（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．事業目的

「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。）では、国内で新たに製造又は輸入される化学物質（以下「新規化学物質」という。）について、事業者から提出された法定試験法に基づく分解性、蓄積性及び毒性等の試験結果をもとに、国による審査を実施している。

一方で、既に製造又は輸入を行っている一般化学物質等については、製造又は輸入事業者からの数量届出（製造・輸入数量、用途分類別出荷量等）や有害性報告等の情報を用いて国がリスク評価を実施している。このリスク評価では、法定試験とは条件（環境媒体、生物種等）が異なる法定試験法以外のデータも評価に利用しているため、法定試験法と法定試験法以外の両方のデータが得られる際、齟齬が生じる場合がある。

さらに、新規化学物質や一般化学物質等の評価において、法定試験法に基づくデータのみでは化学物質の実環境中での挙動をカバーしきれていない、また、国際的に認められた多数の試験法（ＯＥＣＤ（経済協力開発機構）テストガイドライン等）に基づくデータの利用が進んでいない、といった課題もある。

こうした中で近年、様々な利用可能なデータや情報を組み合わせて総合的に評価する手法（ウェイトオブエビデンス（ＷｏＥ））や試験・評価への統合的アプローチ（ＩＡＴＡ）（以下「ＷｏＥ等」という。）が、化学物質の性状評価において活用されてきている。この手法に基づき、単一の試験結果に依存することなく、多様なデータを活用して化学物質の評価を行うことにより、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が期待できる。

本事業は、昨年度に引き続き、化審法へのＷｏＥ等の導入に係る取組の一環として、化審法における生分解性評価マニュアルの改定案とテストケースを用いた妥当性の確認、底質環境への影響や底生生物への蓄積が懸念される化学物質の傾向の把握を行うとともに、低懸念高分子化合物の評価の合理化に向けた基礎資料の取りまとめを行うことを目的とする。

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。）との打合せを実施することとする。

（１）化審法におけるＷｏＥ等の導入に向けた検討

① 分解性評価へのＷｏＥ等の導入検討

令和４年度における本事業[1]では、個別物質の性状や情報の多寡等に応じた分解性評価を行うために令和３年度における本事業で作成した生分解性評価の実施に関するマニュアル案に沿った評価を試行するテストケースを実施し、その上で、有識者の意見を伺いながら、マニュアル案の実効性等の検証、マニュアル案の改訂方針の検討、さらには今後検討すべき課題の抽出を行った。

本年度事業では、昨年度の検討に引き続き、マニュアル案の実効性向上を目指して、多様な情報・データが評価に活用でき、様々なケースにおいてより適切に評価が行えるようにするための課題とその対応策につき整理・検討を行い、マニュアル改訂案の取りまとめを行う。その際、以下の観点・テーマを含め、独立行政法人製品評価技術基盤機構と協同して検討作業を進めることとする。

（ｉ）生分解性評価に用いる情報・データに応じた品質評価の方法及び判断基準の更なる明確化

（検討項目の一例）

・以下の観点も考慮した関連性評価における重み付けの方法及び重みの適切な設定等

- サマリー、二次情報（元となる文献情報が得られない場合）に基づく評価の方法及び判断基準
- OECD 等のガイドラインや GLP に準拠していない又は準拠が不明なデータの評価の方法及び判断基準

・易分解性試験以外の多様な種類のデータ（本質的分解性試験、シミュレーション試験、ＱＳＡＲ予測結果、類似構造物質による類推等）の評価項目及び判断基準

・ＱＳＡＲ予測結果、類似構造物質による類推、試験結果が相互に異なり、評価の判断が困難と考えられる場合の評価の方法

（ⅱ）現状のマニュアル案では評価の対象外としている「評価対象物質の環境媒体への分布」等の評価

（ⅲ）残留性の変化物の存在を推定できる予測モデル及びツールにつき、生分解性評価へ活用可能な範囲の整理

また、マニュアル案に沿った分解性等の評価結果の妥当性等を確認するため、必要に応じて、化審法データベース（Ｊ－ＣＨＥＣＫ [2]）に掲載されている化学物質（１～２物質程度）を対象として、実際にマニュアル案を用いて評価を試行するテストケースを実施することとする。テストケースに用いる情報を収集する際に、有料の文献データを得ることが必要な場合、あらかじめ担当職員と協議の上、具体的な検索方法や範囲を決定する。

さらに、上記の検討結果について、化学物質のリスク評価手法や国内外の化学物質規制制度に精通する有識者及び事業者等に対する意見聴取の機会（５名程度、２回程度）を設

[1] https://www.meti.go.jp/policy/chemical_management/kasinhou/information/report.html
[2] https://www.nite.go.jp/chem/jcheck/top.action?request_locale=ja

け、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。

② 蓄積性評価へのＷｏＥ等の導入検討

令和４年度における本事業では、化審法の蓄積性評価へのＷｏＥ等を導入するために令和２年度及び令和３年度における本事業の有識者ヒアリングで課題として提示された魚類以外の生物を用いた試験データの収集及び整備、さらには整備したデータを評価の材料とする際の課題及び解決方法について、有識者の意見を伺いつつ、具体的検討を行った。

本年度事業では、昨年度事業において蓄積性評価へのＷｏＥ等の導入に当たり有益であると示唆された底生生物の蓄積性とその評価に着目し、底質環境への影響や底生生物への蓄積が懸念される化学物質の構造及び物性又は用途や環境中への排出のされ方等の傾向を検討する際の知見その他の参考情報を得るため、以下の観点等から調査し、その結果を整理する。

・底生生物の蓄積性に関する情報・データが蓄積性評価に活用された海外事例
・化学物質による底質環境への影響を考慮することが必要と想定される、化学物質の使用方法、用途、時期、使用量、排出経路及びフガシティモデル等

（２）低懸念高分子化合物の評価の合理化に向けた検討

現行の化審法では、高分子化合物を評価する試験法として高分子フロースキーム試験を採用している。高分子化合物は一般に毒性等の懸念が低い傾向にあるが、諸外国と比較して、行政・事業者ともに審査や物質の同定等、化学物質管理に多くのコストを要しており、評価の効率化が課題となっている。

このため、令和４年度事業では、過去の判定に際して実施された高分子フロースキーム試験（平成２２年から令和３年までに判定を受けた新規化学物質のうち第６類（有機重合系高分子化合物）に該当する新規高分子化合物）を対象に試験結果をデータベース化し、低懸念と考えられる高分子化合物群を抽出して、評価の合理化案の方向性を検討した。

本年度事業では、令和４年度事業においてデータベース化を行っていない高分子フロースキーム試験（平成２２年から令和４年までに判定を受けた新規高分子化合物約７００物質を対象とし、その調査範囲等は担当職員と協議の上で決定する。これらの情報は、経済産業省から提供（貸与）する。）を対象に試験結果をデータベース化し、令和４年度事業で作成したデータベースに追加する。

また、拡充したデータベースを基に、担当職員と協議の上、令和４年度事業における検討課題への対応も踏まえつつ、少なくとも以下の観点から低懸念と考えられる高分子化合物の抽出・整理を行い、評価の合理化に向けた検討に資する基礎資料をとりまとめる。

・試験サンプルの数平均分子量、重量平均分子量
・水、酸、アルカリ及び有機溶媒への溶解性

・変化しなかった単量体の種類（官能基ごと）
・変化した場合はその単量体の種類
・生成した変化物の種類
・含有するイオン性官能基
・含有する開始剤及び連鎖移動剤
・安定性試験の重量変化率が負の値となる物質の構造的特徴

さらに、上記の検討結果について、高分子化合物の試験法や評価手法に精通する有識者等に対する意見聴取の機会を設け、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。

４．事業実施期間

委託契約締結日から令和６年３月２５日まで

５．納入物

①　調査報告書電子媒体（ＣＤ－Ｒ等）　１式
・調査報告書、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。
・調査報告書については、PDF 形式に加え、WORD 形式のファイル及び EXCEL 形式で整理したデータについては EXCEL 形式のファイルも納入すること。また、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等）　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。

※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/meti_lib/jyutaku/CD-sakuseihouhou.pdf

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。

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。

（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１「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。

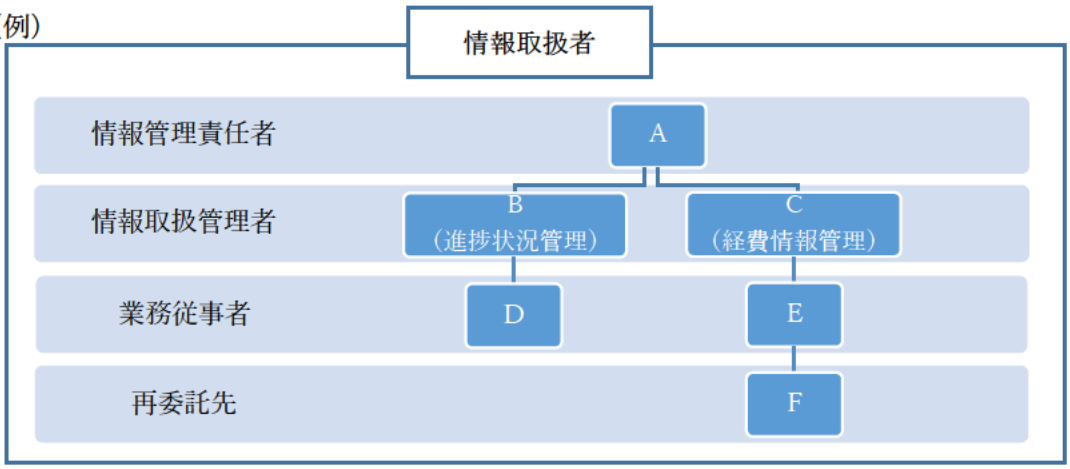
（※３）本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※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１）

○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。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） 受託者は、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、受託者は、委託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、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。