資料25

個人情報保護管理運営会議　付議事項

件名	債権（経営力強化支援事業補助金返還金）回収に係る督促等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：文化観光産業部産業振興課）

事業の概要

事業名	債権（経営力強化支援事業補助金返還金）回収に係る督促等業務の委託について
担当課	産業振興課
目　的	債権（経営力強化支援事業補助金返還金）回収困難案件の解消実現のため
対象者	債権（経営力強化支援事業補助金返還金）滞納者
事業内容	1　概要 区では、令和５年度及び６年度に、区内中小企業等（法人・個人事業主）の経営力強化を図るための取組に対し、経営力強化支援事業補助金を交付した。 この補助金事業においては、概算払いを行った事業者のうち、実績報告書が未提出もしくは交付決定時と実績報告時で差額が生じた際は、当該補助金の全額または差額分の返還を求めている。 これまでは、区の職員が、郵便による通知や電話等により督促及び催告を継続的に実施しているものの、支払いに応じないことや音信不通になるほか、債務者が区外等に転出し追跡（臨戸）が困難となるなど、債権回収が十分に進まない状況にある。 区としては、債権回収に対する確固たる姿勢を債務者に示すとともに、確実に債権を回収するため、専門知識やノウハウを有する弁護士事務所に債権回収の業務を委託する。 2　個人情報保護管理運営会議への付議内容 （1）督促業務 （2）示談折衝業務 （3）合意書の作成及び郵送業務 （4）交渉記録報告書作成業務 3　対象者数 最大５８名 ※個人情報の流れは、資料２５－１のとおり

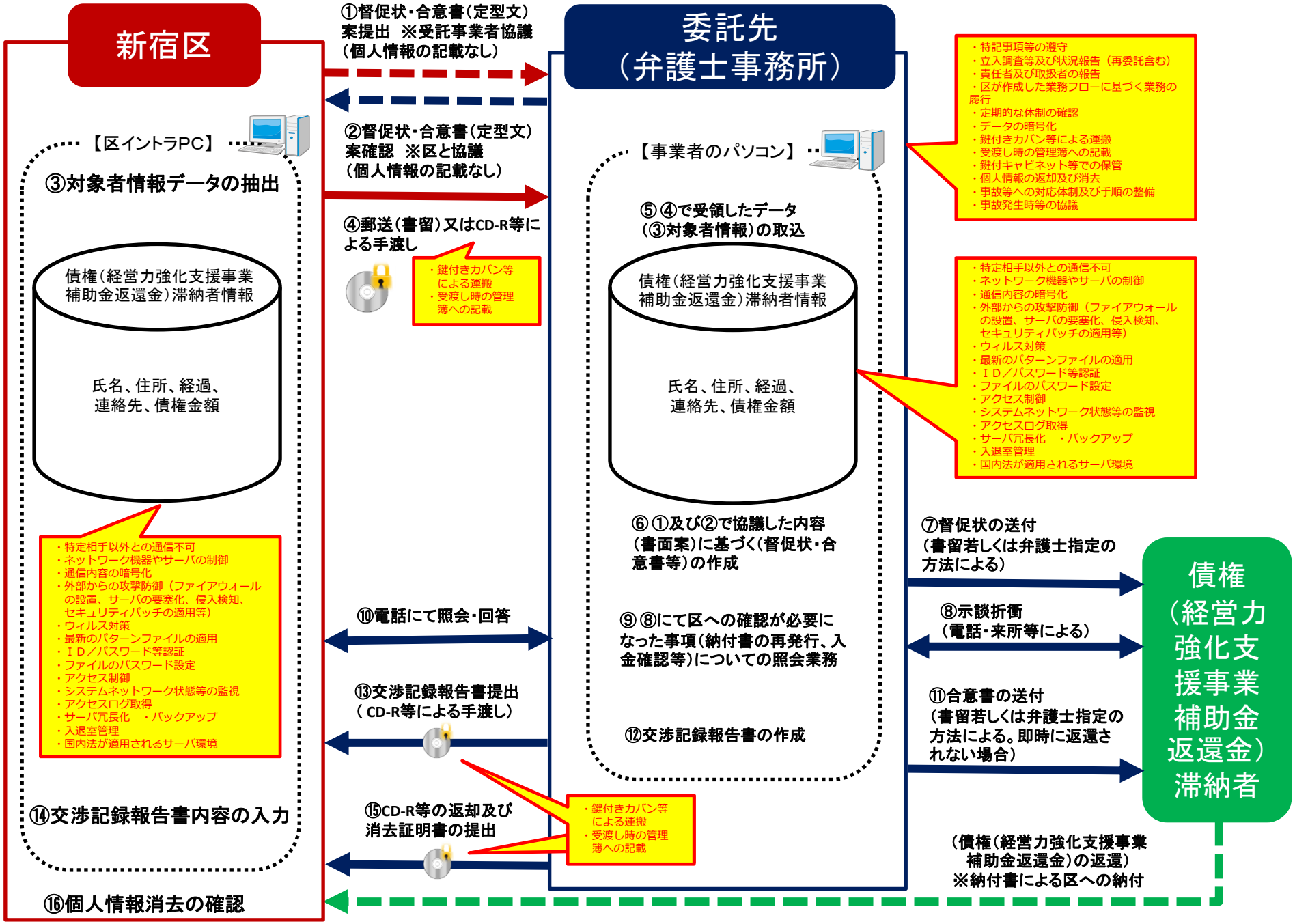
別紙(業務委託)

◇業務委託(第３条第１項第３号)

債権（経営力強化支援事業補助金返還金）回収に係る督促等業務の委託について

保有課(担当課)	産業振興課
登録業務の名称	債権（経営力強化支援事業補助金返還金）回収業務における弁護士事務委託
委託先	神田お玉ヶ池法律事務所（特命随意契約方式により選定を想定）（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 経営力強化支援事業補助金返還金滞納者 ２　情報項目 氏名、住所、連絡先、経過・交渉記録、債権金額、確定申告書・開業届を含む申請書類一式等
処理させる情報項目の記録媒体	紙及び電磁的媒体（ＣＤ−Ｒ等及び委託先のパソコン）
委託理由	債権（経営力強化支援事業補助金返還金）回収業務においては、複数回催告を行っているものの支払いに応じないことや音信不通になるほか、債務者（滞納者）の区外転出等による追跡（臨戸）が困難となるなど、他の業務と並行して業務にあたる区職員だけでは、十分な債権回収対応が進まない状況にある。 区として債権回収に対する確固たる姿勢を対象者に示し、確実に債権を回収するため、専門知識やノウハウを有する弁護士事務所に債権回収の業務を委託する。
委託の内容	１　督促業務 ２　示談折衝業務 ３　合意書の作成及び郵送業務 ４　交渉記録報告書作成業務
委託の開始時期及び期限	令和７年９月中旬から令和８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

【債権（経営力強化支援事業補助金返還金）回収に係る督促等業務における個人情報の流れ】　（資料２５－１）



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。