

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
13	地方税の賦課事務(情報連携) 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、地方税の賦課事務(情報連携)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切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

項目一覧

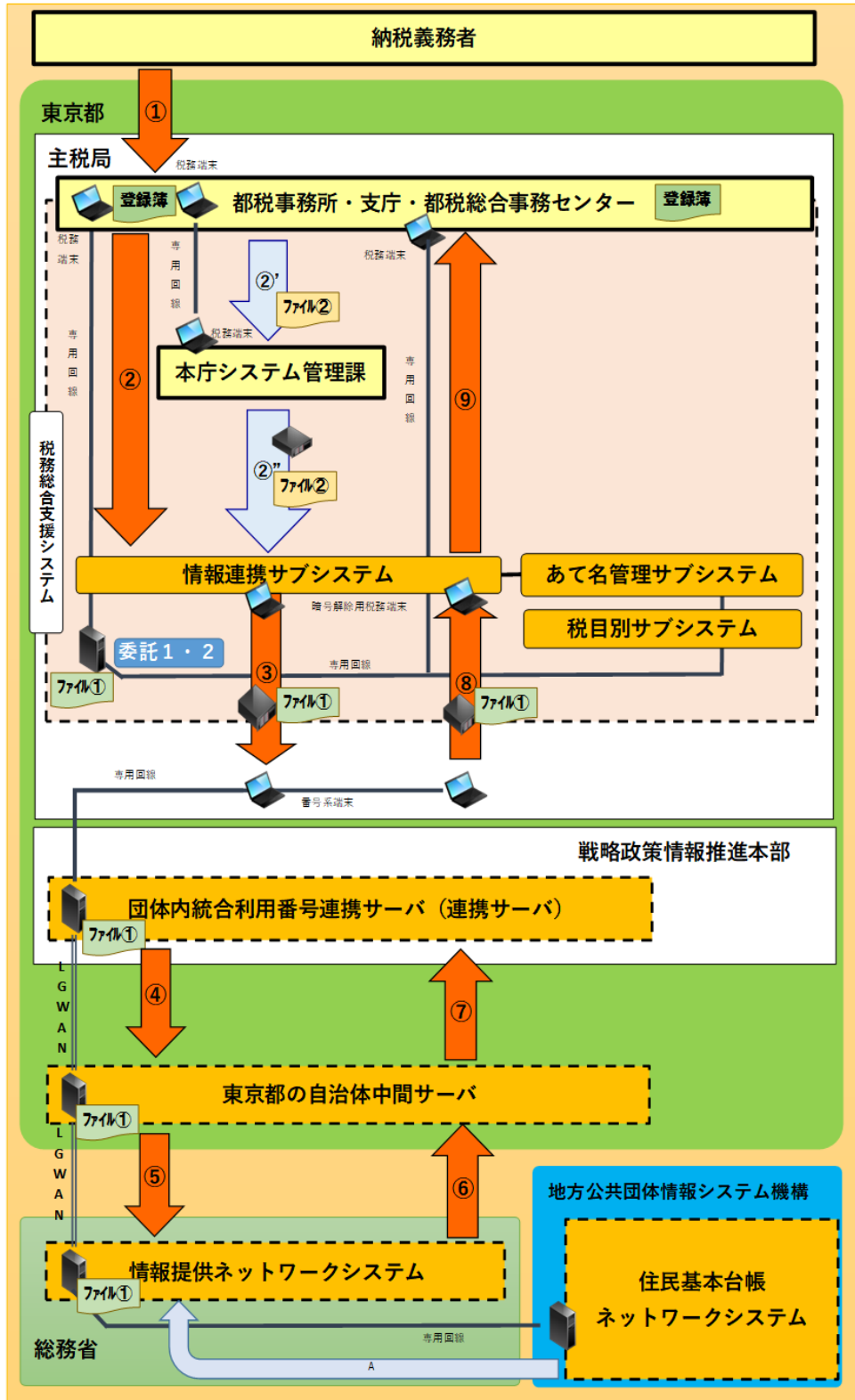
I 基本情報
(別添1) 事務の内容
II 特定個人情報ファイルの概要
(別添2) 特定個人情報ファイル記録項目
III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策
IV その他のリスク対策
V 開示請求、問合せ
VI 評価実施手続
(別添3) 変更箇所

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	地方税の賦課事務(情報連携)
②事務の内容 ※	<ul style="list-style-type: none"> ・「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(以下「番号法」)第19条第7号に基づき、情報提供ネットワークシステムを使用して減免決定に必要な特定個人情報を照会し、提供を受ける。 ・提供を受ける特定個人情報は下記の通り。 <ul style="list-style-type: none"> ① 身体・精神障害者手帳及び障害の程度に関する情報 ② 生活保護実施関係情報
③対象人数	<div style="display: flex; align-items: center;"> <div style="margin-right: 20px;">[10万人以上30万人未満]</div> <div style="text-align: center;"> <p><選択肢></p> <p>1) 1,000人未満</p> <p>2) 1,000人以上1万人未満</p> <p>3) 1万人以上10万人未満</p> <p>4) 10万人以上30万人未満</p> <p>5) 30万人以上</p> </div> </div>
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	<ul style="list-style-type: none"> ・オンライン入力 ・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り込み ・外部へのデータ出力 ・電子帳票機能
③他のシステムとの接続	<div style="display: flex; flex-wrap: wrap;"> <div style="width: 50%;">[] 情報提供ネットワークシステム</div> <div style="width: 50%;">[] 庁内連携システム</div> <div style="width: 50%;">[] 住民基本台帳ネットワークシステム</div> <div style="width: 50%;">[] 既存住民基本台帳システム</div> <div style="width: 50%;">[] 宛名システム等</div> <div style="width: 50%;">[] 税務システム</div> <div style="width: 100%;">[] その他 ()</div> </div>
システム2～5	
システム2	
①システムの名称	団体内統合利用番号連携サーバー(以下、「連携サーバー」とする。)
②システムの機能	<ul style="list-style-type: none"> ・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
③他のシステムとの接続	<div style="display: flex; flex-wrap: wrap;"> <div style="width: 50%;">[] 情報提供ネットワークシステム</div> <div style="width: 50%;">[] 庁内連携システム</div> <div style="width: 50%;">[] 住民基本台帳ネットワークシステム</div> <div style="width: 50%;">[] 既存住民基本台帳システム</div> <div style="width: 50%;">[] 宛名システム等</div> <div style="width: 50%;">[] 税務システム</div> <div style="width: 100%;">[○] その他 (中間サーバー)</div> </div>
システム3	
①システムの名称	中間サーバー
②システムの機能	<ul style="list-style-type: none"> ・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	<input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> 庁内連携システム <input type="checkbox"/> 住民基本台帳ネットワークシステム <input type="checkbox"/> 既存住民基本台帳システム <input type="checkbox"/> 宛名システム等 <input type="checkbox"/> 税務システム <input type="checkbox"/> その他（連携サーバー）
システム6～10	
システム11～15	
システム16～20	
3. 特定個人情報ファイル名	
情報連携ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	賦課事務を適切に行うために、最新かつ正確な障害者関係情報、生活保護関係情報を把握する必要がある。
②実現が期待されるメリット	より正確な賦課事務を行うことができるとともに、納税者からの添付書類の提出を削減できる。
5. 個人番号の利用 ※	
法令上の根拠	番号法第9条第1項 別表第1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等に関する法律別表第一の主務省令で定める事務を定める命令第16条
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	<input type="checkbox"/> 実施する <input type="checkbox"/> 実施しない <input type="checkbox"/> 未定 <small><選択肢> 1) 実施する 2) 実施しない 3) 未定</small>
②法令上の根拠	・番号法第19条第7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
7. 評価実施機関における担当部署	
①部署	東京都主税局税制部システム管理課
②所属長の役職名	システム管理課長
8. 他の評価実施機関	
-	

(別添1) 事務の内容



【凡例】



：特定個人情報の流れ



：税務端末、番号系端末、
暗号解除用税務端末



：特定個人個人情報以外
の情報の流れ



：ファイルサーバ

委託 1

：税務総合支援システム
維持管理委託



：外部記録媒体

委託 2

：税務総合支援システム
運用業務委託

ファイル①

：照会・照会結果ファイル（特定個人情報含む）

ファイル②

：一括登録ファイル（特定個人情報なし）

登録簿

：情報照会依頼登録簿（特定個人情報含む）

（備考）

① 納税義務者から減免申請書を受領。

※地方税の賦課事務（個人事業税・自動車税・固定資産税のみ対象）

② 減免申請者について登録簿を作成し、内容に関し内部承認を得たうえで、「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7号に基づき、減免申請者に係る特定個人情報を税務総合支援システムの情報連携サブシステムへ登録。

②' 減免申請者について登録簿を作成し、内容に関し内部承認を得たうえで、「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7号に基づき、減免申請者に係る個人情報（特定個人情報を除く）を情報連携サブシステムに一括登録するための一括登録依頼ファイルを作成し、税務総合支援システムの内部メールを使用して、システム管理課に送付する。

②'' ②' で送付された一括登録ファイルを、外部記録媒体を用いてバッチ処理を行う環境に移行する。移行後、バッチ処理で情報連携サブシステムへデータを登録するが、データ元となる一括登録ファイルには特定個人情報が含まれていないので、あて名管理サブシステムや情報連携サブシステムに登録済みの特定個人情報を使用して登録を行う。

③ ②及び②'' で登録された対象者について暗号解除用税務端末、外部記憶媒体及び番号系端末経由で団体内統合利用番号連携サーバ（以下「連携サーバ」という）に登録。

④ 【他団体への照会の場合】

自治体中間サーバへ情報提供ネットワーク経由の情報照会依頼を登録。

【庁内連携の場合】

自治体中間サーバへ自団体保有情報を照会。

⑤ 情報提供ネットワークシステムを経由して特定個人情報を照会。

⑥ 情報提供ネットワークシステムを経由して特定個人情報を入手。

⑦ 【他団体への照会の場合】

⑥で提供された特定個人情報を、自治体中間サーバ経由で入手。

【庁内連携の場合】

自治体中間サーバから自団体保有情報を入手。

⑧ ⑦で提供された特定個人情報を暗号解除用税務端末外部記憶媒体、外部記憶媒体及び番号系端末経由で情報連携システムへ登録。

⑨ ⑧で提供された特定個人情報（照会結果）を参照し、登録簿に照会結果（回答の有無）を記録する。

A 団体ごとに異なる機関別符号を紐づけする連携用符号を作成するために使用する住民票コードが、住民基本台帳システムから情報連携ネットワークシステムへ提供される。

II 特定個人情報ファイルの概要

1. 特定個人情報ファイル名	
情報連携ファイル	
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	[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 ※	個人事業税、自動車税、固定資産税の減免に係る者
その必要性	課税事務を適切に行うため
④記録される項目	[100項目以上] <選択肢> 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
主な記録項目 ※	<ul style="list-style-type: none"> ・識別情報 [<input type="checkbox"/>] 個人番号 [] 個人番号対応符号 [<input type="checkbox"/>] その他識別情報(内部番号) ・連絡先等情報 [<input type="checkbox"/>] 4情報(氏名、性別、生年月日、住所) [] 連絡先(電話番号等) [] その他住民票関係情報 ・業務関係情報 [] 国税関係情報 [] 地方税関係情報 [] 健康・医療関係情報 [] 医療保険関係情報 [] 児童福祉・子育て関係情報 [<input type="checkbox"/>] 障害者福祉関係情報 [<input type="checkbox"/>] 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	<ul style="list-style-type: none"> ・個人番号: 情報連携に関する情報を正確に管理するために保有 ・その他識別情報、4情報: 個人番号に係る共通基盤(連携サーバー)と適切に連携するために保有 ・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
全ての記録項目	別添2を参照。
⑤保有開始日	平成29年7月1日
⑥事務担当部署	東京都主税局税制部システム管理課

3. 特定個人情報の入手・使用		
①入手元 ※	<input type="checkbox"/> 本人又は本人の代理人 <input type="checkbox"/> 評価実施機関内の他部署 (福祉保健局) <input type="checkbox"/> 行政機関・独立行政法人等 () <input type="checkbox"/> 地方公共団体・地方独立行政法人 (道府県、区市町村) <input type="checkbox"/> 民間事業者 () <input type="checkbox"/> その他 ()	
②入手方法	<input type="checkbox"/> 紙 [] 電子記録媒体(フラッシュメモリを除く。) [<input type="checkbox"/>] フラッシュメモリ <input type="checkbox"/> 電子メール [] 専用線 [<input type="checkbox"/>] 庁内連携システム <input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> その他 ()	
③入手の時期・頻度	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の都度、入手する。	
④入手に係る妥当性	・減免申請書: 東京都都税条例に基づき納税義務者から入手する ・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: 番号法に基づき入手する。	
⑤本人への明示	地方税法第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7号に特定個人情報を入手することが明示されている。	
⑥使用目的 ※	必要な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を実現する。	
変更の妥当性	—	
⑦使用の主体	使用部署 ※	都税事務所・支庁・都税総合事務センター・主税局各部
	使用者数	<input type="checkbox"/> 500人以上1,000人未満] <ul style="list-style-type: none"> <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 ※	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。	
情報の突合 ※	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 ※	減免決定	
⑨使用開始日	平成29年7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 (2) 件
委託事項1	税務総合支援システム維持管理委託
①委託内容	税務システムおよび関連システムの仕様変更、障害対応等
②取扱いを委託する特定個人情報ファイルの範囲	[特定個人情報ファイルの全体] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
対象となる本人の数	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
対象となる本人の範囲 ※	個人事業税、自動車税、固定資産税の減免に係る者
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保護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	[100人以上500人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法	[<input checked="" type="checkbox"/>] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [] その他 ()
⑤委託先名の確認方法	ホームページ「東京都入札情報サービス」にて公表している
⑥委託先名	株式会社 日立製作所
再委託	
⑦再委託の有無 ※	[再委託する] <選択肢> 1) 再委託する 2) 再委託しない
⑧再委託の許諾方法	委託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	税務総合支援システムの仕様変更、障害対応等の一部
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(情報連携サーバを含む。)の稼働に必要な機能の提供
②取扱いを委託する特定個人情報ファイルの範囲	[特定個人情報ファイルの全体] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
対象となる本人の数	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上

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	<input type="checkbox"/> 提供を行っている () 件 <input type="checkbox"/> 移転を行っている () 件 <input type="checkbox"/> 行っていない	
6. 特定個人情報の保管・消去		
①保管場所 ※	<p>【中間サーバー・プラットフォーム】</p> <p>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。</p> <p>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。</p> <p>【連携サーバー】</p> <p>・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收容する。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。</p> <p>・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。</p> <p>【税務総合支援システム(サーバ)】</p> <p>・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。</p> <p>・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。</p>	
②保管期間	期間	<p style="text-align: center;">＜選択肢＞</p> <p style="text-align: center;">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</p>
	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	<p>【中間サーバー・プラットフォーム】</p> <p>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・運用を行う事業者が特定個人情報を消去することはない。</p> <p>②ディスク交換やハード更改等の際は、中間サーバー・プラットフォームの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。</p> <p>【連携サーバー】</p> <p>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、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。</p> <p>なお、機器のうち特定個人情報等のデータが記録されるものの廃棄等に当たっては、磁氣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。</p> <p>【税務総合支援システム(サーバ)】</p> <p>一定期間経過後、バッチ処理により削除する。</p>	
7. 備考		
—		

(別添2) 特定個人情報ファイル記録項目**1. 身体障害者手帳情報マスタ**

項番	項目名
1	対象者システム利用番号
2	照会連番
3	照会委任用連番
4	障害者手帳繰返番号
5	障害者手帳繰返内一連番号
6	照会結果中間サーバ受付番号
7	照会結果中間サーバ受付明細番号
8	照会結果ステータス
9	照会結果取止年月日
10	照会結果取止時間
11	照会結果取止事由コード
12	照会結果識別項目コード
13	照会結果確定時点
14	照会結果修正時点
15	照会結果未セット事由
16	照会結果連番
17	身体障害者手帳初回交付年月日
18	身体障害者手帳返還年月日
19	身体障害者手帳再交付年月日
20	身体障害者手帳番号
21	身体障害者手帳等級コード
22	身体障害者手帳障害名
23	身体障害者手帳障害程度コード
24	身体障害者手帳部位コード

2. 精神障害者手帳情報マスタ

項番	項目名
1	対象者システム利用番号
2	照会連番
3	照会委任用連番
4	障害者手帳繰返番号
5	障害者手帳繰返内一連番号
6	照会結果中間サーバ受付番号
7	照会結果中間サーバ受付明細番号
8	照会結果ステータス
9	照会結果取止年月日
10	照会結果取止時間
11	照会結果取止事由コード
12	照会結果識別項目コード
13	照会結果確定時点
14	照会結果修正時点
15	照会結果未セット事由
16	照会結果連番
17	精神障害者手帳番号
18	精神障害者手帳交付年月日
19	精神障害者手帳返還年月日
20	精神障害者手帳再交付年月日
21	精神障害者手帳等級コード
22	精神障害者手帳有効期間終了年月日

3. 生活保護情報マスタ

項番	項目名
1	対象者システム利用番号
2	照会連番
3	照会委任用連番
4	生活保護繰返番号
5	生活保護繰返内一連番号
6	照会結果中間サーバ受付番号
7	照会結果中間サーバ受付明細番号
8	照会結果ステータス
9	照会結果取止年月日
10	照会結果取止時間
11	照会結果取止事由コード
12	照会結果識別項目コード
13	照会結果確定時点
14	照会結果修正時点
15	照会結果未セット事由
16	照会結果連番
17	生活保護支給開始年月日
18	生活保護支給終了年月日
19	生活保護支給対象年月
20	生活保護生活扶助有無
21	生活保護住宅扶助有無
22	生活保護教育扶助有無
23	生活保護介護扶助有無
24	生活保護医療扶助有無
25	生活保護出産扶助有無
26	生活保護生業扶助有無
27	生活保護葬祭扶助有無
28	生活保護支給月額合計
29	生活保護一時扶助額

4. 番号連携対象者マスタ

項番	項目名
1	対象者システム利用番号
2	対象者履歴番号
3	対象者個人番号
4	対象者業務グループコード
5	対象者連携サーバ登録削除区分
6	対象者原典更新年月日
7	対象者団体内統合利用番号
8	対象者有効状態フラグ
9	対象者符号状態
10	対象者機関コード
11	対象者システム利用番号登録年月日
12	対象者システム利用番号登録時間
13	対象者符号登録年月日
14	対象者符号登録時間
15	対象者団体内統合利用番号取得状況
16	対象者符号取得状況
17	対象者変更前個人番号
18	対象者団体内統合利用番号取得状況2
19	対象者符号取得状況2
20	対象者漢字住所
21	対象者カナ氏名
22	対象者漢字氏名

※1身体障害者手帳情報マスタ及び2精神障害者手帳情報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	
情報連携ファイル	
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	<p>【減免申請者情報】 対象以外の情報を記載することが無いような書面様式をもとに入力している。</p> <p>【庁内連携】 (連携サーバー) 照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められ、かつ移転者が明示的に回答を承認した場合に限り、連携を行う。照会に対しては、照会条件として指定された対象者に関する情報だけを回答する。なお、チェック項目は、番号法等の改正に応じて、更新する。 (主税局) 庁内連携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、対象者について登録簿を作成し、内部承認を経たうえで、照会ファイル作成のためのシステム登録を行う。</p>
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	<p>【減免申請者情報】 必要な情報以外を誤って登録することが無いような画面形式としている。</p> <p>【庁内連携】 (連携サーバー) 連携サーバーシステムでは、照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められたものだけについて連携を行う。なお、チェック項目は、番号法等の改正に応じて、更新する。 (主税局) 庁内連携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、対象者に係る必要な情報について登録簿を作成し、内部承認を経たうえで、照会ファイル作成のためのシステム登録を行う。</p>
その他の措置の内容	—
リスクへの対策は十分か	<p>[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</p>
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	<p>【減免申請者情報】 必要な情報以外を誤って登録することが無いような画面形式としている。</p> <p>【庁内連携】 (連携サーバー) ・照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められ、かつ移転者が明示的に回答を承認した場合に限り、連携を行う。照会に対しては、照会条件として指定された対象者に関する情報だけを回答する。なお、チェック項目は、番号法等の改正に応じて、更新する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・全ての照会及び回答について、特定個人情報の照会者、移転者、日時等をシステム上でアクセスログとして記録し、7年間保存する。 (主税局) ・庁内連携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、対象者に係る必要な情報について登録簿を作成し、内部承認を経たうえで、照会ファイル作成のためのシステム登録を行う。 ・システム登録については、ID単位でアクセスログを取得する。 ・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、主税局執務室内において、媒体を経由して取り込みを行う。</p>
リスクへの対策は十分か	<p>[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</p>

リスク3: 入手した特定個人情報 that 不正確であるリスク	
入手の際の本人確認の措置の内容	<p>【減免申請者情報】 東京都主税局各事務所等で番号法の規定に基づく本人確認済み。</p> <p>【庁内連携】 (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。 (主税局) 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。</p>
個人番号の真正性確認の措置の内容	<p>【減免申請者情報】 東京都主税局各事務所等で番号法の規定に基づく真正性確認済み。</p> <p>【庁内連携】 (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。 (主税局) 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。</p>
特定個人情報の正確性確保の措置の内容	<p>【減免申請者情報】 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。</p> <p>【庁内連携】 (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。 (主税局) 庁内連携により障害者関係情報及び生活保護関係情報を取得後、登録簿によって照会結果の確認を行う。</p>
その他の措置の内容	—
リスクへの対策は十分か	<p>[十分である] <選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>
リスク4: 入手の際に特定個人情報 that 漏えい・紛失するリスク	
リスクに対する措置の内容	<p>【減免申請者情報】 照会情報の登録に必要な減免申請書は、税務総合支援システムへの入力後は鍵のかかるロッカーで施錠管理している。</p> <p>【庁内連携】 (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。 ・ログイン時に利用者の認証を実施する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・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。 ・全ての照会及び回答について、特定個人情報の照会者、移転者、日時等をシステム上でアクセスログとして記録し、7年間保存する。 ・照会側と提供(回答)側の間で行われる特定個人情報の授受に当たっては、その中継のみを行う。 ・情報連携に用いる機器は、USB機器等に対する制御を行い、外部記録媒体の利用を制限する。 ・情報連携に用いる端末に対し、端末認証を行う。 (主税局) ・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、主税局執務室内に設置された端末で作業し、外部に持ち出すことはない。</p>

リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。)におけるその他のリスク及びそのリスクに対する措置		
-		
3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク		
宛名システム等における措置の内容	<p>【連携サーバー】 連携サーバーは、ユーザIDにより利用者・個別業務システム(事務)等の単位でアクセス可能な範囲を限定し、正当な権限のない利用者・個別業務システム(事務)等からは個人番号を利用できないアクセス制御を行っている。</p> <p>【税務総合支援システム(サーバ)】 ・税務総合支援システムから戦略政策情報推進本部所管の団体内統合利用番号連携サーバ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。</p>	
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	<ul style="list-style-type: none"> ・税務総合支援システムを使用する職員に対して、職員ごとにユーザIDを割り当てるとともに、IDとパスワードによる認証を行っている。 ・パスワードは3ヶ月に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各ユーザIDに必要な権限を付与・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	<ul style="list-style-type: none"> ・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。 ・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、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。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 従業者が事務外で使用するリスク	
リスクに対する措置の内容	<ul style="list-style-type: none"> ・「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、情報資産の外部持ち出しを禁止している。 ・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、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。 ・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。 ・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。 ・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。
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	<ul style="list-style-type: none"> ・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。 ・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。 ・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。 ・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。
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	
<ul style="list-style-type: none"> ・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。 ・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。 ・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。 ・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。 ・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。 ・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・2】 ・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】 ・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2】 ・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、該当委託先はサーバ管理のみ使用するため、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・2】 ・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・2】 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。
-----------------------------------	---

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・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。 ・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	<p>【委託事項1】</p> <ul style="list-style-type: none"> ・ 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。 <p>【委託事項2】</p> <ul style="list-style-type: none"> ・ 管理するサーバ内の特定個人情報は、委託事項1の委託先が消去することとしている。 	
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[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	<p>【委託事項1・2】</p> <ul style="list-style-type: none"> ・ 委託契約で下記事項を規定している。 (1) プログラム、データ等が格納されたサーバ及び端末機器等は、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。 (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	<p>【委託事項1・2】</p> <ul style="list-style-type: none"> ・ 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	<ul style="list-style-type: none"> ・ 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、文書等の取扱い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
-------------	-----	-----------------------	----------

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
-------------	-----	-----------------------	----------

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
-------------	-----	-----------------------	----------

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	<p>【中間サーバー・ソフトウェアにおける措置】</p> <p>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照会リスト(※2)との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから提供許可証を受領してから情報照会を実施することになる。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。</p> <p>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。</p> <p>(※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。</p> <p>(※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。</p> <p>(※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。</p> <p>【連携サーバー】</p> <ul style="list-style-type: none"> ・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。 <p>【税務総合支援システム】</p> <ul style="list-style-type: none"> ・個人事業税、自動車税、固定資産税の減免に係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、対象者について登録簿を作成し、内部承認を経たうえで、照会ファイル作成のためのシステム登録を行う。
リスクへの対策は十分か	<p>[十分である]</p> <p style="text-align: right;"><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</p>

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	<p>【中間サーバー・ソフトウェア】 ①中間サーバーは、特定個人情報保護委員会との協議を経て、総務大臣が設置・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。</p> <p>【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。</p> <p>【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。</p> <p>【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、主税局執務室内に設置された端末で作業し、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。</p>
リスクへの対策は十分か	<p>[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</p>
リスク3: 入手した特定個人情報ที่ไม่正確であるリスク	
リスクに対する措置の内容	<p>【中間サーバー・ソフトウェア】 ①中間サーバーは、特定個人情報保護委員会との協議を経て、総務大臣が設置・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。</p> <p>【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。</p> <p>【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、登録簿によって照会結果の確認を行う。</p>
リスクへの対策は十分か	<p>[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</p>

リスク4: 入手の際に特定個人情報漏えい・紛失するリスク

<p>リスクに対する措置の内容</p>	<p>【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。</p> <p>【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。</p> <p>【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。</p> <p>【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、主税局執務室内に設置された端末で作業し、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、対象者に係る必要な情報について登録簿を作成し、内部承認を経たうえで、照会ファイル作成のためのシステム登録を行う。 ・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、主税局執務室内において、媒体を経由して取り込みを行う。</p>
---------------------	--

<p>リスクへの対策は十分か</p>	<p>[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</p>
--------------------	--

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	
<p>【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制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。</p> <p>【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。 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。</p> <p>【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。</p>	

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	<p>【中間サーバー・プラットフォーム】</p> <p>①中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。</p> <p>②事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。</p> <p>【連携サーバー】</p> <ul style="list-style-type: none"> ・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るものの廃棄等に当たっては、磁氣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。 <p>【税務総合支援システム(サーバ)】</p> <ul style="list-style-type: none"> ・特定個人情報を保管するデータセンターは、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。 ・データセンター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	<p>【中間サーバー・プラットフォーム】</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>【連携サーバー】</p> <ul style="list-style-type: none"> ・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。 <p>【税務総合支援システム】</p> <ul style="list-style-type: none"> ・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。 ・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。さらに、税務総合支援システムはクローズドネットワークにより運用されており、外部ネットワークから接続できないようになっている。なお、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いる。なお、運用拠点への入室はデータセンター同様静脈認証が必要である。

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	<p>①平成30年4月24日、上野動物園で行った動物の観覧抽選に関し、指定管理者の委託先事業者が当選ハガキ状を発送したところ、内209件について、「代表者氏名」「同行者氏名」の全部または一部に他の当選者(代行者・同行者)の氏名が記載されていた。</p> <p>②平成30年5月8日、業務委託先である公益財団法人東京防災救急協会の職員が、444名の受講申請者に対して講習会場案内のメールを一斉送信した際に、誤って他の受講申請者のメールアドレスを閲覧できる状態で送信し、また、当該送信済みメールの取り消し作業においても、一斉送信先のメールアドレスを閲覧できる状態で行ってしまったため、再度、メールアドレスの流出を発生させたもの。</p> <p>③平成30年9月21日、監理団体職員が、メール送信の際、委託事業者のメールアドレスを「BCC」欄に入力し送信すべきところ、誤って「宛先」欄へ入力し送信した。その結果、委託事業者の担当者名、所属会社名及びメールアドレスが送信先に漏れいた。</p> <p>④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</p> <p>⑤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</p> <p>⑥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。</p>	

	再発防止策の内容	<p>①「建設局個人情報漏えい事故等対策本部」を設置し、本件周知と再発防止についての検討を行った上で、同日、局内に通知を発出し、建設局個人情報安全管理基準の趣旨を踏まえ、事故防止に向けて万全を期すよう局内に周知した。また、他の監理団体及び指定管理者に対しても、同様の事故が起きないように指導した。</p> <p>②業務委託先に対してシステム上の対策、メール取扱い時の情報管理対策及び職員への情報セキュリティ教育を指示し、業務委託先において以下のとおり対応した。 (1)誤送信を防止できるメール送信ソフトウェアを導入した。 (2)複数の宛先にメールを送信する際は、事前に情報セキュリティ責任者(部長)に承認を得た上で就業時間内に実施することとし、完了後にも報告することとした。 (3)情報セキュリティ教育を新規職員採用後に速やかに行うとともに、在職職員に対しては、メール送信の取扱要領を年間の教養及び効果確認の際に実施することとした。</p> <p>③平成30年9月26日に「建設局個人情報漏えい事故等対策本部」を設置し、本件周知と再発防止についての検討を行った。同日、総務部長名にて「個人情報に関する事故の再発防止について(通知)」を発出し、建設局個人情報安全管理基準の趣旨を踏まえ、事故防止に向けて万全を期すよう局内に周知した。また、他の監理団体に対しても、同様の事故が起きないように指導した。</p> <p>④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。</p> <p>⑤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31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。</p> <p>⑥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。</p>
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はバックアップセンターで本番データと同様に管理されている。	
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	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。	
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	<p>【連携サーバー】</p> <ul style="list-style-type: none"> ・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るものの廃棄等に当たっては、磁氣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。 <p>【税務総合支援システム(サーバ)】</p> <ul style="list-style-type: none"> ・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。 ・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氣的な破壊によるデータ廃棄作業を行っている。
その他の措置の内容	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。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置	
-	

IV その他のリスク対策 ※

1. 監査	
①自己点検	<p>[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</p> <p>【中間サーバー・プラットフォームにおける措置】 運用規則等に基づき、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。</p> <p>【税務総合支援システム】 情報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、情報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、主税局情報セキュリティ委員会へ報告している。</p>
②監査	<p>[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</p> <p>【中間サーバー・プラットフォームにおける措置】 運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。</p> <p>【税務総合支援システム】 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定期的実施している。 ・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</p> <p>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</p>
2. 従業者に対する教育・啓発	
従業者に対する教育・啓発	<p>[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</p> <p>【中間サーバー・プラットフォームにおける措置】 IPA(情報処理推進機構)が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資料を作成し、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、運用規則(接続運用規程等)や情報セキュリティに関する教育を年次(年2回)及び随時(新規要員着任時)実施することとしている。</p> <p>【税務総合支援システム】 全職員を対象に情報セキュリティ・個人情報(特定個人情報含む)保護の研修を実施している。研修の目的は、個人情報(特定個人情報含む)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(特定個人情報含む)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。 ・3年に1回の悉皆研修 ・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。</p>
3. その他のリスク対策	
<p>【中間サーバー・プラットフォームにおける措置】 中間サーバー・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理(入退室管理等)、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。</p>	

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	東京都主税局税制部システム管理課 〒163-8001 東京都新宿区西新宿2-8-1 都庁第一本庁舎22階中央 Tel.03-5388-2947
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、様式等について東京都公式ホームページ上で分かりやすく表示。
③手数料等	[有料] <選択肢> 1) 有料 2) 無料 (手数料額、納付方法: 納付書により、実費相当分(20円/1枚)の手数料を納付する。)
④個人情報ファイル簿の公表	[行っていない] <選択肢> 1) 行っている 2) 行っていない
個人情報ファイル名	—
公表場所	—
⑤法令による特別の手続	—
⑥個人情報ファイル簿への不記載等	—
2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	東京都主税局税制部システム管理課 〒163-8001 東京都新宿区西新宿2-8-1 都庁第一本庁舎22階中央 Tel.03-5388-2947
②対応方法	問い合わ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2年4月1日
②しきい値判断結果	[基礎項目評価及び全項目評価の実施が義務付けられる] <選択肢> 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 基礎項目評価及び重点項目評価の実施が義務付けられる(任意に全項目評価を実施) 3) 基礎項目評価の実施が義務付けられる(任意に全項目評価を実施) 4) 特定個人情報保護評価の実施が義務付けられない(任意に全項目評価を実施)
2. 国民・住民等からの意見の聴取	
①方法	
②実施日・期間	
③期間を短縮する特段の理由	
④主な意見の内容	
⑤評価書への反映	
3. 第三者点検	
①実施日	
②方法	
③結果	
4. 個人情報保護委員会の承認【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

(別添3)変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成28年4月1日	Ⅱ 特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ①入手元	○ 本人又は本人の代理人 ○ 評価実施期間内の他部署(総務局)	○ 本人又は本人の代理人 ○ 評価実施期間内の他部署(福祉保健局) ○ 地方公共団体・地方独立行政法人(道府県、区市町村)	事前	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため
平成28年4月1日	Ⅱ 特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ②入手方法	○ 紙 ○ 電子記録媒体(フラッシュメモリを除く。)	○ 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 ○ 庁内連携システム ○ 情報提供ネットワークシステム	事前	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため
平成28年4月1日	Ⅱ 特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ①保管場所	【連携サーバー】 ・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、磁氣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。	左記の記述を削除。	事前	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため
平成28年4月1日	Ⅱ 特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ③消去方法	庁内連携について、記載なし	【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、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。 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、磁氣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。	事前	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため
平成28年4月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 (別添2)ファイル記録項目1	以下のマスタについて、評価書記載時点での項目を記載 1. 身体障害者手帳情報マスタ 2. 精神障害者手帳情報マスタ 3. 生活保護情報マスタ	以下のマスタについて、最新情報の項目へ更新 1. 身体障害者手帳情報マスタ 2. 精神障害者手帳情報マスタ 3. 生活保護情報マスタ	事前	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成28年4月1日	<p>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</p> <p>2. 特定個人情報の入手リスク1 『対象者以外の情報の入手を防止するための措置の内容』</p>	庁内連携について、記載なし	<p>【庁内連携】 (連携サーバー) 照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められ、かつ移転者が明示的に回答を承認した場合に限り、連携を行う。照会に対しては、照会条件として指定された対象者に関する情報だけを回答する。なお、チェック項目は、番号法等の改正に応じて、更新する。 (主税局) 庁内連携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、対象者について登録簿を作成し、内部承認を経たうえで、照会ファイル作成のためのシステム登録を行う。</p>	事前	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため
平成28年4月1日	<p>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</p> <p>2. 特定個人情報の入手リスク1 『必要な情報以外を入手することを防止するための措置の内容』</p>	庁内連携について、記載なし	<p>【庁内連携】 (連携サーバー) 連携サーバーシステムでは、照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められたものだけについて連携を行う。なお、チェック項目は、番号法等の改正に応じて、更新する。 (主税局) 庁内連携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、対象者に係る必要な情報について登録簿を作成し、内部承認を経たうえで、照会ファイル作成のためのシステム登録を行う。</p>	事前	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成28年4月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手 リスク2 『リスクに対する措置の内容』	庁内連携について、記載なし	<p>【庁内連携】 (連携サーバー)</p> <ul style="list-style-type: none"> ・照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められ、かつ移転者が明示的に回答を承認した場合に限り、連携を行う。照会に対しては、照会条件として指定された対象者に関する情報だけを回答する。なお、チェック項目は、番号法等の改正に応じて、更新する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・全ての照会及び回答について、特定個人情報の照会者、移転者、日時等をシステム上でアクセスログとして記録し、7年間保存する。(主税局) ・庁内連携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、対象者に係る必要な情報について登録簿を作成し、内部承認を経たうえで、照会ファイル作成のためのシステム登録を行う。 ・システム登録については、ID単位でアクセスログを取得する。 ・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、主税局執務室内において、媒体を経由して取り込みを行う。 	事前	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため
平成28年4月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手 リスク3 『入手の際の本人確認の措置の内容』及び『個人番号の真正性確認の措置の内容』	庁内連携について、記載なし	<p>【庁内連携】 (連携サーバー)</p> <p>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。(主税局)</p> <p>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。</p>	事前	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成28年4月1日	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 2. 特定個人情報の入手 リスク3 『特定個人情報の 正確性確保の措置の内容』	庁内連携について、記載なし	【庁内連携】 (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。 (主税局) 庁内連携により障害者関係情報及び生活保護 関係情報を取得後、登録簿によって照会結果 の確認を行う。	事前	外部機関への情報照会の事 務に加え、庁内連携による情 報照会の事務を追加すること となり、重大な変更にあたる ため

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成28年4月1日	<p>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</p> <p>2. 特定個人情報の入手リスク4 『リスクに対する措置の内容』</p>	<p>庁内連携について、記載なし</p>	<p>【庁内連携】 (連携サーバー)</p> <ul style="list-style-type: none"> ・システムの利用可能な時間を制限している。 ・ログイン時に利用者の認証を実施する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・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。 ・全ての照会及び回答について、特定個人情報の照会者、移転者、日時等をシステム上でアクセスログとして記録し、7年間保存する。 ・照会側と提供(回答)側の間で行われる特定個人情報の授受に当たっては、その中継のみを行う。 ・情報連携に用いる機器は、USB機器等に対する制御を行い、外部記録媒体の利用を制限する。 ・情報連携に用いる端末に対し、端末認証を行う。 <p>(主税局)</p> <ul style="list-style-type: none"> ・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、主税局執務室内に設置された端末で作業し、外部に持ち出すことはない。 	事前	<p>外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため</p>
平成28年4月1日	<p>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</p> <p>3. 特定個人情報の使用リスク2 『ユーザ認証の管理』</p>	<p>税務総合支援システムを使用する職員に対して、個人ごとにユーザIDを割り当てるとともに、IDとパスワードによる認証を行っている。また、パスワードは3か月に1度の頻度で変更を行わないとシステムが使用できないようになっている。さらに、ログイン情報は 税務総合支援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、どのタイミングで誰がログインしたのかが把握できるようになっている。</p>	<p>税務総合支援システムを使用する職員に対して、個人ごとにユーザIDを割り当てるとともに、IDとパスワードによる認証を行っている。また、パスワードは3か月に1度の頻度で変更を行わないとシステムが使用できないようになっている。さらに、ログイン情報は 税務総合支援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、どのタイミングで誰がログインしたのかが把握できるようになっている。また、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。</p>	事前	<p>外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため</p>

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成28年4月1日	<p>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</p> <p>6. 情報提供ネットワークシステムとの接続 リスク1 『リスクに対する措置の内容』</p>	<p>【連携サーバー】</p> <ul style="list-style-type: none"> ・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、主税局執務室内に設置された端末で作業し、外部に持ち出すことはない。 <p>【税務総合支援システム】</p> <ul style="list-style-type: none"> ・対象以外の情報を記載することが無いような書面様式をもとに入力している。 ・必要な情報以外を誤って登録することが無いような画面形式としている。 ・個人事業税、自動車税、自動車取得税、固定資産税の減免に係る者のみにアクセス権限を付与する。 	<p>【連携サーバー】</p> <ul style="list-style-type: none"> ・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。 <p>【税務総合支援システム】</p> <ul style="list-style-type: none"> ・個人事業税、自動車税、自動車取得税、固定資産税の減免に係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、対象者について登録簿を作成し、内部承認を経たうえで、照会ファイル作成のためのシステム登録を行う。 	事前	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため
平成28年4月1日	<p>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</p> <p>6. 情報提供ネットワークシステムとの接続 リスク2 『リスクに対する措置の内容』</p>	<p>【税務総合支援システム】</p> <ul style="list-style-type: none"> ・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、主税局執務室内に設置された端末で作業し、外部に持ち出すことはない。 	<p>【税務総合支援システム】</p> <ul style="list-style-type: none"> ・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、主税局執務室内に設置された端末で作業し、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	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成28年4月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク3 『リスクに対する措置の内容』	【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。	【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、登録簿によって照会結果の確認を行う。	事前	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため
平成28年4月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク4 『リスクに対する措置の内容』	【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及び取得する照会結果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、主税局執務室内に設置された端末で作業し、外部に持ち出すことはない。	【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、主税局執務室内に設置された端末で作業し、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、対象者に係る必要な情報について登録簿を作成し、内部承認を経たうえで、照会ファイル作成のためのシステム登録を行う。 ・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、主税局執務室内において、媒体を経由して取り込みを行う。	事前	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため
平成28年4月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 『その他のリスク及びそのリスクに対する措置』	連携サーバについて、記載なし	【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	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成28年4月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか『その内容』	平成27年発生分の重大事故について記載なし	③平成27年3月9日現在において、福祉保健局の中部総合精神保健福祉センターにおいて、都内の病院に返戻した措置入院患者及び医療保護入院患者の定期報告書等の届出書類309件について所在不明となっていることが判明した。 ④平成27年12月1日(火曜日)、総務局総合防災部職員が、防災関係職員が携帯することになっていた小冊子「災害テレホンメモ」を入れていた鞆を帰宅途中において紛失した。「災害テレホンメモ」には、東京都幹部職員及び防災関係職員に係る電話番号氏名等が記載されていたが、鞆は2日後に発見され、回収した。回収時に鞆の中身は全てあり、個人情報の流出は確認されていない。	事前	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため
平成28年4月1日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 リスク1 ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか『再発防止策の内容』	平成27年発生分の重大事故について記載なし	③返戻した書類の再提出ルール及び届出書類の管理(返戻受理後14日以内の再提出厳守及び督促)を徹底する。また、送付・收受の記録、返戻の進捗及び保管情報を可視化する。さらに、個人情報管理に係る研修の実施及び当該事務に係る定期的な内部検査を実施する。 ④職員に対し、個人情報の重要性及び適正な取扱いの徹底について注意喚起を行うとともに、「災害テレホンメモ」について、携帯者を限定、冊子形式から更新可能な形態へと変更、記載内容の精査を行うこととした。	事前	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため
平成28年4月1日	Ⅳ その他のリスク対策 2. 従業者に対する教育・啓発 『具体的な方法』	情報連携サブシステムの操作者を対象とした研修について記載なし	【税務総合支援システム 情報連携サブシステムの操作者を対象として、セキュリティ対策の重要性の理解及び管理要綱を遵守させることを目的に、年1回の悉皆研修を行うこととしている。	事前	外部機関への情報照会の事務に加え、庁内連携による情報照会の事務を追加することとなり、重大な変更にあたるため
令和1年6月19日	I 基本情報 7. 評価実施機関における担当部署 ②所属長の役職名	システム管理課長 北村 周一	システム管理課長	事後	様式変更による変更
令和2年7月15日	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	東京都主税局税制部システム管理課 〒163-8001 東京都新宿区西新宿2-8-1 TEL03-5388-2947	東京都主税局税制部システム管理課 〒163-8001 東京都新宿区西新宿2-8-1 都庁第一本庁舎22階中央 TEL03-5388-2947	事後	庁舎名及びフロアの追記

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2年7月15日	V 開示請求、問合せ 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	東京都主税局税制部システム管理課 〒163-8001 東京都新宿区西新宿2-8-1 TEL03-5388-2947	東京都主税局税制部システム管理課 〒163-8001 東京都新宿区西新宿2-8-1 都庁第一本庁舎22階中央 TEL03-5388-2947	事後	庁舎名及びフロアの追記
	I 基本情報 1. 特定個人情報ファイルを取り扱う事務 ②事務の内容	・「行政手続きにおける特定の個人を識別するための番号の利用に関する法律(以下「番号法」)」第19条第7号に基づき、情報提供ネットワークシステムを使用して減免決定に必要な特定個人情報を照会し、提供を受ける。 ・提供を受ける特定個人情報は下記の通り。 ① 身体・精神障害者手帳及び障害の程度に関する情報 ② 生活保護実施関係情報	・「行政手続きにおける特定の個人を識別するための番号の利用に関する法律(以下「番号法」)」第19条第7号に基づき、情報提供ネットワークシステムを使用して減免決定に必要な特定個人情報を照会し、提供を受ける。 ・提供を受ける特定個人情報は下記の通り。 ① 身体・精神障害者手帳及び障害の程度に関する情報 ② 生活保護実施関係情報	事前	軽微な誤字修正
	I 基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム2 ①システムの名称	団体内統合利用番号連携サーバー	団体内統合利用番号連携サーバー(以下、「連携サーバー」とする。)	事前	軽微な文言修正

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
	I 基本情報 2.特定個人情報ファイルを取り扱う事務において使用するシステム システム3	新規追加	【①システムの名称】 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他システムとの登録】 情報提供ネットワーク、その他(連携サーバー)	事前	実態に合わせて修正
	I 基本情報 5.個人番号の利用 法令上の根拠	番号法第9条第1項 別表第1第16号	番号法第9条第1項 別表第1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等に関する法律別表第一の主務省令で定める事務を定める命令第16条	事前	軽微な文言修正
	I 基本情報 6.情報提供ネットワークシステムによる情報連携 ②法令上の根拠	・番号法第19条第7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7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	事前	軽微な文言修正
	I 基本情報 8.他の評価実施機関	新規追加	-	事前	軽微な修正

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
	I 基本情報 (別添1)事務の内容 (備考)	<p>①納税義務者から減免申請書を受領。 ※ ②「行政手続きにおける特定の個人を識別するための番号の利用に関する法律」第19条第7号に基づき、減免申請者に係る特定個人情報登録を登録。 ③②で登録された対象者について外部記憶媒体経由で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)に登録。 ④【他団体への照会の場合】 中間サーバへ情報提供ネットワーク経由の情報照会依頼を登録。 【庁内連携の場合】 中間サーバへ自情報を照会。 ⑤情報提供ネットワークシステムを経由して特定個人情報を照会。 ⑥情報提供ネットワークシステムを経由して特定個人情報を入手。 ⑦【他団体への照会の場合】 ⑥で提供された特定個人情報を、中間サーバ経由で入手。 【庁内連携の場合】 中間サーバから自情報を入手。 ⑧⑦で提供された特定個人情報を外部記憶媒体経由で情報連携システムへ登録。 ⑨⑧で提供された特定個人情報を参照。</p> <p>※ 地方税の賦課事務(個人事業税・自動車税・自動車取得税・固定資産税のみ対象)</p>	<p>① 納税義務者から減免申請書を受領。 ※地方税の賦課事務(個人事業税・自動車税・固定資産税のみ対象) ②減免申請者について登録簿を作成し、内容に関し内部承認を得たうえで、「行政手続きにおける特定の個人を識別するための番号の利用に関する法律」第19条第7号に基づき、減免申請者に係る特定個人情報を税務総合支援システムの情報連携サブシステムへ登録。 ②' 減免申請者について登録簿を作成し、内容に関し内部承認を得たうえで、「行政手続きにおける特定の個人を識別するための番号の利用に関する法律」第19条第7号に基づき、減免申請者に係る個人情報(特定個人情報を除く)を情報連携サブシステムに一括登録するための一括登録ファイルを作成し、税務総合支援システムの内部メールを使用して、システム管理課に送付する。 ②" ②'で送付された一括登録ファイルを、外部記録媒体を用いてバッチ処理を行う環境に移行する。移行後、バッチ処理で情報連携サブシステムへデータを登録するが、データ元となる一括登録ファイルには特定個人情報が含まれていないので、あて名管理サブシステムや情報連携サブシステムに登録済みの特定個人情報を使用して登録を行う。 ③ ②及び②"で登録された対象者について暗号解除用税務端末、外部記憶媒体及び番号系端末経由で団体内統合利用番号連携サーバー(以下「連携サーバ」という)に登録。 ④【他団体への照会の場合】 自治体中間サーバへ情報提供ネットワーク経由の情報照会依頼を登録。 【庁内連携の場合】 自治体中間サーバへ自団体保有情報を照会。 ⑤ 情報提供ネットワークシステムを経由して特定個人情報を照会。 ⑥ 情報提供ネットワークシステムを経由して</p>	事前	実態に合わせて修正
	II 特定個人情報ファイルの概要 2 基本情報 ③ 対象となる本人の範囲	個人事業税、自動車税、自動車取得税、固定資産税の減免に係る者	個人事業税、自動車税、固定資産税の減免に係る者	事前	実態に合わせて修正

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
	II 特定個人情報ファイルの概要 3 特定個人情報の入手・使用 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 ○ 庁内連携システム ○ 情報提供ネットワークシステム	○ 紙 ○ フラッシュメモリ ○ 庁内連携システム ○ 情報提供ネットワークシステム	事前	実態に合わせて修正
	II 特定個人情報ファイルの概要 3 特定個人情報の入手・使用 ③ 特定個人情報の入手の次期、頻度	納税義務者からの個人事業税、自動車税、自動車取得税、固定資産税の減免申請の都度、入手する。	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の都度、入手する。	事前	実態に合わせて修正
	II 特定個人情報ファイルの概要 4 特定個人情報の取扱いの委託 委託の有無	1件	2件	事前	実態に合わせて修正
	II 特定個人情報ファイルの概要 4 特定個人情報の取扱いの委託 委託事項1①	税務総合支援システム維持管理及び運用業務委託	税務総合支援システム維持管理委託	事前	実態に合わせて修正
	II 特定個人情報ファイルの概要 4 特定個人情報の取扱いの委託 委託事項1② 対象となる本人の範囲	個人事業税、自動車税、自動車取得税、固定資産税の減免に関係する者	個人事業税、自動車税、固定資産税の減免に関係する者	事前	実態に合わせて修正
	II 特定個人情報ファイルの概要 4 特定個人情報の取扱いの委託 委託事項1② 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障害発生時の対応などを行う上で取扱う必要がある。	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保護ファイルを取り扱う必要がある。	事前	実態に合わせて修正
	II 特定個人情報ファイルの概要 4 特定個人情報の取扱いの委託 委託事項1④	その他(委託先への特定個人情報ファイルの提供はない)	専用線	事前	実態に合わせて修正

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
	II 特定個人情報ファイルの概要 4 特定個人情報の取扱いの委託 委託事項1⑨	税務総合支援システムおよび関連システムの仕様変更、稼働監視、バッチ処理、障害対応等の一部	税務総合支援システムの仕様変更、障害対応等の一部	事前	実態に合わせて修正
	II 特定個人情報ファイルの概要 4 特定個人情報の取扱いの委託 委託事項2①	記載なし	税務総合支援システム運用委託	事前	実態に合わせて修正
	II 特定個人情報ファイルの概要 4 特定個人情報の取扱いの委託 委託事項2②	記載なし	税務総合支援システム(情報連携サーバを含む。)の稼働に必要な機能の提供 特定個人情報ファイルの全体 10万に以上100万人未満 個人事業税、自動車税、固定資産税の減免に関係する者 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。	事前	実態に合わせて修正
	II 特定個人情報ファイルの概要 4 特定個人情報の取扱いの委託 委託事項2③	記載なし	100人以上500人未満	事前	実態に合わせて修正
	II 特定個人情報ファイルの概要 4 特定個人情報の取扱いの委託 委託事項2④	記載なし	専用線	事前	実態に合わせて修正
	II 特定個人情報ファイルの概要 4 特定個人情報の取扱いの委託 委託事項2⑤	記載なし	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。	事前	実態に合わせて修正

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
	II 特定個人情報ファイルの概要 4 特定個人情報の取扱いの委託 委託事項2⑥	記載なし	株式会社 エヌ・ティ・ティ・データ	事前	実態に合わせて修正
	II 特定個人情報ファイルの概要 4 特定個人情報の取扱いの委託 委託事項2⑦	記載なし	再委託する。	事前	実態に合わせて修正
	II 特定個人情報ファイルの概要 4 特定個人情報の取扱いの委託 委託事項2⑧	記載なし	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。	事前	実態に合わせて修正
	II 特定個人情報ファイルの概要 4 特定個人情報の取扱いの委託 委託事項2⑨	記載なし	運用設計支援、運用保守支援、仕様調整支援、運用テスト支援及びその他運用に関わる技術・作業支援	事前	実態に合わせて修正

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
	II 特定個人情報ファイルの概要 6 特定個人情報の保管・消去 ①保管場所	<p>【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おり、データセンターへの入館及びサーバー室への入室を厳重に管理する。②特定個人情報とは、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。</p> <p>【連携サーバー】</p> <ul style="list-style-type: none"> ・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、ガス系消防設備、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。 <p>【税務総合支援システム】特定個人情報を保管するデータセンターは、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。データセンターへの立ち入りはICカード所持者に限定しており、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。</p>	<p>【中間サーバー・プラットフォーム】</p> <p>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。</p> <p>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。</p> <p>【連携サーバー】</p> <ul style="list-style-type: none"> ・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、ガス系消防設備、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。 <p>【税務総合支援システム(サーバ)】</p> <ul style="list-style-type: none"> ・特定個人情報を保管するデータセンターは、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。 ・データセンター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	実態に合わせて修正
	II 特定個人情報ファイルの概要 6 特定個人情報の保管・消去 ③消去方法	<p>【税務総合支援システム】</p> <p>課税から収入までの一連のサイクルを完了し、7年度経過した情報についてシステム管理部署で決裁を経たうえで、プログラムにより削除している。なお、媒体によるデータ授受を行う場合は媒体内のデータを随時消去している。</p>	<p>【税務総合支援システム(サーバ)】</p> <p>一定期間経過後、バッチ処理により削除する。</p>	事前	実態に合わせて修正

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
	II ファイルの概要 (別添2)ファイル記録項目	新規追加	※1身体障害者手帳情報マスタ及び2精神障害者手帳情報マスタには要配慮個人情報を含む。	事前	実態に合わせて修正
	III 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク1	【税務総合支援システム】 税務総合支援システムから総務局所管の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。また、権限設定どおりに接続等が実施できるかどうかを開発時のテストにて確認する。	【税務総合支援システム(サーバ)】 ・税務総合支援システムから戦略政策情報推進本部所管の団体内統合利用番号連携サーバ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。	事前	実態に合わせて修正
	III 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2ユーザ認証の管理	税務総合支援システムを使用する職員に対して、個人ごとにユーザIDを割り当てるとともに、IDとパスワードによる認証を行っている。また、パスワードは3カ月に1度の頻度で変更を行わないとシステムが使用できないようになっている。さらに、ログイン情報は 税務総合支援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、どのタイミングで誰がログインしたのかが把握できるようになっている。	・税務総合支援システムを使用する職員に対して、職員ごとにユーザIDを割り当てるとともに、IDとパスワードによる認証を行っている。 ・パスワードは3ヶ月に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。	事前	実態に合わせて修正
	III 特定個人情報ファイルの 取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2アクセス権限の発行・失効の管理	人事担当部署が職員の異動情報を把握次第、または公表次第、異動情報を記載したメールにて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職員個人ごとの異動発令に合わせて必要な権限を付与・削除している。	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している。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・削除している。	事前	実態に合わせて修正

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
	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2アクセス権限の管理	<p>税務総合支援システムの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」、「参照のみ可」、「更新・参照不可」の権限を設定している。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している。また、反映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。さらに、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。連携サーバーのアクセス権限は、情報連携事務担当のみに設定する。</p>	<ul style="list-style-type: none"> ・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。 ・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している。 	事前	実態に合わせて修正
	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2特定個人情報使用の記録	<p>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、誰がどの情報をアクセス、抽出したかが記録されている。なお、記録は1年以上保存している。</p>	<p>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。</p>	事前	実態に合わせて修正
	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2その他の措置の内容	<p>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する。また、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へ周知している。</p>	記載なし	事前	実態に合わせて修正

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
	<p>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</p> <p>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</p>	<p>「東京都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。また、局内の規定において、原則、情報資産の外部持ち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ち出しができないようになっている</p>	<ul style="list-style-type: none"> ・「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、情報資産の外部持ち出しを禁止している。 ・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、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ち出しができないようになっている。 ・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。 ・不正持ち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。 ・外部持ち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。 	事前	実態に合わせて修正
	<p>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</p> <p>3. 特定個人情報の使用 リスク4 不正に複製されるリスク</p>	<p>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でのみ閲覧が可能となっており、サーバーからのダウンロード等により入手することはできない。また、税務総合支援システム端末では、外部記憶媒体の使用が不可能であるため、情報資産の持ち出しはできない。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、情報資産の持ち出しを可能としている。この際には、例外的に外部記憶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。さらに、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、研修等により注意喚起している。</p>	<ul style="list-style-type: none"> ・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。 ・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、情報資産の持ち出しができないようになっている。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、情報資産の持ち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。 ・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。 ・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。 	事前	実態に合わせて修正

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
	<p>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</p> <p>3. 特定個人情報の使用 特定個人情報の使用におけるその他のリスク及びそれに対する措置</p>	<p>個人番号を含む特定個人情報ファイルについては、税務総合支援システム端末以外の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。</p>	<ul style="list-style-type: none"> ・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。 ・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。 ・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。 ・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。 ・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。 ・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	実態に合わせて修正
	<p>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</p> <p>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</p>	<p>契約時に委託先と取り交わす契約で、・責任者、作業体制、連絡体制及び作業場所を画面にして提出・業務従事者への遵守事項の周知及び実施報告の提出・再委託の承諾申請の提出・作業担当者の名簿の提出等を求めている。また、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。また、委託元が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。</p>	<p>【委託事項1・2】</p> <ul style="list-style-type: none"> ・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。 	事前	実態に合わせて修正

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
	<p>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</p> <p>4 特定個人情報ファイルの取扱いの委託</p> <p>特定個人情報ファイルの閲覧者・更新者の制限</p>	<p>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、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。</p>	<p>【委託事項1】</p> <ul style="list-style-type: none"> ・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。 <p>【委託事項2】</p> <ul style="list-style-type: none"> ・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、該当委託先はサーバ管理のみ使用するため、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	実態に合わせて修正
	<p>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</p> <p>4 特定個人情報ファイルの取扱いの委託</p> <p>特定個人情報ファイルの取扱いの記録</p>	<p>・委託先との契約に際して、施錠できる保管庫等での管理、管理状況の記録、管理記録の報告等を規定した契約を取り交わし、委託処理に係る必要事項を求めている。・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、誰がどの情報をアクセス、抽出したかが記録されている。なお、記録は1年以上保存している。</p>	<p>【委託事項1・2】</p> <ul style="list-style-type: none"> ・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	実態に合わせて修正
	<p>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</p> <p>4 特定個人情報ファイルの取扱いの委託</p> <p>委託先から他者への提供に関するルール内容及びルール遵守の確認方法</p>	<p>委託先から他者への提供はない。なお、提供する必要が発生する場合は、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。</p>	<p>【委託事項1・2】</p> <p>委託先から他者への提供はない。なお、提供する必要が発生する場合は、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。</p>	事前	実態に合わせて修正

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
	<p>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</p> <p>4 特定個人情報ファイルの取扱いの委託</p> <p>委託元と委託先間の提供に関するルール内容及びルール遵守の確認方法</p>	<p>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。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。また、データセンターへの立ち入りはICカード所持者に限定しており、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。</p>	<p>【委託事項1・2】</p> <ul style="list-style-type: none"> ・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。 ・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	実態に合わせて修正
	<p>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</p> <p>4 特定個人情報ファイルの取扱いの委託</p> <p>ルール内容及びルール遵守の確認方法</p>	<p>委託元から委託先への提供はない。なお、提供が発生した場合は契約時に委託業者と取り交わす契約で、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が規定されており、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の報告を求めている。</p>	<p>【委託事項1】</p> <ul style="list-style-type: none"> ・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。 <p>【委託事項2】</p> <ul style="list-style-type: none"> ・管理するサーバ内の特定個人情報は、委託事項1の委託先が消去することとしている。 	事前	実態に合わせて修正
	<p>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</p> <p>4 特定個人情報ファイルの取扱いの委託</p> <p>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</p>	<p>契約時に委託先と取り交わす契約で下記事項を求めている。・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。・外部記憶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。・セキュリティ監査を実施する際は協力すること。・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。</p>	<p>【委託事項1・2】</p> <ul style="list-style-type: none"> ・委託契約で下記事項を規定している。 <ul style="list-style-type: none"> (1)プログラム、データ等が格納されたサーバ及び端末機器等は、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。 (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	実態に合わせて修正

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
	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 4 特定個人情報ファイルの 取扱いの委託 再委託先による特定個人情 報ファイルの適切な取扱いの 確保	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が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 担当者名簿を提出させるとともに、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・2】 ・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	実態に合わせて修正

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
	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4 特定個人情報ファイルの取扱いの委託 その他の措置の内容	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。	・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、文書等の取扱い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。	事前	実態に合わせて修正
	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 6 情報提供ネットワークシステムとの接続 リスク1 目的外の入手が行われるリスク	【中間サーバー・ソフトウェア】①情報照会機能(※1)により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可照合リスト(※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情報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)番号法別表第2及び第19条第14号に基づき、事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。(※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。 【税務総合支援システム】・個人事業税、自動車税、自動車取得税、固定資産税の減免に係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、対象者について登録簿を作成し、内部承認を経たうえで、照会ファイル作成のためのシステム登録を行う。	【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。	事前	実態に合わせて修正

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
	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 7 特定個人情報の保管・消 去 リスク1⑤物理的対策	<p>【中間サーバー・プラットフォーム】 中間サーバー・プラットフォームをデータセン ターに構築し、設置場所への入退室者管理、 有人監視及び施錠管理をすることとしている。 また、設置場所はデータセンター内の専用の 領域とし、他テナントとの混在によるリスクを回 避する。</p> <p>【税務総合支援システム】 特定個人情報を保管するデータセンターは、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。データセンターへの立ち入 りはICカード所持者に限定しており、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。外部記憶媒体及び紙 資料はロッカー等で施錠管理している。なお、 私物の情報処理機器についてはデータセン ターへの持込を制限している。また、主税局職 員が業務を行う執務室については、特定個人 情報の保管をセキュリティが確保されたサー バーで行うとともに、外部記憶媒体及び紙資料 はロッカー等で施錠管理している。</p>	<p>【中間サーバー・プラットフォーム】 ①中間サーバー・プラットフォームをデータセン ターに構築し、設置場所への入退室者管理、 有人監視及 び施錠管理をすることとしている。また、設置場 所はデータセンター内の専用の領域とし、他テ ナントとの 混在によるリスクを回避する。 ②事前に申請し承認されてない物品、記憶媒 体、通信機器などを不正に所持し、持出持込す ることがな いよう、警備員などにより確認している。</p> <p>【税務総合支援システム(サーバ)】 ・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。</p>	事前	実態に合わせて修正

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
	III 特定個人情報ファイルの 取扱いプロセスにおけるリスク 対策 7 特定個人情報の保管・消 去 リスク1⑥技術的対策	<p>【税務総合支援システム】 税務総合支援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。さらに、許可されたデータの持ち出しであっても、データはソフトにより暗号化されているため、税務総合支援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。</p> <p>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、税務総合支援システムはクローズドネットワークにより運用されており、外部ネットワークから接続できないようになっている。なお、税務総合支援システムと連携サーバー間のデータ連携は、執務室内で専用の外部記憶媒体を使用して行う。</p>	<p>【税務総合支援システム】 ・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ち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。</p> <p>・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、税務総合支援システムはクローズドネットワークにより運用されており、外部ネットワークから接続できないようになっている。なお、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。</p>	事前	実態に合わせて修正

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
	Ⅲ 特定個人情報ファイルの 取扱いプロセスにおけるリス ク対策 7 特定個人情報の保管・消 去 リスク1⑨重大事故(その内 容)	①平成26年10月15日(水曜日)、生活文化局 の東京都防災(語学)ボランティアに関する事 務において、業務委託事業者が、研修の案内 に関する通知をメール送信する際に、データ設 定の誤りに気付かず、769名分のメールについ て、本人以外の1名分の氏名が宛先に表示さ れてしまった。 ②平成27年3月9日現在において、福祉保健 局の中部総合精神保健福祉センターにおい て、都内の病院に返戻した措置入院患者及び 医療保護入院患者の定期報告書等の届出書 類309件について所在不明となっていることが 判明した。 ③平成27年12月1日(火曜日)、総務局総合防 災部職員が、防災関係職員が携帯すること となっていた小冊子「災害テレホンメモ」を入 っていた鞆を帰宅途中において紛失した。「災 害テレホンメモ」には、東京都幹部職員及び 防災関係職員に係る電話番号氏名等が記載 されていたが、鞆は2日後に発見され、回収 した。回収時に鞆の中身は全てあり、個人情 報の流出は確認されていない。	①平成30年4月24日、上野動物園で行った 動物の観覧抽選に関し、指定管理者の委託先 事業者が当選ハガキ状を発送したところ、内 209件について、「代表者氏名」「同行者氏名」 の全部または一部に他の当選者(代行者・同 行者)の氏名が記載されていた。 ②平成30年5月8日、業務委託先である公益 財団法人東京防災救急協会の職員が、444 名の受講申請者に対して講習会場案内のメ ールを一齐送信した際に、誤って他の受講申 請者のメールアドレスを閲覧できる状態で送 信し、また、当該送信済みメールの取り消し 作業においても、一齐送信先のメールアドレス を閲覧できる状態で行ってしまったため、再 度、メールアドレスの流出を発生させたもの。 ③平成30年9月21日、監理団体職員が、メ ール送信の際、委託事業者のメールアドレス を「BCC」欄に入力し送信すべきところ、誤 って「宛先」欄へ入力し送信した。その結果、 委託事業者の担当者名、所属会社名及びメ ールアドレスが送信先に漏えいした。 ④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 ⑤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	事前	実態に合わせて修正

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
	<p>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</p> <p>7 特定個人情報の保管・消去</p> <p>リスク1⑨重大事故(再発防止の容)</p>	<p>①東京都防災(語学)ボランティアに関する事務において、委託業務を見直し、今回のミスの元となった作業を不要としたほか、業務委託事業者に対し、複数名での最終確認の徹底、個人情報の取扱いに関する指示系統の確認を指示した。また、庁内全部局に対し、保有個人情報の安全管理の徹底を注意喚起した。</p> <p>②返戻した書類の再提出ルール及び届出書類の管理(返戻受理後14日以内の再提出厳守及び督促)を徹底する。また、送付・收受の記録、返戻の進捗及び保管情報を可視化する。さらに、個人情報管理に係る研修の実施及び当該事務に係る定期的な内部検査を実施する。</p> <p>③職員に対し、個人情報の重要性及び適正な取扱いの徹底について注意喚起を行うとともに、「災害テレホンメモ」について、携帯者を限定、冊子形式から更新可能な形態へと変更、記載内容の精査を行うこととした。</p>	<p>①「建設局個人情報漏えい事故等対策本部」を設置し、本件周知と再発防止についての検討を行った上で、同日、局内に通知を发出し、建設局個人情報安全管理基準の趣旨を踏まえ、事故防止に向けて万全を期すよう局内に周知した。また、他の監理団体及び指定管理者に対しても、同様の事故が起きないように指導した。</p> <p>②業務委託先に対してシステム上の対策、メール取扱い時の情報管理対策及び職員への情報セキュリティ教育を指示し、業務委託先において以下のとおり対応した。</p> <p>(1)誤送信を防止できるメール送信ソフトウェアを導入した。</p> <p>(2)複数の宛先にメールを送信する際は、事前に情報セキュリティ責任者(部長)に承認を得た上で就業時間内に実施することとし、完了後にも報告することとした。</p> <p>(3)情報セキュリティ教育を新規職員採用後に速やかに行うとともに、在職職員に対しては、メール送信の取扱要領を年間の教養及び効果確認の際に実施することとした。</p> <p>③平成30年9月26日に「建設局個人情報漏えい事故等対策本部」を設置し、本件周知と再発防止についての検討を行った。同日、総務部長名にて「個人情報に関する事故の再発防止について(通知)」を发出し、建設局個人情報安全管理基準の趣旨を踏まえ、事故防止に向けて万全を期すよう局内に周知した。また、他の監理団体に対しても、同様の事故が起きないように指導した。</p> <p>④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。</p>	<p>事前</p>	<p>実態に合わせて修正</p>

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
	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7 特定個人情報の保管・消去 リスク3 消去手順の内容	【税務総合支援システム】 課税から収入までの一連のサイクルを完了し、7年度経過した情報についてシステム管理部署で決裁を経たうえで、プログラムにより削除している。なお、媒体によるデータ授受を行う場合は媒体内のデータを随時消去している。	【税務総合支援システム(サーバ)】 ・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。 ・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。	事前	実態に合わせて修正
	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7 特定個人情報の保管・消去 リスク3 その他の措置の内容	文書については、定められた保存期間に基づき管理しており、保存期間が満了した文書については、定期的に廃棄(溶解処理)を行っている。そのなかで、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。 また、主務課において常時利用する必要があるとして、主務課長が指定した常用文書については、保存期間とは別に保存され、施錠可能な所で保管している。	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。	事前	実態に合わせて修正
	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7 特定個人情報の保管・消去 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。		事前	実態に合わせて修正

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
	IV その他のリスク対策 1. 監査 ①自己点検 『具体的な方法』	<p>【中間サーバー・プラットフォームにおける措置】 運用規則等に基づき、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。</p> <p>【税務総合支援システム】 情報セキュリティ責任者・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、情報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、主税局情報セキュリティ委員会へ報告している。</p>	<p>【中間サーバー・プラットフォームにおける措置】 運用規則等に基づき、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。</p> <p>【税務総合支援システム】 情報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、情報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、主税局情報セキュリティ委員会へ報告している。</p>	事前	実態に合わせて修正
	IV その他のリスク対策 1. 監査 ②監査 『具体的な方法』	<p>【中間サーバー・プラットフォームにおける措置】 運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。</p> <p>【税務総合支援システム】 1. 内部監査 以下の観点で内部監査人による監査を毎年実施している。 ・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</p> <p>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</p>	<p>【中間サーバー・プラットフォームにおける措置】 運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。</p> <p>【税務総合支援システム】 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定期的に実施している。 ・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</p> <p>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</p>	事前	実態に合わせて修正

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
	IV その他のリスク対策 2. 従業者に対する教育・啓発 『具体的な方法』	<p>【中間サーバー・プラットフォームにおける措置】</p> <p>①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、セキュリティ研修等を実施することとしている。②中間サーバー・プラットフォームの業務に就く場合は、運用規則等について研修を行うこととしている。</p> <p>【税務総合支援システム】</p> <p>全職員を対象に情報セキュリティ・個人情報保護の研修を実施している。研修の目的は、個人情報保護の重要性及び適正管理等に関する理解を深め、個人情報保護の遵守を徹底することである。具体的には、以下の研修を実施している。</p> <ul style="list-style-type: none"> ・3年に1回の悉皆研修 ・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 <p>また、情報連携サブシステムの操作者を対象として、セキュリティ対策の重要性の理解及び管理要綱を遵守させることを目的に、年1回の悉皆研修を行うこととしている。</p>	<p>【中間サーバー・プラットフォームにおける措置】</p> <p>IPA(情報処理推進機構)が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資料を作成し、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、運用規則(接続運用規程等)や情報セキュリティに関する教育を年次(年2回)及び随時(新規要員着任時)実施することとしている。</p> <p>【税務総合支援システム】</p> <p>全職員を対象に情報セキュリティ・個人情報(特定個人情報含む)保護の研修を実施している。研修の目的は、個人情報(特定個人情報含む)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(特定個人情報含む)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。</p> <ul style="list-style-type: none"> ・3年に1回の悉皆研修 ・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 <p>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。</p>	事前	実態に合わせて修正