資料54

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後期高齢支援システム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：健康部高齢者医療担当課）

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後期高齢支援システムへの移行
担当課	高齢者医療担当課
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後期高齢支援システムをガバメントクラウドへ移行し、安定した後期高齢者医療保険制度事務の継続及び地方公共団体の行政運営の効率化に寄与することを目的とする。
対象者	新宿区後期高齢者医療保険の被保険者及びその世帯員
事業内容	１　概要 現在、後期高齢者医療制度では、都道府県単位に設置される「広域標準システム」と、市区町村単位に設置される「後期高齢支援システム」の両方のシステムを利用して事務処理を行っており、それぞれのシステムの役割としては、後期高齢者医療広域連合が管理する「広域標準システム」は保険料の賦課や給付管理などを分担し、市区町村が管理する「後期高齢支援システム」は住民データの収集・連携、保険料収納、滞納管理などを行っている。（平成１９年度第２回、平成２３年度第６回情報公開・個人情報保護審議会承認済み） その他、区では、入院時負担軽減支援金及び葬祭費について、「高齢者福祉システム」にて処理を行っている。（平成１９年度第６回情報公開・個人情報保護審議会承認済み） 令和３年９月に公布された「標準化法」において、住民基本台帳をはじめとする標準化対象事務について標準仕様書が示され、各市区町村はその基準を満たしたシステム使用することが義務付けられ、「後期高齢支援システム」について、令和７年度末までに標準化へ対応することが求められた。 併せて、標準化法第 10 条により、標準準拠システムの利用において、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を利用し、運用を行う。 なお、標準化対象外である、「高齢者福祉システム」についても、標準化の関連システムであることから、ガバメントクラウドを利用して運用を行う。

	２　個人情報保護管理運営会議への付議内容 （１）電算処理 後期高齢者医療保険に関する事務（資格管理、賦課管理、収納管理、滞納管理）を「標準仕様書」に準拠した「後期高齢支援システム」へ移行する。 （２）外部結合 後期高齢システム標準化にあたり、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。併せて、標準化対象外である「高齢者福祉システム」についても、標準化の関連システムであることから、ガバメントクラウドを利用して運用を行う。 （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 被保険者及び被保険者と同一世帯の者の合計 約８６，０００人（令和６年７月時点） ※個人情報の流れは、資料５４－１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　地方公共団体情報システム標準化に対応した後期高齢支援システムへの移行について

※太字ゴシック（下線）は、平成２３年度第６回情報公開・個人情報保護審議会承認済の内容からの変更箇所

保有課（担当課）	高齢者医療担当課
登録業務の名称	資格管理、賦課管理、収納管理、滞納管理等に関する事務
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 新宿区後期高齢者医療保険の被保険者及びその世帯員 元被保険者及びその世帯員 ２　記録項目 資料５４－２のとおり ３　記録するコンピュータ 後期高齢支援システム・高齢者福祉システム（ガバメントクラウド上に移設）
新規開発・追加・変更の理由	**「標準化法」に基づいた後期高齢支援システムの運用を実現し、安定した後期高齢者医療保険事務の継続及び地方公共団体の行政運営の効率化に寄与することを目的とする。**
新規開発・追加・変更の内容	現在、資格管理、賦課管理、収納管理、滞納整理等の後期高齢者医療保険に関する事務で運用している後期高齢支援システムを、**「標準化法」に基づきガバメントクラウドへ移設する。**
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７年６月から　移行期間** **令和８年３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　地方公共団体情報システム標準化に対応した後期高齢支援システムへの外部結合について

※太字ゴシック（下線）は、平成２３年度第６回情報公開・個人情報保護審議会承認済の内容からの変更箇所

保有課（担当課）	高齢者医療担当課
登録業務の名称	１　後期高齢支援システム（標準化） 資格管理、賦課管理、収納管理、滞納管理等 ２　高齢者福祉システム（標準化対象外） 入院時負担軽減支援金、葬祭費に関する事務
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 新宿区後期高齢者医療保険の被保険者及びその世帯員 元被保険者及びその世帯員 ２　記録項目 資料５４－２のとおり ３　記録するコンピュータ 後期高齢支援システム・高齢者福祉システム（ガバメントクラウド上に移設）
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後期高齢支援システムを利用する必要があるため。** **また、標準化対象外の業務であるが、入院時負担軽減支援金及び葬祭費についても「高齢者福祉システム」にて処理を行っており、標準化の関連システムであることから、ガバメントクラウドを利用して一体的に運用を行う。**
結合の形態	**情報システム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、後期高齢支援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７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　地方公共団体情報システム標準化に対応した後期高齢支援システムへの移行について

保有課（担当課）	高齢者医療担当課
登録業務の名称	１　後期高齢支援システム（標準化対象） 資格管理、賦課管理、収納管理、滞納管理等 ２　高齢者福祉システム（標準化対象外） 入院時負担軽減支援金、葬祭費に関する事務
委託先	株式会社ジーシーシー（特命随契による選定を予定）（プライバシーマーク及び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 新宿区後期高齢者医療保険の被保険者及びその世帯員 元被保険者及びその世帯員 ２　記録項目 資料５４－２のとおり
処理させる情報項目の記録媒体	電磁的媒体（後期高齢支援システム・高齢者福祉システム）
委託理由	「標準化法」に基づき、住民の利便性の向上及び地方公共団体の行政運営の効率化に寄与することを目的とする、地方公共団体情報システムの標準化に対応するため。 なお、上記事業者とは、後期高齢者医療制度の導入にあたり、プロポーザルを経て平成１９年４月から業務整備の委託を締結し、システム整備開発を進め、平成２０年４月から本稼働を実施した。以降、同システムの業務運用保守については、当該システム全体の基本設計・詳細設計・データ移行・区独自外付システムを構築した上記事業者を指定することで、安定かつ効率的な後期高齢者医療保険事務を実現している。 標準化法に基づく環境構築委託及び保守業務を行うにあたっては、高度な専門技術や知識を有するだけでなく、新宿区で運用する後期高齢支援システムに精通している現事業者に業務を委託することで、引き続き、新宿区の実態に即した後期高齢者医療保険事務を実現することができるため。
委託の内容	ガバメントクラウド上に「標準化法」に準拠した「後期高齢支援システム」を構築し、現在管理している後期高齢者医療に関する情報を移行する。 また、標準化対象外である「高齢者福祉システム」も同時に移行する。 移行したシステムについて、運用保守を委託する。
委託の開始時期及び期限	令和７年４月から令和８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

地方公共団体情報システム標準化に対応した後期高齢支援システムへの移行に係る個人情報の流れ　（資料５４－１）

申請者

・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

新宿区
（高齢者医療担当課）

イントラＰＣ
（情報システム課管理）

【後期高齢支援システム（標準化対象）】
(1)資格管理
(2)賦課管理
(3)収納管理
(4)滞納管理

【高齢者福祉システム（標準化対象外事務）】
(1)入院時負担軽減支援金
(2)葬祭費

①申請・納付

④督促状の発行・資格確認書等随時発行・給付決定等・葬祭費の決定等

通信暗号化　（専用回線）

【広域標準システム】
（広域連合管理）
(1)保険料賦課
(2)給付管理
(3)その他照会事務

ガバメントクラウド接続サービス（専用回線）

通信暗号化

②各種後期高齢者情報の異動・入力
（賦課・収納・還付・滞納など）
（入院時負担軽減支援金等の入力）

③各種異動情報の出力
（督促状等の発行・
入院時負担軽減支援金等の給付情報）

【電算処理】
【外部結合】
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

【データ移設】
標準仕様書に準拠したシステムへの移行
【保守委託】
システムの運用保守および障害対応

委託事業者

後期高齢支援システム
（標準準拠・新宿区専用）

被保険者情報

詳細は「資料５４－２」のとおり

・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

記録項目名	記録項目名	記録項目名
個人区分コード	口座利用区分	時効更新事由
住基異動事由コード	徴収猶予区分	還付充当コード
本名通称名区分コード	収納区分	決定理由
外国人区分コード	納入方法コード	処理結果
生年月日年号コード	過誤納状態区分	特別徴収期別番号
性別コード	還付支払方法区分	普通徴収期別番号
広域続柄コード	通知内容コード	特別徴収状態区分
世帯登録区分コード	特別徴収制度コード	２分の１判定結果
国籍コード	特別徴収義務者コード	特別徴収中止事由
広域在留資格コード	年金コード	分割納付取消理由
資格取得事由コード	性別コード（年金）	交渉方法区分
資格喪失事由コード	各種区分（特別徴収対象者情報）	滞納整理記録
減額区分	各種区分（特別徴収追加候補者情報）	口座振替処理区分
申告区分コード	各種区分（資格喪失等通知）	振替結果コード
賦課事由コード	各種区分（仮徴収額変更通知）	時効更新区分
住民税課税非課税区分コード	各種区分（住所地特例該当通知）	時効の完成猶予事由
異動区分コード	後期移管コード	コンビニ速報・確報区分
暫定賦課フラグ	施設入所区分コード	通知書通知理由コード
経過措置対象フラグ	介護待機フラグ	口座管理区分
旧ただし書所得優先フラグ	金融機関	還付保留状態
減額対象所得優先フラグ	支店	返送理由
低Ⅰ低Ⅱ判定所得優先フラグ	口座種別	返送状態
一部負担割合判定所得優先フラグ	滞納処分内容	状況区分
期割情報種別	歳入歳出区分	執行停止事由
通知書発送要否フラグ	過誤納発生事由	未申告区分
住民税更正事由コード	認定結果	異動区分
特別軽減区分	特記区分	納入方法
徴収方法区分コード	証区分コード	指定金融区分コード
所得割減額区分	保険者種別	納付書種別
滞納状態コード	猶予区分	住民種別
不納欠損事由コード	本店支店区分	債券種別区分
業務区分		

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。
	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。
	○	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。
	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。