

個人情報保護管理運営会議 付議事項

件名	e L T A X納付導入に係る共通納税 IFS との外部結合について
----	-------------------------------------

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：会計室）

事業の概要

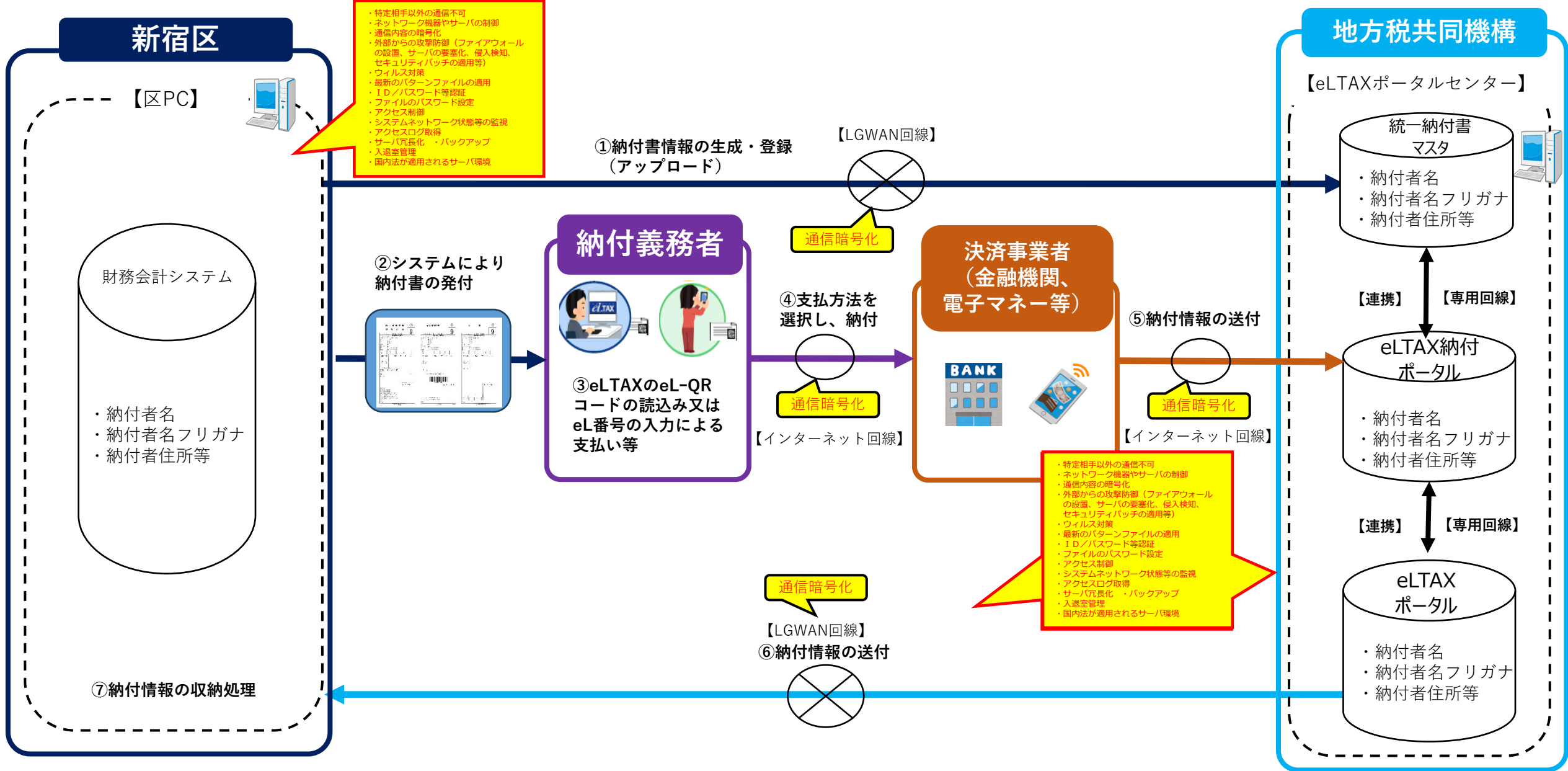
事業名	e L T A X納付導入に係る共通納税 IFS との外部結合について
担当課	会計室
目 的	eLTAX（エルタックス）を活用した地方税統一 QR（以下、「eL-QR」という。）による納付サービスを導入することで、区民の利便性及び業務の効率化を図るため。
対象者	e L T A Xで納付する納付義務者
事業内容	<p>1 概要</p> <p>「地方自治法の一部を改正する法律（令和 6 年法律第 65 号。以下「改正法」という。）が令和 6 年 6 月 26 日に公布された。改正法では「公金の収納事務のデジタル化」について規定されており、また「地方自治法の一部を改正する法律の公布及び施行について（通知）」（令和 6 年 7 月 2 日）においても、eLTAX を活用した納付を可能とする公金への対応を着実に進めるよう、言及されている。国からの要請を踏まえ、新宿区でも、令和 5 年度から税務課において eL-QR を利用した納付サービスが導入され、令和 8 年度第 1 回個人情報保護管理運営会議において、医療保険年金課及び高齢者医療担当課も導入された。</p> <p>このたび、財務会計システムで出力される納付書または納入通知書等についても、eLTAX を活用した eL-QR による納付サービスを導入することにより、区民の利便性の向上及び業務の効率化を図る。</p> <p>2 個人情報保護管理運営会議への付議内容</p> <p>区のイントラネット端末と地方税共同機構が構築・運営する共通納税インターフェースシステム（以下、「共通納税 IFS」という。）を L G W A N 回線で結合し、データの送受信を行う。</p> <p>3 対象者数</p> <p>年間 延べ 7, 5 0 0 人（令和 6 年度実績）</p> <p>※個人情報の流れは、資料 1 9 - 1 のとおり</p>

件名 eLTAXシステムとの外部結合について

保有課(担当課)	会計室
登録業務の名称	eLTAX を活用した電子納付
結合される情報項目(だれの、どのような項目か)	1 対象者 eLTAX で納付する納付義務者 2 情報項目 資料19-2のとおり
結合の相手方	地方税共同機構
結合する理由	eLTAX を活用した eL-QR による納付サービスを導入することにより、区民の利便性の向上及び業務の効率化が見込まれるため。 また、電子納付の納付件数が増加し、窓口での納付が減少することにより、特別出張所の窓口混雑の緩和が見込まれる。
結合の形態	区のイントラネット端末と地方税共同機構が運営する共通納税 IFS を LGWAN 回線(地方公共団体を相互に接続する行政専用の総合行政ネットワーク)で結合し、データの送受信を行う。
結合の開始時期と期間	令和8年9月24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

eLTAX納付導入に係る個人情報の流れ

※令和5年度から税務課にてeL-QRによる納付サービス導入済み。



(資料19-2) 結合される情報項目

財務会計システム及びその他のシステム等におけるの納付義務者の納付情報

【ファイル名：納付書情報登録ファイル】

登録区分、共通納税機関コード、税務事務所コード、所属コード、案件特定キー、確認番号、税目・料金番号、管理番号、公開開始日、賦課年度、課税年度、期別、納期限、指定期限、支払期限（公開終了日）、拡張領域（延滞金自動計算フラグ）、拡張領域（延滞金計算開始年月日）、拡張領域（延滞金免除等区分 1）、拡張領域（延滞金免除等期間 1（自））、拡張領域（延滞金免除等期間 1（至））、拡張領域（延滞金免除等区分 2）、拡張領域（延滞金免除等期間 2（自））、拡張領域（延滞金免除等期間 2（至））、未納額、延滞金、過少申告加算金額、不申告加算金額、重加算金額、各種手数料額、納付額、納税者 ID、拡張領域（関連 ID 区分）、拡張領域（関連 ID）、利用者向け確認用表示情報、還付済データ等への補記情報、納付可否区分、口座振替区分、拡張領域（金融機関コード）、拡張領域（店舗コード）、拡張領域（口座種別コード）、拡張領域（口座番号）、拡張領域（記号）、拡張領域（番号）、納付書情報登録依頼連番、納付書情報登録不可事由区分、納付書情報登録不可事由、拡張予備領域 01、拡張予備領域 02

【ファイル名：納付情報ファイル（納付日／入金日）】

（ヘッダ部）データ区分、ファイル種別、収納団体コード、システム利用領域 01、ファイル作成年月日、ファイル作成時刻、データ件数、エラーデータ件数、ワーニングデータ件数、決済単位年月日、システム利用領域 02、合計金額、システム予備

（データ部）データ区分、システム利用領域 03、制御情報、納付番号、収納団体コード、税目・料金番号、申告区分・課税期間、確認番号、履歴番号、パスワード、システム利用領域 04、システム利用領域 05、システム利用領域 06、システム利用領域 07、システム利用領域 08、システム利用領域 09、システム利用領域 10、システム利用領域 11、レスポンスコード、システム利用領域 12、システム利用領域 13、納付・請求情報、納付金区分、氏名カナ、氏名漢字、今回請求金額合計、請求本体金額、請求固定延滞金額、延滞金随時計算フラグ、納付情報変更年月日、納期限、延滞金計算開始年月日、延滞金表示区分、請求消費税、消費税表示区分、納付内容カナ、納付内容漢字、手数料負担区分、地公体任意情報、納付方式、拡張予備領域 01、機構指定納付受託者、仮消込情報、システム利用領域 14、今回支払金額合計累積、今回支払金額合計、支払納付額、支払延滞金額、支払消費税、領収区分、支払方法、チャネル区分、入力区分、印紙税額、他店券金額、システム利用領域 15、入金年月日、納付年月日、MPN 処理年月日、MPN 処理時刻、MPN 処理通番、仕向センタコード、金融機関コード、店舗コード、仕向処理年月日、仕向処理時刻、仕向処理通番、消込結果区分、決済年月日、MPN 通信サーバ登録年月日、拡張予備領域

02、チャネル区分 2、システム予備

（エンド部）データ区分、システム予備

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」	個人情報保護対策
区が行う個人情報保護対策 【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。
区が行う個人情報保護対策 【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」	個人情報保護対策
結合先に行わせる 個人情報保護対策 【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 個人情報保護対策 【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。