

個人情報保護管理運営会議 付議事項

件名	地方公共団体情報システム標準化に対応した就学事務システム（学齢簿編製等・就学援助）への移行等について
----	--

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：教育委員会事務局学校運営課、教育委員会事務局教育支援課）

事業の概要

事業名	地方公共団体情報システム標準化に対応した就学事務システム（学齢簿編製等・就学援助）への移行等について
担当課	学校運営課、教育支援課
目 的	「地方公共団体情報システムの標準化に関する法律」（令和３年法律第４０号。以下「標準化法」という。）に基づき、地方公共団体情報システムの標準化に対応した就学事務システム（学齢簿編製等・就学援助）をガバメントクラウド上で構築し、就学関連業務の標準化及び効率化に寄与することを目的とする。
対象者	就学児童・生徒及びその保護者
事業内容	1 概要 令和３年９月に公布された標準化法に基づき、現行の学齢簿・就学援助システムから標準仕様書に準拠した就学事務システム（学齢簿編製等・就学援助）への移行を行う。就学事務システム（学齢簿編製等・就学援助）はガバメントクラウドを利用して運用する。 2 個人情報保護管理運営会議への付議内容 (1) 電算処理 就学に関する事務（学齢簿編製、在籍管理、就学援助等）を標準仕様書に準拠した就学事務システム（学齢簿編製等・就学援助）へ移行する。 (2) 外部結合 デジタル庁が提供するガバメントクラウド上に、事業者が構築する就学事務システム（学齢簿編製等・就学援助）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 現行システムからガバメントクラウドへのデータ移行作業及び運用保守業務を委託する。 3 対象者数 約 50,000 人 ※ 個人情報の流れは、資料２９－１のとおり

件名 地方公共団体情報システム標準化に対応した就学事務システム(学齢簿編製等・就学援助)への移行について

保有課(担当課)	学校運営課、教育支援課
登録業務の名称	学齢簿編製、在籍管理、就学援助等に関する業務
記録される情報項目(だれの、どのような項目が、どのコンピュータに記録されるのか)	1 個人の範囲 就学児童・生徒及びその保護者 2 記録項目 資料29-2のとおり 3 記録するコンピュータ 就学事務システム(学齢簿編製等・就学援助) (ガバメントクラウド上に構築)
新規開発・追加・変更の理由	標準仕様書に準拠した就学事務システム(学齢簿編製等・就学援助)をガバメントクラウド上で構築し、就学関連業務の標準化及び効率化に寄与する。
新規開発・追加・変更の内容	現在、学齢簿編製、在籍管理、就学援助等に関する業務を運用している学齢簿・就学援助システムから、標準仕様書に準拠した就学事務システム(学齢簿編製等・就学援助)へ移行する。就学事務システム(学齢簿編製等・就学援助)はガバメントクラウド上に構築する。
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9年4月～令和9年12月 移行期間 令和10年1月 本稼働

件名 地方公共団体情報システム標準化に対応した就学事務システム(学齢簿編製等・就学援助)への外部結合について

保有課(担当課)	学校運営課、教育支援課
登録業務の名称	就学事務システム(学齢簿編製等・就学援助)
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 就学児童・生徒及びその保護者 2 記録項目 資料29-2のとおり 3 記録するコンピュータ 就学事務システム(学齢簿編製等・就学援助) (ガバメントクラウド上に構築)
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、ガバメントクラウドの利用を第一に検討すべきとされているため、デジタル庁が提供するガバメントクラウドに結合する。
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、就学事務システム(学齢簿編製等・就学援助)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9年4月～令和9年12月 移行期間 令和10年1月 本稼働
情報保護対策	別添チェックリストのとおり

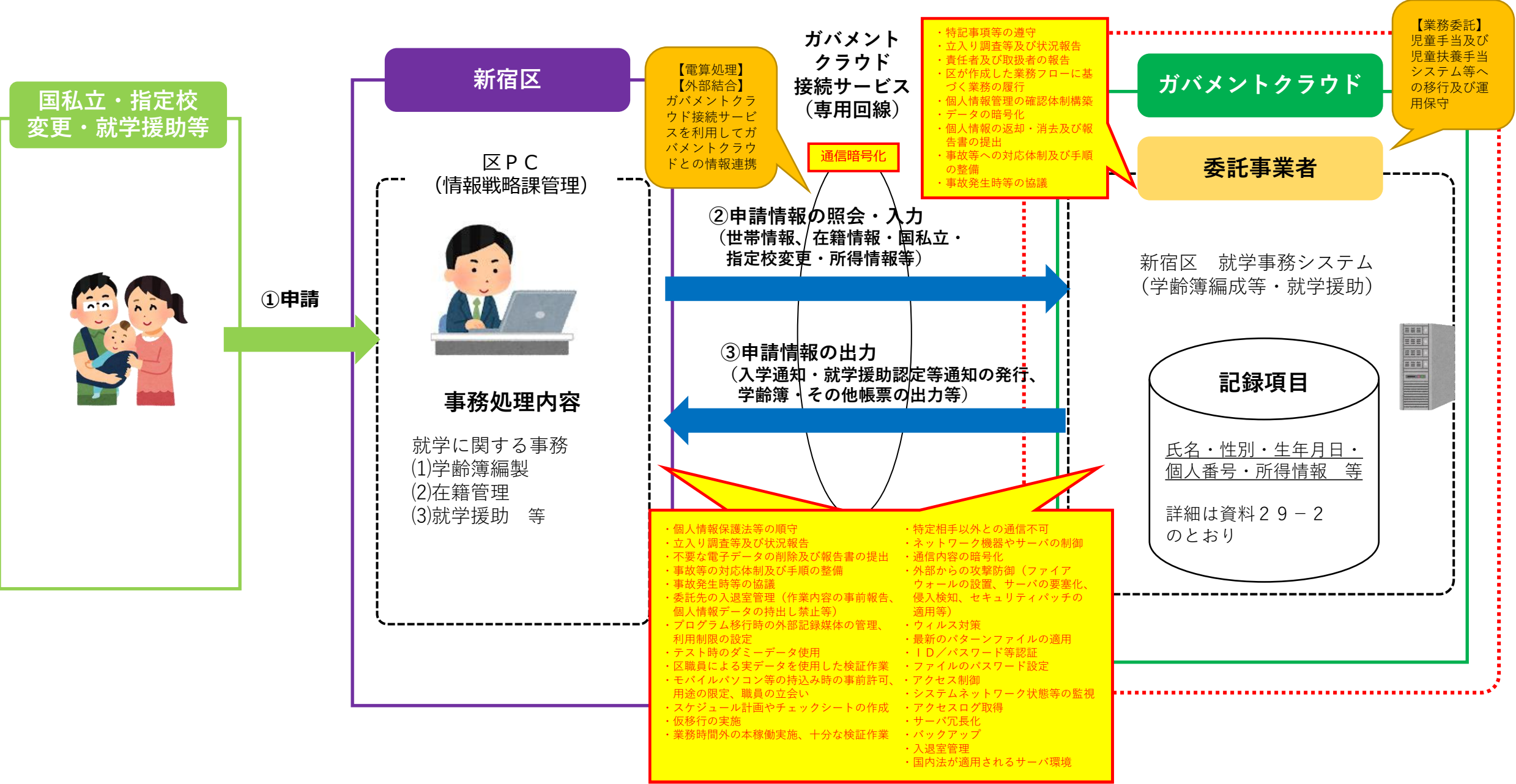
件名 地方公共団体情報システム標準化に対応した就学事務システム(学齢簿編製等・就学援助)への移行について

保有課(担当課)	学校運営課、教育支援課
登録業務の名称	学齢簿編製、在籍管理、就学援助等に関する業務
委託先	未定 (公募型プロポーザルにより委託事業者を決定する予定(プライバシーマーク等取得事業者を予定))
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)	1 個人の範囲 就学児童・生徒及びその保護者 2 記録項目 資料29-2のとおり
処理させる情報項目の記録媒体	電磁的媒体(就学事務システム(学齢簿編製等・就学援助))
委託理由	標準化法に基づき、現行の学齢簿・就学援助システムから地方公共団体情報システムの標準化に対応した就学事務システム(学齢簿編製等・就学援助)に移行するため。 委託先は未定であるが、現行の学齢簿・就学援助システムの開発・運用保守事業者である株式会社アクトは、これまでの業務履行実績が良好であることに加え、本区の業務仕様及び環境を熟知しているため、国が策定した標準仕様書を踏まえたデータ項目、業務機能、業務処理の見直し等を効率的に実施できるとともに、機能検証、データ移行及び本稼働の対応等の業務を限られた期間と体制の中で、安全かつ確実に行うことができると見込まれる。
委託の内容	標準仕様書に準拠した就学事務システム(学齢簿編製等・就学援助)をガバメントクラウド上に構築し、現行の学齢簿・就学援助システムからデータを移行し、就学事務システム(学齢簿編製等・就学援助)の運用保守を行う。
委託の開始時期及び期限	令和9年4月～令和9年12月 移行期間 令和10年1月 本稼働
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

児童手当及び児童扶養手当等が保有する個人情報のガバメントクラウドへ移行の流れ

(資料 2 9 - 1)

※赤枠の部分が、今回の付議事項。



就学事務システム（学齢簿編製等・就学援助）記録項目

【学齢簿編製等】

1 児童生徒データの管理

児童生徒の現住所、児童生徒の生年月日、児童生徒性別、児童生徒宛名番号（個人を識別するための番号、名寄せを行う際に必要）、児童生徒氏名の振り仮名（フリガナ）（外国籍を有する場合は外国人氏名のフリガナ及び通称名のフリガナをそれぞれ管理）、児童生徒通称名、児童生徒通称名のフリガナ、児童生徒国籍、児童生徒郵便番号、児童生徒前住所、児童の住所コード、児童の行政区（地域、地区、自治会）コード、世帯番号、世帯主宛名番号（個人を識別するための番号）、世帯主氏名、世帯主氏名の振り仮名（フリガナ）、居所（現住所と違う場合に使用）、居所不明状況、居所不明年月日※居所不明状況、居所不明年月日は、1年以上居所不明者である場合

2 保護者データの管理

保護者氏名（外国籍を有する場合は外国人氏名英字、外国人氏名漢字及び通称名をそれぞれ管理）、保護者の現住所、保護者と児童生徒との関係（児童生徒に対する保護者の続柄を管理 例：父、母など）、保護者宛名番号（個人を識別するための番号）、保護者氏名の振り仮名（フリガナ）（外国籍を有する場合は外国人氏名フリガナ及び通称名のフリガナをそれぞれ管理）、保護者国籍、保護者郵便番号、保護者電話番号又は携帯番号、保護者送付先情報、監護者情報、保護者のメールアドレス、保護者通称名、保護者通称名のフリガナ、保護者の住所コード、保護者の行政区（地域、地区、自治会）コード、保護者性別、身元引受人宛名番号（個人を識別するための番号）、身元引受人氏名、身元引受人振り仮名（フリガナ）、身元引受人住所、身元引受人電話番号又は携帯番号、身元引受人児童生徒との関係（児童生徒に対する身元引受人の続柄を管理 例：父、母など）、身元引受人のメールアドレス

3 区内学校関連データの管理

就学校名、学校入学年月日、学校編入学年月日、学校転学年月日、学校卒業年月日、指定小学校区（住所から判別されるものを管理）、指定中学校区（住所から判別されるものを管理）、就学指定校名（学校区から判別されるものを管理）、退学年月日※就学指定校名、退学年月日は、小学校・中学校等の記載欄が必要、学級区分（通常の学級、特別支援学級）、学年、就学校変更事由、就学校変更申請年月日、就学校変更許可年月日、就学校変更開始年月日、就学校変更終了年月日、原級留置に関する事項（例 原級留置決定年月日、原級留置開始年月日、原級留置終了年月日、原級留置理由）、不就学情報（例 不就学開始年月日、不就学終了年月日、不就学理由、副籍校名（特別支援学校就学時のみ使用）、転入前学校、就学援助有無、転出先学校、クラス、出席番号、学籍番号、就学校変更区分、就学校変更不許可理由、就学校変更開始学年、希望就学校名（学校選択制導入自治体のみ使用、選択希望校を管理）、希望就学校受付年月日（学校選択制導入自治体のみ使用）、就学校区分

4 区域外学校関連データの管理

就学校名、設置者名、学校入学年月日、学校編入学年月日、学校転学年月日、学校卒業年月日、学校退学年月日、区域外就学事由、区域外就学申請年月日、区域外就学許可年月日、区域外就学開始年月日、区域外就学終了年月日、区域外就学区分、区域外就学不許可理由、区域外就学開始学年

5 特別支援学校関連データの管理

就学校名、部名（特別支援学校就学時のみ使用）、設置者名、学校入学年月日、学校編入学年月日、学校転学年月日、学校卒業年月日、学校退学年月日、障がい区分

6 督促関連データの管理

校長からの通知受理年月日、就学督促年月日、就学督促事由

7 猶予・免除関連データの管理

就学義務猶予年月日、就学義務猶予事由、就学義務猶予開始年月日、就学義務猶予終了年月日、就学義務猶予復学年月日、
就学義務免除年月日、就学義務免除事由、就学義務免除開始年月日、就学義務免除終了年月日、就学義務免除復学年月日、
就学義務が猶予・免除されていた年数

8 学齢簿変更関連データの管理

学齢簿変更届出年月日、学齢簿変更年月日、学齢簿変更事由

9 支援措置対象者関連データの管理

支援措置対象者情報

【就学援助】

1 申請情報管理

児童生徒ごとの申請情報（申請番号、学校コード、仮学校コード、受付年月日、申請区分、申請理由、申請者情報、世帯員情報、児童生徒情報（学校・学年情報を含む）、口座情報、入学前支給対象、就学援助の希望の有無、送付先情報（氏名、住所、郵便番号、方書）、備考情報等）、転入元自治体での支給情報、クラス情報、

認定期間途中の変更（申請番号、学校コード、学校転学年月日、申請者変更、支給方法変更、所得変更、申請区分、申請理由、就学世帯情報、学校情報（在籍学校・学年）、口座変更、送付先情報、備考情報の変更等）、認定期間途中の申請書受付校の変更、認定期間途中の自治体学校コードの変更、取消届の内容（申請取消の事由、受付日等）、申請情報（申請番号、学校コード、受付日、申請区分、申請理由、申請者情報、世帯員情報、児童生徒情報（学校・学年情報を含む）、口座情報、入学前支給対象、備考情報等）の履歴情報、申請情報（児童生徒のクラス情報）の履歴情報、申請情報（申請書受付校）の履歴情報、申請情報（自治体学校コード）の履歴情報、民生委員情報（氏名、担当地区、住所、連絡先）、公金受取口座（公的給付支給等口座）の利用の意思の有無（公金口座区分）、マイナポータルぴったりサービスより受け付けた申請データのうち管理が必要な項目、辞退事由及び辞退受付日、辞退日等、

2 認定基準

生活保護に準ずる基準額（生活扶助（第1類費）、生活扶助（第2類費）、通減率、生活扶助本体における経過的加算、冬季加算、期末一時扶助、基礎控除、住宅扶助、教育扶助、学校給食費、通学交通費、その他任意の値）、認定基準係数、その他の生活保護に準ずる基準額（学校給食費、住宅扶助、その他任意の値）

3 所得情報管理

所得情報（給与（支払総額、給与所得控除後の金額、課税所得金額）、事業所得、不動産所得、利子所得、配当所得、雑所得（その他）、譲渡所得、一時所得、山林所得、退職所得等、各種控除情報（配偶者控除、医療費控除、社会保険料控除、生命保険控除、地震保険料控除、ひとり親・寡婦控除、障害者控除、特定親族特別控除等、個人住民税課税がない当年1月1日以降の転入者等から提出された所得課税状況書類の内容のうち、就学援助に関連する項目（所得額、課税・非課税区分）、

4 その他の認定に係る情報管理

（1）生活保護に係る情報管理

資格情報（生活保護開始・停止・再開・廃止、該当の状態に移行した年月日、教育扶助・生活扶助の有無、生活保護費から支給した入学準備金支給情報等）

（2）個人住民税に係る情報管理

資格情報（非課税情報、減免情報、扶養情報）

（3）国民年金保険料に係る情報管理

資格情報（減免情報）

（4）国民健康保険法の保険料に係る情報管理

資格情報（減免情報）

（5）児童扶養手当に係る情報管理

資格情報（受給中・一部停止・停止及び停止理由等）

（6）固定資産税に係る情報管理

資格情報（減免情報）

5 認定結果管理

認定結果、認定区分、理由、学校長への振込委任有無、認定基準額、支給対象費目、支給予定額、審査日、認定日、認定期間、申請番号、備考情報、学校長への振込委任有無と支給予定額

6 支給

医療機関情報、疾病別の医療費等、支給費情報（支給対象費目・支給額（年額、月額、日額）、支給月、支給履歴、支給日、返納処理（返納金額の算出、返納記録の管理）、追給処理（追給分の振込データ作成、追給記録の管理）、過誤調整情報（金額、事由、結果、振込日、戻入日等）、

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「－」	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。
	－ (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。
	－ (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。
	－ (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。