令和８・９・10年度経験者採用職員募集に係る応募者管理システム提供業務

調達仕様書

独立行政法人都市再生機構

１　業務名称

令和８・９・10 年度経験者採用職員募集に係る応募者管理システム提供業務

２　履行期間

令和８年４月１日から令和 11 年３月 31 日まで

３　目的

経験者採用職員の募集にあたり、転職希望者が利用する就職サイト（以下「転職サイト」という。）等からエントリー受付を行い、応募者情報を一元管理することで、各種試験等の案内や予約受付を行うなど、採用活動の一助とすることを目的とする。

４　業務内容

経験者採用募集にあたり、エントリー受付や選考等の過程において、次の（１）から（５）に定める業務を行うことができるシステムの提供、管理運営及び利用にあたっての支援を行う。なお、システムの提供期間については、履行期間の開始日以降の発注者が指定する日から令和 11 年３月 31 日までとする。

（１） 転職サイト上での当機構へのエントリー受付

① 転職サイト上で当機構へのエントリー受付を可能とする設定を行う。

また、エントリー受付にあたっては、以下のイからルに記載するエントリー者の情報を取り込むこととする。

イ　氏名（漢字表記並びにふりがな又はフリガナ表記）
ロ　生年月日
ハ　現住所（郵便番号、都道府県、市町村区、町名等）
ニ　電話番号（自宅及び携帯電話）
ホ　メールアドレス（※データ送受信の関係から、ＰＣ又は多機能携帯電話（スマートフォン）のメールアドレスを必須とする。）
ヘ　最終学歴（学校種別（大学又は大学院）・学校・学部・学科（専攻）名、卒業年月）
ト　取得資格
チ　職務経歴（会社名、期間、業種、雇用形態、職種、担当業務内容）
リ　希望職種
ヌ　応募理由
ル　自己ＰＲ

② （１）①に記載するエントリー時の個人情報の入力が機構ホームページからも直接できるようにすること。（リンク対応も可とする。）

③　エントリー者に対して個々に識別できるＩＤナンバー（自動付番：６桁程度）

を発行のうえ、かつ、応募サンクスメールを自動で送信できるようにすること。

④　エントリー者の個人情報等の一覧表がＣＳＶファイル又はエクセルファイルでダウンロードできるようにすること。

（２）　エントリーシートの作成及び管理

①　エントリー者が、ＷＥＢ上でのエントリーシートの記入及び提出ができるようにすること。また提出後のエントリーシートを、面接官が確認しやすいようにＰＤＦ形式化や閲覧、出力をできるようにすること。

②　エントリーシートの様式について、カスタマイズできること。

（３）　面接試験等の予約受付案内等

①　面接試験等の日程や会場等にあわせた予約画面の設定ができるようにすること。

②　エントリー者自身がＷＥＢ上で予約ができるようにすること。

③　ＣＳＶデータのアップロード、バーコード等によりフラグ立てを行い、選考段階毎に予約可能な者を限定することができるようにすること。

④　予約者が、自ら予約変更やキャンセルをできるようにすること。

⑤　予約完了時等にサンクスメールを自動で送信できるようにすること。

⑥　予約者等の一覧表がＣＳＶファイル又はエクセルファイルでダウンロードできるようにすること。

（４）　エントリー者等（過去登録者含む）への一括メールの作成及び送信

エントリー受付完了時のほか、各選考段階の予約完了時や選考結果等を通知する際の通知メールを作成し、対象者に対してメールを一括送信することができるようにすること。

（５）　特記事項

①　メールを一括送信する対象者の設定にあたっては、ＣＳＶデータのアップロード、バーコード等によりフラグ立てができるようにすること。

②　当該システムについて、操作マニュアルを提供し、容易に操作、設定等ができること。また、使用に当たって問い合わせ（ヘルプデスク等）についても体制が万全であること。

③　受験する転職希望者が使用するに当たり、面接試験等予約操作がわかりやすいこと。（転職希望者本人が登録を確認できる機能があること。）

④　応募者データに係る検索・抽出・挿入・削除等の操作がわかりやすいこと。

⑤　当該システムは、当機構採用担当者が各種管理項目をカスタマイズして使用できるものであること。

⑥　エントリー者等（過去登録者含む）の登録データ件数は計 10 万件程度を想定しており、同程度の情報量を動作性に問題なく円滑に活用できるシステムであること。

⑦　自社で有する転職サイトがある場合は、その転職サイトで受け付けたエントリーに関する情報を自社でシステムに取り込むこと。

⑧　面接に使用する資料（履歴書、エントリーシート、評定表等）について、様式をカスタマイズし、それぞれの面接の段階ごとに必要な資料を一つにまとめてＰＤＦ形式化できるようにすること。

⑨　当機構が指定する人材紹介会社（最大 20 社程度を想定）から紹介を受けた応募者の情報について、紹介した人材紹介会社名と紐付けて、４に定める業務を行うことができるシステムであること。

⑩　採用活動の各年度における応募者数や選考状況等を、当年度の状況と照合し分析する為、現在、当機構において使用している応募者管理システム上に保存されている約９万件の登録データのうち以下の必須項目を移行できる仕様であること。（必須項目：４（１）①に掲げる候補者基本情報、選考結果情報、その他備考情報等）

５　情報セキュリティ

応募者情報管理システムにおける情報セキュリティ要件については「別紙１　情報セキュリティ要件」のとおりとする。

６　その他

（１）　本業務は、この仕様書に定めるほか、機構の担当者と十分協議しながら作業を実施するものとする。

（２）　成果品に係る一切の著作権及び版権は、原則として機構に帰属するものとし、協議が必要な場合は予め申し出るものとする。

（３）　受注者は、請負代金については、２に規定する本業務の履行期間以降、その支払請求書を発注者に提出するものとし、発注者は、当該請求書を受理した日から起算して 30 日以内に、これを受注者に支払うものとする。

（４）　業務実施にあたり、業務の主たる部分（全体を総括・調整する業務に該当する業務）についての再委託は認めない。また、再委託の必要が生じた場合は、自らが実施する業務の範囲を指定様式にて提出し、あらかじめ発注者の承諾を得なければならない。

（５）　再委託の必要が生じ受注者が業務の一部を再委託する場合、書面（様式自由）により再委託の相手方との契約関係を明確にしておくこととともに、再委託の相手方に対し、業務の適正な履行を求めることとする。また、受注者からの求めに応じ、委託業務に係る契約書、請求書、領収書等の書面の写しを提出すること。

（６）　業務遂行にあたり、機構ホームページを編集・操作する場合は機構の指示に

従うこと。

（７）　本業務において当機構の情報を第三者に漏らしたり、他の目的に使用したりしてはならない。

（８）　この仕様書に記載のない事項、疑義等が生じた場合は、その都度指示者と協議すること。

以　上

令和８・９・10年度経験者採用職員募集に係る応募者管理システム提供業務

別紙１ 情報セキュリティ要件

独立行政法人都市再生機構

目次

1. 情報セキュリティ要件

1.1. 情報セキュリティインシデントに係る情報共有

情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、受注者は、当該事項について速やかに機構に報告すること。

1.2. 要機密情報を取り扱う場合のクラウドサービスの利用に係る調達

受注者が提案するクラウドサービスが具備しているべき条件については、「別紙 2 クラウドサービスの条件」のとおりとすること。なお、提案時には、クラウドサービスの再販提供者として、条件の各項目について具体的な説明（提案）を行うこと。

1.3. 要機密情報を取り扱う場合のクラウドサービスの利用に係るセキュリティ要件の策定

受注者は、クラウドサービスで利用するアカウント管理に関する以下の措置を講ずること。

一　識別コードの作成から廃棄に至るまでのライフサイクルにおける管理を実施すること

二　管理者権限を保有するクラウドサービス利用者に対する強固な認証技術を導入すること

三　クラウドサービス提供者が提供する主体認証情報の管理機能を利用して、以下の全てのパスワード要件が満たせるようにすること

　イ　パスワード長を 8 桁以上とする

1.4. 要機密情報を取り扱う場合のクラウドサービスを利用した情報システムの導入・構築時の対策

クラウドサービスの運用開始前までに、以下のクラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順を整備すること。

一　クラウドサービス提供者との責任分界点を意識したクラウドサービス利用手順

二　クラウドサービス利用者の操作により利用中のクラウドサービスに重大な障害をもたらすことが予想される操作に関する操作手順

1.5. 情報システムの運用・保守時の対策

受注者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能が適切に運用されていることを確認すること。

1.6. 電子メールの導入時の対策

(1)　受注者は、電子メールサーバが電子メールの不正な中継を行わないように設定すること。

(2)　受注者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に、以下の役職員等の主体認証を行う機能を備えること。

一　電子メールの受信時に限らず、送信時においても不正な利用を排除するために SMTP 認証等の主体認証機能を導入する。

(3)　受注者は、以下の送信ドメイン認証技術による電子メールのなりすましの防止策を講ずること。

一　DMARC による送信側の対策を行う。DMARC による送信側の対策を行うためには、SPF、DKIM のいずれか又は両方による対策を行う必要がある。

(4)　受注者は、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、以下の電子メールのサーバ間通信の暗号化の対策を講ずること。

一　SMTP によるサーバ間通信を TLS により保護する。

二　S/MIME 等の電子メールにおける暗号化及び電子署名の技術を利用する。

1.7.　不正なウェブサイトへの誘導防止

受注者は、利用者が検索サイト等を経由して機構のウェブサイトになりすました不正なウェブサイトへ誘導されないよう、以下の対策を講ずること。

一　機構外向けに提供するウェブサイトに対して、以下を例とする検索エンジン最適化措置（SEO 対策）を講ずること。

イ　適切なタイトルを設定する。

1.8.　主体認証機能の導入

(1)　受注者は、主体の識別及び主体認証を行う機能を設けること。なお、主体認証機能を設けるに当たっては、以下の主体認証方式を導入すること。

一　知識（パスワード等、利用者本人のみが知り得る情報）による認証

(2)　受注者は、機構外からリモートアクセス可能な主体及び管理者権限を有する主体に対する認証の強度として2つ以上の主体認証方式を組み合わせる多要素主体認証方式等の強固な認証技術を用いること。

(3)　受注者は、主体認証情報としてパスワードを使用し、主体認証情報を付与された主体自らがパスワードを設定することを可能とする場合には、辞書攻撃等によるパスワード解析への耐性を考慮し、強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用することを利用者に守らせる機能を設けること。

1.9.　アクセス制御機能の導入

受注者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に

従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けること。

1.10. ログの取得・管理

(1) 受注者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために以下を例とする必要なログを取得すること。

一 クラウドサービス及びクラウドサービス上に構築するソフトウェアにおいて、アクセスログを取得すること。

二 ファイルアクセスを伴う場合、データベース及びファイルに対する操作に関するログを取得すること。

三 情報システムの利用記録、例外事象の発生に関するログを取得すること。

なお、情報システムに含まれる構成要素のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう、設定すること。

(2) 受注者は、ログを取得する対象、ログの保存期間、要保護情報の観点でのログ情報の取扱方法等とともに以下のログとして取得する情報項目を管理すること。

一 事象の主体(人物又は機器等)を示す識別コード

二 識別コードの発行等の管理記録

三 正確な日付及び時刻

(3) 受注者は、取得したログに対する、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、ログ情報の保全方法を定めること。

(4) 受注者は、情報システムにおいてユーザ操作等のログを確認可能な機能を設けること。

1.11. 暗号化機能・電子署名機能の導入

(1) 受注者は、暗号化又は電子署名について、以下の措置を講ずること。

一 情報システムのコンポーネント(部品)として、暗号モジュールを交換することが可能な構成とすること。

二 複数のアルゴリズム、鍵長及びそれらに基づいた安全なプロトコルを選択することが可能な構成とすること。

(2) 受注者は、暗号技術検討会及び関連委員会(CRYPTREC)により安全性及び実装性能が確認された「電子政府推奨暗号リスト」に基づき、情報システムで使用する暗号及び電

子署名のアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを採用すること。また、暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること。

以上

令和８・９・10年度経験者採用職員募集に係る応募者管理システム提供業務

別紙2 クラウドサービスの条件

独立行政法人都市再生機構

クラウドサービスの条件

受注者が提案するクラウドサービスが具備しているべき条件については、以下のとおりとする。なお、提案時には、クラウドサービスの再販提供者として、条件の各項目について具体的な説明(提案)を行うこと。

クラウドサービスの条件		
項番	**区分**	**内容**
1	資格・認証	・ISO/IEC27001:2013、ISO/IEC27001:2022 若しくは JIS Q 27001:2014 に基づく情報セキュリティマネジメントシステム（ISMS）適合性評価制度の認証を受けていること。
2	データの所在・適用法と裁判管轄	・外部サービスに保存される情報（バックアップデータ含む）の所在地は日本国内であること。
3		・日本国法に準拠し、紛争については日本国の裁判所が第一審の専属管轄裁判所であること。
4	セキュリティ対策	・管理者権限を持つユーザ等（管理者権限を持たない一般ユーザも含む）に対して、IP アドレス制限による拠点の制限やクライアント証明書等による端末の制限を実施すること。
5	実績	・過去１年以内に情報セキュリティインシデントが発生していないこと。 過去１年以内に情報セキュリティインシデントが発生している場合は、当該インシデント原因に対して適切に対策されていること。

以上