資料57

個人情報保護管理運営会議　付議事項

件名	マイナポータルぴったり電子申請サービスの利用に係る外部結合について（手続の追加）

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：福祉部地域介護保険課）

事業の概要

事業名	行政手続のオンライン化等の推進
担当課	介護保険課
目　的	介護保険資格取得・異動・喪失の届出等に関する事務において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	マイナポータルぴったり電子申請サービスを利用して、介護保険資格取得・異動・喪失の届出等に関する事務の申請を行う者。
事業内容	１　概要 国は令和２年１２月に策定した「デジタル・ガバメント実行計画」において、地方公共団体が優先的にオンライン化を推進すべき手続の内、特に国民の利便性向上に資するオンライン化対象手続については、原則マイナポータルの基盤を活用することとされた。 そのため、区では、対象手続等において、マイナポータルぴったり電子申請サービスを活用し、電子申請手続きの検索から申請まで一貫したサービスを提供することで、区民サービスの向上、行政事務の効率化等を推進している。（令和３年度第９回、令和４年度第７回情報公開・個人情報保護審議会承認済み） 「規制改革実施計画」（令和４年６月７日閣議決定）において、オンライン化する方針が決定している約 12,000 種類の手続について、令和７年末までにオンライン化することとされており、介護保険資格取得・異動・喪失の届出等に関する事務が情報連携の対象事務に追加された。 そのため、区では、介護保険資格取得・異動・喪失の届出等に関する事務においても、マイナポータルぴったり電子申請サービスを活用し、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。 ２　個人情報保護管理運営会議への付議内容 既に外部結合を行っている「総合行政ネットワークシステム（ＬGWAN）を介した地方公共団体情報システム機構（J-LIS)」において、手続の追加を行う。 **３　対象者数** 介護保険（令和７年１２月末現在） ・被保険者数・・・・・・・・・・・・・６７，８８９人 ※個人情報の流れは、資料５７－１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　マイナポータルぴったり電子申請サービスの利用に係る外部結合について（手続の追加）

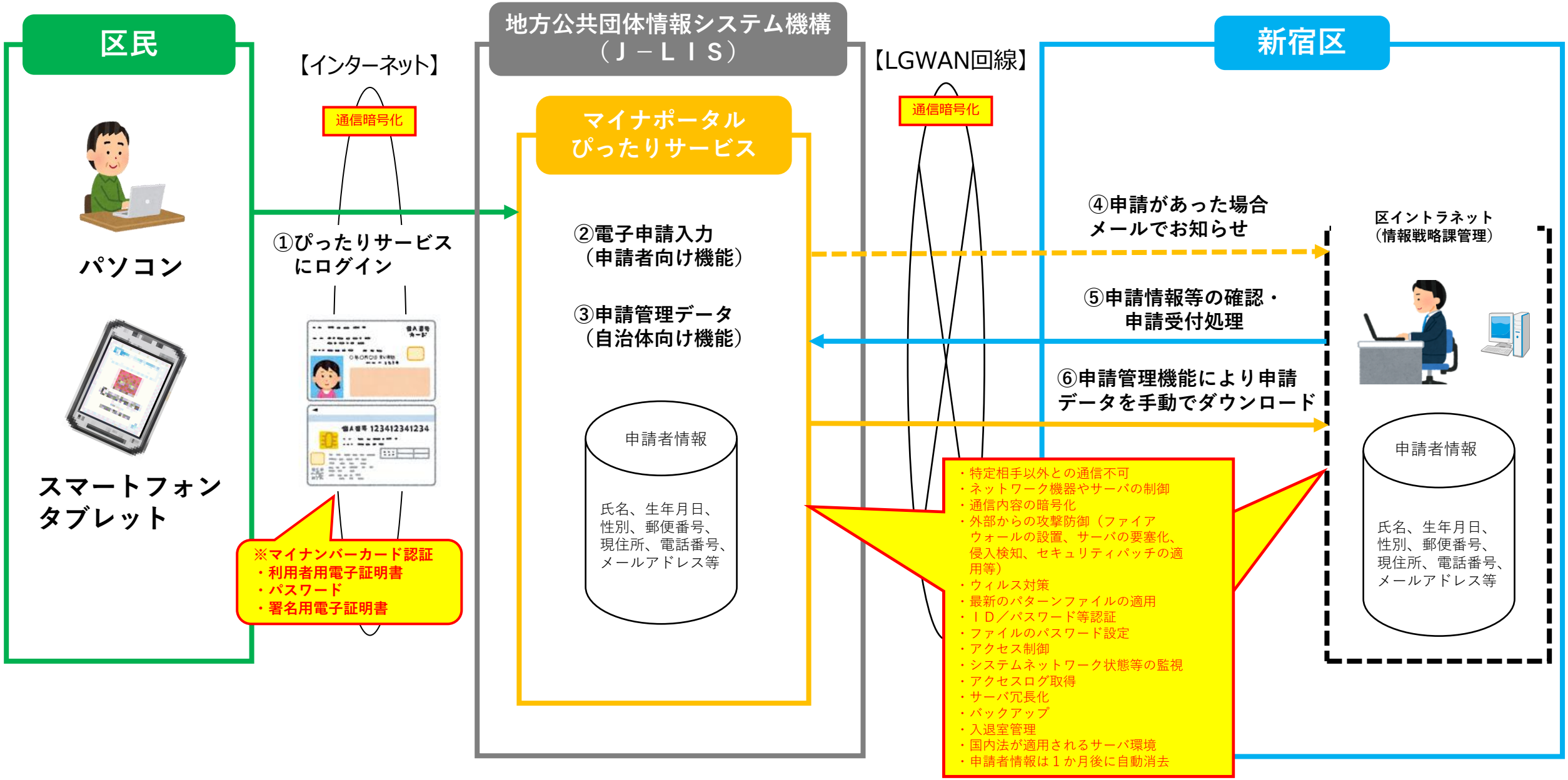
※太字ゴシック（下線）が、令和４年度第７回情報公開・個人情報保護審議会承認済の内容からの変更箇所

保有課（担当課）	介護保険課
登録業務の名称	介護保険資格取得・異動・喪失の届出等に関する事務申請
結合される情報項目（だれの、どのような項目か）	**追加する事業ごとの情報項目は、資料５７－２のとおり**
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	マイナポータルぴったり電子申請サービスは、国がシステムを構築し、日本全体で共同利用することで高品質なサービスの提供を実現している。 このサービスを活用することで、行政手続のオンライン化を推進し、区民の利便性向上を図ることができるため。
結合の形態	総合行政ネットワーク(LGWAN)を介し、地方公共団体情報システム機構(J-LIS)のサーバと、区イントラネットパソコン(LGWAN端末)を接続する。
結合の開始時期と期間	**令和８年３月３０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

マイナポータルぴったり電子申請サービスを利用した電子申請に係る個人情報の流れ
【介護保険資格取得・異動・喪失の届出等事務申請手続】

資料57-1

※本電子申請サービスの利用に係る地方公共団体情報システム機構との外部結合については、令和４年度第７回情報公開・個人情報審議会承認済。
新たに、介護保険資格取得・異動・喪失の届出等事務申請手続きを追加する。（追加項目は資料57-2のとおり）



（資料57-2）

No	事務事業	担当課	利用する情報の項目
1	介護保険資格取得・異動・喪失の届出	介護保険課	届出年月日、届出人氏名、届出人と本人の関係、届出人住所、届出人電話番号、変更年月日、資格異動年月日、資格異動事由、届出事由、新住所、電話番号、旧住所、本年1月1日の住所、世帯員氏名、世帯員氏名（フリガナ）、世帯員生年月日、世帯員続柄、世帯員被保険者番号、世帯員個人番号
2	介護保険住所地特例適用・異動・喪失の届出	介護保険課	申請理由、届出年月日、届出人氏名、届出人と本人の関係、届出人住所、届出人電話番号、被保険者番号、被保険者の個人番号、被保険者氏名、フリガナ、被保険者の生年月日、世帯主との続柄、世帯主の個人番号、世帯主の氏名、世帯主の生年月日、従前の住所、従前の電話番号、異動前の施設の名称、退所（居）年月日、異動後の住所、異動後の電話番号、異動後の施設の名称、施設の入所（居）年月日
3	被保険者証の交付申請	介護保険課	申請年月日、申請者氏名、申請者と本人の関係、申請者住所、申請者電話番号、被保険者個人番号、被保険者氏名（漢字）、被保険者氏名（フリガナ）、被保険者の生年月日、被保険者住所、被保険者電話番号、医療保険者名、医療保険被保険者記号番号
4	介護保険サービスの種類の指定の変更の申請	介護保険課	申請年月日、介護保険被保険者番号、個人番号、医療保険保険者名、医療保険保険者番号、医療保険被保険者記号・番号・枝番、被保険者氏名（漢字）、被保険者氏名（フリガナ）、被保険者の生年月日・性別・住所、現に受けている要介護要支援認定とその有効期間、新たに受けようとするサービスの種類又は現に受けてるサービスの種類記載の消除を求める旨、種類指定変更理由、主治医の氏名・医療機関名・所在地、特定疾病名
5	支払い方法変更及び支払い一時差止等措置に係る終了申請	介護保険課	介護保険保険者番号、介護保険被保険者番号、被保険者氏名（漢字）、被保険者氏名（フリガナ）、被保険者生年月日、被保険者住所、被保険者電話番号、申請理由、申請年月日、申請者住所、申請者氏名、申請者電話番号

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。