

自転車王国とくしまデジタルマップ作成業務仕様書

1. 委託業務名

自転車王国とくしまデジタルマップ作成業務

2. 委託期間

契約締結の日から令和9年3月31日（水）まで

3. 委託業務の目的

「ワールドマスタースゲームズ2027関西の開催」や「大鳴門橋自転車道の開通」などを見据え、サイクリストが安全・安心かつ快適にサイクルツーリズムを楽しむことができるよう、自転車王国とくしま公式コース等及び令和7年度に調査を行った徳島県東部圏域の地域資源（観光施設、ビュースポット、休憩施設等）を反映したデジタルマップを作成する。

4. 委託上限額

2,500,000 円（税込）

5. 業務内容等

(1) デジタルマップの作成

ア 利用方法

- ① デジタル媒体の仕様は問わないが、可能な限り多くのモバイル端末に対応可能なシステム（モバイルアプリやWEBアプリなど）とすること。
- ② Windows、Mac、iPhone、Android 端末に搭載されている汎用ソフトウェアにて利用が可能で、最新版のブラウザ、OS に対応していること。

イ 必要な機能

- ① 次の情報を掲載できること。

A コース

- a 自転車王国とくしま公式コース（6コース）
 - ・お遍路発心コース ・鳴門海峡渦潮コース ・鳴門ウチノ海潮風コース
 - ・鳴門⇒徳島「走ってみんでー！」サイクリングコース
 - ・国府4ヶ寺巡りコース ・焼山寺参った？コース
- b 徳島自転車Tライン
- c 四国一周サイクリングルート（徳島県部分）

B 地域資源（徳島県東部圏域）

170 か所の地域資源について、以下の地域資源情報を適切にカテゴライズして掲載できること。

【地域資源情報】

- a 種 別（観光施設等、ビュースポット、休憩施設等、自転車関連施設）
 - b 写 真
 - c 名 称
 - d 住 所
 - e ホームページ
 - f 営業時間
 - g 定休日
 - h 駐輪場の有無
 - i サイクルラックの有無
 - j 空気入れ貸出の有無
 - k 自転車修理工具貸出の有無
 - l トイレ利用の可否
 - m その他サイクリスト向けのサービスの有無及び内容
 - n 四国一周サイクリングおもてなしサポーターへの登録の有無
 - o Setouchi Velo スポットへの登録の有無
 - p その他サイクリスト支援制度への登録の有無及び内容
 - q その他サイクリストにとって必要な情報
- ② 利用者の現在地表示機能を付加すること。なお、利用者の位置情報や利用履歴等を取得する場合、個人情報の保護に関する法律等を遵守し、アプリ・サイト初回利用時に適切な同意取得およびプライバシーポリシーの提示を行う機能を実装すること。また、システム管理画面へのアクセスには、多要素認証（MFA）または特定の IP アドレスからのアクセス制限等、適切なアクセス制御機能を設けること。
- ③ 英語及び韓国語対応を行うこと。なお、自動翻訳での対応も可とする。
- ④ 自転車王国とくしまホームページからデジタルマップの利用ページまたはアプリダウンロードページへ遷移できること。

ウ 登録方法等

掲載内容の初期登録・追加登録・修正・削除を容易かつ安価に行うことができること。また、これら操作に係るマニュアルを徳島県へ提供すること。

エ サーバー環境等

デジタルマップの運用に必要な高い安全性を備えたサーバー環境等を受託者が用意すること。

オ その他拡張機能（自由提案）

上記以外に、予算内で実施可能な利用者の利便性向上・県内周遊促進に繋がる機能やユーザーデータの確認・分析・活用機能などの拡張機能があれば盛り込むこと。

（2）デジタルマップの保守管理

デジタルマップの公開から適切な保守管理を実施すること。

6. その他特記事項

(1) 再委託

再委託は原則禁止する。ただし、専門性等から、自ら実施するより高い効果が期待される場合等においては、業務の一部を再委託により実施することができる。再委託が必要となる場合は、事前に県と協議し、承認を得ること。

(2) 機密保持

- ア 受託者は、本業務の実施に当たり知り得た情報について承認なく、第三者に漏洩してはならない。本契約が終了し、又は解除された後も同様の義務を負う。
- イ 受託者は、県から提供された資料等を厳重に取り扱うものとし、本業務の目的以外のために利用（複写及び加工を含む）し、又は第三者に提供してはならない。
- ウ 受託者は、本業務終了後、速やかに県から提供された資料等を返還すること。

(3) 情報セキュリティ管理

業務の実施に際して、個人情報の保護に関する法律（平成 15 年法律第 57 号）、徳島県個人情報の保護に関する法律施行条例（令和 4 年 12 月 23 日条例第 50 号）、徳島県情報セキュリティポリシーのほか、関係法令等を遵守すること。

(4) クラウドサービス

クラウドサービスを利用する場合は、以下の要件を満たすこと。また、各条件を満たしていることを証明する書面等を提出すること。

- ア 「政府情報システムのためのセキュリティ評価制度（I S M A P）」認証を取得していること。ただし、ISMAP 未取得のサービスを利用する場合は、個人情報をはじめとする機密性の高い情報資産の漏洩リスクを極小化するため、特に、個人情報の保管領域の分離や高度な暗号化によるセキュアなデータ保護、および「位置情報と個人情報の結び付け・保持期間の最小化」など、個人情報をはじめとする機密性の高い情報資産の漏洩リスクを極小化する手法を提案すること。
- イ ISO/IEC27017（外部サービスセキュリティ）を取得、または、それに相当するセキュリティ管理を行っていることを証明する資料等の提出を行うこと。ただし、I S M A P 認証を取得している場合は、この限りではない。
- ウ 別紙「クラウドサービス提供業者の選定基準について」に記載している項目を全て満たすものとする。

(5) 権利の帰属

本業務の実施による成果品に係る著作権は、原則として全て県に帰属するとともに、作成者は著作者人格権を行使しないこととする。ただし、受託者が従前から保有する著作物、オープンソースソフトウェア、地図データ、クラウドサービス及び第三者が権利を有する素材についてはこの限りではない。

(6) その他

- ア 県は業務期間中、いつでもその業務状況の報告を求めることができるものとし、受託者は、その求めに応じなければならない。
- イ 業務の実施に当たって必要な経費（交通費、印刷費等）は、全て本業務委託の費用に含めるものとする。
- ウ この仕様書に定めのない事項及びこの仕様書に関し、疑義が生じた場合は、その都度、県と協議を行い、業務の円滑かつ適正な実施に努めるものとする。

クラウドサービス提供者の選定基準について

1. 本県とクラウドサービス提供者との情報の受渡し方法や利用終了時の情報の廃棄・返却方法等を含む情報の取扱手順を定め、その計画書を提出すること。
2. 経済安全保障の観点から、クラウドサービスの利用を通じて、本県が取り扱う情報のクラウドサービス提供者において本県の認める目的の外に利用しないこと。
3. クラウドサービス提供者における情報セキュリティ対策の実施内容及び管理体制を示した書面等を提出すること。
4. クラウドサービス提供者においては、クラウドサービス提供者、その従業員、再委託先又はその他の者によって本県の意図しない変更が加えられないための管理体制を示した書面等を提出すること。
5. クラウドサービス提供者の資本関係・役員等の情報、クラウドサービス提供業務に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する事項が記載された書面等を提出すること。
6. クラウドサービス提供者において発生した情報セキュリティインシデントによる被害を最小限に止めるための対処方法（対処手順、責任分界、対処体制等）を示した書面等を提出すること。
7. 情報セキュリティ対策その他の契約の履行状況が確認できる報告（クラウドサービス提供者からの定期的な報告、情報セキュリティ監査等）を作成し提出すること。
8. 情報セキュリティ対策が不十分であると分かった場合は、その対処方法（改善について本県と協議の上、実施すること。）を定めた書面等を提出すること。
9. クラウドサービスの中断又は終了時に際し、円滑に業務を移行するための次の事項を記載した計画書を作成し、提出すること。
 - （１）サービス中断時の復旧要件
 - （２）サービス終了又は変更する場合の事前告知の方法・期限及びデータ移行の方法
10. クラウドサービス提供者への立入検査又は情報セキュリティ監査の受入を認めること。又は立入検査及び監査と同等の効力を持つ書面等（SOC）を示すこと。
11. サービスレベルの保証（可用性、通信の速度及び安定性、データの保存期限及び方法、データ交換の安全性及び信頼性確保のための方法、情報セキュリティインシデントの対策方法等）を定めた書面等を提出すること。
12. 経済安全保障の観点から、バックデータを含む情報が取り扱われる場所については、日本の法令の範囲内で運用できるデータセンター等とし、契約書等において日本国内の裁判所を合意管轄裁判所と記載できること。
13. 経済安全保障の観点から、クラウドサービス提供者がその業務等を一部再委託させた場合は、再委託先にもクラウドサービス提供者と同様に当該選定基準の全てを満たす者とし、再委託先の情報セキュリティ対策の実施が確認でき、本県の承諾を得るための書類が提出できること。

14. クラウドサービスの提供を含む情報の流通経路全般にわたりセキュリティが適切に確保されるにあたり、次のセキュリティ要件を満たすことができる者であること。

- (1) クラウドサービスに係るアクセスログ等の証跡の保存は1年以上であること。
- (2) クラウドサービスのインターネット接続点の通信監視ができること。
- (3) クラウドサービス提供者による管理・保管の実施内容が確認できること。
- (4) クラウドサービス上の脆弱性対策の実施内容が確認できること。
- (5) クラウドサービス上の情報に係る復旧時点目標等の指標が確認できること。
- (6) クラウドサービス上で取り扱う情報は暗号化すること。
- (7) クラウドサービス利用者が指定するクラウドサービス上の情報の確実な削除・廃棄ができること。
- (8) クラウドサービス利用者が求める情報開示請求に対する開示項目及び範囲については、本県と協議の上、契約書等に明記すること。