

平成28年2月15日

第72回 神戸市個人情報保護審議会

災害情報等集約システムの導入について

(建設局)

神建防防 第 1399 号

平成 28 年 2 月 15 日

神戸市個人情報保護審議会 会 長 様

神戸市長 久 元 喜



諮問

神戸市個人情報保護条例第 11 条第 1 項の規定に基づき、下記の事項について貴会の意見を求めます。

記

災害情報等集約システムの導入について
(条例第 11 条「電子計算機処理の制限」に関して)

担当：建設局防災部防災課

災害情報等集約システムの導入について
(条例第 11 条「電子計算機処理の制限」に関して)

【通報者情報】

- ・ 氏名
- ・ 住所
- ・ 電話番号
- ・ FAX 番号
- ・ 通報内容

災害情報等集約システムの導入について

1 概要

建設局では、災害発生時など有事の際に本庁と建設事務所及び水環境センターの情報交換は主に FAX 等を利用しており、迅速に情報共有できる仕組みが必要となっている。

また、建設事務所では、道路など管理する施設に破損等の通報があった場合に、現在は紙媒体による記録を行い、その後処理方針、処理結果を追記し、紙媒体で保存するなど、一連の事務処理は電算システムを使用せずに行っている。一方で、処理件数が平常時の通報として年間 2 万件弱（6 建設事務所）に達しており、処理そのものの迅速化や、データベース化による情報の整理が課題となっている。

以上のことから、迅速な事務処理を図るため、災害情報等集約システムを導入する。今回は現場事務所（6 建設事務所と 3 水環境センター）のうち、2 事務所（東部建設事務所、垂水建設事務所）で導入する。

2. 事務の内容

（1）システムの概要

道路、公園、下水道等に不具合が生じて市民から電話等により通報があった場合に、建設局の現場事務所において、通報者情報や通報内容、処理方針や処理結果をパソコンからサーバーにデータ入力する。職員が通報に基づいて現場を確認する際にタブレット端末の GPS 機能を使って写真とともに位置情報を取得し、コメントと合わせてデータをサーバーに送る。送信されたデータは GIS により地図に表示させたり、各種の集計が可能である。

また、建設局職員が自ら不具合を発見し、スマートフォンを使ってサーバーにデータを送る機能も有する。

なお、使用する端末について、パソコン、タブレットはデータの読み書きが可能、スマートフォンはデータ送信のみ可能である。

（2）諮問対象の事務

① 市民からの通報受付

建設の現場事務所の職員が市民から苦情、要望や災害時の被害情報を受け付ける。その際、通報者の基本情報も入手する。

② 情報収集の内容

通報者の氏名、住所、電話番号、FAX 番号、通報内容

③ 情報の入力・保管

通報者に関する情報は、建設局の現場事務所の職員がサーバーにアクセスし、収集し

た内容を入力フォームへ入力して登録する。

また、その後通報に対する処理結果についても、同様に入力して登録する。

3 効果

- (1) 災害時において、現場で登録された情報を即座に本庁で確認することができるため、情報収集の迅速化が図られ、被害情報や通行止め情報を市民にお知らせする時間の短縮が可能となる。
- (2) 平時においては、事務処理の進捗状況をシステムで管理することで、事務処理の遅延防止等のチェックがしやすくなり、よりスピーディな対応を図ることで可能となる。
- (3) システム化によりデータ集積が図られ、過去の情報を確認する場合に容易に検索することができ、事務の簡素化によって市民サービスの向上につながる。

4 スケジュール

平成 28 年 2 月中旬 ・個人情報保護審議会
下旬 ・システム運用開始

5 登録見込み件数（1 事務所あたり）

災害時 100~200 件程度（台風によって豪雨災害が発生した場合等）
平常時 約 3,000 件／年

6 個人情報の取扱いについて

「神戸市個人情報保護条例」、「電子計算機処理に係るデータ保護管理規程」、「神戸市情報セキュリティポリシー」に基づき、厳格に対処する。

(1) システム上の保護

- ① 個人情報にかかるデータについては端末機には保存せず、サーバーで一括管理する。
- ② 端末機（スマートフォンを含む）の操作にあたっては、個人ごとに ID 及びパスワードによる認証を行い、関係職員に限定する。また、使用する端末を限定する。
- ③ 端末と外部サーバーのデータセンターとの通信は、通信事業者が提供している閉域 IP ネットワーク網を利用して外部等からの不正アクセス行為を受けることを防止する。
- ④ ウイルス対策ソフトウェアを導入し、常に最新のセキュリティ状態で運用する。

(2) 運用上の保護

- ① 外部サーバーの建物は常駐警備による入退室管理を 24 時間 365 日実施する。
- ② 3 段階以上 (ID カード、生体認証、パスワード入力) のセキュリティを有し、生体認証による個人レベルでの認証システムの導入、または有人警備によるセキュリティを施す。
- ③ 監視カメラによる記録を最低 1 か月間保存し、委託先で速やかに画像閲覧できる状態を確保する。
- ④ サーバーのラックは個別施錠を実施する。
- ⑤ サーバーで管理している個人情報は、使用目的を達した時点 (原則 5 年) で確実に削除する。
- ⑥ 保存年限を経過した帳票は、シュレッダーや焼却処分など確実かつ速やかに廃棄する。
- ⑦ 個人情報の適切な取り扱いを確保するために、関係職員に対して、必要な研修及び指導を行うとともに、個人情報の適正管理について点検を行う。
- ⑧ システム構築を請け負う事業者選定の際には、事業者との契約における個人情報保護等に係る特記事項により、個人情報の適切な取り扱いを徹底する。

災害情報等集約システムの構成イメージ

