仕 様 書

1　業務名

番号：令和７年度　（　　）　第　　号

件名：マイナンバーカード申請等オンラインサポート窓口業務委託

2　実施場所

名張市役所庁舎内

（戸籍・住民登録室の待合スペースを予定）

3 履行期間

契約日から令和８年３月３１日まで

※　サポート窓口の運用開始日は令和７年８月１日を予定。契約日から運用開始日までは、準備期間とし、必要な構築作業等を行うこと。

4 業務概要

次の業務について、パソコン端末を用いた画面共有と遠隔操作でのリモート支援、オペレーターとの対話形式（ビデオ通話）による受付・案内により手続きを完結するオンラインサポート窓口業務を行う。

（１）設置窓口数　１窓口

（２）サポートする業務メニュー

Ａ．マイナンバーカードの申請サポート

Ｂ．マイナポータル上の手続きサポート（種類は９（２）Ｂに記載のとおり）

5 サポート窓口運用日・運用時間

名張市役所開庁日の午前９時から午後４時３０分まで

※なお、午後４時３０分までに受付した利用者がいる場合は、その利用者に関するサポートが完了するまでの時間とする。

6 受注要件

受注者は次の要件をすべて満たしていること

① 情報セキュリティマネジメントシステム（ISO/IEC 27001又はJIS Q27001）を取得していること。

② 市区町村を発注者とする契約であり、専用端末を用いた画面共有と遠隔操作でのリモート支援、オペレーターとの対話形式（ビデオ通話）による受付・案内により手続きを完結するオンラインサポート窓口に係る業務委託であって、以下（ア）～（ウ）を満たす契約の履行実績を２件以上有すること。

なお、「マイナンバーカードの申請サポート」と「マイナポータル上の手続きサポート」それぞれについて、１件以上の実績を有することとし、「マイナンバーカードの申請サポート」と「マイナポータル上の手続きサポート」が同一契約の場合は、他にもう１件以上、条件を満たす契約履行実績を有すること。

（ア）「マイナンバーカードの申請サポート」又は「マイナポータル上の手続きサポート（マイナンバーカードの健康保険証利用申込及び公金受取口座の登録を含むこと）」を業務内容とするもの。

（イ）「マイナンバーカード申請のサポート」については、継続して半年以上の履行期間があり、履行完了の確認を受けているもの。

（ウ）「マイナポータル上の手続きサポート」については、継続して半年以上の履行期間があり履行完了の確認を受けているもの、又は入札公告日において契約履行中であって、履行済みの期間が継続して半年以上あるもの。

7 再委託について

受注者は、本業務の全部又は主たる部分を第三者へ委任し又は請け負わせてはならない。ただし、本業務の一部について、あらかじめのその内容を明らかにして発注者の承認を得た場合は、第三者へ委任し又は請け負わせることができる。

8 契約代金の支払い方法

履行完了後、一括払い

9 業務内容の詳細

（1）実施体制

・発注者が指定する場所に専用端末を設置し、画面共有と遠隔操作、オペレーターとの対話形式（ビデオ通話）による受付・案内により手続きを行うオンライン窓口とする。
なお、日本の法令の範囲内で運用できるサービスであること。

・クラウドサービスを利用する場合は、当該クラウドサービスのプロバイダがISO/IEC 27017を取得しているまたは、当該クラウドサービスがＩＳＭＡＰクラウドサービスリストに登録されていること。

・サポート窓口の運用時間中、常時安定的に利用できる通信環境を整備し維持すること。なお、通信にかかる費用は受注者の負担とする。

・受注者が準備する物品等は、受注者において保守管理を行うこと。

・システムや機器の不具合または災害等が発生した場合に窓口運用に制限が生じないよう、バックアップ体制を備えるとともに、窓口運用時間中、常時連絡調整を行える体制を構築すること。

・システムに障害が発生した場合は、原則として、発生から30分以内に復旧することとし、自然災害その他、障害の規模又は性質等により30分以内の復旧が困難なときは、発注者と協議のうえ復旧目標を定め、必要な対応を行うこと。

・名張市セキュリティポリシーに定める機密性２以上のデータが保存されるデータセンターは日本国内にあること。

・本業務について、発注者との連絡調整を行い、業務の履行を管理する管理責任者を選任すること。

・個人情報保護責任者（別添、個人情報の取扱いに関する特記事項第２条）及び情報セキュリティに関する総括責任者（別添、情報セキュリティ遵守特記事項第４条）を選任すること。なお、個人情報保護責任者と情報セキュリティに関する総括責任者は兼任することができる。（ただし、上記の管理責任者との兼務は不可）

・サポート窓口利用開始の操作がなされたときは、遅滞なくビデオ通話が開始できるよう、オペレーターの配置及び接続先の管理を行うこと。

・オペレーターの業務従事場所は、日本国内において受注者が管理する場所であり、必要なセキュリティが確保されていること。

・オペレーターは受注者と雇用関係にある者とし、業務に必要な知識、技能及びコミュニケーション能力を有し同一業務（マイナンバーカードの申請サポート、マイナポータルからの健康保険証利用申込み及び公金受取口座登録のサポート）に習熟した者を配置すること。

・窓口運用開始に先立ち、発注者と協議のうえ、発注者の運用に即した業務マニュアル及びＦＡＱを作成してオペレーターへの研修を行うこと。

・オペレーターについては、発注者の職員ではなく受注者の従業員であることを利用者が認識できるように名札の着用等を行うこと。

・窓口運用日における開始時の端末等及びアプリケーションの立ち上げ、並びに終了時のシャットダウンは受注者が行うこと。

・契約期間終了時に処理中の案件があるときは、発注者と協議のうえ、適宜、発注者への引継ぎを行うこと。

（２）サポート業務の内容

Ａ．　マイナンバーカードの申請サポート

マイナンバーカードの作成を希望する者に対し、J-LIS（地方公共団体情報システム機構）の規定による顔写真撮影を行うとともに、代理入力によりオンラインでの交付申請を行う。

・利用者１名ごとに、本人の意思表示に係る画面操作に基づき、サポートが開始又は終了するシステムとすること。

・利用者の意思表示に係る操作を除き、利用者による入力操作を必須とせず、利用者の負担にならない方法でサポートすること。

・端末のブラウザのパスワード保存機能、過去の入力内容の表示機能や入力予測機能等はすべて無効化又は初期化し、他者の情報が利用者の目に触れることがないようにしておくこと。

・数字23桁の申請書ＩＤが記載されているマイナンバーカード交付申請書の持参がない場合であっても、その場で利用者とのやりとりが完結するシステムとすること。（なお、個人番号は使用しないこと。）

・撮影した顔写真は、申請完了後、速やかに削除されること。

・入力内容の確認など、サポートにあたりスキャン又は撮影した画像等は使用目的を達したのち、速やかに削除すること。画面にエラーメッセージが表示された場合において個人情報を含むスクリーンショットを取得した場合も同様とする。

・サポートした対象者を発注者が把握できること。

・15歳未満の者にかかるマイナンバーカードの申請サポートにおいては、同行の法定代理人による意思表示により手続きを進めること。なお、同行者が法定代理人であることの確認は、同行者本人の自己申告によるものとする。

・ 利用者から質問や相談を受けたときは、発注者との協議により定めたマニュアル等に基づき、対応すること。

・万一、申請が不備となったときは、受注者より利用者へ説明及び再申請の案内を行うこと。なお、発注者においても不備の発生及び再申請の有無が確認できる仕組みとすること。

B． マイナポータル上の手続きサポート（３種類以内）

マイナポータル上の手続き希望する者に対し、サポート窓口の端末を使用し、オペレーターが遠隔操作により手続きを先導する。

サポートする手続きのメニューについては、マイナンバーカードの健康保険証利用申込み及び公金受取口座の登録とするが、窓口の利用状況に応じ、もう１種類追加する場合がある。（追加する期間及び種類については、別途、発注者と受注者が協議のうえ定める。）

・利用者１名ごとに、本人の意思表示に係る画面操作に基づき、サポートが開始又は終了するシステムとすること。

・端末のブラウザのパスワード保存機能、過去の入力内容の表示機能や入力予測機能等はすべて無効化又は初期化し、他者の情報が利用者の目に触れることがないようにしておくこと。

・利用者の意思表示に係る操作及び暗証番号の入力を除き、利用者による入力操作を必須とせず、利用者の状況に応じ手続きが円滑に完結するサポート方法を選択すること。

・手続きに使用するマイナンバーカードが利用者本人のものであることについて、確認したのち、サポートを開始すること。なお、確認方法は、利用者本人の自己申告によるものとするが、自己申告を受けたことを記録すること。（なお、個人が特定できる情報は記録に含めないこと）

・健康保険証利用申込み又は公金受取口座登録において、15歳未満の者にかかるサポートにおいては、法定代理人による意思表示及び暗証番号の入力により手続きを進めること。なお、同行者が法定代理人であること及び使用するマイナンバーカードが法定代理権の対象である15歳未満の者本人にかかるものであることについて、法定代理人の自己申告を受け、自己申告を受けたこ

とを記録すること。（なお、個人が特定できる情報は記録に含めないこと）

・健康保険証利用申込みについては、申込状況の確認や登録内容の閲覧についてもサポートを行うこと。

・公金受取口座登録については、登録口座の変更、削除、及び登録内容の閲覧についてもサポートを行うこと。

・ 利用者から質問や相談を受けたときは、発注者との協議により定めたマニュアル等に基づき、対応すること。

（3）物品等の調達・設置

・下表のとおり物品を調達し、業務可能な状態を整備すること。
・物品の搬入設置の日時は、発注者と調整すること。
・サポート窓口運用開始前に、テスト稼働させ、発注者の確認を受けること。

発注者が用意する物品等	受注者が用意する物品等
窓口スペース	申請支援、写真撮影、ビデオ通話ができるサポート窓口用端末一式 ・タッチパネル式モニター（画面サイズ20インチ程度） ・代理入力補助用書類（交付申請書記載の申請書IDなど）を判読するためのスキャナー又はカメラ ※ ※ 顔写真撮影に使用するカメラはマイナンバーカードオンライン申請に必要な画素数を有すること
機材の電源設備	通信用 Wi-Fiルータ ※ 円滑に業務が実施できる安定した通信及び速度を確保できるもの
机	暗証番号入力用テンキー
利用者用椅子　２脚	ＩＣカードリーダー（マイナンバーカード読取用）
市民向けチラシ （カード受取方法の案内など）	ヘッドセット（マイク付きヘッドホン）
	目隠し用ついたて
	写真背景用スクリーン（目隠し用ついたてとの兼用可）
	照明（現地の状況に応じ、写真撮影用に必要な場合）
	その他サポート業務の実施に必要な物品等

（４）管理業務

① 契約締結時の提出書類

受注者は、契約締結後、速やかに次の報告書等を提出すること。

・連絡体制図（発注者との連絡調整を行う管理責任者の報告書を兼ねる）

・個人情報の管理体制等報告書（別添、個人情報の取扱いに関する特記事項第５条）

・情報管理体制報告書情報（別添、情報セキュリティ遵守特記事項第４条）

・オペレーター業務従事者届（業務に従事する場所、氏名、経験年数を記載。従事者の追加及び変更があるときは、変更届を提出すること）

② 履行状況報告

毎月、当月分のメニュー別サポート件数を記載した実績報告書を作成し、翌月10日までに提出すること。最終月の報告においては、年間の合計サポート件数等を記載した委託業務完了報告書を提出すること。

なお、報告書の記載事項等については、別途協議のうえ定める。

③ サービスレベルの維持向上のための取組

・本業務はオペレーターのスキルレベルが重要であるため、すべてのオペレーターが同じレベルの対応ができるよう、教育の徹底と監督を行うこと。

・業務マニュアルやＦＡＱは、利用者からの質問内容や発注者からの要請に基づき、随時更新し、発注者からの要請以外の更新については、軽微な変更を除き、発注者に遅滞なく報告し、確認を受けること。

・業務マニュアルやＦＡＱの更新にあたっては、常に報道機関やＳＮＳ等で発信されているマイナンバーやマイナンバーカードに関する情報を収集し、利用者の質問を理解できる知識を持つとともに、誤った情報を伝えることがないよう、発注者との情報共有に留意すること。

・利用者から苦情や意見があったときは、速やかに発注者と情報を共有し、必要に応じてその解決を図ること。

・利用者の安心と信頼を得られるよう、オペレーターの服務規律（服装、態度、言葉遣い等）の管理を徹底すること。

10 法令遵守

受注者は、関係法令、名張市の条例、規則、本仕様書、別添「個人情報の取扱いに関する特記事項」並びに「情報セキュリティ遵守特記事項」、及び個人情報保護委員会が定める「個人情報の保護に関する法律についてのガイドライン」並びに「特定個人情報の適正な取扱いに関するガイドライン」を遵守すること。

11　情報セキュリティ対策

別添、情報セキュリティ遵守特記事項の詳細規定として、本業務に使用する情報システム（名張市セキュリティポリシーに定める機密性２以上の情報を取り扱うシステムに限る。以下「システム」という。）の構築、運用及び管理等に関し、以下のとおり定める。

〔基本事項〕

（１）管理体制

①　システムの開発及び運用が発注者の意図しない変更が行われない一貫した品質保証体制の下でなされていること。

②　発注者の意図しない変更が行われるなどの不正が見つかった際に追跡調査や立ち入り検査等、発注者と受注者が連携して原因を究明できる体制が整備されていること。

（２）情報セキュリティインシデント対応

情報セキュリティインシデントが発生した際に、システムの運用状況・影響範囲調査等、事案解決のための調査が可能なこと。

（３）履行状況の確認

発注者によるセキュリティ監査・検査及び外部監査法人によるセキュリティ監査の対象となった場合は、積極的に協力すること。

（４）業務中断・終了時の対応

①　システムを変更しようとするときは、事前に発注者と協議し、セキュリティ要件の確認を受けること。また、変更に際し業務の中断を生じさせないこと。

②　業務の中断が生じたとき又は業務を継続できなくなったときは、市民サービス継続のために必要なデータを発注者が利用可能な形式でセキュリティを確保した方法により引き継ぐこと。

（５）セキュリティ対策

①　障害発生時の状況から影響範囲が調査できるよう、システムログ及びアプリケーションログを取得すること。またそれらの情報についての改ざん、消去、破壊などを防止できる機能を設けること。

②　本業務に係るインターネット接続点の通信を監視していること。

③　脆弱性検査ツールを用いた手法やペネトレーションテスト等により脆弱性診断を実施し必要な対策を実施していること。

〔構築時の対策〕

（１）不正なアクセスを防止するためのアクセス制御

①　インターネット接続にあたっては、情報セキュリティインシデントの早期発見と対処及び他のネットワークへの不適切なアクセス等の監視等の情報セキュリティ

対策を講じなければならない。

② 管理者特権を有する利用者の認証については、多要素主体認証方式等による不正な管理者権限利用の防止が可能なこと。

③ パスワードの管理機能について概ね以下の機能を備えていること

・長さが10文字以上の制限
・英大文字、英小文字、記号及び数字を含める制限
・過去に使用したパスワードを利用できないように制御
・パスワードを暗号化した状態で保存

④ 保存される情報や機能ごとにアクセスする権限を有しない職員がアクセスできないように制限できる仕組みがあること。

⑤ データベースの中身を強制的に書き換えることができる機能や一時的にポートを開放する機能等のユーティリティプログラムが存在する場合、他のセキュリティ対策等に影響がない機能となっていること。

⑥ 仮想マシン（ソフトウェアによって仮想的に再現された物理的なコンピュータと同等の機能を有するコンピュータ）を設定する際に不正プログラム対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策、ログ取得等の実施）を確実に実施できること。SaaSを利用する場合は、これらの対応が受注者側でされること。

（２）機密性保護のための暗号化

① 情報資産の保存場所及び通信経路全般において機密性保護のための暗号化が行われていること。

② 利用する暗号化方式は、「電子政府推奨暗号リスト」に記載された暗号化方式であること。「電子政府推奨暗号リスト」に記載されていない暗号化方式を採用する場合、「推奨候補暗号リスト」や「運用関し暗号リスト」を参照のうえ、リスクを低減するために十分な強度をもち、実際にデータを送受信し復号できることを確認する等により、他の情報システムとの連携に問題がないことを確認すること。

③ 本業務において利用する暗号における一連の管理策が、関連する協定、法令及び規制を遵守していること。「電子政府推奨暗号リスト」に記載されていない暗号化方式を利用する場合、特に輸出規制等に抵触していないこと。

（３）開発時におけるセキュリティ対策

情報セキュリティに配慮した開発の手順が実践されていること。

（４）設計・設定時の誤りの防止

① セキュリティ要件が異なるネットワークを接続する場合、これらの間の通信（トラフィック）を監視、制御していること。なお、設定は定期的な見直しを行うこと。

② 利用実績に応じて自動的にリソースを増減させる場合、リソース不足によりシステム運用が停止しないように適切に監視を行うこと。

③ データ容量や稼働性能の監視と将来予測を行うなどにより、リソース不足によりシステムの稼働に支障をきたさないよう、必要な措置を講じること。

④　確実に時刻が同期するように設計すること。

〔運用・保守時の対策〕

（１）取り扱う資産の管理

①　ウェブサイトの脆弱性対策については、独立行政法人情報処理推進機構（IPA）「安全なウェブサイトの作り方（改訂第7版）」に準拠していることを確認し、脆弱性が発見された場合は、速やかに対策を講じるとともに、必要に応じ発注者に報告すること。

②　システムを構成する機器及びソフトウェアに関する脆弱性対策として以下を実施すること。

ア　関係するセキュリティ情報を常時入手すること。

イ　システムを構成するソフトウェアの脆弱性を悪用した不正を防止するため、脆弱性の有無を確認のうえ、運用上対処が必要な脆弱性は直ちに修正すること。また把握した脆弱性の内容及び対処について、必要に応じ発注者に報告すること。

ウ　システムを構成するＯＳ、ミドルウェア及びソフトウェア等はサポート期限内のものを用いること。

（２）不正アクセスを防止するためのアクセス制御

①　管理者権限を持つ者の操作等について、すべて記録され、保存されること。

②　不正利用を検知することが可能な監視機能を有していること。

（３）機密性保護のための暗号化

①　暗号化に用いる鍵の保管場所は国内のサーバであること。

②　暗号化に用いる鍵を受注者が保管する場合、鍵が窃取される可能性や危殆化した技術等の利用等がなく、安全に管理・利用可能なこと。

（４）通信制御

システム基盤内において、発注者が利用するネットワークが他のテナント及び受注者が利用するネットワークと分離され、論理的に独立していること。

（５）事業継続

不測の事態に対してサービスの復旧を行うため、日次でバックアップを取るとともに、定期的に訓練を実施する等によりバックアップから速やかに復旧できる体制を維持継続すること。

〔更改・廃棄時の対策〕

（１）取り扱った情報の廃棄

①　以下を例とする取扱ったすべての情報がシステム基盤上から確実に削除可能なこと。なお、削除する対象はバックアップ等により複製されたものも含む。

ア　保存されたデータ

イ　仮想リソース（仮想マシン、仮想ストレージ、仮想ネットワーク機器など）

ウ　ファイル（ストレージサービスに格納したファイル、各サービスのログ、開発関連ファイル、設定ファイルなど）

エ　暗号化された情報の復号に用いる鍵

オ　ドメイン情報

② 暗号化された情報の廃棄は、復号に用いる鍵のバックアップを含め、確実な廃棄を行うこと。

③ 廃棄の実施報告書が提出可能なこと。

④ 装置等を処分する際は、セキュリティを確保した対応を行うこと。

⑤ 処分の確認にあたり、受注者が発注者に提供可能な第三者による監査報告書や認証等を取得していること。

（2）本業務のために作成したアカウントの廃棄

① 発注者の利用環境における管理者アカウントは再利用されないこと。

② ストレージアカウントなど特殊なアカウントを作成した場合は、契約終了時に確実に削除できること。また、特殊なアカウントを利用して作成された情報についても確実に廃棄されること。

12　違約金

受注者は、システム障害等により、終日（9：00から16：30）サポート窓口を運用できない日が発生したときは、運用中断日１日につき未履行部分相当額の2,000分の１に相当する額を違約金として発注者へ支払わなければならない。ただし、運用中断が受注者の責めによらない事由によるときはこの限りではない。

なお、名張市契約規則第44条第１項の規定により業務の履行を一時中止した場合、その日数は、前記の運用中断日数に含まない。

13　一般的損害

業務の完了前に、業務の履行につき生じた損害（14の（１）又は（２）に規定する損害を除く。）については、受注者がその費用を負担する。ただし、その損害のうち発注者の責めに帰すべき事由により生じたものについては、発注者が負担する。

14　第三者に及ぼした損害

（1）業務の履行につき第三者に及ぼした損害について、当該第三者に対して損害の賠償を行わなければならないときは、受注者がその賠償額を負担する。

（2）前記（１）の規定にかかわらず、（１）に規定する賠償額のうち、発注者の指示その他発注者の責に帰すべき事由により生じたものについては、発注者がその賠償額を負担する。ただし、受注者が、発注者の指示が不適当であること等発注者の責めに帰すべき事由があることを知りながらこれを通知しなかったときは、この限りではない。

（3） 前記（１）（２）の場合その他業務の履行につき第三者との間に紛争を生じた

場合は、発注者及び受注者は協力してその処理解決に当たるものとする。

15　その他

（1）この契約に係る訴訟の提起又は調停の申立てについては、日本国の裁判所をもって合意による専属的管轄裁判所とする。

（2）本仕様書に記載のない事項は、発注者と受注者が協議のうえ定める。