仕様書

１　件名

生成AIの活用に向けた社員育成等の実施

Implementation of employee training for utilization of generative AI.

２　委託概要

生成AIによる作業効率化の可否の検証及び生成AIを活用できる人材育成のための支援。

３　委託業務の履行期間等

(1)　履行期間

契約締結日から2025年３月31日

(2)　履行場所

作業場所は作業内容及び作業体制等を考慮し、事務統括部総括担当（以下「主管担当」という。）と協議の上、決定する。

４　実施体制

受託者は、契約後において速やかに体制図を提出し、主管担当の承認を得ること。

なお、履行期間中、主要メンバーは原則変更せずに対応すること。

また、作業実施にあたっては、以下の条件を満たす者をアサインすること。

・生成AIに関するプロジェクト経験年数（AIに関するプロジェクト経験年数を含む）が５年以上ある

・金融機関向けに生成AIに関するプロダクト開発の実績がある

・生成AIに関する研修講師の実績が過去２年で10件以上ある

・主管担当の事務室に常駐し、「５　委託業務の範囲」の業務を行える

５　委託業務の範囲

(1)　生成AI活用の可否の検証

現在検討中の以下のテーマ候補について、生成AI技術（LLMやRAG等）を用いて技術検証を実施すること。また、効果検証の際は、後記「効果測定」の観点で検証を行う。

なお、生成AIの活用を検証する業務の対象（テーマ）は、契約締結後に主管担当と調整すること。

・省庁のＨＰから、銀行の手続きに関連する法令改正を抽出し、弊行のマニュアルへの反映・ＦＡＱの作成等を行う

・業務フローやサービスの見直し時に、法令の観点で問題がないか事前確認を行う
・各種施策の説明や報告等に係る資料の作成　など

(2)　生成AIを活用できる人材育成

ア　目標（ゴール）
イ　人材育成観点
ウ　人材育成の進め方及びスケジュール
を含めた人材育成計画書を作成すること。
また、後記(3)「効果測定」の観点で検証を行う。
なお、人材育成計画書の内容は、契約締結後に主管担当と調整すること。

(3)　効果測定

【生成AI活用可否の検討】

当行と受託者が取り決めたテーマ群について、生成AIの活用範囲を明確化するための検証を実施。

【生成AIを活用できる人材の育成】

当行の受講生がプロンプトエンジニアリングの習得及び自発的に生成AIを用いた業務効率化に繋がるテーマを発見し、実現する能力が身についているかの検証を実施。

(4)　結果報告

前記(1)～(3)の実施結果を「検証結果報告書」として主管担当へ報告する。
なお、「検証結果報告書」には以下を含むこととする。

・検証範囲（スコープ）
・検証目的（ゴール）
・検証アプローチ
・検証スケジュールとタスク
・検証結果
・検証課題と対応策（ゴールと検証結果との差異と対応方法）
・実装時の想定効果

(5)　その他

ア　生成AIの条件

当行が指定する業務に適切に対応できるAIを使用すること

イ　生成AIの制限事項

生成AIに対するプロンプト・回答の保存及び本件対応で当行が提示したデータをもとに生成AIが学習しないよう機能を制限すること

ウ　本件構築環境（検証環境）へのアクセス制限
受託者からのみアクセス可能な閉域環境とすること

エ　事前準備
検証において必要な物品等（ＰＣ、インターネット環境、生成ＡＩ等）の準備は受託者において行うこと
※　なお、主管担当において場所、机、椅子、電源は用意。

６　作業方法

受託者は、主管部と密接に連絡を取り合いながら、共同して作業を進めることとし、各作業の実施にあたっての具体的な連絡プロセス（作業指示、作業着手承認、作業完了確認の方法等）や連絡窓口については、受託者と主管部協議の上、別途定めることとする。

業務従事者に対する作業の指示、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行うこと。

７　提出物及び報告物等

(1)　本件業務の提出物と提出期限

人材育成計画書、検証結果報告書を作成し、主管担当へ提出すること。

提出物	提出方法	提出期限
人材育成計画書	電子データのみ	契約締結後速やかに
検証結果報告書	電子データのみ	2025年３月31日

※　電子データの提供形態については別途主管担当と協議するものとするが、原則、Microsoft 社製の Word2016、Excel2016、PowerPoint2016 のいずれか、もしくは互換性のあるものにより作成すること。

※　提出物の具体的な内容及び構成については、別途主管担当と協議の上、決定するものとする。

(2)　本件業務の実績報告時の報告物

「６　委託業務の範囲」に示す本件委託業務に該当する作業について、毎月1日から末日を作業期間とし、各期間の作業実績の報告を、作業報告書（完了届等（作業対象期間、作業内容、作業工数、作業結果等））として、作業完了報告期限までに行うものとする。

作業期間　　毎月1日から末日
作業完了報告期限　　対象作業期間の翌月15日

８　提出場所

提出物・報告物等は、主管担当の指定した場所に提出すること。

９　セキュリティ

受託者は、以下のセキュリティ要件を満たすシステムを提供すること。

・ 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、主管担当あて事前に通知すること。
・ 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こと。

  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対策を講ずること。
・ 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）を行うこと。
・ 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こと。
・ 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こと。
・ 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こと。
・ インターネットを含むオープンネットワークを介してデータを伝送する場合は、伝送途中におけるデータ改ざんを検知するための対策を講じること。
・ 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、正当権限を有した本人であるか、正しい端末に接続されているか等、接続相手先の正当性を確認すること。
・ 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、アカウントロック機能、並びに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こと。
・ アクセス履歴を取得し監査証跡として1年間※保管すること。

  ※　利用するクラウドサービス等においてアクセス履歴の保管期間が1年未満の場合は、当該保管期間とすることも可。
・ 正当なアクセス権を有する者の情報の不正持ち出しを発見できるようにするため、情報を閲覧した履歴（ID、日時、操作内容、件数等）を記録すること。
・ 以下の種類のログを取得すること。

  ✓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

- 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こと。
- 監査証跡に基づいて、許可されていないアクセスの分析、報告を可能とすること。
- 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こと。
  ✓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。
- 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、入口対策を講ずること。
- 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)を講ずること。
- 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こと。
- 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。
- 無線LANに以下のセキュリティ機能を実装・設定すること。
  ✓有線接続は必要最小限にし、業務に必要な端末のみ接続すること。
  ✓アクセスポイント（ルータ）へ接続する際にはパスワードの入力を必須とし、当該パスワードは推測されにくい、かつ十分な文字数に設定すること。
  ✓管理用パスワードは必ず十分な強度のものに設定すること。また、管理者IDをデフォルト値から変更すること。
  ✓業務上の利用者以外にアクセスされないよう、「SSIDステルス機能を有効」、

または「ANY接続を許可しない設定」等の対策を講じること。
✓ファームウェアのバージョンアップ時には、すみやかに最新化すること。
✓バージョンアップやサポートがされなくなる期間を過ぎた機器は利用しないこと。
✓CRYPTRECに準拠した暗号化アルゴリズムを使用した、強度の高い暗号方式を用いること。
✓プライバシーセパレータ機能を有し、ウイルス感染拡大防止を講ずること。

- 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こと。
- 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こと。また、使用予定のないソフトウェアは搭載しないこと。
- 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こと。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こと。
- 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こと。
- 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。
- 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こと。
- 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こと。
  ア　英大文字／英小文字／数字／記号のうち最低3つを組み合わせること
  イ　8桁以上とすること
- 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こと。
- 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こと。

１０　その他

(1) 疑義及び詳細については、主管担当（TEL:03-3477-1741）の指示によること。

(2) 交付した帳票、資料等は、作業終了後速やかに主管担当まで返還すること。

(3) 個人情報データの取扱については、契約書別紙2「情報保護・管理要領」に従うこと。

(4) 受託者は、本契約を遂行するに当たって、使用人等の不当な行為によって当行に損害を与えた場合は、その責めを負うものとする。

(5) 業務従事者に対する作業の指示、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行うものとする。