

個人情報保護管理運営会議 付議事項

件 名	乳児等通園支援事業に係る総合支援システムへの結合について
--------	------------------------------

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）

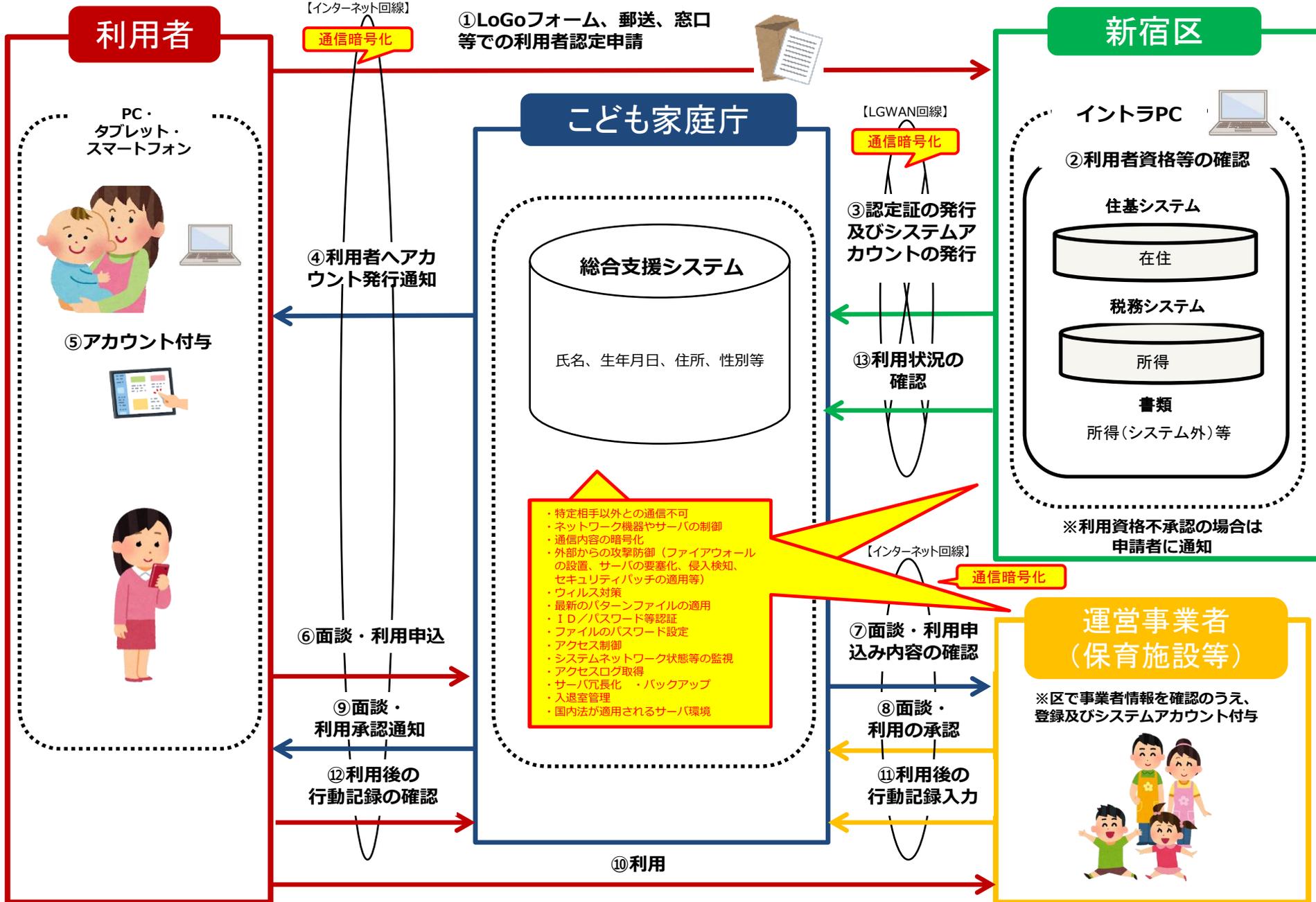
（担当部課：子ども家庭部子ども家庭課、保育課
保育指導課、教育委員会事務局学校運営課）

事業の概要

事業名	新宿区乳児等通園支援事業
担当課	子ども家庭課、保育課、保育指導課、学校運営課
目的	利用者が、区や事業所に来庁することなく申請手続きを可能とすることや、オンラインを利用し事業所検索ができること等により、区民の利便性向上を図る。
対象者	保育園等に通っていない、生後6か月から年度末年齢満3歳までの子ども
事業内容	<p>1 概要</p> <p>子ども・子育て支援法の改正により、児童福祉法において、乳児等通園支援事業が市区町村による認可事業として位置づけることになった。</p> <p>乳児等通園支援事業（国）では、居住区において利用者認定された、保育園等に通っていない生後6か月から満3歳までの子どもが、月10時間を上限とし、実施事業所に通園することで、こどもの育ちに資すること等を目的としている。</p> <p>この度、新宿区では、東京都の上乗せ事業（「多様な他者との関わりの機会の創出事業」）を活用し、対象年齢を年度末年齢満3歳、上限時間を160時間まで拡充し、令和8年4月から事業を実施する。</p> <p>2 個人情報保護管理運営会議への付議内容</p> <p>こども家庭庁が構築する総合支援システムと、区のイントラネット端末の外部結合を行う。</p> <p>3 対象者数</p> <p>利用者 約200名</p> <p>※個人情報の流れは、資料60-1のとおり</p>

件名 乳児等通園支援事業に係る総合支援システムへの外部結合について

保有課(担当課)	子ども家庭課、保育課、保育指導課、学校運営課
登録業務の名称	総合支援システム
結合される情報項目(だれの、どのような項目か)	<p>【保護者情報】 保護者の氏名、生年月日、住所、性別、続柄、生活保護の受給状況、非課税状況、年収360万未満、要支援児童世帯、メールアドレス、電話番号、就労・就学先</p> <p>【児童情報】 氏名、生年月日、住所、性別、医療的ケア児フラグ、障害児フラグ、要支援家庭フラグ、行動記録、緊急連絡先氏名、緊急連絡先年月日、緊急連絡先電話番号、緊急連絡先メールアドレス、緊急連絡先のこもとの続柄等、食事・アレルギー情報、病気・予防接種の状況(医師の診断書含む)、発育情報等</p>
結合の相手方	こども家庭庁
結合する理由	こども家庭庁が構築する総合支援システムにより、区、実施事業者、及び利用者における保育施設等の利用にかかる事務の効率化を図るため。
結合の形態	<p>区においては、LGWAN回線を利用して、当該サービスが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。</p> <p>利用者及び実施事業者は、インターネット回線を利用して、当該サービスの提供がされるクラウドサーバとパソコン等の端末を接続する。</p>
結合の開始時期と期間	令和8年3月2日から令和8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



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「-」	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「－」	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。	