資料17

個人情報保護管理運営会議　付議事項

件名	ＬｏＧｏフォームの利用に係る外部結合について（手続の追加）

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）

（担当部課：総合政策部区政情報課、情報システム課
総務部税務課、子ども家庭部子ども家庭支援課、
健康部保健予防課）

事業の概要

事業名	行政手続のオンライン化等の推進
担当課	区政情報課、情報システム課、税務課、子ども家庭支援課、保健予防課
目　的	申請者が窓口に来庁することなく、２４時間申請手続を可能とするため、行政手続のオンライン化を推進し、区民の利便性向上を図る。
対象者	資料１７－１の手続の申請者
事業内容	１　概要 区では、平成１６年度から東京都及び都内区市町村で構成される東京電子自治体共同運営協議会が提供する「東京共同電子申請・届出サービス」を活用して、子どもや健康、防災、景観などに関する申請やイベントの申込みなどの手続をオンラインで受け付けてきた。 今後、「東京共同電子申請・届出サービス」が令和６年度末で廃止され、よりサービス利用者にとって申請がしやすく、職員にとっても申請フォームを作成しやすい新たな電子申請サービス（ＬｏＧｏフォーム）（以下、「ＬｏＧｏフォーム」という。）が、東京都及び都内区市町村で共同調達・導入されることとなった。（令和６年度第１回個人情報保護管理運営会議承認済） ついては、区の電子申請による行政手続の導入促進等の観点から、下記３点にかかる電子申請のみ付議することとする。 ①単年度手続者が１，０００人を超えることが想定される場合 ②オンライン決済機能を活用する場合 ③マイナンバーカードを活用した電子認証機能を活用する場合 ２　個人情報保護管理運営会議への付議内容 新たに、資料１７－１の手続をＬｏＧｏフォームに追加することで、さらなる区民の利便性の向上を図ることとするため、東京都及び都内区市町村で共同調達・導入するＬｏＧｏフォームに外部結合を行う。 ※申請者から区への個人情報の流れは、資料１７－２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　新たな電子申請サービス（Ｌｏ Ｇｏフォーム）の利用に係る外部結合について

※太字ゴシック（下線）が、令和６年度第１回新宿区個人情報保護管理運営会議承認済の内容からの変更箇所

保有課（担当課）	業務所管課（担当課：区政情報課、情報システム課）
登録業務の名称	**追加する手続（登録業務）は、資料１７－１のとおり**
結合される情報項目（だれの、どのような項目か）	**追加する手続ごとの情報項目は、資料１７－１のとおり**
結合の相手方	株式会社トラストバンク
結合する理由	当該電子申請サービスは、東京都及び都内の自治体が共同調達・利用することで高品質なサービスの廉価な提供を実現しているため。また、同サービスを活用することで、申請者は窓口に来庁することなく、２４時間申請手続が可能となり、区民の利便性向上を図ることができるため。
結合の形態	LGWAN 回線を利用して、当該電子申請サービスの提供がされるクラウドサーバ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６年６月２７日から令和７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

【資料１７－１】

【追加手続及び情報項目】

No	担当課	手続名（登録業務名）	取扱う個人情報項目	年間申請件数（概算）
1	税務課	税証明の請求	氏名、フリガナ、証明書の年度の初日が属する年の１月１日の住所、郵便番号、現在の住所、生年月日、電話番号、メールアドレス	約 1000 件
2	子ども家庭支援課	ベビーシッター利用支援事業助成金交付申請	氏名、郵便番号、住所、生年月日、電話番号、メールアドレス、口座情報	約 2000 件
3	保健予防課	HIV・性感染症検査の予約受付	メールアドレス、電話番号	約 1500 件

電子申請サービスに係る個人情報の流れ（住民等から区への申請）

（資料１７－２）

・特定相手以外の通信不可
・ネットワーク機器等制御による通信限定
・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、分析
・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

・個人情報保護法等の遵守
・立入調査等及び状況報告
・個人情報の消去、消去報告書の提出
・事故等への対応体制及び手順の整備
・事故発生時等の対応協議

株式会社トラストバンク
プライバシーマーク/ISMSクラウドセキュリティ認証取得済

他自治体

他自治体は区の情報にアクセスできない

・特定相手以外の通信不可
・ネットワーク機器等制御による通信限定
・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、分析
・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

申請者

パソコン、スマートフォン等

【インターネット回線】

通信暗号化

①専用サイトからの申請

④申請受付完了メールの通知

本人の同意に基づき利用申請手数料等の支払い

電子申請サービス（LoGoフォーム）

【申請者側機能】

申請

申請状況照会

申請取り下げ／再申請

【自治体側機能】

申請内容の確認

申請受付

申請差し戻し(補正依頼)

申請者情報のダウンロード

申込情報

決済情報

API連携

API連携

電子決済オプション
※必要な手続きのみ
・クレジットカード決済
・PayPay決済

電子認証オプション
※必要な手続きのみ
マイナンバーカードを用いた電子認証

【LGWAN回線】

②申請到達メールの通知

③申請内容の確認・申請受付処理

⑤申請情報等のダウンロード

※電子決済オプション利用の場合
決済手数料の支払い

※電子決済オプション利用の場合
決済金額の納付

新宿区

区イントラネットパソコン
（LGWAN端末）

申請情報

決済情報

⑥申請への対応及び対応記録の管理

（個別で確認が必要な場合は、電話で連絡する。）

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
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。