仕様書別紙３　非機能要件表

項番	要求事項	評価項目	要求内容
1	規模要件	利用者	区職員、委託事業者
2		利用者数	30名程度
3		同時利用	10名想定
4		データ量	街路樹台帳（Excel）：約5,200本
5			診断カルテ（樹木点検及び街路樹診断）（Excel、PDF）：約5,200本
6			苦情処理・対応記録：年間約100件
7	性能要件	性能	システムは原則として 24 時間運用とすること。計画停止をする場合は、あらかじめシステム管理者と協議し、十分に周知してから行うこと。
8			最大 10 名程度が同時にアクセスしても支障なくシステムを利用できること。
9			システムの運用及び保守はシステム事業者が行うこと。
10			障害発生時には、復旧作業に速やかに着手し、最大限の努力をもって復旧作業を行うこと。
11			システムのバージョンアップがあった場合には、随時、委託費の範囲内で最新版を提供できること。
12		ソフトウェア	システム形態はWeb型であること。
13			環境変化等に際しても、バージョンアップ等の手段で、少なくとも5年は最適な状態で利用できるシステムであること。
14			汎用的な OS （Windows11以降）で利用・動作できること。
15			システム全体の操作はシンプルでわかりやすいものであること。
16			導入するソフトウェアは調達段階での最新バージョンを使用すること。ただし、システムの運用に影響を及ぼすと認められる場合は、実績のあるバージョンを使用して差し支えない。
17			ソフトウェアの障害対応については速やかに実施し、以後同様の障害が発生しないよう防止策を講じること。
18			ユーザーが同一のデータを基に作業ができること。また、発注者の要望に応じてユーザーを追加・削除できること。
19			ソフトウェアを使用するに当たって必要となるライセンスを過不足なく用意できること。なお、ライセンス料が発生する場合は、その費用も見積金額に含めること。
20		ハードウェア	ASP・SaaS 方式のサービスであり、クライアント PC にソフトのインストールを必要とする形式でないこと。
21			検索スピードや画面展開が遅延することがない構成であること。
22		ネットワーク	区職員（庁舎内・出先機関）利用端末、現場でのスマートフォン、タブレット等からシステムへアクセスできること。このアクセスに必要な設定作業が発生する場合は、発注者及び関係事業者と協力すること。
23			第三者からの不正アクセスを防ぐ仕組みを有すること。
24	セキュリティ要件	セキュリティ	情報セキュリティ対策を実施するにあたっては、本区における情報セキュリティに係る規定等に準拠すること。また、作業にあたっては、当該規定等を遵守すること。
25			不正な接続及びデータ通信を検知し不正侵入に備えること。不正侵入を検知した場合は、速やかに状況を報告する機能を有すること。また、改ざんを防止する機能を有するソフトウェア等を搭載することによって、被害の拡大を可能な限り抑制すること。
26			本システム稼働時点で必要な機能の組み込みに加えて、稼働期間全体にわたっての継続的な更新（最新かつ実証済みのウイルス定義ファイルやセキュリティパッチ等を遅滞なく取り込むなど）のための仕組みを実現できること。
27			ウイルスに感染しないためのセキュリティ対策がされていること。万が一感染した場合は、速やかに完全に駆除すること。
28			セキュリティホールが発見された場合は、パッチ、サービスパック、アップグレード等の適用といった必要な対策を行い、速やかにセキュリティホールをふさぐこと。
29			セキュリティ事件、事故及びセキュリティ違反については、発注者に速やかに報告し、対応を行うこと。
30			セキュリティパッチの適応は定期的な実施のほか、緊急性の高いものについては本区と協議の上、随時対応すること。
31		権限	利用者はユーザーID・パスワードでログイン認証を行い、ユーザー登録された者以外による不正アクセスを防止すること。
32			利用者のアクセスログを最低１か月間保管し、アクセスの監視及び記録を行うこと。また、必要に応じて、アクセスログの集計及びレポート出力が出来るようにシステムを設計すること。
33			利用者には権限設定を行い、処理・検索・閲覧メニューにおいて利用可能な範囲が限定できること。なお、こうしたアクセス権の設定は、システム管理者が変更できること。
34			システム管理者が適宜必要に応じてユーザーのアクセス遮断等の措置が可能であること。
35	システム要件	信頼性継続性	日本国の法律及び締結された条約が適用される国内データセンターを用いること。また、提供されるサービス全体として日本国に裁判管轄権があること。
36			データセンターは敷地、建物、サーバー室及びラック内の IT 危機へのアクセス管理が実施されていること。
37			データのバックアップを毎日行うこと。また、予期せぬサーバー障害や災害時に、バックアップから確実な復旧が行えるよう対策を講じること。
38			データセンターは地震や火災など災害に対してデータ保全の安全性を保ち、かつ、機器の故障や一部機器に障害が発生しても、サービスを継続して提供できる冗長構成の設備があること。
39			ソフトウェアの障害によって起こるシステムダウンに対して、障害発生前のシステム環境へ修復できること。
40			システムを構成するアプリケーションの改修や、新たなアプリケーションの追加が容易に行える構成とすること。
41		テスト	本システムの本番稼働前に、機能テスト及びシステム全体の運用テストを行うこと。これらのテストに係る費用等は、全て委託範囲に含む。
42			システムが機能要件を満たし適切に稼働できるかを確認するための、区職員立会いのテストを行うこと。
43			テスト実施に当たっては、あらかじめ実施計画を提出し、発注者の承認を得て行うこと。また、テストに合格した際には、実施結果報告書をまとめて発注者に提出すること。
44	運用保守要件		システムの本稼動前に、システム操作を習得させるために、システム管理者・委託事業者それぞれに対する操作研修会（管理者２回、委託事業者２回程度）を実施すること。