（添付資料２）

# 仕様書

１．事業名

令和８年度放射性廃棄物共通技術調査等事業（放射性廃棄物海外総合情報調査）

２．事業目的

我が国において、これまでの原子力発電の利用に伴って放射性廃棄物が発生しており、その処理処分対策を着実に進める必要がある。高レベル放射性廃棄物の地層処分や長半減期低発熱放射性廃棄物（ＴＲＵ廃棄物）をはじめとする低レベル放射性廃棄物の処理処分に係る関連政策や研究開発については、国や関係機関、処分実施主体等の適切な役割分担のもとで進めていくことが重要である。

これらの背景を踏まえて、本調査事業では、放射性廃棄物に係る海外の最新の政策や事業の動向を的確に把握し、国際的動向も踏まえた我が国の政策立案への反映を目的として、海外の放射性廃棄物に関連する情報を収集し、それらを関係者間で参照・活用が可能な形態としてデータベースを整備するとともに、幅広く情報普及を図るための情報の整理・発信を行う。

資源エネルギー庁は、これらの成果を、審議会等の資料として活用し、政策立案へ反映させるとともに、放射性廃棄物処分技術の信頼性向上の観点で国民の信頼感の醸成に役立てる。

３．事業内容及び実施方法

①諸外国における廃棄物処分の現状に関する情報収集と総合的なデータベースの整備

放射性廃棄物（高レベル放射性廃棄物のほか、中・低レベル放射性廃棄物や原子力事故で発生した放射性廃棄物も含む）の処分に係る技術情報として、国際機関における合意形成文書等の検討・策定状況、欧米やアジアの諸外国における処分政策や制度、研究開発、サイト選定（選定基準を含む）、処分事業・技術評価等の状況、法制度についての情報・データを収集し、原典、背景情報、主要文献の翻訳等から構成される総合的なデータベースとして整備する。具体的には、下記ア～エまでの作業を実施する。

ア．廃棄物処分計画・実施体制の状況調査

放射性廃棄物処分に関する具体的活動や計画を有するフィンランド、スウェーデン、フランス、スイス、英国、ドイツ、米国、カナダ等の欧米諸国、ロシア、中国、韓国、台湾等を中心に、各国の処分実施主体などの関係機関を活用するなどして法制度の整備状況、処分場開発の基本計画と体制、資金確保、技術開発、情報提供・広報、処分場サイトの選定動向、処分施設の許認可申請・発給の状況、関連する訴訟などの最新かつ信頼性が高い詳細な情報を収集する。また、原子力発電を小規模に利用しつつ、自国または共同での地層処分を検討している国々での取り組み状況についても情報収集を行う。これら収集した情報について翻訳を行い、データベースに登録する情報として整備する。

イ．諸外国のサイト選定における社会的要件及びサイト選定再実施事例の調査

我が国に先行して地層処分事業を進めているフィンランド、スウェーデン、フランス、英国、スイス、ドイツ、カナダ等を対象に、地層処分サイト選定において適用された社会的要件、適用段階、自治体・住民・規制機関への説明方法について、規制文書および実施主体の方針・実績の両面から情報収集を行う。さらに、サイト選定を再実施した事例については、その経緯や法改正の内容についても情報収集を行い、要点を整理する。これら収集した情報について翻訳を行い、データベースに登録する情報として整備する。

ウ．国際機関の情報収集

経済協力開発機構／原子力機関（ＯＥＣＤ／ＮＥＡ）、国際原子力機関（ＩＡＥＡ）、欧州連合（ＥＵ）等を対象として、放射性廃棄物処分に関する検討状況を調査するとともに、新たな出版物等を対象として関連文書の網羅性も確認しつつ翻訳を行い、データベースに登録する情

報として整備する。

エ．放射性廃棄物処分政策・法令文書等のデータベース整備

上記ア～ウの補完、より詳細レベルでの体系的な情報の取りまとめ等を目的として、収集した放射性廃棄物処分に係る政策文書及び法令等をデータベース化する。整備対象とする国は、フィンランド、スウェーデン、フランス、スイス、英国、ドイツ、米国、カナダ、ロシア、中国、韓国、台湾等を含め、整備対象とする文書には、各国の放射性廃棄物処分に係る政策、実施体制、サイト選定計画（選定基準を含む）、安全、環境、土地利用計画、原子力責任・損害賠償等に係る法令を含むものとする。

なお、データベースは、登録文書をカテゴリやタグで適切に分類し、データ閲覧機能（検索機能を含む）や利用者管理機能を有し、インターネットを通じて登録された利用者が利用可能なものとする。既往の関連調査において整備した「データベース管理システム※」等を用いて適切に管理する。また、データベースの日常的な保守・管理（データ登録作業、障害対応、ソフトウェアの更新等を含む）や改良等を行う。

※放射性廃棄物対策課において、令和７年度まで実施してきた関連調査事業「放射性廃棄物海外総合情報調査」及び「放射性廃棄物重要基礎技術研究調査」で構築されたデータベース（別紙１参照）

②情報の整理・発信・普及

データベースとして整備した情報等を活用し、国の政策立案に必要な情報の取りまとめを行うとともに、インターネット、技術情報資料の作成・配布等を通じて外部に向けて発信し、一般への周知、関係者の情報共有、知識普及を行う。インターネットの掲載場所は、原則として受託事業者のホームページとする。具体的には、以下の作業を実施する。

ア．インターネットでの情報発信

情報の信頼性に配慮しつつ海外の最新動向を即時性を有した形で共有化するための速報の作成とインターネットでの発信を行う。具体的には、主要国での放射性廃棄物処分等の概要、処分の進捗、法制度、資金確保、研究開発、スケジュールなどの最新の状況を整理し、インターネットで情報を提供する。なお、過去に情報発信した最新動向は、原子力環境整備・資金管理センターホームページ（http://www2.rwmc.or.jp/nf/）にて閲覧することができるため、参考とする。

イ．技術情報資料の整備

令和７年度までに作成した冊子のフォーマットを継承しつつ、①の情報収集結果や各国の事業進捗等を反映した改訂を行い、冊子を発行するとともに、それらの冊子を電子化してインターネットで発信する。冊子については、関係省庁、全国電力関係ＰＲ館等、関係原子力機関へ送付する（配布先の実績については別紙２にて記載）。これらの機関以外に、一般の方からの入手要望があった場合には、個別に冊子を送付することとする。印刷部数は、２０００部とする。送付先については経済産業省資源エネルギー庁の指示に従う。

ウ．一般向け技術情報資料の作成

①の情報収集結果や各国の事業進捗等について、一般向けに解説する冊子を試作するとともに、インターネットでの発信についても検討する。冊子で取り扱うトピックについては、これまでに開催された地層処分関連の講演会や説明会等での問合せも踏まえて検討することとする。トピックや冊子の印刷部数、活用方法については、経済産業省資源エネルギー庁と相談・調整の上、検討する。

③事業報告書の作成

受託事業者は、①、②の実施内容について、取りまとめた事業報告書を年度末までに作成し、提出する。なお、この事業報告書の作成に際しては、過去の同種の事業報告書
（http://www.enecho.meti.go.jp/category/electricity_and_gas/nuclear/rw/library/library

06.html）において公開されているものを参考にする。

④ 著作権等の扱い

下記ＵＲＬで取得できる、「契約条項 第２３条～第３３条」を参照する。

https://www.enecho.meti.go.jp/appli/advertisement/entrust/d-bay/2025/r7bayhdole-dml_format.pdf

⑤ 業務の引継ぎ

本事業の終了にともない受託事業者が変更となる場合には、資源エネルギー庁は、３.③ に示す事業報告書等をもとに次期受託事業者への引継ぎを行うため、資源エネルギー庁が業務完了前に受託事業者に対し、引継ぎに必要な資料を求めた場合は、これに応じる。

４．実施期間

委託契約締結日から令和９年３月３１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。
- 調査報告書については、ＰＤＦ形式に加え、機械判読可能[1]な形式のファイルも納入する。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。
- 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。

（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[2]な図表等データを、プロパティを含む状態で納入する。
- 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。
  - 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。
  - 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。
  - 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。

（３） 様式１～様式３について

- （様式１）委託調査報告書骨子[3]

[1] 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]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。

[3]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。

- 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。
- 図表は挿入せずテキスト形式で作成する。
- 見出しについては記載された項目のとおりとする。

- （様式２）委託調査報告書公表用書誌情報[4]
  - ファイル形式はＥｘｃｅｌ形式で納入する。
  - 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。
- （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（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。
- 様式１～３ダウンロード先
  - 委託調査報告書　（METI/経済産業省）

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。なお、具体的な納入方法は担当課室と協議の上、決定する。
- 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。

７．納入場所

資源エネルギー庁電力・ガス事業部放射性廃棄物対策課

８．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）（添付資料３）を契約前に提出し、担当課室の同意を得る（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。）。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。

（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。

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、同意を得る。

９．履行完了後の情報の取扱い

---

4 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。

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。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。

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「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。

別紙１

# データベース管理システムの概要

令和７年度までに関連調査事業で整備してきた放射性廃棄物の諸外国情報に係る「データベース管理システム」について、現行のシステムは、Microsoft Windows Server 2019 コンピュータにおいて動作する、Java サーブレットの動作環境及びデータベースエンジンから構成された Web アプリケーションである。外国語の原典文書及びその翻訳を１セット（組）で管理し、登録された文書の閲覧サービスを提供するものである。

技術情報データベース管理システムは、以下の機能を持つ。

①　データ閲覧機能

・登録文書の分類別表示
・個別文書（本文、原典）の表示（改正・改訂前の旧文書の表示を含む）
・全文検索と書誌情報による検索
・サイトマップ、ヘルプ等

②　データ登録機能

・原典文書ファイル及びその翻訳ファイルの登録（いずれも PDF 形式）
・登録文書の書誌情報及び分類の設定
・ナビゲーションページ用ファイル（HTML ファイル）の登録

【データベースの登録実績】

https://www2.rwmc.or.jp/

令和６年度にデータベースに登録した文書については参考資料に示す。

【現状でのデータ量（令和７年 12 月末時点）】

登録文書数：3,488 件（原典文書と翻訳の組を１件としてカウントする）

| 登録文書種別 | ファイル数 | ファイル容量 |
|---|---|---|
| 原典文書（英語） | 2,378 件 | 8,574MB |
| 原典文書（仏語） | 403 件 | 1,273MB |
| 原典文書（独語） | 338 件 | 699MB |
| 原典文書（フィンランド語） | 83 件 | 109MB |
| 原典文書（スウェーデン語） | 221 件 | 208MB |
| 原典文書（中国語） | 74 件 | 34MB |
| 原典文書（韓国語） | 131 件 | 132MB |
| 原典文書（その他の言語） | 327 件 | 723MB |
| 翻訳（PDF 形式） | 470 件 | 1,649MB |
| 翻訳（HTML 形式） | 3,018 件 | 3,125MB |
| その他（補助データ） | － | 7,560MB |
| 合計 | － | 約 24,086MB |

注：登録文書の原典文書は当該国の標準語で記述された文書であるが、参考英訳がある場合には、英語と英語以外の２つの原典をもつ場合がある。

③　管理者機能

・ユーザ管理（登録済みユーザ情報の管理やユーザ ID 申請関連の操作を行う）
・コメント管理（各データに書き込まれたコメントの一覧を表示）
・全データタイトル一覧表示（データベースに含まれる全てのデータタイトルの一覧を表示）
・履歴管理（各種操作履歴の一覧を表示）
・周知文管理（トップ画面へ表示したい周知文の作成）

以　上

（参考資料）令和 6 年度にデータベースに登録した文書

令和 6 年度

| | 国・機関 | タイトル | タイトル（外国語標記） |
|---|---|---|---|
| 1 | IAEA | 一般安全指針 GSG-18(2023) クリアランスの概念の適用 | General Saferty Guide No.GSG-18 Application of the Concept of Clearance |
| 2 | カナダ | 核燃料廃棄物管理機関とイグナスタウンシップ自治体間の立地活動協力協定 | Hosting Agreement between NWMO and The Corporation of the Township of Ignace |
| 3 | 英国 | 英国における放射性物質法の範囲及び免除に関するガイダンス | Guidance on the scope of and exemptions from the radioactive substances legislation in the UK |
| 4 | ドイツ | 電離放射線による有害な影響からの保護に関する法律（放射線防護法） | Gesetz zum Schutz vor der schädlichen Wirkung ionisierender Strahlung (Strahlenschutzgesetz - StrlSchG) |
| 5 | フランス | 2024 年フランスにおける放射性廃棄物の処分に関する技術情報 | 2024　Technical Information for Disposal of Radioactive Waste in France |
| 6 | フィンランド | 2024 年におけるフィンランドの放射性廃棄物処分制度と資金確保制度 | Radioactive waste disposal system and financing system in Finland in 2024 |
| 7 | スイス | NPB 24-02　放射性廃棄物の処分に関する技術情報、スイスにおける放射性廃棄物処分及び財務システムに関する調査 | NPB 24-02 Technical Information on Disposal of Radioactive Waste A Study on Radioactive Waste Disposal and the Financing System in Switzerland |
| 8 | スウェーデン | スウェーデンにおける放射性廃棄物処分システムに関する技術情報の更新 | Update of Technical Information on Radioactive Waste Disposal System in Sweden |
| 9 | ドイツ | ドイツの放射性廃棄物処分システムに関する調査　2024 年状況報告書 | Study on Radioactive Waste Disposal System in Germany Status Report 2024 |
| 10 | ICRP | ICRP 年報　放射性固体廃棄物の地表及び浅地中処分における放射線防護 | Annals of the ICRP 4 Radiological protection in Surface and 10 Near-Surface Disposal of Solid Radioactive |
| 11 | 米国 | 余剰プルトニウム処分　希釈及び処分オプションに関する独立コスト評価（ICE）レポート | Surplus Plutonium Disposition Dilute and Dispose Option Independent Cost Estimate (ICE) Report |
| 12 | スイス | 最も安全なサイト確保に向けて　スイスにおける地層処分場建設への道 | Securing the Safest Site　The Way to a Deep Geological Repository for Switzerland |
| 13 | スイス | ENSI-G23　その他の原子力施設の設計要件　指針の解説書 | ENSI-G23　Auslegungsanforderungen an andere Kernanlagen　Erlauterungsbericht zur Richtlinie |
| 14 | 英国 | 英国における放射性物質の管理及び廃止措置に関する政策枠組み | managing-radioactive-substances-and-nuclear-decommissioning-uk-policy-framework |
| 15 | ベルギー | 社会的議論に関する報告書と今後の政策案 | Rapport Forum de clôture pour parties prenantes : Un plan concret pour une future politique |

別紙２

技術情報資料の配布実績

技術情報資料「諸外国における高レベル放射性廃棄物の処分について」及び「諸外国における放射性廃棄物関連の施設・サイトについて」の令和６年度の主な配布先を下記に示す。

行政（国）

| | 配布先　部署 | 部数 |
|---|---|---|
| 1 | 経済産業省　放射性廃棄物対策課 | 40 |
| 2 | 内閣府　原子力政策担当室 | 12 |
| 3 | 原子力規制委員会（原子力規制庁） | 30 |
| 4 | 文部科学省放射性廃棄物企画室 | 5 |
| 5 | 環境省関東地方環境事務所 | 2 |
| 6 | 在フィンランド日本大使館 | 2 |
| 7 | 在スウェーデン日本大使館 | 1 |
| 8 | 在ドイツ日本大使館 | 1 |

行政（地方）

| | | |
|---|---|---|
| 1 | 経済産業省　北海道経済産業局 | 2 |
| 2 | 経済産業省　東北経済産業局 | 2 |
| 3 | 経済産業省　資源エネルギー庁　青森原子力産業立地調整官事務所 | 10 |
| 4 | 経済産業省　資源エネルギー庁　青森原子力産業立地調整官事務所六ヶ所連絡室 | 1 |
| 5 | 経済産業省　資源エネルギー庁　福島双葉地域担当官事務所 | 1 |
| 6 | 経済産業省　関東経済産業局 | 2 |
| 7 | 経済産業省　資源エネルギー庁　柏崎刈羽地域担当官事務所 | 1 |
| 8 | 経済産業省　中部経済産業局 | 4 |
| 9 | 経済産業省　資源エネルギー庁　若狭地域担当官事務所 | 1 |
| 10 | 経済産業省　近畿経済産業局 | 2 |
| 11 | 経済産業省　中国経済産業局 | 2 |
| 12 | 経済産業省　四国経済産業局 | 2 |
| 13 | 経済産業省　九州経済産業局 | 2 |
| 14 | 内閣府　沖縄総合事務局 | 2 |
| 15 | 青森県庁　原子力立地対策課 | 2 |

| | | |
|---|---|---|
| 16 | 茨城県庁　原子力立地対策課 | 2 |
| 17 | 福井県庁　原子力立地対策課 | 2 |

全国電力関係 PR 館

| | | |
|---|---|---|
| 1 | 日本原子力研究開発機構　むつ科学技術館 | 2 |
| 2 | エネルギー館　あしたをおもう森 | 2 |
| 3 | グリーンプラザ（仙台） | 2 |
| 4 | 日本科学未来館 | 2 |
| 5 | 科学技術館 | 2 |
| 6 | でんきの科学館 | 2 |
| 7 | 大阪市立科学館 | 2 |
| 8 | エネルギー科学館ワンダー・ラボ | 2 |
| 9 | 中国電力㈱鳥取支社　広報担当 | 2 |
| 10 | 中国電力㈱島根支社　広報担当 | 2 |
| 11 | 中国電力（株）岡山支社広報グループ | 2 |
| 12 | 電遊館エネルギア | 2 |
| 13 | ヨンデンプラザ中村 | 1 |
| 14 | ヨンデンプラザサンポート | 2 |
| 15 | J パワー&よんでん Wa ンダーランド | 2 |
| 16 | カエルぴあ | 2 |
| 17 | 原子力ふれあいコーナー | 2 |
| 18 | 原子力ＰＲセンターとまりん館 | 2 |
| 19 | 北海道原子力環境センター | 2 |
| 20 | 北通り総合文化センター（ウィング） | 2 |
| 21 | 東通原子力発電所「トントゥビレッジ」 | 2 |
| 22 | 宮城県環境放射線監視センター | 2 |
| 23 | 福島県原子力センター | 2 |
| 24 | 原子力科学館 | 2 |
| 25 | 日本原子力発電東海原子力館（東海テラパーク） | 2 |
| 26 | 柏崎刈羽原子力発電所サービスホール | 2 |
| 27 | 柏崎原子力広報センター　アトミュージアム | 2 |
| 28 | 原子力発電所温排水資料展示館 | 2 |
| 29 | 浜岡原子力館 | 2 |
| 30 | 静岡県原子力広報研修センター | 2 |
| 31 | 能登原子力センター | 2 |

| | | |
|---|---|---|
| 32 | アリス館志賀 | 2 |
| 33 | 原子力の科学館 あっとほうむ | 2 |
| 34 | 日本原子力発電敦賀原子力館 | 2 |
| 35 | 日本原子力研究開発機構アトムプラザ | 2 |
| 36 | 美浜原子力ＰＲセンター | 2 |
| 37 | 高浜発電所ビジターズハウス | 2 |
| 38 | 大飯発電所　エル・パークおおい「おおいり館」 | 2 |
| 39 | 若狭たかはまエルどらんど | 2 |
| 40 | 島根原子力館 | 2 |
| 41 | 海来館（みらいかん） | 2 |
| 42 | 原子力保安研修所 | 2 |
| 43 | 伊方ビジターズハウス | 2 |
| 44 | 愛媛県伊方原子力広報センター | 2 |
| 45 | 玄海エネルギーパーク | 2 |
| 46 | 川内原子力発電所展示館 | 2 |
| 47 | 川内環境監視センター | 2 |
| 48 | 六ケ所原燃ＰＲセンター | 2 |
| 49 | 人形峠アトムサイエンス館 | 2 |
| 50 | 日本原子力研究開発機構 きっづ光科学館ふぉとん | 2 |
| 51 | 日本原子力研究開発機構 むつ科学技術館 | 2 |
| 52 | 日本原子力研究開発機構 大洗わくわく科学館 | 2 |
| 53 | 日本原子力研究開発機構 ゆめ地創館 | 2 |
| 54 | 日本原子力研究開発機構　幌延深地層研究センター敷地内　実規模施設展示施設 | 30 |

関係機関（研究所等）

| | | |
|---|---|---|
| 1 | 電気事業連合会　原子力部 | 5 |
| 2 | 電気事業連合会　最終処分推進本部 | 10 |
| 3 | 原子力発電環境整備機構 | 200 |
| 4 | 国立研究開発法人　日本原子力研究開発機構　核燃料サイクル工学研究所　ＢＥ資源・処分システム開発部 | 100 |
| 5 | 国立研究開発法人　日本原子力研究開発機構　バックエンド領域埋設事業センター | 3 |
| 6 | 公益財団法人　北海道科学技術総合振興センター　幌延地圏環境研究所 | 5 |

| | | |
|---|---|---|
| 7 | 国立研究開発法人　産業技術総合研究所　地圏資源環境研究部門 | 5 |
| 8 | 国立研究開発法人　量子科学技術研究開発機構　放射線医学総合研究所　企画部企画課外部資金係 | 3 |
| 9 | 公益財団法人　地震予知総合研究振興会 | 5 |
| 10 | 公益財団法人　原子力安全研究協会 | 5 |
| 11 | NHK 報道局科学文化部 | 3 |
| 12 | 一般社団法人　日本電気協会新聞部　電気新聞　編集局報道室 | 3 |
| 13 | 一般財団法人　電力中央研究所　サステナブルシステム研究本部研究統括室 | 5 |
| 14 | 国立研究開発法人　海洋研究開発機構　経営企画部経営戦略課 | 5 |
| 15 | 一般財団法人　日本原子力文化財団 | 1 |
| 16 | 一般社団法人　日本原子力産業協会 | 1 |
| 17 | 一般社団法人　日本原子力学会 | 1 |
| 18 | 日本学術会議 | 1 |
| 19 | 公益財団法人　原子力バックエンド推進センター | 1 |
| 20 | 一般財団法人　大阪科学技術センター | 1 |

（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

経済産業省資源エネルギー庁○○○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。<br>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。<br>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<br>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。<br>（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。<br>（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。<br>（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。<br>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。<br>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。<br>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。<br>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。<br>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。<br><br>（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。<br>（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。<br>（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。<br>（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。<br>（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。<br>・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。<br>・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。<br>・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。<br>（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。<br>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。<br>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。<br>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<br>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。<br>（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。<br>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。<br>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。<br>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。<br>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。<br>（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。<br>（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。<br>（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。<br>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<br>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。<br>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。<br>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））。）