資料１－２

令和７年度から令和 11 年度原子力規制委員会ホームページシステム更改に係る構築及び運用・保守業務の民間競争入札実施要項（案）

令和７年１月

原子力規制委員会　原子力規制庁

目次

１．趣旨

競争の導入による公共サービスの改革に関する法律（平成 18 年法律第 51 号。以下「法」という。）に基づく競争の導入による公共サービスの改革については、公共サービスによる利益を享受する国民の立場に立って、公共サービスの全般について不断の見直しを行い、その実施について、透明かつ公正な競争の下で民間事業者の創意と工夫を適切に反映させることにより、国民のため、より良質かつ低廉な公共サービスを実現することを目指すものである。

上記を踏まえ、原子力規制委員会原子力規制庁（以下「当庁」という。）は「公共サービス改革基本方針」（令和３年７月９日閣議決定）別表において民間競争入札の対象として選定された「令和７年度から令和 11 年度原子力規制委員会ホームページシステム更改に係る構築及び運用・保守業務」（以下「本業務」）について、公共サービス改革基本方針に従って、民間競争入札実施要項を定めるものとする。

２．本業務の詳細な内容及びその実施に当たり確保されるべき質に関する事項

2-1 本業務の概要

（１）業務の経緯

当庁は、国民の生命、健康及び財産の保護、環境の保全並びに我が国の安全保障に資するため、原子力利用における安全の確保を図ること（原子力に係る製錬、加工、貯蔵、再処理及び廃棄の事業並びに原子炉に関する規制に関することを含む。）を任務とする組織である。

原子力規制委員会ホームページでは規制に関わる情報を公開しており、令和2年度実施のリニューアルにおいてコンテンツマネジメントシステム（CMS）を導入し、スマートフォンを含めた多様な利用環境への対応、探しやすいホームページとしての情報整理を実施し、運用・保守を委託することにより安定した運用を実現してきたが、情報量及びコンテンツの増加等によりページ構成が複雑化しており、利用者が必要な情報を見つけられない、専門的な内容のページが多く、利用者層が限定されている等、ユーザビリティやアクセシビリティに課題が生じている。

この度のシステム更改では、現在のオンプレミスでのCMS運用からセキュリティと災害対策の強化、運用コストの削減などを目的としたガバメントクラウドへの移行を検討している。なお、セキュリティ対策については、内閣サイバーセキュリティセンターが定める要件を達成すること。また、委員会・会合等の意思決定に関わる重要な情報をアーカイブしたうえで、検索性の向上等を目的に令和５年度に更改された、公開情報管理システム（N-ADRES）等との連携を強化し、更なる情報公開の改善を予定している。（具体的な連携方法については、要件定義書「3-4. 外部インターフェースに関する事項」を参照）課題としているユーザビリティの改善に係っては、トップページ構成の見直しを行い、N-ADRESの掲載項目と重複している箇所の削除、掲載情報の削減をすることでページ構成を簡素化し、閲

覧性・利便性の向上を図る予定である。また緊急時トップページについても、正確な情報を従前より素早く利用者に届けられるよう、改修を検討する予定である。

（2）業務の内容

(a) 設計・構築業務

(ア) 設計・構築前

要件定義書「5-2. 設計・構築に関する事項（１）設計・構築前」に記載された内容に従い、設計・構築前の業務を実施すること。

(イ) 設計・構築時

要件定義書「5-2. 設計・構築に関する事項（２）設計・構築時」に記載された内容に従い、設計・構築時の業務を実施すること。

(ウ) テスト

要件定義書「5-3. テストに関する事項」に記載された内容に従い、テストの業務を実施すること。

(エ) 受入テスト支援

要件定義書「5-3. テストに関する事項（２）テストの種類毎の要件」に記載された内容に従い、受入テスト支援の業務を実施すること。

(オ) システムの移行

要件定義書「5-4. 移行に関する事項」に記載された内容に従い、移行の業務を実施すること。

(カ) 教育

要件定義書「5-5. 教育に関する事項」に記載された内容に従い、教育の業務を実施すること。

(キ) 引継ぎ

要件定義書「5-6. 運用に関する事項（７）引継ぎ」及び「5-7 保守に関する事項（５）引継ぎ」に記載された内容に従い、引継ぎの業務を実施すること。

(ク) 定例会等の実施

定例会等の実施に係る基本的な要件を以下に示す。

- 請負事業者は、定例会を隔週開催するとともに、業務の進捗状況を作業実施要領に基づき報告すること。
- 請負事業者は、当庁から要請があった場合、又は、請負事業者が必要と判断した場合、必要資料を作成の上、定例会とは別に会議を開催すること。

- 請負事業者は、会議終了後、３日以内（行政機関の休日（行政機関の休日に関する法律（昭和63年法律第91号）第１条第１項各号に掲げる日をいう。）を除く。）に議事録を作成し、当庁の承認を受けること。

(b) 運用・保守業務

(ア) 運用・保守

要件定義書「5-6. 運用に関する事項」及び「5-7. 保守に関する事項」に記載された内容に従い、運用及び保守の業務を実施すること。

(イ) 中長期運用・保守作業計画の確定支援

運用設計及び保守設計に基づき、計画的に発生する作業内容、その想定される時期等を取りまとめ、当庁担当官の確認を受けたうえで、中長期運用・保守計画の策定を支援すること。

(ウ) 運用・保守計画及び運用・保守実施要領の策定

- 運用設計及び保守設計に基づき、定常時における月次の作業内容、その想定スケジュール、障害発生時における作業内容等を取りまとめ、当庁担当官の確認を受けたうえで、運用計画及び保守計画を策定すること。
- 上項の実施にあたっては、情報システム全体のセキュリティ水準が低下することのないようセキュリティ要件を適切に策定し、情報セキュリティに関する各種機能（アクセス制御、識別コード、主体認証情報の付与、定期的な脆弱性情報の把握と対策、標的型攻撃対策及びログの取得、管理等）が有効に機能するようにすること。また、附属文書として、監視項目、定期保守項目、運用・保守業務フローなどの作業項目、作業内容、スケジュール、担当者等について記載すること。
- 運用計画及び保守計画の策定において、セキュリティインシデントを含む障害の発生に備え、導入機器やソフトウェア等に対して必要な対策及び対策の実施に伴う業務への影響を取りまとめ、当庁担当官の確認を受けること。
- その他に当庁担当官からの求めに応じ、運用・保守計画及び運用・保守実施要領を更新すること。

(c) プロジェクト管理に係る業務

(ア) 統合管理

- 定例会を隔週開催するとともに、業務の進捗状況を作業実施要領に基づき報告すること。
- 当庁から要請があった場合、又は、請負事業者が必要と判断

した場合、必要資料を作成の上、定例会とは別に会議を開催すること。

- 要件のトレース管理等を活用し、変更管理を適切に実施すること。

(イ) スコープ管理

- 本業務の実施範囲及び成果物を明確化するとともに、作業項目、作業内容をより階層化し、担当者等を記載した WBS を作成すること（業務計画書の付属文書）。
- なお、その際、当庁担当官との認識の共有を図ること。
- 要件定義書、調達仕様書及びプロジェクトの目的、目標、実施計画等を明確に記載したプロジェクト計画書（当庁作成資料）の各要件に対して、実現箇所、実現方法等を追跡・管理するために、要件をトレース管理する仕組みを導入すること。
- 本業務の実施段階においても、当庁担当官と調整して作業及び成果物の妥当性を確認しつつ進めること。

(ウ) スケジュール管理

- 当庁担当官の指示に基づき、工程管理等支援業務請負者と調整の上、本業務の業務計画書の案を作成し、当庁担当官の承認を受けること。その際、スケジュール内に完了するために適切なマイルストーン（チェックポイント）を定め、マイルストーンから逆算した各タスクの期間設定及び完了条件を定めておくこと。
- マイルストーンの記載にあたっては、情報資産管理標準シートの提出時期を示すこと。

(エ) 品質管理

- システムの構築を効率的に実施するため、構築やテスト等の標準（例：何をインプット（設計書等）として作業を行い、インプット情報に示された事項を確実に実装しテストしたことを記録するルールやシステムの構成要素毎の重要度に応じたテストの網羅性と密度の設定ルール、さらにはテストの中に占めるセキュリティテストの網羅性と密度等の設定ルール等、設計されたものが確実に実装され適切な品質を保つことを可能とする構築に係る標準）を定め当庁担当官の確認を受けること。
- なお、本標準は、業務ごと（構築標準等）に分けて策定しても良い。

(オ) コミュニケーション管理

- 会議の特性、参加者の勤務場所等を踏まえ、会議の適切な態様（対面、オンライン等）を検討した上で実施すること。

- 会議終了後、３日以内（行政機関の休日（行政機関の休日に関する法律（昭和63年法律第91号）第１条第１項各号に掲げる日をいう。）を除く。）に議事録を作成し、当庁担当官の承認を受けること。

(カ) リスク管理

- リスクの特定にあたっては、請負事業者の内部のリスクについても積極的に洗い出すものとする。なお、リスク登録簿の様式については、プロジェクトマネジメント協会日本支部が公開しているリスク登録簿を参照すること。
- リスク対応の計画においては、事前の対応戦略だけでなく、リスク発生後のコンティンジェンシー対応戦略についても計画すること。その際、対応戦略実行のトリガー条件について決定しておくこと。特にスケジュールが遅延した場合に備え、常にコンティンジェンシー対応戦略を計画すること。
- リスク登録簿の提出は、業務計画書と同時とする。その後、リスク登録簿を随時更新すること。

(キ) その他

- 当庁及び当庁が指示する機関等が実施する工程レビュー等の実施に先立ち、当庁からの指示のもと、必要な情報の提供や資料の作成等の支援を行うこと。

(d) 契約金額内訳及び情報資産管理標準シートの提出

(ア) デジタル・ガバメント推進標準ガイドライン（以下「標準ガイドライン」という。）の別紙２「情報システムの経費区分」に基づき区分等した契約金額の内訳を記載した情報資産管理標準シートを契約締結後に速やかに提出すること。

(イ) 請負事業者は、情報資産管理標準シート及び標準ガイドラインの別紙３「調達仕様書に盛り込むべき情報資産管理標準シートの提出等に関する作業内容」の「３．その他」のうち、次に掲げる事項について記載したエクセル電子データを提出する時期を「運用実施要領及び保守実施要領」等において定め、提出すること。

- 各データの変更管理
  本システムの保守において、構築規模の管理、ハードウェアの管理、ソフトウェアの管理、回線の管理、外部サービスの管理、施設の管理、公開ドメインの管理、取扱情報の管理、情報セキュリティ要件の管理、指標の管理の各項目についてその内容に変更が生じる作業をしたときは、当該変更を行った項目。
- 作業実績等の管理
  本システムの保守中に取り込まれた作業実績、リスク、課題及び障害事由。

2-2　対象業務の対象

（1）原子力規制委員会ホームページ（https://www.nra.go.jp/　及び https://www2.nra.go.jp/）で提供しているコンテンツ（英語で掲載しているコンテンツを含む。）

原子力規制委員会ホームページの運用状況（令和５年１月時点）
主要ファイル数 HTML 約20,000 ファイル PDF ファイル 約150,000 ファイル
月間ページビュー数 約700,000 ページビュー

（2）当庁が提供する動画コンテンツ（別サーバで運用するものを含む。）

（3）当庁が運営するソーシャル・ネットワーキング・サービス上のコンテンツ

（4）原子力委員会ホームページシステムに使用する以下のサーバ等及びこれらに導入するソフトウェア、ハードウェア

- CMS メインサーバ
- バックアップサーバ
- リカバリーシステム
- 冗長化サーバ

2-3　請負業務の引継ぎ

（1）現行請負事業者からの引継ぎ

当庁は、当該引継ぎが円滑に実施されるよう、現行請負事業者及び本業務の請負事業者に対して必要な措置を講ずるとともに、引継ぎが完了したことを確認する。

本業務を新たに実施することとなった請負事業者は、本業務の開始日までに、業務内容を明らかにした書類等により、現行請負事業者から業務の引継ぎを受けるものとする。なお、その際の事務引継ぎに必要となる現行請負事業者に発生した費用は現行請負事業者の負担、本業務の請負事業者に発生した費用は本業務の請負事業者の負担となる。

（2）請負期間満了の際の引継ぎ

当庁は、当該引継ぎが円滑に実施されるよう、請負事業者及び次回請負事業者に対して必要な措置を講ずるとともに、引継ぎが完了したことを確認する。

本業務の終了に伴い請負事業者が変更となる場合には、本業務を受注した請負事業者は、当該業務の開始日までに、業務内容を明らかにした書類等により、次回請負事業者に対し、引継ぎを行うものとする。

なお、その際の事務引継ぎに必要となる本業務を受注した請負事業者に発生した費用は本業務を受注した請負事業者の負担、次回請負事業者に発生した費用は次回請負事業者の負担となる。

2-4 確保されるべき対象業務の質

（1）業務内容

「2-1（2）業務の内容」に示す業務を適切に実施すること。

（2）原子力規制委員会ホームページシステムの稼働率

稼働率は99.0%以上とし、稼働率は以下の計算式により算出すること。

稼働率（%）＝

{1 ―（1か月の停止時間）÷（1か月の稼働予定時間）} × 100

（※1か月の稼働予定時間は計画停電等を除く。）

（3）原子力規制委員会広報総合評価・分析の結果への対応

年に1回の割合で一般利用者に対して「原子力規制委員会広報総合評価・分析」を行っている。次の項目についてアンケート結果を踏まえ、改善の提案と対応方法を検討すること

- 原子力規制委員会の認知度・印象、ツールの認知度
- 原子力規制委員会の情報発信に関する評価
- 原子力規制委員会に対する期待
- 原子力に関する信頼する情報源＋理由（自由記述）

（4）セキュリティ上の重大障害件数

個人情報、施設等に関する情報その他の契約履行に際し知り得た情報漏えいの件数は0件であること。

（5）本業務のシステム運用上の重大障害件数

長期にわたり正常に稼動できない事態・状況及び保有するデータの喪失等により、業務に多大な支障が生じるような重大障害の件数は0件であること。

（6）目標復旧時間

サービスごとの目標復旧時間は1か月当たり60分程度であること。

2-5 創意工夫の発揮可能性

本業務を実施するに当たっては、以下の観点から請負事業者の創意工夫を反映し、公共サービスの質の向上（包括的な質の向上、効率化の向上、経費の削減等）に努めるものとする。

（1）本業務の実施全般に対する提案

請負事業者は、別途定める様式に従い、本業務の実施全般に係る質の向上の観点から取り組むべき事項等の提案を行うこととする。

（2）事業内容に対する改善提案

請負事業者は、事業内容に対し、改善すべき提案（コスト削減に係る提案を含む。）がある場合は、別途定める様式に従い、具体的な方法等を示すとともに、従来の実施状況と同等以上の質が確保できる根拠等を提案すること。

2-6 契約の形態及び支払

契約の形態は、請負契約とする。

当庁は、請負契約に基づき、請負事業者が実施する本業務について、契約の履行に関し、仕様書に定めた内容に基づく監督・検査を実施するなどして適正に実施されていることを確認した上で、適正な支払請求書を受領した日から30日以内に、毎月、契約金額を支払うものとする。確認の結果、確保されるべき対象業務の質が達成されていないと認められる場合、又は達成でき

ないおそれがある場合、当庁は、確保されるべき対象業務の質の達成に必要な限りで、請負事業者に対して本業務の実施方法の改善を行うよう指示することができる。請負事業者は、当該指示を受けて業務の実施方法を改善し、業務改善報告書を速やかに当庁に提出するものとする。業務改善報告書の内容が、確保されるべき対象業務の質が達成可能なものであると認められるまで、当庁は、請負費の支払を行わないことができる。なお、請負費は、本件業務開始以降のサービス提供に対して支払われるものであり、請負事業者が行う引き継ぎや準備行為等に対して、請負事業者に発生した費用は、請負事業者の負担とする。

2-7 法令変更による増加費用及び損害の負担

法令の変更により事業者に生じた合理的な増加費用及び損害は、アからウまでに該当する場合には当庁が負担し、それ以外の法令変更については請負事業者が負担する。

ア　本業務に類型的又は特別に影響を及ぼす法令変更及び税制度の新設

イ　消費税その他類似の税制度の新設・変更（税率の変更含む。）

ウ　上記ア及びイのほか、法人税その他類似の税制度の新設・変更以外の税制度の新設・変更（税率の変更含む。）

３．実施期間に関する事項

本請負契約の契約期間は、契約締結日から令和１２年３月３１日までとする。なお、開発・構築は令和７年４月から令和８年２月上旬、運用管理は令和８年２月上旬から令和１２年３月３１日までとする。

４．入札参加資格に関する事項

（１）法第15条において準用する法第10条各号（第11号を除く。）に該当する者でないこと。

（２）予算決算及び会計令（以下「予決令」という。）第７０条の規定に該当しない者であること。 なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を 得ている者は、同条中、特別の理由がある場合に該当する。

（３）予決令第７１条の規定に該当しない者であること。

（４）令和０４・０５・０６年度環境省競争参加資格（全省庁統一資格）「役務の提供等」の「A」、「B」、「C」又は「D」の等級に格付けされている者であること。（「役務の提供等」の営業品目「ソフトウェア開発」、「情報処理」又は「その他」に登録している者であること。）なお、令和０７・０８・０９年度競争参加資格を引き続き取得すること。

（５）当庁からの補助金交付等停止措置又は指名停止措置が講じられている者ではないこと。

（６）法人税並びに消費税及び地方消費税の滞納がないこと。

（７）労働保険、厚生年金保険等の適用を受けている場合、保険料等の滞納がないこと。

（８）入札説明書において示す暴力団排除に関する誓約事項に誓約できる者であること。
（９）本調達仕様書に基づく作業を実施する部門又は組織を対象として、ISO27001を基準とした認証を取得していること又は当該認証と同等の要件を有すること。当該認証と同等の要件を有することとする場合には、その根拠（JIS Q 2700認定証、ISMS認定証、管理体制、品質マネジメントシステム運営規程、品質管理手順規定等）を明確に示し、PJMO の理解を得ること。
（１０）　本調達仕様書に基づく作業を実施する部門又は組織を対象として、ISO9001を基準とした認証を取得していること又は当該認証と同等の要件を有すること。当該認証と同等の要件を有することとする場合には、その根拠（JIS Q 9001認定証、管理体制、品質マネジメントシステム運営規程、品質管理手順規定等）を明確に示し、PJMO の理解を得ること。
（１１）　女性の職業生活における活躍の推進に関する法律（平成27年法律第64号、以下「女性活躍推進法」という。）、次世代育成支援対策推進法（平成15年法律第120号、以下「次世代法」という。）、青少年の雇用の促進等に関する法律（昭和45年法律第98号、以下「若者雇用推進法」という。）に基づく認定等（えるぼし認定等、くるみん認定、プラチナくるみん認定、ユースエール認定）を取得している場合は、認定等の名称及び認定通知書等の写しを提出すること。ただし、提案書提出時点において認定等の期間中であること。
（１２）　請負事業者は、公共機関（独立行政法人、地方公共団体を含む官公庁）のシステム及びユーザビリティ、アクセシビリティに配慮したホームページにおける運用の実績を有すること。
（１３）　100名以上の職員が利用する情報システムの運用又は保守作業を行った実績を直近５年以内に有すること。
（１４）　情報システムのクラウド環境への移行に係る設計、開発、運用の実績を過去３年以内に有すること。
（１５）　（なお、後述の入札説明会への出席は必須とせず、説明会に出席していない者も競争への参加は可能とする。）

５．入札に参加する者の募集に関する事項

（1）スケジュール

入札公示：官報公示	令和７年１月上旬
入札説明会	１月中旬
質問受付期限	１月下旬
資料閲覧期限	２月上旬
提案書提出期限	２月中旬
入札参加者によるプレゼンテーション	２月下旬
開札	３月上旬
暴力団排除手続き	３月中旬
契約締結	４月上旬
事業開始	４月下旬頃

（なお、従来の当該業務の調達仕様書、提出書類、各サービスの設計書等につい

ては、民間競争入札に参加する予定の者から要望があった場合、所定の手続を踏まえた上で閲覧可能である。）

（２）入札に関する書類

入札参加者は、次に掲げる書類を別に定める入札説明書に記載された期日及び方法により提出すること。

ア　入札説明後の質問受付

入札公告以降、本実施要項の内容や入札に係る事項について、入札説明会後に、当庁に対して質問を行うことができる。質問は原則として電子メールにより行い、質問内容及び当庁からの回答は原則として入札説明書の交付を受けた全ての者に公開することとする。ただし、民間事業者の権利や競争上の地位等を害するおそれがあると判断される場合には、質問者の意向を聴取した上で公開しないよう配慮する。

イ　提案書等

別添２「総合評価基準書」の提案要求事項に示した各要求項目について具体的な提案（創意工夫を含む。）を行い、各要求項目を満たすことができることを証明する書類を提出すること。

ウ　下見積書

人件費の単価証明書及び物件費の価格証明書を含んだ下見積書

ただし、契約後に発生する経費のみとする。

エ　入札書

入札金額（入札参加者が消費税及び地方消費税に係る課税事業者であるか免税事業者であるかを問わず、契約期間内の全ての請負業務に対する報酬の総額の 110 分の 100 に相当する金額）を記載した書類

オ　委任状

代理人に委任したことを証明する書類

ただし、代理人による入札を行う場合に限る。

カ　競争参加資格審査結果通知書の写し

令和０４・０５・０６年度環境省競争参加資格（全省庁統一資格）「役務の提供等」の「A」、「B」、「C」又は「D」の等級に格付けされた者であること（「役務の提供等」の営業品目「ソフトウェア開発」、「情報処理」又は「その他」に登録している者であること。）を証明する審査結果通知書の写し

ただし、電子入札システムにより入札を行う場合は不要。

キ　理由書

電子入札システムにより入札を行うことができない旨の理由を示した書類

ただし、当庁側の事情で電子入札システムを用いた入札を行わない場合には不要。

ク　法第 15 条において準用する法第 10 条に規定する欠格事由のうち、暴力団排除に関する規定について評価するために必要な書類

ケ　法人税並びに消費税及び地方消費税の納税証明書（直近のもの）

前記の４(7)に該当する場合、社会保険料納入確認書等（直近のもの）

コ　主たる事業概要、従業員数、事業所の所在地、代表者略歴、主要株主構成、他の者との間で競争の導入による公共サービス改革に関する法律施行令（平成 18 年７月５日政令第 228 号）第３条に規定する特定支配関係にある場合は、その者に関する当該情報

サ　入札参加グループによる参加の場合は、入札参加グループ内部の役割分担について定めた協定書又はこれに類する書類

シ　指名停止等に関する申出書
　各府省庁から指名停止を受けていないことを確認する書類

ス　誓約書
　本業務を完了できることを証明する書類

６．本業務を実施する者を決定するための評価の基準その他本業務を実施する者の決定に関する事項

以下に本業務を実施する者の決定に関する事項を示す。なお、詳細は別添２「総合評価基準書」を基本とする。

（１）評価方法

本業務を実施する者の決定は、総合評価落札方式によるものとする。

また、総合評価は、価格点（入札価格の得点）に技術点（評価項目一覧による加点）を加えて得た数値（以下「総合評価点」という。）をもって行う。

価格点と技術点の配分

価格点の配分：技術点の配分　＝　１：３

総合評価点　＝　価格点（400 点満点）＋　技術点（1200 点満点）

（２）決定方法

調達仕様書において必須と定められた要求要件を全て満たしている場合に「合格」とし、「基礎点」を与える。なお、一つでも欠ける場合は「不合格」とする。

（３）総合評価点

ア　価格点は、入札価格を予定価格で除して得た値を１から減じて得た値に入札価格に対する得点配分を乗じて得た値とする。

価格点　＝　（１－入札価格÷予定価格）×　400 点

イ　技術点の評価は以下のとおりとする。

(ｱ) 全ての仕様を満たし、「合格」したものに「基礎点」として 50 点を与える。

(ｲ) 「合格」した提案書について、調達仕様書において必須と定められた要求要件を全て満たしている項目に対し「基礎点」を与えた上で、提案書審査委員会の委員ごとに加点部分の評価を行う。当庁に取って有益な提案があった場合に、「評価項目一覧」の提案要求事項の得点配分に基づき、「加点」を与えるものとして、各委員の採点結果を委員会で確認し、事実誤認等があれば各委員において訂正する。なお、各委員が行う加点部分の評価は、以下の評価基準に基づき点数化する。確定した各委員の採点結果について、その平均値を算出し、「加点」とする。

①評価基準

評価	評価基準	配点

		比率
優	提案内容に具体性や実現性がある、又は要求仕様を上回る追加の提案がなされており、本業務の遂行において特筆すべき有益性が認められる。	100%
良	提案内容が具体性や実現性がある、又は要求仕様を上回る追加の提案がなされており、本業務の遂行において一定の有益性が認められる。	60%
可	提案内容が具体性や実現性がある、又は要求仕様を上回る追加の提案がなされており、本業務の遂行において若干の有益性が認められる。	30%
加点なし	提案内容は調達仕様書や要件定義書で定める要件は満たしているが、具体性や実現性がなく、本業務の遂行に有益性は認められない。	0%

(ｳ) 「基礎点」と「加点」の合計点を「技術点」とする。

技術点 ＝ 基礎点（50 点） ＋ 加点（1150 点）

（4）落札者の決定

ア 調達仕様書に示す全ての要求要件を満たし、入札者の入札価格が予決令第 79 条の規定に基づいて作成された予定価格の制限の範囲内であり、かつ、「総合評価落札方法」によって得られた数値の最も高い者を落札者とする。ただし、予決令第 84 条の規定に該当する場合は、予決令第 85 条の基準を適用するので、基準に該当する入札が行われた場合は入札の結果を保留する。この場合、入札参加者は当庁の行う事情聴取等の調査に協力しなければならない。

イ 調査の結果、会計法（昭和 22 年法律第 35 号）第 29 条の６第１項ただし書きの規定に該当すると認められるときは、その定めるところにより、予定価格の制限の範囲内で次順位の者を落札者とすることがある。

ウ 落札者となるべき者が２者以上あるときは、直ちに当該入札者にくじを引かせ、落札者を決定するものとする。また、入札者又は代理人がくじを引くことができないときは、入札執行事務に関係のない職員がこれに代わってくじを引き、落札者を決定するものとする。

エ 契約担当官等は、落札者を決定したときに入札者にその氏名（法人の場合はその名称）及び金額を口頭で通知する。ただし、上記イにより落札者を決定する場合には別に書面で通知する。また、落札できなかった入札者は、落札の相対的な利点に関する情報（当該入札者と落札者のそれぞれの入札価格及び性能等の得点）の提供を要請することができる。

（5）落札決定の取消し

次の各号のいずれかに該当するときは、落札者の決定を取り消す。ただし、契約担当官等が、正当な理由があると認めたときはこの限りでない。

ア 落札者が、契約担当官等から求められたにもかかわらず契約書の取り交わしを行わない場合

イ 入札書の内訳金額と合計金額が符合しない場合

落札後、入札者に内訳書を記載させる場合がある。内訳金額が合計金額と符

合しないときは、合計金額で入札したものとみなすため、内訳金額の補正を求められた入札者は、直ちに合計金額に基づいてこれを補正しなければならない。

（6）落札者が決定しなかった場合の措置

初回の入札において入札参加者がなかった場合、必須項目を全て満たす入札参加者がなかった場合又は再度の入札を行ってもなお落札者が決定しなかった場合は、原則として、入札条件等を見直した後、再度公告を行う。

なお、再度の入札によっても落札者となるべき者が決定しない場合又は本業務の実施に必要な期間が確保できないなどやむを得ない場合は、自ら実施することなどとし、その理由を官民競争入札等監理委員会（以下「監理委員会」という。）に報告するとともに公表するものとする。

7．本業務に関する従来の実施状況に関する情報の開示に関する事項

（1）開示情報

対象業務に関して、以下の情報は別紙１「従来の実施状況に関する情報の開示」のとおり開示する。

ア 従来の実施に要した経費
イ 従来の実施に要した人員
ウ 従来の実施に要した施設及び設備
エ 従来の実施における目標の達成の程度
オ 従来の実施方法等

（2）資料の閲覧

対象業務に関する情報について、以下の要領により所定の手続を踏まえた上で閲覧可能とする。

（ア） 閲覧可能情報

- 前項オ「従来の実施方法等」の詳細な情報
- プロジェクト計画書、プロジェクト管理要領
- 原子力規制委員会ホームページリニューアル構成の変更点解説表
- CMS 機能要件書
- 原子力規制委員会ホームページシステムの運用体制及びシステム概要

（イ） 閲覧場所

原子力規制委員会原子力規制庁長官官房総務課広報室内、あるいは当庁の指定する場所

（ウ） 閲覧期間及び時間

入札説明会で別途指定する期間（閉庁日（日曜日、土曜日、国民の祝日に関する法律（昭和 23 年法律第 178 号）に規定する休日、12 月 29 日から 1 月 3 日）を除く）の 10 時から 17 時まで。

（エ） 閲覧手続

最大２名まで。応札希望者の商号、連絡先、閲覧希望者氏名を別紙 3「資料閲覧申込書」に記載の上、閲覧希望日の３営業日前までに提出すること。また、閲覧日当日までに別紙４「守秘義務に関する誓約書」

に記載の上、提出すること。

（オ） 閲覧時の注意

閲覧にて知り得た内容については、提案書の作成以外には使用しないこと。また、本調達に関与しない者等に情報が漏えいしないように留意すること。閲覧資料の複写等による閲覧内容の記録は行わないこと。

（カ） 連絡先

原子力規制委員会原子力規制庁長官官房総務課広報室 土屋、神田

電話：03-5114-2105

８．請負事業者に使用させることができる国有財産等に関する事項

（１）国有財産等の使用

請負事業者は、本業務の遂行に必要な施設、設備等として、次に掲げる施設、設備等を適切な管理の下、無償で使用することができる。

ア　業務に必要な電気設備

イ　その他、当庁と協議し承認された業務に必要な施設、設備等

（２）使用制限

ア　請負事業者は、本業務の実施及び実施に付随する業務以外の目的で使用し、又は利用してはならない。

イ　請負事業者は、あらかじめ当庁と協議した上で、当庁の業務に支障を来さない範囲内において、施設内に運用管理業務の実施に必要な設備等を持ち込むことができる。

ウ　請負事業者は、設備等を設置した場合は、設備等の使用を終了又は中止した後、直ちに、必要な原状回復を行う。

エ　請負事業者は、既存の建築物及び工作物等に汚損・損傷等を与えないよう十分に注意し、損傷（機器の故障等を含む。）が生じるおそれのある場合は、養生を行う。万一損傷が生じた場合は、請負事業者の責任と負担において速やかに復旧するものとする。

９．請負事業者が、当庁に対して報告すべき事項、秘密を適正に取り扱うために必要な措置その他の本業務の適正かつ確実な実施の確保のために請負事業者が講ずべき措置に関する事項

（１）請負事業者が当庁に報告すべき事項、当庁の指示により講ずべき措置

ア　報告等

(ｱ) 請負事業者は、仕様書に規定する業務を実施したときは、当該仕様書に基づく各種報告書を当庁に提出しなければならない。

(ｲ) 請負事業者は、本業務を実施したとき、又は完了に影響を及ぼす重要な事項の変更が生じたときは、直ちに当庁に報告するものとし、当庁と請負事業者が協議するものとする。

(ｳ) 請負事業者は、契約期間中において、(ｲ)以外であっても、必要に応じて当庁から報告を求められた場合は、適宜、報告を行うものとする。

イ　調査

(ｱ) 当庁は、本業務の適正かつ確実な実施を確保するために必要があると認めるときは、法第 26 条第１項に基づき、請負事業者に対し必要な報告を求め、又は当庁の職員が事務所に立ち入り、当該業務の実施の状況若しくは記録、帳簿書類その他の物件を検査し、又は関係者に質問することができる。

(ｲ) 立入検査をする当庁の職員は、検査等を行う際には、当該検査が法第 26 条第１項に基づくものであることを請負事業者に明示するとともに、その身分を示す証明書を携帯し、関係者に提示するものとする。

ウ　指示

当庁は、本業務の適正かつ確実な実施を確保するために必要と認めるときは、請負事業者に対し、必要な措置を採るべきことを指示することができる。

（２）秘密を適正に取り扱うために必要な措置

ア　請負事業者は、本業務の実施に際して知り得た当庁の情報等（公知の事実等を除く）を、第三者に漏らし、盗用し、又は受託業務以外の目的のために利用してはならない。これらの者が秘密を漏らし、又は盗用した場合は、法第 54 条により罰則の適用がある。

イ　請負事業者は、本業務の実施に際して得られた情報処理に関する利用技術（アイデア又はノウハウ）については、請負事業者からの文書による申出を当庁が認めた場合に限り、第三者へ開示できるものとする。

ウ　請負事業者は、当庁から提供された個人情報及び業務上知り得た個人情報について、個人情報の保護に関する法律（平成 15 年法律第 57 号）に基づき、適切な管理を行わなくてはならない。また、当該個人情報については、本業務以外の目的のために利用してはならない。

エ　請負事業者は、当庁の情報セキュリティに関する規定等に基づき、個人情報等を取り扱う場合は、①情報の複製等の制限、②情報の漏えい等の事案の発生時における対応、③受託業務終了時の情報の消去・廃棄（復元不可能とすること。）及び返却、④内部管理体制の確立、⑤情報セキュリティの運用状況の検査に応じる義務、⑥請負事業者の事業責任者及び請負業務に従事する者全てに対しての守秘義務及び情報セキュリティ要求事項の遵守に関して、仕様書別紙４「守秘義務に関する誓約書」を契約後速やかに当庁に提出しなければならない。

オ　アからエまでのほか、当庁は、請負事業者に対し、本業務の適正かつ確実な実施に必要な限りで、秘密を適正に取り扱うために必要な措置を採るべきことを指示することができる。

（３）契約に基づき請負事業者が講ずべき措置

ア　受託業務開始

請負事業者は、本業務の開始日から確実に業務を開始すること。

イ　権利の譲渡

請負事業者は、債務の履行を第三者に引き受けさせ、又は契約から生じる一切の権利若しくは義務を第三者に譲渡し、承継せしめ、若しくは担保に供してはならない。なお、再委託については調達仕様書に従うこととし、本項の対象には含まない。

ウ　権利義務の帰属等

(ｱ) 本業務の実施が第三者の特許権、著作権その他の権利と抵触するときは、

請負事業者は、その責任において、必要な措置を講じなくてはならない。

(ｲ) 請負事業者は、本業務の実施状況を公表しようとするときは、あらかじめ、当庁の承認を受けなければならない。

エ　契約不適合責任

(ｱ) 当庁は、請負事業者に対し、引き渡された成果物が種類又は品質に関して契約の内容に適合しないものである場合（その不適合が当庁の指示によって生じた場合を除き、請負事業者が当該指示が不適当であることを知りながら、又は過失により知らずに告げなかった場合を含む。）において、その不適合を当庁が知った時から起算して１年以内にその旨の通知を行ったときは、その成果物に対する修補等による履行の追完を請求することができる。ただし、請負事業者は、当庁に不相当な負担を課するものでないときは、当庁が請求した方法と異なる方法による履行の追完をすることができる。

(ｲ) (ｱ)の場合において、当庁が相当の期間を定めて履行の追完の催告をし、その期間内に履行の追完がないときは、当庁は、その不適合の程度に応じて代金の減額を請求することができる。

(ｳ) (ｱ)又は(ｲ)の場合において、当庁は、損害賠償を請求することができる。

オ　再委託

再委託に関する要件については、「別添１　原子力規制委員会ホームページシステム更改に係る構築及び運用・保守業務　調達仕様書」の「９　再委託に関する事項」を参照すること。

カ　契約内容の変更

当庁及び請負事業者は、本業務の質の確保の推進、又はその他やむを得ない事由により本契約の内容を変更しようとする場合は、あらかじめ変更の理由を提出し、それぞれの相手方の承認を受けるとともに法第 21 条の規定に基づく手続を適切に行わなければならない。

キ　機器更新等の際における民間事業者への措置

当庁は、次のいずれかに該当するときは、請負事業者にその旨を通知するとともに、請負事業者と協議の上、契約を変更することができる。

(ｱ) ハードウェアの更新、撤去又は新設、サポート期限が切れるソフトウェアの更新等に伴い運用管理対象機器の一部に変更が生じるとき

(ｲ) セキュリティ対策の強化等により業務内容に変更が生じるとき

(ｳ) 当庁の組織変更や人員増減に伴うシステム利用者数の変動等により業務量に変動が生じるとき

ク　契約の解除

当庁は、請負事業者が次のいずれかに該当するときは、請負事業者に対し請負費の支払を停止し、又は契約を解除若しくは変更することができる。この場合、請負事業者は当庁に対して、契約金額から消費税及び地方消費税を差し引いた金額の 100 分の 10 に相当する金額を違約金として支払わなければならない。その場合の算定方法については、当庁の定めるところによる。ただし、同額の超過する増加費用及び損害が発生したときは、超過分の請求を妨げるものではない。

また、請負事業者は、当庁との協議に基づき、本業務の処理が完了するまでの間、責任を持って当該処理を行わなければならない。

(ｱ) 法第 22 条第１項イからチまで又は同項第２号に該当するとき。

(ｲ) 暴力団員を、業務を統括する者又は従業員としていることが明らかになった場合。
(ｳ) 暴力団員と社会的に非難されるべき関係を有していることが明らかになった場合。
(ｴ) 再委託先が、暴力団若しくは暴力団員により実質的に経営を支配される事業を行う者又はこれに準ずる者に該当する旨の通知を、警察当局から受けたとき。
(ｵ) 再委託先が暴力団又は暴力団関係者と知りながらそれを容認して再委託契約を継続させているとき。

ケ　談合等不正行為

請負事業者は、談合等の不正行為に関して、当庁が定める「談合等の不正行為に関する特約条項」に従うものとする。

コ　損害賠償

請負事業者は、請負事業者の故意又は過失により当庁に損害を与えたときは、当庁に対し、その損害について賠償する責任を負う。また、当庁は、契約の解除及び違約金の徴収をしてもなお損害賠償の請求をすることができる。なお、当庁から請負事業者に損害賠償を請求する場合において、原因を同じくする支払済の違約金がある場合には、当該違約金は原因を同じくする損害賠償について、支払済額とみなす。

サ　不可抗力免責・危険負担

当庁及び請負事業者の責に帰すことのできない事由により契約期間中に物件が滅失し、又は毀損し、その結果、当庁が物件を使用することができなくなったときは、請負事業者は、当該事由が生じた日の翌日以後の契約期間に係る代金の支払を請求することができない。

シ　金品等の授受の禁止

請負事業者は、本業務の実施において、金品等を受け取ること、又は与えることをしてはならない。

ス　宣伝行為の禁止

請負事業者及び本業務に従事する者は、本業務の実施に当たっては、自ら行う業務の宣伝を行ってはならない。また、本業務の実施をもって、第三者に対し誤解を与えるような行為をしてはならない。

セ　法令の遵守

請負事業者は、本業務を実施するに当たり適用を受ける関係法令等を遵守しなくてはならない。

ソ　安全衛生

請負事業者は、本業務に従事する者の労働安全衛生に関する労務管理については、責任者を定め、関係法令に従って行わなければならない。

タ　記録及び帳簿類の保管

請負事業者は、本業務に関して作成した記録及び帳簿類を、本業務を終了し、又は中止した日の属する年度の翌年度から起算して５年間、保管しなければならない。

チ　契約の解釈

契約に定めのない事項及び契約に関して生じた疑義は、当庁と請負事業者との間で協議して解決する。

10. 請負事業者が本業務を実施するに当たり第三者に損害を加えた場合において、その損害の賠償に関し契約により本業務委託者が負うべき責任に関する事項

本業務を実施するに当たり、請負事業者又はその職員その他の本業務に従事する者が、故意又は過失により、本業務の受益者等の第三者に損害を加えた場合は、次のとおりとする。

（１）当庁が国家賠償法第１条第１項等の規定に基づき当該第三者に対する賠償を行ったときは、当庁は請負事業者に対し、当該第三者に支払った損害賠償額（当該損害の発生について当庁の責めに帰すべき理由が存する場合は、当庁が自ら賠償の責めに任ずべき金額を超える部分に限る。）について求償することができる。

（２）請負事業者が民法（明治29年法律第89号）第709条等の規定に基づき当該第三者に対する賠償を行った場合であって、当該損害の発生について当庁の責めに帰すべき理由が存するときは、請負事業者は当庁に対し、当該第三者に支払った損害賠償額のうち自ら賠償の責めに任ずべき金額を超える部分を求償することができる。

11. 本業務に係る法第７条第８項に規定する評価に関する事項

（１）本業務の実施状況に関する調査の時期

当庁は、本業務の実施状況について、総務大臣が行う評価の時期（令和１０年５月を予定）を踏まえ、本業務開始後、毎年３月に状況を調査する。

（２）調査項目及び実施方法

ア　業務の内容

業務報告書等により調査

イ　新システムの稼働率

業務報告書等により調査

ウ　原子力規制委員会広報総合評価・分析の結果

各年度において、ユーザに対する年１回のアンケート（原子力規制委員会広報総合評価・分析）の実施結果により調査

エ　セキュリティ上の重大障害の件数

業務報告書等により調査

オ　システム運用上の重大障害の件数

業務報告書等により調査

カ　復旧時間の調査

業務報告書等により調査

（３）意見聴取等

当庁は、必要に応じ、請負事業者から意見の聴取を行うことができるものとする。

（４）実施状況等の提出時期

当庁は、令和１０年５月を目途として、本業務の実施状況等を総務大臣及び監理委員会へ提出する。

12. その他業務の実施に関し必要な事項

（1）本業務の実施状況等の監理委員会への報告

当庁は、法第26条及び第27条に基づく報告徴収、立入検査、指示等を行った場合には、その都度、措置の内容及び理由並びに結果の概要を監理委員会へ報告することとする。

（2）当庁の監督体制

本契約に係る監督は、主管係自ら立会い、指示その他の適切な方法によって行うものとする。

本業務の実施状況に係る監督は以下のとおり。

監督職員：原子力規制委員会原子力規制庁長官官房総務課広報室室長補佐

検査職員：原子力規制委員会原子力規制庁長官官房総務課広報室専門職

（3）本業務請負事業者の責務

ア　本業務に従事する請負事業者は、刑法（明治40年法律第45号）その他の罰則の適用については、法令により公務に従事する職員とみなされる。

イ　請負事業者は、法第54条の規定に該当する場合は、１年以下の懲役又は50万円以下の罰金に処される。

ウ　請負事業者は、法第55条の規定に該当する場合は、30万円以下の罰金に処されることとなる。なお、法第56条により、法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関し、法第55条の規定に違反したときは、行為者を罰するほか、その法人又は人に対して同条の刑を科する。

エ　請負事業者は、会計検査院法（昭和22年法律第73号）第23条第１項第７号に規定する者に該当することから、会計検査院が必要と認めるときには、同法第25条及び第26条により、同院の実地の検査を受けたり、同院から直接又は当庁に通じて、資料又は報告等の提出を求められたり、質問を受けたりすることがある。

（4）著作権

ア　請負事業者は、本業務の目的として作成される成果物に関し、著作権法（昭和45年法律第48号）第27条及び第28条を含む著作権の全てを当庁に無償で譲渡するものとする。

イ　請負事業者は、成果物に関する著作者人格権（著作権法（昭和45年法律第48号）第18条から第20条までに規定された権利をいう。）を行使しないものとする。ただし、当庁が承認した場合は、この限りではない。

ウ　ア及びイに関わらず、成果物に請負事業者が既に著作権を保有しているもの（以下「請負事業者著作物」という。）が組み込まれている場合は、当該請負事業者著作物の著作権についてのみ、請負事業者に帰属する。

エ　提出される成果物に第三者が権利を有する著作物が含まれる場合には、請負事業者が当該著作物の使用に必要な費用の負担及び使用許諾契約等に係る一切の手続を行うものとする。

（5）本業務の仕様書

本業務を実施する際に必要な仕様は、別添１「原子力規制委員会ホームページシステム更改に係る構築及び運用・保守業務　調達仕様書」に示すとおりである。

従来の実施状況に関する情報の開示

1　従来の実施に要した経費　（単位：千円）

		令和3年度	令和4年度	令和5年度
請負費等	役務	79,874	79,874	79,874
	機器・回線等料	33,754	33,754	33,754
	その他	11,362	11,362	11,362
	消費税	12,499	12,499	12,499
計(a)		13,748	13,748	13,748

（注記事項：請負等の内訳は下記のとおり）
原子力規制庁では、民間競争入札の対象である原子力規制委員会ホームページシステム更改に係る構築及び運用・保守業務の全部を請負契約により実施している。
なお、計(a)の支払金額は、一般競争入札の落札額である。
本事業は国庫債務負担行為5年として予算計上し実施。

令和7年度からはガバメントクラウドの利用を予定。

2 従来の実施に要した人員

（単位：人）

	令和3年度	令和4年度	令和5年度
（受託者における運用管理*業務*従事者）			
PJ責任者(非常駐)	1	1	1
運用チームリーダ（非常駐）	1	1	1
運用チームメンバ(非常駐)	3	3	2
保守チームリーダ(常駐)	1	1	1
保守チームメンバ(非常駐)	3	3	3

（業務従事者に求められる知識・経験等）
運用チームリーダ
・本サイトと同規模以上のサイト運用リーダとして3件以上の経験を有すること。
運用チームメンバ
・サイトディレクション業務経験を2年以上有する者もしくは同等の経歴を有するものを1名以上含むこと。
・CMSによるサイト運用について1年以上の実務経験をメンバー全員が有していること。
・webクリエイター能力試験資格もしくは同等レベルのスキルをメンバー全員が有していること。
保守チームリーダ
・本サイトと同規模以上のCMSならびにサーバ関連保守リーダとして3件以上の経験を有すること。
保守チームメンバ
・本サイトと同規模以上のCMSならいにサーバ関連保守業務経験を1年以上有するものもしくは同等の経歴を有する者。
・情報セキュリティ関連において、情報セキュリティマネジメント、情報処理安全確保支援士の資格保有者を1名以上含むこと。

（令和3年度）

（件）

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	計
HTMLページ作成更新CMS作業	294	151	108	116	120	153	58	426	235	1268	123	349	3401
緊急保守対応	12年10/27以降監視メール外部への受信不可、監視サーバへの接続不可のため保守実績								0	0	1	0	1

（令和4年度）

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	計
HTMLページ作成更新CMS作業	503	150	178	130	257	101	95	362	237	257	166	233	2669
緊急保守対応	0	1	0	0	0	0	0	0	0	0	0	0	1

（令和5年度）

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	計
HTMLページ作成更新CMS作業	471	145	127	106	288	130	106	152	107	68	114	368	2182
緊急保守対応	0	0	0	0	0	0	0	0	0	0	0	0	0

（注記事項）

3 従来の実施に要した施設及び設備

本省
【施設】
施設名称：NTT ExCパートナー　麻布ビル
使用場所：マーケティング部居室
【設備】
規制庁専用端末貸与
PC4台
請負者所有
ノートPC7台、デスクトップPC14台、複合機（FAX、コピー、PR）2台、

外部拠点
なし

4 従来の実施における目的の達成の程度

	令和3年度		令和4年度		令和5年度	
	目標・計画	実績	目標・計画	実績	目標・計画	実績
CMSサービス稼働率	*99.00%*	*99.90%*	*99.00%*	*99.85%*	*99.00%*	*100%*

（注記事項）

5 従来の実施方法等

従来の実施方法（業務フロー図等）

運用業務等に係る業務フロー等については、原子力規制庁と覚書を交わした上で閲覧により開示する。

（注記事項）

別紙2

再委託承認申請書

令和　年　　月　　日

支出負担行為担当官
原子力規制委員会
原子力規制庁長官官房参事官　殿

住　　所
商号又は名称
代 表 者 氏 名

「令和7年度から令和11年度原子力規制委員会ホームページシステム更改に係る構築及び運用・保守業務」に関して、再委託をしたく下記のとおり承諾を求めます。

記

契約件名	
再委託の相手方の住所及び商号又は名称	
再委託を行う業務の範囲	
再委託を必要とする理由	
契約金額	

担当者連絡先
部署名　：
担当者名　：
ＴＥＬ　：
E-mail　：

別紙3

令和　　年　　月　　日

原子力規制委員会原子力規制庁 長官官房総務課 広報室長 殿

資料閲覧申込書

「令和 7 年度から令和 11 年度原子力規制委員会ホームページシステム更改に係る構築及び運用・保守業務」に係る開示書類に対し、以下のとおり閲覧を申込みます。

- 資料閲覧申込者（法人名）：＿＿＿＿＿＿＿＿＿＿＿＿

- 資料閲覧希望日時

➢ 令和＿＿年＿＿月＿＿日＿＿時＿＿分から

- 資料閲覧申込者の代表者

➢ 所　　属　：＿＿＿＿＿＿＿＿＿＿＿＿

➢ 氏　　名　：＿＿＿＿＿＿＿＿＿＿＿＿

➢ 連絡先（TEL）：＿＿＿＿＿＿＿＿＿＿＿＿

（Email）：＿＿＿＿＿＿＿＿＿＿＿＿

- その他閲覧者

項番	所属	氏名
1		
2		

以上

別紙4

原子力規制委員会原子力規制庁 長官官房総務課 広報室長 殿

守秘義務に関する誓約書

令和　　年　　月　　日
住　　所
資料閲覧者（法人名）
代表者名　　印

当社は、「令和 7 年度から令和 11 年度原子力規制委員会ホームページシステム更改に係る構築及び運用・保守業務」の調達（以下「本調達」という。）における提案書等の作成に当たって必要な情報について確認及び検討することを目的とし資料閲覧を希望します。なお、資料閲覧にあたり以下の各事項を遵守することを誓約します。

1．本誓約における機密情報とは、原子力規制委員会原子力規制庁長官官房総務課広報室（以下「原子力規制庁」という。）が開示する全ての情報（資料、電子情報、電子メール・FAX、口頭による連絡・説明等形態を問わない。）とする。ただし、開示の時点で既に公知のもの及び原子力規制庁が公表することを承諾した情報については除く。

2．当社は、原子力規制庁から開示された機密情報を本調達の提案書等の作成に当たって必要な情報を確認する目的にのみ使用するものとし、その他の目的には使用しないものとする。

3．当社は、原子力規制庁から開示された機密情報を本調達の提案書等の作成に当たって必要な情報を確認するために知る必要がある自己の役員、従業員以外に開示、閲覧等させないものとする。

4．当社は、原子力規制庁から開示された機密情報を第三者に開示又は漏えいしないものとする。

5．当社は本調達の提案書を検討するに当たって第三者に機密情報を開示、閲覧等させる必要がある場合には、原子力規制庁の事前承諾を得た上で、当該第三者に開示するものとする。

6．当社は、前項により、機密情報を開示する第三者に対し、本誓約と同様の機密保持誓約をさせるものとする。

7．当社は、本調達が終了または原子力規制庁から要求された場合には、機密情報を原子力規制庁に返却又は廃棄するものとする。

8．当社は、本調達の意見を検討するに当たって機密情報を知る必要のある自己の役員、従業員に、本誓約の内容を遵守させるものとする。

9．当社又は5．で定める第三者が、本誓約のいずれかの事項に違反した場合、又は漏えい等事故により原子力規制庁に損害を与えた場合には、当社は、原子力規制庁が被った損害の賠償をするものとする。

令和７年度から令和11年度原子力規制委員会
ホームページシステム更改に係る
構築及び運用・保守業務

調達仕様書（案）

令和７年１月

目次

1.　調達案件の概要に関する事項

1-1. 調達件名

令和７年度から令和11年度原子力規制委員会ホームページシステム更改に係る構築及び運用・保守業務

1-2. 調達の背景

原子力規制委員会（以下「規制庁」という）は、国民の生命、健康及び財産の保護、環境の保全並びに我が国の安全保障に資するため、原子力利用における安全の確保を図ること（原子力に係る製錬、加工、貯蔵、再処理及び廃棄の事業並びに原子炉に関する規制に関することを含む。）を任務とする組織である。
原子力規制委員会ホームページでは規制に関わる情報を公開しており、令和２年実施のリニューアルにおいてコンテンツマネジメントシステム（CMS）を導入し、スマートフォンを含めた多様な利用環境への対応、探しやすいホームページとしての情報整理を実施し、運用・保守を委託することにより安定した運用を実現してきたが、情報量及びコンテンツの増加等によりページ構成が複雑化しており、利用者が必要な情報を見つけられない、専門的な内容のページが多く、利用者層が限定されている等、ユーザビリティやアクセシビリティに課題が生じている。
この度のシステム更改では、現在のオンプレミスでのCMS運用からセキュリティと災害対策の強化、運用コストの削減などを目的としたガバメントクラウドへの移行を検討している。なお、セキュリティ対策については、内閣サイバーセキュリティセンターが定める要件を達成すること。また、委員会・会合等の意思決定に関わる重要な情報をアーカイブしたうえで、検索性の向上等を目的に令和５年度に更改された、公開情報管理システム（N-ADRES）等との連携を強化し、更なる情報公開の改善を予定している。（具体的な連携方法については、要件定義書「3-4 外部インターフェースに関する事項」を参照）課題としているユーザビリティの改善に係っては、トップページ構成の見直しを行い、N-ADRESの掲載項目と重複している箇所の削除、掲載情報の削減をすることでページ構成を簡素化し、閲覧性・利便性の向上を図る予定である。また緊急時トップページについても、正確な情報を従前より素早く利用者に届けられるよう、改修を検討する予定である。

1-3. 目的及び期待する効果

原子力規制委員会ホームページでは原子力の規制に関わる様々な情報（委員会関連の資料、調達関連情報、発電所別情報等）を公開しており、年間約270万アクセス（2023年度）を記録する等、様々な利用者によって閲覧されている。本業務の目的は、上記背景を踏まえつつ、原子力規制委員会ホームページの運営を効率的かつ継続的に行うためであり、外部公開

Webサーバ及びCMSの運用基盤をガバメントクラウドへと確実に移行することを目指す。
また、本業務は、「令和５年度原子力規制委員会ホームページシステムの更改に関連する調達支援業務」で得られたユーザビリティ評価、職員からのアンケート結果、行政事業レビューにおいて抽出された課題を基に、システム更改方針の具体化と課題の解決を目的とする。

（1）ユーザビリティの課題
- ナビゲーションとメニューの改善
- コンテンツの可読性向上
- カラースキームの最適化

（2）アクセス状況の課題
- 直帰率を下げるUIデザインの見直し
  ユーザの直帰率が高いことから、ナビゲーションと関連情報の表示を改善する必要がある。
- サイト横断を促す関連ページの表示の最適化
  特定ページへの集中的な閲覧と高い離脱率を改善するために、関連ページの表示を強化する。

（3）行政事業レビューで指摘された課題
- 原子力規制の内容の分かりやすい提示
- 検索機能とホームページの使いやすさの改善
- 迅速かつ正確な情報発信による信頼性の向上
- 原子力規制委員会の業務と委員の理解促進のための広報活動
- SNSとの連携強化による情報配信の向上

上記課題を解決するサイト構成・ユーザビリティ設計を実現し、誰もが負担なく情報を取得できるよう、JIS X 8341-3:2016 達成レベルAA適合を行う。

1-4. 業務・情報システムの概要

本システムの概要は次の図のとおりである。

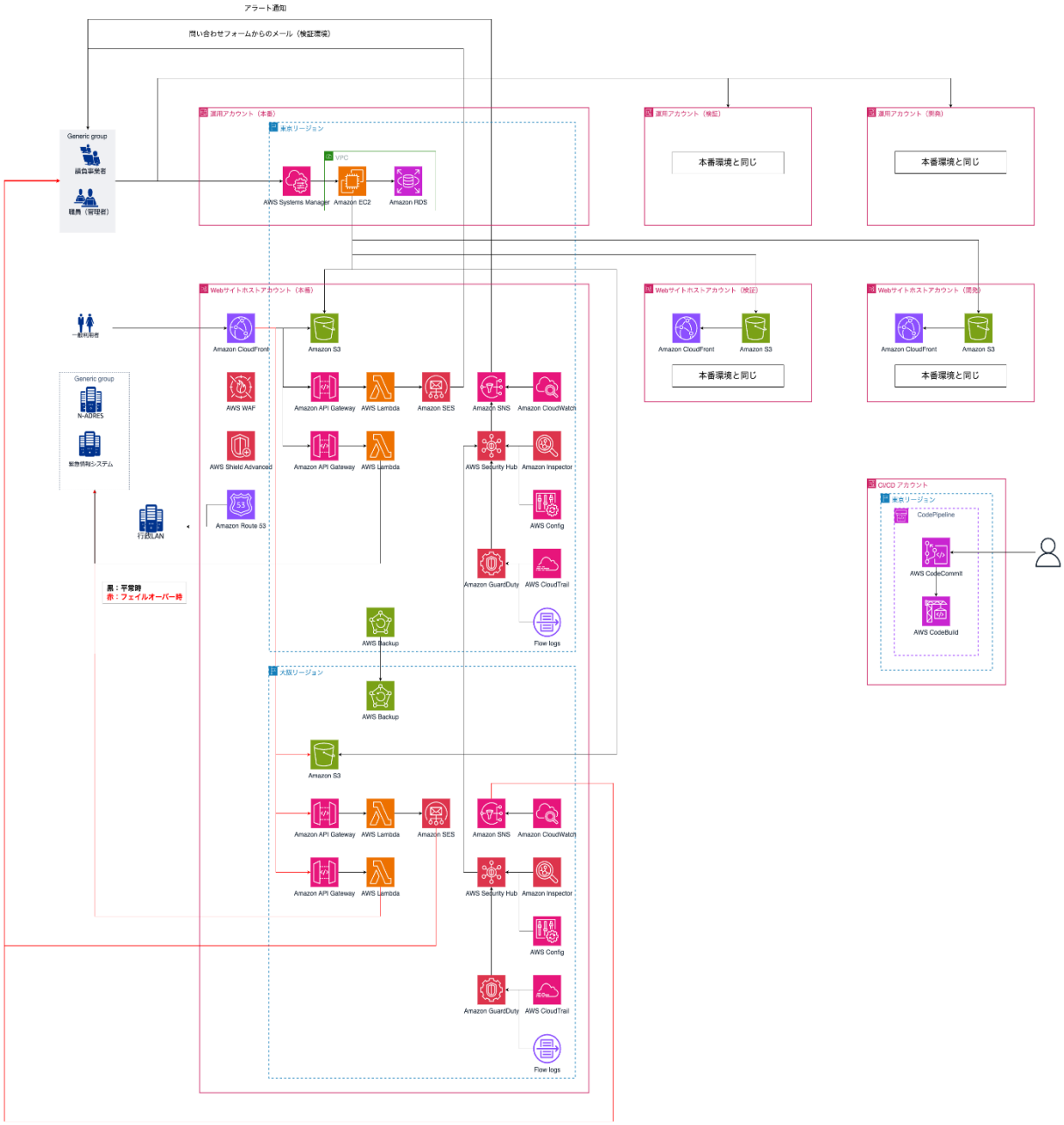


図１　システムの概要

1-5. 契約期間

契約締結日から令和12年３月31日まで

1-6. 作業スケジュール

作業スケジュールは次のとおり想定している。

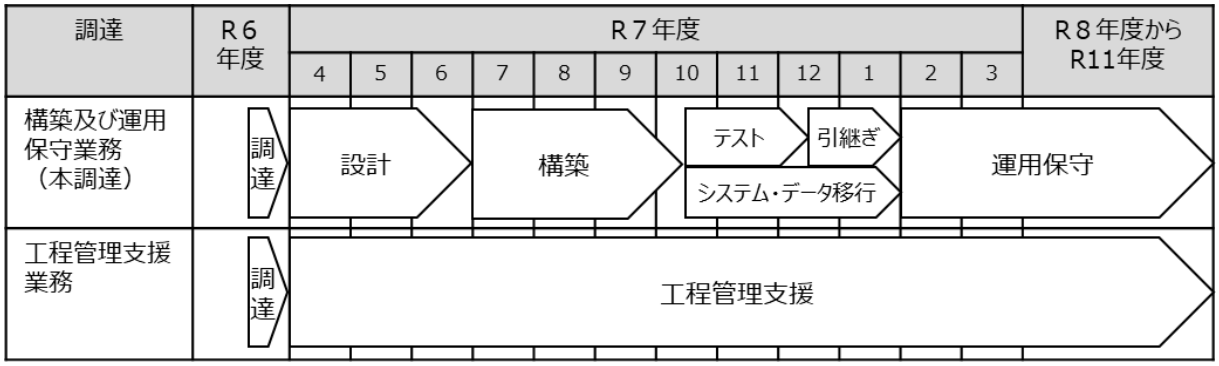


図２　作業スケジュール

1-7. 用語

本書で扱う用語の定義は「デジタル・ガバメント推進標準ガイドライン」（以下「標準ガイドライン」という。）の用語集と同様とし、用語の定義をしていないものは特に指定がない限り一般的な用語の定義を用いるものとする。

2.　調達案件及び関連調達案件の調達単位、調達の方式等に関する事項

2-1. 調達案件及びこれと関連する調達案件の調達単位、調達の方式、実施時期

表１　調達案件及び関連する調達案件の一覧

種別	件名	調達方式	実施時期（予定）
関連調達案件	令和５年度原子力規制委員会ホームページシステムの更改に係る調達支援等業務	総合評価落札方式	令和５年４月３日から 令和６年３月 31 日
関連調達案件	令和６年度次期ホームページ公開システムに係る追加調達支援業務	企画競争方式	契約締結日から 令和７年３月 31 日
本調達	令和７年度から令和 11 年度原子力規制委員会ホームページシステム更改に係る構築及び運用・保守業務	総合評価落札方式	契約締結日から 令和 12 年３月 31 日
関連調達案件	令和７年度原子力規制委員会ホームページシステム更改に係る構築及び運用・保守に係る工程管理支援業務	企画競争方式	契約締結日から 令和８年３月 31 日

2-2. 調達案件間の入札制限

次の受注事業者（再委託先等を含む。）及びこの事業者の「財務諸表等の用語、様式及び作成方法に関する規則」（昭和38年11月27日大蔵省令第59号）第8条に規定する親会社及び子会社、同一の親会社を持つ会社並びに委託先事業者等の緊密な利害関係を有する事業者は、入札には参加できない。また、これらの者については、請負事業者の再委託先となることもできない。

（１）「令和５年度原子力規制委員会ホームページシステムの更改に係る調達支援等業務」の受注者
（２）「令和６年度次期ホームページ公開システムに係る追加調達支援業務」の受注者
（３）「令和７年度から令和11年度原子力規制委員会ホームページシステム更改に係る構築及び運用・保守に係る工程管理支援業務」の受注者

3. 求める要件に関する事項

本業務の実施に当たっては、別添１「要件定義書」の各要件を満たすこと。

4. 作業の実施内容

4-1. 設計・構築業務

（１）設計・構築前
要件定義書「5-2 設計・構築に関する要件（１）設計・構築前」に記載された内容に従い、設計・構築前の業務を実施すること。

（２）設計・構築時
要件定義書「5-2 設計・構築に関する要件（２）設計・構築時」に記載された内容に従い、設計・構築時の業務を実施すること。

（３）テスト
要件定義書「5-3 テストに関する要件」に記載された内容に従い、テストの業務を実施すること。

（４）受入テスト支援
要件定義書「5-3 テストに関する要件（２）テストの種類毎の要件」に記載された内容に従い、受入テスト支援の業務を実施すること。

（５）システムの移行
要件定義書「5-4 移行に関する要件」に記載された内容に従い、移行の業務を実施すること。

（６）教育
要件定義書「5-5 教育に関する要件」に記載された内容に従い、教育の業務を実施すること。

（７）引継ぎ
要件定義書「5-6 運用に関する要件（７）引継ぎ」及び「5-7 保守に関する要件（５）引継ぎ」に記載された内容に従い、引継ぎの業務を実施すること。

（８）定例会等の実施
定例会等の実施に係る基本的な要件を以下に示す。

- 請負事業者は、定例会を隔週開催するとともに、業務の進捗状況を作業実施要領に基づき報告すること。
- 請負事業者は、規制庁から要請があった場合、又は、請負事業者が必要と判断した場合、必要資料を作成の上、定例会とは別に会議を開催すること。
- 請負事業者は、会議終了後、３日以内（行政機関の休日（行政機関の休日に関する法律（昭和63年法律第91号）第１条第１項各号に掲げる日をいう。）を除く。）に議事録を作成し、規制庁の承認を受けること。

4-2. 運用・保守業務

（1）運用・保守
要件定義書「5-6 運用に関する要件」及び「5-7 保守に関する要件」に記載された内容に従い、運用及び保守の業務を実施すること。

（2）中長期運用・保守作業計画の確定支援
運用設計及び保守設計に基づき、計画的に発生する作業内容、その想定される時期等を取りまとめ、規制庁担当官の確認を受けたうえで、中長期運用・保守計画の策定を支援すること。

（3）運用・保守計画及び運用・保守実施要領の策定
- 運用設計及び保守設計に基づき、定常時における月次の作業内容、その想定スケジュール、障害発生時における作業内容等を取りまとめ、規制庁担当官の確認を受けたうえで、運用計画及び保守計画を策定すること。
- 上項の実施にあたっては、情報システム全体のセキュリティ水準が低下することのないようセキュリティ要件を適切に策定し、情報セキュリティに関する各種機能（アクセス制御、識別コード、主体認証情報の付与、定期的な脆弱性情報の把握と対策、標的型攻撃対策及びログの取得、管理等）が有効に機能するようにすること。また、附属文書として、監視項目、定期保守項目、運用・保守業務フローなどの作業項目、作業内容、スケジュール、担当者等について記載すること。
- 運用計画及び保守計画の策定において、セキュリティインシデントを含む障害の発生に備え、導入機器やソフトウェア等に対して必要な対策及び対策の実施に伴う業務への影響を取りまとめ、規制庁担当官の確認を受けること。
- その他に規制庁担当官からの求めに応じ、運用・保守計画及び運用・保守実施要領を更新すること。

4-3. プロジェクト管理に係る業務

（1）統合管理
- 定例会を隔週開催するとともに、業務の進捗状況を作業実施要領に基づき報告すること。
- 規制庁から要請があった場合、又は、請負事業者が必要と判断した場合、必要資料を作成の上、定例会とは別に会議を開催すること。
- 要件のトレース管理等を活用し、変更管理を適切に実施すること。

（2）スコープ管理
- 本業務の実施範囲及び成果物を明確化するとともに、作業項目、作業内容をより階層化し、担当者等を記載した WBS を作成すること（業務計画書の付属文書）。
- なお、その際、規制庁担当官との認識の共有を図ること。
- プロジェクト計画書、要件定義書、調達仕様書の各要件に対して、実現箇所、実現方法等を追跡・管理するために、要件をトレース管理する仕組みを導入すること。
- 本業務の実施段階においても、規制庁担当官と調整して作業及び成果物の妥当性を確認しつつ進めること。

（3）スケジュール管理

- 規制庁担当官の指示に基づき、工程管理等支援業務請負者と調整の上、本業務の業務計画書の案を作成し、規制庁担当官の承認を受けること。その際、スケジュール内に完了するために適切なマイルストーン（チェックポイント）を定め、マイルストーンから逆算した各タスクの期間設定及び完了条件を定めておくこと。
- マイルストーンの記載にあたっては、情報資産管理標準シートの提出時期を示すこと。

（4）品質管理

- システムの構築を効率的に実施するため、構築やテスト等の標準（例：何をインプット（設計書等）として作業を行い、インプット情報に示された事項を確実に実装しテストしたことを記録するルールやシステムの構成要素毎の重要度に応じたテストの網羅性と密度の設定ルール、さらにはテストの中に占めるセキュリティテストの網羅性と密度等の設定ルール等、設計されたものが確実に実装され適切な品質を保つことを可能とする構築に係る標準）を定め規制庁担当官の確認を受けること。
- なお、本標準は、業務ごと（構築標準等）に分けて策定しても良い。

（5）コミュニケーション管理

- 会議の特性、参加者の勤務場所等を踏まえ、会議の適切な態様（対面、オンライン等）を検討した上で実施すること。
- 会議終了後、３日以内（行政機関の休日（行政機関の休日に関する法律（昭和63年法律第 91 号）第１条第１項各号に掲げる日をいう。）を除く。）に議事録を作成し、規制庁担当官の承認を受けること。

（6）リスク管理

- リスクの特定にあたっては、請負事業者の内部のリスクについても積極的に洗い出すものとする。なお、リスク登録簿の様式については、プロジェクトマネジメント協会日本支部が公開しているリスク登録簿を参照すること。
- リスク対応の計画においては、事前の対応戦略だけでなく、リスク発生後のコンティンジェンシー対応戦略についても計画すること。その際、対応戦略実行のトリガー条件について決定しておくこと。特にスケジュールが遅延した場合に備え、常にコンティンジェンシー対応戦略を計画すること。
- リスク登録簿の提出は、業務計画書と同時とする。その後、リスク登録簿を随時更新すること。

（7）その他

- 規制庁及び規制庁が指示する機関等が実施する工程レビュー等の実施に先立ち、規制庁からの指示のもと、必要な情報の提供や資料の作成等の支援を行うこと。

4-4. 契約金額内訳及び情報資産管理標準シートの提出

- 標準ガイドラインの別紙２「情報システムの経費区分」に基づき区分等した契約金額の内訳を記載した情報資産管理標準シートを契約締結後速やかに提出すること。

・ 請負事業者は、情報資産管理標準シート及び標準ガイドラインの別紙３「調達仕様書に盛り込むべき情報資産管理標準シートの提出等に関する作業内容」の「３．その他」のうち、次に掲げる事項について記載したエクセル電子データを提出する時期を「運用実施要領及び保守実施要領」等において定め、提出すること。

(ア)各データの変更管理

本システムの保守において、構築規模の管理、ハードウェアの管理、ソフトウェアの管理、回線の管理、外部サービスの管理、施設の管理、公開ドメインの管理、取扱情報の管理、情報セキュリティ要件の管理、指標の管理の各項目についてその内容に変更が生じる作業をしたときは、当該変更を行った項目。

(イ)作業実績等の管理

本システムの保守中に取りまとめた作業実績、リスク、課題及び障害事由。

4-5. 成果物

(１)設計・構築工程における成果物

表２ 設計・構築工程における成果物一覧

No.	分類	成果物名称	納品期日	備考
1	プロジェクト管理	設計・開発実施計画書	契約締結後２週間	
2		設計・開発実施要領	契約締結後２週間	
3		設計・開発実施要領に基づく管理資料	契約締結後２週間	
4		情報管理計画書	契約締結後２週間	
5		各種会議体議事録	都度	
6	設計・構築	要件定義書（更新案）	令和７年６月末	
7		基本設計書	令和７年６月末	HPのデザイン案含む
8		詳細設計書	令和７年６月末	
9		運用設計書	令和７年６月末	
10		保守設計書	令和７年６月末	
11		中長期運用・保守計画書（案）	令和７年６月末	
12		情報資産管理標準シート	令和７年６月末	
13		ハードウェア構成表及び一覧	令和７年６月末	
14		ソフトウェア構成表及び一覧	令和７年６月末	
15		ライセンス関連情報	令和７年６月末	
16		構築標準、保守標準、運用標準	令和７年６月末	
17		ソースコード	令和７年12月末	
18		実行プログラム	令和７年12月末	
19		ソフトウェア製品パッケージ	令和７年12月末	
20		セキュリティルール	令和７年６月末	
21	テスト	テスト計画書	令和７年９月末	
22		単体テスト結果報告書	令和７年12月末	

23		結合テスト結果報告書	令和７年12月末	
24		総合テスト結果報告書	令和７年12月末	
25		脆弱性診断結果報告書	令和７年12月末	
26		テスト項目表、テスト手順書（テストシナリオ・スクリプト）、テストデータ、セキュリティ対策結果報告書	令和７年12月末	受入テストのテスト項目表やテスト手順書も含む
27	移行	移行計画書（リハーサル含む）、移行ガイドライン、移行データ調査結果報告書	令和７年９月末	
28		移行手順書、移行マニュアル、移行ツール、移行リハーサル計画書、移行リハーサル結果報告書	令和７年12月末	
29		移行実施報告書	令和８年１月末	
30	教育	研修用資料（業務マニュアル）	令和８年１月末	
31		教育結果報告書	令和８年１月末	
32	運用（計画）	運用計画書（案）	令和８年１月末	
33		運用実施要領	令和８年１月末	
34		運用手順書	令和８年１月末	
35		運用マニュアル	令和８年１月末	
36	保守（計画）	保守計画書（案）	令和８年１月末	
37		保守実施要領	令和８年１月末	
38		保守手順書	令和８年１月末	

（2）運用・保守工程における成果物

表３ 運用・保守工程における成果物一覧

No.	成果物名称	納品期日
1	運用報告書（月次）	翌月 10 営業日以内（ただし、最終月分は、令和 12年３月末まで）
2	保守報告書（月次）	翌月 10 営業日以内（ただし、最終月分は、令和 12年３月末まで）
3	運用作業報告書	翌月 ５営業日以内（ただし、最終月分は、令和 12年３月末まで）
4	保守作業報告書	翌月 ５営業日以内（ただし、最終月分は、令和 12年３月末まで）
5	障害対応報告書	翌月 10 営業日以内（ただし、最終月分は、令和 12年３月末まで）
6	運用報告書（年次）	毎年４月下旬（ただし、最終年度分は、令和12年３月末まで）
7	保守報告書（年次）	毎年４月下旬（ただし、最終年度分は、令和12年３月末まで）
8	情報資産管理標準シート	毎年４月下旬（ただし、最終年度分は、令和12年３月末まで）
9	各種管理台帳等	都度
10	突合・確認結果報告書	都度
11	中長期運用・保守計画（改善案）	都度
12	運用計画（改善案）	都度
13	保守計画（改善案）	都度
14	運用実施要領（改善案）	都度
15	保守実施要領（改善案）	都度
16	運用手順書（改善案）	都度
17	保守手順書（改善案）	都度
18	新システム構築事業者への引継ぎ文書	令和12年３月末
19	ライセンス関連情報	都度
20	ハードウェアとソフトウェアの関連図	都度
21	会議資料	実施後3日以内
22	議事録	実施後3日以内

（3）成果物の納品方法

- 成果物は、全て日本語で作成すること。
- 用字・用語・記述符号の表記については、「公用文作成の要領（昭和27年４月４日内閣閣甲第16号内閣官房長官依命通知）」を参考にすること。
- 情報処理に関する用語の表記については、日本産業規格（JIS規格）の規定を参考にすること。

- 電磁的記録媒体による納品について、ソースコード、実行プログラム以外は、Microsoft Word 2016、Microsoft Excel 2016、Microsoft PowerPoint 2016、JustSystems 一太郎 Government 8 のいずれかのファイル形式で作成し、CD-R 又は DVD-R の媒体に格納して納品すること。
- ソースコード、実行プログラムについては、該当するソフトウェアの標準ファイル形式で作成し、CD-R 又は DVD-R の媒体に格納して納品すること。
- 納品後規制庁において改変が可能となるよう、図表等の元データも併せて納品すること。
- 成果物の作成に当たって、特別なツールを使用する場合は、規制庁の承認を得ること。
- 成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。
- 電磁的記録媒体により納品する場合は、最新のパターンファイルを使用した不正プログラム対策ソフトウェアによる確認を行う等して、成果物に不正プログラムが混入することのないよう適切に対処し、対処内容を報告すること。
- 成果物は電磁的記録媒体により作成し、規制庁から特別に示す場合を除き、原則、電磁的記録媒体は２部を納品すること。

（４）　納品場所

原則として、成果物は次の場所において引渡しを行うこと。ただし、規制庁が納品場所を別途指示する場合はこの限りではない。

〒106-8450
東京都港区六本木１丁目９番９号
原子力規制委員会原子力規制庁長官官房総務課広報室

（５）　その他留意点

本業務の成果物の作成にあたっては、以下の要件を満たすこと。

- 作成方針について事前に規制庁と協議や確認を行う機会を十分に設け、規制庁の求める内容を反映すること。
- 規制庁に提出する以前に、内容及び品質について請負事業者において十分に確認を行った上で提出すること。
- 提出時に、請負事業者内での確認者名、確認日、確認内容を明示した確認書を添付すること。
- 提出された成果物について、規制庁による確認を行う期間、確認結果を伝達する機会、確認結果を反映する期間を十分に設けること。
- 専門用語や業界用語の使用を避け、規制庁の担当職員が理解できる資料等を作成す

ること。

- 規制庁による成果物の内容及び品質に係る確認を行い、内容及び品質が妥当であり、納品に当たり問題が無いと規制庁に認められたうえで納品を行うこと。

5. 作業の実施体制・方法に関する事項

5-1. 作業実施体制

本業務の推進体制及び請負事業者に求める作業実施体制の例を次の図に示す。なお、請負事業者内のチーム編成については協議の上決定し、必要に応じて見直しを行うものとする。

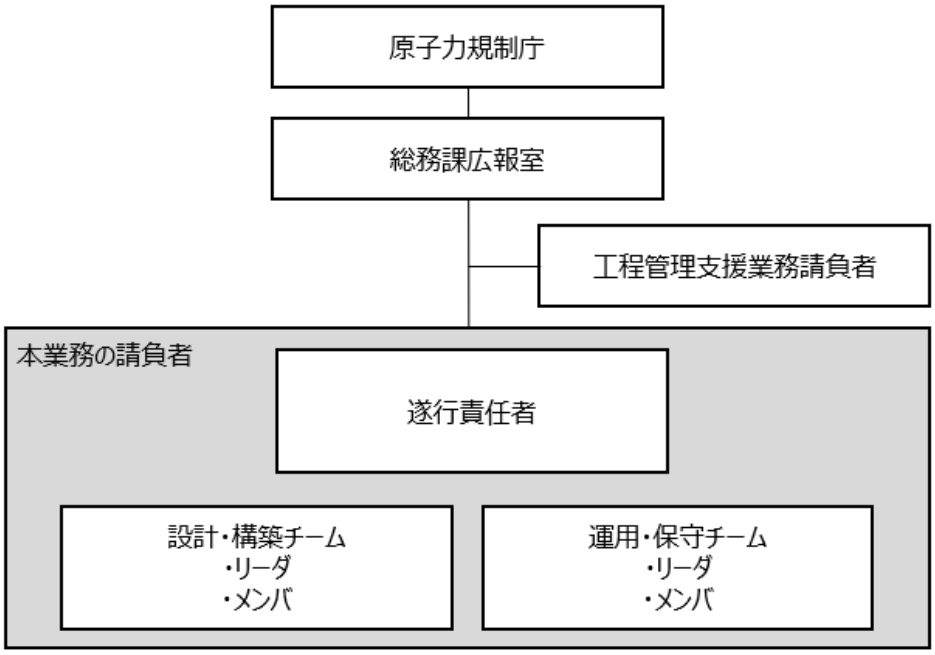


図３ 業務の推進体制例

表４ 作業実施体制例

No.	組織又は要員		役割
1	総務課広報室		本システムの設計・構築及び運用・保守の統括
2	本業務の請負者		―
3		遂行責任者	本業務全体を統括し、必要な意思決定を行う責任者
4		設計・開発チームリーダー	設計・開発に係るチームリーダー（責任者）
5		設計・開発チームメンバー	各業務実施担当者
6		運用・保守チームリーダー	運用・保守に係るチームリーダー（責任者）
7		運用・保守チームメンバー	各業務実施担当者

5-2. 作業要員に求める資格等の要件

- 遂行責任者は、本システムと同規模以上の設計・構築の遂行責任者としての経験を有すること。また、過去５年以内にクラウドサービスの設計開発又は運用保守において責任者としての実績を証明すること。

- 遂行責任者は、ホームページシステム更改業務におけるプロジェクトマネジメントの実績を有すること。加えて、日本工業規格（JIS X 8341－3:2016）をはじめ、アクセシビリティに配慮したホームページの構築業務におけるプロジェクトマネジメントの実績を有することが望ましい。
- 遂行責任者は、以下の試験区分の合格者又は資格保持者と同等以上の資格を有する者又は同等の能力を有することが経歴等において明らかな者とすること（同等の能力を有することが経歴等において明らかな者とする場合には、その根拠を明確に示し、規制庁の理解を得ること。）。
  （ア）経済産業省が認定するプロジェクトマネージャ試験
  （イ）PMI （ Project Management Institute ） が認定する PMP （ Project Management Professional）
- 設計・開発チームリーダーは、本システムと同規模以上の設計・開発の経験をリーダークラスとしての２件以上有すること。
- 設計・開発チームリーダー及び設計・開発メンバーに、経済産業省が認定する情報処理技術者試験のうち、以下のいずれかの試験区分の合格者を１名以上含めること。
  （ア）システムアーキテクト試験
  （イ）データベーススペシャリスト試験
  （ウ）情報処理安全確保支援士試験
- 設計・開発チームリーダー又は設計・開発メンバーに、標準ガイドラインに基づいた設計・開発の業務経験を有するメンバーを配置すること。
- 設計・開発チームリーダー又は設計・開発メンバーに、システムのユーザビリティに関する知識及び設計の実務経験を３年以上有するメンバーを配置すること。
- 設計・開発チームリーダー又は設計・開発メンバーに、採用するクラウドサービスに係る全ての技術領域において当該クラウドサービスの認定技術者としての上位資格[※]、又は同等の知識及び経験を有すること。
  ※ 例として、以下のような資格が挙げられる。
    ・ AWS 認定ソリューションアーキテクト-プロフェッショナルレベル試験
    ・ マイクロソフト認定ソリューションアソシエイト
- 設計・開発チームに、セキュリティ設計の監督、クラウドネイティブなセキュリティ設計を行うリーダーとして、以下のいずれかの資格と同等以上の資格を有する者がいること。
  （ア）経済産業省が認定する情報処理安全確保支援士試験
  （イ）ISACA（Information Systems Audit and Control Association）が認定する公認情報セキュリティマネージャー（CISM（Certified Information Security Manager））
  （ウ）国際情報システムズセキュリティ認証コンソーシアムが認定する情報シス

テムのセキュリティ専門家認定 （CISSP（Certified Information Systems Security Professional））

- 運用・保守チームリーダーは、本システムと同規模以上の運用保守の経験をリーダークラスとしての２件以上有すること。
- 運用・保守業務のチームリーダー及び運用・保守業務のメンバーのいずれかに、以下のいずれかの資格と同等以上の資格を有する者がいること。
  （ア）経済産業省が認定する情報処理安全確保支援士試験
  （イ）ISACA（Information Systems Audit and Control Association）が認定する公認情報セキュリティマネージャー（CISM（Certified Information Security Manager））
  （ウ）国際情報システムズセキュリティ認証コンソーシアムが認定する情報システムのセキュリティ専門家認定 （CISSP（Certified Information Systems Security Professional））
  （エ）ITIL（Information Technology Infrastructure Library）資格認定機関が認定する ITIL 認定のうち、ファウンデーション又はエキスパート
- 運用・保守業務のチームリーダー及び運用・保守業務のメンバーのいずれかに、直近５年間において、業務管理者レベルの役職でクラウドサービスを用いたシステムの運用・保守業務の実績を有する者がいること。

5-3. 作業場所

（１）原子力規制委員会原子力規制庁、日本法が適用される請負事業者の事業所及び請負事業者における従業者の自宅（テレワーク）で作業すること。
（２）「5-4. 作業の管理に関する要領」及び「6. 作業の実施に当たっての遵守事項」の各要件を満たすことが可能な場所で実施すること。なお、上記要件を全て満たすことが可能な場合は、請負事業者における従業員の自宅（テレワーク）のみで作業を実施することも可能である。 また、上記要件を満たせないと規制庁が判断した場合は、規制庁と協議のうえ作業場所の見直しを図ること。

5-4. 作業の管理に関する要領

（１）請負事業者は、規制庁が承認した設計・開発実施要領に基づき、設計・開発業務に係るコミュニケーション管理、体制管理、工程管理、品質管理、リスク管理、課題管理、システム構成管理、変更管理及び情報セキュリティ対策を行うこと。
（２）請負事業者は、規制庁が承認した運用実施要領及び保守実施要領に基づき、保守業務及び運用業務に係るコミュニケーション管理、体制管理、作業管理、リスク管理、課題管理、システム構成管理、変更管理及び情報セキュリティ対策を行うこと。
（３）請負事業者は工程管理において、当初定めたスケジュール内に完了するために適切な

マイルストーン（チェックポイント）を定め、マイルストーンから逆算した各タスクの期間設定及び完了条件を定めておくこと。更に、スケジュールが遅延した場合に備え、常にコンティンジェンシープランを検討すること。

（4）請負事業者は、リスク管理において下流工程で起こり得るリスクについても検討し、リスク低減に向けた検討・確認ポイントを明確にした上で規制庁へ報告すること。

（5）請負事業者は、変更管理（仕様管理）を適切に行うべく、プロジェクト計画書、本調達仕様書及び要件定義書の各要件に対して、実現箇所、実現方法等を追跡・管理するための仕組みを導入すること。

5-5. 会議の開催・記録

定例の進捗状況確認会議を月１回開催し、本業務全体の進行手順の確認、進捗状況の確認、進行上の課題への対応策の協議を行う。なお、進捗状況確認会議は必要に応じて追加開催する。

進捗状況確認会議とは別に、個別の検討案件について詳細な協議を行う個別検討会議を設置する。進捗状況確認会議は、各個別検討会議の目的、役割について決定するとともに、進捗の管理を行う。各個別検討会議は、それぞれ必要に応じて日時を設定し開催する。

進捗状況確認会議及び各個別検討会議の記録は、請負事業者が二部作成し、双方確認の上で保管する。

なお、会議の開催形態としては、状況に応じて対面及びWeb会議での開催とする。

5-6. 業務に関連する支援

本業務の円滑な遂行のため、必要に応じて次のとおり調整を行う。

（1）原子力規制委員会ネットワークシステムの運用業者等との調整

本業務を遂行するために、原子力規制委員会ネットワークシステムの運用業者、又は原子力規制委員会ホームページシステムの運用業者との間で確認や協議が必要な事柄が発生した場合は、規制庁立ち会いの下、随時打ち合わせ等を行う。

（2）関係部署との調整

本業務を遂行するために、関係部署に方針の確認依頼や、移行結果の確認依頼等を行う必要が生じた場合は、規制庁の指示に基づいて資料作成を行うとともに、必要に応じて内容説明等を担当する。

5-7. その他（工程管理支援業者の参画）

本業務には、原子力規制委員会が別途契約する工程管理支援業者が参画し、会議への同席、各種検証などを通じ、規制庁の支援を行う予定である。

6. 作業の実施に当たっての遵守事項

6-1. 機密保持、資料の取扱い

（1）請負事業者は、本業務の実施に際して知り得た規制庁の情報等（公知の事実等を除く）を、第三者に漏らし、盗用し、又は受託業務以外の目的のために利用してはならない。これらの者が秘密を漏らし、又は盗用した場合は、競争の導入による公共サービスの改革に関する法律（平成18年法律第51号。以下「法」という。） 第54条により罰則の適用がある。

（2）請負事業者は、本業務の実施に際して得られた情報処理に関する利用技術（アイデア又はノウハウ）については、請負事業者からの文書による申出を規制庁が認めた場合に限り、第三者へ開示できるものとする。

（3）請負事業者は、規制庁から提供された個人情報及び業務上知り得た個人情報について、個人情報の保護に関する法律（平成15年法律第57号）に基づき、適切な管理を行わなくてはならない。また、当該個人情報については、本業務以外の目的のために利用してはならない。

（4）請負事業者は、規制庁の情報セキュリティに関する規定等に基づき、個人情報等を取り扱う場合は、①情報の複製等の制限、②情報の漏えい等の事案の発生時における対応、③受託業務終了時の情報の消去・廃棄（復元不可能とすること。）及び返却、④内部管理体制の確立、⑤情報セキュリティの運用状況の検査に応じる義務、⑥請負事業者の事業責任者及び請負業務に従事する者全てに対しての守秘義務及び情報セキュリティ要求事項の遵守に関して、別紙４「守秘義務に関する誓約書」を契約後速やか

に規制庁に提出しなければならない。
（５）その他、規制庁は、請負事業者に対し、本業務の適正かつ確実な実施に必要な限りで、秘密を適正に取り扱うために必要な措置を採るべきことを指示することができる。

6-2. 法令等の遵守

（１）当該調達案件の業務遂行に当たっては、法令等を遵守し履行すること。
（２）環境省においては、率先して温室効果ガス削減その他の環境負荷の低減、資源の消費量の削減を含む3Rの取組の推進等、環境省の環境方針を定めており、本調達においても「より環境にやさしいネットワークシステム」を調達の基本としている。したがって、可能な限り環境への負荷（「環境基本法」（平成５年法律第91号）第２条第１項に規定する環境への負荷をいう。以下同じ。）を軽減したものであることを基本要件とする。
（３）物品の調達に当たっては、環境への負荷の低減に資する原材料又は部品を使用していること、使用に伴い排出される温室効果ガス等による環境負荷が少ないこと、使用後にその全部又は一部の再利用又は再生利用がしやすいことにより廃棄物の発生を抑制することができることその他の事由により、より環境への負荷の低減に資する製品を調達する。
（４）納入成果物のうち、「環境物品等の調達の推進を図るための方針」（平成27年４月１日環境大臣）に掲げる特定調達物品等に該当するものは、「環境物品等の調達の推進に関する基本方針」（平成27年２月３日閣議決定。以下「基本方針」という。）の判断の基準を満たすこと。その他の納入成果物についても可能な限り基本方針の判断の基準を満たすものを導入すること。

6-3. その他文書、標準への準拠

（１）プロジェクト計画書
当該調達案件の業務遂行に当たっては、プロジェクトの目的、目標、実施計画等を記載したプロジェクト計画書（規制庁作成資料） との整合を確保して行うこと。
（２）プロジェクト管理要領
当該調達案件の業務の管理に当たっては、プロジェクトを管理する手法、手順、遵守事項等を記載したプロジェクト管理要領（規制庁作成資料） との整合を確保して行うこと。
（３）プロジェクト標準
開発に当たっては、本調達仕様書及び要件定義書にて定める構築標準、運用標準、保守標準に準拠して作業を行うこと。
（４）原子力規制委員会情報セキュリティポリシー及びその関連規程
当該調達案件におけるセキュリティ対策実施に当たっては、規制庁が公開する「原子

力規制委員会情報セキュリティポリシー」及びその関連規程に準拠すること。

（５）経済産業省「IT 製品の調達におけるセキュリティ要件リスト」

請負事業者は、調達機器に対し、経済産業省の「IT 製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を満たすこと。

（６）本調達仕様書及び要件定義書

当該調達案件のシステム構築に当たっては、原子力規制委員会情報セキュリティポリシー、本調達仕様書及び要件定義書に記載されたセキュリティに係る要件を全て満たすこと。

（７）内閣サイバーセキュリティセンター「IT調達に係る国等の物品等又は役務の調達方針及び調達手続きに関する申合せ」

本調達において、「IT調達に係る国等の物品等又は役務の調達方針及び調達手続きに関する申合せ 別紙２」に該当する機器・役務等の調達を行う場合は、候補となる機器・役務等のリストを事前に規制庁に提出すること。また、規制庁がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、代替案やリスク低減対策等、規制庁と迅速かつ密接に連携し提案の見直しを図ること。

（８）独立行政法人情報処理推進機構「セキュリティエンジニアリング」

当該調達案件のソフトウェアの開発を行う場合は、独立行政法人情報処理推進機構の「セキュリティエンジニアリング」の情報を参照し、情報セキュリティ対策を実施すること。

https://www.ipa.go.jp/security/awareness/vendor/software.html

（９）機密情報等の廃棄について

情報システムを構成するハードウェア、ソフトウェア製品を廃棄するときには、廃棄物、数量、所有形態、再利用可否、廃棄方法を記載した廃棄対象物リストを作成し、規制庁に提出すること。また、廃棄時には、情報セキュリティポリシーに基づき、電磁的記録の抹消・物理的破壊等適切な処置を講じること。電磁的記録の抹消には、使用したソフトウェア名称とそのバーション、物理的破壊時には証明写真を添付した証明書類を規制庁に提出し、了承を得ること。

7. 成果物の取扱いに関する事項

7-1. 知的財産権の帰属

（１）本業務における成果物の原著作権及び二次的著作物の著作権（著作権法（昭和45年法律第48号）第21条から第28条に定める全ての権利を含む。）は、請負事業者が本調達の実施の従前から権利を保有していた等の明確な理由によりあらかじめ提案書にて権利譲渡不可能と示されたもの以外は、全て規制庁に帰属するものとする。

（２）規制庁は、成果物について、第三者に権利が帰属する場合を除き、自由に複製し、改

変等し、及びそれらの利用を第三者に許諾することができるとともに、任意に開示できるものとする。また、請負事業者は、成果物について、自由に複製し、改変等し、及びこれらの利用を第三者に許諾すること（以下「複製等」という。）ができるものとする。ただし、成果物に第三者の権利が帰属するとき及び複製等により規制庁がその業務を遂行する上で支障が生じるおそれがある旨を契約締結時までに通知したときは、この限りでないものとし、この場合には、複製等ができる範囲やその方法等について協議するものとする。

（3）本件プログラムに関する権利（著作権法（昭和45年法律第48号）第21条から第28条に定める全ての権利を含む。）及び成果物の所有権は、規制庁から請負事業者に対価が完済されたとき請負事業者から規制庁に移転するものとする。

（4）納品される成果物に第三者が権利を有する著作物（以下「既存著作物等」という。）が含まれる場合には、請負事業者は、当該既存著作物等の使用に必要な費用の負担及び使用許諾契約等に関わる一切の手続を行うこと。この場合、本業務の請負事業者は、当該既存著作物の内容について事前に規制庁の承認を得ることとし、規制庁は、既存著作物等について当該許諾条件の範囲で使用するものとする。

（5）請負事業者は規制庁に対し、一切の著作者人格権を行使しないものとし、また、第三者をして行使させないものとする。

7-2. 契約不適合責任

（1）本業務における成果物等について、種類、品質又は数量が契約書、本調達仕様書その他合意された要件（以下「契約書等」という。）の内容に適合しないもの（以下「不適合」という。）である場合、その不適合が規制庁の責に帰すべき事由による場合を除き、請負事業者は、自己の費用で、規制庁の選択に従い、その修補、代替物の引渡し又は不足分の引渡しによる履行の追完（以下、手段を問わず総称して「履行の追完」という。）をすること。なお、請負事業者は如何なる場合であっても、規制庁の選択と異なる方法で履行の追完をする場合は、規制庁の事前の承諾を受けること。

（2）請負事業者は、その具体的な履行の追完の実施方法、完了時期、実施により発生する諸制限事項について、規制庁と協議し、承諾を得てから履行の追完を実施するものとし、完了時には、その結果について規制庁の承諾を受けること。

（3）請負事業者が規制庁から相当の期間を定めた履行の追完の催告を受けたにもかかわらず、その期限内に履行の追完を実施しない場合、規制庁は、その不適合の程度に応じて代金の減額を請求することができる。ただし、次に掲げる場合、請負事業者に対して履行の追完の催告なく、直ちに代金の減額を請求することができる。

(ア)履行の追完が不能であるとき。

(イ)請負事業者が履行の追完を拒絶する意思を明確に表示したとき。

(ウ)本業務の性質又は契約書等の内容により、特定の日時又は一定の期間内に履行を

しなければ契約をした目的を達することができない場合において、請負事業者が履行の追完をしないでその時期を経過したとき。

(エ)前３号に掲げる場合のほか、前項の催告をしても履行の追完を受ける見込みがないことが明らかであるとき。

7-3. 検収

（１）本業務の請負事業者は、成果物等について、納品期日までに規制庁に内容の説明を実施して検収を受けること。

（２）検収の結果、成果物等に不備又は誤り等が見つかった場合には、直ちに必要な修正、改修、交換等を行い、変更点について規制庁に説明を行った上で、指定された日時までに再度納品すること。

8. 入札参加資格に関する事項

8-1. 競争参加資格

（１）法第15条において準用する法第10条各号（第11号を除く。）に該当する者でないこと。

（２）予算決算及び会計令（以下「予決令」という。）第７０条の規定に該当しない者であること。 なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を 得ている者は、同条中、特別の理由がある場合に該当する。

（３）予決令第７１条の規定に該当しない者であること。

（４）令和０４・０５・０６年度環境省競争参加資格（全省庁統一資格）「役務の提供等」の「Ａ」、「Ｂ」、「Ｃ」又は「Ｄ」の等級に格付けされている者であること。（「役務の提供等」の営業品目「ソフトウェア開発」、「情報処理」又は「その他」に登録している者であること。）なお、令和０７・０８・０９年度競争参加資格を引き続き取得すること。

（５）規制庁からの補助金交付等停止措置又は指名停止措置が講じられている者ではないこと。

（６）法人税並びに消費税及び地方消費税の滞納がないこと。

（７）労働保険、厚生年金保険等の適用を受けている場合、保険料等の滞納がないこと。

（８）入札説明書において示す暴力団排除に関する誓約事項に誓約できる者であること。

8-2. 公的な資格や認証等の取得

（１）本調達仕様書に基づく作業を実施する部門又は組織を対象として、ISO27001を基準とした認証を取得していること又は当該認証と同等の要件を有すること。当該認証と同等の

要件を有することとする場合には、その根拠（JIS Q 2700認定証、ISMS認定証、管理体制、品質マネジメントシステム運営規程、品質管理手順規定等）を明確に示し、PJMOの理解を得ること。

（２）本調達仕様書に基づく作業を実施する部門又は組織を対象として、ISO9001を基準とした認証を取得していること又は当該認証と同等の要件を有すること。当該認証と同等の要件を有することとする場合には、その根拠（JIS Q 9001認定証、管理体制、品質マネジメントシステム運営規程、品質管理手順規定等）を明確に示し、PJMO の理解を得ること。

（３）女性の職業生活における活躍の推進に関する法律（平成27年法律第64号、以下「女性活躍推進法」という。）、次世代育成支援対策推進法（平成15年法律第120号、以下「次世代法」という。）、青少年の雇用の促進等に関する法律（昭和45年法律第98号、以下「若者雇用推進法」という。）に基づく認定等（えるぼし認定等、くるみん認定、プラチナくるみん認定、ユースエール認定）を取得している場合は、認定等の名称及び認定通知書等の写しを提出すること。ただし、提案書提出時点において認定等の期間中であること。

8-3. 複数事業者による共同入札

（１）複数の事業者が共同入札する場合、その中から全体の意思決定、運営管理等に責任を持つ共同提案の代表者を定めるとともに、本代表者が本調達に対する入札を行うこと。

（２）共同入札を構成する事業者間においては、その結成、運営等について協定を締結し、業務の遂行に当たっては、代表者を中心に、各事業者が協力して行うこと。事業者間の調整事項、トラブル等の発生に際しては、その当事者となる当該事業者間で解決すること。また、解散後の契約不適合責任に関しても協定の内容に含めること。

（３）共同入札を構成する全ての事業者は、本入札への単独提案又は他の共同入札への参加を行っていないこと。

（４）共同入札を構成する全ての事業者は、「8-1. 競争参加資格」、「8-2. 公的な資格や認証等の取得」及び「8-4. 入札参加資格者における実績」を満たすこと。

8-4. 入札参加者における実績

（１）請負事業者は、公共機関（独立行政法人、地方公共団体を含む官公庁）のシステム及びユーザビリティ、アクセシビリティに配慮したホームページにおける運用の実績を有すること。

（２）100名以上の職員が利用する情報システムの運用又は保守作業を行った実績を直近５年以内に有すること。

（３）情報システムのクラウド環境への移行に係る設計、開発、運用の実績を過去３年以内に有すること。

9. 再委託に関する事項

9-1. 再委託の制限及び再委託を認める場合の条件

（1）本業務の請負事業者は、業務を一括して又は主たる部分を再委託（再委託先の事業者が受託した事業の一部を別の事業者に委託する再々委託等、多段階の委託が行われる場合の委託を含む。以下同じ。）してはならない。再委託を禁止する作業としては、要件定義書「5. 事業者の作業に関する事項」の各要件に関する規制庁との認識合わせ、作業方針・スケジュールの検討及び作業の全体管理等を想定している。ただし、具体的な再委託可否の範囲については、規制庁と協議のうえ決定すること。
（2）請負事業者における遂行責任者を再委託先事業者の社員や契約社員とすることはできない。
（3）請負事業者は再委託先の行為について一切の責任を負うものとする。
（4）再委託を行う場合、再委託先が「2-2. 調達案件間の入札制限」に示す要件を満たすこと。
（5）再委託先における情報セキュリティの確保については請負事業者の責任とする。
（6）規制庁は本契約の適正な履行の確保のために必要があると判断したときは、請負事業者に対し、さらに本契約の履行体制等について書面による報告を求めることができる。
（7）請負事業者は、前項により報告を求められた場合には、速やかに規制庁に対して報告をしなければならない。
（8）請負事業者は、請負事業者若しくはその従業員、再委託先又はその他の者によって、規制庁の意図せざる変更が加えられないための管理体制を整備すること。
（9）請負事業者は、再委託先の資本関係・役員等の情報、再委託事業の実施場所、再委託事業従事者の所属・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提供を行うこと。
（１０）請負事業者は、再委託先における情報セキュリティ対策及びその他の契約の履行状況を定期的に確認し、履行状況について規制庁に定期的に報告すること。

9-2. 承認手続

（1）本業務の実施の一部を合理的な理由及び必要性により再委託する場合には、あらかじめ再委託の相手方の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性及び契約金額等について記載した別紙２「再委託承認申請書」を規制庁に提出し、あらかじめ承認を受けること。
（2）前項による再委託の相手方の変更等を行う必要が生じた場合も、前項と同様に再委託に関する書面を規制庁に提出し、承認を受けること。
（3）再委託の相手方が更に委託を行う等、複数の段階で再委託が行われる場合（以下「再々委託」という。）には、当該再々委託の相手方の商号又は名称及び住所並びに再々委託を行う業務の範囲を書面で報告すること。

9-3. 再委託先の契約違反等

（1）再委託先において、本調達仕様書の「9-1 再委託の制限及び再委託を認める場合の条件」から「9-2 承認手続」に定める事項に関する義務違反又は義務を怠った場合には、請負事業者が一切の責任を負うとともに、規制庁は、当該再委託先への再委託の中止を請求することができる。

10. その他特記事項

（1）本件受注後に本調達仕様書及び要件定義書の内容の一部について変更を行おうとする場合、その変更の内容、理由等を明記した書面をもって規制庁に申し入れを行うこと。双方の協議において、その変更内容が軽微（契約額、納期に影響を及ぼさない）かつ許容できると判断された場合は、変更の内容、理由等を明記した書面に双方が記名捺印することによって変更を確定する。
（2）本調達の入札者は、支出負担行為担当官が別に指定する反社会的勢力等に該当しない旨の誓約書を提出すること。入札に参加した者が、誓約書を提出せず、又は虚偽の誓約をし、もしくは誓約書に反することとなったときは、当該者の入札を無効とする。

11. 附属文書

（1）別紙１ 要件定義書
（2）別紙２ 再委託承認申請書
（3）別紙３ 資料閲覧申込書
（4）別紙４ 守秘義務に関する誓約書

12. 資料閲覧

12-1. 閲覧可能資料

（1）「別紙１　従来の実施状況に関する情報の開示」のうち「従来の実施方法等」の詳細な情報
（2）プロジェクト計画書、プロジェクト管理要領
（3）原子力規制委員会ホームページリニューアル構成の変更点解説表
（4）CMS機能要件書
（5）原子力規制委員会ホームページシステムの運用体制及びシステム概要
（6）原子力規制委員会情報セキュリティ関連規程

12-2. 閲覧要領

（１）閲覧場所：原子力規制委員会原子力規制庁長官官房総務課広報室内、あるいは規制庁の指定する場所

（２）閲覧期間及び時間：入札説明会で別途指定する期間（閉庁日（日曜日、土曜日、国民の祝日に関する法律（昭和23年法律第178号）に規定する休日、12月29日から1月3日）を除く。）。１０時から１７時まで。

（３）閲覧手続：最大２名まで。応札希望者の商号、連絡先、閲覧希望者氏名を別紙３「資料閲覧申込書」に記載の上、閲覧希望日の３営業日前までに提出すること。また、閲覧日当日までに別紙４「守秘義務に関する誓約書」に記載の上、提出すること。

（４）閲覧時の注意：閲覧にて知り得た内容については、提案書の作成以外には使用しないこと。また、本調達に関与しない者等に情報が漏えいしないように留意すること。閲覧資料の複写等による閲覧内容の記録は行わないこと。

（５）連絡先：原子力規制委員会原子力規制庁長官官房総務課広報室 土屋、神田
電話：03-5114-2105

Title: 評価項目一覧 - 遵守確認事項 -

大項目	中項目	小項目	内容説明	遵守確認
0	遵守確認事項			
	1	競争参加資格		
		1	法第15条において準用する法第10条各号（第11号を除く。）に該当する者でないこと。	
		2	予算決算及び会計令（以下「予決令」という。）第70条の規定に該当しない者であること。 予決令第71条の規定に該当しない者であること。	
		3	令和04・05・06年度環境省競争参加資格（全省庁統一資格）「役務の提供等」の「A」、「B」、「C」又は「D」の等級に格付けされている者であること。（「役務の提供等」の営業品目「ソフトウェア開発」、「情報処理」又は「その他」に登録している者であること。）	
		4	規制庁からの補助金交付等停止措置又は指名停止措置が講じられている者ではないこと。	
		5	法人税並びに消費税及び地方消費税の滞納がないこと。	
		6	労働保険、厚生年金保険等の適用を受けている場合、保険料等の滞納がないこと。	
		7	入札説明書において示す暴力団排除に関する誓約事項に誓約できる者であること。	
	2	組織の実績・資格等		
		1	財団法人日本適合性認定協会又は海外の認定機関により認定された審査機関によるISO27001（ISMS認証）の認証若しくは、これらと同等の認証を有していること。	
		2	財団法人日本適合性認定協会又は海外の認定機関により認定された審査機関によるISO9001（品質マネジメントシステム）の認証若しくは、これらと同等の認証を有していること。	
		3	公共機関（独立行政法人、地方公共団体を含む官公庁）のシステム及びユーザビリティ、アクセシビリティに配慮したホームページにおける運用の実績を有すること。	
		4	100名以上の職員が利用する情報システムの運用又は保守作業を行った実績を直近5年以内に有すること。	
		5	情報システムのクラウド環境への移行に係る設計、開発、運用の実績を過去3年以内に有すること。	

Title: 評価項目一覧 - 遵守確認事項 -

大項目	中項目	小項目	内容説明	遵守確認
	3	従事者の実績・資格等		
		1	遂行責任者は、本システムと同規模以上の設計・構築の遂行責任者としての経験を有すること。また、過去5年以内にクラウドサービスの設計開発又は運用保守において責任者として実績を証明すること。	
		2	遂行責任者は、ホームページシステム更改業務におけるプロジェクトマネジメントの実績を有すること。	
		3	遂行責任者は、以下の試験区分の合格者又は資格保持者と同等以上の資格を有する者又は同等の能力を有することが経歴等において明らかな者とすること（同等の能力を有することが経歴等において明らかな者とする場合には、その根拠を明確に示し、規制庁の理解を得ること。）。 （ア）経済産業省が認定するプロジェクトマネージャ試験 （イ）PMI（Project Management Institute）が認定するPMP（Project Management Professional）	
		4	設計・開発チームリーダーは、本システムと同規模以上の設計・開発の経験をリーダークラスとしての2件以上有すること。	
		5	設計・開発チームリーダー及び設計・開発メンバーに、経済産業省が認定する情報処理技術者試験のうち、以下のいずれかの試験区分の合格者を1名以上含めること。 （ア）システムアーキテクト試験 （イ）データベーススペシャリスト試験 （ウ）情報処理安全確保支援士試験	
		6	設計・開発チームリーダー又は設計・開発メンバーに、標準ガイドラインに基づいた設計・開発の業務経験を有するメンバーを配置すること。	
		7	設計・開発チームリーダー又は設計・開発メンバーに、システムのユーザビリティに関する知識及び設計の実務経験を3年以上有するメンバーを配置すること。	
		8	設計・開発チームリーダー又は設計・開発メンバーに、採用するクラウドサービスに係る全ての技術領域において当該クラウドサービスの認定技術者としての上位資格[※]、又は同等の知識及び経験を有すること。 ※　例として、以下のような資格が挙げられる。 ・ AWS 認定ソリューションアーキテクト–プロフェッショナルレベル試験 ・ マイクロソフト認定ソリューションアソシエイト	
		9	設計・開発チームに、セキュリティ設計の監督、クラウドネイティブなセキュリティ設計を行うリーダーとして、以下のいずれかの資格と同等以上の資格を有する者がいること。 （ア）経済産業省が認定する情報処理安全確保支援士試験 （イ）ISACA（Information Systems Audit and Control Association）が認定する公認情報セキュリティマネージャー（CISM（Certified Information Security Manager）） （ウ）国際情報システムズセキュリティ認証コンソーシアムが認定する情報システムのセキュリティ専門家認定 （CISSP（Certified Information Systems Security Professional））	
		10	運用・保守チームリーダーは、本システムと同規模以上の運用保守の経験をリーダークラスとしての2件以上有すること。	

Title: 評価項目一覧 - 遵守確認事項 -

大項目	中項目	小項目	内容説明	遵守確認
		11	運用・保守業務のチームリーダー及び運用・保守業務のメンバーのいずれかに、以下のいずれかの資格と同等以上の資格を有する者がいること。 (ア) 経済産業省が認定する情報処理安全確保支援士試験 (イ) ISACA(Information Systems Audit and Control Association)が認定する公認情報セキュリティマネージャー(CISM(Certified Information Security Manager)) (ウ) 国際情報システムズセキュリティ認証コンソーシアムが認定する情報システムのセキュリティ専門家認定 (CISSP(Certified Information Systems Security Professional)) (エ)ITIL(Information Technology Infrastructure Library)資格認定機関が認定するITIL認定のうち、ファウンデーション又はエキスパート	
		12	運用・保守業務のチームリーダー及び運用・保守業務のメンバーのいずれかに、直近5年間において、業務管理者レベルの役職でクラウドサービスを用いたシステムの運用・保守業務の実績を有する者がいること。	
	4	情報セキュリティの確保		
		1	原子力規制委員会情報セキュリティポリシーに準拠した情報セキュリティ対策の履行を確保すること。	

Title: 評価項目一覧 - 提案要求事項一覧 -

提案書の目次			提案要求事項	評価区分	得点配分			評価基準		雛形ページ番号	提案書ページ番号
大項目	中項目	小項目			合計	基礎点	加点	基礎点	加点		
1	事業の実施方針										
	1	業務内容の妥当性、独自性									
		1	本調達の背景及び目的を理解しているか	任意		-	20	-	・本システムの調達の背景及び目的を十分に理解しているか。 ・本システムの調達の背景及び目的を踏まえた基本方針が策定されているか。		
		2	要件定義書に示すシステムの機能要件に対して優れた提案がなされているか	-		-	-	-	-		
		3	トップページや目的別メニュー等のデザイン等、画面に対して優れた提案がなされているか	任意		-	50	-	・簡易な操作によってページの作成が可能な工夫がされているか。 ・必要な情報にアクセスできるようホームページ全体の構成について工夫されているか。 ・要件をよく分析して、具体的かつ実現可能な提案となっているか。		
		4	ワークフローや外部インターフェース等、管理機能に対して優れた提案がされているか	任意		-	50	-	・承認フローを理解した上で、ページのステータス（一般利用者への公開・非公開）が適切に管理される提案となっているか。 ・連携システムとの外部インターフェースの設計方法について工夫されているか。 ・要件をよく分析して、具体的かつ実現可能な提案となっているか。		
		5	要件定義書に示すシステムの非機能要件に対して優れた提案がなされているか	-		-	-	-	-		
		6	ユーザビリティ及びアクセシビリティに対して優れた提案がなされているか	任意		-	50	-	・利用者に対するユーザビリティを高めるよう工夫されているか。 ・一般利用者に対するアクセシビリティが確保できるよう工夫されているか。 ・要件をよく分析して、具体的かつ実現可能な提案となっているか。		
		7	システム方式に対して優れた提案がなされているか	任意		-	30	-	・ガバメントクラウドの利用したシステム構成について効率的かつ実現可能な構成及び内容となっているか。 ・要件をよく分析して、具体的かつ実現可能な提案となっているか。		
		8	非機能要件（ユーザビリティ及びアクセシビリティ以外）に対して優れた提案がなされているか	任意		-	30	-	・次期システムの信頼性、拡張性、上位互換性、継続性を効率的に実現する構成及び内容となっているか。 ・要件をよく分析して、具体的かつ実現可能な提案となっているか。		

提案書の目次			提案要求事項	評価区分	得点配分			評価基準		雛形ページ番号	提案書ページ番号
大項目	中項目	小項目			合計	基礎点	加点	基礎点	加点		
		9	仕様書及び要件定義書に示す情報セキュリティの要件に対して優れた提案がなされているか	任意	750	-	50	-	・想定される脅威及びセキュリティリスクが整理され、その対応方法が具体的に示されているか。 ・公開情報（機密性1情報）の完全性を確保できるよう工夫されているか。 ・機密性2情報の機密性を確保できるよう工夫されているか。 ・要件をよく分析して、具体的かつ実現可能な提案となっているか。		
		10	仕様書及び要件定義書に示す設計・構築に関する要件に対して優れた提案がなされているか	任意		-	150	-	・設計・構築が確実かつ効率的に実施できるよう工夫されているか。 ・ガバメントクラウドを利用した設計・構築の実施方法が工夫されているか。 ・原子力規制庁からの要求等に柔軟に対応できる方法の提案が示されているか。 ・要件をよく分析して、具体的かつ実現可能な提案となっているか。		
		11	仕様書及び要件定義書に示すテストに関する要件に対して優れた提案がなされているか	任意		-	50	-	・限られた工期において、品質を確保しつつ効率的なテスト方法が示されているか。 ・原子力規制庁職員の業務負荷を考慮した効果的な受入テスト支援が提案されているか。 ・要件をよく分析して、具体的かつ実現可能な提案となっているか。		
		12	仕様書及び要件定義書に示す移行に関する要件に対して優れた提案がなされているか	任意		-	100	-	・データを正確かつ効率的に移行するための具体的な方法が提案されているか。その際に、ガバメントクラウドへの移行を踏まえた実施方法となっているか。 ・システム停止期間等の業務影響を考慮した提案となっているか。業務影響を低減するための施策が提案されているか。 ・請負事業者と原子力規制庁職員の役割分担が明確に示されているか。 ・要件をよく分析して、具体的かつ実現可能な提案となっているか。		
		13	仕様書及び要件定義書に示す教育に関する要件に対して優れた提案がなされているか	任意		-	50	-	・マニュアルの作成及び職員研修を、効果的に実施する内容となっているか。 ・要件をよく分析して、具体的かつ実現可能な提案となっているか。		
		14	仕様書及び要件定義書に示す運用・保守に関する要件に対して優れた提案がなされているか	任意		-	100	-	・体制及び原子力規制庁職員との役割分担が明確に示されているか。 ・要件をよく分析して、具体的かつ実現可能な提案となっているか。		
		15	仕様書及び要件定義書に示す引継ぎに関する要件に対して優れた提案がなされているか	任意		-	20	-	要件をよく分析して、具体的かつ実現可能な提案となっているか。		
	2	業務実施方法の妥当性、独創性									
		1	業務実施の手法が明確かつ妥当であるか	必須	50	※	-	業務実施にあたっての手法が明確かつ妥当であるか	-		
		2	業務実施の手法に、事業成果を高めるための工夫があるか	任意		-	50	-	・N-ADRESや緊急情報システムとの連携、ユーザビリティやアクセス状況の課題への対応について、効率的かつ効果的な提案がなされているか ・利用者が負担なく利用でき、業務を効率的に実施できるよう工夫されているか。		
	3	作業計画の妥当性、効率性									
		1	作業日程・手順に無理がなく、目的に沿った実現性があるか	必須	50	※	-	作業日程・手順に無理がなく、目的に沿った実現性があるか	-		
		2	事業成果達成のために、日程、体制及び作業手順等が効率的であるか	任意		-	50	-	・システムの円滑な稼働のために、日程、体制及び作業手順等が効率的であるか。 ・限られた工期において、効率的に業務実施がなされるよう工夫されているか		

Title: 評価項目一覧 - 提案要求事項一覧 -

提案書の目次			提案要求事項	評価区分	得点配分			評価基準		雛形ページ番号	提案書ページ番号
大項目	中項目	小項目			合計	基礎点	加点	基礎点	加点		
2	事業実施体制										
	1	組織の類似調査業務の経験									
		1	過去に類似の業務の実績を有しているか	任意	50	-	50	-	類似の業務の実績を有しているか		
	2	組織の業務実施能力									
		1	事業を実施するために必要な人員が確保されているか	必須	50	※	-	・必要な人員が確保されているか ・クラウド環境にシステムを構築し、運用・保守を行う際に必要な知識・知見を持った人員を体制に組み込んでいるか	-		
		2	規制庁からの要求に迅速に対応できる人員補助体制が組まれているか	任意		-	50	-	規制庁からの要求に迅速に対応できる人員補助体制が組まれているか		
	3	事業遂行のための経営基盤・管理体制・技術基盤									
		1	事業を実施する上で適切な経営基盤・管理体制・技術基盤を有しているか	必須		※	-	適切な経営基盤・管理体制・技術基盤を有しているか	-		
3	事業従事予定者の能力										
	1	事業従事予定者の本業務に関する専門知識・適格性									
		1	本業務についての基本的な知識・知見を有しているか	必須	100	※	-	本業務についての基本的な知識・知見を有しているか	-		
		2	本業務についての高度な知識・幅広い経験を有しているか	任意		-	100	-	本業務についての高度な知識・幅広い経験を有しているか		

提案書の目次			提案要求事項	評価区分	得点配分			評価基準		雛形ページ番号	提案書ページ番号
大項目	中項目	小項目			合計	基礎点	加点	基礎点	加点		
4 組織の取組:ワーク･ライフ･バランス等の推進											
	1 ワーク･ライフ･バランス等の推進に関する認定等取得状況										
		1	女性の職業生活における活躍の推進に関する法律(以下「女性活躍推進法」という。)、次世代育成支援対策推進法(以下「次世代法」という。)、青少年の雇用の促進等に関する法律(以下「若者雇用推進法」という。)に基づく認定等(えるぼし認定等、くるみん認定、プラチナくるみん認定、ユースエール認定)を取得している場合は、認定等の名称及び認定通知書等の写しを提出すること。ただし、提案書提出時点において認定等の期間中であること。	任意	50	-	50	ー	●女性活躍推進法に基づく認定等(プラチナえるぼし･えるぼし認定等) ･プラチナえるぼし(※1) 50点 ･えるぼし3段階目(※2) 40点 ･えるぼし2段階目(※2) 30点 ･えるぼし1段階目(※2) 20点 ･行動計画(※3) 10点 ※1 女性活躍推進法(令和2年6月1日施行)第12条に基づく認定 ※2 女性活躍推進法第9条に基づく認定 なお、労働時間等の働き方に係る基準は満たすことが必要。 ※3 常時雇用する労働者の数が300人以下の事業主に限る(計画期間が満了していない行動計画を策定している場合のみ。) ●次世代法に基づく認定(プラチナくるみん認定･くるみん認定) ･プラチナくるみん認定 40点 ･くるみん認定(新基準※4) 30点 ･くるみん認定(旧基準※5) 20点 ※4 新くるみん認定(改正後認定基準(平成29年4月1日施行)により認定) ※5 旧くるみん認定(改正前認定基準又は改正省令附則第2条第3項の経過措置により認定) ●若者雇用推進法に基づく認定(ユースエール認定) 40点 (注) 複数の認定等に該当する場合は、最も得点が高い区分により加点を行うものとする。		
5 組織の取組:企業等の賃上げの実施											
	1 事業年度(又は暦年)における賃上げ										
		1	賃上げの実施を表明した企業等について ･大企業は、事業年度(又は暦年)において、対前年度比(又は対前年比)で給与等受給者一人当たりの平均受給額を3%以上増加させる旨の、従業員への賃金引上げ計画の表明書(別紙4-1)(表明する意思がある者のみ提出すること)の写しを添付すること。 ･中小企業等は、事業年度(又は暦年)において、対前年度比(対前年比)で給与総額を1．5%以上増加させる旨の、従業員への賃金引上げ計画の表明書(別紙4-2)(表明する意思がある者のみ提出すること)の写しを添付すること。	任意	50	-	50	ー	従業員への賃金引き上げ計画の表明が確認できれば加点(50点)。		
				合計	1200	50	1150	※全ての項目の要求事項を満たした場合、基礎点50点を付与する			

令和７年度から令和11年度原子力規制委員会ホームページシステム更改に係る構築及び運用・保守業務

要件定義書（案）

令和７年１月

目次

1.　本書の目的

1-1. 本書の目的

本書は、「令和７年度から令和11年度原子力規制委員会ホームページシステム更改に係る構築及び運用・保守業務」業務におけるホームページシステム及びシステムを活用した業務に係る機能及び非機能要件、並びに事業者の作業に関する要件を示すものである。

1-2. 更改における考慮事項

ホームページシステムは機密性１情報（※）を保有・管理するものである。本システムによって公開情報を管理することから、情報改ざん等の防止等に対する情報セキュリティ確保に万全を期す必要がある。

※「機密性１情報」を含む情報の格付け・区分については、1.4「用語集」の「情報の格付け・区分」を参照すること。

1-3. 更改スケジュール

ホームページシステムの更改スケジュールは以下の通りである。詳細は「３．システムの機能要件の定義」を参照すること。

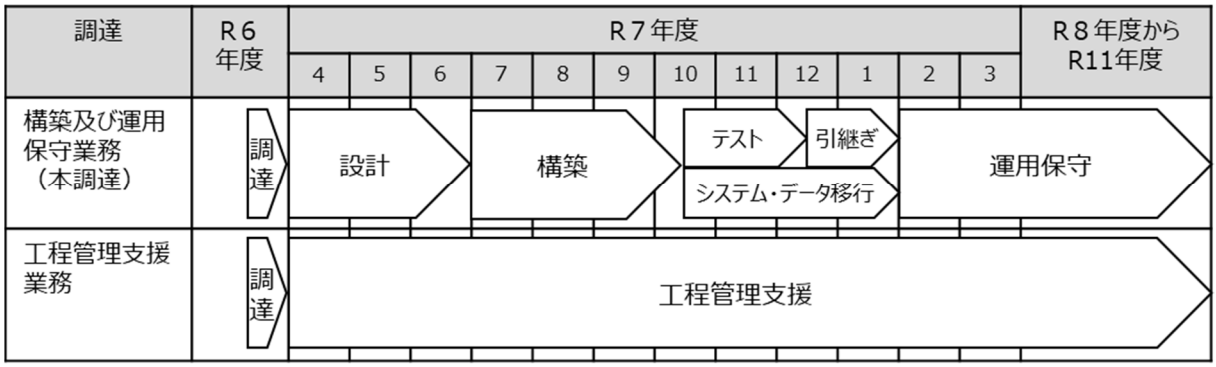


図１　作業スケジュール

1-4. 用語集

本書で使用する用語の定義を以下に示す。

表１　用語集

用語	定義
一般利用者	ホームページシステムを利用する国民を指す。
請負事業者	ホームページシステムの設計・構築及び運用・保守を実施する事業者（本プロジェクトの請負事業者）を指す。
行政 LAN	原子力規制委員会ネットワークシステムを指す。原子力規制庁の職員が業務で利用する、メールやファイルストレージ等を備えた基幹業務システムである。
N-ADRES	原子力規制委員会公開情報管理システムを指す。会議記録等の意思決定に関わる重要な情報をアーカイブしたうえで、一般利用者向けに公開するデジタルアーカイブシステムである。 令和５年度にシステム更改が行われ、従前ではホームページシステム側で管理していたページや資料の多くを本システムに移行している。
広報室	原子力規制庁長官官房総務課広報室を指す。ホームページシステムを所掌する。
原課	原子力規制庁の各課室を指す。
情報の格付け・区分	情報について、機密性、完全性及び可用性の３つの観点で区別した上で、分類の基準に沿って格付けを決定したもの。詳細は「政府機関等の対策基準策定のためのガイドライン」を参照すること。
認証・認可の統合管理基盤	それぞれの情報システムにおいて行っている識別コード、主体認証情報、主体の属性等の管理やそれらを使用した主体認証機能及びアクセス制御機能を一元的に実施することを実現するためのものを指す。

2. 業務要件の定義

2-1. 業務実施手順に関する事項

ホームページシステムの対象となる業務は以下のとおりである。なお、CMSについては、基本的に現行CMS製品（ALAYA）を継続して利用することを想定している。

表２　業務の概要

No.	業務	業務の概要
1	管理	• CMS で利用するメニュー、マニュアル等ポータル画面を通じて表示する • CMS 上のメニュー、お知らせ、メンテナンス情報、FAQ、マニュアル等の掲載内容を変更する • ホームページシステムに登録されたページのステータスや作成者・承認者を表示し確認する
2	ページの作成・公開・削除	• 庁外へ公開する資料を作成し、CMS へアップロードする • CMS にアップロードされた資料の承認又は差し戻しを行う • 緊急時ページを作成し、公開する • CMS 上のページが公開可能な状態であるか、内容をチェックする • CMS からページを削除する（一括削除含む） • CMS から削除する予定のページの承認又は差し戻しを行う
3	ページの属性の変更	• CMS に登録済みのページに対して属性を編集する • CMS に登録されたページの属性を確認し、承認又は差し戻しを行う
4	ページの閲覧	• Web ブラウザ上で公開済みページ及び添付ファイル（ドキュメント、動画、画像等）を閲覧する • 添付ファイルをダウンロードする
5	システム管理	• 人事異動、入庁、退庁等に基づくアカウントの発行/削除/無効化を行う • ヘルプデスク窓口として、職員からの問い合わせに対応する • 各種相談や調査依頼を受けた場合は、助言・参考資料提出等の支援を実施する • インシデント発生時には、インシデント発生時保守作業（原因調査、応急措置、報告等）を実施する • 障害発生時には、障害発生時保守作業（原因調査、応急措置、報告等）を実施する。 • ジョブの実行状況を確認する • 必要に応じてジョブの登録・変更・削除を実施する
6	セキュリティ管理	• アカウントおよびそのアクセス権を管理する • 各アカウントの証跡を記録し、管理する • 共有アカウントでの運用を行う場合は、パスワードの定期的な変更、行政 LAN からの接続のみ許可する等を例とする、セキュリティ対策を講じること • 個別アカウントでの運用を行う場合は、同一主体による複数アクセスを制限する • 利用時間や利用時間帯によるアクセス制御を行う

		・ ファイヤーウォール/WAF の管理（ルール変更・ポリシー見直し等）を実施する ・ IP アドレス等で接続を制限する ・ システムの構成を管理する ・ 外部又は内部者による不審な行動を検知した場合にアラートを発報する ・ システム管理者による操作のログを確認する ・ 通信の暗号化を保持するため、ライセンス及び TSL 証明書を更新する ・ ホームページシステムに対する通信を暗号化する機能を備えること
7	アクセス分析	・ 公開済みページへのアクセス元、アクセス数等を分析する ・ CMS へのアクセス元、アクセス数等を分析する
8	移行関連	・ 現行システムからデータ移行を行う ・ 次期システムへ移行する際に、データ移行の支援を行う ・ 次期システムへ移行する際に、データ消去を行う

2-2. 規模に関する事項

（1） システムの利用者数

・ 年間閲覧者数

表３ 年間閲覧者数

対象	年間閲覧者数(2023 年)	備考
閲覧者（国内・海外）	752,951	アクティブユーザー数合計

・ 作業者数

表４ 作業者数

対象	アカウント数(2023 年)	備考
ALAYA ユーザー（編集）	36	編集・承認作業を行う課室ごとにアカウントを割り当て、共有アカウントでの運用を想定。
ALAYA ユーザー（承認）	35	
ALAYA ユーザー（その他）	9	

（2） 単位（年、月、日、時間等）当たりの処理件数

・ 年間閲覧件数の想定

表５ 年間閲覧件数の想定

対象	閲覧件数（2023 年）	備考
トップページ	1,366,708	
それ以外のページ	1,410,585	

・ 年間処理件数

表６ 年間処理件数

対象	年間処理件数	備考
ＣＭＳ登録	40,749 頁	
N-ADRES 参照	357 頁	令和 6 年 8 月 19 日時点

・ アクセス数

表７　アクセス数

	定義	処理件数（セッション数/日）
平常時	通常の運用状態	8,223
ピーク時	事故や重要なプレスリリースなど緊急の告知があり、アクセスが集中する状態。 （ピーク特定：６～７月に年間の約 19%が集中）	9,272

（３）　情報・データ量

表８　情報・データ量

格納場所	項目	容量等	備考
外部公開 Web サーバ	データ使用量（GB）	853	2024 年３月の N-ADRES 更改の際に、ホームページシステムで管理していたページや資料等を N-ADRES に移行したため、移行対象データの総量が大幅に減少する見込み。（ページ数については現行から 1/9 程度に減少する想定）
	ページ数	92,231	
	ファイル数	201,657	
CMS（ALAYA）	ページ数	92,413	
	ファイル数	381,643	
	テンプレート	61	左記のうち、約 40 のテンプレートを次期システムに移行予定。

3. システムの機能要件の定義

3-1. 機能に関する事項

ホームページシステムにおいて備える機能は別紙１「機能一覧」を参照すること。当該資料の各機能は、設計工程において具体化されるものとする。また、利便性向上等に有用な情報があれば提案の上で機能及び画面の設計に含めることとする。

3-2. 画面に関する事項

ホームページシステムにおいて下記の基本要件を満たした上で、画面設計について提案すること。

（１） 全体

- 色彩、レイアウト、フォント及びその他の視覚的要素について提案とすること。
- ユーザビリティ、アクセシビリティ、ブランドイメージ及び最新のデザイン基準に基づいて、最適なデザインを提案すること。
- 一般利用者及び原子力規制庁職員の利便性を考慮し、必要な画面を追加すること。例えば、登録画面を具備する場合、原課に入力内容を確認させる画面及び登録結果を表示する画面も合わせて作成するなど、請負事業者及び原子力規制庁職員が効率的かつ誤りなく利用できるよう、必要な画面及び画面構成を検討すること。
- 画面設計については、設計工程において原子力規制庁担当官（以下、「担当官」という。）の承認を得ること

（２） トップページ

- トップページの情報をコンパクトにまとめ、視認性・利便性の向上を図ること。
- ファーストレビューに表示される情報を増やし、閲覧者が次のページ遷移を行いやすいように工夫すること。
- 類似コンテンツを集約する等、利便性を高めるよう設計すること。

（３） 外部連携

- N-ADRESから取得した情報を基に、会合開催予定や事故・トラブル情報をトップページ内に表示すること。（連携方法の詳細は別紙２「外部インターフェース一覧」を参照）
- 緊急情報・情報提供ページから取得した情報を基に、新着情報がある場合は自動で展開し、新着情報がない場合は自動で閉じる表示とすること。（連携方法の詳細は別紙２「外部インターフェース一覧」を参照）

（４） 目的別メニュー・グローバルナビゲーション

- 現行の目的別メニュー及びグローバルナビゲーションの項目が類似しており、閲覧者の目的に沿った効果的な遷移を提供していないため、全面的に新たな目的別メニュー及びグローバルナビゲーションの設計を提案すること。
- 新しい目的別メニュー及びグローバルナビゲーションはそれぞれ異なる分類を採用し、閲覧者の目的やニーズを考慮したカテゴリーとすること。

（５）　全ページ共通パーツ

- ヘッダーやフッター等の全ページ共通パーツについては、各ページからインクルードして表示させる等、内容に変更があった際の修正対象を最小限に留めるかたちで構成すること。

3-3. 情報・データに関する事項

（１）　情報の格付け・区分（機密性）について

ホームページシステムにおいて登録・公開する情報は、原則として情報の格付の区分が機密性１情報に該当するものを扱う。一方で、内部管理のために保持するデータ（例えば、当該情報を登録した職員名等）は、機密性２情報にあたる。機密性２情報が公表されないよう、制御すること。

（２）　登録するファイル種別

ホームページシステムにおいて登録・公開するファイルの種別は、別紙１「機能一覧」を参照すること。なお、詳細なファイルの種別や制限については、設計工程において担当官と協議し、決定されるものとする。

3-4. 外部インターフェースに関する事項

外部インターフェースについては別紙２「外部インターフェース一覧」を参照すること。なお、ホームページシステムの外部インターフェースに関する基本要件を以下に示す。ユーザーの主体認証に行政LANのAzure Active Directory 認証を利用する場合についても、下記の基本要件を満たすこと。なお、別紙２「外部インターフェース一覧」に記載の機能を用いたN-ADRES及び緊急情報・情報提供ホームページとの連携を実装すること。

- 各外部インターフェースは、N-ADRES運用保守事業者及び緊急情報・情報提供ホームページの運用保守事業者と連携し、SRU-API等のAPIを用いた連携等、オープンな方式を用いて実現すること。なお、詳細な要件については各システムの運用保守事業者を含めた関係者と協議を行ったうえで原子力規制庁が確定する。（N-ADRESについては、N-ADRES側に新規登録された資料の連携を、緊急情報・情報提供ホームページについては、当該システムの最新情報の連携をそれぞれ想定している）
- 連携先システムの停止時等を想定し、ホームページシステム側でエラー時の制御を行うこと。
- 万が一他システムに影響を与えた場合、請負事業者の責任と負担においてホームページシステムの対処を行い、影響を取り除くこと。

4. システムの非機能要件の定義

非機能要件の定義について、以下に示す。

4-1. ユーザビリティ及びアクセシビリティに関する事項

（1） システムの利用者の種類、特性

システムの利用者の種類、特性を以下に示す。

表 9 システムの利用者の概要

No.	利用者区分	利用者の種類	特性
1	一般利用者（国民）	当該システム利用者	・インターネット経由で本システムにアクセスする。 ・IT リテラシーが高くない利用者も存在する。
2	一般利用者（職員）	当該システムを利用して資料を閲覧する職員	・IT リテラシーが高くない職員も存在する。
3	システム利用者（職員/原課）	当該システムの公開資料の管理を行う原課の職員	・IT リテラシーが高くない職員も存在する。
4	システム利用者（職員/広報）	当該システムの公開資料の管理を行う広報室の職員	―
5	請負事業者	当該システムの運用保守を行う事業者	・インターネット経由で本システムにアクセスする。

（2） ユーザビリティ

ユーザビリティ要件を以下に示す。本要件の詳細については、請負事業者決定後に原子力規制庁と協議の上、確定すること。ユーザビリティ要件は、一般利用者（国民）、一般利用者（職員）に対する画面に定義する。

表10 ユーザビリティ要件

No.	ユーザビリティ分類	ユーザビリティ要件
1	画面の構成	利用者が想定しやすい手順（画面遷移・タブ移動順）にすること
2		無駄な情報、デザイン及び機能を排し、利用者が必要な操作を直感的に想起しやすい画面構成とすること
3		十分な視認性のあるフォント及び文字サイズを用いること
4	操作のしやすさ、分かりやすさ	無駄な手順を省き、最小限の操作、入力等で利用者が作業できるようにすること
5		画面上で入出力項目のコピー及び貼付けができること
6		必要に応じて、ショートカット又は代替入力方法が用意されること（例えば、片手だけで主要な操作が完了することが求められたり、マウスを利用することが困難であったりする場合が考えられる）

No.	ユーザビリティ分類	ユーザビリティ要件
7	指示及び状態の分かりやすさ	操作の指示、説明、メニュー等には、利用者が正確にその内容を理解できる用語を使用すること
8		必須入力項目と任意入力項目の表示方法を変えるなど各項目の重要度を利用者が認識できるようにすること
9		必要に応じて確認画面を用意し、利用者が修正・再入力をできるようにすること
10		システムが処理を行っている間、その処理内容を利用者が直ちに分かるようにすること
11	エラーの防止と処理	利用者が操作、入力等を間違えないようなデザイン及び案内を提供すること
12		入力内容の形式に問題がある項目については、それを強調表示する等、利用者がその都度その該当項目を容易に見つけられるようにすること
13		認証情報の更新等については、確認画面等を設け、利用者が行った操作又は入力の取消し、修正等が容易にできるようにすること
14		重要な処理については事前に注意表示を行い、利用者の確認を促すこと
15		エラーが発生したときは、利用者が容易に問題を解決できるよう、エラーメッセージ、修正方法等について、分かりやすい情報提供をすること
16	習得性	システムの各機能を利用する方法を利用者が容易に習得できるようにすること
17	効率性	業務効率性を考慮し、最適なレイアウトを提案すること。職員や事業者の特性を踏まえた上で極力平易に使えるよう手立てを講じること
18	ヘルプ	利用者が必要とする際に、ヘルプ情報やマニュアル等を参照できるようにすること
19		ヘルプ情報やマニュアル等は、職員や事業者の特性を踏まえ、平易に理解できるよう配慮すること

（3）　アクセシビリティ要件

アクセシビリティ要件を以下に示す。アクセシビリティ要件は、一般利用者に対する画面に定義する。

表11 アクセシビリティ要件

No.	アクセシビリティ分類	アクセシビリティ要件
1	基準への準拠	・ JIS X 8341-3:2016「高齢者・障害者等配慮設計指針―情報通信における機器、ソフトウェア及びサービス―第3部：ウェブコンテンツ」適合レベルAAに準拠していること。 ・ 年に数回程度行われる準拠性検査の結果に基づく修正対応を検討すること。 ・ ホームページシステムの更改前に準拠性を再検査すること。
2	日本語対応	システムの利用者が、すべて日本語で利用できること。 ただし、利用運用上において実質的に支障がないと原子力規制庁が認めた部分については、この限りではない。

4-2. システム方式に関する事項

（1） クラウドサービスの選定

クラウドサービスで構築すること。クラウドサービスは、以下の事項を遵守して選定すること。

- 政府が構築した「ガバメントクラウド」にて、WEBサービスを構築及び運用することとする。
- クラウドサービスは基本的にはAmazon Web Services（以下、AWSという）の利用を想定しているものの、その他のサービスを利用する場合は、「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」に登録されているクラウドサービスを選定すること。
- 大規模災害の発生等を踏まえ、冗長構成をとること。
- ガバメントクラウドの利用において、本書に定める信頼性指標及びセキュリティ対策を遵守すること。

（2） システムの全体構成

ホームページシステムの全体構成は次の図のとおりである。なお、既知の脆弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としないこと。

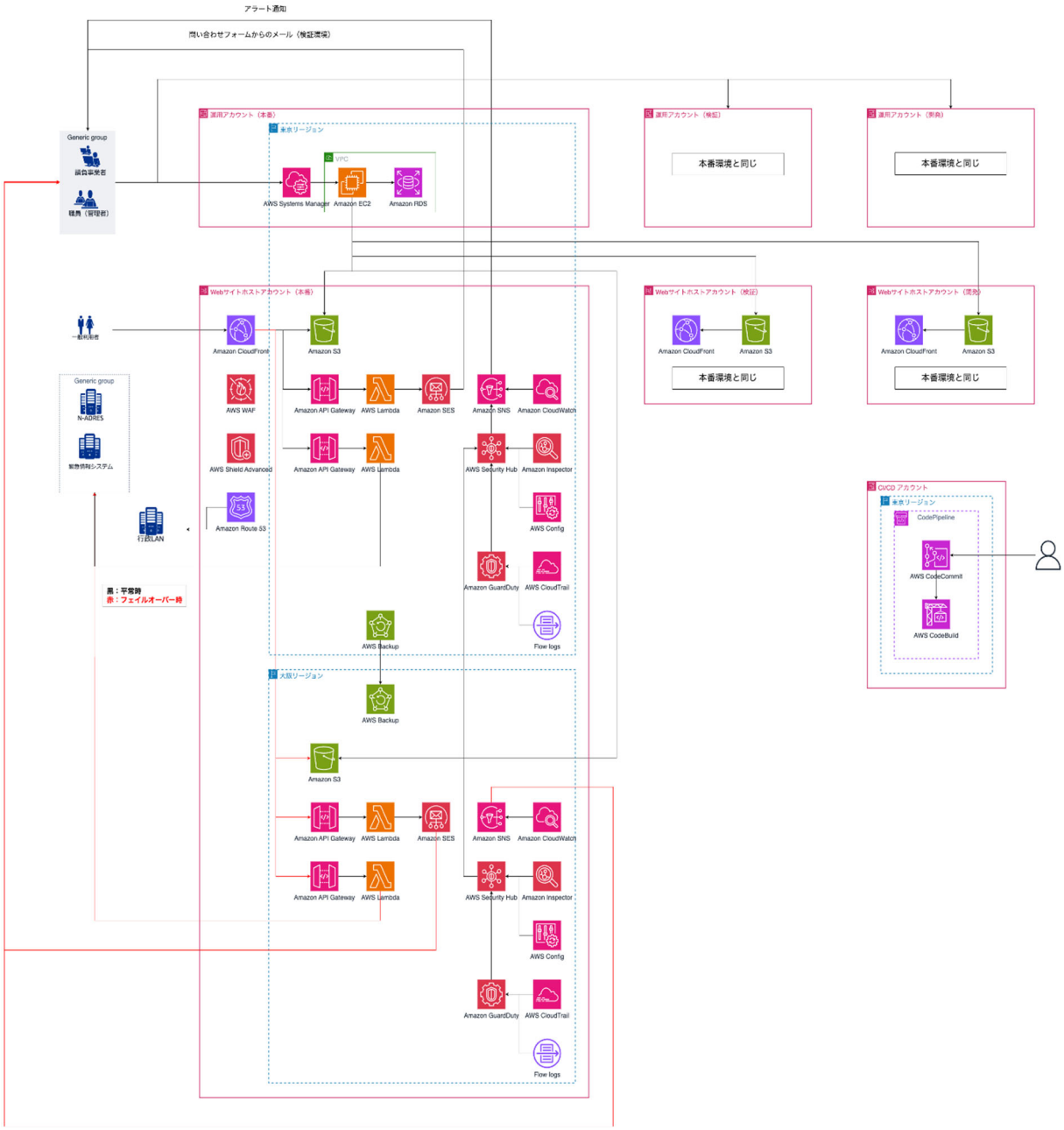


図２　システムの概要

（３）　情報・データに関する事項

ホームページシステムにおいて必要となる情報・データについては、担当官の許可を受けた上で現行システムの基本設計書・詳細設計書を参照すること。

4-3.　規模に関する事項

（１）　機器数及び設置場所

機器類の数量及び設置場所を以下に示す。（メインサイト、バックアップサイトどちらも下記の記載に従うこと。）

表12 機器及び設置場所

No.	機器の区分	機器の用途	機器数	設置場所	補足
1	ガバメントクラウド	-	1式	ガバメントクラウドを利用すること。	-

（2） 利用者数

「2-2. 規模に関する事項 （1）システムの利用者数」を参照のこと。

（3） 処理件数

「2-2. 規模に関する事項 （2）単位（年、月、日、時間等）当たりの処理件数」を参照のこと。

（4） データ量

「2-2. 規模に関する事項 （3）情報・データ量」を参照のこと。

4-4. 性能に関する事項

（1） オンラインレスポンス

平常時およびピーク時における、オンラインレスポンス目標値（返答時間）及びオンラインレスポンス順守率を以下に示す。なお、オンラインレスポンス目標値については、クラウドサービス内の処理時間とする。

表13 オンラインレスポンスの概要

時間帯	処理内容	目標値	順守率
平常時	静的サイト閲覧	1.0秒以内	90%以上
	N-ADRES参照サイト閲覧	1.5秒以内	90%以上
	検索	1.5秒以内	90%以上
ピーク時	静的サイト閲覧	2.0秒以内	80%以上
	N-ADRES参照サイト閲覧	2.5秒以内	80%以上
	検索	2.5秒以内	80%以上

目標値は、国内からアクセスがあった場合のオンラインレスポンスタイムを対象とする。また、上記に示した応答時間について測定を可能とすること。また、「目標値」及び「達成率」の達成状況を測定し、把握及び集計するための具体的な方法を提案すること。
なお、マスタメンテナンス等のリアルタイム性が要求されない処理については除くこととする。

（2） バッチレスポンス（ターンアラウンドタイム）

ホームページシステムのバッチレスポンス（ターンアラウンドタイム）に係る要件を以下に示す。

・システム利用者の要求に基づき実行されるバッチ処理は、目標値を10分以内とすること。

（3） オンラインスループット

ホームページシステムのオンラインスループットに関わる要件を以下に示す。

・オンラインスループットの目標値として、APIトランザクション30件/秒とすること。

4-5. 信頼性に関する要件

（1） 可用性要件

ホームページシステムにおける可用性に係る指標とその目標値を以下に示す。停止時間とは、障害発生時の復旧時間等、計画外の停止時間を指す。以下の時間は稼働率の算出に含めないこととする。

- 計画的な作業等による計画停止時間
- 冗長構成のサーバのうち、片系のみが停止している時間
- メインサイト正常運転時に、バックアップサイトにて発生した障害

表14 可用性要件

No.	対象	目標稼働率	計測方法	集計期間
1	CMS サービス	99.0%	（稼働予定時間－停止時間）／稼働予定時間×100	1回／月
2	Web サービス	99.9%		

なお、バックアップサイトにおける可用性に係る指標とその目標値、停止時間の定義はメインサイトと同様とする。可用性に係る目標値を達成するため、以下のような対策を行うこと。

- システム障害によりサービス停止が予見される機器又は機能について、冗長化を図る、機器単体の稼働率が高い機器を採用する等を実施し、信頼性を確保すること。
- クラウドサービスを利用することとし、使用するサービスに障害が発生した場合に復旧する方式を示すこと。

また、対策の具体的な内容を提案すること。提案には、提案する対策によって求める可用性が達成可能であることを、最低限以下に示す根拠を含めて詳細に示すこと。

- 提案する機器又は機能のMTBF等。稼働率の実績値を用いることが望ましい。
- 想定する障害に対する検知時間。
- 想定する障害に対する回復時間。運用チーム等による判断、作業を要する場合はこれに掛かる時間も計上すること。また、フェイルオーバー、ライブマイグレーション、リブート等を要する場合は実績値をもとに掛かる時間を計上すること。
- 想定する障害に対する回復時間。運用チーム等による判断、作業を要する場合はこれに掛かる時間も計上すること。また、フェイルオーバー、ライブマイグレーション、リブート等を要する場合は実績値をもとに掛かる時間を計上すること。
- 運用体制。運用の人員割り当て等を具体的に示すこと。

（2）　完全性要件

ホームページシステムにおける完全性に関する要件を以下に示す。

- 誤操作等により重要なデータを安易に消去されることのないよう、必要な措置等講じること。
- データの整合性を確保するため、更新処理においては十分なデータチェックを行うこと。また、エラー等により処理が中断された場合には、データを処理実行前の状態に戻すこと。
- Webサイトが意図しない改ざんから保護されるよう改ざん検知の措置を講じること。また、可能な限りクラウドサービスが提供する改竄検知などの機能を利用すること。

4-6.　拡張性に関する要件

（1）　性能の拡張性

法制度改正によるスコープ拡張等、設計開発時の想定範囲外となる事態が発生した場合を想定し、クラウドサービスにおけるスケールアウト、スケールアップが容易に可能な構成とすること。また、実現するために講じる対策の具体的な内容を提案すること。

（2）　機能の拡張性

利用者ニーズ及び環境の変化等に最小コストで対応可能とするため、ホームページシステムはシステム構成等に極力変更を加えずに機能追加可能なシステム構成とすること。機能拡張が発生した場合は、別途、担当官と協議の上で対応を検討すること。

4-7.　上位互換性に関する要件

- ユーザー端末のOS等のバージョンアップに備え、OS等の特定バージョンに依存する機能は、その利用を最低限とするとともに、設計で明示すること。
- 特定のWebブラウザに依存する機能が判明している場合は、その利用を最低限とすること。また、主な利用環境として想定するWebブラウザを一定の範囲に限る場合でも、対象ブラウザのバージョンアップに備え、対象ブラウザの特定バージョンに依存する機能が判明している場合は、その利用を最低限とすること。
- Webブラウザ及び実行環境等のバージョンアップの際、必要な調査及び作業を実施することで、バージョンアップに対応可能なシステムとすること。
- 契約期間中にホームページシステムの稼働環境として導入しているソフトウェア、ハードウェアのバージョンアップが発生した場合は、追加費用なくバージョンアップすること。
- 次期バージョンで互換性を持たないことが発表されているソフトウェアはホームページシステムに導入しないこと。

4-8. 中立性に関する要件

- 提供するクラウドサービスはガバメントクラウドとし、特定の事業者に依存することなく、本業務の落札者以外の事業者に引継ぎ、運用・保守ができること。
- 提供するハードウェア、ソフトウェア等は、特定ベンダの技術・サービスに依存しない、オープンな技術仕様に基づくこと。
- 提供する構成要素は、標準化団体（ISO、IETF、IEEE、ITU、JISC 等）が規定又は推奨する各種業界標準に準拠すること。
- 次期システム更改の際に、移行の妨げや特定の装置や情報システムに依存することを防止するため、原則として情報システム内のデータ形式はXML、CSV等の標準的な形式で取り出すことができるものとすること。

4-9. 継続性に関する要件

（1） 継続性に係る目標値

(ア)目標復旧時間（メインサイト・障害発生時）

メインサイト稼働中に障害が発生した場合を前提とし、障害発生時の継続性に係る指標とその目標値を以下に示す。なお、「目標値（性能：50%）」として示す時間は、サービス停止時間及びサービスを提供しているが性能が「4-4.性能に関する事項」で要求する性能の50%未満である時間の合計がこの時間を下回ることを要求するものである。「目標値（性能：100%）」として示す時間は、サービス停止時間及びサービスを提供しているが性能が「4-4.性能に関する事項」で要求する性能を下回る時間の合計がこの時間を下回ることを要求するものである。例えば同性能のサーバ2台による両現用構成で「4-4.性能に関する事項」で要求する性能を満たしている場合、その内の1台が故障した場合の性能は50%とみなし、この状態で稼働している時間は「目標値（性能：50%）」に算入しないが、「目標値（性能：100%）」には算入する。

表15 継続性に係る目標値

No.	指標	目標値（性能：50%）	目標値（性能：100%）	計測方法	集計期間
1	平均復旧時間	1時間	24時間以内（1営業日以内に復旧）	ダウンタイム／停止回数	1回／年

(イ)目標復旧時間（メインサイト・大規模災害発生時）

メインサイト稼働中に大規模災害が発生し、メインサイトが被災した場合を前提とする。大規模災害発生時の継続性に係る指標とその目標値を以下に示す。

表16 メインサイトの目標復旧時間

No.	指標名	目標値
1	バックアップサイトへの切り替え時間	1時間

(ウ)目標復旧時間（バックアップサイト・障害発生時）

バックアップサイト稼働中に障害が発生した場合を前提とする。バックアップサイト稼働中に障害が発生した場合の継続性に係る指標とその目標値を以下に示す。

表17 バックアップサイト稼働中の目標復旧時間

No.	指標名	目標値（性能：50%）	目標値（性能：100%）
1	サービスダウン発生時の目標復旧時間	1時間	24時間

(エ)目標復旧時点

目標復旧時点は以下のとおりとする。目標復旧時点（大規模災害発生時）を達成することを前提にメインセンタとバックアップセンタのデータ同期を行うこと。目標復旧時点（大規模災害発生時）は、大規模災害によりメインセンタの機能が停止した時点を起点とする。なお、クラウドサービス上にバックアップデータを配置し、そのデー

タを用いてバックアップサイトへの切り替えを実施してもよい。

表18 目標復旧時点

No.	指標	目標復旧時点 (障害発生時)	目標復旧時点 (大規模災害発生時)	対象
1	目標復旧時点	定義なし（単一障害時にデータのリストアが発生する障害は考えにくいため)	障害発生の 24 時間前まで	サービス提供に係る全ての機能

(オ)バックアップ保管世代数

障害からの復旧以外にも、セキュリティ侵害を受けた場合においてバックアップからの復旧を行う場合が想定される。バックアップの保管世代数が少ない場合は、存在するバックアップデータが既にセキュリティ侵害を受けている可能性が高まることから、全てのバックアップデータについて最低3世代を保管すること。

（2） 継続性に係る対策

継続性に関する目標値を達成するため具体的な内容を提案するとともに、提案する対策で、（1）継続性に係る目標値に示す継続性が達成可能であることを示すこと。提案には、提案する対策によって求める継続性が達成可能であることを、最低限以下に示す根拠を含めて詳細に示すこと。

- 提案するクラウドサービスの稼働にかかる実績値を用いることが望ましい。
- 想定する障害に対する検知時間。
- 想定する障害に対する回復時間。運用チーム等による判断、作業を要する場合はこれに掛かる時間も計上すること。また、サーバのリブート等を要する場合は実績値をもとに掛かる時間を計上すること。
- 運用体制。運用の人員割り当て等を具体的に示すこと。

（3） その他の継続性に関する考慮事項

- 災害や事故等が発生した場合において、本業務の継続性を確保するために必要な要件やそのための方策について検討の上、担当官と協議すること。
- 大規模な災害が発生し、原子力規制庁が被災した場合においても、在宅等で業務を継続できるようにすること。なお、システムの一時停止は許容するものとし、復旧作業に時間を要する場合は担当官と協議すること。また、保守契約の範囲を超える被災時の復旧作業については、本調達の範囲には含めないこととする。

4-10. 情報セキュリティに関する要件

ホームページシステムに求める情報セキュリティに関する要件を以下に示す。

表19 情報セキュリティに関する要件

No	情報セキュリティ対策	対策に関わる要件
1	不正プログラム対策	• 不正プログラムによる情報漏えい等の被害を防止するため、システムの導入範囲で不正プログラムの感染防止の対策を行うこと。なお、EDR ソフトウェア等を利用し、サーバ装置（エンドポイント）等の活動を監視し、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についても検討すること。 • 新たに発見されるマルウェアに対応するため、機能の更新が可能な製品・サービスを導入すること。また、定期的に更新すること。
2	脆弱性対策	• 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。 • セキュリティパッチ適用範囲の機器・サービスやソフトウェアについて、パッチの公開について監視すること。 • セキュリティパッチが公開された場合は、公開された脆弱性のリスクの分析を行い、適用の実施可否を判断すること。 • C&C サーバ等への不正な通信の監視及び遮断、他のセグメントと分離した運用管理セグメントへのシステム管理用の専用端末の接続、認証サーバに管理者権限でログインできる端末のシステム管理用の専用端末のみに制限等の標的型攻撃に対する内部対策及び出口対策を実施すること。
3	証跡管理	• 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、5年間保管すること。 • 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。 • ログの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こと。 • システム管理者による不正を検知するため、管理者権限による操作のログを担当官が閲覧できるようにすること。 • 不正利用防止のための職務分掌の徹底及び事後追跡のためのログの取得・管理・分析体制を整備すること。
4	セキュリティ監視	• 外部からの侵入を防止するため、不正侵入の検知を行うこと。 • 不正監視の確認間隔は、不正行為に迅速に対処する必要性から、常時監視とすること。 • 操作ログを分析し、外部又は内部者による不審な行動を検知した場合にアラートを発報すること。なお、リアルタイムでのログの調査・分析を行うための機能の導入についても検討すること。 • 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。 • 不正プログラム感染や踏み台に利用されること等による規制庁外への不正な通信を監視すること。 • ネットワークセグメント間の通信を監視すること。 • 脆弱性に係る注意喚起の監視と対処を行うこと。

5	主体認証	• 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、システムにアクセスする主体のうち一般利用者を除くシステム利用者の認証を行う機能として、二要素認証方式を採用すること。 • パスワードに対し、桁数や文字種など、厳格なパスワードポリシーによる管理機能を備えること。（３種類以上の文字種かつ 12 桁以上のパスワード設定を強制）なお、管理者権限を保有する者に対してはより強固な認証を行うこと。
6	権限管理	• 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。 • 必要最小限のプログラムの実行、コマンドの操作、及びファイルや情報へのアクセスのみを許可するよう、アクセス権の管理を業務等に応じて行うこと。 • アカウントを制御し、各アカウントの証跡の記録と管理をすること。 • 管理者権限の悪用による不正行為を防止するため、管理者権限を適切に保護すること。 • 管理者及び利用者がクラウドサービスに多大な影響を与える誤操作を抑制する対策を講じること。 • クラウドサービスのリソース（ネットワーク、仮想マシン等）の設定を変更するユーティリティプログラムを使用する利用者を制限すること
7	暗号化及び電子署名	• データベース上に保存された要機密情報は暗号化すること。暗号化の際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」に掲載されている暗号化方式を採用すること。 • ホームページシステムに対する通信を暗号化する機能を備えること。 • 暗号化に用いる鍵の保管場所は暗号化した情報とは別の場所で保管すること。 • 暗号鍵の生成から廃棄に至るまで適切に管理すること • TLSインスペクションの機能の実装を検討すること。 • 業務に必要な通信だけを許可し、許可していない不正な通信の発生を防止すること。 • 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。 • ホームページ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。
8	構成管理	• 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）を一元管理すること。 • 情報システムの構成に変更が生じた場合は、最新の構成情報及び稼働状況に更新すること。 • サーバ装置に接続を認めた機器等を定め、接続を認めた機器等以外は接続させないこと。 • 不要なポート開放を行わないこと。 • 不正の防止及び発生時の影響範囲を限定するため、Web サービス等外部との通信を行うサービスと、CMS サービス等が稼働する内部のサービスをクラウドのネットワーク環境上で分離すること。
9	プライバシー保護	• 個人情報の保有期間を本人に明示すること。明示方法としては、ホームページシステムの登録画面上に掲載する、書面で申請する場合は、登録用紙に保有期間を記載する等適切な方法をとること。データの消去契機

		については、死亡届の受理ではなく、保有期間が経過したデータから消去する。

4-11. システム稼動環境に関する要件

（1） 稼働環境

ホームページシステムにおいて、用意すべきシステム環境を以下に示す。

表20 稼働環境の概要

No.	環境	利用用途	備考
1	本番環境	• システム公開用 • システム開発時の連携テスト及び全体リハーサルの実施	• 本番環境と開発／検証環境における各サーバは、それぞれ独立して構築すること。
2	開発／検証環境	• 開発 • 単体テスト及び結合テスト、総合テスト、受入テストの実施 • 業務アプリケーション、バージョンアップ、設定変更の更新等によるシステム影響の確認 • セキュリティパッチの適用に関するシステム影響の確認 • 運用ツール、自動化ツール等、ホームページシステムに導入しているツール類のバージョンアップや設定変更によりシステム影響の確認 • ミドルウェア等のバージョンアップによるシステム影響の確認 • N-ADRES との連携テストの再現 • 機能追加時の システム利用者によるユーザー検証	• 開発／検証環境は、クラウドサービスの利用を想定している。 • 開発／検証環境の利用に伴い、本番環境の性能、機能、データ管理に影響を与えないこと。 • 開発／検証環境について、利用用途を満たせれば、可用性や性能等の要件を満たさなくともよい。

（2） ハードウェア構成

ホームページシステムの構成図は「4-2.（2） システムの全体構成」を参照のこと。ホームページシステムの機能及び非機能の要件を満たすことが可能となる構成を提案すること。また、クラウドサービスを利用することとし、上記に加え仮想サーバ、仮想ストレージ等の機能についての構成を示すこと。

（3） ソフトウェア要件

一般利用者の提供サイトに対する端末のソフトウェア構成はHTML5/CSS3に対応したWebブラウザとする(OS及びWebブラウザの種類とバージョンは任意)。ただし、本調達の請負事業者がテストで使用する環境ではOSとWebブラウザをそれぞれ下記の表のように限定する。なお、Webブラウザのバージョンは試験実施時点の最新バージョンとし、職員が利用する業務画面のWebブラウザは、Edge、Chrome、Firefoxとする。

表21 ソフトウェア要件

No.	OSの種類	OSのバージョン	Webブラウザの種類
1	Windows	10、11	Microsoft Edge Google Chrome Mozilla Firefox
2	macOS	15 (Sequoia)	Safari Google Chrome
3	Android	15	Google Chrome
4	iOS	18	Safari Google Chrome

また、CMSサービスに関しては基本的には現行CMS製品（ALAYA）を次期システムにおいても利用想定とし、費用対効果を考慮の上、最適なライセンス形態にて導入すること。なお、当該ライセンスは契約終了後当庁に帰属するものとする。

（4）　ネットワーク要件

(ア)ネットワーク構成図

ホームページシステム全体のネットワーク構成図は「4-2.（2）システムの全体構成（2）」を参照のこと。ホームページシステムの機能及び非機能の要件を満たすことが可能となる構成を提案すること。なお、構成図は以下のネットワーク要件を満たすものとすること。

(イ)ネットワーク要件

ホームページシステムに係るネットワークの要件は下記のとおりである。

- 職員が利用する端末からシステムにアクセスできるよう、HTTPSによる通信を可能とすること。
- ホームページシステムの機能及び非機能の要件を満たすことが可能となる機器を提案すること。また、クラウドサービスを利用することとし、仮想ネットワーク機器等についての機能を示すこと。
  - ① 利用プロトコル
    使用するプロトコルについては標準プロトコル、又は業界標準のプロトコルの利用を基本とし、物理層・データリンク層についてはIEEE802.3及びその拡張版を採用し、ネットワーク層、トランスポート層についてはTCP/IPを採用すること。
  - ② セグメント分割
    外部との接続に関するセキュリティ対策を踏まえ、DMZと内部のセグメントを分ける等のセグメント分割を検討すること。
  - ③ IPv6対応
    - N-ADRESへのアクセスについては、IPv6でアクセス可能であること。
    - IPv6によるN-ADRESへのアクセスにおいて、送信元IPv6アドレスも含めた

アクセスログの確認が行えること。

- IPv6による通信に対してIPv4による通信と同等のセキュリティが確保されていることを確認すること。
- IPv6アドレスの割り当てが不要な機器又は機能に対しては、IPv6アドレスの割り当てを行わないこと。
- IPv6対応しない機器又は機能については、意図しないIPv6通信を抑止又は遮断するための措置を講ずること。

（ウ）ドメインの要件

現行システムで使用している「nra.go.jp」に使用すること。DNSなど、行政LANが所管する機器等の設定変更内容を取りまとめ、原子力規制庁と協議すること。

5. 事業者の作業に関する事項

5-1. 情報セキュリティに関する要件

（1） 情報セキュリティ要件

請負事業者は、下記の点に留意して情報セキュリティを確保するものとする。

- 本システムの開発工程において、原子力規制庁の意図しない変更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、当該品質保証体制が書類等で確認できること。
- 本システムに対し、原子力規制庁の意図しない変更が行われるなどの不正が見つかった場合に、追跡調査や立入検査等、原子力規制庁と請負先が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。
- 請負事業者の資本関係、役員等の情報、作業要員の氏名、所属、実績、国籍等の情報提供に対応すること。なお、契約締結後速やかに業務従事者名簿等を提出し、従事者が変更になる都度、当該名簿等を更新すること。
- 請負事業者の情報セキュリティ対策の実施について、以下の要件を満たすこと。
  - 情報セキュリティインシデントの対処方法を事前に定め、事案が発生した場合、原因分析及び対処方法を担当官に報告し、承認を得ること。
  - 情報セキュリティ対策その他の契約の履行状況について担当官に定期的に報告を行うこと。
  - 担当官から情報セキュリティ対策の履行が不十分である旨を指摘された場合、改善策を検討し、担当官から承認を受けた上で実施すること。
- 請負事業者は、業務を再委託する場合には、再委託先に対して調達仕様書及び本書に定める情報セキュリティ対策と同等の要件を求めること。また、原子力規制庁に対し、再委託の可否の承認をもとめること。
- 請負事業者は、担当官から要機密情報を提供された場合には、当該情報の機密性の格付けに応じて適切に取り扱うための措置を講ずること。（具体的な対策については、原子力規制委員会情報セキュリティポリシー及びその関連規程を参照）原子力規制庁より提供された要機密情報は、請負業務以外の目的で利用しないこと。また、本業務において請負事業者が作成する情報については、担当官からの指示に応じて適切に取り扱うこと。
- 請負事業者は、機密性２を含む要保護情報を取り扱う保守端末について、盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護すること。なお、端末については行政LAN端末を利用することとし、行政LANにて規定されたセキュリティ要件に従うこと。
- 請負事業者は、要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護すること。

- 請負事業者は、原子力規制委員会情報セキュリティポリシー及びその関連規程に準拠した情報セキュリティ対策の履行が不十分と見なされるとき又は請負事業者において請負業務に係る情報セキュリティ事故が発生したときは、必要に応じて担当官の行う情報セキュリティ対策に関する監査を受け入れること。
- 請負事業者は、担当官から提供された要機密情報が業務終了等により不要になった場合には、確実に返却又は廃棄すること。また、請負業務において請負事業者が作成した情報についても、担当官からの指示に応じて適切に廃棄すること。
- 請負事業者は、本業務におけるシステムの構築・改良等が完了し運用を開始する前に、請負事業者の品質管理責任者による品質報告及びセキュリティ報告を実施すること。セキュリティ報告には、脆弱性診断及びクラウドサービスの設定誤りの診断等の安全点検の結果を「脆弱性検査結果報告書」として作成し、担当官に報告すること。また、不備が指摘された場合は、運用開始までに適切な対処を実施すること。なお、システム構築時における脆弱性診断の実施基準については、標準ガイドライン群のセキュリティに関するドキュメント「DS-221 政府情報システムにおける脆弱性診断導入ガイドライン」（令和４年６月30日、デジタル庁。以下「脆弱性診断導入ガイドライン」という。）の「３　政府情報システムにおける脆弱性診断の実施基準」に準じること。また、ペネトレーションテストやTLPT（脅威ベースのペネトレーションテスト）等の高度な脆弱性診断の実施の検討等、具体的な実施内容は担当官と協議の上で決定すること。
- 請負事業者は、原子力規制委員会情報セキュリティポリシー及びその関連規程に準拠した情報セキュリティ対策を実施すること。
  （参考）原子力規制委員会情報セキュリティポリシー
  https://www.nra.go.jp/data/000129977.pdf
- 請負事業者は、個人情報を扱うことから、以下の法令・ガイドラインを準拠すること。
  - 行政機関の保有する個人情報の保護に関する法律(第6条安全確保の措置)
  - 行政機関の保有する個人情報の適切な管理のための措置に関する指針について(第8条 保有個人情報の提供及び業務の委託等)
  - 個人情報の保護に関する法律及び各種ガイドライン(通則編等)
- 請負事業者は、本業務の終了時に、本業務で実施した情報セキュリティ対策を書面で報告すること。

（２）　システムのライフサイクル

請負事業者は、下記の点に留意してライフサイクルを確保するものとする。

- 請負事業者は、情報システム台帳を作成するため原子力規制庁が指定する様式に、セキュリティ要件に係る内容等を記録又は記載し、原子力規制庁に報告する

こと。

- 請負事業者は、所管するホームページシステムの情報セキュリティ対策を実施するために必要となる文書として、以下を網羅したシステム関連文書を整備すること。
  - システムを構成するクラウドサービス
  - システム構成要素ごとの情報セキュリティ水準の維持に関する手順
  - 情報セキュリティインシデントを認知した際の対処手順
- 請負事業者は、開発等のライフサイクルで不正な変更が加えられないように管理を行う。また、原子力規制庁が確認できる仕組みを設けること。
- 請負事業者は、情報セキュリティ対策の視点を加味して納入時の確認・検査手続を整備し、原子力規制庁に承認を得ること。
- 請負事業者は、原子力規制委員会情報セキュリティポリシーに応じた体制の整備を行うこと。
- 請負事業者は、機器等を調達する場合には、「ＩＴ製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること。
- 請負事業者は、基盤となるシステムを利用してシステムを構築する場合は、基盤となるシステム全体の情報セキュリティ水準を低下させることのないように、基盤となるシステムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定すること。
- 請負事業者は、以下の事項を含む事項を適切に実施すること。
  - システムのセキュリティ要件の適切な実装
  - 情報セキュリティの観点に基づく試験の実施
  - システムの開発環境及び開発工程における情報セキュリティ対策
- 請負事業者は、ホームページシステムの運用・保守において、「調達仕様書」及び本資料を確認のうえホームページシステムに実装されたセキュリティ対策に従い適切に運用すること。
- 請負事業者は、システムの構築において、情報セキュリティの観点から必要な措置を講ずること。
- 請負事業者は、構築したシステムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずること。
- 請負事業者は、システムの受入れ時の確認・検査において、仕様書等に定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認すること。
- 請負事業者は、ホームページシステムの運用・保守業務を行うに当たり、権限外の情報にアクセスできないようアクセス制御や権限管理を行うこと。また、アク

セス制御や権限にかかる設定変更について、ログを取得すること。また、多要素認証により、第三者による不正操作等の脅威から保護すること。加えて、認証・認可の統合管理基盤を用いたアクセス制御や、アクセスの要求ごとに主体等の状況を継続的に認証し認可する仕組みを実現する機能の一部である動的なアクセス制御の実装について、業務影響等を考慮しながら、原子力規制庁と協議のうえ実装の要否を検討すること。

- 請負事業者は、基盤となるシステムを利用して構築されたシステムを運用する場合は、基盤となるシステムを整備し、運用管理する原子力規制庁との責任分界に応じた運用管理体制の下、基盤となるシステムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切にシステムの運用設計を行うこと。
- 請負事業者は、不正な行為及び意図しないシステムへのアクセス等の事象が発生した際に追跡できるように、保守に係る作業についての記録を管理すること。
- 請負事業者は、ホームページシステムの更改又は廃棄を行う場合は、当該システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の措置を適切に講ずること。
  - ホームページシステム更改時において、情報の移行作業における情報セキュリティ対策
  - ホームページシステム廃棄時において、クラウドサービス上の不要な情報に対する適切な消去の実施
- 請負事業者は、ホームページシステムの情報セキュリティ対策について新たな脅威の出現、監視等の状況により見直しを適時検討し、必要な措置を講ずること。

（3）　システムの構成要素

請負事業者は、下記の点に留意して構成要素を定義するものとする。

- 請負事業者は、所管する範囲に対して年1回の頻度で第三者による脆弱性診断（クラウドサービスの設定診断含む）等を実施し、不適切な状態を検出等した場合には改善を図ること。

  なお、システム運用時における脆弱性診断の実施基準については、標準ガイドライン群のセキュリティに関するドキュメント「DS-221 政府情報システムにおける脆弱性診断導入ガイドライン」（令和４年６月30日、デジタル庁。以下「脆弱性診断導入ガイドライン」という。）の「３　政府情報システムにおける脆弱性診断の実施基準」に準じること。また、具体的な実施内容は担当官と協議の上で決定すること。
- その他、情報セキュリティの観点から必要な試験がある場合には、試験項目及び試験方法を定め、これに基づいて試験を実施すること。
- 請負事業者は、原子力規制庁が次期システムへの更改時に本案件にて導入するク

ラウドサービスを継続利用しないと判断した場合、クラウドサービスの契約期間が終了する時点でクラウドサービス上の全ての情報を消去すること。なお、次期システムへのデータ移行の状況によって、最小限必要なライセンスに絞った上でクラウドサービスの契約を延長可能とすること。延長にかかる費用は本調達の範囲には含めないこととする。

- 請負事業者は、原子力規制庁が次期システムへの更改時に本案件にて導入するクラウドサービスを継続利用すると判断した場合、次期システムの構築事業者に、作成したアプリケーションやデータ等を引き継ぐこと。

5-2. 設計・構築に関する要件

（1） 設計・構築前

- 要件定義書（本紙）に基づき、ライフサイクルの定義、ライフサイクル毎のコンテキスト分析及びホームページシステムの利用者に関するユースケース分析を実施し、業務要件及びシステム要件を導出し、要件定義書を更新して成果物について担当官の承認を受けること。その際、調達手続き開始後の事情の変化、本業務請負事業者の提案等を踏まえ、要件定義の内容に関する認識に可能な限り相違が生じないよう、必要に応じて、PJMO とともに関係機関、情報システムの利用者、関係事業者と、要件定義の内容について確認及び調整を行うこと。
- 要件のうち、機能要件については、機能フロー図を活用して抽象度の統一に留意すること。
- 要件のうち、非機能要件については、性能、品質特性についても考慮すること。
- 開発手法（ウォーターフォール、アジャイル等）は、豊富な成功実績を有する確立されたフレームワーク（設計・開発プロセス）を採用すること。また、ウォーターフォール型以外の請負事業者固有の設計・開発プロセスを利用する場合は、ISO/IEC 12207、共通フレームSLCP-JCF2013 等の標準的な開発手法に準拠すること。
- 開発標準を提案すること。また開発時には、当該開発標準を作業担当者に確実に周知すること。
- クラウドサービス提供者、請負事業者における役割と責任の範囲を明確にすること。
- クラウドサービス提供者へセキュリティを保つための開発手順等の情報を要求すること。また、入手した情報と原子力規制庁の求めるセキュリティ要件との違いを確認すること。
- クラウドサービス上に導入するソフトウェアのクラウドサービス上におけるライセンス規定の遵守及びクラウド固有の使用許諾に関する要求事項を特定すること。

（２）　設計・構築時

- 設計及び構築の工程について、必要に応じて PJMO とともに関係機関と調整し、設計・構築実施計画書及び設計・構築実施要領を作成すること。なお、設計・構築実施計画書の記載内容は「デジタル・ガバメント推進標準ガイドライン」（令和４年４月２０日、デジタル社会推進会議幹事会決定。以下「標準ガイドライン」という。）の「第３編 ＩＴマネジメント／第７章 設計・開発」における設計・開発実施計画書として定義されているものとすること。
- 要件定義書に基づいて基本設計及び詳細設計を行い、成果物について担当官の承認を受けること。その際、プロジェクトが円滑に実施されるよう、必要に応じて、PJMO とともに関係機関、情報システムの利用者、関係事業者と、要件定義の内容について確認及び調整を行うこと。
- 要件の細分化にあたっては、追跡可能性を確保するとともに、次期システムへの更改の妨げとなる独自の仕様を含めないよう留意するとともに、PJMO 及び PJMO が指示する機関等の確認を受けること。
- 設計工程の成果物に基づき、ホームページシステムを構築すること。
- クラウドサービス上の仮想マシンを展開する前に外部ネットワークとの通信を制御すること。
- クラウドサービスの設定について定期的に確認すること。
- NTPサーバを利用した時刻同期機能を有すること。
- 独立行政法人情報処理推進機構（IPA）による「安全なウェブサイトの作り方」やOWASP のASVS（Application Security Verification 389 Standard：アプリケーションセキュリティ検証標準）等を参考に、既知の種類の脆弱性を排除したウェブアプリケーションを実装すること。

5-3.　テストに関する要件

（１）　テスト要件

- テスト手法及び品質検証の手法として、過去の情報システム開発案件において、豊富な成功実績を有する手法を利用すること。なお、請負事業者固有のテスト手法及び品質検証手法を利用する場合は、ISO/IEC12207、共通フレームSLCPJCF2013等の標準的なテスト手法、ISO/IEC25040、ISO/IEC/IEEE29119等の標準的な品質評価規格との対応関係について確認すること。
- 各種テストにおいて計画書及び結果報告書を作成し、担当官の承認を受けること。なお、計画書には、N-ADRESシステムとのシステム連携に係る一連の機能等をテストすること。
- 各種テスト実施に際しては、テストに用いる環境（本番環境が必要な場合それも含む）の設計及び設定を行うこと。
- 各種テストデータは、請負事業者が本番を模した擬似データを作成して用いるこ

と。ただし、N-ADRESとのシステム連携テストは、担当官と調整とする。なお、各種テストで使用したテストシナリオ、テストスクリプト、テストデータ等については、運用業務期間における動作確認等において、それらを一部改変して再利用できるように保管しておくこと。

- ソースコードが不正に変更・消去されることを防ぐために、ソースコードの変更管理、ソースコードの閲覧制限のためのアクセス制御及びソースコードの滅失、き損等に備えたバックアップの取得を含むソースコードの管理を適切に行うこと。
- セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビュー及びソースコードレビューの範囲及び方法を定め、これに基づいてレビューを実施すること。

（2） テストの種類毎の要件

本業務における実施すべき各テストの実施内容等を下表に示す。

表22 各テストの概要

No.	テストの種類	テストの実施内容等	テスト環境	実施者
1	単体テスト	• 各機能単体での動作が設計書通り正しく動作するかテストする。 • プログラムソースコードを網羅するホワイトボックステスト（命令網羅、分岐網羅、条件網羅）、関数又は機能の入出力を網羅するブラックボックステストの双方を行うこと。	請負事業者内	請負事業者
2	結合テスト	• 結合したプログラム及びモジュールが設計書通りに正しく動作するかテストする。 • テスト対象機能について、同値分析、境界値分析、原因結果分析を行い、その結果を踏まえてテストケース、テスト項目を設定する。 • テスト対象に対して異常データを含む様々なバリエーションのデータを投入し、動作及び処理結果を確認する。	請負事業者内	請負事業者
3	総合テスト	• 機能テスト、操作マニュアルテストは実運用を想定した環境下でテストを実施し、障害時対応を含めて、各業務シナリオの実運用で定められた手順の通りに正しく動作することをテストする。 • N-ADRES との連携をテストする。本番環境上の API を利用してデータの適切な送受信・データベース操作ができること等を確認する。 • 性能テスト、負荷テスト、災害対策訓練等の運用を想定し、「4-6 性能に関する要件」を満たすことをテストする。	請負事業者内	請負事業者
4	受入テスト	• システムを試運転させ、一通りの業務が正常に行えるか、を確認する。	本番環境	規制庁

		・ 要件定義書に基づいた信頼性、性能・拡張性、セキュリティ等に関する要件が満たされているかを確認する。 ・ 受入テストにおいて、担当官が確認する作業については、手順書、試験項目及びテストデータの整備や作業支援を実施すること。		

5-4. 移行に関する要件

- 本番環境へのシステム移行およびデータ移行に備えて、移行の方法、環境、ツール、段取り等を記載した移行計画書を作成し、担当官の承認を受けること。その際、移行のリスクを低減するため、必要に応じ、PJMO とともに関係機関、関係事業者等と調整を行うこと。
- 担当官の移行判定を受けて、要件定義書及び移行計画書に基づく移行作業を行い、移行結果を担当官に報告すること。
- 移行作業の実施は、夜間帯や週末等を基本とするが、担当官と協議のうえ決定すること。
- 移行に当たり、次期ホームページシステムのデータ構造を明示し、保有・管理するデータの変換、移行方法、例外データ等の処理方法等に関する手順書を作成し、担当官の承認を受けること。なお、上記手順書に従い、データを変換・移行した後は、移行後のデータだけでなく、例外データ等についても確認を行い、データの信頼性の確保を図ること。

（1） 移行リハーサル及び移行後作業

ホームページシステム移行及びデータ移行の手順は以下のとおりである。

(ア)移行リハーサル（移行データの検証、移行時間の測定等）

- 請負事業者は原子力規制庁と移行データの移行方法に関する認識合わせを行う。また「移行計画書」等に基づき移行リハーサルを実施し、システム移行に向けた移行実施手順、移行スケジュールの検証を行う。なお、システム移行リハーサルは、システムの特性やリハーサルの結果によって、複数回実施する場合がある。
- 移行リハーサルのスケジュールは、「1-3.更改スケジュール」の記載に従う。リハーサルの結果を担当官が確認する期間を十分にとることに留意すること。

(イ)システム移行後作業

- 運用が安定していることを確認後、データ移行用に準備したデータが存在する場合は原子力規制庁の承認を得て、データの削除を行う。
- 請負事業者はシステム移行後、「移行実施結果報告書」を原子力規制庁へ提出すること。

（2） 移行対象データ

ホームページシステムの更改に係るデータの移行対象は、以下のとおりである。

(ア)各種公開資料

移行対象となる公開資料の種類、データ量、データ形式、ファイル数及びページ数、データ移行元等については「２-２．規模に関する事項」を参照すること。（※）なお、移行対象となる公開資料のうち、文字データのないPDF資料を抽出し、移行前に

OCR処理を実施することが望ましい。
※ 2024年３月のN-ADRES更改に際し、ホームページシステムで管理していたページや資料等をN-ADRESに移行したため、移行対象データの総量が大幅に減少する見込みである。（ページ数については2023年度から1/9程度に減少する想定）

(イ)原子力規制庁職員情報

表23 職員情報

区分	データ量	内容・備考
原子力規制庁職員情報	最大 150 名	・ 主体認証や、資料属性の一部として利用するための情報

（３） 移行スケジュール

請負事業者は、下記を考慮したうえで、担当官と協議の上で移行スケジュールを決定すること。

- 「1-3. 更改スケジュール」の記載
- 現行システムとの切替時期
- 移行対象データの整理・修正作業

5-5. 教育に関する事項

（１） マニュアルの作成

請負事業者は、ホームページシステムを利用して業務を行う際に業務担当者が参照する「操作手順書（業務担当者向け）」、原子力規制庁職員が本システムに係るシステム管理業務を行う際に参照する「操作手順書（システム管理者向け）」を作成すること。なお、運用・保守業務の請負事業者が利用する「運用・保守手順書」は、これとは別に作成すること。なお、研修資料として、研修開催状況を撮影した動画も含めること。

各操作手順書の要件を以下に示す。

表24 マニュアルの概要

No	対象	作成要件
1	共通	・ 電子ファイルで提供すること。 ・ 用語集、目次を記載すること。 ・ IT の用語等、一般的にわかりにくい用語は、注釈を記載すること。
2	操作手順書（業務担当者向け）	・ サブシステム又は機能別に操作手順書を分割して作成すること。分割単位等については、担当官と協議の上、決定すること。 ・ 業務フローが記載され、本システム全体を俯瞰する内容と、本システムにおける個々の業務に沿った画面の流れを記載すること。 ・ 現行システムと次期システムの主な違いを整理して記載すること。
3	操作手順書（システム管理者向け）	・ 原子力規制庁職員が管理者権限のみで行える機能について記載すること。

		・ サブシステム又は機能別にシステム管理者が異なる場合、操作手順書を分割して作成すること。分割単位については、担当官と協議の上、決定すること。 ・ 請負事業者と職員によるシステム管理業務の責任分界点、作業分担を区別して記載すること。
4	研修動画	・ 研修資料として研修実施状況を撮影した動画を作成すること。なお、当該動画については、原子力規制庁職員に対する研修に利用する範囲において、原子力規制庁での編集等も想定している。 ・ 電子データで納品すること。 ・ 対象内容、展開方法等、担当官と協議すること。

（2） 研修の実施

請負事業者は規制庁職員が実際の業務に沿った画面操作を行って、操作の習熟ができる研修を実施すること。

(ア)運用開始前の操作研修

- 以下のように、対象者別に役割や操作内容に応じた研修内容を用意し実施すること。
- 時期については、規制庁と協議の上決定すること。
- 公開情報の利用は、マニュアルの提供で代替する。（研修は不要）

① 公開情報の内部管理

表 25 内部管理

研修対象（実施体制）	実施回数	補足
原課	2回	各回15名程度、合計30名程度とする。
広報室	1回	5名程度とする。

② 運用保守

表 26 運用保守

研修対象（実施体制）	実施回数	補足
広報	1回	5名程度とする。

(イ)運用開始後の操作研修

- 運用開始後も、「（ア）運用開始前の操作研修」同様の研修を定期的に実施すること。
- 時期や頻度については、規制庁と協議の上決定する。なお、E ラーニング形式のコンテンツ等の納品でも可能とする。

(ウ)研修内容・教材

- 「2-1. 業務実施手順に関する事項」に記載される業務に必要な操作が網羅されていること。
- 前節「（１）マニュアルの作成」で作成するマニュアルを使用するとともに、ホームページシステムを使用し、実際に操作をしながら学習する内容とすること。
- 研修に必要なデータやファイル（例えば、ログイン情報や資料登録用のファイル等）は、請負事業者で用意すること。
- 運用開始後に、必要に応じて教材を更新すること。更新内容案については請負事業者から提案すること。
- その他、規制庁が指示する内容に基づき教材の修正や更新を行うこと。

(エ)研修会場・資材

- 研修で使用する会場や端末、プロジェクター等は原則として規制庁が用意する。なお、開催方法については、Web 会議等のオンラインでの実施も可とする。規制庁と協議のうえ、開催方法を決定すること。
- 操作研修教材を含む、研修に必要なホームページシステム環境や資料は、請負事業者が用意する。研修で使用するテキストやマニュアル等の資料は、請負事業者が研修受講者数の部数を用意するとともに、電子媒体で１部納品すること。
- 研修用の動作環境（OS やブラウザ等）については、事前に規制庁に確認すること。

5-6. 運用に関する事項

請負事業者は、システムの安定的な稼動を可能とするために、システム環境や本システムを構成するアプリケーションやインフラ環境等を適切に管理するための運用環境、運用手順等を整備すること。

（1） 運用設計

請負事業者は、原子力規制庁が承認した「運用・保守計画書」に従い、具体的な運用方法や利用するツール、監視対象や閾値等の運用設計を行い、内容等について原子力規制庁の承認を得ること。また、運用設計に際しては、運用業務の標準化や改善プロセスについて考慮し、属人的作業の排除や運用の自動化等、継続的な運用の効率化に努めること。なお、システムを構成する機器へのセキュリティパッチについて、セキュリティリスクが高い場合は即時適用する、当該情報システムの安定稼働を優先する場合は影響調査及び検証の後に適用する等、適時の適用を前提とした運用設計を行うこと。

（2） 運用管理・監視等要件

(ア)運用管理要件

- 収集・蓄積されたトラブル発生状況や性能情報の分析が可能であること。
- 以下の項目について、月次で実施した作業の有無や内容等をまとめ、報告書の提出及び報告会を開催すること。
  - システム利用実績
  - アカウント利用状況
  - ストレージ利用状況
  - セキュリティ管理
  - 問い合わせ件数及び回答状況
- 年間の運用実績を取りまとめた年次報告書を提出すること。
- システムに何らかの変更を行う場合は、事前に十分な検証のうえ、実施内容を担当官に説明し、承認を得たうえで実施すること。
- 原子力規制庁が実施するセキュリティ監査等により、設定変更を伴う対応指示等を受けた場合には、迅速な調査・検証を実施の上、対応について担当官と協議すること。
- ホームページシステムに関する政府機関からの調査依頼あるいは対応指示事項に関して、担当官等から相談や調査依頼を受けた場合は、遅滞なく助言・参考資料提出等の支援を行うこと。

(イ)監視等要件

- ホームページシステムの監視対象、実施時間、実施内容は以下のとおりとす

る。また、監視間隔は分単位（例：5 分間隔など）とすること。

表 27 監視の概要

対象	実施時間	実施内容
サーバー	24 時間 365 日	• 死活監視 • 資源状況（CPU・メモリ・ディスク使用率、ネットワーク消費帯域） • プロセス監視 • ウイルス検知 • バックアップやバッチ処理の実行 • 不正プログラム監視
ネットワーク機器	24 時間 365 日	• 死活監視 • 資源状況（CPU 使用率、ネットワーク消費帯域）

（3） ヘルプデスク

- ホームページシステムの障害を含めた問合せに対応する窓口を設置すること。
- ヘルプデスクの対応可能時間（利用者が使用可能な時間）は、少なくとも原子力規制庁の就業時間帯（平日 9 時～18 時 30 分）とする。但し、緊急時に 24 時間 365 日対応を受け付ける窓口を別途用意すること。
- 想定問合せ数を以下に示す。システム更改後数年は問合せ件数が比較的多くなる見込みである。
  - 2026～2027 年度：50 件程度/年
  - 2028 年度：30 件程度/年
  - 2029 年度：10 件程度/年

（4） コンテンツ運用支援

- 原子力規制委員会ホームページシステムのコンテンツの運用支援としての実施事項を以下に示す。なお、以下の内容を基に契約としては、月や年単位ではなく、運用期間（50 ヶ月）単位で対応件数を検討すること。契約期間内に当初の想定を超える対応が必要な場合は、追加契約等の対応について規制庁と協議を行い決定すること。

表 28 コンテンツ運用支援の概要

実施事項	想定件数	備考
ページや画像の修正・新規作成	5000 頁/50 ヶ月 （平均 100 頁/月）	既存ページのテンプレート化を行った場合は、左記の対応件数について、ページや画像の管理は減少、テンプレートの管理は増加する可能性がある。
ページテンプレートの修正・新規作成	20 件/50 ヶ月 （平均 5 件/年）	
アカウント管理（追加・削除・変更等）	20 件/50 ヶ月 （平均 5 件/年）	アカウント数の増減により、対応件数の増減の可能性がある。

（5） アクセシビリティチェックへの対応

- 年に数回程度行われるアクセシビリティチェックで抽出された指摘への対応（都度、数十ページ程度の修正が発生する見込み）を行うこと。

（6） バックアップ要件

- すべてのデータを自動でバックアップを取得し、必要に応じて手動でバックアップも可能であること。また、取得した履歴を記録すること。
- バックアップ取得間隔は、日次以上の頻度で取得すること。
- バックアップはシステム停止を伴わずに可能であること。
- バックアップからシステムを復旧できること。
- 大規模災害発生時のデータリカバリ及びシステム復旧の考え方及び手順を整理した災害時システム復旧手順書を作成し、運用保守計画に反映すること。

（7） 改善の提案及び実施

- 原子力規制庁職員の問い合わせ傾向を分析し、ホームページシステムの改善提案を行うこと。
- 原子力規制庁職員からの要望（入力項目の追加、入力チェックの追加やお知らせ機能の追加等、軽微なシステム改修）に基づき、システムの改善を実施すること。改善に要する工数として年間 3 人月を計上すること。
- 大規模災害や利用するクラウドサービスにおいて情報セキュリティインシデントが発生した際のデータリカバリ及びシステム復旧の考え方及び手順を整理した災害時システム復旧手順書を作成し、運用保守計画に反映すること。

（8） 引継ぎ

- 設計・構築業務で作成した設計書、作業経緯、残存課題等を文書化するとともに、要件定義書に基づき、運用チーム、保守チーム及び情報セキュリティチームに対して確実な引継ぎを行うこと。
- 請負事業者は、原子力規制庁がホームページシステムの更改を行う際には、次期システムにおける要件定義支援事業者及び設計・開発事業者等に対し、作業経緯、残存課題等に関する情報提供及び質疑応答等の協力を行うこと。
- 請負事業者は、本契約の終了後に他の運用・保守事業者がホームページシステムの運用を受注した場合には、次期運用・保守事業者に対し、作業経緯、残存課題等についての引継ぎを行うこと。

5-7. 保守に関する事項

請負事業者は、保守計画書、保守手順書等を整備すること。保守業務に置いては、以下の内容を考慮すること。また、請負事業者の保守対象は、クラウドサービス（本調

達にて設定やカスタマイズを行う範囲）とする。

（1） 保守要件

- 請負事業者は、「保守作業計画書」及び「保守手順書」に基づき、保守作業の内容や工数などの作業実績状況、サービスレベルの達成状況、リスク・課題の把握・対応状況について「月次報告書」に取りまとめ提出すること。
- 請負事業者は、月間の保守実績を評価し、達成状況が目標に満たない場合はその要因の分析を行うとともに、達成状況の改善に向けた対応策を提案すること。
- 年間の運用実績を取りまとめた年次報告書を提出すること。

（2） 障害発生時対応

- 監視アラート及び問合せ窓口への申告等により障害を検知した場合は、速やかに切り分けおよび、サービス継続のための一次対応を行うこと。
- 障害等の保守対応業務に係る発生からクローズまでの一連の対応状況を管理し、インシデント対応状況及び分析結果について、障害対応報告書を提出すること。
- 個人情報の漏洩及び計画外のサービスの停止等、重大なインシデントについては速やかに担当部署に報告すること。
- インシデントの管理に係る様式については、運用保守開始時に担当部署に提示すること。
- 保守開始から当面の間は、本システム設計・構築に参画した者（リーダークラス）を１名以上含むこと。
- クラウドサービス提供者、請負事業者における役割と責任の範囲について定期的に確認すること。

（3） 外部システムに起因する障害対応

- 行政 LAN に起因する障害の可能性がある場合は、担当官に状況を報告の上、指示に従うこと。（担当官から原子力規制庁長官官房総務課情報システム室に連携する）。

（4） 保守作業の改善提案

- 請負事業者は、年度末までに必要に応じて「保守作業計画書」及び「保守手順書」に対する改善提案を行うこと。

（5） 引継ぎ

- 請負事業者は、原子力規制庁がホームページシステムの更改を行う際には、次

期のシステム更改における請負業者等に対し、作業経緯、残存課題、設計書等に関する情報提供及び質疑応答等の協力を行うこと。

- クラウドサービス上に保管される情報・データを標準で暗号化する設定とし、ホームページシステムの運用を終了する際には、暗号化に用いた鍵を廃棄することで暗号化データを回復不能とする、通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど、クラウドサービス上の情報・データを確実に消去すること。

機能一覧

機能名			要件
1. ページ作成機能			
1. テンプレート機能			
	1	テンプレートの作成	・定型化（調達情報、報道発表等）された情報を掲載するテンプレートを作成する ・テンプレートの登録数に上限がない
	2	自由度の高い入力欄と低い入力欄の混在	・レイアウトや体裁調整の自動度が高い入力欄と作成書による自由度が低い入力欄を１つのテンプレートに配置する。
	3	スマートフォン表示への対応	・スマートフォン表示にも対応可能なテンプレートを作成する
	4	テンプレートの権限管理	・管理者が作成者毎に選択可能なテンプレートを指定できる
	5	テンプレートのカスタマイズ	・請負者又は管理者等が導入時に作成したテンプレートについて、導入後にコンテンツ領域の変更が容易にできる
	6	著作権の表記	・ページ作成時に個々のページに対して種別を設定することにより、定型の著作権表記を自動的に掲載できる
	7	著作権のタグ	・ページ作成時に個々のページに対して種別を設定することにより、定型の著作権記述タグを自動的に掲載できる ・個々のページに対して記述された著作権表記やタグを、サイト単位又はディレクトリ単位で一括編集できる
	8	静的及び動的コンテンツの埋め込み	・静的に作成されたHTMLや画像等を埋め込むことができる ・動的に生成されるコンテンツを埋め込みことができる
2. ページ作成（作成者）			
	1	タイトル・テキスト入力	・HTMLソースを編集することなく、簡易な操作によって入力・変更することができる
	2	リンク設定	・HTMLソースを編集することなく、簡易な操作によってリンク設定ができる
	3	画像配置	・HTMLソースを編集することなく、簡易な操作によって画像を配置できる
	4	ページの複製	・簡易な操作によって、既存のページを複製し、修正することで新たなページを作成できる ・簡易な操作によって、複数のページを含むカテゴリを複製し、修正することで新たなカテゴリやページを作成できる
	5	動画投稿サイトの動画配置	・HTMLソースを編集することなく、簡易な操作によって動画投稿サイト（Youtube等）の動画を配置できる
	6	表作成	・HTMLソースを編集することなく、簡易な操作によって表の作成、編集ができる ・Microsoft Word、Excelの文書からコピー＆ペーストできる
	7	HTMLソース編集	・HTMLソースを直接編集できる ・ソース編集を行える権限を設定できる ・Microsoft Word、Excelの文書からコピー＆ペーストする際に、ソースクリーニングを行うメニューを選択する等の操作により、タグを変更・削除した上で張り付けることができる
	8	上書きに関する注意喚起	・同名ファイルをライブラリに追加しようとした場合、上書きに関する注意喚起する
3. ページ作成（制御・変換）			
	1	W3C	・W3C基準の文法仕様に則ったHTMLでページ作成する
	2	HTMLバージョンへの対応	・導入時に指定するHTMLのバージョンでページ作成する（例：XHTML、Strict、HTML5）

機能一覧

機能名			要件
	3	CSSによる体裁の制御	・ページの色・サイズ等のHTML要素・属性（table要素、font要素、align属性等）によらず、CSS（スタイルシート）の指定により制御する
	4	属性情報の自動挿入	・あらかじめ登録しておいた作成者の属性情報（所属、名前、問合せ先等）に基づき、自動挿入できる ・コンテンツの掲載日及び更新日を自動挿入できる（任意で変更できる） ・掲載日及び更新日を両方表示できる
	5	ナビゲーション	・「ページトップへ」「前のページへ」等のページ内リングが共通位置へ自動的に挿入できる
	6	title要素	・title要素の内容の入力を強制する ・title要素への共通文字列（タイトル、団体名、HP名等）を自動的に挿入できる
	7	SEO関連META要素	・SEO関連META要素の内容の入力を強制する ・あらかじめ設定されたキーワード等のMETE要素を自動的に挿入できる
	8	alt属性の入力強制	・画像にalt属性が入力されなかった場合、入力を強制する（自動的には入力しない）
4. 添付ファイル掲載機能			
	1	添付ファイルの掲載	・添付ファイルのリンクをページ内に設定し、公開と同時に各ページの添付ファイルの掲載ができる ・添付ファイルの掲載数に上限を設けない。（上限の設定は可能） ・添付ファイルをページ単位で一括削除できる ・添付ファイルのファイル形式に応じたアイコンが表示できる
	2	添付ファイルの確認	・作成者が添付ファイルを一度開かないと承認依頼できない ・承認者が添付ファイルを一度開かないと承認できない
5. 多言語対応機能			
	1	外国語サイト運用	・日本語以外の複数の言語版ホームページを作成できる ・言語別のテンプレートを用意し、各ページに適した属性を付与する
	2	翻訳機能	・日本語サイトと外国語サイトの両方に同様の情報を掲載する場合、日本語で書かれた内容を基に外国語サイト用のページ作成ができる ・利用者が日本語サイトを閲覧時に、多言語へ自動翻訳して表示できる
2. 確認・チェック機能			
1. 作成ページ確認機能			
	1	ブラウザ表示による確認	・簡易な操作によって、ブラウザで表示を確認できる ・ブラウザによる確認時に変更された箇所が分かりやすく表示できる
	2	HTMLソースの確認	・簡易な操作によって、HTMLソースを確認できる ・HTMLソースの変更された箇所が分かりやすく表示できる
	3	一時保存	・簡易な操作によって、作業中のページを一時保存できる ・アクセシビリティ等のチェック結果に問題有る場合でも一時保存できる
	4	スマートフォンの確認	・簡易な操作によって、スマートフォンでの表示を確認できる
2. 公開ページ確認機能			

機能一覧

機能名			要件
	1	公開状態の確認	・簡易な操作によって、添付ファイルを含めてブラウザ等で表示し、ページ遷移できる形で確認できる ・未来日時に設定した際と全体の公開ページの状態を確認できる
	2	公開前確認権限の設定	・管理者が作成者グループに対し、確認可能な範囲を設定できる
3. チェック・ワーニング機能			
	1	必須入力項目チェック	・設定した必須入力項目に問題がある場合、作成者へ注意喚起する
	2	HTML文法チェック	・W3Cの文法に則ったHTMLか否かを公開前に機械的にチェックできる ・HTML文法の問題を検出した場合、注意喚起又は公開制限できる
	3	アクセシビリティチェック	・JIS X8341-3:2016に示されたアクセシビリティ要件に則り、問題の有無を機械的にチェックできる ・JIS X8341-3:2016に示されたアクセシビリティ要件に関する問題を検出した場合、注意喚起又は公開制限できる。また問題箇所をハイライト表示する等により視覚的に特定できる ・管理者がアクセシビリティチェックの項目を指定できる ・色覚障害を持つ利用者が閲覧する際の見え方をシミュレーションできる ・色覚障害を考慮した、背景色と文字色の組み合わせか確認できる ・音声読み上げ機能の音声を作成者が確認できる
	4	サイト別リンクチェック	・サイト内、サイト外のリンク切れを機械的にチェックできる。 ・サイト内、サイト外のリンク切れを検出した場合に注意喚起又は公開制限できる
	5	機種依存文字	・機種依存文字を含むページを自動的に検出できる ・機種依存文字を含むを検出した場合に注意喚起又は公開制限できる
	6	入力文字のバイト数	・入力された文字のバイト数を機械的にチェックできる ・入力された文字のバイト数に関する問題を検出した場合、注意喚起又は公開制限できる ・入力できる文字数を管理者が設定できる。また入力できる文字数を超えた場合のチェックができる
	7	特定文字列	・特定の文字列を用語辞書に登録し、該当用語を含むページを管理者が特定することができる ・特定の文字列を検出した場合、注意喚起及び公開制限できる
	8	特定HTMLタグ	・特定のHTMLタグを含むページを管理者が特定することができる ・特定のHTMLタグを検出した場合、注意喚起及び公開制限できる
	9	ファイル容量	・管理者が設定した容量を超える添付ファイルを機械的にチェックできる ・ファイル容量の問題を検出した場合、注意喚起又は公開制限できる
	10	ファイル拡張子	・許可されている拡張子以外のファイルが添付されているかを機械的にチェックできる ・許可されている拡張子以外のファイルを検出した場合、注意喚起又は公開制限できる
	11	承認申請の制限	・チェック結果に問題があった場合、承認申請を制限できる ・承認申請の制限を管理者が設定できる
	12	作成作業に対するヘルプ	・コンテンツ作成時に注意が必要な事柄についての説明を作成画面から随時参照できる

機能一覧

機能名			要件
3. ページ生成・制御機能			
	1. ページ生成		
		1	静的生成	・静的なHTMLファイルを生成し、サーバに保存できる
		2	動的生成	・利用者のアクセスやリクエストに応じて、情報を出力する動的なHTMLを生成できる
	2. 情報分類		
		1	分野別の分類	・分類の体系を「分野別」で分類できる ・部署名から担当部署が作成したコンテンツを特定できるよう、「組織別」でも情報を探せる
	3. リンク管理		
		1	固有のURL	・作成したページは固有のURLとする ・ページを更新した場合（記載内容、添付ファイルの変更等）でも、URLが変更されない ・公開前に作成者がURLを把握できる
		2	リンクの削除	・リンクを削除する際に、他のページから当該ファイルへ設定されているリンクを自動的に注意喚起する。 ・確認後、自動的にリンク（リンクテキスト、リンクタグ）を削除できる
		3	リンク元・リンク先の一覧表示	・リンクしているページ及びされているページのURL及びタイトルを一覧表示できる
		4	サイト内リンクの制御	・公開する位置に合わせて相対パスで管理できる ・公開ページの配置を変更した場合、自動的にリンクを変更できる
	4. トップページ		
		1	トップページレイアウト	・トップページのレイアウト（案）を参考に画面構成を提示する（「トップページレイアウト案」参照） ・トップページのレイアウトにCMS仕様に起因する制約がない ・「新着情報」、「トピックス」等のトップページのコンテンツ領域を管理者が追加・削除・配置変更できる ・HTMLやCSSソースを編集することなく、管理者がトップページ内の画像、配色を変更できる
		2	新着情報	・ページ作成、更新した際に自動的に「新着情報」、「注目情報」等の領域にリンクが設定される。また、管理者が手動で設定を変更できる ・「新着情報」、「注目情報」等のリンクの掲載期間を設定できる ・「新着情報」、「注目情報」の見出しに掲載日が自動的に設定される。日付は編集できる ・「新着情報」、「注目情報」等の属するカテゴリ名を付加できる ・「新着情報」、「注目情報」等に掲載されたコンテンツを更新した場合でも掲載期間や新着マーク等の設定を維持する ・掲載期間が過ぎた、又は表示件数を超えたリンクを一覧表示するページを生成できる
		3	アクセスランキング・検索キーワードの表示	・アクセス数及び検索キーワード上位のコンテンツへのリンクを自動的に任意のページに掲載できる
		4	バナーの追加・削除	・バナーの画像を追加・削除できる
		5	関連サイトの掲載情報の取得及び掲載	・関連サイトに掲載される情報をRSS等の仕組みを利用して自動的に取得し、トップページ内の関連情報掲載領域に表示できる

機能一覧

機能名			要件
5. 緊急時対応			
	1	緊急時用トップページ	・緊急時用トップページのレイアウト（案）を参考に画面構成を提示する（「緊急時用トップページレイアウト案」参照） ・重要な情報へのリンクを一時的に掲載する緊急時用トップページの領域を作成する ・当該領域を管理者が任意のタイミングで編集できる ・緊急時トップページの情報を時系列（日単位、週単位、月単位等）で分類して表示する ・一定期間経過後に任意のカテゴリに分類され、各カテゴリのメニューページへリンクを表示できる
6. グローバルナビゲーション・ローカルナビゲーション等			
	1	グローバルナビゲーション	・グローバルナビゲーションをサイト全体又は複数ページで共通の位置に表示できる ・サイト内の共有メニューとして表示する項目を管理者が追加・削除・順序変更できる
	2	ローカルナビゲーション	・ローカルナビゲーションをカテゴリ全体で共通の位置に表示できる ・カテゴリ内の共有メニューとして表示する項目を管理者が追加・削除・順序変更できる ・同じ階層にある他のページへのリンク一覧を表示できる ・カテゴリ変更した場合、自動でローカルナビゲーションへ反映する ・ページ内リンク用のインデックスメニューが自動的に作成される
	3	機能リンク	・サイトの使い方、サイトマップ等のページへのリンク等をサイト全体又は複数ページで共通の位置に表示できる
	4	位置を示すナビゲーション	・サイト内の現在位置を示すナビゲーションを自動的に生成する ・カテゴリが変更された場合、現在位置を示すナビゲーションを自動的に変更する
7. メニューページ			
	1	メニューページの生成	・ページに付与する属性情報に基づき、メニューページが自動生成できる ・カテゴリが変更された場合、関連するメニューページを自動的に変更する
	2	新着/注目情報、カテゴリに属する情報、関連サイトの種類別表示	・新着/注目情報、カテゴリに属する情報、関連サイトごとに、個別のマーク付与や視覚的分別等で区別して表示できる
	3	メニューページの注目情報領域	・メニューページ内の注目情報の領域に任意のリンクを表示できる ・注目情報に該当するコンテンツが無い場合は注目情報領域を表示しない
	4	別サイト情報を自動取得する領域	・メニューページ内に別サイトの掲載情報をRSS等の仕組みを利用し自動的に取得・表示できる ・メニューページに別サイトの掲載情報に該当するコンテンツが無い場合は別サイトの掲載領域を表示しない
	5	カテゴリ階層の設定	・カテゴリによって異なる深さの階層を設定できる
	6	メニューリンク	・メニューページ中に掲載されるメニューリンクの表示順序を設定できる ・メニューページ中に掲載されるメニューリンクの種類別に小見出しをつけ、表示できる ・メニューページ中に掲載されるメニューリンクを2列又は3列の段で表示できる
	7	別サイトへのリンク	メニューページに紐づく配下のページ以外のリンクを表示できる

機能一覧

機能名			要件
8. 関連情報			
	1	複数ルートからのアクセス	・組織別/分野別分類、注目/重要情報等、複数の異なるメニューから同一コンテンツへのアクセスルートを自動設定できる
	2	別サイトへのリンク設定	・文章内の箇条書き等の形式で関連する別サイトのリンクを挿入できる。また、別サイトであることがわかるマークを付与する。 ・関連リンクの数に上限が無く、管理者で上限を設定できる
	3	関連ページへのリンク	・関連ページのリンクを決まった場所に自動表示できる ・関連ページへの自動リンクが表示できる
	4	別サイト情報を自動取得する領域	・メニューページ内に別サイトの掲載情報をRSS等の仕組みを利用し自動的に取得・表示できる ・メニューページに別サイトの掲載情報に該当するコンテンツが無い場合は別サイトの掲載領域を表示しない
9. サイトマップ			
	1	サイトマップの生成	・サイトマップを自動的に生成・更新できる ・カテゴリを変更した場合、サイトマップの内容が自動的に反映できる ・サイトマップをツリー状に表示できる ・サイトマップにリンクを追加することができる
10. スマートフォン・タブレット型端末向けページの生成			
	1	スマートフォン・タブレット型端末向けサイトの独立管理	・スマートフォン・タブレット型端末向けサイトの独立したサイトとして構築し、ページを作成できる
	2	スマートフォン・タブレット型端末向けページ生成	・HTMLファイルをスマートフォン・タブレット型端末向けページを同時に生成できる
	3	表示切り替え	・閲覧ブラウザの横幅に合せ、レイアウト表示できる ・閲覧ブラウザにより、スマートフォン向け、PC向けに表示を自動的に切り替える ・スマートフォン向け画面で閲覧にしている際にPC用画面を選択できる。また、PC用画面からスマートフォン向け画面に再度切り替えることができる
4. コミュニケーション機能			
1. 問合せ管理			
	1	問合せ履歴の一元管理	・フォームやメールによる問合せ、職員による回答の履歴を一元管理できる
5. ワークフロー関連機能			
1. 作成～承認依頼			
	1	管理単位	・管理者が、権限を付与する単位を設定できる ・管理者が、作成者が実施できる範囲等、細かく設定できる ・カテゴリやページ単位に複数の作成者/権限グループを設定できる ・管理者が、作成～承認のワークフローの承認権限、承認ルートを設定できる ・組織名変更やディレクトリを跨いだコンテンツの移動が生じた場合、管理者がワークフローや利用権限を変更できる

機能一覧

機能名			要件
	2	サイト構成確認	・Windowsのエクスプローラのような階層表示ができる ・サイト内でのページ公開位置を設定、追加・削除ができる
	3	同時アクセス禁止	・編集中のページは作成者だけに操作を許可すること。また他の作成者には編集中の旨がわかる表示とする ・管理者に限定して作成中のページを操作できる ・同じファイル名、画像を作成しようとした場合、上書きに関する注意喚起できる ・管理者に全ファイルの更新・削除を含む無制限の管理権限を付与する
	4	承認申請	・簡易な操作によって承認申請ができる ・承認操作と同時に承認者へメールが自動配信できる ・管理者が、自動配信メールの設定できる ・簡易な操作によって複数ページの一括承認申請ができる
2. 承認作業～公開			
	1	ステータス確認	・作成者及び承認者は担当したページを一覧表形式で表示し、作業中/差し戻し/公開待ち/公開中/公開期間終了などの承認ステータスを確認できる ・作成者が過去に作成した全ページを作成、公開、履歴を確認できる ・管理者は全ページの作業中/差し戻し/公開待ち/公開中/公開期間終了などの承認ステータスを確認できる ・承認申請後に作成者が申請を取り下げ、ページ内容を修正できる ・承認申請のステータスが変更されると同時に作成者及び任意のグループへ自動的に通知メールを配信する
	2	承認・差し戻し機能	・管理者は承認或いは差し戻しを行える ・複数ページの承認申請を一括で承認できる ・特定のカテゴリーの承認申請を一括で承認できる ・・承認者が内容を修正できる。修正した旨を作成者へ通知できる。差し戻しの際にコメントを付与できる
3. 公開・削除管理			
	1	スケジュール設定	・ページ作成者が公開及び削除予定日時を指定できる ・複数ページ、カテゴリ単位で日時指定し一括公開できる ・承認済み、公開待ちコンテンツを管理者が日時指定又は手動で一括公開できる ・設定した公開及び削除予定日時を公開前、公開後に作成者、管理者が変更できる ・承認を得られ次第、即時に公開処理を開始することができる
	2	ページの保護	・公開までの間、暗号化等の手段で情報漏えい防止対策を講じる

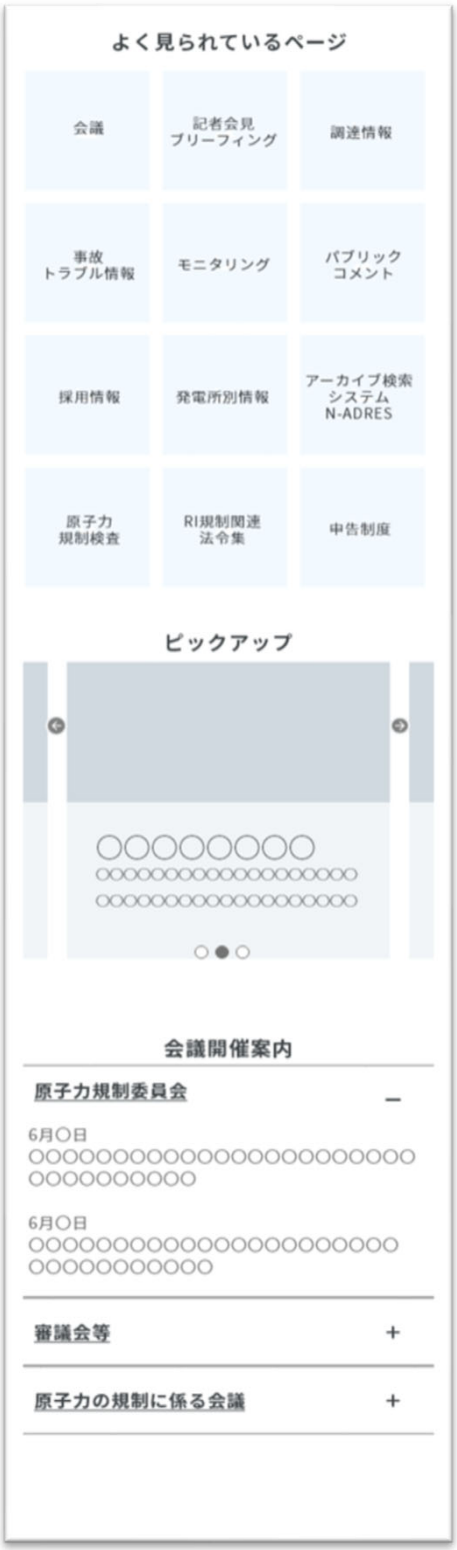
機能一覧

機能名				要件
		3	挿入ファイル	・ページ公開と同時に挿入ファイルを公開できる ・挿入ファイルをページ削除と同時に削除できる ・挿入ファイルの公開及び削除予定日を指定できる。公開後に削除日時を延長することができる ・挿入ファイルのリンク元となるHTMLページを作成する際、挿入ファイルの削除の方が早い場合等、リンク切れが起きることを注意喚起する ・挿入ファイル削除の際に他ページからのリンクがあるか確認できる
		4	ページの削除	・削除するページへのリンクの有無を確認できる。また、リンクが有りの場合、該当ページを一覧表示し、注意喚起できる ・複数ページ、カテゴリ単位で日時指定し一括削除できる ・一括削除時に関係者へ注意喚起できる ・ページ削除された場合、コンテンツ担当者へ通知する ・管理者によるページ削除したことを作成者、承認者へ自動通知できる
		5	ページの差し替え	・公開済みのページ内容を基に修正ページを準備しておき、指定日時に同一のURLのまま差し替えができる
		6	更新のないページ	・アクセス権限に応じた一定期間更新されていないページの一覧を表示できる。また、該当ページの関係者へ注意喚起することができる ・設定したアクセス数より少ないページをリスト化できる。また、該当ページの関係者へ注意喚起することができる ・掲載期間を過ぎたページの一覧を表示できる。また、該当ページの関係者へ注意喚起することができる
6. 管理機能				
	1. サイト管理			
		1	サイト状況	・ドメイン、ホスト名等の異なる複数のサイトを一つのCMSで一元管理できる ・管理者が全てのログインIDやグループ、担当ページの更新状況や承認状況を把握できる ・ページ種別等によるページの検索ができる。また、ページのテキスト情報による検索できる ・トップページからリンクをたどっても到達できないファイルを検出できる ・管理者が設定した時間を超えて作業を中断する場合、自動的にログオフできる
	2. ログ管理			
		1	ログ管理	・作成者、部署ごとにCMSへのアクセスや利用状況ログを管理できる
		2	アーカイブ機能	・作成者、管理者が保存したコンテンツの確認及び内容を修正することができる ・管理者がサイト全体の更新履歴を確認できる
	3. お知らせ・注意喚起			
		1	お知らせ・注意喚起	・管理者から関係者へ注意事項等を伝達できる ・操作等に関する問い合わせ内容やナレッジを作成者・承認者が閲覧できる

■トップページ案

①サイトナビゲーション
②メインビジュアル
③新着情報
④対象者別メニュー
⑤YouTube掲載エリア
⑥よく見られているページ
⑦ピックアップ
⑧会議開催案内

■トップページ（スマートフォン）案



■緊急情報･情報提供がない場合

■緊急情報･情報提供がある場合の展開表示

外部インターフェース一覧

No.	インターフェース名	連携方法	送受信形式	連携元	連携先	連携頻度	連携タイミング	データ形式	概要	内容
1	会合開催予定	API （SRU-API）	PUSH	本システム	N-ADRES	自動（1日2回程度） 手動	リアルタイム	XML	・ホームページシステムからN-ADRESに対して、N-ADRESに関する条件値を渡し、資料検索機能を用いて、N-ADRESでの検索結果をホームページシステムへ返却する ・ホームページシステムはN-ADRESから受信したXMLファイルをカレンダー表示等閲覧者の利便性を考慮した表示に整形する	・フォルダのタイトル ・フォルダのリンク ・資料属性
2	事故・トラブル情報	API （SRU-API）	PUSH	本システム	N-ADRES	自動（1日2回程度） 手動	リアルタイム	XML	・ホームページシステムからN-ADRESに対して、N-ADRESに関する条件値を渡し、N-ADRESでの新着情報をホームページシステムへ返却する ・ホームページシステムはN-ADRESから受信したXMLファイルを閲覧者の利便性を考慮した表示に整形する	・フォルダのタイトル ・フォルダのリンク ・資料属性
3	緊急情報・情報提供	Java Script	PUSH	本システム	緊急情報・情報提供ホームページ	自動（5分間隔） 手動	リアルタイム	String	・ホームページシステムから緊急情報・情報提供ホームページに対して、最新情報を取得する条件値（getParameter）を渡し、ホームページシステムへ返却する ・ホームページシステムは緊急情報・情報提供ホームページから受信した値をトップページに表示する	・タイトル ・資料属性

【次期ホームページシステム】非機能要件一覧

モデルシステム：社会的影響が極めて大きいシステム

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
A.1.1.1	可用性	継続性	運用スケジュール	システムの稼働時間や停止運用に関する情報。	運用時間（通常）	規定無し	定時内（9時～17時）	夜間のみ停止（9時～21時）	1時間程度の停止有り（9時～翌朝8時）	若干の停止有り（9時～翌朝8時55分）	24時間無停止	■定義内容 24時間無停止（計画停止は除く）	【重複項目】 C.1.1.1。運用時間は、システムの可用性の実現レベルを表す項目であると共に、運用・保守性に関する開発コストや運用コストを検討する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【メトリクス】 運用時間は、オンライン/バッチを含みシステムが稼動している時間帯を指す。 【レベル】 （）内の時間は各レベルの一例を示したもので、レベル選定の条件とはしていない。規定無しは、固定のサービス時間が存在しないことを示し、基本的にシステムは停止していて、必要に応じてユーザがシステムを起動するようなケースを想定している（例：障害発生に備えた予備システム、開発・検証用システム等）。定時内や夜間のみ停止は、一般的な業務形態を想定したもので、業務が稼動する時間帯が異なるシステムにおいては、時間帯をスライドさせるなどの読替えが必要である。停止有りとは、システムを停止しなければならない時間帯ではなく、システムを停止できる可能性のある時間帯を指す。24時間無停止は、オンライン業務が稼動していない時間にバッチを稼動させる必要があり、システムを停止することができないようなケースも含まれる。
A.1.1.2					運用時間（特定日）	規定無し	定時内（9時～17時）	夜間のみ停止（9時～21時）	1時間程度の停止有り（9時～翌朝8時）	若干の停止有り（9時～翌朝8時55分）	24時間無停止	■定義内容 24時間無停止	【重複項目】 C.1.1.2。運用時間は、システムの可用性の実現レベルを表す項目であると共に、運用・保守性に関する開発コストや運用コストを検討する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【メトリクス】 特定日とは、休日/祝祭日や月末月初など通常の運用スケジュールとは異なるスケジュールを定義している日のことを指す。特定日が複数存在する場合は、それぞれにおいてレベル値を整合する必要がある（例：「月～金はレベル2だが、土日はレベル0」、「通常はレベル5だが、毎月1日にリブートをするためその日はレベル3」など）。 また、ユーザの休日だけでなく、ベンダの休日についても特定日として認識し、運用保守体制等を整合すること。
A.1.1.3					計画停止の有無	計画停止有り（運用スケジュールの変更可）	計画停止有り（運用スケジュールの変更不可）	計画停止無し				■定義内容 計画停止有り。	【重複項目】 C.2.1.1。計画停止の有無は、システムの可用性の実現レベルを表す項目であると共に、運用・保守性に関する開発コストや運用コストを検討する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【運用コストへの影響】 計画停止が”有り”の場合、事前のバックアップや、システム構成に応じた手順準備など、運用時のコストがかさむ。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
A.1.2.1			業務継続性	可用性を保証するにあたり、要求される業務の範囲とその条件。	対象業務範囲	内部向けバッチ系業務	内部向けオンライン系業務	内部向け全業務	外部向けバッチ系業務	外部向けオンライン系業務	全ての業務	■定義内容 【サイト内障害時、大規模災害時ともに】 外部向けオンライン系業務。（外部向けバッチ業務、内部向け全業務を含む） ・業務の提供に間接的に関連するセキュリティ機能については対象範囲に含める。 ・業務の実施に直接関連しないバックアップ、監視等の運用系機能に関しては、対象外とする。	【メトリクス】 ここでの対象業務範囲とは、稼働率を算出する際の対象範囲を指す。 【レベル】 内部向けとは対象とするシステム内に閉じた処理（業務）、外部向けとは他システムとの連携が必要な処理（業務）を表している。
A.1.2.2					サービス切替時間	24時間以上	24時間未満	2時間未満	60分未満	10分未満	60秒未満	■定義内容 【サイト内障害時、大規模災害時ともに】 60分未満 ※本システムにおけるサービス切り替え時間とは以下の通りとする。 ・メインサイト（バックアップサイト）内の冗長構成機器の片系が異常となった場合に、もう片系に切り替わるまでの時間 ・大規模災害時に、バックアップサイトに切り替わるまでの時間 ・システムによる切替時間とする。（手動切り替え方式を採用する場合の、人の判断等に要する時間は含まない。）	【メトリクス】 サービス切替時間とは、想定できる障害（例えばハードウェアの故障等により業務が一時的中断するケースなど）に対して、対策を施すこと（例えばクラスタ構成でのサーバの切替えなど）により、業務再開までに要する時間を指す。 【運用コストへの影響】 中断を許容する時間が長くなれば、復旧対策としてはシステムでの自動化から人員による手動での対処に比重が移るため、運用コストへの影響が出てくる。
A.1.2.3					業務継続の要求度	障害時の業務停止を許容する	単一障害時は業務停止を許容せず、処理を継続させる	二重障害時でもサービス切替時間の規定内で継続する				■定義内容 【サイト内障害時、大規模災害時ともに】 二重障害時でもサービス切替時間の規定内で継続する ただし、非機能要求グレードにて記載されている機器や部位等については、クラウドサービス側にて十分な冗長化が実現されている。	【メトリクス】 業務継続の要求度とは、発生する障害に対して、どこまで業務を継続させる必要があるかを示す考え方の尺度を示している。 システムを構成する機器や部位には、単一障害点SPOF（Single Point Of Failure）が多数存在し、システム停止となるリスクを多く含んでいる。これらのSPOFを許容するか、冗長化などの対策で継続性をどこまで確保するかが要求の分かれ目となる。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
A.1.3.1			目標復旧水準（サイト内障害時時、大規模災害時）	サイト内障害もしくは大規模災害が発生した際、何をどこまで、どれ位で復旧させるかの目標。	RPO（目標復旧地点）	復旧不要	5営業日前の時点（週次バックアップからの復旧）	1営業日前の時点（日次バックアップからの復旧）	障害発生時点（日次バックアップ+アーカイブからの復旧）			■定義内容 【サイト内障害】 障害発生時点（日次バックアップ+アーカイブからの復旧） 【大規模災害】 1営業日前の時点（日次バックアップからの復旧）	【メトリクス】 RLOで業務の復旧までを指定している場合、該当する業務のデータの復旧までが対象であり、業務再開の整合性の確認は別途必要となる。 【レベル3】 障害発生時点とは、障害が発生する直前のトランザクションなどの処理が完了している時点のことを指し、障害発生時点まで復旧するためには、発生直前の完了した処理のジャーナルログが保証されていることが前提となる。またジャーナルログをアーカイブすることで、障害発生までの任意の時点への復旧に対応することを想定している。
A.1.3.2					RTO（目標復旧時間）	1営業日以上	1営業日以内	12時間以内	6時間以内	2時間以内		【サイト内障害】 2時間以内 ※各サイト業務停止時に「性能100%」の状態に復旧するまでの時間。 ※2台両現用構成のうち1台のみ稼動している状態は「性能100%」に含む。 【大規模災害】 2時間以内 ※バックアップサイトへ切り替わるまでの時間	【メトリクス】 サービス切替時間（A.1.2.2）での復旧時間と異なり、RTOでの復旧時間は、業務の継続対策を実施していない（業務停止となる）ケースでの障害での復旧時間を指している。 RLOで業務の復旧までを指定している場合、該当する業務のデータの復旧までが対象であり、業務再開の整合性の確認は別途必要となる。
A.1.3.3					RLO（目標復旧レベル）	システムの復旧	特定業務のみ	全ての業務				■定義内容 【サイト内障害、大規模災害ともに】 全ての業務 業務の提供に間接的に関連するセキュリティ機能については対象範囲に含める。 業務の実施に直接関連しないバックアップ、監視等の運用系機能に関しては、対象外とする。	【メトリクス】 業務停止を伴う障害が発生した際、何を復旧の対象とするかのレベルを示す。 【レベル0】 システムの復旧は、ハードウェアの復旧だけでなくデータのリストアまでを対象とする。 【レベル1】 特定業務とは、例えばA.1.2.1対象業務範囲で定義する継続性が要求される業務などを指す。
A.1.4.1			システム再開目標	大規模災害が発生した際、どれ位で復旧させるかの目標。 大規模災害とは、火災や地震などの異常な自然現象、あるいは人為的な原因による大きな事故、破壊行為により生ずる被害のことを指し、システムに甚大な被害が発生するか、電力などのライフラインの停止により、システムをそのまま現状に修復するのが困難な状態となる災害をいう。	システム再開目標	再開不要	数ヶ月以内に再開	一ヶ月以内に再開	一週間以内に再開	3日以内に再開	1日以内に再開		■定義内容 1日以内に再開	【メトリクス】 大規模災害としては、RPO、RTO、RLOなどの細かな要求までは確定せず、システム再開目標として大まかな復旧時間を設定する。目標復旧レベルについては、業務停止時の目標復旧水準を参考とする。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
A.1.5.1			稼働率	明示された利用条件の下で、システムが要求されたサービスを提供できる割合。 明示された利用条件とは、運用スケジュールや、目標復旧水準により定義された業務が稼働している条件を指す。その稼働時間の中で、サービス中断が発生した時間により稼働率を求める。	稼働率	95%以下	95%	99%	99.9%	99.99%	99.999%	■定義内容 メインサイト　　：年間99.9% バックアップサイト　：年間99.9% ※以下の時間は稼働率算出の対象外とする。 ①計画停止時間 ②冗長構成のサーバのうち、片系のみが停止している時間 ③メインサイト正常運転時に、バックアップサイトにて発生した障害	【レベル】 24時間365日の稼働の場合、1年間で業務が中断する時間の合計は、それぞれ以下の通りとなる。 95%・・・・・・・・・18.3日 99%・・・・・・・・・87.6時間 99.9%・・・・・・・ 8.76時間 99.99%・・・・・・ 52.6分 99.999%・・・・・ 5.26分 また1日8時間で週5日稼働のシステムではサービス切替時間と稼働率の関係は以下の通りとなる。 週に1時間・・・・97.5% 月に1時間・・・・99.4% 年に1時間・・・・99.95%
A.2.1.1		耐障害性	サーバ	サーバで発生する障害に対して、要求されたサービスを維持するための要求。	冗長化（機器）	非冗長構成	特定のサーバで冗長化	全てのサーバで冗長化				■定義内容 【仮想サーバ】 特定のサーバで冗長化 業務に関わるサーバ、異常検知・通知を行うサーバ、セキュリティ機能を提供するサーバで冗長化を実施する。また、それぞれのサーバは異なるセグメントに配置する。 バックアップを行うサーバ及びリポジトリ管理を行うサーバについては、サービスに直接的に影響が無いため、冗長化を実施しない。 【クラウドサービス】 全てのクラウドサービスで冗長化 クラウドサービス事業者の責任範囲において、全てのクラウドサービスについて冗長化が実現されている。	【メトリクス】 冗長化における機器、コンポーネントは、冗長化の単位を表し、機器は筐体を複数用意することによる冗長化、コンポーネントは筐体を構成する部品（ディスク、電源、FAN、ネットワークカード等）を複数用意することによる冗長化を指す。 また、仮想化技術の適用により、同一ハードウェア上にサーバ機能を集約させることで、冗長化に必要なハードウェア所要量を削減することも可能である。いずれにしても、ハードウェア上で実現される業務継続性の要求を満たすよう機器の冗長化を検討する必要がある。 【レベル1】 特定のサーバで冗長化とは、システムを構成するサーバの種別（DBサーバやAPサーバ、監視サーバなど）で冗長化の対応を分けることを意味する。 また要求としてサーバの単位ではなく、業務や機能の単位で冗長化を指定する場合、それを実装するサーバを想定してレベルを設定する。
A.2.1.2					冗長化（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化				■定義内容 全てのコンポーネントを冗長化 クラウドサービス事業者の責任範囲において、全ての仮想サーバ・クラウドサービスに関するコンポーネントの冗長化が実現されている。	【レベル1】 サーバを構成するコンポーネントとして、内蔵ディスクや、電源、FANなどを必要に応じて冗長化することを想定している（例えば内蔵ディスクのミラー化や、ネットワークIFカードの2重化など）。
A.2.2.1			端末	端末で発生する障害に対して、要求されたサービスを維持するための要求。	冗長化（機器）	非冗長構成	共用の予備端末を設置	業務や用途毎に予備端末を設置				端末の導入予定はないため、対象外	
A.2.2.2					冗長化（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化				端末の導入予定はないため、対象外	【レベル1】 端末を構成するコンポーネントとして、内蔵ディスクや、電源、FANなどを必要に応じて冗長化することを想定している（例えば内蔵ディスクのRAID構成など）。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
A.2.3.1			ネットワーク機器	ルータやスイッチなどネットワークを構成する機器で発生する障害に対して、要求されたサービスを維持するための要求。	冗長化（機器）	非冗長構成	特定の機器のみ冗長化	全ての機器を冗長化				■定義内容 全ての機器を冗長化 クラウドサービス事業者の責任範囲において、全てのネットワーク機器の冗長化が実現されている。	【レベル1】 特定の機器のみとは、ネットワークを構成するルータやスイッチの内、冗長化したサーバを収容するスイッチなどを想定している。
A.2.3.2					冗長化（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化				■定義内容 全てのコンポーネントを冗長化 クラウドサービス事業者の責任範囲において、全てのネットワーク機器に関するコンポーネントの冗長化が実現されている。	【レベル1】 ネットワーク機器を構成するコンポーネントとして、電源やCPU、FANなどを必要に応じて冗長化することを想定している。
A.2.4.1			ネットワーク	ネットワークの信頼性を向上させるための要求。	回線の冗長化	冗長化しない	一部冗長化	全て冗長化する				■定義内容 全て冗長化する クラウドサービス事業者の責任範囲において、全てネットワークに関する回線の冗長化が実現されている。	【メトリクス】 回線の冗長化とは、ネットワークを構成する伝送路（例えばLANケーブルなど）を物理的に複数用意し、一方の伝送路で障害が発生しても他方での通信が可能な状態にすること。 【レベル1】 一部冗長化とは、基幹のネットワークのみ冗長化するケースや、業務データの流れるセグメントなどを想定している。
A.2.4.2					経路の冗長化	冗長化しない	一部冗長化	全て冗長化する				■定義内容 全て冗長化する クラウドサービス事業者の責任範囲において、全てネットワークに関する経路の冗長化が実現されている。	【メトリクス】 経路の冗長化とは、ネットワーク内でデータを送受信する対象間で、データの流れる順序（経由するルータの順序）を複数設定することで、ある区間で障害が発生しても、他の経路で迂回し通信を可能な状態にすること。 【レベル1】 一部冗長化とは、基幹のネットワークのみ冗長化するケースや、業務データの流れるセグメントなどを想定している。
A.2.4.3					セグメント分割	分割しない	サブシステム単位で分割	用途に応じて分割				■定義内容 用途に応じて分割 セキュリティの観点から、DMZセグメント・内部セグメントの分割を行う。 耐障害性の観点から、各サーバの片系は異なるセグメントとする。機能の観点から、クラウドサービス、ネットワーク機能、ファイル共有機能、データベース機能を別セグメントとする。	【レベル2】 用途とは、監視やバックアップなどの管理系の用途から、オンライン、バッチなどの業務別の用途を示している。 サブシステム単位で分割したなかで、更に用途に応じてセグメントを分割することを想定している。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
A.2.5.1			ストレージ	ディスクアレイなどの外部記憶装置で発生する障害に対して、要求されたサービスを維持するための要求。	冗長化（機器）	非冗長構成	特定の機器のみ冗長化	全ての機器を冗長化				■定義内容 全ての機器を冗長化 クラウドサービス事業者の責任範囲において、全てのストレージに関する機器の冗長化が実現されている。	【メトリクス】 NAS、iSCSI対応の装置を含む。 ただしNASやiSCSIはLANなどのネットワークに接続して利用するため、NASやiSCSIの接続環境の耐障害性対策は小項目A.2.4ネットワークに含まれる。 【レベル1】 特定の機器のみとは、導入するストレージ装置に格納するデータの重要度に応じて、耐障害性の要求が装置毎に異なる場合を想定している。
A.2.5.2					冗長化（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化				■定義内容 全てのコンポーネントを冗長化 クラウドサービス事業者の責任範囲において、全てのストレージに関するコンポーネントの冗長化が実現されている。	【レベル1】 ストレージを構成するコンポーネントとして、ディスクを除く、CPUや電源、FAN、インターフェースなどを必要に応じて冗長化することを想定している。
A.2.5.3					冗長化（ディスク）	非冗長構成	単一冗長	多重冗長				■定義内容 単一冗長 クラウドサービス事業者の責任範囲において、全てのストレージに関するディスクの冗長化が実現されている。	【レベル1】 単一冗長とは、単一箇所の障害であれば、サービス継続可能な冗長構成のことである。 【レベル2】 多重冗長とは、同時に複数の箇所が障害の状態となっても、サービス継続可能な冗長構成のことである。
A.2.6.1			データ	データの保護に対しての考え方。	バックアップ方式	バックアップ無し	オフラインバックアップ	オンラインバックアップ	オフラインバックアップ+オンラインバックアップ			■定義内容 オンラインバックアップ 原則として24時間・365日稼動のシステムであるため、オンラインバックアップを行う。	【重複項目】 C.1.2.7。バックアップ方式は、バックアップ運用設計を行う上で考慮する必要があり、運用・保守性と重複項目としている。 【レベル】 オフラインバックアップとは、システム（あるいはその一部）を停止させてバックアップを行う方式、オンラインバックアップとはシステムを停止せず稼働中の状態でバックアップを行う方式を指す。
A.2.6.2					データ復旧範囲	復旧不要	一部の必要なデータのみ復旧	システム内の全データを復旧				■定義内容 一部の必要なデータのみ復旧 業務継続性の要求を満たすために必要となるデータについて復旧を行う。	【重複項目】 C.1.2.1。可用性ではデータをどこまで保全するかという観点で、運用ではデータをどこまで復旧させるかという観点で本項目が必要となり、重複項目としている。 【レベル1】 一部の必要なデータとは、業務継続性の要求を満たすために必要となるようなデータを想定している。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
A.3.1.1		災害対策	システム	地震、水害、テロ、火災などの大規模災害時の業務継続性を満たすための要求。	復旧方針	復旧しない	限定された構成でシステムを再構築	同一の構成でシステムを再構築	限定された構成をDRサイトで構築	同一の構成をDRサイトで構築		■定義内容 同一の構成をDRサイトで構築	【メトリクス】 大規模災害のための代替の機器として、どこに何が必要かを決める項目。 【レベル】 レベル1および3の限定された構成とは、復旧する目標に応じて必要となる構成（例えば、冗長化の構成は省くなど）を意味する。 レベル2および4の同一の構成とは、復旧後も復旧前と同じサービスレベルを維持するため、本番環境と同一のシステム構成を必要とすることを意味する。 レベル1および2のシステムを再構築を選択する場合、被災後の再構築までを契約の範囲として考えるのではなく、被災したサイトあるいは共用センターなどの設備を利用して、あくまでシステムを再構築する方針とすることを要求するものである。 一方レベル3および4のDRサイトで構築は、指定されたDRサイトに復旧用のシステムを構築するところまでを含む。
A.3.2.1			外部保管データ	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、データ・プログラムを運用サイトと別の場所へ保管するなどの要求。	保管場所分散度	外部保管しない	1ヵ所	1ヵ所 (遠隔地)	2ヵ所 (遠隔地)			■定義内容 1ヵ所(遠隔地)	
A.3.2.2					保管方法	媒体による保管	同一サイト内の別ストレージへのバックアップ	DRサイトへのリモートバックアップ				■定義内容 DRサイトへのリモートバックアップ	
A.3.3.1			付帯設備	各種災害に対するシステムの付帯設備での要求。	災害対策範囲	対策を実施しない	特定の対策を実施する	想定する全ての対策を実施する				■定義内容 特定の対策を実施する クラウドサービス事業者の責任範囲において、各種災害に対する対策を実現している。	【メトリクス】 付帯設備については、システム環境・エコロジーにおいてF.4.1.1の耐震震度、F.4.4.4の停電対策で、災害対策の一部として要求を具体化している。 【レベル】 想定する災害対策としては、以下が考えられる。 ・地震対策 ・瞬電・停電対策 ・火災対策 ・漏電対策 ・雷対策 ・水害対策 ・電界・磁界対策

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
A.4.1.1		回復性	復旧作業	業務停止を伴う障害が発生した際の復旧作業に必要な労力。	復旧作業	復旧不要	復旧用製品は使用しない手作業の復旧	復旧用製品による復旧	復旧用製品＋業務アプリケーションによる復旧			■定義内容 復旧用製品による復旧 可能な限り復旧作業を簡便、確実に行うために復旧製品を使用した復旧を行う。 基本的にパブリッククラウドのネイティブのバックアップ・リカバリ機能を使用することを想定する。また、必要に応じて、サードパーティ製のバックアップソフトウェアを使用する。	【重複項目】 C.3.1.1。復旧作業は、可用性と運用・保守性に共通して含まれている。運用・保守性では、復旧目標の運用への影響という観点でその作業を確認するが、可用性は、それを実現するための手段として確認する。 【レベル】 自作ツールを利用するケースは手作業に含む。 復旧用製品とは、バックアップ・リカバリを行う製品を指す。復旧用製品による復旧を行う場合、どこまで自動化するか（自動リカバリー機能充足率など）を定義するケースもあるが、可用性としては、復旧用製品を使用するかしないかでギャップが発生するため、この観点でレベルを検討する。
A.4.1.2					代替業務運用の範囲	無し	一部の業務について代替業務運用が必要	全部の業務について代替業務運用が必要				■定義内容 一部の業務(※)について代替運用が可能 ※災害対策ホームページ、公開情報管理システムを使用し代替運用が可能。	【重複項目】 C.3.1.2。復旧作業は、可用性と運用・保守性に共通して含まれている。運用・保守性では、復旧目標の運用への影響という観点でその作業を確認するが、可用性は、それを実現するための手段として確認する。 【メトリクス】 代替業務運用とは、障害によりシステムが復旧不可能となった場合に、代替業務でカバーすることが可能な運用手段（代替機あるいは人手による運用）を指す。
A.4.2.1			可用性確認	可用性として要求された項目をどこまで確認するかの範囲。	確認範囲	実施しない。または単純な障害の範囲	業務を継続できる障害の範囲	業務停止となる障害のうち一部の範囲	業務停止となる障害の全ての範囲			■定義内容 業務を継続できる障害の範囲とする。 試験工程において、確認を行う。なおパブリッククラウドのため、物理機器の障害を模擬した確認を行うことはできないため、可能な範囲で擬似的な確認試験を実施する。	【レベル】 レベル2および3の確認範囲には、レベル1で定義した内容を含む。
B.1.1.1	性能・拡張性	業務処理量	通常時の業務量	性能・拡張性に影響を与える業務量。 該当システムの稼働時を想定し、合意する。 それぞれのメトリクスに於いて、単一の値だけでなく、前提となる時間帯や季節の特性なども考慮する。	ユーザ数	特定ユーザのみ	上限が決まっている	不特定多数のユーザが利用				■定義内容 上限が決まっている 　職員（編集）：36名 　職員（承認）：35名 　職員（その他）：9名 一般利用者：不特定多数	【重複項目】 F.2.1.1。ユーザ数は性能・拡張性を決めるための前提となる項目であると共にシステム環境を規定する項目でもあるため、性能・拡張性とシステム環境・エコロジーの両方に含まれている。 【レベル】 前提となる数値が決められない場合は、類似システムなどを参考に仮の値でも良いので決めておくことが必要。
B.1.1.2					同時アクセス数	特定利用者の限られたアクセスのみ	同時アクセスの上限が決まっている	不特定多数のアクセス有り				■定義内容 同時アクセスの上限が決まっている。 ※本システムでの同時アクセス数の理論上の上限は上述した「ユーザ数」の合計値であるが、ユーザ全員が同時に接続するケースは考えにくい。 そのため、同時アクセス数を「1秒当たりの処理件数」と定義し「B.2.3.1 B.2.3.2オンラインスループット」に記載の値を同時アクセス数として採用する。	【メトリクス】 同時アクセス数とは、ある時点でシステムにアクセスしているユーザ数のことである。
B.1.1.3					データ量	全てのデータ量が明確である	主要なデータ量のみが明確である					■定義内容 全てのデータ量が明確である	【レベル1】 主要なデータ量とは、システムが保持するデータの中で、多くを占めるデータのことを言う。 例えば、マスター系テーブルや主なトランザクションデータの一次保存分などがある。 主要なデータ量しか決まっていない場合、後工程に於いて、検討漏れデータの出現などによるディスク追加などが発生するリスクがある。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
B.1.1.4					オンラインリクエスト件数	処理毎にリクエスト件数が明確である	主な処理のリクエスト件数のみが明確である					■定義内容 処理毎にリクエスト件数が明確である	【メトリクス】 オンラインリクエスト件数は単位時間を明らかにして確認する。 【レベル1】 主な処理とはシステムが受け付けるオンラインリクエストの中で大部分を占めるものを言う。 例えば、住民情報システムの転入・転出処理やネットショッピングシステムの決済処理などがある。 主なリクエスト件数しか決まっていない場合、後工程に於いて、検討漏れリクエストの出現などによるサーバ能力不足などのリスクがある。
B.1.1.5					バッチ処理件数	処理単位毎に処理件数が決まっている	主な処理の処理件数が決まっている					■定義内容 処理単位毎に処理件数が決まっている	【メトリクス】 バッチ処理件数は単位時間を明らかにして確認する。要件定義時には主な処理（特に該当システムでクリティカルとなる処理）では処理件数のおおよその目安は決まっているはずであり、それを元に性能や拡張性の検討を進める。要件定義時に明確になっていない場合は、確定度合も含め、想定しておく。 【レベル1】 主な処理とはシステムが実行するバッチ処理の中で大部分の時間を占める物をいう。 例えば、人事給与システムや料金計算システムの月次集計処理などがある。 主なバッチ処理件数しか決まっていない場合、後工程に於いて、検討漏れ処理の出現などによるサーバ能力不足などのリスクがある。
B.1.1.6					業務機能数	業務機能が整理されている	確定した業務機能一覧が作成されている	業務機能一覧はあるが、確定していない				■定義内容 確定した業務機能一覧が作成されている	【メトリクス】 要件定義時には業務機能一覧はレベルの差があっても決まっているはずであり、それを元に性能や拡張性の検討を進める。要件定義時に明確になっていない場合は、確定度合も含め、想定しておく。
B.1.2.1			業務量増大度	システム稼動開始からライフサイクル終了までの間で、開始時点と業務量が最大になる時点の業務量の倍率。 必要に応じ、開始日の平均値や、開始後の定常状態との比較を行う場合もある。	ユーザ数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	■定義内容 1倍（サービス開始時点から増大しない）	【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。
B.1.2.2					同時アクセス数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	■定義内容 1倍（サービス開始時点から増大しない）	【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。
B.1.2.3					データ量増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	■定義内容 コンテンツ：年間100～200MB増加する	【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。
B.1.2.4					オンラインリクエスト件数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	■定義内容 1倍（サービス開始時点から増大しない）	【メトリクス】 オンラインリクエスト件数は単位時間を明らかにして確認する。 【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
B.1.2.5					バッチ処理件数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	■定義内容 1倍（サービス開始時点から増大しない）	【メトリクス】 バッチ処理件数は単位時間を明らかにして確認する。 【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。
B.1.2.6					業務機能数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	■定義内容 1倍（サービス開始時点から増大しない）	【レベル】 業務機能数増大率を評価する際は、機能の粒度（1機能あたりの見積規模、サービス範囲など）は具体的数値を示すことが望ましい。 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。
B.1.3.1			保管期間	システムが参照するデータのうち、OSやミドルウェアのログなどのシステム基盤が利用するデータに対する保管が必要な期間。 必要に応じて、データの種別毎に定める。 保管対象のデータを選択する際には、対象範囲についても決めておく。	保管期間	6ヶ月	1年	3年	5年	10年以上有期	永久保管	■定義内容 5年（2026年2月カットオーバ～2031年1月31日）	【レベル】 対象が複数あり、それぞれの保管期間が異なる場合は、それぞれの対象データについて決めること。 【レベル0】 保管期間の制約が短い場合は6ヶ月で代用する。
B.1.3.2					対象範囲	オンラインで参照できる範囲	アーカイブまで含める					■定義内容 一部データにオンラインで参照できる期間に制限があるが、システム内には「保管期間」の間保管する。	【メトリクス】 保管対象のデータを配置する場所を決める。保管場所によっては参照するための手間がかかる場合がある。また、バックアップの取得方法などへの配慮が必要になる。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
B.2.1.1		性能目標値	オンラインレスポンス	オンラインシステム利用時に要求されるレスポンス。 システム化する対象業務の特性をふまえ、どの程度のレスポンスが必要かについて確認する。ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に順守率を決める。具体的な数値は特定の機能またはシステム分類毎に決めておくことが望ましい。（例：Webシステムの参照系/更新系/一覧系など）	通常時レスポンス順守率	順守率を定めない	60%	80%	90%	95%	99%以上	■定義内容 90%以上 ※対象は公開情報の利用のうち以下の画面を対象と想定するが、測定時に原子力規制庁担当官と協議すること ・静的サイト閲覧 ・N-ADRES参照サイト閲覧 ・検索 また、ネットワークの影響を除いた値とする。	【レベル】 具体的な目標値や約束値がある場合、各処理の順守率を規定する。 レベルに示した順守率はおおまかな目安を示しており、具体的にはレスポンスと順守率について数値で合意する必要がある。
B.2.1.2					ピーク時レスポンス順守率	順守率を定めない	60%	80%	90%	95%	99%以上	■定義内容 80%以上 ※対象は公開情報の利用のうち以下の画面を対象と想定するが、測定時に原子力規制庁担当官と協議すること ・静的サイト閲覧 ・N-ADRES参照サイト閲覧 ・検索 また、ネットワークの影響を除いた値とする。	【レベル】 具体的な目標値や約束値がある場合、各処理の順守率を規定する。 レベルに示した順守率はおおまかな目安を示しており、具体的にはレスポンスと順守率について数値で合意する必要がある。
B.2.2.1			バッチレスポンス（ターンアラウンドタイム）	バッチシステム利用時に要求されるレスポンス。 システム化する対象業務の特性をふまえ、どの程度のレスポンス（ターンアラウンドタイム）が必要かについて確認する。更に、ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に順守率を決める、具体的な数値は特定の機能またはシステム分類毎に決めておくことが望ましい。 （例：日次処理/月次処理/年次処理など）	通常時レスポンス順守度合い	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				■定義内容 再実行の余裕が確保できる ※バッチ処理における「完了」とは、「処理結果画面に表示されること」とする。 ※ファイル一括登録処理は日中帯に実行される処理であるため、オンライン業務量が「通常時」のみ保証する時間とする。	【レベル1】 所定の時間には再実行は含まない。
B.2.2.2					ピーク時レスポンス順守度合い	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				■定義内容 再実行の余裕が確保できる ※バッチ処理における「完了」とは、「処理結果画面に表示されること」とする。 ※ファイル一括登録処理は日中帯に実行される処理であるため、オンライン業務量が「通常時」のみ保証する時間とする。	【レベル1】 所定の時間には再実行は含まない。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
B.2.3.1			オンラインスループット	オンラインシステム利用時に要求されるスループット。システム化する対象業務の特性をふまえ、単位時間にどれだけの量の作業ができるかを確認する。更に、ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に処理余裕率を決める、具体的な数値は特定の機能またはシステム分類毎に決めておくことが望ましい。 （例：データエントリ件数/時間、頁めくり回数/分、TPSなど）	通常時処理余裕率	1倍 (余裕無し)	1.2倍	1.5倍	2倍	3倍	10倍以上	■定義内容 ・通常時 　30アクセス/秒 ※対象は外部向けオンライン業務、内部向けオンライン業務のうち以下の画面を対象とする ・トップページ ・検索結果画面 ・コンテンツ詳細画面 ※1PV=10アクセス とする。	【レベル】 ここでの余裕率は、システム全体で処理できるトランザクション量を示す。例えば、レベル3（2倍）であれば、2倍のトランザクションを処理できることを言う。 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。
B.2.3.2					ピーク時処理余裕率	1倍 (余裕無し)	1.2倍	1.5倍	2倍	3倍	10倍以上	■定義内容 ・通常時 　30アクセス/秒 ※対象は外部向けオンライン業務、内部向けオンライン業務のうち以下の画面を対象とする ・トップページ ・検索結果画面 ・コンテンツ詳細画面 ※1PV=10アクセス とする。	【レベル】 ここでの余裕率は、システム全体で処理できるトランザクション量を示す。例えば、レベル3（2倍）であれば、2倍のトランザクションを処理できることを言う。 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
B.2.4.1			バッチスループット	バッチシステム利用時に要求されるスループット。 システム化する対象業務の特性をふまえ、どの程度のスループットを確保すべきか確認する。更に、ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に処理余裕率を決める。具体的な数値は特定の機能またはシステム分類毎に決めておくことが望ましい。 （例：人事異動情報一括更新処理、一括メール送信処理など）	通常時処理余裕率	1倍 (余裕無し)	1.2倍	1.5倍	2倍	3倍	10倍以上	■定義内容 目標値：10分以内	【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。
B.2.4.2					ピーク時処理余裕率	1倍 (余裕無し)	1.2倍	1.5倍	2倍	3倍	10倍以上	■定義内容 目標値：10分以内	【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。
B.2.5.1			帳票印刷能力	帳票印刷に要求されるスループット。 業務で必要な帳票の出力時期や枚数を考慮し、どの程度のスループットが必要かを確認する。 更に、ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に余裕率を決める。具体的な数値は特定の帳票や機能毎に決めておくことが望ましい。	通常時印刷余裕率	1倍 （余裕無し）	1.2倍	1.5倍	2倍	3倍	10倍以上	印刷処理は存在しないため対象外。	【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。
B.2.5.2					ピーク時印刷余裕率	1倍 （余裕無し）	1.2倍	1.5倍	2倍	3倍	10倍以上	印刷処理は存在しないため対象外。	【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
B.3.1.1		リソース拡張性	CPU拡張性	CPUの拡張性を確認するための項目。 CPU利用率は、将来の業務量の増加に備え、どれだけCPUに余裕をもたせておくかを確認するための項目。 CPU拡張性は、物理的もしくは仮想的に、どれだけCPUを拡張できるようにしておくかを確認するための項目。 CPUの専有の有無については「B.4.1 HWリソース専有の有無」で確認する。	CPU利用率	80%以上	50%以上 80%未満	20%以上 50%未満	20%未満			■定義内容 『レスポンス・スループット等の業務量の増加に応じてスケールアップ、またはスケールアウトの方法を用いて柔軟に拡張できること』	【メトリクス】 CPU利用率は単位時間に、実行中のプログラムがCPUを使用している割合を示している。単位時間をどの程度にするか、また、動作するプログラムの特性によって数値は大きく異なる。 【レベル】 レベルに示した利用率はおおまかな目安を示しており、具体的な数値で合意する必要がある。 【運用コストへの影響】 CPU利用率が大きい場合、少しの業務量増大で機器増設などの対策が必要になる。
B.3.1.2					CPU拡張性	1倍 （拡張要求なし）	1.5倍の拡張が可能	2倍の拡張が可能	4倍の拡張が可能	8倍以上の拡張が可能		同上	【運用コストへの影響】 CPU拡張性がない場合、機器自体の増設や、環境や契約の変更が必要になる場合がある。
B.3.2.1			メモリ拡張性	メモリの拡張性を確認するための項目。 メモリ利用率は、将来の業務量の増加に備え、どれだけメモリに余裕をもたせておくかを確認するための項目。 メモリ拡張性は、物理的もしくは仮想的に、どれだけメモリを拡張できるようにしておくかを確認するための項目。 メモリの専有の有無については「B.4.1 HWリソース専有の有無」で確認する。	メモリ利用率	80%以上	50%以上 80%未満	20%以上 50%未満	20%未満			同上	【メトリクス】 メモリ利用率は単位時間に、実行中のプログラムがメモリを使用している割合を示している。単位時間をどの程度にするか、また、動作するプログラムの特性によって数値は大きく異なる。 【レベル】 レベルに示した利用率はおおまかな目安を示しており、具体的な数値で合意する必要がある。 【運用コストへの影響】 メモリ利用率が大きい場合、少しの業務量増大でメモリや機器の増設が必要になる。
B.3.2.2					メモリ拡張性	1倍 （拡張要求なし）	1.5倍の拡張が可能	2倍の拡張が可能	4倍の拡張が可能	8倍以上の拡張が可能		同上	【運用コストへの影響】 メモリ拡張性がない場合、機器自体の増設や、環境や契約の変更が必要になる場合がある。
B.3.3.1			ディスク拡張性	ディスクの拡張性を確認するための項目。 ディスク利用率は、将来の業務量の増加に備え、どれだけディスクに余裕をもたせておくかを確認するための項目。 ディスク拡張性は、物理的もしくは仮想的に、どれだけディスクを拡張できるようにしておくかを確認するための項目。	ディスク利用率	80%以上	50%以上 80%未満	20%以上 50%未満	20%未満			同上	【レベル】 レベルに示した利用率はおおまかな目安を示しており、具体的な数値で合意する必要がある。 【運用コストへの影響】 ディスクに空きが無い場合、単純増加ファイルの監視等が必要になる。
B.3.3.2					ディスク拡張性	1倍 （拡張要求なし）	1.5倍の拡張が可能	2倍の拡張が可能	4倍の拡張が可能	8倍以上の拡張が可能		同上	【運用コストへの影響】 ディスク拡張性がない場合、機器自体の増設や、環境や契約の変更が必要になる場合がある。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
B.3.4.1			ネットワーク	システムで使用するネットワーク環境の拡張性に関する項目。 既存のネットワーク機器を活用する場合は既存ネットワークの要件を確認するために利用する。 ネットワークの帯域については「B.4.1 帯域保証機能の有無」で確認する。	ネットワーク機器設置範囲	無し	フロア内のLAN	同一拠点(ビル)内のLAN	社内複数拠点間の接続(LAN、WAN)	社外拠点との接続		同上	
B.3.5.1			サーバ処理能力増強	サーバ処理能力増強方法に関する項目。 将来の業務量増大に備える方法（スケールアップ/スケールアウト）をあらかじめ考慮しておくこと。どちらの方法を選択するかはシステムの特徴によって使い分けることが必要。 スケールアップは、より処理能力の大きなサーバとの入れ替えを行うことで処理能力の増強を行う。 スケールアウトは同等のサーバを複数台用意し、サーバ台数を増やすことで処理能力の増強を行う。	スケールアップ	スケールアップを行わない	一部のサーバのみを対象	複数のサーバを対象				同上	【メトリクス】 あらかじめ余剰リソースを用意しておくことで速やかにスケールアップを行う等、スケールアップの迅速性についても検討する。 また、スケールアップしている状態は、コスト増に繋がる場合があるため、必要に応じてスケールダウンの迅速性についても考慮する。 【レベル1】 オンライントランザクション処理のような更新系の割合が多いシステムでアプリケーションサーバをスケールアップする場合を想定。 【レベル2】 レベル1に加え、DBサーバのスケールアップを追加する場合を想定。
B.3.5.2					スケールアウト	スケールアウトを行わない	一部のサーバのみを対象	複数のサーバを対象				同上	【メトリクス】 スケールアップと同様、スケールアウトの迅速性についても検討する。 また、必要に応じて、スケールインの迅速性についても検討する。 【レベル1】 Webサーバと負荷分散装置などフロント部分を複数台用意する場合を想定。 【レベル2】 レベル1に加え、バックエンドのサーバを複数台用意する場合を想定。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
B.4.1.1		性能品質保証	帯域保証機能の有無	ネットワークのサービス品質を保証する機能の導入要否およびその程度。 伝送遅延時間、パケット損失率、帯域幅をなんらかの仕組みで決めているかを示す。回線の帯域が保証されていない場合性能悪化につながることがある。	帯域保証の設定	無し	プロトコル単位で設定	各サーバ毎に設定	アプリケーションのエンドツーエンドで検証・保証			同上	
B.4.1.2			HWリソース専有の有無	サーバのリソース（CPUやメモリ）を専有するか、共有するかを示す。HWリソースを他のサーバと共有する場合、他のサーバの影響を受けて、性能悪化につながることがある。	HWリソース専有の設定	無し（共有）	有り（専有）					同上	
B.4.2.1			性能テスト	構築したシステムが当初/ライフサイクルに渡っての性能を発揮できるかのテストの測定頻度と範囲。	測定頻度	測定しない	構築当初に測定	運用中、必要時に測定可能	運用中、定常的に測定			■定義内容 構築当初に測定 試験内で実施する。	
B.4.2.2					確認範囲	確認しない	一部の機能について、目標値を満たしていることを確認	全ての機能について、目標値を満たしていることを確認				■定義内容 対象の機能について、目標値を満たしていることを確認 性能テストにおけるテストモデル、テストデータについては、試験計画時に規制/庁様と合意すること。	
B.4.3.1			スパイク負荷対応	通常時の負荷と比較して、非常に大きな負荷が短時間に現れることを指す。業務量の想定されたピークを超えた状態。 特にB2Cシステムなどクライアント数を制限できないシステムで発生する。システムの処理上限を超えることが多いため、Sorry動作を実装し対策する場合が多い。	トランザクション保護	トランザクション保護は不要である	同時トランザクション数の制限機能	同時トランザクション数の制限機能に加え、Sorry動作	独立したSorry動作を行うサーバの設置			■定義内容 同時トランザクション数の制限機能	
C.1.1.1	運用・保守性	通常運用	運用時間	システム運用を行う時間。利用者やシステム管理者に対してサービスを提供するために、システムを稼動させ、オンライン処理やバッチ処理を実行している時間帯のこと。	運用時間（通常）	規定無し	定時内（9時～17時）	夜間のみ停止（9時～21時）	1時間程度の停止有り（9時～翌朝8時55分）	若干の停止有り（9時～翌朝8時）	24時間無停止	「A.1.1.1 運用時間（通常）」にて定義する。	【重複項目】 A.1.1.1。運用時間（通常）は、システムの可用性の実現レベルを表す項目でもあるため、重複項目となっている。 【メトリクス】 運用時間は、オンライン/バッチを含みシステムが稼動している時間帯を指す。 【レベル】 （）内の時間は各レベルの一例を示したもので、レベル選定の条件とはしていない。規定無しは、固定のサービス時間が存在しないことを示し、基本的にシステムは停止していて、必要に応じてユーザがシステムを起動するようなケースを想定している（例：障害発生に備えた予備システム、開発・検証用システム等）。定時内や夜間のみ停止は、一般的な業務形態を想定したもので、業務が稼動する時間帯が異なるシステムにおいては、時間帯をスライドさせるなどの読替えが必要である。停止有りとは、システムを停止しなければならない時間帯ではなく、システムを停止できる可能性のある時間帯を指す。24時間無停止は、オンライン業務が稼動していない時間にバッチを稼動させる必要があり、システムを停止することができないようなケースも含まれる。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
C.1.1.2					運用時間（特定日）	規定無し	定時内（9時～17時）	夜間のみ停止（9時～21時）	1時間程度の停止有り（9時～翌朝8時）	若干の停止有り（9時～翌朝8時55分）	24時間無停止	「A.1.1.2 運用時間（特定日）」にて定義する。	【重複項目】 A.1.1.2。運用時間（特定日）は、システムの可用性の実現レベルを表す項目でもあるため、重複項目となっている。 【メトリクス】 特定日とは、休日/祝祭日や月末月初など通常の運用スケジュールとは異なるスケジュールを定義している日のことを指す。特定日が複数存在する場合は、それぞれにおいてレベル値を整合する必要がある（例：「月～金はレベル2だが、土日はレベル0」、「通常はレベル5だが、毎月1日にリブートをするためその日はレベル3」など）。 また、ユーザの休日だけでなく、ベンダの休日についても特定日として認識し、運用保守体制等を整合すること。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
C.1.2.1			バックアップ	システムが利用するデータのバックアップに関する項目。	データ復旧範囲	復旧不要	一部の必要なデータのみ復旧	システム内の全データを復旧				■定義内容 一部の必要なデータのみ復旧 具体的には、業務データ、システムデータを復旧対象のデータとする。	【重複項目】 A.2.6.2。可用性ではデータをどこまで保全するかという観点で、運用ではデータをどこまで復旧させるかという観点で本項目が必要となり、重複項目としている。 【メトリクス】 システムを障害から復旧するためには、データバックアップ以外に、OSやアプリケーションの設定ファイル等を保管するシステムバックアップも必要となることが考えられる。システムバックアップの取得方法や保管方法についても、同時に検討すべきである。 【レベル1】 一部の必要なデータとは、業務継続性の要求を満たすために必要となるようなデータを想定している。
C.1.2.2					外部データの利用可否	全データの復旧に利用できる	一部のデータ復旧に利用できる	外部データは利用できない				■定義内容 一部のデータ復旧に利用できる	【メトリクス】 外部データとは、当該システムの範囲外に存在するシステムの保有するデータを指す（開発対象のシステムと連携する既存システムなど）。外部データによりシステムのデータが復旧可能な場合、システムにおいてバックアップ設計を行う必要性が減るため、検討の優先度やレベルを下げて考えることができる。
C.1.2.3					バックアップ利用範囲	バックアップを取得しない	障害発生時のデータ損失防止	ユーザエラーからの回復	データの長期保存（アーカイブ）			■定義内容 障害発生時のデータ損失からの回復に加え、セキュリティ侵害等によるデータ汚染からの回復に利用する。	【メトリクス】 マルウェア等によるデータ損失への備えや、監査のためのログの退避など、セキュリティ観点のバックアップも考慮すること。 【レベル2】 ユーザエラーからの回復の場合、システムとしては正常に完了してしまった処理を元に戻さなければならないため、複数世代のバックアップの管理や時間指定回復（Point in Time Recovery）等の機能が必要となる場合が考えられる。
C.1.2.4					バックアップ自動化の範囲	全ステップを手動で行う	一部のステップを手動で行う	全ステップを自動で行う				■定義内容 全ステップを自動で行う	【メトリクス】 バックアップ運用には、 ・スケジュールに基づくジョブ起動 ・バックアップ対象の選択 ・バックアップ先の選択 ・ファイル転送 などといった作業ステップが存在する。 【運用コストへの影響】 バックアップ運用の自動化を実現するためには、ハードウェア・ソフトウェアに対する投資が必要となり導入コストは増大する。しかし、運用中におけるバックアップ作業をユーザが実施する必要がなくなるため、その分運用コストは減少すると考えられる。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
C.1.2.5					バックアップ取得間隔	バックアップを取得しない	システム構成の変更時など、任意のタイミング	月次で取得	週次で取得	日次で取得	同期バックアップ	■定義内容 業務データ：日次 システムデータ：随時（システムの初期構築時、環境変更作業時）、月次 ログデータ：日次	
C.1.2.6					バックアップ保存期間	バックアップを保存しない	1年未満	3年	5年	10年以上有限	永久保存	■定義内容 5年	【メトリクス】 主に可用性の観点で実施されるバックアップの世代管理とは別に、ここではデータ保全という観点でバックアップデータの保存期間を検討する。
C.1.2.7					バックアップ方式	バックアップ無し	オフラインバックアップ	オンラインバックアップ	オフラインバックアップ+オンラインバックアップ			「A.2.6.1 バックアップ方式」にて定義する。	【重複項目】 A.2.6.1。バックアップ方式は、システムを停止するかどうかの検討が含まれるため、可用性の観点でも考慮する必要があり、重複項目となっている。 【レベル】 オフラインバックアップとは、システム（あるいはその一部）を停止させてバックアップを行う方式、オンラインバックアップとはシステムを停止せず稼働中の状態でバックアップを行う方式を指す。
C.1.3.1			運用監視	システム全体、あるいはそれを構成するハードウェア・ソフトウェア（業務アプリケーションを含む）に対する監視に関する項目。 セキュリティ監視については本項目には含めない。 「E.7.1 不正監視」で別途検討すること。	監視情報	監視を行わない	死活監視を行う	エラー監視を行う	エラー監視（トレース情報を含む）を行う	リソース監視を行う	パフォーマンス監視を行う	■定義内容 ○監視対象 ・エラー監視（ログ等に含まれるエラーを監視） ・プロセス監視（仮想マシン上で稼動するプロセスを監視） ・リソース監視（CPUやメモリ等のリソースの使用状況を監視） ・ジョブ監視（ジョブの実行状態を監視） ・Web応答監視（Webページが応答することを監視） ・死活監視（仮想マシン及びクラウドサービスの健全性を監視） ○監視間隔 リアルタイム監視 ○通知方法 メール通知	【メトリクス】 監視とは情報収集を行った結果に応じて適切な宛先に発報することを意味する。本項目は、監視対象としてどのような情報を発信するべきかを決定することを目的としている。また、監視情報の発報先については、「C.4.5.2 監視システムの有無」で確認すること。 【レベル】 死活監視とは、対象のステータスがオンラインの状態にあるかオフラインの状態にあるかを判断する監視のこと。 エラー監視とは、対象が出力するログ等にエラー出力が含まれているかどうかを判断する監視のこと。トレース情報を含む場合は、どのモジュールでエラーが発生しているのか詳細についても判断することができる。 リソース監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいてCPUやメモリ、ディスク、ネットワーク帯域といったリソースの使用状況を判断する監視のこと。 パフォーマンス監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいて、業務アプリケーションやディスク I/O、ネットワーク転送等の応答時間やスループットについて判断する監視のこと。 【運用コストへの影響】 エラー監視やリソース監視、パフォーマンス監視を行うことによって、障害原因の追求が容易となったり、障害を未然に防止できるなど、システムの品質を維持するための運用コストが下がる。
C.1.3.2					監視間隔	監視を行わない	不定期監視（手動監視）	定期監視（1日間隔）	定期監視（数時間間隔）	リアルタイム監視（分間隔）	リアルタイム監視（秒間隔）		
C.1.3.3					システムレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 システムレベルの監視とは、業務アプリケーションも含め、そのシステムを構成する複数のサーバ等の状態確認結果から、システムとして機能する状態にあるかどうかを判断するものである。バックアップの監視やジョブの監視などが該当する。 【レベル】 監視を行う場合には、システムレベルについての監視情報と監視間隔を個別に確認する必要がある。システムが提供するいくつかの機能のうち、重要度の高い一部の機能のみを対象に監視を行うことを想定している。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
C.1.3.4					プロセスレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 プロセスレベルの監視とは、アプリケーションやミドルウェア等のプロセスが正しく機能しているかどうかを判断するものである。主にOSコマンドによるプロセスの情報（死活、CPU使用率、メモリ使用率など）を監視するものを想定している。 【レベル】 監視を行う場合は、プロセスレベルについての監視情報と監視間隔を個別に確認する必要がある。レベル1の一部とは、システム上で稼動する複数のプロセス（アプリケーションおよびミドルウェア）のうち、重要度の高い一部のプロセスのみを対象に監視を行うことを想定している。
C.1.3.5					データベースレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 データベースレベルの監視とは、DBMSの機能として提供される情報を確認し、正しく機能しているかを判断するものである。ログ出力内容やパラメータ値、ステータス情報、領域使用率等の監視を想定している。 【レベル】 監視を行う場合は、データベースレベルについての監視情報と監視間隔を個別に確認する必要がある。レベル1の一部とは、システム上で稼動する複数のデータベースのうち、重要度の高い一部のデータベースのみを対象に監視を行うことを想定している。
C.1.3.6					ストレージレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 ストレージレベルの監視とは、ディスクアレイ等の外部記憶装置に関して、状態を確認し、正しく機能しているかを判断するものである。OSコマンドによって確認できるディスク使用率等の他、ファームウェアが出力するログ情報などの監視を想定している。 【レベル】 監視を行う場合は、ストレージレベルについての監視情報と監視間隔を個別に確認する必要がある。 レベル1の一部とは、システムに接続される複数のストレージのうち、重要度の高い一部のストレージのみを対象に監視を行うことを想定している。
C.1.3.7					サーバ（ノード）レベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 サーバ（ノード）レベルの監視とは、対象のサーバがOSレベルで正しく機能しているかを判断するものである。ハートビート監視などが該当する。 【レベル】 監視を行う場合は、サーバ（ノード）レベルについての監視情報と監視間隔を個別に確認する必要がある。レベル1の一部とは、システム上に存在する複数のサーバ（ノード）のうち、重要度の高い一部のサーバのみを対象に監視を行うことを想定している。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
C.1.3.8					端末/ネットワーク機器レベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 端末/ネットワーク機器レベルの監視とは、クライアント端末やルータ等のネットワーク機器に関して、状態を確認し、正しく機能しているかを判断するものである。ハートビート監視の他、個別のファームウェア等が出力する情報に基づく監視などを想定している。 【レベル】 監視を行う場合は、端末/ネットワーク機器レベルについての監視情報と監視間隔を個別に確認する必要がある。レベル1の一部とは、システム上に存在する複数の端末/ネットワーク機器のうち、重要度の高い一部の端末/ネットワーク機器のみを対象に監視を行うことを想定している。
C.1.3.9					ネットワーク・パケットレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 ネットワーク・パケットレベルの監視とは、ネットワーク上を流れるパケットの情報を確認し、正しく機能しているかを判断するものである。パケットロスやネットワーク帯域の使用率などの監視などを想定している。 【レベル】 監視を行う場合は、ネットワーク・パケットレベルについての監視情報と監視間隔を個別に確認する必要がある。レベル1の一部とは、システム上の複数のネットワーク経路のうち、重要度の高い一部のネットワーク経路のみを対象に監視を行うことを想定している。
C.1.4.1			時刻同期	システムを構成する機器の時刻同期に関する項目。	時刻同期設定の範囲	時刻同期を行わない	サーバ機器のみ時刻同期を行う	サーバおよびクライアント機器について時刻同期を行う	ネットワーク機器も含めシステム全体で時刻同期を行う	システム全体を外部の標準時間と同期する		■定義内容 システム全体を外部の標準時間と同期する	【レベル4】 システム全体を外部の標準時間と同期する場合、外部との接続に異常が発生した場合にシステム内の時刻同期をどうするかといった設計を行う必要がある。 【運用コストへの影響】 時刻同期を行うことで、複数のサーバ機器が出力するログの順序保証が得られるため、障害調査や監査等の作業コストを下げられる可能性がある。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
C.2.1.1		保守運用	計画停止	点検作業や領域拡張、デフラグ、マスターデータのメンテナンス等、システムの保守作業の実施を目的とした、事前計画済みのサービス停止に関する項目。	計画停止の有無	計画停止有り（運用スケジュールの変更可）	計画停止有り（運用スケジュールの変更不可）	計画停止無し				■定義内容 計画停止有り（運用スケジュールの変更可） ・セキュリティパッチ適用作業やクラウドサービス側のメンテナンス作業等が発生する可能性がある。 ・事前の調整を行った上でシステムを停止することは可能であると考える。	【重複項目】 A.1.1.3。計画停止の有無は、システムの可用性の実現レベルを表す項目でもあるため、重複項目となっている。 【運用コストへの影響】 計画停止有りの場合、事前のバックアップや、システム構成に応じた手順準備など、運用時のコストがかさむ。
C.2.1.2					計画停止の事前アナウンス	計画停止が存在しない	計画停止は年間計画によって確定する	1ヶ月前に通知	1週間前に通知	前日に通知		■定義内容 運用保守報告会の場で翌月の計画停止予定を報告する。 ※緊急メンテナンス実施する際には適宜調整する。	【運用コストへの影響】 計画停止が存在する場合、利用者への通知や運用スケジュールの変更など、イレギュラーな対応が発生する。それらを短時間で実現しなければならないほど、システムの例外処理に対する作り込みを慎重に実施する必要があると考えられ、導入コストが増大すると考えられる。一方、運用コストに関してはその作り込みによって例外処理に対する運用が簡略化されるため減少すると考えられる。
C.2.2.1			運用負荷削減	保守運用に関する作業負荷を削減するための設計に関する項目。	保守作業自動化の範囲	保守作業は全て手動で実施する	一部の保守作業を自動で実行する	全ての保守作業を自動で実行する				■定義内容 運用コストの低減が見込める処理を自動化する	【メトリクス】 保守作業とは、保守運用に伴うシステム基盤を維持管理するための作業を指し、点検作業やパッチ適用等のアップデート作業、領域拡張、デフラグ、ログローテート等を想定している。障害対応や復旧作業などは含まない。 【運用コストへの影響】 システム基盤の保守運用作業を自動化するためには、特別な運用管理ツールを導入したり、さまざまな作り込みを実施する必要がある。そのため導入コストは増大するが、ユーザが実施すべき保守運用作業が簡略化あるいはなくなると考えられるので、運用コストは減少する。
C.2.2.2					サーバソフトウェア更新作業の自動化	サーバへの更新ファイル配布機能を実装しない	サーバへの更新ファイル配布機能を実装し、手動にて配布と更新処理を実行する	サーバへの更新ファイル配布機能を実装し、自動で配布したのち、更新処理を手動で実行する	サーバへの更新ファイル配布機能を実装し、配布と更新処理を自動で実行する			■定義内容 運用コストの低減が見込めるソフトウェアについて、配布及び更新処理を自動化する。	【メトリクス】 サーバソフトウェアとは、サーバ機器のOSやストレージのファームウェア、サーバ機器上で動作するミドルウェアやアプリケーションを指す。 【運用コストへの影響】 サーバへの更新ファイルの配布や更新処理を自動化するためには、特別なツールを導入したり作り込みを実施する必要があるため導入コストは増大する。一方、サーバソフトウェアの更新作業が自動化されることでユーザが運用中に実施すべき作業がなくなり、運用コストは減少する。
C.2.2.3					端末ソフトウェア更新作業の自動化	端末への更新ファイル配布機能を実装しない	端末への更新ファイル配布機能を実装し、手動にて配布と更新処理を実行する	端末への更新ファイル配布機能を実装し、自動で配布したのち、更新処理を手動で実行する	端末への更新ファイル配布機能を実装し、配布と更新処理を自動で実行する			端末なし	【メトリクス】 端末ソフトウェアとは、クライアント端末のOSやネットワーク機器のファームウェア、クライアント端末上で動作するアプリケーションを指す。 【運用コストへの影響】 端末への更新ファイルの配布や更新処理を自動化するためには、特別なツールを導入したり作り込みを実施する必要があるため導入コストは増大する。一方、端末の更新作業が自動化されることでユーザが運用中に実施すべき作業がなくなり、運用コストは減少する。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
C.2.3.1			パッチ適用ポリシー	パッチ情報の展開とパッチ適用のポリシーに関する項目。	パッチリリース情報の提供	ユーザの要求に応じてベンダが受動的にパッチリリース情報を提供する	ベンダが定期的にユーザへパッチリリース情報を提供する	ベンダがリアルタイムに（パッチリリースと同時に）ユーザへパッチリリース情報を提供する				■定義内容 ベンダが定期的にユーザへパッチリリース情報を提供する なお、緊急度の高いものは即時連絡する。	
C.2.3.2					パッチ適用方針	パッチを適用しない	推奨されるパッチのみを適用する	全てのパッチを適用する				■定義内容 パッチ適用可否について検証のうえ適用が必要なパッチを適用する。	【メトリクス】 リリースされるパッチが個別パッチであるか、集合パッチであるかによって選択レベルが変わる場合は、個別に合意する必要がある。 セキュリティパッチについては、セキュリティの項目でも検討すること（E.4.3.2）。
C.2.3.3					パッチ適用タイミング	パッチを適用しない	障害発生時にパッチ適用を行う	定期保守時にパッチ適用を行う	新規のパッチがリースされるたびに適用を行う			■定義内容 四半期に運用報告会にて貴庁へパッチリリース情報を報告のうえシステムメンテナンス日を調整し、適用する。 なお、緊急度の高いものは適宜対応する。	【メトリクス】 リリースされるパッチが個別パッチであるか、集合パッチであるかによって選択レベルが変わる場合は、個別に合意する必要がある。 セキュリティパッチについては、セキュリティの項目でも検討すること（E.4.3.3）。
C.2.3.4					パッチ検証の実施有無	パッチ検証を実施しない	障害パッチのみパッチ検証を実施する	障害パッチとセキュリティパッチの両方でパッチ検証を実施する				■定義内容 障害パッチとセキュリティパッチの両方でパッチ検証を実施する	

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
C.3.1.1		障害時運用	復旧作業	業務停止を伴う障害が発生した際の復旧作業に必要な労力。	復旧作業	復旧不要	復旧用製品は使用しない手作業の復旧	復旧用製品による復旧	復旧用製品＋業務アプリケーションによる復旧			「A.4.1.1 復旧作業」にて定義する。	【重複項目】 A.4.1.1。復旧作業は、可用性の復旧目標（RTO/RPO）を検討するうえで必要な項目であるため、可用性と運用・保守性の両方に含まれている。 【メトリクス】 選定したレベルに応じて、ユーザ側・ベンダ側それぞれの体制や権限の整理を実施する必要がある。 【レベル】 自作ツールを利用するケースは手作業に含む。 復旧用製品とは、バックアップ・リカバリを行う製品を指す。復旧用製品による復旧を行う場合、どこまで自動化するか（自動リカバリー機能充足率など）を定義するケースもあるが、可用性としては、復旧用製品を使用するかしないかでギャップが発生するため、この観点でレベルを検討する。
C.3.1.2					代替業務運用の範囲	無し	一部の業務について代替業務運用が必要	全部の業務について代替業務運用が必要				「A.4.1.2 代替業務運用の範囲」にて定義する。	【重複項目】 A.4.1.2。代替業務運用の範囲は、可用性の復旧目標（RTO/RPO）を検討するうえで必要な項目でもあるため、可用性と運用・保守性の両方に含まれている。 【メトリクス】 代替業務運用とは、障害によりシステムが復旧不可能となった場合に、代替業務でカバーすることが可能な運用手段（代替機あるいは人手による運用）を指す。
C.3.2.1			障害復旧自動化の範囲	障害復旧に関するオペレーションを自動化する範囲に関する項目。	障害復旧自動化の範囲	障害復旧作業は全て手動で実施する	一部の障害復旧作業を自動化する	全ての障害復旧作業を自動化する				■定義内容 RTO（目標復旧レベル）を達成するために必要な作業を自動化する。	【レベル1】 一部の障害復旧作業とは、特定パターン（あるいは部位）の障害復旧作業に関してのみ自動化を行うようなケースを指す。 【運用コストへの影響】 障害復旧作業を自動化するためには、障害のパターン毎に複雑な判断を行うスクリプトを作成する必要があり開発コストが増大する。一方、障害発生時の復旧作業が迅速化され、ミスも少なくなるため運用コストは減少する。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
C.3.3.1			システム異常検知時の対応	システムの異常を検知した際のベンダ側対応についての項目。	対応可能時間	ベンダの営業時間内（例：9時～17時）で対応を行う	ユーザの指定する時間帯（例：18時～24時）で対応	24時間対応を行う				■定義内容 緊急度の高の事象：24時間365日 それ以外：開庁日9:30-18:15	【メトリクス】 システムの異常検知時に保守員が作業対応を行う時間帯。
C.3.3.2					駆けつけ到着時間	保守員の駆けつけ無し	保守員到着が異常検知から数日中	保守員到着が異常検知からユーザの翌営業日中	保守員到着が異常検知からユーザの翌営業開始時まで	保守員到着が異常検知から数時間内	保守員が常駐	クラウドのため駆けつけ時間はなし	【メトリクス】 システムの異常を検出してから、指定された連絡先への通知、保守員が障害連絡を受けて現地へ到着するまでの時間。
C.3.3.3					SE到着平均時間	SEの駆けつけ無し	SE到着が異常検知から数日中	SE到着が異常検知からユーザの翌営業日中	SE到着が異常検知からユーザの翌営業開始時まで	SE到着が異常検知から数時間内	SEが常駐	クラウドのため駆けつけ時間はなし	【メトリクス】 システム異常を検知してからSEが到着するまでの平均時間。
C.3.4.1			交換用部材の確保	障害の発生したコンポーネントに対する交換部材の確保方法。	保守部品確保レベル	確保しない	保守契約に基づき、部品を提供するベンダが規定年数の間保守部品を確保する	保守契約に基づき、保守を提供するベンダが当該システム専用として規定年数の間保守部品を確保する				部品については、クラウド事業者の責任範囲のため、対象外とする。	【メトリクス】 当該システムに関する保守部品の確保レベル。
C.3.4.2					予備機の有無	予備機無し	一部、予備機有り	全部、予備機有り				予備機については、クラウド事業者の責任範囲のため、対象外とする。	

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
C.4.1.1		運用環境	開発用環境の設置	ユーザがシステムに対する開発作業を実施する目的で導入する環境についての項目。	開発用環境の設置有無	システムの開発環境を設置しない	運用環境の一部に限定した開発環境を設置する	運用環境と同一の開発環境を設置する				■定義内容 運用環境と同一の開発環境を設置する	【メトリクス】 開発用環境とは、本番環境とは別に開発専用に使用することのできる機材一式のことを指す。本番移行後に本番環境として利用される開発フェーズの環境は、本項目に含めない。 【レベル】 開発フェーズでは開発環境として使用していたが、本番移行後は本番環境となる環境については、レベル0のシステムの開発環境を設置しないを選択する。
C.4.2.1			試験用環境の設置	ユーザがシステムの動作を試験する目的で導入する環境についての項目。	試験用環境の設置有無	システムの試験環境を設置しない	システムの開発用環境と併用する	専用の試験用環境を設置する				■定義内容 専用の試験用環境（検証環境）を設置する。	【メトリクス】 試験用環境とは、本番環境とは別に試験専用に使用することのできる機材一式のことを指す。本番移行後に本番環境として利用される試験フェーズの環境は、本項目に含めない。 【レベル】 試験フェーズでは試験環境として使用していたものを、本番移行後においても継続して使用することとし、レベル2の専用の試験用環境を設置するを選択する。
C.4.3.1			マニュアル準備レベル	運用のためのマニュアルの準備のレベル。	マニュアル準備レベル	各製品標準のマニュアルを利用する	システムの通常運用のマニュアルを提供する	システムの通常運用と保守運用のマニュアルを提供する	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供する			■定義内容 システムの通常運用と保守運用のマニュアルを提供する。	【レベル】 通常運用のマニュアルには、システム基盤に対する通常時の運用（起動・停止等）にかかわる操作や機能についての説明が記載される。保守運用のマニュアルには、システム基盤に対する保守作業（部品交換やデータ復旧手順等）にかかわる操作や機能についての説明が記載される。 障害発生時の一次対応に関する記述（系切り替え作業やログ収集作業等）は通常運用マニュアルに含まれる。バックアップからの復旧作業については保守マニュアルに含まれるものとする。 【運用コストへの影響】 ユーザの運用に合わせたカスタマイズされたマニュアルは、作成するためにコストがかかるため導入コストが増大するが、ユーザが運用時に手順を調査する負担が減少するため運用コストは減少する。
C.4.4.1			リモートオペレーション	システムの設置環境とは離れた環境からのネットワークを介した監視や操作の可否を定義する項目。	リモート監視地点	リモート監視を行わない	構内LANを介してリモート監視を行う	遠隔地でリモート監視を行う				■定義内容 遠隔地でリモート監視を行う。	【レベル】 監視の内容については、通常運用の運用監視の項目にて確認する必要がある。 【運用コストへの影響】 リモート監視を実装するためには、特別なハードウェア・ソフトウェアを導入する必要があり導入コストが増大する。しかし、運用状況の確認のために管理者がわざわざサーバの設置場所まで移動する必要がなくなるため、運用コストは減少する。
C.4.4.2					リモート操作の範囲	リモート操作を行わない	定型処理のみリモート操作を行う	任意のリモート操作を行う				■定義内容 任意のリモート操作を行う。	【メトリクス】 リモート監視地点から実施できる操作の範囲を検討する。 【レベル】 定型処理のみリモート操作を実現するためのソフトウェアは安価であったり、任意のリモート操作を認める場合はセキュリティやその他の面での検討項目が増えることを考慮し、定型処理よりも任意のリモート操作を行う方のレベルを高く設定している。 【運用コストへの影響】 リモート操作を実装するためには、特別なハードウェア・ソフトウェアを導入する必要があり導入コストが増大する。しかし、メンテナンス操作のために管理者がわざわざサーバの設置場所まで移動する必要がなくなるため、運用コストは減少する。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
C.4.5.1			外部システム接続	システムの運用に影響する外部システムとの接続の有無に関する項目。	外部システムとの接続有無	外部システムと接続しない	社内の外部システムと接続する	社外の外部システムと接続する				■定義内容 社外の外部システムと接続する	【メトリクス】 接続する場合には、そのインターフェースについて確認すること。
C.4.5.2					監視システムの有無	監視システムは存在しない	既存監視システムに接続する	新規監視システムに接続する				外部システムは監視対象外のため、対象外	【レベル2】 新規監視システムに接続とは、当該システムに対する監視機能の新規構築が要件定義範囲に含まれていることを意味している。
C.4.5.3					ジョブ管理システムの有無	ジョブ管理システムは存在しない	既存ジョブ管理システムに接続する	新規ジョブ管理システムに接続する				■定義内容 新規ジョブ管理システムに接続する	【レベル2】 新規ジョブ管理システムに接続とは、当該システムに対するジョブ管理機能の新規構築が要件定義範囲に含まれていることを意味している。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
C.5.1.1		サポート体制	保守契約（ハードウェア）	保守が必要な対象ハードウェアの範囲。	保守契約（ハードウェア）の範囲	保守契約を行わない	ベンダの自社製品（ハードウェア）に対してのみ保守契約を行う	マルチベンダのサポート契約を行う（一部対象外を許容）	マルチベンダのサポート契約を行う（システムを構成する全製品を対象）			■定義内容 クラウドサービスを含むマルチベンダのサポート契約を行う（一部対象外を許容）。 OSSについては、必要に応じて、社内有識者組織に調査を依頼する。	【レベル】 ベンダの自社製品（ハードウェア）に対してのみサポート契約とは、システムを構成する製品個別の提供ベンダと、当該製品に対するサポート契約を行うことを意味しており、当該製品に対してのみサポートサービスが提供される契約形態のことである。 マルチベンダのサポート契約とは、システム全体に対するサポートサービスを提供するベンダと契約を行うことを意味しており、複数のベンダの製品から構成されるシステムに対してワンストップのサポート窓口が提供される契約形態のことである。 【運用コストへの影響】 サポート契約を行うと運用コストが増大するように感じられるが、問題が発生した際に必要となる費用が膨大となるため、サポート契約を行ったほうが結果として運用コストは小さくなる場合がある。
C.5.2.1			保守契約（ソフトウェア）	保守が必要な対象ソフトウェアの範囲。	保守契約（ソフトウェア）の範囲	保守契約を行わない	ベンダの自社製品（ソフトウェア）に対してのみ保守契約を行う	マルチベンダのサポート契約を行う（一部対象外を許容）	マルチベンダのサポート契約を行う（システムを構成する全製品を対象）				【レベル】 ベンダの自社製品（ソフトウェア）に対してのみサポート契約とは、システムを構成する製品個別の提供ベンダと、当該製品に対するサポート契約を行うことを意味しており、当該製品に対してのみサポートサービスが提供される契約形態のことである。 マルチベンダのサポート契約とは、システム全体に対するサポートサービスを提供するベンダと契約を行うことを意味しており、複数のベンダの製品から構成されるシステムに対してワンストップのサポート窓口が提供される契約形態のことである。 【運用コストへの影響】 サポート契約を行うと運用コストが増大するように感じられるが、問題が発生した際に必要となる費用が膨大となるため、サポート契約を行ったほうが結果として運用コストは小さくなる場合がある。
C.5.3.1			ライフサイクル期間	運用保守の対応期間および、実際にシステムが稼動するライフサイクルの期間。	ライフサイクル期間	3年	5年	7年	10年以上			■定義内容 2026年2月～2031年1月まで	【メトリクス】 ここでのライフサイクルとは、次回のシステム更改までの期間と規定している。製品の保守可能期間よりも長い期間のライフサイクルとなる場合は、保守延長や保守可能バージョンへのアップ等の対応が必要となる。
C.5.4.1			メンテナンス作業役割分担	メンテナンス作業に対するユーザ/ベンダの役割分担、配置人数に関する項目。	メンテナンス作業役割分担	全てユーザが実施	一部ユーザが実施	全てベンダが実施				■定義内容 メンテナンス作業は運用保守担当が実施するものとする。 庁内の調整・周知は規制庁側が実施するものとする。	
C.5.5.1			一次対応役割分担	一次対応のユーザ/ベンダの役割分担、一次対応の対応時間、配備人数。	一次対応役割分担	全てユーザが実施	一部ユーザが実施	全てベンダが実施					

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
C.5.6.1			サポート要員	サポート体制に組み入れる要員の人数や対応時間、スキルレベルに関する項目。	ベンダ側常備配備人数	常駐しない	1人	複数人				■定義内容 サービスデスク：監視端末にて運用作業を24時間365日行える体制とする。 運用保守担当：業務、インフラの運用・保守が行え、各保守ベンダがサポートする体制とする。	
C.5.6.2					ベンダ側対応時間帯	対応無し	ベンダの定時時間内（9～17時）	夜間のみ非対応（9～21時）	引継ぎ時に1時間程度非対応有り（9～翌8時）	24時間対応		■定義内容 運用・保守を行う以下の対応時間は以下とする。 サービスデスク：24時間365日 運用保守担当：開庁日9:30～18:15 ただし、緊急度が高の事象が発生した場合は、24時間365日にて対応する。	
C.5.6.3					ベンダ側対応者の要求スキルレベル	指定無し	有識者の指導を受けて機器の操作を実施できる	システムの構成を把握し、ログの収集・確認が実施できる	システムの運用や保守作業手順に習熟し、ハードウェアやソフトウェアのメンテナンス作業を実施できる	システムの開発や構築に携わり、業務要件やユーザの事情にも通じている		■定義内容 システムの運用や保守作業手順に習熟し、ハードウェアやソフトウェアのメンテナンス作業を実施できる。	
C.5.7.1			導入サポート	システム導入時の特別対応期間の有無および期間。	システムテスト稼働時の導入サポート期間	無し	当日のみ	1週間以内	1ヶ月以内	1ヶ月以上		■定義内容 1ヶ月以内（受入テスト・操作説明会におけるサポートを想定）	
C.5.7.2					システム本稼働時の導入サポート期間	無し	当日のみ	1週間以内	1ヶ月以内	1ヶ月以上		■定義内容 問い合わせ窓口にてサポートする。	

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
C.5.8.1			オペレーション訓練	オペレーション訓練実施に関する項目。	オペレーション訓練実施の役割分担	実施しない	全てユーザが実施	一部ユーザが実施	全てベンダが実施			■定義内容 全てベンダが実施（担当者・承認者・広報室向けに説明会を実施）	
C.5.8.2					オペレーション訓練範囲	実施しない	通常運用の訓練を実施	通常運用に加えて保守運用の訓練を実施	通常運用、保守運用に加えて、障害発生時の復旧作業に関する訓練を実施			■定義内容 通常運用の訓練を実施	【レベル】 通常運用とは、システム基盤に対する通常時の運用（起動・停止等）にかかわる操作を指す。保守運用とは、システム基盤に対する保守作業（部品交換やデータ復旧手順等）にかかわる操作を指す。
C.5.8.3					オペレーション訓練実施頻度	実施しない	システム立ち上げ時のみ	定期開催				■定義内容 システム立ち上げ時のみ	
C.5.9.1			定期報告会	保守に関する定期報告会の開催の要否。	定期報告会実施頻度	無し	年1回	半年に1回	四半期に1回	月1回	週1回以上	■定義内容 月1回運用保守の定期報告を行う。	【メトリクス】 障害発生時に実施される不定期の報告会は本メトリクスには含まない。
C.5.9.2					報告内容のレベル	無し	障害報告のみ	障害報告に加えて運用状況報告を行う	障害および運用状況報告に加えて、改善提案を行う			■定義内容 ①システムの稼働状況（計画停止/非計画停止の状況） ②システム障害、セキュリティ障害の発生状況（件数、原因、対応状況等）、その他の課題、対策実施の是非等 ③セキュリティ監視の状況（各種アラートの検出状況） ④修正プログラムの公開状況及び適用是非 ⑤運用窓口業務の実績（問合せ件数、問合せ内容） ⑥システムリソースの利用状況、見直しの是非 ⑦予防保守（点検、ソフトウェア更新等）の実施状況及び直近の予防保守の実施予定 ⑧サービスレベル遵守状況 ⑨今後の予定	

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
C.6.1.1		その他の運用管理方針	内部統制対応	IT運用プロセスの内部統制対応を行うかどうかに関する項目。	内部統制対応の実施有無	内部統制対応について規定しない	既存の社内規定に従って、内部統制対応を実施する	新規に規定を制定し、内部統制対応を実施する				■定義内容 既存の社内規定に従って、内部統制対応を実施する。また規制庁における監査対応を支援する。	【メトリクス】 ここでは内部統制対応の実施有無について確認する。内部統制対応の具体的な対応方法（オペレーションで実施するか、システムへの機能実装で実現するか等）については、有無の確認後に具体化して確認する。
C.6.2.1			サービスデスク	ユーザの問合せに対して単一の窓口機能を提供するかどうかに関する項目。	サービスデスクの設置有無	サービスデスクの設置について規定しない	既存のサービスデスクを利用する	新規にサービスデスクを設置する				■定義内容 24時間/365日対応可能なサービスデスクを設置する。	【メトリクス】 ここでは、ユーザとベンダ間におけるサービスデスクの設置の有無について確認する。サービスデスク機能の具体的な実現方法については、有無の確認後に具体化して確認する。
C.6.3.1			インシデント管理	業務を停止させるインシデントを迅速に回復させるプロセスを実施するかどうかに関する項目。	インシデント管理の実施有無	インシデント管理について規定しない	既存のインシデント管理のプロセスに従う	新規にインシデント管理のプロセスを規定する				■定義内容 インシデント管理を実施する。 インシデント発生時にはインシデントの登録・分類・既知のインシデントの照会を行い対応する。未知のインシデントの場合には、調査を行う。調査結果から問題管理、変更・リリース管理へ連携する。 災害時は以下の対応を実施する。 ・バックアップサイトへの切り替え バックアップサイトへは自動で切り替わる。 ・バックアップサイトからの切り戻し バックアップからの切り戻しはメインサイト復旧後、手動にて行う。 切り戻しにはバックアップサイトでのジョブ停止、データ同期等の作業上、切り戻す。また、切り戻しについては情報システム室と調整の上、切り戻す。	【メトリクス】 ここでは、当該システムで発生するインシデントの管理を実施するかどうかを確認する。インシデント管理の実現方法については、有無の確認後に具体化して確認する。
C.6.4.1			問題管理	インシデントの根本原因を追究し、可能であれば取り除くための処置を講じるプロセスを実施するかどうかに関する項目。	問題管理の実施有無	問題管理について規定しない	既存の問題管理のプロセスに従う	新規に問題管理のプロセスを規定する				■定義内容 問題管理を実施する。 問題を識別・記録して調査と診断を行う。問題のワークアラウンドの確立と根本的な対策検討を行う。改善案に基づく改善活動を行う。インシデント管理・リリース管理と連携する。	【メトリクス】 ここでは、インシデントの根本原因を追究するための問題管理を実施するかどうかを確認する。問題管理の実現方法については、有無の確認後に具体化して確認する。
C.6.5.1			構成管理	ハードウェアやソフトウェアなどのIT環境の構成を適切に管理するためのプロセスを実施するかどうかに関する項目。	構成管理の実施有無	構成管理について規定しない	既存の構成管理のプロセスに従う	新規に構成管理のプロセスを規定する				■定義内容 構成管理を実施する。 変更内容を確認し、構成情報のバックアップを取ったのち構成情報を更新する。構成変更内容について承認を得る。	【メトリクス】 ここでは、リリースされたハードウェアやソフトウェアが適切にユーザ環境に構成されているかを管理するための構成管理を実施するかどうかを確認する。構成管理の実現方法については、有無の確認後に具体化して確認する。
C.6.6.1			変更管理	IT環境に対する変更を効率的に管理するためのプロセスを実施するかどうかに関する項目。	変更管理の実施有無	変更管理について規定しない	既存の変更管理のプロセスに従う	新規に変更管理のプロセスを規定する				■定義内容 変更管理を実施する。 変更要求を識別・記録し、変更要求を実現する変更計画を策定する。変更計画の承認を得たのちリリース管理プロセスへ移行する。	【メトリクス】 ここでは、ハードウェアの交換やソフトウェアのパッチ適用、バージョンアップ、パラメータ変更といったシステム環境に対する変更を管理するための変更管理を実施するかどうかを確認する。変更管理の実現方法については、有無の確認後に具体化して確認する。
C.6.7.1			リリース管理	ソフトウェア、ハードウェア、ITサービスに対する実装を管理するためのプロセスを実施するかどうかに関する項目。	リリース管理の実施有無	リリース管理について規定しない	既存のリリース管理のプロセスに従う	新規にリリース管理のプロセスを規定する				■定義内容 リリース管理を行う。 承認を得た、変更計画に基づく変更が正しくリリースされたことを確認する。 反映された変更は構成管理プロセスに移行し、管理する。	【メトリクス】 ここでは、承認された変更が正しくシステム環境に適用されているかどうかを管理するリリース管理を実施するかどうかを確認する。リリース管理の実現方法については、有無の確認後に具体化して確認する。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
D.1.1.1	移行性	移行時期	移行のスケジュール	移行作業計画から本稼働までのシステム移行期間、システム停止可能日時、並行稼働の有無。（例外発生時の切り戻し時間や事前バックアップの時間等も含むこと。）	システム移行期間	システム移行無し	3ヶ月未満	半年未満	1年未満	2年未満	2年以上	■定義内容 1年未満	
D.1.1.2					システム停止可能日時	制約無し（必要な期間の停止が可能）	5日以上	5日未満	1日（計画停止日を利用）	利用の少ない時間帯（夜間など）	移行のためのシステム停止不可	■定義内容 ・利用機能：レベル4（調整を行ったうえで、利用の少ない時間帯のシステム停止不可） ・内部管理機能：レベル２（5日未満）	【メトリクス】 システムによっては、システム停止可能な日や時間帯が連続して確保できない場合がある。（例えば、この日は1日、次の日は夜間のみ、その次の日は計画停止日で1日、などの場合。） その場合には、システム停止可能日とその時間帯を、それぞれ確認すること。 【レベル】 レベル0はシステムの制約によらず、移行に必要な期間のシステム停止が可能なことを示す。レベル1以上は、システム停止に関わる（業務などの）制約が存在する上での、システム停止可能日時を示す。レベルが高くなるほど、移行によるシステム停止可能な日や時間帯など、移行計画に影響範囲が大きい制約が存在することを示している。
D.1.1.3					並行稼働の有無	無し	有り					■定義内容 無し	【レベル1】 並行稼働有りの場合には、その期間、場所等を規定すること。関係項目にF.4.2.3、F.4.4.3がある。
D.2.1.1		移行方式	システム展開方式	システムの移行および新規展開時に多段階による展開方式をどの程度採用するかの程度。	拠点展開ステップ数	単一拠点のため規定無し	一斉展開	5段階未満	10段階未満	20段階未満	20段階以上	■定義内容 レベル０：規定無し	【レベル】 拠点展開時のリスクによっては難易度が逆転し、一斉展開の難易度が高くなる場合もある。対象システムについて、拠点毎に展開時のリスクを考慮して拠点展開ステップ数を判断すること。
D.2.1.2					業務展開ステップ数	単一業務のため規定無し	全業務一斉切り替え	4段階未満	6段階未満	10段階未満	10段階以上	■定義内容 レベル０：規定無し	【レベル】 業務展開時のリスクによっては難易度が逆転し、全業務一斉切り替えの難易度が高くなる場合もある。対象システムについて、業務毎に展開時のリスクを考慮して業務展開ステップ数を判断すること。
D.3.1.1		移行対象（機器）	移行設備	移行前のシステムで使用していた設備において、新システムで新たな設備に入れ替え対象となる移行対象設備の内容。	設備・機器の移行内容	移行対象無し	移行対象設備・機器のハードウェアを入れ替える	移行対象設備・機器のハードウェア、OS、ミドルウェアを入れ替える	移行対象設備・機器のシステム全部を入れ替える	移行対象設備・機器のシステム全部を入れ替えて、さらに統合化する		■定義内容 レベル４：移行対象設備・機器のシステム全部を入れ替えて、さらに統合化する	【レベル】 移行対象設備・機器が複数あり、移行内容が異なる場合には、それぞれ合意すること。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
D.4.1.1		移行対象（データ）	移行データ量	旧システム上で移行の必要がある業務データの量（プログラムを含む）。	移行データ量	移行対象無し	1TB未満	1PB未満	1PB以上			■定義内容 データ量は「B.1.1.3 データ量」と同一。	
D.4.1.2					移行データ形式	移行対象無し	移行先と形式が同一	移行先と形式が異なる				■定義内容 移行先と形式が同一	【メトリクス】 データ形式は、アプリケーションに依存したフォーマット、テーブル形式や文字コードなど、新システムに移行するために考慮すべきデータ形式のパターンを指す。 【レベル】 移行データ形式のパターンが複数ある場合には、それぞれについてデータ形式を確認すること。
D.4.2.1			移行媒体	移行対象となる媒体の量と移行時に必要となる媒体種類数。	移行媒体量	移行対象無し	10本未満（1TB未満）	1000本未満（1PB未満）	1000本以上（1PB以上）			■定義内容 データ量は「B.1.1.3 データ量」と同一。	
D.4.2.2					移行媒体種類数	移行対象無し	1種類	2種類	3種類	4種類	5種類以上	■定義内容 1種類。 ・データ転送	【メトリクス】 移行する際に使用しなければならない媒体の種類を計数する（例えば、テープ、ディスク、紙の伝票類、など）。 また、ネットワーク接続によるデータ転送も媒体種類として含む。
D.4.3.1			変換対象（DBなど）	変換対象となるデータの量とツールの複雑度（変換ルール数）。	変換データ量	変換対象無し	1TB未満	1PB未満	1PB以上			■定義内容 レベル２	
D.4.3.2					移行ツールの複雑度（変換ルール数）	移行ツール不要 または 既存移行ツールで対応可能	変換ルール数が10未満の移行ツールの複雑度	変換ルール数が50未満の移行ツールの複雑度	変換ルール数が100未満の移行ツールの複雑度	変換ルール数が100以上の移行ツールの複雑度		■定義内容 レベル２	
D.5.1.1		移行計画	移行作業分担	移行作業の作業分担。	移行のユーザ/ベンダ作業分担	全てユーザ	ユーザとベンダと共同で実施	全てベンダ				■定義内容 レベル2：全て請負事業者にて対応する。	【メトリクス】 最終的な移行結果の確認は、レベルに関係なくユーザが実施する。なお、ユーザデータを取り扱う際のセキュリティに関しては、ユーザとベンダで取り交わしを行うことが望ましい。具体的内容については、「F.1.1.1 構築時の制約条件」にて確認する。 【レベル1】 共同で移行作業を実施する場合、ユーザ/ベンダの作業分担を規定すること。特に移行対象データに関しては、旧システムの移行対象データの調査、移行データの抽出/変換、本番システムへの導入/確認、等について、その作業分担を規定しておくこと。
D.5.2.1			リハーサル	移行のリハーサル（移行中の障害を想定したリハーサルを含む）。	リハーサル範囲	リハーサル無し	主要な正常ケースのみ	全ての正常ケース	正常ケース＋移行前の状態に切り戻す異常ケース	正常ケース＋システム故障から回復させる異常ケース		■定義内容 レベル２：全ての正常ケース	
D.5.2.2					リハーサル環境	リハーサル無し	本番データ使用可能	本番データ使用不可				■定義内容 本番データ使用可能	【レベル】 本番データを使用することによる情報漏えい等のセキュリティリスクは、「F.1.1.1 構築時の制約条件」にて判断し、ここではリハーサル環境に限定して判断する。
D.5.2.3					リハーサル回数	リハーサル無し	1回	2回	3回	4回	5回以上	■定義内容 2回（開発環境及び本番環境にて各1回）	
D.5.2.4					外部連携リハーサルの有無	無し	有り（外部接続仕様の変更無し）	有り（外部接続仕様の変更有り）				■定義内容 レベル1：外部接続仕様の変更無し）	【メトリクス】 外部システムとの接続仕様が変更になる場合、システム移行リスクを軽減するために新システムでは新旧両接続仕様をサポートすることがある。その場合には、両接続仕様を確認するための外部連携リハーサルを計画すること。 【レベル】 外部連携リハーサル有りの場合、そのリハーサル対象の外部システムとリハーサル範囲、環境、回数について規定すること。
D.5.3.1			トラブル対処	移行中のトラブル時の対応体制や対応プラン等の内容。	トラブル対処の規定有無	規定無し	対応体制のみ規定有り	対応体制と対応プランの規定有り				■定義内容 対応体制と対応プランの規定有り	【レベル】 トラブル対処の規定有りの場合、その対応体制や対応プランの規定内容について確認すること。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
E.1.1.1	セキュリティ	前提条件・制約条件	情報セキュリティに関するコンプライアンス	順守すべき情報セキュリティに関する組織規程やルール、法令、ガイドライン等が存在するかどうかを確認するための項目。 なお、順守すべき規程等が存在する場合は、規定されている内容と矛盾が生じないよう対策を検討する。 例） ・国内/海外の法律 ・資格認証 ・ガイドライン ・その他ルール	順守すべき社内規程、ルール、法令、ガイドライン等の有無	無し	有り					■定義内容 原子力規制委員会情報セキュリティポリシー 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 IT製品の調達におけるセキュリティ要件リスト 独立行政法人情報処理推進機構「セキュリティエンジニアリング」	【メトリクス】 規程、法令、ガイドライン等を確認し、それらに従い、セキュリティに関する非機能要求項目のレベルを決定する必要がある。 例） ・国内/海外の法律 　不正アクセス禁止法・不正競争防止法・プロバイダ責任法・改正個人情報保護法・SOX法・ 　EU一般データ保護規則(GDPR)・特定電子メール送信適正化法・電子署名法 など ・資格認証 　プライバシーマーク・ISMS/ITSMS/BCMS/CSMS・ISO/IEC27000系・PCI DSS・ 　クラウド情報セキュリティ監査・TRUSTe など ・ガイドライン 　FISC・FISMA/NIST800・政府機関の情報セキュリティ対策のための統一基準 など ・その他ルール 　情報セキュリティポリシー など 【レベル1】 構築するシステムが関係する国や地域によって、順守すべき法令やガイドラインが異なることに注意すること。
E.2.1.1		セキュリティリスク分析	セキュリティリスク分析	システム開発を実施する中で、どの範囲で対象システムの脅威を洗い出し、影響の分析を実施するかの方針を確認するための項目。 なお、適切な範囲を設定するためには、資産の洗い出しやデータのライフサイクルの確認等を行う必要がある。 また、洗い出した脅威に対して、対策する範囲を検討する。	リスク分析範囲	分析なし	重要度が高い資産を扱う範囲、あるいは、外接部分	開発範囲				■定義内容 開発範囲	【メトリクス】 システム開発中に実施するセキュリティリスク分析では、ソフトウェアのサポート終了や暗号の危殆化等の運用期間に顕在化するリスクも考慮する。 【レベル1】 外接部分とは、インターネットへの接続部分や、外部へ情報を持ち出す際に用いる媒体等を接続する部分、また、外部システムとデータのやりとりを行う部分等を意味する。 なお、以降のレベルにおいても同様の意味で用いている。
E.3.1.1		セキュリティ診断	セキュリティ診断	対象システムや、各種ドキュメント（設計書や環境定義書、実装済みソフトウェアのソースコードなど）に対して、セキュリティに特化した各種試験や検査の実施の有無を確認するための項目。	ネットワーク診断実施の有無	無し	有り					■定義内容 有り インターネット向けにサービス提供を行うため、不特定多数の攻撃者からの脅威にさらされる。そのため、侵入検査を代表とするネットワーク診断を実施する。	【メトリクス】 ネットワーク診断には、目視による設定の確認や、疑似攻撃を実施することにより脆弱性を発見する診断（ペネトレーションテスト）、ネットワーク上のサーバや通信機能をもつソフトウェアなどに対する脆弱性調査等がある。 【レベル1】 ネットワーク診断は、システム運用開始前に実施するだけでなく、システム運用中の定期的な実施も検討する。
E.3.1.2					Web診断実施の有無	無し	有り					■定義内容 有り	【メトリクス】 Web診断とは、Webサイトに対して行うWebサーバやWebアプリケーションに対するセキュリティ診断のことを言う。 【レベル1】 Web診断は、システム運用開始前に実施するだけでなく、システム運用中の定期的な実施も検討する。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
E.4.1.1		セキュリティリスク管理	セキュリティリスクの見直し	対象システムにおいて、運用開始後に新たに発見された脅威の洗い出しとその影響の分析をどの範囲で実施するかを確認するための項目。 セキュリティリスクの見直しには、セキュリティホールや脆弱性、新たな脅威の調査等が含まれる。	セキュリティリスク見直し頻度	無し	セキュリティに関するイベントの発生時に実施（随時）	セキュリティに関するイベントの発生時に実施（随時） ＋ 定期的に実施				■定義内容 セキュリティに関するイベントの発生時に実施（随時）＋定期的に実施 セキュリティに関するイベントの発生時に加えて、運用開始後も四半期にパッチ情報の収集等のセキュリティリスクの見直しを行う。	【レベル】 セキュリティに関するイベントとは、重要な脅威や脆弱性の発見、ウィルス感染、不正侵入、DoS攻撃、情報漏えいなどの情報セキュリティに関するインシデントのことを指す。
E.4.1.2					セキュリティリスクの見直し範囲	分析なし	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				■定義内容 システム全体 システム全体について確認・調査を行う。セキュリティリスクの対策は適用可否を検証のうえ、貴庁への報告し、対応する。	
E.4.2.1			セキュリティリスク対策の見直し	対象システムにおいて、運用開始後に発見された脅威に対する対策の方針を確認するための項目。 また、検討するにあたり、発見された脅威についての対応範囲について明らかにする。	運用開始後のリスク対応範囲	対応しない	重要度が高い資産に関連する、あるいは、外接部分の脅威に対応	洗い出した脅威全体に対応				■定義内容 洗い出した脅威全体に対応 リスク対応範囲は原則、洗い出した脅威全体について対応する。セキュリティリスクの対策は適用可否を検証のうえ、貴庁への報告し、対応する。	
E.4.3.1			セキュリティパッチ適用	対象システムの脆弱性等に対応するためのセキュリティパッチ適用に関する適用範囲、方針および適用のタイミングを確認するための項目。 これらのセキュリティパッチには、ウィルス定義ファイル等を含む。 また、セキュリティパッチの適用範囲は、OS、ミドルウェア等毎に確認する必要があり、これらセキュリティパッチの適用を検討する際には、システム全体への影響を確認し、パッチ適用の可否を判断する必要がある。 なお、影響の確認等については保守契約の内容として明記されることが望ましい。	セキュリティパッチ適用範囲	セキュリティパッチを適用しない	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				■定義内容 システム全体	
E.4.3.2					セキュリティパッチ適用方針	セキュリティパッチを適用しない	緊急性の高いセキュリティパッチのみ適用	全てのセキュリティパッチを適用				■定義内容 全てのセキュリティパッチを適用 原則として全てのセキュリティパッチを適用する。 「OS、ミドルウェアのセキュリティパッチ」に関する影響調査、対象のパッチの選定、貴庁へ四半期に運用報告会で報告し、定期保守作業の中で実施する。	
E.4.3.3					セキュリティパッチ適用タイミング	セキュリティパッチを適用しない	障害パッチ適用時に合わせて実施	定期保守時に実施	パッチ出荷時に実施			■定義内容 規制庁へ四半期に運用報告会で報告し、システムメンテナンスにて実施 ただし、緊急度が高いものは適宜対応 「OS、ミドルウェアのセキュリティパッチ」に関しては、影響調査が必要となるため貴庁へ四半期に運用報告会で報告し、定期保守作業の中で実施する。 ウィルス定義ファイルについては、基本的にはOS、ミドルウェアへの影響がないため、リアルタイムで自動適用を行う。 緊急のセキュリティパッチについては、適宜対応を行う。	【レベル】 セキュリティパッチを適用するまでの脅威等にさらされている期間は、監視強化や暫定対策の実施を検討する。 【レベル3】 パッチが出荷されてから適用するまでの期間について検討することが望ましい。パッチ検証を実施する場合、環境準備等を含め、パッチ適用までに期間を要することを考慮する。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
E.5.1.1		アクセス・利用制限	認証機能	資産を利用する主体（利用者や機器等）を識別するための認証を実施するか、また、どの程度実施するのかを確認するための項目。 複数回の認証を実施することにより、抑止効果を高めることができる。 なお、認証するための方式としては、ID/パスワードによる認証や、ICカード等を用いた認証等がある。	管理権限を持つ主体の認証	実施しない	1回	複数回の認証	複数回、異なる方式による認証			■定義内容 複数回、異なる方式による認証	【メトリクス】 管理権限を持つ主体とは、システムの管理者や業務上の管理者を指す。
E.5.1.2					管理権限を持たない主体の認証	実施しない	1回	複数回の認証	複数回、異なる方式による認証			■定義内容 複数回、異なる方式による認証	

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
E.5.2.1			利用制限	認証された主体（利用者や機器など）に対して、資産の利用等を、ソフトウェアやハードウェアにより制限するか確認するための項目。 例） ドアや保管庫の施錠、USBやCD-RWやキーボードなどの入出力デバイスの制限、コマンド実行制限など。	システム上の対策における操作制限度	無し	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可					■定義内容 必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可	【メトリクス】 ソフトウェアのインストール制限や、利用制限等、ソフトウェアによる対策を示す。
E.5.2.2					物理的な対策による操作制限度	無し	必要最小限のハードウェアの利用や操作のみを許可					■定義内容 必要最小限のハードウェアの利用や操作のみを許可 運用・保守業者については、開発、運用用途で本システムへのアクセスを行う端末が設置される居室への入退室管理を実施する。 入退室管理にあたっては、ICカード等により資格を持つ者だけが入退室できるよう対策を施す。 また、設置する端末はセキュリティワイヤを用いた物理的対策を行う。	【メトリクス】 セキュリティゲート等のファシリティによるサーバルームへの入退室管理、情報の保管場所や、サーバ等に対する施錠、USBやCD-RWの入出力デバイスの制限等のための物理的な対策実施を示す。
E.5.3.1			管理方法	認証に必要な情報（例えば、 ID/パスワード、指紋、虹彩、静脈など、主体を一意に特定する情報）の追加、更新、削除等のルール策定を実施するかを確認するための項目。	管理ルールの策定	実施しない	実施する					■定義内容 実施する 運用・保守設計の中で各種ルール策定を行う。	

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
E.6.1.1		データの秘匿	データ暗号化	機密性のあるデータを、伝送時や蓄積時に秘匿するための暗号化を実施するかを確認するための項目。	伝送データの暗号化の有無	無し	認証情報のみ暗号化	重要情報を暗号化				■定義内容 重要情報を暗号化 業務アプリケーションへのアクセスについては、httpsによる伝送経路の暗号化を行う。 基盤システムへのアクセスについては、VPNによる伝送経路の暗号化やhttps,ssh等の形式で伝送経路の暗号化を行う。 なお、暗号化アルゴリズムについては、電子政府推奨暗号リストに記載されているものを採用する。	【レベル1】 認証情報のみ暗号化とは、システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。
E.6.1.2					蓄積データの暗号化の有無	無し	認証情報のみ暗号化	重要情報を暗号化				■定義内容 重要情報を暗号化 暗号化対象は業務データ（データベース）及びバックアップデータとする。 暗号化アルゴリズムについては、電子政府推奨暗号リストに記載されているものを採用する。	【レベル1】 認証情報のみ暗号化とは、システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。
E.6.1.3					鍵管理	無し	ソフトウェアによる鍵管理	耐タンパデバイスによる鍵管理				■定義内容 ソフトウェアによる鍵管理 秘密鍵へのアクセス権限については、極力限定された範囲に設定を行う。	【レベル】 ソフトウェアによる鍵管理とは、秘密鍵情報に対し、ソフトウェアの設定等によりアクセス制御を実施するような管理のことである。 耐タンパデバイスによる鍵管理とは、ICカードのような、物理的な仕掛により、攻撃への耐性を高めた専用デバイスによる管理のことである。これにより、鍵情報の改竄や漏洩といった脅威に対して、より厳密に管理することができる。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
E.7.1.1		不正追跡・監視	不正監視	不正行為を検知するために、それらの不正について監視する範囲や、監視の記録を保存する量や期間を確認するための項目。 なお、どのようなログを取得する必要があるかは、実現するシステムやサービスに応じて決定する必要がある。 また、ログを取得する場合には、不正監視対象と併せて、取得したログのうち、確認する範囲を定める必要がある。	ログの取得	実施しない	実施する					■定義内容 実施する 不正行為を検知するため「セキュリティ」に関わるログは全て取得する。 特に重要情報である業務データへのアクセス・操作に関わるログ、業務アプリケーションへのアクセス・操作に関わるログについては、漏れなく取得する。 ログの種別としては以下を想定するが、詳細については設計工程で定義を行う。 業務アプリケーション動作ログ 業務アプリケーションへのアクセスログ データベースログ 操作ログ ログイン/ログアウト履歴（成功/失敗） セキュリティ機能に関わるログ その他アプリケーションの動作ログ	【メトリクス】 取得対象のログは、不正な操作等を検出するための以下のようなものを意味している。取得したログは個々のログを確認するだけでなく、複数のログを組み合わせて相関分析することも検討する。必要に応じて、ログと作業記録との突き合わせも行う。 ・ログイン/ログアウト履歴（成功/失敗） ・操作ログ ・セキュリティ機器の検知ログ ・通信ログ ・DBログ ・アプリケーションログ 等
E.7.1.2					ログ保管期間	6ヶ月	1年	3年	5年	10年以上有期	永久保管	「C.1.2.6 バックアップ保管期間」にて定義する。	
E.7.1.3					不正監視対象（装置）	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				■定義内容 システム全体 本システムは、インターネット向けにサービスを提供するため、インターネット経由での攻撃等により攻撃範囲が限定されないことを想定し、システム全体に対して監視を実施する。	【メトリクス】 不正監視対象（装置）とは、サーバ、ストレージ等への不正アクセス等の監視のために、ログを取得する範囲を確認するメトリクス。
E.7.1.4					不正監視対象（ネットワーク）	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				■定義内容 システム全体 本システムは、インターネット向けにサービスを提供するため、インターネット経由での攻撃等により攻撃範囲が限定されないことを想定し、システム全体に対して監視を実施する。	【メトリクス】 不正監視対象（ネットワーク）とは、ネットワーク上の不正なパケット等を監視するためのログの取得範囲を確認するメトリクス。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
E.7.1.5					不正監視対象（侵入者・不正操作等）	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				■定義内容 システム全体 本システムは、インターネット向けにサービスを提供するため、インターネット経由での攻撃等により攻撃範囲が限定されないことを想定し、システム全体に対して監視を実施する。	【メトリクス】 不正監視対象（侵入者・不正操作等）とは、不正な侵入者等を監視するために設置する監視カメラ等による監視の範囲を意味する。
E.7.1.6					確認間隔	無し	セキュリティに関するイベントの発生時に実施（随時）	セキュリティに関するイベントの発生時に実施（随時） ＋ 定期的に実施	常時確認			■定義内容 セキュリティに関するイベントの発生時に実施（随時）＋四半期で定期的に実施 セキュリティに関するイベントの発生時に加えて、運用開始後も定期的(月次を想定)にセキュリティに関するイベントのたな卸しを行う。 「セキュリティに関するイベントの発生」については、検知時にメールで通知を行う仕組みを導入する。	【レベル3】 常時確認とは、常に不正なアクセス等を監視し、即座に対応可能な状態を意味する。 自動検知システムを導入し、不正検知時にメール等で通知する仕組みの導入は、セキュリティに関するイベントの発生時に実施（随時）に含まれる。
E.7.2.1			データ検証	情報が正しく処理されて保存されていることを証明可能とし、情報の改ざんを検知するための仕組みとしてデジタル署名を導入するかを確認するための項目。	デジタル署名の利用の有無	無し	有り					■定義内容 有り https通信のために証明書の導入を行う。 使用するサーバ証明書の種別は「企業実在認証」とする。（委員会ホームページと同等の種別のサーバ証明書） また、静的なWebコンテンツに対する改ざん検知の仕組みについても導入を行う。	
E.7.2.2					確認間隔	無し	セキュリティに関するイベントの発生時に実施（随時）	セキュリティに関するイベントの発生時に実施（随時） ＋ 定期的に実施	常時確認			■定義内容 セキュリティに関するイベントの発生時に実施（随時）＋四半期で定期的に実施 セキュリティに関するイベントの発生時に加えて、運用開始後も四半期で定期的にセキュリティに関するイベントのたな卸しを行う。	

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
E.8.1.1		ネットワーク対策	ネットワーク制御	不正な通信を遮断するための制御を実施するかを確認するための項目。	通信制御	無し	有り					■定義内容 有り 本システムはインターネットからのアクセスを受けるため、L7(アプリケーション層)の不正通信対策として、WAF機能の導入を行う。	【レベル1】 通信制御を実現する際には、ファイアウォール、IPS、URLフィルタ、メールフィルタ等の導入を検討する必要がある。
E.8.2.1			不正検知	ネットワーク上において、不正追跡・監視を実施し、システム内の不正行為や、不正通信を検知する範囲を確認するための項目。	不正通信の検知範囲	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				■定義内容 システム全体 本システムは、インターネット向けにサービスを提供するため、インターネット経由での攻撃等により攻撃範囲が限定されないことを想定し、システム全体に対して監視を実施する。	【メトリクス】 検知範囲の設定に応じて、IDS等の導入を検討する必要がある。
E.8.3.1			サービス停止攻撃の回避	ネットワークへの攻撃による輻輳についての対策を実施するかを確認するための項目。	ネットワークの輻輳対策	無し	有り					■定義内容 有り 本システムはインターネットからのアクセスを受けるため、DoS/DDoS攻撃への対策を行う。	
E.9.1.1		マルウェア対策	マルウェア対策	マルウェア（ウィルス、ワーム、ボット等）の感染を防止する、マルウェア対策の実施範囲やチェックタイミングを確認するための項目。 対策を実施する場合には、ウィルス定義ファイルの更新方法やタイミングについても検討し、常に最新の状態となるようにする必要がある。	マルウェア対策実施範囲	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				■定義内容 システム全体	
E.9.1.2					リアルタイムスキャンの実施	実施しない	実施する					■定義内容 実施する	【レベル1】 リアルタイムスキャンは、例えば、以下のようなタイミングで実施する。実施する際は実施するタイミングを検討する必要がある。 ・ファイルサーバへデータをコピーするタイミング ・メールサーバがメールを受信したタイミング ・ファイルへの入出力処理が実行される前 等
E.9.1.3					フルスキャンの定期チェックタイミング	無し	不定期（フルスキャンを行えるタイミングがあれば実施する）	1回/月	1回/週	1回/日		■定義内容 1回/週	

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
E.10.1.1		Web対策	Web実装対策	Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。	セキュアコーディング、Webサーバの設定等による対策の強化	無し	対策の強化					■定義内容 対策の強化 インターネットからアクセスを受ける機能について、Webサーバの設定等によるセキュリティ対策を実施する。 また、実施した結果の有効性を確認するため侵入検査を代表とするネットワーク診断を実施する。	【メトリクス】 Webシステムが攻撃される事例が増加しており、Webシステムを構築する際には、セキュアコーディング、Webサーバの設定等による対策の実施を検討する必要がある。また、実施した結果の有効性を確認するための専門家のレビューやソースコード診断、ツールによるチェック等についても検討する必要がある。
E.10.1.2					WAFの導入の有無	無し	有り					■定義内容 有り 本システムはインターネットからのアクセスを受けるため、L7(アプリケーション層)の不正通信対策として、WAF機能の導入を行う。	【メトリクス】 WAFとは、Web Application Firewallのことである。
E.11.1.1		セキュリティインシデント対応/復旧	セキュリティインシデント対応/復旧	セキュリティインシデントが発生した時に、早期発見し、被害の最小化、復旧の支援等をするための体制について確認する項目。	セキュリティインシデントの対応体制	無し	有り					■定義内容 有り 緊急度の高：24時間365日 それ以外：開庁日9:30-18:15 ヘルプデスクでメール連絡 サービスデスクにて24時間365日、監視を行い、セキュリティインシデントを検知した際には運用保守担当にエスカレーションを行い、対応する。	【メトリクス】 セキュリティインシデント発生時の対応以外にも、インシデント対応マニュアルの整備や、システムの関係者に対するセキュリティ教育を実施する。 【レベル0】 セキュリティインシデント発生の都度、インシデント対応体制を構築する場合も含まれる。 【レベル1】 新たに対応体制を構築する他に、ユーザ企業内のCSIRTを利用する場合や、外部のセキュリティ対応サービスを利用する場合も含まれる。
F.1.1.1	システム環境・エコロジー	システム制約/前提条件	構築時の制約条件	構築時の制約となる社内基準や法令、各地方自治体の条例などの制約が存在しているかの項目。 例） ・J-SOX法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・FISC ・プライバシーマーク ・構築実装場所の制限 など	構築時の制約条件	制約無し	制約有り（重要な制約のみ適用）	制約有り（全ての制約を適用）				■定義内容 制約条件は「E.1.1.1」に沿うこと	【メトリクス】 システムを開発する際に、機密情報や個人情報等を取り扱う場合がある。これらの情報が漏洩するリスクを軽減するために、プロジェクトでは、情報利用者の制限、入退室管理の実施、取り扱い情報の暗号化等の対策が施された開発環境を整備する必要が生じる。 また運用予定地での構築が出来ず、別地にステージング環境を設けて構築作業を行った上で運用予定地に搬入しなければならない場合や、逆に運用予定地でなければ構築作業が出来ない場合なども制約条件となる。
F.1.2.1			運用時の制約条件	運用時の制約となる社内基準や法令、各地方自治体の条例などの制約が存在しているかの項目。 例） ・J-SOX法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・FISC ・プライバシーマーク ・リモートからの運用の可否 など	運用時の制約条件	制約無し	制約有り（重要な制約のみ適用）	制約有り（全ての制約を適用）				■定義内容 制約条件は「E.1.1.1」に沿うこと	

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
F.2.1.1		システム特性	ユーザ数	システムを使用する利用者(エンドユーザ)の人数。	ユーザ数	特定ユーザのみ	上限が決まっている	不特定多数のユーザが利用				「B.1.1.1 ユーザ数」にて定義する。	【重複項目】 B.1.1.1。ユーザ数は性能・拡張性を決めるための前提となる項目であると共にシステム環境を規定する項目でもあるため、性能・拡張性とシステム環境・エコロジーの両方に含まれている。 【レベル】 前提となる数値が決められない場合は、類似システムなどを参考に仮の値でも良いので決めておくことが必要。
F.2.2.1			クライアント数	システムで使用され、管理しなければいけないクライアントの数。	クライアント数	特定クライアントのみ	上限が決まっている	不特定多数のクライアントが利用				本システムにクライアントはないため、対象外	
F.2.5.1			特定製品指定	ユーザの指定によるオープンソース製品や第三者製品(ISV/IHV)などの採用の有無を確認する項目。採用によりサポート難易度への影響があるかの視点で確認を行う。	特定製品の採用有無	特定製品の指定がない	一部に特定製品の指定がある	サポートが困難な製品の指定がある				■定義内容 特定製品の指定はない	
F.2.6.1			システム利用範囲	システム利用者が属する属性の広がり。	システム利用範囲	部門内のみ	社内のみ	社外（BtoB）	社外（BtoC）			■定義内容 社外（BtoC）、社内	
F.2.7.1			複数言語対応	システム構築の上で使用が必要、またはサービスとして提供しなければならない言語。扱わなければならない言語の数や各言語スキル保持者へのアクセシビリティを考慮。	言語数	数値などのみ扱う	1	2	5	10	100	■定義内容 ２（日本語・英語言語対応）	【レベル】 言語数だけでなく、別途、言語の難易度も併せて検討することが必要である。 また、通貨単位なども考慮しておく必要がある。 【レベル0】 数値データなどのみを扱うとは、人に対するプレゼンテーション機能を想定せず、マシン間でのインターフェースを扱うようなシステムを想定している。例えば、GWシステムなどである。
F.3.1.1		適合規格	製品安全規格	提供するシステムに使用する製品について、UL60950などの製品安全規格を取得していることを要求されているかを確認する項目。	規格取得の有無	規格取得の必要無し	UL60950相当取得					■定義内容 定義しない。	
F.3.2.1			環境保護	提供するシステムに使用する製品について、RoHS指令などの特定有害物質の使用制限についての規格の取得を要求されているかを確認する項目。	規格取得の有無	規格取得の必要無し	RoHS指令相当取得						
F.3.3.1			電磁干渉	提供するシステムに使用する製品について、VCCIなどの機器自身が放射する電磁波をある一定以下のレベルに抑える規格を取得していることを要求されているかを確認する項目。	規格取得の有無	規格取得の必要無し	VCCI ClassA取得	VCCI ClassB取得					
F.4.1.1		機材設置環境条件	耐震/免震	地震発生時にシステム設置環境で耐える必要のある実効的な最大震度を規定。建屋が揺れを減衰するなどの工夫により、外部は震度7超でも設置環境では実効的に最大震度4程度になる場合には震度4よりレベルを設定する。なお、想定以上の揺れではサービスを継続しないでも良い場合には、その想定震度でレベルを設定する。	耐震震度	対策不要	震度4相当（50ガル）	震度5弱相当（100ガル）	震度6弱相当（250ガル）	震度6強相当（500ガル）	震度7相当（1000ガル）		【メトリクス】 設置環境での実効的な震度は、屋外の振動がそのまま伝わる建屋の場合は外部の震度と設置環境の震度はほぼ一致すると考えられるので、外部震度からレベルを設定すればよい。ただし、建屋の免震設備などにより、設置環境での最大震度を低く保証できる場合にはその震度を実効的な震度としてレベル設定が可能と考えられる（ユーザからの特段の要請を受けて、より高いレベルで設定する場合も有り）。なお、一定の震度以上では周辺のシステム利用者がシステムを利用できる環境に無いなどで、サービスの継続が不要となる場合は、その震度からレベル設定することも考えられる。いずれに於いても建屋の耐震震度を超える水準での設定には無理がある。 【レベル0】 地震発生によるサービス停止などのリスクを受け入れる心積もりが別途必要となる。

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
F.4.2.1			スペース	どの程度の床面積(WxD)/高さが必要かの項目。保守作業用スペースについても考慮する。また、移行時には新旧システムが並行稼働可能なスペースの確保が可能か否かについても確認が必要である。可能であれば事前確認を実施する。	設置スペース制限(マシンルーム)	スペースに関する制限無し	フロア設置用機材を用いて構成	ラックマウント用機材を用いて構成					【メトリクス】 具体的な面積と高さも併せて確認する。また、スペース形状や場所による耐荷重の差異にも留意すること。
F.4.2.2					設置スペース制限(事務所設置)	スペースに関する制限無し	専用のスペースを割当て可能	人と混在するスペースに設置必要					【メトリクス】 具体的な面積と高さも併せて確認する。また、スペース形状や場所による耐荷重の差異にも留意すること。 【レベル】 設置スペース制限は前提条件として既に規定されていると捉え、その要求に対してシステムを設置する場合の難易度をレベルとしている。スペース確保の視点での難易度ではないことに注意。
F.4.2.3					並行稼働スペース(移行時)	専用スペースの確保が可能	共用スペースの確保が可能	確保不可					【メトリクス】 構築時に、まだ本番運用で用いるスペースが使用できない場合は、構築時のスペースおよび移設に関しても考慮すること。更に、具体的な面積と高さも併せて確認する。また、スペース形状や場所による耐荷重の差異にも留意すること。 【レベル2】 並行稼働有りの場合には、別途対策を検討すること。関係項目に D.1.1.3、F.4.4.3がある。
F.4.2.4					設置スペースの拡張余地	十分な拡張余地有り	一部制約有り(既製品で対応できるレベル)	制約有り(特注対応や工事が必要)					【メトリクス】 設置スペースの拡張余地には、フロアに直接置くだけでなくラックの制約や床荷重なども含まれる。
F.4.3.1			重量	建物の床荷重を考慮した設置設計が必要となることを確認する項目。低い床荷重の場合ほど、設置のための対策が必要となる可能性が高い。	床荷重	2,000Kg/㎡以上	1,200Kg/㎡	800Kg/㎡	500Kg/㎡	300Kg/㎡	200Kg/㎡		【レベル】 床が耐えられる荷重でレベル化。耐荷重が大きいほど設置に関する制約が少ない。 【運用コストへの影響】 床荷重が高い場合、副次的に高密度な実装となり、高ラック位置での保守作業などが必要になる場合がある。
F.4.3.2					設置対策	不要	荷重を分散するための資材(鉄板など)を配備する	ラック当りの重量を制限して、分散構成を採る	設置環境固有の条件(梁の場所など)を考慮して、設置設計を行う				

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
F.4.4.1			電気設備適合性	ユーザが提供する設置場所の電源条件(電源電圧/電流/周波数/相数/系統数/無停止性/必要工事規模など)と導入システムの適合性に関する項目。同時に空調についても評価対象とする。また、移行時の並行稼動が可能か否かについても確認が必要である。可能であれば事前確認を実施する。	供給電力適合性	現状の設備で特に制限無し	電源工事は必要だが、分電盤改造など二次側の工事のみで対応可能	電源工事は必要だが、一次、二次とも工事可能	工事などができず、規模に対して容量が少し足りない	まったく対応できず、設置場所を再考する必要がある			
F.4.4.2					電源容量の制約	制約無し(必要な電源容量の確保が可能)	制約有り(既製品で対応できるレベル)	制約有り(カスタマイズや工事が必要)					
F.4.4.3					並行稼働電力(移行時)	全面的に確保が可能	部分的に確保が可能	確保が困難					【レベル2】 移行時に並行稼働が必要な場合には、別途対策を検討すること。関係項目に D.1.1.3、F.4.2.3がある。
F.4.4.4					停電対策	無し	瞬断(10ms程度)	10分	1時間	1日間	1週間		【レベル1】 UPS, CVCFなど電源安定化の対策を検討する。
F.4.4.5					想定設置場所の電圧変動	±10%以下	±10%を超える						【レベル1】 機材の動作条件を逸脱する場合には、UPS, CVCFなど電源安定化の対策が必要となる。
F.4.4.6					想定設置場所の周波数変動	±2%以下	±2%を超える						【レベル1】 機材の動作条件を逸脱する場合には、UPS, CVCFなど電源安定化の対策が必要となる。
F.4.4.7					接地	接地不要	接地が必要	専用接地が必要					
F.4.5.1			温度（帯域）	システムが稼働すべき環境温度の帯域条件。 周囲環境によってはシステムを正常稼動させるには特別な対策が必要となることがある。	温度（帯域）	対策不要	16度から32度(多くのテープ装置の稼働可能条件)	5度から35度(多くの機器の稼働可能条件)	0度～40度	0度～60度	-30度～80度		【メトリクス】 温度勾配は10℃/h程度以下に抑えることも併せて考慮する。また、レベル2以上の環境では非稼働時の確認も別途必要である。 【レベル】 機器が稼働している状態での周囲環境の変動範囲でレベルを選択する。例えば、周囲環境温度が0～20度で変動している環境であれば、それを満たすレベルの中で一番低いレベル3となる。
F.4.6.1			湿度（帯域）	システムが稼働すべき環境湿度の帯域条件。 周囲環境によってはシステムを正常稼動させるには特別な対策が必要となることがある。	湿度（帯域）	対策不要	45%～55%	20%～80%	0%～85%	結露無し条件のみ		【レベル】 機器が稼働している状態での周囲環境の変動範囲でレベルを選択する。例えば、周囲環境湿度が20～50%で変動している環境であれば、それを満たすレベルの中で一番低いレベル2となる。
F.4.7.1			空調性能	システムを稼働させるのに十分な冷却能力を保持し、特定のホットスポットが存在する場合にはそれを考慮した冷気供給を行える能力。	空調性能	十分な余力有り	ホットスポットなどへの部分的な対策が必要	能力が不足しており、対策が必要					【メトリクス】 必要に応じて塵芥や有害ガスへの対応なども考慮する。
F.4.7.2					空調設備の制約	制約無し(必要な空調の確保が可能)	制約有り(既製品で対応できるレベル)	制約有り(カスタマイズや工事が必要)					

項番	大項目	中項目	小項目	小項目説明	メトリクス（指標）	レベル						要件	備考
						0	1	2	3	4	5		
F.5.1.1		環境マネージメント	環境負荷を抑える工夫	環境負荷を最小化する工夫の度合いの項目。 例えば、グリーン購入法適合製品の購入など、環境負荷の少ない機材・消耗品を採用する。 また、ライフサイクルを通じた廃棄材の最小化の検討を行う。例えば、拡張の際に既設機材の廃棄が不要で、必要な部材の増設、入れ替えのみで対応可能な機材を採用するなどである。また、ライフサイクルが長い機材ほど廃棄材は少ないと解釈できる。	グリーン購入法対応度	対処不要	グリーン購入法の基準を満たす製品を一部使用	グリーン購入法の基準を満たす製品のみを使用					
F.5.1.2					同一機材拡張余力	無し	2倍	4倍	10倍	30倍	100倍以上		【メトリクス】 既設機材を廃棄することなく、単純に追加で拡張可能であることを意味する（契約上は追加であっても実際には機材全体を置き換えてしまい全廃棄が発生するようなものは対象外となる）。製造エネルギー、廃棄物量までを考慮する。 【レベル】 数倍程度まではスケールアップ主体、それ以上はスケールアウト主体での対応となると考えられる。
F.5.1.3					機材のライフサイクル期間	3年	5年	7年	10年以上				【メトリクス】 ここでのライフサイクルとは実質的なハードウェア入れ替え期間と規定している。基本的に長期に渡って使用することが望ましいが、あまりにも長期過ぎると性能向上や省電力技術の進歩などの恩恵が受けられなくなることにも注意が必要である。 【運用コストへの影響】 ライフサイクルの短い機材を使用すると、頻繁な更新が必要となるため、運用コストが増大する懸念がある。
F.5.2.1			エネルギー消費効率	本来はシステムの仕事量をそのエネルギー消費量で除した単位エネルギー当りの仕事量のこと。ただし、汎用的な仕事量の定義が存在しないため、効率を直接求めることは困難である。また、同じ仕事を行う別のシステムも存在しないことが多いため、比較自体も困難である。このため、エネルギー消費効率に関しては、少し視点を変えて、ユーザからの目標値の提示の有無などでレベル化を行っている。なお、電力エネルギーを前提とするシステムでは、消費電力≒発熱量である。 また、システムの仕事量の視点ではなく、データセンターのエネルギー効率を示す指標にPUE(Power Usage Effectiveness)や、DPPE(Datacenter Performance Per Energy)などがある。	エネルギー消費の目標値	目標値無し	目標値の提示有り	目標値の提示が有り、更なる追加削減の要求も有る					【レベル0】 電源設備などとの整合性の再確認が必要である。 【レベル2】 レベル1の目標値達成に止まらず、更に厳しい基準へのオプション要望があることを示す。 【運用コストへの影響】 低いレベルで合意した場合、新法令の制定などで運用後に対応が必要となる場合がある。
F.5.3.1			CO2排出量	システムのライフサイクルを通じて排出されるCO2の量。ただし、単純なCO2排出量でレベル化するのは困難であるため、少し視点を変えて、ユーザからの目標値の提示の有無などでレベル化を行っている。	CO2排出量の目標値	目標値の設定不要	目標値の提示有り	目標値の提示が有り、更なる追加削減の要求も有る					【メトリクス】 運転時のCO2排出量は基本的に電力消費量とリンクする形になる。これに生産・廃棄におけるCO2排出量を加えたものがライフサイクル全体での排出量となる。 【レベル0】 目標値の設定不要とした場合、CSRなどとの整合性の再確認が必要である。 【レベル2】 レベル1の目標値達成に止まらず、更に厳しい基準へのオプション要望があることを示す。 【運用コストへの影響】 低いレベルで合意した場合、新法令の制定などで運用後に対応が必要となる場合がある。
F.5.4.1			低騒音	機器から発生する騒音の低さの項目。特にオフィス設置の場合などには要求度が高くなる傾向がある。また、データセンターなどに設置する場合でも一定以上の騒音の発生は労働環境として問題となることがある。	騒音値	対策不要	87dB(英国RoSPAの騒音基準による防音保護具の使用も考慮に入れた許容限界値)以下	85dB(英国RoSPAの騒音基準による第2アクションレベル)以下	80dB(英国RoSPAの騒音基準による第1アクションレベル)以下	40dB(図書館レベル)以下	35dB(寝室レベル)以下		【運用コストへの影響】 低いレベルで合意した場合、労働環境との整合性の再確認が必要である。