資料２－２

（独）国際協力機構
コンピュータシステム運用等業務
民間競争入札実施要項（案）

令和 5 年（2023 年）

独立行政法人国際協力機構

目次

【別紙資料】

別紙１　従来の実施状況に関する情報の開示（組織図、業務区分表含む）
別紙２　アンケート（サンプル）
別紙３　業務フロー図
別紙４　機構組織図

【別添資料】

別添１　コンピュータシステム運用等業務 調達仕様書
別添２　評価基準書

１　趣旨

競争の導入による公共サービスの改革に関する法律（平成 18 年法律第 51 号。以下「法」という。）に基づく競争の導入による公共サービスの改革については、公共サービスによる利益を享受する国民の立場に立って、公共サービスの全般について不断の見直しを行い、その実施について、透明かつ公正な競争の下で民間事業者の創意と工夫を適切に反映させることにより、国民のため、より良質かつ低廉な公共サービスを実現することを目指すものである。

上記を踏まえ、独立行政法人国際協力機構（以下「当機構」という。）は「公共サービス改革基本方針」（平成 24 年 7 月 20 日閣議決定）別表において民間競争入札の対象として選定された「コンピュータシステム運用等業務」（以下「本業務という」）について、公共サービス改革基本方針に従って、民間競争入札実施要項を定めるものとする。

２　本業務の詳細な内容及びその実施に当たり確保されるべき質に関する事項

(1) 本業務の概要

ア　対象となる業務の概要

(ｱ) 本業務の経緯

機構情報システム部は、機構内 IT 基盤の構築・運用支援を目的として「コンピュータシステム運用等業務（設計・構築フェーズ、2016 年 2 月～2017 年 7 月）」および「コンピュータシステム運用等業務（運用フェーズ、2017 年 6 月～2024 年 5 月）」の委託契約を締結し、同契約の監理を行っている。

現行のコンピュータシステム運用等業務（運用フェーズ）は 2024 年 5 月で履行期限の満了を迎えるため、本事業次期期間の構築・導入・運用を含む調達を行う。なお、現行のコンピュータシステム運用等業務（運用フェーズ）では、2020 年度から流行している「コロナウイルス（COVID-19）」により急増した国内外拠点を含む機構全体での在宅勤務等に対応するためにクラウド化等、機構 IT 環境を大幅に変更しており、本業務においてもオンプレミス環境の更なるクラウド化も行っていく方針である。

(ｲ) 本業務の構成

今回調達するシステム運用等業務においては、機構データセンタ（以下「機構 DC」という。）、機構クラウドデータセンタ（以下「機構クラウド DC」という、バックアップリージョン含む。）、SaaS（Software as a Service）の基盤系システム提供等を用いた）基盤系サービスを対象とする。また、それら IT 環境を用いての全在外拠点、全国内拠点、本部における PC 運用や Microsoft365 等の各種システム運用サービスの提供を対象とする。ネットワークとしては、当機構の全国内拠点、全在外拠点について、別事業者が管理する国内情報通信網、国際情報通信網により接続される。

(ｳ) 本業務の規模

本業務で提供するサービスの利用者は機構職員、非常勤職員、機構が許可した外部事業者等であり、ユーザアカウントの総数は約 6600 である。PC 管理台数は約 6600 台、このうち約 3900 台が国内で、残りが在外拠点で利用する端末である。ヘルプデスクへの問い合わせ件数は月間平均 2258 件程度である。（2021 年度実績で年間合計 27,099 件）

イ　本業務の内容

本業務は、機構情報システム部が管理する IT 基盤の内、基盤システムおよびハウジングサービスの設計、構築、運用に係る業務である。以下に調達内容を示す。

本業務は、「サービス利用環境提供業務」と、システムを円滑に利用していくための「サービス利用計画業務」、「サービス利用支援業務」、「サービス運用管理業務」からなる。

（サービス利用環境提供業務）

(ｱ) 基盤系サービス

・当機構で共通的に使用する各種共通基盤システムの機能を受注者にて設計・構築する。

・運用開始後は、当機構が利用可能なように運用・保守することを求める。

(ｲ) ハウジングサービス

・現在、当機構にて運用する複数の業務系システムを、受注者が整備するデータセンタのハウジングスペースに機器移設し、運用開始後は、当機構が利用可能なようにサービス提供することを求める。

（サービス利用計画業務）

(ｳ) サービスデザイン（運用開始前業務）

後述のサービス利用支援業務及びサービス運用管理業務に含まれる運用業務の設計等を行うことを求める。

（サービス利用支援業務）

(ｴ) サービスオペレーション

各システムの起動・停止、バックアップ運用、点検作業運用、リカバリ運用、PC・スマートフォン等の運用、SaaS の運用、セキュリティ運用、本部ネットワークの一部運用等を行うことを求める。

(ｵ) サービス関連調査・提言

インフラ導入・設定変更、PC 更改、技術動向・運用改善に係る状況把握・提言、および監査（内部・外部）対応支援等を行うことを求める。

(ｶ) IT コンシェルジュサービス

調達仕様書作成支援、プロジェクト実施支援等の各部署システム化支援、および情報システム部にて主管する情報基盤（IT 共通インフラ）整備に係る支援等を行うことを求める。

サービス提供環境における支援業務グループウェアを含む情報共有に係るコンテンツの開発、改修・再構築・機能向上、整理の実施およびユーザからの照会対応を行うことを求める。

(ｷ) BCP 発動時に備えた機構クラウド DC（バックアップリージョン）の運用

バックアップ DC 及び機構クラウド DC（バックアップリージョン）の BCP 発動時に備えた通常運用、BCP 発動時の運用、訓練等を実施することを求める。

（サービス運用管理業務）

(ｸ) サービス管理（インシデント管理）

当機構内・在外利用者向けヘルプデスク業務、ユーザからの申請対応、システム監視、障害対応等を行うことを求める。

(ｹ) 問題管理

障害の原因となる問題の管理等を実施することを求める。

(ｺ) 変更管理

システム変更の管理を実施することを求める。

(ｻ) リリース管理

リリース情報、リリース作業の管理等を実施することを求める。

(ｼ) 構成管理

システム構成情報の管理を行うことを求める。

(ｽ) 資産管理

資産管理ソフトにより各種ハードウェアに関する保有情報、賃貸借情報の統一的な管理を行うことを求める。

(ｾ) ソフトウェア管理

ソフトウェアライセンスの管理等を行うことを求める。

(ｿ) セキュリティ管理

セキュリティインシデント発生時の対応やセキュリティに係る提言等を行うことを求める。

(ﾀ) ドキュメント管理

ドキュメント整備及び管理等を行うことを求める。

(ﾁ) 全体管理

運用者自身の工程管理や関連事業者との調整を行うことを求める。

(ﾂ) セルフモニタリング

当機構と合意したモニタリング項目の管理、見直しを含むセルフモニタリング業務を実施することを求める。

なお、本業務の詳細な内容は別添 1「コンピュータシステム運用等業務調達仕様書」に記されているとおりである。

ウ　本業務に関連する作業の履行

本業務の履行範囲に関連して、設計開発や調査、運用等が追加で必要になった場合には、当機構と受注者とで協議のうえ、対応に応じること。現時点で想定される事項は以下のとおりである。

(ｱ) IT 戦略への対応

当機構では、2022 年 5 月に「IT 戦略（2022～26 年度)」を策定した。本業務も同戦略を実現するための施策の一つとして実施するものである。次期 IT 戦略（2027 年度～）において、当機構の IT 環境に対する方針が変化することも考えられるが、それによって、本調達の実施内容の見直しが必要となった場合には、当機構と受注者とで協議のうえ、対応に応じること。

エ　受託業務の引継ぎ

(ｱ) 現行受注者又は当機構からの引継ぎ

当機構は、当該引継ぎが円滑に実施されるよう、現行受注者及び受注者に対して必要な措置を講ずるとともに、引継ぎが完了したことを確認する。

本業務を新たに実施することとなった受注者は、本業務の開始日までに、業務内容を明らかにした書類等により、現行受注者（又は当機構）から業務の引継ぎを受けるものとする。

なお、その際の事務引継ぎに必要となる現行受注者（又は当機構）側の経費は、現行受注者（又は当機構）の負担となる。

(ｲ) 受託期間満了の際における次回受注者への引継ぎ

当機構は、当該引継ぎが円滑に実施されるよう、本業務受注者及び次回受注者に対して必要な措置を講ずるとともに、引継ぎが完了したことを確認する。

本業務の終了に伴い受注者が変更となる場合には、本業務受注者は、当該業務の開始日までに、業務内容を明らかにした書類等により、次回受注者に対し、引継ぎを行うものとする。

なお、その際の事務引継ぎに必要となる経費は、本業務受注者の負担となる。

(2) 確保されるべき対象業務の質

ア　業務内容：「2(1)イの本業務の内容」に示す運用業務を適切に実施すること。

イ　呼損率

とることができなかった電話件数の割合を10%未満とすること。以下の計算式により算出する。

呼損率＝とることができなかった電話の本数÷かかってきた電話の本数×100

ウ　一次窓口解決率

全問い合わせの件数のうち、問題が解決できた問い合わせ件数の割合が、80%以上であること。以下の計算式により算出する。

一次窓口解決率 ＝ 一次窓口解決件数 ÷ 総問い合わせ件数×100

エ　回答目標時間遵守率

ヘルプデスクでの問い合わせ受付から完了まで1時間以内に総問い合わせ件数の80%以上を解決率すること。以下の計算式により算出する。

回答目標時間遵守率 ＝(回答目標時間遵守件数 ÷ 総問い合わせ件数)×100

オ　システム稼働率

システムごとの主機能の大部分が利用できる時間が99.9%であること。以下の計算式により算出する。

稼働率＝(システム稼動時間－システム停止時間の積上げ）÷ システム稼動時間 × 100

カ　利用者満足度

ヘルプデスク利用者に満足度に関し調査（アンケート）を行い基準スコアを維持すること。基準スコアは4段階評価（満足・やや満足・やや不満・不満）で、全回答の合計の70%以上が「満足」、「やや満足」である

ことを目安とするが、アンケート項目および基準スコアとも機構と協議のうえ決定する。

キ　研修参加者評価

研修参加者に研修の満足度調査を行い基準スコアを維持すること。4段階評価（満足・やや満足・やや不満・不満）で、全回答の合計の70%以上が「満足」、「やや満足」であることを目安とするが、アンケート項目および基準スコアとも機構と協議のうえ決定する

ク　セキュリティ上の重大障害件数

個人情報、施設等に関する情報、その他契約利用に際し知り得た情報漏洩の件数は0件であること。

ケ　サービスレベルアグリーメント（Service Level Agreement）の締結

上記項目以外にも、本業務の効率化と品質向上並びに円滑化を図るため、調達仕様書および要件定義書に示す管理指標に対してサービスレベルアグリーメント（Service Level Agreement、以下「SLA」という。）を締結し、当機構が期待する付加価値（品質）を提供できているかどうか双方協議のうえ、モニタリング項目に基づく定量・定性評価を月次で実施する。なお、受注者の責によらない事由により基準値を満たさない場合にはこの限りではない。

(3) 創意工夫の発揮可能性

本業務を実施するに当たっては、以下の観点から受注者の創意工夫を反映し、公共サービスの質の向上（包括的な質の向上、効率化の向上、経費の削減等）に努めるものとする。なお、提案にあたっては、本業務を当機構と共に実施するパートナーとして、機構からの指摘を待つことなく自律的に取り組むことが求められる。

(ｱ)本業務の実施全般に対する提案

受注者は、当機構との協議により定める形式に従い、本業務の実施全般に係る質の向上の観点から取り組むべき事項等の提案を行うこととする。

(ｲ)事業内容に対する改善提案

受注者は、事業内容に対し、改善すべき提案（コスト削減に係る提案を含む）がある場合は、当機構との協議により定める形式に従い、具体的な方法等を示すとともに、従来の実施状況と機構職員の業務環境が同等以上の質が確保できる根拠等を提案すること。

(4) 契約の形態及び支払

ア　契約の形態は、請負型の契約とする。

イ　当機構は、契約に基づき、受注者が実施する本業務について、契約の履行に関し、調達仕様書に定めた内容に基づく監督・検査を実施するなどして適正に実施されていることを確認した上で、適正な支払請求書を受領した日から30日以内に、契約金額を支払うものとする。なお、設計・構築フェーズにおいては、納入成果物提出の都度検査をし、検査結果合格通知後に納入成果物の対価を支払う。一方、運用フェーズにおいては、四半期毎の実施報告書提出後検査し、検査結果合格通知後に支払う。確認の結果、確保されるべき対象業務の質が達成されていないと認められる場合、又は確保されるべき質が達成できないあるいは達成できない恐れがある場合、当機構は、確保されるべき対象業務の質の達成に必要な限り、受注者に対

して本業務の実施方法の改善を行うよう指示するもしくは以下ウに示す措置をとることができる。受注者は、当該指示を受けて業務の実施方法を改善し、業務改善報告書を速やかに当機構に提出するものとする。業務改善報告の提出から3か月の範囲で、業務改善報告書の内容が、確保されるべき対象業務の質が達成可能なものであると認められるまで、当機構は、委託費の支払を行わないことができる。なお、委託費は、本件業務開始以降のサービス提供に対して支払われるものであり、受注者が行う準備行為等に対して、受注者に発生した費用は、受注者の負担とする。

ウ　減額措置

「2 (3) 確保されるべき対象業務の質」に示すサービスレベルがSLAで双方合意した基準を下回った場合、当機構は未達成度合によりペナルティポイントを課す。一定のポイントが累積した時点で減額対象とし、四半期ごとに受注者に支払う費用から減額して支払うものとする。

ただし、上記ペナルティポイントおよび減額措置はその発生要因が受注者によるものと、受注者および当機構間での協議により合意した場合に限る。

なお、サービスレベルの実績値は、調達仕様書に基づき受注者が作成し、当機構担当部署に提出した報告書の記載内容を踏まえて、双方協議のうえ、当機構が最終判断するものとする。

(5) 法令変更による増加費用及び損害の負担

法令の変更により受注者に生じた合理的な増加費用及び損害は、アからウに該当する場合には当機構が負担し、それ以外の法令変更については受注者が負担する。

ア　本業務に類型的又は特別に影響を及ぼす法令変更及び税制度の新設・変更（税率の変更含む）

イ　消費税その他類似の税制度の新設・変更（税率の変更含む）

ウ　上記ア及びイのほか、法人税その他類似の税制度の新設・変更以外の税制度の新設・変更（税率の変更含む）

3　実施期間に関する事項

前項で提示した各業務について以下の期間で実施するものとする。また、その他の調達を含む作業スケジュールの概要については「別添1　コンピュータシステム運用等業務調達仕様書」を参照すること。

(1) 設計・構築期間（仮運用等含む）

2023年11月下旬から2024年5月31日まで

(2) 運用期間

2024年6月1日から2029年5月31日まで

4　入札参加資格に関する事項

(1) 法第15条において準用する法第10条各号（第11号を除く。）に該当する者でないこと。

(2) 当機構の契約事務取扱細則第 4 条に該当しないこと。
(3) 予算決算及び会計令第 71 条の規定に該当しない者であること。
(4) 令和 4・5・6 年度全省庁統一資格で「役務の提供等」の資格を有すること。
(5) 法人として財務状況に特に問題がないと判断されること。
(6) 業務の履行に当たり、秘密情報保全の適切な体制が構築・保証（親会社等に対しての秘密情報の伝達・漏洩がないことの保証を含む。）されている法人であると判断されること。また、本業務の主要な業務従事者について、秘密情報を取扱うにふさわしい者であると判断されること。
(7) 次の各号に該当する者は本件競争参加を認めない。
ア.　独立行政法人国際協力機構反社会的勢力への対応に関する規程（平成２４年規 程(総)第２５号）第２条第１項の各号に掲げる者、具体的には、反社会的勢力、暴力団、暴力団員、暴力団員等、暴力団準構成員、暴力団関係企業、総会屋等、社会運動等標ぼうゴロ、特殊知能暴力集団等を指す。
イ.　先に行われた業務等との関連で利益相反が生じると判断される者、または同様の個人を主たる業務従事者とする場合
(8)　当機構から「独立行政法人国際協力機構競争参加資格停止措置規程」に基づく契約競争参加資格停止措置を受けている期間中でないこと。
(9) 単独で対象業務を行えない場合は、又は、単独で実施するより業務上の優位性があると判断する場合は、適正に業務を実施できる共同企業体を結成し、入札に参加することができる。その場合、入札書類提出時までに共同企業体を結成し、入札参加資格の全てを満たす者の中から代表者を定め、他の者は構成員として参加するものとする。また、共同企業体の構成員は、上記(1)から(8)までの資格を満たす必要があり、他の共同企業体の構成員となる、又は、単独で参加することはできない。なお、共同企業体の代表者および構成員は、共同企業体の結成に関する協定書（又はこれに類する書類）を作成し、提出すること。
（注）共同企業体とは
「共同企業体」とは、本業務の実施を目的に複数の事業者が組織体を構成し、本業務の入札に参加する者のことを指す。

(10) 情報セキュリティマネジメントシステムに係る規格（ISO27001）の認証を保持している部署が、本業務の主担当部署と連携する体制が組めること。
(11) 品質マネジメントシステムに係る規格（ISO9001）の認証を、本業務の主担当部署が保持していること。
(12) 個人情報保護に関する認証（プライバシーマーク又は同等の認証）を保持していること。
(13) 以下全業務の「社としての経験」を「過去 5 年間で 3 件以上」有していること。
ア. 基盤系サービスの設計開発またはサービス提供業務
イ. 基盤系サービスおよび業務系システムの運用管理業務
ウ. データセンタの移行作業
エ. 情報セキュリティ管理および対策実施業務

５　入札に参加する者の募集に関する事項

(1) 想定スケジュール

入札公示（官報公示）	令和 5 年（2023 年）	8 月下旬頃
入札説明会		9 月中旬頃
質問受付期限		9 月下旬頃
資料閲覧期限		10 月中旬頃
提案書提出期限		10 月下旬頃
入札参加者によるプレゼンテーション		10 月下旬頃
提案書の審査		10 月下旬頃
開札及び落札予定者の決定		11 月中旬頃
契約締結		11 月下旬頃

なお、閲覧資料については、民間競争入札に参加する予定の者から要望があった場合、所定の手続きを踏まえた上、別紙 5「機密保持誓約書（雛形）」へ署名し、遵守することで閲覧可能である。

(2) 書類等の提出先

入札手続き窓口、各種照会先は以下のとおり。なお、本項以降も必要な場合にはこちらが連絡先となる。

〒１０２-８０１２
東京都千代田区二番町５番地２５ 二番町センタービル
独立行政法人国際協力機構 調達・派遣業務部契約第三課
【電話】０８０-７１０７-９００５
上記電話番号でつながらない場合には０３－５２２６－６６０９へ電話すること。
【メールアドレス】e_sanka@jica.go.jp
※ 当機構からのメールを受信できるよう、当機構のドメイン（jica.go.jp）またはメールアドレスを受信できるように設定すること。メールを送付後、受信完了の連絡が無い場合は上記電話番号へ照会すること。

(3) 書類等の提出方法

１）入札手続きのスケジュール及び書類等の提出方法

予め機構が設定した締切日時までに必要となる書類の提出、授受は電子入札システムで行う。ただし、一部書類についてはメールでの提出とする。詳細は別紙「入札手続・締切日時一覧表」をご覧ください。

２）電子入札による各種書類の授受方法については以下の「電子入札システムポータルサイト」を参照すること。

https://www.jica.go.jp/announce/notice/ebidding.html

３）書類等の押印省略

機密保持誓約書、競争参加資格確認申請書、共同企業体結成届、下見積書、技術提案書、委任状及び入札書等の提出書類については、全て代表者印等の押印を原則とする。ただし、押印が困難な場合は、各書類送付時のメール本文に、社内責任者の役職・氏名とともに、押印が困難な旨を記載し、社内責任者より（もしくは社内 責任者に cc を入れて）メールを送信することで押印に代え

ることができる。

⑷ 競争参加資格

１）消極的資格制限

以下のいずれかに該当する者は、当機構の契約事務取扱細則（平成１５年細則(調)第８号）第４条に基づき、競争参加資格を認めない。また、共同企業体の構成員や入札の代理人となること、契約の下請負人（業務従事者を提供することを含む。以下同じ。）となることも認めない。

ア. 破産手続き開始の決定を受けて復権を得ない者

具体的には、会社更生法（平成１４年法律第１５４号）または民事再生法（平成１１年法律第２２５号）の適用の申立てを行い、更生計画または再生計画が発効していない法人をいう。

イ. 独立行政法人国際協力機構反社会的勢力への対応に関する規程（平成２４年規程(総)第２５号）第２条第１項の各号に掲げる者

具体的には、反社社会勢力、暴力団、暴力団員、暴力団員等、暴力団員準構成員、暴力団関係企業、総会屋等、社会運動等標ぼうゴロ、特殊知能暴力集団等を指す。

ウ. 独立行政法人国際協力機構が行う契約における不正行為等に対する措置規程（平成２０年規(調)第４２号）に基づく契約競争参加資格停止措置を受けている者。

具体的には、以下のとおり取扱う。

a) 競争参加資格確認申請書の提出期限日において上記規程に基づく資格停止期間中の場合、本入札には参加できない。

b) 資格停止期間前に本入札への競争参加資格確認審査に合格した場合でも、入札執行時点において資格停止期間となる場合は、本入札には参加できない。

c) 資格停止期間前に落札している場合は、当該落札者との契約手続きを進める。

２）積極的資格制限

当機構の契約事務取扱細則第５条に基づき、以下の資格要件を追加して定める。

ア. 全省庁統一資格

令和０４・０５・０６年度全省庁統一資格で「役務の提供等」の資格を有すること。

３）共同企業体、再委託について

ア. 共同企業体

共同企業体の結成を認める。ただし、共同企業体の代表者及び構成員全員が、上記１）及び２）の競争参加資格要件を満たす必要がある。

共同企業体を結成する場合は、共同企業体結成届（様式集参照）を作成し、競争参加資格確認申請書（各社ごとに必要）に添付すること。結成届には、構成員の全ての社の代表者印等（法的効力をもつ印）を押印すること。

イ. 再委託

a) 再委託は原則禁止であるが、一部業務の再委託を希望する場合は、技術提案書にその再委託予定業務内容、再委託先企業名等を記述すること。

b)再委託の対象とする業務は、本件業務全体に大きな影響を及ぼさない補助的な業務に限る。
c)当機構が、再委託された業務について再委託先と直接契約を締結することや再委託先からの請求の受理あるいは再委託先へ直接の支払いを行うことはない。
d)なお、契約締結後でも、発注者から承諾を得た場合には再委託は可能である。

(5) 応札制限（利益相反の排除）
先に行われた業務等との関連で利益相反が生じると判断される者、または同様の個人を主たる業務従事者とする場合は、本件競争参加を認めない。

(6) 競争参加資格の確認
競争参加資格を確認するため、以下の１）を「（２） 書類等の提出先」まで電子メールで提出すること。 提出方法、締切日時および確認結果通知日は別紙「手続・締切日時一覧」を参照すること。

１） 提出書類：
a）競争参加資格確認申請書（様式集参照）
b）全省庁統一資格審査結果通知書（写）
c）下見積書（「７. 下見積書」参照）
d）財務諸表（決算が確定した過去３会計年度分の財務三表）
e）秘密情報の取扱いにかかる競争参加者の社内規則（本文含む）
f）競争参加者に係る親会社・子会社等の資本関係等に係る関係図:競争参加者に係る親会社、地域統括会社、ブランド・ライセンサー、フランチャイザー、コンサルタントその他の競争参加者に対して指導、監督、業務支援、助言、監査等を行う者の一覧及び競争参加者との資本又は契約（名称の如何を問わない何らかの合意を言い、間接契約、第三者間契約等を含む。）関係図とする。
g）競争参加者の発行済株式の１%以上を保有する株主名、持株数、持株比率
h）競争参加者の取締役（監査等委員を含む。）の略歴
i）情報セキュリティに関する資格・認証（取得している場合）
j）個人情報保護に関する認証（プライバシーマーク又は同等の認証）
k）法第 15 条において準用する法第 10 条に規定する欠落事由にうち、暴力団排除に関する規程について評価するために必要な書類（書類については、落札予定者となった者のみ提出。）
l）共同企業体を結成するときは、次の 2 点を提出すること。
・共同企業体結成届
・共同企業体を構成する社（構成員）の資格確認書類(上記 c)を除くすべての書類 ）
※留意事項：f）及び g)に関連し、発行済株式の 33.4%（1/3）以上を単独で 保有する法人がいる場合は、当該法人に関する d）～i）を説明すること。なお、当該法人についても発行済株式の 33.4%（1/3）以上を単独で保有する法 人がいる場合は、上記基準に従い、同様の報告を行うこと。これ

は発行済株 式の 33.4%（1/3）以上を単独で保有する法人に対して繰り返し適用する。ま た、当該資本関係にある法人との間の情報共有ルールについても e)を含めて説明すること。

２） 追加資料提出の指示：

競争参加資格要件、特に、「財務状況の健全性」及び「秘密情報保全」に係る資格要件の確認・審査において、上記提出資料のみでは判断がつかない場合には、提出期限を明示して、追加資料の提出を求めることがある。提示された提出期限までに追加資料の提出がなかった場合には、当該競争参加者の競争参加資格を認めないことがある。また、「主要な業務従事者が秘密情報を取り扱うにふさわしい者」であるかの判断について、技術提案書が提出された後に、業務従事者にかかる追加資 料の提出を求める場合がある。

３） 競争参加資格の確認の結果はメールで通知する。

(7) 入札説明書の資料の交付及び閲覧方法

１）入札説明書の一部資料（ 業務仕様書（案)、評価基準書、評価表）に関しては 大容量ファイル送受信ソフト（GIGAPOD）もしくはメールを通じて配布しますの で別紙「手続・締切日時一覧」を参照すること。

なお、資料交付の際に「機密保持誓約書」（様式集参照）を PDF でメールにて提出すること

２）閲覧資料の閲覧方法に関して発注者からの参加資格有の確認通知を受領後、入札説明書の一部資料の閲覧が可能なため、必ず「閲覧資料の取扱い」をご確認頂き、「資料閲覧申込書」に必要事項記載の上、申し込むこと。

(8) 業務内容説明会の開催

１）日時：別紙「手続・締切日時一覧」を参照すること。

２）場所：Microsoft Teams を用いて遠隔で実施する。

３）その他:

a)参加希望者は（１）の１営業日前の正午までに電子メールにて、社名、参加希望者の氏名、Microsoft Teams 接続用のメールアドレス（２アドレスまで）を連絡すること。

b)業務内容説明会への出席は競争参加資格の要件とはしない。説明会に出席していない者（社）も競争への参加は可能である。

(9) 下見積書

本競争への参加希望者は、競争参加資格の有無について確認を受ける書類の提出（（４）参照）と共に、以下の要領で、下見積書を提出すること。下見積書には、商号または名称及び代表者氏名を明記すること。

１）様式は任意だが、金額の内訳を可能な限り詳細に記載すること。

２）消費税及び地方消費税の額（以下「消費税額等」）を含んでいるか、消費税額等を除いているかを明記すること。

３)下見積書提出後、その内容について当機構から説明を求める場合がある。

(10) 入札説明書に対する質問

１）業務仕様書（案）の内容等、この入札説明書に対する質問がある場合は、

別紙「手続・締切日時一覧」に従い、質問書様式（別添様式集参照）に記載のうえ、メールに添付して提出すること。
２）公正性・公平性等確保の観点から、電話等口頭でのご質問は原則として認めない。
３）上記 １）の質問に対する回答書は、別紙「手続・締切日時一覧」に従い、原則機密保持誓約書を提出した全ての者に対して、機構よりメールにて送付する。
４）回答書によって、仕様・数量等が変更されることがあるので、本件競争参加希望者は質問提出の有無にかかわらず回答を必ず確認すること。入札金額は回答による変更を反映したものとして取り扱う。

(11) 辞退届の提出
１）競争参加資格有の確定通知を受け取った後に、入札への参加を辞退する場合は、遅くとも入札会１営業日前の正午までに辞退する旨を下記メールアドレスまで送付すること。
宛先：e_sanka@jica.go.jp
件名：【辞退】（調達管理番号）_（法人名）_ 案件名
２） １）の手続きにより競争参加を辞退した者は、これを理由として以降の入札において不利益な取扱いを受けるものではない。
３）一度提出された辞退届は、取り消しを認めない。

(12) 技術提案書・入札書
１）提出方法
提出方法及び締切日時は別紙「手続・締切日時一覧」を参照すること。
a）技術提案書はGIGAPOD（大容量ファイル送受信システム）経由で提出するため、別紙「手続・締切日時一覧」の依頼期限までに提出用フォルダ作成を「（２）書類等の提出先」にメールで依頼すること。そのうえで技術提案書はGIGAPODの専用フォルダにパスワードを付せずに格納すること。技術提案書 PDF ファイルのアップロード完了後、格納が完了した旨を（２）書類等の提出先までメールで連絡すること。
b）入札書は、入札書受付締切日時までに電子入札システムの「入札書」に所定の項目を入力の上、同システム上で提出すること。なお、総合点が同点の場合には、抽選となるので、その際に必要となる「くじ入力番号」（３桁の半角数字）を必ず入力すること。また、入札金額は円単位で記入し、消費税及び地方消費税を抜いた税抜き価格とすること。

２）その他
a）「別添１ コンピュータシステム運用等業務 調達仕様書」及び「別添２評価基準書」に示した各要求項目について具体的な提案（2（3）に記載の「創意工夫」を含む。）を行い、各要求項目を満たすことができることを証明する書類
b）一旦提出された技術提案書及び入札書は、差し替え、変更または取り消しはできない。
c）開札日の前日までの間において、当機構から技術提案書に関し説明を求

められた場合には、定められた期日までにそれに応じること。
d）技術提案書等の作成、提出に係る費用については報酬を支払わない。
e）入札保証金は免除する。

３）技術提案書の無効
次の各号のいずれかに該当する技術提案書は無効とする。
a）提出期限後に提出されたとき。
b）提出された技術提案書に記名・押印がないとき。ただし、押印が困難な場合は、（３）３）を参照の上提出すること。
c）同一提案者から内容が異なる提案が２通以上提出されたとき。
d）虚偽の内容が記載されているとき（虚偽の記載をした技術提案書の提出者に対して契約競争参加資格停止等の措置を行うことがある）
e）前号に掲げるほか、本入札説明書に違反しているとき。

(13) 技術提案書内容に関するプレゼンテーションの実施
技術提案書のご提出後、提出全社に対して、以下のとおり、技術提案内容に関するプレゼンテーション実施を依頼する予定。プレゼンテーションはMicrosoft Teamsでの実施を予定している。
１）日時：別紙「手続・締切日時一覧」を参照すること。
２）実施方法：
参加者からのプレゼンテーション（説明）時間は２０分を上限とし、質疑応答の時間をあわせて、参加者あたり、４０分程度とする。プレゼンテーションの実施者は、原則、本件業務の総括者とすること。プレゼンテーションは、技術提案書内容の要約版の提示も可とするが、提出済みの技術提案書のみによる説明でもよい。

(14) 技術提案書の評価結果の通知
技術提案書は当機構において技術評価を行う。技術提案書を提出した全者に対し、別紙「手続・締切日時一覧」に則し、評価結果の合否をメールで通知する。通知期限までに結果が通知されない場合は、上記「（２）書類等の提出先」までメールで問い合わせること。

(15) 入札執行（入札会）日時等
当機構契約事務取扱細則第１４条第２項「前項に定める競争入札の執行における開札は、立会いによるものに代えて、インターネット上に設置する電子入札システムにより行うことができるものとする」を適用し、電子入札システムで入札を実施する。なお、再入札の場合は、発注者から再入札実施日時を通知するので、締切時間までに再入札書を電子入札システム上で提出すること。
また、締切時間までに再入札もしくは辞退の意思表示がなされない場合には失格となる。
１）入札開始日時：２０２３年１１月Ｘ日（X）１５時００分
２）再入札の実施
再入札の場合は、電子入札システムにより再入札の指示をするので、「（１７）

入札方法等」を参照すること。

(16) 入札書の失格

入札書受付締切日時までに入札書を提出しなかった場合（再入札時の場合も含む）には入札者を失格とする（入札者側の PC のトラブルによる場合も含む）。

(17) 入札方法

１）電子入札システムで入札を行う。

２）入札会の手順

a）開札

入札執行者は、開札時刻に電子入札システムにより開札し、入札結果を同システム上で入札者に開示する。再入札となる場合には再入札通知書を発行する。

b）再入札及び不落随意契約交渉

ァ）開札後、再入札が発生した際には入札者は電子入札システムにより再入札通知書に記載の入札書受付/締切日時、開札日時に従い、記載されている入札最低金額未満の金額で再入札書を提出する。

ィ）開札の結果、すべての入札金額が予定価格を超える場合には、ただちに２回目の再入札を行う。

ゥ）２回まで行っても落札者がないときは入札を打ち切り、不落随意契約の交渉に応じて頂く場合がある。

３）入札途中での辞退

「不調」の結果に伴い、再入札を辞退する場合は、「辞退」ボタンを選択して必要事項を記入の上、電子入札システム上で提出すること。

４）予定価格の範囲内で総合点（技術点と価格点の合計）が同点となった者が２者以上あるときは、抽選により落札者を決定する。その場合、入札書提出時にご入力いただいた任意の「くじ入力番号」をもとに、電子入札システムで自動的に抽選し落札者を決定する。

５）落札者と宣言された者の失格

落札者と宣言された者について、入札金額が著しく低い等、当該応札者と契約を締結することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められる場合には当該落札者を失格とし、改めて落札者を決定する場合がある。

(18) 入札書の無効

次の各号のいずれかに該当する入札は無効とする。

１）競争に参加する資格を有しない者のした入札

２）入札書締切日時後に到着した入札

３）明らかに連合によると認められる入札

４）同一入札者による複数の入札

５）その他入札に関する条件に違反した入札

６）条件が付されている入札

６ 本業務を実施する者を決定するための評価の基準その他本業務を実施する者の決定に関する事項

以下に本業務を実施する者の決定に関する事項を示す。なお、詳細は別添1「コンピュータシステム運用等業務 調達仕様書」と別添2「評価基準書」を参照すること。

(1) 評価方法

本業務を実施する者の決定は、総合評価落札方式（加算方式）によるものとする。

また、総合評価は、価格点（入札価格の得点）に技術点（評価基準書に基づく点数）を加えて得た数値（以下「総合評価点」という。）をもって行う。

価格点と技術点の配分

価格点の配分：技術点の配分　＝　１：2

総合評価点　＝　価格点（100点満点）　＋　技術点（200点満点）

(2) 総合評価点

１）技術評価

別添1「(独)国際協力機構コンピュータシステム運用等業務 業務仕様書」と別添2「評価基準書」に基づき、以下の基準により評価（小数点以下第三位を四捨五入する）し、合計点を技術評価点とする。。

当該項目の評価	評価点
当該項目については極めて優れており、高い付加価値がある業務の履行が期待できるレベルにある。	９０%以上
当該項目については優れており、適切な業務の履行が十分期待できるレベルにある。	９０%未満 ８０%以上
当該項目については一般的な水準に達しており、業務の履行が十分できるレベルにある。	８０%未満 ７０%以上
当該項目については必ずしも一般的なレベルに達していないが、業務の履行は可能と判断されるレベルにある。	７０%未満 ５０%以上
当該項目だけで判断した場合、業務の適切な履行が困難であると判断されるレベルにある。	５０%未満

なお、技術評価点が５０%、つまり２００点満点中１００点（「基準点」という。）を下回る場合を不合格とする。不合格となった場合は、「１０．技術提案書の評価結果の通知」に記載の手続きに基づき、不合格であることが通知され、入札会には参加できない。

また、Work Life Balance (WLB)等推進企業（女性活躍推進法、次世代育成支援対策推進法、青少年の雇用の促進等に関する法律に基づく認定企業や、一般事業主行動計画策定企業）への評価については、別添2「評価基準書」を参照。

２）価格評価

価格評価点については以下の評価方式により算出する。算出に当たっては、小数点以下第三位を四捨五入する。
価格評価点＝（予定価格－入札価格）／予定価格×（１００点）

３）総合評価
技術評価点と価格評価点を合計した値を総合評価点とする。

⑶ 落札者の決定
機構が設定した予定価格を超えない入札金額を応札した者のうち、総合評価点が最も高い者を落札者とする。なお、落札者となるべき総合評価点の者が２者以上あるときは、抽選により落札者を決定する。落札者は、入札金額の内訳書（社印不要）をメールで提出すること。

⑷ 落札者と宣言された者の失格
入札会において上述の落札者の決定方法に基づき落札者と宣言された者について、入札会の後に、以下の条件に当てはまると判断された場合は、当該落札者を失格とし、改めて落札者を確定する。
１）その者が提出した技術提案書に不備が発見され、上述の５．⑿３）に基づき「無効」と判断された場合
２）その者が提出した入札書に不備が発見され、５．⑱に基づき「無効」と判断された場合
３）入札金額が著しく低い等、当該応札者と契約を締結することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められる場合

⑸ 落札決定の取消し
次の各号のいずれかに該当するときは、落札者の決定を取り消す。ただし、当機構が、正当な理由があると認めたときはこの限りでない。
1） 落札者が、当機構から求められたにもかかわらず契約書の取り交わしを行わない場合
2） 入札書の内訳金額と合計金額が符合しない場合
落札後、入札者に内訳書を記載させる場合がある。内訳金額が合計金額と符合しないときは、合計金額で入札したものとみなすため、内訳金額の補正を求められた入札者は、直ちに合計金額に基づいてこれを補正しなければならない。
3） 落札者決定前に、落札者予定者についての暴力団排除条項該当性の有無について警察庁刑事局組織判事対策部暴力団対策課（以下「暴力団対策課」という）に対し意見聴取を行う。このため、落札予定者は暴力団排除条項等の欠格事由審査に必要な書類について別途提出すること。なお、暴力団対策課から「暴力団排除条項に該当する」旨の回答があった場合には、機構は当該落札予定者による入札を無効とする。

⑹ 落札者が決定しなかった場合の措置
初回の入札において入札参加者がなかった場合、必須項目を全て満たす入

札参加者がなかった場合又は再度の入札を2回まで行ってもなお落札者が決定しなかった場合は、当該競争に付するときに定めた予定価格その他の条件を変更せずに随意契約の交渉を行い、契約金額が予定価格を超えない範囲内で契約交渉が成立した場合、契約を締結する。随意契約交渉が成立しなかった場合は、原則として、入札条件等を見直した後、再度公告を行う。

なお、再度の入札によっても落札者となるべき者が決定しない場合又は本業務の実施に必要な期間が確保できないなどやむを得ない場合は、別途、当該業務の実施方法を検討・実施することとし、その理由を官民競争入札等監理委員会（以下、「監理委員会」という。）に報告するとともに公表するものとする。

(7) 契約書の作成及び締結

１）落札者は電子署名による契約を締結することを基本とし、「契約書（案）」に基づき、速やかに契約書を作成し、電子署名により締結する。なお、書面による契約を希望する場合は落札後発注者へ照会すること。

２）契約条件、条文については、「契約書（案）」を参照すること。なお契約書（案）の文言に質問等がある場合は、「５．(10)入札説明書に対する質問」の際に併せて照会すること。

３）契約保証金は免除する。

４）契約書附属書Ⅱ「契約金額内訳書」については、入札金額の内訳書等の文書に基づき、両者協議・確認して設定する。

７　本業務に関する従来の実施状況に関する情報の開示に関する事項

(1) 開示情報

対象業務に関して、以下の情報は別紙 1「従来の実施状況に関する情報の開示」のとおり開示する。

ア　従来の実施に要した経費
イ　従来の実施に要した人員
ウ　従来の実施に要した施設及び設備
エ　従来の実施における目標の達成の程度
オ　従来の実施方法等

(2) 資料の閲覧

前項オ「従来の実施方法等」の詳細な情報は、民間競争入札に参加する予定の者から要望があった場合、運用設計資料等について、所定の手続を踏まえた上で閲覧可能とする。

また、民間競争入札に参加する予定の者から追加の資料の開示について要望があった場合は、当機構は法令及び機密性等に問題のない範囲で適切に対応するよう努めるものとする。

８　受託事業者に使用させることができる当機構の施設・設備等に関する事項

(1) 財産の使用

受注者は、本業務の遂行に必要な施設、設備等として、次に掲げる施設、設備等を適切な管理の下、無償で使用することができる。

ア　常駐施設内において業務に必要な電気、ネットワーク設備

イ　その他、当機構と協議し承認された業務に必要な施設、設備等

(2) 使用制限

ア　受注者は、本業務の実施及び実施に付随する業務以外の目的で使用し、又は利用してはならない。

イ　受注者は、あらかじめ当機構と協議した上で、当機構の業務に支障を来さない範囲内において、施設内に運用管理業務の実施に必要な設備等を持ち込むことができる。

ウ　受注者は、設備等を設置した場合は、設備等の使用を終了又は中止した後、直ちに、必要な原状回復を行う。

エ　受注者は、既存の建築物及び工作物等に汚損・損傷等を与えないよう十分に注意し、損傷（機器の故障等を含む。）が生じるおそれのある場合は、養生を行う。万一損傷が生じた場合は、受注者の責任と負担において速やかに復旧するものとする。

９　受託事業者が、当機構に対して報告すべき事項、秘密を適正に取り扱うために必要な措置その他の本業務の適正かつ確実な実施の確保のために本業務受注者が講じるべき措置に関する事項

(1) 本業務受注者が当機構に報告すべき事項、当機構の指示により講じるべき措置

ア　報告等

(ｱ) 受注者は、仕様書に規定する業務を実施したときは、当該仕様書に基づく各種報告書を当機構に提出しなければならない。

(ｲ) 受注者は、受託業務を実施したとき、又は完了に影響を及ぼす重要な事項の変更が生じたときは、直ちに当機構に報告するものとし、当機構と受注者が協議するものとする。

(ｳ) 受注者は、契約期間中において、(ｲ)以外であっても、必要に応じて当機構から報告を求められた場合は、適宜、報告を行うものとする。

イ　調査

(ｱ) 当機構は、受託業務の適正かつ確実な実施を確保するために必要があると認めるときは、法第 26 条第１項に基づき、受注者に対し必要な報告を求め、又は当機構の職員が事務所に立ち入り、当該業務の実施の状況若しくは記録、帳簿書類その他の物件を検査し、又は関係者に質問することができる。

(ｲ) 立入検査をする当機構の職員は、検査等を行う際には、当該検査が法第 26 条第１項に基づくものであることを受注者に明示するとともに、その身分を示す証明書を携帯し、関係者に提示するものとする。

ウ　指示

(ｱ)　当機構は、受託業務の適正かつ確実な実施を確保するために必要と認めるときは、受注者に対し、必要な措置を採るべきことを指示することができる。

(ｲ)当機構は、利用者満足度調査（アンケート等）を通じた各種クレームやトラブルの対応報告等により、関連の業務が適切なものであるかの確認を行い、不適切と判断する場合には、実施方法の変更を求める。

⑵ 秘密を適正に取り扱うために必要な措置

ア　受注者は、本業務の実施に際して知り得た当機構の情報等（公知の事実等を除く）を、第三者に漏らし、盗用し、又は受託業務以外の目的のために利用してはならない。これらの者が秘密を漏らし、又は盗用した場合は、法第 54 条により罰則の適用がある。

イ　受注者は、本業務の実施に際して得られた情報処理に関する利用技術（アイデア又はノウハウ）については、受注者からの文書による申出を当機構が認めた場合に限り、第三者へ開示できるものとする。

ウ　受注者は、当機構から提供された個人情報及び業務上知り得た個人情報について、個人情報の保護に関する法律（平成 15 年法律第 57 号）に基づき、適切な管理を行わなくてはならない。また、当該個人情報については、本業務以外の目的のために利用してはならない。

エ　受注者は、当機構の情報セキュリティに関する規程等に基づき、個人情報等を取り扱う場合は、①情報の複製等の制限、②情報の漏えい等の事案の発生時における対応、③受託業務終了時の情報の消去・廃棄（復元不可能とすること。）及び返却、④内部管理体制の確立、⑤情報セキュリティの運用状況の検査に応じる義務、⑥受注者の事業責任者及び受託業務に従事する者全てに対しての守秘義務及び情報セキュリティ要求事項の遵守に関して、当機構の規定する誓約書への署名を遵守しなければならない。

オ　アからエまでのほか、当機構は、受注者に対し、本業務の適正かつ確実な実施に必要な限りで、秘密を適正に取り扱うために必要な措置を採るべきことを指示することができる。

⑶ 契約に基づき受注者が講じるべき措置

ア　受託業務開始

受注者は、本業務の開始日から確実に業務を開始すること。

イ　権利の譲渡

受注者は、債務の履行を第三者に引き受けさせ、又は契約から生じる一切の権利若しくは義務を第三者に譲渡し、承継せしめ、若しくは担保に供してはならない。ただし、書面による当機構の事前の承認を得たときは、この限りではない。

ウ　権利義務の帰属等

(ｱ) 本業務の実施が第三者の特許権、著作権その他の権利と抵触するときは、受注者は、その責任において、必要な措置を講じなくてはならない。

(ｲ) 受注者は、本業務の実施状況を公表しようとするときは、あらかじめ、当機構の承認を受けなければならない。

エ　契約不適合責任

(ｱ) 当機構は、受注者に対し、引き渡された成果物が種類又は品質に関して契約の内容に適合しないものである場合（その不適合が当機構の指示によって生じた場合を除き、受注者が当該指示が不適当であることを知りながら、又は過失により知らずに告げなかった場合を含む。）において、その不適合を当機構が知った時から起算して 1 年以内にその旨の通知を行ったときは、その成果物に対する修補等による履行の追完を請求することができる。ただし、受注者は、当機構に不相当な負担を課するものでないときは、当機構が請求した方法と異なる方法による履行の追完を

することができる。

(ｲ) (ｱ)の場合において、当機構が相当の期間を定めて履行の追完の催告をし、その期間内に履行の追完がないときは、当機構は、その不適合の程度に応じて代金の減額を請求することができる。

(ｳ) (ｱ)又は(ｲ)の場合において、当機構は、損害賠償を請求することができる。

オ　再委託

(ｱ) 受注者は、本業務の実施に当たり、その全部を一括して再委託してはならない。

(ｲ) 受注者は、本業務の実施に当たり、その一部について再委託を行う場合には、原則として、あらかじめ書面において、再委託先に委託する業務の範囲、再委託を行うことの合理性及び必要性、再委託先の履行能力並びに報告徴収、個人情報の管理その他運営管理の方法（以下「再委託先等」という。）について記載しなければならない。

(ｳ) 受注者は、契約締結後やむを得ない事情により再委託を行う場合には、再委託先等を明らかにした上で、当機構の承認を受けなければならない。

(ｴ) 受注者は、(ｲ)又は(ｳ)により再委託を行う場合には、受注者が当機構に対して負う義務を適切に履行するため、再委託先の事業者に対し前項「(2)秘密を適正に取り扱うために必要な措置」及び本項「(3)契約に基づき受注者が講じるべき措置」に規定する事項その他の事項について、必要な措置を講じさせるとともに、再委託先から必要な報告を聴取することとする。

(ｵ) (ｲ)から(ｴ)までに基づき、受注者が再委託先の事業者に義務を実施させる場合は、全て受注者の責任において行うものとし、再委託先の事業者の責に帰すべき事由については、受注者の責に帰すべき事由とみなして、受注者が責任を負うものとする。

カ　契約内容の変更

当機構及び受注者は、本業務の質の確保の推進、またはその他やむをえない事由により本契約の内容を変更しようとする場合は、あらかじめ変更の理由を提出し、それぞれの相手方の承認を受けるとともに、法第２１条の規定に基づく手続きを適切に行わなければならない。

キ　機器更新等の際における受注者への措置

当機構は、次のいずれかに該当するときには、受注者にその旨を通知するとともに、受注者と協議の上、契約を変更することができる。

(ｱ) 当機構の IT 環境に大幅な変更が生じた場合

(ｲ) 当機構の組織、制度、及び IT 環境等設備の変更、情報セキュリティ対策の強化等の事由により、本業務の実施内容に変更の必要性が生じた場合。

ク　契約の解除

当機構は、受注者が次のいずれかに該当するときは、受注者に対し受託費の支払を停止し、又は契約を解除若しくは変更することができる。この場合、当機構に損害が生じたときは、受注者は当機構に生じた損害を賠償する責任を負う。また、以下(ｱ)～(ｽ)の規定により、受注者は当機構に対

して、契約金額の 100 分の 10 に相当する金額を違約金として支払わなければならない。その場合の算定方法については、当機構の定めるところによる。ただし、同額の超過する増加費用及び損害が発生したときは、超過分の請求を妨げるものではない。

また、受注者は、当機構との協議に基づき、本業務の処理が完了するまでの間、責任を持って当該処理を行わなければならない。

(ｱ)偽りその他不正の行為により落札者となったとき。(下記ケ　談合等不正行為の場合を除く。)

(ｲ)　法第 14 条第 2 項第 3 号又は第 15 条において準用する第 10 条（第 11 号を除く。)の規定により民間競争入札に参加する者に必要な資格の要件を満たさなくなったとき。

(ｳ) 契約に沿った委託業務を実施できなかったとき、またはこれを実施することができないことが明らかになったとき。

(ｴ)（ｳ）に掲げる場合のほか契約において定められた事項について重大な違反があったとき。

(ｵ) 法令または契約に基づく報告をせず、若しくは虚偽の報告をし、または検査を拒み、妨げ、若しくは忌避し、若しくは質問に対して答弁せず、若しくは虚偽の答弁をしたとき。

(ｶ)法令または契約に基づく指示(本実施要領に掲げる措置を履行しなかった場合を含む。）に違反したとき。

(ｷ)民間事業者またはその役職員その他委託業務に従事する者が、法令または契約に違反して、委託業務の実施に関して知り得た秘密を漏らしまたは盗用した場合。

(ｸ)暴力団員を、業務を統括する者または従業員としていることが明らかになった場合。

(ｹ)暴力団または暴力団関係者と社会的に非難されるべき関係を有していることが明らかになった場合。

(ｺ)他から執行保全処分、強制執行、競売処分、租税滞納処分、その他公権力による処分を受け、若しくは特別清算、会社更生手続、民事再生手続、破産又は私的整理手続を申し立てられ、又は自らそれらのもの、若しくは再生手続開始の申立てをしたとき。

(ｻ)民間事業者が手形交換所から手形不渡処分を受けたとき。

(ｼ)資産状態が悪化し、又はそのおそれがあると認めるに足る相当の理由があるとき。

(ｽ)民間事業者が下記ケ　談合等不正行為に規定したいずれかの事項に該当するものとして機構から不正行為に係る違約金の請求をうけたとき。

ケ　談合等不正行為

受注者は、次のいずれかに該当したときは、機構の請求に基づき、契約金額の 100 分の 10 に相当する額を談合等不正行為に係る違約金として支払わなければならない。

(ｱ)本委託業務の契約に関し、私的独占の禁止及び公正取引の確保に関する法律（昭和 22 年法律第 54 号）第 3 条の規定に違反し、又は受注者が構成事業者である事業者団体が同法第 8 条第 1 項第 1 号の規定に違反したことにより、公正取引委員会が民間事業者に対し、同法第 7 条の 2 第 1 項の規

定に基づく課徴金の納付命令を行い、当該納付命令が確定したとき。
(ｲ)本委託業務の契約に関し、受注者（法人にあたっては、その役員又は使用人を含む。）の刑法（明治 40 年法律第 45 号）第 96 条の 6 又は私的独占の禁止及び公正取引の確保に関する法律第 89 条第 1 項若しくは第 95 条第 1 項第 1 号に規定する刑が確定したとき。

コ　損害賠償

受注者は、受注者の故意又は過失により当機構に損害を与えたときは、当機構に対し、その損害について賠償する責任を負う。また、当機構は、契約の解除及び違約金の徴収をしてもなお損害賠償の請求をすることができる。なお、当機構から受注者に損害賠償を請求する場合において、原因を同じくする支払済の違約金がある場合には、当該違約金は原因を同じくする損害賠償について、支払済額とみなす。

サ　不可抗力免責・危険負担

当機構及び受注者の責に帰すことのできない事由により契約期間中に物件が滅失し、委託業務の全部又は一部の実施が遅滞したり、不能となったりした場合は責任を負わない。

シ　金品等の授受の禁止

受注者は、本業務の実施において、金品等を受け取ること、又は、与えることをしてはならない。

ス　宣伝行為の禁止

受注者及び本業務に従事する者は、本業務の実施に当たっては、自ら行う業務の宣伝を行ってはならない。また、本業務の実施をもって、第三者に対し誤解を与えるような行為をしてはならない。

セ　法令の遵守

受注者は、本業務を実施するに当たり適用を受ける関係法令等を遵守しなくてはならない。

ソ　安全衛生

受注者は、本業務に従事する者の労働安全衛生に関する労務管理については、責任者を定め、関係法令に従って行わなければならない。

タ　記録及び帳簿類の保管

受注者は、本業務に関して作成した記録及び帳簿類を、本業務を終了し、又は中止した日の属する年度の翌年度から起算して 5 年間、保管しなければならない。

チ　契約の解釈

契約に定めのない事項及び契約に関して生じた疑義は、当機構と受注者との間で協議して解決する。

10　受注者が本業務を実施するに当たり第三者に損害を加えた場合において、その損害の賠償に関し契約により本業務受注者が負うべき責任に関する事項

本業務を実施するに当たり、受注者又はその職員その他の本業務に従事する者が、故意又は過失により、本業務の受益者等の第三者に損害を加えた場合は、次のとおりとする。

(1) 当機構が国家賠償法第 1 条第 1 項等の規定に基づき当該第三者に対する賠償を行ったときは、当機構は受注者に対し、当該第三者に支払った損害賠償額

（当該損害の発生について当機構の責めに帰すべき理由が存する場合は、当機構が自ら賠償の責めに任ずべき金額を超える部分に限る。）について求償することができる。

⑵ 受注者が民法第 709 条等の規定に基づき当該第三者に対する賠償を行った場合であって、当該損害の発生について当機構の責めに帰すべき理由が存するときは、受注者は当機構に対し、当該第三者に支払った損害賠償額のうち自ら賠償の責めに任ずべき金額を超える部分を求償することができる。

11 法第７条第８項に規定する評価に関する事項

⑴ 本業務の実施状況に関する調査の時期

当機構は、本業務の実施状況について、総務大臣が行う評価の時期（令和9年7月を予定）を踏まえ、本業務開始後、毎年5（終了月）月に状況を調査する。

⑵ 調査項目及び実施方法

ア　SLA基準値達成状況

報告書等により調査

イ　利用満足度調査の結果

各年度において、ユーザに対する年１回のアンケートの実施結果により調査

ウ　セキュリティ上の重大障害の件数

報告書等により調査

⑶ 意見聴取等

当機構は、必要に応じ、本業務受注者から意見の聴取を行うことができるものとする。

⑷ 実施状況等の提出時期

当機構は、令和9年7月を目途として、本業務の実施状況等を総務大臣及び監理委員会へ提出する。

12　その他業務の実施に関し必要な事項

⑴ 実施状況等の監理委員会への報告

当機構は、法第26条及び第27条に基づく報告徴収、立入検査、指示等を行った場合には、その都度、措置の内容及び理由並びに結果の概要を監理委員会へ報告することとする。

⑵ 当機構の監督体制

ア　本契約に係る監督は、主管係自ら立会い、指示その他の適切な方法によって行うものとする。

本業務の実施状況に係る監督は以下のとおり。

監督職員：情報システム部システム第一課長

検査職員：情報システム部長

イ　実施要項に基づく民間競争入札手続きに係る監督は、調達部が行い、調達部契約担当次長を責任者とする。

⑶ 本業務受注者の責務

ア　受注者は、法第54 条の規定に該当する場合は、１年以下の懲役又は50

万円以下の罰金に処される。

イ　受注者は、法第55条の規定に該当する場合は、30万円以下の罰金に処されることとなる。なお、法第56条により。法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関し、法第55条の規定に違反したときは、行為者を罰するほか、その法人又は人に対して同条の刑を科する。

ウ　受注者は、会計検査院法（昭和22年法律第73号）第23条第１項第７号に規定する者に該当することから、会計検査院が必要と認めるときには、同法第25条及び第26条により、同院の実地の検査を受けたり、同院から直接又は当機構に通じて、資料又は報告等の提出を求められたり、質問を受けたりすることがある。

(4) 著作権

ア　受注者は、本業務の目的として作成される成果物に関し、著作権法第27条及び第28条を含む著作権の全てを当機構に無償で譲渡するものとする。

イ　受注者は、成果物に関する著作者人格権（著作権法第18条から第20条までに規定された権利をいう。）を行使しないものとする。ただし、当機構が承認した場合は、この限りではない。

ウ　ア及びイに関わらず、成果物に受注者が既に著作権を保有しているもの（以下「受注者著作物」という。）が組み込まれている場合は、当該受注者著作物の著作権についてのみ、受注者に帰属する。

エ　提出される成果物に第三者が権利を有する著作物が含まれる場合には、受注者が当該著作物の使用に必要な費用の負担及び使用許諾契約等に係る一切の手続きを行うものとする。

(5) 本業務の調達仕様書

本業務を実施する際に必要な仕様は、別添1「コンピュータ運用等業務調達仕様書」に示すとおりである。

以上

この表は、民間競争入札に使用

別紙1

従来の実施状況に関する情報の開示

1　従来の実施に要した経費

（単位：千円）

		令和1年度	令和2年度	令和3年度
請負費等	役務	1,103,661	1,094,334	1,274,634
請負費等	機器・回線等料	250,847	257,447	257,447
請負費等	その他	158,615	161,037	161,037
計(a)		1,513,123	1,512,818	1,693,118

※必要に応じて項目を追加

・平成27年度（2015年度）に一般競争入札（総合評価落札方式）により契約締結。
・民間競争入札の対象である「コンピュータシステム運用等業務」の全部を請負契約により実施。
・上記記載金額は「コンピュータシステム運用等業務（運用フェーズ）」の契約書に記載の年度別支払計画額（税抜、千円未満切捨）より算出。
・令和3年度の「役務」の主な増額理由は「第612回入札監理小委員会（令和3年2月19日）」で審議・承認されたクラウドサービスの運用追加によるもの。
【委員の指摘事項】
・業務の再編等により従来と業務内容の変更がある場合、経費の見積りに資するよう、対象となる業務範囲や業務量の変更点を記載する必要がある。
→現行契約変更契約時の契約書調達仕様書等において業務変更内容を記載しており、同内容は調達手続き時に閲覧資料として準備予定。

2　従来の実施に要した人員

（単位：人）

	令和1年度	令和2年度	令和3年度
（受託者におけるコンピュータ運用業務従事者）			
コンピュータ運用責任者(常駐)	3	2	2
ヘルプデスク	12	16	17
運用員(常駐)	40	43	45
運用員(非常駐)	5	8	8

（業務従事者に求められる知識・経験等）
コンピュータ運用責任者（2人）
　・5年以上のシステム運用業務経験を有すること
ヘルプデスク（17人）
　日本語並びに英語によるコミュニケーションを充分に取ることができること（TOEICスコア800点以上を有する・英語によるヘルプデスク受付経験がある、等）
運用員（常勤：45人）
　・SharePointおよび関連製品の運用保守業務について1年以上の実績を有していること
　・マイクロソフト認定プログラム（MCTS）等本業務内容を実施するための有益な資格等を有していることが望ましい
【委員の指摘事項】
・端末切換や人事異動時の繁忙期に臨時の人員追加で対応する事が一般的であるが、その人員も含めた延べ人数の記載としたり、非常駐の運用員が従事していることのみを記載したため、実態がわからないという指摘があった。人員追加が常態化しているような場合においては、常駐と非常駐の内訳を示すとともに、非常駐者については延べ人数ではなく、人員追加した延べ日数を20日/月で割って人員数を記載するなど、実際に要した人員がわかる記載とすること。
（例）4月、5月に5人追加人員を投入した場合　40日の人員投入×5 ＝200人日÷240日（年）＝　0.8人（年）を実施に要した人員（非常駐）に追加
→人員追加が常態化している状況にない。

人事異動月および前月に発生する業務（**注記事項参照**）

（令和1年度）　（件）

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	計

（令和2年度）													
	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	計
（令和3年度）													
	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	計

（注記事項）
当機構は基本的に毎月人事発令・異動が行われるため、特定の月における人事異動による業務量の大きな変化はない
【委員の指摘事項】
開示は件数だけでなく、稼働時間がわかれば時間も表として付けること。また、時間だけの掲載の場合については、件数が出せる項目がある場合は、件数の表を付けること。

3 従来の実施に要した施設及び設備

本省
【施設】
施設名称：二番町センタービル（東京都千代田区二番町5-25）
使用場所：二番町センタービル5階情報システム部分室（機構が提供している常駐用スペース）
【設備】
機構貸与
プリンター2台、OAデスク20台、キャビネット7台、椅子20脚、電話3台

請負者所有
OAデスク10台、椅子10脚、ノートPC100台、シュレッダー2台、空気清浄機10台

外部拠点
・竹橋合同ビル8階会議室（東京都千代田区大手町1-4-1、機構竹橋本部用に「竹橋ヘルプデスク」を設置）

4 従来の実施における目的の達成の程度

	令和1年度		令和2年度		令和3年度	
	目標・計画	実績	目標・計画	実績	目標・計画	実績
通報時間順守率（基盤系システム）	90.0%	100.0%	90.0%	100.0%	90.0%	通報対象なし
一次窓口解決率	80.0%	83.7%	80.0%	88.2%	80.0%	93.6%
回答目標時間順守率	80.0%	82.2%	80.0%	82.6%	80.0%	86.1%
呼損率	10.0%	1.5%	10.0%	1.5%	10.0%	2.9%
稼働率	99.9%	100.0%	99.9%	100.0%	99.9%	100.0%

利用者満足度	80.0%	87.4%	80.0%	84.6%	80.0%	80.3%

（注記事項）
・「利用者満足度」は利用者満足度調査の結果に基づく。
【委員の指摘事項】
・従前の事業で目的の達成度を設定していない場合でも、各種報告書から記載出来る部分があれば記載のこと。
→主要な事業内容について「目的の達成度を設定していない場合」に該当するものがない（現行事業では主要な事業内容をServie Level Agreement（SLA)に基づき定量的な目標を定めて評価することとしているため）。
・従前の事業における実績値を記載できない場合は、それを類推できる資料（現行事業者からの月次報告書、障害報告書等）の閲覧を認める等の対応を行うこと。
→上記に同じ。

5 従来の実施方法等

従来の実施方法（業務フロー図等）

別紙1 コンピュータシステム運用等業務のフロー
別紙2 機構組織図

（注記事項）

2017年度下期 利用者満足度調査

別紙2

国際協力機構コンピュータシステム運用等業務におけるヘルプデスクに関する利用者満足度調査（サンプル）

#	回答形態	形式	質問	回答群
0．回答者情報				
1	必須	記述	あなたのメールアドレスを入力してください。	
2	必須	記述	あなたの部署名・拠点名を教えてください。	
1．問合せ対応（電話・メール）について				
3	必須	選択	電話での案内のわかりやすさについて、満足度を教えてください。	満足 やや満足 やや不満 不満 利用したことがないため、分からない
4	必須	選択	電話での案内にかかる時間について、満足度を教えてください。	満足 やや満足 やや不満 不満 利用したことがないため、分からない
5	必須	選択	メールでの案内のわかりやすさについて、満足度を教えてください。	満足 やや満足 やや不満 不満 利用したことがないため、分からない
6	必須	選択	メールでの案内にかかる時間について、満足度を教えてください。	満足 やや満足 やや不満 不満 利用したことがないため、分からない
7	自由	記述	メールおよび電話での案内内容や時間について、ご要望やご意見があればご自由にご記載ください。	
2．申請対応について				
8	必須	選択	申請をする際の申請ルールや事前説明のわかりやすさについて、満足度を教えてください。	満足 やや満足 やや不満 不満 利用したことがないため、分からない
9	必須	選択	申請に関するヘルプデスクの対応時間について、満足度を教えてください。	満足 やや満足 やや不満 不満 利用したことがないため、分からない
10	自由	記述	申請に関する事前説明や対応時間について、ご要望やご意見があればご自由にご記載ください。	
3．ヘルプデスクからの周知（執務参考資料・マニュアル・お知らせ・ヘルプデスクニュース）について				
11	必須	選択	FAQと執務参考資料（マニュアル）の分かりやすさについて、満足度を教えてください。	満足 やや満足 やや不満 不満 利用したことがないため、分からない
12	必須	選択	お知らせ・ヘルプデスクニュースの分かりやすさについて、満足度を教えてください。	満足 やや満足 やや不満 不満 利用したことがないため、分からない

2017年度下期 利用者満足度調査

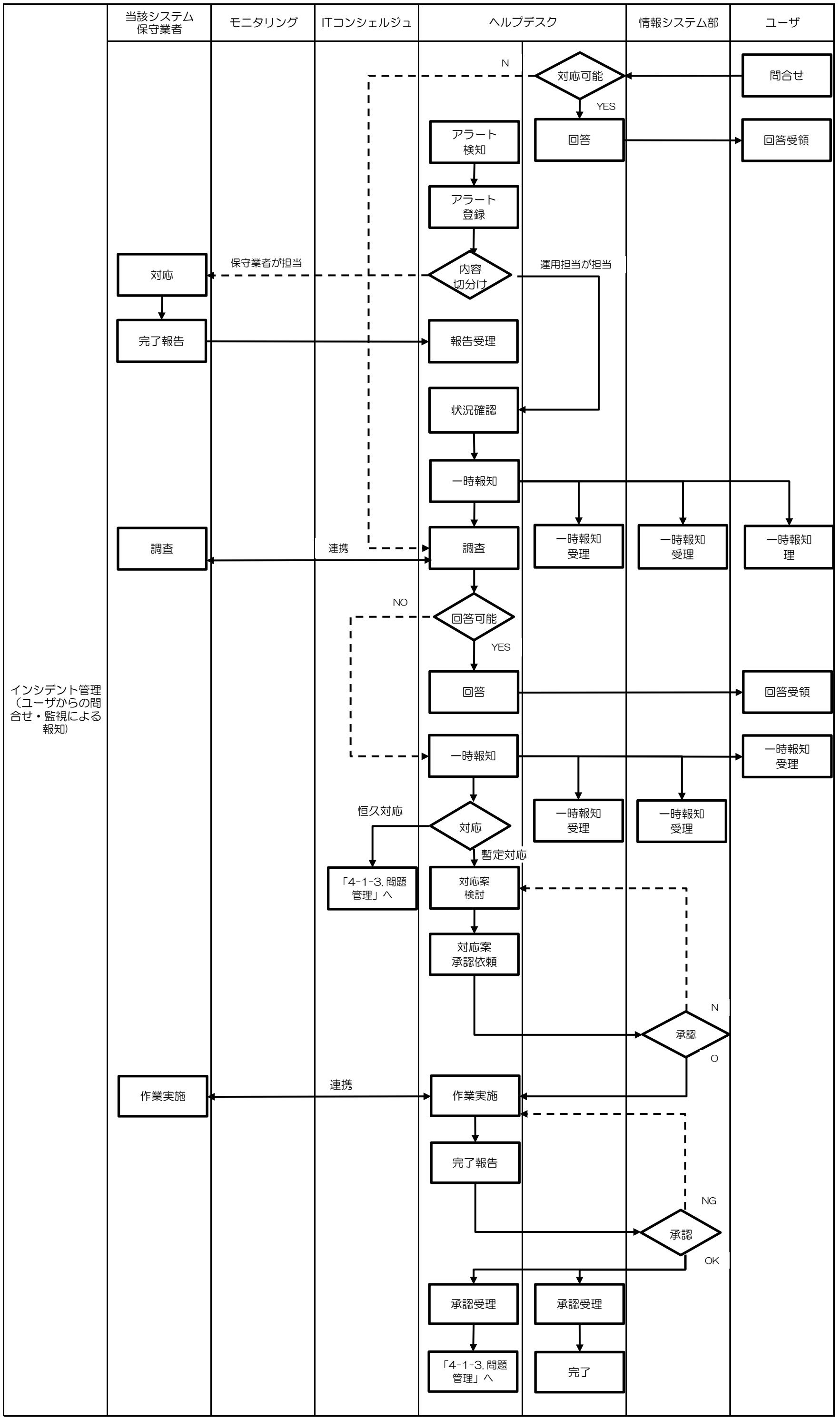
国際協力機構コンピュータシステム運用等業務におけるヘルプデスクに関する利用者満足度調査（サンプル）

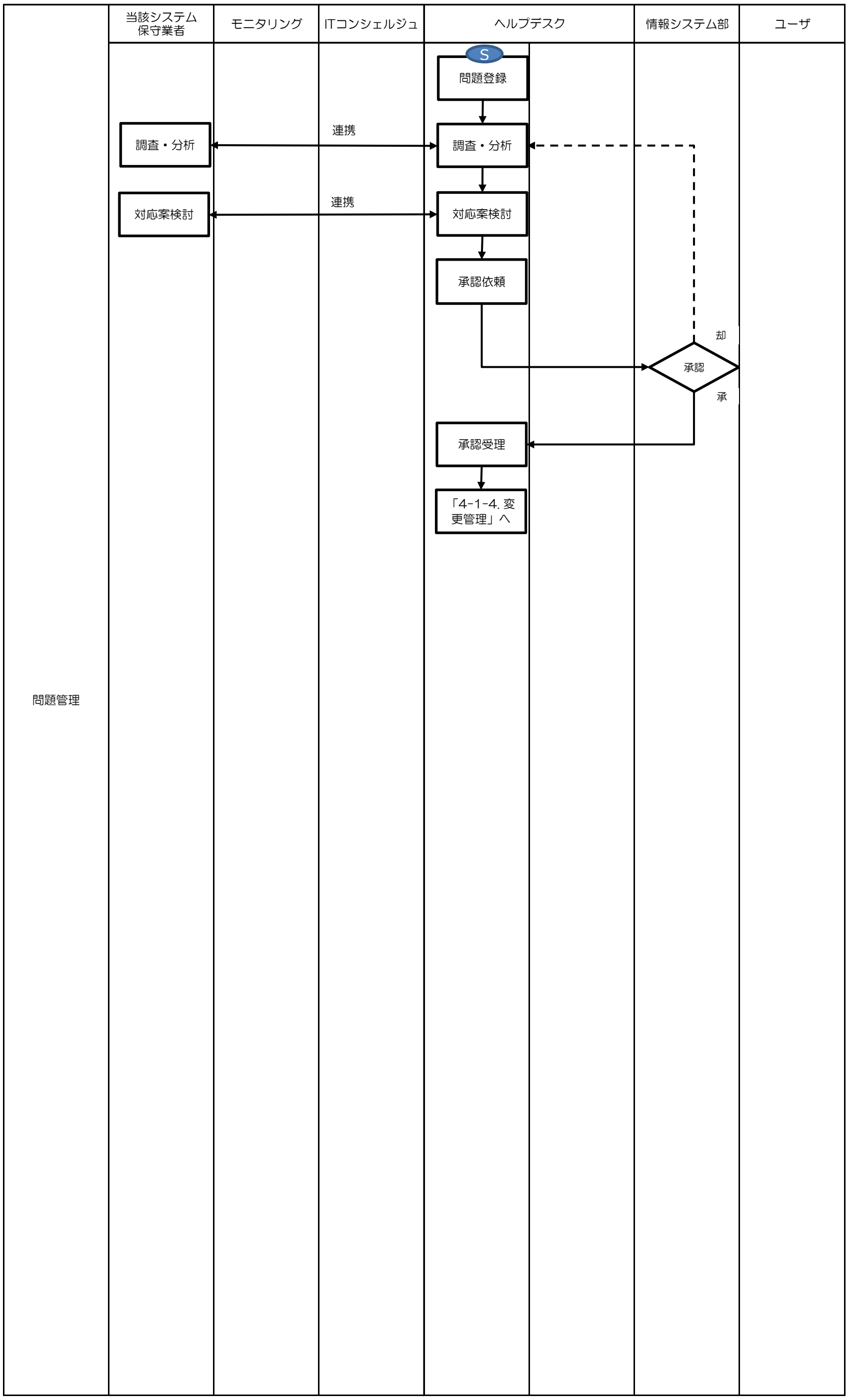
#	回答形態	形式	質問	回答群
13	自由	記述	執務参考資料・FAQやお知らせについて、ご要望やご意見があればご自由にご記載ください。	
4．クラウド関連ツール（Outlook、Teams、OneDrive、SharePoint等）の利用状況について				
14	自由	選択	【共通】 セルフパスワードロック解除を利用したことがありますか	はい 知っているが、利用したことがない 知らない
15	自由	選択	【SharePoint】 「情報システム部ポータル」を利用したことありますか。	はい 知っているが、利用したことがない 知らない
16	自由	選択	【SharePoint】 「情報システムクラウド化ポータル」を利用したことありますか。	はい 知っているが、利用したことがない 知らない
17	自由	選択	【SharePoint】 「デバイスポータル」を利用したことありますか。	はい 知っているが、利用したことがない 知らない
18	自由	記述	【SharePoint】 （15,16,17のいずれかで「はい」と回答した方のみ）ご要望やご意見があればご自由にご記載ください。	
5．クラウド関連（Outlook、Teams、OneDrive等）及びSharePointの満足度について				
19	自由	選択	クラウド関連ツール（Outlook、Teams、OneDrive、SharePoint等）で便利と感じている機能を教えてください。（複数選択可能）	メール機能（Outlook） 会議室予約（Outlook） 機材予約（Outlook） TV会議設備予約（Outlook） インスタントメッセージ（Teams） 電話会議・ビデオ通話（Teams） ストレージ（個人用OneDrive） ストレージ（部署OneDrive） 執務参考資料（JICA Navigation） 準内部規定（JICA Navigation） お知らせ（JICA Navigation） 個人用サイト（JICA Navigation） Newsfeed JICA Navigation） Discussion Board（JICA Navigation） プロジェクトポータル（JICA Navigation） アンケート機能（JICA Naviagtion） 個人用サイト・ブログ（JICA Navigation） 動画マニュアル（SharePointOnline移行ポータル） 特になし
20	自由	選択	情報システム クラウド化ポータルに掲載されている動画マニュアルについて、満足度を教えてください。	満足 やや満足 やや不満 不満 利用したことがないため、分からない

2017年度下期 利用者満足度調査

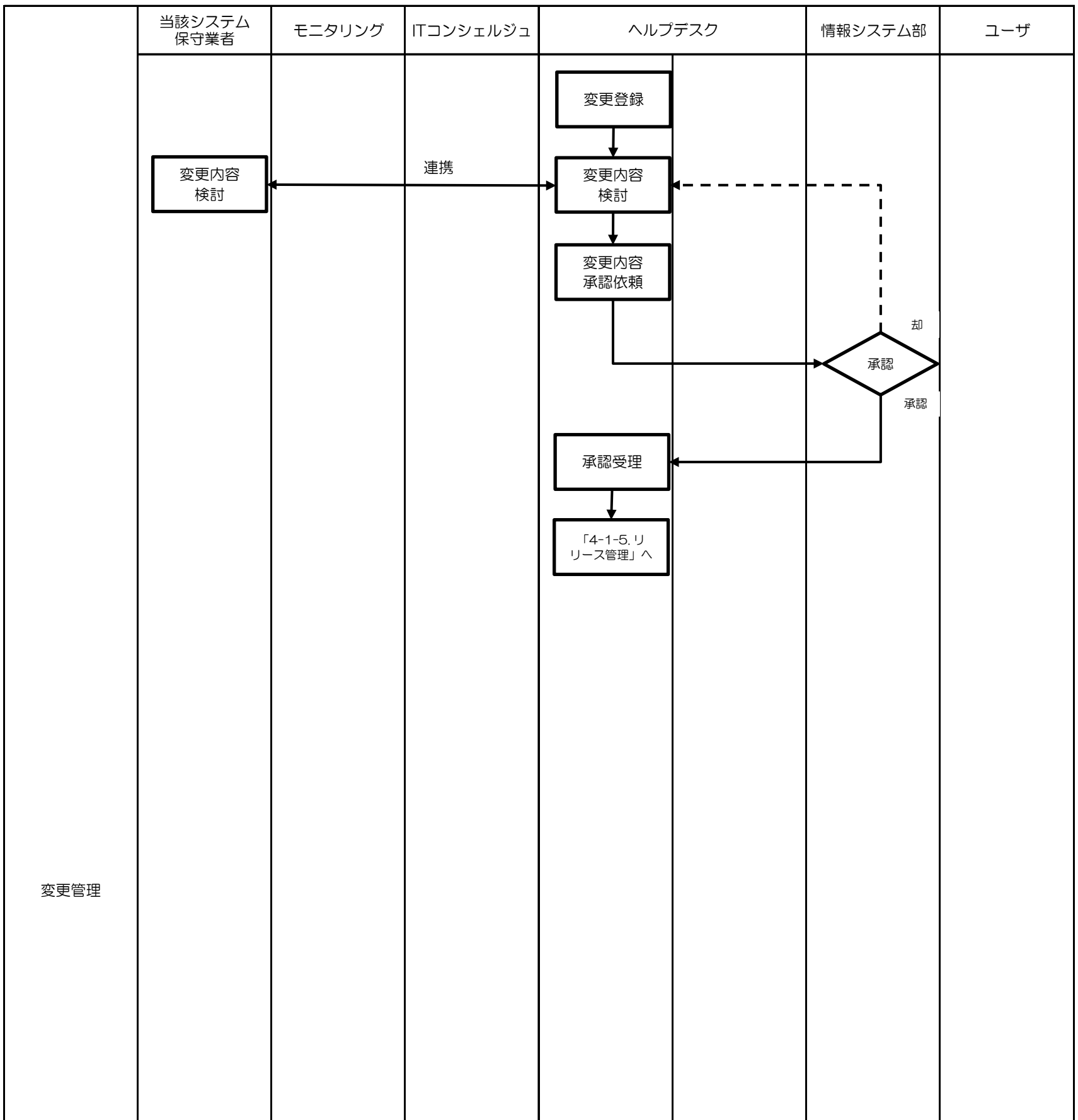
国際協力機構コンピュータシステム運用等業務におけるヘルプデスクに関する利用者満足度調査（サンプル）

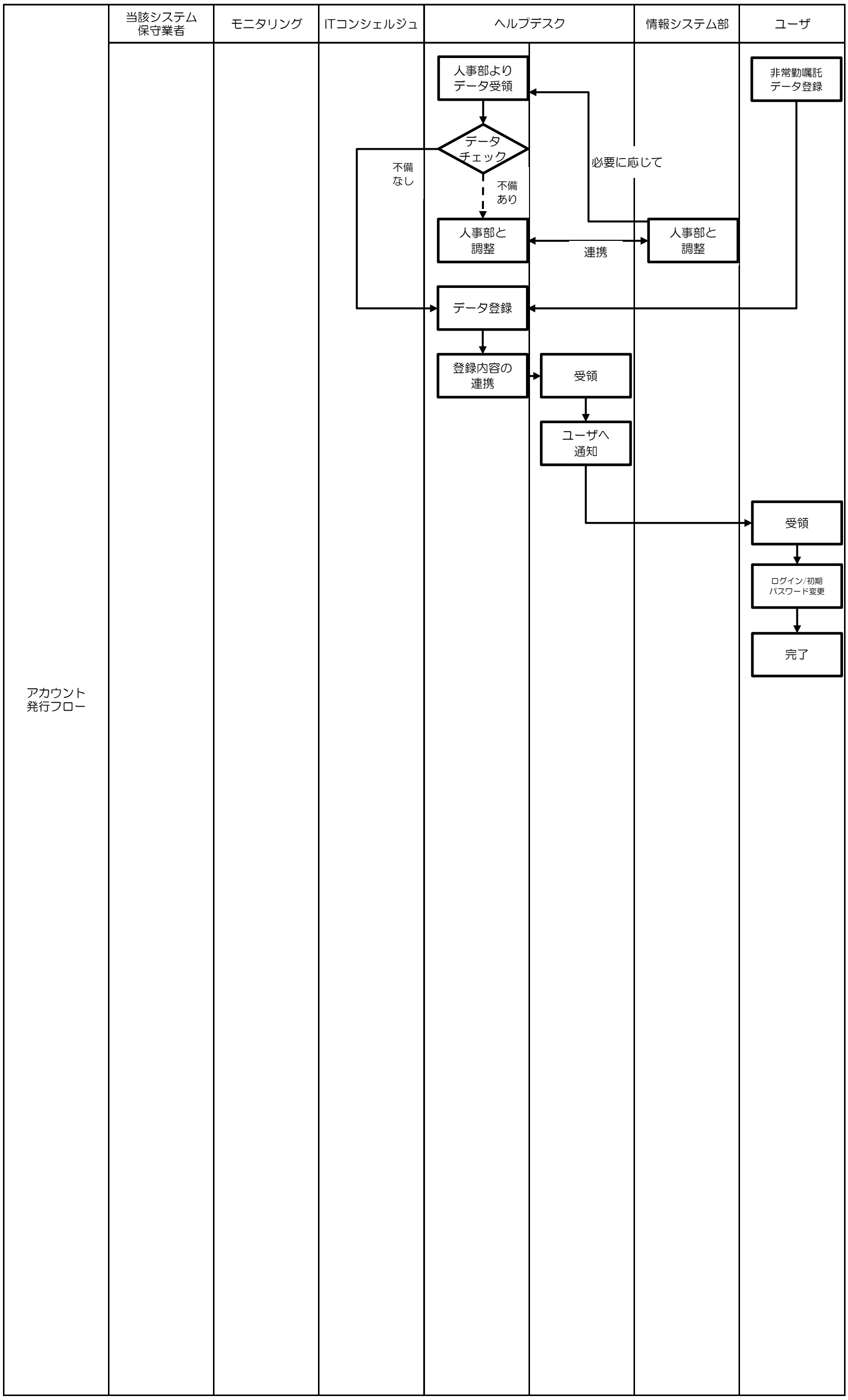
#	回答形態	形式	質問	回答群
21	自由	記述	クラウド関連ツール（Outlook、Teams、OneDrive、SharePoint等）について、ご要望やご意見があればご自由にご記載ください。	
6．本部ヘルプデスクの対応について				
22	自由	選択	麹町本部（5F）ヘルプテスクの受付対応について、満足度を教えてください。	満足 やや満足 やや不満 不満 利用したことがないため、分からない
23	自由	選択	（竹橋拠点に所属の方のみご回答ください） 竹橋ヘルプテスクの受付対応について、満足度を教えてください。	満足 やや満足 やや不満 不満 利用したことがないため、分からない
7．今後、ヘルプデスクに期待すること				
24	自由	記述	今後、ヘルプデスクに期待したいこと、またご要望やご意見があればご自由にご記載ください。	

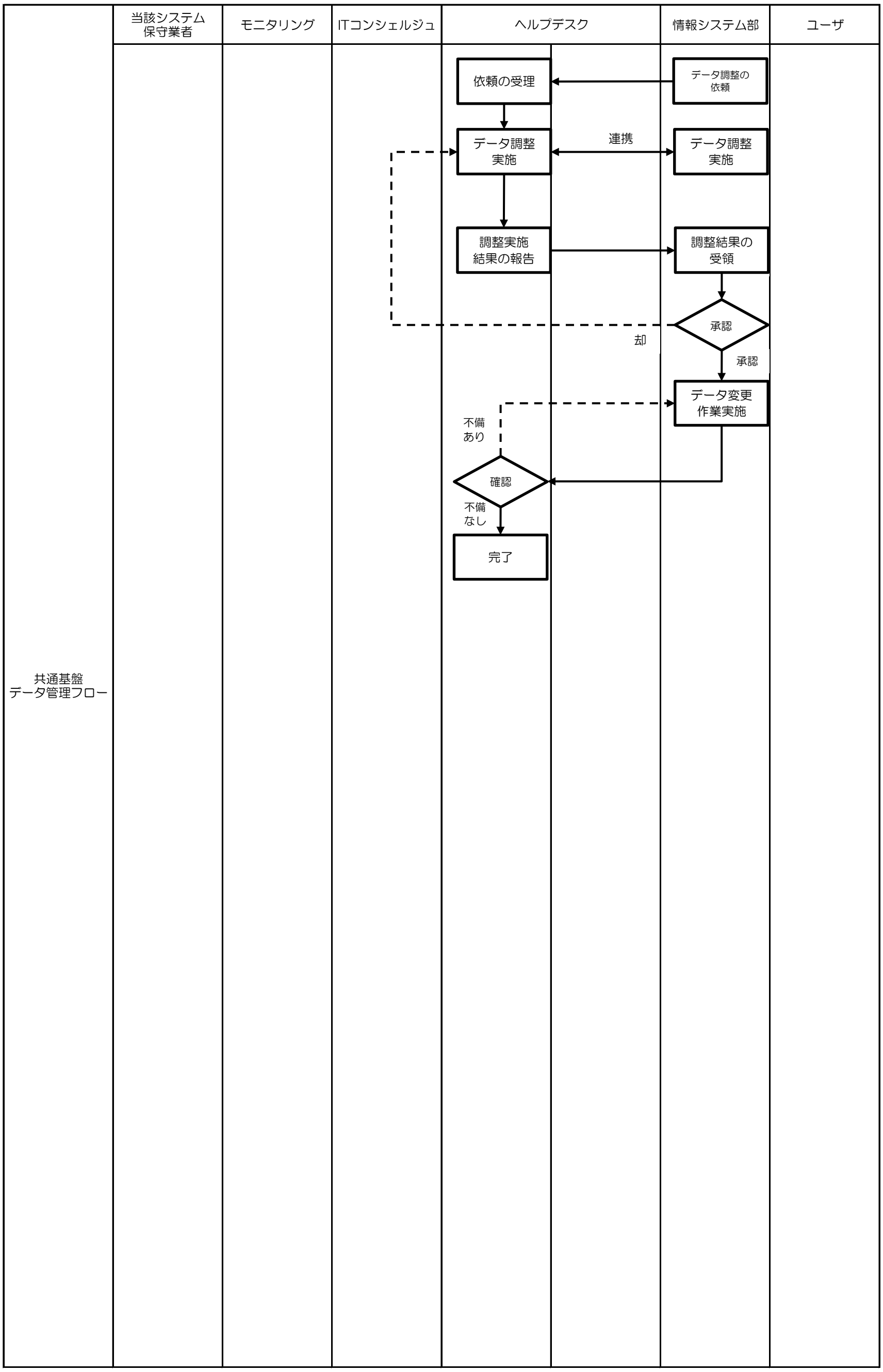

当該システム
保守業者
モニタリング
ITコンシェルジュ
ヘルプデスク
情報システム部
ユーザ
インシデント管理
（ユーザからの問合せ・監視による報知）
問合せ
対応可能
N
YES
回答
回答受領
アラート
検知
アラート
登録
内容
切分け
保守業者が担当
運用担当が担当
対応
完了報告
報告受理
状況確認
一時報知
調査
連携
調査
一時報知
受理
一時報知
受理
一時報知
理
NO
回答可能
YES
回答
回答受領
一時報知
一時報知
受理
一時報知
受理
一時報知
受理
恒久対応
対応
暫定対応
「4-1-3. 問題管理」へ
対応案
検討
対応案
承認依頼
N
承認
O
作業実施
連携
作業実施
完了報告
NG
承認
OK
承認受理
承認受理
「4-1-3. 問題管理」へ
完了

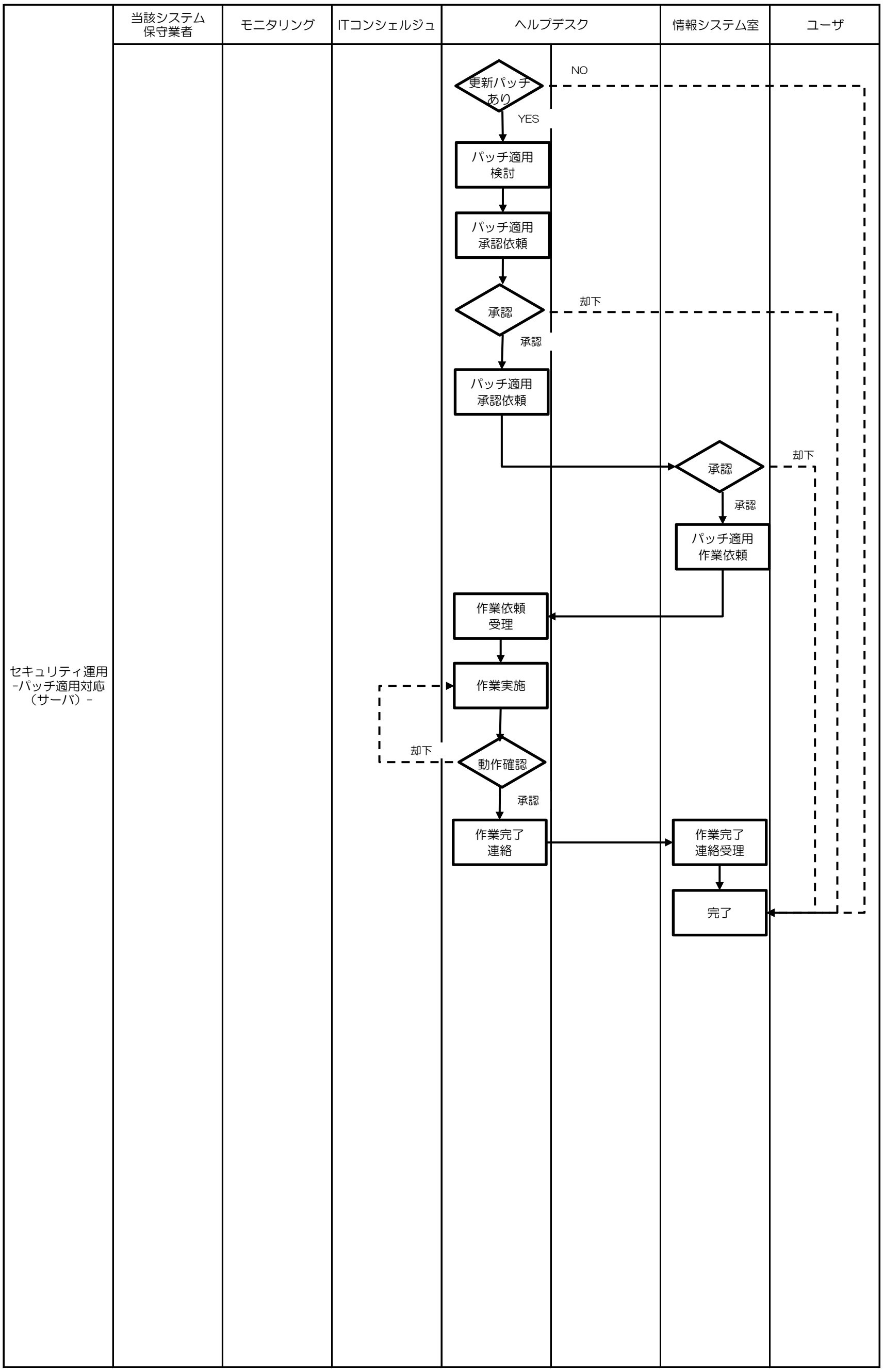

当該システム
保守業者
モニタリング
ITコンシェルジュ
ヘルプデスク
情報システム部
ユーザ
S
問題登録
調査・分析
連携
調査・分析
対応案検討
連携
対応案検討
承認依頼
却
承認
承
承認受理
「4-1-4. 変更管理」へ
問題管理

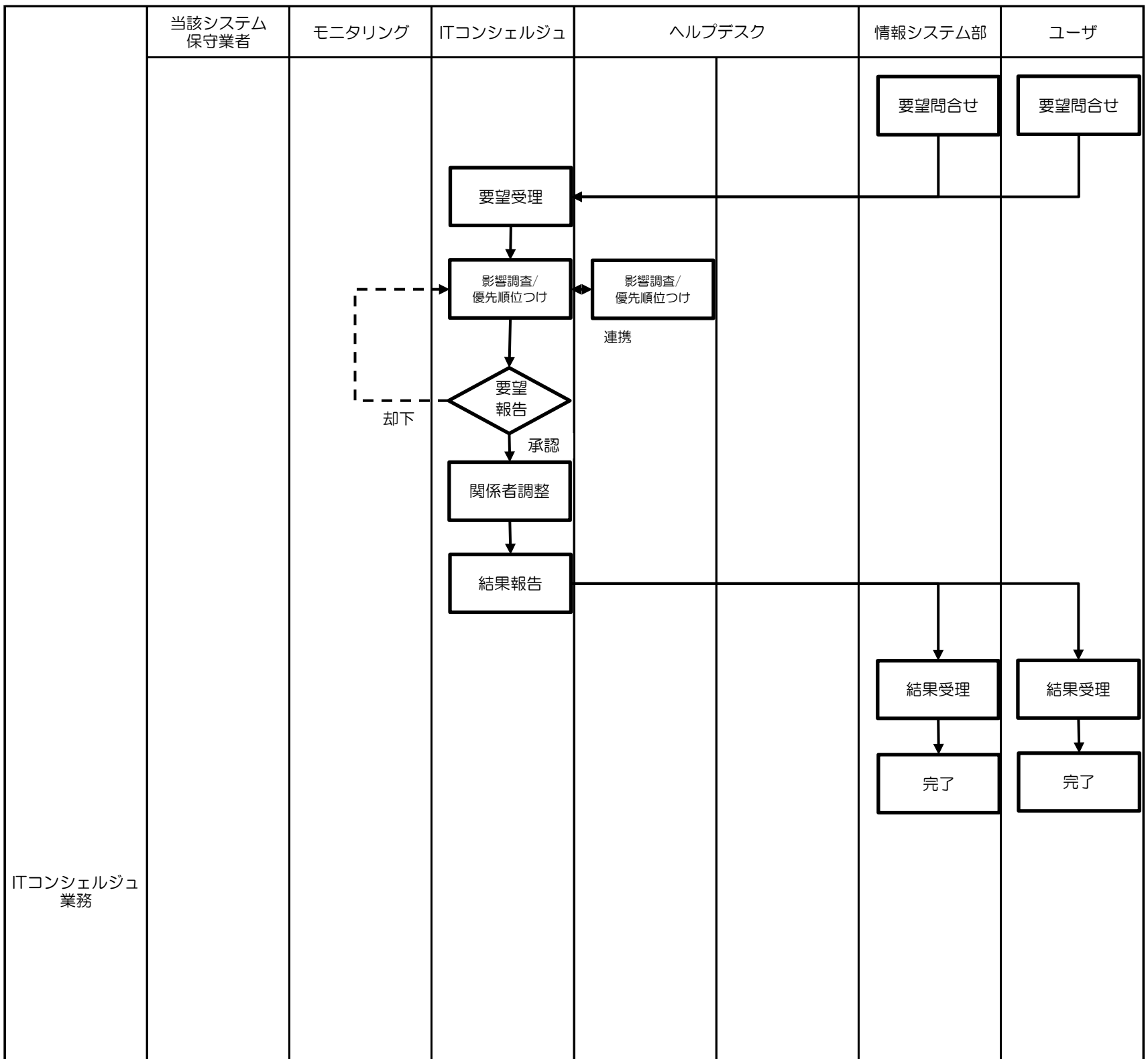
変更管理

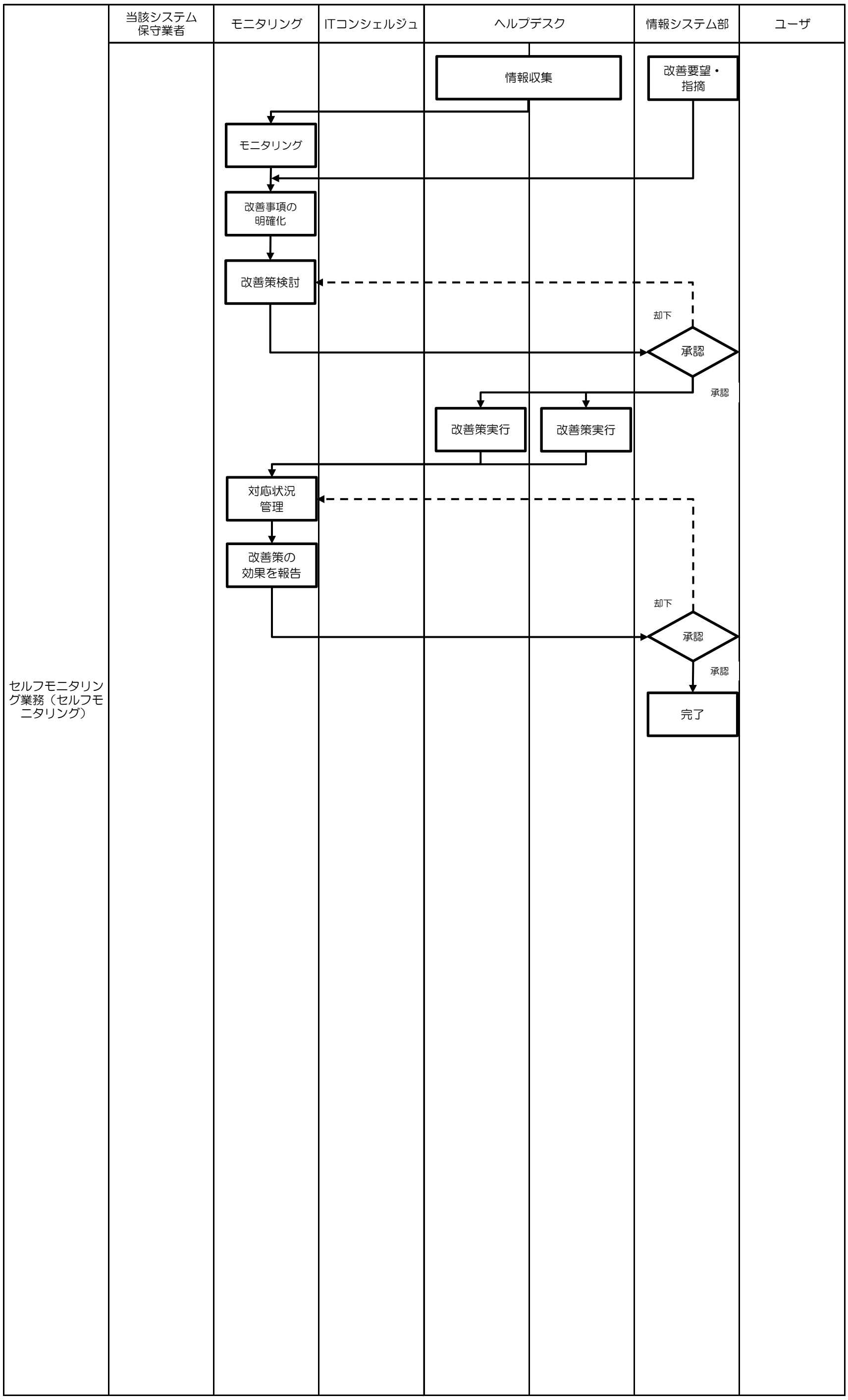

当該システム
保守業者
モニタリング
ITコンシェルジュ
ヘルプデスク
情報システム部
ユーザ
変更登録
変更内容
検討
連携
変更内容
検討
変更内容
承認依頼
却
承認
承認
承認受理
「4-1-5. リ
リース管理」へ


当該システム
保守業者
モニタリング
ITコンシェルジュ
ヘルプデスク
情報システム部
ユーザ
人事部より
データ受領
非常勤嘱託
データ登録
データ
チェック
不備
なし
不備
あり
必要に応じて
人事部と
調整
連携
人事部と
調整
データ登録
登録内容の
連携
受領
ユーザへ
通知
受領
ログイン/初期
パスワード変更
完了
アカウント
発行フロー


当該システム
保守業者
モニタリング
ITコンシェルジュ
ヘルプデスク
情報システム部
ユーザ
依頼の受理
データ調整の
依頼
データ調整
実施
連携
データ調整
実施
調整実施
結果の報告
調整結果の
受領
承認
却
承認
データ変更
作業実施
不備
あり
確認
不備
なし
完了
共通基盤
データ管理フロー


当該システム
保守業者
モニタリング
ITコンシェルジュ
ヘルプデスク
情報システム室
ユーザ
セキュリティ運用
-パッチ適用対応
（サーバ）-
更新パッチ
あり
NO
YES
パッチ適用
検討
パッチ適用
承認依頼
承認
却下
承認
パッチ適用
承認依頼
承認
却下
承認
パッチ適用
作業依頼
作業依頼
受理
作業実施
却下
動作確認
承認
作業完了
連絡
作業完了
連絡受理
完了

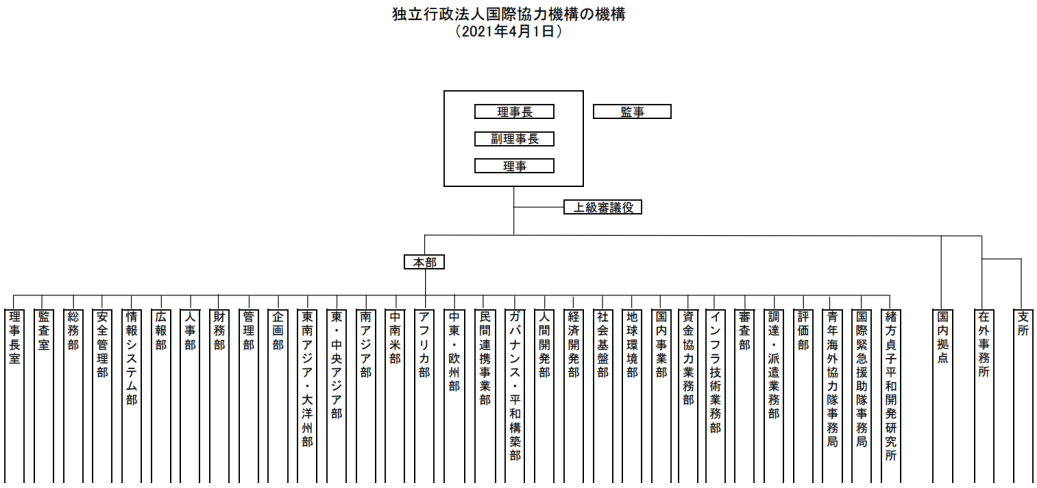

当該システム
保守業者
モニタリング
ITコンシェルジュ
ヘルプデスク
情報システム部
ユーザ
要望問合せ
要望問合せ
要望受理
影響調査/
優先順位つけ
影響調査/
優先順位つけ
連携
要望
報告
却下
承認
関係者調整
結果報告
結果受理
結果受理
完了
完了
ITコンシェルジュ
業務


当該システム
保守業者
モニタリング
ITコンシェルジュ
ヘルプデスク
情報システム部
ユーザ
情報収集
改善要望・
指摘
モニタリング
改善事項の
明確化
改善策検討
却下
承認
承認
改善策実行
改善策実行
対応状況
管理
改善策の
効果を報告
却下
承認
承認
完了
セルフモニタリング業務（セルフモニタリング）

別紙４

機構組織図　（2021 年 4 月 1 日現在）

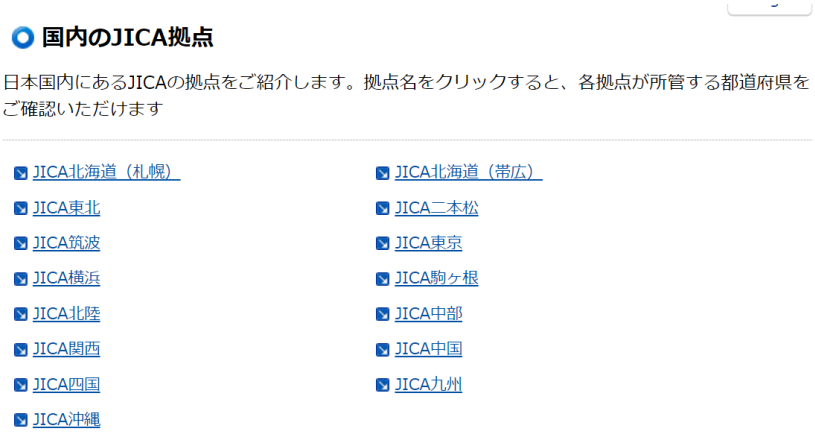
詳細は以下当機構公式ホームページ（HP）参照
https://www.jica.go.jp/about/jica/index.html



１．本部（詳細は以下当機構公式 HP 参照）
https://www.jica.go.jp/about/structure/hq.html

	本部ビル名
麹町本部	二番町センタービル
竹橋本部	竹橋合同ビル
市ヶ谷本部	JICA 市ヶ谷ビル

２．国内拠点（詳細は以下当機構 HP 参照）
https://www.jica.go.jp/about/structure/domestic/index.html



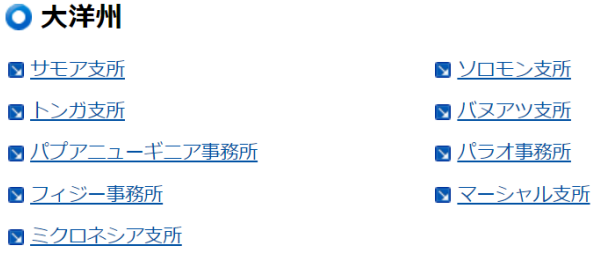
３．海外拠点

① アジア（詳細は以下当機構公式ホームページ参照）

https://www.jica.go.jp/about/structure/overseas/asia.html

② 大洋州（詳細は以下当機構 HP 参照）

https://www.jica.go.jp/about/structure/overseas/oceania.html



③　北米・中南米（詳細は以下当機構 HP 参照）

https://www.jica.go.jp/about/structure/overseas/america.html

北米・中南米

- アメリカ合衆国事務所
- アルゼンチン支所
- ウルグアイ支所
- エクアドル事務所
- エルサルバドル事務所
- キューバ事務所
- グアテマラ事務所
- コスタリカ支所
- コロンビア支所
- ジャマイカ支所
- セントルシア事務所
- チリ支所
- ドミニカ共和国事務所
- ニカラグア事務所
- ハイチ支所
- パナマ事務所
- パラグアイ事務所
- ブラジル事務所
- ベネズエラ支所
- ベリーズ支所
- ペルー事務所
- ボリビア事務所
- ホンジュラス事務所
- メキシコ事務所

④　アフリカ（詳細は以下当機構 HP 参照）

https://www.jica.go.jp/about/structure/overseas/africa.html

アフリカ

- アンゴラ事務所
- ウガンダ事務所
- エチオピア事務所
- ガーナ事務所
- ガボン支所
- カメルーン事務所
- ケニア事務所
- コートジボワール事務所
- コンゴ民主共和国事務所
- ザンビア事務所
- シエラレオネ支所
- ジブチ事務所
- ジンバブエ支所
- スーダン事務所
- セネガル事務所
- タンザニア事務所
- ナイジェリア事務所
- ナミビア支所
- ニジェール支所
- ブルキナファソ事務所
- ベナン支所
- ボツワナ支所
- マダガスカル事務所
- マラウイ事務所
- 南アフリカ共和国事務所
- 南スーダン事務所
- モザンビーク事務所
- ルワンダ事務所

⑤　中東（詳細は以下当機構 HP 参照）

https://www.jica.go.jp/about/structure/overseas/mideast.html

中東

- イエメン支所
- イラク事務所
- イラン事務所
- エジプト事務所
- シリア事務所
- チュニジア事務所
- パレスチナ事務所
- モロッコ事務所
- ヨルダン事務所

⑥　欧州（詳細は以下当機構 HP 参照）

https://www.jica.go.jp/about/structure/overseas/europe.html

欧州

- トルコ事務所
- バルカン事務所
- フランス事務所

- ウクライナフィールドオフィス

コンピュータシステム運用等業務

業務仕様書(案)

令和5年(2023年)

独立行政法人国際協力機構

目 次

別添資料

No.	資料名
別添資料 01	業務系システム一覧(ハウジング対象)
別添資料 02	業務系システム構成(ハウジング対象)
別添資料 03	ネットワーク環境(本部ネットワーク構成図／運用対象機器)
別添資料 04	運用対象標準 PC・提供対象機器の仕様
別添資料 05	要件定義書
別添資料 06	システム概要図
別添資料 07	モニタリング項目案

1. 本書の位置づけ

本書は、「コンピュータシステム運用等業務 民間競争入札実施要項」にて調達するコンピュータシステム運用等業務（以下、「本業務」という。）の調達仕様をとりまとめたものである。

2. 調達対象業務の基本要件

2.1 独立行政法人国際協力機構について

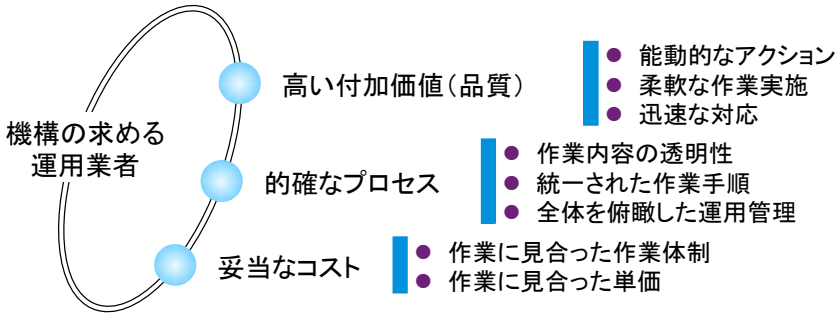
独立行政法人国際協力機構（以下、「機構」という。）は、開発途上にある海外の国・地域に対する技術協力、有償及び無償の資金供与による協力、開発途上地域の住民を対象とする国民等の協力活動の促進に必要な業務、中南米地域等への移住者の定着に必要な業務等、総合的な政府開発援助（Official Development Assistance（ODA））の実施機関である。

本部（麹町、竹橋および市ヶ谷）を含めた 18 の日本国内拠点、98 の在外事務所・在外支所等が存在する。詳細は当機構公式サイト（http://www.jica.go.jp）を参照すること。

2.2 機構の求めるシステム運用事業者・運用業務

2.2.1 基本的な考え方

機構における IT とは、機構のビジョン・使命・戦略を実現するための基盤であり、その基盤（システム等のソフトウェア・ハードウェア・ネットワーク等）について、効率よく、円滑かつ安全に日々用いることができるようにすることが機構における運用業務である。本業務の受託者（以下、「受託者」という。）は、その運用業務を機構と共に実施するパートナーとして存在することが求められる。また、機構の求めるシステム運用業務、具体的には「高い付加価値（品質）」・「的確なプロセス」・「妥当なコスト」を実現できる事業者であることが求められる。



【図表 2-1　機構の求める運用事業者】

このような要求の背景としては、システム・エンジニアリング的な技能は機構人材要件に位置付けられておらず、また、数年を周期とする定期的な人事異動があることにより、同技能に習熟した機構職員を継続的に配置することが難しいという点が挙げられる。他方、IT 活用による戦略的な業務効率化やナレッジマネジメント強化の必要性も組織として存在するところ、エンドユーザ対応を中心とした日常レベルでのシステム運用管理を効果的にアウトソーシングし、より上流の IT 統括マネジメントに機構職員の資源を集中する必要がある。

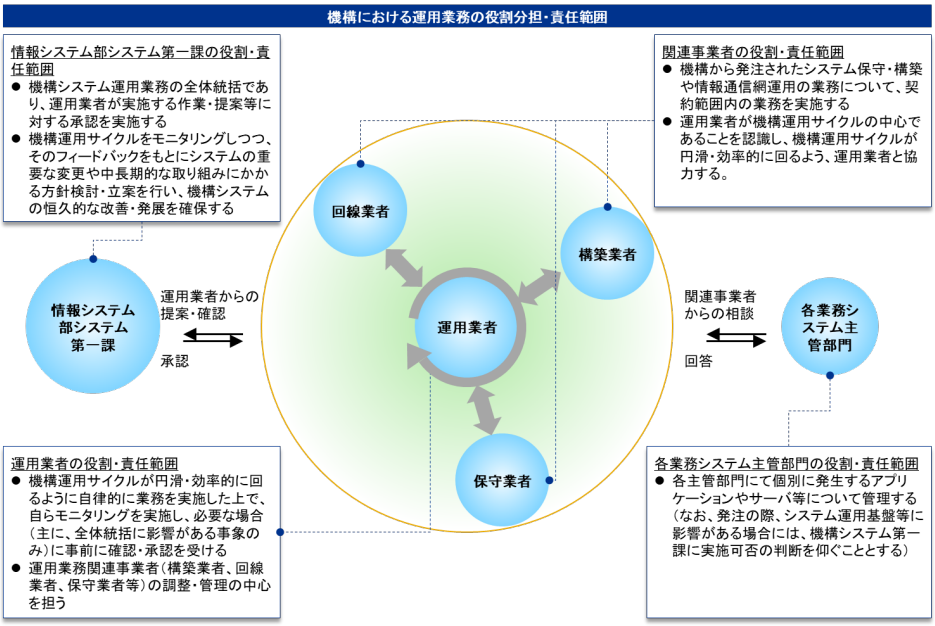
さらに、機構職員の体制のスリム化が図られる場合でも、エンドユーザに対するサービスレベルを維持・向上し続けるためのサイクルを、本業務を実施する受託者が自律的に履行する責

任を負わなければ円滑なシステム運用は実現できないと考える。

よって、受託者は、指示に基づいてのみ業務を実施するのではなく、機構のシステム運用における共同パートナーとして、エンドユーザの要求を日々充足するため、常にサービスの最前線で能動的に行動することを最優先することが強く求められる。このため、非効率な会議の実施や、本件契約履行のために求められるもの以外のプレーヤーを配置することなどは、極力避けなくてはならない。また、機構と別途業務委託契約等を締結している外部委託事業者（本業務の関連事業者）と協働を行う場合には、コミュニケーションを密にして、正確かつ十分な情報共有を行うことが求められる。

2.2.2 機構運用サイクル

機構のシステム運用業務に関わるプレーヤーは、機構（システム第一課、基盤上の各業務系システム主管部門）、本業務受託者、関連事業者（情報通信網の構築・運用事業者・本部 LAN 構築・保守事業者、各業務系システム運用事業者等）であり、それぞれの役割・責任を共有し果たしていくことが重要と考える。

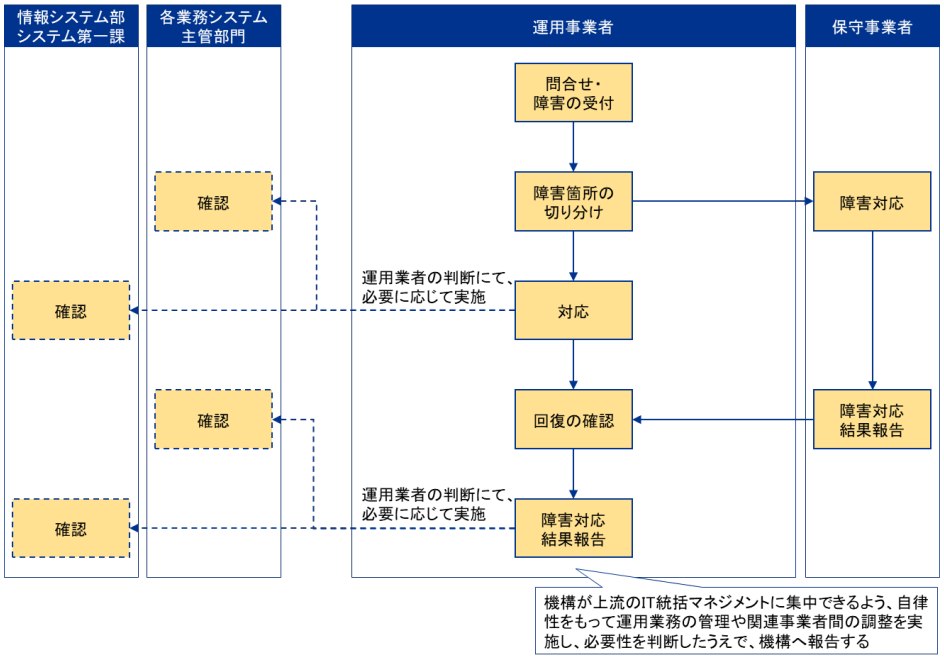


【図表 2-2　機構における運用業務の役割分担・責任範囲】

図表 2-2 に記載されている機構運用サイクルは、受託者が関連事業者の調整・管理の中心を担い、関連事業者は受託者と情報共有等の協力をすることで構成される。その機構運用サイクルを円滑・効率的に回すために、受託者は、自律性を持って運用業務の管理や関連事業者間の調整、情報の収集・一元管理等を実施し、全体統括（システム第一課）・個別発注のシステムの管理（各業務系システム主管部門）を実施する機構が上流の IT 統括マネジメントに集中できるよう業務を実施する（個別指示からプロセスモニタリングに業務管理方法を転換し、職員によるシステム全体統制を強化し、機構システムの恒常的な改善・発展を確保する狙い）。

また、 機構の今後 5 年度間の基本方針を定めた「IT 戦略（2022～26 年度）」に沿って他の業務系システム等との情報共有・調整も含めた対応を行う必要がある。特に、JICA 情報通信網（国内情報通信網・国際情報通信網・セキュリティサービス）の回線事業者とは密接な情報共有・調整を行うことが求められる。

上記の考え方に沿った、運用業務のフロー（イメージ）は以下の通り



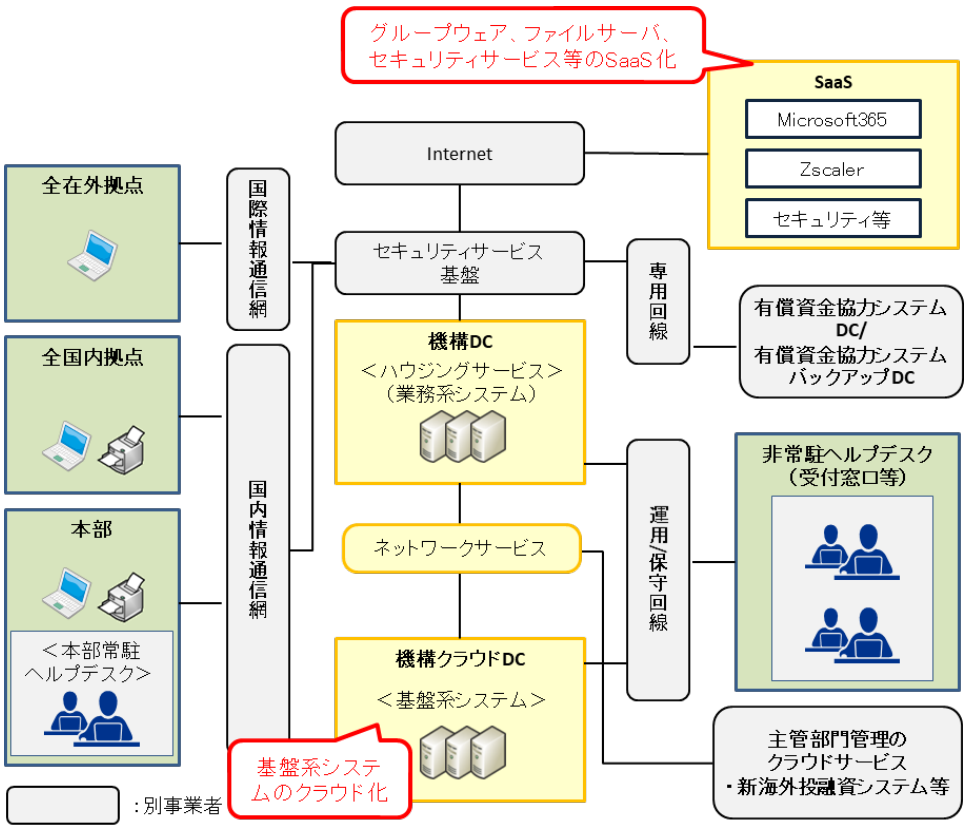
【図表 2-3　機構における運用業務のフロー（イメージ）】

2.2.3 本業務の範囲

(1) 全体構成

機構の IT には情報システム部が管理する「IT 基盤」（本業務に含まれるデータセンター（以下「DC」という。）や本部、国内拠点および在外拠点間の情報通信網、本部 LAN 等）に加えて、本業務が提供する各 DC 上もしくは独自 DC 上で構築・運用され、（情報システム部以外の）機構各部署が所管している「業務系システム」がある。

今回調達するコンピュータシステム運用等業務は、「IT 基盤」の内、機構データセンター（ハウジングサービス含む、以下「機構 DC」という。）、機構クラウドデータセンタ（以下「機構クラウド DC」という。）、SaaS（Software as a Service）の基盤系システム及び機構 DC と機構クラウド DC を含むクラウドサービスを接続するネットワークの提供等を対象とする。また、構築したシステムを用いた本部、全在外拠点、全国内拠点における PC の運用や Microsoft365 等の各種システムの運用、およびそれらの利用者からの問い合わせや各種申請を受け付けるヘルプデスク運用、情報システム部の一部業務支援等の提供を対象とする（対象となる SaaS やシステムは「別添資料 06 システム概要図」を参照）。なお、各 DC 上に構築された主管部門が所管する業務系システムの運用保守は本調達の対象外となる。



【図表 2-4　コンピュータシステム運用業務イメージ】

ネットワークとしては、当機構の全国内拠点、全在外拠点について、別事業者が管理する国内情報通信網、国際情報通信網により接続されるが、基盤系システムと密に連携することから、本ネットワーク及び各拠点における機構内ネットワークの運用も、一部業務の対象となる。

(2) 対象業務

本業務では、基盤系サービス、ハウジングサービスの「サービス利用環境提供業務」と、それらサービスを円滑に利用していくための「サービス利用計画業務」「サービス利用支援業務」「サービス運用管理業務」を調達範囲として求める。

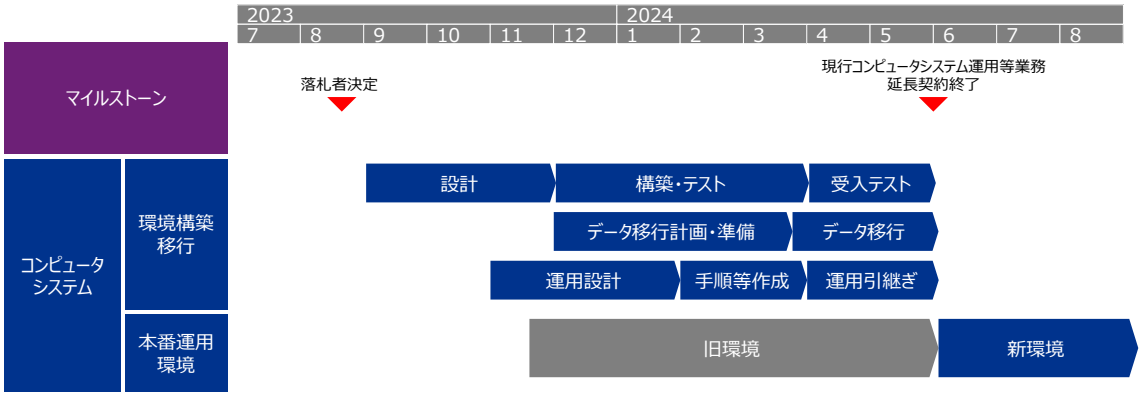
【図表 2-5　対象業務一覧】

業務・サービス名	内容
Ⅰ　サービス利用環境提供業務	
1. 基盤系サービス	機構で共通的に使用する各種共通基盤システムの機能を受託者にて設計・構築し、機構が利用可能なようにサービス提供する。

業務・サービス名	内容
2. ハウジングサービス（基幹業務系）	現在機構にて運用する複数の業務系システムを、受託者が整備するデータセンターのハウジングスペースに機器移設し、機構が利用可能なようにサービス提供する。
Ⅱ サービス利用計画業務	
3. サービスデザイン（運用開始前業務）	サービス利用支援業務及びサービス運用管理業務に含まれる運用業務の設計等を行う。
Ⅲ サービス利用支援業務	
4. サービスオペレーション	システムの起動・停止、バックアップ運用、点検作業運用、リカバリ運用、PC・公用スマートフォン(以下「公用スマホ」という。)等の運用、SaaS の運用、セキュリティ運用、本部ネットワーク運用等を行う。
5. サービス関連調査・提言	インフラ導入・設定変更／技術動向・運用改善に係る状況把握・提言、および監査（内部・外部）対応支援等を行う。
6. IT コンシェルジュサービス	プロジェクト実施支援等の各部署システム化支援、および情報システム部にて主管する情報基盤（IT 共通インフラ）整備に係る支援等を行う。
7. サービス提供環境における支援業務	グループウェアを含む情報共有に係るコンテンツの開発、改修・再構築・機能向上、整理の実施およびユーザからの照会対応を行う。
8. BCP 発動時に備えた機構クラウド DC（バックアップリージョン）の運用	BCP 発動時に備えた通常運用、BCP 発動時の運用、訓練等を実施する。
Ⅳ サービス運用管理業務	
10. サービス管理（インシデント管理）	機構内（本部、国内機関および在外拠点）利用者向けヘルプデスク、ユーザからの申請対応、システム監視、障害対応、セルフモニタリング等を行う。
11. 問題管理	障害の原因となる問題の管理等を行う。
12. 変更管理	システム変更の管理を行う。
13. リリース管理	リリース情報、リリース作業の管理等を行う。
14. 構成管理	システム構成情報の管理を行う。
15. 資産管理	資産管理ソフトにより各種ハードウェアに関する保有情報、賃貸借情報の統一的な管理を行う。
16. ソフトウェア管理	ソフトウェアライセンスの管理等を行う。
17. セキュリティ管理	セキュリティインシデント発生時の対応やセキュリティに係る提言等を行う。
18. ドキュメントの整備及び管理	ドキュメント整備及び管理等を行う。
19. 全体管理	運用者自身の工程管理や関連ベンダーとの調整を行う。

業務・サービス名	内容

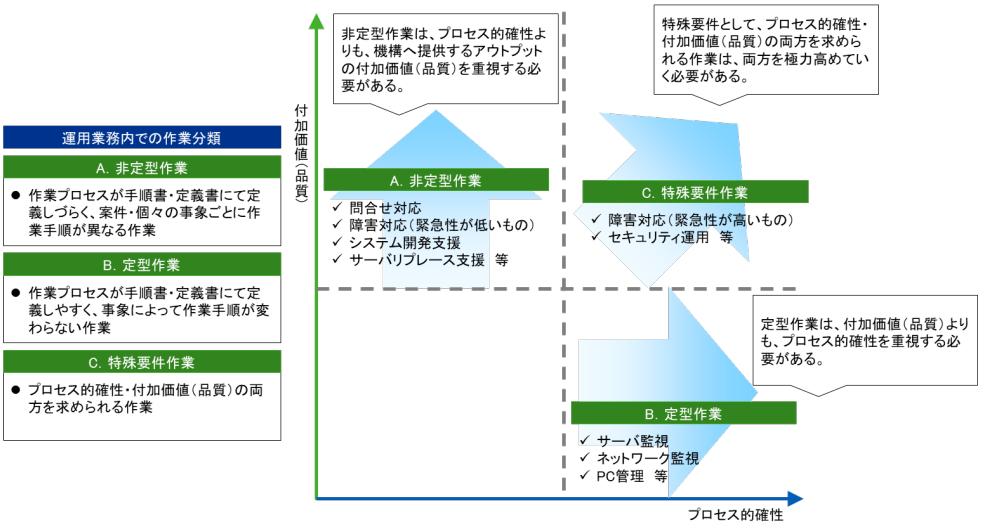
また、作業スケジュールは以下のとおり。



【図表 2-6　作業スケジュール】事業者は候補となる機器等（役務含む）については予め発注者に機器等リストを提出し、発注者がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、代替品選定やリスク低減対策等、発注者と迅速かつ密接に連携し提案の見直しを図ること。

(3) 作業分類

上記のサービス利用支援業務ならびにサービス運用管理業務では、作業に係るプロセスが一定であり、プロセス的確性を高めることにより、機構へ提供するアウトプットの品質・付加価値も向上することが想定される“定型作業”と、作業に係るプロセスが一定でないため、プロセス的確性よりも機構へ提供するアウトプットの付加価値（品質）を重視する“非定型作業”および、プロセス的確性と付加価値のどちらも求められる“特殊要件作業”がある。



【図表 2-7　作業の分類】

(4) 関連する作業の履行

当機構は、次のいずれかに該当するときには、請負者にその旨を通知するとともに、請負者と協議の上、契約を変更または別途個別契約することができる。

・当機構の組織、制度、及び IT 環境等設備の変更、情報セキュリティ対策の強化等の事由により、本業務の実施内容に変更の必要性が生じた場合。

・ Microsoft365 上で稼動する一部コンテンツの改修または新規コンテンツの開発・保守が必要となった場合あるいはファイルメーカー（以下「FM」という。）が稼働する環境の運用保守に係る要員が定常的に必要となった場合。

・ハウジングサービスの対象である業務系システムの一部で、本調達の業務期間中にシステム更改やクラウド移行が予定されている。また、業務系システムのシステム共通基盤である「共通サーバ基盤・共通 DB」も本業務期間中にクラウド化含む更改が予定されており、業務系システム更改、共通サーバ基盤・共通 DB 更改により、基盤系システムでの設計や運用方法の変更が必要となる場合もある。特に「共通サーバ基盤・共通 DB」の更改スケジュールを考慮し、同更改までの過渡期期間における業務系システムとの連携も含めて、本業務内容に追加・変更が生じる可能性がある点も留意すること。また、各更改の仕様によって関連する本業務内容に変更が生じる場合には、協議の上、契約内容の変更あるいは別途個別契約による対応を行う。

(5) 業務の引継ぎ

①現行事業者からの引継ぎ

本業務にかかわる現行事業者からの引継ぎ作業は以下を想定している。これら引継ぎ作業については、業務開始時に実施する予定である。

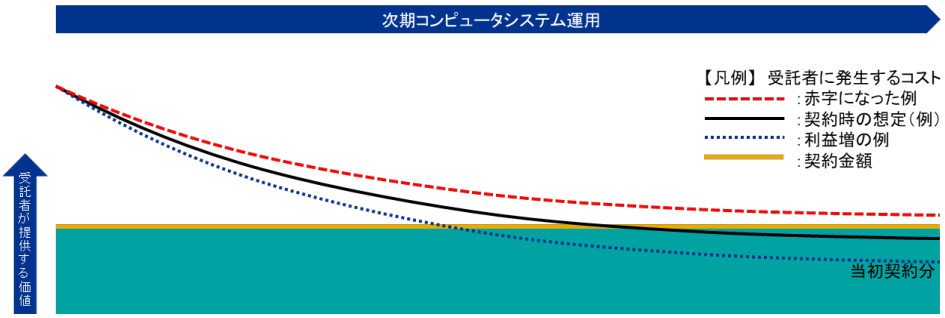
＜現行運用にかかるドキュメント等の提出＞

運用業務に係る以下のドキュメント（及びそれに類するもの）を提示する。

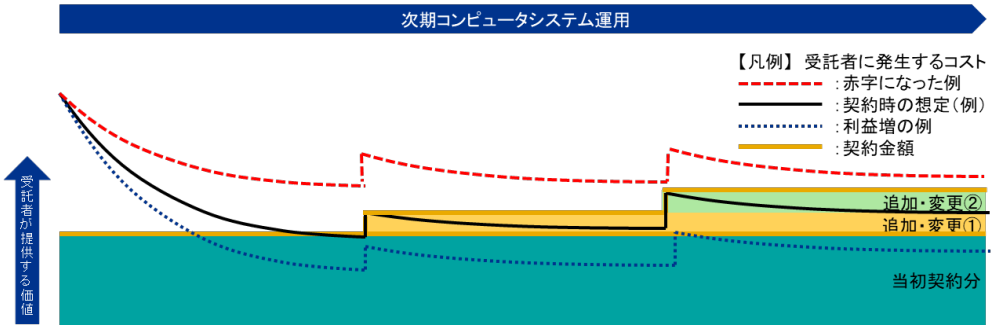
・運用設計書・運用手順書・マニュアル類
・データセンターのネットワーク構成図・機器構成一覧・設計書類
・運用業務にて使用している申請書・様式
＜ 現行事業者との打合せ（サービス導入フェーズ中、週１回程度）＞
受託者の業務引継ぎに必要な現行事業者との打合せ、業務説明会、運用業務の見学対応、質問回答等を必要に応じて実施する。

② 次期事業者（受託者）から次々期事業者への引継ぎ
本業務完了後に、次々期事業者への円滑な引継ぎが行えるように、以下の作業について支援を行うこと。
＜運用にかかる資料等の作成・提示＞
本業務に係わる資料（「6. 納入成果物」で示す資料）を次々期要件定義支援事業者及び次々期設計・開発・運用事業者等へ提示し、業務が円滑に引継げるように、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や十分な説明を行うこと。説明にあたり、別途説明用の補足資料が必要となる場合にはそれら補足資料を作成、提示すること。
＜ 次々期事業者との定期打合わせ対応（設計・準備フェーズ中、週１回程度）＞
次々期事業者への業務引継ぎに必要な打合せ、業務説明会、運用業務の見学対応、質問回答などを実施すること。
＜ 次々期事業者におけるシャドーイング学習への対応＞
次々期事業者が確実かつ早期に本業務の理解深耕を得られるように、業務引継期間中（3、4ヶ月）に次々期事業者が実施するシャドーイング学習（一連の業務を影のように後から追いかけて確認）への対応を積極的に行うこと。
＜移行データの抽出作業及び移行完了後のデータ消去＞
基盤系サービスで運用する各種データを、次々期サービスで利活用できるようにデータ抽出して提供すること。また、本業務の終了後（データ移行完了後）に、基盤系サービスで運用する各種データすべてを機構が指定するメディアに保存した上で、基盤系サービス内（ハードディスク装置内）に格納される全データを消去すること。消去作業完了後に「消去証明書」等の報告書類を提出すること。

2.2.4本業務における提供サービス価値（アウトプット）と対価
(1) 基本的な考え方
図表 2-8、2-9 では、受託者が提供する価値・契約金額・実際に受託者に発生するコストの関係を表している（図表 2-8、2-9 の“当初契約分”は、本業務の契約時に、5 年間の業務実施フェーズの費用を全て合算し、年度ごとに平均化した金額。ただし、サービス利用環境提供業務の導入にかかる初期費用は除く）。
受託者は、本業務を行うにあたって日々発生するコストを管理し、本業務に係る収支の状況を把握し、定期的に収支報告書として機構へ提示する（本業務の開始時点では収支の計画を機構へ提示する）。図表 2-8、2-9 のコストカーブは、収支計画書・報告書にて報告されるコスト及び収支状況のイメージである。



【図表 2-8　受託者が提供する価値と支払う対価：価値の変動が起こらなかった場合】



【図表 2-9　受託者が提供する価値と支払う対価：途中で価値の変動が起こった場合】

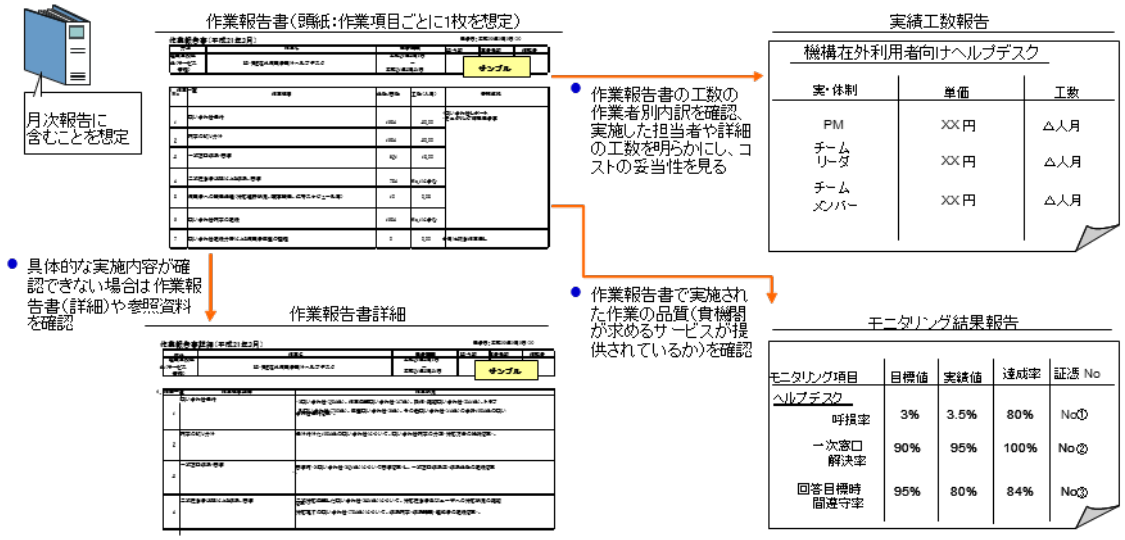
当初契約の仕様に無いアウトプットの追加（定型作業範囲の拡大や新たに追加する非定型作業項目）など、機構が受け取る価値に増加がある場合には、費用見直しのタイミングでその分の費用について契約金額の増額を検討する（当初契約の仕様にあった作業の削除などがある場合には、費用見直しのタイミング《原則として四半期ごと》で費用について契約金額の減額を検討する）。

他方、機構が受け取る価値に変動が無ければ、「2.4 本業務の履行責任範囲」に示す“重大な変更に当たらない事象”を伴った場合で受託者に発生するコストが契約金額より多かった場合にも契約金額の増額は行わない。逆に、機構が受け取る価値の変動にかかわらず、重大な変更と認められる場合は、契約金額の増額を行うこととする。なお、受託者が自らの努力によって業務を効率化して契約金額を大幅に下回る費用にて運用を実施できた場合は、減額は行わない。

(2) 収支計画書・報告書

本業務では、収支計画書・報告書に基づき、受託者に発生するコストの確認と受託者が提供している価値の評価を定期的に実施する。

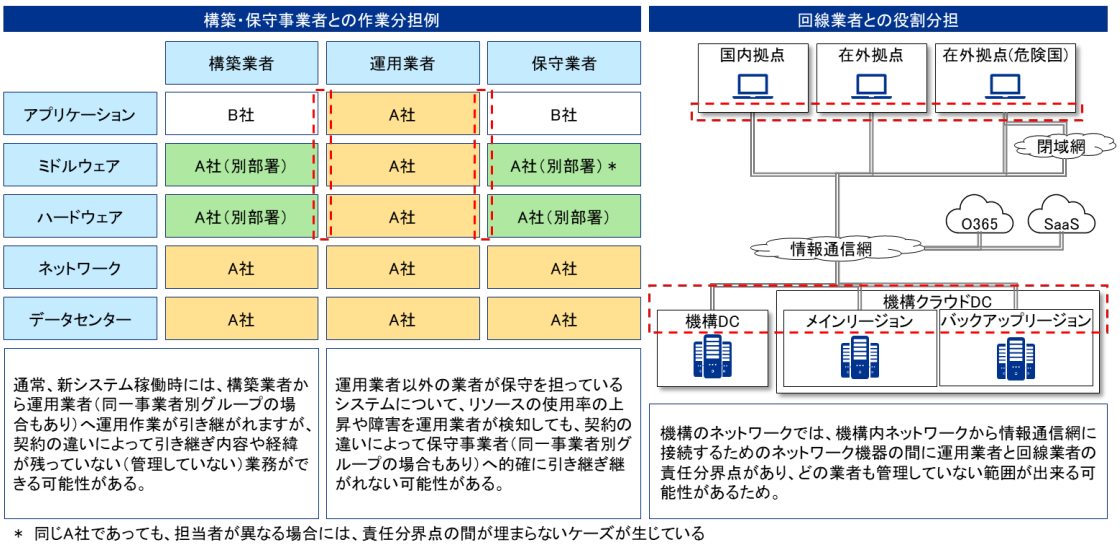
受託者に発生するコストの確認は、収支報告書に加えて、運用業務報告資料内に下記のような作業報告書を含めることで行う。なお、受託者が提供している価値の確認は、図表 2-10 内の“モニタリング結果報告”のように、モニタリング項目ごとの目標達成状況を自己評価し、エビデンスと共に定期的に報告することとする。



【図表 2-10　収支計画の報告イメージ】

2.2.5 本業務に係る関係事業者間の調整

機構システムでは、図表 2-11 の例のように、アプリケーション・ミドルウェア・ハードウェアの構築 事業者・運用事業者（受託者）・保守事業者が異なる場合があるため、それぞれの事業者の業務範囲（責任範囲）の境目に、どの事業者も管理していない業務が発生する可能性がある。境目の業務については機構が対応をする想定であるが、対応への相談受付等のサポートを受託者に求める。また、境目になり得る業務を認識した場合は機構に報告すること。受託者と回線事業者（国内情報通信網・国際情報通信網・機構内ネットワークの設置・運営）の業務範囲（責任範囲）の境目についても同様である。



【図表 2-11 機構システムにおける業務範囲（責任範囲）の例】

2.3 機構の求める情報セキュリティ対策要件

2.3.1基本方針

本業務の遂行にあたっては、情報セキュリティ対策における基本方針として、以下の方針に従った情報セキュリティ対策を実施すること。

- 情報セキュリティ対策として、サービスデザイン（運用開始前業務）の検討等において、システム内で取り扱う情報の機密性の高さや外部からの脅威を踏まえてリスク分析を実施し、網羅的な情報セキュリティ対策を実施すること。
- 上記の情報セキュリティ対策の詳細については、機構が定める「独立行政法人国際協力機構サイバーセキュリティ対策に関する規程」、「サイバーセキュリティ対策実施細則」等に準拠すること。また、これらの規程が変更になった場合には、機構と協議の上、求められる対応を実施すること。
- 情報セキュリティ対策について、セキュリティレベルの維持、向上のための追加対応が頻繁に発生するものについては、安定的に対応が図れるための仕組みを提供すること。
- 機構では、セキュリティインシデント等に迅速に対応できるように情報共有体制を構築する予定である。この体制に参画するとともに、技術支援を実施すること。
- セキュリティインシデント等の対応においても、関連事業者間の調整や情報の収集・一元管理を能動的に実施すること。
- 機構が、セキュリティにかかわる内部あるいは外部監査により、改善の必要性が指摘された場合には、受託者の責任において迅速に対応すること。

2.4 本業務の履行責任範囲

非定型作業や、附帯業務として実施することが必要な以下の業務（重大な変更に当たらない事象）に関しては、本業務上の自律的な履行責任範囲として位置付け、能動的なアクション・提案の実施を求める。

機構システム機能の現状維持：組織改編、人事異動の対応件数は、年間ピークがあるが、その対応のために一時的に対応要員を増強した場合等、機構システムの維持のために当然実施されるべきもの（実施されないことにより機能上の支障を生じるもの）。

機構 DC 及び機構クラウド DC 上への新規システム導入等の対応：機構が、新規システム導入やサービスを検討する際に影響範囲等を確認する必要があるが、必要に応じて、検証環境を用意するなどの業務。検証のための環境提供、環境構築作業。

軽微変更：機構システムの現状維持、新規システム導入等への対応に該当しない、詳細設計の修正に該当するような機器設定変更作業。例えば、ルータのルーティングテーブルの設定変更、DHCP アドレスプールの変更等、AD のグループポリシーの変更等。

業務量の変動対応：機構の IT 環境の変更や職員数の増等による申請・問い合わせ数、管理対象の増等への対応。職員が利用している端末の設定変更（在外拠点を含む。大幅な変更は協議可）。

バージョンアップ作業：基盤系サービスを提供するうえで受託者が準備し設置する機器、パッケージ製品でバージョンアップが必要な場合は対応をすることする。この際、業務への影響が最小限になるように事前に調査・検証・準備のうえ行うこと。セキュリティ面を考慮すると、常に最新の状態に保たれるのが望ましい。また、受託者は標準 PC にインストールされるソフトウェア（「別添

資料 04 運用対象標準 PC・提供対象機器の仕様」参照）についてもバージョンアップが必要な場合は、同様に実施をすること。

クライアントライセンスの増加対応：当機構のユーザ数（クライアントライセンス、クラウドサービス等の申し込みアカウント数等）が増加（最大 15%）した場合の対応。

受託者が（機構の承認に基づき）導入した管理ツールに係るライセンスの増加対応：提供サービスをシステム管理する際に必要となる運用監視システム等のライセンス増加、バージョンアップ時対応。

保守作業：基盤系システムの保守作業（障害対応等）

その一方で、サービスレベル・アグリーメント及びセルフモニタリングの仕組みを活用することにより、上記のような自律的な履行を求める業務についても、本業務の受託者が内容に応じ事前・事後に区別した上で、履行プロセスに関する説明責任及び品質担保責任を確実に履行することが求められる。

2.5 その他

2.5.1 運用作業時間

後述のサービス管理に記載されている「機構内（本部、国内機関および在外拠点）ユーザ向けヘルプデスク」は平日午前 8 時から午後 10 時（日本時間）とし、「ユーザからの申請対応」については、平日午前 9 時から午後 6 時（日本時間）とする（但し、ヘルプデスク・申請の状況により、開始・終了時間を前後する可能性がある）。

機構 DC 及び機構クラウド DC の運用・障害対応は 24 時間 365 日とし、各システムの計画停止のスケジューリング等は運用設計時に検討・確定する。

2.5.2 運用作業場所

後述のサービスデザイン（運用開始前業務）に記載されている「運用業務体制の構築」の要件に基づき、常駐を求められている担当者は原則機構本部内にて作業を実施すること。

なお、担当者の作業・貸出用機器の保管等のために、機構本部内の常駐用スペース（10－15 人程度が常駐可能なスペース）を使用可能である。また、常駐用スペース内のデスク、キャビネ等の什器および機構内ネットワークへのアクセス環境、外線発信が可能な電話機についても機構にて準備・提供する。ただし、常駐用スペースの提供は、現行事業者との業務引継ぎ完了後となる。

2.5.3 ユーザの環境等

システム運用等業務で提供する各種サービスの利用者（ユーザ）は、機構職員及び非常勤職員、機構が許可した外部事業者等であり、大凡のユーザ数等の情報は以下の通り（いずれも在外拠点を含む）。なお、本部・国内機関の機構職員が利用している標準端末のスペックについては、「別添資料 04 運用対象標準 PC・提供対象機器の仕様」を参照のこと。

・ユーザアカウント数：約 6,600　（2022 年 12 月時点）
（機構内で使用するアカウントの総数）

・執務用 PC 台数：6,600 台（2022 年 12 月時点）
※上記のうち約 3,900 台が本部、国内機関で利用する標準端末（ノート PC）、持ち込み PC

が約 280 台、残りが在外拠点で利用する PC（各在外拠点にて調達したもの)。
（執務用 PC 台数は本業務実施期間内に最大で 15%程度の増加の可能性がある）

また、現在実施しているシステム運用等業務に係る作業件数は以下の通り（いずれも年間の概算件数)。機構内の IT 環境変更にともない増減の可能性がある。

・問い合わせ受付件数： 平均約 2,258 件/月（2021 年度 合計 27,099 件）
・ユーザ ID 申請対応： 約 1,764 件 / 月（2021 年度 合計 21,169 件）
・執務用ノート PC の貸出：100 件 /月
（在外拠点から本部、国内機関へ異動した役職員等、および新規採用となった役職員等に対して、新しい標準端末（ノート PC）を貸し出す。標準端末（ノート PC）は国内ユーザに紐付けて管理している。また、本邦の PC は原則情報システム部の調達した標準 PC を貸し出している。（在外拠点においては現地調達している））
・研修・会議用ノート PC 貸出件数：0～35 件（平均約 7 件）/日
・モバイルプリンタ貸出件数： 148 件/年
・プロジェクター貸出件数： 72 件/年
・スクリーン貸出件数： 43 件/年
・組織変更対応；年間 5 回程度
・人事異動対応；月間平均処理件数約 600 件

2.5.4 資料・情報等の英文化

執務参考資料・申請様式・マニュアル・ガイドライン・ヘルプデスクニュース等の情報提供や在外拠点側で実施すべき作業に係る支援のための資料・情報等については、英文化を原則とする。なお、英文化が原則とされる資料・情報等については、本業務であるシステム運用業務に係る業務側の作業のためのドキュメント類を対象とし、新規に作成する在外拠点向けのドキュメント類の英文化を実施する。英文化にあたっては、在外拠点の現地職員が英語のネイティブスピーカーではないことを考慮し、原文の機械的な英訳ではなく、趣意をわかりやすく伝える英文を作成すること。

【図表 2-12　英文化対象の資料】

展開先	内容	英文化のタイミング
在外拠点	各種申請ツール	運用業務の開始時、内容変更時
	その他、システム運用に係る周知文書やヘルプデスクニュース　等各種申請時	適宜

2.5.5 在外拠点等への現地出張について

本業務には、必要に応じて業務従事者が在外拠点へ赴く作業が含まれているが、原則現地への渡航に係る手続は受託者にて行い、旅費等一切の費用は受託者の負担にて実施すること。

なお、現地出張の要否・回数については機構と相談の上、最終決定されるが、作業内容に応じ

てWeb会議等の活用等により現地出張の回数を最小限(年間5回程度を想定)とすること。

また、直接現地に赴く担当者は必ずしも日本から渡航する必要はない。危険度に応じて、再委託契約を締結の上、現地や近隣他国に業務を委託する等、その状況に応じて全体を俯瞰して実施可能な方法を検討すること。

3. 調達対象業務の個別要件

3.1 プロジェクト全体管理

本業務のプロジェクト立上げにあたり、先ずはサービス利用環境提供業務の設計・準備・導入等におけるプロジェクト管理方法を定め、プロジェクト全体管理を円滑に実施すること。なお、サービス利用支援業務、サービス運用管理業務のプロジェクト管理方法については、サービス開始前にサービス利用計画業務にて、機構と協議のうえ定めること。サービス利用環境提供業務の設計・準備・導入等におけるプロジェクト管理の基本的な要件は以下のとおり。

(1) プロジェクト計画書の提示

受託者は、契約締結後 1 ヶ月以内に、プロジェクト全体を円滑に管理するための基礎的かつ統合的な計画を定める成果物として、作業体制、作業スケジュール、プロジェクト管理要領等を含むプロジェクト計画書を機構担当者に提出すること。なお、プロジェクトの途中段階で修正及び見直しが必要となる場合には速やかに再度提出し、機構担当者と協議の上決定すること。

(2) プロジェクト管理方法

受託者は、本作業の遂行にあたり PMBOK（Project Management Body of Knowledge）又はこれに類するプロジェクト管理体系に準拠したプロジェクト管理を行うこと。プロジェクト管理方法については、前項のプロジェクト計画書のプロジェクト管理要領にて定めること。プロジェクト管理要領には以下の項目を含めること。

●進捗管理

各タスクの状況把握及びスケジュール管理を行うことを目的とする。

●コミュニケーション管理

プロジェクト関連情報の作成、共有及び蓄積等に関する基準を定め本プロジェクトの全参画者が円滑かつ効率的にコミュニケーションを行えることを目的とする。

●課題管理

プロジェクト遂行上様々な局面で発生する各種課題について、課題の認識、対応案の検討、解決及び報告のプロセスを明確にすることを目的とする。

●品質管理

本業務が本要件定義書及び各種ドキュメントで定義される要件を満たすこと、又は上回ることを保証することを目的とする。

●リスク管理

各工程における目標の達成に対するリスクを最小限にすることを目的とする。

●セキュリティ管理

各工程において、セキュリティに関する事故及び障害等の発生を未然に防ぐこと及び発生した場合に被害を最小限に抑えることを目的とする。

また、プロジェクト計画書に基づいて本業務を円滑に推進し、進捗状況については WBS(Work Breakdown Structure)をもって、会議体において報告すること。

会議体としては以下のものを想定している。会議体の企画、運営、議事録の記録及び関連する調整等を行うこと。なお、具体的な会議体設置・運営等については、受託後、機構と受託者

とで協議の上決定する。

【図表 3-1　想定する会議体】

会議体	会議目的等	頻度
総括会議	進捗会議（四半期）の年次単位での総括としての位置付け。SLA の指標達成状況を含めた当該年次の業務実施・達成状況報告や課題の振り返り、次年次の計画等について報告・協議を行う。。	年次
進捗会議	SLA の指標の達成状況を含めた業務の進捗状況、課題等を確認し、対応方針等を検討協議する。	四半期
個別会議	本業務の作業単位等で進捗状況、課題等を確認し、対応方針等を検討・協議する。運用フェーズにおける個別会議開催頻度については別途機構と協議の上決定する。	週次
調整会議	機構が目的に応じて設定する会議。	随時

その他のプロジェクト管理に関する事項として以下について留意すること。

- 会議に使用する資料は、原則として、会議開催の前営業日正午までに提出すること。
- 会議の議事録案を、遅くとも会議を行った日から 5 営業日以内に作成し、機構に提出すること。
- 受託者は，作業の進捗状況について機構からの要請がある場合には、口頭又は書面により報告すること。
- 受託者は、機構から本作業を円滑に推進していくために必要な資料の提出を求められた場合にはこれに応じること。なお，提出に当たっては、必要に応じて、機構との間で事前の打ち合わせを実施すること。

(3) 他調整支援

サービス利用環境提供業務の設計・準備・導入等にあたり、機構内の関連部署や利用者、また関連事業者（保守事業者・構築事業者等）等との調整・連絡が必要となった場合には、機構の指示のもと、受託者が主体的となって行うこと。その際に説明資料が必要となる場合には作成・提示すること。

3.2　基盤系サービス

3.2.1 業務内容

(1) 基本的な考え方

本業務では、IT サービスの提供として、機構で共通的に使用する各種基盤システムを受託者にて整備し、機構が利用可能なようにサービスとして提供することを求めるものである。

基盤系サービスの利用に供されるオンプレミス環境およびクラウド環境及び必要なソ

フトウェアがインストールされた機器などを受託者にてすべて用意すること（サービス以外に、サーバ等の機器や必要なライセンス等の賃貸借料金を別途発生させないこと)。また、導入後の基盤系サービスのシステム運用・管理作業、その他付随して発生する作業について、すべて受託者の責任と費用負担において対応すること（これらにかかる費用負担については予め基盤系サービスの利用料に含めること)。

基盤系サービスを提供するために必要となるサーバのライセンス、サーバにアクセスするためのクライアントライセンスおよびそれらに付随して必要となるライセンスについても全て用意すること。

(2) サービス範囲

基盤系サービスのサービス提供範囲は、「機構 DC」、「機構クラウド DC」、「クラウドサービス」、「ネットワークサービス」の 4 つとする。なお、現行事業で利用している Microsoft365、Intune 等については現環境を継続して利用するため、新規構築は不要であるが、運用保守を求める範囲である。なお、Microsoft365 については現行で E5 ライセンスを利用している。新規構築する範囲及び現行を継続利用する範囲に関しては、「別添資料 06 システム構成図」、現行環境および継続利用する環境の構成等に関しては、本調達の入札公告における、「閲覧資料一覧」の各種設計書等を参照すること。

また、「ネットワークサービス」は、機構 DC と機構クラウド DC を含むクラウドサービスを接続するネットワークについては別調達である「次期情報通信網の更改」(2025 年 3 月末頃を予定)の更改後約 6 ヵ月の期間、サービス提供を求める。サービスの提供期間は本調達の更改後から、2025 年 9 月末までを予定している。

「機構 DC」における、DHCP 機能も別調達である「次期情報通信網の更改」(2025 年 3 月末頃を予定)にて移行する想定であるため、更改までの間サービスの提供を求める。

各サービスに求められる機能や性能の詳細に関しては、「別添資料 05 要件定義書」を参照のこと。

(3) 設計開発に係る基本要件

基盤系サービスでは、「別添資料 05 要件定義書」で示す要件をもとに機構にて利用できるようにサービス提供を求める。これら要件について本業務にて開発、カスタマイズ等を要するものについては、以下に即した作業を行うこと。

①要件定義

要件定義では、基盤系サービスに求める要件を明確にし、機構が求める要件との適合や相違等を確認しながら、基盤系サービスとして追加開発を要するものや改修を要するものについて決定すること。

②基本設計

基本設計では、要件定義で決定した要件に対して、基盤系サービスのシステム構成及び処理方式等の仕様を検討し、基本設計書としてとりまとめること。特に、受託者が提案するサービス内容と現行の基盤系サービス内容は、仕組みが異なると考

えられるため、綿密な現状調査と課題抽出とその対策、設計への落とし込みの検討が重要である。

③詳細設計

詳細設計では、基本設計書に定めた基本要件に基づき、基盤系サービスの詳細な仕様を決定すること。基盤系サービスの処理条件、処理方法、プログラム動作等の詳細な仕様を設計し、詳細設計書としてとりまとめること。

④製造

製造では、詳細設計書に基づいてプログラムのコーディングを実施すること。基盤系サービスを構成するプログラムの追加及び改修を実施すること。

⑤単体テスト

単体テストでは、コーディングしたプログラム（追加及び改修分を想定）が詳細設計書の要求仕様や求められた品質を満たしているか確認すること。

⑥結合テスト

結合テストでは、単体テストが完了したプログラムについて、プログラム間の整合性を確認するとともに、追加及び改修したプログラムが詳細設計書の要求仕様に求められた品質を満たしているか確認すること。

⑦総合テスト

総合テストでは、基本設計書で定義した基本要件を完全に実現しているか、各種回線接続や負荷テストを含めて包括的に確認すること。

また、実際のデータを使用しシステムの動作確認・検証を行うこと。

⑧受入テスト

受入テストでは、機構が、実際の利用を想定した状況においても問題なく動作するかを確認する。受託者は機構が実施する受入テストの支援を行うこと。また、運用の開始については、受入テストの結果を踏まえて判断すること。

3.2.2 システム要件

基盤系サービスは基本的に現在使用している機能を維持する方針とする。基盤系サービスの提供時には、システムのユーザ（職員等）の操作性に関わる部分（SW 等）を更新する場合には機能差異を明確にし、必要に応じ、3.2.9 に記載のある利用者への教育訓練の中に含めること。基盤系サービスにて現在実施している運用作業（基盤系サービスの安定した提供・維持として必要な作業）は、移行後も、機構業務に影響が無いよう漏れなく実施すること。

機器の増強やOS・MW・SW のバージョンアップが必要な場合の検討・実施も行うこと。

3.2.3 信頼性等要件

基盤系サービスに求める信頼性目標は以下のとおり。

【図表 3-2　基盤系サービスに求める信頼性目標】

信頼性目標	目標値
サービス運用時間	24 時間 365 日 ※1
サービス運用時間中の稼働率	99.9%以上 ※2

※1 計画停止時間を除く。

※2 稼働率の算定・評価は「3.20 セルフモニタリング」参照

基盤系サービスの信頼性目標を実現するために必要と考えられる要件は以下のとおり。設計工程においては、必要に応じ、これ以外の信頼性向上策も提案すること。

- 基盤系サービスを構成するハードウェア、ソフトウェア等は、製品として動作が十分に保証・確認されたものを用いること。
- 障害の局所化を図るため、機器のクラスタ構成、ハードディスクの RAID 構成等による冗長化方式を採用し、障害発生時には障害要因を発生した機器を切り離して運用できる縮退運転や自動継続運転を実現すること。
- ハードウェアが正常に稼動している状況下においてソフトウェア障害が発生した場合には、障害発生前のできるだけ最新の状態を回復できるよう対策を講じること。
- 基盤系サービスが設置される施設において、電源の瞬断が発生しても、サービス運用継続が可能なこと。
- 誤操作を行った場合にも、安易に重要なデータが消去されてしまうことのないよう、必要な措置を講じること。
- サービス運用中に何らかのトラブルが発生した場合に、その原因を追及できるように必要なログを記録、管理（直ちに出力して解析）できること。

3.2.4 拡張性要件

基盤系サービスの拡張性に関する要件は以下のとおり。

設計工程においては、必要に応じ、これ以外の拡張性向上策も提案すること。

- 利用者数や業務処理量の増加、組織変更、制度変更、今後の機構内 IT 環境の変更等に備えて、十分なスケーラビリティを確保した構成とすること。
- データを保存するサーバは、データ量増加に伴う機器増設などが容易に実現可能な構成とすること。

また、基盤系サービスの上位互換性に関する要件は以下のとおり。

設計工程においては、必要に応じ、これ以外の上位互換性向上策も提案すること。

- OS やミドルウェア等のパッケージソフトウェアのバージョンアップ情報が公開された場合には、必要な調査、改修等を実施することでバージョンアップに対応可能なシステムを構築すること。

- バージョンアップについて技術的な問題等がある場合には、機構と協議し、その指示に従うこと。

3.2.5 システム中立性要件

基盤系サービスのシステム中立性に関する要件は以下のとおり。設計工程においては、必要に応じ、これ以外のシステム中立性向上策も提案すること

- 最新の技術や製品群の採用が可能となるように、汎用性とオープン性を有するシステム構成とすること。
- 業務完了時に円滑なデータ移行が可能なシステム構成であること。

3.2.6 業務継続性要件

基盤系サービスの業務継続性に関する要件は以下のとおり。なお、機構では業務継続性の観点から機構クラウド DC のバックアップリージョンを整備して、災害時バックアップセンター利用と災害時復旧管理業務に取り組む予定である（「3.9 BCP 発動時に備えた運用」を参照)。これら検討においては、必要に応じ、これ以外の業務継続性向上策も提案すること。

- 機構の業務継続が担保されるように、システムを冗長化する等、耐障害性を考慮したシステム構成とすること。
- 首都圏における大規模な災害が発生し、通常時に利用する機構 DC および機構クラウド DC が利用できない状況となる場合にも、機構が指定する最小の基盤系サービスが継続して利用できること。
- 災害や事故等が発生した場合においても、本業務の継続性を確保するために継続すべき機能やそのための方策について検討の上、機構と協議すること。また、協議の結果を踏まえて必要な対策を実施すること。

3.2.7 情報システム稼動環境要件

基盤系サービスの情報システム稼動環境として、本業務では、機構クラウド DC (BCP 発動時に備えたバックアップリージョン含む)、機構 DC、SaaS 環境の 3 つの稼働環境の提供を求める。

上記 3 つの情報システム稼動環境として、「別添資料 05 要件定義書」を満たすこと。

3.2.8 移行要件

現行の基盤系サービスからの移行にあたり、以下の作業を実施すること。移行作業は 2024 年 5 月末までにすべて完了すること。

(1) マスタデータ等の移行

現行のオンプレミス環境で稼働している基盤系サービスと同等のサービスを本業務にてクラウド環境へ移行する場合は、正常に運用するのに必要な全てのマスタデ

ータ、プログラム等を移行すること。なお、同等の機能を持つ現行と異なるシステムやサービスを新規導入する場合にはマスタデータの移行は発生しない。

⑵ トランザクションデータの移行

現行のオンプレミス環境で稼働している基盤系サービスと同等のサービスを本業務にてクラウド環境へ移行する場合は、移行時点で保持されているトランザクションデータを全て移行すること。なお、同等の機能を持つ現行と異なるシステムやサービスを新規導入する場合にはトランザクションデータの移行は発生しない。

⑶ ファイル共有サービスのデータ移行

現行のファイル共有サービスよりデータ（文書等）を移行すること。移行にあたっては現行のフォルダ構成を踏襲し、現在と同様のアクセス権限を設定すること。現行のファイル共有サービスはMicrosoft 社の OneDrive であり、アカウント数及びデータ容量については「別添資料 05 要件定義書」を参照すること。

⑷ データ移行計画書の作成

移行を滞りなく実施するためにデータ移行計画書（対象データ、移行方式、移行手順等）を作成すること。

⑸ データ移行に必要なプログラムの準備

移行元及び移行先にて適切にデータ移行が実施できるようデータ移行用のプログラムを適宜用意すること。但し、プログラム実行に際しては移行前と後でデータ内容に変化がないことが担保されている必要がある。

⑹ リハーサル実施

データ移行計画書に則り、データ移行が適切に実施されるためのリハーサルを実施すること。

⑺ 移行に係る留意事項

現行の機構 DC から受託者の基盤系サービスに移行する方法は、受託者の提案によるため、移行時に暫定的に必要となる通信回線等、移行作業に必要な機材は本調達に含めること。なお、現行の機構 DC は東京都内で運用されている。

⑻ 機構クラウド DC 移行に係る留意事項

現行の機構クラウド DC から受託者の基盤系サービスに移行する方法は、受託者の提案によるため、移行時に暫定的に必要となる通信回線等、移行作業に必要な機材は本調達に含めること。また、本調達の公告から更改までの間に現行機構クラウド DC 上に構築がされる、または構築を予定しているシステムが存在するが、現時点で仕様等が確定しておらず情報提示することができないが、それらシステムの移行も見込むこと。なお、移行対象のシステムについては受託後に機構と協議の上、決定する。

また、現行の機構クラウド DC とネットワーク接続や ID 連携をしているシステム（所管部門にて構築、運用保守される基盤上に構築されたシステム）については、次期機構クラウド DC の新規構築時に所管部門のシステム側との調整が発生することを見込むこと。現時点では以下のシステムへの対応が必要である。

- 新派遣システム(Azure)：ネットワーク切り替え
- 新海投システム(AWS)：ネットワーク切り替え

- マーケットデータ管理システム(Azure)：現機構クラウド DC 上で稼働しているため、基盤移設
- 企業統合 DB システム(PowerPlatform)：機構 DC 上の ID 管理システム再構築に伴う、認証・ID 周りの動作確認、調整
- ディスバースオンラインシステム(PowerPlatform)：同上
- 新渡航管理システム(AWS)：同上

3.2.9利用者への教育訓練

現行と異なるシステムやサービスを導入した場合については、別途機構と協議の上。運用開始時に利用者向けの初回教育訓練を実施すること。また、教育訓練実施後に、教育訓練実施計画書に記載した進捗予定の実績､教育訓練の実施結果、課題等を報告する教育訓練結果報告書を提出すること。

(1) 教育訓練の対象者と実施方法

教育訓練の対象者は、別途機構と協議の上決定することとする。教育訓練の実施方法は以下のとおりである。

【図表 3-3　教育訓練の実施方法】

実施方法	実施概要
自己学習	利用者全体への教育訓練は、教材（集合研修で使用する教材と同様のもの）を用いての自己学習とする。 特別な環境を用意しなくても、自己学習が可能なように教材を用意すること。また、自己学習期間中における利用者からの質問･問い合わせに対応すること。※在外拠点の現地職員も含む。
集合研修	上記の自己学習に加えて、利用者（集合研修への参加希望者）への集合研修による教育訓練を実施すること。 集合研修は、30 名程度のものを、12～15 回（/年）程度の実施を想定している（研修の録画を機構のイントラネットで公開することも想定すること。）。 教育訓練の会場、並びに教育訓練対象者が使用する PC 端末等は機構で提供する。これ以外にも必要なものがあれば、受託者にて用意すること。

(2) 教育訓練の実施内容

教育訓練の実施内容はシステム操作方法（利用者用）を想定している。

また、それ以外にも実施すべきものがあれば提案すること。

(3) 教育訓練の実施担当者

教育訓練は導入したシステムやサービスに精通している者が実施すること。

(4) 教育訓練の実施時期

運用開始までに対象者に対して教育訓練を実施すること。

(5) 教育訓練の実施場所

実施場所については、機構担当者と協議の上、決定すること。

(6) 教育訓練の進め方

教育訓練の実施前に機構と協議の上、教育訓練実施計画書を作成することとし、機構担当者と協議の上で教育・訓練を実施すること。

教育訓練実施計画書には、下記項目を必ず入れること。

①教育訓練の実施体制と役割

②教育訓練の実施内容

③教育訓練の実施スケジュール

④教育訓練の実施環境

⑤教育訓練に使用する教材

※教材は日本語と英語の 2 種類を作成すること。

(7) 自己学習教材の整備

利用者全体への教育訓練は、教材を用いての自己学習とする。

利用者が自己学習できるように自己学習用の教材（集合研修で使用する教材と同様のもの）を用意すること。なお、自己学習用の教材は、機構内で特別な環境を用意しなくても利用できるものとすること。本部だけでなく国内拠点、在外拠点のユーザも多数いること、またこれらユーザの自己学習進捗状況が容易に一元管理できる必要があり、ユーザが操作に慣れている Web 環境での利用を想定している。また、新情報共有基盤運用開始前に、全ユーザが事前の自己学習を完了できるよう、啓蒙すること。自己学習に関する利用者からの質問・問い合わせに対応すること。

自己学習教材は日本語と英語の 2 種類を作成すること。

(8) 教育訓練後のサービス内容変更等に伴う注意事項

サービス内容変更等により、導入したシステムやサービスの操作等に変更が生じる場合には、研修教材に反映すること。教育訓練受講済みの者に対しても最新の操作方法等を確実に周知することができるように、周知のための資料を必要に応じて作成すること。

(9) その他

本要件は、運用開始時の初回教育訓練として実施するものである。この教育訓練とは別に、運用時に定常的に実施する教育訓練（新人職員研修、中途採用職員研修等）が別途ある。これら作業内容については、「3.5.サービスオペレーション」を参照すること。

3.2.10　その他

基盤系サービスの提供に伴って必要となる各種ライセンスの提供についても本調達に含めること。

「認証ディレクトリ」に関しては、機構保有の情報資産として、現行のアプリケーションソフトを、機構より受託者に貸与する。受託者にて別途用意することも可とする。

FM システムサービスに関しては、機構にて保有する以下のソフトウェアライセンスの利用を前提とし、機構クラウド DC 上に構築する（ライセンス（同時接続ライセンス）自体は機構にて調達・更新するため、準備不要)。

・ライセンス供給者：Apple Japan 社（Claris 法人営業本部）

・ライセンス数：同時接続ライセンス（100 名）：2 ライセンス、同（75 名）：4 ライセンス、同（10 名）：3

なお、上記ライセンスを利用するための「FileMaker Server 19.4」は現在機構クラウド DC 上の Infrastructure as a Service（IaaS）基盤上にて運用されている。現時点での計画として、本契約の各フェーズにおいて以下の業務を想定している（下記業務は現時点では本契約とは別の個別契約にて当機構の負担により実施することを想定しているため応札時点で技術提案書および積算に含める必要はない）

①上記 Server の更新（2023 年 10 月時点での最新バージョンへの更新）

②現在機構で利用中の FM データベース（約 400 個（関連部署：約 40）の①への移行対応

③移行された FM での運用

また、現行の基盤系サービスを構成するソフトウェアについては以下の通り。

【図表 3-4　現行の基盤系サービスを構成するソフトウェア(参考情報)】

区分	サービス名	現行ソフトウェア	備考
セキュリティ基盤	ウィルス対策管理サービス	McAfee ePolicy Orchestrator（マネージャ）	機構の標準PC では利用しておらず、機構DC でのみ利用している。
	ソフトウェア起動制御サービス	LAN Scope Cat9.4 クライアント LANDesk Management Suite	機構の標準PC で利用している
	ソフトウェアインストール制御サービス	LAN Scope Cat9.4 クライアント LANDesk Management Suite	機構の標準PC で利用している
	ウィルス対策サービス	McAfee ePolicy Orchestrator（クライアント） VirusScan Enterprise	機構の標準PC では利用しておらず、機構DC でのみ利用している。

区分	サービス名	現行ソフトウェア	備考
	クライアント操作ログ管理サービス	LAN Scope Cat9.4 クライアント LANDesk Management Suite（クライアント）	機構の標準PCで利用している
	メール監査サービス	WISE Audit	過去ログ検索用のWISEAudit 環境が存在
	リモートアクセスサービス	Zscaler Private Access（ZPA） BIG-IP Access Policy Manager（APM）	機構の標準PCにはZPA および APM に必要な設定がセットアップ済み
サービス管理基盤	資産管理サービス	LAN Scope Cat9.4 統合マネージャ	機構の標準PCで利用している

3.3 ハウジングサービス（基幹業務系）

3.3.1 業務内容

(1) 基本的な考え方

ハウジングサービスは、機構の各業務系システム主管部門においてそれぞれ所管する業務系システムを集約して統合管理するためのファシリティ環境として、データセンターのハウジングサービス提供を求めるものである。現在、業務系システムの多くは、現行事業者のデータセンターのハウジングサービス提供環境にて運用管理されている。

また、対象となる業務系システムの多くにおいて、クラウド化に伴う更改（新業務系システムの開発・移行）が、予定されていることから、受託者が整備するデータセンター運用開始にあわせて旧業務系システムを移設した後にハウジングサービスの廃止等の対応が必要となることに留意すること。

(2) サービス範囲

●ラックスペースの提供

ラックスペースの提供を求める業務系システムの構成・規模については、「別添資料01 業務系システム一覧（ハウジング対象）」および「別添資料02 業務系システム構成（ハウジング対象）」を参照のこと。

●付随サービスの提供

ラックスペースの提供に付随して以下の基本サービスを求める。なお、下記の基本サービスに加え、ハウジングに係る追加サービスの提供を必要とする業務系システムに関しては、各システムの保守事業者との間で追加サービスの内容を調整のうえ、個別に契約を締結すること。

●業務系システムが稼働可能な電源、ネットワーク環境等を提供すること。

●稼働監視として、対象ハードウェア、関連のネットワーク機器のPing 監視と通知(常時)、

システム LED ランプ確認（日次）を行うこと。

- セキュリティ監視として、ファイアウォールサービス（不正アクセス監視 / 通知）（随時）を提供すること。
- 障害対応として、システムリブート（電源オフ／オン）、ケーブル状態確認（ケーブル抜き差し踏む）を行うこと（いずれも随時）。
- その他、ラックの開錠、施錠、鍵管理、交換部品の受け取り等。（随時）

3.3.2 情報システム稼動環境要件

ハウジングサービスは、「別添資料 05 要件定義書」を満たすデータセンター内にて提供されること。

3.3.3 移設要件

業務系システムの移設にあたっては、受託者は全体管理（実施計画、進捗管理、課題管理、関係部署との調整等）および実施支援（実施に必要となるデータセンター側の情報提供・準備・基幹業務系システム機器搬送、テスト等）を担うこと。実際の移設作業は各業務系システム主管部門にて実施する。

(1) 業務系システムの機器移設対応

各業務系システム主管部門にて機構の指定場所（現行事業者のデータセンターのハウジングサービス提供環境等）から、受託者が提供するデータセンターのハウジングサービス提供環境に業務系システムの機器移設を行う（機器搬送を除く）。各業務系システム主管部門にて実施するこれらの機器移設に対して全体管理および実施支援の観点から主体的に対応を行うこと。機器移設は 2024 年 5 月末までにすべて作業を完了すること。

3.3.4 その他

(1) 関係者の調整

受託者は、ハウジングサービス開始（提供）前に、業務系システムの各業務系システム主管部門が求めるシステム運用が実現できるように、業務系システムの運用（保守）事業者と協議・調整する等の支援を行うこと。

【図表 3-5　業務系システムの運用（保守）事業者との協議・調整事項】

作業工程	No	主要作業項目		受託者	業務系システム運用/保守事業者	備考
サービスデザイン（運用開始前）	1	全体工程管理		●	-	
	2	受託者 DC 設計		●	-	
	3	運用設計	死活監視	●	-	

作業工程	No	主要作業項目		受託者	業務系システム運用/保守事業者	備考
			上記以外の監視等	● どこまでを監視対象とすることが適切か業務主管部署と検討	●	・本調達対象外 ・受託者は、業務系システム運用/保守事業者と協議し、各業務系システム主管部門が希望する適切な運用を運用／保守事業者との個別契約にて実施する
移設作業	4	全体工程管理		●	－	・受託者が、業務系システム事業者との調整、工程管理を行う
	5	受託者 DC（受け入れ側）テスト		●	－	
	6	機器の取り外し		－	●	・システムの取り外しまでの稼働責任は業務系システム運用/保守事業者が負う
	7	業務系システム搬送		●	－	・システム搬送に係る責は本件受託者が負う
	8	機器の設置		－	●	・システム設置後の稼働責任は業務系システム運用/保守事業者が負う ・DC 側のネットワークテスト等は本件受託者
	9	動作検証 （業務系システムテスト等）		－	●	
ハウジングサービス（運用開始）	10	死活監視		●	－	・システム設置後の稼働責任は業務系システム運用/保守事業者が負う ・DC 側のネットワークテスト等は本件受託者
	11	上記以外の監視等		No3 の結果による	●	No3 の備考参照

(2) システム監視に関する留意事項

障害対応やパッチ適用・ジョブ管理等のその他作業については、原則各業務系システムが個別に契約している保守事業者にて作業を実施することとするが、異常を検知した際の確実な通報を受託者にて実施すること（詳細は受託後に各業務系システムの所管部署および保守事業者と調整のうえ決定する)。各業務系システムでは、各業務系システム運用保守事業者の自動化監視ツール（ただし、保守事業者によって設定変更及びツール変更されることがある。）により自動的に出力されることになっている。受託者は、これらのシステム監視に異常があった場合に、その警報・アラーム等の信号を常時感知できるようにしておき、必要に応じて、当該アラーム等の信号を各業務系システムの保守事業者にすみやかに自動配信メール等にて伝達することとする。なお、警報・アラーム等の信号は受託者が用意した端末に通知できるよう保守事業者にて準備する。

なお、上記のシステム監視に異常があった場合の対処は、一次きり分けを含めて、各業務系システムの保守事業者が行うが、本件契約の締結後、運用設計段階等において、予め実施手順書等の詳細仕様とともに、各保守事業者から依頼があった場合には、受託者が、本件契約とは別に、各保守事業者との委託契約を受注する義務を負い、そのための調整・協議に必ず応じることとする（その対価については、本件契約の単価や工数積算上の基準と同等であることが望ましいが、規模によっては機構と協議の上決定する。)。

各業務系システムの保守事業者の連絡先一覧を受託後に提示する予定である。

3.4 サービスデザイン（運用開始前業務）

3.4.1 業務内容

サービスデザインは、「運用業務体制の構築」、「運用業務工程管理」、「運用設計」、「インフラ導入・設定変更に係る状況把握・提言（設計・構築フェーズ)」、「サービルレベル設計」、「報告・提出資料等の定義」からなる業務である。業務内容の詳細については、「別添資料05 要件定義書」のうち、システム運用要件を参照のこと。

3.5 サービスオペレーション

3.5.1業務内容

サービスオペレーションは、「システムの起動・停止」、「DNS 運用」、「ジョブ運用」、「バックアップ運用」、「点検作業運用」、「リカバリ運用」、「機構内・在外利用者向けヘルプデスク」、「公用スマホ・PC 等の運用」、「周辺機器運用」、「システム設定変更」、「ネットワーク運用」、「教育・研修」からなる業務である。業務内容の詳細については、「別添資料05 要件定義書」のうちシステム運用要件を参照のこと。

3.5.2PC・周辺機器等の提供

サービスオペレーションの「公用スマホ・PC 等の運用」、「周辺機器運用」の実施にかかわり、以下のPC・周辺機器等の提供を求める。詳細については、「別添資料04 運用対象標準PC・提供対象機器の仕様」を参照のこと。

【図表 3-6　提供を求める PC・周辺機器等（ハードウェア)】

No	分類	用途	調達台数
1	研修･会議用ノート PC	本部内の会議、研修時等に利用するための貸出し用	52 台を調達
2	モバイルプリンタ	出張時貸出し用	150 台を調達(キャリーバック、予備機含む)
3	プロジェクター	本部内で会議時等の利用するための貸出し用	12 台を調達

3.6　サービス関連調査・提言

3.6.1 業務内容

サービス関連調査・提言は、「インフラ導入・設定変更に係る状況把握・提言」、「IT 環境変更に係る状況把握・提言」、「監査（内部・外部）対応」からなる業務である。業務内容の詳細については、「別添資料 05 要件定義書」のうちシステム運用要件を参照のこと。

3.7　IT コンシェルジュサービス

3.7.1 業務内容

IT コンシェルジュサービスは、「各部署システム化支援」、「IT 基盤整備支援」、「運用業務全体の状況把握」からなる業務である。業務内容の詳細については、「別添資料 05 要件定義書」のうちシステム運用要件を参照のこと。

3.8　サービス提供環境における支援業務

3.8.1 業務内容

サービス提供環境における支援業務は、「運用支援業務」、「開発支援業務」からなる業務である。業務内容の詳細については、「別添資料 05 要件定義書」のうちシステム運用要件を参照のこと。

3.9　BCP 発動時に備えた機構クラウド DC（バックアップリージョン）の運用

3.9.1 業務背景

首都直下型の震災等により機構 DC または機構クラウド DC（メインリージョン）にアクセスができない事態が発生した場合にも、「人命に係る業務」「金融支払い等の社会的責任を果たすべき業務」等の必要業務が継続利用出来る様に、BCP（事業継続計画）発動時に備えた機構クラウド DC(バックアップリージョン)を整備し、稼働が求められるシステム機能を震災後 48 時間以内に立ち上げる必要がある。

3.9.2 業務内容

BCP 発動時に備えた機構クラウド DC(バックアップリージョン)の運用は、上記背景をもとに、機構の BCP に則ったサービスが提供できるように、BCP 発動時に備えた業務について定

義するものである。「BCP 発動時に必要なサービス」、「BCP 発動時の運用業務」、「BCP 発動時の一時作業（切戻し）」、「BCP 発動時に備えた機構クラウドDC(バックアップリージョン)の通常（平常時）運用」からなり、詳細については「別添資料 05 要件定義書」のうちシステム運用要件を参照のこと。

3.9.3 業務の基本的な考え方

BCP 発動時に備えた機構クラウド DC(バックアップリージョン)の運用に係る基本的な考え方は以下のとおり。

【図表 3-8 BCP 発動時に備えた機構クラウドDC(バックアップリージョン)の運用に係る基本的な考え方】

基本事項	内容
想定被害	首都直下地震は東京湾北部を震源としたマグニチュード（M）7 級を想定し、機構DC・機構クラウドDC ともに利用出来ないものとする。
	本部ヘルプデスク要員は被災・避難しているため機構クラウドDC(バックアップリージョン)への切り替え・運用作業は、確保できないものとする。
BCP 期間	BCP 発動期間は 2 週間としており、当該期間に「BCP 発動時」の運用を行う。ただし、BCP 発動期間が 2 週間を超えた場合は、受託者としての最善を尽くし、可能な限り対応する。
対象者	約 6,600 人。リモートアクセスサービスを利用したサービス同時接続ユーザ数は 400 人。
RPO(Recovery Point Object)	1 日前。
RTO(Recovery Time Objective)	48 時間。
BCP 解除時にどこまで戻すか	震災発生直前まで戻す（BCP 発動中に発生したデータ変更分については、必要に応じて切戻しを実施する）。
バックアップ	BCP 発動時に利用するシステムバックアップを 1 世代のみ取得する（データバックアップは取得しない）。
リストア	障害発生タイミングによって、それぞれ次のデータをリストアする。 ●平常時（機構DC、機構クラウドDC 稼働時）に障害発生 ⇒機構DC、機構クラウドDC より最新データをリストア。 ●BCP 発動時に障害発生 ⇒最後に取得したシステムバックアップ時点のデータをリストア。
監視	サーバ、ネットワーク機器等の PING による死活監視及びセキュリティ監視を実施
可用性	冗長構成としないため、BCP 発動時にサーバ、ネットワーク機器等に障害が発生した場合、復旧までサービスは停止することを許容する。

基本事項	内容
セキュリティ対策	OS パッチについて、平常時は機構クラウド DC に配備された Windows OS セキュリティ対策サービスで管理する。BCP 発動中は、機構クラウド DC(バックアップリージョン)に整備されたサーバ群、クライアント端末への最新 OS パッチ適用は現行で導入済みのシステムにより配布を行う。
	ウィルス対策について、平常時、機構クラウド DC(バックアップリージョン)に配備されたサーバ群は、機構クラウド DC(メインリージョン)に配備されたウィルス対策管理サービスで管理する。 BCP 発動中は、機構クラウド DC(バックアップリージョン)に配備されたウィルス対策管理サービスでセキュリティ対策の提供を行う。
サービス品質/性能	複数サーバで負荷分散させる構成をとっていないため、平常時に比べて応答時間が低下する可能性がある。
機構 DC からの 切替え／切戻し	BCP 発動時、解除時は、被災したことを想定し、極力、機構職員による操作は行わない方針とする。そのため、運用事業者（受託者）により、迅速且つ確実に切り替えが行える方法を定める。
拡張性	BCP 発動時に必要なサービスは、基盤系サービスのみとなっているが、今後、業務系基幹システムが更新される際に追加となる可能性がある。

3.10 サービス管理

3.10.1　業務内容

サービス管理は、「機構内・在外利用者向け業務」、「機構内・在外利用者向けヘルプデスク」、「ユーザからの申請対応」、「セキュリティ運用」、「システム監視」、「障害管理」、「性能管理」、「可用性管理」、「利用者満足度調査」からなる業務である。業務内容の詳細については、「別添資料 05 要件定義書」のうちシステム運用要件を参照のこと。

3.10.2　基本要件

以下の点に留意し、日本語又は英語で対応すること。なお、現行の実績における英語による問い合わせ対応比率は全体の約 1 割程度である。問い合わせ内容（目的・ニーズ、緊急性、困っている点など）を十分に理解すること。

- ユーザから何らかのアクション（問題対応など）を求められた場合は、可能な限り解決策の具体的な提案を行うこと（できないという回答を安易に行わないこと）。
- 最終的に「できない」という回答を行う場合にも、問い合わせ者に納得してもらえるよう常に十分な説明を行うこと。
- 問い合わせ者は、必ずしもシステム等に関する基本理解や情報通信技術に関する知識等を十分に持っているとは限らないため、特に技術的な専門用語の濫用は避け、一般的に分かりやすい説明を行うこと。

なお、ヘルプデスクを効率的に運用するための体制・仕組み、ユーザ申請を効率的に運用するための体制・仕組み、障害管理における関連ベンダーとの責任範囲の調整、システム監視・障害管理・性能管理・可用性管理における管理ツールや自社の方法論の活用による効率化・工夫について提案すること。

3.11 問題管理

3.11.1　業務内容

問題管理は、「障害の原因となる問題対応状況の追跡」、「障害の傾向分析と未然防止策の立案」、「問題対応状況の記録と報告」からなる業務である。業務内容の詳細については、「別添資料 05 要件定義書」のうちシステム運用要件を参照のこと。

なお、再現しない障害についての管理・対応方法について提案すること。

3.12 変更管理

3.12.1　業務内容

変更管理は、「障害・問題・構成管理からのシステム変更要求の管理」、「変更情報の収集・管理」からなる業務である。業務内容の詳細については、「別添資料 05 要件定義書」のうちシステム運用要件を参照のこと。

3.13 リリース管理

3.13.1　業務内容

リリース管理は、「変更・構成管理からのリリース情報の管理」、「リリース情報の収集・管理」、「リリース作業の計画」、「リリース作業への立会い・作業支援」、「リリース内容の走行検証」からなる業務である。業務内容の詳細については、「別添資料 05 要件定義書」のうちシステム運用要件を参照のこと。

3.14 構成管理

3.14.1　業務内容

構成管理は、「構成情報の収集・維持・他ベンダーへの提供」からなる業務である。業務内容の詳細については、「別添資料 05 要件定義書」のうちシステム運用要件を参照のこと。

3.15 資産管理

3.15.1　業務内容

資産管理は、「国際協力機構保有又は賃貸借物件の棚卸実施と管理情報と更新」、「機構への管理情報の提供」からなる業務である。業務内容の詳細については、「別添資料 05 要件定義書」のうちシステム運用要件を参照のこと。

3.16 ソフトウェア管理

3.16.1　業務内容

ソフトウェア管理は、「ソフトウェアライセンス管理」、「機構への管理情報の提供」からな

る業務である。業務内容の詳細については、「別添資料 05 要件定義書」のうちシステム運用要件を参照のこと。

3.17 セキュリティ管理

3.17.1　業務内容

セキュリティ管理は、「セキュリティインシデント発生時の対応手順の整理」、「セキュリティに係る動向の状況把握」、「セキュリティ情報の収集（日次）とセキュリティ脆弱性への対応」、「新規システムの接続に伴うセキュリティの検討」、「セキュリティ標準の変更に伴う検討」からなる業務である。業務内容の詳細については、「別添資料 05 要件定義書」のうちシステム運用要件を参照のこと。

なお、JICA 情報通信網事業者が提供する各種ログ等と連携し、必要に応じてセキュリティログ相関分析機能を駆使し、インシデントに主体的に対応すること。平時のセキュリティ動向（最新情報）の把握方法、迅速な緊急インシデント対応の手順・方法、セキュリティインシデント対応のための通信事業者との連携については提案すること。

3.18 ドキュメントの整備及び管理

3.18.1　業務内容

ドキュメントの整備及び管理は、「ドキュメントの整備及び管理」からなる業務である。業務内容の詳細については、「別添資料 05 要件定義書」のうちシステム運用要件を参照のこと。

3.19 全体管理

3.19.1　業務内容

全体管理は、「関係事業者含めた全体管理」、「運用作業スケジュールの管理」、「運用事業者自身の工程管理」、「セキュリティインシデントに係る対応」からなる業務である。業務内容の詳細については、「別添資料 05 要件定義書」のうちシステム運用要件を参照のこと。

3.20 セルフモニタリング

3.20.1　業務内容

セルフモニタリングは、「セルフモニタリングの実施」、「モニタリング項目一覧及び合意書の維持管理」からなる業務である。業務内容の詳細については、「別添資料 05 要件定義書」のうちシステム運用要件を参照のこと。

3.20.2　基本的な考え方

システム運用等要件ごとに機構が期待する付加価値（品質）を提供できているかのサービスレベルの達成状況を管理するための“モニタリング項目”を設定し、定期的に受託者がその達成度を自己評価（セルフモニタリング）し、機構へ報告する。機構はその報告内容を評価し、最終的な達成度を決定する。

目標が達成できなかった項目についてはその未達成度合によりペナルティポイントが課さ

れ、一定のポイントが累積した時点で減額対象となる。また、受託者が独自に追加アウトプットを提案・報告し、その有効性を機構も評価した場合には、評価ポイントを付与し、ペナルティポイントの相殺に使用することを認める。

受託者は、運用設計時にモニタリング項目等を確認・精査し、機構と協議の上モニタリング項目及びサービスレベルの管理手順を確立させること。

なお、セルフモニタリング業務の流れ、追加モニタリング項目、モニタリング項目の要求値の引き上げのタイミング、その実施方法について提案すること。

3.20.3　管理運用ルール

(1) 日々の運用業務

受託者は、本業務開始当初から日々の運用等業務にてPDCAサイクルが確実に回り、運用等業務が維持・改善・向上する運用等業務を実施する。

その運用等業務において、モニタリング項目に係るサービスの提供状況の把握・管理・改善を実施し、提供するサービスの品質、作業プロセスの的確性やコストの妥当性を自ら検証、改善する。

(2) モニタリング

受託者は、項目毎のサービスレベルの達成状況をチェック（セルフモニタリング）し、問題があれば運用等業務の改善を実施する。そのセルフモニタリング結果については四半期／年次でモニタリング報告書として提出する。

(3) 年次評価

受託者は、セルフモニタリング結果を含む実施した運用等業務が機構における効率的な業務の遂行の実現にどの程度貢献しているかの評価を実施し、その評価の結果問題があれば運用等業務の改善を実施する。その結果を機構と協議し、目標の達成状況を共有（機構より達成状況の判断について説明の場を設定するが、最終判断は機構で行う）する。

3.20.4　サービスレベル管理の対象範囲

「2.2.3本業務の範囲」をサービスレベル管理の対象範囲とする。なお、本業務開始後に機構との調整により、対象範囲を変更する可能性がある。また、サービスレベル管理の開始時期は、受託者のデータセンターにてシステムの稼動が開始した時期とする。よって、システムの移行負荷の平準化等の理由により、前倒して稼動したシステムについては、稼動日をサービスレベル管理の開始日とする。

3.20.5 ペナルティポイント・評価ポイント

機構は受託者からの報告内容（セルフモニタリング結果）を評価し、最終的な達成度を判定する。目標が達成できなかった項目については、その未達成度合によりペナルティポイントが課され、一定のポイントが累積した時点で減額対象となる。また、受託者が独自に追加アウトプットを提案・報告し、その有効性を機構も評価した場合には、評価ポイントを付与し、ペナルティポイントの相殺に使用することが認められる。ペナルティポイント・評価ポ

イントの考え方は以下のとおり。

●定量的に算出するサービスレベル

評価：（目標達成）

（目標未達成）⇒影響度によりポイント設定

●定性的に算出するサービスレベル

評価：

S（要求以上の付加価値（品質））⇒評価ポイント＋1

A（要求通りの付加価値（品質））

B（要求未満（適切な再発防止措置が講じられている））

⇒ペナルティポイント＋1

C（要求未満（適切な再発防止措置が講じられていない））

⇒ペナルティポイント＋2

●ポイントの有効期限

ポイントの有効期限はポイント確定から 1 年間とする（翌年の同一四半期まで持ち越し）。

●ポイントの換算

ペナルティポイントは四半期ごとに支払いを確定させる時点で、累積で 20 ポイントを超過していた場合に超過したポイントについて換算するものとする。四半期ごとの支払時期が到来した時点で、その時点のペナルティポイントと評価ポイントを集計し、以下の計算式による減額金を、その時点の支払額から減額する。なお、ポイントの換算は、古いポイントから順に行うこととする。

●【減額金計算式（20 ポイント超過分）】

［減額金］＝｛［ペナルティポイント］－［評価ポイント］｝　×　10 万円

3.20.6　モニタリング項目

(1) 対象項目

モニタリングを実施すべき必要最低限の要求事項を「別添資料　07 モニタリング項目案」に記載している。受託者には、モニタリング項目案に記載した項目をベースとし、より付加価値（品質）の高いサービスが提供できるよう自律性を持ってモニタリング項目を設定することが求められる。なお、運用開始後初年度については、運用実績がないため、ペナルティの対象外とする項目を検討する場合がある。

(2) モニタリング項目における免責事項

別途契約書にて定める免責事項に該当する場合は、モニタリング結果におけるペナルティ等の適用範囲から除外する。ただし、そのような場合であっても報告対象として報告義務を負う。

3.20.7　モニタリング結果対応

機構は、モニタリング状況が継続して悪化している場合や機構の求めるサービスが提供されていないと判断した場合には、ポイント換算による減額のほか、契約自体の解除など

の対応を行う場合がある。

(1)契約上の対応

機構は、受託者が契約の規程に著しく違反した場合、又は契約内容を的確に履行せず、的確に履行する見込みがない場合、別に、契約書に定める内容に基づき、契約解除等を行う。

(2)財務上の対応

受託者は、モニタリングのポイント換算による減額とは別に、契約書に定める内容に基づき、損害賠償を請求する場合がある。

4. 本業務の実施に係る想定体制

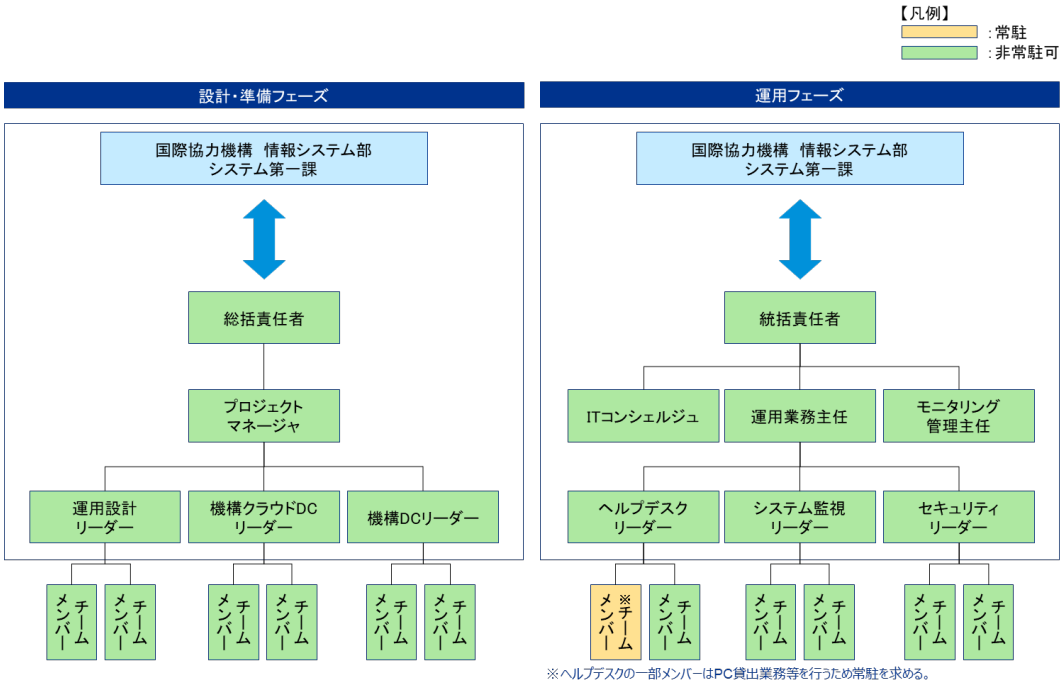
本業務の実施に係わる想定体制は以下のとおりである。具体的な体制については、受託者の提案内容をもとに、機構と受託者にて協議の上決定するものとする。また、「受託者（共同企業体を結成する場合は、その代表者及び構成員）の従業員とする範囲」については、図表 4-1 に示す。なお、業務系システムの移行負荷を平準化する等の理由により、前倒しでシステムの一部を稼働させる場合には、開始日からサービスレベルを管理できる体制を準備することとする。

設計・準備フェーズにおいては、プロジェクトマネージャー、運用設計リーダー、機構クラウドDCリーダー、機構DCリーダー、運用フェーズにおいては、運用業務主任、ITコンシェルジュ、ヘルプデスクリーダー、システム監視リーダー、セキュリティリーダーは専任で本作業にあたること。なお、機構クラウドDCリーダー、機構DCリーダーについては兼任を認める。

また、運用フェーズにおいては、機構からの緊急対応依頼やインシデント対応に即時に対応できる体制を構築できるのであれば常駐、非常駐は問わない。ただし、ヘルプデスクのPC貸出業務等の一部担当者は機構本部内に常駐とする。

なお、統括責任者、プロジェクトマネージャー及び運用業務主任を担う者は、運用等に関する本業務全般の知識を有しており、受託者内部にも機構に対しても説得力を持って調整・交渉ができる必要がある。

また、同じフェーズ内では、一人が複数の主要な業務を兼務しないこと。



【図表 4-1　本業務の実施に係る想定体制】

※総括責任者、プロジェクトマネージャー、運用業務主任、モニタリング業務主任、各リーダー以外の補強又は再委託を認める。

再委託を行う場合、受注者は、再委託先における業務の実施場所および安全管理措置（情報セキュリティ対策）を書面で発注者に提出し、発注者の承諾を得ること。発注者は書面内容を確認し適切な安全管理措置であることを踏まえ書面にて結果を報告する。 業務実施中は定期的に安全管理措置を適切に行われていることを履行状況として発注者に報告する。

4.1　主な業務従事者の役割

上記体制の主な業務従事者の役割は以下の通り。

【図表 4-2　主な業務従事者の役割】

No.	主要な業務従事者	想定する役割
1	統括責任者	受託者における、業務全体の責任者。
2	プロジェクトマネージャー	設計・準備フェーズにおける業務実施計画の立案、業務に係る全作業の統括、品質・進捗・課題（リスク）管理を行う。機構との協議・調整の窓口。
3	運用設計リーダー	本サービス全体の設計（運用、管理、セルフモニタリング等）の実施。
4	機構クラウド DC リーダー	機構クラウド DC の設計、構築、SaaS サービスの利用設計等の実施。
5	機構 DC リーダー	機構 DC のハウジングサービスの設計、構築の実施。
6	運用業務主任	運用フェーズにおける業務全作業の統括、品質・進捗・課題（リスク）管理を行う。当機構との協議・

No.	主要な業務従事者	想定する役割
		調整の窓口。
7	IT コンシェルジュ	運用フェーズにおける作業グループとは一定の距離を置き、プロジェクト実施支援等の各部システム化支援、および情報システム部にて主管する情報基盤（IT 共通インフラ）整備に係る支援を行う。
8	モニタリング管理主任	運用フェーズの主にセルフモニタリングに係る作業の統括、管理を行う。
9	ヘルプデスクリーダー	ユーザ問い合わせ対応の取りまとめ、品質・進捗・課題（リスク）管理を行う。チームメンバー管理も行う。
10	システム監視リーダー	運用監視関連情報の提供、品質・進捗・課題（リスク）管理を行う。
11	セキュリティリーダー	セキュリティの脅威に対する防御策の計画・実施、インシデント時の対応と脅威の除去、恒久的な対策の計画・実施、セキュリティ動向の情報収集・提供および改善の提案を行う。また、CSIRT 要員としての業務を行う。

4.2　実施体制全体の構築

受託者は、上記の統括責任者、プロジェクトマネージャー、運用業務主任、各リーダーに加え、業務従事者（リーダーの下位に属し、個々の業務を行う者。バックヤードも含む。）を全て含めた本業務を行うための全体体制を構築し、組織図、全従事者の氏名、所属部署及び連絡先とともに、**主要な業務従事者**の経歴等について、契約後に機構に提出し、承諾を得ること（原則、技術提案書に記載された体制・要員と同一であること、その体制・要員は本業務完了時まで確保すること）。なお、機構が体制に不備があると判断した場合等においては、体制、要員等の変更を求めることができる。

また、運用フェーズの実施にあたり、月や日により、業務負荷が変動する場合がある。その際にも受託者はユーザに対するサービスレベルを維持・向上し続けるサービス提供体制を確保し、業務を円滑に実施すること（運用業務量に応じた柔軟な対応を行うこと）。

4.3　連絡体制の整備

プロジェクトマネージャー、運用業務主任、モニタリング主任は、障害への対応等のため常時、機構から連絡できる状態を維持しなければならない。ただし、機構の承諾を得て、代理の者が一時的にこれを勤めることができるものとする。

4.4　人員交代等の際における対応

受託者は、人員交代等が発生する場合は、後任者の氏名、所属部署、連絡先及び経歴を機構

に提出し、承諾を得ること。また、受託者は、人員交代等にあたって、それまで蓄積されてきた機構の業務やシステム等に関する知識、ノウハウ等が後任者等に確実に引き継がれるよう留意し、本業務の実施に支障が生じないようにすること。この場合、特別な理由がない限り前任者と後任者が並行して業務に従事する期間を設けるものとし、当該期間について、受託者は事前に機構と協議したうえで決定すること。

4.5 自社以外の業者との連携

受託者は、関係ベンダー等も含めた機構運用サイクルの中心的な役割を担うことを十分に認識すること。特に、複数ベンダー間の各種の調整等については、機構から運用業務全般を一任された者として適切に業務を実施することとし、調整の不備等による不具合が発生しないようにすること。

4.6 一部担当者の常駐場所

ヘルプデスクではPCの貸出・返却等の窓口業務を行うことから常駐が必要となる。窓口業務の常駐場所は本部（麹町および竹橋）を想定しているが、受託後に機構と協議の上で決定する。

他方で、機構外での業務実施するにあたり、受注者は業務実施前に機構外の業務実施場所および安全管理措置（情報セキュリティ対策）を書面で発注者に提出し、発注者の承諾を得ること。発注者は書面内容を確認し適切な安全管理措置であることを踏まえ書面にて結果を報告すること。 業務実施中は定期的に安全管理措置を適切に行われていることを履行状況として発注者に報告する。

5. 受託者に望まれる経験・能力等

本業務では、受託者である社（組織）が持つ経験・能力と、実際に本業務に従事する主要担当者の経験・能力の双方を活かした円滑な業務遂行が必須と考えるため、本業務の受託者が有することが望まれる経験・能力等を以下に列挙する。

5.1 社の経験・能力等

・基盤系サービスの設計開発またはサービス提供業務に関し、過去5年間で3件以上の実績を有していること。※本業務の規模程度の実績を有していることが望ましい。

・基盤系サービス及び業務系システムの運用管理業務に関し、過去5年間で3件以上の実績を有していること。※本業務の規模程度の実績を有していることが望ましい。

・データセンターの移行作業に関し、過去5年間で3件以上の実績を有していること。※本業務の規模程度の実績を有していることが望ましい。

・情報セキュリティ管理および対策実施業務に関し、過去5年間で3件以上の実績を有していること。

・品質マネジメントシステムに係る規格（ISO9001）の認証を、本業務の主担当部署が保持していること。

・情報セキュリティマネジメントシステムに係る規格（ISO27001）の認証を保持している部署が、本業務の主担当部署と連携する体制が組めること。

・個人情報保護に関する認証（プライバシーマーク又は同等の認証）を保持していること。

・本業務内容は多岐にわたっており、多種多様な専門性が必要となる。本要件定義書には現時点での最低限必要となる要件が示されているが、契約期間中に外部環境の変化等に伴い新たな要件が発生することも十分に想定しうる。そのような場合に対応しうる社としてのバックアップ体制があることが望ましい。

5.2 業務従事者の経験・能力等

各業務従事者の経験・能力等については、具体的な業務名称・業務内容・役割を明らかにすること。プロジェクト名のみの記載は認めない。

5.2.1プロジェクトマネージャー（設計・準備フェーズ）の経験・能力等

・プロジェクトマネージャー業務に関し、過去10年間で類似業務（データセンター及び共通基盤の提供、共通基盤を用いてのシステム運用・管理支援、ヘルプデスク、調査・提言の実施等の包括アウトソーシング業務）の経験（業務が分割された案件でも良い）が2件以上を有していること。

※上記は、本業務の規模程度の実績を有していることが望ましい。

・本業務を実施する上で、以下のような有益な資格等を保持していることが望ましい。

- PMP、情報処理技術者試験プロジェクトマネージャー
- ITサービスマネジメントファンデーション
- CISA、情報処理技術者試験システム監査技術者　等

5.2.2運用設計リーダー（設計・準備フェーズ）の経験・能力等

・システム運用設計業務に関し、過去5年間で3件程度の実績を有していること。※運用設計リーダーとして本業務の規模程度の実績を有していることが望ましい。

・本業務を実施する上で、以下のような有益な資格等を保持していることが望ましい。

- ITサービスマネジメントファンデーション
- マイクロソフト認定資格プログラム（MCP）
- 情報処理技術者試験システム監査技術者　等

5.2.3機構クラウドDCリーダー（設計・準備フェーズ）の経験・能力等

・クラウド環境におけるシステムの基盤設計に関し、過去5年で1件以上の実績を有していること。※機構クラウドDCリーダーとして本業務の規模程度の実績を有していることが望ましい。

・本業務を実施する上で、以下のような有益な資格等を保持していることが望ましい。

- ネットワーク技術資格（Cisco認定資格等）
- ITサービスマネジメントファンデーション
- マイクロソフト認定資格プログラム（MCP）
- 情報処理技術者試験データベーススペシャリスト　等

5.2.4機構DCリーダー（設計・準備フェーズ）の経験・能力等

・データセンター環境におけるシステムの基盤設計に関し、過去5年間で1件程度の実績を

有していること。※データセンター準備リーダーとして本業務の規模程度の実績を有していることが望ましい。

・本業務を実施する上で、以下のような有益な資格等を保持していることが望ましい。

- ネットワーク技術資格（Cisco 認定資格等）
- IT サービスマネジメントファンデーション
- マイクロソフト認定資格プログラム（MCP）
- 情報処理技術者試験データベーススペシャリスト　等

5.2.5運用業務主任（運用フェーズ）の経験・能力等

・システム運用業務に関し、5 年以上の実績を有していること。
※運用業務主任として本業務の規模程度の実績を有していることが望ましい。

・本業務を実施する上で、以下のような有益な資格等を保持していることが望ましい。

- PMP、情報処理技術者試験プロジェクトマネージャー
- IT サービスマネジメントファンデーション
- CISA、情報処理技術者試験システム監査技術者　等

5.2.6IT コンシェルジュ（運用フェーズ）の経験・能力等

・システム化企画・調達、システム開発管理業務に関し、3 年以上の実績を有していること。
※担当者として本業務の規模程度の実績を有していることが望ましい。

・本業務を実施する上で、以下のような有益な資格等を保持していることが望ましい。

- PMP、情報処理技術者試験プロジェクトマネージャー
- IT コーディネーター
- IT サービスマネジメントファンデーション
- CISA、情報処理技術者試験 IT ストラテジスト　等

・以下の業務内容を満足するための類似業務経験・知識・意欲・業務姿勢等を有することが望ましい。

※IT コンシェルジュとは、あらゆるユーザとの対応最前線として自ら恒常的に最新情報や教訓・知見を蓄積し、受託者が顧客志向を最大限発揮するために設置する機能及びその要員のことであり、本業務の中でも特に付加価値が求められる業務に関し、機動性・柔軟性・迅速性・プロセス的確性といった複合的な要素にかかる機構が求める品質レベルを十分に満足させるサービス提供を模範的に実践するもののことをいう。

5.2.7　モニタリング管理主任（運用フェーズ）の経験・能力等

・システム運用業務に関し、3 年以上の実績を有していること。※モニタリング管理主任として本業務の規模程度の実績を有していることが望ましい。

・本業務を実施する上で、以下のような有益な資格等を保持していることが望ましい。

- PMP、情報処理技術者試験プロジェクトマネージャー
- IT コーディネーター
- IT サービスマネジメントファンデーション
- CISA、情報処理技術者試験システム監査技術者　等

5.2.8　ヘルプデスクリーダー（運用フェーズ）の経験・能力等

・本業務の規模（ユーザ数等）程度のシステム関連のヘルプデスク（サービスデスク等）の業務およびその管理に関し、3 年以上の実績を有していること。

・本業務を実施する上で、以下のような有益な資格等を保持していることが望ましい。

- コンタクトセンター検定試験
- 情報処理技術者試験 IT サービスマネージャ　等

5.2.9 システム監視リーダー運用フェーズ）の経験・能力等

・本業務の規模（システム数等）程度のシステム運用監視業務に関し、3 年以上の実績を有していること。

・本業務を実施する上で、以下のような有益な資格等を保持していることが望ましい。

- IT サービスマネジメントファンデーション
- CISSP
- 情報処理技術者試験システム監査技術者　等

5.2.10 セキュリティリーダー（運用フェーズ）の経験・能力等

・本業務の規模（システム数等）程度のセキュリティ対策業務ならびにネットワーク機器、サーバおよびPC・スマートフォン等に対するに具体的なセキュリティの管理と対策業務（防御対策の計画・実施、検知、インシデント対応、恒久対策実施等）に関し、3 年以上の実績を有していること。

・本業務を実施する上で、以下のような有益な資格等を保持していることが望ましい。

- 情報処理安全確保支援士
- 情報処理技術者試験システム監査技術者
- CISSP 等

5.2.11　ヘルプデスク受付担当者の経験・能力等

・ヘルプデスクへの問い合わせは、本部・国内拠点に加え、在外拠点からも受け付ける必要があるため、日本語並びに英語によるコミュニケーションを充分に取ることができる（TOEIC スコア 700 点以上相当を有する・英語によるヘルプデスク受付経験がある等）こと。※英語による問い合わせ対応は全体の約 1 割程度であるため、受付担当者全員に対して英語経験・能力を求めるものではない。

・日本語を母国語としない場合は、「日本語能力検定 N1（旧 1 級）」相当の能力を有すること。

6. 納入成果物

受託者は、本業務にて作成した下記の資料を納入すること。なお、本業務上で形成された実務レベルのノウハウは全て本件契約の成果物と見なされる。このため、下記成果物として提出する内容にかかわらず、機構から求めがあった場合は、常時、実務ノウハウをすみやかに開示できるよう恒常的にノウハウの形式知化（第三者にも容易に理解可能なこと）を行うこと。

【図表 6-1　納入成果物】

期間	No.	資料名称	納入期限
設計・準備フェーズ	1	プロジェクト計画書	受託決定後 1 ヶ月以内
	2	サービス利用環境提供業務導入にかかわる各種設計書（要件定義書、基本設計書、詳細設計書等） ※上記には、ネットワーク構成図、フロア設計図、配線図及びラック間配線図等を含む	業務開始後四半期毎に納品（および請求・支払） 2023 年 12 月
	3	サービス利用環境提供業務導入に係わる各種計画書（テスト計画書、移行計画書、教育訓練計画書、引継ぎ計画書等）	
	4	サービス利用支援業務及びサービス運用管理業務実施のための各種設計書	2024 年 3 月
	5	サービス利用支援業務及びサービス運用管理業務実施のための各種計画書（「別添資料 05 要件定義書」のうちシステム運用要件に記載されている作業ごとの計画書等）	
	6	収支計画書	2024 年 5 月
	7	運用マニュアル・操作マニュアル	
	8	各種様式（運用業務で使用する申請書類等の様式）	
運用フェーズ	1	運用業務報告書（四半期／年次）	2024 年 7 月上旬（2024 年 6 月分）から項目に応じ四半期もしくは年次
	2	モニタリング報告書（四半期／年次）	
	3	収支計画書（四半期毎見直し版）	2024 年 7 月上旬（2024 年度第 1 四半期分）から四半期毎
	4	収支報告書（四半期毎）	
	5	その他作業ごとの報告書類・記録類全て	必要に応じて運用業務報告書・モニタリング報告書に添付する。また、機構から指示により随時提示・納入を行うこと。

納入成果物の作成については、プロジェクト計画書作成時に機構と成果物内容・イメージについて合意を得ること。但し、業務遂行中に受託者にて内容の調整を検討し、必要に応じて機構と協議した上で内容を見直し、より実効性の高い成果物となるよう考慮すること。

納入成果物の提出形態は、電子媒体（2 部）とし、日本語で作成すること。印刷出力時のレイアウトを充分に考慮し、用紙サイズは A4 縦置き横書き又は A4 横置き横書き、図表等必要に応じ A3 用紙を含める。納入場所は別途指定する。

以上

ハウジング対象一覧

No,	システム名	備考
1	共通サーバ基盤	2025年9月末でクラウド化する予定。 2025年10月以降は廃止。
2	MPS	
3	TV会議システム	
4	有償システム（通知書電子化システム）	2025年9月末でクラウド化する予定。 2027年5月以降は廃止。
5	無線LANシステム	
6	情報通信網	

業務系システム一覧（ハウジング対象）

No,	システム名	概要	共通サーバ基盤*で稼働 （共通サーバで稼働の場合「〇」）	備考
1	ボランティアシステム	ボランティア事業に係る業務のためのシステムで、募集・選考・訓練・研修、派遣・帰国後手続きを行う機能を有するシステム。	〇	
2	事業管理支援システム	各事業（有償、無償資金協力の本体事業を除く）の案件情報、実施計画（予算・進捗）、事業実績（統計情報）等を管理する機能を有するシステム。	〇	
3	派遣システム	専門家、調査団の派遣手続き、旅費や手当計算等を行うシステム。	〇	
4	経理業務統合システム	事業管理における経理業務・会計処理全般を担うシステム。予算管理、予算執行、資金管理、決算、物品管理、外貨管理機能及びマスタ管理機能（取引先、予算科目、勘定科目他）等の一連の業務機能を網羅する。	〇	
5	人材データベース	専門家、調査団、ボランティア等、国際協力に携わる人材を軸とした派遣関連データを管理するシステム。	〇	
6	無償資金協力実施監理システム	無償資金協力事業の案件進捗監理、資金計画、資金管理等の機能を有するシステム。	〇	
7	人事・勤怠システム	役職員の人事管理業務（評価、意向調査を含む）と勤務管理業務を行うシステム。	〇	
8	調達・契約管理システム	各事業の調達プロセス（契約決裁、公示、契約締結等）を一元的に管理・共有するためのシステム	〇	
9	DIGNITASシステム	機構の債権、債務を管理するためのシステム	〇	
10	ALMシステム	有償勘定の市場リスク管理、ALM（資産（Asset）と負債（Liability）の双方を一元的に総合管理（Management）する手法）において必要なリスク計量用の計算サーバ。	〇	
11	電子決裁システム	決裁の作成、回付、管理を行うためのシステム	〇	
12	研修事業総合システム	研修事業の形成、管理を行うためのシステム	〇	
13	デジタル法令・規程集	機構に関連する法令、機構の規程・細則をまとめたデータベース		

*各業務主管システムが稼働するハードウェアを提供する基盤。なお、データベースとしては共通DB基盤が稼働している。

本資料は2015年4月時点の情報であり業務開始時に最新情報を提示する。

共通サーバ基盤

番号	用途	機器名	ユニット	電源		重量	コンセント形状 ※特殊な形状の場合記載をお願いします。
			U	消費電力（W）	二重化	kg	
1	HB・監視LAN用スイッチ #2	Catalyst 2960-X	1	50.0		4.2	
2	HB・監視LAN用スイッチ #1	Catalyst 2960-X	1	50.0		4.2	
3	バックアップLAN用スイッチ #2	Nexus 3172T	1	440.0	○	10.0	
4	バックアップLAN用スイッチ #1	Nexus 3172T	1	440.0	○	10.0	
5	仮想化基盤サーバ #9	MAGNIA R3520d	2	528.0	○	24.3	
6	仮想化基盤サーバ #8	MAGNIA R3520d	2	528.0	○	24.3	
7	17型コンソールドロワー コンソールドロワー		1	34.0		13.0	
8	仮想化基盤サーバ #7	MAGNIA R3520d	2	528.0	○	24.3	
9	仮想化基盤サーバ #6	MAGNIA R3520d	2	528.0	○	24.3	
10	仮想化基盤サーバ #5	MAGNIA R3520d	2	528.0	○	24.3	
11	仮想化基盤サーバ #4	MAGNIA R3520d	2	528.0	○	24.3	
12	仮想化基盤サーバ #3	MAGNIA R3520d	2	528.0	○	24.3	
13	仮想化基盤サーバ #2	MAGNIA R3520d	2	528.0	○	24.3	
14	仮想化基盤サーバ #1	MAGNIA R3520d	2	528.0	○	24.3	
15	負荷分散装置 #2	Netwiser SX-3840	1	88.0		6.0	
16	負荷分散装置 #1	Netwiser SX-3840	1	88.0		6.0	
17	業務LAN用スイッチ #2	Nexus 3172T	1	440.0	○	10.0	
18	業務LAN用スイッチ #1	Nexus 3172T	1	440.0	○	10.0	
19	企画部次期業務主管システムDBサーバ #2	MAGNIA R3520d	2	324.0	○	24.1	
20	企画部次期業務主管システムDBサーバ #1	MAGNIA R3520d	2	324.0	○	24.1	
21	企画部次期業務主管システム疑似DBサーバ	MAGNIA R3520d	2	324.0	○	24.1	
22	バックアップサーバ #1	MAGNIA R3520d	2	324.0	○	24.1	
23	17型コンソールドロワー コンソールドロワー		1	34.0		13.0	
24	ログ管理サーバ #2	MAGNIA R3520d	2	326.0	○	24.1	
25	ログ管理サーバ #1	MAGNIA R3520d	2	326.0	○	24.1	
26	仮想化基盤サーバ #14	MAGNIA R3520d	2	528.0	○	24.3	
27	仮想化基盤サーバ #13	MAGNIA R3520d	2	528.0	○	24.3	
28	仮想化基盤サーバ #12	MAGNIA R3520d	2	528.0	○	24.3	
29	仮想化基盤サーバ #11	MAGNIA R3520d	2	528.0	○	24.3	
30	仮想化基盤サーバ #10	MAGNIA R3520d	2	528.0	○	24.3	
31	研修事業総合システムDBサーバ#2	MAGNIA R3520d	2	324.0	○	24.1	
32	研修事業総合システムDBサーバ#1	MAGNIA R3520d	2	324.0	○	24.1	
33	研修事業総合システムDBサーバ(ステージングサーバ)	MAGNIA R3520d	2	324.0	○	24.1	
34	調達部次期業務主管システムDBサーバ #2	MAGNIA R3520d	2	324.0	○	24.1	
35	調達部次期業務主管システムDBサーバ #1	MAGNIA R3520d	2	326.0	○	24.1	

本資料は2015年4月時点の情報であり業務開始時に最新情報を提示する。

36	調達部次期業務主管システム検証用DBサーバ	MAGNIA R3520d	2	326.0	○	24.1	
37	派遣システムDBサーバ #2	MAGNIA R3520d	2	324.0	○	24.1	
38	派遣システムDBサーバ #1	MAGNIA R3520d	2	324.0	○	24.1	
39	17型コンソールドロワー コンソールドロワー		1	34.0		13.0	
40	派遣システム疑似派遣DBサーバ	MAGNIA R3520d	2	324.0	○	24.1	
41	経理業務統合システムDBサーバ #2	MAGNIA R3520d	2	324.0	○	24.1	
42	経理業務統合システムDBサーバ #1	MAGNIA R3520d	2	336.0	○	24.1	
43	経理業務統合システム検証用Web/Ap/DB 共用サーバ	MAGNIA R3520d	2	326.0	○	24.1	
44	ボランティアシステムDBサーバ#2	MAGNIA R3520d	2	326.0	○	24.1	
45	ボランティアシステムDBサーバ#1	MAGNIA R3520d	2	324.0	○	24.1	
46	ボランティアシステム(ステージング)DBサーバ	MAGNIA R3520d	2	324.0	○	24.1	
47	FC/SW FCスイッチ #4	HITACHI SWG610	1	108.0	○	9.2	
48	FC/SW FCスイッチ #3	HITACHI SWG610	1	108.0	○	9.2	
49	ストレージ 拡張筐体 #9	VSP G600	2	445.6	○	30.0	
50	ストレージ 拡張筐体 #8	VSP G600	2	445.6	○	30.0	
51	ストレージ 拡張筐体 #7	VSP G600	2	445.6	○	30.0	
52	ストレージ 拡張筐体 #6	VSP G600	2	445.6	○	30.0	
53	ストレージ 拡張筐体 #5	VSP G600	2	445.6	○	30.0	
54	ストレージ 拡張筐体 #4	VSP G600	2	445.6	○	30.0	
55	ストレージ 拡張筐体 #3	VSP G600	2	445.6	○	30.0	
56	ストレージ 拡張筐体 #2	VSP G600	2	445.6	○	30.0	
57	ストレージ 拡張筐体 #1	VSP G600	2	445.6	○	30.0	
58	ストレージ 基本筐体	VSP G600	2	1082.0	○	85.0	
59	FC/SW FCスイッチ #2		1	108.0	○	9.2	
60	FC/SW FCスイッチ #1		1	108.0	○	9.2	
61	負荷分散装置(DMZ用) #2	Netwiser SX-3840	1	88.0		6.0	
62	負荷分散装置(DMZ用) #1	Netwiser SX-3840	1	88.0		6.0	
63	DMZLAN用スイッチ #2	Catalyst 2960-X	1	50.0		4.2	
64	DMZLAN用スイッチ #1	Catalyst 2960-X	1	50.0		4.2	
65	研修事業総合システムWebサーバ(外部公開用) #2	MAGNIA R3310e	1	150.0	○	17.2	
66	研修事業総合システムWebサーバ(外部公開用) #1	MAGNIA R3310e	1	150.0	○	17.2	
67	派遣システム外部WWWサーバ #2	MAGNIA R3310e	1	151.0	○	17.2	
68	派遣システム外部WWWサーバ #1	MAGNIA R3310e	1	151.0	○	17.2	
69	MGC接続サーバ#2	Express5800/R120h-1M	1	190.0	○	18.6	
70	MGC接続サーバ#1	Express5800/R120h-1M	1	190.0	○	18.6	
71	ストレージ 拡張筐体 #18	VSP G600	2	452.8	○	30.0	
72	ストレージ 拡張筐体 #17	VSP G600	2	452.8	○	30.0	
73	17型コンソールドロワー コンソールドロワー		1	34.0		13.0	
74	ストレージ 拡張筐体 #16	VSP G600	2	452.8	○	30.0	
75	ストレージ 拡張筐体 #15	VSP G600	2	452.8	○	30.0	

本資料は2015年4月時点の情報であり業務開始時に最新情報を提示する。

76	ストレージ　拡張筐体　#14	VSP G600	2	452.8	○	30.0	
77	ストレージ　拡張筐体　#13	VSP G600	2	452.8	○	30.0	
78	ストレージ　拡張筐体　#12	VSP G600	2	452.8	○	30.0	
79	ストレージ　拡張筐体　#11	VSP G600	2	450.7	○	30.0	
80	ストレージ　拡張筐体　#10	VSP G600	2	445.6	○	30.0	
81	経理業務統合システム(新環境)DBサーバ　#2	HPE ProLiant DL380 Gen10	2	324.0	○	24.1	
82	経理業務統合システム(新環境)DBサーバ　#1	HPE ProLiant DL380 Gen10	2	336.0	○	24.1	
83	経理業務統合システム(新環境)検証用 Web/Ap/DB 共用サーバ	HPE ProLiant DL380 Gen10	2	326.0	○	24.1	
84	17型コンソールドロワー　コンソールドロワー		1	34.0		13.0	
85	ALMサーバ	Express5800/R120h-2M	2	411.0	○	24.4	
86	人材DB　検証DBサーバ	Express5800/R120h-2M	2	211.0	○	23.5	
87	人材DB　本番DBサーバ#2	Express5800/R120h-2M	2	211.0	○	23.5	
88	人材DB　本番DBサーバ#1	Express5800/R120h-2M	2	211.0	○	23.5	
89	MagicConnect接続サーバ#2	Express5800/R120h-1M	1	190.0	○	16.1	
90	MagicConnect接続サーバ#1	Express5800/R120h-1M	1	190.0	○	16.1	

本資料は2015年4月時点の情報であり業務開始時に最新情報を提示する。

MPS

番号	用途	機器名	ユニット	電源		重量	コンセント形状 ※特殊な形状の場合記載をお願いします。
			U	消費電力（W）	二重化	kg	
1	MPS ICカード認証出力システム　Hyper-Vサーバ#1	HPE ProLiant DL360 Gen10	1	331.0	○	16.3	
2	MPS ICカード認証出力システム　Hyper-Vサーバ#2	HPE ProLiant DL360 Gen10	1	331.0	○	16.3	
3	管理用L2スイッチ	AT-GS950/8	2	9.4		1.5	
4	KVM切替器	ATEN CS1308 KVMサーバーコンソールスイッチ G2 (1x8)	1	2.3		1.9	
5	キーボード一体型 TFTモニター	LCD 8500 コンソール	1	36.0		5.2	
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							

本資料は2015年4月時点の情報であり業務開始時に最新情報を提示する。

TV会議

番号	用途	機器名	ユニット	電源		重量	コンセント形状 ※特殊な形状の場合記載をお願いします。
			U	消費電力（W）	二重化	kg	
1	MCU#1	RMX2000	3	900.0	×	16.5	
2	MCU#2	MGC-50	10	1000.0	×	24.0	W38.1×D50.2×H40.8　非稼働
3	会議録画装置	RSS4000	2	1000.0	○	19.5	W44.1×D48.5×H8.9　非稼働
4	INS1500用DSU(MCU#1用、03-5635-1160)	I-1500DSU	1(据置)	10.0	×	0.6	W11×D17×H3.5
5	インターネットルータ	BUFFALO BBR-4HG	1(据置)	3.6	×	0.3	W14.5×D12.4×H3.3
6	フレッツ光ネクスト(ファミリーHSタイプ)用ONU	GE-PON-ONU	1(据置)	4.0	×	0.5	W16.3×D15.6×H3.3
7	TV会議用L3スイッチ#1	CISCO WS-C3750-24TS-E	1	50.0	×	3.6	W44.5×D30.1×H4.39
8	TV会議用L3スイッチ#2	CISCO WS-C3750-24TS-E	1	50.0	×	3.6	W44.5×D30.1×H4.39
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							

本資料は2015年4月時点の情報であり業務開始時に最新情報を提示する。

有償システム（通知電子化システム）

番号	用途	機器名	ユニット	電源		重量	コンセント形状 ※特殊な形状の場合記載をお願いします。
			U	消費電力（W）	二重化	kg	
1	通知書電子化サーバ	PRIMERGY RX300 S8	4	1660.0	○	50.0	
2	スーパーマルチドライブ	USB DVD スーパーマルチドライブユニット	1	2.0		0.6	
3	汎用テーブル	汎用テーブル(19R-26TR2)	1	-		11.0	
4	通知書電子化サーバ	PRIMERGY RX2540 M5	4	1950.0	○	50.0	
5	スーパーマルチドライブ	USB DVD スーパーマルチドライブユニット	1	10.0		0.4	
6	汎用テーブル	汎用テーブル(19R-26TR2)	1	-		11.0	
7	通知書電子化WAF装置	IPCOM EX2300 SC	2	262.2	○	28.0	
8	通知書電子化サーバ用コンソール	17インチ・ラック・コンソール	1	20.0		12.5	
9	切替器	KVMｽｲｯﾁ(4ﾎﾟｰﾄ)	1	7.3		1.6	
10	通知書電子化WAF装置	IPCOM EX2-3200	1	360.0	○	30.0	
11	通知書電子化サーバ用コンソール	17インチ・ラック・コンソール	1	25.0		12.5	
12	切替器	KVMｽｲｯﾁ(4ﾎﾟｰﾄ)	1	7.3		1.6	
13	通知書電子化DMZ L3スイッチ	Catalyst 3650-24TS	2	114.2	○	13.7	
14	通知書電子化Intra L3スイッチ	Catalyst 3650-24TS	2	114.2	○	13.7	
15	通知書電子化DMZ L2スイッチ	Catalyst 2960X-24TS-L	2	74.2	○	8.0	
16	通知書電子化Intra L2スイッチ	Catalyst 2960X-24TS-L	2	74.2	○	8.0	
17	Cisco Systems 電源冗長化(DMZ L2SW用)	RPS2300	1	380.6		8.5	
18	Cisco Systems 電源冗長化(Intra L2SW用)	RPS2300	1	380.6		8.5	
19							
20							
21							
22							
23							
24							
25							
26							

本資料は2015年4月時点の情報であり業務開始時に最新情報を提示する。

無線LAN

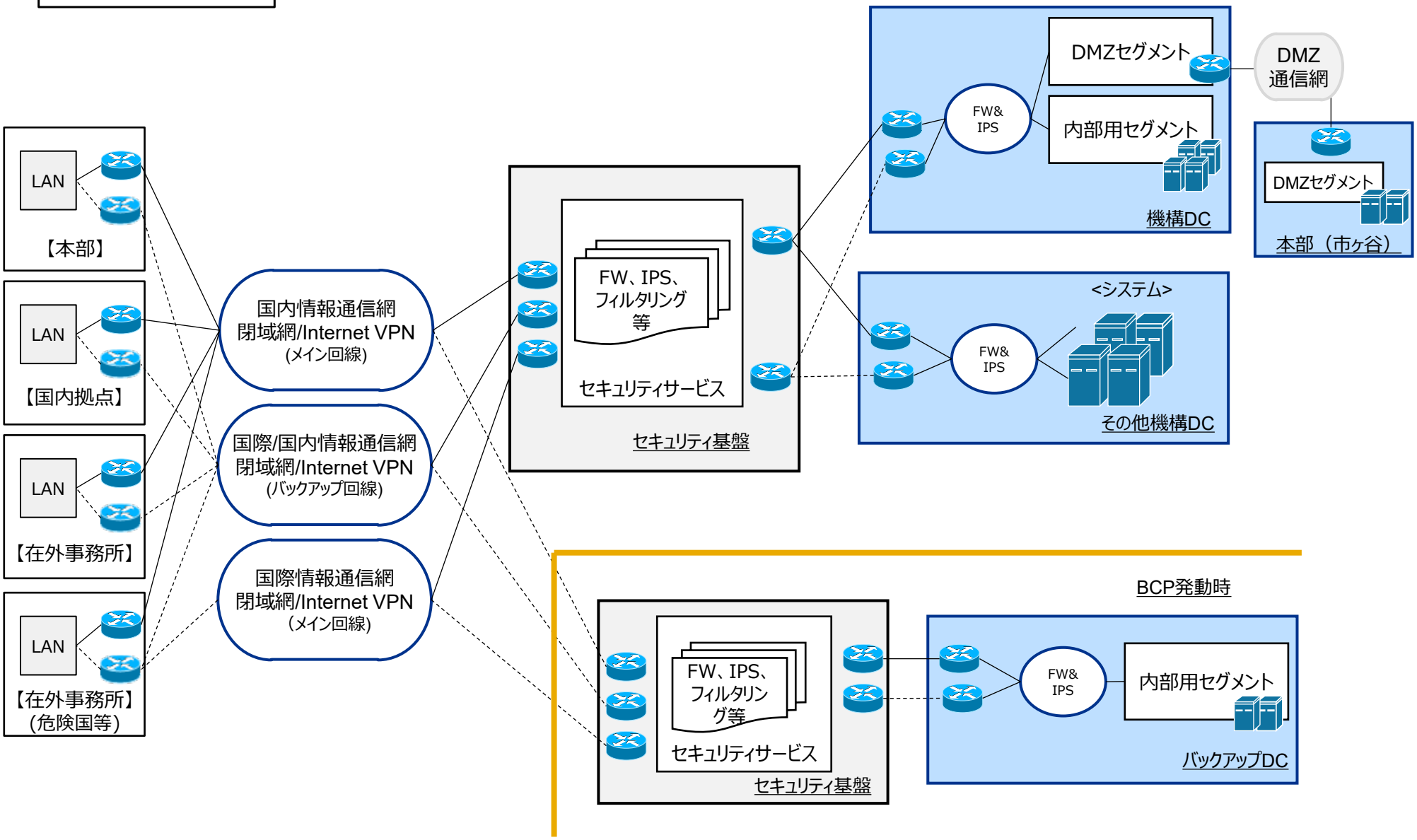
番号	用途	機器名	ユニット	電源		重量	コンセント形状 ※特殊な形状の場合記載をお願いします。
			U	消費電力（W）	二重化	kg	
1	ワイヤレスLANコントローラー(MDCF-03W-	Cisco WLC5520 A2	1	190.0	○	13.6	
2	ワイヤレスLANコントローラー(MDCF-03W-	Cisco WLC5520 A2	1	190.0	○	13.6	
3	無線認証サーバ（MDCF-03W-IS01）	Secure Network Server 3655	1	770.0	○	17.0	
4	無線認証サーバ（MDCF-03W-IS02）	Secure Network Server 3655	1	770.0	○	17.0	
5	アクセススイッチ（MDCF-03W-AS02）	Catalyst2960S-24PS-L	1	370.0		5.7	
6	アクセススイッチ（MDCF-03W-AS02）	Catalyst2960S-24PS-L	1	370.0		5.7	
7	無線LAN管理装置（MDCF-03W-PI01）	NCSアプライアンス	1	780.0		14.0	
8	ワイヤレスLANコントローラー(MDCF-03W-	Cisco WLC5508	1	115.0	○	9.1	
9	ワイヤレスLANコントローラー(MDCF-03W-	Cisco WLC5508	1	115.0	○	9.1	
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							

情報通信網

番号	用途	機器名	ユニット	電源		重量	コンセント形状 ※特殊な形状の場合記載をお願いします。
			U	消費電力（W）	二重化	kg	
1	SD-WANルータ（Intenal用）	C8500L-8S4X	1	1100.0	○	7.7	
2	SD-WANルータ（Intenal用）	C8500L-8S4X	1	1100.0	○	7.7	
3	SD-WANルータ（DMZ用）	C1121-4P	1	66.0		1.6	
4	SD-WANルータ（DMZ用）	C1121-4P	1	66.0		1.6	
5	HUB	ES1008TP	1	3.5		1.1	
6	HUB	ES1008TP	1	3.5		1.1	
7	回線終端装置	ONU	1	–		–	
8	回線終端装置	ONU	1	–		–	
9	回線終端装置	ONU	1	–		–	
10	回線終端装置	ONU	1	–		–	
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							

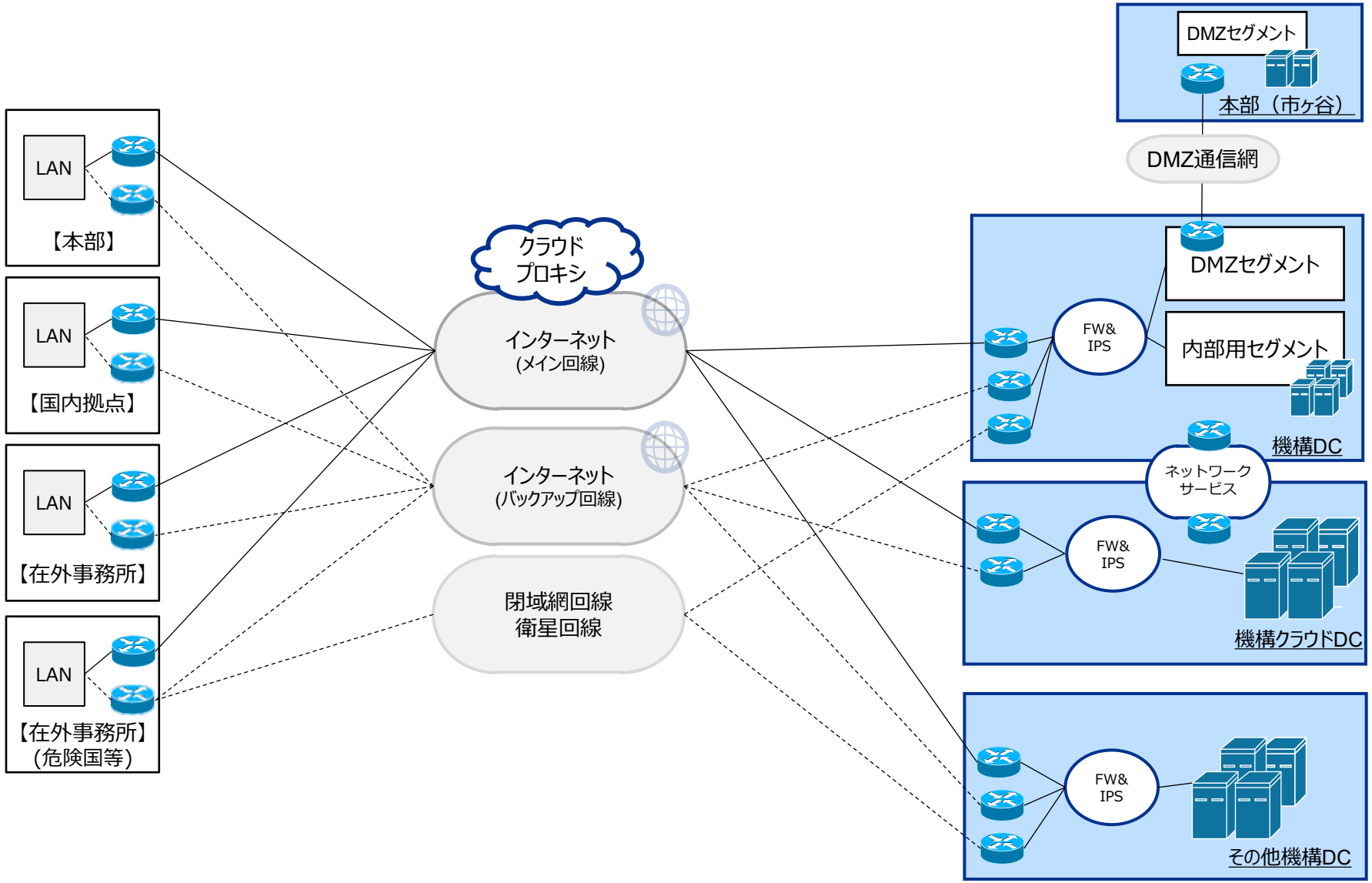
JICA情報通信網概要

現行ネットワーク構成



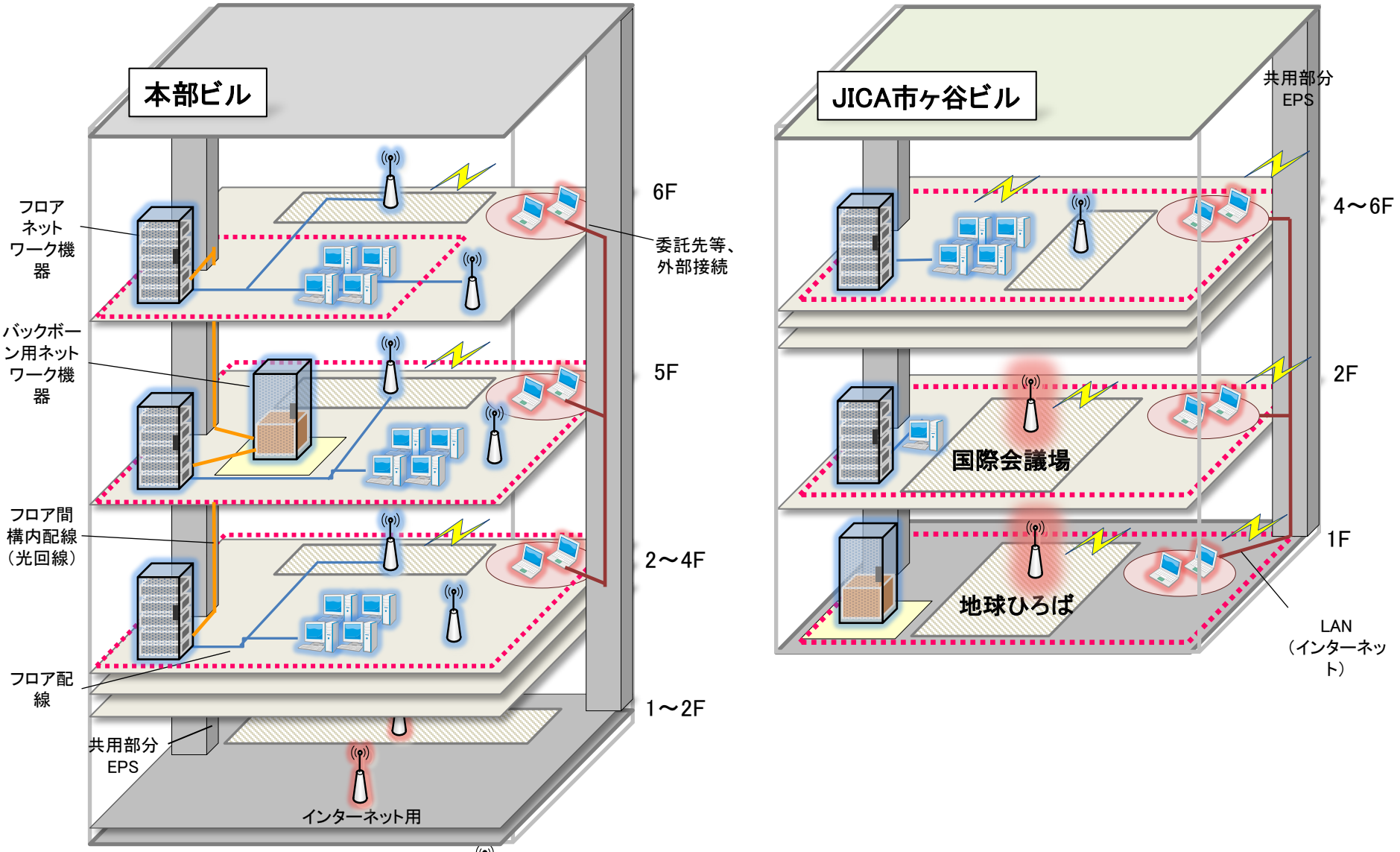
JICA情報通信網概要

新規ネットワーク構成



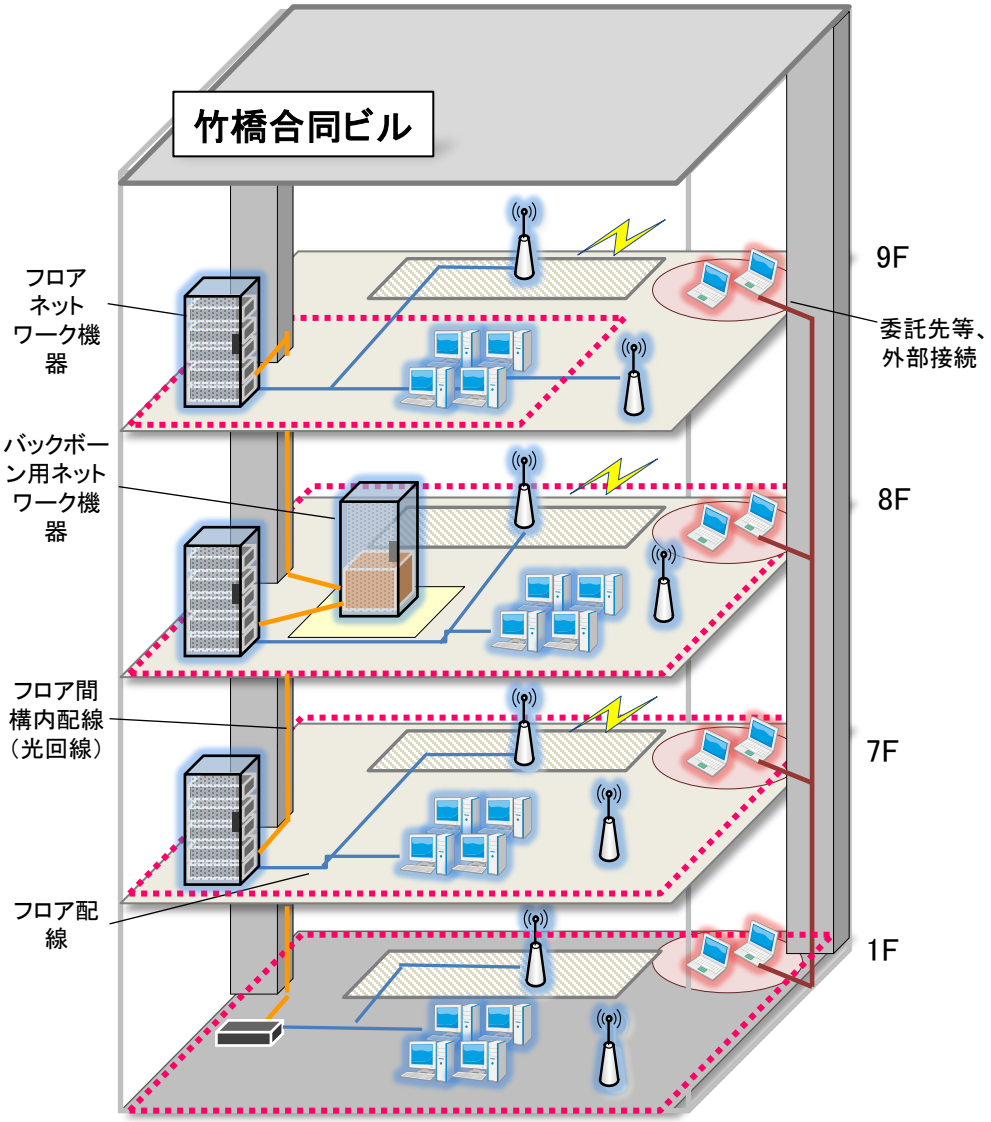
JICA情報通信網概要

本部LAN構成概要



本部LAN構成概要

JICA情報通信網概要



;会議室等　;機械室　;調達機器等（一部、無線LAN用配線含む）　;システム第1課所掌範囲　;執務室LAN　;他事業用LAN

No	用途	機種	数（台）	備考
1	コアスイッチ	Catalyst 6506E	2	
2	ディストリビューション機能	Catalyst 3750X-24T	20	
3	アクセススイッチ	Catalyst 2960S-48	93	POE機能
4	情報システム室分室接続用スイッチ	Catalyst 3750X-48T	2	
5	外部通信接続機能	Catalyst 3750X-24T	2	
6	業務サーバ接続機能	Catalyst 3750X-24T	2	
7	無線LAN接続用スイッチ兼サーバ接続機能	Catalyst 2960	12	POE機能
8	JICAーLAN用無線LANコントローラ		1	
9	JICAーLAN用無線LANアクセスポイント		35	
10	無線LAN用認証システム		1	
11	ファイアウォール		1	
12	インターネット回線			100Mbps程度のISPサービス（ルーター付き）

No	用途	機種	数（台）	備考
1	ディストリビューションスイッチ	Catalyst 3750X-24T	2	
2	アクセススイッチ	Catalyst 2960S-48PST-L	15	POE機能
		Catalyst 2960S-24	5	POE機能
		Catalyst 2960C-8TC-S	30	
3	無線LAN接続用スイッチ（Catalyst 2960S-24）	Catalyst 2960S-24	6	POE機能
4	JICAーLAN用無線LANアクセスポイント	Aironet 3602	35	
5	ファイアウォール		1	
6	インターネット回線			10Mbps程度のISPサービス（ルーター付き）

No	用途	機種	数（台）	備考
1	コアスイッチ	Catalyst 3850-24T	2	
2	ディストリビューションスイッチ	Catalyst 3650-24T	6	
3	アクセススイッチ	Catalyst 2960S-48PST-L	15	POE機能
4	JICAーLAN用無線LANアクセスポイント	Aironet 3602	35	
5	ファイアウォール	Fortigate-900	1	
6	インターネット回線			1Gbps SPサービス（ルーター付き）

標準ノートパソコン

No	分類	機器仕様
1	機種	dynabook G83/HU
2	CPU	Intel® Core™ i7-1165G7
3		2.80GHz（インテル®ターボ・ブースト・テクノロジー2.0対応：最大4.70GHz）
4	メモリ	16GB
5	ディスプレイ	13.3型FHD（IGZO・ノングレア）
6		1920×1080ドット
7	ストレージ	512GB SSD(PCIe対応)
8	LAN	1000Base--T／100Base--TX／10Base--T
9	無線LAN	Wi-Fi 6（IEEE802.11ax）（2.4Gbps）対応＋IEEE802.11ac/a/b/g/n準拠（WPA™ /WPA2™/WPA3™対応、WEP対応、AES対応、TKIP対応）
10	Webカメラ	有効画素数 約92万画素（デュアルマイク付）
11	インターフェース	HDMI®出力端子×１
12		LAN（RJ45）×１
13		USB3.1（Gen1）×２
14		マイク入力/ヘッドホン出力端子×１
15		Thunderbolt™4（USB4™Type-C）コネクタ（電源コネクタ）×２
16	非電源供給時の連続駆動時間	24時間
17	PC本体重量	約888g
18	PC本体サイズ	横306mm×縦210mm×高さ17.9mm
19	周辺機器	ACアダプタ（2式）
20		USBType-C接続ドッキングステーション
21		セキュリティワイヤー

公用スマートフォン

No	分類	機器仕様
1	機種	iPhone 12
2	サイズ	約71.5×146.7×7.4mm ／約162g
3	ディスプレイ	6.1インチ Super Retina XDRディスプレイ(2,532 x 1,170ピクセル)
4	モバイルカメラ	メイン：有効画素数約1200万画素 サブ：有効画素数約1200万画素 TrueDepthカメラ
5	CPU	Apple A14 Bionicチップ
6	Wi-Fi	MIMO対応 IEEE 802.11ax Wi-Fi 6
7	Bluetooth®	Ver.5.0
8	赤外線通信	非対応
9	プラットフォーム	iOS 15.4～
10	容量	64GB
11	充電器規格	Lightning
12	付属品	Lightning - USBケーブル、充電器、保護フィルム、保護ケース、４極ミニプラグ変換コネクタ
13	機能	電話、カメラ、ビデオ撮影、Face ID、Safari(ブラウザ)、App Store、Teamsアプリ、Outlookアプリ、Officeアプリ ・・・等 ※一部機能については制限あり

標準端末ソフトウェア仕様

No	分類	ソフトウェア名	バージョン
1	Windows10 OS	Windows10 (64bit)	Enterprise 64bit版(21H2)
2	Microsoft Office	Microsoft 365 Apps for Enterprise Word、Excel、PowerPoint、Outlook、Acccess、 OneNote、Publisher、OneDrive、Teams	半期エンタープライズチャネル(プレビュー) 2202 32bit
3	Office関連ソフト	Microsoft Outlook テレビ会議用カスタム機能 （アドオン機能）	−
4	ブラウザ	Microsoft Edge	107.0.1418.62
5	セキュリティ	Microsoft Azure Information Protection	2.14.49.0
6		Zscaler	3.9.0.175
7	圧縮・解凍ソフト	Lhaplus	1.74
8	データベースソフト	FileMaker Pro	19.4.2.204(64bit)
9	音楽再生ソフト	Windows Media Player	12
10	動画編集ソフト	Microsoft フォト	−
11	ウイルス・スパイウェア対策ソフト	Microsoft Defender for Office365	−
12		Microsoft Defenderウィルス対策	−
13	PDF Reader	Adobe Reader DC	2.002.20212(64bit)
14		MAIP Plugin ForAdobe Acrobat Reader	21.007.20091(64bit)
15	.Net Framework	Microsoft .NET Framework 3.5	−
16	.Net Framework	Microsoft.NET Framework4.8Advanced Services	−
17	資産管理・運用監視ツール	LanScope CAT	9.4
18	リモート操作	Remote Desktop 日本語版	7
19	VDI	Citrix Workspace	22.02.0.15
20	画面共有ソフト	ISL Light Client	3.5.2
21	リモートアクセス	BIG-IP Edge Client	72.22.0308.1349
22	管理者権限管理	LAPSClient	6.2.0.0
23	ユーザ向けドキュメント	各種マニュアル等	−
24	ユーザ向けスクリプト	持出時に実行するスクリプトファイル	−
25	プリンタドライバ	MPSプリンタドライバ	2.7.0（9/3：1041.2:02070202）（x64）
26		出張用プリンタ（PSX05）用デバイスドライバ	2.41.00
27	証明書	Zscaler用のルート証明書	−

研修・会議用ノートパソコン			
No	スペック名称／実装機器名称	機器仕様	留意事項
1	機種	ノートパソコン(メーカーは統一すること)	
2	台数	52台	
以下現行の研修・会議用PCのスペック（参考情報）			
3	CPU	Intel® Core™ i5-1135G7	
4		4コア / 8スレッド / 2.40GHz [最大4.20GHz] / 8MBキャッシュ	
5	メモリ	8GB	
6	ディスプレイ	14.0型ワイド液晶パネル	
7		1920×1080ドット LEDバックライト / ノングレア	
8	ストレージ	256GB M.2 PCI Express 接続	
9	無線LAN	Wi-Fi 6 AX201 (IEEE 802.11ax/ac/a/b/g/n 最大2.4Gbps対応 ※連続160MHz帯域 Wi-Fi 6対応機器が必要) + Bluetooth 5 内蔵	
10	スピーカー	ステレオ スピーカー(内蔵)	
11	マイク	デュアルアレイマイク(内蔵)	
12	Webカメラ	有効画素数 約100万画素	
13	インターフェース	HDMI®出力端子×１	
14		USB3.0×1	
15		USB3.1×1	
16		マイク入力/ヘッドホン出力端子×１	
17		Thunderbolt™4（USB4™Type-C）×１	
18		電源コネクタ×1	
19	非電源供給時の連続駆動時間	20時間	
20	PC本体重量	約1.13g	
21	PC本体サイズ	横322mm×縦216mm×高さ16.9mm	
22	周辺機器	ACアダプタ（2式）	
23		USBType-C接続ドッキングステーション	
24		セキュリティワイヤー	
25		マウスデバイス（ホイール付き）	マウスデバイスは、ボール式ではないもの
26		ディスプレイ	
27		ディスプレイ台	
28		HDMIケーブル	
モバイルプリンタ			
1	型名	モバイルプリンタ	持ち運びを前提に開発されたプリンタであること
2	台数	150台（予備機含む）	

	3	本体サイズ等	・キャリーバッグに入るサイズであること ・重量約2.0kg以下とすること	
	4	印刷サイズ	A4、A5、レター、はがき等	
	5	その他	キャリーバッグ	キャリーバッグは、途上国への長距離出張時に携行することを考慮し、衝撃緩和材付のケースにすること。
プロジェクター				
	1	台数	12台	-
	2	本体サイズ・重量	約2.0kg程度以下であること	持ち運びが簡易であること
	3	有効光束（明るさ）	3,000lm以上	-
	4	解像度	WXGA（1280×800）以上	-
	5	外部ポート	・RGB（15ピン ミニD-sub）×1 ・HDMI/MHL×1 ・画像、音声の出力インターフェースを備えており、プロジェクター同士を接続して利用できることが望ましい。必要なケーブルも準備すること。	-
	6	スピーカー	1W以上の音声用スピーカーを備えていること	-
	7	レーザーポインター	照射機能のみ（数量；12）	マウス機能等の付加機能は不要
	8	その他	・タテ自動台形歪み補正機能 ・専用キャリーバック（肩掛けあり） ・プロジェクターのメーカーは、1社に統一すること	6～10人程度の会議室での利用を想定

バージョン	最終更新日	最終更新者
1.0.0	2023 年 5 月 22 日	-

独立行政法人　国際協力機構
次期コンピュータシステム運用等業務契約
要件定義書

Ver.1.0.0

2023 年 5 月

バージョン	最終更新日	最終更新者
1.0.0	2023 年 5 月 22 日	-

改版履歴

版数	発行日	改版者	改版内容	理由
1.0.0	2023 年 5 月 22 日	-	初版	新規作成

バージョン	最終更新日	最終更新者
1.0.0	2023 年 5 月 22 日	-

目次

バージョン	最終更新日	最終更新者
1.0.0	2023 年 5 月 22 日	-

1　はじめに

1.1　背景及び本書の位置づけ

独立行政法人国際協力機構（Japan International Cooperation Agency：JICA、以下「機構」という。）は、機構内 IT 基盤の運用支援を目的として「コンピュータシステム運用等業務（運用フェーズ）」及び「JICA 情報通信網の更改」業務（以下「現行 IT 基盤契約」という。）の委託契約を締結し、同契約の監理を行っている。

当機構情報システム部では、機構内 IT 基盤の運用支援を目的として「コンピュータシステム運用等業務（運用フェーズ）」及び「JICA 情報通信網の更改」業務（以下「両運用契約」という。）の委託契約を締結し、同契約の監理を行っている。

現行の両運用契約の履行期限は「コンピュータシステム運用等業務（運用フェーズ）」が 2024 年 5 月まで、「JICA 情報通信網の更改」が 2025 年 3 月までとなっており、履行期限の満了を迎えるため、両運用契約のうち、「コンピュータシステム運用等業務（以下「本業務」という。構築・導入および運用から構成される）」の調達を行うものである。本書は、上記調達における「コンピュータシステム運用等業務（以下「次期コンピュータシステム運用等業務」という。）」に係る要件を定義したものである。

1.2　関連図書

本書に関連する図書について、以下「表 1.2-2 関連図書一覧」に記載する。

表 1.2-1 関連図書一覧

No.	資料名称	説明
1.	現状調査報告書	現行 IT 基盤の現状及び課題を取り纏めた資料。
2.	最適化計画	現行 IT 基盤の現状調査報告書から得られた示唆や市場動向、政府動向等から次期 IT 基盤の目指すべき姿を策定した資料。
3.	製品・サービス調査・分析結果報告書	現行 IT 基盤において導入済みのサービスとそれ以外のサービスを機能やコストの観点で比較し、次期 IT 基盤への導入に適した製品・サービスを定めた資料。
4.	独立行政法人国際協力機構サイバーセキュリティ管理規程	機構が実施すべき情報セキュリティの目的、対象範囲等の基本的な考え方を定めた文書。
5.	サイバーセキュリティ管理細則	機構の情報セキュリティを確保するために必要な対策基準を定めた文書。

バージョン	最終更新日	最終更新者
1.0.0	2023 年 5 月 22 日	-

No.	資料名称	説明
6.	政府機関等のサイバーセキュリティ対策のための統一基準群	政府機関等の情報セキュリティを確保するための対策事項を定めた文書群
7.	デジタル社会推進標準ガイドライン	サービス・業務改革並びにこれらに伴う政府情報システムの整備及び管理についての手続・手順や、各種技術標準等に関する共通ルールや参考ドキュメントをまとめたもの

1.3　別紙一覧

本書の別紙について、以下「表 1.3-1 別紙一覧」に記載する。

表 1.3-1 別紙一覧

No.	資料名称	説明
1.	別紙１ 機能要件一覧	機能要件を記載した資料。
2.	別紙２ 非機能要件一覧	非機能要件を記載した資料。
3.	別紙３ システム運用要件一覧	システム運用要件を記載した資料。

バージョン	最終更新日	最終更新者
1.0.0	2023 年 5 月 22 日	-

2　全体概要

2.1　要件定義の前提事項

要件定義は、次期 IT 基盤要件定義・調達支援業務で作成した「現状調査報告書」、「最適化計画」、「製品・サービス調査・分析結果報告書」、機構の規程である「独立行政法人国際協力機構サイバーセキュリティ対策に関する規程」、「サイバーセキュリティ対策実施細則」、デジタル社会実現のために策定されている「デジタル社会推進標準ガイドライン群」、機構規程が準拠すべき「政府機関等のサイバーセキュリティ対策のための統一基準群」及び現行 IT 基盤の設計書類を基に次期コンピュータシステム運用等業務として必要となるサービスを検討し、サービスに対する機能要件及び非機能要件を定義する。なお、機構規程が準拠している「政府機関等のサイバーセキュリティ対策のための統一基準群」は令和 3 年度版が最新であるが、令和 5 年度に改定予定されるところから、令和 5 年度版決定後は同版に定める対策基準を踏まえた業務実施が求められる点に留意すること。

現行 IT 基盤において、機構が保有しているソフトウェアやクラウドサービスのライセンスと現行 IT 基盤契約の受注者が保有しているソフトウェアやクラウドサービスのライセンスがあり、当機構が保有しているライセンスで構築、運用されているサービスは、次期コンピュータシステム運用等業務においても継続した利用を前提とする。そのため、機構が保有しているライセンスで提供されているサービスにおいて、次期 IT 基盤として変更が発生するサービス、現行 IT 基盤契約の受託業者が保有しているライセンスにて構築、運用されているサービス、及び次期 IT 基盤として新たに必要となるサービスに対して機能要件及び非機能要件を定義する。

2.2　次期コンピュータシステム構成

次期コンピュータシステムのシステム構成について、以下「図 2.23-1 次期コンピュータシステム 全体システム構成」、「表 2.2-1 サービス概要一覧」に記載する。

図 2.23-1 次期コンピュータシステム 全体システム構成

バージョン	最終更新日	最終更新者
1.0.0	2023 年 5 月 22 日	-

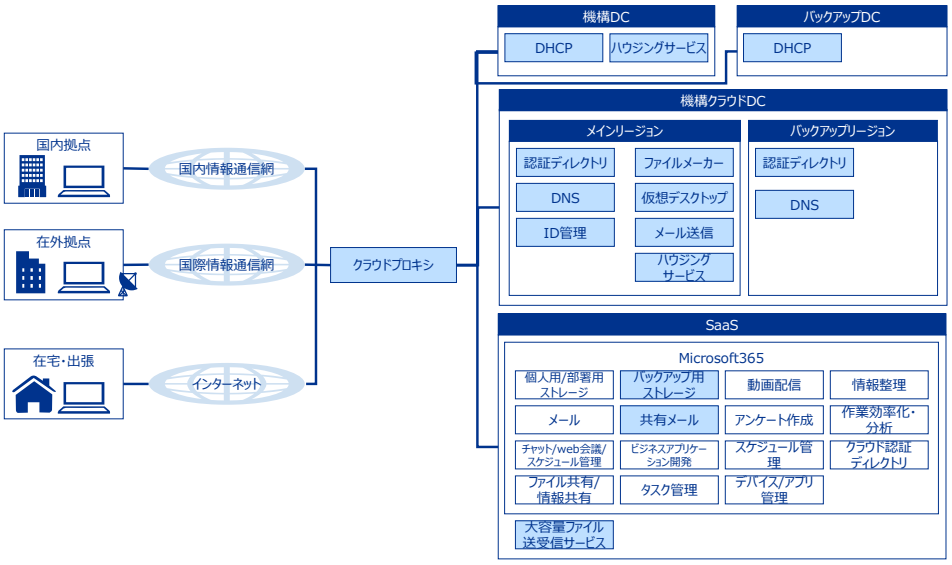


表 2.2-1 サービス概要一覧

No.	サービス	説明
1.	DHCP	国内の端末に対して IP アドレスの自動配布サービスを提供する。
2.	ハウジングサービス	機構にて運用している複数の業務系システムの設置場所を提供する。
3.	認証ディレクトリ	ユーザーアカウント、端末、周辺機器等の管理及び認証サービスを提供する。
4.	DNS	機構内部の名前解決サービスを提供する。
5.	ID 管理	人事システムまたは申請に基づく人事情報からユーザーアカウントを作成し、認証ディレクトリ及び業務システムにユーザーアカウントを登録する。
6.	ファイルメーカー	ファイルメーカーのサービス環境を提供する。
7.	仮想デスクトップ	自宅の PC から機構内の環境にアクセスするための仮想デスクトップサービスを提供する。
8.	メール送信	機構内のシステムから外部にメールを送信するサービスを提供する。
9.	バックアップ用ストレージ	部署用のバックアップ用ストレージのサービスを提供する。
10.	共有メール	部署で利用する共有メールサービスを提供する。
11.	クラウドプロキシ	インターネットアクセスにおけるセキュリティ対策および各環境へのリモートアクセスサービスを提供する。
12.	大容量ファイル送受信	機構外のユーザーとの大容量ファイルの送受信サービスを提供する。

バージョン	最終更新日	最終更新者
1.0.0	2023 年 5 月 22 日	-

3　次期コンピュータシステム運用等業務契約における基盤系システム要件定義

3.1　機能要件

基盤系システムの機能要件について「別紙 1　機能要件一覧」に記載する。

3.2　非機能要件

基盤システムの非機能要件について、「別紙 2　非機能要件一覧」に記載する。

独立行政法人 国際協力機構
次期コンピュータシステム

要件定義書
別紙01：機能要件

No	更新日	更新者	承認者	更新内容	バージョン
1				初版	1.00

DHCP

No	大分類	中分類	小分類	要件
1	DHCP			国内拠点のクライアントに対して、動的にIPアドレスを払い出すこと。
2				特定のクライアントに対して固定のIPアドレスを払い出すこと。
3				払い出すIPアドレスをIPアドレスプールとして管理すること。
4				※DHCPの設置場所については、AzureのIaaS環境がDHCP機能をサポートしていないため、機構DCに設置しているが、今後オンプレの環境は縮小していくことから将来的な移行性等を考慮して設計すること。また可能であればSaaS等のクラウドサービスでの実装をすること。

ハウジングサービス

No	大分類	中分類	小分類	要件
1	ハウジング環境	ラックスペース		ラックスペースを提供すること。
2		電源／ネットワーク		業務系システムが稼動可能な電源、ネットワーク環境等を提供すること。
3		監視		稼動監視として、対象ハードウェア、関連のネットワーク機器のPing 監視と通知（常時）、システムLED ランプ確認（日次）を行うこと。
4		セキュリティ		不正アクセス禁止及び不正侵入防止の機能を提供すること。
5				ハウジング環境には外部のインターネットからアクセスされるシステムがあるため、内部のネットワークとは分離したインターネット公開用のネットワークサービスを提供すること。
6		施錠管理		ラックの開錠、施錠、鍵管理を行うこと。

認証ディレクトリ（内部用）				
No	大分類	中分類	小分類	要件
1	認証ディレクトリ（内部用）	管理機能		管理者は、ユーザー名、所属するグループ、共有フォルダの位置など、ネットワーク上の情報を一元管理できる。ユーザーは、複数のシステムへシングルログオンできること。(ActiveDirectory 等)
2				認証ディレクトリサービスの標準機能を利用して、ログオンアカウントのID、パスワード管理を行うこと。
3		利用者情報の保持		機構内全対象端末数・ユーザー数を管理する能力をもつこと。
4				ユーザー情報には付加情報項目を自由に設定することが可能であること。
5		利用者の認証・アクセス制御		機構の標準PCのWindows OSの認証を統合管理できること。
6				朝夕ピーク時の端末の電源ONからデスクトップ（OS）が速やかに起動できるように、サーバ構成やユーザプロファイルの環境の最適化を行うこと。なお、ネットワーク環境、端末仕様等は最適なものであると仮定した場合のサーバ構成やユーザプロファイルの環境の最適化を検討し、テスト方法等も検討すること。ただし、本要件は国内拠点（本部）を前提とする。
7				利用者情報（プロファイル）に基づき、端末ログオン、ユーザー認証、ファイルサーバへのアクセス権限、各操作の制限を利用者情報毎に設定できること。
8				ユーザーIDの有効期限を設定することが可能であること。有効期限超過後は、自動的に該当ユーザーIDを利用停止状態にするのが設定可能であること。
9				休職等により長期間利用しないユーザーIDは、利用停止状態にすることが可能であること。
10				各ユーザーが複数の組織（グループ）に所属することが可能であること。
11				主所属グループと兼務所属グループの登録が可能であること。
12				組織（グループ）の追加／変更等の管理権限を、権限ユーザーが指定したユーザーに委譲することが可能であること。
13				利用していない組織（グループ）は削除するのではなく、廃止組織（グループ）として管理することが可能であること。
14				組織（グループ）をまたがった任意の複数ユーザーを指定できる、プロジェクトグループの設定が可能であること。
15				ユーザーに、自分のパスワードを変更することを許可するか許可しないかを設定することが可能であること。
16				ユーザーの初回ログイン時、もしくは次回ログイン時には必ずデフォルトパスワードを変更させるように設定することが可能であること。
17				パスワードの有効期限や文字数制限を設定することが可能であること。

	18			パスワード有効期限超過後は、ユーザーに対して自動的にパスワード変更要求を行うことが可能であること。
	19			誤ったパスワードが一定回数入力された場合は、自動的にパスワードを無効化することが可能であること。
	20			パスワードの最小文字数、最大文字数、利用可能文字種、これらの組み合わせなど、パスワード条件の設定を行うことが可能であること。
	21		組織情報の保持	組織（グループ）情報には付加情報項目を自由に設定することが可能であること。
	22			組織（グループ）やプロジェクトグループ内で、複数人が共有する代表アドレスが登録・管理できること。
	23			ユーザー情報、組織（グループ）情報、ユーザーの所属情報、組織（グループ）の階層情報、プロジェクトグループ情報のインポートおよびエクスポートが可能であること。
	25			ユーザーのアドレス帳情報の内容として、氏名、ふりがな、所属組織名、役職、メールアドレス、画像（顔写真）等を登録することが可能であること。
	26			ActiveDirectoryと密接に連携を行い、ユーザー情報の新規追加・変更や組織情報の新規追加・変更情報を受け取り、自動的に反映（同期）可能であること。
	27		同期	内部用の認証ディレクトリより有効なユーザーアカウントを機構が利用するクラウドディレクトリサービスに対して同期可能であること。 ※2022/11時点ではAzure Active Directoryを利用中。
	28	登録ユーザー		ユーザー数の登録が可能であること。
	29	オンライン処理性能		ユーザー数の半数が同時利用可能であること。

DNS

No	大分類	中分類	小分類	要件
1	DNS	名前解決		JICA内部の名前解決を担うこと。
2				DNSサービスに係る各レコードの変更・修正・追加等が可能なこと。
3				DNSのエントリを動的に登録、更新する機能を持つこと。
4				認証ディレクトリと同一のシステム上でサービスの提供が可能なこと。
5				Internet向けの名前解決については、外部のjicaドメインのDNSキャッシュサーバへ転送要求すること。
6		オンライン処理性能		ユーザー数の半数が同時利用可能であること。

ID管理

No	大分類	中分類	小分類	要件
1	ID管理			運用担当者が管理画面等からユーザーID情報、属性情報及びグループ情報を追加・変更・削除できること。
2				運用担当者が人事情報（CSVデータを想定）を取り込み、ユーザー情報が同期できること。
3				認証ディレクトリと連携し、ユーザー情報が同期できること。
4				ユーザー自身でパスワード初期化・ロック解除が行えること。
5				パスワードを失念したユーザーに対して、一時的に有効な仮パスワードが発行できること。
6				ユーザーがWeb画面からパスワード変更できること。また、変更したパスワードを共通サーバ・共通DBシステムに同期できること。
8				パスワードの長さや複雑さの要件、履歴などパスワードポリシーに従ったパスワード変更ができること。
9	オンライン処理性能			ユーザーのアクセス頻度は、月に1回から数回程度を想定すること。 管理者（数名程度）のアクセス頻度は、日に1回から数回程度を想定すること。
10	バッチ処理性能			20件から30件のデータをすみやかに完了できること。

ファイルメーカー

No	大分類	中分類	小分類	要件
1	ファイルメーカー			機構が保有するソフトウェアライセンスを使用し、ファイルメーカのサービス環境を提供すること。
2				認証ディレクトリサービスとユーザーアカウントを連携し、アクセス権管理することができること。
3				クライアント版及びサーバ版のサービスを提供すること。

仮想デスクトップ

No	大分類	中分類	小分類	要件
1	仮想デスクトップ	利用用途	ユーザー数	120ユーザーが同時に接続できる環境を提供すること
2			業務内容	デスクトップアプリ（Word、Excel、PowerPoint）、Webアプリケーション（Teams、SharePoint、Exchange）、FileMaker Clientが利用できること。
3			アクセス元環境	機構内、機構外の端末（標準PC、出張用PC、個人PC）からアクセスできること。
4		仮想PC	マスターイメージ	仮想PCのマスターとなるイメージは1種類とする。
5			リダイレクト	アクセス元の端末のデバイス（オーディオ、ドライブ、プリンター等）のリダイレクト及び制御が可能であること。

	6			ネットワーク	利用するネットワークの帯域、画面転送のフレーム数等の制御が可能であり、狭帯域においても利用可能であること。
	7			時刻	利用者のタイムゾーンと仮想PCのタイムゾーンを合わせること。
	8		性能		ユーザー数の80%が同時利用した状態でも安定した利用が可能であること。

メール送信

No	大分類	中分類	小分類	要件
1	メール送信	メール	-	各種システムがメールを送信するためのメール送信サービスを提供すること。
2			-	100,000件/月
3			SMTP	SMTPを利用したメール送信が可能であること。
4			WebAPI	WebAPI経由でのメール送信が可能であること。
5		セキュリティ	アクセス制御	アクセス元IPアドレス制御によるアクセス制限を実施すること。
6			認証	メール送信時にAPIキー等による認証を実施すること。
7			統計情報	日々のメール送信状況との統計情報が確認できること。

バックアップ用クラウドストレージ

No	大分類	中分類	小分類	要件
1	クラウド用バックアップストレージ（Microsoft OneDriveの利用を想定）	ファイルの構成	-	部署単位でのファイル長期保管領域を現行のフォルダ構成を維持した状態で提供すること。
2			-	ファイルの世代管理について、10世代保持可能であること。
3		マルウェア対策	-	非同期(データアップロードタイミング等とは関係なく)でシグネチャベースのウイルススキャンが実施可能であること。
4			-	データにウイルスが含まれると判断された場合は、該当データにフラグを付与可能であること。
5			-	マルウェア対策機能によるスキャン/検疫が実施されたファイルに対して、マルウェアチェックが可能であること。
6		監査ログ	-	Microsoft365で提供される統合監査機能により、監査ログの可視化が可能であること。
7			-	監査ログが1年間保持可能であること。
8		利用環境	-	MDM(Mobile Device Management)に登録されている端末のみアクセス可能であること。
9			-	認証されたユーザーのみアクセス可能であること。
10			-	Webブラウザベースでのアクセスが可能であること。
11			-	各部署単位でのアカウントが用意可能であること。 ※（参考情報） 現行アカウント数：310アカウント 現行実利用量：総計約60TB
12			-	各フォルダに対し機構内ユーザーに読み取り権限、編集可能権限の付与ができること。
13		管理機能	-	一部の非役職員に対し、アクセスを拒否する権限設定が可能であること。
14			-	管理者のみがユーザーのアクセス権限を変更可能であること。

共有メール

No	大分類	中分類	小分類	要件
1	共有メール	ユーザー	-	共有メールのライセンスを1000ユーザー提供すること。
2		メールボックスの参照	-	個人ではなく部署を代表して連絡する際に用いられるメールアドレス（部署メールアドレス）宛のメールを、複数ユーザーが同じ受信メールボックス（共有メールボックス）で参照可能であること。
3		メールの送信	-	共有メールボックスのアクセス権限を付与されたユーザーは、部署メールアドレスからメール送信が可能であること。
4			-	共有メールボックスのアクセス権限を付与されたユーザーは、部署メールアドレスでの代理メール送信が可能であること。
5		アクセス制御	-	共有メールボックスのアクセス権限を付与されたユーザーのみ、共有メールボックスへアクセス可能であること。

	6		メール監査	-	監査用としてメールをアーカイブし、5年間保持可能であること。
	7		管理機能	-	管理者によって、ユーザーにおける共有メールボックスのアクセス権を付与、削除可能であること。
	8			-	管理者によって、共有メールボックスの容量制限が可能であること。
	9		メールセキュリティ機能	マルウェアチェック	送受信メールにマルウェアチェックを実施し、検知されたメールをブロックすることが可能であること。
	10				マルウェアチェックでブロックされた送受信メールについて、管理者が許可することでユーザーへ配信可能であること。
	11				マルウェアに対し、サンドボックスで自動的にブロックすることが可能であること。
	12			スパムチェック	受信メールにスパムチェックを実施し、検知されたメールをブロックすることが可能であること。
	13				スパムチェックでブロックされた受信メールについて、管理者が許可することでユーザーへ配信可能であること。
	14				スパムとして検知された送信メールは、宛先に寄らず一律ブロックすることが可能であること。
	15				外部ベンダーから定期受信されるトレーニングメール（標的型攻撃メールの訓練サービス）は、スパムチェックの適用外とすることが可能であること。
	16			偽装・なりすましチェック	受信メールに対して、偽装・なりすまし（特定のドメインから送信されていると思わせるもの、なりすましているもの）チェックを実施可能であること。
	17				偽装やなりすましと判定された受信メールに対して、管理者による確認を行うことが可能であること。

クラウドプロキシ

	No	大分類	中分類	小分類	要件
	1	クラウドプロキシ	ユーザー	-	クラウドプロキシのライセンスを全ユーザー分提供すること。 ※想定ユーザー数：約6600
	2		認証	ユーザー制御	クラウドプロキシにアクセス可能なユーザーをクラウド認証ディレクトで制御するすること。
	3			シングルサインオン	利用者は、クラウド認証ディレクトリのアカウントを利用し、クラウドプロキシにシングルサインオン（SAML認証等）すること。
	4		ログ収集/転送	-	利用者のWebアクセスログの収集及び収集したログを全体監視/脅威分析に転送すること。 ※暗号化等の通信によって正常に実施できない場合はこの限りではない。
	5		URLフィルタリング	-	特定のURLに対してのアクセス制限を実施すること。
	6		クラウドファイヤウォール	-	端末からインターネットへの通信間において、クラウド上でファイヤウォール機能（多層防御）を提供すること。
	7		暗号化	-	暗号化通信は、複合した状態で通信すること。また、対象の除外が可能であること。
	8		ファイル拡張子制御	-	ファイル拡張性によりブロック等の制御をすること。

	9		マルウェア対策	-	有害なトラフィックの検知（サンドボックスによる検査）およびブロックすること。
	10			-	パスワード保護されたファイル及びスキャン不可のファイルはブロックすることが可能であること。また、対象の除外が可能であること。
	11			-	Webページのリスク評価を実施し、Webページの閲覧可否を制御すること。
	12		クラウドアプリケーション可視化	-	ユーザーが各デバイスから各種クラウドアプリケーション及びサービスへのアクセス・利用状況を可視化し、不要な通信はブロック可能であること。
	13		SNS制御	-	SNSへのログインや投稿の制御が可能であること。
	14	プライベートアクセス	アクセス環境	-	国内在外問わず機構DC、機構クラウドDC（メインリージョン、バックアップリージョン）、及び各拠点への安全な接続が可能であること。
	15			-	接続元端末の環境やネットワークを判定する等のアクセスポリシーの設定が可能であること。
	16		認証	ユーザー制御	クラウドプロキシにアクセス可能なユーザーをクラウド認証ディレクトで制御するすること。
	17			シングルサインオン	利用者は、クラウド認証ディレクトリのアカウントを利用し、クラウドプロキシにシングルサインオン（SAML認証等）すること。
	18		ログ収集/転送	-	利用者のWebアクセスログの収集及び収集したログを全体監視/脅威分析に転送すること。 ※暗号化等の通信によって正常に実施できない場合はこの限りではない。
	19		セッション管理	-	端末の電源ON/OFFに関わらず、接続セッションの指定が可能であること。

大容量ファイル送受信サービス

No	大分類	中分類	小分類	要件
1	大容量ファイル送受信	ユーザー	-	大容量ファイル送受信サービスのライセンスを140ユーザー提供すること。
3			-	大容量ファイル送受信サービスを利用するために必要なID（部署単位）の払い出し及びメールによるID通知が随時行えること。
2		容量	-	利用総容量が144GB以上であること。
5		操作制限	-	大容量共有フォルダ上のファイルへの操作制限ができること。
4		ログ	-	大容量共有フォルダ上のファイルへのアクセスログが記録できること。
6			-	大容量共有フォルダからファイルをダウンロードした際、ユーザー、日時、ファイル名等のログが記録できること。
7			-	保存したログから、ファイルを指定して、アクセスしたユーザーを検索できること。
8			-	保存したログから、システムへのログインログを記録を検索できること。

不正PC接続検知サービス				
No	大分類	中分類	小分類	要件
1	不正PC接続検知	ユーザー	-	不正PC接続検知サービスのライセンスを全拠点・部署分提供すること。
2		方針	-	ネットワークに不正に接続した端末を検知して、これをネットワークから排除するとともに、当該不正接続に係る情報と機能を一元的に管理できるシステムを導入すること。システムの構成としては、ネットワークの各セグメントにセンサー機を設置して不正接続の検知と排除を行うとともに、機構クラウドデータセンターに設置したマネージャ機でこれらの管理と情報収集を行うタイプを現行で導入しているが、不正PCを接続させないという要件を満たせば、他の提案も可とする。なお、センサー機を導入する場合の設置作業は受託者にて実施すること。
3			-	既存のネットワークやシステムの構成（ソフトウェア、ハードウェア）を変更することなく導入できるものであること。
4			-	本部、国内機関等の全クライアント、全ネットワークプリンタを十分に監視・管理できるように構築すること。
5		対応仕様	-	Ｌ2スイッチ、Ｌ3スイッチ、ルータにおけるVLANで構成された複数のサブネットワークに対応していること。
6			-	IEEE802.1Qに対応した不正PC接続検知・排除監視機能を有していること。
7			-	ネットワークへの接続を許可する機器に対してソフトウェアのインストールや、特殊な機器を接続することなく、不正接続の検知及び排除が可能であること。
8			-	不正接続検知排除システムが停止した場合は、導入前のネットワーク環境に戻ること。不正接続検知排除システムの停止により、ネットワーク障害が発生することがないこと。
9		検知・排除機能	-	MACアドレスとIPアドレスを格納した許可リストを保持し、許可リストに登録されていない機器がネットワークに接続された場合は、これを検知し、自動でネットワークから排除することができること。
10			-	DHCPによるIPアドレス割当を行っているセグメントに対しても、許可リストに登録されていない機器がネットワークに接続された場合は、これを検知し、自動でネットワークから排除することができること。
11			-	許可リストに登録されているMACアドレスをもつ機器がネットワークに接続された場合において、これに異なるIPアドレスが割り当てられているときは、これを検知できること。
12			-	許可リストに登録されているIPアドレスを持つ機器がネットワークに接続された場合において、これが異なるMACアドレスを有するときは、これを検知できること。
13			-	不正接続を排除する機能は、不正に接続された機器だけに作用し、許可リストに登録された機器における通信には、悪影響を受けないこと。
14			-	ネットワーク単位に、未登録PCへの対策（排除、又はアクセス先限定）できること。（許可リストPCは、通常通りの運用）
15		管理機能	-	ネットワークに不正に接続された機器を検知したとき又は排除したときは、その情報をログとして各センサー単位で収集し、一元的に管理することができること。

	16			-	各センサーの機能設定、挙動確認を集中管理できること。
	17			-	ネットワークに不正な機器が接続されたことを検知したときは、電子メールによる警告（アラートメール）を予め設定した管理者のアドレスに通知できること。
	18			-	ネットワークに接続された機器（端末、プリンタ、ネットワーク機器）について、IPアドレス及びMACアドレス並びにコンピュータ名などの情報を管理可能であること。
	19			-	不正接続検知排除システムを管理者として使用する場合は、ログインが必要で、ユーザーIDとパスワードによる認証機能を備えていること。

機構DC及び機構クラウドDCを含むクラウドサービス間のネットワークサービス				
No	大分類	中分類	小分類	要件
1	ネットワークサービス要件	通信回線	サービス方針	機構DC～機構クラウドDCを含むクラウドサービス間を接続する帯域確保型サービスを提供すること。
2				サービスは閉域回線で提供し、冗長構成としない。
3			サービス仕様	保証帯域は200Mbps以上とすること。
4				サービスの接続先拠点は以下を想定すること ・機構DC(オンプレ) ・機構クラウドDC ・各所管部門が管理するクラウドサービス
5				接続先が追加になった場合には追加対応できること。 なお、各所管部門が管理するクラウドサービスは現時点で以下が対象となる。 ・新海外投融資システム
6		サービス提供期間	-	サービス提供期間は2025年9月末までを想定する。正式な期間については機構と協議の上決定すること。 ※別調達にて「次期情報通信網更改」を2025年3月末までに実施する予定であり、更改によって本サービスは不要となるが、更改後6ヵ月程度の期間並行稼働させる想定であるため。

独立行政法人 国際協力機構
次期コンピュータシステム

要件定義書
別紙02 ：非機能要件一覧

No	更新日	更新者	承認者	更新内容	バージョン
1				初版	1.00

非機能要件

No	大分類	中分類	小分類	要件
1	可用性	継続性	システム利用時間	24時間365日（計画停止時間を除く）
2			稼働率	稼働率が99.9%以上であること。但し、クラウドサービスの障害等の運用事業者の責によらないケースについては対象外とする。
3		災害対策	システム	認証ディレクトリ（内部用）、DNSを対象にDRサイトでサービスを継続すること。
4			BCP期間	2週間程度
5	性能・拡張性	拡張性	業務増大率	5年で約15%の増大率に対応できること。
6			リソース拡張性	ユーザ数や業務量の増大に柔軟に対応できるサービスを提供すること。
7	運用・保守	監視	死活監視	サービスを実行するサーバやネットワーク機器等の死活を監視すること。
8			SNMP監視	サービスを実行するサーバやネットワーク機器等をSNMPにより監視すること。
9			性能監視	サービスを実行するサーバやネットワーク機器等の性能（CPU、メモリ、ディスク、ネットワーク）を監視すること。
10			プロセス監視	サービスを実行するサーバのプロセス（ミドルウェアやアプリケーション等）を監視すること。
11			サービス監視	提供するサービスの稼働状態を監視すること。
12			ネットワーク監視	各環境のネットワーク（パケットロス、ネットワーク使用率）、及び回線のオンライン状態を監視すること。
13			ハードウェア監視	サービスを提供するサーバやネットワーク機器等のハードウェア状態を監視すること。
14			ジョブ監視	ジョブの起動、終了を監視し、ジョブ状態を監視すること。
15			ログ監視	各サービス、サーバ、ネットワーク機器等のログを統合的に管理、監視すること。
16			ハウジングシステムの監視	各業務系システムの自動化監視ツール（ただし、保守業者によって設定変更及びツール変更されることがある。）により自動的に出力されることになっている監視項目に異常があった場合について、運用事業者は、その警報・アラーム等の信号を常時感知できるようにしておき、当該アラーム等の信号を各システムの保守事業者にすみやかに伝達（自動配信メール可）することとする。なお、警報・アラーム等の信号は運用事業者が用意した端末に通知できるよう保守業者にて準備することとする。
17		バックアップ		論理障害/物理障害/災害発生時（BCP発動）に備え、可能な限り障害発生前の最新断面にリカバリできるよう、バックアップを取得すること。

	18		資産管理		マイクロソフト製品のボリュームライセンス認証を一括管理すること。
	19				ハードウェアの購入やライセンス、ネットワークに接続されているプリンタ、ルータ等のハードウェアや周辺機器、これらにインストールされているソフトウェアなどの資産を管理すること。
	20				各PCの構成情報の収集、PC操作履歴の管理等、統合デスクトップ管理を実施すること。
	21				ソフトウェアの稼動情報のログをとり、使用頻度が低いものを確認する等の資産管理を実施すること。
	22				ソフトウェア資産管理のために台帳の作成や、ライセンス違反を把握すること。
	23				ソフトウェアライセンスのアップグレード、ダウングレード等、契約情報を管理すること。
	24		運用環境	検証環境の設置	新システムの導入やサービスを検討する際に影響範囲等を確認するため、必要に応じて検証環境を用意すること。
	25		時刻同期	-	システム全体を信頼性の高い外部標準時間と同期するためのTimeサービス（NTP）を提供すること。
	26			-	Timeサービスを利用する対象は、機構DC、機構クラウドDC、各拠点に設置されているサーバ、ネットワーク機器、端末に対して時刻を同期すること。
	27	セキュリティ	ネットワーク対策	不正アクセス禁止	ネットワークの境界において、通信の許可／不許可を監視・制御し、内部ネットワークを保護すること。 ※DMZ等、外部との接続点は本要件の対象外とする。
	28			不正侵入防止	ネットワーク上において、不正追跡・監視を実施し、システム内の不正行為や、不正通信を検知、遮断すること。 ※DMZ等、外部との接続点は本要件の対象外とする。
	29			ネットワークの輻輳対策	ネットワークへの攻撃による輻輳対策を実施すること。 ※DMZ等、外部との接続点は本要件の対象外とする。
	30		アクセス・利用制限	認証機能	管理権限を持つ主体の認証において多要素認証が可能であること。
	31				管理権限を持たない主体の認証において多要素認証が可能であること。
	32		データの秘匿	データの暗号化	盗聴等の脅威に対抗するために、伝送データを暗号化すること。
	33				漏洩の脅威に対抗するために、蓄積データを暗号化すること。
	34		セキュリティリスク管理	セキュリティパッチ適用	クライアントのウィルス対策ソフトの統合管理を実施すること。
	35				端末及びサービスを提供するサーバ等に対して、更新プログラム等のセキュリティパッチ（ファームウェア、ミドルウェアやアプリケーション等を含む）を適用、管理すること。

	36		全体監視/脅威分析	ログ収集	機構DC、機構クラウドDC（メインリージョン/バックアップリージョン）のサーバ、ネットワーク機器、SaaSサービス、端末等からのログを収集すること。
	37			ログ保管期間	1年間保管すること。
	38			脅威の検出	脅威を検出するための分析規則を作成可能であること。
	39				収集したログを総合的に分析し、脅威の検出が可能であること。
	40			インシデント調査	収集したログ、検出した脅威情報を基にインシデント調査が可能であること。
	41				インシデント処理の自動化が可能であること。
	42			通知機能	特定の脅威の検知については、自動的にメール送信等の通知が可能であること。
	43			可視化	環境で発生しているセキュリティ全体の状況をダッシュボード等で可視化可能であること。
	44		端末操作管理		CD/DVD/USBメモリなどの外付けデバイスを、種別単位で使用制限・禁止できること。
	45				外付けデバイスについて、クライアントPCごとに読み書き禁止/ 書き込みのみ禁止などの設定が可能であること。
	46				機構内で利用したUSBメモリを、一覧（いつ、どのユーザ、どのPCかも含む）で表示したり、USBメモリのシリアルを指定し、特定のUSBメモリのみを許可できること。
	47				ユーザ毎に、クライアントPCのファイル操作の履歴を記録すること。
	48				JICA情報通信網以外の通信サービス利用を経由してファイル共有した際のログも取得できること。
	49				ユーザ毎に、クライアントPCのWebサイトアクセス履歴を記録できること。なお、Microsoft Edge経由でWebアクセスしたログを対象とすること。
	50				クライアントPCのホスト名、閲覧先URL、ファイルアップロード/ダウンロード操作、操作日時が取得可能であること。
	51				特定のWEBサイトの閲覧制御機能を有すること。
	52				役割ごとに複数の管理者アカウントで管理できること。
	53				ユーザ単位で、ログの保存と、その操作状況を任意の条件で検索できること。
	54				セキュリティ遵守（違反）状況をレポートにし、数値で状況を確認できること。

	55				ログオンユーザ毎にログを分析し、業務でのPC利用状況を把握できること。
	56				指定時刻にPCの電源を強制的にオフにすることができること。
	57				管理者が、リモートでクライアントの操作をすることができること。
	58	システム環境	システム特性	ユーザ数	約6600ユーザ
	59			クライアント数	JICA標準PC：約3500台 レンタルPC：約100台 持込PC：約280台 在外執務用PC（データ交換・データ共有用PC含む）：約2700台 出張用PC及び私用PC：約150台
	60			拠点数	在外拠点：98拠点 国内拠点：18拠点（麹町、竹橋および市ヶ谷本部含む） システム間連携等の関係があるデータセンタ：1カ所（有償資金協力システムDC）
	61			言語数	多言語（日本語、英語等）に対応可能であること。
	62			システム設置場所	機構DC：機構DCデータセンタ要件を参照 機構クラウドDC（メインリージョン）：東日本で提供されるリージョンを利用すること。 機構クラウドDC（バックアップリージョン）：西日本で提供されるリージョンを利用すること。

機構DC データセンタ要件

No	大分類	中分類	小分類	要件
1	立地要件	交通アクセス	データセンタ施設までの距離	機構本部より公共交通機関を利用して、90分程度で到着可能な場所に立地していること。
2			データセンタ施設へのアクセス方法	公共交通機関の駅・停留所等から容易に到着できる場所に立地していること。
3			交通アクセスの確保	データセンタへの複数の交通アクセス経路が確保されていること。
4			所在地の秘匿性	データセンタの所在地を一般に公開・公表しないこと。また、所在を示す表示板、看板等が外部に設置されていないこと。
5		立地環境	立地場所の条件	地震、風水害、塩害および落雷等、自然災害の影響の少ない場所に立地していること。（国土交通省・各自治体が公開しているハザードマップにて危険性の指摘が無い等）
6			建物の立地条件（隣接建物による影響）	建物は、隣接建物から10m以上離れている等、延焼の危険性が低い場所に設置されていること。
7			建物の立地条件（危険物による影響）	半径100m以内に、消防法に定める指定数量以上の危険物製造施設又は危険物貯蔵施設が存在しない場所に立地していること。
8			建物の立地条件（電波の影響）	近隣に電波塔や地上波放送局等が無く、電磁界の影響が少ない場所に設置されていること。

	9			建物の立地条件（振動による影響）	鉄道や幹線道路等からの振動の影響が少ない場所に設置されていること。
	10	災害対策要件	耐震対策	地震に対する建物の安全性	現行建築基準法に基づいた耐震・防振等の構造上の安全性を配慮した設計・施行が行われていること。 旧建築基準法に基づき設計・施行されている場合には、耐震安全診断を行い、現行建築基準法に基づいた耐震・防振等の構造上の安全性を確保するための補強が実施されていること。
	11			耐震上求められる構造	震度6強クラスの地震に対する耐震構造を持ち、被災後も通常利用が可能であること。
	12		耐火対策	火災に対する建物の安全性	建築基準法、消防法に基づいた耐火建築物であり、火災報知システムを有していること。但し、旧建築基準法に基づき設計・施行されている場合には、現行建築基準法に基づいた延焼防止の措置が講じらていること。
	13			耐火対策	隣接建物からの延焼防止措置が施されていること。また、火災発生時の消火活動に必要となる消火器、消化栓が設置されていること。建築基準法施行令に規定する排煙設備が建物内の適切な箇所に設置されていること。
	14			火災の検知	サーバルームに、煙感知器設備が設けられており、火災の早期発見が可能なこと。
	15			訓練の実施	万一の火災発生に備えて、十分な消化訓練等が実施されていること。
	16		耐水対策	水害に対する建物の安全性	窓および天井、床からの水の浸入を防止できること。また、建物の全ての開口部は地面より高くなっているなど、水害の影響を受ける恐れの無いよう必要な措置を実施すること。
	17		雷害対策	雷に対する建物の安全性	建物は、避雷針およびアース等の雷害対策が施されていること。データセンタの施設・設備および機構における運用業務にて導入される機器等の破損を防止できるような構造であること。
	18		非常用設備	非常用設備の保有	建築基準法および消防法に規定する非常用設備および避難経路を有していること。
	19			非常用備蓄燃料	災害時等備蓄する燃料以上に自家発電装置を運転することに備えて、優先的に燃料供給が受けられる契約を複数の燃料供給会社と締結していること。
	20	搬入出経路要件	搬入出	搬入出に必要十分な建物設備	建物内の扉、エレベータ、廊下等は、情報システム機器を搬入出するために必要十分な寸法および耐荷重値が確保されていること。
	21	セキュリティ管理要件	防犯設備	防犯設備・体制の整備	不審者および部外者の侵入等を防止するための防犯設備を有すること。また、不正侵入を検知した場合、速やかに適切な対応ができる体制が整備されていること。
	22			ラックの開錠・施錠	ラックの施錠は、原則として機構が入室を認める者のみが開錠できること。また、ラックは、入室を希望する人が本人であることを確認後に運用事業者により開錠および施錠を実施すること。ラックの鍵は、原則施設にて責任を持って管理すること。
	23		入退館・入退室管理	入退館の運用方法(建物)	建物への入退館は24時間365日可能であること。また、有人による監視・入退館管理（記録・履歴の保管）を行い、許可された人のみが入退館できるよう制限すること。

	24			入館申請の運用方法	入館の申請は、24時間365日受付できること。なお、入館申請から入室までは出来る限り手間を省き、円滑に行えるよう留意すること。
	25			保管ロッカーの整備	入館者が持参する持ち物において、作業に関係の無い鞄、書類等の荷物を一時保管することができる施錠可能なロッカーあるいは同等の保管機能を有していること。
	26			入室者の確認	施設の入り口から、サーバルームにいたるまで、3回以上の入室者の確認箇所が設けられ、不審者が容易に立ち入りできない対策が講じられていること。
	27			入退室の運用方法(サーバルーム)	サーバルームへの入室は、機構が認めた者が入室する必要がある場合、来訪時に本人確認のうえ、24時間365日、速やかに開錠できること。
	28			入退室におけるセキュリティ整備	サーバルームは、入退室者を識別・記録できるセキュリティ設備（顔写真入IDカードや生体認証システム等）により、許可された特定者のみ入退室できること。
	29			入退室管理の設備	サーバルームの出入り口には入退室管理を行う設備を設置すること。 入退室の状況について常に入退室管理設備により把握できること。 入退室の状況の管理は、以下の機能を有すること。 ・個人識別機能（暗証番号、個人認証カードおよび生体認証等） ・アクセス者、日時、鍵、アクセスの記録機能 ・扉の自動施錠、解錠機能
	30			不正開錠対策	サーバルームに対する不正な開錠を厳重に防止する措置を講ずること。
	31			無許可車両の管理	無許可車両が立ち入られぬよう管理されていること。
	32		セキュリティ区画管理	セキュリティ区画の制限	入館者の権限に応じた、セキュリティ区画の制限が可能なこと。
	33		持込・持出制限	危険物の持込・持出に対する対策	危険物の持込や情報の持ち出しを制限するための設備や方策を有し、運用すること。
	34			その他の持込・持出に対する対策	事前に連絡を受けた交換部品の受取等、機器保守作業の円滑化につながる作業については適宜実施すること。
	35		監視カメラ設備	監視カメラの設置	監視カメラを設置し、建物内全体を24時間365日監視、監視映像の記録、保管をすること。その映像は1ヶ月以上保管管理すること。
	36			監視カメラ用のモニタおよび録画装置の設置	監視カメラ用のモニタおよび録画装置は、サーバルーム以外のセキュリティ対策が施された場所に設置すること。
	37		設備監視	設備監視の実施	空調、電気、エレベータ等の設備を24時間365日集中監視、制御すること。
	38	通信設備要件	回線経路	回線経路の確保	建物の通信回線が、複数回線（経路）にて引き込み可能なこと。複数回線（経路）にて引き込みが不可能な場合、地下埋設等の自然災害発生を考慮した回線の引き込みが可能なこと。

	39		回線引込	回線引込の手続き	通信回線接続に関する手続きおよび工事が容易なこと。
	40			回線引込の事業者	引き込みを行う通信回線の事業者を限定しないこと。
	41		配線仕様	敷設	データセンタ内の配線は、カテゴリ5e以上のLANケーブル又は光ケーブル（マルチモード）で敷設すること。
	42			接続	送信元と送信先をケーブルに添付すること。その際、丸札は利用しないこと。
	43	電気設備要件	受電経路	受電経路の確保	電力会社から建物への受電は、変電所から複数の受電経路が確保されていること。
	44		電気設備の信頼性	電源供給の確保	停電や建物の電源設備の法定点検実施時も含め、24時間365日、電源供給が可能であること。また、電源は電力会社から2系統以上で受電していること。
	45			受電方式	電力会社より特別高圧ループ受電方式、もしくはマルチスポット方式等により複数系統で受電し、冗長化対策が講じられていること。
	46			電源設備の点検実施	電源設備は、機構における全業務を停止せずに点検等を実施できること。
	47		電源容量の確保	電源容量の確保	建物（サーバルーム含む）へ十分な電源を供給できる電源容量であること。
	48		非常用電源設備	非常用発電設備の設置	建物の受電が停止した際に、サーバルームや空調設備等に電源を供給できる非常用発電設備を有すること。 非常用発電設備は、ガスタービン方式やディーゼルエンジン方式等を採用し、停電時でも自動運転が可能なこと。 非常用発電設備による連続運転（最低24時間以上）を行える燃料を備蓄していること。 非常用発電設備使用時にも、電源の無瞬断供給が可能なこと。
	49			無停電電源装置（UPS）の設置	停電時に非常用発電設備が起動するまでの間、瞬断すること無くサーバルームに十分な電力供給が可能な容量を持つ無停電電源装置（UPS）が設定されていること。無停電電源装置（UPS）は、冗長構成（N+1以上）であること。
	50			非常用発電設備への給油	非常用発電設備の運転中であっても、安全に給油が可能な構造であること。
	51			非常用発電設備の稼動テスト	非常用発電設備の稼動テストを定期的（年1回以上）に実施していること。
	52		環境への配慮	環境への配慮	PUE（Power Usage Effectiveness）値<2.0（設計値)を満たすこと。
	53	空調設備要件	空調設備	空調設備の設置	二重床構造に適した空調設備であり、複数台による並行運転を行っていること。空調設備は、サーバルーム毎に冗長構成（N+1以上）であること。
	54			空調設備が水冷式の場合の対応	空調設備が水冷式の場合は、漏水防止措置を講じると共に、漏水のおそれがある場所には、漏水感知器が設置されていること。 空調設備が水冷式の場合は、空調に使用する冷却水について、水道からの供給停止時においても十分な備蓄によりシステムを稼動させるに十分な空調ができること。

	55			空調設備の配管およびダクト類	空調設備の配管およびダクト類は、圧力の変動や火災による機器の損傷を防止するため耐圧性、建築基準法に規定される耐火性に優れた材質を使用し、さらに不燃材で被覆すること。フィルタに使用する断熱材は不燃性とし、火災時の煙や有毒ガスから人命の保護を図ると共に、設備の損傷防止を考慮していること。
	56			空調容量の確保	サーバルーム内に設置された設備の総発熱量に対応可能な容量を有していること。
	57			温度・湿度の監視・調整	システムが安定して稼動できるよう、サーバルームの温湿度監視・調整を実施すること。
	58			結露および漏水の防止	サーバルーム内の結露および漏水を防止するために、結露・漏水検知機能を有すること。
	59			空調設備の運用	不具合や障害発生（例、災害時等の商用電源停止時）時、点検実施に影響無く24時間365日連続運転が可能であること。
	60			予備機の設置	サーバルームの主要な空調設備機器については、予備器が設置されており、主要機器が故障の場合でも予備機により必要な冷却能力を確保できること。
	61	フロアサーバルーム要件	フロア（サーバルーム）	外部との遮断	サーバルームは一般の事務室および居室、電源室等とは、独立したスペースであるとともに建物外部からの視野が遮断されていること。
	62			フリーアクセス	サーバルームは、フリーアクセス（二重床）構造であり、電気、通信ケーブル等の床下配線もしくは天井配線,配線が可能であること。
	63			天井高	サーバラックの立架が可能であり、空調効率を保持できるとともに、運用に必要な天井高が確保できること。
	64			床荷重	設置予定のデータセンタの仕様に基づいた床荷重設計とすること。
	65			サーバ設置場所	水害・防犯等を考慮し、2階以上のフロアにサーバを設置可能なこと。
	66			サーバルーム面積	システムを設置する十分なスペースを確保すること。また、今後のシステム拡張に柔軟に対応可能なこと。（データセンタに、ラック拡張用スペースを確保しておくこと。）
	67			サーバルーム環境	サーバルーム内の内装、床面、備品等は不燃、防災性を有する材料を用いると共に、静電気による影響を防止する措置を講じていること。
	68			防火区画	サーバルームは、建築基準法に規定する独立した防火区画であること。
	69			消火設備	サーバルームの消火設備は、水を使用しないガス消火設備を有すること。
	70			室内環境	室内環境は、腐食性ガス、振動、塵埃が発生しないこと。
	71			サーバルーム監視	サーバルーム内ではラック等で死角が発生しないよう監視カメラを設置し、委託範囲内および出入口を24時間365日監視又はそれに相当する監視を適切に実施すること。

	72	ラック設備要件	ラック設備	ラックの規格	ラック規格は、TIA/EIA準拠とし、必要な機器がラッキングできるラックサイズを採用すること。また、構築事業者、保守事業者等が調達・設置した持込ラックを使用しているシステムについては、そのまま使用可能であること。
	73			ラックサイズ	十分な奥行きを持つこと。
	74			レール取り付けフランジとラックの側面のスペース確保	ケーブルの取り回し・配線の保守性を考慮し、前面および背面のレール取り付けフランジとラックの側面間の幅は十分にスペースが確保できること。
	75			ラックの耐震対策	震度6強クラスの揺れにおいても、ラック内に搭載している機器に損傷を与えないこと。なお、ラック設置工法については、設置予定のデータセンタ全体の耐震（免震）工法を考慮した上で、耐震か免震工法か選択すること。
	76			ラックに必要な電源の確保	電源は、200Vの供給にも対応できること。
	77			ラックの施錠	セキュリティ対策として、ラックの前面、後面、両横面が施錠できるものとすること。（ラックが隣接する場合は、横面の施錠はしなくてもよい）
	78			ラックへの収容	システム運用業務に利用される機器等が全て収容できること。
	79			ラックの設置	設置予定のデータセンタのエアフローに則り、ファンユニットを適した箇所に設置し、放熱対策すること。
	80			ラック間のケーブル接続	ラック間のケーブル接続は、適宜運用性を考慮して、パッチパネルを実装すること。
	81			ラックの配線	ラック内は、ケーブルガイド等を利用し、配線を整理すること。
	82			保安用アース	必要に応じてラック本体に対し、保安用にアースを接続すること。
	83		ラック数および電源容量	ラックの確保	システム運用業務にて利用される機器等が収容できるラック数および電源容量を提供すること。
	84			ラックの配置	ラックは、隣接して設置すること。隣接して設置することができない場合は、少なくとも、電源種別（100V/200V）毎に隣接していること。
	85		その他機材	ラック設置に当たっての必要な部材	ラックの設置に当たっては、別途調達する機器等（システム運用対象機器一覧）を参考に、必要と判断される部材（パッチパネルおよびこれに付随するケーブル、OAタップ、機器設置部品ラック棚板等を含む）を必要な数、用意すること。
	86			部材の準備	運用事業者は、当該部材について、システム運用業務に関係する回線事業者、構築事業者、保守事業者および現行運用事業者と協議・調整の上、必要と判断される部材を、必要な数、用意すること。

	87	環境要件	環境	関係法令・基準遵守	運用事業者は、データセンタに係る環境要件に関して以下の法令・基準等を遵守するとともに、環境に配慮した自主的な取り組みを実施すること。 ・情報システムの設備環境基準（JEITA基準） ・エネルギーの使用の合理化に関する法律等 なお、今後環境に配慮すべき事項（グリーンITに対する取組）が規定された法令・基準等が追加施行された場合でも、対応できる施設であること。

独立行政法人 国際協力機構
次期コンピュータシステム

システム運用要件

No	更新日	更新者	承認者	更新内容	バージョン
1				初版	1.00

No	大分類	中分類	小分類	次期要件
1	サービスデザイン（運用開始前業務）	運用業務体制の構築	運用業務体制の構築及び業務の開始	運用事業者は、コンピュータシステム運用業務を行うための体制について、組織図、リーダーや業務従事者（リーダーの下位に属し業務を行う者及びバックヤードも含む）の氏名、所属部署、連絡先及び経歴等について機構に提出し、承諾を得ること。また、承諾を得た体制にて業務を開始すること。
2	サービスデザイン（運用開始前業務）	運用業務工程管理	工程管理計画作成	運用事業者は、以下の内容を含んだ設計準備フェーズ及び運用フェーズの運用事業者自身の工程管理計画を作成する。 ・工程管理体制 ・業務スケジュール（WBS）(年次・月次・日次等、中長期と短期の状況がわかるもの) ・成果物 ・ドキュメント管理方法 ・情報セキュリティ管理方法 ・進捗管理方法 ・品質管理方法 ・課題管理方法 ・リスク管理方法 ・工程管理計画の改定手順 上記以外にも、運用事業者が必要と判断した事項は、工程管理計画に含めること。 また、運用事業者は、業務スケジュールの作成、進捗・課題報告等のタイミング等は必要十分な頻度を検討・提案し、コンピュータシステム運用業務全般を一任された者として適切に業務を実施する。 なお、運用事業者は、工程管理計画の見直しを適宜実施し、更新を行う。
3	サービスデザイン（運用開始前業務）	運用業務工程管理	工程管理業務の実施（進捗管理）	運用事業者は、運用設計フェーズ及び運用フェーズにおいて、各タスクが業務スケジュールに従って進められているか管理する。 運用事業者は、以下の作業を実施する。 ・業務スケジュール（WBS)の更新 ・進捗管理表での管理 進捗管理表及びそれを補足する資料にて、WBS番号、作業名、作業担当者、作業の開始日及び終了日、ステータス、進捗率等を管理する。 ・進捗状況分析 進捗管理表より、スケジュール差異、予測総工数、残工数等を用いて、進捗状況を定量的に分析し、その結果から進捗に遅れが発生する可能性が確認できた場合には、必要に応じて、システム第一課へ報告を行う。 ・進捗状況報告 進捗会議にて、コンピュータシステム運用業務の進捗状況の報告を行う。 ・進捗遅延への対応 コンピュータシステム運用業務スケジュールから遅れが生じた場合又は遅れが生じる可能性がある場合は、改善策案を立案し、実施する。また、必要に応じて、その結果をシステム第一課へ報告する。

	4	サービスデザイン（運用開始前業務）	運用業務工程管理	工程管理業務の実施（課題管理、リスク管理）	運用事業者は、運用設計フェーズ及び運用フェーズにおいて、コンピュータシステム運用業務中に生じる課題等について潜在的なもの（リスク）も含め継続的に管理し、解決策案を立案し、実施する。 また、運用事業者は、必要に応じて、課題管理状況をシステム第一課へ報告する。
	5	サービスデザイン（運用開始前業務）	運用業務工程管理	工程管理業務の実施（品質管理）	運用事業者は、運用設計フェーズ及び運用フェーズにおいて、システム第一課が求めるシステム運用要件を網羅的に満たせているか、定期的に確認を行う。品質に問題がある場合は、改善策案を立案し、実施する。また、必要に応じて、その結果をシステム第一課へ報告を行う。
	6	サービスデザイン（運用開始前業務）	運用設計	現行運用業務の確認(現状調査)	運用事業者は、現行コンピュータシステム運用業務における運用手順書、システム設計書等のドキュメントを確認し、確認事項を取り纏め、現行運用事業者に対して情報提供及びコンピュータシステム運用業務のレクチャの依頼等を実施する。
	7	サービスデザイン（運用開始前業務）	運用設計	運用設計書の構成要素に基づく整理	本書にて定義されている事項について、運用設計書にて設計されるべき以下の構成要素ごとに整理を実施する。 ・概要（前提事項含む） ・考え方 ・役割分担 ・インプット/アウトプット ・会議体 ・実施作業フロー（フローの表記はBPMNを使用する） ・実施作業内容（詳細内容、実施タイミング、担当者等） ・使用する様式（申請書、報告書等） ・情報セキュリティ対策 等 上記以外にも、運用事業者が運用設計作業を実施するうえで必要と判断した構成要素は追加し、整理すること。 なお、運用設計書の作業項目は、本書における要求を満たすよう作成すること。
	8	サービスデザイン（運用開始前業務）	運用設計	運用設計書の作成	運用事業者は、運用設計書の雛形を提示して、本書に基づいて整理した構成要素を元に、運用設計書を作成する。作成した運用設計書は、システム第一課に報告し、承認を得る。 また、運用事業者は、コンピュータシステム運用業務等の改善実施をうけて運用設計書の随時見直し及び更新を行う。 なお、運用設計書を作成する際には、運用設計書の付属資料との役割・目的を明確に切り分けて作成すること。
	9	サービスデザイン（運用開始前業務）	運用設計	運用設計書の付属資料の作成	運用事業者は、本書の「No17,18,19 報告・提出資料等の定義」に記載されている資料を中心とした、運用設計書の付属資料を作成する。作成された運用設計書の付属資料は、運用設計書同様、システム第一課に報告し、承認を得る。 また、運用事業者は、システム運用業務等の改善実施をうけて運用設計書の付属資料の随時見直し及び更新を行う。 なお、運用設計書の付属資料を作成する際には、運用設計書との役割・目的を明確に切り分けて作成すること。 そのほか、運用設計の際に、電子申請化したほうが効率的と思われるシステム運用業務については、電子申請の設計・開発を行うこと
	10	サービスデザイン（運用開始前業務）	運用設計	運用業務に係るシステム・サービスの対応方針検討・設計・構築作業	コンピュータシステム運用に関連し、機構がシステムやサービスのアウトプット追加等を検討するための設計や調査等が必要になった場合は、運用保守の範囲内で、運用事業者にて対応方針を検討、システム第一課に提案を行い、設計・構築作業を行うこと。 なお、検討時点で見積った作業の規模により、運用保守の範囲内で実施するかどうかを協議することとする。

11	サービスデザイン（運用開始前業務）	運用設計	収支計画書及び収支報告資料の提出	運用事業者は、コンピュータシステム運用業務において、年度の初めに収支計画書及び四半期毎の収支を報告する資料を作成し、システム第一課へ提出する。資料はコンピュータシステム運用業務の開始から終了まで、収支の状況（計画と実績）がわかるような様式を検討すること。 （様式は任意とするが、コンピュータシステム運用業務全体期間のうち、報告時点での収支状況が把握できるようにすること。）
12	サービスデザイン（運用開始前業務）	インフラ導入・設定変更に係る状況把握・提言（設計・構築フェーズ）	在外IT環境診断及び改善提案	運用事業者は、現行の在外拠点のIT環境を診断し、運用方法・環境改善に関する提案を行う。 また、運用事業者は、IT環境改善に係る現地業者への業務指示書等の文書作成への技術的支援・提言を行う。 本項目は運用開始前に在外拠点の新規開設や機器入れ替え等があった場合に対する要件である。
13	サービスデザイン（運用開始前業務）	インフラ導入・設定変更に係る状況把握・提言（設計・構築フェーズ）	在外調達支援	運用事業者は、IT動向を調査し、必要に応じて調達ガイドラインの改善を提案する。システム第一課と協議を行い、IT関連機材（ハードウェア、ソフトウェア）及び役務等の標準仕様を定め、ガイドラインに反映する。 また、運用事業者は、調達ガイドラインをもとに、在外拠点に対してIT関連機材についての要望調査を行い、調査結果をもとにシステム第一課が一括調達する機材について、調達仕様書作成への技術的支援を行う。
14	サービスデザイン（運用開始前業務）	サービルレベル設計	モニタリング項目の設定	運用事業者は、機構が期待する付加価値や品質（サービスレベル）を提供できているかの達成状況を管理するため、システム運用要件ごとにモニタリング項目を設定し、システム第一課と協議の上、モニタリング項目を最終化すること。 なお、運用設計時にモニタリング項目等を確認・精査し、機構と協議の上モニタリング項目及びサービスレベルの管理手順（セルフモニタリング業務の流れ、追加モニタリング項目、モニタリング項目の要求値の引き上げのタイミング、その実施方法）を確立させること。
15	サービスデザイン（運用開始前業務）	サービルレベル設計	モニタリング項目の目標値の設定	運用事業者は、機構が期待する付加価値や品質（サービスレベル）を提供できているかの達成状況を管理するため、システム運用要件ごとにモニタリング項目を設定し、システム第一課と協議の上、モニタリング項目の目標値を最終化すること。
16	サービスデザイン（運用開始前業務）	サービルレベル設計	サービスレベルの合意	運用事業者はコンピュータシステム運用業務範囲、運用対象システム、モニタリング項目、目標値、ポイント精算ルールなどの前提条件等の運営ルールを記載した合意書を作成し、機構と取り交わす。
17	サービスデザイン（運用開始前業務）	報告・提出資料等の定義	報告頻度・内容の定義	運用事業者は、本書において、作成又はシステム第一課に提出すべきとされている資料等（システム第一課に報告すべきとされている内容を記載した資料を含む。）に関し、それぞれの資料等に応じた頻度でシステム第一課に提出する。その際、期限についてはシステム第一課と運用事業者の間で協議、合意した上で、当該期限を遵守する。 運用事業者は、設計・構築フェーズにおいてコンピュータシステム運用業務の開始日から毎月、定例報告として、進捗状況を含む報告書を提出する。 運用フェーズにおいては設定したモニタリング項目に対して機構と合意した報告頻度にてモニタリング報告書を提出する。

18	サービスデザイン（運用開始前業務）	報告・提出資料等の定義	報告資料・提出資料の定義	運用事業者は、運用業務開始前に以下の資料を作成し、報告・提出する。 ・運用設計書（本書をもとに運用体制図、作業ごとの作業概要・作業フロー・インプット・アウトプットを等を明確化し、実際の運用作業を行う際のルールブックとする） ・各種計画書（本書に記載している作業ごとの計画書全て） ・運用マニュアル・操作マニュアル（運用設計書からの参照先として、作業や機器操作手順書を纏めたもの） ・各種様式（コンピュータシステム運用業務で使用する申請書類等の様式を纏めたもの） ・ネットワーク構成図 ・フロア設計図 ・配線図及びラック間配線図 ・ラック搭載図（機構DC及びハウジングサービスも含む） ・移行計画書（データ・システム） ・引継ぎ計画書 運用事業者は、コンピュータシステム運用業務開始後継続的に以下の資料を作成し、報告・提出する。 ・本書に記載している作業ごとの報告書・記録類全て （例：リソース使用状況・システム監視状況・障害対応記録・緊急連絡体制・問題対応状況・システム変更状況・リリース作業計画・リリース作業結果・構成管理情報・ヘルプデスク問い合わせ状況・FAQ・資産管理情報） 上記以外にも、運用事業者が必要と判断する資料は作成し、報告・提出対象とすること。 なお、本部（二番町センタービル、市ヶ谷ビル、竹橋合同ビル）のLANについてはLANの運用事業者にて運用要領書、運用作業手順書、LAN環境物理構成図、LAN環境論理構成図、フロア内配線図等を作成するため、資料の作成対象について重複のないよう業務開始時に協議すること。
19	サービスデザイン（運用開始前業務）	報告・提出資料等の定義	次期運用事業者への引継ぎ計画・引継ぎの実施	運用事業者は、コンピュータシステム運用業務における得られた教訓等を踏まえ、契約期間終了時の引き継ぎをより円滑に実現させるための、中長期的な視点での引き継ぎ計画を策定すること。 当該引き継ぎ計画は、運用開始後必要に応じて更新を行うこと。 策定した計画に基づき、次期運用事業者への引継ぎ作業及び資料の提供を実施し、結果をシステム第一課に報告する。
20	サービスオペレーション	システムの起動・停止	サーバの起動/停止/再起動	運用事業者は、定期的にサーバの起動/停止/再起動を実施すること。
21	サービスオペレーション	DNS運用	DNS運用	運用事業者は、名前解決に必要なホスト名の追加・変更・削除等を実施し、管理を行う。また、運用事業者は、システム第一課から要求があった場合には、これらの情報を必要十分な形で提供する。
22	サービスオペレーション	バックアップ運用	バックアップ計画の策定	運用事業者は、機構DC、機構クラウドDC（メインリージョン/バックアップリージョン）及びSaaSにおけるシステムデータやファイルデータのバックアップ計画を作成する。その際、必要と判断した場合は、システム第一課へ報告を行う。 また、運用事業者はバックアップ計画の見直しを適宜実施し、更新を行う。
23	サービスオペレーション	バックアップ運用	バックアップの実施	運用事業者は、作成したバックアップ計画に従い、運用対象システムのバックアップを行う。
24	サービスオペレーション	バックアップ運用	媒体管理	運用事業者は、運用対象システムのバックアップに使用する媒体の調達・保管・管理を行う。

25	サービスオペレーション	バックアップ運用	世代管理	運用事業者は、システム毎に、バックアップスケジュール表を作成し、スケジュールに沿った媒体の世代管理を行う。なお、何世代管理するかは、運用設計で決定するものとする。
26	サービスオペレーション	バックアップ運用	媒体の外部保管	運用事業者は、災害時のデータ保存のため、最新の数世代分の媒体の外部保管先を検討し、システム第一課に報告、承認を受ける。 運用事業者は定期的に最新の数世代分の媒体を外部保管先に保管管理を実施し、必要に応じて取り寄せを行う。何世代分外部に保管するかは運用設計で決定する。
27	サービスオペレーション	バックアップ運用	媒体のクリーニング	運用事業者は、クリーニング対象装置毎に定められたクリーニング周期又は装置からクリーニング要求が発生した際に、テープ装置のクリーニングを行う。
28	サービスオペレーション	バックアップ運用	媒体の廃棄と廃棄証明書の発行	運用事業者は、確実に読み取り不可能で再使用できない状態にしてから破棄を行う。
29	サービスオペレーション	点検作業運用	点検作業運用	運用事業者は、以下の点検作業を行う。 ・物理環境点検 システム運用対象機器について、目視による点検を実施、破損等の異常がないかを確認することである。 ・ハードウェア点検 システム運用対象機器について、任意のチェックツールやログを点検し、ハードウェアの異常がないかを確認することである。 上記以外にも、運用事業者が必要と判断した点検作業は実施対象とすること。 運用事業者は、点検時期・詳細な点検項目を考察し、作業を行う。ハウジング機器については、各システムの保守業者へ連絡する。
30	サービスオペレーション	リカバリ運用	リカバリ手順書の作成	運用事業者は、災害・事故等予期せぬ事が発生し業務上のデータが損失したり、システム機器が破壊（一部も含む）された場合に備え、データ（業務上のデータや運用管理上のシステム設定値）やサーバ機器等の復旧方法についてリカバリ手順書を作成する。 作成したリカバリ手順書は、システム第一課に報告、承認をうける。 また、運用事業者は、リカバリ手順書をシステムの稼働状況により随時見直しを行う。ただし、BCP発動時（震度6強以上の震災が東京23区内で発生した場合を契機としてコンピュータシステム運用の利用可否を確認し、問題が認められる場合)は別途定める手順に従う。
31	サービスオペレーション	リカバリ運用	リカバリ訓練の計画・実施	運用事業者は、災害・事故発生時に混乱なく対処するために、リカバリ訓練を1回／年計画し、実施する。 想定すべきリカバリ対象事例は以下。 ・自然災害 ・人災 ・機器の破損、破壊 等 また、運用事業者はリカバリ訓練の計画の見直しを適宜実施し、更新を行う。 ただし、BCP発動時（震度6強以上の震災が東京23区内で発生した場合を契機としてコンピュータシステム運用の利用可否を確認し、問題が認められる場合)は別途定める手順に従う。
32	サービスオペレーション	機構内・在外利用者向けヘルプデスク	対応時間	平日午前9時から午後6時（日本時間） 但し、申請の状況により、開始・終了時間を前後させる可能性がある。
33	サービスオペレーション	機構内・在外利用者向けヘルプデスク	問い合わせ方法	ヘルプデスクへの問い合わせ方法は、メール、電話、Webが利用できること。

34	サービスオペレーション	機構内・在外利用者向けヘルプデスク	対応言語	日本語と英語の対応が可能であること。
35	サービスオペレーション	機構内・在外利用者向けヘルプデスク	問い合わせ受付	運用事業者は、機構関係者のあらゆるエンドユーザ、各課、関連ベンダー等から業務系(システムに関する一般的問い合わせ、システム障害情報等)、OA系(PC、スマートフォンの操作方法や障害情報、MS Office等)、情報通信網に関する問い合わせ（回線やNW機器などの不具合等）の機構システムにかかる全ての問い合わせを一元的に受け付ける。その際、運用事業者は、必要な情報(部署名、氏名、担当者名、利用者内線番号、関連システム、PC/プリンター番号、問い合わせ内容等)を、情報共有のために履歴に残す。 ※1 なお、個別にヘルプデスクが開設されているシステム（2022年5月時点では、主に以下のシステム）に関しては、メールやチャットツール等にてエスカレーションを行うこととする。 ・事業管理支援システム ・調達・契約管理システム ・新派遣システム ・人材DBシステム ・経理業務統合システム ・DIGNITASシステム ・ALMシステム ・電子決裁システム ・研修事業総合システム ・ボランティアシステム ・無償資金協力実施管理システム ・人事勤務システム ・デジタル法令・規程集 ・企業情報DB ※2 システム運用に係る過去の問合わせ受付件数は、平均約2,258件/月（2021年度 合計27,099件） ※3 情報通信網に係る過去の問合わせ受付件数は、下記の通り 2021年10月：14件、2021年11月：23件、2021年12月：18件、2022年1月：13件、2022年2月：14件、2022年3月：13件
36	サービスオペレーション	機構内・在外利用者向けヘルプデスク	内容の切り分け	運用事業者は、受け付けた問い合わせ内容を把握し、過去に同様の問い合わせ内容や対応があったか、自社ナレッジを確認し、その上で対応方針を判断する。 他運用事業者に二次対応依頼を出す際には、その旨を履歴として残す。
37	サービスオペレーション	機構内・在外利用者向けヘルプデスク	問題解決・回答	運用事業者は、記録された過去の対応履歴を参照し問い合わせへ回答し、問題を解決するとともに対応結果を履歴に残す。
38	サービスオペレーション	機構内・在外利用者向けヘルプデスク	二次担当者以降による解決、回答	運用事業者は、各課、関連ベンダーらに対応を依頼した問い合わせについては、随時その対応状況を把握する。 二次対応完了後、運用事業者は、その対応を担当した、関連事業者等から報告を受け取り、解決内容、解決時間及び連絡者を確認し、それを対応履歴として記録する。 また、各課、関係ベンダーに対応を依頼した問い合わせについて、問い合わせをしたユーザへも定期的に対応がなされたか確認し、二次対応担当者の対応の遅れを防止する。

39	サービスオペレーション	機構内・在外利用者向けヘルプデスク	利用者への情報伝達（対応進捗状況、障害情報、保守スケジュール等）	運用事業者は、問い合わせや障害対応状況の連絡を、利用者等へ必要に応じて行い、その状況を対応履歴として記録する。 ただし、システム第一課としての判断が必要な、重大な障害等に関してはシステム第一課が内容の確認、利用者への報告を行う。
40	サービスオペレーション	機構内・在外利用者向けヘルプデスク	問い合わせ内容の記録	運用事業者は、利用者等からの問い合わせや、障害対応記録を最新の状態で維持し、ファイルサーバ又は簡易ブラウザ等を介して常時閲覧可能な形で、システム第一課、関連事業者等との情報の共有を図る。
41	サービスオペレーション	機構内・在外利用者向けヘルプデスク	問い合わせ記録分析による利用者要望の整理	運用事業者は、問い合わせ内容の記録を、エンドユーザや関連ユーザ等の問い合わせ主体ごとに分類して分析し、利用者がシステムに対しどのような要望や不満を持っているのかを把握し、システム第一課に分析結果報告や改善提案等を行う。 システムやサービスに関する高度な技術・知識を要する分析や改善案の検討が必要な場合は、システム第一課に報告ののち、各運用事業者に詳細な分析や改善案の検討・報告の依頼をする。 なお、問い合わせ記録分析実施頻度については、原則として定期的に月1回を想定しているが、機構に最適な頻度を検討し、提案することとする。
42	サービスオペレーション	機構内・在外利用者向けヘルプデスク	問い合わせ対応状況に関する報告	運用事業者は、定期的にヘルプデスクの問い合わせ状況や対応品質を確認、分析し、対応状況や改善策等をシステム第一課に報告する。 また、運用事業者は、システム第一課からの調査依頼や情報提供依頼に対しては速やかにそれを取りまとめ、提示する。
43	サービスオペレーション	機構内・在外利用者向けヘルプデスク	サービス内容についての情報提供	運用事業者は、過去の問い合わせ履歴や障害対応履歴の内容から、頻度の高い問い合わせや現象をFAQ・マニュアル・ガイドライン等として取りまとめて掲載し、情報の共有を図る。 必要に応じて、ヘルプデスクニュースなどプッシュ型の情報提供を実施する（発行頻度の目安は隔週1回程度）。 また、運用事業者は、定期的な棚卸しや情報の分類整理、見やすい形への再編、最新規程との内容整合性の確認を行う。
44	サービスオペレーション	機構内・在外利用者向けヘルプデスク	機構システム関係者連絡先リストの作成・維持管理	運用事業者は、全ての機構システムにかかる各課、関連ベンダー等の氏名、所属、連絡先（固定電話、携帯電話、メール、メーリングリスト等）などの必要な情報を常時管理し、担当交代・変更等があった場合の加除を確実に実施すること。
45	サービスオペレーション	機構内・在外利用者向けヘルプデスク	クライアントPCリモート対応の実施	運用事業者は、機構在外拠点の利用者からの問い合わせに対して、電話やメールでの対応が困難な場合又は利用者から要望があった場合、必要に応じてクライアントPCへのリモートデスクトップによる操作を対応を行い、問題の解決等を図る。

46	サービスオペレーション	公用スマホ、PC等の運用	公用スマホ、標準PC等の運用に係る作業	運用事業者は、公用スマホ、本部・国内機関標準PC本体及び在外拠点PC本体の運用に係る以下の作業を行う。 ・アカウント管理 ・IPアドレス管理（機構DC、機構クラウドDC（メインリージョン/バックアップリージョン）上のシステム及びハウジングサービス等も含む） ・PCソフトウェアのバージョンアップ作業 ・PC更改やOS移行等への対応作業 ・プログラム配付と配付状況の確認 ・資産管理（公用スマホは除く） ・ウィルス対策 ・不正PC接続管理 ・初期化、クリーンアップ作業 ・キッティング（autopilotを想定）※公用スマホは除く なお、2022年5月時点での執務用PC台数は6131台（内、本部・国内機関標準PCが3489台、在外事務所PCが2642台）を想定すること。 上記以外にも、運用事業者が必要と判断したコンピュータシステム運用業務は実施対象とすること。
47	サービスオペレーション	公用スマホ、PC等の運用	標準PC等の運用に係る作業	PC予約／貸出管理、PC貸出／返却受付は、人事異動により、在外事務所、支所、出向先等からの転入・転出等があった場合に、標準PCを貸与、返却する手続きを指し、原則機構本部内の運用事業者常駐用スペースにて対応する。 PC移設作業では、職員の異動やレイアウト変更時等のPC移動（設置）に係るPCの動作確認も実施する。また、本部以外の拠点においては、支援作業を中心に実施する。 PC更改やOS移行等への対応作業”については、原則として運用事業者が必要な作業を実施する。なお、標準PCについては、初期インストール時の動作確認は、運用事業者が確認手順を明確に定めた上で、PC更改業者に対応を依頼することが可能であるが、その後の通常運用（OS移行に伴い、新たに運用開始する機能を含む）に関する作業は運用事業者が実施する。 なお、在外拠点に設置されているPCのOSは多言語版も存在する。 定期人事異動等のピークにおける、初期化・クリーンアップ作業の対象となる台数（概数）は1ヶ月当たり340台程度と想定する。 上記以外にも、運用事業者が必要と判断したコンピュータシステム運用業務は実施対象とすること。
48	サービスオペレーション	公用スマホ、PC等の運用	持込PCの運用に係る作業	運用事業者は、各部門の保守委託事業者等において、機構が貸与する標準PC以外のPC（持込PC）を持ち込み、LANに接続する必要がある場合、以下の作業を行う。 対象PCは2022年5月時点で約280台程度あるが、持込PCの接続は推奨しないため、今後台数を減らしていく見込みである。 ・持込PC登録・変更・撤去管理 ・アカウント管理 ・資産管理 ・不正PC接続管理 上記以外にも、運用事業者が必要と判断した運用業務は実施対象とする。

49	サービスオペレーション	公用スマホ、PC等の運用	研修・会議用PCの運用に係る作業	運用事業者は、研修・会議用PCの運用に係る以下の作業を行う。 ・研修・会議用機器予約/貸出管理 ・研修・会議用機器（PC及びPC付属品）管理・保管 ・研修・会議用貸出機器の準備 ・研修・会議用貸出機器の動作確認 ・研修・会議用機器貸出/返却受付 ・研修・会議用機器ウィルス対策 ・資産管理 ・不正PC接続管理 上記以外にも、運用事業者が必要と判断した運用業務は実施対象とする。 なお、研修・会議用PC台数は100台、貸出件数は、0～35件（平均約7件）/日を想定すること。
50	サービスオペレーション	公用スマホ、PC等の運用	稼動PC接続管理	運用事業者は、稼動PC（標準PC、持込PC、研修・会議用PC）の棚卸を実施し、接続状態の把握、管理を行う。 なお、業務実施頻度については機構と協議の上決定する。
51	サービスオペレーション	公用スマホ、PC等の運用	在外機材修理返送手続支援	原則現地での対応だが、運用事業者は、必要に応じて在外拠点で使用する機材等が故障した場合、輸送（受取、返送）作業および修理に係る支援を行う。
52	サービスオペレーション	公用スマホ、PC等の運用	在外空送手続手配	原則現地での調達だが、運用事業者は、国際協力機構にて調達した機材について、空送業者の手配、機材の引渡し、在外拠点への郵送情報の伝達等を行う。

53	サービスオペレーション	周辺機器運用	周辺機器の運用に係る作業	運用事業者は、周辺機器の運用に係る以下の作業を行う。 ・周辺機器予約/貸出管理 ・周辺機器貸出依頼書の準備 ・周辺機器貸出/返却受付 ・周辺機器管理・保管 ・周辺機器設置関連 対象とする周辺機器は以下の物とする。 ・PC周辺機器一式（ディスプレイ、ディスプレイ台、ＨＤＭＩケーブル、キーボード、マウス、ポート拡張ユニット、ポート拡張ユニット用電源アダプタ／電源ケーブル） ・プロジェクタ　12台 ・ポータブルWifiルータ　1台 ・スクリーン　7台 ・モバイルプリンタ　150台 ※PC周辺機器一式は、原則本部および国内機関の全てユーザの執務机に据え置きで設置されるものであり、ユーザは標準PCとこれら周辺機器一式を接続して利用する。執務スペースのユーザ数の増減やレイアウト変更が発生した場合に、貸出／返却を行う。 ※各周辺機器における過去対応件数は以下の通り。 ・PC貸出　貸出：約100台/月　返却：約100台/月 ・プロジェクタの貸し出し　72件/年 ・ポータブルWifiルータの貸出：181件/年 ・スクリーンの貸出：43件/年 ・モバイルプリンタの貸出件数：148件/年
54	サービスオペレーション	周辺機器運用	拠点複合機環境設定	運用事業者は、国際協力機構拠点複合機の保守（導入）事業者に対して環境設定の支援等を行う。 複合機は、現在本部に約99台、国内拠点に約67台接続されているが、複合機の保守/管理は別事業者である。 ・組織変更時等のスキャナフォルダの設定/追加/修正 ・複合機に係る問い合わせに対して機器保守事業者へエスカレーション　等
55	サービスオペレーション	セキュリティ運用	関係法令・基準遵守	運用事業者は、セキュリティ運用に関して以下の法令・基準等を遵守する。 ・不正アクセス行為の禁止等に関する法律 ・個人情報保護法 ・著作権法 ・特定電子メールの送信の適正化等に関する法律 等

56	サービスオペレーション	セキュリティ運用	セキュリティ監視	運用事業者は、セキュリティに関するログおよびメッセージを横断的に24時間365日体制で常に能動的に監視／分析（ログ間の相関チェックも含む。チェック条件については、都度機構と相談のうえ受託者により見直しを行うこと）を行い、異常と疑いのある事象を検知した場合、速やかにインシデントの対応を行うこと。 また、システム第一課から接続を行う旨の通知がされていないPC等のクライアント機器およびスイッチ、ルータ、無線LANアクセスポイント等の接続がないか監視し、接続があった場合は、必要に応じて、設置機器と設置場所をシステム第一課に報告するとともに、当該接続機器からのネットワーク接続を禁止する設定を直ちに行う。設定後、システム第一課の協力を仰ぎながら、接続があった端末の詳細を調査し、原因を特定する。 その他、運用事業者は外部よりセキュリティに関する情報を入手し、事前にFW,IPS等の設定を変更して対応に努めることとする
57	サービスオペレーション	セキュリティ運用	セキュリティインシデント対応	運用事業者は、セキュリティインシデントをアラーム等により検知した場合、対応手順書に沿って速やかに対応策を実施する。必要に応じて、自社または自社グループ会社内で、フォレンジック業務を行う。また、マルウェアの検体を分析し、各種ログを横断的に時系列に解析し、原因および影響範囲を特定し対策を行うこと。発生したセキュリティインシデントに対する対応策が対応手順書に定義されていない、もしくはセキュリティインシデントの優先度が高い場合は、システム第一課に確認の上実施する。 セキュリティインシデントとしては、以下を想定している ・ウイルス感染 ・不正アクセス ・情報漏洩 ・迷惑メール送受信 ・不正ソフトウェアの使用 ・標的型攻撃、早期警戒対応 ・未知の脅威への対応 等 また、運用事業者はセキュリティインシデントについて対応した状況（被害状況、対応結果等）を記録し、定期的にシステム第一課へ報告及び改善策の提案を行う。必要に応じて自社または自社グループ会社内で、フォレンジング業務を実施しマルウェアの検体を分析し、対策を行うこと。
58	サービスオペレーション	セキュリティ運用	アクセスログ管理	運用事業者は、コンピュータシステム運用業務にて運用しているシステム及びサービス（機構DC、機構クラウドDC（メインリージョン/バックアップリージョン）、SaaSのサービス等）に加えて、システム第一課が指示した所定のシステム及びサービス（ハウジングのシステムや情報通信網のサービス等）に関するアクセスログを定期的に分析（ログ間の相関も含む）し、保管する。分析結果で、異常が発見された場合は、障害対応計画や各種対応手順書に沿って速やかに異常事象に対して対応策を実施する。発生したセキュリティインシデントに対する対応策が対応手順書に定義されていない、もしくはセキュリティインシデントの優先度が高い場合は、システム第一課に確認のうえ実施する。 なお、アクセスログ収集対象機器は、システムの安定稼動に必要な機器を運用事業者にて検討する。対象機器はシステム第一課に報告、承認を得る。システムの稼働状況により随時見直すこと。 また、運用事業者は、アクセスログ管理について対応した状況を記録し、定期的にシステム第一課へ報告及び改善策の提案を行う。 ※なお、保守業務を別途契約しているシステム（ハウジング対象システム）については、アクセスログ管理の対象外とする。 ※ログ間の相関分析については、運用設計時に対象とするログを決定する。
59	サービスオペレーション	セキュリティ運用	セキュリティパッチ適用	運用事業者は、検証環境を利用し、サーバやクライアントPCのセキュリティパッチの影響調査の実施と結果報告を事前に実施した上で定期的にセキュリティパッチの適用を実施し、常に最新の状態を保つこと。 ※なお、保守業務を別途契約しているシステム（ハウジング対象システム）については、セキュリティパッチの対象外とする。

	60	サービスオペレーション	セキュリティ運用	セキュリティに係る運用及びメンテナンス	運用事業者は、情報セキュリティ対策、アクセスログ管理、セキュリティパッチ対応等を実施するために、以下の運用及びメンテナンスを実施する。 ■情報セキュリティ対策に係る運用及びメンテナンス ・ウイルス定義データ更新、ソフトウェアバージョンアップ、ポリシー適用作業対応、ソフトウェアレポート確認 ■ネットワークセキュリティに係る運用及びメンテナンス ・ファイル操作ログ確認、クライアントPC操作ログ確認、クライアントPC情報収集スケジュール変更作業、クライアントPCインストール配布モジュール作成、禁止アプリケーション起動時の対象機器情報取得作業、禁止アプリケーション追加作業 ■セキュリティパッチ管理 ・パッチ配布スケジュール作成、パッチ配布作業、サーバセキュリティパッチ適用、パッチ検証 上記以外にも、運用事業者が必要と判断したセキュリティ運用に係るメンテナンスを実施すること。
	61	サービスオペレーション	セキュリティ運用	セキュリティ運用に係る情報収集・一元管理	運用事業者は、情報通信網及びコンピュータシステム運用における情報を包括的に収集し、一元管理すること。また、システム第一課に対し、情報セキュリティ対策を定期的に報告すること。

62	サービスオペレーション	システム設定変更	システム設定変更	運用事業者は、システム設定変更について、対応方針を考え、対応策を実施する。 主な個別設定変更作業は以下となる。 以下、システム共通の作業（一例）となる。 ■作業頻度：随時 ・非監視設定作業 ・ログ退避運用 以下、機構DC、機構クラウドDC（メインリージョン/バックアップリージョン）及びSaaSについての作業（一例）となる。 ■作業頻度：随時 ・【AD】グループポリシー適用、他業務システムとの連携 ・【DHCP】新規スコープ追加作業 ・【Intune】パッチ適用作業等のスケジュール更新 ・【AppleBusinessManager】公用スマホ管理 ・【Autopilot】キッティング作業に係る設定等 ・【Sharepoint Online】サイト管理 ・【Teams電話】電話機払い出し、組織変更対応、番号割り当て等 ・【機構クラウドDC上へのシステム構築依頼時】リソース払い出し対応、リソース設定変更対応、リソース削除対応 ■作業頻度：月次 ・【AAUM】パッチ適用作業等のスケジュール更新※ ・【OneDrive】各部門別使用状況確認 ・【Azure Virtual Desktop】VMマスターイメージ管理 上記以外にも、運用事業者が必要と判断する作業については、機構と協議した上で作業を実施すること。
63	サービスオペレーション	システム設定変更	システム設定変更(ネットワーク)	以下、ネットワークについての作業となる。 ■作業頻度：随時 ・本部L2/L3スイッチ設定変更対応 ・ベンダー開発環境用VLANのアクセス制限追加・変更 ・FW設定変更依頼 ・外部DNS登録情報変更依頼 ・IPS監視停止依頼 ・IPSポリシー変更依頼 ・FW/IPSアップグレード作業対応

	64	サービスオペレーション	ネットワーク運用	有線、無線LAN運用	本部の有線LAN、及び本部・国内・在外拠点無線LANの運用を包括して実施すること（他の事業者が同保守は別契約により他の事業者が行っている）。主な運用業務は以下の通り。 ・wifi等の接続方法、ゲスト用インターネットID、PWに関する問合せ対応 ・ネットワーク障害対応支援 ・ゲスト用インターネットID、PWの管理 ・本部無線LANの証明書管理・運用業務 ・外部向けパスワードの管理・変更 上記以外にも、運用事業者が必要と判断したシステム運用業務は実施対象とすること。 特に本部ネットワークについては重要なため、機器の構成を十分理解のうえ、追加としてメッセージ監視および保守業者と協力して障害対応業務を実施すること。
	65	サービスオペレーション	教育・研修	職員研修関連	運用事業者は、機構ユーザがコンピュータシステムを円滑かつ効率的に活用するために必要な各種研修（新人職員向け研修、中途採用職員等向け研修）を立案・実施する。また、コンピュータシステム運用業務を通して得られる情報およびノウハウを活用して、コンピュータシステムの利用を促進させることを目的とした啓蒙活動やデータ登録等を実施すること。 【参考】 ・過去の研修実績は以下の通り。 ①理事研修：理事着任時（年に数回）　JICA情報基盤、PC等の使い方 ②中途採用者等向け研修：月に1回程度　JICA情報基盤、PC等の使い方 ③新入職員向け研修：年に1回程度　JICA情報基盤、PC等の使い方
	66	サービス関連調査・提言	インフラ導入・設定変更に係る状況把握・提言	インフラ導入・設定変更に係る状況把握・提言	運用事業者は、IT基盤に関するサービス追加や利用機能追加等の計画を当機構が検討する際に、現行IT基盤への影響の検討や関連する技術動向の調査を行い、円滑な導入が行えるような提言を能動的に実施すること。
	67	サービス関連調査・提言	インフラ導入・設定変更に係る状況把握・提言	インフラ導入・設定変更条件の整理	運用事業者は、本調達で導入したハードウェア、OS、ミドルウェア、パッケージソフトウェア及びIaas・Saasに対する各種利用条件等の整理・取り纏めを行い、システム第一課へ報告する。
	68	サービス関連調査・提言	インフラ導入・設定変更に係る状況把握・提言	インフラ導入・設定変更の試験の支援	運用事業者は、当機構が別途調達によりIT基盤のサービス・機能追加を行う場合に、設定変更の試験のオペレーション、環境準備等に関して、機構の支援を実施する。

69	サービス関連調査・提言	インフラ導入・設定変更に係る状況把握・提言	情報通信網関連業務	運用事業者は、別途当機構が実施する情報通信網関連業務について、情報通信網更改時のIPアドレスの振り直し等の支援及び新規拠点開通/拠点廃止/移転時の拠点側の作業を実施する。 ■情報通信網更改時 ・在外拠点の端末のIPアドレス振り直し作業の実施支援及び管理 ■情報通信網運用時 ・IPS設定、ファイアウォールポリシー、コンテンツフィルタリングフィルター、DNSドメインレコード、メールセキュリティ等の申請業務 ・在外の不正PC接続検知システムの設定および情報の一元管理 ・在外無線LANのゲスト用ID.Passwordの発行管理 ・セキュリティ基盤を含め、上記に関する情報の包括的な一元管理 ・在外の不正PC接続検知システム保守対応（障害時の交換機器送付等）・在外の不正PC接続検知システムの員数管理（交換用機器は本部で在外展開の半数を予備品として保管） ■新規拠点開通/拠点廃止/移転時 ・不正PC接続検知システムの導入 ・情報通信網新規開通/廃止支援 ・情報通信網接続/切断作業 上記以外にも、運用事業者が必要と判断した業務は実施対象とすること。
70	サービス関連調査・提言	IT環境変更に係る状況把握・提言	IT環境変更に係る状況把握・提言	運用事業者は、基盤系システムの変更や新たな基盤・ツールの導入、組織体制の変更等機構IT環境が変更される際、業務系システムへの影響、技術動向等を検討把握し、円滑な導入のために必要な提言を能動的に実施すること。 また、システム第一課からの問い合わせについても対応を実施すること。
71	サービス関連調査・提言	監査（内部・外部）対応	監査（内部・外部）対応	日本政府、機構が外部委託した事業者もしくは機構内部の組織が監査を実施する場合、監査対応はシステム第一課が主体的に対応するが、運用事業者は当該監査に必要なデータ(ログデータ等）のシステム第一課への提供や。当該監査結果による要請に対しシステム第一課と協議した範囲で適切な対応を実施すること。 なお、監査は最大で年5回程度を見込むこと。

72	ITコンシェルジュサービス	-	各部署システム化支援	運用事業者は、情報システム部およびシステム第一課の業務である各部署が抱えるシステム化に関する課題の解決に対して、 サービス提供環境(機構DC、機構クラウドDC（メインリージョン/バックアップリージョン）及びSaaS)及びその運用業務事業者としての観点から助言や提案等の支援を行う。 支援内容は以下を想定する。 なお、サービス提供以外で他部署・国内機関・在外拠点で個別調達・開発された業務アプリケーションやアプリケーション用基盤は対象に含まない。 (上流・企画フェーズ) ・情報システム部が作成する調達仕様書(案)への技術的な相談への対応 ・法改正・制度改正、ハード更改等により、各システムのアプリケーションの改修・開発が必要とシステム第一課が判断した場合又は運用事業者が日常業務の中で必要と判断した場合に、サービス提供環境の運用面における対応方針及び前提条件等を整理し、実施した場合のサービス提供環境への影響調査および提言を行う ・国内、在外拠点から情報システム部が受付けたITに係る相談に対する技術的なアドバイス (下流・実行フェーズ) ・システム運用管理やサービスレベル遵守のために各システムのアプリケーションの改修・開発における情報システム部からの技術的な相談への対応
73	ITコンシェルジュサービス	-	IT基盤整備支援	運用事業者は、情報システム部が所管する機構全体に係るIT基盤整備において、運用サービス等の知識を活かしてプロジェクトを支援する。 なお、支援とはサービス提供環境(機構DC、機構クラウドDC（メインリージョン/バックアップリージョン）及びSaaS)及びその運用業務事業者としての観点から情報システム部に対して助言や提案等を指す。 例として過去の事例を以下に記載する。 ・在宅環境整備支援(Teams,メールクラウド化等のクラウド化推進) ・各部署の業務主幹システムの要件定義・設計支援(OS等が変更される場合の留意点や課題を抽出し、展開仕様を決定する支援を行う) ・次期PC更改仕様の策定(これまでの方針と現行の課題を踏まえ、次期PC更改の調達仕様の盛り込むべき仕様を考慮して仕様書の作成支援を行う） 等
74	ITコンシェルジュサービス	-	運用業務全体の状況把握	・コンピュータシステム運用業務全体を俯瞰してシステム第一課へ提言ができるよう、機構・運用事業者内の各担当と密にコミュニケーションをとり、システム運用業務全体の状況把握のために必要な会議へ参加する等の方法にて、コンピュータシステム運用業務全体の状況を把握すること。 ・状況把握のためにシステム第一課の承認や他の事業者の協力が必要な事項が発生した場合にも、出来る限り必要な情報を限定し、効率的に業務が実施できるよう留意すること。 ・別途選定され主として各事業部の業務アプリケーション企画・支援を行うPMO事業や、IT基盤上にハウジングされる業務アプリケーション基盤請負事業者等とは定期的に開催される機構全体の「システム運用連絡会（開催頻度：月1回）」参加を含め、円滑な連携ができるよう務めること。 ・担当者はコンピュータシステム運用業務全般及び情報技術の動向に係る知識を有しており、システム第一課に対し運用作業の内容に係るアドバイス、最新の情報技術の説明ができる必要がある ・ITコンシェルジュ及び後述のサービス提供環境における支援業務はIT基盤にかかる急ぎの依頼対応等を含めたよろず相談対応が求められるが、作業実施規模は2人月/月を上限とし、これを超える場合は当機構と協議することとする。 ・ITコンシェルジュメンバはTeams、メール等を通じ当機構担当職員と密に連絡を取り合える体制を確保すること。 ・ITコンシェジュルメンバの1名は請負者自らの従業員であること ・緊急対応に備えてメンバのうち最低1名は当機構に常駐することが望ましい（特定のメンバの常駐は求めず）いずれかのメンバ1名の常駐を想定）。

75	サービス提供環境における支援業務	-	運用支援業務	運用事業者は、サービス提供環境（機構DC、機構クラウドDC（メインリージョン/バックアップリージョン）及びSaaS）において、以下の支援を行う。 ・サービス提供環境が正常稼動するため、各部署の担当者からの問い合わせや依頼について、その対応にあたること。 ・システム異常時、原因究明と復帰作業及び対策を講じ、各種調整を図ること。 ・サービス提供環境のコンテンツの整理に関し支援作業をすること。なお、コンテンツとは本調達で導入するSaaS機能内において運用事業者あるいは機構が設定あるいは設置・保存した機能やデータを指す。 ・その他、サービス提供環境の運用作業に関する各担当者からの問い合わせや依頼事項について、システム的な立場から対応策の検討に協力すること。また、その受付・窓口を行うこと。
76	サービス提供環境における支援業務	-	開発支援業務	運用事業者は、サービス提供環境（機構DC、機構クラウドDC（メインリージョン/バックアップリージョン）及びSaaS）において、以下の支援を行う。 ・サービス提供環境上の既存コンテンツの変更や、担当部署によるコンテンツの新規追加、ＩＴ基盤自体の小規模な機能拡張・設定変更においてIT基盤の知見をもって、当機構に対し助言等の支援や設定変更等を行うこと。ここでのコンテンツとは本調達で導入するSaas機能内において運用事業者あるいは機構が設定あるいは設置・保存した機能やデータを指す。 具体的事例として、過去には、セキュリティ指針変更に伴うSendGrid導入支援（機能・影響調査、導入方式提言、計画助言）、Microsoft365におけるYammerの有効化設定、チャットボット（Power Virtual Agents）精度改善設定等があった。 ・期間内に発生したサービス提供環境における設定変更や機能追加・追加導入サービス等について当機構担当へ仕様を確認し順次打ち合わせ、実装計画策定や軽微なものの実装・テスト補助・助言を行い、稼働体制への移行支援をすること。 ・サービス提供環境における設定変更や機能追加・追加導入サービス等については、本契約範囲となる既存情報共有基盤の運用開発業務に支障が出ない範囲、すなわち契約工数内（ITコンシェルジュ及びサービス提供環境における支援業務において2人月/月を上限とする）で対応できる範囲での支援とし、各担当者へ要件・仕様を確認し順次打ち合わせ、設計、構築及びテストを行い稼働体制に移行するための作業を行うこと。 ・その他システム第一課が所管するIT基盤に係る企画・計画・検討・調査・機能実装等における、関係する各担当者からの問い合わせについて、IT基盤の知見をもってシステム的な立場から対応策の検討に協力すること。
77	BCP発動時に備えた機構クラウドDC（バックアップリージョン）の運用	-	BCP発動時の運用業務	運用事業者は、以下の業務を行う。 ・機構DCの被災状況を確認すること ・機構クラウドDC（メインリージョン）の稼働状況を確認すること ・切替作業は原則運用事業者にて迅速かつ確実に行える方法を定めるておき実施する ・切替作業後、必要とされているサービスが提供されていることを確認する ・機構DCに対する監視は、ネットワーク機器へのPing及びセキュリティ監視を実施する。 ・セキュリティに関する監視および対策は、発動前と同様に行うこととするが、セキュリティパッチのクライアントPCへの配信や、ウィルス検知のためのパターンファイルの入手が困難となることが想定されるため、この場合は運用事業者は取りえる最善の策をシステム第一課と相談の上実施すること ・BCP解除後には平常時運用への切り戻しを行う
78	BCP発動時に備えた機構クラウドDC（バックアップリージョン）の運用	-	BCP発動時に備えた機構クラウドDC（バックアップリージョン）の通常（平常時）運用	運用事業者は、以下の業務を行う。 ・年に最低１回機構にて実施するBCP発動訓練時の対応を行うこと。 ・システム監視等、BCP発動時に備えた機構クラウドDC（バックアップリージョン）のサービスに対しても、サービス運用管理業務（サービス管理（インシデント管理）、問題管理、変更管理、リリース管理、構成管理、ドキュメントの整備及び管理、全体管理、セルフモニタリング）を実施すること。 ・BCP発動に備え、システムのオンラインバックアップを取得すること

79	サービス管理（インシデント管理）	機構内・在外利用者向け業務	国内拠点IT支援現地出張	機構本部内及び国内拠点の利用者からの問い合わせに対して、電話やメール、Web会議等での対応が困難な場合又は利用者から要望があった場合、運用事業者は、必要に応じて直接現地に赴いて対応を行い、問題の解決等を図る。 機構本部以外の問い合わせへの現地サポートについて、運用事業者は、機構や関連事業者と調整し、対応又は指示する。 （本部以外の現地サポート回数は、年間5～10回程度※を見込んでいるが、必要性と効果を鑑み、回数・行き先を提案すること。また、旅費等一切の費用は運用事業者の負担にて実施すること。すべての国内機関が支援対象となるが、年間回数の目安には東京国際センター、横浜国際センターを除く13拠点を出張先の対象とする。） ※ITコンシェルジュの出張分も含む。 ※「現地サポート」は現地への出張もしくはWeb会議を通じたサポートどちらかの方法とする。最終的な回数（契約締結後）は機構と相談の上決定する。 ※「現地サポート」対応後に利用者に対して満足度調査を実施する。
80	サービス管理（インシデント管理）	機構内・在外利用者向け	在外IT支援現地出張	機構在外拠点の利用者からの問い合わせに対して、電話やメール、Web会議等での対応が困難な場合又は利用者から要望があった場合、運用事業者は、必要に応じて直接現地に赴いて対応を行い、問題の解決等を図る。 （在外拠点への現地出張回数は、年間5～10回程度を見込んでいるが、必要性と効果を鑑み、回数と行き先を提案すること。アジア、大洋州、アフリカ、中南米、中東欧州等すべての地域の在外拠点が支援対象となる。また、旅費等一切の費用は運用事業者の負担にて実施すること。なお、渡航者の安全を考慮するため、「退避勧告」「渡航延期」等の危険情報が出ている国は基本的に対象外とする。） ※直接現地に赴く担当者は必ずしも日本から渡航する必要はない。危険度に応じて、再委託契約を締結の上、現地法人に業務を委託する等、その状況に応じて全体を俯瞰して実施可能な方法を検討し、費用の平準化を図った上で見積を実施すること。 ※「現地サポート」対応後に利用者に対して満足度調査を実施する。
81	サービス管理（インシデント管理）	ユーザからの申請対応	対応時間	平日午前9時から午後6時（日本時間） 但し、状況により、開始・終了時間を前後させる可能性がある。 運用事業者は上記の時間に対応依頼を受け付ける。
82	サービス管理（インシデント管理）	ユーザからの申請対応	ユーザからの申請受付	運用事業者はユーザから各種申請に対して対応を行う。 また、受付内容について情報共有のために履歴を残す。履歴については、システム第一課に定期的に報告する。
83	サービス管理（インシデント管理）	ユーザからの申請対応	ファイル関連対応	サーバ上のファイルに関する以下に該当する申請があった場合、対応を実施する。 ・FileMaker用ファイル削除申請 ・仮想サーバ、メール監査データのファイルリストア申請 ・フォルダアクセス権変更申請（部署用OneDriveは除く） ・組織変更等にともなう、フォルダの作成・変更・アクセス権変更申請 ・FileMakerアプリケーションの加除申請対応（バックアップからのリストア対応） 　等 対応状況及び結果は、実績管理のため、履歴として残す。 また、運用事業者は、これらの情報をシステム第一課が必要と判断した際には、必要十分な形で提供する。

84	サービス管理（インシデント管理）	ユーザからの申請対応	ユーザディレクトリ関連対応	ActiveDirectoryに関する以下に該当する申請があった場合、対応を実施する。 ・組織変更、異動、兼務情報の追加などによるユーザ情報の管理 ・配布グループの管理 ・セキュリティグループの管理 ・スキーマの管理（拡張） 　等 上記に付随して以下の項目についても、ディレクトリ情報にあわせてメンテナンスを行う ・社内SNSの兼務情報（兼務先の組織名、役職等） ・電話帳の兼務情報（兼務先の組織名、役職等） 　等 対応状況及び結果は、実績管理のため、履歴として残す。 また、運用事業者は、これらの情報をシステム第一課が必要と判断した際には、必要十分な形で提供する。 ※組織変更・人事異動対応の時期としては、年度末の3月から新年度のにかけてが最も大規模であり、次に大きい規模が5月、7月、10月、1月となっている。 ※2021年度人事異動対応件数は、役職員等が平均約200件/月、業務委託・派遣等非役職員は平均407件/月となっている。（なお、処理件数は4月が一番多く、2021年4月は役職員559件、非役職員996件）
85	サービス管理（インシデント管理）	ユーザからの申請対応	設備予約対応	設備予約（スケジュール）に関する以下に該当する申請があった場合、対応を実施する。 ・設備情報の登録（追加）・変更申請 ・設備情報の削除申請 ・設備グループの登録・変更申請、設備グループへの個別設備の追加・削除申請 ・設備の利用者登録（追加）申請（※） ・設備の利用者解除申請（※） 　等 ※登録した利用者のみしか利用できないように設定をする。例えば、役員しか利用できない会議室を、役員が予約できるように設定する。 対応状況及び結果は、実績管理のため、履歴として残す。 また、運用事業者は、これらの情報をシステム第一課が必要と判断した際には、必要十分な形で提供する。 なお、設備の利用状況のデータを取得し分析をする部署に定期的にデータ提供すること。

86	サービス管理（インシデント管理）	ユーザからの申請対応	全社ポータル対応	全社ポータルに関する以下に該当する申請があった場合、対応を実施する。 ポータルサイトの設置 ・ポータルサイトの作成、変更申請 ・ポータルサイトの削除申請 ・ポータルサイトへのアクセス権限変更申請 ・組織変更等に伴う、各部発信ページ、各部内共有サイトの設置・変更申請 ・業務公電上の組織階層改修、権限変更 ・目的別ページの設置・変更申請 　等 なお、申請等により以下のようなポータルサイトの改修等が必要になった場合は、No."&B78&"の「"&C78&"」の「"&E78&"」の一環としてこれに対応する。"&" ・既存の障害対応、組織変更や人事異動等による必然的改修 ・既存ポータルサイトの軽微な改修やレイアウト変更 ・既存ポータルサイト上のコンテンツの複製、および軽微な改修 ・既存ポータルサイト上の電子申請の修正・追加 　等 対応状況及び結果は、実績管理のため、履歴として残す。 また、運用事業者は、これらの情報をシステム第一課が必要と判断した際には、必要十分な形で提供する。
87	サービス管理（インシデント管理）	ユーザからの申請対応	メール	メールに関する以下に該当する申請があった場合、対応を実施する。 ・メーリングリストの作成・変更・削除 　等 対応状況及び結果は、実績管理のため、履歴として残す。 また、運用事業者は、これらの情報をシステム第一課が必要と判断した際には、必要十分な形で提供する。
88	サービス管理（インシデント管理）	ユーザからの申請対応	マネージドプリントサービス（MPS）関連対応	マネージドプリントサービス（MPS）に関する以下に該当する申請があった場合、対応を実施する。 ・スキャナフォルダロック解除申請 　等 対応状況及び結果は、実績管理のため、履歴として残す。 また、運用事業者は、これらの情報をシステム第一課が必要と判断した際には、必要十分な形で提供する。

89	サービス管理（インシデント管理）	ユーザからの申請対応	PC設定対応	標準PC、持込PC、研修・会議用PCの設定に関する以下に該当する申請があった場合、対応を実施する。 ・ソフトウェア/ドライバインストール申請 　等 対応状況及び結果は、実績管理のため、履歴として残す。 また、運用事業者は、これらの情報をシステム第一課が必要と判断した際には、必要十分な形で提供する。
90	サービス管理（インシデント管理）	ユーザからの申請対応	アクセス許可対応	アクセス許可に関する以下に該当する申請があった場合、対応を実施する。 ・インターネットアクセス許可申請：特定URLのフィルタを解除するための申請 　等 対応状況及び結果は、実績管理のため、履歴として残す。 また、運用事業者は、これらの情報をシステム第一課が必要と判断した際には、必要十分な形で提供する。
91	サービス管理（インシデント管理）	ユーザからの申請対応	アカウント関連対応	アカウントに関する以下に該当する申請があった場合、対応を実施する。 ・Windowsアカウント管理（登録/修正/削除/通知） ・Windowsパスワード初期化/通知 ・Windowsアカウントロック解除/通知 ・リモートアクセスサービス（FirePass、モバイル端末からのアクセス、仮想デスクトップサービス）のアカウント管理（登録／修正／削除／通知） ・認証プロキシサービス、リモートアクセスサービスのアカウント関連業務 ・大容量ファイル転送サービスのアカウント新規発行／削除 ・上記各アカウント棚卸 ・FileMaker管理者メンテナンス ・FileMaker管理者IDの定期的なパスワード変更 ・ゲストユーザM365招待 　等 対応状況及び結果は、実績管理のため、履歴として残す。 また、運用事業者は、これらの情報をシステム第一課が必要と判断した際には、必要十分な形で提供する。 ※2022年4月時点でWindowsアカウントのユーザ数は、約6,100ユーザ

92	サービス管理（インシデント管理）	ユーザからの申請対応	コード（ID）関連対応	コード（ID）全般に対する管理に関する以下に該当する申請があった場合、対応を実施する。 ・ID関連統一申請（Win　ID発給・廃止） ・コードメンテナンス（共通） ・コードメンテナンス（個別） 　等 対応状況及び結果は、実績管理のため、履歴として残す。 また、運用事業者は、これらの情報をシステム第一課が必要と判断した際には、必要十分な形で提供する。 ※また、実際のユーザID申請対応は、約1,764件 / 月（2021年度 合計21,169件）
93	サービス管理（インシデント管理）	ユーザからの申請対応	その他対応	運用事業者は、以下に該当する申請（組織変更・異動時の対応を含む）があった場合、対応を実施する。 ・社内SNSデータの作成申請 ・大容量ファイル送受信に関する申請 ・ファイル共有（ファイルサーバ）に関する申請 ・Teams固定電話に関する申請 ・その他Windows作業支援 ・機器設置等依頼 ・入室申請 ・データセンタへの入館申請 ・席替え連絡 ・各部門のIT担当者変更申請 ・機器紛失に係わる顛末書（フリーフォーマット）等の受付 ・組織および人に関するコード類の変更修正対応 ・その他IT機器利用に関する一般的な問合せ/相談 　等 対応状況及び結果は、実績管理のため、履歴として残す。 また、運用事業者は、これらの情報をシステム第一課が必要と判断した際には、必要十分な形で提供する。

94	サービス管理（インシデント管理）	セキュリティ運用	セキュリティインシデント対応	セキュリティインシデントが発生した場合、運用事業者は、原因究明の支援を行うこと。 ・ユーザからの申告の確認 ・各運用事業者へのエスカレーション ・各運用事業者から連携のあった障害情報のユーザへの通知 ・対応状況の台帳等での管理 ・復旧後のユーザへの通知 上記以外にも、運用事業者が必要と判断したセキュリティインシデント対応は実施するものとする。 また、セキュリティインシデントとしては、以下を想定している ・ウイルス感染 ・不正アクセス ・情報漏洩 ・迷惑メール送受信 ・不正ソフトウェアの使用 ・標的型攻撃、早期警戒対応 ・未知の脅威への対応 等
95	サービス管理（インシデント管理）	システム監視	サーバ稼動（死活）監視	運用事業者は機構DC、バックアップリージョンを含む機構クラウドDCの各サーバの死活監視を行う。 各種メッセージおよびログについては、監視し正常に稼働していることを常に確認する。 (上位の監視は、それぞれの保守事業者が個別に行う)
96	サービス管理（インシデント管理）	システム監視	サーバ性能監視	運用事業者は基盤系システムのCPU、メモリ、ディスク、データベースやWebサービスへの応答時間等のサーバ性能の閾値を監視し、閾値を超えた場合は必要に応じてシステム第一課及び保守業者に報告すること。 なお、監視項目は運用設計時にシステムの安定稼動に必要な項目を運用事業者にて検討する。閾値についても同様に検討を行い、システム第一課に報告、承認を受ける。また、監視項目及び閾値についてはシステムの稼動状況により随時見直しを行うこと。

97	サービス管理（インシデント管理）	システム監視	ネットワーク機器の監視	運用事業者は、監視サービス等により、機構DCのネットワーク機器に対し常時Pingによる死活監視を行う。 なお、SNMPによるリアルタイムの監視ができるようにすること。 また、ネットワーク機器の監視については、現行運用業務にて本部NW（LAN)環境の以下の運用業務も実施しているため、次期運用業務でも相応の作業を実施すること。 ・コンソリデーション～端末の故障対応（予備部材、ケーブルの交換） ・LANポート管理（ポートの有効/非有効化設定含む。） ・NW機器の変更設計、設定（コンフィグ、ルーティング、フィルター、VLAN等） ※本部LANの運用事業者の準備する手順書に従い、設定変更対応を行う。 ・IPアドレス設計、管理 ・F/W設計、管理 ・障害切り分け、ベンダーへの保守コール ・不正接続検知 ・計画停止、メンテナンス時のサポート　等 その他在外拠点、国内拠点のルータや在外拠点の無線LAN機器、不正PC接続検知・排除機器はそれぞれの事業者によって保守が行われるが、現状を積極的に把握し包括的に管理できるようにすること。
98	サービス管理（インシデント管理）	システム監視	オンライン接続状況の監視	運用事業者は、PINGおよび監視サービス等を使用しての機構DC及びバックアップリージョンを含む機構クラウドDCのシステムへのオンライン接続状況を監視し、定期的に接続可否の確認を行う。
99	サービス管理（インシデント管理）	システム監視	リソース使用状況監視	運用事業者は、各サーバーのディスク、CPU、メモリ、プロセス、ネットワークのトラフィック等の使用状況について監視サービス等により常時監視する。また、運用事業者は、随時リソース情報を取りまとめ、システム第一課から要請があった場合は必要十分な形で提供する。
100	サービス管理（インシデント管理）	システム監視	ハードウェア状態監視	運用事業者は、機構DCにおいてハード障害が発生していないかを監視する。
101	サービス管理（インシデント管理）	システム監視	ソフトウェア状態監視	運用事業者は、監視サービス等によりソフトウェア（サービス又はプロセス）が正常に稼働しているかを監視する。
102	サービス管理（インシデント管理）	システム監視	ログの監視	運用事業者は、機構DC、バックアップリージョンを含む機構クラウドDC及びSaaSの各サーバ・ネットワーク機器・サービス等のログを統合監視する。 なお、監視するログは運用設計時にシステムの安定稼動に必要なログを運用事業者にて検討し、システム第一課に報告、承認を受ける。また、監視するログについてはシステムの稼動状況により随時見直しを行うこと。

103	サービス管理（インシデント管理）	システム監視	業務系システムの監視	運用事業者は、業務系システムの自動化監視ツール（ただし、保守業者によって設定変更及びツール変更されることがある。）により自動的に出力されることになっている監視項目に異常があった場合について、運用事業者は、その警報・アラーム等の信号を常時感知できるようにしておき、当該アラーム等の信号を各システムの保守事業者にすみやかに伝達（自動配信メール可）することとする。なお、警報・アラーム等の信号は運用事業者が用意した端末またはサービスに通知できるよう保守業者にて準備することとする。
104	サービス管理（インシデント管理）	障害管理	障害対応計画の作成	運用事業者は予見される障害を予めリストアップし、障害発生時に取るべき応急措置や関係者への連絡などの一連の対応項目を全てリストアップした障害対応計画の作成を行う。 また、運用事業者は、障害対応計画の見直しを実施し、更新を行う。
105	サービス管理（インシデント管理）	障害管理	障害申告の受付	運用事業者は、障害申告・システム監視・その他で障害発見者（運用事業者自身、機構ユーザまたは、関連事業者等）からの障害申告を受理し、障害状況の把握を行う。
106	サービス管理（インシデント管理）	障害管理	障害発生箇所の切り分けと応急措置及び担当ベンダーへの指示	運用事業者は、受理した障害申告に対し、迅速に障害箇所（ホスト、サーバー、PC、ネットワーク等）及び担当ベンダーの一次切り分け（障害部位と原因の特定、この後の対応方法の判断）を行う。その後、運用事業者は、復旧方法の検討等においてシステム第一課及び関連事業者の意見を聴取し、迅速かつ確実な復旧が行われるように、関連ベンダーに対して障害の復旧を指示するなど、主体的に作業を進める。 また、一次切り分け後、運用事業者の責任範囲であるもの及び、対応可能なものについては運用事業者が実施する。 なお、運用事業者は、障害の影響拡大の防止を目的とし、障害システム及び影響を与えるシステム等に対する応急措置を立案し、システム一課の指示のもと、関連事業者に応急措置の実施を連絡する。
107	サービス管理（インシデント管理）	障害管理	機構及び関連事業者への通報	運用事業者は、原課業務に影響を与える障害については、障害速報を作成し、逐次対応状況を原課及び関連事業者へ報告する。その際、システム第一課への報告も併せて行う。 また、システム第一課の求めに応じた対応状況の報告も随時行う。 なお、共通で使用するシステムの障害（※）については直接システム第一課へ報告すること。 ※ネットワークの不通やグループウェア・ファイルサーバなど、業務に特化されない共通的な機能に関する障害
108	サービス管理（インシデント管理）	障害管理	利用者への障害連絡	運用事業者は、必要に応じてシステムの利用者へ、電話、電子メール、又は現地（現場）へ赴き、障害の状況について連絡する。
109	サービス管理（インシデント管理）	障害管理	回復の確認と報告	運用事業者は、運用事業者内担当者、又は、担当ベンダーより回復措置完了の報告を受け、機能や装置の正常性を確認し、システム第一課及びシステムの利用者へ障害が回復した旨と障害回復時間を報告する。
110	サービス管理（インシデント管理）	障害管理	障害の記録と報告	運用事業者は、障害の発生から回復までの経過措置を、必要があれば関連ベンダーの協力の下、時系列に記録するとともに、障害対応状況を一元的に管理し、システム第一課及び関連ベンダーと共有する。また、運用事業者は、未解決の障害を含む障害の発生状況を報告書に取りまとめてシステム第一課へ提出する。

111	サービス管理（インシデント管理）	障害管理	緊急連絡体制の整備	運用事業者は、障害等の緊急事態発生時に早期復旧に向けた対処を実現するために、機構の関係部門および関連事業者の責任及び役割分担を定義した連絡体制図を作成し、機構の関係部門および関連事業者に周知させる。連絡体制図に変更が生じた場合は、その都度システム第一課へ報告し、変更内容についてシステム第一課の承認を得る。
112	サービス管理（インシデント管理）	性能管理	性能目標値の設定と見直し	運用事業者は、性能に関する実績値、システム第一課及び原課の要望を参考に、性能目標値の検討及び見直しを行う。見直し後、設定された性能目標値に係る影響を明確にした上で、システム第一課に報告し、承認を受ける。 また、運用事業者は、性能に関する実績値の収集に必要なツール・システムを整備する。
113	サービス管理（インシデント管理）	性能管理	実測値データの取得と分析	運用事業者は、設定した性能目標値に関し、継続的に実測し、達成状況を分析、評価する。 なお、本部のLANについてはLANの運用事業者にて分析、評価、報告を行うため、データの提供を行うこと。
114	サービス管理（インシデント管理）	性能管理	性能改善計画の立案	運用事業者は、性能値の分析の結果、目標値の未達成や劣化傾向が確認された場合は、原因調査及び改善策実施計画を検討し、最終的な改善策実施計画案をシステム第一課に提示し、改善実施計画の承認を受ける。
115	サービス管理（インシデント管理）	性能管理	改善計画実行と結果の確認	運用事業者は、改善策の結果について、性能値の実測により確認を行う。改善計画どおりの改善傾向が見られない場合は、対策の再検討を実施し、システム第一課に提示する。
116	サービス管理（インシデント管理）	可用性管理	システム提供時間	機構DC及びバックアップリージョンを含む機構クラウドDCの運用・障害対応は24時間365日とし、各システムの計画停止のスケジューリング等は運用設計時に検討・確定する。 なお、SaaSについては、クラウド事業者のサービス提供時間に準ずる。
117	サービス管理（インシデント管理）	可用性管理	システムの回復目標値の設定と見直し	運用事業者は、可用性に関する実績値、システム第一課及び原課の要望を参考に、可用性目標値の検討及び見直しを行う。見直し後、設定された可用性目標値に係る影響を明確にした上で、システム第一課に報告し、承認を受ける。 また、運用事業者は、可用性に関する実績値の収集に必要なツール・システムを整備する。
118	サービス管理（インシデント管理）	可用性管理	障害回復実績データの収集と分析	運用事業者は、設定した可用性目標値に関し、システムごとの障害対応状況を継続的に収集するとともに、システムの冗長性構成の検証やバックアップや障害回復方法の検証等により、達成状況を分析、評価する。
119	サービス管理（インシデント管理）	可用性管理	可用性改善計画の立案	運用事業者は、可用性の分析の結果、目標値の未達成や劣化傾向が確認された場合は、原因調査及び改善策実施計画を検討し、最終的な改善策実施計画案をシステム第一課に提示し、改善実施計画の承認を受ける。
120	サービス管理（インシデント管理）	可用性管理	改善計画実行と結果の確認	運用事業者は、改善策の結果について、可用性の実測により確認を行う。改善計画どおりの改善傾向が見られない場合は、対策の再検討を実施し、システム第一課に提示する。
121	サービス管理（インシデント管理）	利用者満足度調査	利用者満足度調査方法の決定	運用事業者は、システム利用者のシステムの利用及びユーザ対応等に関する満足度を調査するために、調査内容の検討及びシステム第一課への提案を行い、システム第一課から承認を得る。 頻度については、原則として全職員に対して半年に1回を想定しているが、運用事業者が機構に最適な頻度を検討し、提案するものとする。
122	サービス管理（インシデント管理）	利用者満足度調査	利用者満足度調査実施の準備	運用事業者は、利用者満足度調査方法の準備(調査票・回答ツールの準備等)及びシステム第一課への準備状況の報告を行う。

123	サービス管理（インシデント管理）	利用者満足度調査	利用者満足度調査の実施	運用事業者は、利用者満足度調査を実施する。なお、調査の実施においてインタビュー等が必要な場合は、運用事業者の依頼に基づきシステム第一課において日程調整等の協力を実施する。
124	サービス管理（インシデント管理）	利用者満足度調査	利用者満足度結果の分析	運用事業者は、取りまとめた調査結果について、予め定めた評価方法により利用者満足度の状況を分析する。(期待値と現状のギャップや課題の抽出等)。
125	サービス管理（インシデント管理）	利用者満足度調査	改善策の立案	運用事業者は、抽出した課題に対し、現状システムへの影響範囲や必要なリソース(費用や労力等)を考慮に入れ、改善案の検討・立案を行う。
126	サービス管理（インシデント管理）	利用者満足度調査	利用者満足度調査結果と改善策の報告	運用事業者は、実施した利用者満足度調査結果について、目標の達成状況・課題とその原因・立案した改善策案をシステム第一課に報告する。運用事業者は、システム第一課から提示された今後の方針をもとに、サービスの改善を実施する。
127	問題管理	-	障害の原因となる問題対応状況の追跡	運用事業者は、発生した障害全てに関して、可能な限り再発を防ぐため、障害の根本原因の確認・調査及び解決策案を検討し、定期的に問題対応への経過・状況をシステム第一課に報告する。 また、解決策案の実施にあたって、関連ベンダーへの確認・協力依頼が必要な場合には、自ら確認・依頼を行う。 関連事業者の対応状況を含む解決策案の実施状況を継続的に管理し、定期的にシステム第一課に報告する。 また、運用事業者は、必要に応じて対策を他システム・サーバ等へ横展開することにより、同様な問題が他のシステム・サーバ等に内在していないかを検証し、障害の再発防止に努め、その内容をシステム第一課に報告する。 根本原因の解決に至るまでの間は、再発防止・再発時の迅速な対応を行うための障害対応手順等を準備し、運用事業者内・関連事業者等に周知する。
128	問題管理	-	障害の傾向分析と未然防止策の立案	運用事業者は、障害の傾向分析を行い、顕在化していない問題や、個々の障害分析だけでは発見することが困難なシステム横断的な問題を発見し、それらに対する再発防止策を立案してシステム第一課に報告するとともに、関連事業者に対して再発防止策の実施を指示・依頼する。
129	問題管理	-	問題対応状況の記録と報告	運用事業者は、根本原因解決策の実施状況記録を最新の状態で維持し、根本原因解決後に対応結果を取り纏めて、システム第一課に報告する。 また、運用事業者は、システム第一課及び原課からの情報提供依頼に対して速やかにそれを提示する。
130	変更管理	-	障害・問題・構成管理からのシステム変更要求の管理	運用事業者は、障害・問題・構成管理実施後に必要となったシステムの変更について、以下の変更要求内容を確認し、管理する。また、運用事業者は変更内容に問題がないと判断した場合は変更要求を承認する。 ・変更対象となる内容の記述 ・変更理由 ・変更による効果 ・変更提案書（氏名、連絡先、部署） ・承認者のサイン、印 ・変更対応スケジュール（リリース日、作業予定業者、作業場所） 上記以外にも、運用事業者が必要と判断した項目は確認対象とする。 変更要求の際に、システム第一課の確認が必要と判断した項目については、事前に確認を依頼する。依頼時には変更内容に係るリスクが明確になるよう説明を行う。
131	変更管理	-	変更情報の収集・管理	運用事業者は、変更情報を収集・管理する。また、必要に応じてシステム第一課に変更状況を報告する。

132	リリース管理	-	変更・構成管理からのリリース情報の管理	運用事業者は、変更管理・構成管理実施後に必要となったシステムのリリースについて、以下のリリース内容を確認し、管理する。また、運用事業者はリリース内容に問題がないと判断した場合はリリース内容を承認する。 ・リリース対象となる内容の記述 ・リリース理由 ・リリースによる効果 □リリース日時 ・承認者のサイン、印 ・リリーススケジュール（リリース日、作業予定業者、作業場所） 上記以外にも、運用事業者が必要と判断した項目は確認対象とする。 リリースの際に、システム第一課の確認が必要と判断した項目については、事前に確認を依頼する。依頼時にはリリースに係るリスクが明確になるよう説明を行う。
133	リリース管理	-	リリース情報の収集・管理	運用事業者は、リリース情報を収集・管理する。また、必要に応じてシステム第一課にリリース状況を報告する。
134	リリース管理	-	リリース作業の計画	運用事業者は、リリース作業を行う前までに以下を確認し当日の作業計画を立てる。 □リリース作業対象システム □リリース作業日時 □リリース作業者 □リリース作業時間帯の他作業者の有無 □リリース作業時の抑止有無 □リリース作業時の引継ぎ状態 □リリース作業後の走行検証日時 □バックアップ取得日時 □バックアップ取得作業者 □バックアップ取得媒体 上記以外にも、運用事業者が適切なリリース作業を実施するうえで必要と判断した項目は確認対象とする。
135	リリース管理	-	リリース作業への立会い・作業支援	運用事業者は、必要に応じて、保守事業者が実施するリリース作業に立会い、データセンター内機器の設定変更等、作業の支援を実施する。
136	リリース管理	-	リリース内容の走行検証	運用事業者は、本番環境へのサービス（プログラム）リリース後、安定稼働していることを、走行検証を行うことにより確認する。 運用事業者は、本番環境の安定稼働が問題なくなされていると判断した場合は、リリース結果を事後定期的にシステム第一課に報告を行い、必要と判断した場合は随時個別に報告する。

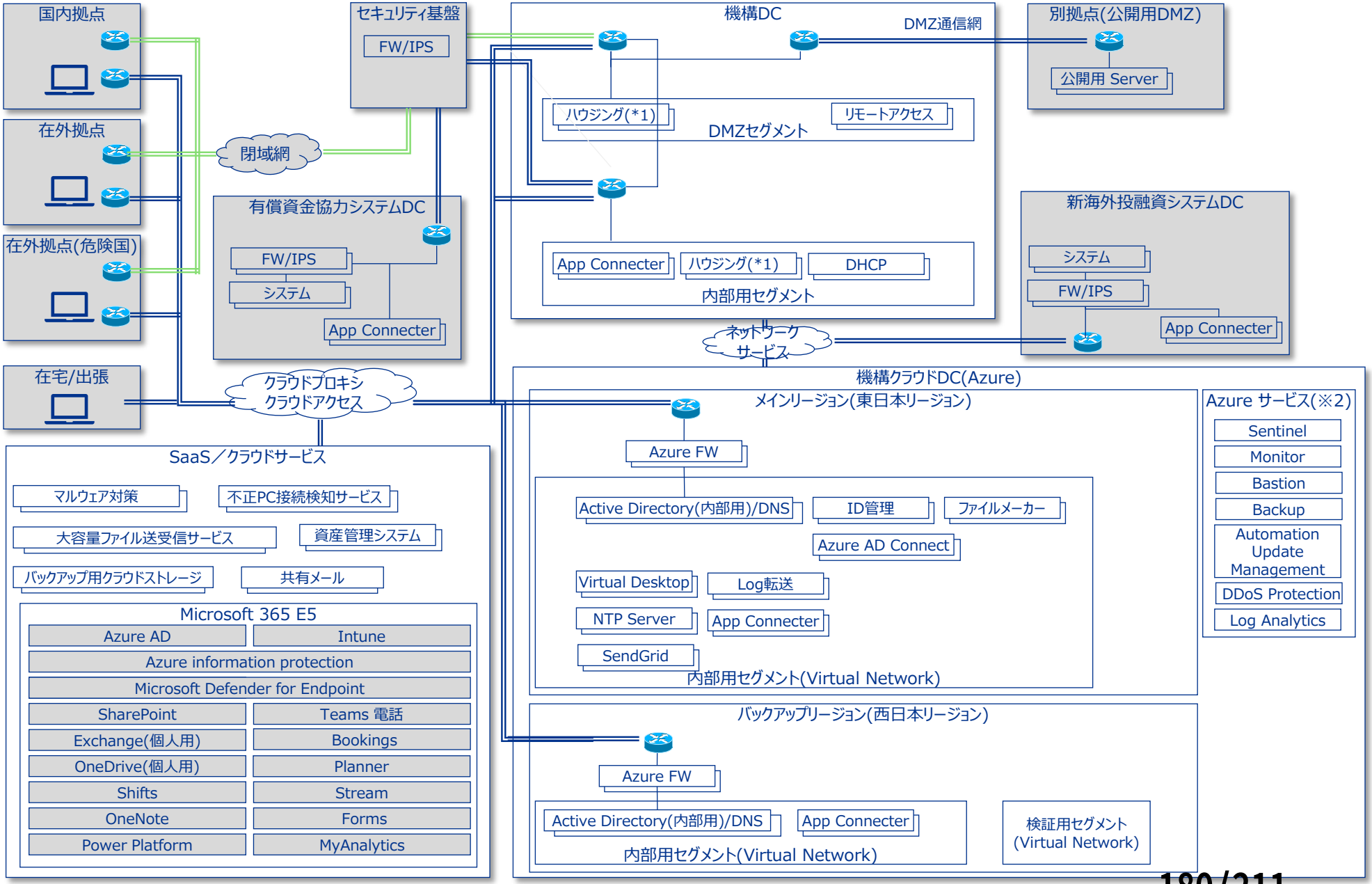
137	構成管理	-	構成情報の収集・維持・他ベンダーへの提供	運用事業者は、変更・リリース管理実施後に必要となった構成変更について、システム第一課、関連事業者から情報を随時収集し、以下のサービスを提供しているシステム全体の構成情報を一元的に、最新の状態で維持・管理する。 ・ハードウェア ・OS ・ミドルウェア ・パッケージソフトウェア ・アプリケーション ・ネットワーク等 上記以外にも、運用事業者が必要と判断した構成情報は維持・管理対象とする。 また、運用事業者は、これらの情報をシステム第一課が必要と判断した際には、必要十分な形で提供する。 なお、運用事業者は、関連事業者側にて実施された変更については、極力最新版を維持するため、定期的に変更の有無及び変動箇所の情報提供を依頼すること。 本部のLANについてはLANの運用事業者にて構成情報を維持・管理するため、最新版の提供のみ求めること。
138	資産管理	-	機構保有又は賃貸借物件の棚卸実施と管理情報と更新	運用事業者は、資産管理ソフト（自動的かつ恒常的に資産管理をできるシステム）を導入し、本部・国内拠点・在外拠点の各種ハードウェアに関する保有情報、賃貸借情報の統一的な管理を行う。管理する情報は製品名、型番、数量に加え、運用事業者にて必要と判断した項目とする。また、システム第一課からの要請により追加される場合がある。 運用事業者は、システム第一課からの要求に応じて管理情報を必要十分な形で随時提供するとともに、ハードウェアの調達、追加、廃棄等の変更が生じた場合、管理情報の更新を行う。また運用事業者は、管理情報と実体情報との整合性を定期的（年1回以上）に確認し、管理情報を適切な状態に維持する。
139	資産管理	-	機構への管理情報の提供	運用事業者は、システム第一課又は機構内他部署からの要求があった場合、要求された資産情報を抽出・整理し、要求元へ提出する。
140	ソフトウェア管理	-	ソフトウェアライセンス管理	運用事業者は、OS、ミドルウェア、パッケージソフトウェアに関するライセンス情報・価格情報を統一的な管理を行う。ここでいう情報とは、「製品名」、「バージョン」、「数量」等を指すが、システム第一課からの要請により追加される場合がある。未使用ライセンスの返却を促しつつ、ソフトウェアライセンス管理を実施すること。また、「いきなりPDF」、「駅すぱーと」に関しては、機構が保有するライセンスをプールし、申請に基づき払い出し／返却の管理を行う。 運用事業者は、システム第一課からの要求に応じて管理情報を随時提供するとともに、パッケージソフトウェアの調達、追加、廃棄等の変更が生じた場合、管理情報の更新を行う。 また運用事業者は、管理情報と実体情報との整合性を定期的（年1回以上）に確認し、管理情報を適切な状態に維持する。
141	ソフトウェア管理	-	機構への管理情報の提供	運用事業者は、システム第一課又は機構内他部署からの要求があった場合、要求されたソフトウェアライセンス情報を抽出・整理し、要求元へ提出する。
142	セキュリティ管理	-	セキュリティインシデント発生時の対応手順の整理	運用事業者は、セキュリティインシデント発生時の対応手順を文書（対応手順書）にて取り纏め、情報システム部に報告する。 また、対応手順書では、対応手順に加えセキュリティインシデントの優先度（緊急度、影響範囲、目標解決時間、等）と優先度ごとの対応方法を定義する。
143	セキュリティ管理	-	セキュリティに係る動向の状況把握	システム改修等を含む、工期がある程度必要なセキュリティに係る動向・改善提案を情報システム部へ提言できるよう、運用業務に関連する最新のセキュリティ動向を常に把握し、必要に応じて情報システム部へ提言すること。

144	セキュリティ管理	-	セキュリティ情報の収集（日次）とセキュリティ脆弱性への対応	日々の運用業務において、運用業務に係る最新のソフトウェア、ハードウェア等及びこれらに影響を与える製品等に関する情報を収集し、早急にセキュリティ対策を実施できるよう、セキュリティ関連の情報を日次で収集する。機構の情報システムに影響を及ぼす可能性がある脅威と判断される情報は情報システム部へ定期的に報告するとともに、パッチ適用や対策の検討を開始すること。また、主な業務システム（※）を対象にしたヒアリング調査を早急に実施し、パッチ適用や対策が必要なものに関しては各保守業者と調整のうえ、対応を依頼し、対応状況を情報システム部へ報告する。 ※調査対象とする業務システムは運用設計時に別途検討する。なお、本部のLANについてはLANの運用事業者にて情報収集を行う。
145	セキュリティ管理	-	新規システムの接続に伴うセキュリティの検討	運用事業者は、新規システムの接続に伴うネットワークの設定変更、またはシステムの外部拠点の増加など、セキュリティ上の影響がある場合に、その影響を洗い出して対策の検討を行う。その結果、セキュリティポリシー等のセキュリティ標準に逸脱している場合は、情報システム部に報告し、改善策の立案し・実施を行う。
146	セキュリティ管理	-	セキュリティ標準の変更に伴う検討	運用事業者は、機構が定めるセキュリティポリシー等のセキュリティ標準に変更が生じた場合、影響範囲の検討及び提案を情報システム部に対して行う。
147	ドキュメントの整備及び管理	-	ドキュメントの整備及び管理	運用事業者は、コンピュータシステム運用全体について、システム第一課や原課、関連事業者との役割分担や業務の流れ等を記述した管理手順に係るドキュメント（運用手順書等）を作成してシステム第一課の承認を得るとともに維持管理を行う。 当該ドキュメントの作成においては、必要に応じてシステム第一課又は関連事業者と調整しつつ整備し、管理手順にてシステム第一課に提示すると定めた運用ドキュメントも同様に、維持管理を行う。 また、運用事業者は、運用管理業務を実施することで蓄積される各サービス項目の業務ノウハウ（引継資料、運用マニュアル、操作手順、資料化されていない業務ノウハウ等）をドキュメントとして整備及び管理し、システム第一課及び原課の要望に応じて提出する。 変更管理の結果、設計書や運用する際に必要な運用関連ドキュメント（資料）についても、常に最新化するように管理すること。 なお、該当ドキュメントのうちマニュアルや手順書については必要に応じて動画での作成を行う。動画の要否については機構と協議すること。
148	全体管理	-	関連事業者含めた全体管理	運用事業者は、全社LAN,WAN,全社PC等機構全体に大きく影響あるシステムにて、関連事業者が別の事業者に変更される場合や機構と関連事業者との契約が更改される場合等においては、システム全体のサービス品質を確保するため、当該変更や契約更改等が円滑に実施され、かつ、運用管理業務の実施、サービスレベルの達成等がなされるよう、運用要件の提示、進捗管理、関連事業者との調整等を行う。 尚、機構の業務系システムについては、本件契約での監視等の業務範囲にかかわらず、最新の状況把握を行うこととし、業務系システムの作業時には、必要に応じて立ち会い等を実施すること。
149	全体管理	-	運用作業スケジュールの管理	運用事業者は、運用事業者自身の作業及びシステム全体の年間・月間等のスケジュールを管理する。 また、システム第一課からのスケジュール変更依頼や、年末年始等長期休暇の作業スケジュールに基づき、年間・月間スケジュール表の変更・追加・削除を行う。また、スケジュールの変更・追加・削除にともなう調整作業も行う。 なお、スケジュールの粒度（年間・月間・週次・日次）は、運用事業者自身の作業及びシステム全体のスケジュールを随時関係者が把握できるように運用事業者において検討すること。
150	全体管理	-	運用事業者自身の工程管理	運用事業者は、作業進捗を確認できる資料（進捗管理表等）を作成し、工程管理を行う。さらに、定期的にリスク・課題管理及び品質管理状況等についてシステム第一課に報告する。 また、スケジュール遅延、品質低下等の事態が発生した場合は、対応策案を作成し、システム第一課に報告するとともに、対応策案の実施を行う。

151	全体管理	-	セキュリティインシデントに係る対応	情報セキュリティの脅威・攻撃の検知、マルウェア検体分析、その他、脆弱性情報の取得等をした際に、対策に必要な調査・分析はCSIRT要員として、全て実施する。その際に、機構のセキュリティの体制と連携し、組織横断的に主体的に解決にあたる。
152	セルフモニタリング	セルフモニタリングの実施	セルフモニタリングの実施	運用事業者は、システム第一課と合意したモニタリング項目に関し、モニタリングに必要なデータの収集方法を検討し、必要に応じた収集のためのツールの整備、日常運用に必要な収集のための運用手順やマニュアルの整備や更新を行うとともに、日常運用においてその実績データを収集、保管する。
153	セルフモニタリング	セルフモニタリングの実施	セルフモニタリング結果の評価と分析	運用事業者は、目標値とモニタリングの結果を比較、達成度合いの評価、過去の達成状況との比較、その傾向の評価を行い、未達成の項目やモニタリング結果が悪化傾向にあるものについてはその原因を分析する。
154	セルフモニタリング	セルフモニタリングの実施	改善案の立案	運用事業者は、モニタリング結果が目標未達成の項目や悪化傾向にあるものについて、改善策を立案し、改善策の実施計画を策定する。
155	セルフモニタリング	セルフモニタリングの実施	セルフモニタリング結果と改善策の報告	運用事業者は、モニタリング結果の目標達成状況と目標未達成の場合の改善策について報告書を作成してシステム第一課へ提出する。 目標達成状況はモニタリング項目毎に運用事業者としての自己評価を記載し、システム第一課に提示する。システム第一課にて最終評価を検討・決定する。評価の結果、ペナルティが発生する場合等は予め定めたペナルティまたはモニタリング項目に記載するルールに従うこととする。 また、改善計画の実施に当たって、関連事業者の支援が必要な場合は、運用事業者はシステム第一課にその旨を報告し、関連事業者に改善策の実施を依頼するとともに、改善策の実施状況を把握する。運用事業者は、改善策の実施状況をモニタリング結果達成状況の報告書に含めてシステム第一課へ提出する。 なお、報告書作成及び報告のタイミングについては「別添7_モニタリング項目案」を参考に、システム第一課と協議の上決定する。
156	セルフモニタリング	モニタリング項目一覧及び合意書の維持管理（運用フェーズ）	サービス要件の見直しと把握	システム第一課は、運用業務の業務範囲等及び運用対象とするシステムを運用事業者に提示する。 運用事業者は、システム第一課及び原課のモニタリング項目の改善要望に対し、要望の実現可能性を検討し、実現のために必要なシステム資源及び作業量の概算見積もりを行い、システム第一課に提示する。 運用事業者は、システム第一課と協議の上、運用業務の業務範囲と運用対象システムを定義する。 なお、サービス要件の見直し時期は年次に加え、システム第一課又は運用事業者が必要と判断したタイミングとする。
157	セルフモニタリング	モニタリング項目一覧及び合意書の維持管理（運用フェーズ）	モニタリング項目の見直し	運用事業者は、業務の範囲と対象システムに対して、提供する支援業務の品質を客観的に評価できる指標となるモニタリング項目を検討し、システム第一課に提示する。 システム第一課は、運用事業者と協議し、次年度の業務の範囲と運用対象システムに対するモニタリング項目を決定する。
158	セルフモニタリング	モニタリング項目一覧及び合意書の維持管理（運用フェーズ）	モニタリング項目の目標値の見直し	運用事業者は、システム第一課との協議により設定したモニタリング項目に対して、システム第一課及び原課からの要望、システムの特性や過去の実績を加味し、運用事業者が達成すべき数値目標を検討し、モニタリング項目の目標値としてシステム第一課へ提示する。 システム第一課は、運用事業者と協議して、モニタリング項目ごとに目標値を設定する。
159	セルフモニタリング	モニタリング項目一覧及び合意書の維持管理（運用フェーズ）	サービスレベルの合意	運用事業者は運用業務範囲、運用対象システム、モニタリング項目、目標値、ポイント精算ルールなどの前提条件等の運営ルールを記載した合意書を作成し、機構と取り交わす。

更改後~2025年3月末まで　システム概要構成図（案）

凡例：　新規構築　継続利用または構築対象外

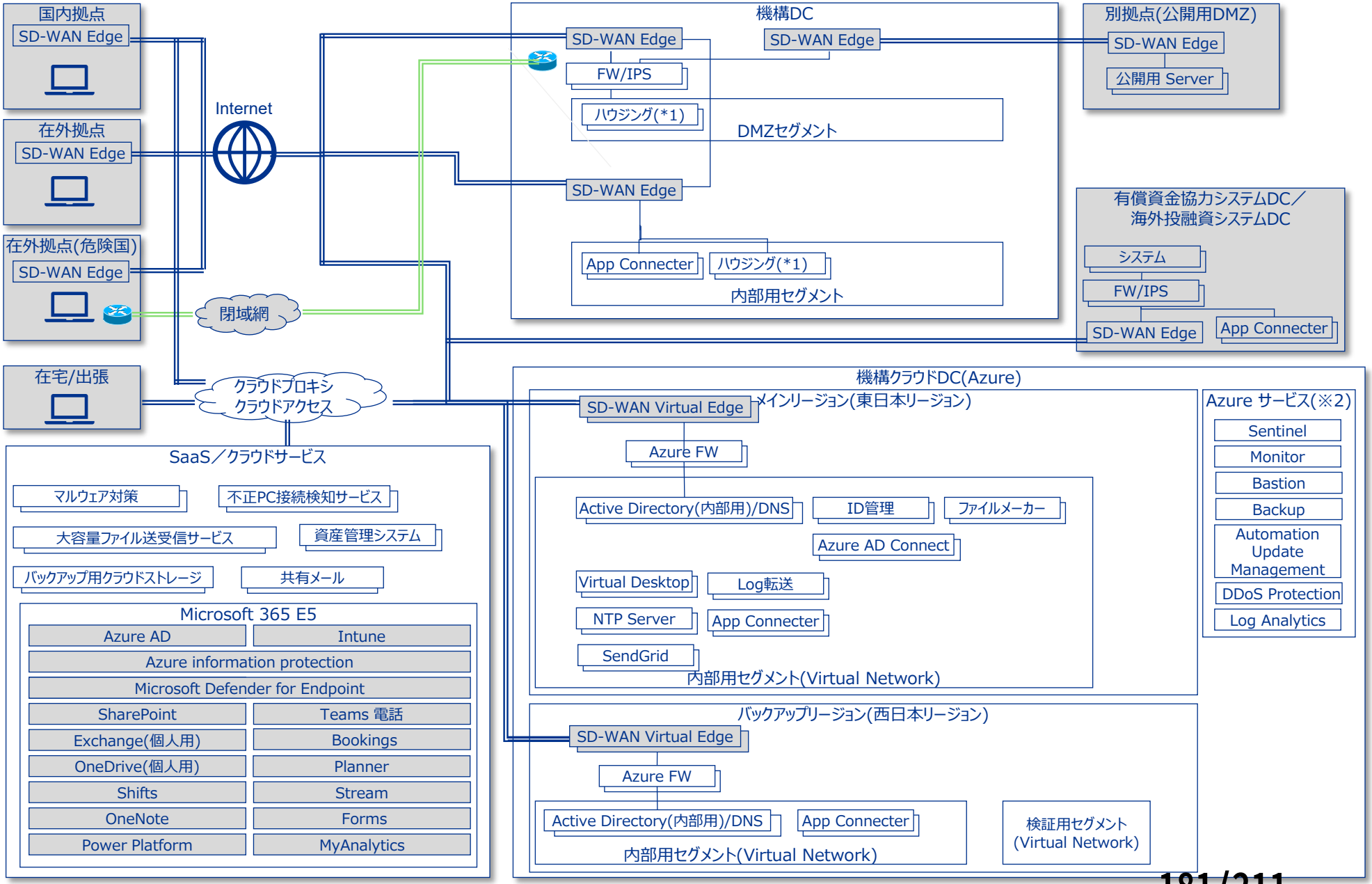


※1　ハウジング上のシステムについては別添「ハウジング対象システム一覧.xlsx」を参照

※2　記載しているサービスは案であり、要件を満たすものであれば別のサービスでの提案も可とする

2025年4月以降　システム概要構成図（案）

凡例：　新規構築　継続利用または構築対象外



※1　ハウジング上のシステムについては別添「ハウジング対象システム一覧.xlsx」を参照

※2　記載しているサービスは案であり、要件を満たすものであれば別のサービスでの提案も可とする

独立行政法人 国際協力機構
コンピュータシステム運用等業務

別添7_モニタリング項目案

No	更新日	更新者	承認者	更新内容	バージョン

モニタリング		
基本的な考え方		
	基本方針	システム運用等要件ごとに機構が期待する付加価値（品質）を提供できているかのサービスレベルの達成状況を管理するためのモニタリング項目を設定し、定期的に受注者がその達成度を自己評価（セルフモニタリング）し、機構へ報告する。機構はその報告内容を評価し、最終的な達成度を決定する。目標が達成できなかった項目についてはその未達成度合によりペナルティポイントが課され、一定のポイントが累積した時点で減額対象となる。また、受注者が独自に追加アウトプットを提案・報告し、その有効性を機構も評価した場合には、評価ポイントを付与し、ペナルティポイントの相殺に使用することを認める。 受注者は、運用設計時にモニタリング項目等を確認・精査し、機構と協議の上モニタリング項目及びサービスレベルの管理手順を確立させること。なお、セルフモニタリング業務の流れ、追加モニタリング項目、モニタリング項目の要求値の引き上げのタイミング、その実施方法について提案すること。
モニタリング開始日		
	開始日	次期コンピュータシステム運用等業務（運用フェーズ）の開始日からとする。
モニタリングタイミング		
	四半期	受注者は、サービスレベルの達成状況をチェック（セルフモニタリング）し、問題があれば運用等業務の改善を実施する。そのセルフモニタリング結果を機構と協議し、サービスレベルの達成状況を共有（機構より達成状況の判断について説明の場を設定するが、最終判断は機構で行う）する。
	年次	受注者は、セルフモニタリング結果を含む実施した運用等業務が機構における効率的な業務の遂行の実現にどの程度貢献しているかの評価を実施し、その評価の結果問題があれば運用等業務の改善を実施する。その結果を機構と協議し、目標の達成状況を共有（機構より達成状況の判断について説明の場を設定するが、最終判断は機構で行う）する。
評価ポイント／ペナルティポイント		
	定量的な評価	（目標達成）／（目標未達成）⇒影響度によりポイント設定
	定性的な評価	S（要求以上の付加価値（品質））⇒評価ポイント＋1 A（要求通りの付加価値（品質）） B（要求未満（適切な再発防止措置が講じられている））⇒ペナルティポイント＋1 C（要求未満（適切な再発防止措置が講じられていない））⇒ペナルティポイント＋2 D（要求未満（調達仕様書の非遵守））⇒ペナルティポイント＋5 E（要求未満（機構のサービス提供・事業継続に影響を及ぼす重大な問題あり））⇒ペナルティポイント＋50
	評価ポイントの有効期限	ポイントの有効期限はポイント確定から1年間（翌年の同一四半期まで持ち越し）とする。
	評価ポイントの換算	ペナルティポイントは四半期ごとに支払いを確定させる時点で、累積で20ポイントを超過していた場合に超過したポイントについて換算するものとする。四半期ごとの支払時期が到来した時点で、その時点のペナルティポイントと評価ポイントを集計し、以下の計算式による減額金を、その時点の支払額から減額する。なお、ポイントの換算は、古いポイントから順に行う。 【減額金計算式（20ポイント超過分）】 ［減額金］＝｛［ペナルティポイント］－［評価ポイント］｝　×　10万円

システム運用業務全般（システム運用業務全般に対する運用状況のモニタリング）

基本事項

No	モニタリング項目	測定方法	評価	要求値	報告タイミング	ペナルティポイント	評価ポイント
1	調達仕様書・提案書記載事項に準じた運用業務の品質	「機構の求めるシステム運用業者・運用業務」の考え方を踏まえて実施した運用業務全体の品質に係る自己評価の報告、及び調達仕様書・提案書の遵守状況に関する報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・運用業務全体において提供された付加価値（品質）	S：機構にとって有益な対応および能動的な業務改善の提案・実施・効果があった場合 A：適切な運用業務ができている B：運用業務はできているものの要求を満たしていない C：運用業務ができていない（改善策が実施できていない）※四半期 D：要求未満（調達仕様書の非遵守） E：要求未満（機構のサービス提供・事業継続に影響を及ぼす重大な問題あり）	A	四半期	B：1点 C：2点 D：5点 E：50点	S:1点
2	本業務のサービスレベル管理の考え方を理解した上で実施した運用業務の品質	「本業務のサービスレベル管理の考え方」を踏まえて実施した運用業務のサービスレベル管理の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・モニタリング全体において提供された付加価値（品質） ・機構運用業務のPDCAサイクルにおける業務の改善状況	S：機構にとって有益な対応および能動的な業務改善の提案・実施・効果があった場合 A：適切な運用業務ができている B：運用業務はできているものの要求を満たしていない C：運用業務ができていない（改善策が実施できていない）	A	四半期	B：1点 C：2点	S:1点
3	運用業務上必要となる機構とのコミュニケーションの品質	「機構における運用業務の役割分担・責任範囲」を踏まえて実施した打ち合わせ等の運用業務上必要なコミュニケーションの品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・コミュニケーションのタイミング ・コミュニケーションの内容・方法 ・コミュニケーションにより提供された付加価値（品質）	S：機構にとって有益な情報発信および能動的なコミュニケーションがとれていた場合 A：適切なコミュニケーションおよび報告ができている B：コミュニケーションおよび報告はしているものの要求を満たしていない C：コミュニケーションおよび報告を実施していない	A	四半期	B：1点 C：2点	S:1点
4	運用に係る工程管理業務の品質	運用業務の工程管理（状況調査・把握、スケジュール管理）の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質） ・工程遅延の有無	S：能動的な管理業務の効率化・改善を実施および効果があった場合 A：適切な管理業務ができている B：管理業務はできているものの要求を満たしていない C：管理業務ができていない	A	四半期	B：1点 C：2点	S:1点

機構内・在外利用者向けヘルプデスク							
5	呼損率、一次窓口解決率、回答目標時間遵守率（定量的項目）	問合せに係る定量的（呼損率・一次窓口解決率・回答目標時間遵守率）な個々のサービスレベル目標値の達成状況で評価を実施する。 【算出式】 ・呼損率＝とることができなかった電話の本数/かかってきた電話の本数 ・一次窓口解決率＝一次窓口解決件数/総問い合わせ件数 （ヘルプデスク内での回答のみで、ユーザからの質問事項が完了した場合） ・回答目標時間遵守率＝回答目標時間遵守件数/総問い合わせ件数 （ヘルプデスクでの問い合わせ受付から完了までの経過時間）	【SLA基準】 ・呼損率：10%未満 ・一次窓口解決率：80%以上 ・回答目標時間遵守率：80%以上 A：全てSLA基準達成 C：要求未満（何れか1つでもSLA基準をクリアできていない）	A	四半期	C：2点	−
6	一次窓口で実施した、問い合わせ切り分けと回答作業の品質	問い合わせ内容の切り分け、一次窓口解決・回答の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質） ・クレームの件数	S：機構にとって有益な対応および能動的な業務改善の提案・実施・効果があった場合 A：適切な運用業務ができている B：運用業務はできているものの要求を満たしていない C：運用業務ができていない（改善策が実施できていない）	A	四半期	B：1点 C：2点	S:1点
7	二次担当者以降が実施した、問合せの解決と内容確認作業の品質	二次担当者以降による解決内容確認、及びクライアントPCリモート対応の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・二次担当者以降にエスカレーションした問合せ件数 ・クライアントPCに係る問題をリモート対応をした件数 ・提供された付加価値（品質） ・クレーム発生後の対処および報告（品質）	S：機構にとって有益な対応および能動的な業務改善の提案・実施・効果があった場合 A：適切な運用業務ができている B：運用業務はできているものの要求を満たしていない C：運用業務ができていない（改善策が実施できていない）	A	四半期	B：1点 C：2点	S:1点
8	ヘルプデスクから利用者に対する情報伝達（対応進捗状況、障害情報、保守スケジュール、サービス内容等）作業の品質	利用者に対するサービス内容・障害に係る情報伝達の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な情報発信および能動的なコミュニケーションがとれていた場合 A：適切なコミュニケーションおよび報告ができている B：コミュニケーションおよび報告はしているものの要求を満たしていない C：コミュニケーションおよび報告を実施していない	A	四半期	B：1点 C：2点	S:1点

9	問い合わせ記録分析による利用者要望の整理を実施した作業の品質	問い合わせ記録分析による利用者要望の整理を実施した作業のプロセスとそれによるアウトプットの品質に係る自己評価の報告を運用事業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な分析・改善策の立案および実施・効果があった場合 A：適切な分析および改善策の立案ができている B：分析および改善策が立案できているものの要求を満たしていない C：分析および改善策が立案できていない	A	四半期	B：1点 C：2点	S:1点
10	問い合わせ対応状況に関する報告を実施した作業の品質	問い合わせ対応状況に関する報告を実施した作業のプロセスとそれによるアウトプットの品質に係る自己評価の報告を運用事業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な情報発信および能動的なコミュニケーションがとれていた場合 A：適切なコミュニケーションおよび報告ができている B：コミュニケーションおよび報告はしているものの要求を満たしていない C：コミュニケーションおよび報告を実施していない	A	四半期	B：1点 C：2点	S:1点
11	現地サポート満足度（定量的項目）	国内・在外における現地サポート満足度についてサービスレベル目標値の達成状況で評価を実施する。 【算出式】 ・国内サポート ・在外サポート 上記の2項目に関して、個々に以下の算出式で評価する。 現地サポート満足度＝アンケートの各項目結果の合計得点/アンケート評価の満点×回答数 【算出式における現地サポートに満足した職員の数の測定方法】 国内・在外共に、サポート満足度調査にて、各項目を5段階評価（満足・やや満足・普通・やや不満・不満）で調査を実施する。アンケート評価の総得点とは、調査項目が10項目だった場合、10項目×5（全項目が満点）とし、アンケート評価結果の総和は、各項目の評価点を合算したものを指す。	【SLA基準】 ・国内80%以上 ・在外80%以上 A：全てSLA基準達成 C：要求未満（何れか1つでもSLA基準をクリアできていない）	A	四半期	C：2点	－
12	現地サポート作業の品質	国内・在外における現地サポート（在外IT支援出張については、IT環境診断、改善提案の実施を含む）の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な作業支援および能動的な改善策立案・実施・効果があった場合 A：適切な支援業務ができている B：支援業務ができているものの要求を満たしていない C：支援業務ができていない	A	四半期	B：1点 C：2点	S:1点

全体管理								
	13	関係ベンダーを含めた全体管理作業の品質	関係ベンダーを含めた全体管理の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：能動的な管理業務の効率化・改善を実施および効果があった場合 A：適切な管理業務ができている B：管理業務はできているものの要求を満たしていない C：管理業務ができていない	A	四半期	B：1点 C：2点	S:1点
	14	セキュリティインシデント発生の際に対応した作業の品質	機構全体で対応が必要なセキュリティインシデントが発生した場合、機構のセキュリティの体制と連携し、組織横断的に主体的に解決にあたる。このプロセスとアウトプットの品質に係る自己評価の報告を運用事業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：運用業務範囲に係らず機構全体に対して、速やか且つ能動的に解決策実施および機構にとって有効な再発防止策の提案・実施があった場合 A：速やか且つ能動的に調査・分析および解決策実施ができている B：解決策実施はできているものの、調査・分析ができていない C：セキュリティインシデントへの対応ができていない	A	四半期	B：1点 C：2点	S:1点
セキュリティ管理と運用								
	15	セキュリティに係る動向の状況調査・把握作業の品質（定量的項目）	機構ITに関するセキュリティに係る動向の収集作業（状況調査・分析）の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 また、脆弱性情報の収集（受領）から目標時間内に状況を調査し、影響範囲を把握し、対象システムの担当者に連絡する。影響がある場合、自システムについては対応に着手する。 【目標時間】 脆弱性情報の収集（受領）後、1営業日以内（情報収集後、翌営業日）に対象システムへ連絡 【算出式】 目標時間内で情報展開した脆弱性の件数/脆弱性情報の全量	【SLA基準】 A：80%以上 C：80%未満 ※備考　対応時間：9:00～18:00 18時以降および夜間・休祝日は除く	A	四半期	C：1点	－
	16	新規システムの接続に伴うセキュリティの検討作業の品質	運用業者より、新規システムの接続に伴うセキュリティの検討作業の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な対応および能動的な業務改善の提案・実施・効果があった場合 A：適切な運用業務ができている B：運用業務はできているものの要求を満たしていない C：運用業務ができていない（改善策が実施できていない）	A	四半期	B：1点 C：2点	S:1点

	17	目標時間内で対応開始・解決されたインシデント比率（定量的項目）	目標時間内に対応開始として適切な初動が実施できた・解決されたインシデント比率のサービスレベル目標値の達成状況で評価を実施する。 【目標時間】 ①目標対応開始時間：インシデント検知を確認後、1時間以内に対象ユーザへ連絡、ネットワーク遮断などの適切な対処を実施。※ ②目標解決時間：ログ取得後、一週間以内（ログ取得日の翌日から5営業日以内）にユーザへ結果連絡。但し、緊急を要するものは別途内容により目標時間を都度定める。 【算出式】 ①目標時間内対応開始率＝目標時間内で対象ユーザへ連絡且つ適切な初動を実施できたセキュリティインシデント件数/総セキュリティインシデント件数 ②目標時間内解決率＝目標時間内で解決されたセキュリティインシデント件数/総セキュリティインシデント件数 【インシデント対象】 相関分析、ユーザ申告等をトリガーとして、検知した不審PC／各種機器の不審な動作	【SLA基準】 A：80%以上 B：80%未満 ※1 対応時間：9:00～18:00（平日）18時以降および夜間・休祝日は除く 但し、同時インシデント検知が下記の場合、超過分は対象外とする。 ・同一事象による同時インシデント件数：10件/時 ・異なる事象による同時インシデント件数：4件/時	A	四半期	B：1点	－
	18	セキュリティに係る脅威の状況調査・分析作業の品質	セキュリティインシデント対応と、アクセスログ管理の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な調査・分析および分析結果をもとに能動的な対策の提案・実施・効果があった場合 A：適切な調査および分析ができている B：調査および分析ができているものの要求を満たしていない C：調査および分析を実施していない	A	四半期	B：1点 C：2点	S:1点
障害管理								
	19	ユーザからの障害申告の受付、切り分け、応急措置と障害の記録作業の品質	利用者からの障害申告の受付、障害発生箇所の切り分け、応急措置の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な対応および能動的な業務改善の提案・実施・効果があった場合 A：適切な運用業務ができている B：運用業務はできているものの要求を満たしていない C：運用業務ができていない（改善策が実施できていない）	A	四半期	B：1点 C：2点	S:1点

		20	アラート検知による機構及び関係ベンダーへの通報と記録作業の品質	アラート検知による障害について、運用業者より機構及び関係ベンダーへの通報作業の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質） 【評価対象システム】 ・機構クラウドDC(バックアップリージョン)に係るシステム・運用を含む	S：機構にとって有益な情報発信および能動的なコミュニケーションがとれていた場合 A：適切なコミュニケーションおよび報告ができている B：コミュニケーションおよび報告はしているものの要求を満たしていない C：コミュニケーションおよび報告を実施していない	A	四半期	B：1点 C：2点	S:1点
		21	通報時間遵守率（業務アプリ、基盤システム）（定量的項目）	機構業務システム、及び基盤システム障害に係る個々の通報時間遵守率のサービスレベルの目標値の達成状況で評価を実施する。 【算出式】 ・業務システム，基盤システム個々に以下の通り評価する。 通報時間遵守率＝通報時間遵守件数/障害発生件数	【SLA基準】 ・業務アプリ90%以上 ・基盤システム90%以上 A：全てSLA基準達成 C：要求未満（何れか1つでもSLA基準をクリアできていない）	A	四半期	C：2点	－

問題管理								
	22	障害時の報告・対応状況・ユーザ影響および障害原因となる問題対応状況の追跡・報告の品質	報告の妥当性、障害回復までの対応状況、障害影響、原因分析および再発防止策の実施状況で評価 ただし、製品ベンダによる再発防止策の回答待ちの場合、評価は暫定とし、持ち越しの評価期間は対象月から翌々月までとする 【評価観点】 ・提供された付加価値（品質） 【評価対象システム】 ・機構クラウドDC(バックアップリージョン)に係るシステム・運用を含む	S：事前の情報収集等で対策を提案しその導入により3か月に渡り、安定したサービスを提供できている A：下記すべてを満たす場合 ・適切な報告および復旧までの対応 ・迅速に適切な再発防止策が講じられている ・サービス品質に大きな支障をきたしていない B：適切な再発防止策が講じられているものの、サービス品質に支障をきたした場合、もしくは報告および復旧までの対応が劣っている場合 C：下記のいずれかに該当する場合 ・再発防止策が講じられていない ・短期間の間に、同一障害を頻発させた場合 ・サービス品質に大きな支障をきたした場合 ただし、製品ベンダに適時適切な働きかけを行った結果、下記の正式回答があった場合は免除とする。（いかなる場合においても、可能な限り再発防止に向けた運用対処などは実施する） ・障害原因が不明であるため、再発防止策の提示を受けられない場合、C評価は免除とする。 ・再発防止策の提示はあるが、機構の判断により適用しない方針となった場合、同原因にて障害が再発してもB,C評価は免除とする。	A	四半期	B：1点 C：2点	S:1点
	23	可用性改善計画の立案・実行と報告作業の品質	可用性改善計画の立案・実行と報告の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な分析・改善策の立案および実施・効果があった場合 A：適切な分析および改善策の立案ができている B：分析および改善策が立案できているものの要求を満たしていない C：分析および改善策が立案できていない	A	四半期	B：1点 C：2点	S:1点
変更管理								
	24	変更内容が原因の障害発生率（定量的項目）	変更内容が原因の障害発生率のサービスレベル目標値の達成状況で評価を実施する。 【算出式】 障害発生件数/システム変更実施件数	【SLA基準】 A：10%未満 C：10%以上	A	四半期	C：2点	－

可用管理							
25	可用性（稼働率）（定量的項目） （システムごとに主機能の大部分が、稼働が記載されている全時間のうち正常に稼動している時間の割合）	システム停止時間のサービスレベル目標値の達成状況で評価を実施する。 ただし、製品不具合により障害が発生し、製品ベンダからの再発防止策の提示待ちの場合、その期間は暫定評価とする。 【算出方法】 (システム稼動時間－システム停止時間の積上げ）/システム稼動時間 ※システムの重要度に応じて、システムごとに目標値を設定することを想定	【SLA基準】 A：99.9%以上 C：99.9%未満 ただし、製品ベンダに適時適切な働きかけを行った結果、下記の正式回答があった場合は免除とする。（いかなる場合においても、可能な限り再発防止に向けた運用対処などは実施する） 製品不具合による原因で障害が発生し、製品ベンダから提示された再発防止策はあるが、機構の判断により適用しない方針となった場合、稼働率99.9%未満となってもC評価は免除とする。	A	四半期	C：2点	－
26	障害回復実績データの取り纏め等の可用性データの収集分析と可用性改善策の立案と報告の品質	障害回復実績データの取り纏め等の可用性データの収集分析と可用性改善策の立案と報告の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な分析・改善策の立案および実施・効果があった場合 A：適切な分析および改善策の立案ができている B：分析および改善策が立案できているものの要求を満たしていない C：分析および改善策が立案できていない	A	四半期	B：1点 C：2点	S:1点
性能管理							
27	応答時間遵守率 （主機能のトランザクションの応答時間を複数回測定し、応答時間の目標値を遵守できたトランザクションの割合をシステムごとに算出）	システムの応答時間のサービスレベル目標値の達成状況で評価を実施する。 【算出方法】 システム応答時間の目標値を遵守できたトランザクション数／総トランザクション数 ※システムの重要度に応じて、システムごとに目標値を設定することを想定 ※目標値は仮設定とし、ユーザからのアクセスが本格化した時点で最終確定とする ※計測方法、条件等は運用設計時に決定する	【SLA基準】 A：60%以上 C：60%未満	A	四半期	C：2点	－
28	実測値データの取得、分析と改善策の立案作業の品質	実測値データの取得と分析、及び性能改善計画の立案と実行（必要に応じて見直しも含む）の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な分析・改善策の立案および実施・効果があった場合 A：適切な分析および改善策の立案ができている B：分析および改善策が立案できているものの要求を満たしていない C：分析および改善策が立案できていない	A	四半期	B：1点 C：2点	S:1点

機構ITシステム/インフラに係る導入・開発・改善の状況把握・提言							
29	【全体IT戦略・企画支援】 機構全体のITシステム/インフラ等に係る基本方針の策定に対する提言や施策推進に対する支援業務の品質	機構ITにおける、個別システム、及びインフラの企画フェーズに関する提言の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な作業支援および能動的な改善策立案・実施・効果があった場合 A：適切な支援業務ができている B：支援業務ができているものの要求を満たしていない C：支援業務ができていない	A	四半期	B：1点 C：2点	S:1点
30	【個別企画支援】 個別システム/インフラ基盤の企画フェーズに係る提言・支援業務の品質	機構ITにおける、個別システム、及びインフラの企画フェーズに関する提言の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な作業支援および能動的な改善策立案・実施・効果があった場合 A：適切な支援業務ができている B：支援業務ができているものの要求を満たしていない C：支援業務ができていない	A	四半期	B：1点 C：2点	S:1点
31	【個別実行支援】 ITコンシェルジュが行う個別システム/インフラの実行フェーズに係る提言・支援業務の品質	ITコンシェルジュが行う業務の内、機構ITにおける、個別システム、及びインフラの実行フェーズに関する支援の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な作業支援および能動的な改善策立案・実施・効果があった場合 A：適切な支援業務ができている B：支援業務ができているものの要求を満たしていない C：支援業務ができていない	A	四半期	B：1点 C：2点	S:1点
32	【個別実行支援】 ヘルプデスクが行うITシステム/インフラ（主にサーバ側）の運用等に係る提言・支援業務の品質	ヘルプデスクが行う業務の内、機構ITにおける、個別システム、及びインフラの実行フェーズに係る支援の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な作業支援および能動的な改善策立案・実施・効果があった場合 A：適切な支援業務ができている B：支援業務ができているものの要求を満たしていない C：支援業務ができていない	A	四半期	B：1点 C：2点	S:1点
33	【個別実行支援】 ヘルプデスクが行うPC等のクライアント端末の運用等に係る提言・支援業務の品質	ヘルプデスクが行う業務の内、機構ITにおける、クライアント端末に関する支援の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な作業支援および能動的な改善策立案・実施・効果があった場合 A：適切な支援業務ができている B：支援業務ができているものの要求を満たしていない C：支援業務ができていない	A	四半期	B：1点 C：2点	S：1点

ユーザ満足度							
34	利用者満足度	利用者満足度のサービスレベル目標値の達成状況で評価を実施する。 【算出式】 利用者満足度＝満足・やや満足と回答のあった項目の総数/回答のあった項目の総数 ※対象となるのは、必須回答とした項目とする。 【算出式における”システムを利用して満足した職員の数の測定方法”】 利用者満足度調査にて、原則4段階評価（満足・やや満足・やや不満・不満）の調査を実施する。	A：70%以上 C：70%未満	A	年次	C：2点	－
35	利用者満足度結果の分析を実施した作業の品質	利用者満足度結果の分析、及び運用業務の改善策の立案の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な分析・改善策の立案および実施・効果があった場合 A：適切な分析および改善策の立案ができている B：分析および改善策が立案できているものの要求を満たしていない C：分析および改善策が立案できていない	A	年次	B：1点 C：2点	S:1点
36	研修の実施回数、参加者評価（定量的項目）	研修の実施回数・参加者評価の個々のサービスレベル目標値の達成状況で評価を実施する。 【算出方法】 ・研修実施回数の積上げ ・参加者評価＝アンケートの各項目結果の合計得点/（アンケート評価の満点×有効回答数） 【算出式における研修に参加して満足した職員の数の測定方法】 参加者評価調査にて、各項目を5段階評価（例：満足・やや満足・普通・やや不満・不満）で調査を実施する。「アンケート評価の満点」とは、調査項目が10項目だった場合、10項目×5点（全項目が”満足”）を選択とし、「アンケートの各項目結果の合計得点」とは、各調査項目の評価点を合算したものを指す。	【SLA基準】 ・年度内の実施回数16回以上 ・参加者評価70%以上 S：研修の累積参加者評価が85%以上 A：全てSLA基準達成 C：要求未満（何れか1つでもSLA基準をクリアできていない）	A	年次 ※原則として年次で評価を行うが、機構にとって大きな効果があったと判断できる場合は四半期で評価を行う。	C：2点	S：1点

37	研修後のアンケート結果から分析と改善策の立案作業の品質	研修後アンケート結果の取得と分析、及び次回研修に向けての改善計画の立案・実行の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な分析・改善策の立案および実施・効果があった場合 A：適切な分析および改善策の立案ができている B：分析および改善策が立案できているものの要求を満たしていない C：分析および改善策が立案できていない	A	年次	B：1点 C：2点	S：1点
セルフモニタリングの実施と維持管理							
38	セルフモニタリングの結果の評価、分析、改善と報告作業の品質	セルフモニタリング結果報告において信頼性のある根拠をもとに評価、分析、改善案の立案及びそれぞれの報告実施の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な分析・改善策の立案および実施・効果があった場合 A：適切な分析および改善策の立案ができている B：分析および改善策が立案できているものの要求を満たしていない C：分析および改善策が立案できていない	A	四半期	B：1点 C：2点	S:1点
39	セルフモニタリング項目、サービス要件、SLAの見直し作業の品質	サービス要件・項目・目標値の見直しの品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な分析・改善策の立案および実施・効果があった場合 A：適切な分析および改善策の立案ができている B：分析および改善策が立案できているものの要求を満たしていない C：分析および改善策が立案できていない	A	年次	B：1点 C：2点	S:1点
監査（内部・外部）対応							
40	セキュリティ監査、システム監査に対するデータと資料の提供と指摘事項への対応を実施した作業の品質	監査（セキュリティ、システム）に対するデータと資料の提供と指摘事項への対応の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。 【評価観点】 ・提供された付加価値（品質）	S：機構にとって有益な作業支援および能動的な改善策立案・実施・効果があった場合 A：適切な支援業務ができている B：支援業務ができているものの要求を満たしていない C：支援業務ができていない	A	四半期	B：1点 C：2点	S:1点

		41	BCP訓練における計画・実施・評価の品質	BCP訓練における計画・実施・評価の品質に係る自己評価の報告を運用業者より受け、機構が評価を実施する。なお、評価の対象範囲としてはBCP訓練当日の前後に含まれる作業も包含して評価する。 【評価観点】 ・提供された付加価値（品質） 【評価対象システム】 ・バックアップデータセンタへの切替に係るシステム・運用のみを評価対象とする	S：機構にとって有益な対応および能動的な業務改善の提案・実施・効果があった場合 A：適切な運用業務ができている B：運用業務はできているものの要求を満たしていない C：運用業務ができていない（改善策が実施できていない）	A	年次	B：1点 C：2点	S:1点

「国際協力機構コンピュータシステム運用等業務」

評価基準書

令和 5 年（2023 年）

独立行政法人国際協力機構

第１ はじめに

本評価基準書は、「国際協力機構コンピュータシステム運用等業務」の受託者を適切に選定するための審査方法をとりまとめものである。

第２ 評価方法

受託者の選定にあたっては、「情報システムの調達に係る総合評価落札方式の標準ガイドライン」に基づき、予定価格の制限範囲内の価格をもって有効な入札を行った者のうち、入札価格及び事業者の幅広い能力･ノウハウ等の技術力を総合的に評価して落札者を決定する、総合評価落札方式によって行う。

総合評価は、価格点（入札価格の得点）に技術点（評価項目一覧表に基づく得点）を加えて得た数値（以下「総合評価点」という。）をもって行う。なお、技術評価点が５０%、つまり２００点満点中１００点（「基準点」という。）を下回る場合を不合格とする。不合格となった場合は、「（１４）技術提案書の評価結果の通知」に記載の手続きに基づき、不合格であることが通知され、入札会には参加できない。また、WLB 等推進企業（女性活躍推進法、次世代育成支援対策推進法、青少年の雇用の促進等に関する法律に基づく認定企業や、一般事業主行動計画策定企業）への評価については、「評価項目一覧表」を参照。

価格点と技術点の配点

総合評価点　＝　価格点（100 点満点）　＋　技術点（200 点満点）

第３ 価格点の評価方法

価格点は、入札価格を予定価格で除して得た値を１から減じて得た値に入昨価格に対する特典配分を乗じて得た値とする。

価格点＝（　1－　入札価格　÷　予定価格　）×　100 点

第４ 技術点の評価方法

技術提案書について、評価項目一覧表に基づき、評価を行う。なお、以下の評価基準及び配点に基づき点数化する。

技術点　＝　200 点　満点とする

１ 評価基準

評価項目一覧表に示す「評価基準（視点）」及び「技術提案書にあたっての留意事項」の視点から以下に記載する当該項目の評価ランクにより評価を行い、ランクに応じ、次節「２ 配点」に定める技術点を付与する。

表 １－１ 当該項目の評価に係る評価点

当該項目の評価	評価点
当該項目については極めて優れており、高い付加価値がある業務の履行が期待できるレベルにある。	９０％以上
当該項目については優れており、適切な業務の履行が十分期待できるレベルにある。	９０％未満 ８０％以上
当該項目については一般的な水準に達しており、業務の履行が十分できるレベルにある。	８０％未満 ７０％以上
当該項目については必ずしも一般的なレベルに達していないが、業務の履行は可能と判断されるレベルにある。	７０％未満 ５０％以上
当該項目だけで判断した場合、業務の適切な履行が困難であると判断されるレベルにある。	５０％未満

２ 配点

配点は以下のとおり。

（１） 業務の具体的な実現方法に係る評価

業務の具体的な実現方法に係る評価については、評価項目一覧表の各項目について、「１．評価基準」に応じて配点に技術点を付与する。

（２） 受託者に望まれる経験・能力等、および業務実施体制に係る評価

受注者に望まれる経験・能力等、および業務実施体制に係る評価については「１．評価基準」に応じて配点に技術点を付与する。

第５ その他

落札者の決定、落札者決定の取り消し、落札者が決定しない場合の措置等に関しては、

別途「(独)国際協力機構コンピュータシステム運用等業務民間競争入札実施要項」にて定める通りとする。

以上

別紙：評価項目一覧表

評　価　表（評価項目一覧表）

評価項目	評価基準（視点）	配点	技術提案書作成 にあたっての留意事項
1．社としての経験・能力等		**6**	業務を受注した際に適切かつ円滑な業務が実施できることを証明するために参考となる、応札者の社としての類似業務の経験、所有している資格等について、記載願います。
（１） 類似業務の経験	・基盤系サービスの設計開発実績：基盤系サービスの設計開発またはサービス提供業務に関し、過去5年間で3件以上の実績を有しているか。 ・基盤系サービスの運用管理実績：基盤系サービスおよび業務系システムの運用管理業務に関し、過去5年間で3件以上の実績を有しているか。 ・データセンタの移行実績：データセンタの移行作業に関し、過去5年間で3件以上の実績を有しているか。 ・情報セキュリティ管理・対策実績：情報セキュリティ管理および対策実施業務に関し、過去5年間で3件以上の実績を有しているか。	必須	左記実績の業務内容（事業内容、サービスの種類、業務規模等）や類似点を記載ください。特に、何が当該業務の実施に有用なのか簡潔に記述してください。
（２）類似業務の規模	「（１）類似業務の経験」で示された業務について、本業務の規模以上の業務実績が記載されている場合は点数を付与する。該当する業務実績をより多く有する場合、又は独立行政法人・国・地方自治体・民間企業等で海外拠点を複数有する類似組織での業務実績を有する場合、高く評価する。	4	該当する実績を確認できる資料を提出ください。
（２）資格・認証等①	**【以下の認証を有していることを必須とする】** ・品質マネジメントシステムに係る認証：本業務の主担当部署が、品質マネジメントシステムに係る規格（ISO9001）の認証を保持しているか。 ・情報セキュリティマネジメントシステムに係る認証：情報セキュリティマネジメントシステムに係る規格（ISO27001）の認証を保持している部署が、本業務の主担当部署と連携する体制が組めることが示されているか。 ・個人情報保護に係る認証：個人情報保護に関する認証（プライバシーマーク又は同等の認証）を保持しているか。	必須	資格・認証を有する場合はその証明書の写しを提出願います。 **「※行動計画策定・周知」** ・従業員が101人以上の企業には、行動計画の策定・届出、公表・周知が義務付けられている一方で、従業員が100人以下の企業には努力義務とされています。 ・行動計画策定後は、都道府県労働局に届け出る必要があります。 ・行動計画策定企業については、行動計画を公表および従業員へ周知した日付をもって行動計

（２）資格・認証等②	**【以下の認証を1つ以上有している、もしくは行動計画の条件を満たしている場合は点数を付与する。より多くの認証を有している、もしくは行動計画の条件を満たしている場合は高く評価する。】** ・女性活躍推進法に基づく「えるぼし認定」または「プラチナえるぼし認定」もしくは「※行動計画策定・周知」 ・次世代育成支援対策推進法に基づく「くるみん認定」、「トライくるみん認定」または「プラチナくるみん認定」もしくは「※行動計画策定・周知」 ・若者雇用促進法に基づく「ユースエール認定」 ・安全衛生優良企業認定 ホワイトマーク ・健康経営優良法人 大規模 ホワイト500認定 ・健康経営優良法人 中小規模 認定	2	提出および従業員へ周知した日付をもって行動計画の策定とみなすため、以下に類する書類をご提出ください。（計画期間が満了していない行動計画を策定している場合のみに限ります。） ー厚生労働省のウェブサイトや自社ホームページで公表した日付が分かる画面を印刷した書類 ー社内イントラネット等で従業員へ周知した日が分かる画面を印刷した書類
２．業務の実施方針等		**126**	
（１）業務実施の基本方針（留意点）・方法・業務実施スケジュール	・本業務の背景、目的、本業務受託者に求める業者姿勢（基本的な考え方、機構運用サイクル、関係事業者間の調整、情報セキュリティ対策等）に係るポイントが具体的に示されているか。 ・システム利用提供業務やシステム運用支援業務、システム運用管理業務の業務範囲を、提案の全体像を把握できる内容が仕様を満たした形で示されているか。 ・本業務の完遂に向けて、具体的かつ実現可能性が高い事業計画（プロジェクト管理方法、想定される作業工程及び作業スケジュール、会議体の設置、懸念されるリスクとその対応策、成果物の内容等）が示されているか。	必須	左記ポイントを中心に業務仕様書案に対する、本業務実施における基本方針及び業務実施方法を記述してください。
（２）業務実施体制（要員計画・バックアップ体制）	・本業務の背景、目的、本受託事業者に求める業者姿勢に係る要件を満たした上で、本業務の実施体制及び各担当者の役割分担が示されているか。その実施体制は業務遂行上において適切な体制であるか。 ・提示された業務実施体制において、要員配置計画が具体的に示されているか。また、体制に起因する業務遂行上の問題が発生した場合の有効な対応策（バックアップ体制等）が示されているか。 ・本業務内容は多岐にわたっており、多種多様な専門性が必要となる。要件定義書には現時点での最低限必要となる要件が示されているが、契約期間中に外部環境の変化等に伴い新たな要件が発生することも十分に想定しうる。そのような場合に対応しうる社としてのバックアップ体制が示されていれば高く評価する。	6	業務仕様書案に記載の業務全体を、どのような実施（管理）体制（直接業務に携わる業務従事者のみならず、組織として若しくは組織の外部のバックアップ体制を含む）、要員計画（業務に必要な業務従事者数、その構成、資格要件等）等で実施するか記述してください。

（３）各要件の充足	**●機構DC** 〇機構DCで稼働するシステムに求める機能・非機能要件を満たしたうえで、特に、次の点について具体的かつ実現可能性が高い提案が示されているか。 ・機構DCで稼働するシステムの設計開発方法（導入方法） ・機構DCで稼働するシステムで求められる機能、性能、信頼性等を実現するためのシステム構成、選定理由等 〇機構DCに求める「機構DC データセンタ要件（非機能要件内に記載）」を全て満たしているか。 **●機構クラウドDC** 〇機構クラウドDCで稼働するシステムに求める機能・非機能要件を満たしたうえで、特に、次の点について具体的かつ実現可能性が高い提案が示されているか。 ・ 機構クラウドDCで稼働するシステムの設計開発方法（導入方法） ・ 機構クラウドDCで稼働するシステムで求められる機能、性能、信頼性等を実現するためのシステム構成、選定理由等 〇機構クラウドDCの情報システム稼動環境について、機構の求める機能・非機能要件を全て満たしているか。 **●SaaS** 〇SaaSに求める機能・非機能要件を満たしたうえで、特に、「SaaSで求められる機能や選定理由等」について具体的かつ実現可能性が高い提案が示されているか。 〇SaaS稼動環境について、機構の求める機能・非機能要件を全て満たしているか。 **●システム運用** 〇システム運用要件に定める要件を満たし、具体的かつ実現可能性が高い提案が示されているか。 〇システム運用要件に定めるサービスオペレーションの一環として、PC等の機器の賃貸借を求める。PC等の機器の賃貸借については、各要件を満たしていることを明言した上で、必要に応じて補足資料を提出すること。	必須	
（３）作業内容・作業方法に対する提案内容①：機構DC	次のそれぞれの観点についての（要件の理解度も含めて）提案内容の具体性および実現可能性を評価する。 ・データセンタの切替時に業務系システムの機器移設を適切かつ効率的に行うための方法、手順、スケジュール、機器移設において留意すべき事項とその対応策。 ・新業務システムへの更改時に、新旧業務系システムの機器入替を適切かつ効率的に行うための方法、手順、スケジュール、機器入替において留意すべき事項とその対応策。 （【補足】新旧業務系システムの機器入替対応については、本業務の対象外ではあるが、本受託者には新旧業務系システム入替の仕様が定まりしだい、機構と本事業受託者とで協議のうえ対応をお願いする予定である。そのため、その対応可否、具体的な実施方法等についてあわせて確認するもの） ・データセンタの切り替え時（機器移設）、および業務系システムの更改時（機器入替）における、システム所管部署および関連事業者（保守事業者・構築事業者等）との具体的な調整の進め方。 （【補足】業務系システムの所管部署および業務系システムの関連事業者（保守事業者・構築事業者等）との調整が非常に重要となるため。） ・柔軟なコスト体系等、将来的にハウジング対象の業務系システムがクラウドへ移行する可能性があることを考慮された提案であるか。	15	業務実施にあたっての作業工程をフロー チャート・作業工程計画書等で作成願います。

（３）作業内容・作業方法に対する提案内容②：機構クラウドDC	次のそれぞれの観点についての（要件の理解度も含めて）提案内容を評価する。 ・機構クラウドDC全般の設計開発にあたっての作業方針、作業工程の考え方、工程毎の作業方法や作業内容等。 ・機構クラウドDCの利用環境の変化等（ 機構クラウドDCを利用するシステムの増加、機構クラウドDCの利用件数の増大、利用PC端末の変更に伴う当機構IT利用環境の変化等）にあわせた拡張性の確保等。 （【補足】今後の当機構IT利用環境の変化が充分に考慮されていることを重視するため。 ・機構クラウドDCに求める機構の要件を十分に理解した上で、現行システムから新システムへの適切なデータ移行方法、手順、スケジュール、データの整合性確保を適切かつ効率的に実施するための方法、データ移行において留意すべき事項とその対応策。 ・BCP発動時に備えたバックアップリージョンの構成が必要最小限であり、且つ拡張性も考慮された構成となっているか。 ・提案するクラウドサービスの機能を用いて効率的なリソース利用を図る等、コストを抑える構成、設計等について優れた提案がなされているか。	25	業務実施にあたっての作業工程をフロー チャート・作業工程計画書等で作成願います。
（３）作業内容・作業方法に対する提案内容③：SaaS	次のそれぞれの観点についての（要件の理解度も含めて）提案内容を評価する。 ・SaaS全般の設計開発にあたっての作業方針、作業工程の考え方、工程毎の作業方法や作業内容等。 ・SaaS利用環境の変化等（利用者数増加、ゼロトラスト化の促進に伴う当機構IT利用環境の変化等）にあわせた拡張性を考慮したサービス選定等。 （【補足】今後の当機構IT利用環境の変化が充分に考慮されていることを重視するため。） ・現行システムからSaaSへの適切なデータ移行方法、手順、スケジュール、データの整合性確保を適切かつ効率的に実施するための方法、データ移行において留意すべき事項とその対応策。	15	業務実施にあたっての作業工程をフロー チャート・作業工程計画書等で作成願います。
（３）作業内容・作業方法に対する提案内容④：サービスデザイン、サービスオペレーション等の効率的な運用等	次のそれぞれの観点についての（要件の理解度も含めた）提案内容の具体性および実現可能性を評価する。 ・システム運用要件に定めるサービスデザイン全般において、様々な専門性を有してのサービス運用支援及び運用管理の役務を全体として効率的に実施していくための工夫等。 （【補足】本業務では、様々な専門性を有してのサービス運用支援及び運用管理の役務を求めるものである一方、本業務受託者が自らの努力によって業務を効率化し、サービスレベルの維持・向上を継続して図っていくことも求めるものである。そのための工夫、提案があれば加点として評価する。） ・システム運用要件に定めるサービスオペレーション業務全般において、本業務受託者の経験・ノウハウを活かした作業効率化の工夫、ユーザの利便性向上の工夫、ユーザの利用手順がシンプルであること等の提案内容。 ・セキュリティインシデント対応に関し、想定されるリスク分析とその対応策および安定的に対応が図られるための体制・仕組み （【補足】昨今のセキュリティ動向を踏まえ、この点を重視している。） ・現行のヘルプデスクからの移行において、ユーザへの影響が最小限となるような手法、ヘルプデスクの要員教育等の工夫について優れた提案がなされているか。	25	業務実施にあたっての作業工程をフロー チャート・作業工程計画書等で作成願います。

（３）作業内容・作業方法に対する提案内容⑤：サービス関連調査・提言、サービス管理の効率的な運用等	次のそれぞれの観点についての（要件の理解度も含めた）提案内容の具体性および実現可能性を評価する。 ・ユーザ申請を効率的に運用するための体制・チャットボットの利用等のユーザ利便性向上に係る仕組み、障害管理における関連ベンダーとの責任範囲の調整、システム監視・障害管理・性能管理・可用性管理における管理ツールや自社の方法論の活用にる効率化・工夫について優れた提案がなされているか。 ・セキュリティ管理における平時のセキュリティ動向（最新情報）の把握方法、迅速な緊急インシデント対応の手順・方法、セキュリティインシデント対応のための機構内システム保守事業者、情報通信網運用の受託者との連携 （【補足】昨今のセキュリティ動向を踏まえ、この点を重視している。）	15	業務実施にあたっての作業工程をフロー チャート・作業工程計画書等で作成願います。
（３）作業内容・作業方法に対する提案内容⑥：システム運用全般	次のそれぞれの観点についての（要件の理解度も含めた）提案内容の具体性および実現可能性を評価する。 ・本業務受託者による能動的な業務実施の工夫や姿勢、そのメリットが根拠や実績とともに具体的に記載されているか。 【補足】付加価値（品質）重視の作業項目の詳細については、調達仕様書別添資料09「システム運用要件」を参照のこと。特に、在外拠点への支援、ITコンシェルジュの具体的な取り組み、情報共有基盤保守・管理の進め方、セルフモニタリングによる改善策の立案と報告等に関し、能動的な工夫・姿勢を期待する。 ・サービスレベル達成に向けたサービスレベルの管理方法、運用管理における手法に係る工夫等について優れた提案がなされているか。	25	業務実施にあたっての作業工程をフロー チャート・作業工程計画書等で作成願います。
３．プロジェクトマネージャー及び評価対象となる業務従事者の経験・能力		68	業務総括者及び評価対象となる業務従事者の経験・能力等（類似業務の経験、実務経験及び学位、資格等）について記述願います。
（１）プロジェクトマネージャー		7	
１）類似業務の経験	プロジェクトマネージャ業務に関し、過去10年間で類似業務（データセンタ及び共通基盤の提供、共通基盤を用いてのシステム運用・管理支援、ヘルプデスク、調査・提言の実施等の包括アウトソーシング業務）の経験（業務が分割された案件でも良い）が2件以上有していること。	必須	当該「類似業務」について類似する内容が具体的 に分かるよう最近のものから時系列順に記述して ください。

２）業務遂行能力	本業務について充分な業務遂行能力を有していることが示されているか 「当機構と類似の組織（独立行政法人、国、地方自治体又は民間企業等で海外拠点を複数有する類似組織での業務経験をより高く評価する）において類似業務をプロジェクトマネージャーとして問題なく遂行し、顧客からの評価が得られていること」 なお、本業務を実施する上で有益な以下のような資格（有益な資格の証明書等を添付すること）を保有している場合は高く評価する。 ・ PMP、情報処理技術者試験プロジェクトマネージャ ・ ITサービスマネジメントファンデーション ・ CISA、情報処理技術者試験システム監査技術者 等	7	左記に該当する資格を保有されている場合は証明書等を提出してください。
（２）運用設計リーダー		7	
１）類似業務の経験	システム運用設計業務に関し、過去5年間で3件以上の実績を有していること。	必須	当該「類似業務」について類似する内容が具体的に分かるよう最近のものから時系列順に記述してください。
２）業務遂行能力	本業務について充分な業務遂行能力を有していることが示されているか 「当機構と類似の組織（独立行政法人、国、地方自治体又は民間企業等で海外拠点を複数有する類似組織での業務経験をより高く評価する）において類似業務を運用設計リーダーとして問題なく遂行し、顧客からの評価が得られていること」 なお、本業務を実施する上で有益な以下のような資格（有益な資格の証明書等を添付すること）を保有している場合は高く評価する。 ・ITサービスマネジメントファンデーション ・マイクロソフト認定プロフェッショナル（MCP） ・情報処理技術者試験システム監査技術者　等	7	左記に該当する資格を保有されている場合は証明書等を提出してください。
（３）機構クラウドDCリーダー		7	
１）類似業務の経験	クラウド環境におけるシステムの基盤設計に関し、過去5年間で1件以上の実績を有していること。	必須	当該「類似業務」について類似する内容が具体的に分かるよう最近のものから時系列順に記述してください。

２）業務遂行能力	本業務について充分な業務遂行能力を有していることが示されているか。特にオンプレミス環境からクラウド環境への移行、またはクラウドツールの導入に係る業務経験を有する場合高く評価する。 「当機構と類似の組織（独立行政法人、国、地方自治体又は民間企業等で海外拠点を複数有する類似組織での業務経験をより高く評価する）において類似業務をデータセンタ準備リーダーとして問題なく遂行し、顧客からの評価が得られていること。」 なお、本業務を実施する上で有益な以下のような資格（有益な資格の証明書等を添付すること）を保有している場合は高く評価する。 ・ネットワーク技術資格（Cisco認定資格等） ・ITサービスマネジメントファンデーション ・マイクロソフト認定プロフェッショナル（MCP） ・情報処理技術者試験データベーススペシャリスト　等	7	左記に該当する資格を保有されている場合は証明書等を提出してください。
（４）機構DCリーダー		5	
１）類似業務の経験	データセンター環境におけるシステムの基盤設計に関し、過去5年間で1件以上の実績を有していること。	必須	当該「類似業務」について類似する内容が具体的に分かるよう最近のものから時系列順に記述してください。
２）業務遂行能力	本業務について充分な業務遂行能力を有していることが示されているか 「当機構と類似の組織（独立行政法人、国、地方自治体又は民間企業等で海外拠点を複数有する類似組織での業務経験をより高く評価する）において類似業務をデータセンタ準備リーダーとして問題なく遂行し、顧客からの評価が得られていること。」 なお、本業務を実施する上で有益な以下のような資格（有益な資格の証明書等を添付すること）を保有している場合は高く評価する。 ・ネットワーク技術資格（Cisco認定資格等） ・ITサービスマネジメントファンデーション ・マイクロソフト認定プロフェッショナル（MCP） ・情報処理技術者試験データベーススペシャリスト　等	5	左記に該当する資格を保有されている場合は証明書等を提出してください。
（５）運用業務主任		10	
１）類似業務の経験	システム運用業務に関し、5年以上の実績を有していること。	必須	当該「類似業務」について類似する内容が具体的に分かるよう最近のものから時系列順に記述してください。

２）業務遂行能力	本業務について充分な業務遂行能力を有していることが示されているか 「当機構と類似の組織（独立行政法人、国、地方自治体又は民間企業等で海外拠点を複数有する類似組織での業務経験をより高く評価する）において運用業務主任として問題なく遂行し、顧客からの評価が得られていること。」 なお、本業務を実施する上で有益な以下のような資格（有益な資格の証明書等を添付すること）を保有している場合は高く評価する。 ・PMP、情報処理技術者試験プロジェクトマネージャ ・ITサービスマネジメントファンデーション ・CISA、情報処理技術者試験システム監査技術者　等	10	左記に該当する資格を保有されている場合は証明書等を提出してください。
（６） ITコンシェルジュ（2名体制を想定（配点は2名分の合計））		7	
１）類似業務の経験	システム化企画・調達、システム開発管理業務に関し、3年以上の実績を有していること。	必須	当該「類似業務」について類似する内容が具体的に分かるよう最近のものから時系列順に記述してください。
２）業務遂行能力	本業務について充分な業務遂行能力を有していることが示されているか 「当機構と類似の組織（独立行政法人、国、地方自治体又は民間企業等で海外拠点を複数有する類似組織での業務経験をより高く評価する）においてIT全般における助言業務を担当者として問題なく遂行し、顧客からの評価が得られていること。」 なお、本業務を実施する上で有益な以下のような資格（有益な資格の証明書等を添付すること）を保有している場合は高く評価する。 ・PMP、情報処理技術者試験プロジェクトマネージャ ・ITコーディネーター ・ITサービスマネジメントファンデーション ・CISA、情報処理技術者試験ITストラテジスト　等 以下の業務内容を満足するための類似業務経験・知識・意欲・業務姿勢等を有するか。 ※ITコンシェルジュとは、情報システム部と協力し、機構内の部署やユーザーのITに関する課題解決や専門的知見を提供する機能およびその要員のことである。恒常的に最新情報や教訓・知見を蓄積・提供し、本業務受託者の顧客志向を最大限発揮するための役割をもっていることから、本件契約業務の中でも特に付加価値が求められる業務に関し、機動性・柔軟性・迅速性・プロセス的確性といった複合的な要素にかかる機構が求める品質レベルを十分に満足させるサービス提供を模範的に実践するもののことをいう。	7	左記に該当する資格を保有されている場合は証明書等を提出してください。
(7) モニタリング管理主任		6	

１）類似業務の経験	システム運用業務に関し、3年以上の実績を有していること。	必須	当該「類似業務」について類似する内容が具体的に分かるよう最近のものから時系列順に記述してください。
２）業務遂行能力	本業務について充分な業務遂行能力を有していることが示されているか 「当機構と類似の組織（独立行政法人、国、地方自治体又は民間企業等で海外拠点を複数有する類似組織での業務経験をより高く評価する）においてモニタリング管理主任として問題なく遂行し、顧客からの評価が得られていること。」 なお、本業務を実施する上で有益な以下のような資格（有益な資格の証明書等を添付すること）を保有している場合は高く評価する。 ・PMP、情報処理技術者試験プロジェクトマネージャ ・ITコーディネーター ・ITサービスマネジメントファンデーション ・CISA、情報処理技術者試験システム監査技術者　等	6	左記に該当する資格を保有されている場合は証明書等を提出してください。
（８）システム監視リーダー		5	
１）類似業務の経験	類似の組織（独立行政法人、国、地方自治体等又は民間企業（海外拠点を複数有する類似組織でも業務経験をより高く評価する）における類似業務のシステム運用監視業務を、3年以上経験していること。	必須	当該「類似業務」について類似する内容が具体的に分かるよう最近のものから時系列順に記述してください。
２）業務遂行能力	本業務について充分な業務遂行能力を有していることが示されているか 「当機構と類似の組織（独立行政法人、国、地方自治体又は民間企業等で海外拠点を複数有する類似組織での業務経験をより高く評価する）においてシステム監視やセキュリティ対応業務として問題なく遂行し、顧客からの評価が得られていること。」 なお、本業務を実施する上で有益な以下のような資格（有益な資格の証明書等を添付すること）を保有している場合は高く評価する。 ・ITサービスマネジメントファンデーション ・セキュリティプロフェッショナル認定資格制度（CISSP） ・情報処理技術者試験システム監査技術者　等	5	左記に該当する資格を保有されている場合は証明書等を提出してください。
（９）セキュリティリーダー		7	

１）類似業務の経験	類似の組織（独立行政法人、国、地方自治体等又は民間企業（海外拠点を複数有する類似組織でも業務経験をより高く評価する）における類似業務の情報セキュリティ管理および対策実施業務を、3年以上経験していること。	必須	当該「類似業務」について類似する内容が具体的に分かるよう最近のものから時系列順に記述してください。
２）業務遂行能力	本業務について充分な業務遂行能力を有していることが示されているか 「当機構と類似の組織（独立行政法人、国、地方自治体又は民間企業等で海外拠点を複数有する類似組織での業務経験をより高く評価する）においてシステム監視やセキュリティ対応業務として問題なく遂行し、顧客からの評価が得られていること。」 なお、本業務を実施する上で有益な以下のような資格（有益な資格の証明書等を添付すること）を保有している場合は高く評価する。 ・情報処理技術者試験情報セキュリティスペシャリスト ・情報処理技術者試験システム監査技術者 ・セキュリティプロフェッショナル認定資格制度（CISSP）等	7	左記に該当する資格を保有されている場合は証明書等を提出してください。
（１０）ヘルプデスクリーダー		7	
１）類似業務の経験	ヘルプデスク運用及びその管理業務に関し、3年以上の実績を有していること。	必須	当該「類似業務」について類似する内容が具体的に分かるよう最近のものから時系列順に記述してください。
２）業務遂行能力	○ヘルプデスクの運用に関する深い知識及び高度な能力を有し、管理者として本業務を円滑に遂行することができること。 ○本業務について充分な業務遂行能力を有していることが示されているか 「当機構と類似の組織（独立行政法人、国、地方自治体又は民間企業等で海外拠点を複数有する類似組織での業務経験をより高く評価する）において類似業務を管理者として問題なく遂行し、顧客からの評価が得られていること。」 なお、本業務を実施する上で有益な以下のような資格（有益な資格の証明書等を添付すること）を保有している場合は高く評価する。 ・コンタクトセンター検定試験 ・情報処理技術者試験 ・ITサービスマネージャ、等	7	左記に該当する資格を保有されている場合は証明書等を提出してください。
（１１）スーパーバイザー			

類似業務の経験・業務遂行能力	本業務と同等以上の規模を持つヘルプデスクにおける業務従事者の監督及び指導の経験及び能力を有すること。	必須	
（１２）オペレータ			
類似業務の経験・業務遂行能力	・日本語並びに英語によるコミュニケーションを充分に取ることができること ・英語の問い合わせ対応を行う者については、TOEICスコア700点以上相当を有する英語力および英語によるヘルプデスク受付経験がある、こと（【補足】英語による問い合わせ対応は全体の約1割程度） ・日本語を母国語としない者の場合は「日本語能力検定 N1（旧1級）」相当の能力を有すること。	必須	

合計　200