# 仕様書

１．件名

令和５年度二国間クレジット取得等のためのインフラ整備調査事業（モーリシャスにおける海洋温度差発電に係るＧＣＦ／ＣＴＣＮに関する実現可能性調査）

２．事業の目的（概要）

ＣＯＰ２１で採択されたパリ協定においては、すべての締約国は温室効果ガスの削減目標等である「国が決定する貢献（ＮＤＣ：Nationally Determined Contribution)」の作成が求められている。令和３年１０月に改定された我が国のＮＤＣにおいては、２０３０年度４６％削減(２０１３年度比)という目標を掲げており、また、この水準にとどまることなく、エネルギーミックス等とも整合的に、中長期の両面で更なる削減努力を追求するとしている。また気候変動問題は、我が国における温室効果ガスの排出削減だけで解決できる問題ではなく、世界全体で排出削減を行っていくことが必要不可欠である。インフラシステムの海外展開の場面においても、パリ協定の目指すカーボンニュートラルへの貢献が期待されており、我が国は、世界の脱炭素化を牽引する国際的リーダーシップを発揮する必要がある。我が国としては、二国間の枠組みを通じて、我が国の優れた環境・エネルギー技術の普及等を進め、地球規模での温室効果ガスの削減に貢献する仕組みとして「二国間クレジット制度」を推進してきたが、当該制度の普及のためには、産業分野ごとの環境・エネルギー技術に関する詳細なシーズ・ニーズを二国間で把握するのみならず、多国間の枠組みを活用していくことも効果的である。

ＣＯＰ１６では、先進国から途上国への技術移転のためのメカニズムとして、技術執行委員会（ＴＥＣ）及び気候技術センター・ネットワーク（ＣＴＣＮ）が設立された。ＣＴＣＮを通じて途上国への技術移転が進められているが、これまでの技術移転のためのメカニズムの採択案件に日本企業が参画している案件が少ないのが現状である。気候変動問題の解決に向けては、同メカニズムが途上国における排出削減や気候変動影響への対策に効果的かつ効率的に活用されることが重要である。特に、同メカニズムの活用により、途上国に対して我が国の優れた環境・エネルギー技術の展開が促進されることが期待される。

また、モーリシャスにおいては、島嶼国における脱炭素技術の導入についての検討が進められており、中でも我が国が技術的優位性を持つ海洋温度差発電（ＯＴＥＣ）が有力候補として挙げられている。この技術については、深海層からの取水管の設計が事業の実現可能性に大きな影響を与えるため、モーリシャス政府は、ＣＴＣＮを活用したプレフィージビリティスタディを行うことを希望している。このような背景から、我が国が、緑の気候基金（ＧＣＦ）等を視野に入れた事業化を準備

する前段階のステップとして、ＣＴＣＮによるプレフィージビリティスタディを実施することが、途上国等において我が国の優れた脱炭素技術・製品の普及等を促進し、当該国での温室効果ガス排出削減を実現する等、世界全体の温室効果ガス排出削減に重要な取り組みとなる。

上記の背景を踏まえ、本事業においては、ＣＴＣＮの活用を念頭に、モーリシャスにおける海洋温度差発電の実現可能性調査を行うことを目的とする。具体的な事業内容は以下のとおり。

３．事業内容

通常のＣＴＣＮにおいては、モーリシャス政府によるリクエストフォーム（Request Submission Form）をＣＴＣＮ事務局が受領した後、国連の調達プロセスを通じて支援実施者が決定されるが、本事業は経済産業省におけるＰｒｏ－ｂｏｎｏ案件として取り扱われるため、リクエストフォームに基づくＣＴＣＮ事務局による技術支援計画に沿った事業を経済産業省が主導することとなる。そのため、より確実で効果的なモーリシャスへの支援が期待できる。事業内容の詳細は以下の通り。

（１）ＣＴＣＮへのリクエストフォーム提出に向けた技術支援

モーリシャスのＣＴＣＮの国家指定機関である環境廃棄物管理気候変動省が、主要関係省庁・機関と協力しＣＴＣＮ事務局に提出予定の海洋温度差発電及び海洋深層水関連産業の導入実現可能性調査に係るリクエストフォームの改訂補助、及び当該リクエストフォームのＣＴＣＮへの提出を受けてモーリシャス政府と経済産業省が共同で提出するレスポンスプラン（Response Plan）の作成・改訂補助、並びにそれらに関するモーリシャス政府、ＣＴＣＮ事務局、経済産業省との間の必要な連絡調整を行うこと。

（２）実施計画書・ＣＴＣＮ事務局への報告文書の作成

業務を円滑に実施し、作業の進捗を関係者間で把握するための実施計画書、及び進捗管理表を英語で作成すること。併せて、プロジェクトの影響を評価するためのモニタリング・評価計画（Monitoring and evaluation plan）及びインパクトステートメント（Impact Statement）を技術支援の開始時に作成し、ＣＴＣＮ事務局に提出すること。なお、インパクトステートメントは技術支援が完了した後に更新・修正を行う。

加えて、技術支援が完了した際に、事業完了報告書（Closure report）を作成し、ＣＴＣＮ事務局に提出すること。なお、これらの文書を作成する際に当たっては、ＣＴＣＮ事務局から提供されるテンプレートがある場合には、それを活用して作成すること。また、業務実施中に追加で書類の作成・提出が求められた場合には、経済産業省担当官と相談の上対応すること。

（３）候補地における取水管及び取水管設置概略検討

以下の項目についてデスクトップ調査を実施する。

a. 概略検討の与条件（海底地形・地質、波浪、潮流、航路等）調査
b. a.の結果を踏まえた候補地における取水管のルート妥当性検討
c. a.の結果を踏まえた海洋深層水・表層水の取水口地点の選定
d. 放流水（発電利用・二次利用後）の適地選定
e. 大口径取水管敷設に関する最新事例の技術動向調査
f. 現地工事における建設（海洋工事）業者のポテンシャルに関する調査

（４）ＧＣＦへの提案可能性の検討

①コンセプトノートの作成

ＣＴＣＮ事務局と連携し、事業実施に向けてＧＣＦ資金動員を念頭に置き提出するコンセプトノート案を作成する。コンセプトノートについては、（３）で検討する取水管設置のプレフィージビリティスタディの結果に加え、新エネルギー・産業技術総合開発機構（ＮＥＤＯ）の実証事業の下で実施した「エネルギー消費の効率化等に資する我が国技術の国際実証事業（実証要件適合性等調査)」におけるモーリシャスにおける海洋温度差発電にかかる調査の結果をも踏まえ、GCF が求める要件を踏まえて作成を行うこと。

②認証機関（ＡＥ）選定の検討

ＧＣＦへのファンディング・プロポーザル提出、事業実施に向けて、ＧＣＦに資金アクセスを行うための認証機関（AE）の選定について検討を行う。

４．報告書の作成

上記の内容を踏まえ、地球環境対策室と協議の上、報告書を作成する。

５．事業期間

委託契約締結日から、令和６年３月２７日まで。

６．成果物

・調査報告書電子媒体（ＣＤ－Ｒ）　１式

- 調査報告書、調査で得られた元データ、委託調査報告書公表用書誌情報（様式１）、二次利用未承諾リスト（様式２）を納入すること。
- 調査報告書については、PDF 形式に加え、機械判読可能な形式のファイルも納入すること。
- 調査で得られた元データについては、機械判読可能な形式のファイルで納入することとし、特に図表・グラフに係るデータ（以下「EXCEL 等データ」という。）につい

ては、EXCEL 形式等により納入すること。

- なお、様式１及び様式２は EXCEL 形式とする。

・調査報告書電子媒体（ＣＤ－Ｒ）　２式（公表用）

- 調査報告書及び様式２（該当がある場合のみ）を一つの PDF ファイル（透明テキスト付）に統合したもの、並びに公開可能かつ二次利用可能な EXCEL 等データを納入すること。
- セキュリティ等の観点から、経済産業省と協議の上、非公開とするべき部分については、削除するなどの適切な処置を講ずること。
- 調査報告書は、オープンデータ（二次利用可能な状態）として公開されることを前提とし、経済産業省以外の第三者の知的財産権が関与する内容を報告書に盛り込む場合は、①事前に当該権利保有者の了承を得、②報告書内に出典を明記し、③当該権利保有者に二次利用の了承を得ること。二次利用の了承を得ることが困難な場合等は、下記の様式２に当該箇所を記述し、提出すること。
- 公開可能かつ二次利用可能な EXCEL 等データが複数ファイルにわたる場合、１つのフォルダに格納した上で納入すること。

◆各データのファイル名については、調査報告書の図表名と整合をとること。

◆Excel 等データは、オープンデータとして公開されることを前提とし、経済産業省以外の第三者の知的財産権が関与する内容を含まないものとすること。

※調査報告書電子媒体の具体的な作成方法の確認及び様式１・様式２のダウンロードは、下記 URL から行うこと。

https://www.meti.go.jp/topic/data/e90622aj.html

７．成果物の納入場所

経済産業省産業技術環境局地球環境対策室（経済産業省別館６階６４８号室）

８．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並びに以下 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、経済産業省（以下「当省」という。）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、当省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省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し、又は廃棄し、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省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、当省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、「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)」、「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)」及び「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群（令和３年度版)」（以下「規程等」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には、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、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。

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、当省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。

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。

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。

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、当省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、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、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当省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、当省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。

９．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１を契約前に提出し、担当課室の同意を得ること（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担当課室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、経済産業省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、担当課室の承認を得た場合は、この限りではない。

③①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、予め担当課室へ届出を行い、同意を得なければならない。

１０．履行完了後の情報の取扱い

国から提供した資料又は国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。