

「茨城県よろず支援拠点」ホームページ制作及び運用管理等業務委託仕様書

1 目的

公益財団法人いばらき中小企業グローバル推進機構（以下「機構」という。）が実施する茨城県よろず支援拠点（以下「拠点」という。）事業において、県内の中小企業・小規模事業者等や支援機関に対して拠点の機能を広く知ってもらうためのホームページの制作及び保守管理を目的とする。

2 業務期間

契約締結日から令和8年3月31日まで
(ホームページの公開予定日は令和7年10月1日を目標とする。)

3 業務の内容

機構から委託を受けた者（以下「受託者」という。）は県内の中小企業・小規模事業者等や支援機関に拠点の機能を広く知ってもらうためのホームページの制作及び保守管理を行うこととする。

なお、コンテンツの制作においては「デジタル庁 ウェブアクセシビリティ導入ガイドブック（2024年12月改訂）」に準拠するものとする。

(1) ホームページの制作

- ア ホームページは、新たに「go.jp」ドメインを取得する必要があるため、その取得・運用費用（1年分）を制作費用に含めること。
- イ PC、スマートフォン等向けのデザインを作成すること。
- ウ 以下のページを作成すること。
 - ・拠点の紹介
 - ・コーディネーターの紹介
 - ・セミナー・勉強会の案内
 - ・相談会の案内
 - ・活用事例の紹介
 - ・アクセス
 - ・資料一覧（関連資料がダウンロードが可能な形式とする。）
 - ・ご相談・お問い合わせ
 - ・お知らせ
- エ PC、スマートフォン等の閲覧に対応させること。PC、スマートフォン等の共通のページは同じURLで作成すること。
- オ 検索エンジンでの基本的な検索性（SEO）に配慮した設計とし、必要なメタ情報や構造化の工夫を施すこと。
- カ 「拠点の紹介」ページは、業務内容等を掲載すること。
- キ 「コーディネーターの紹介」ページは、在籍コーディネーターの増減に伴う更新が必要であるため、機構職員が更新できるように実装すること。
- ク 「セミナー・勉強会の案内」ページは、機構職員が登録・編集・削除を行えるデータベース形式とし、次の仕様を満たすこと。
 - ・必要項目を含む管理機能を実装
 - ・セミナー・勉強会一覧ページにはカレンダーを設置し、登録内容が自動でカレンダーに反映
 - ・月ごとの一覧表示が可能
- ケ 「セミナー・勉強会の案内」ページにはユーザーによる申し込み機能を実装し、以下に対応すること。
 - ・1企業で複数名の申込みが可能な一括入力機能の搭載
 - ・申込情報のCSV出力機能の実装
- コ 「相談会の案内」ページには、拠点への相談申し込み機能を実装し、申し込み情報はCSV形式で出力できるようにすること。また、相談会の日程については年に1回程度の更新が発生するため、機構職員が内容を更新できるように実装すること。
- サ 「活用事例の紹介」ページは、既存パンフレットに基づいた情報掲載とし、更新頻度が少ないため、機構職員による更新機能は不要とすること。
- シ 「ご相談・お問い合わせ」ページは、フォーム入力により個人情報を取得し、その情報をCSV

形式で出力可能とすること。

- ス CSV データのダウンロード機能は機構職員のみが操作できるよう、IP 制限やパスワード設定等のセキュリティ対策を講じること。
- セ CMS へのログインには、IP 制限を設けること。
- ソ 操作マニュアルは、機構職員が更新・操作を行う機能（コーディネーター紹介、セミナー・勉強会、相談会に対する更新）を中心に構成し、対象機能や操作対象範囲を明確に示すこと。

(2) ホスティング（サーバ・システム）

- ア WEB サーバー及び各種システムは、セキュリティ面に十分配慮したレンタルサーバ及びシステムとする。別記「情報セキュリティポリシーに関するガイドライン」に従うこと。
- イ 脆弱性診断により安全性が担保されていること。
- ウ ISMAP への登録がされているクラウドサービスであることが望ましいが、これに準ずる安全性が担保されたクラウドサービスでも可とすること。
- エ サイト内全ページにおいて SSL 証明書による通信の暗号化を実施すること。また、導入する SSL については日本政府や地方公共団体での採用実績のある、有料の SSL 証明書を実装すること。
- オ サーバーの性能要件の目安は以下のとおり。ただし、サーバーの設定は柔軟に変更できるとし、また変更する場合は機構と別途協議すること。
 - (ア) CPU 2 コア以上
 - (イ) メモリ 8 GB 以上
 - (ウ) ディスクのサイズ 300 GB 以上
 - (エ) サービスレベル 稼働率 99.95% 以上

(3) CMS

- ア WEB サーバー及び各種システムは、セキュリティ面に十分配慮したレンタルサーバ及びシステムとする。別記「情報セキュリティポリシーに関するガイドライン」に従うこと。
- イ 安全性が担保されていること。
 - ・適切なセキュリティ対策がされていること。
 - ・脆弱性診断により安全性が担保されていること。
 - ・ISMAP への登録がされているクラウドサービスであるとより適切である。
- ウ 拠点にある事務用パソコンで更新が行えること。また、端末に新たなソフトウェアのインストールを要しないこと。

(4) ホームページの運用保守業務

- ア サーバー・システム・コンテンツの保守、維持管理を行うこと。また、障害発生時の緊急連絡体制を確保すること。
- イ 必要に応じて電話や訪問でのサポート対応を行うこと。
- ウ コンピューターウィルス等による感染への対策等、セキュリティの保護に関する十分な対策をとること。また、不正アクセス、クラッキング等ハッキングについても対処すること。
- エ アクセス解析を設け、機構及び拠点の指示により、必要に応じてデータを提供すること。
- オ 定期的にバックアップを行うこと。

(5) コンテンツ保守業務

- ア ホームページの軽微なデザイン修正に対応すること。
- イ デザインの大きな変更を伴わないページの更新については、機構職員自身が行えるよう必要なサポートを行うとともに、安全性を十分に確保すること。
- ウ 著作権等に関して次の事項に留意すること。
 - (ア) 他人の著作権の侵害、名誉毀損などの問題が生じないようにすること。
 - (イ) 公表されている著作物を引用する際には、必ず出典を明示すること。
 - (ウ) ホームページ制作に使用した文章・画像・音声その他一切の著作権は機構及び拠点に帰属するものとし、著作者人格権は行使しないこと。
 - (エ) 作成したコンテンツ及びファイル等は、契約終了後返却すること。

4 事業実施上の留意点

(1) 基本方針

- ア 閲覧者の視点で見やすく、使いやすいホームページであること。
- イ 閲覧者に理解されるよう、デザイン、表現等に工夫を凝らし分かりやすい内容とし、目的の情報の探しやすさを考慮すること。
- ウ 各ページは同一 URL でパソコン・スマートフォン等の各種端末に最適化した表示がされるように作成すること。スマートフォン端末では、画面サイズに合わせて最適化し、見やすく、タッチ操作しやすい構成とすること。
- エ 外部からの攻撃や、データの漏えいなどのセキュリティリスクにも対応した安全なホームページであること。
- オ 情報セキュリティに関する体制として、プライバシーマーク及び ISMS（情報セキュリティマネジメントシステム）認証を取得していることが望ましい。また、RISS（情報処理安全確保支援士）等の有資格者が関与している場合は、セキュリティ面での信頼性が高いことから、プロポーザルの評価の加点項目とする。
- カ 国や県の行政のホームページ制作の実績を有していること、また、日本政府の情報システムに係るセキュリティ評価制度「ISMAP（イスマップ）」を理解していることが望ましい。記載の実績や理解が図れている場合はプロポーザルの評価の加点項目とする。

（２）ホームページ閲覧予定者

ホームページの主な閲覧者は、県内の中小企業・小規模事業者・個人事業主、支援機関（商工会・商工会議所・金融機関・認定支援機関、自治体等）の担当者とする。

5 成果品（ホームページ）の提出

成果品（ホームページ）のファイル等を収納した媒体（CD-ROM、DVD-ROM 等） 1 部

成果品（ホームページ）操作マニュアル 1 部

6 ホームページの納品期限・公開予定日

ホームページの納品期限は令和 7 年 9 月 3 0 日とし、公開予定日は令和 7 年 1 0 月 1 日を目標とする。

7 秘密の保持

受託者は、本業務を通じて知り得た秘密の第三者への漏えい、資料・データの紛失、滅失、棄損、盗難等を防止するために必要な措置を講じなければならない。また、本業務データ等の使用、保存、処分等にあたっては、秘密の保持に十分配慮するとともに、機構及び拠点の指示に従わなければならない。

8 権利関係（著作権等）

本業務の履行に係る成果物の所有権及び著作権（著作権法第 21 条から第 28 条までに規定する権利を含む）は、機構及び拠点にそれぞれ帰属するものとし、受託者は著作者人格権を行使しないものとする。

なお、拠点のホームページの使用権は、全て機構及び拠点に帰属すること。ただし、受託者が開発したプログラム等がある場合は、その著作権は受託者に留保する。

9 契約不適合責任

受託者は、検査に合格した成果品であっても、当該成果品について直ちに発見することができない、種類、品質又は数量に関して本契約の内容に適合しないものがあつた場合には、無期限でこれを完全なものと引き換え、又は補償をしなければならない。

10 その他

本仕様書に定めのない事項については、協議の上決定する。

別記 情報セキュリティポリシーに関するガイドライン

1 情報セキュリティ関連規程等の遵守

- (1) 受託者は、本業務全体における情報セキュリティの確保のため、「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）、「経済産業省情報セキュリティ管理規程」（平成18・03・22シ第1号）及び「経済産業省情報セキュリティ対策基準」（平成18・03・24シ第1号）（以下「規程等」と総称する。）に基づく、情報セキュリティ対策を講じる。
- (2) 受託者は、経済産業省又は内閣官房内閣サイバーセキュリティセンターが必要に応じて実施する情報セキュリティ監査、マネジメント監査又はペネトレーションテストを受け入れるとともに、指摘事項への対応を行う。

2 情報セキュリティを確保するための体制

- (1) 受託者は、本業務に従事する者を限定する。また、受注者の資本関係・役員の情報、本業務の実施場所、本業務の全ての従事者の所属、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を機構の担当職員（以下、担当職員という。）に提示する。なお、本業務の実施期間中に従事者を変更等する場合には、事前にこれらの情報を担当職員に再提示する。
- (2) 受託者は、本業務の一部を再委託する場合には、再委託することにより生ずる脅威に対して「情報セキュリティポリシーに関するガイドライン」の1から7までの規定に基づく情報セキュリティ対策が十分に確保される措置を講じる。

3 情報の取扱い

- (1) 受託者は、本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）の取扱いには十分注意を払い、機構内に複製が可能な電子計算機等の機器を持ち込んで作業を行う必要がある場合には、事前に担当職員の許可を得る。なお、この場合であっても、担当職員の許可なく複製しない。また、作業終了後には、持ち込んだ機器から情報が消去されていることを担当職員が確認できる方法で証明する。
- (2) 受託者は、本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体）について、担当職員の許可なく機構外で複製しない。また、作業終了後には、複製した情報が電子計算機等から消去されていることを担当職員が確認できる方法で証明する。
- (3) 受託者は、本業務を終了又は契約解除する場合には、受託者において本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）を速やかに担当職員に返却し、又は廃棄し、若しくは消去する。その際、担当職員の確認を必ず受ける。
- (4) 受託者は、契約期間中及び契約終了後においても、本業務に関して知り得た機構の業務上の内容について、他に漏らし、又は他の目的に利用してはならない。なお、機構の業務上の内容を外部に提供する必要が生じた場合は、提供先で当該情報が適切に取り扱われないおそれがあることに留意し、提供の可否を十分に検討した上で、担当職員の承認を得るとともに、取扱上の注意点を示して提供する。

4 情報セキュリティに係る対策、教育、侵害時の対処

- (1) 受託者は、本業務に使用するソフトウェア、電子計算機等に係る脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策、アクセス制御対策、情報漏えい対策を講じるとともに、契約期間中にこれらの対策に関する情報セキュリティ教育を本業務にかかわる従事者に対し実施する。
- (2) 受託者は、本業務の遂行において、情報セキュリティが侵害され又はそのおそれがある場合の対処方法について担当職員に提示する。また、情報セキュリティが侵害され又はそのおそれがあることを認知した場合には、速やかに担当職員に報告を行い、原因究明及びその対処等について担当職員と協議の上、その指示に従う。

5 クラウドサービス

- (1) 受託者は、本業務を実施するに当たり、民間事業者等が不特定多数の利用者に対して提供する、定型約款や利用規約等への同意のみで利用可能となるクラウドサービスを利用する場合には、これらのサービスで要機密情報を取り扱ってはならず、「情報セキュリティポリシーに関するガイドライン」の1に定める不正アクセス対策を実施するなど規程等を遵守する。

(2) 受託者は、本業務を実施するに当たり、利用において要機密情報を取り扱うものとしてクラウドサービスを調達する際は、「政府情報システムのためのセキュリティ評価制度（ISMAP）」の ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリストから調達することを原則とする。

6 セキュアな情報システム（外部公開ウェブサイトを含む）の構築・運用・閉鎖

(1) 受託者は、情報システム（ウェブサイトを含む。以下同じ。）の設計、構築、運用、保守、廃棄等（電子計算機、電子計算機が組み込まれた機器、通信回線装置、電磁的記録媒体等のハードウェア又はソフトウェア（以下「機器等」という。）の調達を含む場合には、その製造工程を含む。）を行う場合には、以下を実施する。

ア 各工程において、機構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。また、具体的な管理手順や品質保証体制を証明する書類等を提出すること。

イ 情報システムや機器等に意図しない変更が行われる等の不正が見つかったときに、追跡調査や立入検査等、当省と連携して原因を調査し、排除するための手順及び体制を整備していること。これらが妥当であることを証明するため書類を提出すること。

ウ 不正プログラム対策ソフトウェア等の導入に当たり、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入すること。また、以下を含む対策を行うこと。

①不正プログラム対策ソフトウェア等が常に最新の状態となるように構成すること。

②不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態となるように構成すること。

③不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。

④不正プログラム対策ソフトウェア等を定期的に全てのファイルを対象としたスキャンを実施するように構成すること。

⑤EDR ソフトウェア等を利用し、端末やサーバ装置（エンドポイント）の活動を監視し、感染したおそれのある装置を早期にネットワークから切り離す機能の導入を検討すること。

エ 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、担当職員に速やかに報告すること。また、情報システムが構築段階から運用保守段階へ移行する際等、他の事業者へ引き継がれる項目に、情報セキュリティ対策に必要な内容を含めること。

オ サポート期限が切れた又は本業務の期間中にサポート期限が切れる予定がある等、サポートが受けられないソフトウェアの利用を行わないこと、及びその利用を前提としないこと。また、ソフトウェアの名称・バージョン・導入箇所等を管理台帳で管理することに加え、サポート期限に関するものを含むソフトウェアの脆弱性情報を収集し、担当職員に情報提供するとともに、情報を入手した場合には脆弱性対策計画を作成し、担当職員の確認を得た上で対策を講ずること。

カ 受託者自身（再委託先を含む。）が管理責任を有するサーバ等を利用する場合には、OS、ミドルウェア等のソフトウェアの脆弱性情報を収集し、セキュリティ修正プログラムが提供されている場合には業務影響に配慮しつつ、速やかに適用を実施すること。

キ ウェブサイト又は電子メール送受信機能を含むシステム等の機構外向けシステムを構築又は運用する場合には、政府機関のドメインであることが保証されるドメイン名「. go. jp」を使用すること。

ク 外部に公開するウェブサイトを構築又は運用する場合には、以下の対策を実施すること。

・サービス開始前および、運用中においては年1回以上、ポートスキャン、脆弱性検査を含むプラットフォーム診断を実施し、脆弱性を検出した場合には必要な対策を実施すること。

・インターネットを介して通信する情報の盗聴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、TLS(SSL)暗号化の実施等によりウェブサイトの暗号化の対策等を講ずること。

・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こと。

ケ 電子メール送受信機能を含む場合には、SPF（Sender Policy Framework）等のなりすましの防止策を講ずるとともにSMTPによるサーバ間通信のTLS（SSL）化やS/MIME等の電子メールにおける暗号化及び電子署名等により保護すること。

コ ウェブサイト又は電子メール送受信機能を含むシステム等の機構外向けシステムを構築又は運用する場合は、機構が指定する期日にドメインの抹消、DNS や CDN 情報の削除、運用環境の削除を行える事業者を選定すること。また、運用を閉鎖する場合は、終了告知を一定期間行うこと。一定期間の終了告知を終えた後は、ドメインの抹消、DNS や CDN 情報の削除、ドメインへのリンクの削除、SNS を利用していた場合はアカウント削除等、なりすましの防止策を漏れなく講ずること。なお、本事項は、「実施」の場合はその実施内容、「未実施」又は「該当なし」の場合はその理由等を必ず報告すること。

7 アプリケーション・コンテンツの情報セキュリティ対策

(1) 受託者は、アプリケーション・コンテンツ（アプリケーションプログラム、ウェブコンテンツ等の総称をいう。以下同じ。）の開発・作成を行う場合には、利用者の情報セキュリティ水準の低下を招かぬよう、以下の内容も含めて行う。

ア 提供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。また、そのために以下を含む対策を行うこと。

- 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い、不正プログラムが含まれていないことを確認すること。
- ②アプリケーションプログラムを提供する場合には、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認すること。
- ③提供するアプリケーション・コンテンツにおいて、機構外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、HTML ソースを表示させるなどして確認すること。

イ 提供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。

ウ 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場合を除き、実行プログラム形式でコンテンツを提供しないこと。

エ 電子証明書を用いた署名等、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。なお、電子証明書を用いた署名を用いるときに、政府認証基盤（GPKI）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。

オ 提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのOS、ソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更をOS、ソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。

カ 機構外へのアクセスを自動的に発生させる機能やサービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないように開発すること。ただし、必要があつて当該機能をアプリケーション・コンテンツに組み込む場合は、機構外へ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確認した上で、他のウェブサイト等のサーバへ自動的にアクセスが発生すること、サービス利用者その他の者に関する情報が第三者に提供されること及びこれらを無効にする方法等が、サービス利用者において容易に確認ができるよう、担当職員が示すプライバシーポリシー等を当該アプリケーション・コンテンツに掲載すること。

(2) 外部公開ウェブサイト上のウェブアプリケーションの構築又は改修を行う場合には、独立行政法人情報処理推進機構が公開する最新の「安全なウェブサイトの作り方」（以下「作り方」という。）に従う。また、ウェブアプリケーションの構築又は改修時においてはサービス開始前に、運用中においてはウェブアプリケーションへ修正を加えた場合や新たな脅威が確認された場合に、「作り方」に記載されている脆弱性の検査等（ウェブアプリケーション診断）を実施し、脆弱性を検出した場合には必要な対策を実施する。併せて、「作り方」のチェックリストに従い対応状況を確認し、その結果を記入したチェックリストを担当職員に提出する。なお、チェックリストの結果に基づき、担当職員から指示があつた場合には、その指示に従う。