仕様書

１　業務名称

令和６・７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６年４月１日から令和８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８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８万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については、以下を満たすものとする。

（１）情報セキュリティ対策に関する事項

情報セキュリティ対策に関する事項については、「別紙１　作業の実施にあたっての遵守事項」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。

（２）システムの提供にあたっての遵守事項

「別紙１　作業の実施にあたっての遵守事項」のとおりとする。なお、

受注者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証するため、主体の識別及び主体認証を行う機能を設けること。

また、主体認証情報としてパスワードを使用し、利用者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桁数や複雑さを利用者に守らせる機能を設けること。

（３）情報セキュリティ対策に関する事項

①　「別紙１　作業の実施にあたっての遵守事項」のとおりとする。また、受注者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、次の各号を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を実施すること。なお、下記事項についても順守すること。

一　不正なアクセスを防止するためのアクセス制御

a）クラウドサービス提供者が付与又はクラウドサービス利用者が登録する識別

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

b) クラウドサービスを利用する際に使用するネットワークに対するサービスごとのアクセス制御

c) 情報システムの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の利用

d) 機構が要求する主体認証情報に係る規定の遵守

e) クラウドサービス上に保存する情報やクラウドサービスの機能に対してアクセス制御できることの確認

f) クラウドサービス利用者によるクラウドサービスに多大な影響を与える操作の特定と誤操作の抑制

g) クラウドサービス上で構成される仮想マシンに対する適切なセキュリティ対策の実施

h) インターネット等の機関等外通信回線から機関等内通信回線を経由せずにクラウドサービス上に構築した情報システムにログインすることの要否の判断と認める場合の適切なセキュリティ対策の実施

二　取り扱う情報の機密性保護のための暗号化

a) クラウドサービス内及び通信経路全般における暗号化

b) 「電子政府推奨暗号リスト」に記載されている暗号化方式の採用

三　開発時におけるセキュリティ対策

a) 情報システムの構築においてクラウドサービスを利用する場合のセキュリティを保つための開発手順の作成

b) クラウドサービス上に構成されたセキュリティ要件の異なるネットワーク間のファイアウォールの設置

c) クラウドサービス上のデータ容量やリソースの稼働状況についての監視と将来の予測の実施

d) 要安定情報を取り扱う場合、データの可用性を考慮した設計

e) クラウドサービス内における時刻同期の方法の確認

② 受注者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、次の各号を含むクラウドサービスを利用して情報システムを運用する際のセキュリティ対策を実施すること。

一　クラウドサービス利用者に対する教育の提供

二　取り扱う資産の管理

a) クラウドサービスの機能に対する脆弱性対策について、クラウドサービス提供者の責任範囲の明確化と対策の実施

三　不正アクセスを防止するためのアクセス制御

a) 管理者権限をクラウドサービス利用者へ割り当てる場合のアクセス管理と操

作の確実な記録

b） クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の機能の確認と利用者の制限

c） 利用するクラウドサービスの不正利用の監視

四　取り扱う情報の機密性保護のための暗号化

a） 暗号化に用いる鍵の管理者と鍵の保管場所の明確化

b） 鍵管理機能をクラウドサービス提供者が提供する場合の鍵管理手順と鍵の種類の情報の要求とリスク評価

c） 鍵管理機能をクラウドサービス提供者が提供する場合の鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価

五　クラウドサービス内の通信の制御

a） 利用するクラウドサービスのネットワーク基盤が他のネットワークと分離されていることの確認

六　設計・設定時の誤りの防止

a） クラウドサービスの設定を変更する場合の設定の誤りを防止するための対策

b） クラウドサービス利用者が行う可能性のある重要操作の手順書の作成と監督者の指導の下での実施

七　クラウドサービスを利用した情報システムの事業継続

a） 不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施。又は、クラウドサービス提供者が提供する機能を利用する場合は、その実施の確認

b） 要安定情報をクラウドサービスで取り扱う場合の十分な可用性の担保、復旧に係る手順の策定と定期的な訓練の実施

c） クラウドサービス提供者からの変更通知の内容確認と復旧手順の確認

d） クラウドサービスで利用しているデータ容量、性能等の監視

八　クラウドサービスを利用した情報システムの事業継続

③　受注者は、次の各号を含むクラウドサービスの利用を終了する際の対策を実施すること。

一 クラウドサービスの利用を終了する場合の移行計画書若しくは終了計画書の作成

二 移行計画書若しくは終了計画書の機構への事前通知

三　クラウドサービスの利用のために作成したアカウントの廃棄

イ　作成されたクラウドサービス利用者アカウントの削除

ロ　利用したクラウドサービス管理者アカウントの削除・返却と再利用の確認

ハ　クラウドサービス利用者アカウント以外の特殊なアカウントの削除と関連

情報の廃棄

④ 受注者は、情報セキュリティ対策を実施するために必要となる文書として、次の各号を網羅した情報システム関連文書を整備すること。

一　情報システムを構成するサーバ装置及び端末関連情報

二　システムを構成する通信回線及び通信回線装置関連情報

三　情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

四　情報セキュリティインシデントを認知した際の対処手順

⑤　受注者は、情報システムの運用・保守において、情報セキュリティ対策による情報システムの変更内容について、速やかに機構に報告すること。

⑥ 受注者は、情報システムの運用・保守において、次の各号を含む必要な措置を講じ、情報システムに実装されたセキュリティ機能を適切に運用すること。

一　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。

二　情報システムにおいて取り扱う情報について、当該情報の格付及び取扱制限が適切に守られていることを確認すること。

三　運用中の情報システムの脆弱性の存在が明らかになった場合には、情報セキュリティを確保するための措置を講ずること。

⑦　受注者は、情報システムのセキュリティ監視を行う場合は、次の各号の内容を含む監視手順を定め、適切に監視運用すること。

一　監視体制

二　監視状況の報告手順

三　情報セキュリティインシデントの可能性を認知した場合の報告手順

四　監視運用における情報の取扱い（機密性の確保）

⑧ 受注者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。

⑨ 受注者は、情報システムの更改（外部サービスの場合はサービス内容の変更）又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、次の各号の措置を適切に講じなければならない。

一　情報システム更改時の情報の移行作業における情報セキュリティ対策

二　情報システム廃棄時の不要な情報の抹消

⑩ 受注者は、主体認証を行う情報システムにおいて、次の各号を含む主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずること。

一　利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して

定期的な変更を促す機能を設けること。また、その他に例として、利用者が定期的に変更しているか否かを確認する機能、利用者が定期的に変更しなければ情報システムの利用を継続させない機能、利用者が主体認証情報を変更する際に以前に設定した主体認証情報の再設定を防止する機能のような機能を設けること。

二　主体認証情報を送信又は保存する場合には、その内容を暗号化すること。

三　主体認証情報に対するアクセス制限を設けること。

また、主体認証情報を他の主体に不正に利用され、又は利用されるおそれを認識した場合の対策として、以下の機能を設けること。

イ　当該主体認証情報及び対応する識別コードの利用を停止する機能

ロ　主体認証情報の再設定を利用者に要求する機能

⑪　受注者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与（発行、更新及び変更を含む。以下本項において同じ。）し、次の各号を含む管理するための措置を講ずること。

一　主体以外の者が識別コード又は主体認証情報を設定する場合に、主体へ安全な方法で主体認証情報を配布するよう、措置を講ずること。

二　識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認証情報（必要に応じて、初期設定の識別コードも含む）を速やかに変更するよう、促すこと。

三　知識による主体認証方式を用いる場合には、他の情報システムで利用している主体認証情報を設定しないよう主体に注意を促すこと。

四　情報システムを利用する主体ごとに識別コードを個別に付与すること。ただし、やむを得ず共用識別コードを付与する必要がある場合には、利用者を特定するための仕組みを講ずること。

五　主体への識別コードの付与に関する記録を残すこと。消去する場合、機構から事前に許可を得ること

⑫　受注者は、主体が情報システムを利用する必要がなくなった場合において、当該主体の識別コード及び主体認証情報の不正な利用を防止するため、以下の措置を速やかに講ずること。

一　当該主体の識別コードを無効にすること。

二　当該主体に交付した主体認証情報格納装置を返還させること。

三　無効化した識別コードを他の主体に新たに発行することを禁止する

（４）システム全般のセキュリティ要件等

①　全般

イ　情報漏洩等の事故発生時の連絡体制及び責任の範囲が明確になっていること。

ロ　取り扱う情報に対して、守秘義務、目的外でのデータ利用の禁止、罰則・規定等が明確になっていること。

ハ　取り扱う情報に対して、国内法が適用されること。

ニ　取り扱う情報が、機構の意思により確実に削除・廃棄されること。

ホ　主体認証（ログイン時の ID・PW 入力等による人の判断を伴う認証方法）、アクセス制御（ＩＰアドレスによる端末のアクセス制限設定）、権限管理等の情報セキュリティ機能を備えていること。

ヘ　通信方式は SSL 等の暗号化の対策が講じられており、利用者の登録及び作業担当者の操作等による通信時の情報の漏えいを防ぐ仕組みが構築されていること。

ト　保存されるデータは、電子政府推奨暗号リストに記載されている暗号化方式による暗号化の対策が講じられていること。

チ　ウイルス対策、脆弱性対策、不正侵入対策が講じられていること。

リ　アクセスログ等の証跡を保存し、機構の求めに応じて提供できること。

ヌ　法律又は政府機関の拘束力ある命令を遵守するために必要な場合を除き、第三者に対してのデータプライバシー及びセキュリティが保証されること。

ル　サービスの利用にあたり、事業者のストレージに蓄積されるデータ（顧客データ、アプリケーションデータ、文書データ、図面データ及びログデータ等）のオーナーシップ（データを作成・改変・消去する権利）が保証され、サービス事業者によるデータの二次的利用（統計処理及びデータマイニング等）を許可しない等の選択ができること。また、個人情報保護法上の個人情報取扱事業者のサービスでは、「個人データを第三者に提供」する場合の「本人の同意」若しくは「事前の通知」が実施されていること。

ヲ　個人情報の保護にあたっては、サービス機能単体、受注者が複数のサービス機能を組み合わせたシステム全体及びデータライフサイクルに対し、セキュリティが最適化されたシステム構成となっていること。

ワ　公開サーバは、外部からのデータ（サーバ更新プログラム及びウィルスパターンファイル）の取得を間接的に行う等の出口を設けない経路設計となっていること。

カ　複数人に電子メールを送信する場合は、必要がある場合を除き、他の送信先の電子メールアドレスが分からないような仕様となっていること。

ヨ　受託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。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。

タ　受注者は、サービス提供に必要なクラウドサービスが装備している機能又

は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うこと。

また、以下のサービス不能攻撃に対抗するための機能を設けている場合は、これらを有効にしてサービス不能攻撃に対処すること。

a)パケットフィルタリング機能

b)3-way handshake 時のタイムアウトの短縮

c)各種 Flood 攻撃への防御

d)アプリケーションゲートウェイ機能

レ　受注者は、サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断する、又は通信回線の通信量を制限するなどの影響を最小とする手段を備えた情報システムを導入すること。

また、通信回線装置に設けられている機能を有効にするだけではサービス不能攻撃の影響を排除又は低減できない場合には、以下の対策を機構の承諾を得たうえで実施すること。

a) インターネットに接続している通信回線の提供元となる事業者が別途提供する、サービス不能攻撃に係る通信の遮断等の対策

b) サービス不能攻撃の影響を排除又は低減するための専用の対策装置の導入

c) 通信回線装置及び通信回線の冗長化

d) コンテンツデリバリーネットワーク（CDN）サービスの利用

ソ　受注者は、サービス不能攻撃を受け、クラウドサービスが過負荷状態に陥り利用できない場合を想定し、攻撃への対処を効率的に実施できる手段の確保について検討し、機構の承諾を得たうえで実施すること。

ツ　受注者は、サービス不能攻撃を受けるクラウドサービスから監視対象を特定し、監視すること。また、特定した監視対象について、監視方法及び監視記録の保存期間を定め、監視記録を保存すること。

ネ　受注者は、クラウドサービスに新たな機能が追加されていないか、アクセス権が適切に付与されているか等を定期的【６か月毎】に確認すること。また、確認の際は、作業日、作業を行ったクラウドサービス、作業内容及び作業者を含む事項を記録すること。

ナ　受注者は、クラウドサービスに対する内部不正を防止し、管理者アカウントの適正な権限管理を行うため、次の各号を含む措置を講ずること。

一　必要に応じて情報システムの管理者とデータベースの管理者を別にすること。

二　データベースに格納されているデータにアクセスする必要のない管理者に対して、データへのアクセス権を付与しないこと。

三　データベースの管理に関する権限の不適切な付与を検知できるよう、措

置を講ずること。

ラ　受注者は、クラウドサービスに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずること。

ム　受注者は、業務を遂行するに当たって不必要なデータの操作を検知できるよう、以下の措置を講ずること。

a）一定数以上のデータの取得に関するログを記録し、警告を発する。

b）データを取得した時刻が不自然であるなど、通常の業務によるデータベースの操作から逸脱した操作に関するログを記録し、警告を発する。

ウ　受注者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を機構に提案すること。

②　サービスの提供環境

イ　稼働信頼性は、99.9%以上の稼働実績があること。（年間停止時間は 8.8 時間以内）

ロ　サービスの中断や終了時に円滑に業務を移行、もしくは移行させるための対策が構築されていること。

ハ　サービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行っていること。

ニ　データベースへのアクセスについて、参照可能なネットワークを限定できること。

ホ　サービスの監視が 24 時間 365 日で行われていること。また、最新のセキュリティパッチ等が随時適用されていること。

ヘ　送信元メールアドレスとメールの送信サーバの関係性を確認する等、なりすましメール対策を行うことができる機能を、サービス提供事業者にて有すること。

ト　ファイアウォール、侵入防止システム（Intrusion Prevention System 以下、「IPS」という。）、WEB アプリケーションファイアウォール（Web Application Firewall 以下、「WAF」という。）により、サービス提供事業者にて外部からの不正アクセス等から保護されていること。

チ　個人情報が含まれるデータベースが非公開の領域に設置され、アプリケーションプログラミングインターフェース（Application Programming Interface 以下、「API」という。）等を介さない外部からの直接のアクセスがサービス提供事業者にて禁止されていること。

リ　受注者は、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。

ヌ　受注者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用すること。

ル　受注者は、主体から対象に対するアクセスの権限を適切に設定するよう、措置を講ずること。

ヲ　受注者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずること。

ワ　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必要なログを取得すること。また、情報システムに含まれる構成要素（サーバ装置・端末等）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。

カ　受注者は、情報システムにおいて、ログを取得する対象の機器等、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、不正な消去や改ざん及びアクセスを防止するための適切なアクセス制御を含むログ情報の保全方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理すること。

また、受注者は、ログとして取得する以下の情報項目を定め、管理すること。

a)　事象の主体（人物又は機器等）を示す識別コード
b)　識別コードの発行等の管理記録
c)　情報システムの操作記録
d)　事象の種類
e)　事象の対象
f)　正確な日付及び時刻
g)　試みられたアクセスに関わる情報
h)　電子メールのヘッダ情報及び送信内容
i)　通信パケットの内容
j)　操作する者、監視する者、保守する者等への通知の内容

ヨ　受注者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。

タ　通信回線を経由してサーバの保守作業を行う際に送受信される情報が漏えいすることを防止するための対策を講ずること。

レ　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。

ソ　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主体認証を行う機能を備えること。

ツ　受注者は、以下の電子メールのなりすましの防止策を講ずること。

一 SPF（Sender Policy Framework）、DKIM（DomainKeys Identified Mail）、DMARC（Domain-based Message Authentication, Reporting & Conformance）等の送信ドメイン認証技術による送信側の対策。

二 SPF、DKIM、 DMARC 等の送信ドメイン認証技術による受信側の対策。

三 S/MIME（Secure/Multipurpose Internet Mail Extensions）等の電子メールにおける電子署名の技術を利用。

ネ　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盗聴及び改ざんの防止策を講ずること。

一 SMTP によるサーバ間通信を TLS により保護する。

ナ　受注者は、ウェブサーバの管理や設定において、次の各号の事項を含む情報セキュリティ確保のための対策を講ずること。

一　ウェブサーバが備える機能不要な機能の停止又は制限として、以下のウェブサーバの管理や設定を行うこと。

a）CGI 機能を用いるスクリプト等は必要最低限のものに限定し、CGI 機能を必要としない場合は設定で CGI 機能を使用不可とする。

b）ディレクトリインデックスの表示を禁止する。

c）ウェブコンテンツ作成ツールやコンテンツ・マネジメント・システム（CMS）等における不要な機能を制限する。

d）ウェブサーバ上で動作するソフトウェアは、最新のものを利用するなど、既知の脆弱性が解消された状態を維持する。

二　ウェブコンテンツの編集作業を担当する主体の限定として、以下のウェブサーバの管理や設定を行うこと。

a）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。

b）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。

三　公開してはならない又は無意味なウェブコンテンツが公開されないよう管理することとして、以下のウェブサーバの管理や設定を行うこと。

イ　公開を想定していないファイルをウェブ公開用ディレクトリに置かない。

ロ　初期状態で用意されるサンプルのページ、プログラム等、不要なものは削除する。

ハ　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。

a) 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。

b) 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。

c) 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。

四　通信時の盗聴による第三者への情報の漏えい及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするための措置として、以下を含むウェブサーバの実装を行うこと。

a) TLS 機能を適切に用いる。

b) TLS 機能のために必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いる。

c) 暗号技術検討会及び関連委員会（CRYPTREC）により作成された「TLS 暗号設定ガイドライン」に従って、TLS サーバを適切に設定する。

ラ　受注者は、ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認すること。

ム　受注者は、DNS キャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずること。

また、機構外からの名前解決の要求に応じる必要性があるかについて検討し、必要性がないと判断される場合は必要であれば機構内からの名前解決の要求のみに応答をするよう、以下の措置を講ずること。

一 DNS キャッシュサーバの設定でアクセス制御を行う。

二ファイアウォール等でアクセス制御を行う 。

なお、DNS キャッシュポイズニング攻撃から保護するため、以下の措置を講ずること。

一ソースポートランダマイゼーション機能を導入する。

二 DNSSEC を利用する。

ウ　受注者は、DNS キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講ずること。また、DNS キャッシュサーバにおいて、ルートヒントファイル（DNS ルートサーバの情報が登録されたファイル）の更新の有無を定期的に確認し、最新の DNS ルートサーバの情報を維持すること。

ゐ　受注者は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認しなければならない。

ノ　メールシステムを構築する際は、当該電子メールのドメイン名に機構ドメイ

ン名（ur-net.go.jp）を使用すること。ただし、電子メールを受信する機構外の者が、機構から送信された電子メールであることを認知できる場合（機構ドメイン名が使用できない場合に限る。）は除く。

（５）情報セキュリティ監査の実施

「別紙１　作業の実施にあたっての遵守事項」のとおりとする。

（６）再委託に関する情報セキュリティ対策

「別紙１　作業の実施にあたっての遵守事項」のとおりとする。

なお、第三者に委託する場合も、当該事業者において同様の措置を定め、その最終的な責任を受注者が負うこと。

（７）情報セキュリティが侵害された場合の対処

「別紙１　作業の実施にあたっての遵守事項」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

別紙１　作業の実施にあたっての遵守事項

1. 情報セキュリティの確保

（情報の目的外利用の禁止）

(1) 受注者は、本業務の遂行のために必要な範囲に限って、情報を利用すること。

（情報セキュリティ対策の実施内容及び管理体制）

(2) 受注者は、次の各号の内容を含む情報セキュリティ対策の実施内容及び情報セキュリティ管理体制等に関する確認書等を提出すること。また、変更があった場合は、速やかに再提出すること。

一　当該委託業務に携わる者の特定

二　当該委託業務に携わる者が実施する具体的な情報セキュリティ対策の内容

（機構の意図せざる変更が加えられないための管理体制）

(3) 受注者は、本業務の遂行において、機構の意図しない変更が行われるなどの不正が見付かったときに、追跡調査や立入検査等、機構と外部サービス提供者が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。

（受注者の情報提供）

(4) 受注者の資本関係・役員等の情報、本業務の実施場所、本業務従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供を行うこと。

（情報セキュリティインシデントへの対処）

(5) 受注者は、本業務の遂行において、以下を含む情報セキュリティが侵害され又はその恐れがある場合には、直ちに機構に報告すること。

一　受注者に提供し、又は受注者によるアクセスを認める機構の情報の外部への漏えい及び目的外利用

二　受注者による本業務の範囲を超えた、機構が認めない情報への不正なアクセス

(6) 受注者は、被害の程度を把握するため、受注者は必要な記録類を契約終了時まで保存し、機構の求めに応じて成果物とともに機構に引き渡すこと。

一　情報セキュリティ侵害の内容及び影響範囲を調査の上、当該情報セキュリティ侵害への対応策を立案し、機構の承認を得た上で実施すること。

二　発生した事態の具体的内容、原因及び実施した対応策等について報告書を

作成し、機構へ納入して承認を得ること。

三　再発防止対策を立案し、機構の承認を得た上で実施すること。

四　上記のほか、発生した情報セキュリティ侵害について、機構の指示に基づく措置を実施すること。

（情報セキュリティ対策その他の契約の履行状況の確認）

(7) 受注者は、本業務の実施にあたり、定期的に情報セキュリティ対策の履行状況の報告を適切に行うこと。

（情報セキュリティ対策の履行が不十分な場合の対処）

(8) 受注者は、情報セキュリティ対策の履行が不十分な場合、もしくは機構により情報セキュリティ対策の利用が不十分と判断された場合には、改善策を提示し、機構の承諾を得た上で、その対策を速やかに実施すること。

2. 機密保持、資料の取り扱い

（機密保持）

(1) 受注者は、機密情報の保持について以下の内容を遵守すること。

一　本業務における各作業の実施中はもとより、作業の実施後も、本業務上のシステム構造、機器及びその他本契約を履行する上で知り得た全ての情報を第三者に開示、漏洩することのないこと。また、そのために必要な措置を講ずること。

二　機構が提供する資料については、原則として貸出しとし、導入完了期限までに返却、もしくは、機構と協議の上、適切な方法で廃棄すること。また、当該資料の複写及び第三者への提供はしないこと。

三　機構が提供した情報を第三者に開示する必要がある場合は、事前に機構と協議を行った上で承認を得ること。

（情報の取扱い）

(2) 受注者は、情報の提供等を受ける際、次の各号に掲げる事項を遵守すること。

一　要保護情報の提供を受ける場合は、提供される情報を必要最小限とし、あらかじめ定められた安全な方法で受渡しすること。

二　提供された要保護情報が不要になった場合は、これを確実に返却又は抹消すること。

(3) 受注者は、機構との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について機構と合意し、定められた手順により情報を取り扱うこと。

(4) 受注者は、本業務の終了時に、取り扱った情報を確実に返却、又は抹消したことを確認すること。

（法令等の遵守）

(5) 受注者は、本業務の遂行において、民法、刑法、著作権法、個人情報保護法、不正アクセス行為の禁止等に関する法律等の関連する法令等を遵守すること。

（情報セキュリティ監査）

(6) 受注者は、情報セキュリティ監査について、以下の内容を遵守すること。

イ　本業務の遂行にあたり、機構が必要と認めた場合は、機構の情報セキュリティ監査を受入れること。

ロ　情報セキュリティ監査の結果、機構が改善を求めた場合には、機構と協議の上、必要な改善策を立案して速やかに実施すること。

ハ　機構が外部からの監査を受けるにあたり、機構から指示があった場合には、受注者は、監査の対応に関して協力をすること。

3. 情報セキュリティ対策

（情報セキュリティポリシーの遵守）

政府機関統一基準等関連ガイドラインを理解した上で、次の機構の定めるセキュリティ関連規程及び個人情報保護規程を遵守し、システムの構成や特性に応じ情報の機密性・完全性・可用性を各々適切に確保し取組を行うものとすること。また、契約締結時に規程等が改正されている場合は、改正後の規程等を遵守すること。

【機構の定めるセキュリティ関連規程及び個人情報保護規程】

イ　独立行政法人都市再生機構情報化等管理規程（平成 20 年規程第 21 号）

ロ　独立行政法人都市再生機構情報化等管理に関する達（平成 20 年達第 21 号）

ハ　独立行政法人都市再生機構情報セキュリティ管理に関する規程（平成 20 年規程第 22 号）

ニ　独立行政法人都市再生機構情報セキュリティ管理に関する達（令和３年達第 29 号）

ホ　独立行政法人都市再生機構個人情報保護規程（平成 17 年規程第１号）

【政府機関統一基準等関連ガイドライン】

イ　政府情報システムの整備及び管理に関する標準ガイドライン（平成 26 年 12 月３日各府省情報化統括責任者(CIO)連絡会議決定）

ロ　政府機関等のサイバーセキュリティ対策のための統一基準群（令和 5 年度版）（令和 5 年７月 4 日、サイバーセキュリティ戦略本部・内閣サイバーセキュリテ

ィセンター）
（イ）政府機関等のサイバーセキュリティ対策のための統一規範
（ロ）政府機関等のサイバーセキュリティ対策のための統一基準（令和 5 年度版）
（ハ）政府機関等の対策基準策定のためのガイドライン（令和 5 年度版）
ハ　「高度サイバー攻撃対処のためのリスク評価等のガイドライン」（内閣サイバーセキュリティセンター）
（イ）『高度標的型攻撃』対策に向けたシステム設計ガイド（独立行政法人情報処理推進機構）
（ロ）『新しいタイプの攻撃』の対策に向けた設計・運用ガイド（独立行政法人情報処理推進機構）
（ハ）『標的型メール攻撃』対策に向けたシステム設計ガイド（独立行政法人情報処理推進機構）
ニ　「クラウドセキュリティガイドライン活用ガイドブック（2013 年度版）」（経済産業省）
ホ　「クラウドサービスの安全・信頼性に係る情報開示指針（総務省）」
（イ）「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）2021 年 9 月」
（ロ）「ASP・SaaS 事業者連携ガイド（平成 24 年 7 月策定）」
（ハ）「データセンターの安全・信頼性に係る情報開示指針（平成 23 年 12 月改定）」
（ニ）「IaaS・PaaS の安全・信頼性に係る情報開示指針（第２版）（平成 29 年３月改定）」
（ホ）「ASP・SaaS の安全・信頼性に係る情報開示指針（ASP・SaaS 編）第 3 版（令和４年 10 月改定」
ヘ　「安全なウェブサイトの作り方　改訂第７版　2021 年 3 月」（独立行政法人情報処理推進機構）
（イ）付属：「セキュリティ実装 チェックリスト」
（ロ）別冊：「安全な SQL の呼び出し方（2010 年 3 月 18 日公開）」
（ハ）別冊：「ウェブ健康診断仕様（2012 年 12 月 26 日公開）」
ト　「ISO／IEC 15408(CC) IT セキュリティ評価及び認証制度(JISEC) 」（独立行政法人情報処理推進機構）
チ　「サイバーセキュリティ経済基盤構築事業クラウドセキュリティ監査制度の見直し（平成 27 年 2 月）」（経済産業省）
リ　「政府情報システムのためのセキュリティ評価制度（ISMAP）」（令和 2 年 1 月 30 日サイバーセキュリティ戦略本部決定）

4. 再委託に関する事項

（再委託に関する対策）

(1) 受注者は、作業の全部を第三者に委託又は請け負わせないこと。作業の一部を第三者へ委託する場合、機構の承認を得ること。

(2) 受注者が作業の一部を第三者に委託する場合、受注者は知的財産権、情報セキュリティ（機密保持及び遵守事項）、ガバナンス等に関して本仕様書が定める受注者の債務一切を再委託先事業者も負うよう、必要な処置を実施し、機構に報告し、承認を得ること。

以　上

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