（別紙１）

実施計画書（仕様書）

１．件名

令和６年度化学物質規制対策（PRTRデータ分析システムの整備）

２．背景と目的

「特定化学物質の環境への排出量の把握等及び管理の改善の促進に関する法律(化管法)」では、一定の要件を満たす事業者に対し、政令で指定する第一種指定化学物質(５１５物質)について、事業所から環境への排出量及び廃棄物に含まれての事業所外への移動量を、事業者自らが把握し、事業所毎に国に届け出ることを義務付けている。

国は事業者から届け出られた排出量･移動量の集計結果及び届出対象外の排出量の推計値の集計結果を公表している。これとともに、個別事業所毎のＰＲＴＲデータについてもホームページ上で公表しており、当該データの集計･比較･印刷･ファイル出力を行うシステムである「ＰＲＴＲデータ分析システム・ＰＲＴＲけんさくん」も併せてホームページ上に掲載している。
(https://www.meti.go.jp/policy/chemical_management/law/prtr/7_6.html)

令和３年の化管法施行令の改正により、届出の対象となる第一種指定化学物質が変更され、また、化管法施行規則の改正により、届出様式が変更されており、これらの変更は、令和６年度の届出（令和５年度排出分）より適用される。本事業では、これらの変更等に対応するため、「ＰＲＴＲデータ分析システム・ＰＲＴＲけんさくん」の改修を行うとともに、システムの機能を向上させ、更なる利便性を高めることにより、国民等がＰＲＴＲデータを活用しやすくすることを目的とする。

３．事業内容

３．１　事業概要

「ＰＲＴＲデータ分析システム・ＰＲＴＲけんさくん」の改修、機能拡充を行うこと。その際、現在運用中のシステムについて、一般公開中のシステム等を参照する他、経済産業省（当省）から提供する概要設計書、詳細設計書、プログラム説明書等の過去の開発ドキュメント及び実際の動作を確認し、全体の機能及び動作を十分に理解して、作業を実施すること。なお本事業は３カ年継続事業であり、令和６年度は最終年度にあたるため、令和５年度までに作成された基本設計書、詳細設計書、単体テスト結果報告書等を十分に確認、理解した上で、システムの実装にむけた作業を実施すること。

３．２　情報システムの要件

以下、（１）から（９）のとおりの改修等を予定している。当該項目について、令和５年度に作成した詳細設計書及び単体テスト結果を踏まえ、結合テスト、統合テスト及び受け入れテストのそれぞれについてテスト計画案、試験結果報告書を作成し、操作マニュアルの作成も行うこと。

（１）ファイル取込及びファイル出力の改修

令和５年度排出分以降の届出では、届出の対象となる第一種指定化学物質、届出事項（届出事業者の法人番号、号番号から管理番号への変更）が変更されることから、令和５年度排出分以降について「本紙」、「別紙」、「その他業種」のファイルを正しく読み込み、出力されるよう改修する。

（２）検索･抽出の改修

令和５年度排出分以降の届出では、届出の対象となる第一種指定化学物質が変更されたことから、検索・抽出条件の「第一種指定化学物質」のリストを変更し、令和５年度排出分以降について検索・抽出が正しく行われるよう改修する。

（３）排出量集計の改修

令和５年度排出分以降の届出では、届出の対象となる第一種指定化学物質が変更されたことから、集計設定画面の「第一種指定化学物質別」のリストを変更し、令和５年度排出分以降について正しく集計結果が表示されるよう改修する。

（４）比較機能の改修

現状の比較機能においては、「経年比較(地域別・事業所別)」、「増減比較(事業所別)」において、それぞれ異なる検索項目が設定されている。いずれの比較機能においても「第一種指定化学物質を指定」することができるが、令和５年度排出分以降について新たな第一種指定化学物質リストでの正しい比較・結果が表示されるよう改修する。

（５）印刷様式の改修

省令改正に伴い、事業所の「法人番号」追加、第一種指定化学物質の号番号が管理番号に変更となっていることから、令和５年度排出分以降について個別事業所ごとの帳票印刷や比較 結果画面の印刷等のシステム内の全ての印刷様式にこれらの項目を追加・修正する。

排出年度は西暦で表示することに変更する。

（６）動作条件のバージョンアップ対応

現状の「ＰＲＴＲデータ分析システム・ＰＲＴＲけんさくん」の動作条件を更新すること。動作検証用の環境を用意し、すべての機能が完全に動作することを確認すること。

表１　動作環境

	現行	改修後
OS	日本語Microsoft Windows XP (SP3) / Vista / 7	Microsoft Windows 11 / 10
CPU	各OSが稼働する環境	各OSが稼働する環境
メインメモリ	OS推奨のメモリ数とする	OS推奨のメモリ数とする
ディスプレイ	解像度1024×768ピクセル以上推奨	解像度1024×768ピクセル以上推奨 （画面拡大率を設定された場合でも正常に表示・ボタン等押下できること。）

（７）メンテナンス機能等について

本システムは、現状と同様にCDから直接起動可能とし、インターネット上からダウンロードして使用する場合には、プログラムをPCにインストールすることなく起動が可能となる形式による仕様とすること。

（８）ヘルプ機能等の修正

今回のシステムの改修により変更された箇所について、ヘルプ機能及び操作マニュアルの修正を行う。また、操作マニュアルについては簡易版も作成する。

（９）コード証明書の組み込み

本システムを配布するにあたり、GPKIから配布されるコード証明書を添付する必要がある。経済産業省が提供するGPKIから発行を受けたコード証明書を本システムに組み込むこと。この時生成される秘匿鍵、公開鍵の扱いについては厳重に注意を払うこと。なお、GPKIから配布されるコード証明書は２要素認証のUSBトークンによって提供されるEV コード証明書である。

３．３　規模等要件

データ量

①本システム一式：　約42MB
（アプリケーション本体、ヘルプ機能ファイル等を含む）

②単年度のデータ量： 約60MB(CSV形式)

３．４信頼性等要件

（１）上位互換性要件

オペレーティングシステム、ミドルウェア、ソフトウェア等がバージョンアップした場合は、必要な調査、改修等を実施することで、バージョンアップに対応可能なシステムとすること。

（２）システム中立性要件

①受託者以外でも、システムの運用・保守が実施できるよう、技術の検討に当たっては国際規格や日本産業規格等のオープンな標準に基づく技術を選択すること。

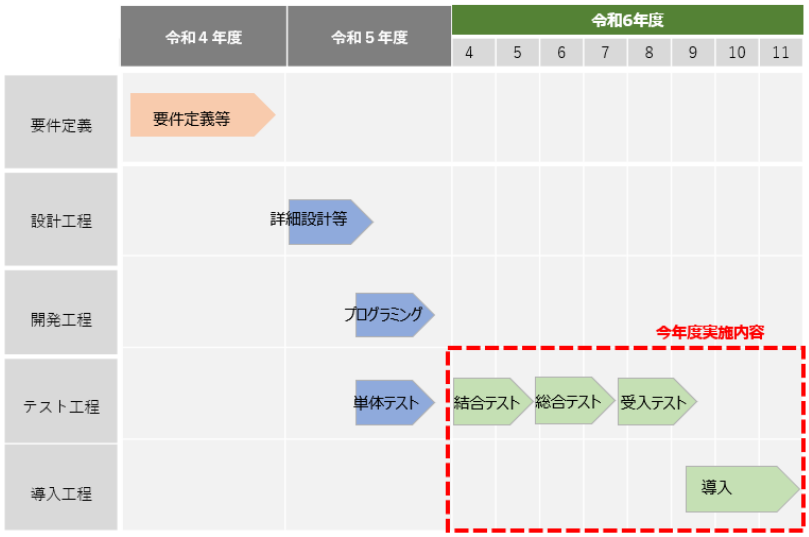
②データに対するインタフェース、通信プロトコル等の技術検討に当たっては、国際規格や日本産業規格等のオープンな標準に基づく技術を選択すること。

４．実施スケジュール

本事業は３年に分けて行う。令和４年度は要件定義書及び基本設計書の作成、試験計画及び項目書の作成まで、令和５年度は詳細設計書の作成から単体テストまでの工程を実施した。令和６年度は、結合テスト、総合テスト、受け入れテストを行い、１０月頃までにシステムの実装を行う。

スケジュールについては受託後に経済産業省担当課室（以下担当課室）と協議の上、必要に応じて変更又は詳細化を行うこと。

・表２　作業スケジュール案



５.作業の体制及び方法

５．１　開発環境等

（１）受託者は、システム開発に必要な作業場所、システム開発に必要な機器、開発機器に必要な設置場所及び備品･消耗品を自ら用意すること。

（２）システム全体について、生産者の如何にかかわらず受託者が最終責任を負うこと。

（３）作業場所の入退室管理、作業場所内での開発機器、情報の取り扱い等については、経済産業省情報セキュリティポリシー等に基づき、受託者が責任を持って管理すること。

（４）現在運用中の「ＰＲＴＲデータ分析システム・ＰＲＴＲけんさくん」のシステムについて、経済産業省が提供する概要設計書、詳細設計書、プログラム説明書等の過去の開発ドキュメント及び実際の動作を確認し、全体の機能及び動作を十分に理解して機能向上を行うこと。なお、経済産業省が提供するデータ等は、以下のとおり。

・ＰＲＴＲ個別事業所データ(本紙、別紙及びその他業種(平成13年度～令和２年度))及び届出事業所台帳データ
・平成23年度に開発した「ＰＲＴＲデータ分析システム･ＰＲＴＲけんさくん」のCD-Rと手引書
・令和4年度化学物質安全対策（PRTRデータ分析システムの整備）にて作成した基本設計書等資料
・令和5年度化学物質規制対策（PRTRデータ分析システムの整備）にて作成した詳細設計書等資料
・届出対象業種、第一種指定化学物質、移動先の下水道終末処理施設の名称、廃棄物の処理方法、廃棄物の種類のリスト
・令和４年度ＰＲＴＲ個別事業所データ(本紙、別紙及びその他業種)のイメージ
・その他、事業実施において必要であると担当職員が認めたもの

５．２　契約不適合責任に関する事項

本件システムの開発、更改において以下に記す事象が発生した場合には、これを契約不適合にあたるものとする。

（１）期限までに納入された成果物の個数が調達仕様書に記す個数に比べて足りないとき。

（２）国の帰責事由によらずに、国と受託者が合意したプロジェクト計画書で予定された工程の全てが納入期限までに完了しないとき、もしくは完了しないことが明らかになったとき。

（３）国の帰責事由によらずに、国と受託者が合意した要件の全てが満たされないとき。

（４）国の帰責事由によらずに、ユーザの業務に支障が出ることが想定される不具合が残存しているとき。

（５）受入試験中および納品後に発見された不具合について、その改修計画または調査計画立案および不具合残存中の対応策検討の為の協議に受託者が応じないとき

（６）受入試験中および納品後に発見された不具合について、その改修計画または調査計画、不具合残存中の対応策について国と受託者が合意した期限までに示されないとき。

（７）国の帰責事由によらずに、国と受託者が合意した期限までに不具合の改修が完了しないとき、もしくは完了しないことが明らかになったとき。

（８）なお、受託者が契約不適合責任を負う期間については、本業務について検収を行った日を起算日として１年間とする。

５．３　著作権

本事業において納品される成果物の著作権は、完成検査が完了した時点で、経済産業省に移転する。

受託者は、成果物の作成に当たり、第三者の著作権、工業所有権、ライセンス又はノウハウ(以下、著作権等という)を実施･使用するときは、その実施･使用に対する一切の責任を負う。また、受託者は、経済産業省以外の組織において成果物を活用する場合に調整が必要となる著作権等を一覧にした「ライセンス等に関する報告書」を作成の上、提出する。

５．４　その他

作業の進捗に関して、定期的（毎週、隔週等）に進捗報告会等を開催し、担当職員に進捗や課題について、 報告を行うこと。また、報告会終了後３営業日以内に議事録を提出し、担当職員の承認を得ること。

本作業の実施に当たっては、原則として「デジタル・ガバメント推進標準ガイドライン」
（https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/8a3b6203/20230331_resources_standard_guidelines_guideline_01.pdf）等に記載された事項を遵守すること。また、今後契約期間中に当該文書が改定された場合には、それに従うこととするが、より良い作業の進め方について提案がある場合には、担当職員に提案、協議の上、当該提案に基づき実施してもよい。

６．事業実施期間

委託契約締結日～令和６年１１月２９日

７．成果物の納入

本調達における納入成果物は以下のとおりである。

受託者は、納入物等について、納入期限までに当省の担当職員に内容を説明し、検収を受けること。内容に不備等が見つかった場合には、直ちに必要な修正等の対応を行い、担当職員に説明を行った上で、指定された期日までに再度納入すること。なお、納入成果物２については、工程の終了時に担当職員に内容を説明し、中間検収を受けること。

納入成果物の詳細及び編集方法並びに納入期限等はこの仕様書に定めるもののほかについては、担当職員と受託者が別途協議の上決定するものとする。また、以下に含まれていない場合であっても、担当職員及び受託者が必要と認める場合はこの限りでない。

プロジェクト計画書は、作業体制、作業内容及びスケジュール等について記載したプロジェクト計画書を策定し、 担当職員の承認を受けること。承認後に同計画書に修正の必要が生じた場合は、担当職員と協議の上、これを行うことができる。

表３　納入成果物

No	納入成果物	納入時期
プロジェクト管理関係		
1	プロジェクト計画書	契約締結日より５営業日以内
開発工程		
2	結合テスト計画書及び結果報告書	納入期限まで
3	総合テスト計画書及び結果報告書	納入期限まで
4	受け入れテスト計画書及び結果報告書	納入期限まで
5	成果物（システム）に関するデータ	納入期限まで

（１）電子媒体（ＣＤ－Ｒ又はＤＶＤ－Ｒ）　１式を提出すること。

（２）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。

８．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リスク評価室

９．不開示情報の取り扱い

（１）情報管理体制

①受託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）別紙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。

１０．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。

別紙様式

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。

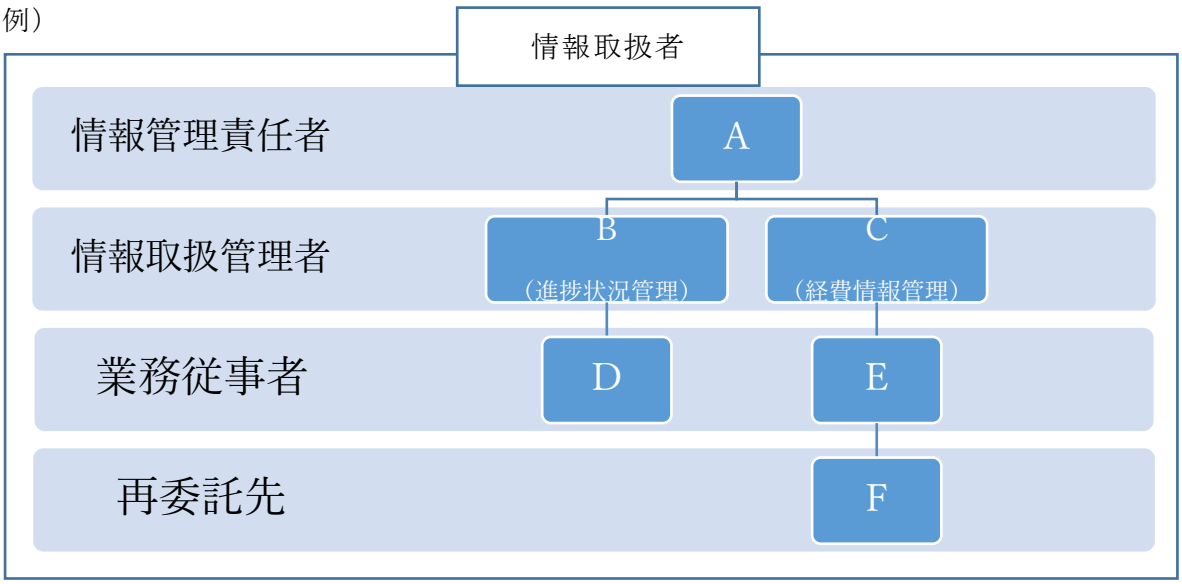
（※３）本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※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。