業務委託仕様書

※本事業は、令和７年度経済産業省関連予算の成立を前提に事業化される停止条件付き事業です。
予算の成立がなければ、提案を公募したことに留まり、いかなる効力も発生しません。

１．件名

令和７年度「６次産業化等における継続的な販路開拓へ向けた持続可能な仕組みづくり及び検証等事業」

２．目的

平成２７年６月１２日に閣議決定された「原子力災害からの福島復興の加速に向けて（福島復興指針）」改訂を踏まえ、平成２７年８月２４日に福島相双復興官民合同チームが創設され、避難指示等の対象である浜通り地域等１２市町村（田村市、南相馬市、川俣町、広野町、楢葉町、富岡町、川内村、大熊町、双葉町、浪江町、葛尾村及び飯舘村）の事業者等を対象とした自立支援に官民の総力を挙げて取り組んでいる。また、福島県の漁業における試験操業が令和３年３月に終了し本格操業への移行期間に入ったことを踏まえ、令和３年５月より、いわき市、相馬市及び新地町（以下「３市町」という。）水産関係の仲買・加工業者等への支援も実施している。

こうした中、事業者の支援ニーズや主要な課題の一つとして、住民の避難等に伴う顧客の減少や顧客層の質的変化及び長期にわたる事業休止に伴う取引先の減少等が挙げられている。

本事業では、これらの課題解決に向けて、当機構が行う個別訪問、事業再開・継続支援及び創業支援等と連携しつつ、事業者の現状等を調査し、継続的な販路開拓へ向けた持続可能な仕組みづくりの検討等を実施することで、事業者の帰還、事業・なりわいの再建とともに、浜通り地域等１５市町村（以下「１５市町村」という。）の復興を後押しすることを目的とする。

３．事業内容

（１）実施内容

・受託者は、当機構のほか、１５市町村の自治体その他関係機関及び当機構による令和７年度「６次産業化等へ向けた事業者間マッチング等支援事業」の受託先に加え、金融機関・商工会等とも連携・協力し、継続的な販路開拓へ向けた持続可能な仕組みづくり及び検証等を実施すること。

・受託者は、支援事業者がより効果的な販売等の促進を図れるよう、令和６年度の検討結果も踏まえ、以下７項目の調査・検討・構築を行うこと。

① 展示会/商談会

② 浜通り地域に特化したECサイトの運営

③ 県内外の施設を活用した首都圏市場向けテスト販売

④ 支援事業者と実需者・消費者を結ぶオンラインマッチングの運営

⑤ 支援事業者へのクラウドファインディング

⑥ 支援事業者のバックオフィスシェアリング

⑦ 販路開拓の意識醸成を目的としたセミナー

なお、受託者の創意工夫によって、より高い事業効果が期待される取組を企画し、代替措置が担保される場合には、上記に限らない。実際の事業実施にあたっては、当機構と協議の上、その内容を確定させ、指示された内容を踏まえて実施に当たるものとする。

（２）実施体制

受託者は、以下の体制を構築し、継続的な販路開拓へ向けた持続可能な仕組みづくり及び検証等を行うこと。具体的な体制は、当機構と協議の上、確定させるものとする。

①事業者のニーズ（販路開拓、事業者間マッチング、商品開発・改良等）や業種の特性を踏まえた仕組みづくり及び検証等ができる体制（コンサルタント等の数及び質を確保すること）。

②再委託・外注を実施する場合は、可能な限り、当該地域の流通実態に知見がある地元事業者を活用すること。

③事業予算の効率的な活用を念頭に置き、報告等の間接業務にかかる工数を最小化すること。このため、必要に応じて当機構に会議体や報告の仕方等の改善提案を実施すること。

（３）事業実施状況の報告

当機構からの指示に従い定期的に事業の進捗状況と成果報告の確認を行ったうえで、当機構及び経済産業省に報告すること。

上記報告を踏まえ、当機構及び経済産業省から指示があった場合には、内容の修正や追加的に必要な調査・分析を行うこと。

（４）成果報告書の作成

当事業における実施状況・成果等について、成果報告書を作成すること。成果報告書の構成・内容等については、当機構と協議の上、決定するものとする。

（５）事業内容の引継ぎ

令和８年度に向け、受託者は令和７年度に実施した支援に関し、当機構および必要により次年度受託者への引継ぎを円滑に行うことができるように協力すること。引き継ぐ情報やその方法については、当機構と調整すること。

４．事業実施における注意事項

・事業実施に当たっては、適宜、当機構と協議し進めること。
・公募の際の企画提案書に基づき、当機構と協議し実施計画書を策定すること。
・事業者に関わる情報の管理に当たっては、管理体制を含め適切な保護措置を講ずること。
・本事業の実施中に問題、事故等が発生した場合は、直ちに当機構担当職員に連絡するとと

もに、受託者の責任において解決を図ること。
・その他、業務の遂行において実施内容等について変更があった場合や疑義が生じた場合は、当機構担当職員と協議し、その指示に従うこと。

５．情報セキュリティに関する事項
業務情報を取り扱う場合又は業務情報を取り扱う情報システムやウェブサイトの構築・運用等を行う場合、別記１「情報セキュリティに関する事項」を遵守し、情報セキュリティ対策を実施すること。

６．実施体制
事業の実施体制図を作成し、実施計画書に記載すること。また、事業の運営にあたっては、実施計画書記載の実施体制図及び別紙２の履行体制図のとおり実施すること。

７．スケジュールの策定
事業の実施予定時期を一覧できる年間スケジュールを作成し、実施計画書に記載すること。

８．支出計画
事業の支出計画について各費目毎に作成し、実施計画書に記載すること。

９．実施期間
委託契約締結日から令和８年３月３１日まで
※契約締結日が４月１日以降となった場合は、４月１日を契約開始日とする。

１０．納入物
成果報告書電子媒体（ＰＤＦ等）　１式
なお、成果報告書は、ＰＤＦ形式以外にも、機械判読可能な形式のファイルも納入する。

１１．納入場所
公益社団法人福島相双復興推進機構　事業者支援グループ　販路開拓・人材支援課

１２．その他
（１）成果物の著作権は当機構に譲渡する（既に所有又は管理していた知的財産権を受託者が納入物に使用した場合には、当機構は、当該知的財産権を、仕様書記載の「目的」のため、本契約終了後も期間の制限なく、また追加の対価を支払うことなしに自ら使用し、又は第三者に使用させることができる。）。
（２）氏名表示権については、当機構の指示に従う。
（３）当機構が行う成果物の改変について、著作者人格権を行使しない。

１３．情報管理体制等について
（１）情報管理体制

① 受注者は本事業で知り得た情報を適切に管理するため、次の履行体制を確保し、発注者に対し「情報セキュリティを確保するための体制を定めた書面（情報管理体制図)」及び「情報取扱者名簿」（氏名、個人住所、生年月日、所属部署、役職等が記載されたもの）様式３を契約前に提出し、当機構の同意を得ること（住所、生年月日については、必ずしも契約前に提出することを要しないが、その場合であっても当機構から求められた場合は速やかに提出すること。)。なお、情報取扱者名簿は、委託業務の遂行のため最低限必要な範囲で情報取扱者を掲載すること。

（確保すべき履行体制）

契約を履行する一環として契約相手方が収集、整理、作成等した一切の情報が、当機構が保護を要さないと確認するまでは、情報取扱者名簿に記載のある者以外に伝達又は漏えいされないことを保証する履行体制を有していること。

② 本事業で知り得た一切の情報について、情報取扱者以外の者に開示又は漏えいしてはならないものとする。ただし、当機構の承認を得た場合は、この限りではない。

③ ①の情報セキュリティを確保するための体制を定めた書面又は情報取扱者名簿に変更がある場合は、予め当機構へ届出を行い、同意を得なければならない。

（２）履行完了後の情報の取扱い

当機構から提供した資料又は当機構が指定した資料の取扱い（返却・削除等）については、担当職員の指示に従うこと。業務日誌を始めとする経理処理に関する資料については適切に保管すること。

（別記１）

情報セキュリティに関する事項

以下の事項について遵守すること。

１） 受託者は、契約締結後速やかに、情報セキュリティを確保するための体制を定めたものを含み、以下２）～１８）に記載する事項の遵守の方法及び提出を求める情報、書類等（以下「情報セキュリティを確保するための体制等」という。）について、当機構の担当職員（以下「担当職員」という。）に提示し了承を得た上で確認書類として提出すること。ただし、別途契約締結前に、情報セキュリティを確保するための体制等について担当職員に提示し了承を得た上で提出したときは、この限りでない。また、定期的に、情報セキュリティを確保するための体制等及び対策に係る実施状況を紙媒体又は電子媒体により報告すること。加えて、これらに変更が生じる場合は、事前に担当職員へ案を提出し、同意を得ること。

なお、報告の内容について、担当職員と受託者が協議し不十分であると認めた場合、受託者は、速やかに担当職員と協議し対策を講ずること。

２） 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こと。

３） 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、当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こと。なお、この場合であっても、担当職員の許可なく複製してはならない。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こと。

４） 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当機構外で複製してはならない。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こと。

５） 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又は廃棄若しくは消去すること。その際、担当職員の確認を必ず受けること。

６） 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当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、当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こと。

7） 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こと。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、その指示に従うこと。

8） 受託者は、当機構の「情報セキュリティ管理ルール（管理者編）」及び「情報セキュリティ管理ルール（利用者編）」（以下「規程関連文書等」と総称する）を遵守すること。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。

9） 受託者は、当機構等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こと。

１０） 受託者は、本業務に従事する者を限定すること。また、受託者の資本関係・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担当職員に提示すること。なお、本業務の実施期間中に従事者を変更等する場合は、事前にこれらの情報を担当職員に再提示すること。

１１） 受託者は、本業務を再委託（業務の一部を第三者に委託することをいい、外注及び請負を含む。以下同じ。）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、上記１）から１０）まで及び１２）から１８）までの措置の実施を契約等により再委託先に担保させること。また、１）の確認書類には再委託先に係るものも含むこと。

１２） 受託者は、外部公開ウェブサイト（以下「ウェブサイト」という。）を構築又は運用するプラットフォームとして、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。また、ウェブサイト構築時においてはサービス開始前に、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。

１３） 受託者は、ウェブサイトを構築又は運用する場合には、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じること。

なお、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。

１４） 受託者は、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。）に基づくこと。また、ウェブアプリケーションの構築又は更改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こと。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こと。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った場合は、それに従うこと。

１５） 受託者は、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を構築又は運用する場合には、非営利団体のドメインであることが保証されるドメイン名「.or.jp」を使用すること。

１６） 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、以下を実施すること。

①各工程において、当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。

②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、当機構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。そ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。

③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。

④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。

⑤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。

⑥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。

１７） 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、画一的な約款や規約等への同意のみで利用可能となる外部サービス（ソーシャルメディアサービスを含む）を利用する場合には、これらのサービスで要機密情報を扱ってはならず、８）に掲げる規程等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こと。なお、受託者は、委託業務を実施するに当たり、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）」において登録されたサービスから調達することを原則とすること。

１８） 受託者は、ウェブサイトの構築又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こと。

①提供するウェブサイト又はアプリケーション・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。

(a) ウェブサイト又はアプリケーション・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。

(b) 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。

(c) 提供するウェブサイト又はアプリケーション・コンテンツにおいて、当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。

②提供するウェブサイト又はアプリケーションが脆弱性を含まないこと。

③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。

④電子証明書を用いた署名等、提供するウェブサイト又はアプリケーション・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、それをウェブサイト又はアプリケーション・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。

⑤提供するウェブサイト又はアプリケーション・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や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やソフトウェア等の利用者に要求することがないよう、ウェブサイト又はアプリケーション・コンテンツの提供方式を定めて開発すること。

⑥当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ウェブサイト又はアプリケーション・コンテンツに組み込まれることがないよう開発すること。ただし、必要があって当該機能をウェブサイト又はアプリケーション・コンテンツに組み込む場合は、当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ウェブサイト又はアプリケーション・コンテンツに掲載すること。