

個人情報保護管理運営会議 付議事項

件 名	新宿区データ入力業務に係る外部結合等について
--------	------------------------

内容は別紙のとおり

要綱の根拠

◇第3条第1項第3号（外部結合、業務委託）

（担当部課：総合政策部情報システム課）

事業の概要

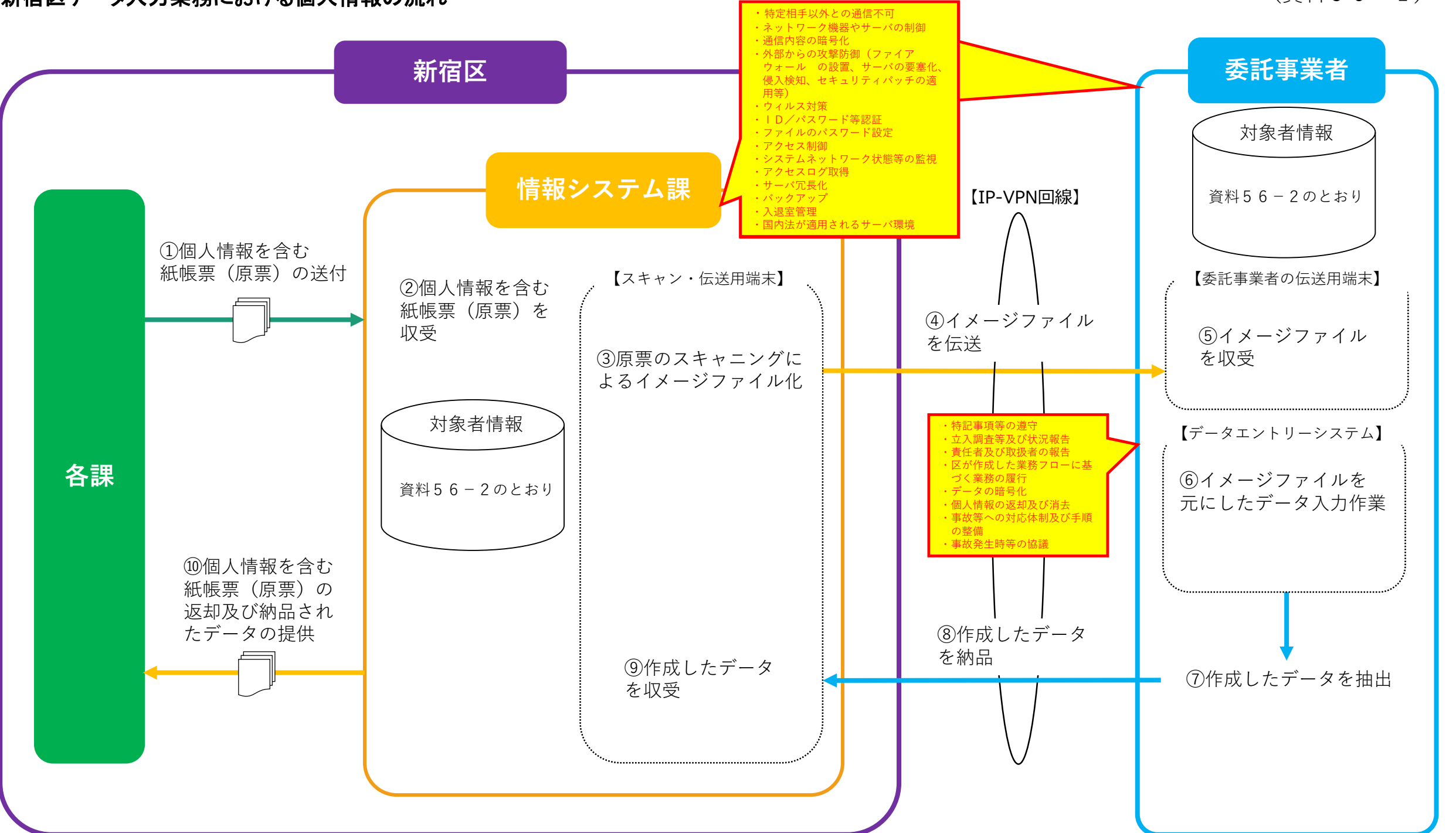
事業名	新宿区データ入力業務
担当課	情報システム課
目 的	各課から依頼されたデータ入力を行う
対象者	各課から情報システム課に依頼されるデータ入力の対象者
事業内容	1 概要 現在、情報システム課では、データエントリーシステム機器を用いて、各課から依頼を受けた個人情報を含む紙媒体を電磁的記録にする作業（データ入力）を行っている。 この度、情報システム課が保有しているデータエントリーシステムが、令和7年7月に保守期限を迎えることから、現在行っている執務室内でのデータ入力運用を廃止し、データ入力業務を包括的に委託することで事務の効率化を図る。 サービス利用型のデータ入力方法は、以下のとおり。 ①情報システム課が各課から個人情報を含む紙帳票を収受する。 ②情報システム課職員がスキャニングし、イメージファイルを作成する。 ③スキャニングしたイメージファイルを、データ暗号化ツールで暗号化し、閉域網である IP-VPN 回線を通じて委託事業者に伝送する。 ④委託業者は受信したイメージファイルを元に、委託業者で導入・運用するデータエントリーシステムを用いて、データ入力作業を行う。 ⑤作成したデータを、データ暗号化ツールで暗号化し、IP-VPN 回線を通じて情報システム課に納品する。 ⑥紙帳票を返却するとともに、納品されたデータを各課に提供する。 2 個人情報保護管理運営会議への付議内容 (1) 外部結合 閉域網である IP-VPN 回線を利用して、新宿区役所の情報システム課執務室内に設置する PC と、委託業者に設置する PC を結合する。 (2) 業務委託 情報システム課が各課から依頼を受けたデータ入力対象の紙帳票を元に、データ入力業務を行う。 3 対象者数 約 31 万件（令和5年度データ入力実績件数） ※個人情報の流れは、資料56-1のとおり

件名 新宿区データ入力業務に係る外部結合について

保有課 (担当課)	情報システム課
登録業務の名称	新宿区データ入力業務
結合される情報項目 (だれの、どのような項目か)	1 対象者 各課から情報システム課に依頼されるデータ入力の対象者 2 情報項目 資料56-2のとおり
結合の相手方	システムズ・デザイン株式会社 (プライバシーマーク、ISO27001 取得済)
結合する理由	情報システム課で導入した機器を使用するデータ入力を廃止し、サービス利用型のデータ入力へ切り替えるにあたり、委託業者と情報システム課間で、電磁的記録の伝送を行う必要があるため。
結合の形態	閉域網である IP-VPN 回線を利用して、新宿区役所の情報システム課執務室内に設置する PC と、委託業者に設置する PC を結合する。
結合の開始時期と期間	令和7年4月1日から令和8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 新宿区データ入力業務に係る業務の委託について

保有課(担当課)	情報システム課
登録業務の名称	新宿区データ入力業務
委託先	システムズ・デザイン株式会社 (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)	1 対象者 各課から情報システム課に依頼されるデータ入力の対象者 2 情報項目 資料5 6 - 2のとおり
処理させる情報項目の記録媒体	委託業者で導入するデータエントリーシステム用端末及びサーバ (データ入力に使用する各機器はインターネットや事務系端末から独立したデータ処理専用のネットワークにのみ接続)、データの授受に用いる、IP-VPN 回線に接続された PC (通常のインターネット等への接続なし)。
委託理由	情報システム課で導入した機器を使用するデータ入力の運用を廃止し、サービス利用型のデータ入力へ切り替えるため。
委託の内容	情報システム課が各課から依頼を受けたデータ入力対象の紙帳票を元に、データ入力業務を行う。
委託の開始時期及び期限	令和7年4月1日から令和8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



資料 56-2 情報項目一覧

- 1 **外国人学校補助金**（児童生徒氏名・保護者氏名・電話番号・住所・転入年月日・在籍学校名・学年・在籍期間・在留カード番号・生年月日・続柄・世帯番号・年間総所得額）
- 2 **読書に関するアンケート集計**（学校番号・学年）
- 3 **区政モニターアンケート同意書**（氏名・性別・生年月日・住所・電話番号・FAX 番号・区内在住期間・職業等・モニター経験・各種団体地域活動経験）
- 4 **福祉情報 おむつ用代金定期更新**（住所・氏名・代金・口座登録者住所及び氏名・おむつ利用者住所及び氏名・住民番号）
- 5 **収入日計（後期高齢者医療制度）**（被保険者番号・相当年度・口座・自治体コード・税目コード・年度・期別・納付書コード・納付額・延滞金・合計金額・収入区分・領収年月日）
- 6 **高齢者インフルエンザ予防接種予診票**（氏名・住所・住民番号・生年月日・自己負担金・健康状態・代筆者氏名及び続柄・接種年月日・実施医療機関）
- 7 **予防接種予診票**（氏名・住所・住民番号・生年月日・性別・自己負担金・健康状態・接種年月日・実施医療機関・保護者または同伴者氏名及び緊急連絡先（電話番号））
- 8 **歯科健康診査受診票/問診票**（氏名・住所・受診番号・生年月日・性別・健診実施日・健診方法・自己負担金・歯の健康状態・その他注意すべき所見・総合判定結果・問診票内容・実施医療機関）
- 9 **フッ化物塗布受診**（氏名・住所・受診番号・生年月日・年齢・電話番号・検査日・アンケート内容・歯の健康状態・検査結果・相談内容・実施医療機関）
- 10 **後期高齢者歯科健康診査受診票/問診票**（氏名・住所・受診番号・生年月日・性別・健診実施日・健診方法・自己負担金額・歯の健康状態・健診結果・問診票内容・実施医療機関）
- 11 **国保高額療養費処理**（保険証番号・世帯主氏名・診療年月・課税区分・所得区分・第三者行為の有無・医療機関等への支払い・請求年月・被保険者氏名・生年月日・性別・実施医療機関・入院又は外来・日数・総医療費・自己負担額・支給金額等・住所・電話番号・銀行口座情報・実施医療機関）
- 12 **国保療養費処理（外部機関）**（受給者番号・保険証番号・療養者氏名・性別・生年月日・続柄・被保険者氏名・傷病の原因・施術内容・施術日施術者住所・施術者氏名・申請者住所・申請者氏名・申請者電話番号・代理人住所・代理人氏名・代理人電話番号・銀行口座情報・医師住所・医師氏名）

- 13 国保療養費処理（旧レイアウト）（保険証番号・傷病名・発病日・被保険者名・性別・生年月日・続柄・受診月・実施医療機関・医師等名・療養費の支給申請・発病等の理由・療養費用・世帯主氏名・住所・電話番号・銀行口座情報・患者負担額・支払済額）
- 14 国保 収入日計処理（納付番号・確認番号・納付区分・保険証番号・賦課年度・対象年度・期別・納付者氏名・保険料・延滞金・合計金額・領収日・口座区分・納付区分）
- 15 介護 納付書兼納入済通知書（納付書コード・自治体コード・科目コード・調定年度・被保険者番号・延滞金区分・口座区分・納付額・保険料・延滞金・期別・領収年月日）
- 16 介護 預金口座振替依頼書（被保険者番号・氏名・住所・電話番号・口座管理者氏名・口座管理者住所・口座管理者電話番号・被保険者との関係・銀行口座情報）
- 17 介護 還付口座登録届出書（被保険者番号・被保険者氏名・口座名義人氏名・口座名義人住所・口座名義人電話番号・被保険者との関係・銀行口座情報・委任者氏名及び住所・受任者氏名及び住所・相続人氏名・相続人住所・相続人続柄・相続人電話番号）
- 18 税務 普徴収入日計MPN納付済通知書（納付番号・確認番号・納付区分・年度期別・納税通知書番号・税額・延滞金・氏名・領収日）
- 19 税務 軽自収入日計MPN納付済通知書（納付番号・確認番号・納付区分・年度期別・納税通知書番号・税額・延滞金・氏名・領収日）
- 20 税務 収入日計（平成用）（指定番号・住所・氏名・年月・納税額・延滞金・領収日）
- 21 税務 収入日計（OCR用）（指定番号・住所・氏名・年月・納税額・延滞金・領収日）
- 22 税務 過誤納還付金 MT 作成入力票（請求者住所・氏名・電話番号・銀行口座情報・納付義務者・還付金額・過誤納発生の理由・賦課年度・対象年度・科目・通知書番号・過誤納番号）
- 23 国政調査調査員報酬口座振替依頼（氏名・銀行口座情報）
- 24 新型コロナワクチン予防接種予診票（氏名・住所・住民番号・生年月日・健康状態・代筆者氏名及び続柄・接種年月日・実施医療機関）

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。