Preserve Kyoto(海外からの寄付受入れの取組)に係る寄付金取扱業務
詳細仕様書

1　概要

⑴　業務名

Preserve Kyoto(海外からの寄付受入れの取組)に係る寄付金取扱業務

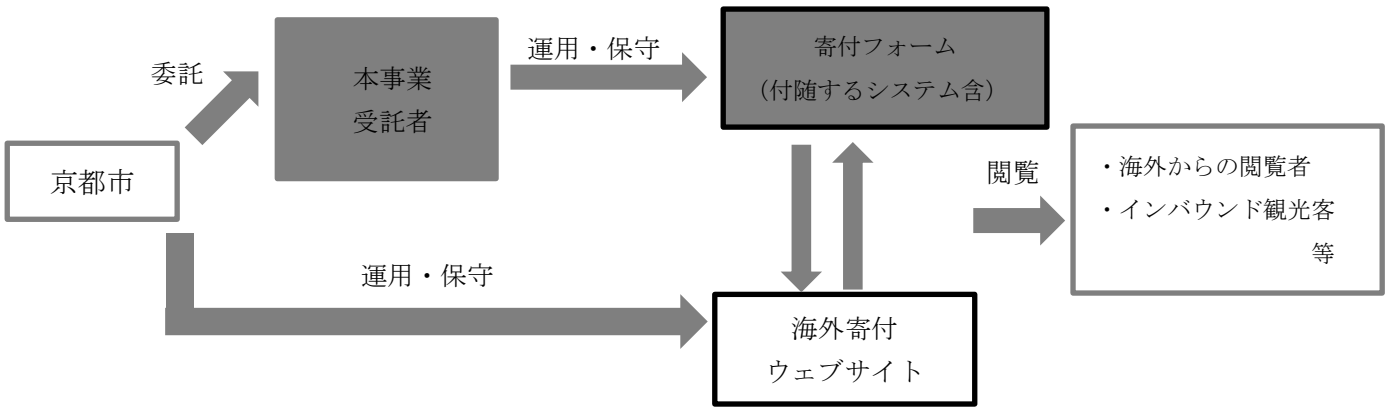
⑵　業務の概要

Preserve Kyoto(海外からの寄付受入れの取組)に係る寄付金取扱に係る以下の業務を行うこと。

なお、寄付フォームを運営するためのシステムを本市が利用するにあたり必要となる回線及び端末については、提案の範囲に含めない。

⑶　業務の範囲

下図に示すとおり、本委託業務は、寄付フォームの提供及び運用・保守（色掛け部分)、寄付金の受付及び収納代行、寄付金の納付を業務範囲とする。



⑷　委託内容と納入成果物

(ｱ) 寄付金の受付及び収納代行、寄付金の納付について

- 本業務の受託者は、地方自治法第 231 条の 2 の 3 第 1 項の政令で定める指定納付受託者の要件を満たす者、または、本市からすでに指定納付受託者と認められている者と協働して寄付金の受付及び収納代行を行うことができる者であること。
- 使用できるクレジットカードのブランドはＶＩＳＡ、ＭａｓｔｅｒＣａｒｄ、AMEX、ＪＣＢを必須とする。なお、寄付金の代理受納を行う者が加盟又は提供する国際ブランドマークが付された寄付金の代理受納を行う者以外の者が発行するクレジットカードの取り扱いも可能であること。
- 取り扱う支払い回数は一括払いの他、分割払いが可能となるよう努力すること
- 受付サイトで受け付けた寄付金を本市に代わって収納し、本市に払い込む業務については、支払い方法の種類等を問わず毎月一定日を締切日とし、締切日後 1 箇月以内に、あらかじめ本市が指定する口座へ一括で振り込むこと。（入金日が、金融機関休業日の場合については、別途協議を行う。）
- クレジットカード納付による立替金を振り込む際の手数料は寄付金の代理受納を行う者の負担とする。

・　寄付金の代理受納を行う者は、代理納付に関する金銭をその他の金銭と区別して管理し、その保全のために必要な措置を講じること。

(ｲ) 寄付フォームの提供

本市のウェブサイト「Preserve Kyoto」から主に外部リンクとして通信を行うための寄付フォームの提供をすること。

(ｳ) 寄付者情報の提供

・　寄付フォームサイト上または付随するシステムで、本市が寄付金の受け入れ状況を随時確認できるようにすること。

・　寄付申込時に取得する個人情報等は次のものを想定する。

氏名、企業名、性別、生年月日、郵便番号、住所、電話番号、メールアドレス、寄付金額、決済方法、寄付目的、寄付事実の公表の可否、コメント、メンバーシップ登録の可否

・　上記寄付者情報をCSV形式などでダウンロードできるようにすること

・　取得する個人情報の内容は今後事業の展開に合わせて随時追加変更できるよう努力すること。

(ｴ) コンテンツの登録・公開

・　職員が容易にコンテンツを管理、更新するために必要な環境を整備すること。

(ｵ) 寄付金収納に係る本市等との連絡調整

・　受託者の運営するファンドレイジングの利用規約、利用条件を明示し、説明すること。

・　本事業の実施体制について明示すること。

(ｶ) その他

・　本業務を開始するに当たっては、本市と事前に十分な調整を行うこと。

・　受託者は、履行期限内に円滑に事務が進められるよう、十分な体制で臨むこと。年度途中で体制の強化が必要であれば、適宜、人員の補充等を行うこと。また、計画的な事務の推進のため、工程表を作成し、本市の確認を受けること。

・　受託者は、本業務の実施のために制作した著作物について、委託期間終了後、本市に全ての著作権（著作権法第２７条及び第２８条の権利を含む。）を無償で譲渡するものとする。

・　受託者は、本業務の実施のために制作した著作物について、委託期間終了後、著作者人格権の行使はしないものとする。

・　本仕様書に記載のない事項又は仕様書に疑義が生じた場合は、本市と協議し、その決定に従うこと。

・　受託者は、契約期間中及び契約期間後において、本業務上知り得た秘密を第三者に漏らしてはならない。

・　受託者は、本市の文書による承認を得なければ、契約に係る義務の履行を第三者に委託し（以下「再委託」という。）、契約に係る権利を第三者に譲渡し、又は契約に係る義務を第三者に継承させてはならない。また、再委託の内容が一括再委託に該当すると判断される場合には、本市は再委託について承認しない。

・　受託者は、公金収納に当たっては、地方自治法、地方自治法施行令及び京都市会計規則その他関係法令並びに京都市業務マニュアル「公金収納受託者の収納事務」を遵守し、疑義がある場合は、委託者と協議のうえ、確認すること。

・　委託期間終了後、当該運営業務の受託者が変更になった場合は、適切に引き継ぎを行うこと。

・　受託者の提案で行う広報業務について、自由に提案を行い、本市と協議のうえ実施すること。

・　寄付者からの問合せ等に真摯に対応すること。
・　その他、業務の履行に当たり必要と認められることを適切に行うこと。

２　情報セキュリティ要件

業務に当たっては、京都市情報セキュリティ対策基準を順守し、本市が要求する情報セキュリティ水準を満たすとともに、以下の対策を講じること。

寄付申込時に取得する個人情報については、マイナンバーカードを含まない個人情報が含まれるため、以下（1）～（7）及び本市「外部サービス選定基準」の要求事項について該当するかについて必ず事前に確認しチェックを行い、プロポーザル資料ともに提出すること。

＜提出資料＞

・以下（1）～（7）についてチェックしたことが分かる資料【自由様式】

・「外部サービス選定基準」

※「外部サービス選定基準」については、情報セキュリティ上の理由より京都市情報館には公開せず窓口交付としておりますので、必ず期日前までに担当者へご連絡ください。様式をお送りします。

⑴　アクセス制御

ア　ユーザ認証

ウェブサイトのコンテンツの更新や運用保守等を行う職員等について、ユーザごとに ID を発行し、ユーザ ID 及びパスワードによる認証を行うこと。

イ　権限制御

ユーザの担当する業務及び役割等によって、ユーザごとにアクセス権限が設定でき、ユーザのアクセス権限に応じ、利用可能な機能の制御が行えること。

なお、アクセス権限は以下を想定する。

ユーザ区分	権限
システム管理者（京都創生課長を想定）	システム情報の変更、ユーザの登録、変更、削除を可能とすること。コンテンツの追加・更新・削除に関する承認を可能とすること。
保守担当者（受託事業者を想定）	システム情報の変更、コンテンツの追加、更新、削除を可能とすること。
コンテンツ作成者（京都創生担当の職員を想定）	コンテンツ情報の追加、更新、削除を可能とすること。
利用者（市民等）	コンテンツの閲覧のみ可能とすること。

ウ　パスワード管理

（ア）パスワードは、英字（大文字・小文字）、数字、記号を組み合わせた１５字以上の文字列を設定できること。

（イ）パスワードは、ユーザ自身が任意のタイミングで変更でき、システム管理者において、パスワードの有効期間を設定できること。

（ウ）パスワードを不正利用されないよう、ハッシュ化の技術を用いて保管するなど、適切に管理できること。

エ　不正ログインの防止

（ア）認証が必要な機能には、イントラネットパソコン又は保守担当者のパソコンからのみアクセ

ス可能とするよう制限を行うこと。

（イ）同一のユーザ ID によるログイン試行が５回失敗した場合は、当該ユーザ ID のアカウントロックが掛かること。

なお、アカウントロックはシステム管理者が解除できることとする。

⑵ 通信

ア　ウェブサイトで公開する全てのページについて、TLS1.2 以降により暗号化すること。

イ　暗号化に必要なサーバ証明書についても、本調達に含めること。

⑶ ログの取得

ア　ウェブサイトのアクセスログを取得すること。

イ　認証が必要な機能の操作については、ユーザ ID ごとに操作ログを取得することとし、取得した操作ログは、システム管理者がウェブサイトの画面から確認できること。

ウ　取得したログは１年間保存し、必要に応じ調査、分析できること。

⑷ バックアップの取得

ア　定期的にシステム及びデータのバックアップを取得し、システム及びデータの復旧を可能とすること。

イ　障害発生時等に、速やかにシステム及びデータを復旧できるよう機能を設計するとともに、復旧手順等を備えること。

⑸ 不正プログラム対策

不正プログラム対策として、次の要件を参考に安全性が担保される対策を講じること。

ア　サーバには、ウイルス対策ソフトを導入すること。

イ　ウイルス対策ソフトは、常に最新のバージョンを利用できるとともに、ウイルス対策ソフトの定義ファイルが更新された場合は、速やかに適用できること。

ウ　スケジューリングにより、定期的にウイルススキャンを行えること。

⑹ ぜい弱性対策

ア　導入するソフトウェアについては、修正プログラムやバージョンアップの提供等、開発元のサポートがある信頼性の高い製品を利用すること。

イ　導入した OS やソフトウェアにぜい弱性が発見された場合は、システムへの影響、重要性等を検証のうえ、速やかに修正プログラムを適用できること。

⑺ その他

ア　独立行政法人情報処理推進機構（IPA）が公開する「安全なウェブサイトの作り方」などを参考に、SQL インジェクション、クロスサイトスクリプティング等の起こりうるセキュリティ面のぜい弱性に対し、最新の対策をしたうえで導入すること。その他、情報漏えいや改ざんへの対策が十分に講じられていること。

イ　外部サービスで個人情報を含むデータを取り扱う場合は、機密性を維持するために保存時に暗号化を行うこと。また、利用を終了する場合は、そのデータが復元困難な状態となるよう消去すること。