第４次会計システムの運用支援業務
調達仕様書

令和５年１２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

第４次会計システムの運用支援業務

（２）　用語の定義

表１-１　用語の定義

用語	概要
医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律 (医薬品医療機器等法、薬機法)	本書では、「薬機法」という。平成 26 年 11 月 25 日に施行された、医薬品、医療機器等の安全かつ迅速な提供の確保を図るため、添付文書の届出義務の創設、医療機器の登録認証機関による認証範囲の拡大、再生医療等製品の条件及び期限付承認制度の創設等の所要の措置を講ずるための法律。
医薬品・医療機器申請・審査システム (Pegasus)	薬機法に定められた許認可に関する申請等を受付けて審査し、行政側の許可・承認等の業務を全国的に一括処理する、独立行政法人 医薬品医療機器総合機構(以下「総合機構」という。)における、基幹業務処理システム。(以下「Pegasus」という。)
給付金	副作用や感染被害にあった方に支払われる給付金。
審査等手数料	薬機法に定める審査業務等に係る手数料。
副作用拠出金	副作用救済給付の給付金やその事務に係る経費に充てるための費用。医薬品や再生医療等製品の売り上げに応じて計算される一般拠出金と副作用救済給付の原因医薬品とされ給付金として支払われた金額の一部である付加拠出金を併せたもの。
感染拠出金	感染救済給付の給付金やその事務に係る経費に充てるための費用。生物由来製品等の売り上げに応じて計算される一般拠出金と感染救済給付の原因とされた生物由来製品等とされ給付金として支払われた金額の一部である付加拠出金を併せたもの。
安全対策等拠出金	医薬品等の安全業務に係る経費に充てるための費用。医薬品・医療機器・再生医療等製品・体外診断用医薬品の売り上げに応じて計算される。

（３）　調達の背景

総合機構は、経理・会計事務処理の効率的な実施のため、ＮＥＣネクサソリューションズ社の財務会計コアシステムをベースにし、総合機構向けにカスタマイズ開発した会計システム（第４次会計システム）を構築し、現行システムは令和５年４月から運用中である。

会計システムは、総合機構の財務会計業務を円滑に処理するためのものであり、財務会計処理を中断することなく維持していく必要がある。そのため会計システムの運用に係るデータ更新や問い合わせ対応や、障害発生時における復旧作業等の業務を円滑に行う必要がある。

本業務では、システムの安定的かつ円滑な運用に資するため、運用支援・保守業務を調達するものである。

（４）　業務・情報システムの概要

総合機構は、経理・会計事務処理の効率的な実施のため、会計システムを導入しており、現行の第四次会計システムは、令和５年４ 月から本番稼働中である。

※具体的な経理・会計事務処理

○　予算編成、予算執行管理、財務分析

○　契約・支出事務（物品等購入申請、経費精算、支払事務）

○　決算処理

○　資産管理

本調達の対象となる、会計システムのシステム化範囲は別紙１「システム概略図」のとおりである。

①　機能要件

会計システムの機能については、会計システムの設計書を閲覧資料として提示するので、必要に応じて参照すること。

②　画面要件

会計システムの画面については、会計システムの設計書を閲覧資料として提示するので、必要に応じて参照すること。

③　帳票要件

会計システムから出力される帳票については、会計システムの設計書を閲覧資料として提示するので、必要に応じて参照すること。

④　情報・データ要件

会計システムの情報・データについては、会計システムの設計書を閲覧資料として提示するので、必要に応じて参照すること。

⑤　外部インタフェース要件

会計システムが連携する外部システムについては、会計システムの設計書を閲覧資料として提示するので、必要に応じて参照すること。

⑥ 利用者

会計システムの利用者数は以下のとおり。

・同時ログインユーザ：最大 1,500 名（内訳：コアユニット：約 100 名、物品購入及び経費精算：約 1,500 名）

⑦ 上位互換性要件

（業務パッケージのバージョンアップ時の対応）

業務パッケージのバージョンアップを適用するか否かの判断を行うこと。ただし、バージョンアップの判断基準は提供する。

（システム基本ソフトウェアのバージョンアップ時の対応）

サーバの OS、ミドルウェア等のバージョンアップ時には、バージョンアップがシステムに与える影響度を調査し、総合機構に報告を行うこと。

端末の OS 及び文書作成管理ソフトウェア等の更新が、稼働後 5 年間のうちに最低 1 回実施されることを想定すること。

（端末等のバージョンアップ時の対応）

総合機構で利用している端末等が更新される際には、以下の作業を実施すること。

・ 業務アプリケーションの動作検証
・ 業務アプリケーションの配布支援
・ 業務アプリケーションのマニュアル等の更新

⑧ 事業継続性要件

災害等が発生し、ハードウェアを含めシステムが使用不能になった場合は、バックアップデータを元に、ハードウェアの復旧後 1 日以内でシステムの復元を行うこと。なお、ハードウェアは総合機構が用意する。

（５） ＳＬＡの締結

運用業務については、受託者と総合機構との間で協議の上、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、「表 1-2　SLA 項目一覧」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、必要に応じて協議の上、見直すこととする。

表 1-2　SLA 項目一覧

No.	SLA 項目	説明	設定値
1	サービス稼働時間	・今回構築システムのサービスが提供される時間帯 ・定期保守、法定停電等による停止時間を除く	24 時間 365 日
2	運用･保守サービス時間	・運用・保守サービスのうち、監視業務、障害対応業務が提供される時間帯	平日:09:00～18:00 土日祝日：対応しない

3	稼働率（正常稼働時）	・No.1 に示すサービス稼働時間における稼働予定時間に対して実際に稼働した時間（稼働時間）の割合であり、以下の式により計算する ＜稼働率（%）＝（1－1 ヶ月の停止時間÷1 ヶ月の稼動予定時間）×100＞ ・ 稼動予定時間とは、定期保守、法定停電等による計画した停止時間を除く、1 ヶ月に稼動すべき時間である ・ 停止時間とは、サービスが停止していると確認された時刻（監視機能で障害を検知した時刻、または、利用者が連絡した時刻のいずれか早い方）から利用可能とされた時刻までの経過時間を指す ・ 停止時間には、待機系システム等への切換えのために発生した停止時間、障害からの本各復旧のために必要になった停止時間、人為的なミスにより発生した停止時間等を含む ・ 冗長化構成されている部分のうち、一部分が停止した場合でも、冗長化によりサービスの提供に支障を来たさなかった場合には、停止時間として取り扱わない ・ 総合機構側に責任があることが確認できた場合には、停止時間として取り扱わない ・障害検知時刻がヘルプデスク（運用保守支援業者）提供時間外の場合、経過時間は翌営業日のヘルプデスク提供時間開始後から起算する	99.50%
4	稼働率（縮退稼働時）	・ 冗長化構成がされている部分のうち一部分が停止した場合で、レスポンスタイムの低下等が生じている時間（縮退稼動時間）を停止時間として取り扱う ・ 縮退稼動時間とは、縮退稼動の開始から正常稼動に復旧するまでの時間とするが、総合機構の都合により正常稼動への復旧作業を延期する場合等は、復旧のための準備がすべて整い、総合機構の承認を得るまでの時間を縮退稼動時間とする ・ 上記以外は正常稼働時と同様	96.0%以上
5	レスポンスタイム（正常稼働時）	・ すべての個別サービスが稼動しており、対象となる利用者がログインしている状態で、対象となる個別サービスすべてにおいて（外部インターネット接続を除く）、利用者が何らかの処理を行った後、システムが処理を行い、再度、利用者に操作が委ねられるまでの時間 ・ 本条件を満たすことができない処理がある場合には、開発期間において、受注者がその根拠・考え方（各システムの標準的な動作環境、前提等）を提示し、総合機構の承認を得ること ・ クライアント PC 内での処理時間がアプリケ	5 秒以内

		ーションのレスポンスに影響を与える場合は、クライアント PC 内での処理時間を排除した実績を計上することも可とする	
6	レスポンスタイム(縮退稼働時)	・ 冗長化されている部分のうち、一部分が停止した場合に許容するレスポンスタイム ・ 上記以外は、正常稼働時と同様	7 秒以内
7	平均故障間隔（MTBF：Mean Time Between Failure)	・ システムに故障が発生してから、次に故障が発生するまでの平均時間で、以下の式により計算する ＜平均故障間隔＝総稼動時間÷総故障件数＞ ・ 個別サービスの稼動状態（停止、縮退稼動、及び通常稼動等）に関らず、特別な対応が必要になるすべての故障・不具合を故障件数として取り扱うこと ・ 総合機構側に責任があることが確認できた場合には、故障件数として取り扱わない	2920 時間（4 ヶ月）以上
8	平均復旧時間（MTTR：Mean Time To Repair)	・ 平均復旧時間とは、ヘルプデスク稼動時間中において、機器に故障が発生した時刻から故障が復旧した時刻までに要した時間の 1 ヶ月間における平均値である ・ 平均復旧時間は、以下の式により計算する ＜平均復旧時間＝1 ヶ月の総復旧時間÷1 ヶ月間の総件数＞ ただし、平均復旧時間の計算には、ヘルプデスク稼動時間外を含まないものとする ・故障が発生した時刻とは、監視機能で障害を検知した時刻、または、利用者が連絡した時刻のいずれか早い方とする ・復旧とは、障害原因を排除し、正常に稼働することを確認し、利用者が使用可能な状態にあることとする（縮退運転等の暫定復旧も復旧とみなす） ・ 総合機構側に責任があることが確認できた場合には、復旧時間計算の対象から除外する	6 時間以内
9	RPO（目標復旧時点）	・データの損失は許容できないため、データの再送や再処理を含め、障害発生時までの復旧を基本とする（大規模災害時を除く）	データの障害：障害発生時 機器等の障害：直近のバックアップ時点 大規模災害時:1 か月以内
10	RTO（目標復旧時間）	・業務停止時間を極力少なくするため、6 時間以内の復旧を目標とする（大規模災害時を除く）	データの障害:6 時間以内 機器等の障害：10 時間以内 大規模災害時：数か月以内

受注者は、締結した SLA の達成状況を月次で総合機構に報告し、総合機構の評価を受けること。SLA 項目のうち､達成基準を達成できていない項目については､達成できなかった原因､原因に対する改善策､改善策を実施した状況及び今後の見込みを報告すること。

総合機構の評価に基づくサービスレベルの改善、向上のための施策を実行すること。

サービスレベルの評価結果により、総合機構において SLA 項目または項目の達成基準を見直す必要が生じた場合、本件の受注者は SLA 見直しのために必要な検証や資料の提示等の支援を実施すること。

（６）　作業スケジュール

運用業務の対象期間は、令和６年４月１日から令和１１年７月 31 日までとする。

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総合機構（または前受託者）より引継ぎを受けること。

本業務に係る想定スケジュールの概要は、表 1-3 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託者が検討すること。

表 1-3　「会計業務・システム」のスケジュール

実施業務	R6 年度	R7 年度	R8 年度～R10 年度	R11 年度 ※7 月末まで
会計業務（ただし、R11 年４月から７月末までは決算処理。）	会計処理(R6～R10 年度分)			
運用支援	運用支援			
保守	保守			
	ソフトウェア等保守			

２　情報システム稼動環境

会計システムが稼働する情報システム稼働環境を参考として示す。

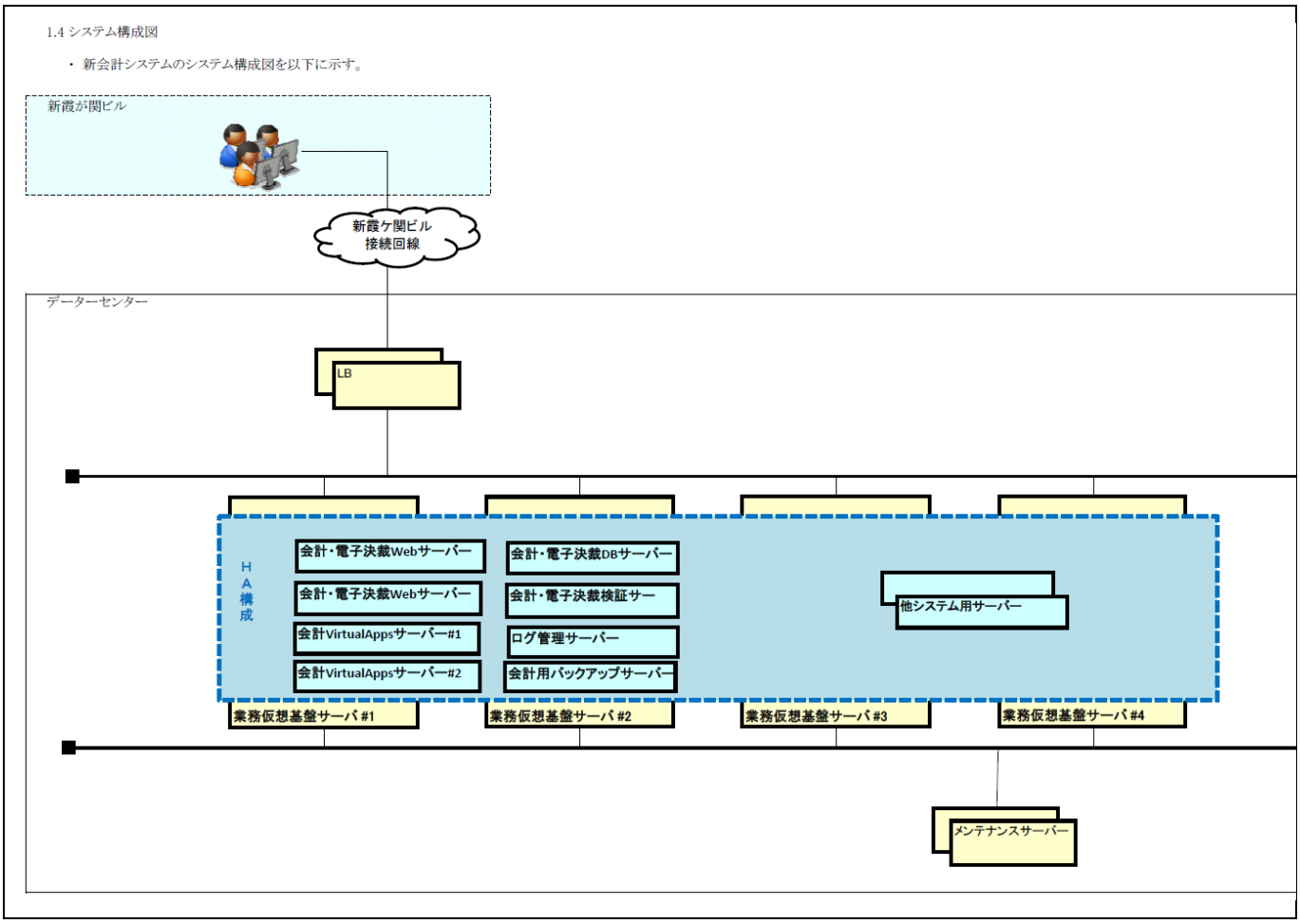
システム稼働環境は共用ＬＡＮシステムの仮想化ソフトウェア上のそれぞれ個別のゲスト OS 上で稼働するような構成とする。

ネットワーク機器、周辺機器等については可能な限り共用する。

（１）　全体構成

稼働環境を次に示す。

図　2-1　全体構成



ハードウェアは仮想化し、他システムとリソースを共有する。

データセンタは、総合機構が契約している既設のシステムが設置されているデータセンタを使用する。

データセンタと総合機構間の回線及びルータ等については、既設の回線を既設のシステムと共用する。この際、物理的には同じ回線を使用するが、論理的には既設のシステムとは別とする。

会計システムの利用可能範囲は、各職員の所掌業務に応じた設定に調整している。

会計システムは、本番環境及び検証環境を持つ。また、会計システムのアーキテクチャは XenApp を利用した仮想アプリケーションと Web アプリケーションから構成される。

（２）　ソフトウェア構成

会計システムを構成する OS・ミドルウェア等及び業務パッケージを「別紙３　ソフトウェア一覧」として添付する。

会計システムは「表 2-1　クライアント環境」に示す環境の利用端末から利用する。

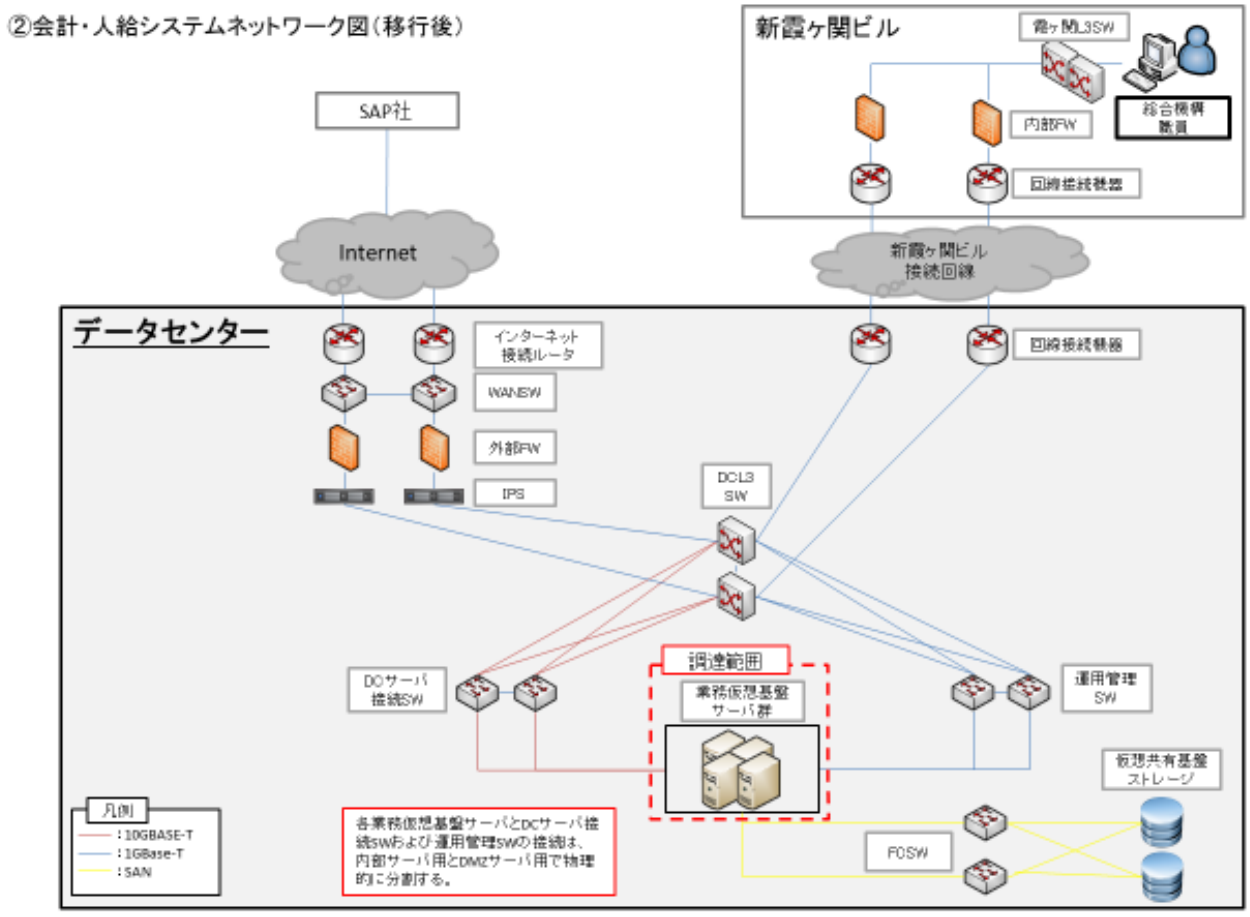
Java、その他のソフトウェアをクライアント環境にインストールする場合において、内閣官房情報セキュリティセンター（NISC）が推奨するバージョンがある場合にはそれに従うこと。

表 2-1　クライアント環境

No.	ソフトウェア	端末	補足
2.1	OS	○	Windows10 (64bit 版)
2.2	ブラウザ	○	MSEdge
2.3	Office ソフトウェア	○	Microsoft 365 (Word/Excel/Outlook)
2.4	PDF ソフトウェア（表示/生成）	○	Adobe Acrobat 11 Standard
2.5	ウィルス対策ソフトウェア	○	Windows Defender
2.6	クライアントソフトウェア	○	CitrixWorkSpace

（３）　ネットワーク構成

図 2-2　ネットワーク構成



３　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

本調達に含まれる役務の実施にあたっては、「表 3-1 会計・人給等全体システム関連業者」に示す業者と連携する必要がある。なお、事業者間で情報のやりとりが必要な場合は、必ず総合機構を介して行うこと。関連する調達案件の調達案件の調達単位、調達の方式、実施時期は「表 3-2 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)」のとおりである。

表 3-１会計・人給等全体システム関連業者

調達名	調達内容	受注者略称
会計システムの運用支援・保守業務	会計システムの運用支援・保守業務	受注者名：NEC ネクサソリューションズ（株）
人事給与システムの運用保守業務	人事給与システムの運用保守業務	受注者名：One 人事（株）（基盤導入ベンダー：ユニアデックス（株)）
文書管理・決裁システムの運用保守業務	文書管理・決裁システムの運用保守業務	受注者名：富士電機（株）
拠出金システムの Pegasus 連携	拠出金システムの Pegasus 連携	受注者名：BIPLOGY（株）

表 3-2　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	補足
1	拠出金オンライン決済対応のための改修	未定	令和 5 年度～令和 6 年度を予定	拠出金オンライン決済対応に伴う第 4 次会計システムの改修が必要となる可能性がある。

４　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を参照の上、以下に関し必要な作業を実施すること。

①　準備作業の内容

ア　実施計画書の作成

（ア）受託者は、契約開始日から令和６年４月１日（予定）の運用業務の開始までに、総合機構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「１０　（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、総合機構の承認を受けること。

（イ）本業務を実施するにあたっての作業従事者名（再委託がある場合は想定される再委託先の会社名を含む)、役割分担、指揮命令系統を記載した作業実施体制図（案）を業務実施計画書の一部として作成すること。

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、総合機構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4「業務要件」の「運用業務の範囲定義」に示す運用業務（システム操作、運転管理・監視、稼動状況監視、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5「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、総合機構に報告すること。

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5参照）
E) インシデント管理状況（別紙5参照）
F) 問題管理状況(別紙5参照)
G) 変更管理状況（別紙5参照）
H) バックアップ取得状況(別紙5参照)
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5参照)
J) 脆弱性管理（別紙5参照）
K) アクセス権管理状況（特権（高権限 ID）管理状況）(別紙5参照)
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5参照)
M) サービスレベル達成状況（別紙5参照）
N) 情報システムの定期点検状況（別紙6「情報セキュリティ対策の運用要件」参照）
O) 教育･訓練状況
P) 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。

(オ) 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、総合機構にその旨を報告し、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、総合機構の指示に基づき、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、条件等を調査の上総合機構に報告すること。
（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総合機構に報告すること。

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、総合機構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４「業務要件」の「保守業務の範囲定義」に示す保守業務（不具合受付等）及び定期点検（サーバ等のヘルスチェック）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（サーバ等のヘルスチェック）の結果について、速やかに総合機構へ報告すること。またシステム設定値等の差異がみられる場合は、総合機構へ報告の上、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）受注者は、年１回、総合機構の指示に基づき、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）受注者は、年１回、総合機構の指示に基づき、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

受注者は、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　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、速やかに総合機構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５「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、「総合機構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、総合機構の指示を受けて、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、総合機構と協議の上、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。

⑤　作業報告

ア　作業工数実績の報告

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

⑥　引継ぎ

ア　本システムの更改時

受託者は、総合機構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提供及び質疑応答等の協力を行うこと。

イ　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６年４月１日（予定）からの運用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。

ウ　次期運用事業者への引継ぎ

受託者は、本調達に係る契約期間終了後、受託者と異なる事業者が本情報システムの運用業務を受注した場合には、次期運用事業者に対し、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。

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

⑦　共用 LAN 基盤更改に伴う会計システムサーバ移行対応

ア　サーバ移行に伴う設定変更

会計システムは共用ＬＡＮ基盤上に構築された仮想サーバ上に構成されている。受託者は、総合機構が共用ＬＡＮ基盤を更改した後に必要な設定変更を行うこと。想定する作業は以下のとおり。

A) 会計システムサーバの IP アドレス変更に伴う設定変更（サーバ IP アドレス、DNS、NW 機器、仮想基盤の設定変更は総合機構の作業とする）
B) OS ライセンス再認証
C）証明書リクエストファイル作成及び証明書設定後の動作確認（証明書の作成、負荷分散装置への証明書投入および負荷分散装置の設定は総合機構の作業とする）
D) V2V 前の会計システムの健常性確認、サーバの停止及び移行作業後の健常性確認
E）その他会計システムの正常動作に必要な作業

イ　除外事項

以下の作業については総合機構が実施するため、受託者の作業範囲から除外する。

A）旧基盤から新基盤へのサーバ移行（V2V）作業
B）会計システムサーバの IP アドレス、DNS、NW 機器、仮想基盤の設定変更
C）システム監視、ウイルス対策ソフトウェアの設定変更

ウ　その他

本作業の実施時期については令和 6 年 4 月～9 月を予定しているが、詳細は別途総合機構と調整すること。

（２）　システム資産簿登録に係る作業

ア　総合機構においては、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総合機構へ報告し、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総合機構と協議の上、合わせて管理すること。

イ　受託者は対象システムに更新等が発生した場合、下記のシステム構成情報に関し、総合機構が指定するシステム資産簿登録用シートを、総合機構が指示する時期に提出すること。

（ア）　IT 機器管理簿
（イ）　導入ソフトウェア一覧（ソフトウェアの名称、版数、パッチ適用状況、ソフトウェアの搭載機器、ライセンス数、サポート期間等）
（ウ）　資産収集情報詳細
（エ）　ハードウェアサポート期限
（オ）　ソフトウェアサポート期限
（カ）　ソフトウェアライセンス
（キ）　ソフトウェア名称
（ク）　その他総合機構が指定する項目

＜補足＞

○総合機構の資産台帳・管理簿(システム台帳)は下記の項目で更新する。

・情報システム名　・管理課室　・当該情報システムセキュリティ責任者の氏名及び連絡先　・システム構成　・機器の名称　・型番　・数量　・脆弱性/アップデート公開情報　・アップデート適用履歴　・機器の設置場所　・サポート期間　・接続する機構外通信回線の種別　・取り扱う情報の格付及び取扱制限に関する事項　・当該情報システムの設計/開発、運用/保守に関する事項

○総合機構のネットワーク機器ソフトウェア資産台帳を下記の項目で更新する。

・ネットワーク機器名　・ソフトウェア名　・バージョン　・脆弱性/アップデート公開情報　・アップデート適用履歴　・外部との通信内容　・設定シートパス名　・その他のサポート状況・リスク　・確認頻度　・最終確認日

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 4.1 に示す。ただし、納入成果物の構成、詳細については、受注後、総合機構と協議し取り決めること。

表 4.1　工程と成果物

項番	工程	納入成果物（注 1）	納入期日	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） ・情報セキュリティ管理計画書（「１０ （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）	令和６年４月１日（予定）の運用業務の開始まで	
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	初版：令和６年４月１日 その後、必要に応じて随時提出	
4	その他	・作業週報 ・月例報告資料 ・アウトソーシングセンター設置サーバ稼働状況報告書 ・打合せ資料 ・議事録 ・障害等作業記録 ・運用支援報告書	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。

㈀ジョブ一覧、㈁起動・停止手順、㈂バックアップ手順、㈃リカバリ手順、㈄障害監視手順、㈅障害対応手順、㈆ログ確認手順、㈇性能監視手順、㈈設定変更手順、㈉ユーザ管理手順、㈊マスタの更新及びそれに伴うデータ修正手順、㈋ ㈀～㈊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。

㈀問合せ管理プロセス　㈁インシデント管理プロセス　㈂変更管理プロセス　㈃リリース管理プロセス　㈄構成管理プロセス　㈅問題管理プロセス　㈆各定期点検プロセス　㈇リスク管理プロセス　㈈課題管理プロセス　㈉情報セキュリティ管理プロセス。

② 納品方法

表 4.1 の納入成果物を含む全ての納入成果物を期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、

総合機構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、総合機構と協議すること。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、総合機構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、総合機構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、総合機構の承認を得ること。

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、構成等について総合機構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、記載様式案を総合機構に提示すること。総合機構は、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　財務管理部

ただし、総合機構が納品場所を別途指示する場合はこの限りではない。

５　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４　業務要件

○別紙５　システム運用管理基準

○別紙６　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)

６　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、総合機構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、総合機構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、当該品質保証体制における責任者及び連絡担当者を明記し書類等で確認できること。

② 本情報システムに総合機構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、総合機構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総合機構と協議の上、決定するものとする。

④ 受託者は、総合機構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総合機構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総合機構と協議の上定めること。

（２）　責任者の要件

全体を統括する責任者（以下「管理責任者」という。）を選任するとともに、以下に示すリーダを置くものとする。なお、それぞれの管理責任者、リーダについては、兼務しないものとする。

管理責任者	プロジェクトすべての運営に係る責任をもつ。
運用支援・保守リーダ	会計システムに係る運用支援・保守業務を統括する。

① 本調達における管理責任者は、契約期間を通して、総合機構からの連絡・要望に対して必要な対応が取れるようにし、意思決定の遅延を発生させないこと。また、不測の事態が発生してもスケジュール遅延を発生させないようにすること。

② 受注者は、原則プロジェクト完了まで継続して続けられる技術者・資格者を責任者・リーダとすること。ただし、適切な業務が期待できないと総合機構が判断した技術者・資格者については、責任者・リーダの変更を要請することがある。このようなケースを含む「真にやむを得ない担当者変更」等の場合は、事前に総合機構と協議して、変更の可否を確認すること。また、責任者・リーダ変更の際は、総合機構と協議した上、十分な引継ぎ期間 を設けて、プロジェクト管理に影響しないよう配慮すること。

（３）　作業要員に求める資格等の要件

① 運用支援・保守リーダの必要スキル

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 3 年以上
C) 類似のシステムの構築経験有りまたは運用保守経験が 3 年以上
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、総合機構の了承を得ること）
E) 日本語による「円滑な意思疎通」が図れること

② 各専門分野のスキル

ア セキュリティ

A) 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。

イ データベース

A) 情報処理技術者(データベーススペシャリスト試験（DB)、又はテクニカルエンジニア(データベース))資格を保持していること。又は、それと同等のデータベース専門スキルを持つ技術者が運用業務者の中に含まれること。

ウ オペレーティングシステム

A） マイクロソフト認定システムアドミニストレータ（MCSA）以上の資格保持者が運用業務者の中に含まれること。又は、それと同等のオペレーティングシステム専門スキルを持つ技術者が運用業務者の中に含まれること。

エ 会計業務を理解しており、本業務システムの運用・保守にあたり、総合機構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。

オ 日本語による「円滑かつ高度な意思疎通」が図れること。

上記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。

（4） 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）総合機構内、又は日本国内で総合機構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 総合機構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、必要に応じて総合機構職員は現地確認を実施できることとする。

（５）　作業の管理に関する要領

① 受託者は、総合機構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、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、総合機構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、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 総合機構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総合機構に対し、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。

７　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、総合機構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、総合機構からの質問、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、総合機構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総合機構が開示した情報（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、総合機構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、速やかに総合機構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総合機構に提出すること。
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。

（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、「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」は非公開であるが、「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（最新版）」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、入札説明会に参加した事業者のうち、事業者が総合機構に「秘密保持等に関する誓約書」を提出した際に開示する。
③　総合機構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、総合機構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、事前に総合機構に提出すること。また、そのような事態が発生した場合は、総合機構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。

８　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、総合

機構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総合機構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。この場合は事前に総合機構に報告し、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総合機構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、総合機構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、総合機構に提出する際は、その旨併せて報告するものとする。

（２） 契約不適合責任

① 受注者は本業務の納入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 1 年以内の期間において、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、総合機構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、事前に総合機構の承認を得てから着手すると共に、修正結果等について、総合機構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、その一覧を総合機構に提出すること。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総合機構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、総合機構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、「4 (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、総合機構が確認し、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、受注者は直ちに引き取り、必要な修復を行った後、総合機構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 総合機構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。

９ 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（日本産業規格）のいずれかを取得していること。

③ 総合機構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。

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、応札後に総合機構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 総合機構の 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

１０ 情報セキュリティ管理

（１） 情報セキュリティ対策の実施

受注者は、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受注後速やかに提出して総合機構の承認を受けること。

① 総合機構から提供する情報の目的外利用を禁止すること。

② 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。

③ 本業務の実施に当たり、受注者又はその従業員、本調達の役務内容の一部を再委託する先、若しくは

その他の者により、総合機構の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。

④ 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総合機構と協議の上、決定するものとする。

⑤ 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。

⑥ 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、総合機構へ報告すること。

⑦ 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、総合機構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、総合機構と協議の上、その指示に従うこと。

⑧ 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、総合機構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。

⑨ 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①～⑧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、総合機構の承認を受けること。

⑩ 総合機構から要保護情報を受領する場合は、予め総合機構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。

⑪ 総合機構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。

⑫ 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、速やかに総合機構に報告すること。

（２） 情報セキュリティ監査の実施

① 総合機構が必要と判断した場合は、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（総合機構が選定した事業者による監査を含む。）ものとする。受注者は、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。

② 受注者は自ら実施した外部監査についても総合機構へ報告すること。

③ 受注者は、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総合機構が改善を求めた場合には、総合機構と協議の上、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。

④ 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。

⑤ 受注者は、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、総合機構と協議の上、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。

１１　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

① 受注者は、受託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 プロジェクト管理責任者を再委託先事業者の社員とすることはできない。

③ ①における「主要部分」とは、以下に掲げるものをいう。

ア 総合的な企画及び判断並びに業務遂行管理

イ 手法の決定及び技術的判断

ウ 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（本調達における工数全体の２分の１以下を目安とし、総合機構が事前に承認したもの）であった機能に係るソフトウェア要件定義等業務

④ 再委託先が「９（２）入札制限」の要件を満たすこと。

⑤ 受注者の責任において、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。

- 総合機構から提供する情報の目的外利用を禁止すること。
- 受注者は、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、総合機構へ報告すること。
- 受注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、その原因について調査・排除するため、総合機構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、その対処方法を検討し、総合機構へ報告すること。
- 受注者は、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。
- 受注者は、再委託先が自ら実施した外部監査についても総合機構へ報告すること。
- 受注者は、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。

（２）　承認手続

受注者は、受託業務を再委託する場合、予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「再委託に関する承認申請書」

を提出し、総合機構の承認を受けること。

申請にあたって、次に掲げる事項を遵守すること。

・ 再委託先が「１０（１）情報セキュリティ管理の実施」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）

・ 再委託の相手方は「9（２）入札制限」の対象となる事業者でないこと。

・ 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、総合機構に報告し、承認を受けること。

・ 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）・実績及び国籍に関して、総合機構から求めがあった場合には情報提供を行うこと。

（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、総合機構は、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。

１２ 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

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

１３ 附属文書

（１） 調達仕様書　別紙

別紙１　「システム概略図」

別紙２　「用語一覧」

別紙３　「ソフトウェア一覧」

別紙４　「業務要件」

別紙５　「システム運用管理基準」
別紙６　「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

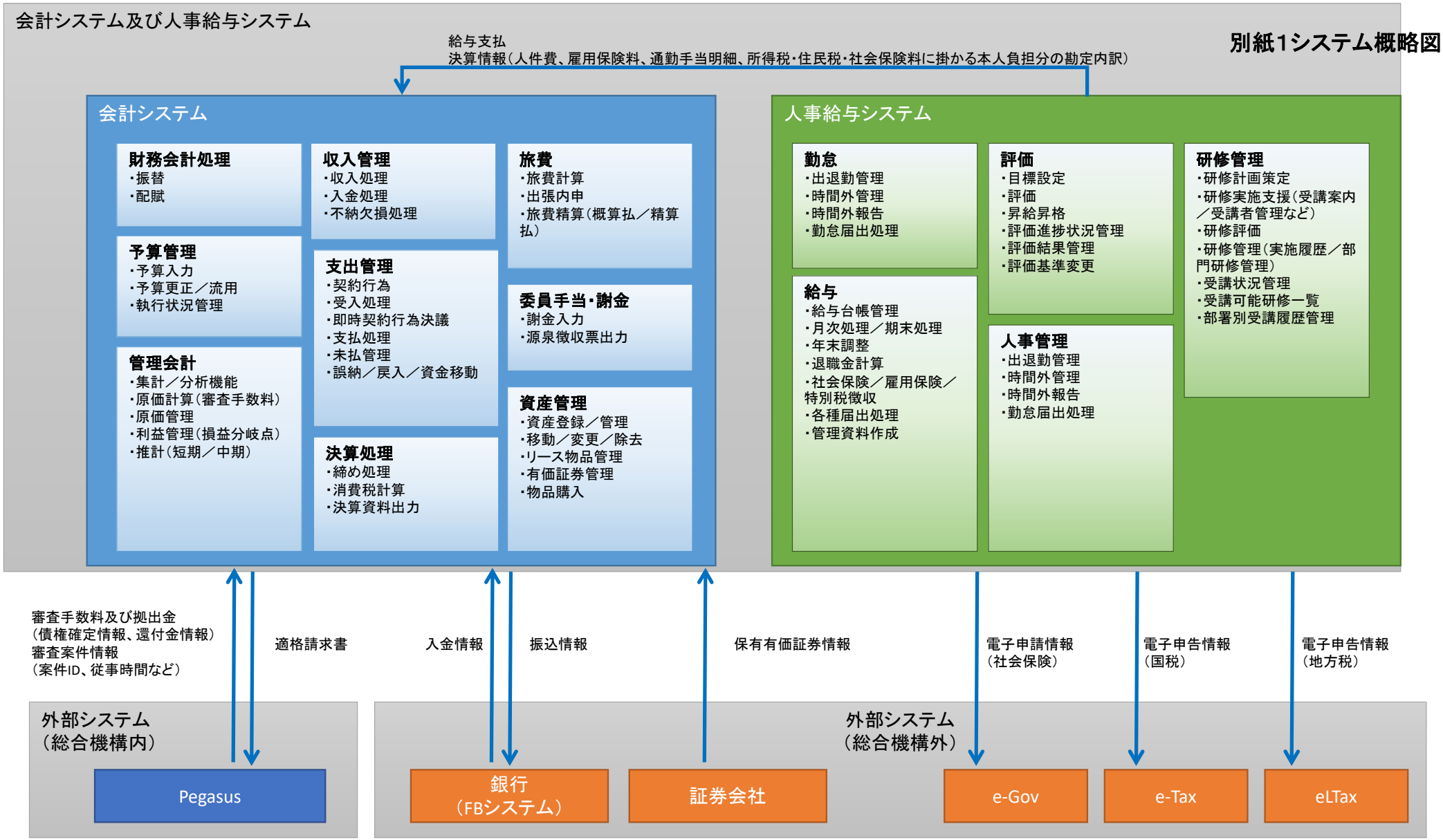
閲覧資料１　独立行政法人 医薬品医療機器総合機構　サイバーセキュリティポリシー
閲覧資料２　総合機構情報セキュリティインシデント対処手順書
閲覧資料３　セキュリティ管理要件書(ひな型)
閲覧資料４　第４次会計システム設計書

（３）　閲覧要領

資料の閲覧を希望する場合は、「秘密保持等に関する誓約書」を提出の上、総合機構が定める期間、場所、方法において閲覧を許可する。閲覧可能としている資料については、複写及び撮影等は禁止する。

１４　窓口連絡先

財務管理部　吉田　圭一
電話：　03（3506）9410
e-mail：　zaimu-info●pmda.go.jp
※　●を@に置き換えてください


会計システム及び人事給与システム
別紙1システム概略図
給与支払
決算情報（人件費、雇用保険料、通勤手当明細、所得税・住民税・社会保険料に掛かる本人負担分の勘定内訳）
会計システム
財務会計処理
・振替
・配賦
予算管理
・予算入力
・予算更正／流用
・執行状況管理
管理会計
・集計／分析機能
・原価計算（審査手数料）
・原価管理
・利益管理（損益分岐点）
・推計（短期／中期）
収入管理
・収入処理
・入金処理
・不納欠損処理
支出管理
・契約行為
・受入処理
・即時契約行為決議
・支払処理
・未払管理
・誤納／戻入／資金移動
決算処理
・締め処理
・消費税計算
・決算資料出力
旅費
・旅費計算
・出張内申
・旅費精算（概算払／精算払）
委員手当・謝金
・謝金入力
・源泉徴収票出力
資産管理
・資産登録／管理
・移動／変更／除去
・リース物品管理
・有価証券管理
・物品購入
人事給与システム
勤怠
・出退勤管理
・時間外管理
・時間外報告
・勤怠届出処理
給与
・給与台帳管理
・月次処理／期末処理
・年末調整
・退職金計算
・社会保険／雇用保険／特別税徴収
・各種届出処理
・管理資料作成
評価
・目標設定
・評価
・昇給昇格
・評価進捗状況管理
・評価結果管理
・評価基準変更
人事管理
・出退勤管理
・時間外管理
・時間外報告
・勤怠届出処理
研修管理
・研修計画策定
・研修実施支援（受講案内／受講者管理など）
・研修評価
・研修管理（実施履歴／部門研修管理）
・受講状況管理
・受講可能研修一覧
・部署別受講履歴管理
審査手数料及び拠出金
（債権確定情報、還付金情報）
審査案件情報
（案件ID、従事時間など）
適格請求書
入金情報
振込情報
保有有価証券情報
電子申請情報
（社会保険）
電子申告情報
（国税）
電子申告情報
（地方税）
外部システム
（総合機構内）
Pegasus
外部システム
（総合機構外）
銀行
（FBシステム）
証券会社
e-Gov
e-Tax
eLTax

【別紙2】用語一覧

ID	用語名	読み方	用語の意味
1	副作用拠出金（一般拠出金、付加拠出金）	ふくさようきょしゅつきん（いっぱんきょしゅつきん、ふかきょしゅつきん）	医薬品等の副作用による健康被害者に対して支払う給付金のための費用のことであり、許可医薬品製造販売業者より拠出される。 一般拠出金は、全ての許可医薬品製造販売業者が前年度の許可医薬品の総出荷数量に応じて納付する。付加拠出金は、健康被害の直接の原因となった許可医薬品製造販売業者が納付する。
2	感染拠出金（一般拠出金、付加拠出金）	かんせんきょしゅつきん（いっぱんきょしゅつきん、ふかきょしゅつきん）	生物由来製品等を介した感染等による健康被害者に対して支払う給付金のための費用のことであり、許可生物由来製品製造販売業者等より拠出される。 一般拠出金は、全ての許可生物由来製品製造販売業者等が前年度の許可生物由来製品等の総出荷数量に応じて納付する。付加拠出金は、健康被害の直接の原因となった許可生物由来製品製造販売業者等が納付する。
3	特定救済拠出金	とくていきゅうさいきょしゅつきん	特定フィブリノゲン製剤及び特定血液凝固第Ⅸ 因子製剤によるC 型肝炎感染被害者を救済するための給付金の支給に関する特別措置法第17条第1項の規定に基づき、製造業者等から拠出される費用のこと。
4	安全対策等拠出金	あんぜんたいさくとうきょしゅつきん	機構が行う安全対策に必要な費用のこと。前年度の医薬品及び医療機器、体外診断用医薬品、再生医療等製品の総出荷数量に応じて、医薬品又は医療機器製造販売業者等より拠出される。
5	医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（薬機法）	いやくひん、いりょうききとうのひんしつ、ゆうこうせいおよびあんぜんせいのかくほとうにかんするほうりつ（やっきほう）	機構が実施している医薬品や医療機器、一般用医薬品、医薬部外品、体外診断用医薬品、再生医療等製品に対する品質、有効性、安全性の審査・調査・相談業務等の根拠法律。
6	審査等手数料	しんさとうてすうりょう	機構で実施している、薬機法に基づく医薬品や医療機器、一般用医薬品、医薬部外品、体外診断用医薬品、再生医療等製品に対する品質、有効性、安全性の審査・調査・相談業務等に係る手数料のこと。手数料の金額は薬機法関係手数料令に基づく。
7	医薬品医療機器申請・審査システム	いやくひんいりょうききしんせいしんさしすてむ	薬機法、薬機法施行令、薬機法施行規則、業務方法書実施細則及びそれらに関する厚生労働省からの通知に基づき行政機関が行う、申請等の受け付け、審査・調査結果の入力、許認可の施行登録、証書・通知書の発行等のいわゆる「許認可業務」及び当該業務に関連する各種業務は薬機法に定められた許認可に関する申請等について、受付から審査、承認までの行政側業務を支援するシステム。

【別紙2】用語一覧

ID	用語名	読み方	用語の意味
8	副作用救済給付システム	ふくさようきゅうさいきゅうふしすてむ	医薬品の副作用被害の救済に係る給付金について、申請受理から支払いまでの情報の管理を行うシステム。
9	感染救済給付システム	かんせんきゅうさいきゅうふしすてむ	生物由来製品、再生医療等製品による感染被害の救済に係る給付金について、申請受理から支払いまでの情報の管理を行うシステム。
10	特定C型肝炎給付金支援等業務システム	とくていしーがたかんえんきゅうふきんしえんとうぎょうむしすてむ	特定C型肝炎ウイルス感染者またはその相続人からの給付金請求の受付、給付金の支給、基金・拠出金等の管理等の業務を行うためのシステム。
11	拠出金徴収管理システム	きょしゅつきんちょうしゅうかんりしすてむ	拠出金徴収業務に係る申請書等の送付、収納・債権管理等の業務支援を行うシステム。
12	受託貸付関連システム	じゅたくかしつけかんれんしすてむ	原因企業や国からの委託で行っている、スモン患者に対する健康管理手当及び介護費用の支払業務を行うためのシステム。
13	受託給付業務データベースシステム	じゅたくきゅうふぎょうむでーたべーすしすてむ	血液製剤によるエイズ患者等のための救済事業（受託給付事業）に係る業務の管理を行うためのシステム。
14	関連表	かんれんひょう	財務諸表3表（貸借対照表、損益計算書、キャッシュフロー計算書）を作成するための計算表のこと。関連表の内訳として、「収入、支出決算(見込)額算出表」、「収入、支出決算と資金収支等との関連表」、「資金収支（見込）と貸借対照表、損益計算書の関連表」、「その他の決算修正取引の内訳」がある。
15	28条	２８じょう	財政法第28条のこと。通称ニッパチ。

【別紙2】用語一覧

ID	用語名	読み方	用語の意味
16	28条予算基礎資料	28じょうよさんきそしりょう	財政法第28条において指定されている書類（財務諸表3表）の元となる関連表を作成するための基礎となる資料。
17	予算流用	よさんりゅうよう	規定の予算の金額を、別の科目に融通して使用すること。
18	予算科目更生	よさんかもくこうせい	科目に対して設定されている予算額を訂正すること。
19	謝金	しゃきん	調査への協力者、講師等への謝礼の為の金銭のこと。
20	債権発生通知	さいけんはっせいつうち	拠出金や手数料など、総合機構に債権が発生したときに行う手続きのこと。各担当者が収納命令役に通知する。システムにより収納命令役に当該振替伝票が承認されたことをもって、通知があったものとみなす。
21	調査決定	ちょうさけってい	債権を確定する際に、関係書類に基づいてその債権に誤りがないか、納入者、期限等が適正であるかの調査を行う。その結果に基づいた決議のこと。システムによる振替伝票で行う。
22	契約行為	けいやくこうい	物品購入等、契約行為後受入処理がある契約の決定を行う行為のこと。購入依頼を入力し、その後承認を行うことで、契約行為が行われている。
23	過誤納金	かごのうきん	誤って納付された金銭の総称のこと。

【別紙2】用語一覧

ID	用語名	読み方	用語の意味
24	算定基礎取引額	さんていきそとりひきがく	算定基礎取引額とは、医薬品をその被害可能性に応じて区分し、各品目の出荷数量にその単価を乗じて得た額に、その区分ごとの一定の係数（傾斜係数）を乗じて得た額をいう ・ 算定基礎取引額 ＝ 各品目の出荷数量 × 単価 × 傾斜係数
25	不納欠損処理	ふのうけっそんしょり	歳入徴収額を調定したもののうち、徴収が行えず、今後も徴収の見込みがたたないため、徴収を諦める処理のこと。
26	契約担当役	けいやくたんとうやく	収入または支出の原因となる契約その他の行為に関することを行う会計機関のこと。
27	収納命令役	しゅうのうめいれいやく	収入金の調査及び徴収の決定、債務者（返納金債権に係るものを除く。）に対する納入の告知又は督促（拠出金に係るものを除く。）、出納役に対する現金、預金又は有価証券の受入命令並びに収入の経理に関連する各勘定科目相互間の振替命令に関することを行う会計機関のこと。
28	支払命令役	しはらいめいれいやく	支出の調査及び決定、出納役に対する現金、預金又は有価証券の支出命令、返納金債権の管理（債権者に対する納入の告知又は督促を含む。）並びに支払の経理に関連する各勘定科目相互間の振替命令に関することを行う会計機関のこと。
29	出納役	すいとうやく	現金、預金又は有価証券の出納保管に関することを行う物品の管理機関のこと。
30	財産管理役	ざいさんかんりやく	物品（現金、預金及び有価証券以外の一切の動産をいう。以下同じ。）及び不動産（現金、預金及び有価証券並びに物品以外のものをいう。）の取得、管理及び処分に関することを行う会計機関のこと。
31	物品供用役	ぶっぴんきょうようやく	所掌する物品の供用及び保管に関する事務を行う会計機関のこと。

【別紙2】用語一覧

ID	用語名	読み方	用語の意味
32	購入依頼	こうにゅういらい	物品等購入依頼書のこと。
33	原課	げんか	機構の業務担当部署の総称。
34	発翰	はっかん	書翰（しょかん：手紙や文書のこと）を発信すること。
35	開示請求手数料	かいじせいきゅうてすうりょう	情報公開の開示請求（申請）に伴い発生する受付手数料（1件300円）。
36	開示実施手数料	かいじじっしてすうりょう	情報公開の開示実施に伴い発生する手数料。料金は、開示方法、開示内容により異なる。
37	トーナメント表	とーなめんとひょう	支払時に各口座から出納口座へ移動する金額とそこから支払方法別（現金、納付依頼書、ファームバンキング）に金額を表示した表のこと。
38	FBデータ	ふぁーむばんきんぐでーた	ファームバンキングとは、インターネットや電話回線を使って銀行の入出金明細や振込などを行うサービスのことであり、FBデータは振込内容などを記載したデータのこと。
39	償還	しょうかん	債券や投資信託などで期限（期日）が到来して投資家に資金が返されること。

【別紙2】用語一覧

ID	用語名	読み方	用語の意味
40	指定都市、甲地方、乙地方、丙地方	していとし、こうちほう、おつちほう、へいちほう	財務省令にて定められたものであり、それぞれの都市、地方ごとに出張の際に支給される宿泊費用が異なる。
41	標示票（ラベル）	ひょうじひょう	資産を取得した時に貼り付けるラベルのこと。
42	用務	ようむ	出張等に課せられている務めのこと。
43	種別	しゅべつ	収入の種類を示す分類のこと。審査手数料、拠出金、開示手数料、運営費交付金、利息等、その他、など。
44	勘定区分	かんじょうくぶん	経理を区分する勘定のこと。「副作用救済勘定」「感染救済勘定」「審査等勘定」「特定救済勘定」「受託・貸付勘定」「受託給付勘定」の6区分がある。
45	セグメント	せぐめんと	審査等勘定の中で、業務毎に区分して経理すべきものをセグメントとしている。 審査セグメント（運営費交付金による事業と手数料収入等による事業（医薬品等の審査及びこれに関連する適合性調査、医薬品の治験等に関する指導及び助言、並びにこれらに関連する事業）と安全セグメント（運営費交付金による事業と拠出金収入等による事業（医薬品の安全性等に関する調査及び分析並びにこれらに関連する事業））の2つのセグメントがある。
46	事業区分コード	じぎょうくぶんこーど	各勘定、セグメント等の下にある各事業にある各支出科目に紐づいているもの。コードはメッシュ化され、最下層の各支出科目に紐づけられている。
47	財源コード	ざいげんこーど	費用計上する際に、財源となる項目を選択するコードのこと。審査手数料、拠出金、国庫補助金、運営費交付金、受託業務、などがある。コードはメッシュ化され、最下層の各支出科目に紐づけられている。

【別紙2】用語一覧

ID	用語名	読み方	用語の意味
48	按分コード	あんぶんこーど	購入依頼や支出決議等の際に、購入依頼部署等により、総額から勘定、セグメントに応じ按分を乗じて支出等することがある。按分は複数あるため、按分率によりコードを割り振っている。
49	国借受物品	くにかりうけぶっぴん	事業を行うために国からの現物出資もしくは出資により購入した物品のこと。その他の資産と分けて管理する必要がある。
50	グリーン調達	ぐりーんちょうたつ	物品調達を行う際に、環境負荷の小さいものを優先的に選択すること。2001年度施行のグリーン購入法に基づく。
51	共用LANシステム	きょうようらんしすてむ	機構で一般事務業務処理に用いられているサーバ計算機群、クライアントPC、内部ネットワーク、インターネット接続機器の総称のこと。
52	サーバ機器等	さーばききとう	サーバ、ストレージ等のハードウェア、及びOS、運用監視ソフト等のソフトウェアを含む。
53	設計・開発作業	せっけいかいはつさぎょう	アプリケーション機能の要件定義、設計、開発、テストの一連の作業。また、業務パッケージソフトウェアの導入及びアプリケーション環境の構築作業並びに受入テスト期間中に必要となる受入テスト支援作業も含まれる。
54	設計・開発事業者	せっけいかいはつじぎょうしゃ	会計システムの設計・開発・移行作業を担当する事業者のこと。
55	ITスキル標準	あいてぃーすきるひょうじゅん	各種IT関連サービスの提供に必要とされる能力を明確化・体系化した指標であり、産学におけるITサービス・プロフェッショナルの教育・訓練等に有用な「ものさし」（共通枠組）を提供しようとするもの。（http://www.ipa.go.jp/jinzai/itss/itss1.html）

【別紙2】用語一覧

ID	用語名	読み方	用語の意味
56	総合機構の休日	そうごうきこうのきゅうじつ	「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」で定められる通りとする。
57	PMBOK	ぴんぼっく	プロジェクトマネジメント協会（PMI：Project Management Institute）が提供するプロジェクトマネジメントに関する知識体系。
58	EVM	いーぶいえむ	EVM（Earned Value Management）：プロジェクト活動の進ちょく状況を管理する手法の1つ。
59	共用LANシステム基盤	きょうようらんしすてむきばん	別途調達となる「共用LANシステムサーバリプレイス」で導入されるシステム基盤。 IT 設備の活用効率化を図り、現在 PMDA で運用している業務システムが本調達時及び将来にわたり共通基盤・セキュリティ基盤として利用できることを目的とする。

別紙3 ソフトウェア一覧

物理サーバ名称	仮想サーバ名称	導入ソフトウェア	ソフトウェア種別	納入業者種別
業務仮想基盤サーバ#1～4				
		VMware vSphere 6.5 Standard	共通利用部分Agentソフトウェア	ハードウェア事業者
		Deep Security Virtual Appliance Anti Virus	共通利用部分Agentソフトウェア	ハードウェア事業者
	会計Webサーバ#1,2			
		Windows Server 2019 Standard Edition	OS	会計システム設計・開発業者
		駅すぱあとイントラネットVer2	会計システム用業務パッケージ	会計システム設計・開発業者
		Arcserve UDP エージェント	バックアップ（エージェント）	会計システム設計・開発業者
		LOGSTORAGE Agent	ログ管理（エージェント）	会計システム設計・開発業者
		Zabbix Agent	稼働監視(エージェント)	ハードウェア事業者
	会計VirtualAppsサーバー#1,2			
		Windows Server 2019 Standard Edition	OS	会計システム設計・開発業者
		Citrix Virtual Apps and Desktops 7 2203 LTSR	アプリケーション仮想化	会計システム設計・開発業者
		Arcserve UDP エージェント	バックアップ（エージェント）	会計システム設計・開発業者
		LOGSTORAGE Agent	ログ管理（エージェント）	会計システム設計・開発業者
		Zabbix Agent	稼働監視(エージェント)	ハードウェア事業者
	会計・電子決裁DBサーバー			
		Windows Server 2019 Standard Edition	OS	会計システム設計・開発業者
		Microsoft SQL Server 2019 Standard Edition	データベース	会計システム設計・開発業者
		Arcserve UDP エージェント	バックアップ（エージェント）	会計システム設計・開発業者
		Arcserve Backup r19.0 Client Agent for Windows	バックアップソフトウェア	会計システム設計・開発業者
		Arcserve Backup r19.0 for Windows Agent for Microsoft SQL	データベースバックアップ	会計システム設計・開発業者
		LOGSTORAGE Agent	ログ管理（エージェント）	会計システム設計・開発業者
		Zabbix Agent	稼働監視(エージェント)	ハードウェア事業者
	会計・電子決裁検証サーバー			
		Windows Server 2019 Standard Edition	OS	会計システム設計・開発業者
		Microsoft SQL Server 2019 Standard Edition	データベース	会計システム設計・開発業者
		Citrix Virtual Apps and Desktops 7 2203 LTSR	アプリケーション仮想化	会計システム設計・開発業者
		Arcserve UDP エージェント	バックアップ（エージェント）	会計システム設計・開発業者
		Arcserve Backup r19.0 Client Agent for Windows	バックアップソフトウェア	会計システム設計・開発業者
		Arcserve Backup r19.0 for Windows Agent for Microsoft SQL	データベースバックアップ	会計システム設計・開発業者
		LOGSTORAGE Agent	ログ管理（エージェント）	会計システム設計・開発業者
		Zabbix Agent	稼働監視(エージェント)	ハードウェア事業者
	会計用バックアップサーバー			
		Windows Server 2019 Standard Edition	OS	会計システム設計・開発業者
		Arcserve UDP 8.1	バックアップソフトウェア	会計システム設計・開発業者
		Arcserve UDP エージェント	バックアップ（エージェント）	会計システム設計・開発業者
		Arcserve Backup r19.0 for Windows	データバックアップ	会計システム設計・開発業者
		LOGSTORAGE Agent	ログ管理（エージェント）	会計システム設計・開発業者
		Zabbix Agent	稼働監視(エージェント)	ハードウェア事業者
	ログ管理サーバ			
		Windows Server 2019 Standard Edition	OS	会計システム設計・開発業者
		Arcserve UDP エージェント	バックアップ（エージェント）	会計システム設計・開発業者
		LOGSTORAGE　WG、集計、検知、レポート	ログ管理（エージェント）	会計システム設計・開発業者
		Zabbix Agent	稼働監視(エージェント)	ハードウェア事業者

別紙4 「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6年4月1日 ～令和11年7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、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。	9:30～18:00 ※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	【全体管理】	運用計画書の内容に基づき運用作業全体の管理を行い、適宜総合機構へ報告を行うこと。 また、会計システムに関する最新のプログラムの管理、開発ドキュメント・設定内容ドキュメントの構成管理を行うこと。 毎月定例会を開催し、SLA 達成状況、情報セキュリティ対応状況、問合せ対応、障害対応、その他運用・保守作業に関する状況及び履歴の報告を行うこと。	左記の内容
2	【システム監視 – 稼動監視】	本システムのハードウェア、ソフトウェア、ネットワークに対して、以下の稼動状況（パフォーマンス）を監視し、監視実績を記録・管理すること。 ※本システムのハードウェア、ソフトウェア、ネットワークに対し、死活監視、障害監視、エラー出力監視を行い、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。監視に当たっては事前に総合機構と協議の上、必要に応じてツール等を用いた常時監視の仕組みを構築すること。 ※各機器の稼働監視、ログ監視、性能監視、サーバやネットワーク機器等の稼働監視やメンテナンス業務等はサーバ等提供業者により実施される場合がある。それらの役割分担については別途総合機構へ確認すること。 (1) ソフトウェア及び開発アプリケーションの稼動状況 (2) ハードウェアの各種状況（性能、容量、故障、縮退）	左記の内容 なお、ハードウェアに関する情報は、必要に応じ、ハードウェア事業者より情報を入手し、管理すること。

No	名称	内容	受託者の役割
		(3) バックアップなどの定期起動ジョブの実行結果 (4) セキュリティアラートの発生状況	
3	【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・監視を行うこと。 収集したログについては、必要に応じて抽出、分析を行い、適宜バックアップを取得の上、必要に応じて外部環境に保管すること。	左記の内容 なお、ハードウェアに関する情報は、必要に応じ、ハードウェア事業者より情報を入手し、管理すること。
4	【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、ウィルス定義ファイルは常に最新の定義ファイルを使用すること。 本システムの機器およびソフトウェア等に対し、セキュリティパッチやアップデートに関する情報を入手し適用の可否を検討し、検討結果を総合機構に報告の後、適用の必要がある場合には、更新作業を行うこと。 セキュリティ対策上の設定変更の必要が生じた場合に、総合機構の了解を得て設定の変更を行うこと。	左記の内容
5	【システム設定・操作 – ジョブ管理】	会計システムの業務ジョブスケジュールについて、総合機構から業務スケジュールの変更依頼に基づき、必要となるジョブスケジュールの設定等を行うこと。また、ジョブの登録／変更／削除が必要となる場合には総合機構に提案し、総合機構の了解の下、当該作業を実施すること。	左記の内容
6	【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）を総合機構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総合機構に提案し、総合機構の了解の下、当該作業を実施すること。	左記の内容 なお、ハードウェアに関する情報は、必要に応じ、ハードウェア事業者より情報を入手し、管理すること。
7	【問い合わせ対応】	問い合わせ対応の時間は、総合機構営業日の9時30分から18時00分までとする。会計システム全体について、総合機構からの問合せに対し一元的に受付を行い、問合せ内容の一次切りわけを行う。切りわけの結果に応じて、適切なエスカレーションを行い、エスカレーション先からの回答を元に、総合機構へ回答を行うこと。なお、問合せは電子メールの他、電話（有人による応答ができる体制とすること））、もしくは直接口頭によるものとするが、それらの内容は記録し報告すること。	左記の内容
8	【業務支援】	(ア) 稼働開始時の問合せ支援・操作方法指導のため、総合機構に	左記の内容

No	名称	内容	受託者の役割
		支援要員が立会い、業務運用に応じた機能の説明等の迅速な問合せ対応を行うこと。(随時／適宜) (イ) 年度切替作業時に一定期間支援要員が立会い、現地問合せ対応及びマスタ設定支援を行うこと。 (ウ) 決算業務時に一定期間支援要員が立会い、現地問合せ対応及び決算業務支援を行うこと。	
9	【サービスレベル管理】	受託者と総合機構との間で締結した、ＳＬＡ(Service Level Agreement)に基づき、SLA の達成状況を管理し、定期的に報告すること。	左記の内容
10	【バックアップ/リカバリ】	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。	左記の内容
		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、総合機構の判断に従いリカバリ手順に沿って作業すること。	左記の内容
11	【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、ASP の設定データ等のデータ管理。	左記の内容
		(1) 必要データの保存と削除 定期的に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。	左記の内容
		(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、総合機構と協議の上、修正、削除の実施、確認、記録業務への対応を行うこと。	左記の内容
12	【その他】	運用・保守業務で使用しているドキュメント(資産管理簿、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、総合機構のレビューを受けて修正・改定を実施すること。	左記の内容

保守業務の範囲定義

No	名称	内容	受託者の役割
1	保守対象範囲		左記の内容
1	【システム設定・操作 － 設定変更】	業務アプリケーションを正常に稼動させるために、ハードウェア、OS、ミドルウェア等の設定の変更が必要となる場合には総合機構に提案し、総合機構の了解の下、ハードウェア事業者と連携して、当該作業を実施すること。	左記の内容
2	【ソフトウェア保守 － ソフトウェア更新】	会計システムはNECネクサソリューションズ社の財務会計コアシステムをベースにした機能と総合機構向けにカスタマイズ開発したものであり、受注者は当該システムの全範囲にわたり問合せ対応、調査対応、障害対応を実施し、総合機構へ対応報告を行うこと。 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)～(5)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、総合機構と協議の上、検証テストを実施の上で本番環境に反映させること。	左記の内容
		(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。	左記の内容
		(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、総合機構の承認を得ること。脆弱性対応	左記の内容

No	名称	内容	受託者の役割
		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、総合機構の承認の上で適用を実施すること。	左記の内容
		(4) 業務アプリケーションへのパッチの緊急適用 必要に応じ、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、総合機構の承認の上で適用を実施すること。	左記の内容
		(5) 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。	左記の内容
5	【不具合修正、軽微な改修】	第 4 次会計システムの稼働開始から令和 6 年 3 月 31 日までに現行の運用保守事業者から改修事項及び PMDA からの要望等を引き継ぐこと。 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、総合機構の指示の下、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。（年間10人月程度の作業を想定。） 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。	左記の内容
6	【上位互換対応】	（1）業務パッケージソフトがバージョンアップされた場合には、判断に必要な情報を提供するとともに、その適用について総合機構の承認を得て、実施すること。 （2）サーバの OS やミドルウェア等がバージョンアップされる場合には、ハー	左記の内容

No	名称	内容	受託者の役割
		ドウェア事業者等から必要な情報を収集するとともに影響度を調査し、適用の可否について総合機構に必要な情報を提供し、適用を行う場合には総合機構の承認を得て、実施すること。大規模な改修が必要なる場合には、必要な情報を提供すること。 （3）端末側の OS や文書作成管理ソフトウェア等のバージョンアップされた場合には、判断に必要な情報を提供するとともに、その適用について総合機構の承認を得て、実施すること。 （4）総合機構で利用している端末等が更新された場合には、以下の作業を実施すること。 ・ 業務アプリケーションの動作検証 ・ 業務アプリケーションの配布支援 ・ 業務アプリケーションのマニュアル等の更新	

別紙５

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」

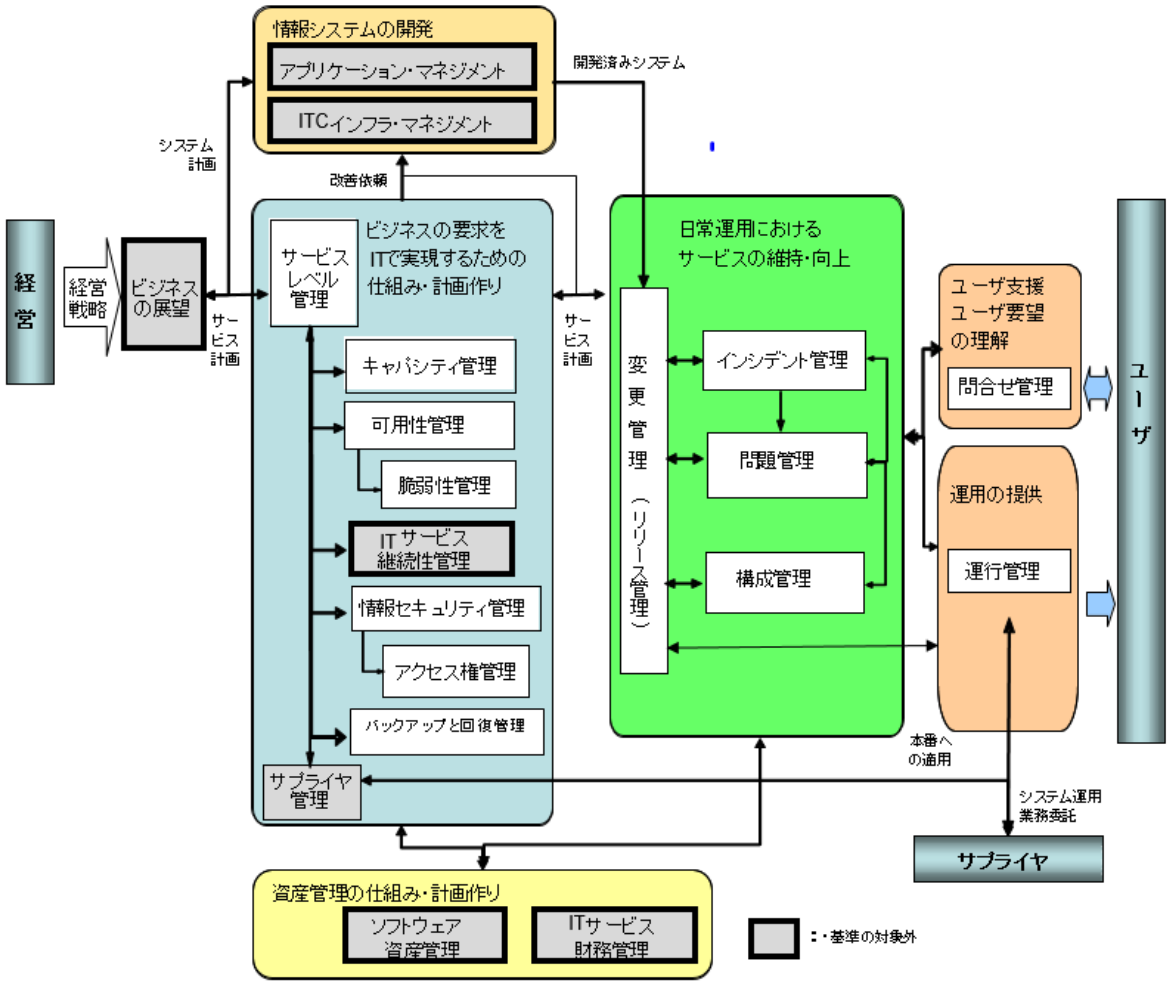
2. システム運用管理業務の概要

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

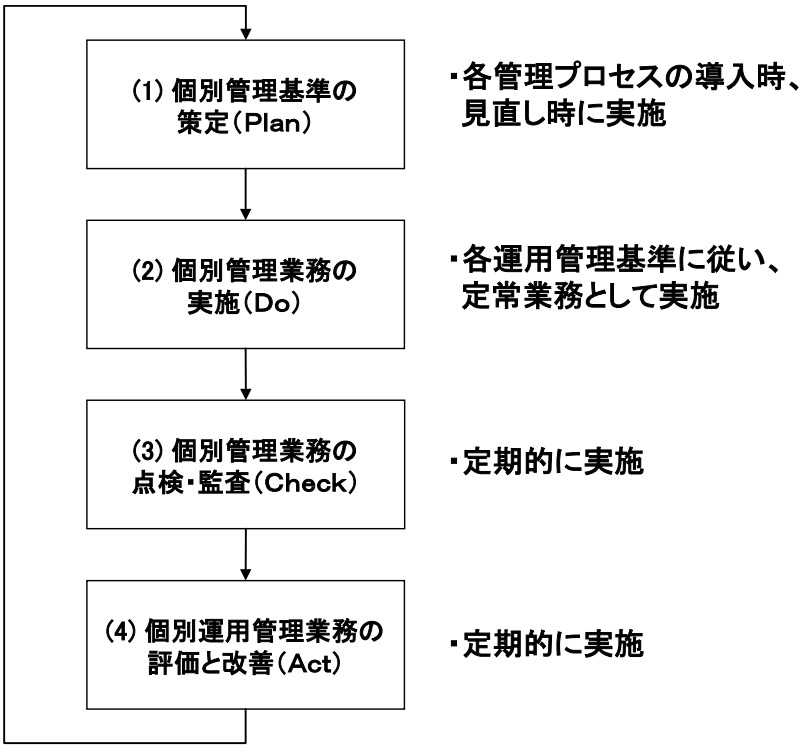


3. 運用管理業務の基本プロセス

（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6　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。	時刻同期に問題ないことを月次で確認する。もしくは、差異がある場合に検知する仕組みを構築する。
	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。