資料48

個人情報保護管理運営会議　付議事項

件名	財産調査システム及び財産調査システム中間処理ユニットの利用に係る外部結合について

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）

（担当部課：福祉部生活福祉課、保護担当課）

事業の概要

事業名	財産調査システム及び財産調査システム中間処理ユニットの利用に係る外部結合について
担当課	生活福祉課、保護担当課
目　的	生活保護受給者・申請者について、財産調査システムを導入することにより、収入・資産の状況をより迅速に把握し、調査の業務効率化および適正な生活保護業務の推進を図る。
対象者	生活保護受給者（過去に受給していた者を含む）・申請者
事業内容	１　概要 生活保護制度は、生活に困窮するすべての国民に対し、その困窮の程度に応じ、必要な保護を行い、その最低限度の生活を保障するとともに、その自立を助長することを目的としている。 保護の開始や支給金額の決定、保護費の返還決定、不正受給への対応等においては、生活保護法第２９条に基づく調査により、受給者・申請者の口座の有無、預金残高、入出金履歴等の収入・資産状況を把握する必要がある。 ついては、既に滞納対策課が導入している財産調査システムを当課でも利用することで、収入・資産状況をより迅速に把握し、調査の業務効率化および適正な生活保護業務の推進を図る。 ２　個人情報保護管理運営会議への付議内容 財産調査システム（pipitLINQ）及び財産調査システム中間処理ユニット（PiMS）と外部結合を行う。 ３　対象者数 約３，０００人 ※個人情報の流れは、資料４８－１のとおり

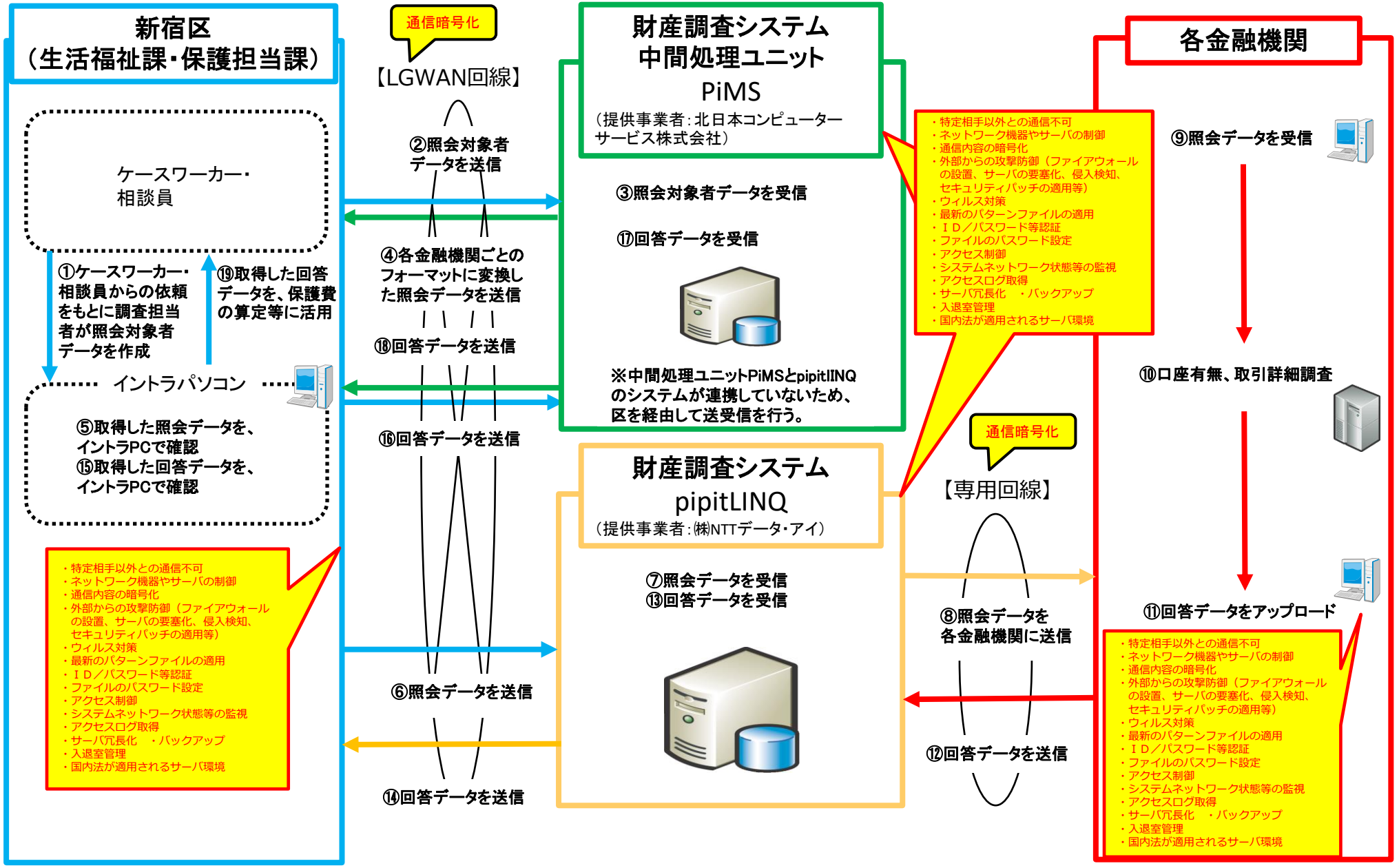
別紙(電子計算機の外部結合関係)

◇外部結合(第３条第１項第３号)

件名　財産調査システム及び財産調査システム中間処理ユニットの利用に係る外部結合について

保有課(担当課)	生活福祉課、保護担当課
登録業務の名称	財産調査（電子照会）
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 生活保護受給者（過去に受給していた者を含む）・申請者 ２　記録項目 資料４８－２のとおり
結合の相手方	株式会社ＮＴＴデータ・アイ（財産調査システム、pipitLINQ 提供事業者） 北日本コンピューターサービス株式会社（財産調査システム中間処理ユニット、PiMS 提供事業者） ※上記２社については、政府のデジタル・ガバメント実行計画連携事業者であり、LGWAN－ASP サービス認定済。
結合する理由	①　財産調査システム（pipitLINQ） 当システムを利用した電子による財産調査を実施した場合、照会から回答までの所要時間を大幅に短縮できるため、収入・資産把握の効率化が見込まれ、適正に生活保護業務を推進することができる。 ※郵送による文書照会で数か月から半年かかっていた預金照会が、１週間程度に短縮する。 ②　財産調査システム中間処理ユニット（PiMS） 上記の財産調査システムを利用した電子照会時に必要な情報（氏名カナ等）は金融機関毎に異なり、其々のルールに対応した電子照会情報を個別に作成する必要がある。当システムでは、金融機関毎の電子照会情報作成ルールに沿って、照会情報を自動変換する機能を有し、利用者側が作成ルールを考慮することなく電子照会が可能となる。電子照会情報の作業時間が大幅に短縮できるほか、当システムは財産調査システムで取得した調査対象者情報を取り込むことで口座照会情報を電子化して一元的な管理が可能となる。
結合の形態	ＬＧＷＡＮ回線を使用し、財産調査システム（pipitLINQ）及び財産調査システム中間処理ユニット（PiMS）と区のイントラネット端末を結合する。
結合の開始時期と期間	令和８年４月１日から令和９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

財産調査システム・財産調査システム中間処理ユニットの利用における個人情報の流れ　　**※滞納対策課にて既に導入済**　　（資料48－1）



（資料４８－２）

財産調査システム及び財産調査システム中間処理ユニットにおける情報項目

送信情報に係る項目
属性(人格)、依頼コード、根拠法令、生(設立)年月日、カナ氏名、住所、住所コード、性別、カナ住所、英字名、漢字氏名、郵便番号、調査基準日、システム連携情報、支店番号、管理番号、顧客番号、登録者、口座種別、更新日、口座番号、行政機関任意項目、照会対象期間。

回答情報に係る項目
属性(人格)、管理番号、最終取引日、カナ氏名、保証人有無、残高、漢字氏名、給与振込有無、口座取引明細表、郵便番号、年金振込有無、科目コード、住所、担保有無・明細、科目名、住所コード、貸金庫・保護預有無、満期日、住所（カナ）、出資金口数、ステータスコード、生(設立)年月日、出資金合計金額、ステータス、連絡先(電話番号)、照会依頼者、回答区分、勤務先、行政機関情報、システム連携情報、勤務先の連絡先、行政機関管理番号、金融機関名、行政機関任意項目１、行政機関任意項目２、金融機関コード、店名、依頼番号、店番、回答基準日、取引有無、調査基準日、顧客番号、取引調査期間、口座番号、金融機関任意情報、口座種別、その他取引(貸出金/その他取引科目)。

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。