仕様書

１　件名

資産運用リモートセンターに関する企画業務の委託

２　委託期間

契約締結後から 2025 年 9 月 30 日まで。

３　委託業務の内容

(1) 請負部分

ア　資産運用リモートセンターの運用開始に係る運行計画の策定

イ　研修資料及びマニュアル等の作成・整備

ウ　資産運用リモートセンターのリモート面談業務に使用する設備及び電話応対システムの調達、導入支援

エ　システムの変更及び追加

オ　事務拡大に向けた検討体制の立案

(2) 準委任部分

ア　本件業務の運営場所の確保

イ　研修の開催・サポート

４　資産運用リモートセンターの運営場所

資産運用リモートセンターの運営場所においては以下記載の条件を満たすようにする。

(1) 運営場所が横浜駅半径 2㎞ 以内である。

(2) 運営場所において、150 ㎡～200 ㎡相当のオペレーター業務の専用ブースを確保できる。

(3) 休憩室を運営場所と同じ施設内に保有している。

５　履行期限等

2024 年 10 月 21 日（予定）からの資産運用リモートセンターの運用開始に当たり、下記(1)～(5)を各項目の期限までに行う。

また、運用開始後も委託期間中に当行が採用した派遣社員の教育や業務スペースの管理(清掃や備品の整備等)、リモートセンターの安定した運営の支援を行う。

なお、本委託に関しては、当該契約の運営管理及びシステムの保守等を行う専属スタッフを２名以上委託先において配置し、専属スタッフの駐在先は、株式会社ゆうちょ銀行営業部門投資信託事業部制度企画担当（以下「主管担当」という。）と調整する。

※　ゆうちょ銀行が別に契約する人材派遣契約で派遣する派遣社員 18 名、当行社員 2 名がオペレーター業務等に従事予定

＜請負部分＞

(1) 資産運用リモートセンターの運用開始に係る運行計画を 2024 年 6 月 21 日までに策定する。

(2) 研修資料及びマニュアル等の作成・整備

本件業務を行うにあたり、資産運用リモートセンターのオペレーター業務のオペレーション手順書や障害対応手順書等のゆうちょ銀行で使用するマニュアル、当該手順書等を実際に従事するオペレーター等に分かりやすく説明するための研修資料及び各種Q&A（以下「各種マニュアル等」という。）を2024年8月23日までに作成する。なお、各種マニュアル等の作成にあたっては当行の類似のマニュアル類を提示するため、それを基に主管担当と協議しながら作成する。

【各業務内容について】

投資信託の口座開設

投資信託の購入、積立

投資信託の解約

投資信託口座の住所変更、取扱店変更などの諸届

ア　研修資料については、オペレーター等の教育時に使用する資料を作成する。なお、研修資料は運行管理補助者であるスーパーバイザー用とリモート通話応対及び事務処理要員のオペレーター用の二種類を作成する。主管担当と相談の上、スーパーバイザー用は6月7日、オペレーター用は8月23日までに用意する。

なお、研修資料の様式は主管担当の審査を受けた上で決定し、内容について主管担当から開示を求められた場合、主管担当が指定する方法で開示する。

イ　各種マニュアル等に沿って業務を行うに当たり、業務の効率化、品質の向上に寄与する運用改善案は随時主管担当に提案し、主管担当が承認した場合は、各種マニュアル等の該当箇所の改版を行う。

ウ　契約締結後、更新した各種マニュアル等は毎月月次の報告と併せ、主管担当に提出する。

なお、提出方法については主管担当の指示に従う。また、期限前に主管担当から提出を求めた場合には作成中であっても同様の扱いとする。

エ　主管担当から要請があった場合は、本件業務にて使用する各種マニュアル等を電子データにてまとめ、主管担当に提出し、内容説明を行う。

(3) 資産運用リモートセンターのリモート面談業務に使用する設備及び電話応対システムの調達、導入支援

ア　受託者において、リモートセンター業務に使用する物品等を貸与又は手配する。

※　PCやヘッドセットなどのリモート業務に使用する機器及び机やロッカー等の什器類、リモートセンター業務に使用する通信設備及び回線(オペレーター15名、スーパーバイザー3名、当行社員2名を含む20名(予定)分)

※　なお、回線使用料については契約金額には含めず、別途当行が実費で支払う。

イ　必要機器及びシステム等について、次の(ｱ)(ｲ)(ｳ)の機能及び要件を満たすようにする。

(ｱ) 次の(1)(2)の要件を満たす電話受付機能を提供する。また、電話受付業務の効率化のため、次に示す機能を有するようにする。並びに電話受付システムの導入に関する構築、運用サポート及び導入後の保守対応も行う。

(1) 次の要件を満たすPBXを提供する

・ IPネットワークで接続ができる電話システム

・ IVRに自動振り分けが出来るようにする

(2) 次の要件を満たすPBXを利用するためのアプリを提供する。

基本的な機能は、次のとおりとする。

・ 閉鎖領域（VPN 接続）で利用する
・ 日本国内に保有するサーバーを利用する
・ 受信受付時に、不在席に着信しない機能
・ 管理責任者がオペレーターの電話受付の状態（待受中、応対中、後処理中、離席中等）及び経過時間を随時把握できる機能
・ 音声自動応答システム（IVR）機能
・ FAQ 管理機能

(ｲ) セキュリティ関連機能

取り扱うデータは、顧客の個人情報が含まれることから、情報の流出・改ざん防止、不正侵入の阻止等のため、受託者が準備するシステム及び機器について、次の A から E までのセキュリティ対策を行う。

A) 通信

資産運用リモートセンターの情報システムのインターネットとの接続点にはファイヤウォールを設置する。

B) 情報漏えいの防止

資産運用リモートセンターの端末にデータを蓄積しないシステム構成とし、かつフロッピーディスク、CD-R、フラッシュメモリ等のリムーバブルメディアに書き込みできないようにする。

C) ユーザー認証

端末、サーバー、通信機器等の操作においては、ID・パスワード等によるユーザー認証を行う。ユーザーの ID により、顧客データベース等の各機能の使用制限を行う。

D) サーバーの稼動管理

資産運用リモートセンターで利用するサーバーについて、稼働状況を 24 時間監視し、記録（ログ）する。正常稼働していない場合は、再起動等正常化に必要な操作を行う。

E) ウイルス等対策

資産運用リモートセンターに設置するサーバー及び端末には、ウイルス対策ソフトを導入し、その更新を行う。さらに、OS 等のセキュリティ対策プログラム（セキュリティ対策バッチ）の導入を行う。

F) データセンタ

「金融機関等コンピュータシステムの安全対策基準」(金融情報システムセンター(FISC)) に準拠している。また、契約後準拠状況を確認できる。

(ｳ) 証券会社、銀行等（金融商品取引業者、金融商品仲介業者、登録金融機関等をいう）において、仕様書内「(3) 資産運用リモートセンターのリモート面談業務に使用する設備及び電話応対システムの調達、導入支援イ」に該当する製品の導入実績を 2 社以上保有している。

ウ 受託者は、主管担当が上記システム等に格納した顧客情報について、閲覧及び編集等を行わない。

(4) システムの変更及び追加

電話受付業務の繁閑や主管担当が実施するサービス内容の改善等において、必要機器等のシステム規模拡大・内容変更を実施する。

なお、システムの変更及び追加を実施する場合は、その内容及び時期について主管担当の承認を

得る。

(5) 事務拡大に向けた検討体制の立案

主管担当の定めるところにより、2024 年 10 月 21 日(月)からの資産運用リモートセンターの運用開始後に業務拡大に向けた体制の検討や業務改善計画の立案を行う。

＜準委任部分＞

(6) 本件業務の運営場所を 2024 年 6 月 7 日までに確保する。

(7) 研修の開催・サポート

ア オペレーターへの研修計画を 2024 年 8 月 23 日までに策定の上、項番(2)で作成した各種マニュアル等を元に実施する研修をサポートする。

イ 研修会場の手配を行う。

ウ 主管担当の定めるところにより、オペレーター業務開始前に研修等をサポートする。

6 報告・納入成果物

(1) 報告

ア 本件業務のうち請負部分に係る履行完了の届出について、履行完了日の翌日から起算して３営業日（行政機関の休日に関する法律（昭和 63 年法律第 91 号）第１条第１項各号に掲げる行政機関の休日以外の日をいう。以下同じ。）までに書面をもって主管担当に報告する。

イ 当月分の本件業務のうち準委任部分に係るオペレーター業務の進捗状況等を、翌月 3 営業日までに「月次報告書」の提出をもって主管担当に報告する。

形式や記載内容については、契約締結後、主管担当と別途協議の上、決定する。

(2) 納入成果物

納入成果物	納入期限	提出先
５(1)で作成した運行計画	2024 年 6 月 21 日	主管担当
５(2)で作成した各種マニュアル等	スーパーバイザー用： 2024 年 6 月 7 日 オペレーター用： 2024 年 8 月 23 日	主管担当
５(3)に記載の必要機器、システム及び回線設備	2024 年 9 月 24 日	主管担当

※ オペレーター研修等を考慮し、前倒しでの納入が必要な場合は、主管担当と相談の上、対応する。

7 業務の再委託

本業務の再委託は禁止する。

8 その他

(1) 本件業務の遂行に当たっては、主管担当と密に連絡を取り、遺漏のないよう取り運ぶ。

なお、詳細については主管担当の定めるところによる。また、この仕様書に記載されていない事項がある場合又はこの仕様書の記載事項について疑義が生じた場合は、随時、主管担当と協議し、

解決する。この場合、受託者は当該協議に関する議事録を作成し、主管担当の確認を受ける。

(2) 受託者は、本件業務の受託にあたりサービス提供を継続するためのコンティンジェンシープランを主管担当に提出する。

なお、同コンティンジェンシープランには、緊急連絡体制が定めるようにする。

(3) 契約金額については、消費税額及び地方消費税額のほか、本件業務の遂行のために受託者側において発生する管理費、施設費、機器又は消耗品費等の一切の必要経費を含むものとする。ただし、本件業務において使用する回線の通信費は実費分を受託者にて立て替えて支払い、主管担当への毎月の請求に含めるようにする。

(4) 派遣先の管理者は主管担当にて配置するが、本件業務に関する責任者を「管理責任者」として配置する。

(5) 本件業務の履行にあたり、労働基準法等、運営要員の使用及び安全衛生に関する諸法令を遵守するものとし、運営要員の行為については、受託者が主管担当に対して、一切の義務と責任を負担する。

(6) 受託者は、契約締結後、速やかに連絡責任者（ゆうちょ銀行本社（東京都千代田区大手町 2-3-1）で協議にあたることができる責任者）を選出し、主管担当に報告する。

(7) 委託期間満了等に伴い、受託者が他の事業者に変更となる場合は、主管担当の依頼により、ゆうちょ銀行の業務に影響を与えないよう、必要な各種調整及び引き継ぎを、作業時間の範囲内（ただし、原則として夜間時間帯は除く。）で実施する。

なお、当該調整及び引継ぎの実施により受託者において追加費用が発生した場合、受託者は当該費用をゆうちょ銀行へ請求できるものとする。

９　サイバーセキュリティ

受託者は、本件業務を履行するためにシステムを利用する場合は、以下の事項について了知・厳守する。

(1) クラウドサービスのアクセス権限設定に関する仕様変更や変更時には、当行所管部あて事前に通知する。

(2) クラウドサービスのアクセス権限設定の仕様変更や変更時には、設定内容の妥当性を確認する。

(3) 端末機における漏洩防止策として、暗証番号・パスワード等は、他人に知られないように、非表示、非印字、記号などへの置換え、覗き見防止等の対策を講ずる。

また、媒体上に暗証番号・パスワード等をそのまま記憶させない等の対策を講ずる。

(4) 機密・厳秘情報をシステム内（端末やバックアップ等も含む）に蓄積する際には、ファイルの不正コピーや盗難の際にもデータの内容がわからないようにするため、CRYPTRECに準拠した暗号アルゴリズムを用いて暗号化する。

(5) システム管理端末及びユーザ端末について、電子記録媒体差込口の制御（システムによる規制、デバイス制御ソフトの導入、差込口の施錠管理）を行う。

(6) システム処理中に重要なデータを含む一時データファイルが生成される場合、重要なデータの漏洩を防止するため、利用状況に応じ不要となった時点で消去する機能を設ける。

(7) メール送付を含む機密・厳秘情報を伝送する場合には、CRYPTRECに準拠した暗号アルゴリズムを用いて暗号化（TLS1.2以上）する。

(8) 故意または過失によるファイルの破損、または不正アクセスからデータを保護するため、重要な

ファイルについては、ソフトウェアによるアクセス制御機能を設ける。

(9) ファイルに対するアクセス制御のため、ファイアウォール・統合脅威管理等でネットワークによるアクセス制御を行う。

(10) コンピュータウイルスの侵入及び不正アクセスによるプログラムの改ざんを防止する対策を講ずること。また、ウイルス対策ソフトを導入し、ウイルス対策ソフトのパターンファイルを常に最新のものにすること。また、それらパターンファイルの更新、適用状況確認を一元的に管理する機能または運用による仕組みを構築すること。

(11) コンピュータシステムの不正使用及びネットワーク拡大による種々の端末を使用した不特定多数の者からの不正アクセスを防止するため、正当な権限を保有した本人であるか、もしくは正しい端末に接続されているかなど、接続相手先の正当性を確認する。

(12) システム、データへのアクセス権を不正使用される危険性を考慮し、IDや暗証番号等の不正使用を防止するため、システムにログオンしたまま一定時間操作が行われない場合のセッションタイムアウト機能もしくは端末のスクリーンロック機能を有する。

(13) アクセス履歴を取得し監査証跡として1年間保管する。

正当なアクセス権を有する者の顧客情報の不正持ち出しを発見できるようにするため、顧客情報を閲覧した履歴（ＩＤ、日時、操作内容、件数等）を記録する。

(14) ①以下の種類のログを取得する。

・ログインとログオフ状況(指示端末、時刻、ID、回線種別、使用したシステムもしくはデータ、行った処理)

・不正なアクセス要求(指示端末、時刻、ID)

・システムによって失効とされたID

・システムにログインしたまま一定時間操作が行われないために、強制的にログオフされたID

・特権IDの利用履歴（成功時及び失敗時）

・印刷ログ

・厳秘、機密情報の取得（DL含む）及び持出した記録

②アクセス記録を定期的にチェックしてサービス利用者が正当なアクセスなのかどうかを調査する。

(15) 監査証跡に基づいて、許可されていないアクセスの分析、報告を可能とする。

(16) 監査証跡、オペレーション記録、運転記録等は、改ざん及び不正アクセスを防ぐために、正当なアクセス権限者以外のものから以下のいずれかの方法により適切に保護する。

・暗号化して保管する。

・ 書換え不能メディアに記録し、保護された場所に保管する。

・ネットワーク経由の不正アクセスや改ざんを防止するために、オフライン媒体に記録する。

(17) ①電子化された共通鍵、秘密鍵を蓄積するICカード等の機器、媒体あるいはそれに含まれるソフトウェアには、共通鍵、秘密鍵を保護する機能を具備する。

②パソコン等を利用する場合においては、共通鍵、秘密鍵は別の機器及び媒体に確保し、必要時にその機器、媒体を接続して使用する。

(18) 共通鍵、秘密鍵をパソコン等の端末機器側に蓄積する場合は、他人に解読されないような措置を講ずる。

(19) 外部ネットワークと接続する場合は、接続部分の不正侵入防止のため、入口対策を講ずる。

(20) 侵入したウイルスの検知、バックドアの構築防止、機密情報の流出防止等を目的とした出口対策（通信ログ、イベントログ等の分析による、不適切な通信の検知・遮断、DLP(Data Loss Prevention)等)を講ずる。

(21) 外部ネットワークからの不正侵入の防止と早期発見のため、内部ネットワークへのアクセスを監視し、アクセス履歴のチェックを行う。

(22) 外部ネットワークからのアクセス経路は、不正アクセスを防止するため、ファイアウォール等で不要なポートを閉塞する等必要最小限にするとともに、ネットワーク構成情報を適切に管理する。

(23) 基本ソフトウェアの脆弱性を最小限にするため、使用しない機能は停止、あるいは使用を制限する。また、使用予定のないソフトウェアは搭載しないようにする。

(24) アクセスの失敗及び不正アクセスを監視する機能を設ける。アクセスの失敗を記録する機能を設け、また、連続した何回かのアクセスの失敗に対しては、強制終了・取引禁止等を行う機能を設ける。

(25) 不正アクセスの拡大防止のための対応策、復旧策を明確にする。

(26) OS等の脆弱性及びWebアプリケーション及びスマートデバイスアプリケーションの脆弱性に関する最新情報を常に把握し、影響有無等の調査を実施し、リスクに応じて適切に対処する。

(27) パスワード等については、以下の通り推測されにくいものを設定するようシステム的に制御する。

ア　英大文字／英小文字／数字／記号のうち最低3つを組み合わせる

イ　8桁以上とする

(28) 初期設定されるパスワード等については、システム的に初回ログイン時のパスワード変更を強制する。

(29) データファイルのバックアップを取得し、その保管管理方法を明確にする。

(30) 業務継続上重要なデータについては、定期的なバックアップを実施し、本番環境から切り離した環境に保管する等ランサムウェア感染を考慮したバックアップを実施する。

(31) 端末へのアプリケーションのインストール制限を行うツール等を活用し、端末への未許可のアプリケーションのインストールを制限する。

(32) 本システムで使用する機器等において、使用しない機能(カメラ、マイク、NFC/Felica、Bluetooth、テザリング)は停止、もしくは使用を制限するとともに、使用しないソフトウェアを搭載しないようにする。

(33) システム管理端末及びユーザ端末について、業務目的以外の電子メールの送受信、ホームページの閲覧等に対処するため、当該機能をシステム的に利用不可とする、またはホワイトリストで制限する等の不正使用防止対策を講ずる。

(34) 社外からのメールが受信できる端末を使用する場合は、以下の内容を遵守する。

① 通信を監視し、不審なメール等を検知・遮断する機能を整備する。なお、当該内容については、当行（主管担当）の承認を得る

② 侵入されることを前提とした被害発生時の対処フローを整備し、当行（主管担当）の承認を得る

③ 電子メールの運用にあたっては、信頼性、安全性を確保するため、その運用方針を明確にする

④ 業務目的以外の電子メールの送受信、ホームページの閲覧等に対処するため、不正使用防止対策が講じられている

(35) インターネットに接続するシステムを使用する場合は、以下の内容を遵守するようにする。

① 通信を監視し、不審な通信を検知・遮断する機器等を整備する。

なお、当該内容については、当行（主管担当）の承認を得る

② 不正アクセス等を検知、監視する体制及び被害発生時の対処フローを整備し、当行（主管担当）の承認を得る

③ クラウドサービス契約のように他社とリソースを共有する場合、他社のシステムへのサイバー攻撃が、当該システムに与えるリスクを明確にし、当行（主管担当）の承認を得る

④ 不正アクセスによるコンピュータシステムへの侵入を防ぐため、外部からアクセス可能な通信経路、通信関連機器等は最小限とし、ネットワーク構成情報を適切に管理しているか。

また、外部ネットワークからアクセス可能な機器へのセキュリティパッチの適用やファイアウォールにおける不要なポートの閉塞等の対応を実施し、感染を防止する。

(36) 本契約の履行に従事する貴社労働者に対する作業指示、労務管理、安全衛生管理等に関する指揮命令は、すべて受託者の責任においておこなう。また本契約の履行に従事する貴社労働者に対する作業指示は、作業責任者を配置し、作業責任者を通じて行う。

(37) クラウド利用に当たっては、以下の内容を遵守する。

① 取扱者を限定するようにする。権限のない者が情報を閲覧等できないようにする。

② クラウド環境の暗号化の強度を十分に行い、暗号化漏れがないようにする。

③ 不正行為が発生し得る操作については、ログが取得されるようにする。不正行為が発覚した場合等は、速やかに主管担当まで連絡し、ログを開示する。なお、ログについては保存期間が十分であるようにする。

④ 取扱者を限定する。権限のない者が情報を閲覧等できないようにする。保存期間が十分である。

⑤アクセス権限設定に関する仕様変更について事前に入手する方法を合意している。

⑥クラウドサービス事業者によるアクセス権限設定の仕様変更や金融機関等による設定の変更時には、設定内容の妥当性を確認する旨を、クラウドサービス事業者あるいはシステム保守の外部委託先と合意する。

(38) ファイアウォールについて、設定値の変更を行う際は、適切性について十分なレビューを実施し、さらにその設定値が正しく反映されていることを定期的に確認することで、セキュリティ評価を行うこと。