

機構 ICT 基盤運用管理サービス等業務

調達仕様書

令和 8 年 10 月
日本年金機構
システム運用部

本紙余白

目 次

第 1 章	調達案件の概要に関する事項	1
1.1	調達案件名	1
1.2	調達の背景	1
1.3	目的及び期待する効果.....	1
1.4	用語の定義	1
1.5	関連事業者の一覧.....	4
1.6	業務・情報システムの概要.....	6
1.7	契約.....	8
1.7.1	契約期間.....	8
1.7.2	契約に関する留意事項.....	8
1.7.3	支払いに関する留意事項.....	8
1.8	作業スケジュール	11
1.9	留意事項	13
1.10	連絡先	13
第 2 章	当該調達及び関連調達案件の調達単位、調達の方式等に関する事項.....	14
2.1	調達案件及び関連する調達案件の調達単位、調達の方式、実施時期	14
2.2	調達案件間の入札制限	14
第 3 章	情報システムに求める要件に関する事項	15
第 4 章	作業の実施内容に関する事項	16
4.1	作業の内容	16
4.1.1	運用管理に係る業務	16
4.1.2	中長期運用・保守作業計画の策定支援.....	16
4.1.3	障害・情報セキュリティインシデント発生時及び大規模災害等の発災時の対応	16
4.1.4	情報システムの現況確認.....	16
4.1.5	運用作業の改善提案.....	17

4.1.6	引継ぎ	17
4.1.7	情報システム台帳の提出.....	17
4.1.8	最終報告書の作成.....	17
4.2	成果物の範囲、納品期限等.....	18
4.2.1	納品成果物等	18
4.2.2	情報システムの経費区分.....	23
4.2.3	納品方法.....	24
4.2.4	納品場所.....	25
第 5 章	作業の実施体制・方法に関する事項	26
5.1	作業実施体制	26
5.2	管理体制	27
5.3	作業要員に求める資格等の要件	28
5.3.1	運用管理統括グループ.....	28
5.3.2	情報セキュリティ管理グループ	29
5.3.3	情報セキュリティ管理責任者	29
5.3.4	品質管理グループ	30
5.3.5	運用管理作業グループ.....	30
5.4	作業場所等	30
5.5	作業の管理に関する要領.....	31
5.5.1	基本事項.....	31
5.5.2	運用管理業務計画書の作成.....	31
5.5.3	運用管理業務及び稼働報告.....	31
5.5.4	作業上の留意事項.....	31
第 6 章	作業の実施にあたっての遵守事項.....	33
6.1	機密保持、情報・資料の取扱い.....	33
6.2	遵守する法令等	34
6.2.1	法令等の遵守	34
6.2.2	その他文書、標準への準拠	34
6.3	情報セキュリティ管理.....	35
6.4	監査.....	36
6.4.1	監査に関する事項	36
6.4.2	情報セキュリティ監査.....	36

6.5	履行完了後の資料の取扱い.....	37
6.6	通報窓口の周知.....	37
第 7 章	成果物の取扱いに関する事項	38
7.1	知的財産権の帰属.....	38
7.2	検査.....	38
7.3	契約不適合責任.....	39
第 8 章	入札参加資格に関する事項.....	40
8.1	入札参加要件	40
8.1.1	公的な資格や認証等の取得	40
8.1.2	受託実績.....	40
8.1.3	履行可能性審査に関する要件	40
8.2	入札制限	40
第 9 章	再委託に関する事項	42
9.1	再委託の制限及び再委託を認める場合の条件	42
9.2	承認手続	42
第 10 章	その他特記事項	43
10.1	前提条件及び制約条件.....	43
10.1.1	情報セキュリティに関する第三者評価の認証を証明できる書類の提出	43
10.1.2	仕様書等の明確化等.....	43
10.1.3	本調達受託者の能力を生かした自由な提案	43
10.1.4	実績及び評価結果の公表	43
10.2	環境への配慮.....	43
10.3	事前現地調査.....	43
10.4	その他.....	44
第 11 章	附属文書.....	45
11.1	要件定義書.....	45

11.2	参考資料.....	45
11.3	応札希望者が閲覧できる資料一覧表.....	45
11.4	閲覧要領.....	46
11.5	提案書等の審査要領.....	46
11.6	契約締結後に開示する資料.....	46

《別紙》

別紙 1:要件定義書

別紙 2:関連事業者との役割分担表

別紙 3:資料閲覧申請書 兼 秘密保持誓約書

別紙 4:守秘義務に関する誓約書

別紙 5:個人情報等の返却・廃棄等に関する報告書

別紙 6:法令及び契約内容の遵守状況に関する報告書

別紙 7:再委託等に係る承認申請書

別紙 8:受託証明書

別紙 9:現地調査申込書兼守秘義務誓約書

別紙 10:クリーニング作業完了報告書

別紙 11:業務内容詳細(拠点装置運用管理)

別紙 12:業務内容詳細(センタ運用管理)

別紙 13:業務内容詳細(ヘルプデスク)

別紙 14:業務内容詳細(運用統制管理)

別紙 15:管理者等申請書

第1章 調達案件の概要に関する事項

1.1 調達案件名

機構 ICT 基盤運用管理サービス等業務

1.2 調達の背景

日本年金機構(以下「機構」という。)では、全国の各拠点で使用している端末及び共通基盤・ネットワーク等のシステム設備(以下「機構 ICT 基盤」という。)の運用管理業務は、正確な運用作業の実行、障害への迅速な対応及び課題管理の確実な実施等によってシステムの安定稼働を図る必要があることから、当該運用管理業務を外部委託により実施している。

機構 ICT 基盤は令和 8 年 1 月に更改を実施し、運用管理サービス等業務は「機構 ICT 基盤(共通基盤システム等)の構築及び運用保守業務」の受託者が令和 10 年 6 月まで行うこととしている。

1.3 目的及び期待する効果

本調達は、令和 10 年 7 月以降の機構 ICT 基盤運用管理サービス等業務を調達するものである。契約終期は ICT 基盤のリース契約に合わせ、令和 13 年 4 月末までとする。

本仕様書は、機構 ICT 基盤に係る運用管理サービス等業務の調達に関し、当該業務に求められる役務の範囲及び内容、遵守されるべきサービスレベル、サービスレベルの管理方法等に係る仕様を記載するものである。

1.4 用語の定義

本仕様書で用いる用語については、以下の「表 1.4.1 用語の定義」に示す。

表 1.4.1 用語の定義

項番	用語	説明
1	G-SCAN	基幹共有フォルダを宛先に設定する、基幹業務系のスキャナ。
2	LPC	グループウェア、イントラメール、電子決済、事務共有フォルダを取扱する端末。共通事務端末、可搬型共通事務端末の総称。
3	L-SCAN	事務共有フォルダを宛先に設定するスキャナ。
4	MWM	市区町村等、年金事務所外で年金記録情報の照会等を行うための可搬型照会用窓口端末。Mobile Window Machine の略。
5	MP	MWM から出力するプリンタ。Mobile Printer の略。
6	SLA	Service Level Agreement の略。サービスの提供者が、サービスの内容や品質を利用者に保証する取り決めを指す。
7	SLCP-JCF2013	ソフトウェアを中心としたシステムの開発及び取引のための共通フレームワーク体系(2013 年版)。
8	TC	窓口装置、コンソール、光学式文字読取装置、プリンタ及び漢字プリンタ等の機構 ICT 基盤全体を制御して、各種業務処理を行うための社会保険オンラインシステム制御装置。
9	TC-ID	同一拠点内に複数の TC が存在する場合、TC を一意にするために付与した枝番号である。
10	WK	年金事務所の窓口等に設置された年金給付用の機能を実行する操作端末。窓口装置(給付用)の略称。
11	WM	年金事務所の窓口等に設置され社会保険オンラインシステムの機能を実行する操作端末。窓口装置の略称。
12	ウイルス対策機能	共通基盤システムにおいて、機構本部及び拠点の全ての端末並びにサーバのウイルス対策(ウイルスパターンファイルの配布、ウイルス検出時の通知等)を一元管理する機能。

項番	用語	説明
13	オンサイト	機器保守サービスの一体系。機器破損時、端末等納品事業者が機器を設置する拠点にて修理を実施する。
14	お客様対応業務システム	相談事跡、相談予約、お客様の声、事件・事故・事務処理誤りの4機能を有し、それらを一元的に管理・集計・分析等を可能とするシステム。
15	コアファイアウォール(コアFW)	統合ネットワークと本部ネットワークの境界に設置するネットワーク装置。統合ネットワークからの通信及び機構本部内の各システムへの通信に対して、ポリシーに基づいた通信の制御を行う。
16	センドバック	機器保守サービスの一体系。機器破損時、端末等納品事業者に返送して修理する。
17	ハードウェア及びソフトウェア等	本システムを構成するハードウェア及びソフトウェア(市販ソフトウェアを含む)の総称。
18	ログ管理機能	共通基盤システムにおいて、端末並びにサーバのファイル操作ログ、外部媒体アクセスログ、印刷ログ等を収集し一元管理する機能。
19	一元化スキャナ(I-SCANB)	公的年金給付総合情報連携システムで利用するスキャナ。I-SCANBとも呼ぶ。
20	運行監視機能	共通基盤システムにおいて、共通基盤及び外部システムの稼働状況、障害発生状況及びハードウェア資源の使用状況等を一元管理するとともに、異常と判断された場合は、各システムの運用管理者に通知する機能。
21	稼働維持環境	本番環境の検証や保守訓練等、システムの維持保守を目的としたシステム環境。
22	外部システム	共通基盤システム等が提供する機能を利用するシステム。 詳細は別紙1「要件定義書」の「表 3.3.5.2 外部システム一覧」を参照すること。
23	監査機能	共通基盤システムにおいて、特権IDを保有する共通基盤システム及び外部システムの運用管理者等が、各システムに対して実施する操作を操作証跡として取得し一元管理する機能。
24	基幹業務	国民年金及び厚生年金保険に係る業務。 ※年金個人情報を取り扱う。
25	基幹共有フォルダ	基幹業務で利用するフォルダ。
26	機構本部	日本年金機構の本部。
27	休日	行政機関の休日に関する法律第一条にて定められた行政機関の休日。
28	共通基盤システム	統合認証ID管理機能、ウイルス対策機能、端末管理機能等で構成されており、システム基盤の共通化と情報セキュリティ強化を実現し、機構職員が利用するシステムを横断的に支える基盤となるシステム。機構ICT基盤(共通基盤システム等)に含まれる。
29	共通事務システム	グループウェア、イントラメール、電子決裁及び事務共有フォルダ等で構成されており、機構職員向けの情報共有プラットフォームシステム。機構ICT基盤(共通基盤システム等)に含まれる。
30	拠点	機構本部、年金事務所等を合わせた総称。
31	経過管理・電子決済サブシステム	被保険者等から提出される届書や申請書について、審査、決裁に係る電子決裁処理及び受付から結果の通知までの経過等を一元管理する業務ソフトウェアを指す。
32	経過スキャナ	経過管理・電子決済サブシステムにおいて、届書や添付書類等を画像データ化するスキャナ。
33	事務共有フォルダ	基幹教務以外で利用するフォルダ。
34	事務センター	各都道府県における届書処理業務等を集約して行う拠点。
35	社会保険オンラインシステム	基礎年金番号管理システム、記録管理システム及び年金給付システムの3つのサブシステムにより構成されるシステム。機構本部に設置された基幹システムと全国の年金事務所等に設置された専用端末機を専用ネットワークで結び運用している。
36	情報セキュリティ対策実施手順書群	以下に示す情報セキュリティに関する手順書一式。 ・情報セキュリティインシデント対応手順書 ・業務委託及び機器等の購入における情報セキュリティ対策実施手順書 ・情報取扱手順書 ・例外措置手順書 ・その他、当該業務の実施にあたり、セキュリティ対策を記載した手順書やマニュアル等(「ソフトウェア情報等の管理及び報告手順書」、「脆弱性対策計画(セキュリティパッチ適用)の実施手順書」等)

項番	用語	説明
37	情報業務	インターネットセグメントを経由した WEB 閲覧、文章作成、外部機関とのデータ授受等の業務。
38	情報業務端末	情報業務を実施する端末。
39	端末ソフトウェア	業務端末に格納する社会保険業務を実施するためのプログラムのこと。
40	端末管理機能	共通基盤システムにおいて、機構本部及び拠点の全ての端末並びにサーバに係るハードウェア及びソフトウェアの構成情報を収集し一元管理するとともに、資材(セキュリティパッチ、ソフトウェア等)の配布を行う機能。
41	定常運用	一定の周期やスケジュールに基づいて、継続的に実施される運用業務。
42	統合認証 ID 管理機能	共通基盤システムにおいて、Active Directory による Windows 統合認証及び生体認証を行う機能。
43	統合ネットワーク (厚生労働省統合ネットワーク)	厚生労働省が構築・運用管理するネットワーク網のこと。機構本部、全国の年金事務所、事務センター及び関連府省庁間のネットワーク通信を提供している。 「厚生労働省ネットワーク(共通システム)最適化計画」に基づき、本省、地方支分部局、検疫所等の各組織において、個別の業務ごとに構築されてきた専用通信回線の集約・統合及び運用管理の一元化を図るため、平成 20 年 4 月から運用を開始した。
44	特権 ID	運用管理事業者がシステム設定等の変更を行うとき使用するシステムユーザ ID。当該 ID の管理は、共通基盤システムにて提供される特権 ID 管理機能を利用する。
45	年金給付システム	公的年金制度の受給権者に係る年金の裁定や支払等の業務処理を行うシステム。
46	年金事務所	年金業務を実施するために、全国に設置されている機構の拠点。
47	非定常運用	実施周期やスケジュールが確定していない運用業務。
48	平日	行政機関の休日に関する法律第一条にて定められた行政機関の休日以外の日。
49	保守機	装置交換等に備え、運用管理事業者の保守拠点に管理されている装置。
50	保守拠点	機構の日本全国の拠点に対し、運用保守業務を提供するために設置される運用管理事業者の拠点。
51	本番環境	機構職員が年金等に関する日常業務を行うために利用するシステム環境。
52	要保護情報	「政府機関の情報セキュリティ対策のための統一基準」に規定された、機密性 2 情報、機密性 3 情報、完全性 2 情報及び可用性 2 情報のいずれかに該当する情報。
53	利用者情報	記録管理システム、年金給付システムにおける業務権限の情報。

1.5 関連事業者の一覧

本調達受託者は、運用管理業務において、「表 1.5.1 関連事業者一覧」に示す関連事業者と連携する必要がある。

なお、機構、本調達受託者及び関連事業者の役割分担については、別紙 2「関連事業者との役割分担表」に示す。

表 1.5.1 関連事業者一覧

項番	名称	説明
1	運用管理事業者 (本調達受託者)	「機構 ICT 基盤運用管理サービス等業務」の受託者。 令和 10 年 7 月から令和 13 年 3 月までの期間について、機構 ICT 基盤に係る運用管理を行う。
2	現行運用管理事業者	「機構 ICT 基盤(共通基盤システム等)の構築及び運用・保守業務一式」の受託者。 令和 8 年 1 月から令和 10 年 6 月までの期間について、機構 ICT 基盤に係る運用管理を行う。
3	機構 ICT 基盤(共通基盤システム等)保守事業者	「機構 ICT 基盤(共通基盤システム等)の構築及び運用・保守業務一式」の受託者。 共通基盤システム等に係る保守を行う。
4	機構 ICT 基盤(拠点端末設備等)保守事業者	「機構 ICT 基盤(拠点端末設備等)のリース及び保守業務一式」の受託者。 拠点端末設備等に係る保守を行う。
5	機構 ICT 基盤(情報業務システム等)運用・保守事業者	「機構 ICT 基盤(情報業務システム等)の構築及び運用・保守業務一式」の受託者。 情報業務システム等に係る運用・保守を行う。
6	プリンタ等保守事業者	「日本年金機構プリンタ設備等(複合機)のリース及び保守業務等」 「日本年金機構プリンタ設備等(カラープリンタ等)のリース及び保守業務等」 「日本年金機構プリンタ設備等(納付書プリンタ)のリース及び保守業務等」 「日本年金機構プリンタ設備等(モノクロプリンタ)のリース及び保守業務等」 の受託者。 プリンタ等に係る納品・保守を行う。
7	社会保険オンラインシステム端末ソフトウェア等保守事業者	「社会保険オンラインシステム端末設備ソフトウェア開発等業務(機構 ICT 基盤の構築対応)及びアプリケーションプログラム保守業務」の受託者。 社会保険オンラインシステム端末設備に係る、アプリケーションの保守を行う。
8	統合ネットワーク事業者	「厚生労働省統合ネットワーク回線・機器に係る供給(第 5 期)一式」の受託者。 統合ネットワークに係る保守を行う。
9	次期運用管理事業者	令和 13 年 1 月以降の機構 ICT 基盤に係る運用管理を行う事業者。
10	外部システム事業者	共通基盤システムの提供する機能を利用する各機構システムの管理事業者。
11	統合運要管理事業者 (統合運管)	公的年金給付総合情報連携システム、お客様対応業務システム、紙台帳検索システム、源泉徴収サブシステム、受付進捗管理システム、障害年金業務支援システムの運用管理を行う事業者。
12	給付運用管理事業者 (給付運管)	年金給付システムの運用管理を行う事業者。
13	共通運用管理事業者 (共通運管)	経過管理電子決裁システム、番号業務事務システム、統計業務システムの運用管理を行う事業者。
14	間接・MACS 運用管理事業者 (間接・MACS 運管)	間接業務システム、業務処理要領確認システム(MACS)の運用管理を行う事業者。
15	維持SI事業者 (維持SI)	基礎年金番号管理システム、記録管理システム、収納対策支援システム、歳入金電子納付システムの運用管理を行う事業者。

項番	名称	説明
16	三鷹統合運用管理事業者 (三鷹統合運管)	電子申請システム、厚年適用業務支援システムの運用管理を行う事業者。
17	ねんきんネット運用管理事業者 (ねんきんネット運管)	ねんきんネットシステム、オンライン事業所年金情報サービスの運用管理を行う事業者。
18	機構 ICT 基盤(情報業務システム等)運用管理事業者 (機構 ICT 基盤(情報業務システム等))	機構 ICT 基盤(情報業務システム等)の運用管理を行う事業者

1.6 業務・情報システムの概要

本調達受託者の、業務対象となる運用管理業務の概要を、「表 1.6.1 運用管理業務概要」に示す。なお、運用管理業務の対象となる機器等を「図 1.6.1 対象機器」に示す。

表 1.6.1 運用管理業務概要

項番	区分	項目		主な作業内容
1	拠点装置運用管理	端末維持管理	管理拠点	保守用マスタ原本の管理(ファイル転送、ウィルス定義ファイル、パッチの適用)及び保守拠点への展開、定期点検対応
2			保守拠点	故障発生時の現地保守対応、保守機管理(棚卸し、起動確認等) 端末設備の増設・移設・撤去工事
3		工事対応		見積書作成、config 等設定値設計、厚生労働省統合ネットワーク調整、日程調整、出荷指示 進捗管理、トラブル対応、センタ側作業実施(TC への登録、ポート開閉設定等)、工事実績取り纏め、装置情報修正 図面修正
4	センタ運用管理	システム監視業務		ウィルス検知状況確認、脆弱性情報確認、障害インシデント対応
5		ハードウェア維持業務		故障対応、定期点検、トラブル対応時のログ取得、設定情報管理、システムバックアップ取得
6		ネットワーク管理業務		ネットワーク構成管理、厚生労働省統合ネットワーク登録管理
7		IT 資産管理		設計書の払出、端末設備ソフトウェアのプログラム管理、デバック環境の管理、ファイル転送 ウィルス定義ファイルの配布・適用状況確認、セキュリティパッチの検証・配布・適用状況確認
8	ヘルプデスク	問い合わせ対応		年金事務所等からの照会対応、問い合わせ登録管理、ハードウェア業者手配
9	運用統制管理	IT 資産管理		拠点情報管理、ハードウェア業者管理、保守機の配備調整、SLA 関連業者調整、ライセンス管理 ソフトウェアサポート期限確認、法定停電対応
10		セキュリティ対応業務		マルウェア等検知時対応
11		影響調査・課題対応		問い合わせ・要望対応、要件の明確化・詳細化、見積り(工数、根拠、証跡の情報収集) トラブル発生時の原因究明・問題解決(業者調整含む)
12		外部機関対応		国家サイバー統括室(NCO)・国会・会計検査院等からの調査対応、データ抽出
13		機構への報告業務		システム運用部との月例報告会対応、情報管理対策室との定例会議対応
14		プロジェクト管理		プロジェクト全体の遂行管理、要員管理、品質管理、スケジュール管理、リスク管理

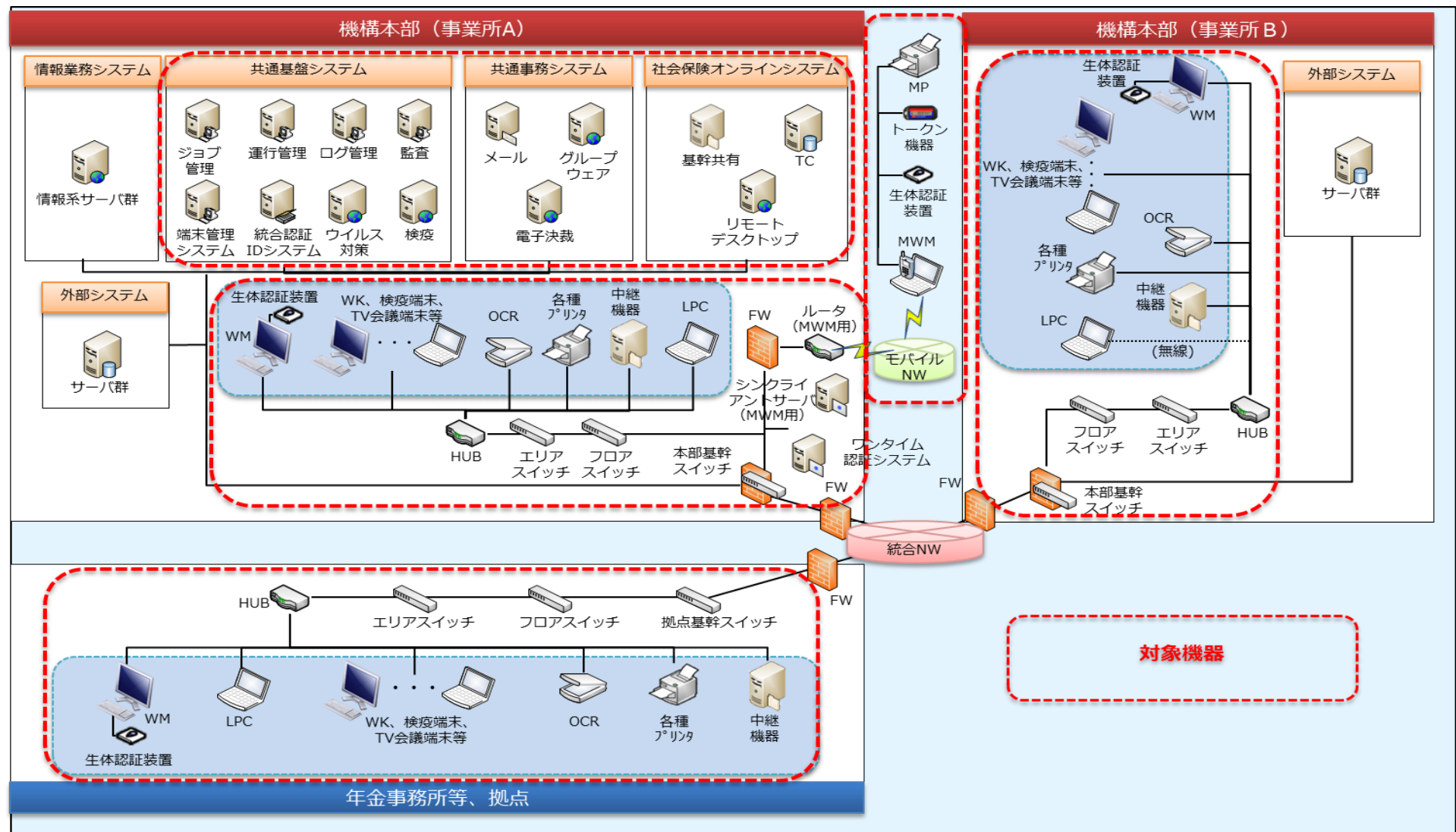


図 1.6.1 対象機器

1.7 契約

1.7.1 契約期間

本調達の契約(以下「本契約」という。)の期間は、契約締結の日から令和 13 年 4 月 30 日までとする。

- (1) 履行開始日
令和 10 年 1 月 21 日
- (2) 事前準備期間
令和 10 年 1 月 21 日から令和 10 年 6 月 30 日
- (3) 運用管理業務期間(支払い対象期間)
令和 10 年 7 月 1 日から令和 13 年 3 月 31 日
- (4) 完了報告、原状回復等の期間
令和 13 年 4 月 1 日から令和 13 年 4 月 30 日

1.7.2 契約に関する留意事項

(1) 定例外作業の取扱い

本調達受託者は、契約締結時に作業規模・実施内容が見込めない定例外作業については、作業項目に応じた作業指示書を受領の上、作業を実施すること。当該作業における作業指示書については、機構の指定した様式を利用する。

なお、入札金額の算定にあたっては、運用期間中に毎月別紙 1「要件定義書」に記載の定例外作業の月平均件数が発生することを前提とすること。

定例外作業については、作業指示書の内容に基づき、影響調査及び見積りを実施すること。

(2) サービスレベルに関する規定

① サービスレベル遵守に関する基本的な考え方

本調達におけるサービスレベルについては、別紙 1「要件定義書」に記載のサービスレベルの設定項目と障害レベルを踏まえ、設定すること。また、契約開始後における役務提供のスコープ変更や管理機器の増減が発生した場合については、サービスレベル合意書の改定に関する協議を機構と行い、決定内容に基づき改定する。

② サービスレベル達成状況の評価

本調達受託者は、機構と本調達受託者の間で合意したサービスレベルの達成状況を監視し、必要に応じて、機構に対し改善策を提案し、サービスレベル達成に向けた改善を実施すること。また、本調達受託者は、関連事業者の支援を受け、サービスレベルの目標値と実績値を比較し、達成度合いの評価、過去の達成状況との比較及びその傾向等の評価を行うこと。その結果、目標値を達成していない項目やサービスレベルの悪化については、その原因を分析すること。上記における監視結果、評価及び分析結果については、「表 1.7.2.1 サービスレベルの報告」に記載の内容を業務実施報告書にまとめ、機構へ報告を行うこと。

表 1.7.2.1 サービスレベルの報告

項番	報告区分	内容	条件
1	サービスレベル報告	・SLA 項目の達成状況の報告 ・SLA が遵守できない場合の原因分析及び改善案の提示	月次
2	改善状況報告	・項番 1 で提案される改善案の実施状況及び改善結果に関する報告	必要に応じて随時

(3) 運用効率の改善

本調達受託者は、運用管理コストの削減及び人的ミスを減らすことを目的に、機構と効率化状況報告会議の開催を定期的に行い、業務の総点検を行うこと。効率化状況報告会議の開催頻度については機構と協議の上決定すること。

1.7.3 支払いに関する留意事項

運用管理サービスに係る契約は、支払い条件により「固定費用」と「変動費用」に分類している。あらかじめ作業の頻度等が確定している定例作業について、見積り工数に応じた費用を固定費用として支

払う。一方、作業の頻度等が見込めない定例外作業については、過去の作業実績から将来発生する費用を見積り、変動費用として支払う。

(1) 固定費用

① 支払額の算定

固定費用の各月の支払い額については、原則として契約金額を業務委託月数で案分して算出した金額とする。

② 支払い条件

本調達受託事業者が提出する「業務実施報告書」の検査の合格をもって、月ごとに支払う。

③ 支払額の変更

(i) サービスレベルの達成度合いに応じた支払い

サービスレベル達成度合いに応じて、固定費用の支払額を変更するものとする。支払金額は、「①支払額の算定」により合意した金額に対して達成条件に応じた支払い割合を乗じて算出する。条件及び支払い割合については、「表 1.7.3.1 サービスレベル達成条件に応じた支払い割合」に記載する。

なお、サービスレベル達成状況の評価は、「業務実施報告書」の検査に合わせて行うものとする。なお、サービスレベルの設定項目等前提条件の詳細については、別紙 1「要件定義書」の「4.6.12(2) サービスレベルの設定項目と障害レベル」を参照すること。

表 1.7.3.1 サービスレベル達成条件に応じた支払い割合

項番	達成度合い	達成条件	支払割合
1	A	全 SLA 項目で条件の達成、 又は SLA 項目のうち未達成が 1 件	100%
2	B	SLA 項目のうち未達成が 2 件、 又は同一の SLA 評価項目が 2 か月連続で未達成	96%
3	C	条件を達成できない SLA 項目が 3 件 又は同一の SLA 評価項目が 3 か月連続で未達成	92%
4	D	条件を達成できない SLA 項目が 4 件以上 又は同一の SLA 評価項目が 4 か月以上連続で未達成	89%

(ii) 効率化に伴う減額調整

運用管理業務の自動化等による工数削減効果がみられる場合は、固定費用の支払金額の減額調整を行う。

固定費用支払金額及び減額開始月については、効率化状況報告会議において、本調達受託事業者からの効率化状況報告の評価を行い機構との協議の上決定する。

なお、効率化状況報告会議の開催頻度については、契約時に機構と協議を行うこととする。

(iii) 装置台数の増減に関する取扱い

本調達受託事業者が管理する装置は、新規イベント等の発生により、装置台数が増減する可能性がある。装置台数の変動について、総装置台数の 5%以下の増減が発生する場合、本調達受託事業者は本契約の範囲内(金額)で運用管理サービスを提供すること。装置台数は、別紙 1「要件定義書」の「図 2.1.1 機構 ICT 基盤運用管理業務の対象範囲」を参照すること。なお、管理対象となる装置の詳細については、閲覧資料「管理対象装置一覧」に示す。

(2) 変動費用

① 対象作業

(i) 定例外作業

契約当初において、作業規模・実施内容が見込めず機構からの作業指示書により依頼を受けた作業。

(ii) 拠点設置等作業

定例外作業のうち、機構 ICT 基盤設置等の工事を伴うもの。

(iii) 次期運用管理事業者への引継ぎ作業

- 次期運用管理事業者への引継ぎに係る作業。
- (iv) 既存 LAN ケーブルの撤去作業
既存端末等に係る LAN ケーブルの撤去作業。
- ② 支払い額の算定
機構からの依頼に基づき、影響調査、要件整理及び見積りを実施し、機構の精査を受け、機構との協議を行い、支払金額を決定する。支払金額は、作業工数に対象作業ごとに設定する人件費単価を乗じた金額とする。なお、人件費単価は入札時に定例外作業の入札金額の算定に使用した単価を上限に、契約時に機構と協議して決定する。
- ③ 支払い条件
作業結果及び作業結果報告書の検査の合格をもって、月ごとに支払う。
- ④ 変動費用支払いの流れ
定例外作業及び機構 ICT 基盤設置等作業の依頼発生から変動費用支払いまでの流れを、「図 1.7.3.1 変動費用支払いの流れ」に示す。

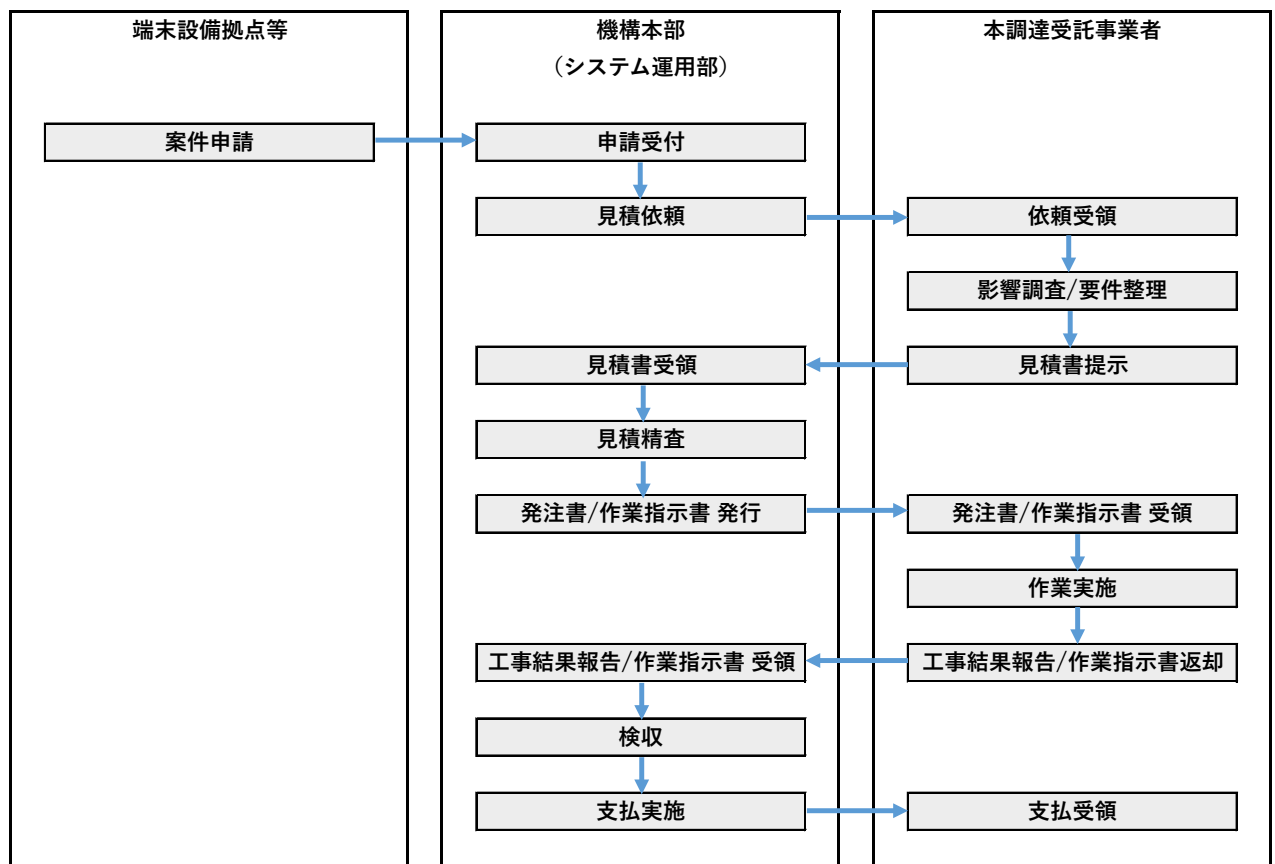


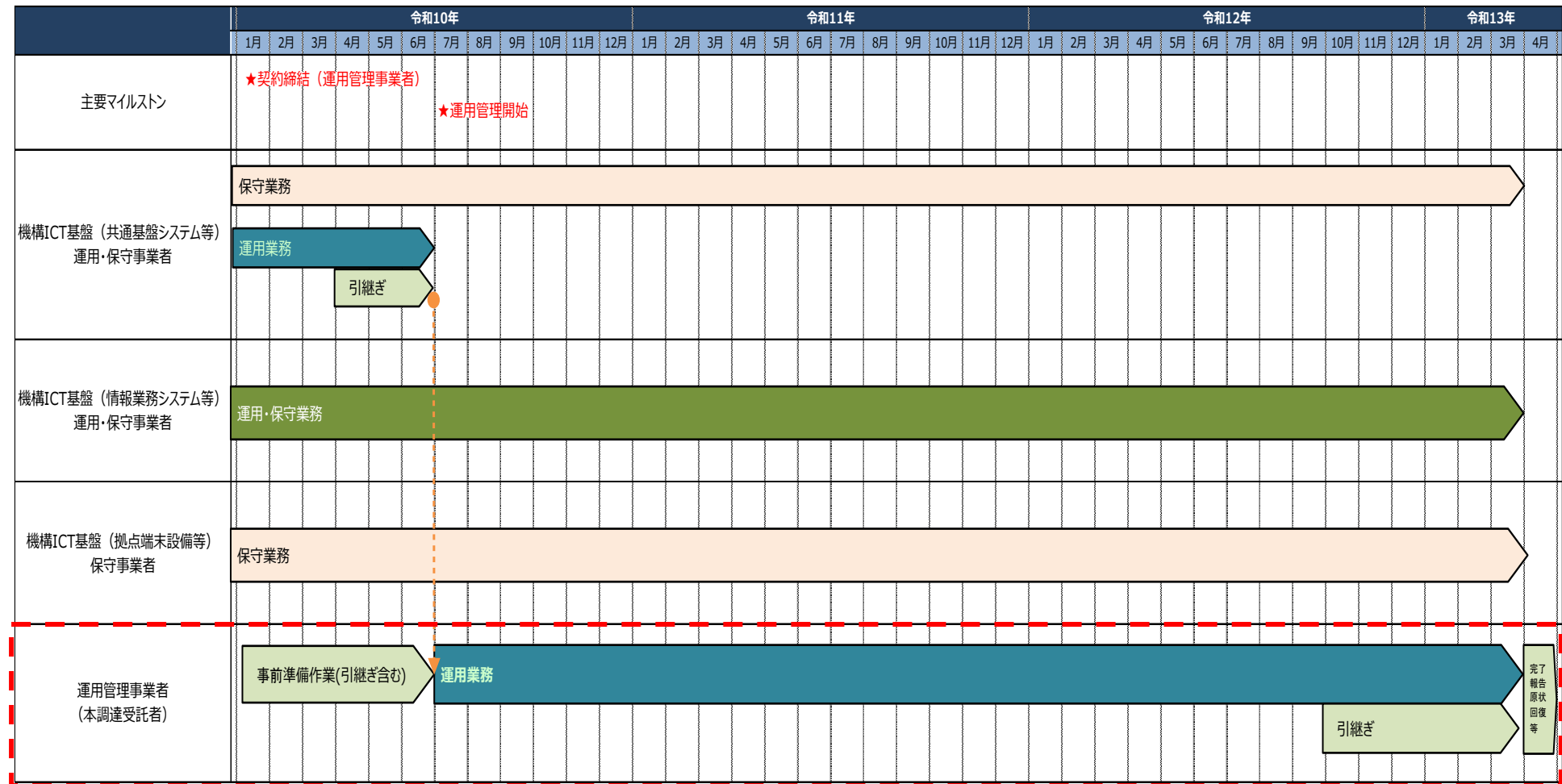
図 1.7.3.1 変動費用支払いの流れ

1.8 作業スケジュール

本調達における作業スケジュールは、「表 1.8.1 作業の実施期間」及び「図 1.8.1 全体概要スケジュール」のとおりである。

表 1.8.1 作業の実施期間

項番	作業内容	実施期間
1	事前準備作業	履行開始日～令和 10 年 6 月 30 日
2	運用管理業務	令和 10 年 7 月 1 日～令和 13 年 3 月 31 日
3	次期運用管理事業者への引継ぎ	令和 12 年 10 月 1 日～令和 13 年 3 月 31 日
4	完了報告、原状回復等	令和 13 年 4 月 1 日～令和 13 年 4 月 30 日



本調達受託者の役務範囲

図 1.8.1 全体概要スケジュール

1.9 留意事項

- (1) 年金の日
年金の日(毎年 11 月 30 日)が、土日の場合は稼働日として業務実施を行うこと。
- (2) その他留意事項
契約締結日以降に業務の追加、削除、増加及び減少が発生した場合、本調達受託者は機構と協議の上、契約の変更又は追加に応じること。また、本仕様書に記載する内容の他、運用・保守マニュアルに記載されている内容についても把握し、遵守すること。

1.10 連絡先

調達仕様書に関する問合せ先は以下のとおりである。

〒168-8505 東京都杉並区高井戸西 3-5-24 日本年金機構本部内

システム運用部 端末運用グループ（担当:吉田・古家）

電話: 03-5344-1127

第2章 当該調達及び関連調達案件の調達単位、調達の方式等に関する事項

2.1 調達案件及び関連する調達案件の調達単位、調達の方式、実施時期

本調達及びこれと関連する調達案件の調達単位、調達の方式、実施時期は、「表 2.1.1 関連する調達案件」に示すとおりである。

表 2.1.1 関連する調達案件

項番	調達案件名	調達方式	実施時期(予定)
1	機構 ICT 基盤運用管理サービス等業務 (本調達)	一般競争入札	調達中 契約期間:令和 10 年 1 月～令和 13 年 4 月
2	機構 ICT 基盤(共通基盤システム等)の構築及び運用・保守業務	随意契約	契約期間:令和 6 年 10 月～令和 13 年 4 月
3	機構 ICT 基盤(情報業務システム等)の構築及び運用・保守業務	一般競争入札	契約期間:令和 7 年 2 月～令和 13 年 4 月
4	機構 ICT 基盤(拠点端末設備等)のリース及び保守業務	一般競争入札	契約期間:令和 6 年 12 月～令和 13 年 6 月
5	日本年金機構プリンタ設備等のリース及び保守業務(令和 10 年度以降)	一般競争入札	調達中 契約期間:令和 9 年 2 月～令和 15 年 6 月
6	スキャナ(公的年金給付総合情報連携システム用)のリース及び保守業務	一般競争入札	契約期間:令和 5 年 7 月～令和 11 年 5 月
7	日本年金機構端末設備(扶養親族等申告書用スキャナ)のリース及び保守業務等(令和 8 年 2 月～令和 13 年 4 月)一式	一般競争入札	契約期間:令和 8 年 2 月～令和 13 年 4 月
8	社会保険オンラインシステム端末設備ソフトウェア開発等業務(機構 ICT 基盤の構築対応)及びアプリケーションプログラム保守業務	一般競争入札	契約期間:令和 6 年 9 月～令和 10 年 12 月
9	テレビ会議システムの再リース及び保守業務(令和 9 年度以降)一式	一般競争入札	調達中 契約期間:令和 9 年 8 月～令和 11 年 12 月

2.2 調達案件間の入札制限

本調達と「表 2.1.1 関連する調達案件」に示す関連する調達案件との間の入札制限は設けないこととするが、本調達における入札制限の詳細については、「8.2 入札制限」を参照すること。

第3章 情報システムに求める要件に関する事項

本調達の実施にあたっては、別紙 1「要件定義書」の各要件を満たすこと。

第4章 作業の実施内容に関する事項

4.1 作業の内容

別紙 1「要件定義書」に基づいて、以下に示す作業を実施すること。

4.1.1 運用管理に係る業務

(1) 業務項目

- ① 事前準備作業
- ② 運用管理業務
 - (i) 拠点装置運用管理
 - (ii) センタ運用管理
 - (iii) ヘルプデスク
 - (iv) 運用統制管理
 - (v) 次期運用管理事業者への引継ぎ

(2) 運用管理業務の概要

運用管理業務の概要は、以下の「表 4.1.1.1 業務概要」のとおりである。

表 4.1.1.1 業務概要

項番	区分	概要
1	事前準備作業	事前準備作業計画書の作成、現行運用管理事業者からの引継ぎ、教育等準備作業
2	拠点装置運用管理(※)	拠点装置管理、端末ソフトウェア管理、故障対応、拠点装置設置等作業
3	センタ運用管理(※)	サーバ機器管理、サーバソフトウェア管理、システム監視/障害対応 セキュリティ対策、業務環境管理の実施
4	ヘルプデスク(※)	現地拠点からの問合せ対応
5	運用統制管理(※)	全体統括、IT 資産管理、セキュリティ管理、影響調査、申請対応、報告業務
6	次期運用管理事業者への引継ぎ	次期運用管理事業者へ、運用要綱、運用マニュアル及び操作手順等の引継ぎ

※項番 2～5 の業務規模については、別紙 1「要件定義書」の「3.3.4 従事要員数」を参照すること。

4.1.2 中長期運用・保守作業計画の策定支援

- (1) 本調達受託者は、機構が情報システムの構成や、ライフサイクル等の中長期の作業を含む運用計画を作成するに当たり、具体的な作業内容や実施サイクル等に関する資料作成の支援を行うこと。
- (2) 本調達受託者は、機構が定める方針に基づき、運用実施計画書を作成し、機構の承認を受けること。

4.1.3 障害・情報セキュリティインシデント発生時及び大規模災害等の発災時の対応

- (1) 本調達受託者は、情報システムの障害発生時(又は発生が見込まれる時)には、原則 10 分以内に機構に報告するとともに、その緊急度及び影響度を判断の上、別紙 1「要件定義書」の運用管理業務に示す障害発生時運用管理業務(障害箇所の切り分け、関連事業者への連絡、復旧確認、報告等)を行うこと。なお、障害には、情報セキュリティインシデントを含めるものとし、被害の程度を把握するため、必要な記録類を事案対応終了時まで保存し、機構の求めに応じて提出すること。具体的な実施内容・手順は機構が定める運用計画書及び運用実施要領に基づいて行うこと。
- (2) 本調達受託者は、情報システムの障害に関して事象の分析(発生原因、影響度、過去の発生実績、再発可能性等)を行い、同様の事象が将来にわたって発生する可能性がある場合には、恒久的な対応策を提案すること。
- (3) 本調達受託者は、大規模災害等の発災時には、機構の指示を受けて、(1)及び(2)に準じた対応を行い、情報システムの早期復旧に尽力すること。

4.1.4 情報システムの現況確認

- (1) 本調達受託者は、機構から提供される情報システム台帳を用いて、業務開始時及び半期に一度、情報システム台帳の記載情報と情報システムの現況との突合・確認(以下、「現況確認」という。)を行い、現況結果確認報告書を提出すること。

- (2) 本調達受託者は、現況確認の結果、情報システム台帳の記載情報と情報システムの現況との間の差異がみられる場合は、運用実施要領に定める変更管理方法に従い差異を解消すること、又は差異を解消する支援を行うこと。
- (3) 本調達受託者は、現況確認の結果、ライセンス許諾条件に合致しない状況が認められる場合は、当該条件への適合可否、条件等を調査の上機構に報告すること。
- (4) 本調達受託者は、現況確認において、SLCP-JCF2013 (IPA)の MyJVN バージョンチェッカを用いる等により、ソフトウェア製品のバージョンを確認すること。
- (5) 本調達受託者は、ソフトウェアのサポート期限等の確認結果を、「利用を認めるソフトウェア及び利用を禁止するソフトウェア」により、機構に月次で報告すること。その際、確認実施日から1年の間にサポートが切れるソフトウェアがある場合は、当該ソフトウェアの更新の可否、また、影響の有無等を調査の上、併せて報告すること。
万が一、サポートが切れたソフトウェア製品の使用が明らかとなった場合は、当該製品の更新の可否、更新した場合の影響の有無等を至急調査の上、機構に報告すること。また、サポート切れのソフトウェア製品を更新した場合は、改めて機構へ報告すること。

4.1.5 運用作業の改善提案

本調達受託者は、本契約の終了までに、運用実績を取りまとめるとともに、必要に応じて運用作業に対する改善提案を行うこと。

4.1.6 引継ぎ

本調達受託者は、以下に関する引継作業を行うこと。

- (1) 受託業務開始前に受託業務に関する事項について、現行運用管理事業者から引継ぎを受けること。
- (2) 次期運用管理事業者が円滑に業務を実施できるよう、以下の項目を明確にした引継書の案を作成し、機構の承認を得ること。
 - 課題
 - リスク引継事項
 - 改善提案引継事項
 - 案件特性及びシステム特性に伴う個別引継事項 等
- (3) 本調達受託者は、機構が本システムの更改や改修を行う際には、次期の情報システムにおける設計・開発事業者等に対し、残存課題に関する情報やデータの提供、質疑応答等の協力を行うこと。
- (4) 情報セキュリティに係る引継ぎを確実に実施するために、本調達受託者から次期運用管理事業者へ引継ぎを行う際には、情報システムに不要なデータ(※)が残存していないことを確認し、別紙 10「クリーニング作業完了報告書」を提出すること。
※例:パスワードが記載されたファイル、パスワード情報が埋め込まれたバッチファイル等
- (5) 電話番号については、次期運用管理事業者へ同じ電話番号を引き継ぐことができるよう検討し機構へ提案すること。

4.1.7 情報システム台帳の提出

本調達受託者は、次に掲げる事項について記載した情報システム台帳を必要に応じて更新し、機構が定める時期に提出すること。

- (1) 各データの変更管理
情報システムの運用において、ハードウェアの管理、ソフトウェア製品の管理、回線の管理、外部サービス(約款による外部サービス以外)の管理、施設の管理、公開ドメインの管理、取扱情報の管理、情報セキュリティ要件の管理、指標の管理の各項目について、その内容に変更が生じる作業をした時は、当該変更を行った項目。
- (2) 作業実績等の管理
情報システムの運用中に取りまとめた作業実績、リスク、課題及び障害事由。

4.1.8 最終報告書の作成

本調達受託者は、本調達案件の運用管理業務期間満了と同時に、最終報告書を作成し、機構の承

認を得ること。

4.2 成果物の範囲、納品期限等

4.2.1 納品成果物等

(1) 納品成果物

本調達における主な成果物は、「表 4.2.1.1 納品成果物一覧」のとおりである。各納品成果物の作成様式については、機構と協議すること。

また、「表 4.2.1.1 納品成果物一覧」に示す、SLCP-JCF2013(情報処理推進機構(IPA)が定める共通フレーム 2013)のアクティビティについては、各成果物の作成工程の目安とし、作成工程の詳細については、別途機構及び関連事業者と協議すること。

表 4.2.1.1 納品成果物一覧

項番	成果物	概要	納品期限	SLCP-JCF2013 のアクティビティ
15	事前準備作業計画書	業務開始までに必要な準備作業(要員の研修、現行事業者からの引継ぎ等)の実施について記載した計画書。 ※詳細については別紙 1「要件定義書」の「4.4.3 事前準備作業計画書の作成」を参照すること。	履行開始後 2 週間以内	1.2.4 契約の実行 3.1.1 運用の準備
16	経費内訳	運用の経費を記載したドキュメント。 なお、詳細は「4.2.2 情報システムの経費区分」を参照すること。		
17	情報セキュリティ管理計画書	情報セキュリティ対策の遵守方法及び管理体制等に関する計画をとりまとめたドキュメント。(情報セキュリティを確保するための体制を定めた書面を含む。)	履行開始後 1 か月以内及び変更の都度	
18	情報取扱者名簿	情報管理責任者(当該業務の情報取扱の全てに責任を有する者)、情報取扱管理者(当該業務の進捗管理を行い、保護を要する情報を取り扱う可能性のある者)、その他保護を要する情報を取り扱う可能性のある者について、氏名、住所、生年月日、所属部署、役職等を、業務の一部を再委託する場合は再委託先も含めて、記載した名簿。		
19	業務従事者名簿	当該業務に従事する者について、氏名、所属部署、役職、学歴、職歴、業務経験、研修実績その他の経歴、専門的知識その他の知見、母語及び外国語能力、国籍等を記載した名簿。		
20	運用実施計画書	運用管理業務の作業範囲、スケジュール、実施体制、実施計画、管理計画等を定めた資料。 ※詳細については別紙 1「要件定義書」の「4.4.7(1) 運用実施計画書」を参照すること。		
21	サービスレベル合意書	機構、本調達受託者間で合意した SLA を記載した合意書。		
22	運用管理業務計画書	運用管理業務工程における具体的なタスクの定義及びスケジュールについて記載したドキュメント。必要に応じて改定を行うこと。	習得訓練開始まで及び変更の都度	3.1 運用プロセス 3.1.4 システム運用
23	運用実施要領・ガイド	各業務内容詳細や統制管理業務等の実施に伴い、何を・いつ・どう実施するのか、どの作業で提供された運用マニュアルを使うのかなどの実施要領や運用ガイド・業務フローなどを纏めた運用構築資料。		
24	現況結果確認報告書	情報システム台帳と情報システムの現況との突合・確認した結果の報告書。	運用開始時及び半期に一度	
25	稼働報告書	前月度の運用・保守に係る活動内容、次月計画、各種対応状況、リソース利用状況、サービスレベル達成状況、インシデント報告等を纏め、報告するためのドキュメント。	月次	
26	業務実施報告書	サービスレベル達成状況を報告するドキュメント。	翌月 5 営業日以内	
27	障害報告書	障害発生日、障害原因、障害対応の作業内容、今後の対応等を記述し報告するためのドキュメント。 ※別紙 1「要件定義書」の「4.6.11 稼働状況管理」を参照すること。	随時	
28	作業計画書	非定常運用、保守作業等を行う際の計画書。	作業開始まで	
29	作業結果報告書	作業計画書を提出した作業が終了した際に作業結果を報告するためのドキュメント。	作業後 1 週間以内	
30	工事实施報告書	機構 ICT 基盤設置等作業の実施内容及び実施結果を記載した報告書。 ※別紙 1「要件定義書」の「4.5.1(4)機構 ICT 基盤設置等作業」を参照すること。		

項番	成果物	概要	納品期限	SLCP-JCF2013 のアクティビティ
31	端末配置図	各機構 ICT 基盤等の配置状況を記載した図面。 ※別紙 1「要件定義書」の「4.5.1(4)機構 ICT 基盤設置等作業」を参照すること。		
32	作業指示書	作業指示書により機構から指示された作業について、受領した作業指示書に作業結果を記入し報告するためのドキュメント。	作業指示書の回答期限まで	
33	会議議事録	会議の議事録。	月次及び開催の都度	
34	特権 ID 等一覧	運用又は保守から引き継いだ特権 ID 等の一覧(システム名、機器種別、機器名称、ホスト名、製品名、ID、利用者、用途等、運用上必要となる情報を記載) 納入は、一覧の変更が発生の都度とする。	随時	
35	利用を認めるソフトウェア及び利用を禁止するソフトウェア	システムに導入されているソフトウェアのサポート期限やバージョン情報を一覧化して報告するための報告書。	月次 年次	
36	改善状況報告書	サービスレベルの改善案の実施状況及び改善結果の報告。	随時	
37	効率化状況報告書	効率化状況報告会議に提出する報告書。効率化に資するツール等の提案、進捗状況の報告、実施による効果等を記載したドキュメント。	開催の都度	
38	情報システム台帳	情報システムにおいて、管理すべき項目(開発規模、ハードウェア、ソフトウェア製品等)を記載したドキュメント。フォーマット及び記載事項は機構から提示する。	記載内容の変更発生時	3.1 運用プロセス 3.1.5 利用者教育
39	運用・保守マニュアル	運用全般の実行及び管理に関する具体的な手順書。関連事業者が機構に納品している運用・保守マニュアルに対し、必要に応じて加筆修正を実施後、決定稿として機構に納品する。	変更の都度	
40	引継ぎ計画書	次期運用管理事業者への引継ぎ計画を記載したドキュメント。 (引継ぎ対象、体制・スケジュール、実施内容、習熟度判定、完了基準、管理方法等)	引継ぎ実施の場合、令和 12 年 9 月 30 日まで	
41	引継ぎ完了報告書	引継ぎ計画書に記載した引継ぎの完了を報告するドキュメント。	引継ぎ実施の場合、引継ぎ完了後 2 週間以内	5.2 プロジェクトアセスメント及び制御プロセス 5.2.4 プロジェクトの終了
42	ナレッジデータ	発生した事象や問合せ等の各種インシデントを管理するナレッジデータ。 (2 回納品すること)	(1 回目)運用管理業務の契約終了 4 か月前まで (2 回目)契約終了まで	
43	クリーニング作業完了報告書	情報システムに不要なデータ(※)が残存していないことを報告するドキュメント。 ※例:パスワードが記載されたファイル、パスワード情報が埋め込まれたパッチファイル等	契約終了まで	
44	最終報告書	受託期間内に実施した運用管理業務の完了報告書。	運用管理業務の契約終了後 10 営業日以内	1.2.6 供給プロセスの終了

(2) その他提出物

本調達における納品成果物以外に、機構への提出が必要となる主な資料等は、「表 4.2.1.2 その他提出物一覧」のとおりである。

表 4.2.1.2 その他提出物一覧

項番	提出資料	概要	提出時期	記載箇所
1	別紙 3 資料閲覧申請書兼秘密保持誓約書	応札を希望する事業者で本調達に係る資料について閲覧を希望する場合は、別紙 3「資料閲覧申請書兼秘密保持誓約書」を提出すること(閲覧日当日の提出で可)。	資料閲覧時	調達仕様書「11.4 閲覧要領」
2	提案書	提案書に以下の事項を記載又は添付すること。 なお、提案書の作成にあたっては、提案書作成要領に従い、必要に応じて社名等にマスクをすること。 また、提案書等の提出後、機構が提案内容等に関するプレゼンテーションを求めた場合に実施すること。	応札前	調達仕様書「8.1.3 履行可能性審査に関する要件」
3	機構が要求した監査項目を準拠できていることが確認できる書類	本調達受託者は、機構が要求した監査項目を準拠できていることが確認できる書類を可能な限り機構へ提出すること。	履行前、履行中、履行後の監査時	調達仕様書「6.4.1 監査に関する事項」
4	別紙 4 守秘義務に関する誓約書	本調達の実施にあたり、契約締結後速やかに、調達仕様書の別紙 4「守秘義務に関する誓約書」を機構に提出すること。 「日本年金機構情報セキュリティポリシー」、「情報セキュリティ対策実施手順書群」及び「日本年金機構個人情報保護管理規程」については、契約締結後、本調達受託者が機構に別紙 4「守秘義務に関する誓約書」を提出した際に開示する。	履行開始の前日まで	調達仕様書「6.1 機密保持、情報・資料の取扱い」 調達仕様書「6.2 遵守する法令等」
5	別紙 7 再委託等に係る承認申請書	・受託業務の一部を再委託する場合は、あらかじめ再委託先の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性及び契約金額について記載した別紙 7「再委託等に係る承認申請書」を提出し、承認を得ること。なお、再委託先は「8.2 入札制限」の対象となる事業者ではないこと。 ・当初申請内容に変更が生じた場合は、別紙 7「再委託等に係る承認申請書」を提出すること。 ・再委託先から更に第三者に委託が行われる場合は、再委託と同様に当該第三者の商号又は名称、住所並びに委託を行う業務の範囲等を記載した別紙 7「再委託等に係る承認申請書」を提出し、機構の承認を得ること。	再委託又は再々委託の実施前まで 申請内容に変更が生じた場合	調達仕様書「9.2 承認手続」
6	別紙 8 受託証明書	機構からの承認通知を受領した日から 2 週間以内に、申請書のとおりに再委託(又は再委託先から更に第三者への委託)が行われていることを証明するため、本調達受託者は別紙 8「受託証明書」を再委託先(又は再委託先から更に委託した先)から徴取し機構へ提出すること。	再委託又は再々委託の承認通知後	調達仕様書「9.2 承認手続」
7	再委託先(又は再々委託先)との守秘義務等の契約書の写し	機構から本調達受託者に課せられている守秘義務等と同等以上の条件(本契約終了後の秘密保持を含む。)及び必要に応じ、本調達受託者が自ら、再委託先に対して調査等を実施することを可能とする条項が含まれた契約を締結することとし、機構からその契約書の写しについて提示の要求があった場合は、速やかにこれを提示するものとする。	再委託又は再々委託の承認通知後、機構から提示の要求があった場合	契約書

項番	提出資料	概要	提出時期	記載箇所
8	別紙 6 法令及び契約内容の遵守状況に関する報告書	外部委託開始後速やかに、別紙 6「法令及び契約内容の遵守状況に関する報告書」を提出すること。 また、外部委託を複数年で契約した場合は、外部委託の開始後 1 年を経過するごとに、調達仕様書の別紙 6「法令及び契約内容の遵守状況に関する報告書」を提出すること。	「委託開始後速やかに」及び「委託開始後 1 年を経過するごとに」	調達仕様書「6.2 遵守する法令等」
9	情報セキュリティ対策その他の契約の履行状況報告書	情報セキュリティ対策その他の契約の履行状況を定期的に確認し、機構へ報告すること。	情報セキュリティ管理計画書に記載のとおり、定期的に	調達仕様書「6.3 情報セキュリティ管理」
10	情報セキュリティ監査対応計画書	本調達受託者は、機構から監査等の求めがあった場合に、速やかに情報セキュリティ監査を受け入れる部門、場所、時期、条件等を「情報セキュリティ監査対応計画書」等により提示し、監査を受け入れること。	機構から監査等の求めがあった場合	調達仕様書「6.4.2 情報セキュリティ監査」
11	第三者評価等の公的資格・認証の証明書	本調達受託者が委託業務開始前に機構へ提出した、情報セキュリティに関する第三者評価の認証を証明できる書類(プライバシーマーク又は ISO/IEC27001 又は JISQ27001 の写し)において、契約期間中にその認証期間が切れる場合、本調達受託者は、その認証期間を更新すること。 本調達受託者は、認証終了日から 1 か月以内に、情報セキュリティに関する第三者評価の認証期間が更新されたことが証明できる書類の写しを機構に提出すること。	認証終了日から 1 か月以内	調達仕様書「10.1.1 情報セキュリティに関する第三者評価の認証を証明できる書類の提出」
12	別紙 5 個人情報等の返却・廃棄等に関する報告書	受託業務完了後、本調達の実施の過程で機構が開示した情報、他の調達受託者が提示あるいは作成した情報を削除又は返却し、調達仕様書の別紙 5「個人情報等の返却・廃棄等に関する報告書」を機構へ提出すること。	受託業務完了後	調達仕様書「6.1 機密保持、情報・資料の取扱い」

4.2.2 情報システムの経費区分

本調達受託者は、履行開始後 2 週間以内に、「表 4.2.2.1 情報システムの経費区分」を参考とし、「対応する調達内容」欄の記載に対応した経費区分から成る「経費内訳」を機構へ提出すること。

表 4.2.2.1 情報システムの経費区分

項番	経費区分	摘要	対応する調達内容
1	整備経費	情報システムの整備(新規開発、機能改修・追加、更改及びこれらに付随する環境の整備をいう。)に要する一時的な経費	
2	調査研究等経費	情報システムの整備にあたり、業務の設計、要件定義を行う目的で行う現状分析、プロトタイプ作成、ドキュメント作成支援、調査研究等に要する経費(最適化計画の策定に要する経費を含む)	
3	設計経費	情報システムの整備に際し、その開発に関する設計書の作成に要する経費	
4	開発経費	情報システムの整備に際し、情報システムのプログラミング、パラメタ設定等による情報システムの開発(単体テストを含む。)に要する経費	
5	据付調整経費	ハードウェアやラックの搬入・据付け、ネットワークケーブルの敷設等、情報システムの物理的な稼働環境の整備に要する経費	
6	テスト経費	開発する情報システムの結合テスト、総合テスト及び受入テストに要する経費	
7	移行経費	情報システムのシステム移行及びデータ移行に要する経費	
8	廃棄経費	情報システムの廃止及び更改に伴う、ハードウェアやラック、ネットワークケーブル等の撤去及び廃棄に要する経費	
9	プロジェクト管理支援経費	情報システムの整備に関するプロジェクト管理に要する経費	
10	施設整備等経費	情報システムを構成するハードウェアを設置する施設、データ等を保管する施設又は運用事業者等が運用、保守等を行うために駐在する施設の整備、改修等に要する経費	
11	ハードウェア買取り経費	情報システムを構成するハードウェアの買取りに要する経費	
12	ソフトウェア買取り経費	情報システムを構成するソフトウェア製品のライセンスの買取り又は更新に要する経費	
13	その他整備経費	項番 2 から 12 までのいずれにも該当しない情報システムの整備に要する経費	
14	運用等経費		
15	システム運用経費	情報システムの正常な稼働を保持するために行うハードウェアの状態把握、ファイルの管理、アプリケーションプログラムの設定等の管理、障害に対する予防等の措置等、仕様変更や構成変更を伴わない情報システムの技術的及び管理的業務の実施に要する経費	4.1.1(1)②(i)拠点装置運用管理 4.1.1(1)②(ii)センタ運用管理 4.1.1(1)②(iv)運用 4.1.1(1)②(v)次期運用管理事業者への引継ぎ
16	業務運用支援経費	情報システムの稼働にあたって、業務実施部門が行う業務(データ作成(Web サイトや e ラーニングのコンテンツ作成等)の運用支援に要する経費	
17	操作研修等経費	情報システムの利用にあたって、当該情報システム部門の担当者又は情報システムの利用者に対する操作研修等(教材作成・更新を含む。)に要する経費	
18	ヘルプデスク経費	情報システム利用者からの問合せに対し、解決策を講ずるために行う業務に要する経費	4.1.1(1)②(iii)ヘルプデスク
19	コールセンタ経費	情報システム利用者からの問合せに対し、あらかじめ決められた事項を案内又は回答する業務に要する経費(主に大量の問合せがある場合が該当)	
20	アプリケーションプログラム保守経費	開発した情報システムについて、障害や技術革新等の外部環境の変化に対して情報システムの機能を仕様どおり正常な状態に保つために行うアプリケーションプログラムの改修、設定変更等に要する経費	

項番	経費区分	摘要	対応する調達内容
21	ハードウェア 保守経費	情報システムを構成するハードウェアについて、障害や技術革新等の外部環境の変化に対して情報システムの機能を仕様どおり正常な状態に保つために行う業務に要する経費	
22	ソフトウェア 保守経費	情報システムを構成するソフトウェア製品について、障害や技術革新等の外部環境の変化に対して情報システムの機能を仕様どおり正常な状態に保つために行う業務に要する経費	
23	監査経費	情報システムについて、システム監査又は情報セキュリティ監査の実施に要する経費	
24	情報セキュリティ 検査経費	情報システムについて、ペネトレーションテスト、脆弱性診断等の情報セキュリティ検査・診断の実施に要する経費	
25	ハードウェア 借料	情報システムを構成するハードウェアについて、その使用に要する借料	
26	ソフトウェア 借料	情報システムを構成するソフトウェア製品について、その使用に要する借料	
27	サービス利用料	情報システムの稼働又は利用にあたって、ASP、SaaS、PaaS、ホスティングサービス等、国の行政機関以外の者が提供するサービスの利用に要する経費	
28	通信回線料	情報システムを構成するネットワークにおいて必要となる通信回線の利用に要する経費	
29	施設利用等経費	情報システムを構成するハードウェアを設置する施設、データ等を保管する施設又は運用事業者等が運用、保守等を行うために駐在する施設の利用等に要する経費	
30	その他運用 等経費	項番 15 から 29 までのいずれにも該当しない情報システムの運用等に要する経費	

4.2.3 納品方法

成果物は、以下の内容を遵守した上で納品すること。

- (1) 成果物は、全て日本語で作成すること。ただし、日本国においても、英字で表記されることが一般的な文言については、そのまま記載してもかまわないものとする。
- (2) 用字・用語・記述符号の表記については、「公用文作成の考え方(令和 4 年 1 月 7 日文化審議会)」に準拠すること。
- (3) 情報処理に関する用語の表記については、原則、日本産業規格(JIS)の規定に準拠すること。
- (4) 「4.2.1(1)納品成果物」に示す成果物は、電磁的記録媒体(CD-R 等や機構が用意するセキュア USB)により作成し、電磁的記録媒体を 1 部納品すること。
ただし、機構からの求めがある場合は、紙媒体での納品に応じること。
また、テスト結果等であって電子ファイルにて納品できないものについては、機構は協議に応じるものとする。
- (5) 紙媒体による納品を求める場合、用紙のサイズは、原則として日本産業規格 A 列 4 番とするが、必要に応じて日本産業規格 A 列 3 番を使用すること。
また、バージョンアップ時等に差し替えが可能なように、バインダ方式とすること。
- (6) 電子ファイルによる納品について、ファイルは Office Open XML の docx 拡張子、xlsx 拡張子又は pptx 拡張子のファイル形式で作成すること。ただし、左記ファイル形式で納品が困難な場合は、機構と事前に協議の上、PDF のファイル形式で作成すること。また、機構が他の形式による提出を求める場

合は、協議の上、これに応じること。なお、本調達受託者側で他の形式を用いて提出したいファイルがある場合は、協議に応じるものとする。

- (7) 納品後、機構において改変が可能となるよう、図表等の元データも併せて納品すること。
- (8) 成果物の作成にあたって、特別なツールを使用する場合は、機構の承認を得ること。
- (9) 成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。
- (10) 電磁的記録媒体により納品する場合は、不正プログラム対策ソフトウェアによる確認を行う等して、成果物に不正プログラムが混入することのないよう、適切に対処すること。なお、対策ソフトウェアに関する情報(対策ソフトウェア名称、定義パターンバージョン、確認年月日)を記載したラベルを貼り付けること。
- (11) 主体認証情報(ログインのためのパスワード)の管理主体は利用者(機構)が主体的に管理することとし、システム ID については、本調達受託者が管理するものとする。
- (12) 特権 ID 等(設定変更可能なアカウント全般を指す)一覧を納品成果物に加えること。なお、当該一覧には、システム名、機器種別、機器名称、ホスト名、製品名、ユーザ名、ユーザ用途、ID 等、運用上必要となる情報を記載すること。ただし、パスワードは記載しないこと。
- (13) 本調達受託者は成果物の品質保証を確認できる手順を運用実施計画書に定めた上、機構と合意すること。また成果物の品質保証に留意すること。

4.2.4 納品場所

原則として、成果物は、「表 4.2.4.1 納品場所一覧」に示す場所において引渡しを行うこと。

ただし、機構が納品場所を別途指示する場合はこの限りではない。

表 4.2.4.1 納品場所一覧

項番	納品品目	納品場所
1	成果物	日本年金機構本部(高井戸) システム運用部端末運用グループ 東京都杉並区高井戸西 3-5-24

第5章 作業の実施体制・方法に関する事項

5.1 作業実施体制

本調達における、本調達受託者に求める作業実施体制は、「図 5.1.1 作業実施体制」及び「表 5.1.1 作業実施体制と役割」のとおりである。

本調達受託者は、運用管理業務の開始から終了までの期間において機構及び関連事業者からの問合せ等について速やかに対応すること。また、機構及び関連事業者からの問合せ等に対応するための十分な体制を整備すること。

なお、本調達受託者内のチーム編成については想定であり、本調達受託者決定後に協議の上、見直しを行う。

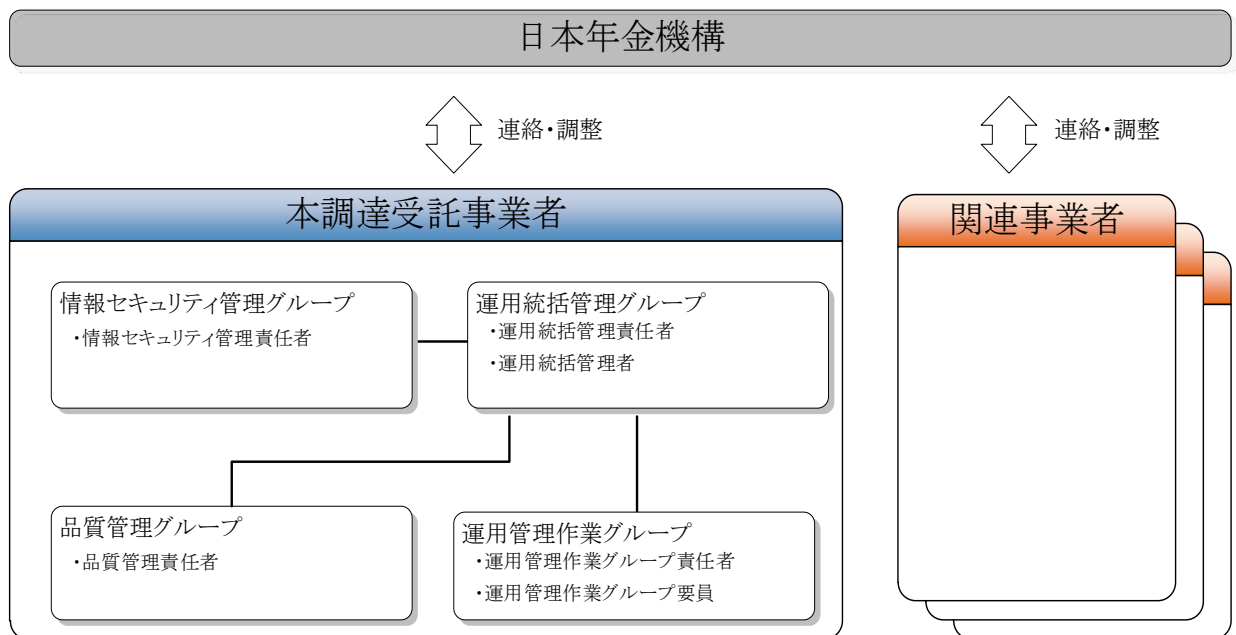


図 5.1.1 作業実施体制

表 5.1.1 作業実施体制と役割

項番	組織又は要員	役割
1	運用統括管理グループ	運用管理業務全体を統括するグループ。
2	運用統括管理責任者	運用管理業務全体を統括し、必要な意思決定を行う。
3	運用統括管理者	運用管理業務全体の管理者として、機構への報告、各種調整作業を行う。
4	情報セキュリティ管理グループ	本調達における情報セキュリティ対策全般について、第三者的な立場で指導・助言・管理を行うグループ。
5	情報セキュリティ管理責任者	独立的な立場から、情報セキュリティの遵守状況を管理する。 本調達内における、他の管理グループの管理者又は要員との兼任は認めない。
6	品質管理グループ	品質マネジメントシステムに基づいて、品質管理を行うグループ。
7	品質管理責任者	役務及び成果物の品質を管理する。
8	運用管理作業グループ	運用管理業務を行うグループ。
9	運用管理作業グループ責任者	担当する作業グループに係る各工程の計画策定及び進捗管理並びに納期・品質の確保に必要なプロジェクト管理を実施するものとする。
10	運用管理作業グループ要員	担当する作業グループに係る保守等の作業を担う。

5.2 管理体制

- (1) 受託業務の実施にあたり、機構の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、当該品質保証体制が書類等で確認できること。
- (2) 本システムに、機構の意図しない変更が行われる等の不正が見つかった時(不正が行われていると疑わしい時も含む。))に、追跡調査や立入検査等、機構と本調達受託者が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。
- (3) 当該管理体制を確認する際の参照情報として、資本関係・役員等の情報、作業の実施場所、委託事業従事者の所属・専門性(情報セキュリティに係る資格・研修実績等)・実績及び国籍に関する情報の提供を行うこと。

なお、国籍に関する情報の確認は、参考資料 1「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」の規定により実施するものであり、主に本調達受託者に対して外国政府からの影響を受けるおそれが十分排除されていることを確認することを目的とする。

- (4) 本調達受託者は、受託業務で知り得た情報を適切に管理するため、次に掲げる体制を確保し、当該体制を確保していることを証明するため、機構に対し「情報取扱者名簿」(要員のうち、保護を要する情報を取り扱う可能性のある者の名簿をいう。業務の一部を再委託する場合は再委託先も含む。)、 「情報セキュリティを確保するための体制を定めた書面(情報管理体制図、情報管理に関する社内規則等) (業務の一部を再委託する場合は再委託先も含む。))及び「業務従事者名簿」(要員の名簿をいう。))を提出すること。

(確保すべき体制)

- 情報取扱者は、受託業務の遂行際して必要最低限な範囲の者にすること。
- 本調達受託者が受託業務で知り得た情報について、機構が承認した場合を除き、本調達受託者の役員等を含め、情報取扱者名簿に記載のある者以外の者に伝達又は漏えいされないこと

を保証する履行体制を有していること。

※ 「情報取扱者名簿」には、情報管理責任者(受託業務の情報取扱の全てに責任を有する者)、情報取扱管理者(受託業務の進捗管理を行い、保護を要する情報を取り扱う可能性のある者)、その他保護を要する情報を取り扱う可能性のある者について、氏名、住所、生年月日、所属部署、役職等を、業務の一部を再委託する場合は再委託先も含めて、記載すること。

※ 「業務従事者名簿」には、要員について、氏名、所属部署、役職、学歴、職歴、業務経験、研修実績その他の経歴、専門的知識その他の知見、母語及び外国語能力、国籍等を記載すること。

- (5) 本調達受託者は(4)の「情報取扱者名簿」、「情報セキュリティを確保するための体制を定めた書面(情報管理体制図、情報管理に関する社内規定等)」及び「業務従事者名簿」に変更がある場合は、あらかじめ機構に申請を行い、承認を得ること。
- (6) 本調達受託者は、受託業務で知り得た情報について、機構が承認した場合を除き、本調達受託者の役員等を含め、情報取扱者以外の者に伝達又は漏えいしてはならない。本調達受託者は、受託業務で知り得た情報について、機構が承認した場合を除き、本調達受託者の親会社、地域統括会社、ブランド・ライセンサー、フランチャイザー、コンサルタントその他の受託者に対して指導、監督、業務支援、助言、監査等を行う者を含め、本調達受託者以外の者に伝達又は漏えいしてはならない。
- (7) 受託業務の実施に当たっては、進捗や作業内容を共有するため、定例会議を毎月 1 回以上開催するものとする。また、定例会議の議事録を作成し、機構の内容確認を受けること。なお、機構が認めた場合は、稼働実績や稼働状況の報告書並びに各種資料や成果物を提出することで定例会議の代わりとすることができるものとする。
- (8) 前述(1)～(4)で求める内容や体制(情報セキュリティ管理体制を含む)等に変更等がある場合は、直ちに機構へ連絡し、指示を受けるとともに、定例会議等でその内容を報告すること。
- (9) 要員の氏名、スキル、主な業務経歴等を記載した要員一覧を作成し、機構へ提出すること。
- (10) 本調達受託者の都合により要員を変更する場合は、前述(5)に従い事前に機構へ届け出ること。この場合、変更後の要員は、「5.3 作業要員に求める資格等の要件」に示す技能について、変更前と同等以上の技能を有するものとする。また、要員の変更に伴い業務に支障が生じないよう、引継ぎ及び習熟訓練を確実に行うこと。
- (11) 予定されているイベントや運用業務に応じ必要な要員を確保し、報告すること。

5.3 作業要員に求める資格等の要件

5.3.1 運用管理統括グループ

- (1) 運用管理統括グループに、以下の要員を配置すること。

- ① 運用統括管理責任者
- ② 運用統括管理者

- (2) 運用統括管理責任者

運用統括管理責任者は、運用管理業務全体を統括し、必要な意思決定を行うことによって、委託業務

を円滑に遂行するものとする。

なお、本調達受託者内において保守管理業務を遂行する主たる組織・部門の長が配置されることを想定している。

(3) 運用統括管理者

以下に示す要件の全てに該当する者を運用統括管理者として配置し、その者に、運用実施計画書の作成、要員の配置等必要な体制の確立及び納期・品質の確保に必要なプロジェクト管理を実施させることによって、委託業務を円滑に遂行すること。

- (i) システム開発等の情報処理業務の経験年数を 8 年以上有し、かつ全国 400 拠点超に展開するオンラインシステム(PC20,000 台、サーバ 500 台超)の運用管理責任者としての経験を有する者又は同等の実績を有する者。
- (ii) 以下に掲げるいずれかの資格等を有すること。
 - 情報処理の促進に関する法律(昭和 45 年 5 月 22 日法律第 90 号)に基づき実施される情報処理技術者試験のプロジェクトマネージャ試験の合格者
 - 技術士(情報工学部門)の称号を与えられた者
 - 技術士(総合技術監理部門(情報工学を選択科目とする者))の称号を与えられた者
 - 「IT スキル標準 v3」における「プロジェクトマネジメント」のいずれかの専門分野で達成度指標及びスキル熟成度ともにレベル 4 以上に相当する知識・経験を有する者。

(4) その他の事項

- ① 運用統括管理者は、原則として全ての進捗会議、品質評価会議及び月次報告会に出席することを義務づけるものとする。
- ② 作業品質の確保のため、運用統括管理者は、契約終了まで継続して従事すること。万一交代する場合は、同等以上の資格及び経験等を有する人物が担当するものとし、事前に機構の承認を得ること。

5.3.2 情報セキュリティ管理グループ

- (1) 情報セキュリティ管理グループには、情報セキュリティ管理責任者を配置すること。

5.3.3 情報セキュリティ管理責任者

- (1) 情報セキュリティ管理責任者は、以下に示す要件の全てを満たすこと。

- ① セキュリティ機能を設計、構築、運用及び保守する業務の管理責任者として、5 年以上の経験を有すること。
- ② 独立的な立場から、情報セキュリティの遵守状況を管理するため、他の管理グループの管理者又は要員でないこと。
- ③ 以下に掲げるいずれかの資格等を有すること。
 - (i) 「情報処理の促進に関する法律」に基づき実施される情報処理技術者試験の情報セキュリティスペシャリスト試験(テクニカルエンジニア(情報セキュリティ)試験及び情報セキュリティアドミニストレータ試験を含む。)の合格者
 - (ii) 「情報処理の促進に関する法律」に基づき実施される情報処理技術者試験の情報処理安全確保支援士試験の合格者
 - (iii) 「情報処理の促進に関する法律」に基づき実施される情報処理技術者試験のシステム監査技術者試験の合格者

- (iv) ISC2 が認定する情報セキュリティプロフェッショナル認定資格「CISSP」の資格保有者
- (v) 情報システムコントロール協会(ISACA)が認定する、公認情報セキュリティマネージャ(CISM)又は公認情報システム監査人(CISA)の資格保有者
- (vi) 日本セキュリティ監査協会(JASA)が認定する、公認情報セキュリティ監査人(CAIS)の資格保有者

5.3.4 品質管理グループ

- (1) 品質管理グループには、品質管理責任者を配置すること。
- (2) 品質管理責任者
品質管理責任者は、品質管理業務の管理責任者として、5 年以上の経験を有すること。

5.3.5 運用管理作業グループ

- (1) 運用管理作業を適正に運用できるよう、別紙1「要件定義書」の「2.1 業務の概要」及び「3.1 情報システムの全体構成」を参照し、運用管理作業グループに以下の要員を配置すること。
 - ① 運用管理作業グループ責任者
 - ② 運用管理作業グループ要員
- (2) 運用管理作業グループ責任者
担当するグループの管理業務を遂行するために必要な見識、スキル及び経歴を有し、「IT スキル標準 v3」において達成度指標及びスキル熟成度ともにレベル 4 以上に相当する知識経験を有する者を配置すること。
- (3) 運用管理作業グループ要員
担当業務を遂行するために必要な見識、スキル及び経歴を有する者を配置すること。

5.4 作業場所等

- (1) 別紙 1「要件定義書」に記載の当運用業務の実施に必要な機構 ICT 基盤等については、機構で準備し、本調達受託者へ提供する。機構が提供する機構 ICT 基盤等以外の設備、備品及び消耗品(事務用 PC、プリンタ、スキャナ、コピー機等)、連絡等に使用する電話機及び電話回線(一般回線、月々に必要となる電話料金を含む)、並びに作業場所については、必要に応じて本調達受託者の負担と責任において用意すること。
なお、電話番号については、次期運用管理事業者へ同じ電話番号を引き継ぐことができるよう検討し機構へ提案すること。
- (2) システムへのアクセスは、マシン室に設置するコンソール又は本調達受託者の責任において用意する作業場所に設置する機構提供の端末からリモートアクセスにて行うものとし、機構が指定する機器及び作業場所以外からアクセスを行うことは不可とする
- (3) 機構の什器や設備を利用する場合は、事前に機構の承認を得ること。
なお、作業場所について、機構は現地確認を実施することができるものとする。
機構で作業を実施するにあたっては、所定の手続に従って承認を得ること。
- (4) 本調達における業務をクラウド環境を用いて実施することは不可とする。

- (5) 本調達受託者側組織内で作業を行う場合、作業実施場所は、IC カード等電磁的管理による入退室管理がなされていること。

5.5 作業の管理に関する要領

5.5.1 基本事項

- (1) 本調達受託者は、機構が承認した運用実施計画書に基づき、運用業務に係るコミュニケーション管理、要員管理、作業管理、リスク管理、インシデント・問題管理、構成管理、変更管理、リリース管理、情報セキュリティ対策、SLA 管理を行うこと。
- (2) 本調達受託者は、作業の進捗状況等を報告するため、機構の担当職員と会議を定期的に行うこと。また、当該会議の開催の都度、原則 3 営業日以内に議事録を作成し、関係者に内容の確認を行った上で、機構の承認を得ること。
- (3) 情報漏えい、作業計画の大幅な遅延等の問題が生じた場合は、機構にその問題の内容について報告すること。

5.5.2 運用管理業務計画書の作成

運用管理業務における具体的なタスクの定義及びスケジュールを具現化することを目的として、「運用管理業務計画書」を本番稼働日までに作成すること。

5.5.3 運用管理業務及び稼働報告

- (1) 運用管理業務
本調達受託者は、「運用管理業務計画書」に基づき、運用管理業務を実施すること。
- (2) 稼働報告の実施
運用管理業務工程における具体的なタスクの実績及びスケジュールの実績を評価することを目的として、「稼働報告書」を月次で作成、報告すること。

5.5.4 作業上の留意事項

- (1) 関連事業者等、機構以外の者との連絡、依頼、報告等が必要となった場合は、原則として機構を通じて行うこと。ただし、内容や効率を考慮し、直接関連事業者等と調整を実施することが適切と判断した場合は、機構の承認を得た上でこれに従い、適切に状況を報告すること。また、緊急性が高い場合も機構へ事後報告とした上で、直接関連事業者等と調整を実施することを認めるが、その際は「緊急性が高い」と判断できる内容も含めて報告し、機構の承認を得ること。なお、報告の内容から緊急性が高いと機構が認めない場合は、改善提案を提出した上で、機構の承認を得ること。
- (2) 関連事業者等から、照会、進捗等を把握するための資料提出の依頼等があった場合は、機構の承認を得た上で適切に対応すること。
- (3) 受託業務の実施において疑義等が生じた場合は、機構と協議を行い、承認を得た上で実施すること。
- (4) 本調達受託者は、本番環境にて作業を実施するに当たっては、以下の点を踏まえて実施すること。
 - ① 本番作業は実績のある手順に従って実施すること。実績のない手順は、検証環境であらかじめ検証した上で本番環境において作業を実施すること。また、運用業務効率化のため、一部作業を自動化す

るためのツール等の導入を検討し提案すること。

- ② 本番作業に係るスケジュールを作成し、機構の承認を得た上で実行し管理・報告すること。
- ③ 本番作業中の全てのオペレーション業務については、最低限 2 人 1 組での体制で実施すること。

第6章 作業の実施にあたっての遵守事項

6.1 機密保持、情報・資料の取扱い

- (1) 本調達受託者は、受託業務の実施の過程で機構が提供した情報(公知の情報を除く。以下同じ。)、他の調達受託者が提示あるいは作成した情報を、受託業務の目的以外に使用又は第三者に開示若しくは漏えいしてはならないものとし、そのために必要な措置を講ずること。また、契約期間終了後も同等の措置を講ずること。
- (2) 本調達受託者は、受託業務を実施するにあたり、機構から入手した資料等については管理台帳等により適切に管理し、かつ、以下の事項に従うこと。
 - ① 機構の許可なく、複製はしないこと。
 - ② 機構の許可なく、情報を指定した場所から持ち出さないこと。なお、個人情報等の重要な情報が記載された情報・資料に関しては、原則として社外に持ち出さないこと。
 - ③ 本調達受託者の組織内に移送する際は、暗号化や施錠等適切な方法により、情報セキュリティを確保すること。また、機構との調整等に必要な場合及び返却時以外は原則として、本調達受託者の組織外に持ち出さないこと。
 - ④ 本調達受託者の組織内で作業を行う場合には、作業を行う施設は、IC カード等電磁的管理による入退館管理がなされていること。
 - ⑤ 作業を行う施設内の作業実施場所は、IC カード等電磁的管理による入退室管理がなされていること。
 - ⑥ 電磁的に情報・資料を保管する場合には、受託業務に係る体制以外の者がアクセスできないようアクセス制限を行うこと。また、アクセスログにより不審なアクセスがないかの確認を行うこと。
 - ⑦ 電子計算組織及び情報へのアクセスの際に使用するパスワードは、12 文字以上で、英大文字、英小文字、数字、記号のうち 3 種以上を組み合わせる設定をすること。なお、パスワードは文字数が多く推測困難な文字列を使用することとし、「氏名、生年月日等の個人情報」、「法人・会社名を類推できるような文字列」、「キーボード配列に従った文字列」、「規則性のある数を含む文字列」及びこれらの組合せ等の推測可能なパスワードは設定しないこと。
 - ⑧ 情報・資料を保管する端末やサーバ装置等は、本調達受託者の情報セキュリティポリシー等により、サイバー攻撃に備え、ウイルス対策ソフト、脆弱性対策及び検知・監視等の技術的対策が講じられ、適切に管理・運用される必要があるため、「参考資料 2「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」や「日本年金機構情報セキュリティポリシー」に準拠し、管理等することとし、準拠した対応ができない場合は、代替のリスク軽減策を講じ、機構の承認を得ること。
 - ⑨ 受託業務に必要ななくなり次第、速やかに、複製を含めて機構に返却すること。
 - ⑩ 受託業務完了後、機構が提供した情報・資料を削除又は返却し、本調達受託者において該当情報を保持しないことを誓約する旨の書類を機構へ提出すること。
- (3) 機密保持及び情報・資料の取扱いについて、適切な措置が講じられていることを確認するため、機構が遵守状況の報告や実地調査を求めた場合には応じること。
- (4) 本調達の実施にあたり、履行開始の前日までに、別紙 4「守秘義務に関する誓約書」を機構に提出すること。

6.2 遵守する法令等

6.2.1 法令等の遵守

- (1) 「日本年金機構情報セキュリティポリシー」及び「情報セキュリティ対策実施手順書群」の最新版を遵守すること。
なお、「日本年金機構情報セキュリティポリシー」及び「情報セキュリティ対策実施手順書群」は非公表であるが、参考資料 1「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」、参考資料 2「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」及び参考資料 3「政府機関等の対策基準策定のためのガイドライン」に準拠しているため、参照すること。
「日本年金機構情報セキュリティポリシー」及び「情報セキュリティ対策実施手順書群」「日本年金機構個人情報保護管理規程」については、契約締結後、本調達受託者が機構に別紙 4「守秘義務に関する誓約書」を提出した際に開示する。
- (2) 受託業務の実施において、現行情報システムの設計書等を参照する必要がある場合は、作業方法等について機構の指示に従い、別紙 3「資料閲覧申請書兼秘密保持誓約書」を提出の上、参照すること。
なお、作業場所は、機構本部内とすること。
- (3) 本調達受託者は、受託業務の実施において、民法、刑法、著作権法、不正アクセス行為の禁止等に関する法律、行政機関の保有する個人情報の保護に関する法律等の関連する法令、労働基準法、労働安全衛生法等を遵守すること。
- (4) 「日本年金機構情報セキュリティポリシー」又は「情報セキュリティ対策実施手順書群」の改正が行われた場合は、改正点に関する影響調査及び対処方法の検討を行い、対応についての協議に応じること。
- (5) 外部委託開始後速やかに、別紙 6「法令及び契約内容の遵守状況に関する報告書」を提出すること。
また、外部委託を複数年で契約した場合は、外部委託の開始後 1 年を経過するごとに、別紙 6「法令及び契約内容の遵守状況に関する報告書」を提出すること。
- (6) 本調達受託者は、政府機関全体の情報セキュリティ対策を強化・拡充するために策定された、参考資料 2「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」及びこれらの関連資料等の内容を正しく理解し、受託業務の実施に当たり遵守すること。

6.2.2 その他文書、標準への準拠

- (1) 「IT サービス業務標準」及び機構が定める標準類に準拠し作業を遂行すること。ただし、当該標準類で規定する内容に疑義等がある場合は、機構にその理由を説明し、協議の上で作業を実施すること。
- (2) 厚生労働省全体管理組織(PMO)が、機構に対して指導、助言等を行った場合は、その方針に従うこと。

6.3 情報セキュリティ管理

- (1) 本調達案件の応札希望者は、情報セキュリティ対策として、以下を含む情報セキュリティ管理計画書(案)を応札時に提出すること。

また、契約締結後、調達仕様書「4.1.3 障害・情報セキュリティインシデント発生時及び大規模災害等の発災時の対応」、「5.2 管理体制」及び「第 6 章作業の実施にあたっての遵守事項」において記載した情報セキュリティ要件及び以下の要件を満たす情報セキュリティ管理計画書を提出し、機構の承認を受けた上で、それに基づき情報セキュリティ対策を実施すること。なお、機構は実施状況について、随時、実地調査できるものとする。

 - ① 機構から提供する情報の目的外利用を禁止すること。
 - ② 受託業務の実施に当たり、本調達受託者又はその従業員、本業務の役務の内容の一部を再委託する先、若しくはその他の者による意図せざる不正な変更が加えられないための管理体制が整備されていること。
 - ③ 本調達受託者の資本関係・役員等の情報、受託業務の実施場所、受託業務従事者の所属・専門性(情報セキュリティに係る資格・研修実績等)・実績及び国籍に関する情報提供を行うこと。
 - ④ 情報セキュリティインシデントへの対処方法が確立されていること。
 - ⑤ 情報セキュリティ対策その他の契約の履行状況を定期的に確認し、機構へ報告すること。
 - ⑥ 情報セキュリティ対策の履行が不十分であると機構が判断した場合は、1 か月以内に改善策を書面にて提出し、機構の承認を受けた上で実施すること。
 - ⑦ 機構が求めた場合に、速やかに情報セキュリティ監査を受入れること。
 - ⑧ 受託業務の役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるように、「情報セキュリティ管理計画書」に記載された措置の実施を担保すること。
 - ⑨ 機構から要保護情報を受領する場合は、情報セキュリティに配慮した受領方法にて行うこと。
 - ⑩ 機構から受領した要保護情報が不要となった場合は、これを確実に返却、又は抹消し、書面にて報告すること。
 - ⑪ 受託業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、対面や電話等の即時性の高い連絡手段にて当該事故に係る第一報を直ちに機構へ伝達し、必要な対策を講ずるとともに、当該事故への対応状況を書面にて第一報から原則 1 日以内に機構に報告すること。
- (2) 機構へ提示する電子ファイルは事前にウイルスチェック等を行い、悪意のあるソフトウェア等が混入していないことを確認すること。
 - ① 受託業務において導入する通信回線設備、サーバ装置、端末、複合機、特定用途機器、ソフトウェア、周辺機器及び外部電磁的記録媒体は、製造業者名、製造業者の法人番号、製品名及び型番等について、情報セキュリティ管理計画書の一部として、機器等リストにより、提案書の提出期限の 15 営業日前までに提出すること。提出された機器等リストについて、機構がサプライチェーンに係る懸念が払拭されないと判断した場合には、当該リスクに対応するため、代替品又はリスク低減対策の提出を求めることがあるので留意すること。なお、機器等リストの機器等を変更する場合には、事前に機構に申請し、承認を得ること。
- (3) 情報セキュリティポリシーに基づき、各環境のクリーニングを実施すること。なお、各環境のクリーニング

結果の証跡については、重要なパスワードファイル等が完全に削除されていることを証明するとともに、機構職員が容易に確認可能な形式で提示すること。

- (4) 以下のリスクに対する対策が確立されていること。
 - ① 業務利用場所の入退室における内部不正(持ち出し、持込み)リスク
 - ② 個人情報等を記録した各種媒体の取扱いに係る内部不正リスク

6.4 監査

6.4.1 監査に関する事項

- (1) 本調達受託者は、機構から立入監査の実施を求められた場合は、予告・無予告に関わらずこれに協力すること。立入監査は履行前、履行中、履行後にそれぞれ行うことがある。
また、複数年契約の場合、履行中の立入監査は1年ごとに行う。
- (2) 本調達受託者は、機構が要求した監査項目を準拠できていることが確認できる書類を可能な限り機構へ提出すること。
- (3) 前項において、本調達受託者の社内規程等のため、書類の提出ができない場合においても、機構が当該書類の閲覧を求めた場合はこれに応じること。
- (4) 再委託先並びに再委託先から更に業務を委託する第三者においても(1)～(3)が適用される。
- (5) 機構が本調達受託者の再委託先等への立入監査を求めた場合、本調達受託者は再委託先等に協力させること。

6.4.2 情報セキュリティ監査

- (1) 受託業務の遂行における情報セキュリティ対策の履行状況を確認するために、機構が情報セキュリティ監査の実施を必要と判断した場合は、機構がその実施内容(監査内容、対象範囲、実施者等)を定めて、情報セキュリティ監査を行う(機構が選定した事業者による外部監査を含む)。
- (2) 本調達受託者は、機構から監査等の求めがあった場合に、速やかに情報セキュリティ監査を受け入れる部門、場所、時期、条件等を「情報セキュリティ監査対応計画書」等により提示し、監査を受け入れること。
- (3) 本調達受託者は自ら実施した外部監査についても機構へ報告すること。
- (4) 情報セキュリティ監査の実施については、これらに記載した内容を上回る措置を講ずることを妨げるものではない。
- (5) 業務履行後において当該業務に関する情報漏えい等が発生した場合であっても、監査を受け入れること。

6.5 履行完了後の資料の取扱い

本調達受託者は、機構から提供した資料又は機構が指定した資料の履行完了後の取扱い(返却・削除等)について、本仕様書の定めその他、機構の指示に従うこと。

6.6 通報窓口の周知

機構では、本調達受託者の社員等からの通報を受け付ける専用窓口を設置しているので、以下の内容を社内で説明・周知すること。

- ・ 機構では、契約の適正な履行の確保を目的として、本調達受託者に契約違反がある場合に、本調達受託者の社員等からの通報を受け付けることができるよう専用窓口を設置しています。
- ・ 今般、貴社との契約を締結しましたので、当該契約について、今後、不適正な業務の実施が確認された場合又は疑われる場合がありますら、専用窓口までご連絡ください。
- ・ (通報窓口)日本年金機構へのご意見・ご要望
 - ① ホームページの場合 機構ホームページの「日本年金機構へのご意見・ご要望」の投稿フォームにより受け付けています。 <https://www2.nenkin.go.jp/do/mail/>
 - ② 郵送の場合 〒168-8505 東京都杉並区高井戸西 3-5-24 日本年金機構「日本年金機構へのご意見・ご要望の手紙」宛てにお送りください。

第7章 成果物の取扱いに関する事項

7.1 知的財産権の帰属

- (1) 受託業務における成果物の著作権及び二次的著作物の著作権(著作権法第 21 条から第 28 条までに定める全ての権利を含む。)は、本調達受託者が調達の実施の従前から権利を保有していた等の明確な理由により、あらかじめ知的財産の帰属に係る表明書にて権利譲渡不可能と示されたもの以外は、全て機構に帰属するものとする。なお、当該表明書は応札時に提案書と併せて提出すること。
- (2) 機構は、成果物について、第三者に権利が帰属する場合を除き、自由に複製し、改変等し、及びそれらの利用を第三者に許諾すること(以下、「複製等」という。)ができるとともに、任意に開示できるものとする。また、本調達受託者は、成果物について、産業技術力強化法(平成 12 年法律第 44 号)に基づき、複製等ができるものとする。ただし、成果物に第三者の権利が帰属する時や、複製等により機構がその業務を遂行する上で支障が生じるおそれがある旨を契約締結時までに通知したときは、この限りでないものとし、この場合には、複製等ができる範囲やその方法等について協議するものとする。
- (3) 受託業務の範囲内で作成されたツール等のプログラムに調達に関する権利(著作権法第 21 条から第 28 条に定める全ての権利を含む。)及び著作物の所有権は、機構から本調達受託者に対価が完済された時、本調達受託者から機構に移転するものとする。なお、「対価が完済された時」の判断は、機構と協議の上、決定する。
- (4) 納品される著作物等に、第三者が権利を有する著作物(以下、「既存著作物等」という。)が含まれる場合には、本調達受託者は、当該既存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関わる全ての手続きを行うこと。この場合、本調達受託者は、当該既存著作物の内容について事前に機構の承認を得ることとし、機構は、既存著作物等について当該許諾条件の範囲で使用するものとする。
- (5) 本調達受託者は機構に対し、一切の著作者人格権を行使しないものとし、また、第三者をして行使させないものとする。

7.2 検査

本調達受託者は、機構の指示に従い納品検査を受けるものとする。

- (1) 成果物は、「表 4.2.1.1 納品成果物一覧」に示す納品時期に、「4.2.4 納品場所」に指定する場所に納品すること。その際、運用実施計画書内で定めた品質保証の手順に沿った成果物を提出すること。
- (2) 検査の結果、成果物の全部又は一部に不合格品が生じた場合には、成果物を直ちに引き取り、必要な修復を行った後、指定した日時までに修正が反映された全ての成果物及び品質保証の状態を確認できる資料を納品すること。
- (3) 「4.2.1 納品成果物等」に記載された以外にも、必要に応じて成果物の提出を求める場合があるので、作成資料は常に管理し、最新状態に保っておくこと。
- (4) 特段の事情がない限り、本調達受託者においても全数検査又はサンプル検査を行うこと。

7.3 契約不適合責任

- (1) 機構は、「7.2 検査」に規定する納品検査に合格した成果物が契約の内容に適合していないこと(以下、「契約不適合」という。)を検査完了した日から1年以内に(数量又は権利の不適合については期間制限なく)その旨を本調達受託者に通知した場合は、次の①、②のいずれかを選択して請求することができ、本調達受託者はこれに応じなければならない。なお、機構は、本調達受託者に対して②を請求する場合において、事前に相当の期間を定めて本項の履行を催告することを要しないものとする。
 - ① 機構の選択に従い、機構の指定した期限内に、本調達受託者の責任と費用負担により、他の良品との引換え、修理又は不足分の引き渡しを行うこと。
 - ② 直ちに代金の減額を行うこと。
- (2) 機構は、前項の通知をした場合は、上記①、②に加え、本調達受託者に対する損害賠償請求及び本契約の解除を行うことができる。
- (3) 本調達受託者が契約不適合について知り若しくは重大な過失により知らなかった場合、又は契約不適合が重大である場合は、上記(1)の責務期間を経過した後においてもなお上記(1)、(2)を適用するものとする。

第8章 入札参加資格に関する事項

8.1 入札参加要件

8.1.1 公的な資格や認証等の取得

プライバシーマーク付与認定、ISO/IEC27001 認証(国際標準規格)、JIS Q 27001 認証(日本産業規格)のうち、いずれかを取得していること。

また、応札時、そのいずれかの認証の写しを提出すること。

8.1.2 受託実績

過去 3 年以内に、全国 400 拠点超に展開するオンラインシステム(PC20,000 台、サーバ 500 台超)の運用管理業務を行った実績があること。また、具体的な実績については、提案書に記載又は添付すること。

8.1.3 履行可能性審査に関する要件

提案書に以下の事項を記載又は添付すること

- (1) 受託業務及び情報セキュリティ管理の履行可能性を証明するため、以下の書類を提出すること。なお、提出された計画書(案)において履行可能性を認めることができないと機構が判断した場合は、入札に参加することはできない。
 - ① 本仕様書に基づいた「運用実施計画書(案)」
なお、IT サービスマネジメントのフレームワーク(ITIL 等)を参考に作成すること。
 - ② 「6.3 情報セキュリティ管理」に基づいた「情報セキュリティ管理計画書(案)」
なお、受託業務で取り扱う情報等の特性を十分に踏まえて作成したものであること
- (2) 障害対応等により機構が本調達受託者へ緊急招集を要請した場合は、「4.2.4 納品場所」に示す成果物の納品場所に、本調達を管理可能な管理者やリーダ相当の者が、2 時間以内に参集すること。また、2 時間以内に参集可能であることを証明する書面を添付すること(様式任意)。
- (3) 「5.3 作業要員に求める資格等の要件」に示す、作業要員の実績、経験年数及び本調達のプロジェクトに参画することを証明する体制図等を記載すること。各責任者及び各管理者について、氏名を記載すること。また、各要員が有する資格の証明書を添付すること。

8.2 入札制限

本件調達の公平性を確保するため、参加者は、以下に挙げる事業者並びにこの事業者の「財務諸表等の用語、様式及び作成方法に関する規則」(昭和 38 年大蔵省令第 59 号)第 8 条に規定する親会社及び子会社、同一の親会社を持つ会社及び委託先事業者等の緊密な利害関係を有する事業者でないこと。

- (1) 「厚生労働省全体管理組織(PMO)の支援【調達支援等】一式」(本調達の契約日の属する年度の前々年度以降)の受託者
- (2) 「日本年金機構におけるシステム支援等業務」(本調達の契約日の属する年度の前々年度以降)の受託者
- (3) 「社会保険オンラインシステム監査に係る外部委託」(本調達の契約日の属する年度の前々年度以降)の受託者

- (4) 「日本年金機構における情報セキュリティ監査に係る支援業務」(本調達の契約日の属する年度の前々年度以降)の受託者
- (5) 「日本年金機構における最高情報セキュリティアドバイザー及び情報セキュリティ対策支援等業務」(本調達の契約日の属する年度の前々年度以降)の受託者

第9章 再委託に関する事項

9.1 再委託の制限及び再委託を認める場合の条件

本調達受託者は、受託業務の全部又は受託業務における総合的な企画及び判断並びに業務遂行管理部分を第三者(本調達受託者の子会社(会社法第2条第3号に規定する子会社をいう。)を含む。)に再委託することはできない。また、受託業務の契約金額に占める再委託金額の割合は、原則2分の1未満とすること。

本調達受託者は、知的財産権、情報セキュリティ(機密保持及び遵守事項、ガバナンス等)に関して本仕様書が定める本調達受託者の債務を、再委託先も負うよう必要な処置を実施すること。また、再委託先の対応について最終的な責任を本調達受託者が負うこと。

なお、本件受託業務における受託業務における総合的な企画及び判断並びに業務遂行管理部分との分類を、「表 9.1.1 再委託不可部分と再委託可能部分」に示す。

表 9.1.1 再委託不可部分と再委託可能部分

項番	業務分類	作業概要
1	再委託不可部分 (総合的な企画・判断、業務遂行管理)	・「4.1.1 運用管理に係る業務」の全体統括役務
2	再委託可能部分 (総合的な企画・判断、業務遂行管理 以外)	・「4.1.1 運用管理に係る業務」の役務の内、全体統括以外の役務 ・その他、上記記載の作業に付帯する作業

9.2 承認手続

- (1) 受託業務の一部を再委託する場合は、あらかじめ再委託先の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性及び契約金額について記載した別紙7「再委託等に係る承認申請書」を提出し、承認を得ること。なお、再委託先は「8.2 入札制限」の対象となる事業者ではないこと。
- (2) 当初申請内容に変更が生じた場合は、別紙7「再委託等に係る承認申請書」を提出すること。
- (3) 再委託先から更に第三者に委託が行われる場合は、再委託と同様に当該第三者の商号又は名称、住所並びに委託を行う業務の範囲等を記載した履行体制図を提出すること。
- (4) 機構からの承認通知を受領した日から2週間以内に、申請書のとおり再委託(又は再委託先から更に第三者への委託)が行われていることを証明するため、本調達受託者は別紙8「受託証明書」を再委託先(又は再委託先から更に委託した先)から徴取し機構へ提出すること。

第10章 その他特記事項

10.1 前提条件及び制約条件

10.1.1 情報セキュリティに関する第三者評価の認証を証明できる書類の提出

本調達受託者が受託業務開始前に機構へ提出した情報セキュリティに関する第三者評価の認証を証明できる書類(プライバシーマーク、ISO/IEC 27001 又は JIS Q 27001 の写し)において、契約期間中にその認証期間が切れる場合、本調達受託者は、その認証期間を更新すること。

本調達受託者は、認証終了日から1か月以内に、情報セキュリティに関する第三者評価の認証期間が更新されたことが証明できる書類の写しを機構に提出すること。

10.1.2 仕様書等の明確化等

- (1) 業務の処理方法等、別途委託要領に定めがある場合は同要領によることとする。
- (2) 調達仕様書等では業務の処理方法が一義に定まらない事項があることを把握したとき、又は調達仕様書等には定めがないが判断を要する事項があるときには、機構と本調達受託者は協議の上、調達仕様書等の不明瞭な点を明確にするための書面を速やかに取り交わすこととする。
- (3) 前項の書面の取り交わしが完了するまでの間の対応方法については、機構と本調達受託者が協議の上決定することとする。

10.1.3 本調達受託者の能力を生かした自由な提案

本調達受託者は調達仕様書で定める仕様を遵守することを前提に、プロジェクト管理手法、運用管理作業を効率化するツール等の提案を行うことを可とする。

10.1.4 実績及び評価結果の公表

機構は、委託業務の終了後、当該業務の実績及び評価結果(本調達受託者名及び契約実績額等を含む。)を機構のホームページにより公表することがある。

10.2 環境への配慮

- (1) 調達に係る納品物については、「国等による環境物品等の調達の推進等に関する法律(グリーン購入法)」に基づいた製品を可能な限り導入すること。
- (2) 納品する機器については、性能や機能の低下を招かない範囲で、消費電力節減、発熱対策、騒音対策等の環境に対する配慮を行うこと。

10.3 事前現地調査

応札を希望する事業者で、現地調査を希望する場合は、「1.10 連絡先」に示す申請窓口まで申込みの連絡を行うこと。

(1) 現地調査実施条件

- ① 現地調査を希望する者は、「8.2 入札制限」に該当せず、「8.1 入札参加要件」を満たしており、当該入札に参加する予定の者又は予定の法人に勤務する者とする。

- ② 現地調査を希望する場合は、別紙 9「現地調査申込書兼守秘義務誓約書」を提出すること(当日の提出で可)。
- ③ 現地調査実施場所
機構が指定する場所
- (2) 現地調査実施日時
調査可能期間:機構が別途指定する(土日祝日を除く)
調査可能時間:10:00 から 17:00 まで(12:00 から 13:00 までを除く)
- (3) 現地調査実施手順
 - ① 調査希望日の 3 営業日前までに希望日時を申請窓口に連絡する。希望日が複数社で重複した場合は、機構において調整を行うのでその指示に従うこと。
なお、希望日時に応じられない場合がある。
 - ② 指定された日時に現地調査場所で、「現地調査申込書兼守秘義務誓約書」の確認及び調査実施者の本人確認を行う。
 - ③ 調査実施者の本人確認は、社員証等、入札予定法人等の社員であることが確認できるもので行う。
 - ④ 調査には機構の職員が立ち会うので、調査実施者はその指示等に従うこと。
 - ⑤ 調査場所にはカメラ等の撮影機器及びパソコン等記録媒体は持ち込めない。
また、調査時に複写又は写真撮影等を禁止する。違反行為があった場合は、機構は調査を中止、退去を求める場合がある。
- (4) 留意事項
 - ① 現地調査人数は 1 事業者あたり 5 名以内とすること。
 - ② セキュリティ上の理由により、立入りを制限する区域があること。

10.4 その他

- (1) 本調達受託者は、デジタル・ガバメント推進に係る政府の各種施策・方針等(今後出されるものを含む)に従うこと。なお、変更に係る対応については、機構及び本調達受託者にて協議を行うものとする。
- (2) 電磁的記録媒体の受渡し及び移送に際し、参考資料 4「電子政府推奨暗号リスト」に掲載された暗号化方式等を利用し、パスワードの設定を行うこと。
- (3) 受託業務の重要事項に関し、機構から代表者又はそれに代わる者の会議体への出席の指示があった場合はその指示に従うこと。

第11章 附属文書

11.1 要件定義書

別紙 1「要件定義書」を参照すること。

11.2 参考資料

調達仕様書に記載の各府省で公表されている各種施策方針については、下の資料を参照すること。

また、各府省で公表されている各種施策方針及びガイドラインについても必要に応じて確認すること。

- 参考資料1 「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」
<https://www.cyber.go.jp/policy/group/general/kijun.html>
- 参考資料2 「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」
<https://www.cyber.go.jp/pdf/policy/general/kijyunr7.pdf>
- 参考資料3 「政府機関等の対策基準策定のためのガイドライン」
https://www.cyber.go.jp/pdf/policy/general/guider7_9.pdf
- 参考資料4 「電子政府推奨暗号リスト」
<https://www.cryptrec.go.jp/list.html>
- 参考資料5 「国等による環境物品等の調達の推進等に関する法律(グリーン購入法)」
<https://laws.e-gov.go.jp/law/412AC1000000100/>
- 参考資料6 「デジタル社会推進標準ガイドライン」
https://www.digital.go.jp/resources/standard_guidelines
- 参考資料7 「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」
https://www.cyber.go.jp/pdf/policy/general/SBD_manual.pdf

11.3 応札希望者が閲覧できる資料一覧表

入札期間中に開示予定の、事業者が閲覧できる資料を以下に示す。

- ① 業務委託及び機器等の購入における情報セキュリティ対策実施手順書
- ② マシン室に関する資料
- ③ 現行システム設計書
- ④ 日本年金機構セキュリティパッチ適用基準書
- ⑤ 脆弱性対策計画(セキュリティパッチ適用)の実施手順書
- ⑥ 情報セキュリティ要件確認実施要領
- ⑦ 定期点検対象装置一覧
- ⑧ 作業指示書処理フロー
- ⑨ 管理対象装置一覧
- ⑩ 関連事業者一覧
- ⑪ 作業単価表
- ⑫ 保守対象拠点一覧
- ⑬ 管理対象ソフトウェア一覧
- ⑭ IT サービス業務標準

11.4 閲覧要領

応札を希望する事業者で本調達に係る資料について閲覧を希望する場合は、「1.10 連絡先」に示す申請窓口に連絡の上、事前に閲覧の許可を得ること。

(1) 閲覧条件

- ① 閲覧する者は、「8.2 入札制限」に該当せず、「8.1 入札参加要件」を満たしており、当該入札に参加する予定の者、又は当該入札に参加する予定の法人に勤務する者とする。
- ② 閲覧を希望する場合は、別紙 3「資料閲覧申請書兼秘密保持誓約書」を提出すること(閲覧日当日の提出で可)。

(2) 閲覧場所

東京都杉並区高井戸西 3-5-24

日本年金機構本部(高井戸)構内の指定場所

※機構の都合により閲覧場所を変更する場合がある。

(3) 閲覧日時

閲覧可能期間:官報公告日から提案書作成要領に示す日まで(土、日、祝祭日を除く)

閲覧可能時間:10:00 から 17:00 まで(12:00 から 13:00 までの時間帯を除く)

(4) 閲覧手順

- ① 閲覧希望日の 3 営業日前までに希望日時を申請窓口連絡する。希望日が複数社で重複した場合は、機構において調整を行うのでその指示に従うこと。
なお、希望日時に応じられない場合がある。
- ② 指定された日時に閲覧場所で、別紙 3「資料閲覧申請書兼秘密保持誓約書」の確認、及び閲覧者の本人確認を行う。別紙 3「資料閲覧申請書兼秘密保持誓約書」については、閲覧期間中に一度提出すれば閲覧日ごとに提出する必要はない。
- ③ 閲覧者の本人確認は、社員証等、入札予定法人等の社員であることが確認できるもので行う。
- ④ 閲覧には機構の職員が立ち会うので、閲覧者はその指示等に従うこと。
- ⑤ 閲覧場所にはカメラ等の撮影機器及びパソコン等の記録媒体は持ち込めない。
また、閲覧時に複写、又は写真撮影等を禁止する。違反行為があった場合は、機構は閲覧を中止、退去を求める場合がある。
- ⑥ 閲覧資料の内容についての質問の受付期限は提案書作成要領に示す日までとし、提案書作成要領に示す日までに回答する。

11.5 提案書等の審査要領

提案書等の審査は、提案された内容及び「総合評価基準書」に基づいて行うものとする。

11.6 契約締結後に開示する資料

契約締結後に開示する資料は以下のとおりである。

- ① 日本年金機構情報セキュリティポリシー
- ② 日本年金機構個人情報保護管理規程
- ③ 情報システムの主体認証方式に係る基準書
- ④ 本調達業務遂行に必要なとなる機構が定める規定及び実施手順等

⑤ 「11.3 応札希望者が閲覧できる資料一覧表」に示す資料

機構 ICT 基盤運用管理サービス等業務

要件定義書

令和 8 年 10 月
日本年金機構
システム運用部

目 次

第 1 章	調達件名	1
第 2 章	業務要件の定義	1
2.1	業務の概要	1
2.2	業務要件の対象システム	2
2.3	時間	3
2.3.1	稼働日	3
2.3.2	運用管理業務の時間	3
2.3.3	計画停止	3
第 3 章	非機能要件の定義	4
3.1	情報システムの全体構成	4
3.1.1	運用対象システムの範囲	4
3.2	アクセスに関する事項	6
3.2.1	運用対象システムへの接続要件	6
3.3	規模に関する事項	6
3.3.1	利用者数	6
3.3.2	拠点数	6
3.3.3	業務量	6
3.3.4	従事要員数	7
3.3.5	提供機能利用先システム	7
3.4	継続性に関する事項	8
3.4.1	サービス停止の対応	8
3.4.2	障害の復旧	8
3.5	情報システム稼働環境に関する事項	8
3.5.1	環境種別の定義	8
3.5.2	ハードウェア構成	9
3.5.3	ソフトウェア構成	10
3.6	引継ぎに関する事項	10
3.6.1	現行運用管理事業者からの運用管理業務の引継ぎ	10
3.6.2	次期運用管理事業者への引継ぎ	10

3.7	教育に関する事項	11
3.7.1	習得訓練.....	11
3.7.2	情報セキュリティ研修.....	12
3.7.3	研修の評価と報告.....	12
3.8	運用条件	12
3.8.1	本調達受託者が設置する運用監視拠点	12
3.8.2	システム監視環境等の用意	12
3.8.3	システムへのアクセス方法(機構が貸与する機器等の使用場所).....	13
3.8.4	作業上の留意事項.....	13
第 4 章	運用に関する事項	14
4.1	運用に関する基本方針.....	14
4.2	役割分担/体制	14
4.3	運用管理業務プロセスの見直し	15
4.3.1	留意事項.....	15
4.4	事前準備作業.....	15
4.4.1	事前準備作業の定義.....	15
4.4.2	事前準備作業の概要.....	15
4.4.3	事前準備作業計画書の作成	15
4.4.4	習得訓練.....	16
4.4.5	運用監視拠点構築.....	16
4.4.6	定例報告.....	16
4.4.7	ドキュメント作成	16
4.5	運用管理業務.....	18
4.5.1	拠点装置運用管理.....	19
4.5.2	センタ運用管理	25
4.5.3	ヘルプデスク	28
4.5.4	運用統制管理	30
4.5.5	定例外作業の取扱い.....	32
4.6	プロジェクト管理	33
4.6.1	コミュニケーション管理.....	33
4.6.2	品質管理.....	33
4.6.3	インシデント管理.....	33
4.6.4	問題管理.....	33
4.6.5	変更管理.....	33
4.6.6	リリース管理	34

4.6.7	リスク管理.....	34
4.6.8	情報セキュリティ管理.....	34
4.6.9	構成管理・ドキュメント管理業務	34
4.6.10	要員管理.....	36
4.6.11	稼働状況管理	37
4.6.12	SLA 管理.....	40
4.7	業務終了	43
4.7.1	次期運用管理事業者への引継ぎ	43
4.7.2	最終報告書	43

第1章 調達件名

機構 ICT 基盤運用管理サービス等業務

第2章 業務要件の定義

2.1 業務の概要

本調達受託者は、「図 2.1.1 機構 ICT 基盤運用管理業務の対象範囲」に示す運用管理業務を行うこと。

また、各運用管理区分における管理対象を「表 2.1.1 運用管理業務の対象機器」に示す。

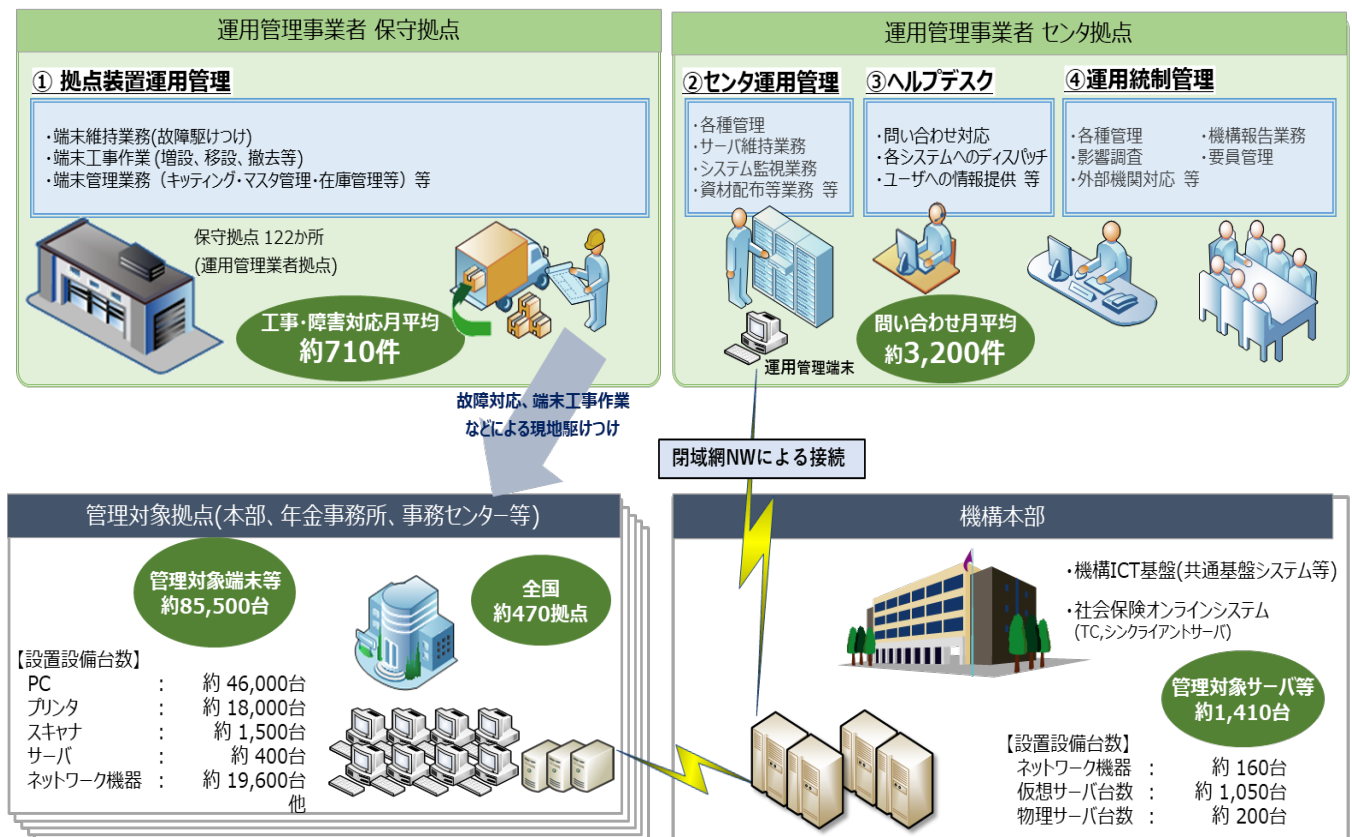


図 2.1.1 機構 ICT 基盤運用管理業務の対象範囲

表 2.1.1 運用管理業務の対象機器

項番	運用管理業務区分	対象機器
1	①拠点装置運用管理	管理対象拠点(本部、年金事務所、事務センター等)に設定の管理対象端末等(以下「拠点装置」という。)
2	②センタ運用管理	機構本部設置の管理対象サーバ等、拠点端末及び通信ネットワーク
3	③ヘルプデスク	機構本部設置の管理対象サーバ等、拠点端末及び通信ネットワーク
4	④運用統制管理	機構本部設置の管理対象サーバ等、拠点端末及び通信ネットワーク

2.2 業務要件の対象システム

本調達受託者は、「表 2.2.1 運用対象システム」に示すシステム(以下、「運用対象システム」という。)を対象とする。各システムにはそれぞれ運用管理事業者が配されているが、本調達受託者はそれらについても問い合わせにかかる連携を行う。

また表内右側の本調達受託者の役務範囲における各役務の詳細は、「4.5 運用管理業務」に示す。

表 2.2.1 運用対象システム

項番	対象システム	運用管理事業者	本調達受託者の役務範囲			
			拠点装置運用管理	センタ運用管理	ヘルプデスク※	運用統制管理
1	ICT 基盤(共通基盤システム等)	本調達受託者	-	○	○	○
2	ICT 基盤(拠点端末設備等)	本調達受託者	○	-	○	○
3	経過管理電子決裁システム	共通運管	-	-	○	-
4	経過管理電子決裁システム(拠点設置機器)	共通運管	-	-	○	-
5	TV 会議システム	本調達受託者	-	○	○	-
6	TV 会議システム(拠点機器)	本調達受託者	○	-	○	-
7	公的年金給付総合情報連携システム	統合運管	-	-	○	-
8	公的年金給付総合情報連携システム(拠点機器)	本調達受託者	○	-	○	○
9	年金給付システム	給付運管	-	-	○	○
10	年金給付システム(拠点機器)	本調達受託者	○	-	○	○
11	お客様対応業務システム	統合運管	-	-	○	-
12	紙台帳検索システム	統合運管	-	-	○	-
13	源泉徴収サブシステム	統合運管	-	-	○	-
14	受付進捗管理システム	統合運管	-	-	○	-
15	障害年金業務支援システム	統合運管	-	-	○	-
16	番号業務事務システム	共通運管	-	-	○	-
17	統計業務システム	共通運管	-	-	○	-
18	間接業務システム	間接・MACS 運管	-	-	○	-
19	MACS システム	間接・MACS 運管	-	-	○	-
20	基礎年金番号管理システム	維持SI	-	-	○	-
21	記録管理システム	維持SI	-	-	○	-
22	収納対策支援システム	維持SI	-	-	○	-
23	歳入金電子納付システム	維持SI	-	-	○	-
24	電子申請システム	三鷹統合運管	-	-	○	-
25	厚年適用業務支援システム	三鷹統合運管	-	-	○	-
26	ねんきんネットシステム	ねんきんネット運管	-	-	○	-
27	オンライン事業所年金情報サービス	ねんきんネット運管	-	-	○	-
28	ICT 基盤(情報業務システム等)	機構 ICT 基盤(情報業務システム等)	-	-	○	-

※:本調達受託者対応範囲外のシステムについては、受け付けた問い合わせ内容を担当の運用管理業者へ連携する。

【凡例】

○:本調達受託者の作業対象

-:本調達受託者の作業対象外

2.3 時間

運用対象システムの稼働日の考え方、運用管理業務時間を以下に示す。

2.3.1 稼働日

運用対象システムの稼働日は、「表 2.3.1.1 稼働日」のとおりである。

表 2.3.1.1 稼働日

項番	稼働日	項目説明
1	平日	月曜から金曜日まで(12 月 29 日～1 月 3 日を除く。)
2	第 2 土曜日	毎月第 2 土曜日はオンライン稼働日とする。
3	特定日	年金の日(11 月 30 日)が、土日の場合。

※ 運用対象システムごとに稼働日が変更になる場合もあるため、変更時においては、機構と協議の上、対応すること。

2.3.2 運用管理業務の時間

運用対象システムの運用時間帯について、「表 2.3.2.1 運用管理業務の時間帯」に示す。

表 2.3.2.1 運用管理業務の時間帯

項番	大分類	運用時間	
1	拠点装置(端末・プリンタ・LAN 環境等)の維持、運用	平日	8:00～18:00
		第 2 土曜日	8:30～17:00
2	センタ設置機器(サーバ機器)の維持、運用	平日	7:30～22:00
		第 2 土曜日及び特定日	7:30～22:00
		非稼働日	8:00～21:30
3	現地拠点(利用拠点)からの問合せ対応	平日	8:15～20:00
		(ヘルプデスク稼働時間※	7:30～20:30)
		第 2 土曜日	8:15～17:00
		(ヘルプデスク稼働時間※	7:30～17:30)
		特定日	8:15～17:00
		(ヘルプデスク稼働時間※	7:30～17:30)
4	運用統制管理業務	平日	7:30～18:00

※ ヘルプデスク稼働開始時間は受付準備、照会内容の情報共有の時間をとるため早めており、終了時間については終了時間間際の照会受付や照会情報入力を実施する時間確保するためである。

2.3.3 計画停止

運用対象システムの計画停止は、センタ設備(本番環境及び稼働維持環境)における定期点検の際に本調達受託者にて実施する。計画停止を安全に実施するため作業計画書の変更が必要な場合は、機構及び関連事業者(閲覧資料「関連事業者一覧」参照)との調整を行い実施すること。なお、法定点検においては、運用対象システム機器の電源遮断、再起動、動作確認に関する作業計画書を策定の上、実施すること。

第3章 非機能要件の定義

3.1 情報システムの全体構成

3.1.1 運用対象システムの範囲

本調達における運用の対象範囲を「図 3.1.1.1 運用対象システムの範囲」に示す。

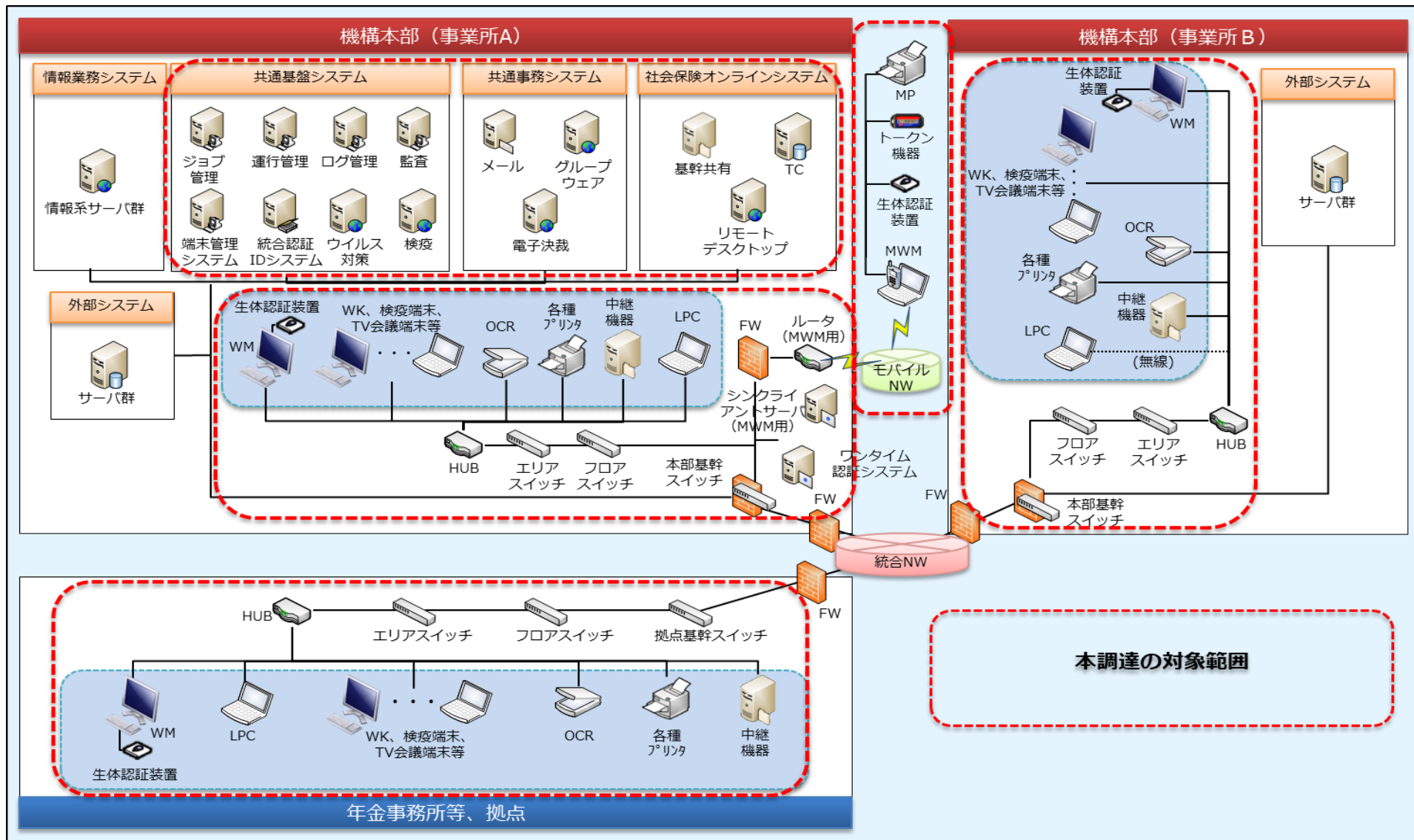


図 3.1.1.1 運用対象システムの範囲

3.2 アクセスに関する事項

3.2.1 運用対象システムへの接続要件

運用対象システムの運用・保守を実施する際は、「表 3.2.1.1 運用対象システムへの接続要件」に従うこと。運用管理業務を実施する上で、決められた以外の場所や権限のない者からの接続を防止するため、接続要件に従い接続すること。また、本調達受託者にて準備する作業場所は、機構との閉域網ネットワークで接続し、機密性を確保すること。

表 3.2.1.1 運用対象システムへの接続要件

項番	要件	内容
1	運用対象システムへの接続	運用対象システムへの接続は、マシン室(機構本部 A)に設置するコンソール又は本調達受託者の責任において準備する運用監視拠点に設置の運用管理端末から、リモート接続にて行うこと。
2		各機器(サーバ、端末、ネットワーク等)に接続する際に利用する管理者権限については、日本年金機構セキュリティポリシーにのっとり、パスワードの設定を行うこと。

3.3 規模に関する事項

3.3.1 利用者数

本運用対象システムの利用者想定数は、「表 3.3.1.1 利用者想定数」のとおりである。

表 3.3.1.1 利用者想定数

項番	利用者想定数
1	約 47,000 人

3.3.2 拠点数

本運用対象システムの利用及び保守対象とする拠点名、拠点数を「表 3.3.2.1 利用拠点」に示す。

表 3.3.2.1 利用拠点

項番	拠点名	拠点数
1	本部	5 か所
2	事務センター	15 か所
3	年金事務所(分室含む)	322 か所
4	中央年金センター	2 か所
5	障害年金センター	1 か所
6	年金相談センター	81 か所
7	コールセンター	7 か所
8	厚生局、厚生労働省年金局	17 か所
9	国税局	12 か所
10	他(協会けんぽ、企業年金連合会、市場化事業者)	5 か所

(1) 対象拠点

受託業務に関する対象拠点については、閲覧資料「保守対象拠点一覧」に示す。なお、組織再編等により、拠点数等の増減が発生する可能性があるが、本調達受託者は追加された拠点に関しても運用管理業務を実施すること。

3.3.3 業務量

本運用対象システムの業務にあたり、参考情報として主な運用業務量を「表 3.3.3.1 業務量一覧」に示す。

表 3.3.3.1 業務量一覧

項番	運用管理業務	月間平均件数
1	ヘルプデスク呼数	3,200 件
2	ヘルプデスク応答数	2,624 件
3	ヘルプデスクメール照会数	730 件
4	センタ運用(パッチ配布業務)	38 件
5	センタ運用(データ復旧)	38 件
6	センタ運用(イベント対応)	95 件
7	センタ運用(ウイルス検知)	50 件
8	拠点装置運管(故障対応)	490 件
9	拠点装置運管(工事件数)	220 件
10	運用統制(問合せ管理)	450 件
11	定例外作業(非定型)	5 件

3.3.4 従事要員数

本運用対象システムの業務にあたり、参考情報として要員数(作業工数ではない)を「表 3.3.4.1 従事要員数(参考値)」に示す。

表 3.3.4.1 従事要員数(参考値)

項番	運用管理業務区分	要員数(人)	
		センタ要員	拠点要員
1	拠点装置運用管理	34	717(※)
2	センタ運用管理	139	—
3	ヘルプデスク	19	—
4	運用統制管理	36	—

※拠点要員は、他顧客の業務を兼務している。

3.3.5 提供機能利用先システム

共通基盤システムでは機構のシステムに対し、機能提供(「表 3.3.5.1 提供機能一覧」参照)を行っており、参考情報として機能提供先のシステム(外部システム)について「表 3.3.5.2 外部システム一覧」に示す。今後、提供先システムが増加する場合は、同様に対象とすること。

表 3.3.5.1 提供機能一覧

項番	機能	機能概要
1	統合認証 ID 管理機能 (人事異動管理機能)	機構のシステムを利用する人事・利用者情報の申請、承認等機能
2	統合認証 ID 管理機能 (アクセス権管理機能)	アクセス権管理認証機能
3	監査機能	機能提供先システム上のサーバやネットワーク機器等に対する特権 ID での操作証跡の取得機能
4	端末管理機能	管理対象装置に対するパッチ、パッケージ等ファイル資材の配布。構成情報の収集、遠隔操作機能
5	運行監視機能	サーバ、ネットワーク機器に対する機器の稼働状況監視及び稼働状況の情報蓄積管理
6	ウイルス対策機能	機器のウイルススキャン(スケジュール/リアルタイム)、検出、ウイルス隔離機能

表 3.3.5.2 外部システム一覧

項番	機能/更改予定 外部システム	人事異動 管理機能	アクセス権 管理機能	監査機能	端末管理 機能	運用監視 機能	ウイルス 対策機能	(参考情報) 更改予定時期
1	機構 ICT 基盤(情報業務システム等)	○	×	×	×	×	×	—
2	TV 会議システム	×	○	○	○	○	○	未定
3	年金給付システム(周辺サーバ含む)	○	○	○	○	×	○	—
4	統計・業務分析システム	×	○	○	○	×	○	令和 12 年 4 月
5	経過管理・電子決裁システム	○	○	○	○	×	○	令和 11 年 4 月
6	個人番号管理システム	○	○	○	○	×	○	令和 12 年 4 月
7	受付進捗管理システム	○	○	○	○	×	○	—
8	障害年金業務支援システム	○	○	○	○	×	○	—
9	個人番号管理情報連携サブシステム	×	○	○	○	×	○	令和 12 年 4 月
10	年金情報総合管理・照合システム	○	○	○	○	×	○	—
11	公的年金給付総合情報連携システム	○	○	○	○	×	○	—
12	電子申請システム	○	○	○	○	×	○	—
13	源泉徴収サブシステム	○	○	○	○	×	○	—
14	厚生年金保険適用業務支援システム	○	○	○	○	×	○	令和 13 年 1 月
15	間接業務システム	○	○	○	○	×	○	令和 12 年 1 月
16	お客様対応業務システム	○	○	○	○	×	○	—
17	MACS システム	×	○	○	○	×	○	令和 12 年 1 月
18	印刷物校正ソフトシステム	×	○	○	○	×	○	令和 12 年 1 月
19	コールセンターシステム	○	○	○	○	×	○	令和 12 年 7 月

※凡例 ○:提供済、×:提供対象外、—:役務期間中の更改予定なし、未定:更改時期未定

一部の提供先システムについては、契約期間中に更改が予定されている。提供先システムの更改に伴い、共通基盤システムにおいて、設定情報の変更作業が想定される。当該作業は、定例外作業として、対応すること。

3.4 継続性に関する事項

本運用対象システムの稼働(以下、「サービス」という。)が停止する障害が発生した場合、以下の対応を実施すること。

3.4.1 サービス停止の対応

障害によりサービスが停止した場合、障害原因がハードウェア若しくは仮想環境によるものか、又はアプリケーションソフトウェアによるものかの確認を行い、速やかに機構へ報告するとともに、関連事業者に連絡の上、必要な対応を実施すること。

3.4.2 障害の復旧

アプリケーションソフトウェア、ハードウェア、端末及び仮想環境の不具合に起因した障害によりサービスが停止した場合は、障害の影響・原因を踏まえ、機構及び関連事業者と協議し、早急な復旧に努めること。

3.5 情報システム稼働環境に関する事項

3.5.1 環境種別の定義

本調達における運用対象システムは、環境別に利用用途を定めており、「表 3.5.1.1 システム環境概要」に示す用途にて運用を行うこと。

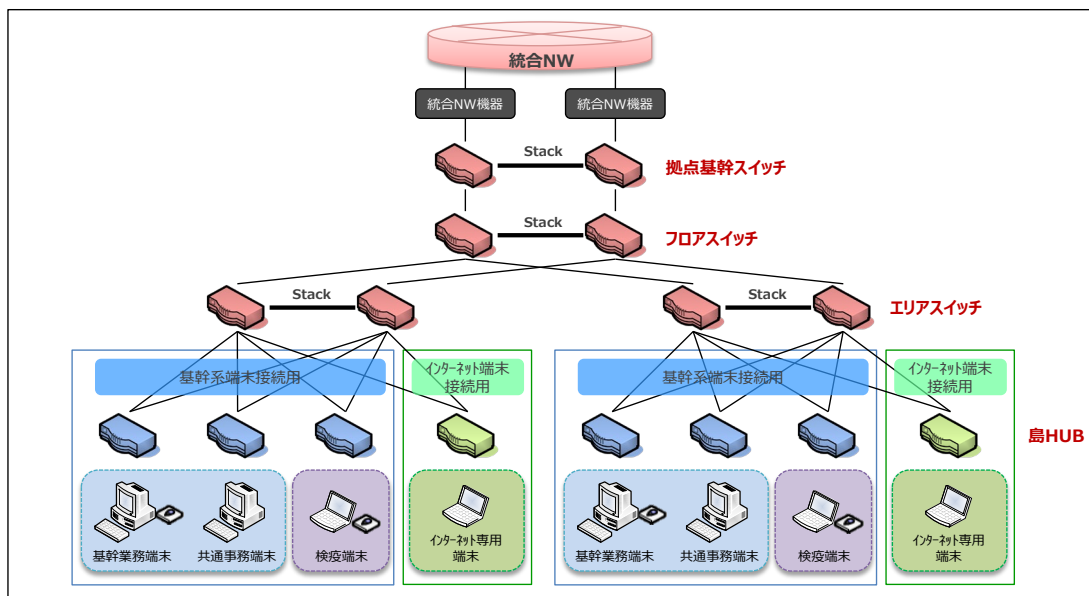
表 3.5.1.1 システム環境概要

項番	名称	概要
1	本番環境	機構職員が年金等に関する日常業務を行うために利用するシステム環境。
2	稼働維持環境	本番環境の検証や保守訓練等、システムの維持保守を目的としたシステム環境。 以下の①から⑥を実施する。 ① アプリケーションソフトウェアのサブシステム間結合テスト、総合テスト、総合運用テスト及び受入テストの実施。 ② 運用対象システムのシステム保守時における、業務ソフトウェアの障害の再現テスト、障害調査・分析、プログラム等の改修・検証、外部システムとの連携検証等の実施。 ③ 運用対象システムのシステム保守時におけるパッチ適用、ソフトウェアバージョンアップによる影響調査。 ④ 障害発生時における各種変更等の事前検証。 ⑤ 本番環境へのアプリケーションソフトウェアリリースに際しての事前検証。 ⑥ 疑似拠点環境(端末、プリンタ等)を設置しての稼働検証や業務研修。

3.5.2 ハードウェア構成

管理対象の機構 ICT 基盤のハードウェア種別及び台数等について、閲覧資料「管理対象装置一覧」に示す。また、各年金事務所におけるハードウェア構成例を「図 3.5.2.1 機構 ICT 基盤構成例」に示す。なお、ハードウェアの構成は、各事務所拠点により異なることを留意すること。

図 3.5.2.1 機構 ICT 基盤構成例



3.5.3 ソフトウェア構成

ソフトウェアは、基本ソフトウェア、ミドルソフトウェア、アプリケーションソフトウェア(社会保険オンラインシステム端末ソフトウェア)の 3 階層に分類され、各装置に搭載されている。「図 3.1.1.1 運用対象システムの範囲」に記載の共通基盤システム、共通事務システム及び社会保険オンラインシステムのソフトウェア構成の概要を「表 3.5.3.1 機構 ICT 基盤(共通基盤システム等)のソフトウェア構成概要」に示す。また、管理対象のソフトウェアは閲覧資料「管理対象ソフトウェア一覧」に示す。

表 3.5.3.1 機構 ICT 基盤(共通基盤システム等)のソフトウェア構成概要

項番	システム区分	項目	ソフトウェア概要
1	システム共通	OS	OS (Windows11、Windows Server、RHEL 等)
2		データベース	データベースソフトウェア(SQL Server)
3	共通基盤システム	統合認証 ID 管理機能	統合認証 ID 管理ソフトウェア(SECUREMASTER、IceWall 等)
4		監査機能	監査ソフトウェア(EAC/EACC/REC 等)
5		端末管理機能	端末管理ソフトウェア(SKYSEA 等)
6		運行監視機能	運行監視ソフトウェア(JP1 等)
7		ウイルス対策機能	ウイルス対策ソフトウェア(Apex One、Deep Security 等)
8	共通事務システム	グループウェア機能	グループウェアソフトウェア(INSUITE 等)
9		イントラメール機能	イントラメールソフトウェア(Outlook、Wise Audit 等)
10		電子決裁機能	電子決裁ソフトウェア(EXPLANNER/FL II 等)
11		ウイルス対策機能	ウイルス対策ソフトウェア(Apex One、Deep Security 等)
12		事務共有機能	ファイル管理ソフトウェア(NIAS、FileShell 等)
13		データベース機能	データベースソフトウェア(PostgreSQL)
14	社会保険オンラインシステム	リモートデスクトップ機能	RDS ソフトウェア(VMware Horizon 等)
15		TC 機能	通信管理ソフトウェア(TPBroker)
16		基幹共有機能	ファイル管理ソフトウェア(NIAS、FileShell 等)

3.6 引継ぎに関する事項

引継ぎに係る要件は、以下の要件以外に別紙 2「関連事業者との役割分担表」を参照すること。

3.6.1 現行運用管理事業者からの運用管理業務の引継ぎ

本調達受託者は、現行運用管理事業者より ICT 基盤(共通基盤システム等)に係る成果物等(設計書、運用実施計画書、運用管理業務計画書、関連事業者一覧、管理対象装置一覧、定期点検対象装置一覧、ナレッジデータ等)、運用管理業務に関わる情報の引継ぎを受けること。引継ぎにあたっては、事前準備作業計画書に「引継ぎ完了判定条件」を定義し、当該条件が満たされるまで引継ぎを実施すること。

また、現行運用管理事業者が全国の保守拠点等で保管している交換部品・保守機等は、本調達受託者の負担と責任において段階的に本調達受託者の保守拠点へ移動すること。

3.6.2 次期運用管理事業者への引継ぎ

本調達受託者は、次期運用管理業務(令和 13 年 1 月開始予定)が円滑に実施されるよう、次期運用管理事業者への引継ぎを、定例外作業として行うこと。

なお、本調達受託者と次期運用管理事業者が同一の場合は実施不要とする。

(1) 引継ぎ対応の範囲と活動

次期運用管理業務の調達において、本調達受託者が変更となる場合、本調達受託者は機構及び関連事業者と調整の上、次期運用管理事業者が円滑に運用管理業務を開始できるよう、(2)に示す引継ぎ

を行うとともに、次期運用管理業務開始までの間、必要に応じて次期運用管理事業者からの問合せ対応等必要な支援を行うこと。

(2) 次期運用管理事業者への引継ぎ

次期運用管理業務が円滑に開始できるよう、次期運用管理事業者への引継ぎを行うこと。引継ぎにあたっては以下①～③の作業を実施するものとし、「引継ぎ計画書」を作成の上、機構へ提出し承認を得ること。

① 運用管理業務に係る引継ぎ計画書の作成

運用管理業務に係る引継ぎ計画書の作成、納品。

② 次期運用管理事業者への引継ぎの実施

運用管理業務に係る引継ぎ計画書に従って引継ぎ作業を実施すること。

③ 次期運用管理事業者からの問合せ対応

引継ぎ期間中の質疑は全て記録し、回答や今後にとるべき対策等を記録した課題一覧表を作成すること。

また、本調達受託者は、以下の 2 条件を満たすまで実施し、引継ぎの完了したこと及び引継ぎ結果は、「引継ぎ完了報告書」として機構へ提出すること。

- 次期運用管理事業者が、自ら定義した「引継ぎ完了判定条件」が充足をされていることを確認したこと
- 機構が、引継ぎが完了したと判断すること

なお、本調達受託者が変わる際に進行中の作業がある場合は、状況や進捗についても引継ぎを実施し、引継ぎ状況を「引継ぎ完了報告書」に記載すること。

3.7 教育に関する事項

本調達受託者は、運用管理業務にかかる要員に対し、運用管理業務の知識、操作の習熟度を向上させるための研修及び倫理・コンプライアンスの研修、情報セキュリティ研修及び個人情報等の保護研修を、当該業務実施前及び随時実施すること。また、機構から要求があった場合は、要員の研修ごとの実施状況を書面にて提出すること。また、要員の変更があった際は、同様の研修を、速やかに実施すること。

3.7.1 習得訓練

本調達受託者は、履行開始後から運用業務開始までの間に、本調達の成果物(運用実施要領・ガイド、運用・保守マニュアル等)を基に、運用管理業務にかかる要員に学習及び習得訓練(机上・実機訓練等)を実施し、本調達の運用対象システムの運用管理業務を円滑に開始すること。

訓練計画については、スケジュールを含めた詳細な計画を策定し「事前準備作業計画書」に含めて、機構の承認を受けた上で納品すること。訓練計画の記載内容について、「表 3.7.1.1 訓練計画記載内容一覧」に示す。

なお、本調達受託者と現行運用管理事業者が同一の場合は実施不要とする。

本調達受託者は、機構が開示(「調達仕様書 11.3 応札希望者が閲覧できる資料一覧表」)する本調達の運用対象システムに関するドキュメント(現行システム設計書)の資料閲覧を可能とする。

表 3.7.1.1 訓練計画記載内容一覧

項番	区分	記載概要
1	訓練スケジュール	履行開始から運用開始までの訓練スケジュール、要員に対する個々の訓練内容等について記載すること。
2	訓練習熟策	段階的な習熟度合い(以下に例を示す)の向上策について記載すること。

項番	区分	記載概要
		①未経験 ②指導の下、作業が可能 ③独力での遂行可能 ④内容を理解し他者への教育が可能
3	習熟度判定	習熟度合いの判定方法、判定結果の分析方法、分析内容への対策等について記載すること。

3.7.2 情報セキュリティ研修

業務の履行に必要な研修及び情報セキュリティ要件に関する研修を事前に実施すること。また、業務の履行期間中においても必要に応じて随時実施すること。

3.7.3 研修の評価と報告

研修を行った後の受託業務の作業実績(具体的な達成目標等)を計測して、その結果を分析し、達成状況や進捗状況を機構に報告する。機構は、報告内容を評価し、承認する。

3.8 運用条件

本調達受託者は、運用管理業務を実施するにあたり、必要となる作業場所及び什器、備品、消耗品等については、本調達受託者の負担と責任において準備すること。なお、以下の点について留意すること。

- ・ 機構内で作業を実施するにあたっては、所定の手続きに従って承認を得ること。
- ・ 障害対応等により機構が緊急招集した場合は、SLA に従い、駆けつけ、参集できること。

3.8.1 本調達受託者が設置する運用監視拠点

受託業務を実施するにあたり、本調達受託者が設置する運用監視拠点は、「表 4.6.12.1 サービスレベル設定項目(運用管理業務)」を遵守できる場所に、機構の承認を得た上で本調達受託者の責任において設置すること。

なお、運用実施にあたっては、本調達受託者の負担と責任により機構との閉域網ネットワークを敷設し、接続を可能とすること。

3.8.2 システム監視環境等の用意

機構が準備し、提供する機構 ICT 基盤以外の設備、備品、消耗品等(事務用 PC、プリンタ、スキャナ、コピー機等)、並びに連絡等に使用する電話機及び電話回線(一般回線、月々に必要となる電話料金を含む。)について、本調達受託者の負担と責任において用意すること。

また、ヘルプデスク業務を行うために必要となる電話機、ヘッドセット、電話回線、音声記録/分析ツール、受付管理ツール等についても本調達受託者の負担と責任により用意すること。

ヘルプデスクの電話回線については、携帯電話からも連絡可能な回線とし、十分なサービスができる回線数を確保すること。なお、電話回線のビジー状態が機構の業務運用に影響を与えるものと機構が判断した場合には、発生原因を分析し、必要な対策を講じ、回線不足の場合には本調達受託者の負担と責任により回線を増設すること。

参考情報として、現行運用管理事業者の準備物を、「表 3.8.2.1 現行運用管理事業者準備物一覧」に示す。

表 3.8.2.1 現行運用管理事業者準備物一覧

項番	業務	準備物品・サービス	利用内容
1	ヘルプデスク	電話関連設備	ヘルプデスクの受付対応に利用。
2		ヘッドセット	
3		ヘルプデスク AI ツール	音声記録(テキスト化)、対応状況評価・分析に利用。
4		ヘルプデスク受付状況管理ツール	問合せ受付状況管理に利用。
5	センタ運管	監視カメラ	セキュリティエリアでの入退室記録に利用。
6		指静脈認証機器	セキュリティエリアへの入退室管理に利用。
7		RFID	装置管理として機器に貼り付け、タグによる読取りに利用。
8		脆弱性情報収集サービス	セキュリティ情報、脆弱性情報の収集に利用。
9	運用統制管理	インシデント管理製品	インシデント対応状況の管理として利用。

3.8.3 システムへのアクセス方法(機構が貸与する機器等の使用場所)

運用対象システムへのアクセスは、マシン室に設置するコンソール又は本調達受託者の責任において準備する運用監視拠点に設置の作業端末からリモートアクセスにて行うものとし、機構が指定する機器及び運用監視拠点以外からアクセスを行うことは不可とする。また、作業実施にあたっては、執務室と隔離されたスペースを確保し、入退室管理や作業状況の監視等の環境を準備し、不正入室の抑止、不正操作の抑止及び入室、操作等の履歴の追跡ができること。

なお、マシン室に入室する場合には必ず 2 名以上で入室し、媒体等を持ち込む際は事前に所定の申請書を提出すること。

3.8.4 作業上の留意事項

作業上の留意事項は、以下に示すとおりである。

- (1) 関連事業者等、機構以外の者との調整が必要となった場合は、原則として機構を通じて行うこと。ただし、内容や効率を考慮した上で直接関連事業者等と調整を実施することが適切と判断した場合は、機構の了解を得た上でこれに従い適切に状況を報告すること。
- (2) 関連事業者等から、照会、進捗等を把握するための資料提出の依頼等があった場合は、機構の了解を得た上でこれに従い適切に対応すること。
- (3) 受託業務の実施において疑義等が生じた場合は、機構と協議を行い、承認を得た上で実施すること。
- (4) 本調達受託者は本番環境において作業を実施するにあたり、以下の点に留意すること。
 - ① 本番作業は実績のある手順に従って実施すること。実績のない手順は、検証環境であらかじめ検証した上で本番環境において作業を実施すること。また、運用管理業務効率化のため、全部又は一部の作業を自動化するためのツール等の導入を検討し提案すること。
 - ② 本番作業におけるスケジュールを作成し機構の承認を受けた上で実行管理・報告すること。
 - ③ 本番作業中の全てのオペレーション業務については、最低限 2 人 1 組での体制で実施すること。
- (5) 本調達受託者が独自で運用管理業務に使用するツール等について、特定の製品、技術等を利用する場合、次期運用管理事業者に必要な情報を支障なく引継ぐこと。電話番号については、次期運用管理事業者が同じ電話番号を引き継ぐことができるよう検討し機構へ提案すること。

第4章 運用に関する事項

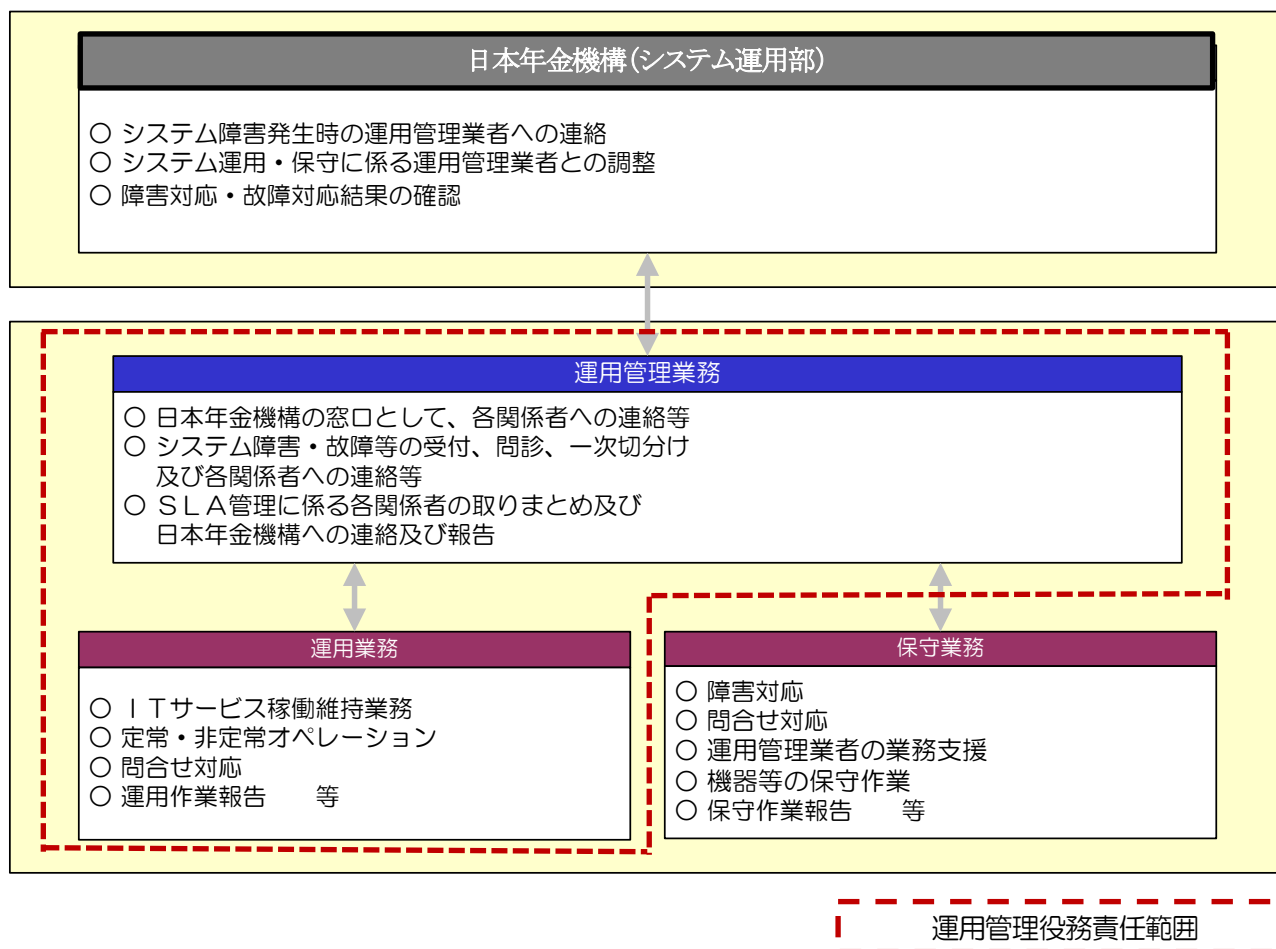
4.1 運用に関する基本方針

本調達受託者は、運用対象システムを正常に稼働させ、不具合が生じた場合でも、関連事業者と協力しこれを直ちに回復させること。本方針に基づき、機構の指示のもと、関連事業者と密接に連携し、以下の要件を踏まえて運用管理業務を行うこと。

4.2 役割分担/体制

「図 4.2.1 運用の枠組み」に示す枠組みに基づき運用管理業務を実施すること。

図 4.2.1 運用の枠組み



4.3 運用管理業務プロセスの見直し

本運用管理業務の効率化、適正化を実現するために、適宜業務プロセスの見直しを実施すること。業務プロセスの見直しに伴い、運用実施計画書等の修正を行うとともに、関連事業者が機構に納品している運用全般の実行及び管理に関する具体的な「運用・保守マニュアル」について、必要に応じて改訂案を機構に提案すること。

4.3.1 留意事項

運用管理業務の効率化を実現するために、運用の自動化等を見直しを実施すること。効率化課題に対しては、実現性を検討の上、効率化状況報告会議にて検討状況の報告及び提案の協議を行い、機構承認のもと見直しを実施し、運用のコスト削減を図ること。

自動化等効率化の効果により工数の削減が可能であることが確認できた場合においては、本調達における運用管理業務の月次提案工数から人月単位での減額等について機構との協議の上、対応すること。

4.4 事前準備作業

4.4.1 事前準備作業の定義

履行開始日から令和 10 年 6 月 30 日までは、運用管理業務開始のための準備作業期間とし、「4.4.2 事前準備作業の概要」から「4.4.7 ドキュメント作成」に示す準備作業を本調達受託者の負担によりこの期間内で実施するものとする。本調達受託者は、この期間内に現行運用管理事業者から引継ぎを受けること。

なお、本調達受託者と現行運用管理事業者が同一の場合は実施不要とする。

4.4.2 事前準備作業の概要

契約締結から令和 10 年 6 月 30 日までの間に対応すべき事前準備作業の概要について、「表 4.4.2.1 事前準備作業の概要」に示す。

表 4.4.2.1 事前準備作業の概要

項番	作業項目	作業概要
1	事前準備作業計画書の作成	準備作業を滞りなく実施するための事前準備作業計画書を作成する。(実施計画、訓練計画、構築計画、管理計画等)
2	習得訓練	設計書、運用・保守マニュアル等により、運用対象システムのシステム構成、運用管理業務の手順等について学習し、理解する。 現行運用管理事業者から業務に関する習得訓練(引継ぎ)を受けること。(詳細は、「3.7.1 習得訓練」に記載。)
3	運用監視拠点の構築	運用監視を行うための拠点を構築する。
4	定例報告	準備作業の進捗状況を報告する。
5	ドキュメント作成	契約締結後に納品するドキュメント(運用実施計画書、SLA 合意書)を作成する。

4.4.3 事前準備作業計画書の作成

履行開始後 2 週間以内に、事前準備作業に係る実施計画、管理計画等を定めた「事前準備作業計画書」を提出し、機構の承認を得ること。事前準備作業計画書の記載項目(必須項目)については、「表 4.4.3.1 事前準備作業計画書の記載項目(必須項目)」に示す。

また、各関係者等との調整結果に基づき、当該計画書の修正又は見直しが必要となった場合は、速やかに修正案等を提出し、機構と協議の上、機構の承認を得ること

表 4.4.3.1 事前準備作業計画書の記載項目(必須項目)

項番	記載項目	記載内容
1	作業対象	事前準備作業に係る作業範囲を記載する。
2	体制・スケジュール	実施体制及びスケジュールを記載する。
3	実施内容	習得訓練の実施形態、習熟度合いの向上策、実施方法等を記載する。
4	習熟度判定	習熟度合の分析方法と判定結果、習熟度向上策等について記載する。
5	拠点構築計画	運用管理業務を行うための拠点の構築計画について記載する。
6	完了基準	事前準備作業の完了基準を記載する。
7	管理方法	進捗管理、課題管理、コミュニケーション管理等の管理項目、管理方法等を記載する。

4.4.4 習得訓練

設計書、運用・保守マニュアル等により、運用対象システムのシステム構成、運用管理業務の手順等について学習し、理解する。

また、現行運用管理事業者から業務に関する習得訓練(引継ぎ)を受けること。

4.4.5 運用監視拠点構築

運用を実施するための拠点を本調達受託者にて準備した場所に構築し、運用管理業務を滞りなく実施すること。

詳細については、「3.8 運用条件」に記載する。

4.4.6 定例報告

本調達受託者は、業務開始までの準備作業に係る進捗状況について週次で報告すること。報告にあたっては、進捗状況、懸案事項、対策案について書面にまとめること。

報告は会議形式として行うこととし、開催日程、場所については都度機構と協議の上決定する。

4.4.7 ドキュメント作成

(1) 運用実施計画書

履行開始後 1 か月以内に、運用管理業務に係る作業範囲、スケジュール、プロジェクト実施体制、実施計画、管理計画等を定めた「運用実施計画書」を提出し、機構の承認を得ること。運用実施計画書の記載項目(必須項目)については、「表 4.4.7.1 運用実施計画書の記載項目(必須項目)」に示す。また、各関係者等との調整結果に基づき、当該計画書の修正又は見直しが必要となった場合は、速やかに修正案等を提出し、機構と協議の上、承認を得ること。なお、運用実施計画書は、履行期間中に適宜見直すとともに、必要に応じて改訂すること。

表 4.4.7.1 運用実施計画書の記載項目(必須項目)

項番	記載項目	備考
1	体制	体制図、役割、責任、当該業務を行う者(氏名)、スキル、経歴等を記載する。 ※別紙 15「管理者等申請書」を参照すること。
2	スケジュール	本運用業務の全体スケジュール及び業務ごとの工数を記載する。
3	作業範囲	本運用業務における作業範囲(作業時間、対象機器等)を記載する。
4	作業内容	作業内容、業務時間帯、業務周期等を記載する。
5	コミュニケーション管理	関連事業者等との合意形成に関する手続き、連絡調整に関する方法、参加すべき会議・開催頻度・議事録等の管理等について記載する。特にインシデント発生時の連絡手段や報告要領についても記載する。
6	進捗管理	進捗管理及び実績管理に関して記載する。
7	品質管理	サービスレベルの維持・向上を含めた品質管理に関して記載する。

項番	記載項目	備考
8	リスク管理	リスク管理方針、リスク管理プロセス、リスク分析結果と対応計画について記載する。
9	課題管理	解決すべき問題について、発生時の対応手順、管理手法等について記載する。
10	情報セキュリティ管理	セキュリティ管理方針、セキュリティ施策(当該業務を行う者以外の者に当該情報にアクセスをさせないための施策、当該業務を行う者が目的外に当該情報を使用しないための施策、再委託を実施する場合は、再委託先の施策)、セキュリティ教育、管理手法、情報漏えい対策等について記載する。
11	文書管理	文書管理方針、管理手法について記載する。
12	要員の教育・訓練	研修の目的と内容、習熟判定と分析方法、リカバリ策の内容等について記載する。
13	インシデント管理	インシデント管理方針、管理手法等について記載する。
14	問題管理	問題管理方針、管理手法等について記載する。
15	構成管理	システムの構成(ハードウェア製品、ソフトウェア製品、アプリケーションソフトウェア、ネットワーク、外部サービス、施設・区域、公開ドメイン等)の管理手法等について記載する。
16	変更管理	発生する変更内容について、管理対象、変更手順、管理手法等について記載する。
17	サービスレベル管理	サービスレベルの測定方法、評価方法、管理手順について記載する。
18	成果物	本運用業務における成果物と納入サイクルについて記載する。

(2) サービスレベル合意書

履行開始後 1 か月以内に、運用管理サービス等業務に係るサービスレベルを定めた「サービスレベル合意書」に押印の上提出し、機構の承認を得ること。なお、機構と本調達受託者との調整結果に基づき、サービスレベル合意書の修正又は見直しが必要となった場合は、速やかに修正案等を提出し、機構の承認を得ること。

(3) 情報セキュリティ管理計画書

履行開始後 1 か月以内に、セキュリティ対策の実施内容及び管理体制について記載した「情報セキュリティ管理計画書」を作成の上、機構に提出し、承認を得ること。

(4) 運用実施要領・ガイド

各業務内容詳細や統制管理業務等の実施に伴い、何を・いつ・どう実施するのか、どの作業で提供された運用マニュアルを使うのかなどの実施要領や運用ガイド、業務フローなどを纏めた資料を、要員の習得訓練開始までに作成すること。また、必要に応じて改訂すること。

4.5 運用管理業務

年金業務の円滑な遂行のために運用対象システムには高品質なサービスが求められる。本調達受託者は効率的かつ安定したシステム運用を行うこと。

受託業務における運用管理業務は「表 4.5.1 機構 ICT 基盤運用管理業務」に示すとおり区分されるが、複数区分にまたがって行われる作業もある。詳細な運用作業項目については、別紙 11「業務内容詳細(拠点装置運用管理)」、別紙 12「業務内容詳細(センタ運用管理)」、別紙 13「業務内容詳細(ヘルプデスク)」及び別紙 14「業務内容詳細(運用統制管理)」を参照すること。

表 4.5.1 機構 ICT 基盤運用管理業務

項番	大区分	中区分	小区分
1	拠点装置運用管理	拠点装置管理	拠点情報管理、在庫管理、キッティング、端末マスタ管理、ファームウェアバージョン管理
2		端末ソフトウェア管理(情報業務端末を除く)	パッチ適用、ソフトウェアバージョンアップ
3		故障対応	端末装置故障時対応
4		機構 ICT 基盤設置等作業	工事調整(図面管理含む)、拠点装置の増設・移設・撤去(機構 ICT 基盤設置等作業)
5		予防保全(定期点検)	予防保全対応として管理対象機器の定期点検の実施
6	センタ運用管理	サーバ機器管理	定例作業、定期点検、ファームウェアバージョン管理、キャパシティリソース管理
7		サーバソフトウェア管理	パッチ適用、ソフトウェアバージョンアップ
8		システム監視/障害対応	サーバ及び拠点装置の監視、障害対応、テスト支援
9		セキュリティ対策	ウイルス定義最新化、各種フィルタリング適用(ホワイトリスト、ブラックリスト、ファイアウォールポリシー)
10		業務環境管理	共通機能提供及び管理
11		ネットワーク管理	ネットワーク構成管理、統合 NW 申請
12	ヘルプデスク	問合せ対応	機構内の各ユーザからの照会応答、回答及び情報提供(各システム担当へのディスパッチ)、応答品質分析/改善等
13	運用統制管理	全体統括	運用スケジュール管理、マシン調整、デバッグ室管理、コミュニケーション管理、インシデント管理、問題管理、変更管理、リリース管理、リスク管理、要員管理、品質管理、ドキュメント管理、関連事業者調整、次期運用管理事業者への引継ぎ管理
14		IT 資産管理	機器情報管理、ライセンス管理、アカウント管理
15		セキュリティ管理	特権 ID 監査運用、権限管理、セキュリティインシデント監視、ウイルス・マルウェア等検知時対応(一次切り分け、解析・調査)
16		影響調査	システム問合せ対応、影響分析、要件整理支援
17		報告業務	SLA 管理、運用報告

4.5.1 拠点装置運用管理

本調達受託者は、機構内の各拠点に設置された端末装置におけるメンテナンスや故障時の対応及び拠点工事対応を実施すること。なお、本調達受託者は、全国の利用拠点で運用管理業務のサービスレベルを遵守することが可能な場所に保守拠点を設置すること。

(1) 拠点装置管理

① 保守機管理

本調達受託者は、機構より貸与される保守機について、適宜、整備を実施し、常に動作可能な状態で保管すること。また、修理や関連事業者への貸与/返却等の管理及び定期的な棚卸を含めた在庫管理を行うこと。

なお、保守機の在庫台数が不足する場合は、機構職員と対応を協議すること(必要台数は機構と協議すること)。

また、本調達受託者は、保守機を保管するためのスペース(保管庫)を本調達受託者の負担と責任にて確保するとともに、機器の増加に伴い保管庫のスペースを拡張する必要がある場合は、必要なスペースを追加で確保すること。

なお、機構要請による保守機の一時保管等に伴い、保管庫での装置受入れ費用等が個別に発生する場合は、機構と協議すること。現在の保管庫の場所は現行運用管理事業者が確保している保管庫となるため、保管庫の場所を変更する必要がある場合は、変更費用及び移送費用等について機構と協議すること。

現地に設置していない保守機についても同様に本調達受託者にてスペース確保の上、保管すること。

(2) 端末ソフトウェア管理

① プログラム配布業務

社会保険オンラインシステムに係る端末ソフトウェアが改修(又は各種設定のための資材の転送)され、機構 ICT 基盤のプログラムを修正する必要がある場合には、本調達受託者は関連事業者とプログラムの配布実施日、配布資材の授受に係る調整を実施し、端末ソフトウェアの構成管理、配布に係る機構職員への説明を行い、配布を実施すること。また、本調達受託者は、プログラム配布が完了したことを機構職員に報告すること。

② セキュリティパッチ・セキュリティ対策製品の定義ファイル配布業務

本調達受託者は、拠点設置機器及びセンタ設置機器に対して、セキュリティパッチ等の配布業務を行うこと。配布にあたり、セキュリティパッチの未適用、ウイルス定義ファイルの未更新等が原因となり、システム侵害を発生させる事態がないよう、機構職員及び関連事業者と十分に調整の上、実施すること。

なお、セキュリティパッチ等の配布は共通基盤システムにて提供される構成管理サーバで実施し、ウイルス定義ファイル等の配布はウイルス対策サーバで実施すること。構成管理サーバ及びウイルス対策サーバにて実施できない機器に対しては、別の手段によりセキュリティパッチ等の適用及びウイルス定義ファイル等の最新化を実施すること。実施にあたり、サーバ再起動を要する場合は、サービスが影響を受けない日に作業を実施すること(※ウイルス定義ファイル配布は、製品により適用タイミングが異なるため、留意すること)。

(3) 故障対応

機構 ICT 基盤について閲覧資料「管理対象装置一覧」に示す。また、ハードウェアの保守形態については、「表 4.5.1.1 ハードウェアの保守形態」に示す区分を参照する。

故障時におけるハードウェアの保守形態について、「表 4.5.1.1 ハードウェアの保守形態」に示されたいずれかの対応を行うこと。機構の買取機器の一部においては、本調達受託者が保守機交換のみを行い、故障機の廃棄は機構が実施する。

また、端末設置に伴い提供機能のクライアント設定等センタ設置機器運用作業が必要となることを留意すること。

なお、本調達にて構築・設置する機器以外の運用対象装置については閲覧資料「管理対象装置一覧」に示す。

表 4.5.1.1 ハードウェアの保守形態

項番	保守形態	概要
1	現地オンサイト	現地にて部品交換又は修理を行う。
2	保守拠点オンサイト	現地では保守機との交換を行い、保守拠点にて装置修理手配等を行う。故障対応に伴う関連保守機の環境構築を行い、保守機設定変更や資材適用等を行う。
3	現地センドバック	現地の機構職員にて本調達受託者へ故障の連絡を実施し、本調達受託者から機構 ICT 基盤ハードウェア事業者へ現地の機構職員宛で代替機の発送を依頼する。現地の機構職員にて代替機を受領し、故障装置と交換を行い、代替機に添付の発送伝票(着払い)の宛先へ故障装置を返送する。
4	保守拠点センドバック	現地の機構職員にて本調達受託者へ故障の連絡を実施する。現地で本調達受託者にて保守機との交換を行い、故障装置を保守拠点へ持ち帰る。本調達受託者から機構 ICT 基盤ハードウェア事業者へ代替機の発送を依頼する。本調達受託者にて代替機を受領し、故障装置を機構 ICT 基盤ハードウェア事業者へ返送する。故障対応に伴う関連保守機の環境構築を行い、設定変更や資材適用等を行う。

(4) 機構 ICT 基盤設置等作業

機構 ICT 基盤設置等作業に係る運用作業項目について、「表 4.5.1.2 機構 ICT 基盤設置等作業の概要」に示す。作業においては、機構と協議の上、機構からの作業依頼により実施し、実施後、工事実施報告書を提出すること。

また、端末設置に伴い提供機能のクライアント設定等センタ設置機器運用作業(情報業務端末は除く)が必要となることを留意し、センタ運管業務として実施すること。

表 4.5.1.2 機構 ICT 基盤設置等作業の概要

項番	作業項目	概要
1	拠点内移設工事	レイアウト変更等により、同一の建物内で、機構 ICT 基盤を移設する。
2	拠点間移設工事	他の年金事務所等の別拠点へ、機構 ICT 基盤を移設する。 ※県跨りの拠点間移設工事が発生した場合は、マスタ資材の再キッティングが発生するため、工事区分を「拠点間移設(移設先) 県跨りあり」と区別する。
3	増設工事	機構 ICT 基盤を追加設置する。
4	撤去工事	機構 ICT 基盤を取り外し撤去する。
5	収容変更	WM が接続されるセンタ側 TC の収容先を変更(接続先 TC-ID の変更)する。業務系端末にのみ発生する工事区分。 ※拠点内移設と同時工事が単独工事かで工事区分を区別する。
6	プリンタ設定	クライアント装置のプリンタ設定を実施する。
7	プリンタ用途変更	プリンタが接続されるセグメントを変更し、プリンタの用途を変更する。 例:業務系 CPR から共通事務 CPR への変更等 ※プリンタ機種により用途変更可能範囲が異なる。
8	経過スキャナ接続 WM 変更	経過スキャナの USB 接続先 WM を変更する場合、変更元の WM から経過スキャナ個別資材のアンインストール及び設定作業を行う。また、変更先の WM へ経過スキャナ個別資材のインストール及び設定作業を行う。なお、WM と経過スキャナを同時に移設した場合は、経過スキャナの接続先 WM が変更とならないため、本作業は発生しない。
9	スキャナ用途変更	スキャナ装置が接続されるセグメントを変更し、スキャナの用途を変更する。 例:G-SCAN から L-SCAN への変更等 ※現段階においてはスキャナ用途変更可能な機種は、G-SCAN⇔L-SCAN のみ。
10	スキャナ宛先追加	スキャナ装置に対し、読み込み情報の保存先ファイルサーバ宛先を追加する。 ※宛先追加 1 件ごとに適用する。
11	スキャナ宛先削除	スキャナ装置に登録されている、読み込み情報の保存先ファイルサーバ宛先を削除する。 ※宛先削除 1 件ごとに適用する。 ※拠点で実施する場合と、センタからリモート接続で実施する場合とで工事区分を区別する。
12	ネットワーク設定変更(ポート開閉)	ネットワーク機器における下位ネットワーク機器の増減、島 HUB における接続装置増減に伴うポート開閉作業を行う。 ※拠点で実施することが前提だが、センタからリモート接続で実施する場合の工事区分も設ける。
13	本部 NW LAN 敷設	本部エリア SW とパッチパネル間のケーブルを敷設する作業。
14	図面修正	項番 1～13 の作業以外の要件に伴う図面修正作業を行う。 例:拠点内移設を拠点職員にて実施した場合等
15	その他来訪等作業	項番 1～14 の作業とは別の作業等で、年金事務所等を訪問する。

① 工事申請

機構 ICT 基盤設置等作業については、機構から提出される工事申請書の内容に基づき、作業を実施する。その際の工事申請書については、機構及び本調達受託者との間で規定した様式のものを利用すること。

以下に工事申請における留意事項を示す。

- (i) 工事申請書は、原則として、工事希望日の 1 か月前までに提出されていることとする。ただし、新規に拠点を開設する場合や新規要件が発生する場合、配管工事等の特殊な工事が発生する場合

合については、機構と協議すること。

- (ii) 工事申請の提出後については、工事希望日直前の工事内容の変更は発生しないことを基本とすること。
- (iii) 工事対象機構 ICT 基盤の設置場所及びその周辺のレイアウトを確認できる図面について、本調達受託者から機構へ提供を行うこと。
- (iv) 機構 ICT 基盤設置等作業に示す工事区分に該当しない個別要件が発生する場合については、機構と協議する。以下に、個別調整が必要となる例を示す。
 - ・機構 ICT 基盤設置拠点にて、回線工事、電気工事、配管工事等の工事を実施する場合
 - ・新規に開設する拠点及び端末機器未設置フロアへの移設、増設等が必要となる場合
 - ・特殊搬入・搬出が必要となる複合機、一元化スキャナ(I-SCANB)等を移設する場合
 - ・TC の追加及び削除等、センタ作業が発生する場合
 - ・一定期間内に複数拠点の工事(移設・増設・撤去配管工事等)を行う場合

② 検査

本調達受託者は、機構 ICT 基盤設置等作業において必要となる資料を作成し、機構へ提出を行うこと。

なお、作業実施後に本調達受託者から提出されるドキュメントを機構にて完了検査を実施する。その際の留意点を以下に示す。

- ・調達受託者は、指定のドキュメントを紙媒体又は電子媒体により日本語で提供すること。
- ・提出するドキュメントの納入時期、納入形式の詳細は、機構と協議すること。
- ・本調達における作業のために必要なドキュメント、端末装置管理情報等については、契約締結後別途提示する。なお、提示時期については別途調整の上決定する。
- ・機構 ICT 基盤設置等作業に係る提出対象ドキュメントについては、「表 4.5.1.3 機構 ICT 基盤設置等に係る提出対象ドキュメント」を参照すること。

表 4.5.1.3 機構 ICT 基盤設置等に係る提出対象ドキュメント

項番	提出対象ドキュメント	運用時間
1	工事実施報告書	作業の実施内容及び実施結果を記載した報告書
2	端末配置図	各機構 ICT 基盤等の配置状況を記載した図面

③ 工事区分

機構 ICT 基盤設置等作業において定める工事区分の詳細について、以下に示す。なお、本調達受託者は機構から提示される申請の内容に従い、作業を実施すること。

- (i) 拠点内移設工事
拠点内移設工事とは、機構 ICT 基盤拠点(既存の同一ビル内)でレイアウト変更等により同一フロア内/フロア間を跨って、既存の機器を移設する工事である。
- (ii) 拠点間移設工事
拠点間移設工事とは、業務集約等により異なるビル間を跨って、既存の機器を移設する工事である。なお、WM 等の端末について移設先が移設元と異なる都道府県となる場合は、別途キッティング作業が必要となる。
- (iii) 増設工事
増設とは、機構 ICT 基盤拠点に新たに機器を追加設置する工事である。
- (iv) 撤去工事

撤去とは、機構 ICT 基盤拠点にて不要となった既存の端末機器を取り外す工事である。

取り外した端末機器は保守機として保管管理する。

(v) 収容変更

収容変更とは、端末機器の移設を行わずに TC-ID を跨る接続変更を行う工事である。事務センター等複数 TC が設置されている場合、窓口装置を移設せずに他の TC へ接続替えを行うこと。

(vi) プリンタ設定

WM(給付)等の端末にプリンタを接続し、使用可能とする。

(vii) プリンタ用途変更

カラープリンタと共回事務プリンタ等の、プリンタ用途の変更を行うこと。

(viii) 経過スキャナ接続先 WM 変更

経過スキャナの接続先 WM を、経過スキャナ、WM の移設を伴わずに変更する。

(ix) スキャナ用途変更

業務系スキャナ(G-SCAN)と共回事務用スキャナ等の、スキャナ用途の変更を行うこと。

(x) スキャナ宛先追加/削除/変更

スキャナ装置に登録されている読み込み情報の保存先ファイルサーバ宛先を追加/削除/変更する。

(xi) ネットワーク設定変更(ポート開閉)

各ネットワーク機器において、端末及びネットワーク機器の接続されていないポートは、セキュリティ観点から必ず閉鎖することとなっている。そのため、ネットワーク機器の増減、端末等装置の増減が発生した際に、ネットワーク機器のポートごとのセグメント設定、ポート開閉作業を実施する。

(xii) 本部 NW LAN 敷設

本部エリア SW とパッチパネル間のケーブルを敷設する作業。

(xiii) 図面修正

拠点職員にて、端末の拠点内移設を行った場合等に、端末等配置図面の修正を行うこと。

(xiv) その他来訪等作業

実地調査や他事業作業の立会い等、工事区分で定めた作業以外の目的で拠点を訪問する。

(5) 予防保全(定期点検)

本調達受託者は、管理対象機器の予防保全対応として、以下に示す定期点検を行うこと。なお、本調達にて導入・構築する機器以外の予防保全の対象装置については、閲覧資料「定期点検対象装置一覧」を参照すること。

① 定期点検の実施

本調達受託者は、業務への影響を考慮した定期点検計画を作成し、機構 ICT 基盤拠点の担当者及び関連事業者と日程調整を実施した上で、定期点検の実施、実施状況管理並びに報告を行うこと。

② 統計データの蓄積、活用

本調達受託者は、障害状況等のデータの蓄積・分析を実施し、予防保全の観点から障害回避策を策定し、月次で機構職員に報告すること。

③ システム動作確認の実施

安定したサービスを提供するために、本調達受託者は、メール疎通確認、WEB 閲覧状況確認等のシステム動作状況を確認すること。

(6) 稼働状況報告等の資料作成

「4.6.11 稼働状況管理」に記載の機構への報告のため、必要に応じ資料作成を行うこと。

4.5.2 センタ運用管理

本調達受託者は、運用対象システムにおける定例作業、システム監視、障害時の対応及び作業指示書による定例外作業等の作業を実施すること。

(1) サーバ機器管理

① バックアップ運用

本調達受託者は、運用対象システムのサーバ等センタ設置機器について、運用保守設計及び運用・保守マニュアルに従い原本データのバックアップ取得を行うこと。バックアップに必要な媒体等については、本調達受託者において準備し管理すること。

② ログ情報等の取得

本調達受託者は、システム故障時の解析やサーバ運用管理業務で必要となる各種ログの取得を行うこと。なお、定例作業以外のログ取得は、機構職員の指示に従い実施すること。ログ取得の際には、必要に応じて関連事業者と連携すること。

③ 予防保全(定期点検)

本調達受託者は、管理対象機器の予防保全対応として、以下に示す定期点検を行うこと。なお、本調達にて導入・構築する機器以外の予防保全の対象装置については、閲覧資料「定期点検対象装置一覧」を参照すること。

(i) 定期点検の実施

本調達受託者は、業務への影響を考慮した定期点検計画を作成し、機構 ICT 基盤拠点の担当者及び関連事業者と日程調整を実施すること。また、定期点検の実施、実施状況管理及び報告を行うこと。

(ii) 統計データの蓄積、活用

本調達受託者は、障害状況等のデータの蓄積・分析を実施し、予防保全の観点から障害回避策を策定し、月次で機構職員に報告すること。

(iii) テープ運用実施

本調達受託事業者は、LTO 等のテープ装置を導入する場合は定期的にクリーニングテープ / LTO の交換を実施すること。

(iv) システム動作確認の実施

安定したサービスを提供するために、本調達受託者は、ランプ確認等の目視確認、実機状況のシステム動作状況を確認すること。

④ 法定点検運用

本調達受託者は機構本部及び全国の年金事務所等において、定期的実施される法定点検に係る運用を行うこと。

(i) 前提条件

法定点検は、準備段階における各種調整、点検日のシステム停止作業、法定点検作業、システムの復旧作業に分かれる。法定点検を実施する際の手順書では、運用で必要となる体制、フロー及び作業詳細を定義すること。また、機構本部及び年金事務所等それぞれにおいて作業内容が異なるため、ロケーション別に運用を定義すること。

なお、本運用で対象とする法定点検は対象拠点の電源設備、空調設備に関する点検であり、水質調査や作業環境測定等の点検は対象としない。

(ii) 準備

本調達受託者は、機構本部及び年金事務所等における機構 ICT 基盤の法定点検に係る情報を把握し、計画を作成すること。また、計画については、関連事業者に周知すること。

(iii) 実施

本調達受託者は、計画に基づき関連事業者とともに作業を実施し、その結果について取りまとめた上で機構に報告すること。

⑤ 統計データ取得

本調達受託者は、センタ設置機器に対するリソース情報(CPU 使用率、メモリ使用率、ディスク使用率等)を取得、管理すること。また、蓄積した統計情報を月次で機構に報告すること。

年金事務所等の事務処理機器に対する使用時間等の統計情報に関しては、センタの運行監視端末等を使用して本調達受託者が取得すること。

(2) サーバソフトウェア管理

① プログラム配布・適用業務

センタ設置機器に搭載されているソフトウェアに、パッチ適用、バージョンアップ等の対応が発生する場合には、本調達受託者は関連事業者と作業の実施日、配布・適用資材の授受に係る調整を実施し、機構への説明を行い、配布・適用を実施すること。配布にあたっては、あらかじめ検証環境等を用いてテストを行った上で、本番環境への適用を行うこと。また、本調達受託者は、適用が完了したことを機構職員に報告すること。

② サポート期限管理

本調達受託者はソフトウェアのサポート期限を管理し、サポート期限が超過しないよう対策を検討し、計画を策定すること。また、機構へ納入しているハードウェアにおいてファームウェアのバージョンアップが必要となった場合に関連事業者と連携してファームウェアのバージョンアップ対応を行うこと。

(3) システム監視/障害対応

本調達受託者は、監視端末及び運用管理端末によるシステム監視を実施すること。また、システム監視によって出力された警告等に対して、運用・保守マニュアルに従い対応を実施すること。

なお、本調達範囲のシステムにおけるシステム障害時の解析で必要とする各種ログの取得は、本調達受託者が行うこと。

システム監視等で検知した事象については、インシデント管理及び問題管理として適切に管理し、障害発生状況について機構へ報告すること。また、障害箇所の切り分け、関連事業者への連絡、復旧確認、報告等の運用管理業務を行うこと。なお、障害対応では、複数の関連事業者との連携、情報共有、調整等が重要であるため、関連事業者の統制、管理を徹底するとともに、対策内容について運用・保守マニュアルの修正等を行うこと。

(4) セキュリティ対策

① ウイルスフルスキャン確認

本調達受託者は、拠点端末装置の増設作業が終了した際に、当該端末のフルスキャンを実施し、機構に報告すること。

② 機構 ICT 基盤設置等作業後のセキュリティチェック

本調達受託者は、拠点工事後に機構が指定したセキュリティチェック項目を日次でチェックし、機構に報告すること。

③ 統合ネットワークの遮断ログの確認

本調達受託者は、統合ネットワークの遮断通信ログ(機構本部 A コアファイアウォール分)を月次でチェックし、機構に報告すること。

④ 情報資産管理台帳の更新

本調達受託者は、情報資産管理台帳の棚卸及び、更新作業を四半期ごとに実施し、機構に報告すること。

⑤ 情報系/業務系のファイル一覧(台帳)の作成

本調達受託者は、各種ファイルサーバに保存されているファイルのうち、機構から指示があった機密性の高い情報(機年/機密性 3)が含まれるファイルの抽出した一覧を機構に提出すること。

⑥ 監査対応

本調達受託者にて個人情報を含むデータやログファイル等を取得した場合は個人情報の管理状況が適切であることの監査を行うこと。個人情報利用における情報取得許可願の完了確認、個人情報の持出し確認を実施し、機構に報告すること。また NCO 等その他監査対応についても機構と協議の上、対応すること。

(5) 業務環境管理

本調達受託者は、機構における業務環境に係る運用管理業務を実施すること。

(6) ネットワーク管理

本調達受託者は、本部ネットワーク、統合ネットワーク、拠点ネットワークを含む機構ネットワークの構成管理及び稼働状況管理を実施すること。なお、構成管理及び稼働状況管理に必要な環境については機構の承認を得た上で本調達受託者の責任において準備すること。また、統合ネットワークへの申請に関する業務を実施すること。

4.5.3 ヘルプデスク

本調達受託者は、機構 ICT 基盤の障害報告及び機構 ICT 基盤の操作方法等について、全国の利用者からの照会に対し、一元的に受付けて適切な回答・案内等を行うため、ヘルプデスクを設置すること。ヘルプデスクは、本調達対象システムや社会保険オンラインシステムに係る問合せのみに留まらず、端末操作方法等の問合せにも対応すること。また、ヘルプデスク業務を実施するにあたり必要となる電話機、ヘッドセット、電話回線（一般回線）、受付けた問合せ内容の記録、通話対応品質分析するためのツール等については、本調達受託者の負担と責任により準備すること。

ヘルプデスクは、利用者からの問合せ対応及び機構職員とのコミュニケーションの総合的窓口であり、以下の要件を満たす必要がある。また、利用者の利便性向上としてヘルプデスクポータルサイト等を作成し、情報共有や業務効率化を図ること。

なお、サービス時間外の問合せについては、サービス終了のアナウンスを流すこと。

(1) 対象範囲

機構 ICT 基盤等に関する照会窓口となるため、年金事務所等をヘルプデスクの対象利用者とする。年金事務所等については、拠点ごとにネットワーク構成や、装置構成が異なるため、照会対応にあたって留意すること。

受付対象システムについては、「表 2.2.1 運用対象システム」に示す。なお、受付対象外のシステムに関する問合せを受けた場合は、対象システムのヘルプデスク等問合せ先を案内すること。

(2) 管理対象

本調達受託者は、機構各拠点での業務中に発生する様々なシステム関連問題（インシデントを含む）について、問題受付から回答までのプロセスを確立し、その内容、原因、対応結果等の情報を一元的に管理すること。また、関連事業者からの依頼に応じてトラブル解決のためのヒアリング等を実施すること。また、

(3) 問合せに対する対応の改善

機構職員からの問合せに対する回答等の品質向上、時間縮減のため、以下を始めとする改善活動を継続して実施すること。

- ① ヘルプデスクへの申告内容、回答内容など恒常的に分析し、必要な対応策（FAQ 登録、受付内容の共有、ヘルプデスクポータルの更新等）の策定
- ② 事務処理関連資料（事務取扱説明書、業務取扱説明書等）を理解し、即時回答範囲の拡大をするための教育の実施
- ③ 問合せが増加する期間（組織改編月、人事異動月等）の問合せ量の削減に向けた施策の策定

(4) 関連事業者への問合せ・対応依頼

本調達受託者による問診及び一次切り分けの後、本調達受託者にて解決できない事象については、関連事業者へ問合せ及び対応依頼を実施すること。なお、本調達受託者の誤った判断による復旧遅延が生じないよう、運用保守マニュアル、過去事象を踏まえた切り分けと関連事業者との密な連携を行うこと。

(5) 障害対応

本調達受託者は、障害の発生による社会保険オンライン業務への影響を最小限に止めるため、障害対応の管理を行うこと。具体的には、障害の発生連絡の受理後に障害の発生箇所の切り分けを行い、担

当の関連事業者へ作業を指示するとともに、障害状況を機構職員及び関連事業者と共有し、障害の発生から回復までの作業を一元的に管理すること。

また、障害のステータスが変更した際は、当該障害の問合せがあった年金事務所等に対し、必要に応じてステータス変更の連絡等フォローアップを行うこと。

(6) 報告

本調達受託者は、社会保険オンラインシステムのサービスが安定的に提供されることに対し、責任を負う立場にあることから、機構職員に対し、システムで発生している障害状況を定期的に報告すること。受付内容については、情報蓄積を行い、機構に報告すること。なお、報告する項目は、「表 4.5.3.1 ヘルプデスク情報蓄積の項目一覧」を参照すること。

また、関連事業者との密な情報共有を必要とする立場にあることから、障害状況の取りまとめに際して、関連事業者からの情報取りまとめ、業務改善に向けた調整を実施すること。

表 4.5.3.1 ヘルプデスク情報蓄積の項目一覧

項番	項目	内容
1	着信件数の集計	ユーザからヘルプデスクへの問合せ着信件数を集計すること。
2	応答件数の集計	項番 1「着信件数」のうち、応答出来た件数を集計すること。
3	応対待ち件数の集計	項番 1「着信件数」のうち、溢れ呼の件数を集計すること。
4	放棄件数の集計	項番 1「着信件数」のうち、応答出来なかった件数を集計すること。
5	平均通話時間の集計	ヘルプデスクにて対応した通話の平均時間を集計すること。

※ 項番 1～5 を実現するにあたり、CTI ツール等の使用を前提とする。

なお、上記ヘルプデスク業務にて蓄積した情報、対応等のナレッジデータは次期運用管理事業者に情報提供すること。

4.5.4 運用統制管理

本調達受託者は、以下の運用統制管理業務を実施すること。

(1) 全体統括

受託業務に伴う以下の運用・作業スケジュールの計画、各種作業進捗状況の確認等の管理業務を実施すること。

① 運用実施計画書の作成

本調達受託者は、運用管理業務に係る作業範囲、スケジュール、実施体制、実施計画、管理計画を定めた、「運用実施計画書(※内容は、「4.4.7ドキュメント作成」を参照すること。)」を作成し、その内容について機構の承認を得ること。運用管理業務は、本要領に基づいて実施する。

② 進捗管理

本調達受託者は、「図 3.1.1.1 運用対象システムの範囲」に示された受託業務の対象範囲内に係る運用管理業務を主体的に実施するとともに、実施状況を正確に把握した上で進捗管理を行うこと。なお、各保守事業者が実施する作業について、状況把握を行い必要に応じて指示する等、適切な進捗管理を行うこと。

(i) 運用管理業務計画書

調達仕様書等を踏まえた運用管理業務の年次、月次、日次等のスケジュールを立案する。(業務が繁忙となる時期や時間帯の運用管理業務の特性要件を踏まえた上で、無理なく実行可能なスケジュールを立案する。)

(ii) 年間計画及び月間計画等の運用スケジュール

- 運用スケジュールを作成の上、月次報告会にて報告し機構の承認を得ること。
- 本番環境・稼働維持環境において、年間計画及び月間計画を関連事業者と調整の上、運用管理業務計画書に基づき、運用対象システムの運用スケジュール作成及び履行状況の管理を行うこと。

(iii) 立案した計画に基づく各種作業の実施と確認

運用スケジュールに基づき、所定の手順に従って定常運用を行うとともに、機構に対して月次報告会で稼働報告を行うこと。

(2) IT 資産管理

① ライセンス管理

本調達受託者は、運用監視拠点、拠点等にて使用している市販ソフトウェア等のライセンス(対象は閲覧資料「管理対象ソフトウェア一覧」を参照すること)において、各種ライセンスが適切に利用されているか使用状況を随時管理し、機構 ICT 基盤の増設・撤去時等におけるライセンス保有数の不足等による業務への支障、法令違反となる不正使用等を回避するため、管理台帳を用いて適正な管理を行うこと。

また、本システム外で使用している管理対象ソフトウェアのライセンスに対し、機構から情報を受領した場合は合わせて管理を実施すること。

(3) セキュリティ管理

① ウイルス検知時の対応

共通基盤システムのウイルス対策機能によりウイルスを検知した場合又は拠点職員等からウイルス感染の申告があった場合は、即座にウイルスの駆除及び削除等の措置を行うこと。また、関連事業者と

連携し影響範囲を調査の上、機構職員と対応について協議を行うこと。

ウイルス対策機能を導入しているサーバ(他システム含む。)においてウイルス感染が発生した際は、関連事業者と連携し駆除及び削除等の措置を行うこと。

(参照:「情報セキュリティ対応手順書 ウイルス検知時の対応手順」)

② 不正アクセス検出時の対応

本調達受託者は、不正アクセスを検出した場合、機構職員に報告すること。また、機構職員の指示に基づき、ログを取得・調査し、原因、影響範囲等に関する調査結果を報告すること。なお、未知の不正アクセスパターンを検知した場合、関連事業者と連携の上、対応方法を検討する必要があることに留意すること。また、必要に応じて、侵入経路の遮断を実施し、作業結果を報告すること。

③ セキュリティインシデントへの対応

本調達受託者は、機構外からの不審通信に関する通報への対応や、機構外で拡大している攻撃等に対する影響の確認、防止対応について、機構からの要請があった場合には、機構との協議に応じること。

④ 運用保守ユーザ ID 管理

本調達受託者は、運用・保守作業で使用する ID を棚卸しし、必要であれば運用保守ユーザ ID の登録削除を実施すること。

⑤ 運用保守ユーザ ID の認証情報管理

本調達受託者は、機構ポリシーに従い、管理対象システムのシステム運用アカウントのパスワード管理を実施すること。

(4) 影響調査

以下の対応を実施すること。

- ① 機構職員からのシステム仕様に係る問合せ
- ② システム改修等の要望に係る影響調査及び見積要件定義の支援
- ③ 関連事業者からの各種照会対応
- ④ 新規イベントや工事発生時の担当間調整

(5) 報告業務

日次での前運用日の運用管理業務状況、定期的なアカウントやソフトウェアライセンス利用状況の報告、月次報告の取りまとめ、資料作成や別途定めている SLA 状況の報告等の報告業務を行うこと。

4.5.5 定例外作業の取扱い

本調達受託者は、「表 4.5.1 機構 ICT 基盤運用管理業務」に示す業務のうち、作業規模・実施内容が見込めない定例外作業について閲覧資料「作業指示書処理フロー」を参照し、作業項目に応じた作業指示書を受領の上、作業を実施すること。当該作業における作業指示書については、機構の指定した様式のものを利用する。

なお、入札金額の算定にあたっては、運用期間中に毎月「3.3.3 業務量」の定例外作業の月平均件数が発生すること及び次期運用管理事業者への引継ぎの実施を前提とした運用対象システムの運用管理業務金額を含めること。

定例外作業については、作業指示書の内容に基づき、影響調査及び見積りを実施すること。

なお、定例外作業の実施については、以下の契約条件にて機構との協議の上、契約形態及び支払い方法に係る条件を別途契約書において定めるものとする。

- 閲覧資料「作業単価表」に示す様式及び記載内容に沿って作成された契約金額の根拠となる単価表を、提案書の一部として提示すること。提示された単価表は契約書の一部として取り扱う。
- 参考情報となる定例外作業の件数は、「3.3.3 業務量」に記載しているが、当該記載事項は契約期間の利用見込みを示したものであり、契約期間中において随時見直しを実施するものとする。
- 定例外作業に係る支払いについては、人月工数に要員単価を乗算した金額とし、作業指示書又は工事実施報告書の受領をもって支払うものとする。
- 単価表に記載された部材費等標準価格が上昇する場合は、契約時と同等の提供価格で作業を実施すること。
- 単価表に記載された部材費等標準価格が低下する場合は、低下した標準価格に最新の単価表に記載された割引率を乗じた提供価格を算出し、単価表を修正した上で、変更契約を行う。
- 作業単価表に記載のない作業は、作業実績を重ねた上で、機構と協議を行い、作業単価表に追加した上で、変更契約を行う。

① 影響調査・見積依頼

機構 ICT 基盤運用管理サービスの契約工数範囲を超える作業が発生する見込みがある場合に、作業指示書の内容に基づき、影響調査、要件整理及び見積りを実施すること。なお、影響調査・見積依頼については、契約工数範囲の中での対応とする。

② 精査の実施

「4.5.5①影響調査・見積依頼」によって、対応が必要と判断された場合に、作業指示書の内容に基づき、作業を実施すること。作業実施にあたっては、あらかじめ「4.5.5①影響調査・見積依頼」の結果について機構により精査が行われていること。

なお、以降同様の作業が発生した際の精査を簡略化するため、順次作業単価表への追加を検討し、契約変更にて反映を図る。

4.6 プロジェクト管理

4.6.1 コミュニケーション管理

本調達受託者は、以下の要件を踏まえオペレーション業務関連の情報の作成、収集、配布、共有、蓄積等の一連のプロセスに関するルールを定め、そのルールを適正に運用することによりコミュニケーション管理を円滑に進めること。

- (1) コミュニケーション管理に係る計画、現行の仕組み及び報告フォームの作成及び見直しを行い、機構の承認を得ること。なお、作成にあたっては以下の事項に留意すること。
作業者がいつ(どのようなタイミング/サイクルで)、誰に対し、何を(どのような情報/メッセージ)、どのように(どのような手法を使って)伝えるのか、フィードバックはどのように実施するのか、というコミュニケーション管理のための仕組みを構築すること。
報告フォームには、現状、計画との差異、今後の予測及び対応策等の記載を必須とし、機構によるオペレーション業務の状況・進捗の把握、各種判断が容易にできるよう配慮すること。
- (2) 本調達受託者は、「図 3.1.1.1 運用対象システムの範囲」に示された受託業務の対象範囲内の機器に係る運用管理サービス業務、オペレーション業務を主体的に実施するとともに、実施状況を正確に把握した上で進捗管理を行うこと。
- (3) 各運用対象システムの保守事業者が実施する作業について、状況把握を行い必要に応じて指示する等、適切な進捗管理を行うこと。
- (4) 作成したコミュニケーション計画を基に会議・報告会を開催し、機構に報告を行うこと。

4.6.2 品質管理

事業及び業務に求められる IT サービスを提供するための全ての設備、資源、環境及び活動に関する品質を管理すること。

4.6.3 インシデント管理

発生したインシデントに対して、早急なサービス復旧や事後検証等適切な対応を行うため、報告の手順や対応状況に関する記録の登録・維持管理を行うこと。

4.6.4 問題管理

インシデントの発生に関する根本原因を究明し、その解決方法を作成して、インシデントの再発を防止すること。また、蓄積されたインシデント情報等を基に、インシデントの根本原因となり得る欠陥を洗い出し、その除去方法を作成することにより、潜在的なインシデントの発生を未然に防止すること。

4.6.5 変更管理

- (1) 業務概要
システムに対する変更要求を記録し、変更に対する対応状況の監視を行うこと。
- (2) 作業概要
本調達受託者は、システムに対する変更要求の受付と管理ツールへの登録及び変更状況の監視を行うこと。また、変更が完了した際は状況をまとめて機構に報告すること。なお、障害発生時の緊急変更

に際しては、事前に機構と調整し対応手順を定めること。

4.6.6 リリース管理

(1) 業務概要

システムのリリース作業の実施計画の策定と管理を実施すること。

(2) 作業概要

本調達受託者は、アプリケーション保守事業者及びハードウェア保守事業者が検証環境で実施したテスト結果、環境変更にあたっての手順書、資材の確認を行うこと。

また、本調達受託者は、本番環境に対するリリース作業の実施計画を策定し、本番環境変更の可否の判断を機構に求め、承認を得た上で関係事業者への作業指示等を実施すること。本番環境の変更作業にあたり、本番用機構 ICT 基盤や社会保険オンラインの停止を必要とする場合は、機構と協議の上、オンラインの停止及び再開始に関する作業の計画及び管理を行うこと。

4.6.7 リスク管理

「日本年金機構リスク管理規程(規定第 7 号)」及び「システムリスク管理要領(要領第 18 号)」を踏まえシステムを安定的に稼働させる上で懸念されるリスクを抽出し、課題管理を行い、対処方針、対処スケジュールを明確にした上で定期的にリスク状況を監視し、監視結果を進捗会議において報告すること。

4.6.8 情報セキュリティ管理

本調達受託者は、「日本年金機構情報セキュリティポリシー(規程第 16 号)」に則した情報セキュリティ対応手順、セキュリティ事故対策手順等の作成を実施すること。

専任の情報セキュリティ管理責任者のもと、セキュリティ管理に係る手順等にのっとり、対応を推進すること。ウイルス定義ファイルやセキュリティパッチの公開情報の管理、及び本システムへの適用状況の管理、セキュリティ事故の発生状況の管理を行うこと。

運用管理においてセキュリティに係る問題が確認された場合、セキュリティ管理に係る手順等にのっとり、確実に対策を実施するとともに、対応状況を管理すること。また、対応状況について機構職員に報告すること。

4.6.9 構成管理・ドキュメント管理業務

本調達受託者は、本番環境にインストールされているプログラム/テーブル、及びドキュメントの資材管理(原本管理、変更履歴管理)を実施すること。

また、本調達受託者は、改修資材又は新規資材を提供する事業者(以下、「資材提供者」という。)、及び資材を受領する事業者(以下、「資材受領者」という。))の依頼に応じて、各種資材及び資材情報の提供、貸与を行うこと。なお、障害時等には緊急の対応が必要であることから、本調達受託者は 24 時間連絡が取れる体制を構築し、これに対応すること。

資材の提供とは、本調達受託者へ返却を必要としない資材の提示形態である。資材の貸与とは、本調達受託者へ返却を必要とする資材の提示形態であり、市販ソフトウェアのインストール媒体等の物理的な資材が対象となる。

構成管理・ドキュメント管理に係る、関連事業者を含めた役割を「表 4.6.9.1 構成管理に係る役割」に示す。

表 4.6.9.1 構成管理に係る役割

項番	区分	主な役割
1	機構	本調達受託者から提示される資材開放・提供・貸与の依頼に対して必要性や資材内容等を確認し、資材開放・提供・貸与の承認を行う。
2	本調達受託者	資材提供者からの資材開放に対して、機構職員に承認依頼を行い、資材管理台帳及び原本の資材の更新を行う。 また、資材受領者からの提供・貸与依頼に対して、機構職員に承認依頼を行い、原本の資材から提供・貸与を行う。
3	アプリケーション開発(保守)事業者	・資材提供者としての役割 機構 ICT 基盤における資材を本番稼働環境へ開放(リリース)する場合、本調達受託者に対して資材開放通知書及び資材を提示すること。 ・資材受領者としての役割 機構 ICT 基盤の維持及び開発において資材が必要な場合、本調達受託者に対して資材提供依頼・資材貸与依頼を提示し、資材を受領すること。
4	各システムハードウェア保守事業者	
5	機構 ICT 基盤ハードウェア事業者	
6	OS 契約事業者	

(1) ドキュメントに係る構成管理

ドキュメントの原本の更新契機は、テスト等で内容の確認が完了して本調達受託者へドキュメントを開放(リリース)する時又は機構へ納品する時とする。仕様の変更等により原本ドキュメントの更新要件が発生した場合、本調達受託者は資材提供者の更新依頼に基づきドキュメント及びドキュメント情報の最新化を行うこと。

ドキュメントの原本及びドキュメント管理台帳の管理・保管は本調達受託者が行うこと。本調達受託者はドキュメント提供事業者、又はドキュメント受領者の依頼に応じて、各種ドキュメント及びドキュメント情報の提供、貸与を行うこと。

なお、ドキュメントの提供とは、本調達受託者へ返却を必要としないドキュメントの提示形態であり、電子ファイルでの提供となる。また、ドキュメントの貸与とは、本調達受託者へ返却を必要とするドキュメントの提示形態である。保管対象となる全ての文書は、「日本年金機構文書管理規程(規程第 12 号)」に基づいて管理実施すること。

① ドキュメントの提供

電子ファイルで保管されたドキュメントについて、ドキュメント受領者からの依頼に基づき、保管しているサーバ等により必要なドキュメントの提供を行うこと。ドキュメントの提供に際しては、機構の承認を必要とする。

② ドキュメントの貸出

紙面のドキュメントについて、ドキュメント受領者からの依頼に基づき、必要なドキュメントを貸与し、貸与状態の管理を行うこと。ドキュメントの貸与に際しては、機構の承認を必要とする。

③ ドキュメントの開放

ドキュメント提供者からの依頼に基づき、原紙(電子ファイル)の更新及び保管しているドキュメント(紙面)の差し替えを行い、ドキュメント管理台帳の更新を行うこと。ドキュメントの更新に際しては、機構の承認を必要とする。なお、保守の手順書については、全国の保守拠点への配布・差し替え作業が必要となることに留意すること。

(2) プログラム、テーブル等に係る構成管理

資材及び資材管理台帳の管理・保管は本調達受託者が行うこと。本調達受託者は資材提供者の依頼に応じて、各種資材及び資材情報の提供、貸与を行う。

なお、資材の提供とは、本調達受託者へ返却を必要としない資材の提示形態である。また、資材の貸

与とは、本調達受託者へ返却を必要とする資材の提示形態であり、市販ソフトウェアのインストール媒体等の物理的な資材が対象となる。

資材原本の更新契機は、本番環境へ資材を開放(リリース)する時とすること。プログラムの修正等により原本の資材更新(新規追加・変更・削除)要件が発生した場合、本調達受託者は資材提供者の更新依頼に基づき資材及び資材情報の最新化を行うこと。

(3) 資材の提供

プログラム等の電子ファイルの資材について、資材受領者からの依頼に基づき、保管している資材より必要な資材の提供を行うこと。資材の提供に際しては、機構の承認を必要とする。

① 資材の貸出

媒体等物理的な資材について、資材受領者からの依頼に基づき、保管している資材より必要な資材の貸与を行い、貸与の状態の管理を行うこと。資材の貸与に際しては、機構の承認を必要とする。

② 資材の開放

資材提供者からの開放依頼に基づき、保管している資材の更新を行い、併せて各種資材管理台帳の更新を行うこと。資材の開放に際しては、機構の承認を必要とする。

4.6.10 要員管理

予定されているイベントや運用管理業務に応じ必要な要員を確保し、要員の配置及びシフト計画を作成、報告すること。

(1) 作業体制

① 要員構成及び必要な技能

本調達受託者は受託業務を実施する上で、「調達仕様書 図 5.1.1 作業実施体制」及び「調達仕様書 表 5.1.1 作業実施体制と役割」に示す職責を担う担当者について、「調達仕様書 5.3 作業要員に求める資格等の要件」を満たす要員とすること。

なお、運用統括管理責任者、運用統括管理者及び運用管理グループについては、日本語をベースとした高いコミュニケーション能力を持つ要員を配置すること。

② 事前届出

本調達受託者は業務開始 3 か月前までに機構へ報告すること。併せて、要員の連絡先、主な業務経歴を記載した書類を作成し機構へ提出すること(任意様式)

③ 代替要員の確保

本調達受託者は、要員の欠勤及び気象状況等により通常の交通機関が利用できないことで従事要員に不足が生じる場合に備え、業務に支障をきたさないよう交代要員を確保すること。

④ 要員の変更

契約期間中において自己都合により要員を変更する場合は、5 営業日前までに「4.6.10(1)②事前届出」に従い書類を作成し、機構へ提出すること。この場合、変更後の要員は、「調達仕様書 5.3 作業要員に求める資格等の要件」を有する者としてすること。また、要員変更に伴い業務に支障が生じないよう、「3.7 教育に関する事項」による教育及び引継ぎを確実にすること。

(2) 要員の研修

研修の実施について、以下のとおり「3.7 教育に関する事項」における研修を実施し、運用対象システムのシステム構成、運用管理業務の手順等について学習し、理解すること。また、新規に運用管理業

務を担当する予定の者がいる場合は、習得訓練を実施し、運用管理業務を円滑に実施すること。

- ① 要員に対し、委託業務の開始前まで、又は委託業務開始後に初めて委託業務を行う要員の業務開始前までに、日本年金機構法や情報セキュリティ要件、個人情報等に関する関係法令に係る教育を実施すること。さらに、業務開始後においても定期的に教育を行い、個人情報等の取扱いを徹底すること。
- ② 日本年金機構法や個人情報等に関する関係法令で定められた守秘義務及び罰則規定、委託業務における遵守事項及び禁止事項、個人情報等の保護に係る就業規則等に違反した場合の処分、情報漏えいとその影響、インシデントが発生した場合の手順、その他必要な留意事項について研修を行うこと。
- ③ 研修資料等及び教育・研修・訓練の実施結果の提出を機構から求められた場合には、速やかに提出すること。なお、本調達受託者が実施する研修において、上記で示す研修項目の一部を実施していないと機構が確認した場合、機構は、総括責任者等へ指導を行い、研修内容の改善及び研修の実施について、本調達受託者に指示することができること。

4.6.11 稼働状況管理

本調達受託者は、運用管理業務において、日々のインシデント、障害内容に関する各関係者間での情報共有や当日の作業内容等の確認、作業の進捗状況の確認を行い、運用管理業務を滞りなく実施すること。

(1) 報告形態

本調達受託者は、対象各システムの稼働状況について機構に月次で報告すること。非正常運用、システム保守業務、障害対応作業については、機構に随時作業内容の説明、作業結果の報告を行うこと。報告形態の詳細について、「表 4.6.11.1 報告形態」に示す。定例報告会の日程については、契約締結後、協議の上、決定する。

表 4.6.11.1 報告形態

項番	会議体名称	開催周期	備考
1	月次稼働報告会	月次	運用管理業務について、月次稼働報告を行う。
2	作業説明、作業結果報告	随時	非正常運用、システム保守業務について、作業説明、作業結果報告を行う。
3	障害対応報告会	随時	障害対応作業について、事象、影響、暫定対応、本格対応、再発防止策等の報告を行う。
4	契約完了報告会	契約終了後 1 週間以内	契約期間内に実施した運用管理業務について報告を行う（「調達仕様書 4.2.1 納品成果物等」参照）。

※1:その他機構の求めに応じて適宜報告を行うこと。

(2) 報告書の作成

① 稼働報告書

前月の運用・保守に係る活動内容、次月計画、各種対応状況、リソース利用状況、サービスレベル達成状況、リスク・課題の把握・対応状況等をまとめた「稼働報告書（「調達仕様書 4.2.1 納品成果物等」参照）」を作成し、機構の承認を得ること。稼働報告書の記載項目については業務開始前に機構よりフォーマット提示する。主な項目については、「表 4.6.11.2 稼働報告書の記載項目例」に示す。

表 4.6.11.2 稼働報告書の記載項目例

項番	記載項目	備考
1	システム運転状況	
2	運転状況報告	報告対象期間における管理対象システムの運転状況の報告。
3	インシデント管理状況報告	報告対象期間におけるインシデント発生件数とその対応状況の報告。
4	問題管理報告	報告対象期間における問題状況、解決に向けた分析や対策の報告。
5	キャパシティ報告	報告対象期間におけるシステムの CPU、メモリ、ディスク、回線等のリソース使用状況。
6	問合せ状況報告	システムの障害時を含め、実際にシステムを使用しているユーザからの問合せ内容、件数、問合せの回答状況を確認する。
7	構成管理報告	ハードウェアやソフトウェアの構成管理、各種マニュアルや設計書等の変更管理状況の報告。
8	保守作業実施報告	定期的なバックアップの取得状況、ハード障害発生状況の報告。
9	リリース管理報告	業務アプリケーション資材のリリース状況、システム変更対応の報告。
10	リスク管理報告	システムの安定稼働を阻害するリスク状況の報告。
11	作業実績報告	
12	運用管理業務	報告対象期間における管理対象システムの運用役務の実施報告。
13	セキュリティ施策実施状況報告	
14	脆弱性対策報告	ハードウェア事業者、NCO 等から提供のセキュリティパッチ一覧とその適用状況の報告。
15	ファームウェア適用状況報告	使用しているハード機器への最新ファームウェア適用状況。
16	ウイルス対策ソフトの状態報告	ウイルス対策ソフトの最新バージョン、パターンファイル適用状況。
17	使用製品のサポート期限切れ報告	搭載ソフトウェアのサポート期限、次期更改までのバージョンアップ含めた対応方針の報告。
18	管理者権限アカウント管理状況報告	管理者権限アカウントの使用状況の報告。
19	ユーザ情報/パスワードの管理	ユーザアカウントのパスワード管理状況の報告。
20	マシン室入室退室等状況報告	マシン室へ、いつ、何の目的で入室したかの報告。
21	危険化情報	安全性レベルが低下している暗号化アルゴリズム使用、対策状況の報告。
22	サービスレベル管理報告	
23	サービス実績報告	調達仕様書、SLA 合意書、サービスレベル合意書等、で定義された SLA 達成状況の報告。
24	運用管理担当者の教育状況報告	運用管理担当者へのセキュリティ等の教育実施状況の報告。
25	その他	
26	お願い事項	本調達受託者からのお願い事項やその他連絡事項。
27	連絡票の発行状況について	作業連絡票の発行状況。
28	次月以降の予定	次月以降のイベント、作業予定。
29	要員の変更について	運用実施体制、要員変更の方向。

② 作業計画書及び作業結果報告書

非定常運用、システム保守業務について、作業内容、対象機器、作業スケジュール、検証観点、業務影響等をまとめた「作業計画書」（「調達仕様書 4.2.1 納品成果物等」参照）を作成し、機構の承認を得ること。また、作業後に「作業結果報告書」（「調達仕様書 4.2.1 納品成果物等」参照）を作成し、機構に報告すること。

作業計画書の記載項目（必須項目）については「表 4.6.11.3 作業計画書の記載項目（必須項目）」に、作業結果報告書の記載項目（必須項目）については「表 4.6.11.4 作業結果報告書の記載項目（必須項目）」に示す。

表 4.6.11.3 作業計画書の記載項目(必須項目)

項番	記載項目	備考
1	作業の内容	作業の内容を記載する。機構が求めた場合には概要図等を挿入し、理解が容易な記載をすること。
2	対象機器	作業の対象機器を記載する。
3	作業スケジュール	作業スケジュールを詳細に記載する。
4	検証観点	検証観点を記載する。
5	影響範囲	業務への影響、国民への影響、年金事務所、事務センター等への影響、外部実施機関への影響、関連システムへの影響を記載する。
6	コンティンジェンシープラン	コンティンジェンシープランを記載する。

表 4.6.11.4 作業結果報告書の記載項目(必須項目)

項番	記載項目	備考
1	作業の内容	作業計画書から転記する。
2	対象機器	作業計画書から転記する。
3	作業スケジュール	作業計画書から転記する。
4	検証観点	作業計画書から転記する。
5	影響範囲	作業計画書から転記する。
6	検証結果	検証結果を記載する。

③ 障害報告書

発生した障害に対する影響範囲、原因、暫定対応、本格対応等をまとめた「障害報告書(「調達仕様書 4.2.1 納品成果物等」参照)」を作成し、機構の承認を得ること。障害報告書の記載項目(必須項目)については、「表 4.6.11.5 障害報告書の記載項目(必須項目)」に示す。

また、障害報告第 1 報(初報)に関しては、項番 1～3 の内容を記載すること。

表 4.6.11.5 障害報告書の記載項目(必須項目)

項番	記載項目	備考
1	発生日時	障害の発生日時、障害の確認日時、確認した契機を記載する。
2	発生事象	事象の概要を記載する。1 報以降は、概要図等を挿入し理解が容易な記載をすること。
3	影響範囲	業務への影響、国民への影響、年金事務所、事務センター等への影響、外部実施機関への影響、関連システムへの影響を記載する。
4	原因	直接原因、根本原因を記載する。
5	対策	暫定対応、本格対応を記載する。
6	類似見直し	類似見直しを行った結果を記載する。
7	再発防止策	再発防止策を記載する。

4.6.12 SLA 管理

(1) サービスレベル管理の目的

システムを運用するにあたり本調達受託者が提供するべきサービスの品質を担保する指標として、サービスレベルを定める。

本システムにより提供されるサービスについては、高い品質が維持されることが必要である。本調達に係る品質は、機構が求める品質を確保するための指標、SLA(Service Level Agreement)として管理する。

(2) サービスレベルの設定項目と障害レベル

本運用対象システムの運用管理業務に関して確保すべきサービス品質の目標に係る SLA は、機構と本調達受託者との間で締結し遵守すること。なお、本調達受託者が遵守すべき SLA 設定項目は、「表 4.6.12.1 サービスレベル設定項目(運用管理業務)」のとおりであるが詳細な条件については、機構と協議の上、決定するものとする。

また障害レベル(障害発生による影響)については、「表 4.6.12.2 サービスレベル(障害レベル)」に示す。

表 4.6.12.1 サービスレベル設定項目(運用管理業務)

項番	SLA 項目	条件			評価水準
1	障害検知等の発生から初期レスポンスまでのリードタイム	業務用機構 ICT 基盤オンライン稼働時間。 社会保険オンラインシステムのサービスが業務用機構 ICT 基盤拠点に提供される時間帯 ※社会保険オンラインシステムセンタ設備のシステム障害によるサービス停止時間を除く ・開所する平日の稼働時間 8:30～18:00 ・開所する土日・祝日の稼働時間 8:30～17:00 ・延長日の稼働時間 8:30～19:30		10 分以内	100%
		上記以外の時間帯		2 時間以内	100%
2	駆け付け時間 (拠点端末装置群) ※各区分については、閲覧資料 「管理対象装置一覧」参照	区分 1	政令指定都市、県庁所在地等	1 時間以内	対象外
			上記以外の地域	2 時間以内	対象外
		区分 2		2 時間以内	対象外
		区分 3		4 時間以内	対象外
		区分 4		5 時間以内	対象外
3	駆け付け時間 (マシン室設置機器群) ※端末機器を除く ※各区分については、閲覧資料 「管理対象装置一覧」参照	区分 5		1 時間以内	100%
4	平均故障復旧時間 (拠点端末装置群) ※各区分については、閲覧資料 「管理対象装置一覧」参照	A 群	政令指定都市等	4 時間以内	対象外
			上記以外の地域	5 時間以内	対象外
		B 群		5 時間以内	対象外
		C 群	保守機対応可能	6 時間以内	対象外
			保守機対応不可	14 時間以内	対象外

項番	SLA 項目	条件			評価水準
		D 群		50 時間以内	対象外
		E 群	INS、NPR、XPR、CPR	2 営業日以内	対象外
			SCAN(複合機無拠点)、QPR	4 営業日以内	対象外
			SCAN(複合機有拠点)	なし	対象外
			上記以外の設置機器	6 時間以内	対象外
		F 群	中継サーバ	8 時間以内	対象外
5	平均故障復旧時間 (マシン室設置機器群) ※端末機器を除く ※各区分については、閲覧資料 「管理対象装置一覧」参照	G 群	アクセス権管理サーバ,生体認証サーバ	4 時間以内	100%
			上記以外の設置機器	6 時間以内	100%
6	脆弱性情報の確認から報告までのリードタイム	-		24 時間以内	100%
7	コンピュータウイルス又はワーム等の確認から報告までのリードタイム	・受託者の監視対象であるウイルス検知対策ソフトでの検知のみ対象とする。 ・ウイルス検知対策ソフトによる検知が複数件同時に発生した場合等、受託者の対応に輻輳が発生する場合は SLA 評価の算定から除く。		20 分以内	100%
8	セキュリティ侵害確認から報告までのリードタイム	-		20 分以内	100%
9	本調達受託者(運用管理業務)の責による障害発生件数	本調達受託者(運用管理業務)の責(構成管理・リリース管理誤り)により発生した障害レベル 1 以上の障害件数		0 件	100%
		本調達受託者(運用管理業務)の責により発生した障害レベル 3 以上の障害件数		0 件	100%

表 4.6.12.2 サービスレベル(障害レベル)

項番	障害レベル	障害発生による影響	
		社会保険オンラインシステム	左記以外
1	レベル 4	同一理由で複数拠点利用不可(1 時間以上)	利用者の 2 割以上が利用不可(4 時間以上)
2	レベル 3	同一理由で複数拠点利用不可(30 分以上 1 時間未満) 一拠点で利用不可(4 時間以上)	利用者の 2 割以上が利用不可(1 時間以上 4 時間未満) 利用者の 2 割未満が利用不可(4 時間以上)
3	レベル 2	同一理由で複数拠点利用不可(10 分以上 30 分未満) 一拠点で利用不可(20 分以上 4 時間未満)	利用者の 2 割以上が利用不可(30 分以上 1 時間未満) 利用者の 2 割未満が利用不可(1 時間以上 4 時間未満)
4	レベル 1	レベル 2 に該当しない範囲で利用不可	レベル 2 に該当しない範囲で利用不可
5	レベル 0	システムの利用継続ができていない	システムの利用継続ができていない

(3) サービスレベル管理の活動計画

サービスレベル管理に関し、活動計画の策定を行うこと。

(4) サービスレベルの遵守及び管理

サービスレベル合意書に記す SLA 項目について、サービスレベルの管理状況をサービス実績報告書、改善状況報告書として報告し、機構の評価を受けるとともに、評価に基づくサービスレベルの改

善、向上のための施策を実行すること。

なお、サービスレベル設定項目について、追加設定すべきと考えるサービスレベル設定項目及び目標値については提案を行い、随時機構と協議すること。

① 業務概要

機構と合意したサービスレベル設定項目の目標値に対して、遵守状況を管理する。

② 作業概要

機構と合意したサービスレベル設定項目に対する実績を確認し、遵守状況をまとめた「サービスレベル管理状況報告」を月次報告会で機構に報告すること。

(i) 基本的な考え方

月次報告会において、「サービスレベル管理状況報告」を提出し、当該 1 か月間のサービスレベルの達成状況を報告すること。

また、合意したサービスレベルが未達成だった場合、原因分析、改善案、改善スケジュールを明示した「改善状況報告書」を作成し、月次で機構へ報告すること。

(ii) 体制維持

異常気象等、交通の混乱から要員の交代等が予定どおりに行えない場合は、勤務の延長等を行うことにより、システム操作員が一人もいない状態がないよう調整すること。

(iii) 無償による対応

サービスレベル協定が遵守できなかった場合に必要となる作業は、本調達の役務範囲に含まれるものとし本調達受託者の負担により無償で行うこと。

(iv) その他

「サービスレベル管理状況報告」作成のために必要な作業があれば実施すること。

(v) 免責事項

以下に起因する障害については免責とする。

- インフラ障害、電源供給や通信の障害
- ハードウェア及びソフトウェアパッケージに起因する障害
- 機構の過失及び故意による障害

(5) サービスレベルの改善

機構と本調達受託者間で合意したサービスレベルの達成度合いを監視し、必要に応じて機構に対し改善策を提案し、サービスレベル達成に向けた改善を実施すること。

(6) サービスレベル改善の支援

運用対象システムの改修等により運用設計に変更が生じる場合、専門的見地から効率的な運用設計の提案を行うこと。提案内容は機構と協議の上、調整する。サービスレベル改善提案として作業効率化かつ品質向上につながる提案を年 2 回実施すること。

4.7 業務終了

本調達受託者は、本調達案件の終了にあたり、以下のとおり、書類を作成し、機構の承認を得ることとする。

4.7.1 次期運用管理事業者への引継ぎ

(1) 引継ぎ計画書

本調達受託者は、契約終了 3 か月前までに、引継ぎ計画書を機構へ提出し承認を得ること。引継ぎ計画書の記載項目(必須項目)については、「表 4.7.1.1 引継ぎ計画書の記載項目(必須項目)」に示す。
上記で、承認を得た計画にて、次期運用管理事業者に対し、期間内に引継ぎを実施すること。
なお、本調達受託者と次期運用管理事業者が同一でかつ現行の運用体制が維持される場合は実施不要とする。

表 4.7.1.1 引継ぎ計画書の記載項目(必須項目)

項番	記載項目	記載内容
1	引継ぎ対象	対象となる契約を明記し、対象システム、対象機器、資材、業務を明記する。
2	体制・スケジュール	引継ぎの体制及びスケジュールを記載する。
3	実施内容	引継ぎの実施形態、実施方法、引継ぎに用いる資料等を記載する。
4	習熟度判定	実施する引継ぎの習熟度判定と分析を実施する。
5	完了基準	次期運用管理事業者と確認した完了基準を記載する。
6	管理方法	進捗管理、課題管理、コミュニケーション管理等の引継ぎの管理項目、管理方法等を記載する。

(2) 引継ぎ完了報告書

本調達受託者は、引継ぎ完了後 2 週間以内に引継ぎ完了報告書を機構へ提出し承認を得ること。引継ぎ完了報告書の記載項目(必須項目)は「表 4.7.1.2 引継ぎ完了報告書の記載項目(必須項目)」に示す。

表 4.7.1.2 引継ぎ完了報告書の記載項目(必須項目)

項番	記載項目	記載内容
1	引継ぎ対象	対象となる契約を明記し、対象システム、対象機器、資材、業務を明記する。
2	体制・スケジュール	引継ぎの体制及びスケジュールを記載する。
3	実施結果	実施結果を記載する。
4	引継ぎ実施方法と結果	引継ぎ計画書に記載した実施方法とその結果(完了日、工数等)を記載する。
5	習熟度判定	引継ぎ計画書で設定した習熟度判定とその分析を記載する。
6	残課題及び申し送り事項	引継ぎ実施において発生した残課題、申し送り事項を記載する。
7	完了確認	引継ぎ計画書において設定した完了基準の達成状況を記載する。
8	管理結果	引継ぎ計画書において設定した管理項目の実施状況を記載する。

4.7.2 最終報告書

本調達受託者は、受託期間満了と同時に、受託期間内に実施した作業の最終報告書を作成、機構へ報告を行うこと。最終報告書の記載項目(必須項目)については、「表 4.7.2.1 最終報告書の記載項目(必須項目)」に示す。

表 4.7.2.1 最終報告書の記載項目(必須項目)

項番	記載項目	記載内容
1	プロジェクト概要	プロジェクトの概要を記載する。
2	契約概要	対象となる契約名、契約期間、契約工数を明記する。
3	変更契約	契約期間内に変更契約が発生した場合は、変更内容、変更後契約工数等を記載する。
4	体制	受託業務を実施した体制を記載する。運用実施計画書にて計画した体制から変更した場合はその履歴を明記する。
5	作業実績	作業実績について記載する。
6	作業工数実績	各作業の工数の予実績を記載する。実績払いの作業が存在する場合は、実績払いの作業工数を記載する。また、予実差がある場合は、その理由を記載する。
7	インシデント及び問題管理	受託業務で発生したインシデント状況及び問題管理状況を記載する。重大障害が発生した場合は、その概要を記載する。未完了の問題がある場合はその内容を明記する。
8	サービスレベル達成状況	サービスレベル合意書で合意したサービスレベル評価項目の達成状況を記載する。
9	情報セキュリティ対策実績	情報セキュリティの対策実績を記載する。
10	作業工数実績	受託業務において発生した情報セキュリティインシデントの対応を記載する。
11	情報セキュリティ監査実施状況	受託業務において実施した情報セキュリティ監査実施実績を記載する。
12	情報セキュリティ自己点検実績	受託業務において実施した情報セキュリティ自己点検の実績を記載する。
13	対策が不十分な事象への対応	本プロジェクトにおいて、情報セキュリティ対策の履行が不十分と認められた事象、改善策、実施状況について記載する。
14	成果物納品	受託業務における成果物の納品状況を記載する。
15	引継ぎ	受託業務の引継ぎの状況を示す。
16	総括	受託業務の今後に向けた教訓等を記載する。
17	改善事項等	受託業務において実施した改善事項等を記載する。
18	作業品質向上施策	受託業務で発生した問題や課題について作業品質の改善や再発防止策等の概要を記載する。

【別紙2】 関連事業者との役割分担表

◎…主たる作業者
○…当該役務に関して作業担当と密に連携し、作業協力
※複数の業者に◎が付いている作業項目においては、各業者は担当する役務範囲の作業を主体的に実施することとする。
※環境毎の個別記載がない場合は原則本書、稼働維持どちらも役務に含む。

項番	作業項目	日本年金機構	等 保守事業者	機構ICT基盤（共通基盤システム	情報業務システム等運用・保守事業者	機構ICT基盤（拠点端末設備等）	プリンタ等保守事業者	社会保険オンラインシア等保守事業者	統合ネットワーク事業者	現行運用管理事業者	運用管理事業者（本調達受託者）	次期運用管理事業者	外部システム事業者	作業内容
1	事前準備													
2	事前準備計画													
3	事前準備作業計画書の作成	○									◎			準備作業を滞りなく実施するための事前準備作業計画書を作成する。（実施計画、訓練計画、構築計画、管理計画等）
4	運用計画支援													
5	運用管理計画作成のための情報受領									◎	○			運用実施計画書の作成に必要な情報を受領する。
6	運用計画													
7	運用実施計画書の作成	○								○	◎			運用管理業務の作業範囲、スケジュール、実施体制、実施計画、管理計画、リストア計画等を定めた「運用実施計画書」を作成する。
8	運用管理業務計画書の作成	○								○	◎			運用管理業務における具体的なタスクの定義及びスケジュールを具現化する（運用管理業務の作業範囲、スケジュール、実施体制、管理計画、作業計画等）運用管理業務計画書の作成を行う。
9	準備作業													
10	運用環境構築										◎			運用作業の場所、運用管理業務に必要な環境構築を行う。
11	引継ぎ、教育									○	◎			現行運用事業者からの引継ぎ、要員教育を行う。
12	運用業務													
13	管理業務													
14	運用管理資料一式の作成	○									◎			運用実施計画書(コミュニケーション管理、作業管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ管理)に基づき、運用管理業務に係る資料一式を作成すること。
15	月次報告	○		○	○					○	◎			月次での報告を行う。管理項目については、「閲覧資料 ITサービス業務標準」を参照し、定めること。(可用性管理、予算管理、キャパシティ管理、文書・データ保管管理、品質管理、インシデント管理、問題管理、リリース管理、セキュリティ施策実施(脆弱性対策、使用製品のサポート期限切れ等))
16	システム操作													
17	定常運用													
18	定常運用の実施	○									◎			運用スケジュールに基づき、所定の手順に従って定常運用を実施し、月次報告会で稼働報告を行う。
19	セキュリティパッチの適用	○									◎			ハードウェア、ソフトウェアに関するセキュリティパッチを適用する。
20	製品バージョンアップ、チューニング	○									◎			ハードウェア及びソフトウェアに関するバージョンアップの適用及びソフトウェアの検知精度向上のためのチューニング作業を実施する。
21	例外運用(非定常運用)													
22	例外運用(非定常運用)の実施	○									◎			作業タイミングがスケジュール化されていない業務を所定の手順に従って運用し、作業終了後及び月次報告会で稼働報告を行う。
23	システム変更	○	○	○	○	○	○	○			◎		○	システム変更作業及び正常動作確認を行う。
24	影響調査	○	○	○	○	○	○	○			◎		○	関連システムのシステム変更に伴う影響調査を行う。
25	作業依頼対応	○									◎			作業依頼に基づき、作業手順書を作成した上で、対応を行う。
26	情報セキュリティ監査	◎									○			定期的に外部専門機関が、情報セキュリティに関する監査及び検査を実施するため、必要な支援を行う。
27	イベント対応	○	○	○	○	○	○	○			◎		○	イベント(組織改編等)特性に応じて運用管理業務と連携し対応を行う。
28	計画停止	○	○	○	○	○	○	○			◎		○	システム停止・起動・起動後の状態／機能確認を行う。
29	マスタイメージ更新		○	○							◎			システム変更後のキッティング用マスタイメージの更新に必要な情報を提供する。
30	個別手順書										◎			端末ごとの個別手順書の作成を行う。
31	機構職員からのシステム質問・要望の確認	○									◎			機構職員からのシステム質問・要望などの問い合わせの対応、状況の確認。
32	関連事業者との照会対応	○	○	○	○	○	○	○			◎		○	関連業者との各種照会内容の対応、状況の確認。
33	システム影響調査	○	○	○	○	○	○	○			◎		○	定例外作業実施におけるシステム影響の調査、確認。
34	定例外作業の見積もり・要件定義支援	○	○	○	○	○	○	○			◎		○	定例外作業実施における見積もり要件定義の支援。新規イベント・工事発生時の要件整理、調整。
35	定例外作業の設計	○	○	○	○	○	○	○			◎		○	定例外作業実施における見積もり要件定義の支援。新規イベント・工事発生時の要件設計、ドキュメント修正。
36	定例外作業の資材・手順準備	○	○	○	○	○	○	○			◎		○	定例外作業実施における見積もり要件定義の支援。新規イベント・工事発生時の資材・手順実装。
37	定例外作業の試験・稼働確認	○	○	○	○	○	○	○			◎		○	定例外作業実施における見積もり要件定義の支援。新規イベント・工事発生時の試験・稼働確認。
38	定例外作業の試験対応（開発・ユーズ側試験支援）	○	○	○	○	○	○	○			◎		○	定例外作業実施における見積もり要件定義の支援。新規イベント・工事発生時の開発・保守側担当側試験の作業支援。
39	定例外作業の本番対応	○	○	○	○	○	○	○			◎		○	定例外作業実施における見積もり要件定義の支援。新規イベント・工事発生時の本番作業対応。
40	システム監視													
41	自動監視													
42	死活監視(システム、プロセス、ジョブ)										◎			システムの死活監視を行う。
43	メッセージ監視										◎			メッセージ監視を行う。
44	リソース監視										◎			CPU、メモリ、ディスク等のしきい値の監視を行う。
45	手動監視													
46	インシデント監視										◎			自動監視対象外(処理結果の確認、複雑な状況判断が必要な項目)となった項目の手動監視を行う。 なお、事故発生時等における例外的な手動監視（インシデント監視）に関しては、例外運用(非定常運用)とする。
47	障害監視										◎			自動監視対象外(処理結果の確認、複雑な状況判断が必要な項目)となった項目の手動監視を行う。 なお、事故発生時等における例外的な手動監視（障害監視）に関しては、例外運用(非定常運用)とする。
48	障害対応													
49	受付(一時切り分け)										◎			障害発生時の一元的な受け付け、適切な回答・案内等を行う。
50	関連事業者への照会、対応依頼		○	○	○	○	○	○			◎		○	利用者からの問合せに対する関連事業者への連携、照会、状況確認を行う。
51	関連事業者からの依頼事項対応		○	○	○	○	○	○			◎		○	関連事業者からの照会に際する依頼事項の対応。
52	対策報告	○									◎			問合せ内容の返答、クローズ対応。
53	ウイルス検知対応													
54	ウイルス検知・感染受付	○							○		◎		○	ウイルス対策機能によるウイルス検知、ウイルス感染の申告の受付。
55	問診・影響特定	○		○					○		◎			ウイルス検知した場合の利用者への連絡、感染状況の問診、状況からの影響特定を行う。
56	各種状況報告	◎		○	○	○	○	○			○			ウイルス感染状況の報告、関連事業者への連携を支援する。
57	ウイルス確認、ベンダ照会										◎			ウイルスの特性、ベンダへの問い合わせ。
58	対応検討、対策	○									◎			NW遮断、駆除及び削除等の措置の対応実施。
59	対策報告	○									◎			対策状況、結果の報告。
60	不正アクセス検出													
61	不正アクセス確認	○									◎			不正アクセス検出の確認。
62	一次報告	○									◎			不正アクセス検出の報告。

【別紙2】 関連事業者との役割分担表

◎…主たる作業者
○…当該役務に関して作業担当と密に連携し、作業協力
※複数の業者に◎が付いている作業項目においては、各業者は担当する役務範囲の作業を主体的に実施することとする。
※環境毎の個別記載がない場合は原則本番、稼働維持どちらも役務に含む。

項番		作業項目	日本年金機構	等 保守事業者	機構ICT基盤（共通基盤システム	情報業務システム等運用・保守事業者	機構ICT基盤（拠点端末設備等）	プリンタ等保守事業者	社会保険オンラインシステム等保守事業者	統合ネットワーク事業者	現行運用管理事業者	運用管理事業者（本調達受託者）	次期運用管理事業者	外部システム事業者	作業内容
63		ログ取得、影響特定、調査	○							○		◎			ログの取得・調査し、原因、影響範囲の特定を行う。
64		対策、遮断	○							○		◎			未知の不正アクセスパターンの対応方法を検討、侵入経路の遮断対応の実施。
65		報告	○									◎			状況、対応の報告。
66		セキュリティインシデント対応													
67		事象確認・情報収集	○						○	○		◎			ベンダや事象状況の情報収集、確認。
68		影響確認、報告	○									◎		○	不審通信に関する通報への対応や、機構外で拡大している攻撃等に対する影響の確認、防止対応。
69		対応検討	○						○	○		◎			対策状況、結果の報告。
70		運用保守ユーザ管理													
71		I D 管理（棚卸）	○									◎			運用・保守作業で使用するIDを棚卸。
72		登録、削除	○						○	○		◎			運用保守ユーザIDの登録、削除対応。
73		システムアカウントのパスワード変更	○									◎			管理対象システムのシステム運用アカウントのパスワード変更の実施。
74		SLA管理													
75		サービスレベルの監視	○									◎			サービスレベル合意書に記すS L A 項目について、サービスレベルの管理状況をサービス実績報告書、改善状況の監視。
76		サービスレベルの改善・支援	○									◎			機構と本調達受託者間で合意したサービスレベルの達成度合いを監視し、必要に応じて機構に対し改善策を提案し、サービスレベル達成に向けた改善。
77		サービスレベルの遵守及び管理	○									◎			月次定例報告において「サービス実績状況として提出し、当該1か月間のサービスレベル達成状況を報告と対処。
78	ヘルプデスク（現地拠点からの問合せ対応）														
79		問い合わせ・故障対応													
80		受付・問診（一時切り分け）	○									◎			機構ICT基盤の障害報告及び機構ICT基盤の操作方法等について、全国の利用者からの照会に対する一元的な受け付け、適切な回答・案内等を行う。またPC操作方法等の問合せの対応。
81		関連事業者への照会		○	○	○	○	○	○	○		◎		○	利用者からの問い合わせに対する関連事業者への作業連絡、照会の実施。
82		関連事業者の対応依頼に伴う作業支援		○	○	○	○	○	○	○		◎		○	関連事業者からの障害対処方法の検討、資材・手順作成の支援。
83		関連事業者からの依頼事項対応		○	○	○	○	○	○	○		◎		○	関連事業者への照会に際し、関連事業者からの依頼事項（センタ問診/調整、故障PC等のMACアドレス状況確認、個別ソフトのアンインストール調整など）の対応。また、拠点故障対応として、拠点職員様、保守業者の拠点対応時の入退所管理を行う。
84		回答	○									◎			問い合わせ内容の返答、クローズ対応。
85	ナレッジ対応														
86		問い合わせ・故障事象のデータベース登録										◎			問い合わせ、故障事象の蓄積、ノウハウの習得。
87		内容集計・分析										◎			問い合わせ個数や応答率など集計した情報、ノウハウなどの蓄積を行い、通話対応などの分析を行う。
88		ナレッジ対応の検討・提案	○									◎			品質維持観点から集計内容、分析結果から業務効率化や問い合わせの減少に向けた検討、提案を行う。
89		職員ポータルサイトメンテナンス	○									◎			職員ポータルサイトなどに、よくある問い合わせなどを表示させるようメンテナンスを実施する。
90		報告	○									◎			修正内容、分析内容、検討策の報告を行う。
91	センタ運営														
92		バックアップ取得													
93		作業計画・調整	○				○		○	○		◎			サーバ等センタ設置機器について、運用保守設計及び運用保守マニュアルに従いデータのバックアップ取得の調整、作業計画。
94		バックアップ取得										◎			サーバ等センタ設置機器について、運用保守設計及び運用保守マニュアルに従いデータのバックアップ取得の実施作業。
95		ログ情報の取得													
96		依頼受け付け、調整	○	○			○	○	○	○		◎		○	システム故障時の解析やサーバ運用業務で必要となる各種ログの取得を行うこと。なお、定例オペレーション等で取得しているログ以外のログ取得作業調整。
97		ログ取得										◎			システム故障時の解析やサーバ運用業務で必要となる各種ログの取得を行うこと。なお、定例オペレーション等で取得しているログ以外のログ取得。
98	予防保全														
99		機器点検（機構ICT基盤（共通基盤システム等）保守事業者）	○	◎								○			定期点検計画を作成し、機構ICT基盤（共通基盤システム等）保守事業者の担当者及び関連事業者と日程調整を実施したうえで、定期点検の実施、実施状況管理ならびに報告を支援する。
100		機器点検（拠点端末設備等事業者）	○				◎					○			定期点検計画を作成し、機構ICT基盤拠点の担当者及び関連事業者と日程調整を実施したうえで、定期点検の実施、実施状況管理ならびに報告を支援する。
101		統計データの蓄積、活用	○									◎			障害状況等のデータの蓄積・分析を実施し、予防保全の観点から障害回避策を作成し、月次に機構本部職員に報告。
102		システム動作確認	○									◎			安定したサービスを提供するために、ランプ確認等の目視確認、メール疎通確認、WEB閲覧状況確認等のシステム動作状況を確認。
103	法定点検														
104		設備計画の共有	◎									○			機構本部及び全国の年金事務所等拠点における定期的に実施される法定点検実施計画の情報共有を支援する。
105		準備・調整	○							○		◎		○	機構本部及び年金事務所等拠点における機構ICT基盤の法定点検にかかる情報を把握し、計画の作成。関連業者への周知を行う。
106		点検対応（サーバ停止、サーバ起動）	○									◎			計画に基づき関連事業者とともに作業を実施する。
107		報告	○									◎			結果について取りまとめ、報告を行う。
108	統計データ取得														
109		統計（リソース）情報取得							○	○		◎		○	センタ設置機器に対するリソース情報（C P U 使用率、メモリ使用率、ディスク使用率等）を取得、管理すること。
110		報告	○									◎			センタ設置機器に対するリソース情報（C P U 使用率、メモリ使用率、ディスク使用率等）を取得し、蓄積した統計情報を月次で機構に報告すること。
111	サーバソフトウェア（機器ソフトウェア）管理														
112		サポート期限管理													
113		製品サポート状況確認（機構ICT基盤（共通基盤システム等）保守事業者）		◎								○			利用しているソフトウェアのサポート期限超過の確認、対策検討し、計画の作成を支援する。
114		製品サポート状況確認（拠点ハードウェア事業者）					◎					○			利用しているソフトウェアのサポート期限超過の確認、対策検討し、計画の作成を支援する。
115		製品サポート状況確認（プリンタ事業者）						◎				○			利用しているソフトウェアのサポート期限超過の確認、対策検討し、計画の作成を支援する。
116		製品サポート状況確認（社会保険オンラインシステム保守事業者）							◎			○			利用しているソフトウェアのサポート期限超過の確認、対策検討し、計画の作成を支援する。
117		報告（機構ICT基盤（共通基盤システム等）保守事業者）	○	◎								○			導入しているハードウェアのファームウェアのバージョンアップ対応及び状況報告を支援する。
118		報告（拠点ハードウェア事業者）	○				◎					○			導入しているハードウェアのファームウェアのバージョンアップ対応及び状況報告を支援する。
119		報告（プリンタ事業者）	○					◎				○			導入しているハードウェアのファームウェアのバージョンアップ対応及び状況報告を支援する。
120		報告（社会保険オンラインシステム保守事業者）	○						◎			○			導入しているハードウェアのファームウェアのバージョンアップ対応及び状況報告を支援する。
121	システム監視・障害対応														
122		システム監視（監視端末/運用管理端末/フロー分析装置）													
123		システム監視										◎			監視端末及び運用管理端末、通信フロー分析装置等（本部NW）によるシステム監視を実施する。 また、ＴＶ会議システムの稼働監視の対応を実施する。
124		メッセージ対応										◎			出力メッセージ、アラートによる対応。（無視、メッセージ種別に応じた手順化済み作業の実施、無影響メッセージのフィルタなど）

【別紙2】 関連事業者との役割分担表

◎…主たる作業者
○…当該役務に関して作業担当と密に連携し、作業協力
※複数の業者に◎が付いている作業項目においては、各業者は担当する役務範囲の作業を主体的に実施することとする。
※環境毎の個別記載がない場合は原則本書、稼働維持どちらも役務に含む。

項番	作業項目	日本年金機構	等 保守事業者	機構ICT基盤（共通基盤システム	情報業務システム等運用・保守事業者	機構ICT基盤（拠点端末設備等）	プリンタ等保守事業者	社会保険オンラインシステム等保守事業者	統合ネットワーク事業者	現行運用管理事業者	運用管理事業者（本調達受託者）	次期運用管理事業者	外部システム事業者	作業内容
125	所管部署への連絡	○	○	○	○	○	○	○	○		◎		○	関係各所へのエラーメッセージの報告、共有。
126	障害イベントの照会・問い合わせの対応		○	○	○	○	○	○	○		◎		○	運用時の問い合わせやシステム障害時の解析で必要とする各種ログの取得、関連事業者、ベンダ照会などの対応。
127	障害イベントの解析、対策検討（機構ICT基盤（共通基盤システム等）保守事業者対応）		◎								○			運用時の問い合わせやシステム障害時の解析、対策検討を支援する。
128	障害イベントの解析、対策検討（情報業務事業者対応）			◎							○			運用時の問い合わせやシステム障害時の解析、対策検討を支援する。
129	障害イベントの解析、対策検討（拠点端末設備等事業者対応）				◎						○			運用時の問い合わせやシステム障害時の解析、対策検討を支援する。
130	障害イベントの解析、対策検討（プリンタ事業者対応）					◎					○			運用時の問い合わせやシステム障害時の解析、対策検討を支援する。
131	障害イベントの解析、対策検討（社会保険オンラインシステム保守事業者対応）							◎			○			運用時の問い合わせやシステム障害時の解析、対策検討を支援する。
132	障害イベントの解析、対策検討（統合ネットワーク事業者対応）								◎		○			運用時の問い合わせやシステム障害時の解析、対策検討を支援する。
133	障害イベントの解析、対策検討（外接システム業者対応）										○		◎	運用時の問い合わせやシステム障害時の解析、対策検討を支援する。
134	障害イベントの対策報告、手順作成（機構ICT基盤（共通基盤システム等）保守事業者対応）		◎								○			運用時の問い合わせやシステム障害時対策方法の報告、手順作成を支援する。
135	障害イベントの対策報告、手順作成（情報業務事業者対応）			◎							○			運用時の問い合わせやシステム障害時対策方法の報告、手順作成を支援する。
136	障害イベントの対策報告、手順作成（拠点端末設備等事業者対応）				◎						○			運用時の問い合わせやシステム障害時対策方法の報告、手順作成を支援する。
137	障害イベントの対策報告、手順作成（プリンタ事業者対応）					◎					○			運用時の問い合わせやシステム障害時対策方法の報告、手順作成を支援する。
138	障害イベントの対策報告、手順作成（社会保険オンラインシステム保守事業者対応）							◎			○			運用管理事業者が障害を1次切り分けた結果、社会保険オンラインシステム端末設備ソフトウェア等保守事業者宛となった問い合わせへの対応、運用管理事業者が稼働維持環境へ適用作業(PPあるいはAPL修正)を実施した後の端末APL環境の検証作業及び検証結果報告を支援する。
139	障害イベントの対策報告、手順作成（統合ネットワーク事業者対応）								◎		○			運用時の問い合わせやシステム障害時対策方法の報告、手順作成を支援する。
140	障害イベントの対策報告、手順作成（外接システム業者対応）										○		◎	運用時の問い合わせやシステム障害時対策方法の報告、手順作成を支援する。
141	障害イベントの稼働維持対応、検証（機構ICT基盤（共通基盤システム等）保守事業者対応）		◎								○			運用時の問い合わせやシステム障害対策の稼働維持検証、検証結果報告を支援する。
142	障害イベントの稼働維持対応、検証（情報業務事業者対応）			◎							○			運用時の問い合わせやシステム障害対策の稼働維持検証、検証結果報告を支援する。
143	障害イベントの稼働維持対応、検証（拠点端末設備等事業者対応）				◎						○			運用時の問い合わせやシステム障害対策の稼働維持検証、検証結果報告を支援する。
144	障害イベントの稼働維持対応、検証（プリンタ事業者対応）					◎					○			運用時の問い合わせやシステム障害対策の稼働維持検証、検証結果報告を支援する。
145	障害イベントの稼働維持対応、検証（社会保険オンラインシステム保守事業者対応）							◎			○			運用時の問い合わせやシステム障害対策の稼働維持検証、検証結果報告を支援する。
146	障害イベントの稼働維持対応、検証（統合ネットワーク事業者対応）								◎		○			運用時の問い合わせやシステム障害対策の稼働維持検証、検証結果報告を支援する。
147	障害イベントの稼働維持対応、検証（外接システム業者対応）										○		◎	運用時の問い合わせやシステム障害対策の稼働維持検証、検証結果報告を支援する。
148	本番対応調整	○	○	○	○	○	○	○	○		◎		○	障害対応に伴う本番対応実施、調整。
149	本番環境への適用	○	○	○	○	○	○	○	○		◎		○	障害対策を本番環境へ適用する。
150	インシデント管理	○	○	○	○	○	○	○	○		◎		○	インシデント管理ならびに問題管理として適切に管理し、障害発生状況について機構への報告。
151	セキュリティ対策													
152	端末設定後対応													
153	ウイルスフルスキャン										◎			機構ICT基盤設置等作業が終了した際に、作業端末のフルスキャンを実施。
154	セキュリティ項目チェック										◎			機構が指定したセキュリティチェックを日次で実施。
155	Radius認証設定管理										◎			Radius認証の設定、内容の管理、チェックの実施。
156	作業報告	○									◎			上記、状況・結果の報告。
157	統合NW遮断ログ確認													
158	統合NWの遮断ログ確認								○		◎			統合NWの遮断通信ログを月次でチェック。
159	情報資産管理台帳の更新													
160	情報資産管理台帳の棚卸、更新										◎			情報資産管理台帳の棚卸、及び更新作業を四半期ごとの実施。
161	報告（四半期）	○									◎			状況、対応の報告。
162	情報系/業務系ファイル一覧の作成													
163	「機3」ファイルの抽出	○									◎			各種ファイルサーバに保存されたファイルのうち、機構から指示があった「機3」が含まれるファイルの抽出、一覧化の上、機構への報告。（月次）
164	監査対応													
165	情報取得許可願の完了確認、及び個人情報の持出し対応の確認	○									◎			情報取得許可願の完了確認、及び個人情報の持出し確認を実施し、機構への報告。
166	NCO等監査対応	○									◎			NCO等監査に伴う調査対応、対策実施検討、対策の実施。
167	報告	○									◎			状況、対応の報告。
168	不審メールアドレスとの送受信メール確認													
169	外部メール送受信ログ確認			◎							○			外部とメール送受信しているログを調査し、過去に不審メールアドレスとされたアドレスとの送受信の有無の確認、機構への報告を支援する。
170	不審メールアドレスの送受信結果の報告	○		◎							○			状況、対応の報告を支援する。
171	業務環境管理													
172	運用依頼作業													
173	生体認証DB再編成要否確認	○									◎			生体認証DBの再編成が必要か確認を行う。
174	拠点追加・廃止・移設・統廃合時の対応	○				○					◎			拠点追加・廃止・移設・統廃合時の端末管理製品（SKYSEA等）の導入・削除等対応を行う。
175	拠点機器管理	○				○					◎		○	拠点毎の機構ICT基盤設置機器の管理。
176	受付管理簿投入	○									◎			機構本部職員より受領した依頼の受付、更新等管理簿の管理を行う。
177	人事異動など人事情報申請者及び承認者登録・削除	○									◎			機構本部職員より申請者及び承認者削除依頼の確認、管理情報の登録、更新などの管理。
178	人事異動対応	○									◎		○	機構本部からの依頼を受け、指定された利用者IDに対する申請情報（登録、削除、変更）の対応を実施する。
179	メールサービス対応（イントラメールボックス、アドレス、アーカイブ）	○									◎		○	職員指示に基づき、イントラメールボックスの復元、メールアドレス設定、アーカイブ検索実施。
180	申請情報配布先管理	○									◎			人事異動情報システム上の組織変更時の該当組織申請情報の拠点配布設定の対応、管理情報の管理。（統合ID認証、組織設定変更、基幹共有アクセス作業等の実施）
181	機構ICT基盤拠点の新設統廃合対応	○									◎			機構ICT基盤拠点の新設/移転/統合/廃止に伴う各種設定対応を行う。
182	TCサービス対応	○									◎		○	TCの運転日設定、プロセス監視設定作業の実施。

【別紙2】 関連事業者との役割分担表

◎…主たる作業者
○…当該役務に関して作業担当と密に連携し、作業協力
※複数の業者に◎が付いている作業項目においては、各業者は担当する役務範囲の作業を主体的に実施することとする。
※環境毎の個別記載がない場合は原則本番、稼働維持どちらも役務に含む。

項番	作業項目												作業内容											
	日本年金機構	保守事業者等（機構ICT基盤（共通基盤システム等）	情報業務システム等運用・保守事業者	機構ICT基盤（拠点端末設備等）	保守事業者	プリンタ等保守事業者	社会保険オンラインシステム等保守事業者	端末設備ソフトウェア等保守事業者	統合ネットワーク事業者	現行運用管理事業者	運用管理事業者（本調達受託者）	次期運用管理事業者	外部システム事業者											
183		他運営事業者連携	○								○			共通運営業者との情報共有・連携の実施。										
184		サーバメンテナンス	○								○		○	月次で人事情報連携サーバのDB不要データの削除を実施する。										
185		生体認証対応	○								○			生体認証データベースサービスの停止、再開対応、生体認証サービスの停止、起動対応。										
186		インデックス再構築	○								○			インデックス再構築等のDBメンテナンスの実施。										
187		定例外作業																						
188		イベント対応	○	○	○	○	○	○	○		○		○	サーバ等センタ設置機器への定例外などのイベント（組織再編作業、共通基盤外接対応など）作業対応を機構と協議の上、実施する。										
189		拠点装置運営																						
190		保守機管理	○			○					○			機構内の各拠点に設置された端末装置におけるメンテナンスや故障時の対応及び拠点工事対応を実施。										
191		予備機管理	○			○					○			機構内の各拠点に設置された端末装置におけるメンテナンスや故障時の対応及び拠点工事対応を実施。										
192		端末ソフトウェア管理																						
193		プログラム配布業務																						
194		配布対象の受付、日程調整		○	○	○		○	○		○			端末ソフトウェアの改修等(又は各種設定用資材の転送)に伴う配布依頼の受付、調整を行う。										
195		機構報告	○								○			配布伴うセンタ設置機器の構成管理、配布に係る機構本部職員への説明。										
196		配布		○	○	○		○	○		○			配布物・資材の配布の実施。										
197		報告	○								○			作業結果報告。										
198		故障対応																						
199		受付・状況確認	○								○			故障機器の受付、状況の問診、事象切り分けの対応。										
200		（現地オンサイト）駆けつけ調整	○	○		○	○				○			現地での部品交換又は修理調整、交換対応。										
201		（現地オンサイト）対応（機構ICT基盤（共通基盤システム等）保守事業者担当）	○	○							○			現地での部品交換又は修理調整、交換対応。										
202		（現地オンサイト）対応（機構ICT基盤（拠点端末設備等）保守事業者担当）	○			○					○			現地での部品交換又は修理調整、交換対応。										
203		（現地オンサイト）対応（プリンタ等保守事業者担当）	○				○				○			現地での部品交換又は修理調整、交換対応。										
204		（保守拠点オンサイト）駆けつけ調整	○			○					○			現地では保守機との交換を行い、保守拠点にて装置修理手配等を行う。										
205		（保守拠点オンサイト）対応	○			○					○			現地では保守機との交換を行い、保守拠点にて装置修理手配等を支援する。										
206		（現地センドバック）調整	○			○					○			機構ICT基盤ハードウェア事業者へ現地の機構職員宛で代替機の発送依頼、現地職員様での到着後の交換対応。										
207		（現地センドバック）対応	○			○					○			機構ICT基盤ハードウェア事業者へ現地の機構職員宛で代替機の発送依頼、現地職員様での到着後の交換対応を支援する。										
208		（保守拠点センドバック）調整	○			○					○			機構職員からの連絡を受け現地で本調達受託業者にて保守機との交換を行い、故障装置を保守拠点へ持ち帰る。機構ICT基盤ハードウェア事業者へ代替機の発送を依頼する。										
209		（保守拠点センドバック）対応	○			○					○			機構職員からの連絡を受け現地で本調達受託業者にて保守機との交換を行い、故障装置を保守拠点へ持ち帰る。機構ICT基盤ハードウェア事業者へ代替機の発送を支援する。										
210		報告	○								○			故障対応に伴う報告を行う。										
211		定例外作業（機構ICT基盤設置等作業）																						
212		イベント対応	○	○	○	○	○		○		○		○	増設・撤去・移設等に伴う工事イベント対応を支援する。										
213		システム保守																						
214		ハードウェア保守(本番/稼働維持/遠隔地)		○		○	○				○			ハードウェア製品故障の修理等の対応を支援する。										
215		パッチ情報/バージョンアップ情報提供						○			○			アプリケーション開発事業者が納品するソフトウェア製品に関するパッチ情報/バージョンアップ情報の提供を受ける。（パッチ情報/バージョンアップ情報・パッチ資材/バージョンアップ資材、標準適用手順）										
216							○					○		拠点端末設備等事業者が納品するソフトウェア製品に関するパッチ情報/バージョンアップ情報を提供を受ける。（パッチ情報/バージョンアップ情報・パッチ資材/バージョンアップ資材、標準適用手順）										
217				○								○		機構ICT基盤（共通基盤システム等）保守事業者が納品するソフトウェア製品に関するパッチ情報/バージョンアップ情報を提供を受ける。（パッチ情報/バージョンアップ情報・パッチ資材/バージョンアップ資材、標準適用手順）										
218		パッチ適用/バージョンアップに係る影響調査						○			○			アプリケーション開発事業者が設計・構築を担当するソフトウェア製品(ウイルス対策ソフトウェア含む)に関するパッチ情報/バージョンアップ情報を元に、システムへの影響調査を支援する。										
219							○					○		拠点端末設備等事業者が設計・構築を担当するソフトウェア製品(ウイルス対策ソフトウェア含む)に関するパッチ情報/バージョンアップ情報を元に、システムへの影響調査を支援する。										
220				○								○		機構ICT基盤（共通基盤システム等）保守事業者が設計・構築を担当するソフトウェア製品(ウイルス対策ソフトウェア含む)に関するパッチ情報/バージョンアップ情報を元に、システムへの影響調査を実施する。										
221		パッチ適用/バージョンアップに係る作業手順書作成		○		○		○			○			ソフトウェア製品に関するパッチ情報/バージョンアップ情報を基に、作業手順書を作成する。										
222		パッチ適用/バージョンアップの検証		○		○		○			○			ソフトウェア製品に関するパッチ適用/バージョンアップを実施しても問題ないか検証を支援する。（適用手順の確認・作業全体のリハーサル・適用後の動作確認の支援）										
223		パッチ適用/バージョンアップ作業		○		○		○			○			パッチ適用/バージョンアップ作業、及び動作確認について、実作業を実施する。										
224		ファームウェア情報提供		○							○			ファームウェア情報を提供を受ける。										
225		ファームウェア適用検証		○				○			○			ファームウェア更新を実施しても問題ないかの検証を支援する。										
226		ファームウェア適用作業		○				○			○			ファームウェアの更新を支援する。										
227		ウイルス定義ファイルの更新作業(共通基盤採用)		○		○		○			○			ウイルス定義ファイルの更新作業について、共通基盤の定義ファイルにより更新される。										
228		システムの定義変更等作業（ファイアウォール等）		○				○			○			システム構成の変更等作業、及び動作確認について、実作業は運用管理事業者が実施する。各事業者は必要な作業手順書を作成する。										
229		障害対応																						
230		ウイルス検知対応																						
231		ウイルス検知・感染受付	○							○			○	ウイルス対策機能によるウイルス検知、ウイルス感染の申告の受付。										
232		問診・影響特定	○		○				○		○			ウイルス検知した場合の利用者への連絡、感染状況の問診、状況からの影響特定を行う。										
233		各種状況報告	○	○	○	○	○	○	○		○			ウイルス感染状況の報告、関連事業者への連携を支援する。										
234		ウイルス確認、ベンダ照会									○			ウイルスの特性、ベンダへの問い合わせ。										
235		対応検討、対策	○								○			NW遮断、駆除及び削除等の措置の対応実施。										
236		対策報告	○								○			対策状況、結果の報告。										
237		不正アクセス検出																						
238		不正アクセス確認	○								○			不正アクセス検出の確認。										
239		一次報告	○								○			不正アクセス検出の報告。										
240		ログ取得、影響特定、調査	○						○		○			ログの取得・調査し、原因、影響範囲の特定を行う。										
241		対策、遮断	○						○		○			未知の不正アクセスパターンの対応方法を検討、侵入経路の遮断対応の実施。										

【別紙2】 関連事業者との役割分担表

◎…主たる作業者
○…当該役務に関して作業担当と密に連携し、作業協力
※複数の業者に◎が付いている作業項目においては、各業者は担当する役務範囲の作業を主体的に実施することとする。
※環境毎の個別記載がない場合は原則本書、稼働維持どちらも役務に含む。

項番	作業項目	日本年金機構	保守事業者等 （機構ICT基盤（共通基盤システム））	情報業務システム等運用・保守事業者	機構ICT基盤（拠点端末設備等） 保守事業者	プリンタ等保守事業者	社会保険オンラインシステム等保守事業者	統合ネットワーク事業者	現行運用管理事業者	運用管理事業者（本調達受託者）	次期運用管理事業者	外部システム事業者	作業内容
242	報告	○								○			状況、対応の報告。
243	セキュリティインシデント対応												
244	事象確認・情報収集	○					○	○		○			ベンダや事象状況の情報収集、確認。
245	影響確認、報告	○								○		○	不審通信に関する通報への対応や、機構外で拡大している攻撃等に対する影響の確認、防止対応。
246	対応検討	○					○	○		○			対策状況、結果の報告。
247	プロジェクト管理												
248	コミュニケーション管理												
249	コミュニケーション計画及び報告フォームの作成									○			コミュニケーション計画及び報告フォームを作成する。
250	運用管理業務及び保守事業者の状況把握		○	○	○	○	○	○		○		○	運用管理業務の実施状況の確認と運用対象システムの保守事業者が実施する作業の状況を把握する。
251	品質管理												
252	品質管理状況の把握									○			設備、資源、環境及び活動に関する品質の確認を実施する。
253	インシデント管理												
254	インシデントの状況管理									○			発生したインシデントに対して、早急なサービス復旧や事後検証等適切な対応を行うため、報告の手順や対応状況に関する記録の登録・維持管理を行う。
255	問題管理												
256	インシデントの再発防止									○			インシデントの発生に関する根本原因を究明し、その解決方法を作成して、インシデントの再発を防止する。
257	インシデントの未然防止									○			蓄積されたインシデント情報等を基に、インシデントの根本原因となり得る欠陥を除去することにより、潜在的なインシデントの発生を未然に防止すること。
258	変更管理												
259	変更管理の実施、報告									○			システムに対する変更要求を記録し、変更に対する対応状況の監視、報告を行う。
260	リリース管理												
261	リリース管理の実施									○			システムのリリース作業の実施計画の策定と管理を実施すること。
262	リスク管理												
263	リスク管理の実施									○			システムを安定的に稼働させる上で懸念されるリスクの抽出と状況監視を行い、監視結果を進捗会議において報告する。
264	情報セキュリティ管理												
265	手順書の作成									○			情報セキュリティ対応手順、セキュリティ事故対策手順等を作成する。
266	情報セキュリティ管理の実施									○			ウイルス定義ファイルやセキュリティパッチの公開情報の管理、及び本システムへの適用状況の管理、セキュリティ事故の発生状況の管理を行う。
267	構成管理・ドキュメント管理												
268	構成管理・ドキュメント管理の実施									○			プログラム/テーブル、及びドキュメントの資材管理(原本管理、変更履歴管理)を実施する。
269	要員管理												
270	要員管理の実施									○			予定されているイベントや運用管理業務に応じ必要な要員を確保し、要員の配置及びシフト計画を作成、報告する。
271	要員研修									○			要員に対する初期研修、個人情報
272	稼働状況管理												
273	稼働状況管理の実施									○			運用管理業務において、日々のインシデント、障害内容に関する各関係者間での情報共有や当日の作業内容等の確認、作業の進捗状況の確認を行う。
274	月次報告	○								○			月次での報告を行う。管理項目については、「閲覧資料 ITサービス業務標準」を参照し、定めること。(可用性管理、予算管理、キャパシティ管理、文書・データ保管管理、品質管理、インシデント管理、問題管理、リリース管理、セキュリティ施策実施(脆弱性対策、使用製品のサポート期限切れ等)
275	作業内容、進捗状況、課題、リスク、インシデント等を含めた稼働実績の報告（月次）									○			各業者が担当する役務範囲の作業において、ハードウェア保守について、月次における作業実績を主体的に報告する。
276	SLA管理												
277	サービスレベルの活動計画作成									○			サービスレベルの活動計画を作成する。
278	サービスレベルの遵守及び管理									○			サービスレベルの管理状況をサービス実績報告書、改善状況報告書として報告するとともに、評価に基づくサービスレベルの改善、向上のための施策を実行すること。
279	運用管理業務												
280	撤去及び原状回復												
281	撤去及びデータ消去計画の作成	○								○			保守契約満了時又は故障時にデータ消去、ハードウェア撤去の計画を作成する。
282	撤去及びデータ消去の実施	○								○			保守契約満了時又は故障時にデータを消去しハードウェアを撤去する。
283	原状回復									○			ラックの設置に際して公示した箇所について、原状回復を実施する。
284	引継ぎ												
285	引継ぎ計画												
286	引継ぎ計画書の作成	○								○			引継ぎ作業を滞りなく実施するための引継ぎ計画書を作成する。（実施計画、訓練計画等）
287	引継ぎ												
288	引継ぎ実施									○	○		引継ぎ計画書に従い、次期運用管理事業者に引継ぎを行う。（ナレッジデータ等）
289	引継ぎ完了報告												
290	引継ぎ完了報告書の作成	○								○	○		引継ぎ完了報告書、引継ぎ課題一覧を作成する。
291	契約完了												
292	最終報告	○								○			最終報告書を作成、提出する。

資料閲覧申請書 兼 秘密保持誓約書

令和 年 月 日

日本年金機構 理事長代理人
システム運用部長 及川 無双 様

住 所
商 号 又 は 名 称
代 表 者 名 印

調達件名「機構ICT基盤運用管理サービス等業務」に関し、以下のとおり資料を閲覧させて頂きたく申請書を提出致します。
また、閲覧にて知り得た情報は、本件以外の目的に使用すること並びに第三者に開示及び漏洩をしないことを誓約します。

■閲覧者

項番	氏 名	ふりがな	TEL
1			
2			
3			
4			
5			

なお、資料閲覧の実施にあたり、下記のとおり誓約します。

記

1. 閲覧において知り得た各種情報について、当該入札の目的以外での使用は致しません。
2. 閲覧において知り得た各種情報について、第三者に漏洩等いたしません。
3. 本件に関して日本年金機構または第三者に損害を与えた場合は、直ちに対策を講じ、これに対応を実施します。なお、当該対応に要する全ての費用について負担します。

令和 年 月 日

日本年金機構 理事長代理人
システム運用部長 及川 無双 殿

所 在 地
法人名又は商号
代 表 者 名 印

守秘義務に関する誓約書

弊社は日本年金機構の下記の委託業務（以下「本業務」という。）に従事するにあたり、下記の秘密保持に関する事項を遵守することを誓約いたします。

また、本業務の全従事者について、下記の事項内容を周知しており、内容を理解し、遵守することを証明いたします。

対象業務：機構 ICT 基盤運用管理サービス等業務
履行期間：令和 10 年 1 月 6 日～令和 13 年 4 月 30 日

記

1. 本業務に従事中、本業務を通じて知り得た一切の情報（以下「秘密情報」という。）について、第三者に開示、漏えい、目的外利用、又は自ら不正に使用しないこと。
※第三者：役員等を含む情報取扱者以外の者並びに親会社・地域統括会社等を含む受託事業者以外の者（機構が承認した場合を除く）
2. 本業務が終了した後においても、前項の秘密情報を第三者に開示、漏えいし、又は自ら不正に使用しないこと。
3. 上記各誓約事項に違反して日本年金機構に損害を与えたときは、その損害を賠償する責任を負うこと。
4. 本業務の実施にあたり、日本年金機構法（平成 19 年法律第 109 号）、個人情報の保護に関する法律（平成 15 年法律第 57 号）及び個人情報関係諸法令を遵守すること。

以上

（参考）日本年金機構法（平成 19 年法律第 109 号）より抜粋

- ・守秘義務（第 31 条第 2 項）：受託者等（委託を受けた者（その者が法人である場合にあっては、その役員）若しくはその職員その他の当該委託を受けた業務に従事する者）は当該業務に関して知り得た秘密を漏らすてはならない。
- ・罰則規定（第 31 条第 3 項）：受託者等にも、機構役職員に対する刑法その他の罰則の適用を準用する。
- ・罰則（第 57 条）：秘密を漏らした者は、1 年以下の拘禁刑又は 100 万円以下の罰金

令和 年 月 日

日本年金機構 理事長代理人
システム運用部長 及川 無双 殿

所 在 地
法人名又は商号
代 表 者 名

印

個人情報等の返却・廃棄等に関する報告書

機構 ICT 基盤運用管理サービス等業務が終了しましたので、当該委託業務における個人情報等の返却、廃棄等に関する実施結果について報告します。なお、各項目の証跡は別添のとおりです。

① 返却について

(※いずれかの□に✓してください。)

- ☐ 当該委託業務において、日本年金機構より貸与された個人情報等が記録された紙媒体、外部電磁的記録媒体は全て返却いたしました。

(個人情報等が記録された紙媒体、外部電磁的記録媒体を保管していた場所(保管庫等)の状況が分かるもの(例:返却後の写真等)を添付してください。)

- ☐ 当該業務委託において、日本年金機構より個人情報等が記録された紙媒体、外部電磁的記録媒体は貸与されていません。

② 消去・廃棄、又は移送について

(※いずれかの□に✓してください。)

- ☐ 当該委託業務において、個人情報等を作成・受け取り・複写複製(電子計算組織に格納した情報等含む。)したもの、その他汚損、毀損した個人情報等については、その全てを復元又は判読等が不可能な方法により完全消去、廃棄等の作業を実施しました。

どのように完全消去・廃棄等を実施したか、電子データ、紙媒体それぞれ具体的に記載してください。

(消去の場合においては、復元又は判読等が不可能となる方法(例:データ消去ソフト名、データ消去方式等。 ※自社開発プログラムの場合は、具体的なデータ消去方法等も明記のこと。)を必ず記載してください。また、消去した際のログが分かるものを添付してください。)

- ☐ 当該委託業務において、個人情報等を作成・受け取り・複写複製したもの、その他汚損、毀損した個人情報等については、その全てを移送しました。

令和 年 月 日

日本年金機構 理事長代理人
システム運用部長 及川 無双 殿

所 在 地
法人名又は商号
代 表 者 名

印

法令及び契約内容の遵守状況に関する報告書

機構 ICT 基盤運用管理サービス等業務の実施にあたり、法令及び契約内容の遵守状況の点検結果について報告します。

1. 当該委託業務の実施にあたり、契約書のほか、契約書に付属する仕様書及び委託する業務の実施方法等について記載された文書（以下「仕様書等」という。）に従い関係諸法令を守り、自ら業務処理計画を立案し、当該業務に従事する者（以下「業務委託員」という。）を適正に配置していますか。

点検結果： ☐ 適 ☐ 不適（※該当する ☐ に ☒ してください。以下同じ。）

2. 当該委託業務の実施にあたり、業務委託員への指導監督と教育指導を行い、業務趣旨に従い誠実かつ善良なる管理者の注意をもって、処理を行っていますか。

点検結果： ☐ 適 ☐ 不適

3. 当該委託業務の実施にあたり、業務委託員に対する雇用者又は使用者として、労働関係法令、社会保険諸法令その他業務委託員に対する法令上の責任を全て負い、責任を持って管理していますか。

点検結果： ☐ 適 ☐ 不適

4. 当該委託業務の実施にあたり、仕様書等において日本年金機構より使用を認められている機器等（機器等の消耗品を含む。以下同じ。）の管理・取扱いは適切に行われていますか。また、使用が認められていない機器等の取扱いを行っている事実はありませんか。

点検結果： ☐ 適 ☐ 不適

5. 当該委託業務の実施にあたり、業務委託員に対し、日本年金機構法、個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律が適用する旨の教育研修を実施しましたか。

点検結果： ☐ 適 ☐ 不適

日本年金機構 理事長代理人
システム運用部長 及川 無双 殿

所 在 地
法人名又は商号
代 表 者 名

⑨

再委託等に係る承認申請書

標記について、下記のとおり申請します。

なお、第三者に請け負わせる業務を含む一切の業務責任は弊社にあること、また再委託先等に対しては、本契約にて弊社に課せられている守秘義務等と同等以上の条件（本契約終了後の秘密保持を含む。）を遵守させるほか、日本年金機構が必要に応じ再委託先等に対して調査等を実施する場合には、これに応じさせることを誓約いたします。

記

1. 対象案件名：機構ICT基盤運用管理サービス等業務

2. 委託する相手方の商号又は名称及び住所：

1) 商号又は名称：△△株式会社 ○○オフィス ※担当部署を明示する。

2) 住所：

×××××× ×××××× ××××××

3. 委託する期間及び相手方の業務の範囲：

再委託等の委託期間：令和○年○月○日～令和○年○月○日

「○○（対象案件名）」一式「契約書」（以下「本契約」という。）のうち、○○○に関する○○○の一部について、弊社が実施する○○○に係る実作業を委託するもの（総合的な企画及び判断並びに業務遂行管理部分を除く）。

※ 受託者や他の再委託先等との作業の境界を具体的に明示する。

（対応工程）

××××××

4. 委託を行う合理的理由：

○○○に関する○○○機能が○○○（作業量が膨大等）であることから、作業の一部を委託するものであり、上記の再委託等は、○○○（弊社との協業プロジェクトにおけるアプリケーションの開発実績を多数有している 等）である。

また、○○○（同様のアプリケーションに携わった経験等）があることから、本件の履行を効率的かつ安全に実施することが見込めるため、当該業務を委託するものである。なお、委託した業務に伴う再委託先等の行為（本業務に関する更なる再々委託以降の行為を含む。）について、弊社は日本年金機構に対して全ての責任を負う。

5. 委託する相手方が、委託される業務を履行する能力：

【別紙 7】

当該再委託先等は、〇〇〇（弊社との協業プロジェクトにおけるアプリケーションの開発実績を多数有しており、また、同様のアプリケーション（〇〇〇）に精通している等）であることから、品質の高い業務遂行が期待できる。

なお、当該再委託先等は、過去３年において、公的年金におけるシステム開発の受託業務で機密情報の漏えいや紛失は生じておらず、成果物やプロジェクト管理等においても特段の問題は生じていないことを弊社で確認している。

6. 契約金額：000,000,000円（税込）

7. その他必要と認められる事項：

（１）委託業務の実施場所：

×××××× ×××××× ××××××

（２）委託先の役員の状況：

役職	氏名	就任年月日	任期	国籍

（３）委託先の資本金の出資者別比率

受託者 00%（国籍）

委託先役員（代表取締役等） 00%（国籍）

上記以外（〇〇株式会社） 00%（国籍）

※個人出資や法人として自社株式を保有している等、例外的な場合の記載については、個別に協議（外国からの出資状況の確認が必須）。

（４）委託先の責任者

	氏名	所属部署	役職	専門性 （経験・資格等）	実績	国籍
統括管理補助者						
情報セキュリティ 管理補助者						
〇〇チームリーダー						

※再委託先等の従事者が受託者と同じ開発環境で開発作業をしている等により、受託者のセキュリティ責任者が再委託先等の責任者等を兼ねる場合は、その旨を提示する。

（５）委託先が請け負う業務の関係者である従業員の国籍の状況

（国籍： ） 人／総数 人

（国籍： ） 人／総数 人

※国籍が不明・非開示等の場合は、国籍欄にその旨を記載する。

（６）ガバナンスの確立

1) 弊社と当該再委託先等は、〇〇〇〇〇（系列会社であるため、同一の品質管理手順が適合されている等）により、一貫したシステム開発体制が確保できるほか、上記（１）の委託業務の実施場所には、弊社の統括責任者を補助する統括管理補助者を設置し、ガバナンスの確立に努める。

実施体制図については、別添のとおり。

【別紙 7】

2) 本契約により新たに作成される成果物の著作権等の取扱い（知的財産権の帰属、著作者人格権の不行使）や必要に応じて発注者が再委託先等に対して調査等を行えることを、当該再委託先等に請け負わせる上記 3 の業務の契約書に明示する。

(7) 情報セキュリティの確保

1) 当該再委託先等には、弊社と同様に、日本年金機構情報セキュリティポリシー等に従って、情報セキュリティ管理計画書のとおり、最新の情報セキュリティ対策を踏まえた取組を実施させる。

2) 上記（1）の委託業務の実施場所には、弊社の情報セキュリティ管理者を補助する情報セキュリティ管理補助者を設置し、上記 3 の業務に関して意図せざる変更が加えられないための管理体制の確保等、情報セキュリティの確保に努める。なお、日本年金機構から提供する情報は、契約した業務に従事する者のみが、担当する業務に必要な情報に限定して利用可能とする。

3) 当該再委託先等が請け負う業務の関係者である従業員からは、上記 3 の業務に求められる情報セキュリティを理解していることを確認済である。

(8) 再々委託先等の情報：

別紙のとおり（上記と同様の情報を添付する）。

(9) その他

受託者は、本件に関して、労働基準法（昭和 22 年法律第 49 号）、労働者災害補償保険法（昭和 22 年法律第 50 号）、職業安定法（昭和 22 年法律第 141 号）、労働安全衛生法（昭和 47 年法律第 57 号）、製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律（昭和 31 年法律第 120 号）、社会保険諸法令その他業務委託員に対する法令を遵守しており、その責任を全て負う。

令和 年 月 日

日本年金機構本部 理事長代理人
システム運用部長 及川 無双 殿

所 在 地
法人名又は商号
代 表 者 名

⑨

受 託 証 明 書

下記の対象案件の業務のうち、 （委託される業務） 業務については、 （機構との契約受託者） から要請がありましたので、必要な業務について、 （受託証明書の提出者との契約相手方） との契約に基づき、責任をもって行うことを証明致します。

また、本契約の履行において知り得た秘密を、他に漏らしたり又は目的外に使用しないこと（本契約終了後においても同様）、及び日本年金機構が必要に応じ弊社に対して調査等を実施する場合はこれに応じることを誓約いたします。

記

（対象案件名） 機構ICT基盤運用管理サービス等業務

（受託内容等） _____

（履行場所住所及び名称）

現地調査申込書 兼 守秘義務誓約書

令和 年 月 日

日本年金機構 理事長代理人
システム運用部長 及川 無双 様

住 所
商 号 又 は 名 称
代 表 者 名 ⑩

「機構ICT基盤運用管理サービス等業務」に係る現地調査につきまして、以下の者の参加を申し込みます。

参加者氏名 1	印
参加者氏名 2	印
参加者氏名 3	印
参加者氏名 4	印
参加者氏名 5	印

なお、現地調査の実施にあたり、下記のとおり誓約します。

記

- 1. 当該現地調査において知り得た各種情報について、当該入札の目的以外での使用は致しません。
- 2. 当該現地調査において知り得た各種情報について、第三者に漏洩等いたしません。
- 3. 当該現地調査が、日本年金機構側のシステムや施設・設備に不具合等の影響を与えた場合には、直ちに対策を講じ、これの対応を実施します。
なお、当該対応に要するすべての費用について負担します。

クリーニング作業完了報告書

本番環境及び検証環境にて、下記のとおりクリーニング作業が完了いたしました旨、ご報告いたします。

記

作業開始日	年	月	日	作業終了日	年	月	日
-------	---	---	---	-------	---	---	---

案件名	機構 ICT 基盤運用管理サービス等業務
-----	----------------------

作業責任者	受託者名 : 責任者氏名 : 連絡先等 :
作業対象、方法	別紙 10-1 参照
証跡	(別紙を受託者で用意)

作業対象	作業方法	作業結果
ユーザ認証情報が含まれた不要な平文のファイル（パスワード一覧等）は削除したか。		
パスワードの使い回し、共通のパスワードを設定していないか。		
パスワードがユーザ名と同じとなっていないか。		
OS ユーザや管理コンソールなどのユーザアカウントに推測可能なパスワードが設定されていないか。		
ソフトウェアが使用するシステムユーザのパスワードがデフォルトのままとなっていないか。		
パスワード変更をしたか又はパスワード変更の計画が立っているか。		
（その他 ある場合追記すること）		

業務内容詳細（拠点装置運用管理）

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想定 回数等 (随時の場合)	作業項目	作業内容
1	4.5.1 (1)保守機管理	定常	月次		【装置情報管理業務(保守機)】 棚卸実施指示文書作成および展開	関連事業者からの修理返却等の在庫管理および日本年金機構より問い合わせがあった際に常に保守機の状態を提示可能とするため、棚卸を保守拠点及び機構本部Aへ指示する。 ・指示文書作成 ・棚卸シートの作成
2	4.5.1 (1)保守機管理	定常	月次		【装置情報管理業務(保守機)】 棚卸の実施(機構本部A)	機構本部Aに配備されている端末台数を調査する。 ・保守機配備台数の確認、チェックシートのチェック ・貸出機ステータスの確認 ・報告 ※棚卸についてはSKYSEAより出力した棚卸用データを元に変分管理を行う。
3	4.5.1 (1)保守機管理	定常	月次		【装置情報管理業務(保守機)】 棚卸の実施（保守拠点）	保守拠点に配備されている端末台数、ステータスを調査し、調査結果を報告する。 ・保守機配備台数確認、チェックシートのチェック ・貸出機ステータスの確認 ・報告 ※棚卸についてはSKYSEAより出力した棚卸用データを元に変分管理を行う。
4	4.5.1 (1)保守機管理	定常	月次		【装置情報管理業務(保守機)】 棚卸結果の確認	保守拠点から受領した棚卸結果について、SKYSEAへの取り込みに向けた精査を行う。 ・報告物の確認、取りまとめ ・保守機台数適正チェック ・保守機一覧メンテナンス ・ワークファイルの作成（ツール化） ・クロスチェック
5	4.5.1 (1)保守機管理	定常	月次		【装置情報管理業務(保守機)】 装置情報DBへの登録	精査した情報をSKYSEAへ取り込む。 ・ワークファイルの取り込み
6	4.5.1 (1)保守機管理	定常	月次		【保守機の整備】 保守用マスタ原本の格納	外付けSSDより保守用マスタ原本を環境構築用PCへ格納する。 各保守拠点にて受領したマスタを使用し保守機の環境構築（1拠点1台）を実施し問題ないことを確認する。
7	4.5.1 (1)保守機管理	定常	半期		【保守機の整備】 保守機状態確認(機構本部A)	保守におけるサービスレベルを遵守するため、機構所有物である保守機について、検証、保管、維持管理を実施。 ・整備券記載の装置名、機器名の名称が正しいか確認 ・付属品が無いかの確認 ・外観確認(歪み、がたつき、破損、トレーの正常性確認) ・起動確認(正常起動の確認) ・ランプ状態確認 ・異音確認 ・整備券(1枚/台)への上記結果の記入
8	4.5.1 (1)保守機管理	定常	半期		【保守機の整備】 保守機状態確認（保守拠点）	保守におけるサービスレベルを遵守するため、機構所有物である保守機について、検証、保管、維持管理を実施。 ・整備券記載の装置名、機器名の名称が正しいか確認 ・数量が正しいかの確認 ・付属品が無いかの確認 ・外観確認(歪み、がたつき、破損、トレーの正常性確認) ・起動確認(正常起動の確認) ・ランプ状態確認 ・異音確認 ・整備券(1枚/台)への上記結果の記入

業務内容詳細（拠点装置運用管理）

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想定 回数等 (随時の場合)	作業項目	作業内容
9	4.5.1 (1)保守機管理	定常	月次		【装置情報管理業務(保守機Ⅱ)】 棚卸の実施（保守拠点）	倉庫に保管されている機器台数、シリアル、倉庫の状況を調査し、調査結果を報告する。 ・保守機Ⅱの棚卸(装置単位の台数チェック) ・報告様式への入力 ・棚卸結果と保守機Ⅱ管理システム登録情報の突合 ・証跡の取得(写真撮影) ・報告(社内ファイルサーバ)
10	4.5.1 (1)保守機管理	定常	月次		【装置情報管理業務(保守機Ⅱ)】 棚卸の実施（機構本部A）	機構本部Aに保管されている機器台数、シリアル、倉庫の状況を調査し、調査結果を報告する。 ・保守機Ⅱの棚卸(装置単位の台数チェック) ・報告様式への入力 ・棚卸結果と保守機Ⅱ管理システム登録情報の突合 ・証跡の取得(写真撮影) ・報告(社内ファイルサーバ)
11	4.5.1 (1)保守機管理	定常	月次		【装置情報管理業務(保守機Ⅱ)】 棚卸結果および出入庫管理簿の突合	倉庫から受領した棚卸結果について、SKYSEAへの取り込みに向けた精査を行う。 ・報告物の取得 ・棚卸結果と装置情報DBの突合 ・ワークファイルの作成（ツール化）
12	4.5.1 (1)保守機管理	定常	月次		【装置情報管理業務(保守機Ⅱ)】 装置情報DBへの登録	精査した情報をSKYSEAへ取り込む。 ・ワークファイルの取り込み
13	4.5.1 (3)故障時対応	随時		0.98回/月 657件/回	【装置情報管理業務(本番機)】 本番機台数精査(保守)	端末設備の増設／移設／撤去や故障対応等で必要となる、事務所ごとの設置台数、端末シリアル、機番等の装置情報を管理するため、保守で変更となった装置情報を精査する。 ・対象工事の抽出 ・管理簿の登録 ・機番報告シートの収集 ・ワークファイルの作成（ツール化） ・クロスチェック
14	4.5.1 (3)故障時対応	随時		0.98回/年	故障復旧作業（保守拠点）	故障発生時における現地保守対応 ・保守拠点作業 ・故障受付 ・故障受付表作成 ・移動(往復)/入所連絡 ・故障対応/ハードウェア事業者作業立会い ・機構への完了報告 ・退所連絡 ・故障受付表の内容サーバ登録 ・故障機整備券の発行
15	4.5.1 (3)故障時対応	随時		0.98回/年	故障復旧作業（機構本部A）	故障対応に伴う、該当年金事務所等拠点に対する保守機の発送、故障機を受領、故障機のメーカー修理の調整、修理完了後の装置保管を機構本部Aにて実施する。
16	4.5.1 (3)故障時対応 4.5.1 (4)端末設備設置等作	随時		8人相当/月	工事統制	工事当日の統制対応（現地からの問い合わせ、進捗状況、作業結果確認等）を行う。

業務内容詳細（拠点装置運用管理）

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想定 回数等 (随時の場合)	作業項目	作業内容
17	4.5.1 (3)故障時対応 4.5.1 (4)端末設備設置等作業	随時		21.2件/月	ローカル管理者パスワード一括設定依頼	・現地で使用する各端末のローカルパスワードを設定するため、センタ運営チームへ工事拠点情報の提供およびローカルパスワード設定作業の申請を行う。 - 申請情報は以下のとおり。 ・ 拠点名 ・ コンピュータ名 ・ 対象期間 ・ 作業者（所属含む） ・ 承認者 ・ 発生契機（工事申請、トラブル・・・など）
18	4.5.1 (4)端末設備設置等作業	随時		0.98回/月 417件/回	【装置情報管理業務(本番機)】 本番機台数精査(工事)	端末設備の増設／移設／撤去や故障対応等で必要となる、事務所ごとの設置台数、端末シリアル、機番等の装置情報を管理するため、工事に変更となった装置情報を精査する。 ・ 対象工事の抽出 ・ 管理簿(AccessDB)の登録 ・ 機番報告シートの収集 ・ ワークファイルの作成（ツール化） ・ クロスチェック
19	4.5.1 (4)端末設備設置等作業	随時		417件/月	工事オーダー処理	・ 工事申請書（見積依頼書・発注書）を受領し、工事オーダー一覧（工事申請書として受け付けた申請の処理状況をまとめた一覧）、進捗管理表（依頼を受けた工事に関する進捗状況を管理するための資料）に登録を行う。 ・ 登録した工事申請書は保守拠点へメール送信する。 ・ 保守拠点は年金事務所等現地と工事調整を行い、調整結果を報告書にまとめ、工事調整に送付する。 ・ オーダの棚卸し。 ・ 機構本部より一括で発出されるイベント工事等、工事内容の詳細を簡潔に取りまとめて、報告書の作成方法等を保守拠点へ展開する。
20	4.5.1 (4)端末設備設置等作業	随時		9,200分/月	随時作業	工事実施前に必要となる、他SG、関連事業者との調整作業等を行う。 ・ 統合NW業者調整 ・ 工事申請書作成依頼に対する対応 ・ イベント工事調整状況の個別管理・報告 ・ 物品調達に伴う対応 ・ 機構本部内部調整資料作成 ・ 機構本部-他省庁間調整 等
21	4.5.1 (4)端末設備設置等作業	随時		355件/月	機構（機構本部）調整／対応	工事内容に関わる不明点について、機構本部と調整を行い、工事内容を決定する。
22	4.5.1 (4)端末設備設置等作業	随時		355件/月	工事実施拠点保守員調整	・ 工事内容に関わる工事実施拠点からの不明点についての調整・対応を行い工事内容を決定する。 ・ 工事実施拠点にて作成した朱書き図面から工事申請書の工事依頼内容と一致していることを確認する。
23	4.5.1 (4)端末設備設置等作業	随時		1,560件/月	AD登録	・ 増設等で新規追加となる端末について、装置名の重複がないか確認を行い、ADサーバへの登録申請書を作成し、センタ運営チームへ申請を行う。 ・ 撤去等で削除となる端末の装置名を確認後、ADサーバへの削除申請書を作成し、センタ運営チームへ申請を行う。
24	4.5.1 (4)端末設備設置等作業	随時		116.8件/月	個別ソフトウェアアンインストール依頼	・ 拠点間移設で発生する個別ソフトウェアのアンインストールについてヘルプデスクへの機構時間調整を依頼する。 ・ 拠点間移設で発生する個別ソフトウェアのアンインストールについて端末設備運用管理センタへ設定したパスワードを展開する。

業務内容詳細（拠点装置運用管理）

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想定 回数等 (随時の場合)	作業項目	作業内容
25	4.5.1 (4)端末設備設置等作業	随時		1,091件/月	設定値払い出し	・ 増設、移設工事で必要となる設定値の払い出し、HOSTSファイルの修正を行う。 ・ 増設、移設工事の対象装置に、装置個別に資材が登録されている装置かを確認し、装置個別情報のメンテナンスを行う。 ・ 必要に応じてNW設計部隊等、関連担当との調整を行う。調整内容は要件共有および作業連携、スケジュール調整、資材作成依頼等の調整を行う。
26	4.5.1 (4)端末設備設置等作業	随時		416件/月	装置出荷対応	進捗管理表より出荷対象装置を抽出し、出荷依頼書を作成する。作成後、キッティングセンタに出荷指示を行う。
27	4.5.1 (4)端末設備設置等作業	随時		1件/月	統合NW申請	新規拠点の設置等で、統合NW事業者に申請が必要な場合、申請書を作成し、統合NW事業者へ設定変更等の依頼を行う。
28	4.5.1 (4)端末設備設置等作業	随時		475件/月	工程管理表作成	工事調整SGが現地工事の実施状況を把握するため、工事前日に工程管理表を作成し、現地保守員に送付する。
29	4.5.1 (4)端末設備設置等作業	随時		1,165件/月	工事開始前レビュー	工事実施日前に工事で必要となる事前準備が行えているか、最終確認を行う。
30	4.5.1 (4)端末設備設置等作業	随時		3,630件/月	工事オーダー作業	・ 月毎に工事完了した工事オーダーの内容をFIXし、請求対象となる工事のインプット情報を決定する。 ・ 工事完了となる、工事オーダーの納品物（工事実施報告書、図面）を確認し、納品対物を格納する。
31	4.5.1 (4)端末設備設置等作業	随時		4件/月	工事状況報告	関連事業者向けに工事状況について、各報告書を作成し送付する。
32	4.5.1 (4)端末設備設置等作業	定常	月次		【工事購買・契約作業（月次）】 工事通知書（概算）の発行	新規開発イベント等で、運用手順、報告書の変更があった場合、必要な管理ドキュメントのメンテナンスを行う。
33	4.5.1 (4)端末設備設置等作業	定常	月次		【工事購買・契約作業（月次）】 通知書ファイルの作成	工事オーダー一覧から作成対象の工事オーダーを抽出し、通知書ファイルを作成する。
34	4.5.1 (4)端末設備設置等作業	定常	月次		【工事購買・契約作業（月次）】 通知書ファイルの編集	作成された通知書ファイルを元に、機器あたりの工事単価を見直す*単価数量の算定など、通知書ファイルを編集する。
35	4.5.1 (4)端末設備設置等作業	定常	月次		【工事購買・契約作業（月次）】 通知書レビューの実施	通知書に対して、レビュー及び修正を行う。
36	4.5.1 (4)端末設備設置等作業	定常	月次		【工事購買・契約作業（月次）】 当月工事対象の集計	作成された通知書から、当月請求対象情報の抽出を実施する。
37	4.5.1 (4)端末設備設置等作業	定常	月次		【工事購買・契約作業（月次）】 工事実績取りまとめ作業（統合ファイル等）	機構への工事実績報告求にあたって必要な情報を通知書をもとに作成する。
38	4.5.1 (4)端末設備設置等作業	定常	月次		【工事購買・契約作業（月次）】 月次処理作業改善（実行）	振り返り結果を元にして作業手順の見直しや手順書の改善などを実施する。
39	4.5.1 (4)端末設備設置等作業	定常	週次		【工事購買・契約作業（週次）】 週次作業の実施	週次で工事オーダーに記載されている工事について、進捗状況を機構（端末運用G）に報告する
40	4.5.1 (4)端末設備設置等作業	定常	週次		【工事購買・契約作業（週次）】 週次納品作業の実施	週次で納品物（実施報告書、図面）を納品単位に整理し、納品作業を実施する。 (対象週に工事があった場合の作業)
41	4.5.1 (4)端末設備設置等作業	定常	日次		【工事購買・契約作業（日次）】 引き継ぎ事項共有	始業時に当日の作業予定や前日からの引き継ぎ事項について共有を行う。
42	4.5.1 (4)端末設備設置等作業	随時		1回/月	【実施報告書の作成】 実施報告書の作成	機構に納品する実施報告書を取りまとめる。
43	4.5.1 (2) 端末ソフトウェア管理	定常	月次		【保守機の整備】 保守用マスタ原本の再構築	保守用マスタ原本に対しフ転※、ウィルス定義ファイル、セキュリティパッチを適用しマスタの再構築を実施する。 ※：社会保険オンラインシステムのファイル転送差分資材

業務内容詳細（拠点装置運用管理）

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想定 回数等 (随時の場合)	作業項目	作業内容
44	4.5.1 (2) 端末ソフトウェア管理	定常	月次		【保守機の整備】 保守用マスタ原本の展開周知	フ転(※)、ウィルス定義ファイル、セキュリティパッチの展開周知とマスタ再構築を実施するよう保守拠点へ指示する。 ・指示文書作成 ・全国展開 ※：社会保険オンラインシステムのファイル転送差分資料
45	4.5.1(5) 予防保全（定期点検）	定常	年次		【定期点検計画】 定期点検スケジュール作成	定期点検を実施するためのスケジュールを作成する。 ・前年度計画からの見直しおよびスケジュール案の作成 前年度計画の見直しを実施し、事務所ごとの点検スケジュールを作成する。
46	4.5.1(5) 予防保全（定期点検）	定常	年次		【定期点検計画】 関連事業者スケジュール調整	定期点検を実施するため、関連事業者の調整を行う。 ・実施計画のメーカ調整 ・スケジュール調整
47	4.5.1(5) 予防保全（定期点検）	定常	年次		【定期点検計画】 定期点検日程調整指示文書作成	定期点検を実施するよう保守拠点へ指示する。 ・指示文書作成 ・全国展開
48	4.5.1(5) 予防保全（定期点検）	定常	年次		【定期点検計画】 定期点検日程調整	定期点検実施日を年金事務所等拠点の機構と調整する。 ・日程調整 ・報告様式への結果投入 ・報告
49	4.5.1(5) 予防保全（定期点検）	定常	年次		【定期点検計画】 日程調整結果のとりまとめ	機構調整日程調整結果を取りまとめる。 ・報告結果の収集 ・取りまとめ
50	4.5.1(5) 予防保全（定期点検）	定常	年次		【定期点検計画】 再日程調整の実施	メーカ希望日と機構希望日が不一致だった場合に再日程調整を実施する。 ・機構日程調整後の再日程調整
51	4.5.1(5) 予防保全（定期点検）	定常	年次		【定期点検計画】 事務所図面の収集・提供	定期点検対象装置は損益工事により台数に変動が生じるため、SKYSEA、事務所図面から対象の装置台数を確定させる。 ・事務所図面の収集 ・図面のPDF化 ・メーカへ図面の提供
52	4.5.1(5) 予防保全（定期点検）	定常	年次		【定期点検実施状況管理】 関連事業者アテンド(NPR保守機)	NPR(保守機)の定期点検のため、保守拠点へ関連事業者をアテンドする。 ・事前申請 ・アテンド ・事後作業
53	4.5.1(5) 予防保全（定期点検）	定常	年次		【定期点検実施状況管理】 関連事業者アテンド(機構本部A、機構本部Bのみ)	機構本部A、機構本部Bのセキュリティエリア内の点検に関連事業者の保守員をアテンドする。 ・事前申請 ・アテンド ・事後作業
54	4.5.1(5) 予防保全（定期点検）	定常	年次		【定期点検実施状況管理】 定期点検結果の確認	定期点検の実績を確認するため、メーカからの報告を取りまとめる。 ・報告物の収集 ・報告結果のとりまとめ
55	4.5.4 (6)⑪稼働状況管理	定常	月次		【作業工数報告業務】 月次報告資料作成	機構本部へ月次報告する資料を作成する。

業務内容詳細（拠点装置運用管理）

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想定 回数等 (随時の場合)	作業項目	作業内容
56	4.5.4 (6)⑪稼働状況管理	定常	月次		【端末装置情報報告業務】 SKYSEA更新	機構本部へ月次報告向けのSKYSEAより取得した情報を精査、加工する。 ・ SKYSEAからの情報取得 ・ Pi/oの取得 ・ 形式変換ツールの実行 ・ 設定値シートの突合 ・ 拠点別台数表の作成 ・ 前月との比較データの抽出 ・ 前月との比較データの妥当性確認 ・ 調達台数との比較データの抽出 ・ 調達台数との比較データの妥当性確認 ・ 担当者レビュー
57	4.5.4 (6)⑪稼働状況管理	定常	月次		【端末装置情報報告業務】 月次報告資料作成	機構本部へ月次報告向けの資料を作成する。 ・ 装置情報一覧の更新 ・ 調達台数との差分表の更新 ・ 担当者レビュー
58	4.5.4 (6)⑪稼働状況管理	定常	月次		【保守機Ⅱ 管理状況報告業務】 月次報告資料作成	設計調整結果をもとにパスワード一覧を更新し、保守拠点へ展開する。 ・ 更新分の受領 ・ 更新部分の修正 ・ クロスチェック ・ 周知文書の作成
59	4.5.4(3)⑤ 運用保守ユーザ IDの認証情報管理	定常	四半期		【システム運用アカウントのパスワード変 更】 ID/パスワード一覧の更新、展開	設計調整結果をもとにパスワード一覧を更新し、保守拠点へ展開する。 ・ 更新分の受領 ・ 更新部分の修正 ・ クロスチェック ・ 周知文書の作成
60	4.5.4(3)⑤ 運用保守ユーザ IDの認証情報管理	定常	四半期		【システム運用アカウントのパスワード変 更】 更新結果のとりまとめ	周知結果資料差し替え、ファイル更新結果を確認する。 ・ 完了状況の確認 ・ 結果のとりまとめ
61	4.5.4(3)⑤ 運用保守ユーザ IDの認証情報管理	定常	年次		【システム運用アカウントのパスワード変 更】 拠点基幹スイッチに関するパスワード変更後 のConfig登録	・ configの受領 ・ NWヘルパーへのconfig登録 ・ 旧configの削除
62	4.5.4(3)⑤ 運用保守ユーザ IDの認証情報管理	定常	年次		【システム運用アカウントのパスワード変 更】 config変更完了周知文書作成	保守用のconfigが更新された旨を保守拠点に周知する。 ・ 指示文書作成 ・ 全国展開
63	4.5.4(5)報告業務	随時		5.67回/月	管理ドキュメントメンテナンス	新規開発イベント等で、運用手順、報告書の変更があった場合、必要な管理ドキュメントのメンテナンスを行う。
64	4.5.4(6)① コミュニケー ション管理	定常	四半期		運用保守に関わる情報共有	全国各支社に対し、運用保守に関わる情報共有をPC会議を用いて各支社の担当者と実施する。 ・ 作業指示に対する対応状況確認 ・ 運用保守に関わる周知 ・ 改善点のヒアリング

業務内容詳細（拠点装置運用管理）

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想定 回数等 (随時の場合)	作業項目	作業内容
65	4.5.5 定例外作業の取扱い	随時		3件/月	スポット単金外工事対応	・工事申請書（見積依頼書・発注書）を受領する。 ・オーダー覧、進捗管理表の登録方法を検討する。 ・損益報告書、工事実施報告書の記載方法を検討する ・工事実施報告書の記載方法を決定し、保守拠点へ周知を行う。
66	4.5.5 定例外作業の取扱い	随時		2回/年	【随時作業（単価）】 工事単価の策定	新たな機器等の工事単価を策定する。
67	4.5.5 定例外作業の取扱い	随時		0.5回/年	【随時作業（単価）】 内容確認・内部承認	策定した工事単価を確認し、内部承認を得る。
68	4.5.5 定例外作業の取扱い	随時		2件/年	【随時作業（標準類、ツール）】 （新単価設定）様式の変更	新単価設定に伴う、機構との申請書のフォーマット調整。
69	4.5.5 定例外作業の取扱い	随時		2件/年	随時作業（標準類、ツール） （新単価設定）各種ツールの改修、設定変更	様式の変更に伴う各種ツールの改修。
70	4.5.5 定例外作業の取扱い	随時		1件/月	随時作業（標準類、ツール） ツール、関連様式の維持	工事オーダー一覧や通知書作成ツールなどに係る毎月発生する維持作業。
71	4.5.5定例外作業の取扱い	定常	日次		【個別案件（定期）】 個別案件抽出作業（日次）	工事オーダー上に個別案件となるオーダーがないか、点検する。（日次観点の点検）
72	4.5.5定例外作業の取扱い	随時		2.2件/月	【個別案件（通常）】 影響調査	該当の案件が工事オーダーに登録されているか、登録されているならばどのようなステータス、計画かを確認する。
73	4.5.5定例外作業の取扱い	随時		2.2件/月	【個別案件（通常）】 要件整理	要件整理資料を作成する。
74	4.5.5定例外作業の取扱い	随時		5回/年	【個別案件（通常）】 対応計画の立案	個別に要件整理が必要な案件が検知、発生した場合、関連メンバーと対応方針や作業項目、スケジュールを整理する。
75	4.5.5定例外作業の取扱い	随時		0.26件/月	【個別案件（新規）】 影響調査	該当の案件が工事オーダーに登録されているか、登録されているならばどのようなステータス、計画かを確認する。
76	4.5.5定例外作業の取扱い	随時		0.26件/月	【個別案件（新規）】 要件整理	要件整理資料を作成する。
77	4.5.5定例外作業の取扱い	随時		2回/年	【個別案件（新規・大規模）】 影響調査結果の回答に向けた関連メンバとの 計画立案	グループを跨る影響調査が必要な案件を検知、発生した場合、関連メンバーと影響調査報告書の作成に向けた対応方針や作業項目、スケジュールを整理する。
78	4.5.5定例外作業の取扱い	随時		0.5回/年	【個別案件（通常・大規模）】 調整事項の集約、展開	①～③の作業を繰り返す。 ①各チームが回答した影響調査結果を確認し、必要に応じて全チーム（本調達受託者及び共通基盤保守事業者）に展開する。 ②集約した結果を機構へ提示する ③機構から受領した結果を各チームへ展開する
79	4.5.5定例外作業の取扱い	随時		0.5回/年	【個別案件（通常・大規模）】 要件整理提示に向けた関連メンバーとの作業 計画立案	要件整理結果提示に向け、関連メンバーと対応方針や作業項目、スケジュールを整理する。
80	4.5.5定例外作業の取扱い	随時		2件/年	【個別案件（通常・大規模）】 要件整理	要件整理資料を作成する。
81	4.5.5定例外作業の取扱い	随時		0.5回/年	2次元コードリーダーの対応	2次元コードリーダーの故障対応を行う。

業務内容詳細（センタ運用管理）

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
1	4.5.2(1)① バックアップ運 用	定常	年次		TC/管理系サーバ/運用管理端末のバックア ップ	年次で実施するサーバのシステムバックアップ取得作業。
2	4.5.2(1)① バックアップ運 用	随時		1回/年	検疫システム自動バックアップ（再走行）	自動バックアップ失敗時の再走行を行う。
3	4.5.2(1)① バックアップ運 用	随時		2回/年	検疫システム手動バックアップ（リハーサル 稼動）	サーバの環境変更時のバックアップを取得する際のリハーサル稼動。
4	4.5.2(1)① バックアップ運 用	随時		2回/年	検疫システム手動バックアップ(本番環境)	サーバの環境変更時のバックアップを取得する。(本番環境)
5	4.5.2(1)① バックアップ運 用	定常	日次		全国共有データバックアップ処理確認	情報管理センタサーバのバックアップ装置のバックアップ状況を確認し、正常にバックアップが行えている事を確認する。
6	4.5.2(1)① バックアップ運 用	定常	年次		システムデータ（物理サーバ）バックアップ 実行	端末設備運用管理サービス事業者は、Arcserveのバックアップ管理機能により、バックアップ対象サーバのバックアップを実行する。
7	4.5.2(1)① バックアップ運 用	定常	年次		システムデータ（物理サーバ）バックアップ 確認	端末設備運用管理サービス事業者は、Arcserveの管理画面から、バックアップが正常に完了していることを確認する。
8	4.5.2(1)① バックアップ運 用	定常	日次		サーバログバックアップ／ログ管理データ バックアップ／ネットワーク機器コンフィグ バックアップ／業務データバックアップ	端末設備運用管理サービス事業者は、ETERNUSの管理画面から、バックアップが正常に完了していることを確認する。
9	4.5.2(1)① バックアップ運 用	定常	日次		資産情報バックアップの結果確認	共通基盤運用管理事業者・外部接続システム運用管理事業者は、資産情報バックアップ・世代管理の実行結果を確認する。
10	4.5.2(1)② ログ情報等の取 得	定常	月次		キャパシティ状況報告	端末運用Gへキャパシティ状況報告資料を報告する。報告内容は、各サーバ（ADサーバ、グループウェア、ファイル共有、メールサーバ、人 事異動情報サーバ、SCCMサーバ、生体認証サーバ、TC）のCPU使用率、メモリ使用率、ディスク使用率、ディスク待ち要求数、NW帯域使 用状況。
11	4.5.2(1)② ログ情報等の取 得	随時		1回/日	（検疫）削除ログファイル収集	届書データ授受用ファイルサーバに格納された削除ログを収集し、端末運用Gに報告する。
12	4.5.2(1)② ログ情報等の取 得	定常	月次		NetLineDancerログ退避運用	NetLineDamcerにおけるログを13ヶ月保存するため、管理画面からログを取得する。
13	4.5.2(1)② ログ情報等の取 得	定常	月次		VBフルスキャン実施状況ログ取得	フルスキャン情報を確認するために、VirusBusterサーバからフルスキャン状況の情報取得を行う。
14	4.5.2(1)② ログ情報等の取 得	随時		11.9回/月	ふるまい・不正操作検出ログ取得及び解析	端末設備運用管理サービス事業者は、ふるまい・不正操作を検出した装置や時間帯等の情報から、共通基盤システムのログ管理機能を利用し てログの検索を行い、不正操作したログ情報の取得を行い、共通基盤環境構築等事業者へログ解析依頼を行う。
15	4.5.2(1)② ログ情報等の取 得	随時		1回/月	RADIUS認証サーバの認証ログ確認	不正端末接続時に不正接続装置の調査に必要なログの確認を行う。
16	4.5.2(1)② ログ情報等の取 得	随時		1回/年	認証代行のログ確認	認証代行運用手順に沿い、以下を確認する。 ・恒常的に出力されるログファイルの参照先 ・コマンド実行で出力するログの取得・参照手順 ・一時的に出力するトレースログの出力方法

業務内容詳細（センタ運用管理）

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
17	4.5.2(1)② ログ情報等の取得	定常	月次		WinActor導入に伴う端末設備運用管理 (WinActorログの収集)	全国に配備されたWinActor端末における、シナリオの実行ログを取得する運用を実施する。
18	4.5.2(1)② ログ情報等の取得	随時		4.8回/年	外部媒体書き出しログ取得運用	外部媒体書き出しログの収集、配布、整形作業を実施する。
19	4.5.2(1)③ 予防保全(定期点検)	定常	月次		端末統計情報取得	運用管理端末を使用し、全TCに格納されている端末統計情報を月次で取得し、機構へ提出する。
20	4.5.2'(1)③ 予防保全(定期点検)	定常	年次		予防保全（定期点検）	ハードウェア事業者にて実施する点検作業の実施調整、対応支援。
21	4.5.2(1)③(iv)システム動作確認の実施	定常	週初め		全台疎通確認	全台起動日に起動されている端末の状況を調査する。
22	4.5.2(1)④ 法定点検運用	定常	年次		停電対応	機構本部B全館点検に伴う停電対応を行う。
23	4.5.2(2)① プログラム配布・適用業務	定常	月次		パッチ公表・適用情報一覧報告	運用総括チーム経由でシステム基盤整備Gへ毎月公表されるMSパッチ及びPPに対するパッチを一覧に整理し、該当するパッチの適応状況を更新する。
24	4.5.2(2)① プログラム配布・適用業務	随時		6回/年	(検疫) セキュリティパッチ配布(随時)	検疫システムの端末に対して、必要な場合、随時でセキュリティパッチの適用作業を実施する。(windows OSセキュリティパッチ適用は隔月実施)
25	4.5.2(2)① プログラム配布・適用業務	定常	日次		クライアントセキュリティパッチ適用(デバック検証配布)	関連事業者からの机上検証結果を受け、デバック環境に対して資材配布するために資材やチェックリストの準備を行い、配布作業を実施する。
26	4.5.2(2)① プログラム配布・適用業務	定常	月次		クライアントセキュリティパッチ適用(机上検証)	セキュリティパッチの公表を受け、関連事業者へ机上検証の依頼を行い、結果受領までを管理する。
27	4.5.2(2)① プログラム配布・適用業務	定常	月次		クライアントセキュリティパッチ適用(機構承認)	本番環境に対して資材配布する前に、機構本部へパッチ配布作業の承認をいただく。
28	4.5.2(2)① プログラム配布・適用業務	定常	月次		クライアントセキュリティパッチ適用(本番配布)	デバック環境の配布結果を受け、本番環境に対して資材配布するためのチェックリストの準備を行い、配布作業を実施する。
29	4.5.2(2)① プログラム配布・適用業務	定常	月次		クライアントセキュリティパッチ適用(未適用装置情報整理)	直近1か月の間にSKYSEAにて配布した資材の適用状況の全ステータスの情報の抽出、VirusBusterサーバより全装置情報を抽出する。
30	4.5.2(2)① プログラム配布・適用業務	随時		13.8回/月	センターサーバセキュリティパッチ適用(デバック検証配布)	関連事業者からの机上検証結果を受け、デバック環境に対して資材配布するために資材やチェックリストの準備を行い、配布作業を実施する。
31	4.5.2(2)① プログラム配布・適用業務	随時		13.8回/月	センターサーバセキュリティパッチ適用(机上検証)	セキュリティパッチの公表を受け、関連事業者へ机上検証の依頼を行い、結果受領までを管理する。
32	4.5.2(2)① プログラム配布・適用業務	随時		13.8回/月	センターサーバセキュリティパッチ適用(機構承認)	本番環境に対して資材配布する前に、機構本部へパッチ配布作業の承認をいただく。
33	4.5.2(2)① プログラム配布・適用業務	随時		13.8回/月	センターサーバセキュリティパッチ適用(本番配布)	デバック環境の配布結果を受け、本番環境に対して資材配布するためのチェックリストの準備を行い、配布作業を実施する

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
34	4.5.2(2)① プログラム配 布・適用業務	随時		20回/年	プログラム配布	ファイル転送作業に伴い、ファイル転送資材の作成、ファイル転送差分CDの作成、ファイル転送リハーサル、及びファイル転送の実施を行 う。
35	4.5.2(2)① プログラム配 布・適用業務	随時		18回/年	プログラム配布関連作業	ファイル転送作業に伴う、他事業者調整、機構本部A試験席装置の更新、及び次回ファイル転送に向けたファイル転送のキャンセル作業を行 う。
36	4.5.2(2)① プログラム配 布・適用業務	随時		18回/年	プログラム配布関連作業報告	ファイル転送の実施に伴う機構への資料作成、及び報告を行う。
37	4.5.2(2)① プログラム配 布・適用業務	定常	隔月		セキュリティパッチ実機検証（機構本部A設 置機器）	マシン室（機構本部A）設置サーバ本番機設備へのセキュリティパッチ適用（装置再起動、動作確認、適用確認等） 機構本部Bのサーバについても本項目で計上する。 パッチ適用は原則情報管理センタからのSKYSEAによって行うため、反映のための再起動の作業となる。 （TC原本装置のみ情管と接続されていないため手動で適用する）
38	4.5.2(2)① プログラム配 布・適用業務	定常	月次		セキュリティパッチの適用	・セキュリティパッチを配布管理する構成管理サーバに対して、管理手順に則り、対象ファイルを登録し、構成管理サーバにて自動配布(適 用)を行う。 ・生体認証サーバ群へのセキュリティパッチを手動により適用する。 ・構成管理サーバによる自動適用が実施できない場合には手動により適用する。
39	4.5.2(2)① プログラム配 布・適用業務	随時		6回/月	脆弱性対応 拠点端末のセキュリティパッチ未適用対応	セキュリティパッチ未適用 SCCMコレクションに反映されない装置に対して、個別復旧を行う。
40	4.5.2(2)① プログラム配 布・適用業務	随時		6回/年	ログ取得用サーバのセキュリティパッチの手 動適用	Skyseaのサポート対象外のサーバへ手動でセキュリティパッチを適用する。
41	4.5.2(2)① プログラム配 布・適用業務	定常	隔月		セキュリティパッチ運用（サーバ）	評価機環境への適用、本番環境への適用を行う。
42	4.5.2(3)システム監視/障害 対応	随時		15件/月	トラブル対応 情報取得、機構報告、故障管理等	ソフトウェア起因でのトラブルや問い合わせ起因でのログ取得、一次解析、メカアサイン等
43	4.5.2(3)システム監視/障害 対応	随時		13件/月	トラブル対応 情報取得、機構報告、故障管理等	ハードウェア起因でのトラブルや問い合わせ起因でのログ取得、一次解析、メカアサイン等
44	4.5.2(3)システム監視/障害 対応	随時		4回/年	トラブル対応 再現試験環境構築 復旧対応等	トラブルに伴う再現試験や復旧に向けた試験環境構築対応。
45	4.5.2(3)システム監視/障害 対応	定常	日次		目視点検	設置機器（機構本部A）の目視点検を行う。
46	4.5.2(3)システム監視/障害 対応	定常	日次		故障状況報告（日次）	監視端末に出力されたメッセージについて、事象、原因、対応を報告資料にまとめ、端末運用Gに報告する。
47	4.5.2(3)システム監視/障害 対応	定常	月次		故障状況報告（月次）	月次で提出する環境変更実績や故障実績報告資料作成、レビューを行い、端末運用Gに報告する。
48	4.5.2(3)システム監視/障害 対応	随時		1件/月	NW機器故障時対応 （通信設定確認等）	本番ネットワーク機器の装置故障に伴う交換後のネットワーク設定値の確認を行う。
49	4.5.2(3)システム監視/障害 対応	定常	四半期		監視が不要となったメッセージの抑止	端末運用Gが監視が不要と承認したメッセージについて、監視サーバからバトランプ鳴動や警告メッセージ発出を抑止するため、定期的にバ トランプ鳴動や警告メッセージの見直しを実施する。

業務内容詳細（センタ運用管理）

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
50	4.5.2(3)システム監視/障害 対応	定常	日次		ハードウェア状態確認（目視点検）	ハードウェアの状態を遠隔で確認する。
51	4.5.2(3)システム監視/障害 対応	随時		1回/日	ソフトウェア障害対応(社保AP以外)	ソフトウェアの障害を検知した際に対応を実施する。
52	4.5.2(3)システム監視/障害 対応	随時		1.1回/日	ハードウェア障害対応（全国拠点）	機構本部B以外の拠点でハードウェア障害を検知した際に対応を実施する。
53	4.5.2(3)システム監視/障害 対応	随時		10回/年	ハードウェア障害対応（機構本部B保守）	機構本部B拠点でハードウェア障害を検知した際に対応を実施する。
54	4.5.2(3)システム監視/障害 対応	随時		1回/月	ハードウェア障害対応（保守作業無）	保守作業を必要としないハードウェアの障害を検知した際に対応を実施する。
55	4.5.2(4)③ 統合ネットワー クの遮断ログの確認	定常	月次		統合NWの月次報告資料作成	統合NWから遮断された通信のログ（機構本部AのFW分）が、平日1日、休日1日分、毎月送付され、その通信の妥当性（意図した通信か否か）を確認する。遮断された通信数、通信の種類等によって調査稼働は増減する。
56	4.5.2(4)⑥ 監査対応	定常	年次		監査ログ取得	監査ログを取得する。
57	4.5.2(4)⑥ 監査対応	随時		7.6回/月	問題のあるURLへのアクセス状況確認	NISCから提供される、以下のようなセキュリティリスクに関する調査を実施する。 ・問題があるURLにアクセスした形跡が無いことを確認する。
58	4.5.2(5) 業務環境管理	随時		1回/年	生体認証アカウント管理者報告	端末運用Gへ生体認証アカウント管理者報告資料を報告する。報告内容は、職員区分毎のアカウント管理者数の集計、組織毎のアカウント管理者数の集計、アカウント管理者の一覧。
59	4.5.2(5) 業務環境管理	定常	週次		サーバラック鍵利用状況報告	端末運用Gへサーバラック鍵の利用状況に関わる資料を報告する。報告内容は、氏名、利用サーバラック鍵、日時。
60	4.5.2(5) 業務環境管理	定常	年次		マシン室利用許可申請	端末運用Gへマシン室に入退室する担当者の情報を報告する。報告内容は、対象マシン室、氏名、所属。
61	4.5.2(5) 業務環境管理	定常	四半期		未使用アカウントの抽出	アクセス権管理システム及び生体認証システムより、対象期間に利用がないアカウントを抽出し、報告する。
62	4.5.2(5) 業務環境管理	定常	月次		アカウント一覧の送付	ADアカウントの最終ログオンの情報を拠点単位（機構が周知しやすい形式）でファイル出力するため、そのファイルの送付作業。 ※アカウントロック作業の承認を頂く
63	4.5.2(5) 業務環境管理	定常	週次		週次運用計画の最終確認及び周知	週次運用計を立案・確認し、端末設備運用管理事業者内部及び関連業者へ周知する。
64	4.5.2(5) 業務環境管理	定常	半期		運用保守ユーザID棚卸	運用保守ユーザIDを適正数に管理するため、年2回の棚卸を行う。運用保守ユーザIDを保有している担当者の利用実態をヒアリングし、利用頻度および利用目的を踏まえて適正数を維持するため、運用保守ユーザIDの削除等を行う。
65	4.5.2(5) 業務環境管理	定常	月次		運用保守ユーザID設定	運用保守ユーザIDを担当者からの依頼を踏まえて、設定（登録または削除）を行う。また、設定に伴い端末運用Gへの申請を行う。
66	4.5.2(5) 業務環境管理	定常	年次		ユーザアカウント棚卸	機構本部（端末運用G）から指示を受領後、アカウントと最終ログインの情報取得を行い、拠点情報を付与した一覧を提出する。

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
67	4.5.2(5) 業務環境管理	定常	月次		外部媒体管理台帳の棚卸対応（月次）	共通基盤運用管理事業者・外部接続システム運用管理事業者は、外部媒体の棚卸し作業を月次で実施し、棚卸し時点で一定期間接続がない外部媒体をSKYSEAサーバの管理台帳から削除する。
68	4.5.2(5) 業務環境管理	定常	月次		月次報告資料作成	機構 L A N センタサーバ、事務ファイル共有、基幹共有ファイルサーバに保存されているファイルのうち、日本年金機構から指示があった「機 3」が含まれるファイルを抽出する。
69	4.5.2(5) 業務環境管理	随時		1 回/年	(検疫) 機構依頼（アクセスログ監査）	機構本部（端末運用G）よりアクセスログの取得依頼を受領後、ALog ConVerter Web コンソール上で、ファイルアクセスログを取得し報告する。
70	4.5.2(5) 業務環境管理	随時		1 回/年	(検疫) 機構依頼（管理投入/ログ監査）	機構本部（端末運用G）よりログの取得依頼を受領後、ALog ConVerter Web コンソール上で、ログを取得し報告する。
71	4.5.2(5) 業務環境管理	随時		1 回/年	(検疫) 機構依頼（証跡ログ）	機構本部（端末運用G）よりアクセスログの取得依頼を受領後InfoTraceの管理コンソールを操作して、端末証跡ログを取得し報告する。
72	4.5.2(5) 業務環境管理	随時		1 回/週	(検疫) 各種一覧管理	定義ファイル適用状況取得（Symantec）する。
73	4.5.2(5) 業務環境管理	随時		7.9 台/月	(検疫) 故障交換対応	現地事務所で利用している検疫端末に対して、故障交換を実施した場合の端末の設定確認（センタサーバとの疎通確認、・セキュリティパッチの配布、・個別資材の配布等）を行う。
74	4.5.2(5) 業務環境管理	定常	年次		JP1カレンダー設定	JP1/AJS3の管理コンソールにログインし、内閣府HPから取得したカレンダー登録作業を実施する。
75	4.5.2(5) 業務環境管理	定常	日次		SKYSEA装置情報エクスポート	SKYSEAの定点的な情報を、SKYSEAの管理コンソールより取得する。
76	4.5.2(5) 業務環境管理	定常	日次		TV会議 ウィルス対策ソフトウェア更新確認	本番環境のサーバへ配布した定義ファイルが最新の状態であることを確認し、必要に応じて再配布の作業を実施する。
77	4.5.2(5) 業務環境管理	定常	週 2 日		Wake On Lanによる全台起動（ウィルス定義ファイル）①	各事務所拠点に設置されている端末のウィルス定義ファイル更新のため、SKYSEAのWakeOnLan機能を用いて各事務所拠点の未起動の端末を起動する。
78	4.5.2(5) 業務環境管理	定常	年次		Windows統合認証検索用アカウントパスワード変更（認証代行）	統合Windows認証用ユーザ（keytabマッピングユーザ）および認証モジュール接続ユーザ（AD 接続ユーザ）のパスワードを変更する。
79	4.5.2(5) 業務環境管理	定常	日次		アルゴリズム危殆化報告	アルゴリズムの危殆化に関する情報を毎日確認し、危殆化に関する公表があった場合に機構本部へ報告を行う。
80	4.5.2(5) 業務環境管理	定常	日次		ウィルス検知状況確認（Deep Security）	前日から作業当日の9時の間にウィルス検知などがなかったことをログを取得して確認する。
81	4.5.2(5) 業務環境管理	定常	日次		ウィルス定義ファイル適用状況確認（Deep Security）	本番環境のサーバへ配布した定義ファイルが最新の状態であることを確認し、必要に応じて再配布の作業を実施する。
82	4.5.2(5) 業務環境管理	定常	日次		ウィルス定義ファイル配布（Deep Security デバック）	毎日DeepSecurityサイトから定義ファイルをダウンロードし、デバック機のサーバへアップロードを行ったのち、デバック環境の端末およびサーバへの適用作業を実施する。
83	4.5.2(5) 業務環境管理	定常	日次		ウィルス定義ファイル配布（Deep Security 本番）	デバック環境にて検証が行われた最新の定義ファイルを本番環境へアップロードし、本番環境の端末およびサーバへ配布が行える設定まで実施する。

業務内容詳細（センタ運用管理）

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
84	4.5.2(5) 業務環境管理	定常	年次		パスワード変更（SKYSEA）	端末設備運用管理事業者は、定期的にパスワードの変更を行う。
85	4.5.2(5) 業務環境管理	定常	月次		ヘルプデスクCEHサーバ・DBサーバ維持管理 （月次作業）	ヘルプデスクのCEHサーバ（AIサーバ）・インシデントDBサーバに対し、セキュリティパッチ適用作業および移設工事に伴う事務所・設備情報の更新を実施する。
86	4.5.2(5) 業務環境管理	定常	週次		ヘルプデスクCEHサーバ・DBサーバ維持管理 （週次作業）	ヘルプデスクのCEHサーバ（AIサーバ）・インシデントDBサーバに対し、稼働状態およびウイルススキャンの実施状況を確認する。
87	4.5.2(5) 業務環境管理	定常	月次		ヘルプデスクウイルス対策サーバ維持管理 （月次）	ヘルプデスクのウイルス対策サーバに対し、セキュリティパッチ適用作業を実施する。
88	4.5.2(5) 業務環境管理	定常	日次		ヘルプデスクウイルス対策サーバ維持管理 （日次）	ヘルプデスクサーバ設置環境のウイルス対策サーバへ日次でウイルス定義ファイルの適用を行う。
89	4.5.2(5) 業務環境管理	随時		16.92回/月	共通基盤サーバセキュリティパッチ適用（デバッグ検証 配布）	デバッグ環境の共通基盤サーバに対してセキュリティパッチの適用作業を実施する。
90	4.5.2(5) 業務環境管理	随時		16.92回/月	共通基盤サーバセキュリティパッチ適用（機構承認）	本番環境に対して資材配布する前に、機構本部へパッチ配布作業の承認を、システム環境変更等作業スケジュールのツールを用いていただく。
91	4.5.2(5) 業務環境管理	随時		16.92回/月	共通基盤サーバセキュリティパッチ適用（本番配布）	デバッグ環境の配布結果を受け、本番環境に対して資材配布するためのチェックリストの準備を行い、配布作業を実施する。
92	4.5.2(5) 業務環境管理	定常	四半期		工事事業者が利用するドメイン参加用のアカ ウントのパスワード変更	工事事業者が端末をドメイン参加させる場合に利用するアカウントの、パスワードの変更を実施する。
93	4.5.2(5) 業務環境管理	随時		1回/年	手動によるログ管理（WinSyslog）	端末設備運用管理事業者は、Backup4allにてログのリネーム、移動が行えなかった場合、手動にて対象のログのリネーム・移動を行う。
94	4.5.2(5) 業務環境管理	定常	日次		脆弱性・ウィルス公表報告(Deep Security)	trendmicroのウィルス公表サイトを毎日確認し、ウィルス情報の公表があった場合に機構本部へ報告を行う。
95	4.5.2(5) 業務環境管理	定常	年次		ジョブ管理サーバカレンダー設定	ジョブ管理サーバの管理コンソールにログインし、内閣府HPから取得したカレンダー登録作業を実施する。 カレンダー登録作業が完了したことを機構本部職員に報告する。
96	4.5.2(5) 業務環境管理	定常	月次		配布資材削除(Windows)	Windowsサーバに対し、不要となった配布資材を削除する。
97	4.5.2(5) 業務環境管理	定常	月次		Pio/Lio事後削除（工事）	工事で不要となったPio/Lioの情報をセンタで削除する。 （Pioとは各装置に割り当てられた、装置を一意に確認できる固定の装置名称。Lioとは、社会保険オンラインシステムが内部で使用している論理的な装置名。）
98	4.5.2(5) 業務環境管理	定常	月次		Pio/Lio事前登録（工事）	工事で登録の必要があるPio/Lioの情報をセンタで事前に登録する。
99	4.5.2(5) 業務環境管理	定常	月次		SKYSEA削除	撤去工事で管理が不要になった端末に対し、SKYSEAの管理サーバ上で削除を行う。
100	4.5.2(5) 業務環境管理	定常	月次		USB接続機器情報追加・削除	機構からの電子決裁での依頼を受け、ADへの媒体権限付与およびSKYSEAへの接続対象USBのシリアル番号もしくは製品情報の登録・削除を行う。 その後、完了報告として登録情報を設備Gへ展開する。

業務内容詳細（センタ運用管理）

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
101	4.5.2(5) 業務環境管理	定常	月次		アクセス権追加／変更／削除	機構本部職員よりアクセス権追加依頼を受領し、依頼内容を確認する。その後、共通基盤システムのアクセス権管理機能を利用しアクセス権追加を実施および完了の報告をする。
102	4.5.2(5) 業務環境管理	定常	四半期		ソフトウェアアプリケーションと使用ユーザ 確認	機構本部より依頼を受け、ソフトウェアの使用状況を確認し、報告する。
103	4.5.2(5) 業務環境管理	定常	月次		ソフト搭載設定	機構本部からの依頼を受けて、指示された端末に個別ソフトウェア（一太郎、Visio、PDFライフ）のインストールもしくはアンインストール作業を実施する。
104	4.5.2(5) 業務環境管理	随時		6回/年	フォルダ/ファイル使用状況確認	機構からの依頼にもとづき、サーバからフォルダ/ファイル使用状況を取得して提供する。
105	4.5.2(5) 業務環境管理	随時		7.1件/月	プロファイル削除	事務所からの問合せを受けたヘルプデスクからの依頼を受け、指示された端末のプロファイル削除を実施する。
106	4.5.2(5) 業務環境管理	定常	月次		ローカル管理者パスワード一括設定（拠点工 事対応）	拠点工事期間にワンタイムパスワードの使用を抑止するため、工事対象拠点の装置全台についてローカル管理者パスワードを一時的に変更する。
107	4.5.2(5) 業務環境管理	定常	月次		拠点中継サーバ停止タスク設定	事務所からの停電連絡を受けたヘルプデスクからの依頼を受け、指示された事務所の中継サーバに対してシャットダウンタスクを設定する。
108	4.5.2(5) 業務環境管理	随時		1回/年 200台/回	拠点追加・廃止・移設・統廃合時の対応	拠点追加・廃止・移設・統廃合時のSKYSEAの導入・削除等対応を行う。 拠点追加：ポリシーの適用、部署ツリーの作成 拠点廃止：部署ツリーの削除 統廃合：ポリシーの適用、部署ツリーの作成・移動
109	4.5.2(5) 業務環境管理	随時		1回/年	申請者及び承認者削除	機構本部職員より申請者及び承認者削除依頼を受領し、依頼内容を確認する。 共通基盤システムの人事異動管理機能を利用し、申請者及び承認者の削除および完了の報告をする。
110	4.5.2(5) 業務環境管理	随時		6回/年	申請者及び承認者登録	機構本部職員より申請者及び承認者登録依頼を受領し、依頼内容を確認する。 共通基盤システムの人事異動管理機能を利用し、申請者及び承認者の登録および完了の報告をする。
111	4.5.2(5) 業務環境管理	随時		8回/年	人事異動申請削除	機構本部からの依頼を受け、指定された利用者IDに対する申請情報の削除を実施する。
112	4.5.2(5) 業務環境管理	随時		1回/月 132件/回	生体認証アカウントロック解除	ヘルプから依頼を受けたユーザアカウントの生体認証ロックを解除する作業を行う。
113	4.5.2(5) 業務環境管理	随時		1回/月 20.5件/回	端末工事のADサーバ設定	工事調整SGからの翌日工事情報を受領し、工事前の事前作業としてADサーバにコンピュータオブジェクトの登録を行う。
114	4.5.2(5) 業務環境管理	随時		1回/月 13.2件/回	端末工事のADサーバ設定（削除）	工事調整SGからの端末撤去情報を受領し、ADサーバから当該端末の削除作業を実施する。
115	4.5.2(5) 業務環境管理	随時		1回/月 17.1件/回	端末工事のウィルス対策サーバ設定	当日工事における端末の設定結果として、VBサーバへの反映確認および端末の環境チェックツールの実行結果を情報管理センタにて確認する。
116	4.5.2(5) 業務環境管理	随時		1回/月 85件/回	端末工事のウィルス対策サーバ設定（削除）	工事調整SGからの端末撤去情報を受領し、VBサーバから当該端末の削除作業を実施する。
117	4.5.2(5) 業務環境管理	随時		10回/年 0.7件/回	特殊メールアドレス作成	機構本部からの依頼を受けて、提示された情報の特殊メールアドレスおよび特殊メールアドレス向けに発行した利用者IDの登録を実施する。

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
118	4.5.2(5) 業務環境管理	随時		1回/年	不正が疑われる操作のレポート出力	機構本部よりレポートの取得指示を受領する。 レポート出力機能によりレポートを出力し、機構本部職員へ提示する。
119	4.5.2(5) 業務環境管理	随時		2.8回/月	Radius登録（保守）	本番機・予備機・保守機のMACアドレスは調達時にすべて登録するが、NW機器については、故障修理時にMACアドレスが変更になる。 そのため、RadiusMAC認証が必要な島HUBのみ故障対応時にMACの登録を実施する。
120	4.5.2(5) 業務環境管理	随時		109台/月	センタ接続確認	現地事務所で利用している端末に対して、故障交換を実施した場合の端末の設定確認を実施。
121	4.5.2(5) 業務環境管理	随時		9.6台/月	個別ソフトウェアアンインストール（工事 分）	拠点間移設時において、移設元の装置に個別ソフトウェアがインストールされている場合、移設工事前に遠隔で個別ソフトウェアのアンイン ストールを実施する。
122	4.5.2(5) 業務環境管理	随時		9.4台/月	特定端末へのソフト搭載設定	現地事務所で利用している端末に対して、故障交換を実施した場合の個別資材のインストール作業を実施。
123	4.5.2(5) 業務環境管理	随時		16件/年	トークン端末の紐付け設定	社会保険オンラインシステムサーバ設備事業者は、トークン端末の交換に伴い必要となるセンタ側作業（シンクライアント端末、仮想デスク トップ環境、トークン端末の紐付け設定）を実施する。
124	4.5.2(5) 業務環境管理	定常	年次		復号化権限アカウント棚卸し	ユーザ情報CSVから復号化権限の棚卸し資料を作成する。
125	4.5.2(5) 業務環境管理	随時		1回/月	緊急時における作業承認	夜間等の作業承認者が不在の時間帯に緊急の作業が発生した場合、端末設備運用管理事業者は、共通基盤システムの監査機能の対象となる サーバ及びネットワーク機器に接続する端末設備運用管理事業者及びその他事業者からの作業申請に対し、機構本部職員に代わって監査機能 を利用して承認する。
126	4.5.2(5) 業務環境管理	随時		1回/年	監査機能の検知設定変更	端末設備運用管理事業者は、機構本部職員から監査機能（ESS REC）による検知設定の変更依頼を受領した場合、設定変更を実施する。
127	4.5.2(5) 業務環境管理	定常	月次		未起動端末の棚卸し	直近1ヶ月起動実績がない端末について機構へ報告する。
128	4.5.2(5) 業務環境管理	随時		1回/年	ハッシュ値検索	NISCから提供される脅威情報に掲載のハッシュ値を持つファイルが、システム上に存在するか検疫PCで取得したハッシュ情報ログを基に検 索を行う。同じハッシュ値を持つファイルがハッシュ情報ログに確認された場合は、SKYSEAのファイル追跡機能等で存在するフォルダ等の 確認を実施する。
129	4.5.2(5) 業務環境管理	随時		6回/年	暗号鍵の変更運用	端末設備運用管理事業者は、共通基盤システムにて取り扱う暗号化対象のデータを暗号化／復号するために、使用する暗号鍵の変更を行う。
130	4.5.2(5) 業務環境管理	定常	月次		不要な作業申請の削除	端末設備運用管理事業者は、監査機能で参照しない不要な作業申請情報の削除を行う。
131	4.5.2(5) 業務環境管理	随時		4件/月	手順書修正	端末維持運用で使用する手順書等の作成や修正等の改善を行う。
132	4.5.2(5) 業務環境管理	定常	月次		月次対応	月単位で実施するデバッグ関連作業等 ・装置故障時の交換対応、復旧対応 ・セキュリティパッチ適用作業
133	4.5.2(5) 業務環境管理	定常	週次		週次対応 （リロードサーバへの資材開放等）	・週次でデバッグ向けにリリースされた改修版APを試験者向け環境構築システム（リロードサーバと呼称）に反映する作業 ・デバッグ装置の見回り（ランプ確認等）

業務内容詳細（センタ運用管理）

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
134	4.5.2(5) 業務環境管理	定常	日次		日次対応 (デバッグ問い合わせ対応)	日次でのデバッグ関連作業 (問い合わせ対応、環境構築依頼への対応、日次見回り等)
135	4.5.2(5) 業務環境管理	随時		1回/月	備品管理	デバッグ環境の消耗品（プリンタトナー等）の管理対応
136	4.5.2(5) 業務環境管理	随時		13回/年	工事資材提供	工事に伴い発生する資材修正（監視サーバ内で保持する装置アドレス情報ファイルの修正、検証、リリース対応）
137	4.5.2(5) 業務環境管理	随時		1回/月	保守資材提供	差分資材（APフ統、セキュリティパッチ等、原本からの差分環境変更を適用する資材）を適用するパッチの改修対応。
138	4.5.2(5) 業務環境管理	随時		0.38回/年	保守担当向け原本作成	保守拠点向けに提供する装置原本の更新（セキュリティパッチ、環境変更の取込）
139	4.5.2(5) 業務環境管理	随時		4回/年	環境のリフレッシュ	試験等で設定変更されたデバッグ環境の装置を原本から復元し、リフレッシュする。
140	4.5.2(5) 業務環境管理	定常	月次		マシン調整WGの開催、調整（月次分）	デバッグ環境の装置を使用する上でのスケジュール管理、調整、マシン管理（月次でのTC環境毎のマシン調整）
141	4.5.2(5) 業務環境管理	定常	週次		マシン調整WGの開催、調整（週次分）	デバッグ環境の装置を使用する上でのスケジュール管理、調整、マシン管理（週次での細かなマシン調整）
142	4.5.2(5) 業務環境管理	随時		1回/月	システム設備管理	評価機及びR T機について、適宜、整備を実施し、常に動作可能な状況で保管するとともに、関連事業者からの修理返却等の在庫管理及び定期的な棚卸を行う。また、関連事業者からの各種問合せにも対応する。
143	4.5.2(5) 業務環境管理	随時		5回/年	資材配布	ツールで対象のWM等へ資材の配布や環境変更を速隔で実施する。 (本来はファイル転送などで実施する作業について、期間的な制約によりツール実行により実施する作業)
144	4.5.2(5) 業務環境管理	随時		1回/年	資材配布（フ転対象外サーバへの資材フ統作業）	ファイル転対象外サーバへの資材ファイル統合作業 (監視サーバ、RASサーバ、RADIUSサーバ、利用者サーバ、生体認証サーバ、運用管理端末等)
145	4.5.2(5) 業務環境管理	定常	年次		年1回の帳票試験対応	帳票の印字試験を行う。
146	4.5.2(5) 業務環境管理	定常	週次		関連担当調整会議対応	関連事業者調整会議に出席する。本会議は、週次で開催される。本会議内容は、翌週以降の開発イベントおよび工事、運用変更にもなうSG連携作業内容の確認。議事内容を踏まえてSG内での情報共有を行う。
147	4.5.2(5) 業務環境管理	随時		2回/年	FENCE監査対応	個人情報を含むログやデータファイル等を取得した案件に対し、個人情報の管理状況が適切であることの本調達受託社内監査を行う対応。
148	4.5.2(5) 業務環境管理	随時		13回/年	端末設備拠点の新設/移転/統合/廃止に伴う監視設定	端末設備拠点の新設/移転/統合/廃止に伴い、工事調整チームからの情報を基に監視サーバ上の監視定義の変更を行う。
149	4.5.2(5) 業務環境管理	随時		4回/年	RADIUSクライアント登録	拠点工事によりRADIUSクライアント（HUB情報）の登録変更があった場合に、RADIUSサーバに登録を行う対応。
150	4.5.2(5) 業務環境管理	随時		2回/年	暗号鍵/復号鍵ファイル開放作業	機構が作成した暗号鍵/復号鍵ファイルを受領し、ファイル転送を行うために資材の正式開放手続きを行う。

業務内容詳細（センタ運用管理）

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
151	4.5.2(5) 業務環境管理	定常	月次		TCの運転日設定	機構HPの開所日程を基に、TCの運転日設定作業を行う。
152	4.5.2(5) 業務環境管理	定常	年次		遠隔地運用 ・事務局作業 シス管への提出等 ・メーカとしての運管分作業 原本の遠隔地資材作成等	システムバックアップやプログラムソース等を機構本部Aビルの被災に備えて遠隔地に退避する運用の対応。
153	4.5.2(5) 業務環境管理	随時		18.5回/月	随時対応（問い合わせ対応）	問い合わせ対応（ヘルプデスク、機構、関連事業者等）
154	4.5.2(5) 業務環境管理	定常	日次		共通基盤ジョブ走行結果確認	SystemOperationManagerよりジョブ走行結果を確認する。 ・ジョブ走行状態一覧と見比べ、走行状態を朝一確認する。 ・証跡を格納し、異常状態だった場合は機構LAN維持業者へ連携する。
155	4.5.2(5) 業務環境管理	随時		1回/年	ファームウェア運用/立会い（機構本部B設置サーバ）	ハードベンダにて手動でファームウェアを適用する場合に立会いを実施する。
156	4.5.2(5) 業務環境管理	随時		1回/月	ウィルス検知（VirusBuster）（検疫システム）	検疫システムのサーバでVirusbusterの検知をした場合の対応を行う。
157	4.5.2(5) 業務環境管理	定常	年次		定期点検作業監査（共通基盤・共通事務サーバ）	ハードウェア事業者による共通基盤・共通事務サーバの点検時に立会いを行う。
158	4.5.2(5) 業務環境管理	随時		1回/月	ウィルス検知対応	ウィルス検知をした際に対応を実施する。
159	4.5.2(5) 業務環境管理	定常	月次		業務ツールサーバ利用状況確認	業務ツールサーバにおける各ファイルサーバの利用者数を確認する。 特定のファイルサーバにおいて利用者数の偏りが見られた場合、業務ツールサーバ利用者数の平準化対応を実施する。
160	4.5.2(5) 業務環境管理	随時		1回/月	セキュア情報交換装置ディスク枯渇対応	・端末設備運用管理事業者は、セキュア情報交換装置のディスク枯渇傾向を確認した場合、機構本部職員へ報告を行うとともに、必要に応じ拠点単位の利用状況を出力のうえ機構本部職員へ提示し、枯渇の防止に向けた対応の協議を行う。 ・機構本部職員は、該当の事務所等拠点において媒体書出しが完了した旨を運用管理サービス事業者へ回答する。 ・運用管理事業者は、セキュア情報交換装置のディスク使用状況を確認、枯渇傾向が解消されたことを確認のうえ、機構本部職員へ報告する。
161	4.5.2(5) 業務環境管理	随時		1回/月	不正端末検知装置	端末設備運用管理事業者が運用管理端末にて不正端末検知メッセージを検知する。不正端末検知した旨、機構本部職員に報告する。 端末設備運用管理事業者は、不正端末検知した年金事務所等拠点の事務所等職員へ連絡し、不正接続の有無を確認する。 端末増設時の事前申請漏れの場合は、別途端末増設の申請を行い、機構本部職員へ申請漏れ装置の接続だった旨報告する。
162	4.5.2(5) 業務環境管理	定常	月次		残留セッション調査	端末設備運用管理事業者は、業務ツールサーバへのリモートデスクトップ接続における残留セッションの有無を調査する。 端末設備運用管理事業者は、残留セッションを確認した場合、運用管理端末を操作し、管理サーバからの強制ログオフを実施する。
163	4.5.2(5) 業務環境管理	随時		11.9回/月	ふるまい・不正操作検出	端末設備運用管理事業者が共通基盤システムの運行監視機能にてふるまい・不正操作検出メッセージを検知する。ふるまい・不正操作検出した旨、機構本部職員に報告する。

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
164	4.5.2(5) 業務環境管理	随時		1回/月	障害時NW機器の遠隔操作	NW機器を直接操作し、監視メッセージ（装置名、IPアドレス、拠点、メッセージ内容）をもとに、装置状態およびエラーの発生有無の解析を行う。
165	4.5.2(5) 業務環境管理	随時		3回/年	HDIカートリッジの再構成	社会保険オンラインシステムサーバ設備事業者は、定期点検時に故障部位を含んだHDI（Hosted Desktop Infrastructure）カートリッジ上の正常ノードを予備カートリッジへ振り替え、HDIカートリッジを交換し、HDIカートリッジの構成の整理を行う。
166	4.5.2(5) 業務環境管理	定常	月次		情対室向けレポートの提出	NIASを用いたデータ（機3ファイル、アクセス権レポート）の取得、各拠点への配布に当たってのデータ加工、およびレポートの作成。
167	4.5.2(5) 業務環境管理	定常	四半期		2年経過ファイルの削除	2年経過ファイルの削除（リスト作成／提出、削除、結果の提出）を行う。
168	4.5.2(5) 業務環境管理	随時		1回/年	暗号化運用 （インデックス再構築）	基幹共有サーバのインデックス再構築を実施する。
169	4.5.2(5) 業務環境管理	随時		13.8回/月	問合せおよびトラブル対応	基幹共有ファイルサーバ、暗号化PP等にかかる問い合わせ対応を行う。
170	4.5.2(5) 業務環境管理	定常	月次		モバイル網の通信使用量の取得	NTTドコモビジネスのサイトから月次でモバイル網の通信量の取得。整形して運用総括に提出する。
171	4.5.2(5) 業務環境管理	定常	月次		ホームページバックアップデータ格納	機構職員がL P Cで機構ホームページを閲覧可能となるよう、ホームページバックアップ資材を事務ファイル共有へ格納を行う。
172	4.5.2(5) 業務環境管理	定常	月次		SKYリモート共有の対応	SKYSEAの画面共有機能を使用した際のログデータを月次で取得してインシデントの内容と突合することでSKYSEAの画面共有機能を不正に使用していないか確認を行う。
173	4.5.2(5) 業務環境管理	定常	週次		SKY媒体接続エラーメッセージの報告	SKYに表示された赤メッセージ(媒体接続エラー)について、週次でユーザーと件数を集計してお客様に報告する。 日次でメッセージ取得後に、赤メッセージを解除する。
174	4.5.2(5) 業務環境管理	定常	週次		プリンタMIB運用	SKYに表示された赤メッセージ(媒体接続エラー)について、週次でユーザーと件数を集計してお客様に報告する。 日次でメッセージ取得後に、赤メッセージを解除する。
175	4.5.2(5) 業務環境管理	定常	月次		情報の格付けに係る点検	月次で事務ファイル共有、基幹共有FSVの前月から更新のあったファイルを一覧化し全国拠点へ配布。（将来的にはさらに個人情報検索機能を用いて該当キーワードの有無も情報として追加する予定）
176	4.5.2(5) 業務環境管理	定常	月次		アクセス権初期化（共通事務）	電子決裁による拠点職員様からの依頼に基づき該当フォルダのアクセス権の初期化を行う。
177	4.5.2(5) 業務環境管理	定常	月次		アクセス権初期化（基幹共有）	電子決裁による拠点職員様からの依頼に基づき該当フォルダのアクセス権の初期化を行う。
178	4.5.2(5) 業務環境管理	随時		10回/月	MWMの初回ログオンの仮パスワード対応	市区町村職員等が初回ログオン時に仮パスワードでログオンできるように一時的な設定変更。
179	4.5.2(5) 業務環境管理	定常	10回/ 月		本部NW運管	端末設備の増設／移設／撤去が必要となる、事務所ごとの設置台数、端末シリアル、機番等の装置情報を管理するため、工事で変更となった、装置情報を精査する。 ・対象工事の抽出 ・管理簿の登録 ・機番報告シートの収集 ・ワークファイルの作成（ツール化） ・クロスチェック

項番	要件定義書 記載箇所	作業区分	サイ クル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
180	4.5.2(5) 業務環境管理	定常	3回/年		本部NW運営	故障対応で必要となる、事務所ごとの設置台数、端末シリアル、機番等の装置情報を管理するため、保守で変更となった、装置情報を精査する。 ・対象保守情報の抽出 ・故障交換データ取得 ・ワークファイルの作成（ツール化） ・クロスチェック
181	4.5.2(5) 業務環境管理	定常	半期		本部NW運営	外部システム接続などのイベント対応の中で機器の設定変更を行った際に、保守コンフィグを台帳に登録する。
182	4.5.2(5) 業務環境管理	随時		9回/月	本部NW運営	機構、ハードウェア事業者、外接事業者からの問合せ対応を行う。
183	4.5.2(5) 業務環境管理	随時		3回/年	本部NW運営	本部NW障害の対応を行う。
184	4.5.2(5) 業務環境管理	随時		6回/月	本部NW運営	イベントが発生した際に、本部NWハードウェア事業者が提供するネットワーク接続仕様書及びヒアリングシート（雛形）を用いてインタフェース等の調整を行い、影響調査を行う。 （新規拠点の増加、既存拠点の廃止、統合ネットワーク拡張L3スイッチからの接続変更、既存システムからのネットワーク変更依頼、端末移設事業者が行う端末増移設等）
185	4.5.2(5) 業務環境管理	随時		1回/月	本部NW運営	JP1に表示されたメッセージのうち、端末運用Gが表示抑止を承認したメッセージについて、監視除外設定を行う。
186	4.5.2(5) 業務環境管理	定常	月次		本部NW運営	月末に当月分のCPU利用率、メモリ使用率、回線利用状況をお客様に報告するため、月次レポートを作成する。
187	4.5.2(5) 業務環境管理	随時		6回/年	本部NW運営	本部NWハードウェア事業者が行うファームアップの対応を行う。
188	4.5.2(5) 業務環境管理	随時		2回/月	PostgreSQL保守	PostgreSQLに関する保守（メッセージ対応等）を行う。
189	4.5.2(5) 業務環境管理	定常	月次		すみずみ君運用	すみずみ君に関する月次時の運用（設定値見直し、ログ集計、報告等）を行う。
190	4.5.2(5) 業務環境管理	随時		4.8回/年	Teams保守作業（定期アップデート等）	Teamsのバージョンアップに伴い、プロキシサーバのホワイトリスト、Windowsファイアウォール、Applockerの見直しを行う。
191	4.5.2(5) 業務環境管理	定常	月次		可搬型照会用窓口装置の使用状況に係る統計情報の取得	運用管理端末を使用し、全TCに格納されている端末統計情報を月次で取得し、機構へ提出する。
192	4.5.2(5) 業務環境管理	随時		3回/年	電子申請義務化対応 （eGov、eltax、シャルフの定期アップデート作業）	eGov、eltax、シャルフのバージョンアップ対応。 バージョンアップによって過去に検知したファイルが更新＝ハッシュが異なり、都度検体の取得、無害判定、既知検知一覧への登録についても実施する。
193	4.5.2(5) 業務環境管理	随時		26.7回/月	INSUITEを利用したMWM運用電子化 （MWM/CDCOM工事時のINSUITE登録作業）	グループウェアシステム（INSUITE）へMWM端末情報を登録する。

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
194	4.5.2(5) 業務環境管理	定常	月次		業務支援ツール定期点検の自動化 (自動化ツールの実行)	月次で事務ファイル共有、基幹共有FSVの未許可ツールを一覧化し全国拠点へ配布。
195	4.5.2(5) 業務環境管理	定常	年次		Officeライセンスの棚卸作業等	Office棚卸対象となる装置を確認する。 手順書等を保守拠点へ展開する。 端末にOCRマスタの適用作業を行う。 作業実施報告シート（端末シリアル一覧）への結果投入と報告 営業所から回収した作業実施報告シート（端末シリアル一覧）を保守拠点総括が確認する。 SKY未登録機器の一覧化を行う。 削除対象の機器に対しOFFICEの削除を行う。 仮想デスクトップ一覧上でOFFICEの削除状態を管理できるよう、削除ステータスの追加を行う。 仮想デスクトップ一覧上でOFFICEの削除状態を管理できるよう、削除ステータスの追加を行う。
196	4.5.2(5) 業務環境管理	定常	半期		「管轄に捉われない事務処理」にかかる統合 ID申請	拠点より兼務申請情報を受領して、統合ID管理システム上で申請を行うためのファイル作成および本番環境への資材アップロードを行う。
197	4.5.2(5) 業務環境管理	定常 随時	日次		情報業務システムへの人事情報連携	情報業務システムへの人事情報連携する。
198	4.5.2(5) 業務環境管理	定常	日次		媒体書き出し申請対応	媒体書き出し申請及びクローズ処理（ファイル持出しに関する事前申請内容と実績に相違が無いことの確認及び端末運用Gの報告）を行う。
199	4.5.4(2)① ライセンス管理	定常	月次		ライセンス利用状況報告	端末運用Gへライセンス利用状況報告資料を報告する。報告内容は、22種類のPPのライセンス保有数、使用数、残数。
200	4.5.4(5)報告業務	定常	日次		端末設備運用管理センタ対応状況報告	端末運用Gへ前運用日のシステム運用状況を報告する。また、報告する資料作成を行う。ご報告内容および資料内容は、システム障害状況、システム運用作業予実。
201	4.5.4(5)報告業務	定常	月次		月次報告資料提示	端末運用Gへ月次報告資料を報告する。報告内容は、端末運用Gより受領したサービス要求作業件数、システム障害発生状況一覧。
202	4.5.4(6)⑨ 構成管理・ド キュメント管理業務	随時		38回/月	ドキュメント構成管理	ソフト保守業者や他業者からの依頼により、設計書及び手順書の払出し／払戻しの対応を実施し、設計書の構成管理を行う。
203	4.5.4(6)⑨ 構成管理・ド キュメント管理業務	随時		26回/月	プログラム構成管理	ソフト保守業者や他業者からの依頼により、プログラムファイル及び実行ファイルの払出し／払戻しの対応を実施し、プログラムの構成管理を行う。

項番	記載箇所	作業区分	サイクル	作業分類	作業項目	作業内容
1	4.5.3(5)故障対応	随時		問合せ対応	一次受付	申告を受付表に記載
2	4.5.3(5)故障対応	随時		問合せ対応	一次受付（メール）	メール申告の対応実施
3	4.5.3(5)故障対応	随時		問合せ対応	回答	対応方針に従い回答する。（調査後の架電を含む。）
4	4.5.3(5)故障対応	随時		問合せ対応	故障切り分け（社会保険オンラインシステム、ICT基盤、インハウス、経過管理システム、核装置）	一次受付分の振分け及び対応方針を決定し、対応する。
5	4.5.3(5)故障対応	随時		問合せ対応	故障切り分け（NW機器）	一次受付分の振分け及び対応方針を決定し、対応する。
6	4.5.3(5)故障対応	随時		問合せ対応	故障切り分け（TV会議システム）	一次受付分の振分け及び対応方針を決定し、対応する。回答は、FAQ・マニュアルレベルとし、回答できない内容はTV会議事業者へディスパッチする。
7	4.5.3(5)故障対応	随時		問合せ対応	故障切り分け（他システム）	保守対象外システムの問合せに関して、切り分けを行い、対象外システムであることを説明の上、適切な参照先を案内する。
8	4.5.3(5)故障対応	随時		問合せ対応	運用管理端末（ヘルプデスク）操作	故障切り分けの一環として運用管理端末（ヘルプデスク）で状況を確認する。
9	4.5.3(5)故障対応	随時		トラブル対応	報告（機構本部B）	エスカレーション基準に基づき機構に報告する。
10	4.5.3(4)関連事業者への問合せ・対応依頼	随時		トラブル対応	トラブル対応	トラブル発生時（NW機器・端末機器・センタ起因）に、トラブル統制及び他の運用チーム（センタ運営、共通基盤保守事業者等）と協力し、以下の対応を実施 ・ 運営要員（保守拠点）及び現地顧客のコントロール ・ 申告状況の管理 ・ ポータルサイト上のテロップに係る情報連携
11	4.5.3(4)関連事業者への問合せ・対応依頼	随時		トラブル対応	他の運用チームへの情報連携	エスカレーション基準に基づき情報連携する。
12	4.5.3(5)故障対応	随時		トラブル対応	NW監視アラーム検知後の復旧対応	監視にてノード停止等を検知した際に、事務所等へ架電にて問診を行い事象の回復を行う。必要に応じ、保守を手配する。
13	4.5.3(5)故障対応	随時		トラブル対応	中継サーバエラー検知	監視にて中継サーバダウン等を検知した際に、事務所等へ架電にて問診を行い原因の特定及び事象の回復を行う。必要に応じ、保守を手配する。
14	4.5.3(5)故障対応	随時		不正アクセス検知時の対応	不正端末検知対応	監視にて不正端末の接続を検知した際に、事務所等へ架電にて問診を行い原因の特定及び事象の回復を行う。
15	4.5.3(5)故障対応	随時		ウイルス検知時の対応	ウイルス検知対応	監視にてウイルスを検知した際に、事務所等へ架電にて問診を行い原因の特定及び端末のフルスキャンを行う。
16	4.5.3(5)故障対応	随時		有償修理の可能性がある申告の対応	有償修理対応	有償修理の可能性がある故障に関して顧客に案内し、運用総括へ情報連携する。
17	4.5.3(2)管理対象	随時		問合せ対応	ヘルプDB登録	問合せ及び監視で検知したエラーを用語集に従い、的確に内容を取りまとめ、ヘルプDBに登録する。
18	4.5.3(2)管理対象	随時		問合せ対応	ヘルプDB入力チェック	ヘルプDBの内容をチェックする。
19	4.5.3(6)報告	随時		問合せ対応	ヘルプデスクソリューション確認	顧客の依頼・トラブル時の対応内容の確認時に、通話内容を確認する。
20	4.5.3(4)関連事業者への問合せ・対応依頼	随時		ユーザインシデント復旧対応	パスワード初期化	アカウントのパスワード初期化対応を統合認証（AD）に依頼する。
21	4.5.3(4)関連事業者への問合せ・対応依頼	随時		ユーザインシデント復旧対応	生体認証アカウントロック解除	ロックされたアカウントの解除を統合認証（生体認証）に依頼する。

項番	記載箇所	作業区分	サイクル	作業分類	作業項目	作業内容
22	4.5.3 ヘルプデスク	随時		事務所停電情報の連携	拠点停電対応	年金事務所等から停電の情報を受領した際、停電管理簿に入力し、必要に応じて、中継サーバ運営に中継サーバのシャットダウンを依頼する。
23	4.5.3(5)故障対応	随時		保守手配	保守手配	各HWの保守手配を行う。
24	4.5.3(5)故障対応	随時		運管要員（保守拠点）作業管理	運管要員（保守拠点）入退所管理	運管要員（保守拠点）の入所から作業完了までの連絡を受け、ヘルプデスクDBに入力する。
25	4.5.3(5)故障対応	随時		故障対応付随作業	RadiusサーバへのMACアドレス登録申請、確認	MAC情報がRadiusサーバに登録されているか確認を行う。存在しない場合は、登録申請を行う。
26	4.5.3(5)故障対応	随時		故障対応付随作業	プリンタのNW設定変更確認	装置のIP設定に誤りがないか、ヘルプデスクから運管端末を用いて確認を行う。
27	4.5.3(5)故障対応	随時		故障対応付随作業	センタ確認依頼	各端末の保守で交換作業が完了した際、センタチームへ設定確認を依頼する。
28	4.5.3(5)故障対応	随時		故障対応付随作業	COMPLOCK設定依頼	COMPLOCK搭載装置の交換が発生した際、ライセンス認証に必要な情報取得をセンタ運営に依頼する。
29	4.5.3(5)故障対応	随時		故障対応付随作業	COMPLOCK代替装置インストール依頼	COMPLOCK搭載装置の交換が故障した際、現地顧客の要望を確認し、必要に応じて他の端末にインストールするようセンタ運営に依頼する。
30	4.5.3(5)故障対応	随時		故障対応付随作業	装置交換時の個別ソフトウェア再インストール依頼	装置交換時に個別ソフトウェアのインストールを拠点端末総括に依頼する。
31	4.5.3(5)故障対応	随時		故障対応付随作業	OU移動、戻し依頼	QWM、QLPCの交換作業が必要な場合依頼する。交換作業完了後に、戻し作業をセンタ運営に依頼する。
32	4.5.3(5)故障対応	随時		故障対応付随作業	NW機器交換後のNW保守への確認依頼	FSW、ASW、HUB等コンフィグが入っているNW機器の装置交換情報をNWチームに展開し、設定の正しさの確認を依頼する。
33	4.5.3(5)故障対応	随時		故障対応付随作業	端末特権ユーザパスワード払出し	現地保守作業で必要となる端末特権ユーザのパスワードをヘルプデスクで発行し、運管要員（保守拠点）へ送付する。
34	4.5.3(5)故障対応	随時		故障対応付随作業	サーバ特権ユーザパスワード払出し	現地保守作業で必要となるサーバ特権ユーザのパスワードをヘルプデスクで発行し、運管要員（保守拠点）へ送付する。
35	4.5.3(6)報告	随時		長時間故障対応管理	HKP長時間故障の状況管理	HKP長時間故障の管理を行う。 3時間超の故障に対しては、状況確認し機構に報告を行い、復旧まで情報連携を実施する。
36	4.5.3(5)故障対応	随時		運管要員（保守拠点）統制	運管要員（保守拠点）問合せ	運管要員（保守拠点）からの問合せに対して回答を行う。
37	4.5.3(2)管理対象	随時		問合せ対応（他事業者、他運用チーム向け）	事務所等への問診、調整（不正端末以外）	他事業者、他運用チームから依頼があった場合、事象確認・状況確認のため、事務所等に問診を行う。
38	4.5.3(5)故障対応	随時		作業連絡	辞書満杯発生対応	端末AP保守事業者から依頼があった場合、事務所等へ連絡し、単語一括削除の実施を案内する。（TCごと）
39	4.5.3(5)故障対応	随時		端末借用調整	個別アプリケーションインストール日程調整	インストール/アンインストール依頼を他運用チーム経由で受け、拠点職員と日程調整及び端末起動依頼を行う。
40	4.5.3(5)故障対応	随時		端末借用調整	アウトバウンド依頼	他運用チームからの依頼を受け、拠点職員に端末の借用・起動依頼を行う。
41	4.5.3(5)故障対応	随時		端末借用調整	PIO対応に伴う端末借用調整 （PIO対応：社会保険オンラインシステムを使用する装置をシステムに登録する作業）	工事調整チームからの依頼を受け、拠点職員に端末の借用・起動依頼を行う。
42	4.5.3(6)報告	随時		過去情報の問合せ対応	他事業者・他運用チームからの情報抽出依頼対応	他事業者・他運用チームからの依頼があった場合、ヘルプDBから情報を抽出する。

項番	記載箇所	作業区分	サイクル	作業分類	作業項目	作業内容
43	4.5.3(6)報告	随時		災害速報対応	自然災害発生メールの発出、管理簿更新	システム管理（受託者内のチーム）より発出された地震速報メールに対し、事務所等からの申告の有無及び震度5以上の拠点への問診結果を記載し、送付する。併せて、当該事務所等の状況を管理簿に投入し、機構へ報告する。
44	4.5.3(6)報告	定常	日次	長時間インシデント管理	オンサイト保守対応2営業日超過報告運用	エスカレーション基準に基づき、機構へ故障対応状況を報告する。
45	4.5.3(6)報告	定常	日次	長時間インシデント管理	HKP保守対応3営業日超過報告運用	HKPの故障対応において、申告から次の対応までの期間が3営業日超となったインシデントを抽出して機構に状況を報告する。
46	4.5.3(6)報告	定常	日次	進捗確認	インシデント棚卸	未解決インシデントの対応状況をディスパッチ先に確認する。
47	4.5.3(6)報告	定常	日次	電話応答状況	フリーダイヤル応答状況の確認	毎日の電話受付率のデータを収集するときのため、受託者が用意しサーバに保管する。
48	4.5.3 ヘルプデスク	定常	日次	ヘルプデスクオープン作業	ヘルプデスクオープン作業（運用管理端末の立上げ）	運要管理端末（ヘルプデスク）及びヘルプデスク端末の立上げを行う。
49	4.5.3 ヘルプデスク	定常	日次	ヘルプデスクオープン作業	ヘルプデスクオープン作業（留守番電話の解除）	留守番電話を解除し、留守番電話が入っていた場合は折り返し電話する。
50	4.5.3 ヘルプデスク	定常	日次	ヘルプデスククローズ作業	ヘルプデスククローズ作業（留守番電話の設定）	留守番電話の設定を行う。
51	4.5.3 ヘルプデスク	定常	日次	ヘルプデスククローズ作業	ヘルプデスククローズ作業（運用管理端末の電源断）	運要管理端末（ヘルプデスク）及びヘルプデスク端末の電源を落とす。
52	4.5.3(6)報告	定常	日次	日報	ヘルプデスク受付状況報告メール送付	当日の問合せ状況（受付件数、応答率、受付内容のトピック）を運用管理全体にメールで共有する。
53	4.5.3(6)報告	定常	日次	受付内容報告（日次）	受付内容報告（日次）	ヘルプデスクDBの当日受付分について、記載がわかりやすい内容が確認した上で取りまとめたファイルを機構に報告する。
54	4.5.3(6)報告	定常	週次	停電予定一覧の報告	共通運用管理事業者への停電情報連携（定例）	統合NW停電情報を編集して、当日を含む未来日のすべての事務所等の停電情報を一覧にしたPDFを、共通運用管理事業者に報告する。
55	4.5.3(6)報告	随時		事務所停電情報の連携	共通運用管理事業者への停電情報連携（休前日申告時）	定例の停電情報連携後、事務センターより当週に発生する停電情報を受け付けた場合、共通運用管理事業者に報告する。
56	4.5.3(2)管理対象	随時	月次	ヘルプデスクソリューション対応	ヘルプデスクソリューションFAQ登録・修正	ノウハウとしてヘルプデスク内部に横展開が必要なインシデントをナレッジとして登録する。
57	4.5.3 (3)問合せに対する対応の改善対応	定常	日次	ポータルサイト編集	ヘルプデスクポータルサイト（日次ポータルサイト編集）	毎朝、ヘルプデスクポータルサイトのお知らせ欄の更新を実施する。
58	4.5.3 (3)問合せに対する対応の改善対応	定常	週次	ポータルサイト編集	ヘルプデスクポータルサイト（週次ポータルサイト編集）	ヘルプデスクポータルサイトのよくあるお問い合わせTOP5の確認、修正及び掲載を行う。
59	4.5.3 (3)問合せに対する対応の改善対応	随時		ポータルサイト編集	ヘルプデスクポータルサイト（随時ポータルサイト編集）	依頼や問合せ内容の分析をもとに、ヘルプデスクポータルサイトのFAQや重要なお知らせ欄の更新を行う。
60	4.5.3 (3)問合せに対する対応の改善対応	定常	半期	ポータルサイト編集	ヘルプデスクポータルサイト（組織改編・人事異動月時のポータルサイト編集）	ヘルプデスクポータルサイトを改修（特設ページの作成、画面レイアウトの変更など）する。
61	4.5.3 (3)問合せに対する対応の改善対応	定常	半期	ポータルサイト編集	組織改編・人事異動月の対応（繁忙期の対応）	繁忙期の応答率や一次回答率など分析し改善活動を実施する。
62	4.5.3 (3)問合せに対する対応の改善対応	随時		ポータルサイト編集	ヘルプデスクポータルサイト（照会先一覧）	機構の指示によりヘルプデスクポータルサイトに掲載している照会先一覧の情報更新を行う。
63	4.5.3 ヘルプデスク	定常	月次	ヘルプデスクサーバパッチ対応	ヘルプデスク受付DB管理	ヘルプデスクのDBサーバに対して、セキュリティパッチ適用等を行う。
64	4.5.3 ヘルプデスク	随時		ヘルプデスク受付DB維持運用	ヘルプデスク受付DB（維持メンテ）	ユーザ登録/削除等のヘルプデスク受付DB上における管理作業を行う。
65	4.5.3 ヘルプデスク	随時		ヘルプデスク受付DB維持運用	ヘルプデスク受付DB（機能追加、改修）	ヘルプデスク受付DBの機能追加・画面レイアウトの改修等を行う。

項番	記載箇所	作業区分	サイクル	作業分類	作業項目	作業内容
66	4.5.3 ヘルプデスク	随時		ヘルプデスク受付DB維持運用	ヘルプデスク受付DB（情報抽出ツール）	ヘルプデスク受付DBの変更が発生した場合、抽出ツールの改修を行う。
67	4.5.3 ヘルプデスク	随時		ヘルプデスク受付DB維持運用	ヘルプデスク受付DB（装置マスタ情報更新）	装置種別の追加/削除があった場合、情報の更新を行う。
68	4.5.3 ヘルプデスク	随時		ヘルプデスク受付DB維持運用	ヘルプデスク受付DB（DB登録時のテンプレート修正）	日常的に受付ける問合せ等のDB登録時に使用するテンプレートを更新する。
69	4.5.3 ヘルプデスク	定常	月次	ヘルプデスクサーバ維持運用	ヘルプデスク受付DB（サーバ定期リポート）	毎月第2土曜の休日開所日に再起動する。
70	4.5.3 ヘルプデスク	定常	日次	ヘルプデスクサーバ維持運用	拠点情報の取り込みツール起動チェック	拠点情報取り込みツールが起動されたことを確認する。
71	4.5.3(4)関連事業者への問合せ・対応依頼	随時		拠点情報変更の連携	拠点一覧の修正依頼	顧客から住所、電話番号変更等を受領した場合、運用総括へ修正依頼を行う。
72	4.5.3 ヘルプデスク	定常	月次	ヘルプデスクサーバパッチ対応	ヘルプデスクソリューションサーバ・DBサーバ維持管理（月次作業）	ヘルプデスクのソリューションサーバ・インシデントDBサーバに対し、稼働状態及びウイルススキャンの実施状況を確認する。
73	4.5.3(4)関連事業者への問合せ・対応依頼	随時		ユーザインシデント復旧対応	情報業務パスワード初期化	アカウントのパスワード初期化対応を、情報業務システム等構築事業者に依頼する。
74	4.5.3(4)関連事業者への問合せ・対応依頼	随時		ユーザインシデント復旧対応	情報業務アカウントロック解除	ロックされたアカウントの解除を、情報業務システム等構築事業者に依頼する。

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
1	4.5.1(1)①保守機管理	定常	月次		保守機の整備	機構の各拠点に設置されている本番機台数および故障発生率、SLAを踏まえて弊社保守拠点に配備する保守機台数の充足状況を確認する。
2	4.5.1(2)②② セキュリティ パッチ・セキュリティ対策製 品の定義ファイル配布業務	定常	月次		ウィルス定義ファイル適用	以下の作業を行う。 ・保守差分資材の作成 ・保守差分資材の実機検証
3	4.5.1 (3) 故障時対応	定常	月次		有償修理対応	機構の過失による装置故障が発生した場合に機構本部、ハードウェア事業者と有償修理にかかる対応を実施する。 ・現地に保守員を手配する。 ・ハードウェア事業者到有償修理にかかる修理代金の見積を依頼する。 ・機構（端末運用G）に修理代金の見積をご提示する。 ・機構（端末運用G）より修理指示を受領する。 ・ハードウェア事業者に修理を依頼し、日程調整する。 ・機構（端末運用G）へ修理の完了報告をする。
4	4.5.2(2)②サポート期限管理	定常	月次		ソフトウェアのサポート期限の確認	機構へ納入しているソフトウェアのサポート期限超過を防止するために期限の確認を行う。
5	4.5.2(2)②サポート期限管理	随時		1回/年	サポート期限超過への対策策定・機構報告	機構へ納入しているソフトウェアのサポート期限超過が判明した場合、対策を検討し、計画を策定する。
6	4.5.2(2)②サポート期限管理	定常	月次		ソフトウェアのサポート期限の確認	機構へ納入しているソフトウェアのサポート期限超過を防止するために期限の確認を行う。
7	4.5.2(2)②サポート期限管理	随時		1回/年	サポート期限超過への対策策定・機構報告	機構へ納入しているソフトウェアのサポート期限超過が判明した場合、対策を検討し、計画を策定する。
8	4.5.2(4)③統合ネットワーク の遮断ログの確認	定常	月次		統合NW遮断ログの確認	統合NWから遮断された通信のログ（機構本部AのFW分）が、平日1日、休日1日分、毎月送付され、その通信の妥当性（意図した通信か否か）を確認する。
9	4.5.2(4)③統合ネットワーク の遮断ログの確認	定常	月次		統合NW遮断ログの確認	統合NWから遮断された通信のログ（機構本部AのFW分）が、平日1日、休日1日分、毎月送付され、その通信の妥当性（意図した通信か否か）を確認する。
10	4.5.2(4)④情報資産台帳の更 新	定常	四半期		情報資産管理台帳の更新	3ヶ月に1回、情報資産管理台帳の棚卸、及び更新作業を実施し、機構へ報告する。
11	4.5.2(4)④情報資産台帳の更 新	定常	四半期		情報資産管理台帳の更新	3ヶ月に1回、情報資産管理台帳の棚卸、及び更新作業を実施し、機構へ報告する。
12	4.5.4(1)②進捗管理	定常	月次		運用スケジュール作成（月次）	翌月の運用保守業務に関わるイベントや各種報告、運用業務の予定について一覧化した資料を作成する。また、前月の予定に対する実績を加えた資料を作成し、報告を行う。
13	4.5.4(1)②進捗管理	定常	年次		運用スケジュール作成（年次）	翌年の運用保守業務に関わるイベントや各種報告、運用業務の予定について一覧化した資料を作成し、報告を行う。
14	4.5.4(1)②進捗管理	随時		1回/日	拠点工事後のセキュリティ対策作業実施チェッ クリストの確認／報告	拠点工事にて設置されるクライアント装置に対するセキュリティ対策作業の実施状況を機構へ報告する。
15	4.5.4(1)②進捗管理	定常	週次		週次運用計画の最終確認および周知	週次運用計画を関連事業者へ通知する。
16	4.5.4(1)②進捗管理	定常	四半期		2年経過ファイル削除	2年経過ファイルの削除（対象範囲／リスト作成ツール修正・実行、集計表作成・配布）を行う。
17	4.5.4(1)②進捗管理	随時		1回/月	NW機器に対するファームウェアバージョンの 定期確認運用	NW機器のファームウェア情報を月次で各ハードウェア事業者を確認を行い、収集した情報を管理簿に投入する。
18	4.5.4(1)②進捗管理	随時		1回/日	問い合わせ対応状況確認	問い合わせ事項のクローズのために、問い合わせ対応のステータスを確認する。関連事業者の対応状況が芳しくない場合は、問い合わせの事項の再送や催促を行う。

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
19	4.5.4(1)②進捗管理(iii)	定常	月次		Symantecの定義ファイル適用管理	検疫システムにおいて、Symantecの定義ファイルが適切に更新されているか確認する。適用状態に問題がある場合は、ハードウェア事業者へ調査依頼を出し、原因究明と対処を行う。
20	4.5.4(1)②進捗管理(iii)	定常	月次		フルスキャン実施状況管理 (Symantec)	フルスキャン実施状況を整理し、機構本部へ報告資料作成／報告を行う。
21	4.5.4(1)②進捗管理4.5.4(iii)	定常	週次		TrendMicroフルスキャン実施状況の確認	週次でクライアント装置のフルスキャン状況を整理し、機構へ報告する。
22	4.5.4(2)①ライセンス管理	定常	年次		ソフトウェア棚卸	年次でSKYSEAよりソフトウェアの棚卸点検を実施する
23	4.5.4(3)①ウイルス検知時の 対応	随時		11.88件/月	マルウェア検知対応	規定のウイルス検知対応フローに従い、事象クローズまでの各対応を実施する。
24	4.5.4(3)①ウイルス検知時の 対応	随時		8回/年	ログ監査	ウイルス検知時に、システムログ管理ソフトウェアを使用したログ確認作業の指示を行う。
25	4.5.4(3)①ウイルス検知時の 対応	随時		8回/年	ファイル操作ログ監査	ウイルス検知時に、端末証跡管理・デバイス証跡管理ソフトウェアを使用したログ確認作業の指示を行う。
26	4.5.4(3)①ウイルス検知時の 対応	随時		8回/年	端末証跡ログ監査	ウイルス検知時に、端末証跡管理・デバイス証跡管理ソフトウェアを使用したログ確認作業の指示を行う。
27	4.5.4(3)①ウイルス検知時の 対応	随時		1.63回/月	ウイルス検出時の運用（WEB閲覧、メール）	過検知、誤検知時の対応を行う。 ・検知内容を確認する。 ・機構（端末運用G、情報管理対策室）に検知連絡する。 ・検体を取得する。 ・ベンダーに解析を依頼する。 ・ベンダーより解析結果を受領する。 ・機構（端末運用G、情報管理対策室）に解析結果を連絡する。 ・情報管理対策室より対処指示を受領する。 ・指示に従い対処を実施する。 ・機構（端末運用G、情報管理対策室）に対処完了の連絡をする。
28	4.5.4(3)①ウイルス検知時の 対応	随時		2.1回/月	不正侵入対策（IDS/IPS）検知対応	規定のウイルス検知対応フローに従い、事象クローズまでの各対応を実施する。
29	4.5.4(3)①ウイルス検知時の 対応	随時		13.44回/月	情報漏洩対策（DLP）検知対応	規定のウイルス検知対応フローに従い、事象クローズまでの各対応を実施する。
30	4.5.4(3)②不正アクセス検出 時の対応	随時		0.7件/月	【統合NW検知対応】 デコイ検知／FW検知対応（未知事象）	統合NWにおいて不正通信を検知した際に、検知起因事象の特定、通信の検知先／検知元を確認し、特定した通信が問題ないことを統合NW事業者 に報告する。また、統合NW事業者に対して検知除外申請も合わせて行う。
31	4.5.4(4)影響調査	随時		2回/年	機器の貸出し運用	機構および関連事業者よりソフト開発等の試験要件が発生した際に依頼元の試験要件を鑑み、貸出を行う装置を選定および貸出に関わる手続きを行 う。
32	4.5.4(4)影響調査	随時		2回/年	機器の返却運用	貸出時に設定した返却期限に基づき、貸出装置の返却手続きを行う。

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
33	4.5.4(4)影響調査	随時		4回/年	トラブル対応	トラブル発生時に問い合わせ対応や原因究明、問題解決に向けた作業整理や取り纏めを行う。 ※自責によるトラブルを除く。 <対応作業フロー> ・トラブル（監視・申告）が展開される ・アクション会議の開催 →関係者集めて状況・情報確認を行う。 ・上記の関係者がそれぞれにおいて問題がないことを確認する。 ・疑いのある箇所を確認し、対応を行う。 ・随時機構報告を行う ・故障速報発出やエスカレーションを行う ・ハード故障である場合、他事業者との連携を行う ・暫定対処が必要な場合は、暫定対処を行う ・本格対処策の「コントロール／機構窓口／記録／情報取得／解析」を行う ・影響調査対応を行う
34	4.5.4(4)影響調査	随時		446件/月	機構問い合わせ対応	機構本部担当職員（主に端末運用G、システム基盤整備Gや情報管理対策室）からの質問や要望に対する対応を行う。
35	4.5.4(4)影響調査	随時		435件/月	関連事業者（ハードウェア事業者以外）／運管事業者内の問い合わせ（調査）対応	関連事業者や運管事業者内からの質問や情報提依頼に対する調査および対応を行う。
36	4.5.4(4)影響調査	随時		168件/月	関連事業者（ハードウェア事業者）からの問い合わせ（調査）対応	ハードベンダからの作業依頼や確認事項に対する問い合わせおよび調査対応を行う。
37	4.5.4(5)報告業務	定常	月次		有償・無償保守の連絡（月次）	前月1ヶ月に東京広域事務センターで実施した有償になる可能性がある保守対応(ディスプレイやキーボードの利用者起因による破損)の一覧を作成し機構（端末運用G）に送付する。
38	4.5.4(5)報告業務	定常	月次		情報管理対策室との定例会議（月次）	情報管理対策室との月次で定例会議を行う。（資料作成含む）
39	4.5.4(5)報告業務	定常	月次		媒体書き出し結果報告	媒体書き出し結果を、機構へ報告する。
40	4.5.4(6)⑤変更管理	随時		7.57件/月	拠点情報／保守拠点情報の更新	機構の拠点名称、住所、拠点ID、事務所コード、TCID、電話番号、ビル情報（EV基数、特殊搬入条件等）を一元管理する。拠点情報に変更要素が発生した場合、これを反映修正する。また、弊社保守拠点の拠点名称、住所、保守対象拠点への駆けつけ時間、支援拠点名称を一元管理する。拠点情報に変更要素が発生した場合、これを反映修正する。
41	4.5.4(6)⑤変更管理	随時		2.6回/月	拠点情報／保守拠点情報のアップロード	変更された拠点情報および保守拠点情報を機構本部A－各保守拠点間の共有ファイルサーバへアップロードする。
42	4.5.4(6)⑤変更管理	随時		13.5回/月	個別設定情報のアップロード	変更された個別設定情報を機構本部A－各保守拠点間の共有ファイルサーバへアップロードする。
43	4.5.4(6)⑤変更管理	定常	年次		関連事業者連絡先一覧更新（定期）	変更された個別設定情報を機構本部A－各保守拠点間の共有ファイルサーバへアップロードする。
44	4.5.4(6)⑦リスク管理	定常	年次		故障演習の実施に向けた準備	疑似的な故障状況を計画し、機構から承認を得る。
45	4.5.4(6)⑦リスク管理	定常	年次		故障演習の実施および結果報告	計画した疑似故障状況を発生させ、当該故障対応における運用管理事業者の対応状況を記録、分析、評価し、運用管理業務へフィードバックを行い、機構へ報告を行う。
46	4.5.4(6)⑦リスク管理	定常	月次		ログインログ監査	ローカル管理者IDによるログインログを監査する。
47	4.5.4(6)⑦リスク管理	定常	月次		ログイン監査結果の機構報告	ローカル管理者IDによるログインログの監査結果を、機構へ報告する
48	4.5.4(6)⑦リスク管理	随時		1回/月	不審ファイル検索	NISCから提供される、以下のようなセキュリティリスクに関する調査を実施する。 ・不審なファイルの情報に該当するファイルが、端末・機構LANシステムに存在しないことを確認する

項番	要件定義書 記載箇所	作業区分	サイク ル	実績からの想 定回数等(随 時の場合)	作業項目	作業内容
49	4.5.4(6)⑪稼働状況管理	定常	月次		【故障状況報告】 月次故障報告会開催	対象月の故障発生状況について、機構へ対面で報告を行う。
50	4.5.4(6)⑫SLA管理	定常	年次		第三者によるSLA監査の実施	S L A 報告内容について、報告内容の妥当性を担保するために、第三者による監査報告を行う。
51	4.5.4(6)⑫SLA管理	定常	月次		【故障状況報告】 SLA関連事業者調整	SLA順守状況を分析及び評価を行うために、関連事業者に対して資料作成を依頼する。また、ハードウェア事業者に対して、SLA違反が発生していないことの確認を行う。
52	4.5.4(6)⑫SLA管理	定常	月次		【故障状況報告】 SLA報告資料作成	関連事業者から対象月の故障発生状況（SLA順守状況、故障発生台数、故障発生率、故障に関わる各種基準（SLA合意書に基づく）との適応状況の確認）に関する情報を収集し、故障発生状況について分析及び評価を行う。
53	4.5.5定例外作業の取扱い	随時		54件/年	影響調査／見積もり要件定義支援	機構からあった要望（新規案件）に対して「影響調査から工数合意」に至るまでの以下の作業を行う。 ・影響調査 ・要件定義支援 ・試算 ・概算見積もり ・詳細見積もり ・委員会対応支援

管理者等申請書

令和 年 月 日

日本年金機構 理事長代理人
システム運用部長 及川 無双 殿

(事業所名)

【個人情報等に関する体制】

事由	1. 設置 2. 変更	変更事由			
			役職名	氏名	連絡先
総括管理責任者					
部署管理者					
点検管理者					
個人情報等や機密情報の取扱い及び情報セキュリティ対策に関する履行状況の点検及び監査体制			別添〇のとおり		

【業務の履行体制】

事由	1. 設置 2. 変更	変更事由			
			役職名	氏名	連絡先
現場責任者					
現場責任者補助者					

体制図については別添〇のとおり

【事故発生時の緊急対応体制の届出】

別添〇のとおり

【別紙 15】

【業務の履行場所】

事由	1. 新規 2. 変更	変更の 場 合	変更前の承認年月日 令和 年 月 日		変更の事由 1. 移転 2. 増改築 3. その他 ()
作業場所			所在地	TEL (- -)	

【委託業務で取り扱う個人情報等の保管場所】

保管場所	場 所	構 造	面 積	施錠責任者名	火災等に対する設備