（別紙）

仕様書

１．事業名

令和７年度エネルギー需給統計整備等調査事業（総合エネルギー統計関係の整備及び分析に関する調査）

２．事業目的

総合エネルギー統計は、我が国に輸入され又は国内で生産され供給された各種のエネルギー源が、どのように転換され、最終的にどのような形態で、どの部門や目的に消費されたかという国内のエネルギー・フローを表す統計である。この統計から我が国のエネルギー需給の実態を把握・分析することができ、また、エネルギー起源ＣＯ２排出量を算定することができる。そのため、総合エネルギー統計は、我が国のエネルギー需給実態を把握・分析し、エネルギー政策の企画・立案に活用され、また、国際エネルギー機関（ＩＥＡ）への我が国のエネルギー需給に関する報告や、国連に報告する我が国の温室効果ガス排出量のうちエネルギー起源ＣＯ２排出量の算定に使われている。

上記の様な重要性に鑑み、質の高い総合エネルギー統計を維持するための点検、考察を常に行い、必要に応じて改善措置を講じる。また、総合エネルギー統計を期日どおりに作成し、作成した総合エネルギー統計から我が国のエネルギー需給動向を適切に把握・分析して、エネルギー政策の企画・立案に資するとともに我が国のエネルギー需給に関する国民の理解の向上を図る。この様な目的の達成に向け、本委託調査を実施する。

３．事業内容

（１）総合エネルギー統計関係の整備

①使用統計の確認

総合エネルギー統計作成で使用している各種統計について変更がないかどうか確認し、変更があった場合には資源エネルギー庁長官官房総務課戦略企画室（以下「担当者」という。）に報告し、対応について相談する。相談の際には考え得る対応案を提示する。

②総合エネルギー統計作成を補足するための調査・分析

ア　総合エネルギー統計補足調査（電気事業者の発電量内訳等調査）［統計法に基づく一般統計調査］の実施

２０１６年４月からの電気事業法の改正に伴う電力調査統計の改正により、総合エネルギー統計のエネルギー転換部門で使用する事業用発電の発電端電力量及び所内用電力量の統計データが得られなくなったことを補うため、「総合エネルギー統計補足調査（電気事業者の発電量内訳等調査）」（以下「総合エネルギー統計補足調査」という）を実施する。総合エネルギー統計補足調査の詳細については別紙１を参照する。調査の実施に当たって必要なデータや資料は担当者から提供を受ける。

イ　総合エネルギー統計補足調査の集計結果の分析

集計結果を用いて発電種別や発電主体の業態別等の発電端電力量と所内用電力量の傾向を分析し、総合エネルギー統計への反映方法を検討する。

③総合エネルギー統計の作成

各種のエネルギー関連統計等を用いて、「総合エネルギー統計の解説２０２３年度改訂版」（別紙２）を参考にして、「総合エネルギー統計作成マニュアル」（別紙３）に基づいて２０２４年度総合エネルギー統計を作成する。作成に使用する総合エネルギー統計作成システムは、担当者から貸与を受ける。作成に当たって必要な統計等のデータについては、上記イで集計・分析した統計データを使用するとともに各統計当局等で公表しているデータを収集して使用し、公表されていないデータは担当者が収集したものの提供を受ける。

スケジュールとしては、まず、２０２５年８月末までに公表又は担当者より提供されているデータを用いて、２０２４年度総合エネルギー統計の速報を１１月１３日までに作成する。更に、２０２６年1月２９日までに公表又は担当者より提供されているデータを用いて、確報を２０２６年2月２７日までに作成する。この際、速報及び確報の作成時に２０２４年度値が未公表及び担当者より提供してないものについては、原則、２０２３年度値を代入して作成する。

④総合エネルギー統計の品質管理

総合エネルギー統計の品質の確保・向上を図るため、担当者から貸与を受ける品質管理システムを用いてエラーチェックを行い、エラーが出た場合は必要に応じて改善措置を講じる。また、品質管理システム上はエラーにならなかった場合であってもエネルギー需給動向上動きがおかしいと思われる点が発見された場合には、その原因を追及し、対応策を検討し改善を図る。これらを踏まえ、品質管理の方法については、改善点を積極的に提案し、担当者との協議に基づき、システムの修正を施す。

スケジュールとしては、２０２４年度総合エネルギー統計速報については、２０２５年１１月１３日までに作成することから、エラーチェックを行った結果を１１月６日までに一度報告する。また、２０２４年度総合エネルギー統計確報については、２０２６年2月２７日までに作成することから、エラーチェックを行った結果を、２月２０日までに一度報告する。

⑤総合エネルギー統計作成マニュアル及び総合エネルギー統計の解説改訂版の更新

２０２４年度の調査で更新した総合エネルギー統計作成マニュアル及び総合エネルギー統計の解説改訂版案について、修正・改善すべき点が生じた場合には、内容を更新する。総合エネルギー統計作成マニュアル及び総合エネルギー統計の解説改訂版案については、担当者から貸与を受ける。

（２）２０２４年度のエネルギー需給動向の把握と分析

①エネルギー需給動向の把握

上記（１）③で作成した２０２４年度総合エネルギー統計をはじめとする各種エネルギー関連統計等を用いて、エネルギー源別の需給動向・時系列推移を示す図表及び一次エネルギー供給・転換・最終消費等の部門別動向を示す図表並びにエネルギー・フロー図等を作成し、２０２４年度のエネルギー需給動向とその特徴を示す。

②国際比較による日本のエネルギー需給構造の特徴の把握

一次エネルギー供給構成、最終エネルギー消費構成、ＣＯ２排出構成等を経年的に国際比較し、日本のエネルギー需給構造やエネルギー起源ＣＯ２排出構成の特徴を示す。

③エネルギー需給増減の要因分析

エネルギー源別・部門別にエネルギー需給増減の要因分析（原単位、寄与度、要因分解等）を行い、２０２４年度のエネルギー需給実態を明らかにする。また、一次エネルギー国内供給のＧＤＰ弾性値の変動要因についても分析を行い、ＧＤＰ変動とエネルギー需給変動の関係を明らかにする。

④エネルギー起源ＣＯ２排出量増減の要因分析

エネルギー起源ＣＯ２排出量増減の要因分析を行い、エネルギー需給動向との関係を整理し、２０２４年度のエネルギー起源ＣＯ２排出実態を明らかにする。

⑤エネルギー需給動向の取りまとめ

上記①～④の検討を踏まえ、資源エネルギー庁が公表する「２０２４年度エネルギー需給実績（速報)」及び「２０２４年度エネルギー需給実績（確報)」の概要版及び本文の原案を作成する。

以上、①～⑤については、２０２３年度のエネルギー需給動向の把握と分析に係る成果物を踏まえるものとし、当該成果物及びその分析方法の説明については、担当者より提供を受けるものとする。

（３）エネルギー源別標準発熱量に関する調査

① 標準発熱量２０２３年度改訂の追加改訂の検討

標準発熱量２０２３年度改訂一部のエネルギー源（廃プラスチック等）については必要に応じて標準発熱量の追加改訂及び取りまとめを実施する。

② エネルギー源別標準発熱量の改訂経緯書の更新

令和６年度総合エネルギー統計関係の整備及び分析に関する調査で改訂した「エネルギー源別標準発熱量・炭素排出係数改訂経緯書」について、最新の状況を反映して更新する。

（４）各種エネルギー関連統計の整備及び総合エネルギー統計の課題に関する調査

①総合エネルギー統計の短期的課題に関する調査

令和６年度総合エネルギー統計関係の整備及び分析に関する調査の調査結果等を踏まえ、総合エネルギー統計の短期的課題について担当者とも相談のうえ検討を行う。

②各種エネルギー関連統計の整備に関する調査

令和６年度総合エネルギー統計関係の整備及び分析に関する調査の調査結果等を踏まえ、総合エネルギー統計作成の観点から電力やガス等の需給に関する統計の改善について担当者とも相談のうえ検討を行う。

③総合エネルギー統計の中長期的課題に関する調査

令和６年度総合エネルギー統計関係の整備及び分析に関する調査の調査結果等を踏まえ、総合エネルギー統計の中長期的課題について担当者とも相談のうえ検討を行う。

（５）総合エネルギー統計検討会の開催

総合エネルギー統計検討会を担当者と相談のうえ２回程度開催（オンラインや書面による開催も含まれる）し、上記（３）及び（４）の調査の状況について報告し、委員の意見を聴取する。なお、委員の委嘱手続きや謝金・交通費の支払い等の事務手続きのほか、委員の日程調整、会場の手配・準備、資料の準備、委員への事前説明なども行う。

（６）外部からの問い合せ等への対応

①他省庁の検討会や外部からの問い合わせ等への対応

国連気候変動枠組条約（ＵＮＦＣＣＣ）に基づき、国連に報告する我が国の温室効果ガス排出量の算定方法については、環境省の温室効果ガス排出量算定方法検討会及びその分科会において検討している。温室効果ガス排出量のうち、総合エネルギー統計から算定しているエネルギー起源ＣＯ２排出量については、その算定方法について、同検討会のエネルギー・工業プロセス分科会において説明や意見を求められることがある。これに対応して、説明資料の作成や意見の提案を行う。

また、上記以外の他省庁の検討会や外部からの問い合わせに対して、担当者からの指示に基づき対応する。

②国際機関からの質問等への対応

ア　ＵＮＦＣＣＣ事務局及び国連専門審査委員等からの質問への対応

我が国がＵＮＦＣＣＣ事務局に報告した総合エネルギー統計から算定した数値に関して、ＵＮＦＣＣＣ事務局や国連専門審査委員から毎年７月から１０月頃に寄せられる質問に対して、担当者の指示に基づき調査、回答案の作成を行う。その他、ＩＥＡや国連統計委員会等からの質問についても担当者の指示に基づき調査、回答案の作成を行う。

イ　国際機関に報告した数値の透明性の向上

我が国がＩＥＡに報告した２０２３年度の我が国のエネルギー需給に関する数値（速報値）をＩＥＡがまとめて公表する「World Energy Statistics, 2025 Edition (OECD/IEA)」の電子版の数値と、２０２５年４月に我が国がＵＮＦＣＣＣ事務局に提出する２０２３年度実績（確報値）のＣＲＦ（共通報告様式）の数値とを比較し、相違する数値についてその相違の原因を調べ、数値の相違と原因について整理する。その上でインベントリ報告書に記載する案を作成する。

４．留意事項

・３．（１）② アの総合エネルギー統計補足調査を実施するに当たっては、委託契約書に記載の内容のほか、統計法上の義務（調査票情報等の適正な管理、調査票情報等の利用制限、守秘義務）や罰則が適用されることに留意し、調査票情報の使用、保管、処分等に当たって、紛失、漏えい等が生じないよう善良なる管理者の注意をもって調査票情報等の適正な管理を行う。別紙４に示す適正な管理の例を社内規定に照らして不足する部分がある場合には、適宜措置を講じる。

・３．（２）③と④の要因分析結果については、業界からのヒアリング等により裏付けを取る。また、ここで行った要因分析の方法についても報告書に記載する。
・３．（６）② イの「２０２５年４月に我が国がＵＮＦＣＣＣ事務局に提出する２０２３年度実績（確報値）のＣＲＦ（共通報告様式)」については、ＵＮＦＣＣＣのホームページからダウンロードして使用する。しかしながら委託契約締結時点で、ＵＮＦＣＣＣのホームページ上に掲載されていない場合は担当者から提供を受ける。
・３．（５）の総合エネルギー統計検討会の委員（１５名）については、令和６年度総合エネルギー統計検討会委員を引き継ぐこととし、人事異動等により委員の変更が必要な場合には、担当者が後任者を決定する。委員のみならず会場の借り上げ等、検討会の運用に関することは担当者と相談の上決定する。
・委託業務が完了した後でも納入物の引き渡し後１年間は、納入物に瑕疵があることが発見された場合には瑕疵を補修すること。
・本調査実施期間中、概ね月に一回程度状況報告を行う。

５．事業期間
委託契約締結日から令和８年３月３１日まで

６．納入物
①総合エネルギー統計補足調査の集計結果及び分析結果
総合エネルギー統計補足調査の集計結果及び分析結果を公表用にまとめたものを納入する。納入時期については、２０２５年１０月下旬を目途とし、詳細な時期については担当者と相談の上、決定する。

②２０２４年度総合エネルギー統計速報と確報
２０２４年度総合エネルギー統計速報と確報について、それぞれ１９９０－２０２４年度まで収めたファイルと統計データまでリンクされているファイルの２種類のファイルをＭｉｃｒｏｓｏｆｔ Ｅｘｃｅｌで作成し、速報は２０２５年１１月１３日まで、確報は完成版を２０２６年２月２７日までに納入する。ただし納入期限については状況によって変更する場合があるので、期日が近づいたら担当者の指示に従って納入すること。

③２０２４年度エネルギー需給実績の原案
上記３.（２）⑤の資源エネルギー庁が公表する「２０２４年度エネルギー需給実績（速報)」の原案についてはＭｉｃｒｏｓｏｆｔ Ｗｏｒｄで作成し２０２５年１１月１３日までに、「２０２４年度エネルギー需給実績（確報)」の概要版及び本文の原案についてもＭｉｃｒｏｓｏｆｔ Ｗｏｒｄで作成し、２０２６年３月３１日までに納入する。ただし納入期限については状況によって変更する場合があるので、期日が近づいたら担当者の指示に従って納入すること。

④インベントリ報告書に記載する案
上記３.（６）②の「インベントリ報告書に記載する案」についてはＭｉｃｒｏｓｏｆｔ Ｗｏｒｄで作成し、２０２６年２月１９日までに納入する。

⑤総合エネルギー統計作成マニュアル及び総合エネルギー統計の解説並びにエネルギー源別標準発熱量炭素排出係数の改訂経緯書の改訂版

上記３．（１）⑤及び３．（３）②により総合エネルギー統計作成マニュアル及び総合エネルギー統計の解説並びにエネルギー源別標準発熱量・炭素排出係数の改訂経緯書の内容を変更した場合には、変更した内容を更新した総合エネルギー統計作成マニュアル及び総合エネルギー統計の解説並びにエネルギー源別標準発熱量・炭素排出係数の改訂経緯書の改訂版を２０２６年3月３１日までに納入する。

⑥総合エネルギー統計作成システム

上記３．（１）①等の総合エネルギー統計の改善を踏まえて修正した総合エネルギー統計作成システムを２０２６年3月３１日までに納入する。

⑦品質管理システム

上記３．（１）④で資源エネルギー庁から貸与を受けた品質管理システムについて、必要に応じて担当者との協議に基づき修正した品質管理システムを２０２６年3月３１日までに納入する。

⑧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。

⑨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、プロパティを含む状態で納入すること。
- 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。
  - 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。
  - Ｅｘｃｅｌデータ等に非表示の行・列が存在しないか。
- 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こと。

⑩様式１～様式３について

---

[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。

- （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Ｗｏｒｄ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Ｅｘｃｅｌ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Ｅｘｃｅｌ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）

７．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。

８．納入場所

資源エネルギー庁長官官房総務課戦略企画室

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４を契約前に提出し、担当課室の同意を得ること。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。

なお、経済産業省との契約に違反する行為を求められた場合にこれを拒む権利を実効性をもって法的に保障されない者を情報取扱者としてはならない。

（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。

経済産業省が個別に承認した場合を除き、契約相手方に係る親会社、地域統括会社、ブランド・ライセンサー、フランチャイザー、コンサルタントその他の契約相手方に対して指導、監督、業務支援、助言、監査等を行う者を含む一切の契約相手方以外の者に対して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。

---

[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。

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。

１１．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。

１２．その他

（１）会議運営について

会議（検討会、研究会及び委員会を含む。）を運営する場合は、別紙５「会議運営について」に基づき、会議運営実績報告書を納入物とともに提出すること。

（様式４）

情報取扱者名簿及び情報管理体制図

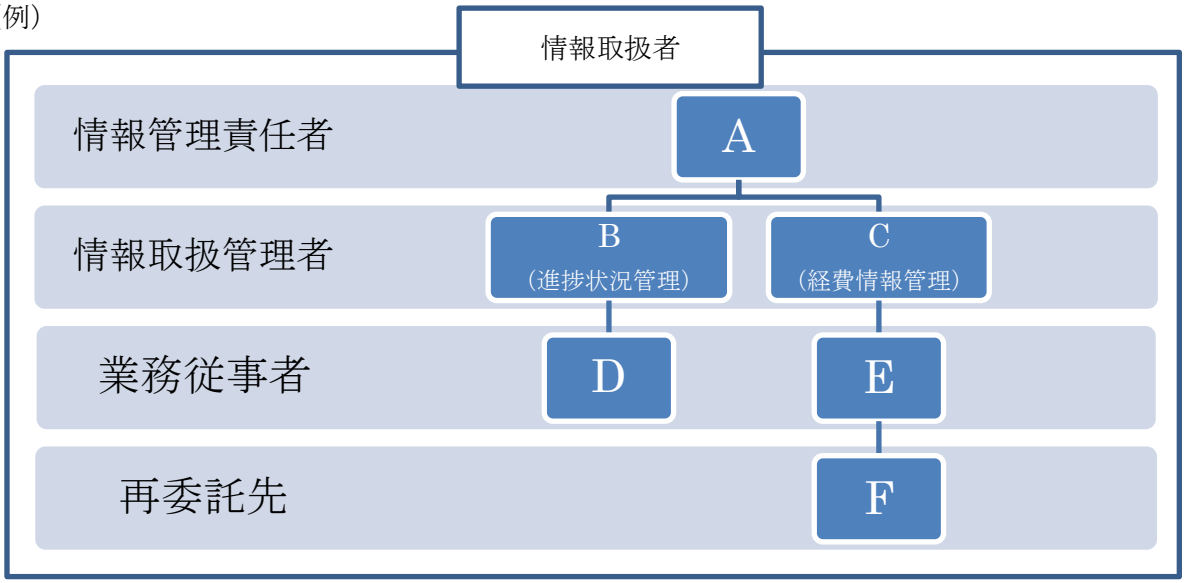
①情報取扱者名簿

		氏名	個人住所	生年月日	所属部署	役職	パスポート番号及び国籍（※４）
情報管理責任者（※１）	A						
情報取扱管理者（※２）	B						
	C						
業務従事者（※３）	D						
	E						
再委託先	F						

（※１）受託事業者としての情報取扱の全ての責任を有する者。必ず明記すること。
（※２）本事業の遂行にあたって主に保護すべき情報を取り扱う者ではないが、本事業の進捗状況などの管理を行うもので、保護すべき情報を取り扱う可能性のある者。
（※３）本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。
（※４）日本国籍を有する者及び法務大臣から永住の許可を受けた者（入管特例法の「特別永住者」を除く。）以外の者は、パスポート番号等及び国籍を記載。

②情報管理体制図

（例）



【情報管理体制図に記載すべき事項】
・本事業の遂行にあたって保護すべき情報を取り扱う全ての者。（再委託先も含む。）
・本事業の遂行のため最低限必要な範囲で情報取扱者を設定し記載すること。
・経済産業省との契約に違反する行為を求められた場合にこれを拒む権利を実効性をもって法的に保障されない者を記載してはならない。

（別記）

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および遵守状況の報告】

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。

3）受注者は、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。

【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】
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。

・サービス開始前および、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。

⑨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。

【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、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。

別紙

令和　　年　　月　　日

経済産業省○○○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５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。	
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。	
情報セキュリティに関する事項１５）	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。 （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。	

	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。 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。 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。 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。 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。 （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。 ・サービス開始前および、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じること。 ・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。 （９）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。	

情報セキュリティに関する事項 １６）	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。 （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。 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。 （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、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。	
情報セキュリティに関する事項 １７）	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。 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には、その指示に従う。	

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））。）