資料39

個人情報保護管理運営会議　付議事項

件名	納税通知書等の印字及び封入封緘に係る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	特別区民税・都民税・森林環境税及び軽自動車税（種別割）の納税通知書、過誤納金還付・充当通知書等送付
担当課	税務課
目　的	納税通知書、過誤納金還付・充当通知書、過誤納金還付請求書の印字及び封入封緘業務を委託することで事務の効率化を図るため。
対象者	特別区民税・都民税・森林環境税及び軽自動車税（種別割）の過誤納金発生者
事業内容	１　概要 現在、区では、特別区民税・都民税・森林環境税（以下「住民税」という。）及び軽自動車税（種別割）の税額が決定または変更した際に、納税通知書を対象者に送付している。住民税（普通徴収分）及び軽自動車税の納税通知書については、事務の効率化を図るため、事業者に印字、封入封緘業務を委託している（昭和６０年度第２回東京都新宿区個人情報保護審議会及び平成３０年度第８回情報公開・個人情報保護審議会了承済み）。 この度、従来から委託していた業務に加え、「過誤納金還付・充当通知書及び過誤納金還付請求書の印字、封入封緘」業務についても、住民税（普通徴収分）納税通知書と併せて委託することで、さらなる事務の効率化を図る。 ２　個人情報保護管理運営会議への付議内容 ① 過誤納金還付・充当通知書・過誤納金還付請求書の印字処理業務 ② 過誤納金還付・充当通知書・過誤納金還付請求書の封入封緘業務（一部、住民税（普通徴収分）の納税通知書と同封） ３　追加となる対象通知件数（年間） 約１０，０００件 （参考：令和５年度過誤納金還付通知書発送件数実績：９，６７９通　） ※個人情報の流れは、資料３９－１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　納税通知書等の印字及び封入封緘に係る業務の委託について（委託内容の追加）

※太字ゴシック（下線）は、平成３０年度第８回情報公開・個人情報保護審議会了承済み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・森林環境税 軽自動車税
委託先	株式会社コタニ（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）	資料３９－２のとおり
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ＰＣ及びＤＶＤ等）
委託理由	納税通知書の印字及び封入封緘業務に加え、過誤納金還付・充当通知書等についても同一事業者に印字及び封入封緘業務を委託することで事務の効率化を図るため。
委託の内容	納税通知書の印字及び封入封緘業務 **過誤納金還付・充当通知書等の印字処理業務** **過誤納金還付・充当通知書等の封入封緘業務（一部、住民税（普通徴収分）の納税通知書と同封）**
委託の開始時期及び期限	**令和６年１１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

納税通知書等の封入封緘に係る個人情報の流れ

（資料３９－１）

※赤色の部分が今回の付議事項

新宿区

税務システム

対象者データ

個人情報の項目については、
資料39－2のとおり

①対象者データ出力

イントラパソコン

・特定相手以外との通信不可
・ネットワーク機器やサーバの制御
・通信内容の暗号化
・外部からの攻撃防御（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）
・ウィルス対策
・最新のパターンファイルの適用
・ＩＤ／パスワード等認証
・ファイルのパスワード設定
・アクセス制御
・システムネットワーク状態等の監視
・アクセスログ取得
・サーバ冗長化　・バックアップ
・入退室管理
・国内法が適用されるサーバ環境

⑦職員による
納品物の検査

・鍵付きカバン等による運搬
・受渡し時の管理簿への記載

②対象者データの提供
（DVD等・手渡し）

⑥納税通知書、過誤納金還付・充当通知書及び過誤納金還付請求書の対象者データの返却及び封入封緘物の納品
（DVD等及び紙・手渡し）

委託事業者

③封入用封筒及び
封入物（納税通知書等）
の作成

委託先PC

④対象者データを確認し、
納税通知書、過誤納金還付・充当通知書及び過誤納金還付請求書に印字

対象者データ

個人情報の項目については、
資料39－2のとおり

・特定相手以外との通信不可
・ネットワーク機器やサーバの制御
・通信内容の暗号化
・外部からの攻撃防御（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）
・ウィルス対策
・最新のパターンファイルの適用
・ＩＤ／パスワード等認証
・ファイルのパスワード設定
・アクセス制御
・システムネットワーク状態等の監視
・アクセスログ取得
・サーバ冗長化　・バックアップ
・入退室管理
・国内法が適用されるサーバ環境

⑤納税証明書等
を封入封緘

・特記事項等の遵守
・立入調査等及び状況報告
・責任者及び取扱者の報告
・区が作成した業務フローに基づく業務の履行
・データの暗号化
・鍵付きカバン等による運搬
・受渡し時の管理簿への記載
・鍵付キャビネット等での保管
・個人情報の返却及び消去
・事故等への対応体制及び手順の整備
・事故発生時等の協議

⑧納税通知書等（当初通知）発送分は、
委託先が郵便局へ搬入し、区民あてに発送
⑧'納税通知書等（随時通知）発送分は、
区職員が後納郵便で区民あてに発送

区民

委託に伴い事業者に処理させる項目

【１．　住民税納税通知書】

賦課年度、相当年度、郵便番号、住所、方書、納税義務者氏名、納税管理人等氏名、賦課住所（1 月 1 日現在）、納税通知書番号、給与特徴番号、一連番号、カスタマーバーコード、発付年月日、所得割額、均等割額、森林環境税額、合計額、給与特徴・既課税額、年金特徴税額、差引普通徴収税額、配当割・株式譲渡割額控除不足額、口座情報（振替方法、金融機関コード、支店コード、口座番号）、普通徴収（期別、納期限、税額、既納付額、充当額、今回納付額）、年金特別徴収（徴収月、税額、過誤納金）、年金特別徴収翌年度仮徴収金額、支払者法人番号、公的年金項目、年金保険者、所得項目、所得金額、給与収入額、公的年金等収入額、特別障害、普通障害、寡婦、特別の寡婦、寡夫、勤労学生、生活保護、未成年者、ひとり親、家屋敷事業所、配偶者控除（内、老人）、同一生計配偶者、特定扶養数、老人扶養数（内、同居老親数）、16 歳未満の扶養数、その他の扶養数、内普通障害者数、内特別障害者数、内同居特別障害者数、所得控除項目、所得控除額、基礎控除、所得控除合計額、課税標準額項目、課税標準額、所得割額項目、特別区民税所得割額、都民税所得割 額

【２．　納付書】

賦課年度、相当年度、税目、合計額、納付番号、確認番号、納付区分、納税通知書番号、年度期別標識、税額、延滞金金額、期限日付、氏名、コンビニバーコードデータ、郵便番号、住所、ＯＣＲライン

【３．　軽自動車税納税通知書】

賦課年度、税目、合計額、納付番号、確認番号、納付区分、納税通知書番号、年度期別標識（車両番号）、税額、延滞金金額、納期限日付、氏名、カスタマーバーコード、コンビニバーコードデータ、一連番号、郵便番号、住所、住民番号、発付日、車検用証明書有効期限、ＯＣＲライン

【４．　過誤納金還付・充当通知書、過誤納金還付請求書】

税目、賦課年度、対象年度（相当年度）、**過誤納金発生事由**、口座情報（金融機関コード、**金融機関名**、支店コード、**支店名**、**預金種別コード**、**預金種別名称**、口座番号、**口座名義人氏名カナ**、**口座名義人氏名漢字**）、カスタマーバーコード、支払予定年月日、**還付処理番号**、郵便番号、住所、氏名、**再発行表示**、**通知済表示（初回発行年月日）**、発付年月日、**還付額**、納税義務者氏名、**納税義務者カナ氏名**、**還付加算金有無**、住民番号、納税通知書番号、**還付発生年月日**、軽自動車税車両番号、**国税更正年月日**、**還付加算金**、期月、**収納年月日**、**領収年月日**、**過誤納金発生時（収納額・延滞金・未納税額・未納延滞金・収納額合計・延滞金合計・未納税額合計・未納延滞金合計）**、**過誤納金（納付額・延滞金・納付額合計・延滞金合計）**、**充当（納付額・延滞金収納額）**、**充当年月日**、**充当前期別調定額（税額）**、**延滞金調定額**、**充当前後（期別収納額・延滞金収納額・期別未納額・延滞金未納額）**、**充当納付額合計**、**充当延滞金収納額合計**、**加算日数**、**還付決議年月日、会計年度、還付原因区分**

※太字ゴシック（下線）が新規に導入する項目である。

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。