資料49

個人情報保護管理運営会議　付議事項

件名	災害弔慰金の支給等に関する事務に係る被災者生活再建支援システム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：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	被災者生活再建支援システムの運用
担当課	地域コミュニティ課、地域福祉課
目　的	災害発生時における効率的な被災者情報の一元管理のため、被災者生活再建支援システムに以下①～③の事務における経過を記録し、発災後の対応の迅速化を図る。 ①災害弔慰金支給事務 ②災害障害見舞金支給事務 ③災害援護資金の支給および免除事務 ※①②地域コミュニティ課、③地域福祉課
対象者	新宿区の住民基本台帳に記録されている住民及び住民登録外者
事業内容	１　概要 現在、国では、被災者支援業務の迅速化・効率化を図るため、「被災者生活再建支援システム」を構築し、区でも令和７年２月１日より導入する予定である。（令和６年度第５回個人情報保護管理運営会議承認済み） この「被災者生活再建支援システム」の１つである「被災者台帳システム」では、被災者に関する情報を一元管理することができる。 そのため、①災害弔慰金の支給事務、②災害障害見舞金の支給事務については地域コミュニティ課、③災害援護資金の貸付及び免除事務については地域福祉課が「被災者台帳システム」を活用し、被災者に対する支援業務の迅速化・効率化を図る。 ２　個人情報保護管理運営会議への付議内容 既に東日本電信電話株式会社（NTT 東日本）と外部結合を行っている被災者生活再建支援システムの LGWAN 回線において、上記①～③の事務における個人情報確認・入力を追加する。 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４９－１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　災害弔慰金の支給等に関する事務に係る被災者生活再建支援システムに係る外部結合について

※太字ゴシック（下線）は、令和６年度第５回新宿区個人情報保護管理運営会議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	被災者生活再建支援システムについて
結合される情報項目（だれの、どのような項目か）	１　対象者 新宿区の住民基本台帳に記録されている住民及び住民登録外者 ２　追加する情報項目 **資料４９－２のとおり**
結合の相手方	東日本電信電話株式会社（ＩＳＭＳ認証取得済）
結合する理由	**災害弔慰金の支給等に関する事務において「被災者生活再建支援システム」の１つである「被災者台帳システム」を活用することで、被災者に対する支援業務の迅速化・効率化を図るため。**
結合の形態	総合行政ネットワーク（ＬＧＷＡＮ）を介し、被災者生活再建支援システムのサーバと、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

災害弔慰金等に係る個人情報の流れ

（資料49－1）

住民

来庁

郵送

電子申請

①本人、代理人又は遺族が申請する（紙又はデータ・窓口、郵送、電子）

⑥不備返戻・再提出

⑦災害弔慰金の支給・却下

新宿区

②申請書を確認

イントラ端末

【LGWAN】

通信暗号化

被災者生活再建支援システム

③被災者台帳システムで罹災状況の確認、経過を記録

⑤災害弔慰金等の支給を審査

- 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

【LGWAN】

通信暗号化

④個人情報の閲覧・確認（戸籍情報、障害者手帳情報、介護保険情報、課税情報、公金受取口座情報）

地方公共団体情報システム機構（Ｊ－LIS）

自治体中間サーバー

- 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

（資料49－2）

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。