

システム要件確認書

※『必須項目』欄が○となっている項目については、当市の必須要件になりますので、1項目でも「対応不可」にてご回答いただいた場合は、自動的に本プロポーザル失格とさせていただきます。あらかじめご了承ください。

防災システム					
No.	質問項目	回答欄	備考欄	備考欄(回答に対し、一部例外や補足等がある場合に追記してください)	必須
■ベンダ情報					
1	事業者名				
2	パッケージシステム名				
■パッケージの導入実績について					
3	導入団体数を示すこと ※同パッケージにて稼働中の自治体数	0 団体	団体数を記載		
4	うち、人口40万人以上の団体への導入数	0 団体	団体数を記載 ※導入状況の詳細は、別途「業務実績書」に記載すること		
■調達前提条件について					
5	町田市個人情報保護条例及び町田市情報セキュリティポリシーを遵守すること。		1.対応可、2.対応不可		○
6	パッケージシステムが利用するプリンタは、町田市が設置した既存の複合機(一般的なオフィス用)を利用すること。また、専用帳票を印刷する等、専用プリンターが必要な場合は、町田市と協議の上決定すること。		1.対応可、2.対応不可		○
7	構築作業はできる限り自社で行い、町田市での作業は最低限とすること。		1.対応可、2.対応不可		○
8	構築にあたっては事務フローを作成し、システムの機能説明に終始するのではなく、運用フローまで含めた構築作業をすること。		1.対応可、2.対応不可		○
9	提案内容について別途費用がかかる場合、その旨を提案時に提示すること。		1.対応可、2.対応不可		○
■契約について					
10	町田市の標準契約書及び約款を適用すること。		1.対応可、2.対応不可		○
11	情報セキュリティ確保・個人情報保護のための特記仕様書を適用すること。		1.対応可、2.対応不可		○
12	構築期間(予定)は、2022年10月から2023年5月とすること。		1.対応可、2.対応不可		○
13	稼働時期は、2023年6月とすること。		1.対応可、2.対応不可		○
■システム要件について					
14	サービス提供形態はクラウドサービス(SaaS方式)にて提供されること。		1.対応可、2.対応不可		○
15	クラウドサービス(SaaS方式)による導入実績があること。		1.有、2.無		○
16	パッケージシステムが「地方公共団体における情報セキュリティポリシーに関するガイドライン」の情報システムの強靱性の向上を図るβモデルに沿ってインターネット接続(※利用可能)		1.対応可、2.対応不可		○
17	データセンタ環境として、ISMAPクラウドサービスリストに登録されていること。それ以外の場合には別紙「データセンタ要件」を満たすこと		登録されている場合にはクラウドサービス名称を記載。それ以外の場合には別紙「データセンタ要件」で回答		
18	本システムは、インターネットに接続可能なパソコン(タブレット端末含む)、スマートフォンにて利用可能であること。		1.対応可、2.対応不可		○
19	町田市が設置した既存の共通端末(DELTA(旧Wyse Technology)社のシンクライアント端末やFAT端末)及びAVD(Azure Virtual Desktop)環境で利用できること		1.対応可、2.対応不可		○
20	本システムは、端末200台の接続を想定し、ストレスなくスムーズに利用可能なこと。		1.対応可、2.対応不可		○
21	本システムは、スマートフォン3,000台の接続を想定し、ストレスなくスムーズに利用可能なこと。		1.対応可、2.対応不可		○
22	本番運用時のクライアント環境は、FAT端末の場合Windows10以降の町田市指定の後継バージョン(関連ツールを含む)、RDSの場合Windows Server2016以降の町田市指定の後継バージョン(関連ツールを含む)及びAVD(Azure Virtual Desktop)環境で動作すること(すべてのサービスパックのサポートを対象とする)		1.対応可、2.対応不可		○
23	Webブラウザについて、サポート切れ前に後続のバージョンの動作保証をすること。		1.対応可、2.対応不可		○
24	Microsoft Edge、Google Chrome、Apple Safariに対応すること。その他、対応しているブラウザを記載すること。		ブラウザ名を記載		○
25	職員が使用する端末のアプリケーションは、ライセンスフリーとすること。		1.対応可、2.対応不可		○
26	参集指示や安否確認に対する回答がスマートフォンまたはスマートフォンアプリで行える場合、対応しているOS(バージョン含む)を記載すること。		OSを記載		
27	参集指示や安否確認に対する回答が携帯電話で行える場合、NTT Docomo、au、Softbank、楽天モバイルのSSL対応ブラウザ搭載機種により動作すること。		1.対応可、2.対応不可		
28	画面構成は、WEBアクセシビリティに配慮したものであること。		1.対応可、2.対応不可		○
29	バージョンアップ及びカスタマイズ等で機能に変更があった際は、仕様書、操作マニュアル等のドキュメントを最新版に更新し、提供すること。		1.対応可、2.対応不可		○
■カスタマイズについて					
30	原則パッケージシステムへのカスタマイズは行わず提案すること。		1.対応可、2.対応不可		○
31	やむをえずカスタマイズを行う場合、他の機能やバージョンアップへの影響がないような方法を提案すること。		1.対応可、2.対応不可		○
32	カスタマイズ内容について、構築・運用のライフサイクルを通じて管理を行い、適宜町田市に内容が分かる仕様書とともに一覧表を提出すること		1.対応可、2.対応不可		○
■セキュリティについて					
33	パッケージシステムの構築・運用・保守を実施する部門が、ISO/IEC 27001(ISMS)の認証を受け、適切に更新をしていること。		1.有、2.無		○
34	クライアントからサーバへの通信について、SSL/TLSの暗号化通信を行うHTTPSへ対応すること。		1.対応可、2.対応不可		○
35	外部からの不正アクセスや内部の不正等の脅威に備え、適切な処置ができていること。		1.対応可、2.対応不可		○
36	外部からの不正アクセスや内部の不正等が発生した場合、ログインアクセス、データベースアクセスのログを取得し、IDや処理単位等で必要に応じて追跡できること。		1.対応可、2.対応不可		○
37	システムに保管されているデータのうち、パスワード等の重要なデータはデータベース内で暗号化されていること。		1.対応可、2.対応不可		○
38	データベース全体の暗号化に対応すること。		1.対応可、2.対応不可		○

39	保管期限を超過した不要データを消去できる仕組みを有すること。		1.対応可、2.対応不可		○
40	SQLインジェクション、クロスサイトスクリプト、その他の脅威に問題なく対応していること。		1.対応可、2.対応不可		○
41	ログイン可能なIPアドレスを制限できる仕組みを有すること。		1.対応可、2.対応不可		○
42	権限の切り分けができること。(例:運用・保守のためのベンダ権限、システム管理のための情報部門課権限、業務主管課権限、業務参照課権限)		1.対応可、2.対応不可		○
43	ユーザ自身でパスワードの管理(変更)が行えること。		1.対応可、2.対応不可		○
44	パスワードの有効期限を設定ができること。		1.対応可、2.対応不可		○
45	パスワードが有効期限切れしている場合、利用を行わせること。		1.対応可、2.対応不可		○
46	パスワードが有効期限切れしている場合、自動的にパスワード変更する画面に遷移すること。		1.対応可、2.対応不可		○
47	パスワードを2世代以上管理できること。		1.対応可、2.対応不可		
48	パスワードの最低文字数、最低文字種を制限することができること。		1.対応可、2.対応不可		
49	パスワード入力時の連続誤り回数によるロックアウトの設定ができること。		1.対応可、2.対応不可		
50	定期的に本システムで利用している製品に関するパッチリリースの情報を収集し、影響を確認したうえで適用すること。		1.対応可、2.対応不可		○
51	情報セキュリティに関する監査及び調査に協力すること。		1.対応可、2.対応不可		○
■保守、サポート体制について		—	—		
1. 保守対象の範囲		—	—		
52	パッケージシステムは基本的に自動運転とし、メンテナンス等であってもシステムを中断することがないように対応すること、もしくは利用可能な状態に復帰できること。		1.対応可、2.対応不可		○
53	稼働から5年以上のサービス提供を確保すること。		1.対応可、2.対応不可		○
54	法令改正時に、パッケージ提供元として速やかに対応することを担保し、説明すること。		1.対応可、2.対応不可		○
55	組織改正について、保守対応を行うこと。(例:組織マスタの変更に伴う関連データの変更など)		1.対応可、2.対応不可		○
56	バージョンアップ等の保守作業を行う際は、事前に調整の上、原則利用時間外で行うこと。		1.対応可、2.対応不可		○
57	システムの操作やパッチ処理手順等に関する業務主管課からの質問に対応すること。 ※通常は規定様式にてメール問合せ、至急時は電話問合せを想定		1.対応可、2.対応不可		○
2. 障害時の対応		—	—		
58	稼働監視、ログ監視、性能監視、URL監視を実施可能で、障害発生時には障害内容が把握できること。		1.対応可、2.対応不可		○
59	ネットワークの定期監視により、障害の未然防止対策を行うこと。		1.対応可、2.対応不可		
60	システム管理者からの問い合わせ及び障害連絡を受付可能な本システム専用の受付窓口を設けること。		1.対応可、2.対応不可		○
3. 操作研修・マニュアル		—	—		
61	本稼働前に、職員向けの操作研修を行うこと。		1.対応可、2.対応不可		○
62	操作研修の資料作成を行うこと。		1.対応可、2.対応不可		○
63	スマートフォンなどでの操作方法のマニュアルを作成すること。		1.対応可、2.対応不可		○