ICMRA ウェブサイトの運用支援業務
調達仕様書

平成 31 年 2 月

独立行政法人　医薬品医療機器総合機構

目次

１　調達案件の概要に関する事項

（１）　調達件名

ICMRA ウェブサイトの運用支援業務

（２）　調達の背景

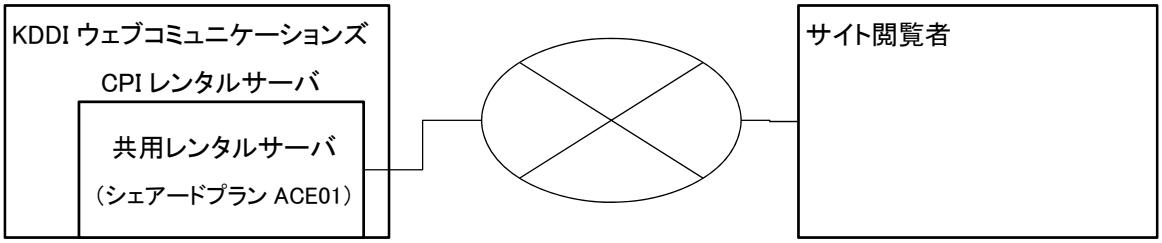
独立行政法人医薬品医療機器総合機構（以下「PMDA」という。）では、International Coalition of Medicines Regulatory Authorities （以下「ICMRA」という。）ウェブサイト（http://www.icmra.info/）の運用を行っている。運用業務として必要なシステム監視、ユーザー管理、保守管理、インシデント発生時対応等を行うには、専門的な知識及び技術が必要であるため、運営支援業務を外部委託したい。

（３）　目的及び期待する効果

本調達は、ICMRA ウェブサイト（以下「本システム」という。）の円滑な運用に資するため、関連する業務を運用支援業務として外部委託することを目的とする。

（４）　業務・情報システムの概要

ICMRA ウェブサイトは、KDDI ウェブコミュニケーションズの共用レンタルサーバ（シェアードプラン ACE01）（以下「ACE01」という。）で稼働するウェブサイト。ACE01 が提供する CMS 機能を利用してサイトコンテンツの作成、リリースを行っている。



（５）　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、必要に応じて協議の上、見直すこととする。

（６）　契約期間及び作業スケジュール

運用業務の対象期間は、2019 年 4 月 1 日から 2021 年 3 月 31 日を予定している。

ア　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。

イ　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、調達の方式等に関する事項

関連する調達案件の調達単位、調達の方式、実施時期等は次の表の通りである。

表　２.１　関連する調達案件の調達単位、調達の方式、実施時期等（既存契約）

項番	調達案件名	調達の方式	実施時期	事業者名	役割	補足
1	ICMRA ウェブサイトのドメイン更新	随意契約	2019 年 1 月 22 日から 2020 年 1 月 21 日	GMO インターネット株式会社	ドメイン名使用権 DNS サービス提供	

表　２.２　関連する調達案件の調達単位、調達の方式、実施時期等（契約予定）

項番	調達案件名	調達の方式	実施時期	役割	補足
1	ICMRA ウェブサイトのレンタルサーバ	随意契約	2019 年 4 月 1 日から 2020 年 3 月 31 日	レンタルサーバ（シェアードプラン ACE01）の提供	
2	ICMRA ウェブサイトのレンタルサーバ	随意契約	2020 年 4 月 1 日から 2021 年 3 月 31 日	レンタルサーバ（シェアードプラン ACE01）の提供	
3	ICMRA ウェブサイトのドメイン更新	随意契約	2020 年 1 月 22 日から 2021 年 1 月 21 日	GMO インターネット株式会社	ドメイン名使用権 DNS サービス提供
4	ICMRA ウェブサイトのドメイン更新	随意契約	2021 年 1 月 22 日から 2022 年 1 月 21 日	GMO インターネット株式会社	ドメイン名使用権 DNS サービス提供

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 作業の概要

ア レンタルサーバの運用支援、保守

ア－1 KDDI ウェブコミュニケーションズ（以下「レンタルサーバ事業者」という。）がレンタルサーバを運用・保守する。

ア－2 レンタルサーバが提供するサービスを活用してウェブサイトを運用・保守する。

ア－3 レンタルサーバが提供するサービスに問題や確認事項がある場合は、受託者がレンタルサーバ事業者への問い合わせ、折衝、調整などを行うこと。

イ ウェブサイトのセキュリティ維持

以下のセキュリティ維持対応を行うこと。

イ－1 HTML ファイル 30 ページ分の改ざん検知対応

イ－2 CMS（Drupal）のセキュリティ更新プログラム（新バージョン）の適用

イ－3 PHP のバージョンアップに伴う設定変更（PHP のバージョンアップ作業はレンタルサーバ事業者が行う）

イ－4 監査対応（９（２）エ参照）

ウ 更新されたコンテンツの本番サイトへのリリース

ウ－1 PMDA がテストサイトで作成・更新したコンテンツの本番サイトへのリリース作業

ウ－2 更新頻度は 1 回/月、作業工数は 4 人日/年程度の想定とする。

エ コンテンツの作成・改修/問い合わせ対応

エ－1 コンテンツ作成・改修、その他に関する問い合わせ対応や技術支援

エ－2 作業工数は 10 人日/年程度の想定とする。

② 準備作業の内容

ア 運用準備作業

受託者は、2019 年 4 月 1 日（予定）の運用業務の開始までに、本情報システムの円滑な運用業務の実施に必要な準備作業として、運用業務に必要な什器等の準備、回線引込等を行うこと。

イ 実施計画書の作成

受託者は、2019 年 4 月 1 日（予定）の運用業務の開始までに、ＰＭＤＡの指示に基づき体制図、作業内容、作業体制、作業分担、マススケジュール、文書管理要領、変更管理要領等を記載した実施計画書及び「９ （１）情報セキュリティ対策の実施」に記載している要件を満足する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。

③　運用に係る作業の内容

ア　定常時対応

ア－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（システム監視、システム設定・操作、ヘルプデスク業務、ユーザー管理、サービスレベル管理、バックアップ／リカバリ等）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。

ア－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　（作用内容、工数等）

C)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)

D)インシデント管理状況（別紙４参照）

E)問題管理状況(別紙４参照)

F)変更管理状況（別紙４参照）

G)バックアップ取得状況(別紙４参照)

H)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）

I)脆弱性管理（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)サービスレベル達成状況（別紙４参照）

L)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）

M)教育･訓練状況（引き継ぎ時のみ）

ア－3　受託者は、月間の運用実績を評価し、達成状況がＳＬＡ要求水準を満たさ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。

④　保守に係る作業の内容

ア　定常時対応

ア－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）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。

ア－2　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。）について月次で保守作業報告書を取りまとめること。

⑤　インシデント発生時の対応

ア　受託者は、インシデントについて、発生日、内容、対応状況等と記録・整理すること。

イ　受託者は、インシデント発生時の１次切り分け業務（検知、発生箇所の特定及び運用・保守に関係する事業者との連携による原因調査）を速やかに行うこと。

ウ　受託者は、情報システムの障害等インシデント発生時（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、インシデント発生時運用業務（検知、障害発生箇所及び原因調査、応急措置、復旧確認、報告等）を行うこと。なお、インシデントには、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、インシデント発生対応を実施のこと。

エ　受託者は、情報システムのインシデント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。

⑥　作業報告

ア　作業実績の報告

受注者は、本業務で実施の作業内容について、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。

⑦　引継ぎ

ア　現行運用事業者からの引継ぎ

受託者は、現行運用事業者から 2019 年 2 月 1 日以降に運用に必要な事項の引継ぎとして、サービスデスクの引継、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。

イ　次期運用事業者への引継ぎ

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）　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	
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） ・情報セキュリティ管理計画書（「９　（１）情報セキュリティ対策の実施」に記載している要件を満足する）	2019 年 4 月 1 日（予定）の運用業務の開始まで	要員名簿及び運用における体制図は、本業務実施者（以下「要員」という。）の作業責任者、窓口及び体制図等が変更になった場合には適宜修正を行い、PMDA の承認を得ること。
3	運用	・システム運用マニュアル(注２) ・システム関連ドキュメント ・プログラム・ツール等	2021 年 3 月 31 日	
4	その他	・月例報告資料 ・打合せ資料 ・議事録 ・障害等作業記録 ・運用支援報告書	2021 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

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 2021 年 3 月 31 日までに納品すること。なお、納入成果物については、以下の条件を満たすこと。

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

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

ウ 外部電磁的記録媒体に保存する形式は MicrosoftWord２０１３、同 Excel２０１３、同 PowerPoint２０１３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。

エ 外部電磁的記録媒体は、２部納品すること。

オ 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。

カ 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。

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

ク 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。

ケ 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。

コ 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　国際部

ただし、ＰＭＤＡが納品場所を別途指示する場合はこの限りではない。

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。

〇別紙３　業務要件

〇別紙４　システム運用管理基準

〇別紙５　情報セキュリティ対策の運用要件

〇閲覧資料　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、ＰＭＤＡ側やその他関連事業者を含めた全体の体制・役割を示した上で、プロジェクトの推進体制及び本件受託者に求める作業実施体制をＰＭＤＡと協議の上定めること。また、受託者の情報セキュリティ対策の管理体制については、作業実施体制とは別に作成すること。

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

（２）　作業要員に求める資格等の要件

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

① Web ページ制作技術、及び CMS（※）に関する専門的な知識を有していること。

② Web ページ制作技術、及び CMS（※）に関して取扱い経験及び専門的な技術知識を有し、現場担当者に対して適切な応答速度で、有効な助言、指示を与える者を配置

すること。

③ PMDA にて ICMRA ウェブサイトの設計書等を閲覧し、内容を十分理解していること。

※Drupal 固有の専門的な取扱経験及び知識は問わないが、資料を参照するなどして 1 週間程度で問い合わせ対応ができるスキルを有していること。なお、緊急を要する作業（脆弱性対応のための Drupal のバージョンアップ作業）は運用手順を参照して実施することができる。

（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 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。

⑤ 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。

⑥ 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 情報セキュリティポリシー

イ 独立行政法人 医薬品医療機器総合機構 情報システム管理利用規程

ウ 独立行政法人 医薬品医療機器総合機構 個人情報管理規程

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情報セキュリティポリシー」は非公開であるが、「政府機関等の情報セキュリティ対策のための統一基準（最新版）」に準拠しているので、必要に応じ参照すること。「ＰＭＤＡ情報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）　瑕疵担保責任

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瑕疵の疑いが生じた場合であって、PMDA が必要と認めた場合は、受託者は速やかに瑕疵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瑕疵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、瑕疵担保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。瑕疵担保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、瑕疵担保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（２）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（日本工業標準）のいずれかを取得していること。

③ プライバシーマーク付与認定を取得していること。

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

（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。

ア ＰＭＤＡから提供する情報の目的外利用を禁止すること。

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

ウ 受託者の資本関係・役員等の情報、本業務の実施場所、本業務従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供を行うこと。具体的な情報提供内容についてはＰＭＤＡと協議の上、決定するものとす

る。

エ　情報セキュリティインシデントへの対処方法が確立されていること。

オ　情報セキュリティ対策その他の契約の履行状況を定期的に確認し、ＰＭＤＡへ報告すること。

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

キ　ＰＭＤＡが求めた場合に、速やかに情報セキュリティ監査を受入れること。

ク　本調達の役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるように情報セキュリティ管理計画書に記載された措置の実施を担保すること。

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

コ　ＰＭＤＡから受領した要保護情報が不要になった場合は、これを確実に返却、又は抹消し、書面にて報告すること。

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

（２）　情報セキュリティ監査の実施

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

イ　受託者は自ら実施した外部監査についてもＰＭＤＡへ報告すること。

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

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

オ　受託者は、指摘や進捗等把握のための資料提出依頼等があった場合は、ＰＭＤＡと協議の上、内容に沿って適切な対応を行うこと。

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

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。

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

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、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「８（２）入札制限」の要件を満たすこと。

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

⑥ 再委託先において、本調達仕様書に定める事項に関する義務違反、義務を怠った場合には、受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。

⑦ 再委託における情報セキュリティ要件については以下のとおり。

・　再委託先が「９（１）情報セキュリティ対策の実施」の要件を満たすこと

・　ＰＭＤＡから提供する情報の目的外利用を禁止すること。

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

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

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

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

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

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

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

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

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

⑧ 上記①～⑦について再委託先が、さらに再委託を行う場合も同様とする。

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）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」

（２）事業者が閲覧できる資料一覧

閲覧資料１　独立行政法人 医薬品医療機器総合機構　情報セキュリティポリシー
閲覧資料２　ＰＭＤＡ情報セキュリティインシデント対処手順書
閲覧資料３　セキュリティ管理要件書(ひな型)
閲覧資料４　設計書
閲覧資料５　2018 年度月例報告書

これら資料は、入札説明会に参加した事業者のうち、ＰＭＤＡに「秘密保持等に関する誓約書」を提出した事業者へ開示する。

また閲覧資料 2～5 の資料に関しては、ＰＭＤＡに「秘密保持等に関する誓約書」を提出した事業者から申出があれば、提供する。

１３ 窓口連絡先

独立行政法人　医薬品医療機器総合機構　国際部国際規制情報調整課

E-mail：ICMRA_website[at]pmda.go.jp

電話：03 (3506) 9456

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
問い合わせ及び依頼事項への一次回答	一次回答の応答時間	応答時刻－問い合わせ受付時刻＜1 営業日の件数／問い合わせ件数	%	100%	問い合わせ一覧表への受付と応答日時の記録	毎月
セキュリティ対策	バージョンアップの対応期限	作業開始時に PMDA と合意した期限までに対応を完了した件数／CMS(Drupal)及びPHPのバージョンアップを依頼した件数	%	100%	問い合わせ一覧表への受付と対応完了日時の記録	毎月
	改ざんの初動対応開始	改ざんを把握（改ざん検知メールの参照、PMDAからの電話受付など）から 15 分以内に調査及び報告の初動対応を行った件数／改ざんの件数	%	100%	障害報告書への改ざん発生と初動対応開始日時の記録	毎月

【別紙2】

作業スケジュール

'2018年 7月 2日

No	セキュリティ対策	実施区分	2019年 3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	2020年 1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	2021年 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	前業者からの引継ぎ	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の承認を受けた後、前業者からの引継ぎを行う。
1-3	月次報告	実施 ◎		▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	原則、翌月第5営業日までに提出
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デントを含む）	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	▲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を翌月第3金曜の2営業日前までに提出
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	▲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を翌月第3金曜の2営業日前までに提出
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	▲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を翌月第3金曜の2営業日前までに提出
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	▲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）。1-3 月次報告に含める。
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	▲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。コンテンツ更新のログ確認を含む。1-3 月次報告に含める。
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	▲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。1-3 月次報告に含める。 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	特権ID検証(棚卸し)	実施 ◎	準備	実施	▲報告																					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、前業者の特権ID及び接続許可IPアドレスの剥奪と後任業者への付与及びパスワード変更の確認
点検																												
4-1	情報システム開発・運用資料確認	実施 ○																							準備	実施	▲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。
内部監査																												
5-1	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											準備		受査					⇒H29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																												
6-1	厚労省・情報セキュリティ監査	支援 △							監査支援												監査支援							
6-2	調達による第3者情報セキュリティ監査	支援 △								監査支援												監査支援						

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	2019 年 4 月 1 日 ～2021 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	受託者の役割
1	【レンタルサーバ運用】	KDDI ウェブコミュニケーションズがレンタルサーバ及び付帯サービス機能を運用する。	問い合わせ、折衝、調整
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収集・確認し、月次で報告すること。	実施
3	【システム監視 – 情報セキュリティ監視】	改ざん検知メールの監視し、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。 セキュリティログを取得･確認し、月次で報告すること。	実施
4	【システム設定・操作 – ジョブ管理】	月次で定期バックアップが正常に取得されていることを確認すること。	実施
6	【ヘルプデスク業務 – 問い合わせ対応】	以下の問い合わせ対応等を実施すること。また、問合せと対応の内容は記録し報告すること。 ・コンテンツ作成・改修に関する技術支援 ・Drupal の操作方法に関する技術支援 ・障害及び情報セキュリティインシデントの調査依頼 ・情報システム監査に関する実態調査 作業工数は 10 人日/年程度の想定とする。	実施
7	【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) Drupal の他、システムを保守・運用に必要な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。	実施
8	【サービスレベル	別紙1 「SLA（Service Level Agreement）項目」参照	実施

No	名称	内容	受託者の役割
	管理】	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。	
9	【バックアップ/リカバリ】	日次の自動バックアップの他、コンテンツ変更時や PMDA から依頼があった場合など必要に応じてマニュアルでバックアップを取得し、不具合があった場合にリカバリを行うこと。但し、コンテンツ編集の最中に必要なバックアップは PMDA が適宜行うものとする。	実施
		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。	実施
10	【その他】	運用・保守業務で使用しているドキュメント（実施計画書、運用マニュアル等）を管理すること。また修正・改定の必要がある場合には、PMDA のレビューを受けて修正・改定を実施すること。	実施

保守業務の範囲定義

No	名称	内容	受託者の役割
1	【レンタルサーバ保守】	KDDIウェブコミュニケーションズがレンタルサーバ及び付帯サービス機能を保守する。	問い合わせ、折衝、調整
2	【ウェブサイト保守】	(1)ウェブサイト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)CMS(Drupal)を正常に運用す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。 (3)PMDA からの依頼に基づき、PMDA がテストサイトで作成・更新したコンテンツを本番サイトへのリリースすること。更新頻度は 1 回/月、作業工数は 4 人日/年程度の想定とする。	実施
3	【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。ソフトウェアの更新作業については、PMDA と協議の上、検証テストを実施の上で本番環境に反映させること。	実施
		(1) Drupal のセキュリティパッチの提供に関する情報、PHP のバージョンアップに関する情報及び脆弱性情報の収集。	実施
		(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、セキュリティパッチの適用に関してリスクが懸念される場合、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	支援

No	名称	内容	受託者の役割
		・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) 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。	実施
4	【コンテンツの作成・改修】	PMDA が作成･改修するために必要な技術支援を行うこと。 必要に応じて Drupal の設定変更、テンプレートの追加などを行うこと。	支援

別紙4

システム運用管理基準

2018 年 9 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 PMDA への報告（情報提供も含む）を統一することにある。

- 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、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

改訂日	改訂理由
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

1. はじめに

1．1　目的

独立行政法人医薬品医療機器総合機構（PMDA：Pharmaceuticals and Medical Devices Agency）（以下、「機構」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

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

1．3　適用の考え方

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

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

1．4　用語の定義

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

1．5　準拠および関連文書

上位規程　：「情報セキュリティポリシー」

関連文書　：「情報システム管理利用規程」

2. システム運用管理業務の概要

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

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

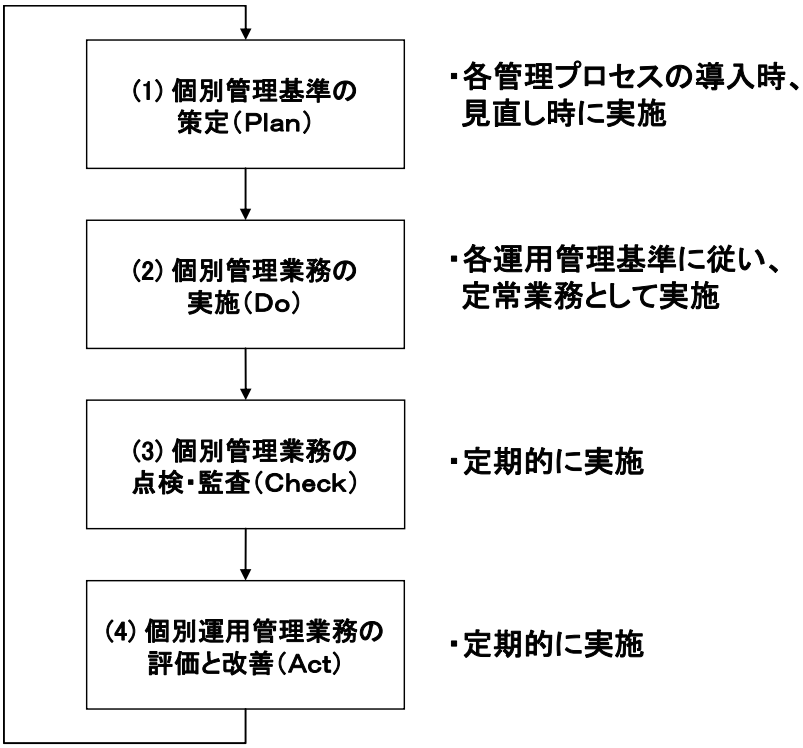
管理業務	概要
バックアップと 回復管理	必要なバックアップを定期的に取得、管理し、障害が発生した場合は、速やかな回復ができるよう、回復要件に基づき必要な回復手順、仕組みを計画、作成、維持する。
情報セキュリティ管理	情報セキュリティポリシーに規定されたセキュリティ対策を実施するために必要な管理要件に基づき、情報セキュリティ管理要領・手順等を作成し、情報セキュリティ管理を行う。
脆弱性管理	情報システムのソフトウェアおよびアプリケーションにおける脆弱性を特定、評価、解消するための管理業務を行う。システム構成を把握したうえで、構成要素ごとに関連する脆弱性情報をいち早く「収集」し、影響範囲の特定と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。

3. 運用管理業務の基本プロセス

（運用管理業務プロセスのPDCAマネジメントサイクル）

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

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



各基本プロセスの概要は、以下のとおりである。

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

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

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

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

4. システム運用管理業務の明確化・標準化

4. 1 問合せ管理

(1) 目的

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

(2) 業務の概要

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

(3) 管理対象

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

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

(4) 業務の管理指標＆標準化

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

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

※報告内容は、各システムの状況に応じて変更しても構わない。

【補足】

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

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

４．２ インシデント管理

(1) 目的

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

(2) 業務の概要

①インシデントの定義

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

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

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

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

②インシデント管理の主な活動

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

インシデント管理のプロセスでは、主に次の活動を実施する。

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

(3) 管理対象

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

(4) 業務の管理指標

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

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

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

(5) 標準化

インシデント管理は、機構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「機構標準書式」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「機構標準書式」を使用する。

※添付「インシデント一覧」を使用する。

４．３ 問題管理（再発防止策）

(1) 目的

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

(2) 業務の概要

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

・問題の傾向分析と課題点の抽出
・是正策の検討
・是正策の実施

(3) 管理対象

本番システム環境で稼動している全てのシステムの問題を管理対象とする。

(4) 業務の管理指標＆標準化

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

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

※報告内容は、各システムの状況に応じて変更しても構わない。

４．４ 変更管理

(1) 目的

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

(2) 業務の概要

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

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

(3) 管理対象

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

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

(4) 業務の管理指標

変更管理業務を評価するための評価指標として以下を定義する。

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

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

(5) 標準化

変更管理は、機構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「機構標準書式」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、機構側の確認・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「機構標準書式」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うえで構成情報を参照可能な状態に維持する。

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

(3) 管理対象

構成管理が対象とする構成情報は以下の通りとする。

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

(4) 業務の管理指標

構成管理業務を評価するための評価指標として以下を定義する。

① 承認されていない構成の件数

② 不正確な構成情報が原因で失敗した変更及び発生した障害の件数

③ CI（管理対象の項目数）の正確さ率

・構成アイテムの管理情報と実態（H/W、S/W、M/W、機器）との整合性の確認

(5) 標準化

〇機構では、「資産台帳・管理簿(システム台帳)」を作成してシステム構成情報を一元管理している。各システムの構成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、更新情報を機構へ報告し、資産台帳・管理簿(システム台帳)を最新の状況に保つこと。

４．６ 運行管理

(1) 目的

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

(2) 業務の概要

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

① 運用引継ぎ
② 運用スケジュールの計画・管理
③ オペレーション実施
④ 稼動監視と障害対応（一次対応）
⑤ ジョブ実行管理
⑥ 帳票管理
⑦ 報告管理

(3) 管理対象

本番システム環境で稼動している全てのシステムの運行を管理対象とする。

(4) 業務の管理指標

運行管理業務を評価するための評価指標として以下を定義する。

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

４．７ バックアップと回復管理

(1) 目的

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

(2) 業務の概要

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

日常運用においては、バックアップ取得、バックアップ媒体の保管を行う。

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

(3) 管理対象

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

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

(4) 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。

(5) 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）

〇機構では、「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、機構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、「外部委託における情報セキュリティ対策実施要領」に則って、適切にセキュリティ管理策が導入され、維持されていることを確実にするために、情報セキュリティ管理計画の維持・管理を行う。合わせて、情報セキュリティ対策が適切に運用されているかを定期的に点検するとともに、コンプライアンス等の観点からのシステム監査の実施対応をおこなう。

(3) 管理対象

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

(4) 業務の管理指標

情報セキュリティ管理業務を評価するための評価指標として以下を定義する。

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

(5) 標準化

①情報セキュリティ遵守状況の報告<次ページ参照>

- 情報セキュリティを遵守していることを定期的(月次)にて報告すること
- 合わせて委託先における自己点検を定期的(年 2 回程度)に実施し、点検結果を報告すること。
  （点検内容は委託先の任意項目で実施）

【補足説明】

情報セキュリティ遵守状況の報告は、以下の内容を確認し、報告すること

① 情報の目的外利用の禁止

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

③ 体制変更の場合の速やかな報告

④ 体制に記載された者以外が委託業務にアクセスできない（していない）ことの確認
※発生した場合は、すぐに検知でき、報告される

~~⑤~~ 要員の所属・専門性（資格や研修実績）・実績および国籍に関する情報提供
※変更があれば、その都度情報提供される。

⑥ 秘密保持契約（誓約書）の提出（要員全員が提出）
※委託業務を離れた者の一定期間の機密遵守を含む
※体制変更があった場合の追加提出も含む

⑦ 情報セキュリティインシデントへの対処方法の明確化され、要員に周知されている

⑧ 再委託がある場合は、上記内容を再委託先においても遵守していることが確認されている

４．９ 脆弱性管理

(1) 目的

サーバ装置、端末及び通信回線装置上で利用するソフトウェアやアプリケーションに関連する脆弱性について、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る。

(2) 業務の概要

脆弱性管理では、脆弱性情報の収集から影響評価、パッチ適用計画の承認、パッチ適用の実施、パッチ適用結果の報告・確認までの一連のプロセスを管理する。

①管理対象の現況把握

②脆弱性情報の収集

③影響・評価と対応要否の判断及び記録

④パッチ適用計画（代替策実施計画）の策定

③パッチ適用計画（代替策実施計画）の承認

④パッチ適用計画の検証 （検証環境での稼動確認）

⑤パッチ適用（代替策）の実施

⑥パッチ適用（代替策）の記録

(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 対策の実施状況（セキュリティパッチ適用、またはその代替策）／予定・実績
・セキュリティカレンダーによる定期報告
・変更管理＝システム変更作業報告（パッチ適用状況報告を含む）
・情報セキュリティ管理情報＝セキュリティ遵守状況の報告

(5) 標準化

脆弱性管理は、機構標準書式を適用する。

① 対象プロダクト・バージョンの把握
各情報システムにおいて管理対象とするプロダクトとバージョンの現況を把握する。
書式は、各情報システムの任意とする。

② 脆弱性情報の公表時

・収集した脆弱性情報をもとに情報システムへ与えるリスク・影響・緊急度を評価し、対応の要否及び対策の内容を判断する。

※添付「脆弱性情報調査表」を使用する。

③ 脆弱性対策の実施時

・セキュリティパッチ適用計画及び適用作業の確認と記録

※標準書式「変更作業申請書」及び「変更作業一覧」を使用する。

・セキュリティパッチ適用状況の管理

※添付「セキュリティパッチ管理台帳」を使用する。

④ 定期的（月次）報告時

脆弱性への対応要否及びセキュリティパッチ適用状況について、「脆弱性情報調査表」及び「セキュリティパッチ管理台帳」により、定時（月次）で報告する。

参考　脆弱性情報収集時の参考 URL 一覧

種別	URL
脆弱性関連情報データベース	・JVN(Japan Vulnerability Notes)　http://jvn.jp/ ・脆弱性対策情報データベース JVN iPedia　http://jvndb.jvn.jp/
ニュースサイト	・CNET ニュース：セキュリティ http://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 http://itpro.nikkeibp.co.jp/security/index.html
注意喚起サイト	・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 http://www.jpcert.or.jp/at/ ・警察庁：警察庁セキュリティポータルサイト http://www.npa.go.jp/cyberpolice/
製品ベンダー	■定例アップデート ・マイクロソフト TechCenter（毎月第 2 火曜日 更新） http://technet.Microsoft.com/ja-jp/security/default.aspx ・オラクル Critical Patch Update（年 4 回 1,4,7,10 月の 17 日に近い火曜日） http://www.oracle.com/technetwork/jp/topics/security/alerts-082677-ja.html
	■クライアント製品など ・アップル http://support.apple.com/kb/HT1222?viewlocale=ja_JP ・アドビ（Adobe Reader/Adobe Flash Player など） http://helpx.adobe.com/jp/security.html

	・Mozilla （FireFox/ThunderBird など） http://www.mozilla-japan.org/security/known-vulnerabilities/
	■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 http://www.cisco.com/cisco/web/support/JP/loc/security/index.html ・HP － サポートセンター https://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/secBullArchive ・日立 －セキュリティ情報 http://www.hitachi.co.jp/hirt/security/index.html ・富士通 － セキュリティ情報 http://www.fujitsu.com/jp/support/security/ http://software.fujitsu.com/jp/security/ ・NEC － NEC 製品セキュリティ情報 http://jpn.nec.com/security-info/ ・IBM －重要セキュリティ情報 http://www-06.ibm.com/jp/services/security/info/index.html ・Red Hat － Errata https://rhn.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 http://www.Symantec.com/ja/jp/security_response/securityupdates/list.jsp?fid=security_advisory
	■オープンソースなど ・Apache Foundation http://httpd.apache.org/ （Apache HTTP サーバ） http://tomcat.apache.org/（Apache Tomcat） http://struts.apache.org/ （Apache Struts） ・ISC （Internet Systems Consortium） http://www.isc.org/downloads/bind/ （BIND） http://www.isc.org/downloads/dhcp/ （DHCP） ・OpenSSL http://www.openssl.org/

4．10 アクセス権管理

(1) 目的

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

(2) 業務の概要

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

(3) 管理対象

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

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

(4) 業務の管理指標

アクセス権管理業務を評価するための評価指標として以下を定義する。

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

(5) 標準化

特権（高権限）IDについて、以下の管理を行う。

①特権ID(システムID)台帳の作成

※添付「特権ID管理台帳」を使用する。

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

※監査等にて提示要求があった場合は、速やかに提示できるよう保管する

②特権ID(システムID)使用管理簿の作成（またはログ抽出）

※添付「特権 ID 使用管理簿」を使用する。

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

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

③定期(月次)報告

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

④特権ID棚卸し

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

棚卸し点検内容は以下の通り

〇台帳は、本当に使用する者を登録しているか?(体制図と一致しているか?)

・体制から外れた者が削除されずに残っていないか?

・使用予定がない者が登録されていないか?

〇台帳と使用管理簿の相関は一致しているか?

〇使用管理簿とログ(または画面コピー)保管の相関は一致しているか?

4．11　キャパシティ管理

(1)　目的

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

① ビジネスの需要に対する供給

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

② キャパシティに対するコスト

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

(2)　業務の概要

このプロセスは、次の3つのサブプロセスから構成される。

① ビジネスキャパシティ管理

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

② サービスキャパシティ管理

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

③ コンポーネントキャパシティ管理

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

(3)　管理対象

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

(4)　業務の管理指標

キャパシティ管理業務を評価するための評価指標として以下を定義する。

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

４．１２　可用性管理

(1)　目的

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

(2)　業務の概要

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

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

① 可用性

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

稼働率（%）＝（サービス提供時間－停止時間）÷サービス提供時間

② 信頼性

提供されるITサービスにおける、不具合の発生しにくさ／故障しずらさを表す。

平均故障間隔＝（使用可能な時間－総停止時間）÷（サービス中断の回数－1）

③ 保守性

ITサービスが停止又は品質低下した際に、いかに早く復旧できるかを示す指標。

平均修理時間＝修理時間の合計÷サービス中断の回数

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

(3)　管理対象

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

(4)　業務の管理指標

可用性管理業務を評価するための評価指標として以下を定義する。

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

4．13　サービスレベル管理

(1)　目的

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

(2)　業務の概要

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

(3)　管理対象

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

(4)　業務の管理指標

サービスレベル管理業務を評価するための評価指標として以下を定義する。

①「サービスレベル合意書」の各サービスレベル項目の達成率

②各個別管理業務での管理指標の達成率

(5)　標準化

サービスレベル管理業務を定期的(月次)に報告する。

①「サービスレベル合意書」の各サービスレベル項目の達成率

②各個別管理業務での管理指標の達成率

以上

別紙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）	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。	脆弱性対策はPMDAの指示に基づいて行い、実施状況は都度報告すること。
アクセス・利用制限（AC：Access）	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）	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。
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。	バックアップの実施状況は、月次で報告すること。
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。