

循環器病情報サービス
公式ホームページ新規作成

仕様書案

国立研究開発法人
国立循環器病研究センター
令和8年8月

循環器病情報サービス 公式ホームページ新規作成

仕様書 目次

A. 本調達の背景と目的、方針

- A.1 背景
- A.2 目的
- A.3 方針

B. システム要件

- B.1 全体要件
- B.2 情報セキュリティ
- B.3 サーバ構築
- B.4 デザイン作成
- B.5 コンテンツ
- B.6 追加機能
- B.7 納品物

C. 役務要件

- C.1 全体要件
- C.2 開発環境
- C.3 テスト
- C.4 教育
- C.5 運用支援
- C.6 保守管理
- C.7 障害対応
- C.8 月次報告
- C.9 サービスレベル (SLA)

項番	内容
A	本調達の背景と目的、方針
A.1	背景
A.1.1	循環器病は我が国の主要な死亡原因及び要介護要因の一つであり、循環器病対策基本法に基づく総合的な循環器病対策の推進が求められている。循環器病対策を推進するためには、国民が循環器病に関する正確かつ信頼性の高い情報へ容易にアクセスできる環境を整備し、予防、早期発見、適切な治療及び再発予防に関する理解を促進することが重要である。一方で、インターネット上には様々な健康情報が存在するものの、情報の質や信頼性には差があり、国民が適切な情報を選択することが必ずしも容易ではない。循環器病対策情報センター（以下、対策情報センターという）では、循環器病に関する情報を収集・整理し、患者・家族及び一般市民に対して分かりやすく発信するための情報基盤として、「循環器病情報サービス（仮称）」ポータルサイト（以下、当ポータルという）の構築を計画している。本事業では、循環器病に関する科学的根拠に基づく情報を一元的に発信するとともに、利用者にとって分かりやすく利用しやすい情報提供環境を整備することを目的として、新たなホームページを構築する。
A.2	目的
A.2.1	本事業は、循環器病情報サービス（仮称）ポータルサイトを構築し、循環器病に関する信頼性の高い情報を国民に分かりやすく提供することを目的とする。特に、患者・家族及び一般市民に対する情報提供機能の充実を図るとともに、循環器病の予防、早期発見、適切な治療及び再発予防に関する普及啓発を推進する。また、利用者が必要な情報へ円滑にアクセスできる環境を整備し、循環器病対策情報センターの活動内容や成果を広く発信することで、我が国における循環器病対策の推進に貢献することを目指す。
A.3	方針
A.3.1	当ポータルは、患者・家族及び一般市民を主な対象とし、循環器病に関する科学的根拠に基づいた情報を、分かりやすく、利用しやすい形で提供するものとする。サイト構築にあたっては、利用者が必要な情報へ容易にアクセスできる情報設計を重視するとともに、スマートフォン、タブレット及びPC等の様々な利用環境に対応したレスポンスデザインを採用する。また、図表、イラスト、インフォグラフィック等を活用することで、専門的な内容についても直感的に理解しやすい情報発信を行う。さらに、ウェブアクセシビリティに十分配慮し、多様な利用者にとって利用しやすいサイトとするとともに、将来的なコンテンツの拡充や機能追加にも柔軟に対応可能な構成とする。
A.3.2	当ポータルは、上記目的実現のため国立循環器病研究センター（以下、当センターという）とは独立した運用形態とすることで、循環器病情報サービスサイトとして公共性をより高めた価値を提供する。
B	システム要件
B.1	全体要件
B.1.1	当ポータルの本調達における納期は2027年3月末であるが、ポータルサイトとして最低限の形態として2027年1月4日に初期稼働を実現すること。初期稼働の範囲は提案者の提案内容を評価するので、当ポータルの目的と方針に則って提案すること。例えばコンテンツ運用管理のためのCMSは求めているが、初期稼働時には暫定的に静的ページでの構築も可とする。ただし、サイト内検索などはできることが望ましい。
B.1.2	本調達での業務範囲は、2027年3月末までのポータルサイト構築と、2027年1月から3月までのポータルサイト運用保守とする。
B.1.3	2027年4月以降の運用保守や機能拡張は本調達の範囲外とし、契約金額には含めない。ただし提案内容の評価対象とするため、想定される要件（本仕様書「C. 役務要件」を参考にすること）に対する年額の概算を提案書に記載すること。実施にあたっては、当センターの予算措置後に別途協議のうえ契約するものとする。
B.1.4	当ポータルは一般の方を対象とし、誰でも閲覧できるものとする。
B.1.5	トップページのアクセス数は初年度平均150,000件程度/月で年間1,800,000件を想定している。
B.1.6	次年度以降に受注者に求めるコンテンツの更新件数は、機能拡張に伴う大量追加分を除き、月間5件程度を想定している。機能追加については別途受託者に対策情報センターとでスケジュールやサーバ資源について協議の上、決定するものとする。
B.1.7	当ポータルに取り込むコンテンツの記事や図表案作成、ならびに医学監修は対策情報センターが行うが、ページ作成に当たり、統一されたイメージ確保のためのコンテンツデザインの作成、アクセシビリティ準拠のために必要と考える修正、追加は受託者にて行うこと。なお、受託者が新規に制作する図版・イラストは、初期稼働時・2027年3月末時点を通じて合計100点程度を上限とし、これを超える分については別途協議のうえ単価により算定する。
B.1.8	本業務は、以下の規格・指針に準拠すること。 ・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 ・デジタル庁「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（DS-221）」 ・デジタル庁「政府機関等のドメイン管理に関するガイドライン（DS-900）」 ・JIS X 8341-3:2016（適合レベルAA） ・総務省「みんなの公共サイト運用ガイドライン（2024年版）」 ・IPA「安全なウェブサイトの作り方」 ・厚生労働省「医療広告ガイドライン」 ・当センターの情報セキュリティポリシーその他の関連規程
B.1.9	当ポータルはISMAP認定のクラウドサービスを利用して構築すること。
B.1.10	当ポータルは国内法の適用される環境に構築すること。

B. 1. 11	将来の機能拡張や規模拡大に備えて、柔軟でリーズナブルなスケーラビリティを担保できること。
B. 1. 12	その他、情報セキュリティポリシーなどの関連するガイドラインなどに可能な限り準拠する。
B. 1. 13	本業務の実施にあたり、対策情報センターが特に必要と認めた場合は、受託者との合意により本仕様書の一部について追加、変更ができるものとする。
B. 1. 14	当ポータル及びCMSに格納される文書・画像等のデータ及び内容に関する諸権利は、原則として当センターに帰属する。ただし、受託者が本業務以前から有する汎用的なプログラム、ライブラリおよび技術に係る権利は、受託者に留保されるものとする。受託業務の実施において、当センターに限らず、原著作者の著作権を不正に侵害することのないよう、厳に注意すること。
B. 1. 15	CMSは特定の事業者依存しない構成とすること。契約終了時に保守費用の範囲で、コンテンツ・データベースの内容を汎用的な形式でエクスポートでき、ソースコードおよびカスタマイズ内容を当センターまたは次期受託者に引き渡せること。
B. 1. 16	受託業務の実施に伴い適用を受ける法令、規程、基準等についてはこれを遵守すること。また、当センターの規程等も遵守すること。
B. 1. 17	仕様書に記載されていない事項、法令により義務付けられている事項及びその他の事項についても、業務上当然必要な事項については、受託業務の範囲に含まれるものとする。なお、疑義が生じた場合、および受託者の提案書に記載のない事項で相当の工数を要する場合には、当センターと受託者の間で協議し、取り決めるものとする。
B. 1. 18	本仕様書要件の実現に必要な費用は、全て本調達に含むこと。ただし、本仕様書において契約締結後の協議により内容を決定するとされた要件については、協議により範囲を確定したうえで、本調達に含む範囲を定めるものとする。
B. 1. 19	本業務の成果物（本ウェブサイト）の検収後、1年の間に、正当な理由無く、この仕様書に記載した要件を満たしていないことが判明した場合および受注者の責任とみなされる不具合が生じた場合には、当組織と協議の上、無償で改良すること。なお、この場合、不足している機能および不具合部分のみの修正すること。
B. 2	情報セキュリティ
B. 2. 1	本業務における情報セキュリティ対策は、契約締結時点における最新版の「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」、当センターの情報セキュリティポリシー、デジタル庁「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（DS-221）」の実施基準、およびIPA「安全なウェブサイトの作り方」に準拠すること。当センターの情報セキュリティポリシーが原則的に優先する。契約期間中に上記基準が改訂された場合の対応要否および費用については、当センターと受託者が協議のうえ決定する。
B. 2. 2	作業の一部を再委託する場合は、提案時に再委託先、再委託内容を提示し、当センターに許可を求めること。
B. 2. 3	受託者は、以下を含む情報セキュリティ対策を実施すること。また、その実施内容及び管理体制についてまとめた情報セキュリティ管理計画書を作成し、当センターの承認を受けること。
B. 2. 4	受託者の資本関係・役員等の情報について情報提供を行うこと。
B. 2. 5	本業務従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）に関する情報提供を行うこと。
B. 2. 6	情報セキュリティ管理計画書には、最低限次の内容を記載すること。 ・業務従事者（再委託先も含む）の情報セキュリティ対策実施状況（講習受講有無なども） ・業務に使用するデバイスの情報セキュリティ対策実施計画・状況 ・情報セキュリティ管理体制図・インシデント対応フロー ・データの共有・廃棄の手順
B. 2. 7	対策情報センターから要保護情報を受領する場合は、情報セキュリティに配慮した受領方法にて行うこと。
B. 2. 8	対策情報センターが提供する情報（資料等）は、情報セキュリティ管理体制の下、第三者への漏えいや目的外利用が行われないよう、適切に管理すること。
B. 2. 9	本業務の実施に当たり、受託者またはその従業員、本調達の役務の内容の一部を再委託する先、若しくはその他の者による機密情報の窃取や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。
B. 2. 10	対策情報センターから受領した要保護情報が不要になった場合は、これを確実に返却、または抹消し、書面にて報告すること。
B. 2. 11	セキュリティ対策を考慮したプログラム及びWEBサイトのコーディングを行うこと。
B. 2. 12	納品前に脆弱性診断を行い、結果について対策情報センターの承認を得ること。
B. 2. 13	初期稼働時の脆弱性診断としては、プラットフォーム脆弱性診断、およびIPA「安全なウェブサイトの作り方」に基づく実装確認の結果報告をもって、これに代えるものとする。
B. 2. 14	年度末納品物に対する脆弱性診断は下記を実施すること。 ①ウェブアプリケーション脆弱性診断：外部に公開する動的機能（コンテンツ管理システムにより動的に生成される公開ページ、問い合わせフォーム、サイト内検索、管理画面、API等）を対象とする。 ②プラットフォーム脆弱性診断：本サイトを配信するサーバ・クラウド基盤・ミドルウェア・通信設定のうち、外部から到達可能な範囲を対象とする。

B. 2. 15	検出した脆弱性の深刻度は、CVSS (v3.1 または v4.0) の基本評価基準による5段階で評価し、評価根拠および現実的な攻撃可能性を明記すること。CVSS 基本値 7.0 以上 (重要・緊急) に該当する脆弱性が存在しない状態を、納品 (検収) の要件とする。CVSS 基本値 6.9 以下 (警告以下) については、悪用可能性および対応の費用対効果を対策情報センターと協議のうえ、改修期限またはリスク受容を決定する。ただし、国内外で悪用が観測されている脆弱性は深刻度にかかわらず速やかに対応すること。
B. 2. 16	当センターでは公的機関または第三者機関により当システムのペネトレーションテストおよび脆弱性診断を行うことがある。その際には、必要に応じて協力対応すること。
B. 2. 17	各種テストまたは診断の結果、重大な情報セキュリティに関わる指摘があった場合、対策情報センターの求めに応じて必要な資料を提供し、速やかに調査や動作環境の改修等を実施すること。この場合に必要費用は、受託者の責めに帰すべき事由による場合は受託者の負担とし、それ以外の場合は両者協議のうえ決定する。
B. 2. 18	本体・テーマ・プラグイン等の脆弱性情報を継続的に把握し、更新を効率的に適用する仕組みおよび更新漏れを防止する仕組みを備えること。
B. 2. 19	CMS及びプラグイン等の脆弱性情報が公開された場合は、影響を対策情報センターと協議の上、バージョンアップを行うこと。
B. 2. 20	サポートが終了した製品・プラグインを使用しないこと。有償ライセンスを要する場合は、費用、必要数量、および2027年4月1日以降に発生する年額を明示すること。
B. 2. 21	公開系サイトにはWAF (Web Application Firewall) を導入すること。
B. 2. 22	本業務において、情報セキュリティインシデントの発生または情報の目的外利用等を認知した場合は、速やかに対策情報センターに報告すること。
B. 2. 23	納品物に含む運用手順書には、情報セキュリティ水準の維持に関する手順や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など情報セキュリティ対策を実施するために必要な手順を含むこと。
B. 2. 24	情報セキュリティ対策に関する履行状況を再委託先含めて定期的に確認し、対策情報センターへ報告すること。
B. 2. 25	情報セキュリティ対策の履行が不十分であると認められた場合、速やかに改善策を提出し、対策情報センターの承認を受けた上で実施すること。
B. 3	サーバ構築
B. 3. 1	サーバの要件
B. 3. 1. 1	当ポータルは、当センターが保有する ncvc.go.jp のサブドメイン (〇〇.ncvc.go.jp) として構築すること。
B. 3. 1. 2	当ポータルには以下の3環境を用意すること。なお同一OS上に公開ディレクトリを分けて、実装しても良い。 ・本番環境 ・事前確認環境 ・検証環境 それぞれ以下の役割で準備したものである。ライセンスなどが必要な場合は、本環境数分の用意を受託者が行うこと。 ・「本番環境」とは、インターネット側から不特定多数が閲覧することを想定した公開用の環境である。 ・「事前確認環境」とは、コンテンツを投稿・確認するための環境である。ここに投稿し完成したコンテンツは、定期的に「本番環境」へ同期して公開される。インターネット側からアクセスできない非公開のHPである。 ・「検証環境」とは、「本番環境」「事前確認環境」に大きな変更を施す前の、CMSやテーマの動作確認を行うための環境である。例えばメニュー階層の変更や、テーマ・デザイン変更などの比較的開発行為に近い業務に用いる。
B. 3. 1. 3	ページ更新などの運用は対策情報センター職員で行うため、前項に示す環境に適応したコンテンツ管理、CMS設計など必要な対応を行うこと。
B. 3. 1. 4	構築したWebコンテンツについては、公開・非公開について適切なアクセス権限を設定し、不正アクセスや情報漏洩が起こらないようにすること。
B. 3. 1. 5	Webコンテンツの管理画面については、IPアドレスやユーザ名によるアクセス制限を施すこと。また、Well Knownなパスは用いないこと。
B. 3. 1. 6	アカウントロックの機能を実装すること。アカウントロックされた場合、管理者へ通知ができ、システム管理者によるロック解除か、一定時間経過でのロック解除を設定可能なこと。対応不可能な場合は提案時に明示すると共に、契約後にセンターと対応を協議すること。
B. 3. 1. 7	ウェブサイト内のリンク切れを検出する機能を実装すること。または、年1回、受託者においてリンク切れを確認すること。
B. 3. 1. 8	入力フォーム等からの送信の際は、SSL (TLS1.2 または TLS1.3) による暗号化通信を行うこと。
B. 3. 1. 9	インターネットに公開するサーバは、ファイアウォールにより本サイトの運用に必要な通信ポートおよびIPアドレスのみを許可し、不正アクセスから保護すること。
B. 3. 1. 10	パスワードが不正利用されないように、パスワードをデータベースに保存する場合は、暗号化を行うこと。
B. 3. 1. 11	可用性向上のためネットワークスイッチを含めサーバ環境は冗長構成とし、UPSなどによる停電対策をおこなうこと。また公開サーバに障害が起こった際も、冗長構成により影響を最小限に留めて継続して運用できること。

B.3.1.12	各環境は万一の障害が発生した際でも、前日の状況に復元できるようにバックアップを取得すること。
B.3.1.13	受託者は、新サーバの公開ディレクトリに、公開する必要のないファイル、例えば作業中のファイルやリネームしたバックアップ目的のファイル類を放置せず、公開前に削除すること。
B.3.1.14	WEB閲覧のプロトコルは全てhttpsに限定する。httpについては、リダイレクトも含めて無効とすること。
B.3.1.15	https 通信に使用するSSLサーバ証明書は、当センターが提供する証明書を使用すること。（本調達には証明書の発行費用を含めないこと。）
B.3.1.16	ドメインの名前解決には当センターのDNSサーバを利用すること。（本調達にはDNSサーバの構築・維持費用を含めないこと。）
B.3.1.17	次期ウェブサイトや他システムに対して、容易にデータ移行を行うことができるように、受託者以外の者でも本ウェブサイト内の全データを汎用的な形式（XML、SQL、CSV等）で取り出すことができること。あわせて、掲載コンテンツの一覧（コンテンツ区分、タイトル、URL、公開日、最終更新日、および紐づくメディアファイル名）をCSV形式で出力できることとし、写真ファイル等は元データのファイル形式で一括して取り出せることとする（移行先でも本ウェブサイトと同様に掲載できるよう配慮すること。）。
B.3.1.18	データ一覧（データ名、データ形式、データ長、データ件数、およびデータベース上で管理している項目のうち対策情報センターが指示した項目）の提出の指示があった場合は対応すること。
B.3.2	ソフトウェアの要件
B.3.2.1	本調達で、サーバに準備されているソフトウェアに加えて、必要とするソフトウェア（プラグインなど含む）およびそのライセンスがある場合は、「本番環境」と「事前確認環境」、「検証環境」の全ての環境に適用すること。
B.3.2.2	Webサイトの管理目的として、複数のユーザーアカウントを登録できること。複数ユーザーによる操作を想定したデザイン、操作とすること。
B.3.2.3	各ユーザーアカウントには、それぞれ編集可能となる領域・コンテンツ・ページなどを設定し、利用できる機能を制限できること。権限ロールはシステム管理者・承認者・編集者・投稿者等の5種類程度を上限として定義し、編集可能領域は当該ロールと領域（部門・カテゴリ）の組み合わせにより設定できる構成とすること。
B.3.2.4	本調達で導入するCMSについて、情報セキュリティ対策として頻回にバージョンアップする必要があると考える。この方針に準拠し、頻回なバージョンアップが可能となるように構築すること。
B.3.2.5	CMSのログイン履歴を取得すること。IPアドレス、ユーザー名、日時、結果（成功か失敗）か、これらは必須項目とする。操作内容（コンテンツの新規投稿、更新、削除など）については、可能な限り詳細に取得すること。ただし負荷やログのサイズの検討も必要であることから、導入工程において対策情報センターと協議の上、決定すること。
B.3.2.6	当ポータルの利用状況の分析を行うことができるように、閲覧記録（閲覧総数、アクセス元情報、閲覧端末の種類等）や各種ログを残す仕組みとすること。保存期間は1年とし、対策情報センターへのアーカイブができること。
B.3.2.7	受託者は本業務を遂行するにあたり、使用する受託者のデバイス(OS問わず)について、常にそのOSなどを最新化して脆弱性対策を施すと共に、マルウェア・ウィルス対策を実施すること。
B.4	デザイン作成
B.4.1	患者や患者家族に限らず循環器病に関心を持つ多くの一般国民が、必要な情報にアクセスしやすいこと、および医師・医療従事者向けに鮮度と客観性の高い情報提供ができることに配慮したトップページとすること。
B.4.2	トップページには、メインイメージ画像、重要なお知らせ、トピックス、新着情報は掲載すること。
B.4.3	ウェブサイト全体の構造はできるだけシンプルなものとし、必要最低限の階層構造に留めること。
B.4.4	新着情報はコンテンツの新規追加と削除に対して、自動的に更新されること。
B.4.5	公開日時、および公開終了日時の設定ができること。
B.4.6	下書き、公開、非公開、アーカイブの状態を管理できること。
B.4.7	変更履歴（リビジョン）を保持し、過去の版に復元できること。
B.4.8	メディア（画像、PDF、動画）を登録・管理でき、代替テキストを必須項目として設定できること。
B.4.9	Webサイトを構成するすべてのページについて、ページ名称、URL、階層、ファイル名、最終更新日、リンク情報などで構成されたディレクトリマップを作成し提出すること。
B.4.10	管理を目的とし、作成した記事の一覧（タイトル、リンク、作成者、作成日）をCSVなどのファイルに出力できること。出力タイミングはユーザーの操作によるものとする。
B.4.11	利用者の利便性を重視したナビゲーションの配置やページ構成とし、利用者別に必要な情報が公開され、すべての利用者にとって「わかりやすく」「探しやすい」サイトを構築すること。
B.4.12	直感的に理解がしやすく迷いにくいナビゲーションの仕組みや、掲載されている情報の識別が容易で内容を読み取りやすいデザインを実現すること。
B.4.13	サイトマップ（HTML、XML）を掲載すること。ページの新規追加と削除に連動して、自動的に更新されること。
B.4.14	全ページである程度統一したデザインとし、操作にも一貫性を持たせること。
B.4.15	デザイン作成では複数案を提示し、対策情報センターと協議の上での決定とすること。

B. 4. 16	コンテンツの掲載承認処理について、ワークフロー機能までは求めないが、1段階の承認ではなく2段階の承認処理ができることが望ましい。
B. 4. 17	マニュアルの作成については、CMSの技術的操作マニュアル、運用マニュアル（システム管理マニュアル、コンテンツ作成者向け操作マニュアル、承認者向け操作マニュアル等）を作成すること。また、マニュアルは、イラストや画面のハードコピーを用いて、分かりやすく解説し、業務に不慣れな職員でも理解できるように平易な用語を用いること。
B. 4. 18	最新のウェブアクセシビリティ（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」への準拠）はJIS AAを基準とした、年齢や性別の違い、インターネット利用の習熟度、障害の有無等に関わらず、それぞれの利用者が状況に応じて快適に利用できるサイトを実現すること。
B. 4. 19	対策情報センターと協議の上、アクセシビリティ配慮の重要性や具体的な対応方法を記した資料（ウェブアクセシビリティ方針、実装チェックリスト、およびコンテンツ作成者向けの留意事項）を作成すること。また、資料は画面のハードコピー等を用いて分かりやすく作成し、アクセシビリティについての知識がなくとも理解できるように平易な用語を用いること。
B. 4. 20	アクセシビリティ試験は年度末納品時に実施する。試験は JIS X 8341-3:2016 附属書JB および WAIC「JIS X 8341-3:2016 試験実施ガイドライン」に基づき、テンプレート種別ごとの代表ページとランダム選択ページを併用し、合計40～50ページ程度を対象とする。試験対象ページ数および選定方針は、事前に対策情報センターの承認を得ること。初期稼働時には、テンプレート単位の自己点検（実装チェックリストによる確認）を行い、その結果を報告すること。
B. 4. 21	総務省「みんなの公共サイト運用ガイドライン（2024年版）」に沿い、「ウェブアクセシビリティ取組確認・評価表」を用いて年1回取組を確認し、結果を公開できる運用手順を整備すること。
B. 4. 22	適用デザインの表現力を高め、当ポータルを戦略的・効果的にPRしていくことで、視覚的訴求力のあるホームページを実現すること。
B. 4. 23	ホームページ制作上の最新技術を提案、活用すること。Adobe FlashやMicrosoft Internet Explorer等、廃止が決定している製品および技術を用いて製作してはならない。
B. 4. 24	下記のOS・ブラウザでの閲覧に対応すること。 ＜OS＞ Windows：Windows11以降、macOS：Apple社がセキュリティアップデートを提供する最新3バージョン、iOS：最新版、Android：最新版 ＜ブラウザ＞ Google Chrome：最新版、Microsoft Edge：最新版、Firefox：最新版、Safari：最新版
B. 4. 25	スマートフォンやタブレット端末などを含めた、あらゆるデバイスからの閲覧に対応し、見やすいレイアウトを維持できるようレスポンシブデザインを基本とすること。
B. 4. 26	印刷を考慮したデザインとすること。具体的には、バナー、サイドバー、画像が本文に重なってしまうような不具合が発生しないこと。
B. 4. 27	削除したページならびに公開を取り下げたページに紐づくファイルが、検索エンジンで表示されないこと。本番環境から物理的に削除しても構わない。上記が難しい場合は、非公開ページに紐づくファイルがCMS上で簡単に判別でき、削除できるような機能・運用を提案すること。
B. 4. 28	複数のページから参照されるファイルについては、部品化してファイル更新の影響が多ページに及ばないようにすること。
B. 4. 29	一般の方に向けたページは、文字が多くなり過ぎないように、かつ、必要な情報が得られるよう構成を提案すること。一般の方が理解しやすい言葉になっているかの確認も行うこと。
B. 4. 30	一般の方に向けたFAQを掲載できる機能を実装すること。FAQの設問・回答の原稿は対策情報センターが作成し、受託者は分類・検索・表示に関する設計および実装を行うとともに、検索ログの分析に基づくFAQ候補の提案を行うこと。
B. 4. 31	トップページには各種のバナー設置に対する要望が多くなることが予想されることから、バナーを多く配置しても分かりやすく、見栄えも損なわないデザインまたは仕組みとすること。
B. 4. 32	新たなコンテンツの追加や既存情報の更新を行う際にデザインの統一性を保持するために必要なテンプレートファイルを作成すること。テンプレートの種別数は、初期稼働時4種類程度、2027年3月末時点で合計6種類程度を想定する。種別、構成および数は、提案を踏まえ、契約後の情報設計工程において対策情報センターと協議のうえ確定する。対策情報センタースタッフによる更新が自由かつ容易となる工夫を提案すること。
B. 4. 33	当ポータルにおける独自のエラーページを作成すること。
B. 4. 34	当ポータル外へのリンクについては、クッションページを設けること。クッションページには遷移先が当ポータル外であることを明記すること。
B. 4. 35	対策情報センターが入力した「重要なお知らせ」を、強調表示するデザインであること。
B. 4. 36	「重要なお知らせ」はトップページに目立つよう掲載できること。
B. 4. 37	「重要なお知らせ」は掲載期限を設定でき、期限が過ぎたらトップページから見えなくなること。
B. 4. 38	当ポータル内の検索が可能であること。検索エンジンを利用してもよい。
B. 4. 39	検索窓はナビゲーションメニューに含み、トップページに表示されているようにすること。
B. 4. 40	ホームページを構成するコードファイルは、HTML、CSS、JavaScriptを原則とすること。廃止が決定している製品および技術を用いて制作してはならない。
B. 4. 41	第三者が制作・配布したコード、画像、マルチメディアデータを使用・流用する場合は、著作権侵害とならないことを確認できる情報を添えて事前に対策情報センターに報告し、承諾を得ること。

B. 4. 42	原則として使用料の発生するコード、画像、図版等は使用しないこと。
B. 4. 43	各ページには内容を的確に表すタイトルを付けるとともに、Googleなどの検索エンジンから本ホームページを容易に見つけ出せるよう、検索キーワードなどに工夫を凝らし、有効なSEO対策を可能な限り実施すること。
B. 4. 44	アクセス統計等の分析を行い、分析結果の報告及び改善に向けた提案を行うこと。
B. 4. 45	PV以外の評価指標も定量指標（KPI）として設定し、計測できるよう提案すること。
B. 4. 46	SNSなどでホームページへのリンクを貼りつけた場合、アイキャッチ画像が動作するようにすること。
B. 5	コンテンツ
B. 5. 1	作成するページ数は、2027年1月の初期稼働時点で概ね30ページ程度、2027年3月末の時点で70ページ程度を想定しているのに対応できること。ただしチャットポッドやBI連携実装などとの優先順位に関して、対策情報センターと合意できた場合はこの限りではない。
B. 5. 2	画像ファイル（図表、写真）の形式は、GIF、JPEG、PNG、WebP、AVIFのいずれかとする。これ以外の形式を使用する場合は、対策情報センターと協議の上、決定すること。
B. 5. 3	第三者が制作・配布したコード、画像、マルチメディアデータを使用・流用する場合は、著作権侵害とならないことを確認できる情報を添えて事前に対策情報センターに報告し、承諾を得ること。
B. 5. 4	原則として使用料の発生するコード、画像、図版等は使用しないこと。
B. 5. 5	「循環器病あれこれ」その他、当センター以外の者が著作権を有するコンテンツを本サイトに掲載する場合、当該著作権者からの利用許諾の取得は対策情報センターの責任において行うこととする。
B. 5. 6	厚生労働省「医療広告ガイドライン」を十分に理解し、ガイドラインに準拠するだけでなく、正確な情報、利用者に誤解や過大な期待を持たせる情報とならないようにコンテンツを作成すること。受託者は、制作の過程において同ガイドラインに照らして疑義のある記載を認めた場合は、速やかに対策情報センターに報告し、協議のうえ修正を行うこと。最終的な適合性の判断は対策情報センターが行う。
B. 6	追加機能
B. 6. 1	2026年12月末納期の初期構築での実装は不要であるが、2027年3月末の時点では下記機能を実装すること。なお内容については契約開始後の協議にて決定するが、提案価格内で実装できる内容を企画書にて提案すること。 ・チャットポット ・BI連携
B. 7	納品物
B. 7. 1	受託者は、以下の内容を含む納品文書を作成し、紙媒体を1部と、編集可能な電子ファイルを納品すること。
B. 7. 2	情報セキュリティ管理計画書
B. 7. 3	システム構成図
B. 7. 4	アカウント一覧
B. 7. 5	ソフトウェア一覧（名称、バージョン、パラメータ等）
B. 7. 6	設計図書（ディレクトリマップ／テンプレート仕様書など）
B. 7. 7	操作マニュアル（管理者用、利用者用）
B. 7. 8	運用マニュアル（障害対応手順を含む）
B. 7. 9	Webアクセシビリティガイドライン
B. 7. 10	脆弱性診断報告書および是正結果報告書
B. 7. 11	打ち合わせ議事録
B. 7. 12	運用計画書
B. 7. 13	月次報告書
C	役務要件
C. 1	全体要件
C. 1. 1	本業務の実施体制として、プロジェクト責任者およびプロジェクトマネージャを置くこと。
C. 1. 2	プロジェクトマネージャは不測の事態を除き本業務の開始から終了まで同一人物とすること。
C. 1. 3	対策情報センターが想定している下記日程を参考に、業務遂行のスケジュールを作成すること。 ・キックオフミーティングの開催・・・2026年11月6日までに開催 ・初期稼働システムの構築完了・・・2026年12月31日 ・本調達範囲での全ての構築完了・・・2027年3月31日
C. 1. 4	キックオフミーティングには下記の資料を用意すること。 ・PJ実施・連絡体制表、 ・業務実施スケジュール案、 ・情報セキュリティ管理計画書（第1版）
C. 1. 5	契約締結後2週間以内に、対策情報センターと合意した業務実施スケジュールを提出すること。また、スケジュールが予定から変更となる場合は対策情報センターへ連絡し、スケジュールを提出の上、再調整の承認を得ること。
C. 1. 6	本業務は短納期のため、基本的に隔週での打ち合わせを実施し、十分な情報共有とタイムリーな意思決定を心がけること。

C.1.7	対策情報センターからのコンテンツの支給などは合意したスケジュールに従った期限とする。具体的には、契2026年11月13日までに初期稼働に掲載するコンテンツの最終版（医学監修済みのもの）の支給およびデザイン案の決定を行うものとし、2027年3月末掲載分のコンテンツ最終版は2027年1月末までに支給するものとする。また、対策情報センターは、受託者からの確認・承認依頼に対し原則5営業日以内（コンテンツの内容確認および医学監修に係る回答は10営業日以内）に回答するものとし、コンテンツの確認・監修の往復は1ページあたり原則2往復以内とする。対策情報センター側の事情によりこれらに遅延が生じた場合は、公開ページ数やスケジュールについて協議により決定するものとする。
C.1.8	受託者は、受託した業務を遂行するための手順を明らかにし、最良の業務水準を維持するために、常にその改善を図ること。
C.1.9	受託者は、デザイン案の決定など、納期を意識したスケジュール管理を心掛け、対策情報センターがこの期限内に意思決定を行えるよう、決定に必要な選択肢と判断材料を提示すること。
C.1.10	受託者は、必要な知識、経験、技能を持った従事者をもって業務実施にあたらせ、適切かつ円滑な業務の遂行のために、常に必要な体制を整備すること。
C.1.11	受託者は、受託したすべての業務の遂行のために、従事者に対策情報センターと常に円滑な連携を図らせること。
C.1.12	受託者は、当ポータルをの目的を理解し、従事者にその達成を常に意識させるとともに常に問題意識を持ち、対策情報センターに対して業務改善のための企画・提案を行うこと。
C.1.13	受託者は、WEB会議によるコミュニケーションが可能であること。なお、対策情報センターがWEB会議を主宰する場合は、Microsoft Teams を活用するので対応すること。
C.1.14	受託者は、会議体の議事録を作成し、会議開催の翌日を初日として数えて3営業日以内に対策情報センターに提出し承認を得ること。
C.1.15	初期稼働時にCMSを実装しなかった場合は、CMS稼働時に以前のページをCMSに取り込むこと。
C.1.16	契約の満了または解除に当たっては、当ポータルに掲載内容に係る一切のデータ、コンテンツ管理システムのカスタマイズ説明書、ソースコードおよびアカウント情報を、対策情報センターまたは次期受託者に遅滞なく引き渡すこと。これに要する費用は本契約の費用に含むこと。
C.2	開発環境
C.2.1	受託者は、本業務の設計・制作・開発作業を受託者の環境、またはクラウド環境において実施すること。対策情報センターの内部環境への接続を要する作業に限り、当センターが提供するリモート接続環境を利用すること。
C.2.2	開発作業場所は受託者オフィスとする。操作研修等で当該施設を利用する場合は、別途協議しスケジュールを調整すること。
C.2.3	開発作業のために必要な機材は、サーバ環境も含めて受託者が準備すること。
C.2.4	本ウェブサイトのサーバ管理に使用する受託者の端末は、IPアドレスまたはMACアドレスによる認証を行い、端末の利用者についてはID・パスワードによる管理を行うこと。
C.2.5	本ウェブサイトのサーバ管理に使用するIDは必要最小限とし、IDに対する権限は明確かつ必要最小限にすること。なお、ログインIDは本委託業務に携わる作業者の人数分とし、共用はしないものとする。
C.2.6	端末には、パスワードを記憶させないこと（オートコンプリート機能は使用しないこと。）。
C.2.7	開発作業場所の施錠や機器の固定等の盗難防止や破損等を防止するための対策を講じること。
C.2.8	本業務に関して行った作業について記録すること。
C.3	テスト
C.3.1	当ポータルの公開前に、システムテストを実施すること。
C.3.2	テストは受託者が主体となって実施すること。
C.3.3	事前検証および最終検証とも事前にテスト計画書を当組織に提出し、承認を得たうえで実施すること。
C.3.4	テスト計画書は、本仕様書に記載するすべての機能、受託者が提案した機能、および打合せにより合意した機能が正常に動作することが確認できるように作成すること。
C.3.5	テスト実施時に併せて、対策情報センターがシステム操作テストを実施できるようにすること。
C.3.6	テスト実施後は、テスト結果表を対策情報センターに提出すること。
C.4	教育
C.4.1	対策情報センター職員向けに以下のマニュアルを作成し、関係職員に対して当ポータルの運営に支障がないよう教育すること。マニュアルは契約満了までにPDF形式および編集可能なファイル形式（Wordファイル等）で提出すること。
C.4.2	CMSの操作マニュアル 必要な事柄を説明する図解マニュアルを作成提出し、承認を得ること。職員向けマニュアルではCMSの操作方法だけでなく、当ポータルを作成するために必要な知識と手順を説明する。テーマの更新や設定の変更、カスタマイズ等で運用手順などに変更がある場合、マニュアルも速やかに改訂すること。
C.4.3	運用マニュアル、障害時対応マニュアル 保守・運用及び緊急時の対応に必要な事柄を説明するマニュアルを作成すること。

C. 4. 4	受託者は、運用マニュアルに基づいて、対策情報センターの職員に以下の導入教育を実施すること。 ・コンテンツ管理（新規追加、更新、削除、予約反映、取下げなど） ・アクセスログ管理（CMSのログ、WEB閲覧ログなど） ・アクセス解析方法 ・ソフトウェアバージョン管理（OS、ライブラリ、CMS） …ソフトウェアの一覧をバージョンを含めて記載すること。 ・障害管理（調査方法、切り分け方法、よくあるエラー） …受託者が本業務の中で導入あるいは設定を変更したソフトウェアについて、本業務完了後に対策情報センターの職員がよくあるエラーとその対応方法を参照できること 対象とする職員は10人前後で、時間は3～5時間程度を想定している。 WEB会議での開催も認める。
C. 5	運用支援
C. 5. 1	受託者は、受託期間中、以下の要件を満たす運用支援を実施すること。
C. 5. 2	運用支援に関連する質問及び相談に対する回答は、電話、メール、Web会議、または対策情報センターに出向いての対面により、3営業日以内に行うこと。時間外の緊急質問及び相談については、可能な限り迅速に対応すること。
C. 5. 3	当ポータルコンテンツを更新する上で、定期的もしくは随時に必要となる業務について、対策情報センターからの依頼に速やかに対応できる体制を整備すること。対応するコンテンツの更新件数は月間5件程度を想定する。これを大きく超える依頼が生じた場合は、対応時期および費用について協議するものとする。
C. 5. 4	CMS上で変更できないコンテンツに関しては、作成・変更を行うこと。その際は、既存CMSに関するカスタマイズ説明書を確認した上で、コンテンツの運用を行うこと。
C. 5. 5	サーバ上でコンテンツのテスト環境、検証環境および本番環境が用意されるので、運用保守管理を行うこと。なお、テスト環境、検証環境は対策情報センター内部のみに公開される。
C. 5. 6	次の場合は、作業前に対策情報センターに報告の上、事前了承を得てから対応すること。 ・テンプレートのテーマに追加・変更を行う場合 ・トップページに追加・変更を行う場合 ・各部門以外のコンテンツに影響を与える修正を行う場合 ・その他、報告が必要と考えられる場合
C. 5. 7	各種不具合が発生した場合、原因の調査および復旧作業を迅速に行い、結果を対策情報センターに報告すること。
C. 5. 8	必要に応じて、テンプレートの作成・追加、デザインの提案・修正・更新を行うこと。ただし新規作成については、作業状況を踏まえて協議の上での決定とする。
C. 5. 9	WEBサイトを構成するすべてのページについて、ページ名称、URL、階層、ファイル名、最終更新日などで構成されたディレクトリマップを作成・更新し、12ヶ月に1回、対策情報センターに報告すること。
C. 5. 10	当ポータルの基本的な改修に関する費用は、本契約に含めること。ただし、全ページの個別リニューアル等、相当数の工数を要する改修については、対策情報センターと別途協議することができる。
C. 5. 11	対策情報センターからの要望、相談に対し、誠実かつ専門的に対応するとともに、積極的に新しい技術・技法の提案や解決策を提案するよう努めること。
C. 6	保守管理
C. 6. 1	契約期間中、コンテンツ、CMSのプラグイン等および独自開発したプログラムに対して保守が行える体制を構築すること。
C. 6. 2	本受託業務に関する責任者及び担当者を定め、責任者及び担当者等が記載された業務体制表を整備し、対策情報センターに提示すること。責任者および担当者に変更になった場合は、遅滞なく対策情報センターに連絡すること。
C. 6. 3	受託者の保守用端末およびサーバは、ウィルス対策ソフトウェアを常時稼働させ、定期完全スキャンおよびパターンファイルの更新を行うこと。定期完全スキャンは自動設定も可とするが、少なくとも週1回以上は行うことまた、パターンファイルの更新は、原則として、ベンダーリリース後1日以内とする。なお、サーバについては、クラウドサービス事業者が提供する脆弱性管理・マルウェア検知・ファイル改ざん検知等の機能により、同等以上の措置を講じることでも良い。
C. 6. 4	サーバへのアクセス状況を監視し、不正アクセス等の被害を検出した場合、または兆候が見られる場合は、速やかに対策情報センターに報告し、指示を仰ぐこと。
C. 6. 5	同一IPアドレスからのセッション数の上限設定をする等、Ddos攻撃への対策を行い、定期的に設定を見直すこと。
C. 6. 6	ソフトウェア・プラグイン等のバージョンアップに関しては、その適用の判断に必要な調査・評価を行ったうえで、バージョンアップ版の提供及びインストール作業を行うこと。
C. 6. 7	CMSデータ、データベースおよび各種ログのバックアップを1日1回実施し、7世代保管すること。
C. 6. 8	プログラムの大幅な改修を行う場合は、フルバックアップを行うこと。
C. 6. 9	少なくとも3ヶ月に1回、SEO対策についての取り組み状況および結果（具体的な検索順位の遷移等）を報告すること。
C. 7	障害対応

C.7.1	当ポータルに障害が発生した場合は、直ちに状況の把握を行い、障害箇所の特定、影響範囲の調査を行い、速やかに必要な障害復旧体制を構築すること。
C.7.2	なお、対応時間帯は原則として土、日曜日、祝日及び年末年始の休日（12月29日～1月3日）を除く9:00-17:00とする。
C.7.3	ただし、当ポータル全体の閲覧不可など、重大な障害の場合には休日でも対応を依頼することがある。
C.8	月次報告
C.8.1	以下の情報について、月次報告書を作成し、報告を行うこと。
C.8.2	障害発生状況
C.8.3	問い合わせ対応状況
C.8.4	サーバパフォーマンス、資源監視状況
C.8.5	ウェブサイトの閲覧状況（各ページの閲覧者数、可能であれば閲覧者の情報）
C.8.6	情報セキュリティ対策状況（ウィルス対策、不正アクセス監視など）
C.8.7	ソフトウェア・プラグイン等のバージョンアップ作業状況
C.9	サービスレベル（SLA）
C.9.1	サービスレベルの評価項目および目標値は、おおむね以下に示す内容を想定しているが、詳細については本仕様書に基づく提案を参考として、別途協議の上、決定する。
C.9.2	サービス提供時間：24 時間365 日（計画停止・定期保守を除く。）
C.9.3	業務対応時間：9:00-17:00（日曜日、土曜日、祝休日および 12月29 日～ 1 月3 日を除く。）メール・電話で受付。重大障害は時間外も連絡可能とする。
C.9.4	計画停止予定通知：2週間前に通知すること。
C.9.5	サービス稼働率目標：本番サイトの稼働率99.9%/月（計画停止を除く）。
C.9.6	障害区分・復旧目標時間：受託者保守窓口が障害を認知した時刻を開始時間とする。 （ア）S1（重大）：全体閲覧不可、トップや重要機能停止 一次応答：1時間以内、暫定復旧：6時間以内、恒久対策：2営業日以内提示、14日以内実装 （イ）S2（中）：一部機能障害、回避策限定 一次応答：4営業時間以内、暫定復旧：1営業日以内、恒久対策：5営業日以内目安 （ウ）S3（軽微）：表示崩れ、誤字等 対応開始：3営業日以内、修正完了：10営業日以内目安
C.9.7	目標復旧時点：1日以内（前日のバックアップ取得時点）
C.9.8	システム監視：1日1回以上のハードウェア・ソフトウェアのパフォーマンス監視
C.9.9	個人情報等の非公開情報の漏えい事故：0件
C.9.10	ウェブサイトの改ざん：0件
C.9.11	問い合わせ対応：受付率 80%以上、即答率 50%以上（調査後回答目標時間 1日以内）
C.9.12	違反時の是正：目標未達が連続する場合は是正計画を提出し、対策情報センター承認のもと改善を実施すること。