（別添）

デザイナーズバンク整備運用業務委託仕様書

この仕様書は、企画提案書作成用である。
企画提案競技後、埼玉県（以下「県」という。）は業務委託先候補者と仕様について協議を行い、協議が整った場合は仕様書を修正の上、業務委託契約を締結する。

１．委託業務名

デザイナーズバンク整備運用業務委託

２．業務の目的

企業と外部デザイナーとのマッチングを効果的に行うための人材データベース（以下「デザイナーズバンク」という。）を整備するため、デザイナーの募集・登録に係る業務を行う。併せて、企業のデザイン活用を総合的に支援するための特設ポータルサイトを制作・保守する。

３．委託期間

契約締結日から令和８年３月３１日まで

４．委託業務の内容

（１）デザイナーの募集・登録

①デザイナーズバンクに登録するデザイナーを募集し、データベースに登録・管理すること。

②業界のネットワークを活用するなど、多様な人材にデザイナーズバンクへの登録を働きかけること。

③サイト公開当初の登録デザイナー数は３０名以上とし、令和７年度末までに５０名以上とすること。

④デザイナーの募集に係る要件等に関しては、別に定めるデザイナー募集要領に従うこと。

⑤デザイナーをデータベースに登録し公開しようとする場合は、当該デザイナーに係る情報を県に提供の上、承認を得ること。

⑥登録デザイナーから登録解除の申請がありデータベースから削除する場合は、県に報告の上、承認を得ること。

⑦登録申請により取得した情報は、内容を整理の上、汎用的な形式（ＣＳＶ等）で県に提供すること。

⑧取得する個人情報は必要最小限とし、個人情報の取扱いについては、個人情報の保護に関する法律（平成１５年法律第５７号）に準拠すること。

⑨不要となった個人情報は、媒体の種類を問わず受託者の責任において速やかに適切な方法によって破棄すること。

（２）データベースの構築・管理

①デザイナーを登録するためのデータベースを構築すること。

②データベースサーバーは、受託者が用意すること。

③データベースは登録情報の正確性が担保されるよう厳密に管理すること。

④その他、システムの要件等に関しては、別紙１のシステム要件特記仕様書に従うこと。

（３）特設ポータルサイトの制作・保守

①ユーザーインターフェースに配慮した見やすく使いやすいＷｅｂサイトを制作すること。

②サイトのＵＲＬは、県のホームページ（https://www.pref.saitama.lg.jp/）のサブドメインとすること。

③Ｗｅｂサーバー及びＣＭＳサーバーは、受託者が用意すること。

④コンテンツの更新やセキュリティ対策など、サイトが最新の状態かつ安全に維持されるよう保守を行うこと。

⑤その他、システムの要件等に関しては、別紙１のシステム要件特記仕様書に従うこと。

５．提出書類

本委託業務の実施にあたり、別に定める必要書類を県に提出すること。詳細事項に関しては、別紙１のシステム要件特記仕様書、別紙２の情報セキュリティ特記仕様書、別紙３のウェブアクセシビリティ特記仕様書に従うこと。

６．スケジュール

特設ポータルサイトの公開時期は、別途協議の上、決定するものとする。ただし、遅くとも令和７年１１月上旬までには公開すること。

７．役割分担

本委託業務における主な役割分担は次のとおりとする。

①システム要件定義の提案（受託者）

②システム要件定義の決定（県）

③サーバー又はクラウドサービスの用意（受託者）

④データベースの構築・管理（受託者）

⑤Ｗｅｂサイトの制作・保守（受託者）

⑥デザイナーの募集（受託者）

⑦デザイナーの選考（県）

⑧デザイナーの登録（受託者）

⑨掲載内容等の校正（県）

⑩更新・運用保守（受託者）

８．成果物

成果物として、以下のデータ及び書類等を納品すること。なお、データによる成果物は、電子

媒体（ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ等）に保存の上、納品するものとする。
①サイト構成データ一式（コンテンツ、データベース、ＣＭＳ等一式）
②システム構成図（サイト構成図）
③マニュアル類一式（運用マニュアル、ユーザーマニュアル等）
④デザイナーズバンク登録者リスト（Ｅｘｃｅｌ又はＣＳＶ形式）
⑤登録デザイナーから提出された書類一式
⑥業務完了報告書
⑦議事録

【納品先】
埼玉県産業技術総合センター
川口市上青木３－１２－１８（ＳＫＩＰシティ内）

９．権利の帰属

（１）本委託業務の履行に伴い発生する成果物等に対する著作権は、原則として全て県に帰属するものとする。また、著作者人格権は行使しないものとする。

（２）その他、著作権等で疑義が生じた場合は、別途協議の上、決定するものとする。

１０．留意事項

（１）委託業務の全部又は一部を第三者に委託し、又は請け負わせてはならない。ただし、次の項目を開示し、あらかじめ県の承諾を得た場合はこの限りではない。なお、再委託受託者においても、セキュリティ対策は本仕様書のほか、別紙１のシステム要件特記仕様書及び別紙２の情報セキュリティ特記仕様書に則った取扱いとすること。
①再委託の相手方の名称及び住所
②再委託の相手方と受託者の関係性（資本関係、契約実績など）
③再委託を行う業務の範囲
④再委託の必要性
⑤再委託の契約金額

（２）再委託受託者が更なる再委託を申請する場合は、「１０（１）」に準ずるものとする。

（３）受託者は、本委託業務の実施にあたり、関係法令、条例及び規則等を遵守すること。

（４）本委託業務に関して知り得た秘密をみだりに他に漏らし、又は委託業務以外の目的に使用してはならない。委託期間が終了し、又は委託契約が解除された後においても同様とする。

（５）受託者が取扱う個人情報は、県が保有する個人情報として個人情報の保護に関する法律（平成１５年法律第５７号）の適用を受けるものとする。

（６）受託者は、本委託業務の履行にあたり、自己の責めに帰すべき事由により県に損害を与えたときは、その損害を賠償しなければならない。

（７）受託者は、本委託業務の履行にあたり、受託者の行為が原因で利用者その他の第三者に損害が生じた場合には、その賠償の責めを負うものとする。

（８）第三者が権利を有するイラスト、写真、映像等を使用する場合、第三者との間で発生する著作権その他知的財産権に関する手続きや使用料等の負担と責任は全て受託者が負うものとする。

（９）本委託業務の履行に係るコンテンツの作成費用及びセキュリティの脆弱性診断等に掛かる費用は、全て委託料に含むものとする。

（１０）県が受託者を決定した後、委託契約を締結するにあたり、この仕様書に定める事項及びこの仕様書に定められた事項以外に疑義が生じた場合は、遅滞なく県と協議を行うものとする。

１１．その他

（１）受託者に求める条件

①デザイナーと連携した企業支援の実績があり、埼玉県内の中小企業を支援できるデザイナーに協力を求めることができること。

②ＩＳＭＳ認証又はプライバシーマークの認定を受けていることが望ましい。

③ＩＳＯ９００１の認証又はこれと同等の認証を取得していることが望ましい。

④ＩＳＯ／ＩＥＣ２７００１又はＪＩＳＱ２７００１の認証を取得していることが望ましい。

（２）従事者に求める条件

①全体を統括する統括責任者を選任すること。

②統括責任者は、プロジェクトマネジメント協会が認定するＰＭＰ又は情報処理推進機構が認定するプロジェクトマネージャの資格を有する者であることが望ましい。

③統括責任者は、本委託業務に係るシステム導入と同規模以上のプロジェクトに関わるプロジェクトマネジメントの経験を有すること。

④要員のうち、少なくとも１人は本委託業務に係るシステム開発と同規模以上のプロジェクトの開発経験を有すること。

以 上

（別紙１）

システム要件特記仕様書

１．緒言

本特記仕様書は、デザイナーズバンク整備運用業務委託におけるシステム要件に関して、必要な事項を定めるものである。

２．データベース

（１）登録情報を効率的に管理・検索できるように設計・構築すること。また、将来的な拡張性を考慮し、柔軟かつスケーラブルな設計とすること。

（２）データベース管理システム（ＤＢＭＳ）を使用し、データの一貫性、整合性、可用性を確保すること。

（３）データベースに登録する情報については、埼玉県（以下「県」という。）と協議の上、決定すること。また、登録情報は汎用的な形式（ＣＳＶ等）で出力できるようにすること。

（４）データベースのアクセス権限は適切に管理し、必要なユーザーのみがアクセスできるようにすること。特に、管理者権限と一般ユーザーの権限を明確に区分すること。

３．特設ポータルサイト

（１）独立行政法人情報処理推進機構が作成している「安全なウェブサイトの作り方（改訂第７版)」に準拠すること。(https://www.ipa.go.jp/security/vuln/websecurity/about.html)

（２）総務省が定める「みんなの公共サイト運用ガイドライン」に基づき、アクセシビリティに配慮すること。(https://www.soumu.go.jp/main_sosiki/joho_tsusin/b_free/guideline.html)

（３）特設ポータルサイト（以下「サイト」という。）のコンテンツ及びデザイン等については、原則として受託者が設計・制作するものとするが、決定にあたっては県と協議を行うこと。

（４）サイトは、閲覧者側で特殊なソフトウェアをインストールすることなく、多くのブラウザで閲覧可能であること。また、パソコンやスマートフォンなどマルチデバイスに対応すること。

（５）データベースからデザイナーに係る情報を検索し、所定のフォーマットに従ってサイトに表示する機能を実装すること。

（６）サイト内に問合せフォームを設け、フォームに入力された情報は県が指定したメールアドレスに転送する設定とすること。

４．運用保守

（１）サイトの管理、コンテンツの更新、サーバー（Ｗｅｂサーバー、ＣＭＳサーバー、データベースサーバー）のインストール及び保守、テストサイト等による適正な管理に係る業務の一切を行うこと。ただし、緊急の対応を要する場合は、県がコンテンツの修正・更新を行えるようにすること。

（２）サイトの公開後、県から修正・更新の依頼があった場合には随時対応し、３営業日以内に作業を完了すること（ただし、大規模な修正・更新は除く）。

（３）ＣＭＳの認証画面はインターネット上に公開しないこと。やむを得ず公開する場合は、接続可能なＩＰアドレスをホワイトリストに登録し接続を制限するとともに、適切なタイムアウト時間を設定すること。また、ＣＭＳのアクセス権限は、受託者及び県にのみ付与すること。

（４）ＣＭＳの認証パスワードは、英字、数字、記号をそれぞれ１字以上含む１０字以上の予測されにくい文字列で設定すること。また、県が認証パスワードの変更を行えるようにすること。

（５）セキュリティ対策を十分に講じるとともに、個人情報の保護に関する法律（平成１５年法律第５７号）に準拠したデータ保護措置を確実に実施すること。

（６）サーバーにセキュリティパッチを適用し、常に最新の状態に保つこと。また、定期的なセキュリティ監査を実施すること。

（７）サーバーにウイルス対策ソフトを導入し、最新のウイルス定義ファイルを適用すること。ウイルススキャンは定期的に実施し、ウイルス感染の防止策を十分に講じること。また、ウイルス対策ソフトの稼働状況を定期的に監視し、問題が発生した場合には速やかに対応すること。

（８）問合せフォームにｒｅＣＡＰＴＣＨＡ等のセキュリティ対策を実装し、スパム攻撃を防ぐための措置を講じること。

（９）サーバーの障害発生時には迅速に対応できる体制を整えること。特に、重大な障害の発生時には、速やかに対応するための連絡体制を確立すること。

（１０）サーバーが攻撃を受けコンテンツが改ざんされるなどの被害が発生した場合は、速やかにサイトを非公開とする措置を講じるとともに県に報告すること。

（１１）各種サーバーのアクセスログを定期的にレビューし、不正アクセス又はこれに準じるインシデントが発生した場合は、速やかに適切な対策を講じるとともに県に報告すること。

（１２）アクセスログ、認証ログ、操作ログ、通信ログ、イベントログ、エラーログ等のログデータは、ログの取得日から１年間は適切に管理・保管すること。

（１３）サイトデータ及びデータベースのバックアップは１週間に１回、２世代を取得すること。また、バックアップデータは別の物理的な場所に保存し、災害やシステム障害に備えること。

（１４）ＳＳＬ／ＴＬＳサーバー証明書（ＤＶ）は適切に管理すること。証明書の取得、更新、インストール、および秘密鍵の管理を受託者が責任を持って行うこと。

（１５）サーバーの設定や構成変更は、適切な変更管理プロセスを経て行うこと。また、変更履歴を記録し、必要に応じてレビューを行うこと。

５．サーバー及びクラウドサービス

（１）Ｗｅｂサーバー、ＣＭＳサーバー、データベースサーバーは受託者が用意し、それぞれのサーバーは物理的に分割すること。

（２）コンテンツ及びデータベースの拡張に対応できるサーバーとすること。特に、サーバーのスケーラビリティを考慮し、将来的なトラフィック増加やデータ増加に対応できること。

（３）サーバーには、電子政府推奨暗号リストに記載された暗号化のアルゴリズムを使用し、個人情報など機密性が高い情報は暗号化して保管すること。

（４）サーバーには、不正アクセスを検知／防御するためのファイアウォール（ＦＷ）等のセキュリティ対策を講じること。また、ネットワークにはＷｅｂアプリケーションファイアウォール（ＷＡＦ）、侵入防止システム（ＩＰＳ）等のセキュリティ対策を講じること。

（５）サーバーとクライアント間の通信には、ＳＳＬ／ＴＬＳ暗号化通信を使用し、データの盗聴や改ざんを防止すること。ＴＬＳのバージョンは１．２以上とすること。

（６）サーバーのパフォーマンスを定期的に監視し、必要に応じてリソースの追加や調整を行うこと。特に、ピーク時のトラフィックにも耐えられる性能を確保すること。

（７）サーバーの設置場所は、出入口を必要最小限にとどめるとともに入退室の記録を取ること。また、監視カメラや認証機能等の活用により、不正な者の侵入を防止する措置を講じること。

（８）クラウドサービスを利用する場合は、以下の要件によること。

①日本国の法律及び締結された条約が適用される国内データセンターにおいてデータが管理され、日本国に裁判管轄権があるクラウドサービスであること。

②政府情報システムのためのセキュリティ評価制度（ＩＳＭＡＰ）のクラウドサービスリスト

に登録されているサービスを利用する場合は、登録状況を証明する書類を提出すること。非登録のサービスを利用する場合は、ＩＳＭＡＰ評価と同等であることを証明すること。

③グローバルにクラウドサービスを展開している場合でも、障害を局地的に限定できる構成になっていること。

④電子政府推奨暗号リストに記載された暗号化のアルゴリズムを使用し、マイクロソフトオフィス形式（Ｗｏｒｄ、Ｅｘｃｅｌ、ＰｏｗｅｒＰｏｉｎｔ等）やＰＤＦ、テキスト、画像、動画、音声ファイル等に対し、暗号化を行った上で保管できる機能を有すること。

⑤不正アクセスを検知／防御するためのＷｅｂアプリケーションファイアウォール（ＷＡＦ）、侵入防止システム（ＩＰＳ）等のセキュリティ対策を講じていること。

⑥ＩＤとパスワードによる認証要素以外にも対応した、多要素認証（ＭＦＡ）ができること。

⑦暗号化鍵をクラウドサービス上で適切に管理し、第三者による復号を防止できること。

⑧通信の不正傍受による漏洩を防ぐため、ＳＳＬ／ＴＬＳ暗号化通信による安全な接続が可能であること。ＴＬＳのバージョンは１．２以上とすること。

⑨クラウド利用時に必要なネットワーク帯域及び平時の標準的な反応速度をあらかじめ提示すること。必要なネットワーク帯域等は、本委託業務の利用シーンを考慮したものであること。

⑩サイトの公開が終了した場合、速やかにデータ消去の完了証明書を提出できるクラウドサービスであること。

⑪過去１年以上の障害情報を公開しているクラウドサービスであること。

６．対応デバイス等

ＣＭＳで生成されるページは、以下のデバイス及びブラウザに対応するものであること。なお、動作確認はそれぞれの最新バージョンで行うこと。

（１）デバイス

・パソコン（Ｗｉｎｄｏｗｓ、ＭａｃＯＳ）
・スマートフォン（Ａｎｄｒｏｉｄ、ｉＯＳ）
・タブレット端末（Ａｎｄｒｏｉｄ、ｉＯＳ）

（２）ブラウザ

・Ｇｏｏｇｌｅ Ｃｈｒｏｍｅ
・Ｍｉｃｒｏｓｏｆｔ Ｅｄｇｅ
・Ｓａｆａｒｉ
・Ｆｉｒｅｆｏｘ

７．データの消去

サイトの公開が終了した場合は、情報がサーバーに残置されないようＷｅｂサーバー、ＣＭＳサーバー、データベースサーバーに格納されたデータを、以下のいずれかの方法により完全消去すること。

（１）物理的消去

記録媒体を物理的な方法により破壊し、データの復元ができないようにする。

（２）磁気的消去
記録媒体を磁気的な方法により破壊し、データの復元ができないようにする。

（３）上書き消去
データ消去装置又はデータ消去ソフトウェアによりアクセス不可領域を含むデータを上書きし、データの復元ができないようにする。

（４）暗号化消去
データを暗号化し、暗号鍵を破棄することでデータの使用ができないようにする。

８．提出書類

（１）データベース設計書
データベースのスキーマ設計、テーブル構成、フィールド定義、リレーションシップ、インデックス設定などを記載すること。

（２）サイトデザイン設計書
デザインコンセプト、ワイヤーフレーム、ＵＩ／ＵＸ設計に関する詳細を記載すること。

（３）サーバー仕様書
Ｗｅｂサーバー、ＣＭＳサーバー、データベースサーバーのハードウェア及びソフトウェアの構成、ネットワーク構成などを記載すること。また、クラウドサービスを利用する場合は、クラウドサービスの詳細、提供するサービスの範囲、サービスレベルアグリーメント（ＳＬＡ）、セキュリティ対策、バックアップ及びリストアの手順、冗長構成などを記載すること。

（４）セキュリティ対策計画書
サーバー又はクラウドサービスにおけるセキュリティ対策の詳細、ウイルス対策ソフトの導入状況、ファイアウォール設定、アクセス制御、データ暗号化、認証方式（多要素認証含む）などを記載すること。

（５）運用管理計画書
サーバー又はクラウドサービスの運用管理体制、連絡体制、メンテナンス計画、バックアップの取得頻度、保存期間、保存場所、データのリストア手順、リストアテストの実施計画などを記載すること。

（６）障害対応計画書
サーバー又はクラウドサービスの障害対応手順、障害報告書及び再発防止策の提出方法などを記載すること。

（７）データ削除計画書

サイトの公開が終了した場合のデータ消去手順、消去完了の証明方法、消去に関する報告書の提出方法などを記載すること。

９．その他

（１）検索エンジンで上位に表示されるよう、サイトのサーチエンジン最適化（ＳＥＯ）対策を行うこと。

（２）Ｇｏｏｇｌｅアナリティクス等のサービスにより、サイトへのアクセス状況を把握できるようにすること。

（３）アクセス分析に必要なアカウントの取得など、必要な作業は受託者の責任において実施すること。

（４）サイトに掲載するイラスト、写真、映像等のコンテンツの著作権・肖像権等の取扱いには十分留意すること。

（５）セキュリティ対策については、本特記仕様書の定めによるほか、別紙２の情報セキュリティ特記仕様書に則った取扱いとすること。

（６）アクセシビリティ対応については、本特記仕様書の定めによるほか、別紙３のウェブアクセシビリティ特記仕様書に則った取扱いとすること。

以 上

（別紙２）

情報セキュリティ特記仕様書

１．緒言

本特記仕様書は、デザイナーズバンク整備運用業務委託における情報セキュリティに関して、必要な事項を定めるものである。

２．実施計画書の提出

（１）受託者（以下「乙」という。）は、本件業務を行うに先立って、実施体制、責任者、実施方法、作業場所、スケジュール等を記した実施計画書を作成し、埼玉県（以下「甲」という。）に提出し、甲の承認を得なければならない。実施計画書を変更する場合も同様とする。
（２）甲は、乙から提出された実施計画書に対して必要な指示をすることができる。

３．従事者の監督

乙は、本件業務に関わる実施体制（連絡体制を含む。）及び要員の一覧表を甲に提出し、甲の承認を得なければならない。要員に変更があった場合も同様とする。

４．状況報告書の提出

（１）乙は、甲、乙双方の合意に基づき定めた期間、方法及び内容等で本件業務の作業状況等について、甲が認めた場合を除き書面により報告しなければならない。
（２）前項の規定にかかわらず、乙は、甲から本件業務の作業状況等について報告を求められたときは、甲が指示する方法及び内容等により、これを報告しなければならない。
（３）甲は、状況報告に対して必要な指示をすることができる。

５．情報及び資料等の管理

本件業務を行うために、甲から提供された情報（以下「情報」という。）が記録された資料（以下「資料」という。）等の管理については、以下の事項に従わなければならない。
（１）乙は、資料等の一覧表を作成しなければならない。
（２）乙は、資料等の複製、提供、業務作業場所以外への持ち出し、送信その他個人情報を含めて適切な管理に支障を及ぼすおそれのある行為をしてはならない。ただし、あらかじめ甲の承諾を受けたときは、この限りではない。
（３）乙は、資料等、作業中のデータ及び甲に帰属した成果物を、甲の承諾を得ずに、甲の指示する目的以外に使用及び第三者への提供をしてはならない。
（４）乙は、甲の承諾を得ずに、資料等、作業中のデータ及び甲に帰属した成果物を作業場所から持ち出してはならない。
（５）乙は、資料等及び作業中のデータをその貸与目的を達したとき又は契約終了時に返却、廃棄又は消去しなければならない。複製物及び貸与された資料をもとに変更したものも同様とする。
（６）乙は、資料等を甲の承認を得て破壊した場合、確実に破壊した旨の証明を書面で甲に提出

しなければならない。
（７）乙は、資料等及び作業中のデータの保護・管理に必要な手続きを作成し、資料等を閲覧できる者や方法の制限等を行わなければならない。
（８）乙は、提供された資料等の内容については、公知の事実となるまで契約終了後も他言してはならない。

６．本人確認

乙は、本件業務の履行に関わる要員が納入場所等に立ち入る場合名札を着用させるとともに、乙の要員であること、要員本人であることを証するものを携帯させなければならない。

７．安全確保上の問題への対応

（１）乙は、本件業務の遂行に支障が生じるおそれのある事故の発生を知り得たときは、直ちにその旨を甲に報告し、遅延なくその措置状況を書面により報告しなければならない。
（２）甲は、前項の規定により報告を受けたときは、乙に対し、被害の拡大の防止又は復旧のために必要な措置に関する指示を行い、乙は当該指示に従わなければならない。
（３）乙は、事案の内容、影響等に応じて、その事実関係及び再発防止策の公表等の措置を甲と協力して講じなければならない。

８．要員の教育

（１）乙は、本件業務にかかわる全要員に対して、本件業務を遂行するために必要な教育を行わなければならない。
（２）乙は、教育に関する計画及び実施実績について甲に報告しなければならない。
（３）乙が行う教育には、ドキュメントの取扱方法、個人識別情報の取扱方法、データの取扱方法、事故時の連絡体制、個人情報の取扱方法を含まなければならない。
（４）甲は、乙の提出した教育に関する計画及び実施実績について必要な指示をすることができる。

９．作業上の権限

（１）乙は、本件業務の実施において、情報へのアクセス制御を設け、要員に対し、必要なアクセス権のみを付与するものとする。
（２）乙は、甲の情報をシステムで操作する場合操作記録を作成すること。（ログを保存すること。）
（３）乙は、甲の要求があったとき、操作記録（ログ）を甲に提示しなければならない。

１０．機器の管理

（１）乙は、本件業務の実施に使用するコンピュータ機器等を限定しなければならない。
ただし、甲の承認を得た場合はこの限りではない。
（２）乙は、前号の機器等の盗難、破壊等の防止策を講じなければならない。
（３）乙は、甲から貸与された機器等についても同様の措置をとらなければならない。

１１．機器及び納品物のウイルスチェック

（１）乙は、本件業務を履行するために使用するコンピュータ等の機器に対してウィルス対策ソフトを導入する等のコンピュータウイルス感染防止策を講じなければならない。

（２）乙は、甲に対して納品する電子データがコンピュータウイルスに感染していないことを甲の指定する方法で保障しなければならない。

（３）乙は、甲から貸与された機器に対しても（１）の措置を行うものとする。

１２．テストの実施方法

（１）テストに際しては、乙は、テストスケジュール、テスト内容、テストデータ内容等を記したテスト計画を作成し、甲の承認を得なければならない。

（２）乙は、テストの実施後、テスト内容、テスト結果、改善スケジュール等を記したテスト報告書を提出し、甲の承認を得なければならない。

１３．管理規定

（１）乙は、本件業務の実施について以下の規定を定めなければならない。

ア．セキュリティ事故の場合の連絡体制

イ．甲から提供された資料等の保管方法と責任者

ウ．甲から提供された資料等にアクセスできる者の名簿、管理責任者

エ．甲から提供された資料等のアクセス記録の管理方法

オ．本件業務の実施において作成された資料等（データ、ドキュメント、出力帳票、入力帳票、プログラム、設定ファイル、ログ等）にアクセスできる者の名簿、管理責任者

カ．本件業務の実施において作成された資料等のアクセス記録の管理方法と管理責任者

キ．甲から提供された資料等及び本件業務の実施において作成された資料等の返却または破壊方法と返却・破壊管理者

ク．コンピュータ等の機器の管理方法と責任者ケ コンピュータウイルス対策

（２）乙は、甲からの請求があった場合、前号の規定により作成されたドキュメントを速やかに提示しなければならない。

１４．検査権

（１）甲は、乙が行う本件業務に関して、口頭、書面及び立入りにより検査を行うことができる。

（２）甲は、乙に対し、必要な指示を出すことができる。

（３）乙は、甲からの検査要求及び甲からの指示に対して誠実に協力しなければならない。

１５．協力会社等に対する責任

（１）乙は、本件業務を実施するに際して自社以外の企業、個人（以下「協力会社等」という。）を利用する場合、協力会社等に対して本契約の定めを周知・指導しなければならない。

（２）協力会社等の行為は、乙の行為とみなす。

１６．その他

乙は、本件業務の実施について本契約書、仕様書及び甲から提出された資料等に明記されていない事態が発生した場合、速やかに甲に報告し、甲の指示を仰がなければならない。

以 上

（別紙３）

ウェブアクセシビリティ特記仕様書

１．緒言

本特記仕様書は、デザイナーズバンク整備運用業務委託におけるウェブアクセシビリティに関して、必要な事項を定めるものである。

２．適用範囲

埼玉県（以下「県」という。）からホームページ作成・保守・運用業務等（以下「作成等」という。）の委託を受けた受託者は、契約書及び仕様書等に定めのない事項について、ウェブアクセシビリティ達成のため、この特記仕様書に定める事項に従って契約を履行しなければならない。なお、この特記仕様書の適用範囲は受託者が本契約で作成等するウェブコンテンツに限る。

３．ウェブアクセシビリティ確保に係る基本的対応

（１）受託者は作成等にあたっては、JIS X 8341-3:2016 に規定する適合レベルＡ及びＡＡの達成基準に該当する事項をすべて満たすこと

（２）ＰＤＦや動画等、ＨＴＭＬ以外の特定の技術を用いたコンテンツについても同様とするが、上記を満たすことが難しいと考えられる場合には、県と協議の上対応すること

（３）受託者が本契約で作成等するウェブコンテンツ一式において、県が別の方針を定めた場合にはこの限りではない

４．ウェブアクセシビリティ試験の実施

受託者はウェブアクセシビリティ基盤委員会が示す「JIS X 8341-3:2016 試験実施ガイドライン」に基づき作成後のコンテンツに対し、ウェブアクセシビリティ試験を実施するものとする。試験実施に当たっては、以下のとおりとする。

（１）対象ページの数が１５ページ未満の場合

JIS X 8341-3:2016 の「JB.1.1 ウェブページ単位」とし、「a 全てのウェブページを選択する場合」にある方法を用いて、全てのページで試験及び確認を実施すること。

（２）対象ページの数が１５ページ以上３９ページ以下の場合

JIS X 8341-3:2016 の「JB1.2 ウェブページ一式単位」とし、「d ウェブページ一式を代表するウェブページとランダムに選択したウェブページとを併せて選択する場合」にある方法を用いて、両方のページを組み合せて１５ページ以上を選択して 試験及び確認を実施すること。なお、組合せにおける「ウェブページ一式を代表するウェブページ」と「ランダムに選択したウェブページ」の割合や、「ウェブページ一式を代表するウェブページ」で選択するページについては県と協議の上決定すること。

（３）対象ページの数が４０ページ以上の場合

JIS X 8341-3:2016 の「JB1.2 ウェブページ一式単位」とし、「d ウェブページ一式を代表するウェブページとランダムに選択したウェブページとを併せて選択する場合」にある方法を用いて、

両方のページを組み合せて４０ページ以上を選択して 試験及び確認を実施すること。なお、組合せにおける「ウェブページ一式を代表するウェブページ」と「ランダムに選択したウェブページ」の割合や、「ウェブページ一式を代表するウェブページ」で選択するページについては県と協議の上決定すること。

５．ウェブアクセシビリティ試験の報告

受託者は、試験の実施後、試験内容、試験結果、改善スケジュール等を記した試験結果報告書を提出し、県の承認を得なければならないこと。

６．保守・運用契約におけるウェブアクセシビリティ品質確保

受託者が保守・運用を行う場合、前項に定めるウェブアクセシビリティ試験のほか、県から契約期間中にウェブアクセシビリティに関する問合せがあった際、別紙４のアクセシビリティ品質確認書により回答を行い、問題と認められた場合にはウェブアクセシビリティ品質確保のための修正を適宜実施または提案すること。

以上

（別紙4）

アクセシビリティ品質確認書

問い合わせ日時　　年　月　日　：

問い合わせ対象ページ（URL）

問い合わせ内容（ページ内の部位、現象、操作上の困難など）

状況確認日時　　年　月　日　：

状況確認結果

（選択してください）

問題と認められた場合には、以下の項目に漏れなく記載のこと

関連する
JIS X 8341-3:2016 達成基準

アクセスできない環境や不便さを感じる利用者に関する説明

改修開始日　　年　月　日

改修完了日　　年　月　日

検証環境・検証に用いたソフトウェア等

改修が不可能な場合、その理由

改修内容に関する問い合わせ先