資料21

個人情報保護管理運営会議　付議事項

件名	住民基本台帳法等の改正に伴う戸籍の附票記載事項の送受信に係る戸籍情報システム等の外部結合等について（情報項目及び結合先の追加）

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	住民基本台帳、戸籍の附票
担当課	戸籍住民課
目　的	令和元年５月３１日に住民基本台帳法及びデジタル手続法等の一部を改正する法律が公布され、令和６年５月２７日に施行されることから、新たに以下の通知について住民基本台帳ネットワークシステムの専用回線を経由し送受信を行い処理することとなった。 （１）住民基本台帳法第９条第２項に基づく住民票記載事項通知 （２）住民基本台帳法第１９条第２項に基づく本籍照合通知 （３）住民基本台帳法第１９条第３項に基づく本籍転属通知 改正法に基づく全国一律の事務処理を適正に行うため、必要な外部結合、システム改修及び業務委託を行う。
対象者	新宿区に住民登録を有する者（日本人住民）及び戸籍の附票を有する者（戸籍を有する者） 新宿区に戸籍の届出をした者
事業内容	１　概要 区では、平成２４年７月から、法令に基づき、戸籍の附票記載事項通知の送受信について、住民基本台帳ネットワークシステムの専用回線により、他の市区町村との外部結合を行っている（平成２４年度第４回本審議会了承済）。 この度、令和元年５月３１日に住民基本台帳法及びデジタル手続法等の一部を改正する法律が公布され、令和６年５月２７日に施行されることから、新たに以下の通知について住民基本台帳ネットワークシステムの専用回線を経由し送受信を行い処理することとなった。 （１）住民基本台帳法第９条第２項に基づく住民票記載事項通知 （２）住民基本台帳法第１９条第２項に基づく本籍照合通知 （３）住民基本台帳法第１９条第３項に基づく本籍転属通知 ２　個人情報保護管理運営会議付議内容 （１）電算処理 上記、１（１）、（２）及び（３）の通知の追加に対応するため、既存の戸籍情報システムを改修する。 （２）外部結合 住民基本台帳ネットワークシステムの専用回線により、既に外部結合を行っている他の市区町村と送受信する通知を追加する。 （３）業務委託 上記（１）の戸籍情報システムの改修業務を開発事業者（富士通 Japan 株式会社）に委託する。 ３　対象者数 新宿区に住民登録を有する者(日本人住民)305,627 人(令和６年４月１日現在) 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（件数）　11,138 件（令和５年度実績） ※個人情報の流れは、資料２１－１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　住民基本台帳法等の改正に伴う戸籍の附票記載事項の送受信に係る戸籍情報システムの改修について

※太字ゴシック（下線）は、令和２年度第６回情報公開・個人情報保護審議会了承済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	戸籍の附票
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 新宿区に戸籍の附票を有する者（戸籍を有する者） ２　記録項目 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住所　⑦住所を定めた年月日　⑧記録日　⑨事由　⑩性別　⑪住民票コード ⑫情報提供用個人識別符号 ３　記録するコンピュータ 戸籍情報システム
新規開発・追加・変更の理由	令和元年５月３１日改正住民基本台帳法等が公布され**（令和６年５月２７日施行）**、マイナンバーを活用した行政機関等の戸籍関係情報の提供を行うことから情報項目及び結合先の追加を行う必要があるため。
新規開発・追加・変更の内容	**（１）他の市区町村（住民登録地）あて送信する住民票記載事項通知に係る機能追加** **（２）他の市区町村（住民登録地）あて送信する本籍照合通知に係る機能追加** **（３）他の市区町村（本籍地）と送受信する本籍転属通知に係る機能追加** **（４）その他運用開始後のシステム不具合修正等**
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５月　本稼働**

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　住民基本台帳法等の改正に伴う戸籍の附票記載事項の送受信に係る戸籍情報システム等の外部結合について（結合先の追加）

※太字ゴシック（下線）は、令和２年度第６回情報公開・個人情報保護審議会了承済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	住民基本台帳、戸籍の附票
結合される情報項目（だれの、どのような項目か）	【新宿区に住民登録（日本人住民）を有する者及び戸籍の附票を有する者に係る情報項目（他の市区町村と送受信する情報項目）】 ① 氏名（漢字）　② 氏名（カナ）　③ 生年月日　④ 性別　⑤ 本籍 ⑥ 筆頭者の氏名（漢字）　⑦ 新しい住所　⑧ 今までの住所 ⑨ 新しい世帯主名（漢字）　⑩ 今までの世帯主名（漢字）　⑪ 続柄 ⑫ 異動事由　⑬ 異動年月日　⑭ 届出年月日　⑮ 住所を定めた年月日 ⑯ 住民票コード 【新宿区に戸籍の附票を有する者に係る情報項目（地方公共団体情報システム機構（以下「J-LIS」という。）と送受信する情報項目）】 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 住所　⑦ 住所を定めた年月日 ⑧ 記録日　⑨ 事由　⑩ 性別　⑪ 住民票コード ⑫ 情報提供用個人識別符号
結合の相手方	他の市区町村及びJ-LIS
結合する理由	平成２４年７月９日から、住民基本台帳法に基づき、住民基本台帳ネットワークシステムの専用回線を通じて、戸籍の附票記載事項通知の送受信を行うこととされた。 令和元年５月３１日に改正住民基本台帳法等が公布され、交付後５年以内にマイナンバーを活用した行政機関等の戸籍関係情報の提供及び市区町村間での戸籍事務内連携を行うことから、情報項目及び結合先を追加し、戸籍の記載事項通知を送受信する必要がある。 **上記改正法について令和６年５月２７日に施行されることとなり、新たに住民票記載事項通知・本籍転属通知・本籍照合通知についても電送による事務を開始することとなった。**
結合の形態	住民基本台帳ネットワークシステムによる送受信
結合の開始時期と期間	**令和６年５月２７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）

◇電子計算機による個人情報の処理委託（第 14 条第1項）・・・報告事項

件名　住民基本台帳法等の改正に伴う戸籍の附票記載事項の送受信に係る戸籍情報システムの改修業務及び保守業務の委託について

※太字ゴシック（下線）は、令和２年度第６回情報公開・個人情報保護審議会了承済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
委託先	富士通 Japan 株式会社（プライバシーマーク及びＩＳＯ２７００１を取得）
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）	【新宿区に戸籍の附票を有する者**及び戸籍の届出をした者**に係る事項】 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　住所　⑦　住所を定めた年月日 ⑧　記録日　⑨　事由　⑩　性別　⑪　住民票コード ⑫　情報提供用個人識別符号　**⑬届出日**　**⑭届出事件名**
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）
委託理由	既存の戸籍情報システムは、富士通 Japan 株式会社が構築したものであるため、当該システムについて熟知している富士通 Japan 株式会社に委託する。
委託の内容	改修業務 地方公共団体情報システム機構が策定する「戸籍附票システム改造仕様書」等に基づき戸籍情報システムを改修する。 改修の内容は、以下のとおりである。 **（１）他の市区町村（住民登録地）あて送信する住民票記載事項通知に係る機能追加** **（２）他の市区町村（住民登録地）あて送信する本籍照合通知に係る機能追加** **（３）他の市区町村（本籍地）と送受信する本籍照合通知に係る機能追加** **（４）その他運用開始後のシステム不具合修正等**
委託の開始時期及び期限	**令和６年４月２３日から令和６年６月２８日まで**
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

戸籍の附票記載事項の送受信等に係る個人情報の流れ

（資料２１－１）

※赤色の部分が本運営会議の報告事項

【システム改修】
住民基本台帳法等の改正に基づき、既存の戸籍情報システムについて、以下の改修を行う。
1　他の市区町村（住民登録地）と送受信する住民票記載事項通知（９条２項通知）に係る機能を追加
2　他の市区町村（住民登録地）あて送信する本籍照合通知（１９条２項通知）に係る機能を追加
3　他の市区町村（本籍地）と送受信する本籍転属通知（１９条３項通知）に係る機能を追加
【業務委託】
改修業務を開発事業者（富士通Japan（株））に委託する。

・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

専用回線（住民基本台帳ネットワーク）

新宿区

住民記録システム

住民基本台帳

届出者

①住所変更の届出

②届出内容の確認
③住民基本台帳の更新

住民票記載事項通知（９条２項通知）の受信

【本籍地が他市区町村の場合】附票記載事項通知の送信

【情報の不整合があった場合】本籍照合通知（１９条２項通知）の受信

他の市区町村

戸籍情報システム

戸籍・戸籍の附票

【外部結合】
住民基本台帳法等の改正に基づき、送受信する通知を追加する。

届出者

各届出

【住所地が他市区町村の場合】
❹住民票記載事項通知（９条２項通知）の送信

住民情報システム

住民基本台帳

（区内通知により処理）
住民基本台帳上の
氏名・本籍等の変更

【本籍地が新宿区の場合】附票記載事項通知の受信

【情報の不整合があった場合】本籍照合通知（１９条２項通知）の送信

戸籍情報システム

❷届出内容の確認
❸戸籍・附票の記録

戸籍・戸籍の附票

届出者

❶戸籍の届出

【従前本籍地から新本籍地あて】
❺本籍転属通知（１９条３項通知）の送信

地方公共団体情報システム機構
（J-LIS）

J-LISのシステム

戸籍の附票情報
（住民票コード
含む）

附票記載事項の送信

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「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。
	○	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。