（別紙）

実施計画書（仕様書）

１．事業名

令和８年度産業保安等調査研究事業（化学物質規制対策（化学物質の分解性及び蓄積性に係る総合的評価の導入に関する調査））

２．事業の背景・目的

我が国では、新規化学物質の製造・輸入をしようとする場合、あらかじめ「化学物質の審査及び製造等の規制に関する法律」（以下「化審法」という。）に基づき、公定試験法に従って実施した分解性、蓄積性及び毒性等の試験結果をもって届出を行い、国による評価・審査を受けることとされている。この新規化学物質の評価・審査においては、実環境での挙動を反映した評価・審査の精緻化や合理化及び科学的妥当性の向上、試験法の国際整合化等の中長期的課題が存在する。

こうした中で、近年当省では、委託事業を通じて、過去の知見や実環境を踏まえた化学物質の性状評価としての公定試験法の運用見直しについて検討を行うとともに、委託事業で取りまとめた成果の法定試験法への反映も進めている。

本年度事業では、化審法の新規化学物質の審査における合理的な化学物質の性状評価に向けた取組の一環として、有識者の意見を聴取しつつ、化審法における分解度試験の国際整合化及び餌料投与法による蓄積性評価の精緻化に関する調査検討を行い、今後の対応の方向を取りまとめるとともに、化学物質の分解性・蓄積性に関する評価・審査を支える試験機関の技術力向上及び専門人材の育成に向けた取組を推進することを目的とする。

３．事業内容及び実施方法

受託者は、本事業の目的を達成させるため、以下に示す事業内容を滞りなく実施する。

なお、本事業の進捗状況の確認、その他作業内容の細部の調整等を行うため、必要に応じて、受託者と経済産業省化学物質安全室の担当者（以下「担当職員」という。）との打合せを実施することとする。また、本事業において試験を実施する場合に、当該試験に供される備品・試薬類を確保するために最低限調達が必要な分については、本事業の経費として支出することができるものとする。

（１）化審法における公定試験法の運用見直しに向けた検討

①分解性評価に関する検討テーマ（分解度試験）

（Ⅰ）分解度試験に係る試験条件の検討

化審法における新規化学物質の審査では、微生物による化学物質の分解度試験の結果に基づき、新規化学物質の分解性を評価している。化審法の公定試験法としては、経済協力開発機構（OECD）が定めているテストガイドライン（TG）に準拠する 301C 相当又は 301F 相当によることを原則としているが、OECD TG301 シリーズの分解度試験で定めている試験条件と異なる部分があり、一部整合性が取れておらず精緻な評価が困難な場合がある。また、一定条件を満たした場合に、化

審法の評価で認められているOECD TG302Cの試験についても、分解度試験で生じた分解生成物の特定が困難な場合もある。

（Ⅱ）分解度試験の活性汚泥の維持管理に係る検討

新規化学物質の審査に用いる 301C 相当の分解度試験を実施するために、分解度試験を実施する国内の優良試験所基準（GLP）試験機関は、平日及び休日を問わず年間を通じて活性汚泥を維持・管理するために人員の確保等の負担が掛かっている。

本年度委託事業では、活性汚泥の維持及び管理の負担を軽減するために、装置のメーカーや海外試験機関へのヒアリング等を通じ、活性汚泥の維持及び管理の自動化の可能性を検討する。

（Ⅲ）委員会の開催

上記（Ⅰ）（Ⅱ）の検討に際しては、化学物質の分解性評価手法に精通する有識者（４～５名程度）に対する意見聴取の機会を設けて２回程度（うち１回程度は対面開催を想定。）実施し、得られた意見等を適宜反映する。具体的な意見聴取の実施方法は、受託者の提案に基づき、担当職員と協議の上で決定する。有識者に謝金や旅費を支出する必要がある場合は、本事業の経費として支出するものとする。

②蓄積性評価に関する検討テーマ（餌料投与法による濃縮度試験及び１－オクタノール／水分配係数測定試験）

（Ⅰ）餌料投与法に係る試験の実施及び試験条件の検討

化審法における新規化学物質の審査では、魚類を用いた化学物質の蓄積性評価として水暴露法（指標：BCF）又は餌料投与法（指標：BMF）を用いた試験法を採用している。このうち、BMFの指標による蓄積性評価は、OECD TG305のガイダンス文書に示されている「餌料投与法試験で得られたBMFからBCFを予測する回帰式」に基づき定められている判定基準により行われているが、評価に際し判断基準の精緻化が課題となっている。

本年度事業では、生物濃縮係数（BCF、BMF）間の回帰式の精度向上を目的として、昨年度までの事業で整理した餌料投与法の試験条件に沿って試験計画を策定し、これに基づき餌料投与法試験を実施してBMF等のデータを取得する。実施する試験数は、昨年度実施した予備的な試験も実施した物質及び次年度以降に検討すべき試験の予備的な試験含め、４試験程度（本試験は１試験、予備試験３試験を想定）とする。さらに、取得した試験データ及び既存の回帰式に含まれるデータ等を基に回帰式を作成し、試験結果や既存の回帰式との比較等に関して考察を行うともに、BMFの濃度依存性の有無及び基準物質のあり方について考察する。

得られた回帰式の作成及び試験結果の考察等について、化学物質の蓄積性評価手法に精通する有識者（７名程度）による委員会を設置し、意見を聴取する。委員会は２回程度開催し（少なくとも１回は対面開催とする）、得られた意見等を適宜反映し、次年度以降に検討すべき課題及び検証方法を取りまとめることとする。有識者に謝金や旅費を支出する必要がある場合は、本事業の経費として支出するものとする。

（Ⅱ）Pow測定試験に基づく蓄積性判定の適用拡大検討

化審法における新規化学物質の審査では、物理化学的性状に基づく蓄積性の評価方法として、1

－オクタノール／水分配係数測定試験（以下「Pow 測定試験」）に基づく方法も採用している。Pow 測定試験の判定は、1－オクタノール／水分配係数（以下「Pow」）の値に基づいて行われており、高濃縮性でないと判定される基準値は 3.5 とされている。生物蓄積性に関する国際的な動向や動物試験削減の要請に鑑み、動物を使用しない試験である Pow 測定試験の結果により評価・判定できる範囲を拡大することにより、審査の効率化、高度化を図ることが可能となる。

本年度事業では、Pow 測定試験による評価の合理化に関する素案について、化学物質の蓄積性評価手法又は統計解析等に精通する有識者（６名程度）から意見を聴取する場を２回程度設ける（原則対面とする）。有識者に謝金や旅費を支出する必要がある場合は、本事業の経費として支出するものとする。

（２）新たな分解性及び蓄積性評価に関する海外動向調査

①分解性評価に関する海外動向調査

新規化学物質の分解性評価では、被験物質の組成又は疎水性や難水溶性等の特性が原因で、分解度試験の実施が困難な物質や得られた試験結果からの評価が困難な物質があり、分解性評価が困難な物質の合理的な分解性評価が求められている。

本年度事業では、分解性の評価困難物質についての海外での最新の検討事例等、新たな分解性評価に関して、海外動向を調査し、その結果をとりまとめる。海外動向の調査にあたっては、現地での調査実施の必要性についても精査し、必要に応じて現地での関係機関へのヒアリング等を行うこととする。

調査結果は、必要に応じ①（Ⅲ）で開催する委員会等においても取り上げ、化審法における新規化学物質の分解性評価への導入可能性について検討することとする。

②蓄積性評価に関する海外動向調査

昨年度事業では、ヨコエビを用いた水暴露法による濃縮度試験（OECD TG321）について、海外での活用事例等の最新の蓄積性評価に関する海外動向調査した。

本年度事業では、昨年度に引き続き蓄積性評価に関する海外動向を調査する。具体的には、欧州 REACH における蓄積性評価方法や、ヨコエビ等の魚類以外を用いた濃縮度試験等、新たな蓄積性評価に関して、海外動向を調査し、その結果をとりまとめる。海外動向の調査にあたっては、現地での調査実施の必要性についても精査し、必要に応じて現地での関係機関へのヒアリング等を行うこととする。

調査結果は、必要に応じ②（Ⅰ）で開催する委員会等においても取り上げ、化審法における新規化学物質の蓄積性評価への導入可能性を検討することとする。

（３）化学物質の分解性・蓄積性に関する試験機関の技術力向上及び専門人材の育成に向けた取組

化審法の事前審査制度は、化学物質の安全性試験を行う化審法 GLP 試験機関の技術力及び化学物質の試験や評価・審査を担う専門人材で成り立っている。化学物質の分解性及び蓄積性の分野において本制度の持続的運用を図るため、本年度事業では、これら技術力の向上と有能な専門人材の確保・育成に資する以下の取組を実施するとともに、今後取るべき必要かつ有効な方策について検討し、提

案する。

具体的な実施内容及び実施方法は、受託者の提案も踏まえ、担当職員と協議の上で決定する。有識者等に謝金や旅費を支出する必要がある場合は、本事業の経費として支出するものとする。

① 分解性・蓄積性に係る化審法 GLP 試験機関等連絡会議（仮称）の開催

分解度試験、濃縮度試験及び分配係数試験を実施する国内の GLP 試験機関及び、高分子フロースキーム試験を実施する試験機関を対象とした連絡会議を原則対面開催にて１～２回程度開催する。本会議では、試験技術や試験成績の評価技術等に係る共通課題を協議し、対応の方向性を取りまとめることを目指す。また、このうち少なくとも１回以上は、化学物質の評価手法に精通する有識者（６名程度）との対話の機会を設け、新規化学物質に係る審査の要諦について相互理解の促進を図ることとする。受託者は、本会議の取りまとめ、資料作成等の事前準備及び運営に係る事務手続を行う。

② 分解性・蓄積性に関する専門人材の確保・育成のためのプロモーション活動

受託者は、化学物質の安全性評価に関係する有識者及び専門人材やその候補が一堂に会する学会主催の会合（本年６月２３日～２６日開催予定の「第５回環境化学物質合同大会」[1]を想定。）において、化審法の事前審査制度に関する認知及び理解の向上を目的とした講演等を行うための会場設営、必要に応じて専門家（２名程度）の派遣、その他運営に係る事務手続を行う。

４．事業実施期間

委託契約締結日から令和９年３月１７日まで

５．納入物

（１） 調査報告書等一式

- 調査報告書、報告書骨子（様式１）、調査で得られた元データ、委託調査報告書公表用書誌情報（様式２）、二次利用未承諾リスト（様式３）を納入すること。
- 調査報告書については、ＰＤＦ形式に加え、機械判読可能[2]な形式のファイルも納入すること。なお、報告書のデータ量が１２８ＭＢ、ページ数が１，０００ページ又は文字数が４００万文字を超過する場合には、いずれの制限も超えないようファイルを分割して提出すること。
- 調査で得られた元データについては、機械判読可能な形式のファイルで納入することとし、特に図表・グラフに係るデータ（以下「図表等データ」という。）については、構造化されたＥｘｃｅｌやＣＳＶ形式等により納入すること。

[1]主催：一般社団法人日本環境化学会、日本環境毒性学会
https://j-ec.smartcore.jp/M022/forum/touron34?jpn

[2]コンピュータプログラムがデータ構造を識別し、データを処理（加工、編集等）できること。例えば HTML, txt, csv, xhtml, epub, gml, kml 等のほか、Word, Excel, PowerPoint 等のデータが該当する（スキャンデータのようなものは該当しない）。

（２）　調査報告書等一式（公表用）

・調査報告書及び様式３（該当がある場合のみ）を一つのＰＤＦファイル（透明テキスト付）に統合したもの、並びに公開可能かつ二次利用可能[3]な図表等データを、プロパティを含む状態で納入すること。

・セキュリティ等の観点から、経済産業省と協議の上、非公開とするべき部分については、特に以下の点に注意し、削除するなどの適切な処置を講ずること。

- 報告書・Ｅｘｃｅｌデータ等に個人情報や不適切な企業情報が存在しないか。
- 報告書（ＰＤＦ）に目視では確認できない埋め込みデータ等が存在しないか。
- Ｅｘｃｅｌデータ等に目視では確認できない非表示情報が存在しないか。
- Ｅｘｃｅｌデータ等に非表示の行・列が存在しないか。

・公開可能かつ二次利用可能な図表等データが複数ファイルにわたる場合、１つのフォルダに格納した上で納入すること。

- 各データのファイル名については、調査報告書の図表名と整合をとること。
- 図表等データは、オープンデータとして公開されることを前提とし、経済産業省以外の第三者の知的財産権が関与する内容を含まないものとすること。

（３）　様式１～様式３について

- （様式１）委託調査報告書骨子[4]
  - レイアウト（余白、フォント等）に従い、３枚以内にまとめた上でＷｏｒｄ形式にて納入すること。
  - 図表は挿入せずテキスト形式で作成すること。
  - 見出しについては記載された項目のとおりとすること。
- （様式２）委託調査報告書公表用書誌情報[5]
  - ファイル形式はＥｘｃｅｌ形式で納入すること。
  - 報告書の英語版や概要版等、公表用の報告書と同一のＰＤＦファイルとすることが適当でない公表用の納入物がある場合には１つのＰＤＦファイルごとに作成すること。
- （様式３）二次利用未承諾リスト
  - 調査報告書は、オープンデータ（二次利用可能な状態）として公開されることが前提だが、二次利用の了承を得ることが困難な場合又は了承を得ることが報告書の内容に大きな悪影響を与える場合は、報告書の当該箇所に出典等を明示し、知的財産権の所在を明らかにした上で、当該データを様式３に記載すること（知的財産権の所在が不明なものも含む）。
  - ファイル形式はＥｘｃｅｌ形式で納入すること。
- 様式１～３ダウンロード先
  - 委託調査報告書　（METI/経済産業省）

[3]営利目的を含む、自由な利用（転載・コピー共有等）を行うこと。

[4]委託調査報告書のデータ利活用を促進するため、報告書の概要を骨子としてまとめるもの。

[5]本事業の報告書のオープンデータとしての公表に際し、データとしての検索性を高めるため、当該データの属性情報に関するデータを作成するもの。

６．納入方法

- メール提出やファイル交換サイト等の手段を用いること。なお、具体的な納入方法は担当課室と協議の上、決定すること。
- 公表用資料一式と非公表資料一式が紛れないように整理して納入すること。

７．納入場所

経済産業省大臣官房産業保安・安全グループ化学物質管理課化学物質安全室

８．情報管理

（１）情報管理体制

①受注者は本事業で知り得た情報を適切に管理するため、次の履行体制を確保し、発注者に対し「情報セキュリティを確保するための体制を定めた書面（情報管理体制図）」及び「情報取扱者名簿」（氏名、個人住所、生年月日、所属部署、役職等が記載されたもの）を記載した情報管理様式を契約前に提出し、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。

③①の情報セキュリティを確保するための体制を定めた書面又は情報取扱者名簿に変更がある場合は、予め担当課室へ届出を行い、同意を得なければならない。

（２）履行完了後の情報の取扱い

国から提供した資料又は国が指定した資料の取扱い（返却・削除等）については、担当職員の指示に従うこと。業務日誌を始めとする経理処理に関する資料については適切に保管すること。

（３）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．その他

①本事業を行うに当たっては、取り扱うデータを厳重に管理し、データが外部に持ち出されることが

ないようにすること。
②受託者は、契約期間中及び契約終了後においても、本調査に関して知り得た情報について、他に漏らし、又は他の目的に利用してはならない。
③事故又は障害が発生した場合には、直ちにその対処を行い、原因及び対処内容等について経済産業省製造産業局化学物質管理課化学物質安全室に報告すること。
④納入物の著作権は経済産業省に譲渡すること。
⑤氏名表示権について経済産業省の指示に従うこと。
⑥経済産業省が行う納入物の改変について著作者人格権を行使しないこと。
⑦納入物は公表を前提とする。

（情報管理様式）

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。

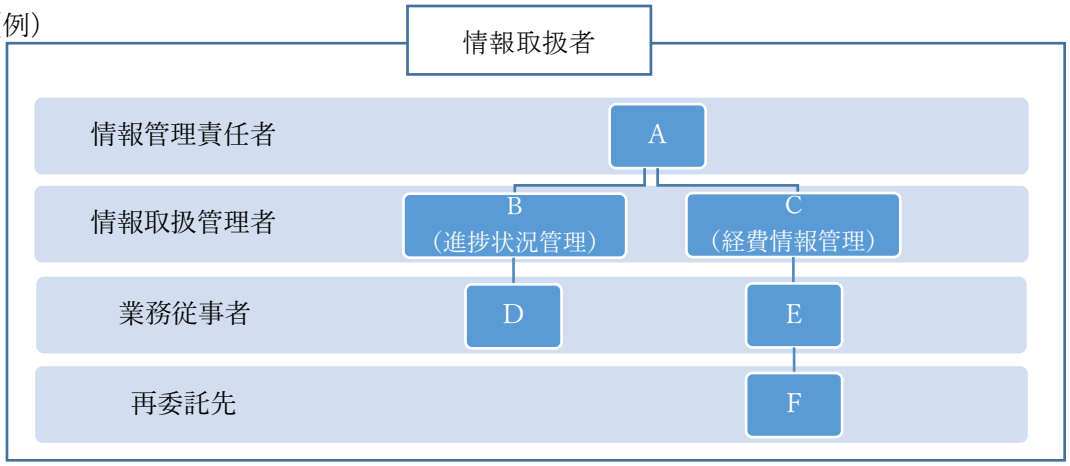
（※３）本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※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。

（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、1)から 17)までの措置の実施を契約等により再委託先に担保させること。また、1)の確認書類には再委託先に係るものも含むこと。

【情報の取扱い】

6）受注者は、本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）の取扱いには十分注意を払い、当省内に複製が可能な電子計算機等の機器を持ち込んで作業を行う必要がある場合には、事前に担当職員の許可を得ること。なお、この場合であっても、担当職員の許可なく複製してはならない。また、作業終了後には、持ち込んだ機器から情報が消去されていることを担当職員が確認できる方法で証明すること。

7）受注者は、本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体）について、担当職員の許可なく当省外で複製してはならない。また、作業終了後には、複製した情報が電子計算機等から消去されていることを担当職員が確認できる方法で証明すること。

8）受注者は、本業務を終了又は契約解除する場合には、受注者において本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）を速やかに担当職員に返却し、又は廃棄し、若しくは消去すること。その際、担当職員の確認を必ず受けること。

9）受注者は、契約期間中及び契約終了後においても、本業務に関して知り得た当省の業務上の内容について、他に漏らし、又は他の目的に利用してはならない。

　なお、当省の業務上の内容を外部に提供する必要が生じた場合は、提供先で当該情報が適切に取り扱われないおそれがあることに留意し、提供の可否を十分に検討した上で、担当職員の承認を得るとともに、取扱上の注意点を示して提供すること。

【情報セキュリティに係る対策、教育、侵害時の対処】

10）受注者は、本業務に使用するソフトウェア、電子計算機等に係る脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策、アクセス制御対策、情報漏えい対策を講じるとともに、契約期間中にこれらの対策に関する情報セキュリティ教育を本業務にかかわる従事者に対し実施すること。

11）受注者は、本業務の遂行において、情報セキュリティが侵害され、又はそのおそれがある場合の対処方法について担当職員に提示すること。また、情報セキュリティが侵害され、又はそのおそれがあることを認知した場合には、速やかに担当職員に報告を行い、原因究明及びその対処等について担当職員と協議の上、その指示に従うこと。

【クラウドサービス】

12）受注者は、本業務を実施するに当たり、民間事業者等が不特定多数の利用者に対して提供する、定型約款や利用規約等への同意のみで利用可能となるクラウドサービスを利用する場合には、これらのサ

ービスで要機密情報を取り扱ってはならず、2)に掲げる規程等で定める不正アクセス対策を実施するなど規程等を遵守すること。

13) 受注者は、本業務を実施するに当たり、利用において要機密情報を取り扱うものとしてクラウドサービスを調達する際は、「政府情報システムのためのセキュリティ評価制度（ISMAP）」の ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリストから調達することを原則とすること。

14) 受注者は、前 2 項におけるクラウドサービスの利用の際は、提供条件等から、利用に当たってのリスクの評価を行い、リスクが許容できることを確認して担当職員の利用承認を得るとともに、取扱上の注意点を示して提供し、その利用状況を管理すること。

【セキュアな情報システム（外部公開ウェブサイトを含む）の構築・運用・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。

別紙

令和　年　月　日

経済産業省○○○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）	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８）	本業務を終了又は契約解除する場合には、受注者において本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）を速やかに担当職員に返却し、又は廃棄し、若しくは消去する。その際、担当職員の確認を必ず受ける。	
情報セキュリティに関する事項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、リスクが許容できることを確認して担当職員の利用承認を得るとともに、取扱上の注意点を示して提供し、その利用状況を管理すること。	
情報セキュリティに関する事項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）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。 ・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））。）