

**次世代安全対策システム（シグナル検出製品）導入業務
調達仕様書**

令和8年10月

独立行政法人 医薬品医療機器総合機構

目 次

1. 調達案件に関する事項	1
1.1. 調達案件名	1
1.2. 用語定義	1
1.3. 概要・背景	3
1.4. シグナル検出製品導入の目的	4
1.5. 業務・情報システムの概要	4
1.6. 業務の履行に関する事項	5
1.6.1. 契約条件	5
1.6.2. スケジュール	5
1.7. 当該調達及び関連調達に関する事項	6
1.7.1. 調達の単位、調達の方式、実施時期	6
1.8. 作業の実施内容に関する事項	7
1.8.1. 作業主体	7
1.8.2. 作業の内容	7
(1) 設計段階の作業に係る事項について	7
(2) 運用・保守に係る作業の内容	14
(3) 管理に係る事項について	19
(4) 契約金額内訳の提出に係るその他の作業の内容	19
(5) 情報の抹消作業について	19
(6) クラウド環境のセキュリティ確保に係る作業内容	20
1.8.3. 納入成果物の範囲、納入期限等	20
(1) 納品方法	21
(2) 納品場所	23
1.9. 作業の実施体制・方法に関する事項	23
1.9.1. 作業の実施体制	23
(1) 作業実施体制	23
(2) 管理体制	24
(3) 作業要員に求める資格等の要件	26
(4) 作業場所	27
1.9.2. 作業の管理に関する要領	27
1.10. 作業の実施に当たっての遵守事項	28
1.10.1. 基本事項	28
1.10.2. 機密保持、情報・資料の取扱い	29

1.10.3.	遵守する法令等	30
1.10.4.	情報セキュリティ管理.....	30
1.10.5.	情報セキュリティ監査.....	31
1.10.6.	履行完了後の資料の取扱い.....	32
1.10.7.	疑義	32
2.	サービス ¹⁾ の変更・終了	32
2.1.	サービス変更・終了時の事前告知.....	32
2.2.	サービス変更・終了時の報告.....	33
2.3.	サービス終了の対応	33
2.4.	サービス窓口.....	33
2.4.1.	営業日・時間.....	33
2.4.2.	サポート対応.....	33
2.4.3.	事故発生時の責任と保障範囲.....	33
3.	成果物の取扱いに関する事項	33
3.1.	知的財産権の帰属.....	33
3.2.	検査	34
3.3.	契約不適合責任	34
4.	入札参加資格に関する事項	35
4.1.	入札参加要件.....	35
4.1.1.	公的な資格や認証等の取得	35
4.2.	入札参加制限.....	36
5.	再委託に関する事項	36
5.1.	再委託の制限及び再委託を認める場合の条件.....	36
5.2.	承認手続き	37
5.3.	再委託先の契約違反	38
6.	その他特記事項	38
6.1.	環境への配慮.....	38
6.2.	その他	38
7.	附属文書	39
7.1.	別紙一覧（要件定義書を含む）	39
7.2.	応札希望者が閲覧できる資料一覧.....	39
7.3.	その他の資料.....	39
7.4.	契約締結後に開示する資料	39
8.	閲覧要領	39

9. 技術提案書等の審査要領	40
10. 窓口連絡先	40

1. 調達案件に関する事項

1.1. 調達案件名

次世代安全対策システム（シグナル検出製品）の導入業務

1.2. 用語定義

表 1 に本調達仕様書における用語定義及び説明を示す。

表 1 用語定義と説明

用語	正式名称（英語）	正式名称（日本語）	説明
Adhoc 計算	Adhoc analysis	—	定型化された条件ではなく、利用者が任意の条件を指定して都度実施する計算
API	Application Programming Interface	—	—
AWS	Amazon Web Services	—	—
BCP	Business Continuity Plan	事業継続計画	災害、障害等の発生時に業務を継続又は早期復旧するための計画
BCPNN	Bayesian Confidence Propagation Neural Network	—	ベイズ統計に基づき医薬品と有害事象の関連性を評価するためのシグナル検出手法
CIO 補佐	—	最高情報責任者補佐	—
CMMI	Capability Maturity Model Integration	能力成熟度モデル統合	—
CRYPTREC	Cryptography Research and Evaluation Committees	—	—
DME	Designated Medical Event	—	特に重要な安全性シグナルとして取り扱うべき有害事象群。副作用報告の評価及びシグナル検出に利用される
E2B 項目	—	—	ICH E2B（R3）で定義された ICSR の標準データ項目。患者情報、医薬品情報、有害事象情報等から構成される
EVM	Earned Value Management	—	—
FAERS	FDA Adverse Event Reporting System	FDA 有害事象報告システム	米国 FDA が運用する有害事象報告データベース
GPS	Gamma Poisson Shrinker	ガンマ・ポアソン・シュリンカー法	ベイズ統計に基づく不均衡分析手法の一つであり、安全性シグナルの検出に利用される
HSM	Hardware Security Module	—	暗号鍵の生成、保管及び利用を安全に行うための専用装置又は機能
ICSR	Individual Case Safety Report	個別症例安全性報告	—
IEEE	Institute of Electrical and Electronics Engineers	米国電気電子学会	—
IME	Important Medical Event	重要な医学事象	死亡又は入院等の重篤性基準に必ずしも該当しないものの、医学的観点から重要と判断される有害事象
IPA	Information-technology Promotion Agency, Japan	独立行政法人情報処理推進機構	—
ISMAP	Information system Security Management	政府情報システムのためのセキュリティ評価制度	日本において、政府が求めるセキュリティ要求を満たすクラウドサービスを評価・登録する制度

用語	正式名称（英語）	正式名称（日本語）	説明
	and Assessment Program		
ISO	International Organization for Standardization	国際標準化機構	—
ISMS	Information Security Management System	情報セキュリティマネジメントシステム	—
ITU-T	International Telecommunication Union Telecommunication Standardization Sector	国際電気通信連合 電気通信標準化部門	—
J-RMP	Japanese Risk Management Plan	医薬品リスク管理計画	—
JADER	Japanese Adverse Drug Event Report Database	医薬品副作用データベース	—
KMS	Key Management Service	—	暗号鍵の作成、保管、利用及び管理を行うサービス
KPI	Key Performance Indicator	重要業績評価指標	システム運用又は業務の達成状況を定量的に評価するための指標
LLT	Lowest Level Term	最下層語	—
MedDRA	Medical Dictionary for Regulatory Activities	ICH 国際医薬用語集	医薬品等の有害事象、適応症、既往歴等を標準化して記録・分析するための国際標準医学用語集
PMAJ	Project Management Association of Japan	日本プロジェクトマネジメント協会	—
PMDA	Pharmaceuticals and Medical Devices Agency	独立行政法人 医薬品医療機器総合機構	—
PMI	Project Management Institute	プロジェクトマネジメント協会	プロジェクトマネジメント分野における主要な専門機関として、プロジェクトの成功に向けた指針の提供、専門職の育成、標準化の推進を行う国際的な非営利団体
PMO	Project Management Office	—	全体管理組織
PMP	—	プロジェクトマネジメント・プロフェッショナル	PMI が認定している国際資格
PMS	—	プロジェクトマネジメント・スペシャリスト	PMAJ が認定している資格
ROR	Reporting Odds Ratio	報告オッズ比	副作用等報告データベースにおける医薬品と有害事象の関連性を評価するための不均衡分析指標の一つ
RPO	Recovery Point Objective	目標復旧時点	障害発生時に、どの時点のデータ状態まで復旧することを目標とするかを示す指標
RTO	Recovery Time Objective	目標復旧時間	障害発生後、業務又はシステムを復旧させるまでの目標時間
S3 バケット	Amazon Simple Storage Service Bucket	—	AWS のオブジェクトストレージサービスにおいて、ファイル等のオブジェクトを格納する単位
SCVX	—	インターネット閲覧環境	PMDA 職員がインターネット閲覧又はクラウドサービス利用時に経由する環境
SFTP	SSH File Transfer Protocol	SSH ファイル転送プロトコル	—

用語	正式名称（英語）	正式名称（日本語）	説明
SLA	Service Level Agreement	サービスレベル合意	サービスの稼働率、応答時間等、提供水準に関する合意又は基準
SMQ	Standardised MedDRA Query	MedDRA 標準検索式	—
SOC	System Organ Class	器官別大分類	—
SSL/TLS	Secure Sockets Layer / Transport Layer Security	—	通信経路を暗号化し、通信内容の盗聴や改ざんを防止するための通信方式
VigiBase	—	WHO 国際副作用報告データベース	—
WBS	Work Breakdown Structure	—	—
WCAG	Web Content Accessibility Guidelines	—	—
安対システム	—	医薬品安全対策支援システム	医薬品副作用等報告の検索、評価、解析、企業面談情報の記録等の支援を行うシステム
医薬品副作用等報告	—	市販後及び治験中の医薬品副作用情報	—
既存著作物等	—	—	調達に係り作成されるドキュメント類等に第三者が権利を有する著作物
業務従事者名簿	—	—	本業務に従事する者の名簿
情報セキュリティ管理計画書等	—	—	情報セキュリティ管理計画書又は設計・開発実施計画書
情報管理責任者	—	—	本業務の情報取扱いの全てに責任を有する者
情報システム	—	—	シグナル検出製品を利用するために必要なクラウド環境、各種設定、外部サービス、監視機能、バックアップ機能等を含めた本調達の対象全体
情報取扱管理者	—	—	本業務の進捗管理等を行い、保護を要する情報を取り扱う可能性のある者
情報取扱者名簿	—	—	本業務に従事する者のうち、保護を要する情報を取り扱う可能性のある者の名簿
デモ環境	—	—	PMDA による導入製品に係る業務理解の促進、操作性の確認及び実導入に向けた手順整備等を円滑に進めることを目的として、受注者が用意する環境
統合システム	—	医薬品副作用・安全対策支援統合システム合システム／不具合情報管理システム	PMDA における安全対策業務に関連するシステムを動作させるためのインフラを構成する基盤
統合基盤システム	—	業務システム統合基盤システム	各業務システムを稼働させるための PMDA におけるシステムインフラ環境。仮想マシンの稼働リソース及び物理サーバを設置するためのファシリティを提供し、各環境の為のセキュリティ機能、バックアップ機能を含む各運用機能とネットワークを含むセキュリティ機能を提供する

1.3. 概要・背景

安全対策業務において、副作用・感染症症例報告、研究報告、外国措置報告等の多様な安全性情報を収集・評価し、必要な安全対策を講じている。

近年、副作用症例報告の件数は継続的に増加しており、限られた人的リソースの中で、全ての症例を同じ粒度で確認する従来型の評価手法の維持が難しくなりつつある。一方、海外規制当局や製薬企業においては、不均衡分析等の統計学的手法を活用したシグナル検出を安全性監視活動の重要な手法として位置付け、リスクベースの安全性評価への移行が進められている。

PMDA においても現行システム上に不均衡分析機能を有しているが、シグナル指標値（ROR 等）、重篤性、予測性、報告件数、報告傾向の変化等を組み合わせた柔軟な検出・アラート機能が限定的であり、シグナル検出を活用したリスクベースの安全性評価への円滑な移行の制約となっている。

PMDA の第 5 期中期目標にあるとおり、安全対策業務の一層の質の向上と高度化が求められており、限られた人的リソースの中でも効果的及び科学的な安全性監視を実現するため、リスクベースの安全性評価手法を支える分析基盤の整備が必要となっている。

本調達は、次世代の医薬品安全性監視業務を見据え、シグナル検出製品を試行的に導入するものである。これにより、シグナルの自動抽出及び優先順位付けを行うことで、リスクベース安全性評価手法の有効性及び実運用への適用可能性を検証し、将来的な安全対策業務の効率化及び高度化を目指すものである。

1.4. シグナル検出製品導入の目的

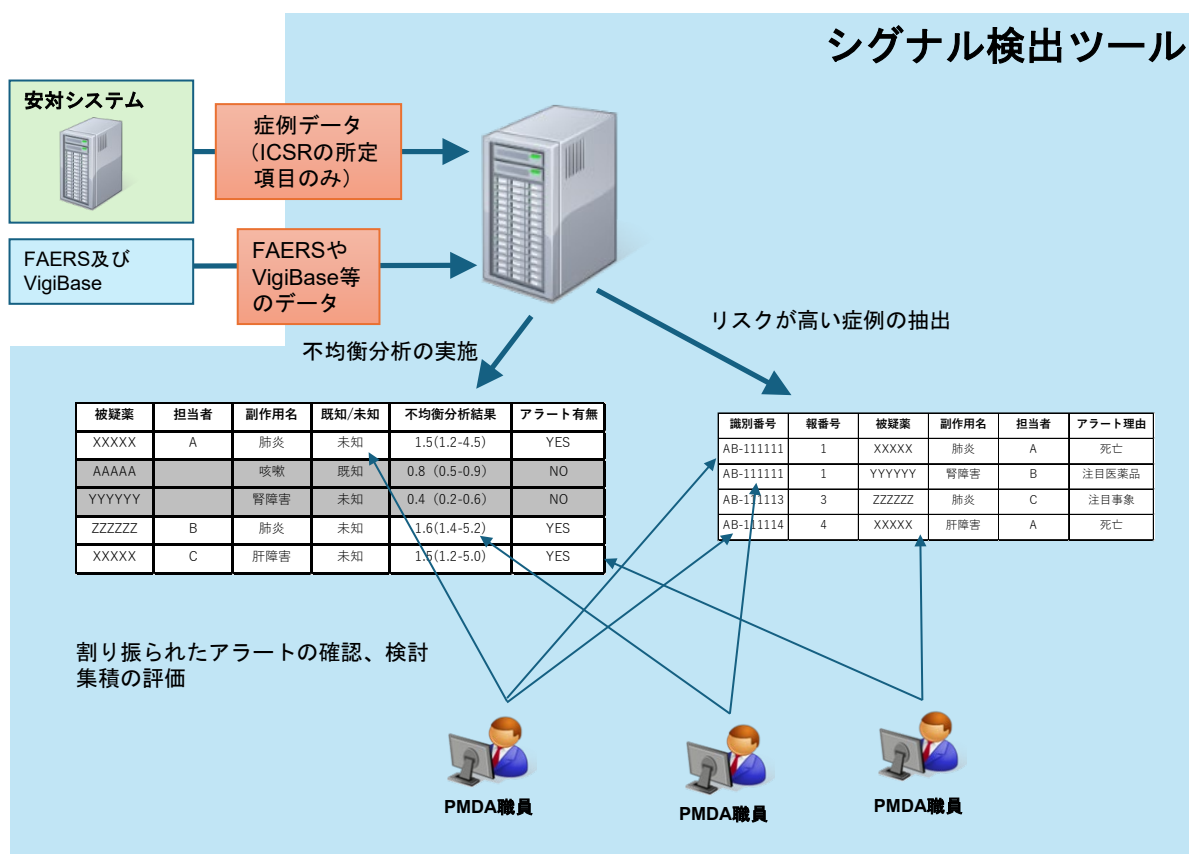
シグナル検出製品を導入することで、データマイニング・注目事象の提示等のシステムによるサポートを活用するとともに、PMDA 職員による因果関係評価はリスクが高い報告に集中させる多層的、かつリスクベースの安全対策を実行する。

1.5. 業務・情報システムの概要

今回調達するシグナル検出製品を用いたリスクベース評価の概要は以下のとおりである。

シグナル検出製品では、新たに提出された市販後副作用等報告について、不均衡分析結果、注目事象（欧州で規定された事象（DME、IME）、重要な潜在的リスク、海外措置等の情報から独自に設定したものも含む。）、注目医薬品、転帰（死亡）等の観点であらかじめ定めた基準に該当する症例が報告された場合にアラートを表示し、特定の担当者に確認作業の割振りを行う。また、アラートの対応期限を設定することで、シグナル検出作業のスケジュール管理を実施する。

図 1 シグナル検出製品を用いたリスクベース評価の概要図



1.6. 業務の履行に関する事項

1.6.1. 契約条件

契約期間

契約締結日から令和 11 年 3 月 31 日

なお、構築期間は契約締結日から令和 9 年 11 月 30 日までとし、運用・保守期間は令和 9 年 12 月 1 日から令和 11 年 3 月 31 日までとする。

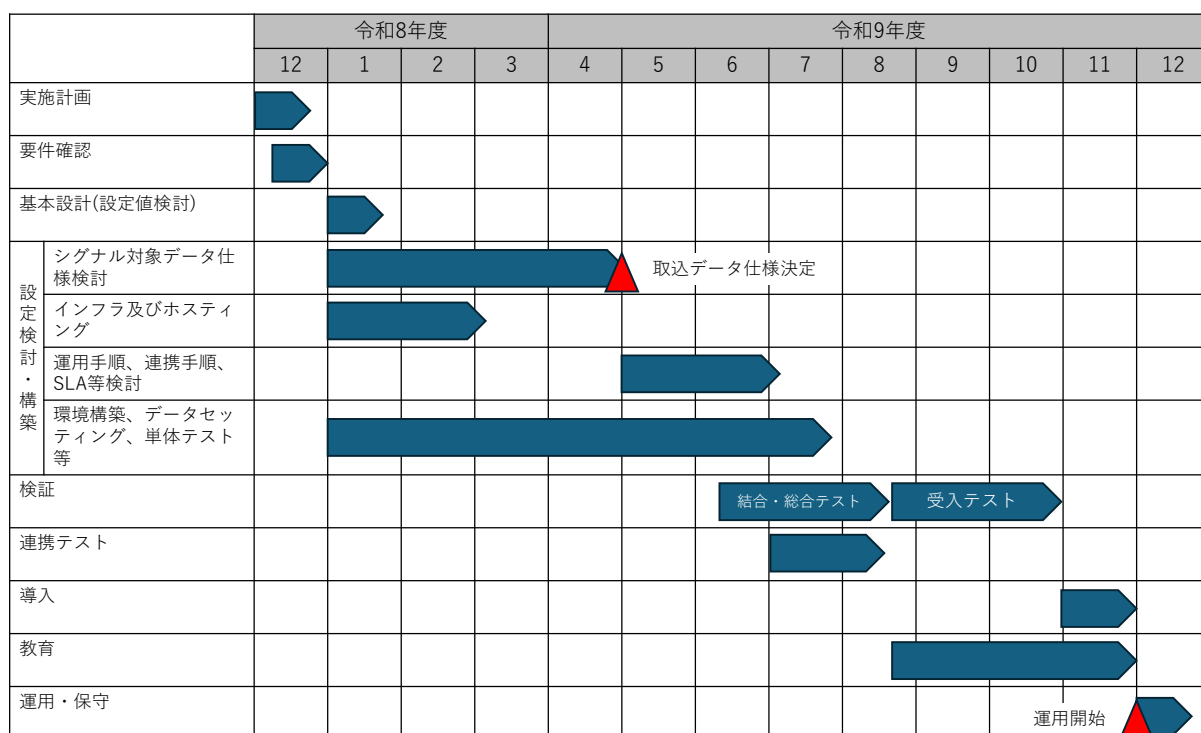
契約形態

請負契約形態とし、支払方法等は契約書にて定める。

1.6.2. スケジュール

図 2 はあくまで想定であり、詳細な実施スケジュールは受注者が検討し、PMDA と協議のうえ、承認を受けること。

図 2 スケジュール概要



1.7. 当該調達及び関連調達に関する事項

1.7.1. 調達の単位、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「表 2 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)」及び「表 3 関連する調達案件の調達単位、調達の方式、実施時期等(契約予定)」のとおりである。

表 2 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)

No.	調達案件名	調達の方式	実施時期	役割	事業者名
1	業務システム統合基盤の構築及び保守	一般競争入札	令和 5 年 4 月から 令和 10 年 10 月	ハードウェア/ソフトウェア 調達・構築/運用・保守	株式会社インターネティニシアティブ
2	医薬品副作用・安全対策支援統合システム及び医療機器不具合情報管理システムの支援業務	一般競争入札	令和 6 年 4 月 1 日から令和 11 年 3 月	ハードウェア/ソフトウェア 運用・保守	株式会社セック
3	医薬品副作用・安全対策支援統合システム及び医療機器不具合情報管理システムの機器更改及び賃貸借業務	一般競争入札	令和 6 年 7 月から 令和 12 年 10 月	ハードウェア/ソフトウェア 調達・構築	株式会社セック
4	予防接種事務のデジタル化等に伴う回線構築及び保守等業務	随意契約	令和 8 年 1 月から 令和 11 年 3 月	回線保守	株式会社セック

表 3 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)

No.	調達案件名	調達の方式	実施時期	役割	事業者名
1	次世代安全対策システム (シグナル検出製品)の導入 に伴う医薬品安全対策支援 システム改修業務	一般競争入札	契約締結日から令和 9 年 12 月 31 日	ソフトウェア改 修	—

1.8. 作業の実施内容に関する事項

1.8.1. 作業主体

本調達は、導入対象となるクラウド型シグナル検出製品を、PMDA の業務要件及びシステム要件に適合する形で導入することを目的とする。

本調達における「設計」及び「開発」とは、クラウドサービスを利用する前提において、次に掲げる事項を指し、クラウドサービス内部の基盤構成又はアプリケーションそのものの設計・開発を求めるものではない。

- ・ 当該サービスの標準機能の活用
- ・ 提供される設定範囲内での利用者側設定
- ・ 導入設計及び運用設計
- ・ 外部システムとの連携等に係る設計・開発

ただし、業務要件上やむを得ず標準機能で対応できない場合に限り、最小限の機能追加について検討することとし、その実施の可否、範囲及び方式については PMDA と協議のうえ、決定するものとする。

1.8.2. 作業の内容

(1) 設計段階の作業に係る事項について

① 計画書等について

- ①-1 受注者は、PMDA の指示に基づき、業務実施計画書(案)及び業務実施要領(案)を作成し、PMDA の承認を受けること。なお、業務実施計画書(案)及び業務実施要領(案)にはそれぞれ以下の内容が含まれていることとする。

○業務実施計画書(案)に含まれている内容

- ・ 作業概要
- ・ 作業体制
- ・ スケジュール
- ・ 想定成果物一覧
- ・ 開発形態、開発手法、開発環境、開発ツール等
- ・ その他(前提条件、制約条件等)

○業務実施要領(案)に含まれている内容

- ・ コミュニケーション管理
- ・ 体制管理
- ・ 工程管理
- ・ 品質管理
- ・ 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

② デモ環境を利用した機能確認の実施について

②-1 受注者は、シグナル検出製品に係る PMDA の業務理解の促進、操作性の確認、実導入に向けた手順整備等が円滑に進められるよう、本調達の契約期間中において、以下に示すとおりシグナル検出製品の機能確認について協力すること。

- ・ 理解促進・検討支援を目的とした参考利用のためのデモ環境を提供すること。当該デモ環境に求める要件は②-2 から②-5 に示すとおりであるが、最終的に納入されるシステムと同一要件であることを求めるものではない
- ・ 機能確認の実施中、PMDA からデモ操作方法等に関する質問又は疑義が提示された場合には、受注者は速やかに回答し、必要に応じて追加説明すること。また、PMDA が作成する機能確認のシナリオ又はチェックリストについて、PMDA の求めに応じ、技術的助言を行うこと
- ・ 機能確認結果を踏まえ、PMDA が要望する機能のうち、標準機能で対応できない項目の整理支援

②-2 デモ環境において使用する症例データ、医薬品情報等は、受注者の責任において用意した検証用データとする。特に、症例データは、最終的に納入される製品へ投入予定のデータ項目及び構造を踏まえ、可能な限り同様の形式となるよう配慮すること。データの種類、範囲及び形式については、デモ環境利用開始までに PMDA と相談のうえ、承認を受けること。なお、データの取扱いについては、PMDA の情報セキュリティ管理要件を遵守すること。

②-3 機能確認に使用するデモ環境及びアカウントは受注者が用意すること。

デモ環境は、原則、標準機能の全容を確認できる状態で提供すること。機能確認の目的上、デモ環境であることを理由とした機能制限や操作制限は設けないこととする。な

お、利用できない機能がある場合は、デモ環境利用開始までにその理由及び利用可能範囲について提示し、PMDAと協議のうえ、承認を受けること。

②-4 表示される画面、メッセージ等は、可能な限り日本語で表示されることが望ましい。

PMDA の利用者ごとに ID、パスワード等の認証情報を設定する等して、PMDA が指定した者のみが当該環境を利用できるよう、適切なアクセス制御を行うこと。利用アカウント数は、概ね 15 アカウント程度を想定する。

②-5 契約後、可能な限り速やかに利用開始できるようにする。デモ環境利用終了は、遅くとも受入テスト開始前を想定している。具体的なデモ環境利用開始時期及び利用期間については契約後、PMDA と相談のうえ、決定する。

デモ環境利用期間中であっても、受注者の都合で当該環境についてバージョンアップ等のメンテナンスによる機能の一時停止やシャットダウン等の実施を妨げるものではない。ただし、利用停止にあたっては、緊急の場合を除き、原則、利用停止の 1 週間前までに PMDA へ通知することとし、緊急の場合は速やかに PMDA に連絡すること。

③ 設計段階に係る事項について

③-1 受注者は、シグナル検出製品が本調達仕様書「別紙 1 機能要件定義書（次世代安全対策システム（シグナル検出製品）の導入業務）」及び「別紙 2 非機能要件定義書」を満たすか確認し、PMDA の業務要件に適合させるために必要な設定、構成検討、外部システム連携設計及び運用設計を行うこと。また、機能要件及び非機能要件ごとに、標準機能又は設定変更による対応可否、追加対応の必要性及び対応方針を整理した成果物（要件適合性評価一覧（Fit&Gap 一覧）、Gap 対応方針書）を作成し、PMDA の承認を受けること。

③-2 要件定義に際し、画面のイメージや操作方法について利用者に周知を行うこと。周知時期は、利用者からの問い合わせに対する回答のために必要な期間を確保できるように、調整すること。また、PMDA の業務要件に適合させるための設定の必要が生じた場合には対応すること。

③-3 受注者は情報システムの移行の方法、環境、ツール、段取り等を記載した導入計画書（案）及び移行計画書（案）を作成し、PMDA の承認を受けること。

③-4 受注者は、運用設計及び保守設計を行い、定常時における月次の作業内容、その想定スケジュール、障害発生時における作業内容等（情報システムの構成やライフサイクル等の中長期の作業を含む）を取りまとめた運用計画書（案）及び保守計画書（案）を作成し、PMDA の承認を受けること。運用設計及び保守設計を行う際には、以下の内容を取りまとめたランニングコスト試算表を作成し、運用計画書（案）及び保守計画書（案）に記載すること。

- ・ 運用段階及び保守段階において発生する各種コストに係る予実管理のための管理様式
- ・ 運用設計及び保守設計実施時点で判明している所要見込額
- ・ 必要となるソフトウェアライセンス所要額及びクラウドサービス利用額

また、情報セキュリティ水準の維持に関する手順については情報セキュリティ管理計画書（案）を作成し、PMDAの承認を受けること。なお、セキュリティ監視については、以下の内容が含まれていることとする。

- ・ 監視するイベントの種類や重要度
- ・ 監視体制
- ・ 監視状況の報告手順や重要度に応じた報告手段
- ・ 情報セキュリティインシデント又はその可能性を認知した場合の報告手順
- ・ 監視運用における情報の取扱い（機密性の確保）

③ー5 受注者は、定常時及び障害発生時において想定される運用体制、実施手順等の案を作成し、PMDA の承認を受けること。

③ー6 受注者は、情報システムにおけるクラウドサービスの利用に必要なクラウド構成等のクラウド環境の設計を行い、PMDA の承認を受けること。また、クラウドサービスの利用形態、使用期間、サービスの種類、内容等を明らかにしたクラウドサービスの一覧を作成すること。受注者はこれらが記載されたクラウド環境設計書（案）を提出し、PMDA の承認を受けること。

③ー7 受注者は、情報システムでクラウドサービスを利用する際の運用設計及び保守設計に当たり、リソースの使用状況に応じてサーバのスペック等を調整し、リソースの効率的な使用を通じてコスト削減を継続的に図っていく取組み（オートスケーリングを利用する場合の変更条件、上下限值等を含む。）を含めること。

③ー8 受注者は、クラウドサービスプロバイダが提供するクラウドサービスの設計支援サポートを契約する等、クラウドサービスの利用方法が適切であることが確認できる手段を確保すること。

④ 開発・構築・テストに係る事項について

④ー1 受注者は、本調達仕様書、「別紙 1 機能要件定義書（次世代安全対策システム（シグナル検出製品）の導入業務）」及び「別紙 2 非機能要件定義書」に記載する機能の実装に当たり、業務要件、セキュリティ要件又は運用上の理由により、クラウドサービスの機能を補完する目的で、PMDA 又は受注者が主体的に管理・運用するハードウェアをやむを得ず導入せざるを得ない場合、アプリケーションプログラムの開発又は保守を

効率的に実施するため、プログラミング等のルールを定めた開発標準（標準コーディング規約、セキュアコーディング規約等）を業務実施要領（案）における品質管理要領に定め、PMDA の承認を受けること。なお、既存プログラムの修正においては、既存のプログラムを考慮し修正方針を定め、PMDA の承認を受けること。

- ④ー2 受注者は、本調達に特化した機能に対する開発が必要な場合、情報セキュリティ確保のためのルール遵守や成果物の確認方法（例えば、標準コーディング規約遵守の確認、ソースコードの検査、現場での抜打ち調査等）についての実施主体、手順、方法等を定め、PMDA の承認を受けること。
- ④ー3 受注者は、本調達仕様書に記載のシステム要件を満たすアプリケーション動作システムの設計及び構築を行うこと。
- ④ー4 受注者は、単体テスト、結合テスト及び総合テストについて、テスト体制、テスト環境、作業内容、作業スケジュール、テストシナリオ、合否判定基準等を記載したテスト計画書を作成し、各テスト実施前に PMDA の承認を受けること。なお、これらのテストにおいて、静的コード解析ツール等を使用することにより合理的に品質の向上を図ることができる場合には、積極的にこれらツールを活用することが望ましい（ただし、対象言語に係る解析の品質が一般に認められているもので、かつ原則として中立性が担保されるオープンソースソフトウェアであることを前提とする。）。この場合、人的レビューと重複する部分については、原則として省略して差し支えない。
- ④ー5 受注者は、連携テストについて、関連する調達案件の受注者と連携し、テスト方針、テスト体制、テスト環境、作業内容、作業スケジュール、テストシナリオ、合否判定基準等を記載したテスト計画書（案）を作成し、テスト実施前に PMDA の承認を受けること。なお、テスト計画書（案）は PMDA 提出前に連携先の受注者と内容について合意形成を行い、それぞれの受注者より提出すること。
- ④ー5 受注者は、本調達に特化した機能に対する開発が必要な場合、設計工程の成果物に基づき、アプリケーションプログラムの開発を行うこと。
- ④ー6 受注者は、設計工程の成果物及びテスト計画書に基づくテストの実施に当たっては、具体的なテスト内容（テスト項目、使用するデータ等を含む。）について規定したテスト計画書（案）を作成し、これに基づきテストを実施すること。その際、総合テスト（必要に応じて結合テスト）に関しては、テスト実施前にテスト計画書（案）について PMDA の承認を受けること。また、各テストの実施状況及び結果については、随時 PMDA に報告すること。
- ④ー7 受注者は、開発・テストの際に、情報システムの稼働に当たって必要なソフトウェア等がある場合は必要に応じて購入する等の対応を行い、作業完了後に PMDA に納品すること。その際、受注者は、納品ソフトウェア製品一式、ソフトウェア構成表、ライセンス

関係資料(ライセンス証書、ライセンス種別、ライセンス数、ライセンス料等)、導入計画書、導入作業手順書及び設定作業報告書を PMDA に提出すること。

- ④ー8 受注者は、環境の設定を行う場合、「別紙 2 非機能要件定義書」の設計に応じた内容で、各種環境の構成、パラメータ等の設定を PMDA に報告すること。
- ④ー9 受注者は、運用を補助するためのツールが必要となる場合、当該ツールの実装及び単体テストの実施状況の報告、運用ツールの操作方法等に関する手順書(案)を作成し、PMDA の承認を受けること。
- ④ー10 受注者は、情報システムでクラウドサービスを利用する際、クラウド環境設計書に基づき、クラウドサービスプロバイダと契約すること。その上で、クラウドサービスの構築を行うと共に、情報システムをクラウドサービス上に構築すること。また、受注者は構築完了後、動作検証結果を記載したクラウドサービス導入報告書(案)を作成し、PMDA の承認を受けること。
- ④ー11 受注者は、情報システムの操作方法を示した利用マニュアル(案)を作成し、PMDA の承認を受けること。

⑤ 受入テスト支援に係る事項について

- ⑤ー1 受注者は、PMDA が受入テスト計画書を作成するに当たり、情報提供等のテスト計画書作成の支援を行うこと。
- ⑤ー2 受注者は、PMDA が受入テストを実施するに当たり、環境整備、運用、受入テスト実施支援等を行うこと。
- ⑤ー3 受注者は、PMDA から報告される受入テスト結果を取りまとめ、必要に応じて指摘事項への対応を行うこと。

⑥ 導入・移行に係る事項について

- ⑥ー1 受注者は、本番環境への移行手順について、移行リハーサルにより、移行シナリオ、移行スケジュールの適切性等を確認すること。
- ⑥ー2 受注者は、移行リハーサル結果報告書(案)を提出し、PMDA の承認を受けること。
- ⑥ー3 受注者は、PMDA の移行判定を受けて、導入計画書及び移行計画書に基づく導入・移行作業を行うこと。
- ⑥ー4 受注者は、データ移行に当たり、新規情報システムのデータ構造、保有・管理するデータの変換、例外データ等の処理方法等を定めた移行要領を策定すること。また、当該要領に基づく移行手順書(案)を作成し、PMDA の承認を受けること。
- ⑥ー5 受注者は、移行手順書に従ったデータ変換・移行完了後、移行後のデータ、例外データ等の確認を行い、当該結果を示す等、データの信頼性の確保を図ること。

- ⑥-6 受注者は、導入計画書及び移行計画書、並びに導入手順書及び移行手順書に基づいた本番環境への移行に対応すること。移行完了後、導入作業結果報告書(案)及び移行作業結果報告書(案)を作成し、PMDA の承認を受けること。
- ⑥-7 受注者は、情報システムでクラウドサービスを利用する際のデータ移行に必要なデータ転送サービスの選定及びデータ移行に必要な環境の構築を行い、データ移行を実施すること。
- ⑥-8 受注者は、システムを稼働させるために初期データ整備が必要な場合には、対応すること。

⑦ 教育に係る事項について

- ⑦-1 受注者は情報システムの運用開始に向け、利用者やPMDAの管理者に対し、必要に応じて説明会等を実施し、機能内容を周知すること。実施内容について定めた教育計画書(案)を作成し、PMDA の承認を受けること。
- ⑦-2 受注者は、教育計画書に基づき実施された教育内容とその結果について、教育作業結果報告書(案)を作成し、PMDA の承認を受けること。
- ⑦-3 受注者は利用者や PMDA の管理者が情報システムを用いた業務を実施できるよう、利用マニュアル(案)を作成し、PMDA の承認を受けること。

⑧ 最終報告書の作成

- ⑧-1 受注者は構築完了時及び運用・保守期間中の作業終了時、以下の内容を含む最終報告書(案)を作成し、PMDA の承認を受けることとする。なお、各期間で作成した他の成果物が、以下の内容を含むものであれば、それを最終報告書の一部とすることで差し支えない。
 - ・ 本調達又は工程の概要レベルの説明
 - ・ 予定作業について、作業の完了基準が満たされていることの証拠
 - ・ 品質目標、本調達や成果物の品質評価に使用される基準、成果物の品質
 - ・ 各工程の完了予定日と実際の完了日の差異の有無及び理由
 - ・ 最終のサービス、成果物の検証概要

⑨ システム資産簿登録に係る作業

- ⑨-1 PMDA においては、システムのインベントリ情報を一元管理するシステム資産簿を作成している。受注者は、情報システムで利用する機器、ソフトウェア、ネットワーク等の構成情報を PMDA へ報告し、一元管理するシステム資産簿の管理情報について常に

最新の状態を保つこと。なお、1.8.2(1) ⑧-2 に示す事項以外に管理が必要と考えられる事項があれば PMDA と協議のうえ、合わせて管理すること。

⑨-2 受注者は対象システムに更新等が発生した場合、PMDA のライセンス管理台帳に以下のインベントリ情報を登録する必要があるため、PMDA が指定するシステム資産簿登録用情報を、PMDA が指示する時期に提供すること。

- ・ ソフトウェアの管理(本調達に特化した機能に対する開発が必要な場合)
本調達情報システムを構成するソフトウェア製品(アプリケーションフレームワークや、ノンプログラミングによる自動生成等のツール、開発時に使用するソフトウェアを含む。)の名称(エディションを含む。)、バージョン、ソフトウェア分類、契約形態、ライセンス形態、サポート期限等
- ・ 外部サービスの管理
情報システムを構成するクラウドサービス等の外部サービス利用形態、外部サービスのデータ保持地域、使用期間等
- ・ ライセンス管理情報(ソフトウェア名称、エディション・バージョン、ライセンス番号(シリアル番号)、提供形態、有効期限、保有ライセンス数等)
- ・ 取扱情報の管理
情報システムが取り扱う情報について、データ・マスタ名、個人情報の有無、格付等
- ・ 指標の管理
情報システムの運用及び保守の間、把握すべき KPI 名、KPI の分類、計画値等の案
- ・ スケジュール、工数等の管理
スケジュール、工数等の計画値及び実績値
- ・ その他 PMDA が指定する項目

⑨-3 受注者は、情報システムを構成するクラウドサービス・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) 運用・保守に係る作業の内容

① 運用計画書及び保守計画書の作成

受注者は、具体的な作業内容、実施時間、実施サイクル等に関する運用計画書(案)及び保守計画書(案)を作成し、PMDA の承認を受けること。

② 運用手順書及び保守手順書の作成

受注者は、具体的な作業内容、実施時間、実施サイクル等に関する運用手順書（案）及び保守手順書（案）を作成し、PMDA の承認を受けること。

③ 情報セキュリティ対策の実施

受注者は、情報セキュリティ対策の対応結果を取りまとめた情報セキュリティ対策実施報告書（案）を作成し、PMDA の承認を受けること。

④ 定常時対応

④－1 受注者は、「別紙 2 非機能要件定義書」の 17. 運用・保守に関する事項に示す業務（システム操作、運転管理・監視、稼働状況監視、サービスデスク提供等）を行うこと。

④－2 受注者は、運用計画書、保守計画書、運用手順書及び保守手順書に基づき、以下の内容が取りまとめられた月次の運用・保守作業報告書を作成すること。

- ・ 運用・保守業務の内容、工数、作業時間等の作業実績状況
- ・ サービスレベルの達成状況
- ・ サービスレベル関連実績データと分析・評価及び対策
- ・ 情報システムの構成と運転状況（情報セキュリティ監視状況を含む）
- ・ 情報システムの定期点検状況
- ・ 情報システムの利用者サポート、教育・訓練状況
- ・ リスク・課題の把握・対応状況
- ・ クラウドサービスの利用状況（リソース使用量の変動、構成変更の実施状況等を含む。なお、クラウドサービスプロバイダから提供される管理ツール等により出力可能な情報があれば、当該情報を管理ツール等から出力したそのままの形で添付することとしても差し支えないが、グラフ化等、参照性の担保には配慮すること。）

④－3 受注者は、月間の運用・保守実績を評価し、達成状況が目標に満たない場合はその要因の分析を行うとともに、達成状況の改善に向けた対応策を PMDA に提案すること。また、クラウドサービスを利用するとき、リソース使用量の変動等を踏まえ、リソース最適化の観点からクラウドの運用に係る方針（オートスケーリングを利用する場合の変更条件、上下限值等を含む。）を変更すべきと考えられる場合には、見直しのための対応策を提案すること。

④－4 受注者は、運用・保守作業報告書の内容について、定期的に運用会議を開催しその内容を報告すること。開催頻度は PMDA と協議のうえ、決定すること。なお、PMDA が認める場合は、書面による報告を運用会議の代替とすることを可能とする。

- ④ー5 受注者は、運用・保守作業が円滑に行われるよう、システムの改修・機能追加、運用・保守作業等の見直しにより、運用手順書等の見直しが必要となった場合は、PMDA に修正を提案し、承認を受けた上で対応すること。
- ④ー6 契約期間内に運用・保守作業に変更が生じない場合でも、運用手順書等の品質について確認し、品質に問題がある場合は PMDA に改善を提案し、承認を受けた上で対応すること。
- ④ー7 受注者は、運用手順書、保守手順書等について、版管理を行うと共に修正の有無に関わらず最新版を維持すること。

⑤ バージョンアップ

- ⑤ー1 クラウドサービスのアップデートが予定される場合、遅くとも 3 か月前にメールにより PMDA 担当者に直接通知すること。通知の内容として、アップデートによる既存機能に対する影響範囲、内容、サービス利用停止有無(停止が必要な場合は、停止期間も含む)及びアップデート採用可否を含めること。
- ⑤ー2 アップデートにより搭載される機能について、PMDA に十分に説明すること。また、本番環境適用前に PMDA による動作確認が行えるようスケジュールを調整すること。
- ⑤ー3 アップデート失敗時には、「別紙 2 非機能要件定義書」に示した RTO 以内に旧バージョンへ復旧できること。その際にアップデート前のデータも保持していること。
- ⑤ー4 セキュリティ脆弱性が発見され、機能アップデートの通知期限前にアップデートが必要であることが判明した場合は即時に PMDA に通知すること。その際には、機能アップデートの通知時と同様の内容を報告すること。

⑥ 情報システムの現状確認

- ⑥ー1 受注者は、業務開始時及びシステム資産簿変更時に運用計画書及び保守計画書と情報システムの現況との突合・確認を行い、当該結果を記載した現況確認結果報告書を提出すること。
- ⑥ー2 受注者は、現況との突合・確認の結果、運用計画書と情報システムの現況との間に差異が判明した場合は、運用計画書に定める変更管理方法に従い、差異を解消すること。
- ⑥ー3 受注者は、現況との突合・確認の結果、ライセンス許諾条件に合致しない状況が認められた場合は、当該条件への適合可否、条件等を調査し、当該結果を PMDA に報告すること。
- ⑥ー4 受注者は、現況との突合・確認において IPA の MyJVN バージョンチェッカ等によるソフトウェア製品のバージョン確認の結果、サポート切れのソフトウェア製品の使用が判

明した場合、当該製品の更新の可否、更新した場合の影響の有無等の調査結果を踏まえ、PMDAに報告すること。

- ⑥ー5 受注者は、⑥ー4におけるPMDAへの報告によりサポート切れのソフトウェア製品の更新が可能と判断された場合は、ソフトウェア製品更新後、改めてPMDAに報告すること。

⑦ 運用・保守作業の改善

- ⑦ー1 受注者は、年度末に年間の運用実績、並びに運用計画書及び運用手順書に対する改善提案をとりまとめ、PMDAに提出すること。
- ⑦ー2 受注者は、運用を継続するにあたって、業務の効率化、利便性の向上に資するために、導入時に設定した内容を変更したい場合、PMDAの指示の下、変更する設定に関する問合せ対応及び変更作業を実施すること。なお、設計書等の改訂・作成作業も含むものとする。(年間1人月程度の作業とする。)

⑧ 引継ぎ

- ⑧ー1 受注者は、本契約の終了後に次期運用・保守支援事業者が本業務の運用・保守を受注した場合には、次期運用・保守支援事業者に対し滞りなく運用・保守業務が担えるよう、作業経緯、残存課題等について以下の事項を整理し、引継ぎを行うこと。

- ・ 各種計画書、各種設計書、実作業で用いていた運用手順書、操作マニュアル等、運用作業を実施するために必要な資料一式
- ・ 残存課題一覧(リスク引継ぎ事項、改善提案引継ぎ事項、案件特性及びシステム特性に伴う個別引継ぎ事項等)

- ⑧ー2 引継ぎに際し、作業経緯、残存課題等に関してPMDA及び次期運用・保守支援事業者から情報提供依頼、質疑等があった場合には速やかに対応すること。それらにかかる費用は本調達に含まれる。

- ⑧ー3 本契約の終了後も、シグナル検出製品を用いて行う業務をそのまま継続する場合があることから、受注者は、本契約期間中に必要に応じてPMDA、次期システム構築事業者及び次期運用・保守支援事業者に対して引継ぎを行うこと。引継ぎの際には、次期システム開発のための要件定義業務支援、データ移行作業、受注者導入システムの仕様理解のための援助(システム仕様が把握できる権限の付与も含む)等を実施し、次期システム構築事業者及び次期運用・保守支援事業者が契約開始日から円滑に業務を実施できるよう、引継ぎ手順等を整備した資料をPMDAに提出すること。

- ・ 本調達の契約終了に伴い次期システムへの移行が発生する場合、受注者は次期システム構築事業者及び次期運用・保守支援事業者に対し、円滑な移行に不

可欠な技術情報(設計書、設定値、API仕様等)を提供し、必要な助言・協議に応じなければならない

- ・ 契約終了前の引継ぎ期間において、次期事業者との定例会議への参加や、QA対応を行うこと。なお、引継ぎ期間については、契約後、PMDAと協議のうえ、決定する
- ・ PMDAの要求に基づき、システム内の全データを汎用的な形式(CSV、JSON、XML等)で一括出力できる機能又は手段を提供すること
- ・ クラウド上のデータの所有権はPMDAに帰属する。契約終了時には、PMDAの指示に従いデータを完全に抹消し、その旨を記載したデータ消去証明書を作成し、当該作業に係る作業ログを添付のうえ、PMDAに提出すること
- ・ 納品される設計書、運用マニュアル等は、PMDA側で改変・再利用が可能な形式(Microsoft Office形式等)で納品すること
- ・ 受注者の権利を侵害しない範囲で、クラウド上のリソース構成図、ネットワーク構成、採用しているマネージドサービスの一覧の最新版を、PMDAに定期的に報告すること
- ・ 本調達に特化した機能に対する開発にて使用したサードパーティ製ソフトウェアのライセンスは、他のシステムに移行した場合もPMDAが継続利用できる(又は名義変更が可能である)形態を選択すること

⑧-4 受注者は、PMDAが将来関連する調達等を行う際には、PMDA及び安対システム運用・保守支援事業者に対し、作業経緯、残存課題等に関する情報やデータの提供及び質疑応答等の協力を行うこと。

⑨ システム資産簿

受注者はシステム資産簿に以下に定める項目を記載すること。

⑨-1 各データの変更管理

情報システムの運用において、ハードウェアの管理、ソフトウェアの管理、回線の管理、外部サービスの管理、施設の管理、公開ドメインの管理、取扱情報の管理、情報セキュリティ要件の管理、指標の管理の各項目についてその内容に変更が生じる作業をした時は、当該変更を行った項目

⑨-2 作業実績等の管理

情報システムの運用中に取りまとめた作業実績、リスク、課題及び障害事由

⑨-3 スケジュール、工数等の管理

スケジュール、工数等の計画値及び実績値

(3) 管理に係る事項について

① プロジェクト管理

PMDA の承認を受けた業務実施要領に基づき、本業務が遅滞なく進捗するよう管理すること。管理にあたっては、以下に留意すること。

- ・ プロジェクトの状況を正しく把握し、計画工数内で所定の期日までに納入成果物を作成することを目的として、業務実施計画書に記載した管理手法に基づき、EVM、WBS 等による予実管理を実施すること
- ・ 受注者側のプロジェクトマネージャが、本業務におけるあらゆるタスクのあらゆるリスクについて、その発現を未然に防ぐための措置を施すとともに、発現時の対応方針を事前に検討しておくこと。発現の蓋然性が高く、また発現がプロジェクトの方針の大幅な変更を要すると考えられるリスクについては、発現時の対応方針案について事前に PMDA と相談する等して、発現時のインパクトを最小限に留めるよう工夫すること
- ・ 万が一、リスクが発現した場合は、可及的速やかに対応し被害を最小化するとともに、速やかに進捗を正常化するための措置を施すこと
- ・ プロジェクト体制の中に複数のサブチームを設ける場合、サブチーム間で必要な情報共有を適切に行うこと
- ・ 受注者は、進捗状況、課題、リスク等を業務実施計画書に基づいて月次で PMDA に報告すること。進捗状況は、報告時点までの計画工数(Planned Value)と実績工数(Earned Value)を示して定量的に報告すること。報告の様式等に関しては、業務開始時に PMDA と協議し決定すること

(4) 契約金額内訳の提出に係るその他の作業の内容

受注者は、契約金額の内訳を記載した Microsoft Excel 形式の電子データを契約締結後速やかに提出すること。

(5) 情報の抹消作業について

情報・資料の取扱いについては、本調達仕様書「1.10. 作業の実施にあたっての遵守事項」も併せて参照すること。

① データの返還・エクスポート

本契約の終了（期間満了、解約、解除を含む。以下同じ）に当たり、受注者は PMDA に対し、以下を実施すること。

- ・ 受注者が保有する全データ(コンテンツ、設定情報、ログ等)について、PMDA が指定する汎用的なデータ形式(CSV、JSON、標準的なファイル形式等)でエクスポート可能にすること。また、受注者自ら実施できるよう必要な技術情報、API、又はツールを提供するこ

と

- ・ PMDA によるデータの回収期間として、契約終了後少なくとも 30 日間は、全データに対して PMDA が提供を求めた場合には受注者は提供すること

② データの修正

- ・ 受注者は、本サービスを提供するために使用した全ての記録媒体（ストレージ、バックアップメディア、キャッシュサーバ等）から、全データを復元不可能な状態で論理的又は物理的に消去すること
- ・ バックアップデータについても、その保持ポリシーに基づく最短の期間内に消去が完了することを確認すること
- ・ 故障等により交換された記録媒体が受託者の管理外へ搬出される場合は、事前に物理的破壊又は磁氣的消去を行い、データの復元を不可能にすること

(6) クラウド環境のセキュリティ確保に係る作業内容

導入製品について、ISMAP を取得していることが望ましい。詳細は「別紙 2 非機能要件定義書」の 11.(4)①を参照すること。

1.8.3. 納入成果物の範囲、納入期限等

本調達における納入成果物を表 4 に示す。ただし、納入成果物の構成、詳細、スケジュールについては、受注後、PMDA と協議し取り決めること。納入成果物の作成にあたっては、SLCP-JCF2013（共通フレーム 2013）を参考とすること。また、各成果物の詳細については、「別紙 4 各納入成果物に記載する事項について」を参照すること。

なお、設計・開発によって納品されるドキュメントについては、記載レベル、記載内容等を明らかにし、メンテナンス性を考慮したものとすること。

表 4 工程と納入成果物

No.	工程	納入成果物	納入期日
1	実施計画	・ 業務実施計画書 ・ 業務実施要領 ・ 情報セキュリティ管理計画書	令和 8 年 12 月 31 日
2	要件確認	・ 要件適合性評価一覧 (Fit&Gap 一覧) ・ Gap 対応方針書	令和 9 年 1 月 31 日

No.	工程	納入成果物	納入期日
3	設定検討・構築	- 方式設計書 - 画面・操作基本設計書 - 権限・ロール基本設計書 - データ基本設計書(論理レベル) - 外部連携基本設計書 - 運用基本設計書 - 設定詳細設計書 - 設定作業報告書 - 権限設定詳細設計書 - 外部連携詳細設計書 - データ移行詳細設計書 - 運用手順詳細設計書 - クラウド環境設計書 - 標準開発ポリシー定義書 - クラウドサービス導入報告書	令和9年7月31日
4	テスト	- テスト計画書 - テスト結果報告書 - テスト結果エビデンス - テストデータ	令和9年11月30日
5	導入	- 導入計画書 - 導入手順書 - 導入作業結果報告書	令和9年12月31日
6	移行	- 移行計画書 - 移行手順書 - 移行作業結果報告書	令和9年12月31日
7	運用・保守	- 運用計画書 - 運用手順書 - 保守計画書 - 保守手順書 - 情報セキュリティ対策実施報告書	令和9年11月30日
8	教育	- 教育計画書 - 教育実施結果報告書 - 利用マニュアル	令和9年11月30日
9	その他	- 打合せ資料(※) - 議事録(※) - 運用・保守作業報告書(※) - 残存課題一覧(※) - 機密情報受理管理簿 - 開発に係る中間成果物(※) - 契約不適合責任対応に係る保有情報の一覧 - 情報の返却又は廃棄若しくは抹消に係る作業実施計画書 - 最終報告書	令和11年3月31日 (※必要に応じて随時提出)
		- データ消去証明書 - 情報の返却又は廃棄若しくは抹消に係る作業完了報告書	令和11年3月31日

(1) 納品方法

- ① 納入成果物は、全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。
- ② 用字・用語・記述符号の表記については、「公用文作成の考え方(建議)(令和4年1月7日文化審議会)」に準拠すること。

- ③ 情報処理に関する用語の表記については、原則、日本産業規格(JIS)の規定に準拠すること。
- ④ 納入成果物は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。なお、納入部数はPMDAと協議すること。
- ⑤ 紙媒体で納品する場合の用紙のサイズは、原則として日本産業規格 A 列 4 番とするが、必要に応じて日本産業規格 A 列 3 番を使用すること。
- ⑥ 外部電磁的記録媒体 1 部を、案件名、受注者名、納入年月日を表記して納品すること。なお、納入成果物一覧(紙)を添付すること。
- ⑦ 外部電磁的記録媒体による納品物のうち、計画書等のドキュメントファイルについて、ファイルは Microsoft 365 で読み込みが可能なファイル形式で作成すること。ただし、当該ファイル形式で納品が困難な場合は、PMDA と事前に協議のうえ、PDF のファイル形式で作成すること。なお、PMDA が他の形式による提出を求める場合、又は受注者側で他の形式を用いて提出したい場合には、協議のうえで決定することとする。
- ⑧ 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。
- ⑨ 納入成果物に修正等があった場合、紙媒体については、それまでの変更内容を表示するとともに変更履歴と変更ページ、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。
- ⑩ 納品後、納入成果物について PMDA において改変が可能となるよう、図表等の元データも納品すること。
- ⑪ 納入成果物の作成に当たって、特別なツールを使用する場合は、PMDA の承認を受けること。
- ⑫ 一般に市販されているツール、パッケージ類の使用は PMDA と協議のうえ、必要と判断された場合であれば使用を認めるが、特定ベンダーに依存する(著作権又は著作者人格権を有する)ツール等は極力使用しないこと。新規のツール等を使用する場合、又はライセンスの追加が必要となる場合は、本稼働後 5 年間のライセンス及びメディアを納入すること。
- ⑬ 納入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、納入成果物の情報セキュリティの確保に留意すること。
- ⑭ 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、納入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。なお、対策ソフトウェアに関する情報(対策ソフトウェア名称、定義パターンバージョン、確認年月日)を記載したラベルを貼り付けること。
- ⑮ 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。
- ⑯ 報告書、計画書等の納入成果物の記載様式については、記載様式案を提示のうえ、PMDA と協議のうえ、決定すること。

- ⑰ 納入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。

(2) 納品場所

原則として、納入成果物は次の場所において引き渡すこと。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。

〒100-0013

東京都千代田区霞が関 3-3-2 新霞が関ビル

独立行政法人 医薬品医療機器総合機構

安全性情報・企画管理部 情報管理課

1.9. 作業の実施体制・方法に関する事項

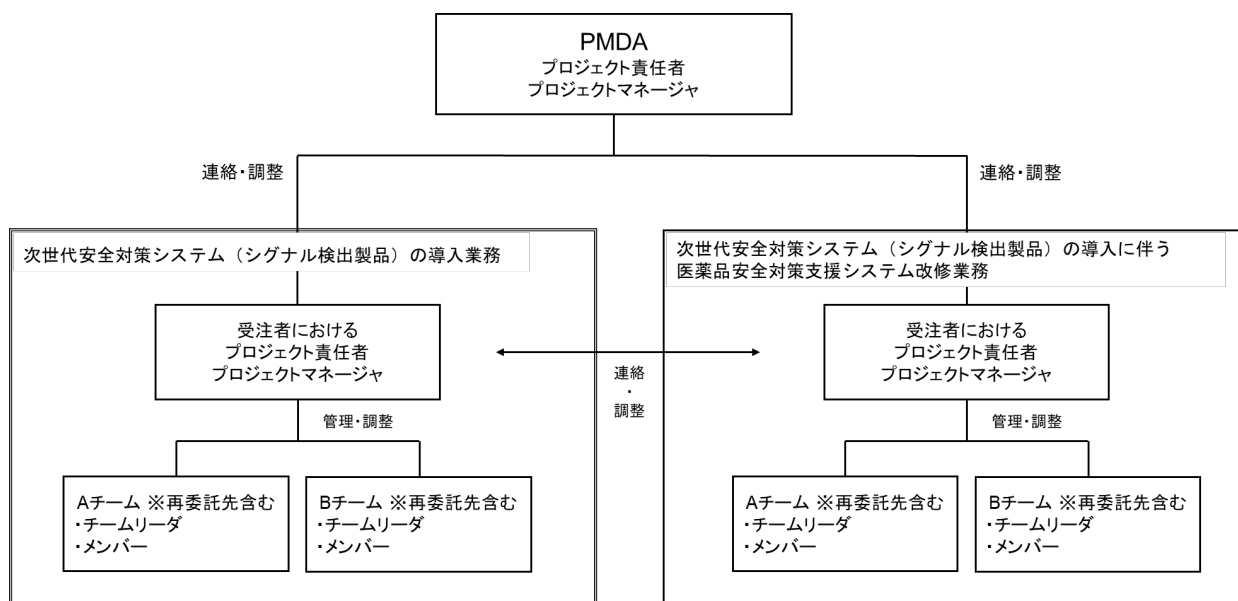
1.9.1. 作業の実施体制

(1) 作業実施体制

受注者に求める作業実施体制は図 3 のとおりである。以下の事項も踏まえて、必要な作業実施体制を構築すること。

- ・ プロジェクトマネジメントに係る品質管理、進捗管理、セキュリティ管理、リスク管理等の必要な機能を体制に組み込むこと
- ・ 作業体制の品質確保のため、本調達のプロジェクト責任者及びプロジェクトマネージャは業務開始から業務終了まで継続して遂行すること。交代する場合は同等以上の要員が担当するものとし、事前に PMDA の承認を受けること
- ・ 受注者は、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受注者に求める作業実施体制を PMDA と協議のうえ決定すること。
- ・ システム設計・開発等を複数事業者が連携(再委託を含む。)して実施する場合は、参画する各事業者の役割分担等を明示すること
- ・ PMDA、製品販売事業者(受注者と同一の場合を含む。)、次世代安全対策システム(シグナル検出製品)の導入に伴う医薬品安全対策支援システム改修業者間の意見調整、技術的調整、進捗管理等を行う体制を構築すること

図 3 作業実施体制



なお、受注者内のチーム編成については想定であり、契約後に協議のうえ、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) 管理体制

受注者は本業務の実施に当たり、以下の管理体制を構築すること。

- 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よう、一貫した品質保証体制の下で管理されていること。また、当該品質保証体制が書類等で確認できること。
 - ・ 情報システムに PMDA の意図しない変更が行われる等の不正が見つかった場合（不正が行われていると疑わしい場合も含む。）に、追跡調査、立入検査等、PMDA と受注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
 - ・ 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）及び実績に関する情報提供を行うこと
- ② 受注者は、本業務で知り得た情報を適切に管理するため、次に掲げる体制（表 5）を確保し、当該体制を確保していることを証明するため、PMDA に対し「情報取扱者名簿」（業務の一部を再委託する場合は再委託先も含む。）、「情報セキュリティを確保するための体制を定めた書面（情報管理体制図、情報管理に関する社内規則等）」（業務の一部を再委託する場合は再委託先も含む。）及び「業務従事者名簿」を提出すること。

表 5 確保すべき体制

- ・ 情報取扱者は、本業務の遂行のために最低限必要な範囲の者とする
- ・ 受注者が本業務で知り得た情報について、PMDA が承認した場合を除き、受注者の役員等を含め、「情報取扱者名簿」※¹に記載のない者に伝達又は漏えいされないことを保証する履行体制を有していること
- ・ 受注者が本業務で知り得た情報について、PMDA が承認した場合を除き、受注者の親会社、地域統括会社、ブランド・ライセンサー、フランチャイザー、コンサルタントその他の受注者に対して指導、監督、業務支援、助言、監査等を行う者を含め、受注者以外の者に伝達又は漏えいされないことを保証する履行体制を有していること
- ・ 受注者は、「情報取扱者名簿」、「情報セキュリティを確保するための体制を定めた書面（情報管理体制図、情報管理に関する社内規則等）」及び「業務従事者名簿」※²に変更がある場合は、あらかじめ PMDA に申請を行い、承認を受けなければならないこと
- ・ 受注者は、本業務で知り得た情報について、PMDA が承認した場合を除き、受注者の役員等を含め、情報取扱者以外の者に伝達又は漏えいしてはならないこと。受注者は、本業務で知り得た情報について、PMDA が承認した場合を除き、受注者の親会社、地域統括会社、ブランド・ライセンサー、フランチャイザー、コンサルタントその他の受注者に対して指導、監督、業務支援、助言、監査等を行う者を含め、受注者以外の者に伝達又は漏えいしてはならないこと
- ・ 本業務の「業務実施計画書」を作成し、PMDA に提出すること。提出後変更が生じた場合には、速やかに変更後の「業務実施計画書」を提出すること
- ・ 本業務の実施に当たっては、作業工程別に責任者を定めるとともに、調査票等の管理に万全を期さなければならない。また、個人情報の管理に当たっては、管理責任者を定めるとともに、台帳等を設け個人情報の管理状況を記録すること。さらに、本業務の責任者の職名・氏名、作業の従事人数及び個人情報の管理状況について、あらかじめ書面で PMDA に提出すること
- ・ 本業務の進捗状況について、定期的に書面等で報告すること。また、PMDA が求めた場合には、速やかに報告すること

※1:「情報取扱者名簿」には、情報管理責任者、情報取扱管理者、その他保護を要する情報を取り扱う可能性のある者について、氏名、所属部署、役職等を、業務の一部を再委託する場合は再委託先も含めて、記載すること。なお、情報管理責任者は、情報の取扱いに関して、情報セキュリティが侵害された又はそのおそれがある場合等の非常時における対策を定めるとともに、その内容を従事者に徹底すること。また、情報取扱管理者を指定

すること。

※2:「業務従事者名簿」には、本業務に従事する者について、氏名、所属部署、役職、業務経験、研修実績その他の経歴、専門的知、その他の知見等を記載すること。

(3) 作業要員に求める資格等の要件

- ① 開発に携わる遂行責任者は IPA の「プロジェクトマネージャ」資格、PMAJ の「PMS」資格、PMI の「PMP」資格のいずれかを取得していること。
- ② 情報セキュリティ対策の管理体制の責任者は、情報処理の促進に関する法律(昭和 45 年 5 月 22 日法律第 90 号)に基づく情報処理安全確保支援士の登録を受けている者又は同等の資格を有する者であること。
- ③ プロジェクトマネージャは、情報システムの設計・開発又はシステム基盤導入の経験年数を 3 年以上有すること。また、その中でリーダクラスとしての経験を 3 件以上有すること。なお、前述の経験に満たない場合には同等の能力を持つことを PMDA に説明し、承認を受けること。
- ④ 設計・開発を行う担当者は、医薬品安全対策のうち医薬品副作用報告等に係る業務を理解しており、本業務システムの設計に当たり、PMDA の業務要件について適切な理解を前提として、必要な技術的・業務的な事項について円滑に協議・意思疎通ができる知識及び経験を有すること。システムのデータ構造の概要を理解できる能力を有しており、システムを構成するハードウェア及びソフトウェアの基礎知識を有し、システム及び関連ソフトの基本操作を理解していること。
- ⑤ PMDA とシグナル検出製品販売事業者(受注者と同一の場合を含む。)との間において意見調整、技術的調整、進捗管理等の調整業務を行う調整担当者は、安全対策業務及び導入対象製品の特性を理解し、PMDA の業務上の要望・課題等を適切に整理し、シグナル検出製品販売事業者に対して技術的に齟齬のない形で伝達するとともに、シグナル検出製品販売事業者から提示される技術的説明、検討結果等について、PMDA が理解できるよう分かりやすく説明する能力及び経験を有すること。また、以下の日本語能力を有すること。
 - ・ PMDA との会議において、通訳を介することなく、業務要件、技術的事項及び進捗状況について正確な説明及び意見交換ができること
 - ・ 日本語で作成された業務資料、設計資料、議事録等を正確に理解し PMDA の求めに応じて日本語による説明及び文書作成(整理資料、説明補足資料、議事録(案)の作成等)ができること

(4) 作業場所

- ① 本業務の作業場所及び作業に当たり必要となる設備、備品、消耗品等については、受注者の責任において用意すること。また、必要に応じて PMDA が現地確認を実施することができるものとする。
- ② PMDA 内での作業は、必要な規定の手続きを実施し承認を受けること。
- ③ 本業務の作業場所等については、以下の要件を満たすことがわかる資料を提出すること。なお、③-1 で言及する作業場所及び設備・機器については、概要が把握できる写真を添付すること。
 - ③-1 作業場所及び作業に必要となる設備・機器、備品、消耗品等は、受注者の責任において用意すること。
 - ③-2 本業務の作業場所は、原則、日本国内とすること。なお、日本国外が作業場所となる場合には、当該環境でも日本国内と同様の管理体制にて作業できることを説明し、PMDA の承認を受けること。
 - ③-3 本業務のデータの保管場所は、日本国内のみとすること。
 - ③-4 本業務の作業場所及びデータの保管場所における情報漏えいを防ぐため、入退室管理等の対策を講じること。
 - ③-5 資料を保管する鍵付きの棚を用意すること。
 - ③-6 本業務で使用する機器に対し必要なセキュリティ対策等を講じること。

1.9.2. 作業の管理に関する要領

受注者は次に掲げる事項を遵守すること。

- ・ 受注者は、PMDA が承認した業務実施要領に基づき、導入業務に係るコミュニケーション管理、体制管理、工程管理、品質管理、リスク管理、課題管理、システム構成管理、変更管理及び情報セキュリティ対策を行うこと
- ・ 受注者は作業の進捗状況等を報告するため、PMDA の担当職員と会議を定期的に行うこと。また、当該会議の開催を業務実施要領に記載すること
- ・ コミュニケーション管理は、会議体(名称、目的、頻度及び参加者)、資料及び議事録(案)の提出期限(3 営業日以内)並びに連絡方法を記載すること
- ・ 進捗管理は、報告頻度、報告様式及び管理方法を記載すること。また、本調達仕様書「1.8.2.(3) 管理に係る事項について」に従うこと
- ・ リスク管理は、報告頻度、報告様式及び管理方法を記載すること。なお、報告様式にはリスク一覧及びリスク対応策を記載し、定期的又は必要に応じて都度報告すること
- ・ 課題管理は、課題管理表の様式を記載し、定期的又は必要に応じて都度報告すること
- ・ 変更管理は、変更一覧の様式及び変更管理プロセスを記載し、定期的又は必要に応じて都度報

告すること

- ・ 構成管理及び文書管理は、受領した資料の管理方法、構成管理の対象、構成管理に使用するツール等を記載すること
- ・ セキュリティ対策は、本調達仕様書「1.10.4. 情報セキュリティ管理」の情報セキュリティ対策を記載し、履行状況報告を月次で報告すること
- ・ 品質管理は、レビュー計画、品質目標及び工程完了基準を記載すること
- ・ 受注者は会議の開催に当たり、都度、原則 1 営業日前までに打合せ資料(ドラフト版も可とする)を送付する。また、会議終了後原則 3 営業日以内に議事録(案)を作成し、受注者側の関係者に内容を確認した上で、PMDA の承認を受けること
- ・ 情報漏えい、作業計画の大幅な遅延等の問題が生じた場合は、PMDA のプロジェクト責任者に報告すること。なお、緊急を要する場合には、PMDA のプロジェクト責任者及び窓口担当者に連絡すること

1.10. 作業の実施に当たっての遵守事項

1.10.1. 基本事項

受注者は、次に掲げる事項を遵守すること。

- ・ 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
- ・ 本業務に従事する要員のうち、PMDA、次世代安全対策システム(シグナル検出製品)の導入に伴う医薬品安全対策支援システム改修業者等との連絡、調整及びその他のコミュニケーションを担当する要員は、日本語による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
- ・ PMDA 内部で作業する際は、本業務の履行場所を他の目的のために使用しないこと。また、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
- ・ 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た火災・盗難等の不祥事が発生した場合、一切の責任を負うこと
- ・ 受注者は、本業務の履行に際し、PMDA からの質問、検査、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、協議の場を設けて対応すること
- ・ 本業務により導入した製品及び関連する設定内容、運用方法、データ連携方式等について、PMDA が将来関連する調達等の実施に当たり技術的な確認を行う必要がある場合は、受注者は合理的な範囲で技術的支援、情報提供、質疑応答及び助言を行うこと。本業務においては、受注者による業務終了後、次期運用・保守支援事業者でも運用等が可能となるよう、手順書等のドキュメント類の整備を詳細に行うこと

1.10.2. 機密保持、情報・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、本業務の実施の過程で PMDA が提供した情報・資料（公知の情報を除く、以下同様）、本調達に係る事業者が提示及び作成した情報・資料を、本業務の目的以外に使用若しくは第三者に開示又は漏えい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。なお、PMDA が提供した情報及び資料を第三者に開示する必要がある場合は、事前に協議のうえ、PMDA の承認を受けること。
- ② 受注者は、本業務を実施するに当たり、PMDA が提供した情報・資料については機密情報受管理管理簿により適切に管理し、かつ、以下の事項に従うこと。
 - ②－1 複製はしないこと。
 - ②－2 受注者組織内に移送する際は、暗号化、施錠等適切な方法により、情報セキュリティを確保すること。また、PMDA との調整等に必要の場合及び返却時以外は原則として、受注者組織外に持ち出さないこと。
 - ②－3 個人情報等の重要な情報が記載された情報・資料に関しては、原則として社外に持ち出さないこと。
 - ②－4 受注者組織内で作業を行う場合には、作業を行う施設は、IC カード等電磁的管理による入退館管理がなされていること。
 - ②－5 作業を行う施設内の作業実施場所は、IC カード等電磁的管理による入退室管理がなされていること。
 - ②－6 電磁的に情報・資料を保管する場合には、情報取扱者名簿に記載のない者がアクセスできないようアクセス制限を行うこと。また、アクセスログにより不審なアクセスがないか確認すること。
 - ②－7 情報・資料を保管する端末、サーバ装置等は、受注者の情報セキュリティポリシー等により、サイバー攻撃に備え、ウイルス対策ソフト、脆弱性対策、検知・監視等の技術的対策が講じられ、適切に管理・運用される必要があるため、政府機関等の対策のための統一基準や PMDA サイバーセキュリティポリシーに準拠して管理等すること。準拠した対応ができない場合は、代替のリスク軽減策を講じ、PMDA の承認を受けること。
 - ②－8 用務に必要ななくなり次第、速やかに PMDA に返却すること。
 - ②－9 本業務完了後、PMDA が提供した情報・資料を返却し、受注者において当該情報を保持しないことを誓約する旨の書類として「別添様式 3 秘密保持等に関する誓約書」を PMDA へ提出すること。
- ③ 応札希望者についても 1.10.2①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 「別添様式 3 秘密保持等に関する誓約書」を提出し、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。
- ⑦ 機密保持及び情報・資料の取扱いについて、適切な措置が講じられていることを確認するため、PMDA が遵守状況の報告や実地調査を求めた場合には応じること。
- ⑧ 本業務で作成したデータ等については、業務の終了に伴い不要となった場合、若しくは PMDA から廃棄又は抹消の指示があった場合には、回復が困難な方法により速やかに廃棄又は抹消すること。なお、受注者が用意するヘルプデスク機材や開発・運用機材等のうち、個人情報を取り扱う場合を含むものとする。実施方法等について以下の項目を履行できるよう、「別添様式 1 情報の返却又は廃棄若しくは抹消に係る作業実施計画書」を定義し PMDA の承認を受けた上で速やかに実施し、実施後においては「別添様式 2 情報の返却又は廃棄若しくは抹消に係る作業完了報告書」を PMDA に速やかに提出すること。また、情報セキュリティ管理計画書等において当該作業実施計画書に相当する内容が記載されている場合は、情報セキュリティ管理計画書等を当該作業実施計画書に代えても差し支えない。

1.10.3. 遵守する法令等

- ① 次の文書の最新版を遵守すること。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。
 - ・ 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
 - ・ 独立行政法人 医薬品医療機器総合機構 情報システム管理利用規程
 - ・ 独立行政法人 医薬品医療機器総合機構 個人情報管理規程なお、「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」は非公表であるが、「政府機関等のサイバーセキュリティ対策のための統一基準」に準拠しているため、必要に応じて参照すること。「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、契約締結後、受注者が PMDA に「別添様式 3 秘密保持等に関する誓約書」を提出した後に開示する。
- ② 本業務の実施において、現行情報システムの設計書等を参照する必要がある場合は、作業方法等について PMDA の指示に従い、「別添様式 3 秘密保持等に関する誓約書」を提出したうえで、作業すること。
- ③ 受注者は、本業務の実施において、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、個人情報の保護に関する法律等の関連する法令等を遵守すること。

1.10.4. 情報セキュリティ管理

受注者は、情報セキュリティ対策として、以下を含む情報セキュリティ管理計画書を契約締結後速やかに提出し、PMDA の承認を受けた上で、それに基づき情報セキュリティ対策を実施すること。なお、

PMDA は実施状況について、随時、実地調査できるものとする。

- ① PMDA から提供する情報の目的外利用を禁止すること。
- ② 本業務の実施に当たり、受注者又はその従業員、本調達の役務の内容の一部を再委託する先、若しくはその他の者による PMDA の意図しない不正な変更が情報システムのハードウェア、ソフトウェア等に加えられないための管理体制が整備されていること。
- ③ 受注者の資本関係、役員等の情報、本業務の実施場所、本業務従事者の所属・専門性(情報セキュリティに係る資格・研修実績等)及び実績に関する情報提供を行うこと。
- ④ 情報セキュリティインシデントへの対処方法(対処手順、責任分界、対処体制、対応時間、情報伝達時間・手段等)が確立されていること。
- ⑤ 情報セキュリティ対策や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。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 の承認を受けたうえで実施すること。
- ⑥ PMDA が求めた場合に、速やかに情報セキュリティ監査を受け入れること。
- ⑦ 本調達の業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。
- ⑧ 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方法にて行うこと。
- ⑨ 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、「別添様式 2 情報の返却又は廃棄若しくは抹消に係る作業完了報告書」にて報告すること。
- ⑩ 本業務において、情報セキュリティインシデントの発生、情報の目的外利用等を認知した場合は、速やかに PMDA に連絡すること。
- ⑪ 業務において導入する通信回線装置、サーバ装置、端末、複合機、特定用途機器、ソフトウェア、周辺機器及び外部電磁的記録媒体がある場合は、製造業者名、製造業者の法人番号、製品名、型番等を記載した機器リストを、「別添様式 4 機器リスト」を用いて作成し、情報セキュリティ管理計画書の一部として、技術提案書の提出期限の 15 営業日前までに提出すること。提出された機器リストについて、PMDA がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、当該リスクに対応するため、代替品又はリスク低減対策の提出を求めることがあるので留意すること。なお、機器リストに記載された機器等を変更する場合には、事前に PMDA に申請し、承認を受けること。

1.10.5. 情報セキュリティ監査

本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、PMDA が情報セキュリティ監査の実施を必要と判断した場合は、PMDA がその実施内容(監査内容、対象

範囲、実施者等)を定めて、情報セキュリティ監査を行う。なお、PMDA が選定した事業者による外部監査を含むこととする。

- ① 受注者は、PMDA から情報セキュリティ監査の求めがあった場合に、速やかに情報セキュリティ監査を受け入れる部門、場所、時期、条件等を情報セキュリティ監査対応計画書等により提示し、監査を受け入れること。
- ② 受注者は自ら実施した外部監査についても PMDA へ報告すること。
- ③ 情報セキュリティ監査の実施については、これら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。
- ④ 業務履行後であっても、本業務に関する情報漏えい等が発生した場合には、監査を受け入れること。
- ⑤ 受注者は、情報セキュリティ監査の結果、本調達における情報セキュリティ対策の履行状況について PMDA が改善を求めた場合には、PMDA と協議のうえ、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。
- ⑥ 本調達に関する監査等が実施される場合、受注者は、技術支援及び情報提供を行うこと。
- ⑦ 受注者は、指摘、進捗等把握のための資料提出依頼等があった場合は、PMDA と協議のうえ、内容に沿って適切な対応を行うこと。

1.10.6. 本業務履行完了後の資料の取扱い

受注者は、PMDA から提供した資料又は PMDA が指定した資料の本業務履行完了後の取扱い(返却、削除等)について、本調達仕様書の定めその他、PMDA の指示に従うこと。

1.10.7. 疑義

本調達仕様書に明記されていない事項、又は疑義が生じた場合は PMDA と協議のうえ、決定するものとする。また、本調達仕様書に明記されていない事項であっても、業務実施のうえで当然行わなければならないと認められるものについては、受注者において補足するものとする。

2. サービスの変更・終了

2.1. サービス変更・終了時の事前告知

受注者は、本サービス¹⁾の全部又は一部を廃止、若しくは業務に重大な影響を及ぼす仕様変更を行う場合、原則として実施の 12 か月前までに PMDA へ書面で通知するものとする。これ以外の軽微な仕様変更については、実施の 1 か月前にまでに PMDA へ書面で通知するものとする。

1) 「サービス」とは、本調達仕様書に記載されている範囲の機能を指す。

2.2. サービス変更・終了時の報告

サービスを変更又は終了した場合は、実施後、5 営業日以内に電子メール又は電話にて報告する。

2.3. サービス終了の対応

サービスの変更・終了に伴い、PMDA が他のサービスへの移行を希望する場合、受注者はデータの移行に必要な技術的支援を無償で行い、汎用的な形式でのデータ抽出を保証すること。

また、受注者の都合によるサービス終了により PMDA に損害が生じた場合、受注者はその賠償責任を負うものとする。

2.4. サービス窓口

2.4.1. 営業日・時間

サービスサポートは、電子メール又は電話により受け付けるものとする。なおサポート受付日時については、別途 PMDA と協議するものとする。

2.4.2. サポート対応

問い合わせを受けた内容については、1 営業日以内を目途に回答するものとする。

2.4.3. 事故発生時の責任と保障範囲

受注者の責めに帰すべき事由によりデータが消失・外部漏洩した場合、受注者は PMDA に対し損害賠償すること。なお、損害の範囲と損害額については、双方協議のうえ、決定する。

3. 成果物の取扱いに関する事項

3.1. 知的財産権の帰属

- ① 本調達に係り作成されるドキュメント類の著作権(著作権法第 21 条から第 28 条までに定める全ての権利を含む。)は、受注者が調達の情報システム開発の従前から権利を保有していた等の明確な理由により、あらかじめ技術提案書にて権利譲渡不可能と示されたもの以外、PMDA が所有する現有資産を移行等して発生した権利を含めて全て 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を行使しないものとする。
- ③ 本調達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 本調達に係り作成されるドキュメント類等に既存著作物等が含まれる場合、受注者は当該既存著作物等の使用に必要な費用負担、使用許諾契約等に係る一切の手続きを行うこと。こ

の場合、受注者は、事前に既存著作物等の内容について PMDA の承認を受けることとし、PMDA は、既存著作物等について当該許諾条件の範囲で使用するものとする。

- ⑤ 本調達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、受注者の責任及び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時は、受注者に通知し、必要な範囲で訴訟上の防衛を受注者に委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受けるものとし、PMDA に提出する際は、その旨併せて報告するものとする。

3.2. 検査

- ① 本調達仕様書「1.8.3.納入成果物の範囲、納入期限等」に則って、納入成果物を提出すること。その際、PMDA の指示により、別途、品質保証が確認できる資料を作成し、納入成果物と併せて提出すること。
- ② 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、指定した日時までに修正が反映された全ての納入成果物を納品すること。
- ③ 本調達仕様書「1.8.3 納入成果物の範囲、納入期限等」に依る以外にも、必要に応じて納入成果物の提出を求める場合があるので、作成資料は常に管理し、最新状態に保っておくこと。
- ④ 特段の事情がない限り、受注者においても全数検査又はサンプル検査を行うこと。

3.3. 契約不適合責任

- ① 受注者は、本業務の納入成果物に対する契約不適合責任を負うものとする。本業務の最終検収後において、委託業務の納入成果物に関して仕様書と異なる、又は契約目的に照らして通常期待される条件を満たしていない等、情報システムの正常な稼働等に関わる契約不適合の疑いが生じた場合であって、PMDA が検収後 1 年以内に調査を求めた場合は、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 の承認を受け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 受注者は、契約不適合責任を果たす上で必要な情報を整理し、その一覧を 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、当該情報が漏洩しないよう、ISO/IEC27001 認証(国際標準規格)又は JISQ27001 認証(日本産業規格)に従って管理すること。加えて、個人情報を取り扱う場合には JISQ15001(日本産業規格)に従い、厳重に管理をすること。ま

た、契約不適合責任の期間が終了した後は、速やかにデータ復元ソフトウェア等を利用してデータが復元されないように当該情報を完全に消去すること。データ消去作業終了後、受注者は、データ消去が完了した旨を記載したデータ消去証明書を作成し、当該作業に係る作業ログを添付のうえ、PMDAに提出すること。なお、データ消去作業に必要な機器等については、受注者の負担により用意すること。

4. 入札参加資格に関する事項

4.1. 入札参加要件

4.1.1. 公的な資格や認証等の取得

- ① 品質管理体制について ISO9001:2015(国際規格)、組織としての能力成熟度について CMMI レベル 3 以上のうち、いずれかの認証を受けていること。認証を有していない場合は、品質管理の取組みについて説明すること。
- ② プライバシーマーク付与認定、JIS Q 15001 認証(日本産業規格)、ISO/IEC27701 認証(国際規格)、ISO/IEC27001 認証(国際規格)、JIS Q 27001 認証(日本産業規格)のうち、いずれかを取得していること。
- ③ 本調達において導入予定のシグナル検出製品について、欧米規制当局又はそれと同等の公的機関若しくは複数の製薬企業への導入経験があること。なお、入札におけるプレゼンテーションにおいては、当該製品の導入実績(導入先、運用期間、現時点の運用状況等)に加え、将来的なシグナル検出手法の高度化、分析機能の追加等への対応方針、今後の機能拡張計画、開発ロードマップの概要及び開発体制について説明すること。
- ④ 応札者は、調達製品並びに医薬品副作用報告等に係る業務内容及び当該業務に関連する制度・手続について一定の理解を有していること。なお、当該理解の程度については、入札におけるプレゼンテーションにおいて確認する。
 - ・ 応札者は、本調達仕様書の「別紙 1 機能要件定義書(次世代安全対策システム(シグナル検出製品)の導入業務)」、「別紙 2 非機能要件定義書」について理解を有していること。また、入札におけるプレゼンテーションにおいて、調達製品における該当機能、及び各機能要件に対する対応内容(標準機能、設定変更又はカスタマイズの別を含む)を明示した上で、機能の利用方法、活用方法、適用範囲、制約等について、本調達で想定される業務を踏まえて具体的に説明すること
- ⑤ 応札時には、遂行する作業ごと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。
- ⑥ 本調達仕様書「7.2. 応札希望者が閲覧できる資料一覧」を指定期間内に閲覧すること。

- ⑦ 応札者は、本業務の実施に当たり、PMDA とシグナル検出製品販売事業者（応札者と同一の場合を含む。）との間の意見調整、技術的調整、進捗管理等を行う体制を構築すること。
- なお、これらの調整業務については、国内の第三者に再委託することを妨げない。その場合は、所定の手続きにより、事前に PMDA の承認を受けること。
- また、業務を行う者のうち、主担当者を入札におけるプレゼンテーションに参加させること。プレゼンテーションへの参加時点では、前述の PMDA の承認は不要とする。ただし、いずれの体制をとる場合であっても、本業務の履行結果及び成果物に係る責任は全て応札者が負うものとする。

4.2. 入札参加制限

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

5. 再委託に関する事項

5.1. 再委託の制限及び再委託を認める場合の条件

- ① 受注者は、本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。
 - ②-1 総合的企画、業務遂行管理、手法の決定、技術的判断等。
 - ②-2 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
 - ・ 機能ごと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

エア要件定義等業務

- 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、「再委託に係る承認申請書」を書面にて作成のうえ、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調達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、必要な措置を実施し、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、再委託先又はその従業員、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及び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ものとする
 - ・ 受注者は、再委託先が自ら実施した外部監査についても PMDA に報告すること
 - ・ 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

5.2. 承認手続き

- ① 本業務の一部を再委託する場合は、あらかじめ再委託の相手方の商号又は名称、住所及び再委託を行う業務の範囲、再委託の必要性並びに契約金額について記載した「再委託に係る承認申請書」を提出し、PMDA の承認を受けること。なお、再委託の相手方は本調達仕様書「4.2 入札参加制限」の対象となる事業者でないこと。

- ② 再委託先が本調達仕様書「1.10.4. 情報セキュリティ管理」の要件を満たしていることを証明する書面²⁾、及びに受注者と再委託先との委託契約書の写し、委託要領等の写しを、「再委託に係る承認申請書」に添付して提出すること。
- ③ 受注者は、機密保持、知的財産権等に関して本調達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、必要な措置を実施し、PMDA に報告し、承認を受けること。
- ④ 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)及び実績に関して、PMDA から求めがあった場合には情報提供を行うこと。
- ⑤ 当初申請内容に変更が生じた場合は「再委託に係る変更承認申請書」を提出すること。
- ⑥ 再委託の相手方から更に第三者に委託が行われる場合は、当該第三者の商号又は名称、住所、委託を行う業務の範囲等を記載した「履行体制図」を提出すること。

5.3. 再委託先の契約違反

再委託先において、本調達仕様書の遵守事項に定める事項に関する義務違反又は義務を怠った場合には、受注者が一切の責任を負うとともに、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。

6. その他特記事項

6.1. 環境への配慮

- 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 導入する機器については、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。

6.2. その他

- ① PMDA PMO が担当課室に対して指導、助言等を行った場合には、受注者もその方針に従うこと。
- ② 受注者は、デジタル・ガバメント推進に係る政府の各種施策、方針等(今後出されるものを含む。)に従うこと。

2) 情報セキュリティに関する管理体制と管理基準、社内規程が整備されている事実を証明する書面。(例：管理体制図、社内規程、ISO 認証、外部監査実績、等)

7. 附属文書

7.1. 別紙一覧（要件定義書を含む）

本調達仕様書にある要件内容等を補足するための文書を以下に定義する。

- ・ 別紙 1 機能要件定義書（次世代安全対策システム（シグナル検出製品）の導入業務）
- ・ 別紙 2 非機能要件定義書
- ・ 別紙 3 機能要件定義書（次世代安全対策システム（シグナル検出製品）の導入に伴う医薬品安全対策支援システム改修業務）
- ・ 別紙 4 各納入成果物に記載する事項について

7.2. 応札希望者が閲覧できる資料一覧

これらの資料は、PMDA に「別添様式 3 秘密保持等に関する誓約書」を提出した事業者に開示する。

- ・ 閲覧資料 1 システム及びネットワーク構成図案
- ・ 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 統合システム設計書
- ・ 閲覧資料 5 連携データ補足
- ・ 閲覧資料 6 クラウド環境セキュリティ関連確認事項

7.3. その他の資料

- ・ 別添様式 1 情報の返却又は廃棄若しくは抹消に係る作業実施計画書
- ・ 別添様式 2 情報の返却又は廃棄若しくは抹消に係る作業完了報告書
- ・ 別添様式 3 秘密保持等に関する誓約書
- ・ 別添様式 4 機器リスト

7.4. 契約締結後に開示する資料

契約締結後に受注者が閲覧を希望する場合に開示する資料は以下のとおり。

- ・ 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

8. 閲覧要領

応札希望者が資料の閲覧を希望する場合、以下の条件を満たした場合に閲覧を許可する。閲覧資料は CD/DVD にて提供する。

- ・ 公告期間中に本調達仕様書「10. 窓口連絡先」に連絡し、事前の了承を得ること。
- ・ 「別添様式 3 秘密保持等に関する誓約書」を閲覧当日までに提出すること。

なお、閲覧申込期間は公告日から開札日の1週間前までとし、閲覧用に貸し出したCD/DVDは開札日までに返却すること。

9. 技術提案書等の審査要領

技術提案書等の審査要領については、参加要項の別紙を参照すること。

10. 窓口連絡先

独立行政法人 医薬品医療機器総合機構 安全性情報・企画管理部 情報管理課

担当者: 滝波 ゆかり

電話: 03-3506-9482

メール: takinami-yukari@pmda.go.jp

※迷惑メール防止対策のため●を半角のアットマークに置き換えてください。

(別添様式 1)

令和 年 月 日

次世代安全対策システム(シグナル検出製品)業務に係る情報の返却又は廃棄若しくは抹消に係る
作業実施計画書

受注者名:

本業務において PMDA から受領した情報及び作成された情報については、下記のとおり返却又は廃棄若しくは抹消する予定です。

記

1 情報の保存媒体

情報の種類 (注1)	情報の 保存場所 (注2)	作業の方法 (注3)	作業の 確認方法	作業実施者	作業確認者
(例)紙媒体	キャビネット	返却	PMDA に手 交	〇〇	△△
(例)電磁的記録 媒体	端末	消去(データ抹 消ソフトウェア)	情報管理責 任者の立ち 会い	〇〇	△△

(注1)「紙媒体」、「電磁的記録媒体」のいずれかを記載すること。

(注2)「キャビネット」、「外部電磁的記録媒体(CD-R、USB メモリ等)」、「端末」、「サーバ装置」等を記載すること。

(注3)返却の場合:「返却」と記載すること。

廃棄・抹消の場合:「焼却」、「溶解」、「裁断」、「消去(データ抹消ソフトウェア)」等を記載すること。

2 全ての作業が完了する予定日

令和 年 月 日

(別添様式 2)

令和 年 月 日

次世代安全対策システム(シグナル検出製品)に係る情報の返却又は廃棄若しくは抹消に係る
作業完了報告書

受注者名:

本業務において PMDA から受領した情報及び作成された情報については、下記のとおり返却又は廃棄若しくは抹消しましたので、報告します。

記

1 情報の保存媒体

情報の種類 (注1)	情報の 保存場所 (注2)	作業の方法 (注3)	作業の 確認方法	作業実施者	作業確認者
(例)紙媒体	キャビネット	返却	PMDA に手 交	〇〇	△△
(例)電磁的記録 媒体	端末	消去(データ抹 消ソフトウェア)	情報管理責 任者の立ち 会い	〇〇	△△

(注1)「紙媒体」、「電磁的記録媒体」のいずれかを記載すること。

(注2)「キャビネット」、「外部電磁的記録媒体(CD-R、USB メモリ等)」、「端末」、「サーバ装置」等を記載すること。

(注3)返却の場合:「返却」と記載すること。

廃棄・抹消の場合:「焼却」、「溶解」、「裁断」、「消去(データ抹消ソフトウェア)」等を記載すること。

2 全ての作業が完了した日

令和 年 月 日

(別添様式 3)

独立行政法人 医薬品医療機器総合機構 御中

秘密保持等に関する誓約書

貴機構における次世代安全対策システム（シグナル検出製品）の導入業務（以下、「本件」という）につき、現行関連システムの設計書等を閲覧するにあたり、〇〇〇〇株式会社（以下「弊社」という。）は次の事項を遵守することを誓約いたします。

記

1. 弊社は、本件のために必要な者（次頁に記載する者をいう。以下同じ。）以外は本件のための業務に従事させません。ただし、本件のための業務の遂行期間中に追加、変更する場合、貴機構に届け出、了承を受けるものとします。
2. 弊社は、媒体および手段を問わずに貴機構から開示もしくは提供された貴機構の秘密情報（以下「本件秘密情報」という。）を、本件のために必要な者を除く第三者に対して開示いたしません。ただし、以下のものについては秘密情報に含みません。
 - (1) 弊社が貴機構より開示を受けた時点で既に公知であったもの
 - (2) 弊社が貴機構より開示を受けた時点で既に所有していたもの
 - (3) 弊社が貴機構より開示を受けた後に弊社の責によらずに公知となったもの
 - (4) 弊社が正当な権限を有する第三者から守秘義務を負わずに適法に入手したもの
 - (5) 法令または裁判所の命令により開示を義務づけられたもの
3. 弊社は、本件のために必要な者がそれ以外の者に秘密情報を開示しないよう、厳正な措置を講じます。
4. 弊社は、本件秘密情報を本件のための業務のみを目的として使用するものとし、他の目的には一切使用いたしません。
5. 弊社は、本件秘密情報を複写または複製いたしません。
6. 弊社は、貴機構から要請がある場合または本件終了後は直ちに本件秘密情報を貴機構に返還いたします。
7. 弊社が本誓約書の内容に違反したことにより本件秘密情報が漏洩し、貴機構に損害が発生した場合には、貴機構に対しその損害を賠償いたします。
なお、賠償額については、貴機構と弊社にて別途協議して定めるものとします。
8. 本誓約書は、本件秘密情報が秘密性を失う日まで有効に存続する事を確認します。

以 上

令和〇年〇〇月〇〇日

東京都〇〇区〇〇町 1 - 6 - 5

〇〇〇〇株式会社

代表取締役

〇〇 〇〇

代表者印

○本件実施のために必要な者
本件実施のために必要な者は以下の者である。

記

○ ○ ○ ○ 株式会社

○ ○ ○ ○ 事業部

○ ○ ○ ○ 事業部

○ ○ ○ ○ 事業部

○ ○ ○ ○

△ △ △ △

□ □ □ □

以上

■機器リスト

No.	区分	製造業者・薬務実施業者	本社所在国	業者の法人番号	製品名・役務実施場所	型番	備考
1	ノートP C	〇〇	日本	1234567890123	〇〇ノート	PC 111	
2	スイッチ	× ×	米国	9876543210987	× × Switch	L3-abc	
3	アプリケーション	OSS	OSS		xx Text Editor		https://www.* * *.com
4							
5							

機能要件定義書
(次世代安全対策システム（シグナル検出製品）の
導入業務)

	機能分類 (グループ)	1	2	3	4	5	6	7
		← 優先度 高						優先度 低 →
A	不均衡分析 (アラート表示)	閾値の設定・管理	バッチ処理	アラート割当	アラート表示	詳細結果表示	結果出力	
	優先度	必須	必須	必須	必須	必須	必須	
B	不均衡分析 (adhoc)	検索条件設定	検索条件保存	検索結果表示	詳細結果表示	結果出力		
	優先度	必須	必須	必須	必須	必須		
C	注目する個別症例の 自動検出	自動検出の設定・管理	バッチ処理	アラート割当	アラート表示	症例一覧表出力		
	優先度	必須	必須	必須	必須	必須		
D	共通設定管理	注目医薬品の設定・管理	注目事象の設定・管理	医薬品毎の注目事象 の設定・管理	注目医薬品、注目事 象の一覧出力	ユーザー/チーム/医 薬品の紐付け	除外条件設定・管理	チーム/医薬品の表 示
	優先度	必須	必須	必須	必須	必須	必須	あれば望ましい
E	データ投入	既知未知リスト	症例データ	外部データベース				
	優先度	必須	必須	あれば望ましい				

機能分類 (グループ)	要件No.	機能	機能詳細	補足
不均衡分析（アラート表示）	A-1	閾値の設定・管理	不均衡分析のアラート判定に使用する閾値を設定・変更できる。	■扱う情報： ・医薬品コード、MedDRAコード、指標の種類（ROR、BCPNN、GPS等）、閾値の値、医薬品×事象の既知・未知の区分。 ■他の機能との関連： ・バッチ処理が不均衡分析を実行する際に、当設定を参照する。 ■バリエーション： ・基本は共通の閾値を適用し、特定の医薬品コード×MedDRAコードの組み合わせに対して個別の閾値を設定できる。 ・医薬品×事象の組み合わせについて、既知の事象として登録されているものは、閾値を超えてもアラート表示の対象外とする。
不均衡分析（アラート表示）	A-2	バッチ処理	特定の頻度で、特定の時間までに、医薬品と事象の組合せに対して不均衡分析を実行する。	■他の機能との関連： ・実行結果をアラート割当てに連携する。 ・閾値設定管理・実行頻度設定管理の設定を参照する。 ・共通設定管理の除外条件設定を参照し、除外対象の症例・副作用を分析対象から除く。 ■バリエーション： ・毎日計算を実行することができる。PMDAが指定する時間までにバッチ処理を終わらせる。 ・頻度について、医薬品と事象との組合せごとに計算実施のタイミングの設定を変えることができる。 一例：注目医薬品リストに合致する医薬品、DMEリスト・IMEリストに合致する事象、医薬品ごとに設定した注目事象リスト（J-RMPの重要な潜在的リスク等）に合致する医薬品-事象の組合せがあれば計算実施タイミングを1週間ごととし、それ以外は6か月単位にする等。
不均衡分析（アラート表示）	A-3	アラート割当て	特定の時間までに、閾値を超えた組合せを、当該医薬品を担当するチームの所属メンバーに自動で割り当てる。	■扱う情報： ・医薬品×担当チームの紐付け、担当チーム×所属メンバーの紐付け。 ■バリエーション： ・PMDAが指定する時間までにアラート割当ての処理を終わらせる。
不均衡分析（アラート表示）	A-4	アラート表示	割り当てられたアラートを、担当者ごとの画面に表示する。	■扱う情報： ・表示項目は、医薬品名、事象名、指標値（ROR、BCPNN、GPS等）、アラート表示理由、データソース等。 ・表示項目はシグナル検出製品のデフォルト機能を踏まえて決定する。 ■バリエーション： ・データベースとして、安対システム、FAERS、VigiBase等が想定される。
不均衡分析（アラート表示）	A-5	詳細結果表示	アラート表示された医薬品×事象の組合せについて、不均衡分析の結果の詳細を確認できる。	■扱う情報： ・時系列データ※（スコア値の推移等）等。その他の詳細項目はシグナル検出製品のデフォルト機能を踏まえて決定する。 ※時系列データの取得方法については、PMDAと相談のうえ、決定する。なお、取得方法は①過去の計算結果を保管しておき、それを呼び出す方法又は②最新のデータから過去の特定のデータロックに遡って計算したものを表示させる方法を想定している。
不均衡分析（アラート表示）	A-6	結果出力	アラート表示された医薬品×事象の組合せごとに、不均衡分析の計算条件と結果を出力できる。	■扱う情報： ・計算条件として、対象期間（yyyy/mm/dd～yyyy/mm/dd）、対象報告・データ、計算日、医薬品（一般名）、副作用（事象名）等。 ・結果として、指標値（ROR等）、経時的変化のグラフ、アラート表示理由等。 ■他の機能との関連： ・アラート表示画面又はバッチ処理の分析結果から、出力対象のデータを取得する。 ・出力形式（PDF、Microsoft Excel等）はシグナル検出製品のデフォルト機能を踏まえて決定する。
不均衡分析（adhoc計算）	B-1	検索条件設定	ユーザが任意のタイミングで、検索条件を指定して不均衡分析を実行できる。検索条件は全て任意設定とし、必要な条件のみを指定して分析できる。	■扱う情報： ・医薬品コード、MedDRAコード（階層レベルとしてLLT、SOC、SMQ等を指定可能）、対象期間、指標の種類（ROR等）、症例の重篤性、転帰（E.i.7の死亡等）、使用理由（G.k.7.r.2b）、報告国、患者背景（性別（D.5）、年代（D.2）、妊婦※）、検索対象データベース（安対システム、FAERS、VigiBase）。 ※妊婦症例の判定方法は、「別紙3 機能要件定義書（次世代安全対策システム（シグナル検出製品）の導入に伴う医薬品安全対策支援システム改修業務）」のA. 症例データの妊娠フラグを参照すること。 ■他の機能との関連： ・分析結果を結果確認に連携する。
不均衡分析（adhoc計算）	B-2	検索条件保存	adhoc計算で設定した検索条件を保存し、再利用できる。	■扱う情報： ・保存名（任意の名称）、検索条件の内容一式。 ■他の機能との関連： ・検索条件設定から条件を受け取り、保存する。保存した条件を検索条件設定に呼び出す。 ■バリエーション： ・保存した検索条件の共有範囲を設定できる（担当者個人のみ、担当チーム内、組織全体等）。その他の詳細（編集、上書き、削除等）はシグナル検出製品のデフォルト機能を踏まえて決定する。
不均衡分析（adhoc計算）	B-3	検索結果表示	検索結果を画面に表示する。	■扱う情報： ・表示項目は、医薬品名、事象名、指標値（ROR、BCPNN、GPS等）、アラート表示理由、データソース等。表示項目はシグナル検出製品のデフォルト機能を踏まえて決定する。 ■バリエーション： ・データベースとして、安対システム、FAERS、VigiBase等が想定される。
不均衡分析（adhoc計算）	B-4	詳細結果表示	adhoc計算した不均衡分析の結果の詳細を確認できる。	■扱う情報： ・時系列データ※（スコア値の推移等）等。その他の詳細項目はシグナル検出製品のデフォルト機能を踏まえて決定する。 ※時系列データの取得方法については、PMDAと相談のうえ、決定する。なお、取得方法は①過去の計算結果を保管しておき、それを呼び出す方法又は②最新のデータから過去の特定のデータロックに遡って計算したものを表示させる方法を想定している。
不均衡分析（adhoc計算）	B-5	結果出力	adhoc計算した不均衡分析の検索条件と結果を出力できる。	■扱う情報： ・設定した検索条件として、対象期間（yyyy/mm/dd～yyyy/mm/dd）、対象報告・データ、計算日、医薬品（一般名）、副作用（事象名）等。 ・結果として、指標値（ROR等）、経時的変化のグラフ等。 ■他の機能との関連： ・検索結果表示から、出力対象のデータを取得する。 ・出力形式（PDF、Microsoft Excel等）はシグナル検出製品のデフォルト機能を踏まえて決定する。
注目する個別症例の自動検出	C-1	自動検出の設定・管理	注目すべき個別症例を自動検出するための条件を設定・変更できる。	■扱う情報： ・注目医薬品の指定、注目事象の指定（DME、IME、J-RMPの重要な潜在的リスク等）、未知・既知の区分、重篤性、転帰（死亡）、各条件に対するアラート有無の設定等。 ■他の機能との関連： ・バッチ処理が自動検出を実行する際に、当設定を参照する。 ■バリエーション： ・検出条件を複数組み合わせで設定できる（例：注目医薬品かつ未知事象かつ重篤等）。
注目する個別症例の自動検出	C-2	バッチ処理	特定の頻度で、特定の時間までに、医薬品と事象の組合せに対してアラート対象とする個別症例の自動検出を実行する。	■他の機能との関連： ・実行結果をアラート割当てに連携する。 ・自動検出管理の設定を参照する。 ・共通設定管理の除外条件設定を参照し、除外対象の症例・副作用を分析対象から除く。 ■バリエーション： ・毎日実行することができる。PMDAが指定する時間までにバッチ処理を終わらせる。
注目する個別症例の自動検出	C-3	アラート割当て	特定の時間までに、検出されたアラートを、当該医薬品を担当するチームの所属メンバーに自動で割り当てる。	■扱う情報： ・医薬品×担当チームの紐付け、担当チーム×所属メンバーの紐付け。 ■バリエーション： ・PMDAが指定する時間までにアラート割当ての処理を終わらせる。
注目する個別症例の自動検出	C-4	アラート表示	割り当てられたアラートを、担当者ごとの画面に表示する。	■扱う情報： ・表示項目は、医薬品名、事象名、アラート表示理由、データソース等。 ・表示項目はシグナル検出製品のデフォルト機能を踏まえて決定する。 ■バリエーション： ・データベースとして、安対システムが想定される。
注目する個別症例の自動検出	C-5	症例一覧表出力	アラート表示された症例を一覧表として出力できる。	■扱う情報： ・受付日（〇/〇～〇/〇受付分）、識別番号、報番号、医薬品（販売名）、医薬品（一般名）、副作用LLT、アラート表示理由等。 ■他の機能との関連： ・アラート表示から出力対象のデータを取得する。 ■バリエーション： ・出力形式（PDF、Microsoft Excel等）はシグナル検出製品のデフォルト機能を踏まえて決定する。

共通設定管理	D-1	注目医薬品の設定・管理	重点的に監視する医薬品を設定・変更できる。	■扱う情報： ・医薬品コード、医薬品名、注目理由（再審査期間内、特に注視したい等）、注目期間（年月日指定）等。 ■他の機能との関連： ・不均衡分析及び注目する個別症例の自動検出のバッチ処理が、当設定を参照する。 ■バリエーション： ・設定方法としては、実装後には②及び③ができることが望ましい。難しい場合には、③のみでもよい。なお、構築段階では①を想定している。 ①システムに受注者が直接データ投入する。 ②システム画面上でユーザが操作して1つずつ登録・削除する。 ③システム画面上でユーザが操作してcsv取込み等により複数の医薬品を一括登録・削除する。
共通設定管理	D-2	注目事象の設定・管理	医薬品を問わず、重点的に監視する事象の分類を設定・変更できる。	■扱う情報： ・事象の分類（DME、IME等）、MedDRAコード、事象名等。 ■他の機能との関連： ・不均衡分析及び注目する個別症例の自動検出のバッチ処理が、当設定を参照する。 ■バリエーション： ・MedDRAのバージョンアップに伴い、コードや事象名の更新が発生する。 ・設定方法としては、実装後には②及び③ができることが望ましい。難しい場合には、③のみでもよい。なお、構築段階では①を想定している。 ①システムに受注者が直接データ投入する ②システム画面上でユーザが操作して1つずつ登録・削除する ③システム画面上でユーザが操作してcsv取込み等により複数の事象を一括登録・削除する
共通設定管理	D-3	医薬品ごとの注目事象の設定・管理	特定の医薬品に紐付く注目事象（J-RMPの重要な潜在的リスク等）を設定・変更できる。	■扱う情報： ・医薬品コード、医薬品名、MedDRAコード、事象名、注目理由（J-RMPの重要な潜在的リスク等）。 ■他の機能との関連： ・不均衡分析及び注目する個別症例の自動検出のバッチ処理が、当設定を参照する。 ・注目医薬品の設定・管理（D-1）、注目事象の設定・管理（D-2）とは独立した設定として管理する。 ■バリエーション： ・J-RMP改訂等に伴い、J-RMPの重要な潜在的リスクの追加・削除が発生する。 ・MedDRAのバージョンアップに伴い、コード及び事象名の更新が発生する。 ・設定方法としては、実装後には②及び③ができることが望ましい。難しい場合には、③のみでもよい。なお、構築段階では①を想定している。 ①システムに受注者が直接データ投入する ②システム画面上でユーザが操作して1つずつ登録・削除する ③システム画面上でユーザが操作してcsv取込み等により複数の医薬品を一括登録・削除する
共通設定管理	D-4	注目医薬品、注目事象の一覧出力	注目医薬品、注目事象に設定された医薬品又は/及び事象の一覧を出力できる。	■扱う情報： ・注目医薬品の管理情報（D-1）。 ・注目事象の管理情報（D-2）。 ・医薬品ごとの注目事象の管理情報（D-3）。 ■バリエーション： ・出力形式（PDF、Microsoft Excel等）はシグナル検出製品のデフォルト機能を踏まえて決定するが、CSV等の編集可能なファイル形式での出力が望ましい。
共通設定管理	D-5	ユーザー/チーム/医薬品の紐付け	医薬品と担当チーム、担当チームと所属メンバーの紐付けを設定・変更できる。	■扱う情報： ・医薬品コード、医薬品名、担当チーム、ユーザ名（所属メンバー）。 ■他の機能との関連： ・不均衡分析のアラート割当てが、当設定を参照する。 ・注目する個別症例の自動検出のアラート割当てが、当設定を参照する。 ■バリエーション： ・人事異動やチーム編成の変更に伴い、紐付けの更新が発生する。 ・1つの医薬品に複数の担当チームが紐付く場合がある。 ・1人のユーザーが複数の担当チームに所属する場合がある。
共通設定管理	D-6	除外条件設定・管理	特定の条件を満たす症例や副作用を、不均衡分析及び注目する個別症例の自動検出の対象から除外できる。実装後にユーザが条件を変更できる。	■扱う情報： ・除外対象の項目名、除外条件の値、適用先（不均衡分析／個別症例の自動検出）。 ■他の機能との関連： ・不均衡分析のバッチ処理が当設定を参照する。 ・注目する個別症例の自動検出のバッチ処理が当設定を参照する。 ■バリエーション： ・不均衡分析及び個別症例の自動検出で、異なる除外条件を設定できる。 ・除外条件の具体的な内容（取下げ症例、因果関係が否定された副作用、非重篤副作用、確認済の症例※等）はPMDAと協議の上決定する。 ・条件の詳細は投入データの所定項目が特定の値である場合に除外するという形式を想定。 ※確認済の症例の除外は個別症例のアラート表示にのみ適用する。確認済ステータスの管理方法はシグナル検出製品のデフォルト機能を踏まえて決定する。
共通設定管理	D-7	チーム/医薬品の表示	医薬品ごとにチームを画面上に表示させることができる。また、チームごとの絞込みやソートを行うことができる。	■扱う情報： ・医薬品コード、医薬品名、担当チーム。 ■他の機能との関連： ・D-5の設定を参照し画面インターフェースに反映する。 ■バリエーション： ・1つの医薬品に複数の担当チームが紐付く場合がある。
データ投入	E-1	既知未知リスト	医薬品×事象の既知未知リストをシステムに投入できる。	■扱う情報： ・「医薬品」×「副作用」に対し、「既知or未知」を定めたリスト。詳細は「別紙3 機能要件定義書（次世代安全対策システム（シグナル検出製品）の導入に伴う医薬品安全対策支援システム改修業務）」のC.既知未知リスト（予測性登録）を参照。 ■他の機能との関連： ・不均衡分析の閾値設定管理において既知・未知の区分を参照する。 ・注目する個別症例の自動検出の設定・管理が既知・未知の区分を参照する。 ■バリエーション： ・投入方法、投入の頻度・タイミングはPMDAと協議の上決定する。
データ投入	E-2	症例データ	安対システムから出力された個別副作用等症例報告のデータをシグナル検出製品に投入し、不均衡分析及び個別症例の自動検出の対象データとして利用できる。	■扱う情報： - 個別症例のデータ範囲は以下のとおり。 ・対象（分類）：安対システム上の市販後医薬品等副作用・感染症報告 ・対象の安対システム上の報告（J2.1a 識別番号（報告分類））：AA、AB、AC、AD、BA、BB、CA、CB、CC、CD ・対象期間：2005/4/1以降に受け付けた報告 ・対象情報：詳細は「別紙3 機能要件定義書（次世代安全対策システム（シグナル検出製品）の導入に伴う医薬品安全対策支援システム改修業務）」のA.症例データを参照 ■他の機能との関連： ・不均衡分析のバッチ処理が対象データとして参照する。 ・注目する個別症例の自動検出のバッチ処理が対象データとして参照する。 ・共通設定管理の除外条件設定により、特定の症例が分析対象から除外される。 ・安対システムから出力されたデータを受け取る。 ■バリエーション： ・投入方法、投入の頻度・タイミングはPMDAと協議上決定する。
データ投入	E-3	外部データベース	FAERS、VigiBase等のデータベースを投入し、不均衡分析の対象データとして利用できる。	■他の機能との関連： ・不均衡分析のバッチ処理が対象データとして参照する。adhoc計算の検索条件設定で、検索対象データベースとして選択される。

非機能要件定義書

目次

1.	ユーザビリティ及びアクセシビリティに関する事項	1
(1)	情報システムの利用者の種類、特性	1
(2)	ユーザビリティ要件	1
(3)	アクセシビリティ要件	2
2.	システム方式に関する事項	3
(1)	情報システムの構成に関する全体の方針	3
(2)	情報システムの全体構成	4
3.	規模に関する事項	5
(1)	利用者数等	5
(2)	処理件数	5
(3)	データサイズ概算（全件データ）	6
4.	性能に関する事項	6
(1)	応答時間（ターンアラウンドタイム）	6
5.	信頼性に関する事項	7
(1)	可用性要件	7
(2)	完全性要件	9
6.	拡張性に関する事項	9
(1)	性能の拡張性	9
7.	上位互換性に関する事項	9
8.	中立性に関する事項	9
9.	継続性に関する事項	9
(1)	継続性に係る目標	9
(2)	継続性に係る対策	10
10.	情報セキュリティに関する事項	10
(1)	基本事項	10
(2)	情報セキュリティ対策機能	10
11.	情報システム稼働環境に関する事項	13
(1)	環境の種類	13
(2)	ネットワーク構成	13
(3)	ハードウェア構成	13
(4)	ソフトウェア構成	14
(5)	リージョン及び適用法令に関する要件	16
(6)	環境の導入に係る要件	16
12.	運用管理機能に関する事項	16
(1)	ログ収集と不正監視要件	16
(2)	運用監視要件	17
(3)	システムで利用する認証情報の管理要件	17
13.	テストに関する事項	17
(1)	テスト工程共通要件	17
(2)	テストデータ及びその取扱い	18
(3)	テスト計画書	18
(4)	単体テスト	19
(5)	結合テスト	19
(6)	総合テスト	19
(7)	負荷テスト／パフォーマンステスト	19
(8)	ドキュメントテスト	20
(9)	セキュリティテスト	20
(10)	受入テストの支援	20

(11)	他システムとの連携テスト	20
(12)	テスト時の障害対応	20
14.	移行に関する事項	20
(1)	移行手順	20
(2)	移行要件	21
(3)	移行対象データ	21
(4)	移行リハーサルに関する要件	21
(5)	導入サポート	22
15.	引継ぎに関する事項	22
(1)	次期システム導入業者への引継ぎ	22
16.	教育に関する事項	22
(1)	教育対象者の範囲、教育の方法	22
(2)	業務マニュアルと教育教材の作成	23
17.	運用・保守に関する事項	23
(1)	運用・保守に係る作業の内容	23
18.	本調達に係る業務実施内容	26
(1)	作業の実施内容に関する事項	26
(2)	情報セキュリティの履行状況の確認に関する事項	26

1. ユーザビリティ及びアクセシビリティに関する事項

(1) 情報システムの利用者の種類、特性

表 1 情報システムの利用者の種類、特性

利用者区分	利用者の種類	特性	補足
PMDA 内	PMDA 職員	特定ユーザ。内部ネットワークからのみのアクセス	－

(2) ユーザビリティ要件

PMDA 職員は、PMDA の専用インターネット閲覧システム（SCVX（インターネット閲覧環境））を経由して、シグナル検出製品へアクセスし、注目すべき個別症例報告を特定する。

本調達において新規導入するシグナル検出製品について、ユーザビリティ要件は少なくとも以下を満たすものとする。ただし、使用しているソフトウェアに依存する機能について、該当ソフトウェアが販売中止で使用できない又は新バージョンにおける機能変更等でやむを得ず変更が発生する場合は、PMDA の承認を受けることで変更を許可する場合がある。

- ・ 欧米規制当局又はそれと同等の公的機関において利用実績のある製品と同等のものであること
- ・ 画面構成、ナビゲーション、ヘルプ機能、エラーメッセージ等のユーザインターフェースは可能な限り日本語表記であること
- ・ ユーザインターフェースについて、表 2 のとおり視認性及び操作性が高いものであること

表 2 ユーザインターフェースについて

項目	概要
ボタンの内容、位置及び名称	「決定」、「登録」、「キャンセル」、「更新」等の各種ボタンの位置が可能な限り標準化され、ユーザがボタンを迷わずすぐに探せるようにする。 ボタン名称は上述のとおり、平易でシンプルなものとする。 同じ処理をするボタンであれば名称を統一する等、ユーザがストレスなく迷わず操作できるようにする。
ボタン押下時の確認	「削除」ボタン等の押下時に確認ポップアップを表示する等して、操作ミスに伴う意図しないデータ更新を防ぐ工夫をする。

メッセージの内容、表示位置及び表示形式	システムに精通していない一般人でもわかるような平易な表現の内容とする。ただし、冗長ではないように工夫する。 エラー等のメッセージについて、表示位置や表示形式といった仕様を標準化してユーザが見やすくするとともに、ユーザがメッセージを見逃さないように視認性の高いデザインとする。
画面遷移と子画面	画面遷移又は子画面表示となるか、直感的に識別可能な表示とする等、ユーザビリティに配慮する。
グローバルメニュー	画面上部等にメニューツリーを配置する等して押下による画面遷移が可能である等、アドホックな画面遷移も円滑に処理される。
ガイダンスやヘルプ表示	必要に応じて次の操作を促すガイダンスを表示する、操作ボタン等の付近にヘルプマークを配置してユーザが参照する可能性が高いメッセージを表示する等、ユーザが都度操作マニュアルを読まなくとも操作できるようにする。
スクロール	基本は 1 画面についてスクロールが発生しないものが望ましい。スクロールが必要な場合は、スクロールの操作がしやすいようにする。表を表示する場合、項目名等、スクロール時に固定化が必要な部分は固定表示する。
画面サイズ	画面や入力枠のサイズをユーザにて変更可能とすることが望ましい。
文字色、フォント、サイズ	ユニバーサルデザインに配慮したものとする。フォントサイズは変更可能とすることが望ましい。
入力フォーム	目的に応じて入力フォームを設定し、ユーザが直感的に入力可能な表示とする。また、必要に応じて補助検索機能を設け、ユーザビリティに配慮する。

(3) アクセシビリティ要件

アクセシビリティ要件として表 3 の要件を標準として求めるが、対応が困難な要件については PMDA の承認を受けること。

表 3 アクセシビリティ要件

アクセシビリティ分類	アクセシビリティ要件
基準等への準拠	・日本産業規格 JISX 8341 シリーズ、「みんなの公共サイト運用ガイドライン（2024 年版）」（総務省）、情報アクセシビリティ自己評価様式をはじめ、各情報システムで策定する要領、指針等に従い、アクセシビリティを確保した設計・開発を行うこと。 ・JISX 8341-3:2016「高齢者・障害者等配慮設計指針—情報通信における機器、ソフトウェア及びサービス—第 3 部：Web コンテンツ」の適合レベル AA に準拠することを目標とする。また、レベル AAA のうち、以下の達成基準についても可能な範囲で適用すること。 ➤ 2.1.3 キーボード（例外なし）の達成基準 ➤ 2.3.2 3 回のせん（閃）光の達成基準 ➤ 2.4.8 現在位置の達成基準 ➤ 3.2.5 要求による状況の変化の達成基準 注記：本調達仕様書における「準拠」という表記は、情報通信アクセス協議会 Web アクセシビリティ基盤委員会「Web コンテンツの JISX 8341-3:2016 対応度表記ガイドライン（令和 3 年 4 月版）」で定められた表記による。 ・デジタル庁が整備する「ウェブアクセシビリティ導入ガイドブック」を参考にすること。
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（視覚障がいのかた等）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。
利用者の特性に合わせた対応	・シグナル検出製品では、可能な限り日本語でのコンテンツ提供に対応すること。

2. システム方式に関する事項

(1) 情報システムの構成に関する全体の方針

本調達は、システムインフラ全体のコスト低減、セキュリティレベルの統一、運用ノウハウの集約を行うため、クラウドサービス上で行う。本調達で納入する製品選定及びクラウドサービスにおける留意事項を以下に示す。

①製品選定における留意事項

- ・ 競争原理によって、適正な価格で調達することが可能な製品であること
- ・ 製品の契約期間は令和 11 年 3 月末日までであるが、本製品は契約期間終了後も継続的な利用が想定されるため、少なくとも令和 12 年 3 月末日までサービスの提供が可能であること、又は同等製品（同製品のバージョンアップ又は後継製品）への移行が可能であること
- ・ 別紙 2「3 規模に関する事項」と同等の規模のトランザクション量及びデータ量での使用実績があり、一定の処理パフォーマンスが期待できること
- ・ シグナル検出製品の次期更改時の移行作業において、特定の業者、製品に依存することなく円滑に業務を移行可能なシステム構成であること

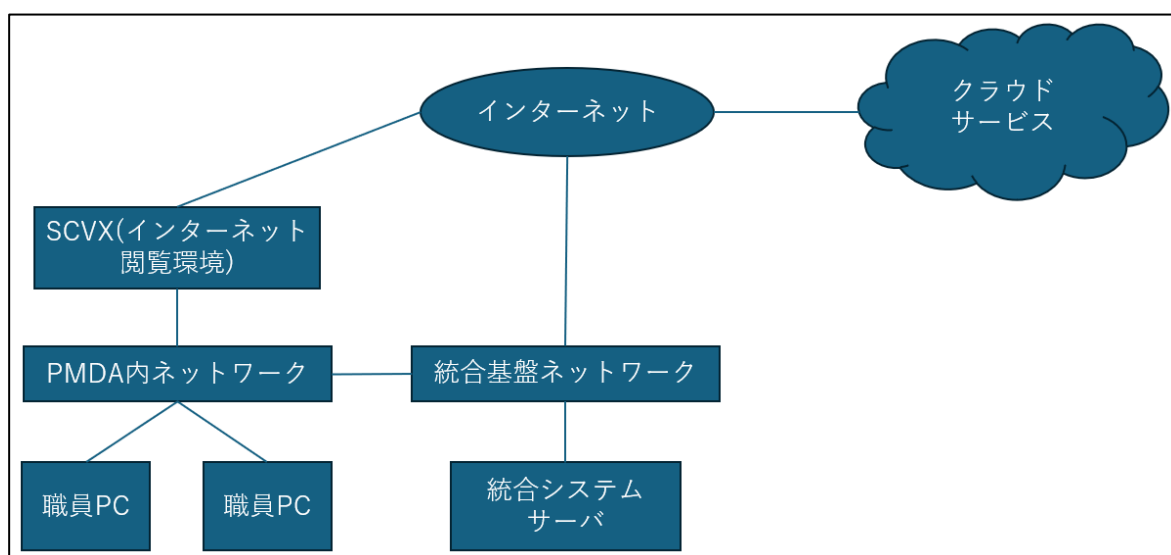
②クラウドサービスにおける留意事項

- ・ クラウドネイティブの構成として、「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」に準拠し、マネージドサービスを活用するなどクラウドサービスの提供機能を最大限活用するようデザインされたアーキテクチャとすること。特に、信頼性、拡張性（スケーラビリティ）、継続性等の向上に寄与するクラウドサービスと構成を選定すること。

(2) 情報システムの全体構成

現時点で想定するシステム全体構成を図 1 に示す。

図 1 システム全体図（想定）



また、この構成を前提とするクライアント環境について以下に記載する。

① クライアント端末環境

職員 PC から、インターネット閲覧環境に接続し、そこから該当クラウドサービスを利用することとする。

職員 PC は表 4 を想定すること。なお、タブレット及びスマートフォンでの利用は想定しない。

表 4 職員 PC

名称	仕様
OS	Windows11 Enterprise
メモリ	4.00GB 以上
CPU	11th Gen Intel (R) Core (TM) i5-1135G7 @ 2.40GHz 2.42 GHz
Web ブラウザ	Chrome (127.0.6533.119 (Official Build) (64 ビット)) Firefox (ver128.1.0esr (64 ビット)) ※稼働させるためのプラグイン等は不要とすること

② ネットワーク

インターネット閲覧環境と受注者のサーバ間の通信は、SSL/TLS 化を実施すること。なお、暗号化に必要なサーバ証明書は受注者が用意すること。

シグナル検出対象データを転送する統合システムサーバと受注者のサーバ間の通信は、SSL/TLS 化を実施すること。なお、暗号化に必要なサーバ証明書は受注者が用意すること。

3. 規模に関する事項

(1) 利用者数等

登録ユーザ数及び同時アクセスユーザ数（通常時及びピーク時）はいずれも最大 10 を想定している。

(2) 処理件数

1 日当たりの処理件数は表 5 を想定している。このうち、安対システムから連携されるのは症例データ、医薬品マスタ及び既知未知リスト（予測性登録）であり、その連携方法は表 6 のとおりである。

表 5 1 日当たりの処理件数（想定）

項目	概算件数
症例データ	13,000,000 件（全件※ ¹ ）、2,500 件（差分※ ¹ ）
医薬品マスタ※ ²	①医療用医薬品マスタ：25,000 件（全件） ②一般用医薬品マスタ：55,000 件（全件） ③暫定医薬品マスタ：5,500 件（全件）

既知未知リスト（予測性登録）	1,150,000 件（全件の下限値）
注目医薬品リスト	920 件（全件）
注目事象リスト	8,000 件（全件）
医薬品ごとの注目事象リスト	5,500 件（全件）

※1：シグナル検出製品の仕様により、「全データ」又は「前回連携分からの差分」の両方を可能とする。

※2：シグナル検出製品で情報を活用できる場合のみ提供する。

なお、医薬品の副作用等報告件数（各年度）は以下資料を参考とすること。

<https://www.pmda.go.jp/files/000281691.pdf>

表 6 既存データベース（安対システム）からの連携ファイル（想定）

一日連携回数	1 回
1 連携の連携ファイル種類	3 種類
連携ファイル種類概要	① 症例データ ② 医薬品マスタ ③ 既知未知リスト（予測性登録） 詳細は「別紙 3 機能要件定義書（次世代安全対策システム（シグナル検出製品）の導入に伴う医薬品安全対策支援システム改修業務）」を参照

(3) データサイズ概算（全件データ）

表 7 対象データサイズ概算

サイズ(Byte)
500M

4. 性能に関する事項

(1) 応答時間（ターンアラウンドタイム）

応答時間に係る要件は、表 8 に示すとおりである。

表 8 応答時間要件（同時接続ピーク時含む）

処理内容	連携先	応答時間目標値 (秒)	目標値達成 率 (%)	備考
機能				

ログイン	—	1.0	99	
安対システムデータ受信	安対システム	—	遵守	日次の連携データ受信が 3 時間以内に完了していること
バッチ処理（ROR 等を計算する、ROR 等のシグナル指標値が特定の閾値を超えたコンビの検出、注目症例の検出、検出されたシグナルの対象者へのアラート表示）	—	—	遵守	日次の連携データ受信以降、バッチ処理が 6 時間以内に完了していること
情報の登録、削除、更新	—	5 未満	99	—
各種検索	—	5 未満	99	目標値は、検索対象のデータやキーワードの難易度（複数キーワード、あいまい検索、前方・後方一致）に依存しないものとする
画面				
画面描画までの時間	—	5 未満	99	—
各画面遷移・子画面の表示（ページングも含む）	—	5 未満	99	—
画面内の並び替え表示	—	5 未満	99	—
帳票				
不均衡分析結果・症例一覧等の帳票出力	—	30 未満	99	—

5. 信頼性に関する事項

(1) 可用性要件

① 可用性に係る SLA

可用性に係る SLA は、表 9 に示すとおりである。

表 9 情報システムの SLA

No.	SLA 項目	説明	設定値
1	サービス稼働時間	・ 情報システムのサービスが提供される時間帯 ・ 定期保守、法定点検等の計画停止期間を除く	24 時間 365 日
2	稼働率	・ No.1 に示すサービス稼働時間における稼働予定時間に対して実際に稼働した時間（稼働時間）の割合であり、以下の式により計算する $\text{稼働率 (\%)} = (1 - 1 \text{ か月の停止時間} \div 1 \text{ か月の稼働予定時間}) \times 100$ ・ 稼働予定時間とは、定期保守、法定停電等による計画した停止時間を除く、1 か月に稼働すべき時間である ・ 停止時間とは、サービスが停止していると確認された時刻（本調達で導入するクラウドサービスの監視機能で障害を検知した時刻、又は利用者が連絡した時刻のいずれか早い方）から利用可能とされた時刻までの経過時間を指す ・ 停止時間には、障害からの本格復旧のために必要になった停止時間、人為的なミスにより発生した停止時間等を含む ・ PMDA 側に責任があることが確認できた場合には、停止時間として取り扱わない	99.9%以上 稼働率は、利用するクラウドサービスの SLA に準拠する 実際の稼働状況は SLA 及び稼働実績を基に継続的に監視・評価すること
3	RPO	・ データの損失は許容できないため、データの再送や再処理を含め、障害発生時までの復旧を基本とする（大規模災害時を除く）	データの障害：障害発生時 大規模災害時：障害発生前 1 か月以内
4	RTO	・ 業務停止時間を極力少なくするため、障害発生時から 6 時間以内の復旧を目標とする（大規模災害時を除く）	データの障害：6 時間以内 大規模災害時：数か月以内

② 可用性に係る対策

ア データベースについては、障害発生時に業務影響を最小限とするため、バックアップ及び復旧が可能な構成とすること。復旧可能な時点については、利用するクラウドサービスの仕様及び SLA に基づき、合理的に設定するものとする。

イ 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。

(2) 完全性要件

データの紛失及び改ざんからデータを保護し、データの正確性及びデータの一貫性を保証することとする。

6. 拡張性に関する事項

(1) 性能の拡張性

受注者は、別紙 2「3. 規模に関する事項」の「(1) 利用者数等」及び「(2) 処理件数」に定義されている数値において、5 年後に 2 割程度増加した場合でも「4. 性能に関する事項」に定義された応答時間を満たす性能とすること。

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に係る最適な構成は異なると考えられることから、実際の構成の検討に際しては、要件に最も適した構成の選定、設計（運用・保守設計を含む。）を図ること。

7. 上位互換性に関する事項

上位互換性に関する変更（バージョンアップ等）については、業務影響の有無を事前に評価した上で実施すること。PMDA の業務及び運用に影響を及ぼすおそれがある変更については、事前に PMDA へ通知し、協議を行うものとする。

8. 中立性に関する事項

特定の製品、技術等に依存することなく、システム拡張時又は次期更改時等において、他の事業者等に必要な情報を、支障なく引き継ぐことが可能なシステム構成とすること。

9. 継続性に関する事項

(1) 継続性に係る目標

大規模災害（地震、火災、風水害等又は第三者による情報システムへの攻撃等による直接的な設備及び情報システムの損壊、若しくは、ライフライン（電力、通信及び交通等）の機能不全による情報システムの長時間停止）が発生した場合を除いて、情報システムを用いた業務処理が維持できること。

(2) 継続性に係る対策

大規模災害が発生した場合に対しては、早急にその状態を把握し、リスクの拡大を防止し、速やかに回復させるための処置を講じることとして、その対策をシステム運用手順書、保守計画書に取りまとめること。

10. 情報セキュリティに関する事項

(1) 基本事項

「独立行政法人医薬品医療機器総合機構情報サイバーセキュリティポリシー」に準拠した情報セキュリティ対策を講じること。なお、「独立行政法人医薬品医療機器総合機構情報サイバーセキュリティポリシー」は非公表であるが、「政府機関等のサイバーセキュリティ対策のための統一基準」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、契約締結後、受注者がPMDA本調達仕様書「別添様式3 秘密保持等に関する誓約書」を提出後に開示する。

(2) 情報セキュリティ対策機能

本調達において受注者が導入する製品（ハードウェア、ソフトウェアパッケージ等）について、以下①及び②に示す機能や運用ルール又は代替手段について PMDA と協議を行い、合意した対策を実施すること。

① 情報セキュリティ機能の実装

ア アクセス・利用制限

アー1 認証情報が、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、以下の措置を講ずること。

- ・シグナル検出製品へのアクセス権限を業務上必要な場合に限定する。
- ・必要最小限の権限のみ付与する。

イ データ暗号化

- イー1 通信経路における盗聴、情報の改ざん等の脅威への対策として、通信内容の秘匿性を確保するため、伝送データを暗号化すること。
- イー2 データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止するため、蓄積データは適切に暗号化をすること。
- イー3 暗号化方式は、性能面や保管媒体を考慮した上で、CRYPTRECにより安全性が確保された「CRYPTREC 暗号リスト（電子政府推奨暗号リスト、<https://www.cryptrec.go.jp/list.html>）」を参照した上で、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運用方法を設定すること。

- イー4 暗号鍵の破損等によりサービスを利用できなくなった場合に備えて、暗号鍵を再作成して暗号化された情報を回復する手順を定めること。
- イー5 システム又はアプリケーションによって自動的に生成される暗号鍵について、システム管理者及び使用者はこれらの暗号鍵の生成、保管、管理、及び配布に関わらないこと。
- イー6 暗号鍵の配布とセキュリティ管理は、PMDA が主体で実施し、受注者は支援を行うこと。
- イー7 契約終了後の暗号鍵の取扱いとして、以下を実施すること。
- ・秘密鍵の破棄
本サービスの契約終了時、受注者は情報システムで使用した暗号化用の秘密鍵を遅滞なく物理的又は論理的に破棄し、復元不可能な状態にすること。
 - ・破棄証明の提出
受注者は、秘密鍵の破棄完了後、当該秘密鍵及び関連するバックアップがすべて消去されたことを示す「消去証明書」又はそれに準ずる報告書をPMDA に提出すること。
 - ・対象範囲
HSM（ハードウェアセキュリティモジュール）内の暗号鍵、およびクラウド上のキーマネジメントサービス（KMS 等）で管理されているすべてのマスターキーを含む。
- イー8 個人情報が含まれる情報をデータベースに保存する場合は、暗号化後に登録すること。また、個人情報については必要最低限の保存期間とし、処理フロー上不要となったタイミングでアプリケーションが自動的に削除する構成とすること。

ウ 不正追跡・監視

- ウー1 サーバ、ストレージ等に対する不正アクセス等への不正監視をおこなうため、別紙2「12. 運用管理に関する事項（1）ログ収集と不正監視要件」を踏まえて機能実装を行うこと。

エ Web サイトに対する対策

- エー1 提供するアプリケーション・コンテンツが、不正プログラムやサービス利用に当たって不要な機能を含まないこと。
- エー2 提供するアプリケーションが脆弱性を含まないこと。製品利用時はリリース時に最新のセキュリティパッチを適用すること。
- エー3 ブラウザ経由にて想定される Web アプリケーションに対する脅威（クロスサイトスクリプティング、SQL インジェクション等）に対する対策を講ずること。

② 脆弱性対策の実施

- ア 受注者は、PMDA が利用するクラウドサービスについて、当該クラウドサービス提供事業者が公表している情報セキュリティ方針、脆弱性対応方針、セキュリティインシデントに関する情報、サービスの提供終了、制限に関する情報等を定期的に収集し、その内容を整理のうえ、PMDA に報告すること。
 - イ 受注者は、別紙 2「10. 情報セキュリティに関する事項」(2)② アに基づき収集した情報のうち、PMDA の業務に影響を及ぼすおそれがあると認められる事項について、影響の有無及び程度を整理し、利用継続、設定変更、利用制限、代替手段の検討等の観点から、PMDA に報告すること。
 - ウ 受注者は、別紙 2「10. 情報セキュリティに関する事項」(2)② イの報告を踏まえ、PMDA の指示に基づき、当該クラウドサービスの利用に係る設定変更、運用上の対応、代替手段の検討等、PMDA が利用者として実施可能な範囲において、必要な対応を支援すること。
 - エ 別紙 2「10. 情報セキュリティに関する事項」(2)②に基づく脆弱性対策には、当該クラウドサービスを構成する内部のソフトウェア、ミドルウェア、ライブラリ、ハードウェア等に対する脆弱性検査、脆弱性情報の個別収集、パッチ適用その他の技術的対策は含まれないものとし、これらは当該クラウドサービス提供事業者の責任範囲とする。
- ③ 製品サポート期間の確認
- ア 業務要件、セキュリティ要件又は運用上の理由により、クラウドサービスの機能を保管する目的で PMDA 又は受注者が主担的に管理・運用するハードウェア又はソフトウェアをやむを得ず導入せざるを得ない場合に限り、これらの製品の導入を認める。なお、当該製品については、当該情報システムのライフサイクル(システム利用期間の終了まで)におけるサポート(部品、セキュリティパッチの提供等)を継続して受けられる製品を選定すること。
 - イ サポートライフサイクルポリシーが事前に公表されていない製品を納入する場合は、サポートが継続して行われるように後継製品への更新計画を提出すること。
- ④ IT セキュリティ評価及び認証制度に基づく認証取得製品の採用

ア 業務要件、セキュリティ要件又は運用上の理由により、クラウドサービスの機能を補完する目的で、PMDA 又は受注者が主体的に管理・運用するハードウェア又はソフトウェアをやむを得ず導入せざるを得ない場合に限り、これらの製品の導入を認める。なお、当該製品については、IT セキュリティ評価及び認証制度に基づく認証を取得している製品を、調達可能な範囲において積極的に採用すること。

イ 採用に当たっては、以下の資料を参照すること。

イー1 IT 製品の調達におけるセキュリティ要件リスト（第 2.1 版）（経済産業省）

イー2 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル（内閣官房 国家サイバー統括室）

イー3 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン（デジタル庁）

11. 情報システム稼働環境に関する事項

(1) 環境の種類

本調達に係る環境は、大きく以下の 2 種類とする。

① 本番環境

ア 情報システムの本番サービスが稼働する環境として利用する。

② 検証環境

ア 環境の利用目的

アー1 アプリケーションソフトウェアの結合テスト、総合テスト、受入テスト及び連携テストを実施するための環境として利用する

アー2 本番環境へのリリースに際して、事前検証を行うための環境として利用する

(2) ネットワーク構成

① 基本事項

ア インターネット閲覧環境及びデータ連携するための回線はインターネット回線とするが、通信は SSL/TLS 暗号化をすること。

イ 連携データをネットワーク経由で受領するためのインタフェースを実装していること。

(3) ハードウェア構成

情報システムは、原則としてクラウドサービスの利用を前提とし、個別のハードウェアの新規導入は想定しない。ただし、業務要件、セキュリティ要件又は運用上の理由により、クラウドサービスの機能を補完する目的で、PMDA 又は受注者が主体的に管理・運用する

ハードウェアをやむを得ず導入せざるを得ない場合に限り、導入を認める。導入する製品は、以下に示す要件を満たたものとする。

① 基本事項

ア オープンなシステム環境の整備を可能とするため、情報システムを構成する製品は以下に示す規定等に準拠していること。また、これらに準拠した製品に対する必要十分なインタフェースを有すること。

アー1 ハードウェア等の構成要素は、ITU-T あるいは ISO 等が規定又は推奨する各種国際標準に準拠していること。

アー2 装置の製造・データ処理に関しては、IEEE 等が規定又は推奨する各種デファクトスタンダードに準拠していること。

イ 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。

ウ 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。

エ ハードウェア内のシステム設定は、可能な限り日本語に対応すること。

オ 納品対象には、製品に付属する取扱説明書等のドキュメント類も含むものとし、構築、運用・保守等の作業に通常利用する製品仕様、操作手順等に係るドキュメント類は、日本語で書かれたものとする。その他ドキュメント類に関しても、納品に際してはその内容（使用言語等）を説明のうえ、PMDA の承認を受けること。

② ハードウェア要件

ア ハードウェアは、統合基盤システム上の物理機器設置領域へ設置する。統合基盤システムの仕様に準拠する下記条件の機器を選定すること。

アー1 EIA 規格の 19 インチラック（42U）に搭載できる仕様とすること。

アー2 200V 電源を利用できること。利用できない場合は、個別に機器が利用可能な電圧に対応すること。

アー3 選定されるハードウェアが外国製品の場合は、国内の電源環境での動作が可能であること。

イ ハードウェアの設置に必要となるラック・テーブル等の什器は、本受注者で用意すること。

ウ 設置場所や配線作業に関しては、統合基盤システム管理者の指示に従うこと。

(4) ソフトウェア構成

① 基本事項

シグナル検出製品は、原則、クラウドサービス又は既存の標準的なソフトウェアの利用を前提とし、新たなソフトウェア製品の導入並びに個別ソフトウェアの新規開発及び過度なカスタマイズは想定しない。ただし、業務要件、セキュリティ要件又は運用上の理由により、やむを得ず新たなソフトウェア製品の導入並びに個別ソフトウェアの開発及びカスタマイズが必要となる場合には、PMDA と協議し、承認を受けること。なお、以下に示す要件を満たすこと。

- ア ボリュームライセンス、ガバメントライセンスの適用を考慮すること。
- イ ソフトウェア製品の設定画面は、可能な場合日本語とすること。
- ウ 選定する製品には、製品に付属する取扱い説明書、並びにシステム環境の構築及び運用・保守作業に利用する製品仕様や操作手順等に係るドキュメント類を含むものであること。
- エ 当該ドキュメント類は、可能な場合日本語で書かれたものであること。
- オ ソフトウェアパッケージ間の連携を考慮した上で、動作保証できるソフトウェアパッケージの組合せとすること。
- カ ISMAP を取得していることが望ましい。ISMAP を取得していない場合には、以下の対応をとること。
 - ・ PMDA が指定するクラウド環境セキュリティ関連確認事項（閲覧資料 6）について回答し、国内監査法人の監査を受けること。
 - ・ 国内監査法人は、ISMAP の HP 上の監査機関リストに掲載のある監査法人が望ましい。監査機関リストに掲載されていない国内監査法人による監査を希望する場合は、ISMAP の監査実績がある等、システム監査が可能な監査法人であることを、過去の業務実績を提示した上で PMDA と協議し、承認を受けること。
 - ・ 国内監査法人から指摘事項を受けた場合には、その対応内容又は対応方針を整理すること。その際、クラウド環境セキュリティ関連確認事項に対する回答及び国内監査法人からの指摘事項への対応内容等については、PMDA における確認期間を確保するため、シグナル検出製品稼働開始前 6 か月を目途に PMDA へ提出し、承認を受けること。
 - ・ 受注者は、PMDA の確認結果を踏まえ、必要な対応をし、シグナル検出製品の稼働開始までに対応の内容について PMDA の承認を受けること。
 - ・ なお、本調達はシグナル検出製品を試行的に導入するものであることから、本契約期間内に ISMAP を取得することを必須要件とするものではない。一方、シグナル検出製品を用いて行う業務をそのまま継続する場合があります。その際には ISMAP の取得が必須となることから、受注者は ISMAP 取得に向けた対応方針及びロードマップを提示することが望ましい。

(5) リージョン及び適用法令に関する要件

情報システムにおいて利用するクラウドサービスは、日本国内のリージョンでの提供が可能であることが望ましい。日本国外のリージョンを利用する場合には、当該クラウドサービスに関する契約が日本法を準拠法として締結され、かつ、PMDA の求めに応じて説明及び資料提示が可能であること。

また、情報システムに係る契約の準拠法は日本法とすること。

(6) 環境の導入に係る要件

情報システムで必要となる各種環境の導入に係る要件は、以下に示すとおりである。

- ① クラウドサービス導入作業の完了後、稼働に必要なデータ、機器等の各種設定について追加、修正等が行われた場合は、必要となる情報を整理した上で、クラウド環境設計書を更新すること。

12. 運用管理機能に関する事項

情報システムの運用・保守を踏まえて、必要となる各種機能の導入と運用ルールを整備する。なお、システムの設定更新を伴わないシステム起動停止、ログローテーション等の定期的な運用・保守業務は、原則自動化を行うことが望ましい。

(1) ログ収集と不正監視要件

以下の事項に留意したログの収集と不正監視機能を有し、運用計画書及び運用手順書を作成した上で、運用・保守支援を実施すること。

① 利用目的

情報システムが正しく利用されていることの検証、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を取得する。また、操作ミスによりファイル/フォルダの喪失時、早期にデータを復旧できるように、ユーザ操作ログの収集を行う。

② 要件

ア 下記セキュリティログを取得すること。

アー1 ログイン・ログアウト等の認証情報のログを取得すること。

アー2 ユーザや特権 ID の操作ログについて、必要となるものを絞って取得すること。

イ 下記アプリケーションログ・システムの動作ログを取得すること。

イー1 障害の原因追及のために利用するログについて、必要となるものを絞って取得すること。

イー2 操作ミスによりファイル/フォルダの喪失時、早期にデータを復旧できるように、ユーザ操作ログの収集すること。

ウ 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能等、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、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。

エ ログは、以下の期間保存すること。

エー1 セキュリティログ：365 日以上

エー2 アプリケーションログ・システムの動作ログ：90 日以上

(2) 運用監視要件

以下の事項に留意した運用監視機能を有し、運用計画書及び運用手順書を作成した上で、運用を実施すること。

① 利用目的

ソフトウェア・プロセス・ジョブ稼働に関して監視を行うことで、業務影響を早急に検知し、対処できるようにする。障害が発生した際は、運用計画書及び保守計画書に基づき速やかに PMDA に連絡をすること。

(3) システムで利用する認証情報の管理要件

以下の事項に留意し、システムで利用する認証情報の管理方法を検討して、運用設計や手順書を作成した上で、運用を実施すること。必要に応じて管理用の機能を構築すること。

① 利用目的

個々のシステムで利用する ID 及びパスワードを、システムごとの独立性を維持した上で、業務の負荷なく管理を行う。

② 要件

ア システムで利用する ID 及びパスワードは、インシデント発生時等、必要な時に変更できるよう、手順及び管理するツール（設定ファイルの配布、集中管理する等）を準備すること。

イ システムで利用する ID 及びパスワードは、可能な限りシステムごとに定義すること。

ウ システムの運用・保守支援事業者が変更となった際に、パスワードの変更が可能になるよう、パスワードの変更及びシステムの設定変更を行う手順を作成すること。

13. テストに関する事項

(1) テスト工程共通要件

実施する単体テスト、結合テスト、総合テスト、連携テスト及び受入テストについて、共通となる要件は以下のとおりである。

- ① 情報システムの正常稼働を保証するためのテストとして、単体テスト、結合テスト、総合テスト及び連携テストを実施すること。また、PMDA が行う受入テストの支援を行うこと。
- ② 各テストを行うため一連のテストケース（入力、出力、及びテスト合否基準）、テストデータ、及びテスト手順を整理したテスト計画書（案）を作成し、PMDA と協議のうえ、承認を受けること。
- ③ 各テスト終了時に、実施内容、品質評価結果、及び次工程への送り事項等について、テスト結果報告書を作成し、PMDA と協議のうえ、承認を受けること。
- ④ テストに使用するテストツール等については、PMDA と協議のうえ、使用すること。

(2) テストデータ及びその取扱い

テスト工程においては、受注者が準備したテスト用データを使用すること。ただし、テスト工程において PMDA の所有するデータを本番データとして使用する場合は、必要性等を PMDA に説明し、PMDA の承認を受けて使用すること。なお、テスト工程における本番データの管理責任は受注者が負うこと。

受入テスト工程においては、本番データを使用するため、その管理責任は PMDA が負うことになる。ただし、受入テストにおける操作ではなく、受注者の操作等により漏洩等のインシデントが発生した場合はその限りではない。

(3) テスト計画書

実施する単体テスト、結合テスト、総合テスト及び連携テストについて、設計し、テスト方針、実施内容及び実施理由を記述し、テスト計画書（案）として提示し、テスト開始 1 か月前までに PMDA と協議のうえ、承認を受けること。

承認されたテスト計画書に基づき、進捗管理を確実に実施すると共に、進捗状況の報告を定期的かつ PMDA の求めに応じて行うこと。

テスト計画書の内容に変更が生じる場合、変更箇所及び内容について PMDA の承認を受けることを条件として、テスト計画書を適切に更新すること。

情報セキュリティの観点から必要なテストがある場合には、テスト項目及びテスト方法を定め、これに基づいてテストを実施し、その実施記録を保存すること。

以下に、テスト計画書で必要と考える事項を示す。

- ① テスト概要
 - ア テスト範囲
 - イ テスト品質目標（テスト項目数、バグ検出数）
- ② テストに関する実施作業及びスケジュール
- ③ テスト環境（テストに使用した回線及び機器構成、その他ツール、場所等）

④ テスト体制（テスト実施者、テスト結果確認者（評価者））

⑤ 使用及び提出するドキュメントとその定義

ア テスト項目一覧

イ テスト計画書

ウ 懸案事項一覧

エ テスト結果報告書

(4) 単体テスト

利用者側で開発又は設定を行うプログラム及びモジュールについて、それぞれ個別単体において正しく機能することを確認する。また、パッケージ製品又はクラウドサービスに含まれる機能については、当該製品等の仕様書、試験結果資料、第三者認証等により、該当機能が正しく動作することを確認するものとする。なお、単体テストを実施しない場合には、その妥当性を示す資料を提示し、PMDA と協議のうえ、承認を受けること。

(5) 結合テスト

プログラム及びモジュールが、情報システムの各システムの単位でそれぞれ正しく機能することを確認するため、段階的に結合した状態でテストを行い、ソフトウェアの結合が完全であることを確認する。

(6) 総合テスト

情報システム全体として要件どおりにシステムが構築されていることを確認するためにテストを行い、システムが納品可能な状態であることを確認する。確認に当たっては、ソフトウェア製品が仕様に適合し、かつ実稼働環境で利用可能であることを確認できる評価指標及び合格条件を設定した上で、テストを実施する。

特に、総合テストにおける性能及び負荷のテストにおいては、想定する最大人数が同時に利用開始した場合であっても問題が生じないことを確認する。

本番相当環境において実施された各種設定内容について確認し、設計書等との齟齬がないことを確認すること。

(7) 負荷テスト／パフォーマンステスト

情報システム全体として規模に関する事項及び性能に関する事項を満たしていることを確認するためにテストを行い、システムが納品可能な状態であることを確認する。個別に実施しない場合は、PMDA が要求する性能を満たすことを説明すること。

(8) ドキュメントテスト

運用手順書及び保守手順書に記載したとおりに動作することを確認するために、テストを行い、システムが納品可能な状態であることを確認する。

(9) セキュリティテスト

アプリケーションが情報セキュリティに関する事項を満たしていることを確認するためにテストを行い、システムが納品可能な状態であることを確認する。

また、第三者による脆弱性検査を実施し、収集した脆弱性情報に係る対処の要否、可否について検討する。対処が必要と判断したものに関して、決定した対処又は代替措置が実施されていることを確認する。なお、クラウドサービスにおいてすでにセキュリティテストを実施している場合、その結果を提出することで代替とすることも可能とする。

(10) 受入テストの支援

PMDA が実施する受入テストにおいて、受注者は、テスト計画の策定、準備、テストの実施、成果物の作成、テスト実施結果の報告等に関して、情報提供等の必要な支援を行うこと。

(11) 他システムとの連携テスト

本受注者は、安対システムから出力されたデータを取り込む機能について必要なテストを行うこと。テストにおいては、次世代安全対策システム（シグナル検出製品）の導入に伴う医薬品安全対策支援システム改修業務受注者と実施時期、実施内容、不具合が発生したときの連携方法、作業担当者等の認識合わせを行うこと。

(12) テスト時の障害対応

受注者は、各テストの実施時に発生した障害や性能に関する課題について、一時切分けを行い、調査結果に基づいて、適切な対応を実施すること。また、安対システム出力データに関する設定変更が必要な場合は、次世代安全対策システム（シグナル検出製品）の導入に伴う医薬品安全対策支援システム改修業務受注者と協議のうえでの対応の依頼を行うこと。

14. 移行に関する事項

(1) 移行手順

移行において想定する作業は以下のとおり。

- ① 移行計画書の策定
- ② 移行設計
- ③ 移行手順の作成・検証
- ④ 移行プログラムの作成・検証

- ⑤ リスクの洗出し・コンティンジェンシープランの作成
- ⑥ 移行リハーサルの実施
- ⑦ 移行判定
- ⑧ 移行作業の実施

(2) 移行要件

新規に稼働するシステムであるため、移行作業は発生しない認識だが、「別紙 3 機能要件定義書（次世代安全対策システム（シグナル検出製品）の導入に伴う医薬品安全対策支援システム改修業務）」で定義した連携データ以外の移行を PMDA が必要と判断した場合には移行作業が発生する可能性がある。その場合、以下の基本方針に基づき、移行計画及び移行作業を行うこと。また、連携先のシステムに影響がある場合は、それも含めて移行計画及び移行作業を行うこと。

- ① 情報システムの安定した稼働及び業務の継続に影響を与えないよう、安全で確実な作業を優先すること。
- ② PMDA が承認した日時を除き、現在稼働中のシステムのサービスを停止することなく、移行作業を行うこと。
- ③ システムの停止を伴う作業が避けられない場合には、システム利用者への影響を最小限に抑えるため、平日においては、勤務時間外、その他土日及び休日を作業実施日の基本として検討し、停止予定日より、原則 1 か月前に停止日時及び停止による影響（停止するサービスの範囲）について、書面にて、PMDA の承認を受けること。
- ④ 移行作業中に障害が発生した場合には、速やかに原因究明にあたりとともに、移行計画書、移行手順書に従い、切戻し作業を行い、PMDA の承認を受け、必要な障害対処作業を受注者の責任と負担により実施すること。
- ⑤ 移行の実施前に、現行機器のデータについて、バックアップを取得すること。

(3) 移行対象データ

本調達で移行が必要なデータやデータ変換方式については、PMDA と協議のうえで決定すること。なお、移行作業に媒体を利用する場合は、PMDA と協議のうえ決定すること。移行計画書において移行対象のデータを確定すること。

(4) 移行リハーサルに関する要件

移行手順・リスクの洗出し・コンティンジェンシープランの作成を行い、リハーサルを実施することでトラブル時の対応を明確にすること。

- ① リハーサル対象

以下のリハーサルを実施すること。

- ・ データ移行作業
- ・ システム切替え作業

② リハーサル環境

本番環境のリリリースに際して、以下環境での事前検証が可能である。

- ・ 現行統合システム検証環境（参照のみ可能）
- ・ 現行統合システム本番環境（参照のみ可能）

③ リハーサル回数

業務影響がない安全な移行が必要となるため、1回は実施すること。

(5) 導入サポート

システムが本格稼働するまでの期間、サポートを行うこと。また、システム本稼働時に発生した問題の早期解決を図るため、本受注者は一定期間の導入サポートを提供する。具体的な期間は、開発内容・移行方法を踏まえて、定義すること。

15. 引継ぎに関する事項

(1) 次期システム導入業者への引継ぎ

以下の事項に留意して、次期システム導入業者、次期システム運用・保守支援事業者に引継ぎを実施すること。

- ① システム業務内容の情報及び資料並びに運用・保守業務の円滑な実施に役立つよう、必要な各種情報及び資料の提供を行うこと。
 - ・ 問合せ、障害等の対応及び管理に関する手法・手順
 - ・ 運用手順書、保守手順書
 - ・ 仕掛中の項目一覧及びその進捗状況
 - ・ 過去の問合せ、障害等の実績及びその対応方法
 - ・ バックログ・未対応作業一覧及びその対応（案）
 - ・ その他業務を引き継ぐ上で必要と思われる事項
- ② 引継ぎの内容は、事前に PMDA に示し承認を受けること。
- ③ 引継ぎの実施に当たっては、PMDA 及び引継ぎ先と日程を調整した上で実施すること。
- ④ 引継ぎに必要な資料等は、受注者において用意すること。
- ⑤ 必要に応じて、実機での操作説明等を行うこと。

16. 教育に関する事項

(1) 教育対象者の範囲、教育の方法

利用者やPMDA内の管理者に対し、必要に応じて説明会を実施し、機能内容等を周知すること。業務の変更度合いにより適切な時間や回数を設けること。実施内容については、教育計画書にて定義し、実施結果については教育作業結果報告書の作成を行うこと。

(2) 業務マニュアルと教育教材の作成

利用者やPMDA内の管理者が業務を実施できるように、利用マニュアルを整えること。

17. 運用・保守に関する事項

(1) 運用・保守に係る作業の内容

受注者は、本調達仕様書に記載された作業内容や各要件を参照のうえ、以下に関し必要な作業を実施すること。

① 準備作業

ア 受注者は、運用・保守業務の開始までに、運用・保守準備作業に関する準備計画書を作成し、PMDAの承認を受けること。

イ 受注者は、運用・保守準備作業が完了した後、準備完了報告書を作成し、PMDAの承認を受けること。

② 実施計画書及び実施要領の作成

受注者は、調達仕様書等に基づき運用計画書及び保守計画書を作成し、PMDAの承認を受けること。

③ 定常時対応

- ア 受注者は、運用・保守業務を行うこと。具体的な実施内容・手順は運用計画書、保守計画書等に基づいて行うこと。
- イ 受注者は、以下の内容について月次で運用・保守作業報告書を取りまとめること。
 - イー1 運用・保守業務の内容、工数、作業時間等の作業実績状況
 - イー2 サービスレベルの達成状況
 - イー3 サービスレベル関連実績データと分析・評価及び対策
 - イー4 情報システムの運転状況
 - イー5 情報システムの利用者サポート、教育・訓練状況
 - イー6 アクセス権管理状況（特権（高権限 ID）管理状況）
 - イー7 システムリソース状況（キャパシティ管理、可用性管理）
 - イー8 リスク・課題の把握、対応状況
 - イー9 問合せ管理運用状況
 - イー10 インシデント管理状況
 - イー11 問題管理状況
 - イー12 変更管理状況
- ウ 受注者は、月間の運用・保守実績を評価し、達成状況が目標に満たない場合はその要因の分析を行うとともに、達成状況の改善に向けた対応策を提案すること。なお、目標はプロジェクト開始後の運用設計で定義する。
- エ 受注者は、運用・保守作業報告書の内容について、定期的に運用会議を開催し、その内容を報告すること。開催頻度は PMDA と協議のうえ、決定すること。なお、PMDA が認める場合は、書面による報告を運用会議の代替とすることを可能する。

④ 障害・情報セキュリティインシデント発生時及び大規模災害等の発災時の対応

- ア 受注者は、PMDA が利用するクラウドサービスに係る障害等の情報セキュリティインシデントについて、発生日、発生事象、影響範囲、対応状況等を記録し、整理のうえ、PMDA に報告すること。
- イ 受注者は、インシデント発生時には、クラウドサービス利用者として把握可能な情報に基づき、検知、影響範囲の確認、発生箇所の一次切分けを行うとともに、クラウドサービス提供事業者その他の関係事業者と連携し、原因の把握及び対応状況の確認を速やかに行うこと。
- ウ 受注者は、インシデントが発生した場合又は発生が見込まれる場合には、速やかに PMDA に報告するとともに、当該インシデントの緊急度及び業務への影響度を整理のうえ、責任分界を踏まえ、受注者がクラウドサービス利用者として実施可能な範囲において、次に掲げる対応を行うこと。

- ウー1 影響状況の確認及び情報整理
- ウー2 応急的な運用上の措置（利用制限、縮退運用等）
- ウー3 復旧状況の確認及び PMDA への報告

なお、インシデントについては、「PMDA 情報セキュリティインシデント対処手順書」を参照し、対応を行うものとする。また、具体的な実施内容及び手順は、情報システムごとのインシデント管理プロセス手順書に基づき実施すること。当該手順書が未整備の場合は、PMDA と協議のうえ、受注者が作成を支援すること。

- エ 受注者は、インシデントに関して、発生原因、影響度、過去の発生実績、再発可能性等について整理・分析を行い、同様の事象が将来にわたり発生するおそれがある場合には、責任分界を踏まえ、クラウドサービス利用者として講じ得る再発防止策又は運用上の改善策について、PMDA に提案すること。
 - オ 受注者は、本調達に係る運用・保守業務に従事する要員に対し、年 1 回以上、情報セキュリティに関する定期的な教育を実施すること。また、新たに要員が当該業務に参画する場合には、参画時に情報セキュリティ教育を実施すること。
 - カ 受注者は、大規模災害その他の非常時においては、PMDA の指示を受けて、クラウドサービスの利用継続可否の判断支援、代替手段の検討支援、及びその他必要な対応を行うこと。また、平常時においても、運用継続計画（情報システム用 BCP）を参照し、PMDA と協議のうえ、大規模災害時の対応手順書の見直し又は整備について必要な支援を行うこと。
 - キ 別紙 2「17. 運用・保守に関する事項」（1）④に基づく対応は、クラウドサービス提供事業者との責任分界を踏まえ、受注者がクラウドサービス利用者として管理又は実施可能な範囲に限り行うものとし、クラウドサービスの内部構成に対する直接的な復旧作業又は恒久対策の実施を受注者に求めるものではない。
- ⑤ 情報システムの現況確認
- ア 受注者は、年 1 回、PMDA の指示に基づき、現況確認を支援すること。現況確認の対象は、当該クラウドサービスのサービス名称、提供されるサービスのバージョン（製品世代）、契約プラン、利用数量、利用条件等、PMDA が利用者として確認可能な範囲に限るものとする。
 - イ 受注者は、現況確認の結果、システム資産簿と当該クラウドサービスの利用状況との間に差異が認められる場合は、その内容を整理のうえ、PMDA に報告すること。
 - ウ 受注者は、現況確認において、当該クラウドサービスの提供終了、サポート終了又はこれらに関する事業者からの公表情報が確認された場合は、当該情報の内容、業務への影響の有無等を整理のうえ、PMDA に報告すること。
 - エ 別紙 2「17. 運用・保守に関する事項」（1）⑤に基づく現況確認には、当該クラウドサービスを構成する内部のソフトウェア、ミドルウェア、ライブラリ等に係るライセンス管理、バージョン管理又はサポート状況の確認は含まれないものとし、これらは当該クラウドサービス提供事業者の責任範囲とする。

⑥ クラウドに係る要件

他のクラウドサービス利用者の行為によりデータ開示が要求された場合でも、PMDA のデータが開示されないことを保証すること。

18. 本調達に係る業務実施内容

(1) 作業の実施内容に関する事項

本調達における業務を実施するにあたり、下記のプロジェクト管理方法と PMDA と合意のうえ、実施すること。

- ① 内部統制方針
- ② インシデント管理
- ③ 問題管理
- ④ 変更管理
- ⑤ リリース管理

(2) 情報セキュリティの履行状況の確認に関する事項

① 情報セキュリティ侵害時の報告

本調達に係る業務遂行に当たり、情報セキュリティが侵害された又はその恐れがある場合には、速やかに PMDA に報告すること。これに該当する場合には以下の事象を含む。

ア 本受注者に対して提供した若しくはアクセスを認めた PMDA の情報を目的外に利用した場合又は外部漏えいした場合

イ 本受注者に対して提供していない又はアクセスを認めていない PMDA の情報にアクセスした場合

② 情報セキュリティ対策の履行状況の報告

本調達に係る業務の遂行におけるセキュリティ対策の履行状況について、PMDA から報告を求めた場合には速やかに提出すること。

③ 情報セキュリティ監査への支援

PMDA が第三者機関等による情報セキュリティ監査を受ける場合には、PMDA を支援すること。情報セキュリティ監査の結果、対策が必要な場合は、PMDA と協議を行い、合意した対策を実施すること。

④ 情報セキュリティ監査への対応

本調達に係る業務の遂行において、受注者における情報セキュリティ対策の履行が不十分であると認められる場合には、受注者は、PMDA の求めに応じ、PMDA と協議を行い、合意した対応を実施すること。

⑤ 管理体制の整備

納入する製品について、不正が見つかったときに、追跡調査、立入検査等により原因を調査・排除できる体制を整備していること。

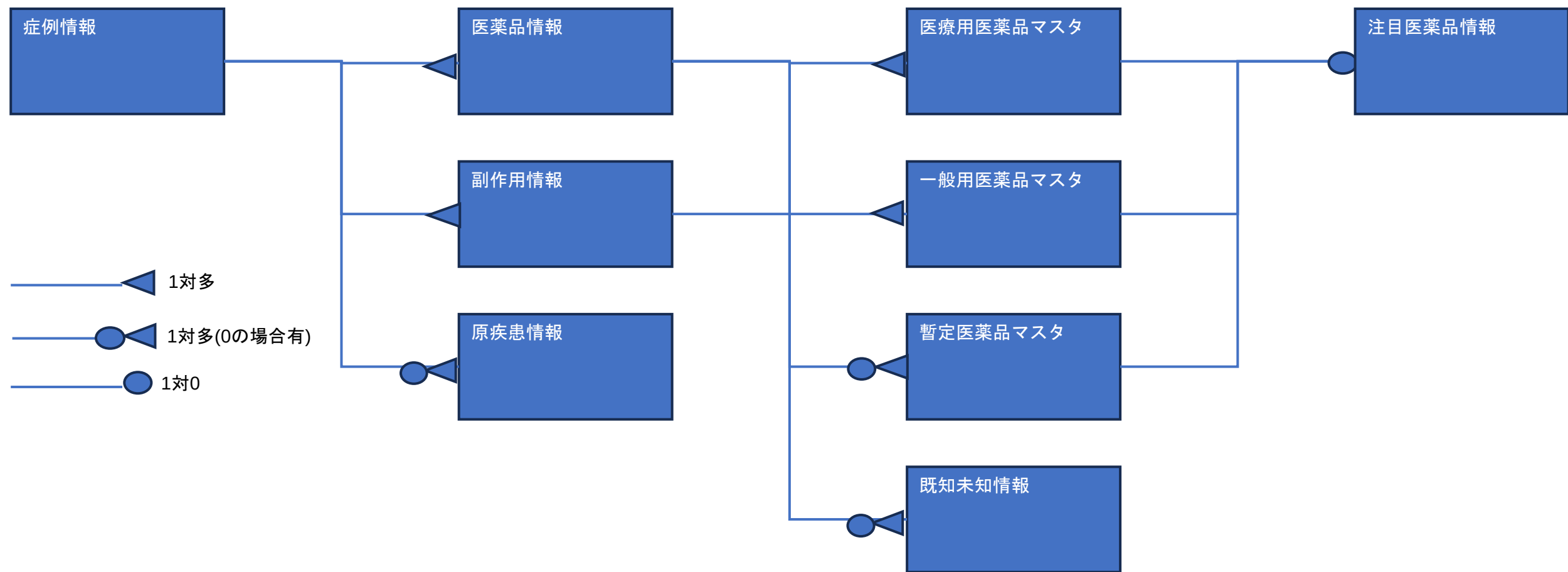
以上

機能要件定義書（次世代安全対策システム（シグナル検出製品）の
導入に伴う医薬品安全対策支援システム改修業務）

連携データの概要

【連携データの概要】	
※A～Cは安対システム上にデータがあり、安対システムからシグナル検出製品へのデータ連携を行う。Dについては、安対システム上にデータがないため、「別紙1 機能要件定義書（次世代安全対策システム（シグナル検出製品）の導入業務）」のD-1、D-2、D-3に記載のとおり、連携を行う。「連携データ関連図（例）」参照。	
A. 症例データ	
対象の報告	安対システム上の市販後医薬品等副作用・感染症報告（J2.1a 識別番号（報告分類））：AA、AB、AC、AD、BA、BB、CA、CB、CC、CD
対象期間	2005/4/1以降に受け付けた報告
対象データ	PMDAが指定するICSR項目のみ連携対象とする。「閲覧資料5 連携データ補足」参照
定期的な連携頻度	日次
定期的な提供データ	シグナル検出製品の仕様により、「全データ」又は「前回連携分からの差分」の両方を可能とする
年2回のMedDRA更新時の対応	定期的な提供データとして「前回連携分からの差分」を連携している場合は、MedDRA更新時に、コードの書換えが発生したものののみパッチデータを作成し、シグナル検出製品に提供する。
データ量の概算	「別紙2 非機能要件定義書」及び「閲覧資料5 連携データ補足」参照
妊娠フラグ	妊婦の症例は、以下の場合に「妊婦」とみなし、該当症例に対して安対システムからの出力時に「妊娠フラグ」を付与し、出力する想定とする。 ・「D.7.1.r 関連する治療歴及び随伴症状の構造化された情報」にMedDRA PT「10036556/妊娠/Pregnancy」（MedDRA（ver.29.1））に紐づくLLTコードが入力されていた場合 ・「G.k.6b 曝露時の妊娠期間（単位）」に情報が入力されていた場合
年齢に対する処理	年齢に関するICSR項目としては、「D.2.2a 副作用／有害事象発現時の年齢（数）」「D.2.2b 副作用／有害事象発現時の年齢（単位）」「D.2.3 患者の年齢群（報告者の表現による）」「D.2.2.1a 胎児での副作用／有害事象発現時の妊娠期間（数）」「D.2.2.1b 胎児での副作用／有害事象発現時の妊娠期間（単位）」の項目があるが、安対システムからの出力時に「胎児、新生児、乳幼児、小児、青少年、成人、高齢者、第一トライメスター、第二トライメスター、第三トライメスター、不明、10歳未満、10歳代、20歳代、…、99歳代」等、JADER公表時のデータと同処理を行ったデータを提供する。JADER公表時のデータ処理については「閲覧資料4 統合システム設計書」参照。
B. 医薬品マスタ（シグナル検出製品で情報を活用できる場合のみ）	
対象のマスタ	①医療用医薬品マスタ、②一般用医薬品マスタ、③暫定医薬品マスタ（PMDAが発番する医薬部外品・化粧品等のコード）「閲覧資料5 連携データ補足」参照。
定期的な連携頻度	①②③日次
定期的な提供データ	前回共有分からの差分（初回のみは全データ）
C. 既知未知リスト（予測性登録）	
データ概要	「医薬品」×「副作用」に対し、「既知or未知orコメント」を定めたリスト。マスタに登録される情報は「閲覧資料5 連携データ補足」参照。
定期的な連携頻度	日次
定期的な提供データ	シグナル検出製品の仕様により、「全データ」または「前回共有分からの差分」の両方を可能とする。
D. 注目医薬品リスト等の情報	
データ概要	①注目医薬品リスト、②特定事象リスト（DME、IME等）、③医薬品ごとに注目したい事象リスト（J-RMPの重要な潜在的リスク等） 「別紙1 機能要件定義書（次世代安全対策システム（シグナル検出製品）の導入業務）」D-1、D-2、D-3参照。
【A～Cの連携概要】	
定期的な連携頻度	日次
ファイル形式	csvを含めた、PMDAと合意した形式。
定期的な連携方法	セキュリティを確保したファイル転送方式により実施するものとし、具体的には、SFTP等の安全なファイル転送方式又はクラウド環境におけるオブジェクトストレージ（AWSのS3バケットを用いる方式を含む。）を利用した方法を想定する。ただし、具体的な連携方式、データの配置場所及び運用方法については、セキュリティ要件及び運用性を考慮のうえ、受注者の提案を踏まえてPMDAと協議のうえ決定するものとする。
【Dの連携概要】	
連携頻度	不定期
連携方法	「別紙1 機能要件定義書（次世代安全対策システム（シグナル検出製品）の導入業務）」D-1、D-2、D-3参照。 <u>「D. 注目医薬品リスト等の情報」については、安対システム上にデータがないため、安対システムからシグナル検出製品への連携には含めない。</u>

連携データ関連図(例)



別紙 4 各納入成果物に記載する事項について

納入成果物のうち、業務実施計画書、業務実施要領、情報セキュリティ管理計画書について、以下の項目を含めること。

1. 業務実施計画書

- (1) プロジェクトの目標
- (2) プロジェクトのスコープ
- (3) 体制図（責任者・契約担当・再委託の有無を含む）
- (4) 作業分担（PMDA との役割分担を含む）
- (5) マスタスケジュール
- (6) WBS
- (7) 納入成果物
- (8) 提案事項
- (9) 前提条件・制約事項

2. 業務実施要領

- (1) コミュニケーション管理要領（会議体、議事録作成ルール、連絡方法）
- (2) 進捗管理要領・リスク管理要領（報告頻度、報告様式、管理方法）
- (3) 課題管理要領・変更管理要領（様式、承認フロー）
- (4) 構成管理要領、文書管理要領（文書の編集ルール、バージョン管理、受領資料の管理方法）
- (5) セキュリティ管理要領（セキュリティ対策、履行状況の報告）
- (6) 品質管理要領（レビュー計画、トレーサビリティ・マトリクス、品質目標、工程完了基準）

3. 情報セキュリティ管理計画書

- (1) ISMS 等認証取得
- (2) 情報管理に関するルール（社内規程明示等）
- (3) 情報管理体制
- (4) 情報セキュリティインシデント対処方法
- (5) PMDA 情報の取扱い（目的外使用・意図しない変更を防止する方法を含む）
- (6) メンバのスキル・資格等
- (7) 自主点検の実施
- (8) 業務環境のセキュリティ
- (9) レポート体制
- (10) 再委託による履行保証措置
- (11) 緊急連絡方法
- (12) 教育・研修の実施

以上