

個人情報保護管理運営会議 付議事項

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
----	---

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：総合政策部行政管理課、情報システム課）

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	行政管理課、情報システム課
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	電子申請サービスによる手続の利用対象者
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。 この度、「東京共同電子申請・届出サービス」が令和6年度末で廃止することに加え、よりサービス利用者にとって申請がしやすく、また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。 区においても、より一層、行政手続のオンライン化等を推進し、さらなる区民の利便性の向上を図るため、今後、新たに電子申請を導入する手続きについては、L o G o フォームを利用することとする。また、これまでの「東京共同電子申請・届出サービス」を活用した電子申請手続（約450件）についても、令和7年度以降のL o G o フォームの利用が決定次第、L o G o フォームに移行する予定である。 （参考）L o G o フォームの主な機能 （1）電子申請機能 ※インターネット環境だけでなく、LGWAN 環境にも申請フォームを公開することが可能であるため、当該サービスを導入する官公庁への電子申請も可能。 （2）マイナンバーカードを活用した電子認証機能 （3）証明書手数料等のオンライン決済機能 2 個人情報保護管理運営会議への付議内容 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。

	※L o G o フォームを活用する手続の類型及び取り扱う個人情報項目は、資料 2－1 のとおり。 ※申請者から区への個人情報の流れは、資料 2－2 のとおり ※区から官公庁への個人情報の流れは、資料 2－3 のとおり
--	--

件名 新たな電子申請サービス（ＬｏＧｏフォーム）の利用に係る外部結合について

保有課（担当課）	業務所管課（担当課：行政管理課、情報システム課）
登録業務の名称	行政手続のオンライン化等の推進
結合される情報項目（だれの、どのような項目か）	結合が想定される情報項目は、資料２－１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４月１５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 2－1】

【新たな電子申請サービス（L o G o フォーム）で結合が想定される情報項目】

No	手続の種類	保有課	取扱う代表的な個人情報項目
1	証明書等の交付手続	業務所管課	氏名、住所、生年月日、電話番号、メールアドレス、利用目的・用途、発行希望枚数
2	各種申請・申込・届出・請求・提出手続	業務所管課	氏名、住所、生年月日、電話番号、FAX 番号、メールアドレス、性別、年齢、個人番号、続柄、顔写真、本籍、国籍、在留資格、銀行口座情報、就労状況、家庭状況、居住状況、就学状況、看護及び介護状況、生活保護等受給状況、所得状況、疾病・障害者情報、申請理由、予防接種情報、妊娠情報、出生場所、履歴書情報、年金種類、死亡日、助成金情報、土地に関する事項、建築物に関する事項、譲渡予定価額に関する事項
3	相談や面談等の事前予約手続	業務所管課	氏名、住所、生年月日、電話番号、メールアドレス、性別、続柄、就学状況、通院情報、疾病・障害者情報、生育情報
4	区の財産（施設や物品等）の利用申請	業務所管課	氏名、住所、生年月日、電話番号、性別、年齢、続柄、就学状況、就労状況
5	会議や講座、イベント等への参加申込	業務所管課	氏名、住所、生年月日、電話番号、FAX 番号、メールアドレス、性別、年齢、年代、在住・在勤・在学の別、就学状況、就労状況、障害の有無、スポーツに関する嗜好・経験の有無、個別要望（託児、手話、車いす）の有無
6	アンケートや調査への回答	業務所管課	氏名、住所、生年月日、電話番号・FAX 番号、メールアドレス、性別、年齢、年代、在住・在勤・在学の別、就労状況、障害の有無・スポーツに関する嗜好・経験の有無

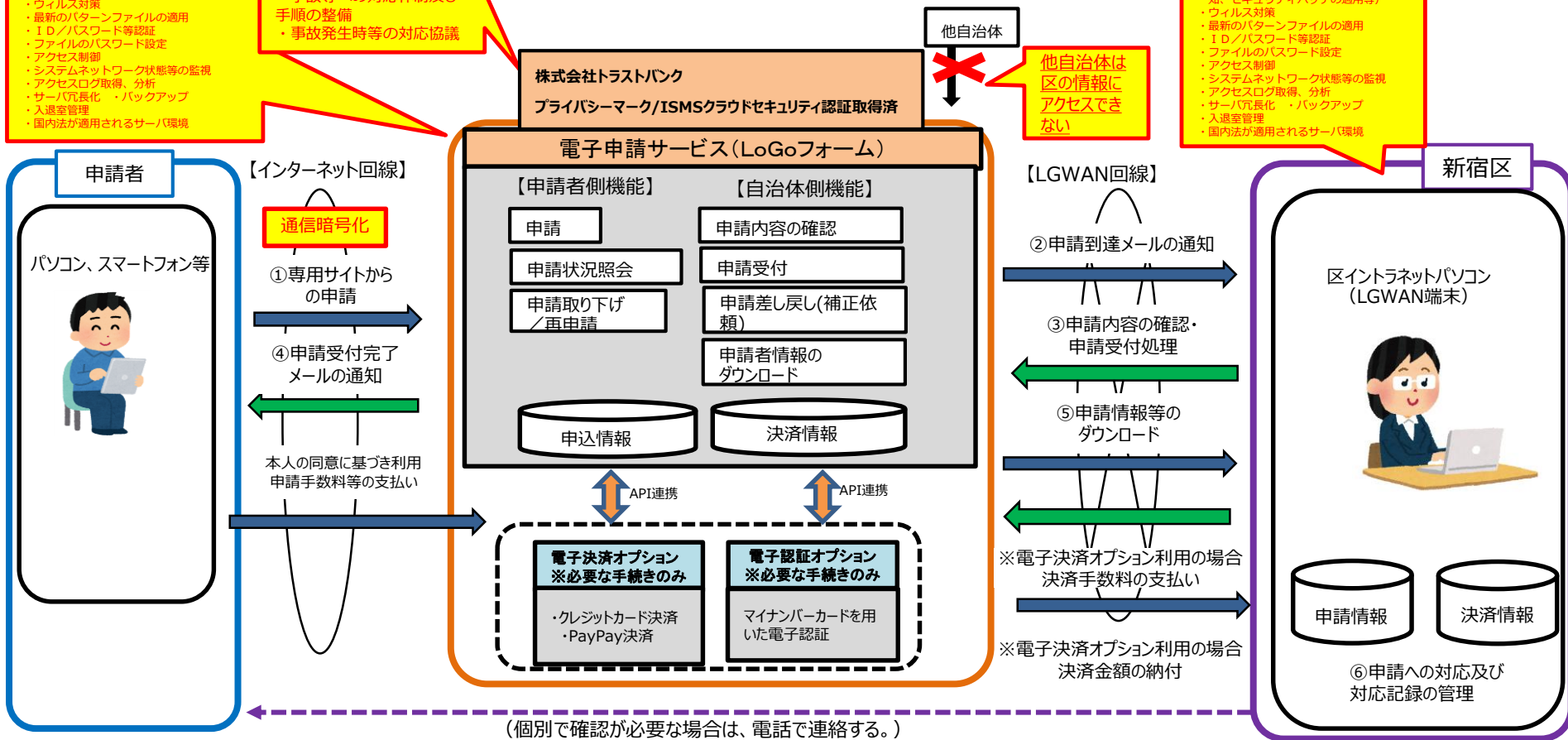
電子申請サービスに係る個人情報の流れ(住民等から区への申請)

(資料2-2)

- ・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)
- ・ウイルス対策
- ・最新のパスワードファイルの適用
- ・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

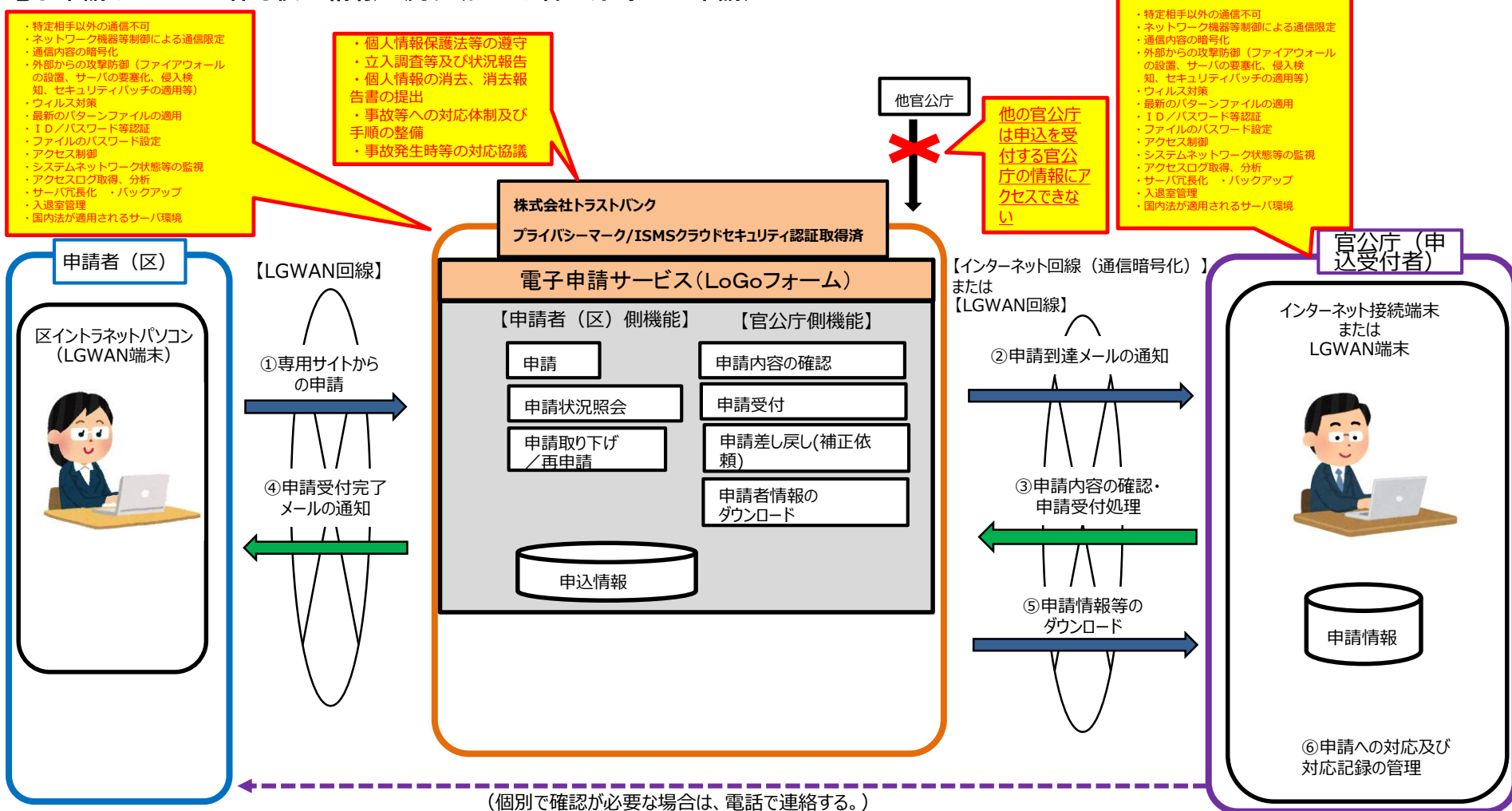
- ・個人情報保護法等の遵守
- ・立入調査等及び状況報告
- ・個人情報の消去、消去報告書の提出
- ・事故等への対応体制及び手順の整備
- ・事故発生時等の対応協議

- ・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)
- ・ウイルス対策
- ・最新のパスワードファイルの適用
- ・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



電子申請サービスに係る個人情報の流れ(区から官公庁等への申請)

(資料2-3)



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。