資料44

個人情報保護管理運営会議　付議事項

件名	多言語化対応システ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：地域振興部戸籍住民課）

事業の概要

事業名	多言語化対応システムの導入
担当課	地域振興部戸籍住民課
目　的	窓口に多言語化対応システムを導入し、様々な言語圏から訪れる外国人とのコミュニケーションを円滑に行えるようにすることで、誤案内等の防止や窓口滞在時間の短縮など窓口サービスの向上を図る。
対象者	窓口に来庁する区民
事業内容	１　概要 現在、窓口に中国語・韓国語・英語に対応ができる複数言語対応会計年度職員を配置し、窓口対応を行っているが、様々な言語を母国語とした外国人が来庁しており、窓口での案内に支障が生じている。 このため、窓口に多言語化対応システムを利用することで、誤案内等の防止や窓口滞在時間の短縮など窓口サービスの向上を図る。 ２　個人情報保護管理運営会議への付議内容 多言語化対応システムを通じて翻訳を行うため、タブレット端末とクラウド上の音声認識・翻訳システムとの外部結合を行う。 ３　対象者数 約 13,400 人（令和 6 年度　戸籍住民課窓口外国人受付数） ※個人情報の流れは、資料４４－１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)

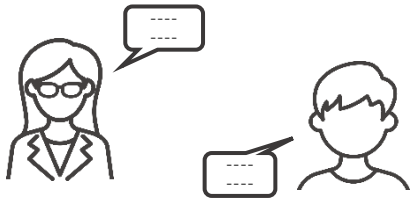
件名　多言語化対応システムの利用に係る外部結合について

保有課（担当課）	地域振興部戸籍住民課
登録業務の名称	住民基本台帳・印鑑登録・公的個人認証サービス・個人番号の指定び個人番号カードに関する事務・特別永住許可事務・市区町村在留関連事務・自動車臨時運航許可・戸籍・戸籍の附票・身分調書作成・身分証明・埋火葬許可・犯歴・震災避難者情報・被仮放免者情報
結合される情報項目（だれの、どのような項目か）	氏名、住所、生年月日、渡来の履歴、その他戸籍住民課窓口事務に必要な情報等
結合の相手方	ISMS認証取得済みの事業者を選定予定
結合する理由	当該システムを利用し、様々な言語を母国語とした外国人とのコミュニケーションを円滑に行うため。また、同システムは、他の自治体でも利用されており、複数の言語を高品質かつセキュアなサービスを廉価に提供されているため。
結合の形態	インターネット回線に接続されたタブレット端末を通して、当該システムが提供されるクラウドサーバを接続する。
結合の開始時期と期間	令和8年2月1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

多言語化対応システムの利用に係る個人情報の流れについて

・特定相手以外の通信不可
・通信内容の暗号化
・ＩＤ／パスワード等認証
・ファイルのパスワード設定
・アクセスログ取得、分析
・サーバ冗長化
・入退室管理
・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）
・ネットワーク機器等制御による通信限定
・ウィルス対策
・最新のパターンファイルの適用
・アクセス制御
・システムネットワーク状態等の監視
・バックアップ
・国内法が適用されるサーバ環境

新宿区窓口



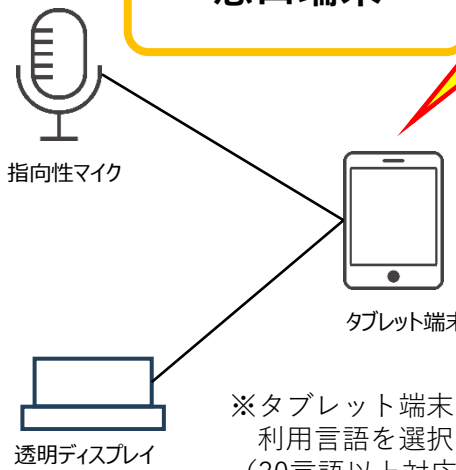
申請情報
審査情報
財産情報
事業関連情報

①マイクへの音声入力

⑤ディスプレイに文字表示された結果を確認

多言語対応システム
（ISMS認証取得済み）

窓口端末



※タブレット端末で利用言語を選択
（30言語以上対応）

④タブレット端末を通じて翻訳結果を透明ディスプレイに表示

【インターネット回線】
通信暗号化
②音声のアップロード
③翻訳結果のダウンロード

音声認識・翻訳システム（クラウドサービス）

＜主な機能＞
① 音声認識機能
② 文字起こし機能
③ 言語選択機能
④ 音声翻訳機能
⑤ 辞書登録機能

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。