する。 ・処理に際して、委託元職員の立会いを認める。 ・機械トラブル等やむを得ない理由により箱を開封する必要が生じた場合は、委託元の監視のもとで開封する。この場合、内容物を直ちに溶解槽に投入し、一片たりとも散逸、抜取り等してはならない。 ・処理完了後、溶解証明書を毎月委託元へ提出する。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月28日	Ⅲリスク対策① 4. 特定個人情報ファイルの取扱いの委託 委託契約中の特定個人情報ファイルの取扱いに関する規定	・委託契約で下記事項を規定している。 【委託事項1、2、5】 （1）プログラム、データ等が格納されたサーバー及び端末機器等は、適切なアクセス権限を設定すること。 （2）外部記録媒体でやり取りするプログラム、データ等は、最新のパターンファイルを適用したウイルス対策ソフトでチェックすること。 【委託事項1～6】 （3）セキュリティ監査を実施する際は協力すること。 （4）委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく委託元に報告すること。 【委託事項7、8】 ・委託契約で下記事項を規定している。 （1）目的外使用の禁止、情報の保管及び管理、再委託の取扱い、実地調査の実施 （2）委託先の担当者名簿の提出 （3）委託の履行に関して知り得た情報を漏らしてはならない。 （4）契約書及び仕様書の内容を遵守する旨記載した誓約書を提出すること。 【委託事項9、10、13】 特定個人情報の提供はない。 【委託事項11、12（予定）】 ・仕様書の内容を遵守する旨記載した誓約書の提出、東京都特定個人情報の保護に関する条例の規定の遵守を委託契約で規定している。 ・委託先が委託元へ提出する誓約書において、当該条例の遵守について明記している。 ・委託先は、委託元による監査、点検及び検査に協力することとなっており、必要に応じて業務改善を指示することができる。 【委託事項14】 委託契約で下記事項を規定している。 ・廃棄処理は、秘密が漏えいすることのないよう、箱ごと溶解する方法で行う。 ・廃棄処理の実施にあたっては、事前に委託元と委託先とで協議の上、実施計画を定める。 ・都職員の要求があった場合には、廃棄処理への立会いを認める。 ・廃棄処理を終了したときは、速やかに委託元の担当者に報告し、後日廃棄処理の完了届を提出する。 【委託事項15】 委託契約で下記事項を規定している。 ・搬入された文書保存箱を開封することなく直接溶解槽に投入し、処理する。 ・処理に際して、委託元職員の立会いを認める。 ・機械トラブル等やむを得ない理由により箱を開封する必要が生じた場合は、委託元の監視のもとで開封する。この場合、内容物を直ちに溶解槽に投入し、一片たりとも散逸、抜取り等してはならない。 ・処理完了後、溶解証明書を毎月委託元へ提出する。	・委託契約で下記事項を規定している。 【委託事項1、2】 （1）プログラム、データ等が格納されたサーバー及び端末機器等は、適切なアクセス権限を設定すること。 （2）外部記録媒体でやり取りするプログラム、データ等は、最新のパターンファイルを適用したウイルス対策ソフトでチェックすること。 【委託事項1～3】 （3）セキュリティ監査を実施する際は協力すること。 （4）委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく委託元に報告すること。 【委託事項4～6】 ・委託契約で下記事項を規定している。 （1）目的外使用の禁止、情報の保管及び管理、再委託の取扱い、実地調査の実施 （2）委託先の担当者名簿の提出 （3）委託の履行に関して知り得た情報を漏らしてはならない。 （4）契約書及び仕様書の内容を遵守する旨記載した誓約書を提出すること。 【委託事項7】 特定個人情報の提供はない。 【委託事項9】 ・目的外使用の禁止、情報の保管及び管理　等 【委託事項10】 （1）目的外使用の禁止、情報の保管及び管理、実地調査及び指示すること。 （2）委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく委託元に報告すること。	事前	実態に合わせ修正
令和7年3月28日	Ⅲリスク対策① 4. 特定個人情報ファイルの取扱いの委託 再委託先による特定個人情報ファイルの適切な取り扱いの確保、具体的な方法	【委託事項1～6】 ①委託元と委託先の間で取り交わされている契約内容と同等の条件を再委託先においても課している。 ②委託元が再委託先に対して実地調査を1年に1回行い、適切な管理体制をとっていることを確認している。 ③委託先が再委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく報告させている。 【委託事項7、8、11、12（予定）、15】 再委託について禁止している。 【委託事項9、10、13】 特定個人情報の提供はない。 【委託事項14】 再委託先への特定個人情報ファイルの受渡し、廃棄作業時に委託元が立ち会っている。	【委託事項1～3】 ①委託元と委託先の間で取り交わされている契約内容と同等の条件を再委託先においても課している。 ②委託元が再委託先に対して実地調査を1年に1回行い、適切な管理体制をとっていることを確認している。 ③委託先が再委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく報告させている。 【委託事項4、5、8、10】 再委託について禁止している。 【委託事項7】 特定個人情報の提供はない。 【委託事項9】 再委託先への特定個人情報ファイルの受渡し、廃棄作業時に委託元が立ち会っている。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月28日	Ⅲリスク対策② 4. 特定個人情報ファイルの取扱いの委託 情報保護管理体制の確認	【委託事項1～5】 ・委託契約で下記事項を規定し、確認している。 （1）責任者、作業体制、連絡体制及び作業場所の提出 （2）業務従事者への遵守事項の周知及び実施報告の提出 （3）再委託の承諾申請の提出 （4）作業担当者の名簿の提出　等	【委託事項1～4】 ・委託契約で下記事項を規定し、確認している。 （1）責任者、作業体制、連絡体制及び作業場所の提出 （2）業務従事者への遵守事項の周知及び実施報告の提出 （3）再委託の承諾申請の提出 （4）作業担当者の名簿の提出　等 ・委託先がプライバシーマーク等を保有していることを確認している。 ・委託事項の内容、委託先等におけるリスクに応じて情報保護管理体制の確認を行っている。	事前	実態に合わせ修正
令和7年3月28日	Ⅲリスク対策② 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限	【委託事項1～5】 ・委託先が使用するユーザIDは、局内のIDに関する規定に基づき、委託元が割り当てを行っている。 ・ユーザIDの設定に際しては、用途を確認した上で必要最小限の権限のみ付与し、使用する期間のみ有効とし、有効期間が経過した場合には当該ユーザIDでは特定個人情報ファイルを閲覧できないようにしている。	【委託事項1～4】 ・委託先が使用するユーザIDは、局内のIDに関する規定に基づき、委託元が割り当てを行っている。 ・ユーザIDの設定に際しては、用途を確認した上で必要最小限の権限のみ付与し、使用する期間のみ有効とし、有効期間が経過した場合には当該ユーザIDでは特定個人情報ファイルを閲覧できないようにしている。	事前	実態に合わせ修正
令和7年3月28日	Ⅲリスク対策② 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの取扱いの記録	【委託事項1～5】 ・施錠された保管庫等での管理、管理状況の記録、管理記録の報告等を委託契約で規定している。 ・システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、いつどの情報にアクセスし、抽出したのかが記録されている。また、操作履歴データは、アクセス制御・暗号化により改竄や削除ができないようにしている。	【委託事項1～4】 ・施錠された保管庫等での管理、管理状況の記録、管理記録の報告等を委託契約で規定している。 ・システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、いつどの情報にアクセスし、抽出したのかが記録されている。また、操作履歴データは、アクセス制御・暗号化により改竄や削除ができないようにしている。	事前	実態に合わせ修正
令和7年3月28日	Ⅲリスク対策② 4. 特定個人情報ファイルの取扱いの委託 委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	【委託事項1～5】 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。	【委託事項1～4】 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月28日	Ⅲリスク対策② 4. 特定個人情報ファイルの取扱いの委託 委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	【委託事項1～4】 ① 委託先から他者への提供はない。なお、提供する必要性が発生する場合は、目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について契約で取り交わしている。 ② 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。 【委託事項2】 データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。 【委託事項5】 　目的外使用の禁止、情報の保管及び管理、再委託の取扱い、実地調査及び指導等について契約で取り交わしている。	【委託事項1～4】 ① 委託先から他者への提供はない。なお、提供する必要性が発生する場合は、目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について契約で取り交わしている。 ② 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。 【委託事項2】 データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。	事前	実態に合わせ修正
令和7年3月28日	Ⅲリスク対策② 4. 特定個人情報ファイルの取扱いの委託 ルールの内容及びルール遵守の確認方法	【委託事項1～5】 ・契約履行完了後に外部記憶媒体上に含まれる当該委託業務に係る情報を全て消去することを、委託契約で規定している。 ・消去した情報項目、数量、消去方法及び消去日等について報告書類等にて確認している。 【委託事項5】 報告書と併せて情報消去済みの記録媒体を返送させ、消去済みであることを委託元において確認している。なお、記録媒体の搬送時には、パスワードロック式のセキュリティボックスを使用している。	【委託事項1～4】 ・契約履行完了後に外部記憶媒体上に含まれる当該委託業務に係る情報を全て消去することを、委託契約で規定している。 ・消去した情報項目、数量、消去方法及び消去日等について報告書類等にて確認している。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月28日	Ⅲリスク対策② 4. 特定個人情報ファイルの取扱いの委託 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	・委託契約で下記事項を規定している。 【委託事項1、3、4、5】 （1）プログラム、データ等が格納されたサーバー及び端末機器等は、適切なアクセス権限を設定すること。 （2）外部記録媒体でやり取りするプログラム、データ等は、最新のパターンファイルを適用したウイルス対策ソフトでチェックすること。 【委託事項1～5】 （3）セキュリティ監査を実施する際は協力すること。 （4）委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく委託元に報告すること。	・委託契約で下記事項を規定している。 【委託事項1、2、4】 （1）プログラム、データ等が格納されたサーバー及び端末機器等は、適切なアクセス権限を設定すること。 （2）外部記録媒体でやり取りするプログラム、データ等は、最新のパターンファイルを適用したウイルス対策ソフトでチェックすること。 【委託事項1～3】 （3）セキュリティ監査を実施する際は協力すること。 （4）委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく委託元に報告すること。	事前	実態に合わせ修正
令和7年3月28日	Ⅲリスク対策② 4. 特定個人情報ファイルの取扱いの委託 再委託先による特定個人情報ファイルの適切な取扱いの確保	【委託事項1～5】 ・委託元と委託先の間で取り交わされている契約内容と同等の条件を再委託先においても課している。 ・委託元が再委託先に対して実地調査を定期的に行い、適切な管理体制をとっていることを確認している。 ・委託先が再委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく報告させている。	【委託事項1～4】 ・委託元と委託先の間で取り交わされている契約内容と同等の条件を再委託先においても課している。 ・委託元が再委託先に対して実地調査を定期的に行い、適切な管理体制をとっていることを確認している。 ・委託先が再委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく報告させている。	事前	実態に合わせ修正
令和7年3月28日	Ⅲリスク対策③ 4. 特定個人情報ファイルの取扱いの委託 情報保護体制の確認	【委託事項1～4】 ・委託契約で下記事項を規定し、確認している。 （1）責任者、作業体制、連絡体制及び作業場所の提出 （2）業務従事者への遵守事項の周知及び実施報告の提出 （3）再委託の承諾申請の提出 （4）作業担当者の名簿の提出　等	【委託事項1～3】 ・委託契約で下記事項を規定し、確認している。 （1）責任者、作業体制、連絡体制及び作業場所の提出 （2）業務従事者への遵守事項の周知及び実施報告の提出 （3）再委託の承諾申請の提出 （4）作業担当者の名簿の提出　等 ・委託先がプライバシーマーク等を保有していることを確認している。	事前	実態に合わせ修正
令和7年3月28日	Ⅲリスク対策③ 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限	【委託事項1～4】 ・委託先が使用するユーザIDは、局内のIDに関する規定に基づき、委託元が割り当てを行っている。 ・ユーザIDの設定に際しては、用途を確認した上で必要最小限の権限のみ付与し、使用する期間のみ有効とし、有効期間が経過した場合には当該ユーザIDでは特定個人情報ファイルを閲覧できないようにしている。	【委託事項1～3】 ・委託先が使用するユーザIDは、局内のIDに関する規定に基づき、委託元が割り当てを行っている。 ・ユーザIDの設定に際しては、用途を確認した上で必要最小限の権限のみ付与し、使用する期間のみ有効とし、有効期間が経過した場合には当該ユーザIDでは特定個人情報ファイルを閲覧できないようにしている。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月28日	Ⅲリスク対策③ 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの取扱いの記録	【委託事項1～4】 ・施錠された保管庫等での管理、管理状況の記録、管理記録の報告等を委託契約で規定している。 ・システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、いつどの情報にアクセスし、抽出したのかが記録されている。また、操作履歴データは、アクセス制御・暗号化により改竄や削除ができないようにしている。	【委託事項1～3】 ・施錠された保管庫等での管理、管理状況の記録、管理記録の報告等を委託契約で規定している。 ・システムの全操作履歴（ユーザID、操作時間、操作内容等）を記録している。データベースに関しては、いつどの情報にアクセスし、抽出したのかが記録されている。また、操作履歴データは、アクセス制御・暗号化により改竄や削除ができないようにしている。	事前	実態に合わせ修正
令和7年3月28日	Ⅲリスク対策③ 4. 特定個人情報ファイルの取扱いの委託 委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	【委託事項1～4】 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。	【委託事項1～3】 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。	事前	実態に合わせ修正
令和7年3月28日	Ⅲリスク対策③ 4. 特定個人情報ファイルの取扱いの委託 委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	【委託事項1～4】 ① 委託先から他者への提供はない。なお、提供する必要性が発生する場合は、目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について契約で取り交わしている。 ② 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。 【委託事項2】 データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。	【委託事項1～3】 ① 委託先から他者への提供はない。なお、提供する必要性が発生する場合は、目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について契約で取り交わしている。 ② 目的外使用の禁止、第三者への提供の禁止、複写及び複製の禁止、情報の保管及び管理等に対する義務違反時の損害賠償の請求等について、委託契約で規定している。 【委託事項2】 データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際しては静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。	事前	実態に合わせ修正
令和7年3月28日	Ⅲリスク対策③ 4. 特定個人情報ファイルの取扱いの委託 ルールの内容及びルール遵守の確認方法	【委託事項1～4】 ・契約履行完了後に外部記憶媒体上に含まれる当該委託業務に係る情報を全て消去することを、委託契約で規定している。 ・消去した情報項目、数量、消去方法及び消去日等について報告書類等にて確認している。	【委託事項1～3】 ・契約履行完了後に外部記憶媒体上に含まれる当該委託業務に係る情報を全て消去することを、委託契約で規定している。 ・消去した情報項目、数量、消去方法及び消去日等について報告書類等にて確認している。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年3月28日	Ⅲリスク対策③ 4. 特定個人情報ファイルの取扱いの委託 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	・委託契約で下記事項を規定している。 【委託事項1、3、4】 （1）プログラム、データ等が格納されたサーバー及び端末機器等は、適切なアクセス権限を設定すること。 （2）外部記録媒体でやり取りするプログラム、データ等は、最新のパターンファイルを適用したウイルス対策ソフトでチェックすること。 【委託事項1～4】 （3）セキュリティ監査を実施する際は協力すること。 （4）委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく委託元に報告すること。	・委託契約で下記事項を規定している。 【委託事項1、2】 （1）プログラム、データ等が格納されたサーバー及び端末機器等は、適切なアクセス権限を設定すること。 （2）外部記録媒体でやり取りするプログラム、データ等は、最新のパターンファイルを適用したウイルス対策ソフトでチェックすること。 【委託事項1～3】 （3）セキュリティ監査を実施する際は協力すること。 （4）委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく委託元に報告すること。	事前	実態に合わせ修正
令和7年3月28日	Ⅲリスク対策③ 4. 特定個人情報ファイルの取扱いの委託 再委託先による特定個人情報ファイルの適切な取扱いの確保	【委託事項1～4】 ・委託元と委託先の間で取り交わされている契約内容と同等の条件を再委託先においても課している。 ・委託元が再委託先に対して実地調査を定期的に行い、適切な管理体制をとっていることを確認している。 ・委託先が再委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく報告させている。	【委託事項1～3】 ・委託元と委託先の間で取り交わされている契約内容と同等の条件を再委託先においても課している。 ・委託元が再委託先に対して実地調査を定期的に行い、適切な管理体制をとっていることを確認している。 ・委託先が再委託先の担当者名簿を提出するとともに、変更があった場合は遅滞なく報告させている。	事前	実態に合わせ修正
令和7年4月1日	Ⅰ 7. ①部署 ②所属長の役職名	①東京都主税局 税制部システム管理課、課税部計画課、課税部課税指導課、課税部法人課税指導課、資産税部固定資産税課、資産税部固定資産評価課、徴収部計画課、徴収部徴収指導課 ②システム管理課長、自動車税担当課長、課税指導課長、法人課税指導課長、固定資産税課長、固定資産評価課長、計画課長（徴収部）、徴収指導課長	①東京都主税局 総務部システム管理課、課税部計画課、課税部課税指導課、課税部法人課税指導課、資産税部固定資産税課、資産税部固定資産評価課、徴収部計画課、徴収部徴収指導課 ②システム管理課長、システム改善担当課長、自動車税担当課長、課税指導課長、法人課税指導課長、固定資産税課長、固定資産評価課長、計画課長（徴収部）、滞納整理対策担当課長	事前	実態に合わせ修正
令和7年4月1日	Ⅱファイルの概要① 2. ⑥事務担当部署	東京都主税局 税制部システム管理課、課税部計画課、課税部課税指導課、課税部法人課税指導課、資産税部固定資産税課、資産税部固定資産評価課、徴収部計画課、徴収部徴収指導課	東京都主税局 総務部システム管理課、課税部計画課、課税部課税指導課、課税部法人課税指導課、資産税部固定資産税課、資産税部固定資産評価課、徴収部計画課、徴収部徴収指導課	事前	実態に合わせ修正
令和7年4月1日	Ⅱファイルの概要② 2. ⑥事務担当部署	主税局税制部システム管理課	主税局総務部システム管理課	事前	実態に合わせ修正
令和7年4月1日	Ⅱファイルの概要③ 2. ⑥事務担当部署	主税局税制部システム管理課	主税局総務部システム管理課	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年5月7日	Ⅰ 2. システム1 ③他のシステムとの接続	[○]その他（審査システム（eLTAX）、国税連携システム（eLTAX）、団体内統合利用番号連携サーバー）	[○]その他（地方税ポータルシステム（eLTAX）、審査システム（eLTAX）、国税連携システム（eLTAX）、団体内統合利用番号連携サーバー、国税データ閲覧機能、地方税外部連携システム（eLTAX）、eLTAX電子納税通知システム（eLTAX））	事前	実態に合わせ修正
令和7年5月7日	Ⅰ 2. システム2 ②システムの機能	・納税者から固定資産税（償却資産）の申告書受領 ・税務総合支援システムとの特定通信を経由した連携 ・申告データ、利用届出データを他システムへ出力 ・プレ申告書データを償却資産所有者へ送信（地方税ポータルセンタ（eLTAX）経由） ・本人確認用データを地方税ポータルセンタ（eLTAX）へ送信	・地方税法等に明文規定を有する申告・申請等データの受領（地方税ポータルシステム（eLTAX）経由） ・税務総合支援システムとの特定通信を経由した連携 ・申告データ、利用届出データを他システムへ出力 ・プレ申告書データを償却資産所有者へ送信（地方税ポータルシステム（eLTAX）経由） ・本人確認用データを地方税ポータルシステム（eLTAX）へ送信	事前	実態に合わせ修正
令和7年5月7日	Ⅰ 2. システム2 ③他のシステムとの接続	[○]その他（地方税ポータルセンタ（eLTAX））	[○]その他（地方税ポータルシステム（eLTAX））	事前	実態に合わせ修正
令和7年5月7日	Ⅰ 2. システム3 ③他のシステムとの接続	[○]その他（地方税ポータルセンタ（eLTAX）、国税データ閲覧機能）	[○]その他（地方税ポータルシステム（eLTAX））	事前	実態に合わせ修正
令和7年5月7日	Ⅰ 2. システム6 ②システムの機能	・中間サーバーへの符号取得要求の仲介 ・団体内統合利用番号の取得、管理 ・符号、団体内統合利用番号、個別業務システム利用番号の紐付管理 ・副本登録における、個別業務システムから中間サーバーへの登録要求の仲介 ・情報照会における、個別業務システムからの照会要求の受付及び中間サーバーと個別業務システムとの情報授受の仲介	・自治体中間サーバーへの符号取得要求の仲介 ・団体内統合利用番号の取得、管理 ・符号、団体内統合利用番号、個別業務システム利用番号の紐付管理 ・副本登録における、個別業務システムから自治体中間サーバーへの登録要求の仲介 ・情報照会における、個別業務システムからの照会要求の受付及び自治体中間サーバーと個別業務システムとの情報授受の仲介	事前	実態に合わせ修正
令和7年5月7日	Ⅰ 2. システム6 ③他のシステムとの接続	[○]その他（中間サーバー）	[○]その他（自治体中間サーバー）	事前	実態に合わせ修正
令和7年5月7日	Ⅰ 2. システム8 ③他のシステムとの接続	[○]その他（国税連携システム（eLTAX））	[○]その他（地方税ポータルシステム（eLTAX）、国税連携システム（eLTAX））	事前	実態に合わせ修正
令和7年5月7日	Ⅰ 2. システム10 ①システムの名称		地方税外部連携システム（eLTAX）	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年5月7日	Ⅰ 2. システム10 ②システムの機能		地方税外部連携システム（eLTAX）は次の3つの機能により構成される。 ・団体間回送機能：地方団体間で提携様式にてデータ連携を行う機能。 ・法人税情報連携機能：国税庁から連携される法人税申告関連データを地方団体へ連携する機能 ・団体間照会・ファイル送信機能：地方団体間で必要となる様々な照会業務を想定し、対象手続を定めずにデータ授受可能な機能	事前	実態に合わせ修正
令和7年5月7日	Ⅰ 2. システム10 ③他のシステムとの接続		[○]税務システム [○]その他（地方税ポータルシステム（eLTAX））	事前	実態に合わせ修正
令和7年5月7日	Ⅰ 2. システム11 ①システムの名称		eLTAX電子納税通知システム	事前	実態に合わせ修正
令和7年5月7日	Ⅰ 2. システム11 ②システムの機能		予め申請があった納税義務者に対して、eLTAXを経由して電子的に納税通知書の副本を送付する。（令和10年4月1日以降、実装予定。） ・マイナポータルから提供される電子通知希望申請の電子データをeLTAX電子納税通知システムで受信する。 ・受信した電子通知希望申請の電子データについて、システム登録を行い、税務総合支援システムへ送信する。 ・税務総合支援システムから送付された副本データについて、システム登録を行い、納税義務者に対して通知する。	事前	実態に合わせ修正
令和7年5月7日	Ⅰ 2. システム11 ③他のシステムとの接続		[○]税務システム [○]その他（地方税ポータルシステム（eLTAX）、マイナポータル（予定））	事前	実態に合わせ修正
令和7年5月7日	Ⅰ 3.	①賦課徴収事務ファイル　②国税連携ファイル ③電子申告ファイル	①賦課徴収事務ファイル　②国税連携ファイル ③電子申告ファイル　④eLTAX電子納税通知システムファイル　⑤地方税外部連携ファイル（仮称）	事前	実態に合わせ修正
令和7年5月7日	Ⅱ ファイルの概要① 2. ④主な記録項目	その他について記載なし	[○]災害関係情報 [○]その他（公的給付支給等口座登録簿関係情報）	事前	実態に合わせ修正
令和7年2月28日	Ⅱ ファイルの概要① 3. ①入手元		評価実施機関内の他部署、行政機関・独立行政法人等、地方公共団体・地方独立行政法人、民間事業者の項目について修正	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年5月7日	Ⅱ ファイルの概要① 3. ②入手方法	[〇]その他（住民基本台帳ネットワークシステム、地方税ポータルシステム（eLTAX））	[〇]その他（住民基本台帳ネットワークシステム、地方税ポータルシステム（eLTAX）、国税連携システム（eLTAX）、審査システム、自動車税登録情報提供システム、軽自動車検査情報登録情報提供システム、地方税共通納税システム、pufure、eLTAX電子納税通知システム（eLTAX）、国税データ閲覧機能、地方税外部連携システム（eLTAX））	事前	実態に合わせ修正
令和7年5月7日	Ⅱ ファイルの概要① 5. 提供先1	他の道府県知事	道府県	事前	実態に合わせ修正
令和7年5月7日	Ⅱ ファイルの概要① 5. 提供方法	[〇]紙 [〇]その他（国税連携（eLTAX）システム）	[〇]紙 [〇]その他（国税連携システム（eLTAX）、地方税外部連携システム（eLTAX））	事前	実態に合わせ修正
令和7年5月7日	Ⅱ特定個人情報ファイルの概要① 6. 特定個人情報の保管・消去 ①保管場所	【税務総合支援システム】 ・データセンタ及び運用拠点が都市計画区域にある場合は、都市計画法における防火・準防火地域に指定されている地域を選定する。または、周辺で火災が発生しても延焼の恐れがない場所とする。停電時に、システム機器を運用するために十分な電源容量を持つ非常用自家発電設備を設置する。 ・データセンタ及び運用拠点への入退館は、24時間365日体制で監視及び管理する。また、常駐警備を配備し、データセンタ及び運用拠点への入退館には、無権限者の立入りが不可能なセキュリティ対策を講じる。データセンタのマシン室へ及び運用拠点のオペレーション室への入退室は、生体認証装置を採用し、不要な物品の持ち込みを防止するための対策も行う。 ・データセンタにおけるサーバースペースは、認証用ICカードを採用することで無権限者の立入りを不可能とし、またサーバースペース内及び出入口を監視する対策も行う。 【紙媒体】 ・文書等の取扱いに関する規定に基づき、施錠された書庫に保管している。 ・文書の預入れを行う場合の保管倉庫は、地盤が強固で、海抜が高く、河川、池沼、運河、ため池等に隣接せず、近隣に危険物貯蔵倉庫及び工場がなく、人口及び建築物の密集地域ではない場所に建設している。 ・上記保管倉庫は、専用保管庫として設計された耐震・耐火構造を備えた堅固な建築物であり、外部からの侵入を防ぐための人的及び施設的管理体制（警備員による警備、監視カメラ、警報装置、赤外線センサー等）を備え、入退室は権限のある者のみ可能とし、入退室の記録をとり、一定期間保管している。 【中間サーバー・プラットフォーム】 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。 【連携サーバー】 ・サーバー等を設置するための専用施設内に他のシステムとは分離した区画を設け、当該サーバー専用のラックに施錠して収容する。当該施設では、入退室者管理、区画ごとの施錠管理、監視カメラによる録画、有人監視等を実施する。 ・当該施設の煙感知装置、ガス系消火設備、耐震対応等により、火災や地震に起因する滅失等のリスクを低減する。 【外部記録媒体】 ・外部記録媒体は、施錠された保管庫に保管している。	【税務総合支援システム（サーバー）】 ・特定個人情報を保管するデータセンタは、都市計画法における防火・準防火地域に指定されていること、サーバ室等へ滞りなく電力を供給できる電源設備及び非常用自家発電設備を備えていること等の防災性を重視した条件により、選定している。 ・データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際してはICカード及び静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。 【紙媒体】 ・文書等の取扱いに関する規定に基づき、施錠された書庫に保管している。 ・文書の預入れを行う場合の保管倉庫は、地盤が強固で、海抜が高く、河川、池沼、運河、ため池等に隣接せず、近隣に危険物貯蔵倉庫及び工場がなく、人口及び建築物の密集地域ではない場所に建設している。 ・上記保管倉庫は、専用保管庫として設計された耐震・耐火構造を備えた堅固な建築物であり、外部からの侵入を防ぐための人的及び施設的管理体制（警備員による警備、監視カメラ、警報装置、赤外線センサー等）を備え、入退室は権限のある者のみ可能とし、入退室の記録をとり、一定期間保管している。 【中間サーバー・プラットフォーム】 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。 【外部記録媒体】 ・外部記録媒体は、施錠された保管庫に保管している。 【連携サーバー】 ・サーバー等を設置するための専用施設内に他のシステムとは分離した区画を設け、当該サーバー専用のラックに施錠して収容する。当該施設では、入退室者管理、区画ごとの施錠管理、監視カメラによる録画、有人監視等を実施する。 ・当該施設の煙感知装置、ガス系消火設備、耐震対応等により、火災や地震に起因する滅失等のリスクを低減する。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年5月7日	Ⅱ特定個人情報ファイルの概要① 6. 特定個人情報の保管・消去 ③消去方法	【AI-OCR】 ・OCR処理を施すためのスキャンデータはスキャナシャットダウン時に自動で削除される。 ・スキャナは他の電子機器同様、日々の業務終了時にはスキャナをシャットダウンしている。 ・共有フォルダ内の不使用となったデータは適宜職員及び利用管理者が削除を行っている。 【電子書庫】 ・データ登録時にデータ種類、属性等に応じて予め指定した保存期限を自動設定できること。また、保存期限を超過したデータの削除を自動的に実施できるようにしている。 【EUC】 ・データ蓄積期間は税務基幹の各マスタと同じ期間とし、完結処理でマスタから削除されるとEUCからも削除するようにしている。 【電子決裁】 ・文書管理規則に則り、文書廃棄を行っている。 【外部連携基盤】 ・保管期間を超過した過去ファイルについては、定期的に自動で削除している。 ・課税から収入までの一連のサイクルを完了した課税データについて、電子データの削除等に関する規定に基づき、バッチ処理により削除している。 ・外部記録媒体については、データ授受後、直ちに保存データを削除することとしている。	【紙媒体】 廃棄等に関する規定に基づき、保存期間経過後、職員の立会いのもとで溶解等により廃棄を行っている。運搬・廃棄にあたっては、委託先から適切に処理する旨の誓約書を徴取している。また、廃棄後にすべての書類等を廃棄したことを示す溶解証明を徴取している。 【中間サーバー・プラットフォーム】 ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの保守・運用を行う事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度（ISMAP）に準拠したデータの暗号化消去及び物理的破壊を行う。さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ③中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。 【連携サーバー】 特定個人情報（副本相当）は、提供・移転の都度、中継されるのみであり、税務総合支援システムの取得後に消去し、且つ一定期間内に自動で消去する。 なお、機器のうち特定個人情報等のデータが記録されうるものの廃棄等に当たっては、磁気的消去又は物理的破壊等により、当該データを復元不可能な状態とする。 【税務総合支援システム（サーバー）】 一定期間経過後、バッチ処理により削除する。 また、機器リース期間満了時には特定個人情報等のデータを全て消去の上、消去結果について、記録媒体ごとに、消去した情報項目、数量、消去方法及び消去日等を明示した書面で委託事業者より報告を受けている。 【外部記録媒体】 ・データ授受後、直ちに保存データを削除することとしている。	事前	実態に合わせ修正
令和7年5月7日	Ⅱファイルの概要⑤		⑤地方税外部連携ファイル（仮称）について新設で記載。	事前	実態に合わせ修正
令和7年5月7日	Ⅲ リスク対策① 6. リスク1	【税務総合支援システム】 ・個人事業税、自動車税、固定資産税の減免に関係する者のみにアクセス権限を付与する。 ・情報提供ネットワークにより障害者関係情報及び生活保護関係情報を取得する際は、対象者について照会ファイル作成のためのシステム登録を行う。なお、照会ファイル作成は、登録された内容に問題がないかを内部承認にて確認した上で行う。	【税務総合支援システム】 ・個人事業税、自動車税、固定資産税の減免に関係する者のみにアクセス権限を付与する。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年5月7日	Ⅲ リスク対策① 6. リスク3	【税務総合支援システム】 ・税務総合支援システムは、情報提供ネットワークシステム・中間サーバー・連携サーバーを使用して、団体内統合利用番号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。 ・障害者関係情報及び生活保護関係情報を取得後、システムの画面及び帳票によって照会結果の確認を行う。	【税務総合支援システム】 ・税務総合支援システムは、情報提供ネットワークシステム・中間サーバー・連携サーバーを使用して、団体内統合利用番号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。	事前	実態に合わせ修正
令和7年5月7日	Ⅲ リスク対策① 6. リスク4	【中間サーバー・プラットフォーム】 ①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、漏えい・紛失のリスクに対応している。 ②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。 ③中間サーバー・プラットフォーム事業者の業務は、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】 ①中間サーバー、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、漏えい・紛失のリスクに対応している。 ②中間サーバ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。 ③中間サーバー・プラットフォーム事業者の業務は、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	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年5月7日	Ⅲ リスク対策① 7. リスク1 ⑤物理的対策	①都市計画区域にある場合は、都市計画法における防火・準防火地域に指定されている地域を選定する。または、周辺で火災が発生しても延焼の恐れがない場所とする。停電時に、システム機器を運用するために十分な電源容量を持つ非常用自家発電設備を設置する。 ②データセンタへの入退館は、24時間365日体制で監視及び管理する。また、常駐警備を配備し、データセンタへの入退館には、無権限者の立入りが不可能なセキュリティ対策を講じる。マシン室への入退室は、生体認証装置を採用し、不要な物品の持ち込みを防止するための対策も行う。 ③税務総合支援システムと外部システム間のデータ連携は委託業者の運用作業場所である、システム運用拠点（以下「運用拠点」と言う。）で専用の外部記録媒体を使用して行っている。なお、運用拠点への入室はデータセンタ同様静脈認証が必要である。	【紙媒体】 ・文書等の取扱いに関する規定に基づき、施錠された書庫に保管している。 ・文書の預入れを行う場合の保管倉庫は、地盤が強固で、海抜が高く、河川、池沼、運河、ため池等に隣接せず、近隣に危険物貯蔵倉庫及び工場がなく、人口及び建築物の密集地域ではない場所に建設している。 ・上記保管倉庫は、専用保管庫として設計された耐震・耐火構造を備えた堅固な建築物であり、外部からの侵入を防ぐための人的及び施設的管理体制（警備員による警備、監視カメラ、警報装置、赤外線センサー等）を備え、入退室は権限のある者のみ可能とし、入退室の記録をとり、一定期間保管している。 【税務総合支援システム（サーバー）】 ・特定個人情報を保管するデータセンタは、都市計画法における防火・準防火地域に指定されていること、サーバ室等へ滞りなく電力を供給できる電源設備及び非常用自家発電設備を備えていること等の防災性を重視した条件により、選定している。 ・データセンタは監視カメラ及び有人による監視を行っているとともに、入室に際してはICカード及び静脈認証を必要とし、持ち込む媒体・機器を制限する等、厳重なセキュリティ対策を行っている。 【中間サーバー・プラットフォーム】 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。 【連携サーバー】 ・サーバー等を設置するための専用施設内に他のシステムとは分離した区画を設け、当該サーバー専用のラックに施錠して収容する。当該施設では、入退室者管理、区画ごとの施錠管理、監視カメラによる録画、有人監視等を実施する。 ・当該施設の煙感知装置、ガス系消火設備、耐震対応等により、火災や地震に起因する滅失等のリスクを低減する。 ・機器のうち、特定個人情報等のデータが記録されうるものの廃棄等に当たっては、磁気的消去又は物理的破壊等により、当該データを復元不可能な状態とする。 【外部記録媒体】 外部記録媒体については施錠したケースに格納し、引渡しの際にはデータ引渡し兼受領書を用いて行っている。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年5月7日	Ⅲ リスク対策① 7. リスク1 ⑥技術的対策	①税務総合支援システム末での外部記録媒体の使用を制限し、予期しないデータの取込み及び持出しができないようにしている。また、データベースは税務総合支援システム端末以外から閲覧できないようにしている。 ②サーバー、端末等の機器にはウイルス対策ソフトを適用するとともに、パターンファイルの更新を一日毎に行うことにより、ウイルス感染を防止している。さらに、住民情報等の流出防止を目的に総務省が提示している三層分離の観点から、税務総合支援システムの外部ネットワーク接続は個人番号利用事務系のみに制限している。	【税務総合支援システム（サーバー）】 ①税務総合支援システム端末での外部記録媒体の使用を制限し、予期しないデータの取込み及び持出しができないようにしている。また、データベースは税務総合支援システム端末以外から閲覧できないようにしている。 ②サーバー、端末等の機器にはウイルス対策ソフトを適用するとともに、パターンファイルの更新を定期的に行うことにより、ウイルス感染を防止している。さらに、住民情報等の流出防止を目的に総務省が提示している三層分離の観点から、税務総合支援システムの外部ネットワーク接続は個人番号利用事務系のみに制限している。 ③税務総合支援システムと外部システム間のデータ連携は委託業者の運用作業場所である、システム運用拠点（以下「運用拠点」と言う。）で専用の外部記録媒体を使用して行っている。なお、運用拠点への入室はデータセンタ同様生体認証が必要である。 ④特定通信として税務総合支援システムに接続している電子申告、国税連携システムに係るネットワークについては、ファイアウォールを運用するとともに、接続状況を監視することにより、不正接続への対策を行っている。 【中間サーバー・プラットフォーム】 ①中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ②中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ④中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤中間サーバーのデータベースに保存される特定個人情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ⑥中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ⑦中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。 【連携サーバー】 ・サーバーが接続されたセグメントとそれ以外のセグメントの境界にファイアウォールを導入するとともに、ログを取得する。 ・ウイルス対策ソフトを導入し、パターンファイルを更新する。 ・基本ソフトウェア（OS）及びミドルウェアは、必要に応じてセキュリティパッチを適用する。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年5月7日	Ⅳ1. ②監査 具体的な内容	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。 1. 内部監査 以下の観点で内部監査人による特定個人情報保護監査を所属ごとに3年に1回実施している。 ・自己点検結果の確認 ・情報資産台帳・情報処理機器等の保有状況簿の確認 ・情報資産の保管・持ち出し等に係る帳票等の確認 ・執務室の視察 2. 外部監査 以下の観点で、税務総合支援システム等を対象とした外部監査人による監査を2年に一度実施している。 ・サーバー機器等に対する脆弱性診断 ・セキュリティポリシー遵守や運用管理体制に関するヒアリング 3. その他 国税連携システム（eLTAX）については、サイバーセキュリティ監査（外部監査）を実施している。 また、地方税法ポータルセンタ（eLTAX）については、運営する地方税共同機構が、毎年度、情報セキュリティ監査（外部監査）を受けている。	運用規則等に基づき、税務総合支援システムについて、定期的に監査を行うこととしている。 1. 内部監査 以下の観点で内部監査人による特定個人情報保護監査を所属ごとに3年に1回実施している。 ・自己点検結果の確認 ・情報資産台帳・情報処理機器等の保有状況簿の確認 ・情報資産の保管・持ち出し等に係る帳票等の確認 ・執務室の視察 2. 外部監査 以下の観点で、税務総合支援システム等を対象とした外部監査人による監査を2年に一度実施している。 ・サーバー機器等に対する脆弱性診断 ・セキュリティポリシー遵守や運用管理体制に関するヒアリング 3. その他 ・国税連携システム（eLTAX）については、サイバーセキュリティ監査（外部監査）を実施している。 ・地方税法ポータルセンタ（eLTAX）については、運営する地方税共同機構が、毎年度、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ついては、運用規則等に基づき、定期的に監査を行うこととしている。また、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者は、定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。	事前	実態に合わせ修正
令和7年5月7日	Ⅳ3.		【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。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年6月2日	Ⅰ 2. システム3 ②システムの機能	・所得税申告書等データの受領 ・他道府県への所得税申告書等データの送付 ・所得税申告書等データの保存 ・媒体による外部へのデータ出力 ・所得税申告書等データの閲覧、印刷	・所得税申告書等データの受領 ・他道府県への所得税申告書等データの送付 ・所得税申告書等データの保存 ・媒体による外部へのデータ出力 ・所得税申告書等データの閲覧、印刷 ・国税及び地方税間の照会・回答	事前	実態に合わせ修正
令和7年6月2日	Ⅰ 2. システム8 ②システムの機能	・所得税申告書等データの取り込み ・所得税申告書等データの保存（7年分） ・所得税申告書等データの閲覧、印刷 （国税連携システムでの保存可能容量が最大2年分のため、容量を超えた年分を参照する目的として使用）	・所得税申告書等データの取り込み ・所得税申告書等データの保存（7年分） ・所得税申告書等データの閲覧、印刷 （国税連携システムでの保存可能容量が最大1年分のため、容量を超えた年分を参照する目的として使用）	事前	実態に合わせ修正
令和7年6月2日	Ⅱ ファイルの概要① 2. ④記録される項目 その妥当性	・個人番号：納税義務者情報を正確に管理するために保有 ・個人番号対応符号：対象者を正確に特定するために保有 ・その他識別情報：対象者を正確に特定するために保有 ・4情報及び連絡先：納税義務者を特定するため、連絡するために保有 ・その他住民票関係情報：納税義務者情報を正確に把握するために保有 ・地方税関係情報：都税の賦課徴収を行うために保有 ・国税関係情報：税額決定に際し所得額等を用いて確認するために保有 ・障害者福祉関係情報、生活保護・社会福祉関係情報：賦課事務を適切に行うために保有	・個人番号：納税義務者情報を正確に管理するために保有 ・個人番号対応符号：対象者を正確に特定するために保有 ・その他識別情報：対象者を正確に特定するために保有 ・5情報及び連絡先：納税義務者を特定するため、連絡するために保有 ・その他住民票関係情報：納税義務者情報を正確に把握するために保有 ・地方税関係情報：都税の賦課徴収を行うため、他道府県との情報連携のため、還付金額清算のために保有 ・国税関係情報：税額決定に際し所得額等を用いて確認するため、還付金額清算のために保有 ・障害者福祉関係情報、生活保護・社会福祉関係情報：賦課事務を適切に行うために保有 ・公的給付支給等口座登録簿関係情報：還付事務を適切行うために保有	事前	実態に合わせ修正
令和7年6月2日	Ⅱ ファイルの概要② 2. ④記録される項目 その妥当性	・個人番号及びその他の識別情報：対象者を正確に特定するために保有 ・4情報及び連絡先：①課税対象者の認定に際し在住要件を確認するため、②本人への通知等送付及び連絡等のために保有 ・国税関係情報：租税の賦課及び国税との情報連携のために保有 ・地方税関係情報：租税の賦課及び他道府県との情報連携のために保有	・個人番号及びその他の識別情報：対象者を正確に特定するために保有 ・5情報及び連絡先：①課税対象者の認定に際し在住要件を確認するため、②本人への通知等送付及び連絡等のために保有 ・国税関係情報：租税の賦課徴収及び国税との情報連携のために保有 ・地方税関係情報：租税の賦課徴収及び他道府県との情報連携のために保有	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年6月2日	Ⅱ ファイルの概要② 4. ④委託先への特定個人情報ファイルの提供方法	[〇]専用線	[〇]専用線 [〇]電子記録媒体(フラッシュメモリを除く。)	事前	実態に合わせ修正
令和7年6月2日	Ⅱ ファイルの概要③ 2. ④記録される項目 その妥当性	・個人番号及びその他の識別情報:対象者を正確に特定するために保有 ・4情報及び連絡先等情報:①課税台帳の台帳記載事項として登録するため、②納税通知書等を送達するため、③本人への連絡等のため、保有する。 ・業務関連情報:租税の賦課を行うために保有する。	・個人番号及びその他の識別情報:対象者を正確に特定するために保有 ・5情報及び連絡先等情報:①課税台帳の台帳記載事項として登録するため、②納税通知書等を送達するため、③本人への連絡等のため、保有する。 ・業務関連情報:租税の賦課を行うために保有する。	事前	実態に合わせ修正
令和7年6月2日	Ⅲ リスク対策① 6. リスク2	【中間サーバー・ソフトウェア】 ①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システムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 【中間サーバー・プラットフォーム】 ①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。 ②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。 【連携サーバー】 ・システムの利用可能な時間を制限している。 ・情報連携に用いる端末に対し、端末認証を行う。 ・ログイン時に利用者の認証を実施する。 ・個別業務システム(事務)との間は、庁内のネットワークを介するとともに、暗号化を行う。 ・連携サーバーから個別業務システム(事務)に提供する照会結果ファイルは、暗号化を行う。 ・中間サーバーとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。 ・サーバー認証により真正性が担保された中間サーバーに接続する。 【税務総合支援システム】 ・連携サーバーに登録する照会ファイルを暗号化する。 ・連携サーバーに登録する照会ファイル及び取得する照会結果ファイルは、システム処理を前提にアクセス制限されたフォルダに格納するため、外部に持ち出すことはない。 ・上記の作業は、情報連携ファイルを管理する職員のみが行う。なお、情報連携ファイルを持ち出す際は事前に許可申請書による内部認証を経るとともに、作業後には報告書を提出している。	【中間サーバー・ソフトウェア】 ①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システムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 【中間サーバー・プラットフォーム】 ①中間サーバー、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、安全性を確保している。 ②中間サーバ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。 【連携サーバー】 ・システムの利用可能な時間を制限している。 ・情報連携に用いる端末に対し、端末認証を行う。 ・ログイン時に利用者の認証を実施する。 ・個別業務システム(事務)との間は、庁内のネットワークを介するとともに、暗号化を行う。 ・連携サーバーから個別業務システム(事務)に提供する照会結果ファイルは、暗号化を行う。 ・中間サーバーとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。 ・サーバー認証により真正性が担保された中間サーバーに接続する。 【税務総合支援システム】 ・連携サーバーに登録する照会ファイルを暗号化する。 ・連携サーバーに登録する照会ファイル及び取得する照会結果ファイルは、システム処理を前提にアクセス制限されたフォルダに格納するため、外部に持ち出すことはない。 ・上記の作業は、情報連携ファイルを管理する職員のみが行う。なお、情報連携ファイルを持ち出す際は事前に許可申請書による内部認証を経るとともに、作業後には報告書を提出している。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年6月2日	Ⅲ　リスク対策① 6. 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】 ①中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 【中間サーバー･プラットフォーム】 ①中間サーバーと既存時ステム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバ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。 ③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。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・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。 【連携サーバー】 連携サーバーと接続する端末に対し端末認証を行い、権限のない職員がアクセスできないようになっている。	【中間サーバー・ソフトウェア】 ①中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 【中間サーバー･プラットフォーム】 ①中間サーバー、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバ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。 ③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。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・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。 【連携サーバー】 連携サーバーと接続する端末に対し端末認証を行い、権限のない職員がアクセスできないようになっている。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年6月16日	Ⅱ ファイルの概要 ① 3. 特定個人情報の入手・使用 ③入手の時期・頻度	【情報連携】 ・納税義務者からの個人事業税、自動車税、固定資産税の減免申請があり、適用要件の確認に情報連携を要する都度、入手する。 ・過誤納金が発生し、還付口座未登録の納税者からの公金受取口座への還付の請求があった都度、て入手する。	【情報連携】 ＜身体・精神障害者手帳及び障害の程度に関する情報、生活保護実施関係情報、公的給付支給等口座登録簿関係情報＞ ・納税義務者からの個人事業税、自動車税、固定資産税の減免申請があり、適用要件の確認に情報連携を要する都度、情報提供ネットワークシステムを使用して入手する。 ・過誤納金が発生し、還付口座未登録の納税者からの公金受取口座への還付の請求があった都度、情報提供ネットワークシステムを使用して入手する。	事前	実態に合わせ修正
令和7年6月16日	Ⅱ ファイルの概要 ① 3. 特定個人情報の入手・使用 ④入手に係る妥当性	【情報連携】 ・番号法第19条第8項に基づき、地方税の賦課徴収事務において認められた情報について、情報連携ネットワークシステムを通じて入手できる。東京都においては、自動車税の減免・固定資産税の減免・個人事業税の減免事務、公金受取口座への還付事務が対象となっている。	【情報連携】 ＜身体・精神障害者手帳及び障害の程度に関する情報、生活保護実施関係情報、公的給付支給等口座登録簿関係情報＞ ・番号法第19条第8項に基づき、地方税の賦課徴収事務において認められた情報について、情報連携ネットワークシステムを通じて入手できる。東京都においては、自動車税の減免・固定資産税の減免・個人事業税の減免事務、公金受取口座への還付事務が対象となっている。	事前	実態に合わせ修正
令和7年6月16日	Ⅱ ファイルの概要 ① 3. 特定個人情報の入手・使用 ⑤本人への明示	【情報連携】 ・地方税法第17条、第72条の62、第128条、第162条、第367条、東京都都税条例第39条の7、第83条、第103条、第134条及び番号法第19条第8号に特定個人情報を入手することが明示されている。	【情報連携】 ＜身体・精神障害者手帳及び障害の程度に関する情報、生活保護実施関係情報、公的給付支給等口座登録簿関係情報＞ ・地方税法第17条、第72条の62、第128条、第162条、第367条、東京都都税条例第39条の7、第83条、第103条、第134条及び番号法第19条第8号に特定個人情報を入手することが明示されている。	事前	実態に合わせ修正
令和7年6月16日	Ⅱ ファイルの概要 ① 3. 特定個人情報の入手・使用 ⑤使用方法	【情報連携】 ・身体・精神障害者手帳及び障害の程度に関する情報、生活保護実施関係情報を入手し、減免適用の可否を確認する。 ・公金受取口座への還付請求を行った申請者の公金受取口座情報を確認する。	【情報連携】 ＜身体・精神障害者手帳及び障害の程度に関する情報、生活保護実施関係情報、公的給付支給等口座登録簿関係情報＞ ・身体・精神障害者手帳及び障害の程度に関する情報、生活保護実施関係情報を入手し、減免適用の可否を確認する。 ・公金受取口座への還付請求を行った申請者の公金受取口座情報を確認する。	事前	実態に合わせ修正
令和7年6月16日	Ⅱ ファイルの概要 ① 3. 特定個人情報の入手・使用 ⑤使用方法 情報の突合	【情報連携】 入手した身体・精神障害者手帳及び障害の程度に関する情報、生活保護実施関係情報と減免申請書を突合する。	【情報連携】 ＜身体・精神障害者手帳及び障害の程度に関する情報、生活保護実施関係情報＞ 入手した身体・精神障害者手帳及び障害の程度に関する情報、生活保護実施関係情報と減免申請書を突合する。	事前	実態に合わせ修正
令和7年6月16日	Ⅱ ファイルの概要 ① 6. 特定個人情報の保管・消去 ③消去方法	【外部記録媒体】 ・データ授受後、直ちに保存データを削除することとしている。	【外部記録媒体】 ・データ授受後、直ちに保存データを削除することとしている。 ・保管している外部記録媒体が不要となった場合は、当該外部記録媒体内部の情報を復元できないように消去した上で廃棄する。	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年6月16日	Ⅱ ファイルの概要 ③ 6. 特定個人情報の保管・消去 ③消去方法	【外部記録媒体】 ・税務総合支援システムと審査システム（eLTAX）の間のデータ授受に使用する外部記録媒体（ハードディスク）については、一定の保存期間の経過後、委託先が手作業でデータを消去している。 ・同目的に使用するUSBフラッシュメモリについては、データ移行後直ちに、職員が手作業でデータを消去している。	【外部記録媒体】 ・税務総合支援システムと審査システム（eLTAX）の間のデータ授受に使用する外部記録媒体（ハードディスク）については、一定の保存期間の経過後、委託先が手作業でデータを消去している。 ・同目的に使用するUSBフラッシュメモリについては、データ移行後直ちに、職員が手作業でデータを消去している。 ・保管している外部記録媒体が不要となった場合は、当該外部記録媒体内部の情報を復元できないように消去した上で廃棄する。	事前	実態に合わせ修正
令和7年6月16日	Ⅳ リスク対策（その他） 1. 監査 ②監査　具体的な内容	運用規則等に基づき、税務総合支援システ等について、定期的に監査を行うこととしている。 1. 内部監査 以下の観点で内部監査人による特定個人情報保護監査を所属ごとに3年に1回実施している。 ・自己点検結果の確認 ・情報資産台帳・情報処理機器等の保有状況簿の確認 ・情報資産の保管・持ち出し等に係る帳票等の確認 ・執務室の視察 2. 外部監査 以下の観点で、税務総合支援システム等を対象とした外部監査人による監査を2年に1回実施している。 ・サーバー機器等に対する脆弱性診断 ・セキュリティポリシー遵守や運用管理体制に関するヒアリング	運用規則等に基づき、税務総合支援システム等について、定期的に監査を行うこととしている。 1. 内部監査 以下の観点で内部監査人による特定個人情報保護監査を所属ごとに3年に1回実施している。 ・自己点検結果の確認 ・情報資産台帳・情報処理機器等の保有状況簿の確認 ・情報資産の保管・持ち出し等に係る帳票等の確認 ・執務室の視察 2. 外部監査 以下の観点で、税務総合支援システム等を対象とした外部監査人による監査を定期的に実施している。 ・サーバー機器等に対する脆弱性診断 ・セキュリティポリシー遵守や運用管理体制に関するヒアリング	事前	実態に合わせ修正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年6月16日	Ⅳ リスク対策（その他） 2. 従業者に対する教育・啓発 従業者に対する教育・啓発 具体的な方法	【税務総合支援システム】 ・全職員を対象にサイバーセキュリティ・個人情報保護の研修を実施している。研修の目的は、個人情報保護の重要性及び適正管理等に関する理解を深め、個人情報保護の遵守を徹底することである。具体的には、以下の研修を実施している。 ・毎年の悉皆研修 ・個人端末からアクセスするeラーニング研修（理解度が基準に達しないと修了できない） なお、未受講者については、翌年度同様の研修を受講させている。また、eラーニングについては、システムにより受講管理を実施し、未受講者に受講を促すことで、未受講者が出ないようにしている。	【税務総合支援システム】 ・全職員を対象にサイバーセキュリティ・個人情報保護の研修を実施している。研修の目的は、個人情報保護の重要性及び適正管理等に関する理解を深め、個人情報保護の遵守を徹底することである。具体的には、以下の研修を実施している。 ・毎年の悉皆研修 ・個人端末からアクセスするeラーニング研修（理解度が基準に達しないと修了できない） なお、未受講者については、翌年度同様の研修を受講させている。また、eラーニングについては、システムにより受講管理を実施し、未受講者に受講を促すことで、未受講者が出ないようにしている。 ・委託業務の従事者に対し、個人情報及び機密情報の取扱いについて必要な教育及び研修を実 施させている。 【税務総合支援システム（サーバー）】 ・データセンタにおける緊急時対応を想定した訓練を毎年度実施している	事前	実態に合わせ修正