

個人情報保護管理運営会議 付議事項

件 名	ふるさと納税管理業務の委託について(委託内容の変更)
--------	----------------------------

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：総務部総務課）

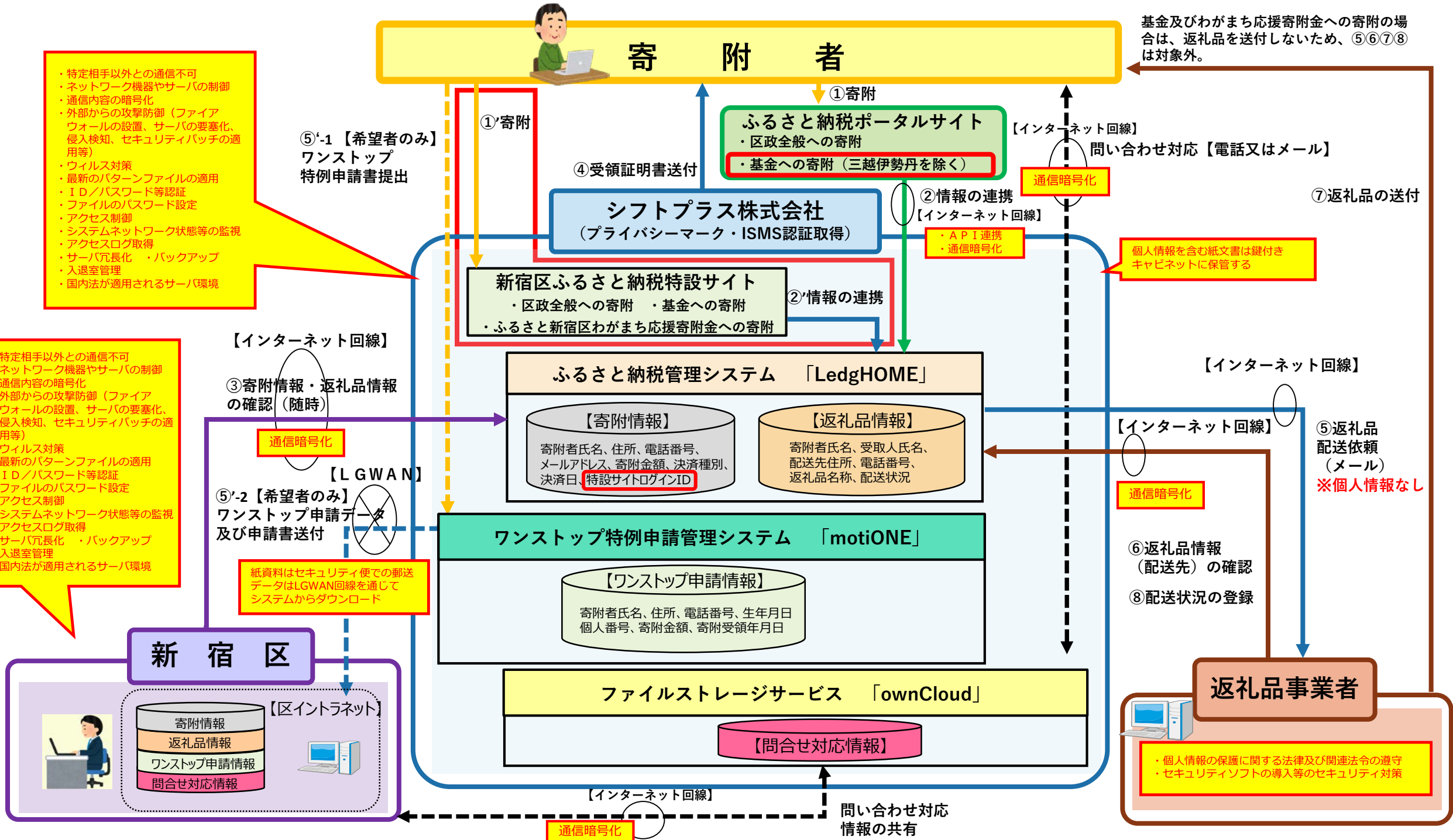
事業の概要

事業名	ふるさと納税管理業務
担当課	総務課
目 的	ふるさと納税の返礼品の企画・開発、返礼品の在庫・配送状況の管理、寄附者への対応等の一連の業務を円滑に行うため。
対象者	新宿区へ寄附した方（返礼品の対象となるのは区外在住者で、区政全般へ寄附した方のみ）
事業内容	1 概要 区では令和5年10月より、区政全般への寄附についてふるさと納税返礼品を導入しており、ふるさと納税ポータルサイト（以下、「ポータルサイト」という。）で寄附を募ることで、寄附機会の拡大と寄附者の利便性向上を図っている。また、寄附の受入に係る収納事務や証明書発行、ワンストップ特例事務といった管理事務を中間事業者へ業務委託することで、業務の効率化を図っている。 一方、ふるさと新宿区わがまち応援寄附金については、技術的にポータルサイトでの受入ができず、キャッシュレス決済にも対応できていない。また、子ども未来基金等の各種基金への寄附については、ポータルサイト（ふるさとチョイスのみ）に掲載しているが、寄附受入に伴う書類発送等の事務は、職員が行っており相当数の事務負担が発生している。 上記の課題に対応するため、区政全般への寄附だけでなく基金への寄附やふるさと新宿区わがまち応援寄附金への寄附についてもインターネット申込及びキャッシュレス決済に対応する「新宿区ふるさと納税特設サイト」を開設し、当該サイトの管理・運営を、中間事業者へ委託する。また、基金への寄附について記載するポータルサイトを増やすとともに、ポータルサイト経由の基金への寄附受入に伴う書類発送等の事務についても中間業者に委託する。 2 個人情報保護管理運営会議への付議内容 （1）業務委託 ・新宿区ふるさと納税特設サイトの管理、運営 ・新宿区ふるさと納税特設サイト及びポータルサイト経由の基金等への寄附受入れに係る書類発送等の事務 3 対象者数 約500人 ※個人情報の流れは、資料7-1のとおり

件名 ふるさと納税管理業務の委託について

※太字ゴシック(下線)が、令和5年度第9回個人情報保護管理運営会議承認済みの内容からの変更箇所

保有課(担当課)	総務課(委託内容の変更)
登録業務の名称	寄附の受領 寄附金税額控除に係る申告の特例に関する事務
委託先	シフトプラス株式会社 (ISMS 認証・プライバシーマーク取得事業者)
委託に伴い事業者処理させる情報項目(だれの、どのような項目か)	1. 寄附情報 寄附者氏名、住所、電話番号、メールアドレス、寄附金額、決済種別、決済日、返礼品情報、 特設サイトログイン ID (ワンストップ特例申請書を提出した寄附者分のみ) 生年月日、個人番号 2. 返礼品情報 寄附者氏名、受取人氏名、配送先住所、電話番号、返礼品名称、配送状況
処理させる情報項目の記録媒体	紙及び電磁的媒体(委託先のパソコン及びサーバ)
委託理由	本事業は民間事業者のノウハウ、創意工夫を最大限活用することが有効であり、かつ大量の業務を円滑かつ効率的に遂行するため。
委託の内容	1. 返礼品の企画・開発 2. 返礼品の在庫・配送状況の管理 3. ふるさと納税ポータルサイト 及び新宿区ふるさと納税特設サイト の掲載情報管理・PR 4. 寄附の受入・寄附者対応(区政全般への寄附・ 各種基金等への寄附) 5. ワンストップ特例受付・処理(区政全般への寄附・ 各種基金等への寄附)
委託の開始時期及び期限	令和6年7月1日から令和7年3月31日まで(次年度以降も同様の業務委託を行う。)
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



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。
	○	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ある場合は、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。
	○	返礼品業者に対しても、監督を含めた個人情報保護対策を行う旨取り決めを交わし、契約させる。
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ある場合は、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。
	○	返礼品業者に対しても、監督を含めた個人情報保護対策を行う旨取り決めを交わし、契約する。
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。