船橋市災害情報共有システム導入業務仕様書

1. 適用範囲

本仕様書は、船橋市（以下「発注者」という。）が実施する「船橋市災害情報共有システム導入業務」（以下「本業務」という。）に適用し、本業務の受注者（以下「受注者」という。）が実施する業務内容を定めるものである。

2. 目的

激甚化する災害に対して適切な対応を行うためには、被害の発生状況、避難所の状況等の必要な情報を正確かつ迅速に把握しつつ、全庁的に即時に情報を共有し、意思決定の効率を図るとともに、市民に対して被害状況や重要情報を正確かつ迅速に伝達する必要がある。

そのため、災害時の情報把握・管理・伝達の機能を有するクラウド型の災害情報共有システム及び防災ポータルサイト（以下、「本システム」という。）を導入し、市の災害対応の強化及び効率化を図り、市民にとって安心して暮らせる地域づくりに寄与することを目的とする。

3. 準拠する法令・指針等

本業務の実施にあたっては、本仕様書によるほか次の法令等に準拠して行うものとする。

⑴ 災害対策基本法
⑵ 個人情報の保護に関する法律
⑶ 船橋市地域防災計画
⑷ 避難情報に関するガイドライン（内閣府（防災担当））
⑸ 船橋市情報セキュリティ基本方針
⑹ 船橋市情報セキュリティ対策基準
⑺ 船橋市個人情報の保護に関する法律施行条例
⑻ その他関係法令、通達等

4. 委託期間

本業務の委託期間は、契約締結日から、令和 8 年 10 月 31 日までとする。
なお、運用保守にかかる契約期間は令和 8 年 11 月 1 日から令和 9 年 3 月 31 日までとする。

5. 提出書類

受注者は、着手後及び完了後、速やかに次の書類を提出することとする。

⑴ 業務着手届
⑵ 業務実施計画書
⑶ 業務主任技術者選任届
⑷ 個人情報管理者届
⑸ その他発注者が必要とする書類

6. 貸与資料及び返却

本業務を実施する上で必要な資料は発注者が受注者に貸与するものとし、貸与された資料は責任をもって保管し、紛失・汚損等を生じないよう取扱いに十分注意するとともに、本業務目的以外に使用しないこと。本業務終了後は速やかに返却又は廃棄処分を行うものとする。

7. 業務概要

本業務の内容は次のとおりとする。

⑴ 計画準備
⑵ データ等収集・整理
⑶ システム環境構築及び設定業務
⑷ 動作確認・操作研修の実施

8. 計画準備

受注者は業務実施計画立案にあたり、一連の業務が円滑に実施されるよう業務手順・人員配置計画等について十分考慮しなければならない。

なお、受注者は契約締結後 10 開庁日以内に、以下の事項を記載した業務実施計画書を発注者に提出し、承認を得ること。

⑴ 業務概要
⑵ 導入作業手順(発注者が対応する必要がある作業内容を含む)
⑶ 導入スケジュール及び体制
⑷ 成果品
⑸ その他必要な事項

9. データ等収集・整理

本業務を進めるにあたって、必要なデータ等を整理するとともに、発注者から提供する必要のあるデータがある場合には、受注者は発注者に請求することができる。

10. システム概要

本仕様書の本システムは、市の災害対応業務に必要となる「災害情報共有システム」と「防災ポータルサイト」の2つの機能システムを総称するシステムをいい、それぞれ以下の機能を有するものとする。なお、各システムの詳細な要件については「12. 機能要件」及び「13. 非機能要件」に記載する。

⑴ 災害情報共有システム

被害情報や対応進捗状況及び避難所開設情報等を収集・一元管理し、各情報を災害対策本部内で即時に共有することで、災害対策本部における意思決定を支援するシステムである。なお、各情報は地図上での登録及び管理が可能で、被害状況等を可視化することにより、被害全体の状況把握を支援する。

⑵ 防災ポータルサイト

平時及び災害時において市民向けの防災専用ホームページとして機能するものであり、被害

状況や避難等に関する市からの重要情報・気象情報等を集約して配信・掲載することで、市民が自ら生命を守る行動につなげることを支援するシステムである。

11. 基本要件

受注者が提供する本システムは、以下のサービス要件を満たすこととする。

⑴ インターネット回線で利用できること。

⑵ 特別なアプリケーション等のインストールを必要とせず、Web ブラウザもしくはアプリ方式により利用できるシステムであること。

⑶ 職員端末（PC）、携帯端末（タブレット・スマートフォン）で利用できること。

なお、職員端末は以下の環境とする。

OS：Windows11　ブラウザ：Microsoft Edge、Google Chrome

※内部ネットワークとインターネットを分離しており、セキュアコンテナ（ローカル環境とは独立した仮想的な環境）内のブラウザ（Microsoft Edge（IE モード使用不可）、Google Chrome）を使用してインターネットへ接続しているため、上記インターネット接続環境にてアクセスできる環境を用意すること。

⑷ 同一サービスにおいて都道府県もしくは市区町村で複数の導入実績を有すること。

⑸ 本システムは、原則として 24 時間 365 日システム稼働を可能とすること（メンテナンス等による計画的停止時間を除く）。

12. 機能要件

本システムに求める機能要件は以下のとおりとする。

⑴ 共通機能要件

① 視認性・操作性に優れたシステムであること。

② スマートフォン・タブレット等の携帯端末に最適化した閲覧・登録画面を有すること。

③ システムへのログインは、ID 及びパスワード認証を必要とすること。

④ 1つの ID アカウントにおいてシステムへの同時ログイン及び操作ができること。

⑤ 基本的な情報は Excel もしくは CSV ファイルにて一覧で出力できること。

⑵ 災害情報共有システム機能要件

機能	条件
災害名管理	災害名管理等の基本機能を有すること。
本部設置機能	災害ごとに体制管理ができ、各部局の配備体制状況を管理できること。
避難情報管理	避難情報の発令対象区域に対して発令・解除を登録・管理できること。発令種別・発令解除理由・発令解除日時・発令区域・対象世帯数・対象人数等を一覧表示できること。
避難所情報管理	避難所の開設・閉鎖状況、避難者・世帯数を登録・管理できること。
被害情報管理	住民からの通報及び職員・関係機関から報告された被害情報を集約・共有できること。被害情報の内容登録後に当該被害情報に対する対応を対象の所属に対して指示でき、その後の対応状況についても登録・管理ができること。

GIS 管理	被害情報や避難所情報等を地図上で登録及び管理できること。登録した情報は地図上で被害種別・対応状況等をアイコンや色等で視覚的に識別できること。電子地図は定期的に最新化が図れること。
レポート・報告書機能	消防庁の報告様式に準じて被害情報の数値情報をとりまとめできること。また、二次加工可能なファイル形式(Excel 等)で出力できること。
データ出力	避難所情報やクロノロジー一覧について、二次加工可能なファイル形式(Excel 等)で出力できること。
モバイル	携帯端末等を使用して、災害現場や避難所等からクロノロジー・避難所情報の登録・閲覧等が行えること。
ダッシュボード	市の災害概況が数値やグラフ等により可視化されていること。
外部システム連携	千葉県防災情報システムと連携し、被害状況、避難所開設状況、避難情報等について報告が可能なこと。

⑶ 防災ポータルサイト機能要件

機能	条件
防災情報の配信	災害情報共有システムと連動して、住民向けの防災情報(避難所情報・避難情報等)を配信できること。
情報の地図化	地図上に避難情報・避難所情報等のレイヤーを表示できること。
リンク集の公開	災害時に備えるべき情報や関係機関のサイト URL を掲載すること。

13. 非機能要件

⑴ 規模要件

利用可能な ID は 100ID とすること。

⑵ 性能要件

システムへの発災時の急激な同時アクセス増加にもレスポンス性能が低下することなく安定して使用可能なサービスであること。

概要	前提条件
システム利用時のレスポンス性能	3.0 秒以内
住民からの防災専用ホームページへのピーク時の同時アクセス数	1,000,000 件/時間

⑶ 操作性要件

項目	要求事項
地図操作	マウス操作(クリック・スクロール)にて地点移動等が可能であること。画面の縮尺に応じて適切な粒度の情報が表示できること。
入力操作	入力はリスト選択・チェックボックス・テンプレート等の活用により、キーボード入力の回数を最小限に抑えること。必須項目の入力は必要最小限で構成し、追加入力及び修正に対応していること。
モバイル操作	PC だけでなくタブレット・スマートフォンなどのモバイル端末にも最適化された画面が表示されること。

⑷ データセンター要件

① 日本データセンター協会（JDCC）が定める「データセンターファシリティスタンダード」の基準項目ティア 3 相当以上のデータセンターであること

② 耐火性を備えた設備を備えていること。

③ システム停止等の障害発生時には即座に故障対応可能な体制が整備されていること。

④ 電源は、停電時でも継続稼働できるよう自家発電設備等を設置していること。

⑤ 入退室管理は生体認証や IC カード等による入退室管理がなされていること。

⑥ 十分な帯域をもつ回線を備えていること。

⑦ サーバの正常な動作に必要な空調システムを設置していること。

⑧ データセンターは本市と同時に被災しないよう複数地域に設置されていること。

⑸ 信頼性要件及び継続性要件

① システム障害等を起因とした機能不全を回避するため、稼働環境はサーバ・ネットワーク機器等の冗長構成を採用し、単一障害によるシステム停止が発生しない構成とすること。

② システムの年間稼働率は受注者の責任分界点範囲において 99.9%以上とすること（発注者が承諾したメンテナンス等による停止及びインターネット通信回線等の受注者が直接関与しないインフラ障害による停止は除く）。

③定期的なオンラインバックアップを取得し、データ保全を行い、障害時にはバックアップデータからのデータ復旧が可能であること。

⑹ セキュリティ要件

① 別表「クラウドサービス選定基準」に定める要件を満たすこと。

② システムへのログインはユーザ ID 及びパスワードの組み合わせ、もしくは同等以上の仕組みによって実施すること。

③ ユーザ権限の設定により、付与された権限の範囲のみ操作できるように不正なアクセス等からデータ保護を図ること。

④ パスワードポリシーの設定及びパスワードを変更できる仕組みを有すること。なお、パスワード設定については、以下の要件を含めることが可能なこと。

長さ：10文字以上

複雑さ: 英大文字、英小文字、記号及び数字をすべて含める

⑤ ファイアウォール等により外部からの不正アクセスを遮断すること。

⑥ サーバ・クライアント間の通信を暗号化し情報漏洩対策を実施すること。取り扱う情報の機密性に応じ、適切な暗号アルゴリズムを用いた暗号化処理を行うこと。

⑦ 常に最新のウィルス対策ソフトウェアによるリアルタイム監視と定期的なウィルス感染チェックを行うこと。

⑧ システムログとして、ID 毎のログイン情報を 5 年以上保管すること。

⑨ 発注者からの要求時に、システムログ等の取得・開示または潜在的な不正使用の有無を識別する報告を提供できること。

14. 導入要件

⑴ 発注者が円滑に対応できるよう、受注者は必要なツール（各種設定シートひな形等）を作成し発注者へ提供すること。

⑵ 外部連携に必要な設定作業は受注者が実施すること。

⑶ 管理者ユーザのアカウントの初期設定については受注者が行うこと。

⑷ 本番稼働開始日は令和 8 年 11 月 1 日とし、本番稼働前 3 週間程度を試行運用期間とする。なお、試行運用期間中のシステム利用料は本業務に含むものとする。

15. 動作確認要件

受注者は、地図情報・連携先の設定内容等が問題なく反映されているかどうか、以下の観点で動作確認を行うこと。なお、発注者がマスタデータを整備しシステムへ取込登録した情報項目については発注者が動作確認を行う。

⑴ アカウント情報、避難所情報等の設定内容が問題なく反映されていること

⑵ 外部情報が問題なく受信できること

⑶ 外部システムへの連携が問題なく実施できること

⑷ 背景地図が問題なく表示されること

16. 操作研修

受注者は、運用開始に際して、1回以上、管理者及び利用者向けの操作研修を実施すること。

⑴ 受注者は操作研修資料及び操作研修実施計画書を作成し、発注者へ提供すること。

⑵ 研修は市役所内の会場で実施することとし、研修会場・端末・電源等は発注者が準備する。

⑶ 研修資料は受注者が準備し、電子データおよび紙資料にて納品すること。

17. 納品物（提出書類及び成果品）

納品物は、原則として A4 判（必要に応じて A3 判）、日本語で記載すること。なお、電子データにより提出する場合には CD-ROM 又は DVD によること。

⑴ 業務実施計画書：契約締結後 10 開庁日以内に提出すること。

⑵ ライセンス証書：受注者が提案するソフトウェアの使用許諾を記載したライセンス証書（必要に応じて）。

⑶ 操作マニュアル（管理者用・利用者用）：システムを利用した業務を遂行する上での操作手順や機能を示した説明書。※電子データで提出すること。

⑷ 研修資料：紙資料（研修参加者数分）及び電子データ

⑸会議関連資料：キックオフ会議資料等、本業務の遂行に伴い作成した資料。会議終了後 10 開庁日以内に提出すること。

⑹ システム設定に係るドキュメント類

⑺ 問い合わせ窓口情報に関する通知書

⑻ 業務報告書：本業務の作業内容及び成果内容、業務に付随する資料、打合せ記録簿等をとりまとめるものとする。

⑼ その他発注者が指示する書類

18. 打合せ協議

受注者は、本業務の内容について発注者と打合せ協議を行うこと。履行期間中においても、進捗状況をメール等の記録に残る方法で報告すること。また、発注者が作業の進捗状況・作業手法等に関して必要と認めた場合は、打合せ協議を行うこととする。

19. 成果品の帰属

本業務で履行した内容（ドキュメント・データ等）は、受注者又は第三者が従前から著作権を有している場合を除き、すべて発注者に帰属するものとする。受注者は、成果品又は収集した資料を発注者の承諾なく他に公表し、貸与又は使用させてはならない。

20. 費用負担

本業務で構築したシステムにおける地図利用にかかる版権・複製使用料については、受注者の負担とする。また、本業務の実施において関係公署への事務手続きが必要となった場合には、発注者と受注者の協議のうえ受注者が実施し、費用は受注者の負担とする。

21. 機密保持及び情報セキュリティの確保

⑴ 受注者は、委託業務に関連して知り得た船橋市の機密に関する事項及び個人情報に関する事項については、「個人情報の保護に関する法律」、「船橋市個人情報の保護に関する法律施行条例」、「船橋市情報セキュリティ基本方針」及び「船橋市情報セキュリティ対策基準」等に基づいて適切に管理し、契約期間中はもとより、契約期間後も第三者に漏洩してはならない。

⑵ 受注者は、発注者の許可なく業務実施場所から個人情報等（機密情報を含む）の情報資産を持ち出してはならない。

⑶ 個人情報等の情報資産の授受は、発注者の指定する方法により、発注者の指定する職員と受注者の指定する者の間で行うものとする。

⑷ 本システムの開発においては、技術的対策はもとより、防犯対策・入退室管理等の物理的対策、規定や情報取扱い手順の遵守徹底等の人的対策をあわせて行い、網羅的な情報セキュリティ対策を導入すること。

⑸ 受注者は、受注業務の全部又は主たる部分を第三者に委託してはならない。ただし、あらかじめ業務実施計画書等で発注者の承諾を得た関係事業者については、業務遂行に必要な範囲においてこの限りではない。

22. 検査

受注者は本業務を完了した場合には、速やかに完了検査を受けるものとする。完了検査において発注者より修正指示があった場合は、直ちに修正等を行い、再検査を受けるものとする。

23. 成果品の契約不適合

受注者は、成果品の受入検査合格日から6ヶ月以内に検査によっては発見し得ない成果品の不具合を発注者から通知された場合、成果品を修正又は交換するものとする。受注者は発注者の指示に従い、必要な補足・修正処理を、業務委託料を上限とし受注者の負担において行うこととする。業務遂行中に生じた事故等に対して一切の責任を負い、内容及び状況を発注者に報告し

指示に従うものとする。

24. 支払い

発注者はすべての成果品を確認し、検査終了後、適法な支払請求を受けた日から 30 日以内に代金を支払うものとする。

25. 運用・保守

本業務完了後の本システムの運用及び保守については、本業務とは別に契約するものとするが、以下の要件を満たす運用保守サービスを提供すること。

⑴ 問合せ対応：本システムに関する問い合わせの窓口として代表電話番号及びメールアドレスを用意し、平日業務時間帯（9:00～18:00）に受付けること（土日・祝祭日・年末年始休業期間を除く）。また、システムサポート窓口には本市の災害時のシステム運用方法や体制等の事情を把握している担当者を設けること。

⑵ 障害受付及び復旧：24 時間 365 日、障害発生時の電話による連絡受付窓口を設けること。障害発生時は原因の一次切り分け・利用者影響の確認を行い、発注者へ速やかに状況を報告すること。緊急を要する障害の場合、原則として問い合わせから 1 時間以内に発注者へ一次回答を行い、早期の復旧を図ること。

⑶ バージョンアップ対応：パッケージ機能の強化や法・制度改正に伴うバージョンアップを一律（追加費用なし）で実施すること。適用にあたっては発注者に対し、必要事項（改修内容・運用スケジュール等）を1か月前までに書面等により事前に説明すること。なお、この期限までに説明ができないやむを得ない理由がある場合はこの限りではない。

⑷ 稼働監視：サービスの稼働状況を常時監視し、問題発生時には速やかに事象検知する仕組みを構築すること。

⑸ 構成管理：システム構成等に変更又は追加が生じた場合は関連する操作マニュアルを更新すること。

⑹ 製品予防保守：導入するソフトウェア（OS・ミドルウェア・その他製品プログラム等）に不具合が公開された場合、又は製品サポート終了が発表された場合は、事象の影響を評価し、必要に応じたバージョンアップ又はパッチ適用を実施して安定した稼働環境を維持すること。セキュリティに関する重大な修正を含むパッチ等は、業務への影響を抑えつつできるだけ速やかに適用すること。

⑺ セキュリティ脆弱性対策：定期的に Web アプリケーションの脆弱性を診断・評価すること。

26. 疑義

本仕様書に定めのない事項、または疑義が生じた場合は、発注者及び受注者で協議のうえ取り決めを行い、受注者において協議記録を作成する。なお、協議記録は発注者の承認を得るものとする。

別表　クラウドサービス選定基準

No	区分	内容
1	クラウドサービス提供者の選定基準	日本の法令の範囲内で運用できるサービスであること。また、日本国内の裁判所を合意管轄裁判所とすること。
2	クラウドサービス提供者の選定基準	個人情報や住民の生命・財産に関わる情報、その他、非公開情報のデータが保存されるデータセンターは日本国内にあること。
3	クラウドサービス提供者の選定基準	利用するクラウドサービスのリージョンを日本国内に限定すること。
4	クラウドサービス提供者の選定基準	当該クラウドサービスの終了又は変更の際に1か月前までに書面等により事前に告知すること。
5	クラウドサービス提供者の選定基準	クラウドサービス提供者による情報資産の利用は、クラウドサービスの提供に必要な範囲で認めるものであり、それ以外の目的で本市の情報資産の利用は認めない。
6	クラウドサービス提供者の選定基準	クラウドサービスの開発及び運用が本市の意図しない変更が行われない一貫した品質保証体制の下でなされていること。意図しない変更とは非公開設定が説明なく、公開設定になることや本市が保存するデータが意図せず書き換えられること等を想定しており、機能追加等はこれに含まれない。
7	クラウドサービス提供者の選定基準	情報セキュリティインシデントが発生した際に、クラウドサービス提供者と連絡がつかない、営業時間外の対応が不可能等の状況にならないこと。また、情報セキュリティインシデントによる被害を最小限に食い止めるために情報セキュリティインシデント発生時に以下の対応を行うこと。 ①クラウドサービス提供者が情報セキュリティインシデントを検知した際は、速やかに本市に報告を行うこと。 ②情報セキュリティインシデントが発生した際に、運用状況・影響範囲調査等、事案解決のために積極的に調査を行うこと。 ③情報セキュリティインシデント発生後、遅くとも 1 時間以内に調査に着手すること。なお、情報セキュリティインシデントの疑いに対する連絡を受けた場合も同様に調査に着手すること。 ④当該事案の原因特定のため、各種システムログを取得すること。また、取得したログの分析に必要な情報を提供すること。 ⑤調査の結果、サービス停止等の措置が必要な場合は、市担当者に報告した上で速やかにその対応を行い、インシデント収束後、速やかに復旧を行うこと。 ⑥調査の結果、ファームウェア・ソフトウェア等のバージョンアップ等が必要となった場合は、速やかに対応すること。
8	クラウドサービス提供者の選定基準	再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されていること。

No	区分	内容
9	クラウドサービス提供者の選定基準	再委託先の情報セキュリティ対策の実施状況を確認するために次をはじめとした情報を本市に提供可能であること。 ・再委託先事業者情報 ・再委託内容 ・再委託先の情報セキュリティ責任者 ・再委託先の個人情報管理者 ・再委託先の従事者の情報　等
10	導入・構築時の対策（アクセス制御に関する事項）	クラウドサービスに影響を与える操作（サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除・利用の終了手順・バックアップ及び復旧等）について、誤操作を抑制するための手順書の作成や誤操作を認識可能なアラート等を実装する等の対策を行うこと。
11	導入・構築時の対策（アクセス制御に関する事項）	クラウドサービス上で構成される仮想マシンに対して適切なセキュリティ対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策、ログ取得等の実施）を行うこと。SaaS を利用する場合は、これらの対応が、クラウドサービス提供事業者側でされていること。
12	導入・構築時の対策（暗号化に関する事項）	取り扱う情報の機密性に応じた保護のための適切な暗号アルゴリズム（CRYPTREC により安全性及び実装性能が確認された「電子政府推奨暗号リスト」）を用いた暗号化処理（情報が保存されている場合、情報が通信され転送されている場合等フローに応じた暗号化）を行うこと。
13	導入・構築時の対策（設計・設定及び開発に関する事項）	クラウドサービス内において確実に時刻同期を行い、取得するログの時刻、タイムゾーンを統一すること。
14	運用・保守時の対策	パスワードなどの認証情報の割り当てがクラウドサービス提供者側で実施される場合、以下の管理手順が実施されること。 ・パスワードは、他者に知られないように管理しなければならない。 ・パスワードを秘密にし、パスワードの照会等には一切応じてはならない。 ・パスワードは十分な長さとし、文字列は想像しにくいもの（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）にしなければならない。 ・パスワードが流出したおそれがある場合には、速やかに報告し、パスワードを変更しなければならない。 ・サーバ、ネットワーク機器、パソコン及びモバイル端末等にパスワードを記憶させてはならない。
15	運用・保守時の対策	当該クラウドサービスに関連する脆弱性情報の提供を行うこと。また、クラウドサービス提供者の責任範囲で発生した脆弱性対応が迅速に行われること。
16	運用・保守時の対策	鍵管理機能をクラウドサービス提供者が提供するものを利用する場合、鍵の生成から廃棄に至るまでのライフサイクルにおける仕組みにリスク（鍵が窃取される可能性や鍵生成アルゴリズムの危殆化の可能性等）がないこと。

No	区分	内容
17	運用・保守時の対策	利用するクラウドサービスのネットワーク基盤が他の利用者のネットワークや通信と分離されていること及び利用するクラウドサービスの仮想マシンのネットワークが他の利用者のネットワークと分離されていること。SaaS の場合は、他の利用者が市のデータにアクセスできないよう確実な制御を行っていること。
18	更改・廃棄時の対策	クラウドサービスの利用終了時に、クラウドサービスで取り扱った業務に関わる全ての情報が、クラウドサービス基盤上から確実に削除可能であること。なお、削除する対象はバックアップ等により複製されたものにも及ぶ点に注意すること。削除にあたっては、情報資産を暗号化した鍵（暗号鍵）を削除するなどにより、復元困難な状態としなければならない。
19	更改・廃棄時の対策	クラウドサービスの基盤となる装置等の処分についてセキュリティを確保した対応が行われること。
20	更改・廃棄時の対策	クラウドサービスの利用終了時に、情報の廃棄の実施報告書を提出すること。
21	更改・廃棄時の対策	クラウドサービス利用者の各アカウント以外に特殊なアカウント（ストレージアカウントなど）がある場合は、関連情報（資格情報等）含めて廃棄可能であること。