資料48

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：地域振興部地域コミュニティ課、
福祉部地域福祉課）

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	地域コミュニティ課、地域福祉課
目　的	災害弔慰金の支給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、災害弔慰金の支給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） この度、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第１９条第８号に基づく利用特定個人情報の提供に関する命令（令和６年デジタル庁・総務省令第９号）が定められたことにより、災害弔慰金の支給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、災害弔慰金の支給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 約４，３００人（令和４年５月　都被害想定） ※個人情報の流れは、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　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）	地域コミュニティ課、地域福祉課
登録業務の名称	災害弔慰金の支給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４８－２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７年２月１６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　【災害弔慰金等事務申請手続】　（資料４８－１）

※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、災害弔慰金等事務申請手続を追加する。

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

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）

③申請管理データ
（自治体向け機能）

申請者情報

氏名、生年月日、
性別、郵便番号、
現住所、電話番号、
メールアドレス等

【LGWAN回線】

通信暗号化

・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

④申請があった場合
メールでお知らせ

⑤申請情報等の確認・
申請受付処理

⑥申請管理機能により申請
データを手動でダウンロード

区イントラネットパソコン
（情報システム課管理）

申請者情報

氏名、生年月日、
性別、郵便番号、
現住所、電話番号、
メールアドレス等

（資料48―2）

No	事務事業	担当課	利用する情報の項目
1	災害弔慰金の支給事務	地域コミュニティ課	災害名、【亡くなった方】住所（被災時）、氏名（フリガナ）、性別、生年月日、亡くなった場所、死亡年月日、亡くなった状況、【ご遺族の方】＜先順位・第2順位＞配偶者（住所・氏名）、子（住所・氏名）、父母（住所・氏名）、孫（住所・氏名）、申請年月日、【申請者】住所、氏名、滞在先住所、電話、マイナンバー、故人の状況（申出人、死亡者との続柄、死亡者氏名、性別、死亡時年齢、災害の発災3か月前から死亡までの経緯、災害発生前の故人の状況について、災害発生後の個人の状況について、あなたが考える故人の死亡と被災との関係）、振込指定金融機関、預金種別、口座番号、口座名義、依頼人氏名、生計同一に関する申立、同意意思確認
2	災害障害見舞金の支給事務	地域コミュニティ課	災害名、【負傷された方】住所（被災時）、氏名（フリガナ）、性別、生年月日、負傷された場所、負傷された年月日、状況、【被災時の世帯状況】同居者続柄、氏名、住所、扶養の有無、【支給に関する事項】障害の種類程度等、生計維持者の確認、調査同意意思確認、申請年月日、申請者郵便番号、住所、滞在先郵便番号、滞在先住所、氏名、電話、マイナンバー、障害を受けた方の状況（申出人、障害を受けた方との続柄、障害を受けた方の氏名、性別、災害を受けた時の年齢、障害を受けるまでの経緯、災害発生前の障害を受けた方の状況について、あなたが考える障害を受けた方と被災との関係）、診断書、振込指定金融機関、預金種別、口座番号、口座名義、依頼人氏名
3	災害援護資金の貸付事務	地域福祉課	被災日時、災害名、被災の種類、被害場所（住所）、氏名（フリガナ）、性別、生年月日、現住所、本籍、郵便番号、電話番号、マイナンバー、職業、勤務先名称、勤務先所在地、勤務先電話番号、世帯の状況と所得（世帯員氏名、世帯主との続柄、年齢、マイナンバー、健否、職業、年間所得、勤務先・学校名）、資産の状況（土地面積、住居の状況、建物面積、生活保護受給有無、負債内容、負債金額）、連帯保証人情報（氏名（フリガナ）、性別、生年月日、年齢、郵便番号、現住所、電話番号、職業、年間所得、申込者との関係、家族数、資産、勤務先名称、勤務先所在地、勤務先電話番号）、調査同意意思確認、連帯保証意思確認

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。