様式１_機能要件

項番(大)	種別	項番(小)	要件項目	項番(細目)	要件	備考
1	システム管理	1	利用権限設定	1	・システム全体の権限等を有するユーザー(以下、システム管理者)とスタンプラリーを作成するユーザー(以下、サイト管理者)等、システムの運用に必要な権限が分けられること。	・利用のみを目的としたユーザー(以下、利用者)はアカウント不要で利用できること
1	システム管理	2	アカウント管理	1	・調整課から利用を希望する所属に対して、アカウント発行ができること。	・発注当初にサービス提供事業者から、一定数(20～30)のアカウント(ID＋PW)を発行し、追加が必要となった場合、新たにアカウント追加可能といった運用が可能であれば「◎」と見做す。
2	セキュリティ	1	パスワード再発行	1	・ログインに用いるパスワードを忘れた場合、利用者自身で変更及び再発行が可能であること。	
2	セキュリティ	2	監査ログ	1	・以下のログを最低1年分取得できること。なお、本市の求めに応じてSE作業等により都度取得しても構わない。 Ex:操作ログ、認証ログ、イベントログ、通信ログ、印刷ログ、ダウンロードログ、設定変更ログ、エラーログ	
3	利用者機能	1	スタンプ獲得方式	1	・QRコード、GPSがそれぞれ単独で選択可能であること。	・「それぞれ単独で」に関して、例えば、QRコードのみを選択できること(他の方式と組み合わせることを必須としないこと) ・現時点では一部あるいは全部を満たせないが、当該機能を実装する予定がある場合、本市と協議する。
3	利用者機能	1	スタンプ獲得方式	2	・スタンプに加えて、ポイントを獲得する方式も選択可能であること。(例:Aの場所では100ポイント、Bの場所では200ポイント等)	獲得方法は3.1.1に準じる
3	利用者機能	2	景品提供形式	1	・応募フォームが選択可能であること。	・現時点では一部あるいは全部を満たせないが、当該機能を実装する予定がある場合、本市と協議する。

3	利用者機能	3	利用者のログイン	1	・利用者は、メール認証機能によるログインができること。 ※ ログインなしでも利用可能だが、Cookie使用不可で獲得履歴が残らない場合のために、ログインを推奨	
3	利用者機能	4	複数同時開催	1	・10程度の複数のスタンプラリーが並行開催できること。	・同一のマップ上で複数のスタンプラリーの実施ではなく、当該PF内で実施期間が重複するスタンプラリーを並行して実施することを想定している。
4	管理者機能	1	管理画面へのログイン	1	・システム管理者及びサイト管理者は、ID・パスワード認証によるログインができること。	
4	管理者機能	2	スタンプラリー・ポイントラリー機能	1	・エントリーページ、ラリーポイント詳細、スタンプ台紙、マップ、特典応募画面をGUIで編集できること。 ・利用規約同意チェック機能を有すること。 ・プレビュー機能を有すること。 ・スポット毎に取得可能なポイントを変更できるポイントラリーにも対応可能であること。	・プレビュー機能に関しては、公開前に本番同等の画面を確認する手段があることを要件とする。 ・現時点では一部あるいは全部を満たせないが、当該機能を実装する予定がある場合、本市と協議すること。
4	管理者機能	3	デジタルマップ機能	1	・施設情報をマッピング(画像ピン)できること。また、デジタルスタンプラリーとシームレスに連携ができること。 ・複数のスタンプラリー等を行う場合、各ラリー毎にマップを設定できること。 ・マップからスポット情報にシームレスに遷移できること。 (オプション:必須ではない)一部のスポットを絞り込んで表示することでおすすめのモデルコースを表示できること。	・例えば、マップ上の画像ピンを押下することでスポットの詳細情報をシームレスに閲覧できることやマップ上でスタンプラリーのスポットの一覧表示ができる等、マップ及びスタンプラリーの一体感を損なわないUIを備えていること。
4	管理者機能	4	アンケート機能	1	・エントリー時、スタンプ取得時、特典応募時にカスタムアンケートを配置することができること。	
4	管理者機能	5	データ分析機能	1	・利用者(デジタルスタンプラリー等の参加者)のアンケート結果を表示できるダッシュボード機能を有すること。なお、これらのデータは、個人が特定されないよう年代や性別あるいは時間帯といった単位でグルーピングすること。 ・分析結果はダウンロードできること。 ・滞在時間を把握するため、GPSによる位置情報をリアルタイムもしくはダウンロード等で把握できること。	滞在時間は、GPSをトラッキングにより計算する想定。ただし、利用者の仕様する端末のOS仕様によりGPS機能が仕様出来ない場合は除く。
4	管理者機能	6	不正防止	1	・不正防止機能として同じQR コードの利用を1日1回に制限可能であること。	

4	管理者機能	7	データ管理	1	・任意のタイミングでデータ削除できること。	
5	データ移行	7	データ移行	1	・任意のタイミングでデータ移行(※)ができること。 ※現行の共通プラットフォーム及び新たに他社サービスから、当該共通プラットフォームへ移行する際のスポット情報(画像含む)、アカウント、ポイント引継ぎを想定。	・移行までに各所管からファイルを受け取り、サービス提供事業者にてデータ移行作業を実施する場合も、適用状況を「◎」とする。 ・令和7年度の移行対象は、5件(全てスタンプラリーのみで、アカウント、ポイントの引き継ぎはない)を想定。

様式２_非機能要件

項番(大)	種別	項番(小)	要件項目	項番(細目)	要件	備考
1	動作環境	1	OS要件	1	・以下の環境で利用できること。(バージョンは、導入時点の最新版に対応すること) iOS、Android	
1	動作環境	2	ブラウザ要件	1	・以下のwebブラウザに対応していること Google Chrome、Safari (オプション)Microsoft Edge	
1	動作環境	3	回線要件	1	・通信にはTLSまたはインターネットVPNを用いること。なお、TLSを用いる場合は「様式3_TLS回線要件」を、インターネットVPNを用いる場合は「様式4 インターネットVPN回線要件」を満たしていること。	
1	動作環境	4	動作要件	1	・アプリのインストールを要さず、WEBブラウザのみでの利用が可能であること。	
1	動作環境	4	動作要件	2	・(オプション)iOS及びAndroid向けアプリ対応ができること。	
2	セキュリティ	1	外部サービス要件	1	・「様式5 外部サービス要件」を満たしていること。なお、システムの一部または全部に外部サービスを用いる場合、当該サービスについても同様。	・「要否」欄が「必須」となっている項目をひとつでも満たさない場合は契約不可 ・外部サービスを複数使用している場合は、サービス毎に確認が必要となる。
2	セキュリティ	2	アクセス制御	1	・接続元IPアドレス制御等、アクセス元を限定するための機能を有すること。	
2	セキュリティ	3	システム利用者	1	・市民:1万PV/月 ・神戸市職員:10,000人程度を想定	
2	セキュリティ	3	システム利用者	2	・神戸市が主催若しくは共催するスタンプラリーイベントに関する業務の受託等を受けた事業者	

2	セキュリティ	4	ドメイン管理	1	・当該共通プラットフォーム利用終了後、最低1年間は保持すること。	
3	アカウント	4	管理アカウント	1	・スタンプラリーの設定をできるアカウントとして、少なくとも2アカウントが作成できること。また、アカウントの増減により、月額利用料に変動がないこと。	・システム管理者アカウントとサイト管理者アカウントの区分を持たせる。 ・サイト管理者アカウントが最大400程度配布できることが望ましいが、サイト管理者アカウントが1つしか提供できず、共用で使用することも許容する。
4	利用条件	1	スポット数	1	・100スポット/マップ以上を登録できること。（最大500スポットを想定すること）	・100スポット/マップをベースとし、これを超える場合、マップ毎に増やすことができること。
4	利用条件	2	ラリー数	1	・年間で実施するラリーは、概ね、スポットでの利用だが、通年で実施するポイントラリーも含めて、20～30件を見込んでいる。	
4	利用条件	3	広告の表示の禁止	1	広告の表示は行わないこと。	
5	全般	1	多言語対応	1	・英語・中国語（繁体・簡体）・ベトナム語に対応できること。	・現時点では一部あるいは全部を満たせないが、当該機能を実装する予定がある場合、本市と協議すること。
6	生成AI	1	生成AI（学習利用の禁止）	1	・生成AIを使用する場合は、神戸市情報セキュリティ対策基準8.1.26ア(1)の規程に従い、入力情報が本市の許可なく生成AIの学習に利用されないことを確認すること。	
6	生成AI	2	生成AI（監査等による閲覧の禁止）	1	・生成AIを使用する場合は、神戸市情報セキュリティ対策基準8.1.26ア(2)の規程に従い、入力情報が本市の許可なく同システムを提供する事業者による監査等により閲覧されないことを確認すること。	
7	ヘルプデスク	1	操作方法	1	・管理画面における操作方法に関する問い合わせに対応したヘルプデスクを有すること。	
7	ヘルプデスク	2	データ移行・運用支援	1	・各所管課におけるデータ移行、運用設計で生じる、確認事項あるいは（当該共通プラットフォームでの）実現可否等に関する相談に対応するためのヘルプデスクを有すること。	データ移行支援について、CSV作成～取込までの作業は、基本、各所管で実施するが、移行用データフォーマットの提供、エラー時の問い合わせや原因調査の支援を想定している。

様式3_TLS回線要件

区分		内　容	適用状況		エビデンス等(URL可)
1.TLS回線のバージョン					
	1.1.	・TLS回線のバージョンは、バージョン1.2以上を使用すること。			
2.付加的なセキュリティ対策 ※下記のいずれかが「あり」であること					
	2.1.	IPアドレス制限			
	2.2.	多要素認証			
	2.3.	WAF			
	2.4.	FW(ファイヤーウォール)			
	2.5.	その他のセキュリティ対策			

（別　紙）

様式4_外部サービス要件

外部サービス名称			記入日			
外部サービス提供者名称			記入者			
区分		要件	取扱情報が機密性2以上の場合			
			要否	適用状況	備考	
1.外部サービス要件（機密性2以上）						
1.1.	セキュリティ評価制度	利用しようとする外部サービス（アプリケーション）が政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））への登録が行われており、かつ利用するサービスが言明対象範囲内であること。	任意			
		1.1でISMAPへの登録が行われていない場合				
1.2.		利用しようとする外部サービス（アプリケーション）が政府情報システムのためのセキュリティ評価制度「ISMAP-LIU」（ISMAP for Low-Impact Use）への登録が行われていること。	任意			
1.3.	SLA	サービスレベルの保証が定められていること。 SLAには以下のような内容が定められていること。 ・情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順及び情報セキュリティインシデントの対応等の取り決め ・外部サービス利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得、保持し、定期的にレビューできること。 ・利用する外部サービス又はシステムの技術的脆弱性に関する情報は、公表された後に速やかにクラウドサービス利用者が入手できるようになっていること。	任意			
1.4.	クラウドサービス情報開示認定制度	利用しようとする外部サービス（アプリケーション）が一般社団法人日本クラウド産業協会(ASPIC)クラウドサービス情報開示認定制度への登録が行われていること。	任意			
1.5.	生成AIを利用したサービスにおける入力情報の取扱	外部サービスが生成AIを利用したサービスに該当する場合においては、同サービスへの入力情報が、本市の許可なく生成AIの学習に用いられたり、サービスを提供する事業者による監査の対象にならないことが確認できること。	必須			
1.1.でISMAPへの登録が行われている場合、1.2.でISMAP-LIUへの登録が行われている場合、または1.4.でASPICへの登録が行われている場合、以下の要件は不要						
1.6.	資格・認証 ※アプリケーション提供事業者(ASP)	サービス提供を行う組織(ASP)が、ISO/IEC 27001：2013認証を取得していること。	任意			
1.7.	資格・認証 ※クラウドサービスプロバイダー(CSP)	利用しようとする外部サービス（アプリケーション）が政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））に登録されているサービス上に構築されており、かつ利用するサービスが言明対象範囲内であること。	任意			
1.8.		1.7でISMAPへの登録が行われている場合、1.8～1.13の要件は不要				
		サーバを提供する組織(CSP)が、ISO/IEC 27001：2013認証を取得していること。	必須			
1.9.		サーバを提供する組織(CSP)が、ISO/IEC 27017：2015認証もしくはPCI DSSを取得していること。もしくはそれに相当する機能や組織体制を有していることが確認できること。	必須			
1.10.		サーバを提供する組織(CSP)が、ISO/IEC 27018：2014認証を取得していること。	任意			
1.11.	データセンター要件	データセンターは、日本データセンター協会が制定するデータセンターファシリティスタンダードのティア3相当の基準を満たした設備とすること。	必須			
1.12.	データの所在・適用法と裁判管轄	サービス上のユーザ所有データ（バックアップデータを含む。）の所在地が日本国内に限定できること。	必須			
1.13.		サービス提供事業者の実施場所（事務所、運用場所）（地域（リージョン）が特定できるようにすること）を情報提供すること。提供にあたっては文書にて内容を確約すること。	必須			
1.14.		準拠法、裁判管轄を国内に指定できること。	必須			
1.15.		市が登録したデータは、本市に確実に提供でき、提供後のデータの所有権・管理権は、市が保有すること。また、市が登録したデータは、本契約に明示的に定められているところを除き、本市の承諾なく、利用できないものとすること。	任意			
1.6 と1.7もしくは、1.6と1.10の認証を取得している場合、以下の要件は不要						

（別　紙）

区分			要件	要否	適用状況	備考	
	1.16.	セキュリティ対策・体制	サービス提供業務の遂行のために提供する情報（契約等の手続に付随して外部サービス事業者が知りうる利用者情報等）を、サービス提供業務の遂行目的外で利用しないこと。情報の目的外利用の禁止に対する遵守（義務）の表明をすること。	必須			
	1.17.		サービス提供を行う組織若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制について提示すること。	必須			
	1.18.		情報セキュリティインシデントが発生した場合に、被害を最小限に食い止めるための対処方法（対処手順、責任分界、対処体制等）について提示すること。	必須			
	1.19.		障害や情報セキュリティインシデントの発生、監査結果等によって、情報セキュリティ対策の履行が不十分であると認められた場合の対処（改善の実施等）方法について提示すること。	必須			
	1.20.	データ暗号化	機密性の高いデータ等については、暗号化等によって蓄積・伝送データを保護できること。	必須			
	1.21.	ログ取得	外部サービス上におけるアクセスログ等の証跡に係る保存期間について、1年間以上の保存が可能であること。その手法について提示すること。	必須			
	1.22.	脆弱性対策	外部サービス上の脆弱性を発見する方法があり、実施可能であること。その手法について提示すること。	必須			
	1.23.	不正アクセス対策	通信内容を監視する等により、不正アクセスや不正侵入を検知及び通知できること。	必須			
	1.24.	機器停止	機器に異常があった場合、検知できること。 また、機器を死活監視し、停止した場合、検知できること。	必須			
	1.25.	データ取扱い時の権限管理	データの取り扱いについて、権限管理及びアクセス制御ができること。	必須			
	1.26.	保守端末	保守端末は、認証管理、持出管理、施錠管理、ログ管理等によりセキュリティを確保していること。	必須			
	1.27.	データ消去	データを消去する際は、ISO27001に準拠してデータを復元できないように電子的に完全に消去又は廃棄すること。また、データを消去又は廃棄した証明書を提示すること。 なお、ISO27001にデータ消去が未規定の場合、サービス終了までに規定し、認証を受けること。	必須			
	1.28.	セキュリティ監査	情報セキュリティ監査の受入れが行われていること。	任意			