

個人情報保護管理運営会議 付議事項

件 名	(仮称) 新宿環境アクションポイントアプリシステムの開発等について
--------	-----------------------------------

内容は別紙のとおり

要綱の根拠

◇第3条第1項第3号（電算処理、外部結合、業務委託、指定管理）

（担当部課：環境清掃部ごみ減量リサイクル課）

事業の概要

事業名	(仮称) 新宿環境アクションポイントのアプリ化について
担当課	ごみ減量リサイクル課
目 的	現行システムに加えてアプリ化することで、より多くの区民の利用を促進し、環境に配慮した行動を意識付け、習慣化を目指すとともに、区民の利便性の向上を図る。
対象者	アプリを利用する区民等
事業内容	1 概要 区では、平成20年度より、新宿エコ自慢ポイント（アプリ化と同時に名称変更予定「(仮称) 新宿環境アクションポイント」）事業として、ごみの発生抑制や二酸化炭素の削減に寄与する行動や環境問題の学習等、環境を配慮した行動を行った者に対し、その内容に応じて発行されるポイントを付与し、ポイント数に応じて環境に配慮した特典を渡している。また、年間のポイント上位者を表彰しており、利用者の環境配慮行動を促している。 事業の流れについて、まず、受付窓口（新宿リサイクル活動センター・西早稲田リサイクル活動センター・環境学習情報センター・新宿区役所ごみ減量リサイクル課）で登録用紙を提出し、IDが入った登録カードの発行手続きを行う。その後、登録カードと新宿区食品ロス削減協力店の利用時に発行するスタンプを押したレシート等を受付窓口で提示し、登録カードに印字されているバーコードを受付窓口職員が端末に読み込むことにより、ポイントが付与される。付与されたポイントについては、ポイント数に応じて、受付窓口にて景品を受け取ることができる。また、付与されたポイントは、インターネットサイトにログインすることで確認することが可能である。 このたび、より多くの区民の利用を促進し、環境に配慮した行動を意識付け、習慣化を目指すとともに、区民の利便性を向上させるため、当該事業のアプリを開発する。アプリ化による変更点は、以下のとおり。 (1) 参加者IDは、アプリを利用登録することで自動的に付与される。 (2) ポイント付与は、食品ロス削減協力店等に設置する店舗ICカードを参加者がアプリで読み込むことで自動的にポイントが付与される。 (3) 付与されたポイントは、アプリで確認できるようになる。 ※アプリ化することにより、アプリのシステム開発や、当該システムと区のイントラネットパソコンとの外部結合、当該システム管理等の業務委託、指定管理者の情報項目の記録媒体の変更が必要となるため付議する。 2 個人情報保護管理運営会議への付議内容 (1) 電算処理 Microsoft Azure、Google データベースを活用し、(仮称) 新宿環境アクションポイントアプリシステムを構築する。 (2) 外部結合 構築した(仮称) 新宿環境アクションポイントアプリシステムのユーザデータやポイントログの履歴等を管理するシステムと区イントラネットとの結合により、参加者の情報を取得する。

	(3) 業務委託 上記(1)の構築を委託するとともに、システム管理、メンテナンス、ポイントログ等の集計について委託する。また、現行のシステム管理、メンテナンス、ポイントログ等の集計、窓口業務を委託する。 (4) 指定管理 現行の窓口業務を指定管理者に業務委託する。 3 対象者数 (1) 令和5年12月末時点の累計参加者数 3,980人(うち、令和5年度新規登録者数175人) (2) 令和6年度推定新規登録者数 280人 ※個人情報の流れは、資料6-1のとおり
--	---

件名 (仮称) 新宿環境アクションポイントアプリシステムの開発について

保有課 (担当課)	ごみ減量リサイクル課
登録業務の名称	新宿環境アクションポイント
記録される情報項目 (だれの、どのような項目が、どこのコンピュータに記録されるのか)	1 個人の範囲 参加者 (アプリを利用登録した区民等) 2 記録項目 ID番号 (現行: カード番号) ・郵便番号・誕生日・ニックネーム・登録年月日・処理者・登録ポイント・最終データアクセス日時・店舗情報・活動情報・配布ポイント・ポイント付与年月日 3 記録するコンピュータ (仮称) 新宿環境アクションポイントアプリシステム (Microsoft Azure で構築)
新規開発・追加・変更の理由	より多くの区民の利用を促進し、環境に配慮した行動を意識付け、習慣化を目指すとともに、区民の利便性の向上を図る。
新規開発・追加・変更の内容	(仮称) 新宿環境アクションポイントのアプリ化 (1) アプリを利用登録することで参加者IDが自動的に付与される。 (2) 食品ロス削減協力店等に設置する店舗ICカードを、参加者がアプリで読み込むことで自動的にポイント付与される。 (3) ポイントをアプリから確認できるようになる。
開発等を委託する場合における個人情報保護対策	別紙チェックリストのとおり
新規開発・追加・変更の時期	令和6年4月 開発 令和6年6月 テスト 令和6年10月 本稼働

件名 (仮称)新宿環境アクションポイントアプリシステムの外部結合について

保有課(担当課)	ごみ減量リサイクル課
登録業務の名称	新宿環境アクションポイント
結合される情報項目(だれの、どのような項目か)	1 個人の範囲 参加者(アプリを利用登録した区民等) 2 記録項目 ID番号(現行:カード番号)・郵便番号・誕生日・ニックネーム・登録年月日・処理者・登録ポイント・最終データアクセス日時・店舗情報・活動情報・配布ポイント・ポイント付与年月日 3 記録するコンピュータ 新宿環境アクションポイントアプリシステム(Microsoft Azureで構築)
結合の相手方	新宿環境アクションポイントアプリシステムサーバ
結合する理由	現行システムに加えてアプリ化することで、より多くの区民の利用を促進し、環境に配慮した行動を意識付け、習慣化を目指すとともに、区民の利便性の向上をめざす。 機械トラブル時や、入力ミス時の対応として、区職員がポイントログ履歴からポイント付与、修正等を行い、参加者のポイント付与を適正管理する。
結合の形態	インターネット回線を利用して、新宿環境アクションポイントアプリシステム(Microsoft Azure)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6年4月15日から令和7年3月31日まで(次年度以降も、同様の外部結合を行う。)
情報保護対策	別紙チェックリストのとおり

件名 (仮称) 新宿環境アクションポイントアプリシステムの構築支援及びポイントログ履歴管理・修正の委託について

保有課(担当課)	ごみ減量リサイクル課
登録業務の名称	新宿環境アクションポイント
委託先	早稲田大学
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)	参加者のID番号(現行:カード番号)・郵便番号・誕生月日・ニックネーム・登録年月日・処理者・登録ポイント・最終データアクセス日時・店舗情報・活動情報・配布ポイント・ポイント付与年月日
処理させる情報項目の記録媒体	電磁的媒体(新宿エコ自慢ポイント((仮称)新宿環境アクションポイント)アプリシステム(Microsoft Azureで構築))
委託理由	現行システムに加えてアプリ化することで、より多くの区民の利用を促進し、環境に配慮した行動を意識付け、習慣化を目指すとともに、区民の利便性の向上をめざす。 新宿環境アクションポイントアプリシステムを構築・運用するにあたり、現行システムの機器管理等を委託しており十分な実績を積んだ専門的なノウハウを有する事業者へ委託することで、統一した管理を行う。
委託の内容	1 システムの構築支援 2 ポイントログ履歴管理・修正
委託の開始時期及び期限	令和6年4月15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

件名 (仮称) 新宿環境アクションポイントアプリシステムの構築及び管理・メンテナンス業務の再委託について

保有課(担当課)	ごみ減量リサイクル課
登録業務の名称	新宿環境アクションポイント
委託先	株式会社レセプター
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)	参加者のID番号(現行:カード番号)・郵便番号・誕生日・ニックネーム・登録年月日・処理者・登録ポイント・最終データアクセス日時・店舗情報・活動情報・配布ポイント・ポイント付与年月日
処理させる情報項目の記録媒体	電磁的媒体(仮称)新宿環境アクションポイントアプリシステム(Microsoft Azureで構築)
委託理由	現行システムに加えてアプリ化することで、より多くの区民の利用を促進し、環境に配慮した行動を意識付け、習慣化を目指すとともに、区民の利便性の向上をめざす。 新宿環境アクションポイントアプリシステムを構築・管理するにあたり、現行システムの開発・管理をしている十分な実績を積んだ事業者へ再委託することで、統一的なシステムとする。
委託の内容	1 システムの構築 2 システムの管理・メンテナンス
委託の開始時期及び期限	令和6年4月15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

件名 (仮称) 新宿環境アクションポイント窓口受付等の委託について

保有課(担当課)	ごみ減量リサイクル課
登録業務の名称	新宿環境アクションポイント
委託先	特定非営利活動法人新宿環境活動ネット
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)	参加者のID番号(現行:カード番号)・郵便番号・誕生月日・ニックネーム・登録年月日・処理者・登録ポイント・最終データアクセス日時・活動情報・配布ポイント・ポイント付与年月日
処理させる情報項目の記録媒体	電磁的媒体(仮称)新宿環境アクションポイントシステム・紙媒体(登録カード)
委託理由	アプリの開発により、環境教育や環境イベントを実施している環境学習情報センターにおいて、新宿環境アクションポイント窓口受付等を委託することにより、より多くの区民の環境に配慮した行動をすぐにポイント付与し、区民の利便性向上を目指す。
委託の内容	新規登録者の受付、ポイントの付与・確認、特典の交付
委託の開始時期及び期限	令和6年4月15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

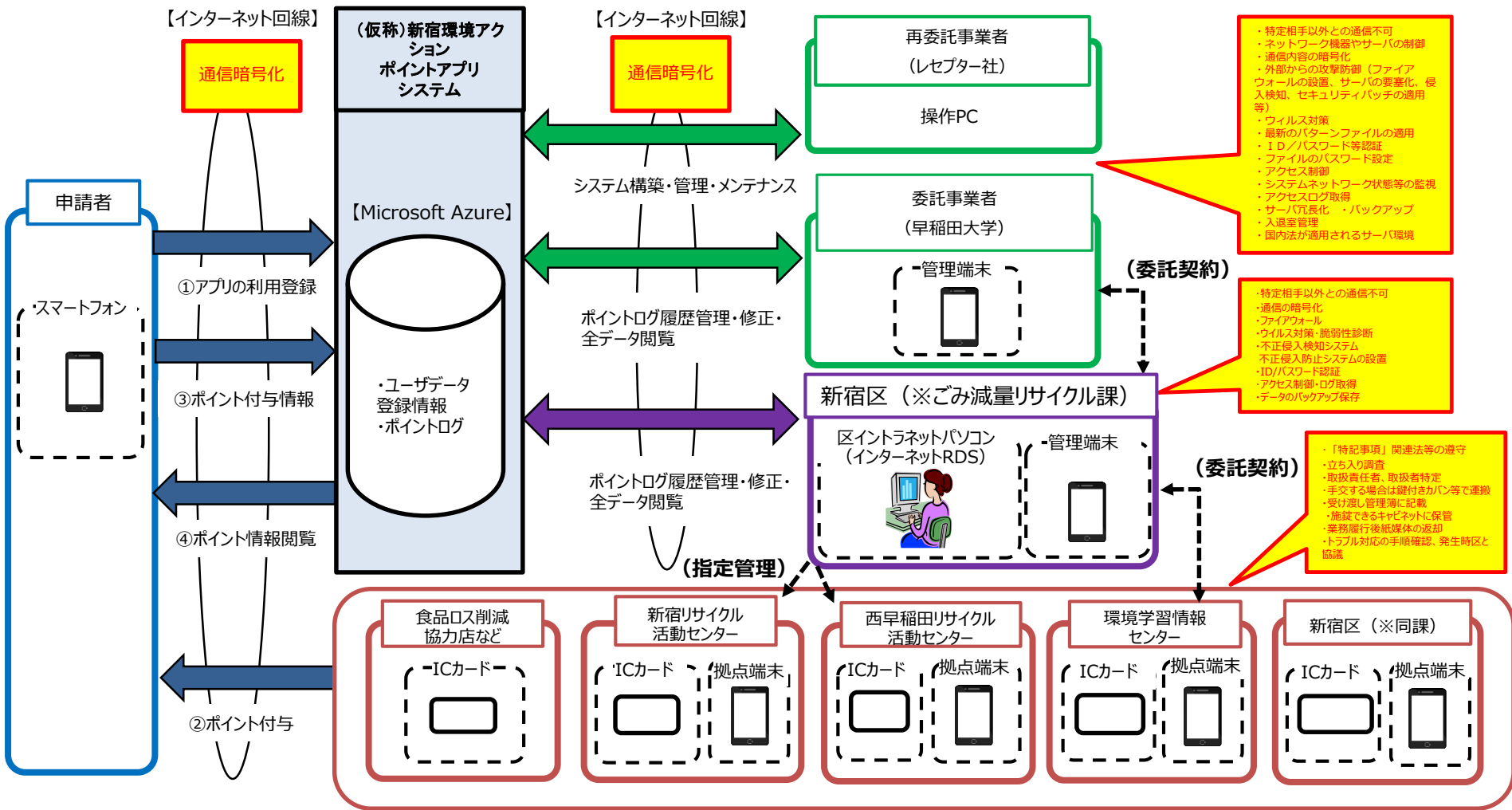
**件名 新宿区立新宿リサイクル活動センター・西早稲田リサイクル活動センター
における指定管理者制度の導入について（情報項目の記録媒体の変更）**

※太字ゴシック(下線)が平成17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

施設の名称	新宿リサイクル活動センター・西早稲田リサイクル活動センター
施設の所管課	ごみ減量リサイクル課
指定管理者の名称 *（委託先）	公益財団法人新宿区勤労者・仕事支援センター
指定管理者が取扱う個人情報の業務 *（委託に係る個人情報の業務）	(1) 施設の利用受付・登録 (2) 不用品交換事業 (3) 環境学習関連事業 (4) 施設の管理従事者の労働環境モニタリング (5) （仮称）新宿環境アクションポイント窓口受付・景品受け渡し業務
指定管理者が取扱う個人情報の項目 *（委託に係る個人情報の項目）	(1)～(3) 申請団体・登録団体・利用者・参加者の代表者等の氏名及び連絡先（住所及び電話番号） (4) 指定管理者に雇用されている職員の氏名（生年月日、性別、住所、雇用契約内容、賃金報酬支払い状況、扶養親族、健康診断の受診状況、雇用保険・社会保険の加入状況） (5) 参加者のID番号（現行：カード番号）・郵便番号・誕生月日・ニックネーム・登録年月日・処理者・登録ポイント・最終データアクセス日時・活動情報・配布ポイント・ポイント付与年月日
個人情報項目の記録媒体	(1)・(3)・(4) 紙媒体 (2) 指定管理者の電磁的媒体 <u>(5) 電磁的媒体（仮称）新宿環境アクションポイントアプリシステム(Microsoft Azure で構築)のサーバ</u>
指定管理の開始時期及び期限 *（業務委託期間）	令和6年4月15日から令和7年3月31日まで（次期指定管理期間以降も、同様の指定管理業務を行う。）
指定管理者としての情報保護対策 *（委託先の個人情報保護対策）	別紙チェックリストのとおり
指定にあたり区が行う情報保護対策 *（委託にあたり指定管理者が行う個人情報保護対策）	別紙チェックリストのとおり

(仮称) 新宿環境アクションポイントアプリシステムに係る個人情報の流れ

(資料6-1)



3 電算処理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「ー」	情報保護対策
開発等を委託する場合 における区が行う 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。
	○	区のシステム機器設置場所へ委託先が入退室する場合は、管理（申請、承認、記録）を行う。また、委託先がシステム機器を操作する場合には、事前に作業内容の報告を求め、区が承認した後に実施するよう指導するとともに、個人情報データの持出しを禁止する。
	○	プログラムの移行等を行う場合は、外部記録媒体の管理を行い、利用時は第三者漏えいがないようパスワードを施す等、利用制限を設ける。
	○	入力及び取込みテストにおいては、ダミーデータを使うよう指導する。
	○	実データを使用した検証作業は、区職員が実施する（委託先には、必要な支援のみ行わせる）。
	○	モバイルパソコン等の電子計算組織を持込む場合は、事前に区の許可をとらせ、用途は、社内事務連絡、設計書等の閲覧に限定させる。また、委託先のモバイルパソコン等と区のネットワーク、システム機器及びUSB等の記録媒体と接続をさせないように、区の職員が立ち会う。
開発等を委託する場合 における区が行う 情報保護対策 【システム上の対策】	○	データ項目定義の修正漏れによるシステム不具合等が無いよう、双方で事前に綿密なスケジュール計画やチェックシートを作成して実施する。なお、稼働にあたっては必ず仮移行を行うこととし、本稼働はシステムを使用していない時間帯（時間外・休日）に実施し、十分な検証を行う。
	○	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。

3 電算処理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「ー」	情報保護対策
開発等を委託する場合における委託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。
	○	区のシステム機器設置場所へ委託先が入退室する場合は、区の管理（申請、承認、記録）に従わせる。また、委託先がシステム機器を操作する場合には、事前に作業内容の報告をさせ、区が承認した後に実施させるとともに、個人情報データの持出しを禁止させる。
	○	プログラムの移行等を行う場合は、外部記録媒体の管理を行い、利用時は第三者漏えいがないようパスワードを施す等、利用制限を設ける。
	○	入力及び取込みテストにおいては、ダミーデータを使わせる。
	○	実データを使用した検証作業は、区職員が実施する（委託先には、必要な支援のみ行わせる）。
	○	モバイルパソコン等の電子計算組織を持込む場合は、事前に区の許可をとらせ、用途は、社内事務連絡、設計書等の閲覧に限定させる。また、委託先のモバイルパソコン等と区のネットワーク、システム機器及びUSB等の記録媒体と接続をさせないように、区の職員の立会いに応じさせる。
開発等を委託する場合における委託先に行わせる情報保護対策 【システム上の対策】	○	データ項目定義の修正漏れによるシステム不具合等が無いよう、双方で事前に綿密なスケジュール計画やチェックシートを作成して実施する。なお、稼働にあたっては必ず仮移行を行うこととし、本稼働はシステムを使用していない時間帯（時間外・休日）に実施させ、十分な検証を行わせる。
	○	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。

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「ー」	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「ー」	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「－」	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。
	－ (電子データのみ の取扱いのため)	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。
	－ (電子データのみ の取扱いのため)	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。
	－ (電子データのみ の取扱いのため)	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。
委託にあたり区が行う 情報保護対策 【システム上の対策】	○	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。
	○	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「－」	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。
	－ (電子データのみ の取扱いのため)	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。
	－ (電子データのみ の取扱いのため)	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。
	－ (電子データのみ の取扱いのため)	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。
委託事業者に行わせる 情報保護対策 【システム上の対策】	○	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。
	○	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。

8 指定管理にかかる個人情報保護対策チェックリスト

(紙媒体のみの取扱い)

	・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
指定管理にあたり 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。
	○	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、指定管理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、指定管理先と共有する。
	○	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紙媒体は返却するよう指導する。
	○	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、指定管理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。

8 指定管理にかかる個人情報保護対策チェックリスト

(紙媒体のみの取扱い)

	・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
指定管理事業者 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。
	○	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、指定管理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紙媒体は返却させる。
	○	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。