開示請求進捗管理・運用支援システム
運用支援業務 調達仕様書

令和３年２月

独立行政法人　医薬品医療機器総合機構

目次

１　調達案件の概要に関する事項.....1
（１）　調達件名.....1
（２）　用語の定義.....1
（３）　調達の背景.....1
（４）　目的及び期待する効果.....2
（５）　業務・情報システムの概要.....2
（６）　契約期間.....6
（７）　作業スケジュール.....6
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.....6
（１）　調達案件及び関連する調達案件の調達単位、調達の方式、実施時期.....6
（２）　調達案件間の入札制限.....6
３　作業の実施内容に関する事項.....7
（１）　作業の内容.....7
（２）　システム資産簿登録に係る作業.....8
（３）　成果物の範囲、納品期日等.....8
４　満たすべき要件に関する事項.....9
（１）　情報セキュリティ対策.....9
（２）　システム操作・監視等要件.....10
（３）　データ管理要件.....13
（４）　運用施設・設備要件.....13
（５）　ソフトウェア保守要件.....13
（６）　ハードウェア保守要件.....14
５　作業の実施体制・方法に関する事項.....14
（１）　作業実施体制.....14
（２）　作業要員に求める資格等の要件.....14
（３）　作業場所.....15
（４）　作業の管理に関する要領.....15
６　作業の実施に当たっての遵守事項.....15
（１）　基本事項.....15
（２）　機密保持、資料の取扱い.....16
（３）　遵守する法令等.....16
７　成果物の取扱いに関する事項.....17
（１）　知的財産権の帰属.....17
（２）　契約不適合責任.....18
（３）　検収.....18
８　入札参加資格に関する事項.....19
（１）　入札参加要件.....19
（２）　入札制限.....19
９　情報セキュリティ管理.....19
（１）　情報セキュリティ対策の実施.....19
（２）　情報セキュリティ監査の実施.....20
１０ 再委託に関する事項.....21
１１ その他特記事項.....22
（１）　環境への配慮.....22
（２）　その他.....22
１２ 附属文書.....22
（１）　別紙.....22
（２）　事業者が閲覧できる資料一覧.....23
１３ 窓口連絡先.....23

１　調達案件の概要に関する事項

（１）　調達件名

開示請求進捗管理・運用支援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
開示請求	総合機構理事長に対し、総合機構が保有する法人文書や個人情報の開示を求めること
法人文書	総合機構の職員が、職務上作成、取得し、組織的に利用するために保有している文書、図画及び電磁的記録（フロッピーディスクなど）のこと
情報公開法	独立行政法人等の保有する情報の公開に関する法律 http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/jyohokokai/shoukai.html
個人情報保護法	独立行政法人等の保有する個人情報の保護に関する法律 http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/kenkyu.htm
補正	開示請求書の受付時に形式上の不備があると認められた場合に、開示請求者に対して、相当の期間を定めて、その不備を修正すること（例えば、手数料の未納、文書特定ができないなど）
開示前例	開示請求があった文書について、過去に同一の文書を開示したもの。また開示請求者の過去の請求履歴も含む。
施行状況調査	独立行政法人等の保有する情報の公開に関する法律第24条によるもの http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/jyohokokai/chousa.html http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/shikojyokyo.html

（３）　調達の背景

情報公開法において、独立行政法人医薬品医療機器総合機構（以下「PMDA」という。）の法人文書の開示状況は、毎年約 2,000 件の請求があり、容量の大きい法人文書の請求が増加傾向にある。そうした中、PMDA 職員が情報公開法で定められた事務処理期限を遵守すると同時に処理精度の向上を図り、PMDA に対する開示請求の進捗を管理するため、平成 28 年 6 月より法人等文書開示請求進捗管理システム（以下「本システム」という。）を運用している。

法人文書開示請求の受付、文書開示等の業務は、経営企画部 情報公開課が担当しており、本システムは、PMDA のイントラネットである「共用 LAN」に接続するための専用

PC 端末に accdb 形式の Access データベースファイルを配置し、請求案件や対応進捗を管理しているものである。

経営企画部 情報公開課の担当者は、自身の端末からアプリケーションを介して本データベースに接続し、情報公開請求のあった案件について、参照・登録・更新などの処理を行っている。

開示請求対応業務の効率的な遂行を実現するためには、本システムの安定的な稼働が不可欠であることから、その実現のために運用保守業務を委託するものである。

（４） 目的及び期待する効果

本調達は、PMDA 職員の開示請求対応業務の効率的な遂行に必要となる本システムの安定的な稼働のため、本システムの運用保守作業を運用支援業務として外部委託する。また、ヘルプデスク業務も委託内容としており、本システムを利用する経営企画部 情報公開課の職員が持つ本システムへの不明点等を解決する役割を担うことで、開示請求対応業務の円滑な遂行に寄与することを期待する。

（５） 業務・情報システムの概要

PMDA では、「独立行政法人等の保有する情報の公開に関する法律」に基づき、法人文書の開示請求手続きを主に実施している。（図 1 参照）

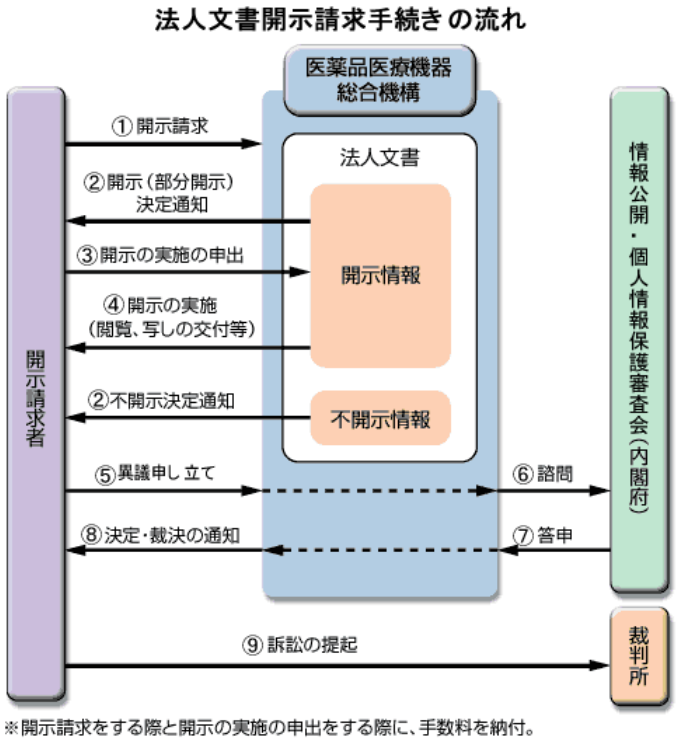


図 1 法人文書開示請求手続きの流れ

また、「独立行政法人等の保有する個人情報の保護に関する法律」に基づき、個人情報の適切な管理を行うべく以下の業務を主に実施している。

・個人情報開示請求制度に基づく業務（図 2 参照）

・個人情報訂正請求制度に基づく業務（図 3 参照）

・個人情報利用停止請求制度に基づく業務（図 4 参照）

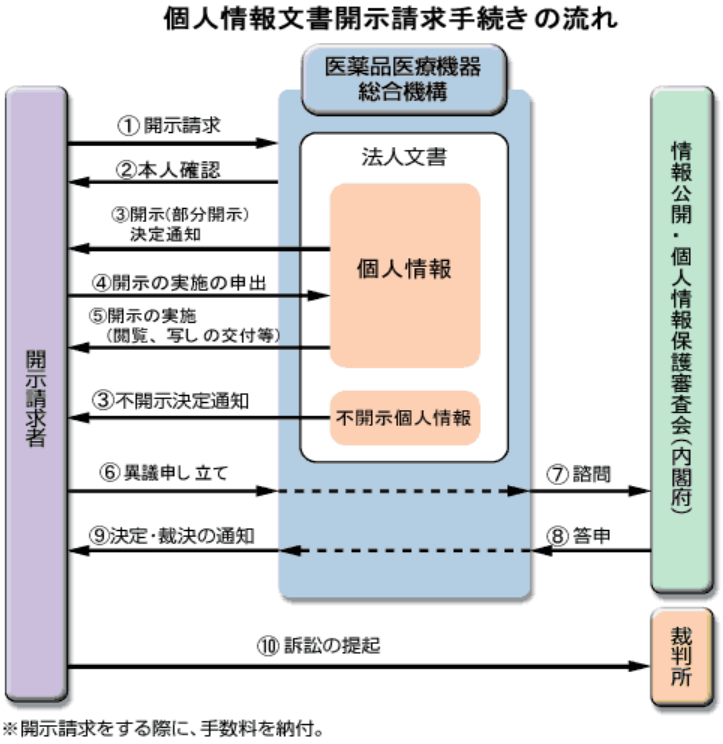


図 2　個人情報文書開示請求手続きの流れ

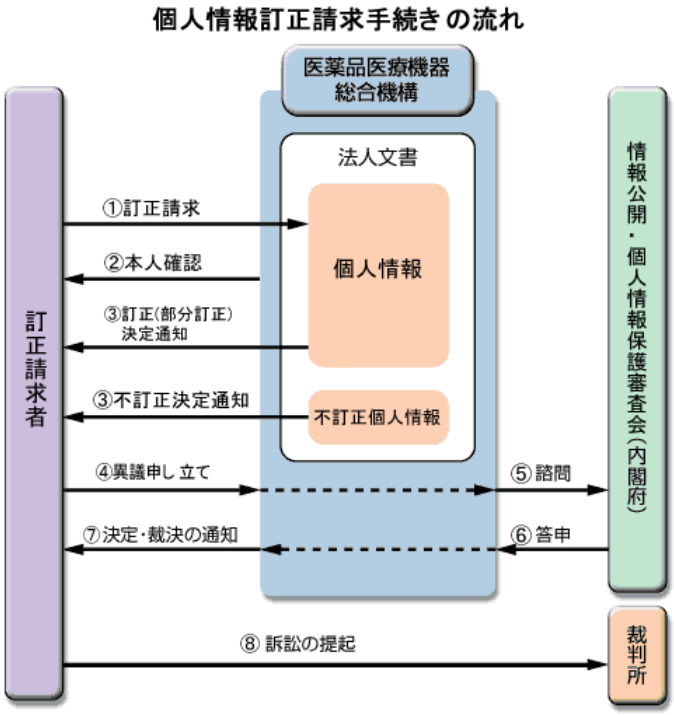


図 3　個人情報訂正請求手続きの流れ

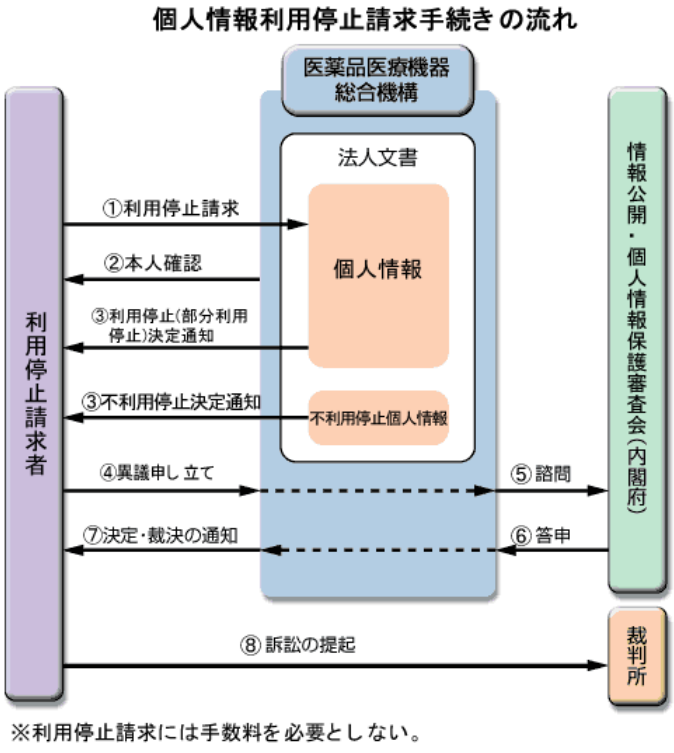
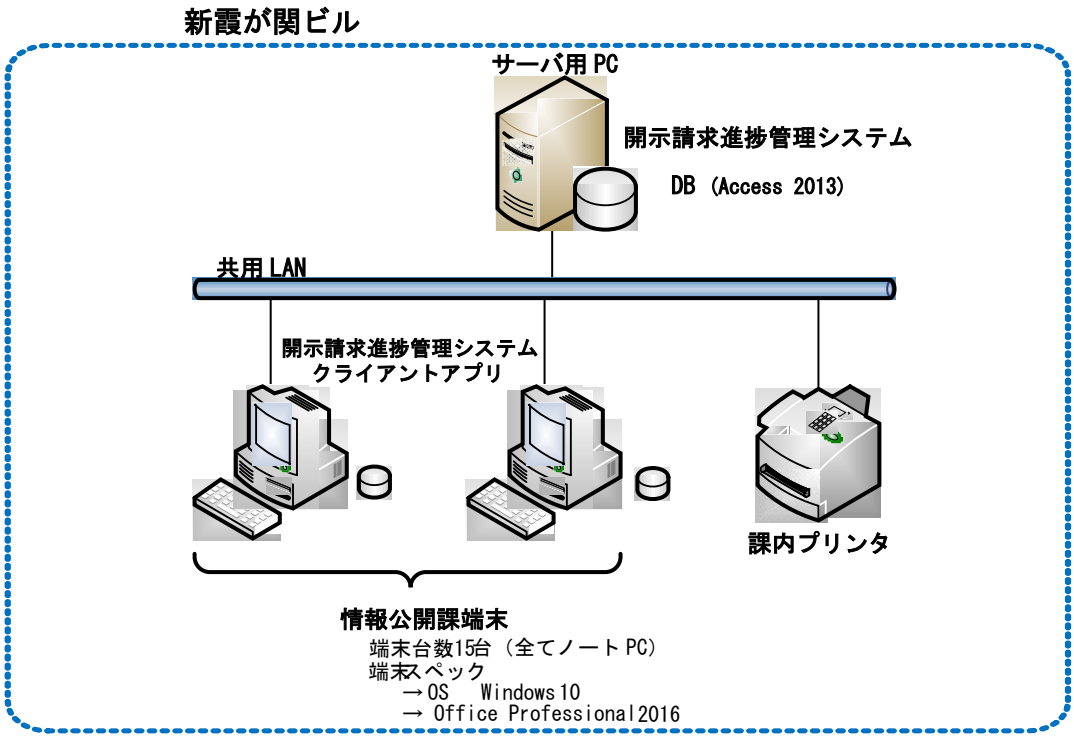


図 4　個人情報利用停止請求の流れ

本システムは、開示請求への対応について、進捗を管理するためのシステムである。PMDA のイントラネットである「共用 LAN」に接続する専用の PC 端末に accdb 形式の

Access データベースファイルを配置し、このデータベースで請求案件や対応進捗を管理する。本システムのユーザである経営企画部 情報公開課の担当者は、自身の端末からアプリケーションを介して、このデータベースに接続し、参照・登録・更新などの処理を行う。構成概要を以下に示す。



クライアントアプリケーションの概要は以下の通り。

- 開発言語：C# (スクラッチで開発)
- ステップ数：63.7KStep
- 画面数：32
- 帳票数：66 (Excel 形式：11, Word 形式：52, Access レポート：3)

令和２年７月時点のデータベースへのデータ格納状況は以下の通り。

- データベース数：3
- テーブル数：30
- レコード数計：約 85,000 件 (1 テーブルの最大約 15000 件)

なお、本システムが扱うデータには、個人情報が含まれる。

本システムの利用者数は以下の通り。

・PMDA 内同時利用者数：約 15 名

・PMDA 内実効登録利用者数：約 15 名

（６）　契約期間

契約締結日から令和４年３月３１日まで

（７）　作業スケジュール

本業務に係る想定スケジュールの概要を図　１.５に示す。図　１.５はあくまで想定のスケジュールであり、詳細な実施スケジュールは受注者が検討すること。

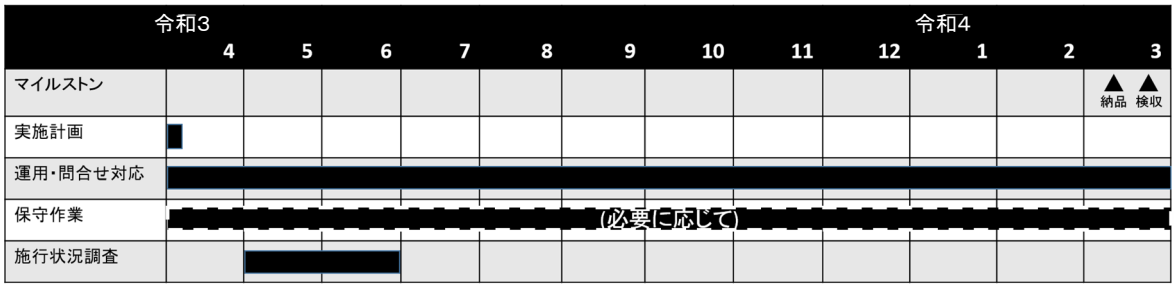


図　１.５　スケジュール概要

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

（１）　調達案件及び関連する調達案件の調達単位、調達の方式、実施時期

関連する調達案件の調達単位、調達の方式、実施時期は次の表の通りである。

表　２.１　関連する調達案件の調達単位、調達の方式、実施時期等（既存契約）

なし。

表　２.２　関連する調達案件の調達単位、調達の方式、実施時期等（契約予定）

なし。

（２）　調達案件間の入札制限

なし。

３　作業の実施内容に関する事項

（１）　作業の内容

ア　運用保守業務

「4　満たすべき要件に関する事項」に基づき、以下のシステム運用・保守業務を行うこと。作業は、基本的に当該業務の業務マニュアル及びシステム運用マニュアルに基づき実施し、必要に応じて PMDA と協議し実施すること。また、必要に応じて PMDA と協議し、ドキュメントの作成・改版等を行うこと。

a システム設定・運用業務に伴うシステム操作

b ヘルプデスク（機構職員からの問合せ対応等　月 2～3 件程度を想定）

c システム障害対応（状況把握・原因調査・復旧支援・機構内復旧作業 等）

d 軽微な改修・修正 (年 2 人月程度の主に利便性向上を目的とした改修)

e 施行状況調査の支援

f その他

・システム運用に必要な調査及び技術提案

・ドキュメント作成業務

・PMDA との打ち合わせ

・上記業務を実施するうえで必要とされる手順の確定と手順書作成業務

イ　報告業務

(ア) 受注者は、別紙 2「システム運用管理基準」を参照の上、本業務で実施した運用作業または軽微改修作業における WBS の各項目単位の作業内容とその工数について、月次で作業報告書を作成し PMDA に提出すること。

(イ) ログ監視等にてシステムやデータベースの障害等が予見された場合には、当該事象を知った後、速やかに PMDA に報告し、その対応については PMDA と協議し、必要に応じて対策を実施すること。

(ウ) その他運用業務を実施するにあたって明らかになった、仕様変更などのシステムの見直しが必要と考えられる事項を整理し、改善策等の提案を含めて報告書としてとりまとめること。報告書は年度末及び、PMDA の求めに応じて提出すること。

ウ　作業期間等

「１－（６）契約期間」に示す期間とする。

支援業務を行う日は、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。

また、支援業務を行う時間については、原則、支援業務を行う日の 9 時 30 分から 18 時までとする。（ただし、12 時から 13 時までは休憩時間とする。）

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。

なお、PMDA に非常勤ではあるが、打合せやデータ確認、ログ確認等は機構にて行う為留意すること。

（２）　システム資産簿登録に係る作業

受注者は、本業務において新たに利用するハードウェア・ソフトウェア・外部サービス等がある場合、PMDA が指定する以下のシステム資産簿登録用シートを、運用実施要領において定める時期に提出すること。

（ア）　ソフトウェアライセンスに関する情報
　　（ソフトウェア名称、バージョン、期限、ライセンス番号、数量 等）

（イ）　外部サービス利用に関する情報
　　（サービス名称、契約形態、契約期間、サポート内容 等）

（ウ）　ハードウェア資産に関する情報
　　（機器名、設置場所、メーカ保守期限、用途 等）

（エ）　その他 PMDA が指定する項目

（３）　成果物の範囲、納品期日等

①　成果物

作業工程別の納入成果物を表 ３.１に示す。ただし、納入成果物の構成、詳細については、受注後、PMDA と協議し取り決めること。

表 ３.１　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	計画	・プロジェクト実施計画書（プロジェクトスコープ、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、変更管理要領、WBS） ・情報セキュリティ管理計画書	契約締結日から 2 週間以内	
2	運用	・システム運用マニュアル ・運用支援要員業務マニュアル ・システム関連ドキュメント ・プログラム・ツール等	令和 4 年 3 月 31 日	注 2
3	その他	・作業週報 ・月例報告資料 ・打合せ資料 ・議事録 ・障害等作業記録 ・運用支援報告書	令和 4 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は、SLCP-JCF2013（共通フレーム 2013）を参考とすること。

注 2 必要に応じて改定したマニュアル（「システム運用マニュアル」「運用支援要員業務マニュアル」等の運用を行うために必須となるマニュアル）は改訂の都度 PMDA に提出し PMDA の了承を得ること。なお、最終納品版として、令和 4 年 3 月 31 日までに当年度中に改訂したマニュアルを提出すること。

② 納品方法

表 3.1 の納入成果物を含む全ての納入成果物を表内記載の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 電子形式の文書を磁気媒体等（CD-R 又は DVD-R 等）により日本語で提供すること。紙媒体の納入は不要とする。

イ 磁気媒体等に保存する形式は、PDF 形式及び Microsoft Office2016 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 磁気媒体等の納入物は、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 本業務を実施する上で必要となる一切の機器物品等は、受注者の責任で手配するとともに、費用を負担すること。

カ 各工程の中間成果物も含め、本調達に係る全ての資料を納品すること。

③ 納品場所

独立行政法人　医薬品医療機器総合機構　経営企画部 情報公開課

4 満たすべき要件に関する事項

（1） 情報セキュリティ対策

本システムの設計・開発・運用保守等に際しては、受注者は、PMDA と調整の上、必要な対策を講じること。なお、情報セキュリティ対策を講じる範囲はシステム全体に係ることであり、本システム（未改修部分）にセキュリティホールが検出された場合も、受注者がセキュリティ対策を講じること。主な対策例を下表に示す。

表 2 情報セキュリティ対策

区分	対策の概要
コンピュータウイルス対策	コンピュータウイルス対策基準（平成 12 年 12 月 28 日（通商産業省告示第 952 号））に準じた対策を講じること。
ボット対策	ボットに感染したコンピュータからのサイバー攻撃等を迅速かつ効果的に停止させるための対策を考慮すること。
不正アクセス対策	ウェブサイトに係る機能等に関しては、クロスサイト・スクリプティングや SQL インジェクション等の脆弱性を狙った攻撃に対する対策を講じること。
脆弱性対策	ソフトウェア等脆弱性関連情報取扱基準（平成 16 年 7 月 7 日（経済産業省告示 第 235 号））に準じた対策を講じること。
監査証跡（ログ管理）	・オンライン処理について、利用者 ID、IP アドレス、利用機能、アクセス日時等について、ログが取得出来ること。 ・ログの収集及び一元管理が可能であること。ログファイルは一定期間ハードディスク上に保存し、それを超えた分については、外部可搬媒体にて保存させること。

（２） システム操作・監視等要件

① サービス提供プロセス

ア サービスレベル管理

下表に基づき、サービスレベル管理を実施すること。サービスレベルの達成状況についてサービスレベル報告書としてとりまとめ、報告書の提出をもって PMDA に報告すること。サービスレベルが遵守できなかった場合、その改善策（手続きや体制の見直し、新たなツールや仕組みの検証・導入等）の検討・実施を必須とする。また、改善策の実施状況や改善の状況についても、報告書にて報告すること。

表 6 評価項目・評価基準一覧

No.	評価項目	評価基準	目標値
1	問合せへの一次回答	職員からの問合せに対し、受付から 1 営業日以内に一次回答を行うこと。	100%/月
2	セキュリティ事故発生件数	本業務の作業範囲において、「セキュリティ対策ソフトウェア」および「人」により検知されるセキュリティ事故が発生しないこと。	0 件/月
3	運用業務サービス・ヘルプデスクサービス提供時間	9 時 30 分から 18 時の時間帯において、[項 3-(1)-ア]記載の各作業を実施すること。	99. 9%/月
4	システム障害対応	システム障害が発生したことを認知した時から 15 分以内に初動対応を開始	100%/月

		すること。	

イ　サービスの継続性及び可用性の管理

(ア) 稼働監視

なし。

(イ) ログ監視

常時監視は必要ないが、定期的なログ監視を実施すること（月 1 回程度）。

(ウ) リカバリ

なし。

(エ) システム再起動

なし。

(オ) 設定変更

本システムを正常に稼動させるために設定の変更が必要となる場合は、PMDA に提案し、PMDA の了解の下、当該作業を実施すること。

ウ　容量・能力管理

なし。

エ　情報セキュリティ管理

本システムへの不正侵入など、本システムに関するセキュリティ監視をログから検出できるレベルで行うこと。

② 関係プロセス

ア　顧客関係管理

(ア) 問い合わせ対応

平日の 9 時 30 分から 18 時において、本システムに関する PMDA 内の利用者からの問い合わせに対応すること。問い合わせの方法は電話または電子メールとする。

システム操作に関する質問については、適切な操作方法を回答すること。また、本システムの動作不具合に関する問い合わせについては、問い合わせ内容を分析し、操作方法に起因する場合には適切な操作方法を回答すること。システム障害が疑われる場合には、障害もしくは要望の切り分けを実施し、適切に解決に向けて対応すること。

適宜発生する PMDA からのセキュリティ状況に関する問合せや、システム構成情報等、本システム（本番環境、検証環境含む）に関する問合せにも対応すること。

また、PMDA では、システム監査を外部機関に委託し、毎年実施している。このシステム監査によって発生した問い合わせやセキュリティホール等の指摘に対しても、

PMDA と協議の上、対応すること。

問合せに関しては機構からの問合せや回答内容、開発業者とのやりとり等含め一覧にて確認出来るよう記録として残すこと。

(イ) 情報提供

PMDA に対し、システム運用に関する情報提供を行うこと。情報提供の手段は電子メールとし、提供件数は 1 件／年程度を想定する。

(ウ) 運用保守、障害対応手順の追加・改訂

運用保守や障害対応においては手順に沿って対応することになるが、手順の追加修正等必要になる可能性がある。その場合において適宜手順の改訂や追加を行うこと。

(エ) 施行状況調査の支援

本システムにより生データ及び統計に必要な情報を付加したデータが Excel 表（約 40 項目）に基礎データとして出力される。この基礎データには、誤入力などの入力不備が含まれ、データとして完成していない。データとして完成させるために、チェックシート（※）を元に不備な部分を調査し、PMDA に報告する。報告を受けて、PMDA はデータを修正するので、その修正後に本システムから Excel 表に改めてデータを出力し、その結果を施行状況調査で指定された様式に入力する。

施行状況調査で指定されたデータ項目数は約 500 項目あるが、実際に PMDA で使用している項目はおおよそ 200 項目になると想定している。

なお、開示請求件数は毎年約 2,000 件あり、半年毎に行う。

※チェックシートは全項目分あり、資料閲覧時に公開する

③ 解決プロセス

ア インシデント管理

利用者からの問い合わせに対して、質問、要望、障害等の区分を整理するとともに、各案件の対応状況について記録管理すること。

また、定期的にインシデントの発生傾向を集計・分析すること。問い合わせの多いものについては、FAQ として情報抽出・整理を行うこと。

イ 問題管理

インシデントのうち、対応方法の検討が必要となる案件について課題として切り出し、課題管理表に記録すること。また、対応策について PMDA と協議し、PMDA の了解の下、必要な作業を実施すること。

④ 統合的制御プロセス

ア 変更管理

課題管理や変更要求等によって、対象となるハードウェア、ソフトウェア等の資源への変更が発生する場合、その対応状況や進捗状況を管理すること。また、受入テストの実施支援を行うこと。

イ　構成管理

変更管理及びリリース管理に伴うハードウェア､ソフトウェア等の資源の版数管理、原本管理を行うこと。

ウ　環境管理

検証環境機器について、本番環境機器と整合性の取れたシステム環境を維持管理すること。

⑤　リリースプロセス

ア　リリース管理

変更管理によって、対象となるハードウェア、ソフトウェア等の資源への変更が発生する場合、リリース可否の判断を行い、PMDA と協議し、PMDA の了解の下、リリースに必要な作業を実施すること。

⑥　年間業務報告

システム運用作業全般として、年度末に PMDA を交えた定期報告会を実施すること。定期報告会開催に当たっては、年間業務報告書を事前に作成し提出すること。尚、作成する年間業務報告書には以下の事項を含めること。また、年間業務報告の議題に挙げる事項は、PMDA と協議し決めること。

・各種ログの分析結果
・障害等、システム状態予測

（３）　データ管理要件

なし。

（４）　運用施設・設備要件

なし。

（５）　ソフトウェア保守要件

①　軽微な改修・修正

業務の効率化、利便性の向上に資するために、PMDA の指示のもと、例えば、アプ

リケーションに発生した不具合や画面・帳票レイアウトの変更、検索条件の修正、小規模ツールの作成といった軽微な改修・修正を実施すること。その際、必要な設計書の改訂・作成も併せて実施すること。（2 人月程度までの作業とする。）

軽微な改修に際して、工数見積もりを行い、PMDA の承諾を得ること。また、工数見積もりに係る時間は、上記に示した「2 人月程度まで」に含めないこと。

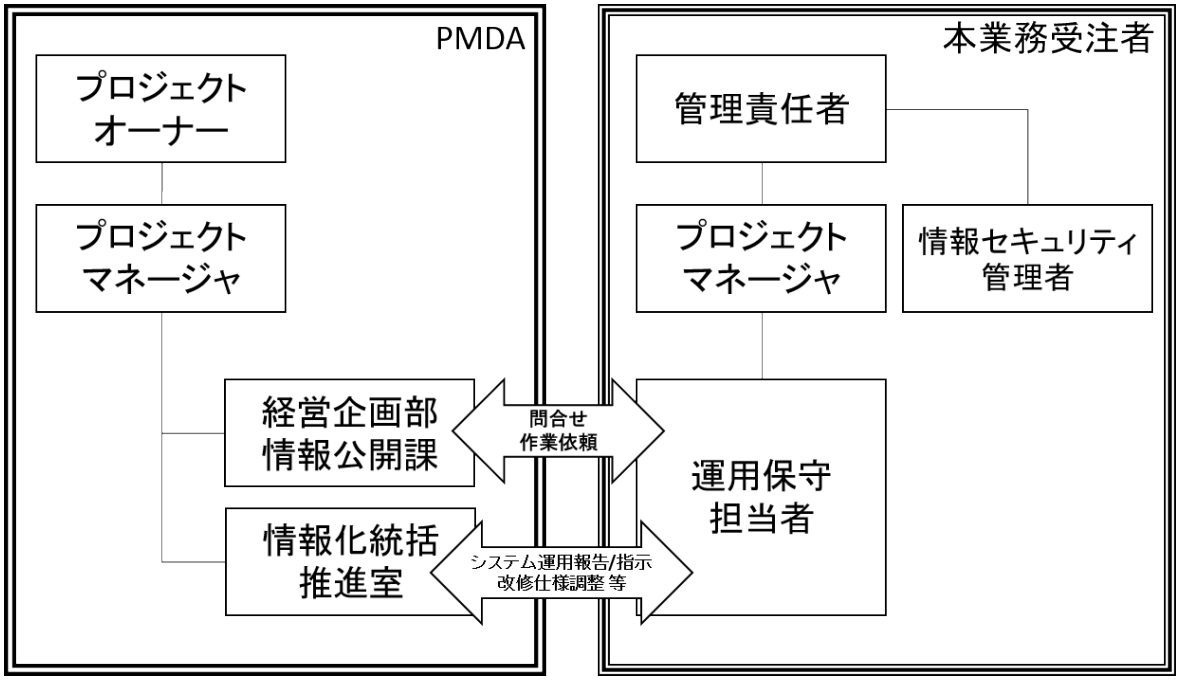
（６） ハードウェア保守要件

なし。

５ 作業の実施体制・方法に関する事項

（１） 作業実施体制

① プロジェクトの推進体制及び本件受注者に求める作業実施体制は次の図及び表のとおりである。なお、受注者内のチーム編成については想定であり、受注者決定後に協議の上、見直しを行うこと。また、受注者の情報セキュリティ対策の管理体制については、作業実施体制とは別に作成すること。



② 本業務を複数業者が連携（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） 作業要員に求める資格等の要件

① 以下のそれぞれの条件に合致する業務を担当した実績を有すること。

ア　Access および C#によるシステム開発業務（それぞれの言語による開発は、別々のシステムであっても良い。）

イ　Access および C#によって開発されたシステムのヘルプデスク業務（Access で開発されたシステム、C#で開発されたシステムの 2 種類のヘルプデスク業務であっても良い）

② 本業務に携わるメンバーの 1 人は独立行政法人情報処理推進機構（IPA）の「情報セキュリティスペシャリスト」もしくは「情報処理安全確保支援士」のいずれかの資格を取得していること。

（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。
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 受注者は、PMDA の指示に従って運用業務または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。

６　作業の実施に当たっての遵守事項

（１）　基本事項

受注者は、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 受注者は、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、受注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 受注者は、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。）、他の受注者が提示した情報及び受注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 受注者は、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、受注者において該当情報を保持しないことを誓約する旨の書類を PMDA 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 受注者は、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 情報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

なお、「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、必要に応じ参照し、その内容を取り込むこと。
「独立行政法人 医薬品医療機器総合機構 情報セキュリティポリシー」の開示については、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。

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 受注者は、本業務の遂行に当たっては、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。

④ 受注者は、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、受注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、受注者は著作者人格権（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、受注者は原著作物の著作権者としての権利を行使しないものとする。

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

（２） 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、本業務実施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、本業務実施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 本業務実施者は、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、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、速やかにその情報を完全に消去すること。データ消去作業終了後、本業務実施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、本業務実施者の負担で用意すること。

（３） 検収

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

なお、以下についても遵守すること。

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

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

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

8 入札参加資格に関する事項

（1） 入札参加要件

応札希望者は、以下の条件を満たしていること。

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

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

③ 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。

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

（2） 入札制限

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

① PMDA の CIO 補佐が現に属する、又は過去 2 年間に属していた事業者等

② 各工程の調達仕様書の作成に直接関与した事業者等

③ 設計・開発等の工程管理支援業者等

④ ①～③の親会社及び子会社（「財務諸表等の用語、様式及び作成方法に関する規則」（昭和 38 年大蔵省令第 59 号）第 8 条に規定する親会社及び子会社をいう。以下同じ。）

⑤ ①～③と同一の親会社を持つ事業者

⑥ ①～③から委託を請ける等緊密な利害関係を有する事業者

9 情報セキュリティ管理

（1） 情報セキュリティ対策の実施

受注者は、「別紙 3 情報セキュリティ対策の運用要件」に記載されている内容および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」をプロジェクト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　受注者の資本関係の情報、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）・実績並びに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「情報セキュリティ管理計画書」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　本業務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。

なお、情報セキュリティ監査の実施については、本項に記載した内容を上回る措置を講ずることを妨げるものではない。

１０　再委託に関する事項

① 受注者は、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 受注者は、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 PMDA に提出すること。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、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注者が負うこと。

④ 再委託先が、更に再委託を行う場合も同様とする。

⑤ 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。

- 受注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。

・ 受注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、PMDA から求めがあった場合には情報提供を行うこと。

・ 受注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、PMDA 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の対処方法を検討し、PMDA 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。

・ 受注者は、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。

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、受注者もその方針に従うこと。

１２　附属文書

（１）　別紙

別紙１　本システム新規開発時の要件定義書

別紙２　システム運用管理基準

別紙３　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　情報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　開示請求進捗管理システム設計書一式

１３　窓口連絡先

独立行政法人　医薬品医療機器総合機構　経営企画部

情報公開課　吉野 康宏

電話：03 (3506)9601

Email：yoshino-yasuhiro ●pmda.go.jp (●は@に読み替えること)

別紙 1

開示請求進捗管理及び
運用支援システムの構築業務

要件定義書

目 次

1. システム化の目的 1
2. システムの概要 1
   2.1 全体構成図 1
3. 機能要件 2
   3.1 機能一覧 2
   3.2 情報・データ要件 2
   3.3 外部インターフェース要件 2
   3.4 個人情報及びプライバシー保護への配慮 2
4. 非機能要件 3
   4.1 規模要件 3
   4.2 性能要件 3
   4.3 信頼性要件 3
   4.4 拡張性要件 3
   4.5 上位互換性要件 3
   4.6 システム中立性要件 3
   4.7 情報セキュリティ要件 3
      4.7.1 権限要件 4
      4.7.2 情報セキュリティ対策 4
   4.8 ユーザビリティ要件 4
      4.8.1 ユーザビリティ向上の目的 4
      4.8.2 想定利用者 4
      4.8.3 要件 4
5. 移行要件 4
   5.1 移行方針 4
   5.2 移行範囲 4
6. 運用要件 5
   6.1 システム操作・監視等要件 5
   6.2 試行運用中の微修正 5
   6.3 データ管理要件 5
7. 用語集 5

1. システム化の目的

独立行政法人医薬品医療機器総合機構（以下「PMDA」という。）では、平成 16 年設立以来、法人文書の特定を的確に行い、開示期限内に対応することに務めてきたところである。しかしながら、年々増加する開示請求や大容量の文書に対して、既存システムを利用して、法で定められた期限を遵守しつつ処理することは非常に困難な状況にあり、業務遅延リスクを防止するべく進捗管理を強化し、業務を支援するための新たなシステムを構築することが必要である。そのため本調達は、作業の効率化を図るべく進捗管理･運用支援システム（以下「進捗管理システム」という。）を構築することを目的としている。なお、本システムには法人文書だけでなく、個人情報保護法に基づく開示請求等の進捗管理システムも含む。

2. システムの概要

2.1 全体構成図

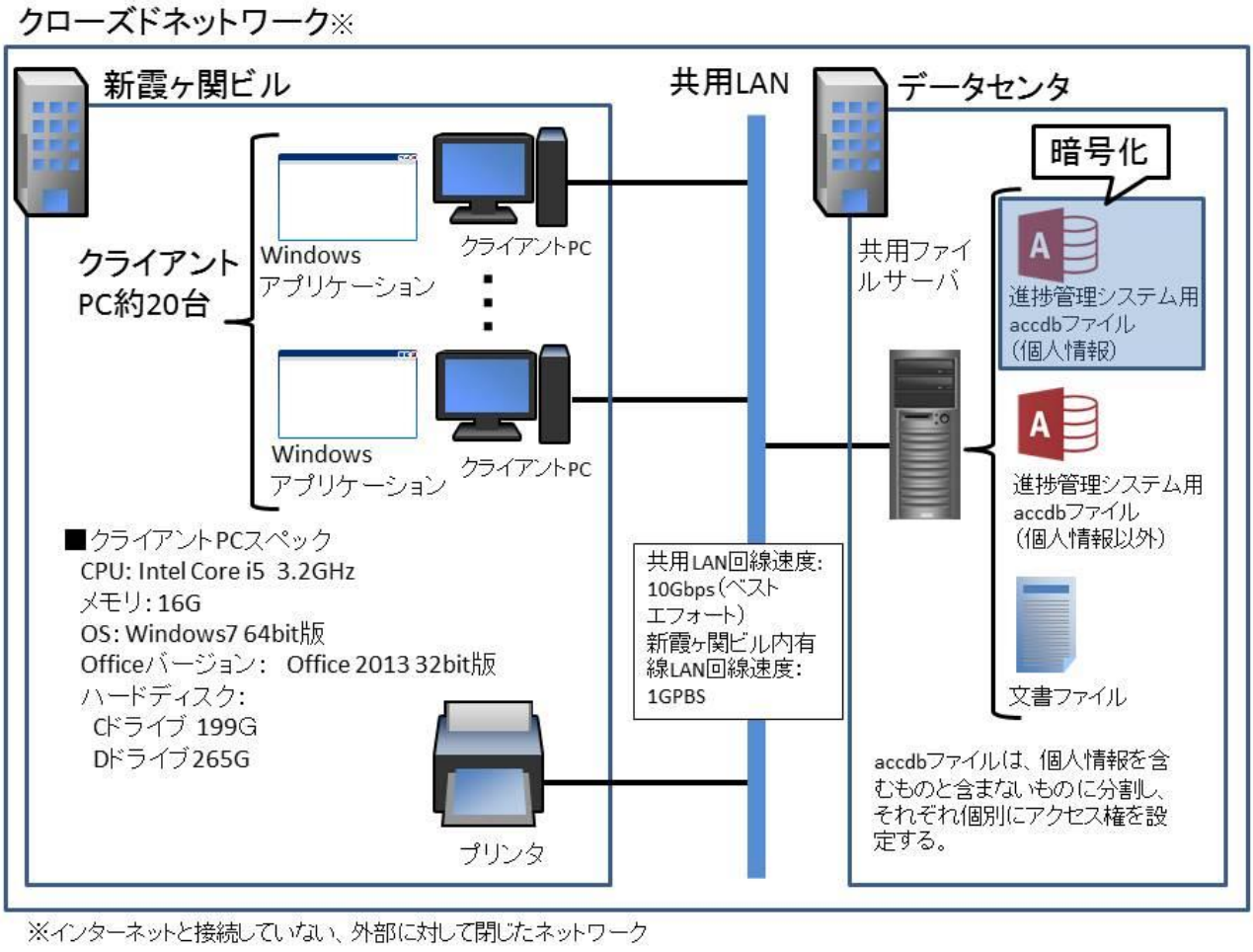


図 2.1 システム概念図（次期システム）

※2020 年 7 月現在は、「データセンタ」の範囲が、「共用 LAN 上の専用 PC」となります。
本紙1－(5)も合わせてご参照ください。

① 進捗管理システム用として用いるデータベースは、accdb ファイルを共有する方式で構築する。
② 共有する accdb ファイルは、PMDA が指定する共用ファイルサーバ上に構築する。
③ 個人情報保護を考慮し、accdb ファイルを個人情報ファイルと個人情報を含まないファイルに分割する。また、個人情報ファイルを暗号化する。
④ 進捗管理システムのクライアント AP は、C# を用いた Windows アプリケーションとして構築する。

3. 機能要件

3.1 機能一覧

機能一覧、画面一覧、帳票一覧を基本設計フェーズにて作成し、基本設計書として管理する。

3.2 情報・データ要件

本システムでは、以下のデータを管理する。

表 3.1 本システムの情報・データ概要

No	情報・データ名	情報・データ概要
1	個人情報開示請求情報	個人情報の開示請求に関する情報。
2	法人文書開示請求情報	法人文書の開示請求に関する情報。
3	個人情報開示決定情報	個人情報の開示請求に対する決定内容に関する情報。
4	法人文書開示決定情報	法人文書の開示請求に対する決定内容に関する情報。
5	第三者意見照会情報	法人文書／個人情報開示請求および異議申立において、PMDA と第三者の間で行われた意見照会に関する情報。
6	異議申立情報	法人文書および個人情報の異議申立に関する情報。
7	審査会履歴情報	審査会の審査履歴に関する情報
8	請求者情報	法人文書および個人情報の開示請求者に関する情報。
9	第三者情報	法人文書／個人情報開示請求において、特定した法人文書／個人情報に対して意見照会を行う第三者（企業）とその担当者に関する情報。
10	手数料情報	手数料の入金、還付、流用などに関する情報。
11	定型文書	本システムで出力する帳票の雛形。
12	ユーザ情報	本システムを利用するユーザに関する情報。
13	アクセス履歴	本システムで管理している情報に対するアクセス履歴（ユーザ、時間、機能等）。
14	マスタ情報	本システムで利用するマスタ情報。

3.3 外部インターフェース要件

PMDA 会計課が業務で使用する手数料管理表を Excel 形式で出力する。

3.4 個人情報及びプライバシー保護への配慮

個人情報およびプライバシーの保護に配慮し、その範囲と方策について以下の通り定める。

① 本システムで保護すべき個人情報およびプライバシーの範囲
- ・請求者情報
- ・第三者情報
- ・開示請求された文書

② 個人情報およびプライバシー保護に対する方策
- ・個人情報となる請求者情報、第三者情報については、個人情報用に accdb を構築し、データベースパスワードを設定して暗号化する。
- ・開示請求された文書は PMDA が指定する共用ファイルサーバ上に配置し、アクセス権により保護する。

4. 非機能要件

4.1 規模要件

① 開示請求件数に係る規模を以下に示す。1 件あたり、A4 用紙 5,000 頁に及ぶものもある。

表 4.1 年度別開示請求件数

年度	件数(約)
平成 23 年度以前	2,600
平成 24 年度	1,600
平成 25 年度	1,800
平成 26 年度	1,600

② 過去の実績から、毎年度 2,000 件の開示請求を考慮する。5 年後の平成 31 年度の開示請求総件数は 17,600 件となる。

③ 20 台の端末より同時アクセスされることを前提にシステムを構築する。情報更新に際してはレコードの排他制御を十分に考慮する。

4.2 性能要件

20 台の端末からの同時アクセスに際して、新規登録・編集・参照に係る一操作(ボタンクリック後のレスポンス等)が 3 秒以内とする。検索は、1,000 件以内の情報を表示する場合 3 秒以内とする。(ただし、フリー入力項目による部分一致検索は 30 秒以内とする。)また、検索を伴わない表示系のレスポンスは 1 秒以内とする。なお、統計用の Excel 出力に関しては、集計に必要なデーター覧を上限 10 分以内に出力する。ただし、ネットワークの性能による影響は考慮しない。

4.3 信頼性要件

稼働中システムの正常動作を保証し、通常業務に重大な影響を与えない。具体的には以下のとおり。

・プログラムリリース以外の計画停止は実施しない。

・基本的に24h365／366稼働とする。ただし、サーバメンテナンス時およびパッチ適用などの緊急時は除く。

・障害が発生した際はデータ不整合が発生しない設計とする。

・データ障害等でデータの復旧が伴う場合は、最大1日前までのデータを用いて復旧できる。

・運用時にパフォーマンス測定が容易に行えるよう、ボタンクリックから画面出力までの時間をログに出力する。(CPU 使用率、メモリ空き容量など、分析に必要な情報も出力する。)

・万が一、障害等でシステムが利用出来なくなった場合を想定し、システムが利用出来なくなった場合の業務についても考慮の上、マニュアル等を作成する。

4.4 拡張性要件

本業務において改修等を施す際には、既存システムのソフトウェア構成やシステム開発言語等を踏襲し拡張等にも対応する。

4.5 上位互換性要件

選定したソフトウェアに関して、設計段階から、バージョンアップのプランを考えて設計する。

4.6 システム中立性要件

他の事業者がシステムの保守や拡張を引き継げるようにする。

4.7 情報セキュリティ要件

4.7.1 権限要件

ユーザ毎に権限設定を可能とする。
設定できる権限は、実務担当者、手数料担当者、管理者とする。

4.7.2 情報セキュリティ対策

検証環境にて検証を行い、共用LANシステムで実装している情報セキュリティ対策に影響がないことを確認する。
また、本システムに関するセキュリティ対策においては、調達仕様書の「情報セキュリティ要件」や「遵守事項」を対応する。
なお、不正アクセス等の監視目的から入力パラメータ等を含めた操作ログ等取得する。

4.8 ユーザビリティ要件

4.8.1 ユーザビリティ向上の目的

本開発では、ユーザビリティの向上に取り組む。ユーザビリティ向上は、以下を目的としている。

① 利用者の作業時間の短縮
② 利用者の負担・ストレスの低減と満足度の向上

4.8.2 想定利用者

本システムの利用者、利用組織は以下の通りである。

① PMDA 審査マネジメント部情報公開課の職員

4.8.3 要件

本開発では、ユーザビリティについて以下の要件を満たすことが求められる。

1. 選択肢が多い場合には、効率的に選択できるよう、プルダウンメニューからの選択等を活用し、選択肢が少ない場合にはチェックボックスを活用し、選択肢が択一の選択であるか複数選択可であるかが画面上で明確に識別できるようにする。
2. データの削除や更新を行う際は、確認メッセージを表示するなどの誤操作の防止に配慮する。
3. 入力画面が縦に長くなるような場合は、ページ切替等の操作性の向上を検討する。

5. 移行要件

5.1 移行方針

① 本番環境の移行作業は、移行手順の作成･整備･事前検証を行い、その結果について PMDA の承認を得て、作業を実施する。
② 業務に影響を出さないよう PMDA と調整の上、作業を実施する。
③ 本番稼動に際しては、直前の業務で発生した現行システムのデータも漏れなく移行し、正常に格納されていることを十分に確認する。
④ システム改修等を施しても、改修した機能を含めて全機能が使用できるように設計する。
⑤ 移行準備作業に際し、PMDA で実施すべきこと、NES にて実施すべき事を明確にし、作業を進める。なお、PMDA が作業する場合、PMDA にて作業誤りが発生しないよう予め埋められるデータは埋めた状態でフォーマット等作成し、PMDA に提供する。

5.2 移行範囲

① データクレンジングに際して、PMDA の指示に従い、以下の作業支援を実施する。

ア）一括変換でのデータクレンジング
イ）一括変換できなかったデータのリスト
ウ） 既存データベースからのデータ抽出

② クレンジング済データに関して、刷新した進捗管理システムへデータ移行する。
③ CD-ROM メディア等で管理している過去の開示請求対象文書等に関して、指定するフォルダに格納する。なお、本システムとの連携を考慮しフォルダ構成等を検討する。

6. 運用要件

6.1 システム操作・監視等要件

① 業務時間
試行運用期間は 2/22～3/31 までとし、試行運用業務を行う日は、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。試行運用期間は PMDA 常駐せず、電話やメールでの対応とする。また、試行運用業務を行う時間については、原則、試行運用業務を行う日の 9 時 00 分から 17 時 30 分までとする(但し、12 時から 13 時までは休憩時間とする。)。ただし、本要件定義書で別途定めるものの他、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。

6.2 試行運用中の微修正

① 試行運用期間における進捗管理システムに対する軽微な改修として、1 件当たり 10 時間程度の改修工数で年間あたり 16 件程度の小規模改修に対応する。なお、端数月数となる初年度に関しても、16 件程度の小規模改修に対して対応する。
② 小規模改修の具体的な内容要件、設計、製造、テスト、時期等)に関しては、都度、総合機構と協議の上、決定する。
③ システム改修後の構成管理およびリリース管理を実施し、総合機構の承認を得る。

6.3 データ管理要件

① システム障害からの復旧
システム障害からの復旧開始は 3 時間以内に実施する。

② バックアップ
進捗管理システムではバックアップを行なわない。共用LANシステムで実装しているバックアップ機能を使用する。バックアップ機能は、Windows 標準機能のシャドウコピーで 1 日 1 回 AM4 時にバックアップを作成し、14 日間保存する。

7. 用語集

本要件定義書および別紙で使用されている用語について、以下の通り定義する。

表 7.1 用語集

用語	定義
PMDA	独立行政法人医薬品医療機器総合機構
開示請求	総合機構理事長に対し、総合機構が保有する法人文書や個人情報の開示を求めること
法人文書	総合機構の職員が、職務上作成、取得し、組織的に利用するために保有している文書、図画及び電磁的記録(フロッピーディスクなど)のこと

用語	定義
情報公開法	独立行政法人等の保有する情報の公開に関する法律 http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/jyohokokai/shoukai.html
個人情報保護法	独立行政法人等の保有する個人情報の保護に関する法律 http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/kenkyu.html
既存システム	現在使用しているアクセス及びエクセルによる管理システム
開示前例	開示請求があった文書について、過去に同一の文書を開示したもの。また開示請求者の過去の請求履歴も含む。

別紙2

システム運用管理基準

2019 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

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

本要領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」

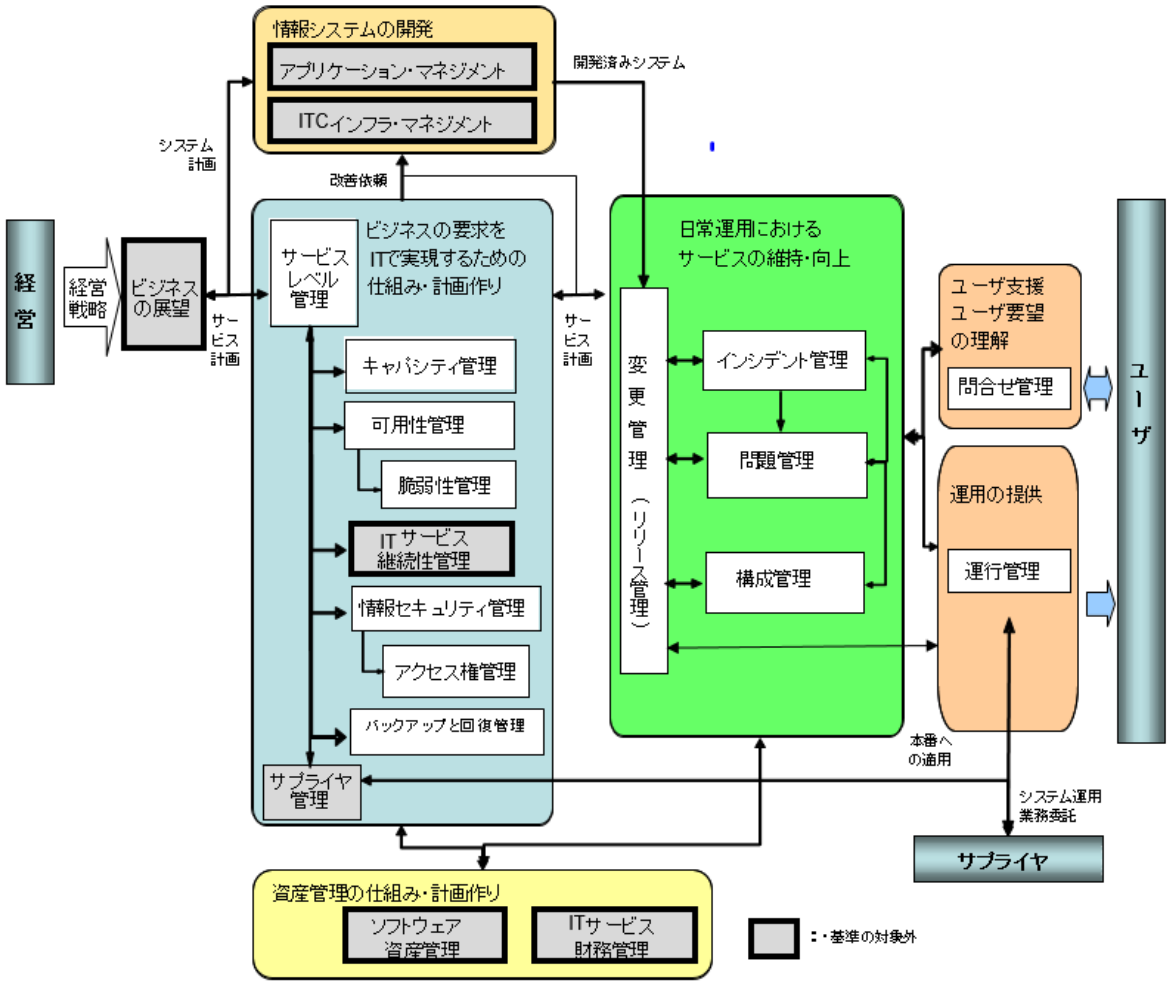
2. システム運用管理業務の概要

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要領で評価・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、本要領においては、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要領・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

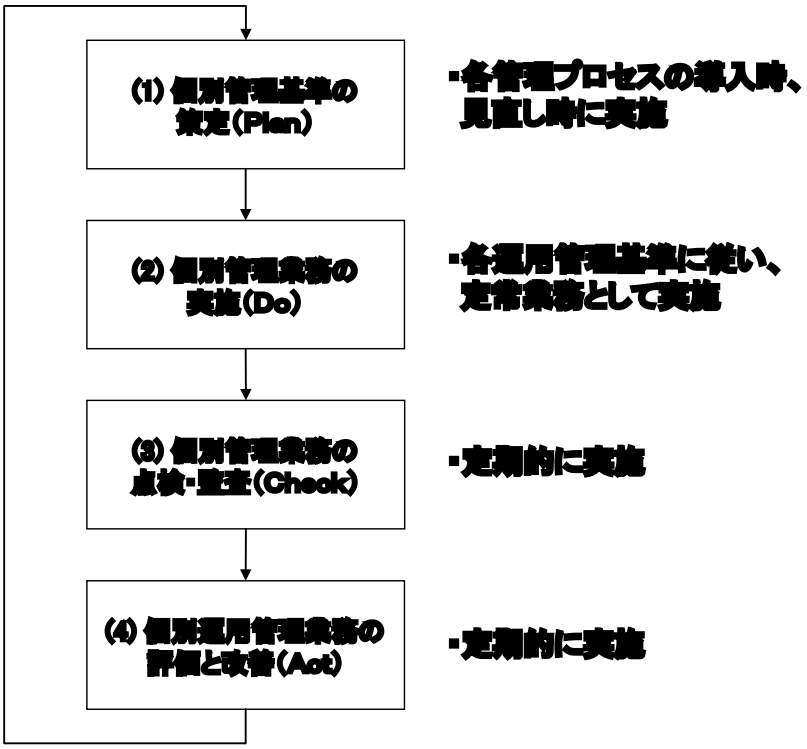


3. 運用管理業務の基本プロセス

（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、個別管理要領の策定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） 個別管理要領の策定 （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要領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、個別運用管理要領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

※具体的にどの管理指標をどう用いるかについては、今後調整の上確定する。
以下同様。

(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「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 ジョブ実行管理
⑥ 帳票管理
⑦ 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

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。

本要領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

①情報セキュリティ遵守状況の報告<次ページ参照>

- 情報セキュリティを遵守していることを定期的(月次)にて報告すること
- 合わせて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こと。

（点検内容は委託先の任意とするが、業務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、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
※発生した場合は、すぐに検知でき、報告される

⑤ 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。

⑥ 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

⑦ 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

⑧ 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) 標準化

脆弱性対策について、以下の管理を行う。

管理状況については PMDA 標準様式を使用する。

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。

※「納品書添付用データフォーマット」のソフトウェア関連項目を元に、標準様式「脆弱性管理対象ソフトウェア一覧」と作成する。

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

④ 定期的(月次)報告時

・各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、「脆弱性管理対象ソフトウェア一覧」を使用し報告する。
(内容に更新があった際は速やかに報告する)

・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。

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) 標準化

特権（高権限）IDについて、以下の管理を行う。

①特権ID(システム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

本要領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3 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	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。

			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。 また受託者の管理区域内のバックアップテープ等の可搬記憶媒体についても、管理（受領、返却、廃棄、等）の内容を台帳に記録し、証跡を保管すること。	情報セキュリティ遵守状況は月次で報告すること。 可搬記憶媒体の棚卸と合わせて実施すること。
		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。