

# 令和6年度外国人材マッチング支援業務 公募型プロポーザルに係る企画提案書作成のための仕様書

## 1. 企画提案書に記載する事項

2の業務内容のうち【提案】と記載している内容を提案すること。

## 2. 業務内容

(1) 受託者が所有するマッチングシステムを活用することとし、大学や送出機関等から情報収集をするとともに、本システムへの登録促進を図ること。

なお、外国人材及び和歌山県内に事業所を有する企業・団体（以下「県内企業」という。）の登録承認権限が和歌山県及び受託者にあり、外国人材及び県内企業双方からのオファー機能を有するシステムとし、県内企業から成功報酬を徴収しても良いこととする。

【提案】 マッチングシステムの運用方法及び運営体制（人員配置、連絡体制等）を具体的に提案すること。

なお、使用するマッチングシステムの概要や強み等が分かる書類及び配置する人員の資格や具体的な実績等が分かる書類を提出すること。

(2) 外国人材及び県内企業が求める人材の情報収集を行い、マッチング促進を図ること。

(3) 会社見学やインターンシップ等による来日の希望があった場合、円滑に来日できるよう希望者及び参加企業に対し、必要な支援を行うこと。

【提案】 支援体制（人員配置、連絡体制等）を具体的に提案すること。

なお、配置する人員の資格や具体的な実績等が分かる書類を提出すること。

(4) マッチング後、外国人材に対し、日本語やビジネスマナー等の教育、住居・給与口座開設等来日に必要な支援を行うこと。

【提案】 日本語やビジネスマナー等の教育体制（人員配置、手法、内容等）及び支援体制（人員配置、連絡体制等）を具体的に提案すること。

なお、配置する人員の資格や具体的な実績等が分かる書類を提出すること。

(5) 適宜、業務の進捗状況を和歌山県に報告すること。

## 3. マッチングシステムの要件

(1) サーバーの設置

ア 概要

マッチングシステムを格納するサーバーは、和歌山県庁の外部に置くものとする。

イ システム要件

(ア) 使用するデータセンターについては、安全性の確保の観点から、一般社団法人日本情報経済社会推進協会のプライバシーマーク又は情報セキュリティマネジメントシステム（ISMS）の認証を取得していること。

(イ) データセンターの設置場所は、日本国内（沖縄本島、佐渡島、淡路島以外の島しょを除く地域）とすること。

(ウ) 日本データセンター協会が制定しているデータセンターファシリティスタンダード (JDCCFS)における「ティアレベル3」相当以上の設備条件を最低限満たしていること。

(エ) データセンターのセキュリティ対策については、別紙『「安全確保の措置」に係る遵守事項』に定める各項目を満たすとともに、総務省の「クラウドサービス提供における情報セキュリティ対策ガイドライン」(第3版)に留意すること。

(オ) サーバーは、冗長構成とすること。

(カ) サーバーは、ユーザーが増加した際にプログラム変更することなく適切な対応が取れる状態であること。

(キ) 障害時に自動又は手動により最終バックアップ地点まで復旧できる仕組みであること。

(ク) サーバーは、SSL/TLS を実装し、SSL サーバー証明書を発行すること。

## (2) 運用要件

ア 毎月データのバックアップを取得し、業務期間中は保管しておくこと。

イ システムの構成、性能、リソース、インシデント等の管理を行うこと。

ウ システムの脆弱性等を契機とした情報漏えいが発生しないよう、十分なセキュリティ対策を施すこと。

エ ウイルス対策ソフトを導入し、常に最新のパターンファイルを適用すること。

## (3) 動作環境

ア 利用者の閲覧ブラウザは、Microsoft Edge、Google Chrome、Firefox 又は Safari 等の最新版、OS は、Windows、Mac OSX、iOS、Android に対応していること。また、対応バージョンについては、その時の最新バージョン又は普及率の高いバージョンに対応すること。

なお、具体的なバージョンについては、和歌山県と協議の上、決定すること。

イ 運用期間中に対応する OS の最新バージョンがリリースされた場合、稼働確認を行い改修など、和歌山県と相談の上、必要な対応を行うこと。

ウ 和歌山県の行政事務用パソコンのシンクライアント環境(Microsoft Edge 及び Google Chrome) で本システムを管理する上で必要となる機能を使用できること。その際、特別なプラグイン・ソフトウェア等のインストールの必要がないこと。また、これらに対してすべての環境での動作確認を実施すること。

## (4) 保守要件

ア 個人情報の取扱方法等に応じて、適宜、システムの通信を暗号化するとともに、個人情報漏洩等のリスクを回避するため、十分な対策を行い、定期的にセキュリティ診断を実施すること。

イ 外部からの不正アクセスやデータ改ざん等の悪意ある攻撃を受けないよう、必要な対策を講じること。また、OS の脆弱性を解消するために、常に最新のセキュリティパッチを適用すること。

ウ 本システムに故障等が発生し、業務運用に支障が生じた場合又はそのおそれがあると

判断される場合には、速やかに故障を回復し、正常な業務運用が可能となる状態に復旧する等の保守作業を確実に実施すること。また、故障等を事前に予防するための定期点検についても実施すること。

エ SQL インジェクションやクロスサイトスクリプティング等の脆弱性を悪用して行われる攻撃に対し、十分な対策を講じて、情報漏洩が発生しないよう留意すること。また、脆弱性が発見された場合は、直ちに対応すること。

オ システムに脆弱性がないか定期的に調査し、その結果を和歌山県へ報告すること。

カ ウイルス対策ソフトを導入し、常に最新のパターンファイルを適用すること。

キ 別紙『「安全確保の措置」に係る遵守事項』に定める各事項を満たすこと。

#### (5) その他

ア 和歌山県からの電話、電子メール等のシステム使用・操作等に係る問い合わせに対応すること。

イ 障害が発生した場合、速やかに復旧作業を行うこと。

ウ サイバーテロ、ウイルス感染及び情報漏えい等のセキュリティインシデント発生時には、和歌山県に報告の上、速やかに対応を行うこと。

エ そのほかサーバー運用、保守に必要な事項について対応すること。

### 4. 留意点

(1) 受託者は、業務を一括して第三者に委託し又は請け負わせることができない。ただし、業務を効果的に行う上で必要と思われる業務については、和歌山県と協議の上、業務の一部を委託することができる。

(2) 個人情報の取扱いには十分留意し、漏えい、滅失及びき損の防止その他個人情報の保護に努めること。

(3) 業務上知り得た秘密を他に漏らし、又は自己の利益のために利用してはならない。また、契約期間が満了し、又は取り消された後においても同様とする。

(4) 賃金台帳、領収書等の実際の支出額が確認できる書類を業務完了時に、和歌山県に提出するとともに、完了後5年間、いつでも閲覧に供することができるよう保管すること。

### 5. その他

(1) 1の留意点に違反したときは、契約の一部又は全部を解除し、委託料の支払いをしない、又は支払った委託料の一部若しくは全部を返還させる場合がある。

(2) (1)により契約を解除した場合は、損害賠償又は違約金を求める場合がある。

(3) 委託先については、ア～エの審査項目に従って評価し、総合得点により決定する。

ア 事業実施に必要な実施体制を整えており、業務遂行能力の高い事業者であるか。

イ 効果的なマッチングシステムであるか。

ウ 効果的な支援体制となっているか。

エ 効果的な日本語やビジネスマナー等の教育体制となっているか。

- (4) 受託者は、次の拠点・機能を有していること。
- ア 受け入れる人材の確保やコンシェルジュサポート等を行うための海外拠点
  - イ 継続的な教育体制やサポートカリキュラム等の支援
  - ウ 必要に応じて、多言語対応も可能なコールセンター
- (5) 業務の履行に当たっては、業務内容を十分に理解し、和歌山県と連絡を密に取りながら誠実に履行すること。
- (6) 本仕様書に記載されていない事項及び疑義が生じた場合は、和歌山県と協議の上、決定すること。
- (7) 受託中に知り得た個人情報 は適正に管理し、決して漏えい、不正使用を行わないこと。当該契約の履行が完了された後においても同様とする。
- (8) 特許権、実用新案権、意匠権、商標権その他日本国の法令に基づき保護される第三者の権利の対象となっているものを使用するときは、受託者がその使用に関する一切の責任を負うこと。
- (9) 受託者は、本業務の成果物に係る著作権を、成果物引き渡し時に、和歌山県に譲渡するものとする。ただし、譲渡する以外に有効な手法がある場合は、適宜提案すること。なお、使用に関して条件や制限があるものについては、その都度両者で別途協議するものとする。
- (10) 和歌山県が上記(9)で譲渡を受ける権利には、著作権法（昭和 45 年法律第 48 号）第 27 条及び第 28 条に定める権利も含むものとする。
- (11) 和歌山県が著作権を行使する場合において、受託者は、著作権法第 19 条第 1 項又は第 20 条第 1 項に規定する権利を行使してはならない。
- (12) 本事業の目的に照らし合わせて新たに盛り込むべきと考えられる独自の手法等があれば、適宜提案すること。
- (13) 和歌山県情報セキュリティ基本方針を遵守して業務を実施すること。

## 「安全確保の措置」に係る遵守事項

### (基本的事項)

第1 受託者(以下、「乙」という)は、この契約による事務の実施に当たっては、和歌山県(以下、「甲」という)の情報を閲覧する者の個人情報を侵害することのないよう、甲から委託を受けて情報を公開するために利用する機器等の管理を適正に行わなければならない。

2 乙は、この契約による事務の実施に当たり、ホスティングサービス、レンタルサーバー、ハウジングサービス又はこれらに類するサービスを利用する場合は、第1項に沿って本遵守事項に定める各事項を満たすよう、この契約による事務を処理するに当たり、事前にサービス提供者との間で取り決め又は確認をすること。

### (ウイルス対策の実践)

第2 乙は、この契約による事務の実施に当たっては、利用するサーバー等の機器について、ウイルス検知用データは常に最新のものに更新すること。

2 Webサーバーの管理用又は更新用等にパソコン等の機器を利用する場合は、乙はこれら機器に対しても第1項で規定する措置を講じること。

### (ソフトウェアの更新)

第3 乙は、本遵守事項の第2の対象となる機器で利用するソフトウェアに対しては、定期的に修正プログラムを適用し、できる限りソフトウェアを最新の状態にしておくこと。

### (ファイアウォールの導入)

第4 乙は、この契約による事務の実施に当たっては、ファイアウォールを設定し通過させるパケットや遮断するパケットに対するルールを設定しておくこと。

2 乙は、侵入防止システム(IPS)を導入すること。ただし、甲の承諾があるときは、この限りでない。

### (セキュリティ診断)

第5 乙は、外部の者によるセキュリティ診断を受けること。ただし、甲の承諾があるときは、この限りでない。

### (ログのチェック)

第6 乙は、この契約による委託期間中、定期的にログ(Webサーバー、OS、ルータ、DB等)をチェックすること。

### (コンテンツ内容の確認等)

第7 乙は、著作権を侵害するような写真やイラスト、ファイル等は使用しないこと。

2 乙は、この契約による事務を処理するに当たっては、コンテンツの取込持出時の検疫方法と取扱手順を事前に定めておくこと。

### (パスワードの管理)

第8 乙は、この契約による事務を処理するに当たっては、本遵守事項の第2の対象となる機器等には安全なパスワードを設定することとし、定期的に変更すること。また、不要なアカウントを登録しないこと。

### (コンテンツ等の管理)

第9 乙は、Webサーバーやデータベースサーバ等、コンテンツや情報等を格納するディレクトリやファイルに対しては適正なアクセス権限を設定すること。

2 乙は、この契約による事務を処理するに当たり、下記の対策を講じること

- (1) SQL インジェクション、クロスサイト・スクリプティング等の脆弱性への対策を講じること。
- (2) 不要なページやウェブサイトを公開しないこと。
- (3) 不要なエラーメッセージを返さないこと。
- (4) 不要なサービスやアプリケーションを起動させないこと。

(セキュリティポリシー)

第10 乙は、この契約による事務を処理するに当たり、セキュリティポリシーを策定すること。

ただし、既にセキュリティポリシーを定めている場合はこの限りではない。

2 乙は、この契約による事務を処理するに当たり、不正侵入やウイルス感染が発生した場合の対応方法を策定しておくこと。ただし、既にこれらの対応方法を定めている場合はこの限りでない。

(調査)

第11 甲は、乙がこの契約による事務を処理するに当たり、本遵守事項に定める各事項の状況について、随時調査することができるものとする。

(契約解除及び損害賠償)

第12 甲は、乙が本遵守事項の内容に反していると認めるときは、契約の解除又は損害賠償の請求をすることができるものとする。