

仕様書（案）

1 件名

こども家庭庁ホームページにおけるこども向けWEBサイト構築業務

2 背景及び目的

(1) 背景

日本国憲法及び児童の権利に関する条約の精神に則り、次代の社会を担う全てのこどもが、生涯にわたる人格形成の基礎を築き、自立した個人として等しく健やかに成長することができ、こどもの心身の状況、置かれている環境等にかかわらず、その権利の擁護が図られ、将来にわたって幸福な生活を送ることができる社会の実現を目指して、こども施策を総合的に推進することを目的として令和5年4月に「こども基本法」が施行される。

同じく、令和5年4月には、こどもが自立した個人として等しく健やかに成長することのできる社会の実現に向け、子育てにおける家庭の役割の重要性を踏まえつつ、こどもの年齢及び発達の程度に応じ、その意見を尊重し、その最善の利益を優先して考慮することを基本とし、こどもと家庭の福祉の増進・保健の向上等の支援、並びにこどもの権利利益の擁護に関する事務を行うことを任務とする「こども家庭庁」が発足されることとなった。

こども政策の充実は待ったなしの課題であり、こども基本法を着実に施行し、こどもにとって最善の利益を第一にした「こどもまんなか社会」の実現に向けた施策の一つとして“こども家庭庁のホームページ”を構築する。

(2) 目的

本事業では、一般ユーザー（大人）向けのオフィシャルサイトとは別に、こども向け、特に小学生から中学生に対してこども家庭庁の役割やその施策、並びに子どもの権利利益等について分かりやすく伝え、相談窓口等を容易に検索できる等のコンテンツを備えた、日常的にアクセスすることを想定（目標）とするこども向けWEBサイト（以下「WEBサイト」という。）の構築を目的とする。

詳細については「5.1.1 WEBサイトに要求する事項」によるものとする。

また、構築にあたっては、「こども政策の新たな推進体制に関する基本指針について（令和3年12月21日閣議決定。以下「基本方針」という。）」に留意する。

【参考】内閣官房ホームページ「こども政策の推進（こども家庭庁の設置等）」

https://www.cas.go.jp/jp/seisaku/kodomo_seisaku_suishin/index.html

3 調達の範囲

- (1) WEBサイトの構築
(WEBサイト設計、デザイン制作、コンテンツ制作、システム設計)
- (2) WEBサイト用システム環境の構築 (ライセンス等を含む)
- (3) 初期運用
- (4) 成果物の提出

4 実施時期

契約締結後から令和6年3月31日(日)まで

(ただし、一次オープン：令和5年11月1日(水)を目標とする)

5 委託業務の内容

- (1) 以下の業務を行うこと。業務の実施に当たっては、随時、官側と十分調整を図りつつ行うこと。なお、請負者は、本業務の実施に当たり必要となる一切の手続を行うこと。
- (2) 業務の実施にあたって、請負者は、作業実施計画書(案)及び作業実施要領(案)を作成し、契約締結後速やかに官側に提出し、承認を受けること。

5.1 WEBサイトの構築

請負者は、デザイン制作等全般について、請負者から企画提案され、官側との技術的対話を行った企画を基に、十分に官側と協議の上決定すること。

5.1.1 WEBサイトに要求する事項

当該WEBサイトは、こどもが日常的にアクセスすることを想定し、こども政策について分かりやすく伝え、相談窓口等を容易に検索できる等のコンテンツを備えたものとするため、以下について、要求するものとする。

- (1) 前提
 - ① 本事業で構築するWEBサイトの主な訴求対象者は、小学生から中学生程度とする。※以下、本仕様書に示す「こども」は、小学生から中学生を指すこととする。
 - ② 基本方針にある内容が十分に反映されていること。
 - ③ こども家庭庁(国)という特性(個性)を活用したホームページであること。
 - ④ WEBサイトのデザインは、PC、タブレットからのアクセスに対応できるものであることのほか、スマートフォンからのアクセスに適合した画面デザインであること。
 - ⑤ WEBサイトの運用開始後に、官側の作成したコンテンツ等を追加、削除等が可能となるよう、拡張性が確保されていること。

(2) 全 般

- ① 親しみやすい（直感的、デザインの、遊び仕掛けの）なUIであること。
- ② 障害を持つ子どもや日本に居住する外国人の子どもなど、さまざまな子どもに配慮する工夫がされていること。
- ③ 親子で楽しむことのできる工夫がされているものであること。
- ④ 繰り返しサイトを訪れるよう日常的に利用できるコンテンツやデザインとすること。（例：天気予報、日めくりカレンダー）
- ⑤ 子どもが楽しめるゲームや動画、コミュニケーション（情報共有・交換）ツール、民間連携（キャラクターとのコラボ等）を活用したコンテンツ等を備えていること。
- ⑥ 別途構築している一般ユーザー（大人）向けのオフィシャルサイトの各コンテンツとWEBサイトの内容が関連する場合、オフィシャルサイトの各コンテンツへのリンクを設けること。

(3) 情報発信

- ① 子ども基本法について分かりやすく紹介すること。なお、基礎情報については、官側が提供するものとする。
- ② 子ども政策について分かりやすく紹介すること。なお、基礎情報については、官側が提供するものとする。
- ③ 子ども家庭庁の仕事について分かりやすく紹介すること。なお、基礎情報については、官側が提供するものとする。
- ④ こどもの悩みに関する解決のヒントや癒しへの考え方などについて紹介すること。
- ⑤ こどもの相談内容に応じた全国都道府県・市区町村の相談窓口等を紹介する仕組みを設けると共に検索が容易にできること。なお、相談窓口の情報については官側が提供するものとする。
- ⑥ こどもの関心事項（例えば、ドリル、時事問題、職業紹介、図鑑、夏休みの宿題、学校では教えてくれない大切なこと、経済の流れ、テレビ動画等）について紹介・提供を行う仕組みを設けること。

(4) その他（子ども家庭庁以外）のコンテンツ

- ① 学校や自治体等などが制作した、子どもに関するコンテンツ情報を掲載することを想定し、その情報を掲示する仕組みを備えること。
- ② 各府省の子ども向けホームページや子ども向けコンテンツへのリンク集を作成すること。

5.1.2 有識者による検証

- (1) サイト内の表現について、有識者によるヒアリングを実施しアドバイスを受けて反映すること。
- (2) 有識者については、「子どもセーフガーディングの観点」、「インクルーシブの観点」から選定すること。
- (3) 有識者への謝金等については、請負者の負担とする。

5.1.3 制作プロセスにおけるこども参加

サイトの制作プロセスにおいて、アンケートやヒアリング等を実施するなど、こどもの意見やアイデアについて反映させること。

5.1.4 アプリケーション・コンテンツの作成に係る事項

- (1) 文字コードはUTF-8。HTML5/CSS3で、W3C推奨の文書構造であること。
- (2) 制作に当たっては、次の対応を行うこと。
 - ① レスポンシブウェブデザインを採用すること。
 - ② SEO対策を行うこと。
- (3) 「Webサイトガイドブック」（内閣官房 情報通信技術（IT）総合戦略室）
（政府CIOポータル：<https://cio.go.jp/guides>に公開されている
https://cio.go.jp/sites/default/files/uploads/documents/1012_web_guidebook.pdf）に準拠すること。ただし「こども」を訴求対象する特性を考慮し、ガイドラインが馴染まないと判断する場合は、必ずしもこの限りではない。
- (4) WEBサイトの利用規約は、政府標準利用規約を使用すること。
（参考：<https://www.cas.go.jp/jp/tyosakuken/index.html>）
- (5) 以下の事項を含む措置を適切に実施すること。
 - ① アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行うこと。
 - ② 作成するアプリケーション・コンテンツが不正プログラムを含まないこと。
 - ③ 作成するアプリケーション・コンテンツが脆弱性を含まないこと。
 - ④ 実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。
 - ⑤ 作製するアプリケーション・コンテンツが改ざん等なく真正なものであることを確認できる手段を設けること。また、改ざん対策等において電子署名を用いる場合、政府認証基盤（GPKI）を利用すること。
 - ⑥ アプリケーション・コンテンツの利用時に、利用者側環境OS、ソフトウェア等の設定変更を要求することがないように、提供方式を定めてアプリケーション・コンテンツを開発すること。なお、ブラウザ設定においてJavaScriptをオン(有効)にする等の最低限の設定変更は許容するが、その旨を利用者に

通知すること。

- ⑦ サービス利用に当たって必須でない機能の悪用やバックドアへの対策を施すこと。
- ⑧ アプリケーション・コンテンツからこども家庭庁外のサーバ等へのアクセスが発生する場合は、当庁に承認を得るとともに、そのアクセスが情報セキュリティ上、安全なものであることを必ず確認すること。

5.2 WEBサーバの導入

5.2.1 システム要件

本サイトは、パブリッククラウド上に構築する。

確認用環境・本番環境それぞれにおいて、以下のとおり導入を行うものとする。

- (1) 当該ホームページを構築するサーバは「政府情報システムのためのセキュリティ評価制度（ISMAP）」を取得しているものを利用すること。
- (2) アプリケーション・コンテンツの作成にあたり、事前にユーザ及び管理者（官側）それぞれの役割（ニーズ）について官側と協議をすること。
- (3) セキュリティ要件

「情報セキュリティ要件については、契約後に別途提示する「(仮称) こども家庭庁情報セキュリティポリシー」、「政府機関等の情報セキュリティ対策のための統一基準群」及び下記の要件を満たすよう整理・検討すること。

- ① 通信経路の分離
 - ・不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離すること。
- ② 不正通信の遮断
 - ・通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。
- ③ 通信のなりすまし防止
 - ・情報システムのなりすましを防止するために、サーバの正当性を確認できる機能を備えること。
- ④ サービス不能化の防止
 - ・サービスの継続性を確保するため、構成機器が備えるサービス停止の脅威の軽減に有効な機能を活用して情報システムを構築すること。
- ⑤ 不正プログラムの感染防止
 - ・不正プログラム（ウイルス、ワーム、ボット等）による脅威に備えるため、想定される不正プログラムの感染経路の全てにおいて感染を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。

- ⑥ 不正プログラム対策の管理
 - ・システム全体として不正プログラムの感染防止機能を確実に動作させるため、当該機能の動作状況及び更新状況を一元管理する機能を備えること。
- ⑦ ログの蓄積・管理
 - ・情報システムに対する不正行為の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関するログを蓄積し、1年以上保管すること。
- ⑧ ログの保護
 - ・ログの不正な改ざんや削除を防止するため、ログに関するアクセス制御機能を備えること。
- ⑨ 時刻の正確性確保
 - ・情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。
- ⑩ 侵入検知
 - ・不正行為に迅速に対処するため、通信回線を介して所属する府省庁外と送受信される通信内容を監視し、不正アクセスや不正侵入を検知及び通知する機能を備えること。
- ⑪ サービス不能化の検知
 - ・サービスの継続性を確保するため、大量のアクセスや機器の異常による、サーバ装置、通信回線装置又は通信回線の過負荷状態を検知する機能を備えること。
- ⑫ 管理者権限の保護
 - ・特権を有する管理者による不正を防止するため、管理者権限を制御する機能を備えること。
- ⑬ システムの構成管理
 - ・情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに、文書どおりの構成とすること。
- ⑭ 調達する機器等に不正プログラム等が組み込まれることへの対策
 - ・機器等の製造工程において、府省庁が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。

- ⑮ 構築時の脆弱性対策
 - ・情報システムを構成するソフトウェア及びハードウェアの脆弱性を悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。
 - ⑯ 運用時の脆弱性対策
 - ・運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を効率的に実施する機能を備えるとともに、情報システム全体の更新漏れを防止する機能を備えること。
 - ⑰ クラウドセキュリティの確保
 - ・クラウドサービスを利用する場合は、使用するクラウドサービス（IaaS、PaaS、SaaS 等）の特性を踏まえて当該 WEB サイトのセキュリティ責任範囲を明確にし、予防的統制と発見的統制を講じること。
 - ⑱ その他
 - ・受諾者は、開発の各工程において、本セキュリティ要件に則ってセキュリティ対策がもれなく実装されていることを検証する方法を定め、要件のトレーサビリティを確保することが求められる。
開発工程以降、セキュリティ対策を具体化する過程でセキュリティ上の懸念が発生した場合は、本要件のみに縛られず、必要に応じて追加のセキュリティ対策を講じること。
- (4) 外部サービスの利用に関する事項（要機密情報を取り扱う場合）
- ① 共通事項
 - ア 要機密情報を取り扱う外部サービスの利用に関しては、「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3年度版）4.2.1 要機密情報を取り扱う場合」の内容に遵守すること。
 - イ クラウドサービス選定においては「政府情報システムにおけるセキュリティバイデザインガイドライン 別紙5政府情報システムにおけるクラウドセキュリティ要件策定、審査手順」の手順に従い、クラウドサービスの選定をおこなうこと
 - ② クラウドサービスに係る個別事項
 - ア 政府情報システムの保護に関する事項
 - ・情報資産を管理するデータセンターの物理的所在地が日本国内であること。
 - ・個人情報保有する場合には、日本国内外からの不正なアクセスが行われないようにすること。
 - ・官側の指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。

- ・障害発生時に縮退運転を行う際にも、情報資産が日本国外のデータセンターに移管されないこと。
- ・クラウドサービスの利用契約に関連して生じる一切の紛争は、日本の地方裁判所を専属的合意管轄裁判所とするものであること。
- ・契約の解釈が日本法に基づくものであること。
- ・情報資産の所有権がクラウドサービス事業者に移管されるものではないこと。従って、官側が要求する任意の時点で情報資産を他の環境に移管させることができること。
- ・法令や規制に従って、クラウドサービス上の記録を保護すること。
- ・情報資産が残留して漏えいすることがないように、必要な措置を講じること。
- ・自らの知的財産権についてクラウドサービス利用者に利用を許諾する範囲及び制約を、クラウドサービス利用者に通知すること。

イ 参考事項

- ・SaaSベースで構築することを前提に検討し、SaaSでは要件を満たさない場合は、PaaS、IaaSなどを選択すること。
- ・今後、利用者の拡大が見込まれることから、今後の発行アカウント数の拡大時の安定稼働や運用費用の抑制等の観点から、本調達の趣旨に適したクラウドサービスを利用すること。

5.2.2 設計

- (1) 基本設計及び詳細設計を行い、成果物について官側の承認を受けること。
- (2) 運用設計及び保守設計を行い、定常時における月次の作業内容、その想定スケジュール、障害発生時における作業内容等を取りまとめた運用・保守作業計画の案を作成し、官側の確認を受けること。
- (3) 請負者は、以下に掲げる事項について記載した情報システム台帳を、作業実施要領において定める時期に、提出すること。なお、民間事業者等が提供する情報処理サービスにより情報システムを構築する場合は⑧から⑬を含むものとする。
 - ① 情報システム名
 - ② 管理課室
 - ③ 情報システムセキュリティ責任者の氏名及び連絡先
 - ④ システム構成
 - ⑤ 接続するこども家庭庁外通信回線の種別
 - ⑥ 取り扱う情報の格付及び取扱制限に関する事項
 - ⑦ 当該情報システムの設計・開発、運用・保守に関する事項
 - ⑧ 情報処理サービス名
 - ⑨ 契約事業者
 - ⑩ 契約期間

- ⑪ 情報処理サービスの概要
- ⑫ ドメイン名
- ⑬ 取り扱う情報の格付及び取扱制限に関する事項

5.2.3 導入・テスト

- (1) 単体テスト、結合テスト及び総合テストについて、テスト体制、テスト環境、作業内容、作業スケジュール、テストシナリオ、合否判定基準等を記載したテスト計画書を作成し、官側の承認を受けること。
- (2) 設計工程の成果物及びテスト計画書に基づき、導入、テストを行うこと。
また、テスト計画書に基づき、各テストの実施状況を官側に報告すること。

5.2.4 受入テスト支援

- (1) 官側が受入テストのテスト計画書を作成するに当たり、情報提供等の支援を行うこと。
- (2) 官側が受入テストを実施するに当たり、環境整備、運用等の支援を行うこと。

5.3 初期運用

テスト環境・本番環境それぞれにおいて、一定の期間、以下のとおり運用・保守を行うものとする。

5.3.1 ウェブサーバ等の初期運用・保守

- (1) 運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を行う方法（手順等）を備えること。
- (2) 運用・保守にあたっては、クラウドのマネージドサービス等を使用するなどし、自動化すること。

5.3.2 定常時対応

- (1) 定常時運用業務として、システム操作（バックアップ管理、情報システムの設定変更、修正プログラム又はアップデートファイルの適用）、運転管理・監視（死活監視、性能監視、稼動状況監視、情報セキュリティ監視）、サービスデスク提供、教育・訓練等を行うこと。
- (2) 定常時保守業務として、軽微なコンテンツ等の更新作業、定期点検、不具合受付等を行うこと。
- (3) 運用・保守作業業務の作業単位ごとに作業内容、回数、工数等の作業実績状況、サービスレベルの達成状況、情報システムの構成と運転状況（情報セキュリティ監視状況を含む。）、情報システムの定期点検状況、情報システムの利用者サポート、教育・訓練状況、リスク・課題の把握・対応状況について、月単位で運用・保守作業報告書を作成し、月次で官側に報告すること。
達成状況が目標に満たない場合はその要因の分析を行うとともに、達成状況の改善に向けた対応策を提案すること。

(4) 請負者は、以下に掲げる事項について提出すること。

① 契約金額内訳

デジタル・ガバメント推進標準ガイドライン「別紙2 情報システムの経費区分」に基づき区分等した契約金額の内訳が記載されたエクセルの電子データを契約締結後速やかに提出すること。

② 情報資産管理標準シート

デジタル・ガバメント推進標準ガイドライン「情報資産管理標準シート」を、官側が定める時期に提出すること。

5.4 引継ぎ

- (1) 請負者は、次年度以降の本WEBサイトの適切な運営のため、アクセスユーザのログ解析等により適切な管理方法や課題等を取りまとめるとともに、サーバ移行等における引継ぎ作業及び次年度のサーバの借用及び運用・保守について、所要の対応、協力を行うこと。
- (2) 請負者は、契約期間の終了までに、引継書（本WEBサイトの運用・保守に必要となる各種ドキュメント等）を作成、整備し、官側の承認を得ること。

5.5 打合せ・協議

- (1) 請負者は、官側と初回打合せを行い、スケジュール感を含め業務全般について認識に問題がないか確認を行うこと。
- (2) 初回の打ち合わせ以後、週に一回の打合せを実施することを基準とする。
- (3) 打合せに関しては、リモート会議・対面のうち速やかに行える方式をその都度選択し、遅滞のないよう行うものとする。
- (4) 打合せに必要な資料は電子媒体にて打合せの前に提供し、求めに応じて紙面にて必要部数を提供すること。
- (5) 打合せ実施後、4開庁日以内に議事録を作成し、官側に提出の上承認を得ること。

6 本業務実施に係る留意事項

6.1 WEBサイトコンテンツの作成等における前提条件

- (1) 専門知識・技術を極力必要としないファイル、スクリプト構成であること。
- (2) 職員によるウェブページの更新作業は、サポートされているOS以上で対応できるものであること。
- (3) 常時SSL対応が可能な記述であること。
- (4) 自ドメイン以外のファイルを読み込まない設定であること。
- (5) 納品前にコンテンツ（ソースコード）に、セキュリティ面での脆弱性がないことを確認すること。
- (6) WEBアクセシビリティにも配慮しつつ、サイト制作を行うこと。

- (7) 滞在時間、直帰率、離脱率等の指標によるWebサイト分析ができる仕組みを設けること。ただし、個人を識別する形での行動追跡を行わないこと。
- (8) 主たるSNS（LINE、ツイッター、Facebook）との連携機能を含めること。ただし、LINEについては「政府機関・地方公共団体等における業務でのLINE利用状況調査を踏まえた今後のLINE サービス等の利用の際の考え方（ガイドライン）（NISC）（令和3年4月30日）」に沿った仕組みを設けること。

6.2 ユーザビリティ要件

請負者は以下のユーザビリティ要件を十分留意すること。なお、利用者の主な年齢は小学生から中学生を想定している。

- (1) 理解性、習得性、機能適合性
 - ・どのような情報が提供されているか、何をすればよいか、そのページの主題と利用目的に対する機能合致度が直感的に理解、習得できる画面構成にすること。
 - ・利用者ニーズを満たす十分なコンテンツ又は機能が用意されており、操作に必要な情報が同一画面内に配置されていること。
 - ・無駄な情報、装飾及び機能を排し、簡潔で分かりやすく、感性的・美的側面も十分に考慮された画面にすること。
 - ・十分な視認性のあるフォント及び文字サイズを用いること。（文字サイズについては、利用者側の環境の設定で拡大等が可能なものとする。）
 - ・利用者がスマートフォンやタブレットなど多様な端末でアクセスした際に、画面サイズに応じ最適化されたレイアウトで表示すること。
- (2) 効率性、最適性（操作のしやすさ、分かりやすさ）
 - ・無駄な手順（ひとつのまとまった作業に複数の画面を行き来しなければならない等）を省き、最小限の操作、入力等で利用者が作業できるようにすること。
 - ・画面上で入出力項目のコピー及び貼り付けができること。
- (3) 指示や状態の分かりやすさ
 - ・操作の指示、説明、メニュー等には、利用者が正確にその内容を理解できる用語を使用すること。
 - ・検索画面等において、必須入力項目と任意入力項目の表示方法を変える等、各項目の重要度を利用者が認識できるようにすること。
 - ・システムが処理を行っている間、その処理内容と処理の実行状況を利用者が直ちに分かるようにすること。
- (4) デザイン・操作感の統一
 - ・トップページを基本として、2段階層以下においても同様の色調等に準拠し、

WEBサイトとして統一感を出すものであること。

- ・初めての訪問者でも容易かつ直感的に操作できるよう、操作性及びデザイン性に配慮すること。
- ・サイト用一式分のソースコード・画像素材等でレスポンス対応できること。
- ・その他、官側との調整に基づき必要な対応を行うこと。

(5) エラーの防止と処理

- ・利用者が操作、入力等を間違えないようなデザインや案内を提供すること。
- ・入力内容の形式に問題がある項目については、それを強調表示する等、利用者がその都度、その該当項目を容易に見つけられるようにすること。
- ・入力内容のフォーマットを統制する必要がある場合（全角、半角、ハイフンの入力など）は、できるだけシステム側で変換を行い、利用者側に正しいフォーマットでの入力を強いないこと。
- ・重要な処理については事前に注意表示を行い、利用者の確認を促すこと。
- ・エラーが発生したときは、利用者が容易に問題を解決できるよう、エラーメッセージ、修正方法等について、分かりやすい情報提供をすること。

(6) ヘルプ

- ・利用者が必要とする際に、ヘルプ情報やマニュアル等を参照できるようにすること。

(7) 言語

- ・日本語に対応すること。ただし、今後さらにマルチ言語化への展開も図る可能性があるため、簡易に拡張できるよう配慮すること。

6.3 アクセシビリティ要件（情報のバリアフリーへの配慮）

請負者は以下のアクセシビリティ要件を十分留意すること。なお、採用するクラウドサービスの機能・特性等により、標準で対応していない場合にはクラウドサービスが提供する機能の範囲内で対応を行う。

- (1) 総務省が推進する「みんなの公共サイト運用ガイドライン（2016年版）」に準拠し、以下を前提とすること。

https://www.soumu.go.jp/main_sosiki/joho_tsusin/b_free/guideline.html

- (2) 特定のブラウザのみで有効な機能、表現及びHTMLの記述は行わないこと。
- (3) スタイルシートを利用しないユーザと利用するユーザにおいて得られる情報に差（表示されない文字や画像がある等）がないこと。レイアウトにおいても大きな差がないことが望ましい。
- (4) 制作するページはプラグインソフトを使用せずに閲覧が可能なこと。
- (5) ウェブアクセシビリティについては、原則としてJIS X 8341-3:2016のレベルAAに準拠していること。本調達仕様書における「準拠」という表記は、情報通信アクセス協議会ウェブアクセシビリティ基盤委員会「ウェブコンテンツの

JIS X 8341-3:2016 対応度表記ガイドライン 2016年3月版」で定められた表記による。範囲は、本WEBサイトとする。

- (6) 利用者の閲覧環境の多様性を鑑み、JavaScriptが無効な状態でもページが表示でき、必要最低限の情報を閲覧可能な機能を有すること。
- (7) 色の違いを識別しにくい利用者（視覚障がいのかた等）を考慮し、利用者への情報伝達や操作指示を促す手段はメッセージを表示する等とし、可能な限り色のみで判断するようなものは用いないこと。

6.4 動作環境

次のOS及びブラウザ等で正常に動作すること。なお、フィーチャーフォンは対象外とする。

- (1) PCでの表示

OS：Windows10以上、macOS 12以上ともにサポートされていること。

- (2) モバイル端末での表示

スマートフォン：iOS 15以上、Android 12以上搭載機

タブレット：iPadOS 15以上、Android 12以上搭載機

- (3) ブラウザ

(Windowsの場合) Microsoft Edge最新版、Google Chrome最新版、Mozilla Firefox最新版

(macOSの場合) Safari最新版、Firefox最新版、Chrome最新版

6.5 WEBサイト稼働環境

6.5.1. サーバ稼働環境

- (1) 利用者がストレスなく操作できる程度のレスポンスを確保すること。また、稼働状況監視を随時実施し、必要な資源増強を行える体制を整えること。
- (2) 対象ごとにバックアップの取得手法や保存先、取得時期等を考慮し、適切なバックアップ処理が可能なものとし、少なくとも日次でバックアップを行うこと。システム障害によりデータ復旧が必要となる場合は、少なくとも前日までの状態に復旧できること。なお、クラウドサービスで提供されるバックアップサービスを活用しても差し支えない。
- (3) 何らかのソフトウェアを利用する場合には、広く市場に流通し、利用実績を十分に有するソフトウェア製品を活用する。その際、アプリケーションプログラムの動作、性能等に支障を来さない範囲において、可能な限りオープンソースソフトウェア（OSS）製品（ソースコードが無償で公開され、改良や再配布を行うことが誰に対しても許可されているソフトウェア製品）の活用を図る。OSS製品を活用する際は、ソフトウェアのバージョン、ソフトウェアベンダによるサポート又は他の事業者によるサポートサービスの利用等を検討し、官側

と協議の上で決定すること。

- (4) (個人情報又はこども家庭庁における要機密情報が取り扱われる場合) 当該クラウドサービスのデータセンター(バックアップセンターを含む。)は国内に限ること。
- (5) クラウドサービスの廃止、サービス内容の変更等に伴い契約を終了する場合は、他のクラウドサービス等に円滑に移行できるよう、十分な期間をもって事前に官側へ通知すること。
- (6) クラウドサービスの契約を終了する場合、クラウドサービス上に保存されたこども家庭庁のデータについて、汎用性のあるデータ形式に変換して提供するとともに、クラウドサービス上において復元できないよう抹消し、その結果を官側に書面で報告すること。
- (7) クラウドサービスに係るアクセスログ等の証跡を保存し、官側からの要求があった場合は提供すること。なお、証跡は1年間以上保存すること。
- (8) インターネット回線とクラウド基盤との接続点の通信を監視すること。
- (9) クラウドサービスに係る業務の一部がクラウドサービス事業者以外の事業者により外部委託されている場合は、当該クラウドサービス事業者以外の事業者により「13. 再委託に関する事項」の措置を講ずること。
- (10) クラウドサービスにおける脆弱性対策の実施内容を官側が確認できること。
- (11) クラウドサービスの可用性を保証するための十分な冗長性、障害時の円滑な切替等の対策が講じられていること。また、クラウドサービスに障害が発生した場合の復旧時点目標(RPO)等の指標を提示すること。
- (12) クラウドサービス上で取り扱う情報について、機密性及び完全性を確保するためのアクセス制御、暗号化及び暗号鍵の保護並びに管理を確実にすること。
- (13) クラウドサービスの利用者が、自らの意思によりクラウドサービス上で取り扱う情報を確実に抹消できること。
- (14) 本業務において、クラウドサービスに係る情報について、業務開始時に開示項目や範囲を明記した資料を提出すること。
- (15) こども家庭庁に対して、クラウドサービスに係る機密性の高い情報を開示する場合は、こども家庭庁において、当該情報を審査又は本業務以外の目的で利用しないよう適切に取り扱うため、必要に応じて当該情報に取扱制限を明記するなどの措置を講ずること。
- (16) 請負者とクラウドサービス事業者との間のサービス契約を、請負者以外の者に引き継ぐことができること。

6.5.2 データベース機能

- (1) 要件に応じてデータベースサービスを用意すること。オブジェクトストレージサービス等による代替も許可する。

- (2) 確認用データベースサーバを用意し、事前に動作確認後、公開データベースサーバで公開できること。確認用データベースサーバはアクセスユーザやスキーマ単位等に、認証等により利用制限できること。確認用データベースサーバは公開データベースサーバと同様のソフトウェアを実装すること。
- (3) データベースの導入・運用における情報セキュリティの確保として、以下を含む情報セキュリティ対策を実施すること
 - ・管理者アカウントの適正な権限管理を行うこと。
 - ・データベー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こと。
 - ・データベースに格納されている一定数以上のデータの取得に関するログを記録し、警告を発すること。
 - ・データベースへのインジェクション攻撃対策のため、ウェブアプリケーションファイアウォールやデータベースファイアウォールの導入など、必要な対策を講ずること。
 - ・データベースサーバへのコンテンツの更新の際は、専用の端末を使用して行うこと。
 - ・データベースサーバへのコンテンツの更新の際は、データベース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し暗号化通信により行うこと。
 - ・データベースサーバへの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こと。

6.6 規模及び性能

- (1) 本システムについては、利用者数は利用の拡大とともに増加することが見込まれる。運用時にはアクセス数の推移等を定期的に分析し、将来的な利用者数を見積もること。
- (2) 本システムについては、ネットワーク環境を含む利用者の条件が多種多様であり、取り扱う情報・データも定型的なものとはならないことが想定されるため、性能要件について一律の定量的な指標を設定することは必ずしも適当ではないが、以下、一定の目安を記載する。リリース前及び性能に影響を及ぼす可能性のある大規模な改修を実施した際は、性能試験を実施し応答時間とスループットを測定すること。
 - ・ 応答時間（ただし、サーバ処理時間。応答時間達成率は95%以上）
 - コンテンツ閲覧 平常時2 秒以内／ピーク時3 秒以内
 - コンテンツ検索 平常時3 秒以内／ピーク時5 秒以内
 - ・ スループット
 - コンテンツ閲覧 100 件/分
 - コンテンツ検索 20 件/分

6.7 信頼性に関する要件

6.7.1 可用性要件

下記の目標値を参考とし、実現可能な可用性に係る目標値を設定する。ただし、管轄外となるネットワーク等に障害の原因がある場合や、システムの計画停止等の期間が必要になることが予め判明している場合は除く。

- ・ 可用性に係る目標値（目安）

稼働率（実稼働時間÷予定稼働時間※）99.9%以上

※ 予定稼働時間：24 時間365 日

※ 計画停止等の期間を除く。

6.7.2 完全性要件

本システムにて管理されるコンテンツ等は、データが喪失されることのないようにバックアップ等の必要な作業を実施すること。

これらの情報・データに関しては、採用するクラウドサービスによって保管・管理のポリシーが異なるため、クラウドサービスのSLA に照らして、完全性の観点でどのような対策がクラウドサービス側で標準的に実施可能か検討すること。

6.8 個人情報の取扱に関する要件

個人情報の取得は行わないこと。

6.9 その他

- (1) 本番用、確認用、開発用の機器・ソフトウェア等は請負者で用意すること。
また、電子証明書及びドメインの申請、管理・保守に必要となる費用及び作業については請負者にて負担を行うこと。
- (2) システムで使用する機器やソフトウェア（ミドルウェア、ライブラリ）等を調達する際は、不正侵入の経路となるバックドアや脆弱性が含まれていないことを確認し、システム稼働中にメーカーサポートを受けられる安全なプロダクトを選定すること。

7 納入成果物等

7.1 納入成果物

- (1) 請負者は、「表 1 納入成果物一覧」に示す書類等について納入成果物として納入すること。

なお、一次オープンに伴う成果物については、「表 1 納入成果物一覧」に示す提出期限に限らず、官側と協議の上、一次オープンまでに提出すること。

また、これらの納入成果物は一般的な納入成果物の体系を示すものであることから、本業務の履行に当たり、納入成果物に追加又は不要とするべき内容がある場合には、契約締結後において、官側と協議の上、納入成果物を確定させること。

表 1 納入成果物一覧

成果物名	記載内容	提出期限
作業実施計画書（案）	作業概要、作業体制、スケジュール、成果物等について記載したもの	契約締結後1週間
作業実施要領（案）	コミュニケーション管理、体制管理、作業管理、品質管理、リスク管理、課題管理、情報セキュリティ対策等について記載したもの	契約締結後1週間
機器・ソフトウェア等一覧	提供される機器・ソフトウェア等の一覧	令和6年3月31日
ウェブコンテンツ一式	HTML、CSS、画像等ソースコードを含むウェブコンテンツ全て	令和6年3月31日
各種設定情報	IaCや使用ツールの設定情報など、環境構築を再現できる各種設定情報	令和6年3月31日
WEBサイト更新マニュアル	資料や動画の更新、新規ページ作成等を行う手順を示したもの	令和6年3月31日
利用規約※	サイト利用者向けの規約（コンテンツの利用使用条件等）をこども向けに表現を平易にしたうえでサイトにも掲載すること。）	令和6年3月31日
引継書	デジタル・ガバメント推進標準ガイドライン解説書「第3編 第7章 設計・開発」の引継ぎに示されているもの	令和6年3月31日

※ こども家庭庁WEBサイトのプライバシーポリシー (<https://www.cfa.go.jp/privacy-policy/>) とコピーライトポリシー (<https://www.cfa.go.jp/copyright-policy/>) に準拠すること。

(2) 成果物については、以下に従って作成するものとする。

- ・成果物は、全て日本語で作成すること。ただし、日本国内においても英字で表記されることが一般的な文言については、そのまま記載しても構わないものとする。
- ・用字・用語・記述符号の表記については、「公用文作成の考え方（令和4年1月7日文化審議会建議）」を参考にすること。
- ・情報処理に関する用語の表記については、日本産業規格（JIS）の規定を参考にすること。

7.2 納入方法

納入成果物は、日本産業規格A列4番で作成の上、書面により正1部・副1部提出するほか、同内容を記録した電子記録（提出方法は別途提示する）により納入すること。

様式、記載内容及び納入期限の詳細については、事前に官側と協議し、承認を受けた上で決定すること。また、各納入成果物は、それぞれ作成完了時に官側に

よって承認されたものとする。

なお、電子記録の納入については、以下のとおりとすること。

- (1) 納入のファイル形式は、「Microsoft Word 2016」、「Microsoft Excel 2016」、「Microsoft Power Point 2016」等で参照・編集可能な形式とする。
- (2) 電子記録の納入に当たっては、事前に最新のウィルス定義ファイルによる検疫を必ず実施すること。
- (3) 納入成果物は納入後、改変が可能となるよう、図表等の元データも併せて納入すること。
- (4) 特別なツールの使用を必要とする場合は、事前に官側の承認を得た上で、ツールとともに納入すること。

7.3 納入場所、納入条件、検収

納入場所は、こども家庭庁とする。また、請負者は、本業務の納入成果物の納入に際して、以下の条件を満たすこと。

- (1) 上記「表 1 納入成果物一覧」に示す各納入時期までに納入すること。
- (2) 納入成果物の納入に係る請負者の作業及び関係書類等の作成等に関する費用は、一切を本業務の範囲に含めること。
- (3) 納入に当たっては、本調達仕様書に示された要件を十分に満足させるとともに、その品質が十分であることを説明できること。
- (4) 各納入成果物については、事前に官側のレビューを受け、請負者と官側の間に認識の齟齬が生じないようにすること。
- (5) 成果物等について、納品期日までに官側に内容の説明を実施して検収を受けること。
- (6) 検収の結果、成果物等に不備又は誤り等が見つかった場合には、直ちに必要な修正、改修、交換等を行い、変更点について官側に説明を行った上で、指定された日時までに再度納品すること。

8 作業の実施体制・方法

8.1 作業実施体制

- (1) 請負者は、本業務を確実に実施するために必要な知識、経験等を有するウェブ関連技術等を確保し、本業務を遅滞なくかつウェブシステムに支障をきたすことなく履行できる体制を確立していること。
- (2) 情報セキュリティの管理体制について、以下のとおり行うこと。
 - ① 情報システムの開発環境、本番環境、検証環境を分離し、各環境で取扱う情報の機微性等に応じてアクセス制御等必要なセキュリティ対策を実施すること。

- ② 情報システムの設計、構築、運用、保守工程において、官側の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。
- ③ 官側の意図しない変更や機密情報の窃取等が行われないことを保証するための具体的な管理手順や品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を官側との協議の上、必要と判断された場合は提出すること。また、第三者機関による品質保証体制を証明する書類等が提出可能な場合は、提出すること。
- ④ 情報システムに官側の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入検査等、官側と連携して原因を調査し、排除するための手順及び体制（例えば、運用・保守業務におけるシステムの操作ログや作業履歴等を記録し、発注元から要求された場合には提出させるようにするなど）を整備していること。また、当該手順及び体制が妥当であることを証明するための書類を官側との協議の上、必要と判断された場合は提出すること。
- ⑤ 情報システムの開発・構築等の各工程において、情報セキュリティに係るサプライチェーン・リスクを低減する対策が行われていること。
- ⑥ セキュリティ関連のテストの実施結果が確認できること。脆弱性検査については、「デジタル庁 政府情報システムにおける脆弱性診断ガイドライン」の実施基準を満たすように脆弱性診断実施事業者の選定、脆弱性診断の実施、検出された脆弱性への対応を行うこと。
- ⑦ 政府情報システムにおいて含有されやすいセキュリティ上の問題点（下記表）についてもれなく対応すること。

認証管理不備	共用アカウントが使用される際に、利用者特定の仕組みや取扱いに関するルールが整備されていない。 推測されやすい脆弱なパスワードが使用されている。 認証情報がファイル等に平文で書かれている。
アクセス制御不備	必要な強度の認証が行われていない。 ネットワーク、システムへのアクセス制限が実施されていない。 アクセス権が必要最小限のアクセス権付与が守られておらず、過剰である。
暗号化不備	重要情報が流れる各機器間の通信経路で必要な暗号化が実施されていない。
資産管理、脆弱性管理不備	利用しているソフトウェアや機器の状態を把握していない（最新状態を維持できていない）

	OS やミドルウェア、ファームウェア等の脆弱性対策が適切に実施されていない。
Web アプリケーションの脆弱性	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初歩的な web アプリケーションの脆弱性が存在している。 パラメータ改ざんにより、本来アクセス権できないデータを操作できるなどの脆弱性が存在している。
ログ管理不備	ログ取得の範囲が目的に応じて定められていない（必要なログが取得されていない） 定期的なログの点検又は分析が実施されていない。
外部委託の管理不備	外部委託に係る契約に、遵守事項で定める委託先の情報セキュリティ対策が含まれていない。 外部委託に係る契約に基づき、委託先における情報セキュリティ対策の履行状況を確認していない。

- (3) 再委託先における情報セキュリティの確保については受注者の責任とし、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、当該調達仕様書のセキュリティ対策にかかる措置の実施を再委託先に担保させること、また再委託先のセキュリティの対策実施状況を確認できるよう、契約に含めること（再々委託先等の取扱いも同様）。

8.2 作業要員に求める資格等の要件

請負者は、本業務を確実に実施するため、以下の人員を配置すること。また、以下は別の者で構成すること。なお、作業開始後、本業務の遂行能力に疑義が生じた場合、官側と請負者の事前協議を踏まえ、作業要員の変更に応じること。

(1) 作業責任者

本業務を確実に実施するため、WEBサイトの構築及び運用に係る専門的な知識を有し、リニューアル業務を行った実績を有すると共に、その責任者の経験を有すること。

(2) 作業担当者

本業務を確実に実施するため、最新のHTMLコーディング技術及びアクセシビリティ対応等の専門的な知識や実績、資格等を有すること。

8.3 作業場所

本業務の作業場所及び作業に当たり必要となる設備、備品及び消耗品等については、請負者の責任において用意すること。また、必要に応じて官側が現地確認を実施することができるものとする。

8.4 作業の管理に関する要領

請負者は、官側が承認した作業実施計画書及び作業実施要領に従い、コミュニケーション管理、体制管理、作業管理、品質管理、リスク管理、課題管理、情報

セキュリティ対策を行うこと。

9 作業の実施に当たっての遵守事項

9.1 機密保持、資料の扱い

- (1) 本業務に関する作業において取り扱う、官側が交付又は使用を許可した全ての情報（電子データ、印刷された情報等を含む。）を「本業務に関する作業における取扱情報」（以下「取扱情報」という。）とする。
- (2) 請負者は、取扱情報を業務の一部を委託した者を除き第三者に開示又は漏えいしてはならない。請負者の責任に起因する情報漏えい等により、損害が発生した場合は、それに伴う弁済等の措置は全て請負者が負担すること。
- (3) 本業務を実施するに当たって、別紙「個人情報取扱特記事項」に基づき、業務上知り得た情報の開示、漏えい、又は本業務以外の用途に使用しないこと。また、そのために必要な措置を講ずること。関係者等に対しメールによる連絡をする場合にあっては、他の受信者のメールアドレスが閲覧できないようBCC機能により送信するなど、個人情報等（他の受信者の個人情報以外の情報を含む。）の流出防止に万全を期すこと。
- (4) この項目について、請負者は契約期間の終了後においても同様とする。なお、請負者は契約期間の終了後、速やかに保有した取扱情報について削除すること。

9.2 情報セキュリティインシデントへの対処

- (1) 請負者が情報セキュリティインシデントを認知した場合には、官側にて定める対処手順又はこども家庭庁CSIRTの指示若しくは勧告に従って、適切に対処すること。
- (2) 請負者は、こども家庭庁CSIRTから応急措置の実施及び復旧に係る指示又は勧告を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それを報告書として取りまとめ、官側に報告すること。

9.3 情報セキュリティに係る資料の提出

- (1) 応札等を希望する請負者は、本業務及び情報セキュリティ管理の履行可能性を証明するため、本業務で取扱う情報等の特性を十分に踏まえ、以下の書類を提出すること。なお、提出された書類において履行可能性を認めることができないと官側が判断した場合は、入札に参加することができない。
 - ・ WBS手法を用いて、作業工程ごとに必要なタスクを分類・定義し、タスクごとに必要となる作業量を記載するとともに、それを実現するためのスケジュール及び体制等を含む作業実施計画書
 - ・ 「情報セキュリティ管理」に基づいた情報セキュリティ管理計画書

- (2) 「情報セキュリティ管理」は以下のとおりとし、応札を希望する請負者は、以下を含む情報セキュリティ対策を実施すること。
- ① 官側から提供する情報の目的外利用を禁止すること。
 - ② 本業務の実施に当たり、応札を希望する請負者又はその従業員、本業務の役務の内容の一部を再委託する先、若しくはその他の者による意図せざる不正な変更が情報システムのハードウェアやソフトウェア等に加えられないための管理体制が整備されていること。
 - ③ 応札を希望する請負者の資本関係・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。
 - ④ 情報セキュリティインシデントへの対処方法が確立されていること。
 - ⑤ 情報セキュリティ対策その他の契約の履行状況を定期的に確認し、官側へ報告すること。
 - ⑥ 情報セキュリティに関して適切な措置が講じられていることを確認するため、履行状況の定期的な報告および必要に応じて官側による実地調査が実施できること。また、履行状況が不十分である場合は、官側と協議の上、改善策を実施すること。
 - ⑦ 官側が求めた場合に、速やかに情報セキュリティ監査を受入れること。
 - ⑧ 本業務において、要安定情報を取り扱うなど、官側が可用性を確保する必要があると認めた場合は、サービスレベルの保証を行うこと。
 - ⑨ 本調達の役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるように情報セキュリティ管理計画書に記載された措置の実施を担保すること。
 - ⑩ 官側から要保護情報を受領する場合は、情報セキュリティに配慮した受領方法にて行うこと。
 - ⑪ 官側から受領した要保護情報が不要になった場合は、官側の指示に従い、これを確実に返却、又は抹消し、書面にて報告すること。
 - ⑫ 本業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は速やかに官側に報告すること。

10 知的財産権等

- (1) 本業務で制作される一切の成果物について、著作権法第27条及び28条に定める権利を含む全ての著作権は、官側に譲渡し、官側が独占的に使用するものとする。
- (2) 請負者は、本業務において発生する全ての著作者人格権を行使せず、また、第三者をして行使しないものとする。

- (3) 納入された成果物に関する権利は全て官側に属し、政府が行う広報活動等に任意に利用できるものとする。
- (4) 成果物に第三者の権利を有する著作物が含まれている場合、官側が特に使用を指示した場合を除き、請負者は当該著作物使用に際して、一切の使用許諾条件等につき、事前に了承を得ることとし、官側は既存の著作物について当該許諾条件の範囲内で使用するものとする。
- (5) 本件仕様書に基づく業務に関して、第三者との間で著作物に関わる権利侵害の紛争等が生じた場合、当該紛争等の原因が専ら官側の責に寄与する場合を除き、請負者は自らの責任と負担について一切の処理を行うこととする。

11 契約不適合責任

- (1) 官側は、請負者に対し、成果物が本契約の内容に適合しないものであるとき（ただし、官側が本契約の内容に適合しないことを本契約締結前に認識している場合を除く。）は、成果物の補修による履行の追完を請求することができる。ただし、請負者は、官側に不相当な負担を課するものでないときは、官側が請求した方法と異なる方法による履行の追完をすることができる。
- (2) (1)の場合において、官側が、相当の期間を定めて履行の追完を催告し、その期限内に履行の追完がないときは、官側はその不適合の程度に応じて代金の減額を請求することができる。
- (3) (1)の場合において、本契約の不適合により損害を被ったときは、官側は、損害賠償の請求又は本契約の解除をすることができる。
- (4) (1)から(3)の請求に当たっては、請負者が本契約に不適合な成果物を引渡した場合において、官側がその不適合を知ったときから1年以内に、請負者に対して不適合の内容を通知するものとする。

12 請負資格に関する事項

12.1 公的な資格や認証等の取得

- (1) 請負者は、品質マネジメントシステムの規格である「JIS Q 9001」又は「ISO9001」（登録活動範囲が情報処理に関するものであること。）の認定を有している、若しくは同等の品質管理手順及び体制が明確化された品質マネジメントシステムを有している事業者であること（管理体制、品質マネジメントシステム運営規程、品質管理手順規定等を提示すること。）。
- (2) 一般財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制度の認定を受けているか、又は同等の個人情報保護のマネジメントシステムを確立していること。

12.2 受注実績

請負者は、本業務を確実に実施するため、WEBサイトの構築又は運用に係る専門的な知識を有し、過去5年以内において、WEBサイト又は同等のシステムのリニューアル又は構築業務を行った実績を有すること。

12.3 履行体制の証明

請負者は、以下の(1)～(7)に示す条件を満たしていることを証明できる書類(様式任意)を提出すること。

- (1) 8.2 (1) に関する実績の証明
- (2) 8.2 (2) に関する実績、資格等の証明
- (3) 9.3 (1) に示す作業実施計画書(案)
- (4) 9.3 (1) に示す情報セキュリティ管理計画書
- (5) 12.1 (1) に関する証明
- (6) 12.1 (2) に関する証明
- (7) 12.2 に関する実績の証明

12.4 入札参加要件

本調達入札をする場合は、別添に示す「調達概要書」を参照し、必要な書類等を期限までに提出すること。

13 再委託に関する事項

13.1 再委託の制限及び再委託を認める場合の条件

- (1) 請負者は、業務を一括して又は主たる部分を再委託してはならない。
- (2) 請負者における遂行責任者を再委託先事業者の社員や契約社員とすることはできない。
- (3) 請負者は再委託先の行為について一切の責任を負うものとする。
- (4) 再委託先における情報セキュリティの確保については請負者の責任とする。

13.2 承認手続

- (1) 本業務の実施の一部を合理的な理由及び必要性により再委託する場合には、あらかじめ再委託の相手方の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性及び契約金額等について記載した別添の再委託承認申請書を官側に提出し、あらかじめ承認を受けること。
- (2) 前項による再委託の相手方の変更等を行う必要が生じた場合も、前項と同様に再委託に関する書面を官側に提出し、承認を受けること。
- (3) 再委託の相手方が更に委託を行うなど複数の段階で再委託が行われる場合(以下「再々委託」という。)には、当該再々委託の相手方の商号又は名称及び住所並びに再々委託を行う業務の範囲を書面で報告すること。

13.3 再委託先の契約違反等

- (1) 再委託先において、本調達仕様書の遵守事項に定める事項に関する義務違反

又は義務を怠った場合には、請負者が一切の責任を負うとともに、官側は、当該再委託先への再委託の中止を請求することができる。

14 スケジュール

- ・業務開始：令和5年7月中旬
- ・設計構築、システム構築：令和5年7月から10月
- ・一次オープン：令和5年11月1日（予定）
- ・初期運用：令和5年11月1日から令和6年3月31日
- ・契約終了：令和6年3月31日

15 その他

- (1) 請負者が官側へ提出する資料は、日本語によるものであること。
- (2) 請負者は、本業務に関する質問に対して、常時回答が可能なようにすること。
- (3) 請負者は、本調達仕様書の内容又は解釈について疑義が生じた場合、その旨を書面にて提出し、官側の指示に従うこと。
- (4) その他特に協議の必要があると認められる場合は、請負者の申し出により官側と協議を行うこと。
- (5) 本業務の履行に当たっては、障害を理由とする差別の解消の推進に関する法律（平成25年法律第65号）第9条第1項に基づく「こども家庭庁における障害を理由とする差別の解消の推進に関する対応要領」（仮称）に規定する合理的配慮について留意すること。

【別紙】

個人情報取扱特記事項

(個人情報保護の基本原則)

- 1 請負者は、個人情報（個人情報の保護に関する法律（平成十五年法律第五十七号）第2条に規定するものをいう。以下同じ。）の保護の重要性を認識し、この契約に基づく業務を実施するに当たり、個人の権利利益を侵害することのないよう、個人情報を適正に取り扱わなければならない。

(体制の整備)

- 2 請負者は、この契約に基づく業務に関して取り扱う個人情報を適切に監理するため、個人情報取扱責任者の設置を含む管理体制を整備しなければならない。

(秘密の保持)

- 3 請負者は、この契約に基づく業務に関して知り得た個人情報をみだりに他人に知らせ、又は契約の目的以外の目的に使用してはならない。
この契約が終了し、又は解除された後においても同様とする。

(業務従事者への周知)

- 4 請負者は、直接的であるか間接的であるかを問わず、請負者の指揮監督を受けてこの契約による業務に従事している者（以下「業務従事者」という。）に対して、在職中及び退職後においてもこの契約に基づく業務に関して知り得た個人情報をみだりに他人に知らせ、又は契約の目的以外の目的に使用してはならないことなど、個人情報の保護の徹底について周知しなければならない。

(適正な安全管理)

- 5 請負者は、この契約に基づく業務に係る個人情報の漏えい、滅失、改ざん、又は損傷の防止その他の個人情報の適切な安全管理のために必要な措置を講じなければならない。また個人情報の漏えい等による被害発生リスクを低減する観点から、利用目的、業務の内容、個人情報の秘匿性等その内容などを考慮し、必要に応じ、氏名を番号に置き換える等の匿名化措置を行わなければならない。

(再委託の制限等)

- 6 請負者は、発注者が承認した場合を除き、個人情報の取り扱い業務を再委託してはならない。また、再委託する場合にあっては、請負者は、再委託先（再委託先が委託先の子会社（会社法（平成17年法律第86号）第2条第1項第3号に規定する子会社をいう。）である場合も含む。）への必要かつ適切な監督を行わなければならない。

(収集の制限)

- 7 請負者は、この契約に基づく業務に係る個人情報を収集するときは、当該業務の目的を達成するために必要な範囲で、適法かつ公正な手段により行わなければならない。

(利用及び提供の制限)

- 8 請負者は、発注者の指示又は承諾がある場合を除き、この契約に基づく業務に関して知り得た個人情報を当該契約の目的以外の目的のために利用し、又は第三者に提供してはならない。

(複写、複製の禁止)

- 9 請負者は、発注者の指示又は承諾がある場合を除き、この契約に基づく業務に関して知り得た個人情報を複写し、又は複製してはならない。

(安全管理の確認)

- 10 発注者は、請負者が取り扱う個人情報の安全管理措置が適切に行われていることを適宜確認することとする。また、発注者は必要と認めたとき、請負者に対し個人情報の取り扱い状況について報告若しくは資料の提出を求め、又は請負者が個人情報を取り扱う場所で、当該取扱状況を検査することができる。

発注者は、委託する業務に係る個人情報の秘匿性等その内容やその量等に応じ、請負者における管理体制及び実施体制や個人情報の管理の状況について、少なくとも年1回以上、原則として実地検査により確認するものとする。

(業務従事者の監督)

- 11 請負者は、業務従事者に対し、個人情報に関する秘密保持義務を負わせるとともに、その目的外利用を禁止するものとする。

請負者は、本件業務の遂行上、実際に個人情報を取り扱う業務従事者の範囲を限定するものとし、当該業務従事者に対して必要かつ適切な監督を行わなければならない。

請負者は、業務従事者が退職する場合、当該業務従事者に対し、退職後の秘密保持義務に関する誓約書の提出を求めるなど、在任若しくは在職中に知り得た全ての個人情報の返還又は破棄を義務づけるために合理的に必要と認められる措置を講ずるものとする。

(改善の指示)

12 発注者は、報告、資料の提出又は実地検査の結果、請負者において個人情報の安全管理措置が十分に講じられていないと認めるときは、請負者に対し、その理由を書面により通知かつ説明した上で、安全管理措置の改善を要請することができるものとする。

請負者は、前項の要請を受けたときは、安全管理措置の改善について発注者と協議を行わなければならない。

(廃棄等)

13 請負者は、この契約に基づく業務に関して知り得た個人情報について、発注者から指示があったとき又は保有する必要がなくなったときは、確実かつ速やかに発注者への返却、廃棄又は消去（以下「廃棄等」という。）しなければならない。なお、請負者がこの契約に基づく業務に関して知り得た個人情報の廃棄等を行った場合には、発注者に対して、速やかにその旨を書面で報告するものとする。

(事故発生時における報告)

14 請負者は、この契約に基づく個人情報に関する事項に違反する事態が生じ、又はおそれがある場合は、直ちに発注者へ報告し、発注者の指示に従うものとする。この契約が終了し、又は解除された後においても同様とする。

(違反した場合の措置)

15 発注者は、請負者が記載事項に違反した場合は、契約を解除することができるとともに必要な措置を求めることができる。