PMDA ウェブサイト基盤運用保守
調達仕様書

平成 31 年 1 月

独立行政法人　医薬品医療機器総合機構

目次

１　調達案件の概要に関する事項

（１）　調達件名

PMDA ウェブサイト基盤運用保守業務

（２）　用語の定義

表 1-1 用語の定義

用語	概要
添付文書	医薬品においては、用法、用量その他使用及び取扱い上の必要な注意等の定められた事項を記載し、医薬品に添付される文書。医療機器においては、使用方法その他使用及び取扱い上の必要な注意等の定められた事項を記載し、医療機器に添付される文書。 医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律にその根拠があり、医薬品、医療機器については添付文書の作成と添付が義務付けられている。
Virtual Private Server（VPS）	仮想環境上で提供される機構が管理者権限を有することが可能なサーバ機器の意。
クラウド	ソフトウェアやハードウェアの利用権などをネットワーク越しにサービスとして利用者に提供する方式を「クラウドコンピューティング」(cloud computing)と呼び、データセンターや、その中で運用されているサーバ群のことをクラウドという。
Infrastructure as a Service（IaaS）	情報システムの稼働に必要な機材や回線などの基盤を、クラウドサービスとして遠隔から利用できるようにしたもの。

（３）　調達の背景と目的

独立行政法人医薬品医療機器総合機構（以下「PMDA」という。）では、以前、独立行政法人医薬品医療機器総合機構ホームページ （http://www.pmda.go.jp/）及び 医薬品医療機器情報提供ホームページ（http://www.info.pmda.go.jp/）（以下「info サイト」という。）の２つのウェブサイトを主に運用してきた。しかしながら、一つの法人でホームページを２つ運用することは望ましくなく、また各々ページに統一感がなかったこと等から、ユーザビリティの向上を目的に 2 つのウェブサイトを平成 27 年３月に統合を行い、現行の PMDA ウェブサイトを運営している。

PMDA ウェブサイトの運営にあたっては、国民や医療従事者等に医薬品や医療機器等の安全性情報等を迅速かつ適切にお知らせすることや、世界に情報発信すること等を行う必要がある。

PMDA ウェブサイトを構成するシステム（以下「本システム」という。）の基盤の契約が平成 31 年 3 月 31 日で満了となる。また、現在使用しているソフトウェアの保守サポートも終了となる。

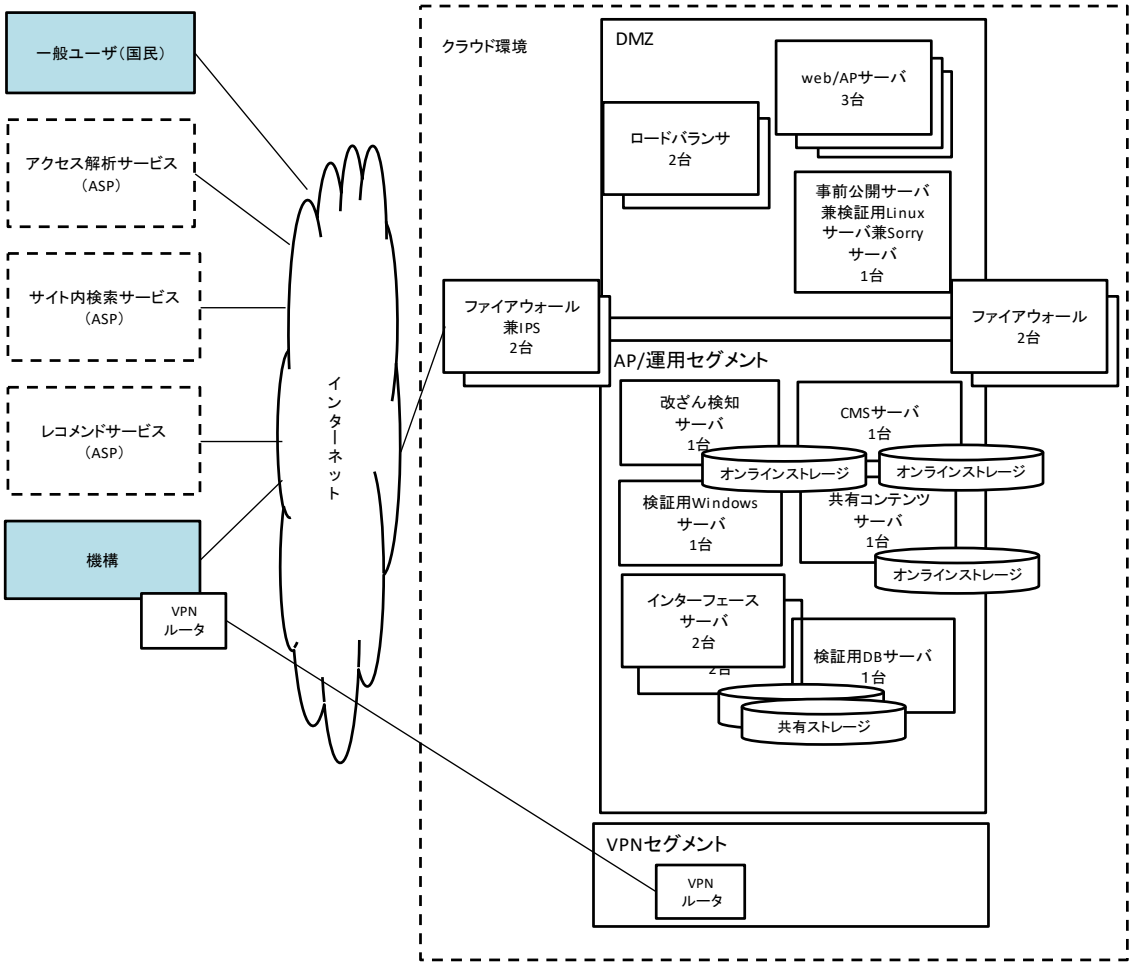
本調達は、契約期間中の保守サポートが継続するバージョンのソフトウェアを導入した新環境を IaaS 上に構築（３（１）① 稼働環境の構築）し、新環境で稼働するために必要となる業務システムの改修、新環境への業務システムおよびデータの移行（３（１）② 業務システムの改修・移行）、ハードウェア、ソフトウェア、インターネット回線及びネットワーク機器等について必要となるライセンス費用を含む環境提供（３（１）③ 運用）及びこれらに係る保守サービス（３（１）④ 保守）を外部委託することを目的とする。

（４） 業務・情報システムの概要

PMDA の中心業務である、審査関連業務、安全対策業務、健康被害救済業務では、それぞれの業務上広範囲への発信が必要な情報は PMDA ウェブサイトに掲載しているが、一部は info サイトにも掲載しており、また、PMDA ウェブサイトの情報検索機能（医療用医薬品、医療機器、一般用・要指導医薬品、体外診断用医薬品）で表示される添付文書やインタビューフォーム等の一部の文書については、info サイトで管理しているデータベースと連携バッチを行ってデータ取得を行っている（info サイトは安全性情報・企画管理部にて運営を行っている）。

本システムは、IaaS 上のウェブサイトを公開するウェブサーバ、コンテンツを作成する CMS サーバ、ウェブサイトで検索する添付文書などを関連システムから取得するインターフェースサーバなどで構成されている（詳しくは「図 1-1 全体構成図」を参照のこと）。

図 1-1 全体構成図



※2019 年 1 月時点の全体構成図

（５） 契約期間

2019 年 4 月 1 日から 2021 年 7 月 31 日までとする。

（６） 構築期間

2019 年 4 月 1 日から 2019 年 9 月 30 日までとする。

（７） 借入・運用保守期間

2019 年 10 月 1 日から 2021 年 7 月 31 日までとする。

（８）　作業スケジュール

本業務に係る想定スケジュールの概要を表 1-2　作業スケジュールに示す。示した作業スケジュールはあくまで想定のスケジュールであり、詳細な実施スケジュールは受託者が検討すること。

表 1-2　作業スケジュール

工程	開始	終了
稼働環境の構築		
要件定義	2019 年 4 月上旬	2019 年 4 月下旬
設計	2019 年 5 月上旬	2019 年 5 月下旬
設置	2019 年 6 月上旬	2019 年 6 月下旬
検証環境構築	2019 年 6 月下旬	2019 年 7 月下旬
本番環境構築	2019 年 8 月上旬	2019 年 8 月下旬
運用設定等	2019 年 9 月上旬	2019 年 9 月下旬
業務システムの改修・移行		
要件定義	2019 年 4 月上旬	2019 年 4 月下旬
調査・改修	2019 年 5 月上旬	2019 年 8 月下旬
テスト	2019 年 8 月上旬	2019 年 9 月中旬
移行	2019 年 9 月中旬	2019 年 9 月下旬
運用・保守	2019 年 10 月上旬	2021 年 7 月下旬

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

（１）　調達案件及び関連する調達案件の調達単位、調達の方式、実施時期

関連する調達案件の調達単位、調達の方式、実施時期は次の表の通りである。

表 2-1　関連する調達案件の調達単位、調達の方式、実施時期等（既存契約）

項番	調達案件名	調達の方式	実施時期	補足
1	平成 30 年度 PMDA コーポレートサイト改修業務	一般競争入札	2019 年 5 月から 2019 年 3 月	2019 年 3 月に行うシステム改修業務

表 2-2　関連する調達案件の調達単位、調達の方式、実施時期等（契約予定）

項番	調達案件名	調達の方式	実施時期	役割	補足
1	PMDA ウェブサイト基盤運用保守	随意契約	2019 年 4 月から 2019 年 9 月	サーバ運用	本調達の基盤更改まで現行環境を提供する
2	PMDA ウェブサイトの運用支援	一般競争入札	2019 年 4 月から 2021 年 3 月	運用支援	項番 1 及び本調達で提供する基盤上で稼働する本システムの運用を支援する

（２）　調達案件間の入札制限

なし

３　作業の実施内容に関する事項

（１）　作業の内容

①　稼働環境の構築

情報システム稼働環境をクラウド（IaaS）に構築に関する以下の作業を行うものとする。非機能要件の詳細は、「別紙 1　非機能要件」に示す。

ア　設計・導入実施計画書等の作成

ア－1　受託者は、PMDA の指示に基づき、プロジェクト管理支援事業者と調整の上、情報システム稼働環境の設計・導入実施計画書及び設計・導入実施要領の案を作成し、PMDA の承認を受けること。

イ　設計

イ－1　受託者は、本システムの現行の設計書等を参照し、機器等の設計を行い、成果物について PMDA の承認を受けること。

イ－2　受託者は、情報システム稼働環境の運用設計及び保守設計を行い、情報システムの次期更改までの間に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た中長期運用・保守作業計画の案を作成し、PMDA の確認を受けること。

イ－3　受託者は、情報システム稼働環境の運用設計及び保守設計を行い、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た運用計画及び保守作業計画の案を作成し、PMDA の確認を受けること。

ウ　ネットワーク回線の提供と敷設

ウ－1　以下に示す本システムに必要なネットワーク回線を提供、敷設、結線すること。

- インターネット回線
- VPN 接続環境（クラウド環境～機構間）及び必要となる機器等

ウ－2　インターネット回線についてはインターネットサービスプロバイダ及び本システムに必要なグローバル IP アドレスの提供も含むものとする。なお、本調達外で回線敷設が発生した場合、回線敷設作業は各調達の落札業者が実施するが、その際の必要な情報提供、支援作業を実施すること。

エ　ネットワークの疎通確認

エ－1　本件受託者は、提供、敷設する全てのネットワーク回線の疎通確認作業を実施すること。実施にあたっては動作確認計画書及び動作確認結果報告書を作成すること。動作確認計画書の記載内容については、機構、及び設計・開発業者と協議し、修正が必要な場合には本件受託者は修正を実施すること。

オ　物品

本調達仕様書に記述する要求仕様を満たす機器等を納品すること。なお、下記の役務に必要な部材を含むものとする。

カ　導入・テスト

カ－1　受託者は、導入に当たり、情報セキュリティ確保のためのルール遵守や成果物の確認方法（例えば、導入場所での調査等についての実施主体、手順、方法等）を定め、PMDA の確認を受けること。

カ－2　受託者は、機器等の導入に係るテストについて、テスト体制、テスト環境、作業内容、作業スケジュール、テストシナリオ、合否判定基準等を記載したテスト計画書を作成し、PMDA の承認を受けること。

カ－3　受託者は、テスト計画書に基づき、機器等の導入・移行に係るテストを行うこと。

カ－4　受託者は、テスト計画書に基づき、各テストの実施状況を PMDA に報告すること。

カ－5　受託者は、使用しなくなった機器の撤去および原状復帰作業を行うこと。

キ　検収支援

キ－1　受託者は、PMDA が機器等の検収を実施するに当たり、環境整備、必要な情報の提供等の支援を行うこと。

ク　引継ぎ

ク－1　受託者は、設計・導入の設計書、作業経緯、残存課題等を文書化し、運用事業者及び保守事業者に対して確実な引継ぎを行うこと。

② 業務システムの改修・移行

３（１）①で構築する新環境で稼働するために必要となる業務システムの改修、新環境への業務システムおよびデータの移行に関する以下の作業を行うものとする。要件の詳細は、「別紙 1　非機能要件」に示す。

ア　設計・導入実施計画書等の作成

ア－1　受託者は、PMDA の指示に基づき、プロジェクト管理支援事業者と調整の上、業務システムの設計・導入実施計画書及び設計・導入実施要領の案を作成し、PMDA の承認を受けること。

イ　既存アプリケーションの改修・テスト・移行

イ－1　受託者は、移行に当たり、情報セキュリティ確保のためのルール遵守や成果物の確認方法（例えば、導入場所での調査等についての実施主体、手順、方法等）を定め、PMDA の確認を受けること。

イ－2　受託者は、現行システムが利用しているソフトウェアのバージョンアップ等に係る改修や設定変更を行うこと。

イ－3　受託者は、改修・移行に係るテストについて、体制、環境、作業内容、作業スケジュール、テストシナリオ、合否判定基準等を記載したテスト計画書及び移行計画書を作成し、PMDA の承認を受けること。

イ－4　受託者は、下記の観点での改修及びテストを実施すること。

- 新システム環境の構築が完了していることを確認するため、環境やコンポーネント等に依存する機能を中心に主要機能が動作することを確認する。
- バージョンアップに伴い問題が生じる機能を洗い出し、修正すること。その際、事前の調査結果に基づき問題の生じる可能性のある機能を中心にシステム観点で基本機能の確認を行うこと。
- バージョンアップに伴い問題が生じることが明示されていない機能について、問題なく動作することを確認すること。
- システムの動作を保証するため、実環境にて、実データを用い、業務シナリオを中心とした動作を確認すること。
- テスト範囲及びテスト方法を PMDA と協議のうえ確定すること。

イ－5　受託者は、テスト計画書に基づき、各テストの実施状況を PMDA に報告すること。

イ－6　受託者は、移行計画書に基づき、移行状況を PMDA に報告すること。

ウ　検収支援

ウ－1　受託者は、PMDA が業務システムの検収を実施するに当たり、環境整備、必要な情報の提供等の支援を行うこと。

エ　引継ぎ

エ－1　受託者は、作業経緯、残存課題等を文書化し、運用事業者及び保守事業者に対して確実な引継ぎを行うこと。

③　運用

３（１）①で構築する新環境のハードウェア、ソフトウェア、インターネット回線及びネットワーク機器等について必要となるライセンス費用を含む環境提供及びこれらに係る運用サービスに関する以下の作業を行うものとする。

ア　中長期運用・保守作業計画の確定支援

ア－1　受託者は、PMDA が中長期運用・保守作業計画を確定するに当たり、情報システムの構成やライフサイクルを通じた運用業務及び保守作業の内容について、計画案の妥当性の確認、情報提供等の支援を行うこと。

イ　運用計画及び運用実施要領の作成支援

イ－1　受託者は、PMDA が運用計画及び運用実施要領を作成するに当たり、具体的な作業内容や実施時間、実施サイクル等に関する資料作成等の支援を行うこと。

ウ　クラウド環境の提供

ウ－1　本システムを稼働するためのクラウド環境を提供すること。クラウド環境には仮想化サーバ、仮想化ストレージ、仮想化ネットワークを含むこと。標準で運用・監視サービスも含むこと。

エ　定常時対応

エ－1　受託者は、「別紙１　非機能要件」の運用要件に示す定常時運用業務（システム操作、運転管理・監視、稼動状況監視、サービスデスク提供等）を行うこと。具体的な実施内容・手順は PMDA が定める運用計画に基づいて行うこと。

エー2　受託者は、運用計画及び運用実施要領に基づき、サービスレベルの達成状況、情報システムの運転状況（情報セキュリティ監視状況を含む。）、情報システムの定期点検状況、リスク・課題の把握・対応状況について月次で運用作業報告書を取りまとめること。

エー3　受託者は、月間の運用実績を評価し、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。

エー4　受託者は、運用作業報告書の内容について、月例の定期運用会議に出席し、その内容を報告すること。

エー5　受託者は、ソフトウェア製品の保守の実施において、ソフトウェア製品の構成に変更が生じる場合には、PMDA にその旨を報告し、変更後の環境がライセンスの許諾条件に合致するか否かの確認を受けること。

オ　障害発生時対応

オー1　受託者は、情報システムの障害発生時（又は発生が見込まれる時）には、速やかに PMDA に報告するとともに、その緊急度及び影響度を判断の上、「別紙 1 非機能要件」の運用要件に示す障害発生時運用業務（障害検知、障害発生箇所の切り分け及び保守事業者との連携による原因調査、応急措置、復旧確認、報告等）を行うこと。障害には、情報セキュリティインシデントを含めるものとする。具体的な実施内容・手順は「PMDA 情報セキュリティインシデント対処手順書」に基づいて行うこと。

オー2　受託者は、情報システムの障害に関して事象の分析（発生原因、影響度、過去の発生実績、再発可能性等）を行い、同様の事象が将来にわたって発生する可能性がある場合には、恒久的な対応策を提案すること。

オー3　受託者は、大規模災害等の発災時には、PMDA の指示を受けて、必要な対応を実施すること。

カ　運用作業の改善提案

カー1　受託者は、年度末までに年間の運用実績を取りまとめるとともに、必要に応じて中長期運用・保守作業計画、運用計画、運用実施要領に対する改善提案を行うこと。

キ　引継ぎ

キー1　受託者は、PMDA が本システムの更改を行う際には、次期の情報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。

キー2　受託者は、本契約の終了後に他の運用事業者が本情報システムの運用を受注した場合には、次期運用事業者に対し、作業経緯、残存課題等についての引継ぎを行うこと。

④　保守

3（1）①で構築する新環境の保守サービスに関する以下の作業を行うものとする。

ア　中長期運用・保守作業計画の確定支援

ア－1　受託者は、PMDA が中長期運用・保守作業計画を確定するに当たり、情報システムの構成やライフサイクルを通じた運用業務及び保守作業の内容について、計画案の妥当性の確認、情報提供等の支援を行うこと。

イ　保守作業計画及び保守実施要領の作成支援

イ－1　受託者は、PMDA が保守作業計画及び保守実施要領を作成するに当たり、具体的な作業内容や実施時間、実施サイクル等に関する資料作成等の支援を行うこと。

ウ　ハードウェア及びソフトウェアの保守

ウ－1　以下に示す本システムに必要な機構内に設置するハードウェアに関する保守を提供すること。

- VPS（クラウド環境）
- ネットワーク機器（VPN 回線に必要となる機器）
- 個々の要件の詳細は「別紙 1　非機能要件」を参照のこと。

ウ－2　本システムに必要なソフトウェア（基本ソフトウェア（OS）、ミドルウェア、パッケージソフトウェア）に関する保守を提供すること。

- 導入するサーバ等の機器類に搭載する OS 及びミドルウェアについて受付窓口を一本化して保守を行うこと。
- 保守の内容は次の通りとする。
  - 障害時に、搭載するソフトウェアとサーバ等の機器どちらかの切分け、及び解析に対する支援。
  - 使用方法に関する技術上の疑問点に対する回答。
  - 基本ソフトウェア製造者へ対する障害内容の取次ぎ支援
- ソフトウェアが原因と判断した場合は、設定変更、パッチ適用等の対応方法を提示する。なお、パッチ等の提供を受けるためのソフトウェア保守契約は同時に契約するものとする。
- 運用上必要な技術情報を得られる体制を構築すること。

- 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 項に掲げる日をいう。）を除く月曜日から金曜日の 9:00 から 18:00、電話受付/障害対応体制がとれること。
- 保守は、システム稼働後、継続的に行うこと。
- 機構職員及び「PMDA ウェブサイトの運用支援」を受託した運用支援業者からの仕様、利用方法、操作方法等の問合せについて対応すること。
- ソフトウェア要件の詳細は「別紙 1　非機能要件」を参照のこと。

エ　定常時対応

エ－1　受託者は、「別紙 1　非機能要件」の保守要件に示す定常時保守業務（定期点検、不具合受付等）を行うこと。具体的な実施内容・手順は PMDA が定める保守作業計画に基づいて行うこと。

エ－2　受託者は、保守作業計画及び保守実施要領に基づき、保守作業の内容や工数などの作業実績状況（情報システムの脆弱性への対応状況を含む。）、サービスレベルの達成状況、情報システムの定期点検状況、リスク・課題の把握・対応状況について月次で保守作業報告書を取りまとめること。

エ－3　受託者は、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。

エ－4　受託者は、保守作業報告書の内容について、月例の定期運用会議に出席し、その内容を報告すること。

オ　障害発生時対応

オ－1　受託者は、情報システムの障害発生時（又は発生が見込まれる時）には、PMDA 又は運用事業者からの連絡を受け、「別紙 1　非機能要件」の保守要件に示す障害発生時保守業務（原因調査、応急措置、報告等）を行うこと。障害には、情報セキュリティインシデントを含めるものとする。具体的な実施内容・手順は PMDA が定める「インシデント管理標準手順書」に基づいて行うこと。

オ－2　受託者は、情報システムの障害に関して事象の分析（発生原因、影響度、過去の発生実績、再発可能性等）を行い、同様の事象が将来にわたって発生する可能性がある場合には、恒久的な対応策を提案及び対応策の実施をすること。

オ－3　受託者は、大規模災害等の発災時には、PMDA の指示を受けて、必要な対応を実施すること。

カ　保守作業の改善提案

カ－1　受託者は、年度末までに年間の保守実績を取りまとめるとともに、必要に応じて中長期保守・保守作業計画、保守計画、保守実施要領に対する改善提案を行うこと。

キ　セキュリティ診断とその報告

キ－1　年１回（2019 年下半期、2020 年下半期の計 2 回）本システムにおけるセキュリティ監査のためのネットワーク診断及び Web 脆弱性診断を実施し、報告書を提出すること。診断要件の詳細は別添 1「セキュリティ脆弱性診断要件」を参照のこと。

ク　引継ぎ

ク－1　受託者は、PMDA が本システムの更改を行う際には、次期の情報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。

ク－2　受託者は、本契約の終了後に他の保守事業者が本情報システムの保守を受注した場合には、次期保守事業者に対し、作業経緯、残存課題等についての引継ぎを行うこと。

⑤　作業報告

ア　作業実績の報告

ア－1　受託者は、本業務で実施した作業について、月次で PMDA に報告すること。報告の様式等に関しては、稼働環境の構築／業務システムの改修・移行、運用／保守の各々の業務開始時に PMDA と協議し決定すること。

（２）　成果物の範囲、納品期日等

①　成果物

作業工程別の納入成果物を表　3-1 に示す。ただし、納入成果物の構成、詳細については、受注後、PMDA と協議し取り決めること。

表　3-1　工程と成果物

項番	工程	納入成果物	納入期日
1	計画	・設計・導入実施計画書（プロジェクトスコープ、体制表、作業分担、スケジュール、文書管理要領、セキュリティ管理要領、品質管理要領、変更管理要領、WBS）	契約締結日から 2 週間以内

項番	工程	納入成果物	納入期日
2	要件定義	・要件定義書	2019 年 4 月 30 日
3	稼働環境の構築 - 設計	・基本設計書	2019 年 7 月 31 日
4	稼働環境の構築 - 設置	・機器及びソフトウェア等一式 ・製品一覧（製品名、メーカー、製造番号、シリアル番号、納入数を記載） ・ネットワーク構成図（論理・物理） ・ネットワークの動作確認計画書及び結果報告書 ・テスト計画書	2019 年 6 月 30 日
5	稼働環境の構築 - 検証環境構築	・環境設計書 ・環境定義書 ・テスト結果報告書 ・テスト結果エビデンス	2019 年 7 月 31 日
6	稼働環境の構築 - 本番環境構築	・環境設計書 ・環境定義書 ・テスト結果報告書 ・テスト結果エビデンス	2019 年 8 月 31 日
7	稼働環境の構築 - 運用設定	・中長期運用及び保守作業計画書 ・運用及び保守作業計画書 ・保守及び手順書 ・テスト結果報告書 ・テスト結果エビデンス	2019 年 9 月 30 日
8	業務システムの改修・移行 - 調査・改修	・調査結果報告書 ・改修済みプログラム ・テスト計画書 ・テスト結果報告書（単体テスト／結合テスト） ・テスト結果エビデンス（単体テスト／結合テスト）	2019 年 8 月 31 日
9	業務システムの改修・移行 - テスト	・テスト結果報告書（総合テスト） ・テスト結果エビデンス（総合テスト） ・テストデータ（総合テスト） ・移行計画書	2019 年 9 月 20 日
10	業務システムの改修・移行 - 移行	・移行手順書 ・移行作業結果報告書 ・教育計画書 ・教育用資料 ・教育作業結果報告書等	2019 年 9 月 30 日
11	運用・保守	・運用及び作業報告書	2021 年 7 月 31 日
12	その他	・打合せ資料 ・議事録 ・機密情報受理管理簿 ・データ消去証明書 ・瑕疵担保責任対応に係る保有情報の一覧 ・セキュリティ診断報告書	2021 年 7 月 31 日 （※必要に応じて随時提出）

② 納品方法

表 3-1 の項番 1 から 10 に関する納入成果物を 2019 年 9 月 30 日までに納品すること。表 3-1 の項番 11 から 12 の納入成果物を 2021 年 7 月 31 日までに納品すること。

受託者の責任による機器の納入遅延および作業遅延が発生し、現行環境の利用を延長する必要が生じた際には受託者の責任及び費用負担で機材の継続利用を可能とすること。

なお、納入成果物については、以下の条件を満たすこと。

ア 文書を磁気媒体等（CD-R 又は CD-RW 等）により日本語で提供すること。

イ 紙のサイズは、日本工業規格 A 列 4 番を原則とする。図表については、必要に応じて A 列 3 番縦書き、横書きを使用することができる。バージョンアップ時等に差し換えが可能なようにバインダー方式とする。

ウ 磁気媒体等に保存する形式は、PDF 形式及び Microsoft Office2013 で扱える形式とする。ただし、PMDA が別に形式を定めて提出を求めた場合は、この限りではない。

エ 磁気媒体については二部ずつ用意すること。また、各種マニュアル及び教育用資料は、PMDA が指定する必要部数の紙媒体を納入すること。

オ 一般に市販されているツール、パッケージ類の使用は PMDA と協議の上、必要であれば使用を認めることとするが、特定ベンダーに依存する（著作権、著作者人格権を有する）ツール等は極力使用しないこと。

カ 本調達で使用した開発ツール等の 2 年間のライセンス及びメディアを納入すること。

キ 本業務を実施する上で必要となる一切の機器物品等は、受託者の責任で手配するとともに、費用を負担すること。

ク 各工程の中間成果物も含め、本調達に係る全ての資料を納品すること。

③ 納品場所

独立行政法人　医薬品医療機器総合機構　経営企画部広報課

4 満たすべき要件に関する事項

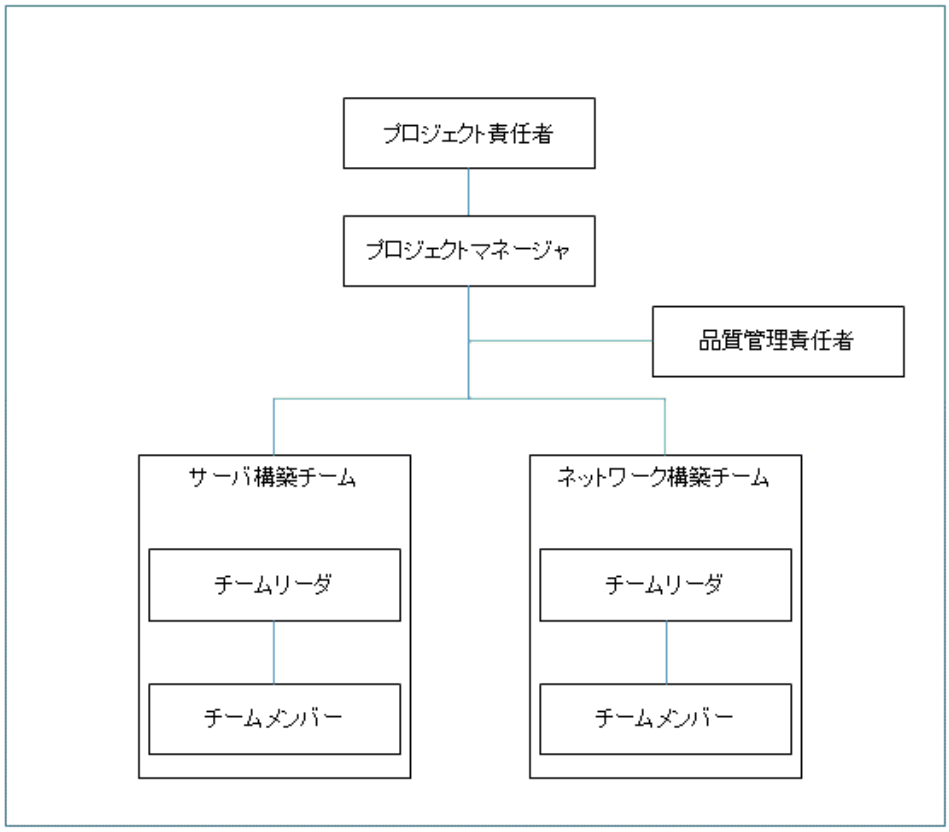
本業務の実施にあたっては、本システムの現行の設計書等及び「別紙 1　非機能要件」を参照し、本業務に求められる各要件を満たすこと。

５　作業の実施体制・方法に関する事項

（１）　作業実施体制

① プロジェクトの推進体制及び本件受託者に求める作業実施体制は「図　5-1　作業体制図」のとおりである。なお、受託者内のチーム編成については想定であり、受託者決定後に協議の上、見直しを行うこと。また、受託者の情報セキュリティ対策の管理体制については、作業実施体制とは別に作成すること。

図　5-1　作業体制図



② システム設計・導入等を複数業者が連携（再委託を含めて）して実施する等の場合は、参画する各業者の役割分担等を明示すること。

③ 開発環境の整備

業務システムの改修およびテストを行うため、開発環境（開発用のハードウェア、開発ツール、データベース（Oracle Database）等のソフトウェアを含む。）及び作業場所等を、受注者の責任において確保すること。なお、開発環境の構築については、調査・改修開始までに構築を完了すること。

（２）　作業要員に求める資格等の要件

① 設計・導入に携わるリーダは特定非営利活動法人 日本プロジェクトマネジメント協会の「プロジェクトマネジメント・スペシャリスト（PMS）」、PMI（Project Management Institute）の「PMP」資格、独立行政法人情報処理推進機構（IPA）の「プロジェクトマネージャ」資格のいずれかを取得していること。

② 本システムの業務を理解しており、設計にあたり、PMDA に逐次業務の説明を求めることなく担当者とスムーズな会話ができる知識を有していること。

（３）　作業場所

① 受注業務の作業場所（サーバ設置場所等を含む）は、（再委託も含めて）PMDA 内、又は日本国内で PMDA の承認した場所で作業すること。

② 受注業務で用いるサーバ、データ等は日本国外に持ち出さないこと。

③ PMDA 内での作業においては、必要な規定の手続を実施し承認を得ること。

④ なお、必要に応じて PMDA 職員は現地確認を実施できることとする。

（４）　作業の管理に関する要領

① 受託者は、PMDA が承認した設計・導入実施要項に基づき、設計・導入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、情報セキュリティ対策を行うこと。

② 受託者は、PMDA の指示に従って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、情報セキュリティ対策を行うこと。

③ 受託者は、PMDA の指示に従って保守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、情報セキュリティ対策を行うこと。

６　作業の実施に当たっての遵守事項

（１）　基本事項

受託者は、次に掲げる事項を遵守すること。

① 本業務の遂行に当たり、業務の継続を第一に考え、善良な管理者の注意義務をもって誠実に行うこと。

② 本業務に従事する要員は、PMDA と日本語により円滑なコミュニケーションを行う能力と意思を有していること。

③ 本業務の履行場所を他の目的のために使用しないこと。

④ 本業務に従事する要員は、履行場所での所定の名札の着用等、従事に関する所定の規則に従うこと。

⑤ 要員の資質、規律保持、風紀及び衛生・健康に関すること等の人事管理並びに要員の責めに起因して発生した火災・盗難等不祥事が発生した場合の一切の責任を負うこと。

⑥ 受託者は、本業務の履行に際し、PMDA からの質問、検査及び資料の提示等の指示に応じること。また、修正及び改善要求があった場合には、別途協議の場を設けて対応すること。

⑦ 次回の本業務調達に向けた現状調査、PMDA が依頼する技術的支援に対する回答、助言を行うこと。

⑧ 本業務においては、業務終了後の運用等を、受託者によらずこれを行うことが可能となるよう詳細にドキュメント類の整備を行うこと。

（２） 機密保持、資料の取扱い

本業務を実施する上で必要とされる機密保持に係る条件は、以下のとおり。

① 受託者は、受注業務の実施の過程で PMDA が開示した情報（公知の情報を除く。以下同じ。）、他の受託者が提示した情報及び受託者が作成した情報を、本受注業務の目的以外に使用又は第三者に開示若しくは漏洩してはならないものとし、そのために必要な措置を講ずること。

② 受託者は、本受注業務を実施するにあたり、PMDA から入手した資料等については管理簿等により適切に管理し、かつ、以下の事項に従うこと。

- 複製しないこと。
- 用務に必要がなくなり次第、速やかに PMDA に返却又は消去すること。
- 受注業務完了後、上記①に記載される情報を削除又は返却し、受託者において該当情報を保持しないことを誓約する旨の書類を PMDA に提出すること。

③ 応札希望者についても上記①及び②に準ずること。

④ 「独立行政法人 医薬品医療機器総合機構 情報システム管理利用規程」の第 52 条に従うこと。

⑤ 「秘密保持等に関する誓約書」を別途提出し、これを遵守しなければならない。

⑥ 機密保持の期間は、当該情報が公知の情報になるまでの期間とする。

（３） 遵守する法令等

本業務を実施するにあたっての遵守事項は、以下のとおり。

① 受託者は、民法、刑法、著作権法、不正アクセス行為の禁止等に関する法律、行政機関の保有する個人情報の保護に関する法律等の関連法規及び労働関係法令を遵守すること。

② 受託者は、次の文書に記載された事項を遵守すること。遵守すべき文書が変更された場合は変更後の文書を遵守すること。

ア 独立行政法人 医薬品医療機器総合機構　情報セキュリティポリシー

イ 独立行政法人 医薬品医療機器総合機構 情報システム管理利用規程

ウ 独立行政法人 医薬品医療機器総合機構 個人情報管理規程

エ 政府機関等の情報セキュリティ対策のための統一規範（最新版）

オ 政府機関等の情報セキュリティ対策の運用等に関する指針（最新版）

カ 政府機関等の情報セキュリティ対策のための統一基準（最新版）

なお、「PMDA 情報セキュリティポリシー」は非公開であるが、「政府機関等の情報セキュリティ対策のための統一基準（最新版）」に準拠しているので、必要に応じ参照すること。「PMDA 情報セキュリティポリシー」の開示については、入札説明会に参加した事業者のうち、事業者が PMDA に「秘密保持等に関する誓約書」を提出した際に開示する。

③ PMDA へ提示する電子ファイルは事前にウイルスチェック等を行い、悪意のあるソフトウェア等が混入していないことを確認すること。

④ 民法、刑法、著作権法、不正アクセス禁止法、個人情報保護法等の関連法規を遵守することはもとより、下記の PMDA 内規程を遵守すること。

- 独立行政法人 医薬品医療機器総合機構 情報システム管理利用規程
- 独立行政法人 医薬品医療機器総合機構 個人情報管理規程

⑤ 受託者は、本業務において取り扱う情報の漏洩、改ざん、滅失等が発生することを防止する観点から、情報の適正な保護・管理対策を実施するとともに、これらの実施状況について、PMDA が定期又は不定期の検査を行う場合においてこれに応じること。万一、情報の漏洩、改ざん、滅失等が発生した場合に実施すべき事項及び手順等を明確にするとともに、事前に PMDA に提出すること。また、そのような事態が発生した場合は、PMDA に報告するとともに、当該手順等に基づき可及的速やかに修復すること。

7　成果物の取扱いに関する事項

（１）　知的財産権の帰属

知的財産の帰属は、以下のとおり。

① 本件に係り作成・変更・更新されるドキュメント類及びプログラムの著作権（著作権法第 21 条から第 28 条に定めるすべての権利を含む。）は、受託者が本件のシス

テム導入の従前より権利を保有していた等の明確な理由により、あらかじめ書面にて権利譲渡不可能と示されたもの以外、PMDA が所有する等現有資産を移行等して発生した権利を含めてすべて PMDA に帰属するものとする。

② 本件に係り発生した権利については、受託者は著作者人格権（著作権法第 18 条から第 20 条までに規定する権利をいう。）を行使しないものとする。

③ 本件に係り発生した権利については、今後、二次的著作物が作成された場合等であっても、受託者は原著作物の著作権者としての権利を行使しないものとする。

④ 本件に係り作成・変更・修正されるドキュメント類及びプログラム等に第三者が権利を有する著作物が含まれる場合、受託者は当該著作物の使用に必要な費用負担や使用許諾契約に係る一切の手続きを行うこと。この場合は事前に PMDA に報告し、承認を得ること。

⑤ 本件に係り第三者との間に著作権に係る権利侵害の紛争が生じた場合には、当該紛争の原因が専ら PMDA の責めに帰す場合を除き、受託者の責任、負担において一切を処理すること。この場合、PMDA は係る紛争の事実を知ったときは、受託者に通知し、必要な範囲で訴訟上の防衛を受託者にゆだねる等の協力措置を講ずる。
なお、受託者の著作又は一般に公開されている著作について、引用する場合は出典を明示するとともに、受託者の責任において著作者等の承認を得るものとし、PMDA に提出する際は、その旨併せて報告するものとする。

（２） 瑕疵担保責任

① 本業務の最終検収後 1 年以内の期間において、委託業務の納入成果物に関して本システムの安定稼動等に関わる瑕疵の疑いが生じた場合であって、PMDA が必要と認めた場合は、受託者は速やかに瑕疵の疑いに関して調査し回答すること。調査の結果、納入成果物に関して瑕疵等が認められた場合には、受託者の責任及び負担において速やかに修正を行うこと。なお、修正を実施する場合においては、修正方法等について、事前に PMDA の承認を得てから着手すると共に、修正結果等について、PMDA の承認を受けること。

② 受託者は、瑕疵担保責任を果たす上で必要な情報を整理し、その一覧を PMDA に提出すること。瑕疵担保責任の期間が終了するまで、それら情報が漏洩しないように、ISO/IEC27001 認証（国際標準）又は JISQ27001 認証（日本工業標準）に従い、また個人情報を取り扱う場合には JISQ15001（日本工業標準）に従い、厳重に管理をすること。また、瑕疵担保責任の期間が終了した後は、速やかにそれら情報を、データ復元ソフトウェア等を利用してもデータが復元されないように完全に消去すること。データ消去作業終了後、受託者は消去完了を明記した証明書を作業ロ

グとともにPMDAに対して提出すること。なお、データ消去作業に必要な機器等については、受託者の負担で用意すること。

（３）　検収

納入成果物については、適宜、PMDAに進捗状況の報告を行うとともに、レビューを受けること。最終的な納入成果物については、「３（２）① 成果物」に記載のすべてが揃っていること及びレビュー後の改訂事項等が反映されていることを、PMDAが確認し、これらが確認され次第、検収終了とする。

なお、以下についても遵守すること。

① 検査の結果、納入成果物の全部又は一部に不合格品を生じた場合には、受託者は直ちに引き取り、必要な修復を行った後、PMDAの承認を得て指定した日時までに修正が反映されたすべての納入成果物を納入すること。

② 「納入成果物」に規定されたもの以外にも、必要に応じて提出を求める場合があるので、作成資料等を常に管理し、最新状態に保っておくこと。

③ PMDAの品質管理担当者が検査を行った結果、不適切と判断した場合は、品質管理担当者の指示に従い対応を行うこと。

８　入札参加資格に関する事項

（１）　入札参加要件

応札希望者は、以下の条件を満たしていること。

① 導入責任部署はISO9001又はCMMIレベル3以上の認定を取得していること。

② ISO/IEC27001認証（国際標準）又はJISQ27001認証（日本工業標準）のいずれかを取得していること。

③ プライバシーマーク付与認定を取得していること。

④ PMDAにて現行関連システムの設計書等を閲覧し、内容を十分理解していること。

⑤ 応札時には、導入作業毎に十分に細分化された工数、概算スケジュールを含む見積り根拠資料の即時提出が可能であること。なお、応札後にPMDAが見積り根拠資料の提出を求めた際、即時に提出されなかった場合には、契約を締結しないことがある。

（２）　入札制限

情報システムの調達の公平性を確保するために、以下に示す事業者は本調達に参加できない。

① PMDA の CIO 補佐が現に属する、又は過去 2 年間に属していた事業者等

② 各工程の調達仕様書の作成に直接関与した事業者等

③ 設計・開発等の工程管理支援業者等

④ ①～③の親会社及び子会社（「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 年大蔵省令第 59 号）第 8 条に規定する親会社及び子会社をいう。以下同じ。）

⑤ ①～③と同一の親会社を持つ事業者

⑥ ①～③から委託を請ける等緊密な利害関係を有する事業者

９ 情報セキュリティ管理

（１） 情報セキュリティ対策の実施

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実施計画書に添付して提出すること。

ア PMDA から提供する情報の目的外利用を禁止すること。

イ 本業務の実施に当たり、受託者又はその従業員、本調達の役務内容の一部を再委託する先、若しくはその他の者による意図せざる変更が加えられないための管理体制が整備されていること。

ウ 受託者の資本関係・役員等の情報、本業務の実施場所、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）・実績及び国籍に関する情報提供を行うこと。具体的な情報提供内容については PMDA と協議の上、決定するものとする。

エ 情報セキュリティインシデントへの対処方法が確立されていること。

オ 情報セキュリティ対策その他の契約の履行状況を定期的に確認し、PMDA へ報告すること。

カ 情報セキュリティ対策の履行が不十分である場合、速やかに改善策を提出し、PMDA の承認を受けた上で実施すること。

キ PMDA が求めた場合に、速やかに情報セキュリティ監査を受入れること。

ク 本調達の役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるように情報セキュリティ管理計画書に記載された措置の実施を担保すること。

ケ PMDA 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及び管理方法にて行うこと。

コ PMDA 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、又は抹消し、書面にて報告すること。

サ　本業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかに PMDA に報告すること。

（２）　情報セキュリティ監査の実施

ア　PMDA がその実施内容（監査内容、対象範囲、実施等）を定めて、情報セキュリティ監査等を行う（PMDA が選定した事業者による監査を含む。）ものとする。受託者は、あらかじめ情報セキュリティ監査等を受け入れる部門、場所、時期、条件等を「実施計画書」に付記し提示すること。

イ　受託者は自ら実施した外部監査についても PMDA へ報告すること。

ウ　受託者は、情報セキュリティ監査の結果、本調達における情報セキュリティ対策の履行状況について PMDA が改善を求めた場合には、PMDA と協議の上、必要な改善策を立案して速やかに改善を実施するものとする。

エ　本調達に関する監査等が実施される場合、受託者は、技術支援及び情報提供を行うこと。

オ　受託者は、指摘や進捗等把握のための資料提出依頼等があった場合は、PMDA と協議の上、内容に沿って適切な対応を行うこと。

情報セキュリティ監査の実施については、本項に記載した内容を上回る措置を講ずることを妨げるものではない。

１０　再委託に関する事項

①　受託者は、受注業務の全部又は主要部分を第三者に再委託することはできない。

②　①における「主要部分」とは、以下に掲げるものをいう。

ア　総合的企画、業務遂行管理、手法の決定及び技術的判断等。

イ　SLCP-JCF2013 の 2.3 開発プロセス、及び 2.4 ソフトウェア実装プロセスで定める各プロセスで、以下に示す要件定義・基本設計工程に相当するもの。

- 2.3.1 プロセス開始の準備
- 2.3.2 システム要件定義プロセス
- 2.3.3 システム方式設計プロセス
- 2.4.2 ソフトウェア要件定義プロセス
- 2.4.3 ソフトウェア方式設計プロセス

ただし、以下の場合には再委託を可能とする。

- 補足説明資料作成支援等の補助的業務
- 機能毎の工数見積において、工数が比較的小規模であった機能に係るソフトウェア要件定義等業務

③ 受託者は、再委託する場合、事前に再委託する業務、再委託先等を PMDA に申請し、承認を受けること。申請にあたっては、「再委託に関する承認申請書」の書面を作成の上、受託者と再委託先との委託契約書の写し及び委託要領等の写しを PMDA に提出すること。受託者は、機密保持、知的財産権等に関して本仕様書が定める受託者の責務を再委託先業者も負うよう、必要な処置を実施し、PMDA に報告し、承認を受けること。なお、第三者に再委託する場合は、その最終的な責任は受託者が負うこと。

④ 再委託先が「８（２）入札制限」の要件を満たすこと。

⑤ 受注者の責任において、サプライチェーンリスクの発生を未然に防止するための体制を確立すること。

⑥ 再委託先において、本調達仕様書に定める事項に関する義務違反、義務を怠った場合には、受注者が一切の責任を負うとともに、PMDA 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。

⑦ 再委託における情報セキュリティ要件については以下のとおり。

- 再委託先が「９（１）情報セキュリティ管理の実施」の要件を満たすこと
- PMDA から提供する情報の目的外利用を禁止すること。
- 受託者は再委託先における情報セキュリティ対策の実施内容を管理し PMDA に報告すること。
- 受託者は業務の一部を委託する場合、本業務にて扱うデータ等について、再委託先またはその従業員、若しくはその他の者により意図せざる変更が加えられないための管理体制を整備し、PMDA に報告すること。
- 受託者は再委託先の資本関係・役員等の情報、委託事業の実施場所、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）・実績及び国籍に関して、PMDA から求めがあった場合には情報提供を行うこと。
- 受託者は再委託先にて情報セキュリティインシデントが発生した場合の再委託先における対処方法を確認し、PMDA に報告すること。
- 受託者は、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の確認方法を整備し、PMDA へ報告すること。
- 受託者は再委託先における情報セキュリティ対策の履行状況を定期的に確認すること。また、情報セキュリティ対策の履行が不十分な場合の対処方法を検討し、PMDA へ報告すること。
- 受託者は、情報セキュリティ監査を実施する場合、再委託先も対象とするものとする。
- 受託者は、再委託先が自ら実施した外部監査についても PMDA へ報告すること。
- 受託者は、委託した業務の終了時に、再委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認すること。

⑧　上記①～⑦について再委託先が、さらに再委託を行う場合も同様とする。

１１　その他特記事項

（１）　環境への配慮

環境への負荷を低減するため、以下に準拠すること。

①　本件に係る納入成果物については、最新の「国等による環境物品等の調達の推進等に関する法律（グリーン購入法）」に基づいた製品を可能な限り導入すること。

②　導入する機器等がある場合は、性能や機能の低下を招かない範囲で、消費電力節減、発熱対策、騒音対策等の環境配慮を行うこと。

（２）　その他

PMDA 全体管理組織（PMO）が担当課に対して指導、助言等を行った場合には、受託者もその方針に従うこと。

１２　附属文書

（１）　要件定義書

別紙１　非機能要件
別添１　セキュリティ脆弱性診断要件
別添２　セキュリティ対応方針と役割分担
別添３　バックアップ・リカバリ方針
別添４　運用監視・保守方針と役割分担

（２）　事業者が閲覧できる資料一覧

閲覧資料１　独立行政法人 医薬品医療機器総合機構　情報セキュリティポリシー
閲覧資料２　PMDA 情報セキュリティインシデント対処手順書
閲覧資料３　セキュリティ管理要件書(ひな型)
閲覧資料４　システム設計書
これら資料は、入札説明会に参加した事業者のうち、PMDA に「秘密保持等に関する誓約書」を提出した事業者から申し出があれば開示する。

１３　窓口連絡先

独立行政法人　医薬品医療機器総合機構　経営企画部広報課

担当：星野 達郎

電話：03（3506）9454

Mail：hp2015-hoshu●PMDA.go.jp

※●は@に置き換えてください。

別紙１　非機能要件

平成３１年１月

独立行政法人　医薬品医療機器総合機構

目次

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）　ユーザビリティ要件

本調達において、現行システムからユーザビリティに原則変更はない。ただし、現行システムで使用しているソフトウェアに依存する機能において、該当ソフトウェアが販売中止で使用できない、または新バージョンにおける機能変更等でやむを得ず変更が発生する場合は、PMDA の承認を得ることで変更を許可する場合がある。

（２）　アクセシビリティ要件

本調達において、現行システムからアクセシビリティに原則要件はない。ただし、新バージョンにおける機能変更等でやむを得ず変更が発生する場合は、JIS X 8341-3:2016 の適合レベル AA に準拠するものとする。

２　システム方式に関する事項

（１）　情報システムの構成に関する全体の方針

本調達で納入する、ハードウェア製品、ソフトウェアパッケージ製品及びネットワーク製品については、原則変更はないものとする。
ただし、市場において導入実績が豊富な一般的な製品であり、開発・保守・拡張・改修等に柔軟性を持つ製品の場合は、PMDA の承認を得ることで変更を許可する場合がある。

製品選定における留意事項を以下に示す。

① 競争原理によって、適正な価格で調達することが可能な製品であること。

② 他の業者においても、市場で調達可能な製品であり、本受託者が独占的に供給する製品ではないこと。

③ 稼働後から 5 年以上、保守サービスが受けられる又は同等製品（同製品のバージョンアップ又は後継製品）が継続的に調達可能であること。

④ 本システムのための独自仕様でないこと。

⑤ 現行システムと同等の規模（トランザクション量とデータ量）での使用実績があること。なお、業務量に依存しない製品については対象外とする。

⑥ 特定の技術及び製品に依存せず、高品質・高信頼と経済性を兼ね備え、継続的に提供される技術を適用可能なハードウェア及びソフトウェアとすること。

⑦ 本システムの次期更改時の移行作業において、特定の業者、製品に依存することなく円滑に移行実施可能なシステム構成であること。

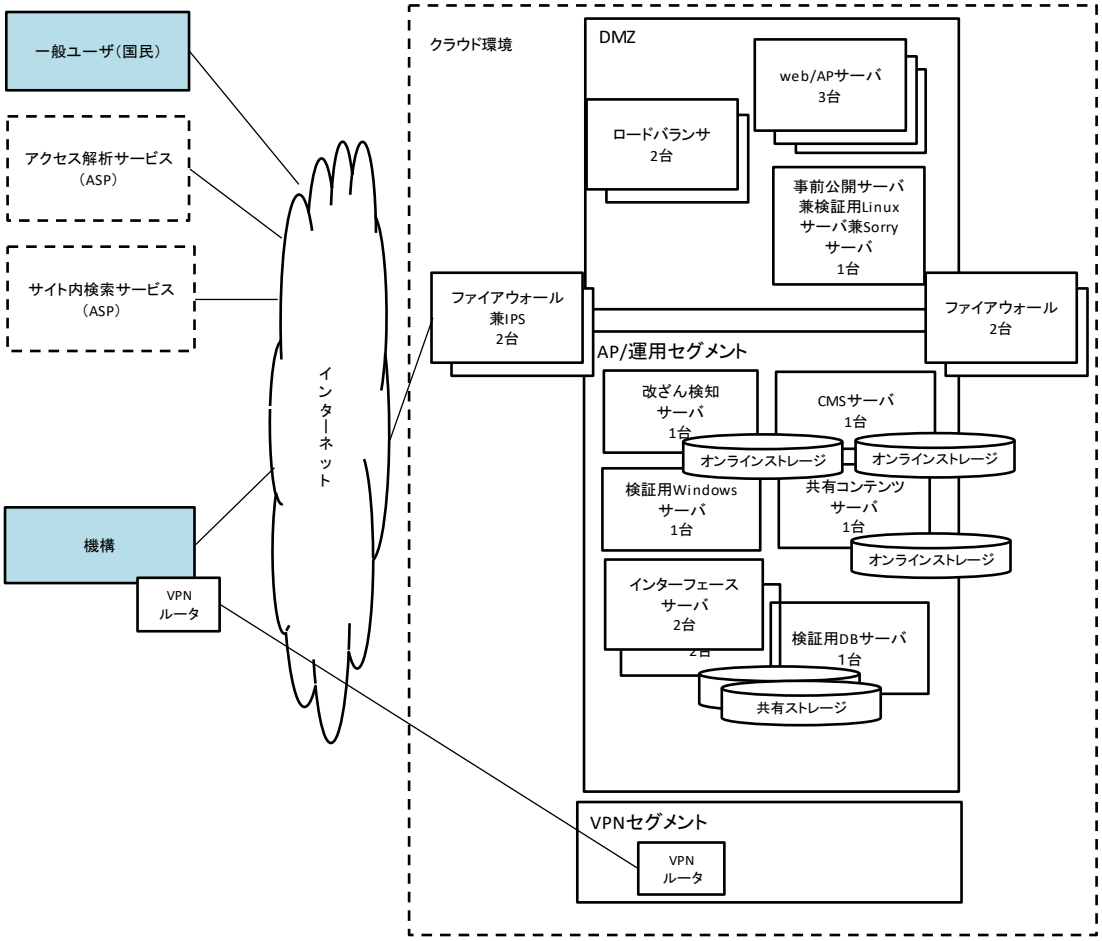
⑧ オープンソースソフトウェアの製品やツールについては、保守や技術サポートを調達することが困難である場合は、採用しないこと。なお、当該製品を組み込むために、本システ

ムのすべて又は一部のソースコードを開示する必要が生じる場合は、事前に PMDA と協議すること。

（２） 情報システムの全体構成

現時点で想定する稼働環境の全体構成は、調達仕様書の図 1-1 に示す現行の全体構成図からレコメンドサービスを廃止した図 2-1 に示す構成とする。

図 2-1 全体構成図



３ 規模に関する事項

運用開始後 2 年後の推定値である。クラウドサービスとして下記要件を満たす構成を提供すること。但し、想定外のアクセス量、データ量発生時にも、必要に応じリソースを拡張し対応していくことが可能であること。

（１）　処理件数

表　3-1　処理件数

項目	2018 年度 (実績)	2021 年度 (想定)
1 日当たりのコンテンツ掲載件数	約 10 件	20 件
月間 PV（平均／最大）	約 342 万／ 約 378 万	約 400 万／ 約 450 万

（２）　データ量

表　3-2　データ量

項目	2018 年 12 月末 (実績)	2021 年 7 月末 (想定)
外部ストレージ容量（使用量）	約 1.2TB	約 1.8TB

外部ストレージ容量（確保容量）は、3.5TB とすること。

4　性能に関する事項

①　一般公開での目標スループット

ア．目標スループット（同時利用者数）は 60 とする。2018 年の 1 日最多ページビュー数が約 40 万であり、ピーク時間帯（5 時間）に集中すると想定した場合、同時利用者数は約 20 となる。同時アクセス数増大率を 3 倍とした。

イ．目標トランザクション数は約 100 万ページビュー／日とする。上記 1 日最多ページビュー数をトランザクション数とし、増大率を 3 倍とした。

②　PMDA 内管理機能における性能要件

ア．画面応答（参照系処理）は 3 秒以内とする。

イ．画面応答（更新系処理）は 10 秒以内とする。（※1）

ウ．DB 検索結果表示は 10 秒以内とする。（※1）

エ．DB 更新処理は 10 秒以内とする。（※1）

オ．文書ファイル（PDF 又は Word ファイルを想定。以下同じ）表示は 10 秒以内とする。（※2）

カ．文書ファイル検索結果応答は 10 秒以内とする。（※1）

キ．文書ファイル全文検索結果応答は 30 秒以内とする。（※1）

ク．ファイルの更新処理（出力処理）は 1 分以内とする。（※3）

上記は、VPN 等を経由したアクセス時や、件数・容量が大きい場合の許容限界である。許容限界を超えるような機能が必要な場合は機構と協議の上、別途適切に定めること。許容限界を超える機能の要因として、対象データが膨大となる場合や検索条件が索引を使えないような複雑な場合などを想定している。

※1：通常は、3 秒以内とする。

※2：通常は、5 秒以内とする。

※3：通常は、10 秒以内とする。

５　信頼性に関する事項

（１）　可用性要件

①　可用性に係る目標値

可用性に係る目標値は、「表 5-1」に示す。

表　5-1　情報システムの SLA

No.	SLA 項目	説明	設定値
1	サービス稼働時間	・情報システムのサービスが提供される時間帯 ・定期保守、法定停電等による計画停止時間を除く	24 時間 365 日
2	運用・保守サービス時間	・運用・保守サービスのうち、監視業務、障害対応業務が提供される時間帯	24 時間 365 日
3	稼働率（正常稼働時）	・No.1 に示すサービス稼働時間における稼働予定時間に対して実際に稼働した時間（稼働時間）の割合であり、以下の式により計算する ＜稼働率（%）＝（1－1 ヶ月の停止時間÷1 ヶ月の稼動予定時間）×100＞ ・ 稼動予定時間とは、定期保守、法定停電等による計画した停止時間を除く、1 ヶ月に稼動すべき時間である ・ 停止時間とは、サービスが停止していると確認された時刻（本調達で導入する監視機能で障害を検知した時刻、または、利用者が連絡した時刻の	99.9%以上

No.	SLA 項目	説明	設定値
		いずれか早い方）から利用可能とされた時刻までの経過時間を指す ・ 停止時間には、待機系システム等への切換えのために発生した停止時間、障害からの本各復旧のために必要になった停止時間、人為的なミスにより発生した停止時間等を含む ・ 冗長化構成されている部分のうち、一部分が停止した場合でも、冗長化によりサービスの提供に支障を来たさなかった場合には、停止時間として取り扱わない ・ PMDA 側に責任があることが確認できた場合には、停止時間として取り扱わない	
7	RPO（目標復旧時点）	・データの損失は許容できないため、データの再送や再処理を含め、障害発生時までの復旧を基本とする（大規模災害時を除く）	データの障害：障害発生時 機器等の障害：直近のバックアップ時点 大規模災害時：1 か月以内
8	RTO（目標復旧時間）	・業務停止時間を極力少なくするため、6 時間以内の復旧を目標とする（大規模災害時を除く） ・共有コンテンツのリストア等、長時間の処理を行う必要がないものについては、2 時間以内の復旧を目標とする。	データの障害：6 時間以内 機器等の障害：10 時間以内 大規模災害時：数か月以内
4	稼働率（縮退稼働時）	・ 冗長化構成がされている部分のうち一部分が停止した場合で、レスポンスタイムの低下等が生じている時間（縮退稼動時間）を停止時間として取り扱う ・ 縮退稼動時間とは、縮退稼動の開始から正常稼動に復旧するまでの時間	96.0%以上

No.	SLA 項目	説明	設定値
		とするが、PMDA の都合により正常稼動への復旧作業を延期する場合等は、復旧のための準備がすべて整い、PMDA の承認を得るまでの時間を縮退稼動時間とする ・ 上記以外は正常稼働時と同様	
5	平均故障間隔（ MTBF ： Mean Time Between Failure）	・ システムに故障が発生してから、次に故障が発生するまでの平均時間で、以下の式により計算する ＜平均故障間隔＝総稼動時間÷総故障件数＞ ・ 個別サービスの稼動状態（停止、縮退稼動、及び通常稼動等）に関らず、特別な対応が 必要になるすべての故障・不具合を故障件数として取り扱うこと ・ PMDA 側に責任があることが確認できた場合には、故障件数として取り扱わない	2920 時間（4 ヶ月）以上
6	平均復旧時間（ MTTR ： Mean Time To Repair）	・ 平均復旧時間とは、機器に故障が発生した時刻から故障が復旧した時刻までに要した時間の 1 ヶ月間における平均値である ・ 平均復旧時間は、以下の式により計算する ＜平均復旧時間＝1 ヶ月の総復旧時間÷1 ヶ月間の総件数＞ ただし、平均復旧時間の計算には、運用支援業者の稼動時間外を含まないものとする ・故障が発生した時刻とは、本調達で導入する監視機能で障害を検知した時	6 時間以内

No.	SLA 項目	説明	設定値
		刻、または、利用者が連絡した時刻のいずれか早い方とする ・復旧とは、障害原因を排除し、正常に稼働することを確認し、利用者が使用可能な状態にあることとする（縮退運転等の暫定復旧も復旧とみなす） ・ PMDA 側に責任があることが確認できた場合には、復旧時間計算の対象から除外する	

② 可用性に係る対策

ア 本調達で導入する機器等は、性能劣化や停止により業務処理が影響を受けることのないよう、本番稼働環境のサーバ、ストレージ、ネットワーク等の冗長化を行うこと。なお、サーバの冗長化に当たっては、可能な限り Active-Active 構成とし、サーバ間の負荷がなるべく均等になるように処理を分散して割り当てるとともに、機器資源の有効活用を図ること。

イ Active-Active 構成で冗長化したサーバは縮退運転を可能とし、その場合のレスポンス順守率は 60%とすること。

ウ ストレージ

ウ－1 ハードディスク等障害時のデータ消失対策として、ホットスワップ可能な RAID 構成とすること。

ウ－2 データファイルは信頼性の高い外部ストレージに配置すること。

ウ－3 ストレージ装置について、可能な限りコントローラ、電源、FAN、I/F 等が冗長構成とすること。

エ ネットワーク

エ－1 LAN 及び SAN は原則、すべての経路・機器ともに 2 重化すること。

エ－2 ネットワーク機器は原則、すべてのコンポーネント（電源、CPU、FAN、I/F 等）を冗長化すること。

エ－3 Web サーバ等既存アプリケーションに影響を及ぼす可能性がある箇所はロードバランサをトランスレータとして利用すること。

（２） 完全性要件

データの紛失や改ざんからデータを保護し、データの正確性及びデータの一貫性を保証することとする。

（３）　機密性要件

利用を許可された者以外の第三者は、システムを利用できないこととする。

６　拡張性に関する事項

（１）　性能の拡張性

利用者数増加によるアクセス負荷の増大および外部インタフェースのトランザクション量の増大を考慮して、将来的にサーバの追加、CPU、HDD、メモリの増設が可能な構成とすること。

表　６-１　拡張対象機器一覧

項番	対象機器	拡張方式	内容
1	共有コンテンツサーバ	スケールアップ	CPU、MEM、HDD
2	インタフェースサーバ		CPU、MEM、HDD
3	改ざん検知サーバ		CPU、MEM、HDD
4	事前公開兼検証用 Linux サーバ		CPU、MEM、HDD
5	検証用 Windows サーバ		CPU、MEM、HDD
6	検証用 DB サーバ		CPU、MEM、HDD
7	ファイアウォール		処理能力
8	ロードバランサ		処理能力
9	オンラインストレージ		ディスク容量
10	Web/AP サーバ	スケールアウト	台数増

７　上位互換性に関する事項

OS、ミドルウェア等のソフトウェアパッケージのバージョンアップに対して、影響範囲が限定的で、小規模の改修で対応可能なシステムとすること。また、バージョンアップへの対応が技術的に困難である場合は、PMDA と協議し、その指示に従うこと

８　中立性に関する事項

特定の製品、技術等に依存することなく、運用・保守を担当するベンダの交替時、システム拡張時、あるいは次期更改時等において、他の業者等に必要な情報を、支障なく引き継ぐことが可能なシステム構成とすること。

９　継続性に関する事項

（１）　継続性に係る目標値

大規模災害（地震、火災及び風水害等又は第三者による情報システムへの攻撃等による直接的な設備及び情報システムの損壊、あるいは、ライフライン（電力、通信及び交通等）の機能不全による情報システムの長時間停止）が発生した場合を除いて、情報システムを用いた業務処理が維持できること。

（２）　継続性に係る対策

大規模災害が発生した場合に対しては、早急にその状態を把握し、リスクの拡大を防止し、速やかに回復させるための処置を講じることとして、その対策をシステム運用マニュアル、保守実施計画書に取りまとめること。

１０ 情報セキュリティに関する事項

（１）　情報セキュリティ対策

受託者は、機構と調整の上、必要な対策を講じること。具体的には、別添２「セキュリティ対応方針と役割分担」を満たす製品、サービスを選定すること。なお、本受託者が納入する基盤製品に求める情報セキュリティ機能については、「IT 製品の調達におけるセキュリティ要件リスト」（経済産業省発行）の要件を満たすこと。また、検討にあたっては「IT 製品の調達におけるセキュリティ要件リスト活用のためのガイドブック」（独立行政法人情報処理推進機構発行）を活用すること。

１１ 情報システム稼働環境に関する事項

（１）　ハードウェア・ソフトウェア構成

①　サーバ台数

クラウド環境のハードウェア台数を下表に示す。

表　１１-１　ハードウェア一覧

項番	機器名称	台数	概要
1	Web/AP サーバ	3 台	Web サイトのコンテンツを公開するサーバおよび添付文書等検索に関するアプリケーションが稼働するサーバ また、外部 ASP サービスと連携する機能を有する

項番	機器名称	台数	概要
2	共有コンテンツサーバ	1 台	静的コンテンツおよび PDF ファイル等を格納するサーバ
3	インタフェースサーバ	2 台	現行システムデータセンター内の現行システムと連携し必要となるデータの受け渡しを行うサーバ（Active-Standby 冗長構成）
4	改ざん検知サーバ	1 台	CMS サーバと Web/AP サーバとの間に介在し、Web/AP サーバ上のコンテンツが改ざんされていないかを監視するサーバ
5	CMS サーバ	1 台	Web サイトのコンテンツを作成、公開するためのサーバ
6	事前公開サーバ兼検証用 Linux サーバ兼 Sorry サーバ	1 台	コンテンツを公開サーバ（Web/AP サーバ）に公開する前にインターネット経由で事前に確認するためのサーバであり且つセキュリティパッチ等を本番サーバに適用する前に事前に検証するための Linux サーバ。インターネットからのアクセスは厚生労働省からのみに制限する必要がある。また全 Web/AP サーバが停止した場合に利用者にシステム停止中であることを提示する Sorry サーバも兼ねる。
7	検証用 Windows サーバ	1 台	セキュリティパッチ等を本番サーバに適用する前に事前に検証するための Windows サーバ
8	オンラインストレージ	3 台	共有コンテンツサーバ、改ざん検知サーバ、CMS サーバに各 1 台ずつ使用する追加ストレージ
9	共有ストレージ	2 台	インタフェースサーバ 2 台間で共有する高性能ストレージ
10	ファイアウォール兼 IPS	2 台	インターネットからのアクセス制御し不要なアクセスを防御するファイアウォール アクティブ・スタンバイの冗長構成。併せて不正侵入を検知する IPS 機能も有する。
11	ファイアウォール	2 台	クラウド内での通信を制御し不要なアクセスを防御するファイアウォール。 アクティブ・スタンバイの冗長構成。

項番	機器名称	台数	概要
12	ロードバランサ	2 台	インターネットからの Web アクセスを複数台の Web/AP サーバに振り分ける負荷分散装置機能 アクティブ・スタンバイの冗長構成。 EV SSL サーバ証明書を搭載する。
13	VPN 接続用ルータ＃1	2 台	クラウドセンター～機構間の拠点間 VPN 接続を行うためのルータ
14	VPN 接続用ルータ＃2	1 台	クラウドセンターへ VPN 接続を行うためのルータ
14	検証用 DB サーバ （検証用インタフェースサーバ） 以降、「検証用 DB サーバ」と記す	1 台	アプリケーションの改修時等、職員等が検証するために利用するデータベースサーバ、info システムのデータセンター内の現行システムと連携し必要となるデータの受け渡しを行うサーバ（Single 構成）

① 詳細仕様

本調達において必要となるハードウェア・ソフトウェア及び提供すべき外部 ASP サービスの詳細仕様を以下に示す。

表 １１-２ ハードウェア仕様

項番	機器名称	仮想 CPU ※1	仮想 MEM (GB)	仮想 HDD (GB)	仮想 NIC (GbE)
1	Web/AP サーバ	4	8	50	2
2	共有コンテンツサーバ	4	8	50	2
3	インタフェースサーバ	12	32	50	3
4	改ざん検知サーバ	2	4	50	2
5	CMS サーバ	4	8	50	2
6	事前公開サーバ兼検証用 Linux サーバ兼 Sorry サーバ	2	4	50	2
7	検証用 Windows サーバ	2	4	50	2
8	検証用 DB サーバ	2	32	50	3

※1 64bit、2.16GHz 相当

表 １１-３　ストレージ構成

項番	機器名称	サイズ（GB）	備考
1	共有コンテンツ用ストレージ	1000	RAID1 構成、実使用量記載、10,000IOPS
2	改ざん検知用ストレージ	1000	RAID1 構成、実使用量記載、10,000IOPS
3	CMS 用ストレージ#1	2000	RAID1 構成、実使用量記載、10,000IOPS
4	インタフェース用ストレージ#1	2000	RAID5 構成、実使用量記載、20,000IOPS
5	インタフェース用ストレージ#2	1500	RAID5 構成、実使用量記載、20,000IOPS
6	検証 DB 用ストレージ	500	RAID1 構成、実使用量記載、10,000IOPS

表 １１-４　ソフトウェア一覧

項番	機能名称	対象ソフトウェア
1	OS	Microsoft Windows Server
2		Redhat Enterprise Linux
3	WEB サーバ	Apache
4	AP サーバ	Apache Tomcat
5	全文検索エンジン	OracleText
6	ファイル共有	NFS サーバ（OS 機能利用）
7	データベース	Oracle Standard Edition ONE
8	改ざん検知	isAdmin Enterprise
9	CMS	ALAYA
10	ウイルス対策	Trendmicro Deep Security (Linux/Windows)相当のリアルタイムスキャンが可能な製品
11	運用監視	Tivoli Network Manager 相当の製品
12	Java 実行環境	Java Platform Standard Edition 相当の製品
13	メール送信	Postfix 相当の製品
14	クラスタソフトウェア	LifeKeeper 相当の製品
15	検証用データベース	Oracle Database Standard Edition 2

※2021 年 7 月 31 日までサポートされる最新バージョンのソフトウェアを使用すること。ただし、ソフトウェアの不具合及び業務システムの改修工数を考慮し、PMDA の承認の受けたうえでバージョンを確定すること。

※保守移管可能なライセンスが存在する場合は、保守移管可能なライセンスを使用すること。

表 １１-５　ソフトウェア構成

項番	機器名称	OS ※1	OS ※2	WEBサーバ	APサーバ	全文検索エンジン	ファイル共有	改ざん検知	ジョブ管理	ウィルス対策	運用監視	JAVA実行環境	メール送信	クラスタソフト
1	Web/AP サーバ	—	○	○	○	—	—	—	—	○	○	○	—	—
2	共有コンテンツサーバ	—	○	—	—	—	○	—	—	○	○	—	—	—
3	インタフェースサーバ	—	○	—	—	○	—	—	○	○	○	○	—	○
4	改ざん検知サーバ	○	—	—	—	—	—	○	—	○	○	—	—	—
5	CMS サーバ	—	○	—	—	—	—	—	—	○	○	○	○	—
6	事前公開サーバ兼検証用 Linux サーバ兼 Sorry サーバ	—	○	○	○	—	—	—	—	○	○	○	—	—
7	検証用 Windows サーバ	○	—	—	—	—	—	○	—	○	○	—	—	—
8	オンラインストレージ	—	—	—	—	—	—	—	—	—	○	—	—	—
9	共有ストレージ	—	—	—	—	—	—	—	—	—	○	—	—	—
10	検証用 DB サーバ	—	○	—	—	○	—	—	○	○	○	○	—	—

表 １１-６　外部 ASP サービス

項番	サービス名称	サービス概要
1	サイト内検索サービス	閲覧資料４「システム設計書」に示す要件を満たす外部サービスを想定利用期間の間提供すること。 アクセスログ解析サービスは、無償版 Google Analytics を可とする。
2	アクセスログ解析サービス	

（１）　ネットワーク構成

①　ネットワーク個別要件

ア．クラウドセンター内 LAN 要件

- 回線速度は 1Gbps 以上とする。
- バックアップ等の大容量転送時にも性能低下が発生しないように、十分なパケット処理能力を確保すること。
- ネットワークセグメントはフロントネットワークセグメント（DMZ）、運要管理セグメントを想定している。必要に応じて外部インタフェース用セグメントを分離する可能性がある。設計に応じて VLAN 設定が行えること。

イ．インターネット接続要件

クラウドセンターとインターネットサービスプロバイダ（以下「ISP」という。）間の接続は、次に示す回線容量と帯域保証を実現すること。またマルチキャリアで冗長化されたインターネット接続環境を提供すること。

表 １１-７　インターネット回線

項番	接続拠点	回線容量・帯域保証
1	クラウドセンター	100Mbps ベストエフォート（※1）

（※1）ベストエフォート型とは、帯域保証のない通信サービスのこと。

クラウドセンターにて用意するインターネット接続回線の要件は以下のとおりとする。

- 本システム利用者が、インターネットを介して本システムにアクセスできるインターネット接続環境を提供できること。
- インターネット接続回線はギガビット対応回線であること。

ウ．外部接続（VPN 接続）要件

クラウドセンターのサービスで専用の外部接続を行う場合は、必要な回線を敷設すること。インターネット接続回線を利用した VPN 接続サービスの場合は、「４．規模・性能要件」を満たすことを前提にユーザからのアクセスに影響が出ない構成を提案すること。また経路は暗号化されているものを提供すること。さらに運用作業時に使用するリモートアクセス用 SSL-VPN 接続サービスを 2 ユーザ分提供すること。リモートアクセス用 SSL-VPN 接続サービスはユーザ ID/パスワード認証にワンタイムパスワード認証を追加した 2 要素認証機能を提供し、セキュアなリモートアクセス環境を実現すること。

なお、VPN 回線の要件は以下のとおりとする。

- 接続する拠点は将来的に増減することが容易であること。
- 回線網は、次に示す回線容量と帯域保証を実現すること。

表 １１-８　VPN 回線

項番	接続拠点	回線容量・帯域保証
1	クラウドセンター～機構間 及び新システム検証環境	100Mbps ベストエフォート（※1） 閉域網サービス（※2）

（※1）ベストエフォート型とは、帯域保証のない通信サービスのこと。

（※2）閉域網サービスとは、始点から終点までプロバイダーの回線を、プロバイダーが管理しない広いインターネットの回線は使用しない通信サービスのこと。

エ．クラウドセンター～現行データセンター間

クラウドセンターと現行データセンター間は機構をブリッジ経由し接続することとする。

オ．グローバル IP アドレス要件

- クラウド環境提供事業者は、本システムに必要となるグローバル IP アドレスを 4 個提供すること。

② ネットワーク機器構成

表 １１-９　クラウドセンター用ネットワーク機器

項番	機器名称	台数	備考
1	ファイアウォール	2 台	1 台はバックアップ
2	ロードバランサ	2 台	1 台はバックアップ
3	VPN 接続用ルータ兼ファイアウォール	1 台	クラウドセンター～機構

※上記機器については、クラウドサービスとして提供可能なものはサービス提供形態とする。別途クラウドセンター内に持ち込み等必要な場合は、本件受注者にてクラウドセンター内への機器納入、設置を行うこと。

表 １１-１０　機構および新システム検証環境用ネットワーク機器

項番	機器名称	台数	備考
1	VPN 接続用ルータ兼ファイアウォール	1 台	クラウドセンター～機構
2	VPN 接続用ルータ兼ファイアウォール	1 台	新システム検証環境～機構及びクラウドセンター

③ ネットワーク機器共通要件

ア．ICMP による死活監視が可能なこと

イ．SNMP による管理が可能なこと

ウ．Syslog 管理サーバにログを転送する機能を有すること

④　ネットワーク機器個別要件

各ネットワーク機器は下表の要件を満たすこと

表　１１-１１　ネットワーク機器個別要件

項番	機器名称	区分	備考
1	ファイアウォール兼 IPS	フィルタリング機能	ルールに基づき通信の許可/拒否の処理を行う
		対応プロトコル	IP、ICMP、TCP、UDP、ESP、AH、GRE
		送信元/宛先 IP アドレス	特定アドレス、サブネットマスク、グループ
		アドレス変換（NAT）	両方向 1 対 1 の NAT、両方向 1 対 N の NAPT、片方向 1 対 N の NAPT
		分割	ファイアウォールはインスタンス単位で分割可能であること
		IP アドレス	インターネット VPN で接続する際に NAT 変換を不要とするため IP アドレスの持ち込みが可能であること
2	ロードバランサ	処理能力	200Mbps ベストエフォート
		対応プロトコル	レイヤ 4
		分散アルゴリズム	ラウンドロビン、最小コネクション（リーストコネクション）、送信元 IP アドレスハッシュ、URL ハッシュ
		セッション維持	送信元 IP アドレス、Cookie（ロードバランサ）、Cookie（サーバ）、URL、SSL セッション ID
		ヘルスチェック	ICMP（IP レベルチェック）、TCP（ポートレベルチェック）、HTTP（リクエストのチェック）
		SSL 暗号化	サーバ、ロードバランサ間の SSL 暗号化

項番	機器名称	区分	備考
		Sorry サーバ	分散対象サーバのヘルスチェックが確認できない場合に決められた Sorry サーバに通信を割り振る
3	VPN 接続用ルータ	インタフェース	10/100/1000BASE-T×2
		ルーティングプロトコル	RIP、RIP2、OSPF、BGP4(EBGP、IBGP)等
		カプセル化	VLAN、PPP、フレームリレー、PPPoE、MP
		トラフィック管理	QoS、重み付けランダム早期検出、階層型 QoS
		セキュリティ	組み込みハードウェア暗号化アクセラレーション、VPN サービス（IPSec と SSL アクセラレーションの両方）
4	リモートアクセス用 SSL-VPN（必要数：2）	利用単位	ユーザ環境毎に一式
		アクセス経路	インターネット経由
		帯域	ベストエフォート
		通信ポート制限	なし
		認証方式	2 要素認証（ユーザ ID/パスワード認証＋ワンタイムパスワード認証）
		ワンタイムパスワードトークン	ソフトウェアトークン

（３） クラウド要件

クラウドの要件について以下の通り定義する。

① クラウド方式の定義

ア．IaaS（Infrastructure as a Service）上の VPS を用いたパブリッククラウドを想定している。インターネット経由のアプリケーション実行用プラットフォーム及びストレージを提供すること。

イ．必要にあわせてサーバやストレージを利用可能なこと。

ウ．様々なプラットフォームからネットワークを通じ利用できること。

② クラウド全体構成要件

ア．サービス提供時間

計画停止時間を除き、24 時間、年中無休でサービス提供を行うこと。尚、ユーザ側の要望がある場合、可能な限り計画停止タイミングについて調整可能であること。

イ．可用性

稼働率 99.9%を実現可能な構成とすること。また、サービス単位でサービスレベルが定義でき、レベルを選択可能であること。

ウ．バックアップ・リカバリ

別添 3「バックアップ・リカバリ方針」に示す事項を満たすサービス提供を行うこと。

エ．拡張性

サーバ、ストレージのリソースはシステムを再構築することなく割り当て変更可能であること。

オ．信頼性

- サーバが停止した場合に一般ユーザに影響が発生する機能を担うサーバは、2 台以上の冗長構成とし、片系のサーバでの障害発生または OS の停止を行っても業務を継続できる構成とする。
- 性能が低下することで一般ユーザに影響が発生する機能を担うサーバは、性能要件を満たすために必要なサーバ台数に 1 台追加した構成をとることで、サーバ 1 台で障害が発生した場合にも性能要件を満たす冗長構成とする。
- サーバが停止しても一般ユーザへの影響が発生しない運用管理機能を担うサーバは、原則 1 台構成とする。ただし運用上必要なデータについては適宜バックアップを取得し、サーバ復旧後速やかにバックアップから復旧を行うこととする。
- 仮想サーバを搭載する物理サーバは原則、サーバの全てのコンポーネントを冗長化（電源ユニットの 2 重化、FAN の 2 重化、内蔵ディスクのミラー化、NIC の 2 重化など）することでサーバ単体の耐障害性を高めることとする。ただし、ブレード型サーバなどで I/F カードの冗長化が難しい場合は port レベルでの冗長化とする。
- 物理サーバ障害やメンテナンス時でも動的に仮想サーバを切り替えることでシステム稼働への影響を少なくすることが可能であること
- 標準で仮想サーバに対する HA(High Availability)機能を提供できること

カ．仮想化ソフト

「ソフトウェア構成」で指定するソフトウェアがサポートされる仮想化ソフトを使用すること。

キ．セキュリティ

本システムの扱うデータのセキュリティレベルを鑑み、クラウド環境は下記事項を満たすこと。

- 仮想化ソフトの管理者権限ユーザを確実に管理すること。
- ISMS クラウドセキュリティ認証（ISO/IEC 27017）を取得し情報セキュリティ外部監査を受けていること
- セキュリティ・インシデント／イベントへの対応をしていること
- 顧客間のリソース分割は VLAN レベルでの分離ではなく、専用の仮想ファイアウォールによる完全分離された構成とすること
- クラウド環境内のセキュリティアップデートを管理する WSUS/yum サーバにより必要なモジュールの適用が可能なこと

ク．管理機能（ポータルツール）

以下について管理可能なポータル機能を日本語で提供すること

- アカウント管理（利用ユーザ作成、変更、削除）
- 仮想サーバ管理（作成、変更、削除、電源 ON/OFF、バックアップ等）
- ネットワーク管理（IP アドレス取得等）
- ファイアウォール管理（ACL、アドレスグループ、NAT 等）
- ロードバランサ管理（負荷分散、SSL 証明書等）
- システム監視状況閲覧
- サービスデスク（IaaS 監視、障害対応）

ケ．時刻同期（NTP）

クラウド環境内の NTP サーバにより時刻同期が可能なこと

（４） クラウドセンター施設設備要件

① 施設建築物に関する要件

ア．データセンター専用の建物または準じた対応が施されていること。

イ．クラウドセンターの所在地は日本国内に設置されていること。

ウ．震度 7 の地震に耐える耐震若しくは免震構造で建築されていること。

エ．日本データセンター協議会（JDCC）が定義するファシリティスタンダードで「Tier3」以上であること。

オ．予想最大損失率 PML（Probable Maximum Loss）値が 5%未満であること。

カ．建築物総合環境性能評価システム CASBEE(Comprehensive Assessment System for Building Environment Efficiency)が「S ランク」であること。

② 立地要件

ア．地震、風水害、塩害及び落雷等、自然災害の影響の少ない場所に立地していること。（国土交通省・各自治体が公開しているハザードマップにて危険性の指

摘がない、文部科学省が示す主要活断層帯を避けた場所であること等）

③　設備要件

ア．電源設備に関する要件

- 電力供給は、災害時等においても無停電電源装置（UPS 設備）、自家発電設備により途切れることなく 24 時間 365 日安定供給すること。なお、無停電電源装置（UPS 設備）の冗長化を実現できる建物であること。自家発電設備は無給油で 72 時間以上の連続稼働を行えること。なお、途中給油によって更にそれ以上の連続稼働を行えること。
- 停電等により通常の電力供給が停止した場合、自家発電装置による電力供給を行うまでの間は、UPS 設備によりサーバ機器設置室等必要な箇所に無瞬断で電力を供給できること。なお、将来の信頼性向上の要求に応えられるよう、自家発電電装の冗長化を実現できる建物であること。また、電力供給は 2 か所の変電所から電源供給を受けられること。
- 電力設備の定期点検等を行う場合も無停止で電力供給が可能であること。
- CVCF（定電圧定周波電源装置）を通して電力供給すること。
- PUE（Power Usage Effectiveness）値は、「1.5 以下」であること。

イ．空調設備に関する要件

- 不具合や障害発生時（災害時等の商用電源停止時等）、点検実施時に影響なく、納入する機器類が正常稼動できる温度（5～35℃）、湿度（20～80%、但し結露しないこと）を 24 時間 365 日維持できること
- 空調効率向上のため、ラックの前面がコールドアイル、裏面がホットアイルとなるレイアウトとし、かつアイルキャッピング等によりホットアイルの暖気をコールドアイルの冷気と分離する等の仕組みを講じること。

ウ．消火設備に関する要件

- 築基準法、消防法に基づいた耐火建築物であり、火災報知システムを有していること。
- 隣接建物からの延焼防止装置が施されていること。また、火災発生時の消火活動に必要となる消火器、消火栓が設置されていること。
- 建築基準法施工令に規定する排煙設備が建物内の適切な個所に設置されていること。

エ．セキュリティに関する要件

- サーバルームへの入退室は、電子錠によりロックされており、生体認証又

はカード認証により個人を特定し、ロックを開錠し、入退室ができること。又、共連れ防止機能を備えていること。

- サーバルームの入退室は、監視カメラにより 24 時間 365 日監視すること
- サーバルームへの入退室の記録は、ログとして保存されていること
- 建物への入館は、有人による 24 時間 365 日の運用、監視を実施すること
- データセンターの建物内への入館管理、サーバルームへの入館管理、ラック開閉管理を行うこと
- データセンターの入館者に対し担当職員からの申請により作業立会いの依頼があった場合は、担当職員に代わり作業立会いを実施すること
- 緊急時の入館ルールが明確化されており、当日等の緊急入館ができること

（5） 環境の種類

本調達で導入する環境は、大きく以下の 2 種類とする。

① 本番環境

情報システムの本番サービスが稼働する環境として利用する。

② 検証環境

ア 環境の利用目的

ア－1. アプリケーションソフトウェアの結合テスト、総合テスト、受入テストを実施するための環境として利用する。

ア－2. 業務ソフトウェアの障害発生時における再現テスト、障害調査・分析、プログラム等の改修・検証、外部システム又は PMDA 内の他システムとの連携検証等を実施する環境として利用する。

ア－3. セキュリティパッチ適用、ウイルスパターンファイルの更新、ソフトウェアバージョンアップによる影響調査を行うための環境として利用する。

ア－4. 障害発生時における、各種変更等に関する環境として利用する。

ア－5. 本番環境へのリリースに際して、事前検証を行うための環境として利用する。

イ 環境の要件

イ－1. ハードウェアは、本番環境と同じ規模又は構成とする必要はない。

イ－2. プログラム及びソフトウェアパッケージは、本番環境と同等の製品及びバージョンとすること

イ－3. テスト、保守作業等を並行して実施できるよう、検証環境を論理的に複数の面に分割すること。

（６）　環境の導入に係る要件

本システムで必要となる各種環境の導入に係る要件は、以下に示すとおりである。

① ハードウェア等の導入作業の完了後、稼働に必要なデータ及び機器等の各種設定について追加、修正等が行われた場合は、必要となる情報を整理した上で、設計書を更新すること。また、当該追加、修正等を行うに当たり、更新前の情報については、必要に応じてバックアップを取得すること。

１２ テストに関する事項

（１）　テスト工程共通要件

実施する単体テスト、結合テスト、総合テスト、受入テストについて、共通となる要件は以下のとおり。

① 情報システムの正常稼働を保証するためのテストとして、単体テスト、結合テスト及び総合テストを実施すること。また、PMDA が行う受入（運用）テストの支援を行うこと。

② 各テストを行うため一連のテストケース（入力、出力、及びテスト合否基準）、テストデータ、及びテスト手順を整理し、テスト計画書として作成し、PMDA と協議の上、承認を得ること。

③ 各テスト終了時に、実施内容、品質評価結果、及び次工程への申し送り事項等について、テスト結果報告書を作成し、PMDA と協議の上、承認を得ること。

④ テストに使用するテストツール等については、PMDA と協議の上、使用すること。

（２）　テスト計画書

実施する単体テスト、結合テスト、総合テストについて、設計し、テスト方針、実施内容、及び実施理由を記述し、テスト計画書として提示し、テスト開始 1 ヶ月前までに PMDA と協議の上、承認を得ること。

承認されたテスト計画書に基づき、進捗管理を確実に実施すると共に、進捗状況の報告を定期的かつ PMDA の求めに応じて行うこと。

以下に、テスト計画書で必要と考える事項を示す。

① テスト概要

ア　テスト範囲

イ　テスト品質目標（テスト項目数、バグ検出数）

② テストに関する実施作業及びスケジュール

③　テスト環境（テストに使用した回線及び機器構成、その他ツール、場所等）。

④　テスト体制（テスト実施者、テスト結果確認者（評価者））

⑤　使用及び提出するドキュメントとその定義

ア　テスト項目一覧

イ　テスト仕様書

ウ　懸案事項一覧

エ　テスト結果報告書

（３）　単体テスト

プログラム及びモジュールが個別単体において正しく機能することを確認する。パッケージ化されたプログラム及びモジュールについてもテスト範囲とする。パッケージ化されている範囲について単体テストを実施しない場合には、実施しなくても該当機能が正しく機能することを別の手段で証明し、PMDA と協議の上、承認を得ること。

（４）　結合テスト

プログラム及びモジュールが、情報システムの各システムの単位でそれぞれ正しく機能することを確認するため、段階的に結合した状態でテストを行い、ソフトウェアの結合が完全であることを確認する。

（５）　総合テスト

情報システム全体として要件どおりにシステムが構築されていることを確認するために、テストを行い、システムが納品可能な状態であることを確認する。確認に当たっては、ソフトウェア製品が仕様に適合し、かつ実稼働環境で利用可能であることを確認できる評価指標及び合格条件を設定した上で、テストを実施する。

特に、総合テストにおける性能及び負荷のテストにおいては、想定する最大人数が同時に利用開始した場合であっても問題が生じないことを確認する。

（６）　受入テストの支援

PMDA が実施する受入テストにおいて、本受託者は、テスト計画の策定、準備、テストの実施、成果物の作成、テスト実施結果の報告等に関して、基盤製品に関する設定変更、情報提供等の必要な支援を行うこと。

１３ 移行に関する事項

（１） 移行手順

移行において想定する作業は以下のとおり。

① 移行計画書の策定

② 移行設計

③ 移行手順の作成・検証

④ 移行プログラムの作成・検証

⑤ リスクの洗い出し・コンティンジェンシープランの作成

⑥ 移行リハーサルの実施

⑦ 移行判定

⑧ 移行作業の実施

（２） 移行要件

現行システムから更改後のシステムへの移行に当たっては、機器の安定稼働及び業務の継続に影響を与えることなく、速やかに実施する必要がある。以下の基本方針に基づき、移行計画・作業を行うこと。

① 情報システムの安定した稼働及び業務の継続に影響を与えることがないよう、安全で確実な作業を優先すること。

② PMDA が承認した日時を除き、現在稼働中のシステムのサービスを停止することなく、移行作業を行うこと。

③ システムの停止を伴う作業が避けられない場合には、システム利用者への影響を最小限に抑えるため、平日においては、勤務時間外、その他土日及び休日を作業実施日の基本として検討し、停止予定日より、原則 1 ヶ月前に停止日時及び停止による影響（停止するサービスの範囲）について、PMDA の承認を書面にて得ること。

④ 移行作業中に障害が発生した場合には、速やかに原因究明にあたるとともに、移行実施計画書、システム切替手順書とに従い、切り戻し作業を行い、PMDA の承認を得て、必要な障害対処作業を本受託者の責任と負担により実施すること。

⑤ 移行の実施前に、現行機器のデータについて、バックアップを取得すること。

（３） 移行対象データ

情報システムで管理している情報全てを移行対象データとする。ただし PMDA が移行不要と判断したデータについては除外する。

１４ 引継ぎに関する事項

（１） 運用・保守業者への引継ぎ

以下の事項に留意して、運用・保守業者等に引継ぎを実施すること。

なお、引継ぎ先、引継ぎ内容及び手順等の概要を、「表 １４ 引継ぎ内容、手順」に示す。

① 運用・保守業務の円滑な実施に役立つよう、必要な各種情報及び資料の提供を行うこと。
② 引継ぎの内容は、事前に PMDA に示し承認を得ること。
③ 引継ぎの実施に当たっては、PMDA 及び引継ぎ先と日程を調整した上で実施すること。
④ 引継ぎに必要な資料等は、本受託者において用意すること。
⑤ 必要に応じて、実機での操作説明等を行うこと。
⑥ 運用・保守業者等へ引継ぐテスト済みの環境については、セキュリティパッチ及びウイルスパターンファイルを最新化の上、引継ぐこと。

表 １４ 引継ぎ内容、手順

No.	引継ぎ発生時（予定）	引継ぎ元	引継ぎ先	引継ぎ内容	引継ぎ手順
1	2019 年 9 月	本受託者	情報システム運用業者	情報システムの運用手順等、本受託者及び PMDA が必要と判断した引継ぎを行うこと。	・引継計画書を策定すること。 ・引継計画書に基づき、引継ぎを実施し、引継ぎ実施後、引継ぎ完了報告書を作成すること。

１５ 教育に関する事項

（１） 教育対象者の範囲、教育の方法

本調達はソフトウェアのバージョンアップによる変更部分のみのため、大幅な運用変更は発生しない想定である。PMDA 内外のシステム利用者に対し、各 1 回程度説明会を実施し、変更点を周知すること。

（２） 教材の作成

説明会の実施にあたり、変更点を抜粋した資料を作成すること。

１６ 運用に関する事項

（１）　運転管理・監視等要件

クラウドセンターは、別添４「運用監視・保守方針と役割分担」に示す運用サービス及び監視サービスを有し、運用・監視対応可能な状態でのクラウド環境提供が可能なこと。

（２）　運用サポート業務

情報システムの運用サポート業務は、別途調達する運用支援業者が実施するため、本調達の対象外とする。

（３）　業務運用支援

情報システムの業務運用支援業務は、別途調達する運用支援業者が実施するため、本調達の対象外とする。

１７ 保守に関する事項

（１）　アプリケーションプログラムの保守要件

情報システムのアプリケーションプログラムの保守業務は、別途調達する運用支援業者が実施するため、本調達の対象外とする。

（２）　ハードウェア及びソフトウェア製品の保守要件

クラウドセンターは、別添４「運用監視・保守方針と役割分担」に示す保守サービスの提供が可能なこと。

１８ 別添

（１） 別添１：セキュリティ脆弱性診断要件

本調達における脆弱性診断とは当該システムに「その時点での脆弱性が存在するか」を調査することである。OS、ミドルウェア、DBMS、あるいは当該システム上で稼働している Web アプリケーションは、リリースされてから使用される期間が長くなればなるほど脆弱性が発見される可能性が高くなり、結果的に、長く使用しているシステム程、脆弱性を内包している危険性が高まる。また、新しい攻撃手法については、当初は開発した攻撃者だけが使用しているため、攻撃対象は限定的であるが、時間を経てその攻撃手法がインターネット等を介して広まっていくとマルウェア化され、被害は加速度的に広がっていく。また、機構のセキュリティ対策の質的向上を期すため、各年度毎に脆弱性及び対策状況の推移を示すことが求められており、期間中、診断項目や精度は、高いレベルで同一に維持される必要がある。
以下に期間中に実施すべきセキュリティ診断要件を示す。

基本要件

- プラットフォーム診断は、診断の網羅性及び正確性を担保するために、1 種類の商用診断ツールのみで行うのではなく、目的に応じた複数の診断ツールを併用し、かつ診断担当者による手動診断を実施すること。
- Web アプリケーション診断は、診断の網羅性及び正確性を担保するために、担当者による手動診断で実施すること。やむを得ず商用診断ツールを使用する場合には、ツール適用範囲は 50%以下とすること。
- 診断にあたっては、事前に診断対象、診断内容、診断スケジュール、診断担当者、緊急時連絡方法等を記載した、診断内容確認書を作成すること。
- 作業時間は、原則平日 10:00～17:00 とするが、必要に応じて夜間・深夜・休日等にも対応すること。
- 診断中に緊急度の高い脆弱性が発見された場合、報告会や報告書作成を待たずして対策を実施するために、問題点とその原因（詳細記述）、脅威の内容、緊急性、考えられる被害、具体的な対応策、関連情報、リスク対策等を記載した速報を診断日の翌営業日までに提出すること。
- 契約期間中、年度毎に検知された脆弱性の数や種類を比較・分析し、年次で報告すること。
- 検出された脆弱性に対して、効果的な対策を提案し、提供できる部門を有すること。
- 診断業務の品質を担保するために、脆弱性診断を担当する部門に置いて ISO9001 の認証を取得していること。また、本件における品質管理体制と役割を示すこと。
- 機構のセキュリティ情報を取り扱うため、診断を実施する当該部門、または全社で ISMS の認証を取得していること。
- プラットフォーム診断について、リモート診断及びオンサイト診断と合わせて、年

間 1000 IP 以上の診断実績を、直近の 5 年以上継続していること。これを客観的に証明できる証憑を提示すること。

- Web アプリケーション診断について、1000 画面遷移以上の診断実績を、直近の 5 年以上継続していること。これを客観的に証明できる証憑を提示すること。
- 診断にあたっては、責任者と実施担当者で構成される診断チームを編成すること。
- 診断チームの責任者は 10 年以上の診断実績を有し、機構との会合に下記いずれかの資格を有する者が参画すること。
  - ✧ 公認システム監査人
  - ✧ 公認情報システム監査人（CISA）
  - ✧ 公認情報システムセキュリティ専門家（CISSP）
  - ✧ 情報セキュリティスペシャリスト
- 診断の実施担当者は、診断経験 3 年以上で、下記いずれかの資格を有する者で構成されること。
  - ✧ 公認システム監査人
  - ✧ 公認情報システム監査人（CISA）
  - ✧ 公認情報システムセキュリティ専門家（CISSP）
  - ✧ 情報セキュリティスペシャリスト
  - ✧ テクニカルエンジニア（ネットワーク）

（２）　別添２：セキュリティ対応方針と役割分担

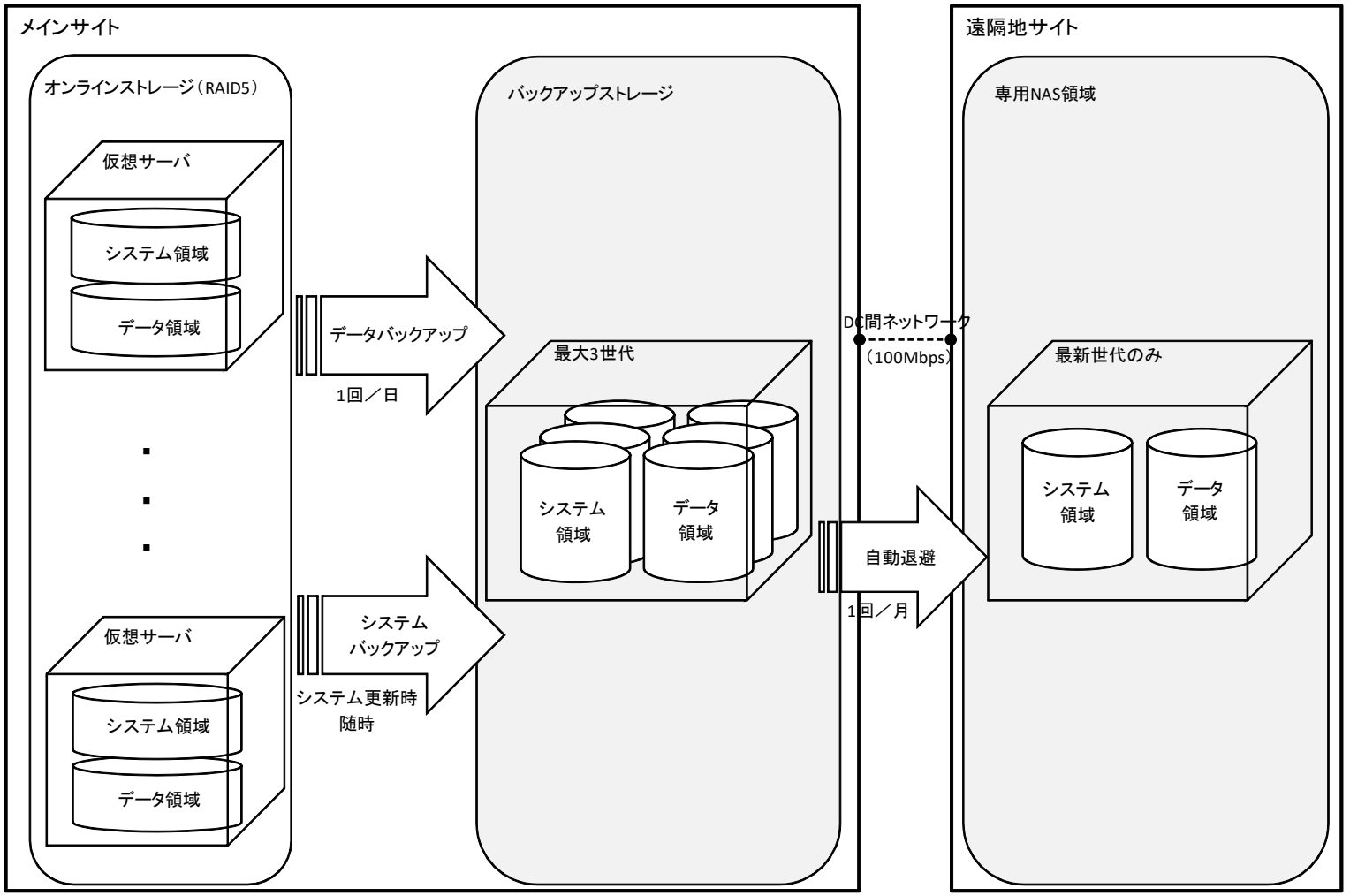
対策区分	対策方針	対策要件	目的	対応方針	実施者	
					本調達業者	運用・保守業者
侵害対策	通信回線対策	通信経路の分離	不正行為の影響範囲を限定的にするため、業務に応じて通信経路（ネットワーク）の分離を行うこと。	FWサーバ又はサービスを提供する	○	-
				FWの設定を行う	○	-
				VLANでDMZによる外部アクセス向けネットワークを分離可能なサービスを提供する	○	-
		不正通信の遮断	不正プログラムによる情報漏洩等の被害を防止するため、マルウェア感染防止の対策を行うこと。	ウィルス対策ソフトまたはサービスを提供する	○	-
		通信のなりすまし防止	通信回線を介したなりすましによる不正を防止すること。	VPS管理画面は特定のVPN接続元以外からの通信を受付けないサービスを提供する	○	-
				インターネットからのユーザ向けサービスにSSLを使用する場合は信頼された証明書を導入する	○	-
				特定利用者にのみ提供するサービスの場合には、APの認証方式を構築する	○	-
		サービス不能化の防止	トラフィック集中によるサービス不能化の脅威を軽減すること。	ロードバランササーバ又はサービスを提供する	○	-
				脆弱性をターゲットにしたDoS攻撃に対してはサーバに対する脆弱性対策（パッチ適用）を実施する	-	○
	不正プログラム対策	マルウェアの感染防止	不正プログラムによる情報漏洩等の被害を防止するため、マルウェア感染防止の対策を行うこと。	ウィルス対策ソフトまたはサービスを提供する	○	-
		マルウェア対策の管理	不正プログラム対策の最新化を確実に行うため、マルウェア対策状況を管理すること。	ウィルス対策ソフトまたはサービスを提供する	○	-
	セキュリティホール対策	構築時の脆弱性対策	情報システムの脆弱性をついた攻撃を予め防ぐため、脆弱性の有無を確認し対処すること。	OSに対するパッチ適用サービスを提供する	○	-
				OS、ミドルウェアに対する脆弱性対策を実施する	○	-
				APのセキュアコーディングを徹底する	○	-
				情報セキュリティに配慮したシステム設定を行う	○	-
				総合テスト前に外部セキュリティ診断を実施、報告する	○	-
		運用時の脆弱性対策	運用開始後に発見される脆弱性について、その改善を行うための対策を実施すること。	OSに対するパッチ適用サービスを提供する	○	-
				OS、ミドルウェアに対する脆弱性対策を実施する	-	○
				年1回外部セキュリティ診断を実施、報告する	-	○
不正監視・追跡	証跡管理	証跡の蓄積・管理	不正行為の検知、原因追求を行うため、情報システムのログの収集・蓄積・保管を行うこと。	FWログ保管サービスを提供する	○	-
				OS、ミドルウェアのログを取得・保管する	-	○
		証跡の保護	不正な証跡の改変や削除を防止するため、証跡保護を行うこと。	FWログへのアクセス可能なインターフェースは読み取り専用となるサービスを提供する	○	-
				OS、ミドルウェアのログに対するアクセス制御を実施する	○	-
		時刻の正確性確保	証跡の発生時刻を正確に把握することで正確な分析を行うため、システム全体の時刻を同期させること。	NTPサービスを提供する	○	-
	不正監視	侵入検知	外部ネットワークから侵入による情報セキュリティの侵害を防止するため、不正侵入の検知を行うこと。	FWサーバ又はサービスを提供する	○	-
				FWの設定を行う	○	-
		サービス不能化の検知	トラフィック集中によるサービス不能化を検知すること。	FWのフロント側のトラフィック量を検知可能なサービスを提供する	○	-
アクセス・利用制限	主体認証	主体認証	許可されていない利用者のアクセスを防止するため、アクセス主体を認証するための機能を備えること。	VPS管理用アクセスはSSL-VPNの二要素認証において制御可能なサービスを提供すること	○	-
				特定利用者にのみ提供するサービスの場合には、APの認証方式を構築する	○	-
				パスワードの定期更新運用の実施	-	○
データ保護	機密性・完全性の確保	通信経路上の盗聴防止	通信経路上に流れるデータが盗聴された場合でも影響を低減させるための措置を行うこと。	VLANで情報を保存する機器を内部セグメントに配備可能なサービスを提供する	○	-
		保存情報の機密性確保	保存されているデータの搾取を防止するため処置及び搾取された場合に影響を低減させるための、措置を行うこと。	通信制御可能なFWサービスを提供する	○	-
				VLANで情報を保存する機器を内部セグメントに配備可能なサービスを提供する	○	-
		保存情報の完全性確保	情報が不正に改ざんさせることを防止するため、システムが取り扱う情報の完全性を確保すること。	改ざん検知ソフトまたはサービスを提供する	○	-
物理対策	情報搾取・侵入対策	侵入の物理的対策	物理的に区画させたエリアに不正に侵入しての不正行為を防止するための、措置を行うこと。	入退館管理やラック開錠・作業ルールの徹底されたデータセンター設備を提供すること	○	-
障害対策（事業継続対応）	構成管理	システムの構成管理	必要な機器のみによって必要なサービスのみを提供するように情報システムの構成及び稼働状況の管理を行うこと。	機器構成や稼働状況の把握が可能なサービスを提供すること	○	-
	可用性確保	システムの可用性確保	システムの異常停止を防止するとともに障害時のシステムの迅速な復旧を行うこと。	VPS環境にて保有するHAサービスを提供すること	○	-
				IaaSにて機器、ネットワークの冗長化が行われていること	○	-
				システムバックアップ、データバックアップ保管サービスの提供が可能なこと	○	-
				定期的にシステムバックアップ、データバックアップを実施すること	-	○
				障害時にリストア作業を実施すること	-	○

（３）　別添３：バックアップ・リカバリ方針

障害の種類	リカバリの考え方	目標復旧時点（RPO）	目標復旧時間（RTO）	バックアップデータの保管先	バックアップ方式の説明	バックアップ頻度と世代数
①HDD障害時	(単独障害) ※HDD1本の故障 ・RAID構成により業務影響が発生しないこと。 ・ホットスペアにより自動的にRAID構成が再構築されること。 ・ホットスワップにより業務を停止することなくHDDの交換が行えること。	障害発生時点	障害発生時点	ディスク内に保管 ※稼働環境とは別の領域に保管すること	RAID5によるミラーリング	常時
	(多重障害) ※HDD2本以上の故障 ・RAIDグループを複数に分割にすることで、HDDの多重障害に対応する。 ただし、同一RAIDグループ内でHDDの多重障害が発生した場合には データの損失が発生する。	障害発生時点	障害発生時点	ディスク内に保管 ※稼働環境とは別の領域に保管すること	RAID5によるミラーリングと RAIDグループの細分化	常時
②ユーザ障害障害時 (ファイルの誤消去等、人為的なもの)	対応不要	–	–	–	–	–
③ディスク装置障害時	・ 障害部位の交換、HDD再装填、ディスク装置の環境再設定等による 対応が行えること。	障害発生時点	6時間以内	–	–	–
④データ障害時 (データベースファイル破損等)	・日次データバックアップからリカバリを行えること。 ※データバックアップの設定は設計・開発業者が行う ・データバックアップからのリカバリ後にアーカイブログ等から可能な限りデータの最新化 が行える様に考慮すること。(運用保守作業) ≪データバックアップ対象≫ ・CMSサーバ：CMS用データベース、コンテンツ更新履歴データ ・改ざん検知サーバ：コンテンツ(マスター) ・インタフェースサーバ：Oracleデータベース(全文検索インデックス含む)、添付文書	障害発生時点	6時間以内	オンラインストレージ上に保管 ※システム領域とは別の領域とすること	ディスク to ディスク	1回／日 (データバックアップ：3世代保管)
⑤システム障害時 （目標復旧時間：6時間以内）	・クラウドサービスが提供する機能でシステムバックアップが取得できること。 ・バックアップ用のオンラインストレージ上に格納されたシステムバックアップからシステムの リストアが行えること。 ・システムのリストア後に、データバックアップからデータの最新化を行う。(運用保守作業)	1週間以内	6時間以内	オンラインストレージ上に保管 ※システム領域とは別の領域とすること	ディスク to ディスク	システム更新時等随時 (システムのフルバックアップ：3世代保管)
⑥災害時 (データセンター被災や、 職員が半数以上出勤できない時)	・週次で遠隔地にあるリモートサイトにバックアップデータの保管が行えること。 ・データセンター復旧後にバックアップデータからシステムの復旧を行う。(運用保守作業)	1ヶ月以内	1週間以内の再開を目標	リモートサイト(遠隔地)のストレージ上に保管	遠隔地保管	1回／月 (バックアップデータのフルバックアップ：1世代保管) ※リモートサイトへのバックアップ中にメインサイトで障害が発生しても最新のバックアップデータには影響がないこと。
⑦広域災害時 (災害時＋遠隔地保管先も被災した時)	・保守資料(設計書等)からシステムの復旧(再構築)が行えること。	–	–	–	–	

※システム障害：クラウドサービスで提供される VPS 等に障害が発生し、サーバの復旧作業が必要となる障害（IaaS 障害は含まない）

（バックアップ概要）


メインサイト
オンラインストレージ（RAID5）
仮想サーバ
システム領域
データ領域
仮想サーバ
システム領域
データ領域
データバックアップ
1回／日
システム
バックアップ
システム更新時
随時
バックアップストレージ
最大3世代
システム
領域
データ
領域
DC間ネットワーク
（100Mbps）
自動退避
1回／月
遠隔地サイト
専用NAS領域
最新世代のみ
システム
領域
データ
領域

（４）　別添４：運用監視・保守方針と役割分担

作業区分	作業項目	作業内容	実施者		
			本調達業者	設計・開発業者	運用・保守業者
稼働業況管理	サービス管理	仮想サーバ、サービスの起動・停止・再起動のオペレータ作業サービスの提供	○	-	-
		仮想サーバ、サービスの起動・停止・再起動のオペレータ作業の実施	-	-	○
ストレージ管理	バックアップ	システムバックアップサービス、データバックアップ保管サービスの提供	○	-	-
		バックアップ設計・自動データバックアップ設定	-	○	-
		運用マニュアルに基づくデータおよびシステムイメージのバックアップの実施	-	-	○
		システムバックアップ管理票の作成、提供	-	-	○
	リストア	保守マニュアルに基づくデータ及びシステムイメージリストアの実施	-	-	○
		システムリストア管理票の作成、提供	-	-	○
ログ管理	ログチェック	ログ監視サービスの提供	○	-	-
		OSログ、ミドルウェアログの運用監視設定	-	○	-
		監視対象ログの確認	-	-	○
ユーザ管理	OS　ID管理	管理者・運用担当者のログインID、パスワードの発行	-	-	○
		管理者等の権限変更への対応	-	-	○
		管理者・運用担当者の登録情報変更への対応	-	-	○
問合わせ管理	照会対応	サービスデスク（IaaS監視、障害対応）を提供すること	○	-	-
セキュリティ管理	パッチ適用	セキュリティパッチ（OS）アップデート環境の提供	○	-	-
		事前検証サーバにおけるパッチ適用及び検証	-	-	○
		本番環境へのセキュリティパッチ（OS）の適用	-	-	○
		本番環境へのセキュリティパッチ（ミドルウェア）の適用	-	-	○
		パッチの適用状況管理	-	-	○
	ウイルスパターンファイル更新	パターンファイルの更新（自動）	○	-	-
		パターンファイルの更新状況管理	-	-	○
	侵入検知	外部からの侵入に対するセキュリティ監視	○	-	-
	ウイルス監視	ウイルス除去・検知に対する監視	○	-	-
稼働状況管理	死活監視	クラウドセンターに設置した仮想サーバ等を対象とした死活監視（Ping）	○	-	-
	閾値監視	CPU/メモリ/ディスクの閾値監視	○	-	-
		データーベースの空き容量監視	○	-	-
	サービス・プロセス稼働監視	サービス稼働監視（ポート番号単位）	○	-	-
		アプリケーション稼働上必要なプロセスの監視	○	-	-

※設計・開発業者は本調達業者を指す