資料15

個人情報保護管理運営会議　付議事項

件名	マイナンバーカードと在留カード等一体化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	マイナンバーカードと在留カード等一体化に係る外部結合
担当課	戸籍住民課
目　的	マイナンバーカードと在留カード等を一体化することで、区民の負担軽減及び利便性の向上を図る。
対象者	マイナンバーカードと在留カード又は特別永住者証明書一体化を希望する区民
事業内容	**１　概要** 在留カード等と個人番号カードの一体化等に係る改正法の施行により、令和8年6月14日から、マイナンバーカードと在留カード又は特別永住者証明書を一体化（特定在留カードまたは特定特別永住者証明書）させることができるようになる。一体化の申請は、住居地届の場合では区の窓口を経由して行うことができ、在留期間更新等の在留関連手続きの場合では出入国在留管理庁で行う。 なお、出入国在留管理庁で申請を受け付ける場合であっても、申請書IDの発番等については区との連携が必要となる。 **２　個人情報保護管理運営会議への付議内容** LGWAN回線を通じてJ-LISの専用サイト及び出入国在留管理庁との外部結合を行う。 **３　対象者数** 入国、転入、転居者のうち希望する者（参考（年間）：入国約12,000人、転入約5,500人、転居約3,400人） ※個人情報の流れは、資料１５－１・資料１５－２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　マイナンバーカードと在留カード等の一体化に係る外部結合について

保有課（担当課）	戸籍住民課
登録業務の名称	個人番号の指定、通知カード及び個人番号カードに関する事務
結合される情報項目（だれの、どのような項目か）	１　対象者 マイナンバーカード（個人番号カード）と在留カード又は特別永住者証明書の一体化を希望する者 ２　情報項目 申請情報（申請書ＩＤ、顔写真、電子証明書希望有無、展示希望有無、**氏名、生年月日、性別、住所**、暗証番号）
結合の相手方	**出入国在留管理庁及び地方公共団体情報システム機構（Ｊ－ＬＩＳ）**
結合する理由	出入国管理及び難民認定法等の一部を改正する法律（令和６年法律第５９号）等の施行により、マイナンバーカードと在留カード又は特別永住者証を一体化することができるようになる。**この一体化の申請の手続きにあたり、顔写真や申請情報をインターネット経由で J-LIS へ送信することや、申請書 ID を出入国在留管理庁へ送信する処理が必要となるため。**
結合の形態	J-LIS 及び出入国在留管理庁とはLGWAN 回線により通信を行う。
結合の開始時期と期間	**令和８年６月 14 日から令和９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

マイナンバーカードと在留カード又は特別永住者証明書の一体化に係る個人情報の流れ（区窓口での申請の場合）

（資料１５－１）

申請者

①一体化を希望する旨の申請

新宿区

②申請書の交付及び記入した申請書の受領

③区職員が申請者の顔写真を撮影

・特定相手以外との通信不可
・ネットワーク機器やサーバの制御
・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
・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

イントラPC又はタブレット端末

申請者情報
氏名、生年月日、性別、住所、申請書ＩＤ、顔写真、電子証明書希望有無、暗証番号

④申請書IDの発番

住民基本台帳ネットワークシステム

申請者情報
氏名、生年月日、性別、住所、申請書ＩＤ

出入国在留管理庁

⑥申請者情報（在留資格）の送信

⑤申請者情報の送信

通信暗号化

【LGWAN回線】

・特定相手以外との通信不可
・ネットワーク機器やサーバの制御
・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
・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

地方公共団体情報システム機構（Ｊ－ＬＩＳ）

申請サイト

⑦申請内容の確認

申請者情報
氏名、生年月日、性別、住所、申請書ＩＤ、顔写真、電子証明書希望有無、暗証番号

⑧特定在留カード等を発行

⑨申請者に特定在留カード等を郵送又は区の窓口で交付

マイナンバーカードと在留カード又は特別永住者証明書の一体化に係る個人情報の流れ
（出入国在留管理庁での申請の場合）

（資料１５－２）

申請者

①一体化を希望する旨の申請

出入国在留管理庁

②申請書の交付及び記入した申請書の受領

③申請者の顔写真を撮影

入管PC

申請者情報

氏名、生年月日、性別、住所、申請書ＩＤ、顔写真、電子証明書希望有無、暗証番号

・特定相手以外との通信不可
・ネットワーク機器やサーバの制御
・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
・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

④住所地区市町村に申請書ID付番依頼

【LGWAN回線】

通信暗号化

⑥申請書IDの送信

新宿区

⑤申請書IDの発番

住民基本台帳ネットワークシステム

申請者情報

氏名、生年月日、性別、住所、申請書ＩＤ

情報連携端末（入管より配布）

申請者情報

氏名、生年月日、性別、住所、申請書ＩＤ、顔写真、電子証明書希望有無、暗証番号

・特定相手以外との通信不可
・ネットワーク機器やサーバの制御
・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
・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

⑦申請者情報を送信

地方公共団体情報システム機構（Ｊ－ＬＩＳ）

申請サイト

⑧申請内容の確認

申請者情報

氏名、生年月日、性別、住所、申請書ＩＤ、顔写真、電子証明書希望有無、暗証番号

⑨特定在留カード等を発行

⑩申請者に特定在留カード等を郵送又は出入国在留管理庁で交付

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。