（資料２）

令和７年１月２３日
新宿区情報公開・個人情報保護審議会資料
総合政策部区政情報課

新宿区個人情報保護管理運営会議における
個人情報保護対策チェックリストの再検証について

現在、新宿区個人情報保護管理運営会議においては、付議案件の審議を行ううえで、個人情報保護対策チェックリストを作成し、資料と合わせて案件内容の審議を行っております。

この度、令和５年度より活用している個人情報保護対策チェックリストについて、情報保護対策項目の再検証を行うことで、より適切な個人情報の管理を図るものです。

記

１　チェックリストについて
別紙１のとおり

２　管理運営会議におけるチェックリストの活用例
別紙２のとおり

３　チェックリストの追加案
（１）区が行う情報保護対策
・取扱う個人情報の管理について、必要に応じて又は定期的に確認する体制を構築するよう指導する。
・再委託先がある場合には、委託先との間に立入り調査等ができる契約内容を付すとともに、必要に応じて又は定期的に立入り調査等を実施するよう指導する。
（２）事業者に行わせる情報保護対策
・取扱う個人情報の管理について、必要に応じて又は定期的に確認する体制を構築させる。
・再委託先がある場合には、委託先との間に立入り調査等ができる契約内容を付すとともに、必要に応じて又は定期的に立入り調査等を実施させる。

１　目的外利用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○	情報保護対策
情報保護対策 【運用上の対策】		担当課の保護管理者は、他の行政機関等に保有個人情報を提供するという目的外利用を行うことについて、相当又は特別な理由があると判断できるか、関係部署と慎重に協議する。また、必要に応じて、個人情報保護委員会へ助言を求める。
		担当課の保護管理者は、利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について提供先との間で書面を取り交わす。
		担当課の保護管理者は、提供先に対し、次に掲げる措置を講ずるよう求める。 ⑴利用目的又は方法の制限 ⑵取扱者の範囲の限定 ⑶第三者への再提供の制限又は禁止 ⑷消去、返却等利用後の取扱いの指定 ⑸取扱状況に関する所要の報告の要求 ⑹訂正の決定を行った場合において、当該訂正に応じる。 ⑺適切な情報保護対策、情報セキュリティ対策の実施
		担当課の保護管理者は、必要があると認めるときは、外部提供を行う前又は随時に実地の調査等を行うことにより、当該措置の状況を確認し、その結果を記録するとともに、改善要求等を行う。
		担当課の保護管理者は、目的外利用により提供する個人情報の取扱者を指定する。

2　外部提供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○	情報保護対策
情報保護対策 【運用上の対策】		担当課の保護管理者は、他の行政機関等に保有個人情報を提供することについて、相当又は特別な理由があると判断できるか、関係部署と慎重に協議する。また、必要に応じて、個人情報保護委員会へ助言を求める。
		担当課の保護管理者は、利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について提供先との間で書面を取り交わす。
		担当課の保護管理者は、提供先に対し、次に掲げる措置を講ずるよう求める。 ⑴利用目的又は方法の制限 ⑵取扱者の範囲の限定 ⑶第三者への再提供の制限又は禁止 ⑷消去、返却等利用後の取扱いの指定 ⑸取扱状況に関する所要の報告の要求 ⑹訂正の決定を行った場合において、当該訂正に応じる。 ⑺適切な情報保護対策、情報セキュリティ対策の実施
		担当課の保護管理者は、必要があると認めるときは、外部提供を行う前又は随時に実地の調査等を行うことにより、当該措置の状況を確認し、その結果を記録するとともに、改善要求等を行う。
		担当課の保護管理者は、提供する個人情報の取扱者を指定する。

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。

6　業務委託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「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。
		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、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。

6　業務委託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「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。
		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。

7　指定管理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
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。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、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、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、直ちに指定管理先と今後の対応を協議する。
指定管理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。

7　指定管理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
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。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、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。
指定管理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。

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「ー」	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「ー」	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。

別紙2

個人情報保護管理運営会議　付議事項

件名	区民意見・ＦＡＱシステムの再構築等について

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：総合政策部区政情報課）

事業の概要

事業名	区民意見・ＦＡＱシステムの再構築等
担当課	区政情報課
目　的	令和７年１月にイントラネットシステム基盤が再構築となることから、現行の区民意見・ＦＡＱシステムの機能を新規インフラ基盤（Microsoft Dynamics365）上で再構築するとともに、必要な機能改善を行う。 また、再構築作業及び再構築完了後の運用保守について、現行事業者に委託するとともに、一部業務について再委託を行う。
対象者	意見等を投稿する者
事業内容	１　概要 現在、区では様々な媒体による意見等について一元的に管理し、迅速かつ的確に対応するとともに、各解答処理後に意見等をデータベース化し、集計及び分析を行う仕組みとして、区民意見・ＦＡＱシステムを運用している（平成２５年第１回情報公開・個人情報保護審議会承認・了承済）。 現行の区民意見・ＦＡＱシステムは、イントラネットシステム基盤上にて構築・運用が行われてきたが、令和７年１月にイントラネットシステム基盤が再構築となることから、現行の区民意見・ＦＡＱシステムの機能を新規インフラ基盤上で再構築する。 ２　個人情報保護管理運営会議への付議内容 （１）電算処理 画面レイアウト等の改善を行うとともに、以下のとおり機能追加を行う。 １．意見及び回答への電子データの添付を可能とする。 ２．パスワードを忘れた方に対するパスワード再発行を行う。 ３．投稿ページにおいて、投稿目的について選択することを可能とする。 （２）外部結合 イントラネットＰＣから委託事業者の構築する区民意見・ＦＡＱシステムとの外部結合を行う。 （３）業務委託 再構築及び再構築完了後の運用保守について、委託するとともに、業務の一部について再委託を行う。 ３　想定投稿数 約 40,000 件 ※個人情報の流れは、資料１－１、資料１－２及び資料１－３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　区民意見・ＦＡＱシステムの再構築等について

※太字ゴシック（下線）が平成２５年度第１回情報公開・個人情報保護審議会承認済みの内容からの変更箇所

保有課（担当課）	区政情報課
登録業務の名称	コールセンター及び区民意見システム
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 ①　区長への投書（一般投書、区長へのはがき、ＷＥＢ）として、区へ意見を提出した者 ②　担当課へ区のホームページから問合せを行い、かつ、回答を要望する者 ③　**コールセンターに問合せを行った者** ２　記録する個人情報の項目 ＩＤ、パスワード、氏名、郵便番号、住所、電話番号、メールアドレス（ＩＤ登録用）、ＦＡＸ番号、意見等の内容、**投稿目的**、回答内容、**意見及び回答に関連する電子データ** ３　記録するコンピュータ **Microsoft Dynamics 365 により構築されたインフラ基盤上に存在する Microsoft のデータベースサーバーに、**コールセンター業務の情報項目とあわせて、上記「個人の範囲」該当者からの意見等を処理する業務の情報項目を記録し、一元管理する。
新規開発・追加・変更の理由	**令和７年１月にイントラネットシステム基盤が再構築となることから、現行の区民意見・ＦＡＱシステムの機能を新規インフラ基盤上で再構築するとともに、必要な機能改善を行う。**
新規開発・追加・変更の内容	**現行の区民意見・ＦＡＱシステムの機能を新規インフラ基盤（Microsoft Dynamics 365）上で再構築する。** **再構築に合わせ、画面レイアウト等の改善を行うとともに、以下のとおり機能追加を行う。** **１．意見及び回答への電子データの添付を可能とする。** **２．パスワードを忘れた方に対するパスワード再発行を行う。** **３．投稿ページにおいて、投稿の目的についてプルダウン方式で選択する。**
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（システム再構築）** **令和６年７月　　開発（機能追加）** **令和６年１１月　　テスト** **令和７年１月　　本稼働**

別紙(電子計算機の外部結合関係)

◇外部との結合(第３条第１項第３号)

件名　区民意見・ＦＡＱシステムの外部結合について

保有課（担当課）	区政情報課
登録業務の名称	コールセンター及び区民意見システム
結合される情報項目（だれの、どのような項目か）	１　個人の範囲 ①　区長への投書（一般投書、区長へのはがき、ＷＥＢ）として、区へ意見を提出した者 ②　担当課へ区のホームページから問合せを行い、かつ、回答を要望する者 ③　コールセンターに問合せを行った者 ２　記録する個人情報の項目 ＩＤ、パスワード、氏名、郵便番号、住所、電話番号、メールアドレス（ＩＤ登録用）、ＦＡＸ番号、意見等の内容、投稿目的、回答内容、意見及び回答に関連する電子データ ３　記録するコンピュータ Microsoft Dynamics 365 により構築されたインフラ基盤上に存在するMicrosoft のデータベースサーバーに、コールセンター業務の情報項目とあわせて、上記「個人の範囲」該当者からの意見等を処理する業務の情報項目を記録し、一元管理する。
結合の相手方	日本電気株式会社（プライバシーマーク、ISMS 認証取得済）
結合する理由	様々な媒体による意見等について一元的に管理し、迅速かつ的確に対応するとともに、各解答処理後に意見等をデータベース化し、集計及び分析を行うため。
結合の形態	イントラＰＣを用い、専用回線から委託先のサーバと結合を行う。
結合の開始時期と期間	令和６年１１月１日から令和７年３月３１日まで（次年度以降も、同様の結合を行う。）
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　区民意見・ＦＡＱシステムの再構築等について

※太字ゴシック（下線）が平成２５年度第１回情報公開・個人情報保護審議会承認済みの内容からの変更箇所

保有課(担当課)	区政情報課
登録業務の名称	コールセンター及び区民意見システム
委託先	**日本電気株式会社（プライバシーマーク、ISMS 認証取得済）**
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)	【該当者（※）に係る情報項目】 ＩＤ、パスワード、氏名、郵便番号、住所、電話番号、メールアドレス（ＩＤ登録用）、ＦＡＸ番号、意見等の内容、**投稿目的**、回答内容、**意見及び回答に関連する電子データ** ※「該当者」の定義 １ 区長への投書（一般投書、区長へのはがき、ＷＥＢ）として、区へ意見等を提出した者 ２ 担当課へ区のホームページから問合せを行い、かつ、回答を要望する者 ３ **コールセンターに問合せを行った者**
処理させる情報項目の記録媒体	**電磁的媒体（Microsoft のデータベースサーバー）**
委託理由	上記委託先は、本システムの開発業者であり、システムの**再構築業務**及び保守業務を安全かつ効率的に行うことができるため。
委託の内容	**１　区民意見・ＦＡＱシステムを新規インフラ基盤(Microsoft Dynamics 365)上に再構築する。** **２　区民意見・ＦＡＱシステムの保守業務を行う。**
委託の開始時期及び期限	**１　再構築　令和６年４月１日から令和７年３月１４日まで** **２　保守　　令和７年１月１日から令和７年３月３１日まで** **（次年度以降も、同様の保守業務委託を行う。）**
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

別紙(業務委託)

◇業務委託(第３条第１項第３号)

件名　区民意見・ＦＡＱシステムの再構築等についての再委託

保有課(担当課)	区政情報課
登録業務の名称	コールセンター及び区民意見システム
委託先(再委託先)	ＮＥＣソリューションイノベータ株式会社（プライバシーマーク、ISMS 認証取得済）
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）	【該当者（※）に係る情報項目】 ＩＤ、パスワード、氏名、郵便番号、住所、電話番号、メールアドレス（ＩＤ登録用）、ＦＡＸ番号、意見等の内容、投稿目的、回答内容、意見及び回答に関連する電子データ ※ 「該当者」の定義 １ 区長への投書（一般投書、区長へのはがき、ＷＥＢ）として、区へ意見等を提出した者 ２ 担当課へ区のホームページから問合せを行い、かつ、回答を要望する者 ３ コールセンターに問合せを行った者
処理させる情報項目の記録媒体	電磁的媒体（Microsoft のデータベースサーバー）
再委託理由	日本電気株式会社が開発するシステムの構築や運用保守を熟知しており、再委託により円滑かつ効率的に作業を実施することができるため
再委託の内容	１　区民意見・ＦＡＱシステムの再構築業務の一部 ２　区民意見・ＦＡＱシステムの保守業務の一部
再委託の開始時期及び期限	１　再構築　令和６年４月１日から令和７年３月１４日まで ２　保守　　令和７年１月１日から令和７年３月３１日まで （次年度以降も、同様の保守業務委託を行う。）
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
委託先（再委託先）に行わせる情報保護対策	別紙チェックリストのとおり

区民意見・FAQシステムに係る個人情報の流れ（インターネット投稿・インターネット回答）

（資料１－１）

【インターネット回線】

【専用回線】

投稿者

区民等

しんじゅく
コール
オペレーター

コールセンター受付
意見は①、⑤のみ

通信暗号化

① 意見等の入力・投稿

② パスワードの表示

③ 受付確認メールの送信

⑧ 回答メールの送付

⑨ パスワード入力
・回答閲覧

Dynamics365(Microsoftクラウドサービス)

区民意見・FAQシステム
（日本電気株式会社　プライバシーマーク･ISMS認証取得）

【投稿者機能】
意見投稿
回答閲覧
パスワード再発行申請

【区側機能】
意見確認
回答送付
意見・回答情報の出力

DB

意見・回答等データ

④ 処理依頼メールの送付

⑤ 意見内容の確認・出力

⑥ 回答・対応経過入力

⑦ インターネット回答
送信処理

新宿区

区職員
（イントラPC）

・特定相手以外の通信不可
・ネットワーク機器等制御による通信限定
・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、分析
・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

・個人情報保護法等の遵守
・立入調査等及び状況報告
・個人情報の消去
・事故等への対応体制及び手順の整備
・事故発生時等の協議

・特定相手以外の通信不可
・ネットワーク機器等制御による通信限定
・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、分析
・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

区民意見・FAQシステムに係る個人情報の流れ（インターネット投稿・郵送回答）

（資料１－２）

【インターネット回線】

【専用回線】

投稿者

通信暗号化

① 意見等の入力・投稿

② 受付確認メールの送信

Dynamics365(Microsoftクラウドサービス)

区民意見・FAQシステム
（日本電気株式会社　プライバシーマーク･ISMS認証取得）

【投稿者機能】
意見投稿
回答閲覧
パスワード再発行申請

【区側機能】
意見確認
回答送付
意見・回答情報の出力

DB

意見・回答等データ

③ 処理依頼メールの送付

④ 意見内容の確認・出力

⑤ 回答・対応経過入力

新宿区

区民等

区職員
（イントラPC）

・特定相手以外の通信不可
・ネットワーク機器等制御による通信限定
・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、分析
・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

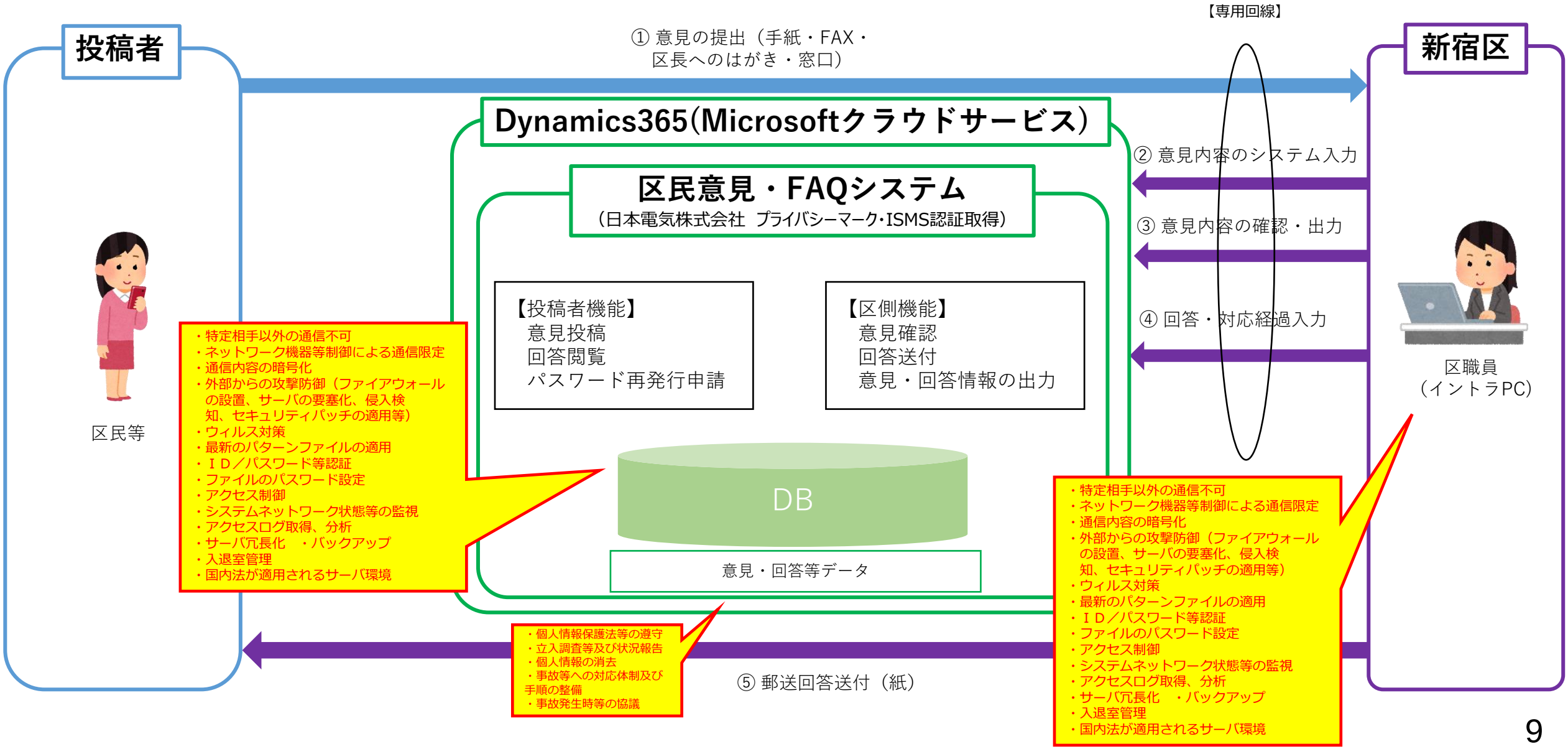
・特定相手以外の通信不可
・ネットワーク機器等制御による通信限定
・通信内容の暗号化
・外部からの攻撃防御（ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等）
・ウィルス対策
・最新のパターンファイルの適用
・ＩＤ／パスワード等認証
・ファイルのパスワード設定
・アクセス制御
・システムネットワーク状態等の監視
・アクセスログ取得、分析
・サーバ冗長化　・バックアップ
・入退室管理
・国内法が適用されるサーバ環境

・個人情報保護法等の遵守
・立入調査等及び状況報告
・個人情報の消去
・事故等への対応体制及び手順の整備
・事故発生時等の協議

⑥ 郵送回答送付（紙）

区民意見・FAQシステムに係る個人情報の流れ（インターネット以外の方法による意見の提出・郵送回答）

（資料１－３）



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。
	ー（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。
	ー（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。
	ー（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。
	○	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。
	ー（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。
	ー（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。
	ー（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。
	○	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。