別添３

業務説明書

１　業務名称

令和８・９・10 年度職員採用の選考に係る総合能力検査問題の提供及び採点等業務

２　履行期間

契約締結日翌日から令和 11 年４月 30 日まで

※　契約締結日翌日から令和８年３月 31 日までは業務準備期間とし、総合能力検査実施は、令和８年４月１日以降履行期間中に、当機構が指定する期間において実施するものとする。

３　目的

令和８年度から令和 10 年度にかけて実施する職員採用の選考にあたり、選考プロセスの一つとして、応募者の基礎的な知的能力及び職務適性等に関する検査を実施することを目的とする。

４　業務内容

本業務は、以下の業務から構成する。

構成	内容
令和８・９・10 年度職員採用の選考に係る総合能力検査問題の提供及び採点等業務	（１）　総合能力検査に係る問題の提供及び実施 ①　検査実施に係る問題様式及び回答様式の提供 ②　検査の実施 （２）　総合能力検査に係る採点及び検査結果の提出 ①　採点 ②　検査結果の提出 （３）　総合能力検査結果データの読取り方及び活用方法に関する説明会の実施 （４）　総合能力検査を活かした選考等に関する独自の企画提案

なお、本件における「総合能力検査」とは、以下の①及び②を包含する検査としている。

①　言語理解及び計数理解等の基礎的な知的能力を測定することができる検査

②　性格、パーソナリティ、職務適性及びストレス耐性等の適性を測定することができる検査

（１）　総合能力検査に係る問題の提供

①　検査実施に係る問題様式及び回答様式の提供

イ　受注者は、総合能力検査の問題様式及び回答様式を用意し、インターネット媒体により供給する。

ロ　受注者は、当機構が指定する期間において、インターネット媒体を利用した検査が可能となるよう準備を行う。

ハ　必要に応じて全国主要都市においてテストセンターを利用したテストが実施

できるようにする。

② 検査の実施

イ 検査の実施においては、受検者が任意に日時及び場所を選択できるものとする。

ロ 検査は、ＷＥＢテスト利用の場合、受検者の自宅等のＰＣで実施する。

テストセンター利用の場合は、テストセンター会場等にて実施する。ただし、この場合も性格検査については自宅等のＰＣで実施する。

ハ 受注者は、受検者に対し、わかりやすく案内を行う。

ニ 受注者は、検査に際し、受検者による不正行為が生じないよう合理的に必要な方策を講ずる。

（２） 総合能力検査に係る採点及び検査結果の提出

① 採点

受注者は、回答の採点を行い、検査結果データをとりまとめることとする。

② 検査結果の提出

イ 受注者は、当機構へ受検者分の検査結果を電子データでインターネット（電子メール等）経由で提出する。

ロ 当機構へ提出される電子データは、Microsoft Excel ファイル又はCSV 形式ファイルとする。

（３） 総合能力検査結果データの読取り方及び活用方法に関する説明会の実施

総合能力検査結果データの読取り方及び活用方法について、毎年４月上旬頃に１回、当機構職員に向けた説明会を実施すること。

なお、日時は当機構と受注者で調整することとし、１回あたり１～２時間程度を想定しているが、令和８年度は４月７日（火）実施を予定している。

（４） 総合能力検査を活かした選考等に関する独自の企画提案

受注者が企画提案書に記載した独自の企画提案内容を、履行期間中に行うものとする。

５ 目的物等

採点結果データ（受検者人数分）

（補足）

（１） 総合能力検査に係る受検者数は、履行期間中（３ヵ年）にＷＥＢテスト利用者は10,000 人、テストセンター利用者は５人を想定している。

（２） 検査予定人数は（１）のとおりであるが、締結する契約は単価契約とし、単価に実際の受検者数を乗ずる。

６ 情報セキュリティ

総合能力検査受検者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。

７ その他

（１） 本業務は、この業務説明書に定めるほか、当機構の担当者と十分協議しながら実

施するものとする。

（２）　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、再委託する業務の範囲について、あらかじめ発注者の承諾を得なければならない。

（３）　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。

（４）　業務実施にあたり、機構ホームページを編集・操作する場合は当機構の指示に従うこと。

（５）　企画提案競技説明書６（１）②で提示した概算費用は、あくまで企画提案の目安となる金額であり、概算費用を確約するものではない。

（６）　本業務において当機構の情報を第三者に漏らしたり、他の目的に使用しないこと。

（７）　業務説明書に記載のない事項、疑義等が生じた場合は、その都度本業務の担当者と協議すること。

以　上

令和８・９・10年度職員採用の選考に係る
総合能力検査問題の提供及び採点等業務

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

(1) 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

(2) 受注者は、以下のクラウドサービスの利用に係るセキュリティ対策を実施すること。

一 クラウドサービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の監視

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

(1) 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

(1) 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. ウェブサーバの導入・運用時の対策

(1) 受注者は、ウェブコンテンツの編集作業を担当するアカウントの限定として、以下のウェブサーバの管理や設定を行うこと。

一 ウェブサーバ上のウェブコンテンツへのアクセス権限は、ウェブコンテンツの作成や更新に必要な者以外に更新権を与えない。

二 OS やアプリケーションのインストール時に標準で作成される識別コードやテスト用に作成した識別コード等、不要なものは削除する。

(2) 受注者は、ウェブコンテンツの編集作業に用いる端末の限定、識別コード及び主体認証情報の適切な管理として、以下のウェブサーバの管理や設定を行うこと。

一 ウェブコンテンツの更新の際は、専用の端末を使用して行う。

二 ウェブコンテンツの更新の際は、ウェブサーバに接続する接続元の IP アドレスを必要最小限に制限する。

三 ウェブコンテンツの更新に利用する識別コードや主体認証情報は、情報セキュリティを確保した管理を行う。

1.7. 不正なウェブサイトへの誘導防止

(1) 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 クローラからのアクセスを排除しない。

ロ 適切なタイトルを設定する。

ハ 不適切な誘導を行わない。

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。

三　選択したアルゴリズム及び鍵長が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へ適切に実装されており、かつ、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及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択すること。

四　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は、耐タンパ性を有する暗号モジュールへ格納すること。

(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年度職員採用の選考に係る
総合能力検査問題の提供及び採点等業務

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、又はプライバシーマーク制度の認証によりプライバシーマーク使用許諾を受けていること。
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