非機能要件定義書

[GMP/GCTP 品質関連情報システム]

目次

1. はじめに

1.1. 本書の位置付け

近年の医薬品に関する供給不足問題を受け、独立行政法人医薬品医療機器総合 PMDA（以下、「PMDA」という。）は品質問題・供給問題に対しての課題解決に向けた「GMP/GCTP 品質関連情報システム」の開発を企画している。

本システムにより、品質の見える化、品質の価値化の推進に寄与する情報発信、規制当局間の連携強化等効率的な監視・指導体制を構築し、国民の皆様への良質で安価な医薬品の継続的な流通と安全・安心の提供及びその環境の実現を目指す。

上記を踏まえ、本書において開発を企画しているシステムの非機能要件を定義する。

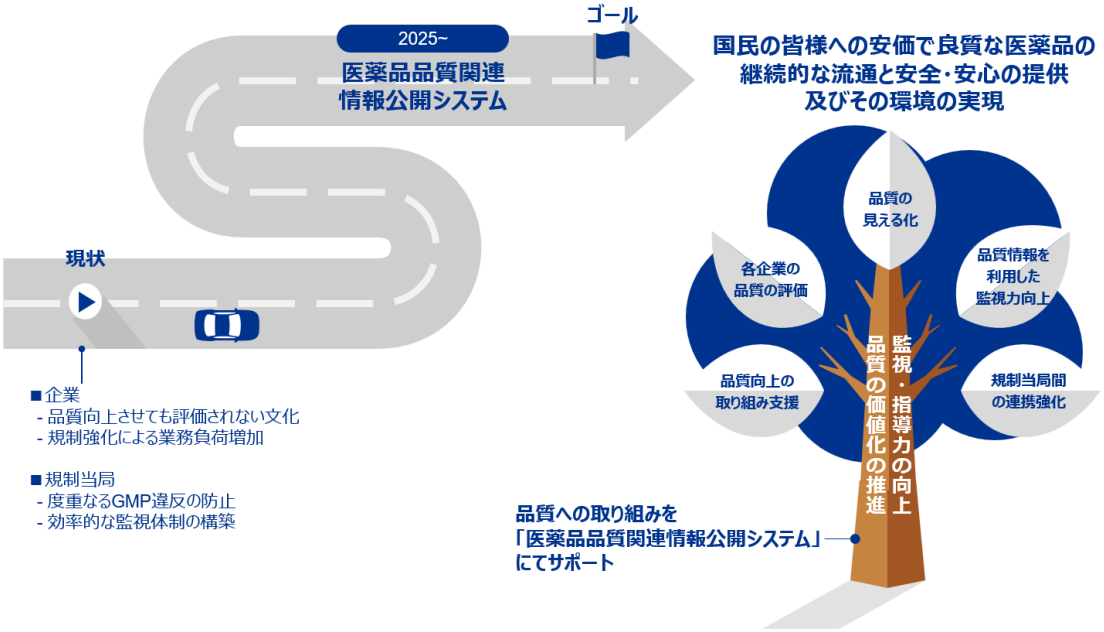


図 1 プロジェクトイメージ

1.2. 本書の読み手

本書の読み手は以下の方を中心として想定している。

- PMDA の調査関連職員
- 厚生労働省の所管部門職員
- 都道府県の調査関連職員
- 本システムをご利用いただく事業者
- 本システムを開発いただく開発事業者
- その他関連する事業者等

1.3. 前提事項

本業務要件定義書に係るドキュメントの位置づけに対しては下記の通り。

表 1 ドキュメント概要説明

ドキュメント番号	ドキュメント名	概要説明
別紙 1	業務要件定義書	デジタル・ガバメント方針に則り、サービス・業務内容及び手順を具体化し、情報システムに求める要求を定めたもの。
別紙 1_付属書①	As-Is 業務フロー_[A01-1]施設調査（製造業者の許可要件）	職員の業務(As-Is)を示したフロー図
別紙 1_付属書②	As-Is 業務フロー_[A01-2]施設調査（外国製造業者の認定要件）	職員の業務(As-Is)を示したフロー図
別紙 1_付属書③	As-Is 業務フロー_[A01-3]GMP 適合性調査（国内・海外）	職員の業務(As-Is)を示したフロー図
別紙 1_付属書④	As-Is 業務フロー_[A01-6]治験薬 GMP の適合性調査（国内）	職員の業務(As-Is)を示したフロー図
別紙 1_付属書⑤	As-Is 業務フロー_ [A01-8]立入検査（国内・海外）	職員の業務(As-Is)を示したフロー図
別紙 1_付属書⑥	As-Is 業務フロー_ [A03-1]不備事項蓄積・分析業務	職員の業務(As-Is)を示したフロー図
別紙 1_付属書⑦	To-Be 業務フロー_ [A00-1]業務共通	職員の業務(To-Be)を示したフロー図
別紙 1_付属書⑧	To-Be 業務フロー_ [A00-2]メンテナンス業務	職員の業務(To-Be)を示したフロー図
別紙 1_付属書⑨	To-Be 業務フロー_ [A00-3]外部データ取り込み	職員の業務(To-Be)を示したフロー図
別紙 1_付属書⑩	To-Be 業務フロー_ [A01-1]施設調査（製造業者の許可要件）	職員の業務(To-Be)を示したフロー図
別紙 1_付属書⑪	As-Is 業務フロー_ [A01-2]施設調査（外国製造業者の認定要件）	職員の業務(To-Be)を示したフロー図
別紙 1_付属書⑫	As-Is 業務フロー_ [A01-3]GMP 適合性調査（国内・海外）	職員の業務(To-Be)を示したフロー図
別紙 1_付属書⑬	As-Is 業務フロー_ [A01-6]治験薬 GMP の適合性調査（国内）	職員の業務(To-Be)を示したフロー図
別紙 1_付属書⑭	As-Is 業務フロー_ [A01-8]立入検査（国内・海外）	職員の業務(To-Be)を示したフロー図
別紙 1_付属書⑮	As-Is 業務フロー_ [A03-1]不備事項蓄積・分析業務	職員の業務(To-Be)を示したフロー図

ドキュメント番号	ドキュメント名	概要説明
別紙 1_付属書⑯	As-Is 業務フロー_ [A03-3]都道府県 GMP 調査	職員の業務(To-Be)を示したフロー図
別紙 2	機能要件定義書	デジタル・ガバメント方針に則り、機能全体構成や概要、機能間のつながりを示す。機能詳細一覧や画面詳細一覧の考え方等を示すもの。
別紙 2_付属書①	業務・機能対応一覧	業務と機能要件(画面・帳票があるものは画面・帳票情報も含む)の関係を定めたもの。
別紙 2_付属書②	機能要件一覧	業務の中でシステム機能化する機能を一覧化したもの。機能は画面・帳票・外部 IF を包含する概念とする。
別紙 2_付属書③	画面要件一覧	機能の中で画面入力や出力が必要なものを一覧化したもの。画面表示の項目の詳細までは基本的に定義せず概要に留める。
別紙 2_付属書④	帳票要件一覧	機能の中で帳票出力が必要なものを一覧化したもの。
別紙 2_付属書⑤	外部インタフェース要件一覧	機能の中で外部 IF との連携が必要なものを一覧化したもの。
別紙 2_付属書⑥	静的データモデル案	新システムを利用するデータモデルを ER 図で示す。
別紙 2_付属書⑦	動的データモデル案	各機能要件一覧に対して、関連する静的データモデルのデータ案に対しての CRUD 処理を示す。
別紙 2_付属書⑧	データ要件一覧	データモデル、データ定義、データの利活用方法、オープンデータの範囲と方法、データ項目の標準化等、データに関する要件を一覧化する。
別紙 2_付属書⑨	システム権限一覧	機能ごとのシステム権限を一覧化したもの。
別紙 2_付属書⑩	画面設計ガイドライン	画面設計における全体ガイドラインをまとめたもの。
別紙 2_付属書⑪	画面イメージ補足	定義した画面等の中でイメージが決まったものを補足するもの。
別紙 2_付属書⑫	システム構成図案	機能要件、非機能要件に対して新システムで必要なシステム図、機能補足を示す。
別紙 2_付属書⑬	画面遷移図	新システムの画面遷移をまとめたもの。
別紙 3	非機能要件定義書	稼働環境やサービス・業務を円滑に開始するためのユーザ教育等、情報システ

ドキュメント番号	ドキュメント名	概要説明
		ムを稼働・運用する上で必要となる機能以外の要件を示す。

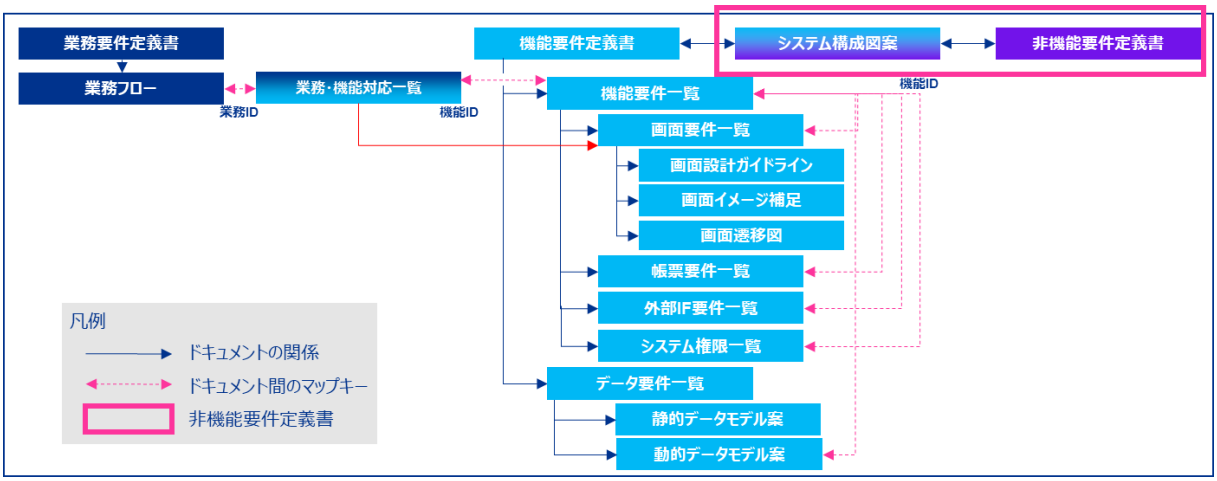


図 2 各ドキュメントの位置づけ

2. ユーザビリティ及びアクセシビリティに関する事項

2.1. 情報システムの利用者の種類、特性

情報システムの利用者の種類・特性は下記の通りである。なお、利用者区分に応じた情報システム機能の詳細については、「別紙２_機能要件定義書」の「別紙 2_付属書⑨ システム権限一覧」を参照すること。

表 2 情報システムの利用者区分等

No.	利用者区分	利用者の種類	特性
1	業務システム機能利用者	行政ユーザ（PMDA 職員）	対象業務に対しての経験が高い。
2	業務システム機能利用者	行政ユーザ（厚生労働省/都道府県職員）	ジョブローテーションにより数年で担当者が変わる。
3	システム運用者	運用事業者	IT リテラシーが高い。

2.2. ユーザビリティ要件

ユーザビリティ要件は下記の通りである。

表 3 ユーザビリティ要件

No.	ユーザビリティ分類	ユーザビリティ要件	補足
1	画面の構成	• 何をすればよいかが見て直ちに分かるような画面構成にすること。 • 無駄な情報、デザイン及び機能を排し、簡潔でわかりやすい画面にすること。 • 十分な視認性のあるフォント及び文字サイズを用いること。 • 画面の大きさや位置の変更ができること。 • タブレットやスマートフォンからのアクセスが想定されることから、アクセスした端末に合わせて適切な画面構成で表示されること。	別紙 2_付属書⑩_画面設計ガイドラインを参照のこと。
2	操作方法の分かりやすさ	• 無駄な手順を省き、最小限の操作、入力等で利用者が作業できるようにすること。 • 画面上で入出力項目のコピー及び貼付けができること。 • 業務の実施状況によっては、ショートカットや代替入力方法が用意されること。（例えば、片手だけで主要な操作が完了することが求められたり、マウスを利用することが困難であったりする場合が考えられる）。	別紙 2_付属書⑩_画面設計ガイドラインを参照のこと。
3	指示や状態の分かりやすさ	• 操作の指示、説明、メニュー等には、利用者が正確に内容を理解できる用語を使用すること。	別紙 2_付属書⑩_画面設計ガイドラインを参

No.	ユーザビリティ分類	ユーザビリティ要件	補足
		• 必須入力項目と任意入力項目の表示方法を変える等各項目の重要度を利用者が認識できるようにすること。 • システムが処理を行っている間、その処理内容を利用者が直ちに分かるようにすること。	照のこと。
4	エラーの防止と処理	• 利用者が操作、入力等を間違えないようなデザインや案内とすること。 • 入力内容の形式に問題がある項目については、強調表示する等、利用者がその都度その該当項目を容易に見つけられるようにすること。 • 電子申請等については、確認画面等を設け、利用者が行った操作又は入力の取消し、修正等が容易にできるようにすること。 • 重要な処理については事前に注意表示を行い、利用者の確認を促すこと。 • エラーが発生したときは、利用者が容易に問題を解決できるよう、エラーメッセージ、修正方法等について、わかりやすい情報提供をすること。	別紙 2_付属書⑩_画面設計ガイドラインを参照のこと。
5	ヘルプ	• 利用者が必要とする際に、ヘルプ情報やマニュアル等を参照できるようにすること。	別紙 2_付属書⑩_画面設計ガイドラインを参照のこと。

2.3. アクセシビリティ要件

アクセシビリティ要件は下記の通り。

表 4 アクセシビリティ要件

No.	アクセシビリティ分類	アクセシビリティ要件	補足
1	基準等への準拠	• 公表システムとして公益性の高い情報システムであるため、日本産業規格 JIS X8341 シリーズ、「みんなの公共サイト運用モデル」（総務省）等に従い、アクセシビリティを確保した設計・開発を行うこと。	—
2	指示や状態の分かりやすさ	• 色の違いを識別しにくい利用者（視覚障害者等）を考慮し、利用者への情報伝達や操作指示を促す手段はメッセージを表示する等とし、可能な限り色のみで判断するようなものは用いないこと。	—
3	言語対応	• 本情報システムでは、日本語のほか、英語対応を行うこと。	—

3. システム方式に関する事項

3.1. 目的

システム方式要件は、本システム（プラットフォーム及び付随する基盤、サービスを指す）全体の概要、及び本システムに求められる全体方針を整理、定義したものであり、設計工程において、物理的な構成等とともに、詳細化されるものとする。

3.2. 情報システムの構成に関する全体方針

情報システムの構成に関する全体方針として、以下の点に留意し設計を進めること。

（1）システムアーキテクチャ

システムアーキテクチャに係る要件は下記の通り。

- Web アプリケーションアーキテクチャを前提とすること。
- アプリケーションのステート管理は、疎結合／高拡張性の実現に向けて、サーバステートレスを基本とした設計を実施すること（SaaS を利用しない場合）。
- フロントエンド／バックエンド間の通信は、REST API による設計を実施すること（SaaS を利用しない場合）。

（2）アプリケーションプログラムの設計方針

アプリケーションプログラムの設計方針に係る要件は下記の通り。

- システムを構成する各コンポーネント（特定の単位で集約されたソフトウェアの機能群）は疎結合な構造となるよう設計すること。また、各コンポーネントの標準化・部品化を進めることで、再利用性を確保すること。
- 開発生産性向上のため、遷移制御、トランザクション制御、ログ出力等の業務処理とは直接関係のない機能を共通機能として実現すること（SaaS を利用しない場合）。

（3）ソフトウェア製品の活用方針

ソフトウェア製品の活用方針に係る要件は下記の通り。

- ベンダロックインを回避するため、広く市場に流通し、十分な利用実績を有するソフトウェア製品を採用すること。
- ソフトウェア製品ベンダによる長期のサポートサービスが提供可能な製品であること。
- SaaS を利用する場合、代替手段等が検討できる製品とすること。

- SaaS を利用しない場合、オープンソースソフトウェア（以下、「OSS」という。）製品を可能な限り活用すること。また、以下の点に留意すること。
  - ✓ ソースコードが無償で公開されており、誰に対しても改良や再配布を行うことが許可されている製品であること。
  - ✓ 十分なサポートサービスが提供されていること。

（４）システム基盤の方針

システム基盤の方針に係る要件は下記の通り。

- クラウド・バイ・デフォルト原則に則り、クラウドサービスの利用を基本とすること。
- マネージドサービスの利用を基本とし、外部連携先システムとの連携等やむを得ない場合を除き、仮想サーバや個別ソフトウェア製品の利用は回避すること。
- 特定の業務／機能に特化してその他のクラウドプラットフォーム又はクラウドサービスを利用する場合、「政府情報システムのためのセキュリティ評価制度（ISMAP）」に登録されたプラットフォーム／サービスの利用を原則とすること。
- 情報資産は、PMDA から特段指示のない限り、日本国内に保管されること。
- SaaS やその他 PaaS/IaaS 等を必要に応じて組み合わせることを可とする。システム利用の増加等に応じて、柔軟にリソース等を調整し、構築・運用コストを最適化できること。SaaS を利用する際にはサービス終了の可能性を考慮し、システムの選定を行うこと。

3.3. データ連携方針

本システムでは外部連携先との情報連携を行う。データ連携方針に係る要件は下記の通り。

（1）外部連携先システムとの連携方式

外部連携先システムとの連携方式に係る要件は下記の通り。

- 外部連携先システムとの連携パターンは、「別紙 2_付属書⑤外部インタフェース一覧」を参照すること。
- 本システム稼働後に生じる改修対応等も見据えた外部連携に係る基本方針は下記の通り。

表 5 外部連携に係る基本方針

No.	項目名	方針
1	インタフェースの種類	• REST API の採用を優先すること。 • REST API を採用することが出来ない場合、可能な限り HTTPS、SFTP 等の汎用的なプロトコルを利用すること。 • 上記でも実現不可である場合、現行システムの仕様を踏まえ、個別仕様の連携方式（メッセージキューイング、個別ツール、SCP、電磁的記録媒体の授受等）を採用すること。
2	インタフェースの構築方法	• API 連携は、API ゲートウェイをクラウド上に構築し、実現すること。 • API ゲートウェイが対応していないプロトコルを利用する場合、可能な限りマネージドサービスを利用すること。 • 個別の連携方式を採用せざるを得ない場合、クラウド上に IaaS（仮想サーバ）を構築し、連携機能を構築すること。ただし、電磁的記録媒体の授受等による連携の場合を除く。
3	インタフェースが利用する物理的通信回線の選択方針	• 本システムと外部連携先システムが異なるクラウドプラットフォームを利用する、又は外部連携先システムがクラウド環境ではない場合、通信の信頼性、セキュリティ等を確保する観点から、閉域網（広域 LAN 又は IP-VPN）を利用すること。ただし、外部連携先システム側が閉域網接続に対応していない等の制約がある場合は、インターネット経由での接続とすること。なお、本システムと外部連携先システムがインターネット経由での接続となる場合は、可能な限り VPN 接続又は HTTPS 等の暗号化通信を前提とすること。
4	回線に関する詳細要件	• 可能な限り帯域が保証される回線を利用すること。 • 必要に応じて QoS 等を利用し、通信の信頼性を確保すること。 • 情報漏えいや改ざん等を防止するため、暗号化、ファイアウォールの導入を実施すること。
5	検証環境の利用方針	• 外部連携先システムが検証環境を備える場合、本システムが備える検証環境と回線を接続し、外部連携先システムと実施する検証作業等に利活用可能な環境を整備すること。

3.4. 開発方式及び開発手法

開発方式及び開発手法に係る要件は下記の通り。

(1) 開発方式

開発方式に係る要件は下記の通り。

- SaaS の利用や、既に開発されている資産を有効活用しリスクやコストを低減すること。その際には開発言語及び開発フレームワークは設計・開発工程において決定すること。
- 開発効率を向上させる観点から、可能な限り開発フレームワークの利活用を検討すること。
- 開発フレームワークは、広く市場に流通し利用実績を十分に有するものを選定すること。また、セキュリティ対策やシステム構成、サポート期間等にも留意すること。さらに、利用する期間全体に亘り、可能な限り最新のバージョンを適用すること。
- フロントエンド開発は、一般的な Web 技術を利用すること。
- バックエンド開発で使用する開発言語、開発フレームワークは、最新の技術動向、開発事業者の実績、業務特性等を考慮し決定すること。
- 画面、業務ロジック、データアクセスを極力疎結合な構造とし、各々の変更における影響範囲を極小化すること。

(2) 開発手法

開発手法に係る要件は下記の通り。

- システム開発手法はウォーターフォール型開発を基本とすること。
- 限られた期間／費用の中で効率的に設計・開発工程を推進することができるよう、必要に応じてパイロット開発検証等の手法を取り入れること。
- 画面設計等を効率的に推進することができるよう、必要に応じてプロトタイピングやアジャイル開発等の手法を取り入れること。

3.5. システム構成案

新システムのシステム構成案図は下記の通り。ただし要件を実現する範囲において異なるシステム構成を取ることは問題がないものとする。

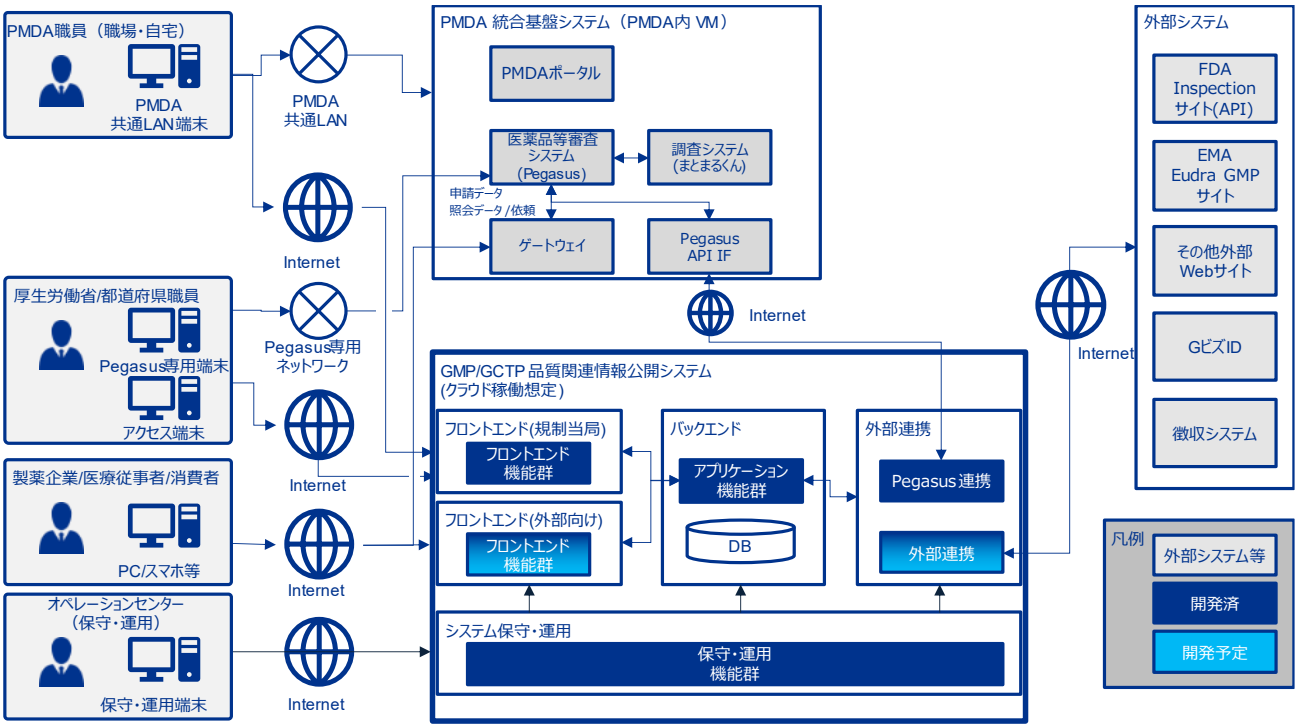


図 3 システム構成案

各システムの概要は下記の通り。

表 6 システム構成案の要素

名称	概要
GMP/GCTP 品質関連情報システム	本システム。GMP 調査等で得られる製造所情報を PMDA や厚生労働省、都道府県職員にて管理し、その中で公開すべきと考えられる情報を公開する。 GMP 調査等で必要となる申請情報は PMDA イントラシステム上で動作する医薬品等審査システム（以下、「Pegasus」という。）等のシステムと連携し、Cloud 上の本システムにて取得する。 フロントエンド部（業務用、公開用）、バックエンド、外部連携、システム保守・運用部で構成予定。
PMDA イントラシステム	PMDA の職員が PMDA の共用 LAN 等でアクセスできるイントラシステム。 医薬品審査システムの Pegasus、及び調査記録補助システムのまとまるくんもイントラシステム上で動作する。 厚生労働省職員や都道府県職員は、Pegasus 専用端末及び、Pegasus 専用ネットワークと呼ばれる専用ネットワークを利用し、イントラシステム内

名称	概要
	Pegasus にアクセスする。
外部システム	インターネット上に配置され、本システムと連携を行う別サービス。

また、本システムのシステム機能概要図（Level2 機能単位）は下記の通り。詳細に関しては機能要件定義書（本編）「別紙 2_機能要件定義書」、機能要件一覧「付属書②_機能要件一覧」を参照されたい。

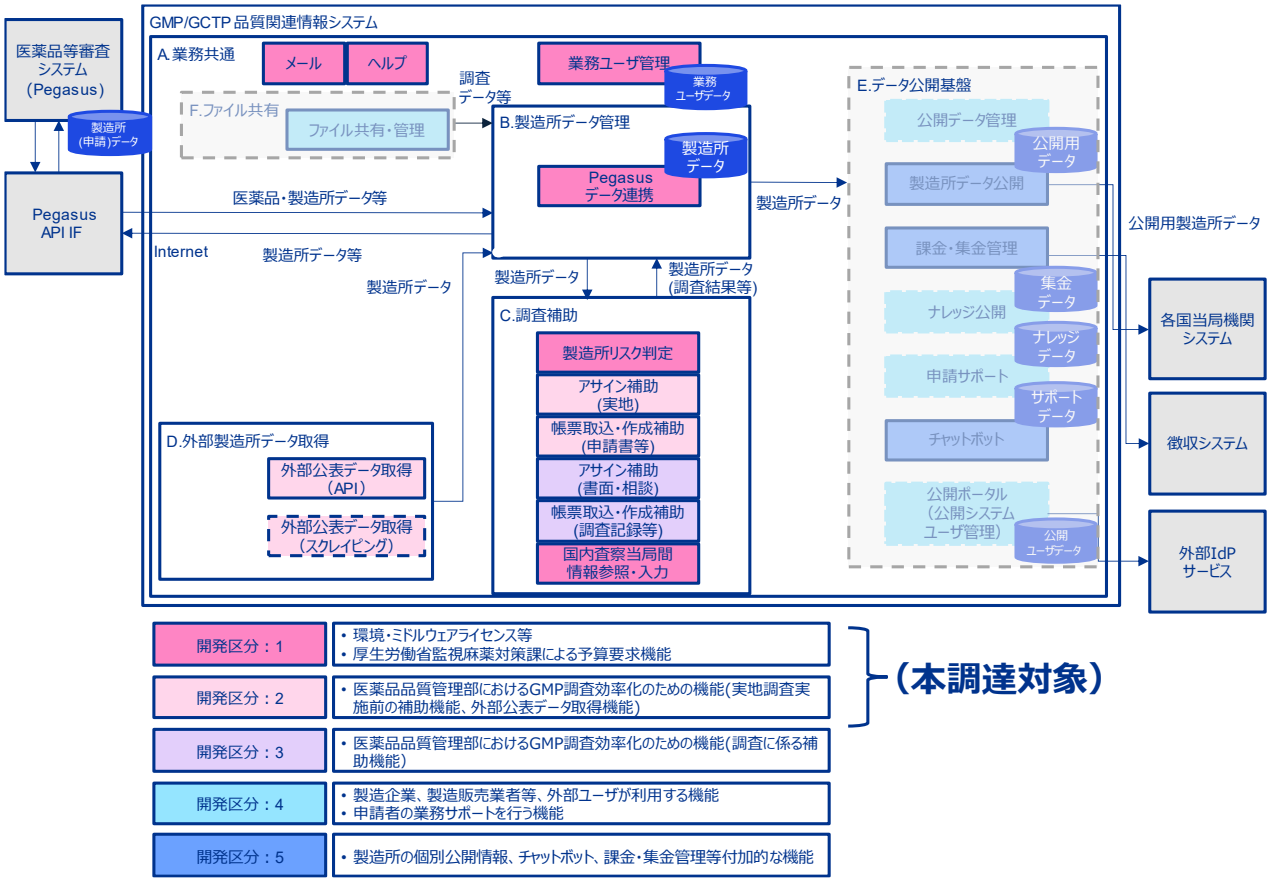


図 4 システム機能概要図

4. 規模に関する事項

4.1. データ量

本調達で想定される新システムにおけるデータ量は下記の通り。

表 7 想定データ量

No.	データ区分	データ量	補足
1	[A:業務共通] 業務システムユーザ認証情報	[新規] • PMDA、都道府県、厚労省の職員約 500 名分	—
2	[B:製造所情報管理] 製造所単位情報（規制当局用・公開用）（移行予定データ）	[移行] • 国内外製造所単位関連情報（管理データ）（2500 製造所分）：計 12G 程度 [増分] • 年間 1G 程度	Pegasus 関連データとして取得 B:製造所情報管理と、E:データ公開基盤は疎の関係にするため、それぞれデータを保持する
3	[D:外部製造所データ取得] 製造所単位情報（規制当局用・公開用）（新システムにて新規取得予定のデータ）	[新規、増分] • （国内外製造所単位（2,500 製造所分）情報 (API+スクレイピング)）×継続年数	取得製造所単位データは高々1k 程度

4.2. 処理件数

本調達における想定の処理件数は下記の通り。

表 8 想定処理件数

No.	項目	処理件数		補足
		定常時	ピークの特性	
1	[B:製造所情報管理] 製造所情報の登録	150 件/年	なし	海外も含め製造所の新規登録の件数を定常時に記載する
2	[B:製造所情報管理] 調査申請情報の登録	約 2,000 件/年	承認時期 （1 月と 7 月）	申請件数
3	[C:調査補助] 製造所調査情報の登録	20 件/月	なし	実地調査の実施回数/月を定常時の件数とするデータは B:製造所情報管理下の情報として管理される
4	[C:調査補助] 調査員情報の登録	10 件/年	なし	導入時に 50 件程度。新規登録は年 10 件程度の想定
5	[D:外部製造所データ取得] 外部公開情報の登録	FDA/EMA 1 回/日	なし	FDA/EMA の更新頻度での情報の登録の件数

4.3. 利用者数

表 9 想定利用者数

No.	利用者区分	利用者数	補足
1	行政ユーザ	約 500 人 （9:00～18:00）	業務システム部分の利用
2	情報システム管理者	約 10 人程度 24h	―

5. 性能に関する事項

5.1. 応答時間

表 10 応答時間等

No.	設定対象	指標名	目標値	応答時間達成率	補足
1	システム全体 オンライン処理	レスポンスタイム	参考値として現行の Pegasus の値を記載する。設計・開発時に調整を行うこと 画面応答（参照系）3 秒 画面応答（更新系）3 秒 （※10 秒） DB 検索結果表示 3 秒 （※10 秒） DB 更新処理 3 秒 （※10 秒） 文書ファイル表示 5 秒 （※10 秒） 文章ファイル検索結果表示 3 秒（※10 秒） 文章ファイル全文検索結果表示 3 秒（※30 秒） ファイル更新（アップロード、ダウンロード）10 秒以内 （※60 秒） ※（）内の値は、VPN 経由のアクセス、100 件以上のダウンロード、1MB 以上のファイル送受信、複雑な組合せでの検索等の場合の目標値	遵守	—
2	システム全体 バッチ処理	バッチ処理時間	翌日のオンライン処理開始までに処理が完了していること	遵守	—

6. 信頼性に関する事項

6.1. 可用性要件

可用性要件のうち、本調達の稼働率に関しての要件は下記の通り。

表 11 稼働率要件

No.	設定対象	指標名	目標値	補足や対応等
1	B.製造所データ管理	稼働率	99.9%	• 単一障害点となりうる各機能群とのハブとなる機能群。 • 新システムの各機能群との独立性は保ちつつ動作をさせるようにする等の対応が望ましい。 • （連携機能側に障害があったとしても機能群としては変わらず連携状態等を表示したうえで過去に連携されたデータで稼働する等）機能としての対策で冗長化等のコストを抑える等の対応も検討すること。 • 業務ユーザ稼働時間 9:00-18:00 稼働で問題なし。
2	C.調査補助	稼働率	99.9%	• 1 からの連携が必要であり、1 の稼働率に影響される。 • 業務ユーザ稼働時間 9:00-18:00 稼働で問題なし。
3	D.外部製造所データ取得	稼働率	99.9%	• バッチやスクレイピング処理であり 1 にデータを流し込むのみのため影響は少ない、取得する対象データの更新頻度も 1 日に一回程度の予定。 • 業務ユーザ稼働時間 9:00-18:00 稼働で問題なし。

その他の可用性に係る対策は、下記の通り。

- 365 日 24 時間の運用を目標とするが、一部の機能群は週末の稼働を止め運用費を低減させること等が可能な構成とすること。
- 通常時の負荷分散及び障害発生時の縮退運転を可能とすること。
- 障害発生時にも業務が継続できるよう待機系への切替えや、最低限の業務継続を可能とすること。
- 障害時のデータ消失対策として、サーバ上のデータベースファイルは、冗長構成をとるものとすること。
- 業務に用いるデータのバックアップ処理は業務への影響を排除した設計とすること。
- 異常な入力や処理を検出しデータの滅失や改変を防止する対策を講ずること。

- 処理の結果を検証可能とする為、ログ等の証跡を残すこと。
- 標準メンテナンスは、開始から 5 日前までに連絡すること。
- 本システムを構成するサーバ、ネットワーク機器及びネットワーク経路を冗長化し、単一障害点（SPOF）を回避すること。
- 本システムに係る運用・保守上の人的ミスに起因する障害が本システムの可用性に影響を与える事態を未然に防止するため、「17．運用に関する事項」及び「18．保守に関する事項」を踏まえ、適切な手順書を整備すること。また、定型的なオペレーションは自動化すること。
- フェールソフトの観点から、障害が発生したコンポーネントを切り離すことによりサービス全体を停止せずに運用可能とすることを考慮する。そのために各種障害発生時の影響を回避又は局所化し、原則として自動縮退運用に対応すること。

6.2. 完全性要件

完全性要件は下記の通り。

- 自動でデータベースファイルのバックアップを取得し、必要に応じ手動バックアップも可能であること。
- 異常な入力や処理を検出し、データの滅失や改変を防止する対策を講ずること。
- 処理の結果を検証可能とするため、ログ等の証跡を残すこと。
- データの複製や移動を行う際に、データが毀損しないよう、保護すること。
- データの複製や移動を行う際に、その内容が毀損した場合でも、毀損したデータ及び毀損していないデータを特定するための措置を行うこと。
- 電子データの送受信を行う際には、電子署名やタイムスタンプを用いることで偽造等から保護することが可能であること。
- システム運用中に障害・トラブル等が発生した際に原因追求が可能となるよう、操作ログやアクセスログ等のシステムログ、例外事象の発生に関するログ等を取得・保管し、必要な時に出力可能とすること。

7. 拡張性に関する事項

7.1. 性能の拡張性

性能の拡張性についての要件は下記の通り。

- 利用者数の増加に向けて、処理能力やデータ保存領域を拡張するための CPU、メモリ、ハードディスク等、導入後の拡張性を有すること。
- システムユーザ数、データボリューム等の増大、ユーザ別業務システムの追加にも容易に対応可能な拡張性を有すること。
- サーバ負荷軽減の為、分散処理可能な構成であること。
- クラウドサービスを利用する場合、業務の繁閑等に柔軟に対応し、リソース（サーバ、CPU、メモリ、ストレージ等）の実際の使用量に合わせて最適化を図ることが可能なクラウドサービスを選定すること。その際、採用するクラウドサービスと対象業務の性質により、具体的に利用するサービス（例：オートスケール、PaaS 等）に係る最適な構成は異なってくると考えられるところ、実際の構成の検討に際しては、可能な限り当該クラウドサービスに係るクラウドサービスプロバイダにも相談し、運用コストの低減を図った上、要件に最も適した（当該クラウドサービスにおけるベストプラクティスに合致又は近似である）構成の選定、設計（運用・保守設計を含む。）を図ること。

7.2. 機能の拡張性

機能の拡張性についての要件は下記の通り。

- 政策の変化に合わせて、PMDA 内外の接続先システムとのインタフェース、バッチ処理の追加、及びユーザ種別の追加対応ができ、開発済み機能群に対しての影響、テスト等が少なくなる構成を目指すこと。
- 機能の追加や、新たな機能開発の必要が生じることが想定されることから、将来開発する機能も含めた機能間の連携が十分に図られるようにすること。
- 利用者ニーズ及び業務環境の変化等に最小コストで対応可能とするため、本システムを構成する各コンポーネント（ソフトウェアの機能を特定単位で分割したまとまり）の再利用性を確保すること。
- 機能の追加や、新たな機能開発の必要が生じることが想定されることから、将来開発する機能も含めた機能間の連携が十分に図られるようにすること。
- 機能、画面、帳票等において固有の ID・項目名等を付する際には、中長期的な重複等を避けつつ可読性を担保するため、あらかじめ系統だった命名ポリシーを策定すること。その際、一見して意味の分からない命名は行わず、同種の項目を複数設定する必要がある場合にはそれぞれの項目の性質の違いが分かるように留意すること。
- アプリケーションやインフラの設計にあたっては、将来の拡張時に効率良く対応ができるように、設定情報の外部化や一元化、機能の共通化等に努めること。

- 本調達で構築するシステムでは、比較的短期間での機能の追加が求められることが想定されることから、簡易な操作で機能の追加が可能であること。また、できるだけ簡潔なアーキテクトかつ簡易な構成とすること。なお、IaaS/PaaS については単一クラウドサービスでの構築を想定している。

8. 上位互換性に関する事項

8.1. 上位互換性

上位互換性についての要件は下記の通り。

- クライアント OS のバージョンアップに備え、OS の特定バージョンに依存する機能が判明している場合は、その利用を最低限とすること。
- 契約期間中にアプリケーション稼働環境として導入しているソフトウェアのバージョンアップが発生した場合は、原則、バージョンアップ後の環境を前提として開発を行うこと。なお、バージョンアップの決定時期によって対応が困難な場合には、PMDA と協議の上、その指示に従うこと。
- バージョンアップについて、技術的な問題等がある場合は、PMDA と協議の上、その指示に従うこと。
- OS やブラウザのバージョンアップ等に伴い、大幅な改修が見込まれる場合は、対応要否や範囲等を別途 PMDA と協議の上、決定すること。
- 特定の Web ブラウザに依存する機能が判明している場合は、その利用を最低限とすること。また、主な利用環境として想定する Web ブラウザを一定の範囲に限る場合でも、対象ブラウザのバージョンアップに備え、対象ブラウザの特定バージョンに依存する機能が判明している場合は、その利用を最低限とすること。
- Web ブラウザ及び実行環境等のバージョンアップの際、必要な調査及び作業を実施することで、バージョンアップに対応可能な情報システムとすること。
- システムの構成にクラウドサービスのマネージドサービスを採用する場合、軽微なバージョンアップについては自動適用を前提とする。大規模なバージョンアップについては、アプリケーションへの影響を事前に精査し、適用を検討すること。

9. 中立性に関する事項

9.1. 中立性

中立性についての要件は下記の通り。

- 提供するソフトウェア等は、原則としてオープンなインタフェースを利用して接続又はデータの入出力が可能であること。
- サービス提供開始後のシステム更改の際に、移行の妨げや特定の装置や情報システムに依存することを防止するため、原則として情報システム内のデータを標準的な形式で取り出すことができるものとすること。
- 特定の事業者に依存することなく、他者による保守、追加開発が可能なシステム構成であること。
- OS やブラウザのバージョンアップ等に伴い、大幅な改修が見込まれる場合は、対応要否や範囲等を別途 PMDA と協議の上、決定すること。
- 本システムを構成するサーバ、ソフトウェア、アプリケーションとして、市場で広く利用されている製品群及びクラウドサービスが提供する標準サービスを除き、原則として特定事業者の技術に依存しないオープンな技術仕様に基づくものを選択すること。なお、開発フレームワークを用いる場合には、上記に加え、後継事業者への業務への引継ぎに支障が生じないよう開発環境構築に必要なドキュメント類及びプログラムの全ソースを提供すること。
- 移行データに関する文字コード等は以下に従うこと。
- 取り扱う日本語文字集合の範囲： JIS X 0213
  - ✓ 文字コード： ISO/IEC 10646
  - ✓ 文字の符号化形式： UTF-8

10. 継続性に関する事項

10.1.本書の位置付け

継続性についての要件は下記の通り。

10.2.想定リスク

(1)地震、火災、風水害等、攻撃等による直接的なセンター設備及びシステムの損壊
(2)センター周辺のライフライン（電力、通信、交通等）の機能不全による情報システムの長時間停止
(3)パンデミック、及び人員や交通機関の被災等によるセンターの運用者不在

10.3.目標値

継続性の目標値に係る要件は下記の通り。

表 12 継続性の目標値に係る要件

No.	要件詳細
1	[Pegasus 同等の想定] （参考値）Pegasus の継続性 ◇データ・サーバ障害(非災害時。データ損失、ネットワーク障害等による異常終了等) RPO（目標復旧時点）：前回取得バックアップ時点 RTO（目標復旧時間）：10 時間以内 ◇災害（災害時。独自の災害対策環境は持たずバックアップから復旧させる） RPO（目標復旧時点）：前回取得バックアップ時点 RTO（目標復旧時間）：機器、データ等必要部材が揃った状態から 1 か月以内
2	予測できる障害（一時的な過負荷等）については、あらかじめ業務停止を回避するための対策を講ずること。また、単一障害発生時は業務停止せずに処理継続可能であること。
3	各構成要素について、故障等を検知した際、クラウドサービスの利用を前提として自動的に予備の環境へ切替える等、適切に冗長化を行い、特定の部分の障害によりシステム全体が停止してしまうような SPOF（単一障害点）を極力排除するよう、設計時に配慮すること。
4	アベイラビリティゾーン（以下「AZ」という。）については、マルチ AZ によって複数の AZ をまたいだシステム冗長化を実現し、可用性を高める方針とする。しかし、頻繁に AZ 間の通信が発生するアプリケーションについては、AZ 間のレイテンシが増幅し性能に影響を与える可能性がある。これらの性能面の影響を評価できるよう、設計・開発期間中の早い段階で性能面の影響を評価し、必要に応じてアプリケーション改修等の手段で性能改善への対応方針を確立すること。
5	バックアップツール バックアップ対象、頻度、バックアップデータへのアクセス権限及び保存期間といったバックアップポリシーを一元的に管理できる機能を持った、クラウドサービスプロバイダが提供するバックアップサービスを

No.	要件詳細
	できるだけ利用すること。なお、個別データの復旧にはデータベース等の PITR：Point In Time Recovery/Restore を実現できることが望ましい。
6	取得したバックアップは、データの損失リスクを回避することを目的として災害対策環境へ分散させる等の信頼性設計を行うこと。なお、災害対策環境は本番環境とは異なるリージョンに配置すること。各リージョンで利用可能な AZ は、物理的に十分に距離の離れた複数のデータセンタで冗長化が確保できること。
7	クラウドサービスのマネージドサービスにおけるバックアップ機能を有効に活用すること。なお、インスタンスを利用してサーバを立てる場合のバックアップ方式は、バックアップ＆リストア、コールドスタンバイ、ウォームスタンバイ、マルチサイトの 4 つのディザスタリカバリ方式のうち、目標復旧時間から考えて、コールドスタンバイ以上の構成を想定している。

11. 情報セキュリティに関する事項

11.1. 情報セキュリティ対策要件

情報セキュリティ対策についての要件は下記の通り。

- 最新の「独立行政法人 医薬品医療機器総合 PMDA サイバーセキュリティポリシー」に従い、必要な対策を講じることとする。
- 独立行政法人 医薬品医療機器総合 PMDA サイバーセキュリティポリシーは、サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 26 条第 1 項第 2 号に定める国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する 対策の基準である、「政府機関等の情報セキュリティ対策の運用等に関する指針」、「政府機関等の情報セキュリティ対策のための 統一規範」、「政府 機関等の情報セキュリティ対策のための統一基準」、「政府機関等の対策基準策定のためのガイドライン」に準拠するとともに、「厚生労働省情報セキュリティポリシー」及び「医療情報システムの安全管理に関するガイドライン」を参照し、政府機関 等の統一的・横断的な情報セキュリティ対策と同等以上のセキュリティ条件を確保するものである。
- 個人情報（「個人情報の保護に関する法律」第 2 条第 1 項に規定する情報をいう。以下、「個人情報」という。）の取り扱いに関し、個人情報保護に関する法令の趣旨に従えるよう設計し、取り扱い及び管理を行えるようにする。なお、技術的制約等により実現が特に困難である場合は、PMDA と協議の上、所要の代替措置をとることを条件に情報セキュリティ対策要件の詳細によらない対策を認める場合がある。

11.2.情報セキュリティ対策要件の詳細（機能詳細）

情報セキュリティ対策要件の詳細は下記の通り。

表 13 情報セキュリティ対策要件の詳細

No	セキュリティ機能	情報システムのセキュリティ対策	
		項目	要件の内容
1	主体認証	主体認証機能の導入	情報システムセキュリティ責任者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設けること。
2			情報システムセキュリティ責任者は、国民・企業と機関等との間の申請、届出等のオンライン手続を提供する情報システムを構築する場合は、オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定すること。
3			情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずること。
4		識別コード及び主体認証情報の管理	情報システムセキュリティ責任者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与し、管理するための措置を講ずること。
5			情報システムセキュリティ責任者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を速やかに講ずること。
6	アクセス制御	アクセス制御機能の導入	情報システムセキュリティ責任者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けること。
7			情報システムセキュリティ責任者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用すること。
8	権限管理	権限の管理	情報システムセキュリティ責任者は、主体から対象に対するアクセスの権限を適切に設定するよう、措置を講ずること。
9			情報システムセキュリティ責任者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずること。
10	ログ取得及びログ管理	ログの取得・管理	情報システムセキュリティ責任者は、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

No	セキュリティ機能	情報システムのセキュリティ対策	
		項目	要件の内容
			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を取得すること。
11			情報システムセキュリティ責任者は、情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理すること。
12			情報システムセキュリティ責任者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。
13	暗号化及び電子署名	暗号化機能・電子署名機能の導入	情報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の措置を講ずること。 (ア) 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。 (イ) 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。
14			情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定めること。 (ア) 職員等が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。 (イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。 (ウ) 暗号化及び電子署名に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。 (エ) 暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること。

No	セキュリティ機能	情報システムのセキュリティ対策	
		項目	要件の内容
15			情報システムセキュリティ責任者は、機関等における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な電子証明書を政府認証基盤（GPKI）が発行している場合は、必要に応じてそれを使用するように定めること。
16		暗号化・電子署名に係る管理	情報システムセキュリティ責任者は、暗号及び電子署名を適切な状況で利用するため、以下の措置を講ずること。 (ア) 電子署名の付与を行う情報システムにおいて、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全な方法で提供すること。 (イ) 暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズムの危殆化及びプロトコルの脆弱性にする情報を定期的に入手し、必要に応じて、職員等と共有を図ること。
17	ソフトウェアの脆弱性対策	ソフトウェアに関する脆弱性対策の実施	情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施すること。
18			情報システムセキュリティ責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上でとり得る対策がある場合は、当該対策を実施すること。
19			情報システムセキュリティ責任者は、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における脆弱性対策の状況を定期的に確認すること。
20			情報システムセキュリティ責任者は、脆弱性対策の状況の定期的な確認により、脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。
21	不正プログラム対策	不正プログラム対策の実施	情報システムセキュリティ責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入すること。 ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。
22			情報システムセキュリティ責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずること。

No	セキュリティ機能	情報システムのセキュリティ対策	
		項目	要件の内容
23			情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行うこと。
24	サービス不能攻撃対策	サービス不能攻撃対策の実施	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下本条において同じ）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うこと。
25			情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築すること。
26			情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること。
27	標的型攻撃対策	標的型攻撃対策の実施	情報システムセキュリティ責任者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずること。
28			情報システムセキュリティ責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）を講ずること。

12. 情報システム稼働環境に関する事項

本システムの稼働環境要件については、原則として調達仕様書に準ずるものとするが、設計工程で詳細化するものとする。

12.1.ソフトウェア要件

本システムのソフトウェア要件については、下記のとおり。

- 「拡張性に関する事項」、「中立性に関する事項」を踏まえたソフトウェアを導入すること。
- 既知の脆弱性が存在するソフトウェアをシステムの構成要素としないこと。
- システムを構成するソフトウェアについては、運用中にサポートが終了しないよう、サポート期間が十分に確保されたものを選定し、可能な限り最新バージョンを採用すること。古いバージョンを採用する場合は、ソフトウェアベンダのサポート期間内であることを前提とすること。
- 脆弱性が発見された時に、その情報を可能な限り早く入手でき、かつ可能な限り早く対応策を講じられること。

12.2.クラウドサービスの要件

「政府情報システムにおけるクラウドサービスの利用に係る基本方針」を踏まえて、クラウドサービスを利用する場合の要件は、下記の通り。

（１）情報システムの保護

- 情報資産を管理するデータセンタの物理的所在地が、日本国内であること。
- PMDA の指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。
- 障害発生時に縮退運転を行う際にも、情報資産が日本国外のデータセンタに移管されないこと。
- クラウドサービスの利用契約に関連して生じる一切の紛争は、日本の地方裁判所を専属的合意管轄裁判所とするものであること。
- 契約の解釈が、日本法に基づくものであること。
- クラウドサービス事業者の管理によって、情報資産に対し適法にアクセスし、その利用をコントロールできる事実上の地位を失うものでないこと。したがって、PMDA が要求する任意の時点又は契約終了時点において、情報資産を他の環境に移管させることができること。
- 法令や規制に従って、クラウドサービス上の記録を保護すること。
- 情報資産が残留して漏えいすることがないよう、必要な措置を講じること。
- 自らの知的財産権について、クラウド利用者に利用を許諾する範囲及び制約を、クラウド利用者に通知すること。

- 運用段階において、PMDA 又は PMDA の委託等を受けた第三者が行うクラウドサービス提供者への情報セキュリティの監査の受入れを認めること。又はクラウドサービス提供者が受けた情報セキュリティに係る外部機関による監査若しくは審査の内容及び結果を提示すること。

（２）技術的要件

クラウドセキュリティに関して、次のいずれかを取得していること。

- ISO/IEC 27017 又は ISMS（情報セキュリティマネジメントシステム）クラウドセキュリティ認証制度に基づく認証
- セキュリティに係る内部統制の保証報告書（SOC 報告書（Service Organization Control Report））

12.3.クラウドサービスの環境定義

本システムのクラウドサービスの環境は下記の通り。本システムの稼働環境は下記に示す環境を設計・開発事業者の負担と責任において用意し、本システムの構築、開発、テスト等を行うこと。本番環境以外は、必要な時のみの稼働を想定する。下記に加え、その他環境を追加する場合は、PMDA と協議の上、追加することとする。なお、設計・開発用の環境に関しては、設計・開発事業者の負担・責任として準備を行うこと。

表 14 クラウドサービス環境

No.	環境名	概要	アクセス制限	該当システム
1	本番環境	システムが本番稼働している環境	運用者 利用者	フロントエンド部（業務用） バックエンド部 外部連携部 システム保守・運用部
2	ステージング環境	本番環境に展開する前に動作確認テスト等を行う環境	運用者 設計・開発業者	フロントエンド部（業務用） バックエンド部 システム保守・運用部
3	検証環境	事業者の総合テスト等を行う環境	運用者 設計・開発業者	フロントエンド部（業務用） バックエンド部 外部連携部 システム保守・運用部

12.4. 本システムの利用環境

本システムは、業務システムを利用する PMDA 職員、厚生労働省職員、都道府県職員、システム管理を行う運用者等、複数の種類のユーザが複数の環境から利用することを前提とする。そのため利用する端末やブラウザについては Windows OS、macOS における Edge 、Chrome、Firefox 及び Android、iOS の Chrome、Safari の調達時点の最新バージョンに対応することとするが、詳細なバージョンやブラウザに制限が存在する場合は設計時に PMDA に確認の上決定すること。

また、本システムでのユーザと各ユーザが使用するネットワーク環境の想定は下記の通りであり、基本的にインターネットでの接続を想定している。設計・実装フェーズにて詳細検討を進めることを期待する。

ユーザ分類		利用環境		
		インターネット	PMDA共用LAN	Pegasus ネットワーク
業務システム利用者（行政）	PMDA職員	○	–	–
	厚生労働省職員	○	–	–
	都道府県職員	○	–	–
システム管理者	システム運用事業者	○	–	–

図 5 ユーザとネットワーク環境

12.5.利用環境で述べた各ネットワーク及び関連する認証に関して

(1)現行関連のネットワーク及び関連認証

利用環境で述べた各ネットワークの説明及び関連する認証方法は下記の通り。

- PMDA 共用 LAN

PMDA 共用 LAN とは、インターネットに接続されない PMDA 内部のイントラネットを表す。ユーザは PMDA 共用 LAN 端末を利用し、Windows のドメイン認証（共用 LAN AD）を行うことで共用 LAN に接続可能となる。共用 LAN AD は後述の Pegasus AD によって信頼されている。共用 LAN AD は Kerberos 認証を提供する。新システムでは直接 PMDA 共用 LAN を使ったネットワークパスはない。PMDA 職員が利用するネットワークは新システムで利用するためのインターネット接続（共用 LAN 端末の App を利用）と、共用 LAN を使った内部のサービス二つがあることを押さえておけばよいと考える。

- Pegasus ネットワーク

Pegasus ネットワークとは、厚生労働省や都道府県職員が Pegasus 等審査システムに接続する際に利用するネットワークを表す。Pegasus 等審査システムとは、本システムにおいても情報連携を行う、新薬や薬の審査等のためのシステムである”Pegasus”等を指す。厚生労働省・都道府県職員は Pegasus 専用端末を利用し、Pegasus 専用の認証（Pegasus AD）を行い、Pegasus ネットワークに接続する。新システムでは、厚生労働省・都道府県職員共にインターネット回線を経て別端末を利用しアクセスを行うため、Pegasus ネットワーク及び Pegasus 専用端末とは切り離して検討を進めること。

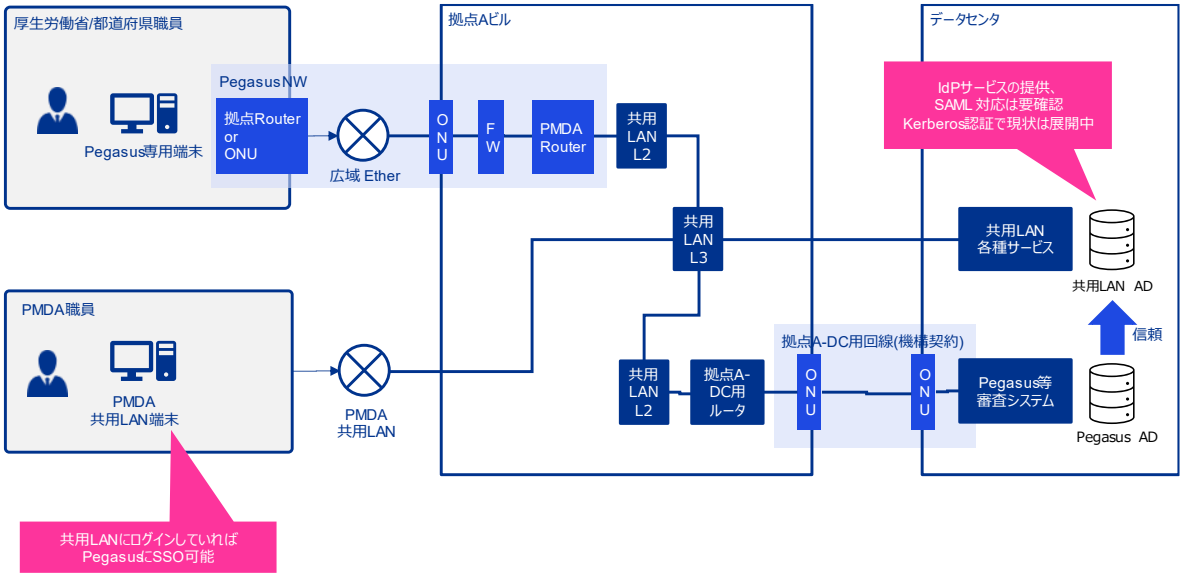


図 6 現行関連システムのネットワーク図と認証

(2)新システム関連ネットワーク関連

新システム関連で必要となるネットワークの説明は下記の通り。

- 新システム接続用インターネット回線

新システムは Cloud で動作させることを想定し、インターネット上にサービスを展開することとなる。Pegasus と情報のやり取りに関しては、Pegasus 側が新システムとの連携のために Pegasus API Server（仮）を開発し、インターネット上に公開し新システムが API call を行う予定である。ただしアクセス制御を IP レイヤにて Pegasus API Server（仮）側で行う想定であり、新システムでは運用を簡単にするため、固定 IP でのアクセスとなるようにネットワークアダプタ等を調整すること。詳細な Pegasus API Server（仮）との仕様調整を新システム側の設計・開発段階にて行い、設計・開発を進めること。また、新システムの公開に関して、新システムの Web アプリケーションのアドレスが xxx.pmda.go.jp などとなるように既に取得している PMDA 側のドメインネームサーバと連携し、ドメイン接続等を利用して PMDA の既存ドメイン名と統一できるように調整すること。

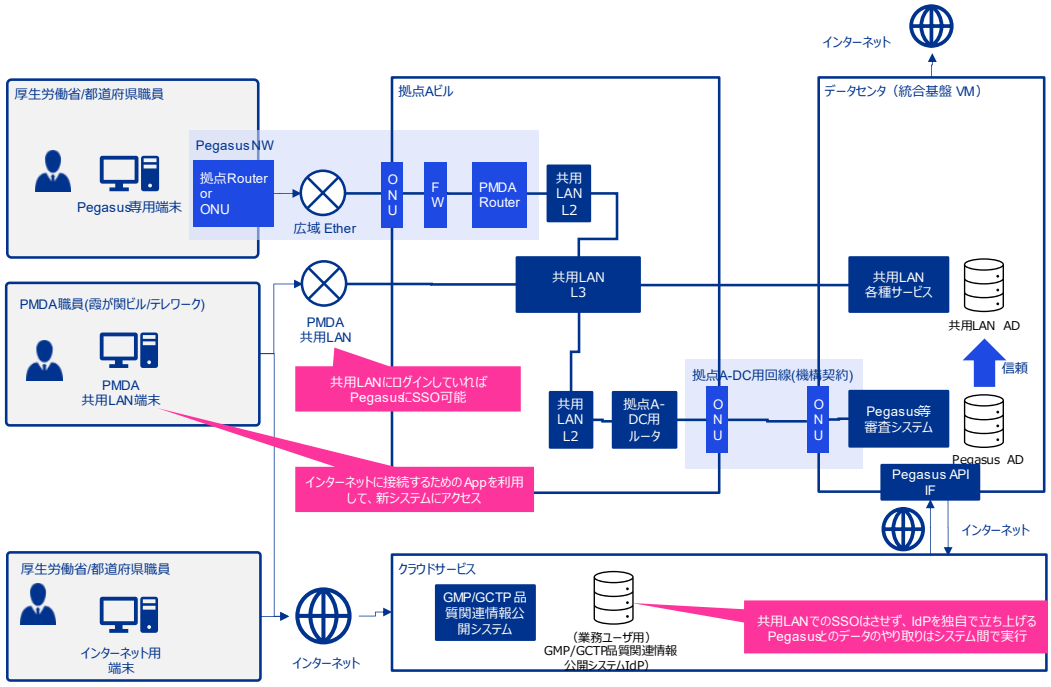


図 7 次期関連システムのネットワーク図と認証

13. テストに関する事項

システムテストの方針として、設計タイミングよりテストを意識したテストファーストの開発を推奨する。

13.1. テストに関する要件

表 15 テスト要件

No.	テストの種類	テストの目的、内容	テスト環境	テストデータ	補足
1	単体テスト	各機能群単位での機能を確認するテスト及び結合テスト前に各機能群とのインタフェース部分を疑似的に確認するテスト	設計・開発事業者環境	テストデータは、原則として設計・開発事業者が擬似データを作成して用いること。ただし、外部の連携情報システムとの調整を踏まえて作成分担を決定すること。	各機能群内で外部インタフェースとの接続テストはこのフェーズで行うこと。
2	結合テスト	各機能群間のインタフェース部分を確認するテスト	検証環境	テストデータは、原則として設計・開発事業者が擬似データを作成して用いること。ただし、外部の連携情報システムとの調整を踏まえて作成分担を決定すること。	—
3	総合テスト	システム全体が設計通りに動作することを確認するテストであり、ユースケースを組み合わせた一連のシステム利用ができることを機能面、非機能面の観点から確認するテスト	ステージング環境	移行データ含め、本番データ※	テスト内容例としては、負荷テスト（パフォーマンステスト、ラッシュテスト、大容量テスト、ストレステスト等）、セキュリティテスト（ペネトレーションテスト、インシデントレスポンス、冗長化／縮退確認、災害対策訓練等）、データテスト（実

No.	テストの種類	テストの目的、内容	テスト環境	テストデータ	補足
					データテスト、イレギュラーデータ等）、運用テスト（連続無停止テスト、定期メンテテスト等）等に分けて実施する。
4	受入テスト	システムが要件どおりに動作することを確認するテスト	本番環境	移行データ含め、本番データ※	実施者は工程管理業者及びPMDA 職員。 システム稼働後においての受入テストはステージング環境にて行うこと。

※テストの一環で本番データを利用する必要がある場合（擬似データの作成に当たり、本番データの匿名化、符号化等を行う場合を含む。）は、次の点に留意して行う必要がある。・

- 作業者、作業場所及び作業に用いる装置の制限
- 暗号化等の対応
- データの持出し、コピー等の禁止
- 本番データを利用する際の承認手続
- 使用後の消去手続と確認方法 等

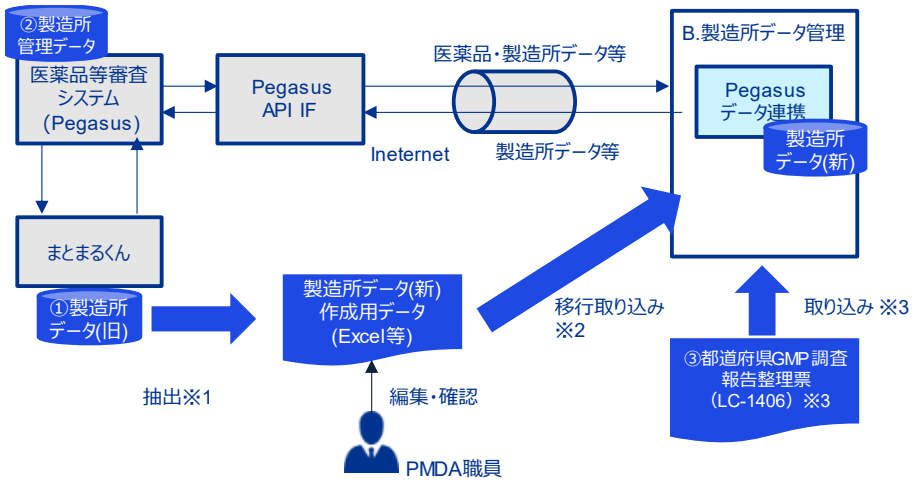
14. 移行に関する事項

移行の概要については下記の通り。

14.1. 移行対象システム

表 16 移行データ概要

No.	移行データ名	移行元	移行対象システム	移行元対象データ概要	移行方式(案)
1	製造所データ（旧）	まとまるくん	B.製造所データ管理	各製造所調査データとして管理しているもの（②の Pegasus 製造所管理データに含まれない独自データがあるため、必要）	バッチでオンプレ側の抽出後、作業ファイル(Excel,csv)を作成し、新システムに移行。まとまるくん側で確認取れる場合、中間確認作業ファイルは不要
2	製造所管理データ	医薬品等審査システム（Pegasus）	B.製造所データ管理	製造所業務台帳、調査対象製造所品目情報 受付記録等	新システムの Pegasus 連携機能を利用し、データを取得
3	都道府県 GMP 調査報告整理票データ	都道府県調査書類（Excel データ）（帳票 LC-1406）	B.製造所データ管理	各都道府県より提出された製造所データを整理したデータ	新システムの FC-14 のデータ取り込み機能を利用し移行



※1：移行設計・開発にて作成する、抽出スクリプト・バッチ
（まとまるくん上でPMDA職員が移行用のデータを確認し、確認済みのデータを ※2の移行取り込みスクリプトで取り込みも可）

※2：移行設計・開発にて作成する、スクリプト・バッチ

※3 LC-1406の帳票として、新システムの機能FC-14にてデータを取り込むため移行用の設計は不要

図 8 データ移行イメージ

14.2. 移行対象データ

表 17 移行対象データ詳細

No.	移行データ名	移行元	移行元対象 データ概要	データ件数	データ量
1	製造所データ （旧）	まとまるくん	各製造所調査データとして管理しているもの	8 万件	100M 程度
2	製造所管理データ	医薬品等審査システム （Pegasus）	製造所業務台帳 調査対象製造所品目情報 調査管理情報等	1800 万件	計 13G 程度
3	都道府県調査書類データ	都道府県調査書類	各都道府県より提出された製造所に係る帳票から抽出された、調査データ	移行設計工程で詳細を確認すること。	移行設計工程で詳細を確認すること。

15. 引継ぎに関する事項

15.1. 引継ぎ事項

表 18 引継ぎ事項

No.	引継ぎ発生時	引継ぎ元	引継ぎ先	引継ぎ内容	引継ぎ手順	補足
1	設計・開発 開始時	要件定義 事業者	設計・開発 事業者	要件定義書 残存課題	引継ぎ書の作成・ 引継ぎ結果確認書	—
2	運用開始時	設計・開発 事業者	初年度 運用事業者	設計書、作業経緯、残存課題	引継ぎ書の作成・ 引継ぎ結果確認書	—
3	運用事業者 交替時	前年度 運用事業者	次年度 運用事業者	設計書、作業経緯、残存課題	引継ぎ書の作成・ 引継ぎ結果確認書	—

16. 教育に関する事項

教育に関するマテリアルの責務は下記の通り。

表 1920 教育マテリアルに関しての責務

No.	ドキュメント	ドキュメント内容	作成者
1	GMP/GCTP 品質関連情報システム 業務システム システムユーザマニュアル	GMP/GCTP 品質関連情報システムにおいて、業務システムに関するシステムユーザマニュアル	設計・運用事業者
2	GMP/GCTP 品質関連情報システム 業務システム 教育動画	1 のドキュメント等の説明やシステム説明のための教育コンテンツをまとめた動画	設計・運用事業者
3	GMP/GCTP 品質関連情報システム 業務マニュアル	GMP/GCTP 品質関連情報システムを利用した、業務全体のマニュアル（一部、業務フロー参考）	PMDA 厚生労働省 都道府県

16.1. 教育対象者の範囲、教育の方法

（1）GMP/GCTP 品質関連情報システム　業務システム システムユーザマニュアル・ 業務システム教育動画

GMP/GCTP 品質関連情報システム　業務システム システムユーザマニュアル・業務システム教育動画に係る教育対象者等の情報は下記の通り。教育の方法としては、教育実施時期によらず、教育対象の利用者に対しての教育コンテンツを作成し配布する形やヘルプページの作成、及びシステム教育動画として作成し、教材とすること。

表 2021 業務システム システムユーザマニュアルに係る教育対象者、内容等

No.	教育対象者の範囲	教育の内容	教育実施時期
1	PMDA_医薬品品質管理部_職員	各メンテナンス機能説明	運用開始前準備期間
2	PMDA_医薬品品質管理部_調査員	調査補助機能説明	運用開始前準備期間
3	PMDA_医薬品品質管理部_調査員	課員プロファイル機能説明	運用開始前準備期間
4	PMDA_医薬品品質管理部_システム担当者	課員プロファイル管理機能説明	運用開始前準備期間
5	PMDA_医薬品品質管理部_システム担当者	システム利用者管理機能説明	運用開始前準備期間
6	PMDA_医薬品品質管理部_調査品質管理責任者	リスク判定結果管理機能説明	運用開始前準備期間
7	PMDA_医薬品品質管理部_取込管理者	各外部情報取り込み管理機能説明	運用開始前準備期間

No.	教育対象者の範囲	教育の内容	教育実施時期
8	PMDA_医薬品品質管理部_アサイン担当	アサイン関連機能説明	運用開始前準備期間
9	PMDA_医薬品品質管理部_事務補助員	データ取り込み機能説明	運用開始前準備期間
10	PMDA_医薬品品質管理部_事務補助員	調査補助機能説明	運用開始前準備期間
11	PMDA_医薬品品質管理部_都道府県担当者	蓄積・分析・リスク判定機能説明	運用開始前準備期間
12	厚生労働省	蓄積・分析・リスク判定機能説明	運用開始前準備期間
13	都道府県	蓄積・分析・リスク判定機能説明	要調整
14	都道府県	調査補助機能説明	要調整

17. 運用基本方針

(1) 運用時間等

システム運用時間等に係る要件を以下に示す。「6.1 可用性要件」に準ずるものとして規定を行う。

- 次期システムの業務ユーザ向け機能は、原則 9:00-18:00 で稼働するものとするが、一部 24 時間の機能として稼働させる。
- 運用事業者の通常業務日は、原則として平日とし、土曜日、日曜日、祝祭日及び年末年始等 PMDA が指定した日を除くものとする。ただし、システム監視については、24 時間 365 日実施するものとする。
- 一部のシステム運用業務（計画停止対応、インシデント対応等）、一部の運用サポート業務（外部連携先との調整、関連する工事への立会い等）において PMDA が要請した場合は、PMDA と協議したうえで、随時運用業務を実施すること。

(2) 運用対象

運用対象に係る要件を以下に示す。

- 運用の対象範囲は本番環境、ステージング環境、検証環境とする。
- 運用の対象業務としては、全体管理業務、システム監視業務、システム運用業務、運用サポート業務、問い合わせ対応業務とする。

17.1. 運用と保守に係る関係組織の役割分担案

運用保守に関わる各組織の役割分担を下記に示す。

表 21 保守・運用に係る組織の役割分担

No.	組織カテゴリ	組織	役割
1	オーナ	PMDA	・ 運用工程における管理・運営、整備計画の策定等を実施する。 ・ 各事業者の作業進捗の管理、運用工程における利用者及び関係者との調整を実施する。 ・ 運用実績の把握、運用改善の検討を実施する。
2	工程管理事業者	工程管理事業者	・ PMDA の調達業務の支援を実施する。また整備計画の策定支援業務として、各事業者の見解を得ながら、システムの改善策に係る提案を実施する。 ・ 開発監理支援業務として、各事業者の作業進捗の管理を実施し、必要に応じて是正に向けた助言を行う。 ・ 品質管理として、設計・開発事業者の品質管理方法のレビュー、テスト実施方法／テスト結果に係る適切性の確認、成果物レビューに係る進捗管理等を実施する。
3	運用保守事業者	運用事業者	・ 運用計画の策定、稼働状況の報告、運用改善の提案等を実施する。 ・ 情報システムの稼働状態を維持するための定常業務を実施する（運転管理、監視、バックアップ管理、セキュリティパッチ適用、情報システム設定変更等）。 ・ 障害時の一次切分け、保守事業者やクラウドサービス保守事業者への問合わせ等を実施する。 ・ 国民及び職員に対するヘルプデスク業務等のサポート業務を実施する。 ・ Web コンテンツの作成、更新等の運用支援業務を実施する。 ・ データの作成・補正・追加変更、抽出作業等を実施する。
4		保守事業者	・ アプリケーション保守、ソフトウェア保守又はクラウドサービス保守を実施する。 ・ アプリケーション保守事業者は、脆弱性の発見、障害発生時等、アプリケーションの是正が必要と

No.	組織カテゴリ	組織	役割
			なる場合の対応及び原因の分析等を実施する。 ・ ソフトウェア保守事業者は、サポートの提供、パッチの提供、製品に起因する障害時の支援等を実施する。 ・ クラウドサービス保守事業者は、サポートの提供、パッチの提供、製品に起因する障害時の支援等を実施する。
5	IaaS サービス事業者	クラウドサービス事業者	・ サービスレベル目標に基づきクラウドサービスを提供する。 ・ クラウドサービスに係る脆弱性情報やパッチ等を公開する。

また、運用事業者と保守事業者の詳細な役割分担例は下記の通り。

表 22 運用業務と保守業務の役割分担

No.	区分	運用事業者	保守事業者
1	全体管理	・ 運用計画の策定、関係者との調整、運用実績の報告、改善支援、監査対応等の各種全体管理業務	・ アプリケーション保守事業者による、保守計画の策定等 ・ 各保守事業者による、運用事業者及び PMDA への保守の作業実績に関する報告
2	システム監視	・ アプリケーションパフォーマンス等を対象にしたアラートの監視、インシデントの起票等	－
3	システム運用	・ 【脆弱性管理、構成・資産管理、変更・リリース・展開管理】 インフラ（開発フレームワーク、個別ソフトウェア等）のパッチ適用、バージョンアップ等における事前に定義されたランブックの一部設定、実行（設計・開発時点でベースとなるランブックを用意しておく） ・ 【構成・資産管理、変更・リリース・展開管理】 クラウドサービスのバージョンアップに伴うメンテナンス日時等の調整 ・ 【変更・リリース・展開管理】 アプリケーションの改修におけ	・ 【脆弱性管理】 製品の脆弱性に関する情報提供、インフラのパッチの提供 ・ 【構成・資産管理】 製品サポートライフサイクルに関する情報提供 ・ 【変更・リリース・展開管理】 アプリケーションの改修等における、改修から検証環境でのリリース作業まで ・ 【インシデント対応、問題管理】 運用事業者からのエスカレーションの受付、障害時の支援

No.	区分	運用事業者	保守事業者
		る、リリース作業後の本番展開作業（ブルーグリーンデプロイ等の手法により、原則本番環境を停止せずに実施） ・【インシデント対応、問題管理】 統合監視ツール等を利用した一次切り分け、原因調査の実施。自身で解決できない場合、保守事業者にエスカレーションを実施	
4	運用サポート	・【問合せ対応】 利用者からの問合せ対応、問合せ傾向の分析、チャットボットへの FAQ 反映・チューン等 ・【データメンテナンス】 PMDA からの依頼に基づくデータ更新、補正等 ・【データ提供】 PMDA からの依頼に基づくデータ計測等	・【問合せ対応】 運用事業者からエスカレーションを受けた場合の調査・回答

18. 保守に関する事項

18.1.保守基本方針

保守に係る基本方針は以下の通り。

- 保守業務に伴うシステムの停止時間（24 時間対応のシステム部分に関して）を可能な限り短縮させるシステム構成とすること。
- アプリケーションを本番環境へリリースする一連の作業プロセス（検証環境へのアプリケーション展開、テスト実行、各種承認作業、本番環境へのリリース）に CI/CD の考え方を取り入れ、可能な限り自動化すること。
- 保守業務は、検証環境での事前テスト等の実施結果を踏まえ、PMDA の承認を得たうえで本番環境向け作業を実施すること。

18.2.保守対象

保守対象に係る要件は以下の通り。

- 保守の対象範囲は本番環境、ステージング環境、検証環境とする。
- 保守の対象業務としては、アプリケーション保守業務、ソフトウェア保守業務及び、クラウドサービス保守業務とする。運用と保守業務の役割案に関しては「17.11 運用と保守に係る関係組織の役割分担案」を参考にすること。

以上