資料70

個人情報保護管理運営会議　付議事項

件名	戸籍への氏名の振り仮名登録に関する電算処理等について

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）

（担当部課：地域振興部戸籍住民課）

事業の概要

事業名	戸籍、戸籍の附票
担当課	戸籍住民課
目　的	令和５年６月９日に戸籍法（昭和２２年法津第２２４号）の一部改正を含む「行政手続における特定の個人を識別するための番号の利用等に関する法律等の一部を改正する法律（令和５年法律第４８号。以下「改正法」という。）」が公布され、令和７年５月２６日に施行されることから、戸籍の記載事項に新たに氏名の振り仮名が追加されることとなった。 なお、同法改正の目的は、以下のとおりである。 １　行政のデジタル化の推進のための基盤整備 ２　本人確認資料としての利用（住民票やマイナンバーカード等への記載） ３　各種規制の潜脱防止
対象者	新宿区に本籍を有する者及び戸籍の附票を有する者 新宿区に戸籍の届出をした者
事業内容	１　趣旨 区では、平成２５年９月より法令に基づき戸籍副本データ管理センターとの外部結合を行っている（平成２５年度第３回情報公開・個人情報保護審議会了承済）。 また、令和６年３月１日から戸籍情報連携システムによる送受信データとして新たに戸籍届書等の情報が追加されている（令和４年度第３回情報公開・個人情報保護審議会了承済）。 今般の改正法の施行に伴い、マイナポータルを使用した振り仮名の届出が可能となる。また、振り仮名を戸籍に記載するにあたり、本籍人あて仮の振り仮名を通知する等の業務が新たに発生することから、円滑に業務を遂行するため業務委託による対応を行う。 ２　個人情報保護管理運営会議への付議内容 （１）電算処理 新たにマイナポータルを利用した氏名の振り仮名の届出を開始する。 （２）外部結合 （１）により、結合先及び送受信する情報項目を追加する。 （３）業務委託（再委託含む） 以下業務につきプロポーザルにより選定した事業者に業務委託を行う。 ①戸籍に記載される予定の振り仮名の通知書の作成・発送（再委託） ②通知に関する質問等に対応するためのコールセンターの設置運営 ③氏名の振り仮名の届出に基づき戸籍情報システムへの入力処理 ３　対象者数 新宿区に本籍を有する者　383,395 人（令和６年３月 31 日現在） 新宿区に戸籍の届出をした者及び新宿区に本籍を有する者で他の市区町村に届出をした者（件数）　　21,141 件（令和５年度実績） ※個人情報の流れは、資料６２－１及び資料６２－２のとおり

別紙(個人情報処理システム開発・変更関係)

◇電算処理(第３条第１項第３号)

件名　戸籍への氏名の振り仮名登録に関する電算処理について

保有課（担当課）	戸籍住民課
登録業務の名称	戸籍情報システム
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 新宿区に本籍を有する者 ２　記録項目 オンライン届出処理通番、オンライン届出等管理情報（署名検証結果等）、オンライン届出データ（届出日・氏名・カナ氏名・戸籍の表示・住所・連絡先）、オンライン届出事項画像 PDF、取下げ情報（届出の取下げがあった場合） ３　記録するコンピュータ マイナポータルから法務省センター、戸籍事務内連携サーバを経由し戸籍情報システムに記録される。
新規開発・追加・変更の理由	令和７年５月２６日に施行される改正法により戸籍の記載事項に新たに氏名の振り仮名が追加されることに伴い、マイナポータルを利用した氏名の振り仮名の届出（オンライン届出）が可能となるため。
新規開発・追加・変更の内容	オンライン届出情報受信対応作業 ※戸籍情報システムにおける重大なシステム変更は発生しないため、現行システムの維持運用事業者である富士通 Japan 株式会社による PTF 等随時作業にて対応予定
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２～３月頃　　PTF 適用作業・検証 令和７年５月２６日　　運用開始

別紙(電子計算機の外部結合関係)

◇外部結合(第３条第1項第３号)

件名　戸籍への氏名の振り仮名登録に関する戸籍情報システムの外部結合等について

※太字ゴシック（下線）が、令和４年度第３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）	戸籍住民課
登録業務の名称	戸籍情報システム
結合される情報項目（だれの、どのような項目か）	1　対象者 新宿区の戸籍簿に登載されている者であって、マイナポータルを利用した氏名の振り仮名の届出（オンライン届出）をした者 2　情報項目 **【マイナポータルより受信する情報（法務省センター（戸籍情報連携システム）経由）】** **オンライン届出処理通番、オンライン届出等管理情報（署名検証結果等）、オンライン届出データ（届出日・氏名・カナ氏名・戸籍の表示・住所・連絡先）、オンライン届出事項画像 PDF、取下げ情報（届出の取下げがあった場合）** **【マイナポータルに送信する情報（法務省センター（戸籍情報連携システム）経由）】** **オンライン届出処理通番、オンライン届出補正通知（届出人あて補正依頼文）** 【法務省センター（戸籍情報連携システム）に送信する情報】 ①戸籍特定ファイル　②戸籍事項　③個人特定ファイル　④氏名 ⑤身分事項　⑥個人状態　⑦除籍特定ファイル　⑧除籍個人特定ファイル ⑨除籍イメージ特定ファイル　⑩外字情報　⑪帳票ファイル ⑫全部事項イメージ（PDF）　⑬異動情報　⑭不受理申出情報 ⑮戸籍届書等をスキャンした画像情報　⑯異動入力情報　⑰受付ファイル 【法務省センター（戸籍情報連携システム）から受信する情報】 戸籍基本５情報（氏名、生年月日、続柄、本籍、筆頭者）、 情報提供用個人識別符号、他の市区町村で受理され当区に本籍のある戸籍届書等をスキャンした画像情報、異動入力情報、受付ファイル
結合の相手方	法務省センター（戸籍情報連携システム）及び**マイナポータル**
結合する理由	**令和７年５月２６日に施行される改正法により戸籍の記載事項に新たに氏名の振り仮名が追加されることに伴い、マイナポータルを利用した氏名の振り仮名の届出（オンライン届出）が可能となるため、情報項目及び結合先を追加し対応する必要がある。**
結合の形態	経由する法務省センターとの通信には総合行政ネットワーク（ＬＧＷＡＮ）を利用し、法務省から提供される戸籍事務内連携サーバにより、データの送受信を行う。
結合の開始時期と期間	**令和７年５月２６日から**（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

別紙(業務委託)

◇業務委託(第３条第1項第３号)

件名　戸籍への氏名の振り仮名登録に係る業務の委託について

保有課(担当課)	戸籍住民課
登録業務の名称	戸籍情報システム
委託先	株式会社NTT ネクシア ※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)	【新宿区に本籍を有する者に係る事項（通知管理情報）】 ①氏名（漢字）　②氏名（カナ）③生年月日　④本籍　⑤筆頭者の氏名（漢字）⑥筆頭者の氏名（カナ）　⑦住所　⑧電話による問い合わせ履歴情報 【新宿区に氏名の振り仮名の届出をした者及び新宿区に本籍を有する者に係る事項（戸籍届出情報）】 ①氏名（漢字）　②氏名（カナ）　③生年月日　④本籍　⑤筆頭者の氏名（漢字）⑥筆頭者の氏名（カナ）　⑦住所　⑧届出日　⑨届出事件名　⑩届出地
処理させる情報項目の記録媒体	電磁的媒体（戸籍情報システム） 委託事業者が通知状況等を管理するために構築する進捗管理システム
委託理由	改正法の施行により戸籍の氏名に振り仮名を記載することとなり、本籍人への仮の振り仮名の通知や問い合わせ対応、氏名の振り仮名の届出対応等の業務が新たに発生する。また、氏名の振り仮名の届出の件数は年間戸籍届け出件数の２倍以上が見込まれるため、これらの業務に適切に対応するために業務委託を実施する。
委託の内容	（１）通知に関する質問等に対応するためのコールセンターの設置運営 （２）氏名の振り仮名の届出に基づき戸籍情報システムへの入力処理
委託の開始時期及び期限	令和７年４月中旬（予定）から令和８年３月３１日まで（次年度においても令和８年６月末まで委託予定)
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

別紙(業務委託)

◇業務委託(第３条第１項第３号)

件名　戸籍への氏名の振り仮名登録に係る業務の再委託について

保有課(担当課)	戸籍住民課
登録業務の名称	戸籍情報システム
再委託先	NTT 印刷株式会社 ※プライバシーマーク取得及び ISO27001 認証取得事業者
再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)	【新宿区に本籍を有する者に係る事項（通知管理情報）】 ①氏名（漢字）　②氏名（カナ）③生年月日　④本籍　⑤筆頭者の氏名（漢字）　⑥筆頭者の氏名（カナ）　⑦住所　⑧通知管理用コード
処理させる情報項目の記録媒体	電磁的媒体（USB メモリ等)
再委託理由	振り仮名法制化に係る通知事務を実施するにあたっては、基準日時点における本籍人の氏名・住所・振り仮名等を抽出したデータを基に、膨大な数の仮の振り仮名の通知書を作成し発送する必要がある。 上記事業者は、委託先である株式会社 NTT ネクシアの同一グループ内企業であり、同社と連携しこれまでも多くの自治体で安全かつ安定的に事業を実施してきたノウハウと実績があるため、通知作成・発送業務につき再委託する。
再委託の内容	戸籍に記載される予定の振り仮名の通知書の作成・発送
再委託の開始時期及び期限	令和７年４月中旬（予定）から令和８年３月３１日まで（次年度においても令和８年６月末まで委託予定)
再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
再委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

マイナポータルを利用した振り仮名の届出に係る個人情報の流れ
（令和４年度第３回情報公開・個人情報保護審議会にて了承済みからの変更）

（資料７０－１）

◎赤点線で囲った部分が、今回の付議内容

：電子署名、署名用電子証明書

・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

届出人
来庁又は郵送

①振り仮名の届出（紙）

新宿区

戸籍情報システム

②❹戸籍情報システムへの登録
③戸籍届書等のスキャナ読込（マイナ届出の場合は原則処理不要）

専用装置による送受信

戸籍事務内連携サーバ

戸籍届書等情報

他の市区町村で受理された新宿区に本籍を有する者の戸籍届書等情報

オンライン受領分届書等情報

法務省センター

戸籍情報連携システム

④戸籍届書等情報の送信

【LGWAN回線】

通信暗号化（SSL）

戸籍届書等情報の受信（他市区町村受理分）

他の区市町村で受理された戸籍届書の内、新宿区に本籍を有する者の戸籍届書等情報を受信する。

戸籍届書等情報

他の市区町村の戸籍届書等情報

届出人

❶振り仮名の届出（マイナポータル）
※補正による再届出含む

マイナポータル

【戸籍情報・券面情報からの自動入力項目】
・氏名
・仮の振り仮名
・戸籍の表示
・住所
【入力項目】
・届け出る振り仮名（仮の振り仮名と異なる場合）
・代理関係（親権者等）

申請状況
・
補正通知

❸オンライン届書等情報を送信

市区町村に送信する情報
・オンライン届出処理通番
・オンライン届出等管理情報（署名検証結果等）
・オンライン届出データZIP
・オンライン届出事項画像PDF
・取下げ情報※取下げの場合

❺オンライン届書等情報を送信

法務省センターに送信する情報
・オンライン届出処理通番
・オンライン届出補正通知（届出人あて補正依頼文）

オンライン届書等情報送信
・
補正通知受信等

❷届出事項を送信

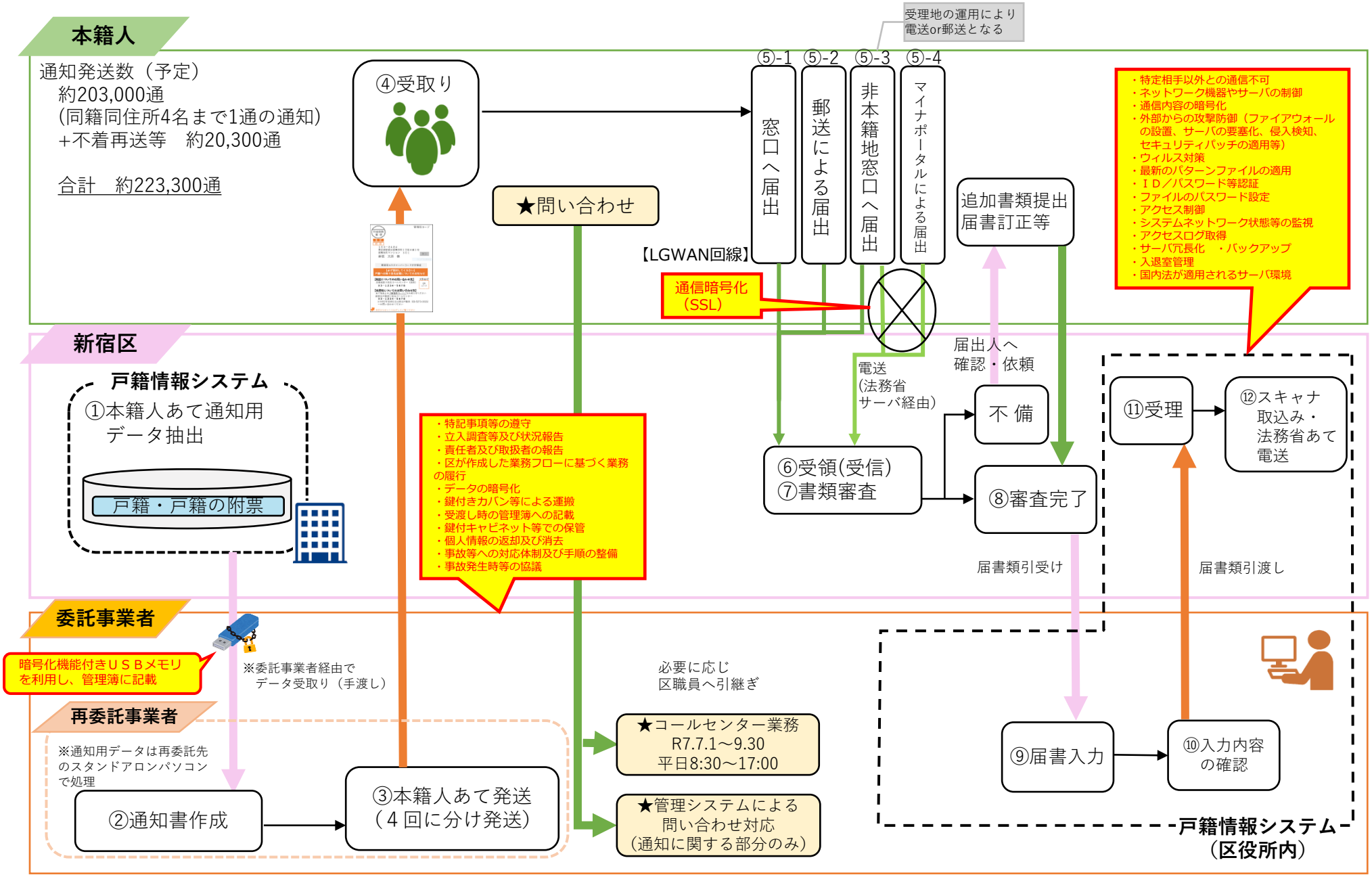
オンライン届出データZIP

通信暗号化（SSL）

❻補正通知・申請状況（手続完了の場合はその旨）

振り仮名法制化対応の業務委託に係る個人情報の流れ

（資料７０－２）



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。
	○	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。
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】	○	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。
	○	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】	○	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。