

## JICA ウェブサイトのリニューアル・保守運用管理業務における 非機能要件/セキュリティ要件/その他要件

### 非機能要件

#### (1) ユーザビリティ及びアクセシビリティに関する要件

ユーザビリティ及びアクセシビリティに関する要件は以下のとおり。

##### (ア) ユーザビリティ

リニューアル後の JICA ウェブサイトでは、利用者を迷わせない、離脱させないよう、ユーザビリティの観点からサイト設計時に留意すべきポイントは主に以下の通り。

- ・ サイト内検索の機能を向上させる。
- ・ 可読性、操作性を向上させ、離脱率を低減し、サイトにおけるコンバージョン向上を図る。
- ・ レスポンシブデザインを利用し、モバイルデバイスからのアクセスに対応すること。

##### (イ) アクセシビリティ

第 2 階層までを JIS8341-3:2016 のレベル AA を目標とし、第 3 階層以降のコンテンツに関しては、優先的に対応する範囲を発注者と協議の上、運用・保守体制で対応可能な範囲を順次対応を行う。

#### (2) システム方式に関する要件

現行のサーバ環境及び実現内容について詳細を確認したうえで、各章に記載の非機能要件を踏まえ必要なシステム基盤の方針を提案すること。

なお、現行のサーバ環境及び実現内容については、別添 3「現行の JICA ウェブサイトのサーバ環境」を参照するとともに、受注後に必要な調査等を実施すること。

#### (3) 規模に関する要件

##### (ア) 静的な WEB コンテンツ

###### ① 現行コンテンツ容量

Web サーバには 100GB の静的な Web コンテンツが格納されており、メール・データベースサーバには、動的コンテンツを含め、39GB のデータが格納されている。

###### ② 現行ファイル数

Web コンテンツの内訳 (2020 年 12 月中旬時点)

<Web サーバ>

- ・ HTML (HTM) ファイル                    . . . 102, 597 ファイル
- ・ PDF ファイル                            . . . 94, 888 ファイル
- ・ 画像ファイル (gif, jpg, png 等) . . . 272, 390 ファイル
- ・ Word ファイル                           . . . 2, 339 ファイル
- ・ Excel ファイル                           . . . 1, 827 ファイル
- ・ PowerPoint ファイル                   . . . 108 ファイル

(イ) WEB アクセス数

Web サーバに対し、現在は最大月間 450 万ページビューのアクセス量が存在し、将来的には 1.5 倍程度のアクセス量が発生した場合でもサイト閲覧に遅延が生じないよう、サーバのスペック、ネットワーク帯域を確保すること。

(ウ) 利用者数

CMS 利用更新者としては、ユーザー数 300 名による更新を想定する。

(エ) 更新数

JICA ウェブサイトの更新実績 (2019 年度) は以下のとおり。

日本語版 : 1 ヶ月当たり約 1195 ページ

英語版 : 1 ヶ月当たり約 386 ページ

フランス語版 : 1 ヶ月当たり約 24 ページ

スペイン語版 : 1 ヶ月当たり約 8 ページ

(オ) リソース使用状況

リソース使用状況については、別添 3「現行の JICA ウェブサイトのサーバ環境」を参照すること。

(4) 性能に関する要件

(ア) オンラインレスポンス

閲覧者が JICA ウェブサイトにアクセスした際の応答速度について現行と同等以上の速度を実現するものであること。

(イ) CMS レスポンス

JICA 職員等が CMS を操作する際の応答速度について現行と同等以上の速度を実現するものであること。CMS の画面遷移、保存作業等について現行の CMS では概ね 1 件あたりおよそ 800,000 byte 程度の容量のデータを平均 3.5 秒程度で配信している。

**(5) 信頼性に関する要件**

以下を実現するための構成や方式の考え方について提案すること。その際の条件等も含めて、複数案の提示があっても良いこととする。

- ・ 障害に伴うシステム停止は、年 2 回以内、年間の合計停止時間は、30 分以内とすること。なお、停止時間については、システムメンテナンスによる停止時間は含まないが、システムメンテナンスの実施については、事前に発注者と合意すること。
- ・ 障害発生からの目標復旧時間を 30 分以内として、復旧を行う手順又は機能を設計すること。
- ・ Web コンテンツやデータベースなどのデータは、毎日バックアップを取得し、7 世代分を保管し、必要に応じてファイル単位でのデータリストアを可能とする仕組みを設けること。

**(6) 拡張性に関する要件**

以下を実現するための構成や方式の考え方について提案すること。その際の条件等も含めて、複数案の提示があっても良いこととする。

- ・ 将来、データ量が調達時に指定した量の 3 割増となっても再調達なく対応できるよう、データ記憶領域およびデータ保存領域に余裕を持たせること。
- ・ アクセス数についても 5 割増までは同等の性能が発揮できるように回線、ネットワーク機器、サーバ性能に余裕を持たせること。

**(7) 上位互換性に関する要件**

使用している OS やソフトウェア等のバージョンアップの際、必要な調査及び作業を実施することで、バージョンアップに対応可能なシステムとすること。また無償バージョンアップについては、原則運用費用内で実施すること。

なお、バージョンアップへの対応が技術的に困難等である場合、システム設計時に発注者と協議し、その指示に従うこと。

**(8) 中立性に関する要件**

- ・ 設計に当たっては、特定の事業者の設計技法に偏ることがないように標準的な設計技法を用い、仕様が更改されている柔軟性の高い技術を用いること。
- ・ 作成するドキュメント類が、第三者にも分かりやすく作成されること。

**(9) 継続運用に関する要件**

受注者はサイトのペネトレーションテスト等を含めた第三者による安全性検証試

験／セキュリティ診断を定期的実施し、結果を発注者へ報告すること。

## (10) 情報システム稼働環境

### (ア) クラウドサービスの構成

本調達はクラウドサービス（IaaS または SaaS）上に構築し、利用すること。当該クラウドサービスが本調達仕様書に示す各要件を満たすものであることをあらかじめ担保すること。

### (イ) クラウドサービスに関する要件

利用するクラウドサービスは、「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」<sup>1</sup>を参考にし、下記要件を満たしていることを提案に含めること。

#### ①情報システムの保護に関する要件

- ・ 情報資産を管理するデータセンターの物理的所在地が日本国内であること。
- ・ JICA の指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。
- ・ 障害発生時に縮退運転を行う際にも、情報資産が日本国外のデータセンターに移管されないこと。
- ・ 情報資産の所有権がクラウドサービス事業者に移管されるものではないこと。したがって、機構が要求する任意の時点で情報資産を他の環境に移管させることができること。
- ・ 法令や規制に従って、クラウドサービス上の記録を保護すること。
- ・ 情報資産が残留して漏洩することがないように、必要な措置を講ずること。
- ・ 自らの知的財産権についてクラウド利用者に利用を許諾する範囲及び制約をクラウド利用者に通知すること。

#### ②技術的要件

クラウドセキュリティに関する次のいずれかを取得していること。

- ・ ISO/IEC 20107:2015 認証
- ・ GS ゴールドマーク
- ・ ISMAP（政府情報システムのためのセキュリティ評価制度）認証

### (ウ) ソフトウェア要件

#### ① CMS（コンテンツマネジメントシステム）

現行の CMS を利用する場合は、WebRelease2 Enterprise Edition を利用し、

---

<sup>1</sup> 「政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版）」：  
<http://www.nisc.go.jp/active/general/kijun30.html>

最新バージョンを導入すること。ライセンスについては発注者が保持するライセンスを利用すること。

現行の CMS を利用しない場合は、現行と同等以上の機能を有し、実現可能な説明を加え、提案すること。また、ライセンス形態についても提案に含むこと。

② その他のソフトウェア

システム稼働に必要なソフトウェアを明記し、提案すること。サーバに導入するソフトウェアについては可能な限り最新バージョンを導入すること。

## **情報セキュリティ要件**

### **(1) 権限要件**

システム管理者のパスワードについては第三者に簡単類推されないよう、英数字を混ぜた 8 文字以上とし、3 ヶ月に 1 回変更するよう設計すること。

### **(2) 情報セキュリティ対策**

#### **(ア) データセンターにおける対策**

##### **① ファイアウォールの導入**

ネットワークへ外部からの侵入をされるのを防ぐため、適切な位置・パラメータにてファイアウォールを設定すること。

##### **1. 不正接続検知・DDos 攻撃検知**

不正侵入による悪意あるシステムダウン、DoS、DDoS 攻撃によるシステムダウン、レスポンス低下を防ぐシステムを導入すること。ログの保存期間は 6 か月とする。

別章で記載するコンテンツデリバリーサービスと組み合わせての提案も可能とする。

##### **2. DMZ セグメントへの公開サーバの配置**

ファイアウォールを使用し、外部ネットワーク（インターネット）と内部ネットワークを分割し、外部ネットワークからの不正なアクセスから保護し、内部ネットワークへの被害の拡散を防止すること。

##### **3. ユーザーとの通信の暗号化**

ユーザーとの通信時にデータの暗号化を実施すること。なお、暗号化方式は「電子政府推奨暗号リスト」に示されている暗号化方式を利用すること。

##### **4. 保有資格**

データセンターについては以下の資格を保有する業者が管理していること。

- ・ ISO27001 (同類の IEC を含む) /情報セキュリティマネジメントシステム (ISMS)
- ・ プライバシーマーク
- ・ ISO/IEC 20107:2015 認証、または GS ゴールドマークを保有していること。

またこれに加え、ISO9001 及び ISO14001 も保有していることが望ましい。

(イ) ソフトウェアにおける対策

① ウイルス／マルウェア対策ソフトの導入

サーバ及び機器等には、ウイルス／マルウェア対策ソフトウェアを導入し、その検知及び除去が可能となる設計・構築とすること。なお、当該対策ソフトウェアの設定を一括で変更できる仕組みを検討し、パターンファイル及びウイルス被害状況を確認できる環境を整備すること。

なお、上記ソフトウェアを導入できない環境のシステムを利用する場合には、同等以上のセキュリティ対策が実現されることを証明すること。

② アクセス制限／監査

システム自体へのアクセス証跡を所得及び保管可能な設計とし、必要に応じて確認が可能とすること。また、内部からの直接アクセスについては接続 IP アドレスによってアクセス制限を行い、適切な管理を実施すること。

(ウ) 別ウインドウが開くリンクの脆弱性対策

「JICA ウェブサイト以外」かつ「別ウインドウで開く」リンクに、rel 属性（リンクの関係性を示すコード）を追加する。ただし、ファイル一式をサーバに移行するだけのウェブサイトは対象外とする。

**その他の要件**

(1) ドメイン・サブドメインに関する要件

対象のドメイン、サブドメインは以下の通り。なお、「3. 現行 JICA ウェブサイトが抱える課題及び対応方針」を踏まえた関連サイトとの導線の見直し等も含まれる。

ドメイン名	利用用途
www. jica. go. jp	JICA ホームページ
www2. jica. go. jp	JICA 動的サイト（別添 4 「現行のウェブサイトの動的コンテンツ一覧」を参照）

**(2) モバイルデバイスに関する要件**

モバイルデバイスについては、PC版と同一コンテンツを提供するレスポンス対応とする。

**(3) 動作保証対応ブラウザに関する要件**

以下のブラウザにおいては動作するよう構築すること。また、公示時点最新バージョンのブラウザでの動作を保障すること。

- ・ Microsoft Internet Explorer 11.0/Microsoft Edge
- ・ Mozilla Firefox 最新版
- ・ Google Chrome 最新版
- ・ Safari 最新版

**(4) コンテンツデリバリーサービスに関する要件（※オプション）**

海外からのアクセス、負荷分散の観点からコンテンツデリバリーサービスを利用した提案も可能とする。コンテンツデリバリーサービスを利用した場合と利用していない場合でのサーバ保守費用の違いについても提案へ含めること。

**(5) オープンデータに関する要件**

オープンデータの活用についての取組は本調達での範囲外とする。

以上