

別添3 運用・保守

第1 運用・保守要件

1. 基本的な考え方

本稿は運用保守における様々なパターンを想定した本市の基本的な考え方を示した資料であり、本件調達仕様書を補足するものとなっている。システム構成形態により要不要があるため、必要な事項を参照の上、運用保守設計時に協議を行うものとする。

2. システム稼働当初における要件

本システムが本番稼働した直後の運用は次の要件を想定している。

運用要件	内容
定常時対応	ユーザーが利用する時間帯である平日 8:00～18:00 を想定しているが、環境変更等、随時作業については夜間・休日等を実施する場合がある。
移行直後のサポート	運用開始日は、不測の事態に即座に対応できるよう、本件の構築・運用に関する豊富な知見を有するエンジニアを配置すること。障害が発生した場合、可及的速やかに復旧作業をとるとともに、対外的に復旧進捗報告・説明が可能になるよう、情報を提供すること。 運用開始日から起算して2週間は、構築に携わったエンジニアが即応できる体制を整えること。質疑応答、操作説明等のヘルプデスク支援、作業立ち合い、操作支援、技術支援等の業務支援を行うこと。（待機者は1名の持ち回りで構わない） なお、本市の周辺に営業拠点がなく待機するエンジニアの確保が難しい場合や保守拠点からのコントロールの方が迅速に対応できると判断する場合については、その他の方法によるサポート体制の場合も認めるものとする。ただし、この場合は一時的に電話等のチャネルを増強すること等、同時に複数の問い合わせやトラブルに対応できる体制とすること。さらに、待機しないことによる、障害の一次切り分け、復旧手順の協議と決定、回避操作の指図等について遅延なく障害対応ができる体制とすること。
障害対応	システム継続が不可能など重大障害における連絡受付については、24 時間 365 日対応できる体制（受付・作業着手までを想定）を整えること。ただし、定常時対応時間帯とは異なる体制でもよい。 障害発生時には、障害発生 の報告受付、初期の原因の切り分けと応急対応、逐次での本市への状況報告、不具合発生状況の確認と、システム復旧・整合性調査、応急対応完了後の正式な原因究明、ソフトウェア・ハードウェア起因の場合の改修、顛末の報告、改善及び再発防止策の

	提案等、障害への復旧及び再発防止対応までの一連の手続きに対応すること。なお、障害発生からの報告から初期対応（原因の切り分けと応急対応、関係者への連絡等）開始までの時間を概ね1時間以内とすること。 障害箇所が冗長化されておりシステム機能が停止していない場合、障害対応はシステム利用時間外の時間帯に行うこと。ただし、システム機能を停止させずに障害対応が可能な場合は、本市の承認を受けた上で実施してもよい。
--	--

3. 大規模災害時対応計画の作成支援

本市では大規模災害時における業務継続性確保のため、情報部門に係る計画として、徳島市ICT-BCPを策定し、点検・見直しを行っている。

本システムにおいても同様に整備が必要であるため、本市における大規模災害等の情報システム運用継続計画書の作成若しくは更改について支援すること。なお、訓練計画・訓練実施までは想定していない。

4. 運用・保守の設計

受注者は、定常時における月次の作業内容及び想定スケジュール等を取りまとめた運用計画書及び保守計画書の案を作成し、本市に提出をすること。その際、保守と契約不適合責任の範囲内で実施する作業の分担を明確にするよう留意するものとする。

本市は受注者等とともに、定常時及び障害発生時において想定される運用体制、実施手順等を取りまとめるものとする。なお、複数の情報システムにより業務で利用されるサービスが構築される場合には、サービス実施手順等を明確にするよう留意するものとする。

受注者は、運用を補助するためのツールが必要となる場合には、本市に対し、当該ツールの実装及び単体テストの実施状況の報告、運用ツールの操作方法等に関する手順書を作成し、提出すること。本市はテスト内容の十分性や手順書の妥当性等を確認し、不明点・不具合があれば課題等の指摘又は指導を行うものとする。

第2 運用・保守業務

1. 運用作業概要

本システムにおける運用監視、運用作業の対象範囲、対象とする作業の概要として次の事項を想定している。

作業名	作業概要	監視項目【単位・具体的な内容】
死活監視	情報システムを構成する機器類の障害発生状況等を把握するために、機器の通信状態の変化や再起動の状況を監視すること。	・再起動回数【計画外停止の場合その理由】 ・機器応答時間【ミリ秒/月平均（※測定可能な場合）】
性能監視	情報システムの性能要件が維持されていること。	・レスポンスタイム【ミリ秒/月平均（※測定可能な場合）】

	ることを確認する。また、業務特性やピーク時特性を踏まえて情報システムの性能等の分析・管理を行うこと。	・ターンアラウンドタイム【ミリ秒/月平均（※測定可能な場合）】 ・サーバ処理時間等【合計 CPU 処理時間/合計サービス提供時間】
稼働状況監視	情報システムの稼働状況や利用状況の監視、ソフトウェアライセンス数の把握等を行うこと。	・サーバ処理時間等【合計 CPU 処理時間/合計サービス提供時間】 ・メモリ空き容量【月当たりの最大使用量と最低使用料】 ・HDD空き容量【基準日時点】 ・情報システム利用状況【月当たりの総アクセス数、月当たりののべ利用者数、月当たりの単位利用者数】 ・ソフトウェアライセンス【ソフトウェアの製品名、バージョン、数量、利用者】
セキュリティ監視	情報セキュリティに関する事象の発生状況を監視すること。	・不正アクセス件数【月当たりのログイン失敗数】 ・ウイルス検知数【月当たりの検知数全て、かつ、検出情報】 ・不正侵入検知数【月当たりの検知数全て】
防犯監視	施設・区域等に対する物理的な不正侵入や火災の発生有無等を監視すること。	・物理的な不正侵入発生状況【月当たり】 ・火災発生状況等【月当たり】
データ一括処理業務	定期又は臨時に手動によるデータ一括処理の必要があった場合、処理の実行及び実行状況の確認を実施すること。	・処理の実行確認（頻度、時間）【すべての実行結果】 ・処理結果の内容確認（成否）【すべての実行結果】
バックアップ管理	情報システムにおけるデータのバックアップ管理を行うこと。	・バックアップ実施回数【全部/一部の実施】 ・バックアップデータからの復旧回数【全部/一部の実施】
障害復旧対応	障害発生時に影響度等の分析を行った上で、障害による影響を最小限にとどめ、情報システムの復旧作業を行うこと。	・障害復旧時間【障害発生日時、受注者が障害を認識、市が障害を認識、障害への対応を開始、障害を復旧した、すべての日時】
情報システムの設定変更	情報システムの設定変更等を行う。 ※情報システムの設定変更の実施方法や変更内容の整理は保守業務とする。	・情報システムの設定変更件数【変更内容すべて】
セキュリティパッチ運用等業務	セキュリティパッチの適用やアップデートを実施する。 ※セキュリティパッチの適用やアップデートの方法等の整理、テストの実施は保守業務とする。	・セキュリティパッチ適用件数【適用予定パッチ、適用完了パッチすべて】 ・アップデート実施件数【アップデート予定パッチ、アップデート完了パッチすべて】

ログ管理	情報システムのログの解析結果を確認し、問題等があれば把握する。	・異常検知件数【月当たり】 ・改ざん検知件数【検知すべて】
廃棄管理	情報資産を廃棄する場合は、廃棄手順に従った実施結果。 ※バックアップデータの世代管理に伴い上書きするなど、運用サイクル上認識しているデータは監視不要。	・廃棄内容【廃棄日、廃棄方法、廃棄した情報資産すべて】
構成管理	ハードウェアやソフトウェア製品、ネットワーク等の情報システムを構成する資産の管理を行う。	・構成変更件数【構成変更予定、構成変更完了すべて】
ネットワーク管理	ネットワークの稼働状況や利用状況の監視を行う。また、ネットワーク機器や管理すべきサービスの構成情報(IPアドレス、ポート接続情報、回線情報等)を管理する。	・ネットワーク障害発生件数【インシデントすべて】 ・ネットワーク設定変更件数【設定変更予定、設定変更完了すべて】
運用サポート業務	情報システムの利用者である職員や外部利用者のサポートを行うためのヘルプデスク又はコールセンタを設置し、運用する。	・ヘルプデスク/コールセンタ稼働状況【問合せ件数、一次回答率等】
業務運用支援作業	データ作成、データ受付・登録、大量帳票印刷等の情報システムや業務の運用に当たり必要となる作業を実施する。	・運用保守委託の中で実施したデータの取り扱い作業内容【作業名、作業時間、作業従事者、取扱件数、警告内容、エラー内容】
運用実績等の評価と改善作業	運用実績値等の取得や評価、運用実績値等が目標に満たない場合の要因分析や改善措置の検討等を行う。	・改善提案【改善案すべて】

2. 保守作業概要

本システムにおける保守作業の対象範囲、対象とする作業の概要次の事項を想定している。なお、情報システムの形態に従って、ハードウェアが無い場合は、適宜割愛するものとする。

作業項目		作業概要
アプリケーションプログラムの保守	アプリケーションプログラムの不具合の受付	アプリケーションプログラムの不具合を受け付ける。
	アプリケーションプログラムの不具合の原因調査	アプリケーションプログラムの不具合の原因を調査し、特定する。
	修正プログラムの作成、提供	アプリケーションプログラムの不具合を修正するための修正プログラムを作成し、検証環境においてテストを行う。 ※修正プログラムの本番環境への適用は

		運用業務とする。
ハードウェアの保守	定期点検	ハードウェアの状態について定期的に点検を行い、稼働状況について確認を行う。
	予防保守	ハードウェアの部品等について、稼働による損耗等による障害を防止するために部品等についてあらかじめ交換を行う。
	保守部品提供・交換	受注者等が行う軽微な部品交換のために部品の提供や交換を行う。
	ファームウェア等保守	ファームウェアなどの組込みソフトウェアの設定変更やアップデートを行う。
	ハードウェアの不具合の受付	情報システムにおけるサーバやディスク等の不具合を受け付ける。
	ハードウェアの修理又は交換	ハードウェアの修理又は交換を行う。
ソフトウェア製品の保守	ソフトウェア製品の不具合の受付	ソフトウェア製品の不具合を受け付ける。
	アップデートファイル(セキュリティパッチ等)の提供	アップデートファイル(セキュリティパッチ等)を提供する。 ※アップデートファイル(セキュリティパッチ等)の本番環境への適用は運用業務とする。
	サポート対応	ソフトウェア製品の利用に関する問合せに対応する。
データの保守	マスタデータや業務データの品質確認	情報システムで用いられるマスタデータや業務において生成される業務データについて完全性等を確認する。
	異常・不整合等が発生したデータの検出	情報システムで用いられるマスタデータや業務において生成される業務データから異常・不整合等が発生したデータを検出する。
	異常・不整合等が発生したデータの修正又は削除	検出された異常・不整合等が発生したデータの修正又は削除を行う。
保守の記録	現地保守	本市にて現地保守を実施した場合は、その保守記録をまとめ、定期報告時に提供すること。
	遠隔保守	クラウド等に情報システムを整備し、遠隔地からリモート保守を行う場合は、その保守記録をまとめ、定期報告時に提供する

		こと。また、保守時に採取するログのうち、データベースにアクセスしたログについてはシステムが保存する最大の年限数保存し(11 会計年度)、本市が提出を求めた際は速やかに提出すること。
保守実績等の評価と改善作業		保守実績値等の取得や評価、保守実績値等が目標に満たない場合の要因分析や改善措置の検討等を行う。

3. 作業体制

受注者は、運用・保守業務に携わる関係者が記載された体制図を提出すること。体制図は、定常時及びインシデント発生時の体制の双方が記載されていること。

4. 遠隔保守

遠隔保守については、受注者決定後に本市と協議のうえ、その範囲と運用手法を事前合意のうえで実施すること。

遠隔保守を行う場合、情報システムに対してセキュアな環境での接続・運用する体制を確保するため、遠隔保守専用端末を使用する、VPN接続等で保守端末と情報システム間の通信のセキュリティを保つ、保守端末には個人情報及び機密情報が残らないようにする、作業は受注者が管理するセキュリティが保たれた区画内で行う等の環境を整えること。

遠隔保守のために受注者が用意するVPN機器については本市の管理物件ではないため、監視対象とはならないが、受注者は JPCERT/CC 等の脆弱性情報を掌理の上、できるだけ最新のセキュリティ対策を実施すること。遠隔保守機器のセキュリティ対策が適用されず、当該機器を経由して本市の情報漏洩、情報システムへのマルウェア及びランサムウェア等の感染があった場合は、本市は、いかなる理由であっても受注者に重大な過失があるものとみなす。

遠隔保守においては、発生する接続・操作履歴(ログ)を残すこととし、本市の求めに応じてその情報を提供すること。

遠隔保守環境の構築・運用についてはその費用を提案価格に含むものとし、その構築・運用によって発生した問題及び損害は受注者の責任において対応・解決・賠償の責任を負うこと。

5. 作業スケジュール

受注者は、運用・保守業務の年次、四半期ごと、月次、週次、日次等のスケジュールをとりまとめること。また、連携する他の情報システムや統合的に運用を行う他の情報システムがある場合には、それらシステムにおける作業のうち、当該情報システムに関係する作業やそのスケジュールについても記載すること。

6. 関係事業者との合意形成手続

受注者は市との合意形成に関する手続、連絡調整に関する方法や手順、頻度、議事録の管理を行う。運用業務では次の会議体を想定している。

会議体名称	会議目的	開催頻度
定期運用・保守会議	運用作業実績、リスク、課題等の確認	毎月等
運用業務年間評価会議	年間の運用作業実績の確認、改善策の検討	年次
対策検討会議	障害対応、再発防止策の検討	障害発生時等
その他調整会議	他の情報システムの運用作業との調整	適宜

なお、定期運用会議の開催頻度は業務及び情報システムの成熟度によって、受注者と本市が合意の上、開催間隔を最大半年程度まで長くすることができる。また、定期運用・保守会議は書面で実施することができる。

対策検討会議及びその他調整会議は、事案が発生する見込み、あるいはした場合に、受注者若しくは市のどちらかが参集を依頼することができる。

会の議事内容及び結果について、書面により議事録を残すものとする。

7. 作業管理

受注者は、定期運用・保守会議の中で、運用状況の月次報告として、運用作業実績、保守作業実績、情報システムの構成、運転状況、及びサービスレベルの達成状況等について報告を行うこと。

月次報告(案)は次のとおり。

報告項目	内容
運用作業実績状況	・運用作業の集計結果(実施件数、工数実績、総作業時間等) ・運用作業の一覧(作業内容、担当者、発生日、完了日等) ・作業実績状況を踏まえた改善提案 等
情報システムの構成と運転状況及びサービスレベルの達成状況	第2「運用・保守業務」1「運用作業概要」の表に基づく監視項目について報告を求める。また、非機能要件等で定めた指標について、目標値に満たない項目がある場合には、要因分析結果の報告や改善策の提案も求める。
保守作業実績状況	・保守作業の集計結果(実施件数、工数実績、総作業時間等) ・保守作業の一覧(作業内容、担当者、発生日、完了日等) ・作業実績状況を踏まえた改善提案 等
サービスレベルの達成状況	第2「運用・保守業務」2「保守作業概要」の表に基づく監視項目について、受注者の責任範囲である項目に問題等が発生した場合の原因分析結果の報告や改善策の提案を求める。
情報システムの定期点検状況	・定期点検の実施有無 ・ハードウェア、ソフトウェア等の異常有無 等
リスク・課題の把握・対応状況	・リスク・課題の一覧 ・リスク・課題の発生理由、対応状況 等

問題・インシデントの把握・対応状況	・発生した問題・インシデントの一覧 ・問題・インシデントの発生理由、対応状況 等
-------------------	---

8. リスク管理

受注者及び市は、運用・保守の中で情報システムに関するリスクがあると判断した場合は、リスク管理対策を整備する。

リスク管理は、リスク管理表により、体系的に実施する。

9. 課題管理

受注者及び市は、運用・保守の中で情報システムに関する問題・インシデントが発生する見込みがある場合は、課題管理対策を整備する。

課題管理は、課題管理表により、体系的に実施する。

10. システム構成管理(情報資産管理標準シート及び情報システム資産台帳シート)

受注者は、管理対象となる情報システムを構成するハードウェアやソフトウェア製品、ネットワーク等の各資産における管理項目をドキュメントとして整備すること。

また、情報システムの構成を変更する予定若しくは実施した場合は、変更内容等の情報について市に報告し、ドキュメントと整合すること。また、ハードウェア、ソフトウェアの構成について個別に管理するだけでなく、稼働環境の確認やライセンス管理の観点からもソフトウェアがどのハードウェアに紐づいているかについても明らかにできる関連図についても提供すること。情報システムを構成する各資産における管理項目(案)を以下に示す。

資産	管理項目
ハードウェア	管理番号、分類、メーカー、品番、シリアル番号、数量、購入日、廃棄日、設置場所、OS、バージョン、実装メモリ、ディスク容量、保守サポート期限 等
ソフトウェア製品	管理番号、分類、名称、バージョン、数量、購入日、廃棄日、契約ライセンス数、使用済ライセンス数、媒体保管場所、保守サポート期限 等
アプリケーションプログラム	管理番号、分類、名称、バージョン、取得日、最新更新日、廃棄日、媒体保管場所 等
ネットワーク	管理番号、分類(アクセス回線、中継回線)、ネットワーク種類、帯域、設置拠点、契約開始日、契約終了日 等
外部サービス	管理番号、サービス分類、名称、契約開始日、契約終了日 等
施設・区域	管理番号、分類、名称、場所 等
公開ドメイン	管理番号、分類、名称、ドメイン数、作成日、終了日 等
その他	証明書有効期限 等

※管理番号は要素を一意に識別する任意の番号。

また、これらを図示するために次のドキュメントを整備すること。

構成	内容
ハードウェア構成図(SaaS クラウド等の場合は、ベースラインとして割り当てた資源)	ハードウェアの概念的な構成を図示する。物理的な区画ごとに、ハードウェアの主要な資源(OS、CPU、メモリ、HDD、拡張 IF カード、バックアップ装置、プリンタ装置、スキャナ装置及び電源等)、主なサービスの機能、入出力情報を記載すること。仮想マシンの場合は、ホストの資源のほか、仮想環境に割り当てた資源を記入すること。
ソフトウェア構成図	ソフトウェアの論理的な構成を図示する。立ち上がっているソフトウェアごとに、主要な機能、データベース、入出力ファイルを記載すること。SaaS 型アプリケーションの場合は、利用するサービスを記入すること。
ハードウェアとソフトウェアの関連図	ハードウェア内にセットアップされたソフトウェアを記述する。情報システム全体で一連のサービスを展開する場合は、鳥観図として全体的な構成を図示すること。
ネットワーク接続構成図	ハードウェア、ソフトウェア及びクライアントPCが利用するネットワークの接続構成について論理的に図示すること。TCP/IP 通信による場合は、識別名、IP アドレス、使用・許可するポート、セグメント、VLAN 等を使用する場合はその区間等を記入すること。
ネットワーク機器構成図	主にサーバ及びスイッチの構成を図示すること。TCP/IP 通信による場合は、機器名、mac アドレス、配線、回線の品質、冗長性等を記入すること。クラウド環境の場合は、展開するリージョンやクラウドセンターの設置個所を記入すること。
建物図面、電源や信号ケーブル等の配線図	本市が管轄する建屋内に電源や光ケーブル等を構築した場合は、その建物の図面、電源及び信号ケーブル等の配線図等を記入すること。

なお、本市では所管している情報システムについて、情報システムの統合や見直しなど、最適なシステム調達への取組を進め、運用コストの削減や業務の効率化を図るため、毎年、情報システム資産台帳の提出を求めている。本番稼働後に本市から様式を提示する。

11. 変更管理

制度改正や運用の見直し等により変更が発生する場合は、管理対象、変更手順、管理手法等を管理すること。管理対象としては、次のドキュメント(案)を整備し、受注者と市が協議を行い、双方が合意のもと、作業を実施するものとする。

ドキュメント	内容
調達仕様書	費用が発生する見込みの場合は、受注者から参考見積書を提出の上、予算措置を行い、調達仕様書を作成する。随意契約の場合であっても、「作業一式」などと、省略するのではなく、体制図、工数、スケジュール及び納品物を定義する。 (調達仕様書は本市が作成するが、受注者はその実施のための資料提供をお願い

	いする)
運用要件定義書	運用に合わせて要件定義が変わる場合はそのドキュメントを作成すること。
設計書	出力帳票や画面などが変更される場合は、外部設計として変更する箇所についてドキュメントを作成すること。
運用計画とその附属文書	見直しによって、作業スケジュール、監視内容及び体制図が変わる場合はそのドキュメントを作成すること。
運用実施要領	変更に伴い、運用実施要領が変わる場合は、その変更後のドキュメント。
作業手順書	変更作業に伴う、実施手順やスケジュールについて明確にすること。
マニュアル等	マニュアルは、開発当初の作業分担に従う。ただし本市側が作成するドキュメントがある場合は、受注者は作成のための素材を提供すること。

12. 運用実施要領

運用管理業務全体を円滑かつ計画的に実施するために、受注者は運用実施要領を策定し、市に報告すること。受注者は本運用実施要領をベースとして、情報システムを管理すること。

第3 運用・保守実施報告

受注者は運用保守契約の報告時期及び履行期間満了(年度末等)において、運用・保守実施報告を提出すること。

運用実施要領に基づく管理資料

運用作業報告書(月次、年次、スポット等)

情報システムの現況確認結果報告書(※いわゆる棚卸により、ドキュメントどおりの場所に機器等が存在すること)

最新のソフトウェア構成

最新のハードウェア構成

最新のネットワーク構成

構成情報の変更履歴

運用作業の改善提案書(改善がある場合)

運用計画の改定案(改善がある場合)

第4 情報システムの引継

受注者は、本システムの更改時には次期システムベンダーに対し、作業経緯、残存課題等に関する情報を提供し、ヒアリング等について協力すること。

第5 情報システムの撤去

契約期間満了時におけるデータ消去及び受注者が設置したハードウェアや配線等の撤去については本事業の範囲で行うこと。リースでの賃貸借契約にも条件として含めるものとする。なお、データ消去の方法については、国の方針に従い将来の時点で確実な抹消方法を受注者と市が合意の上、実施するものとする。