資料48

個人情報保護管理運営会議　付議事項

件名	医師等の免許申請手続き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：健康部衛生課）

事業の概要

事業名	国家資格等情報連携・活用システムを利用した医師等の免許申請手続きのオンライン化
担当課	健康部衛生課
目　的	医師等の免許申請手続きのオンライン化を推進し、区民の利便性向上を図るため。
対象者	医師、歯科医師、保健師、助産師及び看護師の新規免許申請者 （診療放射線技師、臨床検査技師、衛生検査技師、理学療法士、作業療法士、視能訓練士に係る免許申請、死体解剖資格に係る認定申請については、利用開始時期を検討中。）
事業内容	１　概要 区では現在、医師国家試験等の合格者が免許を取得する場合や、免許取得後に氏名等の登録事項に変更が生じた場合に、紙による申請を受け付け、内容の確認等を行った上で、東京都を経由して厚生労働省へ進達している。その後、厚生労働省において免許登録及び免許証の交付が行われている。 このたび、令和8年10月から、マイナンバーを活用した国家資格等情報連携・活用システム（以下「国家資格等システム」という。）を利用した免許申請手続を開始する。国家資格等システムを利用した申請手続きの電子化を行い、さらなる区民サービスの向上、行政事務の効率化等を推進する。 なお、医師、歯科医師、保健師、助産師及び看護師の「籍訂正」「再交付」「抹消」申請については、利用開始時期を検討中である。 ２　個人情報保護管理運営会議への付議内容 LGWAN回線を介して、区のイントラPCと国家資格等システムとの外部結合を行う。 ３　対象者数 新規申請821件（令和７年度実績） （内訳）　医師112件　歯科医師20件　保健師95件　助産師34件 看護師560件 ※個人情報の流れは、別紙資料４８－１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　医師等の免許申請手続きに係る外部結合について

保有課（担当課）	健康部衛生課
登録業務の名称	国家資格等情報連携・活用システムを利用した医師等の免許申請手続
結合される情報項目（だれの、どのような項目か）	１　個人の範囲 医師、歯科医師、保健師、助産師及び看護師の新規免許申請者 ２　記録項目 資料４８－２のとおり
結合の相手方	国家資格等情報連携・活用システム（デジタル庁）
結合する理由	現在、紙申請により行っている免許申請手続きについて、業務効率化を図る等の観点より電子化を実施するため。
結合の形態	LGWAN 回線により、区のイントラネット端末と国家資格等情報連携・活用システムとの外部結合を行う。
結合の開始時期と期間	令和８年１０月２６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

医師等の免許申請手続きに係る個人情報の流れ

資料48-1

区民

パソコン

スマートフォン
タブレット

【インターネット】

通信暗号化

①ぴったり
サービスにログイン

※マイナンバーカード認証
・利用者用電子証明書
・パスワード
・署名用電子証明書

⑥修正通知

⑦再申請

地方公共団体情報システム機構
（Ｊ－ＬＩＳ）

マイナポータル
ぴったりサービス

②電子申請入力
（申請者向け機能）

申請者情報

氏名、性別、生年月日等
詳細は48-2のとおり

・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・申請者情報は１か月後に自動消去

自動連携

国

国家資格等システム

氏名、性別、生年月日等
詳細は48-2のとおり

【LGWAN回線】

③申請内容の
ダウンロード

⑤申請内容に不備が
ある場合、修正依頼

⑧再申請内容の
ダウンロード

・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・申請者情報は１か月後に自動消去

新宿区

区イントラネット
（情報戦略課管理）

④申請内容の審査

申請者情報

氏名、性別、生年月日等
詳細は48-2のとおり

⑨確認後、都に進達

（資料 48-2）

国家資格等情報連携・活用システム記録項目

申請区分名、業務種別名、手続名、受付機関名、受付年月日、申請ステータス、決済ステータス、登録番号、申請 ID、再申請可否、再申請 ID、申請者氏名（漢字)、申請者氏名（かな／カナ)、外字表記希望、旧姓表記希望、旧姓、都道府県名（漢字)、申請者住所、本籍地（和名)、申請者生年月日、申請者性別、申請者電話番号、申請者メールアドレス、郵送元受付機関名、送付先住所、資格仮名、マイナンバーカード（氏名、住所、生年月日、性別、情報取得日時)、合格者番号、合格年月日、一部合格番号、一部合格年月日、一部免除番号、一部免除合格年月日、試験免除番号、免除年月日、施行年月日、実施回、受験地、受験地コード、罰金以上の刑に処せられたことの有無、罪・刑及び刑の確定年月日、医事（歯科医師、保健師、助産師及び看護師）に関し犯罪又は不正の行為を行ったことの有無、違反の事実及び年月日、出願後の本籍又は氏名の変更の有無、出願時の本籍又は氏名、旧姓併記の希望の有無、旧姓、過去に医師（歯科医師、保健師、助産師及び看護師）免許を有していたことの有無、過去に有していた医師（歯科医師、保健師、助産師及び看護師）免許の登録番号、本籍地（国籍)、郵便番号、マイナンバー登録住所と免許証送付先住所との相違の有無（転居予定も含む)、相違が「有」を選択した場合の住所、免許証送付先住所の確認、電話番号２、氏名表記、通称名の併記、通称名、性別、添付資料における診断書の各項目において、「該当する」、「専門家による判断が必要」、又は「あり」の該当の有無、免許申請の同意、マイナポータルでの電子決済の確認、資格管理団体側で登録事項の変更を検知した場合に職権修正することの合意、診断書、罰金以上の刑にかかる判決謄本または略式命令書一式、罰金刑については当該罰金にかかる領収証書、略歴書、反省文、国家試験合格後１年以上経過した申請については現在まで合格職種の業務に従事していない旨の申述書

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。