資料4

個人情報保護管理運営会議　付議事項

件名	新宿区防犯機器等購入緊急補助事業に係るシステムの構築等について（委託内容の追加）

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：危機管理担当部危機管理課）

事業の概要

事業名	防犯機器等購入緊急補助事業
担当課	危機管理課
目　的	住宅における犯罪を未然に防止するため、防犯機器等の購入及び設置工事（以下「購入等」という。）をした区民に対し、その費用の一部補助を行い、区民の防犯意識の高揚と安全で安心な暮らしの実現に寄与することを目的とする。
対象者	防犯機器等の購入等をした住宅（新宿区の区域内に存するものに限る。）に居住している区民
事業内容	1　概要 昨今、いわゆる「闇バイト」が関係すると思われる強盗・侵入窃盗事件等が発生し、区民の体感治安が悪化している。 このような状況の中、住宅における犯罪を未然に防止するため、防犯機器等の購入等をした区民に対し、その費用の一部補助を行い、区民の防犯意識の高揚と安全で安心な暮らしの実現に寄与するため、令和７年度から新宿区防犯機器等購入緊急補助事業を実施している。（令和７年度第１回新宿区新宿区個人情報保護管理運営会議了承済み） ついては、新宿区内に住民登録のある区民が、その居住する住居に実施する防犯対策として、対象となる防犯対策用品の購入等をした場合に、その費用の総額の２分の１（補助金の上限額は２万円とし、申請は１世帯につき１回限りとする。千円未満の端数が生じた場合は、これを切り捨てる）を補助する。 過去に補助金の交付を受けている区民は対象外となることから、重複交付を防止するため、委託事業者が過去の交付実績を確認する。 2　個人情報保護管理運営会議への付議内容 （1）電算処理 補助対象者を正確かつ迅速に把握し、円滑な支給事務に資するとともに、補助対象者からの問い合わせに対応するため、進捗状況を一元的に管理するための補助管理システムを構築する。 （2）外部結合 委託事業者の構築する補助管理システムとのデータの連携を行う。 （3）業務委託 申請書類の受理（LoGo フォームへの電子申請内容の確認**及び新宿区防犯機器等購入緊急補助事業の補助金交付決定者との重複確認**）、補助管理システムの構築及び入力、、交付決定通知書等の印刷、発送及びコールセンター業務について、迅速かつ安全に行う必要があるため、専門的な知識等を有し、豊富なノウハウを備えた業者に委託する。 3　対象者数 １，０００人　※個人情報の流れは、資料４－１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　新宿区防犯機器等購入緊急補助事業に係るシステムの構築について

※太字ゴシック（下線）が、令和７年度第１回新宿区個人情報保護管理運営会議承認済の内容からの変更箇所

保有課（担当課）	危機管理課
登録業務の名称	新宿区防犯機器等購入緊急補助事業
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 ⑴　新宿区防犯機器等購入緊急補助事業の申請者 **⑵　新宿区防犯機器等購入緊急補助事業の補助金交付決定者** ２　記録項目 ⑴　新宿区防犯機器等購入緊急補助事業の申請者 郵便番号、住所、氏名、生年月日、電話番号、メールアドレス、世帯主名（続柄）、購入した防犯対策用品に関する情報、補助申請額、振込先に関する情報（振込先金融機関、預金種目、口座番号、口座名義、口座名義フリガナ）、誓約・同意状況、申請の受付日、審査日、補正依頼日、補正の内容、問合せ対応履歴、入金状況（口座不備による再振込手続き情報を含む）、補助の可否、補助決定額 **⑵　新宿区防犯機器等購入緊急補助事業の補助金交付決定者** **住所、氏名** ３　記録するコンピュータ 補助管理システム（委託先が設置・管理するサーバ上に構築）
新規開発・追加・変更の理由	申請者から提出された申請書の内容を正確に把握し、申請の受付状況等を一元的に管理することにより、補助金交付事務を円滑に実施するとともに、申請者からの問合せに適切に対応するための補助管理システムを構築する。
新規開発・追加・変更の内容	申請者ごとの申請書及び添付書類の内容及び受付状況などの進捗状況を管理するシステムを委託先が設けるサーバ上に構築する。
新規開発・追加・変更の内容	**申請者ごとの申請書及び添付書類の内容及び受付状況などの進捗状況を管理するシステムに、過去の交付決定者リストを追加する。**
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８年４月初旬　　構築 令和８年４月中旬　　テスト 令和８年５月　　本稼働

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　新宿区防犯機器等購入緊急補助事業に係る外部結合について

※太字ゴシック(下線)が、令和７年度第１回新宿区個人情報保護管理運営会議承認済の内容からの変更箇所

保有課（担当課）	危機管理課
登録業務の名称	新宿区防犯機器等購入緊急補助事業
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 ⑴　新宿区防犯機器等購入緊急補助事業の申請者 **⑵　新宿区防犯機器等購入緊急補助事業の補助金交付決定者** ２　記録項目 ⑴　新宿区防犯機器等購入緊急補助事業の申請者 郵便番号、住所、氏名、生年月日、電話番号、メールアドレス、世帯主名（続柄）、購入した防犯対策用品に関する情報、補助申請額、振込先に関する情報（振込先金融機関、預金種目、口座番号、口座名義、口座名義フリガナ）、誓約・同意状況、申請の受付日、審査日、補正依頼日、補正の内容、問合せ対応履歴、入金状況（口座不備による再振込手続き情報を含む）、補助の可否、補助決定額 **⑵　新宿区防犯機器等購入緊急補助事業の補助金交付決定者** **住所、氏名** ３　記録するコンピュータ 補助管理システム（委託先が設置・管理するサーバ上に構築）
結合の相手方	株式会社セゾンパーソナルプラス ※プライバシーマーク及びISMS（ISA1S0383）認証取得事業者
結合する理由	新宿区防犯機器等購入緊急補助事業に係る申請者について、申請書の内容を速やかに入力し、申請の内容を正確に把握することにより、補助金交付事務を円滑に実施するとともに、申請者からの問合せ等を適切に行うため。 また、一元管理された申請者及び受付状況等を、委託事業者の補助管理システムと区に貸与された補助管理システム用専用端末を通じてリアルタイムに情報を確認、共有するため。 （専用端末は委託事業者保有の端末だが、委託契約の仕様上、危機管理課へ１台整備する。）
結合の形態	危機管理課の職員が、室内に整備された専用端末から閉域ネットワーク（ＶＰＮ）に接続の上、委託先の補助管理システムへアクセスし、申請者の情報閲覧、登録内容の更新等を行う。
結合の開始時期と期間	**令和８年５月１日から令和９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

別紙(業務委託)

◇業務委託(第３条第１項第３号)

件名　新宿区防犯機器等購入緊急補助事業に係る業務の委託について

※太字ゴシック(下線)が、令和７年度第１回新宿区個人情報保護管理運営会議承認済の内容からの変更箇所

保有課(担当課)	危機管理課
登録業務の名称	新宿区防犯機器等購入緊急補助事業
委託先	株式会社セゾンパーソナルプラス ※プライバシーマーク取得及びISMS（ISA1S0383）認証取得事業
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)	１　個人の範囲 ⑴　新宿区防犯機器等購入緊急補助事業の申請者 **⑵　新宿区防犯機器等購入緊急補助事業の補助金交付決定者** ２　記録項目 ⑴　新宿区防犯機器等購入緊急補助事業の申請者 郵便番号、住所、氏名、生年月日、電話番号、メールアドレス、世帯主名（続柄）、購入した防犯対策用品に関する情報、補助申請額、振込先に関する情報（振込先金融機関、預金種目、口座番号、口座名義、口座名義フリガナ）、誓約・同意状況、申請の受付日、審査日、補正依頼日、補正の内容、問合せ対応履歴、入金状況（口座不備による再振込手続き情報を含む）、補助の可否、補助決定額 **⑵　新宿区防犯機器等購入緊急補助事業の補助金交付決定者** **住所、氏名**
処理させる情報項目の記録媒体	紙及び電磁的媒体（補助管理システム）
委託理由	当該事業について、迅速かつ安全に行う必要があるため、専門的な知識等を有し、豊富なノウハウを備えた業者に委託する。
委託の内容	１　申請書の受理業務（LoGoフォームへの電子申請内容の確認**及び新宿区防犯機器等購入緊急補助事業の補助金交付決定者との重複確認**） ２　補助管理システムへの申請内容の入力業務 ３　補助金交付決定通知書の作成、印刷及び送付業務 ４　電話による制度や申請方法の案内、申請書作成補助等の相談業務
委託の開始時期及び期限	**令和８年４月１日から令和９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

防犯機器等購入緊急補助事業の個人情報の流れ

（資料４－１）

※赤点線の部分が、今回の変更箇所

区民

①防犯対策用品の購入・設置

防犯カメラ

センサーライト

カメラ付きインターホン

委託事業者

補助管理システム

③提出された申請書の内容を確認し、補助実績台帳に入力することで、区の専用端末と連携（申請の受付状況の進捗管理）

④申請者情報と過年度交付決定者の重複確認

コールセンターの開設

・制度・申請方法の案内
・申請書類の作成補助
・その他相談対応

⑨交付・不交付決定通知書の作成・印刷

・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

※区の専用端末は、委託事業者から貸与されており、データは連携している。

新宿区

補助管理システム用専用端末

⑥補助管理システム用専用端末へ連携された申請書情報をイントラパソコンへ保存（ＵＳＢメモリ）

⑧交付・不交付決定データを補助管理システム用専用端末へ保存（ＵＳＢメモリ）

イントラパソコン

⑦申請書情報等の確認・決定

・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

②申請書の送付（郵送）

②LoGoフォームでの申請

LoGo フォーム

【インターネット回線】　【LGWAN回線】

【専用回線】

⑤申請書の送付（紙・手渡し）

（随時）制度・申請方法の案内等

⑩交付・不交付決定通知書の送付

⑪補助金の振込

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。