（別紙）

仕様書

国立研究開発法人新エネルギー・産業技術総合開発機構

目次

別添 02_2_1：現行システムネットワーク構成
別添 02_2_2：現行機器構成管理情報一覧
別添 02_2_3：現行サーバFQDN名一覧
別添 02_2_4：移行先サービス構成図

1. 件名

日射量データベース、風況マップのクラウド基盤の移行及び運用保守等業務

2. 背景及び目的

日射量データベース、風況マップは、日射量及び風況の情報提供をオンライン上で実施するためにプライベートクラウド基盤上で稼働させてきたが、ハードウェアの老朽化等に伴いこれらのシステムに対して基盤の更改、移行等を行う必要がある。

そのため、アーキテクチャ設計、監視設計、構築、基盤テストを含む更改先「クラウド基盤の構築」、アーキテクチャ変更に伴うソースコード改修、システムテストを含む「日射量データベース、風況マップの移行」及び運用保守設計・テストを含む「クラウド基盤運用保守」を調達することを目的とする。

3. 用語の定義

本仕様書で使用する用語の定義を「表 3-1　用語の定義一覧」に示す。

表 3-1　用語の定義一覧

項番	用語	説明
1	NEDO	国立研究開発法人新エネルギー・産業技術総合開発機構を指す。
2	Azure 計画メンテナンス	Azure のインフラストラクチャーやサービスに対するセキュリティ強化、パフォーマンス向上、機能追加、バグ修正を定期的に行う機能のこと。
3	日射量データベース	今回、移行対象となる日射量データベースシステムとアジア日射量データベースシステムの2つのシステムのこと。
4	風況マップ	今回、移行対象となる風況マップシステムと洋上風況マップシステムの2つのシステムのこと。
5	プライベートクラウド	OS,MW はユーザの所有であり、ライセンス管理・更新等もユーザが実施。
6	パブリッククラウド	HW,OS,MW は、クラウドプロバイダーの所有であり、逐次更新される。
7	情報基盤サービス	発注者が利用しているクライアント PC、ネットワーク等を提供している PC-LAN サービスを指す。
8	マネージドサービス	スケーリング、リソース監視、冗長構成、バックアップ、セキュリティ、自動更新機能等を有するクラウドを構成するサービス。
9	X 社	本クラウド基盤に将来追加するシステムを担当する業者。

4. 業務の概要

業務の概要は以下のとおりとし、各年度の業務内容を「表 4-1　各年度業務内容」に示す。

(1)　クラウド基盤の構築：アーキテクチャ設計、監視設計、構築、基盤テスト

(2)　日射量データベース、風況マップの移行：ソースコード改修、システムテスト

(3)　クラウド基盤運用保守：運用保守設計、運用保守テスト、運用保守業務

表 4-1　各年度業務内容

項番	業務内容	2025 年度	2026 年度	2027 年度
1	クラウド基盤の構築	○	ー	-
2	日射量データベース、風況マップの移行	○	ー	-
3	クラウド基盤運用保守	○ （準備作業）	○ （運用保守）	○ （運用保守）

5. 履行期間及び履行期限

本業務全体の履行期間は、契約締結日から 2028 年 3 月 31 日（金）までとする。

（1） クラウド基盤の構築

履行期限：2026 年 3 月 31 日（火）

（2） 日射量データベース、風況マップの移行

履行期限：2026 年 3 月 31 日（火）

（3） クラウド基盤運用保守

準備作業の履行期限：2026 年 3 月 31 日（火）

運用保守の履行期間：2026 年 4 月 1 日（水）から 2028 年 3 月 31 日（金）まで

6. プロジェクト管理要件

（1） プロジェクト計画書の作成

受注者は、契約締結後発注者の 5 営業日以内にプロジェクト体制、作業内容及びスケジュール（Work Breakdown Structure。以下「WBS」という。）、工程ごとの成果物、開始終了基準等について記載した「プロジェクト計画書」（案）を作成し、発注者の了承を得ること。プロジェクト計画書（案）においては、プロジェクト責任者、品質管理責任者、各担当の役割、作業分担等を明記した体制図及びプロジェクトにおける情報セキュリティを維持するための体制の案を包含すること。また、工程管理を行うために、進捗管理方法、リスクを想定したうえでのリスク管理方法、品質管理方法、課題管理方法を含むこと。

プロジェクト計画書（案）の WBS には、今回の 3 つの業務を跨る工程間の依存関係とクリティカルパスを明記し、手戻り作業防止、品質向上、生産性向上に務めること。

発注者の了承を得たプロジェクト計画書は、受注者にて進捗管理・課題管理・レビュー実施管理等のプロジェクト管理の指標として用いるものとする。なお、プロジェクト進行中に計画の変更が生じた場合は、直ちにプロジェクト計画書を修正し、発注者の了承を得ること。

（2） 進捗管理

受注者は、各タスクの状況把握及びスケジュール管理を実施するため、以下の進捗管理を実施すること。

① WBS により作業工程ごとに必要な納入成果物、作業タスクを明確にすること。

② 業務の進捗状況を管理する進捗管理表及び各作業タスクの進捗状況等を定量的に分析した「進捗管理報告書」を定期的（週 1 回の頻度）に作成及び提出し、発注者の了承を得ること。

③ 計画から遅れが生じた場合は、原因を調査し、遅れを取り戻すための改善策を提示すること。

（3） 課題管理

受注者は、プロジェクト遂行にあたり発生した各種課題を管理するため、以下の課題管理を実施すること。

① 課題の内容、発生日、優先度、解決予定日、担当者、対応状況、対応策、対応結果及び解決日等の情報を一元管理した「課題管理表」を作成すること。

② 定期的（週 1 回の頻度）に対応状況を確認及び報告し、課題の経過状況を発注者と共有し、迅速な解決に取り組むこと。

(4) リスク管理

受注者は、プロジェクトの円滑な進行を阻害する内外のリスクを特定し、対応策の検討及び実施状況等を管理するため、リスク管理表を作成し、以下の要件を満たすリスク管理を実施すること。

① プロジェクトの遂行に影響を与えるリスクを特定し、その発生要因、発生可能性、影響度及びリスク軽減策を整理すること。

② 定期的にリスク監視及び評価を行い、その結果を発注者と共有することでリスクによる影響の把握に努めること。

③ リスクの発生に備え、緊急対応時の体制及び計画を整備すること。

(5) 品質管理

受注者は、システム移行における改修箇所の動作及び設計書等納入物の品質を保証するため、以下の要件を満たす品質管理を実施すること。

① 作業工程ごと、納入成果物ごとに品質評価基準等を設定し、評価結果を発注者に報告すること。

② 品質検証、品質改善策の検討及び品質管理体制を構築すると共に、品質改善のための各種取組が、事前に決められた手続きに則って実施されていることを的確に確認・報告すること。

(6) 変更管理

受注者は、設計書、移行実施手順書等の納入物の構成及び変更履歴を管理するため、以下の要件を満たす構成及び変更管理を実施すること。

① 各種設計書、ソースコード及び手順書等の変更の履歴を管理する構成管理対象を特定し、適切に管理すること。

② 変更履歴を管理するだけでなく、移行スクリプト等の構成管理対象は、プログラム変更によるデグレード(ソフトウェアのバージョンアップに伴う品質低下)対策のため、最新版や特定時点の版(不具合発生前の版等)を、いつでも提供できる仕組みを確立すること。

(7) コミュニケーション管理

受注者は、プロジェクトに関するすべての参画者が円滑かつ効率的なコミュニケーションを可能とするため、以下の要件を満たすコミュニケーション管理を実施すること。

① 作業工程ごとにおける各種作業に関する打ち合わせ及び納入物等のレビューのほか、進捗・課題等に関する報告のため定期的に会議及び報告会(以下「会議等」という。)を開催すること。開催方式は、対面、オンライン(MS Teams)又はハイブリッドのいずれかの方式で行うこと。対面で実施する際の会議室手配等に付帯する費用は受注者が負担すること。なお、発注者の会議室を利用することも可能であり、その場合は事前に希望を発注者へ申し出ること。

② 会議等については、会議等の内容、対象者及び開催頻度等を明確にすること。会議等の開催頻度等は、各作業工程の状況等を鑑みて、発注者と協議のうえ必要に応じて変更すること。

③ 会議等の開催後、発注者の 5 営業日以内に受注者にて「議事録」を作成し、発注者の了承を得ること。なお、課題事項や宿題事項については「議事録」の提出に先行し、会議等終了後ただちに共有すること。

(8) セキュリティ管理

受注者は、各作業工程におけるセキュリティに関する事故及び発生を未然に防ぐため、受注者の品質管理部門等の第三者又は外部機関によるセキュリティ監査が実施される場合、セキュリティ監査に協力すること。また、監査結果に対する改善や対策の実施状況について発注者に報告すること。

(9) 調整事項

受注者は、日射量データベース、風況マップの各システム及び情報基盤サービス等の発注者の請負先との調整が必要と判断した場合は、発注者にその旨を申し出ること。発注者は、受注者の申し出を受けて、他のシステム及びサービス等の開発請負先と受注者が打ち合わせを行う機会を設ける。なお、受注者は、当該打ち合わせに際し、資料等の作成について発注者より依頼があった場合はこれを引き受けること。

7. クラウド基盤の構築

クラウドコンピューティングサービスは、Microsoft Azure Cloud (Azure)とすること。

「クラウド基盤の構築」の業務内容は、現行 IaaS 構成から PaaS 構成への構成変更に伴うアプリログ監視、リソース(メトリック)監視、ネットワーク・セキュリティ設定、オートスケーリング設定、運用保守環境の整備等の調査、設計、構築を実施する。

なお、PaaS 化に伴い、現行のプライベートクラウド基盤で実施していた OS、アプリケーションサーバ、データベース、ログ収集ソフト、アンチウイルスソフト、完全性チェックソフト等のインストール、バージョンアップ、セキュリティーパッチ等のセットアップ作業、ライセンス更新作業が除外される。(現行の OS,M/W の構成については、「別添 02_2_1:現行システムネットワーク構成」「別添 02_2_2:現行機器構成管理情報一覧」参照)

7. 1 クラウド基盤の構築の要件

(1) Azure 権限ロールに関する要件

Azure の全体管理者(Global Administrator)を発注者とし、課金管理者(Billing Administrator)を受注者、日射量データベース、風況マップ用の管理サブスクリプション所有者及び DMZ サブスクリプション所有者を発注者と受注者とすること。

また、将来における他システム用サブスクリプション追加を想定すること。(サブスクリプションの配置については、「別添 02_2_4:移行先サービス構成図」参照)

なお、Azure 利用に係る費用については受注者の負担とし、受注者は課金管理者(Billing Administrator)として Azure への支払いを実施すること。

表 7-1 権限ロール一覧

項番	Azure 権限ロール	アカウント	備考
1	全体管理者(Global Administrator)	NEDO	サブスクリプション追加に必要な権限
2	課金管理者(Billing Administrator)	受注者	Azure への支払いを実施
3	管理サブスクリプション所有者	NEDO、受注者	クラウド基盤保守用
4	DMZ サブスクリプション所有者	NEDO、受注者	今回移行対象システム用
5	X-サブスクリプション所有者	NEDO、X 社	将来システムを追加した場合

(2) サービス構成に関する要件

受注者は、現在プライベートクラウドで稼働している発注者が保有する日射量データベース、風況マップの移行先となるクラウド基盤アーキテクチャの設計、構築を実施すること。

クラウド基盤へ移行するシステムを「表 7-2 移行システム一覧」に示す。

表 7-2 移行システム一覧

項番	システム名称	概要
1	日射量データベースシステム	太陽光発電等導入支援事業における国内日射量データを提供するシステム
2	アジア日射量データベースシステム	太陽光発電等導入支援事業におけるアジア日射量データを提供するシステム
3	風況マップシステム	風力発電等導入支援事業における局所風況マップデータを提供するシステム
4	洋上風況マップシステム	風力発電等導入支援事業における洋上風況マップデータを提供するシステム

現行プライベートクラウド基盤のサーバ構成は「別添 02_2_1:現行システムネットワーク構成」に示すとおり。

① 現行プライベートクラウド基盤は、アーキテクチャの層毎、機能毎に仮想サーバを配置しているが、移行先クラウド基盤では Azure の適切なマネージドサービス(WebApp サーバ、データベース、E-Mail 送信、監視、ウイルス検知、WAF)に置き換えること。

② 第三者製品サービスの利用は、Azure Marketplace に登録されているパートナーサービスに限ること。

③ プレビュー版(試行版)のサービス及びオプションは、移行対象システムの稼働において利用しないこと。

④ 現行プライベートクラウド基盤の仮想サーバで稼働している Web アプリケーション、EJB アプリケーション及び CGI は、PaaS 化を前提とした Azure のマネージドサービスに移行すること。ただし、調査・検証した結果、困難であると判明した時は、速やかに発注者へ報告し仮想サーバ(Azure Virtual Machines)を利用した一部 IaaS 構成の移行に切り替えること。この時、Azure Monitor Agent をインストールし、アプリログ、アクセスログ、システムログ及びリソースログを Azure Monitor にて一括監視できるようにすること。また、アンチウイルス、完全性チェック等のツールをインストールするか、もしくは Microsoft Defender for Servers を導入すること。

⑤ 保守用仮想端末を配置し、そこから各マネージドサービスへロードモジュールをデプロイできるようにすること。

⑥ 保守用仮想端末には、ソース管理、ビルド、障害調査のためのデバッグ実行、負荷試験等を実施できる環境を整備すること。その際必要となる SCM、IDE、負荷試験ツール等第三者製品のツール類は、本調達に含めること。また、受注者がバージョンアップ等随時判断し実施し、管理すること。

⑦ 保守用仮想端末は、MFA(多要素認証)及び NSG(IP フィルタリング)を利用しアクセス制限を実施すること。

⑧ 移行対象となる日射量データベース/アジア日射量データベース、風況マップシステム/洋上風況マップシステムを稼働する上で必要となる共通のマネージドサービス・リソース(監視、ログ蓄積、E-Mail 送信等)は、共用すること。Web アプリケーション、CGI の実装に Azure App Service を利用する場合、Azure App Service Plan を共用できるか検討すること。ログ蓄積における Azure Monitor Log Analytics

は、全システムにおいて共用すること。

(3) リソース要件

Azure の各マネージドサービスは、下記事項を考慮しスペックを決めること。

現行プライベートクラウド基盤の各サーバのスペックは「別添 02_2_2:現行機器構成管理情報一覧」に示すとおり。

① 規模に関する事項

日射量データベースシステム/アジア日射量データベースシステム、風況マップシステム/洋上風況マップシステムの想定する負荷は下記のとおり。

表 7-3 想定負荷一覧

項番	システム名称	リクエスト数/日	ピーク時同時リクエスト数	ダウンロードサイズ	静的データサイズ
1	日射量データベースシステム	100	10	800KB	15 GB
2	アジア日射量データベースシステム	100	10	6KB	400 MB
3	風況マップシステム	100	10	200KB	300 GB
4	洋上風況マップシステム	100	10	1,000KB	3 TB

② 性能に関する事項

リクエストレスポンス性能は、現行プライベートクラウド基盤環境と同等以上とすること。

NEDOイントラネット環境にて下記レスポンスタイムを基準値とする。

表 7-4 性能基準値一覧

項番	リクエストタイプ	通常時	ピーク時
1	単純なクエリ(ログイン)	平均 3 秒	平均 5 秒
2	複雑なクエリ(検索)	平均 5 秒	平均 8 秒
3	アップロード	平均 10Mbps	平均 5Mbps
4	ダウンロード	平均 50Mbps	平均 25Mbps

③ 可用性に関する事項

システム稼働時間は、24 時間 365 日とすること。

使用する各マネージドサービスは、Service Level Agreement(SLA)99.9%以上のサービスまたは冗長構成を選択すること。(トータルではなくプレゼンテーション層、アプリケーション層、データベース層個々の SLA を指す。)

また、使用する各マネージドサービスの冗長化レベルは、デフォルト値(ローカル冗長・ゾーン冗長)を選択すること。

④ 政府の設計・開発ガイドラインに関する事項

使用する各サービスの作成場所は、日本国リージョン(East Japan)を選択すること。

ネットワークの迂回路等日本国以外のリージョンに生成されたリソースはリストアップし、発注者へ報告すること。

(4) ネットワーク・セキュリティ要件

以下の要件を満たすネットワーク設計及びセキュリティ設計を実施すること。

現行プライベートクラウド基盤のネットワーク構成は「別添 02_2_1：現行システムネットワーク構成」に、セキュリティ対策ツールの導入状況は「別添 02_2_2：現行機器構成管理情報一覧」に、FDQN 構成については「別添 02_2_3：現行サーバFQDN名一覧」に示すとおり。

① 現行プライベートクラウド基盤において提供されているセキュリティ対策（ウイルスチェック、完全性チェック）と同等の構成とすること。
ウイルスチェックについては、Microsoft Defender for Cloud を使用すること。
参照専用データについては、Azure Blob Storage の MD5 チェックサム及び不変ストレージ(Immutability Policy)を使用すること。

② 現行プライベートクラウド基盤において DMZ セグメントに配置されているサービスについては、Application Gateway WAF2 経由で接続すること。
マネージドサービス間の接続については、上位層のサービスに限定し SSL 接続及び Entra ID 発行のプリンシパルキーを用いた接続を実施すること。

③ 現行プライベートクラウド基盤において内部セグメント・管理者セグメントに配置されているサービスについては、Application Gateway Network Security Groups(IP フィルタリング)設定にて情報基盤サービスの IP レンジからアクセスに制限すること。

④ 移行先の各システムの FDQN 名を Application Gateway に設定し移行すること。
現行のシステムの DNS サーバの設定削除と共に切り替え時に実施すること。
現行のシステムの DNS サーバの設定削除は発注者経由にて情報基盤サービスへ申請すること。
また、情報基盤サービス担当と協議し、必要ならば DNS 委任の申請を実施すること。

(5) システム監視要件

下記要件を満たす監視設計を実施すること。

① 各マネージドサービスのリソース状況(CPU 使用量、メモリ使用量、ディスク使用量、リクエスト/レスポンスタイム等)を監視・通知ができること。
設定間隔でチェックし設定期間に設定回数、設定閾値を超えた場合、リソースエラーと判定すること。
各リソースの使用状況を示すグラフと主要アプリケーションのログを Azure Portal のダッシュボードに表示すること。

② 各システムの死活監視・通知ができること。
Azure のマネージドサービスにて、死活監視設定を備えている場合は、有効化すること。
設定した間隔で各サービスの URL に応答がない場合、エラーと判定すること。

③ 各システムのアプリケーションログを監視し、エラー、警告、Debug、Info を検知し通知ができること。

④ ウイルス監視・通知ができること。

⑤ 各マネージドサービスのセキュリティ設定の変更（脆弱化）を検知できること。（アカウントの乗っ取りを想定し正規アカウントで変更した場合も検知できること。）

⑥ 監視からの通知先をエラー、警告、Debug、Info レベル毎に設定できること。

⑦ 監視ログの保存期間は、1 年間とする。

(6) バックアップ要件

バックアップは PaaS 化した各マネージドサービスの Default の冗長構成を選択することにより実現する。
バックアップ間隔、保持期間についても Default 冗長構成の Default 値とする。
Default の冗長構成がない場合、LRS(Local Redundant Storage) 冗長構成を本クラウド基盤の基本とする。

(7) クラウド基盤テスト要件

受注者は構築した基盤が下記要件を満たすか、障害時に想定とおりの動作となるかについてテストを実施すること。

① 正常系テスト
上位層下位層のマネージドサービス間の接続確認。

② 異常系テスト
上位層下位層のマネージドサービス停止時のエラー処理確認。
上位層下位層のマネージドサービス再起動時の自動再接続を確認。
マネージドサービス冗長構成パックアップからの復元を確認。

③ 負荷テスト
ピーク時想定の同時リクエスト数の確認。
高負荷時を想定したスケールアップ、スケールアウトが機能することの確認。

④ 監視テスト
各マネージドサービスのリソースログが Azure Monitor Log Analytics へ転送されていることの確認。
各アプリケーションログが Azure Monitor Log Analytics へ転送されていることの確認。
マネージドサービスの死活監視機能が動作していることの確認。

⑤ アプリケーションのリリース・切り戻しテスト
各システムの新バージョンのロードモジュールを保守端末からビルドし、リリース(Deploy)できること。
前のバージョンへロードモジュールを切り戻せること。

7. 2 クラウド基盤の構築に係る作業

受注者は、クラウド基盤の構築業務に際し、6. (1)の「プロジェクト計画書」に以下の項目を WBS として盛り込むこと。

(1) クラウド基盤設計

受注者は、移行対象システムを調査した上で「7. 1 クラウド基盤の構築の要件」に沿ったアーキテクチャ設計・監視設計を実施し、成果物として「クラウド基盤基本設計書」及び「クラウド基盤詳細設計書」を作成し、発注者の了承を得ること。
なお、設計に際しては、政府の設計・開発ガイドライン等に準拠して実施すること。
また、「クラウド基盤詳細設計書」には、構築時に設定するマネージドサービスのパラメータが記載されていること。

(2) クラウド基盤構築

受注者は、「クラウド基盤基本設計書」及び「クラウド基盤詳細設計書」に基づきクラウド基盤を構築すること。

(3) クラウド基盤テスト

① 受注者は、「クラウド基盤基本設計書」及び「クラウド基盤詳細設計書」に基づき「クラウド基盤テスト仕様書」を作成し、発注者の了承を得ること。

② 受注者は、「クラウド基盤テスト仕様書」に基づきテストを実施し、「クラウド基盤テスト成績書」を作成し、発注者の了承を得ること。

③ 受注者は、クラウド基盤構築が完了した場合は、「クラウド基盤構築完了報告書」を作成し、発注者に提出すること。

8. 日射量データベース、風況マップの移行

「日射量データベース、風況マップの移行」の業務内容は、現行 IaaS 構成から PaaS 構成への構成変更に伴うプログラム改修とそのリリース作業とする。

プログラム改修は、以下 2 項目とする。

① Web アプリとデータを Azure マネージドサービスで稼働させるため、Web アプリ層とデータ層を分離する。

② アプリケーション毎に個々のルールで出力していたアプリログをクラウド基盤のアプリ監視機能のルールに則った出力形式、タイミング（1インシデント1行）に改修する。

なお、プログラム改修作業において、発注者から受注者へソースコード一式及び現行システムのロードモジュールのバックアップ、現行システムのロードモジュールのリリース手順を提供する。

8．1 日射量データベース、風況マップの移行の要件

(1) 日射量データベースシステム/アジア日射量データベースシステム移行要件

表 8-1 現行日射量データベースシステム/アジア日射量データベースシステム技術要素

システム名	分類	静的データ	開発言語	ステップ数	備考
日射量データベースシステム	Web アプリ	CSV,TXT,JPG	HTML,Perl,JavaScript	3.1K	CGI
アジア日射量データベースシステム	Web アプリ	CSV,TXT,JPG	HTML,Perl,JavaScript	1.6K	CGI

現行日射量データベースシステム/アジア日射量データベースシステムは、「表 8-1 現行日射量データベースシステム/アジア日射量データベースシステム技術要素」のとおり仮想サーバ上に実装されている（「別添 02_2_1：現行システムネットワーク構成」参照）。

今回、Azure のマネージドサービスへ乗せ換えるにあたって、PaaS 化を前提とし次の作業を実施する（「別添 02_2_4：移行先サービス構成図」参照）。

① OS 更新（PaaS 化可能の場合不要）

Web アプリを調査・検証し PaaS 化に問題がなければ Azure App Service を利用する。また、日射量データベースシステムとアジア日射量データベースシステムでApp Service Plan を共用し、OS は Perl CGI を稼働するため Windows を選択する。

現行とおり仮想サーバを使用すると判断した場合、OS のバージョンを更新する。また、セキュリティーパッチの更新等を運用保守の中で実施する。

② 静的コンテンツの File Path の変更
現行システムでは、Document Root より相対 Path でデータにアクセスしているが、今回、静的コンテンツ(データ)を Azure Blob Storage に格納するため、フロントのサービスから Azure Blob Storage 上のデータにアクセスするよう改修する。

③ 静的コンテンツ(データ)の登録方法
静的コンテンツ(データ)の Azure Blob Storage への初期登録については、物理的な専用デバイスを活用する Azure Data Box を利用する。

④ 静的コンテンツ(データ)の完全性チェック方法
静的コンテンツ(データ)を格納する Azure Blob Storage の完全性チェックには、不変ストレージ(Immutability Policy)の設定を利用する。また、データのみの更新を想定し、保持期間を 1 カ月とし、運用保守の中で 1 カ月毎に期間を更新する。

⑤ CGI 設定の変更
Azure App Service で Perl の CGI を動作させるための記述を Web.config ファイルに設定する。

(2) 風況マップシステム/洋上風況マップシステム移行要件

表 8-2 現行風況マップ/洋上風況マップ技術要素

システム名	分類	静的データ	開発言語	ステップ数	備考
風況マップシステム	Web アプリ	CSV,TXT,JPG	JavaJSP/Servlet	4.6K	
洋上風況マップシステム	Web アプリ	CSV,TXT,JPG	HTML,PHP,JavaScript	16.5K	PHP7→8,Java

現行風況マップシステム/洋上風況マップシステムは、「表 8-2 現行風況マップシステム/洋上風況マップシステム技術要素」のとおり仮想サーバ上に実装されている(「別添 02_2_1:現行システムネットワーク構成」参照)。今回、Azure のマネージドサービスへ乗せ換えるにあたって、PaaS 化を前提とし次の作業を実施する(「別添 02_2_4:移行先サービス構成図」参照)。

① OS 更新(PaaS 化可能の場合不要)
Web アプリを調査・検証し PaaS 化に問題がなければ Azure App Service を利用する。また、風況マップシステムと洋上風況マップシステムでApp Service Plan を共用し、OS は Tomcat ランタイムで稼働するため Linux を選択する。
現行とおり仮想サーバを使用すると判断した場合、OS のバージョンを更新する。また、セキュリティーパッチの更新等を運用保守の中で実施する。

② 静的コンテンツ(データ)の File Path の変更
現行システムでは、Document Root より相対 Path でデータにアクセスしているが、今回、静的コンテンツ(データ)を Azure Blob Storage に格納するため、フロントのサービスから Azure Blob Storage 上の

データにアクセスするよう改修する。

③ 静的コンテンツ(データ)の登録方法

静的コンテンツ(データ)の Azure Blob Storage への初期登録については、物理的な専用デバイスを活用する Azure Data Box を利用する。

④ 静的コンテンツ(データ)の完全性チェック方法

静的コンテンツ(データ)を格納する Azure Blob Storage の完全性チェックには、不変ストレージ(Immutability Policy)の設定を利用する。また、データのみの更新を想定し、保持期間を 1 カ月とし、運用保守の中で 1 カ月毎に期間を更新する。

⑤ PHP ソースコード移行

PHP ソースコードの用途等調査・検証し、機能的に問題なければ Java へ移行する。

PHP ソースコードを引き続き使用する場合、現行の PHP7．0は 2018 年 12 月 3 日にセキュリティサポートを終了しており、Azure App Service の PHP ランタイムを使用するためにも 8.1～8.3 へのバージョンアップを実施する。

8．2 日射量データベース、風況マップの移行に係る作業

受注者は、日射量データベース、風況マップの移行業務に際し、6.(1)の「プロジェクト計画書」に以下の項目を WBS として盛り込むこと。

(1) 移行対象システム変更設計

受注者は、8.1 の要件を満たす「移行対象システム変更仕様書」を作成し、発注者の了承を得ること。

なお、設計に際しては、政府の設計・開発ガイドライン等に準拠して実施すること。

また、単体設計書は納品物に含まない。

(2) 移行対象システムプログラム改修

受注者は、「移行対象システム変更仕様書」に基づき移行対象システムのプログラム改修を実施すること。

なお、単体テスト及び成績書は納品物に含まないが、エビデンスを残すこと。

また、ソースコードの変更履歴をクラウド基盤上に構築した保守環境の SCM（Git）ツールにて記録すること。

(3) 移行対象システムテスト

① 受注者は、「移行対象システム変更仕様書」に基づき「移行対象システムテスト仕様書」を作成し、発注者の了承を得ること。

② 受注者は、「移行対象システムテスト仕様書」に基づきテストを実施し、「移行対象システムテスト成績書」を作成し、発注者の了承を得ること。

③ 受注者は、「移行対象システムソースコード一式」を発注者へ納品すること。

(4) 移行対象システム移行

① 受注者は、「システム移行実施計画書」及び「システム移行実施手順書」を作成し、発注者の了承を得ること。

なお、移行に際し発注者と調整し、受注者が主体となり現行プライベートクラウド運用保守業者や情報基盤サービス運用保守業者と連携し「システム移行実施計画書」を作成すること。

② 受注者は、「システム移行実施計画書」及び「システム移行実施手順書」に基づいて日射量データベース、風況マップの移行を実施すること。移行は、2026 年 2 月 27 日（金）までに完了させること。

③　受注者は、移行実施結果の「システム移行実施報告書」を作成し、発注者の了承を得ること。

9.　クラウド基盤運用保守

「クラウド基盤運用保守」の業務内容は、今回構築したクラウド基盤のアプリログ監視、リソース監視、セキュリティ監視にて異常を検知した際の受付・窓口業務と対処、クラウド基盤自体のリソース（メトリック）の状態、Azure 計画メンテナンスの予定実績、クラウド基盤で稼働している各システムの稼働状況の月次報告とする。また、これらの運用保守設計、運用保守テスト、及び運用保守設計の随時見直しを業務範囲とする。なお、クラウド基盤で稼働している各システムの機能自体に関する不具合については、解決に向けた支援作業は別途調整とする。

9．1 クラウド基盤運用保守の要件

(1)　クラウド基盤運用保守範囲

本調達におけるクラウド基盤運用保守範囲は以下のとおり。

①　クラウド基盤運用保守

②　日射量データベース、風況マップ運用保守支援（受付・窓口業務のみ）

(2)　サービスレベル

クラウド基盤運用保守におけるサービスレベルは以下のとおり。

クラウド基盤運用保守期間中は、サービスレベルを計測できるよう、監視環境、手順等を整備し、月に 1 度「サービスレベル達成状況報告書」を作成し、発注者に報告すること。なお、報告はクラウド基盤運用保守月次報告と同報でもよいこととする。

①　監視サービス稼働率：99.9%以上。ただし、計画メンテナンスの時間は停止時間に含めない。計画停止する場合は、事前に発注者へ連絡すること。

②　障害発生時の発注者への連絡：20 分以内。アラートによる場合はアラートの発報時間を、運用保守要員による発見又は発注者からの連絡の場合は、発見時又は連絡時からとする。

③　目標復旧時間：4 時間以内(リソース等クラウド基盤に関する障害)、目標復旧時点：各マネージドサービスの提供する最短復旧ポイント

(3)　問い合わせ対応

発注者からの問い合わせに対応すること。

問い合わせ窓口は原則 E-Mail とするが、障害発生時等の緊急対応用の連絡先を提示すること。

E-Mail の受付は 24 時間 365 日とするが、回答は土曜日、日曜日、国民の祝日及び年末年始（12 月 29 日から 1 月 3 日）を除いた 9 時から 17 時に対応することとし、回答時間外の受付は翌営業日に対応すること。

問い合わせ事項の管理として、問い合わせ内容の分類、ワークフロー、進捗ステータス等を定義すること。

また、システム毎のアクセス数の集計、平均レスポンスタイムの算出、CPU 使用率閾値オーバー回数のカウント等を考慮すること。

(4) 予防保守

クラウド基盤の利用状況等から、リソース割り当ての変更等について月次報告書で翌月の提案を行うこと。提案又は発注者からの指示を受け、リソース割り当ての変更等について作業を実施すること。

作業の際は、作業担当者、チェック状況、タイムスケジュール、切り戻しタイミング等が分かる作業計画書を作成し、発注者の了承を得ること。また、作業完了後には作業実績を報告すること。

予防保守として、次の項目を定期的に確認すること。

リソースの過不足、アクセス状況、Azure の正常性（メンテナンス実績、予定）、Azure Entra ID セキュリティスコア（各サービスの設定、危険なユーザ）など。また、レスポンス性能の低下など発生時に必要に応じて各サービスの「問題の診断と解決」を実施すること。

(5) 障害対応

障害対応として、障害の重要度の分類や考え方について、障害の切り分け方法、報告ルート・手順、解決までのワークフロー、進捗ステータスを定義しクラウド基盤運用保守手順書に明記すること。発注者への報告タイミング、報告内容等は、障害の分類、重要度等により変更する場合は、クラウド基盤運用保守手順書へ明記し、発注者の了承を得ること。

障害発生時はクラウド基盤運用保守手順書に従って発注者へ連絡し、速やかに復旧に努めること。また、障害内容について、障害報告書を作成すること。障害内容により即時恒久対策が難しい場合は、初版、第 2 版、最終版と複数版提出することで、発注者への状況提供を随時行うこと。

また、障害解析・再現性の確認のためのログ及びデータの保存、復旧手順を記載すること。

(6) システムの操作・監視等

クラウドサービス等の運用管理ツール等を用いて、システムの操作・監視等を実施すること。ウイルス感染等のセキュリティインシデントや障害等の検知方法、報告手順、監視体制とエスカレーション手順・方法についても示すこと。

(7) データ管理

「7．1(6)バックアップ要件」で用意されたバックアップ及びリストア方式を基にして必要なバックアップ・リストアの運用手順等を整備して運用を行うこと。また定期的な訓練を行うこと。

(8) 報告書の作成等

受注者は、以下の報告書を作成し、発注者に報告すること。なお、報告内容については発注者と調整すること。

① 月次報告書

月に 1 度、サービスの稼働実績、運用保守状況、翌月のリソース管理の提案等の内容を含む月次報告書を作成し、発注者に報告すること。

② 障害報告書

障害発生時に障害報告書を作成し、発注者に報告すること。

③ 年度末報告書

年に 1 度、月毎のサービス稼働実績、リソース使用状況、障害発生件数などをまとめた年度末中間報告書を作成し、発注者に報告すること。

(9) セキュリティ監査対応支援

受注者は、クラウド基盤に関するセキュリティ監査（Web アプリケーション診断及び NISC システム監査）において、発注者から以下に示す指示があった場合はそれぞれ対応を行うこと。Web アプリケーション診断については年に 1 回、NISC システム監査については 3 年に 1 回（変動あり）で行われる。

① 監査人によるヒアリング対応及び資料提示
② 監査人が監査に使用する ID の割り当て及び監査実施後のその無効化
③ 監査人が実施する監査作業に必要なシステムの設定変更及び監査実施後のその復旧
④ その他、セキュリティ監査対応として発注者から指示した内容に対する対応

対応について受注者が必要とする場合には、発注者と別途協議するものとする。

９．２ クラウド基盤運用保守に係る作業

受注者は、クラウド基盤運用保守業務に際し、6.(1)のプロジェクト計画書に以下の項目を WBS として盛り込むこと。

(1) クラウド基盤運用保守設計

受注者は、「クラウド基盤基本設計書」に基づき、クラウド基盤運用保守の「運用性」「保守性」「変更要請」を考慮し、移行対象システムのログフォーマット、ログ出力タイミングやクラウド基盤のログ監視ルール等について各担当と連携し、「クラウド基盤運用保守設計書」を作成し、発注者の了承を得ること。

(2) クラウド基盤運用保守手順書の作成

クラウド基盤運用保守を実施するための作業フロー、手順、要領等を記載した「クラウド基盤運用保守手順書」を作成し、発注者へ提出すること。クラウド基盤運用保守手順書は、運用状況に応じて見直しを行い、発注者の了承を得たうえで変更を行うこと。

また、「クラウド基盤運用手順書」には、監視機能や各システムの起動停止方法、リソースログ・アプリログ・アクティビティログの参照方法・保存期間等の情報を含めること。

(3) クラウド基盤運用保守テスト

① 受注者は、「クラウド基盤運用保守設計書」「クラウド基盤運用保手順書」に基づいて、シナリオを作成し、「クラウド基盤運用保守テスト仕様書」を作成し、発注者の了承を得ること。
② 受注者は、「クラウド基盤運用保守テスト仕様書」に基づきクラウド基盤運用保守テストを実施し、「クラウド基盤運用保守テスト成績書」を作成し、発注者の了承を得ること。クラウド基盤運用保守テスト実施後から 2026 年 3 月 31 日（火）までは、現行システム環境と並行稼働を行うこと。なお、移行対象の各システムのデプロイ作業は、クラウド基盤上に構築した保守環境から実施すること。
③ 受注者は、クラウド基盤運用保守準備作業が完了した場合は、「クラウド基盤運用保守準備作業完了報告書」を作成し、発注者に提出すること。

(4) クラウド基盤運用保守障害・月次報告

受注者は、「クラウド基盤運用保守手順書」に基づいて、業務を遂行し、9.1(2)の「サービスレベル達成状況報告書」、9.1(8)の「月次報告書」「障害報告書」を作成し、発注者へ報告をすること。

「サービスレベル達成状況報告書」「月次報告書」は月次報告とし、「障害報告書」は障害発生時報告とする。なお、「サービスレベル達成状況報告書」「月次報告書」「障害報告書」のフォーマットについては、クラウド基盤運用保守開始前に作成し、発注者の了承を得ること。

(5) クラウド基盤保守運用年度末報告書の作成

受注者は、年に 1 度、月毎のサービス稼働実績、リソース使用状況、障害発生件数などをまとめた 9.1.(8)の「年度末中間報告書」を作成し、発注者へ報告すること。

10. 納入成果物等

(1) 納入成果物

納入成果物、記載箇所及び納入期限を「表 10-1 納入成果物一覧」に示す。

表 10-1 納入成果物一覧

項番	納入成果物名	記載箇所	納入期限
1	プロジェクト計画書	6.(1)、7.2、8.2、9.2	(案)を契約締結後発注者の 5 営業日以内
2	進捗管理報告書	6.(2)②	週 1 回
3	課題管理表	6.(3)①	
4	クラウド基盤基本設計書	7.2(1)	2026 年 3 月 31 日(火)
5	クラウド基盤詳細設計書	7.2(1)	
6	クラウド基盤テスト仕様書	7.2(3)①	
7	クラウド基盤テスト成績書	7.2(3)②	
8	クラウド基盤構築完了報告書	7.2(3)③	
9	移行対象システム変更仕様書	8.2(1)	
10	移行対象システムテスト仕様書	8.2(3)①	
11	移行対象システムテスト成績書	8.2(3)②	
12	移行対象システムソースコード一式	8.2(3)③	
13	システム移行実施計画書	8.2(4)①	
14	システム移行実施手順書	8.2(4)①	
15	システム移行実施報告書	8.2(4)③	
16	クラウド基盤運用保守設計書	9.2(1)	
17	クラウド基盤運用保守手順書	9.2(2)	
18	クラウド基盤運用保守テスト仕様書	9.2(3)①	
19	クラウド基盤運用保守テスト成績書	9.2(3)②	
20	クラウド基盤運用保守準備作業完了報告書	9.2(3)③	
21	サービスレベル達成状況報告書	9.1(2)	前月分を発注者の翌第5営業日 ただし、3 月分は 3 月 31 日
22	月次報告書	9.1(8)①	
23	障害報告書	9.1(8)②	発生の都度
24	年度末報告書	9.1(8)③	2026 年度分:2027 年 3 月 31 日

			（水） 2027 年度分:2028 年 3 月 31 日（金）
25	議事録	6.(7)③	会議後発注者の 5 営業日以内

(2) 納入方法

① 納入成果物はすべて日本語で作成すること。ただし、固有名詞及び英字で表記されることが一般的な文言については、そのまま記載しても構わないものとする。

② 情報処理に関する用語の表記については、日本作業規格（JIS）の既定に準拠すること。

③ 受注者は「項番 1 から項番 20」を電子媒体で納入すること。電子媒体に保存する形式は、Adobe PDF 又は Microsoft Office365 で扱える形式とすること。

④ 「項番 21 から 25」については、電子媒体を発注者に提出し、さらに各年度最終営業日に全提出物を格納した電子媒体を納入すること。

⑤ 納入成果物は、納入後に発注者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入すること。

⑥ 電子媒体での納入に際しては、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、納入成果物に不正プログラムが混入することがないよう適切に対処すること。

⑦ 納入成果物の作成及び納入にあたり、内容及び構成等について発注者が指摘した場合には、指摘事項に対応すること。

(3) 納入場所

〒212-8554
神奈川県川崎市幸区大宮町 1310 ミューザ川崎セントラルタワー
国立研究開発法人新エネルギー・産業技術総合開発機構 再生可能エネルギー部

11. 知的財産権の帰属等

(1) 本業務の作業により作成する納入成果物等に関し、著作権法（昭和 45 年法律第 48 号）第 21 条、第 23 条、第 26 条の 3、第 27 条及び第 28 条に定める権利を含む全ての著作権は発注者に帰属するものとする。なお、受注者は発注者に対し、一切の著作者人格権を行使しないものとし、第三者をして行使させないものとする。また、受注者は本調達の納入成果物に係る著作物を自ら使用し、又は第三者として使用させる場合は、発注者と別途協議し、発注者の許可を得るものとする。

(2) 納入成果物に第三者が権利を有する著作物が含まれているときは、発注者が特に使用を指示した場合を除き、受注者は当該著作物の使用に関して費用の負担を含む一切の手続きを行うものとする。

(3) 本調達の作業に関し、第三者との間で著作権に係る権利侵害の紛争等が生じた場合、当該紛争の原因が専ら発注者の責めに帰す場合を除き、受注者は自らの負担と責任において適切に処理するものとする。

12. サプライチェーン・リスク対応要件

本業務のサプライチェーン・リスク対応要件を以下に示す。

(1) 受注者は、システムを構成する候補となる機器等について、あらかじめ発注者に一覧を記載したリストを提出し、発注者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、代替品選定やリスク低減対策等、発注者と迅速かつ密接に連携し提案の見直しを図ること。機器等の構成を変更する場合も同じ。

(2) 受注者は、資本関係・役員の情報、本業務の実施場所、本業務の従事者の所属・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を提示すること。履行期間中に従事者を変更する場合は、事前に発注者へ連絡し、了承を得ること。

(3) 受注者は、システムを構成する要素(機器等)に対して、不正な変更があった場合に識別できる構成管理体制を確立していること。また、当該構成管理体制が書類等で確認できること。

(4) 受注者がシステムを構成する要素として採用した機器等について、不正な変更が加えられていないことを検査する体制が受注者において確立していること。また、当該検査体制が書類等で確認できること。

(5) システムの提供、運用保守の各工程において、発注者の意図しない変更や機密情報の窃取等が行われていないことを保証する管理が、一貫した品質保証体制のもとでなされていること。また、具体的な管理手順や品質保証体制を証明する書類(例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図)を提出すること。第三者機関による品質保証体制を保証する書類等が提出可能な場合は提出すること。

(6) 現行システムに発注者の意図しない変更が行われる等の不正が見つかったときに、追跡調査や立ち入り調査等発注者と連携して原因を調査し、排除するための手順及び体制(例えば、運用保守業務におけるシステム操作ログや作業履歴等を記録し、発注者から要求された場合には提出させるようにする等)を整備していること。また、当該手順及び体制が妥当であることを証明するための書類を提出すること。

(7) 受注者は、本契約の履行について、請負業務の全部又は一部(主体的部分)を第三者に委任し、又は請け負わせてはならない。ただし、請負業務の一部(主体的部分)であって、あらかじめ発注者の承認を得た場合は、この限りではない。発注者の承認を得た場合には、受注者は発注者との契約上受注者に求められる水準と同等の情報セキュリティを請負業務の一部(主体的部分以外を含む。)を委任し、又は請け負わせた第三者(以下「下請負人」という。)においても確保すること。また、受注者は下請負人が実施する情報セキュリティ対策及びその実施状況について、発注者に報告すること。

(8) 本業務において取り扱う情報について、下請負人が閲覧することが無いように、受注者は情報を厳重に管理すること。やむを得ず下請負において業務に係る情報を開示する必要がある場合には、受注者は事前に発注者と調整し、発注者の指示に従うこと。

(9) 受注者は、下請負人における本業務の従事者の所属、専門性(資格等)、実績及び国籍に関する情報を提示すること。履行期間中に従事者を変更する場合は、事前に発注者へ連絡し、許可(又は確認)を得ること。

13. 情報管理体制

受注者は、情報管理体制に係る以下の規定を順守すること。

(1) 受注者は、本業務で知り得た情報を適切に管理するため、次の履行体制を確保し、発注者に対し「情報取扱者名簿」(指名、所属、役職、国籍等が記載されたもの)及び「情報管理体制図」(情報セキュリティを確保するための体制を定めた書面)を契約前に提出し、発注者の同意を得ること。また、本業務の情報

取扱者の個人住所、生年月日、パスポート番号を発注者から求められた場合は、速やかに提出すること。なお、情報取扱者は、本業務の遂行のために最低限必要な範囲で設定すること。

(2) 契約を履行する一環として受注者が収集、整理、作成等を行った一切の情報が、発注者が保護を要さないと確認するまでは、情報取扱者名簿に記載がある者以外に伝達又は漏えいされないことを保証する履行体制を有していること。

(3) 本業務で知り得た一切の情報について、情報取扱者以外の者に開示又は漏えいしてはならない。ただし、発注者の承認を得た場合はこの限りではない。

(4) (1)の情報セキュリティを確保するための体制を定めた書面又は情報取扱者名簿に変更がある場合は、あらかじめ発注者に提出し、同意を得ること。

(5) 発注者が提供した資料又は発注者が指定した資料の取扱い(返却・削除等)については、発注者の指示に従うこと。

14. 機密保持

(1) 受注者は、本業務に係る作業を実施するにあたり、発注者から取得した情報(電子媒体、文書、図面等の形態を問わない。)を含め契約上知り得た情報を、第三者に開示又は本業務に係る作業以外の目的で利用しないものとする。ただし、次の①から⑤のいずれかに該当する情報は除くものとする。

① 発注者から取得した時点で、既に公知であるもの

② 発注者から取得後、受注者の責によらず公知となったもの

③ 法令等に基づき開示されるもの

④ 発注者から秘密でないと指定されたもの

⑤ 第三者への開示又は本業務に係る作業以外の目的で利用することについて、事前に発注者と協議の上、承認されたもの

(2) 受注者は、発注者の許可なく、取り扱う情報を指定された場所から持ち出し、又は複製しないものとする。

(3) 受注者は、本業務に係る作業に関与した受注者の所属職員が異動した後においても、機密が保持される措置を講じるものとする。

(4) 受注者は、本業務に係る検収後、受注者の事業所内部に保管されている本業務に係る発注者に関する情報を、裁断等の物理的破壊、消磁その他復元不可能な方法により速やかに抹消するとともに、発注者から貸与されたものについては、契約終了後発注者の 5 営業日以内に発注者に返却するものとする。

15. 情報セキュリティに関する受注者の責任

(1) 情報セキュリティを確保するための体制の整備

受注者は、受注者組織全体の情報セキュリティを確保するとともに、発注者から求められた本業務の実施において情報セキュリティを確保するための体制を整備すること。

(2) 情報セキュリティが侵害された場合の対処

本業務の遂行において、定期的に情報セキュリティ対策の履行状況を報告するとともに情報セキュリティが侵害され、又はその恐れがある場合には、直ちに発注者に報告すること。これに該当する場合には、以下の事象を含むこととする。

① 受注者に提供し、又は受注者にアクセスを認める発注者の情報の外部への漏えい及び目的外利用

② 受注者による発注者のその他の情報へのアクセス

また、被害の程度を把握するため、受注者は必要な記録類を契約終了時まで保存し、発注者の求めに応じて成果物と共に発注者に引き渡すこと。

情報セキュリティが侵害され、又はその恐れがある事象が本業務に係る作業中及び契約に定める契約不適合期間中に発生し、且つ、その事象が受注者における情報セキュリティ上の問題に起因する場合は、受注者の責任及び負担において次の各号を速やかに実施すること。

① 情報セキュリティ侵害の内容及び影響範囲を調査のうえ当該情報セキュリティ侵害への対応策を立案し、発注者の了承を得たうえで実施すること。

② 発生した事態の具体的内容、原因及び実施した対応策等について報告書を作成し、発注者へ提出して了承を得ること。

③ 再発防止対策を立案し、発注者の了承を得たうえで実施すること。

④ 上記のほか、発生した情報セキュリティ侵害について、発注者の指示に基づく措置を実施すること。

(3) セキュリティ対策の改善

受注者は、本業務における情報セキュリティ対策の履行状況について発注者が改善を求めた場合には、発注者と協議のうえ必要な改善策を立案して速やかに実施するものとする。

16. その他

(1) 受注者は適格請求書発行事業者である場合、発注者に対し適格請求書を交付すること。

(2) 仕様にない事項又は仕様について生じた疑義については、発注者と協議のうえ解決すること。