資料45

個人情報保護管理運営会議　付議事項

件名	新宿区立新宿スポーツセンターにおける指定管理者制度の導入について（情報項目の変更）

内容は別紙のとおり

要綱の根拠

◇第３条第１項第３号（指定管理）

（担当部課：地域振興部生涯学習スポーツ課）

事業の概要

事業名	新宿区立新宿スポーツセンターの指定管理
担当課	生涯学習スポーツ課
目　的	新宿区立新宿スポーツセンター指定管理者が実施するパーソナルプログラム及びスポーツ・文化教室について、支払い方法を拡充することで利用者の利便性向上を図るため。
対象者	新宿スポーツセンター利用者（パーソナルプログラム及びスポーツ等の教室利用者）
事業内容	１　概要 これまでパーソナルプログラム及びスポーツ・文化教室の利用料金の支払い方法について、施設窓口及び券売機で現金・キャッシュレス決済としてきたが、令和８年４月１日から指定管理者の変更に伴い、利用者が教室等の申込システムにクレジットカード情報を登録することで、WEB 上での支払いを可能にするため、利用者から取得する個人情報に、新たにクレジットカード情報を追加する。 なお、クレジットカード情報以外の個人情報の取得については、平成 18 年度第４回情報公開・個人情報保護審議会にて了承済。 ２　個人情報保護管理運営会議への付議内容 指定管理者が取り扱う個人情報項目の追加 ３　想定利用者数 約 9500 人/年間 ※個人情報の流れは、資料４５－１のとおり

別紙(指定管理者関係)

◇指定管理(第 3 条第1項第 3 号)

件名　新宿区立新宿スポーツセンターにおける指定管理者制度の導入について（情報項目の変更）

※太字ゴシック（下線）が平成 18 年度第 4 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

施設の名称	新宿区立新宿スポーツセンター
施設の所管課	生涯学習スポーツ課
指定管理者の名称	**新宿スポーツ＆ウェルビーイング共同事業体**
指定管理者が取扱う個人情報の業務	団体登録業務、施設利用業務、事業運営業務
指定管理者が取扱う個人情報の項目	団体名　登録区分　氏名　住所　年齢　性別　電話番号　勤務先名称 勤務先所在地　勤務先電話番号　メールアドレス　**クレジットカード情報**
個人情報項目の記録媒体	紙及び電磁的媒体（指定管理者のパソコン及び予約システム） ※予約システムを利用する指定管理者は、プライバシーマーク取得済み
指定管理の開始時期及び期限	**令和 8 年 4 月 1 日から令和 13 年 3 月 31 日まで（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	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	別紙チェックリストのとおり

【パーソナルプログラム及びスポーツ・文化教室申込受付業務の個人情報の流れ】

※赤字の部分が、今回の付議事項。

申請者

⑥パーソナル・
教室への参加

【インターネット回線】

通信暗号化

①パーソナル・教室申込
（窓口、郵送又は予約システム）

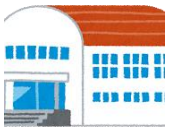
・特定相手以外との通信不可
・ネットワーク機器やサーバの制御
・通信内容の暗号化
・外部からの攻撃防御（ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等）
・ウィルス対策
・最新のパターンファイルの適用
・ＩＤ／パスワード等認証
・ファイルのパスワード設定
・アクセス制御
・システムネットワーク状態等の監視
・アクセスログ取得
・サーバ冗長化　・バックアップ
・入退室管理
・国内法が適用されるサーバ環境

⑤申し込み完了の通知
（メール・郵送）

指定管理者

・特記事項等の遵守
・立入調査等及び状況報告
・責任者及び取扱者の報告
・区が作成した業務フローに基づく業務の履行
・データの暗号化
・鍵付きカバン等による運搬
・受渡し時の管理簿への記載
・鍵付キャビネット等での保管
・個人情報の返却及び消去
・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

【新宿スポーツセンター】



②申込受理

【指定管理者のパソコン】

③申込内容の入力

団体名　登録区分
氏名　住所　年齢　性別　電話番号　勤務先名称　勤務先所在地　勤務先電話番号
メールアドレス
クレジットカード情報

④申し込み確定

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。
	○	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。
	○	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。
	○	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。
	○	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。
	○	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。
	○	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。