資料38

個人情報保護管理運営会議　付議事項

件名	当初課税業務の委託について（委託内容の追加）

内容は別紙のとおり

要綱の根拠

◇第３条第１項第３号（業務委託）

（担当部課：総務部税務課）

事業の概要

事業名	当初課税業務委託
担当課	税務課
目　的	当初課税期における特別区民税・都民税課税業務（以下「当初課税業務」という。）の正確性向上及び効率化を図るため。
対象者	賦課期日に新宿区内に住所等を有する者、特別徴収義務者、新宿区に課税資料等が提出された者
事業内容	１　概要 税務課では、当初課税期（1月～5月）における職員の過度な負担を軽減し、専門性の高い業務に専念できる環境を整備するため、令和７年１月より、当初課税業務のうち定型的な入力作業等について外部委託を実施している。（令和６年度第２回個人情報保護管理運営会議了承済み） その委託業務の１つである「対象者エラーの処理・入力」は、税務システムが対象者不明と判断した課税資料について、対象者を検索し確定させる業務であるが、確定させようとする者が賦課期日に他自治体に住所を有する場合には、当該住所情報（前住地等）の登録が必要になる。 しかし、住民記録システム（以下「住基システム」という。）を利用することができない委託事業者では、対象者の前住地等を確認することができないため、「対象者エラーの処理・入力」の一部は、委託事業者から職員へ戻され、職員が対応している。 ついては、住基システムを委託事業者に利用させることで、「対象者エラーの処理・入力」を委託事業者でも行うことができるようにして、職員と委託事業者における業務の効率化を図る。 ２　個人情報保護管理運営会議への付議内容 （１）業務委託 １　郵便物等の仕分け・開封 ２　課税資料の内容の確認・精査・補記 ３　特別徴収義務者等に対する電話照会 ４　システムにおける検索・入力処理 ５　課税資料のスキャン・イメージデータ化 ６　対象者エラーの処理・入力**（住基システムにおける検索）** ７　課税データ登録・作成 （２）再委託 １　パンチ入力 ３　対象者数 賦課期日に新宿区内に住所を有する者　約35万人／年度 賦課期日に新宿区内に事業所等を有する者　約2千人／年度 特別徴収義務者　約5千社／年度 ※個人情報の流れは、資料３８－１及び資料３８－２のとおり

別紙(業務委託)

◇業務委託(第３条第１項第３号)

件名　当初課税業務委託について（委託内容の追加）

※太字ゴシック（下線）が、令和６年度第２回新宿区個人情報保護管理運営会議承認済の内容からの変更箇所

保有課(担当課)	税務課
登録業務の名称	特別区民税・都民税
委託先	ヒューマンリソシア株式会社（プライバシーマーク取得事業者）
委託に伴い事業者に処理させる情報項目（だれの、どのような項目か）	１　個人の範囲 賦課期日に新宿区内に住所等を有する者、特別徴収義務者、新宿区に課税資料等が提出された者 ２　情報項目 氏名、性別、生年月日、住所、続柄、電話番号、職業、課税資料情報、収入情報、所得情報、控除情報、税額、期別（月割）額、納期限、徴収方法希望、専従者情報、受給者番号、納税者番号、扶養者情報、個人番号、支払者情報、前職分情報、就職日、退職日、台帳番号、異動事由、**住民事由、住民日、転入前住所、転入前方書、消除事由、消除日、転出予定住所、転出予定方書、先住所、先住所方書**
処理させる情報項目の記録媒体	紙（申告書等の課税資料）及び電磁的媒体（税務システム※、**住基システム**） ※区が統合基盤上に構築したパッケージシステムを、委託事業者に提供する
委託理由	①　当初課税業務のうち定型的業務を外部委託し、職員の負担軽減及び専門性特化を図り、当初課税業務の正確性向上及び効率化につなげるため。 ②　**委託業者に住基システムを利用させ、上記①の効果を高めるため。**
委託の内容	１　郵便物等の仕分け・開封 ２　課税資料の内容の確認・精査・補記 ３　特別徴収義務者等に対する電話照会 ４　システムにおける検索・入力処理 ５　課税資料のスキャン・イメージデータ化 ６　対象者エラーリスト処理**（住基システムにおける検索）** ７　住民登録外者のデータ作成 ８　パンチ入力【再委託予定】
委託の開始時期及び期限	令和７年１１月１３日から令和８年５月３１日まで ※令和７年１１月１３日から令和７年１２月３１日までは委託事業者と運営体制を構築する期間とする。 ※次年度以降も、同様の業務委託を行う。 ※成績良好と判断した場合、最長で令和9年5月31日まで同一事業者に契約できるものとする。
委託にあたり区が行う情報保護対策	別紙チェックリストのとおり。
受託事業者に行わせる情報保護対策	別紙チェックリストのとおり。

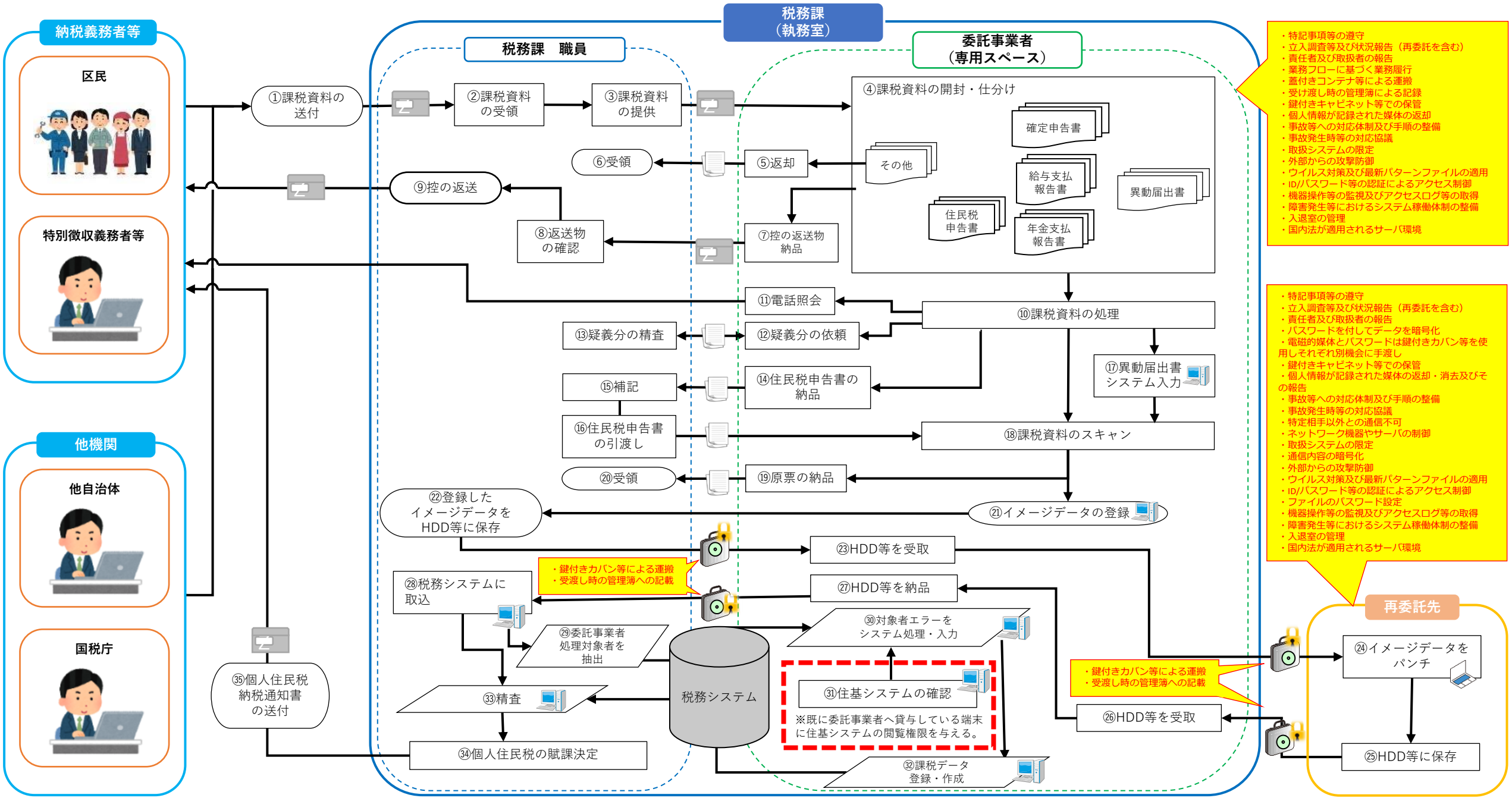
別紙(業務委託、再委託)

件名　課税資料等のパンチ入力業務の再委託について

保有課(担当課)	税務課
登録業務の名称	課税資料のパンチ入力業務の再委託
委託先、再委託する場合の再委託先	【委託先】 ヒューマンリソシア株式会社（プライバシーマーク取得事業者） 【再委託する場合の再委託先】 委託先が指定する事業者 ただし再委託先は、委託案件の入札参加者でないこと、情報セキュリティマネジメントシステム（ISMS）適合性評価制度の認証又はプライバシーマーク認証取得していることを条件とする。
再委託に伴い事業者に処理させる情報項目（だれの、どのような項目か)	１　委託先及び再委託先が共通で取り扱う情報項目 氏名、性別、生年月日、住所、続柄、電話番号、職業、収入情報、所得情報、控除情報、税額、徴収方法希望、専従者情報、受給者番号、納税者番号、扶養者情報、個人番号、事業者情報、摘要欄情報、所得税情報、課税資料情報 ２　対象帳票 給与支払報告書（総括表）、給与支払報告書（個人別明細書）、確定申告書、公的年金支払報告書（個人別明細書）、特別区民税・都民税申告書、添付資料（源泉徴収票、控除証明書、内訳書、計算書等)
処理させる情報項目の記録媒体	電磁的媒体（HDD 等、委託先のパソコン及びサーバ)
再委託理由	毎年度、区に提出される課税資料等は約 20 万件あり、かつ資料の種類や入力項目も多岐に渡るため、、専門的な技術と豊富なノウハウを備えた業者へ再委託することにより、正確かつ効率的な事務処理を図る。 なお、委託先自身で本業務をすべて履行できる事業者を選定した場合、再委託は行わない。
再委託の内容	区が提供する課税資料の内容をパンチ入力し、パンチデータ（HDD 等）として納品する。
再委託の開始時期及び期限	令和７年１１月１３日から令和８年５月３１日まで ※令和７年１１月１３日から令和７年１２月３１日まではパンチテストを行う期間とする。 ※次年度以降も、同様の業務委託を行う。
再委託にあたり区が行う情報保護対策	別紙チェックリストのとおり。
受託事業者に行わせる情報保護対策	別紙チェックリストのとおり。

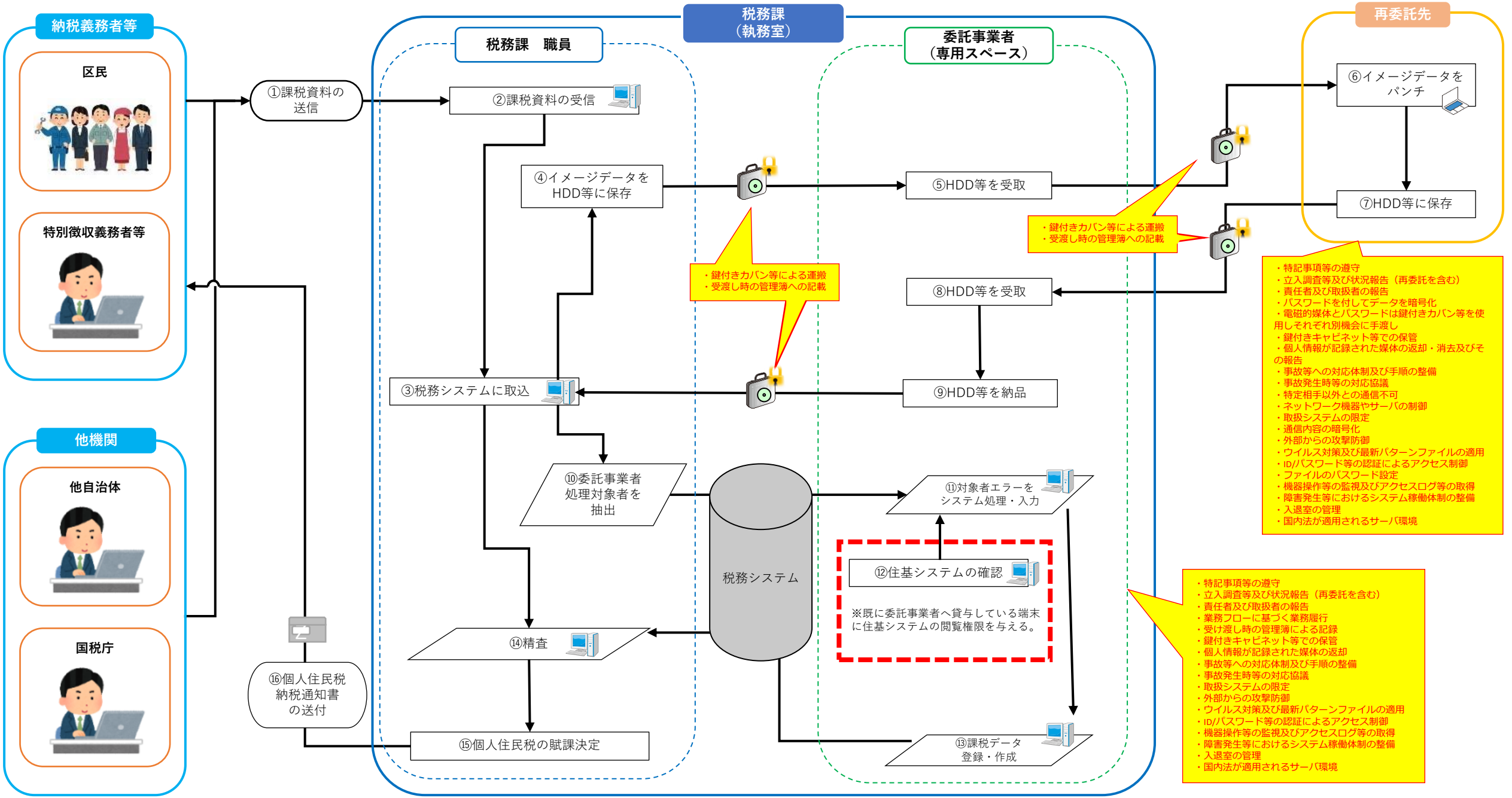
当初課税業務委託に係る個人情報（紙媒体）の流れ　※赤点線の部分が、今回の変更箇所

（資料３８－１）



当初課税業務委託に係る個人情報（電磁的媒体）の流れ　※赤点線の部分が、今回の変更箇所

（資料３８－２）



5　業務委託にかかる個人情報保護対策チェックリスト

（電磁的媒体・紙媒体の取扱い）

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
委託にあたり区が行う 情報保護対策 【運用上の対策】	○	契約にあたり、「特記事項」を付すとともに、個人情報保護法及び新宿区情報セキュリティポリシーを遵守するよう指導する。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠するよう指導する。
	○	契約履行の間、特記事項に基づき立入り調査等を実施するとともに、委託先に対し速やかに状況報告をするよう指導する。
	○	再委託先がある場合には、委託先との間に立入り調査等ができる契約内容を付すとともに、必要に応じて又は定期的に立入り調査等を実施するよう指導する。
	○	取扱責任者及び取扱者をあらかじめ指定し、区に報告するよう指導する。
	○	全体の業務フローを作成し、委託先と共有する。
	○	取扱う個人情報の管理について、必要に応じて又は定期的に確認する体制を構築するよう指導する。
	○	個人情報を含むデータを作成する必要が生じた場合は、パスワードを付してデータを暗号化する。また、電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用して、手渡しで行うよう指導する。
	○	個人情報を手交する場合は、鍵付きカバン等を使用して運搬する。
	○	個人情報の受渡しにあたっては、管理簿に記載する。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにする。
	○	個人情報は、施錠できる金庫又はキャビネット等に保管する。
	○	業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却し、電子データは消去するよう指導する。また、区に電子データの消去を行ったことの報告書を提出するよう指導する。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備し、委託先と緊急時の連絡体制や対応手順を確認する。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに委託先と今後の対応を協議する。
委託にあたり区が行う 情報保護対策 【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定する。
	○	通信内容は暗号化し、通信途上の個人情報の盗用、改ざん、成りすましを防止する。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御する。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用する。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止する。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定するとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底する。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得する。取得したログは、定期的に分析する。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備する。
	○	入退室管理等により情報資産の危殆化を防止する。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にする。

5　業務委託にかかる個人情報保護対策チェックリスト

（電磁的媒体・紙媒体の取扱い）

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
委託事業者に行わせる情報保護対策【運用上の対策】	○	契約にあたり、「特記事項」を付すとともに、個人情報保護法及び新宿区情報セキュリティポリシーを遵守させる。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠させる。
	○	契約履行の間、特記事項に基づき立入り調査等を受けさせるとともに、委託先に対し速やかに状況報告をさせる。
	○	再委託先がある場合には、委託先との間に立入り調査等ができる契約内容を付すとともに、必要に応じて又は定期的に立入り調査等を実施させる。
	○	取扱責任者及び取扱者をあらかじめ指定させ、区に報告させる。
	○	区が作成した業務フローに基づき、業務を行わせる。
	○	取扱う個人情報の管理について、必要に応じて又は定期的に確認する体制を構築させる。
	○	個人情報を含むデータを作成する必要が生じた場合は、パスワードを付してデータを暗号化させる。電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用させ、手渡しで行わせる。
	○	個人情報を手交する場合は、鍵付きカバン等を使用して運搬させる。
	○	個人情報の受け渡しにあたっては、管理簿に記載させる。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにさせる。
	○	個人情報は、施錠できる金庫又はキャビネット等に保管させる。
	○	業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却させ、電子データは消去させる。また、区に電子データの消去を行ったことの報告書を提出させる。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備させ、区と緊急時の連絡体制や対応手順を確認させる。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに区と今後の対応を協議させる。
委託事業者に行わせる情報保護対策【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定させる。
	○	通信内容は暗号化させ、通信途上の個人情報の盗用、改ざん、成りすましを防止させる。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じさせ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御させる。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用させる。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止させる。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定させるとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底させる。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得させる。取得したログは、定期的に分析させる。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備させる。
	○	入退室管理等により情報資産の危殆化を防止させる。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にさせる。