20240215東北第19号

令和5年度東北経済産業局鉱業関係書類電子化業務に係る請負先の公募について

下記について請負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ください。

令和6年2月22日

支出負担行為担当官
東北経済産業局総務企画部長　千嶌　浩

1.契約概要
(1)請負業務の名称等
令和5年度東北経済産業局鉱業関係書類電子化業務
(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04･05･06年度経済産業省競争参加資格(全省庁統一資格)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（平成3年法律第77号）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。

3.質問方法及び問い合わせ先
(1)質問方法
電話で受付けることとする。受付時間は次のとおりとする。
9時30分から12時00分、13時30分から16時30分
（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 資源エネルギー環境部 資源・燃料課
電　話　022-221-4934

(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6年2月29日（木曜日）12時（必着）

(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

イ 2.(1)に係る資格審査結果通知書（全省統一資格）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。

ウ 情報セキュリティの確保・個人情報の取扱い等に関する同意書（別添）

4)見積書に関する注意事項

ア 紙での見積書提出に際しては見積書の様式は任意とするが、

Ⅰ）見積書の宛名は「支出負担行為担当官 東北経済産業局総務企画部長」とし、日付は提出日とすること。

Ⅱ）法人の場合は、会社名、住所、連絡先、代表者の役職及び氏名を記載すること。代表者印及び社印の押印は不要。

Ⅲ）税抜き価格と税込み価格の双方を記載すること。

イ 電子調達システムでの見積書提出に際しては、システムにて税抜き価格を設定し提出すること。ただし見積内訳書（様式は任意）を添付することとし、当該見積内訳書には、税抜き価格と税込み価格の双方を記載すること。

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

・本件は、請書の提出を要する。
・請負先の決定方法は、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。
・受注した場合の支払いは、後日銀行振り込みとし、当局が請求書を受理してから30日以内とする。
・請求書の宛名は、「官署支出官 東北経済産業局長」とすること。

別添

甲：東北経済産業局総務企画部会計課長 殿

作成年月日：　年　月　日

情報セキュリティの確保・個人情報の取扱い等に関する同意書

乙：〇〇〇〇株式会社

下記の事項に同意し、甲の指示があったときにその指示に従いますので、見積書を提出いたします。

記

1. 仕様書の内容及び東北経済産業局役務請負契約条項の情報セキュリティの確保（第16条、第16条の2、第16条の3）（※1）（※2）、及び個人情報の取扱い（第17条）（※2）を遵守すること。

2. 本業務に従事する全ての者において、業務を遂行する能力があることを証明すること。具体的には、各業務従事者の氏名、所属、役職、業務経験、その他甲が指示する項目の略歴を提出し、業務遂行能力を証明すること。

（参考）

ア. 東北経済産業局役務請負契約条項（印刷製造、その他物品製造含む）
https://www.tohoku.meti.go.jp/kaikei/format/downloadfiles/2023_ukeoi_r5-ek-2.pdf

東北経済産業局役務請負契約条項（コンテンツバイドール版）
https://www.tohoku.meti.go.jp/kaikei/format/downloadfiles/2023_ukeoi_r5-ekcb-2.pdf

イ. 経済産業省情報セキュリティ管理規程
https://www.meti.go.jp/intro/data/pdf/kanri_kitei.pdf

ウ. 経済産業省情報セキュリティ対策基準
https://www.meti.go.jp/intro/data/pdf/taisaku_kijun.pdf

エ. 経済産業省個人情報保護管理規程
https://www.meti.go.jp/policy/kojinjyohohogo/kitei.pdf

（※1）外部公開ウェブサイトを構築又は運用する場合には、次条に規定する「外部公開ウェブサイトにおける情報セキュリティ対策」に基づく情報セキュリティ対策を含む。

（※2）経済産業省役務請負契約条項・コンテンツバイドール版の場合には契約条項第26条及び第27条を指す。

令和５年度東北経済産業局鉱業関係書類電子化業務
仕　様　書

１．業務の目的と背景

東北経済産業局では、行政事務の効率化・合理化による行政サービスの質向上及び将来的な電子政府構築への対応準備のため、紙資料を用いた業務の DX 化に取り組んでいる。資源・燃料課（以下「当課」）は、鉱業法（昭和２５年法律第２８９号）に基づく鉱業権を許認可する部署であり、権利の管理及び登記は紙により行われているが、昭和初期以前に作成された鉱業原簿、鉱区図、施業案などの鉱業権関係書類（以下「権利書類」）は劣化が進んでおり文字・記号などの判別が難しくなりつつある。そこで、業務効率化、質向上及び図面の保護を目的とし、電子化するものである。

２．業務実施期間及び納期

（１）業務実施期間

契約締結日から令和６年３月２９日（金）まで

（２）納期

業務期間末日の午後０時までに、当課に成果物を納め、検収・検査に合格すること。

３．作業内容及び留意事項など

（１）作業内容

権利書類について、１枚ごとにスキャニング装置で読み取り電子データを作成する（以下「電子化」）。作成した電子データは将来的に当課が運用する GIS アプリケーションに保存するが、本業務では、まず始めに指定する枚数を電子化し、文字などを明瞭に判別できる解像度とデータサイズの均衡をとれるような条件を決定する。その条件の下、ほかの権利書類も電子化を実施する。詳細は次のとおり。

工程	作業項目	作業内容
Ⅰ	電子化の試行、報告	①　３パターンの解像度（300、400、600dpi）で電子化する。 ②　①の結果を報告する。 　このとき、使用したスキャニング装置、手法、電子データのサイズ、形式（TIFF、JPEGなど）を報告すること。 ③　当課担当職員と協議し、解像度及びデータ形式を決定する。
Ⅱ	電子化	・　工程Ⅰで決定した解像度、データ形式で電子化する。 ・　電子データのファイル名を記したリストをエクセルファイル形式で作成すること。ハイパーリンクは不要。
Ⅲ	作業報告書の作成	作業の経緯が分かるよう作業報告書を作成し提出する。

（２）権利書類について

本業務の対象は、鉱業原簿、鉱区図、施業案、連絡図の４種類である。

①　電子化の対象は別紙１「電子化対象書類」のとおり。

②　状態は次のとおり。

・　手書き記載有り
・　微細な文字の記載有り
・　複数色による記載有り
・　紙質は和紙、普通紙など混在している
・　折り目がついている
・　連絡図については、金属板に張り付けてあり、取り外しはできない

（３）業務実施場所、権利書類の貸与について

①　業務実施場所及び業務履行にかかる資機材については受注者で用意すること。当課では一切用意しない。

② 権利書類は当課で引き渡す。業務実施場所まで配送する場合はセキュリティサービスを利用すること。

（4）作成上の留意事項
① 拡縮することなく、原寸で電子化すること。
② ゆがみ及び権利書類の破損などを防ぐため、資料をキャリアシート、アクリル又はガラスで押さえることは可能とする。
③ ホチキス及びクリップは外して電子化し、電子化後に復元すること。ただし、鉱業原簿は復元する必要はないが、綴じられていた順序のとおりバインダーに戻すこと。
④ 補修紙その他貼付物があった場合は当課担当職員に指示を仰ぐこと。
⑤ 劣化が著しい、判読が難しい、又は破損している資料は取扱いに十分留意すること。
⑥ 劣化及び破損が激しくデジタル化が困難である場合には、当課担当職員と協議すること。
⑦ 資料を破損した際は、当課担当職員の指示に従い補修対応を行うこと。
⑧ 不明点がある場合は、当課担当職員に照会すること。

（5）ファイル名の付与
別紙１「電子化対象書類」を参照のこと。

4．成果物について
（1）電子データを格納した納品用ハードディスク正・副　各１台
（2）電子データのファイル名を記したリスト（エクセルファイル形式）
（3）作業報告書（任意様式）
※　（2）及び（3）は（1）に格納すること。

5．情報管理体制・セキュリティに関する事項
（1）　別紙２「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。
① 契約締結後速やかに、別紙３「情報取扱者名簿及び情報管理体制図」を提出すること。
② 納品後速やかに、別紙４「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」を提出すること。
（2）業務完了のデータの扱いについて
本業務で取得した電子データは速やかに破棄し、書面により破棄した旨の報告を行うこと（任意様式）。

6．事業実施に当たっての留意事項
本事業を遂行するに当たっては、以下の点に留意すること。
（1）　受注者は、本業務上知り得た情報一切について、本業務に携わる者以外に開示及び漏洩をしてはならない。
（2）　本業務は、本仕様書の範囲において、当課の指示に従って実施しなければならない。また、担当者と緊密に連絡を取り、本業務の実施について疑義が生じた場合には、担当者の指示に従うこと。加えて、作業の方針についての相談、状況の経過報告等を随時行うものとする。
（3）　業務に関する詳細事項は、当課担当職員と協議の上、遂行すること。

7．連絡先（当課担当）
経済産業省東北経済産業局　資源エネルギー環境部　資源・燃料課
担当：堀川、川井
電話：022-221-4934　E-mail：bzl-thk-mining@meti.go.jp

電子化対象書類

別紙1

県名	鉱区番号	枚数及びサイズ						工程Ⅰの対象				ファイル名称(拡張子の前に付す名称)			
		鉱業原簿(B4・見開き)	鉱区図		施業案		連絡図(A2)	鉱業原簿	鉱区図	施業案	連絡図	鉱業原簿	鉱区図	施業案	連絡図
宮城県	16	4	4	規格外	76	三本木炭鉱規格外多数		○	○	○ 6枚程度		宮採第16号_鉱業原簿	宮採第16号_鉱区図	宮採第16号_三本木_施業案	
宮城県	20	4	2	規格外								宮採第20号_鉱業原簿	宮採第20号_鉱区図		
宮城県	25	3	2	規格外								宮採第25号_鉱業原簿	宮採第25号_鉱区図		
宮城県	26	7	3	規格外								宮採第26号_鉱業原簿	宮採第26号_鉱区図		
宮城県	44	4	7	規格外								宮採第44号_鉱業原簿	宮採第44号_鉱区図		
宮城県	45	4	3	規格外								宮採第45号_鉱業原簿	宮採第45号_鉱区図		
宮城県	53	10	10	規格外	127	照越炭鉱規格外多数						宮採第53号_鉱業原簿	宮採第53号_鉱区図	宮採第16号_照越_施業案	
宮城県	59	4	4	規格外					○			宮採第59号_鉱業原簿	宮採第59号_鉱区図		
宮城県	62	6										宮採第62号_鉱業原簿			
宮城県	66	3										宮採第66号_鉱業原簿			
宮城県	67	5										宮採第67号_鉱業原簿			
宮城県	73	8										宮採第73号_鉱業原簿			
宮城県	74	4										宮採第74号_鉱業原簿			
宮城県	84	4										宮採第84号_鉱業原簿			
宮城県	85	2										宮採第85号_鉱業原簿			
宮城県	87	2										宮採第87号_鉱業原簿			
宮城県	88	2										宮採第88号_鉱業原簿			
宮城県	90	3										宮採第90号_鉱業原簿			
宮城県	93	4										宮採第93号_鉱業原簿			
宮城県	94	5										宮採第94号_鉱業原簿			
宮城県	97	3										宮採第97号_鉱業原簿			
宮城県	98	4										宮採第98号_鉱業原簿			
宮城県	99	2										宮採第99号_鉱業原簿			
宮城県	100	4						○				宮採第100号_鉱業原簿			
宮城県	102	4										宮採第102号_鉱業原簿			
宮城県	103	4										宮採第103号_鉱業原簿			
宮城県	110	4										宮採第110号_鉱業原簿			
宮城県	111	2										宮採第111号_鉱業原簿			
宮城県	113	4										宮採第113号_鉱業原簿			
宮城県	116	2										宮採第116号_鉱業原簿			
宮城県	118	2										宮採第118号_鉱業原簿			
宮城県	125	2										宮採第125号_鉱業原簿			
宮城県	128	2										宮採第128号_鉱業原簿			
宮城県	135	2										宮採第135号_鉱業原簿			
宮城県	138	4										宮採第138号_鉱業原簿			
宮城県	139	4						○				宮採第139号_鉱業原簿			
宮城県	652	2	1	A1								宮採第652号_鉱業原簿	宮採第652号_鉱区図		
宮城県	659	3	1	A1								宮採第659号_鉱業原簿	宮採第659号_鉱区図		
宮城県	660	2	3	A1					○			宮採第660号_鉱業原簿	宮採第660号_鉱区図		
宮城県	661	2	1	A1								宮採第661号_鉱業原簿	宮採第661号_鉱区図		
宮城県	662	2	1	A1								宮採第662号_鉱業原簿	宮採第662号_鉱区図		
宮城県	663	2	1	A1								宮採第663号_鉱業原簿	宮採第663号_鉱区図		
宮城県	664	2	1	A1								宮採第664号_鉱業原簿	宮採第664号_鉱区図		
宮城県	665	2	1	A1								宮採第665号_鉱業原簿	宮採第665号_鉱区図		
宮城県	668	2	1	A1								宮採第668号_鉱業原簿	宮採第668号_鉱区図		
宮城県	669	2	1	A1								宮採第669号_鉱業原簿	宮採第669号_鉱区図		
宮城県	670	2	1	A1								宮採第670号_鉱業原簿	宮採第670号_鉱区図		
宮城県	691	2	1	A2								宮採第691号_鉱業原簿	宮採第691号_鉱区図		
宮城県	692	2	1	A2								宮採第692号_鉱業原簿	宮採第692号_鉱区図		
宮城県	697	2	2	A2								宮採第697号_鉱業原簿	宮採第697号_鉱区図		
宮城県	698	2	2	A2								宮採第698号_鉱業原簿	宮採第698号_鉱区図		
栗駒山							1				○				宮城県_栗駒山_連絡図
吉岡							1				○				宮城県_吉岡_連絡図
仙台							1				○				宮城県_仙台_連絡図
		168	**54**		**203**			**12**	**11**	**6**	**3**				

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。

1)　受注者は、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)～18)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４））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。

2)　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。

3)　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。

4)　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。

5)　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。

6) 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。

7) 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。

8) 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３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。

9) 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。

10) 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。

11) 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 10)まで及び 12)から 18)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。

12) 受注者は、外部公開ウェブサイト（以下「ウェブサイト」という。）を構築又は運用するプラットフォームとして、受注者自身（再受注先を含む。）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。また、ウェブサイト構築時においてはサービス開始前に、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。

13)　受注者は、ウェブサイトを構築又は運用する場合には、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。

14)　受注者は、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。

15)　受注者は、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。

16)　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。

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。

⑦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。

17) 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、画一的な約款や規約等への同意のみで利用可能となる外部サービス（ソーシャルメディアサービスを含む）を利用する場合には、これらのサービスで要機密情報を扱ってはならず、8）に掲げる規程等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こと。また、外部サービスを利用する場合は、その利用状況を管理すること。

なお、受注者は、受注業務を実施するに当たり、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)」において登録されたサービスから調達することを原則とすること。

18)　受注者は、ウェブサイトの構築又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提供するウェブサイト又はアプリケーション・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）ウェブサイト又はアプリケーション・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）提供するウェブサイト又はアプリケーション・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提供するウェブサイト又はアプリケーション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、提供するウェブサイト又はアプリケーション・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、それをウェブサイト又はアプリケーション・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提供するウェブサイト又はアプリケーション・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、ウェブサイト又はアプリケーション・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ウェブサイト又はアプリケーション・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ウェブサイト又はアプリケーション・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ウェブサイト又はアプリケーション・コンテンツに掲載すること。

別紙３

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						

（※１）請負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。

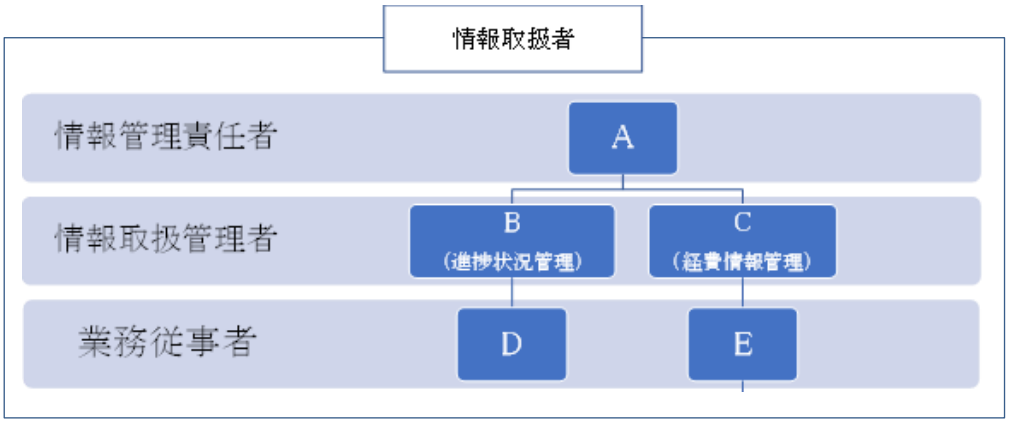
（※３）本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※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。

・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。

別紙４

年　　月　　日

東北経済産業局　資源・燃料課長　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３）	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４）	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５）	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６）	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７）	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８）	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３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９）	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１０）	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１１）	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１０）まで及び１２）から１８）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１２）	外部公開ウェブサイト（以下「ウェブサイト」という。）を構築又は運用するプラットフォームとして、受注者が管理責任を有するサーバ等を利用する場合には、当該ウェブサイト又は当該サーバ等で利用する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。また、ウェブサイト構築時においてはサービス開始前に、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。	
情報セキュリティに関する事項１３）	本業務の実施に当たって、ウェブサイトを構築又は運用する場合には、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。 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。	
情報セキュリティに関する事項１４）	ウェブサイト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、ウェブサイト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。	
情報セキュリティに関する事項１５）	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。	
情報セキュリティに関する事項１６）	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。 （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）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。 （７）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１７）	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、画一的な約款や規約等への同意のみで利用可能となる外部サービス（ソーシャルメディアサービスを含む）を利用する場合には、これらのサービスで要機密情報を扱ってはならず、「情報セキュリティに関する事項８）」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こと。なお、受注業務を実施するに当たり、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）」において登録されたサービス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１８）	ウェブサイトの構築又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。 （１）提供するウェブサイト又はアプリケーション・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ウェブサイト又はアプリケーション・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提供するウェブサイト又はアプリケーション・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）提供するウェブサイト又はアプリケーション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、提供するウェブサイト又はアプリケーション・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、それをウェブサイト又はアプリケーション・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）提供するウェブサイト又はアプリケーション・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、ウェブサイト又はアプリケーション・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ウェブサイト又はアプリケーション・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ウェブサイト又はアプリケ	

	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ウェブサイト又はアプリケーション・コンテンツに掲載すること。	

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１８）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」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））。）