仕様書

１．件名

令和８年度地球温暖化・資源循環対策等調査事業（気候変動緩和の科学的根拠に関する国際動向調査）

２．事業の背景・目的

気候変動に関する政府間パネル（IPCC）は、気候変動に関する科学的知見を収集・評価し、自然科学的根拠（第 1 作業部会)、影響、適応及び脆弱性（第 2 作業部会)、緩和（第 3 作業部会）からなる評価報告書や統合報告書、さらに温室効果ガスの排出量及び吸収量の算出・報告手法に関わるガイドラインや特別報告書を作成する。これまで 6 回の評価報告書作成がなされ、国連気候変動枠組条約（UNFCCC）における取組指針の科学的根拠となったり、各国政府の科学的知見に基づく政策立案の参考になったりするなど、気候変動の国際交渉・国際動向の方向性、さらには気候変動に関連する産業・エネルギーの方向性に多大な影響を与えてきた。2023 年 3 月、IPCC の第 6 次評価プロセスにおいて公表された第 1 作業部会報告書、第 2 作業部会報告書、第 3 作業部会報告書をまとめた統合報告書が公表されたことを受け、第 6 次評価プロセスは終了。同年 7 月には、新たな IPCC 議長含むビューロメンバーが選出され、第 7 次評価プロセスが始動。2025 年 7 月には、第 7 次評価報告書の執筆者が発表され、同年 12 月には、3 つの作業部会の合同の第一回執筆者会合が開催され、第 7 次評価報告書の執筆活動が本格的に始まったところ。

経済産業省は、特に温暖化交渉自体と関連が強い気候変動緩和（第 3 作業部会）を担当し、政府意見の提出・取りまとめや、我が国執筆者間の議論・情報交換や連携を促進する役割を持つ。第３作業部会の担当として、IPCC に関連する国内外の情報の収集・分析・発信等を行う本調査事業は極めて重要となる。具体的には、主要な会合等に専門家等を派遣して情報の収集を行い、第 7 次評価プロセスにおいて公表が予定されている報告書の方向性の検討を行うこととする。また、IPCC 総会等に向けて日本政府が適切なコメントを作成・提出し、適切な対応・発信を行えるよう、適切な情報収集・分析・報告・助言を行う。さらに、AR7 の執筆に関与する日本人の確保・拡大も念頭に、公表された報告書の内容を国内に発信していく。

３．事業内容及び事業実施方法

（１）IPCC 関連会合への出席と専門家派遣を通した情報収集、分析

① IPCC 総会等への出席

令和 8 年度内に開催される IPCC 総会に参加する。総会への参加は、計 2 回程度（4 泊 5 日、開催地は欧州、専門家 1 名の参加を想定)。なお、派遣する専門家については事前に地球環境対策室の承認を得ること。

IPCC 総会出席に当たっては、以下の要領での調査・出席・文書の作成・報告、さらに、政府出席者に対する助言を行う。英語での国際会議に対応できるだけの言語能力・コミュニケーション能力を備える事はもちろん、各作業部会の内容に十分通じた者が業務にあたる必要がある。

・対処方針に関する助言

総会等への対処方針の検討に当たり、地球環境対策室の指示に従い、本仕様書（８）に記載する調査を行って、地球環境対策室に対し助言を行う。その際、必要に応じて、事前に総会等に用いられる資料を元に、当該会合アジェンダに関連する有識者等に対するヒアリング等を行い、その内容を地球環境対策室に報告・助言する。

・会合への出席と助言

総会等では、基本的に毎日会議の開始から終了まで出席し、地球環境対策室の代表者を補助するため、専門的知見を持つ人材を、1 名程度派遣することとなる。

ただし、会合が深夜に差し掛かる、会合が並行して進展する等の場合には、地球環境対策室の指示に従い、出席する会合を決定する。

加えて、出席した会合等の内容を地球環境対策室の代表者に報告・助言する。

・日々の報告資料の作成

地球環境対策室の指示に従い、会合期間中に、毎日 A4 サイズ、ワード等にて 1-3 枚の日々の交渉動向の概要について報告資料を作成する。報告のタイミングは地球環境対策室と調整を行う。

その際、少なくとも、会合の議長（共同議長・副議長）や執行部、中国、インド、英国、ドイツ、スイス、フランス、オランダ、ノルウェー、豪州、カナダ、NZ、ロシア、ブラジル、サウジアラビア、EU 等の主要国の交渉ポジションに係る発言の趣旨を記載することとする。必要に応じて、他事務局（第 1 作業部会、第 2 作業部会担当等）その他専門家等と業務分担を行うこととする。

・会合を総括する概要資料の作成

地球環境対策室の指示に従い、会合全体の報告資料を、遅くとも会議終了後 5 日以内を目安に作成する。ボリュームや記載内容については、地球環境対策室と協議の上決定する。

※ なお、旅費を負担すること。また航空券は、ディスカウントエコノミーを想定する。

※ 上記日程、開催場所については現時点での想定であり、変更の可能性がある。派遣日程については、基本的には政府代表団と同日程で行動することとする。

②IPCC 関連会合への専門家派遣

以下の要領で専門家派遣を行う。

・第 3 作業部会報告書（WG3）の第 2、3 回執筆者会合：第 2 回会合は 2026 年 5 月に開催予定（4 泊 5 日、サウジアラビアで開催、執筆者 9 名、Chapter Scientist1 名の参加を想定)。 第 3 回会合は 2027 年 2 月頃に開催予定（4 泊 5 日、欧州で開催、執筆者 9 名、Chapter Scientist1 名の参加を想定)。
・SLCF 方法論報告書の第 4 回執筆者会合： 時期未定（4 泊 5 日、欧州で開催、執筆者 1 名の参加を想定)。
・CDR・CCUS 方法論報告書の第 3 回執筆者会合： 時期未定（4 泊 5 日、欧州で開催、執筆者 2 名の参加を想定)。
・その他必要に応じて、IPCC 関連会合が開催される場合には、当該会合への専門家派遣

なお、②の会議への専門家の派遣に際して次の業務を行うこと。

・派遣される当該分野の専門家複数名を地球環境対策室に提示し、了解を得るとともに、当該専門家が会議に出席するための日程等の調整を行うこと。
・派遣される専門家と調整し、航空機、ホテルの予約、必要に応じてビザの取得等派遣にかかる所要の手続きを講じること。特に、派遣される専門家が外国から参加する場合や、時差が大きい国での会議が午前から開始される場合の到着日などについては、十分調整を行うこと。また、ディスカウントチケットやパッケージツアーを活用するなど、航空機、ホテルの予約は効率的・経済的に行うとともに、会議日程や内容も考慮しつつ、会議が延長された場合に滞在を延長するといった柔軟な対応もできるよう考慮すること。なお、旅費を負担すること。
・会議終了後すみやかに、派遣された専門家等から会議資料及び会議概要をまとめた報告書（5 頁程度）の提出を求め、地球環境対策室にメールにて送付すること。なお、IPCC 事務局により、出席者以外には非公開とする明確な指示があるものについては、部外秘とし、その旨、経済産業省に報告すること。

（２）IPCC 第 7 次評価サイクル各種報告書のドラフトレビュー支援

報告書ドラフトの政府レビューが行われる際に、専門的知見からの助言、専門家へのヒアリング、レビューコメント案の取りまとめ等の支援を行う。令和 8 年度は、以下の報告書ドラフトの政府レビューが想定される。

第 7 次評価報告書 第 1,2,3 作業部会報告　第一次ドラフト（2026 年後半を想定）
・都市に関する特別報告書　第二次ドラフト（2026 年 5 月―7 月）
・都市に関する特別報告書　最終ドラフト（2026 年 12 月―2027 年 2 月）
・SLCF 方法論報告書　第二次ドラフト　（2026 年後半）
・SLCF 方法論報告書　最終ドラフト　（2027 年前半）
・CDR・CCUS 方法論報告書　第一次ドラフト（2026 年後半）

（３）IPCC 第 3 作業部会に関する幹事会の主催

IPCC 第 3 作業部会の日本人執筆者及び有識者（計 11 名程度）、関係省庁担当者（10 名程度）を対象に、IPCC 報告書に関する情報の共有化・意見交換等を行う。開催時期は地球環境対策室と相談し、2 回程度ハイブリッド形式で実施（開催地は音響設備、映像投影設備を備え、30 名程度収容できる都内近郊の会議室を想定）する。

また、必要に応じ、地球環境対策室と相談の上、SLCF 方法論報告書、CDR・CCUS 方法論報告書、第 1/第 2 作業部会の日本人執筆者や Chapter Scientist、Contributing Author を併せて 2-4 名程度（都内近郊からの参加を想定）の招聘を決定すること。

なお、開催に当たっては、日程調整、事務局による議事概要の作成（委員の確認前の第一次案については会議終了後一週間以内の地球環境対策室への提供を目安とし、委員確認後のセット版については報告書に盛り込むこと。）を行うこと。執筆者及び有識者には交通費・謝金を支払うこと。交通費については、執筆者及び有識者の 4 分の 1 程度は地方から参加することを想定。必要に応じ、第 1、第 2 作業部会事務局と適宜調整すること。

（４）IPCC 国内連絡会の開催補助

今年度、第 3 作業部会が幹事を務める IPCC 国内連絡会（1 回程度の実施、開催地は都内近郊を想定、ハイブリッド形式での開催を想定）の開催に当たって、IPCC 第 3 作業部会の日本人執筆者及び有識者（計 13 名程度）や他 WG 支援事務局（3 名程度）と日程・議題の調整を行う。また、地球環境対策室と相談の上、国内連絡会には事務局から数名出席すること。経済産業省が推薦した IPCC 第 3 作業部会の執筆者及び有識者には交通費・謝金を支払うこと。なお、交通費については、IPCC 第 3 作業部会の執筆者及び有識者の 5 名程度は地方から、5 名程度は都内近郊から参加することを想定。

（５）アウトリーチ活動の準備

必要に応じ、AR7 の緩和に係る重要なテーマについて、一般の理解を深めるために、最新の知見及び今後の方向性に関して報告・議論を行うシンポジウムを、地球環境対策室と適宜調整の上、ハイブリッド形式で開催すること。その際、開催場所は、5 名程度が登壇できるスペースがあり、50 名程度の参加者の座れる座席のある都内近郊のホールを想定。当日の受付、照明、音響、スクリーン等の準備運営等を行う。講師は 3 名程度（うち、海外（マレーシアを想定）から 1 名程度招聘）をそれぞれ想定。なお、講師には交通費・謝金を支払うこと。他省庁と共催の上、シンポジウムを開催する場合には、他 WG 支援事務局と連携し、会議開催に向けた調整を行う。

（６）IPCC 第 3 作業部会の日本人執筆者と産業界の有識者との非公式意見交換会

必要に応じ、日本の産業界（電力・鉄鋼・セメント・自動車・建築など）からの最新の知見を踏まえ、AR7 の各種報告書に含めるべき事項を検討するために、日本の重視する緩和に係るテーマ（イノベーションなど）について、第 3 作業部会の日本人執筆者及び有識者と日本の産業界との非公式の意見交換会を、地球環境対策室と適宜調整の上開催すること。その際、開催地は東京（経済産業省会議室）、規模は 19 名程度（AR7 の関係章の日本人執筆者 11 名程度、日本の産業界から 8 名程度）を想定。

（７）AR7 に向けた検討の補助

AR7 における我が国の対応について、AR7 の各種報告書に含めるべき事項の検討をはじめ、専門的見地から地球環境対策室に助言を行う。

（８）総会・関連会合に関する調査と報告

総会・関連会合支援のため、地球環境対策室の指示に従い、関連するテーマについて適切な資料、情報を収集、分析・整理した後、必要な参考文献を添えて地球環境対策室が指示する期日（おおむね発注から 1－3 週間）までに報告すること。

（９）AR7 において選定された Coordinating Lead Author（CLA）の執筆活動にかかる支援

AR7 WG3 報告書 15 章 Chapter Scientist（CS）を 1 名採用し、15 章の Coordinating Lead Author（CLA）の執筆補助を行う。CS の活動期間は本事業の終了日までとする。採用された CS にはその活動条件に応じて月額最高 20 万円程度の報酬と通勤交通費（月額 5 万円を上限とする）および必要な経費を支

給する。

（１０）その他

・得られた情報については、要点を整理・分析し、地球環境対策室へ速やかに報告すること。なお、上記（（１）①IPCC 総会等への出席）に上げた情報収集については、めまぐるしく状況の変化する交渉現場での調査であることに鑑み、必要に応じて地球環境対策室の指示に基づき、よりタイムリーな口頭若しくは資料配付による報告をすること。

・国内・海外を含む出張・会議等について、対面での開催が困難と考えられる事項については、経済産業省イノベーション・環境局 GX グループ地球環境対策室と相談の上、電話でのヒアリングやオンライン会議を含む、その業務を全うする上で必要な措置を検討し、流動的に対応してよいものとする。

４．報告書の作成

上記の内容を踏まえ、地球環境対策室の指示に従い報告書を作成する。

５．事業期間

委託契約締結日から、令和 9 年 3 月 31 日まで。

６．成果物

（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、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。

[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。

- 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。

（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 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

経済産業省イノベーション・環境局 GX グループ地球環境対策室

9．情報管理体制

[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。

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．業務従事者の経歴
業務従事者の経歴（氏名、所属、役職、学歴、職歴、業務経験、研修実績その他の経歴、専門的知識その他の知見、母語及び外国語能力、国籍等がわかる資料）を提出すること。
※経歴提出のない業務従事者の人件費は計上不可。

１１．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。

１２．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

（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。

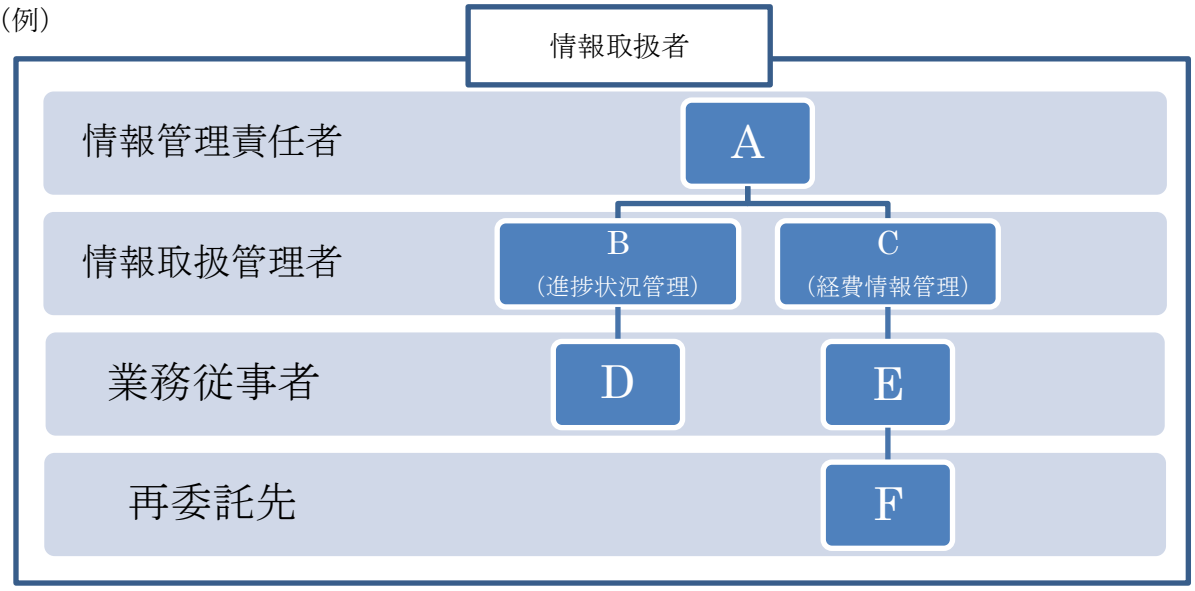
（※３）本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※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。

（※５）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。

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。

（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・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。

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、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、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。 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、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。	

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））。）