

仕様書

1. 件名

令和8年度「学びと社会の在り方改革推進事業」(「未来の教室」実証事業)

2. 事業の背景・目的

経済産業省では、2024年1月、産業界と教育現場の連携・協働の好事例の創出と普及を促進する環境の実現を目指し、教育現場における外部資源の活用を促進する方策を検討するため、「イノベーション創出のための学びと社会連携推進に関する研究会」(※1)を開催し、同年7月、報告書を取りまとめた。2026年1月には「産業界と教育現場の連携を推進するコーディネーターに関する研究会」(※2)を開催し、同研究会の議論内容をまとめた有識者提言を得るに至った。

一方、よりマクロな我が国の人材環境に目を向ければ、2040年にかけて、ホワイトカラー人材が余剰となることが見込まれる中で、理工系・デジタル系人材やエッセンシャルワーカーの不足が懸念されている(※3)。現状では、高校生の約半数が普通科文系、大学生の約半数が人文・社会科学系に在籍しており、将来の産業構造の変化を踏まえた人材需要との間にミスマッチが生じている。こうした状況を踏まえれば、産業界と教育現場が協働し、産業構造の変化を見据えた人材を戦略的に育成していくことの重要性はより一層高まっている。

本事業は、産業界の知見や新たな学習ツールを教育現場に取り入れることで、学びのアップデートを目指してきた「未来の教室」プロジェクトにおける議論や取組を発展的に継承しつつ、今後顕在化が見込まれる人材のミスマッチをできるだけ解決できるよう、将来の人材育成に意欲を有する産業界と、学習内容の充実を図ろうとする教育現場とを実践的につなぐ「コーディネート機能」に着目しながら、その有用性の実証、効果の検証及び効果的な地域の座組の構築を目的とするものである。

(※1) https://www.meti.go.jp/shingikai/mono_info_service/innovation_creation/index.html

(※2) https://www.meti.go.jp/shingikai/mono_info_service/collab_coordinator/index.html

(※3) https://www.meti.go.jp/shingikai/sankoshin/shin_kijiku/030.html

3. 事業内容及び事業実施方法

(1) 事業全体の運営・管理

- 産業界と教育現場の効果的な連携を推進するため、産業界・教育現場双方にプラス効果をもたらす先進モデルを地域ごとに創出する実証を行う。
- 事業実施に当たっては、事業全体の方向性を検討・設定した上で、事業の運営・管理に必要な人員を配置して実施するものとし、複数名の本事業専属の人員配置も含め、経済産業省と調整の上、指示に従い進める。
- 事業全体の進捗を管理するため、週に1回程度、経済産業省との打合せの機会を設ける。打合せ開始前に打合せ資料を送付するとともに、打合せ終了後、3営業日以内に議論した内容について議事録を提出すること。

(2) 実証事業者の公募・採択

- 実証事業の実施に当たっては、①北海道、②東北（青森、岩手、宮城、秋田、山形、福島）、③関東（茨城、栃木、群馬、埼玉、千葉、東京、神奈川、静岡、山梨、長野、新潟）、④東海（岐阜、愛知、三重）、⑤北陸（富山、石川、福井）、⑥近畿（滋賀、京都、大阪、兵庫、奈良、和歌山）、⑦中国（鳥取、島根、岡山、広島、山口）、⑧四国（徳島、香川、愛媛、高知）、⑨九州（福岡、佐賀、長崎、熊本、大分、宮崎、鹿児島）、⑩沖縄（以下、「地域ブロック」という。）を実証地域の単位とする。
- 各地域ブロックにおいて、各経済産業局、企業と自治体（教育委員会を含む。以下、同じ）・学校（小学校、中学校、義務教育学校、高等学校、中等教育学校、特別支援学校、大学、高等専門学校及び専修学校）が連携しながら、コーディネート機能の構築やマッチングを行うプロジェクト（以下、「プロジェクト」という。）の組成等を通じて、産業界と教育現場における広域的かつ持続的な協働の仕組みや組織（以下、「エコシステム」という。）の実装等に向けた事業を行う者（以下、「実証事業者」という。）を公募する。
- 公募に当たっては、以下の点に留意すること。
 - 公募要領について、経済産業省と協議の上、作成すること。
 - 公募を広く周知するための総合的な対策を講じること。
 - 各地域ブロックにつき1者、すなわち計10者の実証事業者を採択すること。ただし、同一の事業者が、2以上の地域ブロックにおいて実証事業者となることは妨げない。
 - 1事業者あたりの契約金額については、事業内容や規模に応じて変動するものの、過去の実績から、規模に応じて1,500万円～2,500万円（合計2億1千万円程度）の実証事業が可能な予算を確保すること。
 - プロジェクトの組成に当たっては、個別又は単発の取組に限らず、広域的又は持続的な取組も対象にすること。
 - 実証事業者は、企業と自治体・学校をマッチングさせるコーディネート業務又はまちづくりを含めた地域貢献を行っている事業者や、それに類する事業を実施する資質を有する事業者とし、各経済産業局と連携の上、エコシステム又は各プロジェクトへ参画を希望する企業、自治体及び学校（以下、「参画主体」という。）に対して、相互の連携に向けた組織づくり等を伴走支援しつつ効果的にマネジメントすること。
 - 実証事業者は、実証期間終了までに成果報告書を事務局に提出すること。
 - 各地域ブロックにおけるエコシステム及び各プロジェクトは、これまでの「未来の教室」プロジェクトの実証成果、「イノベーション創出のための学びと社会連携推進に関する事例集」（※1）、「産業界と教育現場の連携を推進するコーディネーターに関する研究会 提言」（※2）に掲載の事例や「新しい資本主義のグランドデザイン及び実行計画 2025年改訂版」内の産業人材育成プラン（※3）を参考にしつつ、以下のようなヒト・モノ・カネの3つの分野に係る取組を実施する能力を有する実証事業者を採択すること。プロジェクトにおける取組内容は、特に、企業の実課題を活用した課題解決型学習（PBL）や産業界で必要とされるスキルを踏まえた連携の促進など、本仕様書に記載の内容に留まらず、ヒト・モノ・カネの各分野にまたがり、継続性が見える案件等を含め、創意工夫を以って組成することを期待する。
 - ◇ ヒトの連携：情報、プログラミング、英語や金融などの専門的な知識を持つ企業の人材

を教育現場へ派遣、企業の人材と教員等が互いの職場に出向やインターンシップ等を行うことで知見を共有し、異なる職場文化を経験すること、単発の派遣に留まらない実務家教員・博士人材等の採用・活用促進等

- ◇ モノの連携：出前授業や体験プログラムの共同開発、産業界と連携した成長分野への文理融合・学部再編等の推進、専門高校の機能強化・高度化や普通科高校の特色化・魅力化等に資する実践的な教育運営モデルの開発といったソフト面の取組、物品や施設（空き教室・空きオフィス等）の共有といったハード面の取組等
- ◇ カネの連携：GCF（ガバメントクラウドファンディング）、個人版・企業版ふるさと納税、基金等を活用した寄附・拠出、SIB（ソーシャル・インパクト・ボンド）、ネーミングライツなど、教育現場が外部資金を調達する取組、企業が教育機関へ寄附・拠出しやすい環境の整備に資する取組等
- 文部科学省の学習指導要領の改訂及び「高校教育改革に関する基本方針（グランドデザイン）～2040年に向けた「N・E・X・T.（ネクスト）ハイスクール構想」～」（※4）などを踏まえた産業界と教育現場の連携に関する取組を想定していること。
- 事業計画については、2040年に向けた産業構造・就業構造推計の結果や各地域で開催される地域人材育成構想会議や、今後組成される地域連携推進プラットフォームでの議論など、地域の人材需給や産業界等のニーズ等を十分踏まえ、その地域に今後必要となる人材の育成を推進する具体的なものとなっていること。
- プロジェクトは、地域ブロックそれぞれにおいて、各実証事業者が複数組成することが想定される。同一のプロジェクト内容、同一の企業、同一の自治体・学校である場合、事業期間内において複数回の取組を行ったとしても、1つのプロジェクトとしてカウントすること。
- 採択に当たっては、公平性・公正性を確保すべく、採択基準を明文化して評価項目ごとに採点を行う。外部の第三者により構成される審査委員会での審査を経て、事業内容や自走可能性等の妥当性を評価した上で採択すること。

（※1） <https://www.meti.go.jp/statistics/toppage/topics/link/chihokyoku.html>

（※2） https://www.meti.go.jp/shingikai/mono_info_service/collab_coordinator/index.html

（※3） https://www.cas.go.jp/jp/seisaku/atarashii_sihonsyugi/pdf/ap2025.pdf

（※4） https://www.mext.go.jp/a_menu/shotou/kaikaku/1358056_00005.htm

（3）実証事業の運営・伴走支援・効果検証

- 計10者の実証事業者の採択後、経済産業省及び各経済産業局と協議の上、最終的な目標と適切なマイルストーンを置きつつ進捗管理を行う。
- 実証事業者に対して、エコシステム及び各プロジェクトの効果の最大化や実現可能性の確保等の観点から、成果報告を見据えた適切な伴走支援・効果検証を実施する。参画主体にシード・アーリーフェーズ、又は異業種から教育分野へ参入して間もない教育分野に変革をもたらす事業者が含まれる場合、当該スタートアップに対してメンタリングを含めた伴走支援を実施すること。
- 進捗管理及び今後の方針を適宜確認するため、原則、月に1回程度、経済産業省、及び各地域ブロックにおける経済産業局及び実証事業者との連絡会合を設ける（オンラインでも可）。連絡会合の生産性を最大化させる合理的な方法を提案すること。

また、会合終了後3営業日以内に議論した内容の議事概要を提出すること。

(4) ポイント集の作成及び事例集のアップデート

- 10 地域ブロックにおいて創出された連携事例を踏まえ、より良い産学連携体制の構築に向け、ステークホルダーに期待される役割やアクション、検討できる政策の方向性等についてポイント集を作成する。ポイント集には以下の内容を含めること。
 - ステークホルダー（企業、自治体、学校等）の整理
 - ステークホルダーに期待される役割・アクション
 - モデル創出の実証から得られた示唆（成功例から得られた秘訣だけでなく、失敗例における反省を含む）
- 上記に加え、2025年1月に取りまとめた「イノベーション創出のための学びと社会連携推進に関する事例集」を参考に、連携分野であるヒト・モノ・カネ、産業界への効果及び教育現場への効果を考慮した取組の好事例集をアップデートする。

(5) イベント（中間報告会・成果報告会）の開催

- 全国各地で実証事業の中間報告会を3～5回開催する。当該イベント開催に当たっては、以下の点に留意すること。
 - 企業及び自治体・学校の関係者、及び実証事業者を含む参加者を50～150名程度確保すること（対面を想定）。
 - 目指すべき産学連携の認識共有、本事業での取組、これから求められる学びや連携の在り方の啓発等につながる内容とすること。
 - 既存イベントとの併催やオンラインサービスを利用する等、多様な提案を許容するものであり、最適な形式を経済産業省と協議の上、決定すること。
- 各地域ブロックにおける実証事業の成果を報告するため、全国規模の成果報告会を1回開催する。当該イベント開催に当たっては、以下の点に留意すること。
 - 実証期間内における各実証事業者の成果を報告するイベントとすること。
 - 企業及び自治体・学校の関係者、及び実証事業者のマッチングの場としても活用できるような内容とし、参加者を100～300名程度確保すること（対面を想定）。
 - 既存イベントとの併催やオンラインサービスを利用する等、多様な提案を許容するものであり、最適な形式を経済産業省と協議の上、決定すること。
- 両イベントの効果的な広報を実施する。当該イベントの開催経費については、当該広報活動及び各実証事業者・参画主体等の招聘に要する費用等も含めて計上すること。

(6) 調査報告書等の作成

- 上記(1)～(5)の取組について体系的にまとめた報告書を作成する。上記手引きを本報告書の別添とすること。

4. 実施期間

委託契約締結日から令和9年3月19日（金）まで

<事業スケジュール（想定）>

2026年	7月上旬	実証事業者の公募開始
	8月上旬	各実証事業者の採択・契約、事業開始
	10月下旬～	中間報告会開催（3～5回）
2027年	2月下旬	各実証事業者の成果報告書の取りまとめ、契約期間終了
	～3月初旬	成果報告会開催

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。
 - 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。

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。

(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）

6. 納入方法

具体的な納入方法は経済産業省と協議することを前提とし、メール提出やファイル交換サイト等の手段を用いる。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

経済産業省 商務・サービスグループ サービス政策課 教育産業室

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4を契約前に提出し、経済産業省教育産業室（以下、「担当課室」という。）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

³委託調査報告書のデータ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。

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 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) 本事業の遂行に当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。

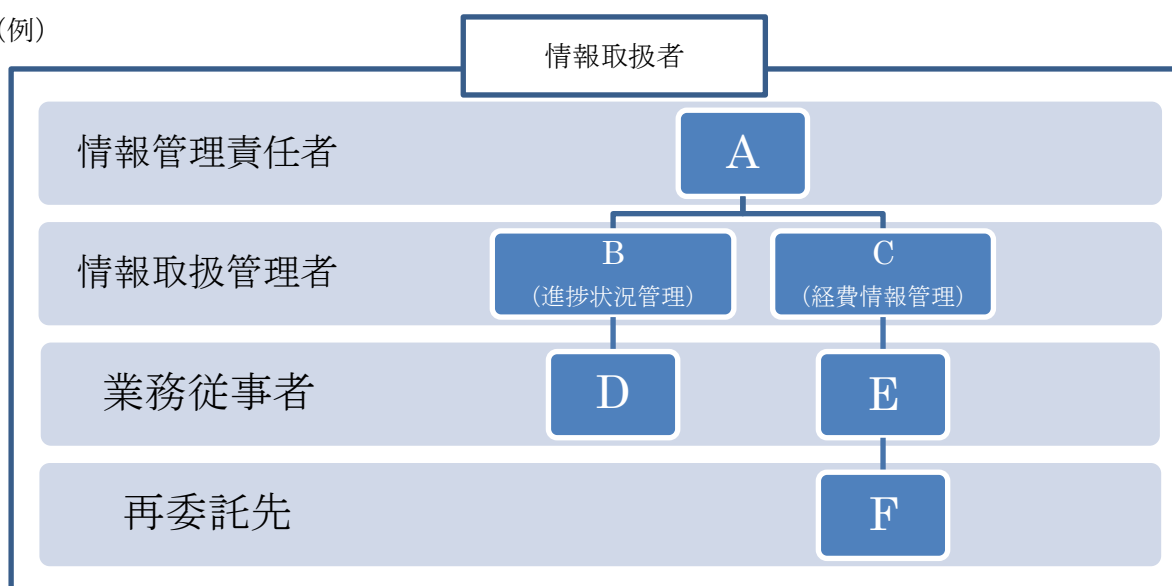
(※3) 本事業の遂行に当たって保護すべき情報を取り扱う可能性のある者。

(※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】

- ・ 本事業の遂行に当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。

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、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が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。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

経済産業省〇〇〇課長 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)	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	

	<p>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。</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に開発すること。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））。