資料61

個人情報保護管理運営会議　付議事項

件名	５歳児健康診査の実施に伴う健康管理システムの改修等について

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：健康部健康づくり課）

事業の概要

事業名	乳幼児健康診査（５歳児健康診査）
担当課	健康づくり課、牛込保健センター、四谷保健センター、東新宿保健センター、落合保健センター
目　的	言語の理解能力や社会性が育つ５歳児の時期に健康診査を行うことで、子どもの行動などの特性に気づく機会を提供するとともに、庁内連携を強化し、健診当日から様々な専門相談に応じることで適切な支援に繋げることを目的とする。
対象者	実施年度に満５歳になる幼児のうち希望する者
事業内容	１　概要 子どもの発達については個々の特性を早期に把握し、当該幼児とその保護者に対して保健や福祉など様々な分野が連携して支援を行い、安心して就学することができる環境を整える必要があり、令和６年７月以降、標準化に対応したガバメントクラウド上に健康管理システムを構築している（令和５年度第９回新宿区個人情報保護管理運営会議承認済み）。 国では、令和５年度以降、乳幼児健康診査（５歳児健康診査）が「母子保健衛生費」の一事業として位置づけられたため、東京都においても、令和７年度に健診後のフォローアップや人材の配置支援を目的とした「５歳児健診区市町村支援事業費」という補助金が新設された。 区においては、上記補助金を活用した支援体制の強化を図るため、５歳児健診についても、既存の健康管理システム（対物系）の対象者情報を一元管理し、庁内での連携を迅速かつ正確に実施する必要があることから、デジタル庁が提供するガバメントクラウドシステムを利用した運用を行う。 ２　個人情報保護管理運営会議への付議内容 （１）電算処理 健康管理システムに５歳児健康診査の管理機能（標準化項目）を実装する。 （２）外部結合 健康管理システム（対物系）標準化にあたり、デジタル庁が提供するガバメントクラウド上に事業者が構築する標準準拠システムを運用し、ガバメントクラウドとの結合を行う。 （３）業務委託 健康管理システムの改修及び運用保守業務を委託する。 ３　対象者数 約９００人（２５人×４保健センター×９か月） ※令和８年７月より事業開始予定 ※個人情報の流れは、資料６１－１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　５歳児健康診査の実施に伴う健康管理システムの改修について

※太字ゴシック（下線）が、令和５年度第９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）	健康づくり課、牛込保健センター、四谷保健センター、東新宿保健センター、落合保健センター
登録業務の名称	乳幼児健康診査**（５歳児健康診査）**
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 **５歳児健康診査の対象者** ２　記録項目 資料６１－２のとおり ３　記録するコンピュータ 健康管理システム（ガバメントクラウド上に設置)
新規開発・追加・変更の理由	子どもの発達については個々の特性を早期に把握し、当該幼児とその保護者に対して保健や福祉など様々な分野が連携して支援を行い、安心して就学することができる環境を整えることが必要であることから、区においても令和８年度より５歳児健康診査を実施する。 実施にあたり、既存の健康管理システム（対物系）において、対象者の情報を一元管理し、迅速かつ正確な事務処理を行う。
新規開発・追加・変更の内容	**５歳児健康診査の管理機能（標準化項目）の追加**
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３月　　開発** **令和８年４月　　テスト** **令和８年７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　５歳児健康診査の実施に伴う健康管理システムの外部結合について

※太字ゴシック（下線）が、令和５年度第９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）	健康づくり課、牛込保健センター、四谷保健センター、東新宿保健センター、落合保健センター
登録業務の名称	乳幼児健康診査**（５歳児健康診査）**
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 **５歳児健康診査の対象者** ２　記録項目 資料６１－２のとおり
結合の相手方	デジタル庁（ガバメントクラウドの運用主体）
結合する理由	標準化法第１０条において、標準準拠システムの利用においてはガバメントクラウドの利用を第一に検討することとされており、セキュリティ面やコスト面等が優れていることから、デジタル庁が提供するガバメントクラウドシステムに構築する生活保護システム等を利用する必要があるため。
結合の形態	情報戦略課が提供する区イントラ端末から、ガバメントクラウド接続サービスを利用して、生活保護システム等が構築されているガバメントクラウドに結合する。
結合の開始時期と期間	**令和８年７月（予定）**（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　５歳児健康診査の実施に伴う健康管理システムの改修に係る業務の委託について

※太字ゴシック（下線）が、令和５年度第９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)	健康づくり課、牛込保健センター、四谷保健センター、東新宿保健センター、落合保健センター
登録業務の名称	乳幼児健康診査**（５歳児健康診査）**
委託先	株式会社両備システムズ (プライバシーマーク、ＩＳＯ２７００１取得)
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 **５歳児健康診査の対象者** ２　記録項目 資料６１－２のとおり
処理させる情報項目の記録媒体	電磁的媒体（健康管理システム）
委託理由	上記委託先は、本システムの開発事業であり、システムの改修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　システム改修業務 **５歳児健康診査の管理機能（標準化項目）の追加** ２　保守業務 （１）システムの保守・障害復旧 （２）運用支援、問い合わせ対応
委託の開始時期及び期限	**令和８年３月１日から令和８年６月３０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

【５歳児健康診査における個人情報の流れ】

（資料６１－１）

※令和５年度第９回管理運営会議で承認された母子保健（乳幼児健康診査）の項目に、５歳児健康診査の情報を追加する。

区民

・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
・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

①LoGoフォーム又はTELで予約

LoGoフォーム

【インターネット回線】　【LGWAN回線】

②予約した保健センターに来庁

新宿区（各保健センター）

③５歳児健康診査の実施

イントラネット
（情報戦略課管理）

事務処理内容

母子保健（乳幼児健康診査）

・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

ガバメントクラウド接続サービス（専用回線）

通信暗号化

④健診情報の照会・入力

【電算処理】
【外部結合】
管理項目の追加
（ガバメントクラウド接続サービスを利用してガバメントクラウドとの情報連携）

・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
・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

ガバメントクラウド

【業務委託】
・管理項目の追加
・システムの運用保守および障害対応

委託事業者
（株式会社両備システムズ）

健康管理システム
（標準準拠・新宿区専用）

対象者データ

氏名、住所、性別、
生年月日、宛名番号、
受診日、健診結果など

・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

（新）健康管理システムの記録項目

【1】基本情報

(1) 住民情報

市区町村コード、宛名番号、個人履歴番号、世帯番号、住民種別、住民状態、個人番号、異動年月日、異動届出日、異動事由、氏名、旧氏、通称、氏名優先区分、性別、生年月日、続柄、住所、方書、郵便番号、住民となった日、転入前住所、消除の届出日、消除の異動年月日、転入通知年月日、転出先住所（予定）、転出先住所（確定）、国籍、在留資格

(2) 支援措置対象者情報

支援措置区分、履歴番号、支援措置期間

(3)-1 課税情報（共通）

課税年度、未申告区分、他団体課税対象者区分、他団体課税対象者の市区町村コード、課税情報履歴番号、課税非課税区分

(3)-2 課税情報（障害者福祉）

課税年度、未申告区分、他団体課税対象者区分、他団体課税対象者の市区町村コード、課税非課税区分、徴収区分、異動事由、異動日、更生日、控除対象配偶者区分、扶養控除対象区分、本人該当区分、扶養人数、所得金額、控除額、収入額、市町村民税所得割額、市町村民税均等割額、都道府県民税均等割額、森林環境税額

(4) 国保情報

被保険者履歴番号、市区町村保険者番号、保険者名称、記号番号、枝番、資格区分、資格取得年月日、資格取得事由、資格喪失年月日、資格喪失事由、適用開始年月日、適用終了年月日、証区分、有効期限、マル学マル遠区分

(5) 後期高齢者医療

被保険者番号、個人区分、被保険者資格取得事由、被保険者資格取得年月日、被保険者資格喪失事由、被保険者資格喪失年月日、保険者番号適用開始年月日、保険者番号適用終了年月日

(6) 生活保護

申請履歴番号、停止年月日、停止解除年月日、単併給区分、扶助フラグ（生活、住宅、教育、医療、出産、生業、葬祭）、生活保護開始年月日、廃止年月日

(7) 介護保険

介護保険者番号、被保険者番号、資格履歴番号、被保険者区分コード、資格取得日、資格喪失日、要介護認定状況、要介護状態区分、要介護認定日、要介護認定有効期間開始日、要介護認定有効期間終了日、公費受給者番号

(8) 障害者福祉

履歴番号、返還日、資格状態、初回交付日、手帳番号、統計部位、障害名、障害種別、総合等級

【2】健康管理業務情報

(1) 業務共通

住登外者情報、医療機関情報、会場情報、事業従事者情報、地区管理、事業予定、個人連絡先、送付先情報、健(検)診予約希望者管理、帳票発送履歴情報、帳票発行対象外者情報、メモ情報、フォロー情報、 実施報告書(日報)情報、伝言情報、メモ情報(世帯)、電子ファイル情報、希望調査結果

(2) 成人保健

希望調査結果情報、胃がん一次検診情報、肺がん一次検診情報、子宮頸がん一次検診情報、骨粗鬆症一次検診情報、歯周疾患一次検診情報、大腸がん一次検診情報、乳がん一次検診情報、肝炎ウイルス一次検診情報、成人保健_独自施策情報(一次)情報、胃がん精密検査情報、肺がん精密検査情報、子宮頸がん精密検査情報、骨粗鬆症精密検査情報、歯周疾患検診精密検査情報、大腸がん精密検査情報、乳がん精密検査情報、肝炎ウイルス精密検査情報、成人保健_独自施策情報(精検)情報、成人保健_訪問申込情報、成人保健_訪問結果情報、成人保健_個別指導申込情報、成人保健_個別指導結果情報、成人保健_集団指導申込情報、成人保健_集団指導結果情報

(3) 成人保健(密接関連業務)

健康診査情報、保健指導等情報

(4) 母子保健

妊娠届出情報、妊娠届出アンケート情報、母子健康手帳交付情報、出産の状態に係る情報、妊婦健診結果情報、妊婦健診費用助成情報、妊産婦歯科健診結果情報、妊産婦歯科精健結果情報、妊婦精健結果情報、産婦健診結果情報、産婦健診費用助成情報、産婦精密健診結果情報、産後ケア事業情報、母子保健_独自施策情報(母)、出生時状況情報、新生児聴覚検査結果情報、新生児聴覚スクリーニング検査費用助成情報、乳幼児健診対象者情報、3～4か月児健診結果情報、3～4か月児健診アンケート情報、1歳6か月児健診結果情報、1歳6か月児健診アンケート情報、1歳6か月児歯科健診結果情報、3歳児健診結果情報、3歳児健診アンケート情報、3歳児歯科健診結果情報、**5歳児健診結果情報、5歳児健診アンケート情報**、健診受診履歴情報、精密健診の依頼情報、乳幼児精密健診結果情報、未受診者勧奨情報、母子保健_独自施策情報(子)、母子保健_訪問申込情報、母子保健_訪問結果情報、母子保健_個別指導申込情報、母子保健_個別指導結果情報、母子保健_集団指導申込情報、母子保健_集団指導結果情報、養育医療申請情報、養育医療実績情報

(5) 予防接種

接種種類、接種回数、予診票発行情報、他市区町村依頼情報、各種予防接種実績、風疹抗体検査実績、健康被害救済制度情報、罹患情報

(6) 医療費公費

精神障害者保健福祉手帳情報、精神通院医療情報、精神通院医療診療内容情報、難病申請情報、小児慢性申請情報

(7) 結核管理

患者基本情報、診査会情報、菌検査情報、勧告管理情報、接触者基本情報、接触者健診情報

(8) 保健師活動

保健相談記録(西暦年度、センター区分、相談保健師名、相談年月日、相談種別、保健相談内容)

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。
	○	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。
	○	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。
	○	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。
	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。
	○	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。
	○	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。
	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。