

## 仕様書

## 1. 件名

令和7年度ユニコーン創出支援事業（女性アントレプレナーのための地域密着型支援事業）

## 2. 事業の背景・目的

我が国が今後の経済成長を実現していくために、イノベーションの担い手として不可欠なのが社会課題の解決に果敢に挑戦するスタートアップの存在であるが、依然として、スタートアップの起業家に占める女性の割合は少なく、新規上場企業に占める女性社長の比率は2%となっている。この原因として、女性起業家はライフイベントの影響を受けやすく、事業との両立の中で資金調達が難しいこと、男性中心の起業家ネットワークの中で情報へのアクセスが限定的であること等、女性特有の課題が存在することが挙げられる。

また、女性は地域に根ざした形で起業するケースも多く、産業支援機関、スタートアップ支援企業、地方銀行や信用金庫といった金融機関や地域の中核企業等、地域において女性起業家を支援する機関をつなぐネットワークを構築し、「面」で女性起業家を支援することが非常に重要である。

これを踏まえ、令和6年度ユニコーン創出支援事業（女性アントレプレナーのための地域密着型支援事業）（以下「令和6年度女性起業家支援事業」という。）において、「GIRAFFES JAPAN」という事業コンセプト※1の下、全国各地で、アントレプレナーシップを持ちスケールアップを目指す女性起業家を対象として、上述の支援機関を巻き込んでの支援体制の構築、ネットワーキングイベントや起業家へのメンタリング、ビジネスプラン発表会等の支援プログラムを実施した。

本事業では、昨年度に引き続き、「GIRAFFES JAPAN」の事業コンセプト（以下「全国統一コンセプト」という。）の下で、全国を8ブロック（北海道、東北、関東、中部、近畿、中国、四国及び九州）に分け、女性起業家や支援機関の更なる掘り起こしを通じて地域に根ざした女性起業家支援ネットワークを構築し、各地域で女性起業家のロールモデルの輩出及び支援機関の育成を行うために、ネットワーキングイベント、起業家へのメンタリング、ビジネスプラン発表会等の各種支援プログラムを実施し、女性起業家を総合的に支援する。

## ※1 GIRAFFES JAPAN について

「GIRAFFES」は「GIRAFFE」（キリン）の複数形で、高い視座で未来を見ながら、多くの仲間と助け合い共にビジネスを展開する女性起業家を日本中で応援するという令和6年度女性起業家支援事業の全国統一コンセプト。各地域での支援プログラムの実施を通じて、地域における女性起業家支援の成功事例を積み上げ、成長指向の女性起業家の増加及び更なる支援機関の参入につなげることで、将来的には各地域で自走可能な女性起業家支援ネットワークが構築できている状態を目指す。

事業ホームページ：<https://giraffes.go.jp/>

## 3. 事業内容及び事業実施方法

本事業は、全国統一コンセプトの下、地域の実情に応じて、各地域で女性起業家支援プログラムを実施する。そのため、各地域で実施する支援プログラムへの助言等の支援業務や全国統一での規程・シス

テム整備等を実施する事務局（以下「全国事務局」という。）並びに地域の実情を勘案して支援プログラムの企画、立案及び実施を行う全国8ブロックごとの機関（以下「代表機関」という。）を選定し、実施する。

本件は、全国事務局の入札公告であり、代表機関の募集は別に行う。

全国事務局が実施する業務は以下のとおり。

#### （１） 事業全体方針の企画立案及び代表機関への助言等

令和6年度女性起業家支援事業の実施内容を踏まえ、本事業全体の実施内容・手法に係る企画立案を行う。事業の実施方針に係る提案は、提案書に含めること。

また、各地域の代表機関が実施する事業が、全国統一コンセプトに基づきつつ、当該地域の実態を踏まえた適切な支援プログラム（ネットワーキングイベント、ビジネスプラン発表会、メンタリング、支援ネットワークに参画する支援機関の巻き込み、その他地域の実情に応じて必要なプログラム）になるよう助言を行う。そのために数週間に1回程度、代表機関との打合せを設け、事業の実施状況等を確認する。

これに加え、各地の代表機関同士の情報交換が可能な場を1年に2回程度設定すること。具体的な方法は経済産業省と協議の上で決定するものとする。

また、各地での代表機関による女性起業家支援を効率的にサポートするための女性起業家や支援機関向けの各種コンテンツの作成を行う。なお、コンテンツの内容は、女性起業家に向けとしては、起業や事業継続・拡大のノウハウやロールモデルとなるような先輩女性起業家の事例をまとめたもの、支援機関向けとしては、女性起業家特有の課題を理解したうえでのメンタリングの実施に関するノウハウをまとめたもの等を想定しているが、その他女性起業家支援に資すると考えられる内容を提案に含めることについては妨げない。なお、最終的なコンテンツやその形式は経済産業省と協議の上決定するものとする。

#### （２） 事業共通で運用する規程及びシステムの作成、管理及び運営

本事業共通で運用する規程及びシステムについて、経済産業省とも協議を行いながら作成、管理及び運営を実施する。

規程は、本事業の広報に係る規程、各地域において実施する女性起業家へのメンタリングの際のコンプライアンスの観点からの留意事項等を定めたメンタリング規程等、事業を実施するうえで必要と認める規程について、経済産業省との協議の上で作成する。

また、作成した規程は各地域の代表機関に共有し、各地域において各種規程が遵守されるよう代表機関と適切に連携すること。

システムについては、女性起業家や支援機関が各種イベントに参加する際の申込みや、各地の支援機関の一覧等、本事業の関連情報の掲載等が事業実施期間中継続して可能なホームページを想定しているが具体的な内容は経済産業省と協議の上、作成するものとする。

なお、上述のシステムを構築する際に利用するクラウドサービスは、政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））において、ISMAPクラウドサービスリストに登録されたものを用いること。

#### （３） 支援機関向けのメンター研修の実施及び各地域におけるメンタリング実施の支援

本事業においては、各地において代表機関及びその他支援機関が中心となり、女性起業家向けにメンタリングを実施することを予定している。各地におけるメンタリングの質を担保するため、女性起業家特有の課題やコンプライアンスの観点を踏まえたメンタリングにおける留意事項等について、支援機関に対してメンター研修を少なくとも1回実施する。また、録画等を行い後日のアーカイブ配信も可能な状態とすること。なお、研修の実施方法は対面又はオンライン会議のいずれでも差し支えないが、最終的な決定は経済産業省と協議の上で行う。実施規模は、研修当日に参加する支援機関数が50機関程度を想定している。

なお、地域の実情も踏まえ、各地の代表機関とも相談のうえ、全国事務局が手配するメンターの派遣等、各地におけるメンタリング実施において適切な支援を必要に応じて実施できる体制を構築することとする。なお、地域の実情に応じて、全国事務局が地域にメンターを派遣する必要があると考える場合のみ、当該メンターの派遣に係る費用は全国事務局において計上する。

#### （４）全国交流イベントの実施

2025年日本国際博覧会におけるウーマンズ パビリオンを活用し、各地域の女性起業家や支援機関の交流が可能なイベントの運営を行う。イベントの時期は6月27日（金）の1日間を想定しており、イベントの内容としては、令和6年度女性起業家支援事業において実施したビジネスプラン発表会において各地で選出されたファイナリスト数名や国内外の女性起業家のロールモデルを集めたパネルディスカッションやビジネス発表等を想定しているが、その他女性起業家支援に資すると考えられる内容を提案に含めることが望ましい。イベントの規模は会場参加の一般参加者が60名程度（計80名）を想定している。一般参加者についてオンラインでの参加も妨げないが、会場参加の一般参加者は、万博の全パビリオン共通の入場券を購入の上、参加することが必要となる。最終的なイベントの内容については経済産業省と協議の上決定するものとする。

なお、イベント実施に伴う費用の計上要否は下記のとおり。

##### （計上不要な費用）

当日の会場費（音響機器、オンライン配信に係る機材等の設備も含む。）、当日対応を行う全国事務局スタッフ及びファイナリストその他の登壇者の入場料（ただし、経済産業省の職員を含めて20人を上限とする。）、一般来場者の入場料

##### （計上が必要な費用）

イベントの実施に係る検討に要する事業費、当日対応を行う全国事務局スタッフの人件費及び旅費、ファイナリストその他の登壇者への謝金及び旅費

#### （５）本事業の周知・広報

本事業について、事業成長を目指す女性起業家及び女性起業家支援に関心がある支援機関に認識され、本事業における支援ネットワークへの参画やイベントへの参加につながるよう、ポスターやリーフレット等の作成を行い、女性起業家及び支援機関に対して広く周知・広報を行う。なお、周知・広報の方法は、メールやHP掲載等の電子的方法で実施することを想定している。

## （６）女性起業家支援に関する好事例の収集・整理及び効果検証並びに有効的な支援の在り方に関する提案

各地域ブロックの女性起業家支援の好事例を収集するとともに、女性起業家や支援機関へのアンケート等を通じて、事業におけるプログラムの効果検証を実施する。

好事例の収集にあたっては、令和６年度女性起業家支援事業において選出したファイナリストに関する調査（支援機関から提供を受けた支援内容や選出後の事業成長状況等）を含むものとする。また、上述の効果検証等を踏まえて、地域に根付いた女性起業家支援ネットワークを構築するために有効と考えられる施策についての提案を実施する。

## （７）調査報告書の作成

上記（１）～（６）に掲げる事業の成果を取りまとめた報告書を作成する。

報告書案については事業完了の１か月前までに担当部局へ提出し、内容の確認を受けること。

また、修正が必要と判断された場合は、事業完了１０日前までに修正版の報告書案を担当部局へ提出し、再度の確認を受けること。

## ４．事業スケジュール

令和７年 ４・５月 システム・規程の整備、公開

６月 全国交流イベント

６月以降 各地の代表機関により順次ネットワーキングイベントを実施

８・９月 コンテンツの作成

１０月 メンター研修

令和８年 １・２月 代表機関が開催するビジネスプラン発表会

ただし、詳細スケジュールについては別途公募する代表機関の提案に基づき最終決定する。

## ５．実施期間

委託契約締結日から令和８年３月３１日まで

## ６．納入物

### （１） 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<sup>１</sup>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

<sup>１</sup> 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）。

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 E x c e l や C S V 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 P D F 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<sup>2</sup>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・E x c e l 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（P D F）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。
  - E x c e l 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。
  - E x c e l 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。

## （３） 様式 1 ～ 様式 3 について

- （様式 1）委託調査報告書骨子<sup>3</sup>
  - 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 W o r d 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<sup>4</sup>
  - ファイル形式は E x c e l 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 P D F 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 P D F 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典拠等を明示し、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 E x c e l 形式で納入すること。
- 様式 1 ～ 3 ダウンロード先

<sup>2</sup>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。

<sup>3</sup>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。

<sup>4</sup>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。

➤ 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 経済産業政策局 経済社会政策室

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（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. 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。

## 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<br>番号及び国<br>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。

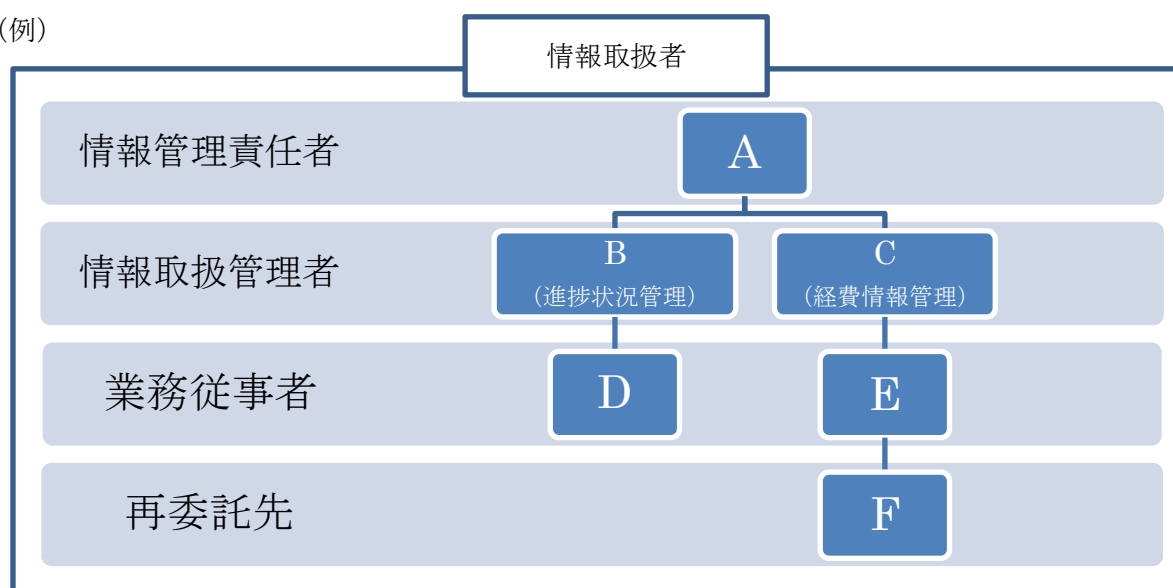
（※3）本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※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。



## 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）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。

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。

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<br>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<br>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<br>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<br>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<br>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、<br>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<br>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<br>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<br>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<br>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<br>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。<br><br>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<br>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<br>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<br>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。<br><br>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<br>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<br>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<br>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<br>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<br>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<br>１５） | <p>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。</p> <p>（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。</p> <p>（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。</p> <p>（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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> |  |



|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |  |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
|                       | <p>(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。</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"> <li>・ 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。</li> <li>・ 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。</li> <li>・ 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。</li> </ul> <p>(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。</p> |  |
| 情報セキュリティに関する事項<br>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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |  |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |  |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
|  | <p>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> <p>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。</p> <p>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。</p> <p>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> <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法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</p> |  |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|

|                       |                                                                                                                                                                                                                                                                                                                                                               |  |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
|                       | 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<br>17) | <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った場合には、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））。)