資料53

個人情報保護管理運営会議　付議事項

件名	新宿区立元気館における貸室予約受付システムの構築に係る開発等について

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、指定管理）

（担当部課：健康部健康政策課）

事業の概要

事業名	元気館貸室予約受付システム
担当課	健康政策課
目　的	予約受付システムを新たに導入することで、予約受付、予約状況の照会、空き状況の検索が容易にできるようになり、区民の利便性を向上させるとともに、元気館の利用促進を目指す。
対象者	元気館利用者（登録団体及びその他団体利用者）
事業内容	1　概要 現在、元気館の施設利用を希望する登録団体（※1）等は、施設の予約受付、予約状況の照会、空き状況の検索などについて、電話等で問い合わせを行うことで、予約や照会などをしている。（平成１７年度第８回情報公開・個人情報保護審議会了承済み） 今後は、新たに予約受付システムを導入することで、インターネットを経由し、いつでも好きな時間帯に施設の予約受付や予約状況の照会等を行うことができるようになる。 また、インターネットからの利用枠抽選機能により、利用者は毎月抽選日に元気館に集まる必要がなくなり、交通費と時間を削減できるため、区民の負担軽減と利便性の向上につながる。 ※1　登録団体とは、新宿区立元気館条例第 20 条第 1 項に規定し、会員数 5 名以上で過半数が区民であり、代表者又は責任者が明確で、かつ、区民である団体。 2　個人情報保護管理運営会議への付議内容 （1）電算処理 レガスシステム（※2）と同一クラウド基盤上に構築する。本システムを用い、元気館における貸室業務を行う。 （2）外部結合 公益財団法人新宿未来創造財団（以下「新宿未来創造財団」という。）が管理するレガスシステムと同一クラウド基盤上に構築させ、そこで利用者情報を保有する。 （3）指定管理 新たな受付システムをレガスシステムと同一クラウド基盤上に構築させる業務を行う。 また、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、システムのサービス提供・保守にかかる業務を行う。 ※2　レガスシステムとは、新宿未来創造財団が保有する総合受付システムであり、区内の生涯学習及びスポーツ施設の利用申請及び利用承認に係る業務をインターネットで行うために開発されたもの。 3　対象者数（コロナ期以外直近） 登録団体：１６７団体（令和２年３月３１日時点） 登録団体利用数：２，３８９件（２７，４３９名） その他団体利用数：１，８７６人（１４，５７１名） ※個人情報の流れは、資料５３－１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　新宿区立元気館における貸室予約受付システムの構築に係る開発について

保有課（担当課）	健康政策課
登録業務の名称	元気館貸室予約受付システムの管理運営
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 元気館利用者（登録団体及びその他団体利用者） ２ 記録項目 ① 代表者に係る記録項目 氏名、住所、電話番号（自宅・携帯） ② 連絡担当者に係る記録項目 氏名、住所、電話番号（自宅・携帯）、メールアドレス ３ 記録するコンピュータ 新たな受付システム（レガスシステムと同一クラウド基盤上に移設）
新規開発・追加・変更の理由	元気館おける施設貸室業務について、新たに貸室予約受付システムを導入することで、利用者の利便性の向上とともに、気軽に施設利用できるようにすることを目指す。
新規開発・追加・変更の内容	・ブラウザサポート環境の変化に極力影響を受けないシステムを構築する。 ・クラウド上にシステムを構築する。 ・標準搭載されているインターネットからの利用枠抽選機能により、オンラインでの抽選を行う。
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４月から　新宿未来創造財団との新システムに関する協定締結・開発開始（予定） 令和８年１月から４月まで　新システム本稼働（予定） 令和８年２月から　インターネット抽選機能利用開始（予定）

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　新宿区立元気館における貸室予約受付システムとの外部結合について

保有課（担当課）	健康政策課
登録業務の名称	元気館貸室予約受付システムの管理運営
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 登録団体及びその他団体利用者 ２ 記録項目 ① 代表者に係る記録項目 氏名、住所、電話番号（自宅・携帯） ② 連絡担当者に係る記録項目 氏名、住所、電話番号（自宅・携帯）、メールアドレス
結合の相手方	公益財団法人新宿未来創造財団
結合する理由	受付システムの導入に当たり、区がこれまでレガスシステムと同一のサーバを使用してきた枠組みを継承し、レガスシステムと同一クラウド基盤を使用することで、個別導入による経費と比較して安価に抑えるため。
結合の形態	元気館内の管理者用パソコン・窓口端末からインターネットに接続し、レガスシステムと同一クラウド基盤上の受付システムに保有された「登録団体及び貸出施設等の利用者」に係る情報の管理を行う。
結合の開始時期と期間	令和８年１月から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

別紙（指定管理関係）

◇指定管理（第３条第１項第３号）

件名　新宿区立元気館における貸室予約受付システムの構築に係る指定管理について

施設の名称	新宿区立元気館
施設の所管課	健康政策課
指定管理者の名称 ＊（委託先）	未定（公募型プロポーザル方式により選定を予定）（プライバシーマーク取得事業者を予定）
指定管理者が取扱う個人情報の業務 ＊（委託に係る個人情報の業務）	新たな受付システムをレガスシステムと同一クラウド基盤上に構築する。 また、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・保守にかかる業務を行う。
指定管理者が取扱う個人情報の項目 ＊（委託に係る個人情報の項目）	１ 個人の範囲 登録団体及びその他団体利用者 ２ 記録項目 ① 代表者に係る記録項目 氏名、住所、電話番号（自宅・携帯） ② 連絡担当者に係る記録項目 氏名、住所、電話番号（自宅・携帯）、メールアドレス
個人情報項目の記録媒体	電磁的媒体（受付システム）
指定管理の開始時期及び期限 ＊（業務委託期間）	令和８年１月から令和１３年３月３１日まで（予定）（次期指定管理期間以降も、同様の指定管理業務を行う。）
指定管理者としての情報保護対策 ＊（委託先の個人情報保護対策）	別紙チェックリストのとおり
指定にあたり区が行う情報保護対策 ＊（委託にあたり指定管理者が行う個人情報保護対策）	別紙チェックリストのとおり

元気館貸室受付予約システムに係る個人情報の流れ

（資料５３－１）

※レガスシステムを保有する新宿未来創造財団が富士通Japan株式会社に委託してシステムを構築する。

施設利用者（登録団体等）

【ケース１】※今回の受付システム
自宅ＰＣ等で、空き施設の予約申請・取消等

【ケース２】
窓口等で空き施設の利用申請・取消等

来館・電話

元気館（指定管理者）

指定管理者（職員ＰＣ）

事務処理内容

【施設貸出業務】
(1)利用者登録・変更
(2)利用申請・変更申請
(3)利用承認・取消
(4)抽選・結果通知
(5)統計処理等
(6)利用料金受払

インターネット回線

通信暗号化

利用者情報

利用者情報

・特定相手以外の通信不可
・通信内容の暗号化
・ＩＤ／パスワード等認証
・ファイルのパスワード設定
・アクセスログ取得、分析
・サーバ冗長化
・入退室管理
・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）
・ネットワーク機器等制御による通信限定
・ウィルス対策
・最新のパターンファイルの適用
・アクセス制御
・システムネットワーク状態等の監視
・バックアップ
・国内法が適用されるサーバ環境

プライベートクラウド（レガスシステムと同一）

※ただし、レガスシステムとデータベースは共有しない

受付システム

（委託事業者）
【保守委託】
システムの運用保守および障害対応

登録団体及び貸出施設等の利用者情報

① 代表者に係る記録項目
- 氏名
- 住所
- 電話番号（自宅・携帯）

② 連絡担当者に係る記録項目
- 氏名
- 住所
- 電話番号（自宅・携帯）
- メールアドレス

（委託事業者）
【電算処理】及び【外部結合】
インターネット接続を利用して、クラウドとの情報連携
※システムの管理者画面へは、元気館のＩＰアドレスのみ接続許可

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。

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。
	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、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。
	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。
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。