

仕様書

1. 件名

令和7年度技術開発調査等の推進事業費（バーゼル法関連事前相談業務）に係る入札可能性調査実施要領

2. 事業の背景・目的

近年のアジア各国等の急速な経済成長による原材料需要の伸び等に伴い、我が国からアジア各国等への再生資源等の輸出量が増加している。

これら輸出される再生資源等の中には、「有害廃棄物の越境移動及びその処分の規制に関するバーゼル条約」（以下「バーゼル条約」という。）や、バーゼル条約の国内担保法である「特定有害廃棄物等の輸出入等の規制に関する法律」（以下「バーゼル法」という。）の規制対象物（以下「特定有害廃棄物等」という。）に該当するものがある可能性があり、その場合、バーゼル法に規定する手続を経なければ、バーゼル法違反となるだけでなく、輸入国との貿易問題や環境被害を引き起こす恐れがある。

再生資源等を輸出入している我が国としては、有害廃棄物の不適正輸出入を防止し、輸入国及び我が国での環境問題の発生等を未然に防止することが重要である。

一方で、特定有害廃棄物等に該当するか否かの判断は、バーゼル法等関係法令についての理解や有害廃棄物等に関する知見を有していない者にとっては困難であり、事業者が輸出入する貨物が特定有害廃棄物等に該当するか否かを判断する際の助言サービス（以下「事前相談」という。）を行っているところ。

また、令和7年1月1日のバーゼル条約付属書改正の施行に伴い、非有害を含むすべての電気・電子機器廃棄物が原則バーゼル該当貨物となるため、従来より多くの事前相談が想定されること。

本事業は、近年の再生資源等の輸出入量の増加により事前相談も件数が増加し、行政のみでの対応が難しいため、輸出入貨物が特定有害廃棄物等に該当するか否かに関する事前相談業務の実施体制を確保するとともに、再生原料、中古品等の輸出入の実態を調査把握するものである。

3. 事業内容及び事業実施方法

3.1 業務内容

(1) 再生原料、中古品等の輸出入貨物についての事前相談への対応

再生原料、中古品等の輸出入事業者、通関業者等からのバーゼル法規制に関する事前相談への対応業務から、データを集計する。

① 事前相談窓口の設置

(ア) 運営体制の構築

事前相談窓口の運営に必要な人員及び相談者から提出される輸出入する貨物についての事前相談に必要な書類を受け付けるための手段（電子メール、電話）を確保した上で、事前相談窓口を設置し、委託契約締結日から相談の受付を開始し、委託契約終了日まで行う。事前相談に際して相談者が提出を要する書類や事前相談の流れについては、経済産業省GXグループ資源循環経済課のホームページ（参考1）参照。

また、業務は以下の体制で行い、従業者は以下に掲げる条件を満たしていること。

(i) 業務責任者

事前相談業務の責任者は、経済産業省GXグループ資源循環経済課とする。

(ii) 事前相談対応業務

事前相談についての、相談者から提出された資料の確認や問い合わせ等への対応を行うものとする。

従業者の条件は、①事業者により提出された書類に記載された内容に基づき、輸出入する貨物について、バーゼル法に規定する特定有害廃棄物等に該当するか否かを判断し、適切な助言を行う上で必要なバーゼル条約及びバーゼル法、廃棄物の処理及び清掃に関する法律（廃棄物処理法）等関係法令に関する知見及び相談対象品目となるメタルスクラップやプラスチックスクラップ等の原材料の組成を判断するために必要な科学的知見を有していること、②①の知見を有した上で、事前相談に的確に対応するためのアドバイザーに関するノウハウ及び技術を有していること、とする。

過去の具体的な相談内容は以下のとおり。

(相談事例)

(A) メキシクラッジ、廃触媒、リサイクル残渣、金属スラグ&ドロス → 製錬所、製造工場の発生工程を確認の上、有害成分の有無の判断（規制基準値以下であることを確認）し、バーゼル該当品と判断した場合は、外為法上のバーゼル手続をすることを勧め、非該当品である場合はそのことを伝えて通常の通関を行うように助言を行う。

(B) ペットボトルプレス&フレーク → 汚れ、飲み残し等の家庭ゴミが含有していないか等を写真で確認 → 該非判定

(C) 金属回収目的のコンプレッサー（黒モーター） → 成分分析結果を確認の上、穴開け油抜き済みであることを写真で確認 → 該非判定

(D) ミックスメタル → 成分分析結果等より、バーゼル法に基づく特定有害廃棄物等の範囲等を定める環境省令の別表第四～六に該当する有害物質が含有しているかいないかを確認 → 該非判定

(E) 被覆電線 → 成分分析結果より、鉛の重量%及び溶質基準値が規制値以下であるか否かを確認 → 該非判定

(F) ミックスメタルスクラップ → 運搬中の火災事故の予防のため、使用済み家電製品が元の形状が確認できる大きさのまま含まれていないことを確認し、可能な限り品目ごと（モーター、被覆電線、鉄スクラップ、アルミ等）に分別するように指示 → 該非判定

(G) 中古品 → 輸出入相手国の規制を確認の上、全ての品が中古品判断基準を満たしたものであるか否か、有価で取引がされているか、相手国に中古市場が存在するか等を確認 → 該非判定

(イ) 運営体制

事前相談の1日の件数は、バーゼル法範囲省令の改正により、すべての電気・電子機器廃棄物がバーゼル該当貨物となるため、令和7年度の事前相談件数は50件～70件程までとなることが想定される。原則1週間以内に回答すること。

相談者から電子メール、FAXで書類、写真等が提出され、提出後、相談者から相談窓口で資料を提出した旨の連絡がメール、もしくは電話で入る。この連絡を受けたら、提出された書類等の内容について、輸出入貨物がバーゼル法の規制対象か否かの該当性について回答案を作成し、経済産業省GXグループ資源循環経済課へメールで内容の照会を行い、了承後、相談者に原則としてメール、もしくは電話で回答する体制を整備する。また、回答時に、「本助言については、輸出又は輸入する際の関係法規遵守の義務を緩和するものではなく、現実に輸出入される貨物そのものについて関係法規適合を証明するものではない。」という旨を述べる（以下、バーゼル法の規制対象物か否かの該当性についての助言及び助言とともに述べる一文を併せて「助言」という。）

相談業務の実施に必要な事項については、経済産業省GXグループ資源循環経済課から、契約時に指示する。

相談対象品目以外の相談案件及び該当性についての判断が難しい案件等については、経済産業省GXグループ資源循環経済課に対応方針等について相談する。また、相談を受け付けるか否かの判断自体が難しい場合には、経済産業省GXグループ資源循環経済課に相談する。

(ウ) その他

事前相談窓口の設置場所は受託者の責任において決定するものとし、事務机、パソコンその他の必要な什器、備品等については受託者側において用意すること。

② 事前相談窓口の運営

(ア) 業務時間

原則、土・日・休日を除く平日とする（ただし、外部からの相談受付時間は9時30分～16時（12時～13時を除く））。

(イ) 相談を受け付ける主な相談対象品目

(A) プラスチック・スクラップ（ポリエチレン、ポリプロピレン、ポリ塩化ビニル等）

(B) メタル・スクラップ（金属（金属化合物を含む。）又は金属を含むもの（廃触媒、ミックスメタル等）

(C) 中古製品

(ウ) 事前相談内容の登録

毎日、その日に助言した全ての事前相談について、その日のうちに、相談者から提出された書類等に記載されている情報（バーゼル法該当判断（該当若しくは非該当）、事業者名など事業者に関する情報、相談者の業種、輸出入予定者・輸出入相手、申告予定税関、申告予定時期、輸出/輸入の別、相手国、貨物分類、貨物量など貨物に関する情報、相談内容と行った助言、提出書類、インボイスナンバー等）をエクセルファイルに入力し、CSVファイルに変換して廃棄物等輸出入管理システム（以下「事前相談管理システム」という）（参考3）に仮登録する（オンライ

ン申請の場合は、既に仮登録の状態になっているので、申請された内容に不備や添付書類の不足等がないかの確認をすること)。

(エ) 事前相談資料のシステムへの添付

助言と事前相談システムへの入力を実施した事前相談案件について相談者から提出された事前相談資料は、スキャナで読み込みPDFに変換した上で、契約時に経済産業省GXグループ資源循環経済課から指示するルールに従ったファイル名を付与して、事前相談管理システムに添付する。

(オ) 経済産業省GXグループ資源循環経済課への報告

当日中に、事前相談管理システムに仮登録するために作成したエクセルファイルのうち、その日に助言した案件全ての分を1つのエクセルファイルにまとめ、契約時に経済産業省GXグループ資源循環経済課から指示する方法で加工する。これら事前相談システムへの仮登録及び公開依頼中へのデータ移行とエクセルファイルの加工が終わったら、その日のうちに経済産業省GXグループ資源循環経済課に、事前相談システムへの公開依頼が完了した旨を記載して加工したエクセルファイルを添付したメールを送付する。メールの宛先や記載例は、契約時に経済産業省GXグループ資源循環経済課から指示する。

毎月最終日に、品目別ごとの相談件数及び問合せ件数を集計の上、経済産業省GXグループ資源循環経済課に報告する。

(カ) アンケート調査

委託契約期間中の特定の期間（1か月程度、時期は問わない）、利用者満足度についてのアンケート調査票を任意に抽出した相談者（当該アンケートを実施するまでに相談のあった者）100者以上に配付し、得た回答について集計の上、(2)の報告書に記載する。なお、配布、回答手段は問わない（メールも可）。また、回収率については、一度催促した結果のものとする。

(キ) その他

バーゼル法に関する一般的な問合せ（メール、もしくは電話による受付）に対し、必要に応じて、パンフレットやバーゼル法に規定する特定有害廃棄物等を定める省令等の資料が掲載されているホームページの紹介、又は、公表資料をFAX送付や手交する等しつつ、規制の内容について説明する。また、経済産業省GXグループ資源循環経済課の指示を受けて、受託事業者のホームページにバーゼル法に関する情報を掲載する等により、周知を図る。

経済産業省GXグループ資源循環経済課、環境省環境再生・資源循環局廃棄物規制課及び各環境省地方環境事務所等から事前相談資料の共有依頼がある場合には、迅速に対応する。

相談業務の実施に必要な事項については、経済産業省GXグループ資源循環経済課から、委託事業実施期間中に追加で指示することがあり得る。

(参考1) 事前相談に際して提出が必要な書類や事前相談の流れ

https://www.meti.go.jp/policy/energy_environment/kankyokeiei/basel/jizen/soudan.html

(参考2) 事前相談件数（バーゼル法に関する一般的な問合せを除く）の年度合計（実績）は、平成28年度は49,319件、平成29年度は43,675件、平成30年度は38,097件、令和元年度は41,016件、令和2年度は約38,519件、令和3年度は16,274件、令和4年

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。

7. 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と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と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。

令和 年 月 日

経済産業〇〇〇課長 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 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)	<p>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。</p> <p>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。</p>	
情報セキュリティに関する事項 7)	<p>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。</p>	
情報セキュリティに関する事項 8)	<p>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。</p>	
情報セキュリティに関する事項 9)	<p>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。</p> <p>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。</p>	
情報セキュリティに関する事項 10)	<p>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。</p>	
情報セキュリティに関する事項 11)	<p>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。</p>	
情報セキュリティに関する事項 12)	<p>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。</p>	
情報セキュリティに関する事項 13)	<p>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。</p>	
情報セキュリティに関する事項 14)	<p>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。</p>	

<p>情報セキュリティに関する事項 15)</p>	<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</p>	
-------------------------------	--	--

	<p>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"> ・サービス開始前および、運用中においては年1回以上、ポートスキャン、脆弱性検査を含むプラットフォーム診断を実施し、脆弱性を検出した場合には必要な対策を実施すること。 ・インターネットを介して通信する情報の盗聴及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするため、TLS(SSL)暗号化の実施等によりウェブサイトの暗号化の対策等を講じること。 ・必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いること。 <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>	
<p>情報セキュリティに関する事項 16)</p>	<p>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。</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> <ol style="list-style-type: none"> 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。 <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</p>	

	<p>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。</p>	
<p>情報セキュリティに関する事項 17)</p>	<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つた場合には、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））。)