仕様書

１．件名

令和7年度地球温暖化対策技術・エネルギー等分析・評価国際連携事業費（地球温暖化対策技術の分析・評価に関する国際連携事業）

２．目的

地球温暖化は、地球全体の環境に深刻な影響を及ぼすものであり、2023年年11月の第28回国連気候変動枠組条約締約国会議（COP28）で実施されたパリ協定の世界全体の実施状況を確認する「グローバルストックテイク（GST）」の決定においてネットゼロという共通の目標に向けて、あらゆるエネルギーや脱炭素技術の活用が言及され、温暖化対策の必要性が強く求められている。しかし、地球温暖化は、世界のあらゆる国、様々な部門に影響を与える一方で、地球温暖化が与える影響は均一ではなく、影響先も多様である。また、各国において取り得る緩和策、緩和費用にも差異が大きい。各国・各地域・各産業の状況を考慮した温暖化対策・政策に関するモデル開発等及びそのモデルに基づく分析・評価を行い、真に有効な気候変動政策を政策立案に資することが重要と考えられる。

GSTの内容を踏まえ、一部の国は国別削減目標（NDC）を更新しており、各国の次期NDCを踏まえ、今後もパリ協定の目標に向けた各国の気候変動対策の実施の加速化などに関する議論が深まると予想される。一方で、米国新政権による米国のパリ協定離脱等、気候変動を巡る世界情勢は刻一刻と変化している。

そのような中で、各国・各地域・各産業において、気候変動政策の立案に貢献し得る様々な評価・分析を行う重要性は一層高まってきている。さらに、気候変動に関する政府間パネル（ＩＰＣＣ）においては、２０２３年に第７次プロセス（AR７）が始動し、気候変動に関する最新の科学的知見の提供が求められている。

本事業では、最新の科学的知見や国際交渉の動向も踏まえながら、海外研究機関とも連携・協力しつつ、温暖化対策（緩和策及び適応策等）やグリーンファイナンス、各国・各産業の気候変動対策について総合的な分析・評価（具体的には３．事業内容に記載）を行い、我が国の気候変動政策の立案や、ＩＰＣＣ、ＣＯＰといった国際的な議論に貢献することを目的としている。これらにより、積極的に地球温暖化対策を行うことが、産業構造・社会構造をクリーンエネルギー中心へ転換する「グリーントランスフォメーション（ＧＸ）」を目指す将来枠組み・我が国の国際戦略立案を進めていく。

３．事業内容

本事業では、以下の項目を実施する。

（１）コンピュータモデルを用いた温暖化対策・政策の総合的な分析・評価

以下（１－１）～（１－４）までの要件を満たす世界エネルギー・温暖化対策技術評価モデル、経済モデル、及び、非ＣＯ２温室効果ガス評価モデルによって、温暖化対策・政策の総合的な分析・評価を行う。また必要に応じて、分析結果を踏まえたわが国の政策立案に向けた助言を行う。

（１－１）国際的に策定・分析が行われてきている共有社会経済パス（Shared Socioeconomic Pathways: SSP）や今後の新シナリオの動向を踏まえた社会経済シナリオを想定し、技術評価モデルで２１００年までの温暖化対策の分析、評価を行う。なお、導入が高まる変動制再生可能エネルギーを適切に評価できるモデル化を行いつつ、エネルギー供給サイドの最新動向の反映に加え、IPCC 1.5℃特別報告書や第6次評価報告書で引用された低エネルギー需要（LED）シナリオに準ずるシナリオについても検討を行い、必要に応じてモデル開発、拡張等を行った上で、分析、評価を行う。
更に、必要に応じて下記（６）項でヒアリング等を行って得た情報を基に評価モデルの更新・拡張も行った上で、分析、評価を行う。
加えて、SSP等のシナリオに関する既往の資料等に関する分析、評価研究について調査、整理を行い、本分析、評価との比較を行う。

（１－２）①２０２０年以降（２０３０年頃）の地球温暖化対策に関する将来枠組み・目標に関して、各国提出の排出削減目標、カーボンバジェットについて、複数の国際衡平性の指標（ＣＯ２排出原単位、限界削減費用均等化、ＧＤＰ比費用均等化、政策強度、製品炭素含有量等）における位置づけや気候変動によるマクロ経済・貿易への影響について、各種統計データおよびコンピュータモデルを用いて分析、評価を行う。その上で、２０５０年カーボンニュートラルに至る過程の分析を行い、必要な投資額等の推計を行う。
②欧米等を中心に議論されている国境調整措置やカーボンクラブなどの貿易と気候変動対策を絡めた経済分析についても実施することとする。
③各国の長期目標・中期目標との関係性についても分析、評価を行う。特に、パリ協定で位置づけられた２℃目標、1.5℃目標、各国の提出したNDCに関しては、同目標達成のための緩和策を評価するとともに、他の持続可能な発展目標とのシナジー効果、トレードオフ効果について分析、評価を行うほか、長期のゼロエミッション達成に向けた対策の方向性の検討とその限界について分析、評価を行う。また、国際機関、研究機関、市民団体等による排出削減目標の評価について、その方法論等を調査し、評価を行う。

（１－３）下記の（２）項を踏まえつつ、上記（１－１）項の社会経済シナリオの下で、気候変動緩和とSDGs等とのコベネフィットを考慮したシナジー効果、トレードオフ効果について、コンピュータモデルを用いた分析、評価を行う。

（１－４）所得階層による温暖化対策の費用負担の衡平性と効率性とのトレードオフについて、コンピュータモデルを用いた分析、評価を行い、今後の大幅な排出削減にあたっての対策の在り方について検討を行う。

※①エネルギー・温暖化対策技術評価モデルの要件
【評価対象期間】
・２１００年頃まで
【対象地域】
・世界全体を対象
・特に、日本、米国、ＥＵ、英国、中国、インド、ブラジル、ロシアなどの主要国は個別に評価
【対象部門】
・少なくともエネルギー起源のＣＯ２排出量全体を評価できるとともに、少なくとも、電力、鉄鋼、セメント部門を個別に分析。ＣＣＵＳについても明示的に分析。

※②経済モデルの要件
【評価対象期間】
・２１００年頃まで
【対象地域】
・世界全体を対象
・特に、日本、米国、ＥＵ、英国、中国、インド、ブラジル、ロシアなどの主要国は個別に評価
【対象部門】
・少なくともエネルギー起源のＣＯ２排出量及びＧＤＰへの影響を評価できるとともに、産業構造を整合的に評価でき、かつ、部門別の経済影響評価（部門別の付加価値変化等）が可能であること。なお、部門については、少なくとも、電力、鉄鋼、セメント、化学、自動車、機械、運輸、サービス部門を個別に分析できること。ＣＣＵＳについても明示的に分析。

※③非ＣＯ２温室効果ガス評価モデルの要件
【評価対象期間】

・２１００年頃まで
【対象地域】
・世界全体を対象
・特に、日本、米国、ＥＵ、英国、中国、インド、ブラジル、ロシアなどの主要国は個別に評価
【対象温室効果ガス種】
・少なくともメタン、一酸化二窒素、代替フロン等３ガス、二酸化硫黄、ブラックカーボンについては評価が可能であること
なお、必ずしも①～③において、３種類のモデルを有する必要はなく、以上のモデル要件を一元的に扱うことができるモデルを有する場合は、１種類のモデルもしくは２種類のモデルを用いて、上記要求の分析・評価を実施してもよい。

（２）気候変動対応のリスクマネージメントについての検討及び温暖化緩和策と適応策の経済影響・経済効果、雇用への影響、気候変動対策におけるイノベーションの可能性に関する分析
気候変動対応の影響・適応の評価について、国際的な最新の学術的な評価についてとりまとめを行い、その含意について検討を行う。加えて、気候変動対応に付随するリスクについて、気候変動対応に大きな影響を及ぼし得る要因を特定し、その影響について定量的な分析を行う。その上で、それらの分析も踏まえつつ、気候変動対応のリスクマネージメントについて、考え方の整理を行うと共に、緩和策と適応策の経済影響・経済効果に関する分析を行う。また、気候変動対策におけるイノベーションの可能性を調査・検討するとともに、イノベーションの気候変動リスクマネージメント戦略における位置づけについても検討を行う。

（３）効果が期待できる温暖化対策の具体的なシステム提案とその分析
必要に応じて経済産業省イノベーション環境局地球環境対策室と相談しつつ、費用対効果の高い具体的な温暖化対策のシステム提案を行う。また、民生、運輸部門を中心とした現在の対策や削減目標をベースとした積み上げアプローチによるモデル分析により、その排出削減効果とシステムの費用およびその経済影響・効果について定量的な評価を行う。

（４）「グリーン成長」、温暖化対策技術の国際展開に関する分析
以下①～⑤の項目を含めて、「グリーン成長」の見通しについて考え方の整理およびデータに基づく分析を行う。
①エネルギー生産性の国際比較とその要因、それに伴う各国、世界のグリーン成長との関係についての分析
②消費ベースＣＯ２に関する評価についても、最新動向の調査等

③国内外の再生可能エネルギー導入とその費用負担の状況などについて調査を行い、グリーン成長との関連についての整理

④欧州等における電力自由化の下でのＣＯ２排出削減対策・政策を調査、整理し、日本の電力システム改革の下でのＣＯ２排出削減対策・政策の課題についての整理

⑤（ⅰ）グリーンファイナンスを含めた気候変動問題に対する金融部門の取り組みを調査（ⅱ）その際、石炭火力発電等のダイベストメントや、タクソノミーの議論や関連分析について調査（ⅲ）また、金融部門を明示的に考慮したモデル評価の課題を整理し、低炭素技術の国際展開に伴う、ファイナンシングを含めた金銭の流れを分析・評価

（５）気候変動問題に関する主要論文の調査、整理

（１）～（４）項の分析、評価の参考とするため、エネルギーシステム、気候変動問題等に関する主要な論文・文献について調査を行い、それをリスト化するとともに、海外論文の和訳概要作成を行う（電子媒体により作成、最大８００ｗｏｒｄ×５ページを２０件程度）。

また、必要に応じ、国内有識者への論考作成依頼を行う（２回程度、それぞれ４００字詰め原稿８０枚程度を想定）。

（６）国内における学会等での気候変動問題の研究動向調査及び研究成果の発信、有識者へのヒアリングによる情報収集等

気候変動問題の研究動向を調査するため、主要な国内における学会・ワークショップ等（東京若しくは地方都市等、２回程度開催を想定）に出席し、（１）～（４）項に関する学会発表及び論文投稿等による研究成果の発信も行う。

また、（１）の分析に資するため、セクター別主要企業・団体・学術専門家へのヒアリングやセミナー・講演会参加により情報収集を行う（ヒアリング、セミナー、講演参加合わせて１５回程度、２名程度ずつ参加、東京若しくは地方都市で実施を想定）。

（７）気候変動に関する国際会議への参加等による各国動向調査・国際的な情報発信

（１）～（４）項の分析、評価の参考にした上で、経済産業省イノベーション環境局地球環境対策室とも相談しつつ、（１）～（４）項の成果を国際的に発信し、主要関係者からの情報収集を行う。外部専門家を招聘し、発信を行う場合は、交通費・謝金を支払うこと。具体的には、以下の要領で発信を行う。

・IEW(International Energy Workshop)：3泊4日を想定、日本（奈良）を想定、2名の派遣を想定。

・GMMI(Green Macroeconomic Modeling Initiative：3泊4日を想定、米国（ワシントンD.C.）を想定、2名の派遣を想定。

（８）国際モデル比較プロジェクトへの参画、海外研究機関等との研究協力

（８－１）欧州主要研究機関とエネルギー需要部門に関する研究協力を行うとともに、欧州主要研究機関への訪問（ウィーン）により、欧州主要研究機関の気候変動に関連する研究成果の情報収集を行う。訪問は１回、主席研究員１名、研究員１名程度参加を想定。

（８－２）米国の研究機関（例えば米国未来資源研究所（ＲＦＦ））と地球温暖化・エネルギー政策分析に関する研究協力、及び特に２０２０年以降の目標として米国を始めとする主要国の掲げる国別貢献ＮＤＣを評価するための関連政策動向分析を行うとともに、当該研究機関（ワシントンＤＣ）への訪問・意見交換により、密に情報収集を行う。訪問は１回、主席研究員１名、研究員１名程度参加を想定。

（８－３）欧州における気候変動緩和シナリオに関する国際モデル分析比較関連の会合への参加、会議出席を行う。欧州の国際モデル分析比較会合については、欧州主要都市等にて１回程度開催が予定（それぞれ主席研究員１名、研究員１名程度を想定）。

（８―４）エネルギー需要サイドの技術革新に関する国際モデル分析比較会合への参加、会議出席を行う。エネルギー需要サイドの技術革新に関する国際モデル分析比較会合については、欧州主要都市等にて１回程度開催が予定（それぞれ主席研究員１名、研究員１名程度を想定）

（８－５）年度内１回予定されている、気候変動緩和シナリオ分析の国際連携のためのコンソーシアムIntegrated Assessment Modeling Consortium （ＩＡＭＣ）会合への参加、会議出席を行う（ブラジル開催を想定。主席研究員１名、研究員１名程度を想定）。

（８－６）国際エネルギー機関（ＩＥＡ）と長期排出削減対策に関する研究協力を行う。研究協力のため、当該研究機関（パリ）への訪問により密な意見交換を行う。訪問は１回、主席研究員１名、研究員１名程度参加を想定。

（９）委員会の設置、運営

本事業を的確・効率的に推進するために、アドバイスを行う１０名前後の外部専門家からなる委員会を設置する（３回程度実施予定）。また、分野が広範に及ぶことから、委員会の下に、１０名程度の外部専門家からなる５つ程度のワーキンググループを設置する（合計２０回程度実施予定）。外部専門家には、交通費・謝金を支払うこと。この委員会、ワーキンググループの運営を行う。

（１０）シンポジウム・ワークショップの開催

研究成果の発信及び地球温暖化対策技術の分析・評価に関する国際連携を促進するため、国際シンポジウムを開催する。開催場所は、２０名程度が登壇できるスペースがあり、３００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。令和７年度内に２日間の日程で開催する（日程については、経済産業省イノベーション環境局地球環境対策室と相談の上、決定すること）。その際、国内外の主要関係者８名程度（国内４名程度、海外４名程度を想定）を招聘する。なお、交通費・謝金を支払うこと。国際シンポジウムは、２日間のうち１日は一般公開とし、３００名程度の聴衆を受け入れる。その際、同時通訳（３名程度を想定）をつけること。１日は関係者によるワークショップを行う。

（１１）報告書作成、報告会開催

報告書を、電子媒体（透明テキストファイル付きＰＤＦファイル（ＣＤ－ＲOM等の記録媒体に保存））で２式作成し、経済産業省イノベーション環境局地球環境対策室まで提出する。

また、報告書（電子媒体）については、（９）にて設置した委員会の委員（１０名程度）及びワーキンググループの委員（４０名程度）に提供する。

必要に応じて、経済産業省イノベーション環境局地球環境対策室に本事業内容の検討結果等の報告を適宜行う（年度内最大１０回程度）。

（１２）その他

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

上記の項目３．の内容を取りまとめの上、経済産業省イノベーション環境局地球環境対策室の指示に従い、報告書を作成する。

５．調査実施期間

委託契約締結日から令和８年３月３１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。

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

７．納入場所

経済産業省イノベーション環境局地球環境対策室

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。

９．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。

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

（様式１）

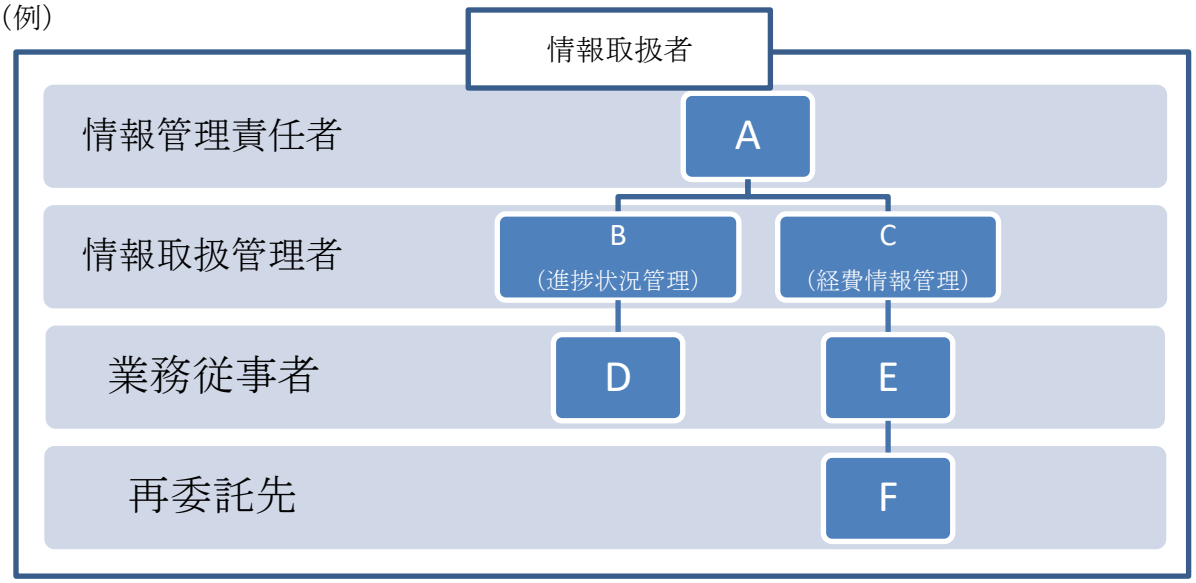
情報取扱者名簿及び情報管理体制図

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】
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））。）