ICMRAウェブサイトの運用支援業務

調達仕様書

令和6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) 調達案件名

ICMRA ウェブサイトの運用支援業務

(2) 調達の背景

1 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、International Coalition of Medicines Regulatory Authorities (以下「ICMRA」という。)ウェブサイト(http://www.icmra.info/)の運用を行っている。運用業務として必要なシステム監視、ユーザー管理、保守管理、インシデント発生時対応等を行うには、専門的な知識及び技術が必要であるため、運用支援業務を外部委託したい。

2 国の行政情報システムについては、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」(2021 年(令和 3 年)9 月 10 日デジタル社会推進会議幹事会決定)において、「『世界最先端IT国家創造宣言・官民データ活用推進基本計画」(平成 29 年 5 月 30 日閣議決定)及び『デジタル・ガバメント推進方針」(平成 29 年 5 月 30 日高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議決定)では、クラウド・バイ・デフォルト原則、すなわち、政府情報システムを整備する際に、クラウドサービスの利用を第一候補とすること」とされており、本システムについても、クラウドサービスの利用を前提とした構築・運用が必要となっている。

(3) 目的及び期待する効果

1 本調達は、ICMRA ウェブサイト(以下「本システム」という。)の円滑な運用に資するため、関連する業務を運用支援業務として外部委託することを目的とする。

2 クラウドサービスを利用することにより情報セキュリティ水準の向上や運用・保守コストの削減等に資することを目的とする。

(4) 用語の定義

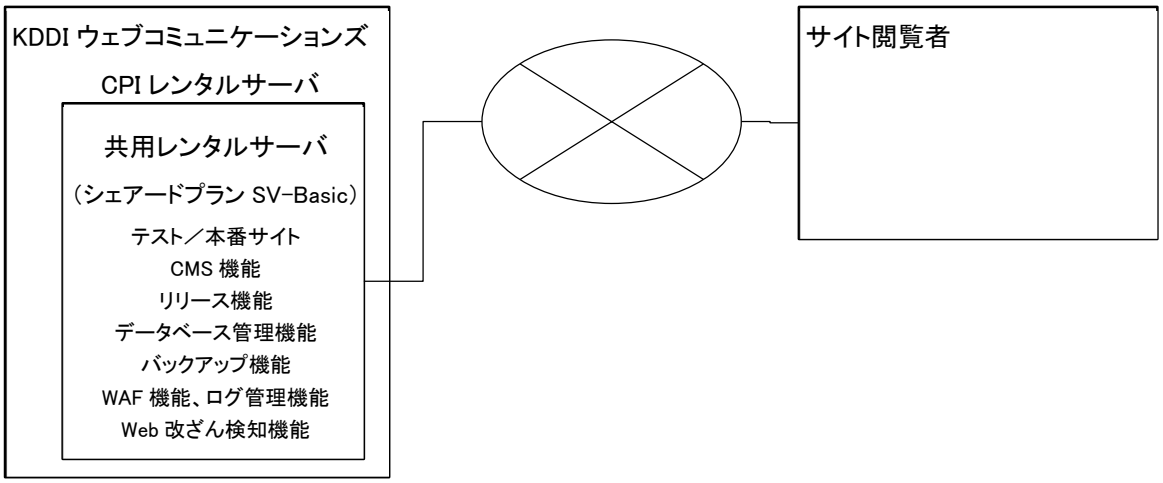
表 1-1 用語の定義

No.	用語	説明
1	運用支援業務	PMDA 国際部にて管理しているICMRA ウェブサイトの運用のためにシステム監視、ユーザー管理、保守管理、インシデント発生時対応等を行う業務。
2	ICMRA ウェブサイト	ICMRA で合意された声明・報告書等を一般に公開するための情報システム。
3	SLCP-JCF2013	ソフトウェアを中心としたシステムの開発及び取引のための共通フレーム体系(2013 年版)のこと。
4	SLA	サービスレベル合意書(Service Level Agreement)の略称。サービスを提供する側とその利用者の間に結ばれるサービスのレベル(定義、範囲、内容、達成目標等)に関する合意書のこと。
5	クラウドサービス	事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキ

		ュリティに関する十分な条件設定の余地があるもの。この構成要素として、SaaS(Software as a Service)、PaaS(Platform as a Service)、IaaS(Infrastructure as a Service)が存在する。
6	クラウドサービス事業者	クラウドサービスを提供する事業者又はクラウドサービスを用いて政府機関の情報システムを開発・運用する事業者。
7	クラウドサービスプロバイダ	クラウドサービス事業者のうち、クラウドサービスを提供する事業者。
8	IaaS (Infrastructure as a Service)	CPU、メモリ、ストレージ、ネットワーク等のハードウェア資産をサービスとして提供するクラウドサービス。
9	PaaS (Platform as a Service)	オペレーティングシステムや実行環境をサービスとして提供するクラウドサービス。
10	SaaS (Software as a Service)	アプリケーションやデータベースをサービスとして提供するクラウドサービス。
11	クラウド	クラウドサービスに基づきクラウドサービスプロバイダから提供される物理的又は仮想的な全てのリソース。

(5) 業務・情報システムの概要

ICMRA ウェブサイトは、KDDI ウェブコミュニケーションズの共用レンタルサーバ(シェアードプラン SV-Basic)(以下「SV-Basic」という。)で稼働するウェブサイト。SV-Basic に用意されているウェブサイトの公開・管理に必要な機能一式(テスト／本番サイト、CMS 機能、テストサイトから本番サイトへのリリース機能、データベース管理機能、バックアップ機能、WAF 機能、ログ管理機能、Web 改ざん検知機能)を利用してサイトコンテンツの作成、リリースを行っている。



(6) 契約条件

ア 契約期間

契約締結日から 2029 年 3 月 31 日まで。

イ 契約形態

請負契約形態とし、検収や支払方法等は契約書にて定める。

（7）作業スケジュール

1　受注者は、契約締結日から運用業務の開始までに本情報システムの運用業務を実施するための準備を実施し、必要な情報について PMDA（または前受注者）より引継ぎを受けること。

2　本業務に係る想定スケジュールの概要は、別紙2「作業スケジュール」のとおりとする。なお、この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注者が検討の上、実施計画書に記載すること。

3　Drupal バージョンアップ及び Drupal のテーマ変更は、Drupal のサポート期限及びリリース・スケジュールやサイトの更新予定を考慮して PMDA と協議して決定するものとする。Drupal バージョンアップは契約期間中に最大 3 回、Drupal のテーマ変更は最大 1 回実施するものとする。

4　サーバ移行は、現行及び新レンタルサーバのプラン（現行のプランは SV-Basic）の提供スケジュール及び Drupal のシステム要件の充足状況を考慮して PMDA と協議して決定するものとする。サーバ移行は契約期間中に最大 1 回実施するものとする。

（8）担当課室・連絡先

本調達仕様書に関する問い合わせ先は以下のとおり。

〒100-0013

東京都千代田区霞が関 3-3-2 新霞が関ビル

独立行政法人 医薬品医療機器総合機構

国際部国際規制調和調整課　巽、髙橋、勝田

03（3506）9456

Email：Kokusaibu-chotatsu●pmda.go.jp

※●を＠（半角）に置き換えて下さい。

2. 当該調達及び関連調達に関する事項

（1）調達の単位、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とおりである。

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

No.	調達案件名	調達の方式	実施時期	補足
1	ICMRA ウェブサイトのドメイン更新	随意契約	2024 年 1 月 22 日から 2025 年 1 月 21 日	契約済 ドメイン名使用権 DNS サービス《お名前.com》提供
2	ICMRA ウェブサイトのドメイン更新	随意契約	2025 年 1 月 22 日から 5 年間	ドメイン名使用権 DNS サービス《お名前.com》提供
3	ICMRA ウェブサイトのレンタルサーバ	随意契約	2023 年 8 月 1 日から 2024 年 7 月 31 日	契約済 レンタルサーバ《シェアードプラン SV-Basic》の提供

No.	調達案件名	調達の方式	実施時期	補足
4	ICMRA ウェブサイトのレンタルサーバ	随意契約	2024 年 8 月 1 日から 5 年間	レンタルサーバ《シェアードプラン SV-Basic》の提供

（2）調達案件間の入札制限

なし

3. 情報システムに求める要件に関する事項

本調達の実施に当たっては、別紙 1 から 5 の各要件を満たすこと。

4. 作業の実施内容に関する事項

（1）作業の内容

ア　運用・保守に係る作業の内容

受注者は、本調達仕様書に記載された作業内容や各要件（「別紙 3 業務要件」等）を参照の上、以下に関し必要な作業を実施すること。

（ア）準備作業

1　受注者は、運用・保守業務の開始までに、本情報システムの円滑な運用・保守業務の実施に必要な準備作業として、運用・保守業務に必要な什器等の準備、回線引込等を行うこと。

2　受注者は、運用・保守業務の開始までに、運用・保守準備作業に関する準備計画書を作成し、PMDA の承認を受けること。

3　受注者は、運用・保守準備作業が完了した後、準備完了報告書を作成し、PMDA の承認を受けること。

（イ）実施計画書及び実施要領の作成

受注者は、別紙 1 から 5 に基づき、実施計画書を作成し、PMDA の承認を受けること。

（ウ）定常時対応

1　受注者は、「別紙 3 業務要件」に示す運用・保守業務を行うこと。具体的な実施内容・手順は実施計画書等に基づいて行うこと。

2　受注者は、「別紙 4 システム運用管理基準」を参照のうえ、以下の内容について月次で運用・保守作業報告書を取りまとめること。

（1）運用・保守業務の内容や工数、作業時間等の作業実績状況
（2）サービスレベルの達成状況
（3）サービスレベル関連実績データと分析・評価及び対策
（4）情報システムの構成と運転状況（情報セキュリティ監視状況を含む）
（5）情報システムの定期点検状況（別紙 2、4、5 参照）
（6）情報システムの利用者サポート、教育・訓練状況
（7）リスク・課題の把握・対応状況
（8）問合せ管理運用状況（サービスデスク稼働状況）（「別紙 4 システム運用管理基準」参照）
（9）インシデント管理状況（「別紙 4 システム運用管理基準」参照）
（10）問題管理状況（「別紙 4 システム運用管理基準」参照）
（11）変更管理状況（「別紙 4 システム運用管理基準」参照）

（12） 脆弱性管理（「別紙 4 システム運用管理基準」参照）

（13） データ外部保管状況

（14） クラウドサービスを利用するとき、その利用状況（リソース使用量の変動、構成変更の実施状況等を含む。なお、クラウドサービスプロバイダから提供される管理ツール等により出力可能な情報があれば、当該情報を管理ツール等から出力したそのままの形で添付することとしても差し支えないが、グラフ化等、参照性の担保には配慮すること。）

3 受注者は、月間の運用・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。

4 受注者は、運用・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。但し、PMDA が認める場合は、書面による報告のみとする。

（エ）レンタルサーバの運用支援、保守

1 KDDI ウェブコミュニケーションズ（以下「レンタルサーバ事業者」という。）がレンタルサーバを運用・保守する。

2 レンタルサーバが提供するサービスを活用してウェブサイトを運用・保守する。

3 レンタルサーバが提供するサービスに問題や確認事項がある場合は、受注者がレンタルサーバ事業者への問い合わせ、折衝、調整などを行うこと。

※PMDA が KDDI ウェブコミュニケーションズのレンタルサーバ《シェアードプラン SV-Basic》を契約するため（「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」参照）、レンタルサーバのサービス提供は、本調達の対象外。

（オ）ウェブサイトのセキュリティ維持

以下のセキュリティ維持対応を行うこと。

1 HTML ファイル 30 ページ分の改ざん検知対応

2 CMS（Drupal）のセキュリティ更新プログラム（新バージョン）の適用

3 PHP のバージョンアップに伴う設定変更（PHP の新バージョンはレンタルサーバ事業者が提供する）

4 監査対応（6（4）6 参照）

（カ）更新されたコンテンツの本番サイトへのリリース

1 PMDA がテストサイトで作成・更新したコンテンツの本番サイトへのリリース作業

2 更新頻度は 3 回/月、作業工数は 10 人日/年程度の想定とする。

（キ）問い合わせ対応

1 コンテンツ作成・改修、その他に関する問い合わせ対応や技術支援など

2 作業工数は 5 年間で 40 人日程度の想定とする。

（ク）Drupal バージョンアップ及びサーバ移行

Drupal バージョンアップとサーバ移行は、同時に実施することでも、別々に実施することでもよい。

① 調査

Drupal の新バージョンの変更点及びバージョンアップ方法／新レンタルサーバのプランに関する情報を収集し、 調査結果報告書及び作業項目とスケジュール（WBS）を記載した移行計画書を作成し、PMDA の承認を受けること。

② 設計

受注者は、Drupal の新バージョン／新レンタルサーバのプランに対応した設計書及び移行手順書を作成し、PMDA の承認を受けること。

③ 構築

受注者は、設計書及び移行手順書に基づき、検証環境を Drupal の新バージョンにバージョンアップ／サーバ移行し、検証環境の移行作業結果を PMDA に報告すること。

④ テスト

受注者は、テスト仕様書を作成し、PMDA の承認を受けること。

受注者は、テスト仕様書に基づいてテストを実施し、テスト結果報告書を作成して PMDA にテストの実施結果を PMDA に報告すること。

⑤ 受入テスト

受注者は、PMDA が受入テストを実施するにあたり、テストの実施方法などの情報提供などの支援を行うこと。

受注者は、PMDA から報告される受入テスト結果の内容を取りまとめ、必要に応じて指摘事項への対応を行うこと。

⑥ 移行

受注者は、移行手順書に基づいて本番環境を Drupal の新しいバージョンにバージョンアップ／サーバ移行し、本番環境の移行作業結果を PMDA に報告すること。

⑦ 初期対応

受注者は、移行後に不具合が発生した場合の不具合修正、バージョンアップによるコンテンツの乱れが発生した場合のコンテンツ及びテーマの修正対応を行うこと。

(ケ) 障害・情報セキュリティインシデント発生時及び大規模災害等の発災時の対応

1 受注者は、インシデントについて、発生日、内容、対応状況等と記録・整理すること。

2 受注者は、インシデント発生時の 1 次切り分け業務（検知、発生箇所の特定及び運用・保守に関係する事業者との連携による原因調査）を速やかに行うこと。

3 受注者は、情報システムの障害等インシデント発生時（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 4 システム運用管理基準 4．2インシデント管理」に示す「インシデント報告書(ひな型)」を参照の上、インシデント発生時運用業務（検知、障害発生箇所及び原因調査、応急措置、復旧確認、報告等）を行うこと。なお、インシデントには、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・手順は情報システムごとのインシデント管理プロセス手順書に基づいて行うこと。（インシデント管理プロセス手順書がない場合は、作成すること） また、情報セキュリティインシデントの場合は、「PMDA 情報セキュリティインシデント対処手順書」を参照の上、インシデント発生対応を実施のこと。

4 受注者は、情報システムのインシデント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。

5 受注者は、運用業務に従事する要員に対して、年1回以上のセキュリティの定期教育を実施すること。また、新たに要員が参画する場合は、参画時にセキュリティ教育を実施すること

(コ) 運用・保守作業の改善提案

受注者は、年度末までに年間の運用・保守実績を取りまとめるとともに、実施計画書、運用・保守手順書に対する改善提案を行うこと。

(サ) 引継ぎ

1 受注者は、現行運用・保守事業者から運用・保守に必要な事項の引継ぎとして、運用監視作業エリアの

引継、サービスデスクの引継、システム資源及びデータの引継を受け、現行事業者から提供される資料（運用・保守作業の計画書や報告書、運用・保守設計書及び運用・保守手順書等の一覧）を基に自主的に業務習熟を行うこと。

現行運用・保守事業者からの引継作業は受注者の負担と責任において実施すること。

2　受注者は、本調達に係る契約期間終了後、受注者と異なる事業者が本情報システムの運用・保守業務を受注した場合には、次期運用・保守事業者に対し、作業経緯、残存課題等下記項目についての引継ぎを行うこと。

・問合せ、障害等の対応及び管理に関する手法・手順
・システム運用・保守マニュアル、運用・保守業務マニュアル
・仕掛中の項目一覧及びその進捗状況
・過去の問合せ、障害等の実績及びその対応方法
・バックログ・未対応作業一覧及びその対応(案)
・その他業務を引継ぐ上で必要と思われる事項

3　受注者は、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やデータの提供及び質疑応答等の協力を行うこと。

受注者は、移行日までに設計・開発事業者等からの引継ぎを受け、本業務への影響を調査し、手順書の見直し・整備、教育等の必要な対応を実施すること。準備作業が完了した後、完了を報告し、PMDA の承認を受けること。

設計・開発事業者等からの引継及び準備作業は受注者の負担と責任において実施すること。

4　受注者は、PMDA が本システムの改修を行う際には、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やデータの提供及び質疑応答等の協力を行うこと。

受注者は、移行日までに設計・開発事業者等からの引継ぎを受け、本業務への影響を調査し、手順書の見直し・整備、教育等の必要な対応を実施すること。準備作業が完了した後、完了を報告し、PMDA の承認を受けること。

設計・開発事業者等からの引継及び準備作業は受注者の負担と責任において実施すること。

イ　契約金額内訳及び情報資産管理標準シートの提出に係るその他の作業の内容

受注者は、契約金額の内訳を記載したエクセルの電子データを契約締結後速やかに提出すること。

（2）成果物の範囲、納品期限等

ア　成果物

本業務の成果物を次の表に示す。ただし、納入成果物の構成、詳細、スケジュールについては、受注後、PMDA と協議し取り決めること。

なお、設計・開発によって納品されるドキュメントについては、記載レベル、記載内容等を明らかにし、メンテナンス性を考慮したものとすること。

表 4-1 工程と成果物

項番	工程	納入成果物（注 1）	納入期日
1	準備作業	・準備計画書 ・準備完了報告書	運用開始日

項番	工程	納入成果物（注 1）	納入期日
2	計画	・実施計画書（注 2） ・情報セキュリティ管理計画書（注 3） ・契約金額内訳	契約締結日から 2 週間以内
3	運用・保守	・運用・保守作業報告書（月次・年次・スポット等） ・改善提案書 ・システム運用マニュアル(注4) ・システム関連ドキュメント	令和 11 年 3 月 23 日 （※必要に応じて随時提出）
4	Drupal バージョンアップ、サーバ移行	・調査結果報告書 ・移行計画書 ・設計書 ・移行手順書 ・移行作業結果報告書(検証環境) ・バージョンアップ済み/移行済み検証環境 ・テスト仕様書 ・テスト結果報告書 ・受入テスト結果報告書 ・移行作業結果報告書(本番環境) ・バージョンアップ済み/移行済み本番環境 ・修正済みコンテンツ/テーマ	令和 11 年 3 月 23 日 （※必要に応じて随時提出）
4	引継ぎ	・引継計画書 ・引継資料 ・引継結果報告書	令和 11 年 3 月 23 日
5	その他	・実施要領に基づく管理資料 ・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 ・契約不適合責任に係る保有情報の一覧 ・成果物一覧 ・最終報告書	令和 11 年 3 月 23 日 （※必要に応じて随時提出）

注1　納入成果物の作成にあたっては、SLCP-JCF2013（共通フレーム 2013）を参考とすること。

注2　実施計画書に記載する事項

（ア）プロジェクトの目標

（イ）プロジェクトのスコープ

（ウ）体制図（責任者・契約担当・再委託の有無、情報セキュリティ責任者・情報セキュリティ技術担当窓口を含む）

（エ）作業分担（PMDA との役割分担を含む）

（オ）SLA

（カ）マスタスケジュール（運用・保守の場合は年間作業スケジュール）

（キ）WBS（運用・保守の場合は N/A）

（ク）納入成果物

（ケ）提案事項・改善計画

（コ）前提条件・制約事項

（サ）実施要領

①　コミュニケーション管理要領（通常時・緊急時の連絡方法）

② 進捗管理要領・リスク管理要領（報告頻度、報告様式、管理方法）
③ 課題管理要領・変更管理要領（様式、承認フロー、管理方法）
④ 構成管理要領、文書管理要領（受領資料の管理方法）
⑤ 品質管理要領（管理方法）

注3 情報セキュリティ管理計画書に記載する事項
（ア）ISMS 等認証取得
（イ）情報管理に関するルール（社内規程明示等）
（ウ）情報管理体制
（エ）情報セキュリティインシデント対処方法
（オ）PMDA 情報の取扱い（目的外使用・意図しない変更を防止する方法を含む）
（カ）メンバのスキル・資格等
（キ）自主点検の実施
（ク）業務環境のセキュリティ
（ケ）レポート体制
（コ）再委託による履行保証措置
（サ）緊急連絡方法
（シ）教育・研修の実施

注4 システム運用上、運用支援要員の行うべき業務内容及び操作手順に関するマニュアルとし、全対象システムについて次の内容を盛り込んだものとする。
(ｱ)ジョブ一覧、(ｲ)起動・停止手順、(ｳ)バックアップ手順、(ｴ)リカバリ手順、(ｵ)障害監視手順、(ｶ)障害対応手順、(ｷ)ログ確認手順、(ｸ)性能監視手順、(ｹ)設定変更手順、(ｺ)ユーザ管理手順、(ｻ)マスタの更新及びそれに伴うデータ修正手順、(ｼ) (ｱ)～(ｻ)の他、本業務の適切な履行のために運用支援要員が準拠すべき内容を網羅した手順書等

イ 納品方法

1 成果物は、全て日本語で作成すること。ただし、日本国においても、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 用字・用語・記述符号の表記については、「公用文作成の考え方（建議）（令和4年1月7日文化審議会）」に準拠すること。
3 情報処理に関する用語の表記については、原則、日本産業規格（JIS）の規定に準拠すること。
4 成果物は電磁的記録媒体（CD-R 等）により作成すること。また、PMDA が要求する場合は紙媒体でも納品すること。紙媒体の納品部数については、PMDA と協議すること。ただし、ソフトウェア、ソースコード等は外武電磁的記録媒体（CD-R など）のみとする。
5 紙媒体での納品を求める場合の用紙のサイズは、原則として日本産業規格A列4番とするが、必要に応じて日本産業規格A列3番を使用すること。
6 厚さ 15 ㎜程度のバインダー1 部に磁気媒体 2 部と成果物一覧（紙）を綴り、背表紙 に案件名、受注業者名、納入年月日を記載すること。
7 電磁的記録媒体による納品について、ファイルは Microsoft 365 で読み込みが可能なファイル形式で作成すること。 ただし、左記ファイル形式で納品が困難な場合は、PMDA と事前に協議の上、PDF のファイル形式で作成すること。ただし、PMDA が他の形式による提出を求める場合は、協議の上、これに応じるこ

と。なお、受注者側で他の形式を用いて提出したいファイルがある場合は、協議に応じるものとする。

8 現存するドキュメント等を変更する必要がある場合はそれらを修正することとし、修正点が分かるように表記すること。

9 納品したドキュメントに修正等があった場合は、紙については、それまでの変更内容を表示するとともに変更履歴と修正ページ、外部電磁的記録媒体については、それまでの変更内容及び修正後の全編を速やかに提出すること。

10 納品後、PMDA 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品すること。

11 成果物の作成に当たって、特別なツールを使用する場合は、PMDA の承認を得ること。

12 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。新規の開発ツール等を使用する場合、又はライセンスの追加が必要となる場合は、本稼働後5年間のライセンス及びメディアを納入すること。

13 成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。

14 電磁的記録媒体により納品する場合は、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、成果物に不正プログラムが混入することのないよう、適切に対処すること。なお、対策ソフトウェアに関する情報(対策ソフトウェア名称、定義パターンバージョン、確認年月日)を記載したラベルを貼り付けること。

15 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。

16 報告書、計画書等の成果物の記載様式については、記載様式案を PMDA に提示すること。PMDA は、案について受注者と協議の上、決定する。

17 成果物の作成及び納品に当たり、内容、構成等について PMDA が指摘した場合には、指摘事項に対応すること。

ウ 納品場所

原則として、成果物は次の場所において引渡しを行うこと。ただし、PMDA が納品場所を別途指示する場合はこの限りではない。

〒100-0013
東京都千代田区霞が関 3-3-2 新霞が関ビル
独立行政法人 医薬品医療機器総合機構
国際部国際規制調和調整課

5. 作業の実施体制・方法に関する事項

(1) 作業実施体制

受注者は、本業務に係る要員の役割分担、責任分担、体制図等を実施計画書の一部として作成し、PMDA に報告するとともに、承認を得ること。また、受注者は、必要な要員の調達を遅滞なく実施し、体制図等の要員配置関連資料を確定すること。

1 プロジェクトマネジメントに係る、品質管理・進捗管理・セキュリティ管理・リスク管理等の必要な機能を、体制に組み込むこと。

2 作業体制の品質確保のため、本業務の運用責任者・リーダーは業務開始から業務終了まで継続して遂行すること。交代する場合は同等以上の要員が担当するものとし、事前に PMDA の承認を得ること。

3　受注者は、PMDA 側やその他関連事業者を含めた全体の体制・役割を示した上で、プロジェクトの推進体制及び本件受注者に求める作業実施体制を PMDA と協議の上定めること。また、受注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。

4　受注者は、インシデント発生時などの連絡体制図を PMDA と協議の上定めること。

（2）管理体制

1　本業務の実施に当たり、PMDA の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、当該品質保証体制が書類等で確認できること。

2　本システムに PMDA の意図しない変更が行われる等の不正が見つかった時（不正が行われていると疑わしい時も含む）に、追跡調査や立入検査等、PMDA と受注者が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。

3　当該管理体制を確認する際の参照情報として、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。

（3）作業要員に求める資格等の要件

1　Web ページ制作技術、及び CMS（※1）に関する専門的な知識を有していること。

2　Web ページ制作技術、及び CMS（※1）に関して取扱い経験及び専門的な技術知識を有し、現場担当者に対して適切な応答速度で、有効な助言、指示を与える者を配置すること。

3　クラウドサービス及び CMS の環境構築（※2）に関して取扱い経験及び専門的な技術知識を有していること。

4　PMDA にて ICMRA ウェブサイトの設計書等を閲覧し、内容を十分理解していること。

※1 Drupal 固有の専門的な取扱経験及び知識は問わないが、資料を参照するなどして1週間程度で問い合わせ対応ができるスキルを有していること。なお、緊急を要する作業（脆弱性対応のための Drupal のバージョンアップ作業）は運用手順を参照して実施することができる。

※2 ICMRA ウェブサイトが使用するクラウド環境や Drupal 固有の専門的な取り扱い経験及び知識は問わないが、資料を参照するなどして計画を立て、計画通りに実施できるスキルを有していること。

（4）作業場所

1　本業務の履行状況を監督するため、必要に応じて PMDA 担当者が、受注者の作業場所やデータ保管場所の立入調査を行えることとする。ただし、データの保管にクラウドサービスを利用している等の理由により、データの保管場所への立入調査が困難な場合については、クラウドサービス業者との契約内容にセキュリティ上の問題がないことの説明の聴取をもって、立入調査に代えることができることとする。

2　本業務の作業場所及び作業に当たり必要となる設備、備品及び消耗品等については、受注者の責任において用意すること。また、必要に応じて PMDA が現地確認を実施することができるものとする。

3　本業務の作業場所及びデータの保管場所は、日本国内の PMDA が承認した場所とすること。

4　PMDA 内での作業は、必要な規定の手続を実施し承認を得ること。

（5）作業の管理に関する要領

1　受注者は、PMDA が承認した運用実施計画書に基づき、運用・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。

2 PMDA が依頼した場合、受注者は作業の進捗状況等を報告するため、PMDA の担当職員と会議を行うこと。

3 当該会議の開催の都度、3 営業日以内に議事録を作成、関係者に内容の確認を行った上で、PMDA の担当職員の承認を得ること。

4 情報漏えい及び作業計画の大幅な遅延等の問題が生じた場合は、PMDA のプロジェクト責任者又は窓口担当者にその問題の内容について報告すること。

6. 作業の実施に当たっての遵守事項

（1）機密保持、情報・資料の取扱い

1 受注者は、受注業務の実施の過程で PMDA が提供した情報・資料(公知の情報を除く。以下同じ。)、他の受注者が提示及び作成した情報・資料を、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えい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。なお、PMDA が提供した情報、資料を第三者に開示する必要がある場合は、事前に協議の上、承認を得ること。

2 受注者は、本受注業務を実施するに当たり、PMDA が提供した情報・資料については管理台帳等により適切に管理し、かつ、以下の事項に従うこと。

- 複製はしないこと。
- 受注者組織内に移送する際は、暗号化や施錠等適切な方法により、情報セキュリティを確保すること。また、PMDA との調整等に必要な場合及び返却時以外は原則として、受注者組織外に持ち出さないこと。
- 個人情報等の重要な情報が記載された情報・資料に関しては、原則として社外に持ち出さないこと。
- 受注者組織内で作業を行う場合には、作業を行う施設は、IC カード等電磁的管理による入退館管理がなされていること。
- 作業を行う施設内の作業実施場所は、IC カード等電磁的管理による入退室管理がなされていること。
- 電磁的に情報・資料を保管する場合には、当該業務に係る体制以外の者がアクセスできないようアクセス制限を行うこと。また、アクセスログにより不審なアクセスがないかの確認を行うこと。
- 情報・資料を保管する端末やサーバ装置等は、受注者の情報セキュリティポリシー等により、サイバー攻撃に備え、ウイルス対策ソフト、脆弱性対策及び検知・監視等の技術的対策が講じられ、適切に管理・運用される必要があるため、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や PMDA サイバーセキュリティポリシーに準拠し、管理等することとし、準拠した対応ができない場合は、代替のリスク軽減策を講じ、PMDA の承認を得ること。
- 用務に必要がなくなり次第、速やかに PMDA に返却すること。
- 受注業務完了後、PMDA が提供した情報・資料を返却し、受注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 へ提出すること。

3 応札希望者についても上記に準ずること。

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。

7 機密保持及び情報・資料の取扱いについて、適切な措置が講じられていることを確認するため、PMDA が遵守状況の報告や実地調査を求めた場合には応じること。

8　本業務で作成したデータ等については、業務の終了に伴い不要となった場合又は PMDA から廃棄又は抹消の指示があった場合には、回復が困難な方法により速やかに廃棄又は抹消すること。なお、受注者が用意するヘルプデスク機材や開発・運用機材等のうち、個人情報を取り扱う場合を含むものとする。PMDA の承認を得た上で速やかに実施し、実施後においては作業完了報告書を PMDA に速やかに提出すること。

(2) 遵守する法令等

ア　法令等の遵守

1　次の文書の最新版を遵守すること。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。

・ 独立行政法人 医薬品医療機器総合機構 サイバーセキュリティポリシー
・ 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

なお、「独立行政法人 医薬品医療機器総合機構 サイバーセキュリティポリシー」は非公表であるが、「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」に準拠しているので、必要に応じ参照すること。「独立行政法人 医薬品医療機器総合機構 サイバーセキュリティポリシー」の開示については、契約締結後、受注者が担当職員に守秘義務の誓約書を提出した際に開示する。

2　受注業務の実施において、現行情報システムの設計書等を参照する必要がある場合は、作業方法等について PMDA の指示に従い、秘密保持契約を締結する等した上で、作業すること。

3　受注者は、受注業務の実施において、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、個人情報の保護に関する法律等の関連する法令等を遵守すること。

(3) 情報セキュリティ管理

本調達案件の受注者は、情報セキュリティ対策として、以下を含む情報セキュリティ管理計画書を契約締結後速やかに提出し、PMDA の承認を受けた上で、それに基づき情報セキュリティ対策を実施すること。なお、PMDA は実施状況について、随時、実地調査できるものとする。

1　PMDA から提供する情報の目的外利用を禁止すること。

2　本業務の実施に当たり、受注者又はその従業員、本調達の役務の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不正な変更が情報システムのハードウェアやソフトウェア等に加えられないための管理体制が整備されていること。

3　受注者の資本関係・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。

4　情報セキュリティインシデントへの対処方法（対処手順、責任分界、対処体制、対応時間、情報伝達時間・手段等）が確立されていること。

5　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。

6　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。

7　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。

8　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。

9　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方法にて行うこと。

10　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、書面にて報すること。

11　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。

（4）情報セキュリティ監査

1　本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、PMDA が情報セキュリティ監査の実施を必要と判断した場合は、PMDA がその実施内容（監査内容、対象範囲、実施者等）を定めて、情報セキュリティ監査を行う（PMDA が選定した事業者による外部監査を含む。）。

2　受注者は、PMDA から監査等の求めがあった場合に、速やかに情報セキュリティ監査を受け入れる部門、場所、時期、条件等を「情報セキュリティ監査対応計画書」等により提示し、監査を受け入れること。なお、実施計画書に付記することでもよい。

3　受注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。

4　情報セキュリティ監査の実施については、これら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。

5　業務履行後において当該業務に関する情報漏えい等が発生した場合であっても、監査を受け入れること。

6　PMDA において本調達に関する監査等が実施される場合、受注者は、技術支援及び情報提供を行うこと。

7　受注者は、PMDA における監査の指摘や指摘対応の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。

（5）履行完了後の資料の取扱い

受注者は、PMDA から提供した資料又は PMDA が指定した資料の履行完了後の取扱い（返却、削除等）について、本仕様書の定めの他、PMDA の指示に従うこと。

7. 成果物の取扱いに関する事項

（1）知的財産権の帰属

1　調達に係り作成・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 条までに定める全ての権利を含む。）は、受注者が調達の情報システム開発の従前から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 が所有する現有資産を移行等して発生した権利を含めて全て PMDA に帰属するものとすること。また、PMDA は、納品された当該プログラムの複製物を、著作権法第 47 条の 3 の規定に基づき、複製、翻案すること及び当該作業を第三者に委託し、当該者に行わせることができるものとする。

2　本件に係り発生した権利については、受注者は著作者人格権を行使しないものとすること。

3　調達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、受注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こと。

4　調達に係り作成・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（以下、「既存著作物等」という。）が含まれる場合、受注者は当該既存著作物等の使用に必要な費用負担や使用許諾契約等に係る一切の手続を行うこと。この場合、受注者は、事前に当該既存著作物の内容について PMDA の承認を得ることとし、PMDA は、既存著作物等について当該許諾条件の範囲で使用するものとする。

5　調達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、受注者の責任、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時は、受注者に通知し、必要な範囲で訴訟上の防衛を受注者に委ねる等の協力措置を講ずる。

なお、受注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、受注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）検査

1　本調達仕様書「4.（2）ア　成果物」に則って、成果物を提出すること。その際、PMDA の指示により、別途、品質保証が確認できる資料を作成し、成果物と併せて提出すること。

2　検査の結果、成果物の全部又は一部に不合格品を生じた場合には、受注者は直ちに引き取り、必要な修復を行った後、指定した日時までに修正が反映された全ての成果物を納品すること。

3　本調達仕様書「4.（2）ア　成果物」に依る以外にも、必要に応じて成果物の提出を求める場合があるので、作成資料は常に管理し、最新状態に保っておくこと。

4　特段の事情がない限り、受注者においても全数検査又はサンプル検査を行うこと。

（3）契約不適合責任

1　受注者は本業務の成果物に対する契約不適合責任を負うものとする。本業務の最終検収後において、委託業務の納入成果物に関して仕様書と異なる、または契約目的に照らして通常期待される条件を満たしていない等、本システムの正常な稼動等に関わる契約不適合の疑いが生じた場合であって、PMDA が検収後 1 年以内に調査を求めた場合は、受注者は速やかに契約不適合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契約不適合等が認められた場合には、受注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　受注者は、契約不適合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。契約不適合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（国際標準規格）又は JISQ27001 認証（日本産業規格）に従い、また個人情報を取り扱う場合には JISQ15001（日本産業規格）に従い、厳重に管理をすること。また、契約不適合責任の期間が終了した後は、速やかにそれらの情報が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、受注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、受注者の負担で用意すること。

8.　入札参加資格に関する事項

（1）入札参加要件

ア　公的な資格や認証等の取得

1　品質管理体制について ISO9001:2015、組織としての能力成熟度について CMMI レベル 3 以上のうち、いずれかの認証を受けていること。

2　ISO/IEC27001 認証（国際規格）、JIS Q 27001 認証（日本産業規格）のうち、いずれかを取得していること。

3　本業務の作業場所及びデータの保管場所は、日本国内とすること。

4　本調達仕様書「11.（3）応札希望者が閲覧できる資料一覧」を指定期間内に閲覧すること。

（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、応札希望者は、以下に挙げる事業者並びにこの事業者の「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、同一の親会社を持つ会社並びに委託先事業者等の緊密な利害関係を有する事業者でないこと。

①PMDA 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

9. 再委託に関する事項

（1）再委託の制限及び再委託を認める場合の条件

受注者は、受注業務の全部又は受注業務における総合的な企画及び判断並びに業務遂行管理部分を第三者（受注者の子会社（会社法第 2 条第 3 号に規定する子会社をいう。）を含む。）に再委託することはできない。また、本事業の契約金額に占める再委託契約金額の割合は、原則 2 分の 1 未満とすること。

受注者は、知的財産権、情報セキュリティ（機密保持及び遵守事項）、ガバナンス等に関して本調達仕様書が定める受注者の債務を、再委託先事業者も負うよう必要な処置を実施すること。

また、再委託先事業者の対応について最終的な責任を受注者が負うこと。

（2）承認手続

1　受注業務の一部を再委託する場合は、あらかじめ再委託の相手方の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性及び契約金額について記載した「再委託に係る承認申請書」を提出し、承認を受けること。なお、再委託の相手方は本調達仕様書「8.（2）入札制限」の対象となる事業者でないこと。

2　再委託先が「6（3）情報セキュリティ管理」の要件を満たしていることを証明する書面※及び受注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、「再委託に関する承認申請書」に添付して提出すること。

※情報セキュリティに関する管理体制と管理基準、社内規程が整備されている事実を証明する書面。（例：管理体制図、社内規程、ISO 認証、外部監査実績、等）

3　受注者は、機密保持、知的財産権等に関して本仕様書が定める受注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。

4　受注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。

5　当初申請内容に変更が生じた場合は「再委託に係る変更承認申請書」を提出すること。

6　再委託の相手方から更に第三者に委託が行われる場合は、当該第三者の商号又は名称及び住所並びに委託を行う業務の範囲等を記載した「履行体制図」を提出すること。

（3）再委託先の契約違反

再委託先において、本調達仕様書の遵守事項に定める事項に関する義務違反又は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。

10.その他特記事項

（1）前提条件及び制約条件

1　例年 10 月から 11 月の期間は、PMDA 国際規制調和調整課の繁忙期に当たるため、職員のプロジェクトへの関与が十分にできなくなるおそれがあることに留意すること。

2　本件受注後に調達仕様書（別紙を含む）の内容の一部について変更を行おうとする場合、その変更の内容、理由等を明記した書面をもって PMDA に申し入れを行うこと。

（2）環境への配慮

1　調達に係る納品物については、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）第6条に基づく環境物品等の調達の推進に関する基本方針に定める判断の基準を満たすこと。

2　導入する機器については、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。

（3）その他

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

2　受注者は、デジタル・ガバメント推進に係る政府の各種施策・方針等(今後出されるものを含む)に従うこと。

11.附属文書

（1）調達仕様書 別紙

別紙1　SLA（Service Level Agreement）項目

別紙2　作業スケジュール

別紙3　業務要件

別紙4　システム運用管理基準

別紙5　情報セキュリティ対策の運用要件

（2）参考資料

なし

（3）応札希望者が閲覧できる資料一覧表

閲覧資料1　PMDA 情報セキュリティインシデント対処手順書

閲覧資料2　セキュリティ管理要件書(ひな型)

閲覧資料3　システム設計書

閲覧資料4　運用・保守手順書

閲覧資料5　前年度運用支援業務納品資料

（4）閲覧要領

応札希望者が資料の閲覧を希望する場合は、公告期間中に本調達仕様書「1．（8）担当課室・連絡先」に事前に連絡し了承を得た上で、「秘密保持等に関する誓約書」（PDF）を提出した場合に閲覧を許可する。なお、「秘密保持等に関する誓約書」（PDF）の提出は閲覧当日でよい。閲覧資料は CD/DVD にて提供する。貸し出した CD/DVD は開札日までに返却すること。

・閲覧申込期間 公告日から開札の 7 日前まで

（5）契約締結後に開示する資料

契約締結後に受注者が閲覧を希望する場合に開示する資料は以下のとおり。

・独立行政法人 医薬品医療機器総合機構 サイバーセキュリティポリシー

別紙1 「SLA(Service Level Agreement)項目」

指標の種類	指標名	計算式	単位	目標値	計測方法	計測周期
問い合わせ及び依頼事項への一次回答	一次回答の応答時間	応答時刻－問い合わせ受付時刻＜1 営業日の件数／問い合わせ件数	%	100%	問い合わせ一覧表への受付と応答日時の記録	毎月
セキュリティ対策	バージョンアップの対応期限	作業開始時に PMDA と合意した期限までにCMS(Drupal)及びPHPのバージョンアップ対応を完了した件数／依頼した件数	%	100%	問い合わせ一覧表への受付と対応完了日時の記録	毎月
	改ざんの初動対応開始	改ざんを把握(改ざん検知メールの参照、PMDAからの電話受付など)から 15 分以内に調査及び報告の初動対応を行った件数／改ざん検知件数	%	100%	障害報告書への改ざん発生と初動対応開始日時の記録	毎月

別紙2：作業スケジュール

No		実施区分	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	実施内容
マイルストン																
1-1	キックオフ（初年度のみ）	実施 ◎		▲ 報告												実施計画書に基づくキックオフを実施
1-2	前業者からの引継ぎ（初年度のみ）	実施 ◎	実施													運用・保守準備作業に関する準備計画書を作成し、PMDAの承認を受けた後、前事業者からの引継ぎを行う。
1-3	月次定例	実施 ◎		▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	
1-4	次年度（新業者）への引継ぎ　（最終年度のみ）	実施 ◎											準備	実施		
運用																
2-1	インシデント一覧報告（システム障害、情報セキュリティインシデントを含む）	報告 ○		▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	「システム運用標準」⇒インシデント管理：インシデント一覧による月次報告を翌月第3金曜の2営業日前までに提出
2-2	システム変更作業報告	報告 ○		▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	「システム運用標準」⇒変更管理：変更作業一覧による月次報告を翌月第3金曜の2営業日前までに提出（DA-1-1）（SC-1-1）
2-3	特権ID使用状況報告 （台帳を含む）	報告 ○		▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	「システム運用標準」⇒特権ID管理台帳・特権ID使用管理簿による月次報告を翌月第3金曜の2営業日前までに提出（AC-2-3）
2-4	データ保全（バックアップ）状況の点検 （回復の机上訓練は５月）	報告 ○		▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	「システム運用標準」⇒バックアップと回復：遵守状況の月次報告、机上訓練（DA-2-1）
2-5	情報セキュリティ：遵守状況の報告	報告 ○		▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	「システム運用標準」⇒情報セキュリティ：遵守状況の報告
2-6	脆弱性対策の実施状況の点検	報告 ○		▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	⇒情報セキュリティ管理： 脆弱性対策管理簿・脆弱性管理対象ソフトウェア一覧による月次報告を翌月第3金曜の2営業日前までに提出（AT-3-2）
権限管理																
3-1	各業務データアクセス権限再検証	支援 △							準備		実施		▲ 報告			不要なアクセス権限の洗い出しと削除。
3-2	ユーザーID棚卸し （各業務システム）	実施 ◎							準備		実施		▲ 報告			不要IDの洗い出しと削除・無効化。不要なID、権限があれば削除する。（AC-2-1）（AC-2-2）（PR-1-2）
3-3	特権ID検証（棚卸し）	実施 ◎					準備		実施	▲ 報告						【システム運用標準】"システム運用管理(要件書）"に基づく運用 ⇒特権ID管理台帳と特権ID使用管理簿の相関チェック（AC-2-1）（AC-2-2）
点検																
4-1	情報システム開発・運用資料確認	実施 ○											準備	実施	▲ 報告	情報システムの開発・運用・保守に必要な各種ドキュメント（各種設計書、手順書等）と実装（システムの構成・設定、プログラム等）が一致していることを確認す
教育・訓練																
5-1	システム運用担当者	実施 ○											受講			年次及び新任者参画時に実施する

No		実施区分	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	実施内容
内部監査																
6-1	委託先における情報セキュリティ対策の履行状況の確認	受査 ◎							準備		受査					初年度及びPMDAが必要と判断した際に実施する
PMDA監査受査への支援																
7-1	厚労省・NISC等情報セキュリティ監査	支援 △							監査支援							監査対象システム及びスケジュールは各年度で決定する
7-2	調達による第3者情報セキュリティ監査	支援 △								監査支援						PMDAが監査業者を調達して行う自己点検の対応 監査対象システム及びスケジュールは各年度で決定する
7-3	監査指摘対応フォロー	支援 △					▲ 報告	・・・・・・・・・・・・・・・・運用フォロー・・・・・・・・・・・・・・・・					▲ 報告	・・・運用フォロー・・・		過去及び契約期間中の7-1、7-2の監査指摘事項に対する改善活動及び改善状況の報告
別紙５ 情報セキュリティ対策の運用要件																
	運用時の脆弱性対策 （ＡＴ－３－２）		No.2-6参照													
	ライフサイクル管理 （ＡＣ－２－１）		No.3-2参照													
	アクセス権管理 （ＡＣ－２－２）		No.3-1参照													
	管理者権限の保護 （ＡＣ－２－３）		No.2-3参照													
	受託者によるアクセス	報告 ○		▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	
	情報の物理的保護 （ＰＨ－１－１）	報告 ○		▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	
	侵入の物理的対策 （ＰＨ－１－２）	報告 ○		▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	▲ 報告	
	システムの構成管理 （ＤＡ－１－１）		No.2-2参照													
	システムの可用性確保 （ＤＡ－２－１） 情報のバックアップの取得		No.2-4参照													
	委託先において不正プログラム等が組み込まれることへの対策（ＳＣ－１－１）		No.2-2参照													
Drupalバージョンアップ、テーマ変更、サーバ移行																
	Drupalバージョンアップ	実施 ○														Drupal v10へのバージョンアップは、運用開始後、速やかに実施 以降のバージョンアップの実施時期は、PMDAと協議して決定
	テーマ変更	実施 ○														実施時期は、PMDAと協議して決定
	サーバ移行	実施 ○														実施時期は、PMDAと協議して決定

情報セキュリティ履行状況

作業計画

No	引用元資料	実施区分	実施頻度	項目	詳細項目	実施内容	実施状況
1	別紙2_作業スケジュール	実施 ◎	1回/年	マイルストン	1-1 キックオフ	実施計画書に基づくキックオフを実施	
2	別紙2_作業スケジュール	実施 ◎	1回/年	マイルストン	1-2 前業者からの引継ぎ	契約後２週間以内に運用準備作業に関する実施計画書（運用準備作業）を作成し、PMDAの承認を受けた後、前事業者からの引継ぎを行う。	
3	別紙2_作業スケジュール	実施 ◎	1回/月	マイルストン	1-3 月次定例	-	
4	別紙2_作業スケジュール	実施 ◎	1回/年	マイルストン	1-4 次年度(新業者)への引継ぎ (最終年度のみ)	-	

情報セキュリティ履行状況

作業計画

No	引用元資料	実施区分	実施頻度	項目	詳細項目	実施内容	実施状況
1	別紙2_作業スケジュール	実施 ○	1回/月	運用	2-1 インシデント一覧報告	「システム運用標準」⇒インシデント管理：インシデント一覧による月次報告	
2	別紙2_作業スケジュール	実施 ○	1回/月	運用	2-2 システム変更作業報告	「システム運用標準」⇒変更管理：変更作業一覧による月次報告（DA-1-1）（SC-1-1）	
3	別紙2_作業スケジュール	実施 ○	1回/月	運用	2-3 特権ＩＤ使用状況報告	「システム運用標準」⇒特権ID管理台帳・特権ID使用管理簿による月次報告（AC-2-3） 補足：月次定例の「特権ID管理簿」にて報告を行う。	
4	別紙2_作業スケジュール	実施 ○	1回/月	運用	2-4 データ保全（バックアップ） 状況の点検	「システム運用標準」⇒バックアップと回復：遵守状況の月次報告	
			1回/年			「システム運用標準」⇒バックアップと回復：遵守状況の月次報告、机上訓練（DA-2-1）	
5	別紙2_作業スケジュール	実施 ○	1回/月	運用	2-5 情報セキュリティ：遵守状況の報告	「システム運用標準」⇒情報セキュリティ：遵守状況の報告	
6	別紙2_作業スケジュール	実施 ○	1回/月	運用	2-6 脆弱性対策の実施状況の点検	⇒情報セキュリティ管理：脆弱性対策管理簿・脆弱性管理対象ソフトウェア一覧による月次報告（AT-3-2）	

情報セキュリティ履行状況

作業計画

No	引用元資料	実施区分	実施頻度	項目	詳細項目	実施内容	実施状況
1	別紙2_作業スケジュール	支援 △	不定期 ※支援のため	権限管理	3-1 各業務データアクセス権限再検証	不要なアクセス権限の洗い出しと削除。	
2	別紙2_作業スケジュール	実施 ◎	1回/年	権限管理	3-2 ユーザーＩＤ棚卸し （各業務システム）	不要IDの洗い出しと削除・無効化。不要なID、権限があれば削除する。（AC-2-1）（AC-2-2）（PR-1-2）	
3	別紙2_作業スケジュール	実施 ◎	1回/年	権限管理	3-3 特権ＩＤ検証 (棚卸し)	【システム運用標準】”システム運用管理(要件書）”に基づく運用 ⇒特権ID管理台帳と特権ID使用管理簿の相関チェック（AC-2-1）（AC-2-2） 補足：特権ID管理簿の見直しを実施する。	

情報セキュリティ履行状況

作業計画

No	引用元資料	実施区分	実施頻度	項目	詳細項目	実施内容	実施状況
1	別紙2_作業スケジュール	実施 ◎	1回/年	点検	4-1 情報システム開発・運用資料確認	前回以降の改修（運用支援業務による改修及び運用支援業務以外による改修）が全て反映されており、情報システムの開発・運用・保守に必要な各種ドキュメント（各種設計書、手順書等）と実装（システムの構成・設定、プログラム等）が一致していることを確認して報告する。	

情報セキュリティ履行状況

作業計画

No	引用元資料	実施区分	実施頻度	項目	詳細項目	実施内容	実施状況
1	別紙2_作業スケジュール	受講 △	1回/年	システム運用担当者	5-1 情報システム開発・運用資料確認	年次及び新任者参画時に実施する １月に２回開催予定 **補足：前方支援担当者及び後方支援担当者に教育を行うこと。また、新しい担当者が参画した場合は、セキュリティ教育を実施すること。**	

情報セキュリティ履行状況

作業計画

No	引用元資料	実施区分	実施頻度	項目	詳細項目	実施内容	実施状況
1	別紙2_作業スケジュール	受査 ◎	初年度及びPMDAが必要と判断した際	内部監査	6-1 委託先における情報セキュリティ対策の履行状況の確認	初年度及びPMDAが必要と判断した際に実施する	

情報セキュリティ履行状況

作業計画

No	引用元資料	実施区分	実施頻度	項目	詳細項目	実施内容	実施状況
1	別紙2_作業スケジュール	支援 △	1回/年	ＰＭＤＡ監査受査への支援	7-1 厚労省・情報セキュリティ監査	監査対象システム及びスケジュールは各年度で決定する	
2	別紙2_作業スケジュール	支援 △	1回/年	ＰＭＤＡ監査受査への支援	7-2 調達による第3者情報セキュリティ監査	PMDAが監査業者を調達して行う自己点検の対応 監査対象システム及びスケジュールは各年度で決定する	
3	別紙2_作業スケジュール	支援 △	1回/年	ＰＭＤＡ監査受査への支援	7-3 監査指摘対応フォロー	過去及び契約期間中の7-1、7-2の監査指摘事項に対する改善活動及び改善状況の報告	

情報セキュリティ履行状況

作業計画

No	引用元資料	実施区分	実施頻度	項目	詳細項目	実施内容	実施状況
	別紙５ 情報セキュリティ対策の運用要件	実施 ○	1回/月	機密性・完全性の確保 （PR-1）	受託者によるアクセス	託者は受託した業務以外の情報へアクセスしないこと。 ⇒情報セキュリティ遵守状況は月次で報告すること。	
	別紙５ 情報セキュリティ対策の運用要件	実施 ○	1回/月	情報窃取・侵入対策 （PH-1）	情報の物理的保護 （PH-1-1）	受託者の管理区域において、受託者がＰＭＤＡより提供された情報を格納する機器は、情報の漏えいを防止するため、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。 ⇒情報セキュリティ遵守状況は月次で報告すること。	
	別紙５ 情報セキュリティ対策の運用要件	実施 ○	1回/月	情報窃取・侵入対策 （PH-1）	侵入の物理的対策 （PH-1-2）	受託者の管理区域において、受託者がＰＭＤＡより提供された情報を格納する機器は、物理的な手段によるセキュリティ侵害に対抗するため、外部からの侵入対策が講じられた場所に設置すること。 ⇒情報セキュリティ遵守状況は月次で報告すること。	

別紙３　「業務要件」

業務の時期・時間の定義

	実施時期・期間	実施・提供時間	補足
通年	2024 年 4 月 1 日 ～2029 年 3 月末日 ※業務を行う日（平日）とは、本仕様書で別途定められている業務の他は、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。）を除く日とする。	9:00～18:00 ※12:00～13:00 は休憩時間とする。	ただし、本仕様書で別途定めるものの他、緊急作業及び本業務を実施するために必要な作業がある場合は、この限りではない。

運用業務の範囲定義

No	名称	内容	受託者の役割
1	【レンタルサーバ運用】	KDDI ウェブコミュニケーションズがレンタルサーバ及び付帯サービス機能を運用する。	問い合わせ、折衝、調整
2	【システム監視 - ログ監視】	本システムを構成する機器及びソフトウェア上で入手可能なログの収集・確認し、月次で報告すること。	実施
3	【システム監視 - 情報セキュリティ監視】	改ざん検知メールの監視し、異常を発見した場合は障害対応手順に沿って対応すること。 セキュリティログを取得･確認し、月次で報告すること。	実施
4	【ヘルプデスク業務 - 問い合わせ対応】	以下の問い合わせ対応等を実施すること。また、問合せと対応の内容は記録し報告すること。 ・コンテンツ作成･改修に関する技術支援（必要に応じて Drupal の設定変更、テンプレートの追加などを含む） ・Drupal の操作方法に関する技術支援 ・障害及び情報セキュリティインシデントの調査依頼 ・情報システム監査に関する実態調査 ・作業工数は 5 年間で 40 人日程度の想定とする。	実施
5	【アカウント管理】	（ア） PMDA から提出されるユーザ登録・削除依頼に基づき、OS 上、及びアプリケーション上のユーザを登録･削除すること。作業内容はすべて作業ログとして蓄積し、PMDA に報告すること。（随時／適宜） （イ）Drupal の他、システムを保守・運用に必要なユーザを管理の対象とすること。 （ウ）アクセス権限管理 管理対象となる各種ユーザのアクセス権限の管理を行うこと。 ※別紙５「運用要件」アカウント管理（AC-2）参照	実施
6	【サービスレベ	別紙１　「SLA（Service Level Agreement）項目」参照	実施

No	名称	内容	受託者の役割
	ル管理】	運用業務については、受託者と PMDA との間で協議の上、SLA（Service Level Agreement）を締結する。サービスレベル評価項目と要求水準については、別紙１「SLA 項目」を参照すること。ただし、サービスレベル評価項目と要求水準については、協議の上、見直すこととする。	
7	【バックアップ/リカバリ】	日次の自動バックアップの他、コンテンツ変更時やPMDAから依頼があった場合など必要に応じてマニュアルでバックアップを取得し、不具合があった場合にリカバリを行うこと。但し、コンテンツ編集の最中に必要なバックアップはPMDAが適宜行うものとする。	実施
		バックアップが所定の要件通りに取得されていることを定期的に確認すること。 ※別紙５「情報セキュリティ対策の運用要件」システムの可用性確保　(DA-2-1) 参照	実施
		バックアップを外部保管（ローカル環境へのダウンロードなど）を月１回以上実施すること。	実施
		バックアップデータのリカバリを行う必要があると考えられる場合には、PMDA の判断に従いリカバリ手順に沿って作業すること。	実施
8	【その他】	運用・保守業務で使用しているドキュメント（実施計画書、運用マニュアル等）を管理すること。また修正･改定の必要がある場合には、PMDAのレビューを受けて修正･改訂すること。	実施

保守業務の範囲定義

No	名称	内容	受託者の役割
1	【レンタルサーバ保守】	KDDI ウェブコミュニケーションズがレンタルサーバ及び付帯サービス機能を保守する。	問い合わせ、折衝、調整
2	【ウェブサイト保守】	(1) ウェブサイトを正常に稼動させるために設定の変更が必要となる場合にはPMDAに提案し、PMDAの了解の下、当該作業を実施すること。 (2) CMS(Drupal)を正常に運用するために設定の変更が必要となる場合にはPMDAに提案し、PMDAの了解の下、当該作業を実施すること。 (3) PMDAからの依頼に基づき、PMDAがテストサイトで作成・更新したコンテンツを本番サイトへのリリースすること。更新頻度は3回/月、作業工数は10人日/年程度の想定とする。	実施
3	【ソフトウェア保守 - ソフトウェア更新】	運用対象システムのソフトウェア資源について、以下の作業を実施する。ソフトウェアの更新作業については、PMDA と協議の上、本番環境に反映させること。 ※別紙５「情報セキュリティ対策の運用要件」運用時の脆弱性対策　(AT-3-2) 参照	実施

No	名称	内容	受託者の役割
		(1) Drupal のセキュリティパッチの提供に関する情報、PHP のバージョンアップに関する情報及び脆弱性情報の収集。	実施
		(2) 脆弱性対応計画 脆弱性情報又はセキュリティパッチの提供に関する情報を入手し、セキュリティパッチの適用に関してリスクが懸念される場合、当該 脆弱性への対応又は当該セキュリティパッチを適用すること。直ちにはパッチ適用できないと判断される場合は、リスクと当面の回避策（案）を報告すること。	実施
		(3) ミドルウェアのセキュリティパッチの適用 Drupal および PHP のセキュリティパッチ適用する計画を作成し、PMDA の承認を得た上で適用を実施すること。	実施
4	【Drupal バージョンアップ及びテーマの変更】	(1) Drupal のサポートが終了するまでに最新バージョンにバージョンアップすること。 ※メジャー・バージョンアップは、最大 3 回とする。 ※マイナー・バージョンアップすることでサポート期限を延長できる場合、PMDA と協議のうえマイナー・バージョンアップを実施してメジャー・バージョンアップを延期することができる。 ※テーマの変更は、最大 1 回とする。 ※Drupal バージョンアップ及びテーマの変更に関する調査から本番移行、初期対応までの全ての作業を含む。 (2) 初回のバージョンアップは、契約後速やかに開始すること。実施スケジュールは PMDA と協議のうえ決定するものとする。 (3) レンタルサーバに関する問い合わせをレンタルサーバ事業者に直接行うこと。ただし、レンタルサーバ事業者が受注者からの直接の問い合わせを受け付けない場合は、問い合わせ内容を PMDA に連絡するものとする。 (4) 移行作業は平日日中も可とするが、コンテンツの更新停止は 3 日以内、公開サーバの停止は半日以内を目途とする。ただし、移行スケジュールは PMDA と調整のうえ決定するものとする。	実施
5	【サーバ移行】	(1)現行の SV-Basic のサービスが終了する、もしくは、Drupal のシステム要件を満たせなくなった場合、SV-Basic と同じレンタルサーバ事業者他提供する新サーバに移行すること。 ※サーバ移行は、最大 1 回とする。 ※Drupal バージョンアップと同時に実施しても、別に実施しても良い。 ※サーバ移行に関する調査から本番移行、初期対応までの全ての作業を含む。 (2)新旧サーバの並行稼働期間は最大 4 か月を目途とし、PMDA	実施

No	名称	内容	受託者の役割
		は、移行完了後 1 か月以内を目途に旧サーバを停止してレンタルサーバの契約を終了するものとする。 ※レンタルサーバのサービス提供は PMDA が契約するため、本調達の対象外。	

別紙4

システム運用管理基準

2020 年 12 月
独立行政法人　医薬品医療機器総合機構

【資料の見方】
- ✧ システム運用業務を「13の領域」に分けている。
  それぞれの業務プロセスは、標準化対象外。各情報システムの体制･特性･リスク等により、最適なプロセスを設計し、運用する。
- ✧ システム運用の標準化（要件）は、システム運用者（委託先）から当機構への報告書式（情報提供も含む）を統一し、各システムの運用状況を定期的に収集して、全体状況の把握と情報共有等を可能とすることにある。
  - 当資料においては「標準化」のタイトル等にて報告を記載している。
  - 標準化（要件）は、「報告書式を統一する領域」と「報告内容を統一（書式任意）」の 2 タイプに分かれる。
  - 「報告書式を統一する領域」は、インシデント管理、変更管理、構成管理、脆弱性管理、アクセス権管理の領域となっている。

改訂履歴

改定日	改定理由
2018 年 6 月 8 日	初版発行
2018 年 7 月 20 日	情報セキュリティ遵守状況報告内容を追記
2018 年 9 月 10 日	脆弱性管理を追記
2019 年 8 月 15 日	2. システム運用管理業務の概要に「【参考】システム運用管理業務の全体像」を追加 4.5 構成管理　最新情報を PMDA に報告する標準書式を定義 4.9 脆弱性管理　管理状況を報告する PMDA 標準書式を定義
2019 年 12 月 20 日	4.7 バックアップと回復管理　バックアップデータの保管方法を追加
2020 年 12 月 10 日	4.6 運行管理　ログ取得・保存、イベント検知対応の報告を標準化 4.9 脆弱性管理　管理要件を追加 4.10 アクセス管理　アカウント管理要件の追加、アカウント台帳作成と棚卸を標準化項目に追記

1. はじめに

1．1　目的

独立行政法人医薬品医療機器総合 PMDA（Pharmaceuticals and Medical Devices Agency）（以下、「PMDA」という。）が調達し、又は、開発した情報システムの運用管理を確実かつ円滑に行い、利用者が要求するサービス品質を、安定的、継続的かつ効率的に提供するために、情報システムの運用管理に関する業務内容を明確化・標準化するために定めるものである。

1．2　対象範囲

PMDA が調達し、又は開発・構築した全ての情報システムの運用保守を担当する組織（情報システムの運用保守業務を外部委託する場合における委託先事業者を含む）に適用する。

1．3　適用の考え方

システム運用管理業務は、既に開発・構築しサービスイン（本番稼動）している情報システムの運用・保守業務の実行と管理に係る業務を対象とする。

情報システムの運用・保守を外部委託する場合は、本資料をもとに委託先事業者において、当該情報システムの種類・規模・用途を踏まえた適切な運用手順を策定のうえ、運用サービスを提供するものとする。

1．4　用語の定義

本基準で使用する用語は情報システムの「ITIL（IT Infrastructure Library）」のガイドラインを踏まえた運用プロセス定義に準拠するものとする。

1．5　準拠および関連文書

上位規程　：「情報セキュリティポリシー」
関連文書　：「情報システム管理利用規程」

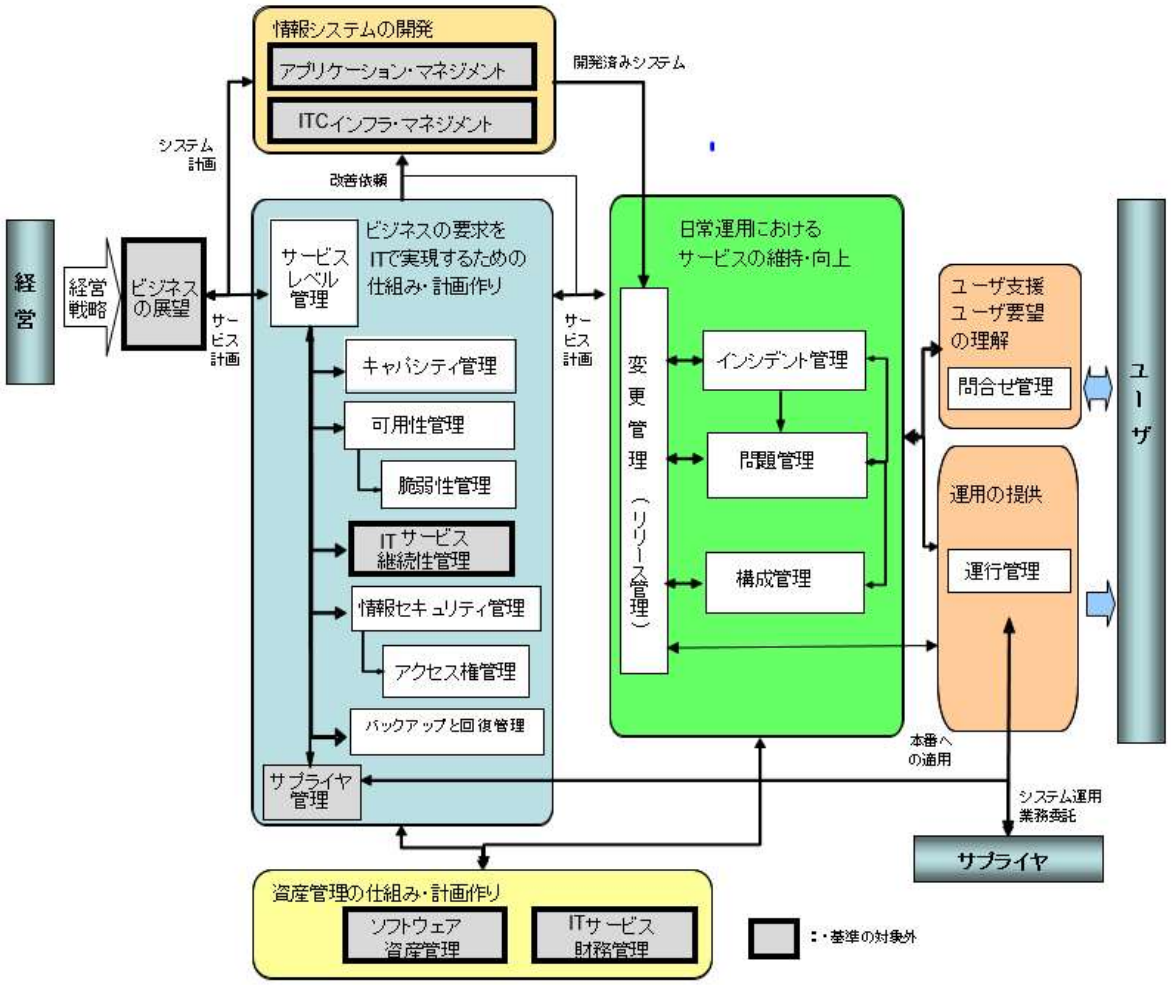
2. システム運用管理業務の概要

PMDA においては情報システムの運用保守を外部委託している状況を踏まえ、運用管理に必要なプロセスのあるべき姿から主要なプロセスを運用管理業務として選定し、以下の13の管理業務について、明確化・標準化を行う。

管理業務	概要
問合せ管理 （サービスデスク）	システムの利用者からの問合せ窓口として、利用者からの各種問合せについて一括受付することにより 問合せに対する早期回答、障害対応への早期エスカレーションを図るとともに、ユーザからの要望を適切に吸い上げる。
インシデント管理	問い合わせに含まれるインシデント、あるいはハードウェア、アプリケーションなどからのインシデント発生の警告／報告を受け、サービスの中断を最小限に抑えながら、可能な限り迅速に通常サービスを回復するよう努める。
問題管理 （再発防止策）	障害（インシデント）の根本的な原因となっている不具合が、ビジネスに与える悪影響を最小化するため、問題を分析し抜本的解決策や回避策を立案する。
変更管理 （課題管理）	情報システムに対する変更の許可と実装を確実に行うための管理をいう。本番環境に対する変更要求を適正な基準で評価・承認を行い、標準化された変更方法、手順が実施されることを確実にする。 また、変更による影響とリスクを最小化し、障害を未然に防止することで、サービス品質の維持・向上に努める。 なお、本基準においては、変更要求の必要性、効果、リスクなど変更の妥当性の評価と承認（変更管理）に加えて、本番環境に対してどのような準備・実行・見直しを行って変更を加えるかの決定（リリース管理）を含めるものとする。
構成管理	情報システムを構成する物理資源・論理資源とその環境を常に把握するための管理をいう。運用・保守業務やそのサービスに含まれる全てのIT資産や構成を明確にし、正確な構成情報と関連文書を提供することで、他のサービスマネジメント・プロセス（インシデント管理、問題管理、変更管理、情報セキュリティ管理等）に信頼できる管理基盤を提供する。
運行管理 （稼動管理）	情報システム全体を予定通り安定的に稼動させるために、システムのスケジュール、稼働監視、オペレーションなど一連の運行を管理する。 ・スケジュール管理 ・オペレーション管理（定型業務、非定型業務） ・稼動監視　・障害対応　・ジョブ運用　・媒体管理 ・本番システム導入・移行時の支援　等

管理業務	概要
バックアップと 回復管理	必要なバックアップを定期的に取得、管理し、障害が発生した場合は、速やかな回復ができるよう、回復要件に基づき必要な回復手順、仕組みを計画、作成、維持する。
情報セキュリティ管理	情報セキュリティポリシーに規定されたセキュリティ対策を実施するために必要な管理要件に基づき、情報セキュリティ管理基準・手順等を作成し、情報セキュリティ管理を行う。
脆弱性管理	情報システムのソフトウェアおよびアプリケーションにおける脆弱性を特定、評価、解消するための管理業務を行う。システム構成を把握した上で、構成要素ごとに関連する脆弱性情報をいち早く「収集」し、影響範囲の特定とリスクの分析によって適用の緊急性と対応要否を「判断」し、判断結果をもとに迅速に「対応」を行う。
アクセス権管理	アクセス方針を定め、アクセス制御の仕組みを構築・維持し、システム・アカウントの申請受付け・登録・変更・削除など管理業務を行う。 ・アプリケーション・システムのアカウント ・サーバのOSアカウント ・DBMSアカウント ・運用支援システムのアカウント ・各種特権アカウント　等
キャパシティ管理	サービス提供に必要となるシステム資源の利用状況の測定・監視を実施し、現在の業務要求（既存の提供サービス量）と将来の業務要求（要求される提供サービス量）とを把握した上で、システム資源がコスト効率よく供給されるように調整・改善策の立案を行う。
可用性管理	ITインフラストラクチャーを整備し、それをサポートするITサービス部門の能力を最適化させることで、ビジネス部門に対して、費用対効果が高いITサービスを持続して提供する。 可用性管理の活動は、既存のITサービスの可用性を日常的に監視・管理する「リアクティブ」なプロセスと、リスク分析や可用性計画の策定や可用性設計基準などの作成を行う「プロアクティブ」なプロセスに分けられる。
サービスレベル管理	「サービスレベル合意書」で定める各種サービスレベル値の達成、維持作業として、管理項目に対する実績データの収集、分析、評価、及び改善策を策定する。 また、運用管理業務における報告データを収集、管理し、月次にユーザへの報告を実施する。

【参考】システム運用管理業務の全体像

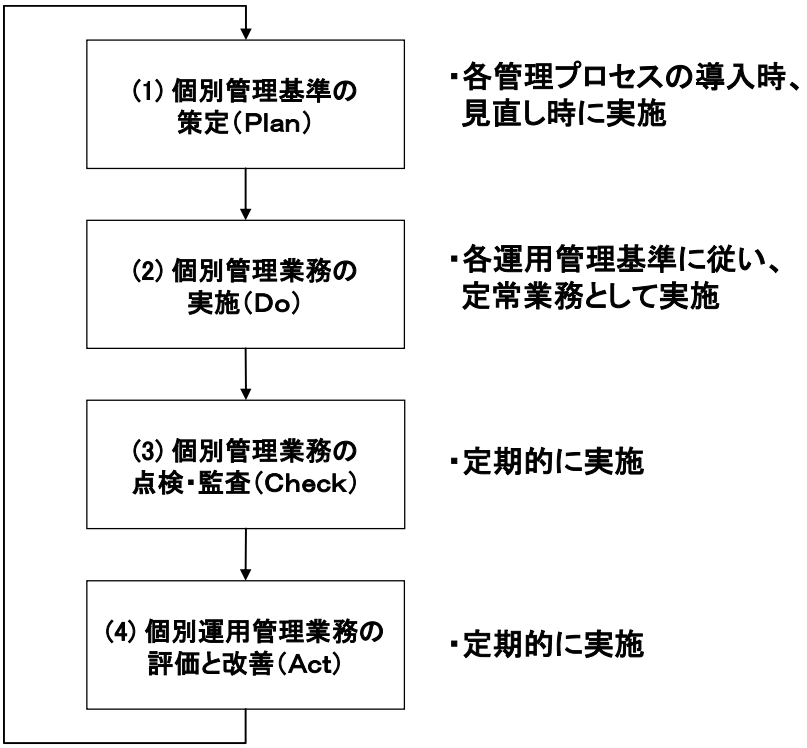


3. 運用管理業務の基本プロセス

（運用管理業務プロセスのPDCAマネジメントサイクル）

他のマネジメント・システムと同様に、運用管理業務プロセスも手順書等を策定して終わりではなく、実際に手順書等に準拠した運用を実施し、定期的に又はシステムの変更やメンバーの入れ替わりなどに合わせて都度、管理プロセスを見直し、必要に応じて改善・是正を行う必要がある。

そのために、運用管理業務プロセスに、個別管理基準の「策定（Plan）」、「実施（Do）」、「点検・監査（Check）」、「評価と改善（Act）」の4つの基本プロセスからなるPDCAマネジメントサイクルを導入し、継続的改善を実施することが重要である。



各基本プロセスの概要は、以下のとおりである。

（1） 個別管理基準の策定（Plan）

各運用管理業務の実施方針、実施範囲、管理プロセス、業務の管理指標等を含めた管理基準書ならびに管理手順を定める。

（2） 個別管理業務の実施（Do）

各運用管理業務の実作業を行うとともに、業務遂行に必要な関連情報の蓄積、実績情報の収集保管、およびに評価指標の実績測定を行う。

（3） 個別管理業務の点検・監査（Check）

各運用管理業務に対し、個別運用管理基準に遵守した運用がなされているか定期的に点検・監査を行い、その結果を分析･評価する。

（4） 個別運用管理業務の評価と改善（Act）

各運用管理業務に対する評価指標に対する実績管理を行うと共に、品質向上に向けた改善計画を立案し、改善実施を行う。

4. システム運用管理業務の明確化・標準化

4. 1 問合せ管理

(1) 目的

ユーザ及び各業務プロセスオーナからの問合せや依頼に対する受付窓口を一元化することで、各業務の利用ユーザの業務効率性を向上させる。

(2) 業務の概要

問合せ対応では、問合せの受付、クローズ、一次回答、管理プロセスの評価・改善の一連のプロセスを実施する。

(3) 管理対象

本番システム環境で稼動している全てのシステムに係る以下の問合せについて対応する。

- アプリケーション仕様、操作、機能、内容に関する問合せ
- ハードウェア／ソフトウェアに関する問合せ
- 要望
- アプリケーション修繕に対する依頼
- その他の依頼作業

(4) 業務の管理指標＆標準化

問合せ対応業務を評価するための評価指標として以下を定義し、定期的(月次)報告を行う。

①問合せ発生件数(日次集計・月次集計を含む)

②問合せ区分別件数

③問合せ一次回答期限遵守率

④問合せ完了率(一定期間経過後(10 営業日経過後)の完了率)

※報告内容は、各システムの状況に応じて変更しても構わない。

【補足】

問合せにより「システム障害」「セキュリティインシデント」が発覚した場合は、該当問合せは一次回答にてクローズとし、その後は「インシデント管理」にて対応する。

問合せにより「変更」実施が必要となった場合は、対応予定日を回答することでクローズとし、その後は「変更管理(課題管理)」にて対応する。

４．２ インシデント管理

(1) 目的

インシデント管理は、ユーザからの問合せ・連絡、あるいはオペレータや監視システム等によるインシデントの検知を受け、ITサービスの中断を最小限に抑えながら、可能な限り迅速に正常なサービスを回復することを目的とする。

(2) 業務の概要

①インシデントの定義

インシデントとは、ユーザや監視システム等の検知により判明したハードウェアやソフトウェアに関する一般的な障害（システム・ダウン、バグによるアプリケーションの機能停止等）だけでなく、ユーザが日常の操作手順によってITサービスを利用する上で支障がある事象は全てインシデントに包含される。

【注】このインシデントには、情報セキュリティインシデント（不正アクセス・マルウェア検知等）を含む。

また、まだITサービスに影響を与えていない構成アイテムの障害もインシデントとして扱う。

例えば、(i) 二重化されたデータベース・システムの一方がダウンした場合で、まだサービス自体が正常に稼働している場合、(ii) 本番環境のバックアップを検証環境にリストアできない場合、これらをインシデントとして扱う。

②インシデント管理の主な活動

インシデント管理は、インシデントの 4 つのライフサイクル（発見－判別－回復－解決）の内、発見－判別－回復（解決）までをカバーする。（再発防止については、次節の「問題管理」で扱う。）

インシデント管理のプロセスでは、主に次の活動を実施する。

- ・インシデントの検知
- ・インシデントの記録
- ・インシデントの通知
- ・インシデントの分類
- ・インシデントの優先度付け
- ・インシデントの初期診断
- ・エスカレーション
- ・インシデントの調査と診断
- ・復旧(解決)策の実施
- ・インシデントのクローズ

(3) 管理対象

本番システム環境で稼動している全てのシステムのインシデントを管理対象とする。

(4) 業務の管理指標

インシデント管理の管理業務を評価するための評価指標として以下を定義し、定期的(月次)報告を行う。

① 当月インシデント発生件数（総件数、障害ランク別・原因別・システム別件数・解決責任部門別）

② 優先度又は緊急度毎に分類されたインシデントの解決までに要した時間（平均時間）
③ ステータス（記録済み、対応中、クローズ済み等）毎のインシデントの内訳
④ 長期間（発生から１カ月以上）未解決のインシデントの件数と理由および業務影響
⑤ 新規に発生したインシデントの件数とその傾向
⑥ ユーザのトレーニングなど、ITテクノロジーに関連しないで解決されたインシデントの件数
⑦ 解決に要したコスト
⑧ インシデント発生件数の削減率（対前年比）

(5) 標準化

インシデント管理は、PMDA 標準書式を適用する。

①インシデント発生(判明)時

インシデントごとに個票を起票する。この個票は「PMDA 標準書式」を使用する。

※添付「インシデント報告書（ひな型）」を使用する。また「インシデント一覧記載要領」を参照し、対応すること。

※各情報システムの状況等によって、一部改修して使用しても構わない。ただし、必須項目の変更・削除は認めない。

②定期的(月次)報告時

インシデントごとの個票を集計表に転記のうえ報告する。この集計表は「PMDA 標準書式」を使用する。

※添付「インシデント一覧」を使用する。

４．３ 問題管理（再発防止策）

(1) 目的

サービスの信頼性を維持・向上するためには、システムの利用・運用上発生した問題（障害を引き起こす根本的な原因）を確実に解決し、同一障害・類似障害の再発防止のための是正を実施することを目的とする。

(2) 業務の概要

本番サービスに影響を与えた障害を分析し、それらの共通の根本原因を取り除く是正策を実施するまでの一連のプロセスを管理する。 問題管理(再発防止)では、以下を実施する。

- ・問題の傾向分析と課題点の抽出
- ・是正策の検討
- ・是正策の実施

(3) 管理対象

本番システム環境で稼動している全てのシステムの問題を管理対象とする。

(4) 業務の管理指標＆標準化

問題管理(再発防止)業務を評価するための評価指標として以下を定義し、定期的(月次)報告を行う。

① 再発防止策が策定された問題件数（総件数、障害ランク別・原因別・システム別件数・解決責任部門別）
② ステータス（記録済み、対応中、クローズ済み等）毎の再発防止策の内訳
③ 再発防止に要したコスト
④ 長期間（策定から１カ月以上）未実施の再発防止策件数と理由
⑤ 再発防止の実施率（対前年比）

※報告内容は、各システムの状況に応じて変更しても構わない。

４．４ 変更管理

(1) 目的

サービスの信頼性を維持・向上するためには、システムに対する変更について、その妥当性を検証し、変更によるユーザへの影響を最小限にすることが重要である。 変更管理プロセスは、システムに対する変更を一元的に管理することを目的とする。

(2) 業務の概要

変更管理では、変更の申請から変更内容の審査、変更の承認または却下、変更の実施、変更実施結果の報告までの一連のプロセスを管理する。

緊急の場合、対応を優先し所定のプロセスを適宜省略することを可能とするが、事後的に対応できるものについては、事後速やかに対応することとする。

(3) 管理対象

システム運用者（委託先）が運用し本番サービスを提供するシステムの全て又はその一部に対して影響を与える全ての変更を管理対象とする。

本番環境	構成要素（主な要素）
ハードウェア	CPU、DASD・DISK、サーバ、ワークステーション、周辺装置
システム・ソフトウェア	OS、サブシステム、サーバ及びワークステーション OS
ミドルウェア	DBMS、ネットワーク OS
アプリケーション・ソフトウェア	ソース、モジュール、シェル、JCL
ネットワーク・ハードウェア	スイッチ、ルータ、ブリッジ
ネットワーク・サービス	基幹ネットワーク、LAN、インターネット　等
データ	データベース及びファイル内のデータ（に対する直接修正）

(4) 業務の管理指標

変更管理業務を評価するための評価指標として以下を定義する。

① 変更実施件数（総件数、領域別・原因別・システム別件数・解決責任部門別）
② 変更の実装が失敗した件数
③ 変更のバックログの件数
④ 予定期間でクローズされなかった変更の件数
⑤ 変更が原因で発生した変更の件数
⑥ 緊急の変更の件数

(5) 標準化

変更管理は、PMDA 標準書式を適用する。

①変更案件発生時

課題管理表に記入し、変更管理のステイタス（未着手（対応予定日記入）～着手(対応中)～完了）を管理する。

※課題管理表の書式は、各情報システムの任意とする。

②変更実施着手時

変更の着手ごとに個票を起票する。この個票は「PMDA 標準書式」を使用する。

※添付「変更作業申請書（ひな型）」を使用する。

※各情報システムの状況等によって、一部改修して使用しても構わない。ただし、PMDA 側の確

認･承認欄の削除は認めない。

※個票は、「単純な定常作業」に関しては使用しなくても良い。

- 「単純な定常作業」は、各システムにて定義する。
- ただし、定期的（月次）報告には、記載する。

※個票は委託先にて保管し、監査等にて提示要求があった場合は、速やかに提示できるよう対応する

③定期的(月次)報告時

変更実施ごとの個票を集計表に転記のうえ報告する。この集計表は「PMDA 標準書式」を使用する。

※添付「変更作業一覧」を使用する。また「変更作業一覧記載要領」を参照し、対応すること。

※「単純な定常作業」に関しては、「変更作業一覧」の「変更申請」欄及び「完了確認」欄に関する内容を記入し、報告する。

４．５ 構成管理

(1) 目的

システムの構成要素（構成情報）を正確に把握し、常に最新状態にあることを保証する事で、他の運用管理プロセス（障害管理や変更管理等）に対して必要な構成情報を提供できるようにする。

(2) 業務の概要

構成管理では、ITサービス開始時より構成情報を一元管理し、他の運用管理プロセスから最新の構成情報を参照可能にする。

本管理プロセスの開始前に、立案した計画に沿って対象とするITサービスやITコンポーネントの範囲、詳細度のポリシーを策定し、開始時のベースラインを把握する。 次に、構成情報の収集と分類を行った上で構成情報を参照可能な状態に維持する。

本管理プロセスの開始後は、変更管理プロセスと連携し、構成情報が常に最新状態として維持されるようにコントロールを行う。 また、定期的に構成情報の点検を行うことにより、課題や問題点を洗い出し、評価・改善を行う。

(3) 管理対象

構成管理が対象とする構成情報は以下の通りとする。

カテゴリー	管理対象の種類
システム運用管理	各種管理プロセス定義書、手順書、依頼書、CI一覧
システム運用	・ハードウェア、ネットワーク・ハードウェアの一覧、構成図 ・ネットワーク・サービス （WAN、インターネット等)の一覧、構成図 ・システム運用各種手順書（障害対応手順書等）
システム保守	・システム・ソフトウェア、ミドルウェアの一覧、構成図 ・アプリケーション・ソフトウェア(ライブラリ、データ、環境設定情報)
ハウジング	環境設備 （空調設備、電源設備、配線室、配線、管理室)の一覧、構成図
アプリケーション保守	・設計ドキュメント、プログラムソース ・アプリケーション保守用各種手順書（定型作業手順書等）

(4) 業務の管理指標

構成管理業務を評価するための評価指標として以下を定義する。

① 承認されていない構成の件数
② 不正確な構成情報が原因で失敗した変更及び発生した障害の件数
③ CI（管理対象の項目数）の正確さ率
・構成アイテムの管理情報と実態（H/W、S/W、M/W、機器）との整合性の確認

(5) 標準化

○PMDA では、「システム資産簿」を作成してシステムのインベントリ情報を一元管理している。各システムのインベントリ情報を各システムの実装状況を反映した最新状況に更新するとともに、「システム資産簿」を最新の状況に保つため、最新のインベントリ情報を PMDA 標準書式「システム資産簿登録用シート」を使用して、PMDA へ報告する。

４．６ 運行管理

(1) 目的

運行管理の目的は、開発部門より引き継いだ業務アプリケーション・システムを、あらかじめ定められた運行計画に基づき、定められた手順に従ってシステム運用を行うことにより、システム運用の品質の維持・向上を図ることにある。

(2) 業務の概要

運用引継ぎから、システムのスケジュール計画、稼働監視、オペレーションなど一連の運行を管理する。 以下のサブプロセスから構成される。

① 運用引継ぎ
② 運用スケジュールの計画・管理
③ オペレーション実施
④ 稼動監視と障害対応（一次対応）
⑤ セキュリティ監視（対象イベントの検知への対応）
⑥ ジョブ実行管理
⑦ 帳票管理
⑧ 報告管理

(3) 管理対象

本番システム環境で稼動している全ての情報システムの運行を管理対象とする。

(4) 業務の管理指標

運行管理業務を評価するための評価指標として以下を定義する。

① 重要バッチ処理終了時間遵守率
② 重要帳票の配布時間遵守率
③ システムの運行業務に起因した障害の発生件数
・プログラム・JCL等の本番移送のミス、ジョブのスケジュール誤り、操作ミス、監視項目の見落とし／発見遅延、等。
④ 非定型依頼業務の実施件数と正常終了率

(5) 標準化

〇情報システムの運行状況を報告する（月次）（書式任意）

情報システムの稼働状況に加えて、以下の項目の報告を必須とする。

・情報システム及びネットワーク内で発生するイベント（事象）の記録である「ログ」の取得・保存のプロセスの状況を監視し、報告する。
・情報システムの稼働により発生する各種検知メッセージへの対処を記録し、報告する。

４．７　バックアップと回復管理

(1)　目的

障害発生時等において、速やかに正確な回復処置が行えるようにバックアップの取得・リストアの手順を明確にし、安定したサービスの提供を図る。

(2)　業務の概要

アプリケーションオーナーとのサービスレベルまたは管理目標の合意に基づき、システムの回復要件（＊）に見合ったバックアップ・リストア方針を定め、バックアップ対象の選定、手順の明確化を実施する。

日常運用においては、バックアップ取得、バックアップ媒体の保管を行う。

また、定期的に、バックアップ・リストア実績報告を行い、バックアップ・リストアにおける体制、役割、手順の見直しを図る。

（＊）業務の優先度を勘案して有事の際に稼動させるシステムのサービスレベルを定めて、データのバックアップと復旧方法を決定する。

RLO （Recovery Level Objective）：どの範囲、レベルで業務を継続するか

RTO （Recovery Time Objective）：いつまでにシステムを復旧するか

RPO （Recovery Point Objective）：どの時点にデータが戻るか

(3)　管理対象

本番システム環境で稼動している全てのシステムのバックアップとリストアを管理対象とする。

本基準の適用システムに関するOS、データベース、テーブル類、ユーザデータなどのバックアップ計画、バックアップ取得、バックアップ媒体の保管、リストア実施および定期的な実績報告の手続きを対象とする。

各情報システムを構成するサーバや通信回線装置等については、運用状態を復元するために必要な重要な設計書や設定情報等のバックアップについても適切な場所に保管する。

(4)　バックアップデータの保管方法

要保全情報(完全性2）又は要安定情報（可用性2）である電磁的記録若しくは重要な設計書は、バックアップを取得する。

① データベースやファイルサーバのバックアップは、インターネットに接点を有する情報システムに接続しないディスク装置、テープライブラリ装置等に保存する。

② 一般継続重要業務で使用するシステムについては、大規模災害やテロ等による設備・機器の破損を想定し、情報システムの復元に必要な電磁的記録については LTO 等の可搬記憶媒体による遠隔地保管を行う。

③ バックアップの取得方法、頻度、世代等は各システムの方式設計、運用要件に応じて定める。

(5)　業務の管理指標

バックアップと回復管理業務を評価するための評価指標として以下を定義する。

① 当月で計画された定期バックアップの内、バックアップに失敗した件数と理由。

② 当月実施されたリストア件数と内訳（障害対応、調査目的、帳票再作成・出力等）。

③ 当月実施されたリストアの内、リストアに失敗した件数と理由。

(6) 標準化

〇定期的なバックアップが取得されていることを報告する（月次）（書式任意）

〇PMDA では、「リストアの机上訓練」を定期的に実施することを推奨している。

各情報システムにおいては、必要に応じて定期的な訓練実施を行い、結果報告を行う。

４．８ 情報セキュリティ管理

(1) 目的

情報セキュリティ管理は、「情報セキュリティ対策の運用要件」に定める情報セキュリティ対策の運用要件に則り、情報システムのセキュリティを維持・管理し、情報資産を適切に保護することを目的とする。

(2) 業務の概要

情報セキュリティ管理プロセスは、PMDA のリスク管理活動の一環として、ITサービス及びサービスマネジメント活動における全ての情報のセキュリティを、首尾一貫した方針に基づき効果的に管理する。

具体的には、「情報セキュリティ対策の運用要件」に則って、適切にセキュリティ管理策が導入され、維持されていることを確実にするために、情報セキュリティ管理計画の維持・管理を行う。合わせて、情報セキュリティ対策が適切に運用されているかを定期的に点検するとともに、コンプライアンス等の観点からのシステム監査の実施対応をおこなう。

(3) 管理対象

ITサービス及びサービスマネジメント活動における全ての情報セキュリティの管理を対象とする。

(4) 業務の管理指標

情報セキュリティ管理業務を評価するための評価指標として以下を定義する。

① 情報セキュリティ違反・事件・事故の発生件数とその内容
② 発生した情報セキュリティ違反・事件・事故への対策の実施状況
③ 情報セキュリティ監査（内部・外部）及び自己点検で検出された不適合の件数
④ 前回の情報セキュリティ監査及び自己点検で検出された不適合の是正状況

(5) 標準化

○情報セキュリティ遵守状況の報告

・情報セキュリティを遵守していることを定期的(月次)にて報告する

※報告内容の詳細は後述の【補足説明】を参照

・委託先における自己点検を定期的(年 2 回程度)に実施し、点検結果を報告する。

（点検内容は委託先の任意とするが、各情報システムの運用保守業務に携わる要員等が自らの役割に応じて実施すべき対策事項を実際に実施しているか否かを確認するだけではなく、運用保守のプロジェクト体制全体の情報セキュリティ水準を確認する内容とすること。）

【補足説明】

情報セキュリティ遵守状況の報告は、以下の内容を確認し、報告すること

① 情報の目的外利用の禁止
② 情報セキュリティ対策の実施および管理体制（プロジェクト計画書記載内容の遵守）

※委託先において実施するセキュリティ研修や委託先の情報セキュリティポリシー遵守のため取組み内容を含む

※責任者による情報セキュリティの履行状況の確認を含む

③ 体制変更の場合の速やかな報告
④ 体制に記載された者以外が委託業務にアクセスできない（していない）ことの確認
⑤ ※発生した場合は、すぐに検知でき、報告される
⑥ 要員の所属・専門性（資格や研修実績）・実績および国籍に関する情報提供
※変更があれば、その都度情報提供される。
⑦ 秘密保持契約（誓約書）の提出（要員全員が提出）
※委託業務を離れた者の一定期間の機密遵守を含む
※体制変更があった場合の追加提出も含む
⑧ 情報セキュリティインシデントへの対処方法の明確化され、要員に周知されている
⑨ 再委託がある場合は、上記内容を再委託先においても遵守していることが確認されている

４．９ 脆弱性管理

(1) 目的

サーバ装置、端末及び通信回線装置上で利用するソフトウェア（含むファームウェア）やアプリケーションに関連する脆弱性情報の収集とその影響評価に基づく適切な対策を実施するための標準的管理要件を定め、脆弱性によりもたらされる情報セキュリティの脅威について迅速かつ適切に対処することを目的とする。

(2) 業務の概要

脆弱性管理では、システム構成を把握したうえで、管理対象とするソフトウェアのバージョン等の確認から、脆弱性情報の収集、影響評価と対策の要否判定、脆弱性対策計画の策定、脆弱性対策の実施、結果の確認、対策の実施状況のモニタリングまでの一連のプロセスを管理する。

①管理対象ソフトウェアの把握 （管理すべきソフトウェアを特定）

②管理対象ソフトウェアの脆弱性対策の状況確認

②脆弱性情報の収集と識別（当該脆弱性が管理対象ソフトウェアに該当するかの確認）

③影響・リスクの評価と対応要否の判断及び記録

④脆弱性対策計画の策定と承認（変更管理手続きに拠る）

⑤脆弱性対策の検証 （検証環境での稼動確認）

⑥脆弱性対策の実施

⑦脆弱性対策の記録・報告

⑧脆弱性対策の実施状況のモニタリングと継続的改善

(3) 管理の対象

本番システム環境で稼動しているサーバ装置、端末及び通信回線装置上で利用するソフトウェアやアプリケーションに関する全ての脆弱性を管理対象とする。

(4) 業務の管理指標

脆弱性管理業務を評価するための評価指標として以下を定義する。

① 管理対象プロダクツ、バージョンに該当する脆弱性情報件数（通常／緊急）
② 脆弱性対策の評価件数（対策要、対策不要）
③ 対策計画の策定・実施状況（セキュリティパッチ適用、またはその代替策）／予定・実績
・定期報告=脆弱性管理の実施報告
・変更管理＝システム変更作業報告（セキュリティパッチ適用状況報告を含む）
④ 実施可能な脆弱性対策を実施しなかったことによる情報セキュリティインシデントが 1 件も発生しないこと。

(5) 脆弱性管理の要件

脆弱性対策について、以下の管理を行う。

① 対象プロダクト・バージョンの把握

・各情報システムにおいて管理対象とするプロダクトとバージョンを特定するとともに脆弱性情報の収集及びパッチの取得方法を(事前に)整備する。

② 脆弱性情報の収集及び対策の要否判断

・管理対象のプロダクトに係る脆弱性情報の公開状況を定期的に収集する。

・収集した脆弱性情報をもとに影響・緊急度、対策の必要性、情報システムへ与える影響・リスクを考慮し、対策の要否を判断する。

③ 脆弱性対策計画の策定と実施

・対策が必要と判断した場合は、セキュリティパッチの適用計画、または、その代替策(回避方法)の実施計画を策定する。

・対策が情報システムに与える影響について事前検証を行った上、実施する。
対策が情報システムの構成変更を伴う場合は、「4.4 変更管理」に拠るものとする。

・対策計画の策定及び実施状況の管理

(6) 標準化

① 管理状況については PMDA 標準書式を使用する。

・管理対象とするソフトウェアのプロダクトとバージョンについては、各情報システムの設計書等のソフトウェア関連項目を基に、「脆弱性管理対象ソフトウェア一覧」を使用し管理する。

・管理対象とするソフトウェアの脆弱性の有無、対策の要否、対策の実施概要については、「脆弱性対策管理簿」を使用し管理する。

② 定期的(月次)報告

・各情報システムにおける管理対象とするプロダクト・バージョンについて内容に更新があった際は、「脆弱性管理対象ソフトウェア一覧」を使用し速やかに報告する。

・脆弱性対策の要否及び対策の実施状況について、「脆弱性対策管理簿」を使用し、定時(月次)で報告する。

※「脆弱性対策管理簿」の作成にあたっては「脆弱性対策管理簿記載要領」を参照すること。

参考 脆弱性情報収集時の参考 URL 一覧 (「IPA 脆弱性対策の効果的な進め方(実践編)」より)

種別	URL
脆弱性関連情報データベース	■国内 ・JVN (Japan Vulnerability Notes) https://jvn.jp/ ・脆弱性対策情報データベース JVN iPedia https://jvndb.jvn.jp/ ■海外 ・NVD(National Vulnerability Database) https://nvd.nist.gov/ ・Vulnerability Notes Database

	https://www.kb.cert.org/vuls/ ・Metasploit（攻撃情報あり） https://www.metasploit.com/ ・Exploit Database（攻撃情報あり） https://www.exploit-db.com/
ニュースサイト	■国内 ・CNET ニュース：セキュリティ https://japan.cnet.com/news/sec/ ・ITmedia エンタープライズ セキュリティ http://www.itmedia.co.jp/enterprise/subtop/security/index.html ・ITpro セキュリティ https://tech.nikkeibp.co.jp/genre/security/ ■海外 ・ComputerWorld Security （米国中心） https://www.computerworld.com/category/security/ ・The Register Security （英国・欧州中心） https://www.theregister.co.uk/security/
注意喚起サイト	■国内 ・IPA：重要なセキュリティ情報一覧 https://www.ipa.go.jp/security/announce/alert.html ・JPCERT/CC 注意喚起 https://www.jpcert.or.jp/at/2018.html
	・警察庁：警察庁セキュリティポータルサイト https://www.npa.go.jp/cyberpolice/ ■海外 ・米国：US-CERT https://www.us-cert.gov/ncas ・米国：ICS-CERT https://ics-cert.us-cert.gov/
製品ベンダー	■定例アップデート ・マイクロソフト セキュリティ更新プログラム ガイド https://portal.msrc.microsoft.com/ja-jp/security-guidance ・オラクル Critical Patch Update と Security Alerts https://www.oracle.com/technetwork/jp/topics/security/alerts-082677-ja.html

■クライアント製品など

・Apple セキュリティアップデート

https://support.apple.com/ja-jp/HT201222

・Adobe セキュリティ速報およびセキュリティ情報

https://helpx.adobe.com/jp/security.html

・Mozilla サポートの検索

https://support.mozilla.org/ja/

■サーバ、ネットワーク製品など

・シスコ - セキュリティアドバイザリ

https://www.cisco.com/c/ja_jp/support/docs/csa/psirt-index.html

・HP - サポートホーム

https://support.hp.com/jp-ja

・日立 -セキュリティ情報

https://www.hitachi.co.jp/hirt/security/index.html

・富士通 - セキュリティ情報

https://www.fujitsu.com/jp/support/security/

https://www.fujitsu.com/jp/products/software/resources/condition/security/

・NEC - NEC 製品セキュリティ情報

https://jpn.nec.com/security-info/

・IBM - IBM Support

https://www.ibm.com/support/home/?lnk=ushpv18hcwh1&lnk2=support

・Red Hat - Red Hat Product Errata

https://access.redhat.com/errata/#/

■セキュリティ製品など

・シマンテック -セキュリティアップデート

https://www.symantec.com/ja/jp/security_response/securityupdates/list.jsp?fid=security_advisory

■オープンソースなど

・Apache Foundation

https://httpd.apache.org/ (Apache HTTP サーバ)

https://tomcat.apache.org/ (Apache Tomcat)

https://struts.apache.org/ (Apache Struts)

・ISC (Internet Systems Consortium)

https://www.isc.org/downloads/bind/ (BIND)

https://www.isc.org/downloads/dhcp/ (DHCP)

・OpenSSL

https://www.openssl.org/

4．10 アクセス権管理

(1) 目的

システムを利用するユーザ・アカウントを保護するため、及び、なりすましによる不正ログインの可能性を低減するために、ユーザ・アカウントを役割権限別に分類した上で管理方法を取決めてセキュリティレベルを維持する。

(2) 業務の概要

システムを利用するサーバ OS、ミドルウェア、アプリケーション・ソフトウェア、及びネットワーク機器のアカウントを対象にアクセス権の管理を行う。

(3) 管理対象

本番システム環境での全てのアカウント（社外の取引先等に提供しているアカウントを含む）のアクセス権を管理対象とする。

本番環境	アクセス権管理の対象
システム・ソフトウェア	OS ユーザID
ミドルウェア	DBMSユーザID、ジョブスケジューラ・ユーザID、他
アプリケーション・ソフトウェア	アプリケーション・ユーザID
ネットワーク機器	各ネットワーク機器の管理者用ID

(4) 業務の管理指標

アクセス権管理業務を評価するための評価指標として以下を定義する。

① 期間内に発生したユーザID登録・変更・削除の件数
② 特権（高権限）ユーザID別の貸出し件数と用途
③ アカウントおよびアクセス権の定期棚卸しで、発見された不備項目
④ 不適切／不正なアクセス権限の設定によって発生したインシデントの件数
⑤ アクセス権限の再設定が必要となったインシデントの件数
⑥ 間違ったアクセス権限の設定によって提供不能になったサービスの件数
⑦ 間違ったアクセス権限の設定によって生じた不正アクセスの件数

(5) アカウント管理の要件

・【アカウント（ID）の付与】

①情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む）する。

②識別コードの付与に当たっては、.単一の情報システムにおいて、ある主体に付与した識別コードを別の主体に対して付与することを禁止する

③主体以外の者が識別コード又は主体認証情報を設定する場合に、主体へ安全な方法で主体認証情報を配布する。

④識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認証情報を速やかに変更するよう、促す。

⑤知識による主体認証方式を用いる場合には、他の情報システムで利用している主体認証情報を設定しないよう主体に注意を促す。

⑥情報システムを利用する主体ごとに識別コードを個別に付与する。ただし、判断の下やむ

を得ず共用識別コード（共有 ID）を付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関するルールを定め、そのルールに従って利用者に付与する。

⑦体認証情報の不正な利用を防止するために、主体が情報システムを利用する必要がなくなった場合には、当該主体の識別コードを無効にする。

・【特権 ID と使用者の限定】

①使用者限定の保証

・パスワードの堅牢性

できだけ長い桁数、推測困難かつ記憶が容易となる工夫

・パスワードの厳正管理

業務で使用する必要がある者しか知ることができないようにする

パスワード情報へのアクセス制限

ID 使用者の離任時はパスワード変更を必須

②利用時の承認と記録

・特権 ID を利用して作業を行った結果の記録 （特権 ID 使用管理簿の記載）

・利用状況のモニタリング

サーバのログイン・ログアウトログの出力リストと特権 ID 使用管理簿の作業実績に記載されている日時を照合し、記載されている日時から逸脱する時間帯のログデータがないことをチェック

※工数の許す範囲で、重要サーバに絞り、無作為に抽出した数件のログインに該当する作業のチェック等工夫する

(6) 標準化

・全てのアカウント（ID）について、以下の管理を行う。

①アカウント（ID）管理台帳の作成

ID管理台帳を基に ID の新規・変更・削減の状況について、定期(月次)報告する。

②定期(月次)報告

ID管理台帳を基に ID の新規・変更・削減の状況について、定期(月次)報告する。

③ID棚卸し

全てのIDの棚卸しを以下の手順を参考にし、定期的（最低1回／年）に実施し、報告を行う。

（棚卸し手順）

a. 登録 ID 抽出リスト出力
b. ID 管理台帳突合
c. 棚卸しリスト作成
d. ID 使用者の確認、権限の妥当性の検証
e. 不要 ID(初期登録（ビルドイン）ID を含む）削除と不適切権限の修正
f. ID 管理台帳更新
g. 棚卸実施報告書の作成

※アカウント（ID）管理用資料は、「参考資料_ID 管理用各書式ひな型」を参考に各情報システムにおいて適宜定める。

・特権IDについて、以下の管理を行う。

①特権ID台帳の作成

※添付「特権ID管理台帳」を使用する。

※各情報システムの状況等によって、一部改修して使用しても構わない。
ただし、項目の削除は認めない。

※監査等にて提示要求があった場合は、速やかに提示できるよう保管する

②特権ID(システムID)使用管理簿の作成(またはログ抽出)

※添付「特権 ID 使用管理簿」を使用する。各情報システムの状況等によって、一部改修して使用しても構わない。ただし、項目の削除は認めない。

※ログイン・ログアウトのログ(または画面コピー)を必ず保管(または添付)し、監査等にて提示要求があった場合は、速やかに提示できるよう保管する

③定期(月次)報告

特権ID(システムID)台帳ならびに特権ID(システムID)使用状況を、定期(月次)報告する。
(ログまたは画面コピーは、月次報告不要)

④特権ID棚卸し

特権IDの棚卸しを定期的(年 2 回程度)に実施し、報告を行う。(報告書式任意)

棚卸し点検内容は以下の通り

〇台帳は、本当に使用する者を登録しているか?(体制図と一致しているか?)
・体制から外れた者が削除されずに残っていないか?
・使用予定がない者が登録されていないか?

〇台帳と使用管理簿の相関は一致しているか?

〇使用管理簿とログ(または画面コピー)保管の相関は一致しているか?

4. 11 キャパシティ管理

(1) 目的

キャパシティ管理の目的は、ビジネスが必要とするときに、必要なキャパシティを適正なコストで提供することである。 すなわち、

① ビジネスの需要に対する供給
ビジネスの変化に合わせて、ITサービスの対応にもスピードが要求される。 キャパシティ管理は、現在から将来にわたるビジネス需要・要件に合わせて、ITインフラストラクチャーのキャパシティを最大限に活用できるようにすることを目的とする。

② キャパシティに対するコスト
一方、必要以上のキャパシティを確保すると購入や運用のための費用が膨らみ、ビジネスの観点からコストを正当化できない。 キャパシティを最適化し、費用対効果が高いITサービスを提供することもキャパシティ管理の目的である

(2) 業務の概要

このプロセスは、次の3つのサブプロセスから構成される。

① ビジネスキャパシティ管理

ITサービスに対する将来のビジネス需要・要件を収集・検討し、それによって、ITサービスのキャパシティを確実に実装させるための計画の立案、予算化、構築がタイムリーに実施されるようにする。

② サービスキャパシティ管理

実際のサービスの利用と稼働のパターン、山と谷を理解して、運用中のITサービスのパフォーマンスを監視し、それによって、SLAの目標値を達成し、ITサービスを要求どおりに機能させる。

③ コンポーネントキャパシティ管理

ITインフラストラクチャーの個々のコンポーネントのパフォーマンスとキャパシティ、使用状況を監視し、それによって、SLAの目標値を達成・維持するために、コンポーネントの利用を最適化する。

(3) 管理対象

本基準の適用システムにおけるハードウェア、ソフトウェア、ネットワーク、アプリケーション、及び人的リソースを対象とする。

(4) 業務の管理指標

キャパシティ管理業務を評価するための評価指標として以下を定義する。

① CPU、ディスク、メモリ、ネットワーク容量などの閾値に対する需要の割合
② ITサービスのパフォーマンス不足に起因するSLA違反やインシデントの発生件数
③ ITコンポーネントのパフォーマンス不足に起因するSLA違反やインシデントの発生件数
④ 正規の購入計画に含まれていなかった、パフォーマンスの問題解決のために急きょ行った購入の数又は金額

4．12 可用性管理

(1) 目的

可用性管理の目的は、ビジネス部門に対して、費用対効果が高いITサービスを持続して提供することであり、そのためにITインフラストラクチャーを整備し、それをサポートするITサービス部門の能力を最適化させる。

(2) 業務の概要

可用性管理の活動は大きく、1）可用性要件の把握、2）可用性の設計、及び3）可用性の改善活動の3つに分けられる。

具体的には、以下の可用性管理の3要素の目標値を設定し、設定した可用性のレベルを達成・維持・向上させることである。

① 可用性

可用性とは、ITサービスが必要なときに使用できる割合のことで、一般的には稼働率という指標を用いて表される。

稼働率（%）＝（サービス提供時間－停止時間）÷サービス提供時間

② 信頼性

提供されるITサービスにおける、不具合の発生しにくさ／故障しずらさを表す。
平均故障間隔＝（使用可能な時間－総停止時間）÷（サービス中断の回数－1）

③ 保守性

ITサービスが停止又は品質低下した際に、いかに早く復旧できるかを示す指標。
平均修理時間＝修理時間の合計÷サービス中断の回数

可用性について極めて重要なことは、ユーザの求めるシステムの可用性レベルをどのように達成するかについて、システム設計時に真剣に検討し、システム構築時に実現し、システムの運用において継続的に改善することである。

(3) 管理対象

本基準の適用システムにおけるハードウェア、ソフトウェア、ネットワーク、及びアプリケーションを対象とする。

(4) 業務の管理指標

可用性管理業務を評価するための評価指標として以下を定義する。

① 可用性の割合
② 平均故障間隔
③ 平均修理時間
④ サービスの中断回数
⑤ 定期的なリスク分析、及びレビューの完了の件数

4．13　サービスレベル管理

(1)　目的

ユーザニーズを満足する適正なサービスレベルおよび管理指標を設定し、これを実績管理することにより質の高いサービスの提供を図る。

(2)　業務の概要

サービスレベルおよび各個別管理業務での管理指標の実績データを定期的に把握し、サービスレベル指標と実績の差異や傾向を継続的に分析することにより、改善策を立案し実施する。

(3)　管理対象

IT 部門が提供する全ての IT サービスに関するサービスレベルおよび各個別管理業務での管理指標を管理対象とする。

(4)　業務の管理指標

サービスレベル管理業務を評価するための評価指標として以下を定義する。

①「サービスレベル合意書」の各サービスレベル項目の達成率

②各個別管理業務での管理指標の達成率

(5)　標準化

サービスレベル管理業務を定期的(月次)に報告する。

①「サービスレベル合意書」の各サービスレベル項目の達成率

②各個別管理業務での管理指標の達成率

以上

別紙5　情報セキュリティ対策の運用要件

情報システムの運用・保守の業務遂行にあたっては、調達・構築時に決定した情報セキュリティ要件が適切に運用されるように、人的な運用体制を整備するとともに、機器等のパラメータが正しく設定されていることの定期的な確認、運用・保守に係る作業記録の管理等を確実に実施すること。

対策区分	対策方針	対策要件	運用要件	定期点検
侵害対策（AT：Attack）	セキュリティホール対策（AT-3）	運用時の脆弱性対策　（AT-3-2）	情報システムを構成するソフトウェア及びハードウェアのバージョン等を把握して、製品ベンダや脆弱性情報提供サイト等を通じて脆弱性の有無及び対策の状況を定期的に確認すること。脆弱性情報を確認した場合は情報システムへの影響を考慮した上でセキュリティパッチの適用等必要な対策を実施すること。 対策が適用されるまでの間にセキュリティ侵害が懸念される場合には、当該情報システムの停止やネットワーク環境の見直し等情報セキュリティを確保するための運用面での対策を講ずること。	脆弱性対策の実施状況は、月次で報告すること。
アクセス・利用制限（AC：Access）	アカウント管理（AC-2）	ライフサイクル管理　（AC-2-1）	主体が用いるアカウント（識別コード、主体認証情報、権限等）は、主体の担当業務に必要な範囲において設定すること。 また、アカウント管理（登録、更新、停止、削除等）の作業内容は記録し、証跡を保管すること。 アカウント棚卸を定期的に実施し、不要なアカウントを削除すること。	アカウント棚卸を定期的（年１回以上）に実施すること。
		アクセス権管理（AC-2-2）	主体が用いるアカウント（識別コード、主体認証情報、権限等）は、主体の担当業務に必要な範囲において設定すること。また、アカウント管理（登録、更新、停止、削除等）の作業内容は記録し、証跡を保管すること。 権限の再検証を定期的に実施し、不要な権限を削除すること。	ユーザーＩＤの棚卸と合わせて実施すること。
		管理者権限の保護（AC-2-3）	システム特権を付与されたアカウント及び使用者を特定し、アカウントの使用状況を記録し、アカウントの不正使用がないことを定常的に確認すること。	管理状況を「特権ＩＤ台帳」及び「特権ＩＤ使用管理簿」により、月次で報告すること。
データ保護（PR：Protect）	機密性・完全性の確保（PR-1）	受託者によるアクセス	受託者は受託した業務以外の情報へアクセスしないこと。	情報セキュリティ遵守状況は月次で報告すること。

物理対策（PH: Physical）	情報窃取・侵入対策（PH-1）	情報の物理的保護（PH-1-1）	受託者の管理区域において、受託者がＰＭＤＡより提供された情報を格納する機器は、情報の漏えいを防止するため、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。	情報セキュリティ遵守状況は月次で報告すること。
		侵入の物理的対策（PH-1-2）	受託者の管理区域において、受託者がＰＭＤＡより提供された情報を格納する機器は、物理的な手段によるセキュリティ侵害に対抗するため、外部からの侵入対策が講じられた場所に設置すること。	情報セキュリティ遵守状況は月次で報告すること。
障害対策（事業継続対応）（DA: Damage）	構成管理（DA-1）	システムの構成管理　（DA-1-1）	情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、情報システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を実際のシステム構成と合致するように維持・管理すること。	変更作業時の構成管理資料の更新については、「変更作業一覧」により、月次で報告すること。
	可用性確保（DA-2）	システムの可用性確保　（DA-2-1） 情報のバックアップの取得	システム及びデータの保全が確実に実施されるため、システム及びデータのバックアップが所定の要件通りに取得されていることを定期的に確認すること。 また、回復手順について机上訓練を実施し、バックアップや回復手順が適切に機能することを確認する。	バックアップの実施状況は、月次で報告すること。 バックアップによるリストア等回復手順については、 机上訓練を年１回以上実施すること。
サプライチェーン・リスク対策（SC: Supply Chain）	情報システムの構築等の外部委託における対策（SC-1）	委託先において不正プログラム等が組み込まれることへの対策（SC-1-1）	情報システムの運用保守において、ＰＭＤＡが意図しない変更や機密情報の窃取等が行われないことを保証するため、構成管理・変更管理を適切に実施すること。	変更管理の状況は「変更作業一覧」により、月次で報告すること。