（別紙）

実施計画書（仕様書）

１．事業名

令和５年度化学物質規制対策（化学物質管理の信頼性確保のための調査）

２．事業目的

ＯＥＣＤテストガイドライン及びＧＬＰ（Good Laboratory Practice：優良試験所基準）に基づく化学品安全性に係る試験データについてＯＥＣＤ加盟国等での相互受入を求めることで、試験実施の重複を避け、貿易の円滑化を促進するための仕組みとして、ＭＡＤ（Mutual Acceptance of Data：データの相互受理。１９８１年にＯＥＣＤ理事会にて採択。）が国際的に運用されている。

このＭＡＤの実効性を担保する観点から、ＯＥＣＤ関係国の監視当局メンバーで構成される国際評価チームによるＯＥＶ（On-Site Evaluation Visit：現地評価査察）が行われ、試験施設における試験データの信頼性やＧＬＰ試験施設としての適合性を確保するために必要な要件が継続的に充足されているかについて、定期的に確認を受けることとされている。

我が国では、化学物質の審査及び製造等の規制に関する法律に基づく化学物質ＧＬＰに対するＯＥＶが本年１０月に予定されていることから、本事業は、ＯＥＶの準備及び当日対応に万全を期すため、令和４年度に引き続き、我が国の化学物質ＧＬＰ制度に関するＯＥＣＤ国際評価チームへの提出資料の取りまとめ等を行う。

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、以下の（１）～（５）に示す事業内容を滞りなく実施する。

事業実施に際し、経済産業省製造産業局化学物質管理課化学物質安全室の担当者（以下「担当職員」という。）に加え、我が国の化学物質ＧＬＰ制度を運用する関係省庁及び関係機関の担当者とも協議を行うことがある。

また、本事業の進捗状況の確認、新たに生じた対応に係る作業方針の決定、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、受託者と担当職員との打合せを実施することとする。

（１） 化学物質ＧＬＰ制度の論点に係る検討

国内外のＯＥＶの評価事例（７事例程度）、ＯＥＣＤ評価チームのコメントがＯＥＣＤ　ＧＬＰ文書のどの部分に基づくものかを調査し、当省が所掌する化学物質の分解度試験及び濃縮度試験の基準適合確認業務に関する監視当局としての運用文書（以下「運用文書」という。）との関係性について確認する。

（２） ＯＥＣＤ国際評価チームへの提出資料の取りまとめ

ＯＥＶに際して、ＯＥＣＤ国際評価チームに提出する資料を用意するため、担当職員と協議の上、以下①及び②の対応を行う。

① 評価報告書テンプレート資料案の検討

我が国の化学物質ＧＬＰ制度における監視当局は、ＯＥＣＤ国際評価チームに対し、化学物質ＧＬＰ試験施設への査察手順や評価手続き等に関する質問事項（１２０問程度）への回答資料（評価報告書テンプレート資料）をＯＥＶの前に提出する必要がある。

このため、運用文書等に基づく評価報告書テンプレート資料案（英語版）について、前回のＯＥＶの際に提出した評価報告書テンプレート資料を参照しつつ、令和５年６月１９日までに取りまとめる[1]。

② 我が国の化学物質ＧＬＰ制度に係る説明資料の作成

ＯＥＶ当日に当省がＯＥＣＤ国際評価チームに対して説明を行う、査察手順や運用文書の体系等の我が国の化学物質ＧＬＰ制度に係る資料案（英語版）を作成する。

（３） 化学物質ＧＬＰ制度における監視当局の運用文書改訂案の取りまとめ

運用文書の改定内容について、ＯＥＣＤ文書との整合性を確認するとともに、前回のＯＥＶから改定があった部分（３０ページ程度）について、日本語から英語へ翻訳を令和５年７月２１日までに実施する。

（４） ＯＥＶ当日及び事後の対応

令和５年１０月２日及び１０月６日に実施予定となっている我が国の化学物質ＧＬＰ関係機関とＯＥＣＤ国際評価チームとの会議における議事録を作成し、その他査察におけるやり取りの記録を取る（実施場所は都内の予定。）。

また、ＯＥＶを受けて、ＯＥＣＤ国際評価チームからコメントがあった場合、担当職員と協議の上、当該コメントに対する対応案の検討を行う。

（５） 調査報告書の作成

本事業における検討結果や各種作成資料及び本事業において実施した打合せの開催状況・協議結果等を調査報告書として取りまとめる。

４．事業実施期間

委託契約締結日から令和６年３月１５日まで

５．納入物

①調査報告書電子媒体（ＣＤ－Ｒ又はＤＶＤ－Ｒ） １式

・調査報告書、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１）、二次利用未承諾リスト（様式２）を納入すること。

---

[1] 運用文書及び前回のＯＥＶの際に提出した評価報告書テンプレート資料については、本事業開始後に担当職員から提供する。また、公募期間中においては、経済産業省製造産業局化学物質管理課化学物質安全室の執務室内において閲覧可能とする。

・調査報告書は、ＰＤＦ形式に加え、機械判読可能な形式のファイルも納入すること。
・調査で得られた元データについては、機械判別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「Excel 等データ」という。）は、Excel 形式等により納入すること。なお、様式１及び様式２は Excel 形式とする。

②調査報告書電子媒体（ＣＤ－Ｒ又はＤＶＤ－Ｒ）　２式（公表用）
・調査報告書及び様式２（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な Excel 等データを納入すること。
・情報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削除するなどの適切な処置を講ずること。
・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報告書に盛り込む場合は、①事前に当該権利保有者の了承を得、②報告書内に出典を明記し、③当該権利保有者に二次利用の了承を得ること。二次利用の了承を得ることが困難な場合等は、下記の様式２に当該箇所を記述し、提出すること。
・公開可能かつ二次利用可能な Excel 等データが複数ファイルにわたる場合は、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取ること。
※Excel 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。
※調査報告書電子媒体の具体的な作成方法の確認及び様式１・様式２のダウンロードは、下記 URL から行うこと。
https://www.meti.go.jp/topic/data/e90622aj.html

６．納入場所
経済産業省製造産業局化学物質管理課化学物質安全室（本館６階西８）

７．情報管理体制
（１）履行体制
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、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。

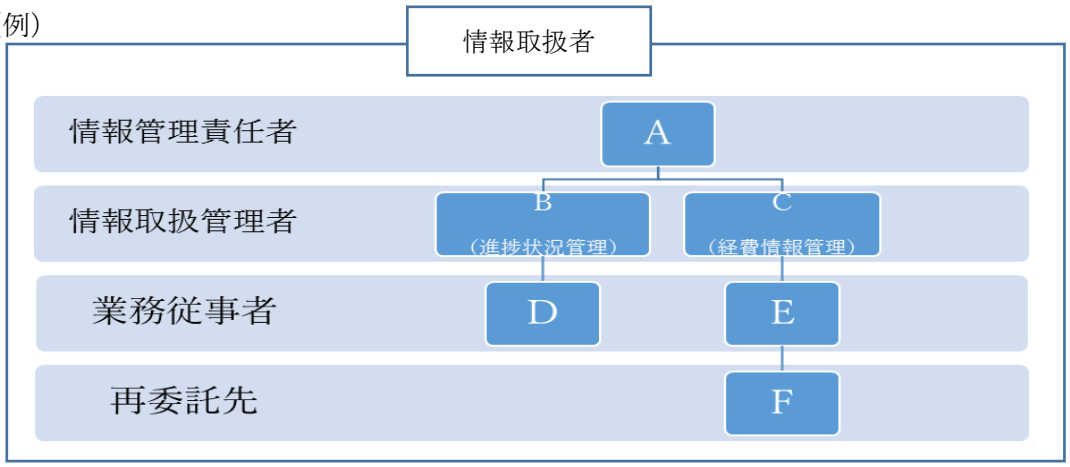
（※３）本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※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。

1）受託者は、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を定めたものを含み、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、担当職員と受託者が協議し不十分であると認めた場合、受託者は、速やかに担当職員と協議し対策を講ずること。

2）受託者は、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）受託者は、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）受託者は、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）受託者は、本業務を終了又は契約解除する場合には、受託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又は廃棄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）受託者は、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）受託者は、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）受託者は、「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「政府機関等の情報セキュリティ対策のための統一基準群（平成３０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）受託者は、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）受託者は、本業務に従事する者を限定すること。また、受託者の資本関係・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）受託者は、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）受託者は、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、受託者自身（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。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）受託者は、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）受託者は、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）受託者は、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）受託者は、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。そ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）受託者は、本業務を実施するに当たり、約款による外部サービスやソーシャルメディアサービスを利用する場合には、それらサービスで要機密情報を扱わないことや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。

18）受託者は、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や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や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。