運用保守要件一覧

No	カテゴリ	要件	作業内容	(参考)関連システム/ツー
1	計画書・要領	運用手順書（運用マニュアル）の作成	-	-
2	計画書・要領	大規模災害等の情報システム運用継続計画の	特に指定なし	-
3	計画書・要領	運用計画書の作成	定常時における月次の作業内容、想定スケジュール、障害発生時に想定される対応等を取りまとめた運用計画書の案を作成し、PMDAの承認を得ること。 PMDAが運用計画書の案を確定するための支援として、技術的知見や過去の業務実績に基づくアドバイスを行うこと。 運用体制、運用ツールを記載し、本システムと関連する他システム（Pegasus）の運用・保守事業者等との作業分担、実施手順等を明確にすること。 記載内容は、デジタル・ガバメント推進標準ガイドライン（以下「標準ガイドライン」という。）「第３編第９章　運用及び保守」で定義されている事項を踏まえたものとする。 本業務で開発した追加機能についても、改修リリース後は本計画書の対象とし、必要に応じて計画書を更改すること。	-
4	計画書・要領	運用実施要領の作成	運用計画書等と整合性を確保しつつ運用実施要領の案を作成し、PMDAの承認を得ること。 記載事項：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	-
5	計画書・要領	保守計画書の作成	定常時における月次の作業内容、想定スケジュール、障害発生時に想定される対応等を取りまとめた保守計画書の案を作成し、PMDAの承認を得ること。 PMDAが保守計画書の案を確定するための支援として、技術的知見や過去の業務実績に基づくアドバイスを行うこと。 保守と契約不適合責任の範囲内で実施する作業分担や、本システムと関連する他システム（Pegasus）の運用・保守事業者等との作業分担、実施手順等を明確にすること。 記載内容は、デジタル・ガバメント推進標準ガイドライン（以下「標準ガイドライン」という。）「第３編第９章　運用及び保守」で定義されている事項を踏まえたものとする。 本業務で開発した追加機能についても、改修リリース後は本計画書の対象とし、必要に応じて計画書を更改すること。	-
6	計画書・要領	保守実施要領の作成	保守計画書等と整合性を確保しつつ保守実施要領の案を作成し、PMDAの承認を得ること。 記載事項：コミュニケーション管理、システムドキュメント管理（設計書等）、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	-
7	障害発生時対応	インシデント管理	インシデント起票・記録・優先度付けを行い、対応状況のモニタリングや月次報告を実施する。	-
8	障害発生時対応	障害復旧対応（インシデント対応）	対応時間帯：平日9:30～18:00（行政機関の休日を除く）。時間外・休日は緊急度に応じて適宜対応をPMDAと相談。 初動対応時間：障害発生から30分以内にPMDA職員へ連絡し、応答を得ること。時間外に発生した場合は、翌営業日の9:30から30分以内に初動を開始する。 使用ツール：CloudWatch、各種監視ツール、ログ収集ツール、障害管理システムなどを活用して障害の検知・切り分け・対応を行う。 レポート対応：障害発生から1時間以内に状況報告を実施。復旧後は、障害日時・分類・内容・対応履歴などを含む要旨記録を作成し、PMDAに報告する。インシデントの分析（発生原因、影響度、過去の発生実績、再発可能性等）を行い、障害報告書と合わせて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。 SLA（復旧時間）：セキュリティに関するインシデントについて、4.5時間以内に復旧する割合を95%以上とする。暫定対応（データ修正、縮退運転、代替手段提供など）も復旧とみなす。その他インシデントについては、障害レベル及び初動対応も含め、契約締結後合意する。 教育・訓練：障害対応に必要なシステム知識・業務知識を有する要員を配置し、受託者の費用負担で教育を実施する。問合せ対応要員にも同様の教育を行う。 関係機関連携：PMDA、ソフトウェアベンダ、厚労省ヘルプデスクなどと連携。障害の一次切り分け後、必要に応じて各機関と調整・	-
9	障害発生時対応	データ維持管理業務	対象データ：新システムで取り扱う全データ（例：サーバの構成情報など）、トランザクションログ、各種操作ログ 保管期間：原則1年間（ログ類）、トランザクションログは最大30分前までの復旧を想定 保管方法：自動取得 データ形式：PDF（文書）、CSV（ログ、XML（定義情報） 対応内容：障害発生時にバックアップからリストアを実施 RPO/RTO：非機能要件定義書に準拠	-
10	障害発生時対応	アプリケーションプログラムの不具合対応	対応時間帯：平日9:30～18:00（ヘルプデスク提供時間内）。時間外・休日は緊急度に応じて適宜対応をPMDAと相談。 対応範囲：本システムのアプリケーション不具合。軽微な修正から暫定対応（データ修正等）まで含む。 SLA：障害復旧遵守率及び障害原因切分け遵守率に関しては、契約締結後合意する。 対応体制：平日日中はヘルプデスクが主体。時間外はPMDA職員が対応。必要に応じてアプリケーション開発業者と連携。 調査ツール：CloudWatch、操作ログ、DBトレース、構成管理台帳、設計書・ソースコード解析。 報告内容：障害日時、対象システム、障害分類、障害内容、対応内容、原因、暫定対応・恒久対応の有無。1時間以内に一次報告。 対応件数（月）：月間10～15件程度（想定）。うち、軽微な不具合対応が大半を占める。	-
11	障害発生時対応	ソフトウェア製品の不具合対応	■アプリケーションプログラムの不具合対応と同様	-
12	障害発生時対応	情報システムの設定変更	■アプリケーションプログラムの不具合対応と同様	-
13	障害発生時対応	大規模災害時対応	大規模災害等の発災時には、PMDAの指示を受けて、PMDAが提示する情報システム運用継続計画に基づく運用及び保守作業業務を実施すること。	Amazon RDS（Relational
14	障害発生時対応	バックアップからの復旧	特に指定なし。	
15	定常時対応	サポート対応	対応時間帯：平日9時30分～18時00分（行政機関の休日を除く）。 初動対応時間：問合せや作業依頼受付から60分以内に初動対応を開始する（初年度の設定。次年度以降は調整）。 保守体制：ヘルプデスク常駐要員による一次対応体制を基本とし、必要に応じてPMDA職員や開発ベンダと連携。 ツール・ナレッジ：CloudWatch、監視ツール、作業依頼管理表、設計書・手順書を活用。FAQやナレッジベースは整備中。 規制対応支援：NISC基準やPMDAの運用方針に基づき、セキュリティ対策や監査対応などの支援を実施。必要に応じて棚卸し・報告を行う。 SLA保証：問合せ回答率（80%以上）、障害原因切分け（80%以上）、障害復旧（95%以上）など、月次・年次で遵守状況を報告。 作成資料：ヘルプデスク業務手順書	-
16	定常時対応	計画停止	停止計画の整備：各システムの影響範囲を考慮し、横断的かつ影響最小化を目的とした停止計画を策定する。 関係者連携：PMDA職員、システム管理者、ベンダ等と事前に調整を行い、作業内容・スケジュールを共有する。 通知・報告：定期停止は毎月同タイミング（土日祝）で行うこととし、停止不要な際は別途通知とする。計画的な停止に関しては、「お知らせ機能」やメールを利用し、ユーザに通知すること。 リスク管理：停止に伴う業務影響、セキュリティリスク、復旧失敗リスク等を事前に洗い出し、回避策・対応策を計画に盛り込む。 復旧体制：停止作業後の復旧確認を含め、障害発生時の対応体制（ヘルプデスク・PMDA・ベンダ連携）を確保する。必要に応じてバックアップ取得・リストア手順も整備する。 教育・訓練：年次または半期で計画停止に関する手順確認・訓練を実施し、要員の対応力を維持する。	-
17	定常時対応	製品・クラウドサービスのアップデート（セキュリティパッチ等）の対応	提供頻度：緊急性の高いパッチは随時対応。 提供方法：PMDAとの協議の上、検証後に本番環境へ反映。アップデート対象はAWS等の公開情報に基づく。 検証体制：影響分析・検証を実施。 規制対応：NISCの統一基準群やJPCERT等の情報に準拠し、セキュリティインシデントの検討・報告・対応方針をPMDAに提示。 サポート体制：アップデートに伴うアプリケーション改修が必要な場合は、PMDAの指示を仰ぎ、保守工数内で対応。その他の作業は受託者負担。 教育・訓練：アップデート手順、影響分析、検証方法に関する教育を年1回以上実施。新規要員には随時教育を行う。	-
18	定常時対応	データ一括処理業務	【現状の想定では、データ一括処理業務は生じない想定。※下記内容は発生した場合の想定】 処理体制：ヘルプデスク要員が設計書・定義書を理解した上で対応。必要に応じてPMDA職員と連携し、手順書の作成・更新も行う。 バッファ対応：処理量の急増やエラー発生時に備え、再投入・エラー修正・一時保留などの柔軟な対応体制を確保する。 ツール・基盤：専用登録ツールは必要に応じて作成。 品質保証：投入データの属性確認、エラー検知・修正、再投入、作業ログの記録・報告を通じて品質を担保する。 レポート対応：月次・年度単位で処理結果を報告。統計表、作業ログ、棚卸調査結果などをPMDAへ提出する。	-
19	定常時対応	情報資産管理	管理対象範囲：各種ドキュメント、プログラムコード等、システムのデータベース内の全テーブル、出力帳票など多岐にわたる情報資産を対象とする。 管理方法：情報資産ごとにシステム的目的、業務的目的、運用での使用方法を整理し、指定様式にてPMDAへ提供する。 アクセス管理：ユーザアカウント・アクセス権限を年4回棚卸し、適切な管理を実施。OSユーザも含めて承認制で管理。 バックアップ：対象資産に応じて自動・手動で取得。トランザクションログの30分間隔取得などを含む。 インシデント対応：情報漏洩や紛失等の重大インシデントを未然に防止し、発生時は迅速にエスカレーション・報告・対応を行う。 教育・訓練：情報資産の取り扱いに関する教育を年1回以上実施。新規要員には随時教育を行う。 規制対応：NISCの統一基準群やJPCERT等の情報に基づき、棚卸し・リスク評価・対応方針の整理を行い、PMDAへ報告する。	-
20	定常時対応	情報システムの更改に関する情報提供変更要求管理作業	管理方法：課題管理・変更管理プロセスに基づき、変更要求の受付・進捗・対応状況を一元管理する。PMDAが承認するための情報提供も含む。 情報提供範囲：設計書、設定情報、改修内容、開発に必要なデータ、技術的質疑応答、リリース予定など、運用保守に関係する情報を対象とする。 変更要求対応：PMDAからの変更要求に対し、影響調査・対応方針の提示・受入テスト支援を行う。必要に応じてアプリケーション保守工数を使用。 ドキュメント整備：変更に伴う設計書・操作手順書・構成管理資料などを更新・作成し、PMDAと共有する。 関係者調整：開発業者（運用保守業者）、PMDA職員、運用保守要員間で密に連携し、情報共有・調整・マージ作業を円滑に進める。 教育・訓練：変更管理手順、影響調査方法、受入テスト支援に関する簡易的な教育を年1回以上実施。新規要員には随時教育を行う。	-
21	定常時対応	ライセンス許諾条件管理	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、ライセンス管理者にその旨を報告し、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。	-
22	定常時対応	アクセス管理	管理方法：サポートデスクで対応。本番環境、検証環境、ヘルプデスク要員などのアカウントを対象に、登録・更新・削除を適切に管理する。OSユーザについても同様に管理し、作成時はシステム管理者の承認を得る。 権限管理：利用者の業務内容に応じたアクセス権限を設定し、機密情報の保護を徹底する。検証環境や外部ユーザも含めて管理対象とする。 ログ・監査：アクセスログを常時取得・保存し、監査対応時にはログの抽出・整理・提示を行う。監査者からの質問には業務・システム両面から適切に回答する。 アカウント棚卸：年4回、ユーザアカウントの棚卸しを実施し、不要なアカウントの削除や権限の見直しを行う。	-
23	定常時対応	定期報告	報告頻度：月1回を基本とし、年度末に取りまとめて報告すること。 報告内容：サービスレベル遵守状況、稼働統計（性能推移含む）、問合せ件数、作業依頼件数、作業内容、障害対応履歴、要員管理（研修・工数）、情報システムの構成と運転状況、セキュリティ監視状況、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、情報システムの利用者サポート、教育・訓練状況、運用改善案など。 作成方法：各業務の記録・ログ・統計データをもとに、様式に沿って運用実績報告書・保守実績報告書を作成。インシデントレベルに応じて別様式で起票。 報告方法：月例の定期運用及び保守作業会議を開催し、運用及び保守作業報告書の内容を報告すること。必要に応じて関係部署にも共有。 フォーマット：各システムごとに異なるが、PMDAの了承を得た上で統合・変更可能。 関係者対応：報告内容に関する質疑応答、改善提案の説明、追加資料の提出などをPMDAと協議の上で対応する。 品質保証：月間の運用及び保守作業実績を評価し、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。 教育・訓練：報告作成手順、様式の理解、内容の精査に関する教育を月1で実施（次年度以降は頻度調整）。新規要員には随時教育を行う。	-
24	定常時対応	データの収集と報告	収集方法：本システム等からデータを抽出。必要に応じて手作業での補正や不整合調査も実施。 報告頻度：月次、四半期、年度、速報（月初8日前後）など、業務内容に応じて複数の報告タイミングを設定。 報告内容：申請件数、アクセス件数、統計処理結果、不整合データの分析結果など。PMDAの指示に応じて内容を調整。 品質管理：抽出データの正確性を確保するため、設計書・定義書を参照し、手順書に基づいて処理。不整合があれば原因調査・修正・再集計を実施。 提出先：PMDA担当者へ報告。必要に応じて部門別・品目別などの形式で提出。 フォーマット：統計表や報告書の様式はPMDA指定のものを使用。変更が必要な場合はPMDAと協議の上で対応。 教育・訓練：統計処理手順、ツール操作、報告様式の理解に関する教育を年1回以上実施。新規要員には随時教育を行う。	-
25	定常時対応	本番環境へのアプリケーションプログラムのリリース	特に指定なし	-
26	定常時対応	本番環境へのソフトウェア製品のリリース作業	特に指定なし	-
27	定常時対応	バックアップ管理	特に指定なし	Amazon RDS（Relational Database Service）
28	定常時対応	システム構成管理	特に指定なし	-
29	ユーザサポート業務	ヘルプデスク	対応時間帯：平日9時30分～18時00分（行政機関の休日を除く）。 初動対応時間：問合せ受付から60分以内に初動対応を開始する。 対応チャネル：メール・電話。必要に応じて対面相談も含む。 FAQ・ナレッジ：問い合わせ内容を記録・分類し、初年度は月次でFAQ候補を抽出・整理（次年度以降4半期等、問い合わせの量を鑑みて調整）。将来的なナレッジベース整備を視野に入れる。 エスカレーション：厚労省ヘルプデスクやPMDA職員への手動エスカレーションを都度判断で実施。 レポート対応：月次で問合せ件数、対応状況、FAQ候補、対応時間などをPMDAへ報告。 教育・研修：年1回、システム知識・業務知識に関する簡易研修を受託者負担で実施。新規要員には随時教育を行う。 SLA：問合せ回答率80%以上（翌営業日以内）を目標とし、月次で遵守状況を報告。	-
30	ユーザサポート業務	業務運用支援作業	支援範囲：本システムの運用に係る支援。 対応時間帯：平日9時30分～18時00分（行政機関の休日を除く）。 支援方法：対面相談（必要に応じて）、メール・電話対応、作業依頼への対応、データ投入・抽出、マスタメンテナンスなどを通じて業務支援を行う。 改善活動：業務支援を通じて得られた知見をもとに、運用改善案を提示。運用サービスレポートにて提案・報告を行う。 ドキュメント整備：作業手順書、FAQ、統計表、報告様式などを整備・更新し、再利用性と品質を確保する。 教育・訓練：業務知識・システム知識に関する教育を年1回以上実施。新規要員には随時教育を行い、業務理解を深める。	-
31	ユーザサポート業務	利用者教育支援	教育支援内容：システム操作方法、申請手順、エラー対応、FAQの活用方法など、業務に必要な基本操作と運用ルールについて、PMDAが教育を実施する際のマテリアル作成等を行う。 対象者：PMDA職員、行政ユーザ（都道府県・厚労省）、外部ユーザ（申請者）など、システム利用者全般。 教材提供：操作マニュアル、FAQ集、動画教材、画面キャプチャ付き手順書などを提供。必要に応じて内容を更新・改訂する。	-
32	ユーザサポート業務	利用者からの定型変更対応	対応時間帯：平日9時30分～18時00分（行政機関の休日を除く）。 対応件数（月）：月数十件程度の定型対応が想定される。（運用状況に合わせて適宜協議） 対応方法：メール・電話・対面相談（必要に応じて）を通じて受付。作業依頼に基づき、マスタメンテナンス、データ投入・抽出、削除取消などを手順書または設計書に基づいて実施。 SLA：問合せ回答率80%以上（翌営業日以内）、障害復旧率95%以上（4.5時間以内）などのSLAに準拠。月次で遵守状況を報告。	-
33	監査	システム監査対応	対応範囲：内部監査（監査室）および外部監査（監査法人）に対し、監査証跡、各種ログ、ユーザ一覧、構成情報などを取得・整理・提示する。必要に応じて事前打ち合わせやヒアリングにも出席する。 対応頻度：年1回以上の定期監査に加え、随時実施される監査にも対応。監査準備・報告・改善対応まで含める。 対応形式：対面・オンライン・文書提出など、監査者の要望に応じた形式で対応。監査資料は共有フォルダ等で管理。 監査対象：本システム、ファイルサーバ、ログ管理システム、アクセス管理台帳など、運用保守対象の全システム。	-
34	監査	セキュリティ監査対応	対象規格例：NISC（内閣官房情報セキュリティセンター）の「政府機関等のサイバーセキュリティ対策のための統一基準群」、JPCERT、JVN、経済産業省のネットセキュリティ関連指針などを参照し、監査対応を実施する。 ログ・証跡提供：監査者の求めに応じて、アクセスログ、操作履歴、構成変更履歴、ユーザ一覧、バックアップ記録などの証跡を抽出・整理し、提示する。必要に応じてログの保管期間（1年）や取得方法も説明する。	-
35	運用及び保守の引継ぎ	情報システムの更改に関する情報提供	提供内容：更改対象システムの構成情報、運用手順書、アクセス管理台帳、障害対応履歴、変更管理履歴、バックアップ方針、SLA項目、保守契約範囲、質疑応答など 対応形式：文書（Excel/Word/PDF）、口頭説明、対面会議、オンライン会議（Teams等）、必要に応じて画面共有や操作デモを実施 対象領域：各種プログラムコード含む、運用・保守対象とする全システム 頻度：更改プロジェクトの各フェーズ（要件定義、設計、テスト、リリース）に応じて随時。最低でも四半期に1回の情報提供を実施 追加支援：設計書の読み解き支援、旧環境との差分説明、マスタデータ移行支援、テスト支援、リリース後の初期運用支援（最大1ヶ月）	-
36	運用及び保守の引継ぎ	更改を伴わない事業者の交代に伴う前事業者からの引継ぎ	対応内容：前事業者と協業し、引継計画書を作成しPMDAの承認を得る。引継の進捗は定期的にPMDAへ報告し、引継完了後は前事業者と協業して引継結果報告書を作成する。保守・運用計画書や実施要領作成後に引き継がれた事項については、適宜、各資料に反映させること。 対応形式：対面協議、オンライン会議（Teams等）、文書提供（Word/Excel/PDF） 作成資料：引継計画書、引継進捗報告書、引継結果報告書 対応期間：仕様書に準ずる	-
37	運用及び保守の引継ぎ	更改を伴わない事業者の交代に伴う次事業者への引継ぎ	支援内容：現行運用・保守業務の内容説明、手順書・設計書の提供、障害対応履歴の共有、作業経緯、残存課題の共有、本業務で作成した開発・テストツールの引継、SLA項目の説明、各種ツールの操作方法の説明 対応形式：対面説明、オンライン会議（Teams等）、文書提供（Word/Excel/PDF）、画面共有による操作デモ 提供資料：運用手順書、保守手順書、構成管理台帳、アクセス管理台帳、障害対応履歴、変更管理履歴、FAQ、月次報告書テンプレート 対応期間：引継ぎ開始から1ヶ月間を標準とし、必要に応じて延長（最大2ヶ月） 追加支援：新事業者による初期運用期間中のQA対応、操作支援、資料補足、PMDAとの調整支援	-
38	契約期間終了後の措置	撤去・搬出作業	本システムはクラウド基盤上に構築されていることから、基本的に設置機器等の撤去・搬出作業は想定していない。 また、利用しているクラウドサービスは次期運用業務において引き続き利用できる条件とすること。 本業務の契約期間終了後も継続してPMDAがクラウドサービスを利用可能となるよう必要な措置をすること。	-
39	契約期間終了後の措置	データ引継業務	本業務において作成した全てのデータをPMDAの求めに応じて提出すること。 また、引継情報が漏えいしないよう、厳重に情報セキュリティ管理を行うこと。	-
40	契約期間終了後の措置	データ消去作業	本業務の契約期間終了後、本業務に使用した受注者が所有する端末及びデータ記憶媒体等に保管されているPMDAに関する情報が一切流出することがないよう、速やかに受注者の負担と責任において物理破壊又はデータ抹消による機器内のデータ消去を行うこと。 クラウドサービスについてはISMAPで規定された方法でデータを消去し、それが正しく運用されているか第三者による監査により証明されていること	-
41	セキュリティ対策	ログ取得及びログ管理	特に指定なし	Amazon CloudWatch
42	セキュリティ対策	暗号化及び電子署名	特に指定なし	Amazon RDS（Relational Database Service）
43	セキュリティ対策	ソフトウェアの脆弱性対策	特に指定なし	Amazon Inspector
44	セキュリティ対策	不正プログラム対策	特に指定なし	Amazon GuardDuty
45	セキュリティ対策	サービス不能攻撃対策	特に指定なし	Amazon GuardDuty
46	セキュリティ対策	標的型攻撃対策	特に指定なし	Amazon GuardDuty
47	監視	死活監視	特に指定なし	Amazon CloudWatch
48	監視	稼働状況監視	特に指定なし	Amazon CloudWatch
49	監視	ネットワーク監視	特に指定なし	Amazon CloudWatch
50	監視	性能監視	特に指定なし	Amazon CloudWatch
51	監視	セキュリティ監視	特に指定なし	Amazon CloudWatch
52	監視	ログ管理	特に指定なし	Amazon CloudWatch
53	監視	データ監視	特に指定なし	Amazon CloudWatch
54	監視	防犯監視	特に指定なし	-