人事給与システムの基盤及びＯＳ運用保守業務
調達仕様書

令和５年 11 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

人事給与システムの基盤及びOS運用保守業務

（２）　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。）は、医薬品や医療機器等の承認審査業務、市販後における安全性に関する情報の収集、分析、提供等を行う安全対策業務、医薬品による副作用等の健康被害に対する健康被害救済業務を行う厚生労働省所管の独立行政法人である。

PMDAにおいては人事情報の管理及び職員の給与、賞与、各種手当等を算出、調整するために人事給与システムを導入しており、令和６年２月より次期人事給与システムが稼働予定である。

今回、次期人事給与システム用の構築済みの基盤における、令和６年１月～３月の運用保守業務を調達する。なお令和６年４月以降の本業務については、別途調達する次期人事給与システム運用保守業務に包含した形で調達予定である。

（３）　調達の範囲

次期人事給与システム基盤の運用保守業務を調達する。受託者は運用保守業務として、PMDAからの問い合わせ対応、脆弱性報告、ハードウェア・ソフトウェア保守対応、報告書等作成の作業を行うこと。

（４）　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。

①　契約期間

契約締結日～令和６年３月３１日までとする。

（運用保守期間は令和６年１月１日～令和６年３月３１日まで）

② 契約形態

請負契約形態とし、検収や支払方法等は契約書にて定める。

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

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構築業務	一般競争入札（総合評価）	令和４年４月～令和６年３月	スマカン㈱（現：One 人事㈱）	
2	次期勤務管理システム構築業務	一般競争入札（総合評価）	令和４年 12 月～令和６年３月	アマノ㈱	
3	次期人事給与システム保守及び運用支援業務	未定	令和６年４月１日～令和７年３月 31 日	未定	
4	次期人事給与システム基板設計・導入及び運用保守業務	一般競争入札（政府調達）	令和５年３月 27 日～令和 10 年 12 月 31 日	ユニアデックス㈱	
5	勤怠管理システム保守及び運用支援業務	未定	令和６年２月１日～令和７年３月 31 日	未定	

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を参照の上、以下に関し必要な作業を受託者の責任において適切に実施すること。これ以外の内容についても実施する必要が生じた場合は、PMDA と協議のうえ適宜実施すること。また作業に当たっては別紙「システム運用管理手順」を参照すること。

①　各種問い合わせ対応

PMDA からの使用方法や操作方法に関する電話やメール等での問い合わせに対し、迅速に対応すること。

また、サービス提供時間は平日 9 時 30 分～17 時 30 分とし、受け付けた問い合わせについてはインシデント管理をし、クローズするまで対応を実施すること。

②　脆弱性報告

月に一度、脆弱性を報告を行うこと。

③　ハードウェア保守対応

機器のハードウェアに障害が発生した場合、ハードウェア保守会社への保守依頼及び技術員の調整を行うこと。

④　ソフトウェア保守対応

サーバー機器の OS を含むソフトウェアについて、障害発生時に解決支援を行うこと。

⑤ 月次報告書作成

以下の資料を作成すること。

i. 脆弱性調査報告書
ii. インシデント一覧
iii. 変更作業一覧
iv. 特権 ID 使用管理台帳
v. 特権 ID 使用管理簿

⑥ 報告書・申請書作成

必要に応じ、以下の資料を作成すること。

i. インシデント報告書
ii. 変更作業申請書
iii. 特権 ID 使用申請書

（２） システム資産簿登録に係る作業

① PMDA においては、システムのインベントリ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。

② 受託者は PMDA が指定する以下の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

③ 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下記表に示す。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。

工程と成果物

項番	工程	納入成果物（注１）	納入期日
1	計画	保守運用業務実施計画書（保守範囲、体制表、作業分担、スケジュール、文書管理要領、セキュリティ管理要領、品質管理要領、変更管理要領、WBS 等） ・情報セキュリティ管理計画書（注２）	契約締結日から２週間以内
2	運用	・操作手順書 ・保守計画書 ・保守手順書 ・運用支援要員業務マニュアル ・その他システム関連ドキュメント（パッチの適用や障害対応、軽微な改修等に より追加・変更した設計書、操作マニュアル等を必要に応じて提出すること） ・プログラム・ツール等 ・使用した開発用データ	令和６年３月 31 日（※PMDA が求めた際は必要に応じて随時提出すること）
3	その他	・打合せ資料 ・議事録 ・障害等作業記録	令和６年３月 31 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 情報セキュリティ管理計画書には、ISMS 等認証取得、情報管理に関するルール（社内規程明示等）、情報管理体制、情報セキュリティインシデント対処方法、PMDA 情報の取扱い（目的外使用・意図しない変更を防止する方法を含む）、メンバーのスキル・資格・国籍等、自主点検の実施、業務環境のセキュリティ、レポート体制、再委託による履行保証措置、緊急連絡方法、教育・研修の実施等を記載

② 納品方法

表「工程と成果物」を含む全ての納入成果物を各納入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　文書を外部電磁的記録媒体（CD-R, DVD-R, BD-R 等)により日本語で提供すること。なお、紙媒体による提供は不要である。
イ　磁気媒体等に保存するファイルの形式は、PDF 形式及び Microsoft 365 で扱える形式とする。ただし、PMDA が別に形式を定めて提出を求めた場合は、この限りではない。
ウ　磁気媒体については二部ずつ用意すること。
エ　一般に市販されているツール、パッケージ類の使用は PMDA と協議の上、必要であれば使用を認めることとするが、特定ベンダーに依存する（著作権、著作者人格 権を有する）ツール等は極力使用しないこと。
オ　本業務で使用した開発ツール等の使用開始後５年間分のライセンス及びメディアを納入すること。
カ　本業務を実施する上で必要となる一切の機器物品等は、受託者の責任で手配すると ともに、費用を負担すること。
キ　各工程の中間成果物も含め、本業務に係る全ての資料を納品すること。

③　納品場所

独立行政法人　医薬品医療機器総合機構　総務部職員課

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を参照し、本業務に求められる各要件を満たすこと。要件に関するその他資料は「12　附属文書」のとおりである。受託者は、これらの資料を横断的に参照して、各要件を満たすように作業を実施すること。

５　作業の実施体制・方法に関する事項

（１）　作業実施体制

①　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、運用保守体制を 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。
②　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。
③　運用保守を複数業者が連携（再委託を含めて）して実施する等の場合は、参画する各業者の役割分担等を明示すること。

（２）　管理体制

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

② 本情報システムに 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。

（３） 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

※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）

D) 日本語による「円滑な意思疎通」が図れること

E) 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。

F) PMDA の社会的役割、本システムの役割（人事・給与・研修、労務管理等業務を持続的に、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、労務管理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) PMDA にて人事給与システムの基盤の設計書等を閲覧し、内容を十分理解していること。閲覧要領については別紙５参照。
E) 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)）、テクニカルエンジニア（情報セキュリティ）、情報処理安全確保支援士のいずれかの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。
F) 日本語による「円滑な意思疎通」が図れること
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。

（４） 作業場所

① 受託業務の作業場所（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 受託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。

（５） 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、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、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。

※受託者のみが権利を有する排他的な独自技術や開発フレームワーク等を採用しないこと

（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、本受託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。

- 受託業務完了後、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。

（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、次の文書に記載された事項を遵守すること。遵守する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」は非公表であるが、「政府機関等のサイバーセキュリティ対策のための統一基準群」に準拠しているので、必要に応じ参照すること。セキュリティポリシーの開示については、契約締結後、受託者が担当職員に「秘密保持等に関する誓約書」を提出した際に開示する。

②　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。

③　民法、刑法、著作権法、不正アクセス禁止法、個人情報保護法等の関連法規を遵守することはもとより、下記の PMDA 内規程を遵守すること。

- 独立行政法人 医薬品医療機器総合機構 情報システム管理利用規程
- 独立行政法人 医薬品医療機器総合機構 個人情報管理規程

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、受託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、受託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（日本工業標準）に従い、また個人情報を取り扱う場合には JISQ15001（日本工業標準）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、受託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、受託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 作業の実施内容に関する事項　(3)成果物の範囲、納品期日等　①成果物」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。ただし②、③についてはどちらかを取得していればよいものとする。

① 管理責任部署は 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 プライバシーマーク付与認定を取得していること。

④ 本調達公告期間中に、次期人事給与システム基盤の設計書・運用手順書等を閲覧し、内容を十分理解していること。閲覧要領については別紙５を参照。

⑤ 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

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

① 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。PMDA から提供する情報、もしくは本業務で知り得た情報の目的外利用を禁止すること。
② 受託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り、PMDA 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。
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、PMDA 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、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 の承認を受けたうえで実施すること。
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、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。

⑨ 本業務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、PMDA の承認を受けること。

⑩ 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。

⑪ 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。

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 PMDA に報告すること。

（２） 情報セキュリティ監査の実施

① 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。

② 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。

③ 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。

④ 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。

⑤ 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） 再委託の制限及び再委託を認める場合の条件

① 受託者は、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。主要部分とは実施計画及び業務報告を指す。

② 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。

③ 受託者は、本業務の実施中に再委託先又は再委託先の要員を変更する場合は、上記項記載の要領で申請し、承認を受けること。

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。

- 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、更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

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。

１２ 附属文書

（１） 調達仕様書 別紙

別紙 1 作業スケジュール
別紙 2 業務要件
別紙 3 システム構成図
別紙 4 可用性要件
別紙 5 資料閲覧要領
別紙 6 システム運用管理基準

（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 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 システム操作手順書

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 恒石

電話：03 -3506-9502 メールアドレス tsuneishi-miyuki●pmda.go.jp

（●を@に変える）

以 上

【別紙1】作業スケジュール

No	セキュリティ対策	実施区分	R5	R6												R7			実施内容
			12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	
マイルストーン																			
1-1	キックオフ	実施 ◎		▲			別途契約予定												実施計画書に基づくキックオフを実施
1-2	月次定例	実施 ◎			▲	▲													必要に応じて
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													「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													「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													「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													「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													「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													⇒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
権限管理																			
3-1	特権ID検証（棚卸し）	実施 ◎																	【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
点検																			
4-1	情報資産棚卸し・リスク評価	支援 △																	⇒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
4-2	システム台帳の最新化	支援 △																	⇒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。
4-3	ログ取得状況の点検	支援 △																	⇒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。
4-4	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 △																	
4-5	情報セキュリティ：遵守状況の自己点検	実施 ○																	「システム運用標準」 ⇒情報セキュリティ：遵守状況の報告
4-6	情報システム開発・運用資料確認	実施 ○																	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																			
5-1	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 ◎																	⇒令和元年度の実施手順を参考に対象システムを選定の上、PMDA内部検査を実施

別紙2 「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 1 月 1 日 ～令和 6 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、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。	9:30～17:30 ※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】	人事給与システム及び人事給与システム基盤（以下本システム）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。 本システムに係る監視項目、監視方式は Zabbix で行うが、詳細は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、人事給与システム基盤上の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】	本システムを構成する機器及びソフトウェアに設定されたジョブスケジュールについて、運用上支障が発生する場合にスケジュールの変更をPMDAに提案し、PMDAの了解の下、当該作業を実施すること。
7	【システム設定・操作 －	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）

No	名称	内容
	容量・能力管理】	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	【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。
9	【ユーザー管理】	① PMDA が承認したユーザ登録・削除依頼に基づき、OS 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。
10	【サービスレベル管理】	別紙4 「可用性要件」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4「可用性要件」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。
11	【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、実際の障害時は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4「可用性要件」を参照。

No	名称	内容
12	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 ➢ 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
13	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(緊急オペレーション含む。) 障害対応(復旧と事後対策含む。) 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	本システムを構成する機器等を維持するために、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。
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】	本システムを正常に稼動させるために本システム構成物の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 本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) 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。
		(4) 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。
		(5)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

No	名称	内容
		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。障害時のハードウェア保守交換、製品ログを送付しての調査、人事給与システム基盤ソフトウェアの仕様確認等は製品ベンダー等へに行うことができる。

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 X_システム構成図」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、必要に応じ月次会議を開催し、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。

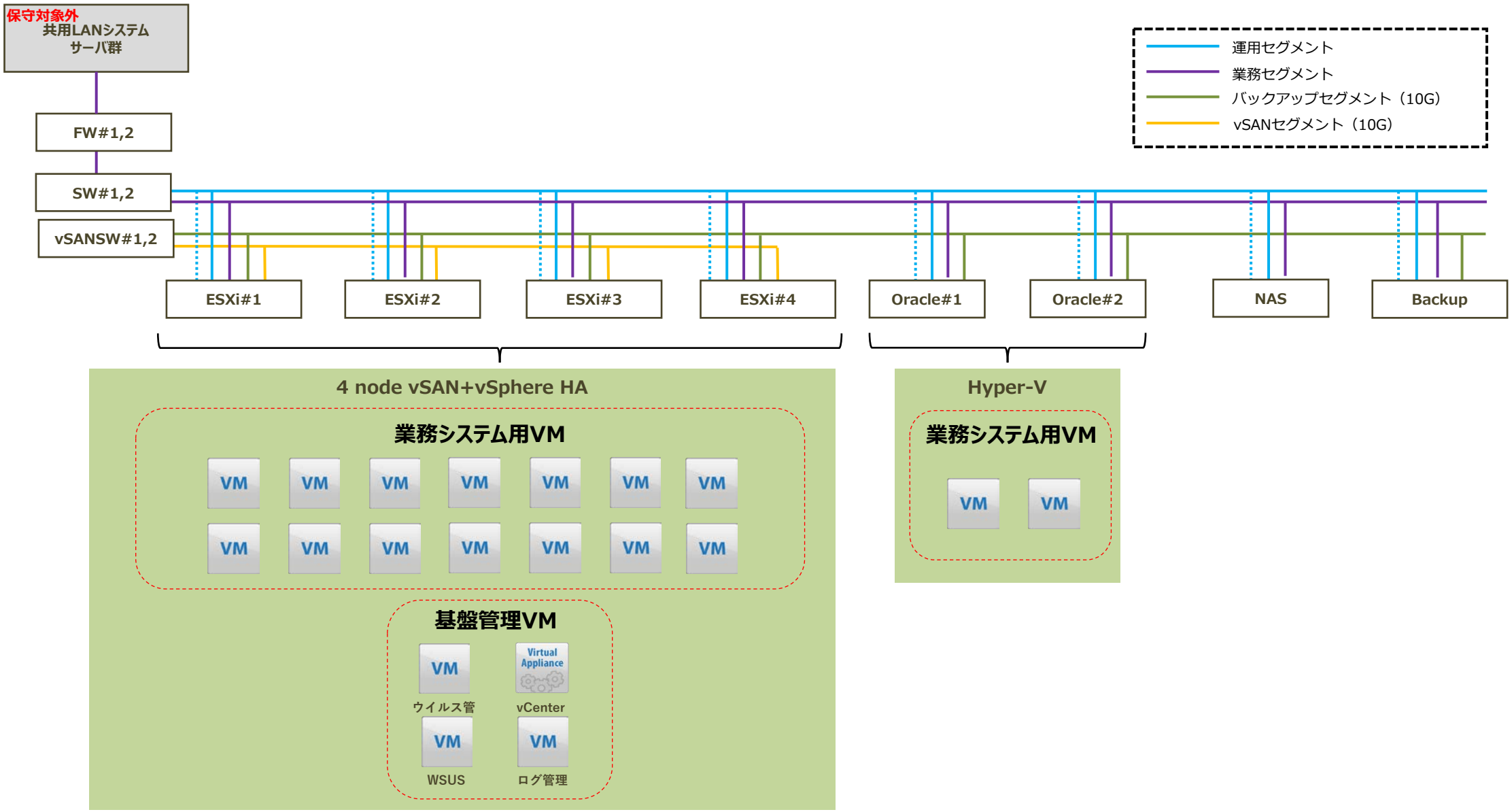
（イ）文書管理

- 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_システム構成図


保守対象外
共用LANシステム
サーバ群
FW#1,2
SW#1,2
vSANSW#1,2
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）
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
vCenter
WSUS
ログ管理
Hyper-V
業務システム用VM

可用性要件

人事給与システム基盤及び OS 運用に求められるサービスレベル

No.	SL 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	原則 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：9:30～17：30 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	99%

		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 ・ PMDA 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	
4	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、PMDA 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	原則 5 秒以内
5	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：直近のバックアップ時点 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

6	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）	目安として データの障害：6 時間以内 大規模災害時：数か月以内

別紙５

資料閲覧要領

1. 閲覧場所

独立行政法人 医薬品医療機器総合機構　会議室

2. 閲覧期間

令和５年 11 月 22 日から令和５年 12 月８日までの平日、10 時から 17 時まで

3. 申し込み方法

(1) 4.の連絡先に以下の事項を連絡すること。

会社名、部署名、担当者氏名、連絡先電話番号・メールアドレス、
閲覧希望時（第二希望まで)、所要時間、来訪人数

(2) 日時確定後 PMDA より「秘密保持誓約書様式」を担当者へ送付するので、閲覧当日までに必要事項を記入し PDF 形式で提出すること。

4. 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　恒石

tsuneishi-miyuki●pmda.go.jp　（●を@に変える）

電話　03-3506-9502

別紙6

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」

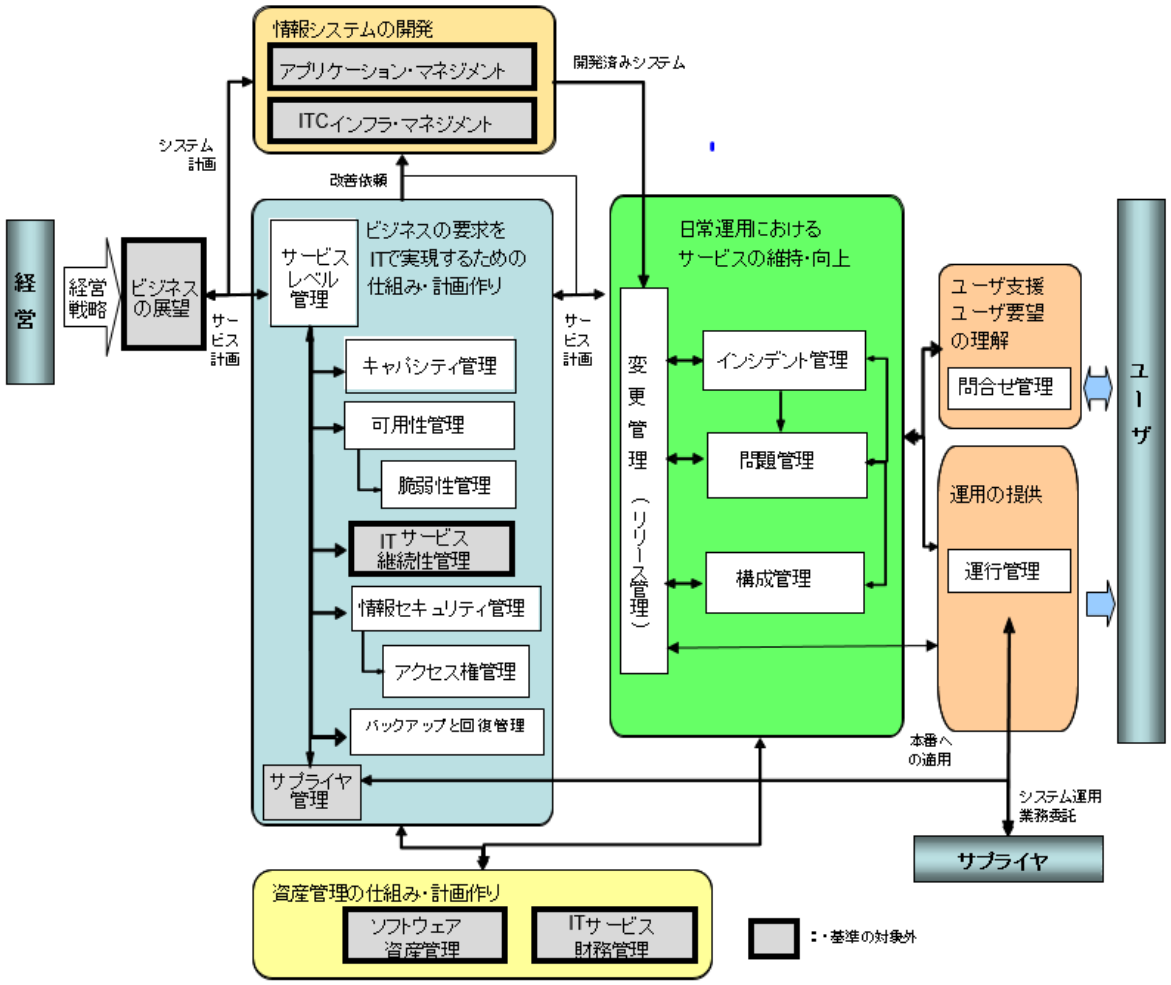
2. システム運用管理業務の概要

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

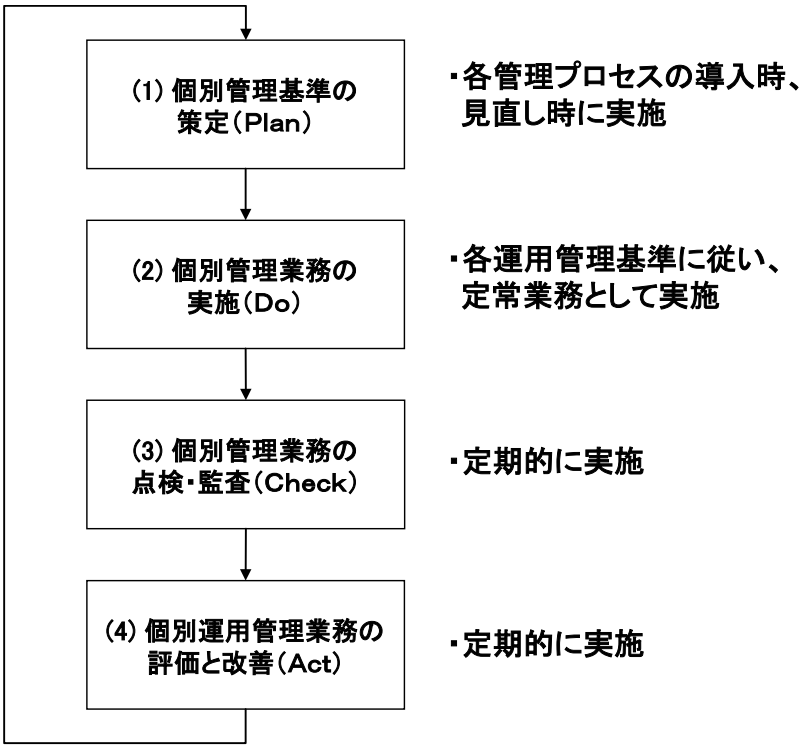


3. 運用管理業務の基本プロセス

（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