

個人情報保護管理運営会議 付議事項

件 名	延長保育料等におけるコンビニ収納等の導入について
--------	--------------------------

内容は別紙のとおり

要綱の根拠

◇第3条第1項第3号（外部結合、業務委託）

（担当部課：子ども家庭部保育課、教育委員会事務局学校運営課）

事業の概要

事業名	延長保育料等におけるコンビニ収納等の導入について
担当課	保育課、学校運営課
目的	延長保育料等について、コンビニエンスストア（以下「コンビニ」という。）及び電子マネー納付を導入することにより納付方法を拡充し、利便性の向上を図る。
対象者	延長保育料等の納付義務者
事業内容	<p>1 概要</p> <p>現在、延長保育料、年末保育料、子ども園預かり保育料（給食費を含む）、基本保育料について、保育課、特別出張所、金融機関、口座振替での納付に対応している。また、幼稚園預かり保育料について、学校運営課、特別出張所、金融機関、口座振替での納付に対応している。</p> <p>これらの納付方法に加え、令和9年4月からはコンビニ及び電子マネーでの納付を導入することで、区民の利便性の向上を図る。</p> <p>2 個人情報保護管理運営会議への付議内容</p> <p>(1) 外部結合</p> <p>収納サービス提供事業者が有する収納データセンターと区のイントラパソコンが結合されるため</p> <p>(2) 業務委託</p> <p>納付された延長保育料等の収納データの作成及び管理、区への収納データの送信等を委託するため</p> <p>3 対象者数</p> <p>保育課 延べ約600人（納付書件数：約1,000件／年）</p> <p>学校運営課 延べ約260人（納付書件数：約280件／年）</p> <p>※ 個人情報の流れは、資料7-1のとおり</p>

件名 延長保育料等におけるコンビニ収納等の導入に伴う収納サービス提供事業

者との外部結合について

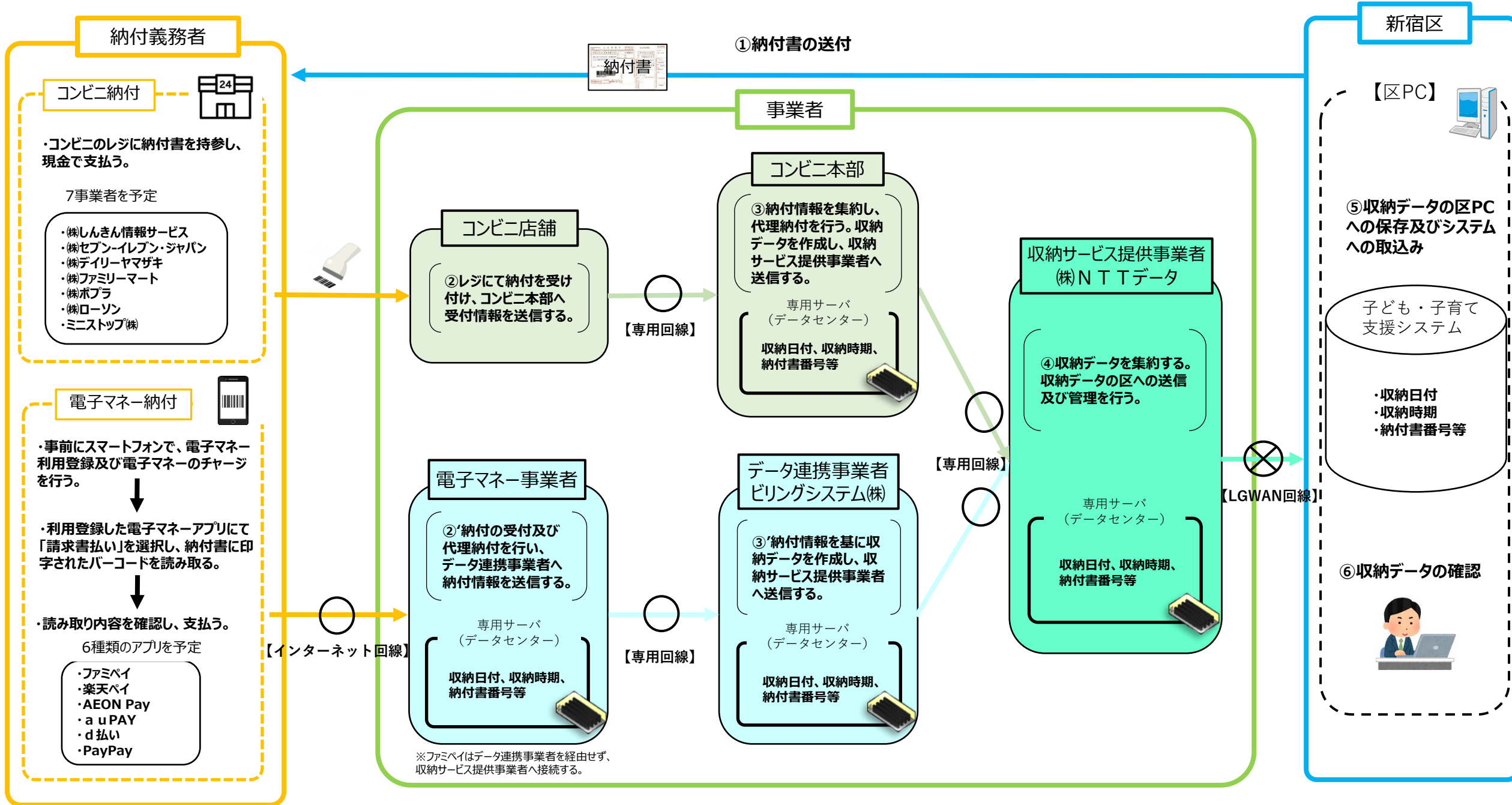
保育課(担当課)	保育課、学校運営課
登録業務の名称	延長保育料等の収納
結合される情報項目(だれの、どのような項目か)	<p>1 個人の範囲 延長保育料等の納付義務者</p> <p>2 情報項目 レコード区分、ファイル作成日、代行会社コード、収納機関コード、利用区分、データ識別コード、<u>収納日付、収納時間、バーコード情報(識別コード、メーカーコード、年度、納付書番号、再発行区分、支払い期限日、印紙フラグ、支払い金額)</u>、<u>収納店舗コード</u>、<u>支払い予定日、経理処理日、小売業企業コード</u>、速報件数合計、速報金額合計、<u>確報件数合計、確報金額合計、速報取消件数合計、速報取消金額合計</u>、レコード総件数</p> <p>※ 電子マネー事業者は下線の情報項目のみ取り扱う。</p>
結合の相手方	株式会社NTT データ (プライバシーマーク及び ISMS 認証取得事業者)
結合する理由	収納サービス提供事業者が有する収納データセンターとの外部結合により区が収納データを取得するため
結合の形態	LGWAN 回線を利用して、収納サービス提供事業者の収納データセンターと区のイントラネット端末を接続する。
結合の開始時期と期間	令和8年5月～令和9年3月(次年度以降も、同様の外部結合を行う。)
情報保護対策	別添チェックリストのとおり

件名 延長保育料等におけるコンビニ収納等の導入に伴う収納データ作成等業務 の委託について

保有課(担当課)	保育課、学校運営課
登録業務の名称	延長保育料等の収納
委託先	<ol style="list-style-type: none"> 1 コンビニ事業者 コンビニの運営事業者 2 電子マネー事業者 電子マネー決済アプリの運営事業者 3 データ連携事業者 ビリングシステム株式会社 (プライバシーマーク及び ISMS 認証取得事業者) 4 収納サービス提供事業者 株式会社NTT データ (プライバシーマーク及び ISMS 認証取得事業者)
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)	<ol style="list-style-type: none"> 1 個人の範囲 延長保育料等の納付義務者 2 情報項目 レコード区分、ファイル作成日、代行会社コード、収納機関コード、利用区分、データ識別コード、<u>収納日付、収納時間、バーコード情報(識別コード、メーカーコード、年度、納付書番号、再発行区分、支払い期限日、印紙フラグ、支払い金額)</u>、<u>収納店舗コード</u>、<u>支払い予定日</u>、<u>経理処理日</u>、<u>小売業企業コード</u>、<u>速報件数合計</u>、<u>速報金額合計</u>、<u>確報件数合計</u>、<u>確報金額合計</u>、<u>速報取消件数合計</u>、<u>速報取消金額合計</u>、レコード総件数 ※ 電子マネー事業者は下線の情報項目のみ取り扱う。
処理させる情報項目の記録媒体	電磁的媒体(委託先のサーバ)
委託理由	<ol style="list-style-type: none"> 1 コンビニ事業者 事業者が運営するコンビニを利用した納付があった場合の受付及び納付情報の収納サービス提供事業者への送信のため 2 電子マネー事業者 事業者が運営する電子マネー決済アプリを利用した納付があった場合の受付及び納付情報のデータ連携事業者又は収納サービス提供事業者への送信のため 3 データ連携事業者 電子マネー事業者からの納付情報に基づき収納データを作成し収納サービス提供事業者へ送信するため

	<p>4 収納サービス提供事業者 コンビニ事業者、電子マネー事業者及びデータ連携事業者からの収納データの集約及び管理を行い、区へ収納データを送信するため</p>
委託の内容	<p>1 コンビニ事業者 コンビニ納付の受付、納付データの管理、収納データの作成、収納サービス提供事業者への収納データの送信</p> <p>2 電子マネー事業者 電子マネー決済アプリによる納付の受付、納付データの管理、データ連携事業者への納付情報の送信又は収納サービス提供事業者への収納データの送信</p> <p>3 データ連携事業者 電子マネー事業者からの納付情報に基づく収納データの作成、収納サービス提供事業者への収納データの送信</p> <p>4 収納サービス提供事業者 コンビニ事業者、電子マネー事業者及びデータ連携事業者からの収納データの集約及び管理、区への収納データの送信</p>
委託の開始時期及び期限	令和8年5月～令和9年3月（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	別添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	別添チェックリストのとおり

延長保育料等におけるコンビニ収納等に係る個人情報の流れ



4 外部結合にかかる個人情報保護対策チェックリスト

	・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
区が行う情報保護対策 【運用上の対策】	○	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。
	○	必要に応じて、事業者への立入り調査等を実施するとともに、結合先に対し速やかに状況報告をするよう指導する。
	○	システム上で不要となった電子データを削除し、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、結合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、直ちに結合先と今後の対応を協議する。
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。

4 外部結合にかかる個人情報保護対策チェックリスト

	・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
結合先に行わせる 情報保護対策 【運用上の対策】	○	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。
	○	必要に応じて、事業者への立入り調査等を受けさせるとともに、結合先に対し速やかに状況報告をさせる。
	○	システム上で不要となった電子データを削除させ、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。
結合先に行わせる 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させる。
	○	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。	

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「-」	個人情報保護対策
委託にあたり区が行う 個人情報保護対策 【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。
委託にあたり区が行う 個人情報保護対策 【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「-」	個人情報保護対策
委託事業者に行わせる 個人情報保護対策 【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。
委託事業者に行わせる 個人情報保護対策 【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。	