マーケティングの高度化にむけた分析と施策管理に関わるツール等の更改

適　合　証　明　書

下記の「受託者の条件」各項について、以下のとおり適合することを証明いたします。

日　　付：　　年　　月　　日
住　　所：
会 社 名：
代表者氏名：
社 員 数：（　　）人

Ⅰ　業務内容

項	受託者の条件	合否	合否判定の根拠となる事由
1	直近 2 年間における通期の決算値について、営業利益が赤字又は債務超過になっておらず、また、資本金が 1 億円以上であること。		財務状況（資本金・売上高・債務超過履歴・B/S・P/L）が確認できる資料を添付。
2	受託者は国内銀行における類似のマーケティングツール導入または更改に係るプロジェクトに（1 次請負業者として）携わり、かつ当該プロジェクトを完遂した実績を有すること。		プロジェクト規模、プロジェクト実施時期（期間）および提供先（個別企業名は伏せてもかまわないが規模、業態等、所在地域を記載）などが確認できる資料を添付。
3	以下に提示する資格・認証を取得していること。 ・ISO/IEC 9001（登録活動範囲が情報処理に関連するものに限る） ・プライバシーマーク又は ISMS ・ISO/IEC 27001		各種資格・認証を取得していることが確認できる資料を添付。
4	社内で情報（取引先情報を含む）管理に関するルールが定められ、社員に対する指導も十分に行われていること。その上で仕様書において当行が提示する機密保持項目を遵守すること。		委託先における情報管理に関する規定（社員に対する守秘義務、規定違反者の懲戒処分を含む）及び管理体制について、確認できる資料を添付。
5	業務遂行のためのルールが書面で明確化されており、かつその内容はリスク管理上十分となっていること。また、その必要に応じて見直しがなされていること。		業務遂行マニュアルを添付
6	業務遂行のためのルールが業務処理担当者に徹底される体制となっていること。また、その徹底状況が十分なこと。		社内教育体制、研修の実施状況等がわかる書類を添付
7	ゆうちょ銀行案件において、過去 2 年間に入札参加停止処分を受けていないこと。		入札参加停止がないことを証明する書類を提出すること（書式適宜）。

Ⅱ　個人データの取扱いの全部又は一部を委託する場合

項	受　託　者　の　条　件		合・否
1	セキュリティ管理を適切に行うため、委託業務を行う要員に対し、委託業務の内容や作業の範囲に応じて、セキュリティポリシーをはじめとした各種ルールの遵守を義務づけ、その遵守状況を確認するルールを整備しているか。		
2	セキュリティ管理状況及び、委託した業務が適切に遂行されているかを確認するため、委託業務の内容または作業の範囲に応じて、委託契約に基づき遂行状況を確認できる委託業務の管理体制を整備しているか。		
3	個人データの安全管理に係る基本方針を策定し、以下の事項を定めているか。 （１）事業者の名称 （２）安全管理措置に関する質問及び苦情処理の窓口 （３）個人データの安全管理に関する宣言 （４）基本方針の継続的改善の宣言 （５）関係法令遵守の宣言		
4	①	システムの安全対策を適切に実施するために、組織体制、関係者の役割及び管理すべき事項を明確にした規程類（セキュリティポリシー等）を策定し、適宜見直しているか。 ※ セキュリティポリシーには、個人情報の取扱い及びその法令遵守に関する内容が盛り込まれていること	
	②	個人データの安全管理における以下の各管理段階に係る取扱規程を定めているか。 （１）取得・入力段階 （２）利用・加工段階 （３）保管・保存段階 （４）移送・送信段階 （５）消去・破棄段階 （６）漏えい事案等への対応の段階 ※ 記憶装置等の故障等により、機器・部品を交換する場合、データ消去も含めた十分な管理を行うこと。	
	③	個人データの取扱状況の点検及び監査に関する規定が整備されているか。	
	④	（受託業務を再委託する場合）受託業務に係る再委託に係る規程が整備されているか。	
5	①	セキュリティ管理を適切に行うため、セキュリティ管理の責任者等を定め、その職務範囲と権限及び責任について定めているか。	
	②	データの安全かつ円滑な運用と不正防止のため、データ管理手順を定め、管理体制を整備しているか。 また、データ保管場所の固有のリスク（データ保管場所が海外の場合、適用される法令等）を考慮し、データ管理を行っているか。	
6	①	個人データの安全管理に係る業務遂行の総責任者である個人データ管理責任者を設置しているか。	
	②	個人データを取扱う各部署における個人データ管理者を設置しているか。	
	③	個人データ管理責任者は、次に掲げる業務を行っているか。 （１）個人データの安全管理に関する規程及び再委託先の選定基準の承認及び周知 （２）個人データ管理者及び「本人確認に関する情報」の管理者の任命 （３）個人データ管理者からの報告徴収及び助言・指導 （４）個人データの安全管理に関する教育・研修の企画 （５）その他個人情報取扱事業者全体における個人データの安全管理に関すること	

項	受　託　者　の　条　件		合・否
	④	委託業務を所管する部署の個人データ管理者は、次に掲げる業務を行っているか。 （１）個人データの取扱者の指定及び変更等の管理 （２）個人データの利用申請の承認及び記録簿の管理 （３）個人データを取り扱う保管媒体の設置場所の指定及び変更等 （４）個人データの管理区分及び権限についての設定及び変更の管理 （５）個人データの取扱状況の把握 （６）再委託先における個人データの取扱状況等の監督 （７）個人データの安全管理に関する教育・研修の実施 （８）個人データ管理責任者に対する報告 （９）適用される国内外の法令等の遵守 （10）その他所管部署における個人データの安全管理に関すること	
7	①	個人データの安全管理に係る取扱規程に従った体制を整備し、運用を行っているか。	
	②	取扱規程に規定する事項の遵守状況の記録及び確認を行っているか。	
8	次に掲げる事項を含む台帳を整備しているか。 （１）取得項目 （２）利用目的 （３）保管場所・保管方法・保管期限 （４）管理部署 （５）アクセス制限の状況		
9	①	個人データを取扱う部署が自ら行う点検体制を整備し、点検を実施しているか。 （１）個人データ取扱部署の点検責任者・点検担当者の選任 （２）点検計画の策定による体制整備 （３）定期的及び臨時の点検の実施 （４）点検の実施後において、規程違反事項等を把握したときは、その改善	
	②	当該部署以外の者による監査体制を整備し、監査を実施しているか。 （１）個人データ取扱部署以外からの監査責任者・監査担当者の選任 （２）監査計画の策定による監査体制整備 （３）定期的及び臨時の監査の実施 （４）監査の実施後において、規程違反事項等を把握したときは、その改善	
10	①	漏えい事案等に対応する次に掲げる体制を整備しているか。 （１）対応部署 （２）漏えい事案等の影響・原因等に関する調整体制 （３）再発防止策・事後対策の検討体制 （４）自社内外への報告体制	
	②	委託業務に係る漏えい事案等発生時に、委託元に対する速やかな報告を実施する体制を整備しているか。	
	③	使用するハードウェア及びソフトウェアについて、適切に管理・使用するための管理方法を明確にし、その内容を、テレワーク勤務者に周知徹底しているか。 （１）テレワークに使用する端末は、会社が許可したものに限ること （２）テレワーク端末を家族と共用しないこと （３）不特定多数の部外者が使用する端末をテレワークに使用しないこと （４）テレワーク端末は、適切に管理し、盗難・紛失防止に努めること （５）テレワーク端末で業務上利用可能と定められたアプリケーション、クラウドサービス等のみを業務に使用すること （６）テレワーク端末へのインストールが許可されたアプリケーションについて、	

項	受　託　者　の　条　件		合・否
		定められた場所（公式アプリケーションストア、アプリケーション提供企業の公式ホームページ等）からのみインストールすること	
11	①	従業者との間で採用時等に個人データの非開示契約等を締結しているか	
	②	従業者との個人データの非開示契約等の締結に際しては、以下の措置を講じているか （１） 当該従業者との、業務上知り得た秘密に関する守秘義務を含む非開示契約の締結 （２） 非開示契約等の締結における非開示契約等の十分な説明、非開示契約等の書面を管理・保管する部署の明確化 （３）派遣社員を従事させる場合の、派遣社員本人との契約・覚書・念書等（電子的手段を含む）による守秘義務の規定 （４）従業者でなくなった後における非開示義務の遵守に関する非開示契約での規定。非開示義務に反した場合の責任の規定	
	③	就業規則等に、次に掲げる事項を定めているか （１）個人データの取扱に関する従業者の役割・責任 （２）非開示契約違反時の懲戒処分	
12	従業者の役割・責任等の明確化のため、次に掲げる措置を講じているか （１）各管理段階における個人データの取扱いに関する従業者の役割・責任の明確化 （２）個人データの管理区分及びアクセス権限の設定 （３）必要に応じた規程等の見直し		
13	①	従業者へ次に掲げる措置を講じているか。 （１）従業者に対する採用時の教育及び定期的な教育・訓練 （２）個人データ管理責任者及び個人データ管理者に対する教育・訓練 （３）個人データの安全管理に係る就業規則等に違反した場合の懲戒処分の周知 （４）従業者に対する教育・訓練の評価及び定期的な見直し	
	②	従業者に対する教育・訓練の評価および定期的な見直しに当たって以下の事項に留意しているか。 （１）教育・研修担当部署の明確化 （２）教育・研修を計画的に実施できる体制の整備 （３）教育・研修の計画的な実施、実施状況の確認、新入社員や中途採用者が確実に教育・研修を受けられる体制の整備 （４）教育・研修が関連法令、自主ルールおよび内部規程等を従業者に対し周知徹底できる内容であること	
14	個人データの利用者の識別・認証に関し、次に掲げる措置を講じているか。また、個人情報を取り扱う情報システムを利用する場合は、ユーザーＩＤ、パスワード、磁気・ＩＣカード等により、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する仕組みとなっているか。その他、 サービスの内容及びリスク特性に応じて、多要素認証や多段階認証を検討しているか。 （１）本人確認機能の整備 （２）本人確認に関する情報の不正使用防止機能の整備 （３）本人確認に関する情報が他人に知らされないための対策 （４）本人確認要素(パスワード、トークンやIDカードなど認証機器、指紋などの身体情報など)の配布時の適切な本人確認および、安全な経路での配布 （５）本人確認要素の紛失時や流出時の即時利用権限停止		

項	受　託　者　の　条　件	合・否
15	個人データの管理に関し、次に掲げる措置を講じているか。 （１）従業者の役割・責任に応じた管理区分及びアクセス権限の設定 （２）アクセス権限所有者を特定し、漏えい等の発生に備えアクセスした者の範囲が把握できるような対応の実施 （３）事業者内部における権限外者に対するアクセス制御 （４）外部からの不正アクセスの防止措置 （５）アクセス可能な通信経路の限定 （６）外部ネットワークからの不正侵入防止機能の整備 （７）インターネットと接続する場合はファイアウォール等を設置し外部からの個人データへの不正アクセスから保護する措置をとること （８）不正アクセスの監視機能の整備 （９）ファイアーウォールにて不要なポートへの通信を閉塞すること	
16	個人データへのアクセス制限に関し、次に掲げる措置を講じているか。 （１）従業者に対する個人データへのアクセス権限の適切な付与及び見直し （２）アクセス権限の付与方法の明定（アクセス権限の承認者及び認定作業者の明確化） （３）アクセス権限の付与方法の明定（管理簿等によるアクセス権限の登録、変更、抹消記録の管理） （４）アクセス権限の付与方法の明定（担当者の役割に応じたアクセス権限が適切に付与されているかの定期的な見直し） （５）個人データへのアクセス権限を付与する従業者数を必要最小限に限定すること （６）従業者に付与するアクセス権限を最小限に限定すること （７）導入するパッケージソフト、アプリケーションソフト等について、納入前に既に登録されているアクセス権限を抹消すること （８）アクセス権限を抹消できない場合は、当該アクセス権が設定されているIDを、管理台帳等を用いて管理し、管理者による適切な管理を実施すること （９）（特権ＩＤを設定する場合） 従業者を限定し特別に留意すること 外部からアクセス可能な場合、限られた環境からのみアクセス可能とする等、対策を講じていること（デバイス認証やアクセス経路の限定等）	
17	①　個人データの漏えい、き損等防止に関し、次に掲げる措置により個人データの保護策を講じているか。 （１）ファイルの不正コピーや盗難の際にも個人データの内容が分からないようにするための蓄積データの漏えい防止措置 （２）データ伝送時に盗聴された場合にもデータの内容が分からないようにするための伝送データ漏えい防止策 （３）コンピュータウイルス等不正プログラムへの防御対策 （４）ウイルス対策ソフトウェアの導入、適用状況を一元的に管理する仕組みの構築 （５）ウイルス等の不正プログラムの検知対策 （６）ウイルス対策ソフトウェアのパターンファイル、検知ロジックを最新化する仕組みの構築 （７）ウイルス対策ソフトウェアのパターンファイル、検知ロジックが最新化されていることの定期的な確認 （８）上記（６）（７）を一元的に管理する仕組みの構築 上記（１）、（２）について、暗号化の仕様（暗号化対象項目、暗号化方式、暗号鍵の管理態勢等）を把握し、個人データの暗号化もれが無いようにすること。 なお、次に掲げる顧客の重要情報の暗号鍵は、ゆうちょ銀行が管理できるようにすること。	

項	受　託　者　の　条　件		合・否
		ア　暗証番号 イ　認証情報 ウ　クレジットカード情報（クレジットカード番号、セキュリティコード、暗証番号、有効期限） エ　生体認証情報 オ　その他（本籍地等センシティブ情報）	
	②	次に掲げる措置により障害発生時の技術的対応・復旧手続の整備の措置を講じているか。 （１）不正アクセスの発生に備えた対応・復旧手続の整備 （２）コンピュータウイルス等不正プログラムによる被害時の対策 （３）リカバリ機能の整備	
	③	テレワークを実施する場合は、テレワーク端末へのデータ保存・保管において、データの保護対策を講じているか	
18	個人データへのアクセスを記録するとともに、当該記録の分析・保存を行っているか。 （１）ネットワークによるアクセス制御機能の整備 （２）アクセス制御機能の有効性の検証 （３）個人データへのアクセス及び個人データの取扱う情報システムの稼動状況についての記録・分析（例：ログインとログオフの状況、不正なアクセス要求、システムによって失効とされたIDなど） （４）取得した記録についての漏えい防止等の観点からの適正な完全管理措置の実施 （５）取得した記録についての、特に漏えいリスクの高い時間帯（例：休日や深夜時間帯等）におけるアクセス頻度の高いケースについての定期的な分析の実施		
19	個人データを取扱う情報システムの稼動状況を記録するとともに、当該記録の分析・保存を行っているか。 ※ログ（システムログ、業務ログ、操作ログ等）の取得範囲・取得頻度・保存期間について、ゆうちょ銀行と予め確認、合意しておくこと。		
20	①	個人データを取り扱う情報システムの利用状況及び個人データへのアクセス状況を監視しているか。 また、サイバー攻撃に対するリスクの洗い出しと影響度の評価を行うための対応を考慮しているか。（TLPT の実施等）	
	②	上記①の監視状況についての点検及び監査を行っているか。	
	③	セキュリティパッチの適用や情報システム固有の脆弱性の発見・その修正等、ソフトウェアに関する脆弱性対策を行っているか。	

（注１）「合・否」判定にあたっては、「〇」又は「×」を記入し、該当しない場合には「－」を記入してください。また、現在未措置でも、履行を開始するまでに措置する場合には、「実施予定日」を記載してください。

（注２）証明書類の添付を必要とする場合は、「合・否」欄に添付書類名を記述してください。

（注３）受託者には責任者等の管理体制、個人情報の管理状況について、必要に応じて書面で提出をしていただく場合があります。

（注４）提出した内容に虚偽があることが判明した場合又は報告について、書類の提出を当社から求められたにもかかわらず提出がなされない場合には、契約条項に違反したものとみなし契約の解除を行います。

（注５）本件に係る諸経費は提出者の負担とします。

（注６）実施予定日を資料に書く場合、例えば、委託業務の実施が数か月以上先の場合等、中長期の準備が許される場合は、予定日ではなく、予定月でも構いません。

（注７）例等として挙げているのは、受託者において証明内容を捉えやすいよう当行が想定している一般的な例を示しているものであり、これに限定する意図ではありません。

（注８）当証明書における用語の定義は以下のとおりとします。

用語	定義
サイバー攻撃	システムやネットワークへの不正侵入等を行い、情報の改ざん・破壊・窃取、サービスの安定稼働を妨害する等を行うこと。
サイバーセキュリティ	サイバー攻撃等からシステムやネットワークの安全を確保すること。
標的型攻撃メール	特定の組織や個人を狙い、情報の詐取等を目的に攻撃者が送信する電子メール。受信者が添付ファイルを開封、または電子メールの中に書かれたURLを受信者がクリックすることによりウイルスがダウンロードされることで攻撃が開始される。
脆弱性	サーバ等のハードウェアの設定やアプリケーション、OS等のソフトウェアのセキュリティ上の不備・欠陥のことであり、情報の改ざん・破壊・窃取、システムの破壊等を行う攻撃に悪用される。