資料12

個人情報保護管理運営会議　付議事項

件名	銀行スマホ決済（モバイルレジ等）を活用した国民健康保険料のインターネットバンキング納付の導入に伴う収納サービス提供事業者との外部結合等について（納付方法の追加）

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：健康部医療保険年金課）

事業の概要

事業名	銀行スマホ決済を活用した国民健康保険料のインターネットバンキング納付の導入について
担当課	医療保険年金課
目　的	国民健康保険料の納付について、新たな決済手段である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	国民健康保険料の納付義務者
事業内容	１　概要 現在、区では、国民健康保険料の納付について、医療保険年金課、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のほか、『モバイルレジ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』など、さまざまなキャッシュレス決済にも対応している。 令和７年６月からは、ＰａｙＢ、楽天銀行を活用したインターネットバンキング納付を新たに追加（※）することにより、区民の利便性の向上及び業務の効率化を図る。 ※インターネットバンキング納付は、既存の「モバイルレジ」を活用したインターネットバンキング納付と今回追加される「ＰａｙＢ、楽天銀行」を加えて「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 銀行スマホ決済で納付されたデータについて、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　納付予定件数 ７００件 ※個人情報の流れは、資料１２－１のとおり

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　銀行スマホ決済（モバイルレジ等）を活用した国民健康保険料のインターネットバンキング納付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

※太字ゴシック（下線）が、平成３０年度第８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）	医療保険年金課
登録業務の名称	国民健康保険料の収納業務
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 国民健康保険料の納付義務者 ２　情報項目 資料１２－２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	国民健康保険料の納付義務者が銀行スマホ決済専用アプリ（モバイルレジ、**ＰａｙＢ、楽天銀行**）を利用して納付手続を行うと、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６月１３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

別紙(業務委託)

◇業務委託(第３条第１項第３号)

件名　銀行スマホ決済（モバイルレジ等）を活用した国民健康保険料のインターネットバンキング納付に係る収納データ作成等業務の委託について

※太字ゴシック（下線）が、平成３０年度第８回情報公開・個人情報保護審議会了承済の内容からの変更箇所

保有課(担当課)	医療保険年金課
登録業務の名称	国民健康保険料の収納業務
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（IS027001 認証取得済） **（２）ＰａｙＢ（ビリ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（IS027001 認証取得済）
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 国民健康保険料の納付義務者 ２　情報項目 資料１２－２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、**ＰａｙＢ、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６月１３日から令和８年３月３１日まで（次年度以降も、同様の外部委託を行う）
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

（資料１２－１）

※モバイルレジについては、平成３０年度第８回情報公開・個人情報保護審議会にて承認済み。
※青字の部分が、今回の追加内容。

三者契約

納付義務者

①納付義務者が、銀行スマホ決済アプリ（モバイルレジアプリ・PayBアプリ、楽天銀行アプリ）をダウンロードする。

②銀行スマホ決済アプリ（モバイルレジアプリ・PayBアプリ、楽天銀行アプリ）を起動後、納付書のバーコードをカメラ機能で読み取る。

③支払内容の確認し、インターネットバンキングによる支払いを行う。

【インターネット回線】

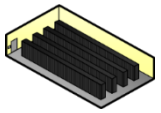
・通信暗号化
・即時送信

④支払い手続きを完了すると、自動的に収納データが送信される。

銀行スマホ決済事業者
・株式会社NTTデータ
・ビリングシステム株式会社
・楽天銀行株式会社

収納センター

サーバ
（事業者直轄管理）



情報項目は、
資料１２－２のとおり

⑤収納データを作成する。

【専用回線】

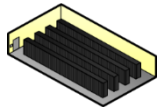
・通信暗号化
・速報及び確報
当日送信

⑥収納データを送信する。

収納サービス提供事業者
株式会社ＮＴＴデータ

収納センター

サーバ
（事業者直轄管理）



情報項目は、
資料１２－２のとおり

⑦収納データの集約及び作成を行う。

【LGWAN回線】

・通信暗号化
・速報及び確報
当日送信

⑧収納データを区に送信する。

新宿区

医療保険年金課

イントラ端末

標準システム

⑨収納データをイントラ端末で受信し、標準システムへ登録する。

・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

・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

（資料１２－２）

銀行スマホ決済による国民健康保険料の収納情報データ項目

国民健康保険料の収納業務に係る項目
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、収納日付、収納時間、バーコード情報（国コード、区自由使用欄（処理区分、賦課年度、相当年度、通知書番号、期別、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、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

（注）既に導入済のモバイルレジによる納付データと、項目・連携内容は同様

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。