非機能要件兼確認書

事業者名

大項目	中項目	No.	小項目	内容	重要度	対応区分		備考
						対応状況	カスタマイズ費（単位：円）	
システム要件	基本要件	1	操作性	様々な年代の市職員が利用すること、また、災害発生時などの緊急時に利用するため、誰にも使いやすいシステムであること。	◎			
		2	可用性	システムは、計画停止を除き、稼働率99.9%を目標に設計・構築され、平常時及び、大規模災害の発生時に利用可能なこと。	◎			
		3	機密性	情報セキュリティに留意し、機密性の高いシステムであること。	◎			
		4	運用時間	本システムは、計画停止を除き24時間365日の運用が可能なこと。	◎			
		5	監視	24時間365日体制でネットワーク・サーバ機器の死活監視とCPU負荷・ディスク容量監視を行い、異常を検知した際には関係者へ緊急連絡を行い、併せて復旧を行えるシステムであること。	◎			
	システム構成	6	基本要件	本市で使用しているLGWANに接続されたPC、インターネットに接続されたPC・タブレット・スマートフォンなどから接続が可能なこと。なお、通信によりこれらの端末へ個人情報が提供されない仕組みを備えること。	◎			
		7	サーバ	本市がシステム及びサーバ等のシステム機器を保有しない「サービス利用形式」とすること。	◎			
		8	システムOS	サーバ機器のオペレーティングシステムのサポート終了などに対する対応は、受注者の責任により、対応を行い脆弱性対策を行うこと。	◎			
		9	機器の設置	システムのサーバ機器等の設置場所は下記の条件をすべて満たすこと。 ①大地震後、構造体の大きな補修をすることなく建築物を使用できることを前提とし、人命の安全及びシステム機能が確保できること。 ②万一の停電においても、速やかにUPSへ切り替わるとともに、発電機により電力供給が可能で、システムが継続的に利用可能なこと。 ③入退室管理が身分証確認などにより、24時間365日行われ、セキュリティ対策が行われていること。 ④マシンラック及び入退室口が映像により監視され、その映像が1か月以上保管されていること。	◎			
		10	バックアップ	毎日1回以上のデータバックアップを行い、障害などによりデータが失われた際には最新データからデータ復旧が可能なシステムであること。 防災情報システムに関する必須データや設定ファイル、集積されたデータ等の日次バックアップを取得し、世代管理（3世代程度）を行うこと。	◎			
		11	ユーザアカウント管理	ユーザアカウントごとに、操作可能な権限の設定ができること。 また、ユーザアカウントの管理は、市職員が登録・編集・削除を行うことができること。	◎			
		12	災害時のアカウント追加	大規模災害発生時においては、焼津市の要請に応じアカウントを追加することが可能なこと。	◎			
	セキュリティ	13	基本	セキュリティの高いデータセンター内でサービスを提供するサーバ等を運用するなど、セキュリティ対策を講じること。 また、システム面、人的及び物理的な運用管理面において、個人情報保護や不正アクセスの防止、暗号化通信やウィルス対策等のISMSに基づく運用・セキュリティ対策を施すこと。	◎			
		14	ウィルス対策	ウィルス対策については、常に最新のウィルス定義ファイルに更新し、適切なウィルス対策を講じること。	◎			
		15	サービス運用時間	サービスの運用時間は、24時間、365日を基本とし、計画停止を除き稼働率は99.9%を目標とする。	◎			
		16	サーバ設置環境	サーバの設置場所では、常に適切な温度・湿度管理を行うこと。	◎			
		17	災害対策	・データセンターにおいては、万一の停電の際もサーバ機器等が運用できるよう、UPSや発電機による電力供給が可能なこと。 ・給電設備（無停電電源装置等）、空調機器類が冗長化されていること ・震度6強から震度7程度の揺れでも耐震設計された建物であること ・風水害による洪水などの各種被害に対する備えを施された建物であること ・災害時においてもサービスを提供すること。	◎			
		18	入館・入退出管理	・24 時間の有人による入退館管理が実施されていること。 ・権限を持った者のみが入退室可能なこと。 ・複数の監視カメラにて目視監視可能であること。 ・サーバ室への入退室には、IC カード以外に生体認証を用いた管理を行うこと。	◎			
		19	冗長化構成	サーバ、ストレージ、ネットワーク機器の冗長化を行など、障害発生時におけるリスク対応を考慮した環境であること。	◎			
		20	ログイン認証	システム利用には、ID及びパスワードによるを必要とすること。パスワードは、アルファベットの大文字、小文字、数字、記号などを組み合わせや文字数の指定設定ができること。	◎			
		21	不正アクセス防止	ファイアウォールやSSL通信など暗号化通信による不正アクセス防止策を実施し、情報漏洩対策を実施すること。 また、不正アクセスや異常アクセスなどに対応するアクセス監視体制を整備すること。また、外部からの不正アクセス等があった場合は、速やかに通信を遮断する等の対応を行い、報告を行うこと。	◎			
		22	セキュリティ教育	サーバの設置場所への入退室管理を徹底するとともに、受注者の社員による情報漏洩が起こらないよう、セキュリティ教育を行うこと。	◎			
		23	情報窃取・情報漏洩防止	システム関係者による悪意の情報窃取や情報漏洩を防ぐこと。	◎			
		24	セキュリティホール解消	常にOSパッチを適用するなど、セキュリティホールの解消を行うこと。	◎			
		25	アクセスログの収集	ユーザーのアクセスログを自動収集し、本市の要請により、いつでも開示可能なこと。または、アクセスログを発注者が検索できる機能を備えること。	◎			
		26	利用ユーザーの特定	システム利用中、または利用履歴のユーザーやIPアドレスなどの特定が行えること。	◎			
研修	研修	27	操作研修計画	操作研修計画を当市と協議し策定すること	◎			
		28	研修	システムを管理する職員、システム利用者向け、それぞれにマニュアルを作成し、操作研修を行うこと	◎			
		29		職員が継続して本システムを利用できるよう、年1回程度研修を実施する	△			
運用保守要件 ※今回提出した本稼働後の利用・保守の見積もり金額にて対応ができるものは、可能、とすること。	基本要件	30	問い合わせ対応	本稼働後の保守契約等により平日の午前9時～午後5時の間で問い合わせ対応が可能な体制が取れること。	◎			
		31	障害対応	本稼働後の保守契約等により障害が発生した場合は、24時間365日対応を行い、速やかに復旧を図る体制を整えること。	◎			
		32	緊急時の連絡体制	災害発生時や障害発生時の連絡体制を発注者へあらかじめ通知し、緊急時の連絡体制を整えること。	◎			
		33	障害報告	本稼働後の保守契約等により発生した障害については、速やかに復旧するとともに、原因調査を行い、発注者へ報告を行うこと。	◎			
		34	監視	本稼働後の保守契約等により24時間365日体制でネットワーク・サーバ機器の死活監視とCPU負荷・ディスク容量監視を行い、異常を検知した際には関係者へ緊急連絡を行い、併せて復旧を行える体制を整えること。	◎			
		35	課題管理	本稼働後の保守契約等によりシステム運用上発覚した課題等を管理し、課題解決のための提案を行い、本市と協議の上、必要な対応をとること。	◎			
		36	ハードウェア管理	本稼働後の保守契約等により常にサービスが利用できるようサーバ機器等のハードウェアについて、必要に応じ保守を行い、故障や老朽化した場合には、入れ替え等を行うこと。	◎			
		37	ソフトウェアの脆弱性対策	本稼働後の保守契約等によりサービスの提供に必要な各種ソフトウェアに脆弱性が発見された場合には、脆弱性に対する対策パッチ適用などの脆弱性対応を行うこと。	◎			
		38	最新ブラウザへの対応	本稼働後の保守契約等により最新のブラウザでサービスが利用できるようにすること。	◎			