

個人情報保護管理運営会議 付議事項

件名	新宿区子育て応援臨時給付金支給事業に係るシステム改修等について
----	---------------------------------

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、業務委託）

（担当部課：子ども家庭部児童育成担当課）

事業の概要

事業名	新宿区子育て応援臨時給付金支給事業について
担当課	児童育成担当課
目 的	物価高の影響が長期化する中で、特にその影響を強く受けている子育て世帯を応援するため
対象者	① 令和8年9月分の児童手当受給者(公務員を含む) ② ①の受給者ではないが、基準日(令和8年9月17日)時点で住民基本台帳に記録されている令和8年9月分の児童手当の受給資格があった児童の父母等 ※ ①のうち公務員及び②については、基準日(令和8年9月17日)に、支給対象者が住民基本台帳に記録されていることを要件とする。
事業内容	1 概要 物価高の影響が長期化する中、特に、その影響を強く受けている子育て世帯を応援し、子どもたちの健やかな成長を応援する観点から、児童手当受給者に区独自の給付金を支給する。 区では公務員の児童手当受給情報を保有していないことから、令和7年度物価高対応子育て応援手当受給者(申請分)の実績情報を基に、当該事業の申請案内を行うこととする。 なお、令和7年度物価高対応子育て応援手当支給事業以降に区に転入した公務員の方については、広報新宿や区公式HP・SNS等の広報施策により幅広く周知し、申請案内を行う。当該対象者については、区公式HPまたは児童育成担当課の窓口にて申請書を交付する。 2 個人情報保護管理運営会議への付議内容 (1) 電算処理 本事業は、既存の児童手当システムを活用し対象者の管理を行うが、臨時的な新規事業であるため、以下の改修を行うことで、事務の効率化及び円滑化や二重支給の防止を図ることとする。 ① 支給対象者の管理機能の追加(児童手当システムに登録のない給付対象者の登録を含む) ② 支給対象者CSVファイル作成機能の追加 ③ 指定口座に子育て応援臨時給付金を支払うための支払データを作成する機能の追加 (2) 業務委託(電算処理) 株式会社電算に委託し、実施することとする。本システムの開発業者であり、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である。 (3) 業務委託(封筒への印字出力及び封入封緘) 支給対象者へ送付する封筒への宛名ダイレクト印字出力及び封入封緘業務委託。 3 対象者数 支給者数 約24,000人 児童数 約38,000人 (プッシュ型約22,000人、申請型約2,000人) ※個人情報の流れは、資料36-1から36-3のとおり

件名 新宿区子育て応援臨時給付金支給事業の実施に係る児童手当システムの開発について

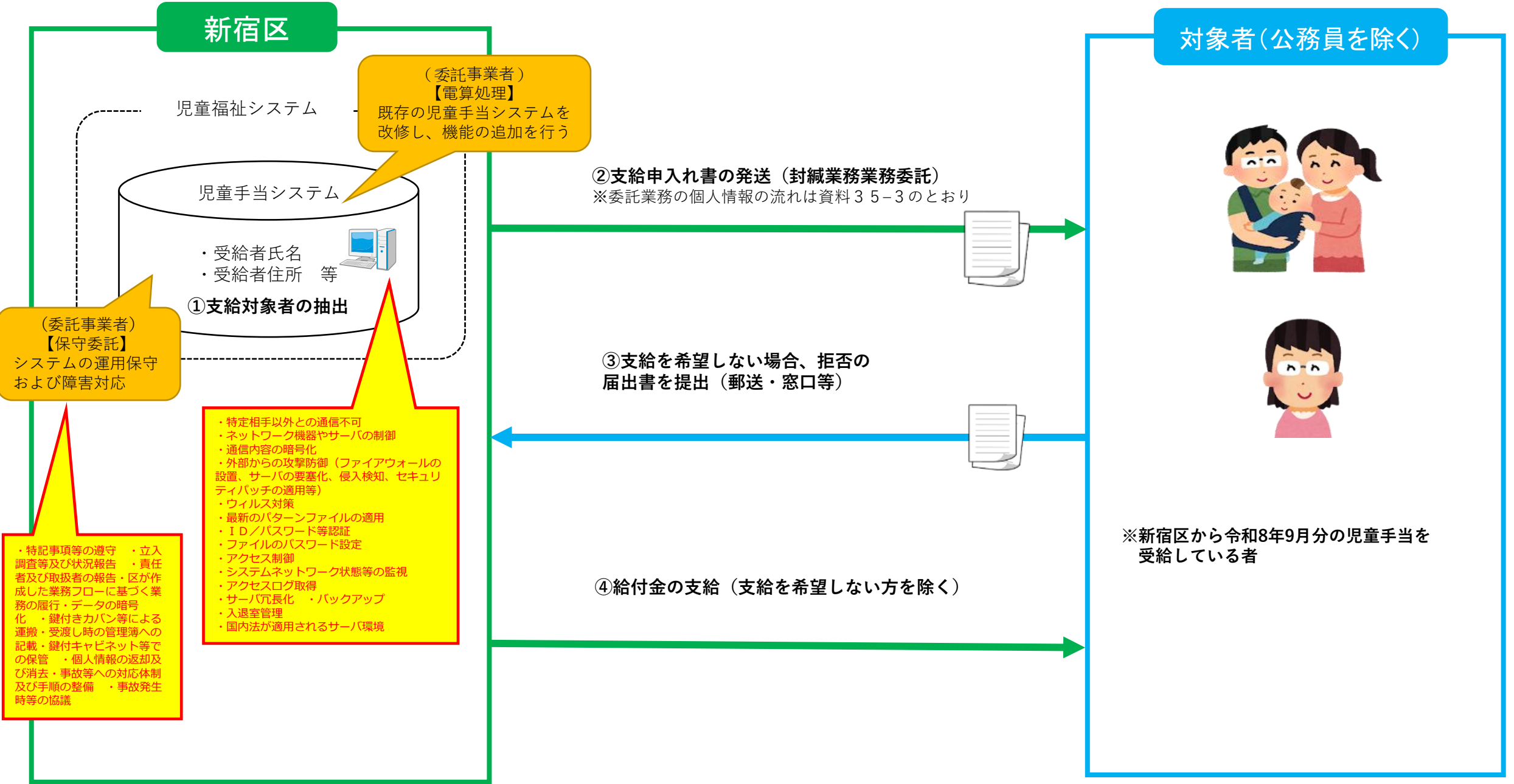
保有課（担当課）	児童育成担当課
登録業務の名称	新宿区子育て応援臨時給付金支給事業
記録される情報項目（だれの、どのような項目が、どここのコンピュータに記録されるのか）	1 個人の範囲 新宿区子育て応援臨時給付金支給事業の支給対象者 2 記録項目 受給者・児童(氏名、住民番号、生年月日、児童順位、住所、続柄、同居別居)、児童手当受給該当年月、喪失年月日、R8 年度所得、支払口座情報、支給実績(年月) 3 記録するコンピュータ 児童福祉システム内の児童手当システム（情報戦略課が管理する情報システム統合基盤サーバー）
新規開発・追加・変更の理由	本事業は、臨時的な新規事業であるため、支給対象者の管理を行う機能の追加等の改修を行うことで、事務の効率化及び円滑化や二重支給の防止を図ることとする。
新規開発・追加・変更の内容	1 支給対象者の管理機能の追加 2 支給対象者 CSV ファイル作成機能の追加 3 指定口座に子育て応援臨時給付金を支払うための支払データ作成機能の追加
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9月 開発・テスト 令和8年10月 本稼働

件名 新宿区子育て応援臨時給付金支給事業の実施に係る児童手当システムの開発について

保有課(担当課)	児童育成担当課
登録業務の名称	新宿区子育て応援臨時給付金支給事業
委託先	株式会社電算 (プライバシーマーク取得済み)
委託に伴い事業者処理させる情報項目 (だれの、どのような項目か)	受給者・児童(氏名、住民番号、生年月日、児童順位、住所、続柄、同居別居)、児童手当受給該当年月、喪失年月日、R8 年度所得、支払口座情報、支給実績(年月)
処理させる情報項目の記録媒体	電磁的媒体 (児童福祉システム内の児童手当システム)
委託理由	上記委託先は、本システムの開発業者であり、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 (1) 支給対象者の管理機能の追加 (2) 支給対象者 CSV ファイル作成機能の追加 (3) 指定口座に子育て応援臨時給付金を支払うための支払データ作成機能の追加 2 保守業務 (1) ハード、ソフトの保守・障害復帰 (2) 運用支援、問い合わせ対応等
委託の開始時期及び期限	令和8年9月18日から令和9年3月31日まで
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

件名 新宿区子育て応援臨時給付金支給事業の実施に係る業務の委託について

保有課(担当課)	児童育成担当課
登録業務の名称	新宿区子育て応援臨時給付金支給事業
委託先	未定
委託に伴い事業者処理させる情報項目(だれの、どのような項目か)	児童手当受給者の住所、氏名、認定番号
処理させる情報項目の記録媒体	電子媒体(委託先PC、CD-R・DVD-R等)
委託理由	大量の通数の印字及び封入封緘を行うため、委託により業務の効率化、処理時間の短縮を図る。
委託の内容	対象者への支給申入れ書の封入封緘業務の委託
委託の開始時期及び期限	令和8年9月18日から令和9年3月31日まで
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



新宿区

区PC



児童福祉システム

児童手当システム

・受給者氏名
・受給者住所 等

②対象者については
7年度支給事業の
公務員実績を利用

(委託事業者)
【電算処理】
既存の児童手当システムを改
修し、機能の追加を行う

(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

・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

①対象者への広報周知（広報新宿、区公式HP等）
及び申請書の交付

③公務員への案内文の発送（申請書同封）

④申請書の提出（郵送・窓口等）
対象者の職場から児童手当の受給していることが分かる書類添付

⑥非該当者への通知文郵送

⑧支給決定通知郵送

⑨給付金の支給

⑤申請書内容の確認及び
児童手当システムへの登録



⑦支払いデータの作成



・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）
・ウイルス対策
・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

対象者

区内在住の公務員



※令和8年9月分の児童手当受給者であり、
基準日（令和8年9月17日）時点で住民基本
台帳に記録されていることを要件とする。

9月分の児童手当の未受給者



※令和8年9月分の児童手当を受給してい
なかったが、基準日時点で児童手当の支
給対象に該当するとみなすことができ
れば、申請に基づき、子育て応援臨時給付
金を支給する。

新宿区子育て応援臨時給付金支給事業にかかる支給申入れ書送付用宛名の印字及び封入封緘業務の委託に係る個人情報の流れ

資料 3 6 - 3

新宿区

委託先

対象者

児童手当システム

①対象者データを抽出

受給者住所、受給者氏名、認定番号

②印字データ（CD-R、DVD-R等）の提供

③封筒に個人情報を印字出力

④印字した封筒への支給申入れ書封入封緘

⑤印字データ（CD-R、DVD-R等）の返却

⑥封入封緘後の封筒の納品（紙・手渡し）

⑧納品検査後、納品（紙・手渡し）

⑦納品検査

- ・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
- ・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
- ・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

- ・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

- ・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

⑨委託先が郵便局に持ち込み対象者に発送



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。
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】	○	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。
	○	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。
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】	○	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、十分な検証を行わせる。
	○	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「－」	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ある場合は、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「－」	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ある場合は、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。