別紙１

情報セキュリティ等に関する要件

１　情報セキュリティ要件

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 を発行すること。

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。

ウ　パスワード管理

⑺　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 10 文字以上の文字列を設定できること。

⑴　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。

⑼　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

⑺　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、IP アドレス制限や端末証明書等によるアクセス元制限を行うこと。

⑴　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。

⑼　同一のユーザ ID による複数アクセスを禁止できること。

⑵　管理者ログインについては、ID・パスワード認証に加え、より強固な認証方式（多要素認証等）を導入すること。

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を調達すること。なお、調達するサーバ証明書については、OV（Organization Validation）証明書または EV（Extended Validation）証明書のいずれかとすることが望ましい。また、サーバ証明書の有効期限が切れることのないよう、適切な時期に更新対応を実施すること。

ウ　不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離すること。なお、DB サーバ等の情報資産を扱うサーバは、DMZ[1]内に設置してはならない。

エ　通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。

[1] DMZ・・・内部ネットワークと外部ネットワークの間に設置する中間領域のこと。

オ　サービスの継続性を確保するため、システムの負荷がしきい値を超えた場合に、通信遮断や処理量の抑制等によってサービス停止の脅威を軽減する機能を備えること。

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。なお、保存場所についてはサーバ上に限定せず、調査・分析が可能であればハードディスク等への保存も認めるものとする。また、ハードディスク等へ保存する場合は、障害発生時にデータ損失やサービス停止を伴うことなく、ディスク交換および自動リビルドにより迅速に復旧できる構成とすること。

エ　ログの改ざんや削除を防止するため、ログに対するアクセス制御機能を備えるとともに、ログのアーカイブデータの保護（消失及び破壊や改ざん等の脅威の軽減）のための措置を含む設計とすること。

オ　システムに対する不正行為の検知、発生原因の特定に用いるために、システムの利用記録、例外的事象の発生に関するログを蓄積し、一定期間（要件定義時に検討）保管すること。

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

以下の対策を実施すること。

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。あわせて、サーバの負荷状況を考慮し、リアルタイムでウイルススキャンを実施できることが望ましい。

⑹　脆弱性対策

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 やソフトウェアに脆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。

ウ　システムを構成するソフトウェア及びハードウェアの脆弱性を悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。

エ　ウェブサイト構築時に、「独立行政法人情報処理推進機構（IPA）」のテクニカルウォッチに掲載された Web 脆弱性診断ツールを用いたテスト又は、「OWASP Top 10」に準拠した脆弱性診断を

行い、その結果と、全ての検出事項について対処の要否を検討し、必要な対処を行うと共に、対処不要と判断した項目については、その根拠を明らかにした文書を提出すること。

オ　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脆弱性に対し、最新の対策をした上で導入すること。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。

⑺　データ保護

ア　通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信回線を暗号化する機能を備えること。暗号化の際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。

イ　システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。また、保護すべき情報を利用者が直接アクセス可能な機器に保存しないことに加えて、保存された情報を暗号化する機能を備えること。暗号化の際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。

ウ　情報が改ざんされた場合にその事実を検知し、早期に対処できること。

⑻　その他機能

ウェブサイトの構築に当たっては、以下の機能を備えること。なお、「ア　ウェブアプリケーションファイアウォール」及び「イ　改ざん検知」については、京都 SC が提供するサービスを利用することができるものとする。ただし、当該サービスの利用に際しては、制限事項等が存在するため、事前に総合企画局デジタル化戦略推進室と協議を行い、承認を得ること。

ア　ウェブアプリケーションファイアウォール

イ　改ざん検知

ウ　NTP（時刻同期）

２　システムの拡張性等の要件

⑴　性能の拡張性

将来的にウェブサイトで取り扱うデータ量やページ数が増加した場合であっても、拡張が容易となるよう設計すること。

⑵　機能の拡張性

今後、新たな機能が追加されることを想定し、機能の追加等が容易となるよう設計すること。

⑶　上位互換性

ウェブサイトで使用する OS やソフトウェアのバージョンアップがあった場合でも、その影響が小さくなるよう設計すること。

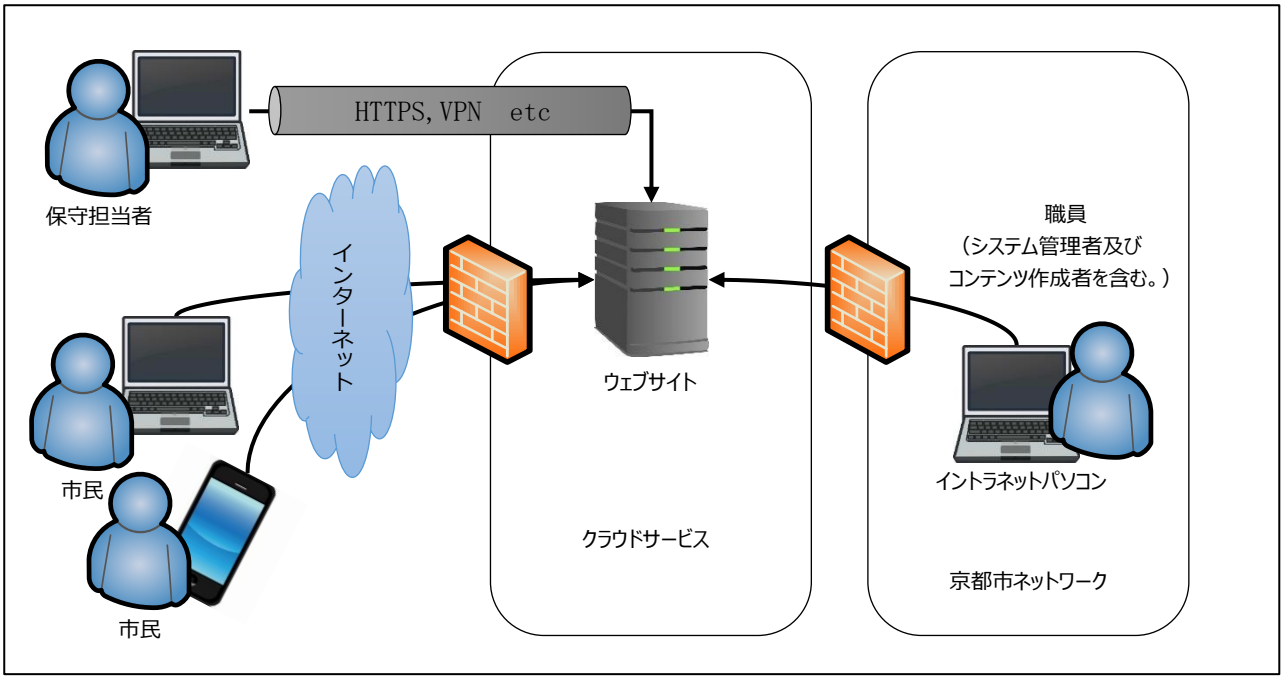
⑷　システム中立性

ア　特定の技術や製品に依存せず、継続的に安定した品質保証が受けられるオープンかつ標準的な技術を採用すること。ウェブサイトの運用保守においても、特定の事業者に依存することなく、他事業者でも変更及び引継ぎが可能であること。

イ　ウェブサイトの移行が必要となった場合に、円滑にデータ移行ができるよう、ウェブサイトで管理するデータを汎用的なデータ形式で出力できるようにすること。

3　システムの稼動環境

⑴　全体構成



ア　本業務において提供されるウェブサイトのサーバは、本市専用の環境とするものとし、他のウェブサイトと物理的または論理的にサーバを共用しないこと。

イ　ウェブサイトの構築、運用保守に当たり追加で必要となるソフトウェア、モジュール及びプラグイン等の導入、設定、運用保守及びそれに伴うウェブサーバの設定については、受託者があわせて行うこと。

ウ　ウェブサイトは次のクライアント要件をサポートすることとし、レイアウトやデザインの崩れが生じないこと。また、利用者のブラウザに対して新たなプラグイン等のインストールを求めるアプリケーションは使用しないこと。

イントラネットパソコン	OS：Microsoft Windows11 以降 ブラウザ: Microsoft Edge のほか、Mozilla Firefox、Google Chrome 等の主要なブラウザのシステム構築時点における最新版において正常に動作すること。
利用者のパソコン、 スマートフォン等	OS：Microsoft Windows、macOS、Android、iOS ブラウザ：主要なブラウザ（Microsoft Edge、Apple Safari、Mozilla Firefox、Google Chrome）のウェブサイト構築時点における最新版

⑵　ソフトウェア要件

ア　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使用すること。

イ　システム構築時点において、安全性及び安定性を確認した最新バージョンを導入すること。

ウ　セキュリティパッチ等の適用を適宜正確かつ迅速に行うこと。

⑶ ネットワーク要件

ア　イントラネットパソコンからウェブサーバへの接続は、本市既存ネットワークを使用すること。

イ　アプリケーション保守又はコンテンツ更新をリモートで実施する場合は、セキュリティを確保するため、安全性の高い回線（HTTPS、VPN、専用線等）を用いること。また、リモートアクセスに関しては、必要最小限の権限のみを付与し、利用者の管理を適切に行うこと。

⑷ ドメイン名要件

ウェブサイトのドメインは、本市が新規に取得する「city.kyoto.lg.jp」を使用したサブドメイン名を使用すること。

⑸ アクセシビリティ要件

高齢者や障害者を含めた誰もが支障なくウェブサイトを利用できるよう、「京都市ホームページ作成ガイドライン」及び総務省「みんなの公共サイト運用ガイドライン」を踏まえ、ウェブアクセシビリティに配慮すること。

なお、以下は総務省「みんなの公共サイト運用ガイドライン」で新規にホームページを構築する際に求める取組の一部を抜粋したものである。

ア　構築前に「ウェブアクセシビリティ方針」を策定すること。

イ　構築時に JIS X 8341-3:2016 の適合レベルＡＡに準拠（試験の実施と公開）すること。

4　運用の要件

⑴ 運用体制

ア　ウェブサイトの管理、運用を円滑に行うため、運用業務の統括者、電話及び電子メールによる連絡窓口を有した運用体制を整備すること。

イ　運用体制、連絡体制を明確にした運用体制図を作成し、提出すること。また、運用体制に変更があった場合は、速やかに運用体制図を更新し、提出すること。

ウ　システムの設計・開発、運用・保守工程において、本市の意図しない変更や機密情報の窃取等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。

エ　本市の意図しない変更や機密情報の窃取等が行われないことを保証するための具体的な管理手順や品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を本市との協議の上、必要と判断された場合は提出すること。また、第三者機関による品質保証体制を証明する書類等が提出可能な場合は、提出すること。

オ　システムに本市の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入検査等、本市と連携して原因を調査し、排除するための手順及び体制を整備していること（例えば、運用・保守業務におけるシステムの操作ログや作業履歴等を記録し、発注元から要求された場合には提出させるようにする等）。また、当該手順及び体制が妥当であることを証明するための書類を本市との協議の上、必要と判断された場合は提出すること。

カ　情報システムの開発・構築等の各工程において、情報セキュリティに係るサプライチェーン・リスクを低減する対策が行われていること。

⑵ 作業内容

ア　ウェブサイトの稼動時間は、24 時間、365 日とする。

イ　ウェブサイトの稼動状況、アクセス状況、リソース状況等について、定期的に確認すること。

ウ　メンテナンス等のため、ウェブサイトを停止する必要がある場合は、事前に本市の承認を得ること。

⑶ 手順書等の整備

ア　ウェブサイトの管理、運用を円滑に行うため、運用手順書を作成し、提出すること。

イ　ウェブサイトにおいて障害等が発生した場合に、速やかに初動対応や保守担当者への連絡等が行えるよう、夜間、休日を含む緊急時の連絡先等を含めた緊急時対応手順書を作成すること。

⑷ 障害対応

ア　本市から障害の連絡等を受けられる連絡体制を整備すること。なお、原則、平日（土日、祝日及び 12 月 29 日から 1 月 3 日までを除く。以下同じ。）の午前 9 時から午後 6 時までとするが、これ以外で、緊急の対応が必要となる障害が発生した場合は、可能な限り対応を行うこと。

イ　障害の連絡を受けた又は障害の発生を確認した場合は、速やかに必要な措置を取ることとし、現地確認の必要がある場合には、原則として 3 時間以内に現地へ到着すること。

ウ　障害が復旧した場合は、速やかに障害の発生状況、原因、対応等を記載した報告書を作成し提出すること。また、同様の障害が発生することを防ぐ是正措置、予防措置を実施すること。

5　保守の要件

⑴ ソフトウェア保守

ア　導入したソフトウェアにおける脆弱性の有無の確認を行うとととともに、ソフトウェアに係る修正プログラムが公開された場合は、ウェブサイトへの影響、重要性等を検証のうえ、速やかに修正プログラムを適用すること。また、修正プログラムの適用状況については本市に報告すること。

イ　レイアウトの変更等、ウェブサイトの軽微な変更、修正は、保守の範囲として対応すること。

なお、軽微な変更、修正の範囲については、本市と協議のうえ、決定することとするが、パソコンやスマートフォン等の OS やブラウザのバージョンアップに伴い、ページの表示崩れなどが発生した場合は、保守の範囲として対応すること。

ウ　導入したソフトウェア、モジュール、プラグイン等の変更にあわせてウェブサーバの設定変更が必要な場合は、保守の範囲として対応すること。

エ　不具合の修正は、保守の範囲として対応すること。

⑵ 不正プログラム対策

以下の対策を実施すること。

ア　ウイルス対策ソフトは、常に最新のバージョンを利用すること。

イ　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、速やかに適用すること。

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うこと。

６　実施体制等の要件

⑴　実施体制

ア　本業務を確実に履行できる体制を設けること。

イ　本業務の実施に当たっては、受託者においてプロジェクトマネージャを設置し、プロジェクトの進行管理を行うこと。

ウ　本市との窓口はプロジェクトマネージャが行うこと。

⑵　管理方法

受託者は、原則として情報セキュリティに係る以下のいずれかの条件を満たすこと。

- 情報セキュリティ実施基準である「JIS Q 27001」、「ISO/IEC27001」又は「ISMS」の認証を有していること。
- 財団法人日本情報処理開発協会のプライバシーマーク制度の認定を受けているか、又は同等の個人情報保護のマネジメントシステムを確立していること。
- 個人情報を扱うシステムのセキュリティ体制が適切であることを第三者機関に認定された事業者であること。

⑶　作業場所等

ア　作業場所及び開発環境等必要な機材については、受託者において用意すること。

イ　本市が承認した作業場所以外で業務を行わないこと。

⑷　システム監査（セキュリティ監査）

ア　本調達において整備・管理を行うシステムに伴うリスクとその対応状況を客観的に評価するために、本市がシステム監査（セキュリティ監査）の実施を必要と判断した場合は、本市が定めた実施内容（監査内容、対象範囲、実施者等）に基づくシステム監査を受託者は受け入れること。（契約後の委託事業開始前より実施される本市が別途選定した事業者による監査を含む。）

イ　システム監査（セキュリティ監査）で問題点の指摘又は改善案の提示を受けた場合には、対応案を本市と協議し、指示された期間までに是正を図ること。

７　制約条件

⑴　作業の実施場所は、本市が指定し、又は許可した場所で実施しなければならない。

⑵　本市のネットワークに、外部から接続することはできない。

⑶　本市のネットワークに、許可されていない端末を接続することはできない。

⑷　令和９年３月３１日までに、全ての作業を完了し、検収を受けなければならない。

⑸　導入に必要な設定変更作業は、本市と調整のうえ実施すること。

８　特記事項

⑴　この調達に係る業務を遂行するに当たって、新たに発生した設計書類等及び開発部分（市販の汎用アプリケーション等パッケージソフトに帰属する部分を除く。）の著作権（著作権法第２７条及び第２８条に規定する権利を含む。）その他権利については、本市に帰属するものとし、受託者は成果物に関する著作者人格権を行使しない。

⑵　この調達の範囲内で、第三者が権利を有する著作物又は知的所有権等を利用する場合は、受託者の

責任において、その権利の使用に必要な費用を負担し、使用許諾契約に係わる一切の手続を行う。

⑶　この調達の範囲内で、本市に帰属しない著作物がある場合にあっては、受託者は、本市に当該著作物の関連文書を成果物として納入するものとし、この関連文書についても上記⑴及び⑵に準じる。

⑷　受託者は、本仕様書によるほか、別紙１－１「電子計算機による事務処理等（システム開発・保守）の委託契約に係る共通仕様書」（以下「共通仕様書」という。）に従い本業務を遂行すること。

なお、本仕様書に定める内容と共通仕様書に定める内容との間に相違がある場合は、本仕様書に定める内容を優先するものとする。