勤務管理システム保守及び運用支援業務

令和５年１２月
独立行政法人 医薬品医療機器総合機構

１　調達案件の概要に関する事項

（１）調達件名

勤務管理システム保守及び運用支援業務

（２）調達の目的及ぶ期待する効果

勤務管理システム保守及び運用支援業務（以下、「本業務」という。）は、勤務管理システムが日々安定的に稼働し、独立行政法人医薬品医療機器総合機構（以下「ＰＭＤＡ」という。）にとって常に有用かつ安全なシステムであり続けるよう適切な状態を維持すること、また万が一の障害等に対する予防策及びその早期復旧を行うことを目的とし、ソフトウェア保守及び運用支援を委託するものである。

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	補足
１	勤務管理システムの構築業務	一般競争入札 （総合評価落札方式）	令和４年１２月１日 ～令和６年３月３１日	
２	次期人事給与システム構築業務	一般競争入札 （総合評価落札方式）	令和４年４月１日 ～令和６年３月３１日	
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	
４	次期人事給与システム基盤設計・導入及び運用保守業務	一般競争入札 （最低価格落札方式）	令和５年３月２７日～ 令和１０年１２月３１日	
５	次期人事給与システムの基盤及びＯＳ運用保守業務	一般競争入札 （最低価格落札方式）	令和６年１月１日～ 令和６年３月３１日	

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。ＰＭＤＡ、受託者、別途ＰＭＤＡにて構築する人事給与システム保守事業者との役割分担については、別紙１「勤務管理システム関係作業・保守役割分担表」を参照すること。

（ｉ）ソフトウェア製品サポート

業務システムの開発には以下のパッケージソフトウェアを活用し構築されており、パッケージソフトウェア標準仕様に係るサポートにおいては委託者の負担において実施することとする。

業務システムソフトウェア

メーカー	アマノ株式会社
ソフトウェア	TimePro-VG 就業一式

①改善対応

パッケージソフトウェア標準仕様（パッケージベースモジュール）の障害対策やバージョンアップのモジュールの提供

②稼働環境変化への対策

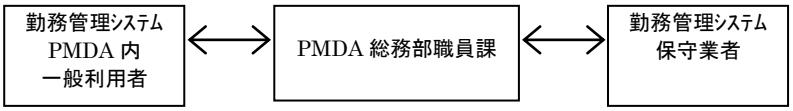
Windows Update やセキュリティパッチ等、対応 OS（環境）で問題が生じた場合、パッケージソフトウェア標準仕様（パッケージベースモジュール）の調査と対応

（ⅱ）各種問い合わせ対応

PMDA 総務部職員課からの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。

① 各種問い合わせに関する一次対応
② 各種問い合わせに関する調査の実施と回答
③ 一次切り分けと必要に応じてエスカレーションの実施
④ 保守要員の手配
等

問い合わせの対応経路は、以下の通り。



その他情報システム部門からの質疑に対し、電話やメール等での問い合わせ対応を随時行うこと。

（ⅲ）障害対応

勤務管理システムにて発生した障害に対し迅速に対応を行うこと。

① 障害発生原因及び影響範囲の調査
② 監視ログの解析と報告
③ 対策検討等の実施と報告
④ 障害対応状況と結果の報告
⑤ 復旧作業または、復旧支援
⑥ 障害メール対応

夜間または休日において運用管理システムより障害通知メールが発せられた場合は、受託者の翌営業日中に連絡し、対応を行うこと。

その他、機構内ネットワークの障害に関しては、基本的に切り分け作業までとし、必要に応じてＰＭＤＡの指示に基づき作業支援を実施すること。

また、ディスク障害に伴う業務システム復旧作業は、ＰＭＤＡにて取得しているバックアップ媒体とＰＭＤＡ側で準備する復旧手順書を元に、復旧作業を行うこと。

（ⅳ）運用課題管理・検討作業

勤務管理システムにて発生した課題に対しては適切に対応を行うこと。

① 発生した課題に対する影響調査や対応策の検討

② 仕様変更や機能追加に対する影響調査や対応策の検討

（ⅴ）ソフトウェア改修作業

制度改正や運用変更に伴う改修作業として、以下の内容について必要に応じて実施すること。

① 制度変更によるソフトウェア改修作業（TimePro-VG 就業）

② 簡易な仕様変更及び機能追加等のソフトウェア改修作業

③ ウイルス対策ソフトバージョンアップに伴う改修作業

④ セキュリティパッチ適用作業

⑤ ソフトウェアの障害に起因する改修作業

また、上記①～⑤の作業に付随する次の作業も委託業務の範囲とする。

⑥ ソフトウェア改修に関する機能仕様変更書の作成

⑦ ソフトウェア改修に関するテストの実施及び確認

⑧ ソフトウェア改修作業に関するＰＭＤＡ受入試験の支援

⑨ 処理結果の確認と報告

⑩ 運用スケジュールの変更支援

⑪ 運用ドキュメント（TimePro-VG 就業操作マニュアル等）の改訂作業

（ⅵ）品質管理・プロジェクト管理

上記全ての実施状況及び課題について管理と報告を実施すること。

①保守計画の立案

契約後、速やかに作成しＰＭＤＡへ説明

②保守及び運用支援全体の管理

月間での進捗状況や課題の管理

③インシデント管理

④変更管理

⑤特権 ID 管理

⑥構成管理

⑦月次報告書の提出

１回／月で、問合せ実績、インシデント管理、変更管理、特権 ID 管理、キャパシティ管理、Windows ログ解析報告等について報告

（ⅶ）システム資産簿登録に係る作業

① ＰＭＤＡにおいては、システム構成情報を一元管理するシステム資産簿を作成している。受託者は、本システムで利用する機器、ソフトウェア、ネットワーク等の構成情報をＰＭＤＡへ報告し、一元管理するシステム資産簿の管理情報について常に最新の状態を保つこと。

② 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、ＰＭＤＡが指定するシステム資産簿登録用シートを、ＰＭＤＡが指示する時期に提出すること。

（ア） 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ＰＭＤＡが指定する項目

＜補足＞

○ＰＭＤＡ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

○ＰＭＤＡ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

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、対応者等を記録し、一元管理を行うこと。

（２）委託期間

令和６年２月１日～令和７年３月３１日

４　作業の実施体制・方法に関する事項

（１）作業の実施に関する基本的な考え

本調達業務に関しては、非常駐保守を原則とし、４（２）に定める保守業務における連絡時間帯において受託者は連絡を受けることを可能とすること。保守作業時間については４（３）に定める。

・受託者は保守担当者、責任者の体制を提示し、ＰＭＤＡからの問い合わせ先を明確にすること。
・３（１）（ｖ）「ソフトウェア改修作業」①、②及び⑥～⑪関しては、TimePro-VG 就業に対し委託期間工数としてＳＥ２０人日を前提としており、改修案件の発生時に工数計画を作成・更新し、ＰＭＤＡと協議して承認を得た後に保守改修を行うこととする。
工数が前提より増加する場合は、別途差額分に対し追加契約をするものとする。

（２）保守作業における連絡時間帯

受託者と連絡可能な時間帯は、土日祝日および受託者の定める休業日を除き、月曜日から金曜日まで以下の時間帯とする。

通常保守　　９：００～１７：００（１２：００～１３：００除く）

（３）保守作業の実施時間帯

保守作業については、特定の指示のない限り、土日祝日およびＰＭＤＡの認める休業日を除き、月曜日から金曜日まで以下の時間帯とする。

通常保守　　９：００～１７：００（１２：００～１３：００除く）

なお、本番運用に影響を与えると思われる場合は、ＰＭＤＡと協議のうえ、受託者営業時間帯で可能な限り最短で対応を行うよう調整に努めること。

（４）保守作業場所

保守対象となるサーバ機器等、保守環境及び開発環境の端末設置場所を以下に示す。

ＰＭＤＡ内所定の場所（作業場所については、７（３）も参照）

５　成果物の範囲、納品期日等

（１）成果物

納品物件を以下に示す。電子データにて各１部とする。

ソフトウェアモジュールについては、本番環境及び保守環境のサーバに格納した状態とし、「完了報告書」によりその納品完了を確認する。

表１

成果物		提出時期
保守及び運用支援計画書	全体（年間）計画書	契約開始前
月次報告書	問合せ実績・課題進捗状況一覧	月次レポート提出
	インシデント管理一覧	
	変更管理一覧	
	特権 ID 管理一覧	
	次月以降の作業予定報告資料	
保守作業に伴う成果物	作業報告書	保守作業時（都度）
改修に伴う成果物	仕様確定書	改修時（都度）
	操作マニュアル（改版時のみ）	

（２）納品方法

表１の納入成果物を含む全ての納入成果物を令和７年３月３１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、日本工業規格（ＪＩＳ）の規定に準拠すること。

エ　受託者は、指定のドキュメントを外部電磁的記録媒体（ＣＤ‐Ｒ等)により納品すること。また、ＰＭＤＡが要求する場合は紙媒体でも納品すること。紙媒体の納品部数については、ＰＭＤＡと協議すること。ただし、ソフトウェア、ソースコード等は外部電磁的記録媒体（ＣＤ‐Ｒ等）のみとする。

オ　紙媒体のサイズは、日本工業規格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MicrosoftWord２０１６、同Excel２０１６、同 PowerPoint２０１６で読み込み可能な形式及びＰＤＦ形式とすること。ただし、ＰＭＤＡが他の形式による提出を求めた場合は、これに応じること。なお、受託者側で他の形式を用いて提出したいファイルがある場合は、協議に応じるものとする。

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

ク　外部電磁的記録媒体は、２部納品すること。

ケ　納品後、ＰＭＤＡにおいて改変が可能となるよう、図表等の元データも併せて納品すること。

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

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

シ　外部電磁的記録媒体により納品する場合は、不正プログラム対策ソフトウェアによる確認を行う等して、成果物に不正プログラムが混入することのないよう、適切に対処すること。

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

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

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

（３）納品場所

納品場所：独立行政法人医薬品医療機器総合機構　総務部

ただし、ＰＭＤＡが納品場所を別途指示する場合はこの限りではない。

6　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 システム運用管理基準
○ 別紙５ 情報セキュリティ対策の運用要件
○ 閲覧資料 情報セキュリティインシデント対処手順書
　　セキュリティ管理要件書(ひな型)

7 作業の実施体制・方法に関する事項

（１） 作業実施体制

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

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

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

③ 当該管理体制を確認する際の参照情報として、資本関係・役員等の情報、本業務の実施場所、本業務従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供を行うこと。具体的な情報提供内容についてはＰＭＤＡと協議の上、決定するものとする。

④ 受託者は、ＰＭＤＡ側やその他関連事業者を含めた全体の体制・役割を示した上で、プロジェクトの推進体制及び本件受託者に求める作業実施体制をＰＭＤＡと協議の上定めること。また、受託者の情報セキュリティ対策の管理体制については、作業実施体制とは別に作成すること。

⑤ 受託者は、インシデント発生時などの連絡体制図をＰＭＤＡと協議の上定めること。

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

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

（２） 作業要員に求める資格等の要件

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

① 運用責任者･リーダの必要スキル

Ａ） システム運用保守業務経験が 10 年以上
Ｂ） システム運用保守業務のマネジメント経験が 3 年以上
Ｃ） PMP 又は、情報処理技術者(プロジェクトマネージャ)資格 ※

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

D） 日本語による「円滑な意思疎通」が図れること

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

F） 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。

G） ＰＭＤＡの社会的役割、本システムの役割（人事・給与、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、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こと。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こと。

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

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

E） TimePro-VG 就業での勤務管理関連の業務を理解しており、本業務システムの設計にあたり、ＰＭＤＡに逐次業務の説明を求めることなく担当者とスムーズな会話ができる 知識を有していること。

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（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。 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。

【ＰＭＤＡの労務管理等業務に係る諸規程】

1　独立行政法人医薬品医療機器総合機構職員就業規則
2　独立行政法人医薬品医療機器総合機構事務補助員就業規則
3　独立行政法人医薬品医療機器総合機構嘱託就業規則
4　独立行政法人医薬品医療機器総合機構継続雇用職員就業規則
5　独立行政法人医薬品医療機器総合機構任期付特任職員就業規則
6　独立行政法人医薬品医療機器総合機構継続雇用事務補助員就業規則
7　独立行政法人医薬品医療機器総合機構役員給与規程
8　独立行政法人医薬品医療機器総合機構役員給与規程の実施細則
9　独立行政法人医薬品医療機器総合機構職員給与規程
10　独立行政法人医薬品医療機器総合機構職員給与規程の実施細則
11　独立行政法人医薬品医療機器総合機構役員退職手当支給規程
12　独立行政法人医薬品医療機器総合機構職員退職手当支給規程
13　独立行政法人医薬品医療機器総合機構人事評価規程の実施細則
14　独立行政法人医薬品医療機器総合機構在外職員の給与等に関する規程
15　独立行政法人医薬品医療機器総合機構在外職員の給与等に関する実施細則
16　独立行政法人医薬品医療機器総合機構事務補助員の賞与係数及び勤務日数に基づく期間率に関する実施細則
17　独立行政法人医薬品医療機器総合機構嘱託等の賞与係数及び勤務日数に基づく期間率に関する実施細則
18　独立行政法人医薬品医療機器総合機構におけるテレワーク勤務に関する規程

（３）　作業場所

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

（４）　作業の管理に関する要領

① 受託者は、ＰＭＤＡの指示に従って運用業務に係るコミュニケーション管理、体制管理、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。

8 作業の実施に当たっての遵守事項

（1） 基本事項 受託者は、次に掲げる事項を遵守すること。

① 本業務の遂行に当たり、業務の継続を第一に考え、善良な管理者の注意義務をもって誠実に行うこと。

② 本業務に従事する要員は、ＰＭＤＡと日本語により円滑なコミュニケーションを行う能力と意思を有していること。

③ 本業務の履行場所を他の目的のために使用しないこと。

④ 本業務に従事する要員は、履行場所での所定の名札の着用等、従事に関する所定の規則に従うこと。

⑤ 要員の資質、規律保持、風紀及び衛生・健康に関すること等の人事管理並びに要員の責めに起因して発生した火災・盗難等不祥事が発生した場合の一切の責任を負うこと。

⑥ 受託者は、本業務の履行に際し、ＰＭＤＡからの質問、検査及び資料の提示等の指示に応じること。また、修正及び改善要求があった場合には、別途協議の場を設けて対応すること。

⑦ 次回の本業務調達に向けた現状調査、ＰＭＤＡが依頼する技術的支援に対する回答、助言を行うこと。

⑧ 本業務においては、業務終了後の運用等を、受託者によらずこれを行うことが可能となるよう詳細にドキュメント類の整備を行うこと。

（2） 機密保持、資料の取扱い

本業務を実施する上で必要とされる機密保持に係る条件は、以下のとおり。

① 受託者は、受注業務の実施の過程でＰＭＤＡが開示した情報（公知の情報を除く。以下同じ。）、他の受託者が提示した情報及び受託者が作成した情報を、本受注業務の目 的以外に使用又は第三者に開示若しくは漏洩してはならないものとし、そのために必要な措置を講ずること。

② 受託者は、本受注業務を実施するにあたり、ＰＭＤＡから入手した資料等については管理簿等により適切に管理し、かつ、以下の事項に従うこと。

- 複製しないこと。
- 用務に必要がなくなり次第、速やかにＰＭＤＡに返却又は消去すること。
- 受注業務完了後、上記①に記載される情報を削除又は返却し、受託者において該 当情報を保持しないことを誓約する旨の書類をＰＭＤＡに提出すること。

③ 応札希望者についても上記①及び②に準ずること。

④ 「独立行政法人 医薬品医療機器総合機構 情報システム管理利用規程」の第 52 条に従うこと。

⑤ 「秘密保持等に関する誓約書」を別途提出し、これを遵守しなければならない。

⑥ 機密保持の期間は、当該情報が公知の情報になるまでの期間とする。

（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、「政府機関等の情報セキュリティ対策のための統一基準（最新版）」に準拠しているので、必要に応じ参照すること。「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、見積りを提出した事業者のうち、事業者がＰＭＤＡに「秘密保持等に関する誓約書」を提出した際に開示する。

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

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

9 成果物の取扱いに関する事項

（1） 知的財産権の帰属 知的財産の帰属は、以下のとおり。

① 本件に係り作成・変更・更新されるドキュメント類及びプログラムの著作権（著作権法第 21 条から第 28 条に定めるすべての権利を含む。）は、受託者が本件のシステム開発の従前より権利を保有していた等の明確な理由により、あらかじめ書面にて権利譲渡不可能と示されたもの以外、ＰＭＤＡが所有する等現有資産を移行等して発生した権利を含めてすべてＰＭＤＡに帰属するものとする。

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

③ 本件に係り発生した権利については、今後、二次的著作物が作成された場合等であっても、受託者は原著作物の著作権者としての権利を行使しないものとする。

④ 本件に係り作成・変更・修正されるドキュメント類及びプログラム等に第三者が権利を有する著作物が含まれる場合、受託者は当該著作物の使用に必要な費用負担や使用許諾契約に係る一切の手続きを行うこと。この場合は事前にＰＭＤＡに報告し、承認を得ること。

⑤ 本件に係り第三者との間に著作権に係る権利侵害の紛争が生じた場合には、当該紛争

の原因が専らＰＭＤＡの責めに帰す場合を除き、受託者の責任、負担において一切を処 理すること。この場合、ＰＭＤＡは係る紛争の事実を知ったときは、受託者に通知し、 必要な範囲で訴訟上の防衛を受託者にゆだねる等の協力措置を講ずる。なお、受託者の著作又は一般に公開されている著作について、引用する場合は出典を明示するとともに、受託者の責任において著作者等の承認を得るものとし、ＰＭＤＡに提出する際は、その旨併せて報告するものとする。

（２） 契約不適合責任

① 委託業務の納入成果物に関して本システムの安定稼動等に関わる契約不適合の疑いが生じた場合であって、ＰＭＤＡが必要と認めた場合は、受注者は速やかに契約不適合の疑いに関して調査し回答すること。調査の結果、納入成果物に関して契約不適合等が認められた場合には、受注者の責任及び負担において速やかに修正を行うこと。なお、修正を実施する場合においては、修正方法等について、事前にＰＭＤＡの承認を得てから着手すると共に、修正結果等についてＰＭＤＡの承認を受けること。

② 受託者は、契約不適合責任を果たす上で必要な情報を整理し、その一覧をＰＭＤＡに提出すること。契約不適合責任の期間が終了するまで、それら情報が漏洩しないように、ISO/IEC27001 認証（国際標準）又は JISQ27001 認証（日本工業標準）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、受注者は消去完了を明記した証明書を作業ログとともにＰＭＤＡに対して提出すること。なお、データ消去作業に必要な機器等については、受注者の負担で用意すること。

（３） 検収

納入成果物については、適宜、ＰＭＤＡに進捗状況の報告を行うとともに、レビューを受けること。最終的な納入成果物については、「５（１）成果物」に記載のすべてが揃っていること及びレビュー後の改訂事項等が反映されていることを、ＰＭＤＡが確認し、これらが確認され次第、検収終了とする。 なお、以下についても遵守すること。

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

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

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

１０ 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 ISO9001 又は CMMI レベル 3 以上の認定を取得していること。

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

③ プライバシーマーク付与認定を取得していること。

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

⑤ 関連システムの設計書等を閲覧していること。

（２）入札制限

情報システムの調達の公平性を確保するために、以下に示す事業者は本調達に参加できない。

① ＰＭＤＡの CI0 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

１１ 情報セキュリティ管理

（１） 情報セキュリティ対策の実施

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

ア ＰＭＤＡから提供する情報の目的外利用を禁止すること。

イ 本業務の実施に当たり、受託者又はその従業員、本調達の役務内容の一部を再委託する先、若しくはその他の者による意図せざる変更が加えられないための管理体制が整備されていること。

ウ 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。

エ 情報セキュリティインシデントへの対処方法が確立されていること。

オ 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。

カ 情報セキュリティ対策の履行が不十分である場合、速やかに改善策を提出し、ＰＭＤＡの承認を受けた上で実施すること。

キ ＰＭＤＡが求めた場合に、速やかに情報セキュリティ監査を受入れること。

ク 本調達の役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に

対して情報セキュリティが十分に確保されるように情報セキュリティ管理計画書に記載された措置の実施を担保すること。

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

コ 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。

サ 本業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかにＰＭＤＡに報告すること。

（２） 情報セキュリティ監査の実施

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

イ 受託者は自ら実施した外部監査についてもＰＭＤＡへ報告すること。

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

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

オ 受託者は、指摘や進捗等把握のための資料提出依頼等があった場合は、ＰＭＤＡと協議の上、内容に沿って適切な対応を行うこと。 情報セキュリティ監査の実施については、本項に記載した内容を上回る措置を講ずることを妨げるものではない。

１２ 再委託に関する事項

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

② ①における「主要部分」とは、以下に掲げるものをいう。

ア 総合的企画、業務遂行管理、手法の決定及び技術的判断等。

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

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

ただし、以下の場合には再委託を可能とする。

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

③ 受託者は、再委託する場合、事前に再委託する業務、再委託先等をＰＭＤＡに申請し、

承認を受けること。申請にあたっては、「再委託に関する承認申請書」の書面を作成の上、受託者と再委託先との委託契約書の写し及び委託要領等の写しをＰＭＤＡに提出すること。受託者は、機密保持、知的財産権等に関して本仕様書が定める受託者の責務を再委託先業者も負うよう、必要な処置を実施し、ＰＭＤＡに報告し、承認を受けること。なお、第三者に再委託する場合は、その最終的な責任は受託者が負うこと。

④ 再委託先が「１０（２）入札制限」の要件を満たすこと。

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

⑥ 再委託先において、本調達仕様書に定める事項に関する義務違反、義務を怠った場合には、受託者が一切の責任を負うとともに、ＰＭＤＡは当該再委託先への再委託の中止を請求することができる。

⑦ 再委託における情報セキュリティ要件については以下のとおり。

・ 再委託先が「１１（１）情報セキュリティ対策の実施」の要件を満たすこと

・ ＰＭＤＡから提供する情報の目的外利用を禁止すること。

・ 受託者は再委託先における情報セキュリティ対策の実施内容を管理しＰＭＤＡに報告すること。

・ 受託者は業務の一部を委託する場合、本業務にて扱うデータ等について、再委託先またはその従業員、若しくはその他の者により意図せざる変更が加えられないための管理体制を整備し、ＰＭＤＡに報告すること。

・ 受託者は再委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関して、ＰＭＤＡから求めがあった場合には情報提供を行うこと。

・ 受託者は再委託先にて情報セキュリティインシデントが発生した場合の再委託先における対処方法を確認し、ＰＭＤＡに報告すること。

・ 受託者は、再委託先における情報セキュリティ対策、及びその他の契約の履行状況の確認方法を整備し、ＰＭＤＡへ報告すること。

・ 受託者は再委託先における情報セキュリティ対策の履行状況を定期的に確認すること。また、情報セキュリティ対策の履行が不十分な場合の対処方法を検討し、ＰＭＤＡへ報告すること。

・ 受託者は、情報セキュリティ監査を実施する場合、再委託先も対象とするものとする。

・ 受託者は、再委託先が自ら実施した外部監査についてもＰＭＤＡへ報告すること。

・ 受託者は、委託した業務の終了時に、再委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認すること。

⑧ 上記①～⑦について再委託先が、さらに再委託を行う場合も同様とする。

１３ 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。

１４ 附属文書

（１）調達仕様書 別紙

別紙１「勤務管理システム関係作業・保守役割分担表」
別紙２ 「システム構成図」
別紙３ 「資料の閲覧について」
別紙４ 「システム運用管理基準」
別紙５ 「情報セキュリティ対策の運用要件」

（２）事業者が閲覧できる資料一覧

閲覧資料１ 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 独立行政法人 医薬品医療機器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 システム設計書
閲覧資料５ 運用継続計画（情報システムＢＣＰ）

これら資料は、見積りを提出した事業者のうち、ＰＭＤＡに「秘密保持等に関する誓約書」を提出した事業者に対し、事業者から申出があれば、閲覧を認める。

１５ 窓口連絡先

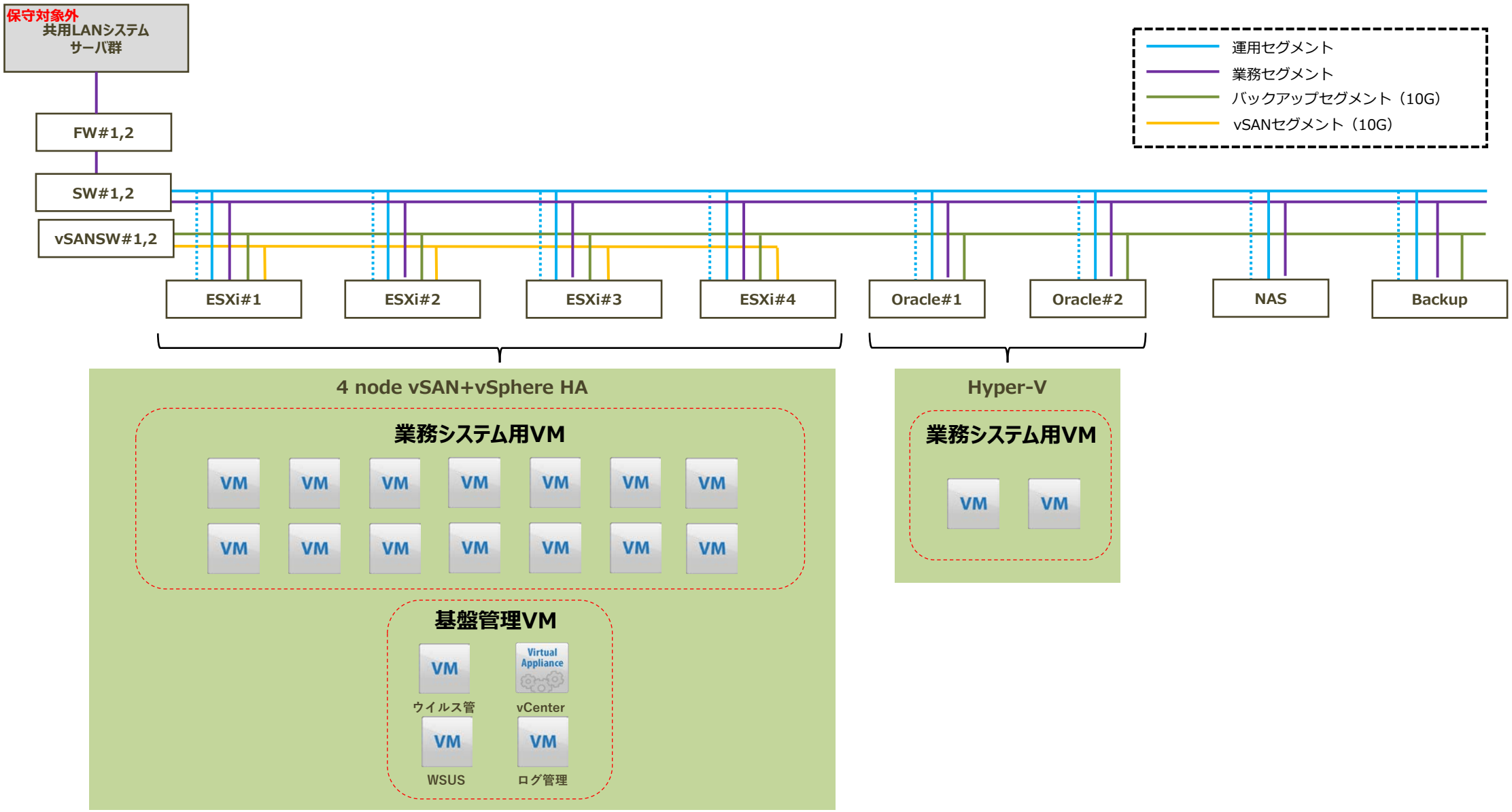
独立行政法人 医薬品医療機器総合機構
総務部職員課　 奈良 雄太
電話：03（3506）9502
E-mail： nara-yuta●pmda.go.jp
※ ●は@に置き換えてください

別紙１　勤務管理システム関係作業・保守役割分担表

項番	作業内容				作業実施者 ◎：主担当 ○：副担当 －：担当外		
	対象	概要		詳細	PMDA	人給保守	勤務管理保守
1	仮想基盤	設計		勤怠サーバが稼働する仮想基盤の設計	○	◎	－
2		構築		勤怠サーバが稼働する仮想基盤の構築	－	◎	－
3		設定変更		勤怠サーバが特定の仮想基盤ホストでのみ稼働するようアフィニティルールを設定	－	◎	－
4				勤怠サーバ用Windows NLBを機能させるための仮想スイッチの設定	－	◎	○
5		保守	問い合わせ		－	◎	－
6			設定変更	キャパシティ管理、キャパシティ拡張　／　月１回	－	○	◎
7			障害対応		－	◎	－
8			月次報告		－	◎	－
9	仮想マシン	設計		勤怠サーバ用仮想マシンの設計	○	◎	○
10				勤怠サーバ用仮想マシンの構築	－	◎	－
11		保守	問い合わせ		－	◎	－
12			バージョンアップ		－	◎	－
13			設定変更		－	◎	－
14			障害対応		－	◎	－
15			月次報告		－	◎	－
16	インフラ	保守	問い合わせ		◎	－	－
17			バージョンアップ		◎	－	－
18			設定変更		◎	－	－
19			障害対応		◎	－	－
20			月次報告		◎	－	－
21	TimePro－VG	保守	問い合わせ		－	－	◎
22			バージョンアップ		－	－	◎
23			設定変更		－	－	◎
24			障害対応		－	－	◎
25			月次報告		－	－	◎
26	OS	ライセンス準備		勤怠サーバ用Windows Serverライセンスの調達	－	－	◎
27				勤怠サーバ用Microsoft SQL Serverライセンスの調達	－	－	◎
28		OSインストール		勤怠サーバ用仮想マシンへWindow Serverをインストール	－	◎	－
29		OS基本設定		勤怠サーバのOS基本設定	－	◎	－
30		OS設定変更		勤怠サーバのOS設定変更	－	－	◎
31		SQLサーバ設定		勤怠サーバへMSSQLのインストール・設定	－	－	◎
32		NLB設定		勤怠サーバ（本番WEB）へWindows NLBの設定	－	－	◎
33		NLB試験		設定したWindows NLBの試験	－	○	◎
34		保守	問い合わせ	設定関連	－	－	◎
35			バージョンアップ	パッチ適用　１回／年	－	－	◎
36			設定変更		－	－	◎
37			障害対応		－	－	◎
38			月次報告		－	－	◎
39	監視	ライセンス準備		勤怠サーバ用Zabbixのライセンスの調達	◎	○	－
40		設計		勤怠サーバの監視の設計	◎	－	◎
41		構築		勤怠サーバの監視の設定（Zabbixサーバ）	－	－	◎
42				勤怠サーバの監視の設定（Zabbixエージェント）	－	○	◎
43		試験		勤怠サーバの監視の試験	◎	－	◎
44		保守	問い合わせ		－	－	◎
45			バージョンアップ	5年に1回	－	－	◎
46			設定変更		－	－	◎
47			障害対応		－	－	◎
48			月次報告		－	－	◎
49	バックアップ	ライセンス準備		勤怠サーバ用ArcserveUDPのライセンスの調達	◎	○	－
50		設計		勤怠サーバのバックアップの設計	○	◎	－
51		構築		勤怠サーバのバックアップの設定（ArcserveUDPサーバ）	－	◎	－
52				勤怠サーバのバックアップの設定（ArcserveUDPエージェント）	－	◎	－
53		試験		勤怠サーバのバックアップ・リストアの試験	－	－	◎
54		保守	問い合わせ		－	－	◎
55			バージョンアップ		－	－	◎
56			設定変更		－	－	◎
57			障害対応		－	－	◎
58			月次報告		－	－	◎

項番	作業内容				作業実施者 ◎：主担当 〇：副担当 －：担当外		
	対象	概要		詳細	PMDA	人給保守	勤務管理保守
59	ウィルス対策	ライセンス準備		勤怠サーバ用CloudOneのライセンスの調達	◎	〇	ー
60		設計		勤怠サーバのウィルス対策ソフトの設計	－	◎	ー
61		構築		勤怠サーバのウィルス対策ソフトの設定（CloudOneサーバ）	－	◎	ー
62				勤怠サーバのウィルス対策ソフトの設定（CloudOneエージェント）	－	◎	ー
63		試験		勤怠サーバのウィルス対策ソフトの試験	－	◎	ー
64		保守	問い合わせ		－	－	◎
65			バージョンアップ		－	－	◎
66			設定変更		－	－	◎
67			障害対応		－	－	◎
68			月次報告		－	－	◎
69	LoadRunner	ライセンス準備		勤怠サーバ用LoadRunnerのライセンスの調達	－	－	◎
70		テスト用PC準備		勤怠サーバの負荷テスト用クライアントPCの準備	◎	－	ー
71		負荷テスト		勤怠サーバの負荷テスト	－	－	◎
72		保守	問い合わせ		－	－	◎

別紙２_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
VM

別紙３　　資料の閲覧について

１．閲覧場所

独立行政法人 医薬品医療機器総合機構内

２．閲覧期間

令和５年 12 月 6 日（水）から令和５年 12 月 19 日（火）までの平日（10:00～17:00）

３．閲覧上の注意

(1) 閲覧に際しては４.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、
閲覧希望日時（第二希望まえ)、所要時間、来訪人数

(2) ２.閲覧期間の後半は閲覧場所を確保できなくなる場合があるので、早めに閲覧希望日時を登録すること。

(3) 閲覧日時確定後、PMDA より「秘密保持誓約書様式」を担当者へ送付するので、作成し、閲覧当日までに PMDA へ提出すること。

(4) 一回あたりの閲覧時間は 1 時間程度とする。閲覧回数は原則制限しない。

(5) 閲覧時に個々の内容に関する質問に応じることはできない。質問がある場合は、所定の手続きをとること。

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　　奈良 雄太
電話：03（3506）9502
E-mail：nara-yuta●pmda.go.jp

※ ●は@に置き換えてください。

別紙4

システム運用管理基準

2020 年 12 月

独立行政法人　医薬品医療機器総合機構

【資料の見方】

✧　システム運用業務を「１３の領域」に分けている。
それぞれの業務プロセスは、標準化対象外。各情報システムの体制･特性･リスク等により、最適なプロセスを設計し、運用する。

✧　システム運用の標準化（要件）は、システム運用者（委託先）から当機構への報告書式（情報提供も含む）を統一し、各システムの運用状況を定期的に収集して、全体状況の把握と情報共有等を可能とすることにある。

- 当資料においては「標準化」のタイトル等にて報告を記載している。
- 標準化（要件）は、「報告書式を統一する領域」と「報告内容を統一（書式任意）」の 2 タイプに分かれる。
- 「報告書式を統一する領域」は、インシデント管理、変更管理、構成管理、脆弱性管理、アクセス権管理の領域となっている。

1. はじめに

1．1　目的

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

1．2　対象範囲

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

1．3　適用の考え方

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

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

1．4　用語の定義

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

1．5　準拠および関連文書

上位規程　：「情報セキュリティポリシー」

関連文書　：「情報システム管理利用規程」

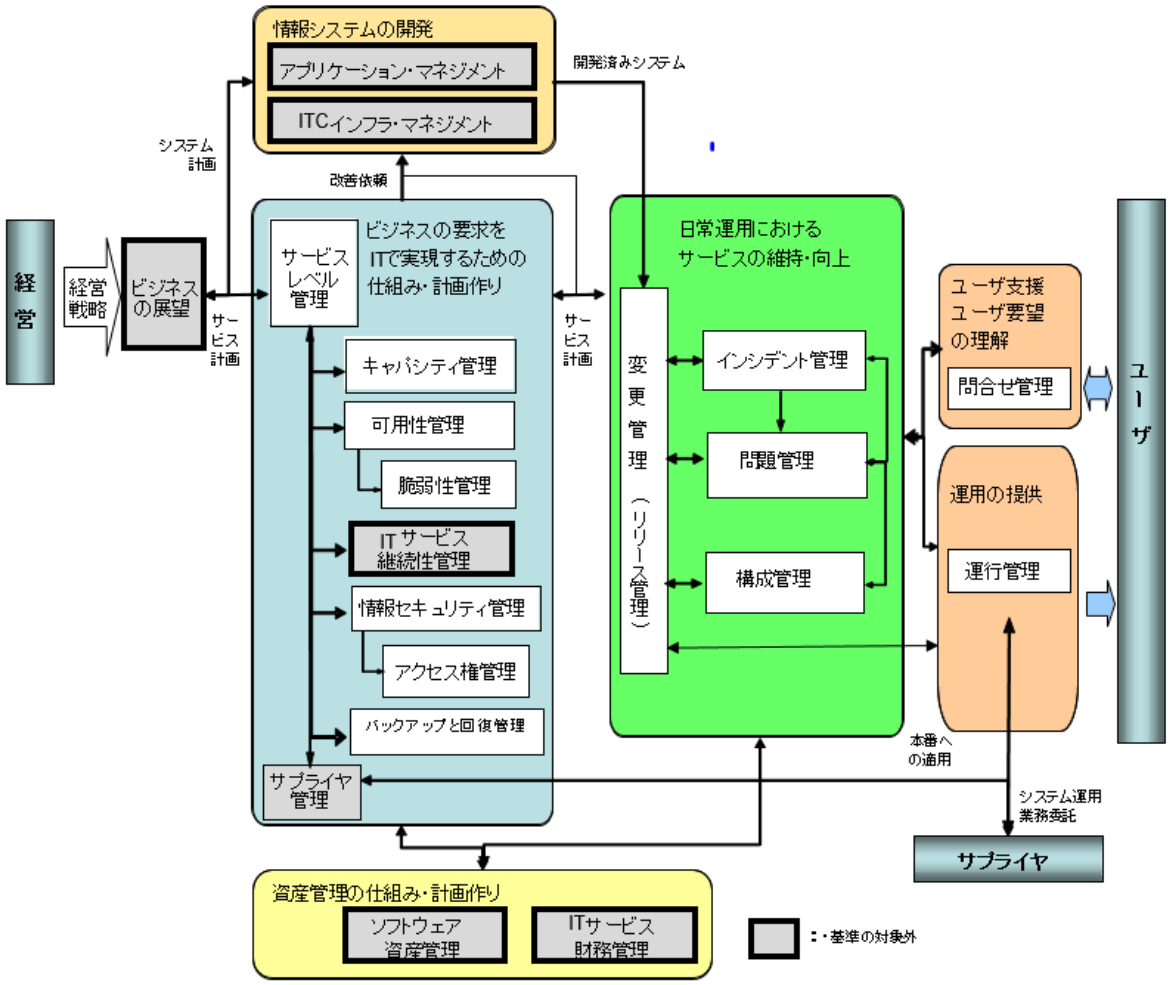
2. システム運用管理業務の概要

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

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

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

【参考】システム運用管理業務の全体像

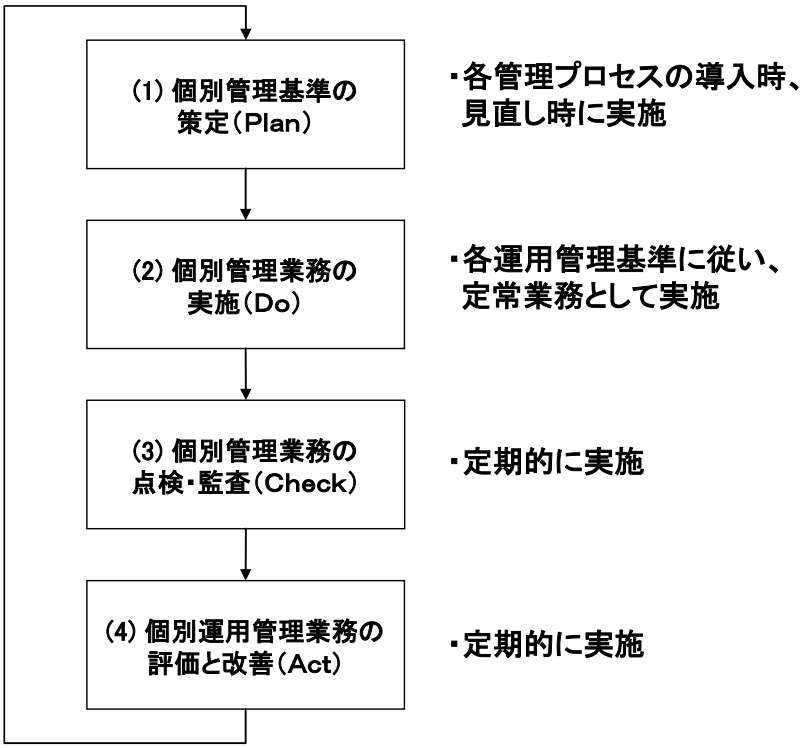


3. 運用管理業務の基本プロセス

（運用管理業務プロセスのPDCAマネジメントサイクル）

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

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



各基本プロセスの概要は、以下のとおりである。

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

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

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

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

4. システム運用管理業務の明確化・標準化

4. 1 問合せ管理

(1) 目的

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

(2) 業務の概要

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

(3) 管理対象

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

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

(4) 業務の管理指標＆標準化

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

①問合せ発生件数（日次集計・月次集計を含む）
②問合せ区分別件数
③問合せ一次回答期限遵守率
④問合せ完了率（一定期間経過後(10 営業日経過後)の完了率）

※報告内容は、各システムの状況に応じて変更しても構わない。

【補足】

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

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

４．２ インシデント管理

(1) 目的

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

(2) 業務の概要

①インシデントの定義

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

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

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

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

②インシデント管理の主な活動

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

インシデント管理のプロセスでは、主に次の活動を実施する。

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

(3) 管理対象

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

(4) 業務の管理指標

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

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

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

(5) 標準化

インシデント管理は、PMDA 標準書式を適用する。

①インシデント発生(判明)時

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

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

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

②定期的(月次)報告時

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

※添付「インシデント一覧」を使用する。

４．３ 問題管理（再発防止策）

(1) 目的

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

(2) 業務の概要

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

- ・問題の傾向分析と課題点の抽出
- ・是正策の検討
- ・是正策の実施

(3) 管理対象

本番システム環境で稼動している全てのシステムの問題を管理対象とする。

(4) 業務の管理指標＆標準化

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

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

※報告内容は、各システムの状況に応じて変更しても構わない。

４．４ 変更管理

(1) 目的

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

(2) 業務の概要

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

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

(3) 管理対象

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

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

(4) 業務の管理指標

変更管理業務を評価するための評価指標として以下を定義する。

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

(5) 標準化

変更管理は、PMDA 標準書式を適用する。

①変更案件発生時

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

※課題管理表の書式は、各情報システムの任意とする。

②変更実施着手時

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

※添付「変更作業申請書（ひな型）」を使用する。

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

認･承認欄の削除は認めない。

※個票は、「単純な定常作業」に関しては使用しなくても良い。

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

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

③定期的(月次)報告時

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

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

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

４．５ 構成管理

(1) 目的

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

(2) 業務の概要

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

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

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

(3) 管理対象

構成管理が対象とする構成情報は以下の通りとする。

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

(4) 業務の管理指標

構成管理業務を評価するための評価指標として以下を定義する。

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

(5) 標準化

〇PMDA では、「システム資産簿」を作成してシステムのインベントリ情報を一元管理している。各システムのインベントリ情報を各システムの実装状況を反映した最新状況に更新するとともに、「システム資産簿」を最新の状況に保つため、最新のインベントリ情報を PMDA 標準書式「システム資産簿登録用シート」を使用して、PMDA へ報告する。

４．６ 運行管理

(1) 目的

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

(2) 業務の概要

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

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

(3) 管理対象

本番システム環境で稼動している全ての情報システムの運行を管理対象とする。

(4) 業務の管理指標

運行管理業務を評価するための評価指標として以下を定義する。

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

(5) 標準化

〇情報システムの運行状況を報告する（月次）（書式任意）

情報システムの稼働状況に加えて、以下の項目の報告を必須とする。

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

４．７　バックアップと回復管理

(1)　目的

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

(2)　業務の概要

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

日常運用においては、バックアップ取得、バックアップ媒体の保管を行う。

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

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

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

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

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

(3)　管理対象

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

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

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

(4)　バックアップデータの保管方法

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

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

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

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

(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5　情報セキュリティ対策の運用要件

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

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

	セキュリティホール対策（AT-3）	運用時の脆弱性対策　（AT-3-2）	情報システムを構成するソフトウェア及びハードウェアのバージョン等を把握して、製品ベンダや脆弱性情報提供サイト等を通じて脆弱性の有無及び対策の状況を定期的に確認すること。脆弱性情報を確認した場合は情報システムへの影響を考慮した上でセキュリティパッチの適用等必要な対策を実施すること。 対策が適用されるまでの間にセキュリティ侵害が懸念される場合には、当該情報システムの停止やネットワーク環境の見直し等情報セキュリティを確保するための運用面での対策を講ずること。	脆弱性対策の実施状況は、月次で報告すること。
不正監視・追跡 （AU: Audit）	ログ管理（AU-1）	ログの蓄積・管理（AU-1-1）	情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログ（システムへのログオンや資源へのアクセスのロギング等）を取得すること。	ログが所定の要件通り、取得・蓄積されていることを確認すること。（年１回以上）
		ログの保護　（AU-1-2）	取得・蓄積されたログが不正な改ざんや削除が行われないようログの格納ファイルのアクセス権を制限する等必要な対策を講じること。	取得・蓄積されたログが不正な改ざんや削除が行われていなことを確認すること。（年１回以上）
		時刻の正確性確保（AU-1-3）	システム内の機器の時刻同期の状況を確認すること。	
	不正監視（AU-2）	侵入検知　（AU-2-1）	不正行為に迅速に対処するため、通信回線を介して所属するＰＭＤＡ外と送受信される通信内容を監視し、不正アクセスや不正侵入を検知した場合は通信の遮断等必要な対処を行うこと。	
アクセス・利用制限（AC: Access）	主体認証（AC-1）	主体認証　（AC-1-1）	主体認証情報（ＩＤ、パスワード）は不正に読み取りできないよう保護すること。	
	アカウント管理（AC-2）	ライフサイクル管理　（AC-2-1）	主体が用いるアカウント（識別コード、主体認証情報、権限等）は、主体の担当業務に必要な範囲において設定すること。 また、アカウント管理（登録、更新、停止、削除等）の作業内容は記録し、証跡を保管すること。 アカウント棚卸を定期的に実施し、不要なアカウントを削除すること。	アカウント棚卸を定期的（年１回以上）に実施すること。
		アクセス権管理（AC-2-2）	主体が用いるアカウント（識別コード、主体認証情報、権限等）は、主体の担当業務に必要な範囲において設定すること。また、アカウント管理（登録、更新、停止、削除等）の作業内容は記録し、証跡を保管すること。 権限の再検証を定期的に実施し、不要な権限を削除すること。	ユーザーＩＤの棚卸と合わせて実施すること。

		管理者権限の保護（AC-2-3）	システム特権を付与されたアカウント及び使用者を特定し、アカウントの使用状況を記録し、アカウントの不正使用がないことを定常的に確認すること。	管理状況を「特権ＩＤ台帳」及び「特権ＩＤ使用管理簿」により、月次で報告すること。
データ保護（PR: Protect）	機密性・完全性の確保（PR-1）	通信経路上の盗聴防止 （PR-1-1）	通信回線に対する盗聴行為による情報の漏えいを防止するため、通信回線を暗号化する機能について、有効に機能していることを定期的に確認すること。	セキュリティヘルスチェック（各種セキュリティ設定の不正変更の有無、および不正操作の痕跡の有無の確認）と合わせて実施し報告すること。
		保存情報の機密性確保 （PR-1-2）	情報システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限すること。構成情報と実際の設定を照合し、所定の要件通りに設定されていることを定期的に確認すること。 また、業務データへのアクセス権限の付与状況を点検し、不要なアクセス権限が付与されていないことを確認すること。	ユーザーＩＤの棚卸と合わせて実施すること。
		業務データへのアクセス管理	情報の格付の見直し及び再決定が行われた際や、当該情報システムに係る職員等の異動や職制変更等が生じた際には、情報に対するアクセス制御の設定や職務に応じて与えられている情報システム上の権限が適切に変更されていることを確認すること。	ユーザーＩＤの棚卸と合わせて実施すること。
		受託者によるアクセス	受託者は受託した業務以外の情報へアクセスしないこと。	情報セキュリティ遵守状況は月次で報告すること。
物理対策（PH: Physical）	情報窃取・侵入対策（PH-1）	情報の物理的保護（PH-1-1）	受託者の管理区域において、受託者がＰＭＤＡより提供された情報を格納する機器は、情報の漏えいを防止するため、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。	情報セキュリティ遵守状況は月次で報告すること。
		侵入の物理的対策（PH-1-2）	受託者の管理区域において、受託者がＰＭＤＡより提供された情報を格納する機器は、物理的な手段によるセキュリティ侵害に対抗するため、外部からの侵入対策が講じられた場所に設置すること。	情報セキュリティ遵守状況は月次で報告すること。
		入退室管理の履行	ＰＭＤＡが管理するサーバ室、事務室等の管理区域への入退出については、ＰＭＤＡ入退室管理規程を遵守すること。 ＰＭＤＡの管理区域内での作業は、原則として、ＰＭＤＡ職員の立会いのもとで行うこと。	

障害対策（事業継続対応）（DA: Damage）	構成管理（DA-1）	システムの構成管理　(DA-1-1)	情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、情報システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を実際のシステム構成と合致するように維持・管理すること。	変更作業時の構成管理資料の更新については、「変更作業一覧」により、月次で報告すること。
	可用性確保（DA-2）	システムの可用性確保　(DA-2-1) 情報のバックアップの取得	システム及びデータの保全が確実に実施されるため、システム及びデータのバックアップが所定の要件通りに取得されていることを定期的に確認すること。 また、回復手順について机上訓練を実施し、バックアップや回復手順が適切に機能することを確認する。	バックアップの実施状況は、月次で報告すること。 バックアップによるリストア等回復手順については、 机上訓練を年１回以上実施すること。
サプライチェーン・リスク対策（SC: Supply Chain）	情報システムの構築等の外部委託における対策（SC-1）	委託先において不正プログラム等が組み込まれることへの対策（SC-1-1）	情報システムの運用保守において、ＰＭＤＡが意図しない変更や機密情報の窃取等が行われないことを保証するため、構成管理・変更管理を適切に実施すること。	変更管理の状況は「変更作業一覧」により、月次で報告すること。