

システム要件及びデータセンタ要件確認書 (システム要件)

回答区分について（各種機能に関して補足事項がある場合は、「備考」欄に補足内容を記載すること）

- ：パッケージ標準提供機能で対応可能（※履行開始前までに対応できること）
 - △：機能要件の一部は対応可能
 カスタマイズや代替手段による対応可能
 - ※ 機能要件の内容に沿ったものであるか判断するため「備考」欄に対応内容を記載し、「対応に係る追加費用」がある場合、その費用も必ず記載すること
 - ※ 「対応に係る追加費用」は見積金額に含めること
 - ※ 履行開始以降に対応予定の場合、予定時期を備考欄に必ず記載すること
 - ※ システムのパフォーマンスに影響する場合は備考欄に必ず記載すること
 - ×：対応不可
- 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「×」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。

道路要望管理システム				
No.	質問項目	必須項目	回答欄	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)
1 ベンダ情報				
1	事業者名	/		
2	パッケージシステム名	/		
3	他自治体での類似システム導入実績（団体数）		0団体	
4	内人口40万人程度以上導入実績 ※構築中を含む ※導入状況の詳細は、別途「類似業務実績書」に記載すること		0団体	
2 調達前提条件について				

No.	質問項目	必須項目	回答欄	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)
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。	○		
6	本調達にはサーバや端末等のハードウェア（特殊機器は除く）及びネットワーク機器を含まないものとする。	○		
7	パッケージシステムは、町田市が設置した既存の共通端末で、AzureVisualDesktopを使用した仮想デスクトップ環境から接続し、利用可能なこと。	○		
8	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。	○		
9	パッケージシステムとして町田市が使用、あるいは町田市へ納品するソフトウェアの使用権やライセンス等については、町田市と協議のうえ決定すること。	○		
10	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。	○		

No.	質問項目	必須項目	回答欄	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)
11	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。			
12	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。	○		
13	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。	○		
3	契約について			
14	町田市の標準契約書及び約款を適用すること。	○		
15	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。	○		
16	賃貸借契約について、自ら行うことができない場合又は他の事業者に行わせる場合は、当該協力会社の法人名を記載すること。	○		
17	システム全体の構築期間(予定)は2026年7月から2027年3月とすること。ただし、要望個別表示機能・要望一覧表示機能・地図表示機能のうち、道路管理業務に直接かかわるものは、2026年10月1日までに稼働開始とすること。左記機能のうち改修を必要とするもの及び進捗公開機能・集計機能等については甲乙協議の上、2027年3月1日までに稼働を開始すること。	○		

No.	質問項目	必須項目	回答欄	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)
4	システムについて			
18	<p>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サービスを利用していること。または、「データセンタ要件」シートの要件を満たすこと。 ※登録されているサービスを利用している場合は、備考欄にクラウドサービス名称ををご記入ください。</p>	○		
19	<p>職員が使用するノート端末及び携帯端末について、使用するアプリケーションが、代表的なブラウザの最新版で正常に動作すること。 ※備考欄に対応するOSとブラウザについて詳細をご記入ください。</p> <p>(参考：町田市の現行環境) 【ノート端末】 OS : Windows11 ブラウザ : MicrosoftEDGE、Google Chrome 【携帯端末】 OS : Android OS 12 ブラウザ : Google Chrome</p> <p>※町田市指定の後継バージョンで動作すること。 ※外部事業者も使用するため、広く対応が可能であること (OS : Mac OS X 10. x以降、iOS 15. 0以上、Android 7. 0以上 ブラウザ : Safari、Firefox) 。</p>	○		
20	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。			
21	OSについては、サポート切れする前に後続のバージョンの動作保証をすること。	○		

No.	質問項目	必須項目	回答欄	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)
22	提案するシステムを構成するOSや各種ソフト等のEOL (End Of Life)が、契約期間内に訪れる製品を動作環境として選定しないこと。	○		
23	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。	○		
5 セキュリティについて				
24	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。			
25	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。	○		
26	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。	○		
27	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。	○		
28	異常または障害が発見された際には、直ちに町田市役所へ連絡し、復旧手段について万全を期す体制及び運用が可能であること。また、障害発生時には原因を調査の上、報告書を提出すること。	○		
29	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。	○		

No.	質問項目	必須項目	回答欄	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)
30	データベース全体の暗号化に対応すること。			
31	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。			
32	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。	○		
33	アクセス権限の切り分けができること。(例：管理者権限、一般権限、閲覧権限)	○		
34	ユーザー毎にパスワードによる管理が行えること。	○		
35	パスワードの有効期限を設定できること。	○		
36	パスワードの有効期限が切れた際、利用者自身でパスワードを変更設定できること。	○		
37	携帯端末からのログインを行う場合は、ワンタイムパスワードなどを利用した不正ログイン対策を行えること。	○		
38	外部事業者に要望内容やファイリングデータを共有する場合、要望ごとに承認を得た上で共有できること。	○		
39	外部事業者に共有する要望内容のうち、氏名や住所など個人情報に関するものはアクセス制限を設定できること。	○		
40	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。	○		

No.	質問項目	必須項目	回答欄	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)
6	保守、サポート体制について			
41	業務の実施にあたって管理技術者を定め、発注者へ届けること。 ※管理技術者は原則として変更できない。ただし、病休、死亡、退職等やむを得ない理由により変更する場合には同等以上の技術者とし、発注者と協議する。	○		
42	国または地方公共団体から道路施設等に関するシステム導入業務の実績または道路等包括的民間委託におけるシステムの活用実績がある者を管理技術者とする事。	○		
43	技術士（総合技術管理部門（建設）または建設部門）またはシビルコンサルティングマネージャー（RCCM（道路））の有資格者を管理技術者として配置すること。			
44	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）	○		
45	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。	○		
46	システムの操作等に関する一般職員からの質問に対する対応方法、体制等について提案すること。（例：ヘルプデスク、メール窓口の開設等）	○		
47	バージョンアップ等の保守作業を行う際は、事前に通知すること。	○		
48	職員や道路管理業務に関連した受託業者がシステムの操作方法を習熟できるよう、実際にシステムを操作しながら学習する形式の研修を実施すること。 研修は対面・オンラインとも可とする。	○		

システム要件及びデータセンター要件確認書
(データセンター要件)

このシートは、「システム要件」シートのNo.18において、データセンター環境として、ISMAPクラウドサービスリストに登録されているサービスを利用していない場合のみ回答してください。

回答区分について

- : 対応可
- × : 対応不可

1項目でも「×」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。

道路要望管理システム		
No	質問項目	回答欄
1	データセンター環境	
	(1) 施設設備	
	①立地条件	
1	(a) 日本国内に立地していること。	
2	(b) 浸水被害を想定し、浸水予測区域図にて0.2m以上浸水する地域でないこと。	
3	(c) 液状化被害を想定し、液状化予測図にて液状化がほとんど発生しない地域であること。	
4	(d) 津波被害を想定し、臨海地域以外、かつ海拔30m以上の地域であること。	
	②建物・フロア・空調条件	
5	(a) 耐震対策のため、建築基準法に準拠した耐震・防振等の構造上の安全性を配慮した設計・施工が行われていること。	
6	(b) 防火対策のため、建物は、建築基準法に規定する耐火建築物であること。	
7	(c) 情報処理施設に雷が直撃した場合を想定した対策を講じること。	

No	質問項目	回答欄
8	(d) 情報処理施設の付近に誘導雷が発生した場合を想定した対策が講じてあること。	
9	(e) 空調設備が設置された室については、温度及び湿度並びに空調設備の作動状況の常時検知・監視が行われていること。	
10	(f) ガス系消火設備の設置があること。	
③電源設備		
11	(a) 電源の二重化による停電対策を講じていること。	
12	(b) 電源の二重化等により、電源断による機器障害が発生しないことを担保すること。	
13	(c) 電力会社での送電系統に障害が発生したことを想定し、予備電源として非常用発電設備を有すること。	
14	(d) 非常用発電設備が安定稼働するまでの電源供給として、UPS設備を装備していること。	
15	(e) 非常用電気設備について年1回以上の法定点検を実施していること。	
④保有資格		
16	(a) ISO14001の認証を受けていること。	
17	(b) ISO/IEC27001 (ISMS) の認証を受けていること。	
(2) セキュリティ対策		
①施設セキュリティ対策		
18	(a) 24時間365日警備員による入退館者の監視・管理を実施していること。	
19	(b) 重要な物理セキュリティ境界出入口には、破壊対策ドアが設置されていること。	
20	(c) 重要な物理セキュリティ境界の出入口を監視カメラで常時監視していること。また、適切な期間保存されていること。	
21	(d) セキュリティ境界から入館者のPCや電子記録媒体の持込、持出の管理が申請管理されていること。	
22	(e) セキュリティ境界への入室者は予め定められた申請者からの事前登録制とし、データセンタ入り口等で、本人確認を行い、24時間365日の有人監視を実施すること。	
23	(f) 入退室の状況の管理は、以下の機能を有する入退室管理システムを利用すること。	

No	質問項目	回答欄
24	①個人識別機能(個人認証カード、生体認証等)	
25	②扉の自動施錠機能	
26	(g) 入退室管理システムは5年以上のログを保存していること。	
2 運用・保守		
(1) ソフトウェアセキュリティ		
①ソフトウェアセキュリティ対策		
27	(a) ウィルス対策ソフトを導入し、リアルタイムにコンピュータ・ウィルスの侵入をチェックすること。	
28	(b) 年一回以上の脆弱性診断を第三者が実施すること。	
29	(c) 定期的に本システムで利用している製品のバージョンアップ、パッチリリースの情報を確認し、適用すること。(月一回以上)	
30	(d) 情報通信の保護のためSSL通信を利用すること。	
31	(e) 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。	
32	(f) 利用者がアクセスするWEBサーバはDMZに、データを管理するデータベースサーバはセキュリティに考慮してTRUSTに分散設置されていること。	
33	(g) 不正アクセス等の脅威に備え、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、必要に応じて追跡できること。	
34	(h) 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。	
(2) ハードウェア・ネットワークセキュリティ		
①ハードウェア・ネットワークセキュリティ対策		
35	(a) 冗長化されたサーバ構成により、サーバ障害が発生した場合でも代替サーバにより運用継続を可能とすること。	
36	(b) ユーザがアクセスするWEBサーバと、AP、DBサーバを分散設置し、アクセス範囲を必要最低限とすること。	
37	(c) 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。	
38	(d) ネットワーク機器、経路を冗長構成とし、障害が発生した場合でも正常なネットワーク経路へ自動的に切り替えることで運用継続を可能とすること。	
(3) 運用条件		

No	質問項目	回答欄
①運用条件		
39	(a) 本システムは、24時間365日利用可能であること。(ただし障害対応や定期システムメンテナンスなどによる停止は除く。)	
40	(b) システム管理者からの問い合わせ及び障害連絡を受け付ける本システム専用の受付窓口を設けること。	
41	(c) データベースのバックアップは毎日取得し、1週間分(7世代)のバックアップデータを保持すること。またバックアップはシステムを停止せずにオンラインで実施できること。	
42	(d) ログのバックアップは毎日取得し、六ヶ月以上保存すること。	
43	(e) システムのバックアップは一ヶ月に一度以上取得し、3世代以上保存すること。	
44	(f) 障害を検知した場合、利用者に速報を通報できること。	
45	(g) 稼働監視、ログ監視、性能監視、URL監視を実施しており、障害発生時には障害内容が把握できること。	