資料45

個人情報保護管理運営会議　付議事項

件名	個別避難計画（災害時要援護者名簿）作成支援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（外部結合、業務委託）

（担当部課：福祉部地域福祉課）

事業の概要

事業名	個別避難計画（災害時要援護者名簿）作成支援業務委託
担当課	福祉部地域福祉課
目　的	本人又は家族のみでは要援護者名簿登録及び個別避難計画作成の申出を行うことが困難な方に対し、福祉サービス事業者による申出の支援を実施することで、要配慮者の要援護者名簿登録及び個別避難計画作成を促進し、災害時の避難支援体制の充実を図る。
対象者	以下のいずれかの要件を満たし、委託先事業所が提供する福祉サービスを利用している者で、自身又は家族等のみでは申請が困難な方。 ・要介護３以上 ・身体障害者手帳２級以上 ・愛の手帳２度以上 ・その他、災害時の避難等に支援を必要とする方
事業内容	１　概要 現在、区では、災害時に支援を必要とする方を対象として、本人又は家族等からの申出により、「災害時要援護者名簿」の登録を行っている。令和８年度より、災害時要援護者名簿登録者に対して、避難先や避難時に必要な支援の内容、支援者の連絡先等を記載した「個別避難計画書」を作成し、本人に交付する事業を開始した。 個別避難計画は本人又は家族による申請を基本としているが、配慮が必要な方の中には、本人または家族だけでは、必要となる情報の整理や申請手続が困難な方が存在すると見込まれる。一方で、区の保有する情報では、そのような状況にある方を捕捉することは困難である。 このため、居宅介護支援事業所や特定相談支援事業所に委託し、各事業所の利用者のうち、個別避難計画を希望するが、本人又は家族による申出が困難な方を対象として、制度説明、面談、申出内容整理及び代理申出支援を実施する。 ２　個人情報保護管理運営会議への付議内容 （１）外部結合 個別避難計画（災害時要援護者名簿）の申出書提出及び委託先からの業務完了報告を受け付けるため、ＬｏＧｏフォームに外部結合を行う。 （２）業務委託 個別避難計画（災害時要援護者名簿）の申出書の提出にあたり、本人又は家族による申出が困難な方への申出内容の整理や代理申出支援業務を委託する。 ３　対象者数 250 人 ※個人情報の流れは、資料４５－１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　個別避難計画作成支援に係る外部結合について

保有課（担当課）	地域福祉課
登録業務の名称	個別避難計画（災害時要援護者名簿）の作成
結合される情報項目（だれの、どのような項目か）	・申出者の氏名、住所 ・登録者の氏名、住所、性別、電話番号、生年月日、町会名、登録区分、特出名、 避難先 ・緊急連絡先の氏名、住所、性別、電話番号、登録者との関係、本人状況 ・避難支援等実施者の氏名、住所、電話番号
結合の相手方	株式会社トラストバンク
結合する理由	当該電子申請サービスは、東京都及び都内の自治体が共同調達・利用することで高品質なサービスの廉価な提供を実現しているため。また、同サービスを活用することで、申請者は窓口に来庁することなく、２４時間申請手続が可能となり、区民の利便性向上を図ることができるため。
結合の形態	LGWAN 回線を利用して、当該電子申請サービスの提供がされるクラウドサーバと区のイントラネット端末を接続する。
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

別紙(業務委託)

◇業務委託(第３条第１項第３号)

件名　個別避難計画作成支援に係る業務委託について

保有課(担当課)	地域福祉課
登録業務の名称	個別避難計画（災害時要援護者名簿）の作成
委託先	以下の事業者のうち区と契約を締結した事業者 ・居宅介護支援事業所 ・特定相談支援事業所 ・その他区長が認める事業所
委託に伴い事業者に処理させる情報項目（だれの、どのような項目か)	・申出者の氏名、住所 ・登録者の氏名、住所、性別、電話番号、生年月日、町会名、登録区分、特出名、 避難先 ・緊急連絡先の氏名、住所、性別、電話番号、登録者との関係、本人状況 ・避難支援等実施者の氏名、住所、電話番号
処理させる情報項目の記録媒体	紙及び電磁記録媒体（委託先PC)
委託理由	本人又は家族のみでは必要となる情報の整理や申出手続が困難な者について、日常的に本人の状況を把握している福祉サービス事業者の専門的知見を活用し、円滑な申出を支援し、要配慮者の防災力向上を図るため。
委託の内容	・制度説明及び同意書の取得 ・面談及び電話相談（緊急連絡先等への連絡調整含む) ・要援護者名簿登録申出の内容整理 ・個別避難計画記載事項の聞き取り及び整理 ・代理申出（※原則、電子申請により実施) ・作成支援結果の報告（同意書の提出を含む)
委託の開始時期及び期限	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、同様の業務委託を行う。）
委託にあたり区が行う情報保護対策	別紙チェックリストのとおり
受託事業者に行わせる情報保護対策	別紙チェックリストのとおり

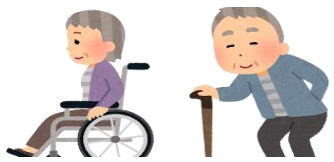
個別避難計画（災害時要援護者名簿）作成支援業務に係る個人情報の流れ

（資料４５－１）

対象者（委託先事業所のサービス利用者）

①委託先から対象者へ説明







②個別避難計画の申出書作成における同意書の提出（紙）

※個人情報を委託先業者が取り扱うことについての本人の同意

④個別避難計画の申出書への記入内容確認（電話・対面）

⑨個別避難計画書の送付（郵送）

委託先

③同意書の保管



⑤個別避難計画の申出書作成



特記事項等の遵守
・立入調査等及び状況報告（再委託を含む）
・責任者及び取扱者の報告
・データを暗号化
・区が作成した業務フローに基づく業務の履行
・鍵付キャビネット等での保管
・事故等への対応体制及び手順の整備
・事故発生時等の協議

⑥個別避難計画の申出書及び同意書提出

【インターネット回線】 LoGoフォーム 【LGWAN回線】

⑩業務完了・廃棄報告

【インターネット回線】 LoGoフォーム 【LGWAN回線】

・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

新宿区（地域福祉課）

災害時要援護者名簿システム



⑦申出書を基に災害時要援護者名簿を作成

対象者データ

氏名、住所、性別、電話番号、生年月日、避難先等

⑧個別避難計画書の出力



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。

5　業務委託にかかる個人情報保護対策チェックリスト

（電磁的媒体・紙媒体の取扱い）

	・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
委託にあたり区が行う情報保護対策【運用上の対策】	○	契約にあたり、「特記事項」を付すとともに、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。
	○	契約履行の間、特記事項に基づき立入り調査等を実施するとともに、委託先に対し速やかに状況報告をするよう指導する。
	○	再委託先がある場合には、委託先との間に立入り調査等ができる契約内容を付すとともに、必要に応じて又は定期的に立入り調査等を実施するよう指導する。
	○	取扱責任者及び取扱者をあらかじめ指定し、区に報告するよう指導する。
	○	全体の業務フローを作成し、委託先と共有する。
	○	取扱う個人情報の管理について、必要に応じて又は定期的に確認する体制を構築するよう指導する。
	○	個人情報を含むデータを作成する必要が生じた場合は、パスワードを付してデータを暗号化する。また、電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用して、手渡しで行うよう指導する。
	ー（電子データのみの取扱いのため）	個人情報を手交する場合は、鍵付きカバン等を使用して運搬する。
	ー（電子データのみの取扱いのため）	個人情報の受渡しにあたっては、管理簿に記載する。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにする。
	ー（電子データのみの取扱いのため）	個人情報は、施錠できる金庫又はキャビネット等に保管する。
	○	業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却し、電子データは消去するよう指導する。また、区に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、委託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、直ちに委託先と今後の対応を協議する。
委託にあたり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。

5　業務委託にかかる個人情報保護対策チェックリスト

（電磁的媒体・紙媒体の取扱い）

	・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
委託事業者に行わせる情報保護対策【運用上の対策】	○	契約にあたり、「特記事項」を付すとともに、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。
	○	契約履行の間、特記事項に基づき立入り調査等を受けさせるとともに、委託先に対し速やかに状況報告をさせる。
		再委託先がある場合には、委託先との間に立入り調査等ができる契約内容を付すとともに、必要に応じて又は定期的に立入り調査等を実施させる。
	○	取扱責任者及び取扱者をあらかじめ指定させ、区に報告させる。
	○	区が作成した業務フローに基づき、業務を行わせる。
	○	取扱う個人情報の管理について、必要に応じて又は定期的に確認する体制を構築させる。
	○	個人情報を含むデータを作成する必要が生じた場合は、パスワードを付してデータを暗号化させる。電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用させ、手渡しで行わせる。
	ー（電子データのみの取扱いのため）	個人情報を手交する場合は、鍵付きカバン等を使用して運搬させる。
	ー（電子データのみの取扱いのため）	個人情報の受け渡しにあたっては、管理簿に記載させる。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにさせる。
	ー（電子データのみの取扱いのため）	個人情報は、施錠できる金庫又はキャビネット等に保管させる。
	○	業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却させ、電子データは消去させる。また、区に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。
委託事業者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。