

個人情報保護管理運営会議 付議事項

件名	後期高齢者医療保険料の納付における銀行スマホ決済（モバイルレジ等）、モバイルレジクレジット決済及び電子マネー決済の導入等について
----	--

内容は別紙のとおり

要綱の根拠

◇第3条第1項第3号（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	後期高齢者医療保険料の納付における銀行スマホ決済（モバイルレジ等）、モバイルレジクレジット決済及び電子マネー決済の導入等について
担当課	高齢者医療担当課
目 的	後期高齢者医療保険料の納付について、銀行スマホ決済（モバイルレジ等）、モバイルレジクレジット決済及び電子マネー決済を導入することにより、区民の納付機会の拡充と利便性の向上を図る。
対象者	後期高齢者医療保険料の納付義務者
事業内容	1 概要 現在、区では、後期高齢者医療保険料の納付について、高齢者医療担当課、特別出張所、金融機関、口座振替、コンビニエンスストアでの納付に対応している。 令和7年7月からは、今までの納付方法に加え、『モバイルレジ等を活用したインターネットバンキング納付（※）』、『モバイルレジを活用したクレジット納付』及び『電子マネー納付』を導入することで、区民の利便性の向上及び業務の効率化を図る。 ※モバイルレジ、P a y B及び楽天銀行を活用したインターネットバンキング納付を「銀行スマホ決済」という。 2 個人情報保護管理運営会議への付議内容 （1）外部結合 収納サービス提供事業者が有する収納センターのサーバと区のイントラパソコンが結合するため。 （2）業務委託 納付された収納データの作成、収納サービス提供事業者や区への収納データ送信及び収納センターのサーバ管理業務を委託するため。 3 対象者数 約36,000名 ※個人情報の流れは、資料13-1、資料13-2及び資料13-3のとおり

件名 銀行スマホ決済(モバイルレジ等)、モバイルレジクレジット決済及び電子マネー決済の導入に伴う収納サービス提供事業者との外部結合について

保有課(担当課)	高齢者医療担当課
登録業務の名称	後期高齢者医療保険料の収納
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 後期高齢者医療保険料の納付義務者 2 情報項目 資料13-4のとおり
結合の相手方	株式会社NTTデータ(ISO27001 認証取得事業者)
結合する理由	後期高齢者医療保険料の納付義務者が納付手続を行うと、それぞれの決済事業者から収納サービス提供事業者が有する収納センターに収納データが送られる仕組みとなっている。 そのため、区が収納データを把握し、管理するためには、収納サービス提供事業者が有する収納センターとの外部結合が必要となる。
結合の形態	LGWAN 回線を利用して、収納サービス提供事業者の収納センターと区のイントラネット端末を接続する。
結合の開始時期と期間	令和7年7月1日から令和8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

件名 銀行スマホ決済(モバイルレジ等)を活用したインターネットバンキング決済に係る収納データ作成等業務の委託について

保有課(担当課)	高齢者医療担当課
登録業務の名称	後期高齢者医療保険料の収納
委託先	1 銀行スマホ決済事業者 (1) モバイルレジ(株式会社NTTデータ (ISO27001 認証取得済)) (2) Pay B (ビルディングシステム株式会社 (プライバシーマーク取得済)) (3) 楽天銀行(楽天銀行株式会社) 2 収納サービス提供事業者 株式会社NTTデータ (ISO27001 認証取得済)
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 後期高齢者医療保険料の納付義務者 2 情報項目 資料13-4のとおり
処理させる情報項目の記録媒体	電磁的媒体(委託先のサーバ)
委託理由	銀行スマホ決済を活用したインターネットバンキング納付の利用にあたっては、納付義務者が銀行スマホ決済専用アプリ(モバイルレジ、Pay B、楽天銀行)を使用して手続きを行うと、銀行スマホ決済事業者が有する収納センターに収納データが送信された後、収納サービス提供事業者が有する収納センターに収納データが送信される仕組みとなっている。 そのため、区が銀行スマホ決済を活用した収納を実施するためには、納付された収納データの作成、収納サービス提供事業者や区への収納データ送信及び収納センターのサーバ管理業務の委託が必要となる。 なお、銀行スマホ決済を活用したインターネットバンキング納付においては、区(甲)、銀行スマホ決済事業者(乙)、収納サービス提供事業者(丙)の「三者契約」を締結する。乙は丙に収納データを送付し、丙は甲に収納データを送付する。甲は乙及び丙のいずれに対しても個人情報保護対策を実施させる必要があるため、三者契約とする。
委託の内容	1 銀行スマホ決済事業者に取り扱わせる内容 (1) 銀行スマホ決済専用アプリの提供及びアプリによる納付サービスの運用 (2) 収納データの作成及び送信業務 (3) 銀行スマホ決済事業者が有する収納センターのサーバ管理業務 2 収納サービス提供事業者に取り扱わせる内容 (1) 収納データの受信及び送信業務 (2) 収納サービス提供事業者が有する収納センターのサーバ管理業務
委託の開始時期及び期限	令和7年7月1日から令和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

件名 モバイルレジを活用したクレジット決済に係る収納データ作成等業務の委託について

保有課(担当課)	高齢者医療担当課
登録業務の名称	後期高齢者医療保険料の収納
委託先	1 収納サービス提供事業者 株式会社N T Tデータ (ISO27001 認証取得事業者) 2 クレジットカード指定代理納付者 株式会社ジェーシービー (ISO27001 認証取得事業者) ユーシーカード株式会社 (ISO27001 認証取得事業者)
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 後期高齢者医療保険料の納付義務者 2 情報項目 資料13-4のとおり
処理させる情報項目の記録媒体	電磁的媒体 (委託先のサーバ)
委託理由	1 収納サービス提供事業者 モバイルレジを活用したクレジット決済の利用にあたっては、後期高齢者医療保険料の納付義務者が、専用アプリを使用し決済を行うと、収納サービス提供事業者が有する収納センターに収納データが送られる。そのため、区がモバイルレジを活用したクレジット収納を実施するためには、収納サービス提供事業者が収納データの作成及び区への送信、サーバの管理業務をすることが必要となる。 2 クレジットカード指定代理納付者 モバイルレジを活用したクレジット決済は、クレジットカード会社への与信照会 (クレジットカードの有効期限や利用限度額の確認) が必要となる。与信照会をして問題がなければ、クレジットカード指定代理納付者が、保険料の代理納付をすることになるが、区では、代理納付をする仕組みを有していないため、与信照会及び保険料の代理納付業務を委託することとする。 ※モバイルレジを活用したクレジット決済においては、区 (甲)、収納サービス提供事業者 (乙)、クレジットカード指定代理納付者 (丙) の『三者契約』を締結する。乙は甲に収納データを送付し、丙は代理納付した金額を甲指定の口座に入金する。甲との関わり方において、乙及び丙は同程度であり、乙と丙も業務上同定度に関係する。乙及び丙のいずれに対しても個人情報保護対策を実施させる必要があるため、三者契約とする。
委託の内容	1 収納サービス提供事業者に取り扱わせる内容 (1) クレジット納付時に利用するモバイルレジ専用アプリの提供及びアプリによる納付サービスの運用 (2) 後期高齢者医療保険料のモバイルレジ納付の収納データに係る作成及び送信業務

	(3) 収納サービス提供事業者が有する収納センターのサーバ管理業務 2 クレジットカード指定代理納付者に取り扱わせる内容 (1) 後期高齢者医療保険料の支払い時のクレジットカード会社への与信照会（クレジットカードの有効期限や利用限度額の確認）業務 (2) クレジットカード会社への与信照会で問題がなかった場合の、後期高齢者医療保険料の代理納付業務
委託の開始時期及び期限	令和7年7月1日から令和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

件名 電子マネー決済の導入に伴う収納データ作成等業務の委託について

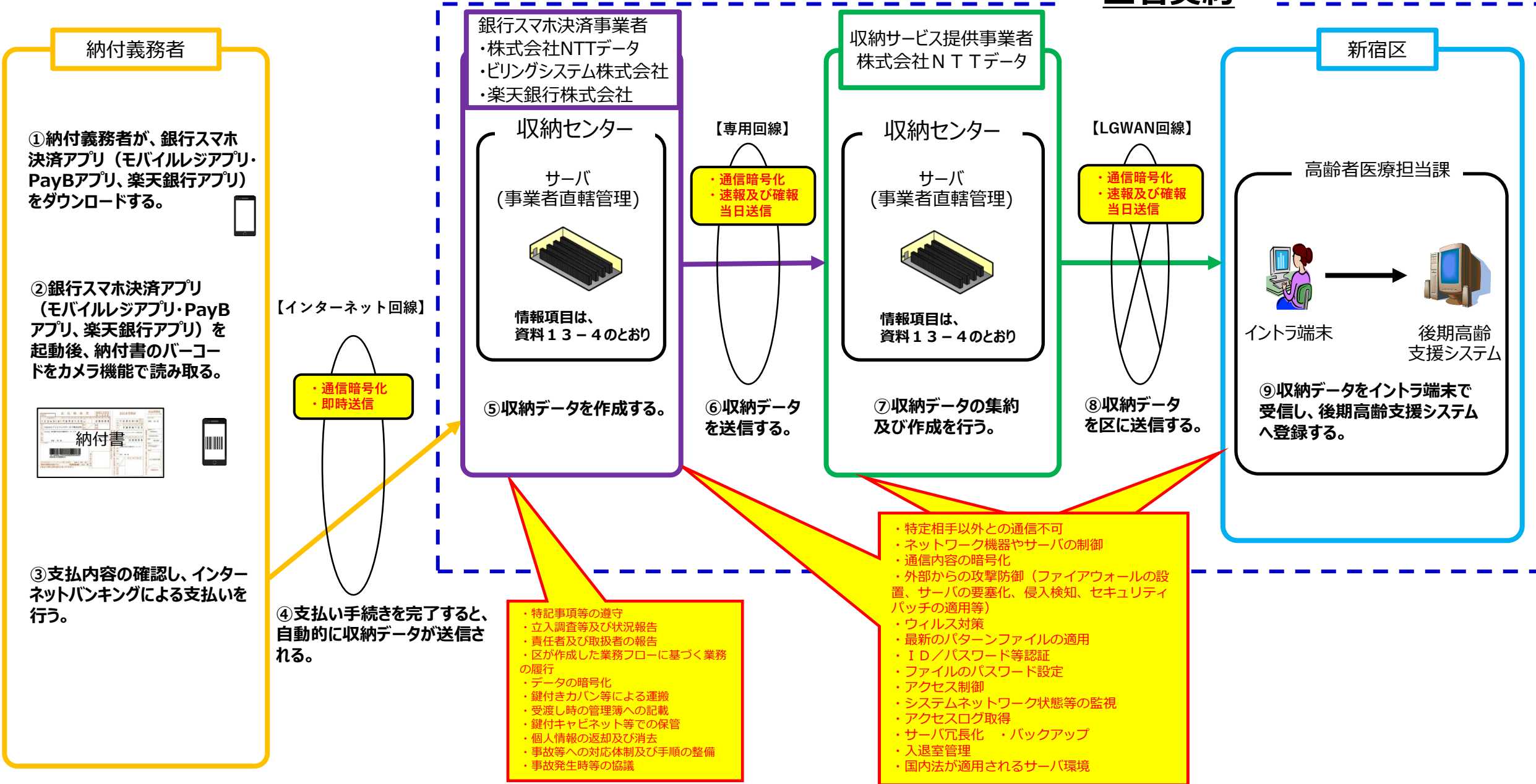
保有課(担当課)	高齢者医療担当課
登録業務の名称	後期高齢者医療保険料の収納
委託先	- 電子マネー事業者 電子マネー決済アプリの運営事業者 - データ連携事業者 ビルディングシステム株式会社(プライバシーマーク取得事業者) - 収納サービス提供事業者 株式会社NTTデータ(ISO27001認証取得事業者)
委託に伴い事業者処理させる情報項目(だれの、どのような項目か)	- 個人の範囲 後期高齢者医療保険料の納付義務者 - 情報項目 レコード区分、ファイル作成日、代行会社コード、収納機関コード、利用区分、データ識別コード、<u>収納日付、収納時間、バーコード情報(識別コード、メーカーコード、年度、納付書番号、再発行区分、支払い期限日、印紙フラグ、支払い金額)</u>、<u>収納店舗コード</u>、支払い予定日、経理処理日、小売業企業コード、速報件数合計、速報金額合計、確報件数合計、確報金額合計、速報取消件数合計、速報取消金額合計、レコード総件数 ※電子マネー事業者は下線の情報項目のみ取り扱う
処理させる情報項目の記録媒体	電磁的媒体(委託先のサーバ)
委託理由	- 電子マネー事業者 事業者が運営する電子マネー決済アプリを利用した納付があった場合の受付及び納付情報のデータ連携事業者への送信を委託することが必要となる。 - データ連携事業者 電子マネー事業者が受付した収納データの作成及び収納サービス提供事業者への送信を委託することが必要となる。 - 収納サービス提供事業者 電子マネー事業者が受付し、データ連携事業者が作成する収納データは、収納サービス提供事業者が有する収納センターを経由し、区と外部結合する専用回線により区に送られる仕組みとなっている。このため、区が電子マネー決済を活用した電子マネー納付の収納を行うには、収納サービス提供事業者が収納データの集約、区への送信、及び収納データの管理業務を委託することが必要となる。 ※本業務の委託においては、区(甲)、収納サービス提供事業者(乙)、データ連携事業者(丙)及び電子マネー事業者(丁)の四者契約を締結する。 丁は電子マネー決済アプリにより受付した納付情報を丙に送信し、収納

	金を丙指定の口座に送金する。丙は丁から受信した納付情報により収納データを作成して乙に送信し、収納金を乙指定の口座に送金する。乙は丙から受信した収納データを取りまとめ甲に送信し、収納金を甲指定の口座に送金する。甲との関わり方において、乙、丙及び丁は業務上同程度に関係し、いずれに対しても個人情報保護対策を実施させる必要があるため、四者契約とする。
委託の内容	1 電子マネー事業者 電子マネー決済アプリによる納付の受付、データの管理、データ連携事業者への納付情報の送信及び収納金データの送金業務 2 データ連携事業者 電子マネー事業者が受付した収納データの作成（収納サービス提供事業者が指定するレイアウトに変更）、収納サービス提供事業者への送信及び収納金データの送金業務 3 収納サービス提供事業者 電子マネー納付に係るデータ連携事業者からの収納データの受信、収納データの集約、区への収納データ送信及び収納金データの送金業務
委託の開始時期及び期限	令和7年7月1日から令和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

銀行スマホ決済を活用したインターネットバンキング納付に係る個人情報の流れ

※モバイルレジについては、税務課などが平成30年度第8回情報公開・個人情報保護審議会で承認済み

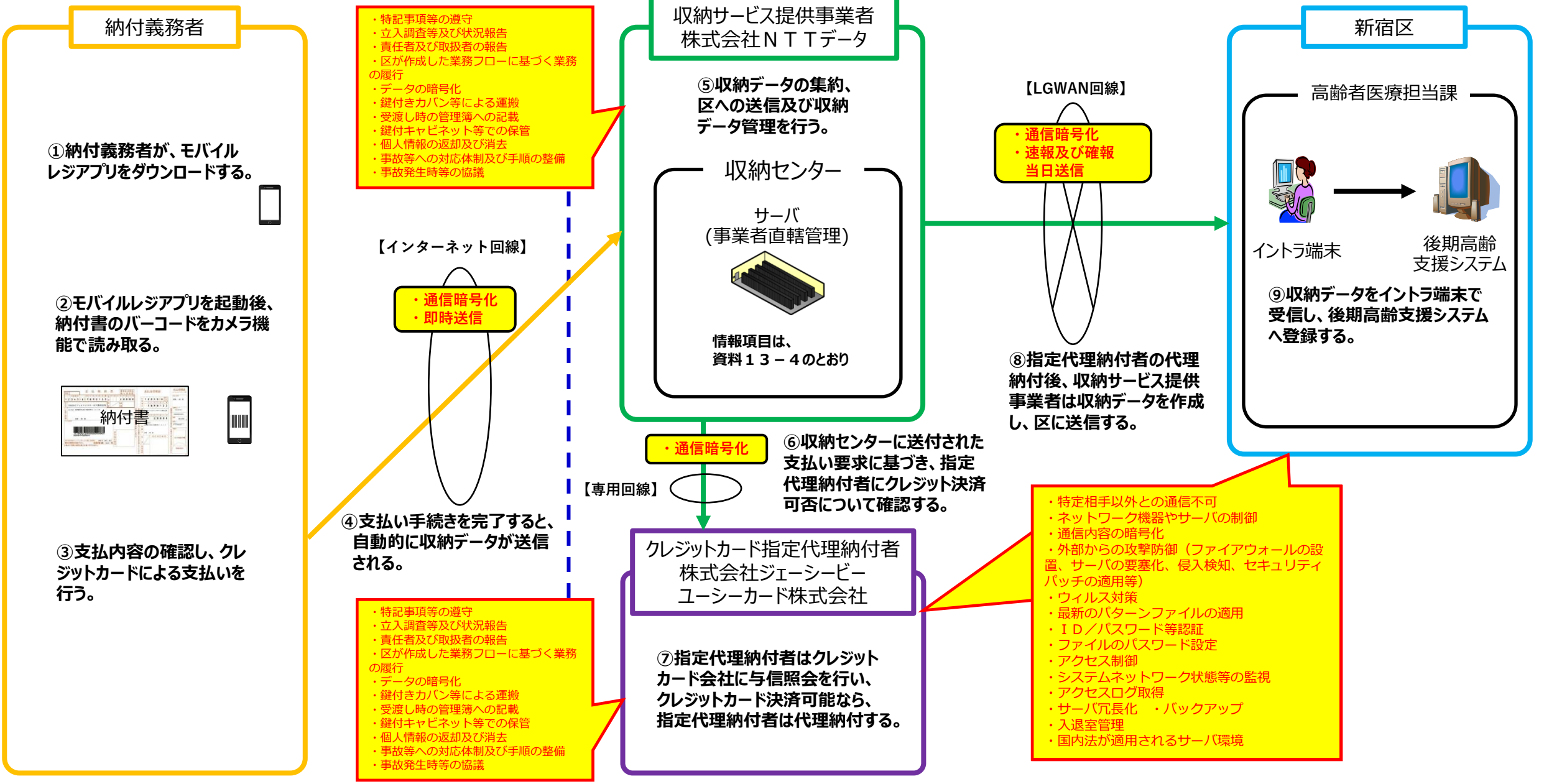
三者契約



モバイルレジを活用したクレジット納付に係る個人情報の流れ

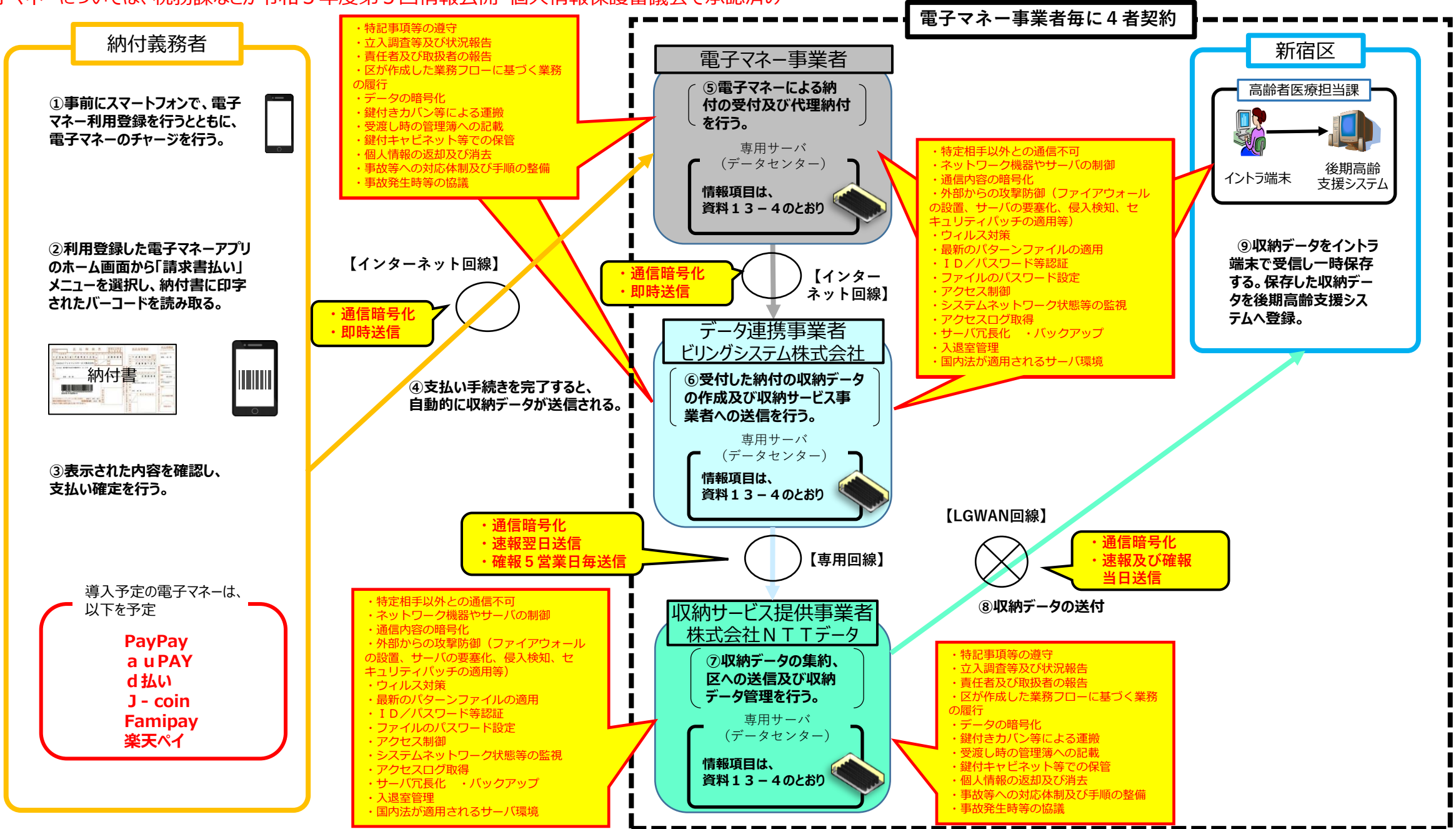
※モバイルレジクレジットについては、税務課などが平成30年度第8回情報公開・個人情報保護審議会で承認済み

三者契約



電子マネー納付の導入に係る個人情報の流れ

※電子マネーについては、税務課などが令和 3 年度第 5 回情報公開・個人情報保護審議会で承認済み



銀行スマホ決済を活用したインターネットバンキング納付・クレジット納付に係るデータ項目**後期高齢者医療保険料の収納業務に係る項目**

通知書番号、レコード区分、ファイル作成日、代行会社コード、収納機関コード、利用区分、データ識別コード、収納日付、収納時間、自治体コード、区自由使用欄（処理区分、賦課年度、対象年度、通知書番号、期別、調定額、収納額、延滞金、再発行区分、支払い期限日、印紙フラグ、支払い金額）、収納店舗コード、支払い予定日、確認番号、発行年月日、クレジット送信年月日、経理処理日、小売業企業コード、速報件数合計、速報金額合計、確報件数合計、確報金額合計、速報取消件数合計、速報取消金額合計、レコード総件数

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「－」	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「－」	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「－」	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。
	－ (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。
	－ (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。
	－ (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。
委託にあたり区が行う 情報保護対策 【システム上の対策】	○	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。
	○	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。