脳卒中・心臓病等総合支援センター
支援システム構築業務（機能検証用）　一式

仕様書

国立研究開発法人
国立循環器病研究センター
令和8年10月

脳卒中・心臓病等総合支援センター
支援システム構築業務（機能検証用）　一式

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　システム基盤
- B.4　システム機能要件
- B.5　納品物

C.役務要件
- C.1　全体要件
- C.2　現状把握、想定課題・ニーズ整理
- C.3　業務フロー
- C.4　必要機能の整理
- C.5　PoC開発の要件定義
- C.6　PoC開発の設計
- C.7　PoC開発
- C.8　開発環境
- C.9　テスト
- C.10　教育

D.2027年4月以降の運用保守要件（参考：本調達範囲外）
- D.1　運用支援
- D.2　保守管理
- D.3　障害対応
- D.4　月次報告
- D.5　サービスレベル（SLA）

項番	機能要件
A	本調達の背景と目的、方針
A.1	背景
A.1.1	日本の循環器病対策は、「脳卒中・循環器病対策基本法」および「第2期循環器病対策推進基本計画」の策定を経て、令和8年度より、国立循環器病研究センターが、脳卒中・心臓病等の対策にかかる総合推進事業を担うこととなり、新たなフェーズを迎えた。令和7年度までにモデル事業として、検討が進められてきた「脳卒中・心臓病等総合支援センター（以下、総合支援センターという）」は、令和8年2月に発出された局長通知（健生発0225第5号）に基づいて、令和8年度に、47都道府県すべてに設置が完了した。
A.1.2	総合支援センターの整備に関する指針には、取組として、循環器病患者・家族の相談支援窓口の設置、地域住民を対象とした循環器病の予防に関する内容等を含めた情報提供及び普及啓発、都道府県内の医療機関、かかりつけ医を対象とした研修会、勉強会等の開催、相談支援を効率的に行うための資材の活用及び提供、その他包括的な支援体制を効率的に提供するために必要と考えられるものが挙げられている。
A.1.3	さらに、「脳卒中相談窓口マニュアル ver5.1（2026年5月改訂）」に示す通り、相談支援は、再発予防や服薬管理にとどまらず、「緩和ケア・意思決定支援」や「治療と仕事の両立支援（復職支援）」など、極めて高度かつ個別性の高い領域へと拡大している。
A.1.4	令和8年2月に発出された局長通知（健生発0225第5号）によると、国立循環器病研究センター（以下、当センターという）は、我が国の循環器病対策の中核的機関として、国全体の循環器病対策を牽引すること、総合支援センターの定期的な評価や、取組事例の収集、情報発信、技術的支援などを国と共に行うことが求められている。
A.2	目的
A.2.1	本事業では、総合支援センターへの支援策の検討と支援の提供について、当センターが中心となって進める業務について支援を行うことを目的としている。
A.3	方針
A.3.1	本事業のPoC検証での利用を前提とし、総合支援センター業務を支援し、全国で収集した相談情報を将来有効活用するための、相談データ収集と報告データ作成のためのプロトタイプを構築する。ただし総合支援センターに新たな業務負担を増やさないように音声データの利活用するユーザーインターフェースを求める。
A.3.2	今年度のシステム化の範囲は機能検証対象施設として2施設を選定し、R9年度の運用についても第1期運用として同施設での運用を目指すものとする。
A.3.3	本事業は、当センター内に設置した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）にて検討と推進をおこなう。
B	システム要件
B.1	全体要件
B.1.1	本調達システムは2027年3月末までに確実に納品すること。
B.1.2	本調達での業務範囲は、2027年3月末までの総合支援センター支援システム構築とし、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、検証された機能を全国展開した場合を想定した導入費用と1年間の運用費用、および機能拡張の提案とその概算費用を提案書に記載すること。その運用要件は「D.2027年4月以降の運用保守要件（参考：本調達範囲外）」を参考にすること。
B.1.3	動作検証や評価のため、2027年3月末までのテスト運用に必要な費用を含むこと。
B.1.4	構築システムは、2027年4月以降も本格展開に先立って検証先医療機関にて運用を継続する可能性があるため、6か月間の運用保守費用を2027年1月末までに提示すること。
B.1.5	本システムは、納品時に以下のユーザーによるPoC検証を実施し、開発した機能の価値や来年度以降に実施する本番開発に向けた課題が特定されていること。 ・全国に設置された脳卒中・心臓病等総合支援センターの相談担当者（2施設で各3名程度、専用端末は各施設2台） ・国立循環器病研究センターの担当職員（収集データの管理と分析に使用、相談支援センター担当者情報等の管理もおこなう。10名程度）
B.1.6	相談件数は、1施設当たり平均50件/月程度を想定している。来年度途中で施設数や相談件数の増加の可能性もあるため、拡張の容易なサーバ基盤を提案すること。
B.1.7	本調達での納品物は下記のとおりとする。 ・構築システムを稼働させるサーバ基盤　一式（クラウドサービスの利用を想定している。認証された利用者および許可された端末のみが接続できるアクセス制御機構を含むこと。また受注者による保守作業についても、認証された作業者のみが実施できる経路を確保すること。これらの実現方式はVPNまたは同等以上のアクセス制御を有する方式とし、契約締結後の協議により決定する） ・ユーザーが使用する端末側ソフトウェア　一式（Webブラウザ上で動作するアプリケーションとして提供。ユーザー数は前項の通り） ・相談を受ける担当者用専用端末ハードウェア　5セット(総合支援センター4+対策情報センター1) なお、各施設におけるインターネット接続回線の敷設および通信費は本調達に含まないものとする。
B.1.8	前項の専用端末以外は各医療機関にて設置済みのWindows端末を利用予定のため、一般的なWindows端末で利用できること。
B.1.9	当システムはISMAP認定のクラウドサービスを利用して構築すること。

項番	機能要件
B.1.10	当システムは国内法の適用される環境に構築すること。
B.1.11	本年度に実施するPoC検証では、同時に5名以上のユーザーが操作できる程度の処理能力を有すること。
B.1.12	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.1.13	デファクトスタンダードに準拠した環境対応を基本とし、システムのOS・通信プロトコル等は国際標準・業界標準を積極的に対応すること。
B.1.14	本調達システムを構成するハードウェア・ソフトウェアは、稼動実績のあるプロダクトを採用すること。
B.1.15	前項に関し、提案者が当センターにとって有益であると判断した場合は、実績のない製品を利用してもよい。ただし、医療機関での利用を前提としたものであることを十分に説明できる資料を添付すること。
B.1.16	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、受注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.1.17	当システム構築における成果物に関する諸権利は、原則として当センターに帰属する。ただし、受注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、受注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.1.18	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.1.19	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、および受注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、当センターと受注者の間で協議し、取り決めるものとする。
B.1.20	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、B.4のシステム機能要件については「C.4 必要機能の整理」において双方が合意した開発対象を本調達の範囲とする。また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.2	情報セキュリティ
B.2.1	本業務は、以下の規格・指針を参考に計画・設計を行うこと。最新版は2026年9月末時点のものとする。 ・「医療情報システムの安全管理に関するガイドライン」の最新版 ・「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」の最新版 ・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）」 ・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.2.2	作業の一部を再委託する場合は、提案時に再委託先と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	受注者は、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	受注者の資本関係・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、受注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	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.2.12	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.2.13	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.2.14	サーバ環境や端末環境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。

項番	機能要件
B.2.15	契約期間中にサーバ環境や端末環境に関連する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.3	システム基盤
B.3.1	システム機能開発の前提
B.3.1.1	以下のシステム機能要件（B.3.1以降）は、現時点で想定する機能・要件であり、現場業務・課題を踏まえて価値創出につながる機能を見極めた上で、期間内で実現可能な機能を選定するとともに、その要件を具体化するものとする。
B.3.2	サーバの要件
B.3.2.1	当システムが稼働するサーバ環境はクラウドサービスを利用して構築すること。
B.3.2.2	本調達で構築するWebサーバは、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.3.2.3	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.3.2.4	インターネットに公開するサーバは、ファイアウォール等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.3.2.5	ログインパスワードの文字種に、以下の条件を満たしたパスワード文字列を設定できること。 "13文字以上かつ文字列中に「英大文字・英小文字・数字・記号」の4種類を含む" (例) ABcd12345!#$%
B.3.2.6	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。暗号化できない場合は、同等の安全性を確保できる機能を有すること。
B.3.2.7	各サーバの管理者用IDとパスワードは全てユニークで、容易に類推されないようものとすること。各サーバ毎にユニークにできない場合は、同等の安全性を確保できる機能を有すること。
B.3.2.8	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.3.2.9	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.3.2.10	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.3.3	ソフトウェアの要件
B.3.3.1	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適用すること。
B.3.3.2	当システムのユーザーは下記を想定しているので、必要な権限に応じた操作制御ができること。 ・総合支援センター担当職員 ・循環器病対策情報センター職員 ・システム管理者
B.3.3.3	デファクトスタンダードに準拠した環境対応を基本とし、システムのOS・通信プロトコル等は国際標準・業界標準を積極的に対応すること。
B.3.3.4	本調達システムを構成するハードウェア・ソフトウェアは、稼動実績のあるプロダクトを採用すること。
B.3.3.5	前項に関し、提案者が当センターにとって有益であると判断した場合は、実績のない製品を利用してもよい。ただし、医療機関での利用を前提としたものであることを十分に説明できる資料を添付すること。
B.3.3.6	データベースの操作ログには操作対象データや操作内容を含むこと。
B.3.3.7	システムの利用状況の分析や問題判別を行うことができるように、システムログ、アクセスログ等、各種ログを残す仕組みとすること。
B.3.3.8	本システム環境保全のためデータベースバックアップを定期的に取得すること。取得時期は対策情報センターと協議の上、決定すること。
B.3.3.9	本システム環境保全のためシステムのバックアップを定期的に取得すること。取得時期は対策情報センターと協議の上、決定すること。
B.3.4	総合支援センター用専用端末
B.3.4.1	ノート型の汎用端末であること。
B.3.4.2	OSはWindows 11 Professionalであること。
B.3.4.3	画面サイズは14インチ以上であること。
B.3.4.4	CPU、メモリは調達システムの円滑な運用に支障を来さない能力を有すること。
B.3.4.5	対面相談の音声を録音、保存できること。電話相談の音声については、各施設の電話環境に応じた録音用の外部機器を端末に接続することで録音、保存できること。外部機器の仕様は、PoC対象施設の電話環境の確認結果を踏まえ、対策情報センターと協議のうえ決定する。当該外部機器は、検証対象2施設分を本調達の範囲に含むこと。
B.4	システム機能要件
B.4.1	共通機能
B.4.1.1	ユーザが直接利用する機能はWebブラウザで操作ができること。
B.4.1.2	下記のOS・ブラウザでの閲覧に対応すること。 ＜OS＞Windows11 ＜ブラウザ＞Microsoft Edge それぞれ稼働時の最新版

項番	機能要件
B.4.1.3	本構築システムでの生成AIの学習内容は本環境のみで使用し、他の顧客向けサービスとして使用しないこと。
B.4.1.4	なお音声から文字起こした仮名加工前の情報は、相談を受けた総合支援センターでのみ利用可能とし、仮名加工した後のデータは当センターを含め各相談支援センターに跨って利用可能とする。
B.4.2	相談記録作成・参照機能（総合支援センター用機能）
B.4.2.1	登録されたユーザーがID、パスワードを使ってログインすることで利用できること。
B.4.2.2	相談を受けるにあたり、新規登録か登録済み相談かを選択して記録の作成ができること。
B.4.3.3	「相談内容を録音すること、音声データを要約、匿名化して二次利用すること」の相談者同意を取得した内容を記録できること。
B.4.2.3	相談者からの相談をトリガーに電話・対面による相談内容を音声データとして取得し、ローカル端末上もしくはクラウドサーバーに保存できること。
B.4.2.4	取得した音声データを、音声認識により自動でテキスト化できること。テキスト化に際しては、医療・福祉分野で用いられる用語の認識精度を高める仕組みがあること。
B.4.2.5	音声データの保存期間、保存場所は対策情報センターと協議の上決定すること。
B.4.2.6	テキスト化されたデータに含まれる氏名・住所・電話番号・生年月日等の個人情報を自動的に検出し、仮名加工できること。以降の要約生成および報告項目抽出には仮名化済みのテキストを用いること。
B.4.2.7	仮名加工されたテキストデータから、相談記録としての要約文を生成AIを用いて自動生成できること。
B.4.2.8	要約文の作成に当たっては相談記録様式の各項目に「どのような情報が入るべきか」を事前定義し、会話内容を該当項目へ自動入力できること。
B.4.2.9	相談事項の分類は全国統一の基準（ルールベース＋AI補助）で候補を提示し、施設間の集計ばらつきを防ぐように配慮すること。
B.4.2.10	相談記録作成時に仮名加工の処理を行い、結果をクラウド上にデータベース化して保存できること。
B.4.2.11	仮名加工に当たっては、同一相談者の複数回相談を自施設内において同一事案として紐づけることができるよう配慮すること。紐づけの主キーは施設内で管理する仮名化IDとし、患者ID等の外部識別子は将来の連携に備えて付加可能な属性として設計すること。なお電子カルテの患者IDやマイナンバーカードとの連携機能の実装は本調達の範囲に含まない。
B.4.2.12	相談記録を画面に表示し、相談員が確認、修正保存できること。
B.4.2.13	相談記録画面は、確認と後利用しやすいように構造化された形式で表示されること。
B.4.2.14	確認、保存した相談記録の一覧画面を提供すること。
B.4.2.15	相談記録一覧画面では検索画面を有することとするが、検索対象は自拠点の相談情報のみとすること。
B.4.2.16	同一相談者からの相談記録は一覧に戻らずに、容易な操作で表示できること。
B.4.2.17	相談記録データベースには検索、ダウンロード機能を有すること。
B.4.3	報告書作成・参照機能
B.4.3.1	相談記録から厚生労働省への報告書項目の抽出を生成AIを用いて自動でできること。
B.4.3.2	抽出データを二次利用がしやすいようにデータベース格納すること。
B.4.3.3	抽出とDBへの格納は日次処理として自動実行できること。
B.4.3.4	抽出結果の一覧を作成できること。
B.4.3.5	報告書データベースには検索、ダウンロード機能を有すること。
B.4.3.6	報告書データは管理者が編集できる機能を有すること。
B.5	納品物
B.5.1	受注者は、本調達目的であるPoc検証のための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.5.2	情報セキュリティ管理計画書
B.5.3	システム構成図
B.5.4	アカウント一覧
B.5.5	ソフトウェア一覧（名称、バージョン、パラメータ等）
B.5.6	要件定義書
B.5.7	設計図書
B.5.8	操作マニュアル（管理者用、利用者用）
B.5.9	打ち合わせ議事録
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	開札後1週間以内にキックオフミーティングを開催すること。
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。

項番	機能要件
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	受注者は、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.1.8	受注者は、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.1.9	受注者は、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.1.10	受注者は、当システムの目的を理解し、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.1.11	受注者は、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.1.12	受注者は、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.1.13	契約の満了または解除に当たっては、PoC用システムのに係る一切のデータ、設計情報、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注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.1.14	本契約期間中は構築システムが要件通り運用できるよう技術支援を行うこと。またクラウド環境を含めて障害が発生した際は復旧に向けて対応すること。対応時間帯は平日9:00から17:00（土曜日、日曜日、祝休日および12月29日から1月3日を除く）とし、重大な障害については時間外も可能な限り速やかに対応すること。クラウドサービス提供事業者に起因する障害については、受注者は状況の把握・報告および復旧後の動作確認を行うものとする。
C.2	現状把握、想定課題・ニーズ整理
C.2.1	対策情報センターと協業の上、現状の相談業務を整理・把握し、相談内容・対応方法、業務上の課題・ニーズ、ならびに既存のツール等について整理すること。
C.2.2	受注者は、対策情報センターから既に調査・収集された相談業務に関する情報の提供を受け、当該情報をもとに、システム構築の観点から不足する情報および追加で確認が必要な事項を整理し、対策情報センターに提示すること。なお、不足する情報および追加確認事項については、対策情報センターが総合支援センターへのヒアリング等を通じて必要な情報を収集し、その結果を受注者に提供することを想定する。また要件の具体化に必要な場合は、対策情報センターの同席のもと、受注者が総合支援センターへのヒアリングに参加できるものとする。
C.3	業務フロー
C.3.1	「C.2 現状把握、想定課題・ニーズ整理」の成果をもとに、総合支援センターの現状業務を業務フローとして整理すること。
C.3.2	前項で整理した総合支援センターにおける現状の業務フローをもとに、相談支援システムを活用した新たな業務フローを設計すること。
C.4	必要機能の整理
C.4.1	相談支援システムを活用した新たな業務フローの実現に必要と考えられる機能を要件定義書として整理すること。なお必要機能とその要件については対策情報センターと十分協議の上で決定すること。
C.4.2	本年度のPoC開発における開発する機能について、対策情報センターが判断できるよう、前項で整理した機能について、課題解決への寄与度や実現可能性等の観点から評価し、実現優先度を検討すること。
C.5	PoC開発の要件定義
C.5.1	「C.4 必要機能の整理」にて確定したPoC開発における開発対象について、各機能の目的・処理内容、利用者・利用場面、入出力情報、画面・操作方法等を具体化し、PoC開発に必要となる要件を定義すること。
C.5.2	「C.4 必要機能の整理」にて確定したPoC開発における開発対象について、想定する利用者数、データ量・形式等の観点から、PoC検証に必要となる非機能要件を定義すること。
C.6	PoC開発の設計
C.6.1	「C.5 Poc開発の要件定義」にて定義した要件をもとに、PoC開発におけるシステムの構成、画面、機能、データ、処理等の具体的な実現方法を設計し「設計図書」として整理すること。
C.7	PoC開発
C.7.1	「C.5 PoC開発の要件定義」および「C.6 PoC開発の設計」の成果を踏まえ、PoC検証において設定した検証事項を適切に評価できるよう、必要な機能を実装したPoC環境を構築すること。
C.8	開発環境
C.8.1	受注者は、本業務の設計・制作・開発作業を受注者の環境、またはクラウド環境において実施すること。
C.8.2	開発作業場所は受注者オフィス、あるいは受注者の開発担当者の自宅とするが、いずれも十分安全な環境であることを説明できること。操作研修等で当センター等を利用する場合は、別途協議しスケジュールを調整すること。
C.8.3	開発作業のために必要な機材は、サーバ環境も含めて受注者が準備すること。
C.8.4	本システムのサーバ管理に使用する受注者の端末は、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.8.5	本システム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。

項番	機能要件
C.8.6	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.8.7	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.8.8	本業務に関して行った作業について記録すること。
C.9	テスト
C.9.1	PoC検証の開始する前に、検証対象とする機能の稼働テストを実施すること。
C.9.2	テストは受注者が主体となって実施すること。
C.9.3	テストにおいては事前にテスト計画書を対策情報センターに提出し、承認を得たうえで実施すること。
C.9.4	テスト計画書は、本仕様書に記載するすべての機能、受注者が提案した機能、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.9.5	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すること。
C.9.6	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.10	教育
C.10.1	PoC検証の実施に必要なシステム操作マニュアルを作成すること（PoC検証の対象者（模擬相談員）等を想定）
C.10.2	教育の対象者はPoC検証の対象者とする。対象者数、実施時期および実施方法については、PoC検証の要件（検証項目、検証期間、評価方法を含む）とあわせて、契約締結後に対策情報センターと協議のうえ決定する。
D	2027年4月以降の運用保守要件（参考：本調達範囲外）
D.1	運用支援
D.1.1	受注者は、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。
D.1.2	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。
D.1.3	電話での質問や相談の受付時間は平日の9:00～17:00とすること。
D.1.4	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。
D.1.5	当システムの軽微な改修に関する費用は、本契約に含めること。ただし、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。
D.1.6	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。
D.2	保守管理
D.2.1	契約期間中、納品物に対して保守が行える体制を構築すること。
D.2.2	本保守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が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。
D.2.3	本調達システムのサーバ、および受注者の保守用端末は、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。
D.2.4	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。
D.2.5	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。
D.2.6	OS等ソフトウェア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。
D.2.7	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。
D.2.8	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。
D.3	障害対応
D.3.1	当システム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。
D.3.2	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。
D.3.3	ただし、当システム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。
D.4	月次報告
D.4.1	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。
D.4.2	障害発生状況
D.4.3	問い合わせ対応状況
D.4.4	サーバパフォーマンス、資源監視状況
D.4.5	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）
D.4.6	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）
D.4.7	ソフトウェアのバージョンアップ作業状況
D.5	サービスレベル（SLA）

項番	機能要件
D.5.1	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。
D.5.2	サービス提供時間：24 時間365 日（計画停止・定期保守を除く。）
D.5.3	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。
D.5.4	計画停止予定通知：2週間前に通知すること。
D.5.5	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）。
D.5.6	障害区分・復旧目標時間：受注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
D.5.7	目標復旧時点：１日以内（前日のバックアップ取得時点）
D.5.8	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
D.5.9	個人情報等の非公開情報の漏えい事故：0件
D.5.10	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）
D.5.11	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。