

実施計画書（仕様書）

1. 事業名

令和8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、FIT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き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10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取りまとめられた「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。

・地域と共生した再生可能エネルギーに関する調査

太陽光発電を主な対象として、地域と共生した再生可能エネルギーについて、定期報告データ等による分析を通じ、費用効率的に事業を実施している案件における共通的な特徴を抽出したうえで、必要に応じてアンケート等により、実態や課題把握等の調査を行う。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9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・分析を行うほか、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。また、データの整理・分析・抽出方法についてのマニュアルを作成し、新エネルギー課へ提出する。

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9年3月31日まで

5. 納入物

(1) 調査報告書等一式

- 調査報告書、報告書骨子(様式1)、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2)、二次利用未承諾リスト(様式3)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¹な形式のファイルも納入すること。なお、報告書のデータ量が128MB、ページ数が1,000ページ又は文字数が400万文字を超過する場合には、いずれの制限も超えないようファイルを分割して提出すること。
- 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「図表等データ」という。)については、構造化されたExcelやCSV形式等により納入すること。

(2) 調査報告書等一式(公表用)

- 調査報告書及び様式3(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²な図表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、特に以下の点に注意し、削除するなどの適切な処置を講ずること。
 - 報告書・Excelデータ等に個人情報や不適切な企業情報が存在しないか。(プロパティの情報も漏れなく確認すること)
 - 報告書(PDF)に目視では確認できない埋め込みデータ等が存在しないか。
 - Excelデータ等に目視では確認できない非表示情報が存在しないか。

¹ コンピュータプログラムがデータ構造を識別し、データを処理(加工、編集等)できること。例えばHTML、txt、csv、xhtml、epub、gml、kml等のほか、Word、Excel、PowerPoint等のデータが該当する(スキャンデータのようなものは該当しない)。

² 営利目的を含む、自由な利用(転載・コピー共有等)を行うこと。

- E x c e l データ等に非表示の行・列が存在しないか。
- プロパティの削除は完了しているか。
- 公開可能かつ二次利用可能な図表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。
 - 図表等データは、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。

(3) 様式1～様式3について

- (様式1) 委託調査報告書骨子³
 - レイアウト(余白、フォント等)に従い、3枚以内にまとめた上でW o r d形式にて納入すること。
 - 図表は挿入せずテキスト形式で作成すること。
 - 見出しについては記載された項目のとおりとすること。
- (様式2) 委託調査報告書公表用書誌情報⁴
 - ファイル形式はE x c e l形式で納入すること。
 - 報告書の英語版や概要版等、公表用の報告書と同一のPDFファイルとすることが適当でない公表用の納入物がある場合には1つのPDFファイルごとに作成すること。
- (様式3) 二次利用未承諾リスト
 - 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が前提だが、二次利用の了承を得ることが困難な場合又は了承を得ることが報告書の内容に大きな悪影響を与える場合は、報告書の当該箇所に出典等を明示し、知的財産権の所在を明らかにした上で、当該データを様式3に記載すること(知的財産権の所在が不明なものも含む)。
 - ファイル形式はE x c e l形式で納入すること。
- 様式1～3ダウンロード先
 - [委託調査報告書 \(METI/経済産業省\)](#)

6. 納入方法

- メール提出やファイル交換サイト等の手段を用いること。なお、具体的な納入方法は担当課室と協議の上、決定すること。
- 公表用資料一式と非公表資料一式が紛れないように整理して納入すること。

7. 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

8. 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4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

³委託調査報告書のデータ利活用を促進するため、報告書の概要を骨子としてまとめるもの。

⁴本事業の報告書のオープンデータとしての公表に際し、データとしての検索性を高めるため、当該データの属性情報に関するデータを作成するもの。

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の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。
- 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、あらかじめ担当課室へ届出を行い、同意を得なければならない。

9. 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、担当課室の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。

10. 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「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。

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。

【情報セキュリティ関連事項の確保体制及び遵守状況の報告】

- 1) 受注者（委託契約の場合には、受託者。以下同じ。）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)～17)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（「情報セキュリティに関する事項の遵守の方法の実施状況報告書」（別紙））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、担当職員と受注者が協議し不十分であると認めた場合、受注者は、速やかに担当職員と協議し対策を講ずること。

【情報セキュリティ関連規程等の遵守】

- 2) 受注者は、「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 7 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。
- 3) 受注者は、当省又は内閣官房国家サイバー統括室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。

【情報セキュリティを確保するための体制】

- 4) 受注者は、本業務に従事する者を限定すること。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。

- 5) 受注者は、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、1)から 17)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。

【情報の取扱い】

- 6) 受注者は、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。

- 7) 受注者は、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。
- 8) 受注者は、本業務を終了又は契約解除する場合には、受注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。
- 9) 受注者は、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。

【情報セキュリティに係る対策、教育、侵害時の対処】

- 10) 受注者は、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。
- 11) 受注者は、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。

【クラウドサービス】

- 12) 受注者は、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、2)に掲げる規程等で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。
- 13) 受注者は、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こと。
- 14) 受注者は、前2項におけるクラウドサービスの利用の際は、提供条件等から、利用に当たってのリスクの評価を行い、リスクが許容できることを確認して担当職員の利用承認を得るとともに、取扱上の注意点を示して提供し、その利用状況を管理すること。

【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】

- 15) 受注者は、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。また、以下を含む対策を行うこと。
 - (a) 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。
 - (b) 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。
 - (c) 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。
 - (d) 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。
 - (e) EDR 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。
- 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 受注者自身（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。
- ⑦ 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。
- ⑧ 外部に公開するウェブサイトや構築又は運用する場合には、以下の対策を実施すること。
 - ・サービス開始前及び、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。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。

⑨ 電子メール送受信機能を含む場合には、SPF (Sender Policy Framework) 、DKIM (DomainKeys Identified Mail) 、DMARC (Domain-based Message Authentication, Reporting & Conformance) による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。

⑩ 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は、ドメインに関する情報が正確であることの定期的な確認、当省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。

【アプリケーション・コンテンツの情報セキュリティ対策】

16) 受注者は、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こと。

① 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。

(a) 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 提供するアプリケーション・コンテンツ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。

⑤ 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に、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アプリケーション・コンテンツに掲載すること。

- 17) 受注者は、外部に公開する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。あわせて、「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。

令和 年 月 日

資源エネルギー庁〇〇〇課長 殿

住 所
名 称
代 表 者 氏 名

情報セキュリティに関する事項の遵守の方法の実施状況報告書

情報セキュリティに関する事項1)の規定に基づき、下記のとおり報告します。

記

1. 契約件名等

契約締結日	
契約件名	

2. 報告事項

項目	確認事項	実施状況
情報セキュリティに関する事項 2)	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7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。	
情報セキュリティに関する事項 3)	経済産業省又は内閣官房国家サイバー統括室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。	
情報セキュリティに関する事項 4)	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担当職員に提示する。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。	
情報セキュリティに関する事項 5)	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に関する事項1)から17)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。	
情報セキュリティに関する事項 6)	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、経済産業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、事前に経済産業省の担当職員（以下「担当職員」という。）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。	
情報セキュリティに関する事項 7)	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経済産業省外で複製しない。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。	

情報セキュリティに関する事項 8)	本業務を終了又は契約解除する場合には、受注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。	
情報セキュリティに関する事項 9)	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経済産業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、経済産業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。	
情報セキュリティに関する事項 10)	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。	
情報セキュリティに関する事項 11)	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。	
情報セキュリティに関する事項 12)	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、「情報セキュリティに関する事項2）」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。	
情報セキュリティに関する事項 13)	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こと。	
情報セキュリティに関する事項 14)	情報セキュリティに関する事項12)及び13)におけるクラウドサービスの利用の際は、提供条件等から、利用に当たってのリスクの評価を行い、リスクが許容出来ることを確認して担当職員の利用承認を得るとともに、取扱上の注意点を示して提供し、その利用状況を管理すること。	
情報セキュリティに関する事項 15)	<p>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。</p> <p>(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。</p> <p>(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。</p> <p>(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。また、以下を含む対策を行うこと。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>(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。</p> <p>(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</p>	

	<p>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。</p> <p>(6) 受注者自身（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。</p> <p>(7) 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。</p> <p>(8) 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。</p> <ul style="list-style-type: none"> ・サービス開始前及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。 <p>(9) 電子メール送受信機能を含む場合には、SPF（Sender Policy Framework）、DKIM（DomainKeys Identified Mail）、DMARC（Domain-based Message Authentication, Reporting & Conformance）による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。</p> <p>(10) 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は、ドメインに関する情報が正確であることの定期的な確認、当省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。</p> <p>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。</p>	
<p>情報セキュリティに関する事項 16)</p>	<p>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。</p> <p>(1) 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。</p> <ol style="list-style-type: none"> 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、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。 <p>(2) 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。</p> <p>(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。</p> <p>(4) 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。</p> <p>(5) 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</p>	

	<p>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。</p> <p>(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、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アプリケーション・コンテンツに掲載すること。</p>	
<p>情報セキュリティに関する事項 17)</p>	<p>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。</p> <p>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。</p>	

記載要領

1. 「実施状況」は、情報セキュリティに関する事項2)から17)までに規定した事項について、情報セキュリティに関する事項1)に基づき提出した確認書類で示された遵守の方法の実施状況をチェックするものであり、「実施」、「未実施」又は「該当なし」のいずれか一つを記載すること。「未実施」又は「該当なし」と記載した項目については、別葉にて理由も報告すること。
2. 上記に記載のない項目を追加することは妨げないが、事前に経済産業省と相談すること。
(この報告書の提出時期：定期的(契約期間における半期を目処(複数年の契約においては年1回以上))。)