千葉県環境研究センター基本計画策定支援業務委託　仕様書（公募用）

１　適用範囲

本仕様書は、千葉県（以下「甲」という。）が発注する「千葉県環境研究センター基本計画策定支援業務」（以下「業務」という。）の企画提案募集及び業務委託に付す場合において適用される主要事項を示すものである。

この仕様書は業務の大要を示すものであり、最終的な業務委託仕様書は、受託者（以下「乙」という。）決定後、協議の上、甲が作成する。

２　委託業務名

千葉県環境研究センター基本計画策定支援業務

３　委託期間

契約締結日から令和７年３月２４日（月）まで

４　業務の目的

令和６年３月に策定した千葉県環境研究センター基本構想（以下「基本構想」という。）において、市原地区（新館、本館）と稲毛地区（水質棟、地質棟）に敷地と庁舎が分散している千葉県環境研究センター（以下「環境研究センター」という。）については、著しい老朽化を契機として、効率的な研究施設への再編整備を図り、１箇所に機能を集約した新たな環境研究センターを整備することとしている。

本業務は、基本構想を踏まえた新たな環境研究センターの整備に向けて、施設に必要な機能を整理し、建設場所の選定に係る調査・分析を行った上で、建設場所における具体的な施設・設備等の検討を行い、有識者の意見を取り入れながら、令和６年度中に甲が「千葉県環境研究センター基本計画（以下「基本計画」という。）」を策定するために必要な支援を行うことを目的とする。

５　業務の内容

以下に業務の概要を示すが、企画提案内容により業務内容を一部変更する場合がある。

（１）環境研究センターの調査及び必要な機能の整理

ア　現況調査

甲と調整の上、環境研究センターを訪問し、建物構造、配線配管、各部屋の間取り、職員の机や分析検査機器の設置状況、倉庫、駐車場等について調査する。また、環境研究センターの職員に対して、現在の施設運用状況、新たな環境研究センター（以下「新センター」という。）に求める施設・設備等に関するヒアリングを行い、現状を把握する。

イ　他事例の調査

新センターの整備の参考となる基礎情報として、環境分野等の他の研究施設（３～５施設）において、以下の項目を参考に調査を行う。

①基本情報（人員及び施設概要（面積等)、平面・立面イメージ図）

②組織の状況（職種構成、人事異動、人事交流等、評価指標）

③施設のあり方、整備コンセプト

・建設場所選定の考え方

・バリアフリー、ユニバーサルデザイン

④分析、研究に係る機器・物品等の状況（検査機器等の配置状況、薬品管理等）

⑤施設の主な機能

・施設の必要スペック（電気容量、排気・廃水処理設備の設計思想、空調・換気等）

・安全対策（建物及び情報のセキュリティ対策、ケミカルハザード対策）

・防災対策

・その他の執務環境（執務室、トイレ、休憩室、会議室等）

⑥環境対策

・再生可能エネルギー等の活用（ＺＥＢ等の対応状況）

・機器等の導入に係る環境配慮物品の調達の考え方

⑦その他、業務環境の向上に係る工夫（職員が意見交換を行うラウンジ等）

⑧大学や他の研究機関等との連携

⑨行政課題と研究をリンクさせる仕組み

⑩外部利用機能（研修室、県民向け学習施設、展示施設）

⑪供用後に判明した施設等に関する課題（設計時に想定しなかった不具合等）

ウ　新センターに必要な機能の整理等

ア、イの調査を踏まえ、新センターに必要な機能とともに、施設整備に関係する法令、資料を整理する。

関係する法令については、建築基準法等の建築関係法令の他、施設の機能や立地の特性上、確認が必要となるものを含めること。

（２）建設場所の選定に係る調査・分析

契約締結後に甲が提示する候補地検討に係る諸条件を踏まえ、乙は建設候補地を甲に提案（３箇所程度）する。また、甲による建設場所の選定に資するよう、当該候補地について、以下の点を参考に調査・分析し、優位性を比較検討する。

ア　基本与件（敷地面積、容積、建ぺい率、用途地域。埋蔵文化財、土壌汚染の可能性について）

イ　建築計画への影響項目（災害による影響（液状化、浸水、土砂災害、倒木)、概算費用（解体、造成、仮移転)、想定地下水位、想定支持地盤）

ウ　計画可能面積（階あたりの床面積、最大延床面積、駐車場）

また、これを踏まえた断面構成イメージ

エ　業務環境の優位性

・交通の利便性

・関係機関（国、県、市町村及び大学等）との連携容易性（近隣の立地状況）

オ　工事施工への影響要因（工事車両の通行、安全性等）

カ　周辺地域への景観面・環境面の影響

キ　その他、整備スケジュールや概算事業費への主な影響項目

（３）施設・設備に係る検討

（２）の検討を経て、甲が選定した建設場所について、（１）ウで整理した、新センターに必要な機能を踏まえ、総事業費の削減に配慮しつつ、以下に掲げる内容等について整理・検討する。

ア　必要な施設機能と必要面積の算出

業務内容を踏まえた新センターに必要な施設機能と必要諸室、諸室に係る必要面積及び整備条件等を整理する。

イ　配置計画の検討

動線、利便性、作業の効率化等を考慮した配置計画（平面、立体のゾーニング）を検討の上、具体化・可視化する。

ウ　設備・備品計画の検討

①　分析機器類・備品に係る、移設・廃棄・新規購入の区分

②　電気、空調、ガスや水道管の配管、配線等の設備計画

③　業務に必要な、ＩＣＴや情報化に対応した設備・備品の導入　他

エ　土地利用計画の検討

敷地の法的条件を考慮した建築物、緑地、駐車場の配置等を具体化し、図示する。

オ　留意事項

①　施設の長寿命化のために、将来の大規模改修を見越した配置・構造であること。

②　設備点検や修繕等のメンテナンスが容易に行える構造とすること。

③　環境対策に万全を期した設計であること。

- 再生可能エネルギー等の活用方針を検討し、原則ＺＥＢ設計とする。
- 「千葉県庁エコオフィスプラン」に基づく、省エネルギー機器導入等の検討。

④　十分な事務作業スペース及び公文書等が適切に保管できるスペースを確保すること。

⑤　共同作業や闊達な意見交換が行いやすいオープンな研究環境の実現に配慮すること。(例：複数の分析機器を集約した分析室、データ解析室の集約、ラウンジの設置等)

⑥　外部利用（研修室、県民向け環境学習施設や展示施設）に関する提案を含めること。

（４）その他整備事業に係る検討

ア　スケジュール

新センター供用までの整備事業に係る全体スケジュールを作成する。スケジュールは建築条件や関係法令を踏まえ、無理が生じないものとすること。また、事業が円滑に進められるよう考慮すべき点についても整理する。

イ　概算事業費

建設場所、施設規模等を踏まえるとともに、既存施設からの移転等を考慮して、概算事業費（総額及び年度別）を算出する。

概算事業費の算出に当たっては、算出の考え方及び手法を甲と十分に調整すること。

ウ　移転

移転作業工程の概要及び新センターの供用準備に関する検討事項を整理する。

エ　設計与件等の整理

基本設計の作成に資するよう、設計与件（建設場所の現況図、諸室面積一覧、施設配置計画案等）について整理する。

（５）外部有識者会議における意見の反映

ア　今後、甲が設置・運営する（仮称）千葉県環境研究センター基本計画検討会議（外部有識者で構成）における意見を（２）～（４）の業務に反映する。

イ　会議の時期及び内容は以下を想定している。

第１回（　９月下旬）：新センターに必要となる機能の整理、建設候補地及びその比較検討方法の提示

第２回（１１月下旬）：建設場所、施設・設備の提示

第３回（　２月上旬）：基本計画案の検討

（６）基本計画作成の支援

ア　甲が作成する基本計画案（１２月頃を予定）に図面の挿入とレイアウト調整を行う。

イ　ビジュアルイメージ図を盛り込んだ基本計画案概要版（基本計画案の概要及び施設の空間構成や施設配置を表現した概略平面図・断面図等）を作成する。

ウ　第３回有識者会議後に甲が作成する（２月下旬を予定）基本計画及び概要版のレイアウト調整を行う。

６　業務スケジュール（予定）

令和６年　７月　　契約

令和７年　１月中旬　基本計画案のレイアウト調整、計画案概要版の作成
令和７年　３月　　成果品の提出（納品）

７　再委託について

（１）乙は、業務の全部を第三者に委任し、又は再委託してはならない。ただし、高い効果が見込めると県が判断した場合、若しくはプロポーザルの企画提案書等に沿った業務体制と認められる場合は、業務の一部を再委託することができる。
（２）（１）で認められた場合、乙は、再委託の相手方、再委託する理由及び内容、契約金額、その他必要事項をあらかじめ甲に提出し、承認を受けなければならない。

８　委託金額

（１）委託金額の上限
　　１７，０００，０００円（消費税及び地方消費税を含む）
（２）支払い方法
　　委託料の支払い方法は、精算払いとする。

９　職員等

業務を実施するに当たり、乙は、甲の意図及び目的を十分理解した上で、一級建築士を含む経験のある職員その他適切な人員を配置し、正確かつ丁寧にこれを行わなければならない。なお、業務従事者の中から県との情報共有、業務の進捗・課題管理を行う統括責任者を１名選任し、契約後、直ちに県へ通知すること。

１０　業務の進め方

（１）乙は、契約締結後、甲が指定する期日までに業務全体の作業工程計画を作成し、甲に事業計画書を提出するものとする。
　なお、作業工程は、５（５）外部有識者会議の開催時期を考慮の上、作成すること。
（２）乙は、業務の遂行に当たり、当該契約に基づき、甲と密接に連携をとり、その指示及び監督を受けなければならない。
（３）当該業務に係る打合せについては、終了後速やかに議事録を作成し、報告すること。
（４）乙は、業務の遂行上疑義が生じた事項、仕様書に明記していない事項については、甲と協議を行い、その指示に従わなければならない。

１１　成果品及び提出期限

以下の成果品を提出期限までに提出すること。
（１）成果品
ア　紙媒体　３部

・本業務において収集、作成した資料
・打ち合わせ資料(議事録含む)
イ　アのデータを記録した電子媒体（データ化できないものを除く）一式

（２）提出期限
令和７年３月２４日（月）まで
ただし、成果品の原稿案を令和７年３月１７日（月）までに提出し、甲の了解を得た上で成果品を提出すること。

１２　資料の貸与等

業務を進めるにあたって、県が所持する以下の情報を提供する。
・　対象施設の図面写し
・　主要備品一覧
・　過去の調査結果（平成 25 年度環境研究センターの機能強化に係る調査業務委託報告書)
なお、県が提供する情報、資料等については、県の許可なく第三者に流布することのないようにすること。その他必要な資料については、協議による。

１３　特記事項

（１）成果品及び作業工程における印刷物、書類等に対する一切の権利は、甲に帰属し、乙は甲の承認を受けずに使用、貸与及び公表等することはできない。
（２）乙は甲に対し、業務の目的の範囲内で成果品（乙が既に著作権を保有しているものを含む）の利用・公開を許諾する。
（３）本業務の成果品に、第三者が権利を有する著作物及び知的財産（以下「既存著作物等」という。）が含まれる場合は、乙は当該既存著作物等の使用に必要な費用負担及び使用許諾契約等に関わる一切の手続きを行い、その費用は委託料に含めるものとする。
（４）著作権等に関する紛争が生じた時は、一切を乙の責任において処理するものとし、その費用は委託料に含めるものとする。
（５）成果品の提出後に不備のある点が発見された場合は、契約終了後であっても、乙はこれについて修正の義務を負うものとする。
（６）乙は、本業務の処理上知り得た情報（個人情報を含む）を、他に漏らしてはならない。なお、契約終了後であっても同様とする。
（７）乙は、個人情報の取扱いについて、別記１「個人情報取扱特記事項」を遵守すること。
（８）乙は、この契約による事務を処理するためのデータの取扱いについては、別記２「データ保護及び管理に関する特記仕様書」を遵守すること。

別記１

個人情報等取扱特記事項

第１　基本的事項

乙は、個人情報等の保護の重要性を認識し、この契約による事務の実施に当たっては、個人の権利利益を侵害することのないよう、個人情報等の取扱いを適正に行う。

第２　事務従事者への周知及び監督

（事務従事者への監督）

１　乙は、この契約による事務を行うために取り扱う個人情報等の適切な管理が図られるよう、事務従事者に対して必要かつ適切な監督を行う。

（事務従事者への周知）

２　乙は、事務従事者に対して、次の事項等の個人情報等の保護に必要な事項を周知させるものとする。

(1) 事務従事者又は事務従事者であった者は、その事務に関して知り得た個人情報等をみだりに他人に知らせてはならないこと

(2) 事務従事者又は事務従事者であった者は、その事務に関して知り得た個人情報等を不当な目的に使用してはならないこと

第３　個人情報等の取扱い

（収集の制限）

１　乙は、この契約による事務を行うために個人情報等を収集するときは、当該事務の目的を達成するために必要な範囲内で、適法かつ公正な手段によりこれを行う。

（秘密の保持）

２　乙は、この契約による事務に関して知り得た個人情報等をみだりに他人に知らせてはならない。この契約が終了し、又は解除された後においても、同様とする。

（漏えい、滅失及びき損の防止等）

３　乙は、この契約による事務に関して知り得た個人情報等について、個人情報等の漏えい、滅失及びき損の防止その他の個人情報等の適切な管理のために必要な措置を講じる。

（持ち出しの制限）

４　乙は、甲が承諾した場合を除き、この契約による事務を甲が指定した場所で行い、個人情報等が記録された機器、記録媒体、書類等（以下「機器等」という。）を当該場所以外に持ち出してはならない。

（目的外利用及び提供の制限）

５　乙は、甲の指示がある場合を除き、個人情報等をこの契約の目的以外の目的のために利用し、又は甲の承諾なしに第三者に対して提供してはならない。

（複写又は複製の制限）

６　乙は、この契約による事務を処理するために甲から引き渡された個人情報等が記録された機器等を甲の承諾なしに複写又は複製してはならない。

第４　再委託の制限

乙は、甲が承諾した場合を除き、この契約による事務については自ら行い、第三者にその取扱いを委託してはならない。

第５　事故発生時における報告

乙は、この契約に違反する事態が生じ、又は生じるおそれのあることを知ったときは、速やかに甲に報告し、甲の指示に従うものとする。

第６　情報システムを使用した処理

乙は、情報システムを使用してこの契約による事務を行う場合には、この特記事項のほか、最高情報セキュリティ責任者（総務部デジタル改革推進局デジタル推進課が所管する千葉県情報セキュリティ対策基準（平成１４年３月１５日制定）５（１）アに規定する職にある者をいう。）の定める「データ保護及び管理に関する特記仕様書」等を遵守する。

第７　機器等の返還等

乙は、この契約による事務を処理するために、甲から提供を受け、又は乙自らが収集し、若しくは作成した個人情報等が記録された機器等は、この契約完了後直ちに甲に返還し、又は引き渡すものとする。ただし、甲が別に作業の方法を指示したときは、当該方法によるものとする。

第８　甲の調査、指示等

（調査、指示等）

１　甲は、乙がこの契約により行う個人情報等の取扱状況を随時調査し、又は監査することができる。この場合において、甲は、乙に対して、必要な指示を行い、又は必要な事項の報告若しくは資料の提出等を求めることができる。

（公表）

２　甲は、乙がこの契約により行う事務について、情報漏えい等の個人情報等を保護する上で問題となる事案が発生した場合には、個人情報等の取扱いの

態様、損害の発生状況等を勘案し、乙の名称等の必要な事項を公表することができる。

第９　契約の解除及び損害の賠償

甲は、次の各号のいずれかに該当するときは、この契約を解除し、及び乙に対して損害の賠償を請求することができる。

(1) 乙又は乙の委託先(順次委託が行われた場合におけるそれぞれの受託者を含む。)の責めに帰すべき事由による情報漏えい等があったとき

(2) 乙がこの特記事項に違反し、この契約による事務の目的を達成することができないと認められるとき

別記2　データ保護及び管理に関する特記仕様書

第１ 目的

本契約において取り扱う各種データについて、適正なデータ保護・管理方策及び情報システムのセキュリティ方策ついて明確にすることを目的とする。

第２ 適用範囲

本契約を履行するに当たり、出版、報道等により公にされている情報を除き、千葉県（以下「発注者」という。）が交付若しくは使用を許可し、又は契約の相手方（以下「受注者」という。）が作成若しくは出力したものであって用紙に出力されたものを含む全ての情報（以下「電子データ等」という。）を対象とする。

第３ 対象とする脅威

本書において対象とする脅威は、次に掲げる情報セキュリティが侵害された又はそのおそれがある場合とする。

（１）不正プログラムへの感染（受注者におけるものを含む。）

（２）サービス不能攻撃によるシステムの停止（受注者におけるものを含む。）

（３）情報システムへの不正アクセス（受注者におけるものを含む。）

（４）書面又は外部記録媒体の盗難又は紛失（受注者におけるものを含む。）

（５）機密情報の漏えい・改ざん（受注者におけるものを含む。）

（６）異常処理等、予期せぬ長時間のシステム停止（受注者におけるものを含む。）

（７）発注者が受注者に提供した又は受注者にアクセスを認めた発注者の電子データ等の目的外利用又は漏えい

（８）アクセスを許可していない発注者の電子データ等への受注者によるアクセス

（９）意図しない不正な変更等（受注者におけるものを含む。）

第４ 本契約を履行する者が遵守すべき事項

受注者は、本契約の履行に関して、以下の項目を遵守すること。

４．１ 業務開始前の遵守事項

受注者は、以下の（1）から（6）までの各項目に定める事項及び契約内容を一部再委託する場合は（7）に定める事項を取りまとめた「データ管理計画書」を作成し、業務開始前までに発注者の承認を得ること。

なお、行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）による個人番号及び特定個人情報（以下「特定個人情報等」という。）を取扱う業務の場合は、他の電子データ等と明確に区分して管理することとし、特定個人情報の適正な取扱いに関するガイドラインに基づく安全管理措置について、「データ管理計画書」の各事項へ、追加で記載すること。

（1）データ取扱者等の指定

受注者は、電子データ等を取り扱う者（以下「データ取扱者」という。）及び、データ取扱者を統括する者（以下「データ取扱責任者」という。）を指定し、その所属、役職及び氏名等を記入した「データ取扱者等名簿」を作成すること。

また、特定個人情報等を扱う業務の場合は、特定個人情報等を明確に管理するため、特定個人情報等を取り扱う者（以下「特定個人情報ファイル取扱者」という。）及び特定個人情報ファイル取扱者を統括する者（以下「特定個人情報ファイル取扱責任者」という。）についても併せて指定し、「データ取扱者等名簿」に記載すること。

なお、データ取扱者、データ取扱責任者、特定個人情報ファイル取扱者及び特定個人情報ファイル取扱責任者（以下「データ取扱者等」という。）は、守秘義務等のデータの取扱いに関する社内教育、又はこれに準ずる講習等を受講した者とし、その受講実績も併せて「データ取扱者等名簿」に記入すること。

（2）データ取扱者等への教育・周知計画

受注者は、データ取扱者等を対象とした、本契約での電子データ等の取扱いや漏えい防止等の教育及び周知に関する「データ取扱者等への教育・周知計画」を作成すること。

（３）電子データ等の取扱いにおける情報セキュリティ確保の措置計画

受注者は、本契約に係る電子データ等の取扱いに関し、電子データ等の保存、運搬、複製及び破棄並びに電子データ等の保管場所を変更する場合において実施する措置を記載した「データ取扱計画」を作成すること。「データ取扱計画」には、以下に示す措置を含めること。

（ア）本契約の作業に係る電子データ等を取り扱うサーバ、パソコン、モバイル端末について、アクセス制御及び脅威に関する最新の情報を踏まえた不正プログラム対策及び脆弱性対策を行うこと。

（イ）機密性２以上の電子データ等の取扱いは、発注者又は受注者のいずれかの管理下にない情報システム等（データ取扱者等の個人所有物であるパソコン及びモバイル端末を含む。）を用いることを原則として禁止し、必要がある場合は発注者の許可を得て用いること。

（ウ）電子データ等名称、データ取扱者名、授受方法、使用目的、使用場所、保管場所、保管方法、返却方法、授受日時、返却日時、特定個人情報等の有無等を記録する「データ管理簿」を整備すること。

（エ）機密性２以上の電子データ等の保存に、発注者又は受注者のいずれかの管理下にない情報システム等又は電磁的記録媒体（データ取扱者等が私的に契約しているサービス及びデータ取扱者等の個人所有物である電磁的記録媒体を含む。）を用いることを原則として禁止し、必要がある場合は発注者の許可を得て用いること。

（オ）データ取扱責任者又は特定個人情報ファイル取扱責任者が、データ取扱者又は特定個人情報ファイル取扱者の作業に立ち会うなど適切な管理を行うこと。

（カ）データ取扱責任者又は特定個人情報ファイル取扱責任者が、データ取扱者又は特定個人情報ファイル取扱者が作業を終了し作業場所を離れる際は、データの持ち出しの有無を厳重に検査すること。

（キ）機密性２以上の電子データ等を電子メールにて送信する場合には、暗号化を行うこと。

（４）外部設置における情報セキュリティ確保の措置計画

受注者は、発注者が指定する場所以外に情報システム機器を設置（外部設置）し、本契約に係る電子データ等を取扱う場合は、情報セキュリティ確保のために、部外者

の侵入等の意図的な情報漏えい等を防止する措置を記載した「外部設置における情報セキュリティ措置計画」を作成すること。「外部設置における情報セキュリティ措置計画」には以下に示す措置を含めること。

（ア）情報システムにアクセス（一般向けに提供されているウェブページへのアクセスを除く。）する作業は、受注者の管理下にあり、部外者の立入りが制限された場所において行うこと。

（イ）電子データ等を取り扱うパソコン、モバイル端末等について、盗難、紛失、表示画面ののぞき見等による漏えいを防ぐための措置を講ずること。また、それらの措置を講じていないパソコン、モバイル端末等を用いた作業を制限すること。

（ウ）入退室記録、作業記録等を蓄積し、不正の検知、原因特定に有効な管理機能を備えること。

（５）外部接続における情報セキュリティ確保の措置計画

受注者は、発注者が指定するネットワーク以外のネットワークへ接続（以下「外部接続」という。）し、本契約に係る電子データ等を取扱う場合は、情報セキュリティ確保のために、外部のネットワークからの侵入や改ざんを防御する措置を記載した「外部接続におけるセキュリティ措置計画」を作成すること。「外部接続におけるセキュリティ措置計画」には、以下に示す措置を含めること。

（ア）外部接続箇所にファイアウォールを設置し、不要な通信の遮断を行うこと。

（イ）外部接続箇所に侵入検知システムを設置し、ネットワークへの不正侵入の遮断を行うこと。

（ウ）外部接続箇所で不正な通信を検出した場合、発注者へ通報を行うこと。

（６）情報セキュリティが侵害された又はそのおそれがある場合における対処手順

受注者は、本契約に係る業務の遂行において情報セキュリティが侵害された又はそのおそれがある場合に備え、事前に連絡体制を整備し、発生した場合の対処手順を記載した「情報セキュリティ侵害時対処手順」を作成すること。「情報セキュリティ侵害時対処手順」には、以下に示す対処を含めること。

（ア）作業中に、情報セキュリティが侵害された又はそのおそれがあると判断した場合には、直ちに、発注者に、口頭にてその旨第一報を入れること。発注者への第一報は、

情報セキュリティインシデントの発生を認知してから１時間以内に行うこと。

（イ）当該第一報が行われた後、発生した日時、場所、発生した事由、関係するデータ取扱者等を明らかにし、平日の午前９時から午後５時の間は１時間以内に、それ以外の時間帯は３時間以内に発注者に報告すること。また、当該報告の内容を記載した書面を遅延なく発注者に提出すること。

（ウ）発注者の指示に基づき、対応措置を実施すること。

（エ）発注者が指定する期日までに、発生した事態の具体的内容、原因、実施した対応措置を内容とする報告書を作成の上、発注者に提出すること。

（オ）再発を防止するための措置内容を策定し、発注者の承認を得た後、速やかにその措置を実施すること。

（７）再委託における情報セキュリティの確保の措置計画

受注者は、本契約内容について一部再委託（更に順次行われる再委託を含む。）する場合、受注者が業務を実施する場合に求められる水準と同一水準の情報セキュリティ対策を再委託先において確保させる必要があり、再委託先における情報セキュリティの十分な確保を受注者が担保するとともに、再委託先の情報セキュリティ対策の実施状況を確認するため、「再委託における情報セキュリティ措置計画」を作成すること。なお、特定個人情報等を取扱う業務を再委託したときは、発注者が行う再委託先の管理状況等の確認について、受注者は必要な協力を行うこと。

４．２ 業務実施中における遵守事項

（１）「データ管理計画書」に基づく情報セキュリティ確保

「データ管理計画書」に記載した、データ取扱者等への教育・周知、電子データ等の取扱い及び作業場所等の情報セキュリティ確保のための措置を実施すること。

（２）データ管理簿への記録

受注者は、データ取扱者等が電子データ等を取り扱う場合、「データ管理簿」に記録し、データ取扱責任者に確認させること。また、特定個人情報等を扱う業務の場合、特定個人情報ファイル取扱責任者に併せて確認させること。

（３）「データ管理計画書」の変更

（ア）受注者は、本契約に基づく請負作業中に、次の事項について作業開始前に提出した「データ管理計画書」の内容と異なる措置を実施する場合は、事前に「データ管理計画書」の変更について発注者に提出し、承認を得ること。また、承認された変更の内容を記録し保存すること。

・データ取扱者等の異動を行う場合

・データ取扱者等に対する教育・周知の計画を変更する場合

・電子データ等の取扱いに関する計画又は作業場所等の情報セキュリティ確保のための措置を変更する場合

・再委託先及び再委託先の情報セキュリティ対策を変更する場合

（イ）一時的に「データ管理計画書」とは異なる措置を実施する場合は、原則として事前にその旨を発注者へ提出し、承認を得ること。ただし、情報セキュリティが侵害された又はそのおそれがある場合など緊急を要する場合等の場合、受注者は、実施内容について事後速やかに発注者へ報告すること。

（４）業務の報告・監査等

（ア）受注者は、発注者へ業務実施中の「データ管理計画書」の遵守状況について定期的に報告すること。

（イ）受注者は、発注者が「データ管理計画書」に係る管理状況について監査を要請した時は、定期・不定期にかかわらず、これを受け入れること。

（ウ）受注者は、「データ管理計画書」の評価、見直しを行うとともに、必要な改善策等について、発注者へ提案すること。

（５）情報セキュリティ対策の履行が不十分であった場合の対応

受注者の本契約に係る作業における情報セキュリティ対策の履行が不十分であると発注者が判断した場合、受注者は発注者と協議の上、必要な是正措置を講ずること。また、是正措置の内容を「データ管理計画書」に反映させること。

４．３ 業務完了時の遵守事項

（１）データ返却等処理

受注者は、本契約に基づく業務が完了したときは、「データ管理簿」に記録されている全てのデータについて、返却、消去、廃棄等の措置を行うものとし、処理の方法、日時、場所、立会者、作業責任者等の事項を記した、「データ返却等計画書」を事前に発注者へ提出し、承認を得た上で処理を実施すること。

また、特定個人情報等を扱う業務の場合は、特定個人情報等であることを「データ返却等計画書」に明示すること。

（２）作業後の報告

受注者は、「データ返却等計画書」に基づく処理が終了したときは、その結果を記載した「データ管理簿」を発注者へ提出すること。

（３）情報セキュリティ侵害の被害に関する記録類の引渡し

受注者は、本契約の業務遂行中に情報セキュリティが侵害された又はそのおそれがある事象が発生した場合、４．１（６）に基づいて取得し保存している記録類を発注者に引き渡すこと。

４．４ 記憶装置の修理及び廃棄等におけるデータ消去

受注者は、契約により発注者が利用する情報システム機器の修理及び廃棄、リース返却（以下、「廃棄等」という。）の場合、記憶装置から、全ての電子データ等を消去の上、復元不可能な状態にする措置（以下、「抹消措置」という。）を実施すること。

（１）抹消措置計画の作成

受注者は、「データ管理計画書」へ作業予定日時、作業予定場所、実施予定者氏名、データ完全消去区分、使用機材名・数量、データ消去対象記憶装置リスト、立会者などを記載した「抹消措置作業計画」を追加するとともに、必要に応じてその他の措置内容を変更したうえ、抹消措置実施日（賃貸借契約の場合は賃貸借期間満了日）の３０日前までに発注者に提出し、承認を得ること。

また、賃貸借契約の場合は賃貸借期間満了日から３０日以内に抹消措置実施日を設

定すること。

（２）抹消措置実施方法

ア マイナンバー利用事務系の領域において住民情報を保存する記憶媒体の抹消措置の方法

（ア）当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすること。なお、対象となる機器について、リース契約による場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行うこと。

（イ）職員が抹消措置の完了まで立ち会いによる確認を行う。ただし、庁舎外で抹消措置を行う場合は、庁舎内において、一般的に入手可能な復元ツールの利用によっても情報の復元が困難な状態までデータの消去を行い、職員が作業完了を確認した上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の証拠写真が添付された完了証明書により確認できること。

イ 機密性２以上に該当する情報を保存する記憶媒体（上記アに該当するものを除く。）の抹消措置の方法

（ア）一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うこと。

（イ）庁舎内において、一般的に入手可能な復元ツールの利用によっても情報の復元が困難な状態までデータの消去を行い、職員が作業完了を確認した上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認できること。

ウ 機密性１に該当する情報を保存する記憶媒体の抹消措置の方法

（ア）一般的に入手可能な復元ツールの利用によっても情報の復元が困難な状態に消去すること。

（イ）庁舎内においてデータの消去を実施し、職員が作業完了を確認するなど適正な方法により確認できること。

エ ＩｏＴ機器を含む特殊用途機器の抹消措置の方法

（ア）デジタル複合機などのＩｏＴ機器を含む特殊用途機器に保存された電子データ等の漏えいの対策について、国際標準に基づくセキュリティ要件と同等以上のセキュリティ要件とその要件に適合した第三者認証（「ＩＴ製品の調達におけるセキュリティ

要件リスト」適合製品など）を取得している機能を有する場合は、当該機能によるデータ消去をもって抹消措置とすることができる。

（イ）庁舎内においてデータの消去を実施し、職員が作業完了を確認するなど適正な方法により確認できること。

（３）抹消措置の報告

受注者は、抹消措置実施日から３０日以内に、作業日時、実施者氏名、データ完全消去区分、使用機材名・数量、データ消去対象記憶装置リスト、立会者及び全ての記憶装置について抹消措置前後の写真を添付した「抹消措置完了報告書」を発注者へ提出し、承認を得ること。

第５ 情報システムの情報セキュリティ要件

受注者は、本契約により情報システムを導入する場合は、対象となる以下の項目を遵守すること。

５．１ 侵害対策

（１）通信回線対策

（ア）通信経路の分離

不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離するとともに、業務目的、所属部局等の情報の管理体制に応じて内部のネットワークを通信回線上で分離すること。

（イ）不正通信の遮断

通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。

（ウ）通信のなりすまし防止

情報システムのなりすましを防止するために、サーバの正当性を確認できる機能を備えるとともに、許可されていない端末、サーバ装置、通信回線装置等の接続を防止する機能を備えること。

（エ）サービス不能化の防止

サービスの継続性を確保するため、情報システムの負荷がしきい値を超えた場合に、通信遮断や処理量の抑制等によってサービス停止の脅威を軽減する機能を備えること。

（２）不正プログラム対策

（ア）不正プログラムの感染防止

不正プログラム（ウイルス、ワーム、ボット等）による脅威に備えるため、想定される不正プログラムの感染経路の全てにおいて感染を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。

（イ）不正プログラム対策の管理

システム全体として不正プログラムの感染防止機能を確実に動作させるため、当該

機能の動作状況及び更新状況を一元管理する機能を備えること。

（３）脆弱性対策

（ア）構築時の脆弱性対策

情報システムを構成するソフトウェア及びハードウェアの脆弱性を悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。

（イ）運用時の脆弱性対策

運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を効率的に実施する機能を備えるとともに、情報システム全体の更新漏れを防止する機能を備えること。

５．２ 不正監視・追跡

（１）ログ管理

（ア）ログの蓄積・管理

情報システムに対する不正行為の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関するログを蓄積し、発注者が指定する期間保管するとともに、不正の検知、原因特定に有効な管理機能（ログの検索機能、ログの蓄積不能時の対処機能等）を備えること。

（イ）ログの保護

ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能及び消去や改ざんの事実を検出する機能を備えるとともに、ログのアーカイブデータの保護（消失及び破壊や改ざんの脅威の軽減）のための措置を含む設計とすること。

（ウ）時刻の正確性確保

情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。

（２）不正監視

（ア）侵入検知

不正行為に迅速に対処するため、情報システムで送受信される通信内容の監視及びサーバ装置のセキュリティ状態の監視等によって、不正アクセスや不正侵入を検知及び通知する機能を備えること。

（イ）サービス不能化の検知

サービスの継続性を確保するため、大量のアクセスや機器の異常による、サーバ装置、通信回線装置又は通信回線の過負荷状態を検知する機能を備えること。

５．３ アクセス・利用制限

（１）主体認証

情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体の認証を行う機能として、ＩＤ／パスワードの方式を採用し、主体認証情報の推測や盗難等のリスクの軽減を行う機能として、パスワードの複雑性及び指定回数以上の認証失敗時のアクセス拒否などの条件を満たすこと。

（２）アカウント管理

（ア）ライフサイクル管理

主体のアクセス権を適切に管理するため、主体が用いるアカウント（識別コード、主体認証情報、権限等）を管理（登録、更新、停止、削除等）するための機能を備えること。

（イ）アクセス権管理

情報システムの利用範囲を利用者の職務に応じて制限するため、情報システムのアクセス権を職務に応じて制御する機能を備えるとともに、アクセス権の割り当てを適切に設計すること。

（ウ）管理者権限の保護

特権を有する管理者による不正を防止するため、管理者権限を制御する機能を備えること。

５．４ 機密性・完全性の確保

（１）通信経路上の盗聴防止

通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信内容を暗号化する機能を備えること。

（２）保存情報の機密性確保

情報システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。また、保護すべき情報を利用者が直接アクセス可能な機器に保存できないようにすることに加えて、保存された情報を暗号化する機能を備えること。

（３）保存情報の完全性確保

情報の改ざんや意図しない消去等のリスクを軽減するため、情報の改ざんを検知する機能又は改ざんされていないことを証明する機能を備えること。

５．５ 情報窃取・侵入対策

（１）情報の物理的保護

情報の漏えいを防止するため、記憶装置のパスワードロック、暗号化等によって、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。

（２）侵入の物理的対策

物理的な手段によるセキュリティ侵害に対抗するため、情報システムの構成装置（重要情報を扱う装置）については、外部からの侵入対策が講じられた場所に設置すること。

５．６ 障害対策（事業継続対応）

（１）システムの構成管理

情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成（ハード

ウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに文書どおりの構成とし、加えて情報システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。

（２）システムの可用性確保

サービスの継続性を確保するため、情報システムの各業務の異常停止時間が復旧目標時間として１日を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。

５．７ サプライチェーン・リスク対策

（１）受注者（再委託先含む）において不正プログラム等が組み込まれることへの対策

情報システムの構築において、発注者が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。当該品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。

（２）調達する機器等に不正プログラム等が組み込まれることへの対策

機器等の製造工程において、発注者が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。

５．８ 利用者保護

（１）情報セキュリティ水準低下の防止

情報システムの利用者の情報セキュリティ水準を低下させないように配慮した上でアプリケーションプログラムやウェブコンテンツ等を提供すること。

（２）プライバシー保護

情報システムにアクセスする利用者のアクセス履歴、入力情報等を当該利用者が意図しない形で第三者に送信されないようにすること。