

福岡市文化財総合サイト構築・運用業務委託仕様書

1 委託件名

福岡市文化財総合サイト構築・運用業務委託

2 履行期間

契約締結日から令和9年3月31日まで

※令和9年4月以降は、CMS・サーバの保守メンテナンス及びサイトの管理運営を行なうこと（別途契約締結予定）

3 履行場所

経済観光文化局文化財活用部文化財活用課（以下「発注者」とする）

4 事業の目的

福岡市文化財総合サイト構築・運用業務委託（以下、「本業務」とする）

は、市内の歴史・文化財等の情報を一元的に整理する「福岡市文化財総合サイト」（以下「本サイト」とする）を新たに構築するものである。

「福岡市の文化財ホームページ」（以下「現サイト」とする）は構築から10年以上が経過し、ウェブアクセシビリティ規格やスマートフォンでの閲覧に対応していない。また、使用目的が多岐にわたり、サイト内の構造が煩雑化しているため、閲覧者・職員双方にとって利用しにくい状態となっている。加えて、現在公開中のコンテンツは専門性が高いため利用者層が限られ、市民や観光客に対し本市が交流の拠点として育んできた歴史や文化の魅力が伝わりにくい点も課題である。

本業務では、こうした課題を解決し、閲覧者が見やすく使いやすいサイトの実現を目指す。加えて、文化財を単なる情報として提示するのではなく、その価値やつながりをストーリーとして発信し、見るだけでなく「実際に訪れたいくなる」サイトにすることで、より幅広い層に向けて文化財への理解や適切な保存、観光・教育への活用を促進することを目的とする。

5 委託業務の内容

本業務の対象は、福岡市の文化財ホームページ（<https://bunkazai.city.fukuoka.lg.jp/>）を中心とし、同一ドメインを共有して運用されている関連サイト（福岡市埋蔵文化財センターHPは除く）を含むものとする。

本仕様書において「発注者と協議のうえ決定」と記載している事項については、受注者が基本案を作成・提示し、発注者は原則として内容確認および承認を行うものとする。受注

者は、前述の4に記載の内容を踏まえ、発注者と十分に協議しながら、以下の業務を行うこと。

(1) 本業務全体の実施計画及び管理

受注者は、本業務における具体的な体制、スケジュール等を記載した実施計画書を作成すること。

また、本業務の実施にあたっては、必要に応じて発注者との協議を適宜開催し、進捗や課題等について管理・共有すること。協議の開催頻度や方法等の詳細については、発注者と協議のうえ決定するものとする。

(2) 現状分析及びリニューアルサイト全体の企画・設計

①現状分析

現サイト及び、同一ドメイン配下で運用されている関連サイトについて、サイト構成、コンテンツ内容、CMS及び管理・保守体制等の現状分析を行い、課題の整理を行うこと。分析にあたっては、他都市の文化財紹介サイト、観光サイト等の事例を参照すること。移行対象とするページ、機能及びコンテンツの範囲については、現状分析の結果を踏まえ、発注者と協議のうえ決定するものとする。

②リニューアルサイト全体の企画・設計

現状分析の結果及び以下に挙げる想定される利用者層、リニューアル方針を踏まえたうえで、リニューアルサイト全体の企画・設計を行うこと。

<想定される利用者層>

- ア 文化財に深い関心を持つ層
- イ 観光資源としての文化財に興味を持つ層
(ファミリー層・若年層・観光客など)
- ウ 文化財を利用、又は遺跡内での土木工事を行う事業者等

<リニューアル方針>

- ア 不正アクセス、データの改ざん、コンピュータウイルスやワームなどの不正プログラムの侵入を防止するため、情報セキュリティ対策が施された信頼性の高いサイトにする。
- イ 市共用サーバではなく、新たに用意する外部サーバに移行すること。
- ウ 専門知識がない市職員であっても、ページの作成・更新が容易にできるよう、分かりやすくシンプルな運用・管理とすること。
- エ ウェブアクセシビリティに対応した、利用者にとって使いやすい設計にすること。
- オ 「文化財に深い関心を持つ層」、「文化財を利用、又は遺跡内での土木工事を行う事業者等」向けに、既存のコンテンツをリニューアルしつつ、「観光資源としての文化

財に興味を持つ層」向けに気軽に文化財に親しむことのできる新規コンテンツを作成すること。

カ 文化観光や文化財の活用に資する情報の公開・蓄積を行うこと。

(3) システム環境の構築

システム環境の構築にあたっては、以下の事項及び別紙1「非機能要件一覧」の内容を満たすこと。

①基本要件

- ・システム利用時間は、原則として24時間365日とする。ただし、保守等の予定された停止に関してはこの限りでない。
- ・サイトの各ページの表示速度は通常時において3秒以内を目標とすること。
- ・イベント開催時や各種広報等によりアクセスが集中する場合であっても、本サイトが著しく表示遅延または停止することのないよう、アクセス集中を考慮した構成及び性能を確保すること。
- ・ブラウザのみで利用できるものとし、専用ソフトウェアのインストールが不要なシステムとすること。
- ・一般的なブラウザ（Edge、Firefox、Chrome、Safari、各最新版）で閲覧可能なものとする。
- ・再構築後も同じURLを使用すること。
- ・サーバ移行に伴いURLが変更となるサイトについては、リダイレクト設定を行うこと。なお、設定方法および実施主体については、旧URLが存在するサーバ環境や管理主体を踏まえ、関係事業者間で調整のうえ決定すること。
- ・検索エンジンで上位に表示されるよう、SEO対策を講じること。
- ・GA4など、汎用的なアクセス解析ツールを用いて本サイトのアクセス解析ができること。
- ・本市情報セキュリティポリシー等の規定を遵守し、必要な対策を講じること。

②サーバ及びネットワーク環境

- ・本サイトの構築に必要なハードウェア、ソフトウェア、ネットワーク機器、各種サービス（レンタルサーバやクラウドサービス、インターネットプロバイダなどのサービスを含む）を受注者側にて用意すること。
- ・市の共用サーバは利用せず、別紙1「非機能要件一覧」に定める条件を満たす外部サーバ環境を利用すること。
- ・外部サーバに移行するサイトは、本サイトおよび同一ドメインを共有して運用されている関連サイト（福岡市埋蔵文化財センターHPは除く）である。
- ・データセンターについては、国内のサービスを利用すること。

<データセンター要件>

データセンターサービスを提供する事業者にて、情報セキュリティマネジメントシステム（ISMS）適合性評価制度に基づく ISMS 認証又はそれと同等の認証を取得された環境を利用すること。

また、データセンター内にて、当該業務を行う場所及び情報を保管する施設その他情報を取り扱う場所において、入退室の規制及び防犯対策その他必要な情報セキュリティ対策を講じること。

③システム（CMS）

- ・機能拡張性及び保守性の高いシステムとすること。
- ・CMS の構成については、運用効率および管理性の向上を目的として整理することを想定し、発注者と協議のうえ決定するものとする。
- ・システム稼働後 5 年間はサポートが行われること。
- ・システムの構築にあたり必要となる開発ソフトウェア等は受注者にて用意すること。
- ・提案にあたっては、初期構築および運用開始までの期間内で実現可能な構成であることを前提とすること。

④システムの管理

- ・CMS の運用・管理においては、ID ごとにアクセス制限（権限管理）を行い、権限外の操作を防止すること。ID の一括登録および初期設定は受注者が行うこと。ID 数や権限設計については、発注者と協議のうえ整理するものとする。
- ・管理画面には各職員の端末から ID 及びパスワード認証によりログインできること。合わせて二段階認証等の外部からの不正ログインを防止する対策を実施すること。
- ・CMS（付随するソフトウェア等含む）は、ID 数や端末台数、ページ数等の増加によって、ライセンス料が変動しないこと。
- ・ID を複数作成する場合は、ログインする ID の権限に応じた管理画面が表示されること。
- ・サイト管理者を除き、ページ一覧には編集する権限のあるページのみ表示されること。

⑤ページの作成

- ・本市職員によるページの修正・更新を基本としつつ、その範囲や権限の考え方については、サイト全体の管理・運用体制を踏まえ、発注者と協議のうえ整理すること。
- ・HTML や CSS 等の専門知識が無い職員であっても、ページの作成・更新が容易にできるよう、シンプルで分かりやすい管理画面とすること。
- ・複数の職員がページの作成・更新をしても、サイト全体のトーン&マナーが揃うようなページテンプレートを用意すること。
- ・アップロードできる画像・ファイルの形式（jpeg、png、pdf、docx 等）及び容量を制限できること。容量を超える場合、画像の自動リサイズができること。難しい場合は警告表示を表示させること。

- ・ ページごとに OGP 画像を設定できること。
- ・ 作成中のページについて、掲載画面がイメージできるようプレビュー機能を設けること。また、できる限り画面表示に近い状態でページを印刷できることが望ましい。
- ・ ページ公開前に、機械的なアクセシビリティチェック（画像の代替テキスト、機種依存文字、全角英数字の有無等）ができること。

⑥セキュリティ対策

- ・ 通信の暗号化（常時 SSL 化）を行うこと。暗号化に必要なサーバ証明書に関しても受注者側が準備すること。利用期間は 5 年間とし、利用期間満了後の継続については、発注者・受注者協議の上、別途契約を締結するものとする。
- ・ 本サイトにおいて個人情報を含む入力フォームを設置する場合は、本市の規定を遵守すること。また、個人情報を保存する場合は、保存期間及び管理方法を明確にし、保存期間経過後のデータは適切に削除又は無効化できること。
- ・ 個人情報の保存の有無、管理方法については発注者と協議のうえ決定するものとする。
- ・ サーバログ及びアクセスログを常時取得し、障害対応等の必要に応じて解析ができるようにすること。
- ・ ホームページの改ざんを検知する機能や WAF 等のセキュリティ対策を実施すること。
- ・ 別紙 2 「ウェブアプリケーションのセキュリティ実装チェックリスト」をもとに、必要なセキュリティ対策を講じること。チェックリストの結果については発注者に提出するものとし、「未対策／対応不要」とした項目については、その理由を示すこと。

(4) リニューアルサイトの構築

リニューアルサイト全体の企画・設計に基づき、リニューアルサイトを構築すること。構築にあたっては、以下の事項を満たすこと。

①基本要件

- ・ 総務省の「みんなの公共サイト運用ガイドライン」に準拠した本サイトのウェブアクセシビリティ方針を作成し、本サイト上に公開すること。ウェブアクセシビリティ方針には、JIS 規格「JIS X 8341-3:2016」の適合レベルを明記するとともに、PC、スマートフォン、タブレット等の利用端末の別なく同一のアクセシビリティ水準を確保する方針を示すこと。
- ・ ウェブアクセシビリティの規格「JIS X 8341-3:2016 の適合レベル AA」に準拠させること。

【参考 URL】

https://www.soumu.go.jp/main_sosiki/joho_tsusin/b_free/guideline.html

- ・ 表示言語は日本語とする。

②デザイン・導線

- ・原則、サイト全体で統一したデザインとすること。ただし、同一ドメイン配下で運用されている関連サイトについては、各サイトの役割や既存のデザインとの整合性を考慮し、必要な場合は適宜修正を行うこと。
- ・デザインや配色、文字のフォント・大きさなどは、「デジタル庁デザインシステム」を参考にしたうえで、誰にとっても見やすいものとする。

【参考 URL】 <https://design.digital.go.jp/>

- ・トップページを含む各ページのデザインには、本市の歴史文化が持つストーリーを想起させる視覚的な表現（画像、イラスト、アニメーション、アイコン等）を活用し、閲覧者が直感的に理解できるとともに、実際に現地に訪れてみたいと感じられるような表現・構成とすること。
- ・よかなび (<https://yokanavi.com/>) などの観光サイトにコンテンツを提供することを想定した、汎用性のあるデザインにすること。
- ・ユーザーからのアクセスは基本的にスマートフォンからを想定しているが、PC、タブレット端末等、今後新しく出現するものも含めて、異なるデバイスからアクセスがあった場合でも、最適な状態で表示・操作ができるように設計すること。
- ・ナビゲーションメニューは必要最小限にし、ユーザーが直感的に必要な操作が行えるよう誘導すること（例：「調べる」「訪れる」「申請する」などの大まかな目的に応じた入り口を3つ程度設ける等）。
- ・災害時や施設休館等の緊急・重要情報については、職員が操作できるものとし、確実にユーザーに届くよう、目立つデザインにすること。
- ・トップページ上部にナビゲーションメニューや緊急情報等を表示し、スクロールの必要なく次の操作に移れるよう誘導すること。
- ・ページのカテゴリ分類や階層構造は、ユーザーが必要な情報に辿り着きやすいよう設定すること。また、目的とするページに、原則1〜3クリックで辿り着くことを目的とするが、利用者動線やコンテンツ量を踏まえて提案すること。
- ・福岡市埋蔵文化財センター (<https://bunkazai.city.fukuoka.lg.jp/maibun/>) や福岡市博物館 (<https://museum.city.fukuoka.jp/>)、ふくおか歴史文化遺産ウィーク (<https://fukuoka-heritage-week.jp/>)、よかなび (<https://yokanavi.com/>)、FUKUOKA CITY Official Tourist Guide(<https://gofukuoka.jp/>)などの関連サイトと閲覧者が双方向的に移行できるようデザイン、表示等を設計すること。

③コンテンツの移行

- ・(2)①で整理した移行対象ページについて、リニューアル後のカテゴリ分類や階層構造に合うよう必要な修正を加えたうえで、移行作業を行うこと。
- ・移行対象ページについては発注者と協議の上決定すること。
- ・HTML ファイルや添付ファイル等のデータについては、受注者が本サイトの公開デー

タから取得作業を行うこと。

- ・ 移行後もページの編集や公開・削除作業が行える状態とすること。
- ・ 移行に伴い、ページデザインが崩れる等の問題が生じた場合は、受注者側で修正を行うこと。
- ・ 文化財情報検索では、時代、テーマ、エリア、キーワード、文化財種別等に応じた、自由度の高い検索を可能とし、その具体的な検索条件の範囲や拡張内容については、発注者と協議のうえ整理すること。
- ・ 文化財詳細ページでは、名称、概要、指定区分、所在地、写真等の基本情報に加え、関連性のある資料や近隣の遺跡の情報をプッシュ型で提示すること。
- ・ 遺跡内での土木工事、撮影、画像利用等に関する各種手続きについては、利用者にとって分かりやすい形で申請が行えるよう申込ページを設け、必要に応じて申請フォームを作成すること。また、AI等の技術を活用し手続きの流れや必要書類等を分かりやすく案内する仕組みを提案すること。対象とする手続きの範囲や提案した仕組みの導入の可否については、発注者と協議の上、決定する。
- ・ 福岡市歴史文化情報データベース（現在約 20 万件登録）については、書籍情報（画像は除く）のみを移行すること。移行後の確認方法については、発注者と協議のうえ決定する。

④新規コンテンツの作成

「観光資源としての文化財に興味を持つ層」に向けて、下記のコンテンツを作成すること。なお、これらの機能やコンテンツについては、優先度や実施範囲を整理したうえで、段階的な実装や将来的な拡張も視野に入れ、発注者と協議のうえ対応方針を決定するものとする。

- ・ 市内の文化財関連施設（展示館やガイダンス施設など）の情報一覧を作成すること。また、情報に変更があった際に直ちに対応できるよう、市職員が編集可能なページとすること。
- ・ 本市の歴史を概観できる年表を作成すること。
- ・ 市内の主要遺跡や文化財を紹介するページ（イラスト付き、7 ページ以上）を作成し、上記の年表とリンク等で連帯させること。
- ・ 本市作成のデジタルマップ、動画、3D モデルを掲載するページを作成すること。その際、新たに作成する上記コンテンツを適宜掲載できるような拡張性を持たせること。なお、各データの本サイト内への保存は基本的に想定しないものとし、その掲載方法については適切な方法を発注者と協議のうえ決定すること。

⑤独自提案

下記の項目について、本事業の目的達成に資する有効なデザイン・機能等を1つ以上提案すること。

- ・文化財関連ページでの関連遺跡・資料の紹介方法（例：GPS や AI 等を活用した周辺遺跡の紹介、閲覧履歴に基づく関連情報の提示など）
- ・遺跡への来訪や市内の周遊性を促進する機能（例：モデルコースの生成など）
- ・閲覧者参加型の機能（例：クイズなど）
- ・AI を活用した利便性の向上、閲覧数の増加、誘客、周遊を促進するための仕組み
- ・文化財の魅力が伝わるような視覚表現、ページデザイン
- ・上記に示す仕様以外で、本事業の目的達成に資するもの

(5) サイトの移行及び公開

- ・現行サイトからリニューアルサイトへの移行期間については、発注者と協議のうえ決定すること。なお、データ移行や設定等、移行に伴う作業は、原則受注者が実施すること。
- ・移行対象ページが漏れなく移行されているか確認すること。なお、移行対象とするページや移行後の確認方法については、発注者と協議のうえ決定する。
- ・移行対象ページについて、移行期間中に更新されたページの差分反映については、発注者と協議のうえ決定すること。
- ・リニューアルサイトの公開前に、デモサイトを構築し、表示や動作を確認すること。また、発注者も確認できる状態とすること。
- ・公開にあたっては、サービスの停止期間ができる限り短くなるよう、発注者と協議の上、対応を決定すること。

(6) 運用・保守管理

①リニューアルサイトの運営

- ・リニューアルサイトの安定稼働のため、(3)②③で用意したハードウェア、ソフトウェア、ネットワーク機器、CMS 等について、定期保守やバージョンアップ反映（大幅な改修や工数が発生するものは除く）等の必要な対応を行うこと。

②操作支援

- ・ページの作成・承認に関する分かりやすい操作マニュアルを作成すること。画面イメージを表示する、分かりやすい表現で記載する等により、専門的知識を持たない職員であっても、ページの作成や更新、公開に関する一連の流れが理解できるようにすること。
- ・操作マニュアルは管理画面上で参照できることが望ましいが、難しい場合には代替方法を発注者と協議のうえ決定するものとする。
- ・職員からの操作方法等に関する問い合わせについて、対応できる体制の確保及び窓口を設置すること。

③アクセスログの取得

- ・リニューアルサイト公開後、各ページのアクセス件数等を取得すること。

④バックアップの実施

- ・定期的にデータのバックアップを実施すること。

⑤障害対応

- ・障害が発生した場合、発注者と密に連携し、早期にシステムを復旧すること。
- ・同一事象及び類似事象の発生を防止するため、原因究明や再発防止策の検討・実施等を行うこと。

⑥サービスの中断に関する項目

- ・構築したシステムの他社への引継ぎについては、最大限の努力を行うこととする。

7 サイトの公開時期

令和9年3月下旬の公開を予定

8 納品物

下記の項目について、各1部納品すること。

項目	提出方法	補足
①本件 Web サイト一式	データ	本要件に準じた Web サイトの公開をもって納品とする。
②実施計画書	データ	体制図、全体スケジュール等を記載
③リニューアルサイト設計書	データ	
④システム・ネットワーク構成図	データ	
⑤緊急時の連絡体制図	データ	
⑥ウェブアプリケーションのセキュリティ実装チェックリスト	データ	チェック結果を記載
⑦ウェブアクセシビリティ方針	データ	ページを作成し、公開することをもって納品とする
⑧移行対象ページ一覧	データ	
⑨デザインデータ	データ	
⑩操作マニュアル	データ、紙	

9 納品物の帰属等

- (1) 納品物の著作権その他関係情報の一切の権利は発注者に帰属するものとする。
- (2) 受注者は、納品物に係る著作者人格権を行使しないものとする。また、受注者は、本委託における納品物の制作に関与した者について、著作権を主張させず、著作者人格権についても行使させないことを約するものとする。

- (3) 発注者は納品物の一部について差替え、削除及び追加の必要が生じた場合には、受注者以外の事業者へ委託、または発注者自身でその改変を行うことができるものとする。
- (4) 発注者は、納品物を他の広報物に使用できるものとする。また、発注者が認める場合に、受注者は第三者による映像等の使用を了承するものとし、使用料がかからないこととする。
- (5) 上記(4)の場合において、受注者以外の著作権者の許諾が必要な場合には、受注者がその手続きを行うものとする。
- (6) 受注者は、納品物について、第三者の商標権、肖像権、著作権その他の諸権利を侵害するものではないことを保証することとし、納品物について第三者の権利を侵害していた場合に生じる問題の一切の責任は受注者が負うものとする。
- (7) 著作権・肖像権処理等、権利関係に関する紛争が生じた場合は、受注者の責任において対応し、発注者は責任を負わないものとする。

10 その他留意事項

- (1) 委託内容等については、提案競技時点におけるものであり、契約締結の際、受注者と協議のうえ変更を加えることがある。
- (2) 本仕様書に定めのない事項及び疑義が生じた場合は、発注者と協議し、指示を受けること。
- (3) 業務の再委託に際しては発注者と協議を行うこと。
- (4) 別紙3「個人情報・情報資産取扱い特記事項」を遵守すること。
- (5) 本業務の全部を第三者に再委託することを禁止する。ただし、発注者の承認を得た場合はこの限りではない。
- (6) 受託者は、本業務を通じて知り得た情報を第三者に漏らしてはならない。契約終了後も同様とする。

非機能要件一覧

要件	対象	内容
可用性	稼働率	・本システムの稼働時間は、原則として24時間365日とすること。ただし、保守等の計画的な停止についてはこの限りではない。
	冗長化	・サーバ障害等が発生した場合に備え、バックアップ及び復旧手段を適切に講じること。 具体的な可用性対策の内容については、発注者と協議のうえ決定するものとする。
	アクセス集中時の耐性	・イベント開催時や各種広報等によりアクセスが集中する場合であっても、著しい表示遅延またはサービス停止が発生しないよう、アクセス集中を考慮した構成及び性能を確保すること。
	RPO (目標復旧地点)	・平常時、営業停止を伴う障害が発生した際には、障害発生地点（日次バックアップ+アーカイブからの復旧）までのデータ復旧を目的とすること。
性能要件	オンラインレスポンスタイム	・オンラインレスポンスタイムは、3秒以内を目標とすること。なお、業務に支障のない状態を確保できるよう構築すること。
セキュリティ要件	セキュリティポリシー等	・本システムの構築・運用に際しては、本市の「福岡市情報セキュリティ管理規程」及び「福岡市情報セキュリティ対策基準」といった情報関連規程等を遵守し、万全の対策を講じること。
	機密性の確保	・庁内外からの不正な接続及び侵入、行政情報資産の漏えい、改ざん、消去、破壊、不正利用等を防止するための対策を講じること。
	ウイルス対策	アンチウイルスソフトウェアを活用する等により、以下の不正プログラム対策を講じること。 ・定時スキャン設定のみならず、個別ファイルをアクセスする都度スキャンが可能な機能を設けること。 ・データ送受信時にウイルスチェックが可能な機能を有すること。 ・最新のエンジン及びパターンファイルの自動更新が可能な機能を有すること。 ・常時監視機能の設定が可能であること。 ・ウイルス感染・検疫・駆除の一元監視機能を有すること。 ・本ホームページは、ウイルスやマルウェア等に対する対策を講じること。
	ドメイン管理	・ホームページのURLにて使用しているドメイン情報は本市専用のものとする。
	セキュリティレベルの維持	・確保すべきセキュリティ実装の詳細に関しては、「別紙2 ウェブアプリケーションのセキュリティ実装チェックリスト」にて提示するので、必要な対策を講じること。
	暗号化	・通信データに対して暗号化を行う機能を設けること。 ・通信経路上の暗号化（常時SSL暗号化通信）を行うこと。 ・個人情報を含む等、機密性の高い情報を取り扱う場合、蓄積データ（データベース含む）や職員への通報経路を含め暗号化を行うこと。なお、暗号化の各機能や強度については、設計時に決定する。
	個人情報を含むフォームの管理	・本サイトにおいて個人情報を含む入力フォームを設置する場合は、本市の規定を遵守すること。また、個人情報を保存する場合は、保存期間及び管理方法を明確にし、保存期間経過後のデータは適切に削除又は無効化できること。 ・個人情報の保存の有無、管理方法については発注者と協議のうえ決定するものとする。
	ログ対応	・サーバログについて、取得できること。 ・システムログ及びアプリケーションログを取得し、取得したログの漏えい、改ざん、消去、破壊等を防止できる機能を設けること。 ・Webサイトへの負担を考慮した上でアクセスログを取得し、発注者が要請した場合、直ちにアクセスログの提示が可能な機能を設けること。
運用・保守性	バックアップ	・障害時等にシステムを復旧できるようなバックアップを実施すること。 ・作成したWebサイトコンテンツファイル等関連データは、環境変更時（情報更新時）バックアップを取得すること。
	世代管理	・バックアップデータは業務上の必要性を加味した上で、複数世代で取得すること。
	復元	・RPO（目標復旧地点）までデータを復元できるよう構築すること。
	監視	・セキュリティ機能の稼働状況監視や、エラー監視を実行し、必要に応じて警告等を発する機能を設けること
使用性・効率性	アクセシビリティ対応	・総務省の「みんなの公共サイト運用ガイドライン」に準拠した本サイトのウェブアクセシビリティ方針を作成し、公開すること。ウェブアクセシビリティ方針には、JIS規格「JIS X 8341-3:2016」の適合レベルを明記すること。 ・PC、スマートフォン、タブレット等の利用端末の別なく、同一のアクセシビリティ水準を確保すること。 ■みんなの公共サイト運用ガイドライン https://www.soumu.go.jp/main_sosiki/joho_tsusin/b_free/guideline.html
	SEO対応	・利用者の多い検索エンジンにおいて、福岡市の文化財等に関連するキーワードについて本市ホームページが上位に表示されるように対策を講じること。

■ ウェブアプリケーションのセキュリティ実装 チェックリスト (1/3)

No	脆弱性の種類	対策の性質	チェック	実施項目	解説
1	SQLインジェクション	根本的解決	※ <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> SQL文の組み立ては全てプレースホルダで実装する。	1-(i)-a
				<input type="checkbox"/> SQL文の構成を文字列連結により行う場合は、アプリケーションの変数をSQL文のリテラルとして正しく構成する。	1-(i)-b
		根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	ウェブアプリケーションに渡されるパラメータにSQL文を直接指定しない。	1-(ii)
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	エラーメッセージをそのままブラウザに表示しない。	1-(iii)
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	データベースアカウントに適切な権限を与える。	1-(iv)
2	OSコマンド・インジェクション	根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> シェルを起動できる言語機能の利用を避ける。	2-(i)
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> シェルを起動できる言語機能を利用する場合は、その引数を構成する全ての変数に対してチェックを行い、あらかじめ許可した処理のみを実行する。	2-(ii)
3	パス名パラメータの未チェック /ディレクトリ・トラバーサル	根本的解決	※ <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> 外部からのパラメータでウェブサーバ内のファイル名を直接指定する実装を避ける。	3-(i)-a
				<input type="checkbox"/> ファイルを開く際は、固定のディレクトリを指定し、かつファイル名にディレクトリ名が含まれないようにする。	3-(i)-b
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	ウェブサーバ内のファイルへのアクセス権限の設定を正しく管理する。	3-(ii)
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	ファイル名のチェックを行う。	3-(iii)
4	セッション管理の不備	根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	セッションIDを推測が困難なものにする。	4-(i)
		根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	セッションIDをURLパラメータに格納しない。	4-(ii)
		根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	HTTPS通信で利用するCookieにはsecure属性を加える。	4-(iii)
		根本的解決	※ <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> ログイン成功後に、新しくセッションを開始する。	4-(iv)-a
				<input type="checkbox"/> ログイン成功後に、既存のセッションIDとは別に秘密情報を発行し、ページの遷移ごとにその値を確認する。	4-(iv)-b
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	セッションIDを固定値にしない。	4-(v)
保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	セッションIDをCookieにセットする場合、有効期限の設定に注意する。	4-(vi)		

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。

■ ウェブアプリケーションのセキュリティ実装 チェックリスト (2/3)

No	脆弱性の種類	対策の性質	チェック	実施項目	解説	
5	クロスサイト・スクリプティング	HTMLテキストの入力を許可しない場合の対策	根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	ウェブページに出力する全ての要素に対して、エスケープ処理を施す。	5-(i)
			根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	URLを出力するときは、「http://」や「https://」で始まるURLのみを許可する。	5-(ii)
			根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<script>...</script> 要素の内容を動的に生成しない。	5-(iii)
			根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	スタイルシートを任意のサイトから取り込めるようにしない。	5-(iv)
			保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	入力値の内容チェックを行う。	5-(v)
		HTMLテキストの入力を許可する場合の対策	根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	入力されたHTMLテキストから構文解析木を作成し、スクリプトを含まない必要な要素のみを抽出する。	5-(vi)
			保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	入力されたHTMLテキストから、スクリプトに該当する文字列を排除する。	5-(vii)
		全てのウェブアプリケーションに共通の対策	根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	HTTPレスポンスヘッダのContent-Typeフィールドに文字コード(charset)の指定を行う。	5-(viii)
			保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	Cookie情報の漏えい対策として、発行するCookieにHttpOnly属性を加え、TRACEメソッドを無効化する。	5-(ix)
			保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	クロスサイト・スクリプティングの潜在的な脆弱性対策として有効なブラウザの機能を有効にするレスポンスヘッダを返す。	5-(x)
6	CSRF (クロスサイト・リクエスト・フォージェリ)	根本的解決	※ <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> 処理を実行するページを POST メソッドでアクセスするようにし、その「hidden パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行する。	6-(i)-a	
				<input type="checkbox"/> 処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。	6-(i)-b	
				<input type="checkbox"/> Refererが正しいリンク元かを確認し、正しい場合のみ処理を実行する。	6-(i)-c	
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	重要な操作を行った際に、その旨を登録済みのメールアドレスに自動送信する。	6-(ii)	
7	HTTPヘッダ・インジェクション	根本的解決	※ <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> ヘッダの出力を直接行わず、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用APIを使用する。	7-(i)-a	
				<input type="checkbox"/> 改行コードを適切に処理するヘッダ出力用APIを利用できない場合は、改行を許可しないよう、開発者自身で適切な処理を実装する。	7-(i)-b	
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	外部からの入力の全てについて、改行コードを削除する。	7-(ii)	

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。

■ ウェブアプリケーションのセキュリティ実装 チェックリスト (3/3)

No	脆弱性の種類	対策の性質	チェック	実施項目	解説
8	メールヘッダ・インジェクション	根本的解決	※ <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> メールヘッダを固定値にして、外部からの入力はずべてメール本文に出力する。	8-(i)-a
				<input type="checkbox"/> ウェブアプリケーションの実行環境や言語に用意されているメール送信用APIを使用する(8-(i))を採用できない場合)。	8-(i)-b
		根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	HTMLで宛先を指定しない。	8-(ii)
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	外部からの入力の全てについて、改行コードを削除する。	8-(iii)
9	クリックジャッキング	根本的解決	※ <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> HTTPレスポンスヘッダに、X-Frame-Optionsヘッダフィールドを出力し、他ドメインのサイトからのframe要素やiframe要素による読み込みを制限する。	9-(i)-a
				<input type="checkbox"/> 処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。	9-(i)-b
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	重要な処理は、一連の操作をマウスのみで実行できないようにする。	9-(ii)
10	バッファオーバーフロー	根本的解決	※ <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> 直接メモリにアクセスできない言語で記述する。	10-(i)-a
				<input type="checkbox"/> 直接メモリにアクセスできる言語で記述する部分を最小限にする。	10-(i)-b
		根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	脆弱性が修正されたバージョンのライブラリを使用する。	10-(ii)
11	アクセス制御や認可制御の欠落	根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	アクセス制御機能による防御措置が必要とされるウェブサイトには、パスワード等の秘密情報の入力が必要とする認証機能を設ける。	11-(i)
		根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	認証機能に加えて認可制御の処理を実装し、ログイン中の利用者が他人になりすましてアクセスできないようにする。	11-(ii)

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。

別紙「個人情報・情報資産取扱特記事項」

1 基本的事項

受託者は、この契約に基づき委託された業務（以下「委託業務」という。）を実施するに当たっては、個人情報の保護に関する法律（平成15年法律第57号。以下「法」という。）、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号。以下「番号法」という。）、福岡市情報セキュリティに関する規則（平成23年福岡市規則第51号）及び情報セキュリティ共通実施手順その他関係法令を遵守し、個人情報（個人番号及び特定個人情報を含む。）及び情報資産の機密性、完全性、可用性を損なうことのないよう、個人情報及び情報資産を適正に取り扱わなければならない。特に個人情報については、法第66条第2項において、受託者に行政機関等と同様の安全管理措置が義務付けられていることから、その保護の重要性を認識し、適正に取り扱わなければならない。

2 定義

（1）個人情報

法第2条第1項に規定する個人情報をいう。

（2）個人番号

番号法第2条第5項に規定する個人番号をいう。

（3）特定個人情報

個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード（住民基本台帳法（昭和42年法律第81号）第7条第13号に規定する住民票コードをいう。）以外のものを含む。）をその内容に含む個人情報をいう。

（4）情報資産

次に掲げるものをいう。

- ・ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体
- ・ネットワーク及び情報システムで取り扱う情報（OAソフトウェアで取扱われるファイルを含む）並びにそれらを印刷した文書
- ・ネットワーク及び情報システムに関連する文書

（5）機密性

情報の利用を認められた者だけがその情報を利用することができることをいう。

（6）完全性

情報が破壊、改ざん又は消去されていないことをいう。

（7）可用性

情報の利用を認められた者が、必要な場合に中断されることなく、情報を利用することができることをいう。

3 秘密保持

受託者は、委託業務に係る個人情報並びに情報資産及び情報資産に関する情報を他人に知らせてはならない。この契約が終了し、又は解除された後においても同様とする。

4 従業者の監督等

受託者は、その従業者に委託業務に係る個人情報及び情報資産を取り扱わせるに当たっては、取り扱う従業者を書面で報告するとともに当該個人情報及び情報資産の安全管理が図られるよう、次に掲げる事項を周知し、その他必要かつ適切な監督及び教育を行わなければならない。

- ・委託業務に係る個人情報及び情報資産について、その適正な取扱い及び機密性、完全性、可用性の維持に必要な事項を遵守すること。
- ・個人情報を正当な理由なく利用したり、他人に提供したり、盗用した場合、法及び番号法に規定する罰則が適用される場合があること。
- ・上記の各事項は、委託業務に従事中のみならず、従事しなくなった後も同様であること。
- ・従業者の情報資産へのアクセス権限は、担当業務の内容に応じた最小限の権限に限定するとともに、取扱う情報資産の重要度に応じて複数人による確認の実施等を行うこと。

5 作業場所の制限

受託者は、定められた履行場所以外で委託業務に係る個人情報及び情報資産を持ち出し、又は取り扱ってはならない。ただし、福岡市（以下「市」という。）の書面による承認があるときは、この限りではない。

6 収集に関する制限

受託者は、委託業務の実施に当たって個人情報を収集するときは、この契約の目的を達成するため必要な範囲内で、適法かつ公正な手段により行わなければならない。

7 使用及び提供に関する制限

受託者は、委託業務以外の目的のために委託業務に係る個人情報及び情報資産を利用し、又は第三者へ提供してはならない。ただし、市の書面による承認があるときは、この限りではない。

8 安全確保の措置

受託者は、委託業務に係る個人情報及び情報資産の適切な管理のために、市が求める個人情報保護及び情報セキュリティの体制を備えるとともに、その他必要な措置を講じなければならない。

9 複写、複製又は加工の制限

受託者は、委託業務に係る個人情報及び情報資産が記録された文書、電磁的記録等を複写、複製又は加工してはならない。ただし、市の書面による指示又は承認があるときは、この限りではない。

10 再委託の制限

受託者は、委託業務に係る個人情報及び情報資産については、自ら取り扱うものとし、第三者に当該個人情報及び情報資産の取扱いを委託してはならない。ただし、市の書面による承認があるときは、この限りでない。なお、市の承認により第三者に委託する場合は、当該第三者に対して、契約書及び特記事項に規定する個人情報及び情報資産の取扱いの義務を遵守させるものとする。

11 委託業務終了時の返還、廃棄等

受託者は、この契約が終了し、又は解除されたときは、委託業務に係る個人情報及び情報資産を、市の指示に従い、市に返還し、若しくは引き渡し、又はその廃棄、消去等を行わなければならない。なお、廃棄又は消去等をしたときは、廃棄又は消去等を行った旨の証明書を提出しなければならない。

12 報告及び監査・検査の実施

市は、受託者における委託業務に係る個人情報及び情報資産の取扱いの状況について、契約内容の遵守を確認するため、年に1回以上、原則として実地検査を行うほか、定期的に書面による報告を求め、必要に応じて監査又は検査をすることができる。

なお、実地検査を行うに当たっては、別添「個人情報・情報資産の委託先監督チェックリスト」により確認を行うものとする。

13 事故等発生時の報告

受託者は、個人情報及び情報資産の機密性、完全性、可用性を損なう、又は損なうおそれのある事故並びに欠陥及び誤動作を発見したときは、直ちに市に報告し、市の指示に従わなければならない。

14 事故等発生時の公表

市は、個人情報及び情報資産の機密性、完全性、可用性を損なう事故等が発生した場合、市民に対して適切な説明責任を果たすために必要な当該事故等の情報の公開を行うことができる。

15 契約の解除及び損害の賠償

市は、受託者がこの特記事項の内容に違反したときは、この契約の解除及び損害賠償の請求をすることができる。この場合において、受託者に損害を生じることがあっても、市はその責めを負わないものとする。

決 裁	課長	係長	担当者

個人情報・情報資産の委託先等監督チェックリスト

このチェックリストは、契約書添付の「個人情報・情報資産取扱特記事項」の各項目に関し、委託先等において適切に実施されていることを確認するためのものです。実地検査を行う場合は、このチェックリストに基づいて、委託先等の安全管理措置状況を確認してください。

契約件名		確認者	
委託先等		補助者	

適→○ 否→× 該当なし→/

確認項目		確認結果	実施日	確認内容
1	組織体制等	①個人情報等の管理体制を確認		
		ア.個人情報等の取扱責任者や取り扱う担当者は明確になっているか。		
		イ.取り扱う文書・データの種類、個人情報等の記載項目は明確にされているか。		
		②漏えい事故等発生時の体制を確認		
		ア.委託業者内での報告体制は明確になっているか。		
		イ.委託業者から市への報告体制は明確になっているか。		
		③従事者に対する研修の実施状況を確認		
		ア.研修資料、対象者、実施回数は適切か。		
		④業務の再委託は原則として認められないことを踏まえた確認		
		ア.業務の再委託を行う場合、市からの承諾を得ているか。		
		イ.再委託先で個人情報の取り扱いがある場合、再委託先でも同等の措置が行われることを確認しているか。		
		2	作業場所、 保管場所	①個人情報等を取扱う作業場所を確認
ア.個人情報等を取り扱う区域や場所を明確に定めているか。				
イ.入退室管理を適切に行っているか。				
ウ.十分なスペースが確保され、整理整頓されているか。				
②個人情報等の保管場所を確認				
ア.個人情報等の保管場所・保管方法は適切か。（個人番号が記載された書類は、施錠できる場所に保管しているか。）				
イ.USBメモリ等の電磁的記録媒体を使用する場合、施錠できる場所に保管されているか。				
ウ.本契約に関係のない他の書類、電磁的記録媒体等と区分されているか。（自社のものや他契約のもの）				
③個人情報を含むデータの保存場所や取り扱いの状況を確認				
ア.個人情報等を含むデータが、アクセス権やパスワード等により、許可された者のみが閲覧できる場所に適切に保存されているか。				
イ.サーバーおよび端末において、修正プログラムが適切に適用され、ウイルス対策ソフトが最新状態で運用されているか。				

3	個人情報の収受、利用	①漏えい等の事故を防止するための対策を確認		
		ア.個人情報等の収受や送付について、記録等の管理が行われているか。(日時・書類名・担当者等)		
		イ.郵送時に、封入物のダブルチェックをするなど誤送付対策が適切に行われているか。		
		ウ.メール送信時には、事前に複数人で確認するなど誤送付対策が適切に行われているか。		
		エ.WEBへの公開時には、事前に複数人で確認するなど公開情報の確認等の対応を行っているか。		
		②作業場所以外への持ち出し時の安全対策を確認		
		ア.契約書等で定められた場所以外に持ち出しを行っていないか。持ち出す場合は、市に書面で承認を得ているか。		
		イ.持ち出す場合、責任者に許可をとるとともに、日時、書類・データの名称、持出先、持ち出し者名などを記録しているか。		
		ウ.施錠可能なバッグを使用するなど、紛失・盗難対策を行っているか。		
		エ.USBメモリ等でデータを持ち出す場合、暗号化やパスワード設定を行っているか。		
		③業務目的以外での利用、外部提供、複製を確認		
		ア.業務以外の目的で複製や加工を行う場合、市に書面で承諾を得ているか。		
イ.業務以外の目的外利用をする場合(自社の営業活動など)、市に書面で承諾を得ているか。				
4	返還・廃棄・消去	①個人情報の返還や廃棄が適切に行われていることを確認		
		(個人情報をもとに返還する場合) ア.返還が必要な書類や電磁的記録媒体等の引き渡しを受けたか。		
		(個人情報を委託業者で廃棄・消去する場合) イ.媒体に応じて適切な方法で、復元不可能な方式により廃棄等を行った旨の証明書は提出されているか。		

【確認要領】

- ① 特記事項に基づき、少なくとも年1回以上、原則として実地検査により確認を行ってください。
 ※委託先が遠隔地にある等の理由により現地に赴くことが難しいような事情がある場合は、例えばテレビ通話や写真等で管理の現況を確認するなど、代替方法により確実に検査を実施してください。
 ※確認項目1及び4については、提出された書類等の確認を持って検査に代えることもできますが、必要に応じて実地検査により確認を行ってください。
- ② 実地検査は原則として本契約の監督員が実施してください。やむを得ず監督員以外の者が実施する場合は、事前に所属長に承認を受けた者が実施してください。また、必要に応じて補助者を指名し、複数人で確認を行ってください。
- ③ 確認項目ごとに、確認結果及び実施日、確認内容を記載してください。
 【確認結果】 適→○ 否→× 該当なし→/ ※業務内容により確認する必要がない項目は「該当なし」を選択
 【実施日】 実地検査を行い確認した日を記載
 【確認内容】 実地検査において確認した内容(適否判定の根拠)を記載
- ④ 確認結果が「否(×)」の場合は、委託先等と協議の上、改善に要する期間を定め、改善を指導してください。
 また、改善結果を報告させるとともに、必要に応じて再度実地検査を実施するなどして、改善状況を確認してください。
 なお、改善が確認できた場合は、確認内容欄にその旨(再確認日・改善結果)を追記してください。
- ⑤ 全ての項目の確認が終了した後、課長まで決裁のうえ、契約の一件書類に編綴してください。

※ 業務内容に応じて項目の追加が必要な場合は、適宜確認項目を追加(行を追加)して実施してください。
 ただし、既存の確認項目について削除または改変する場合は、事前に情報セキュリティ統括管理者に協議が必要です。
 (情報セキュリティ共通実施手順8(1)①エ)