資料14

個人情報保護管理運営会議　付議事項

件名	国外転出者向けマイナンバーカードに係るオンライン申請受付に関す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	国外転出者向けマイナンバーカードに係るオンライン申請受付
担当課	戸籍住民課
目　的	国外転出者向けマイナンバーカードの申請をオンライン化することで、申請者の負担軽減及び利便性の向上を図る。
対象者	本籍人のうち国外転出者でマイナンバーカードの交付を希望する者
事業内容	１　概要 国外転出者向けマイナンバーカードの交付申請については、従来、紙の申請書を用いた郵送又は窓口での申請を受け付けていたところ、国外転出者の利便性向上の観点から、総務省よりオンライン申請システムによる申請受付への移行（令和８年５月 26 日より開始）の周知があった。申請は本人が地方公共団体情報システム機構（以下「J-LIS）という。）の専用サイトにアクセスし行うことを原則とするが、従前のとおり窓口や郵送で申請書を区が受領した場合は、本人に代わり申請処理を行う。 専用サイトについては国が指定するサイトで、各自治体に付与された ID、パスワードを使用しLGWAN回線を通じてアクセスする。 ２　個人情報保護管理運営会議への付議内容 区のイントラネットパソコンとJ-LISの専用システムをLGWAN回線を通じて外部結合を行う。 ３　対象者数 年間約300人（令和８年３月末現在） ※個人情報の流れは、資料１４－１・資料１４－２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　国外転出者向けマイナンバーカードに係るオンライン申請受付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 本籍人のうち国外転出者でマイナンバーカードの交付を希望する者 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、点字希望有無、氏名（振り仮名を含む）、生年月日、性別、本籍、暗証番号）
結合の相手方	地方公共団体情報システム機構（Ｊ－ＬＩＳ）
結合する理由	国外転出者向けマイナンバーカードの申請がオンライン化され、申請の手続きにあたり、申請情報をインターネット経由で J-LIS のシステムに登録する必要があるため。
結合の形態	区のイントラネット端末と地方税共同機構が運営する J-LIS を LGWAN 回線（地方公共団体を相互に接続する行政専用の総合行政ネットワーク）で結合し、データの送受信を行う。
結合の開始時期と期間	令和８年５月 26 日から令和９年３月 31 日（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

国外転出者向けマイナンバーカード交付申請のオンライン化に係る個人情報の流れ（オンライン申請）

（資料１４－２）

申請者

①国外転出者からの申請（オンライン申請）

地方公共団体情報システム機構（Ｊ－ＬＩＳ）

・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

申請サイト

②申請内容の確認

申請者情報

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

⑥申請内容の確認

⑦マイナンバーカードを発行

新宿区

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、本籍、申請書ＩＤ

・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

申請者情報

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

③申請書IDの発番依頼

【LGWAN回線】

通信暗号化

⑤申請者情報の送信

⑧在外公館等本人が希望する交付窓口へマイナンバーカードを送付

国外転出者向けマイナンバーカード交付申請のオンライン化に係る個人情報の流れ（窓口の対応）

（資料１４－１）

申請者

①国外転出者からの申請（窓口または郵送）

新宿区

②申請書の交付及び記入した申請書の受領

※写真は申請者が提出

・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

③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、本籍、申請書ＩＤ

イントラPC

申請者情報

氏名、生年月日、性別、本籍、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申請者情報の送信

通信暗号化

【LGWAN回線】

地方公共団体情報システム機構（Ｊ－ＬＩＳ）

専用サイト

⑤申請内容の確認

申請者情報

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

⑥マイナンバーカードを発行

⑦在外公館等本人が希望する交付窓口へマイナンバーカードを送付

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。