

個人情報保護管理運営会議 付議事項

件名	地方公共団体情報システム標準化に対応した税務システムへの移行等について（特定個人情報保護評価の報告）
----	--

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）

（担当部課：総務部税務課）

事業の概要

事業名	地方公共団体情報システム標準化に対応した税務システムへの移行等
担当課	税務課
目 的	「地方公共団体情報システムの標準化に関する法律」（令和3年法律第40号）（以下、「標準化法」という。）に基づき、令和7年1月から稼働する税務システムを、令和8年2月に標準化基準（標準仕様書）に適合した情報システム（以下、「標準準拠システム」という。）にバージョンアップし、ガバメントクラウド上で当該システムを運用する。
対象者	住民登録のある者及び住民登録外登録者（転出者、住民登録外課税者、特別徴収義務者、納税管理人等）
事業内容	1 概要 令和7年1月より、特別区民税・都民税（令和6年度より森林環境税を含む。以下、「個人住民税」という。）・軽自動車税（種別割）の賦課徴収業務は、事業者が開発した税務システムを利用して業務を行うこととしている（令和5年度第6回個人情報保護管理運営会議承認済）。 「地方公共団体情報システム標準化基本方針」（以下「基本方針」という。）により令和7年度末までにシステムを標準化へ対応することが求められており、令和8年2月に標準準拠システムへの移行を予定している。 併せて、標準化法第10条により、標準準拠システムの利用において、ガバメントクラウドの利用を第一に検討することとされており、セキュリティ面やコスト面等が優れていることから、デジタル庁が提供するガバメントクラウドシステムを利用し、運用を行う。 そのため、電算処理、外部結合、当該システムのサービス提供にかかる業務委託及び当該システムの保守にかかる再委託を行う。 なお、ガバメントクラウドへの移行に係る特定個人情報保護評価書の見直しについては、個人情報保護委員会の指針に定める「重要な変更」に該当するため、特定個人情報保護評価（全項目評価）を再実施する。 2 個人情報保護管理運営会議への付議内容 （1）電算処理 令和7年1月に稼働する税務システム（賦課・収納システム、滞納整理支援システム及び課税資料管理システム）から標準準拠システムに移行する。当該システムを用い、個人住民税及び軽自動車税（種別割）の賦課徴収業務を行う。 （2）外部結合 上記標準準拠システムをデジタル庁が提供するガバメントクラウド上に委託事業者に構築させ、当該システムを運用し、ガバメントクラウドとの結合を行う。 （3）業務委託 事業者が標準準拠システムをデジタル庁が提供するガバメントクラウド上に構築させる業務委託及び当該事業者が構築したシステムを、区民サービスを低下させず安定的に利用するためのシステムのサービス提供・保守にかかる業務委託を行う。 移行予定の標準準拠システムは、いずれも委託先以外が開発したシステムが含まれており、より効果的かつ効率的に業務を進めるため、当該システムの開発元に構築及び保守の一部を再委託する。

	(4) 特定個人情報保護評価書（全項目評価書）（素案） パブリック・コメントにより住民への意見聴取を行う特定個人情報保護評価書（全項目評価書）（素案）の内容について報告する。 ※特定個人情報保護評価書については、コンビニ交付の資料34-4のとおり 3 単年度あたりの対象者数 住民登録のある者、住民登録外登録者 約35万人 ※個人情報の流れは、資料35-1のとおり
--	--

件名 地方公共団体情報システム標準化に対応した税務システムへの移行について

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
記録される情報項目（だれの、どのような項目が、どのコンピュータに記録されるのか）	1 個人の範囲 住民登録のある者、住民登録外登録者 2 記録項目 資料35-2のとおり 3 記録するコンピュータ 標準化基準（標準仕様書）に適合した税務システム（委託事業者が標準準拠システムをガバメントクラウド上に構築する）
新規開発・追加・変更の理由	基本方針により、令和7年度末までにシステムを標準化することが求められており、システムベンダがガバメントクラウド上で提供する標準準拠システムへの移行を行う必要があるため。
新規開発・追加・変更の内容	個人住民税及び軽自動車税（種別割）の賦課徴収業務を継続して行うために、標準化基準（標準仕様書）に適合した税務システムをガバメントクラウド上に構築し、既存税務システムからのデータ移行を行う。
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7年1月 開発 令和7年4月 テスト 令和8年2月 運用開始

件名 地方公共団体情報システム標準化に対応した税務システムの外部結合について

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
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 住民登録のある者、住民登録外登録者 2 記録項目 資料35-2のとおり
結合の相手方	デジタル庁（ガバメントクラウドの運用主体）
結合する理由	これまでの税務システムでは、情報システム課が整備したネットワーク環境の中でのみ運用しているが、標準化後は、デジタル庁が提供するガバメントクラウド上に構築する標準準拠システムを利用するため、ガバメントクラウドとの結合が必要である。
結合の形態	情報システム課が提供する区イントラ端末から、ガバメントクラウド接続サービスを利用して、税務システムが構築されているガバメントクラウドに結合する。
結合の開始時期と期間	令和7年1月（予定）（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 地方公共団体情報システム標準化に対応した税務システムへの移行及び
サービス提供・保守に係る業務の委託について**

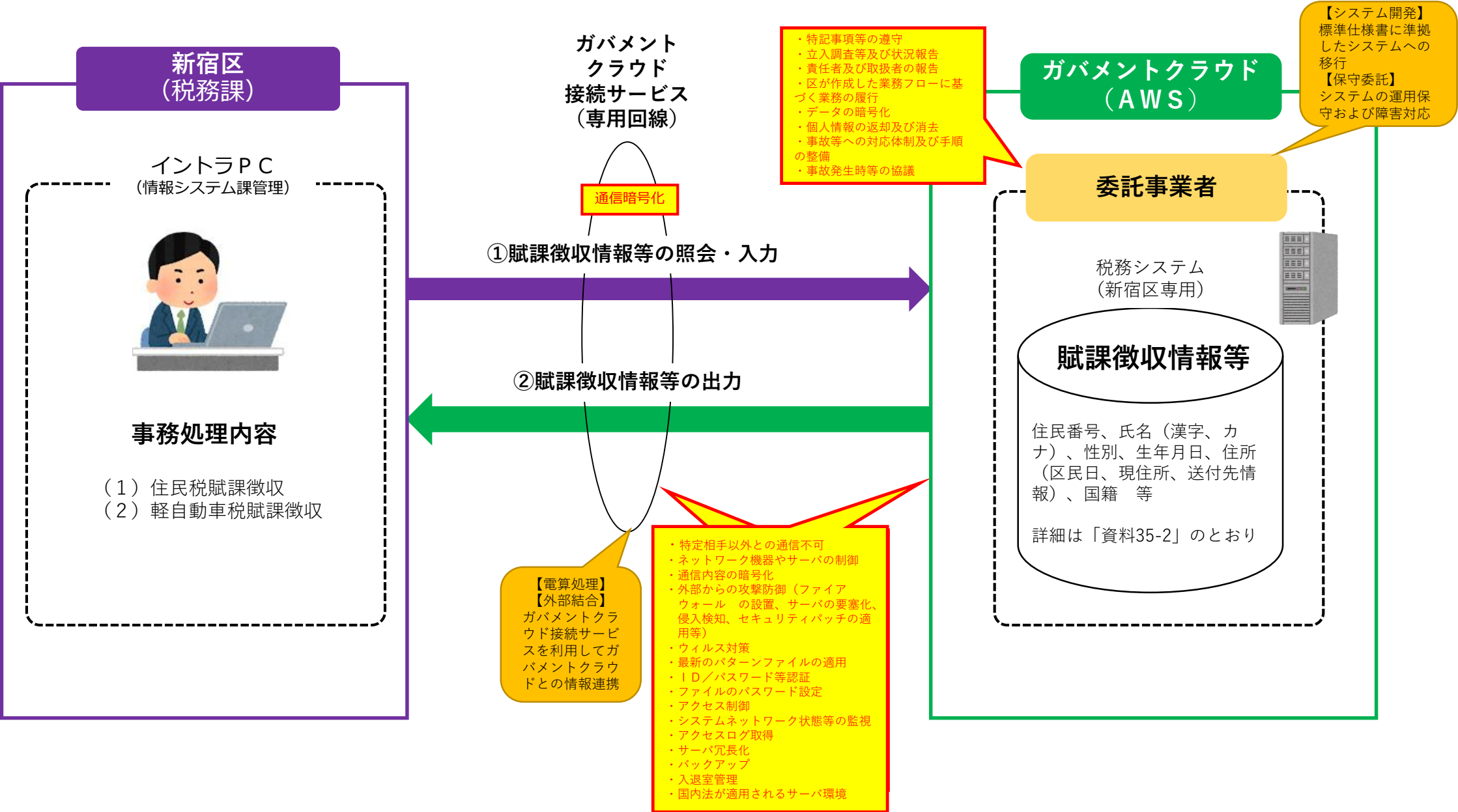
保有課(担当課)	税務課
登録業務の名称	特別区民税・都民税・森林環境税 軽自動車税
委託先	株式会社日立システムズ(プライバシーマーク、ISO27001取得済)
委託に伴い事業者処理 させる情報項目(だれの、 どのような項目か)	対象者:住民登録のある者、住民登録外登録者 情報項目:資料35-2のとおり
処理させる情報項目の記 録媒体	電磁的媒体(ガバメントクラウド上の標準準拠システム)
委託理由	限られた期間内に、迅速かつ確実に移行するため、ICTに関する高度な専門知識と実績等を有する事業者へ構築業務を委託する必要がある。 事業者が提供する税務システムを、区民サービスを低下させず安定的に利用するため、開発事業者によるシステムのサービス提供・保守にかかる業務委託が必要となる。
委託の内容	1. 税務システムの構築 2. サービス提供 3. 保守サポート 1及び3の一部を再委託する ※委託先への個人情報の提供は行わない。
委託の開始時期及び期限	令和7年1月から令和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 地方公共団体情報システム標準化に対応した税務システムへの移行及び保守に係る一部業務の再委託について

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(再委託先)	【委託先】 株式会社日立システムズ(プライバシーマーク、ISO27001取得済) 【再委託先】 上記委託先が指定
再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)	対象者:住民登録のある者、住民登録外登録者 情報項目:資料35-2のとおり
処理させる情報項目の記録媒体	電磁的媒体(ガバメントクラウド上の標準準拠システム)
再委託理由	移行予定の標準準拠システム税務システムは、いずれも委託先以外が開発したシステムが含まれており、より効果的かつ効率的に業務を進めるため、当該システムの開発元に構築及び保守の一部を再委託する。
再委託の内容	1. 税務システムの構築 2. 保守サポート ※委託先への個人情報の提供は行わない。
再委託の開始時期及び期限	令和7年1月から令和7年3月31日まで(次年度以降も、同様の再委託を行う。)
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 地方公共団体情報システム標準化に対応した税務システムへの移行について (特定個人情報保護評価の報告)

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
記録される情報項目 (だれの、どのような項目が、どのコンピュータに記録されるのか)	1 個人の範囲 住民登録のある者、住民登録外登録者 2 記録項目 資料35-2のとおり 3 記録するコンピュータ 標準化基準 (標準仕様書) に適合した税務システム (委託事業者が標準準拠システムをガバメントクラウド上に構築する)
新規開発・追加・変更の理由	基本方針により令和7年度末までにシステムを標準化することが求められており、システムベンダがガバメントクラウド上で提供する標準準拠システムへの移行を行う必要があるため。
新規開発・追加・変更の内容	個人住民税及び軽自動車税 (種別割) の賦課徴収業務を継続して行うために、標準化基準 (標準仕様書) に適合した税務システムをガバメントクラウド上に構築し、既存税務システムからのデータ移行を行う。
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7年1月 開発 令和7年4月 テスト 令和8年2月 運用開始 ※特定個人情報保護評価 (全項目評価) のスケジュールは以下のとおり 令和6年10月10日～11月8日 パブリック・コメント実施 令和6年11月中旬 第三者点検・意見反映 令和7年1月 個人情報保護委員会へ特定個人情報保護評価書提出及び区ホームページ等で公表 ※ 税務課、区政情報課、特別出張所等での窓口での閲覧は令和7年1月6日 (月) からを予定



記録される情報項目、委託に伴い事業者処理させる項目

【基本情報】

住民番号、氏名（漢字、カナ）、性別、生年月日、住所（区民日、現住所、送付先情報）、国籍、世帯情報（世帯番号、続柄）、電話番号、公的扶助

【個人住民税】

住所（賦課住所、家屋敷、事務所）、不現住情報、住登外課税地市区町村コード、課税履歴情報（収入、所得、控除、税額、期別（月割）額、納期限、延滞金、減免）、徴収方法希望、扶養者情報、専従者情報、特別徴収義務者、受給者番号、基礎年金番号、障害程度、相続人・納税管理人情報、通知書発付日、通知書番号、公示情報、課税資料情報、処理注意者情報、証明発行停止情報

【軽自動車税（種別割）】

住所（定置場）、車両情報（車台番号、車種、車両区分、登録年月日、廃車年月日、標識番号、初度検査年月）、課税履歴情報（税率区分、税額、納期限、延滞金、減免）、相続人・納税管理人情報、通知書発付日、通知書番号、公示情報、弁償金徴収有無

【収納情報】

口座情報（金融機関コード、口座番号、預金科目、名義人、納付方法、開始年月日、取消年月日）、収納履歴（収納日、領収日、充当履歴）、納付委託情報、還付情報

【滞納整理情報】

財産状態、分納情報、徴収猶予・換価猶予情報、滞納処分情報、滞納処分の停止情報、交渉情報、相談情報、職業

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。