資料26

個人情報保護管理運営会議　付議事項

件名	梅毒等の性感染症のまん延防止事業に係る業務の委託について

内容は別紙のとおり

要綱の根拠

◇第３条第１項第３号（業務委託）

（担当部課：健康部保健予防課）

事業の概要

事業名	性感染症対策の推進
担当課	保健予防課
目　的	性感染症に対して知識・認識を持っていないものに対して、委託先を活用したアウトリーチ型支援や健康相談等を実施することで、普及啓発・早期発見および感染症予防対策の強化を図る。
対象者	区内の繁華街（主にシネシティ広場や大久保公園周辺）に集まる若者など
事業内容	1　概要 区では、区内の繁華街に対し、さまざまな目的で不特定多数の若者が集まる傾向があり、性感染のおそれがある疾病の発生及びまん延を防止する必要が求められる。 本事業は、性感染症についての正しい知識と理解につなげるためのリーフレット等の作成、アウトリーチ型支援及び健康相談等を事業者に委託することで、性感染症に関する注意喚起やまん延防止対策の普及啓発を図るものである。 2　個人情報保護管理運営会議への付議内容 次の①から③までの業務を委託する。 ① 性感染症についてのリーフレット等を作成する。 ② 区内の繁華街（主にシネシティ広場や大久保公園周辺）に集まる若者などを対象にリーフレット等を配布し、区で実施する無料匿名の性感染症検査の周知を行う。（アウトリーチ型支援） ③ 配布するリーフレット等に健康相談窓口の電話番号やメールアドレスなどを記載し、性感染症に不安を抱える対象者からの相談に電話やメールで対応する。 3　想定人数 健康相談：200 名程度（令和６年８月～令和７年３月） ※個人情報の流れは、資料２６－１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　梅毒等の性感染症のまん延防止事業に係る業務の委託について

保有課(担当課)	保健予防課
登録業務の名称	梅毒等の性感染症のまん延防止事業業務委託
委託先	未定（特命随契方式により決定する予定。）（プライバシーマーク取得事業者を予定）
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)	《健康相談に係る情報項目》 相談者の氏名、電話番号、年齢、性別、メールアドレス、相談内容
処理させる情報項目の記録媒体	紙及び電磁的媒体（委託先のパソコン）
委託理由	性感染症に対して知識・認識を持っていないものに対して、委託先である一般社団法人の知見を活用したアウトリーチ型支援や健康相談等を実施することで、普及啓発・早期発見および感染症予防対策の強化を図る。
委託の内容	① 周知用リーフレット作成 性感染症についての正しい知識と理解につなげるために、リーフレット等を作成し、正確でわかりやすい情報発信に努め、普及啓発を進めていく。 ② アウトリーチ型支援 区内の繁華街（主にシネシティ広場や大久保公園周辺）に集まる若者などを対象にリーフレット等を配布し、梅毒等の性感染症への注意喚起や、区で実施する無料匿名の性感染症検査の周知を行う。 週 3 日（月・水・金)、1 日あたり 3 時間(17～20 時)の対応を予定。 ③ 健康相談 アウトリーチ時に、必要に応じて健康相談に応じる。また、配布するリーフレット等に健康相談窓口の電話番号やメールアドレスなどを記載し、性感染症に不安を抱える対象者からの相談に電話やメールで対応する。 週 5 日（月～金)、1 日あたり 4 時間(14～18 時)の対応を予定。
委託の開始時期及び期限	令和 6 年 8 月 1 日から令和 7 年 3 月 31 日まで (次年度以降も、同様の業務委託を行う予定。)
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。

【梅毒等の性感染症のまん延防止業務委託に係る個人情報の流れ】　（資料２６－１）

区内の繁華街に集まる若者等

受託事業者

①アウトリーチ型支援
（周知用リーフレット配布、
区の性感染症検査周知、
健康相談について周知）

②健康相談（様々な悩み・課題を相談）
（電話・メール）

③健康相談記録作成

・不正侵入検知・通知・遮断
（ファイアウォール/ IDS/IPS）
・Web脆弱性攻撃防止(WAF)
・標的型攻撃対策
・ふるまい検知・通報・遮断
・通信制御(特定通信のみ許可)
・ウイルス対策 ・多要素認証
・データ暗号化 ・アクセス制御
・サーバ冗長化 ・バックアップ
・操作履歴取得 ・ログ取得

新宿区

⑤健康相談記録の確認

【区PC】

健康相談情報
・氏名
・電話番号
・年代
・性別
・メールアドレス
・相談内容

・不正侵入検知・通知・遮断
（ファイアウォール/ IDS/IPS）
・Web脆弱性攻撃防止(WAF)
・標的型攻撃対策
・ふるまい検知・通報・遮断
・通信制御(特定通信のみ許可)
・ウイルス対策 ・多要素認証
・データ暗号化 ・アクセス制御
・サーバ冗長化 ・バックアップ
・操作履歴取得 ・ログ取得

【委託先PC】

健康相談情報
・氏名
・電話番号
・年代
・性別
・メールアドレス
・相談内容

※区の匿名・無料の性感染症検査への申込（電話申請）

④健康相談記録提出（USBメモリ・毎月手渡し）

・カギ付きカバンに入れて運搬
・暗号化機能付きＵＳＢメモリを利用し、管理簿に記載

・責任者及び取扱者の選定
・ウイルス感染の防止
・不正な通信の検知、分析、遮断
・ネットワーク機器の制限及びアクセスの制御
・ID／パスワード認証
・操作ログ管理
・紙媒体の相談記録等は鍵付キャビネットで保管し、委託先PCに転記保存後、すべて廃棄させる。

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。