

紀の川市
総合防災支援システム運用保守業務仕様書
(参考見積書積算用)

目 次

第1章	運用保守要件	3
第1条	職員研修要件	3
第2条	運用保守期間	3
第3条	運用保守範囲	4
第4条	運用保守業務の前提条件	4
第5条	運用支援業務の要件	4
第6条	緊急対応業務の要件	5
第7条	システム維持管理業務の要件	5

第1章 運用保守要件

本市の想定する令和7年度以降の運用保守要件は、以下のとおりとする。

なお、運用保守費用（5年間）については、審査に使用するものであり、保守管理契約の締結を保証するものではない。

第1条 職員研修要件

(ア)職員研修を実施する上で考慮すべき基本的な事項は、次のとおりとする。

No	要件
1	システムの操作手順を示した操作マニュアルを作成し、発注者の承認を得ること。 なお、管理者向け及び一般利用者向けをそれぞれ作成すること。
2	操作説明会等で利用する研修資料を作成し、発注者の承認を得ること。なお、管理者向け及び一般利用者向けをそれぞれ作成すること。
3	研修実施後、質疑応答内容について取りまとめた報告書を提出すること。
4	研修結果により改善が必要と判断された機能や操作マニュアル、研修資料について、改善を図ること。

(イ)研修対象及び内容等

研修対象の人数、研修対象者ごとの研修内容及び実施回数は、次のとおりとする。なお、すべての研修は庁舎内で行う。

No	対象者	人数	研修内容	回数
1	管理者	約5名	・システムの概要 ・操作方法（実機研修） ・運用管理方法 ・障害時の対応方法 ・円滑なシステム利用に資する事項	毎年 1回 以上
2	現場対応班	約50名	・システムの概要 ・操作方法（実機研修）	毎年 1回 以上

第2条 運用保守期間

構築後5年間（令和7年4月1日～令和12年3月31日）

第3条 運用保守範囲

本システムの運用保守範囲は、次のとおりとする。

No	大項目	中項目	時間
1	運用支援業務	ヘルプデスク業務	平日業務時間帯
2		アカウント管理支援	
3	緊急対応業務	緊急対応	365日 24時間
4	システム維持管理業務	定例会議	平日業務時間帯
5		定期点検	
6		簡易改修	
7		セキュリティ対策	
8		バージョンアップ	

第4条 運用保守業務の前提条件

運用保守業務に係る前提条件は、次のとおりとする。

No	観点	条件
1	平日業務時間帯	土日、祝祭日、年末年始等の閉庁日を除く、午前8時45分から午後5時30分までを原則とする。 発災時等において、当該時間以外で市への支援が必要になった場合は、市から受注者（緊急連絡先）へ連絡の上、受注者は市の求めに対し必要な支援を行うこと。
2	体制	運用保守の窓口は一元化し、責任者・保守内容及び保守依頼時の連絡先等を明記した保守体制表を提出すること。また、夜間・休日を含め、緊急時の連絡体制に関しても体制表に明記すること。

第5条 運用支援業務の要件

受注者は、本システムの安定稼働を確保するために必要な作業を実施すること。なお、本システムの安定稼働に係る各種問題が生じた場合に対応できる体制を構築すること。

運用支援業務の要件は、次のとおりとする。

No	項目	要件
1	ヘルプデスク業務	受注者は、本システムに関する問い合わせ及び障害連絡の窓口として、代表電話番号及び連絡先のメールアドレスを用意し、利用者からの問い合わせ等を受け付けること。
2		業務量について、月平均5件程度を想定している。

3		受け付けた問い合わせ及び障害連絡のすべてについて、問い合わせ内容、回答内容等を記録し、定期的に発注者に報告すること。
4	アカウント管理 支援	本システムの利用者情報の追加、更新等が必要となった場合に発注者からの要請に基づき実施すること。

第6条 緊急対応業務の要件

緊急対応業務の要件は、以下とする。

No	項目	要件
1	緊急対応	障害発生時の対応を迅速に行うこと。
2		エラーなどの各種不具合が発生した場合、原因究明調査・プログラム改修・データの入替え・復旧作業を速やかに実施し、対応策を報告すること。

第7条 システム維持管理業務の要件

システム維持管理業務の要件は以下とする。保守作業の迅速性の確保の観点から、インターネット VPN 接続 (IPsec-VPN) によるリモート保守を認める。

No	項目	要件
1	定例会議	定例会議を行うこと (年1、2回程度)。
2	SE 対応	災害対応業務の見直し等に合わせて、設定変更・保守対応を実施すること。
3		システム運用時に発覚した課題等を管理し、課題解決のための提案を本市に行うこと。なお、課題解決に必要な作業は本市と協議の上で分担して実施すること。
4	セキュリティ対策	OS及びミドルウェアのセキュリティパッチの適用を年一回以上行うこと。緊急度の高い脆弱性が発見された場合は、可能な限り迅速に対応すること。導入した機器の脆弱性情報を収集すること。緊急度の高い脆弱性が発見された場合は、可能な限り迅速に暫定対処及び恒久対応を行うこと。特に、リモート保守で使用しているファイアウォールやルーター等に脆弱性が発見された場合は、優先して対応を行うこと。
5		ディスク障害やシステム運用停止後の機器廃棄時等で、ハードディスク・外部記録媒体を廃棄する場合は、物理破壊、またはソフトウェア消去を行うこと。

6	バージョンアップ	システムは定期的にバージョンアップを実施し、上位互換が確保された形で常に最新のバージョンを維持すること。
7		最新ブラウザでシステムが利用できるように対応すること。
8	各種運用費	サービス利用料、ライセンス料を含むこと。