

応募企画提案書作成にあたって

第1 業務名

農林水産省中小企業イノベーション創出推進事業（SBIRフェーズ3基金事業）にかかる
経理支援委託業務（以下「本業務」という。）

第2 業務の目的

農林水産業・食品産業の持続的発展に向けて、農林水産業・食品産業が抱える様々な課題を解決するためには、生物機能等を利用した独創的な製品・素材の生産、スマート技術を利用した画期的なシステム改善、カーボンニュートラルを目指す循環型社会システムの確立等が不可欠であり、これらの実現のためには、革新的な研究開発を行う中小企業（以下「スタートアップ等」という）の有する技術を円滑に社会実装に繋げ、イノベーション創出を図ることが必要である。

公益社団法人 農林水産・食品産業技術振興協会（以下「JATAFF」という。）は、国の補助金の交付を受け、スタートアップ等が社会実装に繋げるための大規模技術実証事業を実施するための基金を造成し、基金設置法人として農林水産省中小企業イノベーション創出推進事業（以下「SBIRフェーズ3基金事業」という。）を執行しているところである（SBIRフェーズ3基金事業のスキーム（別紙1）参照）。

本事業は、SBIRフェーズ3基金事業に採択されたスタートアップ等（以下「補助事業者」という。）が作成・提出した事業計画等について、的確な予算執行や必要に則した計画変更等の処理を通じ、同計画の円滑な進捗や目標達成を確保するため、既にJATAFFが実施している補助事業者への伴走支援に準じ、毎年度の補助金の執行の不具合が同計画の円滑な遂行を妨げることがないように、経理面からも伴走支援を行うことを目的とする。

第3 業務の対象

本業務は、令和6度にSBIRフェーズ3基金事業で採択された補助事業者（13課題16スタートアップ（別紙2））を対象とする。

第4 履行期間

令和7年4月1日～令和8年3月31日

第5 委託費の限度額

本業務の履行期間における委託費の限度額は、30,000,000円以内とする。

なお、支援対象補助事業者数等業務量に大きな変動がある場合は、JATAFFと受託者で協議の上、契約金額及び履行期間を変更する場合がある。

第6 業務内容

JATAFFの指導に基づき、補助事業者が作成する各種申請書類等に対する作成支援業務（以下、ア～キ）及びJATAFFとの調整事務を行う。具体的には、「農林水産省中小企業イノベーション創出推進事業公募要領」、「農林水産省中小企業イノベーション創出推進事業費補助金交付規程（以下「交付規程」という。）」、「補助事業等の実施に要する人件費の算定等の適正化について」、その他JATAFFが別途提示する補助事業の手引き、各種申請書類の記載マニュアル（以下「業務マニュアル」という。）等（以下「関係規程等」という。）に基づき、各種申請書類が適正に作成されているかを確認し、計画変更分の未反映などその内容に不備がある場合には、補助事業者に修正の指示・提案を行う。指示・提案を経て各種申請書類が修正された場合は、修正後の各種申請書類を速やかにJATAFF SBIRフェーズ3基金事務局に提出し、その妥当性やさらなる修正対応の有無等について指示を

受ける。

また、補助事業者が作成・提出した事業計画を的確に踏まえた確認、提案、指示等の業務が適切に遂行されるよう、本事業で実施するフォローアップ委員会及び評価委員会にはオブザーバーとして出席し、委員等からの指摘事項等の正確な把握に努める。

さらに、これらの経理支援委託業務への従事を通じ、事務上の要改善点を整理し、業務マニュアルの修正案を提案する。

(1) 交付申請書にかかる支援

交付規程第4条第1項に基づき、補助事業者から提出された交付申請書及びその添付書類の記載内容等について関係規程等に基づく確認を行い、その内容に不備がある場合には、補助事業者に修正を指示する等必要な支援を行うこと。

(2) 計画変更（等）承認申請書にかかる支援

交付規程第9条に基づき、補助事業者から提出された計画変更（等）承認申請書及びその添付書類の記載内容等について関係規程等に基づく確認を行い、その内容に不備がある場合には、補助事業者に修正を指示する等必要な支援を行うこと。

(3) SBIRフェーズ3基金事業費補助金第三者委託・共同実施契約にかかる届出書にかかる支援

交付規程第10条第2項に基づき、補助事業者から提出された第三者委託・共同実施契約にかかる届出書及びその添付書類の記載内容等について関係規程等に基づく確認を行い、その内容に不備がある場合には、補助事業者に修正を指示する等必要な支援を行うこと。

(4) 繰越承認申請書にかかる支援

交付規程第12条第2項に基づき、補助事業者から提出された繰越承認申請書及びその添付書類の記載内容等について関係規程等に基づく確認を行い、その内容に不備がある場合には、補助事業者に修正を指示する等必要な支援を行うこと。

(5) 状況報告書にかかる支援

交付規程第13条に基づき、補助事業者から提出された状況報告書及びその添付書類の記載内容等について関係規程等に基づく確認を行い、その内容に不備がある場合には、補助事業者に修正を指示する等必要な支援を行うこと。

(6) 実績報告書にかかる支援

交付規程第14条に基づき、補助事業者から提出された実績報告書及びその添付書類の記載内容等について関係規程等に基づく確認を行い、その内容に不備がある場合には、補助事業者に修正を指示する等必要な支援を行うこと。

(7) 概算払請求書の支援

交付規程第17条に基づき、補助事業者から提出された概算払請求書及びその添付書類の記載内容等について関係規定等に基づく審査を行い、その内容に不備がある場合には、補助事業者に修正を指示する等必要な支援を行うこと。

(8) 報告書作成、提出

本業務で実施した業務内容について、報告書及びその概要版を作成し、電子媒体で提出する。納品する電磁的記録媒体は、ウイルスチェックを行ったうえで、ウイルスチェックに関する情報（ウイルス対策ソフト名、定義ファイルのバージョン、チェック年月日等）を記録したラベルを添付する。

なお、報告書類は事前に十分な時間的余裕（概ね1か月前）をもってJATAFFに相談するものとする。

(9) 補助事業終了後の対応

プロジェクト実施主体に対して、補助事業が完了した日の属する年度の終了後5年間、事業継続状況の報告を求める予定のため、受託者は、当該業務に必要な経費を含めJATAFF理事長と協議の上、事業継続状況の調査等の業務を行うものとする。

第7 実績報告書・支払方法等

(1) 支払額の確定方法

受託者は、本委託事業の実施期間中の実績報告書（経理関係「以下同じ。」）を

JATAFFに提出する。JATAFFは、実績報告書に基づき必要に応じて現地調査を行い、支払額を確定する。その際、農林水産省も現地調査を行う場合がある。

また、受託業務に係る取引先（委託先、外注先及びそれ以下の委託先、外注先を含む）に対しても、同様の現地調査等を実施することがある。

支払額は、計画金額の範囲内であって実際に支出を要したと認められる費用の合計となる。このため、全ての支出には、その収支を明らかにした帳簿類及び領収書等の証拠書類が必要となる。また、支出額及び内容についても厳格に審査し、これを満たさない経費については、支払額の対象外となる可能性もあるので注意すること。

(2) 支払い時期

受託業務費用は、原則として、(1)の支払額の確定後の支払いとする。

※ 本受託業務に充てられる自己資金等の状況次第では、受託業務実施中の支払い（概算払）も可能なので、希望する場合は個別に相談すること。なお、受託業務終了後、精算を行い、委託費の原資としてJATAFFから受け取った資金に残余が生じた場合には、これをJATAFFに返還するものとする。

第8 応募資格要件

本業務の参加希望者は、以下の全ての要件を満たすこと。

- ・日本の法人格を有し、かつ国内に活動拠点を有していること。
- ・事業の遂行に必要となる国等の補助金の制度や手続き等その経理実務について高い専門性と豊富な経験を有する組織、人員等を配置できること。
- ・当該委託業務を円滑に遂行するために必要な管理能力を有し、かつ、適正な経理処理が可能な体制を有していること。

第9 委託先の選定方法

(1) 応募から採択決定までの流れ

ア JATAFFは、応募された提案について、「(2)審査の方法」及び「(3)審査基準」に記載された審査を実施する。

イ JATAFFは、委託先として決定された者に対し、その旨を通知し委託契約を締結する。

なお、契約の締結に当たり、審査結果に基づき、条件の追加や業務内容の変更を求めることや、契約額の提案内容からの減額を求めることがある。

(2) 委託先の選定審査の方法

ア JATAFFに設置する企画競争審査委員会が審査を行い、契約候補者を選定する。

イ 企画競争審査委員会は、管理運営体制やその内容、経費見積もりの妥当性等を含めて審査を行う。※委託費用の区分は別紙3のとおりとする。

ウ 審査において、最も優秀な提案を行った1者を委託先とする。

エ 必要に応じてヒアリングや資料の追加等を求める場合がある。

オ 審査は非公開で行われ、審査の経過等、審査に係る問い合わせには応じない。

(3) 審査基準

企画競争審査委員会は、以下の観点で定める審査基準に基づき、審査を行う。

ア 提案内容が本業務の趣旨と合致していること。

イ 提案された内容が優れていること。

ウ 提案内容を確実に遂行するための体制が整っていること。

エ 経費の見積もりが適切であること。

第10 応募時の提出書類

本業務は企画競争により委託先の決定を行うため、応募時に下記のとおり書類を提出すること。提出書類は企画競争公告 3(3)に基づき期限までに提出すること。

(1)応募申請書(様式1)	1部
(2)応募企画提案書(様式2)及びプレゼンテーション資料 15枚程度、PDF) <u>別途、電子データ(PDFファイル等)をJATAFF宛にメール等にて提出すること。</u> メールアドレス:	1部
(3)業務従事者リスト	1部
(4)各業務従事者に係る履歴資料 ※1	1部
(5)保護すべき情報の取扱いに関する資料 ※2	1部
(6)決算書類(直近3年間)	1部

※1 各業務従事者に係る履歴資料は、任意の書式により次の内容を記載する。ただし、必要に応じ、追加資料の提出を求められることがある。

- ・ 各業務従事者の氏名、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、資格、母語及び外国語能力、国籍その他文化的背景、業績等(修業、従事、取得等の時期及び期間を含む。)

※2 保護すべき情報の取扱いに関する資料は、次を標準とする。ただし、必要に応じ、追加資料の提出を求められることがある。

- ① 契約を履行する一環として提案者が収集、整理、作成等した一切の情報について、JATAFFが保護を要しないと確認するまでは保護すべき情報として取り扱うとともに、提案者の代表権を有する者、役員(持分会社にあっては社員を含む。)、管理職員等であっても、当該契約に基づきその取扱いを認められた者以外の者は、これに接してはならず、かつ、職務上の下級者等に対してその提供を要求してはならない旨を定める社内規則(契約締結時までに施行予定であるときは、当該施行期日が明記された決裁済みの未施行規則)の写し(応募企画提案書作成要領の要求に関わらない部分は、残余の部分から当該部分が応募企画提案書作成要領と無関係であると判別できる態様により、黒塗り等の方法により削除することができる。)
- ② 提案者に係る親会社等、兄弟会社、地域統括会社、ブランド・ライセンサー、フランチャイザー、コンサルタントその他の提案者に対して指導、監督、業務支援、助言、監査等を行う者(③において「関係会社」という。)の一覧及び提案者との資本又は契約(名称如何を問わない何らかの合意をいい、間接契約、三者間契約等を含む。以下同じ。)の関係図
- ③ 顧客との契約に基づき提案者以外の者に対する伝達又は漏えいが禁じられた情報が報告、共有その他情報提供の対象とならないことが明記された提案者とその関係会社との関係を規定する契約を化体する書面全ての写し(応募企画提案書作成要領の要求に関わらない部分は、残余の部分から当該部分が応募企画提案書作成要領と無関係であると判別できる態様により、黒塗り等の方法により削除することができる。)

第11 情報保全

受託者は、この契約の履行に際し知り得た保護すべき情報(JATAFFに係る情報であって公になっていないもののうち、JATAFF職員以外の者への漏えいがJATAFFの業務の遂行に支障を与えるおそれがあるため、特に受注者における情報管理の徹底を図ることが必要となる情報をいう。以下同じ。)の取扱いに当たっては、「調達における情報セキュリティ基準」(別紙4)(以下「本基準」という。)及び別紙「調達における情報セキュリティの確保に関する特約条項」(別紙5)に基づき、適切に管理するものとする。

この際、特に、保護すべき情報の取扱いについては、次の履行体制を確保し、これを変更

した場合には、遅滞なくJATAFFに通知するものとする。

- ・ 契約を履行する一環として受注者が収集、整理、作成等した一切の情報が、JATAFFが保護を要しないと確認するまでは保護すべき情報として取り扱われることを保障する履行体制
- ・ JATAFFの同意を得て指定した取扱者以外の者に取り扱わせないことを保障する履行体制
- ・ JATAFFが書面により個別に許可した場合を除き、受注者に係る親会社等（本基準第2項第14号に規定する「親会社等」をいう。）、兄弟会社（本基準第2項第15号に規定する「兄弟会社」をいう。）、地域統括会社、ブランド・ライセンサー、フランチャイザー、コンサルタントその他の受注者に対して指導、監督、業務支援、助言、監査等を行う者を含む一切の受注者以外の者に対して伝達又は漏えいされないことを保障する履行体制

第12 その他

本業務の実施にあたっては、JATAFFと十分に協議を行い、意思疎通を図りつつ進める。受託者は、本業務の実施において、民法、刑法、著作権法、行政機関の保有する個人情報保護に関する法律等の関連法規、労働関係法令及び関連する法令等を遵守すること。

それぞれの業務状況は、JATAFFの指示に基づき、適宜、書面及び電子媒体で提出する。

本業務の目的を達成するために、本応募企画提案書作成要領に明記されていない事項で、契約履行上確認が必要な事項、又は疑義が生じた事項については、JATAFFに確認し、その指示を受けるものとする。

本業務の実施に当たって、受託者自ら一元的に管理・運営することとし、事業の全部を一括して、又は主たる部分（事業全体の企画及び立案並びに根幹に関わる執行管理部分等）を第三者に委託してはならない。なお、再委託の必要が生じた場合は、事前にJATAFFへ報告し、承諾を得ることとする。

また、再委託に当たっては、委託費の限度額に占める再委託金額の割合が、原則として50パーセント以内にする。50%を超える場合は様式3でその理由を報告すること。

第13 担当者

〒100-0011 東京都千代田区内幸町1-2-1 日土地内幸町ビル2階
公益社団法人 農林水産・食品産業技術振興協会SBIRフェーズ3基金担当

(公募手続に関すること)

古瀬

(事業内容に関すること)

鈴木、藤井

電話 03-3509-1161

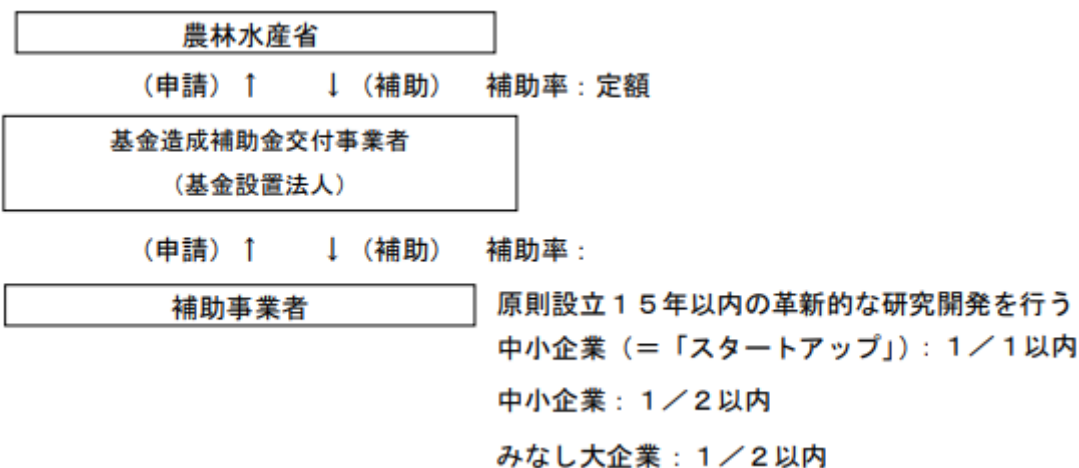
メール sbir3@jataff.or.jp

(注) お問い合わせは、電子メールでお願いします。電話でのお問い合わせは受付できません。

なお、お問い合わせの際は、件名（題名）を必ず「SBIRフェーズ3基金事業にかかる経理支援業務」として下さい。他の件名（題名）ではお問い合わせに回答できない場合があります。

事業スキーム

科学技術・イノベーション創出の活性化に関する法律に基づく指定補助金等として、補助金により造成された基金を用いて造成された基金を用いて、フェーズ3基金事業を行い、補助事業者の申請に基づき交付します。



注1 複数年の交付決定合計額に対する補助率

注2 「中小企業」とは、科学技術・イノベーション活性化法第2条第14項に規定する中 小企業者をいう。また、「スタートアップ」の判断にあたっては、技術の態様に応じ弾 力的に運用することとし、J-Startup 又は J-Startup 地域版選定スタートアップを含む。

注3 「みなし大企業」とは、中小企業者であって、以下のいずれかを満たすものをいう。

- ・ 発行済株式の総数又は出資の総額の2分の1以上が同一の大企業(※)の所有に属している企業
- ・ 発行済株式の総数又は出資の総額の3分の2以上が、複数の大企業(※)の所有に属している企業
- ・ 資本金又は出資金が5億円以上の法人に直接又は間接に100%の株式を保有されている 企業

※「大企業」とは、事業を営むもののうち、中小企業者を除くものをいう。ただし、以下に該当する者については、大企業として取り扱わないものとする。

- ・ 中小企業投資育成株式会社法に規定する中小企業投資育成株式会社
- ・ 廃止前の中小企業の創造的事業活動の促進に関する臨時措置法に規定する指定支援機関 (ベンチャー財団) と基本約定書を締結した者 (特定ベンチャーキャピタル)
- ・ 投資事業有限責任組合契約に関する法律に規定する投資事業有限責任組合

別紙 2

補助事業者等一覧

区分	事業計画名	補助事業者
1	気候変動対策を可能にする拡張ゲノム編集技術による新種苗の開発・実証	グランドグリーン株式会社
2	データ駆動型プラットフォームによる育種ビジネスの革新	ListenField 株式会社
3		株式会社フィットメトリクス
4		株式会社 Quantomics
5	みどりの食料システム戦略実現に寄与する大規模有機スマート農場の開発	株式会社トクイテン
6	革新的乾燥技術「過熱蒸煎機」による、りんご搾汁残渣を活用した新たなエコフィード飼料の開発と経済合理性の確立	ASTRA FOOD PLAN 株式会社
7	森林由来の新素材「改質リグニン」及びその樹脂組成物の大規模製造に向けた技術実証	株式会社木質素研究所
8	輸出促進を実現するウニの短期実入改善システムの構築	株式会社北三陸ファクトリー
9		株式会社カロリアジャパン
10	玄米粉を高配合した完全栄養パンの開発による国産米粉原料の新規需要創出	ベースフード株式会社
11	穀物のマイナス温度下における乾式超微粉粉砕方の製造技術の実証	株式会社フィット&リカバリー
12	調理/盛付/食器仕分け業務の自動化とアプリによるメニューパーソナライズ、AI を活用した厨房オペレーション最適化を通じた次世代スマート食堂の社会実装	TechMagic 株式会社
13	お米生まれ麴育ちの機能性マイコプロテインの商用確立	Agro Ludens 株式会社
14	未利用バイオマス発酵技術を活用したアップサイクルグリーンフード素材の量産実証	株式会社ファーマンステーション
15	農産物粉末化技術のスケールアップおよび未利用食品粉末活用の実証	株式会社グリーンエース
16	リアルな肉に近似な次世代食品の実現に向けた実装化計画	ディーツフードプランニング株式会社

別紙 3

業務費用区分

- (1) 本業務の対象とする経費は、業務の遂行に直接必要な経費及び業務成果の取りまとめに必要な経費であり、具体的には以下のとおりとする。

区 分	内 容
直接経費	人件費、旅費、会場費、会場費、謝金、備品費(10万円未満に限る)、消耗品費 印刷製本費、補助職員人件費、その他諸経費(通信運搬費(郵便料、運送代、通信・電話料等)、光熱水費(電気、水道、ガス)、設備の修繕・保守費、文献購入費、広報費等)、再委託費、外注費
一般管理費	一般管理費

- (2) 直接経費として計上できない経費

- ・建物等施設に関する経費
- ・業務内容に照らして当然備えているべき機器・備品等(机、椅子、書棚等の什器類、事務機器等)
- ・業務実施中に発生した事故・災害の処理のための経費
- ・その他事業に関係のない経費

- (3) 一般管理費の算出

本契約における一般管理費率は、契約の相手方の規程と8%を比較して、いずれか低い方又は規程がない場合は契約時の直近3ヶ年の損益計算書等により算出された一般管理費率と8%を比較して、いずれか低い方を上限とする。

- (4) 再委託、外注費にかかる精算処理等

本契約において、再委託、外注費を計上する業務がある場合は、個別協議にて決定するものとする。

また、グループ企業との取引であることを契約の相手方の選定理由とする契約は原則認められず、経済性の観点から、見積合せ等価格競争を行い、最も低廉な価格を提示した者等を選定すること。

調達における情報セキュリティ基準

1 趣旨

調達における情報セキュリティ基準（以下「本基準」という。）は、農林水産省が行う調達を受注した法人（以下「受注者」という。）において当該調達に係る保護すべき情報の適切な管理を目指し、農林水産省として求める対策を定めるものであり、受注者は、情報セキュリティ対策を本基準に則り実施するものとする。

なお、従来から情報セキュリティ対策を実施している場合は、本基準に則り、必要に応じ新たに追加又は拡充を実施するものとする。また、本基準において示されている対策について、合理的な理由がある場合は、適用の除外について、農林水産省の確認を受けることができる。

2 定義

本基準において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

- (1)「保護すべき情報」とは、農林水産省の所掌事務に係る情報であって公になっていないもののうち、農林水産省職員以外の者への漏えいが我が国の安全保障、農林水産業の振興又は所掌事務の遂行に支障を与えるおそれがあるため、特に受注者における情報管理の徹底を図ることが必要となる情報をいう。
- (2)「保護すべき文書等」とは、保護すべき情報に属する文書（保護すべきデータが保存された可搬記憶媒体を含む。）、図画及び物件をいう。
- (3)「保護すべきデータ」とは、保護すべき情報に属する電子データをいう。
- (4)「情報セキュリティ」とは、保護すべき情報の機密性、完全性及び可用性を維持することをいう。
- (5)「機密性」とは、情報に関して、アクセスを許可された者だけがこれにアクセスできる特性をいう。
- (6)「完全性」とは、情報が破壊、改ざん又は消去されていない特性をいう。
- (7)「可用性」とは、情報へのアクセスを許可された者が、必要時に中断することなく、情報にアクセスできる特性をいう。
- (8)「情報セキュリティ実施手順」とは、本基準に基づき、受注者が受注した業務に係る情報セキュリティ対策についての実施手順を定めたものをいう。
- (9)「情報セキュリティ事故」とは、保護すべき情報の漏えい、紛失、破壊

等の事故をいう。

- (10) 「情報セキュリティ事象」とは、情報セキュリティ実施手順への違反のおそれのある状態及び情報セキュリティ事故につながるおそれのある状態をいう。
- (11) 「経営者等」とは、経営者又は農林水産省が行う調達を処理する部門責任者をいう。
- (12) 「下請負者」とは、契約の履行に係る作業に従事する全ての事業者（農林水産省と直接契約関係にある者を除く。）をいう。
- (13) 「第三者」とは、法人又は自然人としての農林水産省と直接契約関係にある者以外の全ての者をいい、親会社等、兄弟会社、地域統括会社、ブランド・ライセンサー、フランチャイザー、コンサルタントその他の農林水産省と直接契約関係にある者に対して指導、監督、業務支援、助言、監査等を行うものを含む。
- (14) 「親会社等」とは、会社法（平成17年法律第86号）第2条第4号の2に規定する「親会社等」をいう。
- (15) 「兄弟会社」とは、同一の会社を親会社とする子会社同士をいい、当該子会社は会社法第847条の2第2号に規定する「完全子会社」、会社計算規則（平成18年法務省令第13号）第2条第3項第19号に規定する「連結子会社」及び同項第20号に規定する「非連結子会社」をいう。
- (16) 「可搬記憶媒体」とは、パソコン又はその周辺機器に挿入又は接続して情報を保存することができる媒体又は機器のうち、可搬型のものをいう。
- (17) 「情報システム」とは、ハードウェア、ソフトウェア（プログラムの集合体をいう。）、ネットワーク又は記憶媒体で構成されるものであって、これら全体で業務処理を行うものをいう。
- (18) 「取扱施設」とは、保護すべき情報の取扱い及び保管を行う施設をいう。
- (19) 「保護システム」とは、保護すべき情報を取り扱う情報システムをいう。
- (20) 「利用者」とは、情報システムを利用する者をいう。
- (21) 「悪意のあるコード」とは、情報システムが提供する機能を妨害するプログラムの総称であり、コンピュータウイルス、スパイウェア等をいう。
- (22) 「伝達」とは、知識を相手方に伝えることであって、有体物である文書等の送達を伴わないものをいう。
- (23) 「送達」とは、有体物である文書等を物理的に移動させることをいう。
- (24) 「電子メール等」とは、電子メールの送受信、ファイルの共有及びファイルの送受信をいう。
- (25) 「電子政府推奨暗号等」とは、電子政府推奨暗号リストに記載されている暗号等又は電子政府推奨暗号選定の際の評価方法により評価した場合

に電子政府推奨暗号と同等以上の解読困難な強度を有する秘匿化の手段をいう。

(26)「秘匿化」とは、情報の内容又は情報の存在を隠すことを目的に、情報の変換等を行うことをいう。

(27)「管理者権限」とは、情報システムの管理（利用者の登録及び登録削除、利用者のアクセス制御等）をするために付与される権限をいう。

3 対象

(1) 対象とする情報は、受注者において取り扱われる保護すべき情報とする。

(2) 対象者は、受注者において保護すべき情報に接する全ての者（保護すべき情報に接する役員（持分会社にあっては社員を含む。以下同じ。）、管理職員、派遣職員、契約社員、パート、アルバイト等を含む。この場合において、当該者が、自らが保護すべき情報に接しているとの認識の有無を問わない。以下「取扱者」という。）とする。

4 情報セキュリティ実施手順

(1) 情報セキュリティ実施手順の作成

受注者は、5から12までの内容を含んだ情報セキュリティ実施手順を作成するものとし、その際及び変更する場合は、本基準との適合性について、農林水産省の確認を受けるものとする。

(2) 情報セキュリティ実施手順の周知

経営者等は、情報セキュリティ実施手順を、保護すべき情報を取り扱う可能性のある全ての者（取扱者を含む。）に周知しなければならない。また、保護すべき情報を取り扱う下請負者に周知しなければならない。

(3) 情報セキュリティ実施手順の見直し

受注者は、情報セキュリティ実施手順を適切、有効及び妥当なものとするため、定期的な見直しを実施するとともに、情報セキュリティに係る重大な変化及び情報セキュリティ事故が発生した場合は、その都度、見直しを実施し、必要に応じて情報セキュリティ実施手順を変更しなければならない。

5 組織のセキュリティ

(1) 内部組織

ア 情報セキュリティに対する経営者等の責任

経営者等は、情報セキュリティの責任に関する明瞭な方向付け、自らの関与の明示、責任の明確な割当て及び情報セキュリティ実施手順の

承認等を通して、組織内における情報セキュリティの確保に不断に努めるものとし、組織内において、取扱者以外の役員、管理職員等を含む従業員その他の全ての構成員について、取扱者以外の者は保護すべき情報に接してはならず、かつ、職務上の下級者等に対してその提供を要求してはならない。

イ 責任の割当て

受注者は、保護すべき情報に係る全ての情報セキュリティの責任を明確化するため、保護すべき情報の管理全般に係る総括的な責任者及び保護すべき情報ごとに管理責任者（以下「管理者」という。）を指定しなければならない。

ウ 守秘義務及び目的外利用の禁止

受注者は、取扱者との間で守秘義務及び目的外利用の禁止を定めた契約又は合意をするものとし、要求事項の定期的な見直しを実施するとともに、情報セキュリティに係る状況の変化及び情報セキュリティ事故が発生した場合は、その都度、見直しを実施した上、必要に応じて要求事項を修正しなければならない。

エ 情報セキュリティの実施状況の調査

受注者は、情報セキュリティの実施状況について、定期的及び情報セキュリティの実施に係る重大な変化が発生した場合には、調査を実施し、その結果を保存しなければならない。また、必要に応じて是正措置を取らなければならない。

(2) 保護すべき情報を取り扱う下請負者

受注者は、当該契約の履行に当たり、保護すべき情報を取り扱う業務を下請負者に委託する場合、本基準に基づく情報セキュリティ対策の実施を当該下請負者との間で契約し、当該業務を始める前に、農林水産省が定める確認事項に基づき、当該下請負者において情報セキュリティが確保されることを確認した後、農林水産省に届け出なければならない。

(3) 第三者への開示の禁止

ア 第三者への開示の禁止

受注者は、第三者（当該保護すべき情報を取り扱う業務に係る契約の相手方を除く。）に保護すべき情報を開示又は漏えいしてはならない。やむを得ず保護すべき情報を第三者（当該保護すべき情報を取り扱う業務に係る契約の相手方を除く。）に開示しようとする場合には、あらかじめ、農林水産省が定める確認事項に基づき、開示先において情報セキュリティが確保されることを確認した後、書面により農林水産省

の許可を受けなければならない。

イ 第三者の取扱施設への立入りの禁止

受注者は、想定されるリスクを明確にした上で、当該リスクへの対策を講じた場合を除き、取扱施設に第三者を立ち入らせてはならない。

6 保護すべき情報の管理

(1) 分類の指針

受注者は、保護すべき情報を明確に分類することができる情報の分類体系を定めなければならない。

(2) 保護すべき情報の取扱い

ア 保護すべき情報の目録

受注者は、保護すべき情報の現状（保管場所等）が分かる目録を作成し、維持しなければならない。

イ 取扱いの管理策

(ア) 受注者は、保護すべき情報を接受、作成、製作、複製、持出し（貸出しを含む。）、破棄又は抹消する場合は、その旨を記録しなければならない。

(イ) 受注者は、保護すべき情報を個人が所有する情報システム及び可搬記憶媒体において取り扱ってはならず、やむを得ない場合は、あらかじめ、書面により農林水産省の許可を得なければならない。

(ウ) 受注者は、農林水産省から特段の指示がない限り、契約終了後、保護すべき情報を返却、提出、破棄又は抹消しなければならない。ただし、当該情報を引き続き保有する必要があるときは、その理由を添えて農林水産省に協議を求めることができる。

ウ 保護すべき情報の保管等

受注者は、保護すべき情報を施錠したロッカー等に保管し、その鍵を適切に管理しなければならない。また、保護すべき情報を保護すべきデータとして保存する場合には、暗号技術を用いることを推奨する。

エ 保護すべき情報の持出し

受注者は、経営者等が持出しに伴うリスクを回避することができる判断した場合を除き、保護すべき情報を取扱施設外に持ち出してはならない。

オ 保護すべき情報の破棄及び抹消

受注者は、接受、作成、製作又は複製した保護すべき情報を復元できないように細断等確実な方法により破棄又は抹消し、その旨を記録するものとする。

なお、保護すべきデータを保存した可搬記憶媒体を廃棄する場合も同

様とする。

カ 該当部分の明示

(ア) 受注者は、保護すべき情報を作成、製作又は複製した場合は、下線若しくは枠組みによる明示又は文頭及び文末に括弧を付すことによる明示等の措置を行うものとする。

(イ) 受注者は、契約の目的物が保護すべき情報を含むものである場合には、当該契約の履行の一環として収集、整理、作成等した一切の情報について、農林水産省が当該情報を保護すべき情報には当たらないと確認するまでは、保護すべき情報として取り扱わなければならない。ただし、保護すべき情報の指定を解除する必要がある場合には、その理由を添えて農林水産省に協議を求めることができる。

7 人的セキュリティ

(1) 経営者等の責任

経営者等は、保護すべき情報の取扱者の指定の範囲を必要最小限とするとともに、ふさわしいと認める者を充て、情報セキュリティ実施手順を遵守させなければならない。また、農林水産省との契約に違反する行為を求められた場合にこれを拒む権利を実効性をもって法的に保障されない者を当該ふさわしいと認める者としてはならない。

(2) 取扱者名簿

受注者は、取扱者名簿（取扱者の氏名、生年月日、所属する部署、役職、国籍等が記載されたものをいう。以下同じ。）を作成又は更新し、その都度、保護すべき情報を取り扱う前に農林水産省に届け出て同意を得なければならない。また、受注者は、下請負者及び保護すべき情報を開示する第三者の取扱者名簿についても、同様の措置を取らなければならない。

(3) 取扱者の責任

取扱者は、在職中及び離職後において、契約の履行において知り得た保護すべき情報を第三者（当該保護すべき情報を取り扱う業務に係る契約の相手方を除く。）に漏えいしてはならない。

(4) 保護すべき情報の返却等

受注者は、取扱者の雇用契約の終了又は取扱者との契約合意内容の変更に伴い、保護すべき情報に接する必要がなくなった場合には、取扱者が保有する保護すべき情報を管理者へ返却又は提出させなければならない。

8 物理的及び環境的セキュリティ

(1) 取扱施設

ア 取扱施設の指定

受注者は、保護すべき情報の取扱施設（日本国内に限る。）を明確に定めなければならない。

イ 物理的セキュリティ境界

受注者は、保護すべき情報及び保護システムのある区域を保護するために、物理的セキュリティ境界（例えば、壁、カード制御による入口、有人の受付）を用いなければならない。

ウ 物理的入退管理策

受注者は、取扱施設への立入りを適切な入退管理策により許可された者だけに制限するとともに、取扱施設への第三者の立入りを記録し、保管しなければならない。

エ 取扱施設での作業

受注者は、保護すべき情報に係る作業は、機密性に配慮しなければならない。また、取扱施設において通信機器（携帯電話等）及び記録装置（ボイスレコーダー及びデジカメ等）を利用する場合は、経営者等の許可を得なければならない。

(2) 保護システムの物理的保全対策

ア 保護システムの設置及び保護

受注者は、保護システムを設置する場合、不正なアクセス及び盗難等から保護するため、施錠できるラック等に設置又はワイヤーで固定する等の措置を取らなければならない。

イ 保護システムの持出し

受注者は、経営者等が持出しに伴うリスクを回避することができると判断した場合を除き、保護システムを取扱施設外に持ち出してはならない。

ウ 保護システムの保守及び点検

受注者は、第三者により保護システムの保守及び点検を行う場合、必要に応じて、保護すべき情報を復元できない状態にする、又は取り外す等の処置をしなければならない。

エ 保護システムの破棄又は再利用

受注者は、保護システムを破棄する場合は、保護すべきデータが復元できない状態であることを点検した上、記憶媒体を物理的に破壊した後、破棄し、その旨を記録しなければならない。また、再利用する場合は、保護すべきデータが復元できない状態であることを点検した後でなければ再利用してはならない。

9 通信及び運用管理

(1) 操作手順書

受注者は、保護システムの操作手順書を整備し、維持するとともに、利用者が利用可能な状態にしなければならない。

(2) 悪意のあるコードからの保護

受注者は、保護システムを最新の状態に更新されたウイルス対策ソフトウェア等を用いて、少なくとも週1回以上フルスキャンを行うことなどにより、悪意のあるコードから保護しなければならない。なお、1週間以上電源の切られた状態にあるサーバ又はパソコン（以下「サーバ等」という。）については、再度の電源投入時に当該処置を行うものとする。

(3) 保護システムのバックアップの管理

受注者は、保護システムを可搬記憶媒体にバックアップする場合、可搬記憶媒体は（4）に沿った取扱いをしなければならない。

(4) 可搬記憶媒体の取扱い

ア 可搬記憶媒体の管理

受注者は、保護すべきデータを保存した可搬記憶媒体を施錠したロッカー等において集中保管し、適切に鍵を管理しなければならない。また、可搬記憶媒体は、保護すべき情報とそれ以外を容易に区別できる処置をしなければならない。

イ 可搬記憶媒体への保存

受注者は、保護すべきデータを可搬記憶媒体に保存する場合、暗号技術を用いなければならない。ただし、農林水産省への納入又は提出物件等である場合には、農林水産省の指示に従うものとする。

ウ 可搬記憶媒体の廃棄又は再利用

受注者は、保護すべきデータの保存に利用した可搬記憶媒体を廃棄する場合、保護すべきデータが復元できない状態であることを点検した上、可搬記憶媒体を物理的に破壊した後、廃棄し、その旨を記録しなければならない。また、再利用する場合は、保護すべきデータが復元できない状態であることを点検した後でなければ再利用してはならない。

(5) 情報の伝達及び送達

ア 保護すべき情報の伝達

受注者は、通信機器（携帯電話等）を用いて保護すべき情報を伝達する場合、伝達に伴うリスクを経営者等が判断の上、必要に応じそのリスクから保護しなければならない。

イ 伝達及び送達に関する合意

受注者は、保護すべき情報を伝達又は送達する場合には、守秘義務を定めた契約又は合意した相手に対してのみ行わなければならない。

ウ 送達中の管理策

受注者は、保護すべき文書等を送達する場合には、送達途中において、許可されていないアクセス及び不正使用等から保護しなければならない。

エ 保護すべきデータの伝達

受注者は、保護すべきデータを伝達する場合には、保護すべきデータを既に暗号技術を用いて保存していること、通信事業者の回線区間に暗号技術を用いること又は電子メール等に暗号技術を用いることの違いによって、保護すべきデータを保護しなければならない。ただし、漏えいのおそれがないと認められる取扱施設内において、有線で伝達が行われる場合は、この限りでない。

(6) 外部からの接続

受注者は、保護システムに外部から接続（モバイルコンピューティング、テレワーキング等）を許可する場合は、利用者の認証を行うとともに、暗号技術を用いなければならない。

(7) 電子政府推奨暗号等の利用

受注者は、暗号技術を用いる場合、電子政府推奨暗号等を用いなければならない。なお、電子政府推奨暗号等を用いることが困難な場合は、その他の秘匿化技術を用いる等により保護すべき情報を保護しなければならない。

(8) ソフトウェアの導入管理

受注者は、保護システムへソフトウェアを導入する場合、あらかじめ当該システムの管理者によりソフトウェアの安全性の確認を受けなければならない。

(9) システムユーティリティの使用

受注者は、保護システムにおいてオペレーティングシステム及びソフトウェアによる制御を無効にすることができるシステムユーティリティの使用を制限しなければならない。

(10) 技術的脆弱性の管理

受注者は、技術的脆弱性に関する情報について時期を失せず取得し、経営者等が判断の上、適切に対処しなければならない。

(11) 監視

ア ログの取得

受注者は、保護システムにおいて、保護すべき情報へのアクセス等を

記録したログを取得しなければならない。

イ ログの保管

受注者は、取得したログを記録のあった日から少なくとも3か月以上保存するとともに、定期的に点検しなければならない。

ウ ログの保護

受注者は、ログを改ざん及び許可されていないアクセスから保護しなければならない。

エ 日付及び時刻の同期

受注者は、保護システム及びネットワークを通じて保護システムにアクセス可能な情報システムの日付及び時刻を定期的に合わせなければならない。

オ 常時監視

受注者は、保護システムがインターネットやインターネットと接点を有する情報システム（クラウドサービスを含む。）から物理的又は論理的に分離されていない場合は、常時監視を行わなければならない。

10 アクセス制御

(1) 利用者の管理

ア 利用者の登録管理

受注者は、取扱者による保護システムへのアクセスを許可し、適切なアクセス権を付与するため、保護システムの利用者としての登録及び登録の削除をしなければならない。

イ パスワードの割当て

受注者は、保護システムの利用者に対して初期又は仮パスワードを割り当てる場合、容易に推測されないパスワードを割り当てるものとし、機密性に配慮した方法で配付するものとする。なお、パスワードより強固な手段（生体認証等）を採用又は併用している場合は、本項目の適用を除外することができる。

ウ 管理者権限の管理

保護システムの管理者権限は、必要最低限にとどめなければならない。

エ アクセス権の見直し

受注者は、保護システムの利用者に対するアクセス権の割当てについては、定期的及び必要に応じて見直しを実施しなければならない。

(2) 利用者の責任

ア パスワードの利用

受注者は、容易に推測されないパスワードを保護システムの利用者に

設定させ、当該パスワードを複数の機器やサービスで再使用させないとともに、流出時には直ちに変更させなければならない。なお、パスワードより強固な手段（生体認証等）を採用又は併用している場合は、本項目の適用を除外することができる。

イ 無人状態にある保護システム対策

受注者は、保護システムが無人状態に置かれる場合、機密性に配慮した措置を取らなければならない。

(3) ネットワークのアクセス制御

ア 機能の制限

受注者は、保護システムの利用者の職務内容に応じて、利用できる機能を制限し提供しなければならない。

イ ネットワークの接続制御

受注者は、保護システムの共有ネットワーク（インターネット等）への接続に際しては、接続に伴うリスクから保護しなければならない。

(4) オペレーティングシステムのアクセス制御

ア セキュリティに配慮したログオン手順

受注者は、利用者が保護システムを利用する場合、セキュリティに配慮した手順により、ログオンさせなければならない。

イ 利用者の識別及び認証

受注者は、保護システムの利用者ごとに一意な識別子（ユーザーID、ユーザー名等）を保有させなければならない。

ウ パスワード管理システム

保護システムは、パスワードの不正使用を防止する機能（パスワードの再使用を防止する機能等）を有さなければならない。

11 情報セキュリティ事故等の管理

(1) 情報セキュリティ事故等の報告

ア 受注者は、情報セキュリティ事故が発生したときは、適切な措置を講じるとともに、直ちに把握しうる限りの全ての内容を、その後速やかに詳細を農林水産省に報告しなければならない。

イ 次に掲げる場合において、受注者は、適切な措置を講じるとともに、直ちに把握しうる限りの全ての内容を、その後速やかに詳細を農林水産省に報告しなければならない。

(ア) 保護すべき情報が保存されたサーバ等に悪意のあるコードへの感染又は不正アクセスが認められた場合

(イ) 保護すべき情報が保存されているサーバ等と同一のイントラネット

に接続されているサーバ等に悪意のあるコードへの感染又は不正アクセスが認められ、保護すべき情報が保存されたサーバ等に悪意のあるコードへの感染又は不正アクセスのおそれがある場合

ウ 情報セキュリティ事故の疑い又は事故につながるおそれのある場合は、受注者は、適切な措置を講じるとともに、速やかにその詳細を農林水産省に報告しなければならない。

エ アからウまでに規定する報告のほか、保護すべき情報の漏えい、紛失、破壊等の事故が発生した可能性又は将来発生する懸念について受注者の内部又は外部から指摘があったときは、受注者は、直ちに当該可能性又は懸念の真偽を含む把握しうる限りの全ての内容を、速やかに事実関係の詳細を農林水産省に報告しなければならない。

(2) 情報セキュリティ事故等の対処等

ア 対処体制及び手順

受注者は、情報セキュリティ事故、その疑いのある場合及び情報セキュリティ事象に対処するため、対処体制、責任及び手順を定めなければならない。

イ 証拠の収集

受注者は、情報セキュリティ事故が発生した場合、その疑いのある場合及び(1)イ(ア)の場合は証拠を収集し、速やかに農林水産省に提出しなければならない。

ウ 情報セキュリティ実施手順への反映

受注者は、発生した情報セキュリティ事故、その疑いのある場合及び情報セキュリティ事象を情報セキュリティ実施手順の見直し等に反映しなければならない。

12 遵守状況等

(1) 遵守状況の確認等

ア 遵守状況の確認

受注者は、管理者の責任の範囲において、情報セキュリティ実施手順の遵守状況を確認しなければならない。

イ 技術的遵守状況の確認

受注者は、保護システムの管理者の責任の範囲において、情報セキュリティ実施手順への技術的遵守状況を確認しなければならない。

(2) 情報セキュリティの記録

受注者は、保護すべき情報に係る重要な記録（複製記録、持出記録、監査記録等）の保管期間（少なくとも契約履行後1年間）を定めた上、施錠

したロッカー等において保管又は暗号技術を用いる等により厳密に保護するとともに、適切に鍵を管理しなければならない。

(3) 監査ツールの管理

受注者は、保護システムの監査に用いるツールについて、悪用を防止するため必要最低限の使用にとどめなければならない。

(4) 農林水産省による調査

ア 調査の受入れ

受注者は、農林水産省による情報セキュリティ対策に関する調査の要求があった場合には、これを受け入れなければならない。

イ 調査への協力

受注者は、農林水産省が調査を実施する場合、農林水産省の求めに応じ必要な協力（職員又は農林水産省の指名する者の取扱施設への立入り、書類の閲覧等への協力）をしなければならない。

調達における情報セキュリティの確保に関する特約条項

(情報セキュリティ実施手順の確認)

- 第1条 乙は、契約締結後、速やかに情報セキュリティ実施手順（甲の定める「調達における情報セキュリティ基準」（以下「本基準」という。）第2項第8号に規定する「情報セキュリティ実施手順」をいう。以下同じ。）を作成し、甲の定める本基準に適合していることについて甲の確認を受けなければならない。ただし、既に甲の確認を受けた情報セキュリティ実施手順と同一である場合は、特別な指示がない限り、届出をすれば足りる。
- 2 乙は、前項により甲の確認を受けた情報セキュリティ実施手順を変更しようとするときは、あらかじめ、当該変更部分が甲の定める本基準に適合していることについて甲の確認を受けなければならない。
- 3 甲は、乙に対して情報セキュリティ実施手順及びそれらが引用している文書の提出、貸出し、又は閲覧を求めることができる。

(保護すべき情報の取扱い)

- 第2条 乙は、前条において甲の確認を受けた情報セキュリティ実施手順に基づき、この契約に関する保護すべき情報（甲の定める本基準第2項第1号に規定する「保護すべき情報」をいう。以下同じ。）を取り扱わなければならない。

(保護すべき情報の漏えい等に関する乙の責任)

- 第3条 乙は、乙の従業員又は下請負者（契約の履行に係る作業に従事する全ての事業者（乙を除く。）をいう。）の故意又は過失により保護すべき情報の漏えい、紛失、破壊等の事故があったときであっても、契約上の責任を免れることはできない。

(第三者への開示及び下請負者への委託)

- 第4条 乙は、やむを得ず保護すべき情報を第三者に開示する場合には、あらかじめ、開示先において情報セキュリティが確保されることを別紙様式に定める確認事項により確認した上で、書面により甲の許可を受けなければならない。
- 2 乙は、第三者との契約において乙の保有し、又は知り得た情報を伝達、交換、共有その他提供する約定があるときは、保護すべき情報をその対象から除く措置を講じなければならない。

- 3 乙は、契約の履行に当たり、保護すべき情報を下請負者に取り扱わせる場合には、あらかじめ、別紙様式に定める確認事項によって、当該下請負者において情報セキュリティが確保されることを確認し、その結果を甲に届け出なければならない。ただし、輸送その他の保護すべき情報を知り得ないと乙が認める業務を委託する場合は、この限りではない。

(調査)

- 第5条 甲は、仕様書等に定める情報セキュリティ対策に関する調査を行うことができる。
- 2 甲は、前項に規定する調査を行うため、甲の指名する者を乙の事業所、工場その他の関係場所に派遣することができる。
 - 3 甲は、第1項に規定する調査の結果、乙の情報セキュリティ対策が情報セキュリティ実施手順を満たしていないと認められる場合は、その是正のため必要な措置を講じるよう求めることができる。
 - 4 乙は、前項の規定による甲の求めがあったときは、速やかにその是正措置を講じなければならない。
 - 5 乙は、甲が乙の下請負者に対し調査を行うときは、甲の求めに応じ、必要な協力を行わなければならない。また、乙は、乙の下請負者が是正措置を求められた場合、講じられた措置について甲に報告しなければならない。

(事故等発生時の措置)

- 第6条 乙は、保護すべき情報の漏えい、紛失、破壊等の事故が発生したときは、適切な措置を講じるとともに、直ちに把握しうる限りの全ての内容を、その後速やかにその詳細を甲に報告しなければならない。
- 2 次に掲げる場合において、乙は、適切な措置を講じるとともに、直ちに把握しうる限りの全ての内容を、その後速やかにその詳細を甲に報告しなければならない。
 - (1) 保護すべき情報が保存されたサーバ又はパソコン（以下「サーバ等」という。）に悪意のあるコード（本基準第2項第21号に規定する「悪意のあるコード」をいう。以下同じ。）への感染又は不正アクセスが認められた場合
 - (2) 保護すべき情報が保存されているサーバ等と同一のイントラネットに接続されているサーバ等に悪意のあるコードへの感染又は不正アクセスが認められ、保護すべき情報が保存されたサーバ等に悪意のあるコードへの感染又は不正アクセスのおそれがある場合
 - 3 第1項に規定する事故について、それらの疑い又は事故につながるおそれ

のある場合は、乙は、適切な措置を講じるとともに、速やかにその詳細を甲に報告しなければならない。

- 4 前3項に規定する報告のほか、保護すべき情報の漏えい、紛失、破壊等の事故が発生した可能性又は将来発生する懸念について乙の内部又は外部から指摘があったときは、乙は、直ちに当該可能性又は懸念の真偽を含む把握しうる限りの全ての内容を、速やかに事実関係の詳細を甲に報告しなければならない。
- 5 前各項に規定する報告を受けた甲による調査については、前条の規定を準用する。
- 6 乙は、第1項に規定する事故がこの契約及び関連する物品の運用に与える影響等について調査し、その措置について甲と協議しなければならない。
- 7 第1項に規定する事故が乙の責めに帰すべき事由によるものである場合には、前項に規定する協議の結果取られる措置に必要な経費は、乙の負担とする。
- 8 前項の規定は、甲の損害賠償請求権を制限するものではない。

(契約の解除)

- 第7条 甲は、乙の責めに帰すべき事由により前条第1項に規定する事故が発生し、この契約の目的を達することができなくなった場合は、この契約の全部又は一部を解除することができる。
- 2 前項の場合においては、主たる契約条項の契約の解除に関する規定を準用する。

(契約履行後における乙の義務等)

- 第8条 第2条、第3条、第5条及び第6条の規定は、契約履行後においても準用する。ただし、当該情報が保護すべき情報でなくなった場合は、この限りではない。
- 2 甲は、本基準第6項第2号イ（ウ）の規定によるほか、業務に支障が生じるおそれがない場合は、乙に保護すべき情報の返却、提出、破棄又は抹消を求めることができる。
 - 3 乙は、前項の求めがあった場合において、保護すべき情報を引き続き保有する必要があるときは、その理由を添えて甲に協議を求めることができる。

情報セキュリティ対策実施確認事項

(事業名：)

1 下請負者名又は開示先事業者名等

- (1) 事業者名：
 (2) 委託又は開示予定年月日：
 (3) 業務の実施予定場所※：

※（下請負事業者又は開示先事業者の業務の実施予定場所を記入）

2 下請負者又は開示先事業者に対する確認事項

※ 確認事項欄の冒頭の番号及び用語の定義は、「調達における情報セキュリティ基準」（以下「本基準」という。）による。

番号	確認事項	実施 ／未 実施	実施状況の確認方法 又は 未実施の理由
1	4（2）情報セキュリティ実施手順の周知 <ul style="list-style-type: none"> ・保護すべき情報を取り扱う可能性のある全ての者に周知することを定めていること。 ・下請負者へ周知することを定めていること。 		
2	4（3）情報セキュリティ実施手順の見直し <ul style="list-style-type: none"> ・情報セキュリティ実施手順を定期的並びに重大な変化及び事故が発生した場合、見直しを実施し、必要に応じて変更することを定めていること。 		
3	5（1）ア 情報セキュリティに対する経営者等の責任 <ul style="list-style-type: none"> ・経営者等が情報セキュリティ実施手順を承認することを定めていること。 ・取扱者以外の役員（持分会社にあつては社員を含む。以下同じ。）、管理職員等を含む従業員その他の全ての構成員について、取扱者以外の者は保護すべき情報に接してはならないことを定めていること。 ・職務上の下級者等に対して、保護すべき情報の提供を要求してはならないことを定めていること。 		
4	5（1）イ 責任の割当て <ul style="list-style-type: none"> ・総括責任者を置くことを定めていること。 ・管理責任者を置くことを定めていること。 		

番号	確認事項	実施 /未 実施	実施状況の確認方法 又は 未実施の理由
5	5（１）ウ 守秘義務及び目的外利用の禁止 ・取扱者との間で守秘義務及び目的外利用の禁止を定めた契約又は合意をすることを定めていること。 ・定期的並びに状況の変化及び事故が発生した場合、要求事項の見直しを実施し、必要に応じて修正することを定めていること。		
6	5（１）エ 情報セキュリティの実施状況の調査 ・情報セキュリティの実施状況について、定期的及び重大な変化が発生した場合、調査を実施し、必要に応じて是正措置を取ることを定めていること。		
7	5（２）保護すべき情報を取り扱う下請負者 ・保護すべき情報を取り扱う業務を他の業者に再委託する場合には、以下の事項を定めていること。 ①本基準に基づく情報セキュリティ対策の実施を契約上の義務とすること ②下請負者がその実施の確認をした上で、発注者（農林水産省との直接契約関係にある者をいう。以下同じ。）の確認を得た上で、発注者を經由して農林水産省に届け出ること。 ④情報セキュリティ対策に関して農林水産省が行う調査（職員又は指名する者の立入り、資料の閲覧等）に協力すること。 ⑤調査の結果、是正措置を求められた場合、速やかに当該措置を講じ、発注者に報告すること。		

番号	確認事項	実施 / 未 実施	実施状況の確認方法 又は 未実施の理由
8	<p>5（3）ア 第三者への開示の禁止</p> <ul style="list-style-type: none"> ・第三者（法人又は自然人としての農林水産省と直接契約関係にある者以外の全ての者をいい、親会社、兄弟会社、地域統括会社、ブランド・ライセンサー、フランチャイザー、コンサルタントその他の農林水産省と直接契約関係にある者に対して指導、監督、業務支援、助言、監査等を行うものを含む。以下同じ。）への開示又は漏えいをしてはならないことを定めていること。 ・保有し、又は知り得た情報を第三者との契約において伝達、交換、共有その他提供する約定があるときは、保護すべき情報をその対象から除く措置を定めていること。 ・やむを得ず開示しようとする場合には、発注者が、開示先において本基準と同等の情報セキュリティが確保されることを確認した上で、農林水産省の許可を得ることを定めていること。 		
9	<p>5（3）イ 第三者の取扱施設への立入りの禁止</p> <ul style="list-style-type: none"> ・第三者の取扱施設への立入りを認める場合、リスクを明確にした上で対策を定めていること。 		
10	<p>6（1） 分類の指針</p> <ul style="list-style-type: none"> ・保護すべき情報を明確に分類できる分類体系を定めていること。 		
11	<p>6（2）ア 保護すべき情報の目録</p> <ul style="list-style-type: none"> ・目録の作成及び維持を定めていること。 		

番号	確認事項	実施 / 未 実施	実施状況の確認方法 又は 未実施の理由
12	6（2）イ 取扱いの管理策 <ul style="list-style-type: none"> ・取扱施設で取り扱うことを定めていること。 ・接受等を記録することを定めていること。 ・個人が所有する情報システム及び可搬記憶媒体で取り扱ってはならないことを定めていること。 ・（やむを得ない場合）事前に農林水産省の許可を得る手続を定めていること。 ・契約終了後、発注者から特段の指示がない限り、保護すべき情報を返却、提出、破棄又は抹消することを定めていること。 ・契約終了後も引き続き保護すべき情報を保有する必要がある場合には、その理由を添えて、発注者を経由して農林水産省に協議を求めることができることを定めていること。 		
13	6（2）ウ 保護すべき情報の保管等 <ul style="list-style-type: none"> ・保護すべき情報は、施錠したロッカー等において保管することを定めていること。 ・ロッカー等の鍵を適切に管理（無断での使用を防止）することを定めていること。 		
14	6（2）エ 保護すべき情報の持出し <ul style="list-style-type: none"> ・持出しに伴うリスクを回避することができると判断する場合の判断基準を定めていること。 ・持ち出す場合は記録することを定めていること。 		
15	6（2）オ 保護すべき情報の破棄及び抹消 <ul style="list-style-type: none"> ・復元できない方法による破棄又は抹消を定めていること。 ・破棄又は抹消したことを記録することを定めていること。 		

番号	確認事項	実施 / 未 実施	実施状況の確認方法 又は 未実施の理由
16	<p>6 (2) カ 該当部分の明示</p> <ul style="list-style-type: none"> ・ 保護すべき情報を作成、製作又は複製した場合、保護すべき情報である旨の表示を行うことを定めていること。 ・ 契約の目的物が保護すべき情報を含むものである場合には、当該契約の履行の一環として収集、整理、作成等した一切の情報について、農林水産省が当該情報を保護すべき情報には当たらないと確認するまでは、保護すべき情報として取り扱うことを定めていること。 ・ 保護すべき情報の指定を解除する必要がある場合には、その理由を添えて、発注者を經由して農林水産省に協議を求めることができることを定めていること。 ・ 保護すべき情報を記録する箇所を明示する及び明示の方法を定めていること。 		
17	<p>7 (1) 経営者等の責任</p> <ul style="list-style-type: none"> ・ 経営者等は取扱者の指定の範囲を必要最小限とするとともに、ふさわしいと認める者を充て、情報セキュリティ実施手順を遵守させることを定めていること。 ・ 農林水産省との契約に違反する行為を求められた場合にこれを拒む権利を実効性をもって法的に保障されない者を当該ふさわしい者と認めないことを定めていること。 		
18	<p>7 (2) 取扱者名簿</p> <ul style="list-style-type: none"> ・ 以下の内容の取扱者名簿を作成又は更新し、発注者を經由して農林水産省に届け出て同意を得ることを定めていること。 ①取扱者名簿には、取扱者の氏名、生年月日、所属する部署、役職、国籍等が記載されていること。 ②取扱者名簿には、保護すべき情報に接する全ての者（保護すべき情報に接する役員（持分会社にあっては社員を含む。以下同じ。）、管理職員、派遣社員、契約社員、パート、アルバイト等を含む。この場合において、自らが保護すべき情報に接しているとの当該者の認識の有無を問わない。）が記載されていること。 		

番号	確認事項	実施 / 未 実施	実施状況の確認方法 又は 未実施の理由
19	7（3） 取扱者の責任 ・ 在職中及び離職後においても、知り得た保護すべき情報を第三者に漏えいしてはならないことを定めていること。		
20	7（4） 保護すべき情報の返却等 ・ 保護すべき情報に接する必要が無くなった場合は、管理者へ返却又は提出することを定めていること。		
21	8（1）ア 取扱施設の指定 ・ 取扱施設（国内に限る。）を定めていること。		
22	8（1）イ 物理的セキュリティ境界 ・ 物理的セキュリティ境界を用いることを定めていること。		
23	8（1）ウ 物理的入退管理策 ・ 取扱施設への立入りは、許可された者だけに制限することを定めていること。		
24	8（1）エ 取扱施設での作業 ・ 機密性に配慮し作業することを定めていること。 ・ 通信機器及び記録装置を利用する場合は、経営者等の許可を得ること定めていること。		
25	8（2）ア 保護システムの設置及び保護 ・ 保護システムへの保護措置を実施することを定めていること。		
26	8（2）イ 保護システムの持出し ・ 持出しに伴うリスクを回避することができると判断する場合の基準を定めていること。 ・ 持出しする場合は記録することを定めていること。		

番号	確認事項	実施 / 未 実施	実施状況の確認方法 又は 未実施の理由
27	8（2）ウ 保護システムの保守及び点検 ・第三者による保守及び点検を行う場合は、必要な処置を実施することを定めていること。		
28	8（2）エ 保護システムの破棄又は再利用 ・保護すべきデータが復元できない状態であることを点検し、物理的に破壊したのち、破棄し、その旨を記録することを定めていること。 ・復元できない状態であることを点検した後、再利用することを定めていること。		
29	9（1） 操作手順書 ・操作手順書を整備し、維持することを定めていること。 ・操作手順書には、①可搬記憶媒体へ保存時の手順②可搬記憶媒体及び保護システムの破棄又は再利用の手順③電子メール等での伝達の手順④セキュリティに配慮したログオン手順についての記述又は引用がなされていること。		
30	9（2） 悪意のあるコードからの保護 ・保護システムを最新の状態に更新されたウイルス対策ソフト等を用いて、少なくとも週1回以上フルスキャンを行うことなどにより、悪意のあるコードから保護することを定めていること。（なお、1週間以上電源の切られた状態にあるサーバ又はパソコン（以下「サーバ等」という。）については、再度の電源投入時に当該処置を行うことで可）		

番号	確認事項	実施 / 未 実施	実施状況の確認方法 又は 未実施の理由
31	9（3） 保護システムのバックアップの管理 ・可搬記憶媒体へのバックアップを実施する場合、調達における情報セキュリティ基準9（4）に添った取扱いをすることを定めていること。		
32	9（4）ア 可搬記憶媒体の管理 ・保護すべき情報を保存した可搬記憶媒体を施錠したロッカー等により集中保管することを定めていること。 ・ロッカー等の鍵を適切に管理することを定めていること。 ・保護すべき情報とそれ以外を容易に区別できる処置をすることを定めていること。		
33	9（4）イ 可搬記憶媒体への保存 ・可搬記憶媒体へ保存する場合、暗号技術を用いることを定めていること。		
34	9（4）ウ 可搬記憶媒体の廃棄又は再利用 ・保護すべきデータが復元できない状態であることを点検し、物理的に破壊したのち、廃棄し、その旨を記録することを定めていること。 ・復元できない状態であることを点検した後、再利用することを定めていること。		
35	9（5）ア 保護すべき情報の伝達 ・伝達に伴うリスクから保護できると判断する場合の基準を定めていること。		
36	9（5）イ 伝達及び送達に関する合意 ・保護すべき情報の伝達及び送達は、守秘義務を定めた契約又は合意した相手に対してのみ行うことを定めていること。		

番号	確認事項	実施 ／ 未 実施	実施状況の確認方法 又は 未実施の理由
37	9（5）ウ 送達中の管理策 ・保護すべき文書等を送達する場合、許可されていないアクセス及び不正使用等から保護する方法を定めていること。		
38	9（5）エ 保護すべきデータの伝達 ・保護すべきデータを伝達する場合には、保護すべきデータを既に暗号技術を用いて保存していること、通信事業者の回線区間に暗号技術を用いること又は電子メール等に暗号技術を用いることのいずれかによって、保護すべきデータを保護しなければならないことを定めていること（漏えいのおそれのない取扱施設内で有線での伝達をする場合を除く。）。		
39	9（6） 外部からの接続 ・外部からの接続を許可する場合は、利用者の認証を行い、かつ、暗号技術を用いることを定めていること。		
40	9（7） 電子政府推奨暗号等の利用 ・暗号技術を用いる場合には、電子政府推奨暗号等を用いることを定めていること。 ・やむを得ず電子政府推奨暗号等を使用できない場合は、その他の秘匿化技術を用いることを定めていること。		
41	9（8） ソフトウェアの導入管理 ・導入するソフトウェアの安全性を確認することを定めていること。		
42	9（9） システムユーティリティの使用 ・システムユーティリティの使用を制限することを定めていること。		
43	9（10） 技術的脆弱性の管理 ・脆弱性に関する情報を取得すること及び適切に対処することを定めていること。		

番号	確認事項	実施 / 未 実施	実施状況の確認方法 又は 未実施の理由
44	9 (11) ア ログ取得 ・利用者の保護すべき情報へのアクセス等を記録したログを取得することを定めていること。		
45	9 (11) イ ログの保管 ・取得したログを記録のあった日から少なくとも3か月以上保存するとともに、定期的に点検することを定めていること。		
46	9 (11) ウ ログの保護 ・ログを改ざん及び許可されていないアクセスから保護することを定めていること。		
47	9 (11) エ 日付及び時刻の同期 ・保護システム及びネットワークを通じて保護システムにアクセス可能な情報システムの日付及び時刻を定期的に合わせることを定めていること。		
48	9 (11) オ 常時監視 ・保護システムがインターネットやインターネットと接点を有する情報システム（クラウドサービスを含む。）から物理的論理的に分離されていない場合には、常時監視を行うことを定めていること。		
49	10 (1) ア 利用者の登録管理 ・保護システムの利用者の登録及び登録削除をすることを定めていること。		
50	10 (1) イ パスワードの割当て ・初期又は仮パスワードは、容易に推測されないものとするとともに、機密性を配慮した方法で配付することを定めていること（パスワードより強固な手段を併用又は採用している場合はこの限りでない。）。		
51	10 (1) ウ 管理者権限の管理 ・管理者権限の利用は必要最低限とすることを定めていること。		

番号	確認事項	実施 / 未 実施	実施状況の確認方法 又は 未実施の理由
52	10（1）エ アクセス権の見直し ・保護システムの利用者のアクセス権の割当てを定期的及び必要に応じて見直すことを定めていること。		
53	10（2）ア パスワードの利用 ・保護システムの利用者は、容易に推測されないパスワードを選択しなければならないことを定めていること（パスワードより強固な手段を併用又は採用している場合はこの限りでない。）。		
54	10（2）イ 無人状態にある保護システム対策 ・保護システムが無人状態に置かれる場合、機密性を配慮した措置を実施することを定めていること。		
55	10（3）ア 機能の制限 ・保護システムの利用者の職務内容に応じて、利用できる機能を制限することを定めていること。		
56	10（3）イ ネットワークの接続制御 ・保護システムを共有ネットワークへ接続する場合、接続に伴うリスクから保護することを定めていること（FW設置など）。		
57	10（4）ア セキュリティに配慮したログオン手順 ・保護システムの利用者は、セキュリティに配慮した手順でログオンすることを定めていること。		
58	10（4）イ 利用者の識別及び認証 ・保護システムの利用者ごとに一意な識別子（ユーザーID、ユーザー名等）を保有させることを定めていること。		

番号	確認事項	実施 / 未 実施	実施状況の確認方法 又は 未実施の理由
59	10（４）ウ パスワード管理システム ・保護システムは、パスワードの不正使用を防止する機能を有さなければならないことを定めていること。		
60	11（１） 情報セキュリティの事故等の報告 ・情報セキュリティ事故等に関する下記のそれぞれの事項について、以下のことが規定されていること。 ア 情報セキュリティ事故が発生したときは、適切な措置を講じるとともに、直ちに把握し得る限りの全ての内容を、その後速やかにその詳細を発注者に報告しなければならない。 イ 次の場合において、適切な措置を講じるとともに、直ちに把握し得る限りの全ての内容を、その後速やかにその詳細を発注者に報告しなければならない。 （ア）保護すべき情報が保存されたサーバ等に悪意のあるコードへの感染又は不正アクセスが認められた場合 （イ）保護すべき情報が保存されているサーバ等と同一のイントラネットに接続されているサーバ等に悪意のあるコードへの感染又は不正アクセスが認められ、保護すべき情報が保存されたサーバ等に悪意のあるコードへの感染又は不正アクセスのおそれがある場合 ウ 情報セキュリティ事故の疑い又は事故につながるおそれのある場合は、適切な措置を講じるとともに、速やかに、その詳細を発注者に報告しなければならない。 エ アからウまでに規定する報告のほか、保護すべき情報の漏えい、紛失、破壊等の事故が発生した可能性又は将来発生する懸念について、内部又は外部から指摘があったときは、直ちに当該可能性又は懸念の真偽を含む把握し得る限りの全ての内容を、速やかに事実関係の詳細を発注者に報告しなければならない。		

番号	確認事項	実施 / 未 実施	実施状況の確認方法 又は 未実施の理由
61	11（２）ア 対処体制及び手順 ・情報セキュリティ事故（情報セキュリティ事故の疑いのある場合を含む。以下同じ。）及び事象に対処するため、対処体制、責任及び手順を定めていること。		
62	11（２）イ 証拠の収集 ・情報セキュリティ事故が発生した場合（保護すべき情報が保存されたサーバ等に悪意のあるコードへの感染が認められた場合を含む。）、証拠を収集し、速やかに発注者へ提出することを定めていること。		
63	11（２）ウ 情報セキュリティ実施手順への反映 ・情報セキュリティ実施手順の見直しに、情報セキュリティ事故及び事象を反映することを定めていること。		
64	12（１）ア 遵守状況の確認 ・管理者の責任の範囲において、情報セキュリティ実施手順の遵守状況の確認を定めていること。		
65	12（１）イ 技術的遵守状況の確認 ・保護システムの管理者の責任の範囲において、情報セキュリティ実施手順への技術的遵守状況を確認することを定めていること。		
66	12（２）情報セキュリティの記録 ・保護すべき情報に係る重要な記録の保管期間を定めていること。 ・重要な記録は、施錠したロッカー等において保管又は暗号技術を用いる等厳密に保護することを定めていること。 ・適切に鍵を管理することを定めていること。		
67	12（３）監査ツールの管理 ・保護システムの監査に用いるツールは、悪用を防止するため、必要最低限の使用にとどめることを定めていること。		

番号	確認事項	実施 / 未 実施	実施状況の確認方法 又は 未実施の理由
68	12（４）農林水産省による調査 ・農林水産省による情報セキュリティ対策に関する調査を受け入れること及び必要な協力（職員又は指名する者の立入り、書類の閲覧等）をすることを定めていること。		
確認年月日： 確認者（企業名、所属、役職、氏名）： 印			

注：未実施の理由については、実施する必要がないと認められる合理的な理由を記すこと。

(様式1)

受付番号

※記載不要

公益社団法人 農林水産・食品産業技術振興協会
理事長 藤本 潔 あて

「農林水産省中小企業イノベーション創出推進事業（SBIRフェーズ3基金事業）
にかかる経理支援委託業務」応募申請書

申請者	法人番号（*）	
	企業・団体名	
	代表者役職・氏名	
	所在地	
連絡担当窓口	氏名（ふりがな）	
	所属（部署名）	
	役職	
	電話番号 （代表・直通）	
	E-mail	

* 法人番号を付与されている場合には、13桁の番号記載し、法人番号を付与されていない個人事業者等の場合には、記載不要。

(様式2)

受付番号

※記載不要

「農林水産省中小企業イノベーション創出推進事業 (SBIRフェーズ3基金)
にかかると經理支援委託業務」応募企画提案書

1. 受託業務実施計画

※1 「応募企画提案書作成にあたって」第6-(1)~(9)に記載した業務内容の項目(分野毎の特性に応じた業務を含む)ごとに、具体的な実施方法及び内容を記載してください。

※2 本事業の成果を高めるための具体的な提案を記載してください。(※1と記載の重複があっても構いません。)

【記載例】

- ・本事業の効率的、効果的な運営に係る提案
- ・期間中の補助事業者(スタートアップ等)への伴走支援に係る提案
- ・社会実装に向けたプロモート、サポートに係る提案 等

※3 上記※1、※2についての実施スケジュールを記載してください。

2. 実施体制

- ・実施責任者略歴及び実施者等の業務内容
- ・委託、外注を予定しているのであればその内容(申請者自身が行う業務内容(企画、立案及び業務管理部分については申請者自身が行う必要がある)、相手先の名称、相手先の選定方法、予定金額等も含む)
- ・実施体制図(二機関以上で共同実施の場合は、各機関の役割表を添付)
- ・業務管理費に対する委託・外注費の合計の割合が50%を超える場合は、相当な理由がわかる内容(「委託・外注費の額の割合が50%を超える理由書」(様式3)を提出すること。)
- ・グループ企業との取引であることのみを選定理由とする委託、外注(再委託及びそれ以下の委託を含む)は認めない。
- ・情報取扱者名簿及び情報管理体制図、社内規則等に関する資料等

<p>3. 事業実績</p> <ul style="list-style-type: none"> ・類似事業の実績（事業名、事業概要、実施年度、発注者等（自主事業の場合はその旨） ・本事業に関する専門知識・ノウハウ
<p>4. 申請者概要</p> <ul style="list-style-type: none"> ・申請者の営む主な事業を記載してください（会社概要（パンフレット）を添付することで代替可） ・申請者の財務状況（財務諸表等を添付することで代替可） ・特記事項等がある場合には併せて記載してください。
<p>5. 遵守確認事項</p> <p>下記の項目に関して宣誓（チェック）してください。</p> <p><input type="checkbox"/> 応募資格に挙げた要件を満たしていること。</p> <p><input type="checkbox"/> 一般社団法人及び一般財団法人に関する法律（平成18年法律第48号）に基づき設立された一般社団法人又は一般財団法人である場合については、同法第128条又は同法第199条に基づく貸借対照表等の公告を実施していること。</p> <p><input type="checkbox"/> 会社法等、関係法令を遵守していること。</p>
<p>6. 受託業務費総額（円）</p>
<p>I 人件費</p>
<p>II 事業費</p> <ul style="list-style-type: none"> ①旅費 ②会場費 ③謝金 ④備品費 ⑤消耗品費 ⑥印刷製本費 ⑦補助職員人件費 ⑧その他諸経費
<p>III 再委託・外注費</p>
<p>IV 一般管理費</p>
<p>総額千円</p> <p>※1 受託業務費は、各年度の実施分が分かるよう記載してください。</p> <p>※2 総額は、応募企画提案書作成要領第5の委託費の限度額内に収めて下さい。</p>

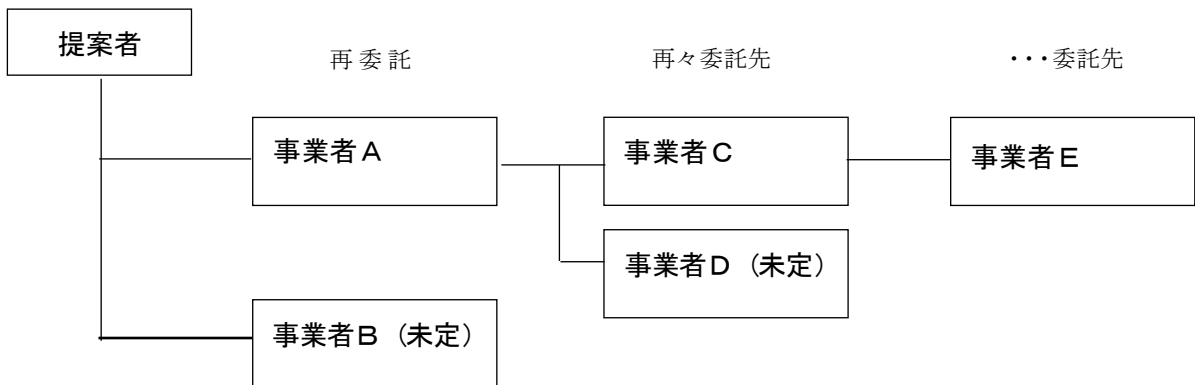
【実施体制図の記載例】

実施体制は原則、下記のように整理表で提示していただくとともに履行体制図もあわせて示してください。実施体制と契約先の事業者名、補助事業者との契約関係、住所、契約金額、契約内容がわかる資料であれば様式は問いません。

実施体制（税込み100万円以上の契約。請負その他委託の形式を問わない。）

事業者名	当社との関係	住所	契約金額（税込み）	業務の範囲
事業者A	再委託先	東京都〇〇区・・・	※算用数字を使用し、円単位で表記	※できる限り詳細に記入のこと
事業者B未定	外注先	上記記載例参照	上記記載例参照	上記記載例参照
事業者C	再々委託先 （事業者Aの委託先）	上記記載例参照	上記記載例参照	上記記載例参照
事業者D未定	再々委託先 （事業者Aの委託先）	上記記載例参照	上記記載例参照	上記記載例参照
事業者E	・・・委託先 （事業者Cの委託先）	上記記載例参照	上記記載例参照	上記記載例参照

履行体制図



(様式3)

受付番号	
※記載不要	

受託業務費総額に対する再委託費の額の割合が50%を超える理由書

1. 件名：農林水産省中小企業イノベーション創出推進事業（SBIRフェーズ3基金事業）
にかかるとの経理支援委託業務

2. 本受託業務における主要な業務（企画立案及び業務管理部分を含む）内容

--

3. 再委託先及び契約金額等

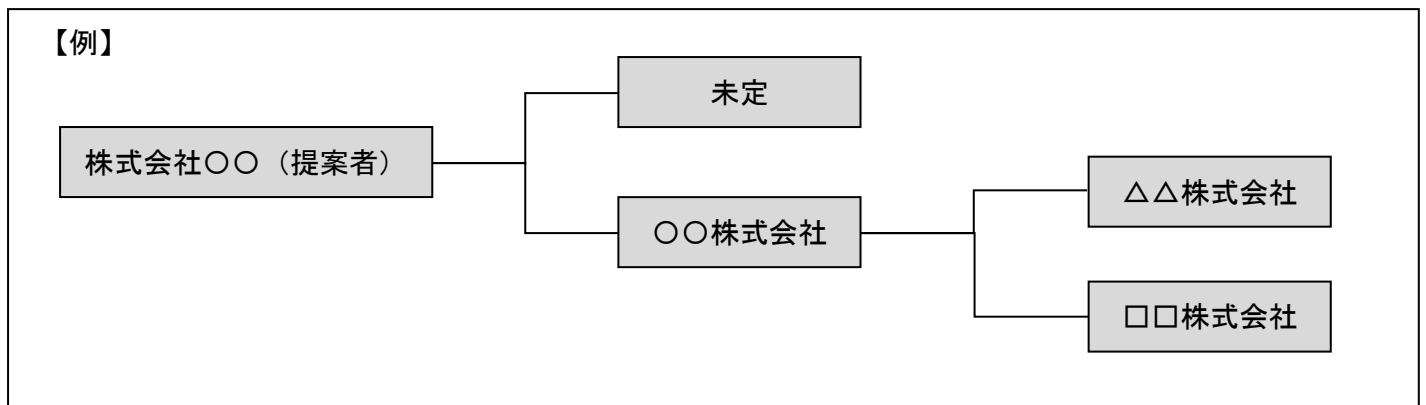
※グループ企業（関連当事者）との取引であることのみを選定理由とすることは認められません。

※再委託先及びそれ以下の委託先の契約金額を含めた情報を記載すること。

※比率は、受託業務費総額に対する再委託・外注費の割合（再々委託先及びそれ以下の委託先は記入不要）

再委託先名	精算の有無	契約金額（見込み）（円）	比率	再委託先の選定方法又は理由※	業務の内容及び範囲
【例】未定 [再委託先]	無	10,000,000	20.0%	見積合わせ
【例】〇〇（株） [再委託先]	有	20,000,000	40.0%	〇〇	コールセンター
【例】△△（株） [再々委託先]	無	2,000,000	—	〇〇
【例】□□（株） [再々委託先]	無	3,000,000	—	〇〇

4. 実施体制図



5. 再委託が必要である理由及び選定理由

Blank area for providing reasons for the need for re-commissioning and selection.