資料60

個人情報保護管理運営会議　付議事項

件名	新宿区外転出者の現地調査に係る業務の委託について

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
健康部医療保険年金課）

事業の概要

事業名	新宿区外転出者の現地調査業務の委託
担当課	（仮称）滞納対策課（令和７年４月より滞納整理業務を一元的に担当する部門）
目　的	区外に転出した滞納者の居住実態を把握し、効率的な滞納整理を実施する。
対象者	特別区民税・都民税・森林環境税、軽自動車税（種別割）の滞納者及び国民健康保険料の滞納世帯主のうち、新宿区外に転出した者
事業内容	１　概要 令和７年１月より、特別区民税・都民税・森林環境税、軽自動車税（種別割）及び国民健康保険料の滞納情報を一元的に管理するシステムを導入しており、令和７年４月からは、当該債権に係る滞納整理業務を一元的に担当する部門を設置する予定である。 それに伴い、令和２年度より税務課で実施している新宿区外転出者の現地調査業務の委託範囲を拡大し（令和２年度第３回情報公開・個人情報保護審議会了承済み）、国民健康保険部門においても、区外滞納者の居住実態調査を委託することで、調査結果を基にした効率的な滞納整理に取り組むことが可能となる。 ２　個人情報保護管理運営会議への付議内容 区外に居住する滞納者の居住地への訪問調査を実施し、居住実態の確認及び連絡票の手渡し等を行う。 ３　対象者数 最大８００件 ※個人情報の流れは、資料６０－１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　新宿区外転出者の現地調査に係る業務の委託について

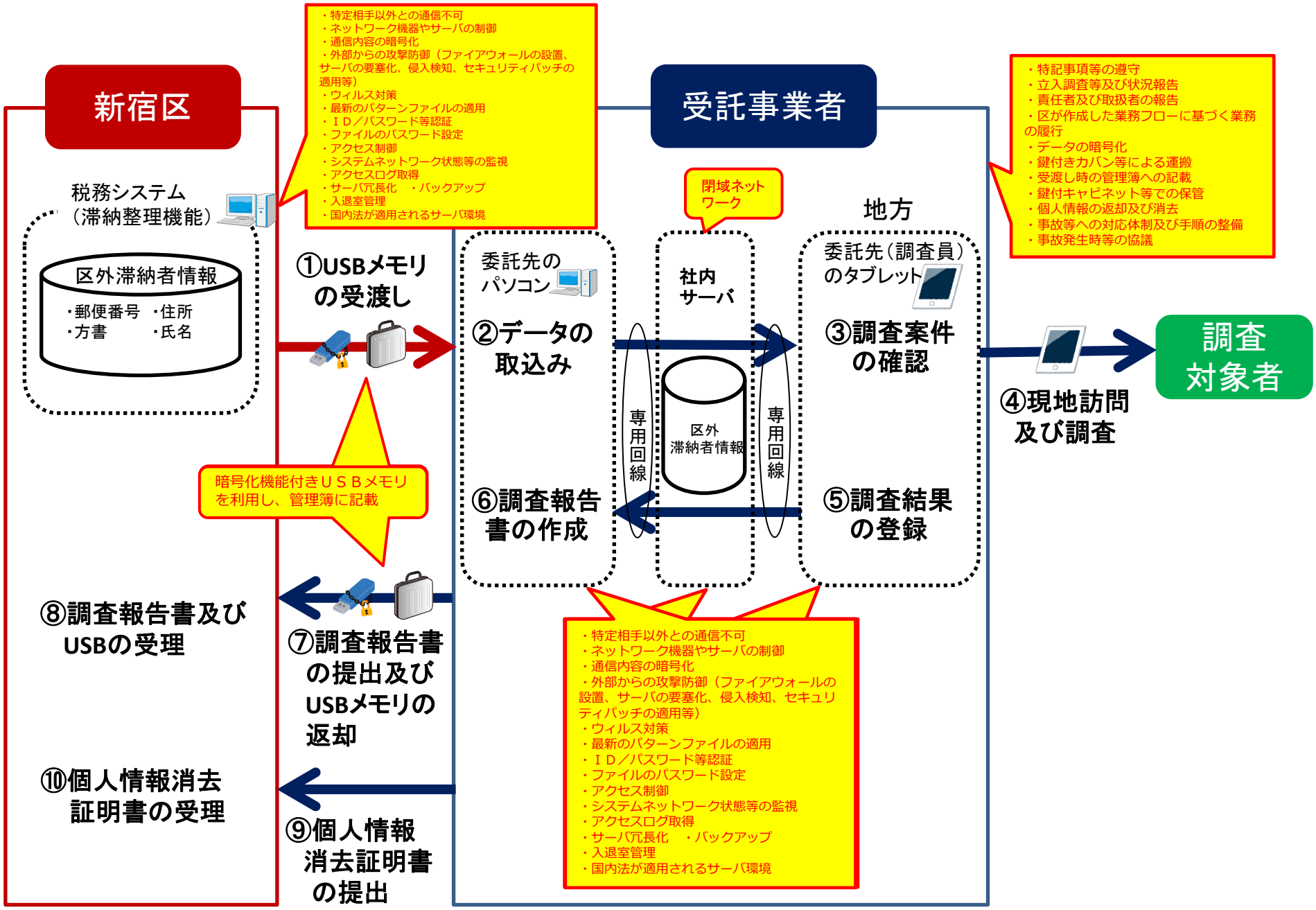
※太字ゴシック（下線）が、令和２年度第３回新宿区情報公開・個人情報保護審議会了承済の内容からの変更箇所

保有課(担当課)	**（仮称）滞納対策課（令和７年４月より滞納整理業務を一元的に担当する部門）**
登録業務の名称	新宿区外転出者の現地調査業務委託
委託先	未定（入札方式により選定を予定）（プライバシーマーク取得事業者を予定）
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 特別区民税・都民税・森林環境税、軽自動車税（種別割）の滞納者**及び国民健康保険料の滞納世帯主のうち、新宿区外に転出した者** ２　記録項目 《委託先に提供する項目》 新宿区外居住滞納者の郵便番号、住所、方書、氏名 《委託先に収集させる項目》 居住の有無、現地の外観状況
処理させる情報項目の記録媒体	電磁的媒体（ＵＳＢメモリ、委託先パソコン及び調査用タブレット）
委託理由	電話、郵送等でも接触できない区外に居住する滞納者について、専門業者が現地確認、調査を行うことで、効率的かつ効果的に居住の実態を把握し、滞納整理につなげるため。
委託の内容	区外に居住する滞納者の居住地への訪問調査を実施し、居住実態の確認及び連絡票の手渡し等を行い、報告書によりその結果を報告させる。
委託の開始時期及び期限	**令和７年７月上旬から令和８年２月２７日まで（次年度以降も、結果の検証をしながら事業を継続する予定）**
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

新宿区外転出者の現地調査業務の個人情報の流れ

（資料６０－１）

※令和２年度より税務課で実施している業務に、国民健康保険部門を追加する。



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「－」	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。
	○	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。
	○	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。
	○	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。
	○	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。