再エネ業務統合システムの
運用保守に係る業務委託

運用保守要件定義書

電 力 広 域 的 運 営 推 進 機 関

目次

1. 調達件名

再エネ業務統合システム運用保守業務委託

2. 運用保守要件の定義

運用保守要件については、本項に記載の内容の他、「参考資料 1_非機能要件_IPA 非機能要求グレード活用シート」も参照すること。

2.1. 性能に関する事項

性能に関する要件を以下に示す。

2.1.1. 応答時間

表 2-1：応答時間

No	項目	内容
1	オンラインレスポンスタイム	・検索、参照、登録、更新及び削除に係る処理については、通常運用時に想定される最大負荷の条件下において、平均応答時間を 3 秒以内とすること。また、当該性能要件に対して過大なシステム構成とならないよう、費用対効果を考慮した適正な構成とすること。 ・ただし、縮退運転時はこの限りではない。
2	バッチレスポンスタイム	・オンライン終了後、翌日開始までに処理を完了させること。 ・オンライン業務への影響が出ないよう処理を完了すること。

2.2. 信頼性に関する事項

本システムは、再エネ事業者に対する FIP 交付金、廃棄等費用積立金、交付金相当額積立の管理を行うことから、滞りのない安定運用が求められる。これを踏まえ、システムの構築・運用・保守において、十分な信頼性の確保に努めること。

2.2.1. 可用性要件

可用性に係る指標は、「稼働率」として目標値を99%以上とする。ただし、本機関と事前に合意した時間帯で実施するパッチ適用等の計画的な作業に伴う停止時間は、稼働率の算出対象には含めないこととする。これを踏まえ、システムの構築・運用・保守において、十分な信頼性の確保に努めること。

算出式：（サービスの稼働した時間　－ 停止した時間）÷（実際に稼働するべき時間）×100

※計画停止した時間は除外する。

2.2.2. 完全性要件

受託者は、現行システムにおけるデータの完全性を確保するための構成及び対策を、運用

保守期間中も維持すること。

・機器の故障に起因するデータの滅失や改変を防止する対策を講ずること。

・異常な入力や処理を検出し、これらによるデータの滅失や改変を防止する対策を講ずること。

・処理の結果を検証可能とするため、ログ等の証跡を残すこと。

・データの複製や移動を行う際にその内容が毀損した場合でも、毀損したデータ及び毀損していないデータを特定するための措置を行うこと。

2.3. 拡張性に関する事項

受託者は、現行システムが有する柔軟性及び拡張性を、運用保守期間中も維持すること。

以下の事項を考慮し、大幅な改修をしなくとも対応可能な、柔軟性・拡張性を有すること。

・本システムのユーザの増加

・本システムで取り扱う業務量・データ量の増加

・管理する情報項目の追加・削除及び形式変更

2.4. 上位互換性（ハードウェアとソフトウェアのバージョンアップ）に関する事項

受託者は、現行システムの構成を前提として、ハードウェア及びソフトウェアのバージョンアップに対応可能な状態を、運用保守期間中も維持すること。

以下の事項を考慮すること。

・応札時点において、OS、ソフトウェア等のバージョンアップ情報が公開されている場合、原則、バージョンアップに対応できるように構築すること。

・契約期間中のバージョンアップは、影響範囲を調査し、その対応方針を本機関に報告すること。また、バージョンアップについて、技術的な問題等がある場合は、本機関と協議すること。

2.5. 中立性に関する事項

受託者は、現行システムにおける特定の事業者、製品又は技術等に依存しない構成及び他の事業者への引継ぎが可能な状態を、運用保守期間中も維持すること。

特定の事業者、製品、技術等に依存することなく、システム拡張時、あるいは次期更改時等において、他の事業者等に必要な情報を、支障なく引継ぐことが可能なシステム構成とすること。

また、システム更改の際に、移行の妨げや特定の装置や情報システムに依存することを防止するため、原則として本システム内のデータ形式は XML、CSV 等の標準的な形式で取り出すことができるものとすること。

2.6. 継続性に関する事項

2.6.1. 継続性に関する基本要件

受託者は、現行システムの継続性を確保するための構成及び対策を、運用保守期間中も維持すること。

単一障害（クラウドサービスのAZ障害)発生時には業務停止を許容せず、処理を継続させるよう、各機器は全て二重化すること。なお、直接的な業務影響のない端末等は二重化の対象外とするが

、コスト対効果の最も良い方式を検討すること。

2.6.2. 継続性に関する目標値

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

継続性に関する指標及び目標値は以下のとおりとする。

表 2-2：継続性に関する目標値

No	指標名	目標値
1	目標復旧地点（RPO）	・1 日前時点
2	目標復旧時間（RTO）	・3 日以内

2.6.3. 継続性に係る対策

災害・事故発生時においても、本システムを用いた事業継続に支障をきたすことのないよう、業務上重要なデータ、並びにシステム稼働に必要なデータの障害に備え、主に以下のデータをバックアップ対象とする。

なお、バックアップの取得については、媒体保管の他、クラウドサービスプロバイダから提供されるバックアップサービスを利用して差し支えない。ただし、バックアップ場所としては、メインサイト、及び同時被災しないことを前提としたバックアップサイトの場所の他、クラウドサービスの全体的な災害や障害に備え、当該クラウドサービスとは別に外部での保管もすること。

また、業務関連データ等の重要情報のバックアップはデータを暗号化した上で実施すること。

表 2-3：バックアップ対象と設定内容

No	バックアップ対象	バックアップの設定
1	システム環境設定情報	2 世代（システム環境変更時）
2	各種ログ情報	日次データを半年分
3	業務関連情報	日次/週次（日次は差分バックアップ、週次はフルバックアップ）2 世代分

※当該クラウドサービスとは別に外部保管する対象は、RPOの目標値を満たす最小範囲とする。

2.6.4. リストア試験及び障害訓練

バックアップデータからシステム及び業務関連情報を正常に復元できることを確認するため、本番業務に影響を与えない方法により、原則として年1回以上、リストア試験を実施すること。

また、障害発生時における対応体制及び対応手順の実効性を確認するため、原則として年1回以上、障害訓練を実施すること。

試験及び訓練の実施内容については、事前に本機関と協議すること。また、実施結果を本機関へ報告し、改善が必要な場合は、関連する手順書等を見直すこと。

2.7.情報セキュリティに関する事項

2.7.1.情報セキュリティ対策要件

2.7.1.1.受託者は、現行システムに実装されている情報セキュリティ機能及び対策を、運用保守期間中も維持すること。

2.7.1.2.セキュリティ機能

2.7.1.2.1.主体認証機能

・事業者ごとにユーザを識別するため、ユーザ毎にID、パスワードを付与すること。
・ユーザのID、パスワード認証を含めた多要素認証の機能を設けること。
・ログイン時のパスワードはマスク表示すること。
・ユーザのパスワード等の情報を暗号化して保存する機能を設けること。
・ユーザが自らのパスワードを変更できる機能を設けること。
・パスワードについては、文字数及び使用する文字の種類を制限する設定ができること。
・管理者権限をもつユーザ（以下「システム管理者」という。）が最終パスワード変更日を確認できる機能を設けること。
・パスワード等を他者に使用された場合又はその危険が発生した場合に、直ちにパスワード等による主体認証を停止する機能を設けること。
・不正ログイン行為を検知又は防止する機能として、パスワードの誤入力が複数回検知された場合に、当該IDによる本システムへのログインを無効にする機能を設けること。その際、検知の回数によるログインの無効化を可能とすること。また、無効になったIDの無効状態を解除することができる機能を設けること。
・パスワード等が他者に使用された場合又はその危険が発生した場合に、そのユーザが使用していたパスワードの変更等をシステム管理者が行うことができる機能を設けること。

2.7.1.2.2.通信の暗号化機能

・ネットワーク上の通信の暗号化を実施することにより、盗聴・漏えい等の技術的な脅威に対し、システムの機密性を確保すること。

2.7.1.2.3.データの暗号化機能

・重要情報の秘匿を保持し、重要情報等への不正アクセス及び改ざんができないよう、データベースを暗号化すること。
・暗号化に使用するアルゴリズムは、原則として「電子政府推奨暗号リスト」に記載されているものの中から選択すること。

2.7.1.2.4.ウイルス対策機能

・ウイルス対策として、ウイルスチェックパターンファイル（以下「パターンファイル」という。）は常に最新にすること。
・パターンファイルの更新については、ソフトウェアベンダー等において、パターンファイルが公開された時点で、迅速に本システムに適用できる仕組みを構築すること。また、ユ

ーザ及び本機関職員の作業負担のない方法を実現すること。

・ウイルス検出時は、本機関職員に電子メール等で日本語（ウイルス名等を除き）により通知すること。

・ウイルススキャンの実施頻度は、1日に1回以上とすること。

2.7.1.2.5. ログ管理機能

・本システムへの不正操作を監視し、各種証跡ログから情報漏えい時に迅速に対応できるよう、原則として、次のログ情報を取得可能とすること。なお、ログ管理機能に求める要件は、「2.9.4.ログ管理要件」を参照すること。

表 2-4：ログ取得情報

No	ログ情報
1	ログイン・ログアウト等の事象を発生させる主体となるユーザ又は機器の識別コード
2	事象の種類（ログイン・ログアウト、ファイルへのアクセス、アプリケーションプログラムへのアクセス、起動等）
3	事象の対象（アクセスしたファイル、アクセスしたアプリケーションプログラム、機器等操作指令の対象等）
4	日付及び時刻
5	事象の結果（成功、失敗、エラー等）

2.7.1.3. 脆弱性対策の実施

2.7.1.3.1. 脆弱性情報の提供

・本システムに導入されるOSもしくはソフトウェア（ファームウェア、ウイルス対策ソフトウェア等）の脆弱性情報がソフトウェアベンダー等から公表された場合、クラウド事業者の対応有無、その対応時期等を含め影響分析を行い、本システムにおける緊急度を判断し、影響分析結果として本機関職員に報告すること。

・提供する脆弱性情報は、原則、日本語による情報であること。

2.7.1.3.2. 脆弱性の影響度の判断

・セキュリティパッチが対応している脆弱性に対する影響度の判断は、深刻度、脆弱性の影響、影響を受ける対象等の脆弱性情報に基づき行うこと。

2.7.1.3.3. 脆弱性検査

・第三者による脆弱性検査（Web診断を含む）を実施し、その結果を本機関に書面にて報告すること。

・なお、本機関主導での脆弱性検査を定期的に実施することから、受託者は協力すること。

2.7.1.3.4. セキュリティパッチ適用

・セキュリティパッチ適用により、本システムの正常稼働に影響がないことを確認するため

、スケジュール、環境、要員、手順等を定めた検証作業計画を策定すること。
・検証の結果、回避できない影響がある場合は、ソフトウェアベンダー等の提供する代替策を検証すること。また、OSもしくはソフトウェアの設定ファイルの変更等による対応可能な方法があれば、設定ファイル及び手順を作成し、検証すること。
・本システムの運用に影響を与えないために、スケジュール、要員及び手順等を定めたセキュリティパッチ適用計画を策定すること。
・必要に応じて、再起動を要すること等を事前にユーザ等の関係者に周知すること。

2.7.1.4. 情報セキュリティが侵害された場合の対策

本調達に係る業務の遂行において情報セキュリティが侵害され又はそのおそれがある場合には、速やかに本機関に報告すること。これに該当する場合には、以下の事象を含む。
・受託者に提供し、又は受託者によるアクセスを認める本機関の情報の外部への漏えい及び目的外利用
・受託者による本機関のその他の情報へのアクセス

2.7.1.5. 情報セキュリティ対策の履行状況の報告

本業務の遂行におけるセキュリティ対策の履行状況について、定期的に報告するとともに、本機関から報告を求めた場合には速やかに提出すること。

2.7.1.6. 情報セキュリティ監査への対応

本機関が第三者機関等による情報セキュリティ監査を受ける場合には、受託者はその監査の実施について本機関の求めに応じ支援すること。情報セキュリティ監査の結果、対策が必要な場合は、本機関と協議を行い、合意した対策を実施すること。

2.7.1.7. 情報セキュリティ対策の履行が不十分な場合の対処

本業務の遂行において、受託者における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る場合には、受託者は、本機関の求めに応じ、本機関と協議の上、合意したセキュリティ対策を実施すること。

2.8. 情報システム稼働環境に関する事項

2.8.1. 基本要件

・情報資産（有形、無形を問わず本システムに含まれる情報とし、帳票、記憶媒体、電気通信等で伝達される情報等を含むものとする。）を管理するデータセンタの物理的所在地が日本国内にあること。また、継続性の観点から、日本国内で地理的に分散管理することが望ましい。
・本機関の指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。
・情報資産の所有権は本機関であること。
・クラウドサービスの利用契約に関連して生じる一切の紛争は、日本の地方裁判所を第一審の専属的合意管轄裁判所とするものであること。

・情報資産が何らかの形で残留して外部に漏えいすることがないよう、必要な措置を講じること。
・クラウドサービスの提供に関して、現行クラウドサービスについて当該要件を維持すること。

2.8.2.構築すべき環境

受託者は、現行システムの本番環境、検証環境及び研修環境について、その構成及び機能を運用保守期間中も維持すること。

・ユーザが業務で用いる本番環境、ユーザがテストを行うための検証環境（運用保守においても常に利用できる環境）を用意すること。なお、受託者が開発を行う開発環境は受託者にて用意すること。
・検証環境及び研修環境については、本番環境と機能構成は同一とするが、スペックについては機能試験が可能な最低限のものとすること。また、IP アドレスによる接続制限を可能とすること。
・各環境については、接続している環境が URL 以外でも判別できるようにすること。

2.8.3.保守端末・監視端末要件

・本システムに関するシステム障害（以下、「障害」という。）の解析、対応作業及び運用監視業務等を円滑に進めるため、保守拠点に、障害発生時の証跡取得等に用いる保守端末及び稼働状況の監視等に用いる監視端末を導入すること。
・本システムで作成された帳票等の確認、及び前述の障害解析・運用作業に係る証跡等の作成を行うため、Microsoft Word（バージョン2021以降）及びMicrosoft Excel（バージョン2021以降）形式のファイルを参照及び編集が可能な仕組みを構築すること。
・PDF形式（バージョン1.5以上）で作成されたファイルが表示可能な仕組みを構築すること。
・作業時の可搬性や電源特性を考慮し、バッテリー稼働可能なノート型PCとすること。また、端末をケーブル等で固定するためのセキュリティロック用ケーブルスロットを有すること。
・不正な持ち出し防止のため、保守端末及び監視端末はセキュリティロック用ケーブルで固定すること。
・セキュリティ対策について本機関と協議し合意を得ること。

2.8.4.保守拠点の要件

・保守端末、監視端末等の機器は本番環境に接続すること。なお、接続に用いる回線は、受託者の責任と負担において用意することとし、IPアドレスによるアクセス制限等の適切なセキュリティ対策を施すこと。
・保守拠点は、受託者の責任と負担において用意すること。
・保守拠点のセキュリティ対策について本機関と協議し合意を得ること。

2.8.5.クライアント環境要件

クライアントの環境要件として、少なくとも以下のブラウザに対応すること。なお、スマートフォン、タブレット端末等のモバイル端末については個別の対応は不要とする。

・Microsoft Edge（Windows11のリリース時同梱バージョン）

・Google Chromeの最新安定バージョン

2.9.運用に関する事項

2.9.1.基本事項

受託者は、本機関が本要件定義書で示す要件を踏まえ、運用に関わる詳細を定める「運用保守計画書」を作成し、運用保守期間を通じて必要に応じて計画の変更・修正等を実施するなど、適切に管理すること。

運用にあたり、本機関の情報セキュリティ関連規程に従い運用手順を定めること。

表 2-5：運用に関する事項

No	項目	内容
1	システム運用時間（通常）	・平日 9 時～21 時とする。ただし、本機関からの依頼に基づき、21 時以降も利用可能とすること。（月 1 回程度の時間延長を想定すること。）※上記は最低限の時間帯を示したものであり、上記以外にも稼働する時間帯はあってもシステム上の不整合が生じないこと。（夜間バッチ処理等と競合しないこと。）
2	システム運用時間（特定）	・通常と異なる運用時間となる特定日は存在しない。
3	計画停止	・計画停止は可能であるが、事前に通知を行ったうえで、本機関と調整のうえ実施すること。
4	緊急対応時間	・本機関が「緊急」と判断する障害発生時に、24 時間 365 日、担当者間で連絡及び対応が可能な体制を確保する。
5	運用負荷削減	・業務機能の起動・停止等、定期的に行う処理は自動化するが、ログの削除等、非定期に実行する処理は運用保守管理者が手動で実施することを想定している。

2.9.2.情報システムの操作・監視等要件

監視対象は、サーバ、ストレージ、ネットワーク、データベース、ソフトウェアパッケージ、ネットワーク機器、アプリケーションプログラム、ログ等とし、システムが正常に動作するために必要な以下の監視を行うものとする。

表 2-6：監視項目

No	監視項目	内容
1	死活監視	・監視対象サーバの状態を定期的に監視すること。
2	プロセス監視	・監視対象サーバ上のアプリケーションプログラム等のシステムの稼働に必須となる常駐プロセスが正常に動作していること（無応答でないこと）を監視すること。
3	ジョブ監視	・ジョブ管理用のソフトウェアと連携し、障害の検知を目的とした

No	監視項目	内容
		監視をすること。
4	ネットワーク監視	・本番環境のネットワーク監視をすること。
5	ログ監視	・不正アクセス発生の有無の確認のため、アプリケーションプログラムのログの確認を、月に 1 回、実施すること。
6	リソース使用状況監視	・監視対象の各サーバの CPU、メモリの使用状況を監視すること。 ・監視対象の各サーバ、ストレージのディスク使用状況を監視すること。 ・リソースの使用状況について、あらかじめ定めた閾値を超えた場合に、自動的に検知できる仕組みを用意すること。
7	性能監視	・応答時間等の状況を監視すること。
8	情報セキュリティ監視	・不正侵入、不正アクセス、データ改ざんの有無等を監視すること。

2.9.3. 運用サポート業務に係る要件

表 2-7：主要な運用サポート業務

No	運用項目	内容
1	バッチジョブ運用	・バッチジョブの定期的な動作（スケジュール）を管理すること。 ・バッチジョブによるインシデントを検知した場合、速やかにインシデント管理及び問題管理の作業フローに従い対応すること。
2	時刻同期	・外部システムやユーザからの問合せ等に対する時刻整合性を保つため、NTP サーバを利用して、時刻同期を実現すること。
3	セキュリティパッチ・ウイルスパターン適用	・開発元、販売元、サービス提供元からサポートを確実に受けられる体制を確保すること。 ・セキュリティパッチ、ウイルスパターン適用に関する影響の調査、検証を実施し、本機関が適用を判断する上で必要な情報（技術的な問題等の有無を当該事業者が判断するための情報等）を提供すること。 ・OS、ファームウェア、ウイルス対策ソフトウェア等のセキュリティパッチ及びウイルスパターン適用を実施し、適用結果を確認すること。 ・変更のリリースに際しては、リリースが与える影響等を考慮し、利用者及び利用者との接点となるヘルプデスクに必要な情報を周知すること。
4	サーバ証明書の更新作業	・システムに登録しているサーバ証明書の期限切れに伴う更新作業を実施すること。
5	システム設定データ更新作業	・システム設定データの更新作業を実施すること。

6	マスタ更新作業	・マスタデータの更新作業を実施すること。
7	月次報告	・運用保守状況を報告する資料を作成し、月次で報告すること。

2.9.4. ログ管理要件

本システム運用におけるセキュリティインシデント、不正操作、ハードウェア・ソフトウェアの障害が発生した際の原因究明（調査・分析）、システムの性能監視等に必要となるログを管理する仕組みを構築すること。なお、サーバのＯＳが出力するログの開示ができない等のクラウドサービス側の制約がある場合においては、少なくとも、原因究明等の結果の報告が可能であることをもって代替可能とする。

2.9.4.1. ログ出力・蓄積・監視要件

・サーバ、アプリケーション等の各種ログを出力できること。
・出力したログは、一定期間、蓄積が可能であること。また、長期保存が必要なログについては、外部の電磁的記録媒体に保存が可能であること。
・ログの保管期間について、契約開始後に現行設計を確認し、本機関と協議の上確定する。
・バックアップしたログを期間が経過した後も参照できるように、特定のソフトウェアに依存しない形式（テキスト形式等）でログの保存が可能であること。
・出力されるログを監視できること。
・ログ監視に必要なレポートが生成されること。
・情報システムセキュリティに関する利用者及び本機関職員が不当に消去、改ざん又はアクセスすることのないように、ログ情報を保存したファイルに適切なアクセス制御ができること。

2.9.4.2. ログ収集要件

・監視対象の各サーバに散在するセキュリティログ及び監視ログをソフトウェアの機能や OS の機能等を利用して自動的に一括収集することが可能であること。
・収集対象のログについては、以下の収集対象ログ一覧を参照のこと。詳細は設計工程において確定することとする。

表 2-8：収集ログ一覧

No	ログ種別	内容
1	各種サーバログ	・サーバへのアクセスユーザ（ログイン、ログアウトしたユーザ）の情報等が特定できるログ（セキュリティ、イベントログ等） ・サーバの OS が出力するシステムログ、アプリケーションプログラムのログ
2	Web サーバアクセスログ	・Web サーバにアクセスがあった時刻、クライアント IP アドレス、ホスト IP アドレス、ポート番号、要求コマンド、ステータス等の情報が特定できるログ
3	データベースアクセスロ	・データベースへアクセスしたユーザを特定することが可

	グ	能なログ
4	アプリケーションプログラムのログ	・アプリケーションプログラムを実行したユーザ及びその操作内容を特定することが可能なログ

・保守拠点の保守端末及び監視端末からログ収集の設定・ログ収集の操作ができること。
・収集したログを分析し、相互に関連付け、保管できること。ログ分析結果については、月次報告書に含めること。
・収集したログの閲覧が可能であること。

2.9.5. 業務運用支援

2.9.5.1. ヘルプデスク

・本機関職員からの問合せに対応すること。
・メール及び電話で受け付けること。（本システムを利用する事業者からの問合せについては、本機関が一次窓口となり、原則直接のやり取りは発生しない。）
・問合せ受付に必要となる機器、回線については、受託者において用意すること。
・操作方法等の頻度の高い問合せについては、FAQ として分類・蓄積し、問合せ対応の迅速化を図ること。
・本機関職員からの依頼に応じて、アプリケーションを通して受け付けた提出書類等の添付ファイルを一括で出力し、安全な方法で本機関に送付すること。
・障害に係る問合せに対して、問題切り分け、原因究明を実施すること。
・ヘルプデスクの開設時間帯は平日（9 時～17 時）を前提とすること。

2.9.6. 運用実績の評価と改善

運用実績（ヘルプデスクの対応状況、サービスレベルの達成状況、情報システムの構成と運転状況（リソース使用量等含む。））の値の取得、評価及び管理、運用実績が目標に満たない場合の要因分析及び改善措置の検討等を行い、その結果を本機関に報告すること。

2.10. 保守に関する事項

2.10.1. AP プログラムの保守要件

障害発生時には、本機関に報告のうえ、問題切り分け、原因究明の結果について、受託者にて調査を実施した上で、本機関職員と協議し、修正等の必要な対応（障害報告書による報告を含む）を実施すること。

また、小規模な改修（画面・帳票レイアウトの変更、検索条件の修正等）について、本機関職員と協議し、年間 36 人月程度の対応を実施すること。

2.10.2. 作業環境

アプリケーションプログラムの修正やテストは、開発環境及び検証環境で実施すること。

2.10.3. 保守時間

障害等緊急の理由により、システムの稼働時間が延長された場合、延長時間に応じて保守対応時間を延長する場合がある。

2.10.4. 保守実績の評価と改善

保守実績（サービスレベルの達成状況等）の値の取得、評価及び管理、保守実績が目標に満たない場合の要因分析、改善措置の検討等を行い、本機関に報告すること。

以上

3. 附属文書

別紙1.「業務仕様書」

別紙2.「全体システム概要図」