（別紙）

仕様書

１．事業名

令和７年度固定価格買取制度等効率的・安定的運用業務事業（再生可能エネルギー発電設備の費用報告データ分析業務）

２．事業目的

２０２５年２月に閣議決定された第７次エネルギー基本計画において、２０５０年カーボンニュートラル実現に向けて、エネルギー安定供給と脱炭素を両立する観点から再生可能エネルギーを主力電源として最大限導入することが掲げられている。こうした目標の実現に向けては、エネルギー政策の原則であるＳ＋３Ｅを大前提に、電力部門の脱炭素化に向け、再生可能エネルギーの主力電源化を徹底し、地域との共生と国民負担の抑制を図りながら最大限の導入を促す方針が掲げられている。

こうした状況の中で、再生可能エネルギーのコスト低減やＦＩＴ制度からの自立化に向けて、中長期価格目標の設定、トップランナーに照準を合わせた基準価格・調達価格の設定、入札制度の活用、ＦＩＰ制度の導入などを進めてきた。また、地域と共生した再生可能エネルギーの導入加速化に向けて、設置の形態等に基づくより詳細なコスト動向を分析による基準価格・調達価格の設定などを行ってきた。今後も国民負担の抑制と地域共生を図りながら再生可能エネルギーを最大限導入していくためには、現在の再生可能エネルギーのコスト動向を的確に把握した上での制度設計が不可欠である。

このため、本事業においては、ＦＩＴ・ＦＩＰ制度の認定を受けた事業者が経済産業大臣に報告した発電設備の設置及び運転維持に要したコストデータの分析等を行うとともに、その中長期的な動向の予測を行う。分析されたデータについては、必要に応じて、例年９月頃から翌年１月頃まで８回程度開催される調達価格等算定委員会における事務局資料等として活用するとともに、経済産業省における政策立案の参考資料とすることを予定している。

３．事業内容

（１）定期報告データの整理・管理等

資源エネルギー庁省エネルギー・新エネルギー部新エネルギー課（以下「新エネルギー課」という。）より提供される定期報告データ等（発電量データ等を含む。）について、データの整理及び管理・分析を行う。記載内容に誤りがある可能性のある事項及び内容に精査が必要な事項については、必要に応じ当該設備の設置者等に内容の照会等を行うことにより、データの精度を高める。また、新エネルギー課から提供される設備ＩＤを用いて、ＦＩＴ・ＦＩＰ認定データ及び運転開始月日のデータと照合の上、報告状況のステータス管理を行う。なお、本調査の実施に当たって必要となる、ＦＩＴ・ＦＩＰ認定データ（事業者の連絡先等）及び運転開始月日のデータの参照権限を付与するが、当該データの取扱いには十分に注意すること。

（２）定期報告以外の追加的な調査等

定期報告以外に、調達価格等算定委員会において２０２５年２月に取りまとめられた「令和７年度以降の調達価格等に関する意見」を踏まえつつ、調達価格等の算定に関連する以下の事項について、対象や件数等を新エネルギー課と協議の上、調査を行う。加えて、以下の事項以外にも、調達価格等算定委員会等における議論及びＦＩＴ・ＦＩＰ制度の政策立案に資する事項について、新エネルギー課と協議の上、調査を行う。

・太陽光発電設備における自然災害の動向と対策に関する調査

再エネの長期安定電源化に向けては、災害・盗難等の事業リスクに備え、設備の改修やメンテナンスを適切に実施するとともに、リスクが発現した際の事業継続性を担保する観

点から、保険への加入が重要であるが、自然災害の増加や銅線ケーブル盗難の増加等を背景に、保険料の高騰や免責金額の増加、保険の新規引受の停止といった事態が生じていることを踏まえ、太陽光発電事業者にアンケートを実施し、自然災害による被害の実態、実施されている対策やそのコスト、対策の効果等を把握する。アンケートの送付件数は最大30,000件程度とし、新エネルギー課と調整の上、決定する。

（３）記載内容の分析・評価

（１）及び（２）によって得られたデータを活用し、令和８年度以降の基準価格等・基準価格等、入札制度、中長期価格目標、複数年度の調達価格等の設定等の制度運用の検討及び中長期における再エネ発電設備の導入量・発電コスト等の検討に当たって、調達価格等算定委員会などの審議会等での事務局資料作成に必要な分析を行う。また、出力規模だけでなく設置の形態ごとなど、さらなる精緻な分析を行う。これらの内容については定期的に新エネルギー課に報告及び協議を行う。

（４）次年度以降の事業への提案

今年度の事業を踏まえ、次年度以降に向けた改善点を新エネルギー課に提案する。

（５）その他

調達価格等算定委員会等の開催日を見据えながら、新エネルギー課と協議・調整を行った上、適切な時期に中間報告としてデータの整理・分析を行い、新エネルギー課に提出する。また、業務実施期間中、新エネルギー課から指示があった場合は、既に入力したデータ及び分析結果の全部又は一部を抽出し、速やかに新エネルギー課に提出する。中間報告後、実施期間の終了の日までに、新エネルギー課と協議の上で追加的な分析を行い、最終報告を新エネルギー課に提出する。

４．事業期間

委託契約締結日から令和８年３月３１日まで

５．納入物

・調査報告書電子媒体（ＣＤ－Ｒ又はＤＶＤ－Ｒ）　１枚

- 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又はＤＶＤ－Ｒ）　２枚（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、資源エネルギー庁と協議の上、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、資源エネルギー庁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、資源エネルギー庁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

６．納入場所
資源エネルギー庁省エネルギー・新エネルギー部新エネルギー課

７．情報セキュリティに関する事項
（１）情報セキュリティ対策
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。

（２）情報管理体制
① 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、新エネルギー課に対し「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）を契約前に提出し、新エネルギー課の同意を得る。（個人住所、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新エネルギー課から求められた場合は速やかに提出する。）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。
（確保すべき履行体制）
契約を履行する一環として本事業で収集、整理、作成等した一切の情報が、新エネルギー課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しないことを保証する履行体制を有する。

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ない。ただし、新エネルギー課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、予め新エネルギー課へ届出を行い、同意を得る。

（３）履行完了後の情報の取扱い
国から提供を受け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、新エネルギー課の指示に従う。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。

（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５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等の当省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。

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システム等の当省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。

⑦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。また、外部サービスを利用する場合は、その利用状況を管理すること。

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。