20251219財東北第7号

令和7年度中小企業地域経済政策推進事業委託費（食品製造業における生産性向上シンポジウム＆技術展示交流会実施事業）に係る開催運営業務の委託先の公募について

下記について委託先を募集しますので、受注を希望される場合は見積書等を提出して下さい。

令和8年1月6日

支出負担行為担当官
東北経済産業局総務企画部長　小林　学

1.契約概要

(1)委託業務の名称等

令和7年度中小企業地域経済政策推進事業委託費（食品製造業における生産性向上シンポジウム＆技術展示交流会実施事業）

(2)業務内容及び実施場所

仕様書のとおり

2.参加資格

オープンカウンターに参加することができる者は、見積書提出期日において、次の各号に定めるすべての事項を満たす者とする。

(1)経済産業省所管の契約に係る競争参加者資格審査事務取扱要領(昭和38年6月26日付け38会第391号)に基づいた、令和7・8・9年度経済産業省競争参加資格(全省庁統一規格)において「役務の提供等」の「B」、「C」又は「D」の等級に格付けされ、競争参加地域を「東北」としている者。

(2)予算決算及び会計令(以下、「予決令」という。)第70条の規定に該当しない者。

なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。

(3)予決令第71条の規定に該当しない者。

(4)経済産業省からの補助金交付等停止措置又は指名停止措置が講じられている者ではないこと。

(5)暴力団員による不当な行為の防止等に関する法律第2条第2号に規定する暴力団及び警察当局から排除要請がある者に該当しない者。

(6)情報管理体制として、過去3年以内に情報管理の不備を理由に経済産業省から契約を解除されている者ではないこと。

3.質問方法及び問い合わせ先

(1)質問方法

電話の受付とし、受付時間は次のとおりとする。
9時30分から12時00分まで、13時30分から16時30分まで
（但し、土曜日、日曜日等閉庁日を除く。）

(2)業務内容に関する問い合わせ先

東北経済産業局地域経済部製造産業課
電　話　022-221-4903

(3)見積書提出に関する問い合わせ先
東北経済産業局総務企画部会計課調度係
電　話　022-221-4869

4.見積書等の提出期限等
(1)提出期限
令和8年1月13日（火曜日）12時00分まで

(2)提出方法
1)電子調達システムを利用した提出
調達ポータル　https://www.p-portal.go.jp/pps-web-biz/UZA01/OZA0101/

2)紙による提出
提出先
〒980-8403 仙台市青葉区本町三丁目3番1号　仙台合同庁舎B棟4階
東北経済産業局総務企画部会計課調度係
電　話　022-221-4869
※郵送により見積書等を提出する場合は、予め電話により調度係に連絡すること。

3)提出する書類
ア　見積書（以下のURLの様式に従って提出すること。）
https://www.tohoku.meti.go.jp/kaikei/kokokushiryo/downloads/sogohyoka_15_21.xlsx

イ　2.(1)に係る競争参加資格証明書の写し。ただし、同一年度内におけるオープンカウンター案件への2回目以降の見積書提出時は不要とする。

5.電子調達システムの利用
・本件は、電子調達システムを利用した手続により、実施するものとする。
・ただし、紙による提出も可とする。

6.その他
・委託先の決定方法は、期限内に見積書を提出した者のうち、予定価格の範囲内で最低の価格をもって有効な見積書を提出した者とする。
・結果は落札者に通知するほか、局ホームページにて公表する。
・本件は、確定契約であり、契約書案をもとに契約を締結することとなるため、契約条項の内容を承知の上、見積書を提出すること。

〇確定契約書
https://www.tohoku.meti.go.jp/kaikei/format.html#itaku

・本事業の事務処理・経理処理については、「委託事業事務処理マニュアル」に従って処理することとなるため、内容を承知の上、見積書を提出すること。

〇委託事業事務処理マニュアル（R3.1）
https://www.meti.go.jp/information_2/publicoffer/jimusyori_manual.html

・別紙「委託等事業における情報セキュリティ及び個人情報の適切な管理について」の内容を承知の上で、見積書を提出すること。

契約書案

番　号

支出負担行為担当官　東北経済産業局総務企画部長　名（以下「甲」という。）は、相手方名称　代表者氏名（以下「乙」という。）と、件名（以下「委託業務」という。）について、以下により委託契約を締結する。

目　　的	甲は、委託業務の実施を乙に委託し、乙はこれを受託する。
委　託　金	○○○，○○○，○○○円 （消費税及び地方消費税額○，○○○，○○○円を含む。）
完了期限	実施計画書（仕様書）に記載のとおり
納　入　物	実施計画書（仕様書）に記載のとおり
納入場所	指示の場所
そ　の　他	約定のとおり

この契約を証するため、本契約書を２通作成し、双方記名押印の上、甲、乙それぞれ１通を保有する。

年月日

甲　宮城県仙台市青葉区本町三丁目３番１号
支出負担行為担当官
東北経済産業局総務企画部長　名

乙　［所在地］
［相手方名称］
［代表者氏名］

（別紙）

委託等事業における情報セキュリティ及び個人情報の適切な管理について

当局では、委託（請負含む。）（以下「委託等」という。）事業において、当局の業務情報を取り扱う場合等、受託者に対し、契約書（案）等に記載のとおり、委託等業務全体において、経済産業省の情報セキュリティポリシーに適合した情報セキュリティ対策の確実な実施を求めるとともに、個人情報等の取扱いに関して、漏えい事故が起こることがないように適切な管理・取扱いを求めています。

しかしながら、当局が委託等契約を結んでいる事業者によって、下記のとおり、局保有個人情報が漏えいした事案が複数発生しております。

情報セキュリティ及び個人情報に関する事故は、被害者に多大な迷惑をかけるだけではなく、当局及び委託等事業者の信用を失墜させるものです。

また、事故が発生したときは、情報の回収・捜索、被害者等への個別の謝罪等の対応に、多大な労力を要することとなり、通常の業務運営に大きな支障が生じることとなります。

これらの点を踏まえ、委託等事業における情報セキュリティ対策、個人情報等の取扱いについて認識していただき、内容を承知の上で入札・公募に参加するようお願いいたします。

記

・当局保有個人情報が漏えいした事案

①委託等事業者が、書類を事業者Ａにメール送信するところ、誤って事業者Ｂにメール送信を行い、事業者Ａ及び書類に記載されていた事業者Ｃの個人情報・企業の秘匿情報が漏えい。
個人情報・企業の秘匿情報等を含む重要書類を送信する際には、宛先は正しいか送信前に再度確認（２名での確認が望ましい）するなど、細心の注意を払いメール送信する。

②委託等事業者が、イベント講師及び外部担当者にメール送信する際、TO及びCCに入力したため、個人情報が漏えい。
複数の宛先にメールを送信する場合には、BCCにアドレスを入力し送信する。

③委託等事業者が、オンラインセミナーの入室案内をメールで送付する際、Teamsの機能を利用して、必須出席者（TO）、任意出席者（CC）にメールアドレスを入力し送信したため、メールアドレスが相互に漏えい。
Teams等ではBCC機能がないため、Teams等で会議用URLを発行した後、別途の案内メールを作成した上で、BCCにアドレスを入力し送信する。

仕様書

１．業務の名称

令和７年度中小企業地域経済政策推進事業委託費（食品製造業における生産性向上シンポジウム＆技術展示交流会実施事業）

２．事業の目的

食品製造業の国内総生産は１４．２兆円（２０２３年）と、製造業の中でも輸送用機械やはん用・生産用・業務用機械に次ぐ規模の産業となっている。近年は、食とテクノロジーの融合による新たな生産プロセスや新商品開発等の取組であるフードテック分野への投資拡大や農林水産物を含む食品輸出額の増加など、市場は堅調に推移している。東北地域においても、食品製造業の域内総生産は製造業全体の約１５％（２０２２年)、雇用は約１７％（同年）を占めており、地域経済を支える重要な基幹産業となっている。

一方、食品製造業における従業員１人あたりの労働生産性（付加価値額）は、全国・東北ともに製造業平均の６５％程度（２０２３年）となっており、特に東北地域においては労働人口が全国に先駆けて減少するなか、生産現場の改善が急務となっている。生産性向上にむけては、生産プロセスの改善に資する新技術やロボット・FA 等の自動化設備の導入が重要とされているが、食品製造業においては、従来の労働集約型の製造現場が主流であり、製造業の中でも特に機械化が遅れている現状にある。

本事業では、食品製造業の生産性向上に資する手法や新技術、導入事例を提示することにより、東北地域の食品製造業の生産性向上の取組を推進することを目的とする。

３．事業内容

本事業では、以下イベントについて（１）（２）のとおり開催及び運営を行う。なお、実施にあたっては、十分な実施体制を整備するとともに、実施内容、スケジュール等について、適宜、東北経済産業局（以下「当局」という。）担当者と協議、調整すること。

また、事業の進捗状況について、定期的に当局担当者に報告を行うこと。

（１）開催概要

① 名　称：（仮称）省力化の時代に知っておきたい食品製造業の最前線
～生産現場の改革のヒント～

② 日　時：令和７年２月中旬～３月中旬を予定。
シンポジウムの時間帯は午後（４時間程度）を予定。

③ 会　場：仙台市内のアクセスの良い会議室で、概ね１００名程度が公聴できる会議室
（一面はスクリーンとし、複数名登壇可能な会議室とする）
※原則、仙台市中小企業活性化センター５階多目的ホール、もしくはそれと同程度の会場を想定

④ 開催方法：上記会場での対面開催とする。

⑤　定　員：会場１００名程度

⑥　参加対象者：東北地域の地域未来牽引企業、食品製造業、技術シーズを有するものづくり企業、食品製造業支援の業務に関わる自治体及び関係機関の職員等

⑦　内　容：食品製造業における生産性向上の取組を促進するため、省力化の取組事例や設備導入事例の紹介等を行うほか、実際の技術、製品等の紹介展示・交流を実施する。
なお、開催イメージは以下のとおり。
※同日午前に別事業にて食ビジネスにかかるイベントを実施予定であり、引き続いて午後の部での開催を想定。

【開催イメージ】

（仮称）省力化の時代に知っておきたい食品製造業の最前線
～生産現場の改革のヒント～

１３：３０～
１．開会挨拶　司会
２．技術ピッチセッション（各８分、１時間半程度）※１０社を想定
休憩（５分）
１５：００～
３．講演（３０分）
テーマ：食品工場における現場改善のススメ
登壇者：企業（代表取締役級、東京都）
休憩・準備（１０分）
１５：４０～
４．パネルディスカッション（５０分）
テーマ：食品製造業生産性向上に向けた取組
登壇社（司　会）：民間企業（代表取締役、東京都）
登壇者：行政機関（管理職級、東京都）、当局職員
民間企業　２社（代表取締役、宮城県南、福島県）
５．閉会挨拶　当局（１分）
１６：３０～
６．技術展示交流会（３０分）
※同会場後方にて、技術展示を実施
（会場後方は別事業で午前から開放しているため出展準備可能）。
食品製造業の生産性向上に資する技術シーズを有する２．企業の技術展示及び参加企業等との交流を実施する。

⑧　主　催：東北経済産業局

（２）業務内容

① 会場の確保

事業者は、撤収時間を考慮して会場の確保を行い、決定した日時で会場の予約を行うとともに、会場借料・備品借料の支払いを行うこと。なお、会場を本予約する際には当局担当者へ了承を取ること。

② 登壇者等への謝金・旅費の支払

事業者は、当局担当者が指定する登壇者等に対し謝金・旅費の必要性を確認し、事業終了後に支払を行い、支払明細を通知すること（但し、２．技術ピッチセッションの登壇者を除く）。また、事業者は法令に基づき源泉徴収を適正に行うこと。

謝金・旅費の額は当省の委託事業事務処理マニュアル※1に従い、既存の内規等に基づき設定し、処理すること。

また、謝金・旅費の支払を想定する登壇者等の役職及び所在については、（１）⑦【開催イメージ】に記載のとおり。

なお、技術展示を実施する企業には、必要性を確認のうえ、日当謝金として１社あたり１万円を支払うこと。

※1委託事業事務処理マニュアル
https://www.meti.go.jp/information_2/downloadfiles/2021_itaku_manual.pdf

③ 参加者募集

事業者は、当局と協議の上、自社 HP やメールマガジン等を用いて、参加者募集を実施する。

④ 会場設営及び運営

イベント当日、事業者は会場にスタッフ５名以上を配置し、以下ア．～ウ．を実施すること。

ア．イベント当日、会議室の備品等の設営・設置のため、スクリーン、有線マイク（２本以上）、ワイヤレスマイク（２本以上）、スピーカー（２台以上）、音響、照明の準備のほか、当局担当者と机・椅子・パーテーション・演台・司会台・展示パネル等のレイアウトを決定し、準備・配置すること。イベント終了後の原状回復を行うこと（ただし、会場の使用条件に従うこと）。

イ．当日の参加受付・司会進行、イベント実施中の立ち会いを行い、写真撮影、マイク回し等イベントが円滑に進むようスタッフを配置すること。技術展示をおこなう企業より展示品の搬出入作業の申出があった場合は、会場の必要手続きを確認し処理すること。

ウ．当日のイベント準備・進行において、当局の指示の下、円滑に運営するように努めること。

⑤ Web アンケートの作成

参加者の理解度、満足度、今後のニーズ等を確認するためのアンケート作成、実施、とりまとめ及び分析を行うこと。アンケートの内容については事前に当局担当者の確認を得ること。参加者全員からの回収を目標とし、集計結果は当局担当者に提出すること。

⑥ 事後業務内容

イベントの内容を実施報告書にまとめ、提出すること。なお、実施報告書には以下の実施概要を含むこと。

【実施概要】：イベント開催日、場所、次第、登壇者発言内容の概要、アンケート集計・分析結果等について記載すること。開催状況写真（４枚以上）を掲載すること。

⑦ その他

講師の選定、連絡調整（謝金等の支払業務、展示物の搬出入等の出展に係る調整業務、資料・URL 等当日の案内を除く。）、参加対象者への広報は当局にて実施する。ただし、登壇者との事前打ち合わせについては、同席すること。

４．納入物

実施報告書　電子媒体（Word 形式及び PDF 形式）１部

５．納入場所

東北経済産業局　地域経済部　製造産業課

６．業務実施期間（納入期限）

契約締結日から令和８年３月３１日

７．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、発注者に対し様式１による「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、住所、生年月日、所属部署、役職等が記載されたもの）を契約前に提出し、担当課室の同意を得ること。（住所、生年月日については、必ずしも契約前に提出することを要しないが、その場合であっても担当課室から求められた場合は速やかに提出すること。）なお、情報取扱者名簿は、委託業務の遂行のため最低限必要な範囲で情報取扱者を掲載すること。

（確保すべき履行体制）

契約を履行する一環として契約相手方が収集、整理、作成等した一切の情報が、 経済産業省が保護を要さないと確認するまでは、情報取扱者名簿に記載のある者以 外に伝達又は漏えいされないことを保証する履行体制を有していること。

（２）本事業で知り得た一切の情報について、情報取扱者以外の者に開示又は漏えいしてはならないものとする。ただし、担当課室の承認を得た場合は、この限りではない。

（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、予め担当課室へ届出を行い、同意を得なければならない。

８．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。

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。

１０．留意事項

（１）事業実施にあたり、トラブルが発生しないよう十分に注意すること。万が一、トラブルが発生した場合、速やかに当局担当者に状況を報告すること。

（２）本事業の実施に際して、当局と適宜打ち合わせを行い、仕様書に定める以外の事項等については、当局担当者と協議すること。

（３）本事業で生じた知的財産及び納入物（チラシデータや報告書等）にかかる使用及び処分に関する一切の権利は、当局に帰属するものとする。

（４）報告書等に掲載する図面、写真等を他の文献等から転載する場合には、出典を明らかにするとともに、著作権者からの利用許諾を得ること。また、利用許諾を得た 図面、写真等の情報を一覧にまとめ、転載許諾書の写しとともに当局に提出すること。

（５）謝金については、既存の内部規定などに基づき適切な経理処理を行うこと。

（６）イベントの集客にあたり、謝金等の便宜提供による参加者募集を禁止する。

１１．本件に関する問い合わせ先

〒980-8403 仙台市青葉区本町３－３－１

東北経済産業局 地域経済部 製造産業課（六沢、櫻井、澤谷）

TEL:022-221-4903

R7-U-1
（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、上記 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。

【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。

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、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。

R7-U-1
別紙

令和　　年　　月　　日

支出負担行為担当官

東北経済産業局総務企画部長　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	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	

8）	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）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。 （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、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。	
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））。）

（様式１）

情報取扱者名簿及び情報管理体制図

①情報取扱者名簿

		氏名	個人住所	生年月日	所属部署	役職	パスポート番号及び国籍（※４）
情報管理責任者（※１）	A						
情報取扱管理者（※２）	B						
	C						
業務従事者（※３）	D						
	E						
再委託先	F						

（※１）受託事業者としての情報取扱の全ての責任を有する者。必ず明記すること。

（※２）本事業の遂行にあたって主に保護すべき情報を取り扱う者ではないが、本事業の進捗状況などの管理を行うもので、保護すべき情報を取り扱う可能性のある者。

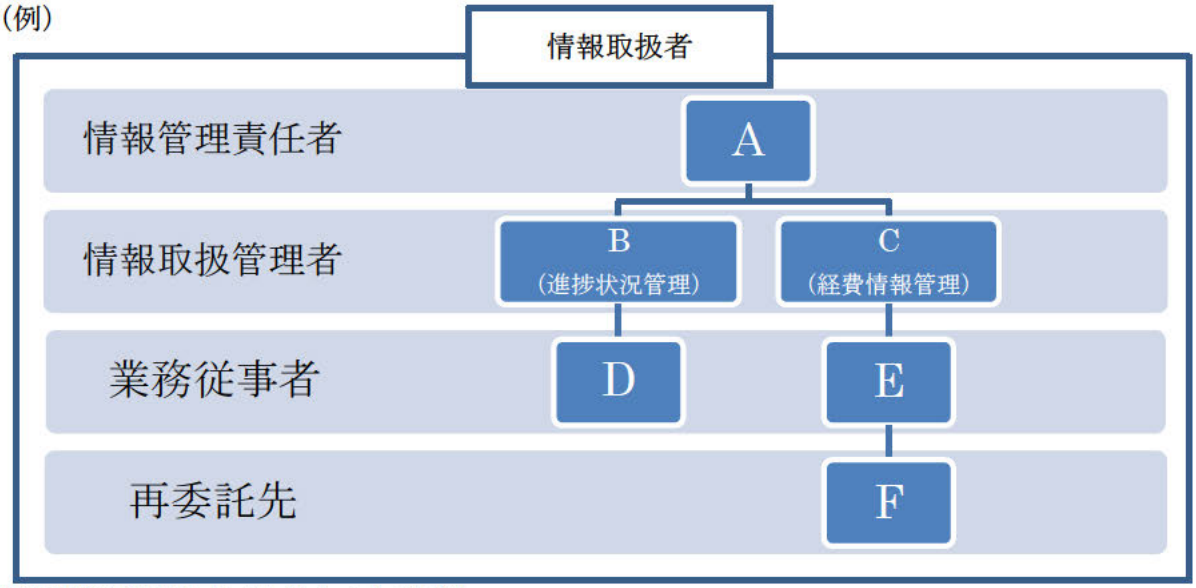
（※３）本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※４）日本国籍を有する者及び法務大臣から永住の許可を受けた者（入管特例法の「特別永住者」を除く。）以外の者は、パスポート番号等及び国籍を記載。

（※５）住所、生年月日については、必ずしも契約前に提出することを要しないが、その場合であっても担当課室から求められた場合は速やかに提出すること。

②情報管理体制図

（例）



【情報管理体制図に記載すべき事項】

・本事業の遂行にあたって保護すべき情報を取り扱う全ての者。（再委託先も含む。）

・本事業の遂行のため最低限必要な範囲で情報取扱者を設定し記載すること。