コンテンツ導入ガイドライン

第 1 版

目次

この文書について

この文書は、大阪観光局の WEB サーバにコンテンツを導入する際に守るべきルールを策定する。
このルールは、保守とセキュリティ確保の為に策定する為、サーバ側でプログラムを使用しないコンテンツについては該当しない。
この文書は、事前にサイトを統括して管理する担当者が、サイトすべてを表にして管理する書類（以後、サイト管理表と記述する。）を作成しておき、その書類の存在を前提とする。

構築前の決定事項

コンテンツ構築の前に下記を決めておき、大阪観光局の担当者、コンテンツ作成業者、保守担当者の3者間で周知しておく事。

- 対象サイトの有効期限
- 使用プログラム言語や、使用モジュール等
- コンテンツのライセンス
- ディスク使用量予測
- アプリケーションバージョンアップ時の動作確認体制

対象サイトの有効期限

サイトの公開期間と、バックアップとして残しておく有効期限を上記3者間で決めておき、サイト管理票に明記する。

使用プログラム言語や、使用モジュール等

使用プログラム言語と使用モジュールについては、保守性を念頭に置いて決定する事。

コンテンツのライセンス

オープンソースや有償のアプリケーションを使用する場合、そのライセンスを周知しておき、保守の観点から問題が無いか解決しておく事。
コンテンツ作成業者が作成するコンテンツについては、その権利を確認しておき、理想としてはコンテンツの権利を大阪観光局に譲渡される事が望ましい。
もし権利の譲渡が不可能である場合は、セキュリティ保持目的での改修をどうするかを解決しておく事。

ディスク使用量予測

概算でも良いので、コンテンツや DB にて使用するディスク使用量を計算しておく事。
ディスク使用量の項目としては、納品初期の状態を記載し、DB やログ、画像等の出力がある場合は年間での増加量も計算する事。

アプリケーションバージョンアップ時の動作確認体制

PHP や perl、MySQL 等のバージョンアップ時、動作確認を誰が担当し、連絡をどの様にするのかを決定しておく事。

セキュリティ確保の為の規約

SSL 通信の利用

個人情報や重要情報を通信する際には、SSL（HTTPS プロトコル）を利用すること。
さらに、非暗号通信（HTTP プロトコル等）にてアクセスしてきたユーザーには、SSLを利用したページにリダイレクトする等して、SSL 通信を強制すること。

管理者用のページのアクセス制限

サイトの変更が可能な管理画面が存在する場合、そのページについては、IP 制限を掛けて必要最低限の開放設定にしておくこと。

POST メソッドによるデータ送信

個人情報や重要情報を入力するページがある場合は、そのデータの送信に POST メソッドによる送信を利用すること。

入力内容のチェック処理

端末からサーバへの送信に入力項目やパラメータがある場合は、そのデータについて型や最大値、整合性のチェックを厳格にチェックする処理を組み込むこと。

ユーザーが入力した文字列の表示をエスケープする

ユーザーが入力した文字列データをブラウザに表示する場合、そのデータをエスケープしてクロスサイトスクリプティング攻撃を防止すること。

エラーページの簡素化

システムエラーや DB エラーが発生した場合に表示するエラーページは、できる限り簡素化してエラーの内容を詳細に表示してはいけない。

アップロードファイルのチェック機能

管理者以外のユーザーが画像や PDF 等のファイルをアップロードする機能がある場合は、アップロードしたファイルがいきなり公開されてはいけない。
アップロードされたファイルは、非公開ディレクトリやデータベースに格納し、一旦管理者がチェックする機構を作り、ファイルがアップロードされた場合は必ずウィルススキャンを実施してから、問題が無い場合に限って公開すること。

アップロードファイルの命名

ユーザーが入力した文字列を、アップロードファイルの命名に使用してはいけない。

本番環境に、テストページやバックアップファイルを置かない

本番環境には公開に必要なファイルだけを設置し、テストページや、更新前のバックアップファイル等は本番環境に置いてはいけない。

アクセス解析

アクセスを解析する為に、国内のサーバに設置するサイトについては Google アナリティクスのタグを導入し、中国のサーバに設置するサイトについては 百度ウェブマスターツールのタグを導入すること。
それぞれのタグについては、大阪観光局が指定するタグを使用すること。

脆弱性診断

サイトの脆弱性診断は、大阪観光局の保守担当者が公開前に脆弱性診断を実施し、サイト構築業者はその結果を受けて保守担当者が指摘する脆弱項目について修正すること。

サイトのプログラムが動作するページを変更する場合も、公開前に脆弱性診断を実施すること。

脆弱性診断において修正箇所が発生した場合、再度脆弱性診断を実施し、問題が解決するまで公開してはいけない。

納品物

コンテンツ作成業者は、コンテンツを導入にするに当って下記を納品する事。

- コンテンツファイル一式
- システムの仕様書
- 管理画面がある場合、そのマニュアル
- テスト結果報告書

コンテンツファイル一式

コンテンツファイルについては、WEB サーバに導入するファイル一式を、大阪観光局の担当者に提出する事。
画像やコンパイルした出力物がある場合、そのソースコードも提出する事。

システムの仕様書

仕様書の精度は概要レベルで良く、詳細な内部設計まで記述する必要はない。
仕様書の観点は、保守を実施するに当って必要な内容を記述する事。
保守担当者の技術レベルは、使用するプログラム言語を理解できている事を前提として記述する事。
記載する内容としては、下記の項目を必須とする。

- 使用言語と使用アプリケーション
- 配布物のディレクトリ構成と、そのディレクトリの概要説明
- バッチ処理がある場合、その実行時刻
- ログを出力している場合、その出力先
- サイト一式を削除する時の手順
- 画像を生成した場合、生成に使用したツールやフォント名

管理画面のマニュアル

管理画面や CMS を使用している場合、そのマニュアルを提出する事。

テスト結果報告書

各テスト操作を実施した時の結果（画面のキャプチャーや、出力内容）を添付する事。