

個人情報保護管理運営会議 付議事項

件 名	被災者生活再建支援システム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：危機管理担当部危機管理課）

事業の概要

事業名	被災者生活再建支援システムの更新及び住家被害認定調査モバイルシステムの導入
担当課	危機管理課
目的	災害発生時における効率的な住家被害認定調査の実施、当該調査の実施結果に基づく被災者情報の一元管理による迅速な「罹災証明書」の発行及び「罹災証明書」に基づく、都、区等の長期かつ多岐にわたる各種生活再建支援業務を公平かつ迅速に実施するため、被災者生活再建支援システムを更新する。 また、合わせて住家被害認定調査モバイルシステムを導入することで、ペーパーレス化を図るとともに、現地調査や判定に要する時間を大幅に短縮し、迅速な罹災証明書の発行につなげる。
対象者	1 新宿区民 2 新宿区民でない者のうち、災害発生後に新宿区から罹災証明書の交付を受け、被災者台帳に登録された者
業内容	1 概要 現在、区では、発災時迅速に罹災証明書を発行するため、「住家被害認定調査システム」、「罹災証明書発行システム」及び「被災者台帳システム」等の機能を備えた「被災者生活再建支援システム(C/S 版) (以下、「C/S 版」という。))」を導入し、罹災証明書の発行体制を構築している。 しかしながら、住民記録システムの標準化に伴い、令和7年1月以降、現行のC/S 版では住民基本台帳データの取り込みが困難となるほか、C/S 版のサポートも令和8年度に終了予定であることから、システムの更新も必要となる。 また、現行の住家被害認定調査システムでは、現地において紙の調査票にチェックした後、本庁に持参しスキャナで読み込む必要があるほか、現地写真を整理して別添するなど、作業工程が多く、罹災証明書の発行までに時間を要してしまう。 これらを踏まえ、より迅速に罹災証明書が発行できるよう、新たな被災者生活再建支援システムへ更新するとともに、住家被害認定調査モバイルシステムを導入することで、区民の利便性向上及び業務の効率化を図る。 2 個人情報保護管理運営会議への付議内容 (1) 外部結合 被災者生活再建支援システムの更新及びモバイルシステムの導入について、東日本電信電話株式会社 (NTT 東日本) のシステム利用にあたって外部結合を行う。 (2) 業務委託 システムの運用・保守について、専門ノウハウを有する事業者へ委託する。 3 対象者数 約28,000人 (推定) ※個人情報の流れは、資料30-1のとおり

件名 被災者生活再建支援システムに係る外部結合について

保有課(担当課)	危機管理課
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 個人の範囲 新宿区民全員及び 新宿区民でない者のうち、災害発生後に新宿区から罹災証明書の交付を受け、被災者台帳に登録された者 2 記録項目 資料30-2のとおり
結合の相手方	東日本電信電話株式会社(I SMS 認証取得済)
結合する理由	より迅速に罹災証明書が発行できるよう、新たな被災者生活再建支援システムへ更新するとともに、住家被害認定調査モバイルシステムを導入することで、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、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1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

件名 被災者生活再建支援システムに係る運用支援・保守業務の委託について

保有課(担当課)	危機管理課
登録業務の名称	被災者生活再建支援システムの管理
委託先	東日本電信電話株式会社（I SMS 認証取得済）
委託に伴い事業者処理させる情報項目（だれの、どのような項目か）	1 個人の範囲 新宿区民全員及び 新宿区民でない者のうち、災害発生後に新宿区から罹災証明書の交付を受け、被災者台帳に登録された者 2 記録項目 資料30-2のとおり
処理させる情報項目の記録媒体	電磁的媒体（被災者生活再建支援システム及びモバイルシステム）
委託理由	本システムの運用、保守にあたっては、区職員が直接行うよりも専門ノウハウを有する事業者が行うほうがよりの確かつ効率的に行うことができる。 また、本当該システムの運用支援や保守は、開発事業者である上記委託先に行わせることが最も効率的であるため。
委託の内容	(1) システム運用支援 (2) システム保守
委託の開始時期及び期限	令和7年2月1日から（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

被災生活再建支援システムに係る個人情報の流れ

(資料 3 0 - 1)

罹災証明書申請者

窓口、パソコン、
スマートフォン等で申請

【申請者端末】



【インターネット回線】

通信暗号化

①罹災証明書の申請
(紙又は電子申請)

③住家被害認定
調査の実施

調査用
タブレット
端末

- ・特記事項等の遵守
- ・立入調査等及び状況報告
- ・責任者及び取扱者の報告
- ・区が作成した業務フローに基づく業務の履行
- ・データの暗号化
- ・個人情報の返却及び消去
- ・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

⑩罹災証明書の交付

新宿区

②申請者の受付

【住家被害認定調査
モバイルシステム】

【インターネット回線】

通信暗号化

クラウドサーバ環境

調査用
タブレット
端末

専用PC
(管理者用)

④調査結果の
ダウンロード

⑤USBメモリで
データ移行

暗号化機能付きUSBメモリ
を利用し、管理簿に記載

【区イントラネットパソコン】

個人情報の項目については、
資料 3 0 - 2 のとおり

⑨罹災証明書の発行

- ・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
- ・インターネットからの分離
- ・区イントラPCと独立した環境
- ・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

- ・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

被災者生活再建 支援システム

- ・罹災証明書発行システム
- ・住家被害認定調査システム
- ・被災者台帳システム

個人情報の項目については、
資料 3 0 - 2 のとおり

⑦内容等を審査し、
罹災状況を判定

【LGWAN回線】

⑥調査結果の
インポート

⑧罹災証明書情報を
ダウンロード

(1) 被災者生活再建支援システム

① 住民基本台帳データのうち、次に掲げる情報項目

住民番号、世帯番号、住民区分、消除フラグ、氏名、フリガナ、通称、通称フリガナ、併記名、併記名フリガナ、世帯主氏名、世帯主フリガナ、住所、方書、従前の住所、前住所方書、転出先の住所、転出先方書、戸籍の表示、性別、生年月日、続柄、住民基本台帳法第 30 条の 45 による区分（住民基本台帳の記載対象となる外国人の区分）、在留資格コード、住民票記載住民年月日、異動事由コード、異動年月日、異動届出年月日

② 固定資産税関連情報のうち、次に掲げる項目

(ア) 一般家屋ファイル及び区分所有家屋ファイルに係る情報項目

事務所コード、町名、丁目コード、地番コード、号コード、先コード、一棟コード本棟、一棟コード枝棟、物件番号、物件明細一棟コード本棟、物件明細一棟コード枝棟、主符棟コード、所在番号(街区番号)、所在番号(住居番号)、所在番号(枝番)、建物番号、家屋番号、所有者漢字氏名、所有者漢字都道府県名、所有者漢字区市郡名、所有者漢字住所、所有者漢字片書、所有者共有者数、登記種類用途コード、登記構造コード、登記屋根コード、登記地上階建、登記地下階建、登記居住階(自)、登記居住階(至)、登記床面積

(イ) 共有者ファイル

事務所コード、町名、丁目コード、地番コード、号コード、先コード、一棟コード本棟、一棟コード枝棟、物件番号、共有者番号、共有者漢字氏名、共有者漢字都道府県名、共有者漢字区市郡名、共有者漢字住所、共有者漢字方書き、共有者持分分母、共有者持分分子

(ウ) 登記種類用途コード、登記構造コード、登記屋根コード

③ 住家のり災状況(り災家屋等の所在地、り災家屋等の種別、り災の程度)

④ 建物被害認定調査の結果内容(住家の被害程度、見取図、現場写真)

⑤ 生活再建支援業務の実施状況(支援事業名、支援対象者、支援内容、支援状況)

(2) 住家被害認定調査モバイルシステム

氏名、住所、電話番号、物件番号、建物の位置情報、住宅等の写真

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「－」	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。
	○	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。
	○	個人情報を含むデータを作成する必要がある場合は、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。
	－ (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。
	－ (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。
	－ (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。
委託にあたり区が行う 情報保護対策 【システム上の対策】	○	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。
	○	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「－」	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。
	○	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。
	○	個人情報を含むデータを作成する必要がある場合は、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。
	－ (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。
	－ (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。
	－ (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。
委託事業者に行わせる 情報保護対策 【システム上の対策】	○	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。
	○	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。