人事給与システム運用保守及び改修業務
調達仕様書

令和７年２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）　調達件名

人事給与システム運用保守及び改修業務

（2）　用語の定義

表 1．用語の定義

用語	概要
人事管理	採用から退職までの人事情報の管理。（人事記録の作成） 採用、退職、異動、昇給、昇格、休職等の辞令発令。
勤怠管理	出退勤、時間外、勤怠提出の管理。
給与管理	・ 人事情報からの採用、退職、異動、昇給、昇格、休職等の情報の連携で、給与、賞与、期末勤勉を計算する。 ・ 追給返納計算、休職等における日割計算をする。 年末調整業務を行う。
実態調査、人件費管理	給与実態調査、指定統計等の調査資料を作成する。
臨時職員管理	雇用管理、賃金計算、期末勤勉計算の管理を行う。
社会保険管理	・ 採用者の取得や退職者の喪失事務を行う。 ・ 定時改定及び随時改定の事務を行う。 ・ 賞与の支払届を作成する。 雇用保険の事務を行う。
研修管理	職員の研修管理を行う。
人事給与システム業務パッケージ	One 人事株式会社（以下「One 人事」という。）の提供するパッケージソフトウェア「U-PDS」及び「Public HR」を指す。
医薬品医療機器総合機構の休日	「独立行政法人医薬品医療機器総合機構職員就業規則第 36 条」で定められるとおりとする。
人事情報管理システム	別調達にて導入済みである人事管理の強化と職能開発計画の運用に資するパッケージソフトウェアを指す。
人事情報管理システム（クラウドサービス）	別調達にて導入予定である人事管理の強化と職能開発計画の運用に資するクラウドサービス型パッケージソフトウェアを指す。

（３）　調達の背景

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、PMDA の理念に共感する優秀な人材の確保や、将来の働き方の多様性への対応等を見据え、人事・給与・研修等業務の効率化・強化等を目的に、人事給与システム（以下「本システム」という。）を使用し、業務を実施している。

PMDA では、今後も、本システムを使用し、人事給与業務等で使用するデータを適切に管理し、人事・給与・研修等業務を正確かつ効率的に実施して行くとともに、中長期的な視点に立ち、本システムを使用した持続的かつ発展的な業務運営を目指して行く予定でいるが、その実現に向けて、本システムの安定的な稼働の維持は不可欠であるため、本システムの設計・構造や特殊性に精通している者の技術的な支援が必要である。

（４）　業務・情報システムの概要

PMDA の人事・給与、研修等業務については、次のとおりである。

①人事関係業務

組織の体制・構造・階層及び役割・責任範囲等を管理する組織管理、PMDA 職員の採用、人材教育、キャリアプラン等を管理する人材管理、人事考課・昇給昇格等の人事評価管理業務

②給与関係業務

給与、賞与、退職金、年末調整、各種税務処理、社会保険・労働保険、各種控除処理等の給与管理業務

③研修管理業務

研修受講状況、研修実績管理等

システムの主たる利用者は、管理者として総務部業務担当職員、一般ユーザとして PMDA の役職員となる。各一般ユーザは、その役職に応じて異なる操作権限を有する。

（５）　契約条件

受託者は、落札後に以下の契約条件にて PMDA と協議の上、契約を行うこと。

ア　契約期間

契約締結日から令和 8 年 3 月 31 日までとする。

イ　SLA の締結

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。

（６）　作業スケジュール

運用業務の対象期間は、令和７年４月１日から令和８年３月 31 日までとする。

ア　受託者は、契約開始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 及び構築業者より引継ぎを受けること。

イ　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 PMDA の想定であり、応札者は本業務の特性に応じた詳細な実施スケジュールは受託者が検討すること。

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

関連する調達案件の調達単位、調達の方式、実施時期等は「表２.１　関連する調達案件の調達単位、調達の方式、実施時期等（既存契約）」及び「表２.２　関連する調達案件の調達単位、調達の方式、実施時期等（契約予定）」の通りである。

表　2.1　関連する調達案件の調達単位、調達の方式、実施時期等（既存契約）

項番	調達案件名	調達の方式	実施時期	事業者名	備考
1	次期人事給与システム運用保守及び改修業務	一般競争入札（最低価格落札方式）	令和６年４月～令和７年３月	One 人事(株)	
2	人事情報管理システム運用保守業務	事前確認型公募	令和５年４月～令和７年３月	(株)サイダス	
3	勤務管理システム保守及び運用支援業務	一般競争入札（最低価格落札方式）	令和６年２月～令和７年３月	アマノ(株)	
4	次期人事給与システム基盤設計・導入及び運用保守業務	一般競争入札（最低価格落札方式）	令和５年３月～令和 10 年 12 月	ユニアデックス(株)	
5	共用 LAN システムに係る運用支援業務	一般競争入札（総合評価落札方式）	令和５年９月～令和７年９月	(株)プロフェース・システムズ	
6	第４次会計システムの運用支援業務	一般競争入札（最低価格落札方式）	令和６年４月～令和 11 年７月	ＮＥＣネクサソリューションズ(株)	
7	文書管理・決裁システムの運用保守業務	随意契約	令和６年４月～令和 11 年３月	富士電機 IT ソリューション(株)	

表 2.2 関連する調達案件の調達単位、調達の方式、実施時期等（契約予定）

項番	調達案件名	調達の方式	実施時期	備考
1	人事情報管理システム運用保守業務	事前確認型公募	令和 7 年 4 月～ 令和 8 年 3 月	
2	人事情報管理システム（クラウドサービス）の調達及び運用保守業務	未定	令和 7 年 10 月～ 令和 11 年 3 月（予定）	
3	人事給与システムと人事情報管理システム（クラウドサービス）の連携構築業務	一般競争入札（最低価格落札方式）	令和 7 年 10 月～ （未定）	
4	勤務管理システム保守及び運用支援業務	一般競争入札（最低価格落札方式）	令和 7 年 4 月～ 令和 8 年 3 月	

なお、上記以外の関係事業者としてデータセンター事業者等がいる。

3　作業の実施内容に関する事項

（1）作業の内容

受託者は、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）に記載された作業内容および納入成果物を参照の上、以下に関し必要な作業を実施すること。
また、追加提案できることがあれば、提案書に記載して追加提案すること。

① 準備作業の内容

ア 運用準備作業

（ア）人事給与システム開発環境の構築

人事給与システム設計・開発業者の構築した人事給与システムの業務サーバは本番環境（人事給与）検証環境（人事給与）として 2 ランドスケープ構成を採用している。

受託者は、自社内での開発／検証環境として、人事給与システム開発環境を構築し、管理すること。

- 受託者は、システムの開発環境（開発用のハードウェア、開発ツール等のソフトウェア、設置場所を含む。）、作業場所、その他必要となる環境については、受託者の責任において確保すること。
- これらの環境に対しても ISO/IEC27001 認証（国際標準）に従い、十分な情報セキュリティ対策を実施すること。
- 構築手段は、検証環境からの環境複製を想定しているが、より適切な手段がある場合はその旨提案し、PMDA の了承を得ること。また、その場合には検証環境、又は本番環境に格納されている職員情報等の人事給与業務データを開発環境に保持してはならない。人事給与システム本番環境、検証環境に対する開発環境としての性能を担保すること。

- 構築作業を行うにあたっては、既に提供中の人事給与業務に影響を与えないように計画を立案し、PMDA に確認の上、作業を行うこと。

イ　実施計画書の作成

受託者は、令和 7 年 4 月 1 日の運用業務の開始までに、PMDA の指示に基づき体制図、作業内容、作業体制、作業分担、スケジュール、文書管理要領、変更管理要領、WBS 及び WBS の項目ごとの工数等を記載した実施計画書及び「９　（１）情報セキュリティ対策の実施」に記載している要件を満足する情報セキュリティ管理計画書を作成し、PMDA の承認を受けること。

② 運用に係る作業の内容

ア　中長期的又は年度ごとの運用・保守作業計画の確定支援

受託者は、PMDA が中長期又は年度ごとの運用・保守作業計画を確定するに当たり、情報システムの構成やライフサイクルを通じた運用業務及び保守作業の内容について、計画案の妥当性に関する意見提示、情報提供等の支援を行うこと。

イ　定常時対応

（ア） 受託者は、別紙３「業務要件」の「運用業務の実施範囲」に示す運用業務（システム監視、システム設定、ヘルプデスク業務、運用管理、ユーザー管理、サービスデスク提供等）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。

（イ） 受託者は、別紙４「システム運用管理基準」を参照の上、以下の内容について月次で運用報告を取りまとめ、PMDA に報告すること。

A) 運用期間・報告日・イベントの概況等の基本状況
B) 作業実績等の運用状況　（WBS 単位の作用内容、工数等）
C) 情報システムの稼働業務状況
D) 問合せ管理運用状況（サービスデスク稼働状況）（別紙４参照）
E) インシデント管理状況（別紙４参照）
F) 問題管理状況(別紙４参照)
G) 変更管理状況（別紙４参照）
H) バックアップ取得状況(別紙４参照)
I) 情報セキュリティ管理状況（情報セキュリティ遵守状況）(別紙４参照)
J) 脆弱性管理（別紙４参照）
K) アクセス権管理状況（特権（高権限 ID）管理状況）(別紙４参照)
L) システムリソース状況　（キャパシティ管理、可用性管理）(別紙４参照)
M) サービスレベル達成状況（別紙４参照）
N) データ外部保管状況

O) 情報システムの定期点検状況（別紙５「情報セキュリティ対策の運用要件」参照）

P) 教育･訓練状況

Q) リスク課題の把握・対応状況

（ウ） 受託者は、月間の運用実績を評価し、達成状況が SLA 要求水準を満たさ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。

（エ） 受託者は、運用作業報告書の内容について、月例の定期運用会議を開催し、その内容を報告すること。

受託者は、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、PMDA 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。

ウ 情報システムの現況確認支援

（ア） 受託者は、年 1 回、PMDA の指示に基づき、システム資産簿と情報システムの現況との突合・確認（以下「現況確認」という。）を支援すること。

（イ） 受託者は、現況確認の結果、システム資産簿と情報システムの現況との間の差異がみられる場合は、運用実施要領に定める変更管理方法に従い、差異を解消すること。

（ウ） 受託者は、現況確認の結果、ライセンス許諾条件に合致しない状況が認められる場合は、当該条件への適合可否、条件等を調査の上、PMDA に報告すること。

（エ） 受託者は、現況確認の結果、サポート切れのソフトウェア製品の使用が明らかとなった場合は、当該製品の更新の可否、更新した場合の影響の有無等を調査の上 PMDA に報告すること。

エ 運用作業の改善提案

受託者は、年度末までに年間の運用実績を取りまとめるとともに、必要に応じて中長期運用・保守作業計画、運用計画、運用実施要領に対する改善提案を行うこと。

③ 保守に係る作業の内容

ア 中長期又は年度ごとの運用・保守作業計画の確定支援

受託者は、PMDA が中長期又は年度ごとの運用・保守作業計画を確定するに当たり、情報システムの構成やライフサイクルを通じた運用業務及び保守作業の内容について、計画案の妥当性の確認、情報提供等の支援を行うこと。

イ　定常時対応

（ア）　受託者は、別紙３「業務要件」の「保守業務の実施範囲」に示す保守業務（不具合受付等）及び定期点検（ソフトウエア保守）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。

（イ）　受託者は、定期点検（ソフトウエア保守）の結果について、速やかに PMDA へ報告すること。またシステム設定値等の差異がみられる場合は、PMDA へ報告の上、変更管理方法に従い、差異を解消すること。

（ウ）　受託者は、保守作業計画及び保守実施要領に基づき、保守作業の内容や工数などの作業実績状況（情報システムの脆弱性への対応状況を含む。）、サービスレベルの達成状況、情報システムの定期点検状況、リスク・課題の把握・対応状況について月次で保守作業報告書を取りまとめること。

（エ）　受託者は、月間の保守実績を評価し、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。

（オ）　受託者は、保守作業報告書の内容について、月例の定期運用会議を開催し、その内容を報告すること。

ウ　情報システムの現況確認支援

（ア）　受託者は、年１回、PMDA の指示に基づき、システム資産簿と情報システムの現況との突合・確認（以下「現況確認」という。）を支援すること。

（イ）　受託者は、年１回、PMDA の指示に基づき、情報システム台帳（セキュリティ要件に係る事項）の作成･更新を支援すること。

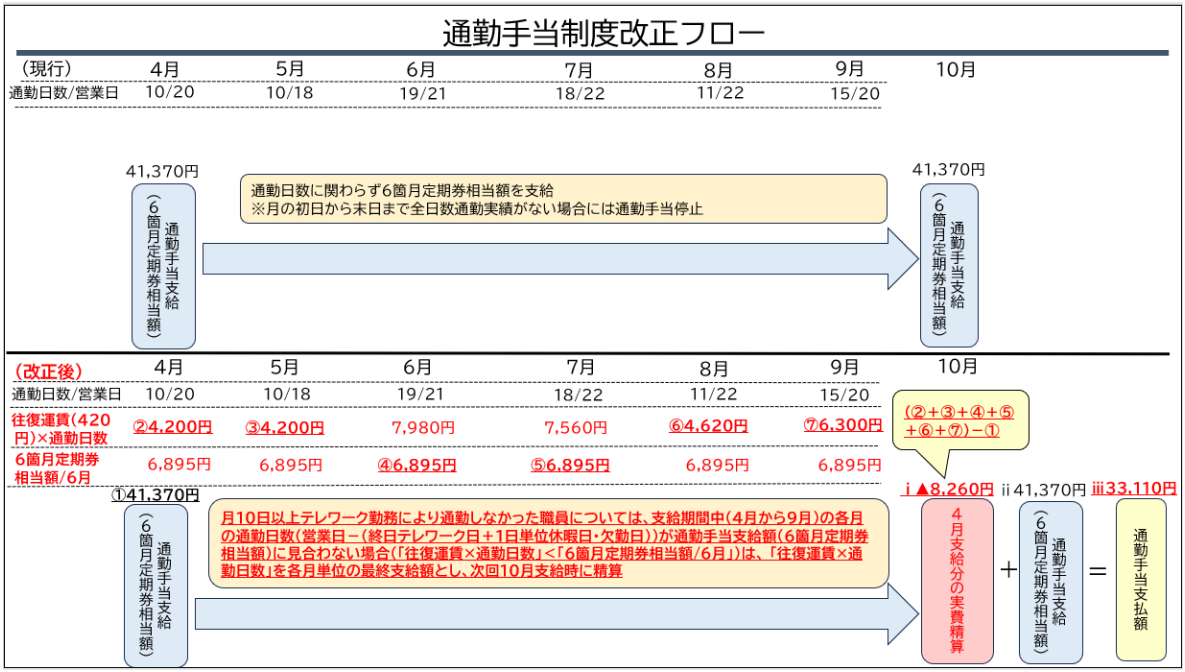
エ　保守作業の改善提案

受託者は、年度末までに年間の保守実績を取りまとめるとともに、必要に応じて中長期保守・保守作業計画、保守計画、保守実施要領に対する改善提案を行うこと。

④通勤手当制度改正に係る改修

PMDA では、令和７年４月から通勤手当の実績ベース（※）での支給に係る運用開始を予定しており（実績ベースでの支給初回は令和７年 10 月を予定）、そのための所要の改修を実施する。

※　通勤手当の支給額は、基本的に６箇月定期券相当額を６箇月に一度支給する運用となっているが、月 10 日以上テレワーク勤務により通勤実績がない場合は、その勤務しなかった日数（終日テレワーク日のほか、１日単位の年次休暇、欠勤含む）相当額分を減額して、次回通勤手当支給月に支給。（下記図参照）



PMDA通勤手当制度改正のシステム実装要件定義

※（ ）は実装対象のシステム

①終日テレワーク実績日数のカウントと、対象者一覧（月10日以上テレワーク勤務により通勤しなかった職員）と対象者の通勤日数（営業日−未通勤日（終日テレワーク日＋1日単位休暇日・欠勤日））の抽出（勤務管理システム）
②登録した6箇月定期券相当額の経路に係る往復運賃の自動算出（UPDSと駅すぱあとの連携）
③往復運賃×通勤日数（営業日−未通勤日（終日テレワーク日＋1日単位休暇日・欠勤日））の自動計算（UPDS ※勤務管理システムと連携）
④6箇月定期券相当額の1/6の数字の自動計算と、往復運賃×通勤日数と照らし合わせた上で、支給対象期間（6箇月）における精算額の自動計算。（UPDS）
⑤支給月において、精算額と通勤手当支給額（6箇月定期券相当額）を相殺し、当月の支払額を自動計算で算出する。（UPDS）

⑤　インシデント発生時及び大規模災害発生時の対応

（ア）　受託者は、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。

（イ）　受託者は、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。

（ウ）　受託者は、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。

（エ） 受託者は、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。

（オ） 受託者は、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

（カ） 受託者は、大規模災害等の発災時には、PMDA の指示を受けて、必要な対応を実施すること。また定常時においても、運用継続計画（情報システム用 BCP）を参照し、PMDA と協議の上、大規模災害時の手順書見直し・整備等の必要な対応を実施すること。

⑥ 作業報告

ア 作業工数実績の報告

受託者は、本業務で実施する WBS の各項目単位の作業内容とその工数について、月次で PMDA に報告すること。報告の様式等に関しては、業務開始時に PMDA と協議し決定すること。

⑦ 引継ぎ

ア 現行運用事業者からの引継ぎ

受託者は、現行運用事業者から令和 7 年 4 月 1 日からの運用に必要な事項（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)）の引継ぎ、及び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（運用作業の計画書や報告書、運用設計書及び運用手順書等の一覧）を基に自主的に業務習熟を行うこと。現行運用事業者からの引継作業は受託者の負担と責任において実施すること。

また、運用に必要な以下のマニュアル等について、受託者の体制等に基づいた見直しを実施し、PMDA の承認を得ること。

- 問合せ、障害等の対応及び管理に関する手法・手順

- システム運用マニュアル、運用業務マニュアル

（２）　システム資産簿登録に係る作業

ア　PMDA においては、システム構成情報を一元管理するシステム資産簿を作成している。受託者は、本システムで利用する機器、ソフトウェア、ネットワーク等の構成情報を PMDA へ報告し、一元管理するシステム資産簿の管理情報について常に最新の状態を保つこと。なお、以下に示す事項以外に管理が必要と考えられる事項があれば PMDA と協議の上、合わせて管理すること。

イ　受託者は PMDA が指定するシステム資産簿登録用シートを、PMDA が指示する時期に提出すること。

（ア）　ハードウェア管理台帳（ハードウェア名称、システムモデル、シリアル番号、サポート内容・期間等）

（イ）　ソフトウェア管理台帳（ソフトウェア名称、エディション・バージョン、ソフトウェアの搭載機器、サポート内容・期間等）

（ウ）　ライセンス管理台帳（ソフトウェア名称、エディション・バージョン、ライセンス番号（シリアル番号）、提供形態、有効期限、保有ライセンス数等）

（エ）　その他 PMDA が指定する項目

ウ　受託者は、本システムを構成する機器・ソフトウェアの変更、業務アプリケーションの変更、仕様書、設計書等の本システムにかかる各種ドキュメントの変更について、変更理由、変更内容、影響範囲、対応状況、責任者、対応者等と記録し、一元管理を行うこと。

（３）　成果物の範囲、納品期日等

① 成果物

作業工程別の納入成果物を表 3.に示す。ただし、納入成果物の構成、詳細については、受注後、PMDA と協議し取り決めること。

表 3.　工程と成果物

項番	工程	納入成果物（注 1）	納入期日	納品に関する注意事項
1	準備	運用準備作業に関する実施計画書（運用準備作業）	契約締結日から 2 週間以内	
2	計画	・実施計画書（体制図、作業内容、作業体制、作業分担、スケジュール、文書管理要領、変更管理要領、WBS）	令和 7 年 4 月 1 日の運用業務の開始まで	

項番	工程	納入成果物（注 1）	納入期日	納品に関する注意事項
		・情報セキュリティ管理計画書（情報セキュリティ対策実施内容及び管理体制）		
3	運用	・システム運用マニュアル(注２) ・運用業務マニュアル(注３) ・システム関連ドキュメント ・プログラム・ツール等	令和 8 年 3 月 24 日	
4	その他	・作業週報 ・月例報告資料 ・打合せ資料 ・議事録 ・障害等作業記録 ・運用支援報告書 ・改修に伴うドキュメント一式	令和 8 年 3 月 24 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　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

注３　システム運用上の業務プロセスを定めた「業務フロー及び手順書」とし、次のシステム運用業務について作成･更新するものとする。

(ｱ)問合せ管理プロセス　(ｲ)インシデント管理プロセス　(ｳ)変更管理プロセス　(ｴ)リリース管理プロセス　(ｵ)構成管理プロセス　(ｶ)問題管理プロセス　(ｷ)各定期点検プロセス　(ｸ)リスク管理プロセス　(ｹ)課題管理プロセス　(ｺ)情報セキュリティ管理プロセス。

② 納品方法

表 3.の納入成果物を含む全ての納入成果物を令和 8 年 3 月 24 日までに納品すること。なお、納入成果物については、以下の条件を満たすこと。

ア　成果物は、すべ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。

イ　用字・用語・記述符号の表記については、「公用文作成の要領」に準拠すること。

ウ　情報処理に関する用語の表記については、日本産業規格（JIS）の規定に準拠すること。

エ　受託者は、指定のドキュメントを外部電磁的記録媒体（CD‐R 等)により納品すること。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部電磁的記録媒体（CD‐R 等）のみとする。

オ　紙媒体のサイズは、日本産業規格 A 列 4 番を原則とする。図表については、必要に応じて A 列 3 番を使用することができる。また、バージョンアップ時等に差替えが可能なようにバインダ方式とする。

カ　外部電磁的記録媒体に保存する形式は Microsoft365 で読み込み可能な形式及び PDF 形式とすること。ただし、PMDA が他の形式による提出を求めた場合は、これに応じること。なお、受託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。

キ　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。

ク　外部電磁的記録媒体は、2 部納品すること。

ケ　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。

コ　成果物の作成に当たって、CAD 等の上記以外の特別なツールを使用する場合は、PMDA の承認を得ること。

サ　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。

シ　外部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。

ス　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。

セ　納品に当たっては、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。

ソ　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、案について受託者と協議の上、決定する。

③　納品場所

独立行政法人医薬品医療機器総合機構　総務部

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。

４　満たすべき要件に関する事項

本業務の実施にあたっては、以下に記載の各要件を満たすこと。

○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

○閲覧資料　セキュリティ管理要件書(ひな型)

情報セキュリティインシデント対処手順書

５　作業の実施体制・方法に関する事項

（１）　作業実施体制

受託者は、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、受託者は、必要な要員の調達を遅滞なく実施し、要員を確定すること。

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 本情報システムに PMDA の意図しない変更が行われるなど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 と受託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）・実績及び国籍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 受託者は、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託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、受託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。

⑤ 受託者は、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。

⑥ 作業実施体制の編成にあたっては、特定の要員への依存、要員ごとの担当領域の縦割りにより、連携性・機動性に乏しい状態にならないようにすること。

⑦ 業務開始後、PMDA が、作業実施体制が十分に機能していないと判断し、体制の変更を依頼した場合、受託者は速やかに応じなければならない。

（２）　作業要員に求める資格等の要件

作業要員に求めるスキル及び資格等の要件を以下に示す。但し、体制構築においては費用対効果の観点を踏まえ、管理者及び作業実施者を適切に配置すること。

① 運用責任者･リーダの必要スキル

A) システム運用保守業務経験が 10 年以上

B) システム運用保守業務のマネジメント経験が 3 年以上

C) ITIL ファウンデーションの資格もしくは ITIL を用いた作業管理の業務経験

D) PMP 又は、情報処理技術者(プロジェクトマネージャ)資格※

※ただし、当該資格保有者等と同等の能力を有することが経歴等において明らかな者については、これを認める場合がある（その根拠を明確に示し、PMDA の理解を得ること）

E) 日本語による「円滑な意思疎通」が図れること

F) PMDA の人事・給与・研修等業務に係る主な諸規程（表 5.参照）に基づき業務の本質を理解しており、本システムの運用・保守にあたり、PMDA に逐次業務の説明を求めることなく担当者とスムーズな会話ができる知識を有していること

G) 上記の専門性について、各業務場面において的確に駆使するとともに、専門性を有していない者にも、端的に理解が行き届くよう、適切な言葉を駆使して説明できる対話力を有していること。

H) PMDA の社会的役割、本システムの役割（人事・給与・研修等業務を持続的に、正確かつ効率的に実施）、組織における基幹業務である人事・給与・研修等業務の重要性を理解し、緊張感を持って業務に従事できること。

② 以下の専門スキル要員を体制に含めること。 各項目の条件に関しては、1 人ですべての条件を充足する必要はないが、条件を充足していない要員がいることが原因で、本業務の円滑な遂行に支障が出ることがないような体制を構築する。

なお、実施計画書に含まれる体制図に、次の内容を明記した資料を添付する。

ⅰ体制の各要員が、以下の各項目のうち満たしている条件とその客観的な根拠

ⅱ本業務の円滑な遂行の観点からの各要員の配置根拠と満たしている条件との関連性

A) システム運用保守業務経験が 5 年以上

B) システム運用保守業務のマネジメント経験があること

C) ITIL ファウンデーションの資格もしくは ITIL を用いた作業管理の業務経験

D) PMP 又は、情報処理技術者(プロジェクトマネージャ)資格

E) PMDA にて現行関連システムの設計書等を閲覧し、内容を十分理解していること

F) 情報処理技術者(情報セキュリティスペシャリスト試験　(SC))、又はテクニカルエンジニア（情報セキュリティ）資格を保持していること。又は、CISSP、CISM 認定資格を保持すること。

G) PMDA の人事・給与・研修等業務に係る主な諸規程（表 5.参照）に基づき業務の本質を理解しており、本システムの運用・保守にあたり、PMDA に逐次業務の説明を求めることなく担当者とスムーズな会話ができる知識を有していること

H)システムでの人事給与関連の業務を理解しており、本業務システムの設計にあたり、PMDA に逐次業務の説明を求めることなく担当者とスムーズな会話ができる知識を有していること。

I) 日本語による「円滑な意思疎通」が図れること

J) 上記の専門性について、各業務場面において的確に駆使するとともに、専門性を有していない者にも、端的に理解が行き届くよう、適切な言葉を駆使して説明できる対話力を有していること。

K) PMDA の社会的役割と、本システムの役割（人事・給与・研修等業務を持続的に正確かつ効率的に実施）、組織における基幹業務である人事・給与・研修等業務の重要性を理解し、緊張感を持って業務に従事できること。

また、業務開始後、PMDA が各要員が十分に機能していないと判断し、体制の変更を依頼した場合、上記の条件の充足に関わらず、受託者は速やかに応じなければならない。

表 5.　PMDA の人事・給与・研修等業務に係る諸規程

No	＜規程名称＞
1	独立行政法人医薬品医療機器総合機構職員就業規則
2	独立行政法人医薬品医療機器総合機構事務補助員就業規則
3	独立行政法人医薬品医療機器総合機構嘱託等就業規則
4	独立行政法人医薬品医療機器総合機構継続雇用職員就業規則
5	独立行政法人医薬品医療機器総合機構任期付職員就業規則
6	独立行政法人医薬品医療機器総合機構特任職員就業規則
7	独立行政法人医薬品医療機器総合機構継続雇用事務補助員就業規則
8	独立行政法人医薬品医療機器総合機構役員給与規程
9	独立行政法人医薬品医療機器総合機構役員給与規程の実施細則
10	独立行政法人医薬品医療機器総合機構職員給与規程
11	独立行政法人医薬品医療機器総合機構職員給与規程の実施細則
12	独立行政法人医薬品医療機器総合機構役員退職手当支給規程
13	独立行政法人医薬品医療機器総合機構職員退職手当支給規程
14	独立行政法人医薬品医療機器総合機構人事評価規程
15	独立行政法人医薬品医療機器総合機構人事評価規程の実施細則
16	独立行政法人医薬品医療機器総合機構在外職員の給与等に関する規程
17	独立行政法人医薬品医療機器総合機構在外職員の給与等に関する実施細則

18	独立行政法人医薬品医療機器総合機構事務補助員の賞与係数及び勤務日数に基づく期間率に関する実施細則
19	独立行政法人医薬品医療機器総合機構嘱託等の賞与係数及び勤務日数に基づく期間率に関する実施細則
20	独立行政法人医薬品医療機器総合機構におけるテレワーク勤務に関する規程

（３）　作業場所

① 受注業務の作業場所（サーバ設置場所等を含む）は、（再委託も含めて）PMDA 内、又は日本国内で PMDA の承認した場所で作業すること。
② 受注業務で用いるサーバ、データ等は日本国外に持ち出さないこと。
③ PMDA 内での作業においては、必要な規定の手続を実施し承認を得ること。
④ なお、必要に応じて PMDA 職員は現地確認を実施できることとする。

（４）　作業の管理に関する要領

① 受託者は、PMDA の指示に従って運用業務に係るコミュニケーション管理、体制管理、進捗管理、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 受託者は、PMDA の指示に従って保守業務に係るコミュニケーション管理、体制管理、進捗管理、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。
③ PMDA が管理するエリアからの情報の持ち出しは許可しない。持ち出しが必要な場合は事前に PMDA に対し、持ち出し目的、対象情報の範囲、情報利用端末、情報の利用者等に関し申請を行うこと。また受託者は、持ち出した情報を台帳等により管理すること。さらに受託者は、持ち出した情報は使用後に確実に消去し、そのエビデンスを提出すること。

６ 作業の実施に当たっての遵守事項

（１）　基本事項

受託者は、次に掲げる事項を遵守すること。
① 本業務の遂行に当たり、業務の継続を第一に考え、善良な管理者の注意義務をもって誠実に行うこと。
② 本業務に従事する要員は、PMDA と日本語により円滑なコミュニケーションを行う能力と意思を有していること。
③ 本業務の履行場所を他の目的のために使用しないこと。
④ 本業務に従事する要員は、履行場所での所定の名札の着用等、従事に関する所定の規則に従うこと。

⑤　要員の資質、規律保持、風紀及び衛生・健康に関すること等の人事管理並びに要員の責めに起因して発生した火災・盗難等不祥事が発生した場合の一切の責任を負うこと。
⑥　受託者は、本業務の履行に際し、PMDA からの質問、検査及び資料の提示等の指示に応じること。また、修正及び改善要求があった場合には、別途協議の場を設けて対応すること。
⑦　次回の本業務調達に向けた現状調査、PMDA が依頼する技術的支援に対する回答、助言を行うこと。
⑧　本業務においては、業務終了後の運用等を、受託者によらずこれを行うことが可能となるよう詳細にドキュメント類の整備を行うこと。

（２）　機密保持、資料の取扱い

本業務を実施する上で必要とされる機密保持に係る条件は、以下のとおり。
①　受託者は、受注業務の実施の過程で PMDA が開示した情報（公知の情報を除く。以下同じ。）、他の受託者が提示した情報及び受託者が作成した情報を、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洩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。
②　受託者は、本受注業務を実施するにあたり、PMDA から入手した資料等については管理簿等により適切に管理し、かつ、以下の事項に従うこと。
- 複製しないこと。
- 用務に必要がなくなり次第、速やかに PMDA に返却又は消去すること。
- 受注業務完了後、上記①に記載される情報を削除又は返却し、受託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 に提出すること。

③　応札希望者についても上記①及び②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。

（３）　遵守する法令等

本業務を実施するにあたっての遵守事項は、以下のとおり。
①　受託者は、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、行政機関の保有する個人情報の保護に関する法律等の関連法規及び労働関係法令を遵守すること。
②　受託者は、次の文書に記載された事項を遵守すること。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。
ア　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

イ　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
ウ　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
エ　政府機関等のサイバーセキュリティ対策のための統一規範（最新版）
オ　政府機関等のサイバーセキュリティ対策の運用等に関する指針（最新版）
カ　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（最新版）

なお、「PMDA サイバーセキュリティポリシー」は非公開であるが、「政府機関等の情報セキュリティ対策のための統一基準（最新版）」に準拠しているので、必要に応じ参照すること。「PMDA サイバーセキュリティポリシー」の開示については、事業者が PMDA に「秘密保持等に関する誓約書」を提出した際に開示する。

③　PMDA へ提示する電子ファイルは事前にウイルスチェック等を行い、悪意のあるソフトウェア等が混入していないことを確認すること

④　受託者は、本業務において取り扱う情報の漏洩、改ざん、滅失等が発生することを防止する観点から、情報の適正な保護・管理対策を実施するとともに、これらの実施状況について、PMDA が定期又は不定期の検査を行う場合においてこれに応じること。万一、情報の漏洩、改ざん、滅失等が発生した場合に実施すべき事項及び手順等を明確にするとともに、事前に PMDA に提出すること。また、そのような事態が発生した場合は、PMDA に報告するとともに、当該手順等に基づき可及的速やかに修復すること。

7　成果物の取扱いに関する事項

（1）　知的財産権の帰属

知的財産の帰属は、以下のとおり。

①　本件に係り作成・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 条に定めるすべての権利を含む。）は、受託者が本件のシステム開発の従前より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 が所有する等現有資産を移行等して発生した権利を含めてすべて PMDA に帰属するものとする。

②　本件に係り発生した権利については、受託者は著作者人格権（著作権法第 18 条から第 20 条までに規定する権利をいう。）を行使しないものとする。

③　本件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、受託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。

④　本件に係り作成・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が含まれる場合、受託者は当該著作物の使用に必要な費用負担や使用許諾契約に係る一切の手続きを行うこと。この場合は事前に PMDA に報告し、承認を得ること。

⑤　本件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、受託者の責任、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ときは、受託者に通知し、必要な範囲で訴訟上の防衛を受託者にゆだねる等の協力措置を講ずる。なお、受託者の著作又は一般

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、受託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）　契約不適合責任

① 委託業務の納入成果物に関して本システムの安定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 が必要と認めた場合は、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 受託者は、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）又は JISQ27001 認証（日本産業標準）に従い、また個人情報を取り扱う場合には JISQ15001（日本産業標準）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、速やかにそれら情報を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。

（３）　検収

納入成果物については、適宜、PMDA に進捗状況の報告を行うとともに、レビューを受けること。最終的な納入成果物については、「3 (3) ①成果物」に記載のすべてが揃っていること及びレビュー後の改訂事項等が反映されていることを、PMDA が確認し、これらが確認され次第、検収終了とする。

なお、以下についても遵守すること。

① 検査の結果、納入成果物の全部又は一部に不合格品を生じた場合には、受託者は直ちに引き取り、必要な修復を行った後、PMDA の承認を得て指定した日時までに修正が反映されたすべての納入成果物を納入すること。

② 「納入成果物」に規定されたもの以外にも、必要に応じて提出を求める場合があるので、作成資料等を常に管理し、最新状態に保っておくこと。

③ PMDA の品質管理担当者が検査を行った結果、不適切と判断した場合は、品質管理担当者の指示に従い対応を行うこと。

８　入札参加資格に関する事項

（１）入札参加要件

応札希望者は、以下の条件を満たしていること。

① 開発責任部署は ISO9001 又は CMMI レベル 3 以上の認定を取得していること。

② ISO/IEC27001 認証（国際標準）又は JISQ27001 認証（日本工業標準）のいずれかを取得していること。

③ プライバシーマーク付与認定を取得していること。

④ 応札時には、開発する機能毎に十分に細分化された工数、概算スケジュールを含む見積り根拠資料の即時提出が可能であること。なお、応札後に PMDA が見積り根拠資料の提出を求めた際、即時に提出されなかった場合には、契約を締結しないことがある。

（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に、以下に示す事業者は本調達に参加できない。

① PMDA 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

④ ①～③の親会社及び子会社（「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をいう。以下同じ。）

⑤ ①～③と同一の親会社を持つ事業者

⑥ ①～③から委託を請ける等緊密な利害関係を有する事業者

９ 情報セキュリティ管理

（１）　情報セキュリティ対策の実施

受託者は、以下を含む情報セキュリティ対策を実施すること。また、その実施内容及び管理体制についてまとめた情報セキュリティ管理計画書を実施計画書に添付して提出すること。

ア　PMDA から提供する情報の目的外利用を禁止すること。

イ　受注者側の情報セキュリティ対策の実施内容及び管理体制が整備されていること。

ウ　本業務の実施に当たり、受託者又はその従業員、本調達の役務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変更が加えられないための管理体制が整備されていること。

エ　受託者の資本関係・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）・実績及び国籍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。

オ　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。

カ　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。

キ　情報セキュリティ対策の履行が不十分である場合、その原因について調査・排除するため、PMDA による追跡調査や立ち入り検査等について連携・協力する体制が構築できていること。また、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。

ク　本業務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 が必要と判断した場合は、速やかに情報セキュリティ監査を受入れること。

ケ　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上記ア～クに関する事項を記載した情報セキュリティ管理計画書を作成し、PMDA の承認を受けること。

コ　PMDA から要保護情報を受領する場合は、予め PMDA と合意した情報セキュリティに配慮した受領及び管理方法にて行うこと。

サ　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、書面にて報告すること。

シ　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。

（２）　情報セキュリティ監査の実施

ア　PMDA がその実施内容（監査内容、対象範囲、実施等）を定めて、情報セキュリティ監査等を行う（PMDA が選定した事業者による監査を含む。）ものとする。受託者は、あらかじめ情報セキュリティ監査等を受け入れる部門、場所、時期、条件等を「実施計画書」に付記し提示すること。

イ　受託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。

ウ　受託者は、情報セキュリティ監査の結果、本調達における情報セキュリティ対策の履行状況について PMDA が改善を求めた場合には、PMDA と協議の上、必要な改善策を立案して速やかに改善を実施するものとする。

エ　本調達に関する監査等が実施される場合、受託者は、技術支援及び情報提供を行うこと。

オ　受託者は、指摘や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。

情報セキュリティ監査の実施については、本項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。

１０ 再委託に関する事項

① 受託者は、受注業務の全部又は主要部分を第三者に再委託することはできない。

② ①における「主要部分」とは、以下に掲げるものをいう。

ア　総合的企画、業務遂行管理、手法の決定及び技術的判断等。

イ　SLCP-JCF2013 の 2.3 開発プロセス、及び 2.4 ソフトウェア実装プロセスで定める各プロセスで、以下に示す要件定義・基本設計工程に相当するもの。

- 2.3.1 プロセス開始の準備
- 2.3.2 システム要件定義プロセス
- 2.3.3 システム方式設計プロセス
- 2.4.2 ソフトウェア要件定義プロセス
- 2.4.3 ソフトウェア方式設計プロセス

ただし、以下の場合には再委託を可能とする。

- 補足説明資料作成支援等の補助的業務
- 機能毎の工数見積において、工数が比較的小規模であった機能に係るソフトウェア要件定義等業務

③ 受託者は、再委託する場合、事前に再委託する業務、再委託先等を PMDA に申請し、承認を受けること。申請にあたっては、「再委託に関する承認申請書」の書面を作成の上、受託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 PMDA に提出すること。受託者は、機密保持、知的財産権等に関して本仕様書が定める受託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。なお、第三者に再委託する場合は、その最終的な責任は受託者が負うこと。

④ 再委託先が「８（２）入札制限」の要件を満たすこと。

⑤ 受託者の責任において、サプライチェーンリスクの発生を未然に防止するための体制を確立すること。

⑥ 再委託先において、本調達仕様書に定める事項に関する義務違反、義務を怠った場合には、受託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。

⑦ 再委託における情報セキュリティ要件については以下のとおり。

- 再委託先が「９（１）情報セキュリティ対策の実施」の要件を満たすこと

・ PMDA から提供する情報の目的外利用を禁止すること。
・ 受託者は再委託先における情報セキュリティ対策の実施内容を管理し PMDA に報告すること。
・ 受託者は業務の一部を委託する場合、本業務にて扱うデータ等について、再委託先またはその従業員、若しくはその他の者により意図せざる変更が加えられないための管理体制を整備し、PMDA に報告すること。
・ 受託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）・実績及び国籍に関して、PMDA から求めがあった場合には情報提供を行うこと。
・ 受託者は再委託先にて情報セキュリティインシデントが発生した場合の再委託先における対処方法を確認し、PMDA に報告すること。
・ 受託者は、再委託先における情報セキュリティ対策、及びその他の契約の履行状況の確認方法を整備し、PMDA へ報告すること。
・ 受託者は再委託先における情報セキュリティ対策の履行状況を定期的に確認すること。また、情報セキュリティ対策の履行が不十分な場合の対処方法を検討し、PMDA へ報告すること。
・ 受託者は、情報セキュリティ監査を実施する場合、再委託先も対象とするものとする。
・ 受託者は、再委託先が自ら実施した外部監査についても PMDA へ報告すること。
・ 受託者は、委託した業務の終了時に、再委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認すること。

⑧ 上記①～⑦について再委託先が、さらに再委託を行う場合も同様とする。

１１ その他特記事項

（１）環境への配慮

環境への負荷を低減するため、以下に準拠すること。

① 本件に係る納入成果物については、最新の「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）」に基づいた製品を可能な限り導入すること。

② 導入する機器等がある場合は、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。

（２）その他

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

② 人事給与システムパッケージ部分の保守についてはシステム構築ベンダー企業と協力すること。

１２ 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

　　添付　人事給与システム全体構成図

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）事業者が閲覧できる資料一覧

閲覧資料１　PMDA サイバーセキュリティポリシー

閲覧資料２　PMDA 情報セキュリティインシデント対処手順書

閲覧資料３　セキュリティ管理要件書(ひな型)

閲覧資料４　システム設計書

閲覧資料５　運用継続計画（情報システム BCP）

閲覧資料６　基盤運用　各種手順書

これら資料は、PMDA に「秘密保持等に関する誓約書」を提出した事業者へ開示する。

閲覧希望者は、公告日から開札日の７日前までに１３．窓口連絡先まで申し出ること。

１３ 窓口連絡先

独立行政法人医薬品医療機器総合機構

総務部職員課　松田

電話：03（3506）9502

E-mail：shokuin●pmda.go.jp

※ ●は@に置き換えてください。

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
問い合わせへの一次回答	一次回答の応答時間	応答時刻ー問い合わせ受付時刻＜60 分の件数／問い合わせ件数	%	100%	問い合わせ一覧表に受付と応答日時の記録	毎月
セキュリティ対策	セキュリティ事故発生件数	セキュリティ事故発生件数	件	0 件	セキュリティ対策ソフトウェアおよび人手により検知されたセキュリティ事故(防御されたものは除く)の発生件数の集計	毎月
運用業務サービス	サービス提供時間	添付1-1「サービス提供時間」のサービスを提供できなかった日数／営業日数×100	%	0%	勤務実績の提出等	毎月
	報告書類の提出期限	期限までに提出した報告書類の件数／報告書類の件数×100	%	100%	提出期日と報告日の比較	都度
問合せ業務	サービス提供時間	添付1-1「サービス提供時間」のサービスを提供できなかった日数／営業日数×100	%	0%	勤務実績の提出	毎月
障害対応	初動対応の開始	異常の発見から 30 分以内に初動対応を行った障害件数／障害件数×100	%	100%	障害発見日時と初動対応開始日時の障害報告書への記録	毎月
	障害発生の連絡	異常の発見から1時間以内に PMDA に連絡した障害件数／障害件数×100	%	100%	障害発見日時と障害発生連絡日時の障害報告書への記録	毎月
	障害報告書の提出期限	期限までに提出した障害報告書の件数／障害報告書の件数×100	%	100%	提出期日と報告日の比較	都度
	サービス停止からの目標復旧時間	給与管理:4時間以内、給与管理以外:6時間以内で復旧しなかった件数(※ただし、移動時間は除く)	件	0 件		
システム稼働	システム稼働率※	(計画サービス時間ー計画外サービス停止時間)／計画サービス時間×100 ※1 分未満のサービス停止時間は切り捨て)	%	99.9%	サービス停止開始・終了日時の記録	毎月

※システム稼働率

・計画サービス時間とは、計画停電又は事前に計画した停止時間を除いたサービス稼働時間(原則 365 日 24 時間)。

・サービス停止時間とは、計画外にシステムが停止していた時間、又は多数の利用者がシステム利用できない状態にあった時間を指し、待機系システム等への切替えのために発生した停止時間、障害からの本格復旧のために必要になった停止時間を含む。

添付１－１　サービス提供時間

項番	サービス提供項目	サービス内容	提供時間	補足
1	オンラインサービス	利用者に対して人事給与システムのサービスを提供する。	24 時間 365 日	定期保守や法定点検等の計画停止期間を除く。
2	運用監視	人事給与システムの運用監視を行う。	項番 1 に同じ	項番 1 に同じ
3	問合せ対応	人事給与システム管理部署に対して人事給与システムに関する問合せ対応を提供する。	9:00～18:15 の間の 8 時間 ※12:00～13:00 は休憩時間とする。	原則PMDAの休日以外 （各月給与計算期間及び賞与計算期間 3 営業日の間は 9:00～22:00 に連絡が取れる体制をとること。）
4	保守対応	ソフトウェアの保守・改修を行う。	項番 3 に同じ	PMDAの休日以外及びPMDAの休日のうちサービス提供が必要とされた日（※） （ただし、保守対応時間中に対応した案件が継続している場合は、必要な作業が収束するまで）

※災害及び重大な障害が発生した場合で、緊急対応が必要と認められる場合には、提供時間に限らずサービスを提供すること。

【別紙２】作業スケジュール

No	セキュリティ対策	実施区分	R7 4	R7 5	R7 6	R7 7	R7 8	R7 9	R7 10	R7 11	R7 12	R8 1	R8 2	R8 3	実施内容
マイルストーン															
1-1	キックオフ	実施 ◎													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	実施 ◎													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。
1-3	月次定例	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
2-2	システム変更作業報告 （パッチ適用状況報告を含む）	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」 ⇒変更管理：変更作業一覧による月次報告
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
2-4	データ保全（バックアップ）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	「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（任意）
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：セキュリティパッチ適用状況の報告 脆弱性に関する新着情報、影響度・適用要否、適用予定と実績
通勤手当制度改正に係る改修															
3-1	業務実施計画書提出	実施 ◎	▲												改修業務の実施に係る計画書提出（受託者）
3-2	設計	実施 ◎	▲	◎											システム設計作業実施（受託者）
3-3	開発	実施 ◎		◎	◎										システム開発作業実施（受託者）
3-4	各種テスト	実施 ◎			◎	◎	◎								要件どおりに動作するか各種テスト実施（受託者）
3-5	検収（受入テスト）	実施 ◎					◎	◎							要件どおりに動作するか検収作業実施（PMDA）
権限管理															
4-1	各業務データアクセス権限再検証	支援 △									準備		実施		不要なアクセス権限の洗い出しと削除
4-2	ユーザーID棚卸し （各業務システム）	実施 ◎									準備		実施		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。
4-3	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 ⇒台帳と使用管理簿の相関チェック、使用管理簿とログの相関チェック
4-4	パソコン等搭載ソフトウェアの定期的な調査、 不要ソフトウェアの削除	支援 △												準備	使用するソフトウェア・バージョン、ソフトウェアの利用可否基準を整理し、棚卸を実施する（パソコン更改時に対応し「台帳」を整備する）
点検															
5-1	情報資産棚卸し・リスク評価	支援 △						準備		実施			▲ 報告		⇒厚労省のガイドラインに従って実施：「情報資産台帳」「情報資産ライフサイクル確認様式」「リスク評価チェックシート様式」の作成・更新
5-2	システム台帳の最新化	支援 △									準備		実施		⇒資産台帳・管理簿（システム台帳）を更新する。 ⇒ネットワーク機器ソフトウェア資産台帳を更新する。
5-3	ログ取得状況の点検	支援 △									準備	実施	▲ 報告		⇒情報資産の重要度に応じて、監視対象となるイベントを絞り込み、ファイル抽出した上で、セキュリティ違反を示す証跡がないかを定期的に確認する。
5-4	セキュリティヘルスチェック（不正プログラム及び不正な設定変更の有無確認）	支援 △							準備	実施	▲ 報告				
5-5	情報セキュリティ：遵守状況の自己点検	実施 ○					準備	実施	▲ 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
5-6	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る。
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		⇒対象システムを選定の上、PMDA内部検査を実施

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	令和 7 年 4 月 1 日 ～令和 8 年 3 月 31 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、PMDA の休日（「独立行政法人医薬品医療機器総合機構職員就業規則第 36 条」で定められるとおりとする。）以外の日とする。	9:00～18:15 の間の 8 時間 ※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。

運用業務の実施範囲

No	名称	内容
1	計画書の策定	運用保守業務の作業範囲、スケジュール、実施体制、実施計画、管理計画等を記載した運用保守業務実施計画書を作成する
2	全体管理	運用報告資料作成及び必要な情報収集の上、定められた頻度で定期報告を行い、必要に応じ適宜、問題、課題に関する状況報告を行う
3	【システム監視 － 稼動監視】	人事給与システムに対する障害監視、リソース監視によりシステムが正常稼動していることを監視すること。また故障発生時にはインシデント検知と記録を行い、速やかに PMDA、及び関連業者に連絡すること。 システム監視のサービス提供時間は 24 時間 365 日とする。 一定期間の監視結果を分析の上、監視報告書を作成し PMDA に報告すること。その際に監視実施記録を併せて提出すること。 人事給与システムに係る監視項目、監視方式は閲覧（別途開示）資料を確認し、PMDA と協議した上で決定すること。なお、データセンタにおける巡回監視（ハードウェアの目視確認）はデータセンタ事業者が実施するものとし、本調達の対象外とする。
4	【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監視を行うこと。ログの保管は、別途調達するソフトウェアで実施する。
5	【システム監視 － 情報セキュリティ監視】	本システムへの不正侵入、不正改ざん検知、ウイルスチェックなど、本システムに関するセキュリティ監視を行うこと。なお、不正侵入、不正改ざんを検知した場合、PMDA より至急の対応依頼が発生する可能性があることに留意すること。
6	【システム設定・操作 － ジョブ管理】	① 運用保守業務実施計画書の策定と更新 運用スケジュールは、年次、四半期、月次、週次、日次のスコープで計画するものとする。 受託者は、PMDA から運用スケジュールに必要な情報を受けて、年次、四半期、月次、週次、日次の運用スケジュールを作成すること。また、必要に応じて運用スケジュールの変更を行うこと。

No	名称	内容
		本件の受託者は、作成、変更した運用スケジュールについて PMDA の承認を得た上で、全ての関係者に確実に周知すること。 ② ジョブスケジュールの登録等 本件の受託者は、令和 6 年度人事給与システム運用保守事業者より継承したジョブスケジュール情報を基に、PMDA から業務スケジュールの変更情報を受けて、当該スケジュールを踏まえたジョブスケジュールの設定変更（登録、変更、削除）を行うこと。 ジョブスケジュールの設定変更に際しては、ジョブの登録、変更、削除による運用スケジュール及び保守スケジュール全体への影響を確認すること
7	【システム設定・操作 － 容量・能力管理】	本システムの性能を計測する指標（CPU 負荷、メモリ使用量、ディスク使用量など）を PMDA と協議の上で確定し、指標データを常時収集し、閾値を超えるなどの異常を発見した場合は障害対応について PMDA に提案し、PMDA の了解の下、当該作業を実施すること。
8	【ヘルプデスク業務 － 問い合わせ対応】	人事給与システムにおける PMDA からの問合せについては、受託者が直接連絡を受けること。 基本的には既定の質問票を起票して問合せを行うが、緊急時などで質問票を起票する暇がない場合や内容を伝えにくい場合は、電話やメール問合せを行うことがあるので、柔軟に対応できる要員の配置等、体制を整えること。 また、適宜発生する PMDA からのセキュリティ状況に関する問合せや、システム構成情報等、本システム（本番環境、検証環境含む）に関する問合せにも対応すること。なお、PMDA では、システム監査を外部機関に委託し、毎年実施している。このシステム監査によって発生した問い合わせやセキュリティホール等の指摘に対しても、PMDA と協議の上、対応すること。 ⑴問合せ窓口業務 本件の受託者は、PMDA から連絡を受けた操作方法や障害等の問い合わせ対応業務を実施すること。回答については、回答に係る作業報告の羅列ではなく、作業の結果を総括し、PMDA からの問い合わせの趣旨に対して、的確かつ簡潔な回答とすること。発生した問合せの受付から回答までの対応状況を管理し、インシデント対応状況報告として、毎月まとめて PMDA に報告すること。なお各インシデント対応状況報告の内容はインシデント管理台帳、又はそれに類する管理ツール等で管理すること。 ⑵Q&A 集等のナレッジベースの構築、管理業務 問合せ対応によって蓄積される問合せ事項についてはその内容、分類、回数等の分析から FAQ(よくある質問と回答)を抽出してナレッジベース化することにより、問合せ対応業務の効率化、利用者の FAQ 情報の共有化を図ること。 本件の受託者は、具体的なナレッジベースの実現方法及び手順並びに問合せ事項の分析から FAQ 情報の登録及び更新までの具体的手順について提案すること。 ⑶その他 PMDA が掲げる本調達の背景の本質（人事・給与・研修等業務を持続的に、正確かつ効率的に実施→本システムを安定的な稼働の基で十分に機能させる）を理解し、PMDA からの各問い合わせへの対応に際しては、背景にある本質を汲み取った上

No	名称	内容
		で、本質に資する対応策を提示すること。また、形式的な対応に留まらず、その後、PMDA が進める対応策の実行にあたり、適宜、設計・構造上の観点から、有効な提案を行うこと。
9	【運用管理】	操作ログ管理や履歴情報管理等を含む。 システム運用上の業務プロセスを定めた「業務フロー及び手順書」について、次のシステム運用業務について作成･更新するものとする。 (ｱ)問合せ管理プロセス　(ｲ)インシデント管理プロセス　(ｳ)変更管理プロセス　(ｴ)リリース管理プロセス　(ｵ)構成管理プロセス　(ｶ)問題管理プロセス　(ｷ)各定期点検プロセス　(ｸ)リスク管理プロセス　(ｹ)課題管理プロセス　(ｺ)情報セキュリティ管理プロセス。 ① 運用保守業務実施計画書の策定と更新 運用スケジュールは、年次、四半期、月次、週次、日次のスコープで計画するものとする。 受託者は、PMDA から運用スケジュールに必要な情報を受けて、年次、四半期、月次、週次、日次の運用スケジュールを作成すること。また、必要に応じて運用スケジュールの変更を行うこと。 本件の受託者は、作成、変更した運用スケジュールについて PMDA の承認を得た上で、全ての関係者に確実に周知すること。 ② ジョブスケジュールの登録等 本件の受託者は、令和 6 年度人事給与システム運用保守事業者より継承したジョブスケジュール情報を基に、PMDA から業務スケジュールの変更情報を受けて、当該スケジュールを踏まえたジョブスケジュールの設定変更（登録、変更、削除）を行うこと。 ジョブスケジュールの設定変更に際しては、ジョブの登録、変更、削除による運用スケジュール及び保守スケジュール全体への影響を確認すること。 ③ 検証環境の運用 本番環境と同様、検証環境についても管理を行うこと。PMDA からの要請に基づき、本番環境から検証環境への情報のコピーを実施すること。
10	【ユーザー管理】	① 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） ② システムを構成する機器やアプリケーション等のユーザ管理 システムを構成する機器やアプリケーション、リモートアクセス機器及びリモートアクセスユーザを管理の対象とすること。 ③ 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。 ④ 操作権限付与に関するメンテナンス 各ユーザの操作権限付与（変更）に関するメンテナンスを行い、実際の運用に支障のないようにすること。また、定期的に報告すること。
11	【サービスレベル管理】	別紙1 「SLA（Service Level Agreement）項目」参照 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

No	名称	内容
		「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。
12	【バックアップ/リカバリ】	ハードウェア事業者の定めるバックアップ方式に従い、以下の作業を実施すること。また、定期的に報告すること。詳細項目については閲覧（別途開示）資料一覧に挙げる「基盤運用　各種手順書」を参照のこと。
		重大な障害が発生し、復旧が必要になる場合に備え、運用手順としてバックアップ並びにリカバリ計画及び手順を確立し、それに基づき実行すること。
		システム障害等の発生時に、状況に応じてバックアップ媒体から本番環境へ必要データのリストアを行い、業務の再開を可能にすること。なお、障害時に要求される目標復旧時間は別紙1 「SLA（Service Level Agreement）項目」参照
13	【各種データ管理】	定期的に取得が必要な運用データ、各種帳票・レポート類、設定データ等のデータ管理。
		(1) 必要データの保存と削除 定期的に夜間バッチ処理により生成される結果データ、操作履歴等の蓄積データに関しては、データを定期的に再利用可能な形式で別媒体に保存した後にデータベースから削除を行うこと。
		(2) データ保守 業務アプリケーションに起因する障害復旧に伴い、過去のデータを含め、不整合データの存在が明らかになった場合、不整合データの修正箇所の特定、報告を行い、PMDA と協議の上、修正、削除の実施、確認、記録業務への対応を行うこと。また関連文書検索用紐付けデータのデータベースへの一括登録、更には登録された紐付けデータに不整合等が判明した場合には、その修復も行うこと。
		(3) 軽微なレポート変更対応 PMDA の指示により、出力可能なクエリレポートの編集内容変更を行う（1か月あたり1レポート程度。保守期間内 12 レポートまでに限る。）。
14	【データベース運用支援】	データベースの性能劣化を防止するため、テーブル再構成やインデックス再構成等の性能劣化防止作業を計画し、PMDA の承認を得た上で定期的に実施すること。
15	【アプリケーション保守】	本件の受託者は人事給与システムにおける障害への対応、または PMDA からの改修要請による軽微なソフトウェア改修を行うこと。 ① ソフトウェアの障害改修対応 ➢ 障害対応の実施にあたっては、関連業者との連携を図り、障害の分析及び障害箇所の特定を行うこと。 ➢ 障害対応の実施においては、関連業者と対応方法についてレビューを行い、その完全性を確認の上、PMDA の承認を得ること。 ➢ ＰＭＤＡに具体的な資料を添付し、障害内容の報告を行うこと。 ➢ ソフトウェアの障害に対して、オンサイト対応（技術者の派遣によるＰＭＤＡ内での障害対応、正常復帰確認作業・報告等）を行うこと。 ② PMDA が想定する改修業務は以下のとおりとし、改修の作業時間は契約期間を通じ、60 人日程度を見込んでいる。 ➢ 修正プログラムの適用 ➢ システム障害に伴うマスターデータの修正

No	名称	内容
16	定例運用	以下の定例作業を行うこと。なお、本件の受託者は作業項目について過不足がある場合は提案すること。 ➢ サーバ運転監視、エラー確認 ➢ リソース監視、エラー確認 ➢ ジョブ監視 、エラー確認 ➢ バックアップ実施 、結果の確認 ➢ システム定期保守の計画、実施、実施状況管理 ➢ セキュリティパッチ等の最新化確認、選定、事前検証、適用、適用監視 ➢ 各種運用業務の結果報告
17	定例外運用	緊急時対応として、本件の受託者は定例外運用の対応を行うこと。 ［定例外運用の例］ 要求ベースオペレーション（ジョブ追加、緊急オペレーション含む。） 障害対応（復旧と事後対策含む。） ウィルス感染時の対応 サーバの立ち上げ、シャットダウン OS、ミドルウェア、アプリケーションの立ち上げ、シャットダウン

保守業務の実施範囲

No	名称	内容
1	計画書の策定	人事給与システムを構成するソフトウェア（ミドルウェア、パッケージソフトウェア（製品本体、カスタマイズ部分）、アドオン開発プログラム）を維持するために、監視による異常検知、利用者からの問合せ等を契機として必要に応じて保守作業を行う。本作業を遂行するための運用保守業務実施計画書を作成すること
2	全体管理	本件の受託者は、保守報告資料作成及び必要な情報収集の上、定められた頻度で定期報告を行い、必要に応じ適宜、問題、課題に関する状況報告を行うこと。 また、会議開催の都度、議事録を作成し PMDA の承認を得ること
3	【システム設定・操作 － 設定変更】	ハードウェア、OS、ミドルウェア等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。
4	【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。なお、(3)～(6)に係る、公表されている脆弱性情報を漏れなく把握すること。ソフトウェアの更新作業については、PMDA と協議の上、検証環境でテストを実施の上で本番環境に反映させること。
		(1) パッチの提供に関する情報及び 脆弱性情報の収集 当システムを構成する全てのソフトウェアについて、ソフトウェアベンダからのパッチ（不具合修正を目的とするパッチ、脆弱性対策を目的とするセキュリティパッチの両方を含む。）の提供情報及び脆弱性に関する情報を継続的に収集すること。
		(2) 脆弱性対応計画の作成 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た場合、当該脆弱性への対応又は当該セキュリティパッチの適用に関する計画を「脆弱性対応計画」（案）として取りまとめ、PMDA の承認を得ること。「脆弱性対応計画」（案）は、以下の内容を含むこと。 ・対策の必要性 ・対策方法又は対策方法が存在しない場合の一時的な回避方法 ・対策方法又は回避方法が情報システムに与える影響 ・直ちにはパッチ適用できないと判断される場合のリスクと当面の回避策（案） ・対策の実施予定 ・テストの必要性 ・テストの方法 ・テストの実施予定 ・テストの合格基準 ・本番環境への適用手順とスケジュール
		(3) 業務アプリケーションへのパッチの定期適用 業務アプリケーションプログラムへのパッチの適用を定期的に適用する計画を作成し、PMDA 等の承認の上で適用を実施すること。 パッケージベンダーが提供するパッチを受領し、影響の調査、PMDA との連携の下に実施判断を行い、検証環境において検証テストを実施の上で本番環境に反映させること。なお、人事給与システム業務パッケージにおける累積パッチ（サポートパッケージ）については、原則 1 年に一度以上は適用する方針とする。
		(4) 業務アプリケーションへのパッチの緊急適用

No	名称	内容
		業務アプリケーションプログラムへのパッチを緊急適用する計画を作成し、PMDAの承認の上で適用を実施すること。
		(5) OS・ミドルウェアの不具合修正の適用 特定ミドル保守業者又はその他の機器保守業者から提供される修正版の OS・ミドルウェアの不具合修正資源を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。
		(6) ウィルスパターンファイルの更新 本システムに導入されているアンチウィルスソフトウェアのうち、パターンファイルの自動更新が行われていないものについては、1 日ごとにウィルスパターンファイル資源を適用すること。
		(7)その他 一連の作業はリリース管理の作業プロセスについて、PMDA と合意した上で実施すること。影響範囲調査と適用作業を行い、本番運用に影響を及ぼさないように注意すること。
5	【ハードウェア保守】	ハードウェア及びファームウェアの不具合、ファームウェア更新等のハードウェア保守に関してサーバ等の保守業者と協力し、分担の役割に応じて対応すること。作業の分担において抜け、漏れが出ないよう充分留意し、最終的な対応は本件受注業者の責任において実施すること。別紙　運用監視・保守方針と役割分担を参照。
6	【不具合修正、軽微な改修】	運用を継続するにあたって、業務の効率化、利便性の向上に資するために、PMDA の指示の下、画面・帳票レイアウトの変更、検索条件及び検索処理の修正、小規模ツールの作成といった軽微なプログラム改修を、システム構造上可能な範囲で実施すること。必要な設計書の改訂・作成及びプログラム入替え作業も含むものとする。 別途、改修案件が調達された場合、当該受注業者との連携、調整を密にし、当該受注業者による改修作業が円滑に進むよう支援をすること。その際にはソースプログラムのデグレード等が発生しないよう、構成管理に留意すること。 本システムの開発方法に適合させること。
7	PMDAからの要請による改修対応	業務規程変更等の理由による PMDA からの要請による改修に対応すること。作業時間は、本項目及び運用業務No.15②の合計で、60人日とする。作業はPMDA担当者の事前承認の上、実施し、その後、PMDA が実施する受入テストが的確な内容になるよう、設計・構造上の観点から、有効な提案を行う。また、作業時間実績を毎月報告すること。 改修終了時にあたっては、改修項目ごとにかかった作業工数、プログラム等の修正内容、影響のあった画面数についても報告すること
8	データ出力に係る軽微な設定変更対応など	PMDAからの要望に応じて、必要なデータを円滑に出力するために、適宜、設定変更対応を行う(1か月あたり 1 事案程度。保守期間内 12 事案までに限る。)。
9	その他	上記以外の改修(瑕疵対応等)についても、本件の受託者は PMDA の指示に従い、ソフトウェアの改修、並びに検証環境及び本番環境へのインストール・設定等業務を行うこと。

システムの範囲

人事給与システムの構成

① 全体構成

本システムの全体構成を「別紙3－1　人事給与システム全体構成図」に示す。本システムの詳細なネットワーク構成や人給システム基盤を構成するソフトウェア等に関する情報については、資料閲覧で設計資料を閲覧できるのでこちらを参照すること。

役割分担

人事給与システム基盤内において、勤務管理システム用の仮想サーバが存在する。勤務管理システム用サーバについては本調達の保守対象外とする。勤務管理システム用の仮想サーバについては資料閲覧時に確認すること。

なお、運用業務の内データセンタにおけるハードウェアの目視監視は本調達の対象外とする。

作業方法

① 基本事項

作業に際しては、以下の事項を遵守し実施すること。

・ 契約締結後、業務一式の運用保守業務実施計画書を提示し、作業体制や役割分担について PMDA に対して報告し、承認を得て業務を進めること。また、契約締結以降に変更が発生した場合には、そのつど速やかに変更後の運用保守業務実施計画書を提出すること。

（ア）会議について

・ 運用保守業務に関しては、月次会議を開催し、PMDA に対し、運用保守作業及び毎月の作業時間の実績、障害や課題の状況等の報告を行うとともに、必要に応じて状況を説明するための資料等の作成及び会議での説明を行うこと。

業務の進め方について改善事項がある場合は月次会議の場で PMDA に提案し、PMDA の了承を得た上で変更する事とする。

・ 本件の受託者が出席する会議においては、会議が開催されるつど、本件の受託者が議事録の作成を行い、全出席者に内容の確認行った上で、3 営業日以内に PMDA に議事録を提出すること。

② 詳細事項

（ア）月次報告書の作成

・ 運用保守業務内容と障害・課題の発生状況及びその対応状況、さらに予防措置としての提案等を月次報告書として毎月作成すること。

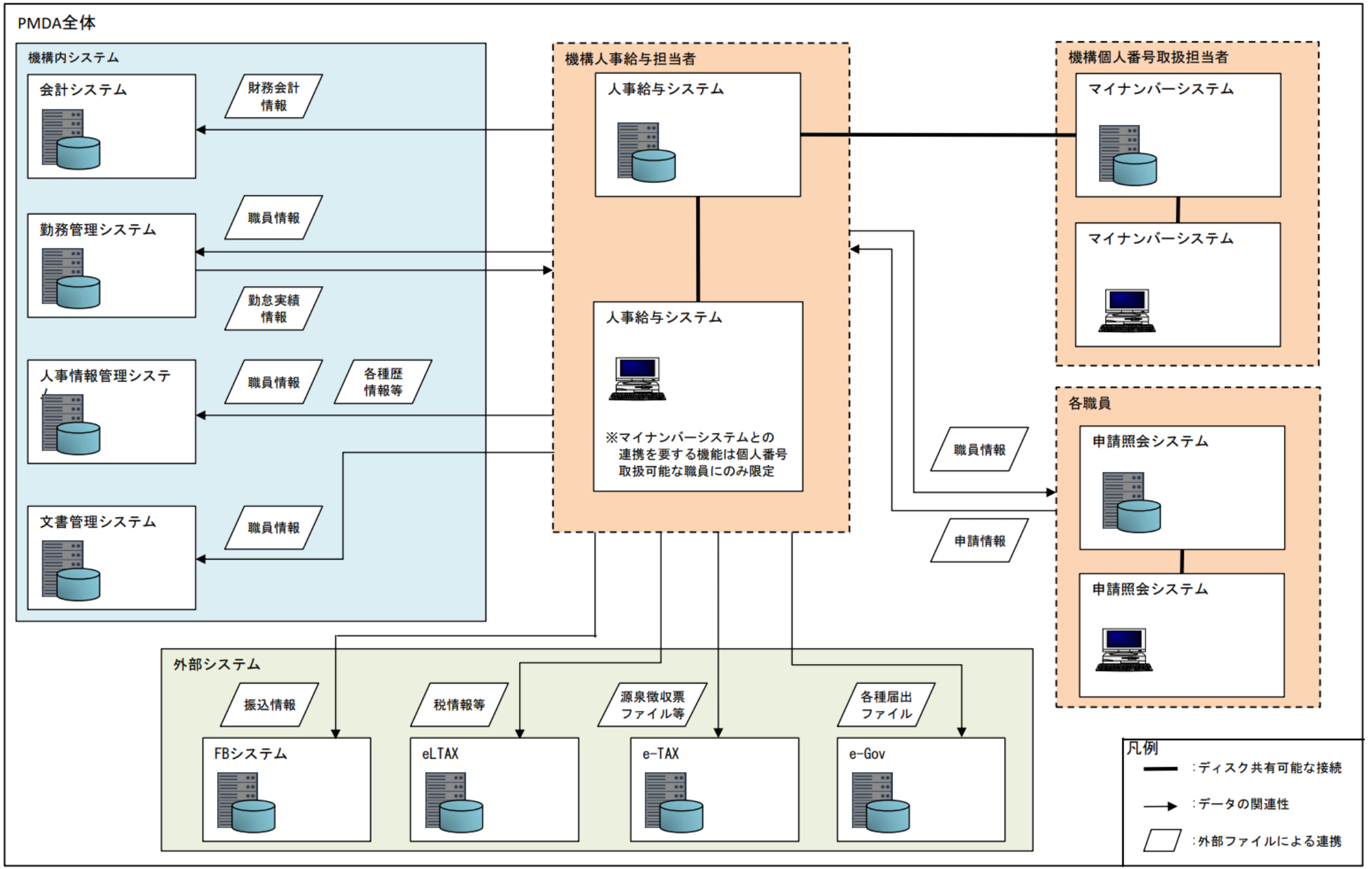
（イ）文書管理

- 改修作業やメンテナンス作業で設計書や手順書の追加・修正が必要な場合はドキュメントの作成、メンテナンスも本業務に含まれる。
- ドキュメント（設計・開発事業者が作成した設計書や手順書を改善・修正したものを含む。）を統合的に管理するための環境構築、及びルール・手順の策定を実施すること。
- サイズの大きいファイルのやり取りを行う事も想定し、共有ポータルサイトなどの仕組みを用意すること。共有ポータルサイトのセキュリティポリシーは PMDA のセキュリティポリシーに準拠すること。

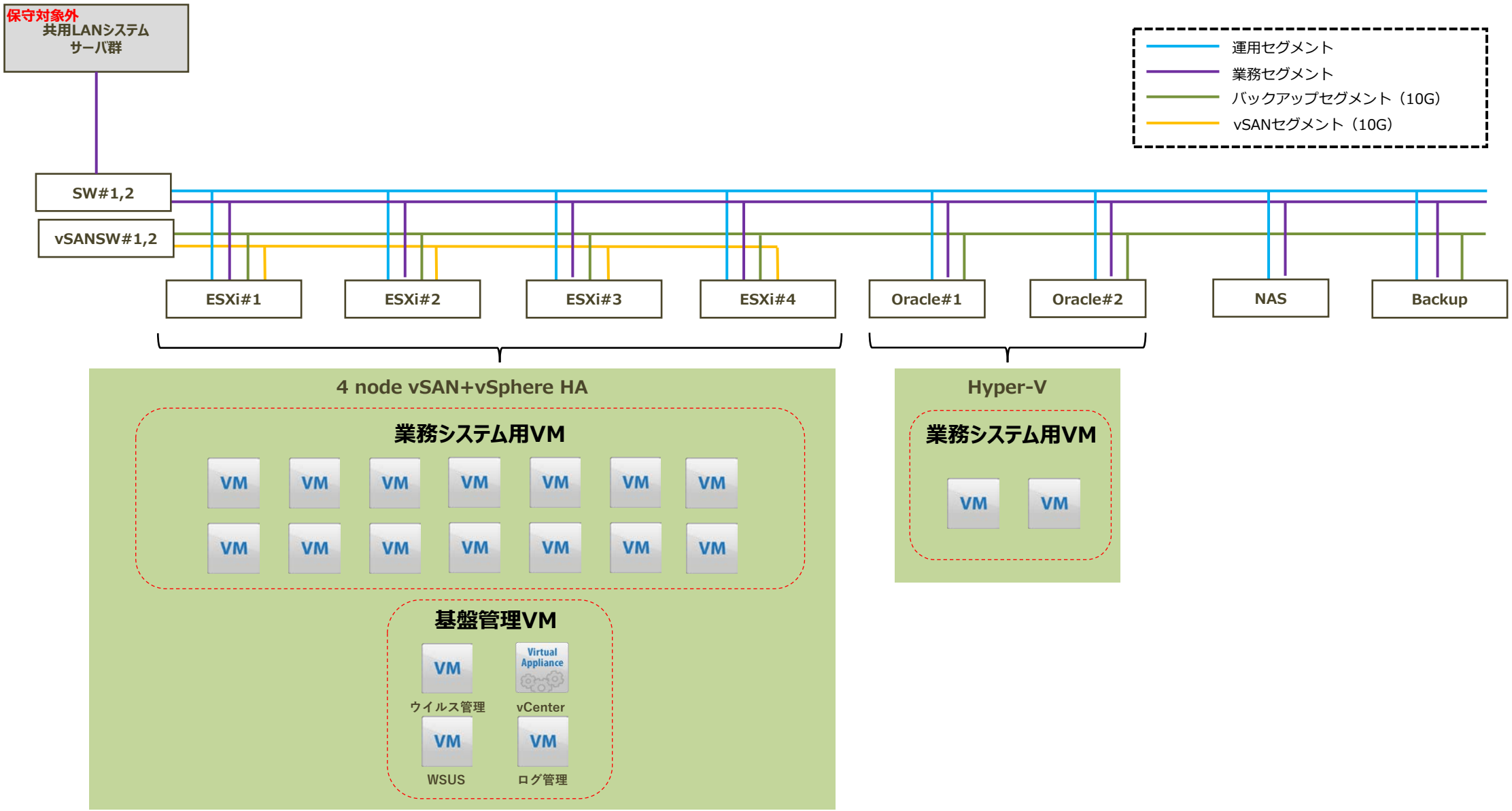
（ウ）その他

- セキュリティパッチ適用にともなうテスト手法、手順書、その他必要資料を整備すること。
- 一部やむを得ない作業を除き、原則、データセンタへ入室しないこと（例外：機器導入、ネットワーク構築、メディアの出し入れを伴う作業等）

別紙３添付
人事給与システム全体構成図



ハードソフト構成図


保守対象外
共用LANシステム
サーバ群
運用セグメント
業務セグメント
バックアップセグメント（10G）
vSANセグメント（10G）
SW#1,2
vSANSW#1,2
ESXi#1
ESXi#2
ESXi#3
ESXi#4
Oracle#1
Oracle#2
NAS
Backup
4 node vSAN+vSphere HA
業務システム用VM
VM
基盤管理VM
Virtual Appliance
ウイルス管理
vCenter
WSUS
ログ管理
Hyper-V
業務システム用VM

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。

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」

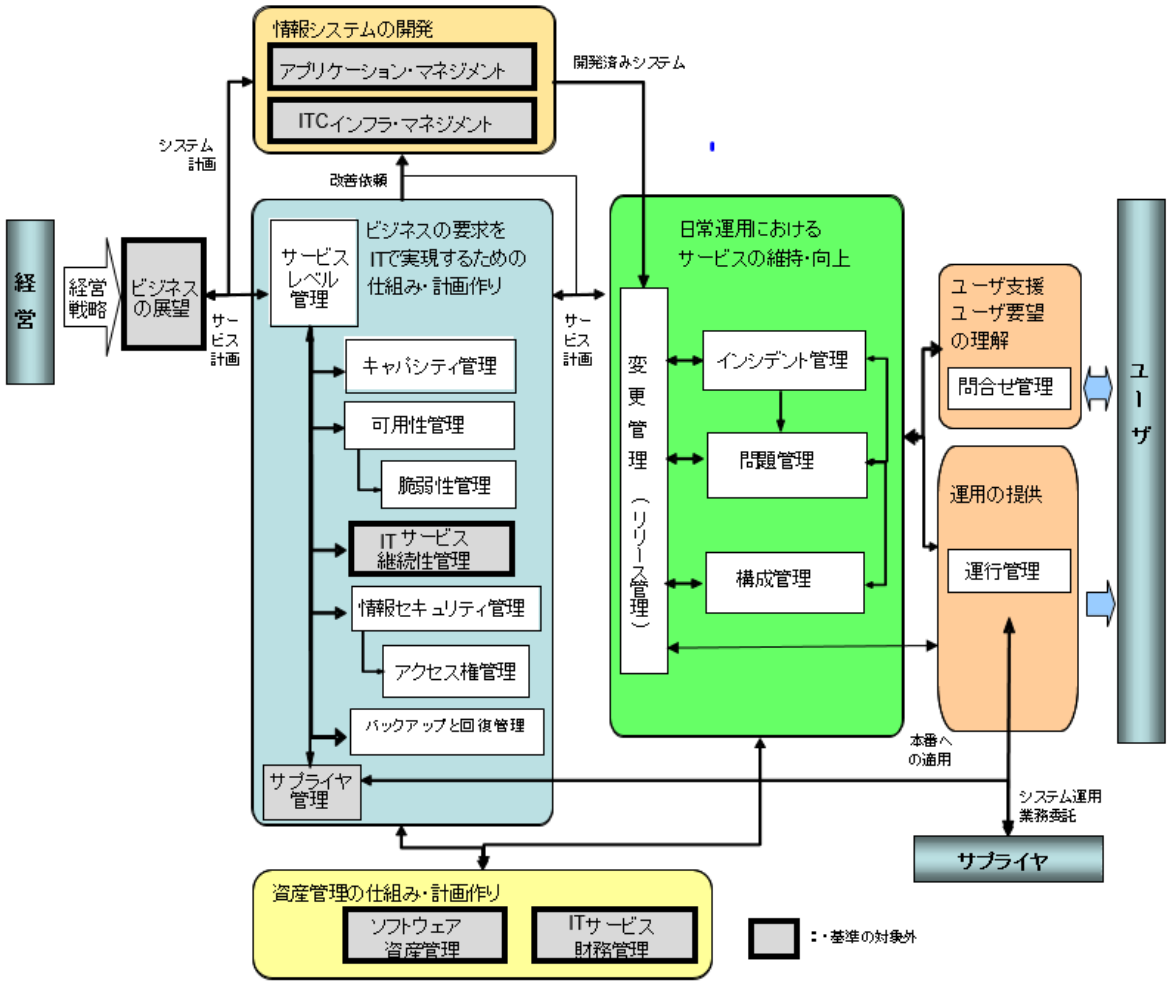
2. システム運用管理業務の概要

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

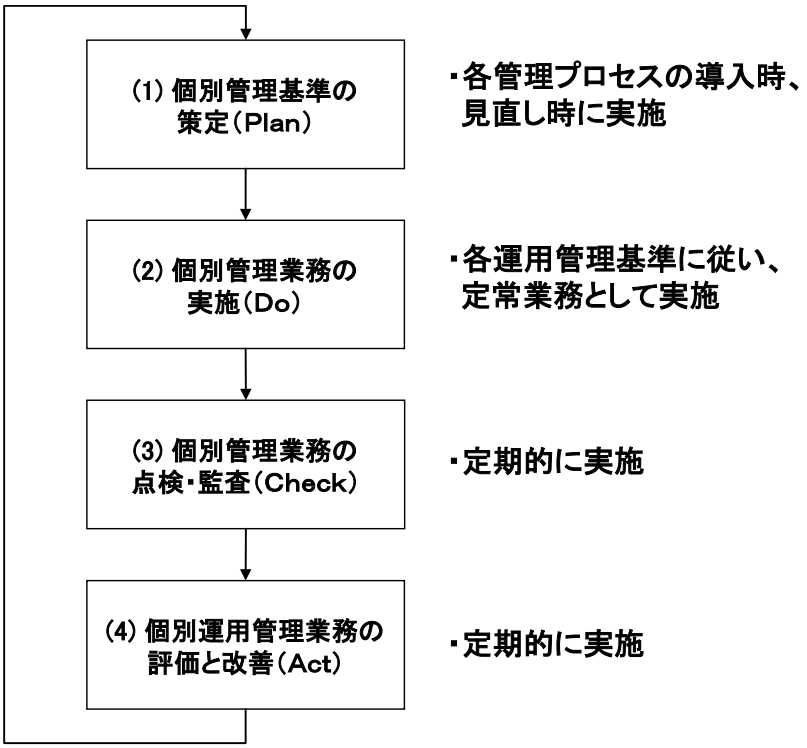


3. 運用管理業務の基本プロセス

（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

〇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。

(6)　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。

（7） 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。

⑤主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）	通信回線対策 （AT-1）	通信経路の分離 （AT-1-1）	不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離すること。ネットワーク構成情報と実際の設定を照合し、所定の要件通りに設定されていることを定期的に確認すること。	セキュリティヘルスチェック（構成管理資料の原本と実際の設定状況を目視にて突合せチェックすることにより各種セキュリティ設定の不正変更の有無をチェックする）と合わせて実施し報告すること。
		不正通信の遮断 （AT-1-2）	通信に不正プログラムが含まれていることを検知したときに、その通信をネットワークから遮断すること。	
		通信のなりすまし防止　（AT-1-3）	通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能について、有効に機能していることを定期的に確認すること。	セキュリティヘルスチェック（構成管理資料の原本と実際の設定状況を目視にて突合せチェックすることにより各種セキュリティ設定の不正変更の有無をチェックする）と合わせて実施し報告すること。
		サービス不能化の防止　（AT-1-4）	サービス不能攻撃を受けているかを監視できるよう、稼動中か否かの状態把握や、システムの構成要素に対する負荷を定量的(CPU 使用率、プロセス数、ディスク I/O 量、ネットワークトラフィック量等)に把握すること。監視方法はシステムの特性に応じて適切な方法を選択すること。	
	不正プログラム対策 （AT-2）	不正プログラムの感染防止　（AT-2-1）	不正プログラム対策ソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持すること。不正プログラム対策ソフトウェア等により定期的に全てのファイルに対して、不正プログラムの検査を実施すること。	
		不正プログラム対策の管理　（AT-2-2）	不正プログラム対策ソフトウェア等の定義ファイルの更新状況を把握し、不正プログラム対策ソフトウェア等が常に有効に機能するよう必要な対処を行うこと。	

	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。
不正監視・追跡 （AU: Audit）	ログ管理（AU-1）	ログの蓄積・管理（AU-1-1）	情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログ（システムへのログオンや資源へのアクセスのロギング等）を取得すること。	ログが所定の要件通り、取得・蓄積されていることを確認すること。（年１回以上）
		ログの保護　（AU-1-2）	取得・蓄積されたログが不正な改ざんや削除が行われないようログの格納ファイルのアクセス権を制限する等必要な対策を講じること。	取得・蓄積されたログが不正な改ざんや削除が行われていなことを確認すること。（年１回以上）
		時刻の正確性確保（AU-1-3）	システム内の機器の時刻同期の状況を確認すること。	
	不正監視（AU-2）	侵入検知　（AU-2-1）	不正行為に迅速に対処するため、通信回線を介して所属するＰＭＤＡ外と送受信される通信内容を監視し、不正アクセスや不正侵入を検知した場合は通信の遮断等必要な対処を行うこと。	
アクセス・利用制限（AC: Access）	主体認証（AC-1）	主体認証　（AC-1-1）	主体認証情報（ＩＤ、パスワード）は不正に読み取りできないよう保護すること。	
	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）	通信経路上の盗聴防止 （PR-1-1）	通信回線に対する盗聴行為による情報の漏えいを防止するため、通信回線を暗号化する機能について、有効に機能していることを定期的に確認すること。	セキュリティヘルスチェック（各種セキュリティ設定の不正変更の有無、および不正操作の痕跡の有無の確認）と合わせて実施し報告すること。
		保存情報の機密性確保 （PR-1-2）	情報システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限すること。構成情報と実際の設定を照合し、所定の要件通りに設定されていることを定期的に確認すること。 また、業務データへのアクセス権限の付与状況を点検し、不要なアクセス権限が付与されていないことを確認すること。	ユーザーＩＤの棚卸と合わせて実施すること。
		業務データへのアクセス管理	情報の格付の見直し及び再決定が行われた際や、当該情報システムに係る職員等の異動や職制変更等が生じた際には、情報に対するアクセス制御の設定や職務に応じて与えられている情報システム上の権限が適切に変更されていることを確認すること。	ユーザーＩＤの棚卸と合わせて実施すること。
		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。
		入退室管理の履行	ＰＭＤＡが管理するサーバ室、事務室等の管理区域への入退出については、ＰＭＤＡ入退室管理規程を遵守すること。 ＰＭＤＡの管理区域内での作業は、原則として、ＰＭＤＡ職員の立会いのもとで行うこと。	

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。