

個人情報保護管理運営会議 付議事項

件名	L o G o 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、健康部
健康づくり課、医療保険年金課）

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、健康づくり課、医療保険年金課
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46-1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（L o G o フォーム）（以下、「L o G o 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46-1の手続をL o G o 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L o G o フォームに外部結合を行う。 なお、当該手続は、上記①単年度手続者が1,000人を超えることが想定及び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ため付議を行う。 ※申請者から区への個人情報の流れは、資料46-2のとおり

件名 新たな電子申請サービス（L o G o 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7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）	区政情報課、情報システム課、健康づくり課、医療保険年金課
登録業務の名称	<u>追加する手続（登録業務）は、資料46-1のとおり</u>
結合される情報項目（だれの、どのような項目か）	<u>追加する手続ごとの情報項目は、資料46-1のとおり</u>
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	<u>令和6年12月20日</u> 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 4 6－1】

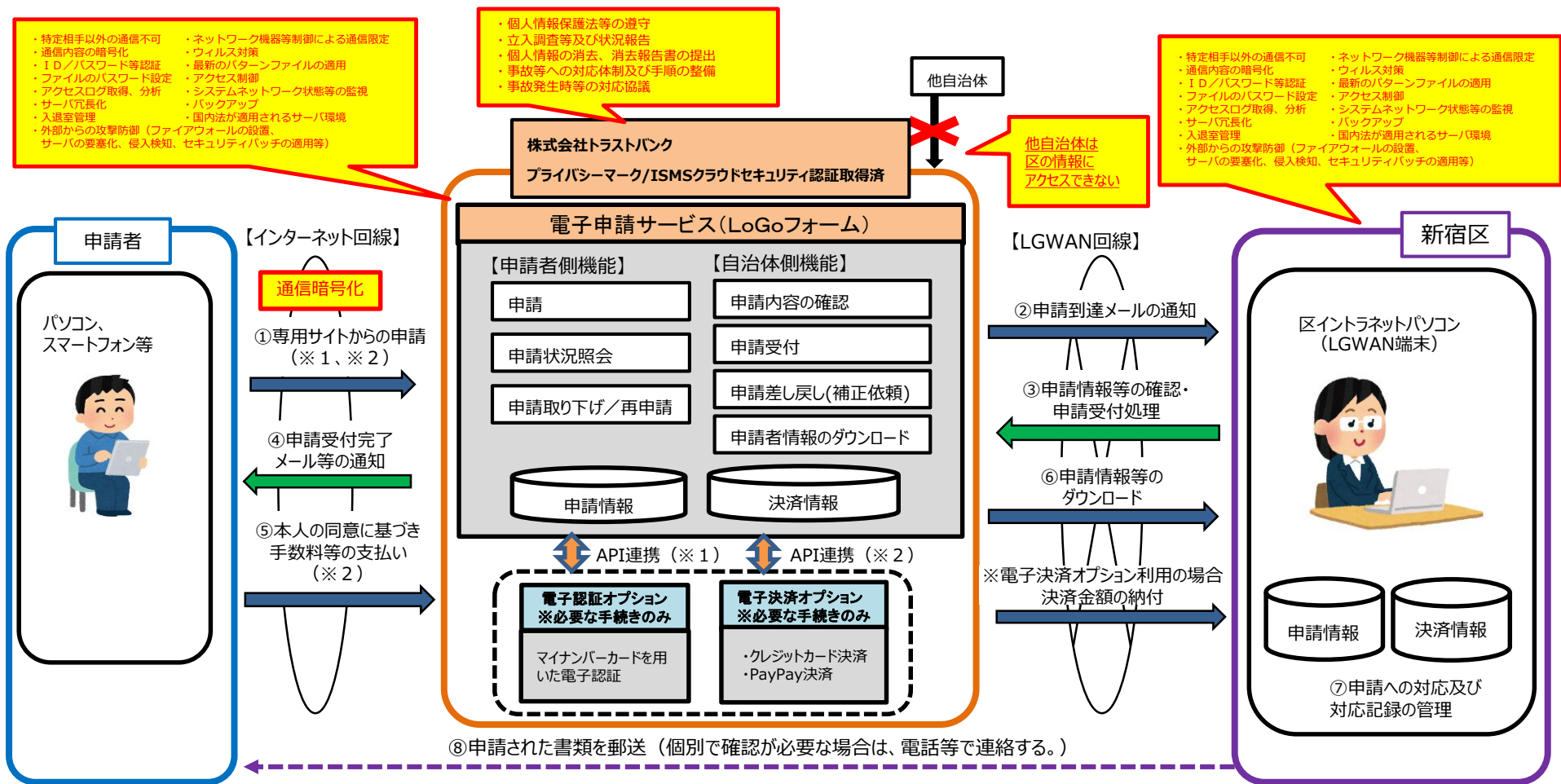
【追加手続及び情報項目】

No	担当課	手続名（登録業務名）	取扱う個人情報項目	付議内容
1	区政情報課	法律相談・交通事故相談 予約受付	氏名、フリガナ、電話番号、区内在住・在勤の別、在住地・ 在勤地の住所、相談内容（選択式）、メールアドレス（任 意）	①約 1,400 件
2	健康づくり課	健康診査・がん検診等受 診券の請求	保険種類、性別、生年月日、フリガナ、氏名、住所、電話 番号、メールアドレス	①約 2,000 件
3	医療保険年金課	国民健康保険被保険者 資格喪失届	現住所、前住所、世帯主の名前、電話番号、届出人の住所、 氏名、続柄、電話番号、資格喪失者の氏名、ふりがな、生 年月日、続柄、職業、在留資格、個人番号、個人番号変更 歴	①約 10,000 件 ③マイナンバーカード
4	医療保険年金課	国民健康保険被保険者 資格取得届	現住所、前住所、世帯主の名前、電話番号、届出人の住所、 氏名、続柄、電話番号、資格取得者の氏名、ふりがな、生 年月日、続柄、職業、在留資格、個人番号、個人番号変更 歴	①約 10,000 件 ③マイナンバーカード

※①単年度手続者が 1, 0 0 0 人を超えることが想定される場合、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

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46-2)



※1 「電子認証オプション」を活用した電子認証は、申請と併せ①の段階で行う。

※2 「電子決済オプション」を活用したオンライン決済は、④申請受付完了メール等の通知で決済金額を請求し、⑤の段階で行うほか、申請と併せ①の段階で行うこともできる。

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。