新健康被害救済業務システムの運用支援業務
仕様書

令和６年 11 月

独立行政法人　医薬品医療機器総合機構

目次

１　調達案件の概要に関する事項

（１）　調達件名

新健康被害救済業務システムの運用支援業務

（２）　用語の定義

表 １.１ 用語の定義

用語	概要
相談カードシステム	救済給付に係る電話相談業務の支援を行うシステム。
副作用及び感染救済給付業務システム（給付システム）	医薬品等による副作用被害の救済に係る給付金及び、生物由来製品等による感染等被害救済に係る給付金について、申請受理から支払までの情報の管理等業務の支援を行うシステム。
救済給付データベース統合・解析システム（統合解析システム）	給付システムに蓄積されたデータ等の活用による関連データの集積・解析 及び、進捗管理、業務付加管理を行うシステム。サブシステムとして、業務サブシステム、現況サブシステム、作業進捗サブシステム、BI サブシステムがある。 業務サブシステムは、副作用被害救済と感染等被害救済の区分により、更に原審サブシステムと感染サブシステムとに分かれる。
拠出金徴収管理システム（拠出金システム）	拠出金徴収業務に係る申告書類の送付、収納、債権管理等の支援を行うシステム。 当拠出金徴収管理システムにおいて言及する「拠出金」とは副作用／感染／安全対策の各拠出金のみを指し、特定Ｃ型肝炎給付金に掛かる拠出金については含まない。
特定Ｃ型肝炎給付金支給等業務システム（特定Ｃ肝システム）	特定Ｃ型肝炎ウイルス感染者またはその相続人からの給付金請求の受付、給付金の支給、基金・拠出金等の管理等業務を支援するシステム。 当特定Ｃ肝システムにおいて言及する「拠出金」とは特定Ｃ型肝炎給付金に掛かる拠出金のみを指し、副作用／感染／安全対策の各拠出金については含まない。
救済相談	医薬品副作用被害救済制度、又は生物由来製品感染等被害救済制度に対する問い合わせに対応する相談事業。
精神面相談	医薬品副作用被害救済制度における副作用救済給付、又は生物由来製品感染等被害救済制度における感染救済給付の支給決定を受けた者、及びそのご家族を対象とした精神面のケア及び福祉サービスに繋げる助言を行うことを目的とする相談事業。
受給者カード	医薬品副作用被害救済制度における副作用救済給付の受給者のうち、希望者に対して公布されるカード。副作用の原因と考えられる又は推定される医薬品名を記載しており、医療機関などで診断や治療を受ける場合に正確に情報提供が行え

用語	概要
	ることなどを目的としている。支給決定の通知と共にカードの案内が受給者に送られて、希望者はPMDAに対して申し込みをすることで発行される。
生物由来製品等	人その他の生物（植物を除く。）の細胞、組織等に由来する原料又は材料を用いた製品のうち、保健衛生上特別の注意を要するもの、並びに再生医療等製品 （例）血液製剤、ワクチン、遺伝子組換製剤、細胞組織医療機器等
健康被害救済制度	医薬品等や生物由来製品等を適正に使用したにもかかわらず発生した副作用や感染等により、一定の健康被害が生じた場合に、医療費等の給付を行うことにより、被害者の救済を図る制度。 医薬品等による健康被害を救済する「医薬品副作用被害救済制度」及び生物由来製品等が原因となった感染等被害を救済する「生物由来製品感染等被害救済制度」がある。
副作用拠出金、感染拠出金	副作用・感染の救済給付に必要な費用に充てるため、許可医薬品等又は許可生物由来製品等製造販売業者から副作用拠出金又は感染拠出金を徴収している。副作用・感染の救済給付の原因となった許可医薬品等の製造販売業者からは、一般拠出金に加えて付加拠出金を徴収している。
安全対策等拠出金	安全対策業務の費用に充てるため、医薬品、医療機器、再生医療等製品又は体外診断用医薬品の製造販売業の許可を受けている者から、安全対策等拠出金を徴収している。
医薬品安全対策支援システム	医薬品副作用等報告の解析結果、データマイニング手法による統計学的評価、企業面談時の情報を統合することによる安全対策業務の支援を行うシステム。 （他部門所管）
副作用救済給付	医薬品副作用被害救済制度に係る給付業務。
感染救済給付	生物由来製品感染等被害救済制度に係る給付業務。
タイムクロック	給付申請してから決定されるまでに要する時間。
及び事例	被害者が同一の申請が複数ある場合に、効率良く調査を行えるよう、親となる事 例に子の事例の情報を集約し、まとめて調査を行う事例。

（３） 調達の背景

独立行政法人医薬品医療機器総合機構（以下「PMDA」という。）では、健康被害救済部（以下「救済部」という。）における救済給付業務、拠出金徴収業務及び救済制度に関する相談業務において、各業務のデータ処理や管理、業務統計の作成等の作業を迅速かつ効率的に実施するため業務ごとにシステムを構築し、必要に応じて各業務間を相互に連携する等、活用している。また平成20年度より「特定C型肝炎給付金支給等業務システム」（以下、「特定C肝システム」という。）を開発し、「特定フィブリノゲン製剤及び特定

血液凝固第Ⅸ因子製剤によるＣ型肝炎感染被害者を救済するための給付金の支給に関する特別措置法」（平成 20 年 1 月 16 日公布）に基づき、特定Ｃ型肝炎ウイルス感染者またはその相続人からの給付金請求の受付、給付金の支給、基金・拠出金等の管理等業務を行っているところである。

（４）　目的及び期待する効果

本調達は、救済部にて稼働している新救済業務システム（相談カードサブシステム、副作用及び感染救済給付業務サブシステム（以下、「給付システム」という。）、救済給付データベース統合・解析サブシステム（以下、「統合解析システム」という。）、拠出金徴収管理サブシステム、特定Ｃ型肝炎給付金支給等業務サブシステムの５つの業務サブシステムを持つシステム）及び住基ネット利用に係る情報機器の円滑な運用に資するため、システム全般にかかる運用支援業務の外部委託を行うものである。

（５）　業務・情報システムの概要

PMDA の前身である「医薬品副作用被害救済・研究振興調査機構」は昭和 54 年に「医薬品副作用被害救済基金」として設立され、その翌年５月から「医薬品副作用被害救済業務」を開始し、さらに、平成 16 年４月からは、生物に由来する原料や材料を使って作られた医薬品と医療機器による感染等の健康被害について救済する「生物由来製品感染等被害救済業務」を、平成 20 年１月 16 日からは、「特定フィブリノゲン製剤及び特定血液凝固第Ⅸ因子製剤によるＣ型肝炎感染被害者を救済するための給付金の支給に関する特別措置法」に基づく給付金の支給等の業務を開始しており、平成 26 年 11 月 25 日からは医薬品医療機器法の施行に伴い、再生医療等製品が医薬品副作用被害救済制度と生物由来製品感染等被害救済制度の対象となり、その支給等の業務も行っている。

併せて救済制度の概要、救済給付の請求方法、必要書類、請求書類の様式やその記載方法等についての問合せへの対応業務も行っているところ。

医薬品等の副作用による健康被害者に対して PMDA が行う救済給付等の業務に必要な費用は、許可医薬品製造販売業者等が納付した副作用拠出金等をもって充てられている。

同様に生物由来製品等を介した感染等による健康被害者に対して PMDA が行う救済給付等の業務に必要な費用は、許可生物由来製品製造販売業者等が納付した感染拠出金等をもって充てられている。更に PMDA が行う安全対策業務に必要な費用には、安全対策等拠出金等が充てられることになっている。

これら副作用拠出金／感染拠出金／安全対策等拠出金は、独立行政法人医薬品医療機器総合機構法に基づき、各年４月１日において医薬品医療機器法の規定によりそれぞれの製造販売業の許可を受けている者が、各年度、7 月 31 日までに PMDA に申告・納付することとされており、PMDA では当該拠出金の徴収管理に関する業務を行っている。

（６）　契約条件

受託者は、落札後に以下の契約条件にて PMDA と協議の上、契約を行うこと。

①　契約期間

契約締結日から令和８年３月 31 日までとする。

②　SLA の締結

運用業務については、受託者と PMDA との間で協議の上、SLA（Service Level Agreement）を締結する。サービスレベル評価項目と要求水準については、別紙１「SLA 項目」を参照すること。ただし、サービスレベル評価項目と要求水準については、協議の上、見直すこととする。

（７）　作業スケジュール

運用業務の対象期間は、契約日から令和８年３月 31 日を予定している。

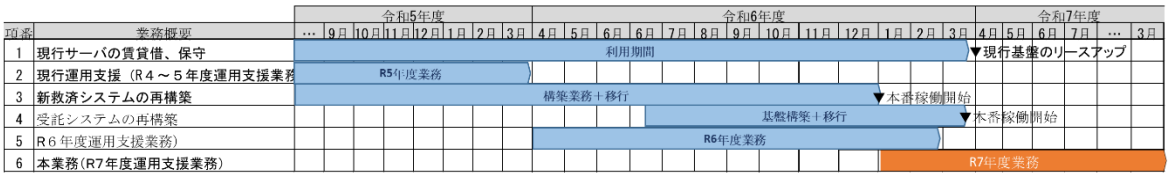
①　受託者は、契約開始日から運用業務の開始までに本情報システムの運用業務を実施するための準備を実施し、必要な情報について PMDA（または前受託者）より引継ぎを受けること。

②　本業務に係る想定スケジュールの概要は、別紙２「作業スケジュール」のとおりとする。なお、このスケジュールはあくまで想定のスケジュールであり、詳細な実施スケジュールは受託者が検討すること。

２　調達案件及び関連調達案件の調達単位、等に関する事項

（１）　調達案件及び関連する調達案件の調達単位、実施時期

図　２.１　関連する調達



（２）　調達案件間の入札制限

特になし。

３　作業の実施内容に関する事項

（１）　作業の内容

受託者は、本調達仕様書に記載された作業内容や各要件（別紙３「業務要件」等）を参照の上、以下に関し必要な作業を実施すること。

①　準備作業の内容

ア　実施計画書の作成

受託者は、契約開始日から令和７年１月の運用業務の開始までに、体制図、作業内容、作業体制、作業分担、スケジュール、文書管理要領、変更管理要領、WBS 等を記載した実施計画書及び情報セキュリティ管理計画書を作成し、PMDA の承認を受けること。

②　運用に係る作業の内容

ア　中長期的又は年度ごとの運用・保守作業計画の確定支援

受託者は、PMDA が中長期又は年度ごとの運用・保守作業計画を確定するに当たり、情報システムの構成やライフサイクルを通じた運用業務及び保守作業の内容について、計画案の妥当性に関する意見提示、情報提供等の支援を行うこと。

イ　定常時対応

イ－1 受託者は、別紙３「業務要件」の「運用業務の範囲定義」に示す運用業務（システム操作、運転管理・監視、稼動状況監視、サービスデスク提供等）を行うこと。具体的な実施内容・手順は実施計画書等に基づいて行うこと。

イ－2 受託者は、別紙４「システム運用管理基準」を参照の上、以下の内容について月次で運用報告を取りまとめ、PMDA に報告すること。

A)　運用期間・報告日・イベントの概況等の基本状況
B)　作業実績等の運用状況
C)　情報システムの稼働業務状況
D)　問合せ管理運用状況（サービスデスク稼働状況）（別紙４参照）
E)　インシデント管理状況（別紙４参照）
F)　問題管理状況(別紙４参照)
G)　変更管理状況（別紙４参照）
H)　バックアップ取得状況(別紙４参照)
I)　情報セキュリティ管理状況（情報セキュリティ遵守状況）（別紙４参照）
J)　アクセス権管理状況（特権（高権限 ID）管理状況）（別紙４参照）
K)　システムリソース状況　（キャパシティ管理、可用性管理）（別紙４参照）
L)　サービスレベル達成状況（別紙４参照）
M)　データ外部保管状況

N)　情報システムの定期点検状況（別紙５「情報セキュリティ対策の運用要件」参照）

O)　教育･訓練状況

P)　リスク課題の把握・対応状況

イ－3 受託者は、月間の運用実績を評価し、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。

イ－4 受託者は、運用作業報告書の内容について、月例の定期運用会議を開催し、その内容を報告すること。

イ－5 受託者は、ソフトウェア製品の保守の実施において、ソフトウェア製品の構成に変更が生じる場合には、PMDA にその旨を報告し、変更後の環境がライセンスの許諾条件に合致するか否かの確認を受けること。

ウ　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発生時の対応

ウ－1 受託者は、情報システムの障害発生時（又は発生が見込まれる時）には、速やかに PMDA に報告するとともに、その緊急度及び影響度を判断の上、別紙４「システム運用管理基準　４．２インシデント管理」に示す「インシデント報告書(ひな型)」を参照の上、障害発生時運用業務（障害検知、障害発生箇所の切り分け及び保守事業者との連携による原因調査、応急措置、復旧確認、報告等）を行うこと。なお、障害には、情報セキュリティインシデントを含めるものとする。具体的な実施内容・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いて行うこと。（インシデント管理プロセス手順書がない場合は、作成すること） また、情報セキュリティインシデントの場合は、「PMDA 情報セキュリティインシデント対処手順書」を参照の上、障害発生対応を実施のこと。

ウ－2 受託者は、情報システムの障害に関して事象の分析（発生原因、影響度、過去の発生実績、再発可能性等）を行い、同様の事象が将来にわたって発生する可能性がある場合には、恒久的な対応策を提案及び対応策の実施をすること。

ウ－3 受託者は、大規模災害等の発災時には、PMDA の指示を受けて、必要な対応を実施すること。

エ　情報システムの現況確認支援

エ－1 受託者は、年１回、PMDA の指示に基づき、システム資産簿と情報システムの現況との突合・確認（以下「現況確認」という。）を支援すること。

エ－2 受託者は、現況確認の結果、システム資産簿と情報システムの現況との間の差異がみられる場合は、運用実施要領に定める変更管理方法に従い、差異を解消すること。

エ－3 受託者は、現況確認の結果、ライセンス許諾条件に合致しない状況が認められる場合は、当該条件への適合可否、条件等を調査の上 PMDA に報告すること。

エ－4 受託者は、現況確認の結果、サポート切れのソフトウェア製品の使用が明らかとなった場合は、当該製品の更新の可否、更新した場合の影響の有無等を調査の上 PMDA に報告すること。

オ　運用作業の改善提案

受託者は、年度末までに年間の運用実績を取りまとめるとともに、必要に応じて中長期運用・保守作業計画、運用計画、運用実施要領に対する改善提案を行うこと。

③　保守に係る作業の内容

ア　中長期又は年度ごとの運用・保守作業計画の確定支援

受託者は、PMDA が中長期又は年度ごとの運用・保守作業計画を確定するに当たり、情報システムの構成やライフサイクルを通じた運用業務及び保守作業の内容について、計画案の妥当性の確認、情報提供等の支援を行うこと。

イ　定常時対応

イ－1 受託者は、別紙３「業務要件」の「保守業務の範囲定義」に示す保守業務（不具合受付等）及び定期点検（サーバ等のヘルスチェック）を行うこと。具体的な実施内容・手順は実施計画書等に基づいて行うこと。

イ－2 受託者は、定期点検（サーバ等のヘルスチェック）の結果、システム設定値等の差異がみられる場合は、PMDA へ報告の上、変更管理方法に従い、差異を解消すること。

イ－3 受託者は、保守作業計画及び保守実施要領に基づき、保守作業の内容や工数などの作業実績状況（情報システムの脆弱性への対応状況を含む。）、サービスレベルの達成状況、情報システムの定期点検状況、リスク・課題の把握・対応状況について月次で保守作業報告書を取りまとめること。

イ－4 受託者は、月間の保守実績を評価し、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。

イ－5 受託者は、保守作業報告書の内容について、月例の定期運用会議を開催し、その内容を報告すること。

ウ　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発生時の対応

ウ－1 受託者は、情報システムの障害発生時（又は発生が見込まれる時）には、速やかに PMDA に報告するとともに、その緊急度及び影響度を判断の上、別紙４「システム運用管理基準　４．２インシデント管理」に示す「インシデント報告書(ひな型)」を参照の上、障害発生時運用業務（障害検知、障害発生箇所の切り分け及び保守事業者との連携による原因調査、応急措置、復旧確認、報告等）を行うこと。なお、障害には、情報セキュリティインシデントを含めるものとする。具体的な実施内容・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いて行うこと。（インシデント管理プロセス手順書がない場合は、作成すること） また、情報セキュリティインシデントの場合は、「PMDA 情報セキュリティインシデント対処手順書」を参照の上、障害発生対応を実施のこと。

ウ－2 受託者は、情報システムの障害に関して事象の分析（発生原因、影響度、過去の発生実績、再発可能性等）を行い、同様の事象が将来にわたって発生する可能性がある場合には、恒久的な対応策を提案及び対応策の実施をすること。

ウ－3 受託者は、大規模災害等の発災時には、PMDA の指示を受けて、必要な対応を実施すること。

エ　情報システムの現況確認支援

エー1 受注者は、年１回、PMDA の指示に基づき、システム資産簿と情報システムの現況との突合・確認（以下「現況確認」という。）を支援すること。

エー2 受注者は、年１回、PMDA の指示に基づき、情報システム台帳（セキュリティ要件に係る事項）の作成･更新を支援すること。

オ　保守作業の改善提案

受注者は、年度末までに年間の保守実績を取りまとめるとともに、必要に応じて中長期保守・保守作業計画、保守計画、保守実施要領に対する改善提案を行うこと。

④　作業報告

ア　作業工数実績の報告

受注者は、本業務で実施した作業の工数について、月次で PMDA 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。

⑤　引継ぎ

ア　受託者は、PMDA が本システムの更改を行う際には、次期の情報システムにおける要件定義支援事業者及び設計・開発事業者等に対し、作業経緯、残存課題等に関する情報提供及び質疑応答等の協力を行うこと。

イ　受託者は、現行運用事業者から令和７年１月からの運用に必要な事項の引継ぎとして、運用監視作業エリアの引継、サービスデスクの引継、システム資源及びデータの引継を受け、現行事業者から提供される資料（運用作業の計画書や報告書、運用設計書及び運用手順書等の一覧）を基に自主的に業務習熟を行うこと。
現行運用事業者からの引継作業は受託者の負担と責任において実施すること。
ただし、こちらは旧救済システム環境における手順であるため、システムに係る手順としてではなく問合せ対応等の運用に係る手順として参照すること。

ウ　受託者は、新救済システム再構築の事業者より、新救済システムにおける各種手順等について引継ぎを受けること。
ただし、令和７年１月～2 月にかけて運用保守計画を予定しており、この中で運用手順等が作成されるため、本業務の開始時点では引継ぎすべき手順が存在しないことが想定される。そのため、本業務開始時点ではシステム仕様について自主的に知識を深めると共に、問合せ対応等にあたっては新救済システム再構築の事業者と相談しつつ対応すること。

エ　受託者は、本調達に係る契約期間終了後、受託者と異なる事業者が本情報システムの運用業務を受注した場合には、次期運用事業者に対し、作業経緯、残存課題等下記項目についての引継ぎを行うこと。

A)　問合せ、障害等の対応及び管理に関する手法・手順

B)　システム運用マニュアル、運用業務マニュアル
C)　仕掛中の項目一覧及びその進捗状況
D)　過去の問合せ、障害等の実績及びその対応方法
E)　バックログ・未対応作業一覧及びその対応(案)
F)　その他業務を引継ぐ上で必要と思われる事項

（２）　システム資産簿登録に係る作業

受注者は、対象システムに更新等が発生した場合、PMDA が指定する以下のシステム資産簿登録用シートを、運用実施要領において定める時期に提出すること。

ア　IT 機器管理簿
イ　導入ソフトウェア一覧
ウ　資産収集情報詳細
エ　ハードウェアサポート期限
オ　ソフトウェアサポート期限
カ　ソフトウェアライセンス
キ　ソフトウェア名称
ク　その他 PMDA が指定する項目

○資産台帳・管理簿(システム台帳)を下記の項目で更新する。

・情報システム名　・管理課室　・当該情報システムセキュリティ責任者の氏名及び連絡先　・システム構成　・接続する機構外通信回線の種別　・取り扱う情報の格付及び取扱制限に関する事項　・当該情報システムの設計/開発、運用/保守に関する事項

○ネットワーク機器ソフトウェア資産台帳を下記の項目で更新する。

・ネットワーク機器名　・ソフトウェア名　・バージョン　・脆弱性/アップデート公開情報　・アップデート適用履歴　・外部との通信内容　・設定シートパス名　・その他のサポート状況・リスク　・確認頻度　・最終確認日

（３）　成果物の範囲、納品期日等

①　成果物

作業工程別の納入成果物を表 ３．１に示す。ただし、納入成果物の構成、詳細については、受注後、PMDA と協議し取り決めること。

表 ３．１　工程と成果物

項番	工程	納入成果物（注 1）	納入期日	納品に関する注意事項
1	準備	・運用準備作業に関する実施計画書（運用準備作業）	契約締結日から 2 週間以内	

項番	工程	納入成果物（注 1）	納入期日	納品に関する注意事項
2	計画	・実施計画書（体制図、作業内容、作業体制、作業分担、スケジュール、文書管理要領、変更管理要領、WBS） ・情報セキュリティ管理計画書（情報セキュリティ対策実施内容及び管理体制）	契約日の運用業務の開始まで	
3	運用	・システム運用マニュアル(注２) ・運用業務マニュアル(注３) ・システム関連ドキュメント ・プログラム・ツール等	令和８年３月 31 日 （※必要に応じて随時提出）	
4	その他	・作業週報 ・月例報告資料 ・アウトソーシングセンター設置サーバ稼働状況報告書 ・打合せ資料 ・議事録 ・障害等作業記録 ・運用支援報告書	令和８年３月 31 日 （※必要に応じて随時提出）	

注１　納入成果物の作成にあたっては、SLCP-JCF2013（共通フレーム 2013）を参考とすること。

注２　システム運用上、運用支援要員の行うべき業務内容及び操作手順に関するマニュアルとし、全対象システムについて次の内容を盛り込んだものとする。

(ｱ)ジョブ一覧、(ｲ)起動・停止手順、(ｳ)バックアップ手順、(ｴ)リカバリ手順、(ｵ)障害監視手順、(ｶ)障害対応手順、(ｷ)ログ確認手順、(ｸ)性能監視手順、(ｹ)設定変更手順、(ｺ)ユーザ管理手順、(ｻ)マスタの更新及びそれに伴うデータ修正手順、(ｼ) (ｱ)～(ｻ)の他、本業務の適切な履行のために運用支援要員が準拠すべき内容を網羅した手順書等

注３　システム運用上の業務プロセスを定めた「業務フロー及び手順書」とし、次のシステム運用業務について作成･更新するものとする。

(ｱ)問合せ管理プロセス　(ｲ)インシデント管理プロセス　(ｳ)変更管理プロセス　(ｴ)リリース管理プロセス　(ｵ)構成管理プロセス　(ｶ)問題管理プロセス　(ｷ)各定期点検プロセス　(ｸ)リスク管理プロセス　(ｹ)課題管理プロセス　(ｺ)情報セキュリティ管理プロセス。

② 納品方法

表 ３．１の納入成果物を含む全ての納入成果物を令和８年３月 31 日に納品すること。なお、納入成果物については、以下の条件を満たすこと。

ア　成果物は、すべて日本語で作成すること。ただし、日本国においても、英字で表記されることが一般的な文言については、そのまま記載しても構わないものとする。

イ　用字・用語・記述符号の表記については、「公用文作成の要領」に準拠すること。

ウ　情報処理に関する用語の表記については、日本工業規格（JIS）の規定に準拠すること。

エ　受託者は、指定のドキュメント，ソフトウェア、ソースコード等を電子媒体（DVD-R 等)により納品すること。

オ　電子媒体に保存する形式は MicrosoftWord2016、同 Excel2016、同 PowerPoint2016 で読み込み可能な形式及び PDF 形式とすること。ただし、PMDA が他の形式による提出を求めた場合は、これに応じること。なお、受託者側で他の形式を用いて提出したいファイルがある場合は、協議に応じるものとする。

カ　納品したドキュメントに修正等があった場合は、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。

キ　電子媒体は、2 部納品すること。

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

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

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

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

シ　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。

ス　納品に当たっては、現存するドキュメント等を変更する必要がある場合はそれらを修正することとし、修正点が分かるように表記すること。なお、現存するドキュメントについては別紙８「資料閲覧について」を参照の上確認すること。

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

③　納品場所

独立行政法人　医薬品医療機器総合機構　健康被害救済部

４　満たすべき要件に関する事項

本業務の実施にあたっては、以下に記載の各要件を満たすこと。

○別紙３　業務要件
○別紙４　システム運用管理基準
○別紙５　情報セキュリティ対策の運用要件
○閲覧資料　セキュリティ管理要件書(ひな型)

５　作業の実施体制・方法に関する事項

（１）　作業実施体制

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

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

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

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

④ 受託者は、プロジェクトの推進体制及び本件受託者に求める作業実施体制を PMDA と協議の上定めること。また、受託者の情報セキュリティ対策の管理体制については、作業実施体制とは別に作成すること。

（２）　作業要員に求める資格等の要件

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

① 運用責任者･リーダの必要スキル

A) システム運用保守業務経験が 10 年以上
B) システム運用保守業務のマネジメント経験が 3 年以上
C) ITIL ファウンデーションの資格もしくは ITIL を用いた作業管理の業務経験

① 従業員 100 名以上の規模を有する事業所等において、以下の製品・システムを取り扱うヘルプデスク業務を担当した実績を有する要員を体制に含めること。 各項目の条件に関しては、1 人ですべての条件を充足する必要はない。

- Windows Server 2012 以上
- Visual Basic で構築されたクライアント/サーバ形式の業務アプリケーション
- データベース製品（Oracle、SQLServer）
- VMware ESX3.5 以上
- NAS 及び SAN ストレージ
- 負荷分散装置
- バックアップソフト

② 救済部企画管理課、給付課、調査第一課、調査第二課、特定救済課、拠出金課の各業務及び安全情報・企画管理部の拠出金関連業務を理解する能力を有しており、本業務システムの運用にあたり、PMDA に逐次業務の説明を求めることなく担当者とスムーズな会話ができること。

（３） 作業場所

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

（4） 作業の管理に関する要領

① 受託者は、PMDA の指示に従って運用業務に係るコミュニケーション管理、体制管理、作業管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。
② 受託者は、PMDA の指示に従って保守業務に係るコミュニケーション管理、体制管理、作業管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。

６ 作業の実施に当たっての遵守事項

（１） 基本事項

受託者は、次に掲げる事項を遵守すること。

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

② 本業務に従事する要員は、PMDA と日本語により円滑なコミュニケーションを行う能力と意思を有していること。
③ 本業務の履行場所を他の目的のために使用しないこと。
④ 本業務に従事する要員は、履行場所での所定の名札の着用等、従事に関する所定の規則に従うこと。
⑤ 要員の資質、規律保持、風紀及び衛生・健康に関すること等の人事管理並びに要員の責めに起因して発生した火災・盗難等不祥事が発生した場合の一切の責任を負うこと。
⑥ 受託者は、本業務の履行に際し、PMDA からの質問、検査及び資料の提示等の指示に応じること。また、修正及び改善要求があった場合には、別途協議の場を設けて対応すること。
⑦ 本業務を実施する上で必要となる機器物品等は、受注者の責任で手配するとともに、費用を負担すること。
⑧ 次回の本業務調達に向けた現状調査、PMDA が依頼する技術的支援に対する回答、助言を行うこと。
⑨ 本業務においては、業務終了後の運用等を、受託者によらずこれを行うことが可能となるよう詳細にドキュメント類の整備を行うこと。

（２） 機密保持、資料の取扱い

本業務を実施する上で必要とされる機密保持に係る条件は、以下のとおり。

① 受託者は、受注業務の実施の過程で PMDA が開示した情報（公知の情報を除く。以下同じ。）、他の受託者が提示した情報及び受託者が作成した情報を、本受注業務の目的以外に使用又は第三者に開示若しくは漏洩してはならないものとし、そのために必要な措置を講ずること。
② 受託者は、本受注業務を実施するにあたり、PMDA から入手した資料等については管理簿等により適切に管理し、かつ、以下の事項に従うこと。
- 複製しないこと。
- 用務に必要がなくなり次第、速やかに PMDA に返却又は消去すること。
- 受注業務完了後、上記①に記載される情報を削除又は返却し、受託者において該当情報を保持しないことを誓約する旨の書類を PMDA に提出すること。

③ 応札希望者についても上記①及び②に準ずること。
④ 「独立行政法人 医薬品医療機器総合機構 情報システム管理利用規程」の第 52 条に従うこと。
⑤ 「秘密保持等に関する誓約書」を別途提出し、これを遵守しなければならない。
⑥ 機密保持の期間は、当該情報が公知の情報になるまでの期間とする。

（３） 遵守する法令等

本業務を実施するにあたっての遵守事項は、以下のとおり。

① 受託者は、民法、刑法、著作権法、不正アクセス行為の禁止等に関する法律、行政機関の保有する個人情報の保護に関する法律等の関連法規及び労働関係法令を遵守すること。

② 受託者は、次の文書に記載された事項を遵守すること。遵守すべき文書が変更された場合は変更後の文書を遵守すること。

ア 独立行政法人 医薬品医療機器総合機構 サイバーセキュリティポリシー

イ 独立行政法人 医薬品医療機器総合機構 情報システム管理利用規程

ウ 独立行政法人 医薬品医療機器総合機構 個人情報管理規程

エ 政府機関等の情報セキュリティ対策のための統一規範（最新版）

オ 政府機関等の情報セキュリティ対策の運用等に関する指針（最新版）

カ 政府機関等の情報セキュリティ対策のための統一基準（最新版）

なお、「PMDA サイバーセキュリティポリシー」は非公開であるが、「政府機関等の情報セキュリティ対策のための統一基準（最新版）」に準拠しているので、必要に応じ参照すること。「PMDA サイバーセキュリティポリシー」の開示については、入札説明会に参加した事業者のうち、事業者が PMDA に「秘密保持等に関する誓約書」を提出した際に開示する。

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

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

7 成果物の取扱いに関する事項

（１） 知的財産権の帰属

知的財産の帰属は、以下のとおり。

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

② 本件に係り発生した権利については、受託者は著作者人格権（著作権法第 18 条から第 20 条までに規定する権利をいう。）を行使しないものとする。
③ 本件に係り発生した権利については、今後、二次的著作物が作成された場合等であっても、受託者は原著作物の著作権者としての権利を行使しないものとする。
④ 本件に係り作成・変更・修正されるドキュメント類及びプログラム等に第三者が権利を有する著作物が含まれる場合、受託者は当該著作物の使用に必要な費用負担や使用許諾契約に係る一切の手続きを行うこと。この場合は事前に PMDA に報告し、承認を得ること。
⑤ 本件に係り第三者との間に著作権に係る権利侵害の紛争が生じた場合には、当該紛争の原因が専ら PMDA の責めに帰す場合を除き、受託者の責任、負担において一切を処理すること。この場合、PMDA は係る紛争の事実を知ったときは、受託者に通知し、必要な範囲で訴訟上の防衛を受託者にゆだねる等の協力措置を講ずる。なお、受託者の著作又は一般に公開されている著作について、引用する場合は出典を明示するとともに、受託者の責任において著作者等の承認を得るものとし、PMDA に提出する際は、その旨併せて報告するものとする。

（２） 契約不適合責任

① 本業務の最終検収後 1 年以内の期間において、委託業務の納入成果物に関して本システムの安定稼動等に関わる契約不適合の疑いが生じた場合であって、PMDA が必要と認めた場合は、受託者は速やかに契約不適合の疑いに関して調査し回答すること。調査の結果、納入成果物に関して契約不適合等が認められた場合には、受託者の責任及び負担において速やかに修正を行うこと。なお、修正を実施する場合においては、修正方法等について、事前に PMDA の承認を得てから着手すると共に、修正結果等について、PMDA の承認を受けること。
② 受託者は、契約不適合責任を果たす上で必要な情報を整理し、その一覧を PMDA に提出すること。契約不適合責任の期間が終了するまで、それら情報が漏洩しないように、ISO/IEC27001 認証（国際標準）又は JISQ27001 認証（日本工業標準）に従い、また個人情報を取り扱う場合には JISQ15001（日本工業標準）に従い、厳重に管理をすること。また、契約不適合責任の期間が終了した後は、速やかにそれら情報をデータ復元ソフトウェア等を利用してもデータが復元されないように完全に消去すること。データ消去作業終了後、受託者は消去完了を明記した証明書を作業ログとともに PMDA に対して提出すること。なお、データ消去作業に必要な機器等については、受託者の負担で用意すること。

（３） 検収

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

なお、以下についても遵守すること。

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

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

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

８　入札参加資格に関する事項

（１）入札参加要件

応札希望者は、以下の条件を満たしていること。

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

② ISO/IEC27001 認証（国際標準）又は JISQ27001 認証（日本産業規格）のいずれかを取得していること。

③ プライバシーマーク付与認定を取得していること。

④ PMDA にて現行関連システムの設計書等を閲覧し、内容を十分理解していること。資料閲覧は別紙 8 を参照すること。

⑤ 応札時には、開発する機能毎に十分に細分化された工数、概算スケジュールを含む見積り根拠資料の即時提出が可能であること。なお、応札後に PMDA が見積り根拠資料の提出を求めた際、即時に提出されなかった場合には、契約を締結しないことがある。

（２）入札制限

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

① PMDA の CIO 補佐が現に属する、又は過去 2 年間に属していた事業者等
② 各工程の調達仕様書の作成に直接関与した事業者等
③ 設計・開発等の工程管理支援業者等
④ ①～③の親会社及び子会社（「財務諸表等の用語、様式及び作成方法に関する規則」（昭和 38 年大蔵省令第 59 号）第 8 条に規定する親会社及び子会社をいう。以下同じ。）
⑤ ①～③と同一の親会社を持つ事業者
⑥ ①～③から委託を請ける等緊密な利害関係を有する事業者

９ 情報セキュリティ管理

（１） 情報セキュリティ対策の実施

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

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、受託者又はその従業員、本調達の役務内容の一部を再委託する先、若しくはその他の者による意図せざる変更が加えられないための管理体制が整備されていること。
③ 受託者の資本関係・役員等の情報、本業務の実施場所、本業務従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供を行うこと。具体的な情報提供内容については PMDA と協議の上、決定するものとする。
④ 情報セキュリティインシデントへの対処方法が確立されていること。
⑤ 情報セキュリティ対策その他の契約の履行状況を定期的に確認し、PMDA へ報告すること。
⑥ 情報セキュリティ対策の履行が不十分である場合、速やかに改善策を提出し、PMDA の承認を受けた上で実施すること。
⑦ PMDA が求めた場合に、速やかに情報セキュリティ監査を受入れること。
⑧ 本調達の役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるように情報セキュリティ管理計画書に記載された措置の実施を担保すること。
⑨ 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。
⑩ PMDA から受領した要保護情報が不要になった場合は、これを確実に返却、又は抹消し、書面にて報告すること。
⑪ 本業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかに PMDA に報告すること。

（２） 情報セキュリティ監査の実施

① PMDA がその実施内容（監査内容、対象範囲、実施等）を定めて、情報セキュリティ監査等を行う（PMDA が選定した事業者による監査を含む。）ものとする。受託者は、あらかじめ情報セキュリティ監査等を受け入れる部門、場所、時期、条件等を「実施計画書」に付記し提示すること。
② 受託者は自ら実施した外部監査についても PMDA へ報告すること。
③ 受託者は、情報セキュリティ監査の結果、本調達における情報セキュリティ対策の履行状況について PMDA が改善を求めた場合には、PMDA と協議の上、必要な改善策を立案して速やかに改善を実施するものとする。
④ 本調達に関する監査等が実施される場合、受託者は、技術支援及び情報提供を行うこと。
⑤ 受託者は、指摘や進捗等把握のための資料提出依頼等があった場合は、PMDA と協議の上、内容に沿って適切な対応を行うこと。

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

１０ 再委託に関する事項

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

② ①における「主要部分」とは、以下に掲げるものをいう。

ア　総合的企画、業務遂行管理、手法の決定及び技術的判断等。

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

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

ただし、以下の場合には再委託を可能とする。

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

③ 受託者は、再委託する場合、事前に再委託する業務、再委託先等を PMDA に申請し、承認を受けること。申請にあたっては、「再委託に関する承認申請書」の書面を作成の上、受託者と再委託先との委託契約書の写し及び委託要領等の写しを PMDA に提出すること。受託者は、機密保持、知的財産権等に関して本仕様書が定める受託者の責務を再委託先業者も負うよう、必要な処置を実施し、PMDA に報告し、承認を受けること。なお、第三者に再委託する場合は、その最終的な責任は受託者が負うこと。

④ 再委託先が、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。

- 受託者は再委託先における情報セキュリティ対策の実施内容を管理し PMDA に報告すること。
- 受託者は業務の一部を委託する場合、本業務にて扱うデータ等について、再委託先またはその従業員、若しくはその他の者により意図せざる変更が加えられないための管理体制を整備し、PMDA に報告すること。

- 受託者は再委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関して、PMDA から求めがあった場合には情報提供を行うこと。
- 受託者は再委託先にて情報セキュリティインシデントが発生した場合の再委託先における対処方法を確認し、PMDA に報告すること。
- 受託者は、再委託先における情報セキュリティ対策、及びその他の契約の履行状況の確認方法を整備し、PMDA へ報告すること。
- 受託者は再委託先における情報セキュリティ対策の履行状況を定期的に確認すること。また、情報セキュリティ対策の履行が不十分な場合の対処方法を検討し、PMDA へ報告すること。
- 受託者は、情報セキュリティ監査を実施する場合、再委託先も対象とするものとする。
- 受託者は、再委託先が自ら実施した外部監査についても PMDA へ報告すること。
- 受託者は、委託した業務の終了時に、再委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認すること。

１１ その他特記事項

（１）環境への配慮

環境への負荷を低減するため、以下に準拠すること。

① 本件に係る納入成果物については、最新の「国等による環境物品等の調達の推進等に関する法律（グリーン購入法）」に基づいた製品を可能な限り導入すること。
② 導入する機器等がある場合は、性能や機能の低下を招かない範囲で、消費電力節減、発熱対策、騒音対策等の環境配慮を行うこと。

（２）その他

PMDA 全体管理組織（PMO）が担当課に対して指導、助言等を行った場合には、受託者もその方針に従うこと。

１２ 附属文書

（１）調達仕様書　別紙

別紙１　「ＳＬＡ（Service Level Agreement）項目」
別紙２　「作業スケジュール」
別紙３　「業務要件」

別紙４　「システム運用管理基準」
別紙５　「情報セキュリティ対策の運用要件」
別紙６　「健康被害救済業務システム概略図」
別紙７　「ハードウェア・ソフトウェア構成一覧」
別紙８　「資料閲覧について」

（２）事業者が閲覧できる資料一覧

閲覧資料１　独立行政法人 医薬品医療機器総合機構　サイバーセキュリティポリシー
閲覧資料２　PMDA 情報セキュリティインシデント対処手順書
閲覧資料３　セキュリティ管理要件書(ひな型)
閲覧資料４　健康被害救済業務システムに係る関連資料
これら資料は、PMDA に「秘密保持等に関する誓約書」を提出した事業者へ開示する。

１３ 窓口連絡先

独立行政法人　医薬品医療機器総合機構　健康被害救済部部企画管理課
柴垣
電話：03 (3506) 9460

E-mail:kaitou●pmda.go.jp
●を@（半角）に変換して送信してください。

別紙1 「SLA(Service Level Agreement)項目」

指標の種類	指標名	計算式	単位	目標値	計測方法	計測周期
問い合わせへの一次回答	一次回答の応答時間	応答時刻－問い合わせ受付時刻＜60 分の件数／問い合わせ件数	%	100%	問い合わせ一覧表に受付と応答日時の記録	毎月
セキュリティ対策	セキュリティ事故発生件数	セキュリティ事故発生件数	件	0 件	セキュリティ対策ソフトウェアおよび人手により検知されたセキュリティ事故(防御されたものは除く)の発生件数の集計	毎月
運用業務サービス	サービス提供時間	9:00～18:00 のサービスを提供できなかった日数／営業日数×100	%	0%	勤務実績の提出	毎月
	報告書類の提出期限	期限までに提出した報告書類の件数／報告書類の件数×100	%	100%	提出期日と報告日の比較	都度
ヘルプデスク業務	サービス提供時間	9:00～18:00 のサービスを提供できなかった日数／営業日数×100	%	0%	勤務実績の提出	毎月
障害対応	初動対応の開始	異常の発見から 15 分以内に初動対応を行った障害件数／障害件数×100	%	100%	障害発見日時と初動対応開始日時の障害報告書への記録	毎月
	障害発生の連絡	異常の発見から 1 時間以内に PMDA に連絡した障害件数／障害件数×100	%	100%	障害発見日時と障害発生連絡日時の障害報告書への記録	毎月
	障害報告書の提出期限	期限までに提出した障害報告書の件数／障害報告書の件数×100	%	100%	提出期日と報告日の比較	都度
システム稼働	システム稼働率	(計画サービス時間－計画外サービス停止時間)／計画サービス時間×100 ※1 分未満のサービス停止時間は切り捨て)	%	99.9%	サービス停止開始・終了日時の記録	毎月

別紙2　作業スケジュール

No	セキュリティ対策	実施区分	2024年度 契約月	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	2025年度 1月	2月	3月	実施内容
マイルストン																			
1-1	キックオフ	実施 ◎	▲																実施計画書に基づくキックオフを実施
1-2	実施計画書の作成	実施 ◎	実施																契約後2週間以内に運用準備作業に関する実施計画書（運用準備作業）を作成し、PMDAの承認を受ける。
1-3	月次定例	実施 ◎		▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	
1-4	次年度(新業者)への引継ぎ	実施 ◎															実施		
運用																			
2-1	インシデント一覧報告（ｼｽﾃﾑ障害、情報ｾｷｭﾘﾃｨｲﾝｼﾃﾞﾝﾄを含む）	報告 ○		▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	「システム運用標準」 ⇒インシデント管理：インシデント一覧による月次報告
2-2	システム変更作業報告 （パッチ適用状況報告を含む）	報告 ○		▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	「システム運用標準」 ⇒変更管理：変更作業一覧による月次報告
2-3	特権ID使用状況報告 （台帳を含む）	報告 ○		▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	「システム運用標準」 ⇒特権ID管理台帳・特権ID使用管理簿による月次報告
2-4	データ保全（バックアップ）状況の点検	報告 ○		▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	「システム運用標準」 ⇒バックアアプと回復：遵守状況の月次報告、机上訓練（任意）
2-5	情報セキュリティ：遵守状況の報告	報告 ○		▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	「システム運用標準」 ⇒情報セキュリティ：遵守状況の報告
2-6	脆弱性対策の実施状況の点検	報告 ○		▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	▲報告	⇒情報セキュリティ管理：セキュリティパッチ適用状況の報告 脆弱性に関し関する新着情報、影響度・適用要否、適用予定と実績
権限管理																			
3-1	各業務データアクセス権限再検証	支援 △							準備		実施		▲報告			▲報告			不要なアクセス権限の洗い出しと削除。
3-2	ユーザーID棚卸し （各業務システム）	実施 ◎							準備		実施		▲報告			▲報告			不要IDの洗い出しと削除・無効化。不要なID、権限があれば削除する。
3-3	特権ID検証(棚卸し)	実施 ◎					準備		実施	▲報告									【システム運用標準】"システム運用管理(要件書)"に基づく運用 ⇒台帳と使用管理簿の相関チェック、使用管理簿とログの相関チェック
3-4	パソコン等搭載ソフトウェアの定期的な調査、不要ソフトウェアの削除	支援 △													準備	実施		▲報告	使用するソフトウェア・バージョン、ソフトウェアの利用可否基準を整理し、棚卸を実施する（パソコン更改時に対応し「台帳」を整備する）
点検																			
4-1	情報資産棚卸し・リスク評価	支援 △				準備	実施				▲報告								⇒　厚労省のガイドラインに従って実施：「情報資産台帳」「情報資産ライフサイクル確認様式」「リスク評価チェックシート様式」の作成・更新
4-2	パソコン等情報資産棚卸し	支援 △													準備	実施		▲報告	台帳と現物との照合（照合結果に基づく「台帳」の作成）
4-3	システム台帳の最新化	支援 △							準備		実施		▲報告						⇒資産台帳・管理簿(システム台帳)を更新する。 ⇒ネットワーク機器ソフトウェア資産台帳を更新する。
4-4	ログ取得状況の点検	支援 △							準備	実施	▲報告								⇒情報資産の重要度に応じて、監視対象となるイベントを絞り込み、ファイル抽出した上で、セキュリティ違反を示す証跡がないかを定期的に確認する。
4-5	セキュリティヘルスチェック（不正プログラム及び不正な設定変更の有無確認）	支援 △					準備	実施	▲報告										
4-6	情報セキュリティ：遵守状況の自己点検	実施 ○			準備	実施	▲報告												「システム運用標準」 ⇒情報セキュリティ：遵守状況の報告
4-7	情報システム開発・運用資料確認	実施 ○								準備	実施				▲報告			▲報告	情報システムの開発・運用・保守に必要な各種ドキュメント（各種設計書、手順書等）と実装（システムの構成・設定、プログラム等）が一致していることを確認する。
教育・訓練																			
5-1	システム運用担当者 （サービスデスク）向け研修	受講 △							受講										6月に2回開催予定
内部監査																			
6-1	委託先における情報セキュリティ対策の履行状況の確認	受査 ◎							準備		受査								⇒過去の実施手順を参考に対象システムを選定の上、PMDA内部検査を実施
PMDA監査受査への支援																			
7-1	厚労省・情報セキュリティ監査	支援 △							監査支援										
7-2	調達による第3者情報セキュリティ監査	支援 △								監査支援									
7-4	監査指摘対応フォロー	支援 △	･･･運用フォロー･･･				▲報告	･･･運用フォロー･･･					▲報告						「過去の監査対応状況について」に基づく進捗管理、半期毎に報告

別紙3 「業務要件」

業務の時期・時間の定義

	実施時期・期間	実施・提供時間	補足
通年	契約日 ～令和 8 年 3 月 31 日 ※業務を行う日（平日）とは、本仕様書で別途定められている業務の他は、行政機関の休日（「行政機関の休日に関する法律」（昭和 63 年法律第 91 号）第 1 条第 1 項に掲げる日をいう。）を除く日とする。	9:00～18:00 ※12:00～13:00 は休憩時間とする。	ただし、本仕様書で別途定めるものの他、緊急作業及び本業務を実施するために必要な作業がある場合は、この限りではない。

運用業務の範囲定義

No	名称	内容
1	【システム監視 － 稼動監視】	本システムのハードウェア、ソフトウェア、ネットワークに対して、以下の稼動状況（パフォーマンス）を監視し、監視実績を記録・管理すること。 ※本システムのハードウェア、ソフトウェア、ネットワークに対し、死活監視、障害監視、エラー出力監視を行い、異常を発見した場合は障害対応手順に沿って対応すること。監視に当たっては事前に PMDA と協議の上、必要に応じてツール等を用いた常時監視の仕組みを構築すること。 (1) ソフトウェア及び開発アプリケーションの稼動状況 (2) ハードウェアの各種状況（性能、容量、故障、縮退） (3) バックアップなどの定期起動ジョブの実行結果 (4) セキュリティアラートの発生状況
2	【システム監視 － ログ監視】	本システムを構成する機器及びソフトウェア上で入手可能なログの管理、監視を行い、必要に応じて外部環境に保管すること。 定期的にログの内容を確認し、異常検知した場合は速やかに総合機構に報告し、問題解決のための対処を行うこと。
3	【システム監視 － 情報セキュリティ監視】	本システムへの不正侵入、不正改ざん検知、ウイルスチェックなど、本システムに関するセキュリティ監視を行うこと。
4	【システム設定・操作 － ジョブ管理】	操作ミスの防止や無人化を目的とした操作の自動化を行う場合、必要となるジョブスケジュールの設定等を行うこと。また、ジョブの登録／変更／削除が必要となる場合には PMDA に提案し、PMDA の了解の下、当該作業を実施すること。
5	【システム設定・操作 － 容量・能力管理】	本システムの性能を計測する指標（CPU 負荷、メモリ使用量、ディスク使用量など）を PMDA と協議の上で確定し、指標データを常時収集し、閾値を超えるなどの異常を発見した場合は障害対応について PMDA に提案し、PMDA の了解の下、当該作業を実施すること。
6	【ヘルプデスク業務 － 問い合わせ対応】	利用者からのシステムに関する問い合わせに対応すること。なお、問い合わせ手段は基本的に電話、電子メールとし、専用のフォーマットを用意し、問合せ内容や

No	名称	内容
		処置内容を漏らさず記録すること。また、システム及び機器の障害に関する問い合わせについては原因の調査を実施し、PMDA 担当者に連絡すること。その際は、解決のための対応策も提案すること。保守サービスや各種メーカーへの問合せ時には窓口となって情報を集約すること。
7	【運用管理】	システム運用上の業務プロセスを定めた「業務フロー及び手順書」について、次のシステム運用業務について作成・更新するものとする。 (ｱ)問合せ管理プロセス (ｲ)インシデント管理プロセス (ｳ)変更管理プロセス (ｴ)リリース管理プロセス (ｵ)構成管理プロセス (ｶ)問題管理プロセス (ｷ)各定期点検プロセス (ｸ)リスク管理プロセス (ｹ)課題管理プロセス (ｺ)情報セキュリティ管理プロセス。 変更管理及びリリース管理に伴うハードウェア、ソフトウェア等の資源の版数管理、原本管理を行うこと。本業務の改修案件に限らず、対象システムに対する全ての変更について構成管理を行うこと。
8	【ユーザー管理】	(ア) PMDA から提出されるユーザ登録・削除依頼に基づき、OS 上、及びアプリケーション上のユーザを登録・削除すること。作業内容はすべて作業ログとして蓄積し、PMDA に報告すること。(随時／適宜) (イ) システムを構成する機器やアプリケーション等のユーザ管理 システムを構成する機器やアプリケーション、リモートアクセス機器及びリモートアクセスユーザを管理の対象とすること。 (ウ) アクセス権限管理 管理対象となる各種ユーザのアクセス権限の管理を行うこと。
9	【サービスレベル管理】	別紙1 「SLA(Service Level Agreement)項目」参照 運用業務については、受託者とPMDAとの間で協議の上、SLA(Service Level Agreement)を締結する。サービスレベル評価項目と要求水準については、別紙1「SLA項目」を参照すること。ただし、サービスレベル評価項目と要求水準については、協議の上、見直すこととする。
10	【バックアップ/リカバリ】	重大な障害が発生し、復旧が必要になる場合に備え、運用手順としてバックアップ並びにリカバリ計画及び手順を確立し、それに基づき実行すること。
		バックアップデータのリカバリを行う必要があると考えられる場合には、PMDA の判断に従いリカバリ手順に沿って作業すること。
11	【各種データ管理】	定期的に取得が必要な運用データ、各種帳票・レポート類、各システムの設定データ等のデータ管理。
		(1) 必要データの保存と削除 定期的に夜間バッチ処理により生成される結果データ、操作履歴等の蓄積データに関しては、データを定期的に再利用可能な形式で別媒体に保存した後にデータベースから削除を行うこと。
		(2) データ保守 業務アプリケーションに起因する障害復旧に伴い、過去のデータを含め、不整合データの存在が明らかになった場合、不整合データの修正箇所の特定、報告を行い、PMDA と協議の上、修正、削除の実施、確認、記録業務への対応を行うこと。また関連文書検索用紐付けデータのデータベースへの一括登録、更には登

No	名称	内容
		録された紐付けデータに不整合等が判明した場合には、その修復も行うこと。
		(3) データ集計 PMDA の指示により、データベースからの条件指定によるデータ検索、抽出、集計を行うこと。(月 4 回程度)
12	【データベース運用支援】	データベースの性能劣化を防止するため、テーブル再構成やインデックス再構成等の性能劣化防止作業を計画し、PMDA の承認を得た上で定期的に実施すること。
13	【住基ネット関連運用支援】	住基ネットに係るシステムについて、適宜以下について対応すること。 (1) 市町村コードマスタファイルの更新 (2) 画面制御情報の設定 (3) 本人確認端末の追加 (4) 情報提供業務メニュー画面における初期表示の設定変更 (5) 情報提供サーバにおけるユーザパスワード変更に伴う対応 (6) 耐タンパー装置の抜き取り/接続 (7) ハードウェア定期点検(日常点検、定期点検、バックアップ装置のクリーニング) (8) 情報提供サーバ/本人確認端末のアップデート (9) 法定停電等におけるシステム停止/起動 (10) 操作ログ検証のための新救済システムデータの抽出 (11) 障害発生時の復旧作業
14	【拠出金システムへのデータ連携支援】	新救済業務システム稼働(令和6年12月)から付加拠出金システム稼働開始(令和7年3月)までの間における給付システムにおいて支給決定される副作用拠出員及び感染拠出金の支給決定情報データについて示される条件に基づき抽出し、提供すること。(副作用及び感染あわせて最大月 4 回程度、通算 10 回想定) その他、新救済業務システムと拠出金システムとの連携により発生した課題等の問い合わせについて対応すること。
15	【その他】	定期的(概ね年 2 回)に実施される新霞が関ビル電気設備のための停電に対応すること。

保守業務の範囲定義

No	名称	内容
1	【システム設定・操作 － 設定変更】	ハードウェア、OS、ミドルウェア等を正常に稼動させるために設定の変更が必要となる場合には PMDA に提案し、PMDA の了解の下、当該作業を実施すること。
2	【ソフトウェア保守 － ソフトウェア更新】	運用対象システムのソフトウェア資源について、以下の作業を実施する。なお、(3)～(6)に係る、公表されている脆弱性情報を漏れなく把握すること。ソフトウェアの更新作業については、PMDA と協議の上、検証テストや事前のバックアップ（スナップショット取得等）を実施の上で本番環境に反映させること。
		(1) パッチの提供に関する情報及び 脆弱性情報の収集 当システムを構成する全てのソフトウェアについて、ソフトウェアベンダからのパッチ（不具合修正を目的とするパッチ、脆弱性対策を目的とするセキュリティパッチの両方を含む。）の提供情報及び脆弱性に関する情報を継続的に収集すること。
		(2) 脆弱性対応計画の作成 脆弱性情報又はセキュリティパッチの提供に関する情報を入手した場合、当該脆弱性への対応又は当該セキュリティパッチの適用に関する計画を脆弱性対応計画」（案）として取りまとめ、PMDA の承認を得ること。脆弱性対応計画」（案）は、以下の内容を含むこと。 ・対策の必要性 ・対策方法又は対策方法が存在しない場合の一時的な回避方法 ・対策方法又は回避方法が情報システムに与える影響 ・直ちにはパッチ適用できないと判断される場合のリスクと当面の回避策（案） ・対策の実施予定 ・テストの必要性 ・テストの方法 ・テストの実施予定 ・テストの合格基準 ・本番環境への適用手順とスケジュール
		(3) 業務アプリケーションへのパッチの定期適用 業務アプリケーションプログラムへのパッチの適用を定期的に適用する計画を作成し、PMDA の承認の上で適用を実施すること。
		(4) 業務アプリケーションへのパッチの緊急適用 業務アプリケーションプログラムへのパッチを緊急適用する計画を作成し、PMDA の承認の上で適用を実施すること。
		(5) OS・ミドルウェアの不具合修正の適用 特定ミドル保守業者又はその他の機器保守業者から提供される修正版の OS・ミドルウェアの不具合修正資源を適用する計画を作成し、PMDA の承認を得た上で適用を実施すること。
		(6) ウィルスパターンファイルの更新 本システムに導入されているアンチウィルスソフトウェアのうち、パターンファイルの自動更新が行われていないものについては、1 日ごとにウィルスパターンファイル資源を適用すること。

No	名称	内容
3	【ハードウェア保守】	ハードウェア及びファームウェアの不具合、ファームウェア更新等のハードウェア保守に関してサーバ等の保守業者と協力し、分担の役割に応じて対応すること。作業の分担において抜け、漏れが出ないよう充分留意し、最終的な対応は本件受注業者の責任において実施すること。別紙　運用監視・保守方針と役割分担を参照。
4	【不具合修正、軽微な改修】	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、PMDA の指示の下、画面・帳票レイアウトの変更、検索条件及び検索処理の修正、小規模ツールの作成、文書管理システムに関連した文書の保存方法といった軽微なプログラム改修・システム構成の変更を実施すること。必要な設計書の改訂・作成及びプログラム入替え作業も含むものとする。（年間 30 人月程度の作業とする。） なお、ローコード基盤であることを考慮し、改修工数を消費する必要があるのか、あるいは消費する必要があるとして当該改修工数が妥当かについては、都度 PMDA と協議すること。 別途、改修案件が調達された場合、当該受注業者との連携、調整を密にし、当該受注業者による改修作業が円滑に進むよう支援をすること。その際にはソースプログラムのデグレード等が発生しないよう、構成管理に留意すること。 本システムの開発方法に適合させること。

追加改修業務の範囲定義

- 各要件の対応スケジュールについては PMDA 担当と議論の上、計画を立てること。業務への影響度を考慮したうえで、優先度の高い要件から対応していくこと。
- 要件の詳細について PMDA 担当に十分ヒアリングし決定すること。詳細化した要件に対する対応方針を明記した要件確認書を作成し、PMDA 担当の了承を得た上で基本設計作業に着手すること。
- 設計の内容について PMDA 担当に十分ヒアリングし基本設計書を作成すること。基本設計書の内容について、PMDA 担当の了承を得た上で詳細設計及び設定・構成変更作業に着手すること。変更の結果、システム構成図や各種設計書等の既存ドキュメントの修正が必要な場合、該当ドキュメントを修正し PMDA の承認を得ること。
- 改修対象機能のテストのみの実施ではなく、リグレッションテスト含めて実施すること。特にシステム連携機能などに想定外の異常が現れていないことを確認すること。（他の救済部内システムに影響があることを確認した場合、他の救済部内システムも合わせて改修すること。

No	名称	内容
1	【統合解析システム －MedDRA コーディング機能】	現行の MedDRA コーディング作業においては、作業準備として MedDRA ファイルと、「新救済システム」上の業務データを Access、Excel へ取り込む必要がある。取り込んだデータをもとに、支給決定された事例の副作用名について、MedDRA の LLT に一致させる業務を行っている。（副作用名が複数ある場合には分割した上で一致させる、副作用名が LLT に一致しない場合には読み替えの変換作業を実施） 現行は、上記の通り「新救済システム」外にある Access、Excel によるデータ管理・

No	名称	内容
		作成となり非効率となっているため、「新救済システム」上で MedDRA コーディング作業を行える仕組みを開発する。 主要機能として以下機能の開発を想定しており、その他必要な機能がないか要件及び操作性のヒアリングを行い確認しながら進めること。本機能は 2025 年 4 月から利用開始想定のため、2025 年 3 月中にテストを完了し、2025 年 4 月にリリースすること。 ⑴MedDRA バージョン差分抽出機能 ・2 バージョンの MedDRA ファイルを指定して、2 バージョン間の差分を確認できる機能 ⑵MedDRA 自動コーディング機能 ・判定結果の副作用名を、MedDRA の LLT と一致させる機能 （副作用名が複数記載されているものは自動分割、副作用名が一致しないものは読み替えの変換を行った上で LLT を一致させる） ・LLT と一致させた結果を「新救済システム」上の判定結果、原因医薬品、MedDRA ファイル等とあわせて紐づけを行い、MedDRA コーディング及び後続の集計業務に必要な項目を含んだデータとしてシステム上へ登録する機能 ⑶MedDRA 未変換確認機能 ・⑵の MedDRA 自動コーディング機能を使用して変換できなかったデータ、または、まだ変換作業を実施していないデータを確認する機能 ⑷MedDRA 手動コーディング機能 ・⑵の MedDRA 自動コーディング機能を使用して変換できなかったデータ、または、個別に修正する事例のデータについて、ユーザが手動で MedDRA コーディングを行える機能
2	【統合解析システム － 集計業務機能】	現行業務においては、MedDRA コーディングを行ったデータを Access、Excel へ取り込みし、ユーザの手作業で集計作業（データ作成、グラフ作成）を実施し報告用資料を作成している。 現行手作業で作成している、これらの集計作業（データ作成、グラフ作成）を自動行い報告書用の資料作成が可能な機能を開発する。 主要機能として以下機能の開発を想定、その他必要な機能がないかヒアリングにて確認をしながら進めること。本機能は 2025 年 4 月から利用開始想定のため、2025 年 3 月中にテストを完了し、2025 年 4 月にリリースすること。 ⑴報告書用データ出力機能 ・各報告書を作成するために必要な項目を全て含んだデータを出力する機能 ・報告書ごとに定められた集計単位に従って集計した結果のデータを出力する機能

No	名称	内容
		⑵報告書用グラフ出力機能 ・報告書ごとに定められた集計単位に従って集計した結果のグラフを出力する機能
3	【過去ナレッジ検索機能】	現行の業務においては、「新救済システム」外にある Access を経由して救済システム上のデータを取得し、業務上で必要となる情報を取得している。 しかしながら、現行の Access が提供するデータ検索機能では、リレーショナルデータベースの知識を前提としており（必要なデータを検索するため関連するテーブルの結合操作等が必要）、使用率が低く、運用支援への作業依頼にてデータ取得を行う状況となっている。 今後は「新救済システム」上で業務に必要なデータの取得をリレーショナルデータベースの知識を必要とせず操作可能な仕組みを開発する。（Access の利用は廃止） 主要機能として以下機能の開発を想定、その他必要な機能がないかヒアリングにて確認をしながら進めること。 ⑴過去ナレッジ検索機能（主要業務データ検索） ・現行、Access を経由して取得している業務上必要となるデータを取得でき、画面に結果を一覧表示できる機能 ・上記に加え、業務上必要となる追加データについても新たなデータ定義を作成し、検索結果を画面一覧表示できる機能 ・上記で画面表示された結果を Excel 形式で出力できる機能 ⑵過去ナレッジ検索機能（詳細業務データ検索） ・（1）で網羅されていないデータについてユーザが必要に応じて検索、画面一覧表示、Excel 形式で出力できる機能 （システム上の各テーブル結合、各項目の条件指定、表示項目の選択等を画面上で指定でき、過去ナレッジ検索機能（主要業務データ）で定義されたデータ定義では取得が難しいデータに対しても検索を可能とする）
4	【文書管理システム構成変更】	新救済システムは、各サブシステムから出力される帳票や請求における添付書類等は文書管理システム（invoiceAgent）に保存する運用を予定している。文書管理システムを運用するにあたって、業務効率・セキュリティの向上を目指し、以下の要件を満たすよう新救済システムの構成や設定を変更すること。 ■新救済システムの仕様に関する課題 ⑴新救済システムはブラウザを介して操作する構成のため、各サブシステムからダウンロードしたファイルは作業端末に保存される。 ⑵各サブシステムからファイルをダウンロードする際、文書管理システムの格納先フォルダは自動作成されるが、ファイルの保存操作は利用者自身で行う必要がある。 ⑶文書管理システムに保存後のファイルは暗号化されているが、各サブシステムからダウンロードしたファイルは暗号化されていない。

No	名称	内容
		■要件 (1)業務効率 ・ファイルの保存操作を利用者自身で行う必要があることによる業務負荷が懸念される。利用者の業務負荷が最低限となるよう、ファイル保存を自動化する仕組みや補助となる仕組み等を検討し実装すること。 (2)セキュリティ ・ファイルの保存操作を利用者自身で行う必要があるため、操作ミスによる資料紛失リスクが懸念される。資料紛失リスクが最低限となるよう、ファイル保存を自動化する仕組みや補助となる仕組み等を検討し実装すること。 ・各サブシステムからファイルをダウンロードする際、ファイルの格納先が作業端末となることを避け、ファイルサーバーやリモートデスクトップサーバ等の閉鎖環境に格納される構成に変更すること。 ・各サブシステムからファイルをダウンロード後、文書管理システムに格納するまでのファイルは自動的に暗号化される構成に変更すること。

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

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

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

別紙4

システム運用管理基準

2020 年 12 月

独立行政法人　医薬品医療機器総合機構

【資料の見方】

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

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

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

改訂履歴

改定日	改定理由
2018 年 6 月 8 日	初版発行
2018 年 7 月 20 日	情報セキュリティ遵守状況報告内容を追記
2018 年 9 月 10 日	脆弱性管理を追記
2019 年 8 月 15 日	2. システム運用管理業務の概要に「【参考】システム運用管理業務の全体像」を追加 4.5 構成管理　最新情報を PMDA に報告する標準書式を定義 4.9 脆弱性管理　管理状況を報告する PMDA 標準書式を定義
2019 年 12 月 20 日	4.7 バックアップと回復管理　バックアップデータの保管方法を追加
2020 年 12 月 10 日	4.6 運行管理　ログ取得・保存、イベント検知対応の報告を標準化 4.9 脆弱性管理　管理要件を追加 4.10 アクセス管理　アカウント管理要件の追加、アカウント台帳作成と棚卸を標準化項目に追記

1. はじめに

1．1　目的

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

1．2　対象範囲

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

1．3　適用の考え方

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

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

1．4　用語の定義

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

1．5　準拠および関連文書

上位規程　：「情報セキュリティポリシー」

関連文書　：「情報システム管理利用規程」

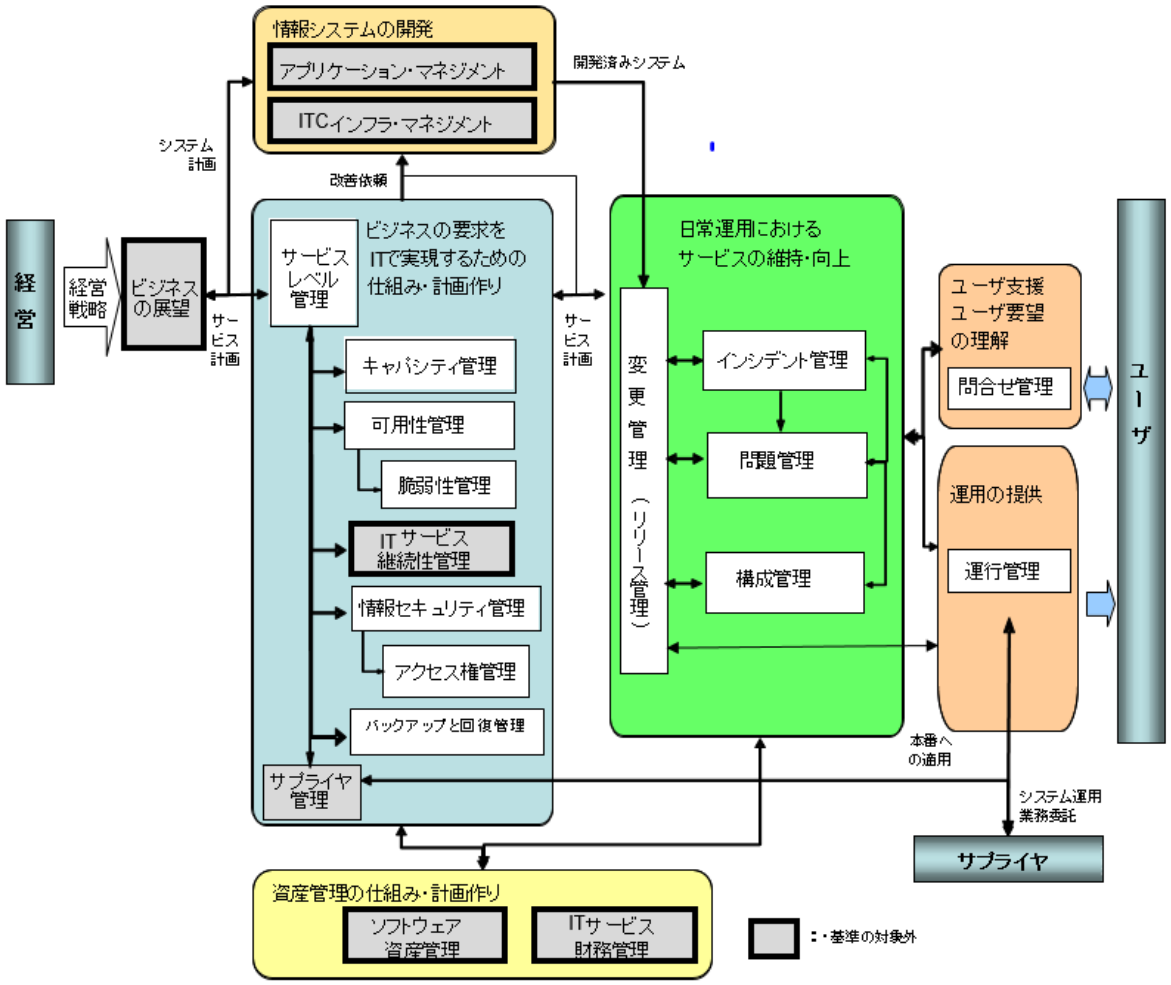
2. システム運用管理業務の概要

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

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

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

【参考】システム運用管理業務の全体像

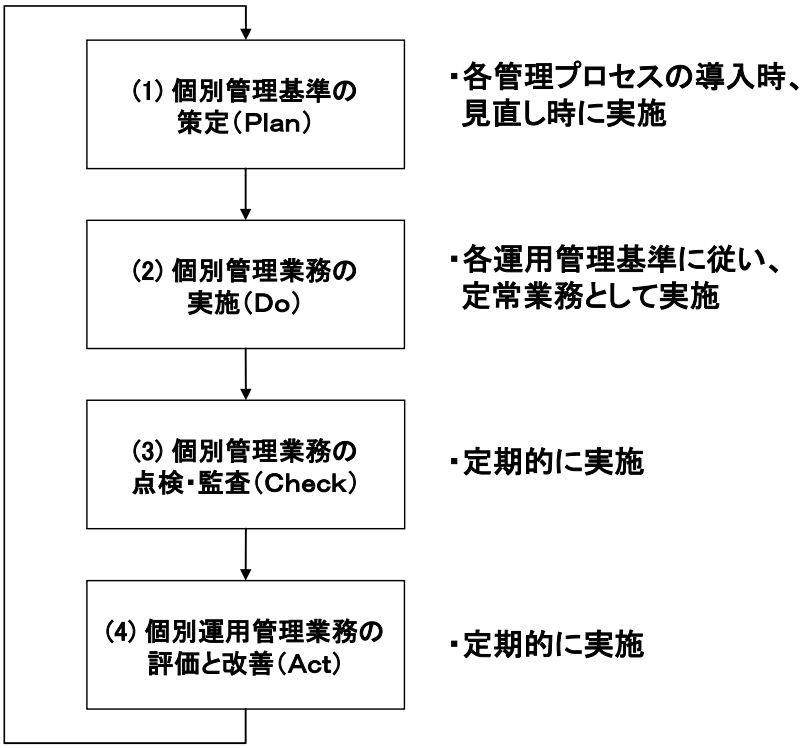


3. 運用管理業務の基本プロセス

（運用管理業務プロセスのPDCAマネジメントサイクル）

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

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



各基本プロセスの概要は、以下のとおりである。

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

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

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

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

4. システム運用管理業務の明確化・標準化

4. 1 問合せ管理

(1) 目的

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

(2) 業務の概要

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

(3) 管理対象

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

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

(4) 業務の管理指標＆標準化

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

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

※報告内容は、各システムの状況に応じて変更しても構わない。

【補足】

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

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

４．２ インシデント管理

(1) 目的

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

(2) 業務の概要

①インシデントの定義

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

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

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

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

②インシデント管理の主な活動

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

インシデント管理のプロセスでは、主に次の活動を実施する。

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

(3) 管理対象

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

(4) 業務の管理指標

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

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

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

(5) 標準化

インシデント管理は、PMDA 標準書式を適用する。

①インシデント発生(判明)時

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

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

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

②定期的(月次)報告時

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

※添付「インシデント一覧」を使用する。

４．３ 問題管理（再発防止策）

(1) 目的

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

(2) 業務の概要

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

- ・問題の傾向分析と課題点の抽出
- ・是正策の検討
- ・是正策の実施

(3) 管理対象

本番システム環境で稼動している全てのシステムの問題を管理対象とする。

(4) 業務の管理指標＆標準化

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

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

※報告内容は、各システムの状況に応じて変更しても構わない。

４．４ 変更管理

(1) 目的

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

(2) 業務の概要

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

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

(3) 管理対象

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

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

(4) 業務の管理指標

変更管理業務を評価するための評価指標として以下を定義する。

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

(5) 標準化

変更管理は、PMDA 標準書式を適用する。

①変更案件発生時

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

※課題管理表の書式は、各情報システムの任意とする。

②変更実施着手時

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

※添付「変更作業申請書（ひな型）」を使用する。

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

認･承認欄の削除は認めない。

※個票は、「単純な定常作業」に関しては使用しなくても良い。

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

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

③定期的(月次)報告時

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

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

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

４．５ 構成管理

(1) 目的

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

(2) 業務の概要

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

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

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

(3) 管理対象

構成管理が対象とする構成情報は以下の通りとする。

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

(4) 業務の管理指標

構成管理業務を評価するための評価指標として以下を定義する。

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

(5) 標準化

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

４．６ 運行管理

(1) 目的

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

(2) 業務の概要

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

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

(3) 管理対象

本番システム環境で稼動している全ての情報システムの運行を管理対象とする。

(4) 業務の管理指標

運行管理業務を評価するための評価指標として以下を定義する。

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

(5) 標準化

〇情報システムの運行状況を報告する（月次）（書式任意）

情報システムの稼働状況に加えて、以下の項目の報告を必須とする。

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

４．７　バックアップと回復管理

(1)　目的

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

(2)　業務の概要

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

日常運用においては、バックアップ取得、バックアップ媒体の保管を行う。

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

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

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

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

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

(3)　管理対象

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

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

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

(4)　バックアップデータの保管方法

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

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

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

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

(6)　業務の管理指標

バックアップと回復管理業務を評価するための評価指標として以下を定義する。

① 当月で計画された定期バックアップの内、バックアップに失敗した件数と理由。

② 当月実施されたリストア件数と内訳（障害対応、調査目的、帳票再作成・出力等）。

③ 当月実施されたリストアの内、リストアに失敗した件数と理由。

（7） 標準化

〇定期的なバックアップが取得されていることを報告する（月次）（書式任意）

〇PMDA では、「リストアの机上訓練」を定期的に実施することを推奨している。

各情報システムにおいては、必要に応じて定期的な訓練実施を行い、結果報告を行う。

４．８ 情報セキュリティ管理

(1) 目的

情報セキュリティ管理は、「情報セキュリティ対策の運用要件」に定める情報セキュリティ対策の運用要件に則り、情報システムのセキュリティを維持・管理し、情報資産を適切に保護することを目的とする。

(2) 業務の概要

情報セキュリティ管理プロセスは、PMDA のリスク管理活動の一環として、ITサービス及びサービスマネジメント活動における全ての情報のセキュリティを、首尾一貫した方針に基づき効果的に管理する。

具体的には、「情報セキュリティ対策の運用要件」に則って、適切にセキュリティ管理策が導入され、維持されていることを確実にするために、情報セキュリティ管理計画の維持・管理を行う。合わせて、情報セキュリティ対策が適切に運用されているかを定期的に点検するとともに、コンプライアンス等の観点からのシステム監査の実施対応をおこなう。

(3) 管理対象

ITサービス及びサービスマネジメント活動における全ての情報セキュリティの管理を対象とする。

(4) 業務の管理指標

情報セキュリティ管理業務を評価するための評価指標として以下を定義する。

① 情報セキュリティ違反・事件・事故の発生件数とその内容
② 発生した情報セキュリティ違反・事件・事故への対策の実施状況
③ 情報セキュリティ監査（内部・外部）及び自己点検で検出された不適合の件数
④ 前回の情報セキュリティ監査及び自己点検で検出された不適合の是正状況

(5) 標準化

○情報セキュリティ遵守状況の報告

・情報セキュリティを遵守していることを定期的(月次)にて報告する
※報告内容の詳細は後述の【補足説明】を参照
・委託先における自己点検を定期的(年 2 回程度)に実施し、点検結果を報告する。
（点検内容は委託先の任意とするが、各情報システムの運用保守業務に携わる要員等が自らの役割に応じて実施すべき対策事項を実際に実施しているか否かを確認するだけではなく、運用保守のプロジェクト体制全体の情報セキュリティ水準を確認する内容とすること。）

【補足説明】

情報セキュリティ遵守状況の報告は、以下の内容を確認し、報告すること

① 情報の目的外利用の禁止
② 情報セキュリティ対策の実施および管理体制（プロジェクト計画書記載内容の遵守）
※委託先において実施するセキュリティ研修や委託先の情報セキュリティポリシー遵守のため取組み内容を含む
※責任者による情報セキュリティの履行状況の確認を含む

③ 体制変更の場合の速やかな報告
④ 体制に記載された者以外が委託業務にアクセスできない（していない）ことの確認
⑤ ※発生した場合は、すぐに検知でき、報告される
⑥ 要員の所属・専門性（資格や研修実績）・実績および国籍に関する情報提供
※変更があれば、その都度情報提供される。
⑦ 秘密保持契約（誓約書）の提出（要員全員が提出）
※委託業務を離れた者の一定期間の機密遵守を含む
※体制変更があった場合の追加提出も含む
⑧ 情報セキュリティインシデントへの対処方法の明確化され、要員に周知されている
⑨ 再委託がある場合は、上記内容を再委託先においても遵守していることが確認されている

４．９ 脆弱性管理

(1) 目的

サーバ装置、端末及び通信回線装置上で利用するソフトウェア（含むファームウェア）やアプリケーションに関連する脆弱性情報の収集とその影響評価に基づく適切な対策を実施するための標準的管理要件を定め、脆弱性によりもたらされる情報セキュリティの脅威について迅速かつ適切に対処することを目的とする。

(2) 業務の概要

脆弱性管理では、システム構成を把握したうえで、管理対象とするソフトウェアのバージョン等の確認から、脆弱性情報の収集、影響評価と対策の要否判定、脆弱性対策計画の策定、脆弱性対策の実施、結果の確認、対策の実施状況のモニタリングまでの一連のプロセスを管理する。

①管理対象ソフトウェアの把握 （管理すべきソフトウェアを特定）

②管理対象ソフトウェアの脆弱性対策の状況確認

②脆弱性情報の収集と識別（当該脆弱性が管理対象ソフトウェアに該当するかの確認）

③影響・リスクの評価と対応要否の判断及び記録

④脆弱性対策計画の策定と承認（変更管理手続きに拠る）

⑤脆弱性対策の検証 （検証環境での稼動確認）

⑥脆弱性対策の実施

⑦脆弱性対策の記録・報告

⑧脆弱性対策の実施状況のモニタリングと継続的改善

(3) 管理の対象

本番システム環境で稼動しているサーバ装置、端末及び通信回線装置上で利用するソフトウェアやアプリケーションに関する全ての脆弱性を管理対象とする。

(4) 業務の管理指標

脆弱性管理業務を評価するための評価指標として以下を定義する。

① 管理対象プロダクツ、バージョンに該当する脆弱性情報件数（通常／緊急）
② 脆弱性対策の評価件数（対策要、対策不要）
③ 対策計画の策定・実施状況（セキュリティパッチ適用、またはその代替策）／予定・実績
・定期報告=脆弱性管理の実施報告
・変更管理＝システム変更作業報告（セキュリティパッチ適用状況報告を含む）
④ 実施可能な脆弱性対策を実施しなかったことによる情報セキュリティインシデントが 1 件も発生しないこと。

(5) 脆弱性管理の要件

脆弱性対策について、以下の管理を行う。

① 対象プロダクト・バージョンの把握

・各情報システムにおいて管理対象とするプロダクトとバージョンを特定するとともに脆弱性情報の収集及びパッチの取得方法を(事前に)整備する。

② 脆弱性情報の収集及び対策の要否判断

・管理対象のプロダクトに係る脆弱性情報の公開状況を定期的に収集する。

・収集した脆弱性情報をもとに影響・緊急度、対策の必要性、情報システムへ与える影響・リスクを考慮し、対策の要否を判断する。

③ 脆弱性対策計画の策定と実施

・対策が必要と判断した場合は、セキュリティパッチの適用計画、または、その代替策(回避方法)の実施計画を策定する。

・対策が情報システムに与える影響について事前検証を行った上、実施する。
対策が情報システムの構成変更を伴う場合は、「4.4 変更管理」に拠るものとする。

・対策計画の策定及び実施状況の管理

(6) 標準化

① 管理状況については PMDA 標準書式を使用する。

・管理対象とするソフトウェアのプロダクトとバージョンについては、各情報システムの設計書等のソフトウェア関連項目を基に、「脆弱性管理対象ソフトウェア一覧」を使用し管理する。

・管理対象とするソフトウェアの脆弱性の有無、対策の要否、対策の実施概要については、「脆弱性対策管理簿」を使用し管理する。

② 定期的(月次)報告

・各情報システムにおける管理対象とするプロダクト・バージョンについて内容に更新があった際は、「脆弱性管理対象ソフトウェア一覧」を使用し速やかに報告する。

・脆弱性対策の要否及び対策の実施状況について、「脆弱性対策管理簿」を使用し、定時(月次)で報告する。

※「脆弱性対策管理簿」の作成にあたっては「脆弱性対策管理簿記載要領」を参照すること。

参考 脆弱性情報収集時の参考 URL 一覧 (「IPA 脆弱性対策の効果的な進め方(実践編)」より)

種別	URL
脆弱性関連情報データベース	■国内 ・JVN (Japan Vulnerability Notes) https://jvn.jp/ ・脆弱性対策情報データベース JVN iPedia https://jvndb.jvn.jp/ ■海外 ・NVD(National Vulnerability Database) https://nvd.nist.gov/ ・Vulnerability Notes Database

	https://www.kb.cert.org/vuls/ ・Metasploit（攻撃情報あり） https://www.metasploit.com/ ・Exploit Database（攻撃情報あり） https://www.exploit-db.com/
ニュースサイト	■国内 ・CNET ニュース：セキュリティ https://japan.cnet.com/news/sec/ ・ITmedia エンタープライズ セキュリティ http://www.itmedia.co.jp/enterprise/subtop/security/index.html ・ITpro セキュリティ https://tech.nikkeibp.co.jp/genre/security/ ■海外 ・ComputerWorld Security （米国中心） https://www.computerworld.com/category/security/ ・The Register Security （英国・欧州中心） https://www.theregister.co.uk/security/
注意喚起サイト	■国内 ・IPA：重要なセキュリティ情報一覧 https://www.ipa.go.jp/security/announce/alert.html ・JPCERT/CC 注意喚起 https://www.jpcert.or.jp/at/2018.html
	・警察庁：警察庁セキュリティポータルサイト https://www.npa.go.jp/cyberpolice/ ■海外 ・米国：US-CERT https://www.us-cert.gov/ncas ・米国：ICS-CERT https://ics-cert.us-cert.gov/
製品ベンダー	■定例アップデート ・マイクロソフト セキュリティ更新プログラム ガイド https://portal.msrc.microsoft.com/ja-jp/security-guidance ・オラクル Critical Patch Update と Security Alerts https://www.oracle.com/technetwork/jp/topics/security/alerts-082677-ja.html

	■クライアント製品など ・Apple セキュリティアップデート https://support.apple.com/ja-jp/HT201222 ・Adobe セキュリティ速報およびセキュリティ情報 https://helpx.adobe.com/jp/security.html ・Mozilla サポートの検索 https://support.mozilla.org/ja/
	■サーバ、ネットワーク製品など ・シスコ - セキュリティアドバイザリ https://www.cisco.com/c/ja_jp/support/docs/csa/psirt-index.html ・HP - サポートホーム https://support.hp.com/jp-ja ・日立 -セキュリティ情報 https://www.hitachi.co.jp/hirt/security/index.html ・富士通 - セキュリティ情報 https://www.fujitsu.com/jp/support/security/ https://www.fujitsu.com/jp/products/software/resources/condition/security/ ・NEC - NEC 製品セキュリティ情報 https://jpn.nec.com/security-info/ ・IBM - IBM Support https://www.ibm.com/support/home/?lnk=ushpv18hcwh1&lnk2=support ・Red Hat - Red Hat Product Errata https://access.redhat.com/errata/#/
	■セキュリティ製品など ・シマンテック -セキュリティアップデート https://www.symantec.com/ja/jp/security_response/securityupdates/list.jsp?fid=security_advisory
	■オープンソースなど ・Apache Foundation https://httpd.apache.org/ (Apache HTTP サーバ) https://tomcat.apache.org/ (Apache Tomcat) https://struts.apache.org/ (Apache Struts) ・ISC (Internet Systems Consortium) https://www.isc.org/downloads/bind/ (BIND) https://www.isc.org/downloads/dhcp/ (DHCP) ・OpenSSL https://www.openssl.org/

4．10 アクセス権管理

(1) 目的

システムを利用するユーザ・アカウントを保護するため、及び、なりすましによる不正ログインの可能性を低減するために、ユーザ・アカウントを役割権限別に分類した上で管理方法を取決めてセキュリティレベルを維持する。

(2) 業務の概要

システムを利用するサーバ OS、ミドルウェア、アプリケーション・ソフトウェア、及びネットワーク機器のアカウントを対象にアクセス権の管理を行う。

(3) 管理対象

本番システム環境での全てのアカウント（社外の取引先等に提供しているアカウントを含む）のアクセス権を管理対象とする。

本番環境	アクセス権管理の対象
システム・ソフトウェア	OS ユーザID
ミドルウェア	DBMSユーザID、ジョブスケジューラ・ユーザID、他
アプリケーション・ソフトウェア	アプリケーション・ユーザID
ネットワーク機器	各ネットワーク機器の管理者用ID

(4) 業務の管理指標

アクセス権管理業務を評価するための評価指標として以下を定義する。

① 期間内に発生したユーザID登録・変更・削除の件数
② 特権（高権限）ユーザID別の貸出し件数と用途
③ アカウントおよびアクセス権の定期棚卸しで、発見された不備項目
④ 不適切／不正なアクセス権限の設定によって発生したインシデントの件数
⑤ アクセス権限の再設定が必要となったインシデントの件数
⑥ 間違ったアクセス権限の設定によって提供不能になったサービスの件数
⑦ 間違ったアクセス権限の設定によって生じた不正アクセスの件数

(5) アカウント管理の要件

・【アカウント（ID）の付与】

①情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む）する。

②識別コードの付与に当たっては、.単一の情報システムにおいて、ある主体に付与した識別コードを別の主体に対して付与することを禁止する

③主体以外の者が識別コード又は主体認証情報を設定する場合に、主体へ安全な方法で主体認証情報を配布する。

④識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認証情報を速やかに変更するよう、促す。

⑤知識による主体認証方式を用いる場合には、他の情報システムで利用している主体認証情報を設定しないよう主体に注意を促す。

⑥情報システムを利用する主体ごとに識別コードを個別に付与する。ただし、判断の下やむ

を得ず共用識別コード（共有 ID）を付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関するルールを定め、そのルールに従って利用者に付与する。

⑤主体認証情報の不正な利用を防止するために、主体が情報システムを利用する必要がなくなった場合には、当該主体の識別コードを無効にする。

・【特権 ID と使用者の限定】

①使用者限定の保証

・パスワードの堅牢性

できだけ長い桁数、推測困難かつ記憶が容易となる工夫

・パスワードの厳正管理

業務で使用する必要がある者しか知ることができないようにする

パスワード情報へのアクセス制限

ID 使用者の離任時はパスワード変更を必須

②利用時の承認と記録

・特権 ID を利用して作業を行った結果の記録 （特権 ID 使用管理簿の記載）

・利用状況のモニタリング

サーバのログイン・ログアウトログの出力リストと特権 ID 使用管理簿の作業実績に記載されている日時を照合し、記載されている日時から逸脱する時間帯のログデータがないことをチェック

※工数の許す範囲で、重要サーバに絞り、無作為に抽出した数件のログインに該当する作業のチェック等工夫する

(6) 標準化

・全てのアカウント（ID）について、以下の管理を行う。

①アカウント（ID）管理台帳の作成

ID管理台帳を基に ID の新規・変更・削減の状況について、定期(月次)報告する。

②定期(月次)報告

ID管理台帳を基に ID の新規・変更・削減の状況について、定期(月次)報告する。

③ID棚卸し

全てのIDの棚卸しを以下の手順を参考にし、定期的（最低１回／年）に実施し、報告を行う。

（棚卸し手順）

a. 登録 ID 抽出リスト出力
b. ID 管理台帳突合
c. 棚卸しリスト作成
d. ID 使用者の確認、権限の妥当性の検証
e. 不要 ID(初期登録（ビルドイン）ID を含む）削除と不適切権限の修正
f. ID 管理台帳更新
g. 棚卸実施報告書の作成

※アカウント（ID）管理用資料は、「参考資料_ID 管理用各書式ひな型」を参考に各情報システムにおいて適宜定める。

・特権IDについて、以下の管理を行う。

①特権ID台帳の作成

※添付「特権ID管理台帳」を使用する。

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

※監査等にて提示要求があった場合は、速やかに提示できるよう保管する

②特権ID(システムID)使用管理簿の作成(またはログ抽出)

※添付「特権 ID 使用管理簿」を使用する。各情報システムの状況等によって、一部改修して使用しても構わない。ただし、項目の削除は認めない。

※ログイン・ログアウトのログ(または画面コピー)を必ず保管(または添付)し、監査等にて提示要求があった場合は、速やかに提示できるよう保管する

③定期(月次)報告

特権ID(システムID)台帳ならびに特権ID(システムID)使用状況を、定期(月次)報告する。
(ログまたは画面コピーは、月次報告不要)

④特権ID棚卸し

特権IDの棚卸しを定期的(年 2 回程度)に実施し、報告を行う。(報告書式任意)

棚卸し点検内容は以下の通り

〇台帳は、本当に使用する者を登録しているか?(体制図と一致しているか?)

・体制から外れた者が削除されずに残っていないか?

・使用予定がない者が登録されていないか?

〇台帳と使用管理簿の相関は一致しているか?

〇使用管理簿とログ(または画面コピー)保管の相関は一致しているか?

4.11 キャパシティ管理

(1) 目的

キャパシティ管理の目的は、ビジネスが必要とするときに、必要なキャパシティを適正なコストで提供することである。 すなわち、

① ビジネスの需要に対する供給

ビジネスの変化に合わせて、ITサービスの対応にもスピードが要求される。 キャパシティ管理は、現在から将来にわたるビジネス需要・要件に合わせて、ITインフラストラクチャーのキャパシティを最大限に活用できるようにすることを目的とする。

② キャパシティに対するコスト

一方、必要以上のキャパシティを確保すると購入や運用のための費用が膨らみ、ビジネスの観点からコストを正当化できない。 キャパシティを最適化し、費用対効果が高いITサービスを提供することもキャパシティ管理の目的である

(2) 業務の概要

このプロセスは、次の3つのサブプロセスから構成される。

① ビジネスキャパシティ管理

ITサービスに対する将来のビジネス需要・要件を収集・検討し、それによって、ITサービスのキャパシティを確実に実装させるための計画の立案、予算化、構築がタイムリーに実施されるようにする。

② サービスキャパシティ管理

実際のサービスの利用と稼働のパターン、山と谷を理解して、運用中のITサービスのパフォーマンスを監視し、それによって、SLAの目標値を達成し、ITサービスを要求どおりに機能させる。

③ コンポーネントキャパシティ管理

ITインフラストラクチャーの個々のコンポーネントのパフォーマンスとキャパシティ、使用状況を監視し、それによって、SLAの目標値を達成・維持するために、コンポーネントの利用を最適化する。

(3) 管理対象

本基準の適用システムにおけるハードウェア、ソフトウェア、ネットワーク、アプリケーション、及び人的リソースを対象とする。

(4) 業務の管理指標

キャパシティ管理業務を評価するための評価指標として以下を定義する。

① CPU、ディスク、メモリ、ネットワーク容量などの閾値に対する需要の割合
② ITサービスのパフォーマンス不足に起因するSLA違反やインシデントの発生件数
③ ITコンポーネントのパフォーマンス不足に起因するSLA違反やインシデントの発生件数
④ 正規の購入計画に含まれていなかった、パフォーマンスの問題解決のために急きょ行った購入の数又は金額

4．12 可用性管理

(1) 目的

可用性管理の目的は、ビジネス部門に対して、費用対効果が高いITサービスを持続して提供することであり、そのためにITインフラストラクチャーを整備し、それをサポートするITサービス部門の能力を最適化させる。

(2) 業務の概要

可用性管理の活動は大きく、1）可用性要件の把握、2）可用性の設計、及び3）可用性の改善活動の3つに分けられる。

具体的には、以下の可用性管理の3要素の目標値を設定し、設定した可用性のレベルを達成・維持・向上させることである。

① 可用性

可用性とは、ITサービスが必要なときに使用できる割合のことで、一般的には稼働率という指標を用いて表される。

稼働率（%）＝（サービス提供時間－停止時間）÷サービス提供時間

② 信頼性

提供されるITサービスにおける、不具合の発生しにくさ／故障しずらさを表す。
平均故障間隔＝（使用可能な時間－総停止時間）÷（サービス中断の回数－1）

③ 保守性

ITサービスが停止又は品質低下した際に、いかに早く復旧できるかを示す指標。
平均修理時間＝修理時間の合計÷サービス中断の回数

可用性について極めて重要なことは、ユーザの求めるシステムの可用性レベルをどのように達成するかについて、システム設計時に真剣に検討し、システム構築時に実現し、システムの運用において継続的に改善することである。

(3) 管理対象

本基準の適用システムにおけるハードウェア、ソフトウェア、ネットワーク、及びアプリケーションを対象とする。

(4) 業務の管理指標

可用性管理業務を評価するための評価指標として以下を定義する。

① 可用性の割合
② 平均故障間隔
③ 平均修理時間
④ サービスの中断回数
⑤ 定期的なリスク分析、及びレビューの完了の件数

４．１３　サービスレベル管理

(1)　目的

ユーザニーズを満足する適正なサービスレベルおよび管理指標を設定し、これを実績管理することにより質の高いサービスの提供を図る。

(2)　業務の概要

サービスレベルおよび各個別管理業務での管理指標の実績データを定期的に把握し、サービスレベル指標と実績の差異や傾向を継続的に分析することにより、改善策を立案し実施する。

(3)　管理対象

IT 部門が提供する全ての IT サービスに関するサービスレベルおよび各個別管理業務での管理指標を管理対象とする。

(4)　業務の管理指標

サービスレベル管理業務を評価するための評価指標として以下を定義する。

①「サービスレベル合意書」の各サービスレベル項目の達成率

②各個別管理業務での管理指標の達成率

(5)　標準化

サービスレベル管理業務を定期的(月次)に報告する。

①「サービスレベル合意書」の各サービスレベル項目の達成率

②各個別管理業務での管理指標の達成率

以上

別紙5　情報セキュリティ対策の運用要件

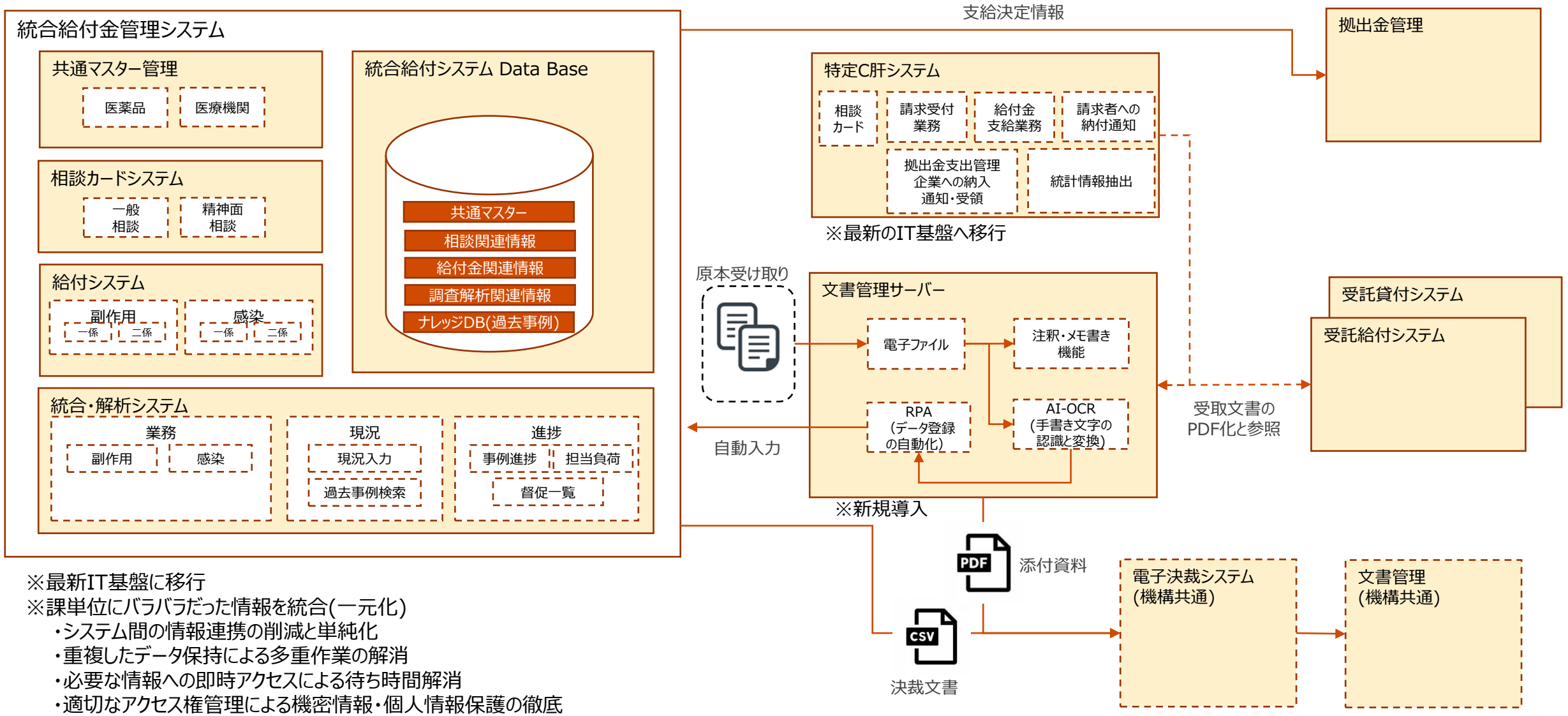
情報システムの運用・保守の業務遂行にあたっては、調達・構築時に決定した情報セキュリティ要件が適切に運用されるように、人的な運用体制を整備するとともに、機器等のパラメータが正しく設定されていることの定期的な確認、運用・保守に係る作業記録の管理等を確実に実施すること。

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

新システムの構成（オンライン化含まず）

別紙6

○現行の給付システム、統合・解析システム、相談カードシステムを対象に、稼働プラットフォームの再構築、ＤＢ統合、機能追加を実施。
　併せて、特定C肝システムを対象に稼働プラットフォームの再構築を実施。



別紙7 ハードウェア一覧 （詳細構成は資料閲覧時にシステム設計書を確認すること）

システムコード	ハードウェア種別	製造元（ベンダー名）	ハードウェア		物理・仮想区分
			機器名称	システムモデル（型番・型式）	
HI-000	SVR	DELL	文書管理DBサーバ(本番)	PowerEdge R750ラック	物理
HI-000	SVR	DELL	文書管理DBサーバ(待機)	PowerEdge R750ラック	物理
HI-000	SVR	–	ライフサイクル管理サーバ	–	仮想
HI-000	SVR	–	ローコード開発基盤サーバ(開発機)	–	仮想
HI-000	SVR	–	ローコード開発基盤サーバ(検証機)	–	仮想
HI-000	SVR	–	ローコード開発基盤サーバ(本番機)	–	仮想
HI-000	SVR	–	文書管理サーバ	–	仮想
HI-000	SVR	–	バックアップ管理サーバ	–	仮想
HI-000	SVR	–	ログ管理サーバ	–	仮想
HI-000	SVR	–	運用管理サーバ	–	仮想

別紙7 ソフトウェア一覧 （詳細構成は資料閲覧時にシステム設計書を確認すること）

システムコード	製造元（ベンダー名）	ソフトウェア		
		ソフトウェア名称	エディション	バージョン
HI-000	Microsoft	Windows Server	Standard	2022
HI-000		Windows Server	Datacenter	2022
HI-000		SQL Server	Standerd	2022
HI-000			Express Edition	2019
HI-000		Microsoft Internet Information Services(IIS)	–	10.0.20348.1
HI-000		Microsoft .NET Framework	–	4.8
HI-000		Microsoft Build Tools	–	2015
HI-000		.NET Core	–	2.1
HI-000		Microsoft Visual C++ 2015 Redistributable Update 3	–	2015
HI-000		OpenSSL	–	3.1.0
HI-000	Oracle	Oracle Database	Standard Edition	19c
HI-000		OpenJDK	–	uild 11.0.17+8)
HI-000	PostgreSQL	PostgreSQL	–	–
HI-000	Apache	Apache Tomcat	–	8.5.84
HI-000	ゾーホージャパン	Op Manager	Professional Edition	12.7.198
HI-000	Arcserve	Arcserve UDP エージェント	–	9.0.6034
HI-000		Arcserve UDP コンソール	–	9.0.6034
HI-000		Arcserve UDP 復旧ポイントサーバ（RPS）	–	9.x
HI-000	infosense	Logstorage コンソール	–	9.1.0
HI-000		Logstorage LogGate	–	9.1.0
HI-000		Logstorage Agent ※ログ収集機能	–	9.1.0
HI-000		Logstorage SecureBatchTransfer（SBT） ※ログ収集機能	–	9.1.0
HI-000	ウィングアーク1ST	invoiceAgent 文書管理	rise（オンプレミス版）	10.9.1.2
HI-000	Outsystems	Outsystems	Standard Edition	11.27
HI-000	Trend Micro	Trend Micro Deep Security Agent ウイルス対策	–	20.0

別紙7 主なソフトウェア構成 （詳細構成は資料閲覧時にシステム設計書を確認すること）

	リモートデスクトップサーバ	DB	開発言語	フレームワーク
給付システム	Windows Server Datacenter 2022	SQL Server Standerd 2022	Outsystems 11.27(Standard Edition)	-
統合解析システム	Windows Server Datacenter 2022	SQL Server Standerd 2022	Outsystems 11.27(Standard Edition)	-
拠出金システム	Windows Server Datacenter 2022	SQL Server Standerd 2022	Outsystems 11.27(Standard Edition)	-

別紙８

資料閲覧について

1. 閲覧対象物

   新健康被害救済業務システムに係る関連資料

2. 閲覧場所

   独立行政法人 医薬品医療機器総合機構内

3. 閲覧期間

   令和６年 12 月４日（水）から令和６年 12 月 13 日（金）までの平日（10:00～17:00）

4. 閲覧上の注意

   (1) 閲覧に際しては、5.閲覧連絡先に電話にて連絡し、社名・連絡先・人数等を登録すること。なお、3.閲覧期間の後半は閲覧場所を確保できなくなる場合があるので、早めに閲覧希望日時を登録すること。

   (2) 閲覧前に別紙様式に基づき秘密保持誓約書を作成し、捺印の上総合機構に提出すること。

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

   (4) 閲覧時に個々の内容に関する質問に応じることはできない。

5. 閲覧連絡先

   独立行政法人　医薬品医療機器総合機構　健康被害救済部

   企画管理課　柴垣

   電話：03（3506）9460

別紙様式

独立行政法人医薬品医療機器総合機構　御中

秘密保持誓約書

貴機構における一般競争入札広告（新健康被害救済業務システムに係る運用支援業務（以下「本件業務」という。）について、＿＿＿＿＿＿＿＿＿＿＿＿＿＿（以下「弊社」という。）が応札するため、現行システムを参照するにあたり、次の事項を遵守することを誓約いたします。

記

１．弊社は、媒体及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、本件業務応札のため必要な者を除く第三者に対して開示しません。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) 弊社が正当な権利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付けられたもの

２．弊社は、本件業務応札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。

３．弊社は、本件秘密情報を本件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。

４．弊社は、本件秘密情報を複写または複製いたしません。

５．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、貴機構に対して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。

６．本誓約書は、本件業務終了後も本件秘密情報が機密性を失う日まで有効に存続することを確認します。

以上

年　　月　　日　　部長印

住　　所

社　　名

部 署 名

担当者氏名

別紙様式

独立行政法人医薬品医療機器総合機構　御中

秘密保持誓約書

貴機構における一般競争入札広告（新健康被害救済業務システムに係る運用支援業務（以下「本件業務」という。）について、＿＿＿＿＿＿＿＿＿＿＿＿＿＿（以下「弊社」という。）が応札するため、現行システムを参照するにあたり、次の事項を遵守することを誓約いたします。

記

１．弊社は、媒体及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、本件業務応札のため必要な者を除く第三者に対して開示しません。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) 弊社が正当な権利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付けられたもの

２．弊社は、本件業務応札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。

３．弊社は、本件秘密情報を本件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。

４．弊社は、本件秘密情報を複写または複製いたしません。

５．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、貴機構に対して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。

６．本誓約書は、本件業務終了後も本件秘密情報が機密性を失う日まで有効に存続することを確認します。

以上

年　　月　　日　　部長印

住　　所

社　　名

部 署 名

担当者氏名