

業務委託仕様書

1. 件名

令和7年度「工業系ものづくり分野における持続可能な販路開拓等発展に資する仕組みづくり及び実証等事業」

2. 目的・背景

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（以下、「官民合同チーム」という。）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、楡葉町、富岡町、川内村、大熊町、双葉町、浪江町、葛尾村及び飯舘村をいい、以下「12市町村」という。）の事業者等を対象とした自立支援に取り組んでいる。近年、復興のフェーズが進むにつれ、個別事業者への支援に加え、12市町村全体を対象とした産業創出に関する面的支援が求められており、国家プロジェクトである福島イノベーション・コースト構想のもと、以下の取組を進める。

同構想では、重点6分野（廃炉、ロボット・ドローン、エネルギー・環境・リサイクル、農林水産業、医療関連、航空宇宙）において、企業と企業、企業と研究機関等の新たな結合が盛んに起こることが期待されており、例えば、関連するスタートアップ企業が12市町村に多く進出するなど、新たな結合の対象となる企業等は増加しつつある。これらのものに対する支援機関等のマッチングや各種支援が奏功し、上市を見据えた成長フェーズに進む企業も出現しているが、より多くの結合がさまざまなレイヤーで頻繁に発生するよう促すための仕組みが求められる。例えば、工業系ものづくり分野においては、12市町村に震災前から立地する地元の工業系ものづくり事業者と、震災後に進出したファブレス型スタートアップ企業、さらには研究機関との間で、試作品の設計・製造等の連携等が一層進むことが期待される。

本事業では、12市町村において企業間等の新たな結合が持続的に創出されるような仕組みを検討・構築することで、これらの企業群の販路開拓を面的に促進するとともに、福島イノベーション・コースト構想の実現を通じた復興の後押しを目的とする。

3. 事業内容及び実施方法等

（1）事業内容

受託者は以下①～⑥の内容について実施すること。

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が提案された場合には、当機構と協議の上事業内容を確定し、当該内容を踏まえて実施する。

① 地域コーディネーターと広域コーディネーターのあり方検討

12市町村には、スタートアップの相談役となる「お節介」的な“地域コーディネーター”が存在し、それぞれの所在する地域にて、自身のコネクションや経験等を駆使して多様な課題に対する解決方法の提供に尽力している。これまで、地域コーディネ

ネーターの活躍により、進出スタートアップ等の孤立が防がれ、地元事業者とのつながりが生み出されるなど、新たな結合を通じたポジティブな成果が現れている。

一方、地域内では解決できない課題や地域コーディネーターの知見や経験が及ばない領域で対処が求められる場面も出現していることから、地域コーディネーターをサポートする体制を確保することが重要。

そのためには12市町村を広域でカバーできる“広域コーディネーター”が、臨機応変に地域コーディネーターと連携し、補完的に機能することが肝要である。(広域コーディネーターは、12市町村を広域で管轄する福島イノベーション・コースト構想推進機構や官民合同チームのような組織が担うことを想定。)

これら地域コーディネーターと広域コーディネーターが有機的に連携できるよう、連携のあり方を検討する。具体的には、それぞれに必要な機能や特性等を明確化し、両者間の連携が求められるパターンを例示する。また、地域コーディネーターや広域コーディネーターへのアプローチの円滑化を図るため、所在を顕示するとともに、その情報が必要とする者に届くよう発信方法を提案する。

なお、昨年度の委託事業において、コーディネーターの重要な機能のひとつとして、12市町村で生み出された製品やサービスが市場に受け入れられるよう、感度高くアンテナを立てフィードバックを実施する需要搬入機能が求められることが分かっている。コーディネーター機能の検討においては、この点にも留意すること。

② 地域コーディネーターの掘り起こし、意識醸成

上記①のとおり、既に地域コーディネーターは存在するものの、コネクションや得意とする領域は区々であることから、多様な課題に対応し、持続的な仕組みとするには、新たに地域コーディネーターとなりうる人材の掘り起こしと顕在化が重要。昨年度委託事業においてリストアップした候補者人材名簿をもとに、拡充を図ること。

さらに掘り起こしだけでなく、既存の地域コーディネーター、広域コーディネーターとのネットワーキング促進や、地域コーディネーターに必要なマインドを備えるための意識醸成を行う。意識醸成に当たっては、単にセミナーを開催するのではなく、既存の枠組みに組み込むなど効果的かつ持続的な方法を検討すること。

③ 福島県内支援機関同士の既存ネットワークとの連携（県域への拡大）

持続的な仕組みとするには既存のネットワークに組み込みを図り、県内支援機関とも連携することが必要。そのために必要な手立てを行う（例：県内支援機関同士の連携会議への参加等）。

④ 有識者座談会の実施

上記①～③の実施に当たり、地元や専門家の意見を反映するべく、地元企業、進出企業（スタートアップ含む）、地元支援機関、アカデミア、研究機関等の有識者による座談会形式の意見交換会を年2回以上開催する。なお、有識者は昨年度と同様とし、原則選定は行わないものとする。

⑤ プロトタイピングの実施

上述した内容が有機的な仕組みとなるために、新結合案件を具体的に組成するプロトタイピングを、令和7年度第4四半期までに最低1件実施する。

⑥ 業務ファシリテーション機能のあり方の検討、類似事業者へのヒアリング

域外からのプレーヤーの呼び込み、新たな結合及び地域への定着を促進するため、特にスタートアップ向けの業務ファシリテーション機能の内容、あり方を検討する他、類似事業を実施している事業者や他地域へのヒアリングを実施する。

機能の例として、1) スタートアップがコア業務に注力できるよう非コア業務を外部機関等が請負、2) より専門性の高い試験等の業務において知見のある外部機関等がサポート、等を想定している。

当該ファシリテーション機能の存在が、コーディネーター業務の実施に当たり提供できるソリューションのひとつとなることを想定しており、上記①～⑤も念頭に置きつつ検討すること。

(2) 実施方法

受託者は、当機構のほか、必要に応じて12市町村の自治体やその他関係機関及び当機構による令和7年度「工業系ものづくり分野における販路開拓実証等事業」の受託先とも連携して12市町村の工業系ものづくり企業等の持続的発展を図る方策の検討を実施すること。

また受託者は、事業開始後速やかに昨年度事業の成果報告書を参照する等によりキャッチアップを行うこと。

(3) 実施体制

・受託者は、以下の体制を構築し、持続可能な仕組みづくりの検討・実証を行うこと。具体的な体制は、当機構と協議の上、指示された内容を踏まえて確定させるものとする。

- ①工業系事業者の販路開拓等に関する持続可能な仕組みづくりの検討を進めていくにあたっての現状の課題の特定、技術的な側面を含めた強み等の整理を行い、これらを通じた成果・課題の分析等ができる体制（コンサルタント等の数及び質を確保すること）。
- ②当機構の他に、12市町村の工業系ものづくりのキーパーソンやイノベ機構を始めとする各種支援機関等と現地で密に連携ができる体制。
- ③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。
- ④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。

(4) 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。

(5) 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、報告書を作成すること。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。

(6) 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実施すること。
- ・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

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. 実施期間

委託契約締結日から令和8年3月31日まで

9. 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。

10. 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

11. 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。

1 2. 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。

1 3. 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）別記2様式を契約前に提出し、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、当機構が保護を要し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。

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。

1 5) 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、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」または、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。

1 6) 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に、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に開発すること。ただし、必要があつ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が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。