（現時点版であり、今後修正の可能性あり）

仕様書（案）

１．件名

令和７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、２０１９年６月に「未来の教室」ビジョンを取りまとめ、「未来の教室」の実現に向けた３つの柱として、①児童生徒一人一人の興味・関心、ワクワクを核に、「探究」等に取り組む、「創る」という取組と、知識習得を新しい技術（ＥｄＴｅｃｈ）を活用し、最大限効率化する、「知る」という取組とを接続・循環させる、『学びのＳＴＥＡＭ化』、②ＥｄＴｅｃｈを活用した『個別最適化された学び』、③児童生徒一人一台のパソコン端末の整備や、学校での部活動改革、学校の業務棚卸し（ＢＰＲ）等の『教育環境の整備』が必要であると整理した。このような考え方のもと、学びの個別最適化、課題解決・科目横断思考のＳＴＥＡＭ教育の確立等、学び手自身が自らの学びを設計していく未来の学び（「未来の教室」）を実現するため、教育の各段階で活用できるＥｄＴｅｃｈの開発や実証、学校で活用する際の課題の抽出や効果検証を、「学びと社会の連携促進事業」として進めてきた。

２０２１年６月には「産業構造審議会教育イノベーション小委員会」を設置し、「学びの自律化・個別最適化」と「学びの探究化・ＳＴＥＡＭ化」を軸にこれまで行ってきた実証事業を通じて得られた成果等を踏まえた議論を行い、２０２２年９月には中間とりまとめを公表した。この中間とりまとめでは、「未来の教室」の目指すべき姿を示し、具体的には①「時間・空間」の組み合わせ自由度向上、②「教材」の組合せ自由度向上、③「コーチ」の組合せ自由度向上、④「出口」の再デザイン、⑤学校の「生まれ変わり」の土台づくりといった内容が示された。

２０２４年１月には、企業等と教育現場の連携・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、企業や地域コミュニティと自治体・学校との連携、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」を設置し、同年７月に報告書を取りまとめた。報告書では、多様な人材の育成を加速させるため、公的支出による「公助」や受益者負担の「自助」に加え、企業や地域社会との連携により、意欲ある学校、子供の挑戦を積極的に支援する社会全体で次世代の育成を支える「共助」の充実を通じて多様な学びの選択肢を用意し、新たな価値を生み出すことのできる価値創造型人材の育成を促す環境を整えることが重要とし、様々な「共助」の取組を拡大させるため、産官学が連携して取り組むべきことを整理している。

本事業においては、上記のような各種検討会等におけるこれまでの議論や、「未来の教室」事業の取組を発展的に継承しつつ、価値創造型人材の育成に向けて、教育委員会と首長部局が連携し「伸ばす学び」の充実に積極的に関与するほか、企業や地域社会、卒業生等との連携や民間資金を活用した「共助」による学びの充実を図ることで、社会全体で子どもたちの特性・個性を伸ばす「多様な学び」を充実させていくための実証、調査・広報を進めることにより、新たな学びの環境づくりを推進する。

３．事業内容及び事業実施方法

事業実施に当たっては、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、指示に従い進めること。経済産業省より状況報告や情報の共有を求められた場合は速やかに対応すること。また、実証事業の実施に当たっては報告書の作成・提出等を鑑みて適切な期日の設定を行うこと。
本事業は、これまでの「未来の教室」事業（参考：https://www.learning-innovation.go.jp/）の成果を踏まえた運営とすること。

（１） 事業全体の運営・管理

本事業は、以下、（２）～（８）までの性質が多岐にわたる事業により構成されるものであるため、事業全体の方向性を検討、設定した上で（２）～（８）までの全ての事業の運営、管理に必要な人員を配置し実施するものとする。事業全体の進捗を共有するため、週に１回程度、経済産業省との打合せの機会を設けること。打合せ資料については、経済産業省に事前に送付するとともに、打合せ終了後は３営業日以内に議論した内容についての議事概要を提出すること。

（２） 研究会・勉強会等の実施

「「未来の教室」とＥｄＴｅｃｈ研究会」（参考：
https://www.meti.go.jp/shingikai/mono_info_service/mirai_kyoshitsu/ ）の提言や、産業構造審議会教育イノベーション小委員会
（https://www.meti.go.jp/shingikai/sankoshin/shomu_ryutsu/kyoiku_innovation/ ）、「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」報告書
（https://www.meti.go.jp/shingikai/mono_info_service/innovation_creation/20240726_report.html）における議論や、これまでの実証事業の成果等を踏まえ、研究会・勉強会等を３回程度実施すること。最終的にどのようなテーマで研究会・勉強会を行うか、経済産業省と協議の上決定すること。研究会・勉強会の議事については議事録を作成し、終了後３週間以内に提出すること。
＜研究会・勉強会詳細＞
想定テーマ：これまでの実証事業における成果を踏まえた公教育と企業等の連携について
参加人数：10 人程度の有識者で議論
開催方法：原則オンライン

（３）「未来の教室」ポータルサイトの運営

「未来の教室」事業で構築したポータルサイト（https://www.learning-innovation.go.jp/）の継続運用を行い、必要に応じて機能の拡充を行うこと。ポータルサイトは最低限下記①②の機能を有するものとし、令和７年度に実施するべき機能については、経済産業省と十分な議論を行った上で決定すること。本ポータルサイトの運営にあたっては、ｇｏ．ｊｐドメインが用いられるものであることから、規定のユニバーサルデザインに沿ったものとすることが求められる。また、サイト運営に必要なサーバなども確保し、令和７年度も確実に継続運用を実施できる体制を整えること。

① ＥｄＴｅｃｈサービスのデータベース機能

現在運用中のＥｄＴｅｃｈサービスデータベースについて、継続運用しつつその掲載内容などを

精査し、他のデータベースとの統合や、運用コストの削減方策を含めて検討・実施すること。

② 「未来の教室」関連の情報発信機能

（４）（５）実証事業の公募情報や（６）広報イベントの情報を掲載する。また、実証事業の成果やその他の先進事例の概要を分かりやすくまとめ、掲載すること。

（４）令和６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）」における実証事業の継続案件と令和７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）」における実証事業の契約、運営、伴走支援、効果検証、実証成果広報、令和８年度実証事業の案件組成（公募・審査）

＜令和６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）」継続案件＞

令和６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）」で採択された実証事業者のうち、当該事業において翌年度も継続すべきと内定した事業者に対して、令和７年度事業においても継続して実証事業に取り組めるよう、契約事務及び伴走支援等を実施すること。

＜令和７年度新規テーマ設定＞

令和６年度までの「未来の教室」事業を振り返ったうえで今後の論点を議論し、実証事業において令和７年度から令和９年度に求めるべき成果目標を定め、それに基づいた実証テーマの設定を行うこと。テーマ設定にあたっては、これまでの「未来の教室」事業の実証成果や「産業構造審議会教育イノベーション小委員会」中間取りまとめ、「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」の議論等を踏まえるとともに、そこからの発展性（いくつかの事業を組み合わせることによるシナジー効果の創出等を含む）を鑑みた提案とすること。また、次期学習指導要領改訂を見据え、「産業構造審議会教育イノベーション小委員会」及び「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」において言及された学びの在り方の追及に資するものとすること。最終的な公募テーマについては、事業開始後、経済産業省と協議の上決定すること。

＜令和７年度案件組成（公募・審査・採択）＞

学びの現場（学校、公教育外の「学びのサード・プレイス」等）をフィールドとしつつ、民間教育サービス事業者その他の主体（自治体、地域の企業群、大学・研究機関等）との連携によって構築された「未来の教室」として効果を検証するプログラムを、令和６年度事業からの継続事業者も含めて全国で計１０件程度組成すること。（１件あたりの金額は、事業内容や規模に応じて変動するが、過去の実績から、規模に応じて５００万円～３，０００万円程度（合計２億円程度）の実証事業が可能な予算を確保すること。また、ここで組成するプログラムは、複数の学びの現場での実証事業であっても、同一の民間教育サービス事業者又はその他の主体（自治体、地域の企業群、大学・研究機関等）とのコンソーシアムによる事業であれば、１つのプログラムとしてカウントする。）

本実証案件において実証事業者として再委託先を選定する際には、公募を行い、評価項目ごとに採点を行った上で必ず第三者による審査を経て、事業内容や価格、自走可能性等の妥当性を評価した上で採択すること。

また実証案件の公募・採択においては、以下の点に留意すること。

- 地方創生の視点も踏まえ、複数の自治体単位で広く実施する実証も行い、今後実証内容の横展開が可能となるようなスキームを一定数採択すること。
- 資金拠出可能性がある関係者を巻き込むことでマネタイズの工夫を組み込むといった形により、実証事業の実施後に当該実証の自走・横展開が見込まれる案件を採択できるように工夫すること。
- 実証事業終了後に、実証場所となった学校等以外にも幅広く普及できる教育プログラムを確立すべく、教育・人材育成プログラムを開発・運用しビジネスモデル化しうる主体を中心として実証案件を採択できるように工夫すること。
- 実証場所となる地域の特性（都市部・過疎地・島嶼部等）、教育段階、実証カテゴリの観点から採択案件数のバランスにも配慮しつつ、適切な実証期間を設定すること。

＜運営・伴走支援・効果検証＞

採択した実証事業については、円滑な運営を行うとともに、教育効果の最大化や事業フィージビリティの確保等の観点から適切な伴走支援を実施すること。本実証は、一部の事業については次年度以降にわたり実証を行う（事業継続の可否に係る判断のため、毎年度、後述の第三者委員による審査を実施）ことを想定しているため、最終的な目標と適切なマイルストーンを置きつつ、事業進捗を管理すること。

また、本事業は事後の効果検証を行うとともに全国の教育機関等への普及活用を念頭においた事例創出を目指すものであり、そのために必要な調査や国内事業者へのヒアリングを行ったうえで事例広報の案を作成すること。

事業全体にかかる実証の運営や伴走支援にあたっては、教育関係の学識経験者、教育委員会関係者等からなる３人程度の有識者の意見を取り入れ、経済産業省と相談をして決定すること。

事業開始後、各実証事業について、事業開始時期も鑑みつつ、原則月に１回程度、経済産業省の担当者もメンバーに含めた連絡会合（進捗や今後の方針などを確認する機会、オンラインでの実施も可）を設けること。会合の開催手法についても、会議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。

＜令和７年度実証事業の内、次年度以降も継続して実施する実証に関する審査について＞

提案時に複数年の実施を想定している事業の場合、次年度以降の実証事業の継続の可否については、第三者委員による審査を行うこと。詳細については、事業開始後、経済産業省と協議の上決定すること。

＜令和８年度の案件組成（公募・審査）＞

令和８年度も「未来の教室」実証事業が継続する前提で、令和８年度に行う実証事業の公募を行い、第三者委員による審査を行うこと。案件組成方法については令和７年度と同様を想定しているが、テーマや１件あたりの金額、件数等の詳細は経済産業省と協議の上決定すること。

＜実証事業の成果報告会の実施＞

令和７年度に実施した実証事業の成果を報告するとともに、自治体や学校関係者、民間企業と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イベント内容を検討すること（対面参加者数１００～１５０名程度を想定。実施回数は１回）。開催に当たっては、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、令和７年度に最適な形式を経済産業省と相談の上決定すること

（５）ＳＴＥＡＭライブラリーの運営及び改修

＜ＳＴＥＡＭライブラリーの運用・改善＞

経済産業省と相談の上、「未来の教室」事業で構築したＳＴＥＡＭ学習（学際的な探究型・課題解決型の学習）コンテンツのオンラインプラットフォームであるＳＴＥＡＭライブラリー（https://www.steam-library.go.jp/）の継続運用を行うのみならず、ライブラリーの運用コストの削減に向け、その方策については経済産業省と協議の上、改修に取り組むこと。

なお、本ライブラリーは、ｇｏ．ｊｐドメインが用いられるものであることから、規定のユニバーサルデザインに沿ったものとすることが求められる。ＳＴＥＡＭライブラリーの運用にあたっては、サイト及びコンテンツ等へのアクセス状況を随時把握・分析すること。

（６）広報・周知普及の取組

経済産業省と相談の上、各種イベントやニュースレターの発行、ＳＮＳでの発信を通じ、数万人規模を対象として「未来の教室」の目指す姿を総合的に推進する。

＜「未来の教室」広報イベントの開催＞

「目指すべき「未来の教室」の姿」の認識共有、本事業での取組やこれから求められる学びの在り方の啓発等につながるイベント（対面参加者１００～１５０名程度を想定）を東京やその他の地域において、最低１回以上開催すること。開催に当たっては、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、ターゲット層の分析と本事業の今後の展開性等の観点から、令和７年度に最適な形式を経済産業省と相談の上決定すること。これらの開催に係る経費については事業費に計上すること。

＜広報ツールの検討＞

それぞれの事業の性質等を踏まえ、ユニバーサルデザインを意識しつつ、集客効果が高まるデザインを施したＰＲ資材（チラシ、ポスター、動画、ＳＮＳ等からの発信等）を企画、作成するとともに、本資材を活用した参加事業者への事前広報活動や取組内容に係る広報活動等も実施し、既存のＳＮＳも活用した情報発信を行うこと。

加えて、学びの主体は学習者自身であることを再認識した上で、効果的な広報・周知普及の在り方について検討し、学習者に効果的に届けるための手法について、関係省庁の取組を参考にしながら実行すること。

（７）教育イノベーター支援プログラム（ＥＯＬ：Ｅｄｖａｔｉｏｎ　Ｏｐｅｎ　Ｌａｂ）の企画・運営

国際競争力があり、かつ日本の教育イノベーションを牽引するような教育産業を育成することを目的に、教育分野のスタートアップ等（＝教育イノベーター）を官民連携で支援するエコシステムの構築を目指し、セミナーやミートアップイベント、採択者へのメンタリング等を行う。その際、これまでの「学びと社会の連携促進事業（教育／ＥｄＴｅｃｈイノベーション創出支援事業)」や「令和６年度学びと社会のあり方改革推進事業（「未来の教室」実証事業）の内の教育イノベーター支援プログラム（ＥＯＬ：Ｅｄｖａｔｉｏｎ　Ｏｐｅｎ　Ｌａｂ)」を参考に実施すること。

（８）報告書の作成

（２）～（７）の調査等の取組について、体系的にまとめた報告書を作成すること。

４．実施期間

委託契約締結日から令和８年３月３１日（火）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、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

[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。

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）

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

経済産業省　商務情報政策局　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、サービス政策

[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。

課教育産業室（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．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。

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。

（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。

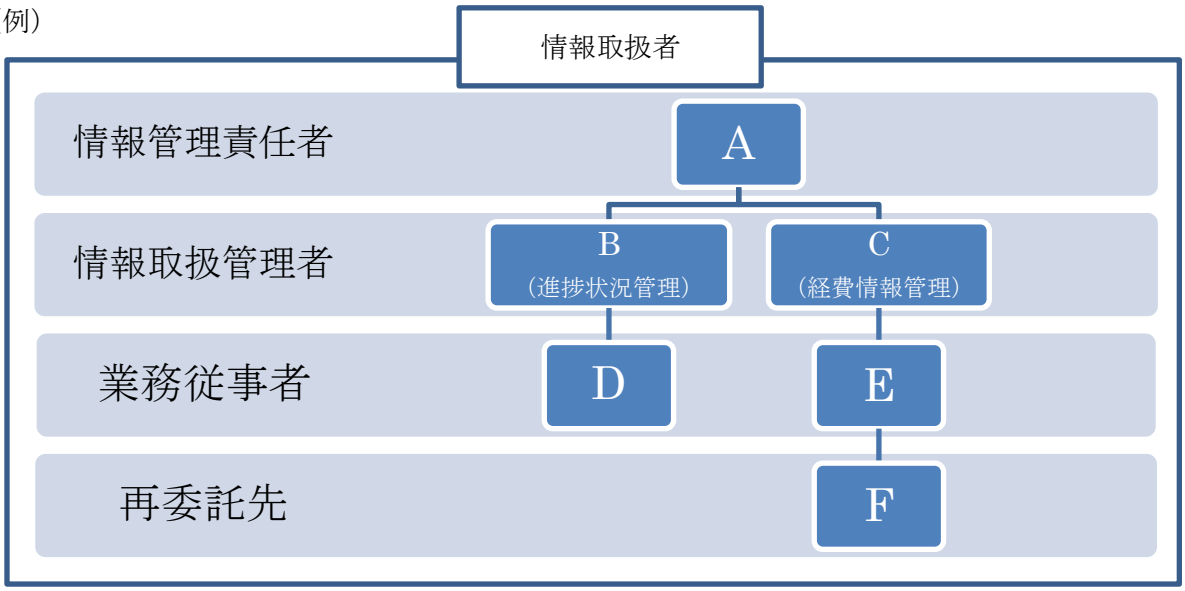
（※３）本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※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】

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））。）