資料40

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特急発行に係る外部結合等について

内容は別紙のとおり

要綱の根拠

◇第３条第１項第３号（電算処理、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特急発行
担当課	戸籍住民課
目　的	マイナンバーカードの交付に要する期間の短縮することで、申請者の負担軽減及び利便性の向上を図る。
対象者	マイナンバーカードの交付申請を行う者
事業内容	1　概要 現在、マイナンバーカードの交付については、申請後、審査を経て概ね1～2か月程度の期間を要しており、速やかな交付が求められていた。 この度、特急発行・交付の仕組みが創設され、マイナンバーカードの交付について、新生児、紛失等による再交付、海外からの転入者など、特に速やかな交付が必要となる場合に、申請から区民にカードが届くまでの期間が１週間以内（最短５日）に短縮となる運用を導入する。 処理の流れは以下のとおり ①　職員等が申請者の顔写真を申請補助端末で撮影する。 ②　職員がインターネットを経由して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、顔写真データと申請データを登録する。 ③　J-LIS はマイナンバーカードを発行し、申請者あてに郵送する。 2　個人情報保護管理運営会議への付議内容 （1）電算処理 マイナンバーカードの特急発行を行うため、申請補助端末に特急発行のアプリをダウンロードする。 （2）外部結合 申請補助端末からインターネット回線を通じてJ-LIS の専用サイトとの結合を行う。 3　対象者数 年間 16,000 人（入国：12,000 人、出生：2,300 人、紛失等：1,700 人） ※個人情報の流れは、資料４０－１のとおり

別紙（個人情報処理システム開発・変更関係）

◇電算処理（第３条第１項第３号）

件名　マイナンバーカード特急発行に係るシステムの開発について

※太字ゴシック（下線）は、令和元年度第６回情報公開・個人情報保護審議会承認済みの内容からの変更箇所

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
記録される情報項目（だれの、どのような項目が、どこのコンピュータに記録されるのか）	１　個人の範囲 マイナンバーカードの交付申請を行う者 ２　記録項目 申請情報（**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、点字希望有無、暗証番号） ３　記録するコンピュータ **電磁的媒体（申請補助端末）**
新規開発・追加・変更の理由	**マイナンバーカードの特急発行の手続きを１台の端末上でできるようにすることにより、申請に係る手続きを簡略化し申請者の負担軽減及び利便性の向上を図る。**
新規開発・追加・変更の内容	行政手続における特定の個人を識別するための番号の利用等に関する法律等の一部を改正する法律（令和５年法律第48号）に基づき、申請時に市区町村の庁舎等に来庁して本人確認が行われた者のうち、**マイナンバーカードの交付を速やかに受ける必要がある者として政令で定めるものに該当する者が申し出た場合は、J-LIS がカードをその者に直接送付する「特急発行」の仕組みが導入される。このマイナンバーカードの特急発行申請に必要となる、①顔写真の撮影、②画像のトリミング、③申請情報の入力までの手順を、１台の端末で行うことができるアプリケーションを導入する。**
開発等を委託する場合における個人情報保護対策	別紙チェックリストのとおり
新規開発・追加・変更の時期	**令和６年１１月　開発** **令和６年１１月　テスト** **令和６年１２月　本稼働**

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特急発行に係る外部結合について

※太字ゴシック（下線）が令和元年度第６回情報公開・個人情報保護審議会承認済みの内容からの変更箇所

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）の交付申請を行う者 ２　情報項目 申請情報（**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、点字希望有無、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	行政手続における特定の個人を識別するための番号の利用等に関する法律等の一部を改正する法律（令和５年法律第48号）に基づき、申請時に市区町村の庁舎等に来庁して本人確認が行われた者のうち、**マイナンバーカードの交付を速やかに受ける必要がある者として政令で定めるものに該当する者が申し出た場合は、J-LIS がカードをその者に直接送付する「特急発行」の仕組みが導入される。このマイナンバーカードの特急発行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 へ送信する必要があるため。**
結合の形態	インターネット回線（暗号化通信）を用いて情報項目の送信を行う
結合の開始時期と期間	**令和６年１２月２日から**（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

マイナンバー特急発行に係る個人情報の流れ

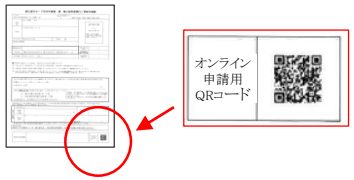
（資料４０－１）

申請者

①新生児、紛失等による再交付、海外からの転入者などが来庁

新宿区

②ID付き申請書を窓口で交付



③申請補助端末で申請書のＱＲコードをスキャン

④区職員が申請補助端末で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
・メモリ内のデータは、送信後に自動消去

申請補助端末（タブレット・パソコン）

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、点字希望有無、暗証番号

SSLによる通信暗号化

【インターネット】

⑤特急発行申請サイトに顔写真及び申請者情報を送信（※氏名、生年月日、性別、住所は送信しない）

・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）

特急発行申請サイト

⑥申請データを手入力

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、点字希望有無、暗証番号

⑦マイナンバーカードを発行

⑧申請者にマイナンバーカードを郵送（簡易書留）

3　電算処理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
開発等を委託する場合における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。
	○	区のシステム機器設置場所へ委託先が入退室する場合は、管理（申請、承認、記録）を行う。また、委託先がシステム機器を操作する場合には、事前に作業内容の報告を求め、区が承認した後に実施するよう指導するとともに、個人情報データの持出しを禁止する。
	○	プログラムの移行等を行う場合は、外部記録媒体の管理を行い、利用時は第三者漏えいがないようパスワードを施す等、利用制限を設ける。
	○	入力及び取込みテストにおいては、ダミーデータを使うよう指導する。
	○	実データを使用した検証作業は、区職員が実施する（委託先には、必要な支援のみ行わせる）。
	○	モバイルパソコン等の電子計算組織を持込む場合は、事前に区の許可をとらせ、用途は、社内事務連絡、設計書等の閲覧に限定させる。また、委託先のモバイルパソコン等と区のネットワーク、システム機器及びUSB等の記録媒体と接続をさせないように、区の職員が立ち会う。
	○	データ項目定義の修正漏れによるシステム不具合等が無いよう、双方で事前に綿密なスケジュール計画やチェックシートを作成して実施する。なお、稼働にあたっては必ず仮移行を行うこととし、本稼働はシステムを使用していない時間帯（時間外・休日）に実施し、十分な検証を行う。
開発等を委託する場合におけ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。

3　電算処理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
開発等を委託する場合における委託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。
	○	区のシステム機器設置場所へ委託先が入退室する場合は、区の管理（申請、承認、記録）に従わせる。また、委託先がシステム機器を操作する場合には、事前に作業内容の報告をさせ、区が承認した後に実施させるとともに、個人情報データの持出しを禁止させる。
	○	プログラムの移行等を行う場合は、外部記録媒体の管理を行い、利用時は第三者漏えいがないようパスワードを施す等、利用制限を設ける。
	○	入力及び取込みテストにおいては、ダミーデータを使わせる。
	○	実データを使用した検証作業は、区職員が実施する（委託先には、必要な支援のみ行わせる）。
	○	モバイルパソコン等の電子計算組織を持込む場合は、事前に区の許可をとらせ、用途は、社内事務連絡、設計書等の閲覧に限定させる。また、委託先のモバイルパソコン等と区のネットワーク、システム機器及びUSB等の記録媒体と接続をさせないように、区の職員の立会いに応じさせる。
	○	データ項目定義の修正漏れによるシステム不具合等が無いよう、双方で事前に綿密なスケジュール計画やチェックシートを作成して実施する。なお、稼働にあたっては必ず仮移行を行うこととし、本稼働はシステムを使用していない時間帯（時間外・休日）に実施させ、十分な検証を行させる。
開発等を委託する場合における委託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。

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。